Wireless Networks

DCAP311/DCAP607

LOVELY PROFESSIONAL UNIVERSITY

LOVELY
PROFESSIONAL
UNIVERSITY

WIRELESS NETWORKS

Produced & Printed by
EXCEL BOOKS PRIVATE LIMITED
A-45, Naraina, Phase-I,
New Delhi-110028
for
Lovely Professional University
Phagwara

CONTENTS

Unit 1:	Introduction to Wireless Networks	1
Unit 2:	Wireless System Architecture	23
Unit 3:	Radio Frequency and Light Signal Fundamentals	41
Unit 4:	Wireless Networks Types and PAN Technologies	59
Unit 5:	Wireless PAN Components	76
Unit 6:	Wireless PAN Systems	89
Unit 7:	Wireless LAN	105
Unit 8:	Wireless MAN	126
Unit 9:	Wireless MAN Systems	140
Unit 10:	Wireless MAN Technologies	153
Unit 11:	Wireless WAN	165
Unit 12:	Space-based Wireless WANs	182
Unit 13:	Wireless Networks Security	206
Unit 14:	Authentication	220

SYLLABUS

Wireless Networks

Objectives: To enable the student to understand architecture of wireless network, wireless LAN, WAN and MAN. Student can manage security and authentication on wireless networks.

Sr. No.	Topics
1.	**Introduction to Wireless Networks**. IEEE Standards for Wireless Networks. Wireless Networks Applications. Types of Wireless Networks. Benefits of Wireless Networks.
2.	**Wireless System Architecture**: Wireless System Components, Network Architecture. Information Signals. **Radio Frequency and Light Signal Fundamentals**: Wireless Transceivers, understanding RF Signals, Working of Light Signals
3.	**Types of Wireless Networks**: WPAN, WLAN, WMAN **Wireless PAN:** Components: User Devices, Radio NIC, USB Adapters, Wireless Routers, Bluetooth Dongles etc. **Wireless PAN Systems:** SOHO Equipments, Printing, Accessing Internet, Accessing PDA's, Mobile Phones **Wireless PAN Technologies**: IEEE 802.15. Bluetooth Version 1 and Version 2.
4.	**Wireless LAN:** Meaning, Components: User Devices, Radio NIC's, Access Points, Routers, Repeaters, And Antennae. **SOHO Applications**: Internet Access, Printing, Remote Accessing. Public Wireless LAN's, and AdHoc Wireless LAN's
5.	**Wireless MAN:** Meaning and Components: Bridges, Bridges Vs. Access Points, Ethernet to Wireless Bridges, Workgroup Bridges
6.	**Wireless MAN Systems:** Point to Point Systems, Point to Multi Point, Packet Radio Systems.
7.	**Wireless WAN:** WAN User Devices, Base Stations, Antennae. **Wireless WAN Systems:** Cellular-Based Wireless WANs, First-Generation Cellular**,** Second-Generation Cellular, Third-Generation Cellular.
8.	**Space-Based Wireless WANs:** Satellites, Meteor Burst Communications
9.	**Wireless Networks Security:** Security Threats, Unauthorized Access, Middle Attacks, DoS Attack (Denial of Service).

Sr. No.	Topics
1.	**Introduction to Wireless Networks**. IEEE Standards for Wireless Networks. Wireless Networks Applications. Types of Wireless Networks. Benefits of Wireless Networks.
2.	**Wireless System Architecture**: Wireless System Components, Network Architecture. Information Signals. **Radio Frequency and Light Signal Fundamentals**: Wireless Transceivers, understanding RF Signals, Working of Light Signals, Modulation: Sending Data packets in the Air.
3.	**Types of Wireless Networks**: WPAN, WLAN, WMAN **Wireless PAN:** Components: User Devices, Radio NIC, USB Adapters, Wireless Routers, Bluetooth Dongles etc. **Wireless PAN Systems:** SOHO Equipments, Printing, Accessing Internet, Accessing PDA's, Mobile Phones **Wireless PAN Technologies**: IEEE 802.15. Bluetooth Version 1 and Version 2.
4.	**Wireless LAN:** Meaning, Components: User Devices, Radio NIC's, Access Points, Routers, Repeaters, And Antennae. **SOHO Applications**: Internet Access, Printing, Remote Accessing. Public Wireless LAN's, and AdHoc Wireless LAN's
5.	**Wireless MAN:** Meaning and Components: Bridges, Bridges Vs. Access Points, Ethernet to Wireless Bridges, Workgroup Bridges, Directional Antennae's, Semi-Directional, Polarization.
6.	**Wireless MAN Systems:** Point to Point Systems, Point to Multi Point, Packet Radio Systems. **Wireless MAN Technologies:** IEEE 802.11 and Wi-Fi and also purpose of IEEE 802.16 Standard
7.	**Wireless WAN:** WAN User Devices, Base Stations, Antennae. **Wireless WAN Systems:** Cellular-Based Wireless WANs, First-Generation Cellular**,** Second-Generation Cellular, Third-Generation Cellular, SMS Application.
8.	**Space-Based Wireless WANs:** Satellites, Meteor Burst Communications
9.	**Wireless Networks Security:** Security Threats, Traffic Monitoring, Unauthorized Access, Middle Attacks, DoS Attack (Denial of Service). **Protective Actions:** WEP, WEP issues, WPA, VPN.
10.	**Authentication:** 802.11 Authentication Vulnerabilities, MAC Filters, Authentication Using Public Key Cryptography, 802.1x , Security Policies.

Unit 1: Introduction to Wireless Networks

CONTENTS

Objectives

Introduction

1.1 Wireless Networking

1.1.1 Advantage of Wireless Networking

1.1.2 Needs of Wireless Networking

1.2 IEEE Standards for Wireless Networks

1.3 Wireless Networks Applications

1.3.1 Internet Access

1.3.2 Voice over Wireless

1.3.3 Inventory Control and Healthcare

1.3.4 Education and Real Estate

1.3.5 Utilities

1.3.6 Field Service

1.3.7 Field Sales

1.3.8 Vending

1.3.9 Public Networks

1.3.10 Location-based Services

1.4 Types of Wireless Network

1.4.1 Wireless PANs

1.4.2 Wireless LANs

1.4.3 Wireless MANs

1.5 Benefits of Wireless Networks

1.6 Summary

1.7 Keywords

1.8 Review Questions

1.9 Further Readings

Objectives

After studying this unit, you will be able to:

- Describe the wireless network
- Explain the IEEE standards for wireless networks
- Explain the wireless networks applications
- Discuss the types of wireless networks
- Discuss the benefits of wireless networks

Notes

Introduction

Wireless network refers to any type of computer network that uses wireless (usually, but not always radio waves) for network connections.

It is a method by which homes, telecommunications networks and enterprise (business) installations avoid the costly process of introducing cables into a building, or as a connection between various equipment locations. Wireless telecommunications networks are generally implemented and administered using radio communication. This implementation takes place at the physical level (layer) of the OSI model network structure.

Wireless networks use electromagnetic waves to communicate information from one point to another without relying on any physical connection. Radio waves are often referred to as radio carriers because they simply perform the function of delivering energy to a remote receiver. The data being transmitted is superimposed on the radio carrier so that it can be accurately extracted at the receiving end. Once data is superimposed (modulated) onto the radio carrier, the radio signal occupies more than a single frequency, since the frequency or bit rate of the modulating information adds to the carrier. Multiple radio carriers can exist in the same space at the same time without interfering with each other if the radio waves are transmitted on different radio frequencies. To extract data, a radio receiver tunes in one radio frequency while rejecting all other frequencies. The modulated signal thus received is then demodulated and the data is extracted from the signal.

1.1 Wireless Networking

A wireless network is a flexible data communications system, which uses wireless media such as radio frequency technology to transmit and receive data over the air, minimizing the need for wired connections (What is Wireless LAN, White Paper). Wireless networks are used to augment rather than replace wired networks and are most commonly used to provide last few stages of connectivity between a mobile user and a wired network.

Bluetooth and 802.11b have the potential to dramatically alter how people use devices to connect and communicate in everyday life. Bluetooth is a low-power, short-range technology for ad hoc cable replacement; it enables people to wirelessly combine devices wherever they bring them.

Conversely, 802.11b is a moderate-range, moderate-speed technology based on Ethernet; it allows people to wirelessly access an organisational network throughout a campus location. Although the technologies share the 2.4 GHz band, have some potentially overlapping applications, and have been pitted against each other in the press, they do not compete and can even been successfully combined for corporate use.

One thing is clear, wireless technologies will continue to evolve and offer organizations and end users higher standard of life by making us more mobile and increasing our ability to interact with each other, removing distance as a barrier. There will be a time when a traveller can sit in any airport or hotel and surf the Web or connect to the home office and work. Users will be able to surf or work in places such as malls, parks, or (with smaller handheld computers) just walking down the street.

Notes Internet service providers will install larger wireless networks allowing users to connect from anywhere in the city. All of these things are possible with wireless technology.

1.1.1 Advantage of Wireless Networking

The advantages of wireless networking include:

1. Wireless routers are equipped with modem, network switch (a device that has multiple connection ports for connecting computers and other network devices), wireless access points.
2. Wireless Router can be connected to/from anywhere in your immediate environment or house. That means you can log on and surf the Internet from anywhere around your surroundings.
3. Some of the wireless routers are equipped with a built in firewall to ward of intruders. The configuration options of the firewall are an important consideration when buying a router. Virtually everyone buys and sell online one way or the other, buying a wireless router with good firewall configuration options can be helpful for security and privacy.
4. The broadband router wireless VoIP technology enables you to can connect to the Internet, using any ordinary phone device. You can then make calls to anybody in the world via your Internet connection. Wireless router provides strong encryption (WPA or AES) and features the filters MAC address and control over SSID authentication.

1.1.2 Needs of Wireless Networking

Wireless local-area networks (WLAN) have evolved as the quantity and types of mobile devices have increased. The number of devices that support Wi-Fi continues to expand. The term Wi-Fi is an industry acronym meaning wireless fidelity for devices with support for the IEEE 802.11 wireless standard. This means the device has been certified to meet interoperability standards established by the Wi-Fi Alliance. The type of devices that include Wi-Fi support continues to expand from laptops to many other devices, such as cameras, phones, automobiles, and other consumer devices. The uses of Wi-Fi have expanded beyond just data usage, often including voice, video, and innovative contextual applications. Contextual usage is a combination of application data, voice, and video services with information provided by the data network, such as device location, security posture, or access media type information. Contextual applications increase the value or relevance of data service by using the additional metadata provided by the wireless network. An example of a contextual data application would be a repair dispatch system generating work orders, using the WLAN's location information to dispatch the closest technician to repair a failed device.

Many organizations use wireless networks with applications specifically created for the mobile environment, which requires the WLAN to provide secure communications anyplace the user might wander. An example would be a hospital where paper records are no longer utilized. This requires access to the patient's electronic medical record that is available at all locations to provide health services. With pervasive WLAN coverage, further optimization to healthcare quality and costs can be achieved utilizing the WLAN. For example, many diagnostic and monitor systems utilize devices that load patient data through the WLAN directly into the patient's medical record. It is practical today to enable more devices to always be on the network because there is no longer wired network cable encumbering device usage. Regardless of the industry or application, everywhere you turn, people and devices are leveraging an always-on network through WLANs. This has driven more pervasive WLANs to be deployed, with increased size and scope of use. The reliance on WLANs has changed from being a convenience to being a critical edge access method.

WLANs have become an essential component for most organizations and are mission critical for many. The increased reliance on WLANs has increased the coverage, security, performance, and reliability requirements. Numerous impairments to usage of WLANs have been identified as the usage and scale of WLANs have increased. Originally, WLANs were deployed with the use of a relatively simple architecture of standalone enterprise access points (AP). The early WLAN APs were built to simply translate between the radio frequency (RF) media and Ethernet media.

1.2 IEEE Standards for Wireless Networks

Wireless networking hardware requires the use of underlying technology that deals with radio frequencies as well as data transmission. The most widely used standard is 802.11 produced by the Institute of Electrical and Electronic Engineers (IEEE). This is a standard defining all aspects of Radio Frequency Wireless networking.

The Institute of Electrical and Electronic Engineers (IEEE) is a professional organization of electrical engineers that has organized a highly successful and unique standards making activity. Arguably the most successful of these standards making activities has been under the auspices of the IEEE's 802 Committee which is responsible for networking standards at the data link (the Media Access Control or MAC) and physical (the PHYsical) network layers. Subcommittees of the 802 Committee have been responsible for the major networking standards that we use every day:

- ***802.3:*** The entire family of Ethernet standards, defining both local and wide area communication on coaxial cable, twisted pair copper and optical fibre.
- ***802.5:*** The legacy standards of Token Ring for network communication over coaxial cable and twisted pair copper and optical fibre.
- ***802.11:*** The entire family of wireless local area network standards. Commercially known as Wi-Fi.
- ***802.16:*** The entire family of wireless metropolitan area network standards. Commercially known as WiMAX.

In particular, the IEEE 802.11 Subcommittee is responsible for the family of evolving wireless local area network (WLAN) standards:

- ***802.11:*** The original WLAN standard in 1997 using 1 and 2 Mbps PHY in the 2.4 GHz band.
- ***802.11b:*** The enhanced standard for the 2.4 GHz band in 1999 providing 11 Mbps PHY.
- ***802.11a:*** The enhanced PHY standard for the 5 GHz band providing 54 Mbps using OFDM (Orthogonal Frequency Division Multiplexing) modulation in 1999.
- ***802.11g:*** The enhanced PHY standard for the 2.4 GHz band providing 54 Mbps using OFDM with backwards compatibility to 802.11b in 2003.

The variants of 802.11 all use a common MAC protocol. Other auxiliary standards in the family (c–f, h, I, j) are service enhancements and extensions or corrections to previous specifications.

The IEEE 802.11n subcommittee was chartered by its parent IEEE 802.11 committee in 2003 to develop high performance enhancements to these standards. Wi-Fi is a brand of the Wi-Fi Alliance – a commercial organization that certifies interoperability of products implementing the 802.11 IEEE standard and promotes the standard though market education.

Did u know? IEEE 802.11n is the most significant change in the wireless LAN world since the adoption of the original standard in 1997. 802.11n defines enhancements for both the MAC and the PHY. The greatest impact of 802.11n is in the technology used for the PHY. The ability to create low-cost radios in CMOS now allows the simultaneous use of multiple radios and antennas in every client. Advanced signal processing enables 802.11n to integrate multiple radios and a number of other PHY improvements to effectively increase the burst transmission speed and the total system capacity by a factor of ten when all of the new enhancements are used.

Self Assessment

Fill in the blanks:

1. .... is a moderate-range, moderate-speed technology based on Ethernet.
2. Wireless networking hardware requires the use of underlying technology that deals with radio frequencies as well as....................................
3. ....is the most significant change in the wireless LAN world since the adoption of the original standard in 1997.
4. The .... is a professional organization of electrical engineers that has organized a highly successful and unique standards making activity.

1.3 Wireless Networks Applications

The various wireless application networks are as follows:

1.3.1 Internet Access

If you've been in an airport, coffee shop, library or hotel recently, chances are you've been right in the middle of a wireless network. Many people also use wireless networking, also called WiFi 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.

WiFi 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 watch streaming movies on your tablet, you may not even notice when you're in a hotspot.

1.3.2 Voice over Wireless

VoWLAN (Voice over Wireless LAN) is the use of a wireless broadband network according to the IEEE 802.11 standards for the purpose of vocal conversation. In essence, it's VoIP over a Wi-Fi network. In most cases, the Wi-Fi network and voice components supporting the voice system are privately owned.

VoWLAN can be conducted over any Internet accessible device, including a laptop, PDA or the new VoWLAN units which look and function like DECT and cellphones. Just like for IP-DECT, the VoWLAN's main advantages to consumers are cheaper local and international calls, free calls to other VoWLAN units and a simplified integrated billing of both phone and Internet service providers.

Although VoWLAN and 3G have certain feature similarities, VoWLAN is different in the sense that it uses a wireless internet network (typically 802.11) rather than a Cellular network. Both VoWLAN and 3G are used in different ways, although with a Femtocell the two can deliver similar service to users and can be considered alternatives.

A company with fixed warehouses or locations would take advantage of their existing WiFi network and use VoIP (hence VoWLAN) for employees to communicate with one another. This system can also be used like Land Mobile Radio System or Walkie-talkie systems with push to talk and emergency broadcast channels.

Another example would be a company that has mobile workers very much like the FedEx delivery person or the CocaCola delivery driver who delivers goods to a store. These workers need to take advantage of 3G type services whereby a cellular company (like AT&T, Verizon, T-Mobile, Sprint/Nextel) provide data access between the handheld device and the companies back-end network.

Benefits

A voice over WLAN system offers tremendous benefits to organizations, such as hospitals and warehouses. The primary benefits are mobility and cost savings. For example, nurses and doctors within a hospital can maintain voice communications at any time at less cost as compared to cellular service.

1.3.3 Inventory Control and Healthcare

A high performance wireless network can help hospitals in numerous ways. Many benefits of wireless focus around improving quality care, decreasing hospital expenses, and increasing communication between patients, doctors and hospital staff. Here are just three main benefits of mobility in healthcare:

1. ***Asset Tracking & Inventory Management:*** With RFID technology, hospitals can easily reduce the cost associated with loss of medical equipment, such as wheel chairs, infusion pumps and computers-on-wheels. Real Time Tracking capability also allows hospital staff the ability to locate these items quickly. This helps eliminate time spent wasted looking for particular items.

   One of the most effective ways to increase profits is to control or reduce costs. For a hospital, real-time inventory management plays a strong role in cost control. With a clear view into the supply chain, hospitals can control the movement of their assets and maximize the utility of stock locations, such as available or used prescription drug counts.

2. ***Quality of Patient care and Clinical Communications:*** There are many ways that wireless can help increase the quality of patient care. The mobility that doctors have allow them to be present with any patient in any hospital via video conferencing and allows them to view real time patient information instantly. As mobility increases the efficiency of hospital staff, patient care becomes more focused, providing increasing quality and standards.

   Better communication means better care. When clinicians communicate easily, they can diagnose and treat patients more quickly. Clinicians get lab results as soon as they're ready. They can easily access vast medical databases from their smartphones, tablets and other mobile devices. Ultimately, patient outcomes improve.

3. ***Patient & Staff Safety:*** Using Wi-Fi RTLS can easily reduce the amount of safety incidents and improve safety and peace of mind for clinical staff. Many patients, including psychiatric patients, trauma patients and the elderly may pose a risk to themselves by wandering or leaving their hospital bed. Keeping track of any wandering patients can sometimes be the difference between life or death for that patient.

   By leveraging a hospitals existing Wi-Fi network, Wi-Fi RTLS locates all tagged patients at any time, anywhere within the footprint of the network. If a patient is in his room or on his assigned floor, RTLS will locate them. Should a patient walk into the fire escape, Wi-Fi RTLS will alert staff and security about the event.

1.3.4 Education and Real Estate

Wireless networks will play an important role in education. New educational models and wireless architectures have been proposed to enhance collaborative training. Wireless networks can provide a dynamic educational environment. However, the lack of fixed infrastructure in

Notes

wireless networks generates new research problems. This paper examines the ways wireless technology work and the required prerequisites to integrate it into the educational area. It also describes educational opportunities and challenges of teaching in a real time wireless classroom environment. Additionally, this paper refers to the constraints and barriers, which prevent wireless networks from being accepted. It provides educational models and techniques in order to easier the transition from traditional computerized training systems to wireless training systems. Lastly, the paper compares models and architectures in educational wireless networks, taking into consideration the shortages of the educational systems, and predicts future trends and perspectives of integrated educational environments.

1.3.5 Utilities

Trango microwave communications solutions are ideal for a wide variety of industrial applications in the utility, energy, oil & gas sectors. Remote monitoring, video, and site interconnectivity applications require low latency, high reliability, and high capacity capability of licensed band solutions from Trango Systems.

Utility and energy providers require reliable networks to carry critical traffic with advanced information security, high capacities and failsafe reliability. Trango Systems' TrangoLINK Sparta Elite™ is the most secure microwave Ethernet point to point system on the market, utilizing integrated NSA Suite B compliant FIPS-197 certified AES256-GCM real-time encryption. The Sparta Elite is also FIPS140-2 and HIPAA compliant, with secure management interfaces over SSH, HTTPS.

In addition to advanced information security, the Sparta Elite features Intelligent Payload Compression (IPC) which compresses packets in real time to provide capacity improvements up to 2.5 x the raw data rate. If the compression does not yield an improvement, the packet will go through uncompressed. Latency is typically only increased by 100 microseconds and in the case of larger packets may be reduced.

Caution Compression ratio is content variable and can be monitored using the management interface. Both compression and encryption can be used simultaneously.

1.3.6 Field Service

A field service organization has five key applications: billing, systems management for remote devices, corporate IM, a Web-based CRM application and email. The field technicians carry laptops throughout the day, and use them occasionally at home and in a branch office. The laptops have a number of background applications which have been installed by the operating system, such as Windows Update, or come from third parties, such as automated antivirus or printer driver updates.

The field technicians typically spend 32 hours a week in the field and 8 hours at a regional office. While in the field they are connected via a wireless carrier's data network. At the regional office they connect via an in-building wireless LAN.

1.3.7 Field Sales

There's nothing more crucial to your company's bottom line than sales—and yet your sales force may not have the tools they need to be performing at their potential. Ultimately, that means less revenue for the company. Not to mention less satisfied customers.

Wireless software ensures that your sales force stays securely connected to the applications they need to answer customer questions, input data into your CRM and make the sale, all right from the customer site. This means improved service, more sales, and less travel time for sales reps.

Field Sales Can:

- Sell more efficiently by not having to reenter data
- Eliminate the need for return calls by solving customer needs on the spot
- Trim redundant technologies and plans and ensure greater efficiency

1.3.8 Vending

A wireless vending machine system based on the GSM network is developed in this unit. First of all, several methods by which we may realize wireless data communication of GSM network are analysed and compared, the overall structure of vending machine system based on USSD is given an in-depth introduction. Furthermore, control modules which realize data transmission and control function of terminal device, middleware which connects application and BOSS (business operation support system), and transaction software embedded in USSD platform, are also developed respectively. Finally, the operating support system of wireless vending machine system is formed, which can not only integrate vending machines, USSD platform and payment system together, but also manage sale information, logistic information and consumer information online. The vending machine system presented in the unit has been put into use in several provinces and cities for more than two years. All performance indexes of the system are satisfying.

1.3.9 Public Networks

Public WiFi 'hotspots' in places like cafés, airports, hotels and libraries are convenient but unlike your home computer you don't know what security these networks have or who else may be connected.

Wireless enabled laptops or smartphones allow you to easily connect to the Internet no matter where you are. The increasing availability of public WiFi 'hotspots' make getting using them to get online simple.

These networks are often not secured and there is likely to be other people using them at the same time. There is a risk that another user on the network could monitor your activity, steal your data or infect your computer with malicious software.

> *Notes* Because of the added risks you should take additional care about what you do online.

Top Tips

- ***Be careful about which hotspots you use.*** Avoid using hotspots that are run by people you don't know or trust. Criminals can set up hotspots known as 'evil twins' and 'rogue hotspots' to steal users' information.
- ***Install and use anti-virus, anti-spyware and firewall software.*** Keep them activated and up-to-date.
- ***Make sure no-one is watching you.*** By simply looking over your shoulder, someone could steal personal information.
- ***If you can't connect securely using a VPN, then consider avoiding online banking or shopping.*** You should also avoid any sites that require you to enter passwords or sending confidential email.

Notes

- ***Encrypt sensitive information.*** If you keep personal or financial information on your computer, consider taking steps to encrypt and protect sensitive files and folders.
- Disable wireless networking when you are not using it.

Be Careful about Which Hotspots You Use

Avoid using hotspots that are run by people you don't know or trust. Criminals can set up hotspots known as 'evil twins' and 'rogue hotspots' to steal users' information. Use encrypted (password protected) networks. Encrypted networks are wireless networks that require you to log in with a password to use them. Choose networks with WPA2 and WPA encryption if they are available, because they are more secure than other types of encryption.

Connect Using the Right Network Type

When you connect to a WiFi network many devices will prompt you to enter a network type ('home', 'work' or 'pubic'). Always connect as 'public' when you connect to a public WiFi network as this will lock down the connection more securely.

Use a Virtual Private Network (VPN) if Possible

Many companies and organisations have a virtual private network (VPN). VPNs allow employees to connect securely to their office network. VPNs encrypt connections at the sending and receiving ends and keep out traffic that is not properly encrypted.

If a VPN is available to you, make sure you log onto it any time you need to use a public wireless access point.

Be Aware of Your Surroundings

Because you're likely to have an unsecured, unencrypted network connection when you use a public wireless access point, be careful about what you do online there's always the chance that another user on the network could be monitoring your activity.

If you can't connect securely using a VPN, then consider avoiding:

- online banking or shopping
- sending confidential email
- entering passwords or credit card details unless using a secure website

Secure Your Information

- Do not send passwords or credit card details. Criminals using the wireless network can steal them. If you must make sensitive transactions, only use secure websites. Look at the web address for https:// instead of http:// and look for a locked padlock or key in the browser window.
- Encrypt sensitive information. If you keep personal or financial information on your computer, consider taking steps to encrypt and protect sensitive files and folders. Check your computer operating system's help section to find out how to do this.
- Disable wireless networking when you are not using it. Whenever you are connected to the Internet, criminals can try to attack your mobile device and steal your information. Reduce their opportunities to do this by turning off your device's WiFi when you are not using it.

1.3.10 Location-based Services

Location-based services (LBSs) are a general class of computer program-level services used to include specific controls for location and time data as control features in computer programs. As such LBS is an information service and has a number of uses in social networking today as an entertainment service, which is accessible with mobile devices through the mobile network and which uses information on the geographical position of the mobile device. This has become more and more important with the expansion of the smartphone and tablet markets as well.

LBS are used in a variety of contexts, such as health, indoor object search, entertainment, work, personal life, etc.

LBS include services to identify a location of a person or object, such as discovering the nearest banking cash machine (a.k.a. ATM) or the whereabouts of a friend or employee. LBS include parcel tracking and vehicle tracking services. LBS can include mobile commerce when taking the form of coupons or advertising directed at customers based on their current location. They include personalized weather services and even location-based games. They are an example of telecommunication convergence.

This concept of location based systems is not compliant with the standardized concept of real-time locating systems (RTLS) and related local services, as noted in ISO/IEC 19762-5 and ISO/IEC 24730-1.

Self Assessment

Fill in the blanks:

5. A voice over .... system offers tremendous benefits to organizations, such as hospitals and warehouses.
6. With .... technology, hospitals can easily reduce the cost associated with loss of medical equipment, such as wheel chairs, infusion pumps and computers-on-wheels.
7. .... enabled laptops or smartphones allow you to easily connect to the Internet no matter where you are.
8. .... allow employees to connect securely to their office network.

1.4 Types of Wireless Network

A wireless network joins two or more than two computers by means of communication without using any wires. Wireless Networks utilizes spread-spectrum or OFDM depends on the technology which is using. Wireless network enable a user to move about within a wide coverage area and still be associated to the network. There are different types of wireless networking such as wide area network, local area network and personal area network but the most common are of two.

1.4.1 Wireless PANs

Wireless personal area networks (WPANs) interconnect devices within a relatively small area, that is generally within a person's reach. For example, both Bluetooth radio and invisible infrared light provides a WPAN for interconnecting a headset to a laptop. ZigBee also supports WPAN applications. Wi-Fi PANs are becoming commonplace (2010) as equipment designers start to integrate Wi-Fi into a variety of consumer electronic devices. Intel "My WiFi" and Windows 7 "virtual Wi-Fi" capabilities have made Wi-Fi PANs simpler and easier to set up and configure.

These are networks that provide wireless connectivity over distances of up to 10 m or so. At first this seems ridiculously small, but this range allows a computer to be connected wirelessly to a nearby printer, or a cell phone's hands-free headset to be connected wirelessly to the cell phone. The most talked about (and most hyped) technology is called Bluetooth.

Personal Area Networks are a bit different than WANs and WLANs in one important respect. In the WAN and WLAN cases, networks are set up first, which devices then use. In the Personal Area Network case, there is no independent pre-existing network. The participating devices establish an ad-hoc network when they are within range, and the network is dissolved when the devices pass out of range. If you ever use Infrared (IR) to exchange data between laptops, you will be doing something similar. This idea of wireless devices discovering each other is a very important one, and appears in many guises in the evolving wireless world.

PAN technologies add value to other wireless technologies, although they wouldn't be the primary driver for a wireless business solution. For example, a wireless LAN in a hospital may allow a doctor to see a patient's chart on a handheld device. If the doctor's handheld was also Bluetooth enabled, he could walk to within range of the nearest Bluetooth enabled printer and print the chart.

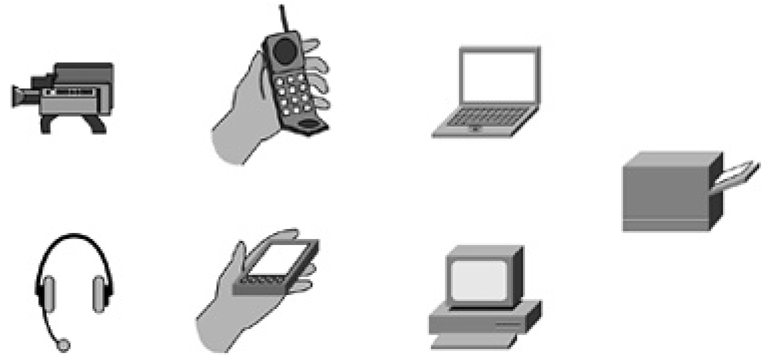
WPANs are short-range networks that use Bluetooth technology. They are commonly used to interconnect compatible devices near a central location, such as a desk. A WPAN has a typical range of about 30 feet.

Wireless PANs make use of both radio and infrared light technologies, which manufacturers embed in many different types of devices.

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 1.1 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.

Figure 1.1: 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/

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.

USB Adapters

Several companies offer a wireless PAN USB adapter (see Figure 1.2), which is also called a wireless dongle. For example, you can purchase a USB Bluetooth adapter and connect it to a USB port on your PC. This makes the PC able to synchronize with other devices having Bluetooth connectivity. Bluetooth which is discussed later is a specification developed for short-range, radio-based transceivers.

Figure 1.2: Bluetooth Wireless USB Adapters Enable PCs and Laptops to Interface with other Bluetooth Devices

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

A PDA utilizing Bluetooth can wirelessly interface with the Bluetooth-enabled PC and synchronize without placing the PDA in a synchronization cradle. A USB connection over Bluetooth, however, is generally slower than having a directly wired interface through the PC's USB port. This is because the wireless USB adapter is mapped to the PC's serial port, which runs slower than the USB port. The wireless solution might be more convenient, but you might need to wait twice as long before synchronization is complete.

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.

Did u know? The advanced technology and development in wireless network topology has unshackled wired communication. Wireless communication technologies are point-to-point, line of sight, scatter, reflective, radio broadcast, satellite, microwave, light-based and cellular technology. The wireless network topologies that are relevant for communication are star, tree, line, mesh and ring.

1.4.2 Wireless LANs

Wireless LAN (WiFi) offers the promise of unhindered access to network resources even outside the reach of a wired setup. In this tutorial, take a closer look at the technical concepts that drive WiFi and how WiFi stacks up against some of the other competing technologies.

Wireless LAN or Wireless Local Area Network is a term to refer to a Local Area Network that does not need cables to connect the different devices. Instead, radio waves are used to communicate. Technologies that can be used to do that include IEEE 802.11 and Bluetooth.

Benefits of Wireless LANs

- 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.

Disadvantages of Wireless LANs

- 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)

Technologies Used

Today, most technologies used for WLANs use Orthogonal Frequency Division Multiplexing. This means that several frequencies are used at the same time. Signals that are close to each other, but that belong to different channels do not disturb each other, as they use different coding schemes. Depending on the material used, it is possible to cover between 30 metres and 100 metres indoors; outdoors, the range is about 100–300 m, if there are no obstacles.

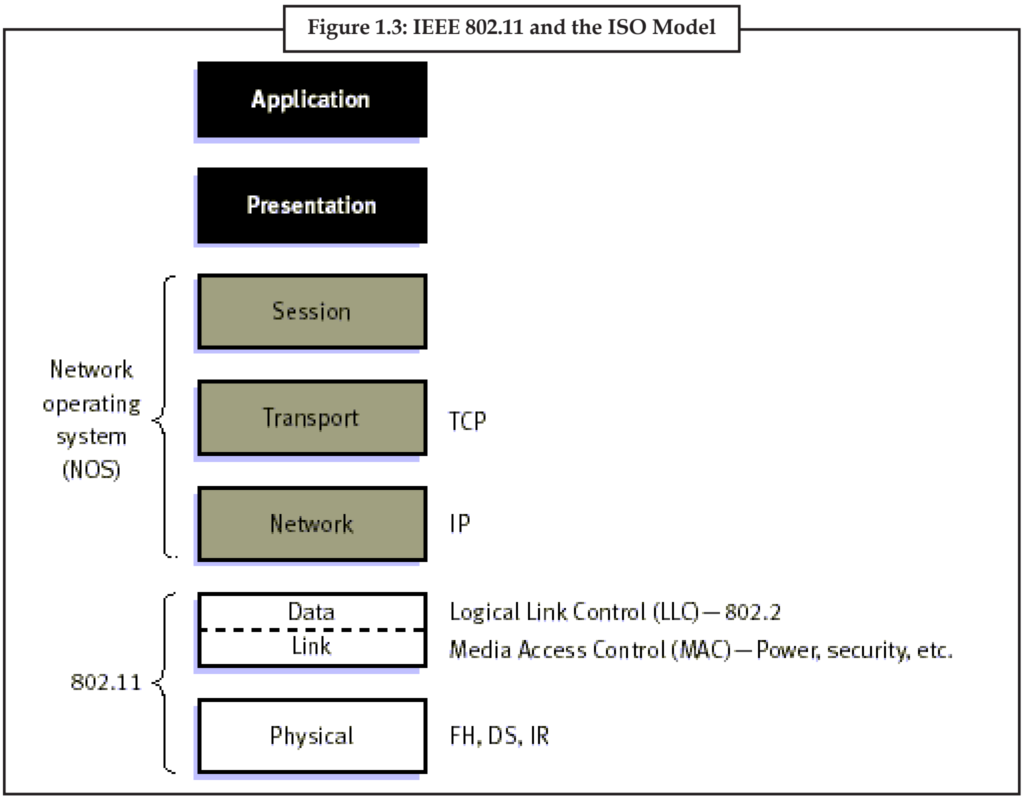
A wireless LAN (WLAN or WiFi) is a data transmission system designed to provide location-independent network access between computing devices by using radio waves rather than a cable infrastructure [IEEE 802.11 Wireless LANs, Technical paper].

In the corporate enterprise, wireless LANs are usually implemented as the final link between the existing wired network and a group of client computers, giving these users wireless access to the full resources and services of the corporate network across a building or campus setting.

The widespread acceptance of WLANs depends on industry standardization to ensure product compatibility and reliability among the various manufacturers.

The 802.11 specification [IEEE Std 802.11 (ISO/IEC 8802-11: 1999)] as a standard for wireless LANS was ratified by the Institute of Electrical and Electronics Engineers (IEEE) in the year 1997. This version of 802.11 provides for 1 Mbps and 2 Mbps data rates and a set of fundamental signalling methods and other services. Like all IEEE 802 standards, the 802.11 standards focus on the bottom two levels the ISO model, the physical layer and link layer (see Figure 1.3). Any LAN application, network operating system, protocol, including TCP/IP and Novell NetWare, will run on an 802.11-compliant WLAN as easily as they run over Ethernet.

Figure 1.3: IEEE 802.11 and the ISO Model


Application
Presentation
Session
Network operating system (NOS)
Transport
TCP
Network
IP
Data
Link
Logical Link Control (LLC)—802.2
Media Access Control (MAC)—Power, security, etc.
802.11
Physical
FH, DS, IR

Source: http://www.tutorial-reports.com/wireless/wlanwifi/introduction_wifi.php

The major motivation and benefit from Wireless LANs is increased mobility. Untethered from conventional network connections, network users can move about almost without restriction and access LANs from nearly anywhere.

The other advantages for WLAN include cost-effective network setup for hard-to-wire locations such as older buildings and solid-wall structures and reduced cost of ownership-particularly in dynamic environments requiring frequent modifications, thanks to minimal wiring and installation costs per device and user. WLANs liberate users from dependence on hard-wired access to the network backbone, giving them anytime, anywhere network access. This freedom to roam offers numerous user benefits for a variety of work environments, such as:

- Immediate bedside access to patient information for doctors and hospital staff
- Easy, real-time network access for on-site consultants or auditors
- Improved database access for roving supervisors such as production line managers, warehouse auditors, or construction engineers
- Simplified network configuration with minimal MIS involvement for temporary setups such as trade shows or conference rooms
- Faster access to customer information for service vendors and retailers, resulting in better service and improved customer satisfaction
- Location-independent access for network administrators, for easier on-site troubleshooting and support
- Real-time access to study group meetings and research links for students

1.4.3 Wireless MANs

Wireless MANs offer connections between buildings and users within a city or campus area through several system configurations. In most cases, the wireless MAN beams RF or infrared light from one point to another using directive antennae.

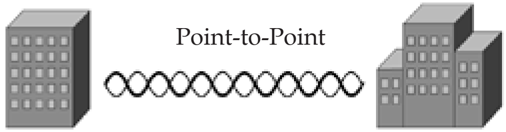
WirelessMAN® is a family of wireless networking standards created by the Institute of Electrical and Electronics Engineers (IEEE). The standards, officially known as IEEE 802.16, complement other wireless technologies like Wi-Fi®. The 802.16 group of standards are meant for use in large, city-sized wireless networks that can deliver broadband Internet access and compete against wired technologies like Digital Subscriber Line (DSL) and cable modems. The WirelessMAN® standards form the basis for WiMAX® and several other wireless broadband technologies.

The organization which created the 802.16 standard, the IEEE, was also responsible for ratifying the popular Bluetooth® and Wi-Fi® wireless standards. Each of these standards enables wireless networks to be built on different scales. Bluetooth®, for example, allows very short-range personal area networks (PANs). Wi-Fi® popularized whole-house wireless Local Area Networks (LANs), and WirelessMAN® is designed for larger Metropolitan Area Networks (MANs) meant to cover entire cities or geographical areas. In many cases, these different types of networks can be complementary. A LAN using Wi-Fi®, for example, could be connected to the Internet through a MAN using 802.16.

Point-to-Point Systems

A point-to-point solution uses RF or infrared signals that utilize either semidirectional or highly directional antennae to extend range across metropolitan areas, such as college campuses and cities. Range can be as high as 30 miles for RF systems using highly directional antennae. Figure 1.4 illustrates a point-to-point wireless MAN system.

Figure 1.4: Point-to-Point Wireless MAN Directly Connects Two Points in the Network



Source: http://etutorials.org/Networking/wn/Chapter+6.+Wireless+MANs+Networks+for+Connecting+Buildings+and+Remote+Areas/Wireless+MAN+Systems/

A medical centre, for example, can use a point-to-point wireless MAN to provide a communications link between the main hospital and a remote clinic within the same city. This resulting system, however, does not provide as much flexibility as point-to-multipoint solutions. However, if there is a need to connect only a couple sites, the cost of implementing a point-to-point system is less compared to a point-to-multipoint system.

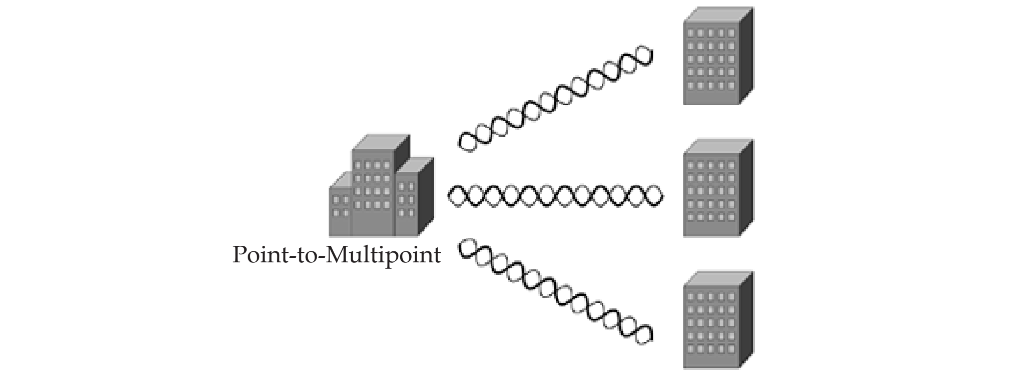
Point-to-Multipoint System

A typical point-to-multipoint link (see Figure 1.5) utilizes a centralized omnidirectional antenna that provides a single transceiver point for tying together multiple remote stations. For example, a building within the centre of a city can host the omnidirectional antenna, and other nearby metropolitan-area buildings can point directional antennae at the centralized location. The central transceiver receives and retransmits the signals.

A strong advantage of the point-to-multipoint wireless MAN is that it makes the addition of new connections easy. In fact, this approach can be less expensive compared to point-to-point systems when there are multiple sites to interconnect or connect to a central location. For example, a company headquarters having many remote warehouses and manufacturing plants within the same city or rural area would benefit from a point-to-multipoint system.

Notes

Figure 1.5: Point-to-Multipoint Wireless MAN Interconnects Users through a Common, Centralized Transceiver

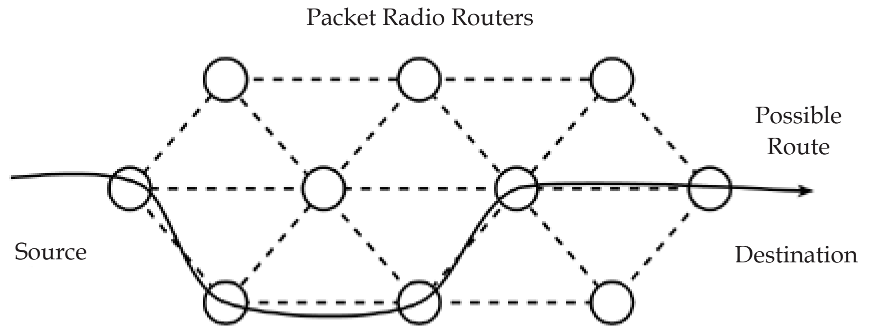


Source: http://etutorials.org/Networking/wn/Chapter+6.+Wireless+MANs+Networks+for+Connecting+Buildings+and+Remote+Areas/Wireless+MAN+Systems/

Packet Radio Systems

A packet radio system (see Figure 1.6) utilizes special wireless routers that forward data contained within packets to the destination. Each user has a packet radio NIC that transmits data to the nearest wireless router. This router then retransmits the data to the next router. This hopping from router to router occurs until the packet reaches the destination. This mesh type networking is not new. Amateur Ham radio operators have used it for decades, and companies such as Metricom have been deploying these types of systems in cities for nearly 10 years.

Figure 1.6: Packet Radio System Hops Data Packets from the Source to Destination



Source: http://etutorials.org/Networking/wn/Chapter+6.+Wireless+MANs+Networks+for+Connecting+Buildings+and+Remote+Areas/Wireless+MAN+Systems/

A city government might want to deploy a packet radio system to offer wireless connectivity for supporting applications through the entire city area. The installation of routers in strategic places through the city provides the necessary infrastructure. There's no need for wires for interconnecting the routers. Each router is capable of receiving, retransmitting and hopping the packets to their destination.

Caution This form of networking is also survivable. If one router becomes inoperative, perhaps because of a lightning strike or sabotage, adaptive routing protocols automatically update routing tables in each router so that data packets will avoid traversing the inoperative router.

1.5 Benefits of Wireless Networks

Wireless LANs offer the following productivity, convenience, and cost advantages over wired networks:

- ***Mobility:*** Wireless LAN systems can provide LAN users with access to real-time information anywhere in their organization. This mobility supports productivity and service opportunities not possible with wired networks. There are now thousands of universities, hotels and public places with public wireless connection. These free you from having to be at home or at work to access the Internet.
- ***Installation Speed and Simplicity:*** Installing a wireless LAN system can be fast and easy and can eliminate the need to pull cable through walls and ceilings.
- ***Reduced Cost-of-Ownership:*** While the initial investment required for wireless LAN hardware can be higher than the cost of wired LAN hardware, overall installation expenses and life-cycle costs can be significantly lower. Long-term cost benefits are greatest in dynamic environments requiring frequent moves and changes.
- ***Scalability:*** Wireless LAN systems can be configured in a variety of topologies to meet the needs of specific applications and installations. Configurations are easily changed and range from peer-to-peer networks suitable for a small number of users to full infrastructure networks of thousands of users that enable roaming over a broad area Wireless networks are a product of convenience for society. Using a wireless network allows an individual to access the Internet when he is not connected to a computer with an ethernet cable. Wireless Networks can be used by devices such as cell phones, laptops, and handheld computers. A wireless network is operated by a network of cellular towers and satellites.
- ***Security:*** When using wireless networks, security is an issue. Make sure it is a password protected network if you are surfing the Internet and entering personal information.
- ***Convenience:*** Wireless Networks can help make connecting to the Internet much more convenient. You don't need an ethernet connection so you can connect anywhere with a strong enough signal and a wireless network that is publicly accessible without a password.
- ***Devices:*** Many different devices can be used over a wireless network. These include laptop computers, Cellular phones, Blackberry devices, and handheld computers.
- ***Speed:*** Wireless networks are less reliable with connection speeds than connections using an ethernet cable. This is due to the risk of dead spots where the signal is either weak or non existant. Weather, and signal interference also play a role in weakening a connection.

Task Compare the devices used in the wireless networks.

Self Assessment

Fill in the blanks:

9. WPANs are ....-range networks that use Bluetooth technology.
10. Wireless PANs don't require much .... to operate, making them ideal for small user devices.
11. Several companies offer a wireless PAN USB adapter, which is also called a ....
12. .... offers the promise of unhindered access to network resources even outside the reach of a wired setup.

Notes

13. The widespread acceptance of WLANs depends on industry standardization to ensure product compatibility and .... among the various manufacturers.

14. The major motivation and benefit from Wireless LANs is increased ....

15. A strong advantage of the .... is that it makes the addition of new connections easy.

16. A .... system utilizes special wireless routers that forward data contained within packets to the destination.

Case Study

Beaverton, Oregon Builds Interoperable Public Safety Wireless Network

As many man-made and natural disasters, from September 11 to Hurricane Katrina, have proven, the key to saving lives in the wake of a tragedy is effective communications. And the key to effective communications, among the many departments and jurisdictions involved in an emergency, is interoperability. Lack of communications interoperability has been blamed for unnecessary delays and resultant increased loss of life, frustrating the recovery efforts of first responders and other public safety personnel. In 2005, Washington County and the city of Beaverton, Oregon worked together to find a solution that would be used by both to develop an interoperable wireless network for public safety agencies within the city and throughout the county. Representatives from Beaverton's Police, Information Systems Division, and Purchasing departments participated in the review of the Request for Proposal responses. The county had received a State Homeland Security.

Program (SHSP) grant that included resources to establish a wireless networking capability to provide field-based public safety personnel access to critical network-based information resources. Beaverton's SHSP grant could also be used to fund their portion of the network.

Working closely with the county to ensure that their mutual needs were met would go a long way in ensuring the ongoing viability of Beaverton's wireless public safety network.

The Challenge

Covering an area of approximately 19 square miles, and with a population of over 84,000, Beaverton ranks as Oregon's 6th largest city. With 100 city parks and 25 miles of bike trails, the city offers an exceptional quality of life. But the concerns of its police department are common to cities throughout the US.

The department wanted to improve the productivity of their officers and maximize their time spent on the beat rather than in the office. As the department's first line of defense in preventing and combating crime they also wanted to ensure that officers had access to timely information and resources needed to ensure effective response. This would necessitate communications capabilities beyond the basic voice services associated with traditional land mobile radio (LMR) systems.

The Solution

The Beaverton Police Department is one of Oregon's first public safety agencies to create and use a mobile broadband wireless network. Taking a leadership position can be risky, but, for Beaverton, it has paid off.

Contd...

Improved Productivity

As David G. Bishop, Chief of the Beaverton Police Department stated: "Real time information enables officers on the beat to be better prepared to make the right decision about the situations they face every day." Officers can now access their desktop, the city network and the Portland Police Data System from their patrol cars enabling real time access to information including mug shots, digitized fingerprints and criminal histories. Officers conducting follow-up investigations no longer have to return to headquarters or stop at a satellite office. Prior to the availability of the network, officers had to call in for histories and written reports, a time consuming and labour-intensive process.

Reliable and Scalable

Beaverton is already experiencing tangible benefits from their wireless deployment. The network's role in supporting an expanding range of day-to-day activities of the police officers in the field requires it to be both reliable and scalable. With Homeland Security grant funding from the federal Law Enforcement Terrorism Prevention Program (LETPP), the network is also designed to adapt to the increased capacity and coverage requirements that often accompany an emergency situation.

Increasing capacity on the network can be accomplished by either adding a node or just adding another wired egress point. The network's patented architecture enables capacity to be added anywhere in the network and directed to wherever it is needed. Quality of Service (QoS) capabilities ensures the prioritisation of critical voice, video and data traffic.

Future-Proof

The subject of interoperability among multiple public safety agencies and jurisdictions predates recent disasters that have clearly brought those issues to the forefront. The FCC has been active in the area of interoperability going back to at least 1986, when they established the National Public Safety Planning Advisory Committee. And, given the number of departments, agencies, advisory committees, and jurisdictions involved, and the constantly changing nature of telecommunications technology, interoperability of public safety communications will continue to evolve even as new solutions are adopted.

The Design

The overall objective of the wireless networking project is to provide a secure wireless infrastructure across the city and county. Through a comprehensive RFP and vendor selection process, an initial field of 12 interested firms was reduced to two finalists: BelAir Networks (bid by wireless integrator, Invictus Networks) and Motorola. Evaluating the finalists according to functionality, customer support, experience and reference, cost, implementation and installation, the winning bid scored an impressive 95%.

High-Performance, Multi-Application

High-performance BelAir200 and BelAir100 wireless multi-service nodes have been installed throughout Beaverton to provide wireless coverage of city hall and the commercial districts.

The city fitted its fleet of forty police cars with wireless-enabled computers. Within just a few months, the Information Systems department of the City of Beaverton, working with Washington County, had the in-house expertise to install, deploy, and run live tests over the new network, and had developed plans for expansion of both the network coverage and its integrated applications.

The Result

Beaverton, home to divisions of leading technology companies such as Intel and IBM, is often referred to as 'Silicon Forest' so it is not surprising that the city would choose industry

Contd...

leading technology for their public safety network. The city's commitment to enhanced law enforcement and the safety of its citizens is reflected in their ranking as the second safest medium/large city in the northwest and certainly contributed to their status as one of the 100 best places to live, according to Money Magazine.

Questions

1. Discuss the solution provided by the department to improve the productivity of their officers.
2. Discuss the features of BelAir100 wireless node.

Source: http://www.techrepublic.com/whitepapers/beaverton-oregon-builds-interoperable-public-safety-wireless network/2710559

1.6 Summary

- Wireless network refers to any type of computer network that uses wireless (usually, but not always radio waves) for network connections.
- It use electromagnetic waves to communicate information from one point to another without relying on any physical connection. Radio waves are often referred to as radio carriers because they simply perform the function of delivering energy to a remote receiver.
- A wireless network is a flexible data communications system, which uses wireless media such as radio frequency technology to transmit and receive data over the air, minimizing the need for wired connections.
- Wireless local-area networks (WLAN) have evolved as the quantity and types of mobile devices have increased. The number of devices that support Wi-Fi continues to expand.
- The Institute of Electrical and Electronic Engineers (IEEE) is a professional organization of electrical engineers that has organized a highly successful and unique standards making activity.
- Wireless networking hardware requires the use of underlying technology that deals with radio frequencies as well as data transmission. The most widely used standard is 802.11 produced by the Institute of Electrical and Electronic Engineers (IEEE).

1.7 Keywords

Institute of Electrical and Electronic Engineers (IEEE): IEEE is a professional organization of electrical engineers that has organized a highly successful and unique standards making activity.

Location-based Services (LBSs): LBSs are a general class of computer program-level services used to include specific controls for location and time data as control features in computer programs.

Packet Radio System: It utilizes special wireless routers that forward data contained within packets to the destination

Point-to-multipoint Link: It utilizes a centralized omnidirectional antenna that provides a single transceiver point for tying together multiple remote stations.

Real-Time Locating Systems: This concept of location based systems is not compliant with the standardized concept of real-time locating systems (RTLS) and related local services.

Vowlan (Voice over Wireless LAN): It is the use of a wireless broadband network according to the IEEE 802.11 standards for the purpose of vocal conversation.

Notes

Wireless MANs: It offer connections between buildings and users within a city or campus area through several system configurations.

Wireless Network: It refers to any type of computer network that uses wireless (usually, but not always radio waves) for network connections.

Wireless Personal area Networks (WPANs): WPAN interconnect devices within a relatively small area, that is generally within a person's reach.

1.8 Review Questions

1. Comment "A high performance wireless network can help hospitals in numerous ways".
2. Describe the role played by wireless networks in education and healthcare.
3. Discuss the advantage of wireless networking.
4. Explain wireless networks applications.
5. List down the benefits that wireless networks offer over traditional wired networks.
6. What are IEEE Standards for Wireless Networks?
7. What are the needs of wireless networking?
8. What are the various types of wireless network?
9. What do you mean by location-based services?
10. Write a brief note on the future of wireless networks.

Answers: Self Assessment

1. 802.11b
2. data transmission
3. IEEE 802.11n
4. Institute of Electrical and Electronic Engineers (IEEE)
5. WLAN
6. RFID
7. Wireless
8. VPNs
9. Short
10. battery power
11. wireless dongle
12. Wireless LAN (WiFi)
13. Reliability
14. Mobility
15. point-to-multipoint wireless MAN
16. packet radio

1.9 Further Readings

Books

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

John Ross, *Introduction to wireless networks.*

Vijay Garg, *Wireless Communications & Networking.*

Theodore S. Rappaport, *Wireless Communications: Principles and Practice.*

Notes

Online links

http://en.wikipedia.org/wiki/Wireless_network

http://www.cwins.wpi.edu/publications/pown/chapter_1.pdf

http://info.bannerengineering.com/xpedio/groups/public/documents/literature/135766.pdf

http://www.pearsonhighered.com/samplechapter/0130930032.pdf

http://www.cse.wustl.edu/~jain/cse574-08/ftp/medical/

http://www.rfidc.com/docs/introductiontowireless_standards.htm

http://www.vicomsoft.com/learning-center/wireless-networking/

www.mhprofessional.com/downloads/products/0071701524/0071701524_chap02.pdf

Unit 2: Wireless System Architecture

Notes

CONTENTS

Objectives

Introduction

2.1 Wireless System Components

2.1.1 Wireless System Networking Equipment

2.1.2 Wireless System Networking Routers

2.1.3 Computer Devices

2.1.4 Network Interface Cards (NICs)

2.1.5 Air Medium

2.1.6 Wireless Network Infrastructures

2.2 Network Architecture

2.2.1 Network Architecture (OSI)

2.3 Information Signals

2.3.1 Digital Signals

2.3.2 Analog Signals

2.4 Summary

2.5 Keywords

2.6 Review Questions

2.7 Further Readings

Objectives

After studying this unit, you will be able to:

- Discuss the components of a wireless network
- Discuss general wireless network architectural elements
- Explain how information flows through a wireless network
- Describe about information signals

Introduction

Wireless networks utilize components similar to wired networks; however, wireless networks must convert information signals into a form suitable for transmission through the air medium. Even though wireless networks directly contribute only to a portion of the overall network infrastructure, attention to all network functions is necessary to counter impairments resulting from the wireless medium. This chapter discusses concepts common to all types of wireless networks, with emphasis on components and information signals.

2.1 Wireless System Components

Although each protocol has different specifications and criteria, there are general characteristics and goals that each protocol tries to achieve. Several of these protocols are discussed in this survey paper as well. Below are some general guidelines these protocols try to follow:

- ***Unlimited roaming and range:*** The location of the user with the portable device is irrelevant. No matter how far or how near a user is from the base provider, data can still be sent and received.
- ***Guarantee of Delivery:*** All messages and data is guaranteed to be delivered regardless of where a user is located or the user's status. Even if the portable device is turned off, when it is turned on again, the user will see a new message.
- ***Dependability of Delivery:*** All messages are guaranteed of accurate and full transmission.
- ***Notification:*** Notifies the user that there is data that has been sent and needs to be looked at.
- ***Connectivity Options:*** Sender and receiver are given a wide range of options not only in hardware for the portable device, but also are given options in receiving messages (choosing a type of connection for instance).
- ***Millions of Users:*** Ability to engage millions of users.
- ***Priority Alerts:*** Able to distinguish between messages and data that are of higher importance than others. Able to control high-priority data traffic and do so correctly and rapidly.
- ***Communication:*** The ability to communicate between one user to another through one portable device to another where each portable device holds reliable and user-friendly software applications.
- ***Host Reconfiguration:*** The ability to reconfigure when changing environments. For example, Person A is carrying a Palm Pilot that uses Bluetooth. Person A enters the office where there is an entire Bluetooth network set-up and Person A's Palm Pilot configures to the settings of the office network. The end of the day comes, and Person A starts driving home. Person A gets home and walks inside where Person A's home is set up with an entirely different Bluetooth network. Person A brings the Palm Pilot out and the Palm Pilot automatically reconfigures itself to the settings of the Bluetooth network in Person A's home. Therefore, whether the Palm Pilot works in one environment and can detect when it has been moved to another environment and can set itself up wherever it is located.
- ***Host Mobility:*** One host contains its settings on a network – its IP address, Subnet Mask, Gateway Address, and so on. Now this one host decides to move somewhere else, this means that the host will have to change its settings all over again, but has to let others know that it has moved. Flexible mobility allows the host to come and go as it pleases and not even needing to alert others of its move. Communication with the host is still possible even if it has moved.
- ***Dynamic Encapsulation:*** The need to register a mobile host with its base agent, perhaps using a login and logout request and alerts of activation and inactivation. This will prevent forged logins and having one's precious date to be re-routed somewhere it should not be.

2.1.1 Wireless System Networking Equipment

What sort of hardware is required to build a wireless network is dependent on the type of network you intend to build.

If you have two devices with wireless network adapters whether wireless enabled PDA's, laptops or desktop computers you can technically connect them in an ad hoc wireless network. Essentially, any devices enabled with wireless network adapters within range of each other can all communicate with each other over such an ad hoc network.

If you want to build a more traditional network where multiple clients connect to a central point which acts as a gateway to the rest of the world you will also need a wireless router or wireless access point to implement an infrastructure mode network.

A wireless router has a physical network connection which would be connected to a wired network. It could be connected to a hub or switch on a network or for home users would generally be connected to your cable or DSL modem. All of the wireless-enabled clients would then connect to the wireless router. Typically the wireless router will act as the DNS server and Internet gateway for the clients attached to it and it can also be configured to provide IP addresses automatically using DHCP.

A wireless access point (AP) can be used to join wireless devices to a wired network, or to extend the range of a wireless network. They don't provide the DNS, DHCP, firewall or other functions commonly found in wireless routers. They simply take a wired or wireless network input and relay it to the wireless devices within its broadcast range.

2.1.2 Wireless System Networking Routers

The process of developing a wireless network becomes complex when you are deploying multiple APs throughout a multi-story building, because in addition to your neighbours Access Points (APs) you need to worry about location, channel selection, and interference from your old APs with each other.

Selecting Channels

You have only three channels to work with in North America when dealing with 2.4 GHz networking. Some people have suggested that you can get away setting up your channels in a four-channel manner by using channels 1, 4, 8, and 11. This setup would give you overlap in the shoulder area of the bands, but the overlap would be fairly small.

Cisco has done lab testing of the concept using four APs and four clients all transferring 50 MB files to and from a server. Even with this limited overlap, data ends up being lost, and stations or computers wait their mandatory wait periods and retransmit data.

These problems slow down the overall throughput. The following table shows the final results. So if you are told that you can use four channels when making your channel selections, this is not advisable and you should stick to the reliable and time tested three channel configuration.

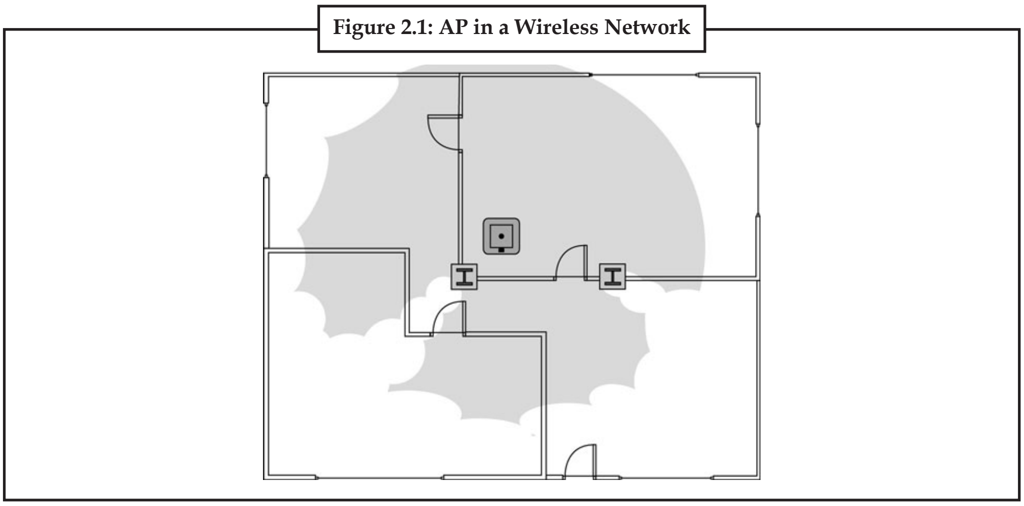
The simplest wireless network contains only one AP and that the issues that you need to deal with for one AP are generally placement and signal loss. A centrally located AP in an office with a few obstructions that may cause signal loss in the unshaded areas.

Notes In addition to the obstructions and construction material, there may be various sources of external interference that can reduce the size of the coverage area.

In addition to the obstructions and construction material, there may be various sources of external interference that can reduce the size of the coverage area.

Notes

Figure 2.1: AP in a Wireless Network

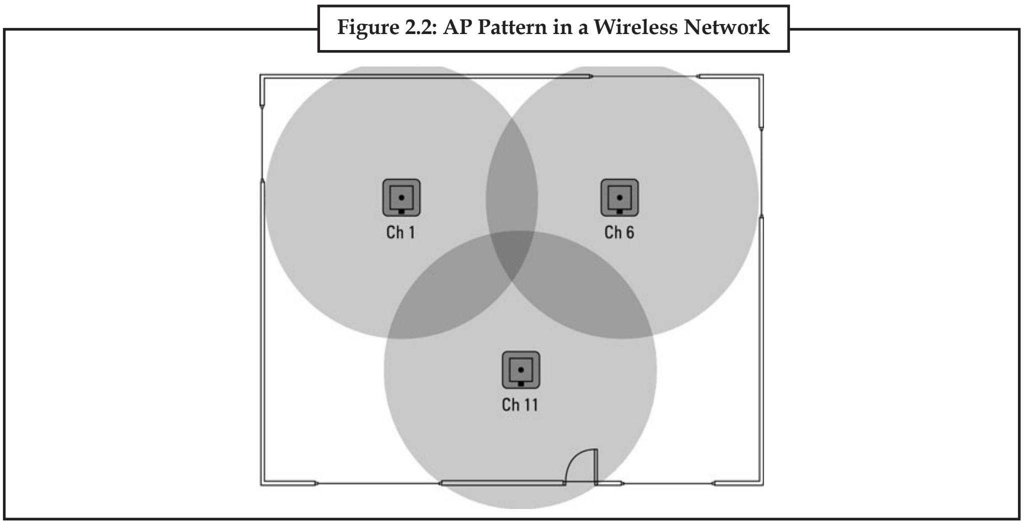


Source: http://www.dummies.com/how-to/content/wireless-network-routing-with-multiple-access-poin.html

Ignoring signal loss from building materials, if you have three APs in your layout and no outside interference, you should use all three of the non-overlapping channels (1, 6, and 11). The only exception to this would be if you had a more linear layout, where the APs at either end of the line were isolated by the middle AP.

A typical pattern may give you a layout that resembles what is shown. Cisco recommends a 10–15 percent overlap between APs to allow complete coverage in the interim area, 15–20 percent for VOIP solutions.

Figure 2.2: AP Pattern in a Wireless Network



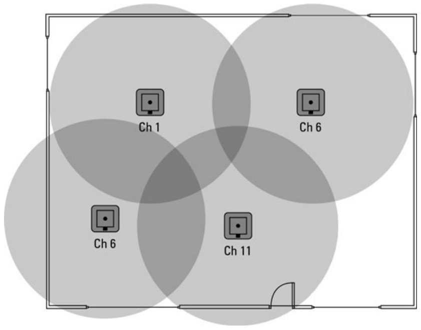
Source: http://www.dummies.com/how-to/content/wireless-network-routing-with-multiple-access-poin.html

This deployment would be more complex if you had to provide coverage using four APs. In that case, you would have to reuse at least one of the non-overlapping channels to complete the deployment. You can do that by isolating the AP with the reused channel from the other AP (which is using the same channel) by having stronger signals from the intermediary APs separate them.

Staggering these AP channels allows you to provide coverage on all your network APs. An example of this is shown, where the two APs on channel 6 are separated by the combined signals from the APs on channels 1 and 11.

Notes

Figure 2.3: Coverage using Four APs

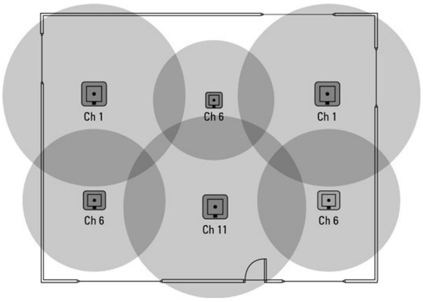


Source: http://www.dummies.com/how-to/content/wireless-network-routing-with-multiple-access-poin.html

If the area gets even more crowded, in an attempt to provide better coverage or to support higher client density, you may need to take additional steps. In the following figure, notice that

- An AP on channel 6 separates the two channel 1 APs, allowing that channel to be reused.
- All three channel 6 APs are primarily separated by the channel 11 AP.
- In addition to the physical placement, the power levels on the channel 6 APs have been reduced to provide a lower radius of coverage, thus preventing these APs from touching each other.

Figure 2.4: AP Pattern in a Wireless Network in a more Crowded Form



Source: http://www.dummies.com/how-to/content/wireless-network-routing-with-multiple-access-poin.html

2.1.3 Computer Devices

Automatic wireless network configuration supports the IEEE 802.11 standard for wireless networks and minimizes the configuration that is required to access wireless networks. When you enable automatic wireless network configuration on your computer, you can roam across different wireless networks without the need to reconfigure the network connection settings on your computer for each location. As you move from one location to a new location, automatic wireless network configuration searches for available wireless networks and notifies you when there are new wireless networks available for you to connect to. After you select the wireless network that you want to connect to, automatic wireless network configuration updates your wireless network adapter to match the settings of that wireless network, and attempts to connect to that wireless network.

Did u know? With automatic wireless network configuration, you can create a list of preferred wireless networks, and you can specify the order in which to attempt connections to these wireless networks.

2.1.4 Network Interface Cards (NICs)

Every computer on a network, both clients and servers, requires a network interface card (or NIC) in order to access the network. A NIC is usually a separate adapter card that slides into one of the server's motherboard expansion slots. However, most newer computers have the NIC built into the motherboard, so a separate card isn't needed.

For client computers, you can usually get away with using the inexpensive built-in NIC because client computers are used to connect only one user to the network. However, the NIC in a server computer connects many network users to the server. As a result, it makes sense to spend more money on a higher-quality NIC for a heavily used server. Most network administrators prefer to use name-brand cards from manufacturers such as Intel, SMC, or 3Com.

Most NICs made today support 1 Gbps networking, and will also support slower 100 Mbps and even ancient 10 Mbps networks. These cards automatically adjust their speed to match the speed of the network. So you can use a gigabit card on a network that has older 100 Mbps cards without trouble. You can find inexpensive gigabit cards for as little as $5 each, but a typical name-brand card (such as Linksys or Intel) will cost around $25 or $30.

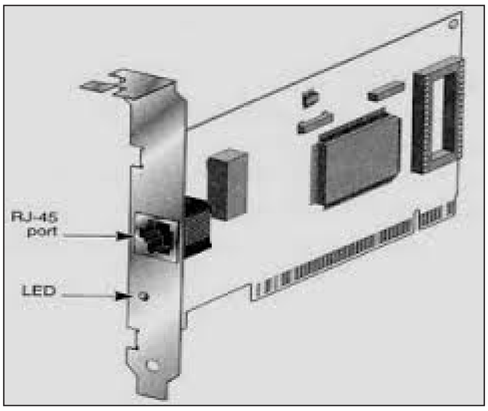
Here are a few other points to ponder concerning network interface cards:

- A NIC is a Physical layer and Data Link layer device. Because a NIC establishes a network node, it must have a physical network address, also known as a MAC address. The MAC address is burned into the NIC at the factory, so you can't change it. Every NIC ever manufactured has a unique MAC address.
- For server computers, it makes sense to use more than one NIC. That way, the server can handle more network traffic. Some server NICs have two or more network interfaces built into a single card.
- Fiber-optic networks also require NICs. Fiber-optic NICs are still too expensive for desktop use in most networks. Instead, they're used for high-speed backbones. If a server connects to a high-speed fiber backbone, it will need a fiber-optic NIC that matches the fiber-optic cable being used.

The network interface card (NIC) is installed in an expansion slot of the computer. This card (Figure 2.5) connects the computer to a network, and contains information on the computer's location and also instructions for sending and receiving data over the network.

It adds a serial port to the computer and the port connects directly to a network. NIC converts the computers' low power signals to high power signals that can be transmitted over the network. NIC's speed is measured in megabits per second (Mbps).

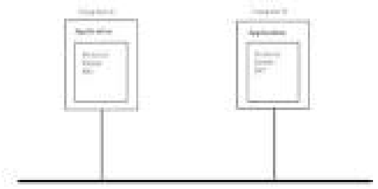
Figure 2.5: Network Interface Card (NIC)



Source: www.netguidea.com/2012/09/introduction-2-network-interface-cards.html

In Figure 2.6, you can see how two computers are connected with network interface cards and network cables.

Figure 2.6: Two Computers Connected through NICs



Source: www.netguidea.com/2012/09/introduction-2-network-interface-cards.html

A device driver, called driver in shorten form, is a specific type of software developed to allow interaction with a hardware device (in this case NIC). Typically this constitutes an interface for communicating with the NIC, through the specific computer bus it is connected to. It also provides commands for transmitting and/or receiving data through the NIC.

Networks (hardware) provide the basic ability of transferring data from one computer to another. In order to use networks we need a set of rules which all of the network's members agree on. Such set of rules is called a protocol.

Communication Protocol is a set of standards designed to specify how computers interact and exchange messages. A Protocol usually specifies:

- format for data representation
- how to handle errors
- signalling
- authentication procedures

In order to simplify the design and implementation of protocols, a set of protocols is defined. Each in the set has different responsibilities instead of the one protocol being responsible for all forms of communication.

2.1.5 Air Medium

Air is the medium for a wireless network, but to utilize the free supply of this medium you need equipment and an environment free of interference. In a home network, the infrastructure might be as simple as a wireless enabled broadband modem, which also acts as router and access controller, and the wire necessary to connect this to the power outlet and perhaps a shared printer. In a larger network, multiple routers, repeaters and monitoring systems may be in place, and whole sections of the network may use wired connections.

You may see the following terms used interchangeably, but basically:

- A base station is a device whose sole purpose is to connect to the wireless network and relay information along it.
- A modem is the device that connects a local network to a remote one.
- A router enables sharing of an internet connection between multiple devices.

An access controller is a device that sits between the local and remote network and adds a layer of security to the network, determining whether connections are secure and should be allowed.

2.1.6 Wireless Network Infrastructures

In the case of wireless networking in Infrastructure mode you are connecting your devices using a central device, namely a wireless access point. To join the WLAN, the AP and all wireless clients must be configured to use the same SSID. The AP is then cabled to the wired network to allow wireless clients access to, for example, Internet connections or printers.

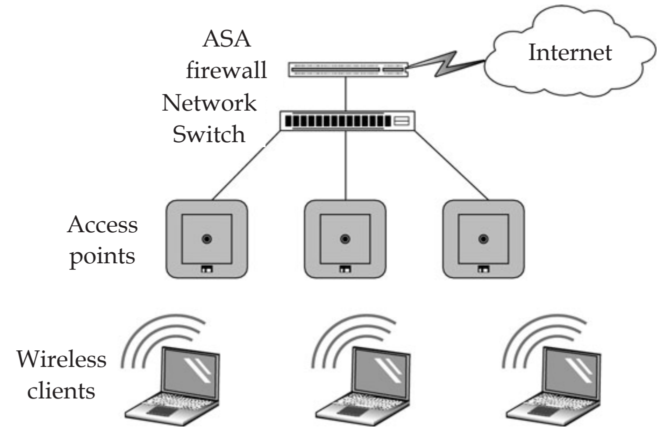
Notes Additional APs can be added to the WLAN to increase the reach of the infrastructure and support any number of wireless clients.

Compared to the alternative, ad-hoc wireless networks, infrastructure mode networks offer the advantage of scalability, centralized security management and improved reach. The disadvantage of infrastructure wireless networks is simply the additional cost to purchase AP hardware.

As opposed to Ad Hoc mode networks, which make wireless connections directly between computers, Infrastructure mode wireless networks use networking infrastructure. In this case, infrastructure refers to switches, routers, firewalls, and access points (APs). Infrastructure mode wireless networking is the mode that you most often encounter in your work as a networking professional supporting networks for clients or in a corporate environment.

At a minimum, the only network infrastructure component that is required for Infrastructure mode is an access point, but if an AP is all you have, you have no more than you would have had when using Ad Hoc mode. However, most Infrastructure mode implementations include other components from your traditional network infrastructure.

Figure 2.7: Wireless Network Infrastructure



Source: http://www.dummies.com/how-to/content/wireless-networking-infrastructure-mode.html

Base Station

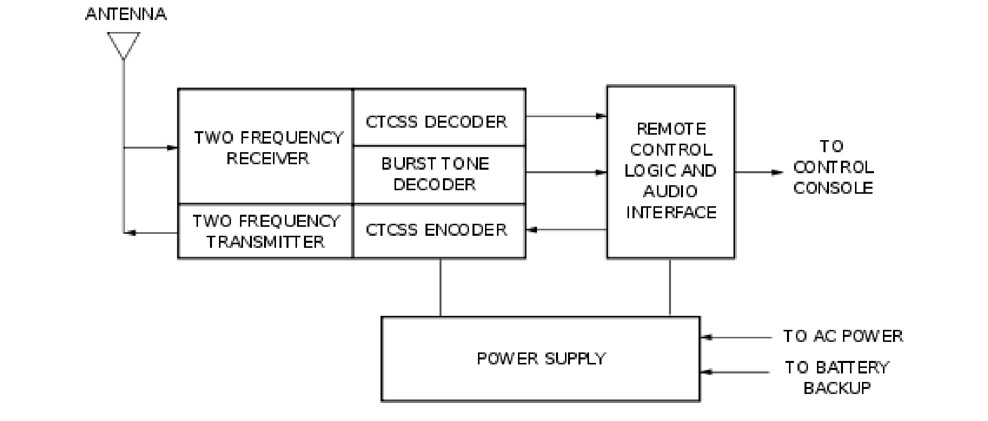
In radio communications, a base station is a wireless communications station installed at a fixed location and used to communicate as part of one of the following:

- A push-to-talk two-way radio system, or;
- A wireless telephone system such as cellular CDMA or GSM cell site
- Terrestrial Trunked Radio

- Two-way radio
- Professional

In professional two-way radio systems, a base station is used to maintain contact with a dispatch fleet of hand-held or mobile radios, and/or to activate one-way paging receivers. The base station is one end of a communications link. The other end is a movable vehicle-mounted radio or walkie-talkie. Examples of base station uses in two-way radio include the dispatch of tow trucks and taxicabs.

