Topic 6 Notes

6.1 Introduction

Many people use wireless networking, also called Wi-Fi or 802.11 networking, to connect their computers at home, and some cities are trying to use the technology to provide free or low-cost Internet access to residents. In the near future, wireless networking may become so widespread that you can access the Internet just about anywhere at any time, without using wires. Wi-Fi has a lot of advantages. Wireless networks are easy to set up and inexpensive. They're also unobtrusive -- unless you're on the lookout for a place to use your laptop, you may not even notice when you're in a hotspot.

Fig 6.1: Wi-Fi hotspot

6.2 Wi-Fi

A wireless network uses radio waves, just like cell phones, televisions and radios do. In fact, communication across a wireless network is a lot like two-way radio communication. Here's what happens: A computer's wireless adapter translates data into a radio signal and transmits it using an antenna. A wireless router receives the signal and decodes it. The router sends the information to the Internet using a physical, wired Ethernet connection. The process also works in reverse, with the router receiving information from the Internet, translating it into a radio signal and sending it to the computer's wireless adapter.

i. The radios used for Wi-Fi communication are very similar to the radios used for walkie-talkies, cell phones and other devices. They can transmit and receive radio waves, and they can convert 1s and 0s into radio waves and convert the radio waves back into 1s and 0s. But Wi-Fi radios have a few notable differences from other radios:

ii. They transmit at frequencies of 2.4 GHz or 5 GHz. This frequency is considerably higher than the frequencies used for cell phones, walkie-talkies and televisions. The higher frequency allows the signal to carry more data.

iii. They use 802.11 networking standards, which come in several flavors: 802.11a transmits at 5 GHz and can move up to 54 megabits of data per second.

It also uses orthogonal frequency-division multiplexing (OFDM), a more efficient coding technique that splits that radio signal into several sub-signals before they reach a receiver. This greatly reduces interference. 802.11b is the slowest and least expensive standard. For a while, its cost made it popular, but now it's becoming less common as faster standards become less

expensive. 802.11b transmits in the 2.4 GHz frequency band of the radio spectrum. It can handle up to 11 megabits of data per second, and it uses complementary code keying (CCK) modulation to improve speeds. 802.11g transmits at 2.4 GHz like 802.11b, but it's a lot faster -- it can handle up to 54 megabits of data per second. 802.11g is faster because it uses the same OFDM coding as 802.11a. 802.11n is the newest standard that is widely available. This standard significantly improves speed and range. For instance, although 802.11g theoretically moves 54 megabits of data per second, it only achieves real-world speeds of about 24 megabits of data per second because of network congestion. 802.11n, however, reportedly can achieve speeds as high as 140 megabits per second. The standard is currently in draft form -- the Institute of Electrical and Electronics Engineers (IEEE) plans to formally ratify 802.11n by the end of 2009.

Other 802.11 standards focus on specific applications of wireless networks, like wide area networks (WANs) inside vehicles or technology that lets you move from one wireless network to another seamlessly.

Wi-Fi radios can transmit on any of three frequency bands. Or, they can "frequency hop" rapidly between the different bands. Frequency hopping helps reduce interference and lets multiple devices use the same wireless connection simultaneously.

As long as they all have wireless adapters, several devices can use one router to connect to the Internet. This connection is convenient, virtually invisible and fairly reliable; however, if the router fails or if too many people try to use high-bandwidth applications at the same time, users can experience interference or lose their connections.

6.2.1 Wi-Fi Hotspots

If you want to take advantage of public Wi-Fi hotspots or start a wireless network in your home, the first thing you'll need to do is make sure your computer has the right gear. Most new laptops and many new desktop computers come with built-in wireless transmitters. If your laptop doesn't, you can buy a **wireless adapter** that plugs into the PC card slot or USB port. Desktop computers can use USB adapters, or you can buy an adapter that plugs into the PCI slot inside the computer's case. Many of these adapters can use more than one 802.11 standard. Once you've installed your wireless adapter and the drivers that allow it to operate, your computer should be able to automatically discover existing networks. This means that when you turn your computer on in a Wi-Fi hotspot, the computer will inform you that the network exists and ask whether you want to connect to it. If you have an older computer, you may need to use a software program to detect and connect to a wireless network.

6.3 Building a WiFi Network

If you already have several computers networked in your home, you can create a wireless network with a wireless access point. If you have several computers that are not networked, or if you want to replace your Ethernet network, you'll need a wireless router. This is a single unit that contains:

i. A port to connect to your cable or DSL modem
ii. A router
iii. An Ethernet hub
iv. A firewall
v. A wireless access point

A wireless router allows you to use wireless signals or Ethernet cables to connect your computers to one another, to a printer and to the Internet. Most routers provide coverage for

about 100 feet (30.5 meters) in all directions, although walls and doors can block the signal. If your home is very large, you can buy inexpensive range extenders or repeaters to increase your router's range.

