WLAN Quick Guide

by Javvin Technologies, Inc.

Publisher: **Javvin Press**
Pub Date: **January 15, 2008**
ISBN: **978-1-60267-008-2**
Pages: **6**

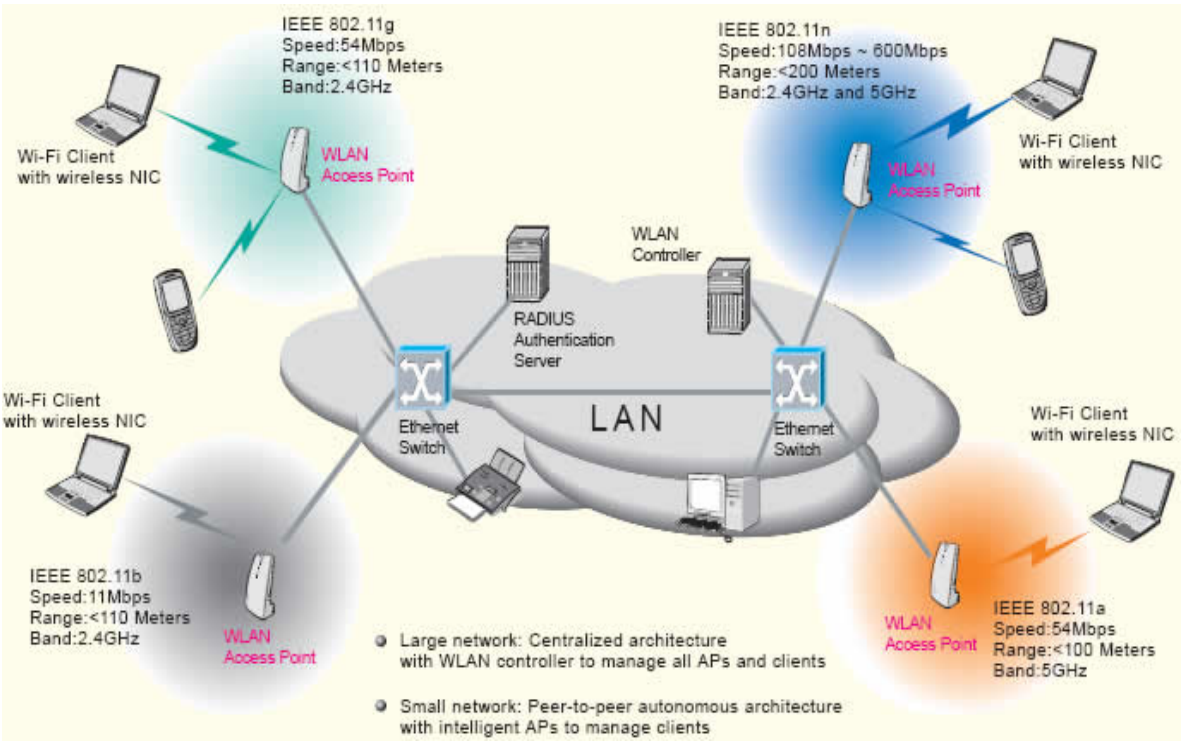
Overview

A comprehensive yet portable Wireless LAN WIFI technology guide for networking and telecom professionals.