Figure 2.8: Two-way Radio Systems



Source: http://en.wikipedia.org/wiki/Base_station

Basic base station elements used in a remote-controlled installation. Selective calling options such as CTCSS are optional.

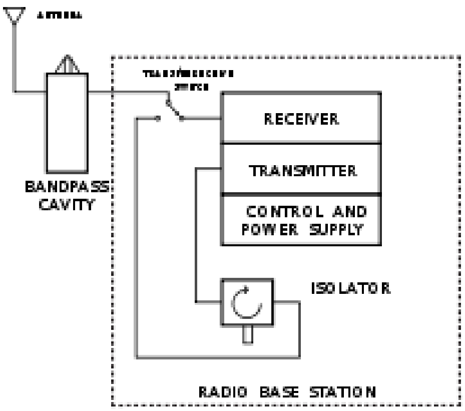
Professional base station radios are often one channel. In lightly used base stations, a multi-channel unit may be employed. In heavily used systems, the capability for additional channels, where needed, is accomplished by installing an additional base station for each channel. Each base station appears as a single channel on the dispatch centre control console. In a properly designed dispatch centre with several staff members, this allows each dispatcher to communicate simultaneously, independently of one another, on a different channel as necessary. For example, a taxi company dispatch centre may have one base station on a high-rise building in Boston and another on a different channel in Providence. Each taxi dispatcher could communicate with taxis in either Boston or Providence by selecting the respective base station on his or her console.

In dispatching centres it is common for eight or more radio base stations to be connected to a single dispatching console. Dispatching personnel can tell which channel a message is being received on by a combination of local protocol, unit identifiers, volume settings, and busy indicator lights. A typical console has two speakers identified as select and unselect. Audio from a primary selected channel is routed to the select speaker and to a headset. Each channel has a busy light which flashes when someone talks on the associated channel.

Base stations can be local controlled or remote controlled. Local controlled base stations are operated by front panel controls on the base station cabinet. Remote control base stations can be operated over tone- or DC-remote circuits. The dispatch point console and remote base station are connected by leased private line telephone circuits, (sometimes called RTO circuits), a DS-1, or radio links. The consoles multiplex transmit commands onto remote control circuits. Some system configurations require duplex, or four wire, audio paths from the base station to the console. Others require only a two-wire or half duplex link.

Notes

Figure 2.9: Two-way Radio Systems



Source: http://en.wikipedia.org/wiki/Base_station

The Figure 2.9 shows a band-pass filter used to reduce the base station receiver's exposure to unwanted signals. It also reduces the transmission of undesired signals. The isolator is a one-way device which reduces the ease of signals from nearby transmitters going up the antenna line and into the base station transmitter. This prevents the unwanted mixing of signals inside the base station transmitter which can generate interference.

Interference could be defined as receiving any signal other than from a radio in your own system. To avoid interference from users on the same channel, or interference from nearby strong signals on another channel, professional base stations use a combination of:

- minimum receiver specifications and filtering
- analysis of other frequencies in use nearby
- in the US, coordination of shared frequencies by coordinating agencies
- locating equipment so that terrain blocks interfering signals
- use of directional antennas to reduce unwanted signals

Base stations are sometimes called control or fixed stations in US Federal Communications Commission licensing. These terms are defined in regulations inside Part 90 of the commissions regulations. In US licensing jargon, types of base stations include:

- A fixed station is a base station used in a system intended only to communicate with other base stations. A fixed station can also be radio link used to operate a distant base station by remote control. (No mobile or hand-held radios are involved in the system.)
- A control station is a base station used in a system with a repeater where the base station is used to communicate through the repeater.
- A temporary base is a base station used in one location for less than a year.
- A repeater is a type of base station that extends the range of hand-held and mobile radios.
- Point-to-point communication systems.

In telecommunications, a point-to-point connection refers to a communications connection between two nodes or endpoints. An example is a telephone call, in which one telephone is connected with one other, and what is said by one caller can only be heard by the other. This is contrasted with a point-to-multipoint or broadcast communication topology, in which many nodes can receive information transmitted by one node. Other examples of point-to-point communications links are leased lines, microwave relay links, and two way radio.

Example: Example of point-to-multipoint communications systems are radio and television broadcasting.

The term is also used in computer networking and computer architecture to refer to a wire or other connection that links only two computers or circuits, as opposed to other network topologies such as buses or crossbar switches which can connect many communications devices.

Caution Point-to-point is sometimes abbreviated as P2P, Pt2Pt. This usage of P2P is distinct from P2P referring to peer-to-peer file sharing networks.

Wireless Internet Service Provider (ISP/WISP)

A wireless Internet service provider (WISP) is an Internet service provider with a network based on wireless networking. Technology may include commonplace Wi-Fi wireless mesh networking, or proprietary equipment designed to operate over open 900 MHz, 2.4 GHz, 4.9, 5.2, 5.4, 5.7, and 5.8 GHz bands or licensed frequencies in the UHF band (including the MMDS frequency band).

In the US, the Federal Communications Commission (FCC) released Report and Order, FCC 05-56 in 2005 that revised the FCC's rules to open the 3650 MHz band for terrestrial wireless broadband operations. On November 14, 2007 the Commission released Public Notice (DA 07-4605) in which the Wireless Telecommunications Bureau announced the start date for licensing and registration process for the 3650-3700 MHz band.

Point-to-multipoint Communication Systems

Point-to-multipoint (PMP) communication refers to communication that is accomplished through a distinct and specific form of one-to-many connections, offering several paths from one single location to various locations. Point-to-multipoint is generally abbreviated as PTMP, P2MP or PMP. PMP communication is commonly used in telecommunications.

PMP is usually used for establishing private enterprise connectivity to offices in remote locations, long-range wireless backhaul solutions for various sites, and last-mile broadband access. As such, it is widely used in IP telephony and wireless Internet by means of gigahertz radio frequencies. These PMP networks are employed in distribution amenities, huge corporate campuses, school districts, public safety applications, etc.

Access Controllers

A wireless access controller is a highly scalable and flexible platform that allows you to manage all the wireless access points in a network as a whole rather than individually. Unlike other devices, a Wireless Access Controller can manage multiple wireless access points. If you have controllers in your network, Foglight NMS retrieves the following information from a wireless access controller:

- View the health status of a controller and of the access points it manages
- Determine which access points are managed by controller
- Determine which devices are connected to which access points
- Track device moves between access points
- View load, noise, interference and coverage of each access point

You can also create an alert or generate a report based on the data collected from a wireless access controller.

Self Assessment

Fill in the blanks:

1. PMP is usually used for establishing private enterprise connectivity to offices in .... locations.
2. Point-to-point is sometimes abbreviated as ....
3. Examples of .... communications systems are radio and television broadcasting.
4. .... stations are sometimes called control or fixed stations in US Federal Communications Commission licensing.
5. ....could be defined as receiving any signal other than from a radio in your own system.
6. An .... controller is a device that sits between the local and remote network and adds a layer of security to the network, determining whether connections are secure and should be allowed.
7. .... provide the basic ability of transferring data from one computer to another.
8. A .... is a Physical layer and Data Link layer device.

2.2 Network Architecture

Network architecture is the design of a communications network. It is a framework for the specification of a network's physical components and their functional organization and configuration, its operational principles and procedures, as well as data formats used in its operation.

In telecommunication, the specification of a network architecture may also include a detailed description of products and services delivered via a communications network, as well as detailed rate and billing structures under which services are compensated.

The network architecture of the Internet is predominantly expressed by its use of the Internet Protocol Suite, rather than a specific model for interconnecting networks or nodes in the network, or the usage of specific types of hardware links.

2.2.1 Network Architecture (OSI)

The Open Systems Interconnection model (OSI model) is a product of the Open Systems Interconnection effort at the International Organization for Standardization. It is a way of sub-dividing a communications system into smaller parts called layers. A layer is a collection of similar functions that provide services to the layer above it and receives services from the layer below it. On each layer, an instance provides services to the instances at the layer above and requests service from the layer below.

- ***Physical Layer:*** The Physical Layer defines the electrical and physical specifications for devices. In particular, it defines the relationship between a device and a transmission medium, such as a copper or optical cable. This includes the layout of pins, voltages, cable specifications, hubs, repeaters, network adapters, host bus adapters (HBA used in storage area networks) and more. Its main task is the transmission of a stream of bits over a communication channel.
- ***Data Linking Layer:*** The Data Link Layer provides the functional and procedural means to transfer data between network entities and to detect and possibly correct errors that may occur in the Physical Layer. Originally, this layer was intended for point-to-point

and point-to-multipoint media, characteristic of wide area media in the telephone system. Local area network architecture, which included broadcast-capable multiaccess media, was developed independently of the ISO work in IEEE Project 802. IEEE work assumed sublayering and management functions not required for WAN use. In modern practice, only error detection, not flow control using sliding window, is present in data link protocols such as Point-to-Point Protocol (PPP), and, on local area networks, the IEEE 802.2 LLC layer is not used for most protocols on the Ethernet, and on other local area networks, its flow control and acknowledgment mechanisms are rarely used. Sliding-window flow control and acknowledgment is used at the Transport Layer by protocols such as TCP, but is still used in niches where X.25 offers performance advantages. Simply, its main job is to create and recognize the frame boundary. This can be done by attaching special bit patterns to the beginning and the end of the frame. The input data is broken up into frames.

- ***Network Layer:*** The Network Layer provides the functional and procedural means of transferring variable length data sequences from a source host on one network to a destination host on a different network, while maintaining the quality of service requested by the Transport Layer (in contrast to the data link layer which connects hosts within the same network). The Network Layer performs network routing functions, and might also perform fragmentation and reassembly, and report delivery errors. Routers operate at this layer – sending data throughout the extended network and making the Internet possible. This is a logical addressing scheme – values are chosen by the network engineer. The addressing scheme is not hierarchical. It controls the operation of the subnet and determine the routing strategies between IMP and insures that all the packs are correctly received at the destination in the proper order.

- ***Transport Layer:*** The Transport Layer provides transparent transfer of data between end users, providing reliable data transfer services to the upper layers. The Transport Layer controls the reliability of a given link through flow control, segmentation/desegmentation, and error control. Some protocols are state and connection oriented. This means that the Transport Layer can keep track of the segments and retransmit those that fail. The Transport layer also provides the acknowledgement of the successful data transmission and sends the next data if no errors occurred. Some Transport Layer protocols, for example TCP, but not UDP, support virtual circuits provide connection oriented communication over an underlying packet oriented datagram network. Where it assures the delivery of packets in the order in which they were sent and assure that they are free of errors. The datagram transportation deliver the packets randomly and broadcast it to multiple nodes.

Notes The transport layer multiplexes several streams on to 1 physical channel. The transport headers tells which message belongs to which connection.

- ***The Session Layer:*** This Layer provides a user interface to the network where the user negotiates to establish a connection. The user must provide the remote address to be contacted. The operation of setting up a session between two processes is called "Binding". In some protocols it is merged with the transport layer. Its main work is to transfer data from the other application to this application so this application is mainly used for transferred layer.

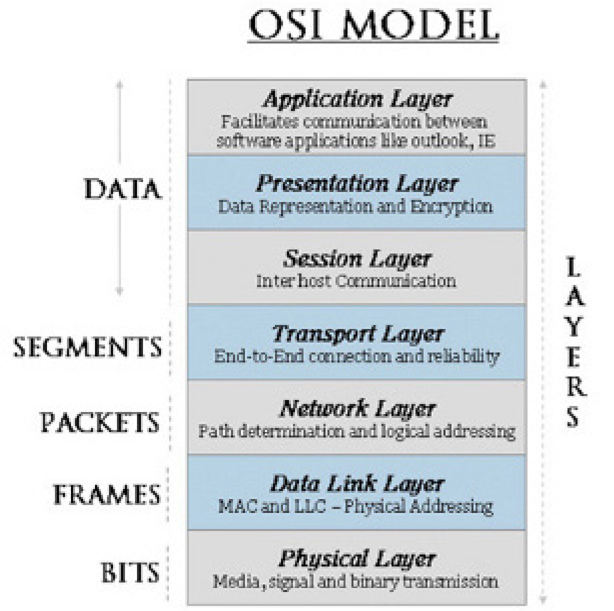
- ***Presentation Layer:*** The Presentation Layer establishes context between Application Layer entities, in which the higher-layer entities may use different syntax and semantics if the presentation service provides a mapping between them. If a mapping is available, presentation service data units are encapsulated into session protocol data units, and passed down the stack. This layer provides independence from data representation (e.g., encryption) by translating between application and network formats. The presentation layer transforms data into the form that the application accepts. This layer formats and

Notes

encrypts data to be sent across a network. It is sometimes called the syntax layer. The original presentation structure used the basic encoding rules of Abstract Syntax Notation One (ASN.1), with capabilities such as converting an EBCDIC-coded text file to an ASCII-coded file, or serialization of objects and other data structures from and to XML.

- *Application Layer:* The Application Layer is the OSI layer closest to the end user, which means that both the OSI application layer and the user interact directly with the software application. This layer interacts with software applications that implement a communicating component. Such application programs fall outside the scope of the OSI model. Application layer functions typically include identifying communication partners, determining resource availability, and synchronizing communication. When identifying communication partners, the application layer determines the identity and availability of communication partners for an application with data to transmit.

Figure 2.10: OSI Model


OSI MODEL
Application Layer
Facilitates communication between software applications like outlook, IE
Presentation Layer
Data Representation and Encryption
Session Layer
Inter host Communication
Transport Layer
End-to-End connection and reliability
Network Layer
Path determination and logical addressing
Data Link Layer
MAC and LLC – Physical Addressing
Physical Layer
Media, signal and binary transmission
DATA
SEGMENTS
PACKETS
FRAMES
BITS
LAYERS

Source: http://www.rockwellautomation.com/news/the-journal/exclusive/2011/july1.page

2.3 Information Signals

A signal as referred to in communication systems, signal processing, and electrical engineering "is a function that conveys information about the behaviour or attributes of some phenomenon". In the physical world, any quantity exhibiting variation in time or variation in space (such as an image) is potentially a signal that might provide information on the status of a physical system, or convey a message between observers, among other possibilities. The IEEE Transactions on Signal Processing elaborates upon the term "signal" as follows:

Caution The term "signal" includes, among others, audio, video, speech, image, communication, geophysical, sonar, radar, medical and musical signals.

Other examples of signals are the output of a thermocouple, which conveys temperature information, and the output of a pH meter which conveys acidity information. Typically, signals are often provided by a sensor, and often the original form of a signal is converted to another form of energy using a transducer. For example, a microphone converts an acoustic signal to a voltage waveform, and a speaker does the reverse.

2.3.1 Digital Signals

Digital signals are quite different from the analog signals because they are based on the numeric methods. It is defined as the types of signal which are used to represent the quantities which use the numeric method to deliver the information are called as the digital signals. Basically they are in discrete form. Sometimes they are said to be more reliable in the field of computer technology because they are used to transfer data. With the presence of continuous waves in the digital signals they really helpful in avoiding the rise a fall like in analog signals.

2.3.2 Analog Signals

There are different forms of signals one of them is the analog signal. It is defined as the type of signal that are used to express the quantities that are based on the variability of time and different type of time based processes such as electrical, some of mechanical and hydraulic are called the analog signals. Different types of minute fluctuations are used for the sake of process by analog signals. They also use the same method to pass on the information between different places. Wires are used for the processes of analog signals.

Self Assessment

State whether the following statements are true or false:

9. Network "is a function that conveys information about the behaviour or attributes of some phenomenon".
10. Application Layer is the OSI layer closest to the end user, which means that both the OSI application layer and the user interact directly with the software application.
11. The Data Link Layer establishes context between Application Layer entities.
12. The operation of setting up a session between two processes is called "Binding".
13. The Transport Layer provides transparent transfer of data between end users, providing reliable data transfer services to the upper layers.
14. The Network Layer provides the functional and procedural means of transferring variable length data sequences from a source host on one network to a destination host on a different network
15. Presentation Layer provides the functional and procedural means to transfer data between network entities and to detect and possibly correct errors that may occur in the Physical Layer.
16. Open Systems Interconnection model (OSI model) is a product of the Open Systems Interconnection effort at the International Organization for Standardization.

Case Study **Securing Wireless Networks**

How do Wireless Networks Work?

As the name suggests, wireless networks, sometimes called WiFi, allow you to connect to the internet without relying on wires. If your home, office, airport, or even local coffee shop has a wireless connection, you can access the network from anywhere that is within that wireless area.

Wireless networks rely on radio waves rather than wires to connect computers to the internet. A transmitter, known as a wireless access point or gateway, is wired into an

Contd...

Notes

internet connection. This provides a "hotspot" that transmits the connectivity over radio waves. Hotspots have identifying information, including an item called an SSID (service set identifier), that allow computers to locate them. Computers that have a wireless card and have permission to access the wireless frequency can take advantage of the network connection. Some computers may automatically identify open wireless networks in a given area, while others may require that you locate and manually enter information such as the SSID.

What Security Threats are Associated with Wireless Networks?

Because wireless networks do not require a wire between a computer and the Internet connection, it is possible for attackers who are within range to hijack or intercept an unprotected connection. A practice known as wardriving involves individuals equipped with a computer, a wireless card, and a GPS device driving through areas in search of wireless networks and identifying the specific coordinates of a network location. This information is then usually posted online. Some individuals who participate in or take advantage of wardriving have malicious intent and could use this information to hijack your home wireless network or intercept the connection between your computer and a particular hotspot.

What Can You Do to Minimize the Risks to Your Wireless Network?

Change default passwords – Most network devices, including wireless access points, are preconfigured with default administrator passwords to simplify setup. These default passwords are easily found online, so they don't provide any protection. Changing default passwords makes it harder for attackers to take control of the device

Restrict access – Only allow authorized users to access your network. Each piece of hardware connected to a network has a MAC (media access control) address. You can restrict or allow access to your network by filtering MAC addresses. Consult your user documentation to get specific information about enabling these features. There are also several technologies available that require wireless users to authenticate before accessing the network.

Encrypt the data on your network – WEP (Wired Equivalent Privacy) and WPA (Wi-Fi Protected Access) both encrypt information on wireless devices. However, WEP has a number of security issues that make it less effective than WPA, so you should specifically look for gear that supports encryption via WPA. Encrypting the data would prevent anyone who might be able to access your network from viewing your data.

Protect your SSID – To avoid outsiders easily accessing your network, avoid publicizing your SSID. Consult your user documentation to see if you can change the default SSID to make it more difficult to guess.

Install a firewall – While it is a good security practice to install a firewall on your network, you should also install a firewall directly on your wireless devices (a host-based firewall). Attackers who can directly tap into your wireless network may be able to circumvent your network firewall – a host-based firewall will add a layer of protection to the data on your computer.

Maintain anti-virus software – You can reduce the damage attackers may be able to inflict on your network and wireless computer by installing anti-virus software and keeping your virus definitions up to date. Many of these programs also have additional features that may protect against or detect spyware and Trojan horses.

Questions

1. Discuss the security threats related with wireless networks.
2. Discuss the importance of anti-virus software.

Source: http://www.us-cert.gov/ncas/tips/ST05-003

2.4 Summary

- Wireless networks utilize components similar to wired networks; however, wireless networks must convert information signals into a form suitable for transmission through the air medium.
- A wireless router has a physical network connection which would be connected to a wired network.
- A wireless access point (AP) can be used to join wireless devices to a wired network, or to extend the range of a wireless network.
- The simplest wireless network contains only one AP and that the issues that you need to deal with for one AP are generally placement and signal loss.
- A NIC is usually a separate adapter card that slides into one of the server's motherboard expansion slots.
- However, most newer computers have the NIC built into the motherboard, so a separate card isn't needed.
- Network architecture is the design of a communications network.
- It is a framework for the specification of a network's physical components and their functional organization and configuration, its operational principles and procedures, as well as data formats used in its operation.

2.5 Keywords

Base Station: Is a wireless communications station installed at a fixed location and used to communicate.

Communication Protocol: It is a set of standards designed to specify how computers interact and exchange messages.

Network Architecture: Network Architecture is the design of a communications network. It is a framework for the specification of a network's physical components and their functional organization and configuration, its operational principles and procedures, as well as data formats used in its operation.

Network Interface Card: It is usually a separate adapter card that slides into one of the server's motherboard expansion slots.

Point-to-multipoint (PMP): PMP communication refers to communication that is accomplished through a distinct and specific form of one-to-many connections, offering several paths from one single location to various locations.

Point-to-point Connection: It refers to a communications connection between two nodes or endpoints.

Wireless Access Controller: Wireless Access Controller is a highly scalable and flexible platform that allows you to manage all the wireless access points in a network as a whole rather than individually.

Wireless Access Point (AP): It can be used to join wireless devices to a wired network, or to extend the range of a wireless network.

Wireless Internet Service Provider (WISP): WISP is an Internet service provider with a network based on wireless networking.

Notes

2.6 Review Questions

1. Describe wireless system networking routers.
2. What is communication protocol?
3. Explain wireless network infrastructures.
4. Describe point-to-point communication systems.
5. Discuss open systems interconnection model.
6. Write a brief note on information signals.
7. Explain network interface cards (NICS).
8. Explain Wireless Internet service provider (ISP/WISP).
9. What is Point-to-multipoint communication systems?
10. Show two way radio system diagrammatically.

Answers: Self Assessment

1. Remote
2. P2P, Pt2Pt
3. point-to-multipoint
4. Base
5. Interference
6. Access
7. Networks (hardware)
8. NIC
9. False
10. True
11. False
12. True
13. True
14. True
15. False
16. True

2.7 Further Readings

Books

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

John Ross, *Introduction to wireless networks.*

Vijay Garg, *Wireless Communications & Networking.*

Theodore S. Rappaport, *Wireless Communications: Principles and Practice.*

Online links

http://www.life123.com/technology/computer-networking/wireless-network/components-of-wireless-network.shtml

http://education-portal.com/academy/lesson/network-interface-card-nic-types-function-definition.html

http://www.cse.wustl.edu/~jain/cse574-08/ftp/medical/

http://www.rfidc.com/docs/introductiontowireless_standards.htm

Unit 3: Radio Frequency and Light Signal Fundamentals

CONTENTS

Objectives

Introduction

3.1 Wireless Transceivers

3.1.1 Digi Wireless Transceiver Modules

3.2 Understanding RF Signals

3.2.1 RF Signal Attributes

3.2.2 RF Signal Pros and Cons

3.2.3 RF Signal Impairments

3.2.4 Interference

3.2.5 Multipath

3.3 Working of Light Signals

3.4 Modulation

3.4.1 Frequency Shift Keying (FSK)

3.4.2 Phase Shift Keying (PSK)

3.4.3 Quadrature Amplitude Modulation (QAM)

3.4.4 Spread Spectrum

3.4.5 Orthogonal Frequency Division Multiplexing (OFDM)

3.4.6 Ultra Wideband (UWB) Modulation

3.5 Sending Data Packets in the Air

3.6 Summary

3.7 Keywords

3.8 Review Questions

3.9 Further Readings

Objectives

After studying this unit, you will be able to:

- Describe the Radio frequency and radio frequency receiver
- Discuss the working of light signals
- Explain about wireless transceiver
- Discuss the modulation and amplification

Introduction

Radio frequency (RF) is a rate of oscillation in the range of about 3 kHz to 300 GHz, which corresponds to the frequency of radio waves, and the alternating currents which carry radio

Notes

signals. RF usually refers to electrical rather than mechanical oscillations; however, mechanical RF systems do exist.

Although radio frequency is a rate of oscillation, the term "radio frequency" or its abbreviation "RF" are also used as a synonym for radio – i.e. to describe the use of wireless communication, as opposed to communication via electric wires.

Example: Radio-frequency identification and ISO/IEC 14443-2 Radio frequency power and signal interface.

To receive radio signals an antenna must be used. However, since the antenna will pick up thousands of radio signals at a time, a radio tuner is necessary to tune in to a particular frequency (or frequency range). This is typically done via a resonator – in its simplest form, a circuit with a capacitor and an inductor forming a tuned circuit. The resonator amplifies oscillations within a particular frequency band, while reducing oscillations at other frequencies outside the band.

Fiber-optic communication is a method of transmitting information from one place to another by sending pulses of light through an optical fiber. The light forms an electromagnetic carrier wave that is modulated to carry information. First developed in the 1970s, fiber-optic communication systems have revolutionized the telecommunications industry and have played a major role in the advent of the Information Age. Because of its advantages over electrical transmission, optical fibers have largely replaced copper wire communications in core networks in the developed world.

The process of communicating using fiber-optics involves the following basic steps: Creating the optical signal involving the use of a transmitter, relaying the signal along the fiber, ensuring that the signal does not become too distorted or weak, receiving the optical signal, and converting it into an electrical signal.

Fiber optics is a medium for carrying information from one point to another in the form of light. Unlike the copper form of transmission, fiber optics is not electrical in nature. A basic fiber optic system consists of a transmitting device that converts an electrical signal into a light signal, an optical fiber cable that carries the light, and a receiver that accepts the light signal and converts it back into an electrical signal. The complexity of a fiber optic system can range from very simple (i.e., local area network) to extremely sophisticated and expensive (i.e., long distance telephone or cable television trunking).

Example: A system could be built very inexpensively using a visible LED, plastic fiber, a silicon photodetector, and some simple electronic circuitry. The overall cost could be less than $20.

On the other hand, a typical system used for long-distance, high-bandwidth telecommunication could cost tens or even hundreds of thousands of dollars.

3.1 Wireless Transceivers

An infrared transceiver, or IR transceiver, is capable of both sending and receiving infrared data. In other words an IR transceiver is a transmitter and a receiver housed together in one single unit and having circuitry in common. IR transceivers are often used for portable or mobile use. Some transceivers can do both functions at the same time, while other transceivers can only do one function at a time. The device may either have a focused beam, thus requiring it to be in a precise position in order to function properly, or it may be a broader beam, depending on the applications that it is designed for.

There are many different kinds of infrared transceivers. The most common types categorized by speed, size, supply voltage, link, data rate, packaging type and maximum idle current.

The most common link size is 1 m. There are also infrared transceivers with link size as low as 875 nm or as high as 6.5 m. The maximum idle current available is 10 A, with the most common infrared transceiver chips having a maximum idle current of 10 mA.

IR transceivers are generally used in communications applications, although they also have other applications as well. In communications, infrared transceivers can often be used in order to synch devices.

Example: A PDA can be synched with a PC through the use of infrared transceivers in both devices. The systems can send data back and forth to synchronize their contents.

IR transceivers can also be used for entering and collecting data in the field. By using a handheld IR transceiver, a researcher can collect data on his portable device and then send it to a PC by using an infrared transceiver. The transceiver can also receive software upgrades, therefore keeping it up to date with the rest of the equipment in the laboratory or the plant.

3.1.1 Digi Wireless Transceiver Modules

The TRX900 is an encrypted digital wireless transmitter with optional internal backup recording and IFB. By incorporating an IFB receiver into the body of a traditional wireless transmitter, both functions are now combined in a package smaller than most transmitters on the market today.

- Fully encrypted audio transmission
- Built-in 2.4 GHz receiver to receive timecode and remote control signals from ZaxNet and/ or IFB100
- Digital modulation wireless transmitter
- Superb audio quality that rivals a mic cable
- Digital drop-out protection
- 5 hour run time on single CR123 battery
- Graphic LCD display
- Integrated timecode reception
- Small and lightweight
- No inter-modulation – up to 50 transmitters, in the same frequency block, can be used together.
- Built-in IFB audio receiver
- 96 hour internal backup recording with timecode stamp

The TRX900AA's 96 hour, 24 bit internal loop-recording option is perfect for those times when there's a lack of available frequencies or when drop-outs cannot be tolerated. The audio is timecode referenced, recorded on and played back from a removable MicroSD memory card that can be used in any standard SD card reader.

Audio can be recorded, played back and timecode referenced either manually or through remote control commands from the IFB100 transmitter.

The audio is automatically recorded full bandwidth as a .ZAX file. The included ZaxConvert file transfer software (available for both MAC and PC) utilizes sample rate conversion to obtain the sample rate and bit depth of choice when files are imported to your computer. There are two timecode stamped file types to choose from: BWF (Broadcast Wave Format) or MP3 (MPEG-1 Audio Layer 3). MP3 files are great for quickly transferring files over the internet to a transcription house. Any number of versions of the same recording can be made from a single file.

Notes

Did u know? The TRX900 internal IFB audio option adds the ability to receive IFB (confidence) audio directly on the bodypack via the built-in 2.4 GHz receiver. To monitor audio an EA100 or Stereo Adapter is required.

3.2 Understanding RF Signals

A frequency of electromagnetic radiation in the range at which radio signals are transmitted, ranging from approximately 3 kilohertz to 300 gigahertz. Many astronomical bodies, such as pulsars, quasars, and possibly black holes, emit radio frequency radiation is called radio frequency.

3.2.1 RF Signal Attributes

All RF waves have characteristics that vary to define the wave. Some of these properties can be modified to modulate information onto the wave. These properties are wavelength, frequency, amplitude, and phase.

- ***Wavelength:*** The wavelength of an RF wave is calculated as the distance between two adjacent identical points on the wave. The wavelength is frequently measured as the distance from one crest of the wave to the next.
- ***Frequency:*** Frequency refers to the number of wave cycles that occur in a given window of time. Usually measured in second intervals, a frequency of 1 kilohertz (KHz) would represent 1000 cycles of the wave in 1 second. To remember this, just keep in mind that a wave cycles frequently and just how frequently it cycles determines its frequency.
- ***Amplitude:*** You might wonder that the volume of sound waves is dependent on the frequency, since lower-frequency waves are heard at a greater distance; however, there is actually another characteristic of waves that impacts the volume. Remember, at greater distances, shorter-wavelength waves are more difficult to detect as the waveform spreads ever wider (though this may be more a factor of the antenna used than of the waveform itself). The characteristic that defines the volume is known as amplitude. In sound wave engineering, an increase in amplitude is equivalent to an increase in volume; hence, an amplifier adds to the volume, or makes the sound louder. While the frequency affects the distance a sound wave can travel, the amplitude affects the ability to detect (hear) the sound wave at that distance. RF waves are similar.
- ***Phase:*** Unlike wavelength, frequency, and amplitude, phase is not a characteristic of a single RF wave but is instead a comparison between two RF waves. If two copies of the same RF wave arrive at a receiving antenna at the same time, their phase state will impact how the composite wave is able to be used. When the waves are in phase, they strengthen each other, and when the waves are out of phase, they sometimes strengthen and sometimes cancel each other. In specific out-of-phase cases, they only cancel each other. Phase is measured in degrees, though real-world analysis usually benefits only from the knowledge of whether the waves are in phase or out of phase. Two waves that are completely out of phase would be 180 degrees out of phase, while two waves that are completely in phase would be 0 degrees out of phase.

Caution When troubleshooting wireless networks, the phase of duplicate RF signals is mostly an implication of reflection or scattering in an area that may cause dead zones due to the out-of-phase signals.

3.2.2 RF Signal Pros and Cons

Notes

Advantages of RF include:

- *Efficiency:* RFID tags do not require line-of-sight to be deciphered They can be read through cardboard, plastic, wood and even the human body. RFID tags can easily track moving objects and send the required information back to the reader. This eliminates human errors, reduces labor and provides quick access to a wealth of information.
- *Return on Investment (ROI):* RFID costs more to implement than a barcode system, but provides a good return on investment in the long run, since RFID is significantly more efficient.
- *Less Vulnerable to Damage:* RFID tags are less susceptible to damage. An RFID tag is securely placed within an object or embedded in plastic, enabling the system to be used in a variety of harsh environments, such as areas of high temperature or moisture, or with exposure to chemicals or the outdoors.

Disadvantages of RF include:

- *Expense:* RFID systems are typically more expensive than alternatives such as barcode systems. While passive tag reading is similar to (and generally less expensive than) barcode reading, active tags are costly due to their complexity. Active tags consist of an antenna, radio transceiver and microchip, increasing the overall cost of an RFID system.
- *Collision:* Tag collision and reader collision are common problems with RFID. Tag collision occurs when numerous tags are present in a confined area. The RFID tag reader energizes multiple tags simultaneously, all of which reflect their signals back to the reader. This results in tag collision, and the RFID reader fails to differentiate between incoming data. RFID reader collision results when the coverage area managed by one RFID reader overlaps with the coverage area of another reader. This causes signal interference and multiple reads of the same tag.
- *Security:* RFID technology gives rise to numerous security concerns. Since the system is not limited to line-of-sight, external (and malicious) high-intensity directional antennas could be used to scan sensitive tags. Fraud is always a possibility when the technology is used for high-security operations, such as payment verification.

3.2.3 RF Signal Impairments

Interference and multipath propagation causes lower performance in the communication between the sender and receiver.

3.2.4 Interference

Electromagnetic radiation which is emitted by electrical circuits carrying rapidly changing signals, as a by-product of their normal operation, and which causes unwanted signals (interference or noise) to be induced in other circuits. The most important means of reducing RFI are: use of bypass or “decoupling” capacitors on each active device (connected across the power supply, as close to the device as possible), rise time control of high speed signals using series resistors and VCC filtering. Shielding is usually a last resort after other techniques have failed because of the added expense of RF gaskets and the like.

The efficiency of the radiation is dependant on the height above the ground or power plane (at RF one is as good as the other) and the length of the conductor in relationship to the wavelength of the signal component [fundamental, harmonic or transient (overshoot, undershoot or ringing)]. At lower frequencies, such as 133 MHz, radiation is almost exclusively via I/O cables; RF noise gets onto the power planes and is coupled to the line drivers via the VCC and ground pins. The Rf is then coupled to the cable through the line driver as common node noise. Since the noise is common mode, shielding has very little effect, even with differential pairs. The RF energy is capacitively coupled from the signal pair to the shield and the shield itself does the radiating.

At higher frequencies, usually above 500 MHz, traces get electrically longer and higher above the plane. Two techniques are used at these frequencies: wave shaping with series resistors and embedding the traces between the two planes. If all these measures still leave too much RFI, shielding such as RF gaskets and copper tape can be used. Most digital equipment is designed with metal, or coated plastic, cases.

Switching power supplies can be a source of RFI, but have become less of a problem as design techniques have improved.

Most countries have legal requirements that electronic and electrical hardware must still work correctly when subjected to certain amounts of RFI, and should not emit RFI which could interfere with other equipment (such as radios).

3.2.5 Multipath

In wireless telecommunications, multipath is the propagation phenomenon that results in radio signals reaching the receiving antenna by two or more paths. Causes of multipath include atmospheric ducting, ionospheric reflection and refraction, and reflection from water bodies and terrestrial objects such as mountains and buildings.

The effects of multipath include constructive and destructive interference, and phase shifting of the signal. Destructive interference causes fading. Where the magnitudes of the signals arriving by the various paths have a distribution known as the Rayleigh distribution, this is known as Rayleigh fading. Where one component (often, but not necessarily, a line of sight component) dominates, a Rician distribution provides a more accurate model, and this is known as Rician fading.

In facsimile and television transmission, multipath causes jitter and ghosting, seen as a faded duplicate image to the right of the main image. Ghosts occur when transmissions bounce off a mountain or other large object, while also arriving at the antenna by a shorter, direct route, with the receiver picking up two signals separated by a delay.

In radar processing, multipath causes ghost targets to appear, deceiving the radar receiver. These ghosts are particularly bothersome since they move and behave like the normal targets (which they echo), and so the receiver has difficulty in isolating the correct target echo. These problems can be overcome by incorporating a ground map of the radar's surroundings and eliminating all echoes which appear to originate below ground or above a certain height.

In digital radio communications (such as GSM) multipath can cause errors and affect the quality of communications. The errors are due to intersymbol interference (ISI). Equalisers are often used to correct the ISI. Alternatively, techniques such as orthogonal frequency division modulation and rake receivers may be used.

Notes In a Global Positioning System receiver, Multipath Effect can cause a stationary receiver's output to indicate as if it were randomly jumping about or creeping. When the unit is moving the jumping or creeping is hidden, but it still degrades the displayed accuracy.

Self Assessment

Fill in the blanks:

1. .... communication is a method of transmitting information from one place to another by sending pulses of light through an optical fiber.
2. Fiber optics is a medium for carrying information from one point to another in the form of ....
3. .... transceivers are often used for portable or mobile use.
4. A frequency of electromagnetic radiation in the range at which radio signals are transmitted, ranging from approximately 3 kilohertz to .... gigahertz.
5. The .... is frequently measured as the distance from one crest of the wave to the next.
6. .... is used for many modern RF modulation algorithms.
7. Tag collision and reader collision are common problems with ....
8. .... collision occurs when numerous tags are present in a confined area.
9. RFID .... collision results when the coverage area managed by one RFID reader overlaps with the coverage area of another reader.
10. .... are often used to correct the ISI.

3.3 Working of Light Signals

Light signals have been in use with communications systems for even longer than RF systems. Lanterns would provide a source of light to use with sending codes between ships at sea hundreds of years ago. Light guns are still in use today at many airports as a backup communication with aircraft having malfunctioning radio gear.

Wireless networks that utilize light signals, however, are not as common as these that use radio signals. Light signals generally satisfy needs for special applications, such as building-to-building links and short-range personal-area networks. Some wireless LANs and inter-building products use laser light to carry information between computers.

A light signal is analog in form and has a very high frequency that's not regulated by the FCC. Most wireless networks that use light for wireless signaling purposes utilize infrared light, which has a wavelength of approximately 900 nanometers. This equates to 333,333 GHz, which is quite a bit higher than RF signals and falls just below the visual range of humans.

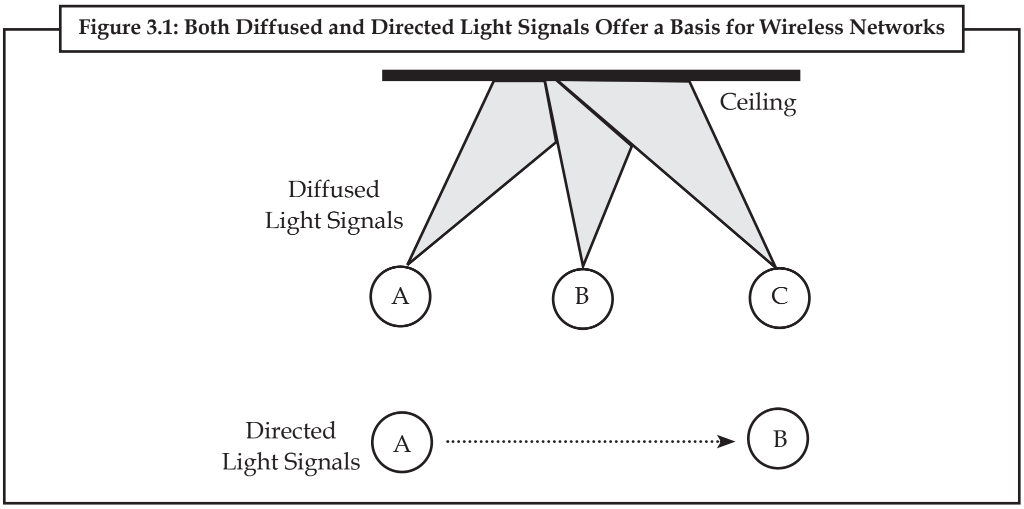
Diffused and direct infrared are two main types of light transmission. Figure 3.1 illustrates these two concepts. Diffused laser light is normally reflected off a wall or ceiling, and direct laser is directly focused in a line-of-sight fashion. Most laser LANs utilize diffused infrared; inter-building modems and PDAs use the direct infrared technique.

Infrared light has very high bandwidth; however, the diffusing technique severely attenuates the signal and requires slow data transmissions (less than 1 Mbps) to avoid significant transmission errors. In addition, this technique limits wireless component spacing to around 40 feet, mainly because of the lower ceilings indoors and resulting signal path geometry. The advantage is relatively easy installation with inexpensive components.

The direct infrared approach, commonly referred to as free-space optics, intensifies the light signal power similarly to a directive radio signal antenna. This increases the range of low-power laser systems to a mile or so at data rates up in the Gbps range.

Notes

Figure 3.1: Both Diffused and Directed Light Signals Offer a Basis for Wireless Networks



Source: http://etutorials.org/Networking/wn/Chapter+3.+Radio+Frequency+and+Light+Signal+Fundamentals+The+Invisible+Medium/Understanding+Light+Signals/

As with RF signals, the amplitude of light also decreases as distance between the sending and receiving stations increase. The range of an infrared light system can vary from a few feet with PDA applications to 1 mile with direct infrared systems. This is significantly less range than with RF systems.

As compared to RF signals, light signals have the characteristics defined in Table 3.1.

Table 3.1: Comparing the Pros and Cons of Light Signals

Light Signal Pros	Light Signal Cons
Extremely high throughput, up to the Gbps range	Variable, unreliable performance in the presence of significant smog, fog, rain, snow, and other airborne particulate matter
High inherent security because of narrow laser beam	Relatively short-range (1 mile) capability
License-free operation	Requirement for line-of-sight operation, free from obstructions such as buildings, trees, and telephone poles
Extremely low potential for RF interference from external systems	Issues dealing with alignment because of building swaying

Source: http://etutorials.org/Networking/wn/Chapter+3.+Radio+Frequency+and+Light+Signal+Fundamentals+The+Invisible+Medium/Understanding+Light+Signals/

These characteristics make the use of light signals most effective for specialized applications where extremely high performance is necessary. For example, a company can install an infrared communications link between two nearby buildings in order to facilitate high-speed server backups over a wireless network.

Light signal propagation is not free from difficulties. Impairments, such as interference and obstructions, limit the performance of the wireless network that uses light signals.

Light signals are free from RF sources of interference such as cordless phones, and microwave ovens. In fact, the FCC doesn’t regulate light signals because of extremely limited potential interference among systems. Light signals have such a high frequency that their emissions are well outside the spectrum of RF systems, which means that the FCC doesn’t regulate light signals.

Interference from other sources of light, however, can still be a problem for systems that use light signals. For example, the installation of a point-to-point infrared transmission system aimed in an easterly or westerly direction can receive substantial interference from infrared light found within sunlight because the sun is low to the horizon. This interference can be high enough in some cases to completely disrupt transmission of data on the infrared link. When installing these types of systems, be certain to follow the manufacturer's recommendations when orienting the antennae.

Obstructions such as buildings, mountains, and trees offer substantial amounts of attenuation to light signals as they propagate through the air. Most of these objects are composed of materials that readily absorb and scatter the light. As a result, be sure that the path between the end points of a light-based communications system are completely clear of obstacles.

Even if the communications path is open, weather can still impress large amounts of attenuation to light signals. The problem with weather is that it varies. For example, heavy fog might be present, and then the skies might be completely clear the following hour. This makes planning link budgets for light-based systems, especially those operating near the range limits, extremely difficult. Planners must be certain that the attenuation imposed by weather will not disrupt communications.

3.4 Modulation

In electronics and telecommunications, modulation is the process of varying one or more properties of a periodic waveform, called the carrier signal, with a modulating signal which typically contains information to be transmitted. This is done in a similar fashion to a musician modulating a tone (a periodic waveform) from a musical instrument by varying its volume, timing and pitch. The three key parameters of a periodic waveform are its amplitude ("volume"), its phase ("timing") and its frequency ("pitch"). Any of these properties can be modified in accordance with a low frequency signal to obtain the modulated signal. Typically a high-frequency sinusoid waveform is used as carrier signal, but a square wave pulse train may also be used.

In telecommunications, modulation is the process of conveying a message signal, for example a digital bit stream or an analog audio signal, inside another signal that can be physically transmitted. Modulation of a sine waveform is used to transform a baseband message signal into a passband signal, for example low-frequency audio signal into a radio-frequency signal (RF signal). In radio communications, cable TV systems or the public switched telephone network for instance, electrical signals can only be transferred over a limited passband frequency spectrum, with specific (non-zero) lower and upper cutoff frequencies. Modulating a sine-wave carrier makes it possible to keep the frequency content of the transferred signal as close as possible to the centre frequency (typically the carrier frequency) of the passband.

A device that performs modulation is known as a modulator and a device that performs the inverse operation of modulation is known as a demodulator (sometimes detector or demod). A device that can do both operations is a modem (from "modulator–demodulator").

The aim of digital modulation is to transfer a digital bit stream over an analog bandpass channel, for example over the public switched telephone network (where a bandpass filter limits the frequency range to between 300 and 3400 Hz), or over a limited radio frequency band.

The aim of analog modulation is to transfer an analog baseband (or lowpass) signal, for example an audio signal or TV signal, over an analog bandpass channel at a different frequency, for example over a limited radio frequency band or a cable TV network channel.

Analog and digital modulation facilitate frequency division multiplexing (FDM), where several low pass information signals are transferred simultaneously over the same shared physical medium, using separate passband channels (several different carrier frequencies).

The aim of digital baseband modulation methods, also known as line coding, is to transfer a digital bit stream over a baseband channel, typically a non-filtered copper wire such as a serial bus or a wired local area network.

The aim of pulse modulation methods is to transfer a narrowband analog signal, for example a phone call over a wideband baseband channel or, in some of the schemes, as a bit stream over another digital transmission system.

In music synthesizers, modulation may be used to synthesise waveforms with an extensive overtone spectrum using a small number of oscillators. In this case the carrier frequency is typically in the same order or much lower than the modulating waveform.

3.4.1 Frequency Shift Keying (FSK)

Frequency shift keying (FSK) is a frequency modulation scheme in which digital information is transmitted through discrete frequency changes of a carrier wave. The simplest FSK is binary FSK (BFSK). BFSK literally implies using a pair of discrete frequencies to transmit binary (0s and 1s) information. With this scheme, the "1" is called the mark frequency and the "0" is called the space frequency. The time domain of an FSK modulated carrier is illustrated in the figures to the right.

3.4.2 Phase Shift Keying (PSK)

Phase shift keying (PSK) is a digital modulation scheme that conveys data by changing, or modulating, the phase of a reference signal (the carrier wave).

Any digital modulation scheme uses a finite number of distinct signals to represent digital data. PSK uses a finite number of phases, each assigned a unique pattern of binary digits. Usually, each phase encodes an equal number of bits. Each pattern of bits forms the symbol that is represented by the particular phase. The demodulator, which is designed specifically for the symbol-set used by the modulator, determines the phase of the received signal and maps it back to the symbol it represents, thus recovering the original data. This requires the receiver to be able to compare the phase of the received signal to a reference signal — such a system is termed coherent (and referred to as CPSK).

Alternatively, instead of operating with respect to a constant reference wave, the broadcast can operate with respect to itself. Changes in phase of a single broadcast waveform can be considered the significant items. In this system, the demodulator determines the changes in the phase of the received signal rather than the phase (relative to a reference wave) itself. Since this scheme depends on the difference between successive phases, it is termed differential phase-shift keying (DPSK). DPSK can be significantly simpler to implement than ordinary PSK since there is no need for the demodulator to have a copy of the reference signal to determine the exact phase of the received signal (it is a non-coherent scheme). In exchange, it produces more erroneous demodulation.

3.4.3 Quadrature Amplitude Modulation (QAM)

Quadrature amplitude modulation (QAM) is both an analog and a digital modulation scheme. It conveys two analog message signals, or two digital bit streams, by changing (modulating) the amplitudes of two carrier waves, using the amplitude-shift keying (ASK) digital modulation scheme or amplitude modulation (AM) analog modulation scheme. The two carrier waves, usually sinusoids, are out of phase with each other by 90° and are thus called quadrature carriers or quadrature components — hence the name of the scheme. The modulated waves are summed, and the resulting waveform is a combination of both phase-shift keying (PSK) and amplitude shift keying (ASK), or (in the analog case) of phase modulation (PM) and amplitude modulation. In the digital QAM case, a finite number of at least two phases and at least two amplitudes are

Notes

used. PSK modulators are often designed using the QAM principle, but are not considered as QAM since the amplitude of the modulated carrier signal is constant. QAM is used extensively as a modulation scheme for digital telecommunication systems. Arbitrarily high spectral efficiencies can be achieved with QAM by setting a suitable constellation size, limited only by the noise level and linearity of the communications channel.

QAM modulation is being used in optical fiber systems as bit rates increase; QAM16 and QAM64 can be optically emulated with a 3-path interferometer.

3.4.4 Spread Spectrum

Spread-spectrum communications technology was first described on paper by an actress and a musician! In 1941 Hollywood actress Hedy Lamarr and pianist George Antheil described a secure radio link to control torpedos. They received U.S. Patent #2.292.387. The technology was not taken seriously at that time by the U.S. Army and was forgotten until the 1980s, when it became active. Since then the technology has become increasingly popular for applications that involve radio links in hostile environments.

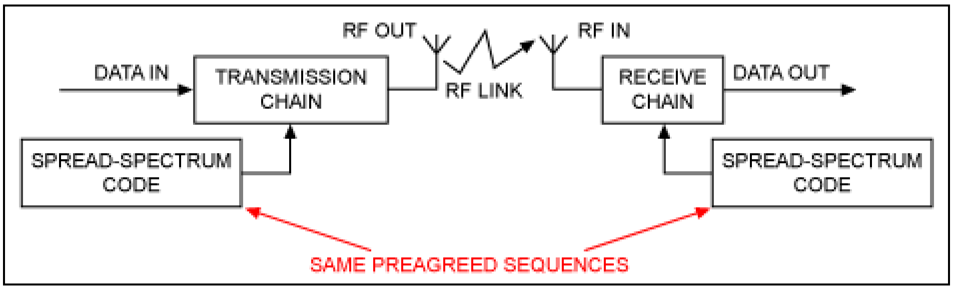
Typical applications for the resulting short-range data transceivers include satellite-positioning systems (GPS), 3G mobile telecommunications, W-LAN (IEEE® 802.11a, IEEE 802.11b, IEEE 802.11g), and Bluetooth. Spread-spectrum techniques also aid in the endless race between communication needs and radio-frequency availability – situations where the radio spectrum is limited and is, therefore, an expensive resource.

Different spread-spectrum techniques are available, but all have one idea in common: the key (also called the code or sequence) attached to the communication channel. The manner of inserting this code defines precisely the spread-spectrum technique. The term "spread spectrum" refers to the expansion of signal bandwidth, by several orders of magnitude in some cases, which occurs when a key is attached to the communication channel.

The formal definition of spread spectrum is more precise: an RF communications system in which the baseband signal bandwidth is intentionally spread over a larger bandwidth by injecting a higher frequency signal (Figure 3.2). As a direct consequence, energy used in transmitting the signal is spread over a wider bandwidth, and appears as noise. The ratio (in dB) between the spread baseband and the original signal is called processing gain. Typical spread-spectrum processing gains run from 10 dB to 60 dB.

To apply a spread-spectrum technique, simply inject the corresponding spread-spectrum code somewhere in the transmitting chain before the antenna (receiver). (That injection is called the spreading operation.) The effect is to diffuse the information in a larger bandwidth. Conversely, you can remove the spread-spectrum code (called a despreading operation) at a point in the receive chain before data retrieval. A despreading operation reconstitutes the information into its original bandwidth. Obviously, the same code must be known in advance at both ends of the transmission channel. (In some circumstances, the code should be known only by those two parties.)

Figure 3.2: Spread-spectrum Communication System



Source: http://www.maximintegrated.com/app-notes/index.mvp/id/1890

3.4.5 Orthogonal Frequency Division Multiplexing (OFDM)

Orthogonal frequency division multiplexing (OFDM) is a method of encoding digital data on multiple carrier frequencies. OFDM has developed into a popular scheme for wideband digital communication, whether wireless or over copper wires, used in applications such as digital television and audio broadcasting, DSL broadband internet access, wireless networks, and 4G mobile communications.

OFDM is essentially identical to coded OFDM (COFDM) and discrete multi-tone modulation (DMT), and is a frequency division multiplexing (FDM) scheme used as a digital multi-carrier modulation method. The word "coded" comes from the use of forward error correction (FEC). A large number of closely spaced orthogonal sub-carrier signals are used to carry data on several parallel data streams or channels. Each sub-carrier is modulated with a conventional modulation scheme (such as quadrature amplitude modulation or phase-shift keying) at a low symbol rate, maintaining total data rates similar to conventional single-carrier modulation schemes in the same bandwidth.

The primary advantage of OFDM over single-carrier schemes is its ability to cope with severe channel conditions (for example, attenuation of high frequencies in a long copper wire, narrowband interference and frequency-selective fading due to multipath) without complex equalization filters. Channel equalization is simplified because OFDM may be viewed as using many slowly modulated narrowband signals rather than one rapidly modulated wideband signal. The low symbol rate makes the use of a guard interval between symbols affordable, making it possible to eliminate intersymbol interference (ISI) and utilize echoes and time-spreading (on analogue TV these are visible as ghosting and blurring, respectively) to achieve a diversity gain, i.e. a signal-to-noise ratio improvement. This mechanism also facilitates the design of single frequency networks (SFNs), where several adjacent transmitters send the same signal simultaneously at the same frequency, as the signals from multiple distant transmitters may be combined constructively, rather than interfering as would typically occur in a traditional single-carrier system.

3.4.6 Ultra Wideband (UWB) Modulation

Ultra-wideband (UWB) signals are generally defined as signals with fractional bandwidth greater then twenty percent of their central frequency or as signals with bandwidth more than 500 MHz, whichever is less. The bandwith is specified by 10 dB decrease of the signal power spectral density. Many different generation techniques may be used to satisfy these requirements. The principal group of generation techniques is based on spectral characteristics of very short pulses and we can denominate these techniques as Impulse Radio concepts. These very short duration pulses (hundreds of picoseconds) have very wide spectrum, which must adhere to the spectral mask requirements. Very low power levels are permitted for typical UWB transmission because of the compatibility with other radiocommunication services. Many pulses are typically combined to carry the information for one bit and to separate individual transmissions of several users. For the same purposes, a variety of pulse shapes, wavelets and waveforms can be used. Pulses can be sent individually, in bursts, or in near-continuous streams, and they can encode information in pulse amplitude, polarity, shape, and position.

3.5 Sending Data Packets in the Air

A central problem for business individuals on the move, concerns the ability to communicate data between the work base and remote locations. A new technology has evolved over the past few years which allows the transmission of digital data across existing air link analogue cellular voice channels as well as across existing Circuit Switched telephone networks. This technology is known as Cellular Digital Packet Data (CDPD).

Notes

This technology allows data from a portable computer or a Personal Digital Assistant (PDA) to be transmitted to Wide Area Computer Networks (WAN) and Public Switched Telephone Networks (PSTN) as well as other mobile units i.e.: mobile phones or portable computers. This allows individuals total freedom to transmit data back to the office from remote locations.

Self Assessment

Fill in the blanks:

11. The three key parameters of a periodic waveform are its............................., its phase ("timing") and its frequency ("pitch").

12. The aim of digital baseband modulation methods, also known as line coding, is to transfer a digital bit stream over a ....channel.

13. .... is a digital modulation scheme that conveys data by changing, or modulating, the phase of a reference signal (the carrier wave).

14. .... technology allows data from a portable computer) to be transmitted to Wide Area Computer Networks (WAN) and Public Switched Telephone Networks (PSTN) as well as other mobile units.

15. .... is used extensively as a modulation scheme for digital telecommunication systems.

Case Study

Stark RFID-Enabled System Helps Brick and Ceramic Product Manufacturers Improve Inventory Control and Delivery Accuracy

The growing acceptance and reliability of RFID technology for supply chain management and asset tracking is spurring software companies to develop RFID solutions that will help them penetrate new markets.

One such example is Stark RFID, based in Greenville, South Carolina, a systems integrator and provider of turnkey RFID solutions designed to transform supply chain efficiency for brick and refractory products manufacturers. The company's innovative StarkFG™ RFID application delivers an accurate, real-time asset tracking solution that greatly improves inventory visibility, management and control.

According to Lance Burnett, the company's cofounder and president, although this market sector has adopted technology-based enterprise solutions for running business processes efficiently, a large majority of companies still rely heavily on manual processes for managing inventory and fulfilling orders.

"For these industries, the challenge of managing inventory is due in large part to the sheer volume of manufactured products in the brickyard or warehouse, which makes manual, line-of-sight inventory difficult, if not impossible," says Burnett. "As we explored the capabilities of RFID technology, we decided to be first-to-market with an inventory tracking system that would make the job faster and easier. Now, having implemented StarkFG in several customer sites, it is clearly proving to be a transformative RFID solution."

Brick Industry Challenges

Brick manufacturers serve the residential and commercial construction industries, typically selling through distribution channels to builders and contractors. In the commercial building market especially, where on-site labor costs are high and sequential workflow is

Contd...

carefully planned, the right materials must be delivered to the right place at the right time to meet construction schedules. This is essential to customer satisfaction.

Burnett explains: "If a load of bricks is not delivered on time, if a shipment is sent to the wrong location, or if the product delivered does not match the order specifications, the entire construction job can be delayed until the right materials can be obtained. This is a costly proposition for builders and, for their suppliers, it can result in punitive fines and even law suits."

Many of the problems experienced by brick manufacturers occur not in the factory, but rather in the brickyard where inventory is stored and prepared for shipment. Manufactured bricks for the construction trade are massed in strapped loads of about 500 bricks to a cube, often called a hack. The cubes are delivered to the brickyard where they sit outdoors, subject to dust, dirt, rain, sleet and snow – making it difficult to label the cubes with vital product information such as electronic product codes and lot numbers. Lot numbers are important, since the same type of bricks manufactured on one day will vary somewhat in color from bricks made the next day. Builders and contractors may refuse to accept a 'mixed run' shipment if the colors are poorly matched.

Before Stark RFID developed the StarkFG solution, entering the newly manufactured cubes of brick into inventory and deciding where it should be stored was a manual process typically performed by brickyard personnel. It was a time- and labor-intensive process, prone to human error. Similarly, when it was time to assemble and load an order for shipping, the process was reversed. This also led to frequent mistakes as workers spent a great deal of time finding, identifying and loading the right cubes of bricks to transport via forklift to waiting trucks.

"We knew these inventory management and quality control issues were the major pain points to be addressed in creating a solution that would bring a higher level of automation to brickyard management," says Burnett. "The concept of building a system for this application on RFID technology struck us as the perfect answer."

Real-Time Inventory Tracking

StarkFG is the first RFID-enabled solution designed specifically to help brick manufacturers automate their inventory management and order fulfillment processes. With this system, the company can print and encode rugged 8-inch wide labels with all the necessary product information, then fold the labels and affix them to each strapped cube of new bricks.

When the cubes are delivered to the brickyard, StarkFG's bin loading module informs the forklift operator's computer where to place the cubes in the yard, based on the type of product being unloaded. Once the bricks have been placed in the proper bin, the inventory system is automatically updated. Likewise, once they are removed from the yard for shipping, they are automatically removed from the inventory count.

More Accurate Order Fulfilment

When an order is scheduled for shipping, the enterprise system generates a pick list and bill of lading and beams them to the computer of a forklift operator, who is directed to the right product location. There the RFID reader reads the tag to verify that the product specifications match the order printed on the pick list and bill of lading before the brick cubes are lifted and loaded for transport to the assigned truck. This process of order location, product identification and verification, which could take a significant amount of time in a manual system, has now been reduced to mere minutes. And, with positive RFID tag identification, the inventory manager and brickyard personnel have the assurance that the right order has been picked.

Combining rugged hardware and weather-proof RFID tags, the StarkFG system eliminates the physical counting of and finding cubes in the brickyard by enabling the product

Contd...

identification tags to be read from virtually any angle, without a direct line of sight. “This capability alone saves significantly on inventory management time and labor and greatly improves inventory and shipping accuracy. RFID tagging could also make it easier for brick suppliers to sell their products to big box retailers with RFID compliance mandates,” notes Burnett.

HackTrac System Components

The components comprising the StarkFG system include:

StarkFG proprietary software, built on a Microsoft MS.Net platform, and incorporating 802.11b wireless communication protocol to integrate with a user’s centralized wireless local area network (WLAN).

Forklift-mounted computers made by Noax Technologies AG, a German producer of ruggedized, industrial touch-panel computers.

RFID readers from Alien Technology, also forklift-mounted.

Rugged, weather-resistant, 8-inch wide, wet inlay RFID tags (Class 1 Gen 2) incorporating Intermec antennas and Avery Dennison RFID’s AD-220 Inlays.

An 8-inch RFID label printer/encoder, supplied by Avery Dennison.

Since each manufacturer has its own inventory management procedures, Stark RFID works closely with customers to map out their processes and configure the system to their specific requirements. The company also provides users with middleware to allow them to integrate the inventory management system with their ERP system, providing a convenient end-to-end turnkey solution.

Burnett adds that Stark RFID performed its own extensive ‘guerilla’ testing of the RFID tags in real-world outdoor environments to ensure their performance, durability and reliability, even under extreme weather conditions.

Real-World Results: Cost Savings, Improved Customer Service.

The true test of an RFID-enabled solution is how well it performs in the real world. According to reports from Stark RFID’s customers, the system has proven to be so reliable that not a single mis-shipment has occurred since StarkFG has been up and running. Among Stark RFID’s brick manufacturing customers are Lee Brick of Sanford, North Carolina, a manufacturer of high quality residential, commercial and architectural brick, and Columbus Brick, a regional brick producer in Columbus, Mississippi.

StarkFG has proven to be a highly effective automation tool for companies in the refractory manufacturing industry as well. One StarkFG user in this market sector is a leading global provider of custom-engineered, high-temperature insulating fibers, firebrick and monolithics used in industrial furnaces and for fire protection. For all users, the primary benefits of the RFID-enabled track-and trace system include improved inventory accuracy, elimination of incorrect shipments, and increased speed and productivity in order picking, loading and shipping. In fact, the inventory manager at Lee Brick said his company was able to completely eliminate manual cycle counts due to the dead-on accuracy of the StarkFG system.

Once StarkFG is implemented and workflow becomes faster and more streamlined, manufacturers may find that fewer forklifts are required in the brickyard or warehouse. The result: more efficient asset utilization, significant cost savings, improved profitability, and higher customer satisfaction.

Burnett asserts that the toughness and durability of the system’s RFID tags are key to its successful performance in these harsh industrial environments. “For a track-and-trace system like StarkFG to work effectively, you need to ensure 100 percent RFID tag read rates

Contd...

Notes

– and we have achieved that goal," he states. "Avery Dennison RFID's technical support team was extremely helpful in guiding our choice of RFID inlays, antennas and tags to be sure they would perform and hold up well over time, even in the toughest environmental conditions."

Questions:

1. Discuss the purpose of designing Stark RFID.
2. Discuss the performance of RFID-enabled system in the real world.

Source: http://www.starkrfid.com/about/rfid-case-studies/stark-rfid-brick-case-study.php

3.6 Summary

- Radio frequency (RF) is a rate of oscillation in the range of about 3 kHz to 300 GHz, which corresponds to the frequency of radio waves, and the alternating currents which carry radio signals.
- Electric currents that oscillate at radio frequencies have special properties not shared by direct current or alternating current of lower frequencies.
- Fiber-optic communication is a method of transmitting information from one place to another by sending pulses of light through an optical fiber.
- Fiber optics is a medium for carrying information from one point to another in the form of light. Unlike the copper form of transmission, fiber optics is not electrical in nature.
- All RF waves have characteristics that vary to define the wave. Some of these properties can be modified to modulate information onto the wave. These properties are wavelength, frequency, amplitude, and phase.
- Wireless networks that utilize light signals, however, are not as common as these that use radio signals.
- Light signals have been in use with communications systems for even longer than RF systems.

3.7 Keywords

Frequency: It refers to the number of wave cycles that occur in a given window of time.

Frequency Shift Keying (FSK): FSK is a frequency modulation scheme in which digital information is transmitted through discrete frequency changes of a carrier wave.

Line Coding: Line Coding is to transfer a digital bit stream over a baseband channel, typically a non-filtered copper wire such as a serial bus or a wired local area network.

Modulation: Modulation is the process of varying one or more properties of a periodic waveform, called the carrier signal, with a modulating signal which typically contains information to be transmitted.

Multipath: Multipath is the propagation phenomenon that results in radio signals reaching the receiving antenna by two or more paths.

Orthogonal Frequency Division Multiplexing (OFDM): OFDM is a method of encoding digital data on multiple carrier frequencies.

Phase-shift Keying (PSK): PSK is a digital modulation scheme that conveys data by changing, or modulating, the phase of a reference signal (the carrier wave).

Radio Frequency (RF): RF is a rate of oscillation in the range of about 3 kHz to 300 GHz, which corresponds to the frequency of radio waves, and the alternating currents which carry radio signals.

TRX900: TRX900 is an encrypted digital wireless transmitter with optional internal backup recording and IFB.

Ultra-wideband (UWB) Signals: UWB signals are generally defined as signals with fractional bandwidth greater then twenty percent of their central frequency or as signals with bandwidth more than 500MHz, whichever is less.

3.8 Review Questions

1. Describe the process of communicating using fiber-optics.
2. What are wireless transceivers?
3. Discuss the properties of RF waves.
4. Discuss the RF signal pros and cons.
5. Describe RF signal impairments.
6. Explain the working of light signals.
7. What do you mean by modulation?
8. Discuss phase shift-keying.
9. Describe quadrature amplitude modulation.
10. Explain orthogonal frequency division multiplexing.

Answers: Self Assessment

1. Fiber-optic
2. Light
3. IR
4. 300
5. Wavelength
6. Phase
7. RFID
8. Tag
9. Reader
10. Equalisers
11. Amplitude (“volume”)
12. Baseband
13. Phase-shift keying (PSK)
14. Cellular Digital Packet Data
15. QAM

3.9 Further Readings

Books

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

John Ross, *Introduction to wireless networks.*

Vijay Garg, *Wireless Communications & Networking.*

Theodore S. Rappaport, *Wireless Communications: Principles and Practice.*

Notes

Online links

http://www.digi.com/technology/rf-articles/wireless-transceiver-module

http://faculty.ccri.edu/jbernardini/JB-Website/ETEK1500/1500Notes/CWNA-ed4-Chapter-2.pdf

http://www.ehow.com/list_6116737_advantages-disadvantages-rfid.html

http://www.urel.feec.vutbr.cz/ra2008/archive/ra2006/abstracts/088.pdf

Unit 4: Wireless Networks Types and PAN Technologies

Notes

CONTENTS

Objectives

Introduction

4.1 Types of Wireless Networks

4.1.1 WPAN (Wireless Personal Area Network)

4.1.2 WLAN (Wireless Local Area Network)

4.1.3 Wireless Metropolitan Area Network (WMAN)

4.2 Wireless PAN Technologies (WPAN)

4.2.1 IEEE 802.15

4.2.2 Bluetooth

4.3 Summary

4.4 Keywords

4.5 Review Questions

4.6 Further Readings

Objectives

After studying this unit, you will be able to:

- Discuss the various types of wireless networks
- Explain wireless PAN Technologies (WPAN)

Introduction

Wireless LAN (WLAN) is very popular nowadays. Maybe you have ever used some wireless applications on your laptop or cellphone. Wireless LANs enable users to communicate without the need of cable. Each WLAN network needs a wireless Access Point (AP) to transmit and receive data from users. Unlike a wired network which operates at full-duplex (send and receive at the same time), a wireless network operates at half-duplex so sometimes an AP is referred as a Wireless Hub.

The major difference between wired LAN and WLAN is WLAN transmits data by radiating energy waves, called radio waves, instead of transmitting electrical signals over a cable. WLAN uses CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) instead of CSMA/CD for media access. WLAN can’t use CSMA/CD as a sending device can’t transmit and receive data at the same time.

Nowadays there are three organizations influencing WLAN standards. They are: ITU-R: which is responsible for allocation of the RF bands , IEEE which specifies how RF is modulated to transfer data and Wi-Fi Alliance that improves the interoperability of wireless products among vendors.

But the most popular type of wireless LAN today is based on the IEEE 802.11 standard, which is known informally as Wi-Fi. The 802.11a operates in the 5.7 GHz ISM band. Maximum transmission speed is 54 Mbps and approximate wireless range is 25–75 feet indoors. 802.11b operates in the

2.4 GHz ISM band. Maximum transmission speed is 11 Mbps and approximate wireless range is 100–200 feet indoors and 802/11g: operates in the 2.4 GHz ISM band. Maximum transmission speed is 54 Mbps and approximate wireless range is 100–200 feet indoors.

The ISM (Industrial, Scientific and Medical) band, which is controlled by the FCC in the US, generally requires licensing for various spectrum use. To accommodate wireless LAN's, the FCC has set aside bandwidth for unlicensed use including the 2.4 Ghz spectrum where many WLAN products operate.

Wi-Fi stands for Wireless Fidelity and is used to define any of the IEEE 802.11 wireless standards. The term Wi-Fi was created by the Wireless Ethernet Compatibility Alliance (WECA). Products certified as Wi-Fi compliant are interoperable with each other even if they are made by different manufacturers. Access points can support several or all of the three most popular IEEE WLAN standards including 802.11a, 802.11b and 802.11g.

4.1 Types of Wireless Networks

There are three primary usage scenarios for wireless connectivity:

1. Wireless Personal Area Networking (WPAN)
2. Wireless Local Area Networking (WLAN)
3. Wireless Wide Area Networking (WWAN)

4.1.1 WPAN (Wireless Personal Area Network)

WPAN describes an application of wireless technology that is intended to address usage scenarios that are inherently personal in nature. The emphasis is on instant connectivity between devices that manage personal data or which facilitate data sharing between small groups of individuals. An example might be synchronizing data between a PDA and a desktop computer. Or another example might be spontaneous sharing of a document between two or more individuals. The nature of these types of data sharing scenarios is that they are ad hoc and often spontaneous. Wireless communication adds value for these types of usage models by reducing complexity (i.e. eliminates the need for cables).

A wireless personal area network (WPAN) is a personal area network – a network for interconnecting devices centred around an individual person's workspace – in which the connections are wireless. Wireless PAN is based on the standard IEEE 802.15. The two kinds of wireless technologies used for WPAN are Bluetooth and Infrared Data Association.

A WPAN could serve to interconnect all the ordinary computing and communicating devices that many people have on their desk or carry with them today; or it could serve a more specialized purpose such as allowing the surgeon and other team members to communicate during an operation.

A key concept in WPAN technology is known as "plugging in". In the ideal scenario, when any two WPAN-equipped devices come into close proximity (within several meters of each other) or within a few kilometres of a central server, they can communicate as if connected by a cable. Another important feature is the ability of each device to lock out other devices selectively, preventing needless interference or unauthorised access to information.

The technology for WPANs is in its infancy and is undergoing rapid development. Proposed operating frequencies are around 2.4 GHz in digital modes. The objective is to facilitate seamless operation among home or business devices and systems. Every device in a WPAN will be able to plug into any other device in the same WPAN, provided they are within physical range of one another. In addition, WPANs worldwide will be interconnected.

Example: An archeologist on site in Greece might use a PDA to directly access databases at the University of Minnesota in Minneapolis, and to transmit findings to that database.

- ***Bluetooth:*** Bluetooth uses short-range radio waves over distances up to approximately 10 metres. For example, Bluetooth devices such as a keyboards, pointing devices, audio head sets, printers may connect to personal digital assistants (PDAs), cell phones, or computers wirelessly.

  A Bluetooth PAN is also called a piconet (combination of the prefix "pico," meaning very small or one trillionth, and network), and is composed of up to 8 active devices in a master-slave relationship (a very large number of devices can be connected in "parked" mode). The first Bluetooth device in the piconet is the master, and all other devices are slaves that communicate with the master. A piconet typically has a range of 10 metres (33 ft), although ranges of up to 100 metres (330 ft) can be reached under ideal circumstances.

- ***Infrared Data Association:*** Infrared Data Association (IrDA) uses infrared light, which has a frequency below the human eye's sensitivity. Infrared in general is used, for instance, in TV remotes. Typical WPAN devices that use IrDA include printers, keyboards, and other serial data interfaces.

- ***WiFi:*** WiFi uses radio waves for connection over distances up to around 91 metres, usually in a local area network (LAN) environment. Wifi can be used to connect local area networks, to connect cellphones to the Internet to download music and other multimedia, to allow PC multimedia content to be stream to the TV (Wireless Multimedia Adapter), and to connect video game consoles to their networks (Nintendo WiFi Connection).

- ***Body area network:*** A body area networks is based on the IEEE 802.15.6 standard for transmission via the capacitive near field of human skin allowing near field communication of devices worn by and near the wearer. The Skinplex implementation can detect and communicate up to 1 metre (3 ft 3 in) from a human body. It is used for access control to door locks and jamming protection in convertible car roofs.

4.1.2 WLAN (Wireless Local Area Network)

WLAN on the other is more focused on organisational connectivity not unlike wire based LAN connections. The intent of WLAN technologies is to provide members of workgroups access to corporate network resources be it shared data, shared applications or e-mail but do so in way that does not inhibit a user's mobility. The emphasis is on a permanence of the wireless connection within a defined region like an office building or campus. This implies that there are wireless access points that define a finite region of coverage.

Wireless local area networks (WLANs) are the same as the traditional LAN but they have a wireless interface. With the introduction of small portable devices such as PDAs (personal digital assistants), the WLAN technology is becoming very popular. WLANs provide high speed data communication in small areas such as a building or an office. It allows users to move around in a confined area while they are still connected to the network.

Example: Example of wireless LAN that are available today are NCR's waveLAN and Motorola's ALTAIR.

Transmission Technology

There are three main ways by which WLANs transmit information : microwave, spread spectrum and infrared.

1. ***Microwave Transmission:*** Motorola's WLAN product (ALTAIR) transmits data by using low powered microwave radio signals. It operates at the 18 GHz frequency band.

2. ***Spread Spectrum Transmission:*** With this transmission technology, there are two methods used by wireless LAN products: frequency hopping and direct sequence modulation.

   (a) *Frequency Hopping:* The signal jumps from one frequency to another within a given frequency range. The transmitter device "listens" to a channel, if it detects an idle time (i.e. no signal is transmitted), it transmits the data using the full channel bandwidth. If the channel is full, it "hops" to another channel and repeats the process. The transmitter and the receiver "jump" in the same manner.

   (b) *Direct Sequence Modulation:* This method uses a wide frequency band together with Code Division Multiple Access (CDMA). Signals from different units are transmitted at a given frequency range. The power levels of these signals are very low (just above background noise). A code is transmitted with each signal so that the receiver can identify the appropriate signal transmitted by the sender unit. The frequency at which such signals are transmitted is called the ISM (industrial, scientific and medical) band. This frequency band is reserved for ISM devices. The ISM band has three frequency ranges: 902–928, 2400–2483.5 and 5725–5850 MHz. An exception to this is Motorola's ALTAIR which operates at 18 GHz. Spread spectrum transmission technology is used by many wireless LAN manufacturers such as NCR for wave LAN product and SpectraLink for the 2000 PCS.

3. ***Infrared Transmission:*** This method uses infrared light to carry information. There are three types of infrared transmission: diffused, directed and directed point-to-point.

   (a) *Diffused:* The infrared light transmitted by the sender unit fills the area (e.g. office). Therefore the receiver unit located anywhere in that area can receive the signal.

   (b) *Directed:* The infrared light is focused before transmitting the signal. This method increases the transmission speed.

   (c) *Directed point-to-point:* Directed point-to-point infrared transmission provides the highest transmission speed. Here the receiver is aligned with the sender unit. The infrared light is then transmitted directly to the receiver.

The light source used in infrared transmission depends on the environment. Light emitting diode (LED) is used in indoor areas, while lasers are used in outdoor areas.

⚠ *Caution* Infrared radiation (IR) has major biological effects. It greatly affects the eyes and skin. Microwave signals are also dangerous to health. But with proper design of systems, these effects are reduced considerably.

