



GLOSSARY

Numerics

- 802.11a** The IEEE standard that governs the deployment of 5-GHz OFDM systems. It specifies the implementation of the physical layer for wireless UNII bands (see UNII, UNII 1, and UNII 2) and provides four channels per 100 MHz of bandwidth.
- 802.11b** The IEEE standard that specifies carrier sense media access control and physical layer specifications for 5.5- and 11-Mbps 2.4-GHz wireless LANs.
- 802.11g** The IEEE standard that specifies carrier sense media access control and physical layer specifications for high-speed 2.4 GHz wireless networking

A

AAA Authentication, Authorization, and Accounting. The WLSE monitors LEAP, PEAP, EAP-MD5, RADIUS, and EAP-FAST AAA services provided by AAA servers running CiscoSecure ACS Server software.

See also [EAP-MD5 server](#), [LEAP server](#), [PEAP server](#), [RADIUS](#), [EAP-FAST](#).

access point Access points are wireless LAN transceivers that serve as the center point of a standalone wireless network or as the connection point between wireless and wired networks. In large installations, wireless users within radio range of an access point can roam throughout a facility while maintaining seamless, uninterrupted access to the network.

ad-hoc network See [IBSS](#).

admin	The default user on the WLSE, created during initial setup of the WLSE. The admin user has the System Administrator role and level 15 CLI privileges. The admin user cannot be deleted.
ARP	Address resolution protocol. An Internet protocol used to map an IP address to a MAC address. Defined in RFC 826.
AVVID	Cisco Architecture for Voice, Video and Integrated Data. Cisco provides the baseline infrastructure that enables enterprises to design networks that scale to meet Internet business demands. Cisco AVVID delivers business infrastructure and intelligent network services.

B

BDPU	Bridge Protocol Data Unit. <i>See</i> STP .
black hole mitigation	Radio Manager feature that recommends the optimal beacon interval for an AP based on data collected from AP radio scan and client walkabout.
BOOTP	Bootstrap Protocol. The protocol used by a network node to determine the IP address of its Ethernet interfaces to affect network booting.
bridge	<i>See</i> wireless bridge .
BSS	Basic Service Set—a set of 802.11 stations associated with a single AP.
BSSID	Basic Service Set Identifier (see BSS)

C

CCK	Complementary Code Keying. Modulation technique used by IEEE 802.11-compliant wireless LANs for transmission at 5.5 and 11 Mbps.
------------	--

- CCMP** Based on the Advanced Encryption Standard (AES) defined in the National Institute of Standards and Technology's FIPS Publication 197, AES-CCMP is a symmetric block cipher that can encrypt and decrypt data using keys of 128, 192, and 256 bits. AES-CCMP is superior to WEP encryption and is defined in the IEEE 802.11i standard.
- CKIP** Cisco Key Integrity Protocol. Cisco's WEP key permutation technique based on an early algorithm presented by the IEEE 802.11i security task group.
- CCKM** Cisco Centralized Key Management. Using CCKM, authenticated client devices can roam from one access point to another without any perceptible delay during re-association. An access point or WLSM (Wireless LAN Services Module) on your network provides wireless domain services (WDS) and creates a cache of security credentials for CCKM-enabled client devices on the subnet. The WDS's cache of credentials dramatically reduces the time required for re-association when a CCKM-enabled client device roams to a new access point.
- CDP** Cisco Discovery Protocol. Media- and protocol-independent device-discovery protocol that runs on all Cisco-manufactured equipment, including routers, access servers, bridges, and switches. Using Cisco Discovery Protocol, a device can advertise its existence to other devices and receive information about other devices on the same LAN or on the remote side of a WAN. Runs on all media that support SNAP, including LANs, Frame Relay, and ATM media.
- CDP distance** The CDP distance determines the depth of the discovery and applies to all seed devices. If CDP distance is 1, only the immediate neighbors of the seed device are discovered. If CDP distance is 2, devices A and B that are directly connected to the seed devices are discovered and the immediate neighbors of A and B are also discovered.
- CLI** The command line interface for administering the WLSE. You use the CLI through a console attached to the WLSE's console port or by opening a Telnet connection to the WLSE. CLI commands are described in the *User Guide for the CiscoWorks Wireless LAN Solution Engine* —from the online help, click **PDF**.
- CMIC** Cisco Message Integrity Check. MIC prevents bit-flip attacks on encrypted packets. During a bit-flip attack, an intruder intercepts an encrypted message, alters it slightly, and retransmits it, and the receiver accepts the retransmitted message as legitimate. The client's adapter driver must support MIC functionality, and MIC must be enabled on the access point.

community strings	Text strings that act as passwords to authenticate communication with devices that contain an SNMP agent.
CoS	Class or Service. An indication of how an upper-layer protocol requires a lower-layer protocol to treat its messages.
CSR	Certificate Signed Request. Request sent to a certificate authority for using HTTPS.
CSV	Comma-separated values. A file format used by CiscoWorks application, such as Resource Manager Essentials, to exchange information on managed devices.

