





Presented by:



Copyright 2000i½

## What is WLAN ?

### Wireless LAN

[Home](#)  
[Search](#)

▼ ▼ ▼ ▼  
[About Pulse](#)  
[Products](#)  
[Services](#)

▼ ▼ ▼ ▼  
[Contact Us](#)  
[Email Us](#)

▼ ▼ ▼ ▼  
[Ordering](#)

▼ ▼ ▼ ▼  
[Manufacturers](#)

▼ ▼ ▼ ▼  
[Learn](#)  
[Datacomm](#)

▼ ▼ ▼ ▼  
[Mailing List](#)

#### Executive Summary

This document introduces the benefits, uses and basic technologies of wireless LANs (WLANs). A WLAN is an on-premise data communication system that reduces the need for wired connections and makes new applications possible, thereby adding new flexibility to networking. Mobile WLAN users can access information and network resources as they attend meetings, collaborate with other users, or move to other campus locations. But the benefits of WLANs extend beyond user mobility and productivity to enable portable LANs. With WLANs, the network itself is movable. WLANs have proven their effectiveness in vertical markets and are now experiencing broader applicability in a wide range of business settings.

This document describes the business benefits and applications of WLANs and explains how WLANs differ from other wireless technologies. It explains the basic components and technologies of WLANs and how they work together. It explores the factors that customers must consider when evaluating WLANs for their business applications needs. Finally, it introduces the Wireless LAN Alliance (WLANA), a non-profit consortium of wireless LAN vendors that provides ongoing education about specific applications, current technologies, and future directions of wireless LANs.

#### Overview

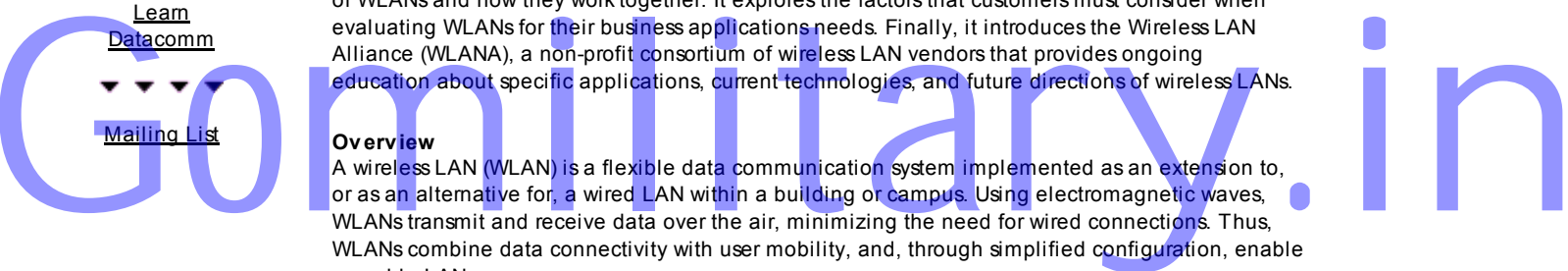
A wireless LAN (WLAN) is a flexible data communication system implemented as an extension to, or as an alternative for, a wired LAN within a building or campus. Using electromagnetic waves, WLANs transmit and receive data over the air, minimizing the need for wired connections. Thus, WLANs combine data connectivity with user mobility, and, through simplified configuration, enable movable LANs.

Over the last seven years, WLANs have gained strong popularity in a number of vertical markets, including the health-care, retail, manufacturing, warehousing, and academic arenas. These industries have profited from the productivity gains of using hand-held terminals and notebook computers to transmit real-time information to centralized hosts for processing. Today WLANs are becoming more widely recognized as a general-purpose connectivity alternative for a broad range of business customers. The U.S. wireless Lan market is rapidly approaching \$1 billion in revenues.

