Wi-Fi Scanner

Glossary

Table of Contents

802

802.11

IEEE 802.11 is a set of medium access control (MAC layer) and physical layer (PHY layer) specifications for implementing wireless local area network (WLAN) computer communication in the 2.4, 3.6, 5 and 60 GHz frequency bands (See Wi-Fi Generations).

802.11a

An IEEE standard for a wireless network that operates at 5 GHz with rates up to 54Mbps.

802.11b

An IEEE standard for a wireless network that operates at 2.4 GHz with rates up to 11Mbps.

802.11d

An IEEE specification that allows for configuration changes at the Media Access Control layer (MAC layer) level to comply with the rules of the country in which the network is to be used. (See MAC address).

802.11e

An IEEE standard that adds Quality of Service (QoS) features and multimedia support to the existing 802.11b, 802.11g, and 802.11a wireless networks. (See QoS, WMM).

802.11g

An IEEE standard for a wireless network that operates at 2.4 GHz Wi-Fi with rates up to 54Mbps.

802.11h

802.11h supports Dynamic Frequency Selection(DFS) and Transmit Power Control(TPC) requirements to ensure coexistence between Wi-Fi and other types of radio frequency devices in the 5 GHz band.

802.11i

An IEEE standard specifying security mechanisms for 802.11 networks. 802.11i makes use of the Advanced Encryption Standard (AES) block cipher. The standard also includes improvements in key management, user authentication through 802.1X and data integrity of headers. (See 802.1X, AES, WPA2).

802.11j

An IEEE specification for wireless networks that incorporates Japanese regulatory requirements concerning wireless transmitter output power, operational modes, channel arrangements and spurious emission levels.

802.11n

A taskgroup of the IEEE 802.11 committee whose goal is to define a standard for high throughput speeds of at least 100Mbps on wireless networks. The standard is expected to be ratified by 2007. Some proposals being fielded by the taskgroup include designs for up to 540 Mbps. Multiple-Input-Multiple-Output (MIMO) technology, using multiple receivers and multiple transmitters in both the client and access point to achieve improved performance is expected to form the basis of the final specification. (See Mbps, MIMO).

802.1X

A standard for port-based authentication, first used in wired networks, that was adapted for use in enterprise WLANs to address security flaws in WEP, the original security specification for 802.11 networks. 802.1X provides a framework for authenticating users and controlling their access to a protected network and dynamic encryption keys to protect data privacy. (See EAP, WEP, WPA, WPA2).

802.3

The standard defining wired Ethernet networks. (See Ethernet).

A

Ad-Hoc mode

An old term used to describe a device-to-device network. (See Device-to-device network, Peer-to-peer network).

AES

Advanced Encryption Standard. The preferred standard for the encryption of commercial and government data using a symmetric block data encryption technique. It is used in the implementation of WPA2. (See 802.11i, WPA2).

AP

Access point. Often a wireless router, a device that connects wireless devices to another network.

Access Point

Access Point. often a wireless router, a device that connects wireless devices to another network. (See AP.)

B

Bandwidth

The maximum transmission capacity of a communications channel at any point in time. Bandwidth, usually measured in bits per second (bps), determines the speed at which information can be sent across a network. If you compare the communications channel to a pipe, bandwidth represents the pipe width and determines how much data can flow through the pipe at any one time. The greater the bandwidth, the faster data can flow. (See bps).

bps

Bits per second. Network performance has traditionally been measured in units of bits per second (bps).

BSSID

Basic Service Set Identifier. A unique address that identifies the access point/router that creates the wireless network. LizardSystems Wi-Fi Scanner obtains BSSID and other information.

C

Channel

One portion of the available radio spectrum that all devices on a wireless network use to communicate. Changing the channel on the access point/router can help reduce interference. **Wi-Fi Scanner make graphical visualization of channel allocation**.

D

Data rate

Also known as the “PHY” rate, this number captures the speed at which all data bits pass over the Wi-Fi network. Many Wi-Fi devices will report this number as the “speed” at which your network is performing. Actual throughout rates will always be lower than the data rate, due to available network capacity and overhead in real-world environments. The data rate communicates the maximum possible rate at which a device can transmit data. See also Throughput, which is a real-world measure of performance and is always lower than data rate.

Device-to-device network

Two or more devices that connect using wireless network devices without the use of a centralized wireless access point. Also known as a peer-to-peer network. (See Ad-Hoc mode, Peer-to-peer network).

