liberty-i

Liberty-i Wireless Glossary

2G

Second generation technology. A term used to describe the digital cellular networks such as GSM which were introduced as a replacement for analogue cellular networks (1st generation). See also GSM, 2.5G, 3G.

2.5G

Technological upgrades to standard GSM mobile networks which increase data transmission speeds and efficiency. Seen as an intermediate technology between 2G and 3G. See also GSM, 2G, 3G.

3G

Third generation of mobile networks, providing video calling, browsing and faster download speeds - up to 7 times faster than GPRS (General Packet Radio Service).Implemented in Europe as UMTS and in North America as CDMA2000.1st Generation was analogue; 2nd Generation was digital. 2.5G means GPRS. See also GSM, 2G, 2.5G, UMTS.

802.11

A family of specifications for wireless local area networks (WLANs) developed by a working group of the Institute of Electrical and Electronics Engineers (IEEE). There are several specifications in the family and new ones are developed on an ongoing basis.The original version of the standard IEEE 802.11 was released in 1997 and specified two raw data rates of 1 and 2 Mbit/s.

802.11a

An IEEE specification for wireless networking that operates in the 5 GHz frequency range (5.725 GHz to 5.85GHz) with a maximum 54 Mbps raw data transfer rate (ratified 1999).
The specification uses a modulation scheme known as orthogonal frequency-division multiplexing (OFDM).

There is less interference with 802.11a than with 802.11b, because 802.11a provides more available channels, and because the frequency spectrum employed by 802.11b (2.400 GHz to 2.4835 GHz) is shared with various household appliances and medical devices.

802.11b

An IEEE specification for wireless networking that operates in the 2.4 GHz frequency range (2.4 GHz to 2.4835GHz) and provides a throughput of up to 11 Mbps (ratified 1999).
The dramatic increase in throughput of 802.11b (compared to the original 802.11 standard) along with substantial price reductions led to the rapid acceptance of 802.11b as the definitive wireless LAN technology.

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 (ratified 2001).
Rules subject to variation include allowed frequencies, power levels, and signal bandwidth. The specification eliminates the need for designing and manufacturing dozens of country specific products. The 802.11d specification is thus well suited for systems that want to provide global roaming.

802.11e

An enhancement to the 802.11a and 802.11b wireless LAN (WLAN) specifications (ratified November 2005).
It defines quality of service (QoS) mechanisms for wireless equipment to prioritize delaysensitive applications such as voice and video.
See also QoS

802.11g

An IEEE specification for wireless networking that operates in the 2.4 GHz frequency range (2.4 GHz to 2.4835GHz) and provides a throughput of up to 54 Mbps (ratified June 2003). Networks employing 802.11g operate in the same band as 802.11b, using the modulation scheme employed 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.

802.11i

An IEEE standard specifying security mechanisms for 802.11 networks (ratified June 2004). Also known as WPA2, it introduces a range of new security features that are designed to overcome the shortcomings of WEP (Wired Equivalent Privacy), which had several well-documented security deficiencies.
Wi-Fi Protected Access (WPA) had previously been introduced by the Wi-Fi Alliance as an intermediate solution to WEP insecurities. WPA implemented a subset of 802.11i.
802.11i makes use of the Advanced Encryption Standard (AES) block cipher, where as WEP and WPA used the RC4 stream cipher.

802.11k

A proposed IEEE standard, aiming to provide key client feedback to wireless LAN access points and switches. The proposed standard defines a series of measurement requests and reports that detail client statistics. Here are some of the measurements 802.11k defines:

- Roaming decisions o RF channel knowledge o Hidden nodes

- Client statistics

- Transmit Power Control (TPC)

802.11n

An upcoming specification for wireless LAN (WLAN) communications: it is intended to increase network speed and reliability and to extend the operating distance of wireless networks. 802.11n is based on MIMO (multiple input, multiple output) technology, which uses multiple antennas at both the source (transmitter) and the destination (receiver) to minimize errors and optimize data speed. A first draft of the standard was approved in March 2006. See also MIMO, Spatial Multiplexing

802.11r

A proposed IEEE specification designed to speed handoffs between Access Points in a wireless LAN, from hundreds of milliseconds currently to less than 50ms, which is necessary for voice applications to avoid hiccups and degradation of voice quality. Faster handoffs are essential for 802.11-based voice to become widely deployed.
See also Roaming.