#### Applications for Wireless LANs

Wireless LANs frequently augment rather than replace wired LAN networks-often providing the final few meters of connectivity between a backbone network and the mobile user. The following list describes some of the many applications made possible through the power and flexibility of wireless LANs:

- *Doctors and nurses in hospitals* are more productive because hand-held or notebook computers with wireless LAN capability deliver patient information instantly.
- *Consulting or accounting audit engagement teams* or small workgroups increase productivity with quick network setup.
- *Network managers in dynamic environments* minimize the overhead of moves, adds, and changes with wireless LANs, thereby reducing the cost of LAN ownership.
- *Training sites at corporations and students at universities* use wireless connectivity to



facilitate access to information, information exchanges, and learning.

- *Network managers installing networked computers in older buildings* find that wireless LANs are a cost-effective network infrastructure solution.
- *Retail store owners* use wireless networks to simplify frequent network reconfiguration.
- *Trade show and branch office workers* minimize setup requirements by installing preconfigured wireless LANs needing no local MIS support.
- *Warehouse workers* use wireless LANs to exchange information with central databases and increase their productivity.
- Network managers implement wireless LANs to provide *backup for mission-critical applications* running on wired networks.
- *Senior executives in conference rooms* make quicker decisions because they have real-time information at their fingertips.

### Benefits of WLANs

The widespread strategic reliance on networking among competitive businesses and the meteoric growth of the Internet and online services are strong testimonies to 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 or augment networks without installing or moving wires. Wireless LANs offer the following productivity, service, convenience, and cost advantages over traditional wired networks:

- **Mobility**-Wireless LAN systems can provide LAN users with access to real-time information anywhere in their organization. This mobility supports productivity and service opportunities not possible with wired networks.
- **Installation Speed and Simplicity**-Installing a wireless LAN system can be fast and easy and can eliminate the need to pull cable through walls and ceilings.
- **Installation Flexibility**-Wireless technology allows the network to go where wire cannot go.
- **Reduced Cost-of-Ownership**-While the initial investment required for wireless LAN hardware can be higher than the cost of wired LAN hardware, overall installation expenses and life-cycle costs can be significantly lower. Long-term cost benefits are greatest in dynamic environments requiring frequent moves, adds, and changes.
- **Scalability**-Wireless LAN systems can be configured in a variety of topologies to meet the needs of specific applications and installations. Configurations are easily changed and range from peer-to-peer networks suitable for a small number of users to full infrastructure networks of thousands of users that allows roaming over a broad area.

### Wireless LAN Technology Options

Manufacturers of wireless LANs have a range of technologies to choose from when designing a wireless LAN solution. Each technology comes with its own set of advantages and limitations.

#### Spread Spectrum

Most wireless LAN systems use spread-spectrum technology, a wideband 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 that 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 types of spread spectrum radio: frequency hopping and direct sequence.

#### Narrowband Technology

A narrowband 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 communications 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 noninterference are accomplished by the use of separate radio frequencies. The radio receiver filters out all radio signals except the ones on its designated frequency.

**Frequency-Hopping Spread Spectrum Technology**

Frequency-hopping spread-spectrum (FHSS) uses a narrowband carrier that changes frequency in a pattern known to both transmitter and receiver. Properly synchronized, the net effect is to maintain a single logical channel. To an unintended receiver, FHSS appears to be short-duration impulse noise.