Copyright

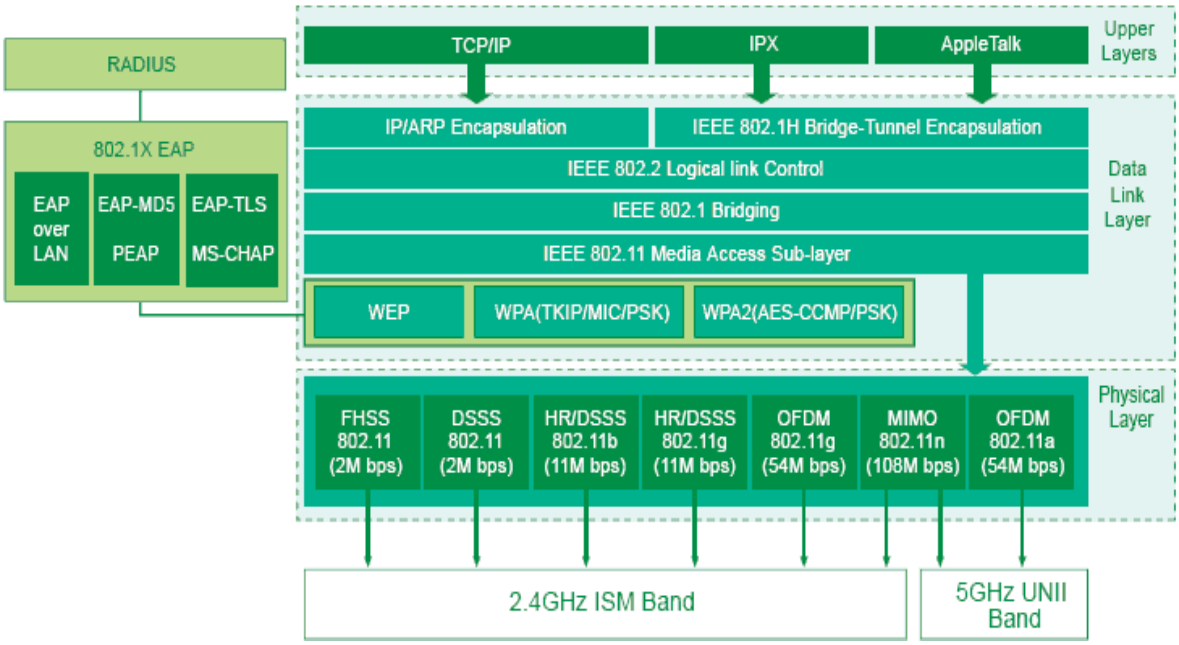
Chapter 01. WLAN Architecture

Figure 01.



Chapter 02. IEEE 802.11 WLAN Protocols

Figure 02.