802.11x

A way to refer to the whole set of standards falling under the 802.11 umbrella. There is no single 802.11x standard.

802.16

A group of broadband wireless communications standards for metropolitan area networks (MANs) developed by a working group of the Institute of Electrical and Electronics Engineers (IEEE). The original 802.16 standard, published in December 2001, specified fixed point- tomultipoint broadband wireless systems operating in the 10-66 GHz licensed spectrum. An amendment, 802.16a, approved in January 2003, specified non-line-of-sight extensions in the 211 GHz spectrum, delivering up to 70 Mbps at distances up to 31 miles. Officially called the WirelessMANTM specification, 802.16 standards are expected to enable multimedia applications with wireless connection and, with a range of up to 30 miles, provide a viable last mile technology.

802.1X

A standard for port-based authentication, first used in wired networks, and later 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 the network and dynamic encryption keys to protect data privacy. See also EAP, WEP, WPA, WPA2.

802.3

See Ethernet.

☎ +44 (0)808 2819 500   💻 www.liberty-i.com   ✒ info@liberty-i.com
🖨 +44 (0)125 2718 636   ✉ Unit 14 Riverside Park, Farnham, Surrey, GU9 7UG

f t in

802.3af

An IEEE specification for Power over Ethernet (PoE). The standard provides the capability to deliver both power and data over standard Ethernet cabling. Power over Ethernet enables remote devices (such as VoIP phones or Wireless Access Points) to operate without a separate power source, which simplifies equipment installation.

AES (Advanced Encryption Standard)

A block cipher adopted as an encryption standard by the US government in October 2000. Also known as "Rijndael", after its inventors Joan Daemen and Vincent Rijmen, it is used in the implementation of WPA2. (See also 802.11i, WPA2).

Access Point (AP)

A device that transmits and receives data in a wireless local area network (WLAN).
Also referred to as "Base Station", or "Wireless Hub", it connects users to other users within the wireless network and also can serve as the point of interconnection between the WLAN and a fixed wired network (Ethernet).

Ad-Hoc mode

One of two types of wireless network modes, in which computers discover others within range and form a network based on peer-to-peer connectivity. The alternative is the "Infrastructure" mode, where devices communicate with each other through an Access Point.

Bandwidth

1) In electronic communication, bandwidth is the width of the range (or band) of frequencies that an electronic signal uses on a given transmission medium. In this usage, a given bandwidth is the difference (in Hertz) between the highest frequency the signal uses and the lowest frequency it uses. A typical voice signal has a bandwidth of approximately 3 kHz (kilo Hertz); an 802.11b channel has a bandwidth of 22 MHz (Mega Hertz).

2) In computer networks, bandwidth is often used as a synonym for capacity, ie the amount of data that can be carried from one point to another in a given time period (usually a second). This kind of bandwidth is usually expressed in bits (of data) per second (bps).

Beamforming

A signal-processing technique used to control the directionality of the reception or transmission of a signal on a transducer array(such as audio speakers or radio antennae).

Beamforming takes advantage of interference to change the directionality of the array. For example, if multiple transducers are set next to each other sending out signals, an interference pattern will form, just like throwing several stones in a pond at once creates interfering ripples. By adjusting the spacing between the transducers and the delay in the transducers' signals, the interference pattern may be manipulated, so that the majority of the signal energy all goes out in one particular direction.

Applications include SONAR and IEEE 802.11n.

Bluetooth

A telecommunications industry specification for wireless personal area networks (PANs). Bluetooth eliminates the need for wires between PCs/laptops and their peripherals, like personal digital assistants (PDAs), mobile phones, printers and digital cameras.

