

Wireless LANs

A Wireless LAN (W-LAN) is a data transmission system designed to provide location independent network access between computing devices by using radio waves, rather than a cable infrastructure.

Using Radio Frequency (RF) technology, wireless LANs transmit and receive data over the air, minimizing the need for wired connections. Thus, Wireless LANs combine data connectivity with user mobility.

The widespread reliance on networking in business and the growth of the Internet and online services are strong indicators of the benefits of shared data and shared resources. With wireless LANs, users

can access shared information without looking for a place to plug in, and network managers can set up networks without installing or moving wires.

How Wireless LANs work?

In a typical Wireless LAN configuration, a transmitter/receiver (transceiver) device, called an **Access Point**, connects to the wired network from a fixed location using standard cabling. At a minimum, the access point can support a small group of users and can function within a range of less than one hundred to several hundred feet. The access point (or the antenna attached to the access point) is usually mounted essentially anywhere that it is practical as long as the desired radio coverage is obtained.

End users access the wireless LAN through wireless LAN adapters, which are implemented as

PC cards in notebooks or palmtop computers, as cards in desktop computers or integrated within handheld computers. Wireless LAN adapters provide an interface between the client Network Operating System (NOS) and the airwaves via an antenna. The nature of the wireless connection is transparent to the NOS.

WLAN standards:

The IEEE Standards board approved the 802.11 wireless LAN standard. IEEE 802.11 brings multi - vendor interoperability. The main features of IEEE 802.11 standard include:

- ✍ Robust (because of Acknowledgement, RTS/CTS features)
- ✍ Multi channel Roaming
- ✍ Power management scheme providing longer battery life
- ✍ Automatic rate selection
- ✍ Security WEP (Wired Encryption Privacy)

IEEE 802.11 Standard specifies the frequency band for WLAN applications as 2.4Ghz ISM (Industry Science, and Medical) band.

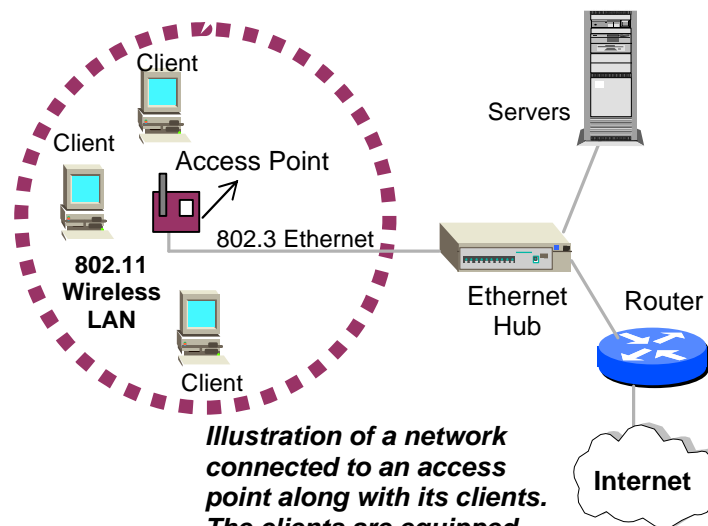


Illustration of a network connected to an access point along with its clients. The clients are equipped with a WLAN radio card.

Wireless LAN Technologies:

W-LANs have a range of technologies to choose from, while designing a W-LAN solution. Each one comes with its own set of advantages & limitations.

✍ **Narrowband:** A narrow band radio system transmits and receives user information on a specific radio frequency. Narrowband radio keeps the radio signal frequency as narrow as possible just to pass the information. Undesirable crosstalk between communication channels is avoided by carefully coordinating different users on different channel frequencies.

A private telephone line is much like a radio frequency. When each home in a neighborhood has its own private telephone line, people in one home cannot listen to calls made to other homes. In a radio system, privacy and non-interference are accomplished by the use of separate radio frequencies. The radio receiver filters out all radio

signals except the ones on its designated frequency.

✍ **Spread Spectrum:** Most wireless LAN systems use spread spectrum technology, a wide-band radio frequency technique developed by the military for use in reliable, secure, mission-critical communications systems. Spread spectrum is designed to trade off bandwidth efficiency for reliability, integrity and security. In other words, more bandwidth is consumed than in the case of Narrowband transmission, but the tradeoff produces a signal that is, in effect, louder and thus easier to detect, provided the receiver knows the parameters of the spread spectrum signal being broadcast. If a receiver is not tuned to the right frequency, a spread spectrum signal looks like background noise. There are two kinds of Spread Spectrum **Radio Frequency Hopping (FHSS)** and **Direct Sequence (DSSS)**.