D

DFS	Dynamic Frequency Selection. Anti-contention rules for critical radar applications (for mostly military and weather operations) imposed by the ETSI and the FCC.
DHCP	Dynamic Host Configuration Protocol. Provides a mechanism for allocating IP addresses dynamically so that addresses can be reused when hosts no longer need them.
DNS	Domain Name System. An Internet service that translates domain names into IP addresses. Domain names are a clear way of representing an Internet address. The Internet, however, is actually based on IP addresses. For example, the URL <code>http://www.website.com</code> might actually point to the IP address <code>http://123.456.789.0</code> . Because maintaining a central list of domain name/IP address correspondences would be impractical, the lists of domain names and IP addresses are distributed throughout servers on the Internet in the Domain Name System. If one DNS server cannot translate a particular domain name, it contacts another one, and so on, until the correct IP address is returned.
DTIM	Deliver Traffic Indication Message. Used by access points to tell power-save client devices that a packet is waiting for them.
DSCP	Differentiated Services Code Point is a model in which traffic is treated by intermediate systems with relative priorities based on the type of services.

E

- EAP** Extensible authentication protocol.
- EAP-MD5 server** Servers running EAP and providing dynamic, session-specific wireless encryption keys, central user administration, and authentication between clients and access points. EAP-MD5 uses MD5 hashing on client and challenge passwords. The WLSE monitors EAP-MD5 servers.
- See also* [AAA](#).
- EAP-FAST** EAP-FAST is a two-phase authentication protocol:
- Phase 0, provisioning. Provision client with a credential called PAC (Protected Access Credentials).
 - Phase 1, authentication. Use the PAC to establish a tunnel with the server and authenticate the username and password.
- The WLSE monitors EAP-FAST servers. *See also* [AAA](#).
- EAP-TLS** EAP with Transport Level Security.
- EAPOL** Extensible Authentication Protocol Over LAN
- exception** A group of related faults.

F

- fast secure roaming** Cisco software feature that allows Cisco and Cisco-compatible clients to layer-2 roam in under 150ms (under 10ms in most cases). Fast secure roaming uses a complex key hierarchy that is closely based on industry-standard WPA, and improves on WPA by adding WDS and establishing trust between the WDS and wireless APs and clients. This allows clients to re-establish WEP keys when roaming.
- See also* [WDS](#), [WPA](#), [WEP keys](#).

G

GMT Greenwich Mean Time. Mean solar time at the meridian of Greenwich, England, formerly used as a basis for standard time throughout the world.

See also [UTC](#).

GRE Generic Routing Encapsulation. A tunneling protocol developed by Cisco that can encapsulate a wide variety of protocol packet types inside IP tunnels, creating a virtual point-to-point link to Cisco routers at remote points over an IP internetwork. By connecting multi protocol subnetworks in a single-protocol backbone environment, IP tunneling that uses GRE allows network expansion across a single-protocol backbone environment.

H

HTTP Hypertext Transfer Protocol. The protocol used by Web browsers and Web servers to transfer files, such as text and graphic files.

HTTPS Secure HTTP with SSL (secure socket layer). *See also* [SSL](#).

I

IBSS Independent Basic Service Set. A local network configuration that is set up by clients and in which the clients communicate directly with each other. This ad-hoc network mode is specified by the 802.11 standard for client radio network interface cards (NIC).

ICMP Internet Control Message Protocol. Network layer Internet protocol that reports errors and provides other information relevant to IP packet processing.

IGMP Internet Group Membership Protocol. Used by IP hosts to report their multicast group memberships to an adjacent multicast router.

infrastructure access points The access points that participate in WDS and register with a WDS device. *See also* [WDS devices](#).

L

- LDAP** Netscape Lightweight Directory Access Protocol. Provides a standard way for Internet clients, applications, and WWW servers to access directory information across the Internet, such as user names, e-mail addresses, security certificates, and other contact information.
- LEAP server** Light EAP server, which combines centralized two-way authentication with dynamically generated wireless equivalent privacy keys or WEP keys.
- See also* [AAA](#) and [WEP keys](#).

M

- MHAE** Mobile home authentication extension. Mobile IP uses a strong authentication scheme to protect communications to and from visiting clients. All registration messages between a visiting client and the home agent must contain the MHAE. Proxy Mobile IP also implements this requirement in the registration messages sent by the access point on behalf of the visiting clients to the home agent.
- See also* [proxy mobile IP](#).
- IMIC** Message integrity check. MIC prevents bit-flip attacks on encrypted packets. During a bit-flip attack, an intruder intercepts an encrypted message, alters it slightly, and retransmits it, and the receiver accepts the retransmitted message as legitimate. The client adapter's driver must support MIC functionality, and MIC must be enabled on the access point.
- MOK** A type of modulation used before the IEEE finished high-speed 802.11 standard and may still be used in older wireless networks.