It should not be confused with Wireless LANs, whose aim is to network computers, although both operate in the 2.4 GHz band. Its range is restricted to 10 meters.

The name Bluetooth comes from the 10th century king of Denmark, King Harald Bluetooth, who preferred diplomacy to war: the parallel seemed appropriate to the inventors of the technology, since it allows different devices to talk to each other.

Bridging mode

An AP setting useful to create wireless building-to-building links: in this configuration, two or more APs only communicate with one another, forming a dedicated link, with no client device allowed.

CDMA (Code-Division Multiple Access)

A generic term for a type of digital mobile telephony technology which supports a number of mobile connections. Used in second-generation (2G) and third-generation (3G) wireless communications, it is a form of multiplexing, which allows numerous signals to occupy a single transmission channel, optimizing the use of available bandwidth. The technology is used in the 800-MHz and 1.9-GHz bands.

CDPD (Cellular Digital Packet Data)

A digital wireless transmission system deployed as an enhancement to the analogue cellular networks (1G). Developed in the early 1990's with speeds up to 19.2 kbit/s, it was considered a promising technology but never quite gained widespread acceptance before newer, faster standards such as GPRS became dominant.

Centrino

A technology package from Intel that provides built-in wireless support for laptop computers.

Client/Server

Client/server describes the relationship between two computer programs in which one program, the client, makes a service request from another program, the server, which fulfils the request. The client/server model has become one of the central ideas of network computing.
Typically, multiple client programs share the services of a common server program: for instance, a Web browser is a client program that requests services (the sending of Web pages) from a Web server hosted in another computer somewhere on the Internet.
In the WLAN, client devices include PC Cards that slide into laptop computers, PCI adapters for desktop PCs; the server being the AP.

CSMA-CA (Carrier Sense Multiple Access/Collision Avoidance)

The principal media access control strategy used in 802.11 networks to avoid data collisions. It is a "listen before talk" method of minimizing collisions: the network node checks to see if the transmission channel is clear before a data packet is sent. If the channel is clear, then the packet is sent.

If the channel is not clear, the node waits for a randomly chosen period of time, and then checks again to see if the channel is clear. This period of time is called the backoff factor, and is counted down by a backoff counter.

CSMA-CD (Carrier Sense Multiple Access/Collision Detection)

The principal media access control strategy used to manage traffic and reduce noise on wired Ethernet networks: each device senses whether the line is idle and therefore available to be used. If it is, the device begins to transmit its first frame. If another device has tried to send at the same time, a collision is said to occur and the frames are discarded. Each device then waits a random amount of time and retries until successful in getting its transmission sent.

CTIA (Cellular Telecommunications & Internet Association)

An international non-profit organization representing all sectors of wireless communications – cellular, personal communication services and enhanced specialized mobile radio. Founded in 1984, the CTIA represents service providers, manufacturers, wireless data and Internet companies and other contributors to the wireless universe.

DHCP (Dynamic Host Configuration Protocol)

A protocol for dynamically assigning IP addresses from a pre-defined list to nodes on a network. When connecting to the network, clients send out a query requesting a response from a DHCP server on the locally attached network. The DHCP server then replies to the client with its assigned IP address, along with other IP parameters, like the address of a DNS server. Using DHCP to manage IP addresses simplifies client configuration and efficiently utilizes IP addresses. Without DHCP, an IT Manager would have to manually enter in all the IP addresses of all the computers on the network.

Dipole antenna

A straight electrical conductor measuring 1/2 wavelength from end to end. This is one of the simplest types of antenna. For best performance, a dipole antenna should be more than 1/2 wavelength above the ground, the surface of a body of water, or other horizontal, conducting medium such as sheet metal roofing. The element should also be at least several wavelengths away from electrically conducting obstructions such as supporting towers, utility wires and other antennas.

DNS (Domain Name System)

An essential component of Internet use, it translates URLs, i.e. www.dlink.eu into IP addresses, eg 213.216.192, and vice-versa. DNS servers hosted at ISPs hold databases that allow them to perform such translations.

