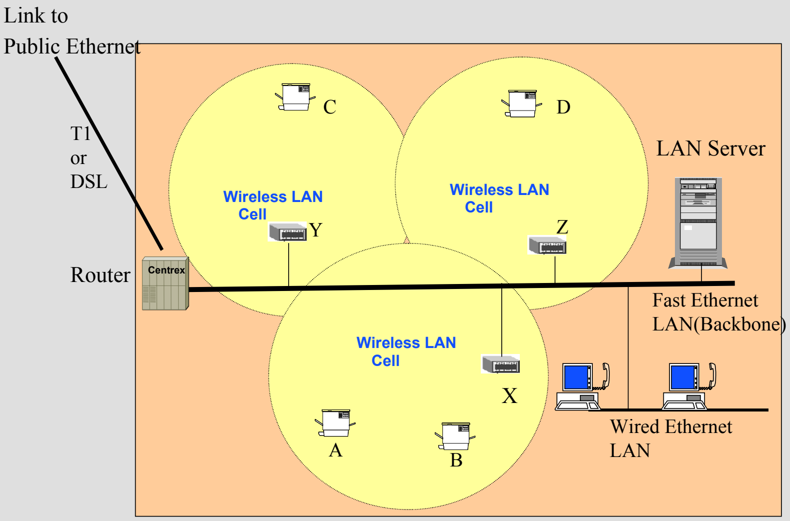
6 Wireless LANs – 802.11 and Mobile Ad Hoc Networks

Example: A Small Office Wireless LAN

The following figure shows a wireless LAN in a small office. The network consists of three cells, handled by access points X, Y, and Z. The access points (APs) are connected to a Fast Ethernet LAN that serves as a backbone and controls access to a LAN server. The backbone also connects to a few wired Ethernet LANs, and provides access to the public Ethernet through a router.

Wireless LANs with this type of configuration are commonly used in offices, universities, and SoHos (small offices, home offices). This type of wireless LAN allows users to access the Internet from laptops equipped with a wireless network card. Properly authorized laptops can also access the corporate databases and the wired LAN resources.



6.1 Introduction

Wireless LANs (WLANs) allow mobile devices in a small area (around 100 meters) to communicate with each other without using physical cables. The wireless LAN devices communicate with each other by using special cards that transmit and receive information over wireless media. In addition to flexibility for users, these LANs are relatively cheap because LAN wiring can be the most expensive component of a LAN. Large numbers of enterprise as well as domestic and hobbyist applications are being developed around wireless LANs. The WLAN market has continued to grow at a brisk pace since the late 1990s, despite a general industry slowdown. In particular, the IEEE 802.11 LANs, also known as the wireless Ethernet LANs, have been widely deployed in numerous offices and homes. In addition, many "hot spots," based on WLAN technologies, are becoming common in airports, shopping centers, coffee shops, and apartment buildings where a WLAN is set up for user access to the Internet and for email exchanges.

The first generation of WLAN products, such as Lucent's WaveLAN, provided data rates of about 1-2 Mbps – a factor of 10 slower than the traditional Ethernet. Most of the current generation of wireless LANs offer 10-11 Mbps (with some approaching 54 Mbps) – still a factor of 2 to 10 times slower than the 100 Mbps of wired Ethernet. Several attempts to standardize WLANs are underway. Examples are the IEEE 802.11 (for 11 to 54 Mbps) and the HiperLAN (for 54 Mbps). We will discuss IEEE 802.11 and HiperLAN later in this chapter. Bluetooth LANs, with data rates in the 700 Kbps to 1 Mbps range, will be discussed in the next chapter as part of the wireless personal area networks (WPANs) due to their short distance (10 meters).

Wireless LANs focus on local coverage – an important distinction from the corresponding wide area networking solutions that transmit data across broad coverage regions using either cellular or satellite technology. Wireless LANs operate under FCC rules similar to the rules for cordless telephones used in homes. Data transmission is free. Thus, as compared to wireless wide area networks, wireless LANs require no usage fees and provide a 100 to 1000 times faster data transmission rate. Wireless WANs such as cellular networks involve costly infrastructures, provide data rates in few Kbps, and require users to pay for bandwidth on a time or usage basis.

This chapter gives an overview of wireless LAN (WLAN) technologies with special attention to the IEEE 802.11 WLANs (also known as the wireless Ethernet LANs). As we will see, other standards such as Hiperlan2 are popular in Europe, and Bluetooth as well as HomeRF are supporting smaller LANs (discussed in the next chapter). Why are there different and competing standards in WLANs? Obviously, the basic problem that needs to be solved by any wireless standard is how to transport data via radio transmission in a way that is both secure and efficient, at a high data rate. However, standards have to keep up with changing requirements. Some standards change quickly, and new standards are introduced where the existing standards change too slowly or are not adequate. In addition, differences between countries, the NIH ("not invented here") syndrome, and the desire by companies to dominate market segments play an important role. Differences also arise due to diverse approaches to security, interoperability, reliability, management, and flexibility to migrate from the ***small office home office (SoHo)*** environment to an enterprise-class organization. In short, the differences in WLAN standards are driven by the same reasons as in other technical standards areas (no surprise!).

Chapter Highlights

- Wireless LANs are one of the fastest growing areas of wireless technologies due to their flexibility, lack of usage fees, and high data rates.
- Most wireless LANs are based on the spread-spectrum technology, although infrared and narrowband microwaves are also in use.
- Connectivity to wired networks is provided through an "access point" (AP) that can be connected to a wired LAN or to any other type of network for access to corporate databases and/or to the Internet. The mobile devices (e.g., laptops, wireless printers, headsets) connect to the AP when they are in the range of the AP – a cell that may span 10 to 100 meters. Once connected to the AP, the mobile devices can communicate with other devices in the cell or other resources through the AP.
- The IEEE 802 wireless LAN is by far the most commonly used WLAN standard that has been issued as several parts.
  - The first part, issued in 1997, is simply called 802.11 and operates at 1 and 2 Mbps.
  - The second part, issued in 1999, is called 802.11a and operates at data rates up to 54 Mbps.
  - The third part, also issued in 1999, is known as 802.11b and operates at data rates up to 11 Mbps.
  - The fourth part, the IEEE 802.11g, was introduced in 2002 and operates at 54 Mbps.
- At the time of this writing 802.11b, also known as Wi-Fi, is most popular in the 802.11 family but the faster 802.11g is steadily gaining ground.
- Mobile Ad Hoc Networks (MANETs) represent peer-to-peer networks in which new

devices can be quickly added or deleted on an as-needed basis. A MANET basically does not need an AP.

- HiperLAN2, developed by the European Telecommunications Standards Institute (ETSI), is mainly popular in Europe. The proponents claim that it is not merely a LAN solution but provides superior connectivity technology.

The Agenda
- Overview and Main Concepts
- IEEE 802.11 Wireless LANs
- Mobile Ad Hoc Networks and HiperLAN2

6.2 Wireless LAN Overview

6.2.1 Principles of Wireless LANs

Figure 6-1 shows a simple wireless LAN configuration. Each mobile device in the wireless LAN has a wireless LAN adapter (in fact a radio transmitter/receiver) that operates in certain frequency ranges. Connectivity to wired networks is provided through an "access point," also known as a local bridge. The access point (AP) can be connected to a wired LAN or to any other type of network for access to corporate databases and/or to the Internet. The mobile devices (e.g., laptops, wireless printers, headsets) connect to the AP when they are in the range of the AP – a cell that may span 10 to 100 meters. Once connected to the AP, the mobile devices can communicate with other devices in the cell or other resources through the AP.

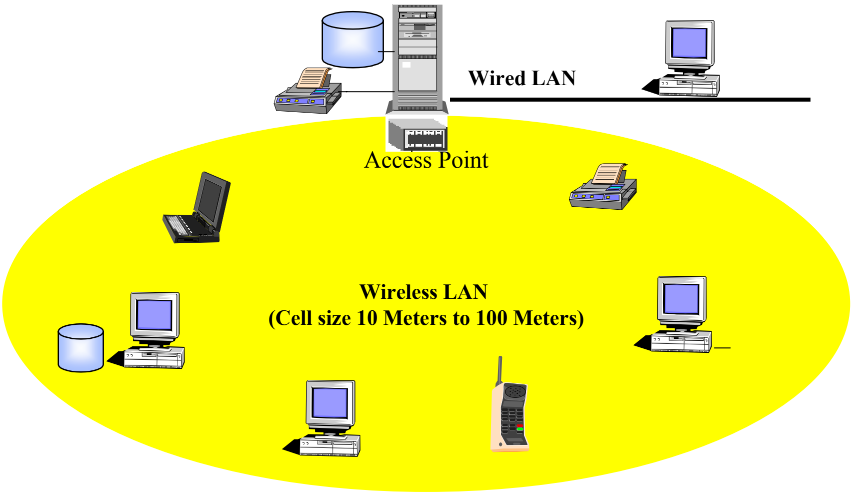


Figure 6-1: A Simple Wireless LAN Configuration

Wireless LANs augment rather than replace wired LAN networks – they support the final few meters of connectivity between a backbone network and the in-building or on-campus mobile user. The benefits of wireless LANs are:

- **Flexibility:** Wireless technology allows the users to roam around a building with their laptops. This is particularly useful for wireless Internet access. I, for example, sit in a presentation with my laptop and when the presenter discusses a web link, I display the site while the presenter is still talking about it (isn't technology just wonderful!).
- **Improvements in Productivity**: Wireless LANs can provide LAN users with access to real-time information anywhere in their organization. This improves productivity.
- **Installation Speed and Simplicity**: Wireless LANs can be installed quickly because they eliminate the need to pull cable through walls and ceilings.
- **Reduced Cost:** The initial investment required for wireless LAN hardware can be higher than the cost of wired LAN hardware. However, the overall installation expenses, especially in dynamic environments, are lower due to savings in cabling costs.
- **Scalability:** Wireless LANs can be configured in a variety of topologies to meet the needs of specific applications and installations.

Wireless LANs basically provide all the functionality of wired LANs, but without the physical constraints of the wire itself. Due to these benefits, numerous interesting applications of wireless LANs are possible. Examples of applications can be found in healthcare, manufacturing, car rental, airline, education, defense, restaurants, and many other industries. Sample applications include training sites and universities using wireless LAN connectivity to deliver instruction in any classroom in a building, and doctors and nurses in hospitals using hand-held or notebook computers with wireless LAN capability to deliver patient information instantly. Additional applications include car rental agents greeting the customers in parking lots for convenient car returns, trade show and branch office workers minimizing setup requirements by installing pre-configured wireless LANs, and restaurant waitresses and car rental service representatives providing faster service with real-time customer information input and retrieval.

The wireless LAN industry has grown at a notable rate of between 40 and 60% per year since the mid-1990s and is expected to keep growing at this rate in the future. There are several reasons for this growth. First, a widely accepted wireless LAN standard has been approved by the Institute of Electrical and Electronic Engineers (IEEE). In July 1997, the IEEE 802.11 committee, a subgroup with the IEEE, adopted a worldwide ISO standard for wireless LANs. Second, product prices have decreased dramatically over the past several years. Third, new wireless LAN applications are continually being adopted. Fourth, the mobile computing paradigm is being rapidly adopted by corporate users for office settings.

A wide range of WLAN products are now commercially available. A Wireless LAN Alliance (WLANA) has been formed as a consortium of wireless LAN vendors. WLANA provides ongoing education and promotional services about current applications of wireless local area networking and the future of the industry. The Wireless LAN Alliance web site (www.wlana.com) contains a wide range of information.

The main limitation of wireless LANs, as compared to the rival wired LANs, is the security risk of wireless LANs. Horror stories abound, about eavesdropping and connecting to WLANs just by being in their range. We will discuss wireless security in a later chapter. In addition, WLANs are slower. While wireless LANs are achieving 11 to 54 Mbps, the wired LANs such as fast Ethernet have been delivering 100 Mbps for a while. This factor needs to be considered while evaluating the tradeoffs between the two types of LANs. Interoperability, reliability and management is also important in competing with wired LANs. In particular, if a wireless LAN solution is to migrate from the small office home office (SoHo) environment to an enterprise-class organization, it must be robust and secure.

Table 6-1 shows characteristics of wireless LANs. For additional discussion and analysis of these characteristics, please visit the Wireless LAN Alliance website (http://www.wlana.com).

Table 6-1: Characteristics of Wireless LANs (Source: www.lana.com)

Security	Security provisions such as encryption are typically built into wireless LANs. The wireless LAN nodes must be security-enabled before they are allowed to participate in network traffic.
Interoperability	Interoperability can be defined at two levels: - Wireless to wired LANs/WANs. Industry-standard interconnections exist between wireless LANs and wired systems such as Ethernet (802.3) and Token Ring (802.5). - Wireless to wireless LANs IEEE 802.11 specifications allow compliant products to inter-operate without explicit collaboration between vendors.
Interference	Radio-based wireless LANs operate in unlicensed frequency ranges. Thus other products such as microwave ovens and other wireless LANs that transmit energy in the same frequency spectrum can potentially cause interference. Most wireless LAN vendors at present provide some safeguards against interference. This factor should be considered in LAN selection.
Cost	Cost of a wireless LAN implementation includes: - Wireless LAN adapter cost. Each Wireless LAN user must have an adapter, with price ranges from $50 to $100. . - Interconnectivity costs (also known as "infrastructure costs"). This cost depends primarily on the number of "access points" deployed. Access points range in price from $200 to $400. The access points act as repeaters in wireless LANs. The number of access points typically depends on the required coverage region and/or the number and type of users to be serviced (see the discussion on access points in sections on Wireless LAN technologies and configurations). - Installation and maintenance cost. This is generally lower than the cost of installing and maintaining a traditional wired LAN, due to savings in cable costs and the labor associated with installing and repairing cables.
Scalability	Wireless networks can support large numbers of nodes and/or large physical areas by adding access points to boost or extend coverage.
Battery	End-user wireless products are capable of being completely untethered, and run off the battery power from their host notebook or hand-held computer.

6.2.2 Wireless LAN Technologies at a Glance

Table 6-2 displays the highlights of wireless LANs in terms of data rates, distance covered, target applications, frequency allocation, location management, and physical communications. We will use this framework to capture the salient features of all wireless networks as we go along.

6.2.2.1 Data Rates and Distance Covered

WLAN data rates typically range from 11 to 54 Mbps. The data rates could be affected by airwave congestion (number of users), range, and the type of WLAN system used, as well as the latency and bottlenecks on the wired portions of the WLAN.

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 is around 100 100 meters. Coverage can be extended and roaming can be supported through microcells and bridges.

6.2.2.2 Target Applications

The applications targeted for WLANs are mostly data applications for offices and home networking situations. Thus WLANs are used commonly for emails, Web browsing, and corporate applications/data access. However, many new voice over 802.11 systems from companies such as Cisco are currently becoming available.

6.2.2.3 Frequency Allocations

WLANs mostly use unregulated bands. For example, 802.11 uses the ISM band. The use of unregulated bands has two major implications: a) the users do not have to pay a usage fee, and b) greater interference from other devices that also use these bands is possible.

6.2.2.4 Location Management

Due to the relatively short communication distances covered by WLANs, the senders and receivers do not travel far from each other. WLAN users typically sit in a spot and walk around in offices or homes. This is quite different from cellular phone users who use the cellular phone while travelling in cars and trains. Thus extensive location management is not needed in WLANs.

6.2.2.5 Physical Communications

Many serious problems must be faced at the physical communication (layer 1 and 2) by WLANs. First, multiple access mechanisms is important because contention and interference from other devices can be high. One of the main reasons is that WLANs typically operate in unregulated frequency bands which are very crowded. For example, 802.11 LANs (especially the very popular 802.11b and 802.11g) operate in the same band (ISM at 2.4 GHz) as Bluetooth. The techniques used are mainly based on spread spectrum (FHSS or DSSS). As discussed in Chapter 5, spread spectrum sends signals in such a fashion that only the receiver with the right code can understand it – the others receive a noise. This reduces the interference. In addition, forward error correction (FEC) and ARQ is used for handling errors and a combination of PSK and FSK are used for modulation.