Technical Standards

Technical standards are one of the main concerns of users of wireless LAN products. Users would like to be able to buy wireless products from different manufacturers and be able to use them on one network. The IEEE Project 802.11 has set up universal standards for wireless LAN. In this section we will consider some of these standards.

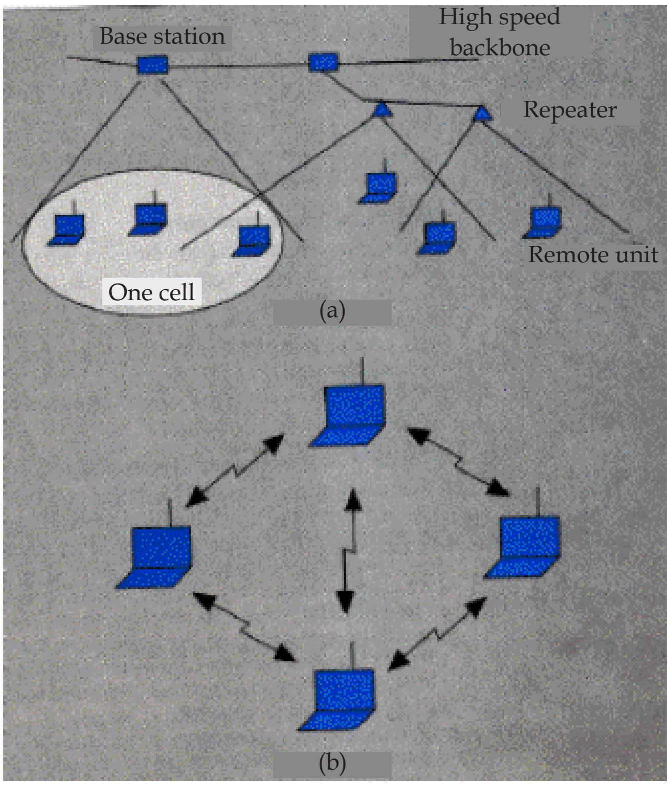
Requirements

In March 1992 the IEEE Project 802.11 established a set of requirements for wireless LAN. The minimum bandwidth needed for operations such as file transfer and program loading is 1 Mbps. Operations which need real-time data transmission such as digital voice and process control, need support from time bounded services.

Types of Wireless LAN

The Project 802.11 committee distinguished between two types of wireless LAN: "ad-hoc" and "infrastructured" networks.

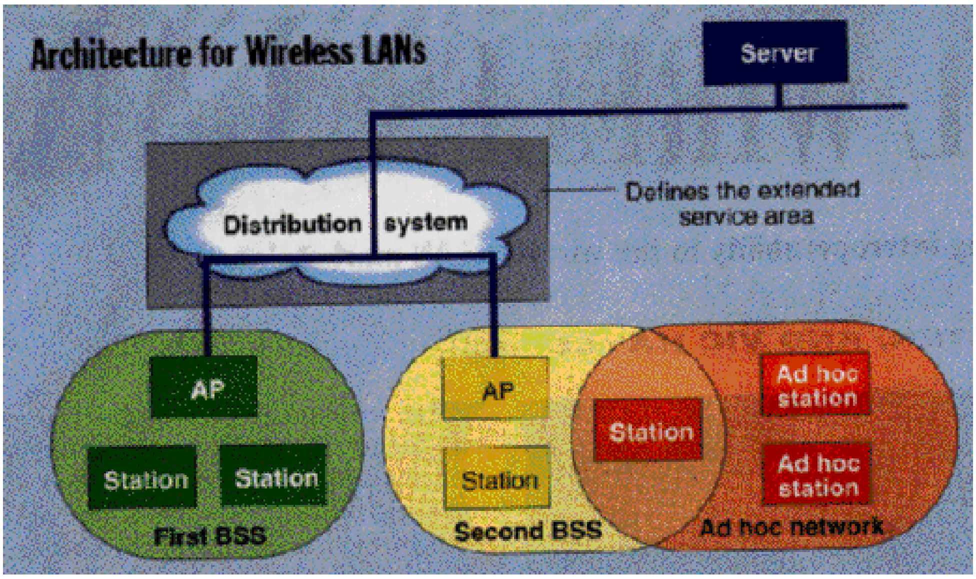
Figure 4.1: (a) Infrastructured Wireless LAN; (b) Ad-hoc Wireless LAN



Source: http://www.doc.ic.ac.uk/~nd/surprise_95/journal/vol2/mjf/article2.html

- ***Ad-hoc Networks:*** Figure 4.1b shows an ad-hoc network. This network can be set up by a number mobile users meeting in a small room. It does not need any support from a wired/ wireless backbone. There are two ways to implement this network.
- ***Broadcasting/Flooding:*** Suppose that a mobile user A wants to send data to another user B in the same area. When the packets containing the data are ready, user A broadcasts the packets. On receiving the packets, the receiver checks the identification on the packet. If that receiver was not the correct destination, then it rebroadcasts the packets. This process is repeated until user B gets the data.
- ***Temporary Infrastructure:*** In this method, the mobile users set up a temporary infrastructure. But this method is complicated and it introduces overheads. It is useful only when there is a small number of mobile users.
- ***Infrastructure Networks:*** Figure 4.1a shows an infrastructure-based network. This type of network allows users to move in a building while they are connected to computer resources. The IEEE Project 802.11 specified the components in a wireless LAN architecture. In an infrastructure network, a cell is also known as a Basic Service Area (BSA). It contains a number of wireless stations. The size of a BSA depends on the power of the transmitter and receiver units, it also depends on the environment. A number of BSAs are connected to each other and to a distribution system by Access Points (APs). A group of stations belonging to an AP is called a Basic Service Set (BSS). Figure 4.2 shows the basic architecture for wireless LANs.

Figure 4.2: Architecture for Wireless LANs



Source: http://www.doc.ic.ac.uk/~nd/surprise_95/journal/vol2/mjf/article2.html

Conclusion

Wireless LAN provide high speed data communication. The minimum data rate specified by the IEEE Project 802.11 is 1 Mbps. NCR's waveLAN operates at 2 Mbps, while Motorola's ALTAIR operates at 15 Mbps.

Because of their limited mobility and short transmission range, wireless LANs can be used in confined areas such as a conference room.

Did u know? In the U.S., almost all WLANs products use spread spectrum transmission. Therefore they transmit information on the ISM band. But with this frequency band, users can experience interference from other sources using this band.

4.1.3 Wireless Metropolitan Area Network (WMAN)

Whereas WLAN addresses connectivity within a defined region, WWAN addresses the need to stay connected while travelling outside this boundary. Today, cellular technologies enable wireless computer connectivity either via a cable to a cellular telephone or through PC Card cellular modems. The need being addressed by WWAN is the need to stay in touch with business critical communications while travelling.

Input and Output, Information Processes

WiMAX works with radio wave for transmission and microwaves for reception in frequencies between 2,3 and 3,5 GHz. This allows reaching speeds of 70 Mbps within distances up to 50 km from the access point. Thus, a radial area of 100 km could be cover with only one access point. Thus, a radial area of 100 km could be cover with only one access point.

Applications Fields

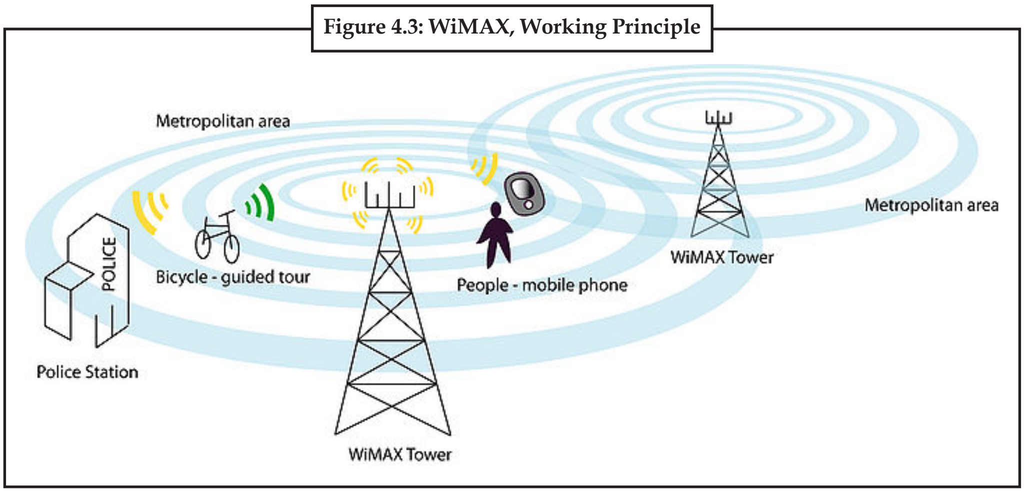
The technology is commonly used to provide internet to rural areas in which installing other types of technology becomes too expensive. Installed in the cities, WiMAX will allow people to connect to the internet whenever they want without looking for 'hotspots'. This will transform the user internet mobile lifestyle.

Working Principal

The first WiMAX standard IEEE 802.16, was created to administrate the interoperability of all devices working between 10 and 66 GHz. It will allow, as WiFi does, receive and transmit encrypted information among devices that have the technology. Within this standard, we should make some remarks to the IEEE 802.16a, IEEE 802.16e-2005 and IEEE802.16m which will allow to work with frequencies from 2 to 11 GHz, mobility and speed up to 1 GB, respectively.

In order to clarify this, an example will be given. Imagine you have a bike which you pick up in a renting point. This point allows you to create your own touristic routes around the city and this is automatically uploaded to your bicycle. Using WiMAX working technology the bicycle (mobile device) will be capable to guide you according to the uploaded touristic tour. In case that you follow the wrong direction or get lost, the wireless connection will allow you to put you again on track. Furthermore, if your bike is stolen, it can send a message to the closest police station or to your smart phone and keep track of it. All this, will be possible just using one access point with high connection reliability.

Figure 4.3: WiMAX, Working Principle



Source: http://wikid.eu/index.php/Wireless_Metropolitan_Area_Networking_%28WMAN%29

Future Development

Wimax forum is planning to release in 2012 WiMAX Release 2 (standard IEEE802.16m) which will enable more efficient, faster, and more converged data communications. WiMAX Release 2 will provide, as well, compatibility with Release 1 solutions by upgrading channel cards or software of the old system.

Self Assessment

Fill in the blanks:

1. The two kinds of wireless technologies used for WPAN are Bluetooth and ....

Notes

2. .... uses short-range radio waves over distances up to approximately 10 metres.
3. A Bluetooth PAN is also called a ....
4. The intent of .... technologies is to provide members of workgroups access to corporate network resources be it shared data, shared applications or e-mail but do so in way that does not inhibit a user's mobility.
5. .... method uses a wide frequency band together with Code Division Multiple Access (CDMA).
6. There are three types of infrared transmission: ...., directed and directed point-to-point.
7. A group of stations belonging to an AP is called ....

4.2 Wireless PAN Technologies (WPAN)

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 travelling, 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 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 Networks) are dependent on the Bluetooth or infrared technologies for the transmission of wireless signals. 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 200 metres 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 kilometres, 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

Notes

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.

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.

> *Notes* PAN (Personal Area Network) has enabled the transfer of data within the small geographical areas with the help of many small and portable carrying devices.

4.2.1 IEEE 802.15

Wireless PAN technologies utilize both radio frequencies and infrared light, depending on the application. The IEEE 802.15 standards working group focuses on the development of standards for wireless PANs and coordinates with other standards, such as 802.11 wireless LANs.

The 802.15 standards working group contains the following elements:

- 802.15.1: This working group, Task Group 1, defines a wireless PAN standard based on Bluetooth v1.1 specifications, which uses frequency hopping spread spectrum (FHSS) and operates at up to 1 Mbps. The 802.15 group published 802.11.1 in June of 2002, and it is meant to serve as a resource for developers of Bluetooth devices.
- 802.15.2: The group responsible for this standard, Task Group 2, is defining recommended practices to facilitate the coexistence of 802.15 and 802.11 networks. An issue is that both networks operate in the same 2.4 GHz frequency band, making coordination between operations necessary. The group is quantifying the interference and proposing methods to counter the interference.
- 802.15.3: This is Task Group 3, which is drafting a new standard for higher-rate wireless PANs. Data rates include 11, 22, 33, 44, and 55 Mbps. Combined with these higher data rates, quality of service (QoS) mechanisms make this standard good for satisfying needs for multimedia applications. This group is also focusing on lower cost and power requirements. A draft of the 802.15.3 standard is now available for purchase.
- 802.15.4: This group, Task Group 4, is investigating the definition of a standard with low data rates that leads to extremely low-power consumption for small devices where it’s not practical to change batteries within months or years. For example, sensors, smart badges, and home automation systems are candidates for this technology. Data rates include 20, 40, and 250 kbps. A draft of the 802.15.4 standard is now available for purchase.

4.2.2 Bluetooth

The introduction of Bluetooth in 1998 was the result of several companies, including Ericsson, IBM, Intel, Nokia, and Toshiba, working together to create a solution for wireless access among computing devices. Bluetooth, which is a specification and not a standard, is ideal for small devices with short-range, low-power, and inexpensive radio links. This makes Bluetooth a good solution for connecting small devices within range of a person in a small working area. That’s why the 802.15 chose Bluetooth as the basis of the 802.15.1 standard.

Notes

Basic Features

The Bluetooth Special Interest Group (SIG) published the initial version of the specification in mid-1999. There have been updates since then, but the technical attributes are essentially the same. Bluetooth transceivers operate at up to 1 Mbps data rate in the 2.4 GHz band, using FHSS technology. It constantly hops over the entire spectrum at a rate of 1,600 hops per second, which is much faster than the 802.11 version of frequency hopping.

Low-power Bluetooth devices have a range of 30 feet. High-power Bluetooth devices, however, can reach distances of around 300 feet. The high-power mode, though, is rare.

Bluetooth modules have relatively small form factors. Typical measurements are 10.2 × 14 × 1.6 millimeters, which is small enough to fit in a variety of user devices.

Bluetooth enables automatic connection among Bluetooth devices that fall within range of each other, but a user has the ability to accept and disallow connections with specific users. Users, however, should always be aware of whether their Bluetooth connection is enabled. To ensure security, disable the Bluetooth connection. Encryption is also part of the specification.

Could Bluetooth Replace Wireless LANs?

Bluetooth has characteristics similar to wireless LANs. Through the use of the high-power version of Bluetooth, manufacturers can develop Bluetooth access points and routers with a similar range as 802.11 networks. The current Bluetooth products, however, are mostly low power and focus on wireless PAN functions. In addition, it would be difficult for any Bluetooth wireless LAN products to gain a strong foothold in the market because 802.11 products already have widespread adoption.

The place where Bluetooth falls behind 802.11 is performance and range. 802.11 components can reach data rates of up to 54 Mbps, while Bluetooth lags way behind at around 1 Mbps. This might be good enough for most cable replacement applications such as an interface between headphones and a PDA. But higher performance is necessary when surfing the web through a broadband connection or participating on a corporate network. Also, the range of 802.11 is typically 300 feet inside offices, which is much greater than Bluetooth. Bluetooth would require many access points to fully cover larger areas.

As a result, it's highly unlikely that Bluetooth products will win over 802.11. This is certainly apparent because electronics stores primarily sell 802.11 (Wi-Fi) solutions for wireless LAN applications, not Bluetooth.

Could Wireless LANs Replace Bluetooth?

It's possible that 802.11 wireless LANs could have a big impact on the sale of Bluetooth devices, mostly because 802.11 meets or exceeds nearly all of the characteristics of Bluetooth. Because widespread adoption of Bluetooth is still lacking, there's time for 802.11 vendors to get their foot in the door with manufacturers needing support for wireless PANs.

Some modifications would need to be made, however. The size of 802.11 components needs to be smaller, but that is becoming more of a reality as semiconductor companies strive for miniaturization of their 802.11 chipsets. These smaller components require less power, making them more competitive for devices, such as mobile phones, that have smaller batteries. With the 802.15 group defining standards for wireless PANs based on Bluetooth and the 802.11 group focusing on wireless LANs, it's likely that both Bluetooth and 802.11 will continue to coexist and complement each other.

Minimizing Bluetooth Interference

As more wireless products become available, you need to carefully manage potential frequency interference. Tests have shown significant interference between Bluetooth and other systems

Notes

operating in the 2.4 GHz band, such as 802.11 wireless LANs. A critical problem is that Bluetooth and 802.11b neither understand each other nor follow the same rules. A Bluetooth radio might haphazardly begin transmitting data while an 802.11 station is sending a frame. This results in a collision, which forces the 802.11 station to retransmit the frame. This lack of coordination is the basis for radio frequency (RF) interference between Bluetooth and 802.11.

Because of the potential for collisions, 802.11 and Bluetooth networks suffer from lower performance. An 802.11 station automatically lowers its data rate and retransmits a frame when collisions occur. Consequently, the 802.11 protocol introduces delays in the presence of Bluetooth interference.

The full impact of RF interference depends on the utilization and proximity of Bluetooth devices. Interference occurs only when both Bluetooth and 802.11b devices transmit at the same time. Users might have Bluetooth devices in their PDAs or laptops, but no interference will exist if their applications are not using the Bluetooth radio to send data.

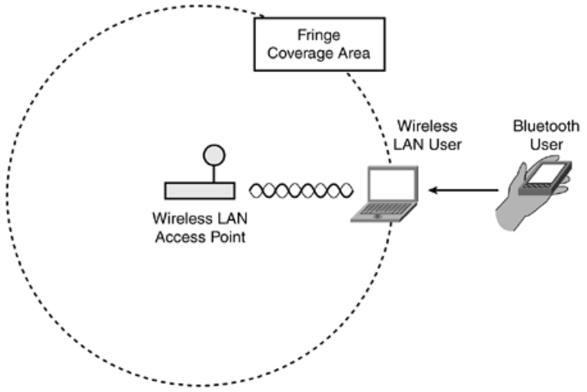
Some Bluetooth applications, such as printing from a laptop or synchronizing a PDA to a desktop, utilize the radio for a short period of time. In this case, the Bluetooth devices are not active long enough to noticeably degrade the performance of an 802.11 network. For example, a user might synchronize her PDA to her desktop when arriving at work in the morning. Other than that, their Bluetooth radio might be inactive and not cause interference the rest of the day.

The biggest impact is when a company implements a large-scale Bluetooth network, such as one that enables mobility for doctors and nurses using PDAs throughout a hospital. If the Bluetooth network is widespread and under moderate-to-high levels of utilization, the Bluetooth system will probably offer a substantial number of collisions with an 802.11 network residing in the same area. In this case, Bluetooth and 802.11 would have difficulties coexisting, and performance would likely suffer.

In addition to utilization, the proximity of the Bluetooth devices to 802.11 radio NICs and access points has a tremendous affect on the degree of interference. The transmit power of Bluetooth devices is generally lower than 802.11 wireless LANs. Therefore, an 802.11 station must be relatively close (within 10 feet or so) of a transmitting Bluetooth device before significant interference can occur.

A typical application fitting this scenario is a laptop user utilizing Bluetooth to support connections to a PDA and printer and 802.11 to access the Internet and corporate servers. The potential for interference in this situation is enormous, especially when the user is operating within outer limits of the coverage area of the 802.11 network. Figure 4.4 illustrates this situation. The signal from the Bluetooth device will likely drown out the weaker 802.11 signal because of the distance of the access point.

Figure 4.4: RF Interference Can Occur Between Bluetooth and 802.11 Wireless LAN Devices



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

Here are some tips on how to avoid interference from Bluetooth devices:

- ***Manage the use of RF devices:*** One way to reduce the potential for interference is to regulate the types of RF devices within your home or office. In other words, establish your own private regulatory body for managing unlicensed RF devices. The extreme measure would be to completely ban the use of Bluetooth; however, that is not practical or even possible in all cases. For example, you can't feasibly prohibit the use of Bluetooth in public areas of large offices. For private applications, you could set company policies to limit the use of Bluetooth to specific applications, such as synchronizing PDAs to desktops.
- ***Ensure adequate 802.11 coverage:*** Strong, healthy 802.11 signals throughout the coverage areas reduce the impact of the Bluetooth signals. If wireless LAN transmissions become too weak, the interfering Bluetooth signals will be more troublesome. Perform a thorough RF site survey, and determine the appropriate location for access points.
- ***Move to the 5 GHz band:*** If none of the preceding steps solve the problem, consider using a 5 GHz wireless LAN such as 802.11a. You can completely avoid RF interference in this band, at least for the foreseeable future.

Self Assessment

Fill in the blanks:

8. The basic purport of establishing .... is provide a communication channel to the individuals, who want to carry their own digital devices.
9. Wireless Personal Area Network (WPAN) is based on .... technology.
10. The purpose of .... is to make the use of electric field around human beings.
11. The full impact of .... interference depends on the utilization and proximity of Bluetooth devices.
12. .... was the first research scientist to introduce the idea of Personal Area Network (PAN).
13. Wireless PAN (Personal Area Network) is connected to the wired PAN (Personal Area Network) system either using ....

Case Study

Wireless LAN

The Situation

Prior to their implementation of a Meru wireless LAN, Greene County Public Schools (GCPS) had a wireless network system that wasn't "making the grade." Their legacy system consisted of mobile carts within each of the schools which were equipped with low-end Linksys® wireless routers. Because of this system configuration, wireless access was only active within the rooms where the carts were connected.

Difficulty of Use and Technology Adoption. Operating under the old system, teachers found the process of connecting a class to the wireless carts difficult and disruptive. At times, they were unable to connect to the devices correctly. The cumbersome nature of the process led to dampened enthusiasm for the system which adversely affected GCPS' efforts to use the technology for instructional purposes.

System Management As GCPS' legacy wireless network grew over time, it became increasingly more disparate. Consequently, the IT team found themselves lacking an

Contd...

Notes

efficient way to implement system management and controls – including preventing the infiltration of unauthorised devices. At the same time, with the number of users steadily growing, finding an effective way to segregate student and public access from the private faculty/staff wireless network was also becoming a priority. With no single point of management, the IT staff was spending increasing amounts of time performing hands-on maintenance and troubleshooting of individual components throughout all the different school buildings. They also had to find a way to abate the growing number of students and faculty using their own personal wireless devices on the school network (laptops, mobile phones and other hand held devices). These critical issues related to system management and security became a drain on IT department resources which translated into an unacceptable level of cost for the school system.

Performance: The legacy wireless network lacked the required throughput capability and, in turn, the predictability needed for running critical school applications. The old network would often exhibit "shaky" performance when used for state required Standards of Learning (SOL) testing. As a result, ensuring Quality of Service (QoS) during SOL testing and other on-line assessments became a high priority concern for the IT staff. With a plan for growth in the number of wireless devices in classrooms, GCPS needed a scalable system that provided all the required capacity without compromise in performance.

Scalability: Like most public school systems, GCPS is subject to the push to devote more space to learning and less to other areas of school operations. With physical space at a premium, the IT department was running out of viable options for housing their expanding LAN equipment. This dilemma made the idea of expanding the wireless network under a centralized system an even more attractive option.

The Meru Solution

With its list of technology priorities in hand, a short window of opportunity to deploy a new solution, and a fixed budget, GCPS turned to their technology service partner, Advanced Network Systems, to find a wireless system that met all of their requirements. During the summer of 2008, GCPS replaced its legacy system with a Meru solution consisting of an MC3100 controller and 74 AP311 dual radio access points. The solution was deployed at the County's high school, middle school and two elementary schools.

Reaping the Benefits of Meru

According to Dale Herring, the benefits realized as a result of the Meru solution deployment were numerous. "We've been extremely pleased with Meru. We now have a really powerful system that has all the capabilities that we need," said Herring. He added, "From an IT perspective, the Meru system's centralized configuration and management features have cut down on a lot of time we used to spend maintaining all the different systems we had." Herring noted that another benefit of the Meru system is its high level of flexibility. "Because we now have a consistent wireless solution, device compatibility issues have been eliminated; this allows GCPS' IT team to easily share laptops and other devices between schools when demands shift. Since there are no configuration changes to perform, devices move seamlessly from school to school. Having this kind of flexibility means we spend less of our time on management and a smaller budget needed because we don't have to have as many devices at every school." Herring noted, "One of the big reasons we chose a Meru solution is its compatibility and technology investment protection. No matter what type of device is connected to the network, a/b/g or n, Meru's access points can accommodate all the least common denominator in terms of performance as we go forward."

Expanding on the idea of better system performance Herring added, "Because Standards of Learning testing is considered a mission-critical application for the school district, we need to have guaranteed quality of service when it comes to its implementation. 'Hiccups'

Contd...

in the system are incredibly disruptive and are not an option. With Meru's built in QoS, the on-line SOL testing process has gone very smoothly; the system has reliably supported this and all the other bandwidth-intensive applications we use it for."

According to Dale Herring, "We've had a lot of positive feedback and increased use of the wireless system because connectivity is now a more seamless, transparent process. Disruptions to the teaching process in our classrooms are minimal; plus we were able to easily segregate access for students and the public from the private portion of the network. Everyone in the IT department loves the flexibility and we don't worry the way we used to about adding more devices or new applications. We are all definitely benefiting from having a pervasive system that provides access wherever and whenever it's needed; both inside and outside of the school buildings."

New Opportunities with a Meru Solution

The 2008/2009 school year brought forth new opportunities for GCPS to improve the learning environment using their state-of-the-art Meru wireless network. Students and school personnel alike are reaping the benefits of being able to successfully run applications over the air including web-based assessments, instructional videos and presentations, along with Internet-based learning and staff training.

Opportunities on the horizon are all about learning and teaching processes. The technology and cost/benefit analysis of implementing an e-reader program is now under consideration. The GCPS' IT department is currently piloting e-reader technology to support the County's reading program in the Middle School. If successful, the program will be expanded to all schools. According to Dale Herring, "We considered the option of e-readers before the Meru installation. But now since we have the technology to effectively support this kind of program, the concept has gained a lot of traction and taken on a new meaning. Students are now able to access the most up to date material throughout the facility, not just in certain designated locations." With the number of electronic formats consolidating and significant improvements in device battery life, the use of hand-held devices containing e-books has grown significantly within the educational market. Herring added, "The concept of e-readers appeals to students and school administrators alike. Students already lug around enough laptops and heavy books. On the other side, books are expensive and quickly fall out of date which makes it challenging for schools to stay current."

As part of the teacher development and evaluation process, GCPS administrators are using iPod's to wirelessly connect to a web portal to run their classroom observation software. So far this year, over 1000 informal classroom observations have been conducted and recorded. That data collected is used to insure that best instructional practice is being followed, to provided specific feedback to teachers, and to help administrators stay in touch with what is going on in the classrooms. According to Herring, "Using a secure wireless/web-based system, we've made big strides in recording evaluation info in real time and keeping it secure. We essentially eliminated the need to keep data on a device which could get lost or stolen and need for any further data transfer." Purchased with private enterprise grant funds, the implementation of these mobile devices has had a significant, positive impact on the collection, storage and utilization of this vital information.

Plans for the Future

GCPS has plans to expand the implementation of Meru products in its primary school and school board office in the near future. Further out on the horizon are plans for a VoIP telephony solution which could ultimately also be run over their Meru wireless network.

About Greene County Public Schools Greene County is located in central Virginia at the foot of the Blue Ridge Mountains, with the Shenandoah National Park and the Skyline Drive forming its western boundary. Although rural in nature, this picturesque County is part of the Charlottesville metropolitan region which includes the University of Virginia.

Contd...

As a result, the County has become a community that has experienced significant growth in its residential population as well as business investment and economic development. The Greene County Public School System has a student enrollment of approximately 2,800 and is comprised of seven schools including one primary, two elementary, one middle, one high school, an alternative education centre, and a technical educational centre. The school system's popular tag phrase, "Every child, every chance, every day," echoes its formal commitment to build a positive, responsible and effective learning community where students, teachers and staff are encouraged to believe, achieve and succeed.

About Advanced Network Systems, Inc. Advanced Network Systems specializes in the design, installation and support of information technology solutions. The company's expertise covers a wide variety of IT applications, including network security, virtualization, managed IT services, core infrastructure, networked storage, and wireless, as well as IP-based telephone and conferencing systems. With multiple locations, serving Virginia and West Virginia, Advanced Network Systems supports a diverse base of clients, including small and medium-sized businesses, government agencies, and educational institutions.

Questions:

1. Discuss the difficulties face by GCPS in implementing system management and controls.
2. Discuss the use of Meru wireless network in improving the learning environment.

Source: http://www.getadvanced.net/wlancasestudy

4.3 Summary

- Wireless LAN (WLAN) is very popular nowadays.
- Wireless LANs enable users to communicate without the need of cable. Each WLAN network needs a wireless Access Point (AP) to transmit and receive data from users.
- The major difference between wired LAN and WLAN is WLAN transmits data by radiating energy waves, called radio waves, instead of transmitting electrical signals over a cable.
- WPAN describes an application of wireless technology that is intended to address usage scenarios that are inherently personal in nature.
- WLAN on the other is more focused on organizational connectivity not unlike wire based LAN connections.
- WLAN addresses connectivity within a defined region, WWAN addresses the need to stay connected while travelling outside this boundary. Today, cellular technologies enable wireless computer connectivity either via a cable to a cellular telephone or through PC Card cellular modems.
- 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.
- Wireless PAN technologies utilize both radio frequencies and infrared light, depending on the application.

4.4 Keywords

Body Area Networks: It is based on the IEEE 802.15.6 standard for transmission via the capacitive near field of human skin allowing near field communication of devices worn by and near the wearer.

Notes

Personal area network (PAN): The communication network established for the purpose of connecting computer devices of personal use.

Piconet: Piconet is composed of up to 8 active devices in a master – slave relationship (a very large number of devices can be connected in "parked" mode).

Wireless personal area network (WPAN): WPAN is a personal area network , a network for interconnecting devices centred around an individual person's workspace

WLAN: WLAN is more focused on organizational connectivity not unlike wire based LAN connections.

4.5 Review Questions

1. What are the various types of wireless networks?
2. Define the following: transmission technology, microwave transmission and spread spectrum transmission.
3. Describe the various types of wireless LAN.
4. Explain the working principal of WiMAX.
5. Could Bluetooth replace wireless LANs?
6. Could wireless LANs replace Bluetooth?
7. Discuss the steps used to avoid the interference from Bluetooth devices.

Answers: Self Assessment

1. Infrared Data Association
2. Bluetooth
3. Piconet
4. WLAN
5. Direct Sequence Modulation
6. Diffused
7. Basic Service Set (BSS)
8. PAN (Personal Area Network)
9. Plug-in
10. PDAs
11. RF
12. Thomas Zimmerman
13. Firewire or USB

4.6 Further Readings

Books

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

John Ross, *Introduction to wireless networks.*

Vijay Garg, *Wireless Communications & Networking.*

Theodore S. Rappaport, *Wireless Communications: Principles and Practice.*

Online links

http://wikid.eu/index.php/Wireless_Metropolitan_Area_Networking_%28WMAN%29

http://www.tutorial-reports.com/wireless/wlanwifi/wifi_architecture.php

http://en.wikipedia.org/wiki/Personal_area_network

http://www.doc.ic.ac.uk/~nd/surprise_95/journal/vol2/mjf/article2.html

Notes

Unit 5: Wireless PAN Components

CONTENTS

Objectives

Introduction

5.1 User Devices

5.2 Radio NIC (Network Interface Card)

5.3 USB Adapters

5.4 Wireless Routers

5.5 Bluetooth Dongles

5.5.1 Use

5.5.2 Applications

5.5.3 Features

5.5.4 Reliability

5.6 Summary

5.7 Keywords

5.8 Review Questions

5.9 Further Readings

Objectives

After studying this unit, you will be able to:

- Explain about the user devices in wireless network
- Discuss the radio NIC
- Explain the wireless USB adapter
- Describe the wireless router
- Discuss about Bluetooth dongle

Introduction

A personal area network – PAN – is a computer network organized around an individual person. Personal area networks typically involve a mobile computer, a cell phone and/or a handheld computing device such as a PDA. You can use these networks to transfer files including email and calendar appointments, digital photos and music.

Personal area networks can be constructed with cables or be wireless. USB and FireWire technologies often link together a wired PAN, while wireless PANs typically use Bluetooth or sometimes infrared connections. Bluetooth PANs are also sometimes called piconets.

Personal area networks generally cover a range of less than 10 meters (about 30 feet). PANs can be viewed as a special type (or subset) of local area network (LAN) that supports one person instead of a group.

Typically, a wireless personal area network uses some technology that permits communication within about 10 meters – in other words, a very short range. One such technology is Bluetooth, which was used as the basis for a new standard, IEEE 802.15.

A WPAN could serve to interconnect all the ordinary computing and communicating devices that many people have on their desk or carry with them today – or it could serve a more specialized purpose such as allowing the surgeon and other team members to communicate during an operation.

5.1 User Devices

- ***Mobile Phone:*** A mobile device (also known as a handheld device, handheld computer or simply handheld) is a small, handheld computing device, typically having a display screen with touch input and/or a miniature keyboard and weighing less than 2 pounds (0.91 kg). Apple, HTC, LG, Research in Motion (RIM) and Motorola Mobility are just a few examples of the many manufacturers that produce these types of devices.

  A handheld computing device has an operating system (OS), and can run various types of application software, known as apps. Most handheld devices can also be equipped with Wi-Fi, Bluetooth, and GPS capabilities that can allow connections to the Internet and other Bluetooth-capable devices, such as an automobile or a microphone headset. A camera or media player feature for video or music files can also be typically found on these devices along with a stable battery power source such as a lithium battery.

- ***Personal Digital Assistant (PDA):*** A personal digital assistant (PDA), also known as a palmtop computer, or personal data assistant, is a mobile device that functions as a personal information manager. PDAs are largely considered obsolete with the widespread adoption of smartphones.

  Nearly all current PDAs have the ability to connect to the Internet. A PDA has an electronic visual display, enabling it to include a web browser, all current models also have audio capabilities enabling use as a portable media player, and also enabling most of them to be used as mobile phones. Most PDAs can access the Internet, intranets or extranets via Wi-Fi or Wireless Wide Area Networks. Most PDAs employ touchscreen technology.

Did u know? The first PDA was released in 1984 by Psion, the Organizer II. Followed by Psion's Series 3, in 1991, which began to resemble the more familiar PDA style. It also had a full keyboard.

The term PDA was first used on January 7, 1992 by Apple Computer CEO John Sculley at the Consumer Electronics Show in Las Vegas, Nevada, referring to the Apple Newton.

In 1994, IBM introduced the first PDA with full mobile phone functionality, the IBM Simon, which can also be considered the first Smartphone. Then in 1996, Nokia introduced the a PDA with full mobile phone functionality, the 9000 Communicator, which became the world's best-selling PDA. The Communicator spawned a new category of PDAs: the "PDA phone", now called "smartphone". Another early entrant in this market was Palm, with a line of PDA products which began in March 1996.

- ***Headset or Headphones:*** Headphones are a pair of small loudspeakers that are designed to be held in place close to a user's ears. Headphones either have wires for connection to a signal source such as an audio amplifier, radio, CD player, portable media player or mobile phone, or have a wireless receiver, which is used to pick up signal without using a cable. They are sometimes known as ear speakers or, colloquially, cans. The in-ear versions are also known as earphones or earbuds. In the context of telecommunication, a headset is a combination of headphone and microphone.

- *PC input devices:* The input unit is formed by the input devices attached to the computer. E.g. – Keyboard, Microphone etc. An input unit takes the input and converts it into binary form so that it can be understood by the computer.
- *Global Positioning System (GPS) receiver:* The Global Positioning System (GPS) is a space-based satellite navigation system that provides location and time information in all weather conditions, anywhere on or near the Earth where there is an unobstructed line of sight to four or more GPS satellites. The system provides critical capabilities to military, civil and commercial users around the world. It is maintained by the United States government and is freely accessible to anyone with a GPS receiver.
- *Dial-up modem:* Dial-up Internet access is a form of Internet access that uses the facilities of the public switched telephone network (PSTN) to establish a dialed connection to an Internet service provider (ISP) via telephone lines. The user's computer or router uses an attached modem to encode and decode Internet Protocol packets and control information into and from analogue audio frequency signals, respectively.
- *Wireless remote control:* A remote control is a component of an electronics device, most commonly a television set, DVD player and home theater systems originally used for operating the device wirelessly from a short line-of-sight distance. Remote control has continually evolved and advanced over recent years to include Bluetooth connectivity, motion sensor-enabled capabilities and voice control.
- *Sensor modem:* Wireless sensor nodes comprises a variety of low power, battery-operated wireless data acquisition devices to which different sensors may be directly connected.

5.2 Radio NIC (Network Interface Card)

The hardware required to connect a computer to a network is a network interface card (NIC). Each network interface card has a unique number called a MAC address, which is a six-figure hexadecimal number such as AB:1C:FF:56:4D:33. Most NICs are designed to connect to twisted-pair cable; however, there are NICs that connect to all types of network cable and wireless NICs that send and receive radio waves through an aerial. Wireless ATM networks will provide multimedia information to end users anywhere and anytime. A key technology component in the integration of a wireless ATM (WATM) network is the WATM network interface card (NIC). Similar to ATM NICs, the WATM NIC requires the support of the ATM and AAL layer transfer protocols. But, in order to provide a reliable wireless transmission platform, WATM NICs should also incorporate data link control (DLC), media access control (MAC), and radio physical (RPhy) layer functionality. As a result, the WATM NICs processing requirements are more demanding than that of ATM NICs at equivalent transmission rates. Thus, the design of a high-performance WATM NIC software/hardware low-cost architecture poses a new challenge. This paper presents a new architecture and implementation of a first generation 8 Mb/s WATM NIC developed at NEC Princeton for the WATMnet network.

In the early days of computing, individual computers operated as stand-alone systems. The earliest personal computers did not have an easy way to connect to other computers. In order to transfer files between computers, you had to use a portable storage medium such as a floppy disk; however, in modern day computers, connecting to a network is essential. For example, you need it to use e-mail, access information on the Internet, share documents within a corporate network.

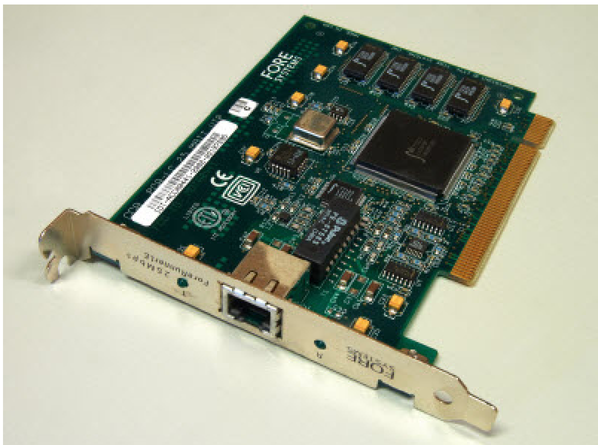
A computer uses a network interface card (NIC) to become part of a network. The NIC contains the electronic circuitry required to communicate using a wired connection (e.g., Ethernet) or a wireless connection (e.g., WiFi).

Notes

Notes A network interface card is also known as a network interface controller, network adapter, or Local Area Network (LAN) adapter.

Early NICs typically consisted of an expansion card connected to the motherboard. This separate card contained the electronic circuitry and the physical connectors. The Figure 5.1 shows an example of a typical NIC.

Figure 5.1: Typical Network Interface Card

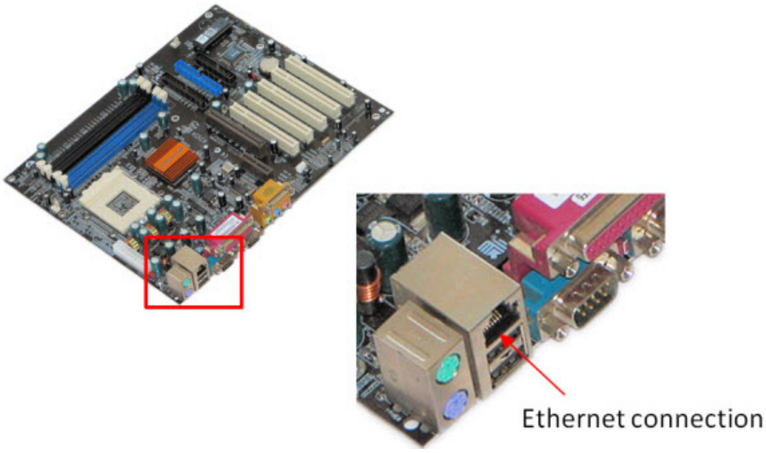


Source: http://education-portal.com/academy/lesson/network-interface-card-nic-types-function-definition.html

The most widely used network connection for personal computers is an Ethernet connection. Ethernet is really a standard for computer network technologies that describes both the hardware and the communication protocols. Ethernet was commercially introduced in 1980 and has largely replaced other wired network technologies.

Since Ethernet is so widely used, most modern computers have a NIC built into the motherboard. A separate network card is not required, unless some other type of network is used. The Figure 5.2 shows an Ethernet connection built into a motherboard. Several other connections are located directly adjacent to the Ethernet connection.

Figure 5.2: Ethernet Connection Integrated on a Motherboard

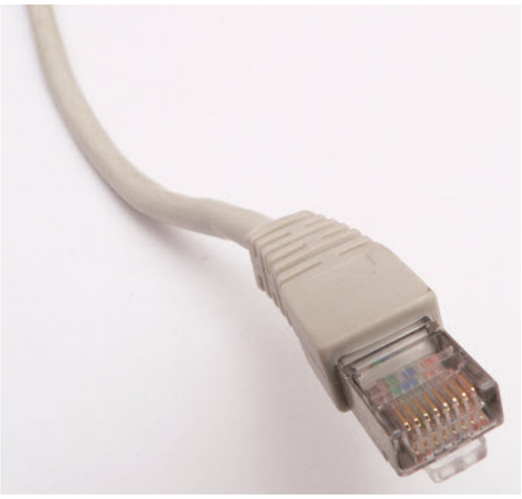


Source: http://education-portal.com/academy/lesson/network-interface-card-nic-types-function-definition.html

Notes

An Ethernet connection uses a standard interface known as a RJ45 connector. RJ stands for registered jack. The Figure 5.3 shows an Ethernet cable with a RJ45 connector.

Figure 5.3: Ethernet Cable Using a RJ45 Connector



Source: http://education-portal.com/academy/lesson/network-interface-card-nic-types-function-definition.html

This cable plugs into the Ethernet connection of a computer. Smalls LED lights built into the connection will show that a connection is active and whether data is being transferred.

While most desktop computers rely on a wired connection, mobile computing devices such as laptops, tablets and smart phones use a wireless connection. The most widely used system for wireless connections is WiFi, which relies on radio signals.

Most laptop computers have both an Ethernet and a WiFi connection, while smaller devices typically only have a WiFi connection. The NIC controls both types of connections, so whether you use an Ethernet or WiFi connection, you can use your computer for the same tasks independent of the type of connection. Wireless connections tend to be slower and are sometimes less secure, but, in a typical network, the two connections are designed to work seamlessly with each other.

Self Assessment

Fill in the blanks:

1. A .... has an electronic visual display, enabling it to include a web browser.
2. The .... is a space-based satellite navigation system that provides location and time information in all weather conditions.
3. Wireless .... nodes comprises a variety of low power, battery-operated wireless data acquisition devices to which different sensors may be directly connected.
4. A computer uses a network interface card (NIC) to become part of a ....
5. The most widely used network connection for personal computers is an .... connection.

5.3 USB Adapters

Most personal computers had a built-in D-sub serial RS232 port, also referred to as a COM port, which could be used for connecting the computer to most types of serial RS232 devices. By the

Notes

late 90's many computer manufacturers started to phase out the serial COM port in favor of the USB port. By the mid 2000's some computers had both a serial COM port and a USB port, however many did no longer have a serial COM port by that time; and today almost all modern computers have no serial COM port but only USB ports instead. Since many serial devices with a RS232, RS485 or RS422 port are still in use and even still produced today, the disappearing of the serial COM port from personal computers has created a need for the USB to serial adapter.

A USB adapter is a type of protocol converter which is used for converting USB data signals to and from other communications standards. Commonly, USB adaptors are used to convert USB data to standard serial port data and vice versa.

Most commonly the USB data signals are converted to either RS232, RS485, RS422 or TTL serial data. The older serial RS423 protocol is rarely used anymore, so USB to RS423 adapters are hard to find.

USB to serial RS232 adapters are often used with consumer, commercial and industrial applications and USB to serial RS485/RS422 adapters are usually mainly used only with industrial applications.

Caution Adapters for converting USB to other standard or proprietary protocols also exist; however, these are usually not referred to as a serial adapter.

The primary application scenario is to enable USB based computers to access and communicate with serial devices featuring D-Sub (usually DB9 or DB25) connectors or screw terminals, where security of the data transmission is not generally an issue.

USB serial adapters can be isolated or non-isolated. The isolated version has opto-couplers and/or surge suppressors to prevent static electricity or other high-voltage surges to enter the data lines thereby preventing data loss and damage to the adapter and connected serial device. The non-isolated version has no protection against static electricity or voltage surges, which is why this version is usually recommended for only non-critical applications and at short communication ranges.

As a simplified example a typical standard USB to serial adapter consists of a USB processor chip which processes the USB signals. The USB processor sends the processed USB signals to a serial driver chip which applies the correct voltages and sends the processed data signals to the serial output. For the computer to be able to detect and process the data signals drivers must be installed on the computer. When the USB to serial adapter is connected to the computer via the USB port the drivers on the computer creates a virtual COM port which shows up in Device Manager. This virtual COM port can be accessed and used as if it was a built-in serial COM port. However, the characteristics of the virtual COM port are not exactly the same as a real internal COM port, mainly due to data latency; which means that if very sensitive and precise data transfer is required, the USB to serial adapter might be unreliable and not a desired solution. Virtual COM drivers are usually available for Windows, Linux and MAC only.

5.4 Wireless Routers

A wireless router is a device that performs the functions of a router but also includes the functions of a wireless access point. It is commonly used to provide access to the Internet or a computer network. It does not require a wired link, as the connection is made wirelessly, via radio waves. It can function in a wired LAN (local area network), in a wireless-only LAN (WLAN), or in a mixed wired/wireless network, depending on the manufacturer and model.

Most current wireless routers have the following characteristics:

- One or multiple NICs supporting Fast Ethernet or Gigabit Ethernet integrated into the main SoC.

Notes

- One or multiple WNICs supporting a part of the IEEE 802.11-standard family also integrated into the main SoC or as separate chips on the Printed circuit board. It also can be a distinct card connected over a MiniPCI or MiniPCIe interface.
    - ❖ So far the PHY-Chips for the WNICs are generally distinct chips on the PCB. Dependent on the mode the WNIC supports, i.e. 1T1R, 2T2R or 3T3R, one WNIC have up to 3 PHY-Chips connected to it. Each PHY-Chip is connected to a Hirose U.FL-connector on the PCB. A so called pigtail cable connects the Hirose U.FL either to a RF connector, in which case the antenna can be changed or directly to the antenna, in which case it is integrated into the casing. Common are single-band (i.e. only for 2.4 GHz or only for 5 GHz) and dual-band (i.e. for 2.4 and 5 GHz) antennas.
- Often an Ethernet Switch supporting Gigabit Ethernet or Fast Ethernet, with support for IEEE 802.1Q, integrated into the main SoC (MediaTek SoCs) or as separate Chip on the PCB.
- Some wireless routers are also include a xDSL-, DOCSIS- oder a LTE-modem in addition to the other components.

Figure 5.4: Linksys-Wireless-G-Router

Source: http://en.wikipedia.org/wiki/File:Linksys-Wireless-G-Router.jpg

If you don’t have an ADSL connection, but have a cable broadband connection, then don’t buy an ADSL wireless router. You want one that you can plug your modem in to. Look for any wireless router that DOESN’T have the words ADSL in the title.

The modem you got from your ISP will probably be connected to your computer via an ethernet cable. Unfortunately, you can’t just plug this in to your shiny new wireless router and expect it to work! When you plug your Ethernet cable in to your computer, you’re plugging it in to an ethernet card. Your ethernet card has a unique address called a MAC address. Cable providers connect you via the MAC address of your ethernet card. Your new router will have a different MAC address. So if you plug your ethernet cable in to this, your provider won’t know where you are, and you won’t get any web pages!

The good news is that there’s something called MAC address spoofing. This is when the router pretends to be your ethernet card. If you get a wireless router like the Buffalo AirStation G54 High Power then the install process will take care of this for you. The process will be fairly painless. The bad news is that some routers expect you to do all this for yourself! The manual will then explain how to get the MAC address of your ethernet card, and how to enter this information in to the router. The wireless cable routers we’ve chosen on our recommended pages all have easy setup options for MAC address spoofing.

5.5 Bluetooth Dongles

Bluetooth technology is a wireless technology that allows devices like computers, cell phones, headsets and PDAs to communicate with each other. This communication facilitates data transfers quite easily, and has heralded a new age in wireless computer and cell phone accessories. If you have a computer and you want to use Bluetooth accessories with it (such as a printer, keyboard, headset or mouse) then you will first need a Bluetooth adapter.

5.5.1 Use

The function of a Bluetooth adapter is to allow you to create a Bluetooth network for your computer if it is not already Bluetooth-enabled. Once this network has been created, your computer will be compatible with all Bluetooth-enabled wireless devices. Other uses of a Bluetooth dongle include:

- ***Listening to Music:*** Bluetooth can be used to stream audio to headphones or even speakers. These speakers or headphones will typically be battery-powered. By using such devices, you can play music on your computer and listen in from another room.
- ***Transferring Files:*** A Bluetooth connection between computers can be used to stream files. By pairing two computers together, a shared folder can be established, allowing multiple users access to a database. This makes it convenient to work on files that are frequently updated.
- ***Customizing your Phone:*** Unless your phone has had its usability crippled by your carrier, you can send ringtones and wallpapers to your phone. This gives you the option to take your own collection of pictures and music, and transfer them to your phone using the software that is included and activated with your dongle.
- ***Streaming Media:*** If you have the proper hardware, such as a TV that can interface with a laptop or a Bluetooth-enabled TV receiver, you can activate a connection between your main computer, with a dongle installed, and your TV or laptop. You can use this connection to stream movies or pictures to your TV from your now Bluetooth-enabled computer.
- ***Controlling Mechanical Devices:*** If you're tech-savvy, it is possible to take advantage of a Bluetooth receiver to engage physical switches. With the proper set-up, you can use a Bluetooth dongle on your home computer to activate lights, sprinklers, cameras or other such devices within a range of about 100 meters. Such a set up may require some technical know-how and a good bit of solder.

5.5.2 Applications

Bluetooth dongle namely Bluetooth adaptor is a supernatural gadget. Wow, it is bad when you want to transfer music files from your PC to your Bluetooth mobile phone, however, the data cable is lost and your PC does not have Bluetooth port, what should you do now? Please do not worry, Bluetooth dongle will solve it, please plug one Bluetooth adaptor into the USB port of your PC, and turn on it, now, your PC has been transformed a Bluetooth PC, you can transfer files at ease. How marvelous the Bluetooth dongle it is. And you may ask is it very expensive? "No!", on Thesource.com would like gladly to answer you it is not dear at all. Bluetooth adaptor from on Thesource.com is not only good but also at very featured prices.

5.5.3 Features

There are several benefits to having a Bluetooth adapter. If you like using wireless devices, then installing a Bluetooth adapter to create a Bluetooth network is essential. Instead of your wireless devices all working on their own small network, a Bluetooth adapter enables them to all work together, which will increase productivity. It will also prevent problems caused by competing networks.

5.5.4 Reliability

The internal antenna in a dongle is used to deliver interference-free reception under optimal conditions. The passwords and user names provide the user-level authentication.

Self Assessment

Fill in the blanks:

6. The internal antenna in a dongle is used to deliver .... reception under optimal conditions.
7. The function of a Bluetooth .... is to allow you to create a Bluetooth network for your computer if it is not already Bluetooth-enabled.
8. A .... adapter is a type of protocol converter which is used for converting USB data signals to and from other communications standards.
9. A wireless .... is commonly used to provide access to the Internet or a computer network.
10. The USB processor sends the processed USB signals to a serial driver chip which applies the correct .... and sends the processed data signals to the serial output.
11. The internal .... in a dongle is used to deliver interference-free reception under optimal conditions.

Task Compare the major Bluetooth dongles available in the market.

Case Study **How Cisco Upgraded Its Wireless Infrastructure**

In 2000, Cisco® IT designed and deployed a global WLAN infrastructure that serves all Cisco offices. Originally designed as a secondary network for intermittent data usage, the WLAN proved very popular with Cisco's highly mobile workforce. Within two years, nearly 25 percent of Cisco employees were using the WLAN as their primary network access medium, and many were also using a variety of wireless voice services.

By 2005, it was clear that an upgrade of the WLAN infrastructure was necessary as user adoption continued to increase. What was originally a secondary network was now deemed business-critical by the majority of Cisco employees, with 81 percent of users describing the WLAN as "critical" or "extremely important" for their day-to-day productivity. The original infrastructure was reaching the end of its useful lifetime, and many components were no longer sold or supported. Additionally, Cisco business managers were calling for improvements in service availability and operations; business objectives for the upgraded infrastructure included reduced support costs, enhanced stability and security, and an increased Service Level Agreement. Perhaps most importantly in today's business environment, the existing WLAN could not offer the performance and stability required for high levels of wireless voice and video traffic.

Challenge

The challenge for Cisco IT was to continue providing a global wireless LAN that could serve as a primary access medium and deliver more bandwidth and coverage to more

Contd...

users, while satisfying the company's business requirements. The next-generation WLAN would also need to provide native support for wireless voice and video, with high levels of accessibility, availability, and security to reduce service-impacting incidents.

Our goal was to deploy an enterprise-class, on-demand wireless network that is suitable as a primary access medium," says Oisín Mac Alasdair, Cisco IT program manager for wireless strategy and architecture. "In the short term, we want to support at least 50 percent of our users adopting wireless as their regular network access method. Over the longer term, that percentage should continue to rise."

Solution

The Cisco Next-Generation WLAN program, which began in May 2006, will evolve Cisco IT's existing indoor wireless network infrastructure into a more available, stable, and secure network. Cisco IT will increase the number of access points – from 3100 to more than 6000 - in more than 300 Cisco locations worldwide and deploy the latest intelligent and fully integrated Cisco wireless products.

The next-generation WLAN is based on the Cisco Unified Wireless Network solution, which combines centralized Cisco Wireless LAN Controllers with Lightweight Access Point Protocol (LWAPP)-enabled access points, and distributed, autonomous access points based on Cisco IOS Software.

Campus sites: At main campuses, the new WLAN design uses 100 or more Cisco Aironet® 1130AG Series access points. The Cisco Aironet 1130AG Series is an ideal choice for these large sites, because it offers enterprise-class features such as high-performance 802.11a and 802.11g radios, integrated antennas, and 802.11i security compliance.

Campus buildings are served by two or more Cisco Catalyst® 6500 Series switches with Wireless Services Modules (WiSMs). Authorized user traffic is carried over LWAPP tunnels, while guest traffic is carried in a generic routing encapsulation (GRE) tunnel.

The WLAN is managed with internal systems and the Cisco Wireless Control System (WCS), which provides comprehensive tools for planning, monitoring, and control. Location servers installed in a Cisco data center enable delivery and management of location-based services for users.

Large and midsized field sales offices. Large and midsized field offices will also use a centralized WLAN solution, with up to 98 Cisco Aironet 1130AG Series access points that are controlled by dual Cisco 4400 Series Wireless LAN Controller appliances and managed by the Cisco WCS. The Cisco 4400 Series controllers manage officewide WLAN functions such as security policies, intrusion prevention, Auto RF, QoS, and mobility.

Small field sales offices: The smallest offices will use up to four Cisco Aironet 1200 Series access points running Cisco IOS Software. No local WLAN controller is required because a dedicated access point provides wireless domain services. These small office WLANs will be managed with the Cisco Wireless LAN Solution Engine (WLSE).

Wireless clients: In conjunction with the global upgrade of the WLAN architecture, the Cisco Secure Services Client will be supported on all client endpoints. The adoption of a single authentication framework allows Cisco IT to standardize on a single client for all devices, which simplifies support and reduces the company's total cost of ownership for wireless networking. The Cisco Secure Services Client is also compatible with a wide range of wireless adaptors that support the Cisco Certified Extensions (CCX) program.

New capabilities: The new WLAN architecture supports enhanced capabilities such as location-based services; improved guest access; enhanced wireless voice services for dual-band phones and other user devices; and outdoor coverage on campus sites. The architecture also enables security through an integrated wireless intrusion detection

Contd...

Notes

system (IDS), improved detection of rogue access points, as well as the security features Wi-Fi Protected Access (WPA2) and wireless network admission control (NAC).

Result

As of late 2006, the WLAN upgrade was complete for the Cisco headquarters campus in San Jose, California, and deployment was under way in other locations. With nearly 40 percent of Cisco employees working at the headquarters site, the early results achieved at this campus indicate the value to be obtained from the remaining deployments.

With the next-generation WLAN and Cisco Unified Wireless Network solutions, Cisco employees will experience a better wireless network. In addition, Cisco will gain the benefits of cost savings, greater network stability, and continued productivity gains.

Lessons Learned

Cisco customers can benefit from the lessons learned by Cisco IT during the initial WLAN deployment and the next-generation upgrade.

Regulatory issues: Different access points and wireless interface cards are required in certain parts of the world because the 802.11a standard may not be approved in some countries, or not yet approved in its most recent version. Particularly in emerging market countries, regulatory requirements are more complex, and wireless standards are more controlled. As a result of these issues, Cisco has not been able to use the same access point model in every country. This difference has not significantly affected the support requirements or benefits achievable from the new WLAN.

Transition resources: Certain operational and support resources were required during the deployment of the new WLAN solutions. During the architecture and design phases of the project, several network design engineers created and tested the design, and all required documentation using local and remote labs. In addition, several network operations engineers implemented the proposed design at pilot sites for limited-duration tests and Cisco network management personnel created the interface to Cisco IT's internal network management systems. Additional Cisco IT staff created technical documentation and conducted training globally for the implementation and support engineers.

During the implementation phase, several project managers monitored the implementation schedule and activity. The installation of the new wireless equipment was performed by both Cisco employees and outsourcers.

Indoor and outdoor deployments: Cisco IT developed separate deployment plans for indoor and outdoor coverage, reflecting differences in scope, architecture design, and user needs and expectations for service levels. Upgrading indoor coverage was given a higher priority than installing new outdoor access.

Questions:

1. Discuss the challenge faced by Cisco in upgrading its wireless infrastructure.
2. Discuss the features of the new WLAN architecture.

Source: http://www.cisco.com/web/about/ciscoitatwork/mobility/ngwlan_web.html

5.6 Summary

- A personal area network – PAN – is a computer network organized around an individual person.
- Personal area networks generally cover a range of less than 10 meters (about 30 feet).

- A WPAN (wireless personal area network) is a personal area network – a network for interconnecting devices centered around an individual person's workspace – in which the connections are wireless.
- A key concept in WPAN technology is known as plugging in.
- The hardware required to connect a computer to a network is a network interface card (NIC).
- Each network interface card has a unique number called a MAC address, which is a six-figure hexadecimal number such as AB:1C:FF:56:4D:33.
- A wireless router is a device that performs the functions of a router but also includes the functions of a wireless access point.
- It is commonly used to provide access to the Internet or a computer network.

5.7 Keywords

Dial-up Internet access: It is a form of Internet access that uses the facilities of the public switched telephone network (PSTN) to establish a dialed connection to an Internet service provider (ISP) via telephone lines.

Global Positioning System (GPS): GPS is a space-based satellite navigation system that provides location and time information in all weather conditions, anywhere on or near the Earth where there is an unobstructed line of sight to four or more GPS satellites.

Headphones: Headphones are a pair of small loudspeakers that are designed to be held in place close to a user's ears.

Mobile device: Mobile Device (also known as a handheld device, handheld computer or simply handheld) is a small, handheld computing device.

Personal digital assistant (PDA): PDA also known as a palmtop computer, or personal data assistant, is a mobile device that functions as a personal information manager.

Remote control: It is a component of an electronics device, most commonly a television set, DVD player and home theater systems originally used for operating the device wirelessly from a short line-of-sight distance.

USB adapter: It is a type of protocol converter which is used for converting USB data signals to and from other communications standards.

Wireless router: It is a device that performs the functions of a router but also includes the functions of a wireless access point.

WPAN (wireless personal area network): WPAN is a personal area network – a network for interconnecting devices centered around an individual person's workspace.

5.8 Review Questions

1. Discuss the characteristics of wireless routers.
2. What are the uses of a Bluetooth dongle?
3. What is RJ45 connector?
4. Explain Network Interface Card.

Notes

Answers: Self Assessment

1. PDA
2. Global Positioning System (GPS)
3. Sensor
4. Network
5. Ethernet
6. interference-free
7. adapter
8. USB
9. Router
10. Voltages
11. Antenna

5.9 Further Readings

Books

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

John Ross, *Introduction to wireless networks.*

Vijay Garg, *Wireless Communications & Networking.*

Theodore S. Rappaport, *Wireless Communications: Principles and Practice.*

Online links

http://education-portal.com/academy/lesson/network-interface-card-nic-types-function-definition.html

http://www.homeandlearn.co.uk/bc/bcs6p3.html

http://en.wikipedia.org/wiki/Modem

http://www.ehow.com/about_5112558_bluetooth-adapter.html

Unit 6: Wireless PAN Systems

Notes

CONTENTS

Objectives

Introduction

6.1 Basics of Wireless PAN Systems

6.1.1 Synchronization

6.1.2 Streaming Multimedia

6.1.3 Control

6.1.4 Internet Connections

6.2 SOHO Equipments

6.2.1 Designing a Small Home Office

6.2.2 Equipment Needed to Set Up a Small Office

6.3 Networking Technologies

6.3.1 Ethernet

6.3.2 Phone Line

6.3.3 Wireless

6.3.4 Mixing Media

6.4 Printing

6.4.1 Benefits of Wireless Printing

6.4.2 Wi-Fi Protected Setup

6.4.3 Wireless Setup

6.5 Accessing Internet

6.6 Accessing Personal Digital Assistant (PDAs)

6.7 Mobile Phones

6.8 Summary

6.9 Keywords

6.10 Review Questions

6.11 Further Readings

Objectives

After studying this unit, you will be able to:

- Discuss the basics of wireless PAN system
- Define about SOHO equipment's
- Explain the network technology in PAN system
- Understand the accessing Internet

Notes

- Explain how to access PDAs
- Discuss about mobile phone accessing

Introduction

A wireless network enables people to communicate and access applications and information without wires. This provides freedom of movement and the ability to extend applications to different parts of a building, city, or nearly anywhere in the world. Wireless networks allow people to interact with e-mail or browse the Internet from a location that they prefer.

Many types of wireless communication systems exist, but a distinguishing attribute of a wireless network is that communication takes place between computer devices. These devices include personal digital assistants (PDAs), laptops, personal computers (PCs), servers, and printers. Computer devices have processors, memory, and a means of interfacing with a particular type of network. Traditional cell phones don't fall within the definition of a computer device; however, newer phones and even audio headsets are beginning to incorporate computing power and network adapters. Eventually, most electronics will offer wireless network connections.

As with networks based on wire, or optical fibre, wireless networks convey information between computer devices. The information can take the form of e-mail messages, web pages, database records, streaming video or voice. In most cases, wireless networks transfer data, such as e-mail messages and files, but advancements in the performance of wireless networks is enabling support for video and voice communications as well.

6.1 Basics of Wireless PAN Systems

Wireless PAN is based on the standard IEEE 802.15. The two kinds of wireless technologies used for WPAN are Bluetooth and Infrared Data Association.

A WPAN could serve to interconnect all the ordinary computing and communicating devices that many people have on their desk or carry with them today; or it could serve a more specialized purpose such as allowing the surgeon and other team members to communicate during an operation.

6.1.1 Synchronization

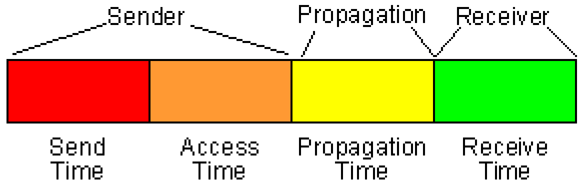
The definition of time synchronization does not necessarily mean that all clocks are perfectly matched across the network. This would be the strictest form of synchronization as well as the most difficult to implement. Precise clock synchronization is not always essential, so protocols from lenient to strict are available to meet one's needs.

There are three basic types of synchronization methods for wireless networks. The first is relative timing and is the simplest. It relies on the ordering of messages and events. The basic idea is to be able to determine if event 1 occurred before event 2. Comparing the local clocks to determine the order is all that is needed. Clock synchronization is not important.

The next method is relative timing in which the network clocks are independent of each other and the nodes keep track of drift and offset. Usually a node keeps information about its drift and offset in correspondence to neighbouring nodes. The nodes have the ability to synchronize their local time with another nodes local time at any instant. Most synchronization protocols use this method.

The last method is global synchronization where there is a constant global timescale throughout the network. This is obviously the most complex and the toughest to implement. Very few synchronizing algorithms use this method particularly because this type of synchronization usually is not necessary.

Figure 6.1: Breakdown of Packet Delay Components



Source: http://www.cse.wustl.edu/~jain/cse574-06/ftp/time_sync/

As shown in Figure 6.1, all the wireless synchronization schemes have four basic packet delay components: send time, access time, propagation time, and receive time. The send time is that of the sender constructing the time message to transmit on the network. The access time is that of the MAC layer delay in accessing the network. This could be waiting to transmit in a TDMA protocol. The time for the bits to by physically transmitted on the medium is considered the propagation time. Finally, the receive time is the receiving node processing the message and transferring it to the host. The major problem of time synchronization is not only that this packet delay exists, but also being able to predict the time spent on each can be difficult. Eliminating any of these will greatly increase the performance of the synchronization technique.

As illustrated there are many different variations of time synchronization or wireless networks. They range from very complex and difficult to implement to simpler and easy to implement. No matter the scheme used, all synchronization methods have the four basic components: send time, access time, propagation time, and receive time.

There are many synchronization protocols, many of which do not differ much from each other. As with any protocol, the basic idea is always there, but improving on the disadvantages is a constant evolution. Three protocols will be discussed at length: Reference Broadcast Synchronization (RBS), Timing-sync Protocol for Sensor Networks (TPSN), and Flooding Time Synchronization Protocol (FTSP). These three protocols are the major timing protocols currently in use for wireless networks. There are other synchronization protocols, but these three represent a good illustration of the different types of protocols. These three cover sender to receiver synchronization as well as receiver to receiver. Also, they cover single hop and multi hop synchronization schemes.

6.1.2 Streaming Multimedia

A wireless sensor network with multimedia capabilities typically consists of data sensor nodes, which sense, for instance, sound or motion, and video sensor nodes, which capture video of events of interest. In this survey, we focus on the video encoding at the video sensors and the real-time transport of the encoded video to a base station. Real-time video streams have stringent requirements for end-to-end delay and loss during network transport. In this survey, we categorize the requirements of multimedia traffic at each layer of the network protocol stack and further classify the mechanisms that have been proposed for multimedia streaming in wireless sensor networks at each layer of the stack. Specifically, we consider the mechanisms operating at the application, transport, network, and MAC layers. We also review existing cross-layer approaches and propose a few possible cross-layer solutions to optimise the performance of a given wireless sensor network for multimedia streaming applications.

6.1.3 Control

A Wireless PAN network does not use wires. They are more reliable as they have less number of cables.

6.1.4 Internet Connections

A wireless PAN interface can be used to connect to the Internet. A user has the capability to stay within a range and use it without having to forcefully sit in front of the desk.

6.2 SOHO Equipments

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.

Did u know? 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.

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.

6.2.1 Designing a Small Home Office

This checklist is provided so you can successfully set up your home network using the Network Setup Wizard. The checklist is a guideline of the steps needed, in the order they should be completed. Once you complete a step, or if it does not apply to you, check it off and then go on to the next step.

1. Sketch out your network: draw a diagram of your house or office where each computer and printer is located. Or, you can create a table that lists the hardware on each computer.
2. Next to each computer, note the hardware, such as modems and network adapters, each computer has.
3. Choose your Internet Connection Sharing (ICS) host computer. It is recommended that this computer be running Windows XP Home Edition or Windows XP Professional and have a working Internet connection. Choosing your Internet Connection Sharing host computer

4. Determine the type of network adapters you need for your home or small office network: Ethernet, home phoneline network adapter (HPNA), wireless, or IEEE 1394.
5. Make a list of hardware you need to purchase. This includes modems, network adapters, hubs, and cables. Buying the right hardware.
6. Purchase the hardware.
7. Install the network adapters and modems to create your network connections on each computer.
8. Physically connect the computers together. Plug in the cables to hubs, phone jacks, and the computer. Connect your computers together.
9. Turn on all computers and printers.
10. Make sure your ICS host computer has an active Internet connection. To establish your Internet connection, run the New Connection Wizard. Internet Connection Sharing.
11. Run the Windows XP fissional Network Setup Wizard on the ICS host computer.
12. Run the Network Setup Wizard on the other computers on your network.

6.2.2 Equipment Needed to Set Up a Small Office

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 covered in this document:

- PC Card Radio
- Mini-PCI Modules and Embedded Radios
- USB Adapters
- PCI and ISA Bus Adapters
- Compact Flash and Other Small-Client Formats
- Access Points and Gateways

6.3 Networking Technologies

Networking technology allow your computers to send information to each other. Some of the networking technologies include:

- Ethernet
- Phone line
- Wireless
- Mixing Media

6.3.1 Ethernet

Ethernet is a physical and data link layer technology for local area networks (LANs). Ethernet was invented by engineer Robert Metcalfe.

When first widely deployed in the 1980s, Ethernet supported a maximum theoretical data rate of 10 megabits per second (Mbps). Later, so-called "Fast Ethernet" standards increased this maximum data rate to 100 Mbps. Today, Gigabit Ethernet technology further extends peak performance up to 1000 Mbps.

Higher level network protocols like Internet Protocol (IP) use Ethernet as their transmission medium. Data travels over Ethernet inside protocol units called frames.

The run length of individual Ethernet cables is limited to roughly 100 meters, but Ethernet networks can be easily extended to link entire schools or office buildings using network bridge devices.

6.3.2 Phone Line

Phone-line networking is one of several ways to connect the computers in your home. If your computers are in different rooms, then phone-line networking could be a good solution for you.

Phone-line networking is easy to install, inexpensive and fast, and it doesn't require any additional wiring.

Phone-line networking, most commonly referred to as HomePNA, is based on the specifications developed by the Home Phone Networking Alliance (HPNA). The HPNA is a consortium of key networking technology companies that created a phone-line standard for the networking industry. HPNA 1.0, the original version of the standard, operated at a rather slow 1 megabit per second (Mbps). The current specification, HPNA 3.0, is based on technology developed by Broadcom and Copper Solutions. It operates at 128 Mbps.

HomePNA has several distinct advantages:

- It's easy to install.
- It's inexpensive.
- It's standardized.
- It's reliable.
- It operates at a constant 128 Mbps, even when the phone is in use.
- It requires no additional networking equipment (such as hubs or routers).
- It supports up to 50 devices.
- It is fast enough for bandwidth-intensive applications, such as video.
- It is compatible with other networking technologies.
- It works on Macs and older PCs (in addition to Windows and Linux systems).

HomePNA does have some drawbacks, though. You need a phone jack close to each computer. Otherwise, you will have to run phone extension cords or install new wiring. There is a physical limit of 1,000 feet (304.8 m) of wiring between devices, and the overall area of coverage should not exceed 10,000 square feet (929 m^2). Rarely (in fewer than 1 percent of U.S. homes), HomePNA will not work on the existing wiring. And while this author did not notice any interference with voice use, there have been reports of voices sounding "funny" or of a lot of noise on the phone once HomePNA is installed.

6.3.3 Wireless

Wireless is a term used to describe telecommunications in which electromagnetic waves (rather than some form of wire) carry the signal over part or all of the communication path. Some monitoring devices, such as intrusion alarms, employ acoustic waves at frequencies above the range of human hearing; these are also sometimes classified as wireless.

The wireless method of communication uses low-powered radio waves to transmit data between devices. High powered transmission sources usually require government licenses to broadcast on a specific wavelength. This platform has historically carried voice and has grown into a large industry, carrying many thousands of broadcasts around the world. Radio waves are now increasingly being used by unregulated computer users.

Humans communicate in order to share knowledge and experiences. Common forms of human communication include sign language, speaking, writing, gestures, and broadcasting. Communication can be interactive, transactive, intentional, or unintentional; it can also be verbal or nonverbal. In addition, communication can be intrapersonal or interpersonal.

We owe much to the Romans that in the field of communication it did not end with the Latin root communicare. They devised what might be described as the first real mail, or postal system, in order to centralize control of the empire from Rome. This allowed Rome to gather knowledge about events in its many widespread provinces.

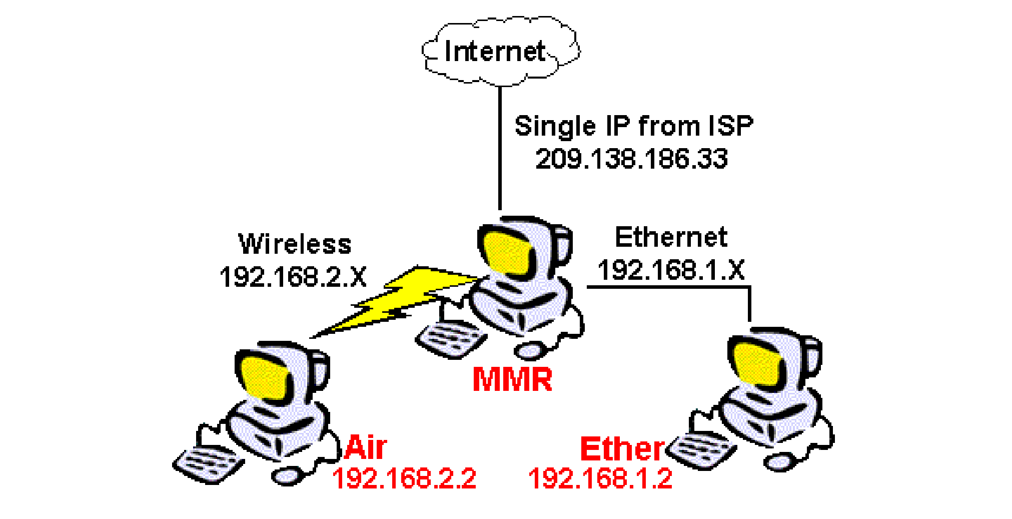
Did u know? The first wireless transmitters went on the air in the early 20th century using radiotelegraphy (Morse code). Later, as modulation made it possible to transmit voices and music via wireless, the medium came to be called "radio." With the advent of television, fax, data communication, and the effective use of a larger portion of the spectrum, the term "wireless" has been resurrected.

6.3.4 Mixing Media

The Figure 6.2 illustrates a simple example of a Mixed Media network. This network has only 3 computers:

- one with a Wireless network adapter;
- one with an Ethernet network adapter; and
- one with both Wireless and Ethernet adapters.

Figure 6.2: Mix Media Network



Source: http://www.practicallynetworked.com/networking/mmr_intro.htm

Notes

The computer that has both adapters also has an Internet connection. This connection can be via Dialup modem, cable modem, DSL, ISDN or any other method to connect to the Internet. This well-connected computer will be used as the MMR. The Mixed Media Router manages the data flow among the three networks that use different connection media, so that a single Internet connection will be shared among the computers in all the sub networks, and File and Printer sharing will work.

Self Assessment

Fill in the blanks:

1. Wireless PAN is based on the standard ....
2. Global .... is the most complex and the toughest to implement.
3. A wireless .... interface can be used to connect to the Internet.
4. .... is a physical and data link layer technology for local area networks (LANs).
5. Higher level network protocols like Internet Protocol (IP) use Ethernet as their .... medium.
6. The run length of individual Ethernet cables is limited to roughly .... meters.
7. .... networking is easy to install, inexpensive and fast, and it doesn't require any additional wiring.
8. Phone-line networking, most commonly referred to as ....
9. .... is a term used to describe telecommunications in which electromagnetic waves (rather than some form of wire) carry the signal over part or all of the communication path.
10. The wireless method of communication uses low-powered .... to transmit data between devices.

