CWNP Exam Terms (Revised: 08/17/2009)

Active Mode - 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.

Adjacent Overlapping Channel / Adjacent Non-overlapping Channel - 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

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.

> **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 in a case where AP-1 (channel 1) is located near AP-2 (channel 2).

The CWNP Program has decided to define two separate terms for clarity: ***Adjacent Overlapping Channel*** (e.g. channels 1 and 2 that are overlapping, and are directly next to each other in the band) and ***Adjacent Non-overlapping Channel*** (e.g. channels 1 and 6, that are the first immediately side-by-side channels that do not overlap). Channels 1 and 7, 1 and 8, etc are simply considered ***Non-overlapping*** channels, and are not adjacent.

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 results in both throughput degradation and latency.

A-MSDU - A structure containing multiple MSDUs, transported within single (unfragmented) or multiple (fragmented) Data MPDUs.

A-MPDU - A structure containing multiple MPDUs, transported as a single PSDU by the PHY.

Announcement Traffic Indication Message (ATIM) – 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.

Autonomous Access Point – This type of access points contains full MAC layer processing locally within the AP and is sometimes known as a "fat" or "thick" AP. In the early days of WLANs, all APs were autonomous. While autonomous APs typically have greater memory and processing performance than controller-based APs, the original drawback of autonomous APs was that they required individual management, which limited scalability. In modern WLANs, controller-based architectures are predominant, though autonomous APs that are centrally managed via a WNMS may be used as well.

Channel Stacking / Channel Spanning / Channel Blankets – 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.

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 latency.

Controller-based Access Point – This type of access point is a part of a controller-based system, often called a "Split MAC" architecture. In this system, WLAN controllers communicate with controller-based (also called "lightweight" or "thin") access points (APs). Controller-based 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 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.

DSSS – Direct Sequence Spread Spectrum (clause 15). This transmission technology is specified in the 802.11-1999 standard and uses 1 and 2 Mbps data rates. 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.

DSSS-OFDM – An optional ERP modulation specified by the 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 are defined in 19.7. The supported rates are the same as the ERP-OFDM supported rates.

Dynamic Rate Switching (DRS) – This name is used in 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.

Enterprise Encryption Gateway (EEG) – An EEG is 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.

ERP – Extended Rate Physical (clause 19). This clause specifies further rate extension of the PHY (physical layer specification) for the Direct Sequence Spread Spectrum (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.

ERP-DSSS – A required ERP modulation specified by the 802.11g amendment that uses the capabilities of clause 18 (HR/DSSS) with the following exceptions:

1. Support of the short PLCP PPDU header format capability of 18.2.2.2 is mandatory.
2. CCA (see 18.4.8.4) has a mechanism that will detect all mandatory Clause 19 sync symbols.
3. The maximum input signal level (see 18.4.8.2) is -20 dBm.
4. Locking the transmit center frequency and the symbol clock frequency to the same reference oscillator is mandatory.

ERP-OFDM – A required ERP modulation specified by the 802.11g amendment that uses the capabilities of clause 17 (OFDM) with the following exceptions:

1. The frequency plan is in accordance with 18.4.6.1 and 18.4.6.2 instead of 17.3.8.3.
2. CCA has a mechanism that will detect all mandatory Clause 19 sync symbols.
3. The frequency accuracy (see 17.3.9.4 and 17.3.9.5) is ±25 PPM.
4. The maximum input signal level (see 17.3.10.4) is -20 dBm.
5. The slot time is 20 µs in accordance with 18.3.3, except that an optional 9 µs slot time may be used when the BSS consists of only ERP STAs.
6. SIFS time is 10 µs in accordance with 18.3.3. See 19.3.2.3 for more detail.

In a nutshell, this is our way of saying 802.11g using OFDM.

ERP-PBCC – An optional ERP modulation specified by the 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 Clause 18. ERP-PBCC modes with payload data rates of 22 and 33 Mbps are defined in 19.6.

Fast BSS Transition (FT) / Fast Secure Roaming (FSR) – This is 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 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 802.1X/EAP authentication. FT is necessary for high-quality VoIP over 802.11 WLANs (VoWiFi).

High Throughput – This name represents the 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).

HR/DSSS – High Rate Direct Sequence Spread Spectrum (clause 18). 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. 802.11b was the first 802.11 amendment to support HR/DSSS. The 802.11g amendment specifies support for HR/DSSS for backwards compatibility with the 802.11b amendment. The 802.11a amendment does not offer support for HR/DSSS.

IEEE 802.3-2005, clause 33 PoE – This name refers to the Power-over-Ethernet (PoE) standard formerly known as IEEE 802.3af. The 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.

IEEE 802.11 standard (as amended) – This name refers to the most current 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.

Information Element – Information Elements are flexible data structures within 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 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.

Information Field – A fixed-length, mandatory component within 802.11 management frames. These are sometimes called "fixed fields" due to the terminology used by the 802.11-1999 (R2003) standard. In the 802.11-2007 standard, these fields have been renamed to "Information Field."

MMPDU – 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.

MPDU – 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 – Medium Access Control (MAC) Service Data Unit. This is 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.

Multiple Channel Architecture (MCA) – 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.

Non-ERP – Non Extended Rate Physical (clauses 15 and 18). This term describes STAs that are not ERP STAs but that can interoperate with ERP STAs, specifically DSSS and HR/DSSS.

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."

OFDM – 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 802.11g amendment at a later time.

Power Save (PS) mode - Power management of a non-AP station (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.

Robust Security Network (RSN) - 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 wired equivalent privacy (WEP). This means that the group cipher suite will be either CCMP or TKIP.

Single Channel Architecture (SCA) – 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 creating layers of single channels for higher network capacity.

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

Virtual BSSID / Virtual Cell – When 2 or more access points coordinated by a WLAN Controller appear to be the same access point (have the same BSSID).

VoWiFi / VoWi-Fi / wVoIP / VoWLAN / VoFi – These terms refer to the transmitting of voice over Internet Protocol (VoIP) over an 802.11 data link. These terms are considered interchangeable, though The CWNP Program has standardized on VoWiFi.

Wi-Fi Alliance – 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. 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).

Wi-Fi Multimedia (WMM) – A certification created by the Wi-Fi Alliance for support of multimedia applications with quality of service (QoS) in Wi-Fi networks. The Wi-Fi Alliance started interoperability certification for WMM (Wi-Fi Multimedia) 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.

Wireless Network Management System (WNMS) – A network device management system that is used for monitoring, configuring, and updating autonomous access points or WLAN controllers with controller-based 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.

WLAN Controller – also known as a "WLAN switch." WLAN controllers communicate with controller-based (also called "lightweight" or "thin") access points (APs). The architecture that uses WLAN controllers and controller-based APs is often called a "Split MAC" architecture. Controller-based 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.

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.

WMM-PS or U-APSD – 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.

WPA-Enterprise and WPA2-Enterprise – 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 of each user, making the encryption code extremely difficult to break. For WPA2, either CCMP/AES, TKIP/RC4, or both encryption methods may be 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. WPA and WPA2 were developed by the Wi-Fi Alliance based upon the IEEE 802.11i amendment.

WPA-Personal and WPA2-Personal – 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 typically entered manually 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. CCMP/AES, TKIP/RC4, or both are supported 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. WPA and WPA2 were developed by the Wi-Fi Alliance based upon the IEEE 802.11i amendment.