# SSG EAP Transparency

The SSG EAP Transparency feature allows the Cisco Service Selection Gateway (SSG) on a Cisco router to act as a RADIUS proxy during Extensible Authentication Protocol (EAP) authentication and to create the host. This feature also prevents of the use of previously valid IP addresses after an Access Zone Router (AZR) reboot and allows EAP users who have logged out to reconnect through Subscriber Edge Services Manager (SESM).

### Feature History for the SSG EAP Transparency Feature

| Release | Modification |
|---|---|
| 12.2(16)B | This feature was introduced. |
| 12.3(4)T | This feature was integrated into Cisco IOS Release 12.3(4)T. |

### Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

# Contents




**Corporate Headquarters:**
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

# Prerequisites for SSG EAP Transparency

The SSG EAP Transparency features operates in the environment described in the "SSG EAP Environment" section on page 3. Before you can use this feature, you must set up each of the components of the environment, as specified in other Cisco documents.

The SSG EAP Transparency feature has the following requirements:

- You must set up the SSG RADIUS proxy feature on the router that has SSG. It enables the SSG to be aware of EAP authentication and process the user's SSG service information sent in the Access-Accept packet. You also must configure the access point (AP) and AZR as the RADIUS proxy client.
- The AP must use SSG as the authentication, authorization, and accounting (AAA) server for EAP authentication.
- The AZR must use the Domain Host Configuration Protocol (DHCP) accounting feature and the Address Resolution Protocol (ARP) log feature.
- SESM must be in RADIUS mode.

# Information About SSG EAP Transparency

To use SSG EAP transparency, you should understand the following concepts:



## EAP Implementations Supported by SSG

SSG supports the following EAP implementations, which are designed to support 802.1x requirements for public wireless LANs (PWLANs) and Ethernet LANs:

- EAP-Subscriber Identity Module (SIM)
- EAP-Transport Layer Security (TLS)
- Microsoft Protected Extensible Authentication Protocol (PEAP)
- Any other EAP mechanisms that use Microsoft Point-to-Point Encryption (MPPE) to share Wired Equivalent Privacy (WEP) keys

**Note** SSG does not terminate native EAP messages. SSG supports EAP transparency by looking at the RADIUS packets generated by APs or switches.

# SSG EAP Environment

EAP authentication is an enhancement to Global System for Mobile communications (GSM) authentication and operates over the IEEE 802.1x standard. The Cisco implementation of EAP transparency for PWLANs operates in conjunction with the following components:

- Wireless LAN (WLAN) Access Point (AP)— A Network Access Server (NAS) to which wireless device users connect to this to reach the network. APs have radio channels on the user side and IP infrastructure on the network side.
- Access Zone Router (AZR)—A router that represents a "hotspot," or access zone, and serves multiple clients in a populated area, such as an airport or coffee shop. Multiple Access Points are served by one AZR. The AZR is also the DHCP server for clients. The AZR is generally a lower-end Cisco router such as a Cisco 1700 or Cisco 2600-XM series routers.
- Cisco Service Selection Gateway (SSG)—A Cisco IOS feature that implements Layer 3 service selection through selective routing of IP packets to destination networks on a per-subscriber basis. When configured as a RADIUS proxy between a WLAN AP and the corresponding AAA server, SSG enables users to access SSG functionality after they connect to the AP.
- Subscriber Edge Services Manager (SESM)—An extensible set of applications for providing support for on-demand value-added services and access control at the network edge. Together with the SSG, SESM provides subscriber authentication, service selection, and service connection capabilities to subscribers of Internet services. Subscribers interact with an SESM web application and portal using a standard Internet browser. In RADIUS mode, SESM obtains subscriber and service information from a RADIUS server. (SESM in RADIUS mode is similar to the Cisco Service Selection Dashboard (SSD), which was replaced by SESM.)
- Authentication, authorization, and accounting (AAA) server—This server validates the claimed identity of a user device, grants access rights to a user or group, records who performed a certain action, and tracks user connections and certain activities, such as service and network resource usage. An AAA database is managed and accessed by a RADIUS security server.
- RADIUS server—An access server that uses the AAA protocol. It is a system of distributed security that secures remote access to networks and network services against unauthorized access. The server runs on a central computer, typically at the customer's site, and the clients reside in the dialup access servers and can be distributed throughout the network.
- Signaling System 7 (SS7) network—A system that stores information that is required for setting up and managing telephone calls on the public switched telephone network (PSTN). The information is stored on a network separate from the network on which the call was made. The AAA server communicates with a Cisco IP Transfer Point (ITP), which acts as a gateway between the IP and SS7 networks. Using Mobile Application Part (MAP) messages, the system gets user service profiles from the subscriber's Home Location Register (HLR). In addition, the system includes an authentication center (AuC), which provides authentication and encryption parameters to verify each user's identity and ensure call confidentiality.