N

non-serving channel One or more channels on which an AP is *not* transmitting. Non-serving channel monitoring means that the channels the AP is not transmitting on are monitored. By monitoring non-serving channels, Radio Manager can detect rogue APs that you might not have discovered had it monitored only the channel the AP is transmitting on (the serving channel). See [serving channel](#).

nslookup The NSLookup tool is used to look up device or host information via the name server. You must enter a device name, not an IP address, to use this function. You must have a DNS server in order to look up network servers.

NTP Network Time Protocol. Protocol built on top of TCP that ensures accurate local timekeeping with reference to radio and atomic clocks located on the Internet. This protocol is capable of synchronizing distributed clocks within milliseconds over long time periods.

O

OFDM Orthogonal Frequency Division Multiplexing. A radio modulation technique that provides 54 Mbps in the 5 GHz band.

P

PAC Protected access credentials. Credentials that are either automatically or manually provisioned and used to perform mutual authentication with the RADIUS server during EAP-FAST authentication. PACs are created by the Cisco Secure ACS server and are identified by an ID. The user obtains a copy of the PAC from the server, and the ID links the PAC to the profile created in ACU. When manual PAC provisioning is enabled, the PAC file is manually copied from the server and imported onto the client device.

See also [EAP-FAST](#).

- PEAP server** Protected EAP server, which combines centralized two-way authentication with dynamically generated wireless equivalent privacy keys or WEP keys.
- See also* [AAA](#) and [WEP keys](#).
- ping** A common method for troubleshooting the accessibility of devices.
- A ping tests an ICMP echo message and its reply. Because ping is the simplest test for a device, it is the first to be used. If ping fails, try using traceroute.
- Run ping to view the packets transmitted, packets received, percentage of packet loss, and round-trip time in milliseconds.
- proxy mobile IP** An access point feature that works in conjunction with the Mobile IP feature on Cisco devices on the wired network. When you enable proxy Mobile IP on your access point and on your wired network, the access point helps client devices from other networks remain connected to their home networks. The visiting client devices do not need special software; the access point provides proxy Mobile IP services on their behalf.
- PSPF** Publicly Secure Packet Forwarding. A feature that prevents client devices associated to a bridge or access point from inadvertently sharing files with other client devices on the wireless network.

Q

- QoS** Quality of Service. Measure of performance for transmission systems that reflects their transmission quality and service availability.

R

- radio measurement aggregation** WDS service for collecting all of the radio measurements in the layer 2 domain and sending aggregated radio reports to the WLSE.
- See also* [WDS](#).

RADIUS	Remote Authentication Dial-In User Service. Database for authenticating connections and for tracking connection time. The WLSE monitors RADIUS servers. The WLSE also provides a RADIUS module for authenticating users. <i>See also</i> AAA .
repository	The repository stores WLSE images and provides software update services. A repository can be a WLSE (local repository) or another system that functions as an FTP server (remote repository). From a local repository, you can update the WLSE that contains the repository and update other WLSEs.
RSA	Public-key cryptographic system that can be used for encryption and authentication.
RSSI	Received signal strength indication.
runstats	Database facility that runs (automatically) periodically. Keeps database system tables up-to-date and improves efficiency and performance of the database. Tables are updated as necessary and these changes are logged in the db2runstatat.last.log and db2runstat.times.log.

S

SCP	Secure copy protocol. Commonly used to securely copy files between hosts in a network. SCP uses SSH for data transfer and provides the same security and authentication as SSH. Unlike RCP, SCP asks for passwords or pass phrases if they are needed for authentication. SCP is usually available on all UNIX-type systems.
seed	A CDP-enabled device used as a starting point for discovery. For example, by adding a seed device (or set of seed devices), the neighbors of the seed device are discovered using CDP.
serving channel	The channel on which an AP is transmitting. See non-serving channel .
SMTP	Simple Mail Transfer Protocol. Internet protocol providing e-mail services.

