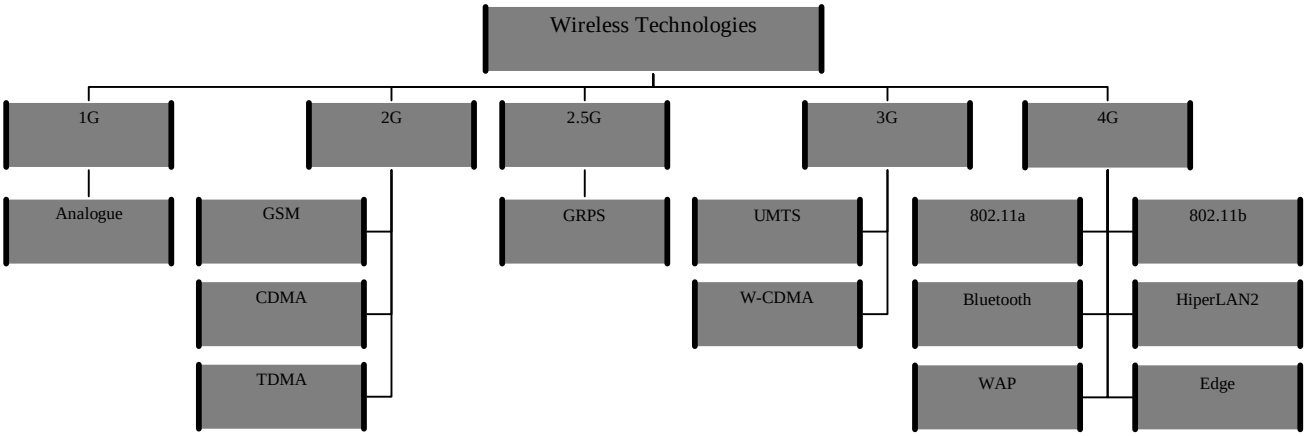
WIRELESS NETWORKING[i]

Overview of wireless technologies

The term wireless networking refers to technology that enables two or more computers to communicate using standard network protocols, but without network cabling. Strictly speaking, any technology that does this could be called wireless networking. The notion of wireless technology has been around for a long time, starting with the first analogue cellular phones. Technologies existing today are best classified in the following diagram:



All together the above technologies, excluding analogue, are referred to as 11.5G and are considered competing as industry experts expect the each technology will roll out highly competitive products. The current buzzword however generally refers to wireless local area networks (LANs). This technology, fuelled by the emergence of cross-vendor industry standards such as IEEE 802.11, has produced a number of affordable wireless solutions that are growing in popularity with business and schools as well as sophisticated applications where network wiring is impossible, such as in warehousing or point-of-sale handheld equipment.

Types of wireless network

An ad-hoc, or peer-to-peer wireless network, consists of a number of computers each equipped with a wireless networking interface card. Each computer can communicate directly with all of the other wireless enabled computers. They can share files and printers this way, but may not be able to access wired LAN resources, unless one of the computers acts as a bridge to the wired LAN using special software. (This is called "bridging".)

A wireless network can also use an access point, or base station. In this type of network the access point acts like a hub, providing connectivity for the wireless computers. It can connect (or "bridge") the wireless LAN to a wired LAN, allowing wireless computer access to LAN resources, such as file servers or existing Internet Connectivity.

Each access point has a finite range within which a wireless connection can be maintained between the client computer and the access point. The actual distance varies depending upon the

environment; manufacturers typically state both indoor and outdoor ranges to give a reasonable indication of reliable performance. Also, it should be noted that when operating at the limits of range the performance may drop, as the quality of connection deteriorates and the system compensates.

Typical indoor ranges are 150-300 feet, but can be shorter if the building construction interferes with radio transmissions. Longer ranges are possible, but performance will degrade with distance.

Outdoor ranges are quoted up to 1000 feet, but again this depends upon the environment.