Table 6-2: Basic Information about WLANs

Factor	Key Points
Data rate and Distance covered	11 to 54 Mbps data rate over a range of about 100 meters.
Target Applications	Mostly data applications in LAN settings, Currently, voice over 802.11 is becoming popular.
Frequency Allocations	Mostly in unregulated bands (ISM band is common)
Location Management	Extensive location management is not needed because the users do not move around very much.
Physical Communications, Signal Encoding, Error Correction	Mainly spread spectrum: FHSS or DSSS Forward error correction, a combination of PSK and .FSK. .

6.2.3 Wireless LAN Applications and Requirements

Figure 6-2 shows some possible applications of wireless LANs in corporations. This figure shows how wireless LANs can be used to extend wired LANs, provide nomadic access for roaming users, and support ad hoc networking. In building 1, there are two wireless LANs that are linked into a wired LAN through access points. This is an example of ***LAN Extension***. In LAN extensions, the wired LAN is used for backbone that interconnects several wireless LAN stations in large open areas such as a classroom or office. A nomadic station (e.g., a laptop) can connect to wireless LAN1 or wireless LAN2. This, known as ***Nomadic Access,*** provides wireless links between a LAN hub and mobile stations equipped with antennas.

One of the wireless LANs (LAN1) uses ***Ad Hoc Networking***, which allows mobile devices to talk to each other without the need for an access point. In this configuration, temporary peer-to-peer networks are set up to meet immediate customer needs. For example, an ad hoc network can link computers as a temporary network just for the duration of a meeting. The other wireless LAN (LAN2) uses a ***Master/Slave***, also known as ***Centralized***, LAN configuration. In this case, the devices communicate with each other through a master (an access point in this case). The Wireless LANs can also be used for ***Cross-building Interconnection***: Wireless LANs connect LANs in nearby buildings (in our case between building 1 and 2) by using point-to-point wireless. The devices connected are typically bridges or routers on top of buildings.

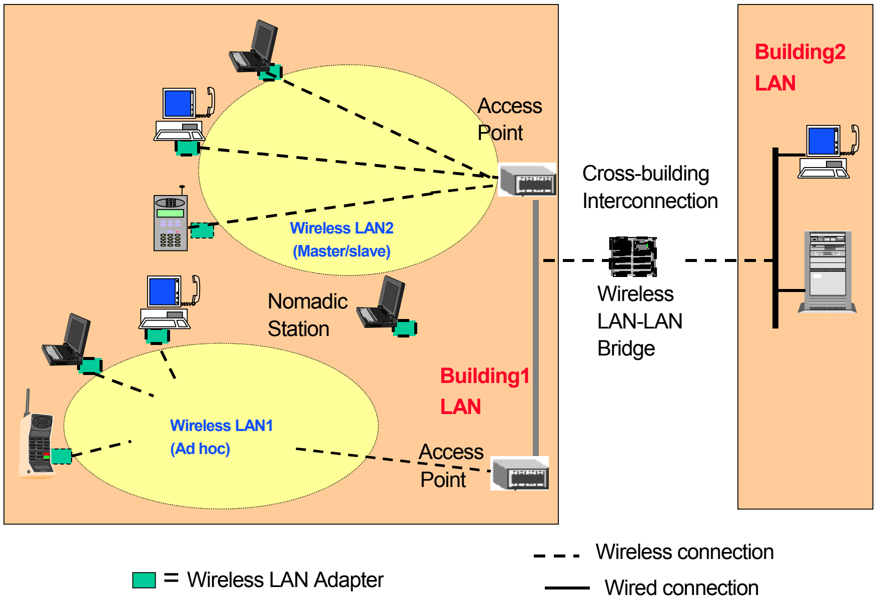


Figure 6-2:; LAN Applications

To support these and other applications, a wireless network needs to satisfy a wide range of requirements such as the following:

- Connection to backbone LANs must be supported for corporate use. Basically the wireless LAN must be able to connect to a backbone network to provide value.
- Service area for mobile devices should be 100+ meters.
- Battery power consumption should be minimized; i.e., the user devices should go to sleep when not in use.
- Throughput needs to be high; i.e., more work needs to be completed per unit time.
- Transmission robustness and security – i.e., reliable transmission and maintenance of security – are naturally important.
- Collocated network operation must be supported by minimizing interference between neighboring networks.

- License-free operation should be supported because it is better to operate without licensed frequencies.
- Handoff/roaming and dynamic configurations must be supported. Medium access control (MAC) layer is responsible for these features; i.e., MAC protocol should support smooth handoffs and MAC addressing should support automatic addition and deletion of addresses.

6.2.4 Wireless LAN Technologies

Figure 6-3 shows the key wireless technologies: LAN adapters, access points, and wireless communication technologies.

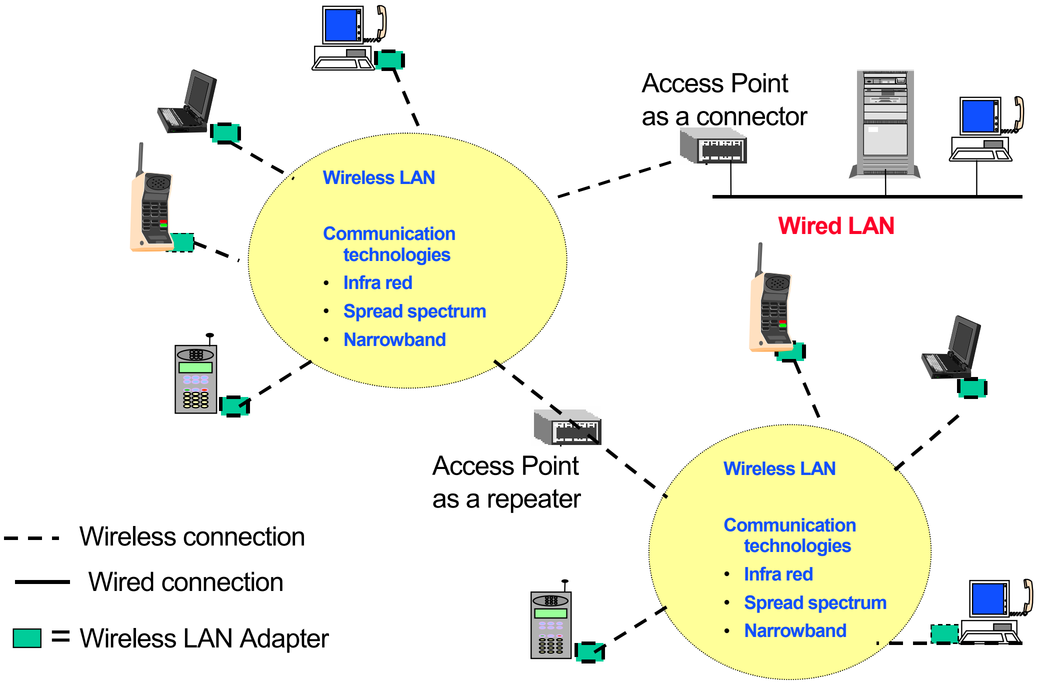


Figure 6-3: Wireless LAN Technologies

6.2.4.1 Wireless LAN Adapters

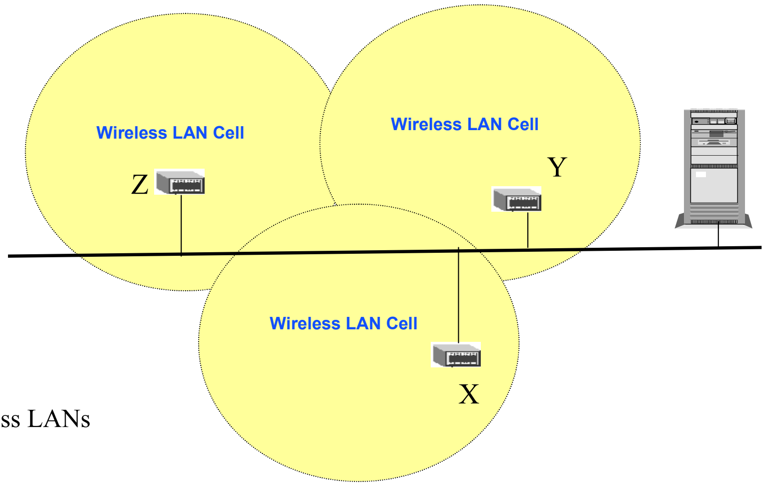
End users access WLANs through wireless LAN adapters, which are implemented as PC cards in laptops, or use appropriate adapters in desktop computers, or fully integrated devices within handheld computers. Wireless LAN adapters are in fact miniature transceivers that provide an interface between the client network operating system (NOS) and the airwaves via an omnidirectional antenna. The nature of the wireless connection is transparent to the NOS.

6.2.4.2 Access Points

An access point is a transmitter/receiver (transceiver) device that connects wireless LANs to other wired or wireless networks by using a omnidirectional antenna. It performs two functions: a) it acts as a repeater between two wireless LANs, and b) it acts as a connector (bridge) between wired and wireless networks. For example, an access point can connect your wireless LAN to an Ethernet network from a fixed location using standard Ethernet cable. It can also act as a repeater between two wireless LANs, thus increasing the area covered – it effectively doubles the distance between wireless PCs. The access point receives, buffers, and transmits data between the wireless LAN and the wired/wireless networks by using omni-directional antennas. 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. For wider radio coverage, the access point (or the antenna attached to the access point) is usually mounted high. An example of access points is the Cisco Aironet 340 AP (visit the Cisco site, http://www.cisco.com/ for detailed specification). See the wireless LAN configuration discussion for more information on access points.

6.2.4.3 Microcells and Roaming

Wireless communication is limited by how far signals carry for a given power output. Wireless LANs 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 wireless LAN adapter is associated with a single access point and its microcell, or area of coverage. Individual microcells overlap to allow continuous communication within a wired network. They handle low-power signals and "hand off" users as they roam through a given geographic area. Figure 6-4 illustrates microcells in a wireless LAN environment.



X, Y, Z are
access points
for the wireless LANs

Figure 6-4: Microcells and Roaming in a Wireless LAN Environment

6.2.5 Wireless Communication Technologies

Wireless LANs use electromagnetic airwaves (typically radio) to communicate between LAN users without relying on any physical connection**.** The data being transmitted is modulated/demodulated on the radio waves (see the sidebar "Modulation/Demodulation for Wireless LANs"). Currently available wireless LANs use one of three signal types to transmit data:

- spread spectrum (most commonly used)
- narrowband microwave
- infrared

In addition, carrier-current LANs, based on existing power lines, are also being used.

6.2.5.1 Spread-Spectrum Wireless LANs

Spread spectrum is most widely used in wireless LANs. These LANs transmit in the ***industrial, scientific, and medical (ISM)*** bands designated by the FCC. These bands, around 2.4 GHz, are not regulated so the LAN suppliers have to worry about preventing interference.

This technology was developed for military and intelligence operations (the message is “spread” over a range of frequencies to make it jam-resistant).

Spread-spectrum technology, as discussed in a previous chapter, is a wideband radio frequency technique that basically transmits different data bits on different signals, based on a secret scheme, for secure communications. The receiver must know the parameters of the spread-spectrum signal being broadcast to understand the signal. If a receiver is not tuned to the right frequency, a spread-spectrum signal looks like background noise. In spread-spectrum systems, more bandwidth is consumed than in the case of narrowband transmission, but the tradeoff produces a signal that is secure and louder. There are two types of spread-spectrum radio: frequency-hopping and direct sequence.

- **Frequency-hopping spread spectrum (FHSS)** uses a narrowband carrier that changes frequency in a pattern known to both transmitter and receiver. For example, the transmitter can transmit 8 bits of data at frequency f1, send the next 12 bits at frequency f2, the next 16 bits at f3, and then back to 8 bits at f1. To an unintended receiver, FHSS appears to be short-duration impulse noise. Wireless LANs such as Bluetooth use FHSS.
- **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. The IEEE 802.11 Wireless Ethernet LAN uses DSSS as well as FHSS.

Spread-spectrum LANs are organized around multiple-cell arrangements where within a cell, either peer-to-peer or hub architectures are used. In peer-to-peer topology, no hub is used. Due to this, access is controlled by typical shared access MAC algorithms such as CSMA. These LANs are appropriate for ad hoc LANs. Hub topology, also known as master-slave topology, supports an access point, typically mounted on the ceiling, that is connected to the backbone. Hubs may control access and/or serve as multiport repeaters. They can support automatic handoff of mobile stations. Stations in a cell either transmit to / receive from hub only, or broadcast using omnidirectional antennas.

6.2.5.2 Narrowband Microwave

Wireless LANs based on **narrowband microwave** technology use the 18.82-to-18.87 GHz and 19.6-to-19.21 GHz frequency ranges. These frequency ranges are licensed by the FCC, which means that a vendor must be approved by the agency to use these frequency ranges. Many wireless LAN vendors consider this to be a restriction. 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 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.

Narrowband Microwave LANs use a microwave radio frequency band for signal transmission. These bands have relatively narrow bandwidth and are licensed within specific geographic areas to avoid potential interference. These frequencies are “owned” by various suppliers. For example, Motorola holds 600 licenses in the 18 GHz range. These frequencies cover all metropolitan areas. The main advantage of licensed microwave LANs is that by paying for a license, you are assured that LANs in nearby locations do not interfere with your frequencies. In addition, encrypted transmissions prevent eavesdropping. Unlicensed narrowband microwave LANs use unlicensed ISM spectrum. An early example is the RadioLAN narrowband wireless LAN in 1995 that used low power (0.5 watts or less) within a range of 50 to 100 meters. These LANs operate at 10 Mbps in the 5.8 GHz band.

6.2.5.3 Infrared (IR) Wireless LANs

Infrared signals operate at very high frequencies (300 GHz and above) and behave like ordinary light (they cannot penetrate solid objects). Thus infrared wireless LANs are limited to data transmission along line of sight. Infrared technology is simple and well proven (it is used commonly in remote controls for VCRs and TVs). In addition, infrared signals are not regulated by the Federal Communications Commission (FCC). Technically, 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 (reflective) technology. Inexpensive directed systems provide very limited range (3 to 5 ft.) and typically are used for personal area networks (PANs) such as appliances in the kitchens of the future. High-performance directed IR is impractical for mobile users due to potential obstacles and is therefore used primarily to implement fixed subnetworks. Diffuse (or reflective) IR WLAN systems do not require line-of-sight (you use reflectors such as mirrors). However, you cannot make magic with mirrors too long, thus cells are limited to individual rooms.

In general, the following IR data transmission techniques are used:

- **Directed Beam Infrared** is used to create point-to-point links between wireless nodes. The range depends on emitted power and degree of focusing of the transceiver. A focused IR data link can have a range of kilometers that is not needed for indoor LANs but could be readily used for cross-building interconnection.
- **Ominidirectional Transmission** is used for single base stations in line of sight of all other stations on LAN. The base station transmits in all directions and is typically mounted on a ceiling. The ceiling transmitter broadcasts signals in all directions. This signal is received by IR transceivers and is transmitted back the the IR transceivers. Omnidirectional IR technology is used in the IEEE802.11 LANs.
- **Diffused Infrared**: All IR transmitters are focused and aimed at a point on a diffusely reflecting ceiling. IR radiation strikes the ceiling, is re-radiated omnidirectionally and is picked up by all receivers.

