Data Communication & Network

MBA IT-409

DIRECTORATE OF DISTANCE EDUCATION

SWAMI VIVEKANAND
SUBHARTI UNIVERSITY
Meerut (National Capital Region Delhi)

Contents

SYLLABUS

Data Communication and Network

Course Code: MBA IT-409		
Course Credit: 3	**Lecture: 2**	**Tutorial-1**
Course Type:	Skill Enhancement Course	
Lectures delivered:	**20 L+10T**	

End Semester Examination System

Maximum Marks Allotted	**Minimum Pass Marks**	**Time Allowed**
70	28	3 Hours

Continuous Comprehensive Assessment (CCA) Pattern

Tests	Assignment/ Tutorial/ Presentation/class test	**Attendance**	**Total**
15	5	10	30

Course Objective: The objective of studying ths paper is to help students understand communication networks and web related technologies.

UNIT	**Course Content**	**Lectures**
I	**Fundamentals of Communication System;** Communication Links, Communication System Formats; Character Codes, Digital Data Rates; Asynchronous and Synchronous Data. **Types of Signals:** AM; FM; PM; PCM; TDMS; FDMA; SDMA; CDMA; ASK; FSK; PSK features; Error detection and Correction Codes; Hamming codes.	10
II	**LAN topologies:** Workstation; Server; Cables; Types of Ethernet; Broadband; and Base-band; Optical fibers; Network Interface Card. **Networks and Accessories:** LAN, MAN, WAN, Hub;Bridges; Switches; Routers; Gateways Cell Relay; Frame relay; ISDN; B-ISDN	10
III	**OSI Model:** Broadcasting; Multicasting; Point-to-point communication; IP Adressing; Concept fo Port; Socket; ATM; Tunnelijhg; Virtual Priate Network, Network Operating systems: Unix; Linux; Windows	10
IV	**Mobile Communication:** Applicatinos of Mobile Communication; Wireless Communication: Bandwith Transmission Impairment, Interference, Terrestrial Microwave, Broadcast Radio, Infrared & Light waves, Mobie Internet & WML: Mobile IP, Wireless TCP & UDP, WEAP, WML	10

Unit 1

Fundamentals of Communication System

Notes

Structure

1.0 LEARNING OBJECTIVES

After reading this chapter students will be able to:

- Know about the fundamentals of communication system.
- Discuss the communication links
- Know about the character codes
- Describe the types of signals and modulations
- Understand the error detection codes
- Discuss hamming codes
- Explain the asynchronous and synchronous data

Notes

1.1 INTRODUCTION

The word data refers to information presented in whatever form is agreed upon by the parties creating and using the data. Data communications are the exchange of data between two devices via some form of transmission medium such as a wire cable.

Data communication systems enable transfer of data using one of the three transmission modes. Data communication systems has 4 fundamental characteristics; which are delivery, accuracy, timeliness and jitter. Each of these 4 fundamental characteristics has it part in the effectiveness of a data communication system. However, data communication systems work through network systems and there are 3 necessary criteria for an effective and efficient network. Thus a data communication system also depend on the underlying network system's effectiveness.

For data communications to occur, the communicating devices must be part of a communication system made up of a combination of hardware (physical equipment) and software (programs). The effectiveness of a data communications system depends on four fundamental characteristics: delivery, accuracy, timeliness, and jitter.

1. **Delivery:** The system must deliver data to the correct destination. Data must be received by the intended device or user and only by that device or user. The primary task of a data communication system is to deliver or transfer data from sender to receiver, which are the 2 components of the 5 components of data communication system. The system must deliver data to the exact destination. No other receiver should receive the data. This characteristics includes the security of the system, that is, the protection of data.

2. **Accuracy:** The data communication system must deliver data to the receiver without being altered or damaged. The receiver should receive the exact same data which was sent by the sender. The protocol might require to alter the sent data to protect and optimize the process. However, the protocol should also reverse and restore the data back to its original form before representing it to the receiver. The accuracy must be maintained.

3. **Timeliness:** The system must maintain timeliness. It must deliver data in a timely manner. Delayed delivery can make the data useless to the receiver. Data must be delivered as they are produced, in the order they are produced and without any significant delay, timely delivery means delivering data as they are produced, in the same order that they are produced, and without significant delay. This kind of delivery is called real-time transmission.

4. **Jitter-Jitter refers to the variation of packet arrival time.** Data is sent as packets, that is, a chunk of the whole data is sent in each turn. These packets get re-joined back in the target device to represent the complete data as it is. Each packet is sent with a predefined delay or acceptable amount of delay. If packets are sent without maintaining the predefined delay then an uneven quality in the data might result.

   For example, let us assume that video packets are sent every 3D ms. If some of the packets arrive with 3D-ms delay and others with 4D-ms delay, an uneven quality in the video is the result.

1.2 DESCRIPTION OF DATA COMMUNICATION

Communication can be defined as the exchange of information between two or more bodies. In engineering, exchange of information is not only between people, information exchange also takes place between machines or systems. Communication has increased significantly in importance in recent years. Voice services have seen unprecedented increase in use throughout the world with the introduction of mobile phones, with embedded data services such as SMS, and web browsing.

Data is referred to as a piece of information formatted in a special way. Data can exist in a variety of forms, such as numbers or text on pieces of paper, as bits and bytes stored in electronic memory, or as facts stored in a person's mind. Strictly speaking, data is the plural of datum, a single piece of information. In practice, however, people use data as both the singular and plural form of the word.

In electronics terms data is a digital bit or digitized analog signal. Signals are physical quantity that changes with time. Signal can be a voltage that is proportional to the amplitude of message. It could also be a sequence of pulses in fiber optics cable or electromagnetic wave irradiated by an antenna. When these signals are transfer between two or more points we say data is transmitted.

Transmission of data from source to destination usually takes place via some transmission media and this depends on two main factors; quality of signal being transmitted and characteristics of transmission medium. Data transmission always uses the form of electromagnetic waves and they are classified into guided electromagnetic waves and unguided electromagnetic waves. Examples of guided waves are twisted pair, coaxial cable and optical fiber. Unguided waves means transmitting electromagnetic waves but they are not guided as example propagation through air, vacuum and seawater.

1.3 COMMUNICATION LINKS

Communication link means a connection between a hyperlink or graphical element (button, drawing, image) and one or more such items in the same or different electronic document wherein upon clicking on a hyperlinked item, the user is automatically transferred to the other end of the hyperlink which could be another.

Examples of communication link in a sentence Where the Buyer has submitted a bid on behalf of a Customer, the Buyer shall by 19.30 hours on the second Business Day after the Closing Time ensure that Transfer Requests have been made by it to the Registry through its Communication Link, or by such other means as the Registry may direct from time to time. The CPPS Communication Link shall use Open Standards for all communication layers to enable functions.

Any entity for which the consumer has provided explicit permission to access the CPPS connected functionality, in whole or in part, via a Communication Link. Where applicable, a Link Extension is charged in addition to the monthly rate for the associated Control Link or Communication Link. All K series swaps will have a stored code p0600/Code 39 (Serial Communication Link Malfunction/Multiplex) unless disabled with a Hondata Kpro or other K series ECU software.

Notes

Definitions to be applied to these criteria are:

"Communication Link" means all communications equipment, processes and arrangements that facilitate the collection of energy data from a data logger or a measurement element so as to enable a remote interface to be established that lie:

a) if the data logger is internal to the device containing the measurement elements - between the data logger and the telecommunications network; and

b) if the data logger is external to the device containing the measurement elements but is located at the same site — between the meter and the data logger and between data logger and the telecommunications network; and

c) if the data logger is not located at the same site as the device containing the measurement elements — between the meter and the telecommunications network.

"economically feasible" means the annual cost to manually read a site is greater than the annual cost of installing and maintaining a communication link.

- • "GSM" means the acronym for Global System for Mobile Communications, and is a standard for digital mobile phone networks using radio frequency.
- • "Interval meter" means a meter that measures interval energy data and records it in a data logger.
- • "Modem" means a device that converts data into a signal that is compatible with a telephone or radio network and back again.
- • "Satellite" means a satellite communications platform for areas where GSM is not available

Communication Link Criteria

Clause 3.16(2) of the Metering Code mandates that the Network Operator must ensure a type 1 to type 4 metering installation includes a communication link to enable a meter of a metering point to be read from a remote location. The Network Operator may also require the installation of a communication link for types other than types 1 to 4.

The installation of a communication link may be required where:

(a) the geographical remoteness of a metering installation makes the manual collection of interval energy data (type 5) or accumulated energy data not economically feasible.

(b) access to the meters is restricted by a security system or process; or (c) multiple master or distributed master meters are located on more than 3 levels, including below, on or above ground level.

Link Requirements

If a metering installation is required to include a communications link, then the communications link must, where necessary, include a modem and isolation device approved under the relevant telecommunications regulations, to allow accumulation and interval energy data to be downloaded to the metering database via a telecommunications network.

Where a communication link has been installed, the metering installation must include facilities for the on-site storage of energy data that comply with the requirements of the Metrology Procedure.

1.4 COMMUNICATION SYSTEM FORMATS

The communication system enables the successful transmission of idea or any other important information among individuals. The person from whom the thought originates carefully encodes his ideas into a sensible content which is now ready to be shared with everyone. He is commonly referred to as the sender and the other party who receives the information from him is called the receiver or the recipient. The free flow of information between the sender and the receiver takes place because of the communication system.

The flow of information can be between two individuals. The information can flow from the individual to a machine, from the machine to the individual and even between two machines. Machines coupled together through networks also provide signals for the individuals to respond, thus a type of communication system. In the above cases all the machines must work on similar lines and patterns, must be technically compatible and has to provide the same information, so that the individuals can decode the information well.

Let us study the various types of communication system for the smooth flow of information between two parties.

Optical Communication System

The word "Optical" stands for light. As the name itself suggests, optical communication system depends on light as the medium for communication. In an optical communication system the transmitter converts the information into an optical signal (signal in the form of light) and finally the signal then reaches the recipient. The recipient then decodes the signal and responds accordingly.

In optical communication system, light helps in the transmission of information. The safe landing of helicopters and aeroplanes work on the above principle. The pilots receive light signals from the base and decide their next movements. On the roads, red light communicates the individual to immediately stop while the individual moves on seeing the green light.

In this mode of communication light travels through the optical fibre.

Radio Communication System

In the radio communication system the information flows with the help of a radio. Radio communication system works with the aid of a transmitter and a receiver both equipped with an antenna.

The transmitter with the help of an antenna produces signals which are carried through radio carrier wave. The receiver also with the help of an antenna receives the signal. Some information is unwanted and must be discarded and hence the electronic filters help in

Notes

the separation of radio signals from other unwanted signals which are further amplified to an optimum level Finally the signals are decoded in an information which can be easily understood by the individuals for them to respond accordingly.

Duplex Communications System

In Duplex communications system two equipments can communicate with each other in both the directions simultaneously and hence the name Duplex. When you interact with your friend over the telephone, both of you can listen to each other at the same time. The sender sends the signals to the receiver who receives it then and there and also give his valuable feedback to the speaker for him to respond. Hence the communication actually takes place between the speaker and the receiver simultaneously.

In the Duplex communication system, two devices can communicate with each other at the same time.

A type of communication system involves the sender and the receiver where the sender is in charge of sending signals and the recipients only listen to it and respond accordingly. Such communication is also called Simplex communication system.

Half Duplex Communication System

In half Duplex communication system, both the two parties can't communicate simultaneously. The sender has to stop sending the signals to the recipient and then only the recipient can respond.

A walkie talkie works on the half duplex communication system. The military personnel while interacting has to say "Over" for the other person to respond. He needs to speak the security code correctly for the other person to speak. The other party will never communicate unless and until the code is correct and complete.

Tactical Communication System

Another mode of communication is the tactical mode of communication. In this mode of communication, communication varies according to the changes in the environmental conditions and other situations.

All the above modes of communication work for a common objective ie to transfer the information from one party to the other party. The various models of communication system help us to understand the route of flow of information from the sender to the recipients through some medium.

Digital Communication System

The transmission of information from the sender to the recipient through some medium is called as communication. Communication enables us to know what is happening around us. It helps us to share our knowledge with others and also gain from other individual's thoughts and ideas. Communication takes place through various routes and channels and with the help of a medium. A person can chat with his distant relative over the phone and thus the medium of communicatjon in this case is the telephone.

Communication can also take place with the help of light. The airport officials give various signals through light to the pilots for their safe landing. In this case communication is through light and hence is termed as Optical communication.

Satellites also play a vital role in communication by receiving signals from the earth station, amplifying it and then resending it back to the earth. Communication can take place with the aid of an artificial satellite between two points on the earth. In the same way signal can also be sent in a digitalized form as in case of Digital communication.

The process of communication is initiated the moment the sender gets some thought in his brain. To share his ideas with others, the thoughts must be converted into a meaningful content by careful selection of words. This process is also called as encoding. In digital communication, the thought is converted in a digital format for the recipient to understand. In this mode of communication, the data or the information is transferred electronically with the help of computers.

Thus digital communication is a mode of communication where the information or the thought is encoded digitally as discreet signals and electronically transferred to the recipients. Digital communication is one of the most commonly used mode of communication in the current scenario. Organizations generally rely on this mode for all their business communications.

Let us understand digital communication with the help of an example.

Jim wanted to meet all his team members at the conference room to discuss their key responsibility areas and areas of expertise. He didn't have the time to go to their workstations and invite them individually. Instead he opted an easier and cheaper mode to communicate his idea. He sent an email marking a cc to all the participants, inviting them for the meeting. This is an example of Digital communication where the information was sent electronically.

In digital communication information flows in a digital form and the source is generally the keyboard of the computer. A single individual is capable of digital communication and thus it also saves wastage of manpower and is one of the cheapest modes of communication. Digital communication is also a really quick way to communicate. The information can reach the recipient within a fraction of a second. An individual no longer has to wait to personally meet the other individual and share his information.

Digital communication can take place anytime. You just need to have your computer and you can communicate and share your ideas and thoughts anytime anywhere just by the click of a button.

The disadvantage of digital communication is the recipient can't view the expressions of the sender and has to rely only on the information sent to him. Facial expressions don't really matter in digital communication. One must master the art of writing emails for an effective digital communication.

Always remember the other person can't see you; he just has to depend on the mail. Your e mail has to be impressive and relevant to create the desired impact and for the recipient to respond and give his feedback. A person putting up in India can now very easily chat and even see his friend putting up in Los Angeles, thanks to video conferencing and Digital

Notes

communication. Faceboook, Orkut, Twitter are also instrumental in digital communication. Through these social networking sites individuals try to communicate what is new in their lives or share any other important information with friends and relatives. A simple tweet or a scrap can actually let the other person know a lot about the other individuals.

Digital communication system has indeed made our lives easier and is one of the quickest and most reliable modes of communication.

1.5 CHARACTER CODE IN DATA COMMUNICATION

History of Data Communications

- 1753- Scottish magazine suggested running a communications line between villages comprised of 26 parallel wires.
- 1833- Carl Friedrich Gauss developed an unusal system based on a five-by-five matrix representing 25 letters.
- 1832- Samuel F.B.Morse invented telegraph. Morse developed the first practical data communication code which he called the Morse Code. With telegraph, dots and dashes analogous to logic 1s and 0s are transmitted across a wire using electromechanical induction. Various combination of dots and dashes and pauses represented binary codes for letters, numbers and special characters.
- 1844- The first telegraph line was established between Baltimore and Washington, D.C.
- 1849- The frist slow-speed telegraph printer was invented.
- 1850- Western Union Telegraph company was formed in Rochester, NewYork for the purpose of carrying coded messages from one person to another.
- 1874- Emile Baudot invented a telegraph mulitplexer, which allowed signals from up to six different telegraph machines to be transmitted simulatneously over a single wire.
- 1875- Alexander Graham Bell invented telephone.
- 1899- Marconi succeeded in sending radio(wireless) telegraph messages.
- 1930- German engineer Konrad Zuis developed first electrical computer.
- 1940- Bell laboratories developed first special purpose computer using electromechanical relays for performing logical operations.
- 1946- ENIAC computer was developed.
- 1949- The U.S. National Bureau of Standardds developed the first all-electronic diode-based computer capable of executing stored programs.
- 1950- Computers used punch cards for inputting information, printers for outputting information and magnetic tape reels for permanently storing information.

- 1960- Batch-processing systems were replaced by on-line processing systems with terminals connected directly to the computer through serial or parallel communication lines.
- 1970- Microprocessors based Microcomputers were introduced.
- 1980s- Personal computers and Main frame computers were introduced.
- 1980s to 1995- Internet connection was developed slowly.

Standards Organizations for Data Communications

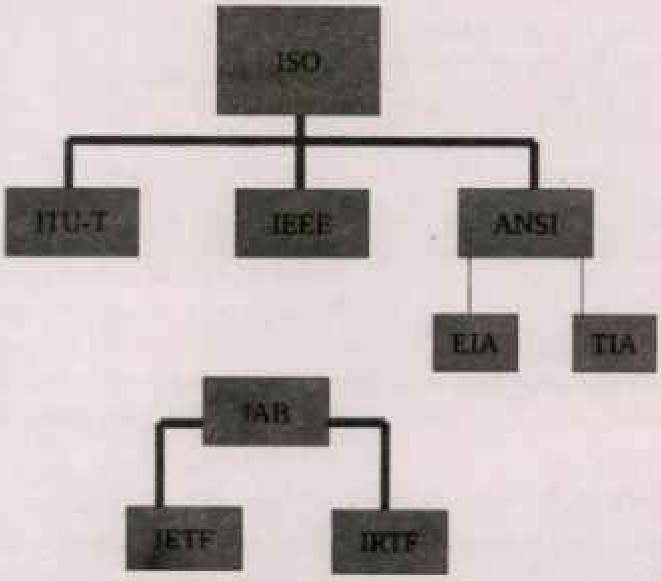


Fig. 1. Standards Organizations for Data and Network Communications

International Standards Organization (ISO)

ISO was started in 1946. The members of ISO are selected from various governments throughout the world. The ISO creates the sets of rules and standards for graphics and document exchange and provides models for equipment and system compatibility, quality and reduced costs.

The ISO is responsible for coordinating the work of the other standards organizations. The member body of the ISO from the United States is the American National Standards Institute (ANSI).

International Telecommunications Union-Telecommunications Sector(ITU-T)

It was formerly called as CCITT (Committe Consultant for International Telephony and Telegraphy). It is situated in Geneva, Switzerland. Membership in the ITU-T consists of government authorities and representatives from many countires. It develops the recommended sets of rules and standards for telephone and data communications. It has developed three sets of specifications:. The V series for modem interfacing and data transmission over telephone lines. The X series for data transmission over public digital networks,Email and directory serivces. The I and Q series for Integrated Services Digital Network (ISDN) and its extension is Broadband ISDN. The ITU-T is separated into 14 study groups.

Institute of Electrical and Electronics Engineering (IEEE)

The IEEE is an international professional organization founded in united states and is comprised of electronics, computer and communications engineers. The IEEE works along with ANSI to develop communications and information processing standards with the aim of advancing theory, creativity and product quality in any field associated with electrical engineering.

American National Standards Institute(ANSI)

It is an official standards agency for the united states and is the U.S voting representative for the ISO. ANSI is a completely private, nonprofit organization comprised of euipment manufacturers and users of data processing equipment and services.

ANSI membership is comprised of people from professional societies, industry associations, governmental and regulatory bodies and consumer groups.

Electronics Industry Association(ESA)

EIA acti\ ,ies include standards development and inncreasing public awareness. The EIA is responsible for RS(Recommended Standard) series of standards for data and telecommunications.

Telecommunications Industry Association (TIA)

Its a trade assocaition in the communications and information technology industry. It represents manufacturers of communications and information technology products and services providers for the global marketplace.

Internet Architecture Board(IAB)

The responsibilities of IAB are:

(1. Internet Architecture protocol.

(2) Create Internet standards.

(3) Administration of the various Internet assigned numbers.

(4) Acts as representative for Internet Society.

(5) Acts as a source of advice and guidance.

Internet Engineering Task Force (IETF)

Its a large international community of network designers, operators, venders, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet.

Internet Research Task Force (IRTF)

It promotes the research on evolution of future internet in the topics related to Internet protocols, applications, architecture and technology.

1.6 DATA COMMUNICATIONS CIRCUITS

The underlying purpose of a digital communications circuit is to provide a transmission path between locations and to transfer digital information from one station (node, where computers or other digital equipment are located) to another using electronic circuits. Data communications circuits utilize electronic communications equipment and facilities to interconnect digital computer equipment. Communication facilities are physical means of interconnecting stations and are provided to data communications users through public telephone networks (PTN), public data networks (PDN), and a multitude of private data communications systems.

The following figure shows a simple two-station data communications circuit.

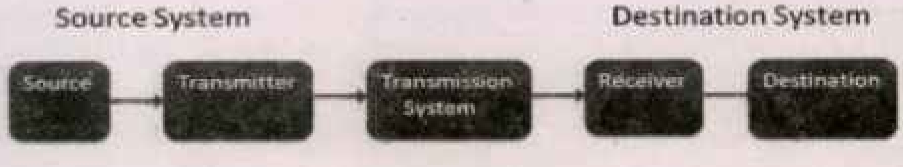


Fig. 2: Simplified Block Diagram of a two-station data communications circuit.

Data Communication Circuit – Its purpose is to provide a transmission path between locations and to transfer digital information from one station to another using electronic circuits.

- Station- is simply an endpoint where subscribers gain access to the circuit.
- Node- A station is sometimes called as node, which is the location of computers, computer terminals, workstation and other digital computing equipment. The communication facilities are provided to data communication users through public telephone networks (PTN), public data networks(PDN) and a multitude of private data communications systems.

The main components are:

- Source: This device generates the data to be transmitted; examples are mainframe computer, personal computer, workstation etc. The source equipment provides a means for humans to enter data into system.
- Transmitter: A transmitter transforms and encodes the information in such a way as to produce electromagnetic signals that can be transmitted across some sort of transmission system. For example, a modem takes a digital bit stream from an attached device such as a personal computer and transforms that bit stream into an analog signal that can be handled by t he telephone network.
- Transmission medium: The transmission medium carries the encoded signals from the transmitter to the receiver. Different types of transmission media include free-space

radio transmission (i.e. all forms of wireless transmission) and physical facilities such as metallic and optical fiber cables.

- Receiver: The receiver accepts the signal from the tranemission medium and converts it into a form that can be handled by the destination device. For example, a modem will accept an analog signal coming from a network or transmission line and convert it into a digital bit stream.

1.7 DATA COMMUNICATIONS CODES

Data communications codes are used to represent characters and symbols such as letters, digits and punctuation marks. Data communications codes are called character codes, character sets, symbol codes or character languages. The relationship of bytes to characters is determined by a character code. Each time a user presses a key on a terminal/PC, a binary code is generated for the corresponding character. Various character codes have been used in data communication including:

Baudot Code

The Baudot code (sometimes called the Telex code) was the first fixed-length character code. One of first codes developed for machine to machine communication. It uses 1's and 0's instead of dots and dashes. It was used for transmitting telex messages (punch tape).

- Fixed character length (5-bits)
- 32 different codes
- increased capacity by using two codes for shifting
- 11111 (32) Shift to Lower (letters)
- 11011 (27) Shift to Upper (digits, punctuation)
- 4 special codes for SP, CR, LF & blank
- Total = 26 + 26 + 4 = 56 different characters

Problems with Baudot:

- required shift code to switch between character sets
- no lower case, few special characters
- no error detection mechanism
- characters not ordered by binary value
- designed for transmitting data, not for data processing

International Baudot

- Added a 6th bit for parity

Used to detect errors within a single character

Character		Data bit				
Lower case	Upper case	5	4	3	2	1
A	-	0	0	0	1	1
B	?	1	1	0	0	1
C	:	0	1	1	1	0
D	$	0	1	0	0	1
E	3	0	0	0	0	1
F	!	0	1	1	0	1
G	&	1	1	0	1	0
H	#	1	0	1	0	0
I	8	0	0	1	1	0
J	'	0	1	0	1	1
K	(	0	1	1	1	1
L	)	1	0	0	1	0
M	.	1	1	1	0	0
N	,	0	1	1	0	0
O	9	1	1	0	0	0
P	0	1	0	1	1	0
Q	1	1	0	1	1	1
R	4	0	1	0	1	0
S	BELL	0	0	1	0	1
T	5	1	0	0	0	0
U	7	0	0	1	1	1
V	;	1	1	1	1	0
W	2	1	0	0	1	1
X	/	1	1	1	0	1
Y	6	1	0	1	0	1
Z	"	1	0	0	0	1
Letters (shift to Lower case column)		1	1	1	1	1
Figures (shift to Upper case column)		1	1	0	1	1
Space		0	0	1	0	0
Carriage return		0	1	0	0	0
Line feed		0	0	0	1	0
Blank		0	0	0	0	0

Baudot code

ASCII Code

- American Standard Code for Information Interchange.
- 7-bit code developed by the American National Standards Institute (ANSI).
- Most popular data communication character code today.
- Allows for 128 different character representations (27).
- Includes upper and lower case.
- Lots of special characters (non-printable).
- Generally used with an added parity bit.
- Better binary ordering of characters than EBCDIC.
- Extended ASCII uses 8 data bits and no parity
- Used for processing and storage of data.
- Allows for international characters.
- 8th bit stripped of for transmission of standard character set.

EBCDIC Code

- extended Binary Coded Decimal Interchange Code.
- 8-bit character code developed by IBM.

Notes

- used for data communication, processing and storage.
- extended earlier proprietary 6-bit BCD code.
- designed for backward compatibility or marketing?
- still in use today on some mainframes and legacy systems.
- allows for 256 different character representations (28).
- includes upper and lower case.
- lots of special characters (non-printable).
- lots of blank (non-used codes).
- assigned to international characters in various versions

SUMMARY OF CHARACTER CODES

Morse = . _

Baudot = 5 bit (no parity)

Int. Baudot = 6 bit (5 data + 1 parity)

ASCII = 8 bit (7 data + 1 parity)

EBCDIC = 9 bit (8 data + 1 parity)

UNICODE = 16 bits (no parity)

Data Modems

The primary purpose of a data modem is to interface computers, computer networks and other digital terminal equipment to analog communication lines and radio channels. The word modem is a contraction derived from the words modulator and demodulator. In a modem transmitter, digital signals modulate an analog carrier and in a receiving modem, analog signals are demodulated and converted into digital signals.

A modem is sometimes called as DCE(Data communication equipment), a data set, a dataphone. Modems are generally classified as either asynchronous or synchronous. Modems use one of the following modulation techniques:

(1) Amplitude Shift Keying (ASK)

(2) Frequency Shift Keying (FSK)

(3) Phase Shift Keying (PSK)

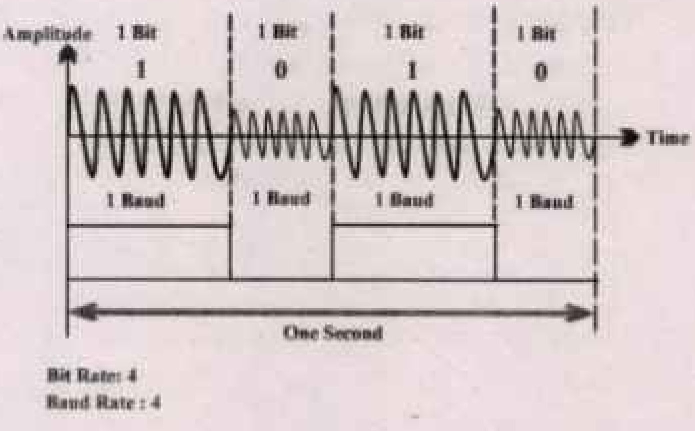
(4) Quadrature Amplitude Modulation (QAM)

Any of the three characteristics can be altered in this way, giving us at least three types for modulating digital data into an analog signal: amplitude shift keying (ASK), frequency shift keying (FSK), and phase shift keying (PSK). In addition, there is a fourth (and better) mechanism that combines changing both the amplitude and phase, called quadrature amplitude modulation (QAM). QAM is the most efficient of these options and is the mechanism commonly used today.

Amplitude Shift Keying

Amplitude Shift Keying (ASK) is a Modulation technique that is used in Digital to analog Conversions. This technique uses strength of signal to represent binary 0 or 1 value.in this only amplitude changes while frequency and phase both are kept constant.it uses finite number of amplitudes, each assigned a unique pattern of binary digits that represents binary 1 or 0.

In amplitude shift keying, the amplitude of the carrier signal is varied to create signal elements. Both frequency and phase remain constant while the amplitude changes. Binary ASK (BASK) although we can have several levels (kinds) of signal elements, each with a different amplitude, ASK is normally implemented using only two levels. This is referred to as binary amplitude shift keying or on-off keying (OOK). The peak amplitude of one signal level is 0; the other is the same as the amplitude of the carrier frequency. Figure 57 gives conceptual views of binary ASK.



Bandwidth for ASK also shows the bandwidth for ASK. Although the carrier signal is only one simple sine wave, the process of modulation produces a nonperiodic composite signal. This signal, as was discussed earlier, has a continuous set of frequencies. As we expect, the bandwidth is proportional to the signal rate (baud rate). However, there is normally another factor involved, called d, which depends on the modulation and filtering process. The value of d is between 0 and 1. This means that the bandwidth can be expressed as shown, where 5 is the signal rate and the B is the bandwidth.

$B =(1 +d) \times S$

The formula shows that the required bandwidth has a minimum value of 5 and a maximum value of 25. The most important point here is the location of the bandwidth.

The middle of the bandwidth is where *le* the carrier frequency, is located. This means if we have a bandpass channel available, we can choose our *Ie* so that the modulated signal occupies that bandwidth. This is in fact the most important advantage of digital-to- analog conversion. We can shift the resulting bandwidth to match what is available.

Implementation of ASK

The complete discussion of ASK implementation is beyond the scope of this book. However,

Notes

the simple ideas behind the implementation may help us to better understand the concept itself. Figure illustrate how we can simply implement binary ASK.

If digital data are presented as a unipolar NRZ, digital signal with a high voltage of IV and a low voltage of 0 V, the implementation can achieved by multiplying the NRZ digital signal by the carrier signal coming from an oscillator. When the amplitude of the NRZ signal is 1, the amplitude of the carrier frequency is held; when the amplitude of the NRZ signal is 0, the amplitude of the carrier frequency is zero.

1.8 DIGITAL DATA RATE

The data transfer rate (DTR) is the amount of digital data that is moved from one place to another in a given time. The data transfer rate can be viewed as the speed of travel of a given amount of data from one place to another. In general, the greater the bandwidth of a given path, the higher the data transfer rate.

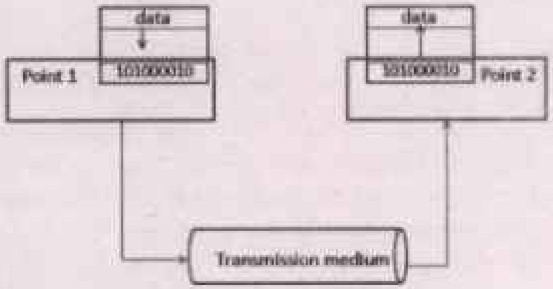
DTR can be defined as the ratio of the total amount of digital data transferred between two points in some defined period of time. Where the two points can be two network components say two computers or data can be transferred between a thumb drive and a hard drive.

Data transfer rate is actually a measure of the speed at which network components can exchange data(send or receive). It is measured in either bits per second or bytes per second. For practical purposes, it is measured in Megabits per second or Megabytes per second. But you have usually seen KBps (Kilobyte per second) while uploading or downloading something. Japan has shown the highest data transfer rate of 14 terabits per second using only a single optical fiber cable.

Data Transfer Rate(DTR) = Total amount of Digital data transmitted/Total time taken

Some data transfer rate units are:

- 1 Kbps = 210bps = 1024 bps
- 1 Mbps = 220bps = 1024 Kbps
- 1 Gbps = 230bps = 1024 Mbps
- 1 Tbps = 240bps = 1024 Gbps



Transmission of data from one point to another

Importance of data transfer rate in the computer network:

Data transfer rate is of utmost importance in today's world because of the following reasons:

- It has a direct effect on one's business especially if it is some kind of online service because then you must have a high data transfer rate to provide services without any interruption.
- Data transfer rate is also important in performing some complex tasks like online streaming, having a video call, or any work which is life and is of high priority.
- Data transfer rate is also used in the assessment of different devices and technologies.
- Data transfer rate gives an insight into the performance of a system and network, so it is useful for making improvements.

Factors affecting data transfer rate

There are several factors that affect the data transfer rate, some of them are:

1. **Network Congestion:** Network Congestion can be understood as a situation that may arise if the user sends data at a greater rate than that permissible by network resources. When the network resources reaches their maximum capacity then it affects the data transfer rate.

   Following problems arise due to network congestion :

   - Packet Loss: Packets are lost due to network congestion as after the expiry of the time to live or having no more hop limit the data packet automatically drops.
   - Increase in Delay: Due to packet loss no acknowledgment will receive at the sender side so after a timeout period sender will send new data packets so which will increase the delay in communication.
   - Network termination: Network will face connection issues as sessions will be dropped because due to network congestion too many packets are lost. One will get session timeout messages on the screen or page that is taking too long to respond to messages.

2. **Condition of Client or Server:** It means the client or server should be in a good condition meeting all the criteria for making a better network. It should have all the necessary hardware along with the latest software. The data transfer rate will surely be affected if the minimum processor, RAM, and other components are not fulfilling the defined minimum requirement criteria. Suppose for achieving a data transfer rate of X KBps we need a minimum of 4 GB ram and an octacore processor if these criteria are not fulfilled then the data transfer rate will get affected.

3. **Latency:** Latency is defined as the amount of time needed by the network to transfer a data packet from source to destination. If latency is affected by one or more parameters then in turn it will affect the data transfer rate. There is an inter-dependent relationship between latency and data transfer rate which depends on the protocols which are used to carry data.