DSSS (Direct Sequence Spread Spectrum)

A radio transmission technique that spreads a signal over a wide frequency band for transmission, thus avoiding narrowband interference. It is used in GPS, CDMA cellular phones, cordless phones operating in the 2.4 and 5.8 GHz bands, and 802.11 b Wi-Fi.

EAP (Extensible Authentication Protocol)

An authentication framework which supports multiple authentication methods. EAP may be used on dedicated links, as well as switched circuits, and wired as well as wireless links. EAP encapsulation on IEEE 802 wired media is described in IEEE-802.1X, and encapsulation on IEEE wireless LANs in IEEE-802.11i.

Encryption

Encryption is the conversion of data into a form that cannot be easily understood by unauthorized people. Decryption is the process of converting encrypted data back into its original form, so it can be understood.
Simple ciphers include the substitution of letters for numbers or the rotation of letters in the alphabet. More complex ciphers work according to sophisticated computer algorithms that rearrange the data bits in digital signals. The stronger the cipher, the harder it is for unauthorized people to break it which therefore means the higher the protection.
In order to easily recover the contents of an encrypted signal, the correct decryption key is required. The key is an algorithm that "undoes" the work of the encryption algorithm. Encryption/decryption is especially important in wireless communications, because the medium used, air, makes it easy to capture the data.

ESSID (Extended Service Set Identifier)

See SSID

Ethernet

An IEEE standard for computer networking. It is now the most widespread LAN technology, having replaced competing LAN standards such as Coaxial-cable Ethernet, Token Ring or FDDI. It provides from 10 Mbps bandwidth on basic 10BaseT Ethernet networks, to 100 Mbps on Fast Ethernet , 1000 Mbps on Gigabit Ethernet, and 10,000 Mbps on 10Gigabit Ethernet.

EVDO (Evolution-Data Optimized)

A wireless radio broadband data standard, providing faster wireless data transmission speeds of 400K bit/sec. to 700K bit/sec. with a theoretical peak of 2.4M bit/sec.
Adopted by many CDMA mobile phone service providers in Japan, Korea, the Czech Republic, Russia, Latvia, Romania, Portugal, Brazil, Israel, the United States, Australia, Canada, New Zealand, Venezuela, Angola, Mexico, Norway and Puerto Rico.

Firewall

A system of software and/or hardware that resides between two networks to prevent access by unauthorized users. The most common use of a firewall is to provide security between a local network and the Internet. Hardware and software firewalls monitor and control the flow of data in and out of computers.

FLASH-OFDM (Fast Low-latency Access with Seamless Handoff OFDM)

A proprietary cellular broadband technology that network operators can deploy either for notebook computers of mobile users or serve as a fixed wireless access system, bridging the "last mile" to connect computers in homes and small offices. Key features include an all-IP architecture and fast speeds. The technology is capable of letting users traveling at 250 kilometers per hour to download data at speeds up to 1.5Mbit/sec. or upload at speeds up to 500Kbit/sec. and would compete with GSM and 3G networks.

Gateway

A network point that acts as an entrance to another network.

GPRS (General Packet Radio Service)

An enhancement to the GSM mobile communications system that supports data packets. It enables a continuous flow of data packets over the system for applications that support web browsing and file transfer for example. With GPRS, your phone is always connected to WAP and other data services, so you do not need to dial in each time you want to access data services. See also GSM, 2.5G

GPS (Global Positioning System)

A system of 24 satellites for identifying earth locations, run by the U.S. Department of Defense. By triangulation of signals from three of the satellites, a receiving unit can pinpoint its current location anywhere on earth to within a few meters. Europe plans to have its own system operational by the end of 2010. Called Galileo, it will provide a highly accurate, guaranteed global positioning service under civilian control, and had its first experimental satellite launched in December 2005.

GSM (Global System for Mobile Communications)

The most popular standard for mobile phones in the world. Thanks to roaming agreements between operators worldwide, users can often continue to use their mobile phones when they travel to other countries.
GSM uses a variation of time division multiple access (TDMA) and is the most widely used of the three digital wireless telephony technologies (TDMA, GSM, and CDMA). It operates in either the 900 MHz or 1800 MHz frequency band.