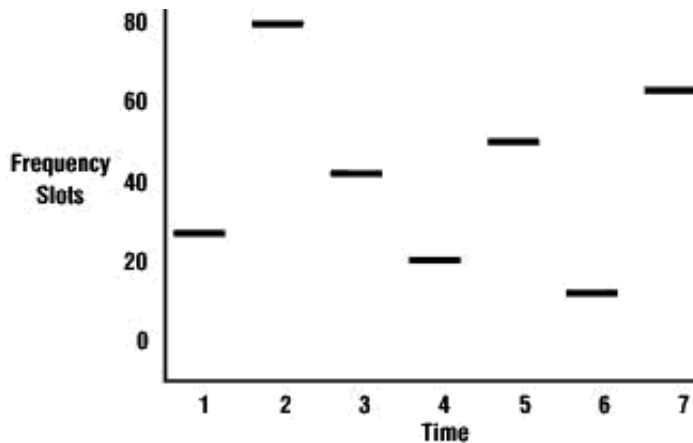
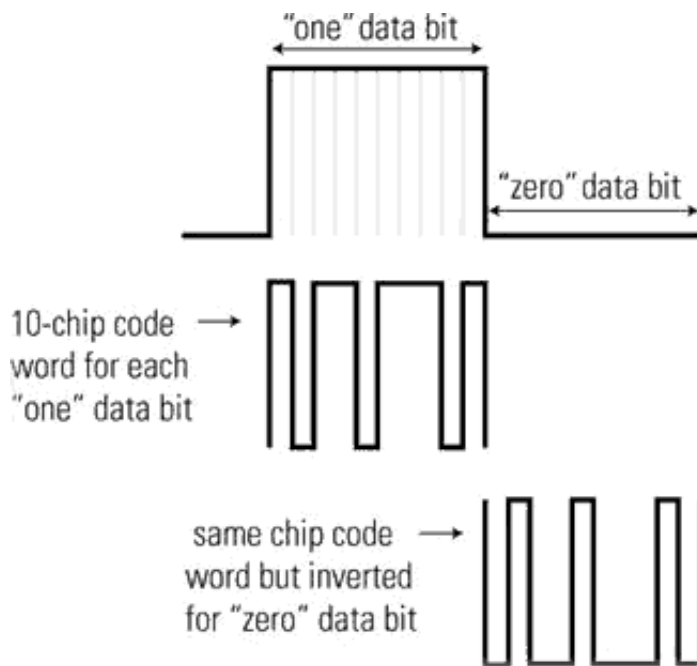


Figure 7. Frequency Hopping Spread Spectrum

**Direct-Sequence Spread Spectrum Technology**

Direct-sequence spread-spectrum (DSSS) generates a redundant bit pattern for each bit to be transmitted. This bit pattern is called a chip (or chipping code). The longer the chip, the greater the probability that the original data can be recovered (and, of course, the more bandwidth required). Even if one or more bits in the chip are damaged during transmission, statistical techniques embedded in the radio can recover the original data without the need for retransmission. To an unintended receiver, DSSS appears as low-power wideband noise and is rejected (ignored) by most narrowband receivers.



**Infrared Technology**

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 directed (line-of-sight) or diffuse technology. Inexpensive directed systems provide very limited range (3 ft) and typically are used for PANs but occasionally are used in specific WLAN applications. High performance directed IR is impractical for mobile users and is therefore used only to implement fixed subnetworks. Diffuse (or reflective) IR WLAN systems do not require line-of-sight, but cells are limited to individual rooms.

**How WLANs Work**

A wireless LAN (WLAN) is a flexible data communication system implemented as an extension to, or as an alternative for, a wired LAN within a building or campus. Using electromagnetic waves, WLANs transmit and receive data over the air, minimizing the need for wired connections. Thus, WLANs combine data connectivity with user mobility, and, through simplified configuration, enable movable LANs. Over the last seven years, WLANs have gained strong popularity in a number of vertical markets, including the health-care, retail, manufacturing, warehousing, and academic arenas. These industries have profited from the productivity gains of using hand-held terminals and notebook computers to transmit real-time information to centralized hosts for processing. Today WLANs are becoming more widely recognized as a general-purpose connectivity alternative for a broad range of business customers. The U.S. wireless Lan market is rapidly approaching \$1 billion in revenues.

