

Official CWNP Dictionary Of Wireless Terms & Acronyms

SAMPLE ONLY

Selected Definitions from the Official Dictionary available at CWNP.com

The full CWNP Dictionary contains over 1200 terms and acronyms. This free sample edition only has about 200 entries.

Author

Joel Barrett, CWNE #6, CWNT

SAMPLE EDITION

CWNP, Inc.

Official CWNP Dictionary of Wireless Terms and Acronyms SAMPLE EDITION

Copyright © 2009 by Brainslap Productions and CWNP, Inc.

Production Date: December, 2008.

License Agreement

PLEASE READ THESE TERMS AND CONDITIONS CAREFULLY BEFORE USING THIS BOOK (“MATERIALS”). BY USING THE MATERIALS YOU AGREE TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS LICENSE.

Ownership

The Book is proprietary to CWNP, INC. and BRAINSLAP PRODUCTIONS, who retain exclusive title to and ownership of the copyrights and other intellectual property rights in the Book. These rights are protected by the national and state copyright, trademark, trade secret, and other intellectual property laws of the United States and international treaty provisions, including without limitation the Universal Copyright Convention and the Berne Copyright Convention. You have no ownership rights in the Book. Except as expressly set forth herein, no part of the Book may be modified, copied, or distributed in hardcopy or machine-readable form without prior written consent from CWNP, INC. All rights not expressly granted to you herein are expressly reserved by CWNP, INC. Any other use of the Book by any person or entity is strictly prohibited and a violation of this Agreement.

Scope of Rights Licensed (Permitted Uses)

CWNP, INC. is granting you a limited, non-exclusive, non-transferable license to use the Book, in part or in whole, for your internal business or personal use. Any internal or personal use of the Book content must be accompanied by the phrase “Used with permission from CWNP, INC.” or other phrasing agreed upon in writing by CWNP, INC.

Restrictions on Transfer

Reproduction or disclosure in whole or in part to parties other than the CWNP, INC. client that is the original subscriber to this Book is permitted only with the written and express consent of CWNP, INC. This Book shall be treated at all times as a confidential and proprietary document for internal use only.

Any purported sale, assignment, transfer or sublicense without the prior written consent of CWNP, INC. will be void and will automatically terminate the License granted hereunder.

Limited Warranty

THE INFORMATION CONTAINED IN THIS BOOK IS BELIEVED TO BE RELIABLE BUT CANNOT BE GUARANTEED TO BE CORRECT OR COMPLETE. If the Book’s format is defective, CWNP, INC. will replace it at no charge if CWNP, INC. is notified of the defective formatting within THIRTY days from the date of the original receipt of the Book. CWNP, INC., MAKES NO WARRANTY, EXPRESS OR IMPLIED, OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE

Limitation of Liability

IN NO EVENT WILL CWNP, INC. OR BRAINSLAP PRODUCTIONS BE LIABLE TO YOU FOR ANY DAMAGES, INCLUDING, WITHOUT LIMITATION, ANY LOST PROFITS, LOST SAVINGS, OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF YOUR USE OR INABILITY TO USE THE BOOK REGARDLESS OF WHETHER SUCH DAMAGES ARE FORESEEABLE OR WHETHER SUCH DAMAGES ARE DEEMED TO RESULT FROM THE FAILURE OR INADEQUACY OF ANY EXCLUSIVE OR OTHER REMEDY. IN ANY EVENT, THE LIABILITY OF CWNP, INC. SHALL NOT EXCEED THE LICENSE FEE PAID BY YOU TO CWNP, INC.

Recommending Updates

If you find a term or acronym that needs to be added or requires modification, please contact the author, Joel Barrett, by emailing joel@brainslap.com. New editions of this dictionary will be published as appropriate.

Volume, Corporate, and Educational Sales

CWNP offers favorable discounts on products when ordered in quantity. For more information, please contact CWNP directly:

CWNP, Inc.
4381 Beech Haven Trail
Suite 400
Smyrna, GA 30080 USA
Phone: 770-433-9339
Fax: 866-422-8354
Customercare@cwnp.com

About CWNP

CWNP is the industry standard for vendor neutral enterprise Wi-Fi certification and training. CWNP offers four levels of enterprise Wi-Fi certifications: CWTS, CWNA, CWSP, and CWNE. For complete information on how to get trained and certified in enterprise Wi-Fi technologies, please visit us at www.cwnp.com

About the Author

Joel Barrett is a senior-level wireless networking expert with Cisco Systems. Joel has attained networking certifications such as Cisco's CCNP and CCDP, Microsoft's MCSE, and Novell's Master CNE. For wireless certifications, he holds Cisco's Wireless Design and Support specializations, as well as CWNP's Wireless#, CWNA, CWSP, CWAP, CWNT, and CWNE certifications. He is CWNE #6 and a founding member of the CWNE Roundtable, a steering committee for the CWNE certification program. Joel is also certified to instruct Cisco's Unified Wireless and Mesh Networking courses and holds the WiMAX Forum's RF Networking Engineer certification.

Within Cisco, Joel consults primarily with large enterprise customers concerning wireless deployments. He is a field advisor for Cisco's global wireless virtual team. He is also an author and technical editor for books such as "CWNA Official Study Guide, 4th Edition", "CWNP Wireless# Exam Mega Guide", "Wireless Networks First-Step", "CWSP Official Study Guide, First Edition", and "Managing and Securing a Cisco Structured Wireless-Aware Network". He is the series editor for McGraw-Hill's "CWNP Study Guides".

Joel and his wife, Barbara Kurth, live with their three children, Ashley, Shane, and Paige in the Atlanta, Georgia metro area. Joel has two tenets he lives by:

“Do what you love, the money will come.”

“If it were easy, anyone could do it.”

Organization of Acronyms and Terms

In this dictionary, for commonly used acronyms, the acronym is listed first followed by expansion of the acronym and then the definition, if needed. For example:

AP (WF) - Access Point; any entity that has station (STA) functionality and provides access to the distribution services, via the wireless medium (WM) for associated STAs. See also **AP types**.

Notice also for this term that “WF” is shown in parentheses indicating *this* term is specific to Wi-Fi. There is a legend at the beginning of the Definitions that shows the specific wireless industry to which terms apply, when appropriate. Some terms are generic to networking, computing, or all wireless industries and therefore have no indication in parentheses. Some terms also have different meanings depending on the industry being discussed.

Terms with “” in front of them come directly from the CWNP Exam Terms document, formerly known as the “CWNP Rosetta Stone”. You should understand these terms particularly well.*

If a term is more commonly seen in acronym form, the acronym will be expanded then defined. If a term is more commonly used in its expanded form, the acronym will precede the definition. For terms that are commonly seen both ways, each term will include a pointer to the other but only one will provide the definition. Hyphenated or underscored terms (like “Pre-RSNA” or “BD_ADDR”) are sorted as if the hyphen or underscore doesn’t exist. Some terms include a reference to the standard in which they were introduced. This reference occurs in parentheses at the end of the definition.