Notes

Some of the factors which affect latency are:

- Path Length traveled by the packet from source to destination.
- Effectiveness and reliability of network devices.
- Count of devices which are being hoped in reaching to the destination.
- Latency also depends on the performance of individual devices used in data transfer from source to destination.

4. **Transmission Media:** The data transfer rate is different for different media available like if we are using an optical fiber cable and a twisted pair cable then the data transfer rate will obviously be different. For example, USB 1.0 has a data transfer rate of 12 Mbps while USB 2.0 has a rate of 480 Mbps. Similarly, USB 3.0 and 3.1 have a data transfer rate of 5 GB per second and 10 GB per second respectively.

Calculating Data Transfer Rate

Suppose your internet provider has advertised to give you a speed of 80 Mbps (Megabits per second) and you have a file of say 80 MB then how much time will it take?

Let's calculate, we know that there are 8 bits in 1 byte so speed should be divided by 8 as our file is in bytes not in bits.

So speed will be 80/8 = 10 MBps (Megabytes per second)

now 80 MB file will be transferred in 80/10 = 8 seconds.

This is how we calculate the downloading speed and time of files.

Now there are two terms :

- Downloading Speed: Downloading Speed tells us how fast data/files can be transmitted from server to your computer.
- Uploading Speed: Uploading Speed tells us how fast we can upload data/files to a server from our system by using the internet.

There are a number of tools available online to measure downloading and uploading speed some of them are broadband performance and speedtest. One can also test hardware by using software like HDTach and CrystalDiskMark.

1.9 SYNCHRONOUS AND ASYNCHRONOUS DATA

In any organization, networking infrastructure features several software and hardware that help establish a connection between different devices and computers on a network. These hardware and software devices facilitate data transmission in a computer network. Most times, this data transmission is conducted in either of the two modes – asynchronous or synchronous. Now, you may think of how these modes differ and which mode is better? Read this post to know the answers.

In synchronous data transmission, the data is transferred in the form of frames or chunks between a receiver and a sender. The data is transferred in a paired approach, and thus, the synchronization of sender and a receiver is necessary. This synchronization becomes possible only when these systems share an internal clock. This data transmission method is employed to transfer time-sensitive data such as voice and real-time video through CCTV.

What is Asynchronous Data Transmission?

Asynchronous data transmission is exactly opposite to synchronous data transmission and doesn't require active synchronization between the receiver and the sender. The data moves in the form of character or byte in a half-paired approach. The character size of data transferred is 8 bits, which becomes 10 bit when the parity bit is added at the beginning and end of the data. This transmission method utilizes parity bits for informing the receiver about data translation. Usually1 character or byte of data is transferred at a time. This data transmission method doesn't require 2-way or parallel communication to work, which is why it is considered to be simpler than synchronous data transmission. Emails, letters, and forums are a few of the best examples of asynchronous data transmission.

Difference between Synchronous and Asynchronous Data Transmission

Although the basic differences between synchronous and asynchronous data transmission have been covered before, it is important to know how they differ in terms of application. The following pointers will help you understand it better.

- **Data Gap:** Owing to synchronization, there is no gap between the data sent and received in a synchronous data transmission. In case of asynchronous data transmission, as receiver and sender do not synchronize in real time, so there is a gap between the data sent and received. The start and stop bits are added to data to inform the receiver about the start and end of data character. Although the asynchronous data transmission doesn't follow a clock for synchronization, the bits added to the front and end synchronize the data transmission by indicating if the character has been received or sent. The timing of each character begins and ends with a start and stop bit. The gap between the transmission of characters is known as a mark state. This state usually has a binary 1 or negative voltage.
- **Operational Costs:** As said before, the sender and the receiver use a synchronized clock for data transfer, and this makes data transfer faster, and costlier. Against this, the sender and the receiver uses their own input clocks, thus, the data transfer is slow and the transmission is much cheaper than synchronized transmission.
- **Transmission Line:** Synchronous data transmission makes efficient use of transmission line; against this, the transmission line remains idle between the character transmissions.
- Time Interval: As synchronization is the key to data transfer in synchronous data transmission so the time interval is constant. On the other hand, in asynchronous data transmission, the time interval is random and not constant.

As seen, there are several benefits and limitations of each of these data transmission modes, so the choice entirely depends on the type of application. If the application is operated in real time then synchronous data transmission is ideal and if not then asynchronous data transmission is preferred.

Whichever mode of transmission exists, its proper implementation depends on the quality of receiving and sending devices used. It is important that you source these devices from trusted suppliers like VERSITRON. The company provides one of the vast selections of fiber optic media converters, Ethernet media converters, Ethernet network switches, fiber optic multiplexers, and so on.

Difference between Synchronous and Asynchronous Modems

Synchronous Data	Asynchronous Data
In these type of Modems, clocking information is recovered in the receiver.	In these type of Modems, clocking information is not recovered at receiver and may not require
These Modems uses the modulation techniques like PSK and QAM	These Modems uses the modulation techniques like ASK and FSK
It can be used for Medium and High Speed applications up to 57.6 Kbps	It can be used for Low Speed applications below 2.4 Kbps.

Low-Speed Modems

- Low speed modems are generally asynchronous.
- It uses Non-coherenr FSK.
- The transmit carrier and clock frequencies need not be recovered by the receive modem.
- Therefore, they don't need scrambler and descrambler circuits.
- Speed 1200 to 1800 baud.

Medium and High-Speed Modems

- Medium and High speed Modems are used where transmission rates of 2400 bps or baud are required.
- PSK or QAM modulation techniques are used.
- These Modems are synchronous.
- Because these Modems are synchronous, clock timing recovery and carrier recovery must be required.
- These Modems contain scrambler and descrambler circuits and adaptive equalizers.
- Example: the 208 Modem is a synchronous, 4800 baud rate, 8-DPSK modulation technique. Each symbol represents three bits and is 0.625 milliseconds duration.

Modem Control

The smart Modems are controlled by other larger computers through a system of commands. The most common system of modem commands is the AT command set which is also known as the Hayes command set. Hayes Microcomputer Products originally developed the AT command set for its own line of modems

Characters	Commands
At	Attention
A	Answer an incoming call
DT	Dial using DTMF tones

DP	Dial using Pulse dialing
E0	Do not echo transmitted data to terminal screen
E1	Echo transmitted data to terminal screen
F0	Half-duplex communications
F1	Full-duplex communications
H	Go on-hook (Hang up)
O	Switch from command to on-line mode
Z	Reset Modem
+++	Escape code; switch from on-line mode to command mode

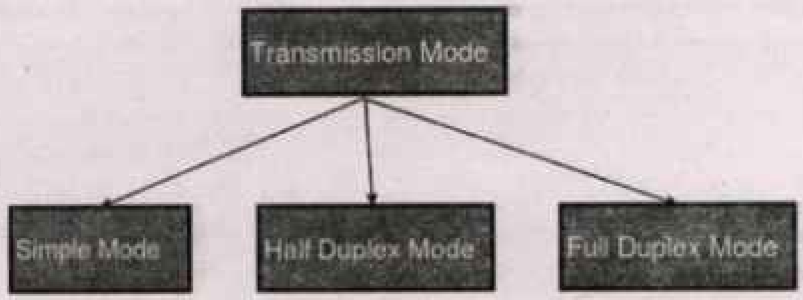
AT command mode

- All modem commands in the AT command set begin with the ASCII characters AT (Attention).
- In the command mode, the modem monitors the information sent to it through the DTE(Data Terminal Equipment-Computer system)[Modem called as DCE-Data Communication Equipment] by the local terminal looking for the ASCII characters AT.
- ASCII character 'T' is the command to use tones rather than pulses and the character 'D' is the command to dial.
- For example to dial the telephone number 91-424-2533279, the character sequence would be ATDT914242533279. AT on-line mode
- Once communications have been established with a remote modem, the local modem switches to the on-line mode.
- The local modem simply accepts the characters and allows them to modulate its carrier before sending them to a remote location.
- The local terminal (computer system) can switch the modem from the on-line mode to the command mode by sending three consecutive plus signs (+ + +). This sequence is called as escape code.
- In response to the escape code, the modem switches to the command mode and begins monitoring data for the ASCII AT command code.

1.10 TRANSMISSION MODES

A transmission may be simplex, half duplex, or full duplex. In simplex transmission, signals are transmitted in only one direction; one station is transmitter and the other is receiver. In half-duplex operation, both stations may transmit, but only one at a time. In full-duplex operation, both stations may transmit simultaneously.

Notes



Transmission mode is of three types.

i) Simplex Transmission

ii) Half Duplex Transmission

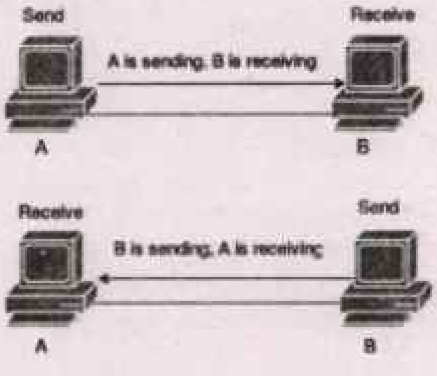
iii) Full Duplex Transmission

Simplex Transmission

In simplex mode, the communication is unidirectional, as on a one-way street. Only one of the two devices on a link can transmit; the other can only receive. Keyboards and traditional monitors are examples of simplex devices. The keyboard can only introduce input; the monitor can only accept output. The simplex mode can use the entire capacity of the channel to send data in one direction. Examples are Radio and Television broadcasts. They go from the TV station to your home television.

Half Duplex Transmission

In half-duplex mode, each station can both transmit and receive, but not at the same time. When one device is sending, the other can only receive, and vice versa. The half-duplex mode is like a one-lane road with traffic allowed in both directions. When cars are traveling in one direction, cars going the other way must wait. In a half- duplex transmission, the entire capacity of a channel is taken over by whichever of the two devices is transmitting at the time.



Full Duplex Transmission

In full-duplex mode, both stations can transmit and receive simultaneously. The full-duplex mode is like a two way street with traffic flowing in both directions at the same time. One common example of full-duplex communication is the telephone network.

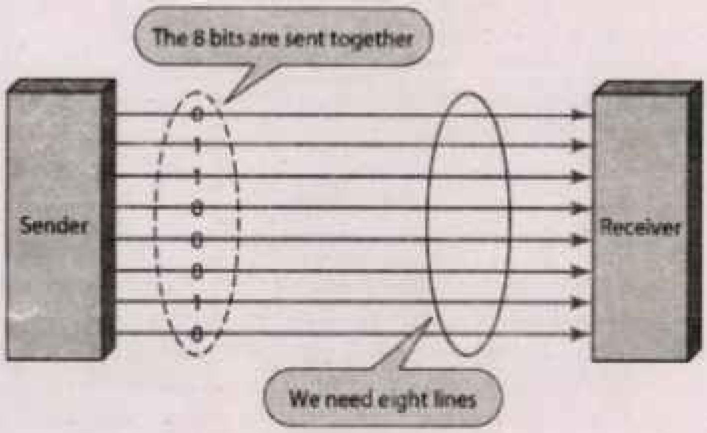
When two people are communicating by a telephone line, both can talk and listen at the same time.

1.11 DIGITAL DATA TRANSMISSION METHODS

Above, we see that for communication to occur there will be a channel of communication through which the devices are interconnected. In digital data transmission where we have more than one bits to send from sender to receiver. Our primary when we are considering the wiring is the data stream. Do we send 1 bit at a time; or do we group bits into larger groups and, if so, how?

The transmission of binary data across a link can be accomplished in either parallel or serial mode. In parallel mode, multiple bits are sent with each clock tick. In serial mode, 1 bit is sent with each clock tick. While there is only one way to send parallel data, there are three subclasses of serial transmission: asynchronous, synchronous, and isochronous

Parallel Transmission



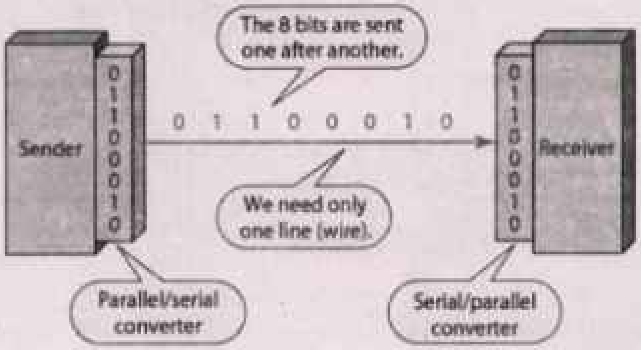
Binary data, consisting of 1s and 0s, will be organized into groups of n bits each. Computers produce and consume data in groups of bits. By grouping, we can send data n bits at a time instead of 1. This is called parallel transmission.

The advantage of parallel transmission is speed. All else being equal, parallel transmission can increase the transfer speed by a factor of *n* over serial transmission. Shortcoming of parallel transmission it requires n communication lines just to transmit the data stream. Hence it is expensive, parallel transmission is usually limited to short distances.

Notes

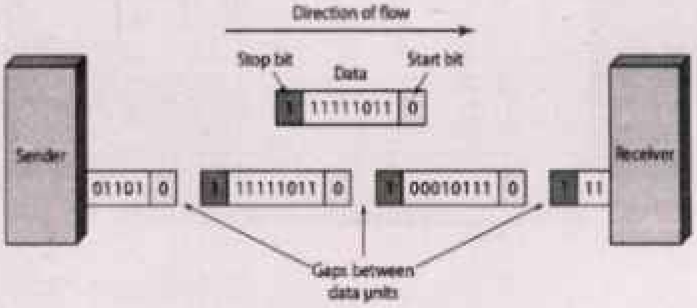
Serial Transmission

In serial transmission one bit follows another, so we need only one communication channel rather than n to transmit data between two communicating devices. The advantage of serial over parallel transmission is that with only one communication channel, serial transmission reduces the cost of transmission over parallel by roughly a factor of n. Since communication within devices is parallel, conversion devices are required at the interface between the sender and the line (parallel-to-serial) and between the line and the receiver (serial-to-parallel). Serial transmission occurs in one of three ways: asynchronous, synchronous, and isochronous


The 8 bits are sent one after another.
Sender
0 1 1 0 0 0 1 0
0 1 1 0 0 0 1 0
Receiver
We need only one line (wire).
Parallel/serial converter
Serial/parallel converter

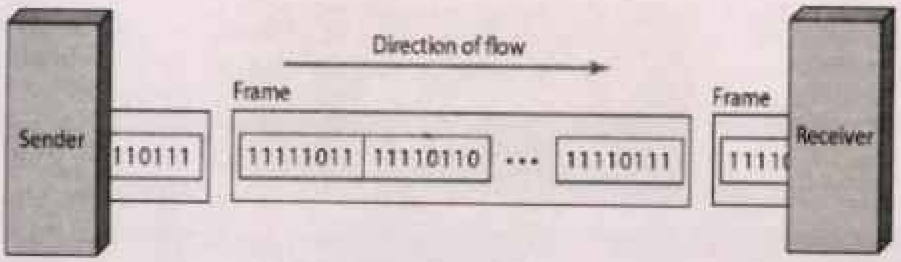
A Synchronous Transmission

- In asynchronous transmission, send 1 start bit (0) at the beginning and 1 or more stop bits (1s) at the end of each byte. There may be a gap between each byte.
- Asynchronous here means "asynchronous at the byte level," but the bits are still synchronized; their durations are the same.

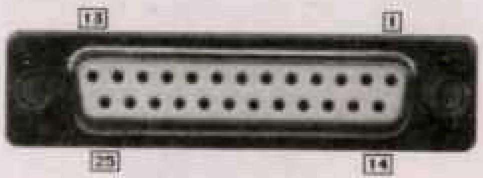


Synchronous Transmission

In synchronous transmission, we send bits one after another without start or stop bits or gaps. It is the responsibility of the receiver to group the bits. The bits are usually sent as bytes and many bytes are grouped in a frame. A frame is identified with a start and an end byte.

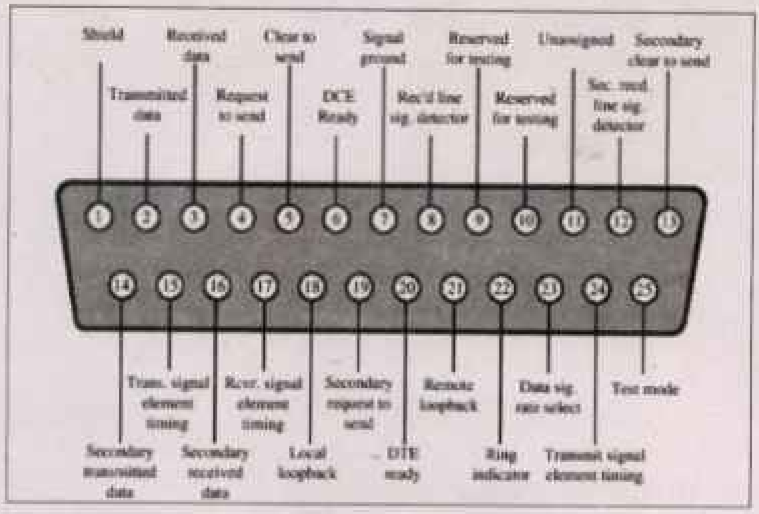


Serial Interfaces - RS 232



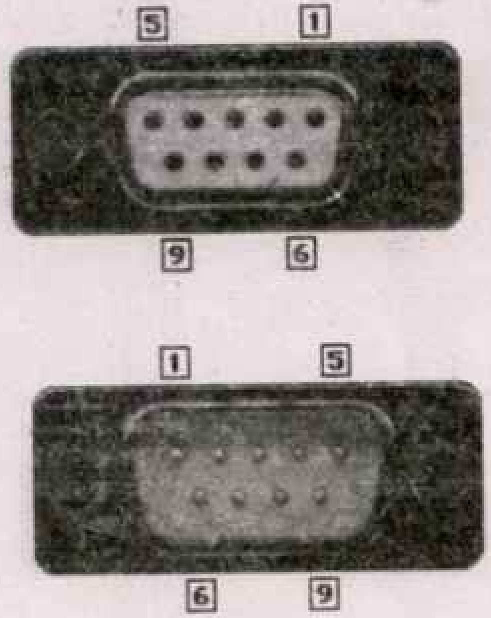
DB-25 Female

DB-25 Male

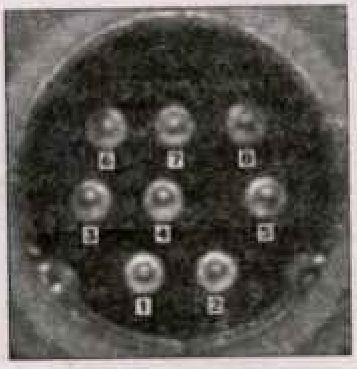


RS-232 DB-25 Pinouts

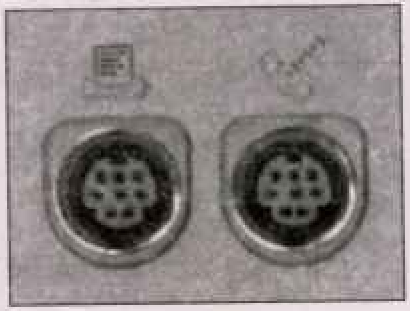
Notes



RS-232 DB-9 Connectors



DIN-8 Male



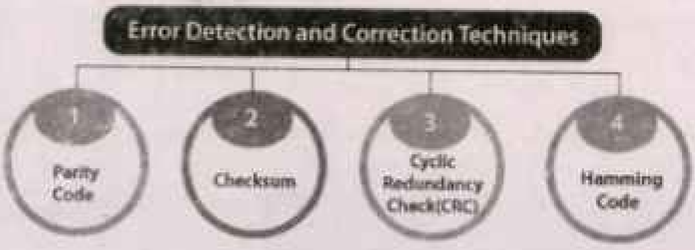
DIN-8 Female

1.12 ERROR DETECTION AND ERROR CORRECTION CODES

Networks must be able to transfer data from one device to another with complete accuracy. Data can be corrupted during transmission. For reliable communication, errors must be detected and corrected. Error control can be divided into two general categories:

1. Error Detection
2. Error Correction

Error detection and correction code plays an important role in the transmission of data from one source to another.


Error Detection and Correction Techniques
1
Parity Code
2
Checksum
3
Cyclic Redundancy Check(CRC)
4
Hamming Code

The noise also gets added into the data when it transmits from one system to another, which causes errors in the received binary data at other systems. The bits of the data may change(either 0 to 1 or 1 to 0) during transmission.

Error detection and correction code plays an important role in the transmission of data from one source to another. The noise also gets added into the data when it transmits from one system to another, which causes errors in the received binary data at other systems. The bits of the data may change(either 0 to 1 or 1 to 0) during transmission.

It is impossible to avoid the interference of noise, but it is possible to get back the original data. For this purpose, we first need to detect either an error z is present or not using error detection codes. If the error is present in the code, then we will correct it with the help of error correction codes.

Networks must be able to transfer data from one device to another with complete accuracy. Data can be corrupted during transmission. For reliable communication, errors must be detected and corrected. Error control can be divided into two general categories:

1. Error Detection
2. Error Correction

Error detection and Error correction are implemented either at the data link layer or the transport layer of the OSI model.

Error detection code

The error detection codes are the code used for detecting the error in the received data bitstream. In these codes, some bits are included appended to the original bitstream.

Error detecting codes encode the message before sending it over the noisy channels. The encoding scheme is performed in such a way that the decoder at the receiving can find the errors easily in the receiving data with a higher chance of success.

Parity Code

In parity code, we add one parity bit either to the right of the LSB or left to the MSB to the original bitstream. On the basis of the type of parity being chosen, two types of parity codes are possible, i.e., even parity code and odd parity code.

Features of Error detection codes

These are the following features of error detection codes:

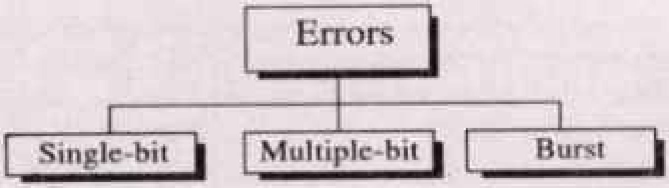
Notes

These codes are used when we use message backward error correction techniques for reliable data transmission. A feedback message is sent by the receiver to inform the sender whether the message is received without any error or not at the receiver side. If the message contains errors, the sender retransmits the message.

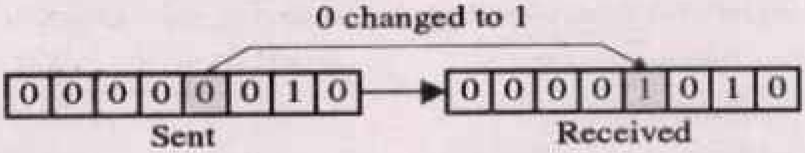
In error detection codes, in fixed-size blocks of bits, the message is contained. In this, the redundant bits are added for correcting and detecting errors. These codes involve checking of the error. No matter how many error bits are there and the type of error.

Parity check, Checksum, and CRC are the error detection technique.

Types of Errors



1. Single-bit error

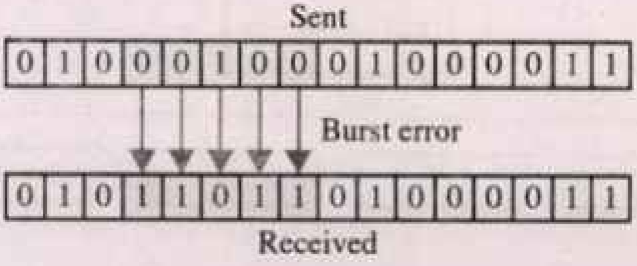


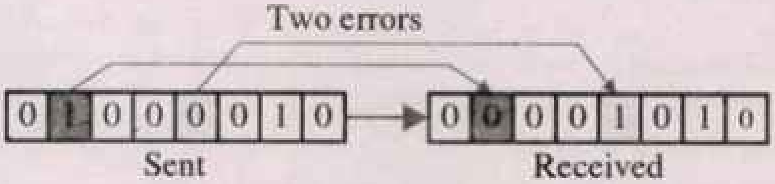
Single bit errors are the least likely type of errors in serial data transmission because the noise must have a very short duration which is very rare. However this kind of errors can happen in parallel transmission.

2. Burst error

The term burst error means that two or more bits in the data unit have changed from 1 to 0 or from 0 to 1. Burst errors does not necessarily mean that the errors occur in consecutive bits, the length of the burst is measured from the first corrupted bit to the last corrupted bit. Some bits in between may not have been corrupted.

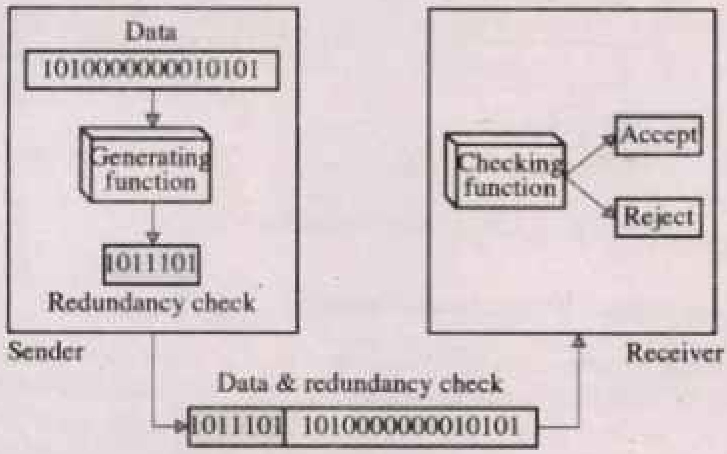
Burst error is most likely to happen in serial transmission since the duration of noise is normally longer than the duration of a bit. The number of bits affected depends on the data rate and duration of noise.





Error detection

Error detection means to decide whether the received data is correct or not without having a copy of the original message. Error detection uses the concept of redundancy, which means adding extra bits for detecting errors at the destination.



Redundancy Checks Types:

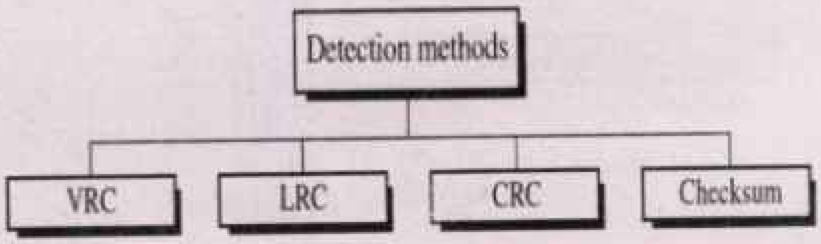
(1). VRC - Vertical Redundancy Check

(2). LRC - Longitudinal Redundancy Check

(3). CRC - Cyclic Redundancy Check

(4). Checksum

Notes



(1) VRC - Vertical Redundancy Check

VRC is also referred to as character parity. With character parity, each character has its own error-detection bit called the parity bit. The parity bit is considered as a redundant bit. An n-character message would have 'n' redundant parity bits.

- It can detect single bit error.
- It can detect burst errors only if the total number of errors is odd.

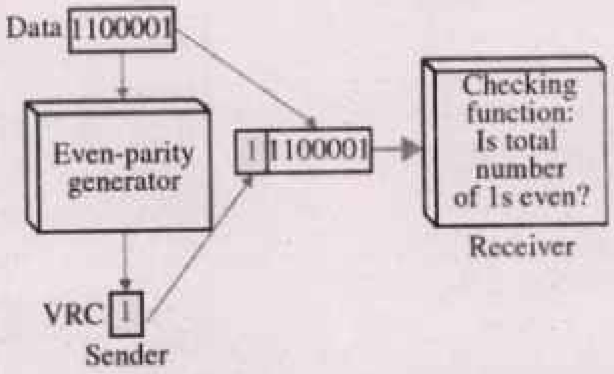


Fig. 3. VRC-Vertical Redundancy Check

(2) LRC - Longitudinal Redundancy Check

LRC is also referred to as message parity since it is used to check error occurred within a message. With LRC each bit position has a parity bit. LRC is the result of XORing the bits present in all the characters present in a message whereas VRC is the result of XORing the bits within a single character.

- In LRC even parity is generally used, whereas with VRC odd parity is generally used.
- LCR increases the likelihood of detecting burst errors.
- If two bits in one data units are damaged and two bits in exactly the same positions in another data unit are also damaged, the LRC checker will not detect an error.

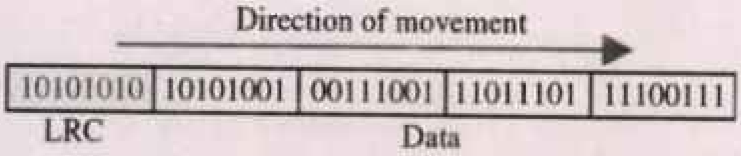


Fig. 4. LRC - Longitudinal Redundancy Check

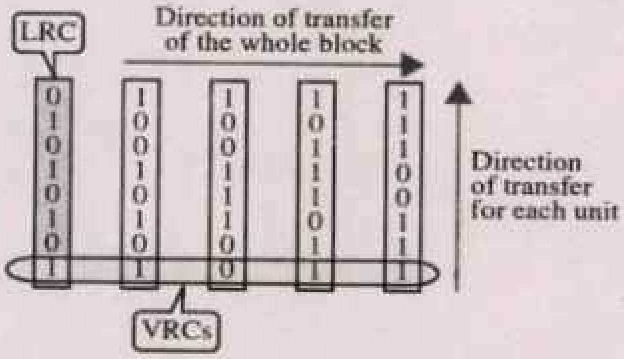

LRC
Direction of transfer of the whole block
01010101
10010101
10011100
10111011
11100111
Direction of transfer for each unit
VRCs

Fig. 5. VRC and LRC

(3) Checksum

The characters within a message are combined together to produce an error-checking character called as checksum, which can be as simlple as the arithmetic sum of the numerical values of all the characters in the message. The checksum is appended to the end of the message.

The receiver replicates the combining operation and determines its own checksum. The receivers checksum is compared with transmitter checksum appended with the message, and if they are the same, it is assumed that no transmission errors have occurred.

(4). CRC - Cyclic Redundancy Check

It's a most reliable redundancy checking technique for errror detection is a convolutional coding scheme called Cyclic Redundancy Check(CRC). Given a k-bit frame or message, the transmitter generates an (n-k) bit sequence, known as a frame check sequence (FCS)(or) Block Check Code(BCS), so that the resulting frame, consisting of 'n' bits, is exactly divisible by some predetermined number.

The receiver then divides the incoming frame by the same number and, if there is no remainder, assumes that there was no error.

Notes

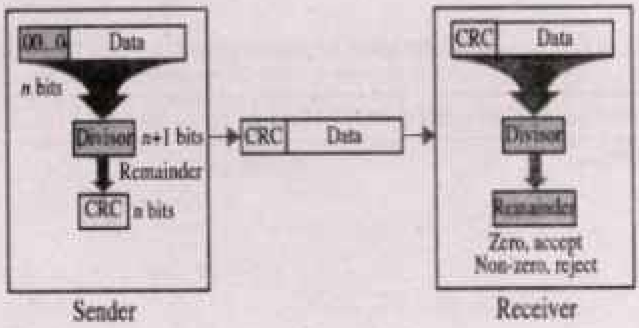
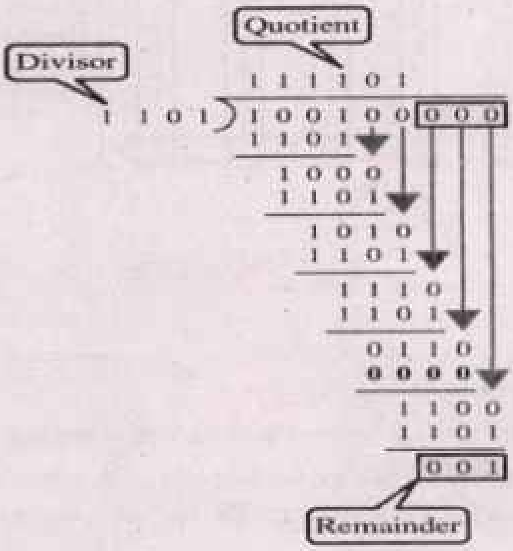


Fig. 6. Cyclic Redundancy Check



$$\frac{G(x)}{P(x)}=Q(x)+R(x)$$

G(x) = Message Polynomial (message or Data)

P(x) = Generator Polynomial

Q(x) = Quotient

R(x) = Remainder (CRC bits)

For this example

G(x)=x^5+x^2 P(x)=$x^3+x^2+x^0$

G(x)={1,0,0,1,0,0}

P(x)={1,1,0,1}

Here in this example CRC bits are {0,0,1}

Error Correction

Error correction codes are generated by using the specific algorithm used for removing and detecting errors from the message transmitted over the noisy channels. The error-correcting codes find the correct number of corrupted bits and their positions in the message. There are two types of ECCs(Error Correction Codes), which are as follows.

Block codes

In block codes, in fixed-size blocks of bits, the message is contained. In this, the redundant bits are added for correcting and detecting errors.

Convolutional codes

The message consists of data streams of random length, and parity symbols are generated by the sliding application of the Boolean function to the data stream. The hamming code technique is used for error correction

1.13 TYPES OF SIGNALS

A signal is an electromagnetic or electrical current that carries data from one system or network to another. In electronics, a signal is often a time-varying voltage that is also an electromagnetic wave carrying information, though it can take on other forms, such as current. There are two main types of signals used in electronics: analog and digital signals. This article discusses the corresponding characteristics, uses, advantages and disadvantages, and typical applications of analog vs. digital signals.

Analog and Digital Signal

The entire world is full of signals, both natural and artificial. Signals can be analog or digital. Figure 7 illustrates an analog signal. The term analog signal refers to signal that is continuous and takes continuous value. Most phenomenon's in the world today are analog. There are an infinite amount of colours to paint an object (even if the difference is indiscernible to the eye), it is possible for us to hear different sounds and also smell different odours. The common theme among all of these analog signals is their infinite possibilities.