Infrared LANs have several strengths such as the following:

- The spectrum for infrared is virtually unlimited and unused above 300 GHz, thus the possibility of high data rates exists.
- Infrared spectrum is unregulated, thus there is no need to file for licenses.
- Infrared equipment is inexpensive and simple.
- Infrared waves are reflected by light-colored objects, thus ceiling reflection can provide coverage for an entire room.
- Infrared waves do not penetrate walls. Thus infrared LANs are more easily secured against eavesdropping and there is less interference between different rooms.

Drawbacks of infrared LANs are:

- Indoor environments experience infrared background radiation that creates noise.
- Sunlight and indoor lighting also creates background noise.
- Ambient radiation appears as noise.
- Transmitters of higher power are required but are limited by eye safety concerns.

6.2.5.4 Carrier-Current LANs – Powerline LANs

An interesting development not commonly discussed under wireless LANs is the carrier-current LANs (pseudo wireless LANs). These LANs do not require installation of network cables because they use power cables and a powerline modem. These LANs, still under development at the time of this writing, can be used to carry 1 to 2 Mbps of data. An example is the Radioshack Master Console to control coffee machine, lamps, and heating systems. We will look at these LANs in Chapter 10.

6.2.6 Wireless LAN Configurations

Wireless LANs can be intermixed and configured with disparate networks in different locations of an organization for ease of access. These LANs can be configured as point-to-point LANs, peer-to-peer LANs, master-slave LANs, and LANs connected through bridges and access points. Figure 6-5 shows the main configurations.

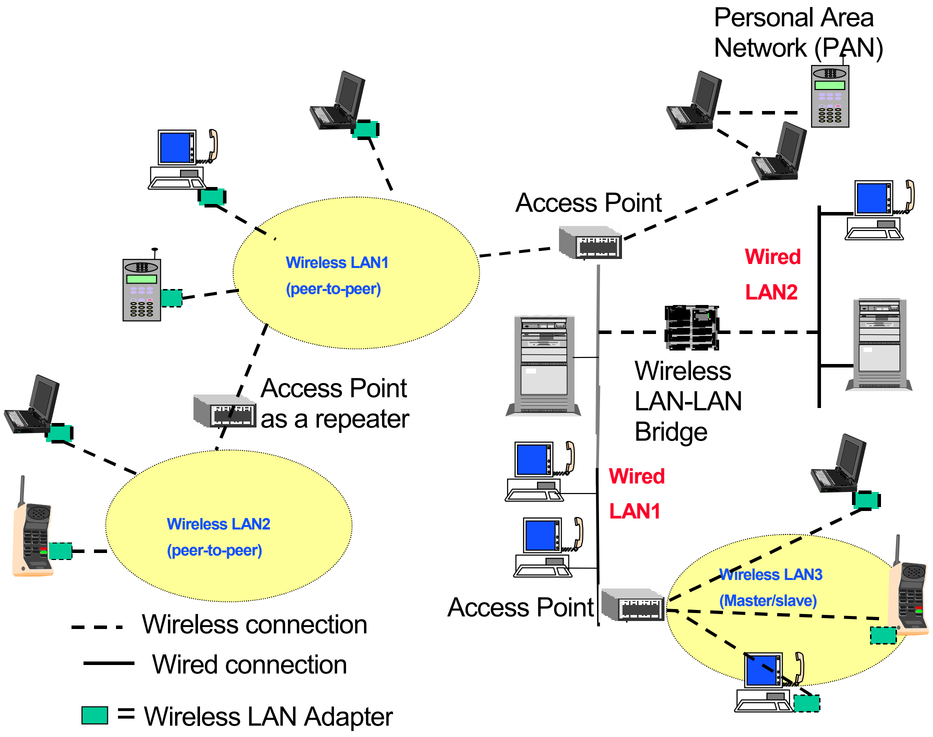


Figure 6-5: Wireless Configurations in an Enterprise

Point-to-point local area wireless solutions provide direct wireless links between participating devices. For example, directed beam infrared LANs, discussed previously, create point-to-point links between wireless nodes. Many examples of point-to-point wireless LAN solutions can be found in personal area networks (PANs). **Wreless PANs (WPANs)** typically cover the few feet surrounding a user's workspace and provide the ability to synchronize computers, transfer files, and gain access to local peripherals. Bluetooth can be thought of as a wireless PAN (not everyone agrees with this view). Figure 6-5 shows a WPAN.

Peer-to-Peer wireless LANs, also known as ad hoc or independent wireless LANs, are the simplest WLAN configurations. These wireless LANs connect a set of PCs with wireless adapters. Any time two or more wireless adapters are within range of each other, they can set up a peer-to-peer network. These on-demand networks typically require no administration or pre-configuration. Communications are established between multiple stations in a given coverage area without the use of an access point or server. Standards for peer-to-peer LANs specify the protocols that each station must observe so that they all have fair access to the wireless media. They provide methods for arbitrating requests to use the media to ensure that throughput is maximized for all of the users in the base service set. Wireless LAN1 and LAN2 in Figure 6-5 are examples of peer-to-peer LANs. Section 6.4 gives a closer look at ad-hoc LANs.

A **Master/slave** (also known as client/server) network uses an access point that controls the allocation of transmission time for all stations and allows mobile stations to roam from cell to cell. The access point is used to handle traffic from the mobile radio to the wired or wireless backbone of the client/server network. This arrangement allows for point coordination of all of the stations in the basic service area and ensures proper handling of the data traffic. The access point routes data between the stations and other wireless stations or to and from the network server. Typically WLANs controlled by a central access point will provide better throughput performance. LAN3 in Figure 6-5 is an example of a master/slave wireless LAN.

In addition to controlling a wireless LAN, access points can extend the range of independent wireless LANs by acting as repeaters (see Figure 6-5). This effectively doubles the distance between wireless PCs. Multiple access points can link the wireless LANs to the wired network and allow users to efficiently share network resources such as file servers and fast printers. 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 6-5 shows various uses of access points.

A wireless ***LAN-LAN bridge*** is an alternative to cable that connects LANs in two separate buildings. Building-to-Building or LAN-LAN wireless bridges are being used by many industries because you do not have to install and maintain cables between buildings. Wireless LAN-LAN bridging products are available from companies such as Cisco, ELAN, and Wireless Central. The wireless LAN-LAN bridge shown in Figure 6-5 interconnects two LANs in two different buildings.

6.2.7 The Wireless LAN Stack

The LAN standards for wired and wireless LANs have been developed by the IEEE 802 Committee. However, some popular LANs such as Bluetooth have been developed by industries. The Committee is organized into the following subcommittees (the number identifies the committee that defines a standard):

- 802.1: High Level Interface
- 802.2: Logical Link Control
- 802.3: CSMA/CD Networks
- 802.4: Token Bus Networks
- 802.5: Token Ring Networks
- 802.6: Metropolitan Area Networks
- 802.7: Broadband Networks
- 802.8: Fiber Optic Networks
- 802.9: Integrated Data and Voice Networks
- 802.10 Virtual LANs
- **802.11 Wireless LANs**

- 802.12 Communication media\
- 802.14 Data transport over traditional cable TV network
- 802.15 Personal Area Networks
- 802.16 Wireless Local Loops

Each subcommittee is responsible for developing standards in its designated area, and the published standards are associated with the subcommittee title. For example, the IEEE 802.11 standard for wireless Ethernet was developed by the subcommittee 802.11. Figure 6-6 shows protocol layered views of a WAN and a LAN. For LANs, layer 2 has been divided into two sublayers: Medium Access Control (MAC) and Logical Link Control (LLC).

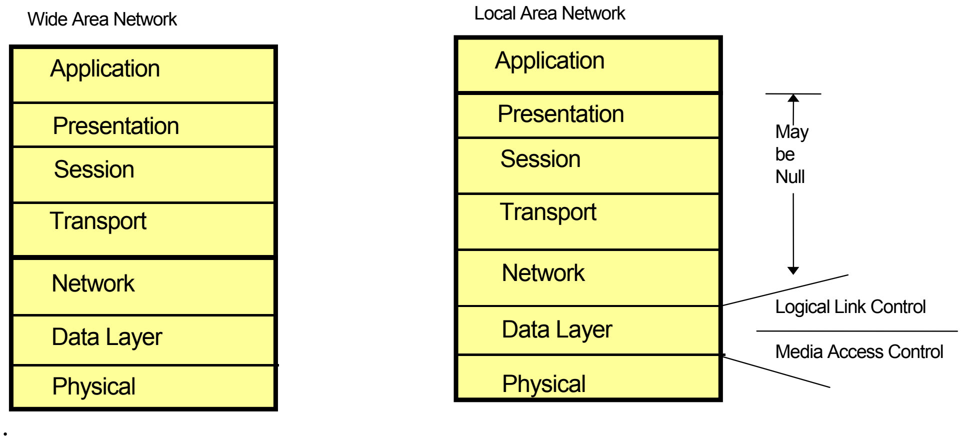


Figure 6-6: Protocol Stacks for Wide and Local Area Standards

The **MAC layer** controls the I/O to the physical layer entities. On transmission, this layer assembles the data into a frame with address and error-detection fields. On reception, it disassembles the arriving frame, and performs address recognition and error-detection. This layer also manages the communication over a physical medium such as fiber optics cables.

The **Logical Link Control** layer is responsible for the transfer and formatting of data needed by applications. It basically makes sure that a frame received by the MAC layer is passed to the appropriate application in a station. LLC provides one or more service access points (SAPs) for the applications to interface directly with the LAN.

In some cases, it is conceptually easier to think of MAC and LLC layers performing functions that are similar to IP and TCP, respectively. In effect, LLC interfaces with applications in a manner somewhat similar to TCP, while MAC is responsible for delivering messages over the physical LAN media and is similar to IP. The main difference is that LLC-MAC is intended for LANs while TCP-IP is designed for WANs.

Figure 6-7 shows another view of the stack and illustrates how the wireless LAN standard fits with other LAN standards.

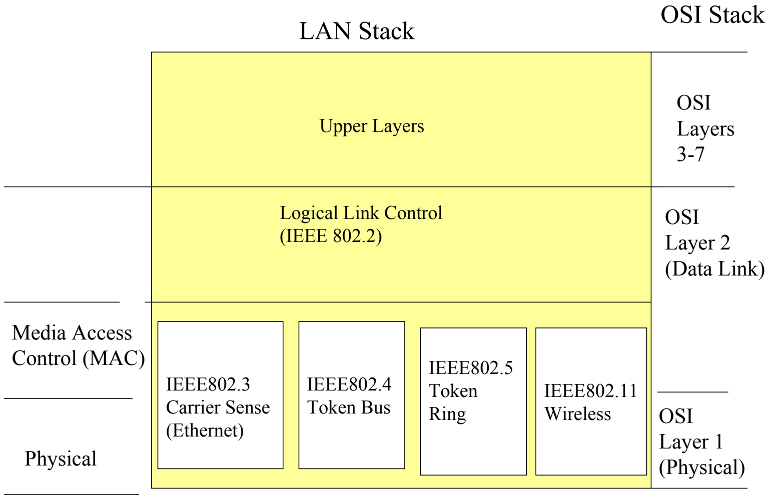


Figure 6-7: Wireless LAN Stack

Time to Take a Break

- ✓ Overview and Main Concepts
- IEEE 802.11 Wireless LANs
- Mobile Ad Hoc Networks and HiperLAN2

6.3 IEEE 802.11 Ethernet Standard for Wireless LANs

6.3.1 Overview

The IEEE 802 standards committee formed the 802.11 Wireless Local Area Networks Standards Working Group in 1990. The standard has been issued in several stages. The first part, issued in 1997, is simply called 802.11 and operates at 1 and 2 Mbps. The second part, issued in 1999, is called 802.11a and operates at data rates up to 54 Mbps. The third part, also issued in 1999, is known as 802.11b and operates at data rates up to 11 Mbps. The IEEE 802.11g was introduced in 2002 and operates at 54 Mbps. The following table summarizes the main players in the IEEE 802.11 standard family.

Table 6-3: Popular IEEE 802.11 LANs

IEEE 802.11 Type	Characteristics
802.11	Three specifications introduced in 1997 - 1 or 2 Mbps in the 2.4 GHz zone using FHSS - 1 or 2 Mbps in the 2.4 GHz zone using DSSS - 1 or 2 Mbps in the Infrared zone

802.11a	Up to 54 Mbps in the 5 GHz zone using Orthogonal FDM (introduced in 1999)
802.11b	Up to 11 Mbps in the 2.4 GHz zone using DSSS (introduced in 1999)
802.11g	54 Mbps and higher in the 2.4 GHz zone using OFDM (Introduced in 2002)

At the time of this writing, 802.11b is very popular although 802.11g is gaining ground steadily. 802.11b, also known as ***Wi-Fi*** (abbreviated from wireless fidelity), supports up to 11 Mbps data rates and provides great vendor interoperability. Thus it competes with the wired Ethernet LANs. You can find Wi-Fi LANs in offices, universities, hotel lobbies, apartment buildings, and "hot spots" at airports and shopping malls. The IEEE802.11b LANs operate in a manner very similar to the wired Ethernet LANs. Of course, there are no cables – the data packets are sent over radio waves. These LANs use the 2.2-to-2.4835 GHz band – the ISM (Industrial, Scientific, and Medical) unlicensed bandwidth reserved for short-range, low-power devices. As stated previously, a government license is not required to use the devices or the radio transmitter, or to operate other equipment in this frequency range.

How do they work? The 802.11b LANs are standardized around the direct-sequence spread-spectrum (DSSS) radio signals. This scheme divides the frequency spectrum into 14 slightly overlapping channels, each 22 MHz wide. So, if each wireless LAN is configured to use one channel, then an office building or a high school can operate 14 wireless LANs in the same physical space. The transmitters in each channel "spread" their signals on the entire 22 MHz bandwidth to improve reception. To discuss how the 802.11b LANs (in fact, all 802.11 LANs) work, let us look at the sample environment shown in Figure 6-8. This environment, commonly found in several small offices, shows several wireless LANs that are connected to a wired LAN to allow the students to access the LAN server as well as the public Internet. The steps in operating this environment are:

- Each access point (AP) is assigned a frequency within the ISM band. The APs X, Y, and Z may be assigned, say, channel 1, 2, and 3 (each 22 MHz). Eleven more APs could be allocated the remaining 11 channels in the same office.
- Each user laptop has an 802.11b card that can send and receive signals in the ISM band. These laptops can thus receive a signal at channel 1 through 14.
- Laptop A and B are in the vicinity of X and thus detect and transmit at signals in channel 1. Similarly, laptop C operates in channel 2 and D in channel 3.
- If laptop A moves from one cell to another (say from X to Y), then its card recognizes a stronger signal in channel 2 and starts listening now to channel 2. This is how the PCs switch from one AP to another.
- Since all 802.11b cards can send and receive information in the ISM band, then theoretically one laptop can establish a connection with any AP by just moving into its range. This presents a serious security problem and requires special approaches such as authentication at AP or encryption (we will discuss security later).

How is interference handled in 802.11b LANs? Wireless Ethernet turns each bit into a pattern of eight radio signals called a "chip." To achieve high throughput, the transmitters send 64 chips together in one burst. Even if most of the signals are distorted, typically enough will get through to help the receiver assemble an unambiguous result. If there is too much interference, then the receiver asks the transmitter to resend the entire message. If there are too many retries, the receiver may ask the sender to transmit at a lower rate (e.g., 5.5 Mbps or even 1 Mbps). This extra overhead of error checking reduces the effective data rate of wireless Ethernet from 11 Mbps to 10 Mbps (recall that 10 Mbps is the data rate of a wired Ethernet LAN). An attractive feature of 802.11b wireless Ethernet is that about 100 users can be supported on one channel (i.e., each wireless cell can support up to 100 users.