As with wireless adapters, many routers can use more than one 802.11 standard. 802.11b routers are slightly less expensive, but because the standard is older, they're slower than 802.11a, 802.11g and 802.11n routers. Most people select the 802.11g option for its speed and reliability. Once you plug in your router, it should start working at its default settings. Most routers let you use a Web interface to change your settings. You can select:

i. The name of the network, known as its service set identifier (SSID) -- The default setting is usually the manufacturer's name.
ii. The channel that the router uses -- Most routers use channel 6 by default. If you live in an apartment and your neighbors are also using channel 6, you may experience interference. Switching to a different channel should eliminate the problem.
iii. Your router's security options -- Many routers use a standard, publicly available sign on, so it's a good idea to set your own username and password.

Security is an important part of a home wireless network, as well as public Wi-Fi hotspots. If you set your router to create an open hotspot, anyone who has a wireless card will be able to use your signal. Most people would rather keep strangers out of their network, though. Doing so requires you to take a few security precautions. It's also important to make sure your security precautions are current.

To keep your network private, you can use one of the following methods:

i. Wi-Fi Protected Access (WPA) is a step up from WEP and is now part of the 802.11i wireless network security protocol. It uses temporal key integrity protocol (TKIP) encryption. As with WEP, WPA security involves signing on with a password. Most public hotspots are either open or use WPA or 128-bit WEP technology, though some still use the vulnerable WEP approach.
ii. Media Access Control (MAC) address filtering is a little different from WEP or WPA. It doesn't use a password to authenticate users -- it uses a computer's physical hardware. Each computer has its own unique MAC address. MAC address filtering allows only machines with specific MAC addresses to access the network. You must specify which addresses are allowed when you set up your router. This method is very secure, but if you buy a new computer or if visitors to your home want to use your network, you'll need to add the new machines' MAC addresses to the list of approved addresses. The system isn't foolproof. A clever hacker can **spoof** a MAC address -- that is, copy a known MAC address to fool the network that the computer he or she is using belongs on the network.

6.3.1 Wireless Application Protocol (WAP) and the Cellular Explosion

Probably the most important factor in the birth of wireless Internet has been the proliferation of digital cell phones in the last few years. The expanding network of digital cellular and personal communication services (**PCS**) has created a solid foundation for wireless Internet services. It is estimated that there are more than 50 million Web-enabled cell phones in use. In 1997, Nokia, Motorola, Ericsson and Phone.com came together to create the WAP because they believed that a universal standard is critical to the successful implementation of wireless Internet. Since then, more than 350 companies have joined them in the WAP Forum.

Making a Web site accessible through a wireless device is quite a challenge. So far, only a small portion of the more than a billion Web sites provide any wireless Internet content. As the use of WAP-enabled devices grows, you can expect that many more Web sites will be interested in creating wireless content.
WAP is designed to work on any of the existing wireless services, using standards such as:

i. Short Message Service (SMS)
ii. High-Speed Circuit-Switched Data (CSD)
iii. General Packet Radio Service (GPRS)
iv. Unstructured Supplementary Services Data (USSD)

6.4 Satellite Communication

Satellite communication is one type of self-contained wireless communication technology, it is widely spread all over the world to allow users to stay connected almost anywhere on the earth. When the signal (a beam of modulated microwave) is sent near the satellite then, satellite amplifies the signal and sent it back to the antenna receiver which is located on the surface of the earth. Satellite communication contains two main components like the space segment and the ground segment. The ground segment consists of fixed or mobile transmission, reception and ancillary equipment and the space segment, which mainly is the satellite itself.

Fig 6.1:Satellite Communication

6.5 Infrared Communication

Infrared wireless communication communicates information in a device or systems through IR radiation. IR is electromagnetic energy at a wavelength that is longer than that of red light. It is used for security control, TV remote control and short-range communications. In the electromagnetic spectrum, IR radiation lies between microwaves and visible light. So, they can be used as a source of communication

Fig 6.2: Infrared Communication

For a successful infrared communication, a photo LED transmitter and a photo diode receptor are required. The LED transmitter transmits the IR signal in the form of non-visible light, that is captured and saved by the photoreceptor. So the information between the source and the target is transferred in this way. The source and destination can be mobile phones, TVs, security systems, laptops etc supports wireless communication.

6.6 Broadcast Radio

The first wireless communication technology is the open radio communication to seek out widespread use, and it still serves a purpose nowadays. Handy multichannel radios permit a user to speak over short distances, whereas citizen's band and maritime radios offer communication services for sailors. Ham radio enthusiasts share data and function emergency communication aids throughout disasters with their powerful broadcasting gear, and can even communicate digital information over the radio frequency spectrum.

