



*Beta Draft for Review - Cisco Confidential*

## GLOSSARY

- 802.11** The IEEE standard that specifies carrier sense media access control and physical layer specifications for 1- and 2-megabit-per-second (Mbps) wireless LANs operating in the 2.4-GHz band.
- 802.11a** The IEEE standard that specifies carrier sense media access control and physical layer specifications for wireless LANs operating in the 5-GHz frequency band.
- 802.11b** The IEEE standard that specifies carrier sense media access control and physical layer specifications for 5.5- and 11-Mbps wireless LANs operating in the 2.4-GHz frequency band.
- 802.11g** The IEEE standard that specifies carrier sense media access control and physical layer specifications for wireless LANs operating in the 2.4-GHz frequency band.

### A

- access point** A wireless LAN data transceiver that uses radio waves to connect a wired network with wireless stations.
- AC\_BE** Access Category Best Effort
- AC\_BK** Access Category Background
- AC\_VI** Access Category Video
- AC\_VO** Access Category Voice
- AES Counter-Mode/CBC-MAC protocol (AES CCMP)** A protocol based on AES using the CCM mode of operation. The CCM mode combines *Counter* (CTR) mode privacy and *Cipher Block Chaining Message Authentication Code* (CBC-MAC) authentication
- ad hoc network** A wireless network composed of stations without access points.
- antenna gain** The gain of an antenna is a measure of the antenna's ability to direct or focus radio energy over a region of space. High-gain antennas have a more focused radiation pattern in a specific direction.
- associated** A station is configured properly to enable it to wirelessly communicate with an access point.
- authentication suite** A suggested set of authentication methods

**Beta Draft for Review - Cisco Confidential**

<b>B</b>	
<b>backoff time</b>	The random length of time that a station waits before sending a packet on the LAN. Backoff time is a multiple of slot time, so a decrease in slot time ultimately decreases the backoff time, which increases throughput.
<b>beacon</b>	A wireless LAN packet that signals the availability and presence of the wireless device.
<b>BID</b>	Bridge identifier used in spanning-tree calculations. The BID contains the bridge MAC address and its spanning-tree priority value. If all bridges in the spanning tree are assigned the same priority, the bridge with the lowest MAC address becomes the spanning-tree root.
<b>BOOTP</b>	Boot Protocol. A protocol used for the static assignment of IP addresses to devices on the network.
<b>BPDU</b>	Bridge protocol data unit. When STP is enabled, bridges send and receive spanning-tree frames, called BPDUs, at regular intervals and use the frames to maintain a loop-free network.
<b>BPSK</b>	A modulation technique used by IEEE 802.11b-compliant wireless LANs for transmission at 1 Mbps.
<b>broadcast packet</b>	A single data message (packet) sent to all addresses on the same subnet.
<b>C</b>	
<b>CCK</b>	Complementary code keying. A modulation technique used by IEEE 802.11b-compliant wireless LANs for transmission at 5.5 and 11 Mbps.
<b>CCKM</b>	Cisco Centralized Key Management. Using CCKM, authenticated client devices can roam from one access point to another without any perceptible delay during reassociation. An access point on your network acts as a subnet context manager (SCM) and creates a cache of security credentials for CCKM-enabled client devices on the subnet. The SCM's cache of credentials dramatically reduces the time required for reassociation when a CCKM-enabled client device roams to a new access point.
<b>cell</b>	The area of radio range or coverage in which the wireless devices can communicate with the base station. The size of the cell depends upon the speed of the transmission, the type of antenna used, and the physical environment, as well as other factors.
<b>client</b>	A radio device that uses the services of an Access Point to communicate wirelessly with other devices on a local area network.
<b>Cipher Suite</b>	A set of one or more cryptographic algorithms designed to protect data traffic. A cipher suite may provide data privacy, data authenticity or integrity, and/or replay protection