6.4 Printing

Wireless printing is a cost-effective way to easily and flexibly produce barcodes wherever you are. Virtually any printing application can go wireless – especially situations where cabling is either inconvenient or impossible. Realize great benefits from wireless printing technology.

> *Notes* Bluetooth wireless printing is a proprietary open wireless technology standard for exchanging data over short distances from fixed and mobile devices.

Wireless LAN 802.11b or 802.11g provides for secure data transfer of sensitive information.

Here are three ways to turn any printer into a wireless one.

1. ***Plug into a wireless print server:*** If your printer has a USB port, you can plug in a wireless print server, a small box into which you can connect your printer. The advantage of investing in a print server is that you don't have to connect the printer to a PC, which means you can use your laptop and print anywhere in your home. During the setup, you will have to plug the printer into the printer server, and connect that to the router using an Ethernet cable. Meanwhile, you'll have to install software on your computer and configure the connection, as you would when setting up a router.

2. ***Share your printer with other PCs in your home or office:*** If you have several computers sharing a printer (say, in a small office or your family's home) a cost-effective way to make the printer wireless is by connecting it to a host computer, going into the Control Panel in Windows, and enabling the printer to be shared on the network. Although this solution is free, the downside is that if the host computer is powered down, other computers on the network can't use the printer.

3. ***Buy a Bluetooth adapter:*** Almost every manufacturer sells an optional Bluetooth adapter, although they won't necessarily work with the model you're using.

6.4.1 Benefits of Wireless Printing

The benefit of connecting via Bluetooth is that if you have a simpler phone without Wi-Fi, you can still send files and pictures to the printer via Bluetooth (most laptops nowadays have Bluetooth as well). The trade-off is that older Bluetooth products, that use Version 1.1 or 1.2, have a rated range of 10 meters (about 33 feet), which is shorter than your router or Wi-Fi-enabled notebook's range. (Bluetooth 2.0 and 2.1, however, have a rated range of 100 meters.) The longer the range, of course, the more options you have when it comes time to find homes for your printer and laptop.

6.4.2 Wi-Fi Protected Setup

Wireless networks have evolved over the years. It used to be a royal pain to set up security, hand out IP addresses and connect other Wi-Fi devices to the network.

Nowadays, however, the equipment is much easier to set up initially, and connecting all kinds of devices is a snap because of something called Wi-Fi Protected Setup (WPS). With WPS, it's really easy to add devices on the fly.

Many Wi-Fi connectable devices have WPS buttons on them these days, as do most D-Link routers. To see if yours does, just look for an icon featuring two opposite-facing arrows (see image on right). To add a WPS-enabled device to your network, simply press the WPS button on your router then press the WPS button on the device. They identify each other, and you're off and running.

There are other WPS connection methods, too, namely:

- PIN number
- USB drive set-up (code is transferred from the USB stick to the new device)
- "Near Field Communication" NFC (just position the device next to the other, and they identify each other)

6.4.3 Wireless Setup

To make a wireless setup:

1. Make sure your printer has wireless network adapters or a wireless router.
2. Power on the printer and wireless router.
3. Configure the printer to connect the wireless router. Enable the DHCP option on the printer. Obtain the IP address automatically. Configure the DHCP server of wireless router. Again, assign the IP address automatically.
4. Verify connectivity. Try doing some test prints. If it doesn't work, check the IP addresses.

Notes

6.5 Accessing Internet

To access a wireless network, follow the steps below:

1. ***Connect to the Internet:*** The DSL or cable modem should be working as this sets up the wireless network.
2. ***Connect your Wireless Router:*** Setting up a wireless router is straightforward as long as you have a PC with a wireless network adapter, as well as an active high-speed Internet connection. You might also need a computer with a wired network adapter and router-specific setup software, which is typically included on a disc packaged with your router or available for download on the router manufacturer's support site.

Set Up Your Wireless Router on a Windows 7 PC

1. Connect the wireless router to your modem using an Ethernet cable.
2. Connect your wireless router to a power source. Wait about a minute, and then continue to the next step.
3. Click the network icon in the notification area; the icon should look like a series of vertical bars, or a tiny PC with a network adapter alongside it.
4. Select your wireless network from the list of available networks to complete the setup process. By default, your network name will be the name of your router manufacturer.

Set Up Your Router Using the Setup Software

1. Make sure that your wireless router is completely disconnected from the modem, the computer, and the power source.
2. On your PC, insert the disc that came with your router, or download and run the latest version of the router's software from the vendor website.
3. Follow the on-screen instructions. The setup routine will ask you to connect components (including your modem and PC) in a certain order, and it may request that you temporarily connect your wireless router to a computer via an ethernet cable. You will also create a wireless network name and password at this point. If something goes wrong, you may want to consider manually configuring your wireless router.

Manually Configure Your Router Without Setup Software

1. Connect your wireless router to the modem, using an ethernet cable.
2. Connect the wireless router to a power source. Wait about a minute to ensure that your router is fully operational.
3. Connect the wireless router to your computer using an ethernet cable.
4. Log in to your router's Web interface by opening a browser and entering the IP address of your router into the address bar. The IP address should be listed within your router's documentation; if you can't find it, most routers use a common IP address such as http://192.168.1.1, http://192.168.0.1, or http://192.168.2.1.
5. Enter the default username and password, which you should find within your router's documentation. Alternatively, visit Port Forward's Default Router Passwords page.
6. Use the Web interface to set up a network name and password.

7. Disconnect your computer from the wireless router and then reconnect wirelessly.

8. Caution: Be sure to use a password to protect your wireless network. Unauthorized parties can easily connect to an unprotected network, stealing your bandwidth as well as your personal data.

9. Connecting Computers, Printers, and Other Devices to the Wireless Network

10. Sharing Files, Printers, and More: We can share files, printers, games, etc. after all the setup.

6.6 Accessing Personal Digital Assistant (PDA)

A personal digital assistant (PDA) is a handheld computer. Personal digital assistants were designed to replace non-electronic day planners. Many PDAs can work as an address book, a calculator, a clock, and a calendar. Some also have games on them. Newer PDAs are now called smartphones and have Wi-Fi, touch screens, can read e-mail, record video, play music and make phone calls.

6.7 Mobile Phones

A cellular network or mobile network is a radio network distributed over land areas called cells, each served by at least one fixed-location transceiver, known as a cell site or base station. In a cellular network, each cell uses a different set of frequencies from neighboring cells, to avoid interference and provide guaranteed bandwidth within each cell.

When joined together these cells provide radio coverage over a wide geographic area. This enables a large number of portable transceivers (e.g., mobile phones, pagers, etc.) to communicate with each other and with fixed transceivers and telephones anywhere in the network, via base stations, even if some of the transceivers are moving through more than one cell during transmission.

Cellular networks offer a number of advantages over alternative solutions:

- flexible enough to use the features and functions of almost all public and private networks
- increased capacity
- reduced power use
- larger coverage area
- reduced interference from other signals

An example of a simple non-telephone cellular system is an old taxi drivers' radio system, in which a taxi company has several transmitters based around a city that can communicate directly with each other.

Self Assessment

Fill in the blanks:

11. An example of a simple non-telephone cellular system is an old .... radio system.

12. In a .... network, each cell uses a different set of frequencies from neighbouring cells, to avoid interference and provide guaranteed bandwidth within each cell.

13. Personal digital assistants were designed to replace .... day planners.

14. Wireless LAN 802.11b or 802.11g provides for secure data transfer of .... information.

Notes

15. .... wireless printing is a proprietary open wireless technology standard for exchanging data over short distances from fixed and mobile devices.

16. .... printing is a cost-effective way to easily and flexibly produce barcodes wherever you are.

Case Study

Wireless Microphone

A wireless microphone is a microphone without a physical cable connecting it directly to the sound recording or amplifying equipment with which it is associated. Also known as a radio microphone, it has a small, battery-powered radio transmitter in the microphone body, which transmits the audio signal from the microphone by radio waves to a nearby receiver unit, which recovers the audio. The other audio equipment is connected to the receiver unit by cable. Wireless microphones are widely used in the entertainment industry, television broadcasting, and public speaking to allow public speakers, interviewers, performers, and entertainers to move about freely while using a microphone to amplify their voices.

There are many different standards, frequencies and transmission technologies used to replace the microphone's cable connection and make it into a wireless microphone. They can transmit, for example, in radio waves using UHF or VHF frequencies, FM, AM, or various digital modulation schemes. Some low cost (or specialist) models use infrared light. Infrared microphones require a direct line of sight between the microphone and the receiver, while costlier radio frequency models do not.

Some models operate on a single fixed frequency, but the more advanced models operate on a user selectable frequency to avoid interference, and allow the use of several microphones at the same time.

Advantages and disadvantages

Wireless microphones awaiting pickup by performers in a musical.

The advantages are:

- Greater freedom of movement for the artist or speaker.

Contd...

Notes

- Avoidance of cabling problems common with wired microphones, caused by constant moving and stressing the cables.
- Reduction of cable "trip hazards" in the performance space.

The disadvantages are:

- Sometimes limited range (a wired balanced XLR microphone can run up to 300 ft or 100 meters). Some wireless systems have a shorter range, while more expensive models can exceed that distance.
- Possible interference with or, more often, from other radio equipment or other radio microphones, though models with many frequency-synthesized switch-selectable channels are now plentiful and cost effective.
- Operation time is limited relative to battery life; it is shorter than a normal condenser microphone due to greater drain on batteries from transmitting circuitry, and from circuitry giving extra features, if present.
- Noise or dead spots (places where it doesn't work, especially in non-diversity systems).
- Limited number of operating microphones at the same time and place, due to the limited number of radio channels (frequencies).

Techniques

The professional models transmit in VHF or UHF radio frequency and have 'true' diversity reception (two separate receiver modules each with its own antenna), which eliminates dead spots (caused by phase cancellation) and the effects caused by the reflection of the radio waves on walls and surfaces in general. (See antenna diversity).

Another technique used to improve the sound quality (actually, to improve the dynamic range), is companding. Nady Systems, Inc. was the first to offer this technology in wireless microphones in 1976, which was based on the patent obtained by company founder John Nady.

Some models have adjustable gain on the microphone itself, to be able to accommodate different level sources, such as loud instruments or quiet voices. Adjustable gain helps to avoid clipping.

Some models have adjustable squelch, which silences the output when the receiver does not get a strong or quality signal from the microphone, instead of reproducing noise. When squelch is adjusted, the threshold of the signal quality or level is adjusted.

Products

The original manufacturer of the wireless microphone was Vega Electronics Corporation. AKG Acoustics, Audio Ltd, Audio-Technical, Electro-Voice, Lectrosonics, MIPRO, Nady Systems, Inc, Samson Technologies, Sennheiser, Shure, Sony and Zaxcom are all major manufacturers of wireless microphone systems. They have made significant advances in dealing with many of the disadvantages listed above. For example, while there is a limited band in which the microphones may operate, several high-end systems can consist of over 100 different microphones operating simultaneously. However, the ability to have more microphones operating at the same time increases the cost due to component specifications, design and construction. That is one reason for such large price differences between different series of wireless systems.

Generally there are three wireless microphone types: handheld, plug-in and bodypack: Handheld looks like a 'normal' wired microphone, but may have a bigger body to accommodate the transmitter and battery pack.

Contd...

Plug-in, plug-on, slot-in, or cube-style transmitters attach to the bottom of a standard microphone, thus converting it to wireless operation (see below).

Bodypack is a small box housing the transmitter and battery pack, but not the microphone itself. It is attachable to belt or elsewhere and has a wire going to headset, lavalier microphone or a guitar.

Several manufacturers including Sennheiser, AKG, Nady Systems, Lectrosonics and Zaxcom offer a plug-in transmitter for existing wired microphones, which plugs into the XLR output of the microphone and transmits to the manufacturer's standard receiver. This offers many of the benefits of an integrated system, and also allows microphone types (of which there may be no wireless equivalent) to be used without a cable. For example a television, or film, sound production engineer may use a plug-in transmitter to enable wireless transmission of a highly directional rifle (or "shotgun") microphone, removing the safety hazard of a cable connection and permitting the production engineer greater freedom to follow the action. Plug-in transmitters also allow the conversion of vintage microphone types to cordless operation. This is useful where a vintage microphone is needed for visual or other artistic reasons, and the absence of cables allows for rapid scene changes and reducing trip hazards. In some cases these plug-in transmitters can also provide 48 volt phantom power allowing the use of condenser microphone types. DC-DC converter circuitry within the transmitter is used to multiply the battery supply, which may be three volts or less, up to the required 48 volts.

Receivers

Wireless microphone receiver racks backstage at a large televised music awards event.

There are many types of receiver. True Diversity receivers have two radio modules and two antennas. Diversity receivers have one radio module and two antennas, although some times the second antenna may not be obviously visible. Non-diversity receivers have only one antenna.

Receivers are commonly housed in a half-rack configuration, so that two can be mounted together in a rack system (that is to say the receiver is enclosed in a box 1U high and half-width, so two receivers can be installed in 1U). For large complex multi-channel radio microphone systems, as used in broadcast television studios and musical theatre productions, modular receiver systems with several (commonly six or eight) true diversity receivers slotting into a rack mounted mainframe housing are available. Several mainframes may be used together in a rack to supply the number of receivers required. In some musical theatre productions, systems with forty or more radio microphones are not unusual.

Receivers specifically for use with video cameras are often mounted in a bodypack configuration, typically with a hotshoe mount to be fitted onto the hotshoe of the camcorder. Small true diversity receivers which slot into a special housing on many professional broadcast standard video cameras are produced by manufacturers including Sennheiser, Lectrosonics and Sony. For less demanding or more budget conscious video applications small non-diversity receivers are common. When used at relatively short operating distances from the transmitter this arrangement gives adequate and reliable performance.

Questions:

1. Discuss the techniques used to improve the sound quality of wireless microphones.
2. What are the different types of wireless microphone receivers?

Source: http://en.wikipedia.org/wiki/Wireless_microphone

6.8 Summary

- A wireless network enables people to communicate and access applications and information without wires.
- Many types of wireless communication systems exist, but a distinguishing attribute of a wireless network is that communication takes place between computer devices.
- As with networks based on wire, or optical fibre, wireless networks convey information between computer devices. The information can take the form of e-mail messages, web pages, database records, streaming video or voice.
- A wireless sensor network with multimedia capabilities typically consists of data sensor nodes, which sense, for instance, sound or motion, and video sensor nodes, which capture video of events of interest.
- A Wireless PAN network does not use wires. They are more reliable as they have less number of cables.
- Ethernet is a physical and data link layer technology for local area networks (LANs). Ethernet was invented by engineer Robert Metcalfe.
- Phone-line networking is easy to install, inexpensive and fast, and it doesn't require any additional wiring.
- The wireless method of communication uses low-powered radio waves to transmit data between devices.

6.9 Keywords

Cellular network or mobile network: It is a radio network distributed over land areas called cells, each served by at least one fixed-location transceiver, known as a cell site or base station.

Ethernet: It is a physical and data link layer technology for local area networks (LANs).

Personal digital assistant (PDA): PDA is a handheld computer. Personal digital assistants were designed to replace non-electronic day planners.

Phone-line networking: It is one of several ways to connect the computers in your home.

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

Wireless: Wireless is a term used to describe telecommunications in which electromagnetic waves (rather than some form of wire) carry the signal over part or all of the communication path.

Wireless printing: It is a cost-effective way to easily and flexibly produce barcodes wherever you are.

Wireless sensor: Network with multimedia capabilities typically consists of data sensor nodes, which sense, for instance, sound or motion, and video sensor nodes, which capture video of events of interest.

6.10 Review Questions

1. What are the basic types of synchronization methods for wireless networks?
2. Explain SOHO equipment's.
3. Explain the procedure for designing a small home office.

4. What are the equipment needed to set up a small office?
5. Describe mix media network.
6. What are the three ways to turn any printer into a wireless one?
7. Discuss the benefits of wireless printing.
8. What are the advantages of cellular networks over alternative solutions?

Answers: Self Assessment

1.	IEEE 802.15.	2.	Synchronization
3.	PAN	4.	Ethernet
5.	Transmission	6.	100
7.	Phone-line	8.	Home PNA
9.	Wireless	10.	Radio waves
11.	Taxi drivers’	12.	Cellular
13.	Non-electronic	14.	Sensitive
15.	Bluetooth	16.	Wireless

6.11 Further Readings

Books

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

John Ross, *Introduction to wireless networks.*

Vijay Garg, *Wireless Communications & Networking.*

Theodore S. Rappaport, *Wireless Communications: Principles and Practice.*

Online links

http://www.mhprofessional.com/downloads/products/0071789111/0071789111_chap19.pdf

http://www.wi-fi.org/files/kc_25_Five%20Steps%20to%20Creating%20a%20Wireless%20Network.pdf

http://wordinfo.info/unit/4003/ip:1/il:W

Notes

Unit 7: Wireless LAN

CONTENTS

Objectives

Introduction

7.1 History of Wireless LAN

7.2 Wireless Local Area Network

7.2.1 Why Wireless?

7.2.2 How Wireless LANs Are Used in the Real World?

7.2.3 How Wireless LANs Work?

7.2.4 Wireless LAN Configurations

7.2.5 Wireless LAN Technology

7.3 Wireless LAN Components

7.3.1 User Devices

7.3.2 Radio NICs

7.3.3 Access Points

7.3.4 Routers

7.3.5 Repeaters

7.3.6 Antennae

7.4 Small Office/Home Office (SOHO) Applications

7.4.1 SOHO Wireless Network Components

7.4.2 SOHO Network to Internet Access

7.5 Public Wireless LAN Network

7.5.1 Benefits of Wireless LAN

7.5.2 Disadvantages of Wireless LAN

7.6 Ad Hoc Wireless LAN Network

7.7 Summary

7.8 Keywords

7.9 Review Questions

7.10 Further Readings

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 bidirectional 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 2 Mbps 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 2.4 GHz 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:

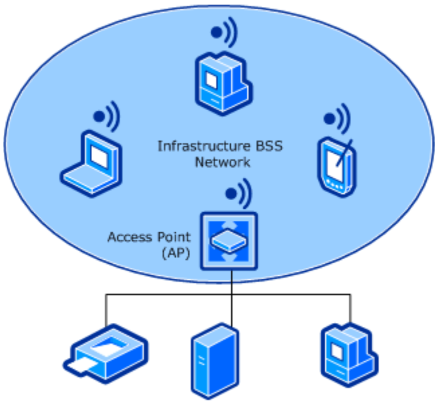
1. ***Infrastructure BSS Networks:*** In this topology, all stations within the BSS communicate with each other through an access point (AP). In this situation, the AP establishes the BSS network. In addition, an infrastructure BSS can consist of more than one interconnected APs that establishes an extended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

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



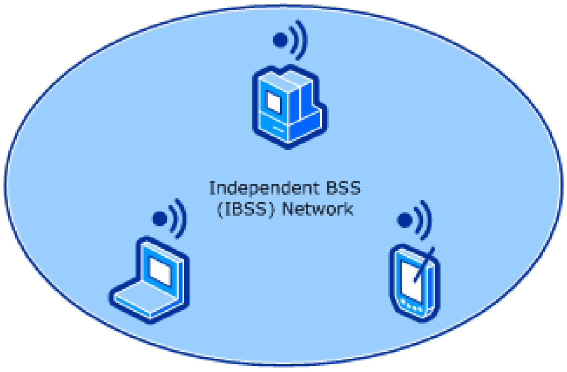
Source: http://msdn.microsoft.com/en-us/library/windows/hardware/ff556962%28v=vs.85%29.aspx

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.

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 already relatively widely used. As in a majority of cases, WLAN is used to enhance an already 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 through 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 already 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.

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.

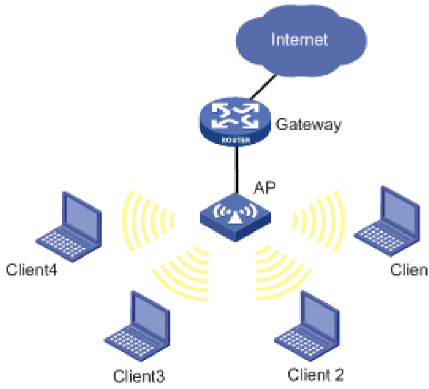
3. ***Infrared Technology:*** Infrared (IR) systems use very high frequencies, just below visible light in the electromagnetic spectrum, to carry data. Like light, IR cannot penetrate opaque objects; it is either directed (line-of-sight) or diffuse technology. Inexpensive directed systems provide very 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, unauthorised 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

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.

- 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.

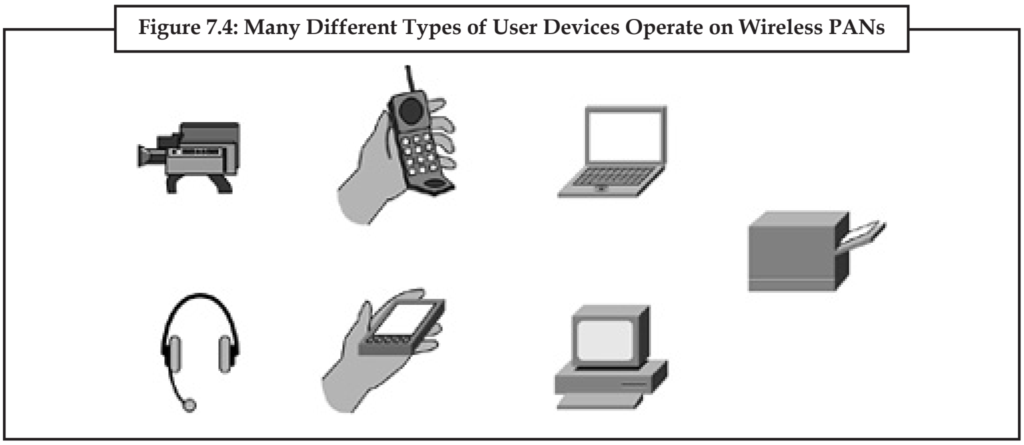
7.3.1 User Devices

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.

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

- 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:

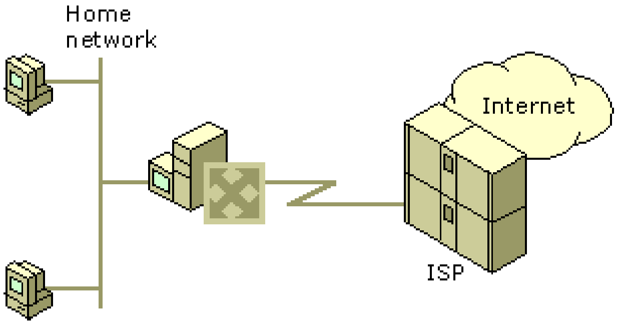
   (a) One network segment.

   (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.

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

   This scenario describes a small office or home office (SOHO) network that connects to the Internet by using a routed 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 travelling, 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 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) 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 200 metres 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 kilometres, 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.

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:

8. A .... is a device that allows wireless devices to connect to a wired network using Wi-Fi, or related standards.
9. 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.
10. An important property of an antenna is the ability to focus and shape the .... power in space.
11. The communication network established for the purpose of connecting computer devices of personal use is known as the ....
12. Wireless LANs use .... waves to communicate.
13. A wireless ad hoc network is a .... type of wireless network.
14. .... often refers to a mode of operation of IEEE 802.11 wireless networks.
15. The earliest wireless ad hoc networks were the .... networks.

Case Study **Wireless IP**

Introduction

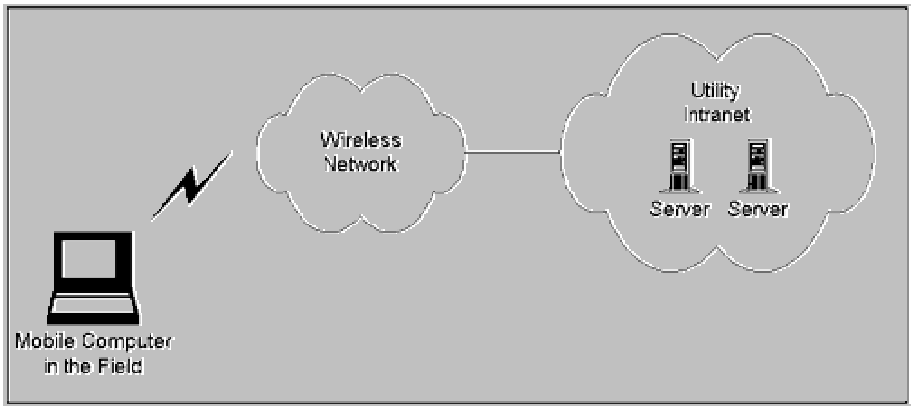
What if field workers of a public utility had online access to inventory databases, work orders, maps and other essential information from anywhere? What if crew chiefs had access to e-mail and schedules without having to return to their offices? This is the vision that the City of Seattle Public Utilities 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.

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...

Notes

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



Goals

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

Contd...

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.

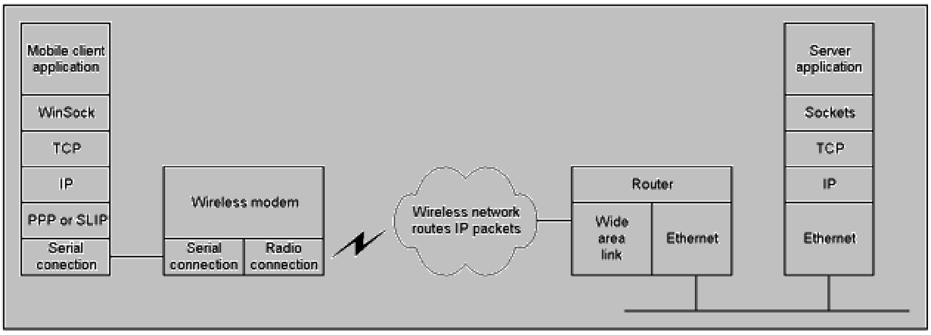
Despite some of the advantages of Windows CE, the utility was concerned about the range of applications it could deploy on the platform. Because the utility expects the requirements for mobile workers to evolve over time, and for the types of work performed in the field to expand, it needs the greatest 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 rugged 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.

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 2: 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; fibre 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

Contd...

Notes

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

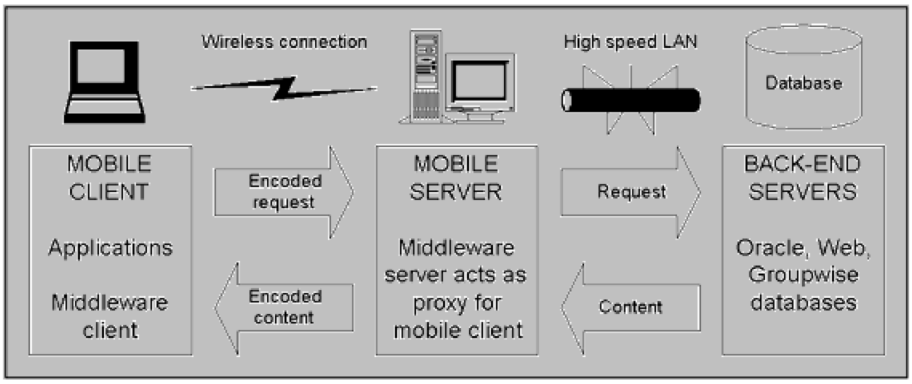
In an ideal world, a computer connected over a wireless network would work just like a computer on a LAN. But wireless networks operate at lower speeds with higher latency, and connections can be lost at any moment, especially when mobile. The utility has considered a number of software approaches, seeking 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 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 optimise communications. The utility has looked at wireless middleware designed specifically for MAXIMO, as well as general purpose middleware that optimises 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



Contd...

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 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.

Contd...

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. 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-optimised 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.

Contd...

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.

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.

1. Discuss the different types of remote workers related with wireless system.
2. Discuss various software approaches used for wireless IP.

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.
  - ❖ 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

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

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

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

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

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

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

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.

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

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

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

John Ross, *Introduction to wireless networks.*

Vijay Garg, *Wireless Communications & Networking.*

Theodore S. Rappaport, *Wireless Communications: Principles and Practice.*

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

Notes

Unit 8: Wireless MAN

CONTENTS

Objectives

Introduction

8.1 Meaning of Wireless MAN

8.2 Components

8.2.1 Bridges

8.2.2 Bridges versus Access Points

8.2.3 Ethernet to Wireless Bridges

8.2.4 Workgroup Bridges

8.2.5 Directional Antenna

8.2.6 Semi-directional

8.2.7 Highly Directional Antenna

8.2.8 Polarization

8.3 Summary

8.4 Keywords

8.5 Review Questions

8.6 Further Readings

Objectives

After studying this unit, you will be able to:

- Discuss the wireless MAN
- Explain the component of wireless MAN

Introduction

A metropolitan area network (MAN) is a computer network in which two or more computers or communicating devices or networks which are geographically separated but in same metropolitan city and are connected to each other are said to be connected on MAN. The limits of Metropolitan cities are determined by local municipal corporations and we cannot define them. Hence, the bigger the Metropolitan city the bigger the MAN, smaller a metro city smaller the MAN.

8.1 Meaning of Wireless MAN

Wireless Metropolitan Area Network (WMAN) enables you to access the Internet and multimedia streaming services via a wireless region area network (WRAN).

These networks provide a very fast data speed compared with the data rates of mobile telecommunication technology as well as other wireless network, and their range is also extensive.

There are following three major issues with Wireless Networks.

- ***Quality of Service (QoS):*** One of the primary concerns about wireless data delivery is that, like the Internet over wired services, QoS is inadequate. Lost packets, and atmospheric interference are recurring problems wireless protocols.

Notes

- ***Security Risk:*** This has been another major issue with a data transfer over a wireless network. Basic network security mechanisms like the service set identifier (SSID) and Wireless Equivalency Privacy (WEP). These measures may be adequate for residences and small businesses but they are inadequate for entities that require stronger security.
- ***Reachable Range:*** Normally wireless network offers a range of about 100 meters or less. Range is a function of antenna design and power. Now a days the range of wireless is extended to tens of miles so this should not be an issue any more.

WMAN (Wireless Metropolitan Area Networking) allows communication between two or more terminals (nodes) using just one access point, within a radius up to 40 km. The most well-known wireless networking technology is WiMAX (World Wide Interoperability for Microwave Access)` created by WiMAX Forum which was founded by Esemble, Nokia, Harri and Cross Span in 2001. This wireless network is also known as IEEE 802.16 (Institute of Electrical and Electronics Engineers), standard which defines the technology.

WiMAX works with radio wave for transmission and microwaves for reception in frequencies between 2,3 and 3,5 GHz. This allows reaching speeds of 70 Mbps within distances up to 50 km from the access point. Thus, a radial area of 100 km could be cover with only one access point. Thus, a radial area of 100 km could be cover with only one access point.

The technology is commonly used to provide internet to rural areas in which installing other types of technology becomes too expensive. Installed in the cities, WiMAX will allow people to connect to the internet whenever they want without looking for ‘hotspots’. This will transform the user internet mobile lifestyle.

The first WiMAX standard IEEE 802.16, was created to administrate the interoperability of all devices working between 10 and 66 GHz. It will allow, as WiFI does, receive and transmit encrypted information among devices that have the technology. Within this standard, we should make some remarks to the IEEE 802.16a, IEEE 802.16e-2005 and IEEE802.16m which will allow to work with frequencies from 2 to 11 GHz, mobility and speed up to 1 GB, respectively.

8.2 Components

The various components are as follows:

8.2.1 Bridges

A wireless bridge is a hardware component used to connect two or more network segments (LANs or parts of a LAN) which are physically and logically (by protocol) separated. It does not necessarily always need to be a hardware device, as some operating systems (such as Windows, GNU/Linux, Mac OS X and FreeBSD) provide software to bridge different protocols. This is seen commonly in protocols over wireless to cable. So in a sense the computer acts as a bridge by using bridging OS software.

Many wireless routers and wireless access points offer either a “bridge” mode or a “repeater” mode, both of which perform a similar common function, the difference being the bridge mode connects two different protocol types and the repeater mode relays the same protocol type. Wireless routers, access points, and bridges are available that are compliant with the IEEE802.11a, b, g and n standards. The frequency bands for these wireless standards can be used license-free in most countries.

Wireless bridge devices work in pairs (point-to-point), one on each side of the “bridge”. However, there can be many simultaneous “bridges” using one central device (point to multipoint).

Bridging can be via WDS (Wireless Distribution System) which creates a transparent Level 2 wireless bridge between two or more points. Alternately the bridge can be set up as an access point – client relationship which requires the wireless devices used for the bridge to be set to the same service set identifier (SSID) and radio channel.

An example of a point-to-point bridge application would be connecting two commercial buildings.

Example: Example of a combination point-to-point bridge and point to multipoint application would be connecting multiple farm buildings.

Bridging has historically referred to propagation of data across a device without traversing a network stack, such as TCP/IP. Wireless bridging is a colloquial term. A more accurate description of connecting two local area networks would be a Wireless LAN to LAN bridge. The distinction is important. While a device may not support bridging to a remote wireless access point to connect two LANs, it may be desirable (and supported) that a wireless access point support true bridging; where packets traverse from a wireless to wired network without passing through an internal protocol stack, firewall or other network abstraction. Two bridged networks could be treated as parts of a single subnet under Internet Protocol (IP). A wireless client would be able to make a DHCP request to a wired DHCP server if the wired and wireless networks were bridged. In the ISO OSI model, a device in which packets traverse the network layer is considered a router, a device in which packets traverse the data link layer only is considered a bridge.

Unless a user has a wireless card with a PXE-ROM chip built into it, it is not easy to directly netboot over a wireless connection. BIOS-based PXE algorithms usually only search for a wired NIC to be used in a PXE netboot.

It is possible to connect a "wireless bridge" (i.e. a wireless router or access point set to the "bridge" mode) to the wired NIC of a PC. The PC then netboots through the wired Ethernet NIC as usual, but the data is then transmitted from the NIC to the wireless AP/router connected to it and then wirelessly "across the bridge" to a central wireless access point/router.

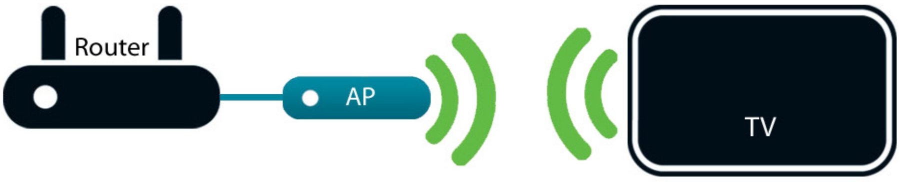
This requires two wireless devices (one wireless access point and one client device), making it a more expensive solution. It is sometimes, however, easier or less expensive than running extra Ethernet cables between the two points.

8.2.2 Bridges versus Access Points

A network bridge can connect wired devices to a wireless network. The benefits are obvious: say goodbye to the miles of cable you'd otherwise need to connect faraway wired devices to your router. When you connect wired devices to a bridge, they can communicate wirelessly with your router and all of the devices on your network.

The confusion sets in when the term "bridge" is interchanged with the phrase "access point." Calling a device a bridge is a shorthand way to say that it supports network bridging, but you won't often see a standalone bridge for sale. Instead, you'll find wireless access points with bridging capability built in — and switching between either mode is as easy as flicking a switch on the rear of the access point.

Figure 8.1: AP Positioning



Source: http://resource.dlink.com/connect/the-difference-between-bridges-and-access-points/

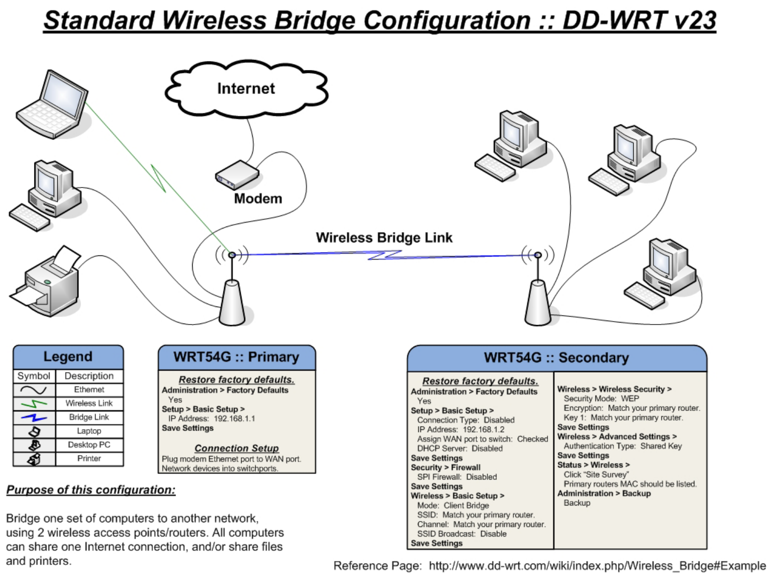
An access point connects to your home network with an Ethernet cable and creates a new sphere of wireless coverage, letting you add wireless devices to your home network. Access points can either be used to add wireless capabilities to a non-wireless router or improve the speed and range of an existing wireless network. When devices connect to your access point's SSID, they join your preexisting wired LAN.

To avoid confusion, resist the urge to call this bridging. (While an access point might appear to bridge the connection between wireless devices and a network, it's not connecting separate networks.) The distinction is important: A wireless access point connects users to a network by creating a wireless signal they can use. A bridge, in contrast, connects separate networks —your preexisting wireless home network to all of the devices connected to the bridge.

8.2.3 Ethernet to Wireless Bridges

Wireless Bridging is used to connect two LAN segments via a wireless link. The two segments will be in the same subnet and look like two Ethernet switches connected by a cable to all computers on the subnet. Since the computers are on the same subnet, broadcasts will reach all machines, allowing DHCP clients in one segment to get their addresses from a DHCP server in a different segment. You could use a Wireless Bridge to transparently connect computer(s) in one room to computer(s) in a different room when you could not, or did not want to run an Ethernet cable between the rooms. Contrast this with Client Mode Wireless, where the local wireless device running DD-WRT connects to the remote router as a client, creating two separate subnets. Since the computers within the different subnets cannot see each other directly, this requires the enabling of NAT between the wireless and the wired ports, and setting up port forwarding for the computers behind the local wireless device. Segments connected via Client Mode Wireless cannot share a DHCP server.

Figure 8.2: Wireless Bridge Configuration



Legend

Symbol	Description
∼	Ethernet
⚡	Wireless Link
⚡	Bridge Link
	Laptop
	Desktop PC
	Printer

WRT54G :: Primary

Restore factory defaults.
Administration > Factory Defaults
  Yes
Setup > Basic Setup >
  IP Address: 192.168.1.1
Save Settings

Connection Setup
Plug modem Ethernet port to WAN port.
Network devices into switchports.

WRT54G :: Secondary

Restore factory defaults.
Administration > Factory Defaults
  Yes
Setup > Basic Setup >
  Connection Type: Disabled
  IP Address: 192.168.1.2
  Assign WAN port to switch: Checked
  DHCP Server: Disabled
Save Settings
Security > Firewall
  SPI Firewall: Disabled
Save Settings
Wireless > Basic Setup >
  Mode: Client Bridge
  SSID: Match your primary router.
  Channel: Match your primary router.
  SSID Broadcast: Disable
Save Settings

Wireless > Wireless Security >
  Security Mode: WEP
  Encryption: Match your primary router.
  Key 1: Match your primary router.
Save Settings
Wireless > Advanced Settings >
  Authentication Type: Shared Key
Save Settings
Status > Wireless >
  Click "Site Survey"
  Primary routers MAC should be listed.
Administration > Backup
  Backup

Purpose of this configuration:

Bridge one set of computers to another network, using 2 wireless access points/routers. All computers can share one Internet connection, and/or share files and printers.

Reference Page: http://www.dd-wrt.com/wiki/index.php/Wireless_Bridge#Example

Source: www.dd-wrt.co.in/wiki/index.php/Wireless_Bridge

In the case in which we are interested, a wireless device running DD-WRT such as a WRT54G is configured as a Wireless Bridge between a remote wireless router (of any make/brand) and the Ethernet ports on the WRT54G.

A wireless Ethernet bridge allows the connection of devices on a wired Ethernet network to a wireless network. The bridge acts as the connection point to the Wireless LAN.

Notes

8.2.4 Workgroup Bridges

In workgroup bridge mode, the workgroup bridge associates to an access point, or bridge as a client and provides a wireless network connection for up to eight Ethernet-enabled devices connected to its Ethernet port. It informs the associated root device of the attached wired clients using IAPP messaging. The workgroup bridge does not accept wireless client associations.

A workgroup bridge:

- Associates to the following devices:
  - ❖ Root access points
  - ❖ Root devices
- If the router contains a 2.4 GHz WMIC, it operates with 2.4 GHz (802.11b/g) Cisco IOS-based bridges. If the router contains a 4.9 GHz WMIC, it operates with 4.9 GHz IOS-based bridges.
- Accepts only wired clients.
- Informs its root parent of all attached wired clients by using Inter-Access Point Protocol (IAPP) messaging.

In addition, you can configure the wireless device to support the following workgroup bridge features:

- ***Interoperability:*** The universal workgroup bridge can forward routing traffic using a non-cisco root device as a universal client. The universal workgroup bridge appears as a normal wireless client to the root device.
- ***World Mode:*** In standard world mode configuration, the wireless device passively scans for world mode only when the workgroup bridge boots up and performs a first scan. When the workgroup bridge receives a response from the root device for its world mode scan, it updates its frequency list and output power level according to the current country of operation. Thereafter, the workgroup bridge always performs an active scan.

  To support continued operation during inter-country travel (such as airplane travel from New York to London), the workgroup bridge must perform a passive scan. In this configuration, the workgroup bridge associates to the root device, and it obtains the country-specific list of frequency and output power levels through passive scan.

  To support this operational change, add the roaming keyword to the world-mode command. This option instructs the workgroup bridge that it must always passively scanning.

  The workgroup bridge uses the 802.11d option for world mode. The wireless device tries to receive information about the country-specific list of frequency and output power levels through the 802.11d Information Element.

> *Notes* With roaming added to the world-mode command, roaming takes a longer time; therefore, it is recommended only for situations in which it is required to assure continuous operation.

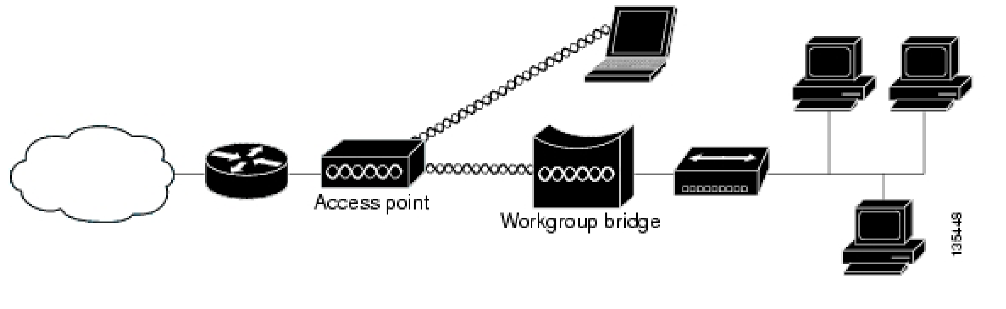
- ***Multiple Client Profiles:*** The workgroup bridge can support multiple client profiles. A client device with multiple configurable profiles can automatically select a client profile based on available infrastructure and set of profiles. For more information, see Cisco 3200 Series Wireless MIC Software Configuration Guide.

Notes

For example, to provide wireless connectivity for a group of network printers, connect the printers to a hub or to a switch, connect the hub or switch to the Ethernet port of the workgroup bridge. The workgroup bridge transfers data through its association with an access point or bridge on the network.

Figure 8.3 shows a typical scenario where the device functions as a workgroup bridge.

Figure 8.3: Workgroup Bridge Mode



To enable the router in workgroup-bridge mode:

- wd(config)#interface dot11radio interfacenumber
- wd(config-in)#station-role workgroup-bridge

The device to which a workgroup bridge associates can treat the workgroup bridge as an infrastructure device or as a simple client device.

For increased reliability, set the infrastructure-client parameter on the access point or bridge to treat the workgroup bridge as an infrastructure device. When a workgroup bridge is treated as an infrastructure device, the access point reliably delivers multicast packets, which include Address Resolution Protocol (ARP) packets to the workgroup bridge.

If an access point or bridge is configured to treat a workgroup bridge as a client device, more workgroup bridges are allowed to associate to the same access point or to associate with use of a service set identifier (SSID) that is not an infrastructure SSID.

The performance cost of reliable multicast delivery – in which the duplication of each multicast packet is sent to each workgroup bridge – limits the number of infrastructure devices (including workgroup bridges) that can associate to an access point or bridge. To increase the number of workgroup bridges that can associate to the access point beyond 20, the access point must reduce the delivery reliability of multicast packets to the workgroup bridges. With reduced reliability, the access point cannot confirm that multicast packets reached the intended workgroup bridge. The workgroup bridges at the edge of the access point coverage area might lose IP connectivity.

8.2.5 Directional Antenna

802.11 protocols are a LAN based protocol. If you want to connect on the road, a more appropriate, and usually far more expensive, solution would be to use a cell-phone modem, using a technology such as GPRS. There are other technologies, but that is outside the scope of this paper.

The 2.4 GHz 802.11b/a/g protocols are, when using an omnidirectional antenna, limited to about 30m indoors and 100 m outdoors; but these are ideals and you'll find performance at these distances to be quite unsatisfactory. 802.11n has a range typically 150% that of 11b/a/g protocols. The range can be extended by using different antennas, which change the shape of the coverage volume, usually either making it into a cone (directional), or a flattened sphere (omnidirectional).

Notes

Directional Links

Directional antennas are all the rage in networking applications where you want to hook up branches of your network that are not in the same building. For instance, wireless links could be used to cheaply connect sites in a Metropolitan Area Network; running cable through streets can be very expensive. Alternatively, you could connect sites using a Virtual Private Network (VPN) over the Internet or a "leased line" from an telecommunications provider.

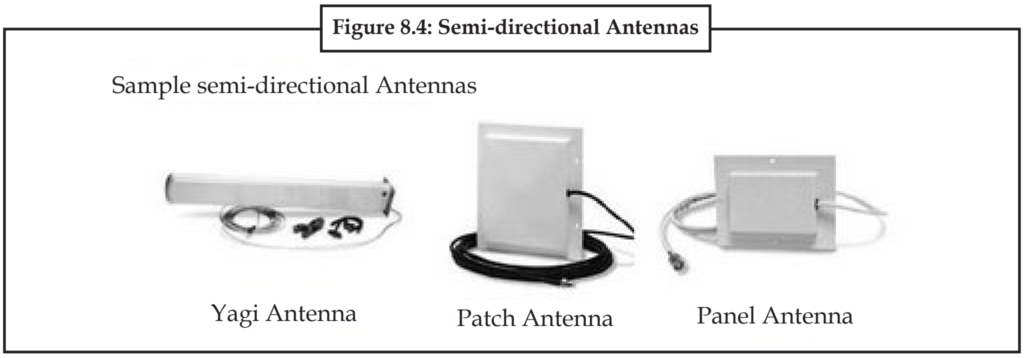
Wireless provides a cheap solution but is considerably more difficult to troubleshoot. Consider trying to move a building out of the way to see if the link quality improves. It is this reliability issue that may rule out wireless for primary links, but still be useful as a backup or transient link.

Did u know? There are systems other than those in the 802.11 suite of protocols that are designed for high-speed point-to-point wireless networking. 802.16 (WiMax) is a Metropolitan Area Networking (MAN) standard designed for point-to-point applications at a speed of up to 280Mbps. There are also laser-based point-to-point networking technologies, but I won't go into those here.

8.2.6 Semi-directional

Semi-directional antennas come in many different styles and shapes. Some semidirectional antennas types frequently used with wireless LANs are Patch, Panel, and Yagi (pronounced "YAH-gee") antennas. All of these antennas are generally flat and designed for wall mounting. Each type has different coverage characteristics. Figure 8.4 shows some examples of semi-directional antennas.

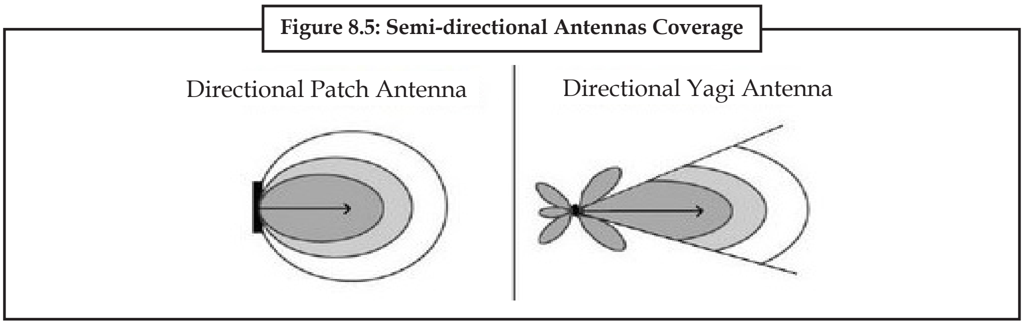
Figure 8.4: Semi-directional Antennas



Source: http://docstore.mik.ua/univercd/cc/td/doc/product/access/mar_3200/wlsnotes/cfwlsmod.htm#wp1012118

These antennas direct the energy from the transmitter significantly more in one particular direction rather than the uniform, circular pattern that is common with the omnidirectional antenna. Semi-directional antennas often radiate in a hemispherical or cylindrical coverage pattern as can be seen in Figure 8.5.

Figure 8.5: Semi-directional Antennas Coverage

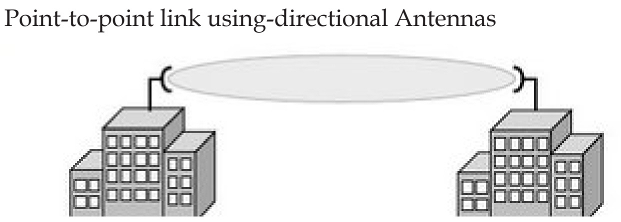


Source: http://docstore.mik.ua/univercd/cc/td/doc/product/access/mar_3200/wlsnotes/cfwlsmod.htm#wp1012118

Notes

Usage Semi-directional antennas are ideally suited for short and medium range bridging. For example, two office buildings that are across the street from one another and need to share a network connection would be a good scenario in which to implement semidirectional antennas. In a large indoor space, if the transmitter must be located in the corner or at the end of a building, a corridor, or a large room, a semi-directional antenna would be a good choice to provide the proper coverage. Figure 8.6 illustrates a link between two buildings using semi-directional antennas.

Figure 8.6: Two Buildings Using Semi-directional Antennas



Source: http://docstore.mik.ua/univercd/cc/td/doc/product/access/mar_3200/wlsnotes/cfwlsmod.htm#wp1012118

Many times, during an indoor site survey, engineers will constantly be thinking of how to best locate omnidirectional antennas. In some cases, semi-directional antennas provide such long-range coverage that they may eliminate the need for multiple access points in a building.

Example: In a long hallway, several access points with omni antennas may be used or perhaps only one or two access points with properly placed semi-directional antennas – saving the customer a significant amount of money.

In some cases, semi directional antennas have back and side lobes that, if used effectively, may further reduce the need for additional access points.

8.2.7 Highly Directional Antenna

Highly directional antennas are of two kinds, the grid style seen on top of television sets and the dish-shaped ones commonly used to receive satellite TV stations. A highly directional antenna offers a number of advantages over the other two types, which are omnidirectional and semi-directional antennas. As its name suggests, the design of the highly directional antenna allows it to hone in on one direction more efficiently

Types of Highly Directional Antennas

Grid antennas are flat with slightly curved edges. They look rather like barbecue grills with a device in a central point to collect the signals as they are relayed off a mesh of bars which make up the grid. Dish antennas are more properly known as parabolic antennas, from their inverted-bowl shape. They work by concentrating all the signals into a centre point, usually a raised receiver or transmitter located a distance above the surface of the bowl, which is the point where the signal is at its strongest.

How Highly Directional Antennas Work?

To explain how this kind of antenna offers better reception or transmission, imagine one hand cupped around one of your ears and pointed in one direction, while the other ear is covered by the other hand. You have in effect transformed yourself into something similar to a highly directional antenna. Sounds from the direction at the open end of the cupped hand reach the ear more loudly and more clearly, while noises from the direction of the blocked ear are muted or inaudible. This is how a highly directional antenna works.

Advantages of Highly Directional Antennas

A highly directional antenna improves the signal reception because it is pointed at the origin of the signal. Multi- and omnidirectional antennas pick up all signals from all directions, resulting in too many incoming signals and a weaker signal from the direction of choice. Highly directional antennas also "ignore" signals coming from places other than the one they are directed to, which cuts down the interference with a chosen signal. Another advantage these antennas offer is the ability to change the focus of the receiver to another direction. For example, when switching channels on a TV set, the grid aerial, or antenna, is moved around to get the best reception or signal. To get the best signal from any highly directional antenna, it is recommended to mount it as high as possible on a given building. This cuts down the chances of signals being blocked by tall buildings and landscape features such as trees, hills and mountains.

8.2.8 Polarization

Polarization (or Polarisation for our British friends) is one of the fundamental characteristics of any antenna. First we'll need to understand polarization of plane waves, then we'll walk through the main types of antenna polarization.

Now that we are aware of the polarization of plane-wave EM fields, antenna polarization is straightforward to define.

The polarization of an antenna is the polarization of the radiated fields produced by an antenna, evaluated in the far field. Hence, antennas are often classified as "Linearly Polarized" or a "Right Hand Circularly Polarized Antenna".

This simple concept is important for antenna to antenna communication. First, a horizontally polarized antenna will not communicate with a vertically polarized antenna. Due to the reciprocity theorem, antennas transmit and receive in exactly the same manner. Hence, a vertically polarized antenna transmits and receives vertically polarized fields. Consequently, if a horizontally polarized antenna is trying to communicate with a vertically polarized antenna, there will be no reception.

In general, for two linearly polarized antennas that are rotated from each other by an angle ϕ, the power loss due to this polarization mismatch will be described by the Polarization Loss Factor (PLF):

$$PLF = \cos^2\phi.$$

Hence, if both antennas have the same polarization, the angle between their radiated E-fields is zero and there is no power loss due to polarization mismatch. If one antenna is vertically polarized and the other is horizontally polarized, the angle is 90 degrees and no power will be transferred.

As a side note, this explains why moving the cell phone on your head to a different angle can sometimes increase reception. Cell phone antennas are often linearly polarized, so rotating the phone can often match the polarization of the phone and thus increase reception.

Circular polarization is a desirable characteristic for many antennas. Two antennas that are both circularly polarized do not suffer signal loss due to polarization mismatch. Antennas used in GPS systems are Right Hand Circularly Polarized.

Suppose now that a linearly polarized antenna is trying to receive a circularly polarized wave. Equivalently, suppose a circularly polarized antenna is trying to receive a linearly polarized wave. What is the resulting Polarization Loss Factor?

Recall that circular polarization is really two orthongal linear polarized waves 90 degrees out of phase. Hence, a linearly polarized (LP) antenna will simply pick up the in-phase component of the circularly polarized (CP) wave. As a result, the LP antenna will have a polarization mismatch loss of 0.5 (–3dB), no matter what the angle the LP antenna is rotated to. Therefore:

$$PLF \text{ (linear to circular)} = 0.5 = -3 \text{ dB}.$$

⚠ *Caution* The Polarization Loss Factor is sometimes referred to as polarization efficiency, antenna mismatch factor, or antenna receiving factor. All of these names refer to the same concept.

Self Assessment

Fill in the blanks:

1. .... enables you to access the Internet and multimedia streaming services via a wireless region area network.
2. The most well-known wireless networking technology is ....
3. The first WiMAX standard ...., was created to administrate the interoperability of all devices working between 10 and 66 GHz.
4. A network .... can connect wired devices to a wireless network.
5. .... can either be used to add wireless capabilities to a non-wireless router or improve the speed and range of an existing wireless network.
6. Wireless Bridging is used to connect two .... segments via a wireless link.
7. A wireless .... bridge allows the connection of devices on a wired Ethernet network to a wireless network.
8. Usage Semi-directional antennas are ideally suited for short and medium range ....
9. A highly .... antenna offers a number of advantages over the other two types, which are omnidirectional and semi-directional antennas.
10. Two antennas that are both circularly .... do not suffer signal loss due to polarization mismatch.

Case Study **WMAN Implementations in India**

Network Magazine – Issue of September 2002

Pravara Village IT Project (PRAGATI) is a classic example of how new technology can narrow the digital divide. Thanks to this project the rural communities of Ahmednagar district in Maharashtra are able to compete with their urban counterparts…wirelessly by Akhtar Pasha.

Promoted by National Informatics Centre (NIC), Delhi; the PRAGATI project aims to connect a hundred villages in Ahmednagar covering a population of more than 2.5 lakh with a wireless MAN solution (WMAN). When completed, it will empower the rural population and improve their quality of life. The seven lane program will help the villages in establishing local IT centres, dissemination of information regarding government schemes, marketing of agricultural products, healthcare, education, agro processing and economic development.

Contd...

Notes

Convergent Communications was selected for implementing the wireless solution as they had executed most of the NIC's projects in the past. After initial talks with Pravara Group, NIC and Indian Space Research Organization (ISRO), the project was kicked off in 1999. It was executed in two phases. In Phase I, Convergent connected 13 sites using a WMAN. Institutions were networked and connected to the Internet using a 64 Kbps VSAT connection. During Phase II, the wireless solution was extended to six other remote sites—Shirdi, Satral, Kolhar, Rahata, Babhleshwar and Loni. The remote sites use an 11 Mbps pipe shared between six locations.

The project is expected to bring a host of benefits to the farming community. The villagers can communicate with agricultural experts at Krishi Vigyan Kendra (a knowledge centre for farmers) and gain knowledge on better agriculture methods and storing and packing their products. The wireless solution will also be useful in tele-medicine and keep abreast with new government schemes.

Infrastructure Blues

Arun Nale, System Administrator, Shirdi Sai Rural Institute, said, "There was no proper telecom infrastructure. A leased line was not feasible as most of the electromechanical exchanges did not support data transmission. Lack of proper roads created hurdles in transportation of equipment during Phase I.

In addition to this, there was a hillock in Loni (Lontek) because of which there was no clear Line of Sight (LOS) and the RF network required clear LOS.

The institutes like Pharmacy College, ITI and Home Science Institute were not connected. The wireless RF towers were installed by Convergent in a record time of three days at ten locations."

Technically the range of the RF specified by Convergent was for a 5 km radius. Since this proved insufficient for connecting faraway towns like Shirdi and Rahata that were 19 kms from the hub, custom enclosures were designed to boost the range of the transmitters.

WLAN for WMAN

Chidambara, Consultant-Wireless & Education, Convergent Communications (India) Pvt. Ltd., said, "The products which were available that time were typically used in a WLAN solution. To make it work in a WMAN was a technical challenge. We developed and manufactured certain products in-house in Bangalore like the accessories—antennas, RF amplifiers, lightning arrestors, power dividers and weather-proof outdoor housing enclosures. Lucent's Wireless LAN bridges and wireless NICs were the core products that were used in the implementation. The reason why we chose to implement WMAN was because Pravaranagar does not have basic telephone infrastructure and getting a leased line was not only difficult during those days but also expensive. With WMAN in place Pravaranagar has dedicated 2 Mbps connectivity."

People Behind the Movement

PRAGATI began four years back. Shri Balasaheb Vikhe Patil, Minister of Heavy Industries Government of India and Dr. Y.K.Alagh, M.P & former Minister for Science & Technology, Government of India, took a personal interest in the project. They visited ISRO to assess the possibility of getting their interactive technology in 1999. Then they had a series of discussions with then Director General, Dr. N. Seshagiri, of National Informatics Centre (NIC), Delhi.

The final decision to assign the project to NIC was taken in June 1999. The target date for the completion of Phase I was set as 15th August 1999 and it took six weeks to complete this phase.

Contd...

Building WMAN-Phase I

First, a suitably high location—Rural Polytechnic for Women—was identified. The VSAT was installed by the NIC engineers and was connected to a typical Windows NT setup of Primary Domain Controller (PDC) and Backup Domain Controller (BDC). During Phase I, 13 sites were networked including schools, professional colleges, Pravara Medical Trust hospital, Pravara Cooperative Bank, Krishi Vigyan Kendra and Padmashri Dr. Vitthalrao Vikhe Patil Sahakari Sakhar Karkhana (sugar factory). These institutions were then connected to the Intranet using a 64 Kbps FTDMA VSAT at the Rural Polytechnic for Women. RF towers at 11 other institutions with clear line of sight with the main hub were constructed. At the remote sites 16 Pentium II PCs from Wipro were used. The wireless network was connected through Avaya Access Points to a hub and the PDC and BDC were also connected to the same hub.

With this, all the institutions have Internet access (for browsing and also sending and receiving mail) and can communicate amongst themselves. Within each institution, there can be any number of computers connected through a cable network and all these computers can also access the Internet and communicate with PCs in other institutions.

The equipment used in phase I are 64 KBPS FTDMA VSAT- Gilat with Sky surfer accessories, RF Access Point-WavePOINT-II_99UT12206350, Wireless Cards - 2 Mbps Lucent's Wavelan Cards, 10 Mbps NICs, and 10 Mbps Hubs.

"Communication has become faster and more efficient. Extensive computer training at all levels in Marathi and data input services have been planned to ensure that the facilities are utilized by the target population," says Nale. The test run of the system was taken on August 14th 1999. It went live on Independence Day 1999 and all centres were declared operational.

Phase II

In January 2000, the management of Pravara Group decided to upgrade the 64 Kbps FTDMA VSAT to a 256 Kbps high-speed SCPC VSAT in order to extend the Internet to six other remote sites located in Shirdi, Satral, Kolhar, Rahata, Babhleshwar and Loni. The work began on June 2001. NABARD sponsored six village IT centres to the tune of ₹15 lakh.

Installation of the SCPC VSAT lead to faster communication, browsing and video-conferencing with other locations. An IBM Netfinity server is used for proxy and caching services while an xSeries200 server is used as the mail server (pravara.ren.nic.in). Other products used in Phase II are – Cisco 2600 series router with 16 ASYNC ports, RF Access Point - Orinoco Outdoor routers, Wireless Cards – 11 Mbps Lucent's Wavelan Cards, 10/100 Mbps NICs and 10/100 Mbps Switches.

Benefits of the Implementation

The advantages of providing a wireless MAN in a setting like Pravara for different population segments are many.

Linking all high schools in around 50 villages within a radius of 10 km lets teachers and staff stay in touch with the HO of their Education Society. This helps them introduce modern methods of teaching, including computer-based learning (virtual school) at convenient timings for children who have to work during the day. Students from professional colleges can acquire knowledge using the Internet and it will help them find new jobs.

Farmers can communicate with the agricultural experts at the Krishi Vigyan Kendra and learn new farming techniques as well as better ways of storing and packing their products for marketing.

Contd...

Health care professionals at the villages can consult specialists at the Medical College and Hospital thereby providing specialized treatment, especially during emergencies, at people's doorsteps.

Information about government programs for the welfare of the people can be made available to the people and they can interact with the concerned government official right from their village. This will particularly benefit rural women. The villagers can interact with the sugar factory as well as with the Pravara Cooperative Bank saving time in the process.

Going forward, the Pravara group is planning to connect at least seven more villages using RF and 15 through dial-up by the end of 2002. The ultimate goal is to connect 100 villages through PRAGATI.

Questions:

1. Discuss the use of PRAGATI project in helping the villagers.
2. Discuss the hurdles faced by NIC in building WMAN.

Source: http://www.convergentindia.com/wl-case-wman.asp

8.3 Summary

- A metropolitan area network (MAN) is a computer network in which two or more computers or communicating devices or networks which are geographically separated but in same metropolitan city and are connected to each other are said to be connected on MAN.
- Wireless Metropolitan Area Network (WMAN) enables you to access the Internet and multimedia streaming services via a wireless region area network (WRAN).
- These networks provide a very fast data speed compared with the data rates of mobile telecommunication technology as well as other wireless network, and their range is also extensive.
- WiMAX works with radio wave for transmission and microwaves for reception in frequencies between 2,3 and 3,5 GHz.
- The first WiMAX standard IEEE 802.16, was created to administrate the interoperability of all devices working between 10 and 66 GHz.
- It will allow, as WiFI does, receive and transmit encrypted information among devices that have the technology.

8.4 Keywords

Highly directional antenna: It offers a number of advantages over the other two types, which are omnidirectional and semi-directional antennas.

Metropolitan area network (MAN): MAN is a computer network in which two or more computers or communicating devices or networks which are geographically separated but in same metropolitan city and are connected to each other are said to be connected on MAN.

Polarization: Polarization is one of the fundamental characteristics of any antenna.

Wireless bridge: Wireless bridge is a hardware component used to connect two or more network segments (lans or parts of a LAN) which are physically and logically (by protocol) separated.

8.5 Review Questions

1. Discuss the wireless Man.
2. Explain the major issues with wireless networks.
3. Discuss wireless bridge.
4. What do you mean by directional antenna?
5. How highly directional antennas work?
6. What are the advantages of highly directional antennas?
7. Describe the concept of polarization.

Answers: Self Assessment

1. Wireless Metropolitan Area Network (WMAN)
2. WiMAX
3. IEEE 802.16
4. Bridge
5. Access points
6. LAN
7. Ethernet
8. Bridging
9. Directional
10. Polarized

8.6 Further Readings

Books

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

John Ross, *Introduction to wireless networks.*

Vijay Garg, *Wireless Communications & Networking.*

Theodore S. Rappaport, *Wireless Communications: Principles and Practice.*

Online links

http://grouper.ieee.org/groups/802/16/

http://www.wisegeek.com/what-is-wirelessman.htm

http://www.sis.pitt.edu/~dtipper/2700/2700_Slides17_2.pdf

Notes

Unit 9: Wireless MAN Systems

CONTENTS

Objectives

Introduction

9.1 Metropolitan Area Network (MAN)

9.1.1 Types of MAN Technologies

9.1.2 Advantages of MAN

9.2 Point-to-point Wireless Networks

9.3 Cable Networking of Point-to-point Wireless Network

9.4 Point-to-multipoint System

9.4.1 Point-to-multipoint Bridging

9.5 Packet Radio Networks

9.6 Summary

9.7 Keywords

9.8 Review Questions

9.9 Further Readings

Objectives

After studying this unit, you will be able to:

- Discuss the metropolitan area network (MAN)
- Explain the point-to-point wireless networks
- Describe the cable networking of point-to-point wireless network
- Explain the points-to-multipoint system
- Discuss the packet radio networks

Introduction

A metropolitan area network (MAN) is a computer network in which two or more computers or communicating devices or networks which are geographically separated but in same metropolitan city and are connected to each other are said to be connected on MAN. The limits of Metropolitan cities are determined by local municipal corporations and we cannot define them. Hence, the bigger the Metropolitan city the bigger the MAN, smaller a metro city smaller the MAN.

The IEEE 802-2002 standard describes a MAN as being:

A MAN is epitomised for a larger geographical area than a LAN, ranging from several blocks of buildings to entire cities. MANs can also depend on communications channels of moderate-to-high data rates. A MAN might be owned and operated by a single organization, but it usually will be used by many individuals and organizations. MANs might also be owned and operated as public utilities. They will often provide means for inter-networking of local networks.

9.1 Metropolitan Area Network (MAN)

Authors Kenneth C. Laudan and Jane P. Laudon (2001) of Management Information Systems: Managing the Digital Firm 10th ed. define a metropolitan area network as:

A Metropolitan Area Network (MAN) is a large computer network that spans a metropolitan area or campus. Its geographic scope falls between a WAN and LAN. MANs provide Internet connectivity for LANs in a metropolitan region, and connect them to wider area networks like the Internet.

9.1.1 Types of MAN Technologies

Some technologies used for this purpose are Asynchronous Transfer Mode (ATM), FDDI, and SMDS. These technologies are in the process of being displaced by Ethernet-based connections (e.g., Metro Ethernet) in most areas. MAN links between local area networks have been built without cables using either microwave, radio, or infrared laser links. Most companies rent or lease circuits from common carriers because laying long stretches of cable can be expensive.

DQDB, Distributed-queue dual-bus, is the metropolitan area network standard for data communication. It is specified in the IEEE 802.6 standard. Using DQDB, networks can be up to 20 miles (30 km) long and operate at speeds of 34 to 155 Mbit/s.

- ***Asynchronous Transfer Mode (ATM):*** ATM is, according to the ATM Forum, "a telecommunications concept defined by ANSI and ITU (formerly CCITT) standards for carriage of a complete range of user traffic, including voice, data, and video signals," and is designed to unify telecommunication and computer networks. It uses asynchronous time-division multiplexing, and it encodes data into small, fixed-sized cells. This differs from approaches such as the Internet Protocol or Ethernet that use variable sized packets or frames. ATM provides data link layer services that run over a wide range of OSI physical layer links. ATM has functional similarity with both circuit switched networking and small packet switched networking. It was designed for a network that must handle both traditional high-throughput data traffic (e.g., file transfers), and real-time, low-latency content such as voice and video. ATM uses a connection-oriented model in which a virtual circuit must be established between two endpoints before the actual data exchange begins. ATM is a core protocol used over the SONET/SDH backbone of the public switched telephone network (PSTN) and Integrated Services Digital Network (ISDN), but its use is declining in favour of all IP.

  ATM was developed to meet the needs of the Broadband Integrated Services Digital Network, as defined in the late 1980s.

- ***Fibre Distributed Data Interface (FDDI):*** FDDI provides a 100 Mbit/s optical standard for data transmission in local area network that can extend in range up to 200 kilometers (120 mi). Although FDDI logical topology is a ring-based token network, it does not use the IEEE 802.5 token ring protocol as its basis; instead, its protocol is derived from the IEEE 802.4 token bus timed token protocol. In addition to covering large geographical areas, FDDI local area networks can support thousands of users. As a standard underlying medium it uses optical fibre, although it can use copper cable, in which case it may be referred to as CDDI(Copper Distributed Data Interface), standardized by ANSI as TP-PMD (Twisted-Pair Physical Medium-Dependent), also referred to as TP-DDI (Twisted-Pair Distributed Data Interface). FDDI offers both a Dual-Attached Station (DAS), counter-rotating token ring topology and a Single-Attached Station (SAS), token bus passing ring topology.

  FDDI was considered an attractive campus backbone technology in the early to mid 1990s since existing Ethernet networks only offered 10 Mbit/s transfer speeds and Token Ring networks only offered 4 Mbit/s or 16 Mbit/s speeds. Thus it was the preferred choice of that era for a high-speed backbone, but FDDI has since been effectively obsolesced by fast Ethernet which offered the same 100 Mbit/s speeds, but at a much lower cost and, since 1998, by Gigabit Ethernet due to its speed, and even lower cost, and ubiquity.

FDDI, as a product of American National Standards Institute X3T9.5 (now X3T12), conforms to the Open Systems Interconnection (OSI) model of functional layering of LANs using other protocols. FDDI-II, a version of FDDI, adds the capability to add circuit-switched service to the network so that it can also handle voice and video signals. Work has started to connect FDDI networks to the developing Synchronous Optical Network (SONET).

A FDDI network contains two rings, one as a secondary backup in case the primary ring fails. The primary ring offers up to 100 Mbit/s capacity. When a network has no requirement for the secondary ring to do backup, it can also carry data, extending capacity to 200 Mbit/s. The single ring can extend the maximum distance; a dual ring can extend 100 km (62 mi). FDDI has a larger maximum-frame size (4,352 bytes) than standard 100 Mbit/s Ethernet which only supports a maximum-frame size of 1,500 bytes, allowing better throughput.

Designers normally construct FDDI rings in the form of a "dual ring of trees" (see network topology). A small number of devices (typically infrastructure devices such as routers and concentrators rather than host computers) connect to both rings – hence the term "dual-attached". Host computers then connect as single-attached devices to the routers or concentrators. The dual ring in its most degenerate form simply collapses into a single device. Typically, a computer-room contains the whole dual ring, although some implementations have deployed FDDI as a Metropolitan area network.

- ***Switched Multi-megabit Data Service (SMDS):*** SMDS was a connectionless service used to connect LANs, MANs and WANs to exchange data, in early 1990s. In Europe, the service was known as Connectionless Broadband Data Service (CBDS).

  SMDS was specified by Bellcore, and was based on the IEEE 802.6 metropolitan area network (MAN) standard, as implemented by Bellcore, and used cell relay transport, Distributed Queue Dual Bus layer-2 switching arbitrator, and standard SONET[3] or G.703 as access interfaces.

  Its a switching service that provides data transmission in the range between 1.544 Mbit/s to 45 Mbit/s. SMDS was developed by Bellcore as an interim service until Asynchronous Transfer Mode matured. In the mid-1990s, SMDS was replaced, largely by Frame Relay.

Did u know? SMDS was notable for its initial introduction of the 53-byte cell and cell switching approaches, as well as the method of inserting 53-byte cells onto G.703 and SONET.

9.1.2 Advantages of MAN

MAN can cover a wider area than a LAN. MAN networks are usually operated at airports, or a combination of several pieces at a local school. By running a large network connectedness, information can be disseminated more widely, rapidly and significantly. Public libraries and government agencies typically use a MAN.

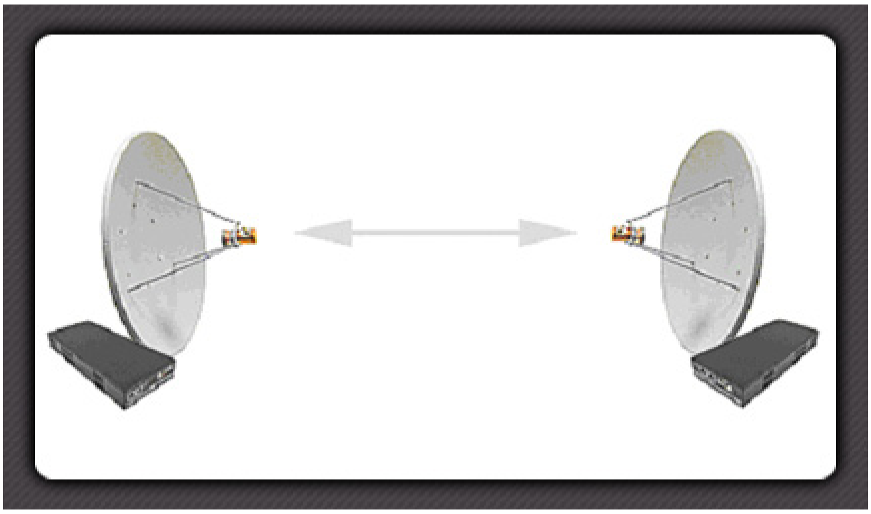
Disadvantages MAN: MAN will only apply if the personal computer or a terminal can compete. If a personal computer is used as a terminal, move the file (file transfer software) allows users to retrieve files (downloaded) from the hose or hose to deliver the data (upload). Download files means open and retrieve data from a personal computer to another and deliver the data to the computer pertaining requested by the user.

Notes

9.2 Point-to-point Wireless Networks

Point to Point links are an excellent way how to make connections between two sites and achieve high data transfer speeds. This is an ideal way how to connect two offices. Also these types of wireless links are very useful if you need to create backbone link from some distant radio access point to your main Internet source. For creating such connections we recommend to use our 5 GHz and 2.4 GHz wireless client kits

Figure 9.1: Point to Point Network



Source: http://www.eleconinfotech.com/Wireless%20Solutions.html

9.3 Cable Networking of Point-to-point Wireless Network

Cable is the medium through which information usually moves from one network device to another. There are several types of cable which are commonly used with LANs. In some cases, a network will utilize only one type of cable, other networks will use a variety of cable types. The type of cable chosen for a network is related to the network's topology, protocol, and size. Understanding the characteristics of different types of cable and how they relate to other aspects of a network is necessary for the development of a successful network.