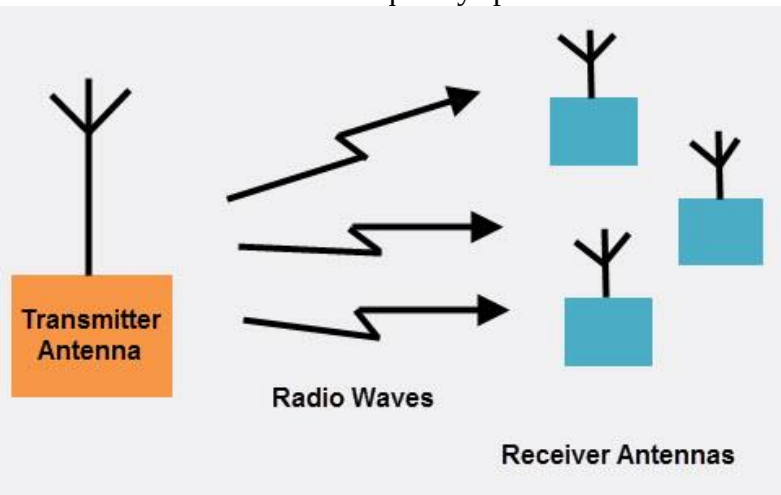

Fig 6.3: Broadcast Radio

Mostly an audio broadcasting service, radio broadcasts sound through the air as radio waves. Radio uses a transmitter which is used to transmit the data in the form of radio waves to a receiving antenna. To broadcast common programming, stations are associated with the radio N/W's. The

broadcast happens either in simulcast or syndication or both. Radio broadcasting may be done via cable FM, the net and satellites. A broadcast sends information over long distances at up to two megabits/Sec (AM/FM Radio).
Radio waves are electromagnetic signals, that are transmitted by an antenna. These waves have completely different frequency segments, and you will be ready to obtain an audio signal by changing into a frequency segment.
For example, you can take a radio station. When the RJ says you are listening to 92.7 BIG FM, what he really means is that signals are being broadcasted at a frequency of 92.7megahertz, that successively means the transmitter at the station is periodic at a frequency of 92.700,000 Cycles/second.
When you would like to listen to 92.7 BIG FM, all you have to do is tune the radio to just accept that specific frequency and you will receive perfect audio reception.

6.7 Microwave Communication

Microwave wireless communication is an effective type of communication, mainly this transmission uses radio waves, and the wavelengths of radio waves are measured in centimeters. In this communication, the data or information can be transfers using two methods. One is satellite method and another one is terrestrial method.

Fig 6.4: Microwave Communication

Wherein satellite method, the data can be transmitted though a satellite, that orbit 22,300 miles above the earth. Stations on the earth send and receive data signals from the satellite with a frequency ranging from 11GHz-14GHz and with a transmission speed of 1Mbps to 10Mbps. In terrestrial method, in which two microwave towers with a clear line of sight between them are used, ensuring no obstacles to disrupt the line of sight. So it is used often for the purpose of privacy. The frequency range of the terrestrial system is typically 4GHz-6GHz and with a transmission speed is usually 1Mbps to 10Mbps.
The main disadvantage of microwave signals is, they can be affected by bad weather, especially rain.

6.8 Bluetooth Technology

Bluetooth technology allows you to connect a variety of different electronic devices wirelessly to a system for the transfer and sharing of data and this is the main function of Bluetooth. Cell phones

are connected to hands-free earpieces, wireless keyboard, mouse and mike to laptops with the help of Bluetooth as it transmits information from one device to another device. Bluetooth technology has many functions, and it is used most commonly in wireless communications' market.

Fig 6.5: Bluetooth Technology

Features

i. Bluetooth technology uses radio waves to communicate between devices. Most of these radio waves have a range of 15-50 feet.
ii. According to the official Bluetooth website, Bluetooth uses a low-power signal with a maximum range of 50 feet with sufficient speed to enable transmission of data.
iii. The pairing process identifies and connects any two devices to each other. It also prevents interference from other non-paired Bluetooth devices in the area.
iv. It uses maximum power only when it is required, thus preserving battery life.

6.9 ZigBee

ZigBee is a wireless communication standard designed to address the unique needs of low-power, low-cost wireless sensor, and control networks. ZigBee can be used almost anywhere, as it is easy to implement and requires little power to operate. Zigbee has been developed looking into the needs of the communication of data with a simple structure like the data from the sensors.

Fig 6.6: Zigbee Technology

Features

i. ZigBee devices are designed for low-power consumption.
ii. ZigBee is used in Commercial Applications like sensing and monitoring applications.
iii. ZigBee uses very low power and extremely long device battery life.
iv. ZigBee gives flexibility to do more with the reliable wireless performance and battery operation.

Revision questions

1. What is wireless technology
2. How does Wi-Fi differ from WiMAX?
3. What are the requirements for setting up a Wi-Fi hotspot?
4. Why is infrared referred to as LoS technology?
5. How does Bluetooth facilitate communication between two devices?