Definitions

Legend

* = Terms from the CWNP Exam Terms document

11n = 802.11n

AKA = Also known as

AR = Amateur Radio

BT = Bluetooth

Cell = Cellular

Cisco = Cisco Systems

IR = Infrared

WF = Wi-Fi

WMX = WiMAX

ZB = ZigBee

Numerics

3GPP (WMX) - Third Generation Partnership Project; a collaboration agreement established in December 1998 that brought together a number of telecommunications standards bodies. The original scope of 3GPP was to produce globally applicable Technical Specifications and Technical Reports for a 3rd Generation Mobile System based on evolved GSM core networks and the radio access technologies that they support. The scope was subsequently amended to include the maintenance and development of GSM Technical Specifications and Technical Reports including evolved radio access technologies, like GPRS and EDGE.

4-Way Handshake - a pairwise key management protocol defined by a standard. In IEEE 802.11, the handshake confirms mutual possession of a pairwise master key (PMK) by two parties and distributes a group temporal key (GTK).

A

AAA - Authentication, Authorization and Accounting; authentication confirms a user who is requesting services is a valid user of the network services requested. Authorization is the process of denying or permitting a client permission to do something on the network, such as accessing a file. Accounting is the process of tracking a user's time, possibly for internal billing purposes.

***ACI** - Adjacent Channel Interference; a performance condition that occurs when two or more access point radios are providing RF coverage to the same physical area using overlapping frequencies. Simultaneous RF transmissions by two or more of these access point radios in the same physical area can result in corrupted 802.11 frames due to the frequency overlap. Corrupted 802.11 frames cause retransmissions, which result in both throughput degradation and added latency. See also **Channel comparisons** for a description of adjacent versus non-adjacent and overlapping channels.

ACK - Acknowledgment; a frame passed between communicating processes or devices to signify acknowledgement, or receipt of response, as part of a communications protocol.

***Active Mode** (WF) - power management of a non-AP station (STA) operates in either active mode or power-save mode. A STA in active mode is always in an awake state. Vendors have called this, "Continually Aware mode (CAM)" and other similar variations. Wireless STAs that

are always powered by an AC outlet should always be configured for active mode to realize better performance. See also **PS Mode**.

AES - Advanced Encryption Standard; a method that uses up to 256-bit key encryption to secure data. AES is the encryption standard that replaced the Digital Encryption Standard (DES) in order to improve encryption strength. It is based on the Rijndael algorithm.

***A-MPDU** (11n) - Aggregate MAC Protocol Data Unit; a structure containing multiple MPDUs, transported as a single PSDU by the PHY.

***A-MSDU** (11n) - Aggregate MAC Service Data Unit; a structure containing multiple MSDUs, transported within single (unfragmented) or multiple (fragmented) Data MPDUs.

Antenna - the element used in a wireless device or system to transmit and receive radio signals. Antennas come in many forms and sizes and can be omnidirectional, sector/semidirectional, or highly directional. See also **Antenna types**.

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.

Antenna types:

- **Dipole** - a type of low-gain (2.2-dBi) omnidirectional antenna consisting of two (often internal) elements.
- **Directional antenna** - an antenna that concentrates transmission power into a direction thereby increasing coverage distance at the expense of coverage angle. Directional antenna types include Yagi and patch or sector. Directional antennas typically have beamwidths between 90° and 15° and one main lobe with several minor lobes.
- **Diversity antennas** - an intelligent radio system that uses two antennas to continually sense incoming radio signals and then automatically selects the antenna best positioned for reception.
- **Highly directional** - radiates greater power in one or more directions allowing for increased performance on transmit and receive and reduced interference from unwanted sources. Highly directional antennas include parabolic dish antennas. Many highly directional antennas have beamwidths of less than 10°.
- **Omnidirectional** - an antenna that provides a 360° transmission pattern. These types of antennas are used when coverage in all directions is required.
- **Sector, semidirectional, or patch** - radiates in a specific direction and indicates the beamwidth of the radiation pattern, for example: a 45° E-plane (elevation) and a 60° H-plane (horizon/azimuth).

AP (WF) - Access Point; any entity that has station (STA) functionality and provides access to the distribution services, via the wireless medium (WM) for associated STAs. See also **AP types**.

AP types:

- **Autonomous or standalone AP** - an access point that operates without a vendor-specific central controller. AKA: **Thick** or **fat AP**.
- **HT-AP-19** (11n) - High Throughput Access Point 19; an HT AP that is operating on a 20 MHz channel or set of 20 MHz channels that belong to the channel set that is defined in IEEE 802.11 Clause 19.

- **Lightweight or controller-based AP** - an access point that depends on a centralized controller and LWAPP or similar protocols to provide services to WLAN clients. Typically only includes partial distribution service functionality internally. AKA: **Thin AP, LAP**.
- **Mesh AP** - employ wireless to transmit backhaul traffic from one access point to another and eventually to the network. In this way, wireless mesh access points operate much like the router nodes of a wired network, with traffic flowing from one access point to another over the most efficient path. AKA: **RAP** or **MAP**.
- **RAP** - Root AP; provides a wired connection to a network-based controller. RAPs use their backhaul wireless interface(s) to communicate to neighboring mesh access points. RAPs are the parent node to any bridging or mesh network and connect a bridge or mesh network to the wired network. In most cases, there is only one RAP for each bridged or mesh network. AKA: **MAP** and **Rooftop AP**.
- **Rogue AP** - a wireless access point that has either been installed on a secure company network without explicit authorization from a local network administrator, or has been created to conduct man-in-the-middle attacks.
- **WDS (Cisco)** - Wireless Domain Service; a Cisco access point providing WDS on the autonomous wireless LAN maintains a cache of credentials for CCKM-capable client devices on the 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.
- **Workgroup bridge (WGB)** - a small stand-alone unit that can provide a wireless infrastructure connection for Ethernet-enabled devices. Devices that do not have a wireless client adapter in order to connect to the wireless network can be connected to the WGB through the Ethernet port. The WGB associates to the root AP through the wireless interface. In this way, wired clients get access to the wireless network. The WGB connects to a switch through a standard Ethernet port.

Associated - a station is properly configured and allowed to wirelessly communicate with an Access Point.

Association - the service used to establish access point/station (AP/STA) mapping and enable STA invocation of the distribution system services (DSSs).

***ATIM (WF)** - Announcement Traffic Indication Message; a frame (message) sent between peers in an ad hoc network indicating that data is awaiting delivery to the station that receives the ATIM frame from the station that sent the ATIM frame.

Authentication - the service used to establish the identity of one station (STA) as a member of the set of STAs authorized to associate with another STA.

Authentication Server (AS) - an entity that provides an authentication service to an Authenticator. This service determines, from the credentials provided by the Supplicant, whether the Supplicant is authorized to access the services provided by the Authenticator. (IEEE 802.1X-2004)

Authenticator - an entity at one end of a point-to-point LAN segment that facilitates authentication of the entity attached to the other end of that link. (IEEE 802.1X-2004)

B

Backoff time - 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.

Band - a set of frequencies.

Bandwidth - the transmission capacity of a given device or network. Also, either the difference between the upper and lower frequencies used by a channel, or the sheer number of bits per second that may be communicated through the channel, including all frame protocol overhead, or else sometimes the number of payload bits that can be communicated through the channel in a second. In the latter senses, it is more properly called *throughput*.

Beacon (WF) - frames sent from the AP to the clients on the wireless network that keep the network synchronized. Also produced by non-AP stations in an IBSS. Signals the availability and presence of the wireless device.

Bluetooth (BT) - a wireless communication link, operating in the unlicensed ISM band at 2.4 GHz using a frequency hopping transceiver. It allows real-time AV and data communications between Bluetooth Hosts. The link protocol is based on time slots.