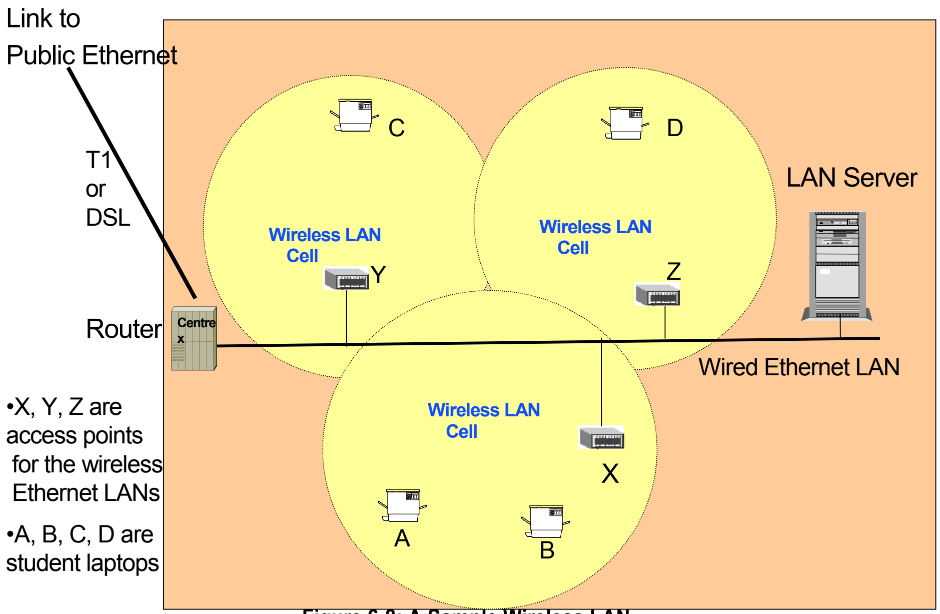


Figure 6-8: A Sample Wireless LAN

The IEEE 802.11a standard operates in the 5 GHz band and can go up to 54 Mbps. This standard directly competes with the newer 802.11g standard that can also deliver 54 Mbps. We will compare and contrast 802.11a and 802.11g in Section 6.3.3.4.

Security provisions in 802.11 are addressed in the standard by a complex encryption technique know as the ***Wired Equivalent Privacy Algorithm (WEP).*** WEP protects transmitted data over the RF medium by using a 64-bit seed key and the RC4 encryption algorithm. WEP only protects the data packet information and does not protect the physical layer header. Thus other stations on the network can listen to the control data needed to manage the network but they cannot decrypt the data portions of the packet.

Power management is supported at the MAC level for battery operation. Portable stations go to low power “sleep” mode during a time interval defined by the base station.

In many environments, the IEEE802.11b LANs are ideal. But still some problems need to be addressed. Roaming support is a major problem because handoffs from one access point to the next are not clean. While the standards bodies are working on refining the roaming specifications, the wireless LAN users are mostly restricted to desktops and notebooks but not handheld devices. At the time of this writing, Bluetooth and wireless Ethernet LANs (especially 802.11b) are incompatible but share the same 2.4 GHz band.

6.3.2 A Closer Look at IEEE 802.11

6.3.2.1 General LAN Protocol Architecture

As stated previously, the protocol architecture concentrates on the first 2 layers, which have been subdivided into the following 3 sublayers (see Figure 6-9):

- **Logical link control (LLC)** provides an interface to higher layers, through service access points (SAPs), and performs flow and error control.
- **Medium access control (MAC)** governs access to the LAN transmission medium and plays a central role in wireless transmissions. This layer is responsible for dealing with ad hoc or master-slave LANs and handoffs between cells as wireless users move from one

cell to another. On transmission, MAC assembles data into a frame with address and error detection fields; on reception, it disassembles the frame and performs address recognition and error detection.

- The **physical layer** deals with the wireless transmission medium and includes specification of the transmission medium. It is responsible for encoding/decoding of signals (e.g., modulation), preamble generation/removal (for synchronization), and bit transmission/reception over the wireless medium.

We will take a closer look at these layers later on in this section.

The IEEE 802.11 specification, like other specifications, is loaded with intricate technical information and uses somewhat new terminology. Simplified versions of the key terms used in the 802.11 standard are:

- ***Station.*** Any device that contains an IEEE 802.11-conformant MAC and physical layer
- ***Access point (AP).*** A station that provides access to the distribution system
- ***Basic service set (BSS)*** A collection of stations (a cell) competing for access to a shared wireless medium. A BSS is isolated or connected to the backbone DS through an AP.
- ***Distribution system (DS).*** A system that interconnects several BSSs
- ***Extended service set (ESS).*** Two or more basic service sets interconnected by DS

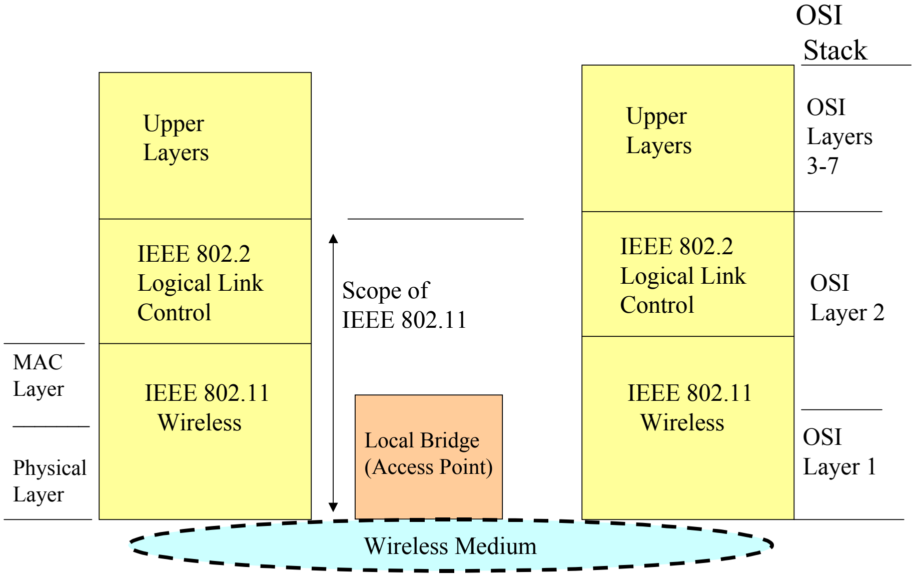


Figure 6-9: IEEE 802.11 Stack

Figure 6-10 shows the sample wireless school we described earlier by using IEEE 802.11 terms.

6.3.2.2 IEEE 802.11 Services

Figure 6-11 shows a more detailed view of the 802.11 Protocol Architecture that can be used to highlight the 802.11 services. The architecture subdivides the MAC layer into a Distributed Coordination Function (required) that is useful in ad hoc networks, and a Point Coordination Function (optional), that is suitable for a centralized (master/slave) LAN. The architecture also shows the stages of the 802.11 physical layer: 802.11, 802.11a, 802.11b, and 802.11g. As can be seen, the physical layer supports data rates that range from 1 Mbps to 54 Mbps. Note that the MAC and LLC layers are the same whether you support 802.11, 802.11a, 802.11b, or 802.11g.

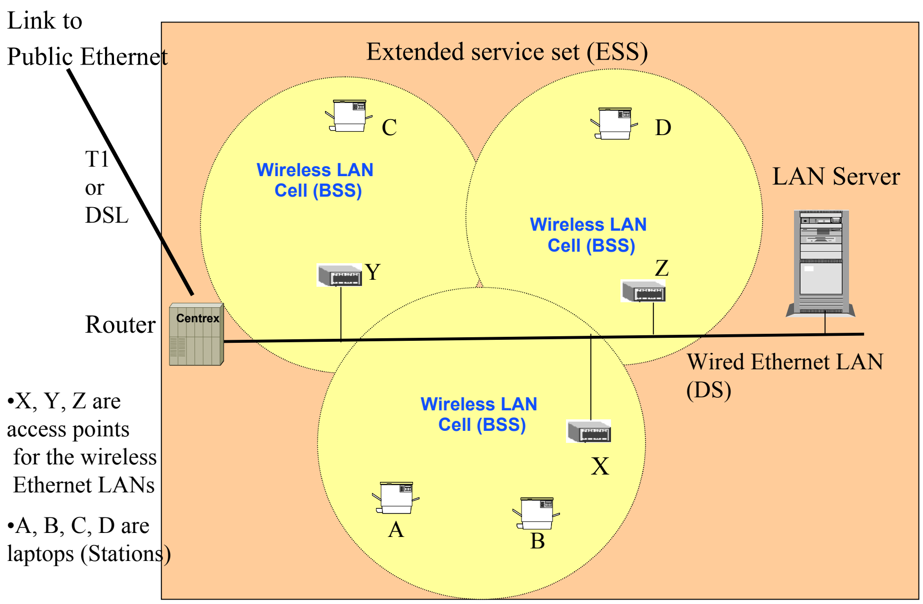


Figure 6-10: Sample Wireless School – IEEE 802.11 Terms

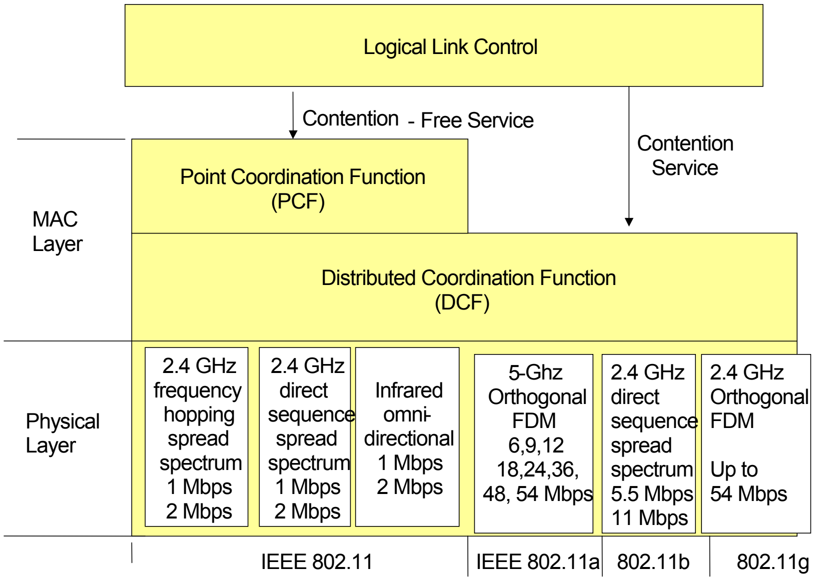

Logical Link Control
Contention - Free Service
Contention
Service
MAC
Layer
Point Coordination Function
(PCF)
Distributed Coordination Function
(DCF)
Physical
Layer
2.4 GHz frequency hopping spread spectrum 1 Mbps 2 Mbps
2.4 GHz direct sequence spread spectrum 1 Mbps 2 Mbps
Infrared omni-directional 1 Mbps 2 Mbps
5-Ghz Orthogonal FDM 6,9,12 18,24,36, 48, 54 Mbps
2.4 GHz direct sequence spread spectrum 5.5 Mbps 11 Mbps
2.4 GHz Orthogonal FDM Up to 54 Mbps
IEEE 802.11
IEEE 802.11a
802.11b
802.11g

Figure 6-11: IEEE 802 Protocol Architecture

IEEE 802.11 specifies several services that can be categorized into association-related, distribution-related, and privacy-related services. :

Association-Related Services. In mobile environments, association services are needed to identify what stations are associated with an access point (AP). Since this is very closely related to mobility (i.e., some stations may not move a lot while others are always wandering around), the standard defines different transition types based on mobility: a) No transition – a station does not move or moves only within the BSS, b) BSS transition – a station moves from one BSS to another BSS in the same ESS, and c). ESS transition – a station moves from a BSS in one ESS to a BSS within another ESS. To deliver a message to a station, the distribution service needs to know the AP identification to which the message should be sent so that it reaches the destination station. Thus a station must maintain an association with an access point (AP). The following three services support this requirement:

- **Association** – Establishes initial association between station and AP
- **Re-association** – Enables transfer of association from one AP to another, allowing station to move from one BSS to another
- **Disassociation** – Association termination notice from station or AP

Distribution-Related Services are needed to distribute messages within a DS. These services are of two types:

- **Distribution service** is used to exchange MAC frames from a station in one BSS to a station in another BSS
- **Integration service**: is used to transfer data between stations on an IEEE 802.11 LAN and stations on an integrated IEEE 802.x LAN (wired LAN). This supports exchange of information between wired and wireless LANs.

Access and Privacy Services have special requirements in the mobile environment because the stations can wander around and associate with an access point that is within the transmitter frequency ranges. The following three services are designed for adequate security:

- **Authentication** is used to establish identity of stations to each other.
- **De-authentication** is invoked when existing authentication is terminated.
- **Privacy** prevents message contents from being read by an unintended recipient.

6.3.3 IEEE 802.11 Physical Layer

The physical layer of IEEE 802.11 has been issued in several stages (see Figure 6-11). The first part, simply called IEEE 802.11, was issued in 1997. The other two, known as IEEE 802.11a and IEEE 802.11b, were issued in 1999. The IEEE 802.11g was introduced in 2002. Through these options at the physical layer level, IEEE 802.11 supports data rates that range from 1 Mbps to 54 Mbps. Let us look at these.

6.3.3.1 Original IEEE 802.11 Physical Layer

This is the oldest 802.11 physical layer specification and includes the following two RF transmission methods and one infrared – all operating at data rates of 1 Mbps and 2 Mbps (see Figure 6-11):

- **Frequency-Hopping Spread-Spectrum (FHSS) Physical Layer.** The physical layer data rate for an FHSS system is 1 Mbps – the FHSS physical layer has 22 hop patterns to choose from. The frequency hop physical layer is required to hop across the 2.4GHz ISM (Industrial, Scientific, Medical) band covering 79 channels. Each channel occupies 1Mhz of bandwidth.
- **Direct-Sequencing Spread-Spectrum (DSSS) Physical Layer.** The DSSS supports both 1 Mbps and 2 Mbps data rates, operating in the 2.4 GHz ISM band. The DSSS physical layer uses an 11-bit sequence to spread the data before it is transmitted. The receiver de-spreads the RF input to recover the original data. As stated previously, this technique reduces the effect of interference (i.e., the receiver can reconstruct the message in spite of interference).

Infrared Physical Layer. One infrared standard is supported which operates in the 850-to-950 nM band. The physical layer supports two data rates; 1 and 2Mbps. The standard uses omnidirectional infrared technology.

Operation of the WLAN in unlicensed RF bands requires the use of spread-spectrum modulation to meet the requirements for operation in most countries. The RF transmission standards in the standard are Frequency-Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS). Both architectures are defined for operation in the 2.400 GHz to 2.483 GHz band. The choice between FHSS and DSSS will depend on a number of factors related to the user's application and the environment in which the system will be operating. Each of the physical layers use their own unique header to synchronize the receiver and to determine signal modulation format and data packet length.

6.3.3.2 IEEE 802.11a and IEEE 802.11b Physical Layers

The **IEEE 802.11a** specification makes use of 5 GHz band to provide data rates of 6, 9, 12, 18, 24, 36, 48, and 54 Mbps. It operates in the 5 GHz frequency band – a much less congested frequency band than 2.4 GHz. It supports twelve separate non-overlapping channels; thus you can use up to twelve access points set to different channels in the same physical location without any interference with each other. This makes access point channel assignment much easier and significantly increases the throughput of the wireless LAN. Instead of spread spectrum, 802.11a uses orthogonal frequency division multiplexing (OFDM). OFDM is similar to FDM but all subchannels are dedicated to a single source. Thus, a given frequency band is subdivided into several subchannels and then all subchannels are used for a single source, thus increasing the effective data rate. The system uses a variety of modulation techniques, such as BPSK and QPSK, depending on the data rate needed. See the sidebar, "OFDM – A Closer Look" for more information.

