Unit 7: Wireless LAN

Notes

CONTENTS

Objectives

After studying this unit, you will be able to:

- Discuss the history of wireless LAN
- Explain the wireless LAN
- Explain the wireless LAN component

Notes

- Discuss the SOHO application Notes
- Describe about public wireless LAN network
- Explain the ad hoc wireless LAN network

Introduction

Wireless LAN technology is evolving at a rapid pace. Within just a few years the industry has seen the highest data rates provided by products based on the 802.11 standards migrate from 2 Mbps (802.11) to 11 Mbps (802.11b) and now to 54 Mbps (802.11a/g). Currently, active efforts are underway within the IEEE to define a next generation standard to be known as 802.11n that will enable rates potentially as high as 600 Mbps in a 40 MHz channel. In addition, efforts are also underway to define the 802.11s standard for mesh networking. These developments, as well as potential future technologies such as cooperative diversity, are creating new challenges and opportunities in the design of low power wireless LAN products.

7.1 History of Wireless LAN

Heinrich Herz discovered and first produced radio waves in 1888 and by 1894 the modern way to send a message over telegraph wires was first conducted. Marconi sent and received signals up to two miles using radio waves. Marconi became known as the "father of radio". By 1899, Marconi sent a signal nine miles across the Bristol Channel and 31 miles across the English Channel to France. In 1901 he was able to transmit across the Atlantic Ocean.

During World War II, the United States Army first used radio signals for data transmission. This inspired a group of researchers in 1971 at the University of Hawaii to create the first packet based radio communications network called ALOHNET. ALOHNET was the very first wireless local area network (WLAN). This first WLAN consisted of 7 computers that communicated in a bi-directional star topology. The first generation of WLAN technology used an unlicensed band (902-928 MHz ISM), which later became crowded with interference from small appliances and industrial machinery. A spread spectrum was used to minimize this interference, which operated at 500 kilobits per second. The second generation of WLAN technology was four times faster and operating at 2Mbps per second. Third generation WLAN technology operates on the same band as the second generation and we currently use it today.

Caution In 1990, the IEEE 802 Executive Committee established the 802.11 Working Group to create a wireless local area network (WLAN) standard. The standard specified an operating frequency in the 2.4GHz ISM band. In 1997 the group approved IEEE 802.11 as the world's first WLAN standard with data rates of 1 and 2 Mbps.

7.2 Wireless Local Area Network

A wireless LAN (WLAN) provides network connectivity between devices, also known as stations, by using radio as the communication medium. Devices that communicate over the WLAN conform to the interfaces and procedures defined through the IEEE 802.11 standards. The basic building block of the WLAN network is the 802.11 basic service set (BSS). A BSS defines a coverage area where all stations within the BSS remain fully connected.

There are two BSS network topologies:

1. ***Infrastructure BSS Networks:*** In this topology, all stations within the BSS communicate with each other through an access point (AP). In this situation, the AP establishes the BSS network. In addition, an infrastructure BSS can consist of more than one interconnected APs that establishes an extended service set (ESS) network.

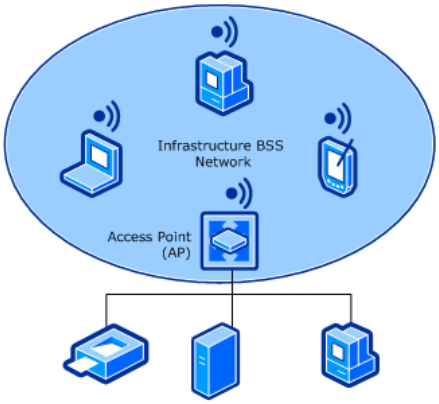
Notes

Each AP within the BSS network provides 802.11 authentication and authorization services for access to the BSS network, as well as privacy services for the encryption of data sent through the BSS network.

In addition, each AP can act as a bridge between the wireless and wired LANs, allowing stations on either LAN to communicate with each other.

The following figure shows the infrastructure BSS network topology.

Figure 7.1: Infrastructure BSS network Topology



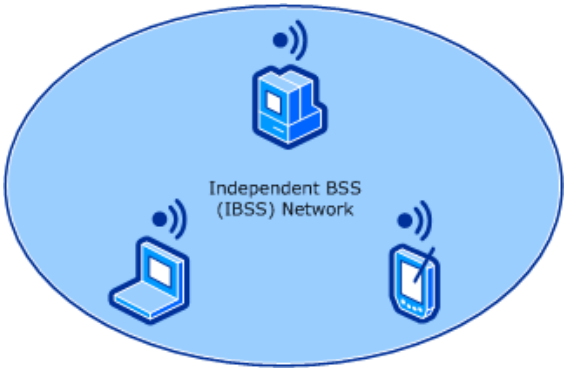
Source: http://msdn.microsoft.com/en-us/library/windows/hardware/ff556962%28v=vs.85%29.aspx

2. ***Independent BSS (IBSS) Networks:*** In this topology, all stations within the BSS communicate directly with each other. In this situation, one station creates, or starts, the BSS network and other stations join the BSS network

   IBSS networks, which are also known as "ad hoc" networks, provide limited support for 802.11 authentication, authorization, and privacy services for the BSS network.

   The following figure shows the independent BSS network topology.

Figure 7.2: Independent BSS Network Topology



Source: http://msdn.microsoft.com/en-us/library/windows/hardware/ff556962%28v=vs.85%29.aspx

7.2.1 Why Wireless?

The world around us is going wireless; we stream music and movies from our home PCs to any room in the house, we can play music from our phones on car stereos and we can go to any number of public places and hook up to the internet.

Notes

But one place has stayed resolutely wired: the enterprise. Yes, many offices these days will have Wi-Fi but often it is reserved for senior management or visitors. Even if it is available for all workers, the connection is rarely the most reliable.

While a physical infrastructure may be good from a management point of view and offer cheap deployment, having all those wires running throughout a building can be costly and awkward to maintain. For example, if a business increases its workforce, all those new workers will need physical connections at their desk – connections that will need to be manually set up. Any breakages in the wired connection will also have to be manually fixed as there is no software solution to a broken Ethernet pin.

With the explosion in mobile devices over the last few years – Apple alone has sold around 100 million iPads since the tablet was introduced in 2010 – many workers are bringing their own devices into the office. It is vital these employees have access to the corporate network to get the most out of them, and that means giving them wireless access. As well as being able to use their own devices, wireless infrastructure means freedom to move around the office, from desk to desk or meeting room to meeting room.

A wireless network is also neater, getting rid of all those unsightly cables that usually run around an office.

7.2.2 How Wireless LANs are Used in the Real World?

Wireless LANs have many applications in the real world. They are frequently used to enhance a wired network, not to completely replace them. The following describes some of the applications that are made possible through the power and flexibility of wireless LAN technology.