Hot Spot (also referred to as Public Access Location)

A location where users can access the Internet using Wi-Fi enabled devices like laptops or PDAs. Access may be provided free or for a fee. Hotspots are often found at coffee shops, hotels, airport lounges, train stations, petrol stations and other public meeting areas.

Hz (Hertz)

The international unit for measuring frequency, replaces the older unit of cycles per second (cps). One megahertz (MHz) is one million Hertz. One gigahertz (GHz) is one billion hertz. The unit of measure is named after Heinrich Hertz, German physicist.

i-Mode

Packet-based information service for mobile phones from NTT DoCoMo (Japan); first to provide Web browsing from cell phones.

IEEE (Institute of Electrical and Electronics Engineers)

A global technical professional society and standards-setting organization serving the public interest and its members in electrical, electronics, computer, information and other technologies.

Infrastructure mode

One of two types of wireless network modes, in which devices connect to a network using a centralized access point; the other mode is a device-to-device network, also known as ad-hoc mode or peer-to-peer.

IP (Internet Protocol)

The method by which data is sent from one computer (host) to another on the Internet: data, eg e-mails or web pages, is split into packets, and routed across networks until it reaches its destination. The most widely used version of IP today is Internet Protocol Version 4 (IPv4). However, IP Version 6 (IPv6) is also beginning to be supported. IPv6 provides for much longer addresses and therefore for the possibility of many more Internet users.

IP address

A 32-bit number that uniquely identifies hosts on the Internet, like a postal address, i.e: 212.58.227.79.

IP telephony

A general term for the technologies that use the Internet Protocol's packet-switched connections to exchange voice, fax, and other forms of information that have traditionally been carried over the dedicated circuit-switched connections of the public switched telephone network (PSTN). Using the Internet, calls travel as packets of data on shared lines, avoiding the tolls of the PSTN.

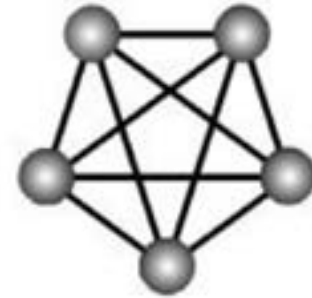**LAN (Local Area Network)**

See Ethernet

MAC address (Media Access Control address)

A 48-bit number that is hard-coded into each network adapter, ie an Ethernet port or a wireless adapter, providing a unique identifier for a device on a network. MAC addresses can not be routed, and are specific to the LAN, i.e.: 00-14-22-C9-4F-ED.

Mesh Networks

A local area network (LAN), with at least two pathways to each node, forming a net-like organization. When each node is directly connected to every other node, the network is said to be fully meshed. Otherwise, it is said to be partially meshed, or partially connected.

The illustration shows a full mesh network with five nodes.

D-Link Wireless Glossary Copyright 2006 D-Link, All Rights Reserved.

Mesh network

A mesh network is reliable and offers redundancy: if one node can no longer operate, all the rest can still communicate with each other. The chief drawback is expense, because of the large number of cables and connections required.

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 108Mbps. See also 802.11n, and Spatial Multiplexing.

NAS (Network Attached Storage)

A hard disk storage that is set up with its own network address rather than being attached to a computer. The network-attached storage device is attached to a local area network (typically, an Ethernet network) and assigned an IP address.

NAT (Network Address Translation)

A technique that allows multiple hosts on a private LAN to share a single Internet IP address. It was invented to save the pool of IP addresses in IPv4 which is limited (0.0.0.0 to 255.255.255.255). A –good- side effect is to hide the local network from the Internet, hence hackers, as there is no way to know how many devices -and what they are- behind a single IP address.

Network name

See SSID.

OFDM (Orthogonal Frequency Division Multiplexing)

A modulation technique that works by splitting radio signals into multiple smaller sub-signals that are then transmitted simultaneously at different frequencies to the receiver, reducing crosstalk and using bandwidth efficiently, but decreasing range.
OFDM is used in many communications systems such as: ADSL, Wireless LAN, Digital Audio Broadcasting and UWB.