BOOTP - Boot Protocol; a protocol used for the static assignment of IP addresses to devices on the network.

Broadcast packet - a single data message (packet) sent to all addresses on the same subnet basic service area (BSA).

BSS - Basic Service Set; a set of stations (STAs) that have successfully synchronized using the JOIN service primitives and one STA that has used the START primitive. Membership in a BSS does not imply that wireless communication with all other members of the BSS is possible. See also **BSS types**.

BSSID - Basic Service Set Identification; the 48-bit globally unique identifier for a basic service set (BSS). In infrastructure WLANs, the Ethernet MAC address of the AP is used as the BSSID. In ad hoc WLANs, the first station generates a random 48-bit value which is used as the BSSID.

C

CAPWAP - Control and Provisioning of Wireless Access Points; an IETF draft expected to be ratified in 2008. Addresses standardization of lightweight access point control and defines how WLAN data traffic is managed over the backend network. See also **LWAPP**.

***CCI** - Co-Channel Interference; a performance condition that occurs when two or more independently coordinated access point radios are providing RF coverage to the same physical area using the same 802.11 channel. Additional RF medium contention overhead occurs for all radios using this channel in this physical area resulting in throughput degradation and added latency. See also **Channel comparisons** for a description of adjacent versus non-adjacent and overlapping channels.

CCKM (Cisco) - Cisco Centralized Key Management; Cisco's mechanism for handling fast roaming by caching user credentials. 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 provides wireless domain services (WDS) and creates a cache of security credentials for CCKM-enabled client devices on the subnet. The WDS access point's cache of

credentials dramatically reduces the time required for reassociation when a CCKM-enabled client device roams to a new access point. See also **AP-assisted Roaming**.

CCX (Cisco) - Cisco Compatible Extensions; a Cisco program that provides independent verification of interoperability between Cisco wireless infrastructure products and wireless client devices from third-party companies.

Cell - 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.

Cell surfing - the “long ride” effect a Wi-Fi client incurs when it remains associated to a distant AP and does not roam after moving into a cell on the same channel, even after traversing a cell on a different channel.

***Channel comparisons for adjacent channels, non-adjacent channels, and overlapping channels** - the IEEE 802.11-2007 standard defines the following terms:

	DSSS	HR/DSSS	ERP	OFDM
Adjacent	≥ 30 MHz	≥ 25 MHz	$= 25$ MHz	$= 20$ MHz
Non-Adjacent	N/A	N/A	> 25 MHz	> 20 MHz
Overlapping	< 30 MHz	< 25 MHz	< 25 MHz	N/A

- **Adjacent channels** - channel with a separation between their center frequencies of less than or equal to the IEEE standard specifications for adjacent channels. The 802.11 standard loosely defines an adjacent channel as any channel with non-overlapping frequencies for the DSSS and HR/DSSS PHYs. With ERP and OFDM PHYs, the standard loosely defines an adjacent channel as the first channel with a non-overlapping frequency space. Adjacent channels create ACI. See also **ACI (Adjacent Channel Interference)**.

NOTE: This contradicts how the term “adjacent channel interference” is typically used in the marketplace. Most Wi-Fi vendors use this term to loosely mean both 1) interference resulting from overlapping cells, and 2) interference resulting from the use of overlapping frequency space. For example, vendors typically use this terminology to describe a situation where AP1 (on channel 1) is located near AP2 (on channel 2). AP1 would receive ACI from AP2 and vice versa.

- **Non-adjacent channels** - channels with a separation between their center frequencies of more than the IEEE standard specifications for adjacent channels. Only ERP and OFDM specify non-adjacent channels as of IEEE 802.11-2007. DSSS and HR/DSSS consider channel separations greater than the IEEE standard specified minimums for adjacent channels as adjacent channels. Non-adjacent channels should not create interference with other non-adjacent channels.
- **Overlapping channels** - DSSS, HR/DSSS, or ERP channels with center frequencies separated by less than that which is specified as the minimum separation for adjacent channels in the IEEE 802.11-2007 standard. Overlapping channels create CCI. See also **CCI (Co-Channel Interference)**.

*NOTE: The CWNP Program has decided to define two separate terms for clarity: **Adjacent Overlapping Channel** (e.g., Channels that are overlapping and directly next to each other in the band, such as Wi-Fi channels 1 and 2 in the 2.4 GHz spectrum) and **Adjacent Non-***

overlapping Channel (e.g., Channels that are the first immediately side-by-side channels that do not overlap, such as Wi-Fi channels 1 and 6 in the 2.5 GHz spectrum). Wi-Fi channels 1 and 7 and 1 and 8 in the 2.4 GHz spectrum are simply considered **Non-overlapping** channels and are not adjacent.

***Channel Stacking** (WF) – when a Single Channel Architecture (SCA) is used, WLANs may be co-located in the same physical area on different 802.11 channels for the purpose of high-density/high-capacity client deployments. AKA: **Channel Spanning** and **Channel Blankets**.

Client - a radio device that uses the services of an Access Point to communicate wirelessly with other devices on a local area network.

CSMA/CA (WF) - Carrier Sense, Multiple Access with Collision Avoidance; a method of data transfer that is used to prevent data collisions (e.g. Wi-Fi) and is specified by the IEEE.

D

Data rates - the range of data transmission rates supported by a device. Data rates are measured in megabits per second (Mbps).

dB - decibel; a numerical unit designed to avoid the direct use of exponential numbers. Zero decibels is ten to the power of zero tenths, or one. Three decibels is ten to the power of three tenths or about two. Ten decibels is ten to the power of ten tenths or ten. Decibel is a convenient unit for expressing exponential power gain and loss of an RF signal.

dB_i - decibel gain or loss referenced to an isotropic antenna. Commonly used to measure antenna gain. The greater the dB_i value, the higher the gain, and the more acute the angle of coverage.

dBm - decibels referenced to 1 milliwatt. An absolute measurement of power where 0 decibels is equal to 1 milliwatt.

DHCP - Dynamic Host Configuration Protocol; a networking protocol that allows administrators to assign temporary IP addresses to network computers by “leasing” an IP address to a user for a limited amount of time, instead of assigning permanent IP addresses. DHCP servers are also capable of providing much more information to the client through DHCP options and Vendor Specific Information (VSI) entries. The device retains the assigned address for a specific administrator-defined period.

Diffraction - the bending of an RF signal around an obstacle that often results in a redirection of the signal’s main path and may result in RF shadow

DNS - Domain Name System; a server-based program that translates text names into IP addresses. The server maintains a database of host alphanumeric names and their corresponding IP addresses.

Domain name - 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.

***DRS** - Dynamic Rate Switching; this name is used in IEEE 802.11g Clause 9.6 referring to multirate support, whereby stations may change their data rate (and hence coding and modulation types in use) as they move toward or away from an access point in order to maintain a high quality connection. This was previously referred to as either “Automatic Rate Switching (ARS)” or “Dynamic Rate Selection (DRS)”- both of which were vendor-specific names for this functionality.

***DSSS** - Direct Sequence Spread Spectrum; transmission technology specified in the 802.11-1999 standard that uses 1 and 2 Mbps data rates. IEEE 802.11b and 802.11g amendments specify support for DSSS for backwards compatibility with 802.11 networks. The 802.11a amendment does not offer support for DSSS. AKA: **IEEE 802.11 clause 15 PHY** and **IEEE 802.11b** (when operating at 1 and 2mbps data rates).