An analog signal is time-varying and generally bound to a range (e.g. +12V to -12V), but there is an infinite number of values within that continuous range. An analog signal uses a given property of the medium to convey the signal's information, such as electricity moving through a wire. In an electrical signal, the voltage, current, or frequency of the signal may be varied to represent the information.

Analog signals are often calculated responses to changes in light, sound, temperature, position, pressure, or other physical phenomena. When plotted on a voltage vs. time graph, an analog signal should produce a smooth and continuous curve. There should not be any discrete value changes (see Figure 7).

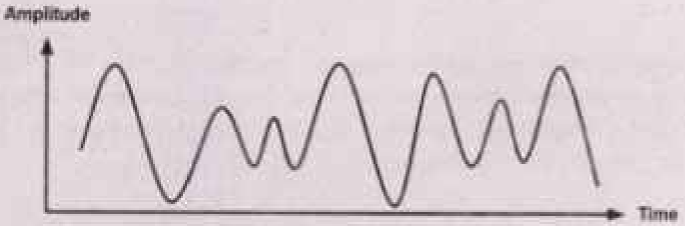


Fig. 7: Typical Analog signal

Figure 7 shows a typical representation of analog signal. Because the signal varies with time, time is plotted on horizontal (x-axis), and voltage on the vertical (y-axis). While this signals may be limited to a range of maximum and minimum values. There are still an infinite number of possible values within that range. For example the analog voltage that light the bulbs is clamped between -220V and +220V, but as you increase the resolution more and more, you discover an infinite number of values that the signal can be. For example, pure audio signals are analog.

The signal that comes out of a microphone is full of analog frequencies and harmonics, which combine to beautiful music. A digital signal is a physical signal that is a representation of a sequence of discrete values.

Digital Signal

A digital signal is a signal that represents data as a sequence of discrete values. A digital signal can only take on one value from a finite set of possible values at a given time. With digital signals, the physical quantity representing the information can be many things:

- Variable electric current or voltage
- Phase or polarization of an electromagnetic field
- Acoustic pressure
- The magnetization of a magnetic storage media

Digital signals are used in all digital electronics, including computing equipment and data transmission devices. When plotted on a voltage vs. time graph, digital signals are one of two values, and are usually between 0V and VCC (usually 1.8V, 3.3V, or 5V) (see Figure 8).

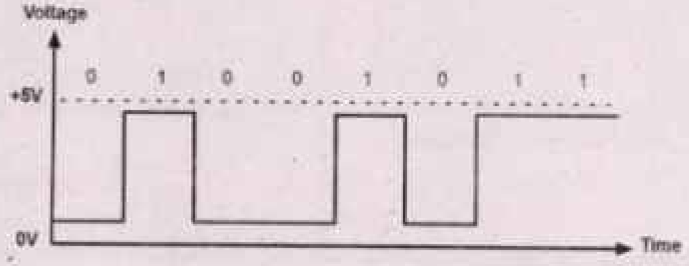


Fig. 8. Typical Digital Signal

Data Communication

Data communication refers to the movement of encoded information from one point to another by means of electronic transmission system. It can also be defined as the exchange of data between two devices via some form of transmission medium which can be wired or wireless. Another definition for data communications simply mean the transferring of digital information (usually in binary form) between two or more points (terminals). At both the source and destination, data are in digital form; however, during transmission, they can be in digital or analog form Information is carried by signal, which is a physical quantity that changes with time.

The signal can be a voltage proportional to the amplitude of the voice like in simple telephone, a sequence of pulses of light in an optical fiber, or a radio-electric wave radiated by an antenna. The fundamental purpose of data communication is to exchange information which is done by following certain rules and regulations called protocols and standards. Communications between devices are justified for the following reasons: i.Reduces time and effort required to performbusiness taskii.Captures business data at its sourceiii.Centralizes control over business dataiv.Effect rapid dissemination of informationv.Reduces current and future cost of doing businessvi.Supports expansion of business capacity atreasonably incremental cost as the organizationvii.Supports organization□s objective in centralizingcomputer systemviii. Supports improved management control of anorganization.

As a rule, the maximum permissible transmission rate of a message is directly proportional to signal power and inversely proportional to channel noise. It is the aim of any communications system to provide the highest possible transmission rate at the lowest possible power and with the least possible noise.

Communication uses electronic circuits to transmit, process, and receive information between two or more locations. The elementary components of a communication system comprise a source, a communication medium or channel, a destination and noise. Information is transferred into the system in analog or digital form. It is then processed and decoded by the receiver

Information needs to be converted into digital form before it can be transmitted electronically. A signal is that information which has been converted into a digital format. Signals are divided into two forms; Analog signals and Digital signals.

The signals have continuous variations of voltage and current. For instance, human voice is an analog signal. The signals that are transmitted via discreet stepwise values such as 0 and 1 are digital signal. Proper modulation scheme is required to transmit various signals through a media. Modulation refers to the act of accumulation of information to an electronic or optical waveform. The information may be added by modifying the amplitude, frequency and phase of the waveform.

Modulation is required because most of the time information is produced and transferred via signals having low frequencies. A low frequency signal is highly susceptible to attenuation and therefore it cannot be transferred to long distant locations. In order to resolve this problem, the original carrier wave having a low frequency is superimposed upon a high-frequency carrier wave. The modulation process is also needed to reduce the quantity of noise present in the communication band. There are two types of modulation analog and digital. Analog modulation deals with the voice, video and regular waves of base band signals, whereas digital modulations are with bit streams or symbols from computing devices as base band

Notes

signals. Analog modulation is the process of transferring analog low frequency baseband signal, like an audio or TV signal over a higher frequency carrier signal.

Baseband signal is always analog for this modulation. There are three properties of a carrier signal amplitude, frequency and phase. The three basic types of analog modulations are Amplitude Modulation (AM), Frequency Modulation (FM), Phase modulation (PM).

Digital modulation is similar to the analog modulation except base band signal is of discrete amplitude level. For binary signal it has only two level, either high or logic 1 or low or logic 0. The three types of modulation schemes are Amplitude shift Key (ASK), Frequency shift key (FSK), Phase shift key (PSK) [3].

What is modulation?

Modulation is the process of converting data into radio waves by adding information to an electronic or optical carrier signal. A carrier signal is one with a steady waveform – constant height, or amplitude, and frequency.

How modulation works

Information can be added to the carrier by varying its amplitude, frequency, phase, polarization —for optical signals— and even quantum-level phenomena like spin.

Modulation is usually applied to electromagnetic signals: radio waves, lasers/optics and computer networks. Modulation can even be applied to a direct current—which can be treated as a degenerate carrier wave with a fixed amplitude and frequency of 0 Hz – mainly by turning it on and off, as in Morse code telegraphy or a digital current loop interface. The special case of no carrier— a response message indicating an attached device is no longer connected to a remote system— is called baseband modulation.

Modulation can also be applied to a low-frequency alternating current – 50-60 Hz – as with powerline networking.

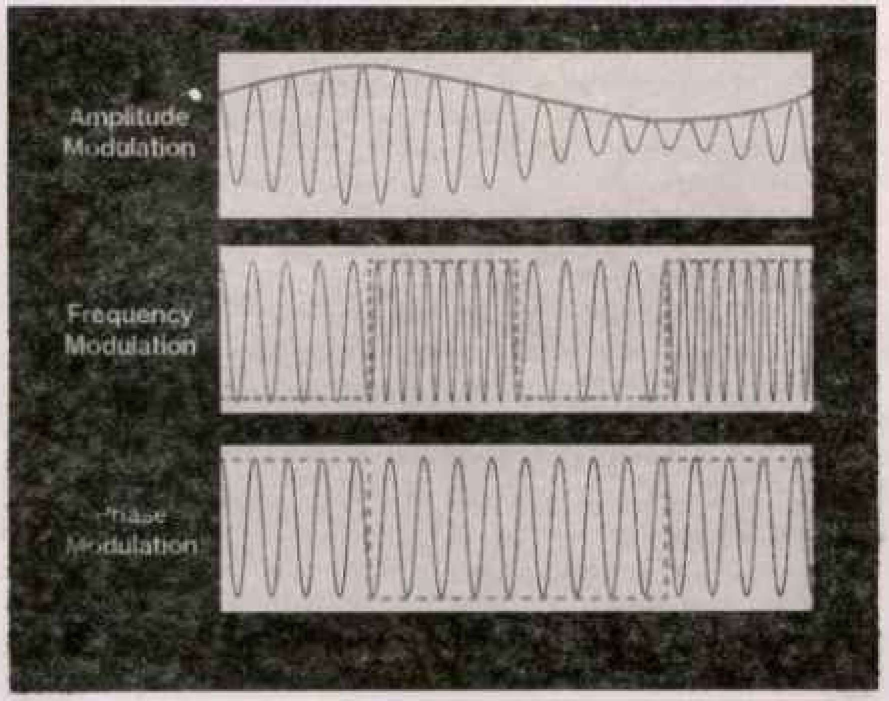
Types of modulation

Modulation Techniques are methods used to encode digital information in an analog world. Additionally, digital signals usually require an intermediate modulation step for transport across wideband, analog-oriented networks. Modulation is the process where a Radio Frequency or Light Wave's amplitude, frequency, or phase is changed in order to transmit intelligence. Digital information changes the carrier signal by modifying one or more of its characteristics (amplitude, frequency, or phase). This kind of modification is called modulation (shift keying).

There are many common modulation methods, including the following, which is an incomplete list:

A. Amplitude Modulation

AM is a type of modulation where the amplitude of the carrier signal is modulated (changed) in proportion to the message signal, while the frequency and phase are kept constant.



B. Frequency Modulation

FM is a type of modulation where the frequency of the carrier signal is modulated (changed) in proportion to the message signal while the amplitude and phase are kept constant.

C. Phase Modulation

PM is a type of modulation where the phase of the carrier signal is varied accordance to the low frequency of the message signal is known as phase modulation.

D. Amplitude-shift keying

It is a form of modulation that represents digital data as variations in the amplitude of a carrier wave. The amplitude of an analog carrier signal varies in accordance with the bit stream (modulating signal), keeping frequency and phase constant. This digital modulation scheme is used to transmit digital data over optical fiber, point to point military communication

E. Phase-shift keying

It is a digital modulation scheme that conveys data by changing, or modulating, the phase of a reference signal (the carrier wave). PSK uses a finite number of phases; each assigned a unique pattern of binary bits. Usually, each phase encode an equal number of bits. The simplest form of PSK is binary phase shift keying (BPSK).

F. Frequency-shift keying

It 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 couple of discrete frequencies to transmit binary (0s and 1s) information. The input message signal is multiplied with the carrier signal are given to the modulator It is very much important to retrieve the originally transmitted signal at the receiver side, for which a demodulator and some filter are required. Demodulation reverses modulation. It takes a modulated signal and extracts the original message out of it.

1.14 HAMMING CODE

Hamming code is an example of a block code. The two simultaneous bit errors are detected, and single-bit errors are corrected by this code. In the hamming coding mechanism, the sender encodes the message by adding the unessential bits in the data. These bits are added to the specific position in the message because they are the extra bits for correction.

Hamming code is an error-correcting code used for correcting transmission errors in synchronous data streams. The Hamming code will correct only single-bit errors. It cannot correct mulitple-bit errors. Hamming bits also sometimes called as error bits are inserted in to a character at random manner.

The combination of data bits (m bits) and Hamming bits(n bits) called as Hamming code (m+n bits).

To correct an error, the receiver reverses the value of the altered bit. To do so, it must know which bit is in error.

Number of redundancy bits (Hamming bits) 'n' needed:

- Let data bits = m
- Redundancy bits = n
- Total message sent = m+n

The value of 'n' must satisfy the following relation:

$$2^n \geq m+n+1$$

SUMMARY

- Data communication refers to the movement of encoded information from one point to another by means of electronic transmission system. It can also be defined as the exchange of data between two devices via some form of transmission medium which can be wired or wireless.
- Another definition for data communications simply mean the transferring of digital information (usually in binary form) between two or more points (terminals). At both the source and destination, data are in digital form; however, during transmission, they can be in digital or analog form Information is carried by signal, which is a physical quantity that changes with time.
- Communication facilities have an ancient history, but we tend to think of the advent

of the telegraph and later the telephone as the beginning of modern communications. Extensive telegraph and telephone networks were established all over the world, decades before the emergence of computers.

- Data communication equipment (DCE) is the hardware devices that can be used to establish, maintain and terminate communication between a data source and its destination. Data communications equipment is most used to perform signal exchange, coding and line clocking tasks as part of intermediate equipment or DTE. A typical example of data communication equipment is the modem.
- The basic concept behind data communication and network is for the two or more computer or electronic devices to see each other and share resources. For that to be archived there must be a program or software responsible for the communication to take place. The software in this case is refers to as data communication software. Data communication Software is basically a computer program that.
- It is a computer program required on DTE (PC) to bridge the gap and interpret the bits/bytes that are transmitted via the communication media through the interface.
- The Core of Data Communication is Communication Software without software, Data communication is incomplete. Communication Software is responsible for controlling data formatting, data transmission, and total communication control. It may completely resides on central PC or part of it may be located on the front end communication PC, a concentrator, remote concentrator or in intelligent terminals.
- Types of Transmission Mode and Data Flow Transmission mode is of three types.
- In simplex mode, the communication is unidirectional, as on a one-way street. Only one of the two devices on a link can transmit; the other can only receive. Keyboards and traditional monitors are examples of simplex devices. The keyboard can only introduce input; the monitor can only accept output.
- In half-duplex mode, each station can both transmit and receive, but not at the same time. When one device is sending, the other can only receive, and vice versa. The half-duplex mode is like a one-lane road with traffic allowed in both directions.
- In full-duplex mode, both stations can transmit and receive simultaneously. The full-duplex mode is like a two way street with traffic flowing in both directions at the same time.

KEY WORDS

- ACD (Automatic Call Distributor) - A switching system which automatically distributes incoming calls in the sequences they are received to a centralized group of receivers without human interface. If no receivers are available, the calls will be held until one becomes free.
- ACK - This is a control character found in bisync protocol. When combined with NAK, the ACK character would indicate that the previously transmit ted data block was correctly received (acknowledge) or incorrectly received (NAK-Negative Acknowledge).

- Analog, Analog data - Any data in the form of continuously variable physical qualities, which are "analogous" to the data source. Continuously variable as opposed to discretely variable. Contrast with digital data.
- **Analog loopback:** A diagnostic test that forms the loop at the modem 's telco line interface to isolate faults to the analog signal.
- **ANSI (American National Standards Institute)**: A voluntary organization that represents the USA in the ISO, and is responsible for defining ASCII. Members include manufacturers, common carriers, and other standards organizations such as the IEEE.

REVIEW QUESTIONS

1. Define data and Data Communication.
2. Compare analog and digital data
3. What is hamming codes?
4. List and explain components of data communicationsystem.
5. Define and gives example of basic components of data communication network.
6. What is digital data rate?
7. What are the features of error detection and error correction?
8. What are the types of signals?
9. Define Data communication equipment and dataterminal equipment. Give at least two examples in

FURTHER READINGS

1. Kurose James F., Ross Keith W. Computer Networking – By Pearson.
2. https://www.javatpoint.com/error-detection-and-correction-code-in-digital-electronics

Unit 2

LAN Topology

Notes

Structure

2.0 LEARNING OBJECTIVES

After reading this chapter students will be able to:

- know about the lan topologies
- discuss workstations, server, cables and types of ethernet
- understand broadband and base-band
- describe the network and accessories.

2.1 INTRODUCTION

A computer network is a set of devices connected through links. A node can be computer, printer, or any other device capable of sending or receiving the data. The links connecting the nodes are known as communication channels. It is interconnectivity of two or more computer system for purpose of sharing data. A computer network is a communication

Notes

system much like a telephone system, any connected device can use the network to send and receive information. In essence a computer network consists of two or more computers connected to each other so that they can share resources. Networking arose from the need to share resources in a timely fashion.

Sharing expensive peripherals is often promoted as the primary reason to network. But this is not a sufficient reason. In considering the cost benefits of sharing, we find some impressive arguments against networking. With today more affordable technology, we can easily dedicate inexpensive peripherals and not bother with a network. Desktops and laptops are getting less expensive as their capacities increase. As a result the local hard disk is becoming common place and is frequently dedicated to a local desktop or laptop. Flash drives and external hard disks now has enough storage for uses.

Following are the advantages of Distributed processing:

- Security: It provides limited interaction that a user can have with the entire system. For example, a bank allows the users to access their own accounts through an ATM without allowing them to access the bank's entire database.
- Faster problem solving: Multiple computers can solve the problem faster than a single machine working alone.
- Security through redundancy: Multiple computers running the same program at the same time can provide the security through redundancy. For example, if four computers run the same program and any computer has a hardware error, then other computers can override it.

2.2 WHY COMPUTER NETWORKING

These are serious considerations but only part of the picture. When viewed as a system, networking has some powerful arguments in its favor. In most cases organizations with multiple computer systems should network them for the following reasons:

1. Sharing of peripherals can be justified as a "shared resource", with the result that speed and quality are improved and Mean Time Between Failure (MTBF) is increased. Sharing in a properly designed network improves the reliability of the entire system. When a device fails, another one is ready to fill the void while repairs are being made.
2. Better response time can be achieved through networking. The speed with which a request is answered is a crucial factor in computing. After all, most jobs performed by a computer can be done with pencil and paper. When you buy a computer, you are buying speed more than capability. Better response time through networking is in no way guarantee. In fact, inefficient use of the network will quickly result in unacceptably poor response. The elements needed for superior performance, however, are part of most networks. If properly implemented, a computer network will be more efficient that stand-alone computers or network terminals and will equal or surpass stand-alone computer performance.
3. The peripherals attached to a network tend to be faster than those dedicated to stand-alone computers. The bandwidth of all the local area network far exceeds the speed capability

of a stand-alone computer. For many applications the computer, not the network, is the bottleneck. But since a local area network is by definition a multiple processor system, the possibility exists for sharing the processing load across several microprocessors, which is similar to parallel processing. You may not be able to speed up the computer itself, but you can speed up the results.

4. Often overlooked in an evaluation of networking is its organization benefit. Departments, companies, corporations, and institutions are all organizations, which imply interaction and team work. Without networking, the personal computer has been a powerful but isolated device. Its output has been difficult to integrate into the organization mainstream, so its value has been limited. In some instances the isolated personal computer has even created serious threats of data loss.

Networking is a communications mechanism that ties the isolated computer systems into the organization. In a networking environment, being able to communicate and share data encourages continuity and compatibility so that administrative chores can be systematized.

For example, the task of backing up the data can be assigned to a particular individual, rather than left as an afterthought to each employee.

2.3 NETWORK TOPOLOGIES

Network topology is the arrangement of the elements (links, nodes, etc.) of a communication network. It can be used to define or describe the arrangement of various types of telecommunication networks, including command and control radio networks, industrial fieldbusses and computer networks. It is the topological structure of a network and may be depicted physically or logically. It is an application of graph theory wherein communicating devices are modeled as nodes and the connections between the devices are modeled as links or lines between the nodes.

·Physical topology is the placement of the various components of a network (e.g., device location and cable installation), while logical topology illustrates how data flows within a network. Distances between nodes, physical interconnections, transmission rates, or signal types may differ between two different networks, yet their logical topologies may be identical. A network's physical topology is a particular concern of the physical layer of the OSI model.

Examples of network topologies are found in local area networks (LAN), a common computer network installation. Any given node in the LAN has one or more physical links to other devices in the network; graphically mapping these links results in a geometric shape that can be used to describe the physical topology of the network.

A wide variety of physical topologies have been used in LANs, including ring, bus, mesh and star. Conversely, mapping the data flow between the components determines the logical topology of the network. In comparison, Controller Area Networks, common in vehicles, are primarily distributed control system networks of one or more controllers interconnected with sensors and actuators over, invariably, a physical bus topology.

Two basic categories of network topologies exist, physical topologies and logical topologies. The transmission medium layout used to link devices is the physical topology of the network. For conductive or fiber optical mediums, this refers to the layout of cabling, the locations of nodes, and the links between the nodes and the cabling. The physical topology of a network is determined by the capabilities of the network access devices and media, the level of control or fault tolerance desired, and the cost associated with cabling or telecommunication circuits.

Topologies

In contrast, logical topology is the way that the signals act on the network media,[6] or the way that the data passes through the network from one device to the next without regard to the physical interconnection of the devices. A network's logical topology is not necessarily the same as its physical topology.

For example, the original twisted pair Ethernet using repeater hubs was a logical bus topology carried on a physical star topology. Token Ring is a logical ring topology, but is wired as a physical star from the media access unit.

Physically, AFDX can be a cascaded star topology of multiple dual redundant Ethernet switches; however, the AFDX Virtual links are modeled as time-switched single-transmitter bus connections, thus following the safety model of a single-transmitter bus topology previously used in aircraft. Logical topologies are often closely associated with media access control methods and protocols. Some networks are able to dynamically change their logical topology through configuration changes to their routers and switches.

Links

The transmission media (often referred to in the literature as the physical media) used to link devices to form a computer network include electrical cables (Ethernet, HomePNA, power line communication, G.hn), optical fiber (fiber-optic communication), and radio waves (wireless networking). In the OSI model, these are defined at layers 1 and 2 — the physical layer and the data link layer.

A widely adopted family of transmission media used in local area network (LAN) technology is collectively known as Ethernet. The media and protocol standards that enable communication between networked devices over Ethernet are defined by IEEE 802.3. Ethernet transmits data over both copper and fiber cables. Wireless LAN standards (e.g. those defined by IEEE 802.11) use radio waves, or others use infrared signals as a transmission medium. Power line communication uses a building's power cabling to transmit data.

2.4 WORKSTATIONS

A workstation refers to an individual computer, or group of computers, used by a single user to perform work. For example, a "workstation" may be an average-powered computer connected to a larger network. It can also refer to a powerful computer intended for serious academic or professional computation.

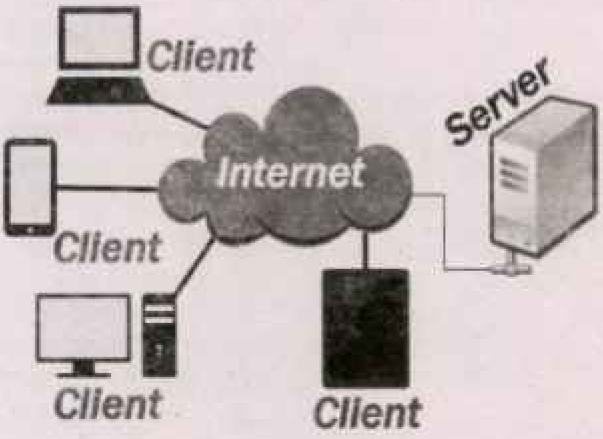
Workstation is a high-performance computer system that is basically designed for a single user and has advanced graphics capabilities, large storage capacity, and a powerful central processing unit. A workstation is more capable than a personal computer (PC) but is less advanced than a server (which can manage a large network of peripheral PCs or workstations and handle immense data-processing and reporting tasks). The term workstation was also sometimes ascribed to dumb terminals (i.e., those without any processing capacity) that were connected to mainframe computers.

Their raw processing power allows high-end workstations to accommodate high-resolution or three-dimensional graphic interfaces, sophisticated multitask software, and advanced abilities to communicate with other computers.

Workstations are used primarily to perform computationally intensive scientific and engineering tasks. They have also found favour in some complex financial and business applications. In addition, high-end workstations often serve a network of attached "client" PCs, which use resident tools and applications to access and manipulate data stored on the workstation.

2.5 SERVER

A server is a machine or computer program that provides data or functionality for other machines or programs. We call the other devices or programs 'clients.' Most commonly, the term refers to a computer that provides data to other computers. The data may be served to systems on a wide area network (WAN) over the Internet. Alternatively, it may serve the data to LAN systems. LAN stands for local area network.



Servers are the lifeblood of any network. They provide the shared resources that the network users need, such as e-mail, Web services, databases, file storage, etc. In computing, a server is a computer program or a device that provides functionality for called clients which are other programs or devices. This architecture is called the client-server model. A single overall computation is distributed across multiple processes or devices.

Servers can provide various functionalities called services. These services include sharing data or resources among multiple clients, or performing computation for a client. Multiple clients can be served by a single server, and a single client can use multiple servers. A client process may run on the same device. It can also connect over a network to a server to run on a different device.

Notes

Example of servers may include database servers, mail servers, print servers, file servers, web servers, application servers, and game servers.

Most frequently client-server systems are implemented by the request-response model., i.e., a client sends a request to the server. In this model server performs some action and sends a response back to the client, typically with a result or acknowledgement. Designating a computer as server-class hardware means that it is specialized for running servers on it. This implies that it is more powerful and reliable than standard personal computers. But large computing clusters may be composed of many relatively simple, replaceable server components.

Server vs. client

In the world of computers, clients and servers are computers that we use for different purposes.

Clients

Clients are computers or software that access a service that servers provide. In most cases, servers are located on separate computers. Clients access servers through networks.

Client-server networks are computer networks that use a dedicated computer (server) to store data, manage/provide resources and control user access. The server acts as a central point on the network upon which the other computers connect to. A computer that connects to the server is called a client. A client-server network is usually preferred over a peer-to-peer network that doesn't have a central server to manage the network.

Servers

Servers are computers that run services to serve the needs of other computers. There are, for example, home media servers, web servers, and print servers. There are also file servers and database servers.

One company employee, for example, may log in to the client computer to access the files and applications that the server runs. We call this two-tier architecture a client-server architecture.

Servers vs. hosts

In computing, hosts are computers that connect to a network. Servers, on the other hand, are hardware devices or software that provide services to other computers or programs within networks.

Software includes all the programs, i.e., instructions and codes within a computer. The computer itself - the physical components of any device - is the hardware.

Every computer that is connected to a network acts as a host to other peers on the same network.

"A host is a computer, connected to other computers for which it provides data or services over a network. In theory, every computer connected to a network acts as a host to other peers on the network. In essence, a host reflects the logical relationship of two or more computers on a network."

Network Server Functions

A client-server network may have more than one server, each dedicated to handling a specific function.

Functions may include:

- Data storage
- Handling security
- Hosting shared applications
- Managing an internet connection
- Scheduling and running backups
- Email services
- Print jobs
- Domain name services
- Storing usernames and passwords to control access
- Assigning levels of access to resources
- Monitoring network traffic

Benefits of a client-server network

- Generally more secure than peer-to-peer networks
- One client computer crashing does not effect the other computers
- Easier to recover files as backups can be controlled centrally by the network administrator
- Files and resources are easier to share and control from server
- Improved levels of security as files are centralised
- It's easier to administrate the whole network using a server
- Faster performance as each computer is only fulfilling one role
- Security is potentially cheaper and easier when done centrally
- Individual users do not have to worry about backups or security
- Larger networks can be created

Drawbacks of a Client-server Network

- Servers can be expensive to buy and maintain
- A network technician will often be required

- Trickier to set up with specialist knowledge needed
- Over-all set up cost is more expensive than a peer-to-peer network
- Server failure will probably disrupt all computers on the network

2.6 TYPES OF SERVERS AND THEIR APPLICATIONS

Application Server

These servers hosts web apps (computer programs that run inside a web browser) allowing users in the network to run and use them preventing the installation a copy on their own computers. These servers need not be part of the World Wide Web. There clients are computers with a web browser.

Catalog Server

These servers maintains an index or table of contents of information that can be found across a large distributed network. Distributed network may include computers, users, files shared on file servers, and web apps. Examples of catalog servers are Directory servers and name servers. Their clients are any computer program that needs to find something on the network. Example can be a Domain member attempting to log in, an email client looking for an email address, or a user looking for a file

Communications Server

These servers maintains an environment needed for one communication endpoint to find other endpoints and then communicates with them. These servers may or may not include a directory of communication endpoints and a presence detection service, depending on the openness and security parameters of the network. Their clients are communication endpoints.

Computing Server

These servers share vast amounts of computing resources which include CPU and random-access memory over a network. Any computer program that needs more CPU power and RAM than a personal computer can probably afford can use these types of servers. The client must be a networked computer to implement the client-server model which is necessity.

Database Server

These servers maintains and shares any form of database over a network. A database is a organized collections of data with predefined properties that may be displayed in a table. Clients of these servers are spreadsheets, accounting software, asset management software or virtually any computer program that consumes well-organized data, especially in large volumes.

Fax Server

These servers share one or more fax machines over a network which eliminates the hassle of physical access. Any fax sender or recipient are the clients of these servers.

File Server

Shares files and folders, storage space to hold files and folders, or both, over a network Networked computers are the intended clients, even though local programs can be clients

Game Server

These servers enables several computers or gaming devices to play multiplayer games. Personal computers or gaming consoles are their clients.

Mail Server

These servers makes email communication possible in the same way as a post office makes snail mail communication possible. Clients of these servers are senders and recipients of email

Print Server

These servers share one or more printers over a network which eliminates the hassle of physical access. Their clients are computers in need of printing something.

Proxy Server

This server acts as an intermediary between a client and a server accepting incoming traffic from the client and sending it to the server. Reasons to use a proxy server includes content control and filtering, improving traffic performance, preventing unauthorized network access or simply routing the traffic over a large and complex network. There clients are any networked computer.

Web Server

These servers hosts web pages. A web server is responsible for making the World Wide Web possible. Each website has one or more web servers. There clients are computers with a web browser.

2.7 CABLES

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.

The following sections discuss the types of cables used in networks and other related topics.

- Unshielded Twisted Pair (UTP) Cable
- Shielded Twisted Pair (STP) Cable
- Coaxial Cable
- Fiber Optic Cable
- Cable Installation Guides
- Wireless LANs

Unshielded Twisted Pair (UTP) Cable

Twisted pair cabling comes in two varieties: shielded and unshielded. Unshielded twisted pair (UTP) is the most popular and is generally the best option for school networks (See fig. 1).

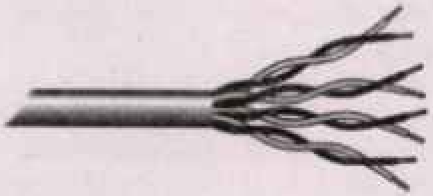


Fig. 1. Unshielded twisted pair

The quality of UTP may vary from telephone-grade wire to extremely high-speed cable. The cable has four pairs of wires inside the jacket. Each pair is twisted with a different number of twists per inch to help eliminate interference from adjacent pairs and other electrical devices. The tighter the twisting, the higher the supported transmission rate and the greater the cost per foot. The EIA/TIA (Electronic Industry Association/Telecommunication Industry Association) has established standards of UTP and rated six categories of wire (additional categories are emerging).

Categories of Unshielded Twisted Pair

Category	*Speed*	*Use*
1	1 Mbps	Voice Only (Telephone Wire)
2	4 Mbps	LocalTalk & Telephone (Rarely used)
3	16 Mbps	10BaseT Ethernet
4	20 Mbps	Token Ring (Rarely used)
5	100 Mbps (2 pair) 1000 Mbps (4 pair)	100BaseT Ethernet Gigabit Ethernet
5e	1,000 Mbps	Gigabit Ethernet
6	10,000 Mbps	Gigabit Ethernet

Unshielded Twisted Pair Connector

The standard connector for unshielded twisted pair cabling is an RJ-45 connector. This is a plastic connector that looks like a large telephone-style connector (See fig. 2). A slot allows the RJ-45 to be inserted only one way.

RJ stands for Registered Jack, implying that the connector follows a standard borrowed from the telephone industry. This standard designates which wire goes with each pin inside the connector.

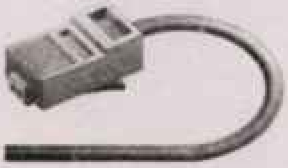


Fig. 2. RJ-45 connector

Shielded Twisted Pair (STP) Cable

Although UTP cable is the least expensive cable, it may be susceptible to radio and electrical frequency interference (it should not be too close to electric motors, fluorescent lights, etc.). If you must place cable in environments with lots of potential interference, or if you must place cable in extremely sensitive environments that may be susceptible to the electrical current in the UTP, shielded twisted pair may be the solution. Shielded cables can also help to extend the maximum distance of the cables.

- Shielded twisted pair cable is available in three different configurations:
- Each pair of wires is individually shielded with foil.
- There is a foil or braid shield inside the jacket covering all wires (as a group).
- There is a shield around each individual pair, as well as around the entire group of wires (referred to as double shield twisted pair).

Coaxial Cable

Coaxial cabling has a single copper conductor at its center. A plastic layer provides insulation between the center conductor and a braided metal shield (See fig. 3). The metal shield helps to block any outside interference from fluorescent lights, motors, and other computers.

Fig. 3. Coaxial cable

Although coaxial cabling is difficult to install, it is highly resistant to signal interference. In addition, it can support greater cable lengths between network devices than twisted pair cable. The two types of coaxial cabling are thick coaxial and thin coaxial.

Thin coaxial cable is also referred to as thinnet. 10Base2 refers to the specifications for thin coaxial cable carrying Ethernet signals. The 2 refers to the approximate maximum segment length being 200 meters. In actual fact the maximum segment length is 185 meters. Thin coaxial cable has been popular in school networks, especially linear bus networks.

Thick coaxial cable is also referred to as thicknet. 10Base5 refers to the specifications for thick coaxial cable carrying Ethernet signals. The 5 refers to the maximum segment length being 500 meters. Thick coaxial cable has an extra protective plastic cover that helps keep moisture away from the center conductor. This makes thick coaxial a great choice when running longer lengths in a linear bus network. One disadvantage of thick coaxial is that it does not bend easily and is difficult to install.

Coaxial Cable Connectors

The most common type of connector used with coaxial cables is the Bayone-Neill-Concelman (BNC) connector (See fig. 4). Different types of adapters are available for BNC connectors, including a T-connector, barrel connector, and terminator. Connectors on the cable are the weakest points in any network. To help avoid problems with your network, always use the BNC connectors that crimp, rather screw, onto the cable.