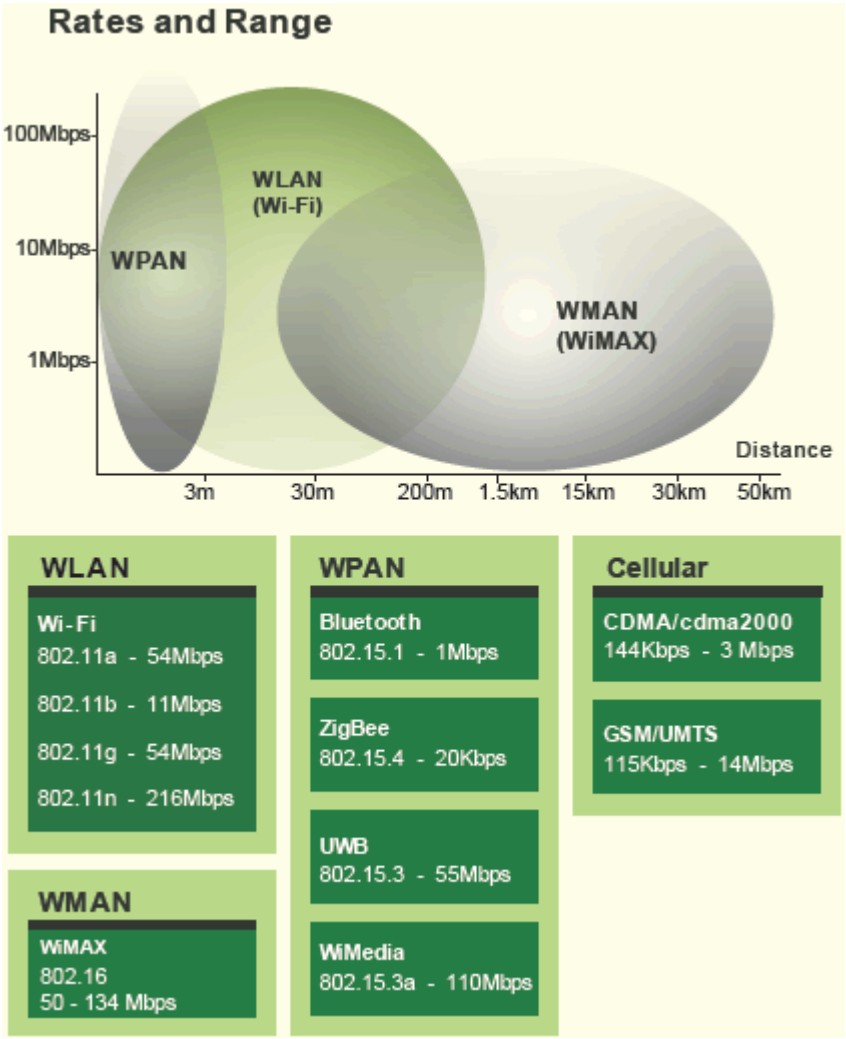


Chapter 03. Key Parameters of WLAN and Other Wireless Technologies

Technology	WLAN (IEEE)					WPAN (IEEE)			
Standard	802.11 Legacy	802.11a	802.11b	802.11g	802.11n	802.15.1 (Bluetooth)	802.15.3 (UWB)	802.15.3a (WiMedia)	ZigBee 802.15.4 2003 802.15.4 2006
Release year	1997	1999	1999	2003	2008	2002	2003	*	2003 and 2006
Frequency Band	2.4GHz	5.8GHz	2.4GHz	2.4GHz	2.4GHz-5.8GHz	2.4GHz	3.1 to 10.6Ghz	2.4GHz	868 MHz MHz, 2.4
Maximum Range	~70 meters	~100 meters	~100 meters	~110 meters	~200 meters	~10meters	~10meters	~10meters	~100 me
Maximum data rate	2Mbps	54Mbps	11Mbps	54Mbps	248Mbps	3Mbps	55Mbps-1Gbps	110Mbps-1Gbps	250 Kbp
Number of users	Dozens	Dozens	Dozens	Dozens	Dozens	Dozens	Dozens	Dozens	Dozens
Access Method	DSSS, FHSS	OFDM	DSSS, CCK	OFDM	MIMO	FHSS	DS-UWB,OFDM	MB-OFDM	DSSS
Modulation Method	GFSK, BPSK, DBPSK, DQPSK	BPSK, QPSK, 16-QAM, 64-QAM	DPSK, DBPSK, DQPSK	BPSK, QPSK, 16-QAM, 64-QAM and DBPSK, DQPSK	BPSK, QPSK, 16-QAM, 64-QAM	GFSK, 2PSK, DQSP, 8PSK	OPSK, BPSK, OOK, PAM, PPM, Bi-Phase	QPSK, DCM	BPSK (868/928 OPSK (2.4GHz)

Chapter 04. Wireless Landscape

Figure 03.