PC card

A removable, credit-card-sized memory or I/O (input/output) device that fits into a personal computer, usually a laptop computer. PC card peripherals include wired and wireless adapters. The PC card is based on standards published by the Personal Computer Memory Card International Association (PCMCIA), hence is also referred to as PCMCIA card.

PCI (Peripheral Component Interconnect)

A standard that specifies a computer bus for attaching peripheral devices to a computer motherboard. These devices can take any one of the following forms:

- an integrated circuit fitted onto the motherboard itself

- an expansion card that fits in sockets, i.e. wireless adapters for desktops.

PCMCIA

See PC card.

Peer-to-peer network

See ad-hoc mode.

PoE (Power over Ethernet)

See 802.3af

PSK (Pre-Shared Key)

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 and each PC that is on the Wi-Fi network. After entering the password, Wi-Fi Protected Access automatically takes over. It keeps out 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 (AES). See also TKIP, WPA-Personal, and WPA2.

QoS (Quality of Service)

A mechanism that enables routers and gateway devices to prioritize traffic and optimize the way shared network resources are allocated among different applications. Without QoS, all applications running on different computers have equal opportunity to transmit data frames. That works well for 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 are addressed in the IEEE 802.11e standard. See also 802.11e and WMM.

Range

The maximum distance at which a wireless device can get a signal from an AP or another device.

Repeater

A device that regenerates the digital signal that it receives, and transmits it on, enabling the extension of a signal over a distance.
Repeaters remove the unwanted noise in an incoming signal. Unlike an analog signal, the original digital signal, even if weak or distorted, can be clearly perceived and restored. With analog transmission, amplifiers must be used, which unfortunately also amplify noise as well as information.

RFID (Radio Frequency Identification)

A technology that uses low-powered radio transmitters to read data stored in a tag at distances ranging from a few cm to 30m. RFID is coming into increasing use in industry

as an alternative to the bar code: tags are used to track assets, manage inventory and authorize payments.

RJ-45

The type of connector used in Ethernet networks. "RJ-45 port" refers to the Ethernet port of a computer.

Roaming

The ability to move seamlessly from one area of Wi-Fi coverage to another with no loss in connectivity.

Rogue Access Point

An unauthorized access point installed on a company's WLAN, typically by a user. Rogue access points present security risks, because they rarely conform to the organization's security policies and, typically, no security at all is enabled on them. Rogues present open, insecure interfaces to the company's network.

Router

In packet-switched networks such as the Internet, a device that determines the next network point to which a packet should be forwarded toward its destination. The router is connected to at least two networks, and decides which way to send each information packet.
In the home network scenario, the router sits between the LAN and the ISP's network. See also gateway.

Satellite broadband

A wireless high-speed Internet connection provided by satellites. Satellite Internet systems provide an option for people in rural areas where Digital Subscriber Line (DSL) and cable modem connections are not available.

Site survey

The process of planning and designing a wireless network, to provide a wireless solution that will deliver the required wireless coverage, data rates, network capacity, roaming capability and Quality of Service (QoS). Site surveys can also be used to detect rogue access points.

liberty-i

Spatial Multiplexing

The process of splitting a data stream into independent substreams that are then transmitted via separate antennas.

For instance, with N=3 antennas at the transmitter and receiver, the stream of bits {b1, b2, b3, b4, b5, b6..} is split into N=3 independent substreams {b1, b4,..}, { b2, b5,..}, {b3, b6,..}, which are applied separately to the N transmit antennas. At the receiver, a signal processing technique is applied to recover the original substreams and finally merge the symbols back together.

This technique effectively allows for a possible N-fold improvement of the link speed, and forms the basis of the MIMO technology used in the emerging 802.11n standard. See also 802.11n, MIMO.

SSID (Service Set Identifier)

A name used to identify a wireless network. The SSID can be any alphanumeric entry up to a maximum of 32 characters.