The **IEEE 802.11b** is the most common physical layer implementation and is commonly known as wireless Ethernet because it competes with the old copper Ethernet LANs. IEEE 802.11b uses an extension of the 802.11 DSSS scheme and provides data rates of 5.5 and 11 Mbps. To achieve a higher data rate in the same bandwidth, a modulation scheme known as complementary code keying (CCK) modulation is used. CCK is quite complex and is not discussed here.

6.3.3.3 IEEE 802.11g

802.11g is an enhancement of 802.11b – it basically extends the 802.11b's data rates to 54 Mbps within the 2.4 GHz band using OFDM (orthogonal frequency division multiplexing) technology. It is compatible with 802.11b, thus the 802.11b access points can be upgraded to be 802.11g compliant relatively easily. An issue with 802.11g and also with 802.11b is that the 2.4 GHz band is very congested; thus considerable RF interference from other 2.4 GHz devices can cause problems. Many other devices such as Bluetooth and some cordless phones operate in 2.4 GHz. To cut down the interference, the power of the access points can be reduced to decrease the range of the 802.11g devices. This means that the access points can be placed closer to each other, but doing this could be expensive because more access points are needed to cover a given area.

6.3.3.4 802.11a Versus 802.11g

802.11a and 802.11g both deliver the same data rates, so they are fierce competitors. However, there are major differences between the two. The major difference is that 802.11a operates in the 5 GHz frequency band, which is less crowded than the 2.4 GHz band. However, the distance range is lower than 802.11g because higher frequencies have shorter ranges (the loss is higher at higher frequencies). Because of the shorter distance, the cost of 802.11a could be higher – you need more access points for the same area. A major limitation of 802.11a is that it is not compatible with 802.11b, thus a device equipped with an 802.11b or 802.11g card cannot interface directly to an 802.11a access point. This situation can be taken care of by multimode NICs (Network Interface Cards) that are becoming commercially available.

Table 6-4 captures the differences between 802.11a and 802.11g. What should you do if you want to use higher data rates in the 54 Mbps range? Basically, you should use 802.11a if you are starting from scratch but use 802.11g if you have a large embedded base of 802.11b LANs.

Table 6-4: 802.11a versus 802.11g

Factor	**802.11a**	**802.11g**	**Comments**
Data rate	54 Mbps	54 Mbps	Competitors for same data rates
Frequency	5 GHZ	2.4 GHz	802.11a shorter range (needs more AP) 802.11a has less interference because it operates in 5 GHz band
Compatibility with Wi-Fi (802.11b)	Not compatible	Compatible	Need new access points if an 802.11b LAN is to be converted to 802.11a.

What is OFDM?

OFDM (Orthogonal Frequency Division Multiplexing) is a very popular technique at present for delivering fast data rates in WLANs as well as cellular networks. It is a variation of the frequency division multiplexing (FDM) technique, in that multiple signals are sent simultaneously over a single transmission path by using different frequencies. For example, user u1 is transmitted at frequency f1, u2 at f2, u3 at f3, etc., on the same cable. The receiver “tunes” to f1 to receive u1 data, f2 for u2 data, etc. OFDM uses a similar concept, but instead of sending different data sources over different frequencies, it sends the same data source on all frequencies. Basically a bit stream from a data source is subdivided into n segments, and these n segments of data bits are sent in *parallel* over the same medium by using frequencies f1, f2, f3, ..., fn. Each frequency is separated from the next to minimize interference. The main advantage of OFDM is that it handles fading and inter-symbol interference (ISI) very well at high data rates. This is why it is so popular for high data rate communications.

Let us take a closer look. OFDM distributes the data over a large number of carriers that are spaced apart at precise frequencies. This spacing provides the “orthogonality” in this technique which prevents the receivers from seeing frequencies other than their own. This orthogonality is useful because in a typical terrestrial broadcasting scenario there are multipath-channels (i.e., the transmitted signal arrives at the receiver using various paths of different lengths). Since multiple versions of the signal interfere with each other, leading to inter-symbol interference (ISI), it becomes very hard to extract the original information. Using properly spaced different frequencies helps with multi-path impairments and ISI.

802.11a specifies an OFDM Physical Layer that splits the information signal across 52 separate sub-carriers. These 52 subcarrieres are further subdivided as following:

- Four are resesrved as pilot sub-carriers that the system uses to monitor and handle impairments.
- The remaining 48 sub-carriers provide separate wireless “pathways” for sending the information in a parallel fashion.

This division of the information flow and use of the pilot sub-carriers makes OFDM signals much more resilient to multi-path propagation and ISI. In addition, the parallel-form of transmission over multiple sub-carriers enables IEEE 802.11a-based wireless LANs to operate at data rates up to 54 Mbps.

An issue with OFDM is that there is no single standard. In addition to IEEE 802.11a, HiperLAN/2 implements a similar, but different version of OFDM. In addition, there are several proprietary implementations of OFDM such as Florion's Flash OFDM for cellular networks (see Chapter 10). To counter this problem, the OFDM Forum is in the process of establishing a common, global OFDM standard for wireless transmission.

6.3.4 IEEE 802.11 Medium Access Control (MAC) Layer

The MAC layer specification for 802.11 is similar to the 802.3 Ethernet wired line standard. The protocol for 802.11 uses the carrier-sense, multiple access, collision avoidance (CSMA/CA) protocol. This protocol *avoids* collisions instead of detecting a collision like the algorithm used in 802.3. Collision avoidance is used because it is difficult to detect collisions in a radio transmission network. The CSMA/CA protocol allows for options that can minimize collisions by using different techniques.

The MAC layer covers three functional areas: reliable data delivery, access control, and security. The following sections give an overview (for details, see [Grier 2002, Stallings 2002]).

6.3.4.1 Reliable Data Delivery

MAC must handle interference, noise, fading, etc. Although some of these errors can be handled at higher levels, it is more efficient to deal with errors at the MAC level than at a higher layer (such as TCP). IEEE 802.11 includes a frame exchange protocol according to which the source station transmits data and the destination responds with acknowledgment (ACK). If the source does not receive ACK, it retransmits the frame. Thus the basic 802.11 data transfer mechanism only supports two frame exchanges (a frame is sent and an ACK is received). A four-frame exchange may be used to enhance reliability. In this case, the source issues a request to send (RTS), the destination responds with "clear to send" (CTS), source transmits data, and destination responds with ACK.

It is interesting to note how free channels are detected to avoid collisions in 802.11. The physical layer uses a clear channel assessment (CCA) algorithm to determine if the channel is clear. This is accomplished by measuring the RF energy at the antenna and determining the strength of the received signal. If the received signal strength is below a specified threshold, the channel is declared clear and the MAC layer is given the clear channel status for data transmission. If the RF energy is above the threshold, data transmissions are deferred in accordance with the protocol rules. The standard provides for a more sophisticated option for CCA that verifies that the signal is the same carrier type as from 802.11 transmitters. Thus non- 802.11 signals in the environment are filtered out.

6.3.4.2 Access Control

To support centralized as well as ad hoc LANs, the following two approaches have been proposed and accepted by the IEEE 802.11:

- Distributed Coordination Function (required) that uses Ethernet-type CSMA. DCF is useful in ad hoc networks.

- Point Coordination Function (optional), implemented on top of DCF, uses polling, typically done by an access point. PCF is suitable for a centralized LAN. As can be seen from Figure 6-11, PCF resides above the DCF services.

Medium access control (MAC) must deal with the situation when more than one station wants to access the medium. The 802.11 MAC does not implement CSMA/CD (CSMA with Collision Detection) because it is very difficult to detect collisions in a wireless environment due to different types of scattering and fading. Instead a delay, known as Interframe Space (IFS), is used to avoid conflicts and prioritize handling of requests. Figure 6-12 shows the control logic. Basically, MAC waits for a delay period of IFS before transmitting. In reality, DCF includes a set of delays (IFSs) with the following values instead of one:

- Short IFS (SIFS). This is the shortest IFS and is used for immediate response actions (high-priority) messages.
- Point coordination function IFS (PIFS). This is a mid-length IFS that is used by the centralized controller in the PCF scheme when using polls.
- Distributed coordination function IFS (DIFS). This is the longest IFS, used as a minimum delay for ordinary asynchronous frames contending for access.

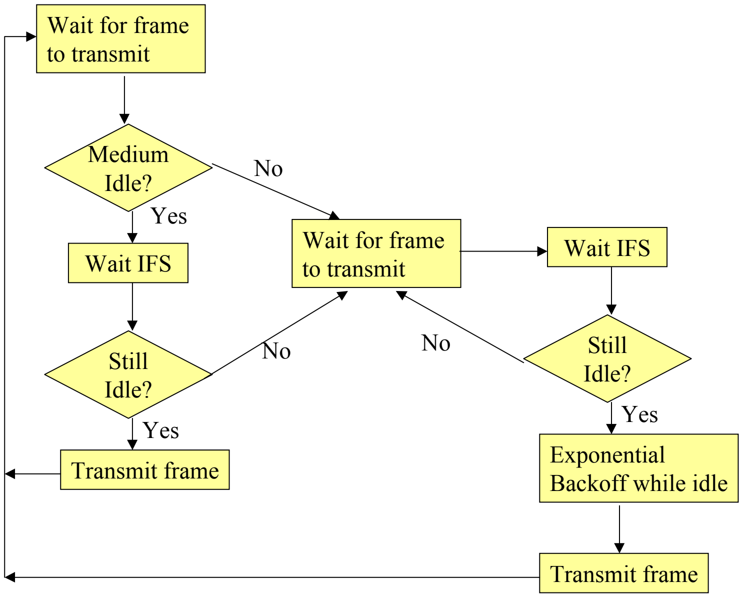


Figure 6-12: IEEE 802.6 Medium Access Control Logic

Different values of IFS are used automatically for different situations. For example, most of the data traffic uses DIFS, but SIFS are used to carry ACKs. PIFS are used during polling for PCF. For example: suppose a MAC is supporting 7 stations in an ad hoc network. In this case, the data is sent by using DIFS delays, but when the acknowledgement is sent it uses the shorter delay value of SIFS. Thus responses do not have to wait long before transmission. Consider now the situation when an access point supports a centralized network. In this case, the access point first polls the stations and then receives data from selected stations. The response to polling uses PIFS, a very short delay, while data messages have a longer delay of DIFS.

A wide range of MAC frame formats are used in the IEEE 802.11 standard. A discussion of these frame formats is beyond the scope of this chapter. For frame formats, see [Stallings 2002, Grier 2002].

6.3.4.3 Security Services and the Wired Equivalent Privacy Algorithm (WEP)

Security provisions are addressed in the standard as an optional feature to address concerns about eavesdropping. The data security is accomplished by a complex encryption technique know as the Wired Equivalent Privacy Algorithm (WEP). WEP is part of the IEEE802.11standard and is designed to protect wireless communication from eavesdropping at the MAC layer level. WEP is also intended to prevent unauthorized access to a wireless network. Although this is not an explicit goal of the 802.11 standard, it is frequently considered to be a feature of WEP.

WEP is intended to provide modest security (only encryption and authentication) for 802.11 LANs. WEP is based on protecting the transmitted data over the RF medium using a 64-bit seed key and the RC4 encryption algorithm. WEP, when enabled, only protects the data packet information and does not protect the physical layer header, so that other stations on the network can listen to the control data needed to manage the network. However, the other stations cannot decrypt the data portions of the packet. The WEP encryption process is based on the following steps:

- An integrity algorithm creates and appends a CRC.
- A pseudo random number generator (PRNG) is used to generate a ciphertext.

Authentication in 802.11 is provided at two levels: a) open system authentication that involves only exchange of identities between two parties and provides no security benefits, and b) shared secret key authentication that requires two parties to share a secret key; this is more secure.

Let us look at shared secret key authentication in more detail. The secret key is shared between a mobile station (e.g., a laptop with a wireless Ethernet card) and an access point (i.e. a base station). The secret key is used to encrypt packets before they are transmitted, and an integrity check is used to ensure that packets are not modified in transit. The standard does not discuss how the shared key is established. In practice, most installations use a single key that is shared between all mobile stations and access points. More sophisticated key management techniques can be used to protect the wireless LAN from attacks; however, commercial systems do not support such techniques widely.

A number of flaws have been found in the WEP algorithm which could seriously undermine the security claims of the system. In particular, a group of researchers at Berkeley (www.drizzle.com/~aboba/IEEE/wep-draft.zip) found that the following types of attacks against WEP are practical to mount using only inexpensive off-the-shelf equipment:

- Passive attacks to decrypt traffic based on statistical analysis.
- Active attack to inject new traffic from unauthorized mobile stations, based on known plain text.
- Active attacks to decrypt traffic, based on tricking the access point.
- Dictionary-building attack that, after analysis of about a day's worth of traffic, allows real-time automated decryption of all traffic.

Note that these attacks apply to both 40-bit and the 128-bit versions of WEP equally well. They also apply to networks that use 802.11b standard (802.11b is an extension of 802.11 to support higher data rates; it leaves the WEP algorithm unchanged). There have been some additional security methods to supply additional security for the 802.11 standard, such as the 802.1x standard that can operate with 802.11 networks.

Based on these experiments, it is recommend that anyone using an 802.11 wireless network not rely on WEP for security, but employ higher level (e.g., application) security measures to protect their wireless network data. A new specification, called 802.11i, is being developed to address the limitations of WEP (see Chapter 12 for a discussion of 802.11i). See the following for additional discussion of WEP security:

[1] Jwww.drizzle.com/~aboba/IEEE/11-01-253r0-I-WEP2SecurityAnalysis.ppt – A summary presentation on WEP security issues

[2] www.drizzle.com/~aboba/IEEE/wep-draft.zip – Berkeley WEP Security Analysis Presentation (PDF)

[3] www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pdf – Fluhrer, Mantin and Shamir's paper on cracking WEP

[4] www.drizzle.com/~aboba/IEEE/wepimprovF.ppt – Possible ways of improving WEP

6.3.5 IEEE 802.11 Logical Link Control (LLC)

Let us now start with LLC, the highest layer in 802.11. It should be noted that LLC is not specifically addressed by 802.11 because of its emphasis on MAC and physical layers. However, we should mention the LLC services that are important to 802.11. Basically, an LLC must support multi-access, shared-medium nature of the link with the following services

- **Unacknowledged connectionless service (datagram)**. This service provides no flow- and error-control mechanisms and data delivery is not guaranteed. Thus higher-level applications are responsible for reliable delivery. This LLC service, also known as "fire and forget," could be used with TCP (let TCP worry about reliable delivery).
- **Connection-mode service.** This provides the logical connection that is set up between two users with support for flow and error control. The connection-mode service builds tables to keep track of session activities. Because this service takes care of many connection-oriented details, it could be used in situations where thin application software is needed (e.g., controllers).
- **Acknowledged connectionless service.** This is a cross between the previous two. It is basically a datagram service but the datagrams are acknowledged. This service is useful in situations where no prior logical setup between the communicating parties is needed but some acknowledge is desirable. It can be used when many users are involved in a session, but the connection-mode tables could be too many. By using this service, no connection tables are needed.

6.3.6 Additional 802.11 Standards and Industrial Notes

So far, we have mainly concentrated on 802.11, 80211a, 802.11b, and 802.11g. However, there are many other members of the 802.11 family, as shown in Table 6-5, that go up to 802.11i at the time of this writing. These standards are being developed by Working Groups (for example, 802.11f indicates results produced by the 802.f Working Group) that are concentrating on security, QoS, and regulatory issues. It is natural to ask: why are there different standards within 802.11? Here are some thoughts.

The main reason is that standards change with time, often due to changes in requirements. For example, concerns of security and interoperability have dominated wireless LAN solutions, and the 802.11a standard has had to respond to these requirements. IEEE developed supplemental standards (such as 802.11i for security) to address these issues.

