



WildPackets

Wireless Network Glossary

802.11 The IEEE standard for wireless connectivity at 1 Mbps and 2 Mbps in the 2.4 GHz band.

802.11a The IEEE standard for wireless connectivity in the range of 54 Mbps in the 5.0 GHz band.

802.11b The IEEE standard for wireless connectivity at data rates up to 11 Mbps in the 2.4 GHz band.

802.11c Bridge Operation Procedures - 802.11c provides required information to ensure proper bridge operations. This project is completed, and related procedures are part of the IEEE 802.11c standard. Product developers utilize this standard when developing access points. There's really not much in this standard relevant to wireless LAN installers.

802.11d Global Harmonization - When 802.11 first became available, only a handful of regulatory domains (e.g., U.S., Europe, and Japan) had rules in place for the operation of 802.11 wireless LANs. In order to support a widespread adoption of 802.11, the 802.11d task group has an ongoing charter to define PHY requirements that satisfy regulatory within additional countries. This is especially important for operation in the 5GHz bands because the use of these frequencies differ widely from one country to another. As with 802.11c, the 802.11d standard mostly applies to companies developing 802.11 products.

802.11e IEEE working group that has the following task: Enhance the 802.11 Medium Access Control (MAC) to improve and manage Quality of Service, provide classes of service, and enhanced security and authentication mechanisms. Consider efficiency enhancements in the areas of the Distributed Coordination Function (DCF) and Point Coordination Function (PCF).

802.11f IEEE 802.11 Working group F: This Task Group is developing a Standard for ESS Mesh Networking.

802.11g The IEEE standard for wireless local area networks (WLANs) that offers transmission over relatively short distances at up to 54 megabits per second (Mbps). Networks employing 802.11g operate at radio frequencies between 2.400 GHz and 2.4835 GHz, the same band as 802.11b. But the 802.11g specification employs orthogonal frequency division multiplexing (OFDM), the modulation scheme used in 802.11a, to obtain higher data speed. Computers or terminals set up for 802.11g can fall back to speeds of 11 Mbps. This feature makes 802.11b and 802.11g devices compatible within a single network.

802.11h IEEE 802.11 working group H: The purpose of Task Group H was the Spectrum and transmit power management extensions in the 5 GHz band in Europe.

802.11i This IEEE standard 802.11i is a standard for wireless local area networks that provides improved encryption for networks that use the popular 802.11a, 802.11b and 802.11g standards. The 802.11i standard requires new encryption key protocols, known as Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES). The 802.11i standard was officially ratified by the IEEE in June of 2004, and thereby became part of the 802.11 family of wireless network specifications.

802.11j IEEE 802.11 working group J: The purpose of Task Group J is to enhance the 802.11 standard and amendments, to add channel selection for 4.9 GHz and 5 GHz in Japan; to conform to the Japanese rules on operational mode, operational rate, radiated power, spurious emissions and channel sense.

802.11k IEEE 802.11 Working group K: This Task Group will define Radio Resource Measurement enhancements to provide mechanisms to higher layers for radio and network measurements

802.11n IEEE 802.11 Working group N: This Task Group is developing a Standard for Enhancement for High Throughput (100Mbit +).

802.11r IEEE 802.11 Working group R: This Task Group is developing a Standard for Fast Roaming.

802.11s IEEE 802.11 Working group S: This Task Group is developing a Standard for ESS Mesh Networking.

802.1x As the IEEE standard for port access control for wireless and wired LANs, 802.1x provides a means of authenticating and authorizing devices to attach to a LAN port. This standard defines the Extensible Authentication Protocol (EAP), which uses a central authentication server to authenticate each user on the network.

Access point (AP) An interface between the wireless network and a wired network. Access points combined with a distribution system (e.g. Ethernet) support the creation of multiple radio cells (BSSs) that enable roaming.

Ad hoc network A wireless network composed only of stations and no access point. Also referred to as an Independent Basic Service Set Network (IBSS Network).

AES (Advanced Encryption Standard) A symmetric 128-bit block data encryption technique developed by Belgian cryptographers Joan Daemen and Vincent Rijmen. AES has been selected by NIST to replace DES and triple DES. It is one of the encryption available in 802.11i.

ARQ See Automatic repeat-request.

Association service An IEEE 802.11 service that enables the mapping of a wireless station to the distribution system via an access point.

Authentication The process a station uses to announce its identify to another station. IEEE 802.11 specifies two forms of authentication: open system and shared key.

Automatic repeat-request (ARQ) A method of error correction where the receiving node detects errors and uses a feedback path to the sender for requesting the retransmission of incorrect frames.

Bandwidth The amount of data you can send through a channel (measured in bits per second).

Base Station Access point.

Basic Service Set (BSS) A set of 802.11-compliant stations that operate as a fully connected wireless network.