Point-to-point topology is the simplest of the physical layouts of network devices. Point-to-point connections mean that two devices (nodes) have a single path for data to travel between them and there is nothing that breaks up that path.

A prime example of how this topology is implemented in networking is the manner in which terminals are now connected to mainframes or mini-computers. Instead of having many cables from numerous terminals hooked into one of these computers, a device known as a terminal server allows the data from several terminals to be transmitted over a single cable. This single cable connection between the computer's front-end processor and the terminal server forms a point-to-point link. In addition, some terminal servers form point-to-point links with the individual terminals.

The point-to-point topology can be seen as one of the basic building blocks of larger, more complicated topologies. All major topologies include point-to-point connections, even if there is no wire between two devices, but some other medium instead. Satellite transmissions are considered to be point-to-point communications. Similarly, laser transmissions can also be viewed in this manner. A variant on point-to-point connections is a multipoint topology in which a single cable may split into several segments in order to connect to several devices.

Notes

⚠ *Caution* Point-to-point topology is not just limited to networking use. You should be aware that the direct connection of a PC to a printer follows a point-to-point topology. In fact, any externally connected device, including modems or hard disk drives would also fall under this classification.

Self Assessment

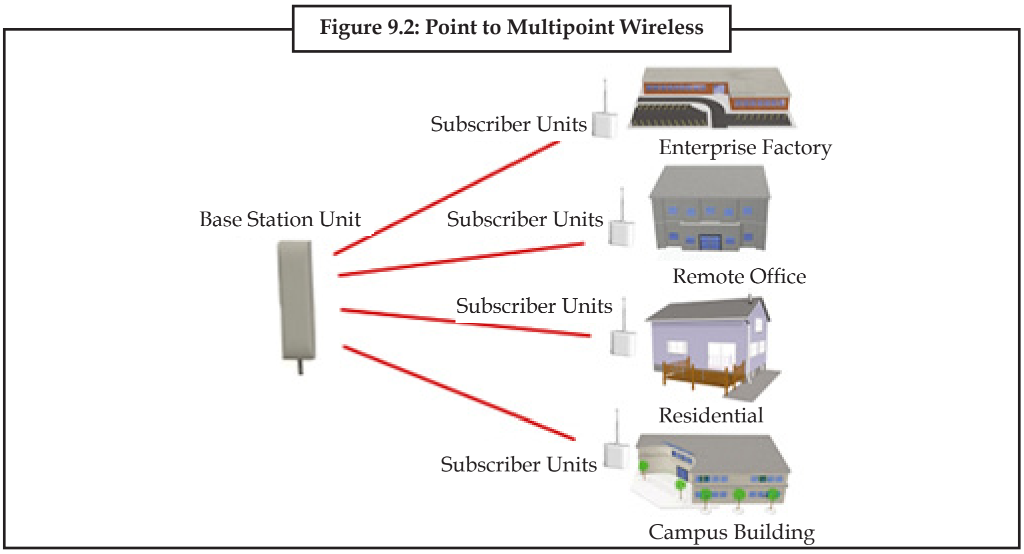
Fill in the blanks:

1. A .... is optimised for a larger geographical area than a LAN.
2. .... is the metropolitan area network standard for data communication.
3. .... provides a 100 Mbit/s optical standard for data transmission in local area network that can extend in range up to 200 kilometers (120 mi).
4. Public libraries and .... agencies typically use a MAN.
5. .... links are an excellent way how to make connections between two sites and achieve high data transfer speeds.
6. .... is the medium through which information usually moves from one network device to another.

9.4 Point-to-multipoint System

Point to multipoint wireless backhaul systems are made up of a Base Station Unit (BSU or AP) that can communicate with multiple Subscriber Units (SU's). Many systems can handle over 100 plus SU's per BSU. In most cases the BSU's provide a sector antenna beam pattern (typical is 60 degree, with some systems allowing external antenna configurations for expanding to 90 and 120 degree sector antennas). Multiple BSU's can be installed to create a 360 degree sector (like a typical cell site configuration).

Figure 9.2: Point to Multipoint Wireless



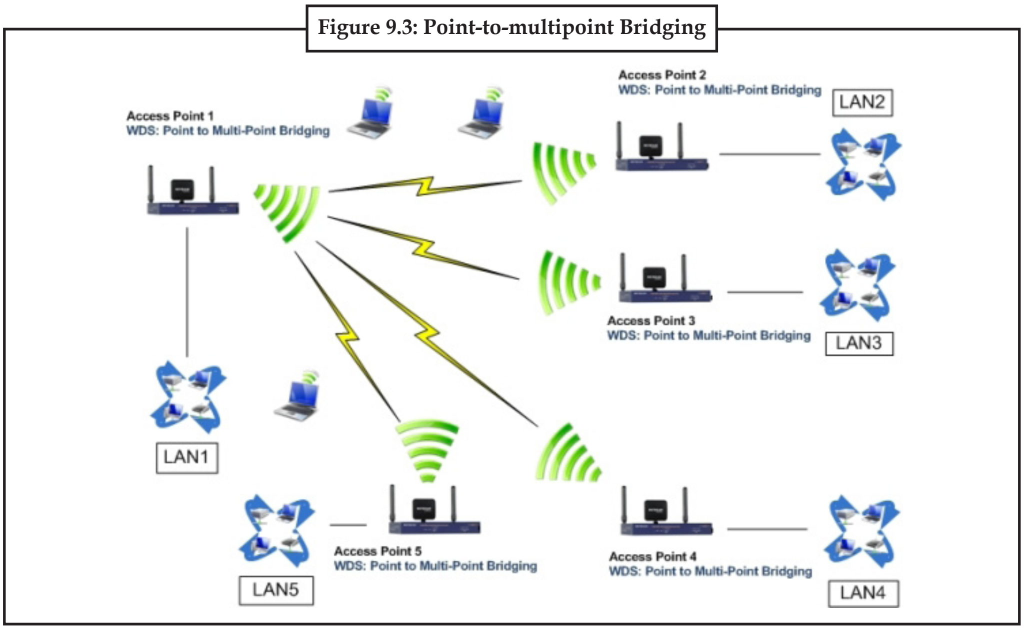
Source: http://www.aowireless.com/solutions/point-to-multipoint-wireless/

9.4.1 Point-to-multipoint Bridging

A wireless bridge is a device that allows two or more complete networks of users to transparently communicate to one another over long distances without wires. These networks can be in the same building but are normally in either adjacent buildings or with the proper antennas and line of sight bridges can even connect networks up to 30 miles apart. Wireless bridges connect to the wired network through the Ethernet port and replicate that data to a remote network bridge or access point via 802.11a/b/g wireless (Wi-Fi) protocol.

A point to Multipoint topology wirelessly connects multiple locations together allowing them to share the same network resources. The bridge at the main, central, location is called the root bridge or base station bridge and all data passing between the wireless bridge clients must pass through the root bridge first. These point-to-multipoint networks are used in wireless internet service providers (WISP), large corporate campuses, distribution facilities, school districts, public safety applications and many other. Point-to-multipoint bridging is when an access point talks directly to more than one access point:

Figure 9.3: Point-to-multipoint Bridging


Access Point 1
WDS: Point to Multi-Point Bridging
Access Point 2
WDS: Point to Multi-Point Bridging
LAN2
Access Point 3
WDS: Point to Multi-Point Bridging
LAN3
LAN1
Access Point 5
WDS: Point to Multi-Point Bridging
LAN5
Access Point 4
WDS: Point to Multi-Point Bridging
LAN4

What Do I Need to Build a Point to Point Bridge Link?

Line of sight between the two locations. You may need to install a pole or tower on your roof top in order to achieve this. A site survey is recommended before installation.

Select a Wireless Bridge: Here are some things to consider when selecting a wireless bridge.

Distance: Distance will determine what gain antenna will be required and if you need an external antenna or if an integrated antenna will be sufficient.

Wireless protocol: Do you want to use a bridge base on 802.11 standards so that you have interoperability with other bridge manufacturers or would you like something with a protocol proprietary to a particular vendor? There are some added security benefits when using a proprietary over a standard protocol.

Frequency: Do you want to use a licensed or unlicensed (2.4, 5–5.8 GHz) band?

Indoor or Outdoor: Indoor wireless bridges are less expensive but you will have to buy quite a bit of LMR-400 cable to connect to the outdoor antenna. This adds a great deal of signal loss and in the end you will need a higher gain antenna to compensate. An outdoor bridge can be placed right next to the antenna and therefore cuts down on the amount of cable you need to buy as well as the amount of signal loss.

Notes

Select a Wireless Antenna: If the bridge you selected does not already have an integrated antenna you will need to choose one now. For point to point links we suggest a directional panel, grid or solid parabolic dish antennas.

Peripherals: You will need to select the appropriate lightning arrestors and RF antenna cables to get you connected and protected.

Double it: Now double the amount of hardware you selected so that you have the identical setup on both sides.

9.5 Packet Radio Networks

Packet radio is a form of packet switching technology used to transmit digital data via radio or wireless communications links. It uses the same concepts of data transmission via Datagram that are fundamental to communications via the Internet, as opposed to the older techniques used by dedicated or switched circuits.

Packet radio is a particular digital mode of Amateur Radio ("Ham" Radio) communications which corresponds to computer telecommunications. The telephone modem is replaced by a "magic" box called a terminal node controller (TNC); the telephone is replaced by an amateur radio transceiver, and the phone system is replaced by the "free" amateur radio waves. Packet radio takes any data stream sent from a computer and sends that via radio to another amateur radio station similarly equipped.

Did u know? Packet radio is so named because it sends the data in small bursts, or packets.

What Is the History of Packet Radio?

Data packet technology was developed in the mid-1960's and was put into practical application in the ARPANET which was established in 1969. Initiated in 1970, the ALOHANET, based at the University of Hawaii, was the first large-scale packet radio project. Amateur packet radio began in Montreal, Canada in 1978, the first transmission occurring on May 31st. This was followed by the Vancouver Amateur Digital Communication Group (VADCG) development of a Terminal Node Controller (TNC) in 1980.

The current TNC standard grew from a discussion in October of 1981 at a meeting of the Tucson Chapter of the IEEE Computer Society. A week later, six of the attendees gathered and discussed the feasibility of developing a TNC that would be available to amateurs at a modest cost.

Why Packet over Other Modes?

Packet has three great advantages over other digital modes: transparency, error correction, and automatic control.

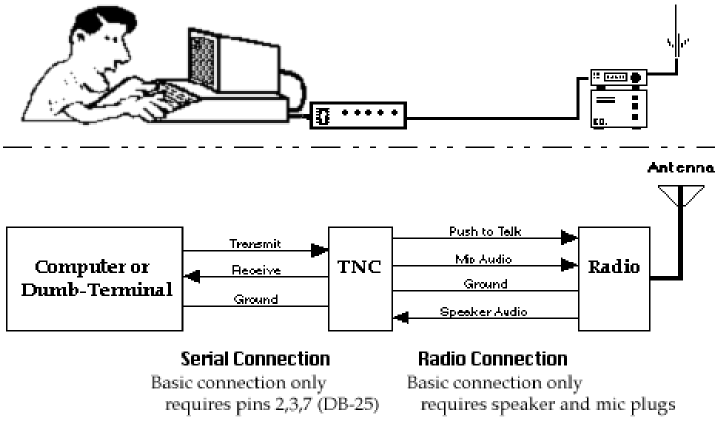
The operation of a packet station is transparent to the end user; connect to the other station, type in your message, and it is sent automatically. The terminal Node Controller (TNC) automatically divides the message into packets, keys the transmitter, and then sends the packets. While receiving packets, the TNC automatically decodes, checks for errors, and displays the received messages. Packet radio provides error free communications because of built-in error detection schemes. If a packet is received, it is checked for errors and will be displayed only if it is correct. In addition, any packet TNC can be used as a packet relay station, sometimes called a digipeater. This allows for greater range by stringing several packet stations together.

Users can connect to their friends' TNCs at any time they wish, to see if they are at home. Some TNCs even have Personal BBSs (sometimes called mailboxes) so other amateurs can leave messages for them when they are not at home. Another advantage of packet over other modes is the ability for many users to be able to use the same frequency channel simultaneously.

What Elements Make up a Packet Station?

Figure 9.4 shows an illustration of a typical station setup with a schematic diagram of a station wiring.

Figure 9.4: Station Setup


Antenna
Computer or Dumb-Terminal
Transmit
Receive
Ground
TNC
Push to Talk
Mic Audio
Ground
Speaker Audio
Radio
Serial Connection
Basic connection only requires pins 2,3,7 (DB-25)
Radio Connection
Basic connection only requires speaker and mic plugs

TNC (Terminal Node Controller)

A TNC contains a modem, a computer processor (CPU), and the associated circuitry required to convert communications between your computer (RS-232) and the packet radio protocol in use. A TNC assembles a packet from data received from the computer, computes an error check (CRC) for the packet, modulates it into audio frequencies, and puts out appropriate signals to transmit the packet over the connected radio. It also reverses the process, translating the audio that the connected radio receives into a byte stream that is then sent to the computer.

Most amateurs currently use 1200 bps (bits per second) for local VHF and UHF packet, and 300 bps for longer distance, lower bandwidth HF communication.

Notes Higher speeds are available for use in the VHF, UHF, and especially microwave region, but they often require special (not plug-and-play) hardware and drivers.

Computer or Terminal

This is the user interface. A computer running a terminal emulator program, a packet-specific program, or just a dumb terminal can be used. For computers, almost any phone modem communications program (i.e. Procomm+, Bitcom, X-Talk) can be adapted for packet use, but there are also customized packet radio programs available. A dumb terminal, while possibly the cheapest option, does have several limitations. Most dumb terminals do not allow you to scroll backwards, store information, upload, or download files.

A Radio

For 1200/2400 bps UHF/VHF packet, commonly available narrow band FM voice radios are used. For HF packet, 300 BPS data is used over single side band (SSB) modulation. For high speed packet (starting at 9600 bps), special radios or modified FM radios must be used. 1200 bps AFSK TNCs used on 2-meters (144 - 148Mhz) is the most commonly found packet radio.

Notes

What Is the Distance Limitation for Packet Radio?

Since packet radio is most commonly used at the higher radio frequencies (VHF), the range of the transmission is somewhat limited. Generally, transmission range is limited to "unobstructed line-of-sight" plus approximately 10–15%. The transmission range is influenced by the transmitter power and the type and location of the antenna, as well as the actual frequency used and the length of the antenna feed line (the cable connecting the radio to the antenna). Another factor influencing the transmission range is the existence of obstructions (hills, groups of buildings ,etc). Thus, for two-meter packet (144–148Mhz), the range could be 10 to 100 miles, depending on the specific combination of the variables mentioned above.

What Do You Mean We Can all Use the Same Channel?

Packet radio, unlike voice communications, can support multiple conversations on the same frequency at the same time. This does not mean that interference does not occur when two stations transmit at the same time, known as a collision. What 'same time' means in this sense is that multiple conversations are possible in a managed, time shared fashion. Conversations occur during the times when the other conversations are not using the channel. Packet radio uses a protocol called AX.25 to accomplish this shared channel.

AX.25 specifies channel access (ability to transmit on the channel) to be handled by CSMA (Carrier Sense Multiple Access). If you need to transmit, your TNC monitors the channel to see if someone else is transmitting. If no one else is transmitting, then the TNC keys up the radio, and sends its packet. All the other stations hear the packet and do not transmit until you are done. Unfortunately, two stations could accidentally transmit at the same time. This is called a collision. If a collision occurs, neither TNC will receive a reply back from the last packet it sent. Each TNC will wait a random amount of time and then retransmit the packet. In actuality, a more complex scheme is used to determine when the TNC transmits. See the "AX.25 Protocol Specification" for more information (ARRL, 1988).

What Is AX.25?

AX.25 (Amateur X.25) is the communications protocol used for packet radio. A protocol is a standard for two computer systems to communicate with each other, somewhat analogous to using a business format when writing a business letter. AX.25 was developed in the 1970's and based on the wired network protocol X.25. Because of the difference in the transport medium (radios vs wires) and because of different addressing schemes, X.25 was modified to suit amateur radio's needs. AX.25 includes a digipeater field to allow other stations to automatically repeat packets to extend the range of transmitters. One advantage of AX.25 is that every packet sent contains the sender's and recipient's amateur radio callsign, thus providing station identification with every transmission.

Networking and special packet protocols: This is a sample of some of the more popular networking schemes available today. By far, there are more customized networking schemes used than listed. Consult your local packet network guru for specific network information.

Are there any other protocols in use other than AX.25?

⚠

Caution AX.25 is considered the standard protocol for amateur radio use and is even recognized by many countries as a legal operation mode.

However, there are other standards. TCP/IP is used in some areas for amateur radio. Also, some networking protocols use packet formats other than AX.25. Often, special packet radio protocols are encapsulated within AX.25 packet frames. This is done to insure compliance with regulations requiring packet radio transmissions to be in the form of AX.25. However, details of AX.25 encapsulation rules vary from country to country.

Self Assessment

Fill in the blanks:

7. .... is the communications protocol used for packet radio.

8. A .... is a standard for two computer systems to communicate with each other, somewhat analogous to using a business format when writing a business letter.

9. For .... speed packet (starting at 9600 bps), special radios or modified FM radios must be used.

10. A .... contains a modem, a computer processor (CPU), and the associated circuitry required to convert communications between your computer (RS-232) and the packet radio protocol in use.

Case Study

City Deploys Municipal Wireless Network

Business Challenge

The City of Moncton, with a population of around 130,000, is situated in southeastern New Brunswick, in the heart of the Maritimes. It is one of the top ten fastest growing metropolitan areas in Canada and is known for its friendly atmosphere, rich cultural scene, and exceptional quality of life. The city is situated in southeastern New Brunswick, at the geographic centre of the Maritime Provinces. The community has the nickname "Hub City," because of its central location and also because Moncton has historically been the railway and land transportation hub for the Maritime Provinces.

The city knows that to maintain its strength in the future depends on attracting entrepreneurs and technology-based businesses. To foster its image of a technology-friendly city and enhance its attractiveness to business and citizens, the city decided to cover its downtown area with a free WiFi network. The challenge was that a free Wi-Fi network is not really free, so it had to be implemented in the most cost-saving way and at the same time be able to support citizen services. The network design also had to take into account low cost of operating the network and possible future expansion of the municipal wireless network.

Network Solution

The city chose the Cisco ® Wireless Mesh Network Solution as the basis for its municipal wireless network for several reasons. The City of Moncton already had a Cisco network in place, which could easily be extended through a wireless mesh deployment. A standard wireless network, in which each access point is directly wired back to the main network, would have meant a lot of additional cabling and installation cost. In a wireless mesh network, the network dynamically routes packets from node to node. Only a few access points (the root access points) have to be connected directly to the wired network, but the rest stay connected though wireless connections with mesh technology. Furthermore, the Cisco wireless mesh network is centrally managed through the Cisco Wireless LAN Controllers that provide insight into all wireless network components through the Wireless Control System (WCS) software.

Because it was particularly important for the City of Moncton to keep installation and future maintenance costs low, the Cisco Wireless Mesh Network provided the ideal solution.

Contd...

Notes

The Cisco Wireless Mesh Solution provides centralizing key functions, such as scalable management, configuration, and security and transparent mobility between indoor and outdoor environments. The solution can easily be expanded at any time, and is designed to support zero-configuration deployments in which the Cisco access points easily and securely join the mesh network as soon as they are installed.

"The low deployment cost of the Cisco Wireless Mesh Network made it a compelling solution," says Dan Babineau, director of information systems, City of Moncton. In addition, the scalability and interoperability of this mesh network will enable the city to expand the network cost efficiently in the future and also add additional services, applications, and upgrade to future wireless technologies. HP Canada, the integration partner for this project, determined the best placement for the Cisco access points throughout the downtown area to provide the best coverage. Most of the access points were placed on light poles, which the city owns. To avoid any impact from maintenance work on the city lighting, the access points were placed inside special mounting boxes. With good planning, the city was able to install the entire network, using its own personnel, within three days.

Business Results

As soon as the Wi-Fi network became available in the area of downtown Moncton, an area of about six city blocks, people started using the network immediately. Since the deployment was completed, uptake has been consistent with hotels, cafes, and retail shops taking advantage of the new city service. Small businesses are now able to conduct part of their day-to-day business operations via the Internet for improved customer service and operational cost savings. The Wi-Fi network, reaching into city buildings, benefits the productivity of city workers, who now can stay connected via wireless handheld devices while moving around the downtown area.

"It is exciting to see people sitting all over downtown with laptops or handhelds," says Babineau. "The free Wi-Fi was a valuable investment in our infrastructure as a technology-friendly city." Not only are business travelers now able to conduct business from hotel lobbies and public downtown areas, but tourists also can look up businesses and call up maps at their convenience. The free WiFi attracts new small businesses to downtown Moncton, and it helps the city be true to its image as a vibrant hub city, where it is fun to work and play. With the successful installation of Wi-Fi in the downtown area, the city of Moncton is now considering expanding the network to further support city and cultural services to its citizens and visitors.

Questions

1. Discuss the challenges faces by City in implementing free WiFi network.
2. Discuss the solution taken by the City of Moncton to have free WiFi network.

Source: http://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps8368/case_study_c36-468205_v1.pdf

9.6 Summary

- A metropolitan area network (MAN) is a computer network in which two or more computers or communicating devices or networks which are geographically separated but in same metropolitan city and are connected to each other are said to be connected on MAN.
- A MAN is optimised for a larger geographical area than a LAN, ranging from several blocks of buildings to entire cities. MANs can also depend on communications channels of moderate-to-high data rates.

- Some technologies used for this purpose are Asynchronous Transfer Mode (ATM), FDDI, and SMDS.
- MAN links between local area networks have been built without cables using either microwave, radio, or infra-red laser links.
- MAN can cover a wider area than a LAN. MAN networks are usually operated at airports, or a combination of several pieces at a local school.
- By running a large network connectedness, information can be disseminated more widely, rapidly and significantly.
- Public libraries and government agencies typically use a MAN.

9.7 Keywords

Asynchronous Transfer Mode (ATM): ATM is, according to the ATM Forum, "a telecommunications concept defined by ANSI and ITU (formerly CCITT) standards for carriage of a complete range of user traffic, including voice, data, and video signals," and is designed to unify telecommunication and computer networks.

Distributed-queue dual-bus: Distributed-queue dual-bus is the metropolitan area network standard for data communication. It is specified in the IEEE 802.6 standard.

Fibre Distributed Data Interface (FDDI): FDDI provides a 100 Mbit/s optical standard for data transmission in local area network that can extend in range up to 200 kilometers (120 mi).

Metropolitan area network (MAN): MAN is a computer network in which two or more computers or communicating devices or networks which are geographically separated but in same metropolitan city and are connected to each other are said to be connected on MAN.

Packet radio: Packet radio is a form of packet switching technology used to transmit digital data via radio or wireless communications links.

Switched Multi-megabit Data Service: Switched Multi-megabit Data Service was a connectionless service used to connect LANs, MANs and WANs to exchange data, in early 1990s.

9.8 Review Questions

1. Describe the cable networking of point-to-point wireless network.
2. Discuss the packet radio networks.
3. Explain the concept of metropolitan area network (MAN).
4. Describe points-to-multipoint system.
5. Explain the point-to-point wireless networks.

Answers: Self Assessment

1. MAN
2. Distributed-queue dual-bus
3. Fibre Distributed Data Interface (FDDI)
4. Government
5. Point to Point
6. Cable
7. AX.25 (Amateur X.25)
8. Protocol
9. High
10. TNC

Notes

9.9 Further Readings

Books

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

John Ross, *Introduction to wireless networks.*

Vijay Garg, *Wireless Communications & Networking.*

Theodore S. Rappaport, *Wireless Communications: Principles and Practice.*

Online links

http://www.tapr.org/pr_intro.html

http://bnrg.eecs.berkeley.edu/~randy/Courses/CS294.S96/PRnet.intro.pdf

http://lca.ceid.upatras.gr/~kirousis/publications/j15.pdf

Unit 10: Wireless MAN Technologies

CONTENTS

Objectives

Introduction

10.1 IEEE 802.11 and Wi-Fi

10.1.1 Wi-Fi Standards

10.1.2 Adaptive Modulation

10.2 IEEE 802.16: Broadband Wireless MAN Standard (WiMAX)

10.2.1 WiMAX and the IEEE 802.16a PHY Layer

10.2.2 IEEE 802.16a MAC Layer

10.3 Summary

10.4 Keywords

10.5 Review Questions

10.6 Further Readings

Objectives

After studying this unit, you will be able to:

- Understand IEEE 802.11 and Wi-Fi
- Define IEEE 802.16 and its purpose

Introduction

IEEE 802.11 is a set of physical layer standards for implementing wireless local area network (WLAN) computer communication in the 2.4, 3.6, 5 and 60 GHz frequency bands. They are created and maintained by the IEEE LAN/MANStandards Committee (IEEE 802). The base version of the standard was released in 1997 and has had subsequent amendments. These standards provide the basis for wireless network products using the Wi-Fi brand.

10.1 IEEE 802.11 and Wi-Fi

The 802.11 family consist of a series of half-duplex over-the-air modulation techniques that use the same basic protocol. The most popular are those defined by the 802.11b and 802.11g protocols, which are amendments to the original standard. 802.11-1997 was the first wireless networking standard, but 802.11a was the first widely accepted one, followed by 802.11b and 802.11g. 802.11n is a new multi-streaming modulation technique. Other standards in the family (c–f, h, j) are service amendments and extensions or corrections to the previous specifications.

802.11b and 802.11g use the 2.4 GHz ISM band, operating in the United States under Part 15 of the US Federal Communications Commission Rules and Regulations. Because of this choice of frequency band, 802.11b and g equipment may occasionally suffer interference from microwave ovens, cordless telephones and Bluetooth devices. 802.11b and 802.11g control their interference and susceptibility to interference by using direct-sequence spread spectrum (DSSS) and orthogonal frequency-division multiplexing (OFDM) signalling methods, respectively. 802.11a uses the 5 GHz U-NII band, which, for much of the world, offers at least 23 non-overlapping channels rather than the 2.4 GHz ISM frequency band, where adjacent channels overlap – see list of WLAN channels. Better or worse performance with higher or lower frequencies (channels) may be realized, depending on the environment.

The segment of the radio frequency spectrum used by 802.11 varies between countries. In the US, 802.11a and 802.11g devices may be operated without a license, as allowed in Part 15 of the FCC Rules and Regulations. Frequencies used by channels one through six of 802.11b and 802.11g fall within the 2.4 GHz amateur radio band. Licensed amateur radio operators may operate 802.11b/g devices under Part 97 of the FCC Rules and Regulations, allowing increased power output but not commercial content or encryption.

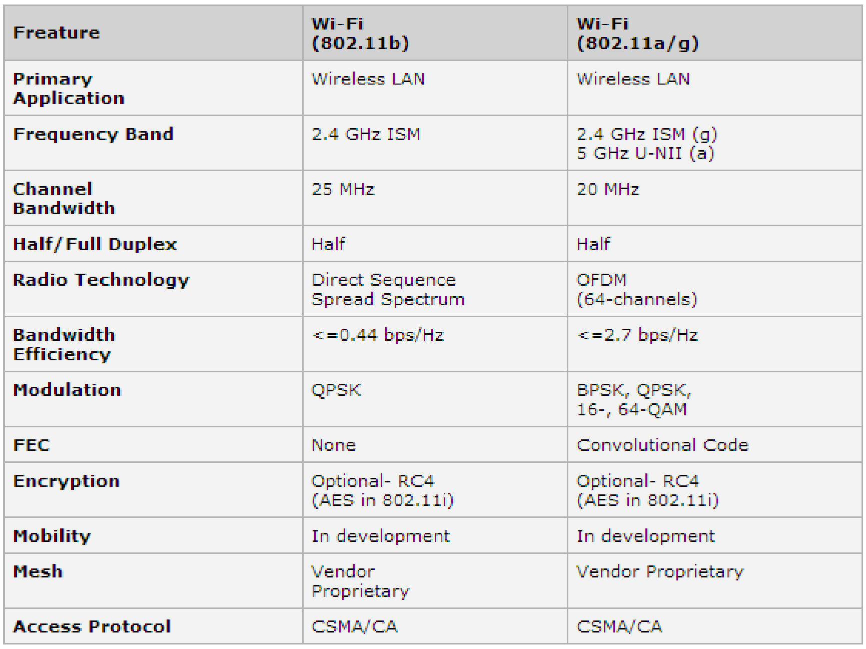
10.1.1 Wi-Fi Standards

The 802.11 standard is defined through several specifications of WLANs. It defines an over-the-air interface between a wireless client and a base station or between two wireless clients.

There are several specifications in the 802.11 family:

- *802.11:* This pertains to wireless LANs and provides 1- or 2-Mbps transmission in the 2.4-GHz band using either frequency-hopping spread spectrum (FHSS) or direct-sequence spread spectrum (DSSS).
- *802.11a:* This is an extension to 802.11 that pertains to wireless LANs and goes as fast as 54 Mbps in the 5-GHz band. 802.11a employs the orthogonal frequency division multiplexing (OFDM) encoding scheme as opposed to either FHSS or DSSS.
- *802.11b:* The 802.11 high rate Wi-Fi is an extension to 802.11 that pertains to wireless LANs and yields a connection as fast as 11 Mbps transmission (with a fallback to 5.5, 2, and 1 Mbps depending on strength of signal) in the 2.4-GHz band. The 802.11b specification uses only DSSS. Note that 802.11b was actually an amendment to the original 802.11 standard added in 1999 to permit wireless functionality to be analogous to hard-wired Ethernet connections.
- *802.11g:* This pertains to wireless LANs and provides 20+ Mbps in the 2.4-GHz band.

Here is the technical camparison between the three major Wi-Fi standards.



Freature	Wi-Fi (802.11b)	Wi-Fi (802.11a/g)
Primary Application	Wireless LAN	Wireless LAN
Frequency Band	2.4 GHz ISM	2.4 GHz ISM (g) 5 GHz U-NII (a)
Channel Bandwidth	25 MHz	20 MHz
Half/Full Duplex	Half	Half
Radio Technology	Direct Sequence Spread Spectrum	OFDM (64-channels)
Bandwidth Efficiency	<=0.44 bps/Hz	<=2.7 bps/Hz
Modulation	QPSK	BPSK, QPSK, 16-, 64-QAM
FEC	None	Convolutional Code
Encryption	Optional- RC4 (AES in 802.11i)	Optional- RC4 (AES in 802.11i)
Mobility	In development	In development
Mesh	Vendor Proprietary	Vendor Proprietary
Access Protocol	CSMA/CA	CSMA/CA

Source: http://www.tutorialspoint.com/wi-fi/wifi_ieee_standards.htm

IEEE 802.11 wireless LANs use a media access control protocol called Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). While the name is similar to Ethernet.s Carrier Sense Multiple Access with Collision Detection (CSMA/CD), the operating concept is totally different.

Wi-Fi systems are half duplex shared media configurations where all stations transmit and receive on the same radio channel. The fundamental problem this creates in a radio system is that a station cannot hear while it is sending, and hence it impossible to detect a collision. Because of this, the developers of the 802.11 specifications came up with a collision avoidance mechanism called the Distributed Control Function (DCF).

According to DCF, A Wi-Fi station will transmit only if it thinks the channel is clear. All transmissions are acknowledged, so if a station does not receive an acknowledgement, it assumes a collision occurred and retries after a random waiting interval.

The incidence of collisions will increase as the traffic increases or in situations where mobile stations cannot hear each other.

There are plans to incorporate quality of service (QoS) capabilities in Wi-Fi with the adoption of the IEEE 802.11e standard. The 802.11e standard will include two operating modes, either of which can be used to improve service for voice:

1. ***Wi-Fi Multimedia Extensions (WME):*** This uses a protocol called Enhanced Multimedia Distributed Control Access (EDCA), which is Extensions an enhanced version of the Distributed Control Function (DCF) defined in the original 802.11 MAC.

   The enhanced part is that EDCA will define eight levels of access priority to the shared wireless channel. Like the original DCF, the EDCA access is a contention-based protocol that employs a set of waiting intervals and back-off timers designed to avoid collisions. However, with DCF, all stations use the same values and hence have the same priority for transmitting on the channel.

   With EDCA, each of the different access priorities is assigned a different range of waiting intervals and back-off counters. Transmissions with higher access priority are assigned shorter intervals. The standard also includes a packet-bursting mode that allows an access point or a mobile station to reserve the channel and send 3- to 5-packets in sequence.

2. ***Wi-Fi Scheduled Multimedia (WSM):*** True consistent delay services can be provided with the optional Wi-Fi Scheduled Multimedia (WSM). WSM operates like the little used Point Control Function (PCF) defined with the original 802.11 MAC.

   In WSM, the access point periodically broadcasts a control message that forces all stations to treat the channel as busy and not attempt to transmit. During that period, the access point polls each station that is defined for time sensitive service.

   To use the WSM option, devices must first send a traffic profile describing bandwidth, latency, and jitter requirements. If the access point does not have sufficient resources to meet the traffic profile, it will return a busy signal.

   Security has been one of the major deficiencies in Wi-Fi, though better encryption systems are now becoming available. Encryption is optional in Wi-Fi, and three different techniques have been defined. These techniques are given here:

   (a) *Wired Equivalent Privacy (WEP):*

   An RC4-based 40-or 104-bit encryption with a static key.

   (b) *Wi-Fi Protected Access (WPA):*

   This is a new standard from the Wi-Fi Alliance that uses the 40 or 104-bit WEP key, but it changes the key on each packet. That changing key functionality is called the Temporal Key Integrity Protocol (TKIP).

Notes

(c) *IEEE 802.11i/WPA2:*

The IEEE is finalized the 802.11i standard, which is based on a far more robust encryption technique called the Advanced Encryption Standard. The Wi-Fi Alliance designate products that comply with the 802.11i standard as WPA2.

However, implementing 802.11i requires a hardware upgrade.

The picture has become somewhat confused as service providers started using Wi-Fi to deliver services for which it was not originally designed. The two major examples of this are wireless ISPs and city-wide Wi-Fi mesh networks.

(d) *Wireless ISPs (WISPs):*

One business that grew out of Wi-Fi was the Wireless ISP (WISP). This is the idea of selling an Internet access service using wireless LAN technology and a shared Internet connection in a public location designated a hot spot.

From a technical standpoint, access to the service is limited based on the transmission range of the WLAN technology. You have to be in the hot spot (i.e. within 100 m of the access point) to use it. From a business standpoint, users either subscribe to a particular carrier service for a monthly fee or access the service on a demand basis at a fee per hour. While the monthly fee basis is most cost effective, there are few intercarrier access arrangements so you have to be in a hot spot operated by your carrier in order to access your service.

(e) *City-Wide Mesh Networks:*

To address the limited range, vendors like Mesh Networks and Tropos Networks have developed mesh network capabilities using Wi-Fi's radio technology.

The idea of a radio mesh network is that messages can be relayed through a number of access points to a central network control station. These networks can typically support mobility as connections are handed off from access point to access point as the mobile station moves.

Some municipalities are using Wi-Fi mesh networks to support public safety applications (i.e. terminals in police cruisers) and to provide Internet access to the community (i.e. the city-wide hot spot).

WiFi systems use two primary radio transmission techniques.

802.11b (<=11 Mbps): The 802.11b radio link uses a direct sequence spread spectrum technique called complementary coded keying (CCK). The bit stream is processed with a special coding and then modulated using Quadrature Phase Shift Keying (QPSK).

802.11a and g (<=54 Mbps): The 802.11a and g systems use 64-channel orthogonal frequency division multiplexing (OFDM). In an OFDM modulation system, the available radio band is divided into a number of sub-channels, and some of the bits are sent on each. The transmitter encodes the bit streams on the 64 subcarriers using Binary Phase Shift Keying (BPSK), Quadrature Phase Shift Keying (QPSK), or one of two levels of Quadrature Amplitude Modulation (16, or 64-QAM). Some of the transmitted information is redundant, so the receiver does not have to receive all of the sub-carriers to reconstruct the information.

Did u know? The original 802.11 specifications also included an option for frequency hopping spread spectrum (FHSS), but that has largely been abandoned.

10.1.2 Adaptive Modulation

Notes

WiFi make use of adaptive modulation and varying levels of forward error correction to optimise transmission rate and error performance.

As a radio signal loses power or encounters interference, the error rate will increase. Adaptive modulation means that the transmitter will automatically shift to a more robust, though less efficient, modulation technique in those adverse conditions.

There are following issues which are assumed to be the cause of the sluggish adoption of Wi-Fi technology:

- ***Security Problems:*** Security concerns have held back Wi-Fi adoption in the corporate world. Hackers and security consultants have demonstrated how easy it can be to crack the current security technology, known as wired equivalent privacy (WEP), used in most Wi-Fi connections. A hacker can break into a Wi-Fi network using readily available materials and software.
- ***Compatibility and Interpretability:*** One of the bigger problems with Wi-Fi is compatibility and interpretability, for example 802.11a products are not compatible with 802.11b products, due to the different operating frequencies, and 802.11a hotspots would not help a 802.11b client. Due to lack of standardization, harmonization and certification, different vendors come out with products that do not work with each other.
- ***Billing Issues:*** Wi-Fi vendors are also looking for ways to solve the problem of back-end integration and billing that has dogged the roll-out of commercial Wi-Fi hotspots. Some of the ideas under consideration for Wi-Fi billing include per day, per hour and unlimited monthly connection fees.

WiFi is a universal wireless networking technology that utilizes radio frequencies to transfer data. WiFi allows for high speed Internet connections without the use of cables or wires.

The term Wi-Fi is a contraction of "wireless fidelity" and commonly used to refer to wireless networking technology. The Wi-Fi Alliance claims rights in its uses as a certification mark for equipment certified to 802.11x standards.

Wi-Fi is a freedom, freedom from wires. It allows you to connect to the Internet from just about anywhere – a coffee shop, a bed in a hotel room or a conference room at work without wires. And the best thing of all, it's super fast – almost 10 times faster than a regular dial-up connection. Wi-Fi networks operate in the unlicensed 2.4 radio bands, with an 11 Mbps (802.11b) or 54 Mbps (802.11a) data rate, respectively.

To access Wi-Fi, you need enabled devices (laptops or PDAs). These devices can send and receive data wirelessly from any location equipped with Wi-Fi access.

What Is Next?

Now the focus in wireless is shifting to the wide area. WiMax, short for Worldwide Interoperability for Microwave Access, is defined in IEEE 802.16 standards is designed to deliver a metro area broadband wireless access (BWA) service, and is being promoted by the WiMax Forum.

Caution WiMAX is similar wireless system to Wi-Fi, but on a much larger scale and at faster speeds. A nomadic version would keep WiMAX-enabled devices connected over large areas, much like today's cell phones.

Notes

Self Assessment

Fill in the blanks:

1. The term Wi-Fi is a contraction of "wireless fidelity" and commonly used to refer to ....
2. Wi-Fi networks operate in the unlicensed .... bands, with an 11 Mbps or 54 Mbps data rate, respectively.
3. A .... can break into a Wi-Fi network using readily available materials and software.
4. .... modulation means that the transmitter will automatically shift to a more robust, though less efficient, modulation technique in those adverse conditions.
5. The .... radio link uses a direct sequence spread spectrum technique called complementary coded keying (CCK).
6. The 802.11a and g systems use ....
7. The idea of a .... network is that messages can be relayed through a number of access points to a central network control station.
8. .... is the idea of selling an Internet access service using wireless LAN technology and a shared Internet connection in a public location designated a hot spot.
9. To use the .... option, devices must first send a traffic profile describing bandwidth, latency, and jitter requirements.

10.2 IEEE 802.16: Broadband Wireless MAN Standard (WiMAX)

Satisfying the growing demand for BWA in underserved markets has been a continuing challenge for service providers, due to the absence of a truly global standard. A standard that would enable companies to build systems that will effectively reach underserved business and residential markets in a manner that supports infrastructure build outs comparable to cable, DSL, and fibre. For years, the wildly successful 802.11x or WiFi wireless LAN technology has been used in BWA applications along with a host of proprietary based solutions. When the WLAN technology was examined closely, it was evident that the overall design and feature set available was not well suited for outdoor BWA applications. It could be done, it is being done, but with limited capacity in terms of bandwidth and subscribers, range and a host of other issues made it clear this approach while a great fit for indoor WLAN was a poor fit for outdoor BWA.

This analysis and review was conducted by the IEEE and it was decided that a new, more complex and fully developed standard would be required to address both the physical layer environment (outdoor versus indoor RF transmissions) and the Quality of Service (QoS) needs demanded by the BWA and last mile access market. The IEEE conducted a multi-year effort to develop this new standard, culminating in final approval of the 802.16a Air-Interface Specification in January 2003. This standard has since received broad industry support from leading equipment makers. Many WiMAX company members are active in both the IEEE 802.16 standards development and the IEEE 802.11 efforts for Wireless LAN, and envision the combination of 802.16a and 802.11 creating a complete wireless solution for delivering high speed Internet access to businesses, homes, and WiFi hot spots. The 802.16a standard delivers carrierclass performance in terms of robustness and QoS and has been designed from the ground up to deliver a suite of services over a scalable, long range, high capacity "last mile" wireless communications for carriers and service providers around the world.

In BWA, applications include residential broadband access – DSL-level service for SOHO and small businesses, T1/E1 level service for enterprise, all supporting not just data but voice and video as well, wireless backhaul for hotspots and cellular tower backhaul service to name a few.

Caution In reviewing the standard, the technical details and features that differentiate WiMAX certified equipment from WiFi or other technologies can best be illustrated by focusing on the two layers addressed in the standard, the physical (PHY) or RF transmissions and the media access control (MAC) layer design.

10.2.1 WiMAX and the IEEE 802.16a PHY Layer

The first version of the 802.16 standard released addressed Line-of-Sight (LOS) environments at high frequency bands operating in the 10–66 GHz range, whereas the recently adopted amendment, the 802.16a standard, is designed for systems operating in bands between 2 GHz and 11 GHz. The significant difference between these two frequency bands lies in the ability to support Non-Line-of-Sight (NLOS) operation in the lower frequencies, something that is not possible in higher bands. Consequently, the 802.16a amendment to the standard opened up the opportunity for major changes to the PHY layer specifications specifically to address the needs of the 2–11 GHz bands. This is achieved through the introduction of three new PHY-layer specifications (a new Single Carrier PHY, a 256 point FFT OFDM PHY, and a 2048 point FFT OFDMA PHY); major changes to the PHY layer specification as compared to the upper frequency, as well as significant MAC-layer enhancements. Although multiple PHYs are specified as in the 802.11 suite of standards (few recall that infrared and frequency hopping were and are part of the base 802.11 standard), the WiMAX Forum has determined that the first interoperable test plans and eventual certification will support the 256 point FFT OFDM PHY (which is common between 802.16a and ETSI HiperMAN), with the others to be developed as the market requires.

The OFDM signalling format was selected in preference to competing formats such as CDMA due to its ability to support NLOS performance while maintaining a high level of spectral efficiency maximizing the use of available spectrum. In the case of CDMA (prevalent in 2G and 3G standards), the RF bandwidth must be much larger than the data throughput, in order to maintain processing gain adequate to overcome interference. This is clearly impractical for broadband wireless below 11 GHz, since for example, data rates up to 70 Mbps would require RF bandwidths exceeding 200 MHz to deliver comparable processing gains and NLOS performance.

Some of the other PHY layer features of 802.16a that are instrumental in giving this technology the power to deliver robust performance in a broad range of channel environments are; flexible channel widths, adaptive burst profiles, forward error correction with concatenated Reed-Solomon and convolutional encoding, optional AAS (advanced antenna systems) to improve range/capacity, DFS (dynamic frequency selection)-which helps in minimizing interference, and STC (space-time coding) to enhance performance in fading environments through spatial diversity.

10.2.2 IEEE 802.16a MAC Layer

Every wireless network operates fundamentally in a shared medium and as such that requires a mechanism for controlling access by subscriber units to the medium. The 802.16a standard uses a slotted TDMA protocol scheduled by the BTS to allocate capacity to subscribers in a point-to-multipoint network topology. While this on the surface sounds like a one line, technical throwaway statement, it has a huge impact on how the system operates and what services it can deploy. By starting with a TDMA approach with intelligent scheduling, WiMAX systems will be able to deliver not only high speed data with SLAs, but latency sensitive services such as voice and video or database access are also supported.

The standard delivers QoS beyond mere prioritization, a technique that is very limited in effectiveness as traffic load and the number of subscribers increases. The MAC layer in WiMAX certified systems has also been designed to address the harsh physical layer environment where interference, fast fading and other phenomena are prevalent in outdoor operation.

Differentiating the IEEE 802.16a and 802.11 Standards – WiFi versus WiMAX Scalability

At the PHY layer the standard supports flexible RF channel bandwidths and reuse of these channels (frequency reuse) as a way to increase cell capacity as the network grows. The standard also specifies support for automatic transmit power control and channel quality measurements as additional PHY layer tools to support cell planning/deployment and efficient spectrum use. Operators can re-allocate spectrum through sectorisation and cell splitting as the number of subscribers grows. Also, support for multiple channel bandwidths enables equipment makers to provide a means to address the unique government spectrum use and allocation regulations faced by operators in diverse international markets. The IEEE 802.16a standard specifies channel sizes ranging form 1.75 MHz up to 20 MHz with many options in between.

WiFi based products on the other hand require at least 20 MHz for each channel (22 MHz in the 2.4 GHz band for 802.11b), and have specified only the license exempt bands 2.4 GHz ISM, 5 GHz ISM and 5 GHz UNII for operation. In the MAC layer, the CSMA/CA foundation of 802.11, basically a wireless Ethernet protocol, scales about as well as does Ethernet. That is to say – poorly. Just as in an Ethernet LAN, more users results in a geometric reduction of throughput, so does the CSMA/CA MAC for WLANs. In contrast the MAC layer in the 802.16 standard has been designed to scale from one up to 100's of users within one RF channel, a feat the 802.11 MAC was never designed for and is incapable of supporting.

- *Coverage:* The BWA standard is designed for optimal performance in all types of propagation environments, including LOS, near LOS and NLOS environments, and delivers reliable robust performance even in cases where extreme link pathologies have been introduced. The robust OFDM waveform supports high spectral efficiency (bits per second per Hertz) over ranges from 2 to 40 kilometers with up to 70 Mbps in a single RF channel. Advanced topologies (mesh networks) and antenna techniques (beam-forming, STC, antenna diversity) can be employed to improve coverage even further. These advanced techniques can also be used to increase spectral efficiency, capacity, reuse, and average and peak throughput per RF channel. In addition, not all OFDM is the same. The OFDM designed for BWA has in it the ability to support longer range transmissions and the multi-path or reflections encountered.

  In contrast, WLANs and 802.11 systems have at their core either a basic CDMA approach or use OFDM with a much different design, and have as a requirement low power consumption limiting the range. OFDM in the WLAN was created with the vision of the systems covering tens and maybe a few hundreds of meters versus 802.16 which is designed for higher power and an OFDM approach that supports deployments in the tens of kilometers.

- *QoS:* The 802.16a MAC relies on a Grant/Request protocol for access to the medium and it supports differentiated service levels (e.g., dedicated T1/E1 for business and best effort for residential). The protocol employs TDM data streams on the DL (downlink) and TDMA on the UL (uplink), with the hooks for a centralized scheduler to support delay-sensitive services like voice and video. By assuring collision-free data access to the channel, the 16a MAC improves total system throughput and bandwidth efficiency, in comparison with contention-based access techniques like the CSMA-CA protocol used in WLANs. The 16a MAC also assures bounded delay on the data (CSMA-CA by contrast, offers no guarantees on delay).

Notes The TDM/TDMA access technique also ensures easier support for multicast and broadcast services. With a CSMA/CA approach at its core, WLANs in their current implementation will never be able to deliver the QoS of a BWA, 802.16 system.

The WiMAX Forum-Interoperability for 802.16 Compliant Systems

Establishment of a standard is critical to mass adoption of a given technology; however by itself a standard is not enough. The 802.11b WLAN standard was ratified in 1999, however it did not reach mass adoption until the introduction of the WiFi Alliance and certified, interoperable equipment was available in 2001. In order to bring interoperability to the Broadband Wireless Access space, the WiMAX Forum is focused on establishing a unique subset of baseline features grouped in what is referred to as "System Profiles" that all compliant equipment must satisfy. These profiles and a suite of test protocols will establish a baseline interoperable protocol, allowing multiple vendors' equipment to interoperate; with the net result being System Integrators and Service Providers will have option to purchase equipment from more than one supplier.

Profiles can address, for example, the regulatory spectrum constraints faced by operators in different geographies. For example, a service provider in Europe2 operating in the 3.5 GHz band, who has been allocated 14 MHz of spectrum, is likely to want equipment that supports 3.5 and/or 7 MHz channel bandwidths and, depending on regulatory requirements, TDD (time-division duplex) or FDD (frequency-division duplex) operation. Similarly, a WISP (Wireless Internet Service Provider) in the U.S. using license-exempt spectrum in the 5.8 GHz UNII band might desire equipment that supports TDD and a 10 MHz bandwidth.

WiMAX is establishing a structured compliance procedure based upon the proven test methodology specified by ISO/IEC 9646.3 The process starts with standardized Test Purposes written in English, which are then translated into Standardized Abstract Test Suites in a language called TTCN.4 In parallel with the Test Purposes, the Test Purposes are also used as input to generate test tables referred to as the PICS (Protocol Implementation Conformance Statement) Proforma is generated. The end result is a complete set of test tools that WiMAX will make available to equipment developers so they can design-in conformance and interoperability during the earliest possible phase of product development. Typically, this activity will commence when the first integrated prototype becomes available.

Self Assessment

Fill in the blanks:

10. The .... MAC relies on a Grant/Request protocol for access to the medium and it supports differentiated service levels.

11. The .... standard is designed for optimal performance in all types of propagation environments, including LOS, near LOS and NLOS environments.

12. The first version of the 802.16 standard released addressed Line-of-Sight (LOS) environments at high frequency bands operating in the .... range.

13. Satisfying the growing demand for BWA in underserved markets has been a continuing challenge for service providers, due to the absence of a truly .... standard.

Case Study

Redline Debuts its 802.16-2004 Compliant Broadband Wireless Solution at WCA Symposium

About Redline Communications

Redline Communications is a technology leader in the design and manufacture of standards-based broadband wireless access solutions. Using industry leading OFDM technologies, Redline's award-winning products provide unmatched high capacity and non-line-of-

Contd...

sight capabilities with proven performance, reliability and security. Ideal for a variety of access, backhaul and private network applications, Redline products meet the needs of carriers, service providers and enterprises worldwide. Redline is a principal member of the WiMAX Forum(TM), and was first in the world to market an 802.16 compliant product. Redline has over 10,000 installations in 75 countries across six continents through a global distribution network of 80+ partners.

Redline Communications, a leading provider of standards-based broadband wireless equipment, announced today that it is unveiling its WiMAX ready product at the WCA International Symposium and Business Expo (Booth #306) taking place January 12 – 14 at the Fairmont Hotel in San Jose, Calif. On display will be Redline's universal platform, the AN-100U, a fully compliant IEEE 802.16-2004 platform. The AN-100U, which functions as a base station and subscriber station, advances Redline's readiness for WiMAX(TM) interoperability testing and commercial viability.

As a principal member of the WiMAX Forum(TM), Redline plays an active role in the technical development of IEEE 802.16 standards. The company is now actively participating in the development of the 802.16e standard for mobile applications.

"From our earliest days of product development, Redline has been committed to delivering solutions that support the standardization needs of the industry," said Keith Doucet, VP of Marketing and Product Management. "We led the market with our introduction of an 802.16a compliant product, the AN-100, which today is being used worldwide by Tier 1 operators primarily for backhauling wireless access networks. The AN-100 has demonstrated the viability of the standards based technology for backhaul applications, while the AN-100U will serve the access market, representing Redline's foyer into the residential space".

Redline achieved a world first when it introduced the AN-100 802.16a compliant solution to the industry early 2004. This product received the Telecommunication Industry Association's (TIA) SUPERQuest award in the Backbone/Edge Networking Equipment category.

Roger B. Marks, Chairman of IEEE 802.16, says the evolution of 802.16 has been instrumental in accelerating broadband wireless deployment. "Interest in IEEE Standard 802.16 continues to explode around the world, with hundreds of engineers from global industry cooperating on its evolution. As companies introduce new products based upon on that foundation, the synergies created by the standard are set to bring about a rapid evolution of broadband wireless access as an essential communications tool."

Doucet adds, "We are now ready with 802.16-2004 and will once again be counted among the first to move forward on this important initiative that will see true interoperability become a reality for the industry."

"We are pleased that Redline has chosen the WCA International Symposium as its venue of choice to preview its new 802.16-2004 compliant broadband wireless solution," said Andrew Kreig, President of Wireless Communications Association International. "The achievements to date from the broadband wireless community are commendable as they advance their solutions towards WiMAX interoperability. The dedication from companies like Redline will ensure that the promise of WiMAX will soon become a reality."

Questions:

1. Discuss the role of redline communications in the design of standards.
2. Discuss various achievements of redline communications.

Source: http://www.businesswire.com/news/home/20050110005400/en/Redline-Debuts-802.16-2004-Compliant-Broadband-Wireless-Solution

10.3 Summary

- IEEE 802.11 is a set of physical layer standards for implementing wireless local area network (WLAN) computer communication in the 2.4, 3.6, 5 and 60 GHz frequency bands.
- The 802.11 family consist of a series of half-duplex over-the-air modulation techniques that use the same basic protocol. The most popular are those defined by the 802.11b and 802.11g protocols, which are amendments to the original standard. 802.11-1997 was the first wireless networking standard.
- The 802.11 standard is defined through several specifications of WLANs.
- Wi-Fi systems are half duplex shared media configurations where all stations transmit and receive on the same radio channel.
- One business that grew out of Wi-Fi was the Wireless ISP (WISP). This is the idea of selling an Internet access service using wireless LAN technology and a shared Internet connection in a public location designated a hot spot.

10.4 Keywords

802.11a: This is an extension to 802.11 that pertains to wireless LANs and goes as fast as 54 Mbps in the 5-GHz band.

802.11b: The 802.11 high rate Wi-Fi is an extension to 802.11 that pertains to wireless LANs and yields a connection as fast as 11 Mbps transmission (with a fallback to 5.5, 2, and 1 Mbps depending on strength of signal) in the 2.4-GHz band.

802.11g: This pertains to wireless LANs and provides 20+ Mbps in the 2.4-GHz band.

IEEE 802.11: It is a set of physical layer standards for implementing wireless local area network (WLAN) computer communication in the 2.4, 3.6, 5 and 60 GHz frequency bands.

Wi-Fi Multimedia Extensions (WME): This uses a protocol called Enhanced Multimedia Distributed Control Access (EDCA), which is Extensions an enhanced version of the Distributed Control Function (DCF) defined in the original 802.11 MAC.

10.5 Review Questions

1. What are the various specifications in the 802.11 family?
2. Do a technical camparison between the three major wi-fi standards?
3. What are the two operating modes that are included in the 802.11e standard?
4. Explain the two primary radio transmission techniques of the Wi Di system.
5. Discuss the issues which are assumed to be the cause of the sluggish adoption of wi-fi technology.
6. Distinguish between the IEEE 802.16a and 802.11 standards – wifi versus wimax scalability.

Answers: Self Assessment

1. wireless networking technology
2. 2.4 radio
3. Hacker
4. Adaptive
5. 802.11b

Notes

6. 64-channel orthogonal frequency division multiplexing (ofdm)
7. Radio mesh
8. Wireless ISP (WISP)
9. WSM
10. 802.16a
11. BWA
12. 10–66 GHz
13. global

10.6 Further Readings

Books

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

John Ross, *Introduction to wireless networks.*

Vijay Garg, *Wireless Communications & Networking.*

Theodore S. Rappaport, *Wireless Communications: Principles and Practice.*

Online links

http://www.tutorialspoint.com/wi-fi/wifi_summary.htm

http://www.tra.gov.eg/uploads/technical%20material/Wi-Fi%20report.pdf

http://www.hp.com/rnd/library/pdf/understandingWiFi.pdf

www.cs.tut.fi/kurssit/TLT-6556/Slides/3-802.16e.pdf

Notes

Unit 11: Wireless WAN

CONTENTS

Objectives

Introduction

11.1 Wireless WAN User Devices

11.1.1 Packet Radio WANs

11.1.2 Cellular Digital Packet Data (CFPD)

11.1.3 Personal Communications Services (PCS)

11.1.4 Antennae

11.2 Wireless WAN Systems

11.2.1 Cellular WANs

11.2.2 Space-based Wireless WANs

11.3 Short Message Service (SMS) Applications

11.3.1 Person-to-Person Text Messaging

11.3.2 Provision of Information

11.3.3 Downloading

11.3.4 Alerts and Notifications

11.3.5 Two-way Interactive Text Messaging Applications

11.4 Summary

11.5 Keywords

11.6 Review Questions

11.7 Further Readings

Objectives

After studying this unit, you will be able to:

- Discuss the concept of Wireless WAN User Devices
- Explain the Wireless WAN Systems
- Describe the Short Message Service (SMS) Applications

Introduction

As the term implies, a WAN spans a large physical distance. The Internet is the largest WAN, spanning the Earth. A WAN is a geographically-dispersed collection of LANs. A network device called a router connects LANs to a WAN. In IP networking, the router maintains both a LAN address and a WAN address. A WAN differs from a LAN in several important ways. Most WANs (like the Internet) are not owned by any one organization but rather exist under collective or distributed ownership and management. WANs tend to use technology like ATM, Frame Relay and X.25 for connectivity over the longer distances.

Notes

11.1 Wireless WAN User Devices

WAN stands for Wide Area Network. As its name suggests, it is a computer network that covers a far wider area than a LAN (Local Area Network). WANs cover cities, countries, continents and the whole world. A WAN is formed by linking LANs together.

Example: Several major LANs in a city can connect together forming a WAN.

A Wide Area Network (WAN) is a communication network made up of computers that are non-local to one another, exchanging data across a wide area or great distance. The most common example is the Internet, though a WAN need not be global to qualify as a wide area network. Since computer acronyms have become virtual words, the terminology "WAN network" is often used in the public sector, even though redundant. For those new to these acronyms, adding the word "network" can be a reminder of what a WAN is, so while this article uses the common term, the proper term is WAN, pronounced like ran with a "W."

Computers interoperate on a WAN network by using a set of standards or protocols for communication. Each computer on the WAN is assigned a unique address known as an Internet Protocol (IP) address. When a computer sends a request out on the WAN network, it gets routed to a specific server that hosts the requested information. The server responds by sending the information back to the IP address of the requesting computer.

When networks connect to form a bigger network (a bigger WAN), the resulting network is called an internetwork, which is generically abbreviated to 'an internet'. Now when all WANs in the world connect forming a global internet, we call it The Internet, which everyone knows. That's why the Internet is always written with a capital I. It is the biggest WAN we have.

Wireless WANs satisfy both mobile and stationary applications. Components, therefore, vary depending on the technology and configuration of the wireless WAN. A satellite-based wireless WAN, for example, has different components than a cellular-based system.

Example: Some examples of smaller networks in the WAN include Municipal Area Networks (MANs), Campus Area Networks (CANs) and Local Area Networks (LANs). MANs provide connectivity throughout a city or regional area for public access to the Internet, while CANs offer connectivity to students and faculty for on-site resources and online access. LANs can be either private or public, but are usually private networks with optional online access. The home or office network is a good example of a LAN.

A LAN can also become a WAN if, for example, a company with headquarters in both Los Angeles and Chicago links their two LANs together over the Internet. This geographic distance would qualify the network as a WAN. The linked LANs can use encryption software to keep their communications private from the public Internet, creating a Virtual Private Network (VPN). This technology of creating a secure, encrypted channel through the Internet to link LANs is sometimes called tunneling.

Notes The architecture of the Internet, the most familiar WAN, is non-centralized by design, making it nearly impossible to destroy. Like a freeway system in a large metropolis, if one freeway or information highway is taken out, data traffic is automatically re-routed around the breakdown through alternate routes. The highways, in the case of the Internet, are actually leased telephone lines and a combination of other technologies and structures including smaller networks that are linked by the WAN network to become part of the whole.

A Personal Area Network (PAN) is created by Bluetooth technology to wirelessly link personal devices together for interoperability. You might use Bluetooth to send print jobs from a laptop

Notes

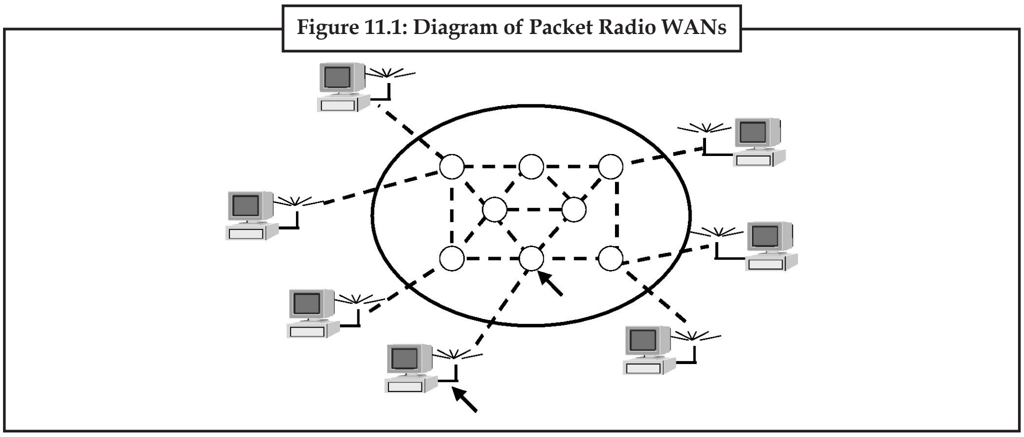
to a printer, for example, or to synchronize a personal digital assistant with your computer. Bluetooth can also be used to share Internet access between devices, and therefore also plays a part in the many technologies that can contribute to a WAN network, more properly known as a WAN.

Caution Except for large organizations that can afford to put up their own satellites or string their own cables across long distances, wide area networks use a public carrier such as a phone company to carry communications. Commonly used wireless WAN technologies include packet radio, cellular telephone, and satellite.

11.1.1 Packet Radio WANs

Packet radio WANs function much like a wired packet switching wide area network. Users transmit messages to one another across a network of relay nodes. In a wired network these nodes are routers or switches connected by copper or fibre optic lines or satellites. In a wireless network the nodes are connected by radio transmissions as shown in Figure 11.1.

Figure 11.1: Diagram of Packet Radio WANs



Source: http://k-12.pisd.edu/currinst/network/11_806A_4-2_SG.pdf

Packet radio WAN users connect to their computers a packet radio modem with an omnidirectional antenna. These modems are currently relatively slow, not suitable for surfing the web, but sufficient for transmissions like short e-mail messages. An advantage that packet radio has over cellular services is the way users are charged to use the network. Packet radio fees are charged by the packet. Cellular charges are by the minute. For a user sending lots of short messages that take far less than a minute to transmit, packet radio can be less expensive. In a cellular network, each connection is charged a certain rate. ARDIS and RAM Mobile Data are services that provide packet radio networks.

A common use of packet radio WANs is for service technicians in the field who need to order parts or check inventory or report how much time they spent on a particular job. The Toronto Sun newspaper uses a packet radio WAN. Each distributor who fills the newspaper vending machines reports each night how many papers were left unsold. Using this data, the newspaper plans how many papers to print the next day. Another application is remote monitoring.

Example: A packet radio modem could be connected to a water meter in a hard to reach location. The meter would periodically transmit the current reading.

To transfer data across the network, packet radio WANs follow similar routing protocols to wired networks, maintaining routing tables and sending a packet on in the direction of the destination according to the table. The main difference is that a wireless relay node can only transmit to other nodes within reach of its transmissions, its propagation pattern.

11.1.2 Cellular Digital Packet Data (CFPD)

CDPD allows mobile users to transmit digital signals over the analog cellular telephone network in the 800 MHz band. It can achieve data rates up to 19.2 Kbps, much faster than a typical analog cellular phone link being used for data. CDPD transmits very short bursts of data on the cellular channels when no one is using them. Analog cellular networks are idle about 20 percent of the time, even when networks that get very heavy use. For example, the time between one call being disconnected and the next one being connected is idle time for an analog network. A CDPD modem searches for an idle channel and then transmits the data in 128-byte packets.

11.1.3 Personal Communications Services (PCS)

PCS is a fully digital version of cellular wireless that uses very small cells called microcells. Because it is fully digital, PCS has enhanced features, better encryption, and uses less power. Because they use less power, handheld PCS devices can be smaller and lighter. PCS uses a digital cellular standard called GSM, Global System for Mobilization. GSM is widely used in Europe. The frequency band between 1.850 and 1.990 GHz was recently allocated to PCS in the United States. The frequencies were auctioned to companies that planned to provide PCS. These companies paid the government $7.7 billion for a band of frequencies in 1995 and additional frequencies were auctioned for $6 billion in 1996.

11.1.4 Antennae

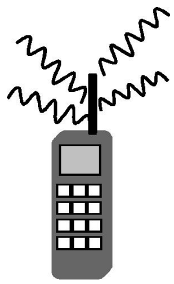
The WNI (Wireless Network Interface) connects to an antenna that transmits and receives the radio signal. The transmit power of an antenna is measured in watts. Many radio stations use 50,000 watts of power. Wireless networks do not need to send their signals as far as a broadcast radio station and so they require much less power. Typically, the transmit power for a wireless network is one watt or less.

An antenna can increase the power of the radio signal so that it can travel farther. A good analogy is a sprinkler that sprays water in many directions. If all but one of the holes is covered, the water will spray out of the one open hole with much greater power and will travel much farther. An antenna increases the power of a radio signal by keeping the radio waves from going up but allowing them to go out toward the receiver, that is, the antenna compresses the vertical propagation to increase the horizontal propagation. The increase in power provided by an antenna is called gain and measured in decibels (dB).

Did u know? As a rule of thumb, a 6 dB antenna will increase the power of a signal by 4 and a 9 dB antenna will multiply the power by 8. A typical cellular phone antenna has a 3 dB gain.

Types of Antenna

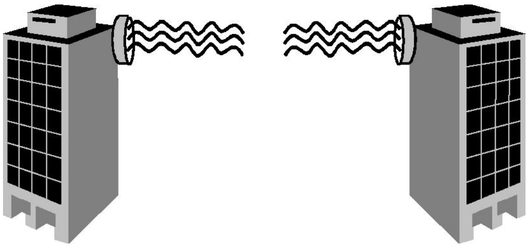
Figure 11.2: Omnidirectional Antenna



Source: http://k-12.pisd.edu/currinst/network/11_806A_4-2_SG.pdf

An omnidirectional antenna (Figure 11.2) transmits radio waves in all directions. Its gain is equal to one, also called unity gain. For cellular phones unity gain antennas are good to use in cities where there are tall buildings or in the mountains because they allow the signal to travel up and over the buildings or mountains. Omnidirectional antennas are also good for indoor wireless networks.

Figure 11.3: Directional Antenna



Source: http://k-12.pisd.edu/currinst/network/11_806A_4-2_SG.pdf

A directional antenna (Figure 11.3) concentrates its power in a certain direction and therefore has higher gain. A directional antenna is good for point to point connections.

Task If you were using a cellular phone in a remote rural location, far from the nearest base station, what type of antenna would you want to use?

Self-Assessment

State whether the following statements are true or false:

1. A WAN is formed by linking LANs together.
2. A VAN is created by Bluetooth technology to wirelessly link personal devices together for interoperability.
3. Packet radio WAN users connect to their computers a packet radio modem with an omnidirectional antenna.
4. A directional antenna transmits radio waves in all directions.
5. An antenna can decrease the power of the radio signal so that it can travel farther.

11.2 Wireless WAN Systems

Most wireless WANs are cellular based, but some make use of space. Take a closer look at both of these.

11.2.1 Cellular WANs

The convergence of telephony and computer networking means that cellular telephone networks, designed for voice transmission, will be used more and more for data transmission. Cellular phones currently transmit at about 14.4 Kbps but the technology, and speed is improving rapidly.

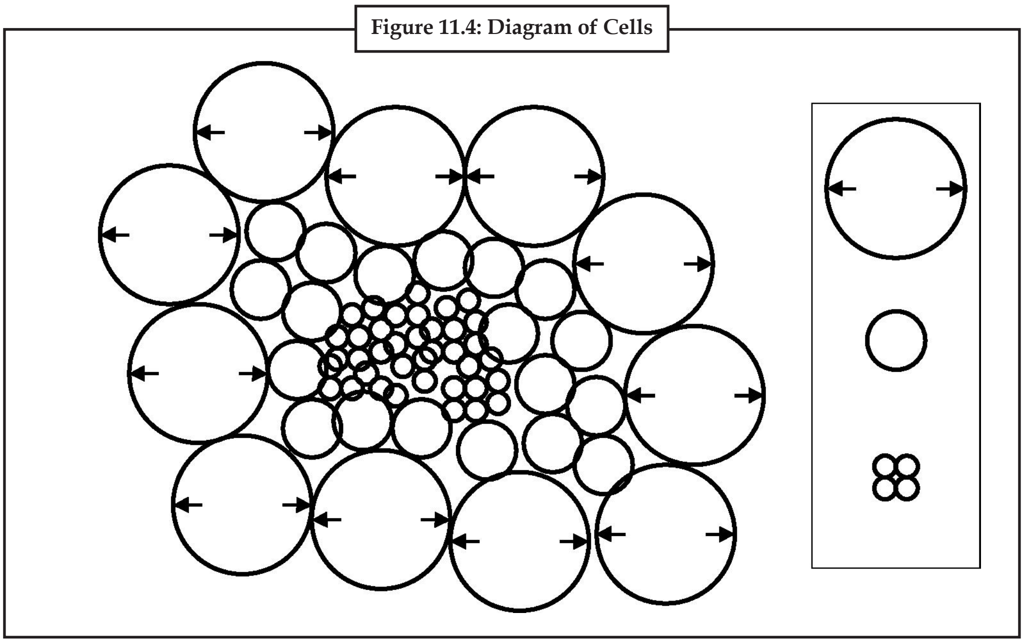
The original cellular telephone system was analog (called Analog Mobile Phone Service, AMPS) because it was designed to carry data from an analog source: people,s voices. Telephone companies have invested billions of dollars to create an infrastructure for carrying voice transmissions nearly anywhere in the world. Now that network is being used more and more for data instead of voice. This is pushing the cellular telephone carriers to switch from analog to digital transmissions. Among other advantages, digital signals can be encrypted for better security and can have better error control.

The cellular system uses radio waves to transmit signals. A call on a cellular system uses two frequencies for each call, one frequency for each direction the signal travels between the base station and the mobile user. When a call is made using a cellular phone, the phone searches for the nearest base station. The call is routed through the antenna for that base station to the public switched telephone network where it is transmitted over that network like a regular phone call. As the phone moves from one cell to another during a call, the network automatically roams and switches the call to the next cell.

Did u know? Cellular technology was developed to overcome the problem of more and more people using mobile phones. In the beginning, engineers would solve the problem of network growth by adding frequencies or by subdividing the frequencies they had into narrower and narrower channels. But it became obvious that there would never be enough individual frequencies to carry all of the calls.

Cellular networks offer a different solution called frequency reuse. Each frequency is only used in a limited area called a cell. Two cells can use the same frequency if they are separated by a certain amount that depends on the power of the transceiver and the topography. This increases the number of "available" frequencies without actually increasing the number of frequencies. The smaller the cells, the more the frequencies can be reused. In fact, when the size of the cell is reduced by 50%, capacity will increase four times. Frequency reuse has always been used for radio and television. Two television stations can use the same frequency if they are at least 150 miles apart. It is not uncommon to experience radio stations reusing frequencies while driving between cities with the car radio tuned to a particular station. At a certain point the signal changed from one station to another with a short time in between when the two signals overlapped.

Figure 11.4: Diagram of Cells



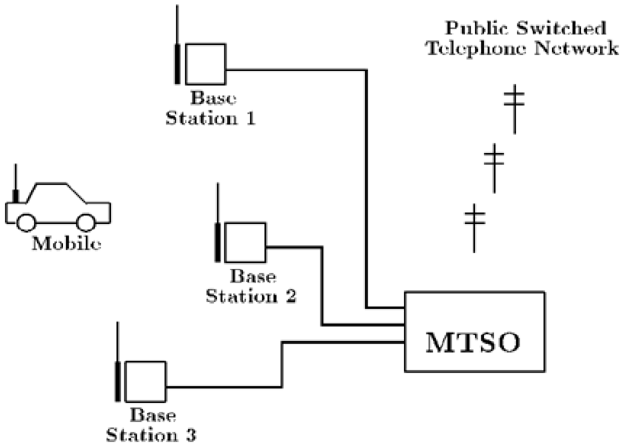
Source: http://k-12.pisd.edu/currinst/network/11_806A_4-2_SG.pdf

Cell sizes (Figure 11.4) range from one kilometre to 50 kilometers in radius. Larger cells are used for less densely populated places and especially for highways where mobile telephone users are moving so fast that they would pass through smaller cells too quickly. Smaller cells are used in more densely populated urban areas. PCS (Personal Communications Service) is a popular digital cellular WAN that uses very small cells that are no more than 10 kilometers across.

Example: The Omnipoint PCS network for the greater New York City area uses over 500 cell sites to cover the 161,300-square-kilometer area.

At the centre of each cell is a tower called the base station that holds the antennas, and some switching equipment. Each base station uses carefully chosen frequencies that will not interfere with adjacent cells. Each cell is grouped with seven other cells in an organization called a cluster. Within each cluster is a Mobile Telephone Switching Office (MTSO). The MTSO connects the network to the Public Switched Telephone Network (PSTN), which is the local wire-based telephone company.

Figure 11.5: Cellular Telephone Network



Source: http://www.decodesystems.com/mt/96dec/

The MTSO decides when to 'hand-off' a call to another cell. MTSOs may also hand off calls when the cell has a lot off call traffic. The MTSO will scan the airwaves looking for a channel from an adjacent cell that can be used, then hands off the call. If the network is overloaded and the MTSO cannot find another channel to "borrow," the caller may get a busy signal while trying to make a call. Hand-offs present a problem when transferring data as the connection sometimes drops briefly during a hand-off.

11.2.2 Space-based Wireless WANs

The use of space-based systems basically facilitate the means for networking users over wide areas.

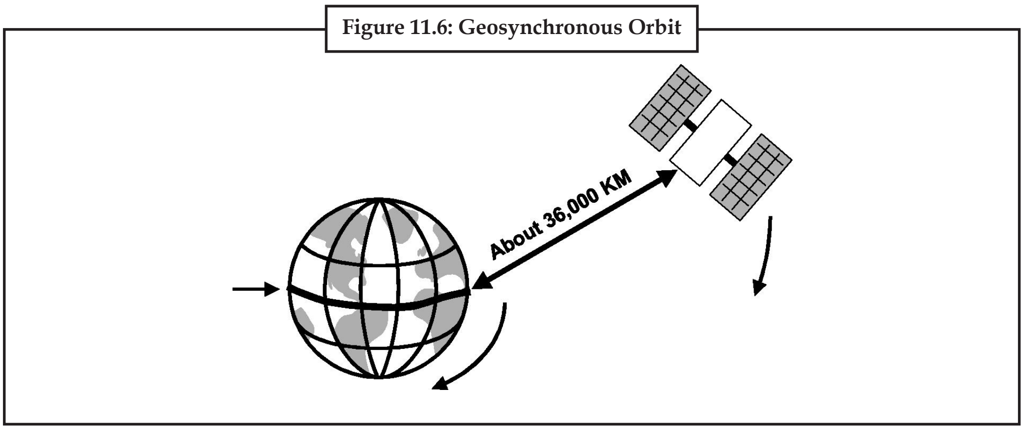
Satellites

A step further in telecommunications networks is the use of satellite networks.