**WLANs and other Wireless Technologies**

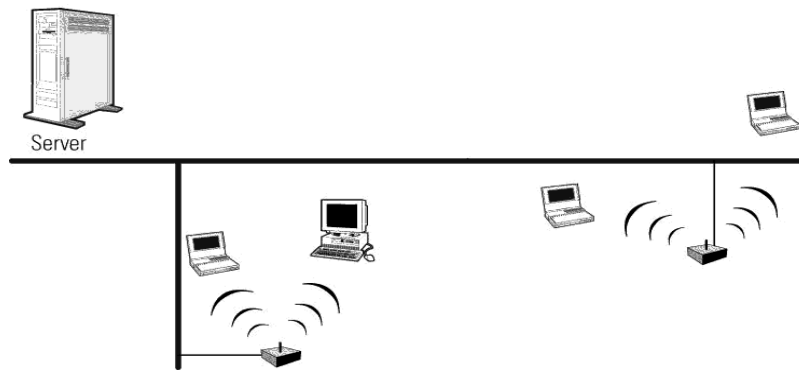
Wireless LANs use electromagnetic airwaves (radio and infrared) to communicate information from one point to another without relying on any physical connection. Radio waves are often referred to as radio carriers because they simply perform the function of delivering energy to a remote receiver. The data being transmitted is superimposed on the radio carrier so that it can be accurately extracted at the receiving end. This is generally referred to as modulation of the carrier by the information being transmitted. Once data is superimposed (modulated) onto the radio carrier, the radio signal occupies more than a single frequency, since the frequency or bit rate of the modulating information adds to the carrier.

Multiple radio carriers can exist in the same space at the same time without interfering with each other if the radio waves are transmitted on different radio frequencies. To extract data, a radio receiver tunes in (or selects) one radio frequency while rejecting all other radio signals on different frequencies.

In a typical WLAN configuration, a transmitter/receiver (transceiver) device, called an access point, connects to the wired network from a fixed location using standard Ethernet cable. At a minimum, the access point receives, buffers, and transmits data between the WLAN and the wired network infrastructure. A single 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 high but may be mounted essentially anywhere that is practical as long as the desired radio coverage is obtained.

End users access the WLAN through wireless LAN adapters, which are implemented as PC cards in notebook computers, or use ISA or PCI adapters in desktop computers, or fully integrated devices within hand-held computers. WLAN 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.

**Bluetooth** technology is a forthcoming wireless personal area networking (WPAN) technology that has gained significant industry support and will coexist with most wireless LAN solutions. The Bluetooth specification is for a 1 Mbps, small form-factor, low-cost radio solution that can provide links between mobile phones, mobile computers and other portable handheld devices and connectivity to the internet. This technology, embedded in a wide range of devices to enable simple, spontaneous wireless connectivity is a complement to wireless LANs which are designed to provide continuous connectivity via standard wired LAN features and functionality.



### WLAN Customer Considerations

#### Benefits of WLANs

Range/Coverage

Throughput

Multipath Effects

Integrity and Reliability

Interoperability with Wired Infrastructure

Interoperability with Wireless Infrastructure

#### Interference and Coexistence

Simplicity/Ease of Use

Security

Cost

Scalability

Battery Life for Mobile Platforms

Safety

### Benefits of WLANs

The widespread strategic reliance on networking among competitive businesses and the meteoric growth of the Internet and online services are strong testimonies to 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 or augment networks without installing or moving wires. Wireless LANs offer the following productivity, service, convenience, and cost advantages over traditional wired networks:

#### **Range/Coverage**

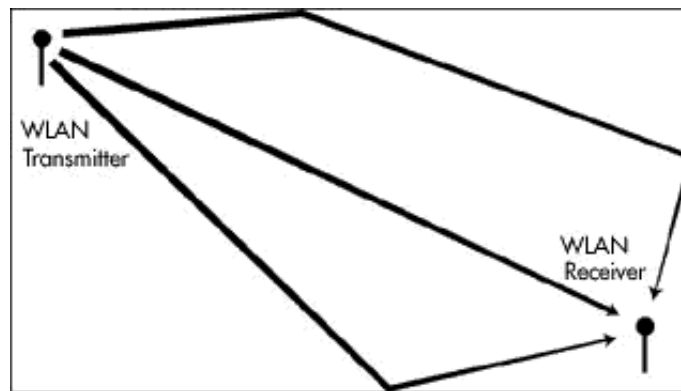
The distance over which RF waves can communicate is a function of product design (including transmitted power and receiver design) and the propagation path, especially in indoor environments. Interactions with typical building objects, including walls, metal, and even people, can affect how energy propagates, and thus what range and coverage a particular system achieves. Most wireless LAN systems use RF because radio waves can penetrate many indoor walls and surfaces. The range (or radius of coverage) for typical WLAN systems varies from under 100 feet to more than 500 feet. Coverage can be extended, and true freedom of mobility via roaming, provided through microcells.