- ***Healthcare:*** Doctors and nurses equipped with laptops or PDAs have faster access to patient data. Furthermore, in an emergency situation they can communicate with other departments within the hospital by using WLAN in order to provide quick diagnostics. This is an area where WLAN is allready relatively widely used. As in a majority of cases, WLAN is used to enhance an allready existing wired network.
- ***Conducting everyday business:*** In business, people can work productively with customers or suppliers in meeting rooms - there is no need to leave the room to check if important emails have arrived or print big files. Instead you can send them from one laptop to another. Senior executives in meetings can make quicker decisions because they have access to real-time information.
- ***Network managers in older buildings:*** Network managers in older buildings, such as schools, hospitals, and warehouses, find WLANs to be a most cost-effective infrastructure solution. When building a new network or expanding the old in-house network, few if any cables need be drawn thru the walls and ceilings.
- ***Network managers in dynamic environments:*** Network managers in dynamic environments minimize the cost of moves, network extensions, and other changes by eliminating the cost of cabling and installation. The mobile nature of WLAN allows the building and testing of a new network before moving to mission-critical surroundings.

7.2.3 How Wireless LANs Work?

WLANs use radio, infrared and microwave transmission to transmit data from one point to another without cables. Therefore WLAN offers way to build a Local Area Network without cables. This WLAN can then be attached to an allready existing larger network, the internet for example.

A wireless LAN consists of nodes and access points. A node is a computer or a peripheral (such as a printer) that has a network adapter, in WLANs case with an antenna. Access points function as transmitters and receivers between the nodes themselves or between the nodes and another network. More on this later.

Notes

WLAN data transfer in itself is implemented by one of the following technologies:

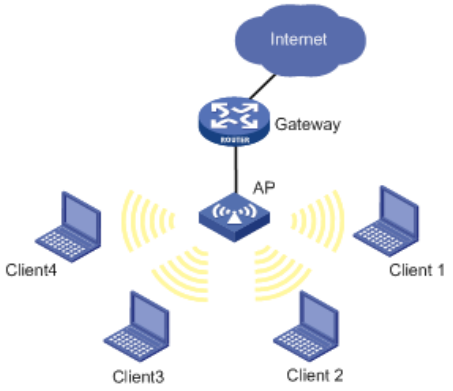
1. ***Frequency Hopping Spread Spectrum:*** Frequency Hopping Spread Spectrum (FHSS) uses a narrowband carrier that changes frequency in a pattern known to both transmitter and receiver. Properly synchronized, the net effect is to maintain a single logical channel. To an unintended receiver, FHSS appears to be short-duration impulse noise.
2. ***Direct Sequence Spread Spectrum:*** 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 (the more bandwidth required also). Even if one or more bits in the chip are damaged during transmission, statistical techniques can recover the original data without the need for retransmission. To an unintended receiver, DSSS appears as low-power wideband noise and is ignored by most narrowband receivers.
3. ***Infrared Technology:*** Infrared (IR) systems use very high frequencies, just below visible light in the electromagnetic spectrum, to carry data. Like light, IR cannot penetrate opaque objects; it is either directed (line-of-sight) or diffuse technology. Inexpensive directed systems provide very limited range (3 ft) and are occasionally used in specific WLAN applications. High performance directed IR is impractical for mobile users and is therefore used only to implement fixed subnetworks. Diffuse (or reflective) IR WLAN systems do not require line-of-sight, but cells are limited to individual rooms.

7.2.4 Wireless LAN Configurations

In hot spots such as airport and coffee shops, some users need to access the Internet through WLAN. In this case, if user authentication cannot be performed, unauthorized users are able to use network resources, which may occupy wireless channels to increase bandwidth cost, decrease the service quality for authorized users, and bring losses to wireless service providers. Used together with IEEE 802.11i, RADIUS authentication and accounting, wireless user isolation can provide security protection for users.

Notes User isolation enables a fat AP to isolate Layer-2 packets (unicast/broadcast) exchanged between wireless clients associated with it, thus disabling them from direct communication.

Figure 7.3: User Isolation Network Diagram



Source: http://www.h3c.com/portal/Technical_Support___Documents/Technical_Documents/WLAN/Access_Point/H3C_WA2200_Series_WLAN_Access_Points/Configuration/Operation_Manual/H3C_WA_Series_WLAN_Access_CG-6W100/02/201009/691527_1285_0.htm#_Ref239669396

Notes

As shown in the figure 7.3, after the fat AP is enabled with user isolation, clients 1 through 4 cannot access each other directly, or learn one another's MAC and IP addresses.

7.2.5 Wireless LAN Technology

There are many technologies that can be used to design a wireless LAN solution. Some of them are discussed below.

- ***Narrowband Technology:*** In radio, narrowband describes a channel in which the bandwidth of the message does not significantly exceed the channel's coherence bandwidth.

  In the study of wired channels, narrowband implies that the channel over consideration is sufficiently narrow that its frequency response can be considered flat. The message bandwidth will therefore be less than the coherence bandwidth of the channel. This is no channel has perfectly flat fading, but the analysis of many aspects of wireless systems is greatly simplified if flat fading can be assumed.

  Narrowband can also be used with the audio spectrum to describe sounds which occupy a narrow range of frequencies. In telephony, narrowband is usually considered to cover frequencies 300–3400 Hz.

- ***Spread Spectrum Technology:*** In telecommunication and radio communication, spread-spectrum techniques are methods by which a signal (e.g. an electrical, electromagnetic, or acoustic signal) generated with a particular bandwidth is deliberately spread in the frequency domain, resulting in a signal with a wider bandwidth. These techniques are used for a variety of reasons, including the establishment of secure communications, increasing resistance to natural interference, noise and jamming, to prevent detection, and to limit power flux density (e.g. in satellite downlinks).

- ***Frequency-Hopping Spread Spectrum Technology:*** Frequency hopping is one of two basic modulation techniques used in spread spectrum signal transmission. It is the repeated switching of frequencies during radio transmission, often to minimize the effectiveness of "electronic warfare" - that is, the unauthorized interception or jamming of telecommunications. It also is known as frequency- hopping code division multiple access (FH-CDMA).

  Spread spectrum modulation techniques have become more common in recent years. Spread spectrum enables a signal to be transmitted across a frequency band that is much wider than the minimum bandwidth required by the information signal. The transmitter "spreads" the energy, originally concentrated in narrowband, across a number of frequency band channels on a wider electromagnetic spectrum. Benefits include improved privacy, decreased narrowband interference, and increased signal capacity.