***DSSS-OFDM (WF)** - Direct Sequence Spread Spectrum-Orthogonal Frequency Division Multiplexing. See **Modulation types**.

E

EAP (WF) - 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. A general authentication protocol used to control network access without relying on the network OS. Many specific authentication methods work within this framework, such as certificates, passwords, and tokens. See also **EAP types**. (IETF RFC 3748-2004)

EAP types:

- **EAP-FAST (WF, Cisco)** - Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling; a publicly accessible IEEE 802.1X EAP type developed by Cisco. It is available as an IETF informational draft. EAP-FAST provides protection from a variety of network attacks. EAP-FAST uses symmetric key algorithms to achieve a tunneled authentication process.
- **EAP-LEAP (WF, Cisco)** - EAP-Lightweight Extensible Authentication Protocol; an 802.1X (EAP) authentication type developed by Cisco that uses a username and static login password, usually a Windows login password. Cisco recommends that organizations using LEAP implement a strong password policy to protect the WLAN from dictionary attacks.
- **EAP-PEAP-MSCHAPv2 (WF)** - EAP-Protected Extensible Authentication Protocol-Microsoft Challenge Handshake Authentication Protocol version 2; a mutual authentication method that uses a combination of authentication techniques to protect the exchange of user credentials.
- **EAP-PEAP-GTC (WF, Cisco)** - EAP-PEAP-Generic Token Card; a Cisco 802.1X (EAP) authentication type where authentication follows this sequence of events:
 - The client uses a digital certificate to authenticate the authentication server
 - The client and server create an encrypted SSL/TLS tunnel
 - The server authenticates the client through EAP messages in the tunnel
 - With PEAP-GTC, authentication of the client occurs via EAP-GTC, which provides support for several types of passwords, including one-time passwords, to user databases such as Active Directory, Novell Directory Services, and those that use Lightweight Directory Access Protocol (LDAP).
- **EAP-TLS (WF)** - Extensible Authentication Protocol-Transport Layer Security; a mutual authentication method that uses digital certificates.
- **EAP-TTLS (WF)** - Extensible Authentication Protocol-Tunneled Transport Layer Security; a mutual authentication method that extends EAP-TLS. EAP-TTLS

authenticates the server to the client and does not use client-side certificates. The server uses the established secure tunnel to authenticate the client.

***EEG (WF)** - Enterprise Encryption Gateway; a L2 encryption device (similar to VPN) that allows for strong authentication and encryption of data across a wireless medium. The client devices have client-side authentication/encryption software, and the EEGs are the encryption termination point in the network. Autonomous access points are placed downstream from the EEGs and may act as an 802.1X authenticator.

F

FCC Part 15 - in the U.S., FCC Part 15 is a section of Federal Communications Commission (FCC) rules and regulations, for unlicensed transmissions. It is a part of Title 47 of the Code of Federal Regulations (CFR), and regulates everything from spurious emissions to unlicensed low-power broadcasting. It is cited as 47 CFR §15. Frequently encountered types of Part 15 transmitters include: IEEE 802.11abg Wi-Fi 2.4 GHz and 5 GHz, IEEE 802.15 PANs such as Bluetooth and ZigBee in the 2.4 GHz spectrum, and 900 MHz cordless phones.

FHSS - Frequency Hopping Spread Spectrum; a type of spread spectrum radio transmission in which the transmitter and receiver hop in synchronization from one frequency to another according to a prearranged pattern. One of the three Physical layer technologies specified in the original IEEE 802.11-1997 standard that allowed for 1 and 2 Mbps data rates in the 2.4 GHz spectrum; now obsolete.

File server - a repository for files so that a local area network can share files, mail, and programs.

Firmware - the programming code that runs a networking device. Typically programmed into a memory chip.

Frequency - the rate at which an RF wave, or any wave, repeats itself. Commonly measured in hertz, MHz, or GHz.

***FSR (WF)** - Fast Secure Roaming; a generic term for describing fast, secure handoffs between access points within an ESS. Using Robust Security Network (RSN) features such as CCMP with fast authentication methods such as preauthentication, PMK Caching, Opportunistic PMK caching, and IEEE 802.11r FT, client stations can roam from BSS to BSS performing only a 4-Way Handshake (802.11i) or over-the-air/over-the-DS exchanges (802.11r FT) instead of a full IEEE 802.1X/EAP authentication. FT is necessary for high-quality VoIP over 802.11 WLANs (wVoIP). AKA: **FT** and **Fast BSS Transition**.

G

Gain - the increase of a signal's strength.

Gateway (WF) - a device that interconnects networks with different, incompatible communications protocols.

GHz - Gigahertz; one billion cycles per second. A unit of measure for frequency.

GSM (Cell) - Global System for Mobile Communications; a 2G standard digital cellular technology. GSM operates in multiple frequency bands: 900 MHz, 1800 MHz, and 1900 MHz.

H

Hidden node (or station) - a problem that occurs in WLANs when two transmitting stations cannot hear each other but can both be heard by one of the intended receivers. This problem was

addressed in the original 802.11-1997 standard by RTS/CTS and given the name “hidden node” by the IEEE 802.11 Handbook.

***HR/DSSS (WF)** - High Rate Direct Sequence Spread Spectrum. See **Modulation types**.

***HT (11n)** - High Throughput; the set of features as defined in IEEE 802.11 Clause 20 and IEEE P802.11n. This name represents the IEEE 802.11 Clause 20 PHY where MIMO technology is used. This PHY is currently in draft format, but is in use by the Wi-Fi Alliance as an interoperability certification (draft 2.0). AKA: **IEEE 802.11n**. See also **IEEE P802.11n** and **IEEE 802.11 Clause 21**.

Hz - Hertz; the international unit for measuring frequency, equivalent to *cycles per second*. One megahertz (MHz) is one million hertz. One gigahertz (GHz) is one billion hertz. The standard U.S. electrical power frequency is 60 Hz, the AM broadcast radio frequency band is 0.55-1.6 MHz, the FM broadcast radio frequency band is 88-108 MHz, and IEEE 802.11 WLANs operate at 2.4 GHz and 5 GHz.

I

IBSS (WF) - Independent Basic Service Set; a basic service set (BSS) that forms a self-contained network, and in which no access to a distribution system (DS) is available. AKA: **Ad hoc**. See also **IBSS types**.

IBSS types (WF):

- **Ad hoc** - a group of wireless devices communicating directly with each other (peer-to-peer) without the use of an access point. AKA: **IBSS**.
- **QoS IBSS** - Quality of Service Independent Basic Service Set; an IBSS in which one or more of its stations (STAs) support the QoS facility.

***IE (WF)** - Information Element; flexible data structures within IEEE 802.11 management frames defined to have a common general format consisting of a 1 octet Element ID field, a 1 octet length field, and a variable-length element-specific information field. Each element is assigned a unique Element ID as defined in the IEEE 802.11 standard. The Length field specifies the number of octets in the Information field. Information elements occur in the frame body in order of increasing IDs. This arrangement allows for the flexible extension of the management frames to include new functionality without affecting older implementations.

IEEE - The Institute of Electrical and Electronic Engineers; a professional society serving electrical engineers through its publications, conferences, and standards development activities. The body responsible for IEEE 802.3 (Ethernet), 802.11 (WLAN), and many other specifications.