Another reason is the output power and sub-bands which are used. This is important when there are other radios in the same frequency as your solution. The solution needs to be able to detect these other radios and react by lowering its power output in order to keep them from interfering with each other. This has become a mandatory requirement in many European countries and also in other countries around the world. The standard group working to address this is the IEEE 802.11h working group. This new draft standard is intended to provide for attenuating transmission power as well as flexibly selecting transmission frequency in order to keep from interfering with other potential devices in that same frequency spectrum.

Roaming is a major issue in wireless systems. Having the ability to roam freely between service sets and extended service sets has been traditionally an unsuccessful aspect of wireless LANs. The IEEE specification does not give detailed information on roaming, but in practice within the 802.11b technology, roaming does not work very well. Each wireless station must have complete loss of signal from a base station to connect to another base station. Data rates and signal strength can be degraded, and loss of data can occur during the service set transition. The 802.11f Working Group is addressing this problem.

Operation outside the United States is another issue that has been plaguing the 802.11 technology. Operating frequencies fall into unlicensed national information structure (U-NII) bands at 5.15 to 5.25 GHz, 5.25 to 5.35 GHz, and 5.725 to 5.825 GHz. The US allows all of the above frequencies to be used. The upper portion of the band is mainly intended to be used for point-to-point communications, mainly for WMAN connections. Outside the US, Europe and Japan have more restrictions and regulations within the 5 GHz frequency spectrum. The 802.11h Working Group is developing enhancements of 802.11a at the MAC and physical layer level to enable regulatory acceptance of 802.11a products in Europe.

Not all requirements result in a new working group. For example, power management is an important consideration in WLANs. This is supported in 802.11 at the MAC level for those applications requiring mobility under battery operation. Provisions are made in the protocol for the portable stations to go to low power "sleep" mode during a time interval defined by the base station. There is no need, so far, to introduce a new standard (but who knows!).

Table 6-5: IEEE 802.11 Family

Extension	Scope
802.11a	5 GHz (OFDM) PHY specification
802.11b	2.4 GHz (DSSS) PHY specification
802.11d	2.4 GHz Regulatory Domain Update
802.11e	Quality of service. QoS supporting a broad range of applications such as voice, video-conferencing, and streaming video.
802.11f	Inter Access Point Protocol (IAPP). Roaming extensions that let mobile devices remain connected when they are moved between different Access Points
802.11g	2.4 GHz higher rates (22 Mbps)
802.11h	Enhancements of 802.11a at MAC and PHY level (enables regulatory acceptance of 802.11a products in Europe)
802.11I	security (server-based authentication)

Let us conclude this discussion by examining some industrial/business realities. IEEE 802.11 LAN products are being implemented on ISA or PCMCIA cards for use in handheld personal computers, PDAs, laptops or desktop applications. The need for higher data rates, for applications requiring wireless connectivity at 10 Mbps and higher is pushing wireless LANs to higher data rates. Manufacturers and globe-trotting users of WLAN products need to be aware of the Electromagnetic Compatibility (EMC) requirements that vary from one country to another. The regulations are intended to minimize the interference between the numerous users of radio equipment in the unlicensed bands. The 802.11 standard defines the specifications for the WLAN transceivers for the major market areas and identifies the minimum technical requirements for interoperability and compliance based upon established regulations for Europe, Japan, and the North America.

For up-to-date information on the topic, visit the Wireless LAN Association Web site (http://www.wlana.com/). The wireless information site (http://www.palowireless.com) also has a complete section devoted to IEEE802.11.

Sources of Information for 802.11

Chen, James C. *Measured Performance of 5-GHz 802.11a Wireless LAN Systems.* Atheros Communications, August 2001.

Geier, J. *Wireless LANs*. 2nd ed. SAMs Books, 2002.

http://www.80211-planet.com/tutorials/article/0,,10724_981611,00.html

www.palowireless.com/80211

www.wireless.ittoolbox.com

http://www.80211-planet.com/columns/article/0,4000,1781_1000821,00.html

http://www.80211-planet.com/tutorials/article/0,4000,10724_990101,00.html

http://www.80211-planet.com/columns/article/0,4000,1781_975841,00.html

Time to Take a Break

✓ • Overview and Main Concepts

✓ • IEEE 802.11 Wireless LANs

• Mobile Ad Hoc Networks and HiperLAN2

6.4 Mobile Ad-hoc Networks (MANETs)

6.4.1 Overview

In Latin, *ad hoc* means "for this purpose only," and is used to imply a temporary setup for a specific purpose. An ad hoc network, also known as ***MANET (Mobile Ad hoc Network***), is a spontaneous, typically wireless local area network in which some of the network devices are part of the network only for the duration of a communications session (e.g., a meeting). The term is used to describe peer-to-peer networks in which new devices can be quickly added or deleted on an as-needed basis. Basically, an ad hoc network is a wireless LAN without an access point (AP). When an AP is present, stations do not communicate on a peer-to-peer basis, thus APs are not part of ad hoc networks (see Figure 6-13).

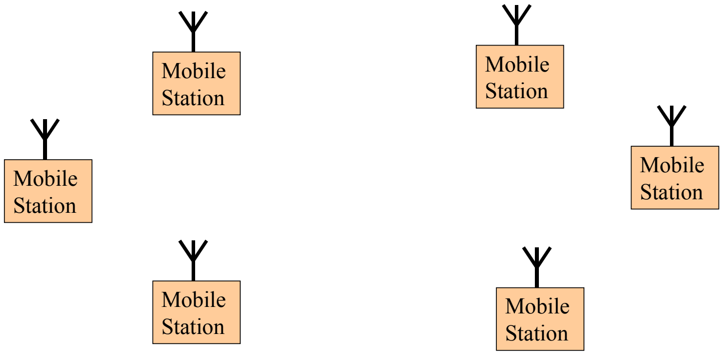


Figure 6-13: Ad hoc Network

The main advantage of ad hoc networks is that they are self-organizing wireless networks composed of mobile stations that communicate with each other without a fixed and pre-planned infrastructure. Due to this, diverse applications of MANET are possible. MANETs also raise interesting technical problems in routing and media access. Let us review some applications and technical problems.

We will take a closer look at MANETs in Chapter 10. Additional information about ad hoc networks can be found in (http://searchnetworking.techtarget.com) and M. Naraghi-Pour, "Investigation of Media Access Control Protocols for Mobile Ad-hoc Networks," *Technical Report for NIST Contract Q-912364*, June 2000.

6.4.2 MANET Examples

Because they do not require an existing infrastructure, MANETs can be rapidly deployed to provide communication in a variety of applications. Examples of these applications are in military (tactical communication in the battlefield), civilian (e.g., electronic classrooms, convention centers, construction cites), law enforcement (e.g., crowd control, search and rescue), and disaster recovery (e.g., fire, flood, earthquake). For example, in a battlefield, it is impossible to first set up a network infrastructure, install access points, and start fighting (obviously!). In this case, various battlefield devices (tanks, jeeps, soldier guns) can be equipped to form MANETs and communicate with each other to exchange battlefield information.

Although MANETs have been around for a while, and many applications are possible, most applications were in the battlefield area before turn of the century. Everyday commercial applications gained popularity due to the ad hoc network support by Bluetooth. As we will see later in discussion about Bluetooth, it is possible to organize a given set of Bluetooth devices in many different configurations representing ad hoc networks in home networking and small office settings. Given a collection of Bluetooth devices, an explicit topology construction protocol is needed for forming ad hoc networks. Another large application area for MANETs is wireless sensor networks (WSNs). These networks are formed by thousands of tiny sensors that communicate with each other in an ad hoc manner. We will discuss Bluetooth and MANETs in the next chapter.

6.4.3 Routing Protocols for Ad Hoc Mobile Wireless Networks

The interconnections between nodes of an ad hoc network are capable of changing on a continual basis. Thus a routing protocol needs to discover routes between nodes on an ongoing basis. This is unlike a wired network where the routes are predetermined. The primary goal of ad hoc network routing protocol is to construct routes with a minimum of overhead and bandwidth consumption. These routing protocols may be categorized as table-driven or source-initiated on-demand driven.

The table-driven routing protocols attempt to maintain consistent, up-to-date routing information from each node to every other node in the network. These protocols require each node to maintain one or more tables to store routing information. The nodes respond to changes in network topology by propagating updates throughout the network to maintain a consistent network view. The areas where they differ are the number of necessary routing-related tables and the methods by which changes in network structure are broadcast.

A different approach from table-driven routing is **source-initiated on-demand routing**. This type of routing creates routes only when needed by the sending node. When a sending node requires a route to a destination, it initiates a route-discovery process. This process is completed once a route is found or all possible route permutations have been examined. Once a route has been established, it is not changed until either the destination becomes inaccessible along every path from the source or until the route is no longer desired.

6.4.4 Media Access Control Protocols for Mobile Ad Hoc Networks

Many applications of ad hoc networks intermix emergency (e.g., medical alert), real-time and non-real-time traffic. This creates different priority classes, each with their own QoS requirements. Access to media to satisfy these sometimes-conflicting QoS requirements is a challenge.

Carrier-sense multiple access (CSMA) protocol is a possible candidate for ad hoc wireless networks. CSMA is a simple distributed protocol whereby nodes control their packet transmission attempts based on their perception of the state (busy or idle) of the common radio channel. A station transmits if it finds the channel to be idle (no carrier) and defers transmission if it finds it to be busy (carrier detected). CSMA is very successful in wired LANs (it is the foundation of Ethernet), however it does not provide satisfactory performance in the wireless environment. Furthermore, CSMA cannot provide QoS guarantees to multimedia applications because all traffic sources are treated equally and performance guarantees cannot be provided. In addition, CSMA cannot support different priority classes in ad hoc WLAN or in ad hoc mobile networks.

Split-channel reservation multiple access (SRMA) is a protocol specifically designed for wireless networks. SRMA avoids collisions of data packets by introducing a control-signal handshake between the transmitter and the receiver. When node A wishes to send a packet to node B, using Aloha or CSMA, it sends a Request-to-Send (RTS) packet to B. Upon receiving the CTS (Clear-to-Send) packet from B, node A commences transmission of its data packet. SRMA uses separate control channels for RTS and CTS packets and thus can control traffic for QoS.

6.5 HiperLAN2

6.5.1 Overview

HiperLAN Type 2, or HiperLAN2, is a wireless LAN standard developed by the European Telecommunications Standards Institute (ETSI). The adopters of HiperLAN2 are mainly Europeans who claim that it accommodates current and future evolving wireless network environments, and that it is not merely a wireless LAN solution, but provides superior connectivity technology. A HiperLAN2 Global Forum (http://www.hiperlan2.com/) has been established to promote this standard. Specifically, the following benefits have been highlighted about HiperLAN2:

- Data rate of 54 Mbps
- A high level of security
- QoS capabilities to support virtually any type of service or application
- High and scalable capacity as the number of users increase in the system
- Managed bandwidth with predictable performance for each user and application
- Robust protocols that also optimize the overall throughput of the available radio resource, making it the most spectrum-efficient WLAN technology operating at 5 GHz
- Ease of use through a set of auto-configuration tools

The HiperLAN2 specifications are developed by ETSI BRAN (Broadband Radio Access Network) – a standardization effort within ETSI. HiperLAN2 is a flexible Radio LAN standard designed to provide high speed access (up to 54 Mbps at the physical layer) to a variety of networks including 3G mobile core networks, ATM networks and IP based networks. It is also intended for private use as a wireless LAN system. It operates in the 5 GHz band – the band that is allocated to wireless LANs worldwide. Thus, it has been claimed that HiperLAN2 has the potential to enable the success of wireless LANs on a global basis. ETSI BRAN is collaborating with other associations to develop specifications for access interfaces with 3G wireless networks. ETSI BRAN is also developing conformance test specifications for the core HiperLAN2 standards, to assure interoperability of devices and products produced by different vendors. The HiperLAN2 solution has the following features that proponents claim will be necessary for any long-lasting wireless standard:

- QoS for real-time multimedia communication – at least for operators, it will be vital to find new ways of increasing the revenue streams besides offering plain best-effort Internet services.
- Efficient power-save control for integration into portable devices – if WLAN can’t be integrated into portable devices, the mass consumer market will be left out.
- Medium Access Control (MAC) layer developed and optimized for radio communication on 5 GHz to deliver highest possible throughput over the air interface, and also for when users increase to potentially very high numbers (e.g., a big conference room) within one cell
- Dynamic Frequency Selection (DFS), realizing Automatic Frequency Planning that greatly simplifies the radio network installation and expansion – important to all users, but almost a showstopper if not realized in residential areas
- Plug ’n’ play; ideal for multiple access points within an enterprise environment
- Convergence Layer, offering backbone network independence by allowing for interoperability with Ethernet, ATM, IEEE1394 (Firewire) and 3G Mobile systems
- Strong security features with support for individual authentication and per-session encryption keys, including support to use either pre-shared keys or PKI along with DES/3DES

- Advanced state of standardization (ahead of 802.11 “g” and “h” extensions) and test specifications – HiperLAN2 is extremely well defined to facilitate interoperability and robust protocol operation.

6.5.2 HiperLAN2 – Technology Overview

HiperLAN2 is a broadband radio networking technology that allows interconnection into almost any type of fixed network technology. As stated previously, HiperLAN2 supports different levels of Quality of Service (QoS) and security, and is interoperable with existing wired networks such as ATM and TCP/IP.

Figure 6-14 shows a conceptual view of a typical HiperLAN2 radio network. At first glance, HiperLAN2 appears similar to the other WLANs (802.11 and Bluetooth). Mobile Terminals (MT) communicate with Access Points (AP) through wireless technology. The APs are typically connected to a wired LAN for outside access. MTs can also communicate directly with each other to form ad hoc networks and may move around freely within the wireless network. An MT, after login has been performed, can only communicate with one AP at a time, and the AP ensures that the radio network is automatically configured. The terminal requests handover if an AP with a better signal strength is available. Communicating with an AP (master-slave mode) is referred to as Centralized Mode communication in HiperLAN2, and communication between MTs (ad hoc peer-to-peer mode) without passing information via the AP is referred to as Direct Mode.

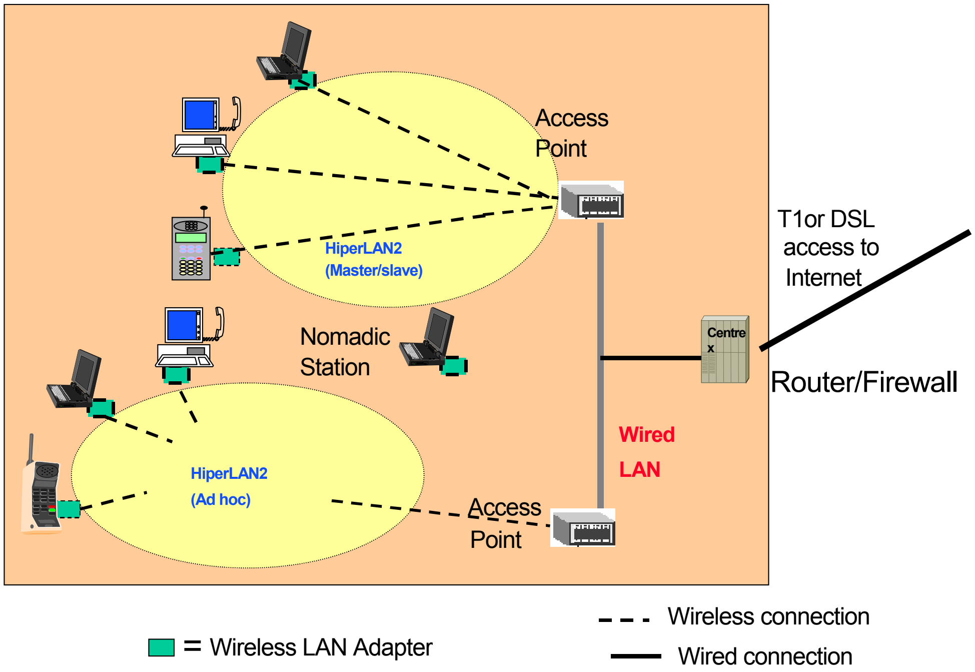


Figure 6-14: HiperLAN2 Conceptual View

Figure 6-15 shows the HiperLAN2 protocol stack. The protocol stack is partitioned into two parts: (i) Control Plane and (ii) User Plane. The user plane includes functions for end users while the control plane supervises flow and control of information. The HiperLAN2 protocol consists of three basic layers: (i) Physical Layer, (ii) Data Link Control Layer (DLC), and (iii)

Convergence Layer (CL). The Physical Layer (PHY) is virtually the same as for the IEEE 5 GHz standard, 802.11a. The MAC and link sub-layers (part of the DLC layer) provide all the functionality for access control to the medium. Let us review these layers briefly.