BSS see Basic Service Set.

CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) The preferred encryption protocol in the 802.11i standard. It is a mode of AES and is mandatory for RSN.

Cell The geographic region that is serviced by one base station (either analog cellular or digital).

CKIP (Cisco Key Integrity Protocol) Cisco's WEP key permutation technique based on an early algorithm presented in the 802.11i security task group.

Clear channel assessment A function that determines the state of the wireless medium in an IEEE 802.11 network.

CMIC (Cisco Message Integrity Check) Cisco's message integrity check mechanism designed to detect forgeries attacks.

CSMA/CA Carrier Sense Multiple Access with Collision Avoidance.

DHCP See Dynamic Host Configuration Protocol.

Direct sequence spread spectrum (DSSS) Combines a data signal at the sending station with a higher data rate bit sequence, which many refer to as a chip sequence (also known as processing gain). A high processing gain increases the signal's resistance to interference. The minimum processing gain that the FCC allows is 10, and most products operate under 20.

Disassociation service An IEEE 802.11 term that defines the process a station or access point uses to notify that it is terminating an existing association.

Distribution service An IEEE 802.11 station uses the distribution service to send MAC frames across a distribution system.

Distribution system An element of a wireless system that interconnects Basic Service Sets via access points to form an Extended Service Set.

DSSS See direct sequence spread spectrum.

Dynamic Host Configuration Protocol (DHCP) Issues IP addresses automatically within a specified range to devices such as PCs when they are first powered on. The device retains the use of the IP address for a specific lease period that the system administrator can define. DHCP is available as part of many operating systems, including Microsoft Windows NT Server and UNIX. **EAP (Extensible Authentication Protocol)** An extension to PPP. EAP is a general protocol for authentication that also supports multiple authentication methods, such as token cards, Kerberos, one-time passwords, certificates, public key authentication and smart cards. IEEE 802.1x specifies how EAP should be encapsulated in LAN frames.

EAP-TLS (Extensible Authentication Protocol - Transport Layer Security) Created by Microsoft and accepted as RFC 2716: PPP EAP TLS Authentication Protocol. It is the de facto EAP used in 802.11i

EAP-TTLS (EAP-Tunneled TLS) Competing EAP-TLS makes it possible to authenticate wireless LAN clients without requiring them to have certificates, simplifying the architecture of secure wireless LANs.

ESS See Extended Service Set.

Extended Service Set (ESS) A collection of Basic Service Sets connected to each other through a distribution system.

FHSS See frequency hopping spread spectrum.

Frequency hopping spread spectrum (FHSS) Takes the data signal and modulates it with a carrier signal that hops from frequency to frequency as a function of time over a wide band of frequencies.

GHz Gigahertz, which equals 1 billion cycles per second.

Global Positioning System (GPS) A worldwide, satellite-based radio navigation system providing three-dimensional position, velocity and time information to users having GPS receivers anywhere on or near the surface of the Earth.

GSM Global system for mobile communications. A type of digital cellular or PCS network.

Home RF An IEEE 802.11 working group whose goal is to enable the existence of a broad range of interoperable consumer devices by establishing an open industry specification for unlicensed, RF digital communications for PCs and consumer devices in and around the home.

IBSS Network See Independent Basic Service Set Network.

IEEE See Institute of Electrical and Electronic Engineers.

Independent Basic Service Set Network (IBSS Network) An IEEE 802.11-based wireless network that has no backbone infrastructure and consists of at least two wireless stations. This type of network is often referred to as an ad hoc network because it can be constructed quickly without much planning.

Industrial, scientific, and medicine bands (ISM bands) Radio frequency bands that the Federal Communications Commission (FCC) authorized for wireless LANs. The ISM bands are located at 902 MHz, 2.400 GHz, and 5.7 GHz.

Integration service enables the delivery of MAC frames through a portal between an IEEE 802.11 distribution system and a non-802.11 LAN.

Interframe space Defines spacing between different aspects of the IEEE 802.11 MAC access protocol to enable different transmission priorities.

Inward interference Interference coming from other devices, such as microwave ovens and other wireless network devices, that will result in delay to the user by either blocking transmissions from stations on the LAN, or by causing bit errors to occur in data being sent.

ISM Bands See Industrial, scientific, and medicine band.

LEAP (Cisco LEAP-Lightweight Extensible Authentication Protocol) Also known as Cisco-Wireless EAP, provides username/password-based authentication between a wireless client and a RADIUS server like Cisco ACS or Interlink AAA.

MHz Megahertz, which equals 1 million cycles per second.

MIC (Message Integrity Check) An additional 8 byte field which is placed between the data portion of an 802.11 (Wi-Fi) frame and the 4 byte ICV (Integrity Check Value). Where the ICV protected only the packet payload, the MIC protects both the payload and the header. The algorithm which implements the MIC is known as Michael. Michael also implements a frame counter, which discourages replay attacks.