✍ **Infrared:** A third technology, little used in commercial wireless LANs, is infrared. Infrared (IR) systems use very high frequencies, just below visible light in the electromagnetic spectrum, to carry data. Like light, IR cannot penetrate opaque objects; it is either a directed (line-of-sight) or diffuse technology.

Inexpensive directed systems provide a very limited range, generally three feet and typically are used for personal area networks but occasionally are used in specific wireless LAN applications. High performance directed IR is impractical for mobile users and is therefore used only to implement fixed sub-networks. Diffuse (or reflective) IR wireless LAN systems do not require line-of-sight, but cells are limited to individual rooms.

How secure is a Wireless LAN?

One of the main concerns of users of W-LANs is the assumed reduction in privacy and security. Next to all standard LAN Access Control mechanisms

offered by network operating systems, Wireless LANs uses multiple levels of security to prevent unauthorized access to network resources.

The W-LAN offers up to five layers of added protection. The following elements add to the security:

✍ **Spread Spectrum Technology:** Most of the W-LAN products use low power Spread Spectrum technology in sending the signal. In doing so, it transmits data by converting the signal from digital to analog and spreading it eleven times over the waveband. This spreading is done using a unique code that is built into the product. Physical access to the LAN does not yield intelligible results unless the W-LAN product is used to decode the signal.

✍ **“Close Wireless System” option:** W-LAN systems provide the so called “Close Wireless System” option, which will prevent wireless stations

to associate with an Access Point if the Network Name differs.

✍ **Station Authentication:** Shared key authentication feature allows Access Points to verify the user as being authorized to associate to the Access Point. It requires WEP (Wired Encryption Privacy) to be present. The actual authentication procedure consists of an exchange of four messages between the station and the Access Point, allowing the Access Point to verify that the station has the proper key.

✍ **Hardware Encryption using WEP:** As an added option wireless solutions use hardware encryption to provide added privacy to transmitted data. The traffic between the stations will be encrypted in order to prevent eavesdropping. Wireless LANs use encryption based on various algorithms.

✍ **Access Control Table:** Wireless Solutions have the included capability to restrict access to the infrastructure network to those stations of which the hardware MAC address is included in a preloaded filter table. Network

administrators who wish to deploy this capability will create a table of MAC addresses of wireless stations that are allowed to have access to the backbone. Stations with MAC addresses that do not appear in this table are not granted access, and the traffic generated by these stations will be filtered out. This mechanism is known as ‘Access Control’ and the specific table mentioned is called the Access Control Table.

In addition to the above, user defined schemes can be added such as user passwords on network servers. With the provided security provisions in place, Wireless systems will have equal or more privacy than can be expected from existing wired stations.

W-LANs in Operation

W-LANs devices don't operate at their maximum 11 Mbps rate across their entire range. Depending upon the size of the antenna used with a particular PC card or access point, 802.11b products all claim to support transmission over distances of at least 150 feet. But transmission rates will fall

off to 1 or 2 Mbps near the edge of this coverage area. Distance and maximum available bandwidth can be affected by obstructions. W-LAN range in open air where line-of-sight exists, is considerably more than in a closed office environment.

For greater geographic coverage, additional access points can be added, tied together via wired LAN connections. The capability to roam between access point areas (cells) without dropping connections is claimed by some vendors; otherwise, users can simply reconnect if they move their W-LAN linked computer to another access point area.

W-LAN advantages over Wired LANs:

- ✍ Mobility
- ✍ Installation Speed and Simplicity
- ✍ Installation Flexibility
- ✍ Reduced Cost of Ownership
- ✍ Scalability

Wireless LAN Configurations:

Wireless LANs can be simple or complex. At its most basic, two PCs equipped with wireless adapter cards can setup an independent network whenever they are within range of one another. On-demand networks require no administration or pre-configuration. In this case, each client would only have access to the resources of the other client & not to a central server.

WLANs configurations range from simple Peer-Peer topologies to complex networks offering distributed data connectivity and roaming. Besides offering end-user mobility within a networked environment Wireless LANs enable portable networks, allowing LANs to move with the knowledge workers that use them.