Satellites that orbit the Earth at an altitude of 22,237 miles revolve around the Earth at the same speed that the Earth rotates. This means that the satellites remain over the same area on the ground at all times. This is known as a geosynchronous orbit and was proposed by the physicist and science fiction writer Arthur C. Clarke. Satellites in geosynchronous orbit can relay signals from one part of the Earth to another and can therefore take the place of wired links between distant locations.

Notes

Figure 11.6: Geosynchronous Orbit

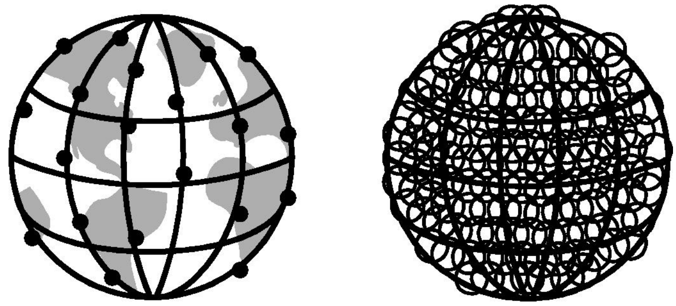


Source: http://k-12.pisd.edu/currinst/network/11_806A_4-2_SG.pdf

Because geosynchronous orbit satellites are so far away from the Earth, it takes a lot of power to transmit a signal that will reach them. This makes them less suitable for use by small wireless networks or mobile users. Another problem with geosynchronous satellites is latency. It takes a relatively long time for a signal to reach a satellite, get processed, and then travel back to Earth. This delay is called latency and can create problems for data transmissions. A third problem arises because the signals are more susceptible to interference since they are transmitted over such a long distance.

One way to overcome the power, latency, and interference problems is to use satellites closer to Earth. But satellites in lower orbits do not maintain their position relative to the ground. If a low orbit satellite were relaying data, the transmission would be interrupted when the satellite moved out of range. The only way to use lower orbit satellites is to put enough of them in orbit so that when one satellite moves out of range, another satellite has already moved into range and can pick up the transmission. Think of this system as a cellular system in which the base stations are moving as well, and hand-offs happen as the base stations and the mobile users move.

Figure 11.7: Low Earth Orbit (LEO) Satellite Network



Source: http://k-12.pisd.edu/currinst/network/11_806A_4-2_SG.pdf

A system of low Earth orbit (LEO) satellites (Figure 11.7) requires so many satellites that the price has been prohibitive until very recently. With the explosion of wireless users, consortiums of companies have invested huge sums of money to create LEO satellite networks.

The Iridium system uses 66 satellites in LEO (750 kilometers). The satellites act as the base stations for more than 1,600 cells that cover the entire surface of the globe. Each cell has 174 channels; the system can handle over 280,000 calls simultaneously.

Another system called Teledesic will have 288 LEO satellites by 2002. The goal is to have systems that can transmit (downlink) at 64 Mbps to the users and can receive (uplink) at 2 Mbps.

Meteor Burst Communications

Meteor burst communications (MBC), also referred to as meteor scatter communications, is a radio propagation mode that exploits the ionized trails of meteors during atmospheric entry to establish brief communications paths between radio stations up to 2,250 kilometres (1,400 mi) apart. As the earth moves along its orbital path, billions of particles known as meteors enter the earth's atmosphere every day; a small fraction of which have properties useful for point to point communication. When these meteors begin to burn up, they create a trail of ionized particles in the E layer of the atmosphere that can persist for up to several seconds. The ionization trails can be very dense and thus used to reflect radio waves. The frequencies that can be reflected by any particular ion trail are determined by the intensity of the ionization created by the meteor, often a function of the initial size of the particle, and are generally between 30 MHz and 50 MHz.

The distance over which communications can be established is determined by the altitude at which the ionization is created, the location over the surface of the Earth where the meteor is falling, the angle of entry into the atmosphere, and the relative locations of the stations attempting to establish communications. Because these ionization trails only exist for fractions of a second to as long as a few seconds in duration, they create only brief windows of opportunity for communications.

Self Assessment

Fill in the blanks:

6. The cellular system uses ……………………...... to transmit signals.
7. Cellular networks offer a different solution called ……………………......
8. ……………………...... sizes range from one kilometer to 50 kilometers in radius.
9. ……………………...... that orbit the Earth at an altitude of 22,237 miles revolve around the Earth at the same speed that the Earth rotates.
10. With the explosion of wireless users, consortiums of companies have invested huge sums of money to create ……………………...... satellite networks.

11.3 Short Message Service (SMS) Applications

SMS stands for Short Message Service. It is a technology that enables the sending and receiving of messages between mobile phones. SMS first appeared in Europe in 1992. It was included in the GSM (Global System for Mobile Communications) standards right at the beginning. Later it was ported to wireless technologies like CDMA and TDMA. The GSM and SMS standards were originally developed by ETSI.

Did u know? ETSI is the abbreviation for European Telecommunications Standards Institute. Now the 3GPP(Third Generation Partnership Project) is responsible for the development and maintenance of the GSM and SMS standards.

As suggested by the name "Short Message Service", the data that can be held by an SMS message is very limited. One SMS message can contain at most 140 bytes (1120 bits) of data, so one SMS message can contain up to:

- 160 characters if 7-bit character encoding is used. (7-bit character encoding is suitable for encoding Latin characters like English alphabets.)
- 70 characters if 16-bit Unicode UCS2 character encoding is used. (SMS text messages containing non-Latin characters like Chinese characters should use 16-bit character encoding.)

SMS text messaging supports languages internationally. It works fine with all languages supported by Unicode, including Arabic, Chinese, Japanese and Korean. Besides text, SMS messages can also carry binary data. It is possible to send ringtones, pictures, operator logos, wallpapers, animations, business cards (e.g. VCards) and WAP configurations to a mobile phone with SMS messages.

There are many different kinds of SMS applications on the market today and many others are being developed. Applications in which SMS messaging can be utilized are virtually unlimited. We will describe some common examples of SMS applications below to give you some ideas of what can be done with SMS messaging.

11.3.1 Person-to-Person Text Messaging

Person-to-person text messaging is the most commonly used SMS application and it is what the SMS technology was originally designed for. In these kinds of text messaging applications, a mobile user types an SMS text message using the keypad of his/her mobile phone, then he/she inputs the mobile phone number of the recipient and clicks a certain option on the screen, such as "Send" or "OK", to send the text message out. When the recipient mobile phone receives the SMS text message, it will notify the user by giving out a sound or vibrating. The user can read the SMS text message some time later or immediately and can send a text message back if he/she wants.

A chat application is another kind of person-to-person text messaging application that allows a group of people to exchange SMS text messages interactively. In a chat application, all SMS text messages sent and received are displayed on the mobile phone's screen in order of date and time. SMS text messages written by different mobile users may be displayed in different colours for better readability, like this:

11.3.2 Provision of Information

A popular application of the SMS technology other than person-to-person text messaging is the provision of information to mobile users. Many content providers make use of SMS text messages to send information such as news, weather report and financial data to their subscribers. Many of these information services are not free. Reverse billing SMS is a common way used by content providers to bill their users. The user is charged a certain fee for each reverse billing SMS message received. The fee will either be included in the monthly mobile phone bill or be deducted from prepaid card credits.

11.3.3 Downloading

SMS messages can carry binary data and so SMS can be used as the transport medium of wireless downloads. Objects such as ringtones, wallpapers, pictures and operator logos can be encoded in one or more SMS messages depending on the object's size. Like information services, wireless download services are usually not free and reverse billing SMS is a common way used by content providers to bill their customers. The object to be downloaded is encoded in one or more reverse billing SMS messages. The mobile user who requests the object will be charged a certain fee for each reverse billing SMS message received. If the mobile user is using a monthly mobile phone service plan, the download fee will be included in his/her next monthly bill; if the mobile user is using a prepaid SIM card, the download fee will be deducted from the prepaid credits.

11.3.4 Alerts and Notifications

SMS is a very suitable technology for delivering alerts and notifications of important events. This is because of two reasons:

A mobile phone is a device that is carried by its owner most of the time. Whenever an SMS text message is received, the mobile phone will notify you by giving out a sound or by vibrating. You can check what the SMS text message contains immediately.

Notes

SMS technology allows the "push" of information. This is different from the "pull" model where a device has to poll the server regularly in order to check whether there is any new information. The "pull" model is less suitable for alert and notification applications, since it wastes bandwidth and increases server load.

Some common SMS alert and notification applications are described below.

1. ***Email, Fax and Voice Message Notifications:*** In an email notification system, a server sends a text message to the user's mobile phone whenever an email arrives in the inbox. The SMS text message can include the sender's email address, the subject and the first few lines of the email body. An email notification system may allow the user to customize various filters so that an SMS alert is sent only if the email message contains certain keywords or if the email sender is an important person. The use cases for fax or voice message are similar.
2. ***E-commerce and Credit Card Transaction Alerts:*** Whenever an e-commerce or credit card transaction is made, the server sends a text message to the user's mobile phone. The user can know immediately whether any unauthorized transactions have been made.
3. ***Stock Market Alerts:*** In a stock market alert application, a program is constantly monitoring and analysing the stock market. If a certain condition is satisfied, the program will send a text message to the user's mobile phone to notify him/her of the situation. For example, you can configure the alert system such that if the stock price of a company is lower than a certain value or drops by a certain percentage, it will send an SMS alert to you.
4. ***Remote System Monitoring:*** In a remote system monitoring application, a program (sometimes with the help of a group of sensors) is constantly monitoring the status of a remote system. If a certain condition is satisfied, the program will send a text message to the system administrator to notify him/her of the situation.

Example: A program may be written to "ping" a server regularly. If no response is received from the server, the program can send an SMS alert to the system administrator to notify him/her that the server may be hanged.

11.3.5 Two-way Interactive Text Messaging Applications

SMS messaging technology can be used as the underlying communication medium between wireless devices and servers in a two-way interactive text messaging application. For example, search engines are two-way interactive text messaging applications. Let's say there is a dictionary search engine that supports queries in SMS text messages. It may operate like this:

To find out the meaning of the term "SMS text messaging", you can type "find: SMS text messaging" in an SMS text message and send it to the search engine's phone number. After receiving your SMS text message, the search engine parses it and finds that it begins with the command "find" and follows by the words "SMS text messaging". The search engine then knows you want to find out the meaning of the term "SMS text messaging". So, it sends a text message, which contains the meaning of the term "SMS text messaging", back to your mobile phone.

If the search result is very long and it cannot contain within a single SMS text message, the search engine adds "Page 1 of 2", "Page 1 of 3", etc., at the end of the reply SMS text message. The search engine also creates a session using your mobile phone number as the session ID and stores the term that you searched for (i.e. "SMS text messaging") in the session object.

To request the second page, you can send a text message with the content "page: 2" to the search engine's phone number. After receiving your SMS text message, the search engine parses it and finds that it begins with the command "page" and follows by "2". The search engine then knows you want the second page of the search result. It retrieves the term that you searched for last time from the session object and finds that it is "SMS text messaging". The search engine then sends a text message that contains the second page of the search result for the term “SMS text messaging” back to your mobile phone.

Many other two-way interactive text messaging applications can be built using a similar way. For example, a company may want to build an SMS messaging application to enable its employees to query the corporate database while they are working outdoors.

Task Critically examine the types of user devices are most common with wireless WANs.

Self Assessment

State whether the following statements are true or false:

11. SMS stands for Small Message Service.
12. The GSM and SMS standards were originally developed by ETSI.
13. SMS messages can carry binary data.
14. A mobile phone is a device that is carried by its owner most of the time.
15. SMS is a not suitable technology for delivering alerts and notifications.

Case Study

A Case Study in High-Speed Wireless WAN

Increasingly, county governments need systems that allow all branches of public service – from courthouses and police stations to public schools and emergency services – to share information quickly and efficiently. This is particularly important for rural counties, which have historically been extremely decentralized. With the help of Motorola’s wireless solutions, Orange County, Virginia is on its way to providing services to all its businesses and residents.

Orange County

Located 55 miles southwest of Washington, D.C. and 72 miles northwest of Richmond, Virginia, historical Orange County is a rural community with rolling landscapes and spectacular views of the Blue Ridge Mountains. Founded in 1734, the County’s diversified economy and location make it ideal for business and industry, and its nearly 354 square miles are home to more than 32,000 residents.

Advanced Network Systems

Advanced Network Systems, Inc., headquartered in Charlottesville, Virginia, was selected to provide design and implementation services for the county-wide project. The Company specializes in advanced wireless WAN communication technologies and was responsible for furnishing all systems consulting, engineering, procurement, deployment, systems support and maintenance services.

Situation and Challenge

Faced with performance limitations and infrastructure inefficiencies, multiple Orange County government agencies collaborated to create a high-speed wireless network that would provide a county-wide Local Area Network (LAN), a Wide Area Network (WAN)

Contd...

for each designated government entity and public school, a Metropolitan Area Network (MAN) for inter-governmental connectivity, and a shared infrastructure for Internet access.

Upon review, Orange County found that the wire-line solutions it used in the past were cost prohibitive and that certain locations were too distant to establish connectivity. In addition to spanning a large geographical area that contains many obstructions, Orange County faced a number of technological and logistical challenges associated with their existing network. These included limited intra- and inter-governmental connectivity, an inability to share resources and offer consolidated access to high-speed Internet services, inadequate broadband capacity for new applications, and disparate data and voice systems. The County also required reliable support for a wide range of bandwidth-intensive applications, such as voice-over-Internet Protocol (VoIP), geographic information systems (GIS), video conferencing, video surveillance and distance learning.

Technical Requirements

1. Support for a wide range of applications, including real-time streaming video and IP telephony Ability to operate emergency services from alternative sites
2. High data rates of at least 10 Mbps
3. Ease of management and maintenance
4. Ability to use existing tower structures within the County
5. Stability in obstructed paths and high-interference environments
6. High security to protect sensitive government information over a broadband network
7. Design for future backbone redundancy

Deployment Detail and Interoperability

Utilizing systems that operate in the 5.8 GHz band, Orange County deployed Motorola's wi4 Fixed Point-to-Point (PTP) 400 and 600 Series Wireless Ethernet Bridges to connect 24 locations including administration offices, public schools, the courthouse, the airport, and police and emergency services.

The County used the Motorola PTP 600 Series radios to construct a subscriber-access backbone that extends over 30 miles. To overcome radio frequency interference challenges and path obstructions, Connectorized models with drum antennas were deployed. The radios were mounted on the County's existing tower structures, making it easier to expand the network.

User networks are segmented via high-performance Ethernet switches with virtual LAN and access control points. The same network solution also supplies all government entities with Internet connectivity from a 45 Mbps DS-3 link. A security platform that includes firewall appliances, VLANs, global anti-virus, content filtering and bandwidth management applications is deployed at each network entry point to protect sensitive government data. Large users, such as the public schools, utilize Motorola PTP 400 Series radios with integrated antennas to provide data rates of at least 18 Mbps, exceeding the County's expectations. Smaller subscriber sites, such as the Orange County courthouse, use four-cell Motorola Canopy solutions.

After successful completion of the initial phase, the project was expanded to include many fire and rescue locations, allowing E-911 to print dispatch reports at the fire and rescue stations. E-911 sends the dispatch report to the printer located at the fire and rescue stations that have connectivity.

Contd...

Notes

Results

To date, the wireless solution designed by Advanced Network Systems with the Motorola PTP 400 and PTP 600 Series radios has proven to be an extremely reliable, high-performance, converged voice and data network. Paired with the County's existing VoIP communication system, the solution effectively deploys telephony services at every government facility. Agencies immediately took advantage of computer management for e-mail, anti-virus control, file sharing and Internet services such as online Standards of Learning (SOL) testing capabilities for the County's public schools. Plus, specialized services have been added, including video surveillance at the airport and E-911 information applications for police, fire and rescue departments. Substantial cost savings and ROI have resulted from the removal of analog voice lines that previously existed throughout the County's system.

Later, the County added redundancy to its backbone for traffic re-routing. They have plans to connect three public libraries and two more emergency services locations. Other future plans may include the implementation of mobile data connectivity for emergency services enabled through the wireless network.

Why Motorola?

1. Secure, reliable wireless connectivity for rural communities across 24 diverse government entities
2. Ability to implement new and innovative applications such as IP telephony, GIS, video conferencing, video surveillance and distance learning
3. Substantial cost savings and immediate ROI benefits
4. Network expansion that easily accommodates future growth

About Motorola

Motorola, a Fortune 100 company, is known around the world for innovation and leadership in wireless and broadband communications. Inspired by our vision of seamless mobility, the people of Motorola are committed to helping you connect simply and seamlessly to the people, information, and entertainment that you want and need. We do this by designing and delivering "must have" products, "must do" experiences and powerful networks — along with a full complement of support services.

About Advanced Network Systems, Inc.

Advanced Network Systems specializes in the design, installation and support of information technology solutions. The company's expertise covers a wide variety of IT applications, including network security, virtualization, managed IT services, core infrastructure, networked storage, and wireless, as well as IP-based telephone and conferencing systems. With multiple locations, serving Virginia and West Virginia, Advanced Network Systems supports a diverse base of clients, including small and medium-sized businesses, government agencies, and educational institutions.

Questions:

1. Discuss various challenges faced by the Orange Country.
2. Discuss the benefits of using Motorola wireless solutions.

Source: http://www.getadvanced.net/wirelesswancasestudy

11.4 Summary

Notes

- A Wide Area Network (WAN) is a communication network made up of computers that are non-local to one another, exchanging data across a wide area or great distance.
- Computers interoperate on a WAN network by using a set of standards or protocols for communication.
- Wireless WANs satisfy both mobile and stationary applications.
- Packet radio WANs function much like a wired packet switching wide area network.
- Packet radio WAN users connect to their computers a packet radio modem with an omnidirectional antenna.
- PCS is a fully digital version of cellular wireless that uses very small cells called microcells.
- An antenna can increase the power of the radio signal so that it can travel farther.
- Cellular phones currently transmit at about 14.4 Kbps but the technology, and speed is improving rapidly.
- Cellular technology was developed to overcome the problem of more and more people using mobile phones.
- Satellites that orbit the Earth at an altitude of 22,237 miles revolve around the Earth at the same speed that the Earth rotates.
- Meteor burst communications (MBC), also referred to as meteor scatter communications, is a radio propagation mode that exploits the ionized trails of meteors during atmospheric entry to establish brief communications paths between radio stations up to 2,250 kilometres (1,400 mi) apart.
- SMS is a technology that enables the sending and receiving of messages between mobile phones.

11.5 Keywords

Antennae: An antenna (or aerial) is an electrical device which converts electric power into radio waves, and vice versa.

Directional Antenna: A directional antenna concentrates its power in a certain direction and therefore has higher gain.

Internet Protocol (IP) address: An Internet Protocol address (IP address) is a numerical label assigned to each device (e.g., computer, printer) participating in a computer network that uses the Internet Protocol for communication.

Internetwork: When networks connect to form a bigger network (a bigger WAN), the resulting network is called an internetwork.

Meteor burst communications: Meteor burst communications (MBC), also referred to as meteor scatter communications, is a radio propagation mode that exploits the ionized trails of meteors during atmospheric entry to establish brief communications paths between radio stations up to 2,250 kilometres (1,400 mi) apart.

Omnidirectional Antenna: An omnidirectional antenna transmits radio waves in all directions. Its gain is equal to one, also called unity gain.

Personal Area Network (PAN): A Personal Area Network (PAN) is created by Bluetooth technology to wirelessly link personal devices together for interoperability.

Notes

Personal Communications Services (PCS): PCS is a wireless phone service similar to cellular telephone service but emphasizing personal service and extended mobility.

Satellites: An artificial body placed in orbit around the earth or another planet in order to collect information or for communication.

Short Message Service: It is a technology that enables the sending and receiving of messages between mobile phones.

Virtual Private Network (VPN): A VPN is a network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network.

Wide Area Network(WAN): A WAN is a communication network made up of computers that are non-local to one another, exchanging data across a wide area or great distance.

11.6 Review Questions

1. Define WAN.
2. Do you think that a LAN can also become a WAN? If yes, give reason with example.
3. What is Packet Radio WANs?
4. Discuss the types of Antennae.
5. Explain Cellular Digital Packet Data (CFPD).
6. Highlight the uses of cellular system.
7. Write brief note on Space-based Wireless WANs.
8. Describe Meteor burst communications.
9. "Person-to-person text messaging is the most commonly used SMS application." Elucidate.
10. Explain some common SMS alert and notification applications.

Answers: Self Assessment

1. True
2. False
3. True
4. False
5. False
6. Radio Waves
7. Frequency Reuse
8. Cell
9. Satellites
10. LEO
11. False
12. True
13. True
14. True
15. False

11.7 Further Readings

Books

Glisic, Savo & Lorenzo, Beatriz (2009). "*Advanced Wireless Networks: Cognitive, Cooperative & Opportunistic 4G Technology*." John Wiley & Sons.

Notes

Golmie. "*Coexistence in Wireless Networks.*" Cambridge University Press.

Pan, Yi & Xiao, Yang (2005). "*Design and Analysis of Wireless Networks.*" Nova Publishers.

Rackley, Steve (2011). "*Wireless Networking Technology: From Principles to Successful Implementation.*" Elsevier.

Stojmenovic (2006). "*Handbook of Wireless Networks & Mobile Computing.*" John Wiley & Sons.

Syngress (2001). "*Designing A Wireless Network*". Syngress.

Online links

http://voip.about.com/od/voipbasics/g/whatisWAN.htm

http://etutorials.org/Networking/wn/Chapter+7.+Wireless+WANs+Networks+for+Worldwide+Connections/Wireless+WAN+Systems/

http://www.wisegeek.com/what-is-a-wan-network.htm

http://k-12.pisd.edu/currinst/network/11_806A_4-2_SG.pdf

https://www.usenix.org/legacy/event/bsdcon03/tech/pozar.pdf

Notes

Unit 12: Space-based Wireless WANs

CONTENTS

Objectives

Introduction

12.1 Satellites

12.1.1 Evolution of Communication Satellites

12.1.2 How Satellites Work?

12.1.3 Satellite Applications

12.1.4 The Future of Satellite Communication

12.1.5 Orbits for Communication Satellite

12.2 Meteor Burst Communications (MBC)

12.2.1 Historical Overview

12.2.2 Basic Characteristics

12.2.3 Meteor Burst Communication Basics

12.2.4 Meteor Burst Communication Network Applications

12.2.5 Principles of Meteor Burst Communication

12.2.6 The Meteor Burst Communication (MBC) Network

12.2.7 Meteor Scatter

12.2.8 Future Developments

12.3 Summary

12.4 Keywords

12.5 Review Questions

12.6 Further Readings

Objectives

After studying this unit, you will be able to:

- Discuss the concept of Satellite and how it works
- Describe the evolution and applications of MBC.
- Identify the future of Satellite Communication
- Explain the Orbits for Communication Satellite
- Define concept of Meteor Burst Communications and its characteristics
- Discuss the Meteor Burst Communication Network Applications and Principles
- Identify the Meteor Burst Communication (MBC) Network
- Explain the concept of Meteor Scatter

Introduction

Today's satellite operators are planning to be in the business for the long-term. Providers are investing heavily in developing new platforms capable of carrying large communication payloads. A satellite is basically any object that revolves around a planet in a circular or elliptical path. Although anything that is in orbit around Earth is technically a satellite, the term "satellite" is typically used to describe a useful object placed in orbit purposely to perform some specific mission or task. Meteor burst communication is a way of communicating using the ionized trails made by meteors as they enter the earth's atmosphere. It is also called Meteor scatter communication. The Earth encounters thousands of tiny bits of meandering space debris (rock, sand) every day. The number, and perhaps the average size, of these particles increases sharply during meteor showers, but there is significant meteor activity almost every day.

12.1 Satellites

A satellite is basically a self-contained communications system with the ability to receive signals from Earth and to retransmit those signals back with the use of a transponder—an integrated receiver and transmitter of radio signals. A satellite has to withstand the shock of a launch into orbit at 28,100 km (17,500 miles) an hour and a hostile space environment where it can be subject to radiation and extreme temperatures for its projected operational life, which can last up to 20 years. In addition, satellites have to be light, as the cost of launching a satellite is quite expensive and based on weight. To meet these challenges, satellites must be small and made of lightweight and durable materials. They must operate at a very high reliability of more than 99.9 percent in the vacuum of space with no prospect of maintenance or repair.

Satellite communication, in telecommunications, the use of artificial satellites to provide communication links between various points on Earth. Satellite communications play a vital role in the global telecommunications system.

Did u know? Approximately 2,000 artificial satellites orbiting Earth relay analog and digital signals carrying voice, video, and data to and from one or many locations worldwide.

The main components of a satellite consist of the communications system, which includes the antennas and transponders that receive and retransmit signals, the power system, which includes the solar panels that provide power, and the propulsion system, which includes the rockets that propel the satellite. A satellite needs its own propulsion system to get itself to the right orbital location and to make occasional corrections to that position. A satellite in geostationary orbit can deviate up to a degree every year from north to south or east to west of its location because of the gravitational pull of the Moon and Sun. A satellite has thrusters that are fired occasionally to make adjustments in its position. The maintenance of a satellite's orbital position is called "station keeping," and the corrections made by using the satellite's thrusters are called "attitude control." A satellite's life span is determined by the amount of fuel it has to power these thrusters. Once the fuel runs out, the satellite eventually drifts into space and out of operation, becoming space debris.

A satellite in orbit has to operate continuously over its entire life span. It needs internal power to be able to operate its electronic systems and communications payload. The main source of power is sunlight, which is harnessed by the satellite's solar panels. A satellite also has batteries on board to provide power when the Sun is blocked by Earth.

Caution The batteries are recharged by the excess current generated by the solar panels when there is sunlight.

12.1.1 Evolution of Communication Satellites

In 500 years, when humankind looks back at the dawn of space travel, Apollo's landing on the Moon in 1969 may be the only event remembered. At the same time, however, Lyndon B. Johnson, himself an avid promoter of the space program, felt that reconnaissance satellites alone justified every penny spent on space. Weather forecasting has undergone a revolution because of the availability of pictures from geostationary meteorological satellites – pictures we see every day on television. All of these are important aspects of the space age, but satellite communications has probably had more effect than any of the rest on the average person. Satellite communications is also the only truly commercial space technology – generating billions of dollars annually in sales of products and services.

The Billion Dollar Technology

In fall of 1945 an RAF electronics officer and member of the British Interplanetary Society, Arthur C. Clarke, wrote a short article in Wireless World that described the use of manned satellites in 24-hour orbits high above the world's land masses to distribute television programs. His article apparently had little lasting effect in spite of Clarke's repeating the story in his 1951/52 The Exploration of Space . Perhaps the first person to carefully evaluate the various technical options in satellite communications and evaluate the financial prospects was John R. Pierce of AT&T's Bell Telephone Laboratories who, in a 1954 speech and 1955 article, elaborated the utility of a communications "mirror" in space, a medium-orbit "repeater" and a 24-hour-orbit "repeater." In comparing the communications capacity of a satellite, which he estimated at 1,000 simultaneous telephone calls, and the communications capacity of the first transatlantic telephone cable (TAT-1), which could carry 36 simultaneous telephone calls at a cost of 30–50 million dollars, Pierce wondered if a satellite would be worth a billion dollars.

In 1960 AT&T filed with the Federal Communications Commission (FCC) for permission to launch an experimental communications satellite with a view to rapidly implementing an operational system. The U.S. government reacted with surprise – there was no policy in place to help execute the many decisions related to the AT&T proposal. By the middle of 1961, NASA had awarded a competitive contract to RCA to build a medium-orbit (4,000 miles high) active communication satellite (RELAY); AT&T was building its own medium-orbit satellite (TELSTAR) which NASA would launch on a cost-reimbursable basis; and NASA had awarded a sole- source contract to Hughes Aircraft Company to build a 24-hour (20,000 mile high) satellite (SYNCOM).

By 1964, two TELSTARs, two RELAYs, and two SYNCOMs had operated successfully in space. This timing was fortunate because the Communications Satellite Corporation (COMSAT), formed as a result of the Communications Satellite Act of 1962, was in the process of contracting for their first satellite. COMSAT's initial capitalization of 200 million dollars was considered sufficient to build a system of dozens of medium-orbit satellites. For a variety of reasons, including costs, COMSAT ultimately chose to reject the joint AT&T/RCA offer of a medium-orbit satellite incorporating the best of TELSTAR and RELAY. They chose the 24-hour-orbit (geosynchronous) satellite offered by Hughes Aircraft Company for their first two systems and a TRW geosynchronous satellite for their third system.

Did u know? On April 6, 1965 COMSAT's first satellite, EARLY BIRD, was launched from Cape Canaveral. Global satellite communications had begun.

The Global Village: International Communications

Some glimpses of the Global Village had already been provided during experiments with TELSTAR, RELAY, and SYNCOM. These had included televising parts of the 1964 Tokyo Olympics. Although COMSAT and the initial launch vehicles and satellites were American, other countries had been involved from the beginning. AT&T had initially negotiated with its European telephone cable "partners" to build earth stations for TELSTAR experimentation. NASA had expanded these negotiations to include RELAY and SYNCOM experimentation. By the time EARLY BIRD was launched, communications earth stations already existed in the United Kingdom, France, Germany, Italy, Brazil, and Japan. Further negotiations in 1963 and 1964 resulted in a new international organization, which would ultimately assume ownership of the satellites and responsibility for management of the global system. On August 20, 1964, agreements were signed which created the International Telecommunications Satellite Organization (INTELSAT).

By the end of 1965, EARLY BIRD had provided 150 telephone "half- circuits" and 80 hours of television service. The INTELSAT II series was a slightly more capable and longer-lived version of EARLY BIRD. Much of the early use of the COMSAT/INTELSAT system was to provide circuits for the NASA Communications Network (NASCOM). The INTELSAT III series was the first to provide Indian Ocean coverage to complete the global network. This coverage was completed just days before one half billion people watched APOLLO 11 land on the moon on July 20, 1969.

From a few hundred telephone circuits and a handful of members in 1965, INTELSAT has grown to a present-day system with more members than the United Nations and the capability of providing hudreds of thousands of telephone circuits.

Notes Cost to carriers per circuit has gone from almost $100,000 to a few thousand dollars. Cost to consumers has gone from over $10 per minute to less than $1 per minute. If the effects of inflation are included, this is a tremendous decrease. INTELSAT provides services to the entire globe, not just the industrialized nations.

Hello Guam: Domestic Communications

In 1965, ABC proposed a domestic satellite system to distribute television signals. The proposal sank into temporary oblivion, but in 1972 TELESAT CANADA launched the first domestic communications satellite, ANIK, to serve the vast Canadian continental area. RCA promptly leased circuits on the Canadian satellite until they could launch their own satellite. The first U.S. domestic communications satellite was Western Union's WESTAR I, launched on April 13, 1974. In December of the following year RCA launched their RCA SATCOM F- 1. In early 1976 AT&T and COMSAT launched the first of the COMSTAR series. These satellites were used for voice and data, but very quickly television became a major user. By the end of 1976 there were 120 transponders available over the U.S., each capable of providing 1500 telephone channels or one TV channel. Very quickly the "movie channels" and "super stations" were available to most Americans. The dramatic growth in cable TV would not have been possible without an inexpensive method of distributing video.

The ensuing two decades have seen some changes: Western Union is no more; Hughes is now a satellite operator as well as a manufacturer; AT&T is still a satellite operator, but no longer in partnership with COMSAT; GTE, originally teaming with Hughes in the early 1960s to build and operate a global system is now a major domestic satellite operator. Television still dominates domestic satellite communications, but data has grown tremendously with the advent of very small aperture terminals (VSATs). Small antennas, whether TV-Receive Only (TVRO) or VSAT are a commonplace sight all over the country.

New Technology

The first major geosynchronous satellite project was the Defense Department's ADVENT communications satellite. It was three-axis stabilized rather than spinning. It had an antenna that directed its radio energy at the earth. It was rather sophisticated and heavy. At 500–1000 pounds it could only be launched by the ATLAS-CENTAUR launch vehicle. ADVENT never flew, primarily because the CENTAUR stage was not fully reliable until 1968, but also because of problems with the satellite. When the program was cancelled in 1962 it was seen as the death knell for geosynchronous satellites, three-axis stabilization, the ATLAS-CENTAUR, and complex communications satellites generally. Geosynchronous satellites became a reality in 1963, and became the only choice in 1965. The other ADVENT characteristics also became commonplace in the years to follow.

In the early 1960s, converted intercontinental ballistic missiles (ICBMs) and intermediate range ballistic missiles (IRBMs) were used as launch vehicles. These all had a common problem: they were designed to deliver an object to the earth's surface, not to place an object in orbit. Upper stages had to be designed to provide a delta-Vee (velocity change) at apogee to circularize the orbit. The DELTA launch vehicles, which placed all of the early communications satellites in orbit, were THOR IRBMs that used the VANGUARD upper stage to provide this delta-Vee. It was recognized that the DELTA was relatively small and a project to develop CENTAUR, a high-energy upper stage for the ATLAS ICBM, was begun. ATLAS-CENTAUR became reliable in 1968 and the fourth generation of INTELSAT satellites used this launch vehicle. The fifth generation used ATLAS-CENTAUR and a new launch-vehicle, the European ARIANE. Since that time other entries, including the Russian PROTON launch vehicle and the Chinese LONG MARCH have entered the market. All are capable of launching satellites almost thirty times the weight of EARLY BIRD.

In the mid-1970s several satellites were built using three-axis stabilization. They were more complex than the spinners, but they provided more despun surface to mount antennas and they made it possible to deploy very large solar arrays. The greater the mass and power, the greater the advantage of three-axis stabilization appears to be. Perhaps the surest indication of the success of this form of stabilization was the switch of Hughes, closely identified with spinning satellites, to this form of stabilization in the early 1990s. The latest products from the manufacturers of SYNCOM look quite similar to the discredited ADVENT design of the late 1950s.

Much of the technology for communications satellites existed in 1960, but would be improved with time. The basic communications component of the satellite was the travelling-wave-tube (TWT). These had been invented in England by Rudoph Kompfner, but they had been perfected at Bell Labs by Kompfner and J. R. Pierce. All three early satellites used TWTs built by a Bell Labs alumnus. These early tubes had power outputs as low as 1 watt. Higher-power (50–300 watts) TWTs are available today for standard satellite services and for direct-broadcast applications. An even more important improvement was the use of high-gain antennas. Focusing the energy from a 1-watt transmitter on the surface of the earth is equivalent to having a 100-watt transmitter radiating in all directions. Focusing this energy on the Eastern U.S. is like having a 1000-watt transmitter radiating in all directions. The principal effect of this increase in actual and effective power is that earth stations are no longer 100-foot dish reflectors with cryogenically-cooled maser amplifiers costing as much as $10 million (1960 dollars) to build. Antennas for normal satellite services are typically 15-foot dish reflectors costing $30,000 (1990 dollars). Direct-broadcast antennas will be only a foot in diameter and cost a few hundred dollars.

Mobile Services

In February of 1976 COMSAT launched a new kind of satellite, MARISAT, to provide mobile services to the United States Navy and other maritime customers. In the early 1980s the Europeans launched the MARECS series to provide the same services. In 1979 the UN International Maritime Organization sponsored the establishment of the International Maritime Satellite Organization (INMARSAT) in a manner similar to INTELSAT. INMARSAT initially leased the MARISAT and MARECS satellite transponders, but in October of 1990 it launched the first of its own satellites, INMARSAT II F-1. The third generation, INMARSAT III, has already been launched.

An aeronautical satellite was proposed in the mid-1970s. A contract was awarded to General Electric to build the satellite, but it was cancelled. INMARSAT now provides this service. Although INMARSAT was initially conceived as a method of providing telephone service and traffic-monitoring services on ships at sea, it has provided much more. The journalist with a briefcase phone has been ubiquitous for some time, but the Gulf War brought this technology to the public eye.

The United States and Canada discussed a North American Mobile Satellite for some time. In the next year the first MSAT satellite, in which AMSC (U.S.) and TMI (Canada) cooperate, will be launched providing mobile telephone service via satellite to all of North America.

Example: Mobile Satellite Communications Operator Inmarsat.

Inmarsat was the world's first global mobile satellite communications operator, founded in the late 1970s. It focuses on communications services to maritime, land-mobile, aeronautical and other users. Inmarsat now supports links for phone, fax and data communications at up to 64 Kbps to more than 210,000 ship, vehicle, aircraft and portable terminals.

The range of Inmarsat systems includes mobile terminals from handhelds to consoles, with easy set-up mechanisms that allow users wherever they are to connect via a global fleet of geostationary Inmarsat satellites to the terrestrial communications network and to carry out telephone conversations, data transfers, and increasingly multimedia applications and Internet access. Inmarsat is aimed at professionals who need a reliable communications system wherever they are: ship owners and managers, journalists and broadcasters, health and disaster-relief workers, land transport fleet operators, airlines, airline passengers and air traffic controllers, government workers, national emergency and civil defence agencies, and peacekeeping forces. The cost is rather high while the capacity is still rather limited: voice/fax/data systems achieve a maximum data rate of 64 Kbps at connection costs starting at almost US$ 3 per minute. Dedicated mobile IP systems can achieve a maximum download speed of up to 144 Kbps.

Prospect and Retrospect

Arthur C. Clarke's 1945 vision was of a system of three "manned" satellites located over the major land masses of the earth and providing direct-broadcase television. The inherent "broadcast" nature of satellite communications has made direct-broadcast a recurrent theme – yet one never brought to fruition. The problems are not technical – they are political, social, and artistic. What will people be willing to pay for? This is the question – especially with the availability of 120-channel cable systems. Hughes is apparently about to enter this field and may encourage others to do the same. Only then will Clarke's prophetic vision be fulfilled.

There are currently six companies providing fixed satellite service to the U.S.: GE Americom, Alascom, AT&T, COMSAT, GTE, and Hughes Communications. They operate 36 satellites with a net worth of over four billion dollars. The ground stations which communicate with these satellites are innumerable and may have a similar net worth. INTELSAT has had competition in the international market from Pan American Satellite since 1986. Orion Satellite is expected to begin international service in 1994. Since Canada began domestic satellite service in 1972, that country has been joined by the United States (1974), Indonesia (1976), Japan (1978), India (1982), Australia (1985), Brazil (1985), Mexico (1985), and many others. Each year from 10–20 communications satellites are launched valued at about $75 million each. The launch vehicles placing them in orbit have similar values. Both satellites and launch vehicles are multi-billion dollar businesses. The earth station business is equally large. Finally the communications services themselves are multi-billion dollar businesses. John R. Pierce was right – it would be worth a billion dollars.

12.1.2 How Satellites Work?

Not so long ago, satellites were exotic, top-secret devices. They were used primarily in a military capacity, for activities such as navigation and espionage. Now they are an essential part of our daily lives. We see and recognize their use in weather reports, television transmission by DIRECTV and the DISH Network, and everyday telephone calls. In many other instances, satellites play a background role that escapes our notice:

- Some newspapers and magazines are more timely because they transmit their text and images to multiple printing sites via satellite to speed local distribution.
- Before sending signals down the wire into our houses, cable television depends on satellites to distribute its transmissions.
- The most reliable taxi and limousine drivers are sometimes using the satellite-based Global Positioning System (GPS) to take us to the proper destination.
- The goods we buy often reach distributors and retailers more efficiently and safely because trucking firms track the progress of their vehicles with the same GPS. Sometimes firms will even tell their drivers that they are driving too fast.
- Emergency radio beacons from downed aircraft and distressed ships may reach search-and-rescue teams when satellites relay the signal.

Did u know? **Business Radio and TV**

Narrowcasting or business TV and radio is a term used for satellite broadcasters who use transmission time to reach a very specific audience. Technically speaking, there is no difference with broadcast satellite TV applications described in the previous section. Digital television has made it possible to distribute information within organisations and companies that are geographically dispersed, or to deliver distance education. Similarly, digital radio allows for the delivery of radio services to relatively small closed user groups.

MPEG-2/DVB technology is the dominant standard for digital television, but other computer-based media coding techniques (such as MPEG-1, Real Video, etc.) are also used to embed video and/or audio into data streams, often integrated with other multimedia or Internet services. Transmission via satellite requires there to be digital receivers available at relatively low prices on the consumer market. The advantage is that more advanced or popular audio coding techniques (for example MP3) can also be used and that the same stream can be used for other applications, such as data distribution, outside broadcast hours.

12.1.3 Satellite Applications

Advances in satellite technology have given rise to a healthy satellite services sector that provides various services to broadcasters, Internet service providers(ISPs), governments, the military, and other sectors. There are three types of communication services that satellites provide: telecommunications, broadcasting, and data communications. Telecommunication services include telephone calls and services provided to telephone companies, as well as wireless, mobile, and cellular network providers.

Broadcasting services include radio and television delivered directly to the consumer and mobile broadcasting services. DTH, or satellite television, services (such as the DirecTV and DISH Network services in the United States) are received directly by households. Cable and network programming is delivered to local stations and affiliates largely via satellite. Satellites also play an important role in delivering programming to cell phones and other mobile devices, such as personal digital assistants and laptops.

Data communications involve the transfer of data from one point to another. Corporations and organizations that require financial and other information to be exchanged between their various locations use satellites to facilitate the transfer of data through the use of very small-aperture terminal (VSAT) networks. With the growth of the Internet, a significant amount of Internet traffic goes through satellites, making ISPs one of the largest customers for satellite services.

Satellite communications technology is often used during natural disasters and emergencies when land-based communication services are down. Mobile satellite equipment can be deployed to disaster areas to provide emergency communication services.

One major technical disadvantage of satellites, particularly those in geostationary orbit, is an inherent delay in transmission. While there are ways to compensate for this delay, it makes some applications that require real-time transmission and feedback, such as voice communications, not ideal for satellites.

Satellites face competition from other media such as fibre optics, cable, and other land-based delivery systems such as microwaves and even power lines. The main advantage of satellites is that they can distribute signals from one point to many locations. As such, satellite technology is ideal for "point-to-multipoint" communications such as broadcasting. Satellite communication does not require massive investments on the ground—making it ideal for underserved and isolated areas with dispersed populations.

Satellites and other delivery mechanisms such as fibre optics, cable, and other terrestrial networks are not mutually exclusive. A combination of various delivery mechanisms may be needed, which has given rise to various hybrid solutions where satellites can be one of the links in the chain in combination with other media. Ground service providers called "teleports" have the capability to receive and transmit signals from satellites and also provide connectivity with other terrestrial networks.

Example: Satellite transmission technologies can be used to bring the signal that needs to be broadcast to the place where it can be processed and prepared for re-distribution, for example: to a broadcaster's main studio; to a number of cable-head end stations; to an Internet Service Provider where it can be injected into the Internet; or to a network of local Points-of-Presence for distribution in local networks. These links respond to the need for point-to-point and point-to-multipoint transmission and are often called a 'hop'. The signal can be digital or analogue and can include video, audio, data or multimedia.

12.1.4 The Future of Satellite Communication

In a relatively short span of time, satellite technology has developed from the experimental (Sputnik in 1957) to the sophisticated and powerful. Future communication satellites will have more onboard processing capabilities, more power, and larger-aperture antennas that will enable satellites to handle more bandwidth. Further improvements in satellites' propulsion and power systems will increase their service life to 20–30 years from the current 10–15 years. In addition, other technical innovations such as low-cost reusable launch vehicles are in development. With increasing video, voice, and data traffic requiring larger amounts of bandwidth, there is no dearth of emerging applications that will drive demand for the satellite services in the years to come. The demand for more bandwidth, coupled with the continuing innovation and development of satellite technology, will ensure the long-term viability of the commercial satellite industry well into the 21st century.

12.1.5 Orbits for Communication Satellite

There is only one main force acting on a satellite when it is in orbit, and that is the gravitational force exerted on the satellite by the Earth. This force is constantly pulling the satellite towards the centre of the Earth. A satellite doesn't fall straight down to the Earth because of its velocity. Throughout a satellites orbit there is a perfect balance between the gravitational force due to the Earth, and the centripetal force necessary to maintain the orbit of the satellite.

The formula for centripetal force is: $F = (mv^2)/r$

The formula for the gravitational force between two bodies of mass M and m is $(GMm)/r^2$

The most common type of satellite orbit is the geostationary orbit. This is described in more detail below, but is a type of orbit where the satellite is over the same point of Earth always. It moves around the Earth at the same angular speed that the Earth rotates on its axis.

We can use our formulae above to work out characteristics of the orbit.

$(mv^2/r) = (GMm)/r^2$

$\rightarrow v^2/r = (GM)/r^2$

Now, $v = (2\pi r)/T$.

$\rightarrow (((2\pi r)/T)^2)/r = (GM)/r^2$

$\rightarrow (4\pi^2 r)/T^2 = (GM)/r^2$

$\rightarrow r^3 = (GMT^2)/4\pi^2$

We know that T is one day, since this is the period of the Earth. This is 8.64×10^4 seconds. We also know that M is the mass of the Earth, which is 6×10^{24} kg.

Lastly, we know that G (Newton's Gravitational Constant) is 6.67×10^{-11} $m^3/kg.s^2$

So we can work out r.

$r^3 = 7.57 \times 10^{22}$

Therefore, $r = 4.23 \times 10^7 = 42{,}300$ km.

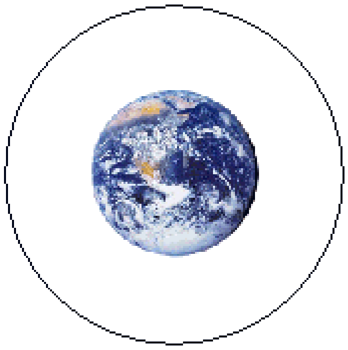
So the orbital radius required for a geostationary, or geosynchronous orbit is 42,300 km. Since the radius of the Earth is 6378 km the height of the geostationary orbit above the Earth's surface is ~36000 km.

There are many different types of orbits used for satellite telecommunications, the geostationary orbit described above is just one of them. Outlined below are the most commonly used satellite orbits. The orbits are sometimes described by their inclination – this is the angle between the orbital plane and the equatorial plane.

Geostationary Orbit

The most common orbit used for satellite communications is the geostationary orbit (GEO) (Figure 12.1). This is the orbit described above – the rotational period is equal to that of the Earth. The orbit has zero inclination so is an equatorial orbit (located directly above the equator). The satellite and the Earth move together so a GEO satellite appears as a fixed point in the sky from the Earth.

Figure 12.1: Diagram of Geostationary Orbit



Source: http://www.satcom.co.uk/article.asp?article=11

The advantages of such an orbit are that no tracking is required from the ground station since the satellite appears at a fixed position in the sky. The satellite can also provide continuous operation in the area of visibility of the satellite. Many communications satellites travel in geostationary orbits, including those that relay TV signals into our homes.

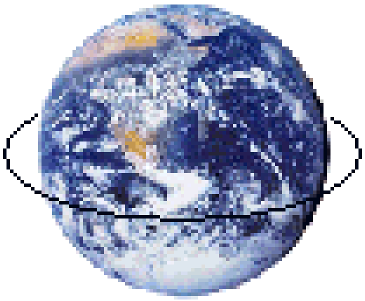
However, due to their distance from Earth GEO satellites have a signal delay of around 0.24 seconds for the complete send and receive path. This can be a problem with telephony or data transmission. Also, since they are in an equatorial orbit, the angle of elevation decreases as the latitude or longitude difference increases between the satellite and earth station. Low elevation angles can be a particular problem to mobile communications.

Low Earth Orbit/Medium Earth Orbit

A low earth orbit (LEO), or medium earth orbit (MEO) describes a satellite which circles close to the Earth. Generally, LEOs have altitudes of around 300–1000 km with low inclination angles, and MEOs have altitudes of around 10,000 km.

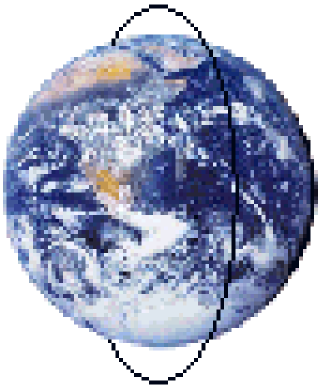
A special type of LEO (Figure 12.2) is the Polar Orbit. This is a LEO with a high inclination angle (close to 90 degrees). This means the satellite travels over the poles.

Figure 12.2: LEO Orbit



Source: http://www.satcom.co.uk/article.asp?article=11

Figure 12.3: Polar Orbit



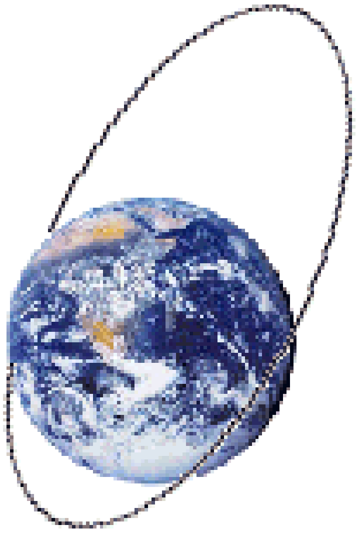
Source: http://www.satcom.co.uk/article.asp?article=11

Satellites that observe our planet such as remote sensing and weather satellites often travel in a highly inclined LEO so they can capture detailed images of the Earth's surface due to their closeness to Earth. A satellite in a Polar orbit (Figure 12.3) will pass over every region of Earth so can provide global coverage. Also a satellite in such an orbit will sometimes appear overhead (unlike a GEO which is only overhead to ground stations on the equator). This can enable communication in urban areas where obstacles such as tall buildings can block the path to a satellite. Lastly, the transmission delay is very small.

Any LEO or MEO system however, for continuous operation, requires a constellation of satellites. The satellites also move relative to the Earth so widebeam or tracking narrowbeam antennas are needed.

Elliptical Orbits

Figure 12.4: Diagram of Elliptical Orbits



Source: http://www.satcom.co.uk/article.asp?article=11

A satellite in elliptical orbit (Figure 12.4) follows an oval-shaped path. One part of the orbit is closest to the centre of Earth (perigee) and another part is farthest away (apogee). A satellite in this type of orbit generally has an inclination angle of 64 degrees and takes about 12 hours to circle the planet. This type of orbit covers regions of high latitude for a large fraction of its orbital period.

Task Critically examine the different applications of satellite TV viewing depending on the needs and objectives of the broadcaster or the viewers.

Self Assessment

State whether the following statements are true or false:

1. Satellites have to be light, as the cost of launching a satellite is quite cheap and based on weight.
2. Satellite communications play a vital role in the global telecommunications system.
3. By 1924, two TELSTARs, two RELAYs, and two SYNCOMs had operated successfully in space.

4. The EARLY BIRD series was a slightly more capable and longer-lived version of INTELSAT II.
5. In 1965, ABC proposed a domestic satellite system to distribute television signals.
6. The last major geosynchronous satellite project was the Defense Department's ADVENT communications satellite.
7. An aeronautical satellite was proposed in the mid-1970s.
8. A special type of LEO is the Polar Orbit.

12.2 Meteor Burst Communications (MBC)

Meteor Burst Communications use a form of radio communications system that is dependent on radio signals being scattered or reflected by meteor trails. Meteor burst communications is a specialized form of propagation that can be successfully used for radio communications over paths that extend up to 1500 or 2000 km. Meteor burst communication provides form of radio propagation that can be sued when no other form of radio propagation may be available.

Caution While data has to be transmitted in bursts and there may be delays, it provides a very useful form of non-real-time communications that can be used in many circumstances.

Seamless full-coverage communications technology offers the opportunity for immediate penetration of a multitude of potential high yield markets. The system can easily be linked to the fixed telephone network to send and receive e-mail in areas where there is no telephone cable in the ground. Interconnection with GSM networks to send and receive SMS messages in non-covered areas is also possible.

Government and commercial organizations in Africa are considering the use of the MBC system in rural areas for elections, education, spreading national news, population registration, payment of pensions, and remote reading of electricity meters. Additional serious options include tracking and tracing of trucks, trailers and railway wagons to optimise logistics and prevent theft.

12.2.1 Historical Overview

The fact that the ionized trails of meteors entering the earth's atmosphere can reflect the radio signal has been known since the early 1930s, when Pickard noticed that bursts of long distance, high frequency propagation occurred at times of major meteor showers. In 1935, Skellet found that when a meteor entered the earth's atmosphere, the denser air caused the meteor to heat up and eventually burn, creating an ionized trail which could be used to reflect a radio signal back to earth. Skellet postulates that the mechanism was reflection or scattering from electrons in meteor trail. During the World War II radio engineers observed meteor trail echoes, which were sometimes confused with incoming missiles.

It was not until after the war when radio technology had extended into the VHF and UHF bands that radio engineers became interested in the meteor scatter phenomena. From the 1950s, through the 1970s, meteor burst technology was studied and actual tests were conducted to determine the feasibility of using meteor trails. Some interesting information were found. Unfortunately, until the availability of integrated solid-state microcomputer, meteor burst communications was not considered practical except for slow-speed data system. The waiting time between meteor trails seemed too long for modern use.

A usable system became operational when Canada installed the JANET systems between Toronto and Port Arthur in the 1950s. Another one-way link was installed between Bozeman (Montana) and Stanford (California). In the late 1970s, the Alaska SNOTEL (SNOpacTELemetry) system was installed to provide meteorological information from remote locations through Alaska.

Notes

12.2.2 Basic Characteristics

Telecommunications systems developed to use meteor trails transmit data in bursts as intermittent meteor trails arrive for use; however, not all meteors create trails usable for communications. Though meteors of all sizes continuously are bombarding or being swept up by the Earth's atmosphere, their numbers, or frequency of occurrence, vary relative to their size. Those that create usable trails for propagating radio waves for effective beyond line of sight (BLOS) telecommunications are near a milligram in size. They collide with our atmosphere travelling thousands of miles per hour. At that velocity, friction causes them to heat up and vaporize. The vaporized atoms escaping from the surface of the meteor collide with those of the atmosphere, ionizing them and leaving trails of free electrons. This occurs at between 50 and 75 miles altitude. The trails range from 10 to 20 miles in length with a radius of close to a meter at the head, when created. However, they dissipate rapidly, generally within one half of a second, though some trails may last up to several seconds. The latter type is called an overdense trail, because the density of the free electrons is more than 1014 electrons per meter. Trails with less electron density are termed underdense. Overdense trails result from larger meteors and thereby are fewer in number and occur less frequently. When planning an MBC, system, communicators generally ignore overdense trails due to their lower frequency of occurrence.

Did u know? MBC, systems are designed around predicted availability of the larger numbers of underdense trails.

The trails are useful for telecommunications because they reflect radio waves back to the Earth's surface. The reflections occur in two ways, depending on whether the trail is overdense or underdense. Overdense trails are packed tightly enough to reflect radio waves in much the same manner as do layers of the ionosphere; however, underdense trails are less tightly packed, allowing penetration by the waves, which excites the free electrons and causes them to act as individual antennas reradiating the wave back to Earth in a scattering fashion. The reflection properties of meteor trails vary by frequency. Attenuation of waves radiating at frequencies above 50 MHz increases with the cube of the frequency. Thus, frequencies above 30 MHz but below 50 MHz, in the lower very high frequency (VHF) spectrum, propagate most efficiently using meteor trails. Also, radio waves of these frequencies travel in line of sight (LOS) paths. Thus, to be useful for communications between two points, the trail must be connected to both points through specular angles of reflection. That is, the signalling wave will be reflected at an angle equal to the angle of incidence of the transmitted RF wave and will travel in a straight LOS path.

Another MBC feature is the variation in numbers of meteor trails available to reflect radio waves. Two principal variations based on movements of the planet must be considered when planning an MBC system. As the Earth rotates toward the sun in the morning (meteors are moving away from the sun), it sweeps-up or overtakes meteors, thereby causing large numbers of trails. But in the evening hours, near sunset, when meteors must overtake the rotation of the planet, the overtaking trails are fewer. This phenomenon is called the diurnal variation, and its order of magnitude is approximately 4:1. Similarly, the nominal orbits of meteors are such that most intersect the Earth's orbit in the Northern Hemisphere in August and fewest in February. This seasonal variation is in the order of 3:1. Other variations, such as showers of meteors from specific points in the heavens, occur but are so infrequent that they are not useful for continuous communications.

MBC system planning should rely on meteors arriving sporadically and occurring at normal (Gaussian) frequency. This leads to reliance on statistical predictions and the use of models in identifying link parameters in MBC system designs. Accurate forecasting of meteor trail availability is critical to successful system design.

Optimization of MBC links to satisfy required performance parameters requires weighing and trading-off system design factors, such as operating frequency, antenna gain, transmitter power and receiver threshold levels. In the 1980s MBC systems provided an average throughput in the area of 75 to 100 words per minute (wpm), but careful system design using much more powerful microprocessors now available should produce orders of magnitude increases to that average performance level.

Performance requirements for MBC systems usually are stated relative to wait times (for message transmission) and information throughput time (user information transfer rate). Both of these are based on the arrival frequency and usable lifetime of trails. Thus, performance must be stated in terms of averages and it is customary to use daily average. Also, the performance requirement is identified relative to the type of telecommunications service to be provided. MBC has great flexibility in usable applications. Point-Multipoint and Multi-Single Point or Mesh-network configurations all are feasible services available from MBC systems.

A further significant characteristic of MBC systems, relative to their flexibility, is the connectivity range, covering both line-of-sight (LOS) and beyond LOS (BLOS). Unlike other BLOS systems, such as those using high frequency (HF) radio waves, the same VHF configuration used to communicate BLOS using meteor trails has the capability to provide connectivity to terminals within LOS range. This allows continuous geographic coverage, with some realignment of configuration, to almost 1,200 miles.

12.2.3 Meteor Burst Communication Basics

Meteor meteor burst radio communications relies on the fact that meteors continually enter the Earth’s atmosphere. As they do so they burn up leaving a trail of ionisation behind them. These trails which typically occur at altitudes between about 85 and 120 km can be used to “reflect” radio signals. In view of the fact that the ionisation trails left by the meteors are small, only minute amounts of the signal are reflected and this means that high powers coupled with sensitive receivers are often necessary.

Meteor scatter propagation uses the fact that vast numbers of meteors enter the Earth’s atmosphere. It is estimated that around 10^{12} meteors enter the atmosphere each day and these have a total weight of around 10^{6} grams.

Fortunately for everyone living below, the vast majority of these meteors are small, and are typically only the size of a grain of sand. It is found that the number of meteors entering the atmosphere is inversely proportional to their size. For a tenfold reduction in size, there is a tenfold increase in the number entering the atmosphere over a given period of time. From this it can be seen that very few large ones enter the atmosphere. Although most are burnt up in the upper atmosphere, there are a very few that are sufficiently large to survive entering the atmosphere and reach the earth.

12.2.4 Meteor Burst Communication Network Applications

A meteor burst communications system (MBCS) uses ionized meteor trails as a means of radio signal propagation. These trails exist in the 80 to 120 km region of the earth’s atmosphere, and reflect the RF energy between two stations. The height of the trails allows over-the-horizon communication at distances up to 2000 km. However, because the ionized trails exist for only short periods of time (usually from a few milliseconds to a few seconds) communication is intermittent, and high-speed digital transmission techniques must be used to convey the information. The system is particularly well suited for long-range, low data rate applications for both messaging and data acquisition.

Meteor Burst communications has been a viable communications medium since the 1950s. It was quickly recognized as an alternative to Satellite. In addition, since no equipment has to be placed in orbit, it is not susceptible to conventional or nuclear war side-effects.

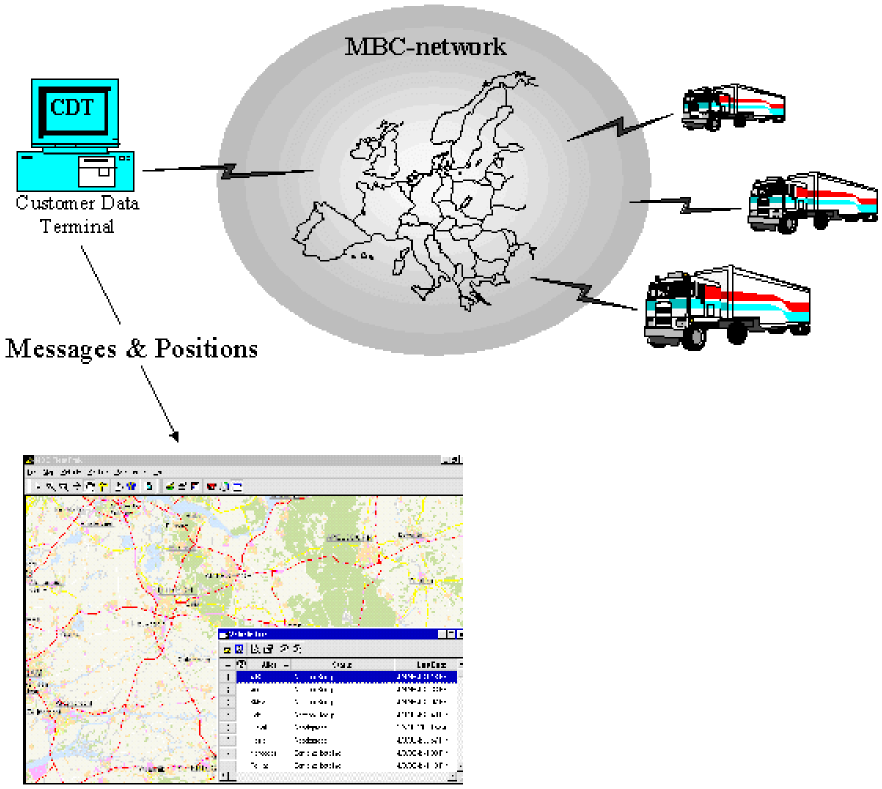
Notes

Following are the MBC Network Applications:

FleetTrak Service

FleetTrak is a two-way messaging system for the transport sector, providing communication between mobiles stations (in particular trucks) and a central office for vehicle dispatch and tracking in support of fleet management systems (Figure 12.5).

Figure 12.5: FleetTrak Application



Source: http://www.itu.int/ITU-D/fg7/case_library/documents/MBC001.html

A standard subscription to the FleetTrak service includes the exchange of messages between the dispatch centre and the vehicle and (automatic) position reports by the vehicle. The messages may include free text and a large variety of status and control information, efficiently coded for reliable transmission.

For the FleetTrak application, a radio modem is installed in a suitable place inside the truck cabin. A GPS unit is connected to the radio modem, providing the position of the vehicle with an accuracy of about 10 meters using the Global Positioning System (GPS). The GPS antenna can be installed inside the truck cabin as well. The FleetTrak mobile antenna is mounted on the roof of the vehicle.

A simple hand-held terminal can be connected, providing the driver with the means to input status and text messages. Input connectors are provided for connection of other car systems (e.g. engine and trailer system sensors, board computer) to the FleetTrak system, for status monitoring and logging.

Notes

Notes A service connector is available for maintenance purposes.

ProTrak Service

ProTrak is a service for the localization and tracking of stolen vehicles. Upon activation by the Data Centre or, optionally, by an alarm system in the car, the position of the car is reported to a central desk of the customer. Here the information is processed and the appropriate action can be taken.

For the ProTrak application, a radio modem is installed in a place inside the car that is not easily accessible. Because of the small dimensions of the unit, it can be hidden easily in various spots in the car. A GPS receiver antenna and a ProTrak mobile antenna are also installed unobtrusively. The unit has no external user controls, since its purpose is to be activated by the customer Call Center or an alarm system only.

When the ProTrak unit is activated, the processor sends a unique identification plus the last known position to the modem for transmission to the Call Centre for action. As long as the unit remains activated, regular position updates are transmitted to allow tracking of the stolen vehicle.

The ProTrak service can be extended with an alarm or assistance call activated by the car driver. The data is then sent to the Call Centre for appropriate action. Using a set of push buttons the user may specify one out of a number of request types such as technical assistance, medical assistance or police assistance. The radio modem for this so-called ProTrak Plus service is slightly different from the ProTrak unit; it is controlled and activated in a different way. Furthermore, it is not necessary to hide the Pro Trak Plus equipment.

12.2.5 Principles of Meteor Burst Communication

Meteor burst refers to a unique means of long-distance communication via reflections by ionized gas trails in the upper atmosphere. These gas trails are generated by the burn up of small meteors impacting on the Earth's atmosphere. The typical meteor trail is only available for a few hundred milliseconds.

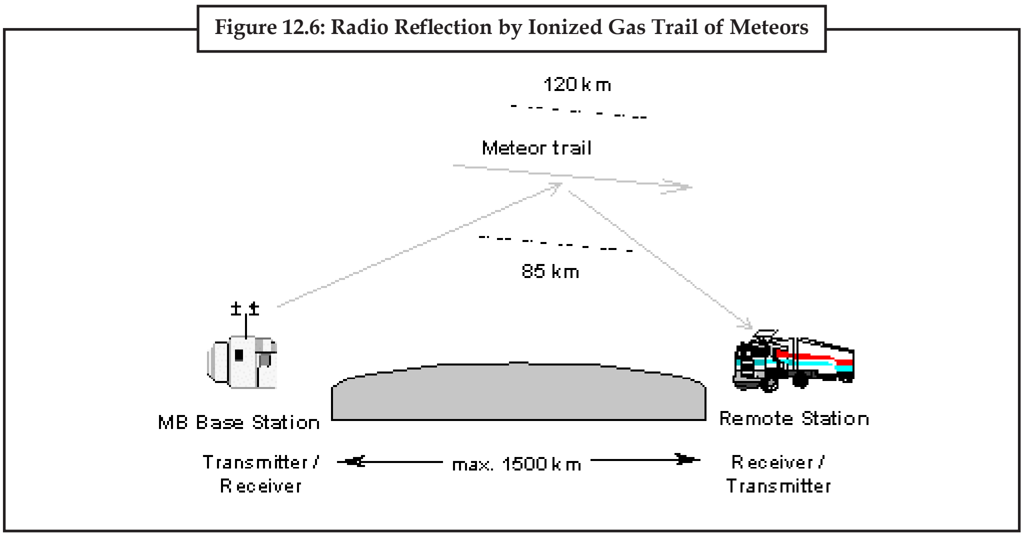
As communication is only possible in very short intervals, the term 'burst' is introduced. Due to the nature of the phenomenon used, waiting times are introduced. The delay between the appearance of two consecutive trails ranges from seconds to minutes, depending on the time of year, the time of day and design factors of the system.

The network supports a variety of data communication services for road transport and telemetry applications. The FleetTrak service has been developed for fleet management systems and provides two-way data communication plus vehicle tracking for trucks. A second service, offered under the name ProTrak, has been developed for private cars and provides after-theft tracking and alarm messaging as shown in Figure 12.6.

In remote areas the meteor burst communication system can be used to transfer data from a measurement site to the central office. Examples of these telemetric applications are snow height and tide gauge measurements.

Most meteor scatter applications operate between 30 and 50 MHz. At frequencies below 30 MHz absorption and noise, both galactic and artificial, increase drastically. Furthermore, the antenna size and cost increase at lower frequencies. The data communication capacity will decrease when frequencies above 50 MHz are used, as the average burst length decreases with increasing frequency. Additionally, radio and television allocations preclude meteor burst operation above 50 MHz.

Figure 12.6: Radio Reflection by Ionized Gas Trail of Meteors



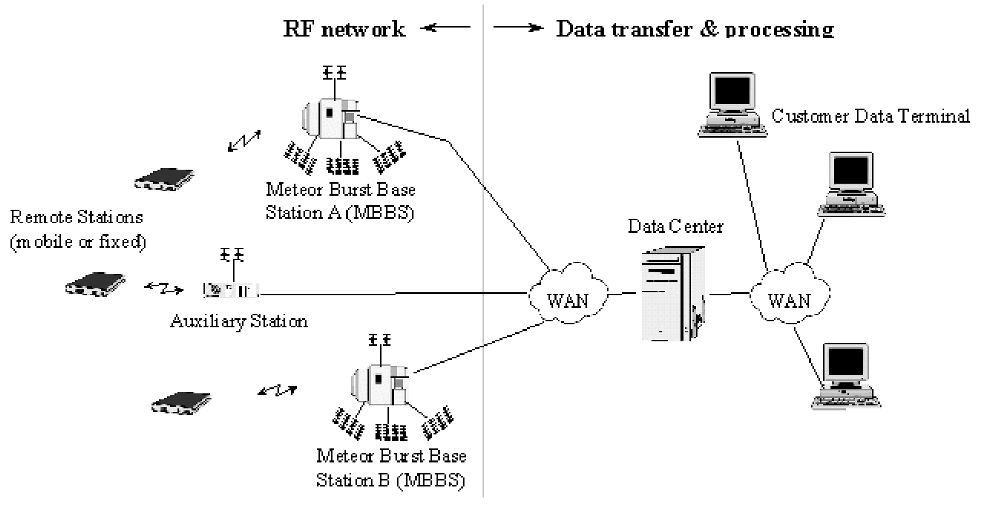
Source: http://www.itu.int/ITU-D/fg7/case_library/documents/MBC001.html

Did u know? MBC Europe BV is the first and only provider of meteor scatter communication in Europe. Since only two 25 kHz channels are required for the entire MBC network, in total four operators can be assigned within this harmonized band. For Europe the harmonized frequency band for meteor scatter applications is allocated to 39.0–39.2 MHz.

12.2.6 The Meteor Burst Communication (MBC) Network

The MBC network can be divided into the radio frequency (RF) part and the data transfer and processing part, as shown in the Figure 12.7 below.

Figure 12.7: MBC Network System Overview


RF network
Data transfer & processing
Customer Data Terminal
Meteor Burst Base Station A (MBBS)
Remote Stations (mobile or fixed)
Data Center
Auxiliary Station
WAN
WAN
Meteor Burst Base Station B (MBBS)

Source: http://www.itu.int/ITU-D/fg7/case_library/documents/MBC001.html

The number of Meteor Burst Base Stations (MBBS) depends on the size of the area which has to be covered. To cover an area of one million square kilometers, which could meet the needs of a country such as Senegal, the MBC network system would use three ground stations and a computer system with tailormade software. The price for a complete network such as this, installed and tested, would be about 5 million Euro. The time between sending and receiving a message for such a network is around 5 minutes. Leaving out one ground station would decrease the investment but increase the waiting time.

All network subsystems are described below.

Meteor Burst Base Station

Using meteor trails, a meteor burst base station (MBBS) can communicate with remote stations, either mobile or fixed, over distances between 500 and 1500 km. Using meteor burst technology, a few tens of base stations provide the infrastructure for the pan-European data communication network. The data exchange between a base station and a remote station is initiated by a test signal (probe) transmitted into space by the base station. If and when a meteor trail is in the right position and reflects the signal back to Earth, the remote station answers the call by the base station and data is exchanged. The base stations are connected directly to the Data Centre of the network.

Auxiliary Station

For communication in a densely populated, industrial area, auxiliary stations might be installed to supplement the coverage by the base stations. The auxiliary stations do not use the meteor burst phenomenon, but work in a Line-of-Sight (LOS) mode. The data received can be transferred to one of the base stations using a meteor burst connection after which it will be delivered at the Data Centre. A direct link between the auxiliary station and the Data Centre is possible as well. In the current network planning, no auxiliary stations have been adopted.

Remote Station

A remote station can either be mobile or fixed. Mobile stations are for example the trucks and cars from the FleetTrak and ProTrak service. The mobile stations use a radio modem and an omnidirectional antenna that is mounted on the roof of the vehicle. Fixed stations, for example meteorological sites located in remote areas, use the same radio modem. For the fixed stations, however, a directive antenna can be used to communicate with the meteor burst base stations. The use of a directive antenna will improve the communication link and reduce the waiting times. The power necessary to operate the equipment can be generated via solar cells.

Data Centre

The heart of the network is the Data Centre, where the information from the remote station and customer terminal is gathered and passed on. Until the data is passed to either base station or customer terminal, it is stored in so-called Call Detail Records (CDRs). The CDRs contain a flag indicating whether the message is delivered or not. After a message is delivered, the CDR is used for Billing and Accounting purposes and deleted from the database.

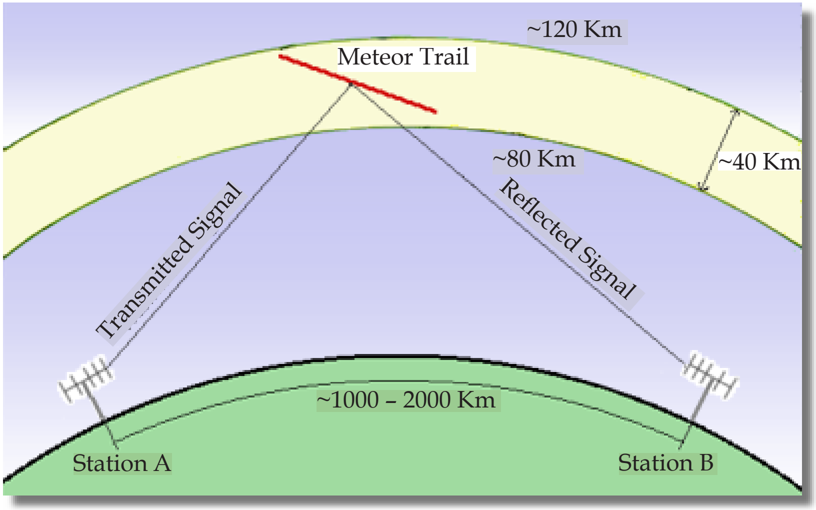
The customer is able to contact the Data Centre by means of a modem. In the future, the Data Centre will be accessible via the Internet. As a standard SMS protocol is used to transfer the data across the MBC network, the customer is free to use any SMS interface at the remote station or at the customer end of the network.

12.2.7 Meteor Scatter

Meteor Scatter (MS) propagation is not new, it has been used for many years especially on 2M using SSB and HSCW (high speed cw). The advent of WSJT modes FSK441 and JT6M has shown MS to be viable propagation mode especially during times of little or no propagation modes such as F2 ES, TEP or Aurora.

Notes

Figure 12.8: Diagram of Meteor Scatter



Source: http://jt6m.org/meteor-scatter.php

Meteor Scatter as shown in Figure 12.8 allows propagation of up to 2500 km during peak meteor shower activity and using "random" meteors, can provide qso's at almost any time of the day and year. Results can be quite spectacular at times and at other times very disappointing. Signals are usually very weak and of short duration.

So What Is Meteor Scatter?

As meteors fall into the earths atmosphere – commonly known as "shooting stars", ionisation occurs typically in the E layer and acts as a reflector for very high frequency signal . Meteors typically are small pieces of debris left by a passing comet but can also be small pieces of matter floating around space or even pieces of man-made space junk falling back into the atmosphere.

Cometry debris can be as small as a grain of sand and cause ionisation to occur. Small pieces of debris usually burn up completely as they pass into the atmosphere but larger pieces can partially ionise and the remainder falling to earth, known as "meteorites". The meteor trails which typically occur at altitudes between about 80 and 120 km can be effectively used to reflect radio signals.

Meteor scatter activity can use either annual meteor showers or random meteors. Meteor showers are experienced at specific times during the year, the number of meteors entering the atmosphere rising significantly as the Earth's path passes through debris in its orbit around the Sun. Some of these have been traced back to the passage of a comet. The number of visible trails rise significantly during some of the larger meteor showers, the Perseids shower in August is probably the best.

Meteor showers appear to originate form a point in the sky which is termed as their radiant. The radiant usually identified by the name of the constellation or major star in the area of the sky from which they appear to originate, and this name is usually given to the shower itself.

Random Meteors

The majority of meteors entering the atmosphere are random meteors. These are the space debris that is within our solar system. Unlike the meteor showers they enter in all directions and they do not have a radiant.

Meteor Trails

Meteors enter the earth's atmosphere at speeds between 10 and 80 Kilometres per second and burn up due to friction at altitudes between 80 km and 120 km, dependent on their size, speed and angle of entry. As the meteors burn up their atoms vaporise leaving a trial of positive and negative electrons. The trial formed is typically only a few metres wide but can be over 20 km long.