On the client side, the EAP protocol is implemented in the EAP supplicant. The supplicant code is linked into the EAP framework provided by the operating system; currently, supplicants exist for Microsoft Windows XP and Windows 2000. The EAP framework handles EAP protocol messages and communications between the supplicant and the AAA server; it also installs any encryption keys provided to the supplicant in the client's WLAN radio card.

On the network side, the EAP authenticator code resides on the service provider's AAA server. Besides handling the server side of the EAP protocol, this code is also responsible for communicating with the service provider's AuC. In a Cisco implementation of EAP, the AAA server communicates with a Cisco IP transfer point (ITP). The Cisco ITP translates messages from the AAA server into standard GSM protocol messages, which are then sent to the AuC.

# EAP Transparency

The SSG EAP Transparency feature allows SSG on a Cisco router to act as a RADIUS proxy during EAP authentication. SSG creates the host after successful EAP authentication, so the user does not have to log in through the web portal. Instead, the user is automatically logged in.

The AP does the authentication for the client. SSG looks like a AAA server, which proxies relevant packets to the real AAA server. To create a host automatically, SSG has to know that the authentication was successful. By proxying messages, it obtains this information. The IP address is not assigned until authentication is complete, so SSG creates an inactive host and uses the MAC address as an identifier. To get the IP address, it waits for a DHCP Accounting Start from the AZR, so the AZR must be configured as an SSG RADIUS proxy client.

# Prevention of IP Address Reuse

When the AZR reboots, it sends Accounting On/Off packets. SSG receives these packets and, even though EAP users may be connected, it moves hosts to the inactive state and starts an inactive-period timer. During the DHCP renewal, the AZR performs an ARP lock and sends an Accounting Start packet to SSG. After receiving an Accounting Start packet, SSG activates the corresponding hosts using the MAC address as the identity. If the inactive-period timer expires, SSG removes all of the inactive hosts.

This functionality prevents the use of previously valid IP addresses after an AZR reboot. It closes a security hole that could allow an illegal user to hijack the session of a valid user through the IP address, and at the same time it removes the inconvenience of reauthentication for the user. In order to prevent the reuse of IP addresses, clients must be configured with a short DHCP lease interval. If users are not configured with a short lease interval, they will have to reauthenticate whenever the AZR reboots.

# User Reconnect

The SSG EAP transparency implementation allows EAP users to access the SESM, perform an account logoff, and access the SESM again later without having to log on. Without the user reconnect functionality, EAP users that attempt to reconnect to SESM after having logged off are presented with the SESM logon page. Because the initial authentication is performed by the EAP mechanism, EAP users do not know their credentials (username and password information) for SESM login, so they are unable to access SESM services again.

The following steps describe the SSG EAP transparency user reconnect process:

1. The user connects to SSG via an EAP mechanism, and SSG creates the host (as explained in the "EAP Transparency" section).
2. The user accesses the SESM. The SESM queries SSG about the user, and SSG provides the SESM with the user profile information. The SESM displays the service logon page for the user to select services.
3. When the EAP user logs off the SESM, SSG does not remove the host (as it does for other types of users), but rather inactivates the host.
4. The user attempts to access the SESM again to use a service. The SESM queries SSG. SSG activates the host and enables autologon services.

SSG deletes an active or inactive host when it receives an Accounting Stop packet from the AZR.