There are ways to extend the basic operating range of Wireless communications, by using more than a single access point or using a wireless relay /extension point.

The single access point capacity depends upon the manufacturer. Some hardware access points have a recommended limit of 10, with other more expensive access points supporting up to 100 wireless connections. Using more computers than recommended will cause performance and reliability to suffer.

Software access points may also impose user limitations, but this depends upon the specific software, and the host computer's ability to process the required information.

WLAN standards

Wireless networking hardware requires the use of underlying technology that deals with radio frequencies as well as data transmission. The most widely used standard is 802.11 produced by the Institute of Electrical and Electronic Engineers (IEEE). This is a standard defining all aspects of Radio Frequency wireless networking.

The broad group of standards, 802.11, was approved by IEEE in 1999. Technologies included into 802.11 standard operate based on the following three methods of signal transmission:

DSSS

Acronym for ***d**irect-**s**equence **s**pread **s**pectrum*. DSSS is one of two types of spread spectrum radio, the other being frequency-hopping spread spectrum. In DSSS a data signal at the sending station is combined with a higher data rate bit sequence, or chipping code, that divides the user data according to a spreading ratio. The chipping code is a redundant bit pattern for each bit that is transmitted, which increases the signal's resistance to interference. If one or more bits in the pattern are damaged during transmission, the original data can be recovered due to the redundancy of the transmission.

FHSS

Acronym for ***f**requency-**h**opping **s**pread **s**pectrum*. FHSS is the other type of spread spectrum radio, the other being direct-sequence spread spectrum. In FHSS the data signal is modulated with a narrowband carrier signal that "hops" in random but in a known sequence from frequency to frequency as a function of time over a wide band of frequencies. The signal energy is spread in time domain rather than chopping each bit into small pieces in the frequency domain. This technique reduces interference because a signal from a narrowband system will only affect the spread spectrum signal if both are transmitting at the same frequency at the same time. Devices based on FHSS cannot interoperate with devices based on DSSS.

The transmission frequencies are determined by a spreading, or hopping, code. The receiver must be set to the same hopping code and must listen to the incoming signal at the right time and correct frequency in order to properly receive the signal. Current FCC regulations require manufacturers to use 75 or more frequencies per transmission channel with a maximum dwell time (the time spent at a particular frequency during any single hop) of 400 ms.

OFDM

Short for ***O**rthogonal **F**requency **D**ivision **M**ultiplexing*, a frequency division multiplexing 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 (disturbance, caused by electromagnetic interference) in signal transmissions.

Today there are three standards of the IEEE 802.11: 802.11b, 802.11a and 802.11g.

802.11 b

Also known as 802.11 high-rate or Wi-Fi ('wireless fidelity'), the 802.11b technology was approved by IEEE in 1999 and is currently the mainstream technology adopted by wireless device manufacturers. As outlined by the 802.11b specification, chip sets would use a modulation scheme known as Complementary Code Keying (CCK) to transmit data signals at 11 megabits-per-second (Mbps) through an unlicensed portion of the spectrum found at about 2.4GHz. Considered revolutionary at the time (and by some measures even still today), 802.11b gave way to a new generation of products that allowed an Ethernet connection to finally break free of wires but its speed was still only one-tenth that of its wired brethren. 802.11b operates based on DSSS.

The 802.11b technology has found numerous supporters including, Microsoft, Cisco, Alcatel, Agere Systems, and other 120 companies that had joined WECA (Wireless Ethernet Compatibility Alliance). Supporting companies rolled out a number of products based on 802.11b that has been well-received by users despite remaining general wireless security concerns.

802.11 a

802.11a standard was approved concurrently with 802.11b. 802.11a utilizes OFDM method of signal transmission and is not compatible with 802.11b devices. 802.11a technology promises to deliver speed of 54 Mbps (compared to 11Mpbs of 802.11b) and operates in 5GHz frequency spectrum.