Meteor trial can be divided in to 2 types depending on the density of the electrons. These are known as "over dense" and "under dense". Over dense trials produce relatively strong signal reflections. With a high electron density signals do not totally enter these trails and are reflected. The duration can be several seconds and are the result of larger sized meteors.

Under dense trails are formed by very small meteors, typically the size of a grain of sand. With a lower electron density these act in different way to over dense trails. A signal penetrates the trail and is scattered rather than being reflected. Only a small amount of signal is returned to earth, the signal typically rising in strength for a few hundred milliseconds and then decays but can last for a few seconds.

Caution Signals are subject to Doppler shift but are less affected at lower frequencies, 4 and 6 M bit can be as much as 2 kHz on high frequencies.

12.2.8 Future Developments

The functionality of the MBC network will make it suitable for a large number of other applications where tracking and/or messaging on an occasional basis is required.

Example: Examples are the tracking of cargo containers or complete trailers, alarms in remote and stationary objects, and control of (environmental) monitoring equipment in remote places.

The advantage of a fixed application is the use of a directive antenna increasing the quality of the communication link and thus reducing the waiting time. Due to its low cost and high reliability, the system is ideal for communication from remote areas where other communication systems are not available or expensive.

The evolving proliferation of less expensive and improved microprocessor technology applied to adaptive signal processing techniques, electronic system controllers, cryptographic devices and user terminal microprocessors offers great promise to improve significantly the performance of MBC systems. A careful assessment of the advantages offered by technologically advanced MBC systems likely will confirm that such systems can improve the diversity of information transport services available to our national security operations of the 21st Century.

Self Assessment

Fill in the blanks:

9. Meteor burst communications is a specialized form of propagation that can be successfully used for ………………...… over paths that extend up to 1500 or 2000 km.

10. Frequencies above 30 MHz but below 50 MHz in the lower very high frequency (VHF) spectrum propagate most efficiently using ………………...…

11. Meteor Burst communications has been a viable communications medium since the ………………...…

12. ………………...… is a two-way messaging system for the transport sector, providing communication between mobiles stations and a central office for vehicle dispatch and tracking in support of fleet management systems.

Notes

13. …………………...… is a service for the localization and tracking of stolen vehicles.

14. The …………………...… network can be divided into the radio frequency (RF) part and the data transfer and processing part.

15. The auxiliary stations do not use the meteor burst phenomenon but work in a …………………...… mode.

16. …………………...…trails are formed by very small meteors, typically the size of a grain of sand.

Case Study

Nevada Research Uses Falling Stars for Data Transmission

Even in today's world of sophisticated communication technology, there are still some remote locations that are not serviced by a communication system. In most cases, this situation does not present a problem. For those responsible for data collection from these distant sites, however, the lack of a suitable communication system can be a major drawback.

The Nevada Department of Transportation (NDOT) collects traffic-related data at remote locations over an area of 110,540 square miles. Fortunately, only a small part of this area is not serviced by either telephone lines or a cellular communication network. NDOT's problem lies in the fact that it locates its traffic-related data-collection sites based on need instead of the availability of a communication system. The manpower required to collect data at these sites taxes the department's resources with an annual cost in excess of 1,000 man-hours. The Meteor Burst Project began with the awareness of this problem and the desire to find an effective solution. Although Meteor Burst Communication (MBC) has been used for 30 years in military applications and for various types of remote environmental data collection, it had never been used in this application.

Working together, NDOT and the Electrical Engineering Department of the University of Nevada-Reno developed a self-contained, roadside MBC station. In addition to the existing data-collection devices, this station consisted of a solar panel, a rechargeable 12-volt battery power supply, the meteor burst transmission unit, an interface board, and a five element yagi antenna. This remote roadside station is completely controlled by the interface board, a microprocessor-based unit that acts as the brains of the system. This board is designed to connect multiple traffic monitoring devices to a single transmitter/receiver. It can also perform duties such as automatically downloading data from the traffic-recording devices before their memory storage overflows, or downloading data at programmed intervals. Once these data are in the interface board, they are reformatted and compressed before copies of the data are transferred to the meteor burst transmitter. A status report of the system can also be transmitted in order to alert operators that repair or service is required. During NDOT's research, the data were sent to an MBC master station located in Bozeman, Montana. The data were then forwarded to a data centre in Kent, Washington, via telephone lines, where they were reformatted back to their original configuration and finally sent to the NDOT headquarters in Carson City, Nevada.

NDOT continued to use MBC to retrieve data at one remote station for four months, saving the department approximately 150 manhours. At that time, the cellular communication network serving Nevada was expanded, eliminating the benefits of MBC for current NDOT traffic data-collection sites. However, NDOT is currently reviewing MBC for data collection in conjunction with FHWA's continuation of the SHRP anti-icing study. The results of this research project have served to break new ground in the area of data

Contd...

transmission and should provide a base of technical knowledge that will stimulate use for a variety of transportation-related data transmission throughout remote areas of the world.

Questions:

1. What are the benefits provided by NDOT?
2. Discuss the current situation of NDOT.

Source: http://onlinepubs.trb.org/onlinepubs/trnews/rpo/rpo.trn171.pdf

12.3 Summary

- Satellite communications play a vital role in the global telecommunications system.
- A satellite is basically a self-contained communications system with the ability to receive signals from Earth and to retransmit those signals back with the use of a transponder—an integrated receiver and transmitter of radio signals.
- The first major geosynchronous satellite project was the Defense Department's ADVENT communications satellite.
- Advances in satellite technology have given rise to a healthy satellite services sector that provides various services to broadcasters, Internet service providers(ISPs), governments, the military, and other sectors.
- Telecommunications systems developed to use meteor trails transmit data in bursts as intermittent meteor trails arrive for use; however, not all meteors create trails usable for communications.
- A meteor burst communications system (MBCS) uses ionized meteor trails as a means of radio signal propagation.
- The network supports a variety of data communication services for road transport and telemetry applications.
- Meteors enter the earth's atmosphere at speeds between 10 and 80 Kilometres per second and burn up due to friction at altitudes between 80 and 120 km, dependent on their size, speed and angle of entry.
- Meteor scatter activity can use either annual meteor showers or random meteors.

12.4 Keywords

Broadcasting: Broadcasting, electronic transmission of radio and television signals that are intended for general public reception, as distinguished from private signals that are directed to specific receivers.

Elliptical Orbits: An elliptic orbit is a Kepler orbit with the eccentricity less than 1; this includes the special case of a circular orbit, with eccentricity equal to zero.

Geostationary Orbit: GEO satellites are synchronous with respect to earth and are placed in the space in such a way that only three satellites are sufficient to provide connection throughout the surface of the Earth (that is; their footprint is covering almost 1/3rd of the Earth).

Low Earth Orbit: These satellites are placed 500–1500 kms above the surface of the earth as LEOs circulate on a lower orbit, hence they exhibit a much shorter period that is 95 to 120 minutes.

Medium Earth Orbit: MEO, sometimes called intermediate circular orbit (ICO), is the region of space around the Earth above low Earth orbit altitude of 2,000 kilometres (1,243 mi) and below geostationary orbit altitude of 35,786 kilometres (22,236 mi).

Meteor Burst Communication: Meteor burst communication is a way of communicating using the ionized trails made by meteors as they enter the earth’s atmosphere. It is also called Meteor scatter communication.

Meteor Scatter: Meteor scatter communications, is a radio propagation mode that exploits the ionized trails of meteors during atmospheric entry to establish brief communications paths between radio stations up to 2,250 kilometres (1,400 mi) apart.

Over dense Trials: Over dense trials produce relatively strong signal reflections.

ProTrak Service: ProTrak is a service for the localization and tracking of stolen vehicles.

Satellite: An artificial body placed in orbit around the earth or another planet in order to collect information or for communication.

Under dense trails: Under dense trails are formed by very small meteors, typically the size of a grain of sand.

12.5 Review Questions

1. Define Satellite.
2. Discuss the evolution of communication satellites.
3. How satellites work?
4. Explain the future of satellite communication.
5. Distinguish between geostationary orbit and Elliptical Orbits.
6. What do you understand by Meteor Burst Communications?
7. Highlight the basic characteristics of Meteor Burst Communications.
8. Describe MBC Network Applications.
9. What are the principles of Meteor Burst Communication?
10. Write brief note on the network of Meteor Burst Communication (MBC).
11. Discuss Meteor Trails.
12. Highlight the future developments of MBC.

Answers: Self Assessment

1. False
2. True
3. False
4. False
5. True
6. False
7. True
8. True
9. Radio Communications
10. Meteor Trails
11. 1950s
12. FleetTrak
13. ProTrak
14. MBC
15. Line-of-Sight (LOS)
16. Under dense

12.6 Further Readings

Notes

Books

Glisic, Savo & Lorenzo, Beatriz (2009). "*Advanced Wireless Networks: Cognitive, Cooperative & Opportunistic 4G Technology*." John Wiley & Sons.

Golmie. "*Coexistence in Wireless Networks*." Cambridge University Press.

Pan, Yi & Xiao, Yang (2005). "*Design and Analysis of Wireless Networks*." Nova Publishers.

Rackley, Steve (2011). "*Wireless Networking Technology: From Principles to Successful Implementation*." Elsevier.

Syngress (2001). "*Designing A Wireless Network*". Syngress.

Stojmenovic (2006). "*Handbook of Wireless Networks & Mobile Computing*." John Wiley & Sons.

Online links

http://www.howstuffworks.com/satellite.htm

http://history.nasa.gov/satcomhistory.html

http://www.electronicsforu.com//EFYLinux/efyhome/cover/January2008/Satcom-Evolution%284%29.pdf

http://www.telesat.com/about-us/why-satellite/brief-history

http://www.bamcom.co.nz/articles/the-evolution-of-satellite-communication/

http://www.britannica.com/EBchecked/topic/524891/satellite-communication

http://www.satcom.co.uk/article.asp?article=11

http://faza1.tripod.com/mbc2.htm

http://meteorcomm.com/tech_burst.aspx

http://ronaldelliott.com/mbc.html

Notes

Unit 13: Wireless Networks Security

CONTENTS

Objectives

Introduction

13.1 Need of Security

13.2 Security Threats

13.3 Traffic Monitoring

13.3.1 Monitoring Requirements

13.3.2 Additional Equipment

13.4 Unauthorised Access

13.5 Middle Attacks

13.5.1 Address Resolution Protocol (ARP) Poisoning

13.6 Denial of Service (DoS) Attack

13.6.1 Types of Denial of Service (DoS) Attacks

13.6.2 Distributed Denial of Service (DDoS) Attacks

13.7 Protective Actions

13.7.1 Wired Equivalent Privacy (WEP)

13.7.2 Wi-Fi Protected Access (WPA)

13.7.3 Virtual Private Network (VPN)

13.8 Summary

13.9 Keywords

13.10 Review Questions

13.11 Further Readings

Objectives

After studying this unit, you will be able to:

- Discuss the need for security
- Explain the concept of security threats
- Describe traffic monitoring
- Explain unauthorised access
- Explain middle attacks
- Describe denial of service
- Discuss various types of protective actions

Introduction

Notes

Wireless security is the prevention of unauthorised access or damage to computers using wireless networks. The most common types of wireless security are Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). WEP is a notoriously weak security standard. The password it uses can often be cracked in a few minutes with a basic laptop computer and widely available software tools. WEP is an old IEEE 802.11 standard from 1999 which was outdated in 2003 by WPA or Wi-Fi Protected Access. WPA was a quick alternative to improve security over WEP. The current standard is WPA2; some hardware cannot support WPA2 without firmware upgrade or replacement. WPA2 uses an encryption device which encrypts the network with a 256 bit key; the longer key length improves security over WEP.

Many laptop computers have wireless cards pre-installed. The ability to enter a network while mobile has great benefits. However, wireless networking is prone to some security issues. Crackers have found wireless networks relatively easy to break into, and even use wireless technology to crack into wired networks. As a result, it's very important that enterprises define effective wireless security policies that guard against unauthorised access to important resources. Wireless Intrusion Prevention Systems (WIPS) or Wireless Intrusion Detection Systems (WIDS) are commonly used to enforce wireless security policies.

The risks to users of wireless technology have increased as the service has become more popular. There were relatively few dangers when wireless technology was first introduced. Crackers had not yet had time to latch on to the new technology and wireless was not commonly found in the work place. However, there are a great number of security risks associated with the current wireless protocols and encryption methods, and in the carelessness and ignorance that exists at the user and corporate IT level. Cracking methods have become much more sophisticated and innovative with wireless. Cracking has also become much easier and more accessible with easy-to-use Windows or Linux-based tools being made available on the web at no charge.

Some organizations that have no wireless access points installed do not feel that they need to address wireless security concerns. In-Stat MDR and META Group have estimated that 95% of all corporate laptop computers that were planned to be purchased in 2005 were equipped with wireless. Issues can arise in a supposedly non-wireless organization when a wireless laptop is plugged into the corporate network. A cracker could sit out in the parking lot and gather info from it through laptops and/or other devices as handhelds, or even break in through this wireless card-equipped laptop and gain access to the wired network.

13.1 Need of Security

Wireless networking is inherently risky because you are transmitting information via radio waves. Data from your wireless network can be intercepted just like signals from your cellular or cordless phones. Whenever you use a wireless connection, you might want to ensure that your communications and files are private and protected. If your transmissions are not secure, it may be possible for others to intercept your e-mails, examine your files and records, and use your network and Internet connection to distribute their own messages and communications.

How secure you want your network to be depends on how you use it. If you're just surfing to do research or watch movies, you may not care if anyone picks up part of the transmission, but that's up to you. Even if you're shopping and purchasing items over the net, those financial transactions are usually protected by Secure Socket Layer (SSL). However, if your data is confidential or if you want additional security, there are several different technologies you can install. Keep in mind that security is a personal decision, but it's almost essential to use at least some level of security as a deterrent to intrusion and interception.

Notes

Did u know? In a home wireless network, you can use a variety of simple security procedures to protect your Wi-Fi connection. These include enabling Wi-Fi Protected Access, changing your password or network name (SSID) and closing your network. However, you can also employ additional, more sophisticated technologies and techniques to further secure your business network.

13.2 Security Threats

All computer systems and communications channels face security threats that can compromise systems, the services provided by the systems, and/or the data stored on or transmitted between systems. The most common threats are:

- Denial-Of-Service (DOS) occurs when an adversary causes a system or a network to become unavailable to legitimate users or causes services to be interrupted or delayed. Consequences can range from a measurable reduction in performance to the complete failure of the system. A wireless example would be using an external signal to jam the wireless channel. There is little that can be done to keep a serious adversary from mounting a denial of service attack.
- Interception has more than one meaning. A user's identity can be intercepted leading to a later instance of masquerading as a legitimate user or a data stream can be intercepted and decrypted for the purpose of disclosing otherwise private information. In either case, the adversary is attacking the confidentiality or privacy of the information that is intercepted.
- For example: eavesdropping and capturing the wireless interchanges between a wireless device and the network access point.
- Since wireless systems use the radio band for transmission, all transmissions can be readily intercepted. Therefore, some form of strong authentication and encryption is necessary in order to keep the contents of intercepted signals from being disclosed.
- Manipulation means that data has been inserted, deleted, or otherwise modified on a system or during transmission. This is an attack on the integrity of either the data transmission or on the data stored on a system. An example would be the insertion of a Trojan program or virus on a user device or into the network. Protection of access to the network and its attached systems is one means of avoiding manipulation.
- Masquerading refers to the act of an adversary posing as a legitimate user in order to gain access to a wireless network or a system served by the network.
- For example, a user with inappropriate access to a valid network authenticator could access the network and perform unacceptable functions (e.g., break into a server and plant malicious code, etc.). Strong authentication is required to avoid masquerade attacks.
- Repudiation is when a user denies having performed an action on the network. Users might deny having sent a particular message or deny accessing the network and performing some action. Strong authentication of users, integrity assurance methods, and digital signatures can minimize the possibility of repudiation.

13.3 Traffic Monitoring

13.3.1 Monitoring Requirements

To plan for wireless traffic monitoring, there are few thing to consider. It's not hard and you just need to prepare something software and hardware.

- Determine why and where to capture wireless traffic. To get quality wireless signal, try your best to get close to the object that you want to monitor wireless traffic from.
- Install wireless monitoring software on your computer or laptop. You can find lots of wireless traffic sniffer tools on the web. And lots of them are freeware.
- Prepare a wireless adapter. Some wireless monitor tools require specific wireless adapter or specific driver. So you may need to get one wireless adapter for your wireless traffic monitor software.
- Get wireless security key for the wireless network if it uses encryption. It's often that wireless networks implement encryption for security purposes. So you need the key for the wireless traffic monitor software to decode the wireless data.

13.3.2 Additional Equipment

Because wireless traffic transmits in air, it's helpful if you have better equipment to perform wireless traffic monitoring. Equipment that may be useful for wireless traffic monitoring includes:

- a wireless network card supports 802.11a, b, g, n
- an omni-directional antenna
- a high-gain yagi directional antenna
- pigtail cables for the yagi and omni-directional antennas
- a USB GPS adapter

13.4 Unauthorised Access

The modes of unauthorised access to links, to functions and to data is as variable as the respective entities make use of program code. There does not exist a full scope model of such threat. To some extent the prevention relies on known modes and methods of attack and relevant methods for suppression of the applied methods. However, each new mode of operation will create new options of threatening. Hence prevention requires a steady drive for improvement. The described modes of attack are just a snapshot of typical methods and scenarios where to apply.

- ***Non-traditional networks:*** Non-traditional networks such as personal network Bluetooth devices are not safe from cracking and should be regarded as a security risk. Even barcode readers, handheld PDAs, and wireless printers and copiers should be secured. These non-traditional networks can be easily overlooked by IT personnel who have narrowly focused on laptops and access points.
- ***Identity theft (MAC spoofing):*** Identity theft (or MAC spoofing) occurs when a cracker is able to listen in on network traffic and identify the MAC address of a computer with network privileges. Most wireless systems allow some kind of MAC filtering to allow only authorized computers with specific MAC IDs to gain access and utilize the network. However, programs exist that have network "sniffing" capabilities. Combine these programs with other software that allow a computer to pretend it has any MAC address that the cracker desires, and the cracker can easily get around that hurdle.

  MAC filtering is effective only for small residential (SOHO) networks, since it provides protection only when the wireless device is "off the air". Any 802.11 device "on the air" freely transmits its unencrypted MAC address in its 802.11 headers, and it requires no special equipment or software to detect it. Anyone with an 802.11 receiver (laptop and wireless adapter) and a freeware wireless packet analyser can obtain the MAC address of any transmitting 802.11 within range. In an organizational environment, where most wireless

Notes

devices are "on the air" throughout the active working shift, MAC filtering provides only a false sense of security since it prevents only "casual" or unintended connections to the organizational infrastructure and does nothing to prevent a directed attack.

- ***Network injection:*** In a network injection attack, a cracker can make use of access points that are exposed to non-filtered network traffic, specifically broadcasting network traffic such as “Spanning Tree” (802.1D), OSPF, RIP, and HSRP. The cracker injects bogus networking re-configuration commands that affect routers, switches, and intelligent hubs. A whole network can be brought down in this manner and require rebooting or even reprogramming of all intelligent networking devices.
- ***Caffe Latte attack:*** The Caffe Latte attack is another way to defeat WEP. It is not necessary for the attacker to be in the area of the network using this exploit. By using a process that targets the Windows wireless stack, it is possible to obtain the WEP key from a remote client. By sending a flood of encrypted ARP requests, the assailant takes advantage of the shared key authentication and the message modification flaws in 802.11 WEP. The attacker uses the ARP responses to obtain the WEP key in less than 6 minutes.

Self Assessment

Fill in the blanks:

1. .... is an attack on the integrity of either the data transmission or on the data stored on a system.
2. .... is when a user denies having performed an action on the network
3. Non-traditional networks such as personal network Bluetooth devices are not safe from cracking and should be regarded as a .... risk.
4. Identity theft (or MAC spoofing) occurs when a ....is able to listen in on network traffic and identify the MAC address of a computer with network privileges.
5. .... is effective only for small residential (SOHO) networks, since it provides protection only when the wireless device is "off the air".
6. In a network ....attack, a cracker can make use of access points that are exposed to non-filtered network traffic.

13.5 Middle Attacks

A man-in-the-middle attacker entices computers to log into a computer which is set up as a soft AP (Access Point). Once this is done, the hacker connects to a real access point through another wireless card offering a steady flow of traffic through the transparent hacking computer to the real network. The hacker can then sniff the traffic. One type of man-in-the-middle attack relies on security faults in challenge and handshake protocols to execute a “de-authentication attack”. This attack forces AP-connected computers to drop their connections and reconnect with the cracker’s soft AP (disconnects the user from the modem so they have to connect again using their password which you can extract from the recording of the event). Man-in-the-middle attacks are enhanced by software such as LANjack and AirJack which automate multiple steps of the process, meaning what once required some skill can now be done by script kiddies. Hotspots are particularly vulnerable to any attack since there is little to no security on these networks.

13.5.1 Address Resolution Protocol (ARP) Poisoning

Address Resolution Protocol (ARP) poisoning is a type of attack where the Media Access Control (MAC) address is changed by the attacker. Also, called an ARP spoofing attacks, it is effective

Notes

against both wired and wireless local networks. Some of the things an attacker could perform from ARP poisoning attacks include stealing data from the compromised computers, eavesdrop using man-in-the middle methods, and prevent legitimate access to services, such as Internet service.

A MAC address is a unique identifier for network nodes, such as computers, printers, and other devices on a LAN. MAC addresses are associated to network adapter that connects devices to networks. The MAC address is critical to locating networked hardware devices because it ensures that data packets go to the correct place. ARP tables, or cache, are used to correlate network devices' IP addresses to their MAC addresses.

In for a device to be able to communicate with another device with a known IP Address but an unknown MAC address the sender sends out an ARP packet to all computers on the network. The ARP packet requests the MAC address from the intended recipient with the known IP address. When the sender receives the correct MAC address then is able to send data to the correct location and the IP address and corresponding MAC address are store in the ARP table for later use.

ARP poisoning is when an attacker is able to compromise the ARP table and changes the MAC address so that the IP address points to another machine. If the attacker makes the compromised device's IP address point to his own MAC address then he would be able to steal the information, or simply eavesdrop and forward on communications meant for the victim. Additionally, if the attacker changed the MAC address of the device that is used to connect the network to Internet then he could effectively disable access to the web and other external networks.

13.6 Denial of Service (DoS) Attack

A Denial-of-Service attack (DoS) occurs when an attacker continually bombards a targeted AP (Access Point) or network with bogus requests, premature successful connection messages, failure messages, and/or other commands. These cause legitimate users to not be able to get on the network and may even cause the network to crash. These attacks rely on the abuse of protocols such as the Extensible Authentication Protocol (EAP).

The DoS attack in itself does little to expose organizational data to a malicious attacker, since the interruption of the network prevents the flow of data and actually indirectly protects data by preventing it from being transmitted. The usual reason for performing a DoS attack is to observe the recovery of the wireless network, during which all of the initial handshake codes are re-transmitted by all devices, providing an opportunity for the malicious attacker to record these codes and use various "cracking" tools to analyse security weaknesses and exploit them to gain unauthorised access to the system. This works best on weakly encrypted systems such as WEP, where there are a number of tools available which can launch a dictionary style attack of "possibly accepted" security keys based on the "model" security key captured during the network recovery.

13.6.1 Types of Denial of Service (DoS) Attacks

The most common type of Denial of Service attack involves flooding the target resource with external communication requests. This overload prevents the resource from responding to legitimate traffic, or slows its response so significantly that it is rendered effectively unavailable.

Resources targeted in a DoS attack can be a specific computer, a port or service on the targeted system, an entire network, a component of a given network any system component. DoS attacks may also target human-system communications (e.g. disabling an alarm or printer), or human-response systems (e.g. disabling an important technician's phone or laptop).

DoS attacks can also target tangible system resources, such as computational resources (bandwidth, disk space, processor time); configuration information (routing information, etc.); state information (for example, unsolicited TCP session resetting). Moreover, a DoS attack can be designed to: execute malware that maxes out the processor, preventing usage; trigger errors in machine microcode or sequencing of instructions, forcing the computer into an unstable state; exploit operating system vulnerabilities to sap system resources; crash the operating system altogether.

The overriding similarity in these examples is that, as a result of the successful Denial of Service attack, the system in question does not respond as before, and service is either denied or severely limited.

13.6.2 Distributed Denial of Service (DDoS) Attacks

A DDOS attack (better known as a Distributed Denial of Service attack) is a type of web attack that seeks to disrupt the normal function of the targeted computer network. This is any type of attack that attempts to make this computer resource unavailable to its users. While this type of attack typically follows the same sorts of patterns, the definition of the term Distributed Denial of Service does not make any specific indications of how this type of attack is to be pulled off. What makes this type of attack "distributed" is the concerted efforts between a large number of disruptors all for the common goal of preventing web servers (and therefore websites) from functioning effectively at all. These users may be willing participants, or in some cases be tricked into downloading software that will use their terminal to aid in the offensive. All in all, regardless of the means, a DDOS attack is simply a combined effort to prevent computer systems from working as well as they should, typically from a remote location over the internet.

The most common method of attack is to send a mass saturation of incessant requests for external communication to the target. These systems are flooded with requests for information from non-users, and often non-visitors to the website. The goal of this attack is to create a large enough presence of false traffic such that legitimate web traffic intended for actual web users is slowed down and delayed. If this type of service becomes too slow, time sensitive information such as live video footage may be rendered entirely useless to legitimate end users.

For a DDOS to work effectively, the process has to be heavily automated on the attacker's end. Customized software is designed to flood these services with false traffic, and is run on as many computers as possible. There are a few instances in which this type of software was set up like a virus, infecting computers and taking control of their communication functions. These users unwillingly are aiding in a DDOS attack, sometimes without being the slightest bit aware of it. If there seems to be large delays in normal internet service, there may be outbound requests being made consuming your internet connections given throughput, and can sometimes be an indication of foul play. Users seeking to limit this risk should keep anti-virus software up to date, and scan frequently for these types of programs.

While there are few court cases on the books of Distributed Denial of Service perpetrators being held accountable for their actions, as well as the potential lost income for commercial websites, this type of activity almost always violates the terms of service and acceptable use policies of internet service providers, as well as often violating individual communication law within the nation. These types of attacks have become more and more prevalent as time goes on, and in many nation legislation is in the works, with hopes of criminal penalties for those involved with this sort of attack.

All in all, a DDOS attack is a very real threat to businesses and organizations across the world, and it's important that they be prepared in case some group of people decides to cause trouble for your organization. Being prepared to identify these types of threats is an important part of proper internet use, and should be a part of your daily life online.

13.7 Protective Actions

The various protective actions are as follows:

13.7.1 Wired Equivalent Privacy (WEP)

Wired Equivalent Privacy (WEP) is a security algorithm for IEEE 802.11 wireless networks. Introduced as part of the original 802.11 standard ratified in September 1999, its intention was to provide data confidentiality comparable to that of a traditional wired network. WEP, recognizable by the key of 10 or 26 hexadecimal digits, is widely in use and is often the first security choice presented to users by router configuration tools.

Although its name implies that it is as secure as a wired connection, WEP has been demonstrated to have numerous flaws and has been deprecated in favour of newer standards such as WPA2. In 2003 the Wi-Fi Alliance announced that WEP had been superseded by Wi-Fi Protected Access (WPA). In 2004, with the ratification of the full 802.11i standard (i.e. WPA2), the IEEE declared that both WEP-40 and WEP-104 have been deprecated as they fail to meet their security goals

WEP was included as the privacy component of the original IEEE 802.11 standard ratified in September 1999. WEP uses the stream cipher RC4 for confidentiality, and the CRC-32 checksum for integrity. It was deprecated in 2004 and is documented in the current standard.

Standard 64-bit WEP uses a 40 bit key (also known as WEP-40), which is concatenated with a 24-bit initialization vector (IV) to form the RC4 key. At the time that the original WEP standard was drafted, the U.S. Government's export restrictions on cryptographic technology limited the key size. Once the restrictions were lifted, manufacturers of access points implemented an extended 128-bit WEP protocol using a 104-bit key size (WEP-104).

A 64-bit WEP key is usually entered as a string of 10 hexadecimal (base 16) characters (0-9 and A-F). Each character represents four bits, 10 digits of four bits each gives 40 bits; adding the 24-bit IV produces the complete 64-bit WEP key. Most devices also allow the user to enter the key as five ASCII characters, each of which is turned into eight bits using the character's byte value in ASCII; however, this restricts each byte to be a printable ASCII character, which is only a small fraction of possible byte values, greatly reducing the space of possible keys.

A 128-bit WEP key is usually entered as a string of 26 hexadecimal characters. Twenty-six digits of four bits each gives 104 bits; adding the 24-bit IV produces the complete 128-bit WEP key. Most devices also allow the user to enter it as 13 ASCII characters.

A 256-bit WEP system is available from some vendors. As with the other WEP-variants 24 bits of that is for the IV, leaving 232 bits for actual protection. These 232 bits are typically entered as 58 hexadecimal characters. (58 × 4 bits =) 232 bits + 24 IV bits = 256-bit WEP key.

13.7.2 Wi-Fi Protected Access (WPA)

Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2) are two security protocols and security certification programs developed by the Wi-Fi Alliance to secure wireless computer networks. The Alliance defined these in response to serious weaknesses researchers had found in the previous system, WEP (Wired Equivalent Privacy).

WPA (sometimes referred to as the draft IEEE 802.11i standard) became available in 2003. The Wi-Fi Alliance intended it as an intermediate measure in anticipation of the availability of the more secure and complex WPA2. WPA2 became available in 2004 and is a common shorthand for the full IEEE 802.11i (or IEEE 802.11i-2004) standard.

Notes

Notes A flaw in a feature added to Wi-Fi, called Wi-Fi Protected Setup, allows WPA and WPA2 security to be bypassed and effectively broken in many situations. WPA and WPA2 security implemented without using the Wi-Fi Protected Setup feature are unaffected by the security vulnerability.

A flaw in a feature added to Wi-Fi, called Wi-Fi Protected Setup, allows WPA and WPA2 security to be bypassed and effectively broken in many situations. WPA and WPA2 security implemented without using the Wi-Fi Protected Setup feature are unaffected by the security vulnerability.

WPA and WPA 2

The Wi-Fi Alliance intended WPA as an intermediate measure to take the place of WEP pending the availability of the full IEEE 802.11i standard. WPA could be implemented through firmware upgrades on wireless network interface cards designed for WEP that began shipping as far back as 1999. However, since the changes required in the wireless access points (APs) were more extensive than those needed on the network cards, most pre-2003 APs could not be upgraded to support WPA.

The WPA protocol implements much of the IEEE 802.11i standard. Specifically, the Temporal Key Integrity Protocol (TKIP), was adopted for WPA. WEP used a 40-bit or 104-bit encryption key that must be manually entered on wireless access points and devices and does not change. TKIP employs a per-packet key, meaning that it dynamically generates a new 128-bit key for each packet and thus prevents the types of attacks that compromised WEP.

WPA also includes a message integrity check. This is designed to prevent an attacker from capturing, altering and/or resending data packets. This replaces the cyclic redundancy check (CRC) that was used by the WEP standard. CRC's main flaw was that it did not provide a sufficiently strong data integrity guarantee for the packets it handled. Well tested message authentication codes existed to solve these problems, but they required too much computation to be used on old network cards. WPA uses a message integrity check algorithm called Michael to verify the integrity of the packets. Michael is much stronger than a CRC, but not as strong as the algorithm used in WPA2. Researchers have since discovered a flaw in WPA that relied on older weaknesses in WEP and the limitations of Michael to retrieve the keystream from short packets to use for re-injection and spoofing.

WPA2 has replaced WPA. WPA2, which requires testing and certification by the Wi-Fi Alliance, implements the mandatory elements of IEEE 802.11i. In particular, it introduces CCMP, a new AES-based encryption mode with strong security. Certification began in September, 2004; from March 13, 2006, WPA2 certification is mandatory for all new devices to bear the Wi-Fi trademark

13.7.3 Virtual Private Network (VPN)

A virtual private network (VPN) extends a private network across a public network, such as the Internet. It enables a computer to send and receive data across shared or public networks as if it were directly connected to the private network, while benefitting from the functionality, security and management policies of the private network. This is done by establishing a virtual point-to-point connection through the use of dedicated connections, encryption, or a combination of the two.

A VPN connection across the Internet is similar to a wide area network (WAN) link between the sites. From a user perspective, the extended network resources are accessed in the same way as resources available from the private network.

VPNs allow employees to securely access their company's intranet while travelling outside the office. Similarly, VPNs securely and cost effectively connect geographically disparate offices of an organization creating one cohesive virtual network. VPN technology is also used by ordinary Internet to connect to proxy servers for the purpose of protecting one's identity.

Caution To prevent disclosure of private information, VPNs typically allow only authenticated remote access and make use of encryption techniques.

VPNs provide security by the use of tunneling protocols and through security procedures such as encryption. The VPN security model provides:

- confidentiality such that even if the network traffic is sniffed at the packet level (see network sniffer and Deep packet inspection), an attacker would only see encrypted data
- sender authentication to prevent unauthorised users from accessing the VPN.
- message integrity to detect any instances of tampering with transmitted messages

Secure VPN protocols include the following:

- Internet Protocol Security (IPsec) as initially developed by the Internet Engineering Task Force (IETF) for IPv6, which was required in all standards-compliant implementations of IPv6 before RFC 6434 made it only a recommendation. This standards-based security protocol is also widely used with IPv4 and the Layer 2 Tunneling Protocol. Its design meets most security goals: authentication, integrity, and confidentiality. IPsec uses encryption, encapsulating an IP packet inside an IPsec packet. De-encapsulation happens at the end of the tunnel, where the original IP packet is decrypted and forwarded to its intended destination.
- Transport Layer Security (SSL/TLS) can tunnel an entire network's traffic (as it does in the OpenVPN project) or secure an individual connection. A number of vendors provide remote-access VPN capabilities through SSL. An SSL VPN can connect from locations where IPsec runs into trouble with Network Address Translation and firewall rules.
- Datagram Transport Layer Security (DTLS) – used in Cisco Any Connect VPN and in OpenConnect VPN[9] to solve the issues SSL/TLS has with tunneling over UDP.
- Microsoft Point-to-Point Encryption (MPPE) works with the Point-to-Point Tunneling Protocol and in several compatible implementations on other platforms.
- Microsoft Secure Socket Tunneling Protocol (SSTP) tunnels Point-to-Point Protocol (PPP) or Layer 2 Tunneling Protocol traffic through an SSL 3.0 channel.
- Multi Path Virtual Private Network (MPVPN). Ragula Systems Development Company owns the registered trademark "MPVPN".

Secure Shell (SSH) VPN – Open SSH offers VPN tunneling (distinct from port forwarding) to secure remote connections to a network or to inter-network links. Open SSH server provides a limited number of concurrent tunnels. The VPN feature itself does not support personal authentication.

Self Assessment

Fill in the blanks:

7. A .... attacker entices computers to log into a computer which is set up as a soft AP.

8. .... poisoning is a type of attack where the Media Access Control (MAC) address is changed by the attacker.

9. A .... is a type of web attack that seeks to disrupt the normal function of the targeted computer network.

10. Wired Equivalent Privacy (WEP) is a security algorithm for .... wireless networks.

11. Twenty-six digits of four bits each gives 104 bits; adding the 24-bit IV produces the complete .... WEP key.

12. .... allow employees to securely access their company's intranet while travelling outside the office.

Case Study

Wireless Network Security

With the explosion in "WiFi" wireless networks, a new and very real threat to companies has emerged, against which most are as yet unprotected. Many organisations are introducing this new and very useful technology to their networks without fully understanding the security implications.

What Are the Dangers?

Recent intruder activities such as "warchalking" and "wardriving" have captured the media's attention and increased awareness of wireless network security risks. These risks are basically:

1. Unauthorised use of your internet connection.

   Alongside the enormous growth in WiFi, there is a broadband revolution going on. This means that fast internet connections could be used by intruders, causing excess traffic and overloading of your service.

2. Unauthorised access to your internal servers and confidential data.

   Given enough time, an intruder could work out your computer passwords and gain access to your data.

3. An intruder reading the network traffic as it flows across the network.

By using a WiFi listening tool, an intruder can listen in on network traffic. When a document is viewed from across the network, the intruder can see that information. This requires sophisticated software and some expertise on the part of the intruder, but is still a real danger.

Making Your Wireless Network More Secure

The designers of WiFi have incorporated measures to prevent intruders from gaining access to your wireless network. Depending on your specific requirements, you can use some or all of them. The main measures are as follows:

1. Introducing access lists. Each WiFi card has a unique identification number. Most WiFi networks have a list of allowed cards. Adding only your cards will stop an intruder's card from accessing your WiFi network.

2. Using encryption. A basic encryption is available in WiFi. Using this will stop an intruder from accessing your wireless network in the short term. It will also stop a casual intruder from seeing data on your network.

Contd...

Notes

3. Hiding your network. Most access points broadcast their WiFi name. This name is used to access a wireless network. Turning this feature off stops the WiFi network from drawing attention to itself. There are some further precautions you might consider taking, such as:

4. Monitoring WiFi traffic. Software is now available to allow a WiFi network owner to monitor cards that have access to the network. This can alert the network owner if an intruder gains access.

5. Implementing secure VPN for wireless users. For near impenetrability, a WiFi owner can introduce another level of security between the wireless network and the standard wired network. This is a costly exercise really only implemented on networks that contain particularly confidential and sensitive data.

Risks versus Benefits of Wireless

Wireless is a very flexible, cheap, highly useful and desirable new technology. There are very good reasons to implement it on your network. However, because it can offer intruders an entry point, you need to understand and guard against the dangers. Bridge Partners can help you weigh the benefits of wireless against the risks, and to manage these risks in line with your own security needs. By implementing some of the measures described here, you can greatly reduce the risk of a security breach and still enjoy the many benefits of WiFi.

Questions:

1. Discuss some risks related to wireless network security.

2. Discuss the measures to prevent intruders from gaining access to your wireless network.

Source: http://www.bridgepartners.co.uk/wireless-network-security

13.8 Summary

- Wireless security is the prevention of unauthorised access or damage to computers using wireless networks. The most common types of wireless security are Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA).
- The risks to users of wireless technology have increased as the service has become more popular.
- Wireless networking is inherently risky because you are transmitting information via radio waves. Data from your wireless network can be intercepted just like signals from your cellular or cordless phones.
- The modes of unauthorised access to links, to functions and to data is as variable as the respective entities make use of program code.
- Non-traditional networks such as personal network Bluetooth devices are not safe from cracking and should be regarded as a security risk.
- Address Resolution Protocol (ARP) poisoning is a type of attack where the Media Access Control (MAC) address is changed by the attacker. Also, called an ARP spoofing attacks, it is effective against both wired and wireless local networks.
- Wired Equivalent Privacy (WEP) is a security algorithm for IEEE 802.11wireless networks.
- Although its name implies that it is as secure as a wired connection, WEP has been demonstrated to have numerous flaws and has been deprecated in favour of newer standards such as WPA2.

Notes

- A virtual private network (VPN) extends a private network across a public network, such as the Internet.
- VPNs allow employees to securely access their company's intranet while travelling outside the office.
- VPNs provide security by the use of tunneling protocols and through security procedures such as encryption.

13.9 Keywords

Address Resolution Protocol (ARP): Poisoning is a type of attack where the Media Access Control (MAC) address is changed by the attacker.

Denial-Of-Service (DOS): DOS Occurs when an adversary causes a system or a network to become unavailable to legitimate users or causes services to be interrupted or delayed.

Distributed Denial of Service attack: It is a type of web attack that seeks to disrupt the normal function of the targeted computer network.

Identity theft (or MAC spoofing): It occurs when a cracker is able to listen in on network traffic and identify the MAC address of a computer with network privileges.

Manipulation: It means that data has been inserted, deleted, or otherwise modified on a system or during transmission.

Masquerading: It refers to the act of an adversary posing as a legitimate user in order to gain access to a wireless network or a system served by the network.

Repudiation: is when a user denies having performed an action on the network.

Virtual private network (VPN): VPN extends a private network across a public network, such as the Internet.

Wired Equivalent Privacy (WEP): WEP is a security algorithm for IEEE 802.11 wireless networks. Introduced as part of the original 802.11 standard ratified in September 1999, its intention was to provide data confidentiality comparable to that of a traditional wired network.

Wireless security: It is the prevention of unauthorised access or damage to computers using wireless networks.

13.10 Review Questions

1. Describe denial of service.
2. Describe the concept of security threats.
3. Explain the need for wireless security.
4. Explain the procedure of traffic monitoring.
5. What are the various types of protective actions?
6. What do you mean by unauthorised access?
7. What is middle attacks?

Answers: Self Assessment

1. Manipulation
2. Repudiation
3. Security
4. Cracker

5. MAC filtering
6. Injection
7. man-in-the-middle
8. Address Resolution Protocol (ARP)
9. Distributed Denial of Service attack
10. IEEE 802.11
11. 128-bit
12. VPNs

13.11 Further Readings

Books

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

John Ross, *Introduction to wireless networks.*

Vijay Garg, *Wireless Communications & Networking.*

Theodore S. Rappaport, *Wireless Communications: Principles and Practice.*

Online links

http://whatismyipaddress.com/ddos-attack

http://www.incapsula.com/ddos/ddos-attacks/denial-of-service

http://www.computer-network-security-training.com/what-is-arp-poisoning/

Notes

Unit 14: Authentication

CONTENTS

Objectives

Introduction

14.1 Concept of User Authentication

14.1.1 Importance of User Authentication

14.1.2 Creating Strong User Authentication

14.1.3 Approaches in User Authentication

14.1.4 Risk-Based Analytics

14.1.5 Compensating Controls

14.1.6 Emerging Megatrends Developments in the Online User-Authentication Space

14.1.7 Authentication vs. Authorization

14.2 The 802.11 Authentication Vulnerabilities

14.2.1 Use of SSID

14.2.2 Open Authentication Vulnerabilities

14.2.3 Shared Key Authentication Vulnerabilities

14.2.4 MAC Address Authentication Vulnerabilities

14.3 Medium Access Control (MAC) Filters

14.4 Public-key Cryptography

14.4.1 How Public-key Cryptography Works

14.4.2 Putting Public Key Cryptography Together with Message Security

14.4.3 Public Key Cryptography and Digital Signatures

14.4.4 Public Key Cryptography and Message Encryption

14.4.5 Understanding How Public Key Cryptography in Digital Signatures and Message Encryption Work Together

14.5 The 802.1X

14.6 Security Policies

14.6.1 Data Security Policy

14.6.2 End-User Security

14.7 Summary

14.8 Keywords

14.9 Review Questions

14.10 Further Readings

Objectives

After studying this unit, you will be able to:

- Discuss the concept of User Authentication
- Describe the 802.11 Authentication Vulnerabilities
- Explain the Medium Access Control (MAC) Filters
- Define concept of Public-key Cryptography
- Discuss the 802.1X
- Explain the Security Policies

Introduction

Identification and authentication are used to establish a user's identity. It appears that a user-authentication system for consumer communities on the Web is growing beyond the traditional database-driven and/or directory-driven component of a Web application, for organizations that have higher data-confidentiality requirements. Implementation approaches for strong authentication span a full spectrum that ranges from highly integrated and interconnected/dependent to simple extensions of existing stand-alone architectures. The escalating trend of moving data and services into the cloud also necessitates methodical planning to ensure secure access to authorized users over the Internet. While existing simple-password–based authentication might continue to work for many consumer-oriented Web sites, its inherent vulnerabilities have been identified as security risks for institutions that have higher data-privacy requirements. To mitigate the risk of online identity fraud, organizations look to strong user authentication as the solution for improving their Web-based authentication systems.

14.1 Concept of User Authentication

User authentication is a means of identifying the user and verifying that the user is allowed to access some restricted service. Identity theft remains one of the more prevalent issues on the Internet today. Still digital identity fraud is still on the rise, with an increase in sophistication (that is, "phishing," "man-in-the-middle," DNS poisoning, malware, social engineering, and so forth) and an expansion of attack vectors (that is, unregulated financial systems, lottery and sweepstakes contests, healthcare data, synthetic identities, and so on). With the upward trend of moving data and services into the Web and cloud-based platforms, the management and control of access to confidential and sensitive data is becoming more than verifying simple user credentials at the onset of user sessions for one application, and with higher interconnectivity and interdependencies among multiple applications, services, and organizations.

One of the more exploited methods today is the gaining of account access by stealing reusable credentials for Web sites that have not yet implemented "strong" user authentication. This is so, because most common forms of credentials today are knowledge-based (that is, user ID and password) and are requested only once during sign-on, which provides a higher level of convenience to users, but also requires less effort for attackers to exploit. Many attacks are manifested as "phishing" messages that masquerade as ones that are sent by legitimate organizations and contain URLs that point to fraudulent Web sites that have the same appearances as genuine ones. Often, they act as "man-in-the-middle" and eventually do forward visitors to the actual Web sites; but, in the process, they have captured valid credentials that can be used to gain access to actual accounts.

The ease with which online identities can be stolen and used effectively has prompted many organizations and governing bodies to raise alarms. In the U.S., the October 2005 Federal Financial Institutions Examination Council (FFIEC) "Authentication in an Internet Banking Environment" guide identified that simple-password authentication is insufficient for ensuring authorized access to important financial services. Many other regulatory provisions also have identified similar needs, such as the Homeland Security Presidential Directive (HSPD)-12, Electronic Signatures in Global and National Commerce (E-SIGN) Act, Federal Information Processing Standards Publication (FIPS PUB) 201-1, HIPAA, SOX, GLBA, PATRIOT, and so on.

Subsequently, various methods have been developed to improve the "strength" of an authentication system in withstanding identity-theft attacks. While the spectrum of methods spans a wide range of concern areas—such as enterprises, consumers, hardware, mobility, and so on—this article focuses on methods that are used to implement strong user authentication for online-consumer identities. It discusses effective solution approaches, overall architecture design, and emerging developments.

14.1.1 Importance of User Authentication

Each user is required to log in to the system. The user supplies the user name of an account and a password if the account has one (in a secure system, all accounts must either have passwords or be invalidated). If the password is correct, the user is logged in to that account; the user acquires the access rights and privileges of the account. The /etc/passwd and /etc/security/passwd files maintain user passwords.

By default users are defined in the Files registry. This means that user account and group information is stored in the flat-ASCII files. With the introduction of plug-in load modules, users can be defined in other registries too. For example, when the LDAP plug-in module is used for user administration, then the user definitions are stored in the LDAP repository. In this case there will be no entry for users in the /etc/security/user file (there is an exception to this for the user attributes SYSTEM and registry). When a compound load module (i.e. load modules with an authentication and database part) is used for user administration, the database half determines how AIX® user account information is administrated, and the authentication half describes the authentication and password related administration. The authentication half may also describe authentication-specific user account administration attributes by implementing certain load module interfaces (newuser, getentry, putentry, etc).

The method of authentication is controlled by the SYSTEM and registry attributes that are defined in the /etc/security/user file. A system administrator can define the authcontroldomain attribute to the /etc/security/login.cfg file to force the SYSTEM and registry attributes to be retrieved from the authcontroldomain. For instance, authcontroldomain=LDAP forces the system to look for user's SYSTEM and registry from LDAP to determine the authentication method that was used for the user. There is an exception for locally defined users where the authcontroldomain setting is ignored, and the SYSTEM and registry are always retrieved from /etc/security/user file.

The acceptable token for the authcontroldomain attribute is files or a stanza name from the/usr/lib/security/methods.cfg file.

The value of the SYSTEM attribute is defined through a grammar. By using this grammar, the system administrators can combine one or more methods to authenticate a particular user to the system. The well known method tokens are compat, DCE, files and NONE.

The system default is compat. The default SYSTEM=compat tells the system to use the local database for authentication and, if no resolution is found, the Network Information Services (NIS) database is tried. The files token specifies that only local files are to be used during authentication, whereas SYSTEM=DCE results in a DCE authentication flow.

The NONE token turns off method authentication. To turn off all authentication, the NONE token must appear in the SYSTEM and auth1 lines of the user's stanza.

You can specify two or more methods and combine them with the logical constructors AND and OR. For instance SYSTEM=DCE OR compat indicates that the user is allowed to login if either DCE or local authentication (crypt()) succeeds in this given order.

In a similar fashion a system administrator can use authentication load module names for the SYSTEM attribute.

Example: When SYSTEM attribute is set to SYSTEM=KRB5files OR compat, the AIX host will first try a Kerberos flow for authentication and if it fails, then it will try standard AIXauthentication.

SYSTEM and registry attributes are always stored on the local file system in the/etc/security/user file. If an AIX user is defined in LDAP and the SYSTEM and registry attributes are set accordingly, then the user will have an entry in the /etc/security/user file.

The SYSTEM and registry attributes of a user can be changed using the chuser command.

Acceptable tokens for the SYSTEM attribute can be defined in the /usr/lib/security/methods. cfgfile.

Notes The root user is always authenticated by means of the local system security file. The SYSTEMattribute entry for the root user is specifically set to SYSTEM=compat in the/etc/security/user file.

Alternative methods of authentication are integrated into the system by means of the SYSTEMattribute that appears in /etc/security/user. For instance, the Distributed Computing Environment (DCE) requires password authentication but validates these passwords in a manner different from the encryption model used in etc/passwd and /etc/security/passwd. Users who authenticate by means of DCE can have their stanza in /etc/security/user set to SYSTEM=DCE.

Other SYSTEM attribute values are compat, files, and NONE. The compat token is used when name resolution (and subsequent authentication) follows the local database, and if no resolution is found, the Network Information Services (NIS) database is tried. The files token specifies that only local files are to be used during authentication. Finally, the NONE token turns off method authentication. To turn off all authentication, the NONE token must appear in the SYSTEM and auth1 lines of the user's stanza.

Notes The root user is always authenticated by means of the local system security file. The SYSTEM attribute entry for the root user is specifically set to SYSTEM = "compat" in /etc/security/user.

14.1.2 Creating Strong User Authentication

The most common solution approaches that are used today involve, in more generalized terms, various forms of enhanced shared-secret and/or multifactor authentication.

Enhanced shared-secret authentication refers to extensions of conventional knowledge-based (single-factor) authentication—for example, additional passwords, site keys, preregistered graphical icons to support mutual authentication, challenge-response, randomised code selections that are based on input patterns, CAPTCHA, and so on.

Multifactor authentication refers to a compound implementation of two or more classes of human-authentication factors:

- Something known to only the user—Knowledge-based (for example, password, pass phrase, shared secrets, account details and transaction history, PIN, CAPTCHA, and so on).

- Something held by only the user—Possession-based (for example, security token, smart card, shared soft tokens, mobile device, and so on).
- Something inherent to only the user—Biological or behaviour biometric traits (for example, facial recognition, fingerprint, voice recognition, keystroke dynamics, signature, and so on).

Example: Many enterprise extranet/VPN solutions today require both simple credentials (something known, such as ID and password) and hardware tokens (something held, such as secure ID with time-based one-time password generators, smart cards that use embedded PKI solutions, and so on) in order to gain access. The combination of the two "known" and "held" factors makes up the multifactor authentication method, and significantly improves the authentication strength, as it curtails the threat of stolen digital identities.

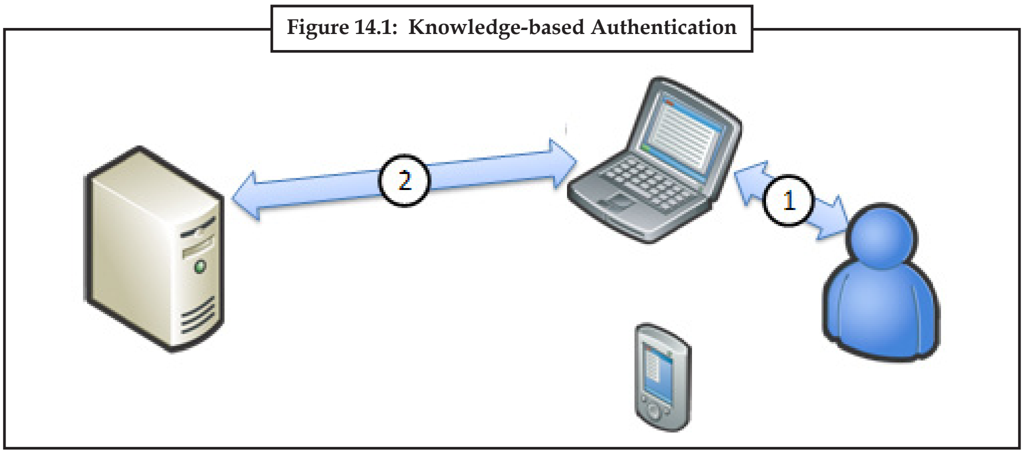
In practice, however, there is a wealth of implementations, methods, and permutations of them—all with varying trade-offs in terms of cost, complexity, usability, and security. Next, let's discuss viable solution approaches.

14.1.3 Approaches in User Authentication

Following are the approaches in User Authentication:

1. ***Solution Approaches:*** Now, not all of the available strong-authentication options that are available today lend themselves well to the Web. Conventional multifactor authentication methods (that involve the deployment of custom hardware tokens, such as RSA SecurID, smart cards, and so on) are effective for closed communities—such as employees and partners—but they are too costly, inconvenient, and logistically difficult—for example, distribution, administration, management, support, and so on—for the open consumer communities on the Web. In this case, authentication solutions have to work primarily within the confines of the browser's security sandbox. Here, we discuss a few solution approaches that are relatively cost-effective to implement for online consumers, based on today's standards:

Figure 14.1: Knowledge-based Authentication



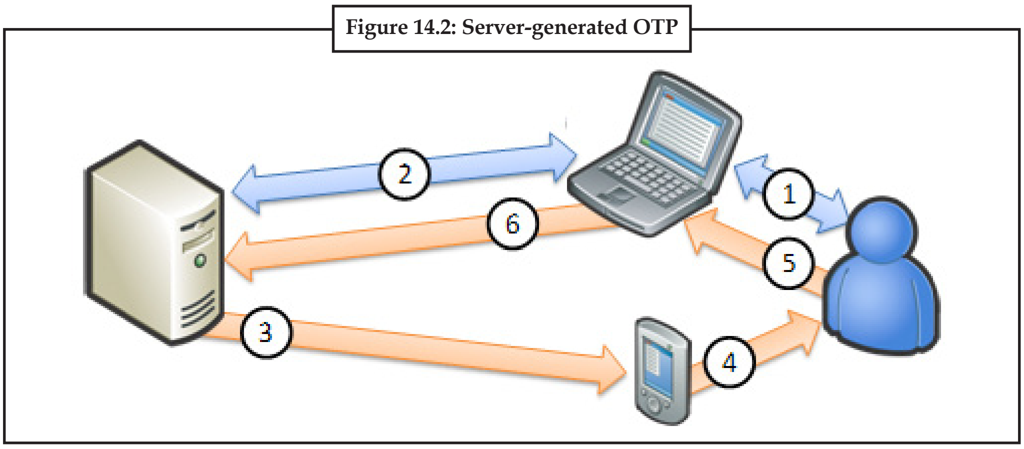
Source: http://msdn.microsoft.com/en-us/library/cc838351.aspx#_Architectural_Perspectives

Knowledge-based authentication (KBA) (Figure 14.1) typically is implemented as extensions to existing simple-password authentication. Knowledge-based credentials include chosen information, personal and historical information, on-hand information, deductive and derived responses, patterns, images, and so on. However, it generally boils down to additional set(s) of challenge-response that allows users to prove that the claimed identities belong to them. Some well-known examples include Bank of America's

Notes

"SiteKey," HSBC's virtual keyboard, and so on. KBA is used also as an identity-verification method for self-service password-reset processes; but, when implemented effectively, they can be used as methods to complement primary authentication. This approach moderately improves authentication strength, as it is still single-factor (in-band within the browser) and prone to phishing attacks, but it might be sufficient for some Web sites.

Figure 14.2: Server-generated OTP

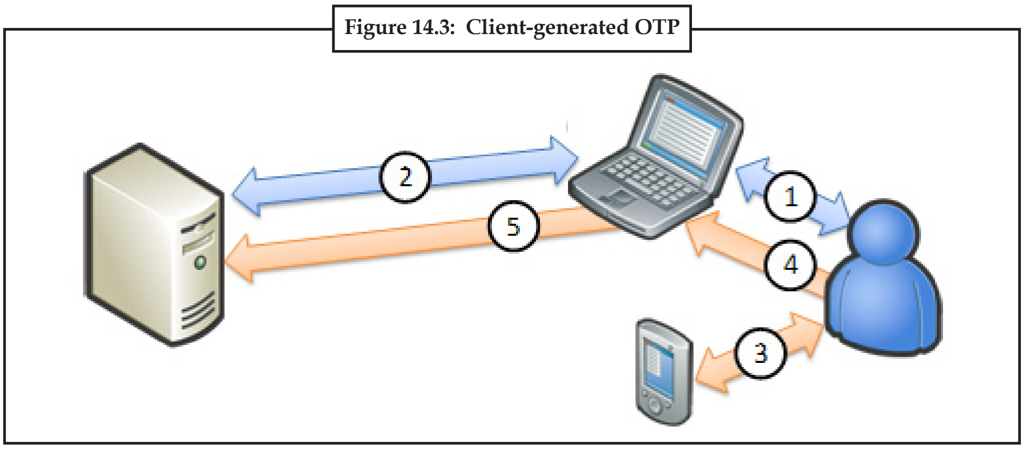


Source: http://msdn.microsoft.com/en-us/library/cc838351.aspx#_Architectural_Perspectives

Server-generated one-time passwords (OTPs) (Figure 14.2) commonly are implemented as randomised password strings that are generated in real time after verifying simple-password credentials. Some more advanced implementations combine KBA elements to facilitate derived OTPs (such as server-generated grid cards for shared pattern recognition, digitally signed OTPs that are based on server-generated data, and so on). The generated OTPs then are delivered to users via a different channel (out-of-band) from the session in the browser, such as e-mail, SMS (Short Message Service) text messaging to mobile devices, direct phone calls that use computer-generated speech, and so on. Users then can use the OTP to sign-in to the application, by entering it into a designated field on the page.

Many organizations in the public sector have started to deploy this type of solution to implement strong user authentication. This approach significantly improves authentication strength as it employs two-factor authentication and out-of-band delivery of OTPs. However, it still is not completely secure, as it is prone to the "man-in-the-middle" real-time phishing attacks that try to capture and use the OTP in real time. Plus OTP delivery latencies potentially could affect overall user experience.

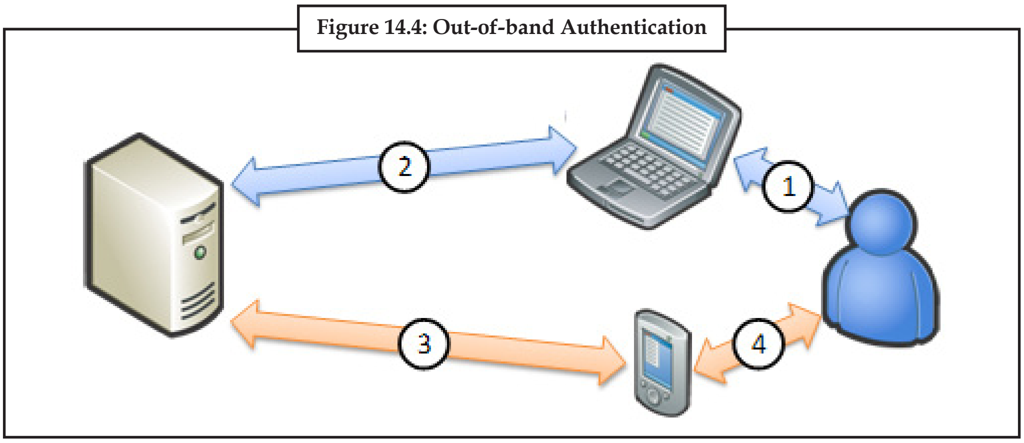
Figure 14.3: Client-generated OTP



Source: http://msdn.microsoft.com/en-us/library/cc838351.aspx#_Architectural_Perspectives

Client-generated one-time passwords (Figure 14.3) are similar to conventional OTP hardware tokens (such as RSA SecurID, VeriSign VIP OTP, and so on). However, with the level of near-ubiquitous proliferation of mobile devices today, cellular phones have become a viable alternative as the soft-token (or "something held") authentication factor. In this case, individualized cryptographic software components can be installed on mobile devices to generate time-based or event-based OTPs. Users then can use the OTP to sign-in to the application after authenticating simple Web-based credentials (examples include RSA SecurID software, Java ME applications, and so on). This approach has the benefits of OTPs, not having to deal with out-of-band delivery latencies and inconsistent service coverage.

Figure 14.4: Out-of-band Authentication



Source: http://msdn.microsoft.com/en-us/library/cc838351.aspx#_Architectural_Perspectives

Out-of-band (OOB) (Figure 14.4) authentication leverages the second factor for authentication, instead of delivery of individualized information. Current implementations include speech recognition that is facilitated via out-bound or in-bound voice calls (to/from land or cellular lines) or KBA via SMS request/reply. This type of solution offers higher authentication strength, as both the browser and a second factor are used to verify credentials, which works to impede common phishing attacks.

In general, these high-level approaches rank in increasing relative authentication strength. However, higher authentication strength does not necessarily represent the best-of-breed solution, as security often requires trade-offs in user convenience. Studies indicate that different user populations respond differently to strong-authentication methods. The choice of an approach (or combinations of approaches) should consider user segments, as well as the types of activities and interactions that they perform with the application.

Example: Online consumers who view account balances (considered a relatively low-risk type of activity) should require comparatively less effort to access than consumers who conduct account transfers or physicians who view patient's medical records.

Finally, the implementation of strong user authentication often is a balancing act between security and usability. Many implementations have not achieved their intended effectiveness by either delivering significantly deteriorated user experiences or compromising security postures by simply satisfying requirements on paper. Furthermore, there is no one-size-fits-all solution approach. For example, not all Web sites require multifactor authentication, while enhanced knowledge-based authentication might be "secure enough"; and some carefully designed single-factor methods actually might be "stronger" than some multifactor methods. A well-balanced design tends to be more cost-effective than force-fitting various best-of-breed approaches into one solution.

2. *Architectural Perspectives:* We've just discussed how strong user authentication can be implemented as a component of a Web application architecture. Are there other areas of concerns and challenges that we should pay attention to, and how does this component affect or relate to the rest of the architecture?

   From an architectural perspective, strong user authentication involves more than just ensuring an effective identity and credentials verification at the point of user sign-on. A fully integrated and highly coordinated architecture is required to deliver an effective strong user authentication.

3. *Identity Proofing Approach:* Identity proofing is the process of verifying user identities (for example, if a user is indeed who the individual claims to be) before provisioning user credentials. A strong user-authentication implementation is ineffective, and the identity infrastructure becomes unreliable, if verifiable identity assurance cannot be ensured.

   In-person identity proofing that is based on valid IDs and credentials remains one of the more reliable methods today, and is commonly used by various financial, government, and healthcare organizations. On the other hand, in self-service scenarios in which identity proofing is handled completely online, organizations typically use knowledge-based systems to verify user identities. However, in this case, the pieces of information that are requested from an individual for identification purposes should be resistant to social-engineering attacks.

   Furthermore, the same level of identity proofing is required also when reissuing credentials (for example, resetting passwords, recovering forgotten IDs, requesting elevated access, and so on) and terminating credentials. Compromising the level of strength in identity proofing in any stage of an identity's life cycle will affect adversely the overall effective authentication strength.

   The point at which user provision occurs is also where additional authentication factors should be registered and associated with a new user's profile; these factors are used then to support strong user authentication—for example, answering sets of challenge-response to support KBA, registering/verifying a mobile phone number to support out-of-band OTP delivery, capturing voice recordings to support speech recognition, and so forth.

4. *Integration Architecture Approach:* A comprehensive, robust, and reliable user-authentication system is becoming more than a database-driven component of one stand-alone application. A strong-authentication system must be tightly integrated and synchronized with the security infrastructure in an organization, such as identity management (IdM), Web access management (WAM), enterprise single sign-on (ESSO), certificate and key management (PKI), vulnerability management, audit management, policy management, user directories/repositories, and so on. In some cases, these systems provide capabilities that can be leveraged to implement a strong-authentication system, while some downstream systems depend on the authentication system to pass relevant contextual information and authenticating decisions (for example, role-mapping) that are needed for user authorization and access control.

   Increasingly, an organization's security infrastructure will include capabilities that live in the cloud (or are hosted by other service providers). Although these services do not reside in an organization's own infrastructure, the same integration concerns and security-access policies and requirements still must be applied consistently, in order to maintain a uniformly reliable security architecture.

5. *Layered Approach:* The initial logon page does not have to be the only point at which users are authenticated. A layered approach can be implemented, so that different strength levels of authentication are implemented in different areas, according to the varying levels of data confidentiality and/or value. When it is implemented with a balanced design between

data requirements and authentication strengths and points, this approach can improve overall usability while ensuring security, as it allows convenient access to less confidential areas of a Web site, and more credentials are required only to access the more confidential areas. Furthermore, additional authentication/verification can be required on individual transactions that are deemed more risky. These potentially can leverage the stronger authentication methods, such as multifactor and out-of-band authentication approaches.

Alternatively, in systems that have implemented role-based access control (RBAC) for user authorization, different methods of authentication can be presented to users who are mapped to different roles; or, in a more dynamic implementation, if a user logs on by using partial credentials (when higher-strength credentials are made optional), that user is mapped to a role that has lower access privileges for that Web session.

14.1.4 Risk-Based Analytics

Risk-based analytics are similar to what credit card companies use to assess risk levels for each requested transaction and make authorization decisions in real time. Assessments are based on real-time evaluation of various data points that are collected about the user and the requested transaction; depending on the scoring and data-confidentiality requirements, a transaction can be authorized or unauthorised, or additional credentials can be requested from the user to facilitate stronger authentication and reliable auditing.

The data points that are collected often are contextual information (or location-based, behavior-based, and so on) and used as supplemental credentials to support strong authentication. For example, client-device identification (CDI) can be used to simplify valid repeated authentication requirements from the same client device, if a verified set of credentials has signed in to a Web site from the same device previously. This is often facilitated by saving specific "remember me" cookies, and sometimes by using a combination of data points that are collected from the HTTP request and client-side JavaScript code. Subsequently, based on the risk-based assessment that the same user had signed in successfully to the same application previously, a lower-strength authentication is presented to the user to improve convenience.

Historical and social data points also are included often in the risk assessment, and often are used from the perspective of transaction-anomaly detection (TAD), as these data points help establish a "normal" usage profile about a user and can be compared against the requested transaction to identify contextual anomalies.

Example: A transaction that is identified with unusual characteristics (for example, originating from a different physical location, different client device, unusual time of day/week, fund transfers to new and unverified account, and so on) contributes to a higher risk profile, which prompts the authentication system to require stronger authentication from the user in order to authorize the transaction.

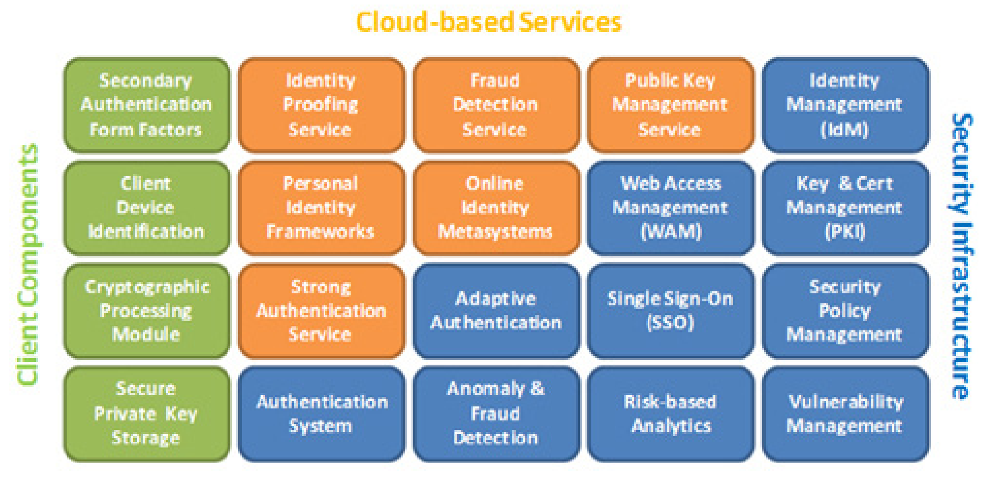
This is also referred to as fraud detection, and it works well together with a layered approach to implement a dynamically adaptive authentication system.

14.1.5 Compensating Controls

An authentication system also can take into account other components that are not integrated directly into this architecture, which can potentially influence (positively or negatively) users' security postures and/or risk profiles, and contribute to risk-based analysis. For example, Extended Validation SSL (EV-SSL), digital watermarking, site keys, and so on contribute to mutual authentication and help improve end-user behaviour, which in a way improves the risk profile. Host intrusion detection, anti-spyware, anti-phishing network services, and so on all contribute to a user's overall risk profile.

Finally, the view of authentication architecture that is presented here falls on the more comprehensive and complex side of the various design approaches. It certainly is not required for all organizations to implement all of the identified capabilities, but can serve as a reference to each implementation project to support evaluation of required capabilities, and assess how they should be implemented—although some complex enterprise environments might require this level of meticulous planning and design in order to deliver an effective identity-assurance infrastructure and proficiently safeguard important data.

Figure 14.5: Strong User Authentication Architecture Components


Cloud-based Services
Client Components
Security Infrastructure
Secondary Authentication Form Factors
Identity Proofing Service
Fraud Detection Service
Public Key Management Service
Identity Management (IdM)
Client Device Identification
Personal Identity Frameworks
Online Identity Metasystems
Web Access Management (WAM)
Key & Cert Management (PKI)
Cryptographic Processing Module
Strong Authentication Service
Adaptive Authentication
Single Sign-On (SSO)
Security Policy Management
Secure Private Key Storage
Authentication System
Anomaly & Fraud Detection
Risk-based Analytics
Vulnerability Management

Source: http://msdn.microsoft.com/en-us/library/cc838351.aspx#_Architectural_Perspectives

However, regardless of how simple or complex each implementation might be, it is necessary that security policies and authentication systems be applied homogeneously to all user-contact surfaces.

Caution An inconsistent implementation across the entire operational architecture could expose certain loopholes for attackers to exploit; and, sometimes, these can include nontechnical areas, such as administrative processes, instructions for call-centre customer service reps, and so on.

14.1.6 Emerging Megatrends Developments in the Online User-Authentication Space

Several emerging megatrends also influence developments in the online user-authentication space. Let's discuss both their impacts and how they are related to strong user-authentication concerns.

1. ***Cloud Computing:*** From a user-authentication perspective, moving data into the cloud and integrating cloud-based services should be implemented with the same level of overall effective authentication strength as the enterprise perspective of authentication architecture. However, organizations have significantly less control over the authentication strengths of the interdependent cloud-based services of their counterparts/partners. For example, whether via identity federation or delegation, the overall security posture of the resulting interconnected architecture can be compromised if the integrated services themselves have comparatively lower-strength authentication systems in place.

   The same is true for SaaS (software-as-a-service) providers, as extra attention must be focused on ensuring appropriate levels of authentications strengths for different user communities in a multitenancy model, without compromising overall and individual security and usability.

Thus, the focus on authentication systems becomes one of the primary evaluation factors for organizations that are looking to adopt cloud-based services. Organizations must ensure that service providers provide the flexibility to deliver varying levels of strong authentication to meet required security policies, or extend existing security implementations by leveraging identity federation (via SAML or WS-Federation) or authentication delegation to support single sign-on (SSO) or reduced sign-on (RSO). However, in these cases, organizations must incur the costs to deploy secure and accessible identity-federation and/or authentication-delegation services.

From a capabilities perspective, many of the authentication architecture components are being deployed as cloud-based services—for example, identity-proofing services that are deployed by credit bureaus, consumer-identity frameworks and providers, vulnerability-management networks, PKI and certificate-management services, secondary-factor channel providers (voice telephony, SMS messaging, speech recognition, patterns recognition, and so forth), fraud detection, strong-authentication service providers, and so on. These services provide much-needed capabilities to compose a strong-authentication system; however, the same integration-security concerns remain such that any one weak link in the connected-systems architecture will compromise the overall security posture.

2. ***Identity Metasystems:*** The consumer-identity frameworks that are available now as cloud-based platforms and their growing adoption means that organizations eventually will need to integrate these identity metasystems to improve user convenience—for example, OpenID identity providers, Google Account, Windows Live ID, Yahoo! ID, and so on—although, in order to integrate these online communities, the authentication strengths that are implemented for these services must be evaluated against the security policies and requirements for the organizations that are looking to leverage them.

   Similarly, online identity providers increasingly will need to add flexibility to configure varying levels of authentication strengths for different user segments, in addition to integrating various authentication form factors and standards (Higgins, PKCS, OpenID, Windows Cardspace, and so on) if they intend to provision services to data-sensitive organizations.

3. ***Smart-Card Proliferation:*** With the availability of more sophisticated smart-card solutions and ecosystem support, more physical credentials are adopting smart-card (standard plastic cards embedded with microprocessors and/or integrated circuits) deployments. For example, many countries and states (for example, Austria, Belgium, Estonia, Hong Kong, and Spain) already have rolled out government-sponsored electronic ID programs to national citizens. Subsequently, smart cards are becoming another form of authentication factor, where smart-card readers are available and are integrated into authentication systems.

   Furthermore, many vendors are consolidating multiple authenticators into the ISO 7816 smart-card form factor—for example, integrated LCDs to display OTPs, and biometric (fingerprint) readers. We might find smart-card deployments materialize in more cases, such as from financial institutions that already are issuing physical credentials (that is, credit cards, debit cards, and so on). Cryptographic smart cards that use biometric readers provide very high identity assurance, as they tightly bind the private keys to the users' biometrics (multifactor authentication).

4. ***Mobile Identity:*** From a physical-hardware perspective, SIM (Subscriber Identity Module) cards have improved significantly in terms of storage capacity and capability to perform cryptographic processing. Computing power and memory capacity also have improved exponentially in mobile devices. Subsequently, the SIM card and mobile phone have become the smart card and smart-card reader that constitute the most ubiquitous "something held" (or in-possession) authentication factor.

This makes it possible to store symmetric keys on SIM cards and, along with simple cryptographic software modules, to turn the mobile device into a seeded OTP generator. The generated OTPs can be used as credentials for out-of-band, multifactor authentication.

Furthermore, with wireless data plans, mobile devices can communicate directly with authentication systems by using wireless PKI. In this case, SIM cards provide secure storage of users' private PKI keys. The private keys then can be used to facilitate strong authentication—implemented with corresponding certificates to facilitate digital signatures—and, in some cases, to facilitate client-authenticated SSL. Some of the projected applications of this approach include mobile banking, contactless/proximity mobile payments, identity and credential verification, and so on. At some point, mobile devices might become the most ubiquitous form of mobile digital identities for consumers.

14.1.7 Authentication vs. Authorization

It is easy to confuse the mechanism of authentication with that of authorization. In many host-based systems (and even some client/server systems), the two mechanisms are performed by the same physical hardware and, in some cases, the same software.

It is important to draw the distinction between these two mechanisms, however, since they can (and, one might argue, should) be performed by separate systems.

What, then, distinguishes these two mechanisms from one another?

Authentication is the mechanism whereby systems may securely identify their users. Authentication systems provide an answers to the questions:

- Who is the user?
- Is the user really who he/she represents himself to be?

An authentication system may be as simple (and insecure) as a plain-text password challenging system (as found in some older PC-based FTP servers) or as complicated as the Kerberos system described elsewhere in these documents. In all cases, however, authentication systems depend on some unique bit of information known (or available) only to the individual being authenticated and the authentication system – a shared secret. Such information may be a classical password, some physical property of the individual (fingerprint, retinal vascularization pattern, etc.), or some derived data (as in the case of so-called smart card systems). In order to verify the identity of a user, the authenticating system typically challenges the user to provide his unique information (his password, fingerprint, etc.) – if the authenticating system can verify that the shared secret was presented correctly, the user is considered authenticated.