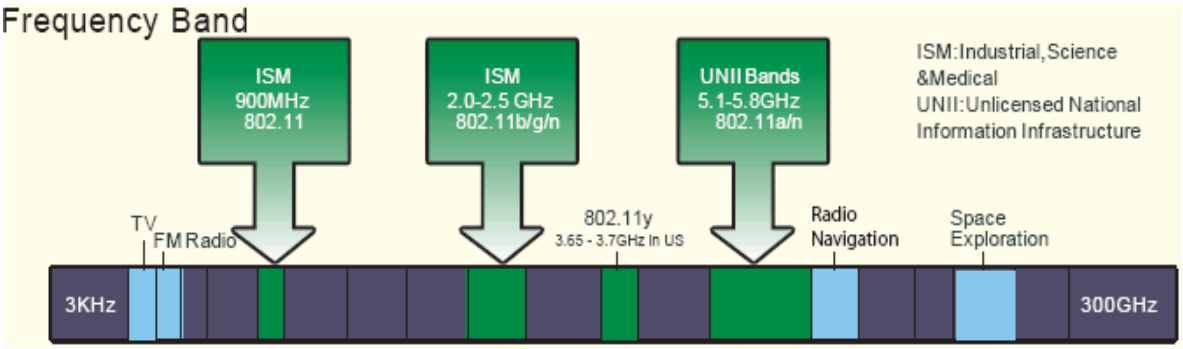


Chapter 05. Wi-Fi Standards

IEEE 802.11 - The original WLAN standard (1997)
IEEE 802.11a - Enhancement to 802.11 with 54 Mbit/s at 5 GHz (1999)
IEEE 802.11b - Enhancements to 802.11 to support 5.5 and 11 Mbit/s (1999)
IEEE 802.11c - Bridge operation procedures; included in the IEEE 802.1D standard (2001)
IEEE 802.11d - International (country-to-country) roaming extensions (2001)
IEEE 802.11e - Enhancements: QOS, including packet bursting (2005)
IEEE 802.11f - Inter-Access Point Protocol (2003) Withdrawn February 2006
IEEE 802.11g - Enhancement to 802.11b and 802.11a (backwards compatible with b) (2003)
IEEE 802.11h - Spectrum Managed 802.11a (5 GHz) for European compatibility (2004)
IEEE 802.11i - Enhanced security (2004)
IEEE 802.11j - Extensions for Japan (2004)
IEEE 802.11-2007 - A release of the standard that includes 802.11 amendments a, b, d, e, g, h, i & j. (2007)
IEEE 802.11k - Radio resource measurement enhancements
IEEE 802.11m - Maintenance of the standard; odds and ends.
IEEE 802.11n - Enhancement to 802.11a,b,g with Higher throughput improvements using MIMO
IEEE 802.11p - WAVE - Wireless Access for the Vehicular Environment (such as ambulances and passenger cars)
IEEE 802.11r - Fast roaming
IEEE 802.11s - ESS Extended Service Set Mesh Networking
IEEE 802.11t - Wireless Performance Prediction (WPP) - test methods and metrics recommendation
IEEE 802.11u - Interworking with non-802 networks (for example, cellular)
IEEE 802.11v - Wireless network management
IEEE 802.11w - Protected Management Frames
IEEE 802.11y - 3650-3700 Operation in the U.S.
IEEE 802.11z - Extensions to Direct Link Setup (DLS)

Chapter 06. Wi-Fi Frequency Bands and Channels

Figure 04.



Chapter 07. Channels for IEEE

802.11a

Channel Identifier	Frequency (in MHz)	Regulatory Domains			
		Americas	EMEA	Japan	Rest of World
34	5170	-	-	x	-
36	5180	x	x	-	x
38	5190	-	-	x	-
40	5200	x	x	-	x
42	5210	-	-	x	-
44	5220	x	x	-	x
46	5230	-	-	x	-
48	5240	x	x	-	x
52	5260	x	x	-	x
56	5280	x	x	-	x
60	5300	x	x	-	x
64	5320	x	x	-	x
100	5500	-	x	-	x
104	5520	-	x	-	x
108	5540	-	x	-	x
112	5560	-	x	-	x
116	5580	-	x	-	x
120	5600	-	x	-	x
124	5620	-	x	-	x
128	5640	-	x	-	x
132	5660	-	x	-	x
136	5680	-	x	-	x

140	5700	-	x	-	x
149	5745	x	-	-	x
153	5765	x	-	-	x
157	5785	x	-	-	x
161	5805	x	-	-	x

Chapter 08. Channels for IEEE 802.11b/g

Channel Identifier	Frequency (in MHz)	Regulatory Domains			
		Americas	EMEA	Japan	Rest of World
1	2412	x	x	x	x
2	2417	x	x	x	x
3	2422	x	x	x	x
4	2427	x	x	x	x
5	2432	x	x	x	x
6	2437	x	x	x	x
7	2442	x	x	x	x
8	2447	x	x	x	x
9	2452	x	x	x	x
10	2457	x	x	x	x
11	2462	x	x	x	x
12	2467	-	x	x	x
13	2472	-	x	x	x
14	2484	-	-	x	-