DHCP

Dynamic Host Configuration Protocol. A protocol for dynamically assigning IP addresses from a pre-defined list to nodes on a network. When they log on, network nodes automatically receive an IP address from a pool of addresses served by a DHCP. The DHCP server provides (or leases) an IP address (to a client for a specific period of time. The client will automatically request a renewal of the lease when the lease is about to run out. If a lease renewal is not requested and it expires, the address is returned to the pool of available IP addresses. Using DHCP to manage IP addresses simplifies client configuration and efficiently utilizes IP addresses. (See IP address).

Dual-band

A device that is capable of operating in two frequencies. On a wireless network, dual-band devices are capable of operating in both the 2.4 GHz (802.11b/g) and 5 GHz (802.11a) bands. In cellular phone technology, dual-band devices typically operate in both the GSM900 and GSM1800 frequencies, allowing a greater number of roaming options. (See Tri-mode).

E

EAP

Extensible Authentication Protocol. A protocol that provides an authentication framework for both wireless and wired Ethernet enterprise networks. It is typically used with a RADIUS server to authenticate users on large networks. EAP protocol types are used in the 802.1X-based authentication in WPA-Enterprise and WPA2-Enterprise. (See 802.1X, EAP, TLS, WPA - Enterprise, WPA2 - Enterprise).

Encryption

A mechanism for providing data confidentiality. (See 802.11i, RC4, TKIP, WEP, WPA, WPA2).

Ethernet

The most popular international standard technology for wired Local Area Networks (LANs). It provides from 10 Mbps transmission speeds on basic 10BastT Ethernet networks to 100 Mbps transmission speeds on Fast Ethernet networks, 1000 Mbps on Gigabit Ethernet, and 10,000 Mbps on 10 Gigabit Ethernet. (See 802.3)

G

Gateway

In the wireless world, a gateway is an access point with additional software capabilities such as providing NAT and DHCP. Gateways may also provide VPN support, roaming, firewalls, various levels of security, etc.

H

Hz

Hertz, not the car rental company. The international unit for measuring frequency equivalent to the older unit of cycles per second. One megahertz (MHz) is one million hertz. One gigahertz (GHz) is one billion hertz. The standard US electrical power frequency is 60 Hz

I

IP address

Internet Protocol address. IP Version 4, the most widely used Internet protocol, provides 32-bit number that identifies the sender or receiver of information sent across the Internet. An IP address has two parts: The identifier of the particular network on the Internet and the identifier of the particular device (which can be a server or a workstation) within that network. The newer IP, Version 6, provides a 128-bit addressing scheme to support a much greater number of IP addresses. (See DHCP, IP).

M

MAC address

Media Access Control address. A unique hardware number that identifies each device on a network. A device can be a computer, printer, etc. (See IP address).

MAC layer

In the seven-layer OSI model of computer networking, media access control (MAC) data communication protocol is a sublayer of the data link layer, which itself is layer 2. The MAC sublayer provides addressing and channel access control mechanisms that make it possible for several terminals or network nodes to communicate within a multiple access network that incorporates a shared medium, e.g. Ethernet. The hardware that implements the MAC is referred to as a medium access controller.

The MAC sublayer acts as an interface between the logical link control (LLC) sublayer and the network's physical layer. The MAC layer emulates a full-duplex logical communication channel in a multi-point network. This channel may provide unicast, multicast or broadcast communication service.

Mbps

Megabits per second. A measurement of data speed that is roughly equivalent to a million bits per second. (See bps).

MIC

Message Integrity Check. A technology that is employed to prevent an attacker from capturing data packets, altering them and resending them. The MIC provides a strong mathematical function in which the receiver and the transmitter each compute and then compare the MIC. If it does not match, the data is assumed to have been tampered with and the packet is dropped. (See Packet, TKIP, WPA, WPA2).

MIMO

Multiple-Input-Multiple-Output. An advanced signal processing technology that uses multiple receivers and multiple transmitters in both the client and access point to achieve data throughput speeds of 100Mbps. (See 802.11n).