Also referred to as Network Name, Preferred Network, ESSID or Wireless LAN Service Area.

TCP/IP (Transmission Control Protocol/Internet Protocol)

The basic communication language -or protocol- of the Internet. Computers with access to the Internet all have a copy of the TCP/IP program.

TCP/IP is a two-layer program. The higher layer, Transmission Control Protocol, manages the dividing of a message into smaller packets that are transmitted over the Internet and received by a TCP layer that reassembles the packets into the original message. The lower layer, Internet Protocol, handles the address part of each packet so that it gets to the right destination. Each gateway computer on the network checks this address to see where to forward the message.

TDMA (Time Division Multiple Access)

A technology used in digital cellular telephone communication that divides each cellular channel into three time slots in order to increase the amount of data that can be carried. It is also used for Digital Enhanced Cordless Telecommunications (DECT).

Throughput

The amount of data that can be sent from one location to another in a specific amount of time. Usually measured in Bps, Kbps, Mbps or Gbps.

A distinction should be made between "raw" throughput and "actual" data throughput; the former is higher because it includes all the overhead, i.e the source and destination IP address, as well as the "interesting" data as such, eg the content of an e-mail.

TKIP (Temporal Key Integrity Protocol)

The encryption mechanism included as part of the IEEE 802.11i standard for wireless LANs (WLANs). It was designed to provide more secure encryption than the notoriously weak Wired Equivalent Privacy (WEP), the original WLAN security protocol. TKIP 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. It also includes a Message Integrity Check (MIC), designed to prevent an attacker from capturing data packets, altering them and resending them.

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 also 802.11i.

TPC (Transmit Power Control)

A technical mechanism used within some networking devices in order to prevent too much unwanted interference between different wireless networks. It works by automatically reducing the transmission output power when other networks are detected within range. Reduced power means reduced interference problems. TPC is mandatory in IEEE 802.11a devices.

UDP (User Datagram Protocol)

One of the core protocols of the Internet Protocol suite, with TCP: using UDP, programs on networked computers can send short messages known as datagrams to one another. UDP does not provide the reliability and ordering guarantees that TCP does. Datagrams may arrive out of order or go missing without notice. Without the overhead of checking if every packet actually arrived, UDP is faster and more efficient for many lightweight or time-sensitive purposes.

Common network applications that use UDP include the Domain Name System (DNS), streaming media applications, Voice over IP, and online games
See also TCP/IP

UMTS (Universal Mobile Telecommunications System)

Also known as 3G, the third generation digital standard for mobile telecommunications.

USB (Universal Serial Bus)

A specification for high-speed bidirectional connection between a PC and peripherals such as printers, scanners, digital cameras and speakers. The new USB 2.0 specification (adopted in 2000) provides a data rate of up to 480 Mbps, compared to the original specification at only 12 Mbps.

UWB (Ultrawideband)

A wireless technology for transmitting digital data over a wide swath of the radio frequency spectrum with very low power. Because of the low power requirement, it can carry signals through doors and other obstacles that tend to reflect signals at more limited bandwidths and a higher power. It can carry large amounts of data and is used for ground-penetrating radar and radio locations systems.

VoIP (Voice over IP)

A technology for transmitting telephone calls over the Internet in digital form rather than by using the traditional circuit-committed protocols of the public switched telephone network (PSTN).

VoWLAN (Voice over WLAN)

A method of sending voice information in digital form over a wireless broadband network. Essentially, VoWLAN is VoIP delivered through wireless technology. Also referred to as "VoWi-Fi" or "Wi-Fi VoIP".

VPN (Virtual Private Network)

A network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network. A VPN works by using the shared public infrastructure while maintaining privacy through security procedures and protocols that encrypt

data at the sending end and decrypt it at the receiving end, thus creating a "tunnel" that cannot be "entered" by data that is not properly encrypted.

W-CDMA (Wideband CDMA)

A type of 3G cellular network. W-CDMA is the technology behind the 3G UMTS standard and is allied with the 2G GSM standard.
W-CDMA can support mobile/portable voice, images, data, and video communications at up to 2 Mbps (local area access) or 384 Kbps (wide area access). A 5 MHz-wide carrier is used, compared with 200 kHz-wide carrier for narrowband CDMA.