Chapter 09. Channels for 802.11n

802.11n operates at both the 2.4G and 5G spectrums. Some example channels for 802.11n at the 5G spectrum with channel bonding (each channel with 40 MHz) are shown below:

Channel Identifier	Frequency (in MHz)	Regulatory Domains			
		Americas	EMEA	Japan	Rest of World
(36, 1) (40,-1)	5190	x	-	x	-
(44, 1) (48,-1)	5230	x	-	x	-
(52, 1) (56,-1)	5270	x	-	x	-
(60, 1) (64, -1)	5310	x	-	-	x
(100, 1) (104, -1)	5510	-	x	-	x
(108, 1) (112, -1)	5550	-	x	-	x
(116, 1) (120, -1)	5590	-	x	-	x
(124, 1) (128,-1)	5630	-	x	-	x
(132, 1) (136,-1)	5670	-	x	-	x
(149, 1) (153,-1)	5755	x	-	-	x
(157, 1) (161,-1)	5795	x	-	-	x

Chapter 10. WiFi Data Rates

802.11a/b/g Data Rates

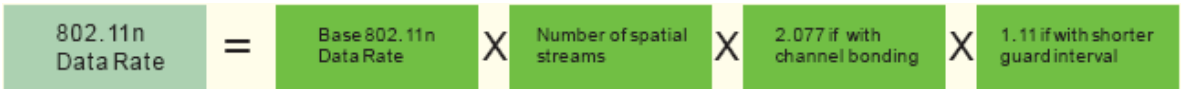
Access/Modulation Method	802.11b	802.11a	802.11g
DSSS/DBPSK	1 Mbps		1 Mbps
DSSS/DQPSK	2 Mbps		2 Mbps
CCK/DQPSK	5.5 Mbps-11 Mbps		5.5 Mbps-11 Mbps
OFDM/BPSK		6-9 Mbps	6-9 Mbps
OFDM/QPSK		12-18 Mbps	12-18 Mbps
OFDM/16-QAM		24-36 Mbps	24-36 Mbps
OFDM/64-QAM		48-54 Mbps	48-54 Mbps

802.11n Data Rates (One Spatial Stream)

Access/Modulation Method	Base Data Rate	With Channel Bonding	With Short Guard Interval
MIMO/BPSK	6.5-13.5 Mbps	13.5-27 Mbps	15-30 Mbps
MIMO /QPSK	19.5-26 Mbps	40.5-54 Mbps	45-60 Mbps
MIMO /16-QAM	39-52 Mbps	81-108 Mbps	90-120 Mbps
MIMO /64-QAM	58.5-65 Mbps	121.5-135 Mbps	135-150 Mbps

Formula to calculate 802.11n data rates:

Figure 05.


802.11n Data Rate
=
Base 802.11n Data Rate
X
Number of spatial streams
X
2.077 if with channel bonding
X
1.11 if with shorter guard interval

Chapter 11. WLAN Security

Security problems

- The spread spectrum modulation technique used in 802.11 and 802.11b is not secure because the code is open to the public.
- Service Set Identifier (SSID) is very easy to break because anyone with a sniffing tool can detect it.
- DHCP hurts security in a WLAN because it allows anyone to get a legitimate IP address in the network and access to the shared resources.
- Wired Equivalent Privacy (WEP) is a very weak encryption to break.
- Man-in-the-middle attacks by using a wireless analyzer.
- Denial of Service (DoS) attacks: using a wireless client to insert bogus packets into the wireless LAN to cause access point malfunction, or using a high power signal generator to produce RF interference to block other radio NICs from accessing the medium.