#### **Throughput**

As with wired LAN systems, actual throughput in wireless LANs is dependent upon the product and how it is configured. Factors that affect throughput include airwave congestion (number of users), propagation factors such as range and multipath, the type of WLAN system used, as well as the latency and bottlenecks on the wired portions of the WLAN. Typical data rates range from 1 to 11 Mbps.

#### **Multipath Effects**

As Figure 9 shows, a radio signal can take multiple paths from a transmitter to a receiver, an attribute called multipath. Reflections of the signals can cause them to become stronger or weaker, which can affect data throughput. Affects of multipath depend on the number of reflective surfaces in the environment, the distance from the transmitter to the receiver, the product design and the radio technology.



**Figure 9. Radio Signals Traveling over Multiple Paths**

### **Integrity**

Wireless data technologies have been proven through more than fifty years of wireless application in both commercial and military systems. While radio interference can cause degradation in throughput, such interference is rare in the workplace. Robust designs of proven WLAN technology and the limited distance over which signals travel result in connections that are far more robust than cellular phone connections and provide data integrity performance equal to or better than wired networking.

### **Interoperability with Wired Infrastructure**

Most wireless LAN systems provide industry standard interconnection with wired systems including Ethernet (802.3) and Token Ring (802.5). Standards based interoperability makes the wireless portion of the network completely transparent to the rest of the network. Wireless LAN nodes are supported by network operating systems(NOS) in the same way any other LAN node via network device drivers. Once installed, the NOS treats the wireless nodes like any other component of the network.

### **Interoperability with Wireless Infrastructure**

There are several types of interoperability that are possible between wireless LANs. This will depend both on technology choice and on the specific vendor's implementation. Products from different vendors employing the same technology and the same implementation typically allow for the interchange of adapters and access points. An eventual goal of the IEEE 802.11 specification, currently being drafted by a committee of WLAN vendors and users, is to allow compliant products to interoperate without explicit collaboration between vendors.

### **Interference and Coexistence**

The unlicensed nature of radio-based wireless LANs means that other products that transmit energy in the same frequency spectrum can potentially provide some measure of interference to a WLAN system. Micro-wave ovens are a potential concern, but most WLAN manufacturers design their products to account for microwave interference. Another concern is the co-location of multiple WLAN systems. While co-located WLANs from different vendors may interfere with each other, others coexist without interference. This issue is best addressed directly with the appropriate vendors.

### **Simplicity/Ease of Use**

Users need very little new information to take advantage of wireless LANs. Because the wireless nature of a WLAN is transparent to a user's NOS, applications work the same as they do on tethered LANs. WLAN products incorporate a variety of diagnostic tools to address issues associated with the wireless elements of the system; however, products are designed so that most users rarely need these tools.

WLANs simplify many of the installation and configuration issues that plague network managers. Since only the access points of WLANs require cabling, network managers are freed from pulling cables for WLAN end users. Lack of cabling also makes moves, adds, and changes trivial operations on WLANs. Finally, the portable nature of WLANs lets network managers pre-configure and troubleshoot entire networks before installing them at remote locations. Once configured, WLANs can be moved from place to place with little or no modification.

### **Security**

Because wireless technology has roots in military applications, security has long been a design criterion for wireless devices. Security provisions are typically built into wireless LANs, making them more secure than most wired LANs. It is extremely difficult for unintended receivers (eavesdroppers) to listen in on wireless LAN traffic. Complex encryption techniques make it impossible for all but the

most sophisticated to gain unauthorized access to network traffic. In general, individual nodes must be security-enabled before they are allowed to participate in network traffic.

### Cost

A wireless LAN implementation includes both infrastructure costs for the wireless access points and user costs for the wireless LAN adapters. Infrastructure costs depend primarily on the number of access points deployed; access points range in price from \$800.00 to \$2,000.00. The number of access points typically depends on the required coverage region and/or the number and types of users to be serviced. The coverage area is proportional to the square of the product range.