Modulation and Coding Index 802.11n

		Data Rate			
HT MCS Index	**Spatial Streams**	**20MHz**		**40MHz**	
		(GI = 800ns)	**(GI = 400ns)**	**(GI = 800ns)**	**(GI = 400ns)**
0	1	6,5	7,2	13,5	15
1	1	13	14,4	27	30
2	1	19,5	21,7	40,5	45
3	1	26	28,9	54	60
4	1	39	43,3	81	90
5	1	52	57,8	108	120
6	1	58,5	65	121,5	135
7	1	65	72,2	135	150
		Data Rate			
HT MCS Index	**Spatial Streams**	**20MHz**		**40MHz**	
		(GI = 800ns)	**(GI = 400ns)**	**(GI = 800ns)**	**(GI = 400ns)**
8	2	13	14,4	27	30
9	2	26	28,9	54	60
10	2	39	43,3	81	90
11	2	52	57,8	108	120
12	2	78	86,7	162	180
13	2	104	115,6	216	240
14	2	117	130,3	243	270
15	2	130	144,4	270	300
		Data Rate			
HT MCS Index	**Spatial Streams**	**20MHz**		**40MHz**	
		(GI = 800ns)	**(GI = 400ns)**	**(GI = 800ns)**	**(GI = 400ns)**
16	3	19,5	21,7	40,5	45
17	3	39	43,3	81	90
18	3	58,5	65	121,5	135
19	3	78	86,7	162	180
20	3	117	130	243	270
21	3	156	173,3	324	360
22	3	175,5	195	364,5	405
23	3	195	216,7	405	450
		Data Rate			
HT MCS Index	**Spatial Streams**	**20MHz**		**40MHz**	
		(GI = 800ns)	**(GI = 400ns)**	**(GI = 800ns)**	**(GI = 400ns)**
24	4	26	28,9	54	60
25	4	52	57,8	108	120
26	4	78	86,7	162	180
27	4	104	115,6	216	240
28	4	156	173,3	324	360
29	4	208	231,1	432	480
30	4	234	260	486	540
31	4	260	288,9	540	600

		Data Rate			
HT MCS Index	**Spatial Streams**	**20MHz**		**40MHz**	
		(GI = 800ns)	**(GI = 400ns)**	**(GI = 800ns)**	**(GI = 400ns)**
32	1	6	6,7	-1	-1

		Data Rate			
HT MCS Index	**Spatial Streams**	**20MHz**		**40MHz**	
		(GI = 800ns)	**(GI = 400ns)**	**(GI = 800ns)**	**(GI = 400ns)**
33	2	39	43,3	81	90
34	2	52	57,8	108	120
35	2	65	72,2	135	150
36	2	58,5	65	121,5	135
37	2	78	86,7	162	180
38	2	97,5	108,3	202,5	225

		Data Rate			
HT MCS Index	**Spatial Streams**	**20MHz**		**40MHz**	
		(GI = 800ns)	**(GI = 400ns)**	**(GI = 800ns)**	**(GI = 400ns)**
39	3	52	57,8	108	120
40	3	65	72,2	135	150
41	3	65	72,2	135	150
42	3	78	86,7	162	180
43	3	91	101,1	189	210
44	3	91	101,1	189	210
45	3	104	115,6	216	240
46	3	78	86,7	162	180
47	3	97,5	108,3	202,5	225
48	3	97,5	108,3	202,5	225
49	3	117	130	243	270
50	3	136,5	151,7	283,5	315
51	3	136,5	151,7	283,5	315
52	3	156	173,3	324	360

		Data Rate			
HT MCS Index	**Spatial Streams**	**20MHz**		**40MHz**	
		(GI = 800ns)	**(GI = 400ns)**	**(GI = 800ns)**	**(GI = 400ns)**
53	4	65	72,2	135	150
54	4	78	86,7	162	180
55	4	91	101,1	189	210
56	4	78	86,7	162	180
57	4	91	101,1	189	210
58	4	104	115,6	216	240
59	4	117	130	243	270
60	4	104	115,6	216	240
61	4	117	130	243	270
62	4	130	144,4	270	300
63	4	130	144,4	270	300
64	4	143	158,9	297	330
65	4	97,5	108,3	202,5	225
66	4	117	130	243	270

67	4	136,5	151,7	283,5	315
68	4	117	130	243	270
69	4	136,5	151,7	283,5	315
70	4	156	173,3	324	360
71	4	175,5	195	364,5	405
72	4	156	173,3	324	360
73	4	175,5	195	364,5	405
74	4	195	216,7	405	450
75	4	195	216,7	405	450
76	4	214,5	238,3	445,5	495

N

Network name

A name used to identify a wireless network. (See SSID)

NIC

Network Interface Card. A wireless or wired PC adapter card that allows the client computer to utilize network resources. Most office wired NICs operate at 100 Mbps. Wireless NICs operate at data rates defined by 802.11 standards.