The SSG EAP transparency user reconnect functionality can be enabled or disabled using the command-line interface, as described in the "How to Enable SSG EAP Transparency" section on page 5.

**Note** If user reconnect is enabled and a user refreshes or reloads the SESM page after an account logoff, SESM sends a query to SSG, which causes SSG to activate the host. It is recommended that users be made aware of this behavior so they do not accidentally activate the host.

# How to Enable SSG EAP Transparency

This section contains the following procedures:


- Configuring SSG EAP Transparency, page 5
- Enabling EAP User Reconnect, page 7


## Configuring SSG EAP Transparency

Perform this task to enable SSG to receive and forward EAP packets.

### Prerequisites

The SSG EAP transparency feature has the following requirements:

- You must set up the SSG RADIUS proxy feature on the router that has SSG. It enables the SSG to be aware of EAP authentication and process the user's SSG service information which is sent in the Access-Accept packet. You also must configure the AP and AZR as the RADIUS proxy client.
- The AP must use SSG as the AAA server for EAP authentication.
- The AZR must use the DHCP Accounting feature.
- The SESM must be in RADIUS mode.

#### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ssg enable**
4. **ssg radius-proxy**
5. **client-address** *IP-address*
6. **key** *secret*
7. **session-identifier** {**auto** | **msid** | **correlation-id** | **accounting-session-id**}
8. **timeouts**
9. **idle** *timeout*
   or
   **ip-address** *timeout*
10. **exit**
11. **exit**
12. Repeat Steps 5 to 9 to configure the AZR as a RADIUS client.

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **ssg enable**<br><br>**Example:**<br>`Router(config)# ssg enable` | Enables SSG. |
| **Step 4** | **ssg radius-proxy**<br><br>**Example:**<br>`Router(config)# ssg radius-proxy` | Enables SSG RADIUS proxy and SSG-radius-proxy configuration mode. |
| **Step 5** | **client-address** *IP-address*<br><br>**Example:**<br>`Router(config-radius-proxy)# client-address 123.123.123.123` | Configures the RADIUS client IP address.<br>• Use this command to configure the AP as a RADIUS client to proxy requests from the specified IP address to the RADIUS server. |
| **Step 6** | **key** *secret*<br><br>**Example:**<br>`Router(config-radproxy-client)# key cisco` | Configures the shared secret.<br>• Use the *secret* argument to configure each client IP with a unique shared secret. This shared secret should be the same one that is configured on the RADIUS client. |
| **Step 7** | **session-identifier** {**auto** \| **msid** \| **correlation-id** \| **accounting-session-id**}<br><br>**Example:**<br>`Router(config-radproxy-client)# session-identifier auto` | (Optional) Overrides the SSG automatic RADIUS client session identification. Keywords are as follows:<br>• **auto**—Automatically determines the session identifier.<br>• **msid**—Uses the MSID as the client session identifier.<br>• **correlation-id**—Uses the Correlation-ID as the session identifier.<br>• **accounting-session-id**—Uses the Accounting-Session-ID as a session identifier. |
| **Step 8** | **timeouts**<br><br>**Example:**<br>`Router(config-radproxy-client)# timeouts` | (Optional) Enters SSG-Radius-Proxy-Timeouts mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 9** | **idle** *timeout*<br>or<br>**ip-address** *timeout*<br>**Example:**<br>`Router(config-radproxy-timer)# idle 30` | (Optional) Specifies a timeout value. Use one of two commands:<br>• The first command configures a host object timeout value. The valid range is from 30 to 65536 seconds.<br>• The second command configures an SSG RADIUS proxy IP address timeout. The valid range is from 1 to 180 seconds. |
| **Step 10** | **exit**<br>**Example:**<br>`Router(config-radproxy-timer)# exit` | Exits to SSG-radius-proxy-client configuration mode. |
| **Step 11** | **exit**<br>**Example:**<br>`Router(config-radproxy-client)# exit` | Exits to SSG-radius-proxy configuration mode. |
| **Step 12** | Repeat Steps 5 to 9 to configure the AZR as a RADIUS client. | |

# Enabling EAP User Reconnect

Perform this task to enable EAP users to reconnect to SESM services after they log off or an idle timeout occurs.