## ***Beta Draft for Review - Cisco Confidential***

<b>Cisco Centralized Key Management (CCKM)</b>	CCKM is the basis of Cisco Fast reassociation and reauthentication solution, which utilizes a central node, an AP, as the key distributor to enable protected communications between the AP and the Wireless Stations. Station using CCKM use proprietary supports SSN Group Key update.
<b>CKIP</b>	Cisco Temporal Key Integrity Protocol
<b>client</b>	A radio device that uses the services of an access point to communicate wirelessly with other devices on a local area network.
<b>CMIC</b>	Cisco Message Integrity Check
<b>CW</b>	Contention Window
<b>CSMA</b>	Carrier sense multiple access. A wireless LAN media access method specified by the IEEE 802.11 specification.
<b>D</b>	
<b>data rates</b>	The range of data transmission rates supported by a device. Data rates are measured in megabits per second (Mbps).
<b>dBi</b>	A ratio of decibels to an isotropic antenna that is commonly used to measure antenna gain. The greater the dBi value, the higher the gain, and the more acute the angle of coverage.
<b>DHCP</b>	Dynamic host configuration protocol. A protocol available with many operating systems that automatically issues IP addresses within a specified range to devices on the network. The device retains the assigned address for a specific administrator-defined period.
<b>dipole</b>	A type of low-gain (2.2-dBi) antenna consisting of two (often internal) elements.
<b>domain name</b>	The text name that refers to a grouping of networks or network resources based on organization-type or geography; for example: name.com—commercial; name.edu—educational; name.gov—government; ISPname.net—network provider (such as an ISP); name.ar—Argentina; name.au—Australia; and so on.
<b>DNS</b>	Domain Name System server. A server that translates text names into IP addresses. The server maintains a database of host alphanumeric names and their corresponding IP addresses.
<b>DSSS</b>	Direct sequence spread spectrum. A type of spread spectrum radio transmission that spreads its signal continuously over a wide frequency band.
<b>E</b>	
<b>EAP</b>	Extensible Authentication Protocol. An optional IEEE 802.1x security feature ideal for organizations with a large user base and access to an EAP-enabled Remote Authentication Dial-In User Service (RADIUS) server.

**Beta Draft for Review - Cisco Confidential**

<b>EAPOL-Key Key</b>	Combination of EAPOL-Key Encryption key and EAPOL-Key MIC Key.
<b>EAPOL Key Encryption Key (KEK)</b>	Key that encrypts key material in EAPOL-key packet
<b>EAPOL-Key MIC Key (KCK)</b>	Key used to integrity check an EAPOL-Key Message.
<b>Ethernet</b>	The most widely used wired local area network. Ethernet uses carrier sense multiple access (CSMA) to allow computers to share a network and operates at 10, 100, or 1000 Mbps, depending on the physical layer used.
<b>F</b>	
<b>file server</b>	A repository for files so that a local area network can share files, mail, and programs.
<b>firmware</b>	Software that is programmed on a memory chip.
<b>G</b>	
<b>gateway</b>	A device that connects two otherwise incompatible networks.
<b>GHz</b>	Gigahertz. One billion cycles per second. A unit of measure for frequency.
<b>I</b>	
<b>IEEE</b>	Institute of Electrical and Electronic Engineers. A professional society serving electrical engineers through its publications, conferences, and standards development activities. The body responsible for the Ethernet 802.3 and wireless LAN 802.11 specifications.
<b>infrastructure</b>	The wired Ethernet network.
<b>IP address</b>	The Internet Protocol (IP) address of a station.
<b>IP subnet mask</b>	The number used to identify the IP subnetwork, indicating whether the IP address can be recognized on the LAN or if it must be reached through a gateway. This number is expressed in a form similar to an IP address; for example: 255.255.255.0.
<b>isotropic</b>	An antenna that radiates its signal in a spherical pattern.

**Beta Draft for Review - Cisco Confidential****M**

- MAC** Media Access Control address. A unique 48-bit number used in Ethernet data packets to identify an Ethernet device such as an access point or your client adapter.
- Message Integrity Code (MIC)** A cryptographic checksum, designed to make it computationally infeasible for an adversary to alter data. This is usually called a Message Authentication Code, or MAC, in the literature, but the acronym MAC is already reserved for another meaning in this standard.
- modulation** Any of several techniques for combining user information with a transmitter's carrier signal.
- multipath** The echoes created as a radio signal bounces off of physical objects.
- multicast packet** A single data message (packet) sent to multiple addresses.

**O**

- omni-directional** This typically refers to a primarily circular antenna radiation pattern.
- Orthogonal Frequency Division Multiplex (OFDM)** A modulation technique used by IEEE 802.11a-compliant wireless LANs for transmission at 6, 9, 12, 18, 24, 36, 48, and 54 Mbps.

**P**

- packet** A basic message unit for communication across a network. A packet usually includes routing information, data, and sometimes error detection information.
- pairwise** Two entities that is associated with each other; an access point and one associated station, or a pair of stations in an IBSS network, used to describe the key hierarchies for keys that are shared only between the two entities in a pairwise.
- Pairwise Master Key (PMK)** The key that is generated on a per-session basis and is used as one of the inputs into the PRF to derive the Pairwise Transient Keys (PTK). For EAP-TLS authentication, the Pairwise Master Key is the key from the RADIUS MS-MPPE-Recv-Key attribute. For Pre-Shared Key authentication, the Pairwise Master Key is the Pre-Shared Key.
- PMKID** PMK identification
- Pairwise Transient Key (PTK)** A value that is derived from the PRF using the SNonce and ANonce, and is split up into as many as five keys (Temporal Encryption Key, two Temporal MIC Keys, EAPOL-Key Encryption Key, EAPOL-Key MIC Key) for use by the rest of the system.