Wireless LAN adapters are required for standard computer platforms, and range in price from \$200.00 to \$700.00. The cost of installing and maintaining a wireless LAN is generally lower than the cost of installing and maintaining a wired LAN for two reasons. First, a WLAN eliminates the direct costs of cabling and the labor associated with installing and repairing it. Second, because WLANs simplify moves, adds, and changes, they reduce the indirect costs of user downtime and administrative overhead.

### Scalability

Wireless networks can be designed to be extremely simple or quite complex. Wireless networks can support large numbers of nodes and/or large physical areas by adding access points to boost or extend coverage.

### Battery Life for Mobile Platforms

End-user wireless products are capable of being completely untethered, and run off the battery power from their host notebook or hand-held computer. WLAN vendors typically employ special design techniques to maximize the host computer's energy usage and battery life.

### Safety

The output power of wireless LAN systems is very low, much less than that of a hand-held cellular phone. Since radio waves fade rapidly over distance, very little exposure to RF energy is provided to those in the area of a wireless LAN system. Wireless LANs must meet stringent government and industry regulations for safety. No adverse health effects have ever been attributed to wireless LANs.

### WLAN Configurations

#### Independent WLANs

The simplest WLAN configuration is an independent (or peer-to-peer) WLAN that connects a set of PCs with wireless adapters. Any time two or more wireless adapters are within range of each other, they can set up an independent network (Figure 3). These on-demand networks typically require no administration or preconfiguration.

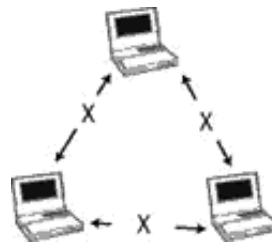
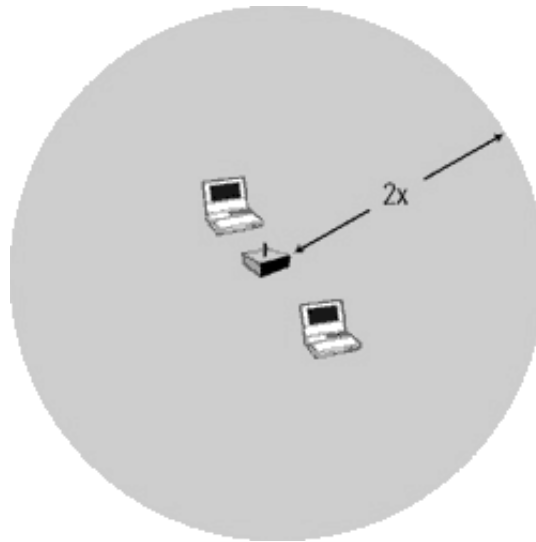


Figure 3.  
Independent WLAN

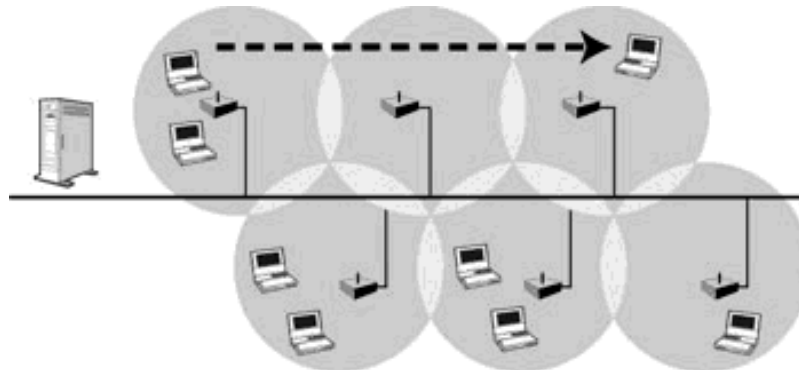
Access points can extend the range of independent WLANs by acting as a repeater (see Figure 4), effectively doubling the distance between wireless PCs.