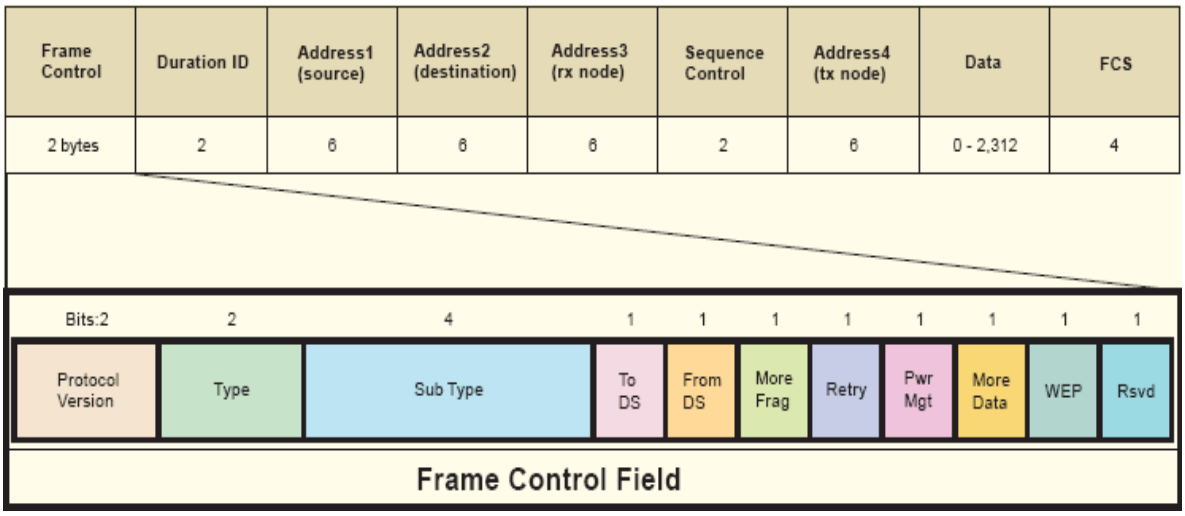
Security solutions

- Use the latest Wi-Fi technologies such as 802.11g and 802.11n that have more advanced modulation methods.
- Use encryption technologies such as 802.1x, EAP, TLS, RADIUS, to protect SSID and other user identities.
- Use 802.11i (WPA 2) with AES technologies for strong encryption.

- Encrypt wireless traffic using a VPN (Virtual Private Network), such as IPSEC or other VPN solutions.
- Use encryption for all applications over the wireless network, e.g., use SSH and TLS/HTTPS.
- Use a proxy with access control for outgoing requests (web proxy, and others).
- Regularly test the security of wireless network.
- Enable strict logging on all devices, and check wireless log files regularly to see if security policy is still adequate.

Chapter 12. 802.11 Frame Format

Figure 06.



Field	Bits	Notes/Description
Frame Control	15 - 14	Protocol version.
	13 - 12	Type
	11 - 8	Subtype
	7	To DS.1 = to the distribution system.
	6	From DS.1= exit from the Distribution System.
	5	More Frag.1 = more fragment frames to follow(last or unfragmented frame = 0)
	4	Retry.1 = this is a re-transmission.
	3	Power Mgt.1 = station in power save mode,1 = active mode.
	2	More Data.1 = additional frames buffered for the destination address(address x).

	1	WEP.1 = data processed with WEP algorithm.0 = no WEP.
	0	Order.1 = frames must be strictly ordered.
Duration ID	15 - 0	For data frames = duration of frame.For Control Frames the associated identity of the transmitting station.
Address 1	47 - 0	Source address(6 bytes).
Address 2	47 - 0	Destination address(6 bytes).
Address 3	47 - 0	Receiving station address(destination wireless station)
Sequence Control	15 - 0	
Address 4	47 - 0	Transmitting wireless station.
Frame Body		0 - 2312 octets(bytes).
FCS	31 - 0	Frame Check Sequence (32 bit CRC).defined in P802.11.