## EAP User Reconnect After Logoff

EAP users do not have a username and password as other types of SSG users do. If they access SESM, log off, and try to reconnect to the service later, SESM presents them with a logon page, which they cannot use. To allow EAP users to reconnect without being asked to log on again, enable the user reconnect functionality with the **ssg wlan reconnect** command.

When this functionality is enabled, if a user logs off through SESM or an idle timeout occurs, SSG inactivates the host. If the user tries to access the network or service again, SESM queries SSG, and SSG activates the host and enables autologon services.

The SSG host, whether active or inactive, is deleted when the AZR sends an Accounting Stop packet to SSG (when the user walks out of the PWLAN or the DHCP address is released).

**Note** If user reconnect is enabled and a user refreshes or reloads the SESM page after an account logoff, SESM sends a query to SSG, which causes SSG to activate the host It is recommended that users be made aware of this behavior so they do not accidentally activate the host.

## Prerequisites

SSG EAP transparency must be configured before you can use EAP user reconnect.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ssg enable**
4. **ssg radius-proxy**
5. **client-address** *IP-address*
6. **key** *secret*
7. **exit**
8. **exit**
9. **ssg wlan reconnect**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **ssg enable**<br><br>**Example:**<br>`Router(config)# ssg enable` | Enables SSG. |
| **Step 4** | **ssg radius-proxy**<br><br>**Example:**<br>`Router(config)# ssg radius-proxy` | Enables SSG RADIUS proxy and enters SSG-radius-proxy mode. |
| **Step 5** | **client-address** *IP-address*<br><br>**Example:**<br>`Router(config-radius-proxy)# client-address 10.10.10.10` | Configures the RADIUS client to proxy requests from the specified IP address to the RADIUS server and enters SSG-radius-proxy-client mode. |
| **Step 6** | **key** *secret*<br><br>**Example:**<br>`Router(config-radproxy-client)# key cisco` | Configures the shared secret.<br>• Use the *secret* argument to configure each client IP with a unique shared secret. This shared secret should be the same one configured on the RADIUS client. |
| **Step 7** | **exit**<br><br>**Example:**<br>`Router(config-radproxy-client)# exit` | Exits to SSG-Radius-Proxy mode. |

| | Command or Action | Purpose |
|---|---|---|
| Step 8 | **exit**<br><br>**Example:**<br>`Router(config-radius-proxy)# exit` | Exits to global configuration mode. |
| Step 9 | **ssg wlan reconnect**<br><br>**Example:**<br>`Router(config)# ssg wlan reconnect` | Enables EAP users to reconnect after logging off or having idle time out occur. |

# Configuration Examples for SSG EAP Transparency

This section contains the following configuration example:

- SSG EAP Transparency and User Reconnect Configuration: Example, page 9

## SSG EAP Transparency and User Reconnect Configuration: Example

The following example shows the configuration of SSG EAP transparency with EAP user reconnect:

```
.
.
.
radius-server host 9.2.36.253 auth-port 1645 acct-port 1646 key cisco

ssg enable

ssg radius-proxy
 server-port auth 1645 acct 1646
 client-address 1.1.1.1
  key cisco
  session-identifier auto
!
 client-address 1.1.1.1
  key cisco
!
  timeouts
   ip-address 60
!

ssg wlan reconnect
```

# Additional References

For additional information related to SSG EAP transparency, consult the following references:

## Related Documents

| Related Topic | Document Title |
|---|---|
| SSG commands | *Cisco IOS Wide-Area Networking Command Reference*, Release 12.3 T |
| SSG configuration tasks | *Service Selection Gateway,* 12.3(4)T new-feature document |
| | *Service Selection Gateway Accounting Update Interval per Service*, 12.2(13)T new-feature document |
| | *Service Selection Gateway Hierarchical Policing*, 12.2(13)T new-feature document |
| | *SSG AutoDomain*, 12.2(13)T new-feature document |
| | *SSG Autologoff Enhancement*, 12.3(4)T new-feature document |
| | *SSG Autologon Using Proxy Radius*, 12.2(13)T new-feature document |
| | *SSG Autologoff*, 12.2(13)T new-feature document |
| | *SSG Proxy for CDMA2000,* 12.3(4)T new-feature document |
| | *SSG Direction Configuration for Interfaces and Ranges*, 12.3(4)T new-feature document |
| | *SSG EAP Transparency*, 12.3(4)T new-feature document |
| | *SSG L2TP Dial-Out*, 12.3(4)T new-feature document |
| | *SSG Open Garden*, 12.2(13)T new-feature document |
| | *SSG Port-Bundle Host Key*, 12.2(13)T new-feature document |
| | *SSG Prepaid*, 12.2(13)T new-feature document |
| | *SSG Prepaid Idle Timeout*, 12.3(4)T new-feature document |
| | *SSG Service Profile Caching*, 12.3(4)T new-feature document |
| | *SSG Suppression of Unused Accounting Records*, 12.3(4)T new-feature document |
| | *SSG TCP Redirect for Services*, 12.2(13)T new-feature document |
| | *SSG Unconfig*, 12.3(4)T new-feature document |
| | *SSG Unique Session ID*, 12.3(4)T new-feature document |
| SESM | *Cisco Subscriber Edge Services Manager and Subscriber Policy Engine Installation and Configuration Guide* |
| | *Cisco Service Selection Dashboard Installation and Configuration Guide* |
| | *Cisco Service Selection Dashboard Web Developer Guide* |
| RADIUS commands | *Cisco IOS Security Command Reference*, Release 12.3 T |

| Related Topic | Document Title |
|---|---|
| RADIUS configuration tasks | *Cisco IOS Security Configuration Guide* |
| DHCP accounting | *DHCP Accounting* new-feature document |

## Standards

| Standards | Title |
|---|---|
| IEEE 802.1x | *Port Based Network Access Control* |
| European Telecommunication Standardization Institute (ETSI) Global System for Mobile communication (GSM) standards | GSM standards |

## RFCs

| RFCs | Title |
|---|---|
| RFC 2284 | *PPP Extensible Authentication Protocol* |
| RFC 2865 | *Remote Authentication Dial-In User Services (RADIUS)* |
| RFC 2869 | *RADIUS Extensions* |
| RFC 2548 | *Microsoft Vendor-Specific RADIUS Attributes* |

## Technical Assistance

| Description | Link |
|---|---|
| Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content. | http://www.cisco.com/public/support/tac/home.shtml |

# Command Reference

This section documents the **ssg wlan reconnect** command. All other commands used with this feature are documented in the Cisco IOS Release 12.3 T command reference publications.

# ssg wlan reconnect

To enable Extensible Authentication Protocol (EAP) users to reconnect after logging off or after idle timeout has occurred, use the **ssg wlan reconnect** command in global configuration mode. To disable the ability of EAP users to reconnect, use the **no** form of this command.

**ssg wlan reconnect**

**no ssg wlan reconnect**

## Syntax Description

This command has no arguments or keywords.

## Defaults

EAP users cannot reconnect.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(16)B | This command was introduced. |
| 12.3(4)T | This command was integrated into Cisco IOS Release 12.3(4)T. |

## Usage Guidelines

EAP users do not have a username and password. If they access Subscriber Edge Services Manager (SESM), log off, and try to reconnect to the service later, SESM presents them with a logon page, which they cannot use. To allow users to reconnect without being asked to logon again, enable the user reconnect feature with the **ssg wlan reconnect** command.

When the SSG EAP transparency user reconnect functionality has been enabled, if a user logs off through SESM, Service Selection Gateway (SSG) inactivates the host. If the user tries to access the service again, SESM queries SSG, and SSG activates the host and enables autologon services.

The SSG host, whether active or inactive, is deleted when the Access Zone Router (AZR) sends an Accounting Stop packet to SSG (when the user walks out of the private wireless LAN (PWLAN) or the Dynamic Host Configuration Protocol (DHCP) address is released).

**Note** If user reconnect is enabled and a user refreshes or reloads the SESM page after an account logoff, SESM sends a query to SSG, which causes SSG to activate the host. It is recommended that users be made aware of this behavior so they do not accidentally activate the host.