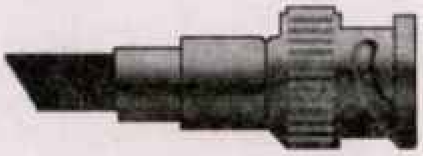


Fig. 4. BNC connector

Fiber Optic Cable

Fiber optic cabling consists of a center glass core surrounded by several layers of protective materials (See fig. 5). It transmits light rather than electronic signals eliminating the problem of electrical interference. This makes it ideal for certain environments that contain a large amount of electrical interference. It has also made it the standard for connecting networks between buildings, due to its immunity to the effects of moisture and lighting.

Fiber optic cable has the ability to transmit signals over much longer distances than coaxial and twisted pair. It also has the capability to carry information at vastly greater speeds. This capacity broadens communication possibilities to include services such as video conferencing and interactive services. The cost of fiber optic cabling is comparable to copper cabling; however, it is more difficult to install and modify. 10BaseF refers to the specifications for fiber optic cable carrying Ethernet signals.

The center core of fiber cables is made from glass or plastic fibers (see fig 5). A plastic coating then cushions the fiber center, and kevlar fibers help to strengthen the cables and prevent breakage. The outer insulating jacket made of teflon or PVC.

Fig. 5. Fiber optic cable

There are two common types of fiber cables – single mode and multimode. Multimode cable has a larger diameter; however, both cables provide high bandwidth at high speeds. Single mode can provide more distance, but it is more expensive.

2.8 TYPES OF ETHERNET

Ethernet is primarily a standard communication protocol used to create local area networks. It transmits and receives data through cables. This facilitates network communication between two or more different types of network cables such as from copper to fiber optic and vice versa.

In short, an Ethernet media converter is a device that is able to support communications between two different types of network media. The media converter consists of a circuit card within a case. The card typically has 2 ports to connect two differing types of network cables. This post will attempt to answer any questions you might have regarding the functionality of fiber media converters and Ethernet networks.

Ethernet Network

As mentioned, Ethernet network is used to create local area network and connect multiple computers or other devices such as printers, scanners, and so on. In a wired network, this is done with the help of fiber optic cables, while in a wireless network, it is done through wireless network technology. An Ethernet network uses various topologies such as star, bus, ring, and more.

Various Types of Ethernet Networks

Fiber optic media converters connect an Ethernet device with CAT5/CAT6 copper cables to a fiber optic cable. An Ethernet network usually is active in a 10-km periphery. This extension to fiber optic cable significantly increases the distance covered by the network. Here are some types of Ethernet networks:

- **Fast Ethernet:** As the term suggests, this is quite a high-speed internet, and can transmit or receive data at about 100 Mbps. This type of network is usually supported by a twisted pair or CAT5 cable. If a laptop, camera, or any other device is connected to a network, they operate at 10/100Base Ethernet and 100Base on the fiber side of the link.
- **Gigabit Ethernet:** This type of network transfers data at an even higher speed of about 1000 Mbps or 1Gbps. Gigabit speed is an upgrade from Fast Ethernet which is slowly being phased out. In this type of network, all the four pairs in the twisted pair cable contribute to the data transfer speed. This network type finds a large application in video calling systems which use CAT5e or other advanced cables. For extended networks, the distance of up to 500m, 1000Base SX fiber cables may be used for multimode, as well as 1000Base LX for single mode systems. VERSITRON manufactures Gigabit Ethernet Media Converters that can handle 10/100/1000Base speeds on the Ethernet side and 1000Base Gigabit speed on the fiber side by using Fiber SFP modules.
- **10-Gigabit Ethernet:** This is an even more advanced and high speed network type with a data transfer rate of 10 Gigabit/second. It is supported by CAT6a or CAT7

twisted pair cables, as well as fiber optic cables. By using a fiber optic cable, this network area can be extended up to around 10,000 meters.

- **Switch Ethernet:** This type of network requires a switch or hub. Also, instead of a twisted pair cable, a normal network cable is used in this case. Network switches are used for data transfer from one device to the other, without interrupting any other devices in the network.

Ethernet may be either a wired or wireless network. In a wired network, various types of cables are used. Here are some widely used Ethernet cables:

- 10Base2: This is a thin twisted pair coaxial cable.
- 10Base5: This is thick twisted pair coaxial cables.
- 10Base T: This is a twisted pair cable which offers a speed of around 10 Mbps.
- 100BaseTX: This is a twisted pair cable and offer a speed of 100 Mbps.
- 100Base FX: Fiber optic protocol which offers a speed of 100 Mbps.
- 1000Base SX: Fiber optic protocol which utilizes a wavelength of 850 nm for multimode networks.
- 1000Base LX: Fiber optic protocol which utilizes a wavelength of 1310 nm, for multimode networks and up to 1550 nm for singlemode networks.

Advantages of Ethernet Media Converters

- Ethernet media converters can be installed as standalone or rack mountable in a media converter chassis, and can be placed in cramped areas, as they are quite small and compact.
- They can also be easily wall mounted or DIN rail mounted in industrial applications.
- Allow a user to transmit data over distances up to 100km by using fiber optic conversion
- They can be used to convert any IP device such as a camera to fiber optic.
- For optimal use of your network and increasing your speed of communication, you can opt for a top quality Ethernet Media converter manufactured by VERSITRON.

We supply Media Converters to military, government, and commercial end users worldwide. VERSITRON works closely with each customer to ensure that the most practical and cost effective solution is utilized for any specific application. Click RFQ to know the fiber media converter price from our product range.

2.9 BROADBAND AND BASEBAND

Baseband refers to a single-channel digital system and that single channel is used to communicate with devices on a network. Broadband, on the other hand, is wide bandwidth data transmission which generates an analog carrier frequency, which carries multiple digital signals or multiple channels.

Difference between Broadband and Baseband Transmission

- Broadband system use modulation techniques to reduce the effect of noise in the environment. Broadband transmission employs multiple channel unidirectional transmission using combination of phase and amplitude modulation.
- Baseband is a digital signal is transmitted on the medium using one of the signal codes like NRZ, RZ Manchester biphase-M code etc. is called baseband transmission.

These are following differences between Broadband and Baseband transmission.

S.No.	Baseband Transmission	Broadband Transmission
1.	In baseband transmission, the type of signalling used is digital.	In broadband transmission, the type of signalling used is analog.
2.	Baseband Transmission is bidirectional in nature.	Broadband Transmission is unidirectional in nature.
3.	Signals can only travel over short distances.	Signals can be travelled over long distances without being attenuated.
4.	It works well with bus topology.	It is used with a bus as well as tree topology.
5.	In baseband transmission, Manchester and Differential Manchester encoding are used.	Only PSK encoding is used.
6.	Baseband transmission have 50 ohm impedance.	Broadband transmission have 70 ohm impedance.
7.	Baseband transmission is easy to install and maintain	Broadband transmission is difficult to install and maintain.
8.	This transmission is cheaper to design.	This transmission is expensive to design.

2.10 OPTICAL FIBERS

A fiber optic cable is a network cable that contains strands of glass fibers inside an insulated casing. They're designed for long-distance, high-performance data networking, and telecommunications. Compared to wired cables, fiber optic cables provide higher bandwidth and transmit data over longer distances. Fiber optic cables support much of the world's internet, cable television, and telephone systems.

Fiber Optic Cables Work

A fiber optic cable consists of one or more strands of glass, each only slightly thicker than a human hair. The center of each strand is called the core, which provides the pathway for light to travel. The core is surrounded by a layer of glass called cladding that reflects light inward to avoid loss of signal and allow the light to pass through bends in the cable.

The two primary types of optical fiber cables are single mode and multi-mode. Single-mode fiber uses extremely thin glass strands and a laser to generate light, while multi-mode optical fiber cables use LEDs.

Notes

Single-mode optical fiber networks often use Wave Division Multiplexing techniques to increase the amount of data traffic that the strand can carry.

WDM allows light at multiple different wavelengths to be combined (multiplexed) and later separated (de-multiplexed), effectively transmitting multiple communication streams through a single light pulse.

Advantages of Fiber Optic Cables

- Fiber cables offer several advantages over long-distance copper cabling.
- Fiber optics support a higher capacity. The amount of network bandwidth a fiber cable can carry easily exceeds that of a copper cable with similar thickness. Fiber cables rated at 10 Gbps, 40 Gbps, and 100 Gbps are standard.
- Because light can travel for much longer distances over a fiber cable without losing its strength, the need for signal boosters is lessened.
- A fiber optic cable is less susceptible to interference. A copper network cable requires shielding to protect it from electromagnetic interference. While this shielding helps, it is not sufficient to prevent interference when many cables are strung together in proximity to one another. The physical properties of fiber optic cables avoid most of these problems.
- Whereas most fiber optics are installed to support long-distance connections between cities and countries, some residential internet providers have invested in extending their fiber installations to suburban neighborhoods for direct access by households. Providers and industry professionals call these last-mile installations.

Some better-known fiber-to-the-home services in the market include Verizon FIOS and Google Fiber. These services can provide gigabit internet speeds to households. However, they typically also offer lower capacity packages to customers. Different home-consumer packages are often abbreviated with these acronyms:

- FTTP (Fiber to the Premises): Fiber that's laid all the way to the building.
- FTTB (Fiber to the Building/Business/Block): The same as FTTP.
- FTTC/N (Fiber to the Curb of Node): Fiber that is laid to the node but then copper wires complete the connection inside the building.
- Direct fiber: Fiber that leaves the central office and is attached directly to one customer. This provides the greatest bandwidth, but direct fiber is expensive.
- Shared fiber: Similar to direct fiber except that as the fiber approaches the premises of nearby customers, it splits into other optical fibers for those users.

Dark Fiber

The term dark fiber (often spelled dark fibre or called unlit fibre) most commonly refers to installed fiber optic cabling that is not currently in use. The term sometimes also refers to privately operated fiber installations.

Better depends upon your perspective. Since no electricity is involved, fiber optic internet is less likely to shut down during a power outage than other types of high-speed internet.

Along with being more reliable, fiber optic internet is also faster—and more expensive—than traditional internet cables.

Cable technology currently supports approximately 1,000 Mbps of bandwidth, while fiber optic internet supports speeds of up to 2,000 Mbps. At 1,000 Mbps, you can download a 2-hour HD movie in about 32 seconds. At 2,000 Mbps, it takes approximately 17 seconds to download a 2-hour HD movie.

2.11 NETWORK INTERFACE CARD

A network interface card (NIC) is a hardware component, typically a circuit board or chip, which is installed on a computer so it can connect to a network. Modern NICs provide functionality to computers, such as support for I/O interrupt, direct memory access (DMA) interfaces, data transmission, network traffic engineering and partitioning.

A NIC provides a computer with a dedicated, full-time connection to a network. It implements the physical layer circuitry necessary for communicating with a data link layer standard, such as Ethernet or Wi-Fi. Each card represents a device and can prepare, transmit and control the flow of data on the network.

The NIC uses the OSI model to send signals at the physical layer, transmit data packets at the network layer and operate as an interface at the TCP/IP layer.

A network interface card (NIC) is a hardware component without which a computer cannot be connected over a network. It is a circuit board installed in a computer that provides a dedicated network connection to the computer. It is also called network interface controller, network adapter or LAN adapter.

Purpose

- NIC allows both wired and wireless communications.
- NIC aiiows communications between computers connected via local area network (LAN) as well as communications over large-scale network through Internet Protocol (IP).
- NIC is both a physical layer and a data link layer device, i.e. it provides the necessary hardware circuitry so that the physical layer processes and some data link layer processes can run on it.

Types of NIC Cards

NIC cards are of two types:

Network Interface Card
Internal Network Card
External Network Card

Notes

Internal Network Cards

In internal networks cards, motherboard has a slot for the network card where it can be inserted. It requires network cables to provide network access. Internal network cards are of two types. The first type uses Peripheral Component Interconnect (PCI) connection, while the second type uses Industry Standard Architecture (ISA).

External Network Cards

In desktops and laptops that do not have an internal NIC, external NICs are used. External network cards are of two types: Wireless and USB based. Wireless network card needs to be inserted into the motherboard, however no network cable is required to connect to the network. They are useful while traveling or accessing a wireless signal.

2.12 NETWORKS AND ACCESSORIES

Components of Computer Networks

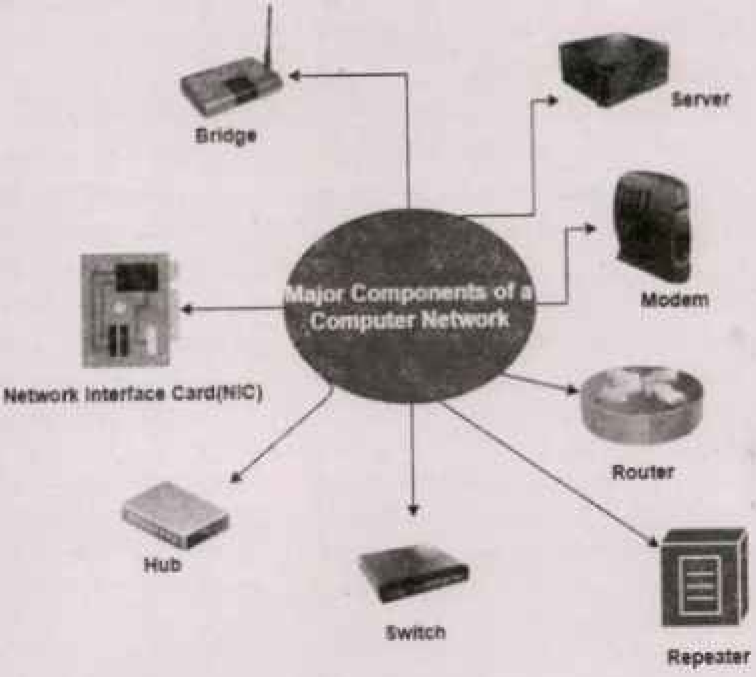
The key parts that are required to install a network are included in the components of the Computer network. From simple to complex there are numerous types of networks in Computer networks. The componects that we need to install for a network mainly depend upon the type of Network. We can also remove some network components according to our needs.

For example: In order to establish a wireless network there is no need for cables.

Given below is a list of components of a Computer Network:

- Network Interface Card(NIC)
- HUB
- Switch

- Repeater
- Router
- Modem
- Server
- Bridge


Bridge
Server
Modem
Major Components of a Computer Network
Network Interface Card(NIC)
Router
Hub
Switch
Repeater

Protocol and Standards In Networking

In computer networks, communication occurs between entities in different systems. An entity is anything capable of sending or receiving information. However, two entities cannot simply send bit streams to each other and expect to be understood. For communication to occur, the entities must agree on a protocol.

A protocol is a set of rules that govern data communications. It defines what is communicated, how it is communicated, and when it is communicated. The key elements of a protocol are syntax, semantics, and timing.

- **Syntax.** The term syntax refers to the structure or format of the data, meaning the order in which they are presented. For example, a simple protocol might expect the first 8 bits of data to be the address of the sender, the second 8 bits to be the address of the receiver, and the rest of the stream to be the message itself.
- **Semantics.** The word semantics refers to the meaning of each section of bits. How is a particular pattern to be interpreted, and what action is to be taken based on that interpretation? For example, does an address identify the route to be takenor the final destination of the message?

Notes

- **Timing.** The term timing refers to two characteristics: when data should be sent and how fast they can be sent. For example, if a sender produces data at 100 Mbps but the receiver can process data at only 1 Mbps, the transmission will overload thereceiver and some data will be lost.

Standards are essential in creating and maintaining an open and competitive market for equipment manufacturers and in guaranteeing national and international interoperability of data and telecommunications technology and processes.

Standards provide guidelines to manufacturers, vendors, government agencies, and other service providers to ensure the kind of interconnectivity necessary in today's marketplace and in international communications.

Data communication standards fall into two categories: de facto (meaning "by fact" or "by convention") and de jure (meaning "by law" or "by regulation").

- De facto. Standards that have not been approved by an organized body but have been adopted as standards through widespread use are de facto standards. De facto standards are often established originally by manufacturers who seek to define the functionality of a new product or technology.
- De jure. Those standards that have been legislated by an officially recognized body are de jure standards

Standards Organizations

Standards are developed through the cooperation of standards creation committees, forums, and government regulatory agencies.

Standards Creation Committees

While many organizations are dedicated to the establishment of standards, data telecommunications in North America rely primarily on those published by the following:

- International Organization for Standardization (ISO). The ISO is a multinational body whose membership is drawn mainly from the standards creation committees of various governments throughout the world. The ISO is active in developing cooperation in the realms of scientific, technological, and economic activity.
- International Telecommunication Union- Telecommunication Standards Sector (ITU-T). By the early 1970s, a number of countries were defining national standards for telecommunications, but there was still little international compatibility. The United Nations responded by forming, as part of its International Telecommunication Union (ITU), a committee, the Consultative Committee for International Telegraphy and Telephony (CCITT). This committee was devoted to the research and establishment of standards for telecommunications in general and for phone and data systems in particular. On March 1, 1993, the name of this committee was changed to the International Telecommunication Union Telecommunication Standards Sector (ITU-T).
- American National Standards Institute (ANSI). Despite its name, the American National Standards Institute is a completely private, nonprofit corporation not affiliated with the U.S. federal government. However, all ANSI activities are undertaken with

the welfare of the United States and its citizens occupying primary importance.

- Institute of Electrical and Electronics Engineers (IEEE). The Institute of Electrical and Electronics Engineers is the largest professional engineering society in the world. International in scope, it aims to advance theory, creativity, and product quality in the fields of electrical engineering, electronics, and radio as well as in all related branches of engineering. As one of its goals, the IEEE oversees the development and adoption of international standards for computing and communications.
- Electronic Industries Association (EIA). Aligned with ANSI, the Electronic Industries Association is a non- profit organization devoted to the promotion of electronics manufacturing concerns. Its activities include public awareness education and lobbying efforts in addition to standards development. In the field of information technology, the EIA has made significant contributions by defining physical connection interfaces and electronic signalling specifications for data communication.

Types of Network

There are several different types of computer networks. Computer networks can be characterized by their size as well as their purpose. The size of a network can be expressed by the geographic area they occupy and number of computers that are part of the network. Networks can cover anything from a handful of devices within a single room to millions of devices spread across the entire globe.

Personal Area Network

A personal area network (PAN) is the interconnection of information technology devices within the range of an individual person, typically within a range of 10 meters. For example, a person traveling with a laptop, a personal digital assistant (PDA), and a portable printer could interconnect them without having to plug anything in, using some form of wireless technology. Typically, this kind of personal area network could also be interconnected without wires to the Internet or other networks.

PANs can be used for communication among the personal devices themselves (intrapersonal communication), or for connecting to a higher level network and the Internet (an uplink). However, it is possible to have multiple individuals using this same network within a residence. If this is the case we can refer to the network as Home Area network (HAN). In this type of setup, all the devices are connected together using both wired and/ or wireless. All networked devices can be connected to a single modem as a gateway to the Internet. See figure 6.

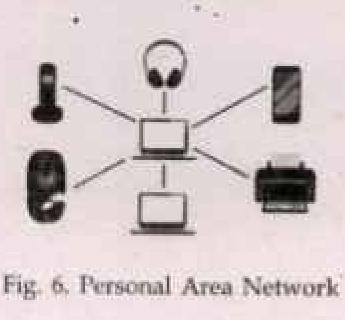


Fig. 6. Personal Area Network

Notes

Local Area Network

A local area network (LAN) is usually privately owned and links the devices in a single office, building, or campus. Depending on the needs of an organization and type of technology used, a LAN can be as simple as two desktops and a printer in someone□s home office; or it can extend throughout a company and include audio and video peripherals. Currently, LAN size is limited to a few kilometers.

In addition to the size, LANs are distinguished from other types of networks by their transmission media and topology. In general, a given LAN will use only one type of transmission medium. LANs are designed to allow resources to be shared between personal computers or workstations. Early LANs had data rates in the 4 to 16 mega-bits-per-seconds (Mbps). Today, however, speeds are normally 100Mbps or 1000Mbps. Wireless LANs (WLAN) are the newest evolution in LAN technology. See figure 7.

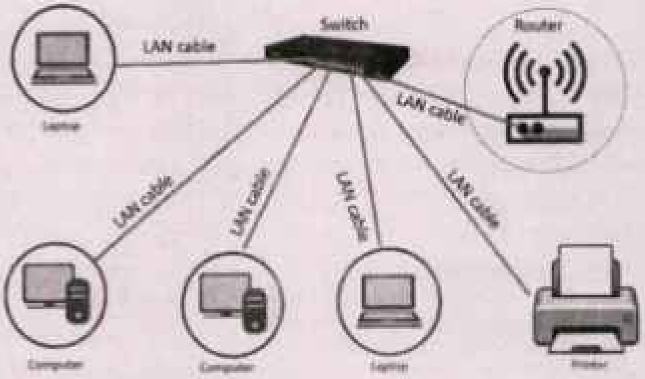


Fig. 7. Local Area Network

Metropolitan Area Network

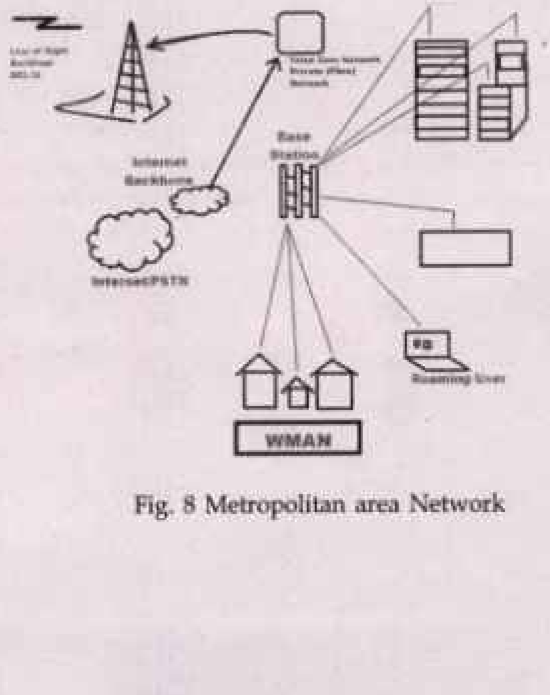


Fig. 8 Metropolitan area Network

A metropolitan area network (MAN) is a network with a size between a LAN and a WAN. It normally covers the area inside a town or a city. It is designed for customers who need a high- speed connectivity, normally to the internet, and have endpoints spread over a city or part of city. A good example of a MAN is part of the telephone company network that can provide a high-speed DSL line to the customer.

Wide Area Network

A wide area network (WAN) provides long-distance transmission of data, image, audio, and video information over large geographic areas that may comprise a country, a continent, or even the whole world. A WAN can be as complex as the backbones that connect the Internet or as simple as a dial-up line that connects a home computer to the internet.

We normally refer to the first one as a switched WAN and to the second as a point-to-point WAN.

The switched WAN connects the end systems, which usually comprise a router (internetworking connecting device) that connects to another LAN or WAN. The point-to-point WAN is normally a line leased from a telephone or cable TV provider that connects a home computer or a small LAN to an internet service provider (ISP). A good example of a switched WAN is X.25, the asynchronous transfer mode (ATM) network. See figure 9.

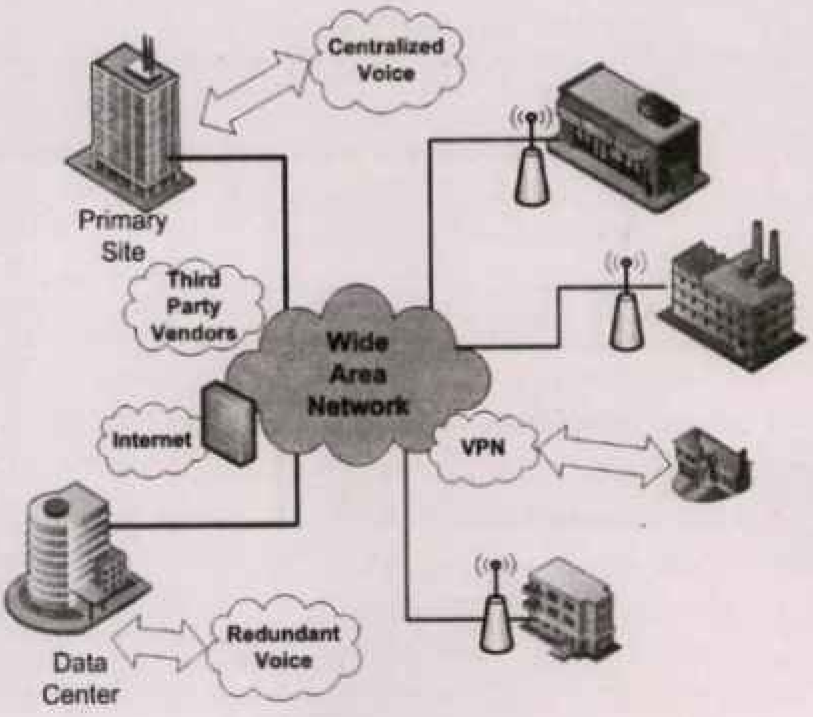


Fig. 9. Wide Area Network

Notes

Network Topologies

The term topology in computer networking refers to the way in which a network is laid out physically. Two or more devices connect to a link; two or more links form a topology. The topology of a network is the geometric representation of the relationship of all links and linking devices (usually called nodes) to one another. The cost and flexibility of a network installation are partly affected by as is system reliability. Many network topologies are commonly used, but they all have certain similarities. Information is carried either through space (wireless) or cable. The cable must control the movement of information on the network so that data can be transmitted in a reliable manner. There are four basic topologies possible: mesh, star, bus, and ring.

Bus Topology

The Bus topology consists of a single cable that runs to every work-station. See figure 10. The bus topology is also known as linear bus. In other words, all the nodes (computers and servers) are connected to the single cable (called bus), by the help of interface connectors. This central cable is the back bone of the network and every workstation communicates with the other device through this bus.

Computers on a bus topology network communicate by addressing data to a particular computer and putting that data on the cable in the form of electronic signals. To understand how computers communicate on a bus you need to be familiar with three concepts:

1. **Sending the signal:** Network data in the form of electronic signals is sent to all of the computers on the network; however, the information is accepted only by the computer whose address matches the address encoded in the original signal. Only one computer at a time can send messages.

   Because only one computer at a time can send data on a bus network, network performance is affected by the number of computers attached to the bus. The more computers on a bus, the more computers there will be waiting to put data on the bus, and the slower the network.

   There is no standard measure for the impact of numbers of computers on any given network. The amount the network slows down is not solely related to the number of computers on the network. It depends on numerous factors including:

   - Hardware capacities of computers on the network
   - Number of times computers on the network transmit data
   - Type of applications being run on the network
   - Types of cable used on the network
   - Distance between computers on the network

   The bus is a passive topology. Computers on a bus only listen for data being sent on the network. They are not responsible for moving data from one computer to the next. If one computer fails, it does not affect the rest of the network. In active topology computers regenerate signals and move data along the network.

2. **Signal Bounce:** Because the data, or electronic signal, is sent to the entire network, it will travel from one end of the cable to the other. If the signal were allowed to continue uninterrupted, it would keep bouncing back and forth along the cable and prevent other computers from sending signals. Therefore, the signal must be stopped.

   The Terminator: To stop the signal from bouncing, a component called a terminator is placed at each end of the cable to absorb free signals. Absorbing the signal clears the cable so that other computers can send data. Every cable end on the network must be plugged into something. For example, a cable end could be plugged into a computer or a connector to extend the cable length. Any open cable ends-ends not plugged into something – must be terminated to prevent signal bounce.

   In bus topology nodes are connected to the bus cable by drop lines and taps. A drop line is a connection running between the device and the main cable. A tap is a connector that either splices into the main cable or punctures the sheathing of a cable to create a contact with the metallic core. As a signal travels along the backbone, some of its energy is transformed into heat. Therefore, it becomes weaker and weaker as it travels farther and farther. For this reason there is a limit on the number of taps a bus can support and on the distance between those taps.

Bus Topology with three stations Advantages of Linear Bus Topology

1) It is easy to set-up and extend bus network.
2) Cable length required for this topology is the least compared to other networks.
3) Bus topology very cheap.
4) Linear Bus network is mostly used in small networks.

Disadvantages of Linear Bus Topology

1) There is a limit on central cable length and number of nodes that can be connected.
2) Dependency on central cable in this topology has its disadvantages. If the main cable (i.e. bus) encounters some problem, whole network breaks down.
3) Proper termination is required to dump signals. Use of terminators is must.
4) It is difficult to detect and troubleshoot fault at individual station.
5) Maintenance costs can get higher with time.
6) Efficiency of Bus network reduces, as the number of devices connected to it increases.
7) It is not suitable for networks with heavy traffic.
8) Security is very low because all the computers receive the sent signal from the source.

Ring Topology

The ring topology connects computers on a single circle of cable. There are no terminated ends. A ring topology connects one host to the next and the last host to the first. The signal

Notes

travels around the loop in one direction and pass through each computer. Unlike the passive bus topology, each computer acts like a repeater to boost the signal and send it on to the next computer. Because the signal passes through each computer, the failure of one computer can impact the entire network.

One method of transmitting data around a ring is called token passing. The token is passed from computer to computer until it gets to a computer that has data to send. The sending computer modifies the token, puts an electronic address on the data, and sends it around the ring.

Advantages of Ring Topology

1) This type of network topology is very organized. Each node gets to send the data when it receives an empty token. This helps to reduces chances of collision. Also in ring topology all the traffic flows in only one direction at very high speed.

2) Even when the load on the network increases, its performance is better than that of Bus topology.

3) There is no need for network server to control the connectivity between workstations.

4) Additional components do not affect the performance of network.

5) Each computer has equal access to resources.

Disadvantages of Ring Topology

1) Each packet of data must pass through all the computers between source and destination. This makes it slower than Star topology.

2) If one workstation or port goes down, the entire network gets affected.

3) Network is highly dependent on the wire which connects different components.

4) MAU's and network cards are expensive as compared to Ethernet cards and hubs.

Star Topology

In the star topology, computers are connected by cable segments to centralized component, called a hub or switch.

Signals are transmitted from the sending computer through the hub or switch to all computers on the network. This topology originated in the early days of computing with computers connected to a centralized mainframe computer. It is now a common topology in microcomputer networking. Each device has a dedicated point-to-point link only to a central controller, usually called a hub. The devices are not directly linked to one another.

Unlike a mesh topology, a star topology does not allow direct traffic between devices. The controller acts as an exchange: If one device wants to send data to another, it sends the data to the controller, which then relays the data to the other connected device.

The star network offers centralized resources and management. However, because each computer is connected to a central point, this topology requires a great deal of cable in a large network installation. Also, if the central point fails, the entire network goes down.

Advantages of Star Topology

1) As compared to Bus topology it gives far much better performance, signals don't necessarily get transmitted to all the workstations. A sent signal reaches the intended destination after passing through no more than 3-4 devices and 2-3 links. Performance of the network is dependent on the capacity of central hub.

2) Easy to connect new nodes or devices. In star topology new nodes can be added easily without affecting rest of the network. Similarly components can also be removed easily.

3) Centralized management. It helps in monitoring the network.

4) Failure of one node or link doesn□t affect the rest of network. At the same time it is easy to detect the failure and troubleshoot it.

Disadvantages of Star Topology

1) Too much dependency on central device has its own drawbacks. If it fails whole network goes down.

2) The use of hub, a router or a switch as central device increases the overall cost of the network.

3) Performance and as well number of nodes which can be added in such topology is depended on capacity of central device.

Mesh Topology

In a mesh topology, every device has a dedicated point-to- point link to every other device. The term dedicated means that the link carries traffic only between the two devices it connects. In a mesh topology, Node1 must be connected to n-1 nodes, node 2 must be connected to (n - 1) nodes, and finally node n must be connected to (n - 1) nodes. We need n (n - 1) physical links. In other words, we can say that in a mesh topology, we need n (n1) / 2 .

To accommodate many links, every device on the network must have (n - 1) input/ output (I/O) ports to be connected to the (n - 1) stations as shown in Figure above. For these reasons a mesh topology is usually implemented in a limited fashion, as a backbone connecting the main computers of a hybrid network that can include several other topologies. One practical example of a mesh topology is the connection of telephone regional offices in which each regional office needs to be connected to every other regional office.

Advantages of Mesh topology

1) Data can be transmitted from different devices simultaneously. This topology can withstand high traffic.

2) Even if one of the components fails there is always an alternative present. So data transfer doesn't get affected.

Notes

3) Expansion and modification in topology can be done without disrupting other nodes.

Disadvantages of Mesh topology

1) There are high chances of redundancy in many of the network connections.

2) Overall cost of this network is way too high as compared to other network topologies.

3) Set-up and maintenance of this topology is very difficult. Even administration of the network is tough.

Hybrid Topology

Before starting about Hybrid topology, we saw that a network topology is a connection of various links and nodes, communicating with each other for transfer of data. We also saw various advantages and disadvantages of Star, Bus, Ring, Mesh. Hybrid, as the name suggests, is mixture of two different things. Similarly in this type of topology we integrate two or more different topologies to form a resultant topology which has good points (as well as weaknesses) of all the constituent basic topologies rather than having characteristics of one specific topology. This combination of topologies is done according to the requirements of the organization.

For example, if there is an existing ring topology in one office department while a bus topology in another department, connecting these two will result in Hybrid topology. Remember connecting two similar topologies cannot be termed as Hybrid topology. Star-Ring and Star-Bus networks are most common examples of hybrid network.

1) **Reliable:** Unlike other networks, fault detection and troubleshooting is easy in this type of topology. The part in which fault is detected can be isolated from the rest of network and required corrective measures can be taken, WITHOUT affecting the functioning of rest of the network.

2) **Scalable:** It's easy to increase the size of network by adding new components, without disturbing existing architecture.