- ***Direct-Sequence Spread Spectrum Technology:*** In telecommunications, direct-sequence spread spectrum (DSSS) is a modulation technique. As with other spread spectrum technologies, the transmitted signal takes up more bandwidth than the information signal that is being modulated. The name 'spread spectrum' comes from the fact that the carrier signals occur over the full bandwidth (spectrum) of a device's transmitting frequency.

- ***Infrared Technology:*** infrared radiation is the region of the electromagnetic spectrum between microwaves and visible light. In infrared communication an LED transmits the infrared signal as bursts of non-visible light. At the receiving end a photodiode or photoreceptor detects and captures the light pulses, which are then processed to retrieve the information they contain. Some common applications of infrared technology are listed below.

Notes

- Augmentative communication devices
- Car locking systems
- Computers
- Emergency response systems
- Environmental control systems
- Headphones
- Home security systems
- Navigation systems
- Signage
- Telephones
- TVs, VCRs, CD players, stereos
- Toys

Self-Assessment

Fill in the blanks:

1. The basic building block of the WLAN network is the ..... basic service set (BSS).
2. In Infrastructure BSS Networks topology, all stations within the BSS communicate with each other through an .....
3. ..... Spectrum (DSSS) generates a redundant bit pattern for each bit to be transmitted.
4. In the study of wired channels, ... implies that the channel over consideration is sufficiently narrow that its frequency response can be considered flat.
5. In telephony, narrowband is usually considered to cover frequencies ..... Hz.
6. Spread spectrum enables a signal to be transmitted across a frequency band that is much wider than the ..... bandwidth required by the information signal.
7. ..... is the region of the electromagnetic spectrum between microwaves and visible light

7.3 Wireless LAN Components

The different WLAN components are discussed below.

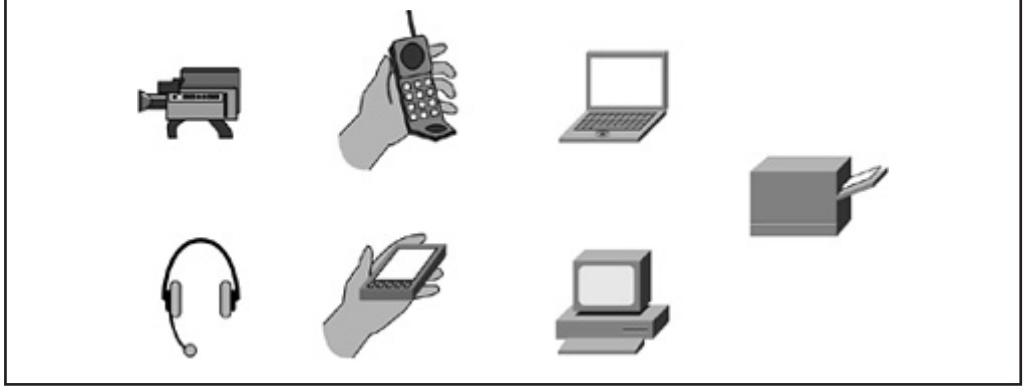
7.3.1 User Devices

Wireless PANs don't require much battery power to operate, making them ideal for small user devices, such as audio headsets, cell phones, PDAs, game controls, GPS units, digital cameras, and laptops. Figure 7.4 illustrates several of these types of devices.

For example, a wireless PAN enables someone to listen to music on headsets wirelessly from their PDA. Or a person can transfer his phone book from his laptop to a cell phone. As with these cases, wireless PANs eliminate wires that often frustrate users.

Notes

Figure 7.4: Many Different Types of User Devices Operate on Wireless PANs



Source: http://etutorials.org/Networking/wn/Chapter+4.+Wireless+PANs+Networks+for+Small+Places/Wireless+PAN+Components/

7.3.2 Radio NICs

Radio NICs are available for wireless PANs in PC Card and Compact Flash (CF) form factors. If you have a laptop, for example, it's easy to add wireless PAN connectivity by installing a PC Card. These products are available from different vendors. Many of the newer PDAs and laptops come equipped with one or more wireless PAN interfaces. This makes these wireless devices ready to connect with other devices, such as printers, PDAs, and cell phones that also have wireless PAN interfaces. The larger PC Cards are uncommon for wireless PANs, mainly because wireless PAN technologies are ideal for small devices.

7.3.3 Access Points

In computer networking, a wireless access point (WAP) is a device that allows wireless devices to connect to a wired network using Wi-Fi, or related standards. The AP usually connects to a router (via a wired network) as a standalone device, but it can also be an integral component of the router itself.

7.3.4 Routers

Most wireless PAN applications simply involve cable replacement, but some vendors sell Bluetooth-equipped routers to support wireless connections to the Internet. Because of limited range, though, these wireless PAN routers are primarily for home and small office use. In order to satisfy more connectivity needs, some wireless PAN routers also support wireless LAN interfaces, such as 802.11.

7.3.5 Repeaters

A wireless repeater (also called wireless range extender) takes an existing signal from a wireless router or access point and rebroadcasts it to create a second network. When two or more hosts have to be connected with one another over the IEEE 802.11 protocol and the distance is too long for a direct connection to be established, a wireless repeater is used to bridge the gap. It can be a specialized stand alone computer networking device. Also, some WNICs optionally support operating in such a mode. Those outside of the primary network will be able to connect through the new "repeated" network. However, as far as the original router or access point is concerned only the repeater MAC is connected. So safety features must be enabled on the wireless repeater as well. Wireless repeaters are commonly used to improve signal range and strength within homes and small offices.

Notes

7.3.6 Antennae

That part of a transmitting or receiving system which is designed to radiate or to receive electromagnetic waves". An antenna can also be viewed as a transitional structure (transducer) between free-space and a transmission line (such as a coaxial line). An important property of an antenna is the ability to focus and shape the radiated power in space e.g.: it enhances the power in some wanted directions and suppresses the power in other directions.

7.4 Small Office/Home Office (SOHO) Applications

Small office/home office (or single office/home office; SOHO) refers to the category of business or cottage industry that involves from 1 to 10 workers.

Before the 19th century, and the spread of the industrial revolution around the globe, nearly all offices were small offices and/or home offices, with only a few exceptions. Most businesses were small, and the paperwork that accompanied them was limited. The industrial revolution aggregated workers in factories, to mass-produce goods. In most circumstances, the so-called "white collar" counterpart—office work—was aggregated as well in large buildings, usually in cities or densely populated suburban areas.

Beginning in the mid-1980s, the advent of the personal computer and fax machine, plus breakthroughs in telecommunications, created opportunities for office workers to decentralize. Decentralization was also perceived as benefiting employers in terms of lower overheads and potentially greater productivity.

Many consultants and the members of such professions as lawyers, real estate agents, and surveyors in small and medium-size towns operate from home offices.