***IEEE 802.3-2005, Clause 33 PoE** - refers to the Power-over-Ethernet (PoE) standard, formerly known as IEEE 802.3af. IEEE 802.3af is an amendment to the IEEE 802.3-2002 standard. Occasionally, this may be referred to in a shortened form as “Clause 33 PoE” or just “PoE”. Clause 33 of the IEEE 802.3-2005 standard refers to the ability to deliver DC power over Category 5 (or greater) data cable for the purpose of powering network infrastructure (or other) devices. For example, access points are typically powered via PoE. AKA: **802.3af** and **Power over Ethernet (PoE)**.

***IEEE 802.11 standard (as amended) (WF)** - refers to the most current IEEE 802.11 standard (currently 802.11-2007) including all ratified amendments, supplements, and corrigenda. Many definitions in this document refer to clauses of the 802.11 standard. For example, DSSS is specified in IEEE 802.11-2007 clause 15 but is often simplified as “Clause 15”. Amendments are updates (changes) to the standard. Standards bodies like the IEEE often create several

amendments to a standard before “rolling up” the ratified amendments (finalized or approved versions) into a new standard. Corrigenda, or errata, is the correction of a book and is most commonly issued shortly after the original text was published

IEEE 802.11a-1999 (WF) - uses Orthogonal Frequency Division Multiplexing (OFDM) instead of DSSS. Provides data rates up to 54 Mbps. Uses the 5 GHz U-NII bands. Not compatible with PHYs that use the 2.4 GHz ISM band such as DSSS and HR/DSSS. See also **IEEE 802.11 Clause 17** and **OFDM**.

IEEE 802.11b-1999 (WF) - amended slightly in 2001; uses High-Rate Direct Sequence Spread Spectrum (HR/DSSS) instead of the original DSSS. Provides data rates up to 11 Mbps. Uses the 2.4 GHz ISM band. Backward compatible with DSSS. See also **IEEE 802.11 Clauses 15 and 18, DSSS**, and **HR-DSSS**.

IEEE 802.11g-2003 (WF) - supports DSSS and HR/DSSS and adapts OFDM modulation to 2.4 GHz band. Provides data rates up to 54 Mbps. Not compatible with the 5 GHz OFDM PHY due to the use of the 2.4 GHz band. AKA: **ERP-OFDM**. See also **IEEE 802.11 standard (as amended)**.

IEEE 802.11i-2004 (WF) - one of the most important enhancements to the IEEE 802.11 standard. Specifies the use of Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP), which is reliant on the Advanced Encryption Standard (AES) and allows for the use of the Temporal Key Integrity Protocol (TKIP). Requires the use of either IEEE 802.1X or preshared key (PSK) for authentication. See also **IEEE 802.11 standard (as amended)**.

IEEE P802.11n - ratification expected late in 2008 or early 2009; defines modifications to the IEEE 802.11 physical and media access control layers that will allow for much higher throughputs and a maximum throughput of at least 100 Mbps. This is currently being accomplished with the use of MIMO (multiple-input-multiple-output) technology in conjunction with OFDM technology.

***Information Field** (WF) - a fixed-length, mandatory component within IEEE 802.11 management frames. These are sometimes called “fixed fields” due to the terminology used by the IEEE 802.11-1999 (R2003) standard. In the IEEE 802.11-2007 standard, these fields have been renamed to “Information Field.” AKA: **Fixed field**.

Infrastructure (WF) - the infrastructure includes the distribution system medium (DSM), access point (AP), and portal entities. It is also the logical location of distribution and integration service functions of an extended service set (ESS). An infrastructure contains one or more APs and zero or more portals in addition to the distribution system (DS).

IP - Internet Protocol; a protocol used to address and send data over a network.

IP address - the Internet Protocol address used to identify a computer or device on a network.

IP subnet mask - 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.

Isotropic radiator - a theoretical device that can radiate energy equally in all directions. The sun is the closest thing we have to an isotropic radiator but it is not a “true” isotropic radiator. The Sun has its own internal power source versus one that comes from an external-ported-to-internal power source (like an antenna or light bulb) but it does not radiate equally in all directions. If humans could develop a zero-point energy engine or a perpetual motion machine, we could achieve something close to an isotropic radiator. See also **Hairy ball theorem**.

L

LAN - Local Area Network; a high-speed, data network covering a relatively small geographic area (up to a few thousand meters). LANs connect workstations, peripherals, terminals, and other devices in a single building or other geographically limited area that make up your local network. LAN standards specify cabling and signaling at the physical and data link layers of the OSI model. Ethernet, FDDI, and Token Ring are widely used LAN technologies. See also **WLAN**.

LWAPP (Cisco) - Lightweight Access Point Protocol; a standardized protocol that governs how lightweight access points communicate with WLAN systems. The protocol is independent of wireless Layer 2 technology, but an 802.11 binding is provided. The CAPWAP standard is based on LWAPP. See also **CAPWAP**.

M

MAC - Media Access Control; the MAC protocol sub-layer is a part of the Data Link layer (Layer 2) specified in the OSI model. It provides addressing and channel access control mechanisms that make it possible for several terminals or network nodes to communicate within a multipoint network such as a LAN or MAN. The MAC sub-layer acts as an interface between the Logical Link Control sublayer and the network's physical layer (PHY). The MAC layer provides an addressing mechanism called the physical address or MAC address. This is a unique serial number assigned to each network adapter, making it possible to deliver data packets to a destination within a subnetwork.

MIMO (11n) - Multiple Input, Multiple Output; a PHY configuration in which both transmitter and receiver use multiple antennas. The standardized American English pronunciation of MIMO is "my-mow."

***MMPDU** (WF) - Medium Access Control (MAC) Management Protocol Data Unit; the unit of data exchanged between two peer MAC entities to implement the MAC management protocol. MMPDUs are sourced and sunk at layer 2 of the OSI model (between immediate transmitters and receivers). They are never forwarded across an access point like an MSDU.

Modulation - any of several techniques for combining user information with a transmitter's carrier signal by changing one or more properties of the signal. See also **Modulation types**.

Modulation types:

- ***DSSS-OFDM** (WF) - Direct Sequence Spread Spectrum-Orthogonal Frequency Division Multiplexing; an optional ERP modulation specified by the IEEE 802.11g amendment. This is a hybrid modulation combining a DSSS preamble and header with an OFDM payload transmission. DSSS-OFDM has payload data rates of 6, 9, 12, 18, 24, 36, 48, and 54 Mbps as defined in Clause 19.7. The supported rates are the same as the ERP-OFDM supported rates.
- ***ERP** (WF) - Extended Rate Physical; Clause 19 specifies further rate extension of the PHY for the DSSS system of Clause 15 and the extensions of Clause 18 (HR/DSSS). This PHY operates in the 2.4 GHz ISM band and builds on the payload data rates of 1 and 2 Mbps, as described in Clause 15, that use DSSS modulation and builds on the payload data rates of 1, 2, 5.5, and 11 Mbps, as described in Clause 18, that use DSSS, CCK, and optional PBCC modulations. ERP-OFDM draws from Clause 17 (OFDM) to provide additional payload data rates of 6, 9, 12, 18, 24, 36, 48, and 54 Mbps. Of these rates, transmission and reception capability for 1, 2, 5.5, 11, 6, 12, and 24 Mbps data rates is mandatory. AKA: **IEEE 802.11b**, **IEEE 802.11g**, and **Clause 19**.