Middleware An intermediate software component located on the wired network between the wireless appliance and the application or data residing on the wired network.

Mobile IP A protocol developed by the Internet Engineering Task Force to enable users to roam to parts of the network associated with a different IP address.

Mobility Ability to continually move from one location to another.

OFDM Orthogonal Frequency Division Multiplexing, an FDM modulation technique for transmitting large amounts of digital data over a radio wave. OFDM works by splitting the radio signal into multiple smaller sub-signals that are then transmitted simultaneously at different frequencies to the receiver. OFDM reduces the amount of crosstalk in signal transmissions. 802.11a WLAN, 802.16 and WiMAX technologies use OFDM.

Open system authentication The IEEE 802.11 default authentication method, a two-step process. First, the station wanting to authenticate with another station sends an authentication management frame containing the sending station's identity. The receiving station then sends back a frame alerting whether it recognizes the identity of the authenticating station.

PCS See Personal Communications Services

PCMCIA See Personal Computer Memory Card International Association

PEAP (Protected Extensible Authentication Protocol) Like the competing standard Tunneled Transport Layer Security (TTLS), PEAP makes it possible to authenticate wireless LAN clients without requiring them to have certificates, simplifying the architecture of secure wireless LANs.

Personal Communications Services (PCS) A spectrum allocation located at 1.9 GHz, a new wireless communications technology offering wireless access to the World Wide Web, wireless e-mail, wireless voice mail, and cellular telephone service.

Personal Computer Memory Card International Association form factor (PCMCIA form factor) A standard set of physical interfaces for portable computers. PCMCIA specifies three interface sizes—Type I (3.3 millimeters), Type II (5.0 millimeters), and Type III (10.5 milli-meters).

Physical layer convergence procedure sublayer (PLCP) Prepares MAC protocol data units (MPDUs) as instructed by the MAC Layer for transmission and delivers incoming frames to the MAC Layer.

PLCP See Physical layer convergence procedure sublayer.

Point coordination function (PCF) An IEEE 802.11 mode that enables contention-free frame transfer based on a priority mechanism. Enables time-bounded services that support the transmission of voice and video.

Portability Defines network connectivity that can be easily established, used, and then dismantled.

Portal A logical point where MSDUs from a non-IEEE 802.11 LAN enter the distribution system of an extended service set wireless network.

Processing gain Equal to the data rate of the spread direct sequence signal divided by the data rate of the actual data.

Pseudo-noise An actual signal having a long pattern that resembles noise pulse code modulation (PCM)- A common method for converting analog voice signals into a digital bit stream.

Reassociation service enables an IEEE 802.11 station to change its association with different access points as it roams from one cell to another.

RF Radio Frequency - any frequency within the electromagnetic spectrum associated with radio wave propagation. When an RF current is supplied to an antenna, an electromagnetic field is created that then is able to propagate through space. Many wireless technologies are based on RF field propagation.

Roaming Traveling from the range of one access point to another.

RSN (Robust Secure Network) A protocol for establishing secure communications over an 802.11 wireless network. RSN is part of the 802.11i standard.

Service Set Identifier (SSID) an identifier attached to packets sent over the wireless LAN that functions as a "password" for joining a particular radio network (BSS). All radios and access points within the same BSS must use the same SSID, or their packets will be ignored.

SFD Start Frame Delimiter.

Shared key authentication A type of authentication that assumes each station has received a secret shared key through a secure channel independent from an 802.11 network. Stations authenticate through shared knowledge of the secret key. Use of Shared Key authentication requires implementation of the 802.11 Wireless Equivalent Privacy algorithm.

Spectrum analyzer An instrument that identifies the amplitude of signals at various frequencies.

Spread spectrum A modulation technique that spreads a signal's power over a wide band of frequencies. The main reasons for this technique is that the signal becomes much less susceptible to electrical noise and interferes less with other radio-based systems.

SSID See Service Set Identifier.

Station In IEEE 802.11 networks, any device that contains an IEEE 802.11-compliant medium access control and physical layers.

Transceiver A device for transmitting and receiving packets between the computer and the medium.

WEP See Wired Equivalent Privacy.

Wired Equivalent Privacy (WEP) An optional IEEE 802.11 function that offers frame transmission privacy similar to a wired network. The Wired Equivalent Privacy generates secret shared encryption keys that both source and destination stations can use to alter frame bits to avoid disclosure to eavesdroppers.

Wi-Fi Wireless Fidelity Wi-Fi is meant to be used generically when referring of any type of 802.11 network, whether 802.11b, 802.11a, dual-band, etc. The term is promulgated by the Wi-Fi Alliance.