6.5.2.1 Layer 1: Physical Layer

As stated previously, the HIPERLAN type 2 operates in the 5.2 Ghz frequency band with a very high transmission rate of up to 54 Mbps. This is achieved by making use of Orthogonal Frequency Digital Multiplexing (OFDM), which is also used in 802.11a. As discussed in Section 6.3.3.2, OFDM transmits high data rate information by dividing the data into several interleaved, parallel bit streams, that are carried by separate sub-carriers. Since the physical layer of HiperLAN2 is very similar to 802.11a, we do not discuss this here.

6.5.2.2 Layer 2: Data Link Control Layer

The Data Link Control Layer supports the logical link between an access point (AP) and the mobile terminals (MTs). The DLC includes functions for medium access and transmission (user plane) as well as terminal/user and connection handling (control plane) and consists of the following sublayers as shown in Figure 6-15:

- **MAC Protocol**. The air interface is based on time-division duplex (TDD) and dynamic time-division multiple access (TDMA). The basic MAC frame structure on the air interface has a fixed duration of 2 ms and comprises transport channels for broadcast control, frame control, access control, downlink and uplink data transmission and random access. Downlink or uplink traffic consists of PDU trains to and from MTs. A PDU train consists of both user PDUs (long transport channels – LCH) and control PDUs (short transport channel – SCH) to be transmitted and received by one MT. Several other transport channels also exist for broadcast, feedback, etc.
- **Error Control (EC) Protocol.** Selective repeat (SR) ARQ is the Error Control (EC) mechanism that is used to increase the reliability over the radio link. EC refers to detection of bit errors, and the resulting retransmission of U-PDUs if necessary. EC also supports QoS.
- **Radio Link Control Protocol (Signaling and Control).** The RLC protocol gives a transport service for the signaling entities: (i) Association Control Function (ACF) to associate an MT with an AP, (ii) Radio Resource Control function (RRC) to support handoffs and power save functions., and (iii) the DLC User Connection Control function (DCC) for the MT to request user connections. These entities comprise the DLC control plane for the exchange of signaling messages between the AP and the MT.

6.5.2.3 Convergence Layer

The Convergence Layer (CL) adapts to the network environment. Several types of Convergence Layer services have been defined, and new ones can be added if demanded. For example, the Ethernet Convergence Layer makes the HiperLAN2 network operate as a wireless Ethernet extension. This layer has two main functions: (i) adapting service requests from higher layers to the service offered by the DLC and (ii) converting the higher-layer packets with variable or possibly fixed size into a fixed size that is used within the DLC. The generic architecture of the CL makes HiperLAN2 suitable as a radio access network for a diversity of fixed networks, e.g. Ethernet, IP, ATM, UMTS, etc.

The structure of the CL includes a common and service-specific part to allow for easy adaptation to different configurations and fixed networks. As a starting point, the HiperLAN2 standard specifies the common part and a service-specific part for interworking with a fixed Ethernet network. The main function of the common part of the convergence layer is to segment packets received from the services.

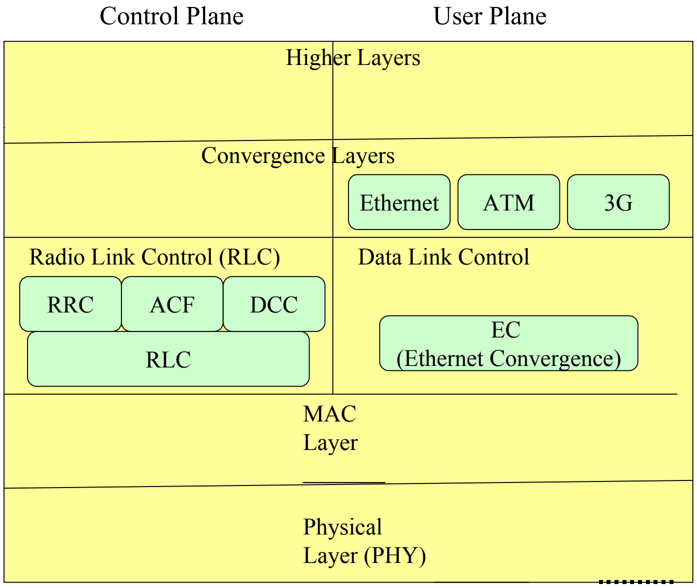


Figure 6-15: HiperLAN2 Protocol Stack

6.5.2.4 Additional Technical Feature of HiperLAN2

- Traffic scheduling is centralized to the AP in HiperLAN2. This is important for optimizing the use of radio resources, especially as the number of users increases. Centralized scheduling is also important for the efficient support of QoS.
- In HiperLAN2, each connection can be assigned either a simple relative priority level or a specific QoS in terms of bandwidth, delay, jitter, bit error rate, etc.
- The HiperLAN2 Access Points have a built-in support for automatic transmission frequency allocation within the APs' coverage area. Thus, there is no need for manual frequency planning as in cellular networks like GSM.
- The HiperLAN2 network supports authentication and encryption. Both the AP and the MT can authenticate each other to ensure authorized access to the network or to a valid network operator. The encryption can be used on established connections to protect against eavesdropping and man-in-the-middle attacks. In HiperLAN, each communicating node is given a HiperLAN ID (HID) and a Node ID (NID). The combination of these two IDs uniquely identifies any station, and restricts the way it can connect to other HiperLAN nodes. All nodes with the same HID can communicate with each other using a dynamic routing mechanism denoted Intra-HiperLAN Forwarding.
- The support for handover enables mobility of MTs. The handover scheme is MT-initiated; i.e., the MT uses the AP with the best signal, as measured for instance by S/N-ratio; and as the user moves around, all established connections move to the AP with the best radio transmission performance, while the MT stays associated to the HiperLAN2 network. The HiperLAN2 architecture is easily adapted and integrated with a variety of fixed networks. All applications running over a fixed infrastructure can also run over a HiperLAN2 network.
- The power-save mechanism in HiperLAN2 is based on MT-initiated negotiation of sleep periods. The MT requests the AP for a low power state and a specific sleep period. At the expiration of the sleep period, the MT searches for a wakeup indication from the AP, and in the absence of that, sleeps for the next period, and so forth. The MT receives any pending data as the sleep period expires. Different sleep periods are supported depending

on the requirements. Traffic is carried over multiple connections (a user can have several connections established), and each connection can be assigned a specific QoS or just support best effort (i.e., the connection tries to deliver the fastest it can without any guarantees).

6.5.3 Tradeoffs Between HiperLAN2 and 802.11

HiperLAN2 and 802.11 (especially 802.11a and 802.11g, termed 802.11a-g) directly compete with each other because they provide the same data rate of 54 Mbps with around a 100-meter coverage area. Here are the key tradeoffs:

- HiperLAN2 is primarily popular in Europe but 802.11a-g has a global following.
- The total complexity and the resulting price of 802.11a-g are roughly the same as HiperLAN2.
- HiperLAN2 is more frequency-efficient. Therefore, deployment of HiperLAN2 networks demands fewer Access Points (at least a saving ratio of 3:4).
- HiperLAN2 has stronger QoS and security features as compared to 802.11a-g.

Due to the relative newness of 802.11g, past studies have compared the performance of HiperLAN2 and IEEE 802.11a. An example is the comparison performed by Janne Korhonen of the Helsinki University of Technology [Kornhonen 1999]. The main difference has been found in the medium access methods, where HiperLAN2 uses a centralized controller and IEEE 802.11a is based on decentralized competition. The overall findings of the research was that a higher performance in terms of throughput and dropping could be seen for HiperLAN2.

Can 802.11a-g and HiperLAN2 coexist? The main problem is that the 5 Ghz bands have been reserved for HiperLAN2 systems in Europe and 802.11a also operates in the same part of the frequency spectrum (802.11g operates in the 2.4 GHz band). Thus 802.11a is not yet certifiable in Europe by the ETSI. This is being rectified to allow both HiperLAN2 and 802.11a to coexist by allowing clients to detect the most available channels and use the minimum output power necessary if interference is evident.

Is HiperLAN2 better than 802.11a? Both have strengths and weaknesses (so what is new?). IEEE 802.11a suffers from poor quality of service, security inadequacies, and can only handle Ethernet traffic, but is a global standard. HiperLAN2 appears to be technically better but is not receiving global acceptance, and HiperLAN2-compliant products are almost a year behind the comparable 802.11a products. At present, although 802.11a is being favored more around the globe, it is competing against 802.11g, as discussed in Section 6.3.3.4. It seems that 802.11g is more popular than both 802.11a and HiperLAN2.

Additional Sources of Information about HiperLAN2

HiperLAN2 Global Forum Website – http://www.hiperlan2.com/

Korhonen, Janne. “Performance Comparison: HiperLAn2 Versus 802.11a.” Masters thesis, Helsinki University of Technology, 1999.

www.wireless.ittoolbox.com

http://www.theregister.co.uk/content/archive/18000.html

http://www.chipcenter.com/wireless/news072.html http://www.hiperlan.uk.com/pages/hiperlan.htm#18

http://www.mtecwireless.com/htdocs/products/HL2doormanrev.pdf

http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/wttpr_pg.pdf

http://zdnet.com.com/2100-1107-821805.html

http://www.80211-planet.com/columns/article/0,4000,1781_975841,00.html

http://www.nd.edu/~mhaenggi/NET/wireless/hiperlan/Resources.htm

http://www.envara.com/global_protocal_roadmap_-_bran.pdf

6.6 Short Case Studies and Examples

6.6.1 Example of an 802.11 LAN at Home

Figure 6-16 shows example of an actual home network. This network consists of two desktops (one for the father, the other for the mother – both working professionals) in two different rooms. A printer is attached to one of the desktops and two laptops are used by two teenagers – both in high school. Initially, only the father's desktop (in room 1) was connected to the public Internet through a cable modem. This caused problems when the other members of the family wanted to access the Internet or print something.

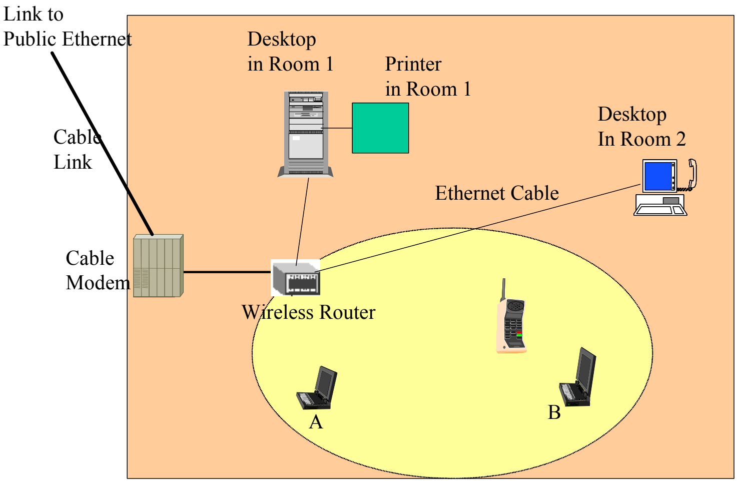


Figure 6-16: A Sample Home Network

A "family council" meeting decided to install a network in the house – this decision resulted in the network shown below. The heart of this home network is a wireless router that consists of four Ethernet slots and an 802.11b access point. This router is connected to the two desktops and the cable modem. The access point of the router supports the laptops, both equipped with 802.11b cards. This router allows all computers in the house to access the

Internet and also share the printer – source for delight and happiness for all! The family is considering using voice over 802.11, but this is not working yet. The total cost of setting up this network was less than $300 that included the wireless router, the adapter cards, etc (the cost of computers was not included in this estimate). It took less than two hours to get the whole network operational, without any 'professional" help.

6.6.2 A Mobile Access Point on a Passenger Bus

The Karnataka state government in India has computerised land records but the records are not easily accessible to villages because they do not have access to phone lines. DakNet, a wireless broadband network, solved this problem by using a Mobile Access Point (MAP) *mounted on a regular passenger bus* to transmit information between village and district headquarters. A villager can request information about their land records (or other services) through a PC in a WiFi-enabled village kiosk. The request for information is stored in the kiosk computer until a bus with a MAP passes and collects the information wirelessly. The information is then transferred to the district headquarters when the bus is within range of the WiFi-enabled systems based at headquarters. The computer on the bus captures the response from the headquarter and delivers it to the villager when the bus goes by the village kiosk again. The information delivered can include land record and related service transactions.

Source: http://www.e-devexchange.org/eGov/topic4.htm

6.6.3 Delivering Voice Over 802.11

The IEEE 802.11 WLANs were initially targeted for data applications. But now, 802.11 is also beginning to support telephone services, creating new competition for 3G cellular. The advantage of using 802.11 for voice services is that no frequency allocation fees have to be paid. In addition, higher data rates can be provided by the 802.11 network for wireless Internet access. Several companies are beginning to provide "hybrid" cellular services where part of the phone service, for example in an office, is supported over 802.11 but the other is provided over cellular network. Here is an interesting example.

Vocera Communications, founded in 2000, has developed a wireless voice communications system for organizations. The wireless system is based on a small wearable, hands-free, voice-activated unit to transmit voice over an 802.11b Wi-Fi LAN. Since the underlying network is 802.11b, the wireless voice service is limited to small geographic coverage such as within an office building or campus. However, the system connects to the corporate PBX and is therefore capable of making and receiving outside calls as well. Vocera's target market is a business environment where workers need to constantly be mobile within a building or campus, but also need to frequently communicate with colleagues and in other parts of the organization who may be located remotely. Potential industries that fit this description include regular office settings, healthcare (doctors and nurses in a hospital), and retail.

The system uses speech recognition software to make the wearable transmitter completely hands-free, thereby making the call initiation and receipt process more convenient. The underlying 802.11 network uses Direct Sequence Spread Spectrum (DSSS) on frequencies of 2.4 and 5 GHz ranges, therefore avoiding disturbances to other devices within the premises. The system takes advantage of three converging markets: Wireless LAN, VoIP, and speech recognition software. The system is designed to make use of existing or planned 802.11b wireless networks to allow in-building workers to communicate with one another while roaming and away from wired telephones and other hardwired communication systems.

The Vocera system consists of three parts (see Figure 6-17): Vocera Communications software, which runs on a Windows 2000 based server at the customer premises; the Vocera Communication Badges, small wearable devices that permit one-button voice access to other users on the system; and an additional software component for the system's connection to the organization's PBX for external calls. The server software contains the system's intelligence, including Call Manager, User Manager and Connection Manager, as well the speech recognition voiceprint security certification software. User preferences are configured on the server via browser-based Administration and User Consoles. The Vocera Telephony Solution Software works with either an analog or digital T1 line card installed in the Vocera server to allow Badge users to place and receive calls from traditional phone systems including outside calls and calls from internal extensions.