WAP (Wireless Application Protocol)

A global, open standard for providing mobile phones, pagers and other handheld devices with secure access to e-mail and simple web pages.

War Chalking

The practice of making chalk marks on outdoor surfaces (walls, pavements, buildings, trees) to indicate the existence of an open wireless network connection, offering free Internet access. The chalk symbols indicate the type of access point that is available at that specific location: a pair of back-to-back semi-circles for an open node; a closed circle for a closed node; a closed circle with a "W" inside for a node equipped with WEP.

War Driving

The practice of driving around with a GPS, a laptop equipped with a wireless adapter and/or an antenna, in order to document the location of secured and unsecured WLANs. Because a wireless LAN may have a range that extends beyond an office building, an outside user may be able to intrude into the network, obtain a free Internet connection, and possibly gain access to company records and other resources.
The name derives from the film "War Games", in which hackers gained access to traditional networks by randomly dialling telephone numbers until a modem answered.

☎ +44 (0)808 2819 500   💻 www.liberty-i.com   🖰 info@liberty-i.com
🖨 +44 (0)125 2718 636   ✉ Unit 14 Riverside Park, Farnham, Surrey, GU9 7UG

Liberty-i is a trading name of Liberty-izone Ltd. Registered in England, 04942248 | Registered Office: Leytonstone House, Leytonstone, London, E11 1GA | VAT Number 822 0974 39

WDS (Wireless Distribution System)

An AP mode that allows multiple wired networks to be linked together over wireless. With WDS, an AP can act as both a bridge and an AP, ie client devices are allowed as well. See also Bridging mode.

WEP (Wired Equivalent Privacy)

A security protocol, specified in the IEEE 802.11b standard that is designed to provide a WLAN with a level of security and privacy similar to that of a wired LAN.
WEP encrypts the data portion of each frame using one of the predefined keys.

Wi-Fi (Wireless Fidelity)

Term describing WLAN products that are based on the IEEE's 802.11 standards.

Wi-Fi Alliance (formerly WECA – Wireless Ethernet Compatibility Alliance)

A global, non-profit organization formed in 1999 to test and certify the compatibility of Wi-Fi products based on IEEE 802.11 specifications. In 2006, the alliance counted more than 250 members and had certified the interoperability of more than 2,800 products.

WME (Wireless Multimedia Extensions) or WMM (Wi-Fi Multimedia)

A set of features based on the IEEE 802.11e draft standard that provide basic Quality of Service (QoS) to IEEE 802.11 networks. It prioritizes traffic from different applications such as voice, audio and video applications under different environment and conditions. Traffic priority is based on four access categories, listed here in their order of importance: voice, video, best effort (Web surfing and e-mail, for example) and background (applications not dependent upon latency, such as printing).

WML (Wireless Mark-up Language)

The language behind WAP

WPA (Wi-Fi Protected Access)

A subset of the 802.11i specification for security on wireless networks, adopted while 802.11i was still under development. It comes in two flavours, "Enterprise" and "Personal".

WPA-Enterprise (Wi-Fi Protected Access - Enterprise)

A wireless security method that provides strong data protection for multiple users in 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, such as RADIUS.

WPATM - Personal (Wi-Fi Protected Access - Personal)

A wireless security method that provides strong data protection and prevents unauthorized network access for small networks where there is no central authentication server. It uses TKIP encryption and protects against unauthorized network access through the use of a pre-shared key (PSK), hence the reference to WPA-PSK. The PSK is easily configured as a password.

WPA2

See 802.11i

WiMAX (Worldwide Interoperability for Microwave Access)

A wireless industry coalition formed in April 2001 to promote IEEE 802.16 standards for broadband wireless access (BWA) networks.
See also 802.16

WLAN (Wireless LAN)

A type of local-area network (LAN) that uses high-frequency radio waves rather than wires to communicate between nodes.