- ***ERP-DSSS (WF)** - a required ERP modulation specified by the IEEE 802.11g amendment that uses the capabilities of Clause 18 (HR/DSSS) with the following exceptions:
 - Support of the short PLCP PPDU header format capability of Clause 18.2.2.2 is mandatory.
 - CCA (see Clause 18.4.8.4) has a mechanism that will detect all mandatory Clause 19 sync symbols.
 - The maximum input signal level (see 18.4.8.2) is -20 dBm.
 - Locking the transmit center frequency and the symbol clock frequency to the same reference oscillator is mandatory.
- ***ERP-OFDM (WF)** - a required ERP modulation specified by the 802.11g amendment that uses the capabilities of clause 17 (OFDM) with the following exceptions:
 - The frequency plan is in accordance with Clause 18.4.6.1 and 18.4.6.2 instead of 17.3.8.3.
 - CCA has a mechanism that will detect all mandatory Clause 19 sync symbols.
 - The frequency accuracy (see Clause 17.3.9.4 and 17.3.9.5) is ± 25 PPM.
 - The maximum input signal level (see Clause 17.3.10.4) is -20 dBm.
 - The slot time is 20 μ s in accordance with 18.3.3, except that an optional 9 μ s slot time may be used when the BSS consists of only ERP STAs.
 - SIFS time is 10 μ s in accordance with 18.3.3. See Clause 19.3.2.3 for more detail.

AKA: **IEEE 802.11g**. See also **OFDM** and **IEEE 802.11g**.
- ***ERP-PBCC (WF)** - Extended Rate Physical Packet Binary Convolutional Coding; an optional ERP modulation specified by the IEEE 802.11g amendment. This is a single-carrier modulation scheme that encodes the payload using a 256-state packet binary convolutional code. These are extensions to the PBCC modulation in IEEE 802.11 Clause 18. ERP-PBCC modes with payload data rates of 22 and 33 Mbps are defined in Clause 19.6.
- ***HR/DSSS (WF)** - High Rate Direct Sequence Spread Spectrum; new modulation types were introduced to enhance data rates to 5.5 and 11 Mbps. HR/DSSS is backwards compatible with DSSS, meaning an HR/DSSS station can also understand DSSS transmissions at 1 and 2 Mbps. IEEE 802.11b was the first 802.11 amendment to support HR/DSSS. The IEEE 802.11g amendment specifies support for HR/DSSS for backwards compatibility with the IEEE 802.11b amendment. The IEEE 802.11a amendment does not offer support for HR/DSSS. AKA: **IEEE 802.11 clause 18** and **IEEE 802.11b** when operating at 1, 2, 5.5, and 11mbps data rates.
- ***OFDM (WF)** - Orthogonal Frequency Division Multiplexing (clause 17). This transmission technology was introduced in the IEEE 802.11a amendment and is used in the 5 GHz UNII bands. It allows data rates of 6, 9, 12, 18, 24, 36, 48, and 54 Mbps, with mandatory support of 6, 12, and 24 Mbps. OFDM is not backwards compatible with HR/DSSS or DSSS because it is used in a different frequency band and it uses a different modulation technique. The acronym OFDM is also used to describe the modulation technique it pioneered which was then used as one of the several modulations supported by the ERP. The IEEE 802.11a amendment introduced use of OFDM which was then

also used in the IEEE 802.11g amendment at a later time. AKA: **IEEE 802.11 clause 17 PHY** and **IEEE 802.11a**. See also **IEEE 802.11 clause 17** and **IEEE 802.11a**.

***MPDU** (WF, WMX) - Medium Access Control (MAC) Protocol Data Unit. The unit of data exchanged between two peer MAC entities using the services of the physical layer (PHY). It is comprised of an MSDU (data payload), a MAC header, and a trailer.

***MSDU** (WF, WMX) - Medium Access Control (MAC) Service Data Unit; the data presented at the MAC service access point (the entry point into the MAC sublayer) by upper layer protocols. An MSDU can be comprised of data from the LLC sublayer and/or any number of layers above the Data-Link layer.

Multicast - when applied to a medium access control (MAC) service data unit (MSDU), it is an MSDU with a multicast address as the destination address (DA). When applied to a MAC protocol data unit (MPDU) or control frame, it is an MPDU or control frame with a multicast address as the receiver address (RA).

Multicast packet - a single data message (packet) sent to multiple addresses.

Multipath - that which occurs when multiple copies of the original signal arrive at the receiver close to the same time after experiencing reflection, diffraction, scattering, and other RF behaviors.

Multiple Basic Service Set Identifier (MBSSID) (Cisco) - the goal of MBSSID is to create unique beacon transmissions for each BSSID allowing access points to appear to client devices to be several distinct co-located AP's or multiple-virtual AP's. This allows up to 8 MBSSIDs per radio or 16 MBSSIDs per AP (in a dual-radio AP), multiple multicast streams, and support for existing clients with no changes/impact on client devices. See also **SSIDL**.

***Multiple Channel Architecture** (WF) - a WLAN architecture where three or more channels are used in a tiled pattern within a frequency band (2.4 or 5 GHz) for the purpose of minimizing co-channel and adjacent channel interference. This is often referred to as "channel reuse" or "micro-cell" architecture. More non-overlapping channels in the reuse pattern are used for higher capacity.

mW - milliwatt; the measurement most frequently used when referencing output power of WLAN devices.

O

***Octet** - a term used to describe 8 bits of data. Interchangeable with the term "byte". The term 'octet' is used more often in standards such as IEEE 802.11 because it is considered more accurate than "byte". AKA: **byte**.

P

Packet - a basic message unit for communication across a network. A packet usually includes routing information, data, and sometimes error detection information.

PCI - Payment Card Industry; a general term which collectively describes the debit, credit, pre-paid, e-purse, ATM, and POS cards and associated businesses.

Polarization - the physical orientation of an antenna, typically vertical or horizontal but there are some antennas that have circular polarization as well. An antenna will generate an electromagnetic wave that varies in time as it travels through space. If a wave traveling "outward" varies "up and down" in time with the electric field always in one plane, that wave (or antenna) is

said to be linearly polarized (vertically polarized since the variation is up and down rather than side to side). Linear polarization also includes the possibility of the electromagnetic waves traveling “right to left” (horizontally) as well. If a wave rotates or “spins” in time as it travels through space, the wave (or antenna) is said to be elliptically polarized. As a special case, if that wave spins out in a circular path, the wave (or antenna) is circularly polarized. This implies that certain antennas are sensitive to particular types of electromagnetic waves. The practical implication of this concept is that antennas with the same polarization provide the best transmission/reception path.

***PS mode (WF)** - Power Save (Mode); power management of a non-AP STA operates in either active mode or power-save mode. A STA in power-save mode is either in an awake or doze state. Power-save mode conserves battery life while the STA dozes, but complicates frame delivery with additional queuing, frame types, and frame exchange sequences. Vendors have called this, “Power Save Poll (PSP)” mode or sleep mode. Wireless STAs that are always powered by an AC outlet should never be configured for power-save mode. See also **Active mode**.

Q

QoS - Quality of Service; guaranteeing that certain types of network traffic that depend on low latency (like VoIP) will be given priority.

R

Range - a linear measure of the distance that a transmitter can send a signal.

Receiver sensitivity - a measurement of the weakest signal a receiver can receive and still correctly translate it into data.