**Beta Draft for Review - Cisco Confidential**

<b>Pre-Shared Key (PSK)</b>	A key that is distributed to the units in the system by manual means. Legacy WEP systems without authentication used Pre-Shared Keys as the WEP keys. The Robust Security Network (RSN) specification allows a system to use a Pre-Shared Key if there is no other authentication method available, but using a Pre-Shared Key is not as secure.
<b>public key infrastructure (PKI)</b>	A system that uses digital certificates and certificate authority to verify the identify of network users.

**Q**

<b>quadruple phase shift keying</b>	A modulation technique used by IEEE 802.11b-compliant wireless LANs for transmission at 2 Mbps.
-------------------------------------	---

**R**

<b>range</b>	A linear measure of the distance that a transmitter can send a signal.
<b>receiver sensitivity</b>	A measurement of the weakest signal a receiver can receive and still correctly translate it into data.
<b>RF</b>	Radio frequency. A generic term for radio-based technology.
<b>roaming</b>	A feature of some access points that allows users to move through a facility while maintaining an unbroken connection to the LAN.
<b>RSN</b>	Robust Security Network
<b>RSNIE</b>	RSN Information Element
<b>RP-TNC</b>	A connector type unique to Cisco radios and antennas. Part 15.203 of the FCC rules covering spread spectrum devices limits the types of antennas that may be used with transmission equipment. In compliance with this rule, Cisco, like all other wireless LAN providers, equips its radios and antennas with a unique connector to prevent attachment of non-approved antennas to radios.

**S**

<b>slot time</b>	The amount of time a device waits after a collision before retransmitting a packet. Short slot times decrease the backoff time, which increases throughput.
<b>spread spectrum</b>	A radio transmission technology that spreads the user information over a much wider bandwidth than otherwise required in order to gain benefits such as improved interference tolerance and unlicensed operation.
<b>SSID</b>	Service Set Identifier (also referred to as Radio Network Name). A unique identifier used to identify a radio network and which stations must use to be able to communicate with each other or to an access point. The SSID can be any alphanumeric entry up to a maximum of 32 characters.

**Beta Draft for Review - Cisco Confidential**

<b>SSN</b>	Simple Security Network
<b>SSN-PSK</b>	Authenticated Key Management using pre-shared Key over 802.1X. SSN is enabled and there exists a per-configured pre-shared key. In this mode, the station use 802.1X for key management.
<b>T</b>	
<b>Temporal Encryption Key</b>	Key used to encrypt data packets.
<b>Temporal Key</b>	Combination of temporal encryption key and temporal MIC key.
<b>Temporal MIC Key</b>	Key used to integrity check data packets
<b>TID</b>	Traffic Identifier (802.1Q user priority value)
<b>TKIP</b>	Temporal Key Integrity Protocol
<b>transmit power</b>	The power level of radio transmission.
<b>U</b>	
<b>UNII</b>	Unlicensed National Information Infrastructure—regulations for UNII devices operating in the 5.15- to 5.35-GHz and 5.725- to 5.825-GHz frequency bands.
<b>UNII-1</b>	Regulations for UNII devices operating in the 5.15- to 5.25-GHz frequency band.
<b>UNII-2</b>	Regulations for UNII devices operating in the 5.25- to 5.35-GHz frequency band.
<b>UNII-3</b>	Regulations for UNII devices operating in the 5.725- to 5.825-GHz frequency band.
<b>unicast packet</b>	A single data message (packet) sent to a specific IP address.
<b>W</b>	
<b>WDS</b>	Wireless Domain Services. An access point providing WDS on your wireless LAN maintains a cache of credentials for CCKM-capable client devices on your wireless LAN. When a CCKM-capable client roams from one access point to another, the WDS access point forwards the client's credentials to the new access point with the multicast key. Only two packets pass between the client and the new access point, greatly shortening the reassociation time.
<b>WEP</b>	Wired Equivalent Privacy. An optional security mechanism defined within the 802.11 standard designed to make the link integrity of wireless devices equal to that of a cable.

***Beta Draft for Review - Cisco Confidential***

<b>WLSE</b>	Wireless LAN Solutions Engine. The WLSE is a specialized appliance for managing Cisco wireless LAN infrastructures. It centrally identifies and configures access points in customer-defined groups and reports on throughput and client associations. WLSE centralized management capabilities are further enhanced with an integrated template-based configuration tool for added configuration ease and improved productivity.
<b>WNM</b>	Wireless Network Manager.
<b>workstation</b>	A computing device with an installed client adapter.
<b>WPA</b>	Wi-Fi Protected Access (WPA) is a security solution from the Wireless Ethernet Compatibility Alliance (WECA). WPA, mostly synonymous to Simple Security Network (SSN), relies on the interim version of IEEE Standard 802.11i. WPA supports WEP and TKIP encryption algorithms as well as 802.1X and EAP for simple integration with existing authentication systems. WPA key management uses a combination of encryption methods to protect communication between client devices and the access point.