3) **Flexible:** Hybrid Network can be designed according to the requirements of the organization and by optimizing the available resources. Special care can be given to nodes where traffic is high as well as where chances of fault are high.

4) **Effective:** Hybrid topology is the combination of two or more topologies, so we can design it in such a way that strengths of constituent topologies are maximized while there weaknesses are neutralized. For example we saw Ring Topology has good data reliability (achieved by use of tokens) and Star topology has high tolerance capability (as each node is not directly connected to other but through central device), so these two can be used effectively in hybrid star-ring topology.

Disadvantages of Hybrid Topology

1) Complexity of Design: One of the biggest drawbacks of hybrid topology is its design. It is not easy to design this type of architecture and it□s a tough job for designers. Configuration

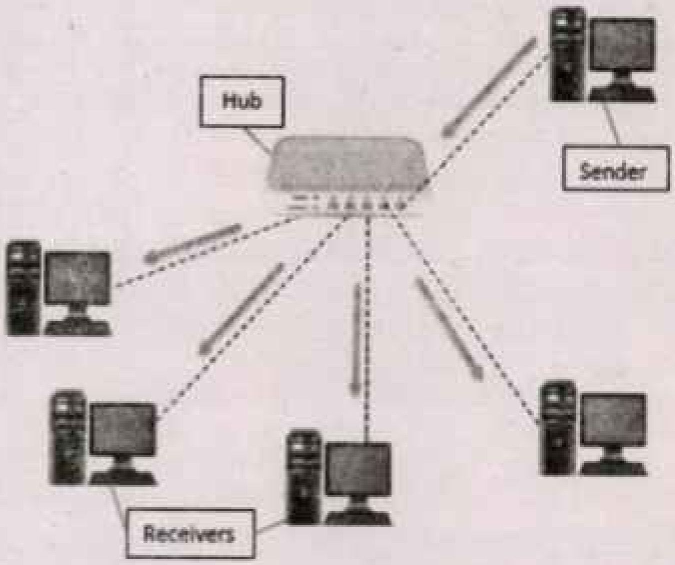
and installation process needs to be very efficient.

2) Costly Hub: The hubs used to connect two distinct networks, are very expensive. These hubs are different from usual hubs as they need to be intelligent enough to work with different architectures and should be function even if a part of network is down.

3) Costly Infrastructure: As hybrid architectures are usually larger in scale, they require a lot of cables; cooling systems, sophisticate network devices, etc.

2.13 HUB

A network hub is a node that broadcasts data to every computer or Ethernet-based device connected to it. A hub is less sophisticated than a switch, the latter of which can isolate data transmissions to specific devices. Network hubs are best suited for small, simple local area network (LAN) environments. A network hub is a node that broadcasts data to every computer or Ethernet-based device connected to it. A hub is less sophisticated than a switch, the latter of which can isolate data transmissions to specific devices. Network hubs are best suited for small, simple local area network (LAN) environments.



Types of Hub

- **Active Hub:** These are the hubs that have their own power supply and can clean, boost, and relay the signal along with the network. It serves both as a repeater as well as a wiring center. These are used to extend the maximum distance between nodes.
- **Passive Hub:** These are the hubs that collect wiring from nodes and power supply from the active hub. These hubs relay signals onto the network without cleaning and boosting them and can't be used to extend the distance between nodes.

Notes

- Intelligent Hub: It works like active hubs and includes remote management capabilities. They also provide flexible data rates to network devices. It also enables an administrator to monitor the traffic passing through the hub and to configure each port in the hub.

2.14 SWITCHES

A switch is a data link layer networking device which connects devices in a network and uses packet switching to send and receive data over the network.

Differences between Hub and Switch

Hub	Switch
They operate in the physical layer of the OSI model.	They operate in the data link layer of the OSI model.
It is a non-intelligent network device that sends message to all ports.	It is an intelligent network device that sends message to selected destination ports.
It primarily broadcasts messages.	It is supports unicast, multicast and broadcast.
Transmission mode is half duplex.	Transmission mode is full duplex.
Collisions may occurs during setup of transmission when more than one computers place data simultaneously in the corresponding ports.	Collisions do not occur since the communication is full duplex.
They are passive devices, they don't have any software associated with it.	They are active devices, equipped with network software.
They generally have fewer ports of 4/12.	The number of ports is higher – 24/48.

Like a hub, a switch also has many ports, to which computers are plugged in. However, when a data frame arrives at any port of a network switch, it examines the destination address and sends the frame to the corresponding device(s). Thus, it supports both unicast and multicast communications.

2.15 BRIDGES

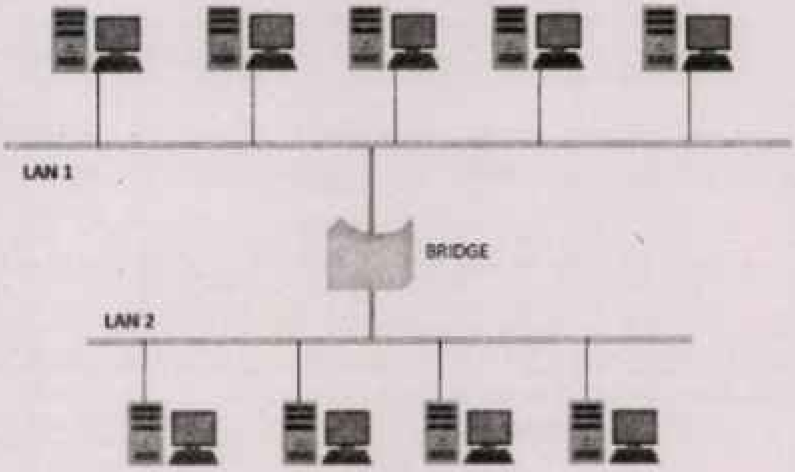
A bridge is a network device that connects multiple LANs (local area networks) together to form a larger LAN. The process of aggregating networks is called network bridging. A bridge connects the different components so that they appear as parts of a single network. Bridges operate at the data link layer of the OSI model and hence also referred as Layer 2 switches.

The following diagram shows a bridges connecting two LANs –

Uses of Bridge

- Bridges connects two or more different LANs that has a similar protocol and provides communication between the devices (nodes) in them.

- By joining multiple LANs, bridges help in multiplying the network capacity of a single LAN.
- Since they operate at data link layer, they transmit data as data frames. On receiving a data frame, the bridge consults a database to decide whether to pass, transmit or discard the frame.
- If the frame has a destination MAC (media access control) address in the same network, the bridge passes the frame to that node and then discards it.



- If the frame has a destination MAC address in a connected network, it will forward the frame toward it.
- By deciding whether to forward or discard a frame, it prevents a single faulty node from bringing down the entire network.
- In cases where the destination MAC address is not available, bridges can broadcast data frames to each node. To discover new segments, they maintain the MAC address table.
- In order to provide full functional support, bridges ideally need to be transparent. No major hardware, software or architectural changes should be required for their installation.
- Bridges can switch any kind of packets, be it IP packets or AppleTalk packets, from the network layer above. This is because bridges do not examine the payload field of the data frame that arrives, but simply looks at the MAC address for switching.
- Bridges also connect virtual LANs (VLANs) to make a larger VLAN.
- A wireless bridge is used to connect wireless networks or networks having a wireless segment.

Notes

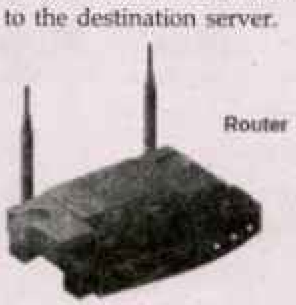
Types of Bridges

- Transparent Bridges: These are the bridge in which the stations are completely unaware of the bridge's existence i.e. whether or not a bridge is added or deleted from the network, reconfiguration of the stations is unnecessary. These bridges make use of two processes i.e. bridge forwarding and bridge learning.
- Source Routing Bridges: In these bridges, routing operation is performed by the source station and the frame specifies which route to follow. The host can discover the frame by sending a special frame called the discovery frame, which spreads through the entire network using all possible paths to the destination.

2.16 ROUTERS

A Router is a networking device that forwards data packets between computer networks.

Let us understand this by a very general example, suppose you search for www.google.com in your web browser then this will be a request which will be sent from your system to the google's server to serve that webpage, now your request which is nothing but a stream of packets don't just go the google's server straightaway they go through a series of networking devices known as a router which accepts this packets and forwards them to correct path and hence it reaches to the destination server.



A router has a number of interfaces by which it can connect to a number of host systems.

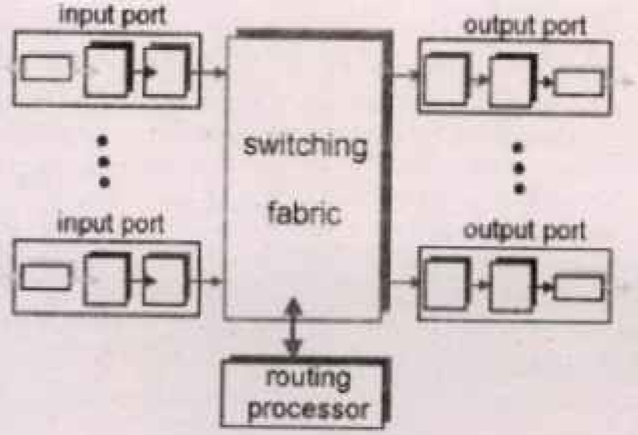
Functions of a Router

The router basically performs two major functions:

- Forwarding : The router receives the packets from its input ports, checks its header, performs some basic functions like checking checksum, and then looks up to the routing table to find the appropriate output port to dump the packets onto, and forwards the packets onto that output port.
- Routing : Routing is the process by which the router ascertains what is the best path for the packet to reach the destination, It maintains a routing table which is made using different algorithms by the router only.

The architecture of a Router:

A Generic router consist of the following components:



Input Port:

This is the interface by which packets are admitted into the router, it performs several key functions as terminating the physical link at the router, this is done by the leftmost part in the below diagram, the middle part does the work of interoperating with the link-layer like decapsulation, in the last part of the input port the forwarding table is looked up and is used to determine the appropriate output port based on the destination address.

Switching Fabric:

This is the heart of the Router, It connects the input ports with the output ports. It is kind of a network inside a networking device. The switching fabric can be implemented in a number of ways some of the prominent ones are:

- Switching via memory: In this, we have a processor which copies the packet from input ports and sends it to the appropriate output port. It works as a traditional CPU with input and output ports acting as input and output devices
- Switching via bus: In this implementation, we have a bus that connects all the input ports to all the output ports. On receiving a packet and determining which output port it must be delivered to, the input port puts a particular token on the packet and transfers it to the bus.

  All output ports are able to see the packets but it will be delivered to the output port whose token has been put in, the token is then scraped off by that output port and the packet is forwarded
- Switching via interconnection network: This is a more sophisticated network, here instead of a single bus we use a 2N bus to connect n input ports to n output ports.

Output Port

This is the segment from which packets are transmitted out of the router. The output port looks at its queuing buffers (when more than one packets have to be transmitted through the same output port queuing buffers are formed) and takes packets, does link layer functions, and finally transmits the packets to an outgoing link

Notes

Routing Processor

It executes the routing protocols, it works like a traditional CPU. It employs various routing algorithms like link-state algorithm, distance-vector algorithm, etc. to prepare the forwarding table, which is looked up to determine the route and the output port.

Gateway

A gateway, as the name suggests, is a passage to connect two networks together that may work upon different networking models. They basically work as the messenger agents that take data from one system, interpret it, and transfer it to another system. Gateways are also called protocol converters and can operate at any network layer. Gateways are generally more complex than switches or routers. Gateway is also called a protocol converter.

Brouter

It is also known as the bridging router is a device that combines features of both bridge and router. It can work either at the data link layer or a network layer. Working as a router, it is capable of routing packets across networks, and working as the bridge, it is capable of filtering local area network traffic.

NIC - NIC or network interface card is a network adapter that is used to connect the computer to the network. It is installed in the computer to establish a LAN. It has a unique id that is written on the chip, and it has a connector to connect the cable to it. The cable acts as an interface between the computer and router or modem. NIC card is a layer 2 device which means that it works on both physical and data link layer of the network model.

2.17 CELL RELAY

In computer networking, cell relay refers to a method of statistically multiplexing small fixed-length packets, called "cells", to transport data between computers or kinds of network equipment. It is a reliable, connection-oriented packet switched data communications protocol.,

Cell relay is data transmission service that uses transmission technology referred to as Asynchronous Transfer Mode (ATM). As the name suggests, the data transmission unit is a fixed length of data known as a cell. High-speed transmission compared to other services like frame relay is possible with the cell relay method. The cell relay is considered by most to be the transport service of the future.

Advantages

- High-speed Transmission The purpose of ATM is to provide high speed and low-delay switching networks to support any type of user traffic, such as voice, data or video applications.
- Multiplexing Transmission As in X.25 networks and frame relay, multiple channels can be set within one physical line and communication is possible with multiple parties simultaneously. ATM segments and multiplexes use traffic into small, fixed length units called cells to reduce and control delay. ATM can support different speeds, traffic types and quality of service matched to applications.

Disadvantages

- Cell Discarding Occurs with Congestion When congestion occurs in the network, the cells (data) within the network are discarded and retransmission control cannot be carried out within the network. The user must be responsible for carrying out retransmission control with other party.
- ATM provides no error detection operations on users payload inside the cell. It provides no retransmission services, and few operations are performed on the small header. The purpose of this approach is to implement a network fast enough to support multi-megabit transfer rates.
- High Cost As the technology is new and not commercially available; standards are still in development stage.

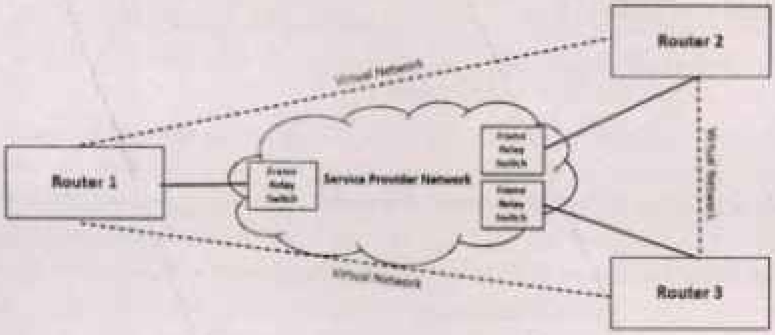
Cell Relay and the OSI Reference Model

The cell relay protocol corresponds to first two layer of OSI reference model. The part that corresponds to second layer, that is, data link layer is referred as ATM layer. However, ATM layer does not have all functions of data link layer. Therefore, a protocol referred as the ATM Adaptation Layer (AAL) is prescribed above the data link layer AAL is user defined and is not mandatory for cell relay usage.

2.18 FRAME RELAY

Frame Relay is a packet-switching network protocol that is designed to work at the data link layer of the network. It is used to connect Local Area Networks (LANs) and transmit data across Wide Area Networks (WANs). It is a better alternative to a point-to-point network for connecting multiple nodes that require separate dedicated links to be established between each pair of nodes. It allows transmission of different size packets and dynamic bandwidth allocation.

Also, it provides a congestion control mechanism to reduce the network overheads due to congestion. It does not have an error control and flow management mechanism.



Working:

1. Frame relay switches set up virtual circuits to connect multiple LANs to build a WAN. Frame relay transfers data between LANs across WAN by dividing the data in packets known as frames and transmitting these packets across the network. It supports communication with multiple LANs over the shared physical links or private lines.
2. Frame relay network is established between Local Area Networks (LANs) border devices such as routers and service provider network that connects all the LAN networks. Each LAN has an access link that connects routers of LAN to the service provider network terminated by the frame relay switch. The access link is the private physical link used for communication with other LAN networks over WAN. The frame relay switch is responsible for terminating the access link and providing frame relay services.
3. For data transmission, LAN's router (or other border device linked with access link) sends the data packets over the access link. The packet sent by LAN is examined by a frame relay switch to get the Data Link Connection Identifier (DLCI) which indicates the destination of the packet. Frame relay switch already has the information about addresses of the LANs connected to the network hence it identifies the destination LAN by looking at DLCI of the data packet. DLCI basically identifies the virtual circuit (i.e. logical path between nodes that doesn't really exist) between source and destination network. It configures and transmits the packet to frame relay switch of destination LAN which in turn transfers the data packet to destination LAN by sending it over its respective access link. Hence, in this way, a LAN is connected with multiple other LANs by sharing a single physical link for data transmission.
4. Frame relay also deals with congestion within a network. Following methods are used to identify congestion within a network:

Forward Explicit Congestion Network (FECN)

FECN is a part of the frame header that is used to notify the destination about the congestion in the network. Whenever a frame experiences congestion while transmission, the frame relay switch of the destination network sets the FECN bit of the packet that allows the destination to identify that packet has experienced some congestion while transmission.

Backward Explicit Congestion Network (BECN)

BECN is a part of the frame header that is used to notify the source about the congestion in the network. Whenever a frame experiences congestion while transmission, the destination sends a frame back to the source with a set BECN bit that allows the source to identify that packet that was transmitted had experienced some congestion while reaching out to the destination. Once, source identifies congestion in the virtual circuit, it slows down to transmission to avoid network overhead.

Discard Eligibility (DE)

DE is a part of the frame header that is used to indicate the priority for discarding the packets. If the source is generating a huge amount of traffic on the certain virtual network then it can set DE bits of less significant packets to indicate the high priority for discarding the packets in case of network overhead. Packets with set DE bits are discarded before the packets with unset DE bits in case of congestion within a network.

Types

Permanent Virtual Circuit (PVC)

These are the permanent connections between frame relay nodes that exist for long durations. They are always available for communication even if they are not in use. These connections are static and do not change with time.

Switched Virtual Circuit (SVC)

These are the temporary connections between frame relay nodes that exist for the duration for which nodes are communicating with each other and are closed/ discarded after the communication. These connections are dynamically established as per the requirements.

Advantages:

- High speed
- Scalable
- Reduced network congestion
- Cost-efficient
- Secured connection

Disadvantages:

- Lacks error control mechanism
- Delay in packet transfer
- Less reliable

2.19 ISDN AND B-ISDN

ISDN stands for Integrated Services Digital Network. It's a set of communication standards that uses digital transmission to make phone calls, video calls, transmit data and other network services over the circuits of the traditional PSTN (Public Switched Telephone Network). ISDN was introduced in 1986 by BT. Let us understand in detail:

- The B-ISDN (broadband integrated services digital network) is a virtual circuit-switched network that can use high-speed packet switching services. The B-ISDN will use a flexible multiplexing format called ATM (asynchronous transfer mode).

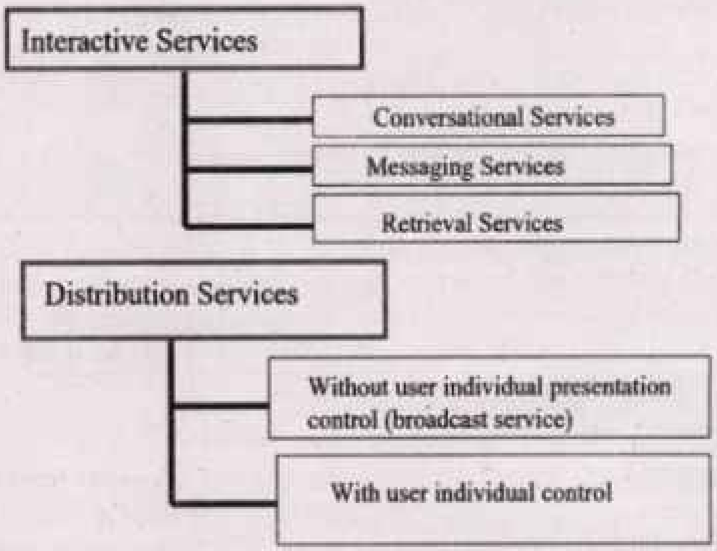
- B-ISDN services are classified into interactive and distribution services. Interactive services contain the bidirectional flow of user information between two subscribers or between a subscriber and a service provider.
- BISDN is an extension of ISDN, that is, it has narrowband capability of ISDN but also the broadband capability.
- The purpose of BISDN is to achieve complete integration of services, ranging from low-bit- rate burst signals to high-bit-rate continuous real-time signals.

B-ISDN Services

There are two types of B-ISDN services which are as follows:

- Interactive Services – Two-way exchange of information (other than control signalling information) between two subscribers or between a subscriber and a service provider.
- Distribution Services – Primarily one way transfer of information, from service provider to B-ISDN subscriber.

These services are shown in the diagram format below:



Technology Developments

The key technology developments for B-ISDN are as follows:

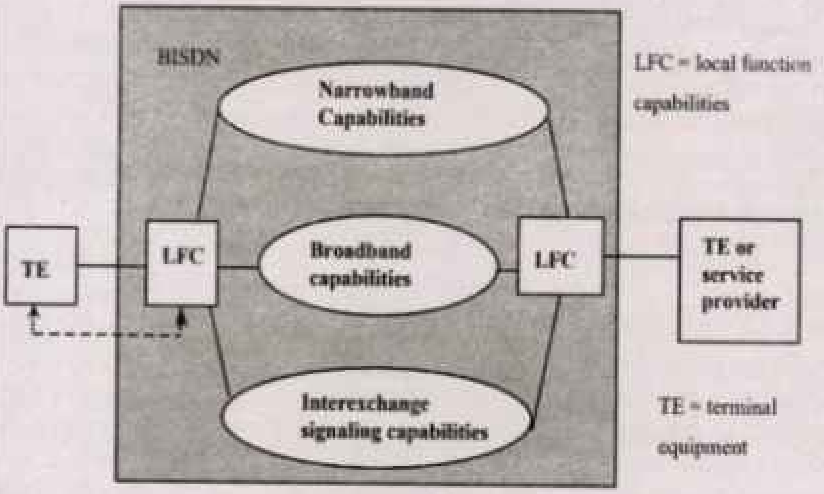
- Optical fiber transmission systems that can offer low-cost, high-data rate transmission channels for network trunks and subscriber lines.
- The Microelectronic circuits which offer high-speed, low-cost building blocks for switching, transmission, and subscriber equipment.

Notes

High-quality video monitors and cameras that have sufficient production quantities are offered at low cost.

B-ISDN Architecture

The B-ISDN architecture is shown in the diagram below –



The architecture of the B-ISDN includes low Layer capabilities and high Layer capabilities. These capabilities support the services within the B-ISDN and other networks by means of interworking B-ISDN with those networks.

Low Layer capabilities

The low layer capabilities of B-ISDN architecture are explained below:

- From the functional capabilities of the B-ISDN, as shown in Figure, the information transfer capabilities require further description.
- Broadband information transfer is provided by an ATM at the B-ISDN user-network interface (UNI) and at switching entities inside the network.

High Layer capabilities

The high layer capabilities of B-ISDN architecture are explained below:

Normally, the high Layer functional capabilities are involved only in the terminal equipment.

The support of some services, provision of high layer functions could be made through special nodes in the B-ISDN belonging to the public network or to centres operated by other organizations and accessed via B-ISDN user-network or network node interfaces (NNIs).

Interactive services

The interactive services are further divided into three sub-categories which are as follows–

Conversational

Conversational service involves the real-time exchange of information such as sound, video, data or entire documents. Examples include video-telephony, video-conference, and high-speed data transfer. Video-telephony is like the normal video telephony service but also has video capture, transmission and display capabilities. Video-conference supports voice and video communication between two conference rooms or between several individuals.

Messaging

Messaging service involves the non-real-time exchange of information between subscribers in a store-and-forward fashion.

Retrieval

Retrieval services provide subscribers with retrieval access to centrally-stored public information. Examples include broadband videotext (retrieval of video images/sequences with sound, text and graphics), video retrieval (subscriber create to video libraries of movies) and return of high-resolution pictures and records from multiple archives and data centers.

Distribution Services

Distribution services contain the unidirectional flow of user information from a service provider to a subscriber.

Distribution services are divided into two sub-categories, which are as follows:

- Distribution services without user presentation control involve the central broadcast of information to many subscribers, where subscribers have no control over data display. Examples include the broadcast of TV programs, electronic newspapers, and electronic publishing.
- Distribution services with user presentation control are the same as the previous category. The information is offered as cyclically repeated frames, thereby enabling the subscribers to control the start and the order of the frames presentation. Examples include electronic newspaper and tele-advertising.

SUMMARY

- Computer Network is a group of computers connected with each other through wires, optical fibres or optical links so that various devices can interact with each other through a network. The aim of the computer network is the sharing of resources among various devices.
- Network topology is the arrangement of the elements (links, nodes, etc.) of a communi-

cation network. It can be used to define or describe the arrangement of various types of telecommunication networks, including command and control radio networks, industrial fieldbusses and computer networks. It is the topological structure of a network and may be depicted physically or logically. It is an application of graph theory wherein communicating devices are modeled as nodes and the connections between the devices are modeled as links or lines between the nodes.

- A workstation refers to an individual computer, or group of computers, used by a single user to perform work. For example, a "workstation" may be an average-powered computer connected to a larger network. It can also refer to a powerful computer intended for serious academic or professional computation.
- Servers are computers that run services to serve the needs of other computers. There are, for example, home media servers, web servers, and print servers. There are also file servers and database servers.
- One company employee, for example, may log in to the client computer to access the files and applications that the server runs. We call this two-tier architecture a client-server architecture.
- 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.
- A bridge is a network device that connects multiple LANs (local area networks) together to form a larger LAN. The process of aggregating networks is called network bridging. A bridge connects the different components so that they appear as parts of a single network. Bridges operate at the data link layer of the OSI model and hence also referred as Layer 2 switches.
- A gateway, as the name suggests, is a passage to connect two networks together that may work upon different networking models. They basically work as the messenger agents that take data from one system, interpret it, and transfer it to another system. Gateways are also called protocol converters and can operate at any network layer. Gateways are generally more complex than switches or routers. Gateway is also called a protocol converter.
- Cell relay is data transmission service that uses transmission technology referred to as Asynchronous Transfer Mode (ATM). As the name suggests, the data transmission unit is a fixed length of data known as a cell. High-speed transmission compared to other services like frame relay is possible with the cell relay method. The cell relay is considered by most to be the transport service of the future.
- Frame Relay is a packet-switching network protocol that is designed to work at the data link layer of the network. It is used to connect Local Area Networks (LANs) and transmit data across Wide Area Networks (WANs). It is a better alternative to a point-to-point network for connecting multiple nodes that require separate dedicated links to be established between each pair of nodes. It allows transmission of different size packets and dynamic bandwidth allocation.

- ISDN stands for Integrated Services Digital Network. It's a set of communication standards that uses digital transmission to make phone calls, video calls, transmit data and other network services over the circuits of the traditional PSTN (Public Switched Telephone Network). ISDN was introduced in 1986 by BT.

KEY WORDS

- **BISDN** : It is an extension of ISDN, that is, it has narrowband capability of ISDN but also the broadband capability. The purpose of BISDN is to achieve complete integration of services, ranging from low-bit- rate burst signals to high-bit-rate continuous real-time signals.
- **Digital-to-analog conversion:** Digital-to-analog conversion is the process of changing one of the characteristics of an analog signal based on the information in digital data.

REVIEW QUESTIONS

1. What are bridges in computer network?
2. What are the uses of Computer Network?
3. Uses of Computer Networks
4. What are the types of ethernet? Explain.
5. What is the use of routers?
6. What is BISDN in the Computer Network?
7. Discuss network topologies.
8. Differentiate between boradband and baseband.
9. What is the use of server? Discuss the types of server.
10. What is frame relay?

FURTHER READINGS

1. Kurose James F., Ross Keith W. Computer Networking – By Pearson.
2. https://www.javatpoint.com/error-detection-and-correction-code-in-digital-electronics

Unit 3

OSI Model

Structure

3.0 LEARNING OBJECTIVES

After reading this chapter students will be able to:

- know the concept of port and OSI model
- understand the broadcasting and multicasting
- disucuss the point to point communication and IP address
- disucuss the tunneling, virtual private network and network operating systems.

Notes

3.1 INTRODUCTION

The Open Systems Interconnection (OSI) model is a reference tool for understanding data communications between any two networked systems. It divides the communications processes into seven layers. Each layer both performs specific functions to support the layers above it and offers services to the layers below it. The three lowest layers focus on passing traffic through the network to an end system. The top four layers come into play in the end system to complete the process.

This unit will provide you with an understanding of each of the seven layers, including their functions and their relationships to each other. This will provide you with an overview of the network process, which can then act as a framework for understanding the details of computer networking. Since the discussion of networking often includes talk of "extra layers", this paper will address these unofficial layers as well.

Finally, this unit will draw comparisons between the theoretical OSI model and the functional TCP/IP model. Although TCP/IP has been used for network communications before the adoption of the OSI model, it supports the same functions and features in a differently layered arrangement.

When dealing with networking, you may hear the terms "network model" and "network layer" used often. Network models define a set of network layers and how they interact. There are several different network models depending on what organization or company started them.

The Open Systems Interconnection model (OSI) is a conceptual model that characterizes and standardizes the internal functions of a communication system by partitioning it into abstraction layers. The model is a product of the Open Systems Interconnection project at the International Organization for Standardization (ISO), maintained by the identification ISO/IEC 7498-1.

The model groups communication functions into seven logical layers. A layer serves the layer above it and is served by the layer below it. For example, a layer that provides error-free communications across a network provides the path needed by applications above it, while it calls the next lower layer to send and receive packets that make up the contents of that path. Two instances at one layer are connected by a horizontal connection on that layer.

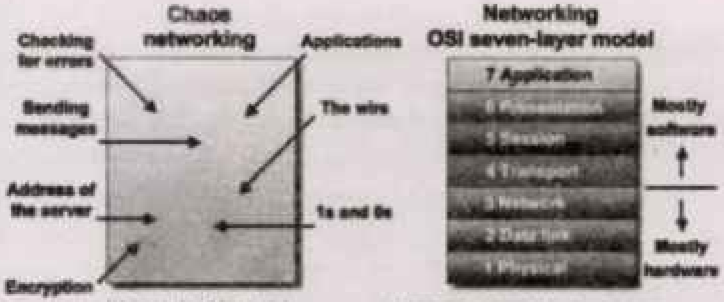
3.2. OSI MODEL

The Open Systems Interconnect (OSI) model has seven layers. This unit describes and explains them, beginning with the 'lowest' in the hierarchy (the physical) and proceeding to the 'highest' (the application). The layers are stacked as follows:

- Application
- Presentation
- Session
- Transport
- Network

- Data Link
- Physical

An Overview of the OSI Model



Without the OSI model, networks would be very difficult to understand and implement.

With the OSI model, networks can be broken up into manageable pieces. The OSI model provides a common language to explain components and their functionality.

A networking model offers a generic means to separate computer networking functions into multiple layers. Each of these layers relies on the layers below it to provide supporting capabilities and performs support to the layers above it. Such a model of layered functionality is also called a "protocol stack" or "protocol suite".

Protocols, or rules, can do their work in either hardware or software or, as with most protocol stacks, in a combination of the two. The nature of these stacks is that the lower layers do their work in hardware or firmware (software that runs on specific hardware chips) while the higher layers work in software.

The Open System Interconnection model is a seven-layer structure that specifies the requirements for communications between two computers. The ISO (International Organization for Standardization) standard 7498-1 defined this model. This model allows all network elements to operate together, no matter who created the protocols and what computer vendor supports them.

The main benefits of the OSI model include the following:

- Helps users understand the big picture of networking
- Helps users understand how hardware and software elements function together
- Makes troubleshooting easier by separating networks into manageable pieces
- Defines terms that networking professionals can use to compare basic functional relationships on different networks
- Helps users understand new technologies as they are developed
- Aids in interpreting vendor explanations of product functionality

Physical Layer

The physical layer of the OSI model defines connector and interface specifications, as well as the medium (cable) requirements. Electrical, mechanical, functional, and procedural specifications are provided for sending a bit stream on a computer network. The physical layer, the lowest layer of the OSI model, is concerned with the transmission and reception of the unstructured raw bit stream over a physical medium. It describes the electrical/optical, mechanical, and functional interfaces to the physical medium, and carries the signals for all of the higher layers. It provides:

- Data encoding: modifies the simple digital signal pattern (1s and 0s) used by the PC to better accommodate the characteristics of the physical medium, and to aid in bit and frame synchronization. It determines:
  - What signal state represents a binary 1
  - How the receiving station knows when a "bit-time" starts
  - How the receiving station delimits a frame
- Physical medium attachment, accommodating various possibilities in the medium:
  - Will an external transceiver (MAU) be used to connect to the medium?
  - How many pins do the connectors have and what is each pin used for?
- Transmission technique: determines whether the encoded bits will be transmitted by baseband (digital) or broadband (analog) signaling.

Components of the physical layer include:

- Cabling system components
- Adapters that connect media to physical interfaces
- Connector design and pin assignments
- Hub, repeater, and patch panel specifications
- Wireless system components
- Parallel SCSI (Small Computer System Interface)
- Network Interface Card (NIC)

In a LAN environment, Category 5e UTP (Unshielded Twisted Pair) cable is generally used for the physical layer for individual device connections. Fiber optic cabling is often used for the physical layer in a vertical or riser backbone link. The IEEE, EIA/TIA, ANSI, and other similar standards bodies developed standards for this layer.

The Data Link Layer

The data link layer provides error-free transfer of data frames from one node to another over the physical layer, allowing layers above it to assume virtually error-free transmission over the link. To do this, the data link layer provides:

- Link establishment and termination: establishes and terminates the logical link between two nodes.

- Frame traffic control: tells the transmitting node to "back-off" when no frame buffers are available.
- Frame sequencing: transmits/receives frames sequentially.
- Frame acknowledgment: provides/expects frame acknowledgments. Detects and recovers from errors that occur in the physical layer by retransmitting non- acknowledged frames and handling duplicate frame receipt.
- Frame delimiting: creates and recognizes frame boundaries.
- Frame error checking: checks received frames for integrity.
- Media access management: determines when the node "has the right" to use the physical medium.