**Figure 4. Extended-Range Independent WLAN Using Access Point as Repeater**

### Infrastructure WLANs

In infrastructure WLANs, multiple access points link the WLAN to the wired network and allow users to efficiently share network resources. The access points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood. Multiple access points can provide wireless coverage for an entire building or campus.



**Figure 5. Infrastructure WLAN**

### Microcells and Roaming

Wireless communication is limited by how far signals carry for given power output. WLANs use cells, called microcells, similar to the cellular telephone system to extend the range of wireless connectivity. At any point in time, a mobile PC equipped with a WLAN adapter is associated with a single access point and its microcell, or area of coverage. Individual microcells overlap to allow continuous communication within wired network. They handle low-power signals and hand off users as they roam through a given geographic area.



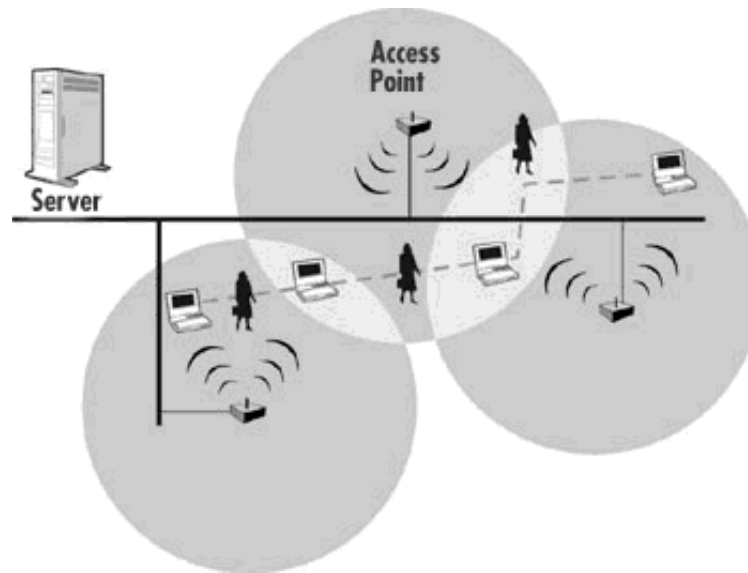


Figure 6. Handing off the WLAN Connection Between Access Points

### WLAN Glossary

#### Access Point

A device that transports data between a wireless network and a wired network (infrastructure).

#### IEEE 802.X

A set of specifications for Local Area Networks (LAN) from The Institute of Electrical and Electronic Engineers (IEEE). Most wired networks conform to 802.3, the specification for CSMA/CD based Ethernet networks. The 802.11 committee completed a standard for 1 and 2 Mbps wireless LANs in 1997 that has a single MAC layer for the following physical-layer technologies: Frequency Hopping Spread Spectrum, Direct Sequence Spread Spectrum, and Infrared. IEEE 802.11 HR, an 11 Mbps version of the standard is expected to be completed by the end of 1999.

#### Independent network

A network that provides (usually temporarily) peer-to-peer connectivity without relying on a complete network infrastructure.

#### Infrastructure network

A wireless network centered about an access point. In this environment, the access point not only provides communication with the wired network but also mediates wireless network traffic in the immediate neighborhood.

#### Microcell

A bounded physical space in which a number of wireless devices can communicate. Because it is possible to have overlapping cells as well as isolated cells, the boundaries of the cell are established by some rule or convention.

#### Multipath

The signal variation caused when radio signals take multiple paths from transmitter to receiver.

#### Radio Frequency (RF) Terms: GHz, MHz, Hz

The international unit for measuring frequency is Hertz (Hz), which is equivalent to the older unit of cycles per second. One Mega-Hertz (MHz) is one million Hertz. One Giga-Hertz (GHz) is one billion Hertz. For reference: the standard US electrical power frequency is 60 Hz, the AM broadcast radio frequency band is 0.55 -1.6 MHz, the FM broadcast radio frequency band is 88-108 MHz, and microwave ovens typically operate at 2.45 GHz.

#### Roaming

Movement of a wireless node between two microcells. Roaming usually occurs in infrastructure networks built around multiple access points.

#### Wireless Node

A user computer with a wireless network interface card (adapter).