Several ranges of products, such as the armoire desk and all-in-one printer, are designed specifically for the SOHO market. A number of books and magazines have been published and marketed specifically at this type of office. These range from general advice texts to specific guidebooks on such challenges as setting up a small PBX for the office telephones.

Technology has also created a demand for larger businesses to employ individuals who work from home. Sometimes these people remain as an independent businessperson, and sometimes they become employees of a larger company.

In popular literature, the home office has not been the topic of as many works as the "normal" modern office. Brian Basset, the author of the newspaper comic strip Adam@home, has sometimes described its more humorous aspects.

The small office home office has undergone a transformation since its advent as the internet has enabled anyone working from a home office to compete globally. Technology has made this possible through email, the World-Wide Web, e-commerce, videoconferencing, remote desktop software, webinar systems, and telephone connections by VOIP.

7.4.1 SOHO Wireless Network Components

There are currently two types of Wi-Fi components you'll need to build your home or office network: Wi-Fi radio (also known as client devices) devices (desktops, laptops, PDAs, etc.), and access points or gateways that act as base stations. A third type, Wi-Fi equipped peripherals, is emerging and will soon be commonplace. This group includes printers, scanners, cameras, video monitors, set-top boxes and other peripheral equipment.

Types of equipment include:

- PC Card Radio
- Mini-PCI Modules and Embedded Radios

Notes

- USB Adapters
- PCI and ISA Bus Adapters
- Compact Flash and Other Small-Client Formats
- Access Points and Gateways

7.4.2 SOHO Network to Internet Access

To connect a small office or home office (SOHO) network to the Internet, you can use one of two methods:

1. ***Routed connection:*** For a routed connection, the server running Routing and Remote Access acts as an IP router that forwards packets between SOHO hosts and Internet hosts.

   This scenario describes a small office or home office (SOHO) network that connects to the Internet by using a routed connection.

   A SOHO network has the following characteristics:

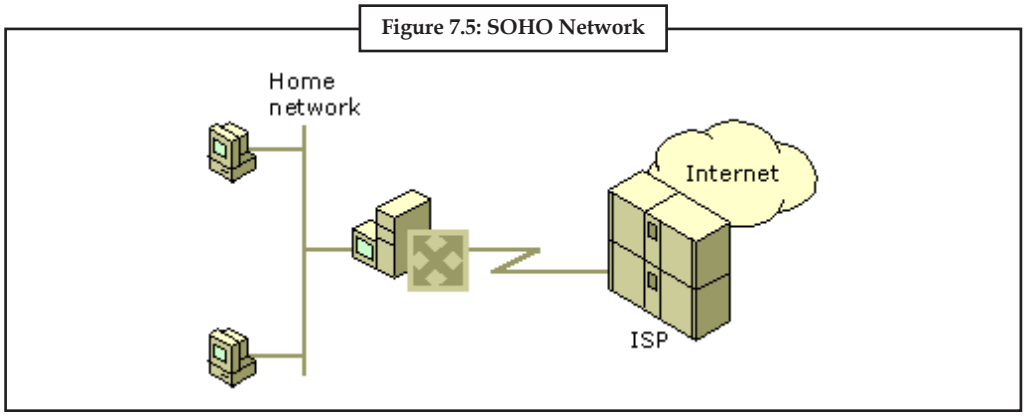
   (a) One network segment.

   (b) A single protocol: TCP/IP.

   (c) Demand-dial or dedicated-link connections to the Internet service provider (ISP).

   The following illustration shows an example of a SOHO network.

Figure 7.5: SOHO Network



The server running Routing and Remote Access is configured with a network adapter for the media that is used in the home network (for example, Ethernet) and an ISDN adapter or an analog modem. You can use a leased line or other permanent connection technologies, such as xDSL and cable modems, but this scenario describes the more typical configuration that uses a dial-up link to a local ISP.

This section covers:

- Planning for a routed connection
- Configuring a routed connection
- Testing a routed connection
- Translated connection

For a translated connection, server running Routing and Remote Access and NAT acts as a network address translator, an IP router that translates addresses for packets that are forwarded between SOHO hosts and Internet hosts.

Notes

This scenario describes a small office or home office (SOHO) network that connects to the Internet by using a translated connection.

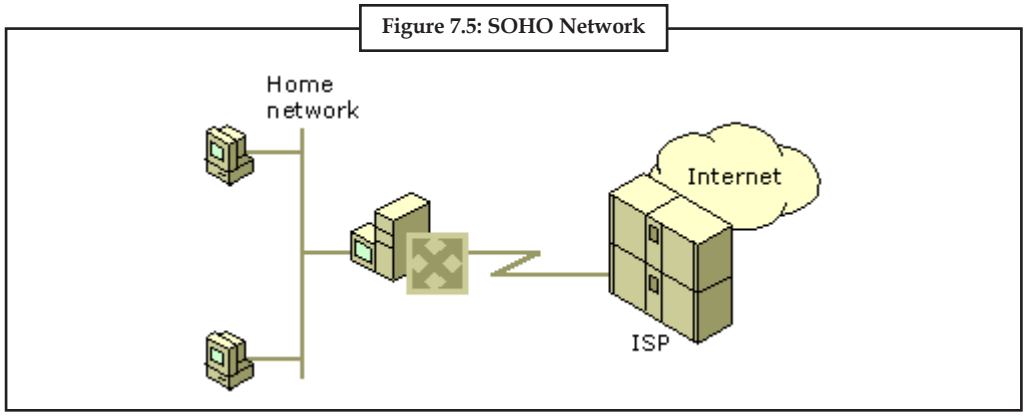
The network configuration is simplified through the use of the network address translation (NAT) routing protocol, which provides network address translation, addressing, and name resolution services for SOHO network computers.

A SOHO network has the following characteristics:

- One network segment.
- A single protocol: TCP/IP.
- Demand-dial or dedicated-link connections to the Internet service provider (ISP).

The following illustration shows an example of a SOHO network.

Figure 7.5: SOHO Network



The server running Routing and Remote Access is configured with a network adapter for the media that is used in the home network (for example, Ethernet) and an ISDN adapter or an analog modem. You can use a leased line or other permanent connection technologies, such as xDSL and cable modems, but this scenario describes the more typical configuration that uses a dial-up link to a local ISP.

This section covers:

- Planning for a translated connection
- Configuring a translated connection
- Testing a translated connection

7.5 Public Wireless LAN Network

The communication network established for the purpose of connecting computer devices of personal use is known as the personal area network PAN (Personal Area Network).when a network is established by connecting phone lines to personal digital devices or PDAs (personal digital assistants), this communication is known as PAN (Personal Area Network). Thomas Zimmerman was the first research scientist to introduce the idea of Personal Area Network (PAN).