Due to public attention skewed in favor of 802.11b as well as smaller number of supporting companies, the standard had evolved dramatically since its introduction in 1999. In September 2001, Intel and 3Com announced introduction of product line based on 802.11a. A number of smaller companies came out with niche-specific support products.

802.11g

In order to enhance the 802.11 standard, the IEEE's overall Working Group that oversaw the development of 802.11 assigned individual tasks to several specialty groups -- each with the goal of further advancing the technology. The mission of 802.11g was to boost the data transmission to the so-called "turbo" rates of 54 Mbps while still maintaining interoperability with earlier

specs. This way, consumers (and enterprise users, vendors, investors and just about everyone else) who bet on earlier versions of the technology would know how the market would eventually evolve.

But the road to the next generation was bumpy along the way. Task Group G (which totals about 175 people) broke off into two separate camps after May when a proposal by Texas Instruments was taken out of consideration despite the fact that they had been working for years on that proposal. They made sure their modulation scheme, known as Packet Binary Convolution Coding (PBCC), became an accepted alternative to the original CCK schema in order to ensure full backward-capability. In fact, they even invested $300 million to acquire a company (Alantro Communications) that helped develop PBCC.

After prolonged debates, on November 16, 2001 the IEEE approved the new 802.11g standard, which promises to deliver speed of 20-54 MBps the 2.4GHz band.

Security concerns

Wireless communications obviously provide potential security issues, as an intruder does not need physical access to the traditional wired network in order to gain access to data communications. However, 802.11 wireless communications cannot be received --much less decoded-- by simple scanners, short wave receivers etc. This has led to the common misconception that wireless communications cannot be eavesdropped at all. However, eavesdropping is possible using specialist equipment.

To protect against any potential security issues, 802.11 wireless communications have a function called WEP (Wired Equivalent Privacy), a form of encryption that provides privacy comparable to that of a traditional wired network. If the wireless network has information that should be secure then WEP should be used, ensuring the data is protected at traditional wired network levels. Several industry players have recently offered secure wireless solutions. For example, on September 12, 2001 Harrison Communications introduced its SecNet-11 for government and military solutions, which has already been approved by the National Security Agency.

Economic impact

The question that most IT specialists are trying to answer when considering whether or not to deploy wireless LANs is whether the benefits will outweigh the costs. The ultimate success of the technology will depend very much on the willingness of end-users to embrace it. While increased flexibility, productivity, and accuracy are recognized as potential benefits, it is very difficult to quantify the cost savings of using WLANs.

Time savings

The strongest and most quantifiable benefit seen in WLAN use is in terms of time saving. According to the study performed by the Wireless Industry's Information Source, "a wireless LAN user can save up to eight hours per week versus a wired LAN user. In monetary terms these savings range from $30 to $750 per week per user." It is interesting to note that the biggest time savings result from the ability to catch up on emails and obtain information from the LAN without having to call other colleagues. An example is a nurse working on one floor of a hospital

and having to access a patient's information. Instead of calling the receptionist or some other assistant, she could access the information on her own with the help of a wireless device.

Flexibility and quality of work

Flexibility and quality are some of the "soft" benefits that cannot be quantified but often drive WLAN adoption. Wireless LAN users are able to access the LAN from a variety of areas inside and outside their buildings. The broad coverage gives users the flexibility to remain linked to the network and remain mobile at the same time. The level of flexibility will of course depend on the variety of wireless access point locations but wireless LAN users recognize the increased convenience and the boost to productivity allowed by their ability to access the network from a multitude of locations.

The improvements in the quality of work that wireless LAN users underline results primarily from improved accuracy. By using a wireless LAN, data can now be fed directly from various locations instead of being manually input at a later date.

---

[i] This document represents compilation from the following publications:

http://www.vicomsoft.com/knowledge/reference/wireless1.html*track=internal

http://www.webopedia.com

Bob Liu, 802.11g-reenlighted After Task Group Battle, **www.80211-planet.com**

Wireless LANs: Improving Productivity and Quality of Life, **www.wlana.com**