RF - Radio Frequency; a frequency used to carry radio signals.

Roaming (WF) - the ability to take a wireless device from one access point's range to another, usually without losing the WLAN connection (system dependent).

RP-TNC - Reverse Polarity-Threaded Naval Connector; a connector type unique to Cisco Aironet 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 Aironet, like all other wireless LAN providers, equips its radios and antennas with a unique connector to prevent attachment of non-approved antennas to radios, however, these “unique” connectors are no longer unique since it is easy to convert from one type to another using adapters.

***RSN (WF)** - Robust Security Network; a security network that allows only the creation of robust security network associations (RSNAs). An RSN can be identified by the indication in the RSN Information Element (IE) of Beacon frames that the group cipher suite specified is not WEP. This means that the group cipher suite will be either CCMP or TKIP.

S

***Single Channel Architecture (WF)** - a WLAN architecture where all access points in the network can be deployed on one channel in 2.4 GHz or 5 GHz frequency bands. Uplink and downlink transmissions are coordinated by a WLAN Controller on a single 802.11 channel in such a manner that the effects of co-channel and adjacent channel interference are minimized. Additional non-overlapping channels can be used to create layers of single channels for higher network capacity.

Site survey - the process of evaluating RF behavior in an environment and determining the best way to implement a WLAN based on this information. Site surveys can be manual, predictive, virtual, or RF (the actual environment is surveyed).

Slot Time (WF) - the amount of time a device waits after a collision before retransmitting a packet. You can increase throughput on 802.11g, 2.4-GHz radios by enabling short slot time (most .11g radios enable this by default). *Reducing the slot time from the standard 20 microseconds to the 9-microsecond short slot time decreases the overall backoff, which increases throughput.* Backoff, which is a multiple of the slot time, is the random length of time a station waits before sending a packet on the LAN. Many 802.11g radios support short slot time, but some do not. When short slot time is enabled, the wireless device uses the short slot time only when all clients associated to the 802.11g, 2.4-GHz radio support short slot time. Short slot time is an 802.11g-only feature and does not apply to 802.11a radios. *Slot times should transition from 20us to 9us when a "pure" .11g environment exists for that AP.* Most 802.11g (ERP) radios enable short slot times by default. If you have a .11b/g radio and there are .11b (HR-DSSS) clients associated to that AP, then, per the standard, the AP MUST switch to "Short Slot Time = 0" in the Beacon frames. HR-DSSS and DSSS radios only understand long (20us) slot times. Short slot times (9us) only exist when .11g-only (ERP) devices are associated to a .11g (ERP) AP. Typically, you don't "disable" short slot times; instead, the AP enables/disables them depending on the type of associated client radios (Pure ERP-OFDM = 1, Mixed = 0). Some vendors allow you to turn it off if you want, but there is no sense in doing so.

Split MAC Architecture - the Cisco Unified Wireless Network (CUWN) architecture centralizes WLAN configuration and control on a device called a wireless LAN controller (WLC). This allows the WLAN to operate as an intelligent information network and to support advanced services, unlike the traditional 802.11 WLAN infrastructure, which is built from autonomous, discrete entities. The Cisco Unified Wireless Network architecture simplifies operational management by collapsing large numbers of managed endpoints, autonomous APs, into a managed system of WLAN controllers. In this architecture, APs are lightweight, meaning that they cannot act independently of a WLC. The WLC manages the AP configurations and firmware. The APs are "zero-touch" deployed, and no individual configuration of APs is required. The APs are also lightweight in the sense that they handle only real-time MAC (media access control) functionality, leaving the WLC to process all the non-real-time MAC functionality.

Spread Spectrum (WF) - wideband radio frequency technique used for more reliable and secure data transmission. A 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.

SSID (WF) - Service Set Identifier; 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. The SSID is actually the ID of the ESS and not the BSS. The BSS has an ID and it is the BSSID. The ESS has an ID too and it is the SSID.

STA - station; any device that contains an IEEE 802.11-conformant medium access control (MAC) and physical layer (PHY) interface to the wireless medium (WM). A station can only be associated with one BSS at a time.

T

Throughput (WF) - the amount of data moved successfully from one node to another in a given time period.

Transmit power - the effective isotropic radiated power (EIRP) when referring to the operation of a 5 GHz IEEE 802.11 orthogonal frequency division multiplexing (OFDM) physical layer (PHY) in a country where so regulated.

U

Unicast - when applied to a medium access control (MAC) service data unit (MSDU), it is an MSDU with a single recipient address as the destination address (DA). When applied to a MAC protocol data unit (MPDU) or control frame, it is an MPDU or control frame with a single recipient address as the receiver address (RA).

Unicast packet - a single data message (packet) sent to a specific IP address.

***Unlicensed National Information Infrastructure (UNII) bands** - these bands are located between 5 GHz and 6 GHz and are defined by the FCC for use by unlicensed RF transmitters. They consist of the following frequency bands.

Band	CWNP name:	Often called:
5.15 - 5.25 GHz	UNII-1	Lower UNII
5.25 - 5.35 GHz	UNII-2	Middle UNII
5.470 - 5.725 GHz	UNII-2E	UNII-2 Extended
5.725 - 5.825 GHz	UNII-3	Upper UNII

Note: The FCC formally uses “U-NII” but it is acceptable to use “UNII”.

V

***Virtual BSSID** (WF) - when two or more access points coordinated by a WLAN Controller appear to be the same access point (i.e., they have the same BSSID). AKA: **Virtual Cell**.

***VoWiFi** - Voice over Wi-Fi; refers to the transmitting of voice over Internet Protocol (VoIP) over an 802.11 data link. There are several interchangeable terms although The CWNP Program has standardized on VoWiFi. AKA: **VoFi, VoWi-Fi, VoWLAN, and wVoIP**.

VSWR - Voltage Standing Wave Ratio; a reflected signal caused by an impedance mismatch between devices (i.e., connectors, cables, Access Points) in an RF system. VSWR is the ratio of the maximum voltage to the minimum voltage in a standing wave pattern. A standing wave is developed when power is reflected from a load. So the VSWR is a measure of how much power is delivered to a device as opposed to the amount of power that is reflected from the device. If the source and load impedance are the same, the VSWR is 1:1; there is no reflected power. So the VSWR is also a measure of how closely the source and load impedance are matched. For most antennas in WLAN, it is a measure of how close the antenna is to a perfect 50 Ohms.

W

WDS (WF) - Wireless Distribution System; a mechanism for wireless communication using a four address frame format specified in the IEEE 802.11 standard. The standard describes such a frame format, but does not describe how such a mechanism or frame format would be used.

WEP (WF) - 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 wired network. A deprecated cryptographic data confidentiality algorithm specified by IEEE 802.11 that may be used to provide data confidentiality that is subjectively equivalent to the data confidentiality of a wired local area network (LAN) medium that does not employ cryptographic techniques to enhance data confidentiality.

Wi-Fi - a vendor consortium brand name for IEEE 802.11 devices guaranteed to interoperate in certain ways. The name was chosen by the predecessor of the Wi-Fi Alliance, the Wireless Ethernet Compatibility Alliance (WECA); sometimes erroneously thought to mean “Wireless Fidelity”.