The basic purport of establishing PAN (Personal Area Network) is provide a communication channel to the individuals, who want to carry their own digital devices .however at the same they want to stay in contact with the network. PAN (Personal Area Network) networks often cover an area of 30 feet. Personal computer devices may include palm tops mobile phones, potable media players, play stations and net books. These devices help a person to browse internet while traveling, to write notes and to send instant messages. These personal digital devices assist a person to develop networks and communicate via intranet, internet or even extranet. There are

Notes

many wireless technologies which are helpful in developing wireless personal area network. Personal area networks (PAN) are developed either using cables or wireless technologies. Wireless PAN (Personal Area Network) is connected to the wired PAN (Personal Area Network) system either using firewire or USB.

PANs (Personal Area Network)s are dependent on the Bluetooth or infrared technologies for the transmission of wireless signals. Blue tooth wireless PAN (Personal Area Network) is referred to as piconets. Piconets are ad hoc networks. In this piconets network number of devices are connected by using Bluetooth technology. One key master device is further attached to seven or more than dynamic slave seven devices. Master device has a control and option to activate these devices at any time. Piconets work over a range of 200metres and transmit data of about 2100 kbit/ sec. the main focus point of wireless PAN (Personal Area Network) is to facilitate individual workspace. The Bluetooth technology used in wireless PAN (Personal Area Network) connection is based on IEEE 802.15 standard.

Wireless Personal Area Network (WPAN) can perform really efficient operations if we connect them with specialized devices. For examples it can help surgeons to seek guidance from other surgeons or team members during a surgical operation. Wireless Personal Area Network (WPAN) is based on plug –in technology. When wireless equipments come into contact with each other within the range of few kilometers, give an illusion if they are connected with a cable. Rapid development and improvement in this technology is needed in this area. This further development would help develop a seamless network between office and home devices. This development would help scientists, archeologists and people associated to other departments to transfer their findings to any database around them.

The wearable and portable computer devices communicate with each other. These devices while communicating transfer digital signals and information, these signals are transferred using the electrical conductivity coming out of human body. This linkup information exchange can take place even between two people who are carrying digital assistance devices while they are shaking hands. In this process of hand shake, an electric field is generated around people, and they emit Pico amps. These emissions complete the circuit and hence an exchange of information takes place. This information exchange includes the transfer of personal data such as email address, phone numbers etc.

Did u know? The purpose of PDAs is to make the use of electric field around human beings. Mobile phones (smart phones only), palmtops and even pagers serve this purpose. Wireless digital devices work twenty four hours a day and seven days a week. This enables you to stay in communication circle always. PAN (Personal Area Network) network has enabled the transfer of data within the small geographical areas with the help of many small and portable carrying devices.

7.5.1 Benefits of Wireless LAN

The advantages of WLAN are listed below:

- People can access the network from where they want; they are no longer limited by the length of the cable
- Some cities have started to offer Wireless LANs. This means that people can access the internet even outside their normal work environment, for example when they ride the train home.
- Setting up a wireless LAN can be done with one box (called Access point). This box can handle a varying number of connections at the same time. Wired networks require cables to be laid. This can be difficult for certain places.
- Access points can serve a varying number of computers.

Notes

7.5.2 Disadvantages of Wireless LAN

The disadvantages of WLAN are listed below:

- Wireless LANs use radio waves to communicate. Special care needs to be taken to encrypt information. Also the signal is much worse, and more bandwidth needs to be spent on error correction.
- A typical IEEE 802.11 access point has a range of meters from where devices can connect. To extend the range more access points are needed.
- There are many reliability problems, especially those connected to interference from other devices.
- Wireless LANs are much slower than wired ones; this may not matter for most users though, because the bottleneck in a home network is usually the speed of the ADSL line (used to connect to the Internet)

7.6 Ad Hoc Wireless LAN Network

A wireless ad hoc network is a decentralized type of wireless network. The network is ad hoc because it does not rely on a preexisting infrastructure, such as routers in wired networks or access points in managed (infrastructure) wireless networks. Instead, each node participates in routing by forwarding data for other nodes, so the determination of which nodes forward data is made dynamically on the basis of network connectivity. In addition to the classic routing, ad hoc networks can use flooding for forwarding the data.

An ad hoc network typically refers to any set of networks where all devices have equal status on a network and are free to associate with any other ad hoc network device in link range. Ad hoc network often refers to a mode of operation of IEEE 802.11 wireless networks.

It also refers to a network device's ability to maintain link status information for any number of devices in a 1-link (aka "hop") range, and thus, this is most often a Layer 2 activity. Because this is only a Layer 2 activity, ad hoc networks alone may not support a routeable IP network environment without additional Layer 2 or Layer 3 capabilities.

The earliest wireless ad hoc networks were the "packet radio" networks (PRNETs) from the 1970s, sponsored by DARPA after the ALOHA net project.

The decentralized nature of wireless ad hoc networks makes them suitable for a variety of applications where central nodes can't be relied on and may improve the scalability of networks compared to wireless managed networks, though theoretical and practical limits to the overall capacity of such networks have been identified.

Minimal configuration and quick deployment make ad hoc networks suitable for emergency situations like natural disasters or military conflicts.

Notes The presence of dynamic and adaptive routing protocols enables ad hoc networks to be formed quickly.

Self-Assessment

Fill in the blanks:

1. A ..... is a device that allows wireless devices to connect to a wired network using Wi-Fi, or related standards.

Notes

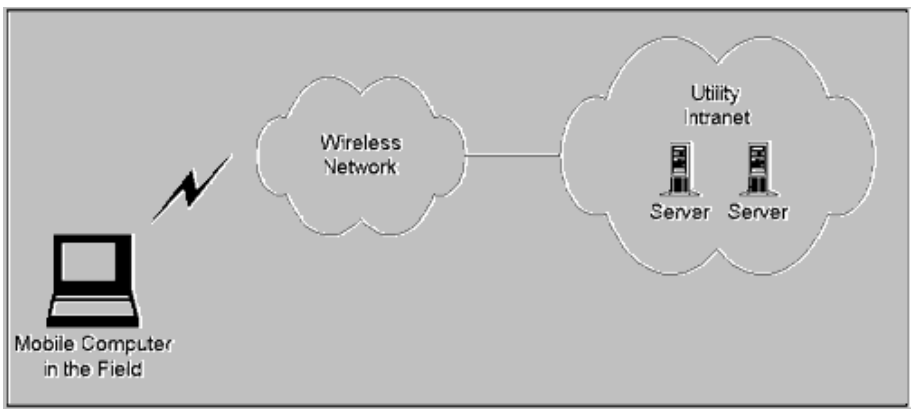
2. When two or more hosts have to be connected with one another over ..... protocol and the distance is too long for a direct connection to be established, a wireless repeater is used to bridge the gap.
3. An important property of an antenna is the ability to focus and shape the ..... power in space
4. The communication network established for the purpose of connecting computer devices of personal use is known as the .....
5. Wireless LANs use ..... waves to communicate.
6. A wireless ad hoc network is a ..... type of wireless network
7. ..... often refers to a mode of operation of IEEE 802.11 wireless networks.
8. The earliest wireless ad hoc networks were the ..... networks

Case Study **Wireless IP**

Introduction

What if field workers of a public utility had online access to inventory databases, work orders, maps and other essential information from anywhere? What if crew chiefs had access to e-mail and schedules without having to return to their offices? This is the vision that the City of Seattle Public Utilities is making a reality in a project spearheaded by its Information Technology Division. This case study shows not only the issues the utility has faced and the solutions it has found; but, more importantly, how the lessons learned can be applied by almost any organization today to make wireless data an effective and successful tool.