P

Packet

A unit of information transmitted from one device to another on a network. A packet typically contains a header with addressing information, data, and a checksum to insure data integrity. (See MIC).

Pass phrase

A series of characters used to create a key which is used by Wi-Fi Protected Access (WPA). (See PSK, WPA).

PC Card

A removable, credit-card-sized memory or I/O device that fits into an expansion slot on a notebook computer or a personal digital assistant (PDA). PC Cards are used primarily in notebook computers and PDAs. PC Card peripherals include Wi-Fi network cards, memory cards, modems, wired NICs, and hard drives. (See NIC, PCI).

PCI

Peripheral Component Interconnect. A high-performance I/O (input/output) computer bus that allows expansion slots to be spaced closely for high-speed operation. (See NIC, PC Card).

Peer-to-peer network

A wireless or wired computer network that has no server or central hub or router. All the networked PCs are equally able to act as a network server or client, and each client computer can talk to all the other wireless computers without having to go through an access point or hub. However, since there is no central base station to monitor traffic or provide Internet access, the various signals can collide with each other, reducing overall performance. (See Ad-Hoc mode, Device-to-device network).

PHY

he physical, or lowest, layer of the OSI Network Model. In a wireless network, the PHY defines parameters such as data rates, modulation method, signaling parameters, transmitter/receiver synchronization, etc. Within an actual radio implementation, the PHY corresponds to the radio front end and baseband signal processing sections. Wi-Fi Scanner make graphical visualization PHY layer statistics.

PHY layer

In the seven-layer OSI model of computer networking, the physical layer or layer 1 is the first (lowest) layer. The implementation of this layer is often termed PHY.

The physical layer consists of the basic networking hardware transmission technologies of a network. It is a fundamental layer underlying the logical data structures of the higher level functions in a network. Due to the plethora of available hardware technologies with widely varying characteristics, this is perhaps the most complex layer in the OSI architecture.

The physical layer defines the means of transmitting raw bits rather than logical data packets over a physical link connecting network nodes. The bit stream may be grouped into code words or symbols and converted to a physical signal that is transmitted over a hardware transmission medium. The physical layer provides an electrical, mechanical, and procedural interface to the transmission medium. The shapes and properties of the electrical connectors, the frequencies to broadcast on, the modulation scheme to use and similar low-level parameters, are specified here.

Within the semantics of the OSI network architecture, the physical layer translates logical communications requests from the data link layer into hardware-specific operations to affect transmission or reception of electronic signals.

PSK

A mechanism in Wi-Fi Protected Access (WPA)-Personal that allows the use of manually entered keys or passwords to initiate WPA security. The PSK is entered on the access point or home wireless gateway and each PC that is on the Wi-Fi network. After entering the password, Wi-Fi Protected Access automatically takes over. It keeps out eavesdroppers and other unauthorized users by requiring all devices to have the matching password. The password also initiates the encryption process which, in WPA is Temporal Key Integrity Protocol (TKIP) and in WPA2 is Advanced Encryption Standard (WPA2). (See TKIP, WPA - Personal, WPA2 - Personal).

Q

QoS

Quality of Service. Required to support wireless multimedia applications and advanced traffic management. QoS enables Wi-Fi access points to prioritize traffic and optimize the way shared network resources are allocated among different applications. Without QoS, all applications running on different devices have equal opportunity to transmit data frames. That works well for data traffic from applications such as web browsers, file transfers, or e-mail but it is inadequate for multimedia applications. Voice over Internet Protocol (VoIP), video streaming, and interactive gaming are highly sensitive to latency increases and throughput reductions and require QoS. QoS extensions for 802.11 networks will be addressed in the upcoming IEEE 802.11e standard. (See 802.11e, WMM).

R

Range

The distance covered by a wireless network or radio device. Depending on the environment and the type of antenna used, Wi-Fi signals can have a range of up to a mile.

RC4

An encryption cipher designed RSA Data Security. It allows key lengths up to 1024 bits and is a component in many encryption schemes, including SSL, WEP, and TKIP. (See WEP, TKIP).

S

Site survey

A comprehensive facility study performed by network managers to insure that planned service levels will be met when a new wireless LAN, or additional WLAN segments to an existing network, are deployed. Site survey's are usually performed by a radio frequency engineer and used by systems integrators to identify the optimum placements of access points to insure that planned levels of service are met. Site surveys are sometimes conducted following the deployment to insure that the WLAN is achieving the necessary level of coverage. Site surveys can also be used to detect rogue access points.