Authorization, by contrast, is the mechanism by which a system determines what level of access a particular authenticated user should have to secured resources controlled by the system. For example, a database management system might be designed so as to provide certain specified individuals with the ability to retrieve information from a database but not the ability to change data stored in the database, while giving other individuals the ability to change data. Authorization systems provide answers to the questions:

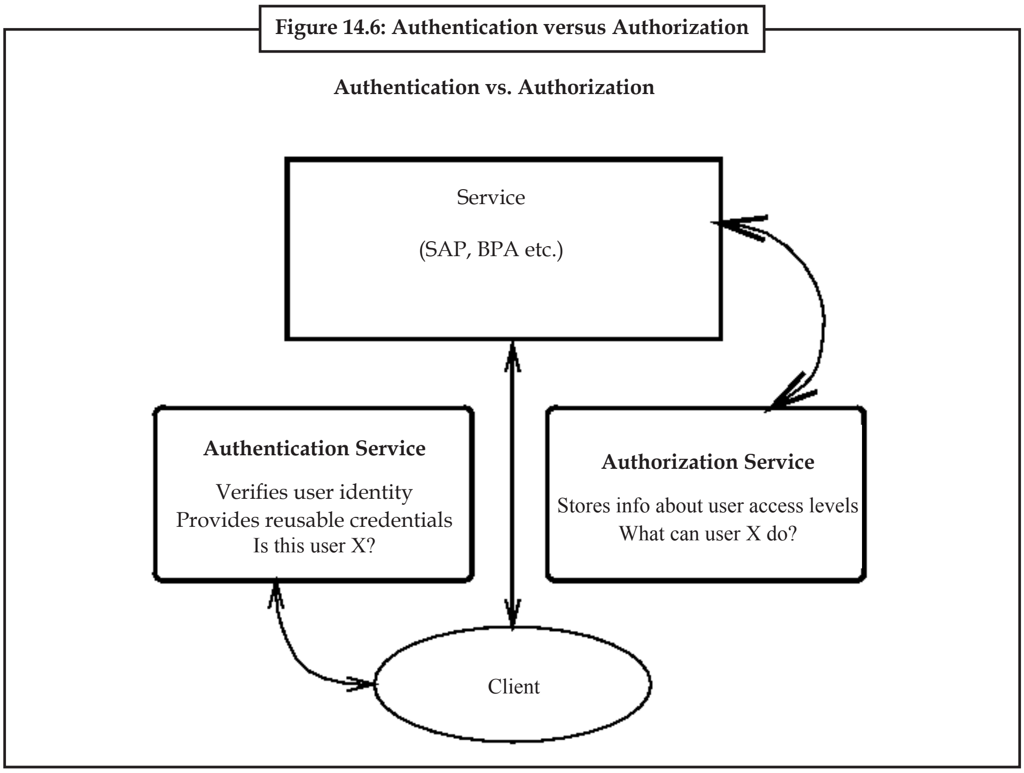
- Is user X authorized to access resource R?
- Is user X authorized to perform operation P?
- Is user X authorized to perform operation P on resource R?

Authentication and authorization are somewhat tightly-coupled mechanisms – authorization systems depend on secure authentication systems to ensure that users are who they claim to be and thus prevent unauthorised users from gaining access to secured resources.

Figure 14.6, below, graphically depicts the interactions between arbitrary authentication and authorization systems and a typical client/server application.

Notes

Figure 14.6: Authentication versus Authorization



Source: http://people.duke.edu/~rob/kerberos/authvauth.html

In the Figure 14.6 above, a user working at a client system interacts with the authentication system to prove his identity and then carries on a conversation with a server system. The server system, in turn, interacts with an authorization system to determine what rights and privileges the client's user should be granted.

Task: As security pass cards are often used to gain entry into areas and buildings with restricted access. Find out what data is kept on an encoded security pass card and how they work.

Self Assessment

State whether the following statements are true or false:

1. Each user is required to log in to the system.
2. Server-generated one-time passwords are similar to conventional OTP hardware tokens.
3. Authorization is the mechanism whereby systems may securely identify their users.

14.2 The 802.11 Authentication Vulnerabilities

With the rapidly increasing adoption of 802.11 technology, WLAN products have become mainstream and increasingly common in business, education, and home environments. The enhanced mobility and productivity offered by wireless technology, along with the long-term cost saving and ease of installation, have attracted organizations to make the move to this innovative technology. However, both federal departments and private companies are deploying wireless networks often without fully understanding the security risks associated with their use.

In today’s fast-paced world, Ethernet continues its dominance on the LAN. Defined by the Institute of Electrical and Electronic Engineers (IEEE) with the 802.3 standard, Ethernet has provided an evolving, cooperative, scalable and interoperable networking standard. With line speeds ranging from 10 mbps to 1000 mbps, Ethernet has attempted with fairly good success to keep pace with the public demand for higher bandwidth. Twelve years ago the IEEE established the 802.11 Working Group to create a wireless local area network (WLAN) standard. The standard specified an operating frequency in the 2.4 GHz band, which lay the groundwork for this technology. In 1997 the group approved IEEE 802.11 as the first WLAN standard. Data rates for 802.11 at that time were a mere 1 and 2 Mbps. Due to the disparity between the 1 to 2 mbps WLAN and the current wired LAN with speeds of 10–100 mbps, the committee quickly agreed that more work needed to be done in this area, that is, a technology that was more scalable and faster. The group began work on another 802.11 extension that would satisfy these future needs. In 1999, the group approved two new extensions to 802.11 which were designed to work with the existing 802.11 MAC layer, one being the IEEE 802.11a – 5GHz, and the other IEEE 802.11b – 2.4GHz.

Wireless LANs, because of their broadcast nature, require the addition of:

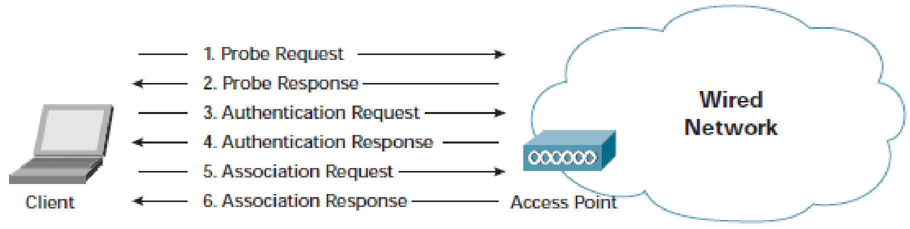
- User authentication to prevent unauthorised access to network resources
- Data privacy to protect the integrity and privacy of transmitted data

The 802.11 specification stipulates two mechanisms for authenticating wireless LAN clients: open authentication and shared key authentication. Two other mechanisms—the Service Set Identifier (SSID) and authentication by client Media Access Control (MAC) address—are also commonly used. This section explains each approach and its weaknesses. The use of Wired Equivalent Privacy (WEP) keys can function as a type of access control because a client that lacks the correct WEP key cannot send data to or receive data from an access point. WEP, the encryption scheme adopted by the IEEE 802.11 committee, provides encryption with 40 bits or 104 bits of key strength.

Authentication in the 802.11 specification is based on authenticating a wireless station or device instead of authenticating a user. The specification provides for two modes of authentication: open authentication and shared key authentication. The 802.11 client authentication process consists of the following transactions (Figure 14.7):

1. Client broadcasts a probe request frame on every channel
2. Access points within range respond with a probe response frame
3. The client decides which access point (AP) is the best for access and sends an authentication request
4. The access point will send an authentication reply
5. Upon successful authentication, the client will send an association request frame to the access point
6. The access point will reply with an association response
7. The client is now able to pass traffic to the access point

Figure 14.7: 802.11 Client Authentication Process



Source: http://www.cisco.com/warp/public/cc/pd/witc/ao1200ap/prodlit/wswpf_wp.pdf

Notes

802.11 Client Authentication Process as shown in Figure 14.7 are describe below:

1. *Probe Requests and Responses:* Once the client becomes active on the medium, it searches for access points in radio range using the 802.11 management frames known as probe request frames. The probe request frame is sent on every channel the client supports in an attempt to find all access points in range that match the SSID and client-requested data rates. All access points that are in range and match the probe request criteria will respond with a probe response frame containing synchronization information and access point load. The client can determine which access point to associate to by weighing the supported data rates and access point load. Once the client determines the optimal access point to connect to, it moves to the authentication phase of 802.11 network access.

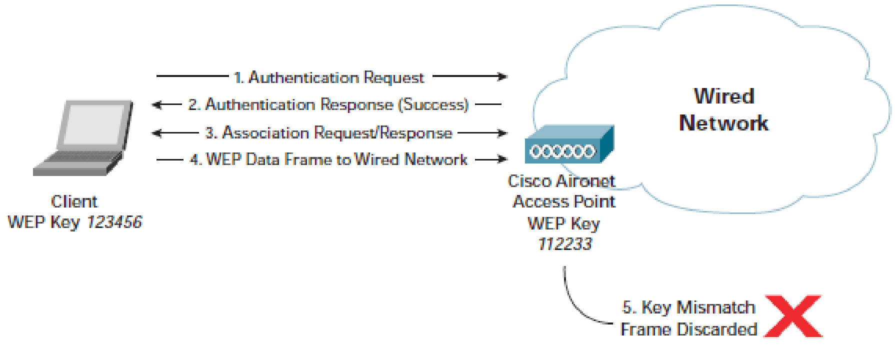
2. *Open Authentication:* Open authentication is a null authentication algorithm. The access point will grant any request for authentication. It might sound pointless to use such an algorithm, but open authentication has its place in 802.11 network authentication. Authentication in the 1997 802.11 specification is connectivity-oriented. The requirements for authentication are designed to allow devices to gain quick access to the network. In addition, many 802.11-compliant devices are hand-held data-acquisition units like bar code readers. They do not have the CPU capabilities required for complex authentication algorithms.

   Open authentication consists of two messages:

   - The authentication request
   - The authentication response

   Open authentication allows any device network access. If no encryption is enabled on the network, any device that knows the SSID of the access point can gain access to the network. With WEP encryption enabled on an access point, the WEP key itself becomes a means of access control. If a device does not have the correct WEP key, even though authentication is successful, the device will be unable to transmit data through the access point. Neither can it decrypt data sent from the access point (Figure 14.8).

Figure 14.8: Open Authentication with Differing WEP Keys


1. Authentication Request
2. Authentication Response (Success)
3. Association Request/Response
4. WEP Data Frame to Wired Network
Client
WEP Key 123456
Cisco Aironet
Access Point
WEP Key
112233
Wired
Network
5. Key Mismatch
Frame Discarded

Source: http://www.cisco.com/warp/public/cc/pd/witc/ao1200ap/prodlit/wswpf_wp.pdf

3. *Shared Key Authentication:* Shared key authentication is the second mode of authentication specified in the 802.11 standard. Shared key authentication requires that the client configure a static WEP key. Figure 14.9 describes the shared key authentication process.

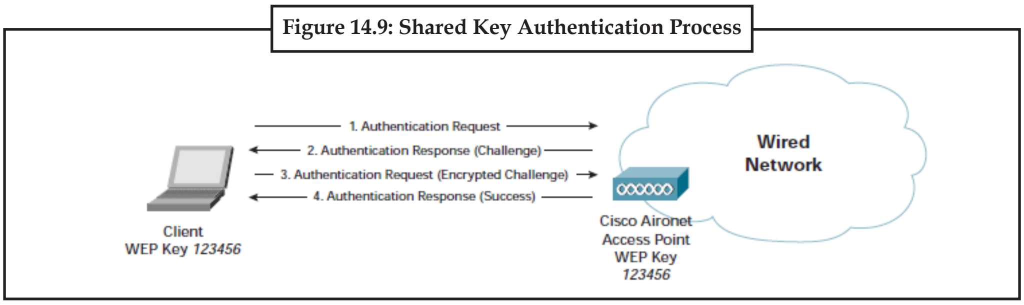
   (a) The client sends an authentication request to the access point requesting shared key authentication

   (b) The access point responds with an authentication response containing challenge text

(c) The client uses its locally configured WEP key to encrypt the challenge text and reply with a subsequent authentication request

(d) If the access point can decrypt the authentication request and retrieve the original challenge text, then it responds with an authentication response that grants the client access.

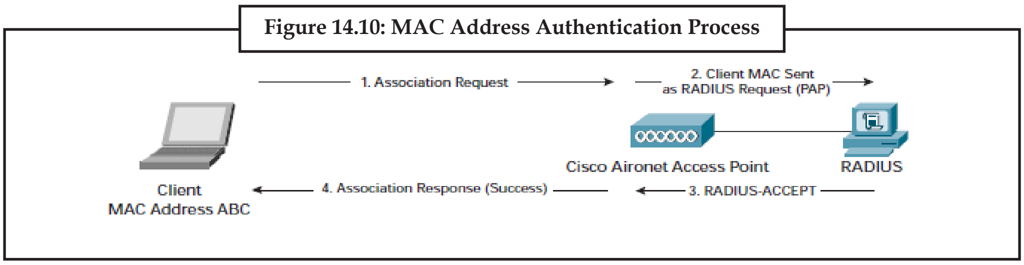
Figure 14.9: Shared Key Authentication Process


1. Authentication Request
2. Authentication Response (Challenge)
3. Authentication Request (Encrypted Challenge)
4. Authentication Response (Success)
Wired Network
Client
WEP Key 123456
Cisco Aironet Access Point
WEP Key 123456

Source: http://www.cisco.com/warp/public/cc/pd/witc/ao1200ap/prodlit/wswpf_wp.pdf

4. ***MAC Address Authentication:*** MAC address authentication is not specified in the 802.11 standard, but many vendors—including Cisco—support it. MAC address authentication verifies the client's MAC address against a locally configured list of allowed addresses or against an external authentication server (Figure 14.10). MAC authentication is used to augment the open and shared key authentications provided by 802.11, further reducing the likelihood of unauthorised devices accessing the network.

Figure 14.10: MAC Address Authentication Process


1. Association Request
2. Client MAC Sent as RADIUS Request (PAP)
Cisco Aironet Access Point
RADIUS
Client
MAC Address ABC
4. Association Response (Success)
3. RADIUS-ACCEPT

Source: http://www.cisco.com/warp/public/cc/pd/witc/ao1200ap/prodlit/wswpf_wp.pdf

14.2.1 Use of SSID

The SSID is advertised in plain-text in the access point beacon messages. Although beacon messages are transparent to users, an eavesdropper can easily determine the SSID with the use of an 802.11 wireless LAN packet analyser, like Sniffer Pro. Some access-point vendors, including Cisco, offer the option to disable SSID broadcasts in the beacon messages. The SSID can still be determined by sniffing the probe response frames from an access point. The SSID is not designed, nor intended for use, as a security mechanism. In addition, disabling SSID broadcasts might have adverse effects on Wi-Fi interoperability for mixed-client deployments.

14.2.2 Open Authentication Vulnerabilities

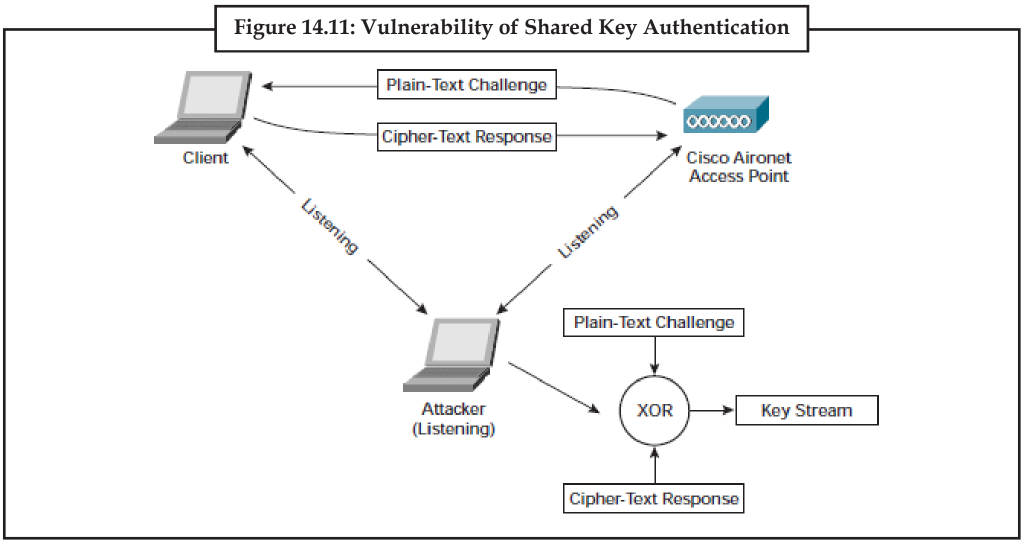
Open authentication provides no way for the access point to determine whether a client is valid. This is a major security vulnerability if WEP encryption is not implemented in a wireless LAN. In scenarios in which WEP encryption is not needed or is not feasible to deploy, such as public wireless LAN deployments strong, higher-layer authentication can be provided by implementing a Service Selection Gateway (SSG).

Notes

14.2.3 Shared Key Authentication Vulnerabilities

Shared key authentication requires the client use a preshared WEP key to encrypt challenge text sent from the access point. The access point authenticates the client by decrypting the shared key response and validating that the challenge text is the same. The process of exchanging the challenge text occurs over the wireless link and is vulnerable to a man-in-the-middle attack. An eavesdropper can capture both the plain-text challenge text and the cipher-text response. WEP encryption is done by performing an exclusive OR (XOR) function on the plain-text with the key stream to produce the cipher-text. It is important to note that if the XOR function is performed on the plain-text and cipher-text are XORed, the result is the key stream. Therefore, an eavesdropper can easily derive the key stream just by sniffing the shared key authentication process with a protocol analyser (Figure 14.11).

Figure 14.11: Vulnerability of Shared Key Authentication



Source: http://www.cisco.com/warp/public/cc/pd/witc/ao1200ap/prodlit/wswpf_wp.pdf

14.2.4 MAC Address Authentication Vulnerabilities

MAC addresses are sent in the clear as required by the 802.11 specification. As a result, in wireless LANs that use MAC authentication, a network attacker might be able to subvert the MAC authentication process by "spoofing" a valid MAC address. MAC address spoofing is possible in 802.11 network interface cards (NICs) that allow the universally administered address (UAA) to be overwritten with a locally administered address (LAA). A network attacker can use a protocol analyser to determine a valid MAC address in the business support system (BSS) and an LAA-compliant NIC with which to spoof the valid MAC address.

Self Assessment

Fill in the blanks:

4. Authentication in the ……………........……….. specification is based on authenticating a wireless station or device instead of authenticating a user.

5. Open authentication is a ……………........……….. authentication algorithm.

6. ……………........……….. authentication is the second mode of authentication specified in the 802.11 standard.

14.3 Medium Access Control (MAC) Filters

A Media Access Control (MAC) address is a hardware address that uniquely identifies each node of a network. All IEEE 802 network devices share a common 48-bit MAC address format, usually displayed as a string of 12 hexadecimal digits separated by colons, for example FE:DC:BA:09:87:65.

Media Access Control (MAC) technology provides unique identification and access control for computers on an Internet Protocol (IP) network. In wireless networking, MAC is the radio control protocol on the wireless network adapter. Media Access Control works at the lower sublayer of the data link layer (Layer 2) of the OSI model.

Wireless networks are a helpful method for easily sharing network resources and connections. But these types of networks are susceptible to security risks, which means that they should be secured. On way to secure a wireless network is through Media Access Control (MAC) filtering. This method of security involves creating a list of MAC addresses that are allowed to access the network. If a device is not included in this list, then it won't be allowed on the network. It is possible to enable MAC filtering through your router's interface.

Each wireless network interface card (NIC) used by a wireless client has a unique MAC address. You can control client access to your wireless network by switching on "MAC Filtering" and specifying a list of approved MAC addresses. When MAC Filtering is on, only clients with a listed MAC address can access the network.

For the Guest interface, MAC Filtering settings apply to both Basic Service Set (BSS).

Table 14.1: MAC Filtering Settings

Field	Description
Filter	To set the MAC Address Filter, click one of the following radio buttons:
	Allow only stations in the list
	Allow any station unless in list
Stations List	To add a MAC Address to Stations List, enter its 48-bit MAC address into the lower text boxes, then click Add.
	The MAC Address is added to the Stations List.
	To remove a MAC Address from the Stations List, select its 48-bit MAC address, then click Remove.
	The stations in the list will either be allowed or prevented from accessing the AP based on how you set the Filter.

Source: http://support.dlink.com/emulators/dwl2210ap/help/mac_filtering.help.html

It allows you to control access to D-Link DWL-2210AP based on Media Access Control (MAC) addresses. Based on how you set the filter, you can allow only client stations with a listed MAC address or prevent access to the stations listed.

Did u know? **What is BSS?**

A basic service set (BSS) is an Infrastructure Mode Wireless Networking Framework with a single access point. Also see extended service set (ESS) and independent basic service set (IBSS).

As part of the 802.11b standard, every Wi-Fi radio has its unique Media Access Control (MAC) number allocated by the manufacturer. To increase wireless network security, it is possible for an IT manager to program a corporate Wi-Fi access point to accept only certain MAC addresses and filter out all others. The MAC control works like call blocking on a telephone: if a computer with an unknown MAC address tries to connect, the access point will not allow it.

Notes

However, programming all the authorized users MAC addresses into all the company's access points can be an arduous task for a large organization and can be time consuming – but for the home technology enthusiast, or for small network installations, using a MAC filtering technique can be a very effective method to prevent unauthorised access.

Media Access Control assigns a unique number to each IP network adapter called the MAC address. A MAC address is 48 bits long. The MAC address is commonly written as a sequence of 12 hexadecimal digits as follows:

48-3F-0A-91-00-BC

MAC addresses are uniquely set by the network adapter manufacturer and are sometimes called physical addresses. The first six hexadecimal digits of the address correspond to a manufacturer's unique identifier, while the last six digits correspond to the device's serial number. MAC addresses map to logical IP addresses through the Address Resolution Protocol (ARP).

Some Internet service providers track the MAC address of a home router for security purposes. Many routers support a process called cloning that allows the MAC address to be simulated so that it matches one the service provider is expecting. This allows households to change their router (and their real MAC address) without having to notify the provider.

Self Assessment

State whether the following statements are true or false:

7. All IEEE 802 network devices share a common 50-bit MAC address format.
8. Wireless networks are a helpful method for easily sharing network resources and connections.
9. MAC addresses are uniquely set by the network adapter manufacturer.

14.4 Public-key Cryptography

Cryptography is the study of protecting information through the use of codes and ciphers. Cryptography forms a fundamental part of message security.

At its simplest, a code is a process of methodically changing information to make it unreadable without knowing how that information was changed. One of the earliest and simplest codes (called a Caesar cipher) worked by taking the alphabet and shifting all the letters by a fixed number. The sender and recipient would both know how many letters to shift and thus could use this code to change information so that each would be able to understand, but no one else could understand. This process of changing information into a code is encryption and the process of changing code back is decryption. The original message is referred to as "plaintext." The changed message is referred to as "ciphertext." The information that is used to change the plain text into ciphertext is referred to as the key. The particular way in which a key changes information is referred to as the algorithm.

> *Notes* Plaintext (or cleartext) in this context should not be confused with plain text when referring to the format of an e-mail message. In that context, plain text is used to differentiate a message's format from HTML format or Rich Text Format (RTF). In the context of message security, plaintext is used to differentiate from ciphertext to indicate that the text is not encrypted.

Notes

Example: If a sender wants to encrypt a message using this method, the sender knows that every instance of the letter A in plaintext would be changed by the key to the letter D in ciphertext; every instance of the letter B in plaintext would be changed to the letter E in the ciphertext, and so on. Using this key, which has an algorithm of "shift the letters forward by three," the word "help" in plaintext would be encrypted to be "khos" as ciphertext.

When the recipient receives the ciphertext message, the recipient would transform it back into plaintext by using the key to decrypt the information, in this case by shifting the letters backward by three, reversing the change.

In this example, both the sender and the recipient must keep the key secret because anyone who knows the key can use it to decrypt and read the message. A lost key renders the encryption useless. In addition, the strength of the algorithm is important. An unauthorised party can take encrypted ciphertext and attempt to break the encryption by determining the key based on the ciphertext.

Note that both the sender and the recipient use the same key. This type of encryption is referred to as "symmetric key" encryption, because both parties use the same key.

Although this is a simple example, it illustrates the core concepts and functionality of cryptography. Recent improvements and advancements in cryptography are ones of degree.

14.4.1 How Public-key Cryptography Works

In 1976, Whitfield Diffe and Martin Hellman created public key cryptography. Public key cryptography represents a major innovation because it fundamentally alters the process of encryption and decryption.

Instead of a single shared, secret key, Diffe and Hellman proposed the use of two keys. One key, called the "private key" remains a secret. Instead of being shared between parties, it is held by only one party. The second key, called the "public key," is not a secret and can be shared widely. These two keys, or "key pair" as they are called, are used together in encryption and decryption operations. The key pair has a special, reciprocal relationship so that each key can only be used in conjunction with the other key in the pair. This relationship ties the keys in the pair exclusively to one another: a public key and its corresponding private key are paired together and are related to no other keys.

This pairing is possible because of a special mathematical relationship between the algorithms for the public keys and private keys. The key pairs are mathematically related to one another such that using the key pair together achieves the same result as using a symmetrical key twice. The keys must be used together: each individual key cannot be used to undo its own operation. This means that the operation of each individual key is a one-way operation: a key cannot be used to reverse its operation. In addition, the algorithms used by both keys are designed so that a key cannot be used to determine the opposite key in the pair. Thus, the private key cannot be determined from the public key. The mathematics that makes key pairs possible, however, contributes to one disadvantage of key pairs as opposed to symmetric keys. The algorithms used must be strong enough to make it impossible for people to use the known public key to decrypt information that has been encrypted with it through brute force. A public key uses mathematical complexity and its one-way nature to compensate for the fact that it is publicly known to help prevent people from successfully breaking information encoded with it.

Applying this concept to the preceding example, the sender would use the public key to encrypt the plaintext into ciphertext. The recipient would then use the private key to decrypt the ciphertext back into plaintext.

Because of the special relationship between the private key and public key in the key pair, it is possible for one person to use the same key pair with many people rather than having to use a different key with each individual person. As long as the private key remains secret, the public key can be given to any number of people and used securely. The ability to use a single key pair with many people represents a major breakthrough in cryptography because it makes cryptography substantially more usable by significantly lowering the key management requirements. A user can share one key pair with any number of people rather than having to establish a single secret key with each person.

14.4.2 Putting Public Key Cryptography Together with Message Security

Public key cryptography is a fundamental element of message security. Without public key cryptography, it is doubtful that there would be practical message security solutions, due to the fact that key management before public key cryptography was cumbersome. With an understanding of the basic concepts of public key cryptography, the next step is to learn how those concepts work to make message security possible.

14.4.3 Public Key Cryptography and Digital Signatures

The reciprocal nature of the relationship of the key pair makes this unique identification possible through public key cryptography.

Because the private key in a key pair belongs to only one party, any time that it is shown that the private key has been used, it can be concluded that only the owner of that key has used it. In this way, the use of the private key is like a signature on a paper because only the owner of a signature can actually make it. The signature confirms its owner's presence just as the use of the private key confirms its owner's presence.

If a key pair is successfully used in an encryption and decryption operation, the pair's private key must have been used for one part of the operation. Because a public key is tied to only one private key, the corresponding public key can be used to identify its related private key and only its related private key. If a particular public key is used successfully in an encryption and decryption operation, it can be inferred that the corresponding private key was used for one part of the operation. Because only the key owner can use the private key, this means that the key owner and only the key owner could have performed part of the encryption and decryption operation.

Using a private key to establish identity shows that the full encryption and decryption operation was accomplished successfully. Showing a full operation means that plaintext would have to be encrypted to ciphertext using a private key and then decrypted back to plaintext using the corresponding public key. If this operation is successfully shown, the use of the private key, and only the private key, is demonstrated.

To show a successful encryption and decryption operation, the plaintext before the encryption and decryption operations must match the plaintext after the encryption and decryption operation. Both sets of plaintext must be compared directly and shown to match absolutely. There must be a control that is used for comparison and validation.

In e-mail, this control is the actual message. Because the message is available to both the sender and the recipient, it is a convenient control element.

To be used in this comparison operation, the message is converted into a "hash," which is a numerical representation of the complete text. Identical message text will yield identical hash values.

By taking the hash value of the message and combining it with the private key at the time of sending, the owner of the private key proves that he or she, and only he or she, sent the message.

Combining the message with the private key is accomplished by encrypting the hash value with the sender's private key, which creates the actual digital signature. Depending on how the sender's e-mail system has been configured, the digital signature is appended either to the bottom of the message, creating a "clear signed" message, or the result is combined with the original message into a binary attachment, creating an "opaque signed" message.

Because the digital signature is added to the original message as an attachment, clear signed messages can be read by e-mail clients that do not support S/MIME. The signature is discarded and the original message is displayed by non-S/MIME clients. However, there is no way the message can be verified; it is essentially the same as an unsigned message. The disadvantage of clear signed messages is that there is an increased chance for intervening mail gateways to alter the message, and thus invalidate the signature.

Conversely, because the message and the digital signature are treated as a single binary attachment in opaque signed messages, they are much less likely to be altered in transit. However, only an S/MIME client can read the attachment. If a non-S/MIME client receives an opaque signed message, the message is unreadable.

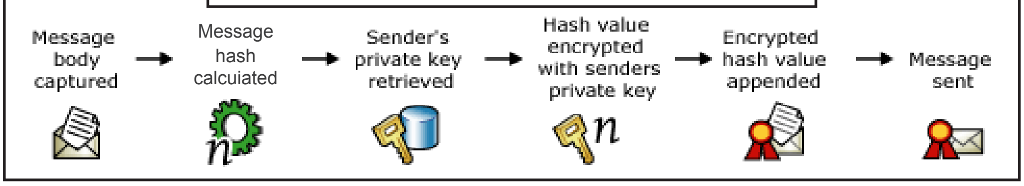
Opaque-signed messages were, in part, created to solve the problem of e-mail systems that altered message bodies while e-mail was in transit. It should be noted here that current e-mail solutions that comply with S/MIME standards do not alter the message body. However, there are many clients that cannot read opaque-signed e-mail messages. Therefore, sending clear-signed messages is recommended.

When the message is received, the digital signature can be retrieved and the sender's public key applied in a decryption operation, which yields the original hash value of the message. A comparison of this hash value with the hash value of the received message can then be performed. Because only one private key can correspond to a public key, and only the owner of the public key could use it to encrypt the hash value successfully, decrypting the hash with the public key shows that the private key owner encrypted the hash value. Because the hash value is a numerical representation of the message text, if the encrypted hash value matches the hash value of the message received, it indicates that the message text that was sent matches the text that was received. When coupled with the fact that only the private key owner could have sent the message, the result is that the recipient is assured that only the key owner sent the message, which provides authentication and, consequently, nonrepudiation. It also shows that the message has not been changed, which provides data integrity. If the hash values did not match, the recipient would know that the message had either been altered in transit or that the public key used does not match the private key used. In both cases, the recipient knows that the message is not valid and should not be trusted.

Thus, the way that public key cryptography provides the security services that make up digital signatures can be seen.

The following Figure 14.12 shows the sequence of signing with the addition of the supporting elements of public key cryptography.

Figure 14.12: Sequence of Signing Public Key Cryptography


Message body captured
Message hash calcuiated
Sender's private key retrieved
Hash value encrypted with senders private key
Encrypted hash value appended
Message sent
n
n

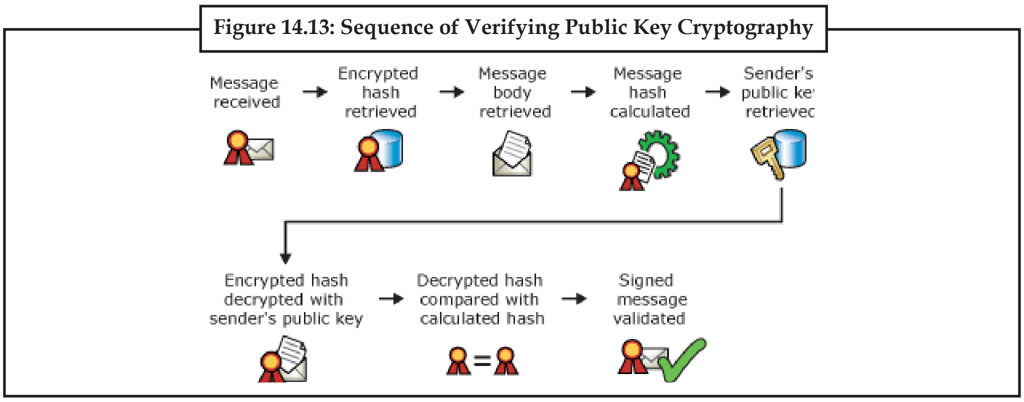
Source: http://technet.microsoft.com/en-us/library/aa998077(v=exchg.65).aspx

- Message is captured.
- Hash value of the message is calculated.
- Sender's private key is retrieved.

- Hash value is encrypted with the sender's private key.
- Encrypted hash value is appended to the message as a digital signature.
- Message is sent.

The following Figure 14.13 shows the sequence of verifying with the addition of the supporting elements of public key cryptography.

Figure 14.13: Sequence of Verifying Public Key Cryptography


Message received
Encrypted hash retrieved
Message body retrieved
Message hash calculated
Sender's public ke retrievec
Encrypted hash decrypted with sender's public key
Decrypted hash compared with calculated hash
Signed message validated
=

Source: http://technet.microsoft.com/en-us/library/aa998077(v=exchg.65).aspx

- Message is received.
- Digital signature containing encrypted hash value is retrieved from the message.
- Message is retrieved.
- Hash value of the message is calculated.
- Sender's public key is retrieved.
- Encrypted hash value is decrypted with the sender's public key.
- Decrypted hash value is compared against the hash value produced on receipt.
- If the values match, the message is valid.

The sequence shows how public key cryptography provides the capabilities that give a digital signature its core security services: authentication, nonrepudiation, and data integrity.

14.4.4 Public Key Cryptography and Message Encryption

Unlike digital signatures, the relationship between public key cryptography and message encryption is generally more straightforward, because encryption is a core function of public key cryptography. However, message encryption is not accomplished by only encrypting and decrypting the message using the key pair. The key pair is used in message encryption, but not for the entire message.

Because the goal of message encryption is to ensure that only authorized recipients can view the message, the private key of each recipient is suited to provide that service. Because the private key can only be successfully used by its owner, the use of the key during the reading of a message ensures that the owner of that key, and only the owner of that key, can read the message. This capability provides the confidentiality that underlies message encryption. Further, because the public key can be distributed widely, it allows any number of people to send information to a single private key holder.

However, the key pair is not used on the entire message. This is because the encryption and decryption operation using a key pair is an expensive process, due to the necessary complexity of the keys' algorithms. Although a key pair needs to be used, it does not necessarily have to be used on the entire message. It needs to be part of the process that "locks" and "unlocks" the information. As long as the message is unreadable until the private key is presented, the goal of message encryption is met.

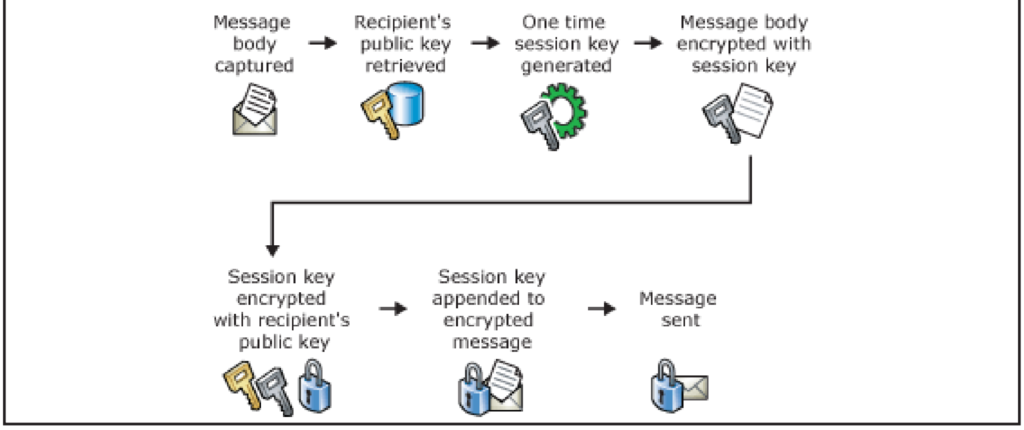
As noted in "How Public Key Cryptography Works" earlier in this topic, public keys use strong algorithms to compensate for being publicly known. These strong algorithms mean that they are larger, and thus computations that use them are slower, than the older symmetric keys. Because a private key is only used to unlock information before it is viewed, and not on the entire message, it is more economical to use a key pair on as little information as possible and use a faster, symmetric key on as much information as possible while ensuring that the information cannot be used until the private key is presented.

Symmetric keys use a secret key, which both parties must know. This process is sometimes called "key negotiation." With key pairs, there is no key negotiation because one public key can be used by many people. Key pairs can also be used in conjunction with symmetric keys to handle key negotiation. A symmetric key can be chosen and that key can be encrypted, using the public key of a key pair, and sent to the owner of the private key. When sending to multiple recipients, the same symmetric key can be used for all recipients, and then encrypted using the public key of each specific recipient. Because only the private key owner can decrypt the symmetric key, the symmetric key remains a secret shared among authorized people. You can generate symmetric keys for a one-time use during a particular operation or session. These are referred to as "session keys". Public key encryption can enhance rather than replace symmetric key encryption.

The goal of message encryption is to ensure that a message is unreadable until the private key is presented. The private key can be used in symmetric key negotiation to securely transmit a symmetric key. Because a symmetric key can be securely transmitted to a recipient, you can use a symmetric key to encrypt a message and then encrypt that symmetric key using the public key in a key pair. Only the private key holder can unlock the symmetric key, which is then used to decrypt the message. This operation functions as if the entire message had been encrypted and decrypted using the key pair. However, because it uses a faster, symmetric key on most of the information, the operation is faster than it would otherwise be. Throughout this process, the message remains protected until the presentation of the private key, thus providing confidentiality, which is the fundamental service of message encryption. Because of the encryption and decryption process, any alteration of a message after it has been encrypted will cause the decryption operation to fail, providing for data integrity.

Although the use of a symmetric key may be unexpected and its benefit not immediately obvious, it enhances message security by making the process of message encryption faster without sacrificing the security of the message. The following Figure 14.14 shows the sequence of encrypting with the supporting elements of public key cryptography.

Figure 14.14: Sequence of Encrypting Public Key Cryptography



Message body captured
Recipient's public key retrieved
One time session key generated
Message body encrypted with session key
Session key encrypted with recipient's public key
Session key appended to encrypted message
Message sent

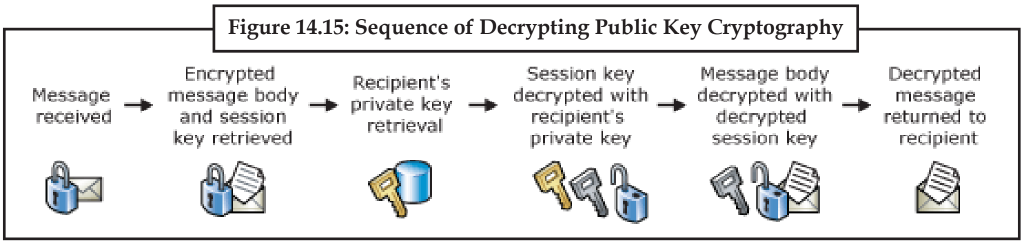
Source: http://technet.microsoft.com/en-us/library/aa998077(v=exchg.65).aspx

Notes

- Message is captured.
- Recipient's public key is retrieved.
- One-time symmetric session key is generated.
- Encryption operation is performed on the message using the session key.
- Session key is encrypted using the recipient's public key.
- Encrypted session key is included with the encrypted message.
- Message is sent.

The following Figure 14.15 shows the sequence of decrypting with the addition of the supporting elements of public key cryptography.

Figure 14.15: Sequence of Decrypting Public Key Cryptography


Message received
Encrypted message body and session key retrieved
Recipient's private key retrieval
Session key decrypted with recipient's private key
Message body decrypted with decrypted session key
Decrypted message returned to recipient

Source: http://technet.microsoft.com/en-us/library/aa998077(v=exchg.65).aspx

- Message is received.
- Encrypted message and encrypted session key are retrieved from the message.
- Recipient's private key is retrieved.
- Session key is decrypted with the recipient's private key.
- Message is decrypted with decrypted session key.
- Unencrypted message is returned to the recipient.

The sequence shows how public key cryptography provides support for the core services of message encryption: confidentiality and data integrity.

14.4.5 Understanding How Public Key Cryptography in Digital Signatures and Message Encryption Work Together

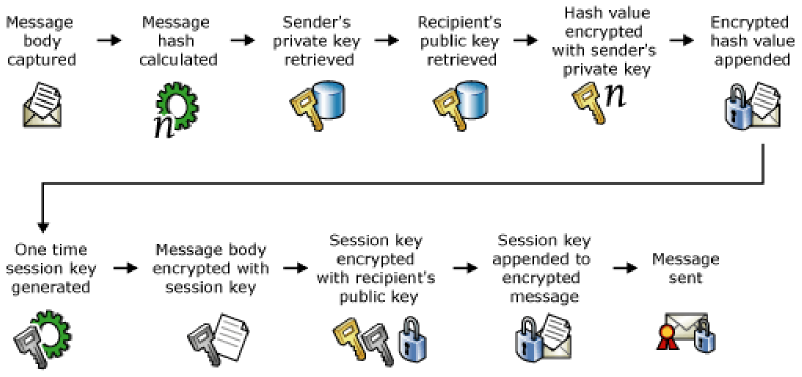
Digital signatures and message encryption are complimentary services. After considering how public key cryptography integrates with each service individually, it is helpful to consider how these services are used together.

The following Figure 14.16 shows the sequence of signing and encrypting with the addition of the supporting elements of public key cryptography.

- Message is captured.
- Hash value of the message is calculated.
- Sender's private key is retrieved.
- Recipient's public key is retrieved.
- Hash value is encrypted with the sender's private key.
- Encrypted hash value is appended to the message as a digital signature.
- One-time symmetric session key is generated.
- Encryption operation is performed on a message using the session key.
- Session key is encrypted using the recipient's public key.

- Encrypted session key is included with the encrypted message.
- Message is sent.

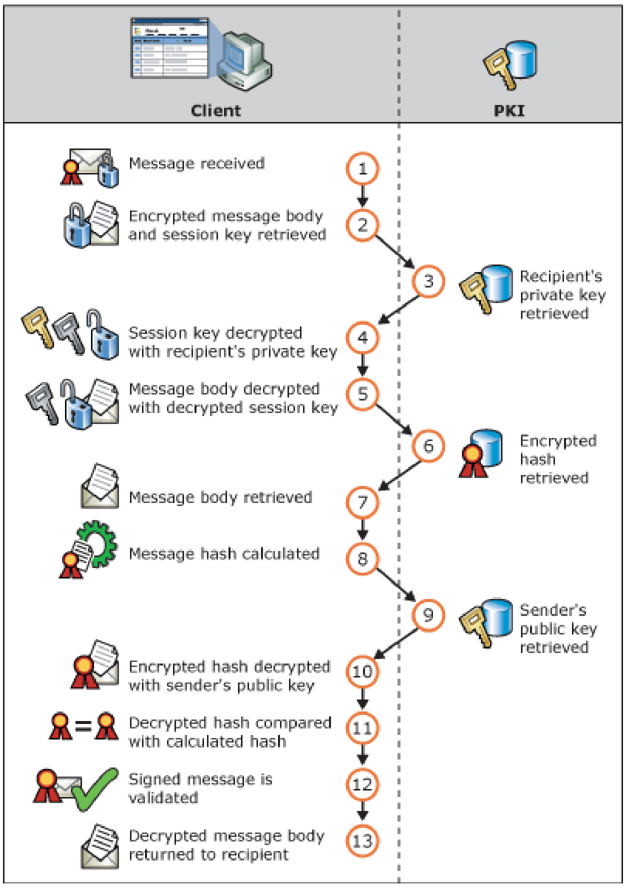
Figure 14.16: Sequence of Signing and Encrypting Public Key Cryptography


Message body captured
Message hash calculated
Sender's private key retrieved
Recipient's public key retrieved
Hash value encrypted with sender's private key
Encrypted hash value appended
One time session key generated
Message body encrypted with session key
Session key encrypted with recipient's public key
Session key appended to encrypted message
Message sent

Source: http://technet.microsoft.com/en-us/library/aa998077(v=exchg.65).aspx

The following Figure 14.17 shows the sequence of decrypting and verifying the digital signature with the addition of the supporting elements of public key cryptography.

Figure 14.17: Sequence of Decrypting and Verifying the Digital Signature Public Key Cryptography


Client
PKI
1 Message received
2 Encrypted message body and session key retrieved
3 Recipient's private key retrieved
4 Session key decrypted with recipient's private key
5 Message body decrypted with decrypted session key
6 Encrypted hash retrieved
7 Message body retrieved
8 Message hash calculated
9 Sender's public key retrieved
10 Encrypted hash decrypted with sender's public key
11 Decrypted hash compared with calculated hash
12 Signed message is validated
13 Decrypted message body returned to recipient

Source: http://technet.microsoft.com/en-us/library/aa998077(v=exchg.65).aspx

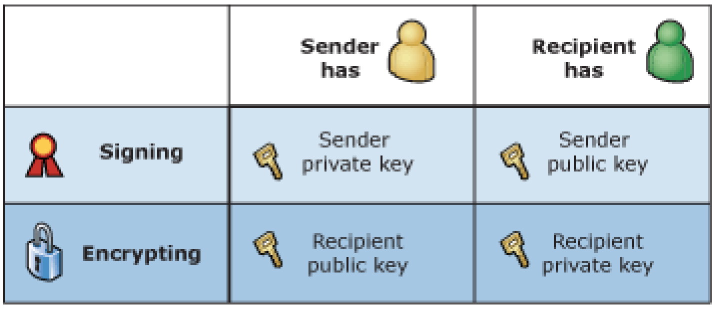
Notes

- Message is received.
- Encrypted message and encrypted session key are retrieved from the message.
- Recipient's private key is retrieved.
- Session key is decrypted with the recipient's private key.
- Message is decrypted with the decrypted session key.
- Digital signature containing encrypted hash value is retrieved from the message.
- Hash value of the message is calculated.
- Sender's public key is retrieved.
- Encrypted hash value is decrypted with the sender's public key.
- Decrypted hash value is compared against the hash value produced on receipt.
- If the values match, the message is valid.
- Unencrypted message is returned to the recipient.

The sequence shows how public key cryptography makes digital signatures and message encryption possible.

Note how the public key or the private key of one party is required by the other party based on the specific operation. For example, the sender must have his or her private key to digitally sign e-mail, but must have the recipient's public key to send encrypted e-mail. Because this can be confusing, a chart showing which keys are needed by which parties for which operation is shown in the following Figure 14.18.

Figure 14.18: Requirement of Keys to Parties



	Sender has	Recipient has
Signing	Sender private key	Sender public key
Encrypting	Recipient public key	Recipient private key

Source: http://technet.microsoft.com/en-us/library/aa998077(v=exchg.65).aspx

The next element to understand is digital certificates. Digital certificates make using digital signatures and encryption possible by distributing key pairs.

Self Assessment

Fill in the blanks:

10. …………………........ is the study of protecting information through the use of codes and ciphers.

11. The reciprocal nature of the relationship of the key pair makes this unique identification possible through …………………........ key cryptography.

12. Using a …………………........ key to establish identity shows that the full encryption and decryption operation was accomplished successfully.

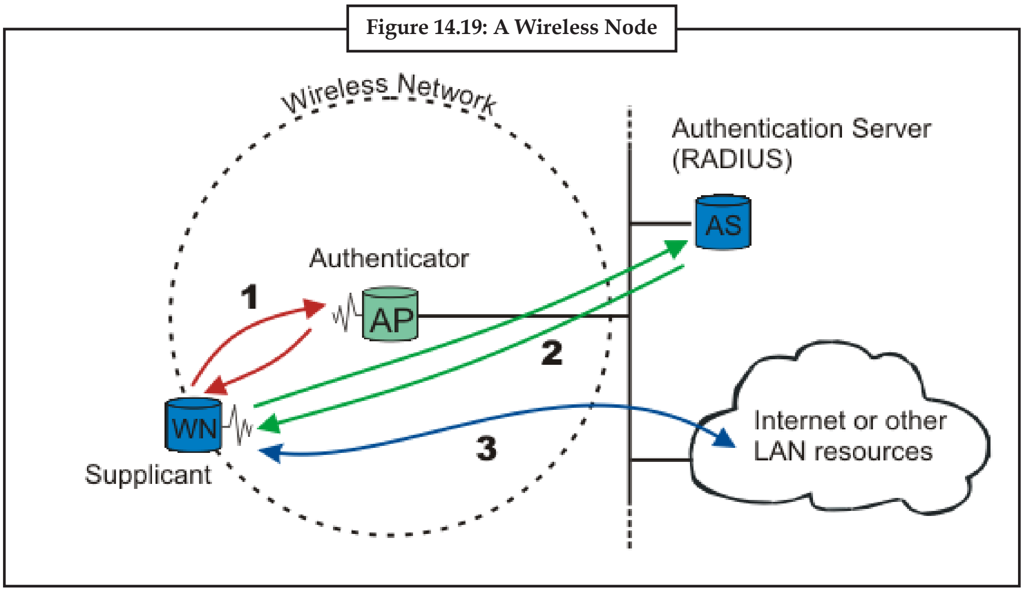
14.5 The 802.1X

Notes

The 802.1X-2001 standard states:

"Port-based network access control makes use of the physical access characteristics of IEEE 802 LAN infrastructures in order to provide a means of authenticating and authorizing devices attached to a LAN port that has point-to-point connection characteristics, and of preventing access to that port in cases which the authentication and authorization fails. A port in this context is a single point of attachment to the LAN infrastructure."

Figure 14.19: A Wireless Node



Source: http://tldp.org/HOWTO/html_single/8021X-HOWTO/

802.1X: A wireless node as shown in Figure 14.19 must be authenticated before it can gain access to other LAN resources.

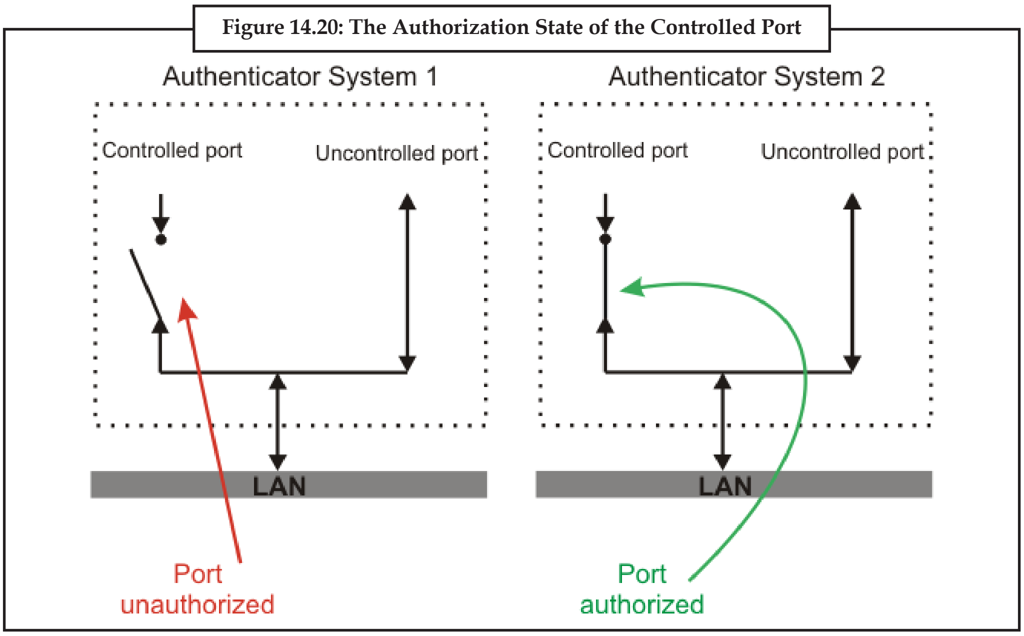
- When a new wireless node (WN) requests access to a LAN resource, the access point (AP) asks for the WN's identity. No other traffic than EAP is allowed before the WN is authenticated (the "port" is closed).
- The wireless node that requests authentication is often called Supplicant, although it is more correct to say that the wireless node contains a Supplicant. The Supplicant is responsible for responding to Authenticator data that will establish its credentials. The same goes for the access point; the Authenticator is not the access point. Rather, the access point contains an Authenticator. The Authenticator does not even need to be in the access point; it can be an external component.
- EAP, which is the protocol used for authentication, was originally used for dial-up PPP. The identity was the username, and either PAP or CHAP authentication [RFC1994] was used to check the user's password. Since the identity is sent in clear (not encrypted), a malicious sniffer may learn the user's identity. "Identity hiding" is therefore used; the real identity is not sent before the encrypted TLS tunnel is up.
- After the identity has been sent, the authentication process begins. The protocol used between the Supplicant and the Authenticator is EAP, or, more correctly, EAP encapsulation over LAN (EAPOL). The Authenticator re-encapsulates the EAP messages to RADIUS format, and passes them to the Authentication Server.

Notes

- During authentication, the Authenticator just relays packets between the Supplicant and the Authentication Server. When the authentication process finishes, the Authentication Server sends a success message (or failure, if the authentication failed). The Authenticator then opens the "port" for the Supplicant.
- After a successful authentication, the Supplicant is granted access to other LAN resources/ Internet.

Authentication means making sure that something is what it claims to be. E.g., in online banking, you want to make sure that the remote computer is actually your bank, and not someone pretending to be your bank. The purpose of 802.1x is to accept or reject users who want full access to a network using 802.1x. It is a security protocol that works with 802.11 wireless networks such as 802.11g and 802.11b, as well as with wired devices. The Authenticator deals with controlled and uncontrolled ports. Both the controlled and the uncontrolled port are logical entities (virtual ports), but use the same physical connection to the LAN (same point of attachment).

Figure 14.20: The Authorization State of the Controlled Port



Source: http://tldp.org/HOWTO/html_single/8021X-HOWTO/

Before authentication, only the uncontrolled port is "open". The only traffic allowed is EAPOL; see Authenticator System 1 on figure port. After the Supplicant has been authenticated, the controlled port is opened, and access to other LAN resources are granted;

The main parts of 802.1x Authentication are:

- A supplicant, a client end user, which wants to be authenticated.
- An authenticator (an access point or a switch), which is a "go between", acting as proxy for the end user, and restricting the end user's communication with the authentication server.
- An authentication server (usually a RADIUS server), which decides whether to accept the end user's request for full network access.
- In a wireless network, 802.1x is used by an access point to implement WPA. In order to connect to the access point, a wireless client must first be authenticated using WPA.

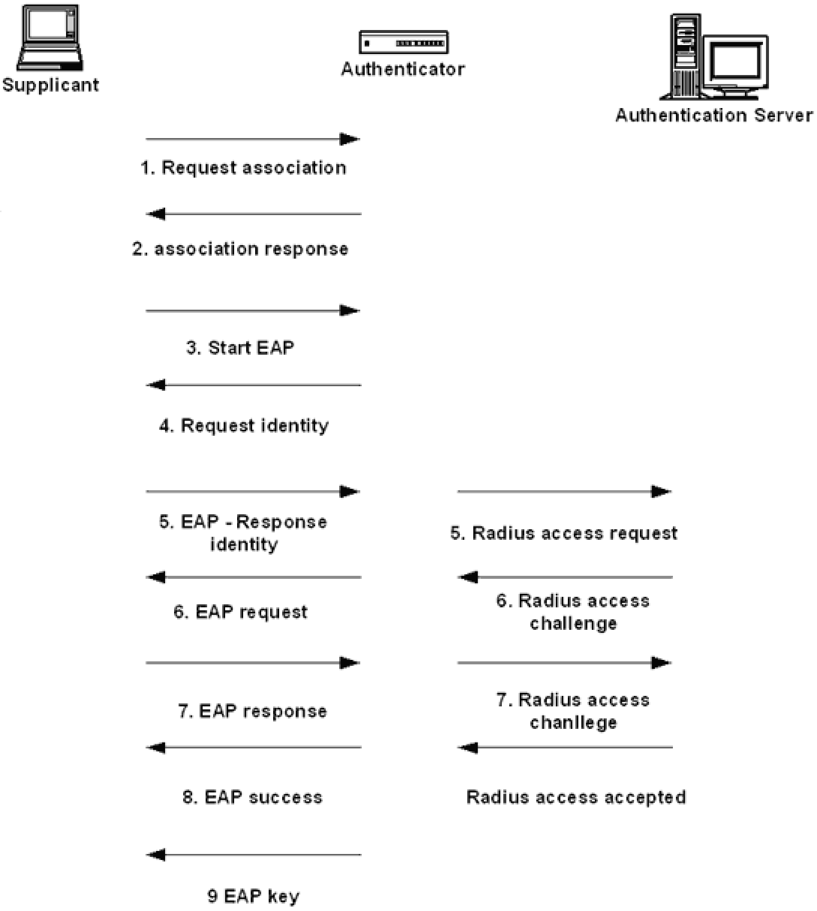
In a wired network, switches use 802.1x in a wired network to implement port-based authentication. Before a switch forwards packets through a port, the attached devices must be authenticated. After the end user logs off, the virtual port being using is changed back to the unauthorised state.

A benefit of 802.1x is the switches and the access points themselves do not need to know how to authenticate the client. All they do is pass the authentication information between the client and the authentication server. The authentication server handles the actual verification of the client's credentials. This lets 802.1x support many authentication methods, from simple user name and password, to hardware token, challenge and response, and digital certificates.

802.1x uses EAP (Extensible Authentication Protocol) to facilitate communication from the supplicant to the authenticator and from the authenticator to the authentication server.

This Figure 14.21 shows the steps of 802.1x and EAP used in authenticating a supplicant:

Figure 14.21: Steps of 802.1x and EAP



Source: http://kb.netgear.com/app/answers/detail/a_id/1209/~/what-is-802.1x-security-authentication-for-wireless-networks%3F

EAP supports various authentication methods. As a user seeking authentication, you just need to use a method supported by the authentication server. As an administrator, you need to select which methods your server will use. 802.1X uses three terms that you need to know. The user or client that wants to be authenticated is called a supplicant. The actual server doing the authentication, typically a RADIUS server, is called the authentication server. And the device in between, such as a wireless access point, is called the authenticator. One of the key points of 802.1X is that the authenticator can be simple and dumb – all of the brains have to be in

Notes

the supplicant and the authentication server. This makes 802.1X ideal for wireless access points, which are typically small and have little memory and processing power.

802.1X authentication can help enhance security for 802.11 wireless networks and wired Ethernet networks by requiring a certificate or a smart card for network access. This type of authentication is typically used for workplace connections.

To enable 802.1X on a wireless network

- Open Manage Wireless Networks by clicking the Start button , clicking Control Panel, clicking Network and Internet, clicking Network and Sharing Centre, and then, in the left pane, clicking Manage wireless networks.
- Right-click the network that you want to enable 802.1X authentication for, and then click Properties.
- Click the Security tab, and then, in the Security Type list, click 802.1X.
- In the Encryption Type list, click the encryption type you want to use. On wireless networks, 802.1X can be used with Wired Equivalent Privacy (WEP) or Wi-Fi Protected Access (WPA) encryption.
- In the Choose a network authentication method list, click the method you want to use. To configure additional settings, click Settings.

To enable 802.1X on a wired network

You must be logged on as an administrator to perform these steps.

To complete this procedure, you must first enable the Wired AutoConfig service, which is turned off by default.

- Click the Start button , and then, in the Search box, type services.msc, and then press ENTER. If you are prompted for an administrator password or confirmation, type the password or provide confirmation.
- In the Services dialog box, click the Standard tab, right-click Wired AutoConfig, and then click Start.
- Open Network Connections by clicking the Start button , clicking Control Panel, clicking Network and Internet, clicking Network and Sharing Centre, and then clicking Manage network connections.
- Right-click the connection that you want to enable 802.1X authentication for, and then click Properties. If you are prompted for an administrator password or confirmation, type the password or provide confirmation.
- Click the Authentication tab, and then select the Enable IEEE 802.1X authentication check box.
- In the Choose a network authentication method list, click the method you want to use. To configure additional settings, click Settings.

Self Assessment

State whether the following statements are true or false:

13. The wireless node that requests authentication is often called Supplicant.

14. During authentication, the Authenticator just relays packets between the Supplicant and the Authentication Server.

15. In a wireless network, 802.1x is not used by an access point to implement WPA.

14.6 Security Policies

Most IT environments have some type of remote access. VPN, e-mail, and many other services expose your user accounts to the world.

Proper password aging policies will naturally take care of old or unused accounts. The idea behind password aging is that after a certain amount of time, a password expires. A password is less prone to compromise if it is changed frequently. Likewise, if an account is compromised, its usefulness will be limited to the amount of time left before the expiry timer concludes. Aging account passwords can reduce exposure if brute-force, social engineering, or sniffing attempts are successful.

The strength of the password itself is also extremely important. It is imperative that the systems requiring users to change their passwords also enforce some level of strictness with regards to what passwords are accepted. An unguessable password makes brute-force attacks—the premiere method by which accounts are compromised—mostly futile. An exhaustive brute-force attack will eventually discover all passwords, given enough time, but the idea is to use a password of sufficient length, so that it can't be guessed in a reasonable amount of attempts. The successful guessing attempts normally find extremely trivial passwords, such as ones that are the same as the username. In next week's article we'll explore the password strength issue in more detail, when we dispel many myths about password security. For now, just know that password strength is quite important.

Account aging, that is the disabling of unused accounts, is just as important as having a decent password policy. Unused accounts are probably the second most commonly compromised. If you don't have a password aging policy, at least be certain to disable old or unused accounts. Ideally, though, password aging should be your priority. There's a few different ways to implement password aging. The aging of a password will naturally disable unused accounts. A since a user must login to be given notice that their password has expired, and if they fail to do so within a certain amount of time, the account itself can be disabled. The question is then, "how do we implement this enterprise-wide?"

In practical terms, Windows Active Directory and various Unix-based LDAP servers support the setting of password policies. Unfortunately, simply enabling password expiry will be problematic. Services that use LDAP may not implement the necessary "goo" to talk about expired accounts. They simply get an authentication failure, and the user won't know why. This also happens with Active Directory, for example a VPN user will not be able to authenticate with an expired password until they first login to an actual Windows machine and set a new password.

There are two viable solutions. Well, one that "works," and one that is truly viable. It would work to require that all systems that authenticate users implement password aging. Each system would have to keep track of these policies, possibly previously used passwords, and of course they would have to implement the mechanism by which a user can be notified and subsequently change their password. Not likely.

The only viable solution, then, is to use a central authentication system. CAS, a central authentication system for Web-based applications, is the ideal solution. CAS is extremely popular, and it provides an extremely effective and secure method by which users can be centrally authenticated, complete with a method to support changing passwords on expired accounts.

Example: Kerberos-based services like AD in Windows or a Kerberos-enabled LDAP server in Unix provide authentication for workstations and other site-local applications, but with the drawbacks previously mentioned.

Interestingly enough, it should be noted that improving security through account aging requires central authentication, which provides the added benefit of single sign-on. Now, don't forget that single sign-on can mean two things: having the same password everywhere, or using a "ticket" (or cookie, when talking about Web applications) to only need to sign on to one service, but gain access to many. Synchronizing passwords between services isn't usually done for security reasons; instead it's for user convenience. In the rare instances where a password change on one system, not a central system, propagates to all others, it is possible to implement a password aging policy. Generally, these types of setups are organically grown because a diverse set of applications don't support a coherent set of protocols, and password aging is impossible.

As contrary as it may sound, central authentication is the only way to ensure proper security. Administrators can instantly disable access to all services at the same time with central authentication, and they can also ensure that password policies are enforced. The fact that a user is supplying the same password for all services isn't as much of a concern as one might think. Indeed, there will always be multiple levels of security requirements. The most critical and secure financial systems, for example, can still be kept separate to alleviate concerns about a password compromise, but only if it also implements appropriate password strictness and aging policies.

Finally, be sure to pay close attention to how your chosen systems will handle passwords set before your change in policy. Some systems may continue to allow old users with weak password to continue using them after you've turned on password complexity requirements. Likewise, be sure to verify that new aging policies apply to all existing user accounts, not just new ones.

Properly managed accounts, that is, accounts that are automatically disabled after too much idle time, will shut down the main vehicle of attack used today. Of course, disabling ex-employee accounts is just as important. Leaving an account open so that people can have access to an ex-employee's e-mail is risky, and should be carefully considered. It's generally best to make a copy of all existing e-mail, and then configure an e-mail forward to their supervisor. Combine constant user education about social engineering tactics, sysadmin education about security best practices, and vigilance in account policies; now your enterprise can be much more secure and easier to manage.

14.6.1 Data Security Policy

Data security includes the mechanisms that control the access to and use of the database at the object level. Your data security policy determines which users have access to a specific schema object, and the specific types of actions allowed for each user on the object. For example, the policy could establish that user can issue SELECT and INSERT statements but not DELETE statements using the emp table. Your data security policy should also define the actions, if any, that are audited for each schema object.

Your data security policy is determined primarily by the level of security you want to establish for the data in your database. For example, it may be acceptable to have little data security in a database when you want to allow any user to create any schema object, or grant access privileges for their objects to any other user of the system. Alternatively, it might be necessary for data security to be very controlled when you want to make a database or security administrator the only person with the privileges to create objects and grant access privileges for objects to roles and users.

Overall data security should be based on the sensitivity of data. If information is not sensitive, then the data security policy can be more lax. However, if data is sensitive, a security policy should be developed to maintain tight control over access to objects.

14.6.2 End-User Security

Security administrators must define a policy for end-user security. If a database has many users, the security administrator can decide which groups of users can be categorized into user groups, and then create user roles for these groups. The security administrator can grant the necessary privileges or application roles to each user role, and assign the user roles to the users. To account for exceptions, the security administrator must also decide what privileges must be explicitly granted to individual users.

Using Roles for End-User Privilege Management

Roles are the easiest way to grant and manage the common privileges needed by different groups of database users.

Consider a situation where every user in the accounting department of a company needs the privileges to run the accounts receivable and accounts payable database applications (ACCTS_REC and ACCTS_PAY). Roles are associated with both applications, and they contain the object privileges necessary to execute those applications.

The following actions, performed by the database or security administrator, address this simple security situation:

- Create a role named accountant.
- Grant the roles for the ACCTS_REC and ACCTS_PAY database applications to the accountant role.
- Grant each user of the accounting department the accountant role.

Self Assessment

Fill in the blanks:

16. Proper …………..............… aging policies will naturally take care of old or unused accounts.

17. …………..............… is extremely popular, and it provides an extremely effective and secure method by which users can be centrally authenticated, complete with a method to support changing passwords on expired accounts.

18. …………..............… security includes the mechanisms that control the access to and use of the database at the object level.

Case Study

2FA Helps a US Based Mortgage Servicing Company in Meeting Their Compliance Requirements

Customer is an end-to-end provider of loss mitigation and portfolio management services for mortgage lenders, servicers, asset managers and investors. Customer based out of USA provides a single-source solution for reducing costs and mitigating loss at every stage of the mortgage process.

Business Challenge

Due to the specialist nature of their work, customer's employees are frequently required to work from any of the firm's offices as well as at client premises, which means needing to have flexible and secure access to data at all times. Customer have invested heavily in providing the necessary IT infrastructure to support this critical business requirement and are continually reviewing their corporate network to ensure that the system keeps pace with the evolving needs of the business and developments in technology as well as ensuring it meets the latest security compliance standards required to protect client information. Customer complies with various Data Security Accreditions like ISO 27001, PCI DSS LevelI, SAS 70 TypeII and HIPAA. The customer has identified the need for a

Contd...

Notes

Strong authentication technology to strengthen their remote access so that the confidential client files will be secured from various hacking attacks as well as they meet the various compliances.

Solution

Customer evaluated multiple two-factor authentication options available in the market to meet their needs. The criterion applied by the customer is to make sure the product offers Industry level security, product is easily configurable with the Juniper SSL VPN and is a cost effective solution so that they can offer it to all their employees enabling them to work remotely and increase their productivity. ArrayShield IDAS delivered robust Two Factor Authentication Solution that met all customer needs. ArrayShield IDAS provides a robust two factor authentication leveraging user's ArrayCard and a pattern that is remembered by the user. Before users are allowed access to the VPN they must enter a unique Secret-Code derived from the ArrayShield IDAS technology. The Secret-Code is generated through the combination of a pattern that each user remembers and an ArrayCard (credit-card sized translucent card) that the user carries with them. This simple process ensures that only authorized personnel are able to access the system and protects users' identities from being intercepted or stolen, without the need for an expensive token based system typically used with other strong authentication technologies. Another key advantage is that the user need not remember any complicated password which makes the whole system experience easier.

Securing Customer Remote Access

IDAS integration and deployment with Juniper SSL VPN at Customer premise was very smooth and happened in a few hours. The whole of the deployment and integration was carried out remotely by the ArrayShield Expert technical team and the customer was impressed with the ease of installation, configuration and the remote support provided by the ArrayShield team. As the IDAS system is lightweight and high performing, it required Customer to allocate just a minimal hardware in their premise to deploy IDAS Authentication manager. Customer was very happy with the technology and business benefits provided by the solution, and within few weeks have taken more licenses to roll-out the solution to the wider use base.

Outcome

1. ***Meet Compliance Requirements:*** By implementing Two Factor Authentication technology, customer has met the various data accreditation security requirements of ISO 27001, PCI DSS Level1 and HIPAA.
2. ***Improved Productivity:*** By enabling IDAS for Remote Access VPN, the Customer's employees can now connect to their corporate network from anywhere, and respond to critical communications with-out having to wait for the next day.
3. ***Security and Cost Targets Met:*** With a cost effective IDAS Two Factor Authentication solution integrated with VPN, the customer is satisfied that their security requirements are met within the budget available.

Questions:

1. Discuss some authentication options evaluated by the customers.
2. Discuss the benefits of implementing two factor authentication technology.

Source: http://www.arrayshield.com/uploads/IDAS-2FA-CaseStudy-Financial-Services-Remote-Access-VPN.pdf

14.7 Summary

- Building a strong user-authentication architecture requires focus beyond just improving the credential-verification component.
- The overall architecture might include additional aspects, such as a layered system that is driven by risk-based analytics, which enables an adaptive authentication system.
- Also, the design of an authentication approach should be weighed against various requirements, such as data (that is, availability, confidentiality, integrity, accountability, and so on), identity assurance, usability, compliance and auditing, portability/scalability, manageability, and user-community dynamics.
- More importantly, however, just the same as other security initiatives, strong user authentication also requires a carefully planned, well-balanced, and concerted approach across the entire IT architecture to ensure a consistently secure environment.
- With the growing adoption of cloud-based services, consumer-identity metasystems, and mobile devices, while attack methods gain maturity and sophistication, the future outlook for strong user authentication is set for many innovative developments.
- However, implementing strong user authentication often is not a straightforward task, as projects have myriad options from which to choose, a multitude of trade-offs to consider, and a cluster of intricacies to manage.
- Defined by the Institute of Electrical and Electronic Engineers (IEEE) with the 802.3 standard, Ethernet has provided an evolving, cooperative, scalable and interoperable networking standard.
- Media Access Control (MAC) technology provides unique identification and access control for computers on an Internet Protocol (IP) network.
- Cryptography forms a fundamental part of message security.
- Without public key cryptography, it is doubtful that there would be practical message security solutions, due to the fact that key management before public key cryptography was cumbersome.
- The purpose of 802.1x is to accept or reject users who want full access to a network using 802.1x.
- Data security includes the mechanisms that control the access to and use of the database at the object level.

14.8 Keywords

Address Resolution Protocol (ARP): ARP converts an Internet Protocol (IP) address to its corresponding physical network address. ARP is a low-level network protocol, operating at Layer 2 of the OSI model.

Authentication: Authentication is a process which a user gains the right to identify himself.

Cloud Computing: Cloud computing is a colloquial expression used to describe a variety of different computing concepts that involve a large number of computers that are connected through a real-time communication network (typically the Internet).

Cryptography: Cryptography is the study of protecting information through the use of codes and ciphers.

Extensible Authentication Protocol (EAP): EAP is an authentication framework which supports multiple authentication methods. EAP typically runs directly over data link layers such as Point-to-Point Protocol (PPP) or IEEE 802, without requiring IP.

Internet Protocol: IP (Internet Protocol) is the primary network protocol used on the Internet, developed in the 1970s and is often used together with the Transport Control Protocol (TCP) and referred to interchangeably as TCP/IP.

Knowledge-based authentication (KBA): KBA typically is implemented as extensions to existing simple-password authentication.

Network Adapter: A network adapter interfaces a computer to a network.

Open Systems Interconnection Model (OSI): The OSI model defines internetworking in terms of a vertical stack of seven layers.

Server-generated one-time passwords (OTPs): OTPs commonly are implemented as randomised password strings that are generated in real time after verifying simple-password credentials.

User Authentication: User authentication is a means of identifying the user and verifying that the user is allowed to access some restricted service.

14.9 Review Questions

1. Define User Authentication. Why is it important?
2. How will you create Strong User Authentication?
3. Discuss the approaches in User Authentication.
4. Distinguish between Authentication and Authorization.
5. Describe the process of 802.11 client authentication.
6. What are the vulnerabilities in the 802.11 Authentication?
7. Define Media Access Control.
8. How Public-key Cryptography Works?
9. Write brief note on Public Key Cryptography and Digital Signatures.
10. Describe Public Key Cryptography and Message Encryption.
11. Highlight the main parts of 802.1x Authentication.
12. Write short note on the security policies in authentication.

Answers: Self Assessment

1. True
2. False
3. False
4. 802.11
5. Null
6. Shared key
7. False
8. True
9. True
10. Cryptography
11. Public
12. Private
13. True
14. True

15. False

16. Password

17. CAS

18. Data

14.10 Further Readings

Books

Glisic, Savo & Lorenzo, Beatriz (2009). "*Advanced Wireless Networks: Cognitive, Cooperative & Opportunistic 4G Technology*." John Wiley & Sons.

Golmie. "*Coexistence in Wireless Networks*." Cambridge University Press.

Pan, Yi & Xiao, Yang (2005). "*Design and Analysis of Wireless Networks*." Nova Publishers.

Rackley, Steve (2011). "*Wireless Networking Technology: From Principles to Successful Implementation*." Elsevier.

Stojmenovic (2006). "*Handbook of Wireless Networks & Mobile Computing*." John Wiley & Sons.

Syngress (2001). "*Designing A Wireless Network*". Syngress.

Online links

http://people.duke.edu/~rob/kerberos/authvauth.html

http://pic.dhe.ibm.com/infocenter/aix/v7r1/index.jsp?topic=%2Fcom.ibm.aix.security%2Fdoc%2Fsecurity%2Fuser_authentication.htm

http://msdn.microsoft.com/en-us/library/cc838351.aspx#_Architectural_Perspectives

http://www.cisco.com/warp/public/cc/pd/witc/ao1200ap/prodlit/wswpf_wp.pdf

http://yourbusiness.azcentral.com/enable-mac-address-filtering-18969.html

http://technet.microsoft.com/en-us/library/aa998077(v=exchg.65).aspx

http://www.networkworld.com/news/2010/0506whatisit.html

http://omnitraining.net/security/198-increase-security-with-proper-authentication-policies

LOVELY PROFESSIONAL UNIVERSITY
Jalandhar-Delhi G.T. Road (NH-1)
Phagwara, Punjab (India)-144411
For Enquiry: +91-1824-300360
Fax.: +91-1824-506111
Email: odl@lpu.co.in