Figure 1: The Utility Plans to Make Applications and Information on its Intranet Available to Field Workers



The applications the utility is extending to its mobile workers include both work management and office applications, a combination common to many organizations. Developing wireless networking solutions requires special considerations. The utility has identified effective approaches, is about to proceed with a pilot program, and has a plan that accommodates the inevitable changes in applications, platforms and wireless technologies.

Contd...

Goals

Notes

The utility's work and inventory management application is MAXIMO*, a system that uses an Oracle database, developed by PSDI (Bedford, MA, http://www.psdi.com/). Since MAXIMO is developed for specific types of job functions, it can be considered a vertical market-type application. From the point-of-view of providing wireless access to an enterprise database, however, it is similar to any number of other applications based on SQL (Structured Query Language), one of the most common protocols used today for client/server applications.

The office-based applications that the utility intends to extend to the field include Novell's GroupWise* and Web-hosted applications on the utility's intranet. These are horizontal market applications in that their use is not restricted to any particular job function or type of industry. In addition, the utility plans to make a GIS (graphical information system) available eventually, though it realizes that current wireless networks are not well-suited for such intensive graphical content. The goal for all these applications is to provide reliable remote operation with preferably the same user interface as a direct LAN connection. Though slower response times are acceptable and somewhat inevitable, applications must operate in a reliable and effective manner.

The utility has two types of remote workers who will use the wireless system: leads that will use MAXIMO primarily and crew chiefs that will use the office applications in addition to MAXIMO. Because it is difficult to predict what applications may be needed in the future, a key goal is to provide a flexible wireless architecture that allows new applications to be added easily.

Another goal is security. Wireless connections should be no less secure than existing remote access methods based on dial-up connections. Finally, while the utility is willing to commit to a particular wireless technology in its initial deployment, it wants an approach that allows it to migrate easily to other wireless technologies in the future.

Choosing the Computing Platform

The utility recently adopted the Microsoft Windows* 95 platform across multiple departments. For the wireless IP project, it needed to decide whether to use Windows 95 notebook computers or to consider a somewhat more specialized platform such as Windows CE.

Though MAXIMO client software is not available for Windows CE, Windows CE was an option because Syclo Corporation (Barrington, Illinois) supplies middleware that enables Windows CE computers to access MAXIMO databases through a gateway. Using Windows CE would have provided advantages such as lower device cost, greater portability and longer battery life.

Despite some of the advantages of Windows CE, the utility was concerned about the range of applications it could deploy on the platform. Because the utility expects the requirements for mobile workers to evolve over time, and for the types of work performed in the field to expand, it needs the greatest degree of flexibility possible for the types of applications it can deploy. For this overwhelming reason, the utility chose Windows 95 over Windows CE. In addition, because the computers are mounted in the vehicles and not used outside the vehicles, the extra portability Windows CE was not a factor. Finally, there are a number of ruggedized laptops available that can address the demanding field conditions that utility workers encounter.

Choosing the Wireless Network

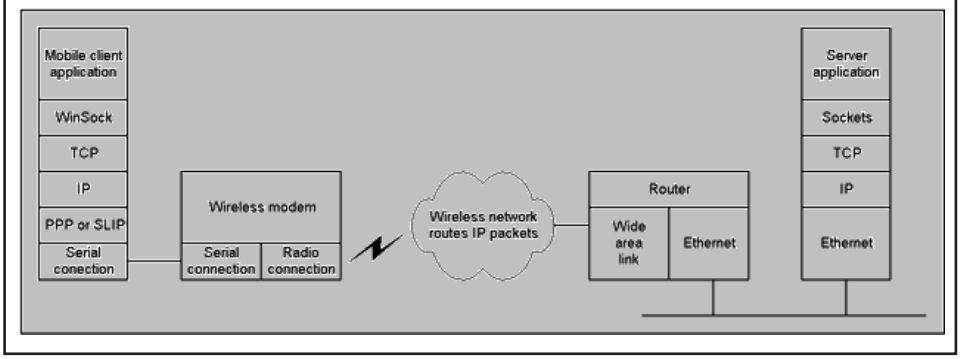
The utility faced a bewildering situation when it began evaluating the wireless networks available. There was the analog cellular network, new digital cellular and PCS technologies, and four wireless packet networks with service in the Seattle area.

Contd...

Notes

The utility decided to base their applications on TCP/IP communications, so this quickly disqualified the BellSouth Wireless Data and ARDIS networks which do not directly support TCP/IP. Moreover, the utility believed that a packet-based approach would better support the frequent communications that workers in the field require. This requirement eliminated circuit-switched cellular connections. Since packet-based services are not yet available for digital PCS networks, the remaining choices were CDPD and the Metricom Ricochet* network. CDPD and Metricom Ricochet* are both IP-based packet networks. However, data services for GSM and CDMA digital PCS networks are expected to be deployed in the 1999 time frame and so may be candidates in the future.

Figure 1: The Utility Chose a Wireless Network that is IP-packet Based for Greatest Flexibility



Since wireless data services are evolving rapidly, the utility decided to implement an architecture that insulates its applications from the actual network used to the maximum extent possible. Using an IP-based approach, where applications make no assumptions about the nature of the physical connection, achieves this goal. This is not unlike Internet-based communications, where packets may flow across copper cable, one moment; fiber optic cable, the next; and a satellite. It should be possible to deploy applications using one wireless network; and with minimal effort, migrate the application to another wireless network in the future, should that network become more desirable.

Migrating between network types is indeed possible, though some adjustments may be necessary for each network. For example, CDPD uses fixed IP addresses and Metricom Ricochet uses dynamically assigned addresses. This difference could affect how firewalls are configured. The effective throughput rates of Ricochet and CDPD also differ, with Ricochet operating at 20 to 30 Kbps and CDPD at about 10 Kbps.