Network Layer

The network layer controls the operation of the subnet, deciding which physical path the data should take based on network conditions, priority of service, and other factors. It provides:

- Routing: routes frames among networks.
- Subnet traffic control: routers (network layer intermediate systems) can instruct a sending station to "throttle back" its frame transmission when the router's buffer fills up.
- Frame fragmentation: if it determines that a downstream router's maximum transmission unit (MTU) size is less than the frame size, a router can fragment a frame for transmission and re-assembly at the destination station.
- Logical-physical address mapping: translates logical addresses, or names, into physical addresses.
- Subnet usage accounting: has accounting functions to keep track of frames forwarded by subnet intermediate systems, to produce billing information.

Communications Subnet: The network layer software must build headers so that the network layer software residing in the subnet intermediate systems can recognize them and use them to route data to the destination address.

This layer relieves the upper layers of the need to know anything about the data transmission and intermediate switching technologies used to connect systems. It establishes, maintains and terminates connections across the intervening communications facility (one or several intermediate systems in the communication subnet). In the network layer and the layers below, peer protocols exist between a node and its immediate neighbor, but the neighbor may be a node through which data is routed, not the destination station. The source and destination stations may be separated by many intermediate systems

Transport Layer

The transport layer ensures that messages are delivered error-free, in sequence, and with no losses or duplications. It relieves the higher layer protocols from any concern with the transfer of data between them and their peers. The size and complexity of a transport protocol depends on the type of service it can get from the network layer. For a reliable network layer

Notes

with virtual circuit capability, a minimal transport layer is required. If the network layer is unreliable and/or only supports datagrams, the transport protocol should include extensive error detection and recovery.

The transport layer provides:

- Message segmentation: accepts a message from the (session) layer above it, splits the message into smaller units (if not already small enough), and passes the smaller units down to the network layer. The transport layer at the destination station reassembles the message.
- Message acknowledgment: provides reliable end-to- end message delivery with acknowledgments.
- Message traffic control: tells the transmitting station to "back-off" when no message buffers are available.
- Session multiplexing: multiplexes several message streams, or sessions onto one logical link and keeps track of which messages belong to which sessions (see session layer).

Typically, the transport layer can accept relatively large messages, but there are strict message size limits imposed by the network (or lower) layer. Consequently, the transport layer must break up the messages into smaller units, or frames, prepending a header to each frame.

The transport layer header information must then include control information, such as message start and message end flags, to enable the transport layer on the other end to recognize message boundaries. In addition, if the lower layers do not maintain sequence, the transport header must contain sequence information to enable the transport layer on the receiving end to get the pieces back together in the right order before handing the received message up to the layer above.

End-to-end layers

Unlike the lower "subnet" layers whose protocol is between immediately adjacent nodes, the transport layer and the layers above are true "source to destination" or end-to-end layers, and are not concerned with the details of the underlying communications facility. Transport layer software (and software above it) on the source station carries on a conversation with similar software on the destination station by using message headers and control messages.

Sesson Layer

The session layer allows session establishment between processes running on different stations. It provides:

- Session establishment, maintenance and termination: allows two application processes on different machines to establish, use and terminate a connection, called a session.
- Session support: performs the functions that allow these processes to communicate over the network, performing security, name recognition, logging, and so on.

Presentation Layer

The presentation layer formats the data to be presented to the application layer. It can be viewed as the translator for the network. This layer may translate data from a format used by the application layer into a common format at the sending station, then translate the common format to a format known to the application layer at the receiving station.

The presentation layer provides:

- Character code translation: for example, ASCII to EBCDIC.
- Data conversion: bit order, CR-CR/LF, integer-floating point, and so on.
- Data compression: reduces the number of bits that need to be transmitted on the network.
- Data encryption: encrypt data for security purposes. For example, password encryption.

Application Layer

The application layer serves as the window for users and application processes to access network services. This layer contains a variety of commonly needed functions:

- Resource sharing and device redirection
- Remote file access
- Remote printer access
- Inter-process communication
- Network management
- Directory services
- Electronic messaging (such as mail)
- Network virtual terminals

3.3 TCP/IP MODEL OVERVIEW

The OSI model describes computer networking in seven layers. While there have been implementations of networking protocol that use those seven layers, most networks today use TCP/IP. But, networking professionals continue to describe networking functions in relation to the OSI layer that performs those tasks.

- The TCP/IP model uses four layers to perform the functions of the seven-layer OSI model.
- The network access layer is functionally equal to a combination of OSI physical and data link layers (1 and 2).
- The Internet layer performs the same functions as the OSI network layer (3).

Notes

- Things get a bit more complicated at the host-to-host layer of the TCP/IP model. If the host-to-host protocol is
- TCP, the matching functionality is found in the OSI transport and session layers (4 and 5). Using UDP equates to the functions of only the transport layer of the OSI model.
- The TCP/IP process layer, when used with TCP, provides the functions of the OSI model's presentation and application layers (6 and 7). When the TCP/IP transport layer protocol is UDP, the process layer's functions are equivalent to OSI session, presentation, and application layers (5, 6, and 7).
- Some of the layers use equipment to support the identified functions. Hub related activity is "Layer One".
- The naming of some devices designates the functional layer such as "Layer Two Switch" or "Layer Three
- Switch". Router functions focus on "Layer Three". User workstations and servers are often identified with "Layer Seven".

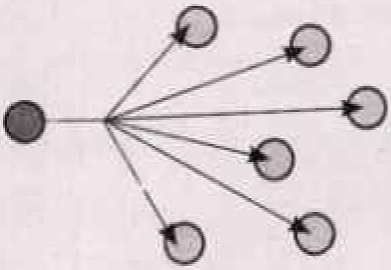
3.4 BROADCASTING

In computer networking, broadcasting is a method of transferring a message to all recipients simultaneously. Broadcasting can be performed as a high-level operation in a program, for example, broadcasting in Message Passing Interface, or it may be a low-level networking operation, for example broadcasting on Ethernet.

All-to-all communication is a computer communication method in which each sender transmits messages to all receivers within a group. In networking this can be accomplished using broadcast or multicast. This is in contrast with the point-to-point method in which each sender communicates with one receiver.

In computer networking, broadcasting refers to transmitting a packet that will be received by every device on the network. In practice, the scope of the broadcast is limited to a broadcast domain.

Broadcasting is the most general communication method, and is also the most intensive, in the sense that many messages may be required and many network devices are involved. This is in contrast to unicast addressing in which a host sends datagrams to another single host, identified by a unique address.



Broadcasting may be performed as all scatter in which each sender performs its own scatter in which the messages are distinct for each receiver, or all broadcast in which they are the same.

The MPI message passing method which is the de facto standard on large computer clusters includes the MPI_Alltoall method.

Not all network technologies support broadcast addressing; for example, neither X.25 nor frame relay have broadcast capability. The Internet Protocol Version 4 (IPv4), which is the primary networking protocol in use ıoday on the Internet and all networks connected to it, supports broadcast, but the broadcast domain is the broadcasting host's subnet, which is typically small; there is no way to do an Internet-wide broadcast. Broadcasting is largely confined to local area network (LAN) technologies, most notably Ethernet and Token Ring, where the performance impact of broadcasting is not as large as it would be in a wide area network.

The successor to IPv4, IPv6 does not implement the broadcast method, so as to prevent disturbing all nodes in a network when only a few may be interested in a particular service. Instead IPv6 relies on multicast addressing – a conceptually similar one-to-many routing methodology.

However, multicasting limits the pool of receivers to those that join a specific multicast receiver group.

Both Ethernet and IPv4 use an all-ones broadcast address to indicate a broadcast packet. Token Ring uses a special value in the IEEE 802.2 control field.

Broadcasting may be abused to perform a type of DoS-attack known as a Smurf attack. The attacker sends forged ping requests with the source IP-address of the victim computer. The victim computer is flooded by the replies from all computers in the domain.

Addressing Method

There are four principal addressing methods in the Internet Protocol:

- Unicast delivers a message to a single specific node using a one-to-one association between a sender and destination: each destination address uniquely identifies a single receiver endpoint.
- Broadcast delivers a message to all nodes in the network using a one-to-all association; a single datagram (or packet) from one sender is routed to all of the possibly multiple endpoints associated with the broadcast address. The network automatically replicates datagrams as needed to reach all the recipients within the scope of the broadcast, which is generally an entire network subnet.
- Multicast delivers a message to a group of nodes that have expressed interest in receiving the message using a one-to-many-of-many or many-to-many-of-many association; datagrams are routed simultaneously in a single transmission to many recipients. Multicast differs from broadcast in that the destination address designates a subset, not necessarily all, of the accessible nodes.
- Anycast delivers a message to any one out of a group of nodes, typically the one nearest to the source using a one-to-one-of-many association where datagrams are routed to any single member of a group of potential receivers that are all identified by the

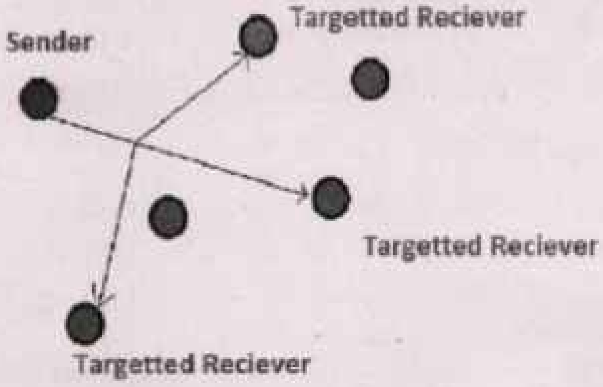
same destination address. The routing algorithm selects the single receiver from the group based on which is the nearest according to some distance or cost measure.

3.5 MULTICASTING

Multicast is group communication where data transmission is addressed to a group of destination computers simultaneously. It can be one-to-many or many-to-many distribution. Multicast should not be confused with physical layer point-to-multipoint communication. Multicast is often employed in Internet Protocol (IP) applications of streaming media, such as IPTV and multipoint videoconferencing.

Multicast is a method of group communication where the sender sends data to multiple receivers or nodes present in the network simultaneously. Multicasting is a type of one-to-many and many-to-many communication as it allows sender or senders to send data packets to multiple receivers at once across LANs or WANs. This process helps in minimizing the data frame of the network.

Multicasting works in similar to Broadcasting, but in Multicasting, the information is sent to the targeted or specific members of the network. This task can be accomplished by transmitting individual copies to each user or node present in the network, but sending individual copies to each user is inefficient and might increase the network latency. To overcome these shortcomings, multicasting allows a single transmission that can be split up among the multiple users, consequently, this reduces the bandwidth of the signal.



Applications:

Multicasting is used in many areas like:

- Internet protocol (IP)
- Streaming Media
- It also supports video conferencing applications and webcasts.

IP Multicast:

Multicasting that takes place over the Internet is known as IP Multicasting. These multicast follow the internet protocol(IP) to transmit data. IP multicasting uses a mechanism known as

'Multicast trees' to transmit to information among the users of the network. Multicast trees; allows a single transmission to branch out to the desired receivers. The branches are created at the Internet routers, the branches are created such that the length of the transmission will be minimum.

IP multicasts also use two other essential protocols to function; Internet Group Management Protocol (IGMP), Protocol Independent Multicast (PIM). IGMP allows the recipients to access the data or information. The network routers use PIM to create multicast trees.

To conclude, multicasting is an efficient way of communication; it reduces the bandwidth usage.

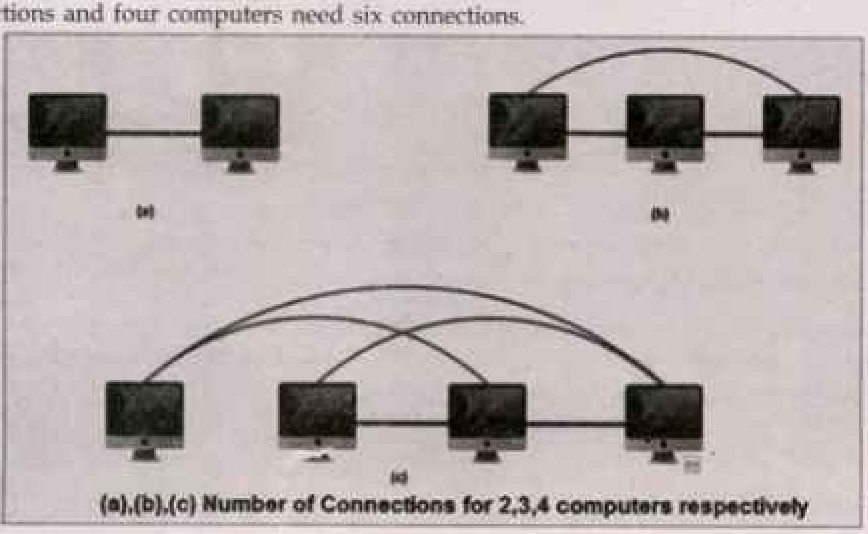
3.6 POINT TO POINT COMMUNICATION

In telecommunications, a point-to-point connection refers to a communications connection between two communication endpoints or nodes. 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 connection, in which many nodes can receive information transmitted by one node. Other examples of point-to-point communications links are leased lines and microwave radio relay.

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.

Point-to-point is sometimes abbreviated as P2P. This usage of P2P is distinct from P2P meaning peer-to-peer in the context of file sharing networks or other data-sharing protocols between peers.

The point-to-point scheme provides separate communication channels for each pair of computers. When more than two computers need to communicate with one another, the number of connections grows very quickly as number of computer increases. Above figure illustrates that two computers need only one connection, three computers need three connections and four computers need six connections.



(a),(b),(c) Number of Connections for 2,3,4 computers respectively

The point-to-point scheme provides separate communication channels for each pair

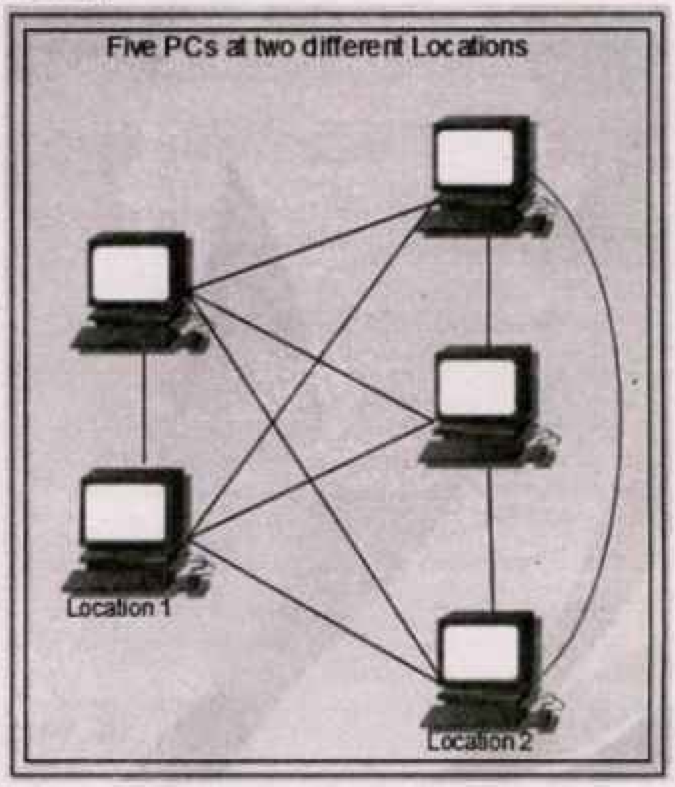
Notes

of computers. When more than two computers need to communicate with one another, the number of connections grows very quickly as number of computer increases. Above figure illustrates that two computers need only one connection, three computers need three connections and four computers need six connections.

As the Figure illustrates that the total number of connection grows more rapidly than the total number of computers. Mathematically, the number of connection needed for N computers is proportional to the square of N.

Point-to-point connections required = (N2 (N)/2.

Adding the Nth computer requires N 1 new connections which becomes a very expensive option. Moreover, many connections may follow the same physical path. Figure shows a point- to-point connection for five computers located at two different locations, say, ground and first floor of a building.



As there are five PCs, total ten connections will be required for point-to-point connection. Out of these ten connections six are passing through the same locution and thereby making point-to-point connection an expensive one.

Increasing the PC by one in the above configuration at location 2 as shown in Figure will increase the total number of connections to fifteen. Out 'of these connections eight connections will pass through the same area.

Logical Channels

The terminal connected to the packet switched network can communicate with multiple terminals at the same time using a single physical line. This makes it possible to set multiple logical paths called logical channels on a single physical line.

Multiple communication thus takes place through these logical channels. Based on the X.25 roles, 4096 logical channels can be set on a single physical line connected to a DTE.

These 4096 logical channels can be grouped into 16 groups and each group containing up to 256 channels. These channel groups are known as LCGN (Logical Channel Group Number) and LCN (Logical Channel Number) as shown in Figure. When data is transferred over virtual circuits, specific channel numbers and channel group numbers are allocated for use by all packets included in that transfer.

3.7 IP ADDRESSING

An IP address is a unique address that identifies a device on the internet or a local network. IP stands for "Internet Protocol," which is the set of rules governing the format of data sent via the internet or local network.

In essence, IP addresses are the identifier that allows information to be sent between devices on a network: they contain location information and make devices accessible for communication. The internet needs a way to differentiate between different computers, routers, and websites. IP addresses provide a way of doing so and form an essential part of how the internet works.

We assumed that network card on both computer are installed and working properly, for the network configuration, we create a simple network by assigning following IP address and subnet mask settings to each computer's network card, so that both computers know how to talk to each other:

Computer A:

- IP Address: 10.1.1.1
- Subnet mask: 255.255.255.0
- Gateway: [leave-it-blank]
- DNS Servers: [leave-it-blank]

Computer B:

- IP Address: 10.1.1.2
- Subnet mask: 255.255.255.0
- Gateway: [leave-it-blank]
- DNS Servers: [leave-it-blank]

As these 2 computers are directly connected, no gateway and DNS servers are required to be configured. After assigning IP address, try to ping the other computer from command prompt, you should be able to ping each other and then sharing printers or files as you wish.

- Configuring of IP Address and Other Network Information in On Windows 7
- IP address must be configured on computer in order to communicate with other com-

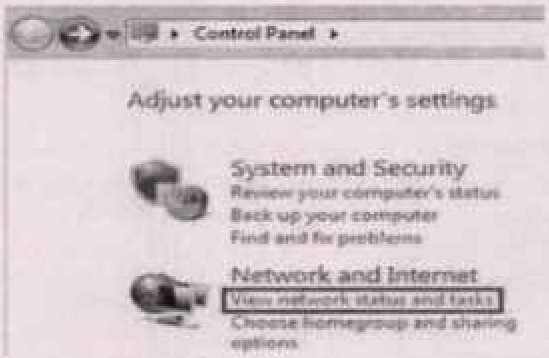
Notes

puters, because this IP address is the standard address understood by computers and other networking devices in networking world.

- We can configure IP address, subnet mask, gateway and DNS servers manually on computer, we can also configure computer to obtain IP address and other network information from DHCP server (most of the time is configured on router).

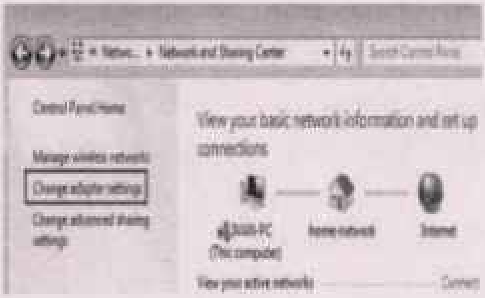
Procedure

1. Go to Start and click on Control Panel.
2. Click View network status and tasks in Control Panel window. See figure 73.


Control Panel ▸
Adjust your computer's settings
System and Security
Review your computer's status
Back up your computer
Find and fix problems
Network and Internet
View network status and tasks
Choose homegroup and sharing options

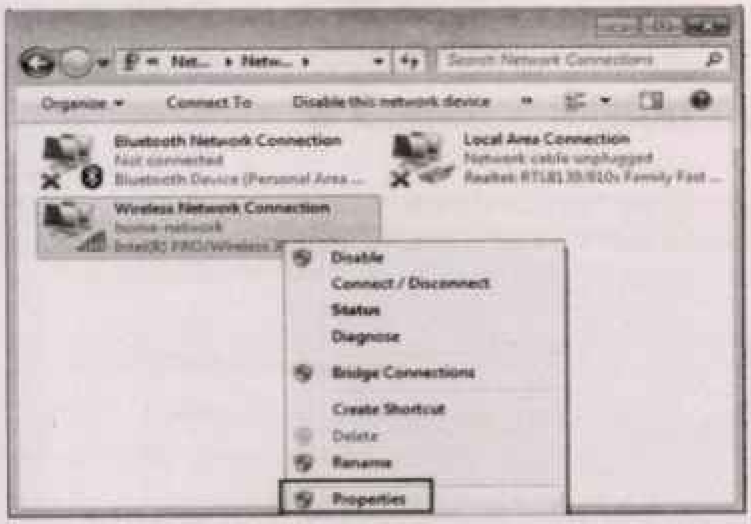
Control Panel Window

3. Network and Sharing Center window will appear, and then click change adapter settings. See figure


Netwo... ▸ Network and Sharing Center
Search Control Panel
Control Panel Home
Manage wireless networks
Change adapter settings
Change advanced sharing settings
View your basic network information and set up connections
(This computer)
Home network
Internet
View your active networks
Connect

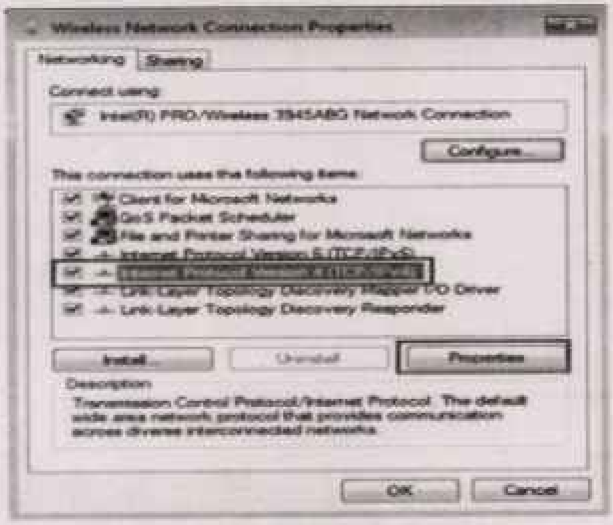
Network and Sharing Center window.

4. Network Connections window will appear. Here you can right click on the network adapter (can be wireless adapter or wired Ethernet adapter) that you wish to configure and click Properties. See figure 75.


Net... ▸ Netw... ▸
Search Network Connections
Organize ▾
Connect To
Disable this network device
Bluetooth Network Connection
Not connected
Bluetooth Device (Personal Area ...
Local Area Connection
Network cable unplugged
Realtek RTL8139/810x Family Fast ...
Wireless Network Connection
home-network
Intel(R) PRO/Wireless 3...
Disable
Connect / Disconnect
Status
Diagnose
Bridge Connections
Create Shortcut
Delete
Rename
Properties

Network Connections window

5. In the Network Connection Properties window, tick on Internet Protocol Version 4 (TCP/IPv4) and click Properties. See figure .


Wireless Network Connection Properties
Networking
Sharing
Connect using:
Intel(R) PRO/Wireless 3945ABG Network Connection
Configure...
This connection uses the following items:
Install...
Uninstall
Properties
Description
OK
Cancel

☑ Client for Microsoft Networks
☑ QoS Packet Scheduler
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol Version 6 (TCP/IPv6)
☑ Internet Protocol Version 4 (TCP/IPv4)
☑ Link-Layer Topology Discovery Mapper I/O Driver
☑ Link-Layer Topology Discovery Responder

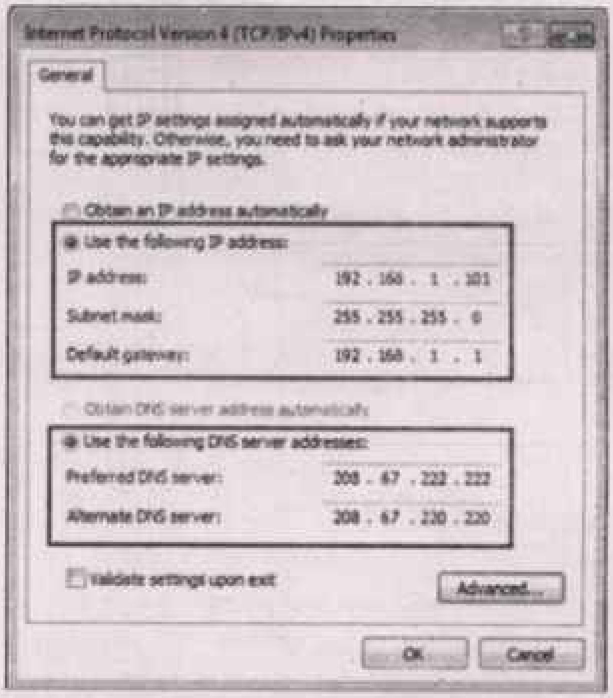
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

Network Connection Properties window

6. Assigning IP Address

   a) After clicking properties, TCP/IPv4 window appear. (See figure) For manual IP Assigning we can now key in the IP address, Subnet mask, Default gateway and DNS servers. IP address of your computer must be unique. None of the 2 computers in the same network can share same IP address, because it will cause IP address conflict.

Notes



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 101

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 1 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 208 . 67 . 222 . 222

Alternate DNS server: 208 . 67 . 220 . 220

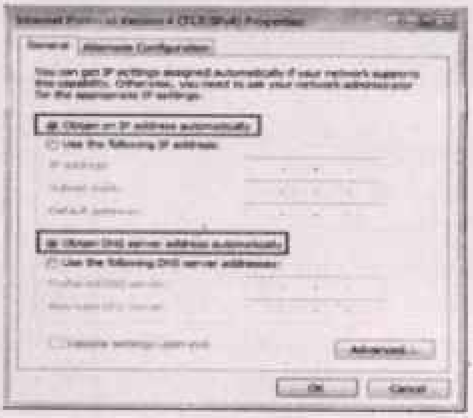
☐ Validate settings upon exit

TCP/IPv4 window

Note: Default gateway is a router that can route the traffic to the other network or Internet. DNS server is an application server that can translate URL to IP address. Check with your ISP on what DNS servers you should use. If not, you can try this free Opendns or Google DNSservers.

b) IP Assigned by DHCP server

If you have DHCP server setup on your router or you have dedicated DHCP server, your computer can be assigned IP address and other network information automatically by selecting Obtain an IP addressm automatically and Obtain DNS server address automatically. See figure.



Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address:

Subnet mask:

Default gateway:

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

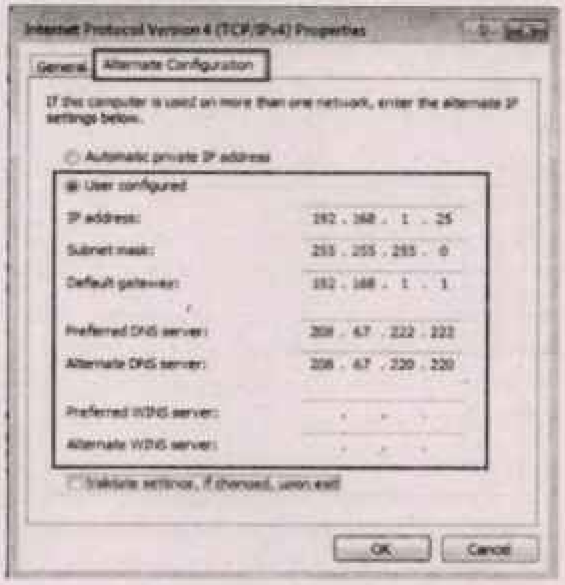
Preferred DNS server:

Alternate DNS server:

☐ Validate settings upon exit

IP Assigned by DHCP server

Note: If you have a laptop, and you use static IP at home and the IP assigned by DHCP server at the office, you can make use of alternate configuration to set IP and network information for these 2 different networks. Set Obtain an IP address and DNS automatically on General Tab as in the figure 79 so that the laptop will be assigned IP addresses automatically at the office. After that, click Alternate Configuration tab, select User configured option and key in your home network's static IP and other network information. By setting this, when there is no IP information assigned due to no DHCP server at home, this alternate configuration will be applied automatically, so that you don□t have to spend time on configuring IP manually every time at home.



If this computer is used on more than one network, enter the alternate IP settings below.

○ Automatic private IP address

● User configured

IP address: 192 . 168 . 1 . 25

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 1 . 1

Preferred DNS server: 208 . 67 . 222 . 222

Alternate DNS server: 208 . 67 . 220 . 220

Preferred WINS server: . . .

Alternate WINS server: . . .

□ Validate settings, if changed, upon exit

Using alternate configuration

3.8 CONCEPT OF PORT

A port in networking is a software-defined number associated to a network protocol that receives or transmits communication for a specific service. A port in computer hardware is a jack or socket that peripheral hardware plugs into.

A network port is a process-specific or an application-specific software construct serving as a communication endpoint, which is used by the Transport Layer protocols of Internet Protocol suite, such as User Diagram Protocol (UDP) and Transmission Control Protocol (TCP).

A specific network port is identified by its number commonly referred to as port number, the IP address in which the port is associated with and the type of transport protocol used for the communication.

A port number is a 16-bit unsigned integer that ranges from 0 to 65535.

A port is a physical docking point using which an external device can be connected to the computer. It can also be programmatic docking point through which information flows from a program to the computer or over the Internet.

A network port which is provided by the Transport Layer protocols of Internet Protocol suite, such as Transmission Control Protocol (TCP) and User Diagram Protocol (UDP) is a number which serving endpoint communication between two computers.

To determine what protocol incoming traffic should be directed to, different port numbers are used. They allow a single host with a single IP address to run network services. Each port number have a distinct service, and for each host can have 65535 ports per IP address. Internet Assigned Numbers Authority (IANA) is responsible for managing the uses of these ports. There are three categories for ports by IANA –

If you could consider all the addresses a computer processor could talk to as the address space, then certain addresses will have specialized purposes. For example, an address could be a memory address or another address could be a port address. A port address could be used to talk to external processes or devices. A port then, is simply a hole in the processor address space where data can be sent and received from.

Any networking process or device uses a specific network port to transmit and receive data. This means that it listens for incoming packets whose destination port matches that port number, and/or transmits outgoing packets whose source port is set to that port number. Processes may use multiple network ports to receive and send data.

The port numbers that range from 0 to 1023 are known as well-known port numbers. Well-known port numbers are allotted to standard server processes, such as FTP and Telnet. They are referenced by system processes providing widely used types of network services. Specific port numbers are assigned and recorded by the Internet Assigned Numbers Authority (IANA).

However, in common practice, there is much unofficial use of both officially assigned numbers and unofficial numbers. Additionally, some network ports are in use for multiple applications and may be designated as either official or unofficial.

Some well-known ports are –

Port number	Transport protocol	Service name
20,21	TCP	File Transfer Protocol
23	TCP	Telnet
25	TCP	Simple Mail Transfer Protocol(SMTP)
53	TCP and UDP	Domain Name System(DNS)
110	TCP	Post Office Protocol(POP3)
123	UDP	Network Time Protocol(NTP)

- 1024 to 49151 – registered ports assigned by IANA to a specific service upon application by a requesting entity.
- 49152 to 65 535 – dynamic (private, high) ports range from 49,152 to 65,535. Can be used by private or customer service or temporal purposes.

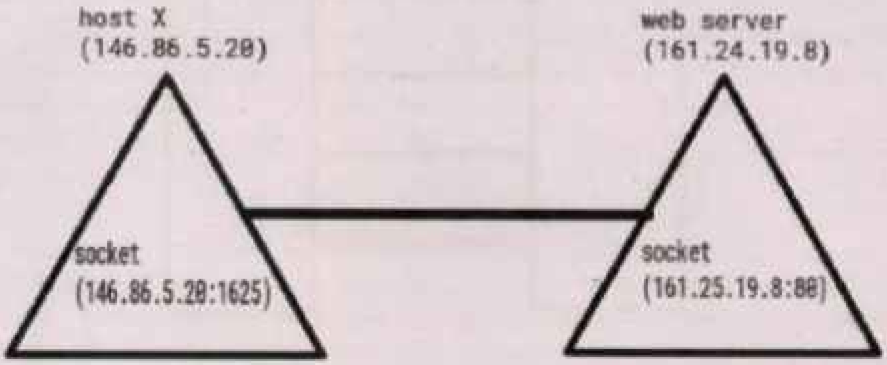
3.9 SOCKET

A socket is one endpoint of a two way communication link between two programs running on the network. The socket mechanism provides a means of inter-process communication

(IPC) by establishing named contact points between which the communication take place.

Like 'Pipe' is used to create pipes and sockets is created using 'socket' system call. The socket provides bidirectional FIFO Communication facility over the network. A socket connecting to the network is created at each end of the communication. Each socket has a specific address. This address is composed of an IP address and a port number.

Socket are generally employed in client server applications. The server creates a socket, attaches it to a network port addresses then waits for the client to contact it. The client creates a socket and then attempts to connect to the server socket. When the connection is established, transfer of data takes place.



Types of Sockets :

There are two types of Sockets: the datagram socket and the stream socket.