Wireless metropolitan area network Provides communications links between buildings, avoiding the costly installation of cabling or leasing fees and the down time associated with system failures.

Wireless network interface Couples the digital signal from the end-user appliance to the wireless medium, which is air.

Wi-Fi Protected Access (WPA) WPA is an industry-supported, pre-standard version of 802.11i utilizing the Temporal Key Integrity Protocol (TKIP), which fixes the problems of WEP, including using dynamic keys.

WME (Wireless Multimedia Enhancement) Provides an interim QoS solution for 802.11 networks until the release of 802.11e. WRAP (Wireless Robust Authenticated Protocol) An encryption protocol in the 802.11i standard. WRAP is based upon the Offset Codebook (OCB) mode of AES. WRAP is being replaced with CCMP.

==

Wireless Solutions from WildPackets

Wireless LANs (WLANs) offer mobility and convenience for end users, but they create significant challenges for IT departments. Networks that were previously secured by physical boundaries and perimeter defenses are now exposed to new security threats and new modes of attack, such as war driving. In place of “standard issue” desktop systems, end user devices become smaller, more various, and often more difficult to configure and secure. Network engineers face the ongoing difficulty of relying on a low-bandwidth radio technology to meet users’ expectations for high performance network services.

To troubleshoot, secure, and monitor WLANs, network engineers need four distinct technical capabilities:

- Expert analytics for Ethernet networking in general
- Expert analytics specifically for 802.11 protocols
- RF monitoring and packet capture for assessing signal strength, detecting rogue APs, etc.
- RF spectrum analysis

WildPackets offers a variety of cost-effective products that work together to address all these needs.

Products

AiroPeek NX

AiroPeek NX, WildPackets’ expert wireless LAN analyzer, provides network engineers with the expert diagnostics they need to deploy, secure, and troubleshoot wireless LANs. AiroPeek NX covers the full spectrum of wireless LAN management requirements, including site surveys, security assessments, client troubleshooting, WLAN monitoring, remote WLAN analysis, and application layer protocol analysis. Designed to accelerate the troubleshooting of WLAN-specific problems, AiroPeek NX features powerful problem detection heuristics and 802.11-specific diagnostic capabilities.

More information at: http://www.wildpackets.com/products/airopeek_nx

AiroPeek Standard Edition (SE)

AiroPeek Standard Edition (SE), a comprehensive packet analyzer for IEEE 802.11 wireless LANs, is designed to identify and solve wireless application anomalies. Used extensively by 802.11 testing facilities and 802.11 equipment manufacturers, AiroPeek SE’s complete 802.11 decodes and powerful user interface, combine to quickly isolate hardware and software application problems. The analyzer is used to measure wireless network performance, monitor signal strength, as well as channel and data rates. AiroPeekSE supports all 802.11 standards and has complete WPA, 802.1X, TKIP, and 802.11 Management, Data, and Control frame decodes. WildPackets offers a version of AiroPeek SE localized for the Japanese market.

More information at: <http://www.wildpackets.com/products/airopeek>

RFGrabber Probe

WildPackets' RFGrabber is a WLAN analysis probe that can be installed in fixed locations to perform remote packet capture for AiroPeek NX. By deploying RFGrabber probes in WLAN coverage zones across the enterprise, network engineers gain access to packet streams in remote locations. This remote access accelerates troubleshooting and enables network engineers to fix problems on remote network segments without traveling. The results: reduced network downtime and reduced IT labor costs.

More information at: <http://www.wildpackets.com/products/rfgrabber>

Peek DNX and the OmniPeek Console

Peek DNX is a packet capture and analysis engine for the Omni³ platform, WildPackets' distributed solution for troubleshooting and optimizing enterprise networks. Running on standard PC or laptop system configured with a supported 802.11 NIC, Peek DNX can capture and locally analyze traffic from 802.11 networks. This wireless configuration of Peek DNX combines the functionality of AiroPeek NX and the RF Grabber probe in a PC solution that has the added benefit of supporting remote analysis through the OmniPeek console. Network engineers can use OmniPeek analyze multiple network segments at once, comparing packets and traffic patterns, without requiring full packet captures to be streamed across the network.

More information at: <http://www.wildpackets.com/products/omni3>

Omni³ Wireless Sensor

The Omni³ Wireless Sensor is a stand-alone device that monitors and analyzes wireless traffic and the RF spectrum in real time. The Omni³ Wireless Sensor captures packet streams, analyzes them, and reports results to the OmniPeek Console. By deploying a Omni³ Wireless Sensor with every WLAN, network engineers gain real-time visibility into WLAN traffic and RF conditions across the enterprise.

For more detailed information on WildPackets' wireless solutions, please visit: <http://www.wildpackets.com/solutions/wireless>