Chapter 13. WLAN Glossary

16-QAM

Quadtrative Amplitude Modulation (QAW) with 16 different symbols.

64-QAM

Quadtrative Amplitude Modulation (QAW) with 64 different symbols.

800.11

IEEE original Wi-Fi standard.(1997)

800.11a

IEEE Wi-Fi standard.(1999)

800.11b

IEEE Wi-Fi standard.(1999)

800.11g

IEEE Wi-Fi standard.(2003)

800.11i

IEEE standard for Wi-Fi security.

800.11n

IEEE Wi-Fi standard.(2008)

Access Point(AP)

Base starions for the WLAN to transmit and receive radio frequencies.

Ad-Hoc Mode--

Peer-to-peer connectivity in a wireless LAN.

AES

Advanced Encryption Standard.

Analog modulation

The modulation is applied continuously in response to the analog information signal.

Antenna gain

The relative increase in radiation at the maximum point expressed as a value in dB above a standard.

ASK

Amplitude shift keying:carrier on = 1,carrier off = 0

Attenuation

The decrease in intensity of electromagnetic radiation due to absorption or scattering of phptons.

Authentication server

Provide authentication services to users or other systems.

Band

RF spectrum range available for certain communication.

Bi-Phase Modulation

Amodulation method using two opposite signal phases(0 and 180 degrees).

Bluetooth

A short range wireless communication technology as defined in IEEE 802.15.1.

BPSK

Binary Phase-Shift Keying.

BSS

Basic Service Set.

CAPWAP

Control And Provisioning of Wireless Access Polnts.

CCK

Complementary Code Keying.

CCMP

Counter mode with Cipher-block chaining Message authentication code Protocol.

Cell

An Access Point RF coverage area.

Channel

A RF spectrum with certain bandwidth in a RF band to transmit information.

Channel bonding

Using two adjacent channels together as one to increase data rates.

CHAP

Challenge Handshake Authentication Protocol.

Client adaptor

See [**Wireless Network Card**]

Clients

Any mobile or fixed devices such as laptops,personal digital assistants.and desktops that are equipped with a wireless network interface.

CSMA/CA

Carrier Sense multiple Access/Collision Avoidance. CSMA/CA is the medium access method used by IEEE 802.11 WLANs.

DBPSK

Differential Binary Phase Shift Keying.

DCF

Distributed Coordination Function.

Dependent(thin)Access Point

A simple AP that relies on WLAN controller for RF management and configuration.

DES

Data Encryption Standard.

Digital modulation

An analog carrier signal is modulated by a digital bit stream of either equal length signals or varying length signals.

Diversity antenna system

Incorporates multiple antenna elements at the base station to improve reception.

DQPSK

Differential Quadrature Phase-Shift Keying.

EAP

Extensible Authentication Protocol.

EBSS

Extended basic service set.

ECP

Encryption Control Protocol.

EHSS

Frequency-Hopping Spread-Spectrum.

FSK

Frequency Shift Keying.

GFSK

Gaussian Frequency Shift Keying.

Hidden node Problem

A node is visible from a wireless hub,but not from other nodes communicating with said hub.

HiperMAN

The ETSI defined broadband wireless standard that is compatible with WiMAX(IEEE 802.16).

Hotspot

The venues that offer Wi-Fi access.

IAS

Internet Authentication Service server,a RADIUS Server which performs connection authentication and accounting for remote access.

IBSS

Independent Basic Service Set.

IDEA

International Data Encryption Algorithm.

IEEE

Institute of Electrical and Electronics Engineers.

Independent(fat)Access Point

A standalone AP that provides configuration and management for clients.

Infrastructure Mode

A client setting providing connectivity to a central Access Point(AP).

Interference

Distortion of the wireless signal be other RF waves.

ISM

The industrial,scientific and medical (ISM) radio bands.

LCP

Link Control Protocol.

LWAPP

Light Weight Access Point Protocol.

MAC

Medium Access Control.In a WLAN network card,the MAC is radio controller protocol.