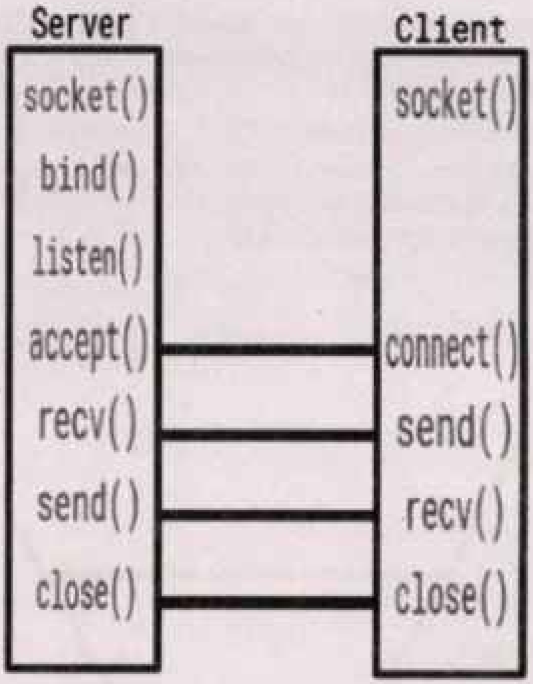
Datagram Socket:

This is a type of network which has connection less point for sending and receiving packets. It is similar to mailbox. The letters (data) posted into the box are collected and delivered (transmitted) to a letterbox (receiving socket).

Stream Socket

In Computer operating system, a stream socket is type of interprocess communications socket or network socket which provides a connection-oriented, sequenced, and unique flow of data without record boundaries with well defined mechanisms for creating and destroying connections and for detecting errors. It is similar to phone. A connection is established between the phones (two ends) and a conversation (transfer of data) takes place.

Notes



Function Call	Description
Create()	To create a socket
Bind()	It's a socket identification like a telephone number to contact
Listen()	Ready to receive a connection
Connect()	Ready to act as a sender
Accept()	Confirmation, it is like accepting to receive a call from a sender
Write()	To send data
Read()	To receive data
Close()	To close a connection

3.10 ASYNCHRONOUS TRANSFER MODE (ATM)

Driven by the integration of services and performance requirements of both telephony and data networking: "broadband integrated service vision" (B-ISON).

- Telephone networks support a single quality of service and are expensive to boot.
- Internet supports no quality of service but is flexible and cheap.
- ATM networks were meant to support a range of service qualities at a reasonable cost-intended to subsume both the telephone network and the Internet.

Asynchronous Transfer Mode (ATM)

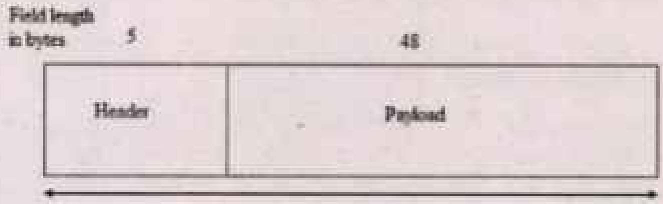
It is an International Telecommunication Union- Telecommunications Standards Section (ITU-T) efficient for call relay and it transmits all information including multiple service types such as data, video, or voice which is conveyed in small fixed-size packets called cells. Cells are transmitted asynchronously and the network is connection-oriented.

ATM is a technology that has some event in the development of broadband ISDN in the 1970s and 1980s, which can be considered an evolution of packet switching. Each cell is 53 bytes long – 5 bytes header and 48 bytes payload. Making an ATM call requires first sending a message to set up a connection.

Subsequently, all cells follow the same path to the destination. It can handle both constant rate traffic and variable rate traffic. Thus it can carry multiple types of traffic with end-to-end quality of service. ATM is independent of a transmission medium, they may be sent on a wire or fiber by themselves or they may also be packaged inside the payload of other carrier systems. ATM networks use "Packet" or "cell" Switching with virtual circuits. Its design helps in the implementation of high-performance multimedia networking.

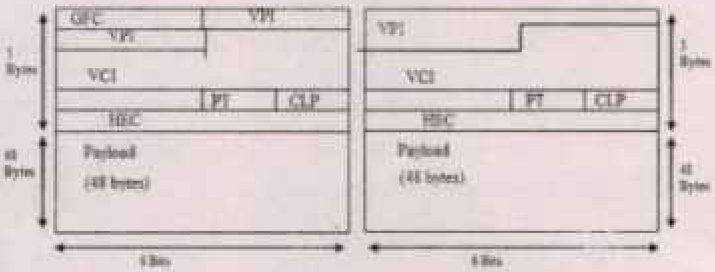
ATM Cell Format

As information is transmitted in ATM in the form of fixed-size units called cells. As known already each cell is 53 bytes long which consists of a 5 bytes header and 48 bytes payload.



ATM Cell Format

Asynchronous Transfer Mode can be of two format types which are as follows:



UNI Cell Format

NNI Cell Format

UNI Header: This is used within private networks of ATMs for communication between ATM endpoints and ATM switches. It includes the Generic Flow Control (GFC) field.

Notes

NNI Header: is used for communication between ATM switches, and it does not include the Generic Flow Control(GFC) instead it includes a Virtual Path Identifier (VPI) which occupies the first 12 bits.

Working of ATM

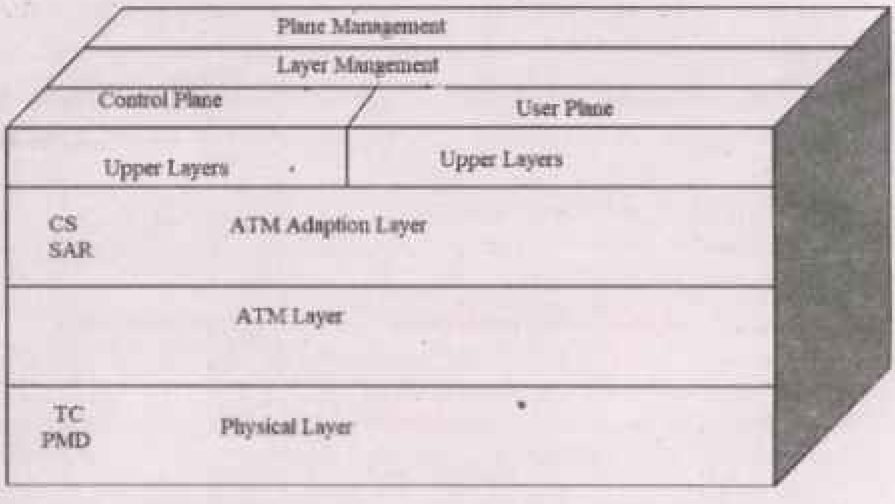
ATM standard uses two types of connections. i.e., Virtual path connections (VPCs) which consist of Virtual channel connections (VCCs) bundled together which is a basic unit carrying a single stream of cells from user to user. A virtual path can be created end-to-end across an ATM network, as it does not rout the cells to a particular virtual circuit. In case of major failure, all cells belonging to a particular virtual path are routed the same way through the ATM network, thus helping in faster recovery.

Switches connected to subscribers use both VPIs and VCIs to switch the cells which are Virtual Path and Virtual Connection switches that can have different virtual channel connections between them, serving the purpose of creating a virtual trunk between the switches which can be handled as a single entity. Its basic operation is straightforward by looking up the connection value in the local translation table determining the outgoing port of the connection and the new VPI/VCI value of connection on that link.

ATM vs DATA Networks (Internet)

ATM is a "virtual circuit" based: the path is reserved before transmission. While Internet Protocol (IP) is connectionless and end-to-end resource reservations are not possible. RSVP is a new signaling protocol on the internet.

- ATM Cells: Fixed or small size and Tradeoff is between voice or data. While IP packets are of variable size.
- Addressing: ATM uses 20-byte global NSAP addresses for signaling and 32-bit locally assigned labels in cells. While IP uses 32-bit global addresses in all packets.
- ATM Layers:



ATM Adaption Layer (AAL):

It is meant for isolating higher-layer protocols from details of ATM processes and prepares for conversion of user data into cells and segments it into 48-byte cell payloads. AAL protocol excepts transmission from upper-layer services and helps them in mapping applications, e.g., voice, data to ATM cells.

Physical Layer

It manages the medium-dependent transmission and is divided into two parts physical medium-dependent sublayer and transmission convergence sublayer. The main functions are as follows:

- It converts cells into a bitstream.
- It controls the transmission and receipt of bits in the physical medium.
- It can track the ATM cell boundaries.
- Look for the packaging of cells into the appropriate type of frames.

ATM Layer

It handles transmission, switching, congestion control, cell header processing, sequential delivery, etc., and is responsible for simultaneously sharing the virtual circuits over the physical link known as cell multiplexing and passing cells through an ATM network known as cell relay making use of the VPI and VCI information in the cell header.

ATM Applications:

ATM WANs

It can be used as a WAN to send cells over long distances, a router serving as an end-point between ATM network and other networks, which has two stacks of the protocol.

Multimedia virtual private networks and managed services– It helps in managing ATM, LAN, voice, and video services and is capable of full-service virtual private networking, which includes integrated access to multimedia.

Frame relay backbone – Frame relay services are used as a networking infrastructure for a range of data services and enabling frame-relay ATM service to Internetworking services.

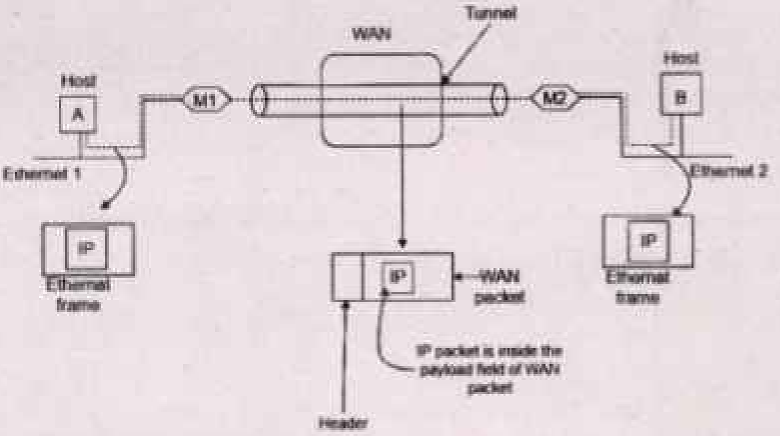
Residential broadband networks – ATM is by choice provides the networking infrastructure for the establishment of residential broadband services in the search of highly scalable solutions.

Carrier infrastructure for telephone and private line networks – To make more effective use of SONET/SDH fiber infrastructures by building the ATM infrastructure for carrying the telephonic and private-line traffic.

Notes

3.11 TUNNELING

A technique of internetworking called Tunneling is used when source and destination networks of same type are to be connected through a network of different type. For example, let us consider an Ethernet to be connected to another Ethernet through a WAN as:



The task is sent on an IP packet from host A of Ethernet-1 to the host B of ethernet-2 via a WAN.

Sequence of events

Host A construct a packet which contains the IP address of Host B.

It then inserts this IP packet into an Ethernet frame and this frame is addressed to the multiprotocol router M1

Host A then puts this frame on Ethernet.

When M1 receives this frame, it removes the IP packet, inserts it in the payload packet of the WAN network layer packet and addresses the WAN packet to M2. The multiprotocol router M2 removes the IP packet and send it to host B in an Ethernet frame.

Why is this Technique called Tunneling?

In this particular example, the IP packet does not have to deal with WAN, the host A and B also do not have to deal with the WAN. The multiprotocol routers M1 and M2 will have to understand about IP and WAN packets.

Therefore, the WAN can be imagined to be equivalent to a big tunnel extending between multiprotocol routers M1 and M2 and the technique is called Tunneling.

Tunneling uses a layered protocol model such as those of the OSI or TCP/IP protocol suite. So, in other words, when data moves from host A to B it covers all the different level of the specified protocol (OSI, TCP/IP, etc.), while moving between different levels, data conversion (encapsulation) to suit different interfaces of the particular layer is called tunneling.

3.12 VIRTUAL PRIVATE NETWORK

VPN stands for "Virtual Private Network" and describes the opportunity to establish a protected network connection when using public networks. VPNs encrypt your internet traffic and disguise your online identity. This makes it more difficult for third parties to track your activities online and steal data. The encryption takes place in real time.

How does a VPN work?

A VPN hides your IP address by letting the network redirect it through a specially configured remote server run by a VPN host. This means that if you surf online with a VPN, the VPN server becomes the source of your data.

This means your Internet Service Provider (ISP) and other third parties cannot see which websites you visit or what data you send and receive online. A VPN works like a filter that turns all your data into "gibberish". Even if someone were to get their hands on your data, it would be useless.

Benefits of a VPN Connection

A VPN connection disguises your data traffic online and protects it from external access. Unencrypted data can be viewed by anyone who has network access and wants to see it. With a VPN, hackers and cyber criminals can't decipher this data.

Secure encryption: To read the data, you need an encryption key. Without one, it would take millions of years for a computer to decipher the code in the event of a brute force attack. With the help of a VPN, your online activities are hidden even on public networks.

Disguising your whereabouts: VPN servers essentially act as your proxies on the internet. Because the demographic location data comes from a server in another country, your actual location cannot be determined. In addition, most VPN services do not store logs of your activities.

Some providers, on the other hand, record your behavior, but do not pass this information on to third parties. This means that any potential record of your user behavior remains permanently hidden.

Access to regional content: Regional web content is not always accessible from everywhere. Services and websites often contain content that can only be accessed from certain parts of the world. Standard connections use local servers in the country to determine your location. This means that you cannot access content at home while traveling, and you cannot access international content from home.

With VPN location spoofing , you can switch to a server to another country and effectively "change" your location.

Secure data transfer: If you work remotely, you may need to access important files on your company's network. For security reasons, this kind of information requires a secure connection. To gain access to the ne:..ork, a VPN connection is often required. VPN services connect to private servers and use encryption methods to reduce the risk of data leakage.

Why should you use a VPN connection?

Your ISP usually sets up your connection when you connect to the internet. It tracks you via an IP address. Your network traffic is routed through your ISP's servers, which can log and display everything you do online.

Your ISP may seem trustworthy, but it may share your browsing history with advertisers, the police or government, and/or other third parties. ISPs can also fall victim to attacks by cyber criminals: If they are hacked, your personal and private data can be compromised.

This is especially important if you regularly connect to public Wi-Fi networks. You never know who might be monitoring your internet traffic and what they might steal from you, including passwords, personal data, payment information, or even your entire identity.

What should a good VPN do?

You should rely on your VPN to perform one or more tasks. The VPN itself should also be protected against compromise. These are the features you should expect from a comprehensive VPN solution:

Encryption of your IP address: The primary job of a VPN is to hide your IP address from your ISP and other third parties. This allows you to send and receive information online without the risk of anyone but you and the VPN provider seeing it.

Encryption of protocols: A VPN should also prevent you from leaving traces, for example, in the form of your internet history, search history and cookies. The encryption of cookies is especially important because it prevents third parties from gaining access to confidential information such as personal data, financial information and other content on websites.

Kill switch: If your VPN connection is suddenly interrupted, your secure connection will also be interrupted. A good VPN can detect this sudden downtime and terminate preselected programs, reducing the likelihood that data is compromised.

Two-factor authentication: By using a variety of authentication methods, a strong VPN checks everyone who tries to log in. For example, you might be prompted to enter a password, after which a code is sent to your mobile device. This makes it difficult for uninvited third parties to access your secure connection.

History of VPNs

Since humans have been using the internet, there has been a movement to protect and encrypt internet browser data. The US Department of Defense already got involved in projects working on the encryption of internet communication data back in the 1960s.

The Predecessors of the VPN

Their efforts led to the creation of ARPANET (Advanced Research Projects Agency Network), a packet switching network, which in turn led to the development of the Transfer Control Protocol/Internet Protocol (TCP/IP).

The TCP/IP had four levels: Link, internet, transport and application. At the internet level, local networks and devices could be connected to the universal network – and this is where the risk of exposure became clear. In 1993, a team from Columbia University and AT&T Bell Labs finally succeeded in creating a kind of first version of the modern VPN, known as swIPe: Software IP encryption protocol.

In the following year, Wei Xu developed the IPSec network, an internet security protocol that authenticates and encrypts information packets shared online. In 1996, a Microsoft employee named Gurdeep Singh-Pall created a Peer-to-Peer Tunneling Protocol (PPTP).

Early VPNs

Contiguous to Singh-Pall developing PPTP, the internet was growing in popularity and the need for consumer-ready, sophisticated security systems emerged. At that time, anti-virus programs were already effective in preventing malware and spyware from infecting a computer system. However, people and companies also started demanding encryption software that could hide their browsing history on the internet.

The first VPNs therefore started in the early 2000s, but were almost exclusively used by companies. However, after a flood of security breaches, especially in the early 2010s, the consumer market for VPNs started to pick up.

VPNs and their Current Use

According to the GlobalWebIndex, the number of VPN users worldwide increased more than fourfold between 2016 and 2018. In countries such as Thailand, Indonesia and China, where internet use is restricted and censored, one in fiveinternet users uses a VPN.

In the USA, Great Britain and Germany, the proportion of VPN users is lowerat around 5%, but is growing.

One of the biggest drivers for VPN adoption in recent years has been the increasing demand for content with geographical access restrictions.

For example, video streaming services such as Netflix or YouTube make certain videos available only in certain countries. With contemporary VPNs, you can encrypt your IP address so that you appear to be surfing from another country, enabling you to access this content from anywhere.

How to surf securely with a VPN

A VPN encrypts your surfing behavior, which can only be decoded with the help of a key. Only your computer and the VPN know this key, so your ISP cannot recognize where you are surfing. Different VPNs use different encryption processes, but generally function in three steps:

- Once you are online, start your VPN. The VPN acts as a secure tunnel between you and the internet. Your ISP and other third parties cannot detect this tunnel.
- Your device is now on the local network of the VPN, and your IP address can be changed to an IP address provided by the VPN server.
- You can now surf the internet at will, as the VPN protects all your personal data.

Notes

Kind of VPNs

There are many different types of VPNs, but you should definitely be familiar with the three main types:

SSL VPN

Often not all employees of a company have access to a company laptop they can use to work from home. During the corona crisis in Spring 2020, many companies faced the problem of not having enough equipment for their employees. In such cases, use of a private device (PC, laptop, tablet, mobile phone) is often resorted to. In this case, companies fall back on an SSL-VPN solution, which is usually implemented via a corresponding hardware box.

The prerequisite is usually an HTML-5-capable browser, which is used to call up the company's login page. HTML-5 capable browsers are available for virtually any operating system. Access is guarded with a username and password.

Site-to-site VPN

A site-to-site VPN is essentially a private network designed to hide private intranets and allow users of these secure networks to access each other's resources.

A site-to-site VPN is useful if you have multiple locations in your company, each with its own local area network (LAN) connected to the WAN (Wide Area Network). Site-to-site VPNs are also useful if you have two separate intranets between which you want to send files without users from one intranet explicitly accessing the other.

Site-to-site VPNs are mainly used in large companies. They are complex to implement and do not offer the same flexibility as SSL VPNs. However, they are the most effective way to ensure communication within and between large departments.

Client-to-Server VPN

Connecting via a VPN client can be imagined as if you were connecting your home PC to the company with an extension cable. Employees can dial into the company network from their home office via the secure connection and act as if they were sitting in the office. However, a VPN client must first be installed and configured on the computer.

This involves the user not being connected to the internet via his own ISP, but establishing a direct connection through his/her VPN provider. This essentially shortens the tunnel phase of the VPN journey. Instead of using the VPN to create an encryption tunnel to disguise the existing internet connection, the VPN can automatically encrypt the data before it is made available to the user.

This is an increasingly common form of VPN, which is particularly useful for providers of insecure public WLAN. It prevents third parties from accessing and compromising the network connection and encrypts data all the way to the provider. It also prevents ISPs from accessing data that, for whatever reason, remains unencrypted and bypasses any restrictions on the user's internet access (for instance, if the government of that country restricts internet access).

The advantage of this type of VPN access is greater efficiency and universal access to company resources. Provided an appropriate telephone system is available, the employee can, for example, connect to the system with a headset and act as if he/she were at their company workplace.

For example, customers of the company cannot even tell whether the employee is at work in the company or in their home office.

How do I install a VPN on my computer?

Before installing a VPN, it is important to be familiar with the different implementation methods:

VPN client

Software must be installed for standalone VPN clients. This software is configured to meet the requirements of the endpoint. When setting up the VPN, the endpoint executes the VPN link and connects to the other endpoint, creating the encryption tunnel.

In companies, this step usually requires the entry of a password issued by the company or the installation of an appropriate certificate. By using a password or certificate, the firewall can recognize that this is an authorized connection. The employee then identifies him/herself by means of credentials known to him/her.

Browser extensions

VPN extensions can be added to most web browsers such as Google Chrome and Firefox. Some browsers, including Opera, even have their own integrated VPN extensions. Extensions make it easier for users to quickly switch and configure their VPN while surfing the internet.

However, the VPN connection is only valid for information that is shared in this browser. Using other browsers and other internet uses outside the browser (e.g. online games) cannot be encrypted by the VPN.

While browser extensions are not quite as comprehensive as VPN clients, they may be an appropriate option for occasional internet users who want an extra layer of internet security. However, they have proven to be more susceptible to breaches.

Users are also advised to choose a reputable extension, as data harvesters may attempt to use fake VPN extensions. Data harvesting is the collection of personal data, such as what marketing strategists do to create a personal profile of you. Advertising content is then personally tailored to you.

Router VPN

If multiple devices are connected to the same internet connection, it may be easier to implement the VPN directly on the router than to install a separate VPN on each device. A router VPN is especially useful if you want to protect devices with an internet connection that are not easy to configure, such as smart TVs. They can even help you access geographically restricted content through your home entertainment systems.

Notes

A router VPN is easy to install, always provides security and privacy, and prevents your network from being compromised when insecure devices log on. However, it may be more difficult to manage if your router does not have its own user interface. This can lead to incoming connections being blocked.

Company VPN

A company VPN is a custom solution that requires personalized setup and technical support. The VPN is usually created for you by the company's IT team. As a user, you have no administrative influence from the VPN itself and your activities and data transfers are logged by your company.

This allows the company to minimize the potential risk of data leakage. The main advantage of a corporate VPN is a fully secure connection to the company's intranet and server, even for employees who work outside the company using their own internet connection.

Using a VPN on my Smartphone

There are a number of VPN options for smartphones and other internet-connected devices. A VPN can be essential for your mobile device if you use it to store payment information or other personal data or even just to surf the internet. Many VPN providers also offer mobile solutions - many of which can be downloaded directly from Google Play or the Apple App Store, such as Kaspersky VPN Secure Connection.

VPN is Secure

It is important to note that VPNs do not function like comprehensive anti-virus software. While they protect your IP and encrypt your internet history, a VPN connection does not protect your computer from outside intrusion. To do this, you should definitely use anti-virus software such as Kaspersky Internet Security . Because using a VPN on its own does not protect you from Trojans, viruses, bots or other malware.

Once the malware has found its way onto your device, it can steal or damage your data, whether you are running a VPN or not. It is therefore important that you use a VPN together with a comprehensive anti-virus program to ensure maximum security.

Selecting a secure VPN provider

It is also important that you choose a VPN provider that you can trust. While your ISP cannot see your internet traffic, your VPN provider can. If your VPN provider is compromised, so are you. For this reason, it is crucial that you choose a trusted VPN provider to ensure both the concealment of your internet activities and ensure the highest level of security.

VPN connection on your smartphone

As already mentioned, there are also VPN connections for Android smartphones and iPhones. Fortunately, smartphone VPN services are easy to use and generally include the following:

The installation process usually only downloads one app from the iOS App Store or Google Play Store. Although free VPN providers exist, it's wise to choose a professional provider when it comes to security.

The setup is extremely user-friendly, as the default settings are already mostly designed for the average smartphone user. Simply log in with your account. Most apps will then guide you through the key functions of the VPN services.

Switching on the VPN literally works like a light switch for many VPN apps. You will probably find the option directly on the home screen.

Server switching is usually done manually if you want to fake your location. Simply select the desired country from the offer.

Advanced setup is available for users requiring a higher degree of data protection. Depending on your VPN, you can also select other protocols for your encryption method. Diagnostics and other functions may also be available in your app. Before you subscribe, learn about these features to find the right VPN for your needs.

In order to surf the internet safely from now on, all you have to do is first activate the VPN connection through the app.

But keep the following in mind: A VPN is only as secure as the data usage and storage policies of its provider. Remember that the VPN service transfers your data to their servers and these servers connect over the internet on your behalf. If they store data logs, make sure that it is clear for what purpose these logs are stored. Serious VPN providers usually put your privacy first and foremost. You should therefore choose a trusted provider such as Kaspersky Secure Connection .

Remember that only internet data is encrypted. Anything that does not use a cellular or Wi-Fi connection will not be transmitted over the internet. As a result, your VPN will not encrypt your standard voice calls or texts.

A VPN connection establishes a secure connection between you and the internet. Via the VPN, all your data traffic is routed through an encrypted virtual tunnel. This disguises your IP address when you use the internet, making its location invisible to everyone. A VPN connection is also secure against external attacks. That's because only you can access the data in the encrypted tunnel – and nobody else can because they don't have the key. A VPN allows you to access regionally restricted content from anywhere in the world. Many streaming platforms are not available in every country. You can still access them using the VPN. VPN solutions from Kaspersky are available for both Windows PCs and Apple Macs.

There are now also many providers of VPN connections for smartphones which keep mobile data traffic anonymous. You can find certified providers in the Google Play Store or the iOS App Store. However, remember that only your data traffic on the internet is anonymized and protected by using a VPN. The VPN connection does not protect you from hacker attacks, Trojans, viruses or other malware. You should therefore rely on an additional trusted anti-virus software.

3.13 NETWORK OPERATING SYSTEMS

A network operating system (NOS) is a computer operating system (OS) that is designed primarily to support workstations, personal...

The basic definition of an operating system is that the operating system is the interface between the computer hardware and the user. And in daily life, we use the operating system

Notes

on our devices which provides a good GUI, and many more features with it. Similarly, a network operating system(NOS) is software that connects multiple devices and computers on the network and allows them to share resources on the network. Let's see what are the functions of the network operating system.

Functions of the NOS:

Following are the main functions of NOS :

- Creating and managing user accounts on the network.
- Controlling access to resources on the network.
- Provide communication services between the devices on the network.
- Monitor and troubleshoot the network.
- Configuring and Managing the resources on the network.

Now let's see the type of Network Operating systems.

Types of Network Operating Systems:

There are mainly two types of networks, one is peer to peer and another is client/server. Now let's see each type one by one.

- **Peer to Peer** – Peer-to-peer network operating systems allow sharing resources and files with small-sized networks and having fewer resources. In general, peer-to-peer network operating systems are used on LAN.
- **Client/server** -Client-server network operating systems provide users access to resources through the central server. This NOS is too expensive to implement and maintain. This operating system is good for the big networks which provide many services.

Features of Network Operating Systems:

Let's see what are the functions of the network operating system.

- Printers and application sharing on the network.
- File systems and database sharing.
- Provide good security by using functionality like user authentication and access control.
- Create backups of data.
- Inter-networking.

Now let's see what are the advantages of NOS.

Advantages of Network operating systems :

- Highly stable due to central server.
- Provide good security.
- Upgradation of new technology and hardware can be easily implemented in the network.

Provide remote access to servers from different locations.

Disadvantages of Network operating systems :

- Depend on the central location to perform the operations.
- High cost to buying server.
- Regular updating and maintenance are required.

Now let's see what are the examples of network operating systems.

Following are the examples of network operating systems.

- Microsoft Windows Server
- UNIX/Linux
- Artisoft's LANtastic
- Banyan's VINES
- Unix;

Generally speaking, a network lets two or more computers communicate and work together. Partly because of its open design, UNIX has been one of the operating systems where a lot of networking development is done. Just as there are different versions of UNIX, there are different ways and programs to use networks from UNIX. We don't cover networking in this book (1.32).

A worldwide network of computers. Internet users can transfer files, log into other computers, and use a wide range of programs and services. WWW The World Wide Web is a fast-growing set of information servers on the Internet. The servers are linked into a hypertext web of documents, graphics, sound, and more. Point-and-click browser programs turn that hypertext into an easy-to-use Internet interface. (For many people, the Web is the Internet. But UNIX lets you do much more.) mail A UNIX program that's been around for years, long before networking was common, is mail.

It sends electronic memos, usually called email messages , between a user and one or more other users. When you send email, your message waits for the other user(s) to start their own mail program. The people who get your message can file it, print it, reply to it, forward it to other people, and much more.

System programs can send you mail to tell you about problems or give you information. You can send mail to programs, to ask them for information. Worldwide mailing lists connect users into discussion groups.

There's more, of course. There are zillions of mail programs for UNIX-some standard, some from vendors, and many freely available. The more common email programs include mailx, Pine, mush, elm, and MH (a package made up of many utilties including comp, inc, show, and so on).

Find one that's right for you and use it! ftp The ftp program is one way to transfer files between your computer and another computer with TCP/IP, often over the Internet network. ftp requires a username and password on the remote computer.

Anonymous ftp (52.7) uses the ftp program and a special restricted account named anonymous on the remote computer. It's usually used for transferring freely available files

Notes

and programs from central sites to users at many other computers. UUCP UNIX-to-UNIX Copy is a family of programs (uucp (52.7) , uux , uulog , and others) for transferring files and email between computers.

UUCP is usually used with modems over telephone lines. Usenet Usenet isn't exactly a network. It's a collection of thousands of computers worldwide that exchange files called news articles . This "net news" system has hundreds of interactive discussion groups, electronic bulletin boards, for discussing everything from technical topics to erotic art. telnet This utility logs you into a remote computer over a network (such as the Internet) using TCP/IP. You can work on the remote computer as if it were your local computer.

The telnet program is available on many operating systems; telnet can log you into other operating systems from your UNIX host and vice versa. A special version of telnet called tn3270 will log into IBM mainframes. rlogin Similar to telnet but mostly used between UNIX systems.

Special setups, including a file named .rhosts in your remote home directory, let you log into the remote computer without typing your password. rcp A " r emote cp " program for copying files between computers. It has the same command-line syntax as cp except that hostnames are added to the remote pathnames. rsh Starts a " r emote sh ell" to run a command on a remote system without needing to log in interactively. NFS NFS isn't a user utility.

The Network FileSystem and related packages like NIS (the Network Information Service) let your system administrator mount remote computers' filesystems onto your local computer. You can use the remote filesystem as easily as if it were on your local computer. write Sends messsages to another user's screen.

Two users can have a discussion with write. talk A more sophisticated program than write , talk splits the screen into two pieces and lets users type at the same time if they want to. talk can be used over networks, though not all versions of talk can talk to one another. If you'd like more information, there are quite a few books about networking.

Some Nutshell Handbooks on networking and communications include The Whole Internet User's Guide and Catalog - ail, Usenet, ftp , telnet , and more); Using Usenet ; !%@:: The Directory of Electronic Mail Addressing & Networks ; and many more advanced books for programming and administration. docstore.mik.ua/orelly/unix/upt/ch01_33.htm

3.14 LINUX

As you get started learning about Linux, you'll likely have many of the same questions that thousands of other people have had since the beginning of Linux time. For that reason, we'll start this chapter by answering the most common questions about Linux.

Networking is an essential part as we start learning about any operating system. Networks can be as small as two computers connected at your home and as large as in a large company or connected systems worldwide known as Internet.

Linux operating system has a very strong set of networking instruments to provide and manage routing, bridging, virtual networks and monitoring.

History of Linux

Before we dive into Linux, let's first take a step back in history. The creation of Linux starts with another operating system known as UNIX, which was first released in 1971. In 1983, the GNU Project (which stood for "GNU's not Unix") was started to create a complete UNIXcompatible operating system. Efforts stalled, and the project was missing a kernel. Around 1987, a UNIX-like operating system for students was released called MINIX, but its licensing prevented it from being distributed freely.

Linus Torvalds) at the University of Helsinki in Finland was frustrated by the licensing of MINIX and began working on his own operating system kernel. His kernel, released in 1991, when combined with the GNU applications and open-source licensing, became the Linux operating system we know today.

Why should you learn Linux

What if you don't know Linux and are asking yourself, "Is this book really worth my time?" The short answer is a resounding YES, but to back that up, let me give you six good reasons why you should invest some of your time to learn Linux.

1. Linux is the Future

Although Linux has been around for over 25 years, it has enjoyed a continuous rise in business-critical usage, and many see Linux as being the most popular operating system for the future. The reason as to why Linux is the lingua franca of the modern data center relates to the points below.

2. Linux is on Everything

Linux runs more than two-thirds of the servers on the Internet, all Android phones, most consumer network gear, such as NetGear and Linksys devices, 99% of the top supercomputers in the world, many Internet of Things (IoT) devices, Tesla cars, and even PlayStation gaming consoles.

3. Linux is Adaptable

The very reason everything is on Linux is because it's such an adaptable operating system. Thanks to Linux's modularity and open-source nature, you can choose the pieces you need for your product or service and develop any pieces that may not already exist. You can install tiny versions of Linux for specialized use cases (such as operating water sprinklers in the gorilla exhibit at the zoo), modify it to work on appliances that route packets across a large enterprise network, or use it as your desktop operating system. Your choices are practically endless.

4. Linux has a strong community and ecosystem

Linux has been so successful mainly because of the strong community and ecosystem that surrounds it. There are Linux contributors (developers who write code to make the product

Notes

better); Linux forums and communities; Linux instructors; Linux training options; Linux blogs; Linux third-party tools; Linux distributions; Linux conferences; and even Linux books such as this one!

5. Linux is fun!

Linux is a lot of fun because you can do just about anything with it. Linux is commonly used in Internet of Things (IoT) projects; it runs on tiny Raspberry Pi computers commonly used by hobbyists, and it even makes a great operating system on your laptop or desktop computer.

More examples of the many uses of Linux are found throughout the book.

6. Linux is open-source and sometimes free

Linux is open-source, meaning that the original source code is made freely available and may be redistributed and modified. That said, there are paid and fully supported commercial editions available, too. The open nature of Linux has made it the adaptable OS of the future, allowing it to run on everything, and has resulted in the creation of a strong ecosystem.

The Components that Comprise the Linux

Operating System

Linux is an open-source OS that can be installed on a variety of different types of hardware to allow you to develop software, run applications, and more. At the heart of Linux is the kernel. Linux was developed in C and assembly language to run on i386 personal computers, but it has since been ported to more hardware than just about any other operating system in history. Today, Linux is the most installed operating system globally. In fact, the Space X Falcon 9 rocket and the International Space Station both use Linux!