SNMP	Simple Network Management Protocol. Network management protocol used almost exclusively in TCP/IP networks. SNMP provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.
SSH	Secure Shell. Provides a secure Telnet connection, encrypting all traffic, including passwords
SSID	Service Set ID. It is a unique identifier that client devices use to associate with the access point. The SSID helps client devices distinguish between multiple wireless networks in the same vicinity. The SSID can be any alphanumeric entry up to 32 characters long.
SSL	Secure Socket Layer. Provides a secure connection between the WLSE and Web clients.
STA	Station (802.11 radio device).
STP	Spanning-Tree Protocol. Bridge protocol that uses the spanning-tree algorithm, enabling a learning bridge to dynamically work around loops in a network topology by creating a spanning tree. Bridges exchange BPDU messages with other bridges to detect loops, and then remove the loops by shutting down selected bridge interfaces. Refers to both the IEEE 802.1 Spanning-Tree Protocol standard and the earlier Digital Equipment Corporation Spanning-Tree Protocol upon which it is based. The IEEE version supports bridge domains and allows the bridge to construct a loop-free topology across an extended LAN. The IEEE version generally is preferred over the Digital version.
SWAN	Structured Wireless-Aware Network. Comprehensive Cisco framework for deploying, operating, and managing Cisco access points through use of the Cisco infrastructure. Extends to the wireless LAN the same level of security, scalability, and reliability that customers have come to expect in their wired LAN by introducing wireless-aware capabilities into the Cisco infrastructure.

T

- TACACS+** Terminal Access Controller Access Control System Plus. Proprietary Cisco enhancement to Terminal Access Controller Access Control System (TACACS). Provides additional support for authentication, authorization, and accounting.
- TCP** Transmission Control Protocol. Connection-oriented transport layer protocol that provides reliable full-duplex data transmission. TCP is part of the TCP/IP protocol stack.
- TFTP** Trivial File Transfer Protocol. Simplified version of FTP that allows files to be transferred from one computer to another over a network, usually without the use of client authentication (for example, username and password).
- threshold** A range within which you expect your network to perform. If a threshold is exceeded or goes below the expected bounds, you examine the areas for potential problems. You can create thresholds for a specific device.
- TKIP** Temporal Key Integrity Protocol, also known as key hashing, is used as part of server-based EAP authentication.
- traceroute** This is a diagnostic tool that helps you understand why ping fails or why applications time out. Using it, can view each hop (or gateway) on the route to your device and how long each took.

U

- UDP** User Datagram Protocol. Connectionless transport layer protocol in the TCP/IP protocol stack. UDP is a simple protocol that exchanges datagrams without acknowledgments or guaranteed delivery, requiring that error processing and retransmission be handled by other protocols. UDP is defined in RFC 768.
- UTC** Coordinated Universal Time. Time zone at zero degrees longitude. Formerly called Greenwich Mean Time (GMT) and Zulu time.

V

- VLAN** Virtual LAN. Group of devices on one or more LANs that are configured (using management software) so that they can communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, they are extremely flexible.
- VLAN ID** Virtual Local Area Network identification used by the standard 802.1Q. Being on 12 bits, it allows the identification of 4096 VLANs.

W

- WDC** Windows Domain Controller.
- WDS** Wireless Domain Services. A device providing WDS on the wireless LAN maintains a cache of credentials for clients that are capable of using CCKM (Cisco Centralized Key Management). When a CCKM-capable client roams from one access point to another, WDS forwards the client's credentials to the new access point with the multicast key. *See also* [WLCCP](#).
- WDS devices** Devices that provides WDS to other access points. *See also* [infrastructure access points](#), [WLSM](#).
- WEP keys** Wired equivalent privacy (WEP) keys are the IEEE 802.11b standard that offers a mechanism for securing wireless LAN data streams. The goals of WEP include access control to prevent unauthorized users who lack a correct WEP key from gaining access to the network, and privacy to protect wireless LAN data streams by encrypting them and allowing de-encryption only by users with the correct WEP keys.
- WGB** Workgroup bridges connect Ethernet-enabled laptops or other portable computers to a wireless LAN (WLAN), providing the link from these devices to any Cisco access point or wireless bridge.
- WINS** Microsoft Windows Internet Naming Service is a name resolution service that resolves computer names to IP addresses.

wireless bridge	Device that connects two or more networks (typically located in different buildings). Bridges connect hard-to-wire sites, non-contiguous floors, satellite offices, school or corporate campus settings, temporary networks, and warehouses. For functional flexibility, the wireless bridge may also be configured as an access point.
WISPr	Wi-Fi Service Provider Roaming.
WLCCP	Wireless LAN Context Control Protocol. Protocol used by the WLSE to authenticate with a device that provides WDS to the wireless LAN network. <i>See also</i> WDS .
WLSM	Wireless LAN Services Module. A module for the Cisco Catalyst 6500 series switch that provides WDS to the wireless network. <i>See also</i> WDS .
WNM	Wireless network manager. WNM manages the devices on your wireless LAN.
WPA	Wi-Fi Protected Access. WPA is a standards-based, interoperable security enhancement that strongly increases the level of data protection and access control for existing and future wireless LAN systems. It is derived from and will be forward-compatible with the upcoming IEEE 802.11i standard. WPA leverages TKIP for data protection and 802.1X for authenticated key management.