SSID

A unique 32-character network name, or identifier, that differentiates one wireless LAN from another. All access points and clients attempting to connect to a specific WLAN must use the same SSID. The SSID can be any alphanumeric entry up to a maximum of 32 characters. Wi-Fi Scanner obtains SSID and other information. (See Network name).

T

TCP

Transmission Control Protocol. The Transport level protocol used with the Internet Protocol (IP) to route data across the Internet. (See IP, TCP/IP).

TCP/IP

The underlying technology of Internet communications. While IP handles the actual delivery of data, TCP tracks the data packets to efficiently route a message through the Internet. Every computer in a TCP/IP network has its own IP address that is either dynamically assigned at startup (See DHCP) or permanently assigned as a static address. All TCP/IP messages contain the address of the destination network, as well as the address of the destination station. This enables TCP/IP messages to be transmitted to multiple networks (subnets) within an organization or worldwide. For example, when a user downloads a web page, TCP divides the page file on the web server into packets, numbers the packets, and forwards them individually to the user's IP address. The packets may be routed along different paths before reaching the user's address. At the destination, TCP reassembles the individual packets, waiting until they have all arrived to present them as a single file. (See IP, IP address, Packet, TCP).

Throughput

A real-world performance measure. The average rate of successful delivery over a wireless system. Throughput is usually measured in bits per second (bps) or Megabits per second (Mbps) and sometimes in data packets per second or data packets per time slot. Throughput of a particular device will always be lower than its stated Data rate. Throughput is the amount of data that can be sent from one location to another in a specific amount of time. (See bps, Mbps).

TKIP

Temporal Key Integrity Protocol. The wireless security encryption mechanism in Wi-Fi Protected Access. TKIP uses a key hierarchy and key management methodology that removes the predictability that intruders relied upon to exploit the WEP key. It increases the size of the key from 40 to 128 bits and replaces WEP's single static key with keys that are dynamically generated and distributed by an authentication server, providing some 500 trillion possible keys that can be used on a given data packet. It also includes a Message Integrity Check (MIC), designed to prevent an attacker from capturing data packets, altering them and resending them. By greatly expanding the size of keys, the number of keys in use, and by creating an integrity checking mechanism, TKIP magnifies the complexity and difficulty involved in decoding data on a Wi-Fi network. TKIP greatly increases the strength and complexity of wireless encryption, making it far more difficult-if not impossible-for a would-be intruder to break into a Wi-Fi network. (See AES, WPA, WPA2).

TLS

Transport Layer Security. A newer version of the SSL protocol, It supports more cryptographic algorithms than SSL. TLS is designed to authenticate and encrypt data communications, preventing eavesdropping, message forgery and interference. (See EAP).

Tri-mode

In the Wi-Fi context, tri-mode refers to devices which are 802.11b, a, and g-compatible. In the mobile context, tri-mode describes a cellular phone that is capable of using analog, digital and GSM frequencies. (See Dual-band).

V

Voice over Wi-Fi

VoIP services delivered over wireless networks. Sometimes referred to as wireless voice over IP. (See VoIP).

VoIP

Voice over Internet Protocol. A technology for transmitting ordinary telephone calls over the Internet using packet-based networks instead of standard public switched telephone networks or Plain Old Telephone Service (POTS). (See Voice over Wi-Fi).

W

WAN

Wide Area Network. A data communications network that spans large local, regional, national or international areas and is usually provided by a public carrier (such as a telephone company or service provider).The term is used to distinguish between phone-based data networks and Wi-Fi networks. Phone networks are considered WANs and Wi-Fi networks are considered Wireless Local Area Networks.

WEP

The original security standard used in wireless networks to encrypt the wireless network traffic. (See WPA).

WiMAX

Worldwide Interoperability for Microwave Access. Refers to the 802.16 standard being developed by the IEEE to provide a wireless coverage of up to 31 miles. It operates in the 2 to 11 GHz bands and enables connectivity without a direct line-of-sight to a base station although line-of-site is probably required to achieve connectivity at the distance of 31 miles.. It provides shared data rates up to 70 Mbps, which, according to WiMAX proponents, is enough bandwidth to simultaneously support more than 60 businesses and hundreds of homes.

Wireless network

Devices connected to a network using a centralized wireless access point. Wi-Fi Scanner allows you to scan the Wireless networks.(See WLAN).

WLAN

Wireless Local Area Network. A type of local-area network in which data is sent and received via high-frequency radio waves rather than cables or wires. Wi-Fi Scanner allows you to scan the WLAN (See Wireless network).