## Examples

The following example enables EAP users to reconnect after logging off:

```
ssg wlan reconnect
```

# Glossary

**AAA**—authentication, authorization, and accounting. *Authentication* is the process of validating the claimed identity of an end user or a device, such as a host, server, switch, or router router. *Authorization* is the act of granting access rights to a user, groups of users, system, or a process. *Accounting* refers to the methods to establish who or what performed a certain action, such as tracking user connections and logging system users.

**Access-Accept**—Response packet from the RADIUS server notifying the access server that the user is authenticated.

**AP**—access point. In a WLAN, a station that transmits and receives data. It can be used to connect network users with each other and to connect the WLAN to a fixed wire network.

**ARP**—Address Resolution Protocol. Internet protocol used to map an IP address to a MAC address. It is defined in RFC 826.

**AuC**—authentication center. A protected database that provides authentication and encryption parameters to verify user identities and ensure the confidentiality of each call as a protection against fraud.

**AZR**—Access Zone Router. On a WLAN, represents a "hotspot," or access zone, which serves multiple clients in a populated area, such as an airport or coffee shop. Multiple access points are served by one AZR. The AZR is also a DHCP server for clients.

**DHCP**—Dynamic Host Configuration Protocol. A communications protocol that allows the central management and automatic assignment of IP addresses in an organization's network.

**EAP**—Extensible Authentication Protocol. Framework that supports multiple optional authentication mechanisms for PPP, including cleartext passwords, challenge-response, and arbitrary dialog sequences.

**EAP-SIM**—Extensible Authentication Protocol-Subscriber Identity Module. Authentication that is designed for use in public WLANs with clients containing SIM smart cards in PC/SC-compliant smart card readers.

**GPRS**—general packet radio service. A service defined and standardized by the European Telecommunication Standards Institute (ETSI). GPRS is an IP packet-based data service for GSM networks.

**GSM**—Global System for Mobile communication. A widely used digital mobile telephone system that employs a variation of time division multiple access (TDMA).

**HLR**— Home Location Register. The main database used for storage and management of subscriptions for a mobile network.

**ITP**—Cisco IP Transfer Point. A solution that acts as a gateway between the IP and SS7 networks.

**MAP**— Mobile Application Part. Information carried within Transaction Capabilities Application Part (TCAP) messages in mobile networks. This information is sent between mobile switches and databases and helps with authentication, equipment identification, and roaming.

**NAS**—Network Access Server. A computer server that enables an ISP to provide customers with Internet access. The server is connected both to the local telecommunication service provider and to the Internet backbone.

**RADIUS**—Remote Authentication Dial-In User Service. RADIUS is an access server that uses AAA protocol.

**RADIUS proxy**—Feature that gives users connected through an NAS (for example, WLAN AP, GPRS support node [GGSN], and PDSN) access to SSG functionality when SSG is configured to act as a RADIUS proxy between the NAS and the AAA server.

**SESM**—Subscriber Edge Services Manager. An extensible set of applications for providing on-demand value-added services and access control at the network edge. Together with the SSG, SESM provides subscriber authentication, service selection, and service connection capabilities to subscribers of Internet services.

**SS7**—Signaling System 7. A system that stores information required to set up and manage telephone calls on the public switched telephone network (PSTN).

**SSG**—Service Selection Gateway. Switching solution for service providers who offer intranet, extranet, and Internet connections to subscribers using broadband access technology such as *x*DSL, cable modems, or wireless to allow simultaneous access to network services.

**supplicant**—As specified in the 802.1x framework, software running on an Ethernet or Wireless Fidelity (Wi-Fi) station. It can request access from an authenticator (a switch or access point).

**WEP**—Wired Equivalent Privacy. Security protocol that is specified in the IEEE Wireless Fidelity (Wi-Fi) standard.

**WLAN**—wireless local area networks. Similar to a traditional LAN except that it uses radio waves to transmit data rather than cables.

**Note** Refer to the *Internetworking Terms and Acronyms* for terms not included in this glossary.