Software Approaches

In an ideal world, a computer connected over a wireless network would work just like a computer on a LAN. But wireless networks operate at lower speeds with higher latency, and connections can be lost at any moment, especially when mobile. The utility has considered a number of software approaches, seeking to strike a balance among these factors: ease of use, performance, reliability, and cost of deployment. To complicate matters, it discovered that the best approach for supporting one application is not always the best approach for another.

The first approach is to use all applications in their native form, with client software installed on the mobile computer and communicating using TCP/IP protocols. Because some workers will be working with the same applications both in an office environment and in the field, the advantage of this approach is that the user interface stays the same in both environments. Also, IT managers can set up mobile computers in the same way as desktop computers. A disadvantage is that this approach does not address some of

Contd...

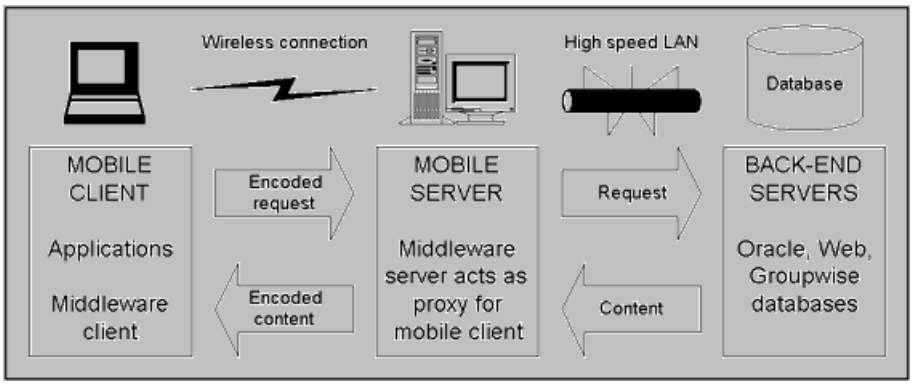
Notes

the connectivity issues associated with wireless, such as throughput and latency. Another disadvantage is the requirement for software installation on field computers, which can add to maintenance and support.

Another approach is to use Citrix MetaFrame* (combined with Microsoft Terminal Server), where applications run on an application server at a central location, and mobile nodes operate as terminals (thin clients). The utility has already deployed Citrix MetaFrame to support dial-up users. The advantage of this approach is that installing and maintaining mobile computers is simplified because they only need the Citrix client software to access multiple applications. The disadvantage is that Citrix MetaFrame has some significant limitations when operating over wide area wireless connections. We learn about these limitations in the next section when we look at test results.

The third approach is to use wireless middleware (specialized software installed on a mobile computer and on a centralized server that acts as an intermediary between client applications and server processes) to optimize communications. The utility has looked at wireless middleware designed specifically for MAXIMO, as well as general purpose middleware that optimizes IP communications over wireless links. The advantage of wireless middleware is it allows applications to run with much better response times and much greater reliability, however, it increases complexity and adds cost.

Figure 3: Wireless Middleware Adds a Mobile Server that Handles Transactions on Behalf of the Mobile Client



Because wireless coverage is not always available everywhere the workers spend time, an approach also considered was Oracle Lite where workers can download a subset of the database they need, operate on it locally during the day, and then synchronize at the end of the day. This approach reduces the demand for wireless connectivity, but it is not as flexible as the other approaches where field workers remain in constant communications during the day and can respond quickly to changing circumstances.

By using a flexible computing platform such as Windows 95 on a laptop, the utility realized it could also consider a mix of approaches. Perhaps one application would work best in its native form, and another would work best using a thin-client approach. This indeed was the case as we see next.

Test Results

Whereas architecting different wireless approaches on paper may be an entertaining diversion, it is difficult to predict how the approaches will actually perform until tested in the real world. The utility has tested the architectures discussed earlier with results that did not always match expectations. For instance, the utility expected that an IP-based client would perform reasonably well over a wireless IP connection. This was the case for certain

Contd...

Notes

applications but not for others, which performed better using a different approach. Testing emphasized three scenarios:

Given the slower speed of wireless connections, what are the issues when starting (and restarting) sessions and applications?

How do applications perform once started, under normal operating conditions?

What happens when a connection is lost due to driving outside a coverage area or to strong interference?

Interestingly, every application and every software approach performed somewhat differently under the three different test scenarios.

Here are the various configurations and how they performed.

Remote IP-based Clients

The first configuration tested was with remote clients, specifically MAXIMO and Web browser clients installed on laptops using TCP/IP communications. The version of GroupWise used at the time did not provide a TCP/IP client, so GroupWise could not be tested using this configuration.

Because both Metricom Ricochet and CDPD are based on IP, the applications operate in the same fashion as if installed on LAN-based workstations using TCP/IP protocol stacks. What is different, of course, is the slower speed of wireless connections. Also, the mobile nodes are not necessarily always in wireless coverage. The first comprehensive series of tests used the Metricom Ricochet network. Compared to CDPD, Ricochet has higher average throughput but it does not support seamless hand-offs between base stations. This means that active applications may lose their connections when the vehicle drives out of range of the original base station.

In looking at the first test scenario (how applications started), Web applications experienced no problems. But MAXIMO would sometimes require more than five minutes during the logon process. Subsequent research revealed that because MAXIMO is an Oracle database application, large data dictionaries are downloaded at startup. This is clearly not acceptable in a field environment. Fortunately, it is possible to cache local versions of these dictionaries on a local hard disk. Such up-front synchronization is common to many applications and is often a performance issue for wireless communications.

Once connected (the second test scenario), the Web client performed acceptably as long as the content was more textual than graphical. MAXIMO, in contrast, ran extremely slowly. Opening new modules (e.g., the inventory module or the work-order module) within MAXIMO would take 60 to 90 seconds. Once a module opens, a screen update (such as looking at a new order) would take about 30 seconds. It is easy to understand why operations were so slow. Oracle transactions, based on SQL, involve a considerable amount of back-and-forth traffic. The slow screen updates make a remote MAXIMO client practically unusable. However, users entering text in either application posed no problems.

The last operating scenario examined the effect of lost connections. The Web client was highly tolerant of intermittent connections, which was expected since HTML applications are stateless; each page entails a new TCP connection. With MAXIMO running, a dropped connection would generate an error message for transactions in process and result in the module closing; but the overall session is maintained. If no transactions were in progress, MAXIMO readily tolerated the underlying connection being lost and regained.

Citrix MetaFrame

The second software scenario tested was the thin-client approach using Citrix MetaFrame. Starting a remote MetaFrame session over a wireless connection took about 60 seconds.

Contd...