MD5

Message-Digest Algorithm 5.

MIMO

Multiple-Input Multiple-Output.

Modulation

The process of varying a periodic waveform.

Multipath

Multiple copies of the original transmitted signal due to reflections,scattering,etc.

Multipath distortion

When parts of the same radio wave arrive at a receiver at different times.

NDIS

Network Driver Interface Specification.

OFDM

Orthogonal Frequency-Division Multiplexing.

OOK

On Off Keying.

PAM

Pulse Amplitude Modulation.

Path Loss

The reduction in signal strength as it travels through the air or other media.

PCF

Point Coordination Function.

PEAP

Protected Extensible Authentication Protocol.

PHY

Physical Layer in the OSI Network Model.

PLCP

Physical Layer Convergence Procedure.

PMD

Physical Medium Dependent.

Polling

A technique for enabling multiple transmitters to share a medium when transmitters take turns in a defined sequence.

PPM

Pulse Position Modulation.

PSK

Phase shift keying.

QAM

Quadrature Amplitude Modulation.

QPSK

Quadrature Phase Shift Keying.

RADIUS

Remote Authentication Dial In User Service.

RADIUS server

A server using RADIUS technology to provide authentication and accounting services.

Receive Sensitivity

The minimum signal strength required to pick up a signal.

RFID

Radio Frequency Identification.

Roaming

The movement of a mobile device from one wireless network location to another without interruption in service or loss in connectivity.

RSA Algorithm

Rivest-Shamir-Aldeman algorithm.

RSSI

Received Signal Strength Indicator.

RTS/CTS

Request-to-send/clear-to-send,or request-to-send(RTS) protocol.

Single Channel Access Point

A type of dependent thin Access Point.

SNR

Signal to Noise Ratio.The number of decibels difference between the signal strength and background noise.

Spatial Multiplexing

Transmit two or more separate data streams on different antennas at the same time in the same.

Spread Spectrum Transmission

A RF transmission technique that takes a narrow band signal and spreads it over a broader portion of the RF band.

SSID

Service Set Identifier - wireless network name.

SWAP

Shared Wireless Access Protocol.

TKIP

Temporal Key Integrity Protocol.

TLS

Transport Level Security,a protocol for mutual authentication, integrity-protected negotiation and key exchange between.

Transmit Power

The power usually expressed in mW or db that the wireless device transmits at.

UNII(U-NII)

Unlicensed National Information Infrastructure.

UWB

Ultra-Wide-Band.

War Chalking

To marking buildings or sidewalks with chalk to show others where it's possible to access an exposed wireless network.

War Driving

The process of traveling around looking for wireless access point signals that can be used to get network access.

WECA

The Wireless Ethernet Compatibility Alliance.

WEP

Wired Equivalent Privacy.Encryption-based security using a preshared key.

WiFi(Wi-Fi)

Wireless Fidelity refers to WLAN standard based on IEEE 802.11 and its amendments.

Wi-Fi Alliance

Organization that certifies 802.11 products.

WiMAX

A wireless MAN technology defined in IEEE 802.16-2004 and 802.16-2005

WiMedia

A not-for-profit association to promote UWB.

Wireless Network Card

A card that has drivers and utilities to set specific parameters and sends and receives information over the air.They are installed or imbedded into client devices such as laptops.

WLAN(W-LAN)

Wireless Local Area Network (LAN).

WLAN Array

A device that connects wireless devices/users to another network,It usually contains a switch or a router,and a WLAN AP controller.

WLAN Controller

A device that manages thin AP, provides channel selection,roaming and other services.

WMAN

Wireless Metropolitan Area Network.

WML

Wireless Markup Language

WPA

Wireless Markup Language

WPA2

Wi-Fi Protected Access 2 as defined in IEEE 802.11i.

WPAN

Wireless Personal Area Network.

ZigBee

The technology used in the low data rate Wireless Personal Area Network (WPAN) as defined in IEEE 802.15.4.