***Wi-Fi Alliance (WF)** - formerly known as the Wireless Ethernet Compatibility Alliance (WECA), the Wi-Fi Alliance is a nonprofit international association formed in 1999 to certify interoperability of Wireless Local Area Network products based on the IEEE 802.11 standard and amendments. Wi-Fi Alliance certification programs address Wi-Fi products based on IEEE radio standards (e.g. IEEE 802.11a, 802.11b, 802.11g), wireless network security (WPA, WPA2, and WPS for personal and enterprise deployments), authentication mechanisms used to validate the identity of network devices (EAP), and support for multimedia content over Wi-Fi networks (WMM and WMM-PS).

WLAN (WF) - Wireless Local Area Network; a system that includes the distribution system (DS), access points (APs), and portal entities. It is also the logical location of distribution and integration service functions of an extended service set (ESS). A WLAN system contains one or more APs and zero or more portals in addition to the DS.

***WLAN Controller (WF)** - typically network appliances or enterprise switch modules that communicate and manage lightweight (also called “thin”) access points. The architecture that uses WLAN controllers and lightweight APs is often called a “Split MAC” architecture. Lightweight APs typically have less intelligence or processing capabilities than autonomous (also called “thick” or “fat”) APs. A WLAN controller houses most of the intelligence in this architecture and is used to centrally control (thus the name) and manage the access points. The predominant reason for the industry migration to this architecture is the simplified, centralized management and control of large groups of access points from a single controller or cluster of controllers. AKA: **WLAN Switch and Controller**.

***WLAN Profile** - a group of settings within an 802.11 WLAN controller that characterizes the parameters needed for a client station to connect to the network infrastructure wirelessly. For example, authentication type, cipher suite, QoS, VLAN, RADIUS parameters, ESSID, and protocol filters can be configured as a group of WLAN Profile parameters, and a WLAN controller may have many such profiles configured simultaneously. The purpose of WLAN Profiles is to simulate many independent wireless LANs within a single WLAN infrastructure.

WLSE (Cisco) - Wireless LAN Solution Engine; a network appliance for managing Cisco Aironet autonomous wireless LAN infrastructures.

WLSM (Cisco) - Wireless LAN Services Module; a module for the Cisco Catalyst 6500 Switch family that enables network management for Cisco Aironet autonomous APs and provides fast secure campus-wide wireless Layer 3 roaming.

***WMM (WF)** - Wi-Fi Multimedia; a certification created by the Wi-Fi Alliance for support of multimedia applications with QoS in Wi-Fi networks. The Wi-Fi Alliance started interoperability certification for WMM as a profile of the IEEE 802.11e QoS extensions for 802.11 networks. WMM prioritizes traffic demands from different applications and extends Wi-Fi’s high quality end-user experience from data connectivity to voice, music, and video applications under a wide

variety of environment and traffic conditions. WMM defines four access categories (voice, video, best effort, and background) that are used to prioritize traffic so that these applications have access to the necessary network resources. Additionally, WMM-enabled Wi-Fi networks concurrently support legacy devices that lack WMM functionality. The WMM best effort access category and legacy devices transmit with the same priority.

***WMM-PS (WF)** - the IEEE 802.11e amendment introduced Automatic Power Save Delivery (APSD) functionality in two flavors: Scheduled and Unscheduled. The acronyms used by the standard for these are S-APSD and U-APSD. The Wi-Fi Alliance adopted U-APSD in their Wi-Fi Multimedia Power Save (WMM-PS) certification. Both U-APSD and WMM-PS refer to the same power saving functionality introduced by the IEEE 802.11e amendment. AKA: **U-APSD**. See also **U-APSD** and **S-APSD**.

***WNMS (WF)** - Wireless Network Management System; a network device management system that is used for monitoring, configuring, and updating autonomous access points or WLAN controllers with lightweight access points. Some vendors make only WNMS systems to manage other vendors' equipment and some vendors make WNMS to manage only their own WLAN controllers and access points. Sample features include device configuration and management, user monitoring, government and industry compliance reporting, and automating of routine tasks.

***WPA-Enterprise and WPA2-Enterprise (WF)** - Enterprise Mode operates in a managed mode to meet the rigorous requirements of enterprise security. It leverages the IEEE 802.1X authentication framework which uses an Extensible Authentication Protocol (EAP) method with an authentication server to provide strong mutual authentication between the client and authentication server via the access point or WLAN controller. In this mode, each user is assigned a unique key mechanism for access to the WLAN. This affords a high level of individual privacy. For WPA, TKIP/RC4 encryption is used. TKIP employs an encryption cipher that issues encryption keys for each data packet communicated in each session for each user, making the encryption code extremely difficult to break. For WPA2, CCMP/AES encryption is used. CCMP/AES is stronger than TKIP/RC4, thus providing additional network protection; however, CCMP/AES requires more processing power than many legacy WLAN devices provide. A hardware upgrade to more modern equipment is usually required for CCMP/AES support. TKIP uses the RC4 encryption cipher originally used in WEP, typically requiring only a firmware upgrade to most legacy equipment. WPA2 also supports TKIP v2, which is not compatible with the TKIP v1 used by WPA. WPA and WPA2 were developed by the Wi-Fi Alliance based upon the IEEE 802.11i amendment. See also **WPA** and **WPA2**.

***WPA-Personal and WPA2-Personal (WF)** - Wi-Fi Protected Access Personal Mode (versions 1 and 2) are designed for home and small office/home office (SOHO) users who do not have authentication servers available. It operates in an unmanaged mode that uses a preshared key (PSK) for authentication instead of IEEE 802.1X/EAP. This mode uses applied authentication in which a passphrase is manually entered on the access point to generate an encryption key (called the PSK). Consequently, it does not scale well in the enterprise. The PSK is typically shared among users. A PSK of sufficient strength - one that uses a mix of letters, numbers and non-alphanumeric characters - is recommended. Personal Mode uses the same encryption methods as Enterprise Mode. It supports per-user, per-session, per-packet encryption via TKIP/RC4 with WPA or CCMP/AES with WPA2. Home and SOHO users should consult a vendor to learn more about deploying WPA-Personal or WPA2-Personal and PSK for their environments. WPA2 also supports TKIP v2, which is not compatible with the TKIP v1 used by WPA. WPA and WPA2 were developed by the Wi-Fi Alliance based upon the IEEE 802.11i amendment. See also **WPA** and **WPA2**.

Bibliography

Bluetooth SIG

- <http://www.bluetooth.com>
- <http://www.bluetooth.org>

Cisco Systems, Inc.

- <http://www.cisco.com/go/wireless>

CWNP

- Certification Overview: <http://www.cwnp.com/certifications>
- Discussion Forum: <http://www.cwnp.com/phpBB2/index.php>
- CWNA Official Study Guide, 4th Edition
(ISBN: 0-07-149490-1), Carpenter, Tom. McGraw-Hill, 2007.

IEEE

- IEEE Main Website:
<http://www.ieee.com>
- IEEE Standards:
<http://standards.ieee.org>
- IEEE books:
<http://standards.ieee.org/standardspress>

Infrared Data Association (IrDA)

- <http://www.irda.org>

Wi-Fi Alliance

- <http://www.wi-fi.org>

WiMAX Forum

- <http://www.wimaxforum.org>

WiMedia Alliance

- <http://www.wimedia.org>

ZigBee Alliance

- <http://www.zigbee.org>

**Official CWNP Dictionary
Of Wireless Terms & Acronyms**

SAMPLE ONLY

Selected Definitions from the Official Dictionary available at CWNP.com