Source: http://www.vocera.com

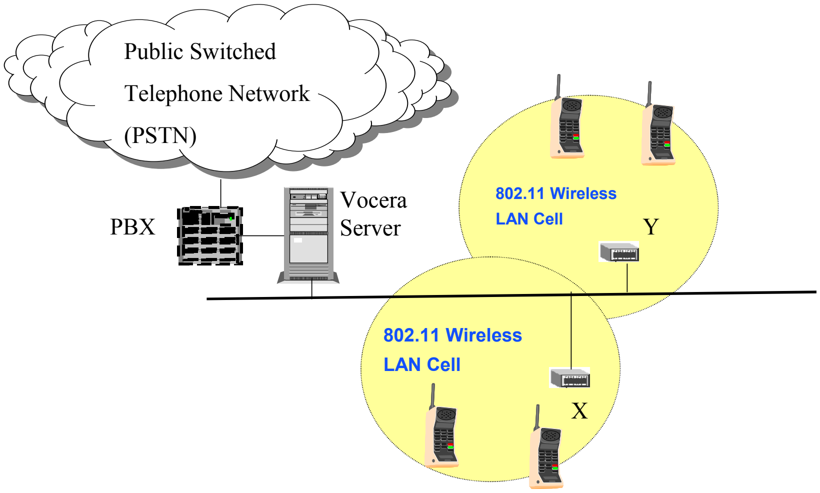


Figure 6-17: Conceptual View of Vocera system

6.6.4 Honeywell uses WLAN for Production Tracking[1]

Honeywell is a global provider of integrated avionics, engines, systems and service solutions to customers around the globe. The Honeywell aerospace division, headquartered in Phoenix, Arizona, produces 9 billion dollars in revenues. A WLAN is implemented in the Phoenix Repair and Overhaul subdivision in Phoenix. This is a 300,000 square-foot facility housing 800 employees repairing engine components for commercial and military aircrafts. The facility consists of different work centers on various workshop floors. Parts flow through these workshop floors and are eventually reassembled as an overhauled engine. The facility generates around 250,000 data transactions a day. Each transaction is important for managing the process flow.

The old system used light pens to gather data on the work in process. These pens were connected to a desktop computer with a wired network where the transaction data was entered as a batch process. The problem was that the parts were moving much faster than the batch data was being collected. Due to this mismatch, the decision makers never knew where the parts really were. Management needed a method to collect labor transactions appropriately so that they could assign them to specific work orders. To conduct a shop-wide inventory,

[1] Suggested by Sy Tran.

Honeywell's staff wrote everything down on papers and keyed in the information at a computer terminal. Then they went to the scanner station and waited for the information to download. The old system took about 2 days to complete the inventory.

The new initiative system used WLAN with portable computers, Web-based data collection screens, and wireless bar code scanners to track the parts and labor associated with each work order. Figure 6-18 shows the conceptual diagram of how the WLAN is implemented at Honeywell's Phoenix facility. The wireless handheld scanners and Web-based data collection screens are used in the individual repair stations. A corporate database collects this information in real time and makes it available to production control and corporate offices at additional access points. To materialize this vision, the facility installed a large WLAN on its workshop floors, and the corporate offices also installed access points allowing their employees to get data seamlessly between buildings and production floors.

The WLAN reportedly reduced labor collection issues by 99.6% in the first week of use. The management is expected to save 15% of time in production control and coordination operations. Additionally, the continuous information helps to increase the speed of parts movement throughout the workshop floors. The WLAN enables real-time information gathering and provides a platform for improving processes to isolate and correct the defective processes quickly. The inventory time has dropped from 2 days to 4 hours because the workers can now scan in the data immediately. In addition, while on the shop floors, the production coordinators can use their portable computers to run a mini-inventory in a specific area and fix any problems immediately. The portable computers can also be used to find any items that appear to be missing, or to order rework if needed.

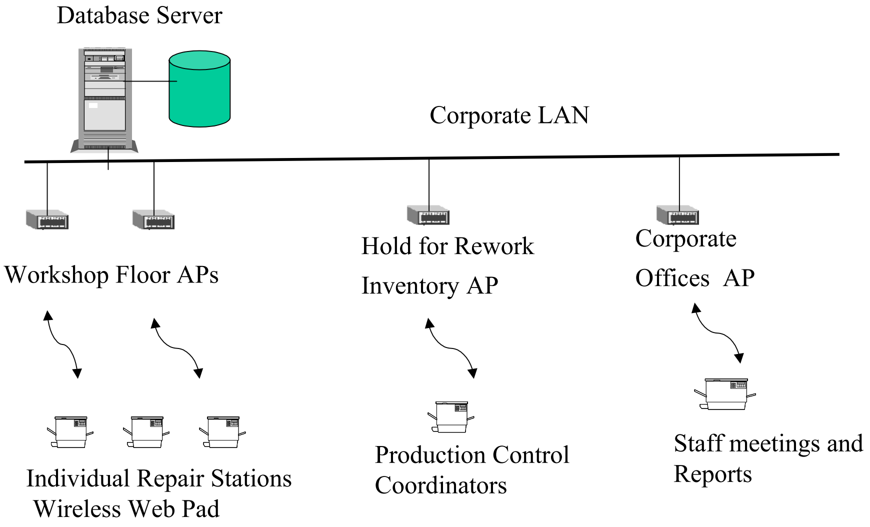


Figure 6-18: Honeywell WLAN

Source: Honeywell, *Honeywell goes Wireless*, an Intermec Technologies Corporation report, 2004.

6.6.5 Using Wireless Carts for Patient Care

Children's Hospital of Wisconsin was founded in 1894 with the mission to provide a comprehensive and integrated pediatric healthcare delivery model and to offer the best solution for the total healthcare needs of children.

The hospital used a traditional approach to place orders for medications for treatment. The orders were placed by taking a piece of the patient's chart with the order entry, writing up the order, and putting the chart where the patient's nurse would see and use it. This was done for each patient. It was a time-consuming and cumbersome process. So the hospital installed hard-wired PCs and Ethernet ports in the ICU (Intensive Care Unit) rooms. The results were not satisfactory because most rooms lacked space for permanent PCs and the Ethernet jacks would get unplugged when things were moved around in the hospital rooms.

In 2001, the hospital adopted a wireless solution, provided by Cisco Systems, that introduced an 802.11b wireless LAN in various divisions of the hospital. To implement this system, the hospital acquired 16 mobile workstations from Tremont Medical, each with its own 802.11b PC card. Access points (Aironet 340 APs from Cisco) were installed in strategic locations throughout the hospital for maximum coverage. The Aironet 340 APs were connected to the main hard-wired Ethernet network for access to other parts of the network. The Cisco Aironet AP, like many other commercially available APs, is a wireless LAN transceiver that serves a wireless cell or as the connection point between wireless and wired networks. Cisco Aironet 340 series APs receive power through the Ethernet cable, so there was no need to use a separate power cord to the access point. The Ethernet cable was plugged into the Ethernet port on the back of the access point and the other end was plugged into a power source. The access point's omni-directional antennas provided diversity coverage to help maintain a clear radio signal between the access point and wireless client devices. The Cisco access point could also be configured as a standalone repeater to forward traffic between wireless users and the wired LAN by sending packets to either another repeater or to an access point connected to the wired LAN. For detailed specification of Cisco Aironet 340 AP, visit the Cisco site (http://www.cisco.com/).

By using the wireless solution, the hospital team started their rounds accompanied by two wireless carts (typically one for the resident and one for the attending physician or a specialist). The therapists could now place orders with greater ease and also look up certain graphic trends and results while visiting the patient. Since the carts also had Internet access – the APs were connected to the Ethernet LAN that had Internet access – instant research was possible if needed. The wireless LAN proved invaluable for emergency cases where numerous orders had to be placed quickly and accurately. The staff could wheel a wireless cart in and keep it there until the patient was stabilized. The wireless network also proved extremely helpful in recovery rooms where post-surgery patients needed constant care and appropriate pain medications were needed immediately. The wireless carts played a vital role in effective treatment of patients and helping the hospital to operate far more efficiently.

Source: www.cisco.com/en/US/products

6.6.6 Wireless Network for a Delivery System[2]

Business Express, a subsidiary of Littlewoods in UK, is a 48-hour home delivery specialist. It has 32 depots, 2 sort centers, 2,000 vehicles, 4,000 employees, and delivers approximately 69 million parcels annually (20,000 to 40,000 items per day). The company tracks goods as they leave the distribution center, to the sorting center, and then to the depots, and finally to the doorstep.

The old distribution system was manual and too labor-intensive. The movement of items was tracked manually. At the depot, the recording and checking was done through paper lists and

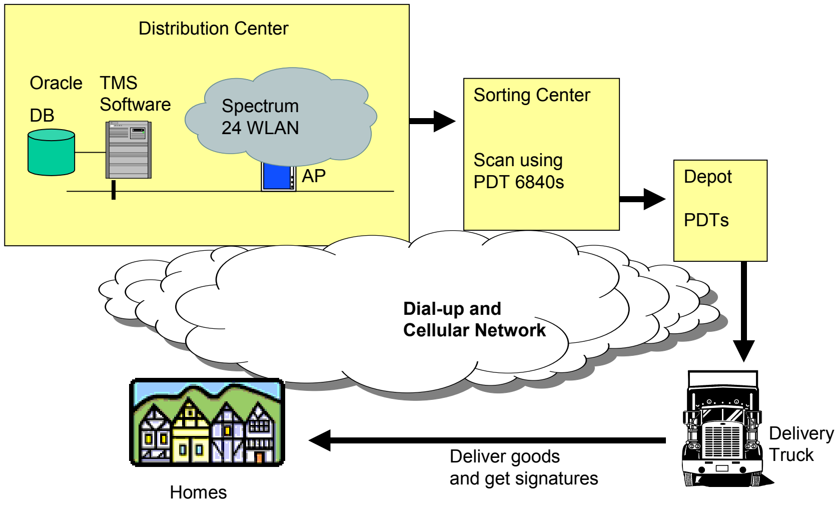
[2] Suggested by Amy Wang.

there was no tracking after a parcel left the depot. This caused delays, and it was harder to identify exactly where the parcel was.

The manual checking system was replaced with a wireless solution in which mobile devices were used to capture the bar codes. The mobile devices were connected to a Spectrum 24 wireless LAN and could also access a database via the wireless LAN (see Figure 6-19). Specifically, the PDT 6840 (portable data terminals) were used to capture the bar code – goods were scanned leaving the distribution center and also when entering the sorting center using the PDT 6840. These terminals operated in real time and reported to the central track and trace system. The van driver also scanned parcels sorted to his route and scanned/captured signatures at the doorstep using the SPT 1740 pocket computers. Drivers then used their pocket computers to transmit the information to the central system via a dial-up modem cradle.

Each of the over thirty depots have a Spectrum24 wireless LAN, so the terminals connect in real time via the Spectrum24 access points to the central system. The Task Master TMS software requests and obtains data, manages it, and reports back information to the central track and trace system. A SUN Solaris UNIX platform is the server behind the system, and contains an Oracle 8i relational database as well as the Task Master TMS software. The server can support data from 2,500 client terminals. The database can be queried via Web browsers for parcel progress.

As a result, the distribution system is more efficient. When customers call about a parcel, the company can identify the parcel's step along the chain. Delays can also be identified more easily for elimination. In addition, management processes are improved because the performance of the drivers and the depots can be measured more easily.



Legend: Solid arrow indicates movement of items

Figure 6-19: Business Express Network

Sources:

http://www.businessexpress.co.uk/who_news_jun.htm

http://www.symbol.com/uk/Solutions/case_study_littlewoods_lo.html

http://www.symbol.com/products/wireless/ap4131.html http://www.symbol.com/products/mobile_computers/mobile_kb_pdt_6800.html

http://www.symbol.com/products/mobile_computers/mobile_palm_spt1800.html

6.7 Concluding Comments

Wireless LANs allow workstations in a building to communicate with each other without having to be connected to physical cables. Many vendors provide wireless LANs with different capabilities. The most promising technology in this area at present is based on the IEEE 802.11 standard. The IEEE802.11 LANs operate in a manner very similar to the wired Ethernet LANs and provide data rates up to 54 Mbps while operating in the unlicensed bandwidth reserved for short-range, low-power devices. A government license is not required to use the devices or the radio transmitter, or to operate other equipment in this frequency range. Spread spectrum is used to avoid interference in this band. Although HiperLAN is getting some attention in Europe, 802.11 wireless LANs are extremely popular. Another competitor, Bluetooth, is a slower technology intended for personal area networks (1 Mbps data rate, 10 meter distance). We will discuss Bluetooth in the next chapter.

6.8 Review Questions and Exercises

1) List five different applications of wireless LANs.

2) What are the main requirements of wireless LANs?

3) Describe a wireless LAN that you are familiar with.

4) What are the key advantages and disadvantages of infrared WLANs?

5) Which WLAN technology is used more often? Explain through an example.

6) What is a MANET? Explain through an example.

7) Briefly define the main layers of the 802.11 WLANs.

8) What are the different family members of IEEE802.11 and what are the tradeoffs between the different options?

9) List and briefly describe the 802.11 services.

10) What is the difference between 802.11 MAC and LLC services? Explain through an example.

11) What is the difference between PCF and DCF? Explain through an example.

12) What is IFS and how it is used to support multiple access in 802.11 networks?

13) What is HiperLAN2 and how does it compare and contrast with 802.11?

6.9 References

Books and Articles

Bhola, J. *Wireless LANs Demystified*. McGraw Hill, 2002

Chen, James C. *Measured Performance of 5-GHz 802.11a Wireless LAN Systems*. Atheros Communications, August 2001.

Davis, P., McGuffin, P. *Wireless Local Area Networks: Technology, Issues, and Strategies.* McGraw-Hill Computer Communications, 1995.

Geier, J. *Wireless Networking Handbook*. New Riders, 1996.

Geier, J. *Wireless LANs*. 2nd ed. SAMs Books, 2002.

Maufer, T. *A Field Guide to Wireless LANs for Administrators and Power Users*. Prentice Hall, 2003.

Stallings, W. *Wireless Communications and Networks*. Prentice Hall, 2002.

Polizzi, T. *WCCN Handbook: RF Terminals and LANs.* WCCN Publications, 1993.

Santamaria, A. and Lopez-Hernandez, F. J. (eds.), *Wireless LAN Systems.* The Artech House Telecommunications Library, 1994.

Varshney, U. "Recent Advances in Wireless Networking." *IEEE Computer*, June 2000, pp. 100-102.

Varshney, U. and Vetter, R. "Emerging Mobile and Wireless Networks." *Comm of ACM*, June 2000, pp. 73-91.

Useful Web Links

http://www.wlana.org

http://ww.palowireless.com

http://www.hiperlan2.com/top

http://www.80211-planet.com/tutorials/article/0,,10724_981611,00.html

www.palowireless.com/80211

www.wireless.ittoolbox.com

http://www.theregister.co.uk/content/archive/18000.html

http://www.chipcenter.com/wireless/news072.html

http://www.hiperlan.uk.com/pages/hiperlan.htm#18

http://www.networkcomputing.com/1201/1201ws1.html

http://www.comnets.rwth-aachen.de/publications/Abstracts/HabethaSCI2001.html

http://www.mtecwireless.com/htdocs/products/HL2doormanrev.pdf

http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/wttpr_pg.pdf

http://zdnet.com.com/2100-1107-821805.html

http://www.80211-planet.com/columns/article/0,4000,1781_1000821,00.html

http://www.80211-planet.com/tutorials/article/0,4000,10724_990101,00.html

http://www.80211-planet.com/columns/article/0,4000,1781_975841,00.html

http://www.nd.edu/~mhaenggi/NET/wireless/hiperlan/Resources.htm

http://170.12.99.3/researchpdf/IMOB122401RPT_FULLREPORT.PDF

http://www.envara.com/global_protocal_roadmap_-_bran.pdf