Notes

Once the session was started, application startup was not an issue at all, which was expected since the applications run on an application server that has a high speed LAN connection to back-end services. Screen updates for all applications tested (MAXIMO, Web client and GroupWise) ranged from 10 to 15 seconds. This was about the same speed as a remote Web client but significantly faster than a remote MAXIMO client.

The biggest problem with using MetaFrame, however, is that it is not tolerant of intermittent connections. Even in the absence of any application processing, driving out of range of the Metricom base station would terminate the MetaFrame session as well as all the application sessions. With this architecture, text input proved very slow for all applications—not surprising since every character typed by the user would have to be echoed over the wireless link by the application server.

Wireless Middleware

The last architecture tested was wireless middleware. The particular middleware chosen for testing was Smart IP* from Nettech Systems, Inc. Smart IP has a number of different capabilities, but the one of greatest interest is its ability to make IP communications more efficient over wireless networks. It achieves its efficiency through a number of mechanisms, including compression as well as replacing TCP with its own wireless-optimized transport protocols. These transport protocols are used over the wireless connection between the middleware client software that is installed on the mobile computer and the mobile server as Figure 3 shows. The net result is transmission of fewer and smaller packets.

Actual test results with Smart IP showed noticeable data transfer gains. Using a browser application, Smart IP reduced the time required to download pages by an average of about 25%. For example, a page that took 20 seconds to download without Smart IP would on average take 15 seconds with Smart IP. The utility tried to configure Smart IP to operate directly with MAXIMO, but tests were postponed due to configuration difficulties.

The utility found that different applications worked better using different approaches. Only through testing could the utility determine how their applications would function in a wireless environment. Though applications generally ran slower than over dial-up modem connections, with the right approach, applications run well enough to be deployed in the field. The utility also found that the number of software approaches available increased during the course of its project.

The Changing Application Landscape

Computer technology continues to evolve rapidly, as software vendors keep revising and improving their applications. The utility experienced a number of changes that had implications on their wireless strategy. In particular, the number of software approaches available to support wireless networking expanded.

The utility upgraded from GroupWise version 4.1 to version 5.2. With the older 4.1 version there was no easy way to provide remote access other than by using Citrix MetaFrame. But version 5.2 includes TCP/IP support as well as a Web browser client thus adding two new paths for providing remote wireless access. The most attractive approach appears to be the TCP/IP client; testing is under way to confirm this.

Another change involves PSDI, the maker of MAXIMO. Realizing the importance of wireless communications for field service workers, PSDI began to architect their next generation of software to better support wireless networking. In the new version, MAXIMO offers a Web-based interface to mobiles using HTML protocols. HTML is a far more efficient approach than extending the SQL database protocols all the way to the mobile computer. This new "wireless friendly" version of MAXIMO is release 4 and the utility plans to upgrade from release 3. Once it does, the Web interface to MAXIMO will probably be the preferred approach for mobile field workers.

Contd...

Notes

As the utility proceeds with its deployment, and as it expands the number of field workers using wireless networking, it will need to rely on a hybrid set of approaches to address their application needs. In some cases, the utility will run applications in their normal LAN-based or modem-based modes. In other cases, the utility will take advantage of wireless middleware products. And for other applications, a thin-client software approach may be the most effective.

By using a strategy that includes an IP-based communications infrastructure and a flexible computing platform, combining the various software approaches is completely feasible. Such a strategy provides the utility, and any organization for that matter, maximum flexibility when supporting both field workers with specific job functions and office workers with more generalized computing needs.

Source: http://www.rysavy.com/Articles/WirelessIP_case_study/wirelessipcase.htm

7.7 Summary

Heinrich Herz discovered and first produced radio waves in 1888 and by 1894 the modern way to send a message over telegraph wires was first conducted.

A wireless LAN (WLAN) provides network connectivity between devices, also known as stations, by using radio as the communication medium.

Wireless LANs have many applications in the real world. They are frequently used to enhance a wired network, not to completely replace them.

WLANs use radio, infrared and microwave transmission to transmit data from one point to another without cables. Therefore WLAN offers way to build a Local Area Network without cables.

There are many technologies that can be used to design a wireless LAN solution. Some of them are discussed below.

Narrowband Technology

Spread Spectrum Technology

Frequency-Hopping Spread Spectrum Technology

Direct-Sequence Spread Spectrum Technology

Infrared Technology

Wireless PANs don't require much battery power to operate, making them ideal for small user devices, such as audio headsets, cell phones, PDAs, game controls, GPS units, digital cameras, and laptops.

Small office/home office (or single office/home office; SOHO) refers to the category of business or cottage industry that involves from 1 to 10 workers.

7.8 Keywords

Wireless LAN (WLAN): provides network connectivity between devices, also known as stations, by using radio as the communication medium.

Frequency Hopping Spread Spectrum (FHSS): uses a narrowband carrier that changes frequency in a pattern known to both transmitter and receiver.

Direct Sequence Spread Spectrum (DSSS): generates a redundant bit pattern for each bit to be transmitted.

Narrowband Technology: In radio, narrowband describes a channel in which the bandwidth of the message does not significantly exceed the channel's coherence bandwidth.

Notes

Spread Spectrum Technology: In telecommunication and radio communication, spread-spectrum techniques are methods by which a signal (e.g. an electrical, electromagnetic, or acoustic signal) generated with a particular bandwidth is deliberately spread in the frequency domain, resulting in a signal with a wider bandwidth.

Frequency hopping: is one of two basic modulation techniques used in spread spectrum signal transmission.

Infrared radiation: is the region of the electromagnetic spectrum between microwaves and visible light.

Small office/home office: refers to the category of business or cottage industry that involves from 1 to 10 workers.

7.9 Review Questions

1. Write a brief the history of wireless LAN.
2. Describe the wireless LAN network.
3. What are the components of wireless LAN?
4. Discuss the SOHO application Notes.
5. Describe about public wireless LAN network.
6. Explain the ad hoc wireless LAN network.

Answers: Self-Assessment

1. 802.11
2. Access point (AP).
3. Direct Sequence Spread
4. Narrowband
5. 300–3400
6. Minimum
7. infrared radiation
8. wireless access point (WAP)
9. IEEE 802.11
10. Radiated
11. personal area network
12. radio
13. decentralized
14. Ad hoc network
15. Packet radio

7.10 Further Readings

Books

802.11 Wireless Networks: The Definitive Guide, Second Edition, Matthew Gast

Introduction to wireless networks, John Ross

Wireless Communications & Networking, Vijay Garg

Wireless Communications: Principles and Practice, Theodore S. Rappaport

Online links

http://simple.wikipedia.org/wiki/Wireless_LAN

http://www.usr.com/download/whitepapers/wireless-wp.pdf

http://www.motorolasolutions.com/IN-EN/Business+Product+and+Services/Wireless+LAN