WMM

Wi-Fi Multimedia. A group of features for wireless networks that improve the user experience for audio, video and voice applications. WMM is based on a subset of the IEEE 802.11e WLAN QoS draft standard. WMM adds prioritized capabilities to Wi-Fi networks and optimizes their performance when multiple concurring applications, each with different latency and throughput requirements, compete for network resources. By using WMM, end-user satisfaction is maintained in a wider variety of environments and traffic conditions. WMM makes it possible for home network users and enterprise network managers to decide which data streams are most important and assign them a higher traffic priority. (See 802.11e, QoS).

WMM Power Save

WMM Power Save is a set of features for Wi-Fi networks that increase the efficiency and flexibility of data transmission in order to conserve power. WMM Power Save has been optimized for mobile devices running latency-sensitive applications such as voice, audio, or video, but can benefit any Wi-Fi device. WMM Power Save uses mechanisms included in the IEEE 802.11e standard and is an enhancement of IEEE 802.11 legacy power save. With WMM Power Save, the same amount of data can be transmitted in a shorter time while allowing the Wi-Fi device to remain longer in a low-power dozing state.

WPA - Enterprise

Wi-Fi Protected Access-Enterprise. A wireless security method that provides strong data protection for multiple users and large managed networks. It uses the 802.1X authentication framework with TKIP encryption and prevents unauthorized network access by verifying network users through an authentication server. (See 802.1X, TKIP, WPA).

WPA - Personal

Wi-Fi Protected Access-Personal. A wireless security method that provides strong data protection and prevents unauthorized network access for small networks. It uses TKIP encryption and protects against unauthorized network access through the use of a pre-shared key (PSK). (See WPA, PSK).

WPA

Wi-Fi Protected Access. An improved security standard for wireless networks that provides strong data protection and network access control. WPA was developed by the Wi-Fi Alliance and addresses all known WEP vulnerabilities. It provides strong data protection by using encryption, as well as strong access controls and 802.1X-based user authentication which was largely missing in WEP. WPA is designed to secure all versions of 802.11 devices, including 802.11b, 802.11a, and 802.11g, dual-band and tri-mode. WPA can be enabled in two versions, WPA-Personal and WPA-Enterprise. WPA-Personal protects against unauthorized network access by utilizing a set-up pass phrase, or pre-shared key. WPA-Enterprise verifies network users through an authentication server. In either mode, WPA utilizes 128-bit encryption keys and dynamic session keys to ensure the wireless network's privacy and security. (See PSK, WEP, WPA2).

WPA2 - Enterprise

Wi-Fi Protected Access 2 - Enterprise. The follow on wireless security method to WPA that provides stronger data protection for multiple users and large managed networks. It prevents unauthorized network access by verifying network users through an authentication server. (See WPA2).

WPA2 - Personal

Wi-Fi Protected Access 2 - Personal. The follow on wireless security method to WPA that provides stronger data protection and prevents unauthorized network access for small networks. (See WPA2, PSK).

WPA2

Wi-Fi Protected Access 2. The follow on security method to WPA for wireless networks that provides stronger data protection and network access control. It provides enterprise and consumer Wi-Fi users with a high level of assurance that only authorized users can access their wireless networks. Based on the ratified IEEE 802.11i standard, WPA2 provides government grade security by implementing the National Institute of Standards and Technology (NIST) FIPS 140-2 compliant AES encryption algorithm and 802.1X-based authentication. There are two versions of WPA2: WPA2-Personal, and WPA2-Enterprise. WPA2-Personal protects unauthorized network access by utilizing a set-up password. WPA2-Enterprise verifies network users through a server. WPA2 is backward compatible with WPA. Like WPA, WPA2 uses the 802.1X/EAP framework as part of the infrastructure that ensures centralized mutual authentication and dynamic key management and offers a pre-shared key for use in home and small office environments. Like WPA, WPA2 is designed to secure all versions of 802.11 devices, including 802.11b, 802.11a, and 802.11g, multi-band and multi-mode. (See WPA2 - Enterprise, WPA2 - Personal).

WPS

Wi-Fi Protected Setup is an optional certification program developed by the Wi-Fi Alliance designed to ease set up of security-enabled Wi-Fi networks in the home and small office environment. Wi-Fi Protected Setup supports methods (pushing a button or entering a PIN into a wizard-type application) that are familiar to most consumers to configure a network and enable security.

LizardSystems
lizardsystems.com