Linux is typically administered from a command line interface (CLI), also known as a shell. Besides the kernel, which manages the hardware and software processes, Linux distributions include a collection of Linux software, such as device drivers for accessing and controlling hardware, shared libraries, applications, and system daemons, which run the in background and respond to network requests.

Applications are installed from packages, which contain the application itself and metadata about the application.

Benefits of Using Linux

Besides the fact that Linux is a great operating system, is continually being enhanced, and has a huge community following, Linux has gained such tremendous popularity because there are so many different benefits to using it. Some of these benefits include:

Consistent operating model. No matter what version or distribution of Linux you use, whether you're on a supercomputer or a tiny embedded device, the general operation of Linux is the same no matter where you go. What this means is that, with some exceptions, the command line syntax is similar, process management is similar, basic network administration is similar, and applications can be (relatively) easily ported between distributions. The end result of this consistent operating model is a cost savings generated by greater staff efficiency and flexibility.

Scalability. At this point, you already know that Linux is eminently scalable and is able to run on everything from wristwatches to supercomputers to globally distributed computing clusters. Of course, the benefit of this scalability isn't just the device mix, but also that its basic functionality – command line tools, configuration, automation, and codecompatibility – remains the same no matter where you're using it.

- Open-source and community optimized. With Linux's open-source, freely available nature, you might be concerned about future enhancements, bug fixes, and support.
- Fortunately, you can put those worries aside. If you look at the Linux kernel alone, with its 22 million lines of code, you'll find a strong community developing it behind the scenes. In 2016, one report said that over 5,000 individual developers representing 500 different corporations around the world contributed to enhancements in the Linux kernel, not to mention all the other surrounding applications and services. A staggering 13,500 developers from more than 1,300 companies have contributed to the Linux kernel since 2005.
- You might wonder why commercial entities contribute code to Linux. While many open-source advocates see the open-source nature of Linux as purely idealistic, commercial contribution of code is actually a strategic activity. In this sense, the for-profit companies who are dependent on Linux contribute their changes to the core to ensure that those changes carry forward into future distributions without having to maintain them indefinitely.
- Full function networking. Over the years, Linux has built up a strong set of networking capabilities, including networking tools for providing and managing routing, bridging, DNS, DHCP, network troubleshooting, virtual networking, and network monitoring.
- Package management. The Linux package management system allows you to easily install new services and applications with just a few simple commands.

Linux Package Management

A Linux package management system is a tool that helps Linux administrators install and manage applications and extensions for the Linux operating system. Each Linux distribution carries its own package management capabilities.

A Linux package includes all the bits necessary for a new application or service to operate. The package management system can also help an administrator address any dependencies that a package may have.

A dependency is a software package necessary for another package to operate. By layering these dependencies, newly developed packages can then leverage the work of others without having to constantly reinvent the wheel.

However, maintaining dependencies can be difficult, particularly as you continue to add packages. A good package management system will ensure that all dependencies are handled at the same time that you install new packages.

Linux Used in the Enterprise

Many modern ideas in data center computing have Linux underpinnings. Here are just a few examples:

- Automation and orchestration. Automation is used to perform a common task in a programmatic/scripted way, whereas orchestration is used to automate tasks across multiple systems in a data center. Linux is being used to automate and orchestrate just about every process in the enterprise data center.
- Server virtualization. Server virtualization is the ability to run a full operating system on top of an existing bare metal server. These virtual machines (VMs) can be used to increase server utilization, simplify server testing, or lower the cost of server redundancy. The software that allows VMs to function is called a hypervisor. Linux includes an excellent hypervisor called KVM.
- Private cloud. Another open-source project called OpenStack, which also runs on Linux, has become a leading cloud management platform for creating a private cloud. With private cloud, companies can leverage many of the same advantages of public cloud (scalability, self-service, multi-tenancy, and more) while running their own IT infrastructure on-premises.
- Big data. More and more companies are having to deal with exponentially increasing amounts of data in their data center, and because Linux offers such scalability and performance, it has become the go-to operating system for crunching big data via applications like Hadoop. Even Microsoft recently announced a big data solution based on Linux.
- Containers. Linux can also be used to run containerized applications, such as Docker containers, which are being used more and more by many companies. In fact, Linux is the foundation of the modern container movement; all container packaging and orchestration relies on Linux namespace and isolation mechanisms in order to operate

Windows

The Windows networking (WNet) functions allow you to implement networking capabilities in your application without making allowances for a particular network provider or physical network implementation. This is because the WNet functions are network independent.

SUMMARY

- The most identified benefit of the OSI model is that it organizes thinking about networks and give novices, journeymen, and masters a common, computer networking language. Human communication, discussions, and collaboration can use this language to remove ambiguity and clarify intent.
- The Open Systems Interconnection (OSI) model is a reference tool for understanding data communications between any two networked systems. It divides the communications processes into seven layers. Each layer both performs specific functions to

support the layers above it and offers services to the layers below it. The three lowest layers focus on passing traffic through the network to an end system. The top four layers come into play in the end system to complete the process.

- The Open Systems Interconnect (OSI) model has seven layers. This unit describes and explains them, beginning with the 'lowest' in the hierarchy (the physical) and proceeding to the 'highest' (the application).
- The physical layer of the OSI model defines connector and interface specifications, as well as the medium (cable) requirements. Electrical, mechanical, functional, and procedural specifications are provided for sending a bit stream on a computer network. The physical layer, the lowest layer of the OSI model, is concerned with the transmission and reception of the unstructured raw bit stream over a physical medium. It describes the electrical/optical, mechanical, and functional interfaces to the physical medium, and carries the signals for all of the higher layers.
- The transport layer ensures that messages are delivered error-free, in sequence, and with no losses or duplications. It relieves the higher layer protocols from any concern with the transfer of data between them and their peers. The size and complexity of a transport protocol depends on the type of service it can get from the network layer.
- In computer networking, broadcasting is a method of transferring a message to all recipients simultaneously. Broadcasting can be performed as a high-level operation in a program, for example, broadcasting in Message Passing Interface, or it may be a low-level networking operation, for example broadcasting on Ethernet.
- Multicast is group communication where data transmission is addressed to a group of destination computers simultaneously. It can be one-to-many or many-to-many distribution. Multicast should not be confused with physical layer point-to-multipoint communication. Multicast is often employed in Internet Protocol (IP) applications of streaming media, such as IPTV and multipoint videoconferencing.
- An IP address is a unique address that identifies a device on the internet or a local network. IP stands for "Internet Protocol," which is the set of rules governing the format of data sent via the internet or local network.
- A port in networking is a software-defined number associated to a network protocol that receives or transmits communication for a specific service. A port in computer hardware is a jack or socket that peripheral hardware plugs into.
- A network port is a process-specific or an application-specific software construct serving as a communication endpoint, which is used by the Transport Layer protocols of Internet Protocol suite, such as User Diagram Protocol (UDP) and Transmission Control Protocol (TCP).
- A specific network port is identified by its number commonly referred to as port number, the IP address in which the port is associated with and the type of transport protocol used for the communication.
- A network port which is provided by the Transport Layer protocols of Internet Protocol suite, such as Transmission Control Protocol (TCP) and User Diagram Protocol (UDP) is a number which serving endpoint communication between two computers.
- A socket is one endpoint of a two way communication link between two programs running on the network. The socket mechanism provides a means of inter-process

Notes

communication (IPC) by establishing named contact points between which the communication take place.

- ATM standard uses two types of connections. i.e., Virtual path connections (VPCs) which consist of Virtual channel connections (VCCs) bundled together which is a basic unit carrying a single stream of cells from user to user.
- VPN stands for "Virtual Private Network" and describes the opportunity to establish a protected network connection when using public networks. VPNs encrypt your internet traffic and disguise your online identity.

KEY WORDS

- **Application Layer:** The application layer contains all the management information for the distributed applications. The data units here is the real user data. Active devices for internetworking are called gateways.
- **Presentation Layer:** The presentation layer is responsible for formating data in such way that it is ready for presentation to the application. This means translation of different character formats (ASCII/EBCDIC) is done here, but also text (de)compression, virtual terminal emulation and encryption/decryption. It is completely responsible for translation, formatting and the syntax selection.

REVIEW QUESTIONS

1. What are the concerns of the physical layer in the Internet model?
2. What are the responsibilities of the transport layer in the Internet model?
3. What is the difference between a port address, a logical address, and a physical address?
4. How are OSI and ISO related to each other?
5. What is point-to point communication.
6. What is the concept of port?
7. Describe the network operating systems
8. Write a brief note on Virtual Private Netwok and Tunneling.

FURTHER READINGS

1. Kurose James F., Ross Keith W. Computer Networking – By Pearson.
2. https://www.javatpoint.com/error-detection-and-correction-code-in-digital-electronics

Unit 4

Mobile Communication

Notes

Structure

4.0 LEARNING OBJECTIVES

After reading this chapter students will be able to:

- define and describe the mobile communication and wireless communication
- discuss the about mobile internet
- understand bandwidth, transmission impairment, inference and terrestrial microwave.

4.1 INTRODUCTION

Mobile Communication is the use of technology that allows us to communicate with others in different locations without the use of any physical connection (wires or cables). Mobile communication makes our life easier, and it saves time and effort.

Notes

A mobile phone (also called mobile cellular network, cell phone or hand phone) is an example of mobile communication (wireless communication). It is an electric device used for full duplex two way radio telecommunication over a cellular network of base stations known as cell site

Mobile technology is exactly what the name implies - technology that is portable. Examples of mobile IT devices include:

- laptop and notebook computers
- palmtop computers or personal digital assistants
- mobile phones and 'smart phones'
- global positioning system (GPS) devices
- wireless debit/credit card payment terminals

Mobile devices can be enabled to use a variety of communications technologies such as:

- wireless fidelity (WiFi) - a type of wireless local area network technology
- Bluetooth - connects mobile devices wirelessly
- 'third generation' (3G), global system for mobile communications (GSM) and general packet radio service (GPRS) data services - data networking services for mobile phones
- dial-up services - data networking services using modems and telephone lines
- virtual private networks - secure access to a private network

It is therefore possible to network the mobile device to a home office or the internet while traveling.

4.2 INTRODUCTION TO MOBILE COMMUNICATION

The growth in popularity of new wireless devices continuously increasing day by day. The wireless networks have the ability to start small if necessary, but expand in terms of coverage and capacity as needed - without having to overhaul or build an entirely new network.

Now a day, wireless networks are much more complex and may consist of hundreds or even thousands of access points, firewalls, switches, managed power and various other components. The wireless networks have a smarter way of managing the entire network from a centralized point.

Role based access control (RBAC) allows you to assign roles based on what, who, where, when and how a user or device is trying to access your network. Once the end user or role of the devices is defined, access control policies or rules can be enforced. It is important that your wireless system has the capability of adding indoor coverage as well as outdoor coverage.

Network access control can also be called as mobile device registration. It is essential to have a secure registration. Network access control (NAC) controls the role of the user and enforces policies. NAC can allow your users to register themselves to the network. It is a helpful feature that enhances the user experience.

Mobile Device Management

Suppose, many mobile devices are accessing your wireless network; now think about the thousands of applications are running on those mobile devices.

Mobile device management can provide control of how you will manage access to programs and applications. Even you can remotely wipe the device if it is lost or stolen.

Roaming allows your end-users to successfully move from one access point to another without ever noticing a dip in a performance. For example, allowing a student to check their mail as they walk from one class to the next.

The level or amount of redundancy your wireless system requires depends on your specific environment and needs. For example: A hospital environment will need a higher level of redundancy than a coffee shop. However, at the end of the day, they both need to have a backup plan in place.

Proper Security means using the right firewall: The backbone of the system is your network firewall. With the right firewall in place you will be able to:

- See and control both your applications and end users.
- Create the right balance between security and performance.

Reduce the complexity with:

- Antivirus protection.
- Deep Packet Inspection (DPI)
- Application filtering

Protect your network and end users against known and unknown threads including:

- Zero- day.
- Encrypted malware.
- Ransomware.
- Malicious botnets.

Switching: Basically, a network switch is the traffic cop of your wireless network which making sure that everyone and every device gets to where they need to go.

Switching is an essential part of every fast, secure wireless network for several reasons:

- It helps the traffic on your network flow more efficiently.
- It minimizes unnecessary traffic.
- It creates a better user experience by ensuring your traffic is going to the right places.

Advantages of Mobile Communication

There are following advantages of mobile communication:

- Flexibility: Wireless comm...ication enables the people to communicate with each other regardless of location. There is no need to be in an office or some telephone booth in order to pass and receive messages.

- Cost effectiveness: In wireless communication, there is no need of any physical infrastructure (Wires or cables) or maintenance practice. Hence, the cost is reduced.
- Speed: Improvements can also be seen in speed. The network connectivity or the accessibility was much improved in accuracy and speed.
- Accessibility: With the help of wireless technology easy accessibility to the remote areas is possible. For example, in rural areas, online education is now possible. Educators or students no longer need to travel to far-flung areas to teach their lessons.
- Constant connectivity: Constant connectivity ensures that people can respond to emergencies relatively quickly. For example, a wireless device like mobile can ensure you a constant connectivity though you move from place to place or while you travel, whereas a wired landline can't.

Features of Mobile Communication

The following are the features of mobile communication:

- High capacity load balancing: Each wired or wireless infrastructure must incorporate high capacity load balancing.
- High capacity load balancing means, when one access point is overloaded, the system will actively shift users from one access point to another depending on the capacity which is available.

Mobile Telephony Devices

Mobile phones are a familiar feature of business life. The traditional telephony features of mobile phones, such as making calls, receiving voicemail, and call diversion, are important to business users. Mobile phones also offer data transmission services such as:

- Global system for mobile communications (GSM) - allows mobile phones to send and receive data, e.g. connecting to the internet at a rate similar to a dial-up modem
- General packet radio service (GPRS) - an 'always-on' data service similar to broadband, but at slower transfer rates
- 'Third generation' (3G) cellular data services, also offering always-on connection at rates comparable to broadband from as little as £10 per month

Many mobile handsets are capable of accessing these data services, and include functions such as email and web access, and simplified office applications. These handsets are often known as smart phones.

Uses

- A mobile handset can provide network connection for other devices, such as personal digital assistants (PDAs) and laptops. The handset could connect to the laptop using Bluetooth, a wireless technology. It could then provide data connection to the laptop using GSM, 3G or GPRS. However, most new laptops and PDAs have wireless capability built in making this method redundant.

- 'Smart phones' such as BlackBerry phones can combine phone and PDA into a single device. This is a versatile business tool - handling email, offering diary functions, providing data connection for a laptop along with conventional mobile phone use.
- Near-universal availability of cellular networks and the established billing systems between operators, which allow you to use your device outside your service provider's network, make these services very useful for keeping in contact while travelling.

Mobile Networking Devices

Mobile IT devices can use almost any wired and wireless networking technologies, as long as they are enabled to do so, either by in-built capability or via a network adapter. The options include:

- dial-up networking, via a modem or a mobile phone
- use of the global system for mobile communications (GSM), general packet radio service (GPRS) and third-generation (3G) services offered by mobile networks
- cable connection to 'wired' local area networks (LANs), at office locations and at public internet cafes - Ethernet is the most popular wired LAN technology
- 'wireless LANs' within office buildings, or offered at public 'hot spots' where internet access is available such as internet cafes - wireless fidelity (WiFi) is the most popular wireless LAN technology
- Bluetooth or infra-red connection to another mobile device that offers one or more of the above connection capabilities
- extranets that can be accessed remotely, allowing mobile staff to use limited areas of your business' website and data
- use of 'smart phones' such as BlackBerry phones to facilitate instant email access

Uses

Sometimes you don't need networking capability on the move. It might be sufficient to download and upload the information required at the start and end of the day from the office computer system.

However, real-time communication with the office can be important in delivering business benefits, such as efficient use of staff time, improved customer service, and a greater range of products and services delivered. Examples include:

- making presentations to customers, and being able to download product information to their network during the visit
- quotations and interactive order processing
- checking stock levels via the office network
- interacting with colleagues while travelling - sending and receiving emails, collaborating on responses to tenders, delivering trip reports in a timely manner

Notes

Mobile Computing

Mobile computing evolved during the last few years as a result of shrinking portables and growing (wireless) networks. It enlarges the usability of computers, but raises demanding challenges. A mobile user has to deal with the problems of slow albeit expensive connection lines, frequent interruption of wireless connections, and limited host performance. "Requirements for mobile services are stability, bandwidth/cost considerations, integration into the familiar environment, application transparency, security and extendibility.

There are several tasks from these requirements :

- Connection management: Checking for the availability of lines, selecting the best suited one, watching the line thus noticing line disruption and in such cases following a certain strategy including attempts to reconnect.
- Line parameter management: Determining QoS and cost parameters, comparing them with given requirements, notifying the user in case of problems and providing a set of alternatives.
- Caching: Copying a certain amount of data (determined directly by the user or by predicted access probabilities) onto the mobile device, providing strategies for situations of simultaneous update or inconsistencies.
- Authentication and encryption
- Localization management: Locating required resources in a foreign environment and tracking the user if required.
- Accounting: Negotiating the costs of the usage of resources in foreign domains
- Profiling: Adapting the system to the needs and habits of the user.

4.3 APPLICATIONS OF MOBILE COMMUNICATION

Following is a list of applications in wireless communication:

Vehicles

Many wireless communication systems and mobility aware applications are used for following purpose:

- Transmission of music, news, road conditions, weather reports, and other broadcast information are received via digital audio broadcasting (DAB) with 1.5Mbit/s.
- For personal communication, a universal mobile telecommunications system (UMTS) phone might be available offering voice and data connectivity with 384kbit/s.
- For remote areas, satellite communication can be used, while the current position of the car is determined via the GPS (Global Positioning System).
- A local ad-hoc network for the fast exchange of information (information such as distance between two vehicles, traffic information, road conditions) in emergency situations or to help each other keep a safe distance. Local ad-hoc network with vehicles close by to prevent guidance system, accidents, redundancy.

- Vehicle data from buses, trucks, trains and high speed train can be transmitted in advance for maintenance.
- In ad-hoc network, car can comprise personal digital assistants (PDA), laptops, or mobile phones connected with each other using the Bluetooth technology.

Emergency

Following services can be provided during emergencies:

- Video communication: Responders often need to share vital information. The transmission of real time situations of video could be necessary. A typical scenario includes the transmission of live video footage from a disaster area to the nearest fire department, to the police station or to the near NGOs etc.
- Push To Talk (PTT): PTT is a technology which allows half duplex communication between two users where switching from voice reception mode to the transmit mode takes place with the use of a dedicated momentary button. It is similar to walkie-talkie.
- Audio/Voice Communication: This communication service provides full duplex audio channels unlike PTT. Public safety communication requires novel full duplex speech transmission services for emergency response.
- Real Time Text Messaging (RTT): Text messaging (RTT) is an effective and quick solution for sending alerts in case of emergencies. Types of text messaging can be email, SMS and instant message.

Business

- Travelling Salesman
- Directly access to customer files stored in a central location.
- Consistent databases for all agents
- Mobile office
- To enable the company to keep track of all the activities of their travelling employees.

In Office

- Wi-Fi wireless technology saves businesses or companies a considerable amount of money on installations costs.
- There is no need to physically setup wires throughout an office building, warehouse or store.
- Bluetooth is also a wireless technology especially used for short range that acts as a complement to Wi-Fi. It is used to transfer data between computers or cellphones.

Transportation Industries

- In transportation industries, GPS technology is used to find efficient routes and tracking vehicles.

Notes

Replacement of Wired Network

- Wireless network can also be used to replace wired network. Due to economic reasons it is often impossible to wire remote sensors for weather forecasts, earthquake detection, or to provide environmental information, wireless connections via satellite, can help in this situation.
- Tradeshows need a highly dynamic infrastructure, since cabling takes a long time and frequently proves to be too inflexible.
- Many computers fairs use WLANs as a replacement for cabling.
- Other cases for wireless networks are computers, sensors, or information displays in historical buildings, where excess cabling may destroy valuable walls or floors.

Location dependent service

It is important for an application to know something about the location because the user might need location information for further activities. Several services that might depend on the actual location can be described below:

Follow-on Services:

- Location aware services: To know about what services (e.g. fax, printer, server, phone, printer etc.) exist in the local environment.
- Privacy: We can set the privacy like who should get knowledge about the location.
- Information Services: We can know about the special offers in the supermarket. Nearest hotel, rooms, cabs etc.
- Infotainment: (Entertainment and Education)
- Wireless networks can provide information at any appropriate location.

Outdoor internet access

- You may choose a seat for movie, pay via electronic cash, and send this information to a service provider.
- Ad-hoc network is used for multiuser games and entertainment.
- Mobile and Wireless devices
- Even though many mobile and wireless devices are available, there will be many more devices in the future. There is no precise classification of such devices, by sizes, shape, weight, or computing power. The following list of given examples of mobile and wireless devices graded by increasing performance (CPU, memory, display, input devices, etc.)
- Sensor: Wireless device is represented by a sensor transmitting state information. One-example could be a switch, sensing the office door. If the door is closed, the switch transmits this information to the mobile phone inside the office which will not accept

incoming calls without user interaction; the semantics of a closed door is applied to phone calls.

- **Embedded Controller:** Many applications already contain a simple or sometimes more complex controller. Keyboards, mouse, headsets, washing machines, coffee machines, hair dryers and TV sets are just some examples.
- **Pager:** As a very simple receiver, a pager can only display short text messages, has a tiny display, and cannot send any messages.
- **Personal Digital Assistant:** PDAs typically accompany a user and offer simple versions of office software (calendar, notepad, mail). The typically input device is a pen, with built-in character recognition translating handwriting into characters. Web browsers and many other packages are available for these devices.
- **Pocket computer:** The next steps towards full computers are pocket computers offering tiny keyboards, color displays, and simple versions of programs found on desktop computers (text processing, spreadsheets etc.)
- **Notebook/laptop:** Laptops offer more or less the same performance as standard desktop computers; they use the same software - the only technical difference being size, weight, and the ability to run on a battery. If operated mainly via a sensitive display (touch sensitive or electromagnetic), the device are also known as notepads or tablet PCs.

4.4. WIRELESS COMMUNICATION

Wireless networks utilize radio waves and/or microwaves to maintain communication channels between computers. Wireless networking is a more modern alternative to wired networking that relies on copper and/or fiber optic cabling between network devices.

A wireless network offers advantages and disadvantages compared to a wired network. Advantages of wireless include mobility and elimination of unsightly cables. Disadvantages of wireless include the potential for radio interference due to weather, other wireless devices, or obstructions like walls.

Wireless communication is a telephone service based on signaling over radio frequencies rather than over fixed wires. Wireless telephony includes mobile wireless and wireless local loop, as well as microwave, satellite and spread spectrum radio based telephony. It is telephony without wires, usually employing electric waves of high frequency emitted from an oscillator or generator, as in wireless telegraphy.

A telephone transmitter causes fluctuations in these waves, it being the fluctuations only which affect the receiver. Wireless Telephony Application is a collection of telephony-specific extensions for call- and feature-control mechanisms that make advanced mobile network services available to end users. WTA essentially merges the features and services of data networks with the services of voice networks.

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 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.

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.

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

- Mobility: provide mobile users with access to real-time information so that they can roam around in the network without getting disconnected from the network. This mobility supports productivity and service opportunities not possible with wired networks.
- Installation speed and simplicity: installing a wireless system can be fast and easy and can eliminate the need to pull cable through walls and ceilings.
- Reach of the network: the network can be extended to places which can not be wired
- More Flexibility: wireless networks offer more flexibility and adapt easily to changes in the configuration of the network.
- Reduced cost of ownership: while the initial investment required for wireless network hardware can be higher than the cost of wired network hardware, overall installation expenses and life-cycle costs can be significantly lower in dynamic environments.
- Scalability: wireless systems can be configured in a variety of topologies to meet the needs of specific applications and installations. Configurations can be easily changed and range from peer-to-peer networks suitable for a small number of users to large infrastructure networks that enable roaming over a broad area.

Types of Wireless Networks and Usage

There are three primary usage scenarios for wireless connectivity:

- Wireless Personal Area Networking (WPAN)
- Wireless Local Area Networking (WLAN)
- Wireless Wide Area Networking (WWAN)

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).

WLAN on the other is more focused on organizational 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.

Whereas WLAN addresses connectivity within a defined region, WWAN addresses the need to stay connected while traveling 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 traveling. The following table summarizes each wireless connectivity usage scenario by a wireless technology.

Bluetooth and 802.11 are emerging as the preferred technology in the commercial space for WPAN and WLAN respectively. Higher throughput, longer range and other characteristics make 802.11 better suited for WLAN than Bluetooth.

Wireless LAN Overview

WLANS allow users in local area, such as in a university or a library to form a network and gain wireless access to the internet. A temporary network can be formed by a small number of users without the need of access point; given that they do not need to access the resources.

A wireless local area network (WLAN) links devices via a wireless distribution method (typically spread-spectrum or OFDM) and usually provides a connection through an access point to the wider internet. This gives users the mobility to move around within a local coverage area and still be connected to the network.

The first generation of wireless data modems was developed in the early 1980s by amateur radio operators, who commonly referred to this as packet radio. They added a voice band data communication modem, with data rates below 9600-bit/s, to an existing short distance radio system, typically in the two meter amateur band.

The second generation of wireless modems was developed immediately after the FCC announcement in the experimental bands for non-military use of the spread spectrum technology. These modems provided data rates on the order of hundreds of kbit/s. The third generation of wireless modem then aimed at compatibility with the existing LANs with data rates on the order of Mbit/s. Several companies developed the third generation products with data rates above 1 Mbit/s and a couple of products had already been announced by the time of the first IEEE Workshop on Wireless LANs.

WLAN hardware was initially so expensive that it was only used as an alternative to cabled LAN in places where cabling was difficult or impossible.

Notes

Early development included industry-specific solutions and proprietary protocols, but at the end of the 1990s these were replaced by standards, primarily the various versions of IEEE 802.11 (Wi-Fi). An alternative ATM-like 5 GHz standardized technology, HiperLAN/2, has so far not succeeded in the market, and with the release of the faster 54 Mbit/s 802.11a (5 GHz) and 802.11g (2.4 GHz) standards, almost certainly never will.

Applications of Wireless Technology

Security systems

Wireless technology may supplement or replace hard wired implementations in security systems for homes or office buildings.

Television remote control

Modern televisions use wireless (generally infrared) remote control units. Now radio waves are also used.

Cellular telephone (phones and modems)

Perhaps the best known example of wireless technology is the cellular telephone and modems. These instruments use radio waves to enable the operator to make phone calls from many locations worldwide. They can be used anywhere that there is a cellular telephone site to house the equipment that is required to transmit and receive the signal that is used to transfer both voice and data to and from these instruments.

Wi-Fi

Wi-Fi is a wireless local area network that enables portable computing devices to connect easily to the Internet. Standardized as IEEE 802.11 a,b,g,n, Wi-Fi approaches speeds of some types of wired Ethernet. Wi-Fi hot spots have been popular over the past few years. Some businesses charge customers a monthly fee for service, while others have begun offering it for free in an effort to increase the sales of their good.

Wireless energy transfer

Wireless energy transfer is a process whereby electrical energy is transmitted from a power source to an electrical load that does not have a built-in power source, without the use of interconnecting wires.

Computer Interface Devices

Many scientists have complained that wireless technology interferes with their experiments, forcing them to use less optimal peripherals because the optimum one is not available in a wired version. This has become especially prevalent among scientists who use trackballs as the number of models in production steadily decreases.

Digital Cellular Standard

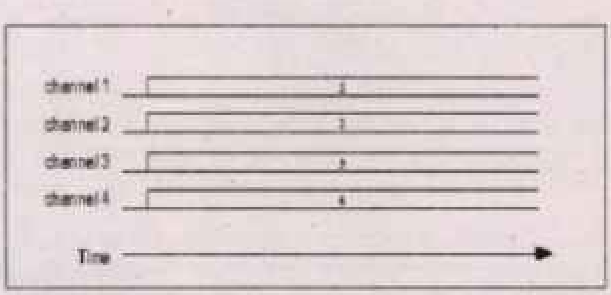
Digital technology offers the opportunity for improved transmission in cellular systems. This is due to powerful error detection and recovery techniques, which can be used to counter the debilitating effects of noise, fading and interference. Digital technology also provides the basis for security in the forms of encryption and authentication.

Finally, digital technology requires less in the way of mobile transmit power, which increases battery life in portable mobile units.

Digital cellular technologies also offer the promise of effective data transmission via cellular services. Although their vocoders prohibit the use of conventional modems, recent extensions to standards provide low-throughput data traffic in either a circuit-switched mode or via a digital control channel. Packet-switched data services are also being developed by the proponents of digital cellular standards.

Before presenting the primary digital cellular technologies, understanding the basic differences between FDMA, TDMA and CDMA is essential. As depicted in following figure, a frequency division multiple access (FDMA) system, such as AMPS, separates individual conversations in the frequency domain-different conversations use different frequencies (channels).

In this depiction, the frequency domain is represented by the horizontal dimension.



Time vs. Frequency for an FDMA System (e.g., AMPS)

The next figure shows how time division multiple access (TDMA) systems, such as IS-54/136, GSM or PDC, separate conversations in both the frequency and time domains; each frequency (channel) supports multiple conversations, which use the channel during specific timeslots. Typically there is a maximum number of conversations which can be supported on each physical channel. Each conversation occupies a logical "channel."

4.5 GSM (GLOBAL SYSTEM FOR MOBILE COMMUNICATION)

Global System for Mobile (GSM) is a second generation cellular standard developed to cater voice services and data delivery using digital modulation.

Global system for mobile communication (GSM) is a globally accepted standard for digital cellular communication. GSM is developed by Group Special Mobile (founded 1982) which was an initiative of CEPT (Conference of European Post and Telecommunication) to create a common European mobile telephone standard that would formulate specifications for a pan-European mobile cellular radio system operating at 900 MHz. It is estimated that many countries outside of Europe will join the GSM partnership. Presently the responsibility of GSM standardization resides with special mobile group under ETSI (European telecommunication Standards Institute). Today it have many providers all over the world use

GSM (more than 135 countries in Asia, Africa, Europe, Australia, America) and more than 1300 million subscribers in world and 45 million subscriber in India.

The GSM cellular technology had a number of design aims when the development started:

- It should offer good subjective speech quality
- It should have a low phone or terminal cost
- Terminals should be able to be handheld
- The system should support international roaming
- It should offer good spectral efficiency
- The system should offer ISDN compatibility

The resulting GSM cellular technology that was developed provided for all of these. The overall system definition for GSM describes not only the air interface but also the network or infrastructure technology.

By adopting this approach it is possible to define the operation of the whole network to enable international roaming as well as enabling network elements from different manufacturers to operate alongside each other, although this last feature is not completely true, especially with older items.

GSM development started in the early 1980s to replace first generation analogue cellular technology. The essential difference between a cellular and fixed telephony network is that the subscriber's terminal (Mobile Station - MS) is not linked by a fixed physical connection to the network.

- Connection is a radio based wireless connection

In order to support this terminal mobility, the geographic area which the mobile network covers, is subdivided into cells. The proposed system had to meet certain criteria

- Good subjective speech quality
- Low terminal and network equipment costs
- Support of international roaming
- Efficient use of available spectrum

Global system for mobile (GSM) is thus the second generation digital cellular system. It is the world's first cellular system to specify digital modulation network level architectures and services and has become world's most popular 2G technology.

Gsm System Architecture

The GSM architecture as defined in the GSM specifications can be grouped into three main areas:

- Switching Subsystem (NSS)
- Base-station subsystem (BSS)

Notes

- The Operation and Support System

The Switching System

The switching system (SS) is responsible for performing call processing and subscriber-related functions. The switching system includes the following functional units.

- **Home Location Register (HLR)**—The HLR is a database used for storage and management of subscriptions. The HLR is considered the most important database, as it stores permanent data about subscribers, including a subscriber's service profile, location information, and activity status.
- **Mobile Services Switching Center (MSC)**—The MSC performs the telephony switching functions of the system. It controls calls to and from other telephone and data systems.
- **Visitor Location Register (VLR)**—The VLR is a database that contains temporary information about subscribers that is needed by the MSC in order to service visiting subscribers. The VLR is always integrated with the MSC. When a mobile station roams into a new MSC area, the VLR connected to that MSC will request data about the mobile station from the HLR. Later, if the mobile station makes a call, the VLR will have the information needed for call setup without having to interrogate the HLR each time.
- **Authentication Center (AUC)**—A unit called the AUC provides authentication and encryption parameters that verify the user's identity and ensure the confidentiality of each call. The AUC protects network operators from different types of fraud found in today's cellular world.
- **Equipment Identity Register (EIR)**—The EIR is a database that contains information about the identity of mobile equipment that prevents calls from stolen, unauthorized, or defective mobile stations.

The Base Station System (BSS)

All radio-related functions are performed in the BSS, which consists of base station controllers (BSCs) and the base transceiver stations (BTSs).

- **BSC**—The BSC provides all the control functions and physical links between the MSC and BTS. It is a high-capacity switch that provides functions such as handover, cell configuration data, and control of radio frequency (RF) power levels in base transceiver stations. A number of BSCs are served by an MSC.
- **BTS**—The BTS handles the radio interface to the mobile station. The BTS is the radio equipment (transceivers and antennas) needed to service each cell in the network. A group of BTSs are controlled by a BSC.

4.6 BANDWITH COMMUNICATION

The concept of bandwidth is closely linked to the ability of a system to transmit information. To transfer data, a signal must change in some way and the rate at which these changes occur influences the rate at which information can be transferred.

- If a signal has more bandwidth—in this case meaning that it includes or is compatible with higher frequencies—it can change more rapidly. Thus, more bandwidth corresponds to a higher maximum rate of data transfer.
- The term "bandwidth" is used to describe not only the rate at which data is transferred but also the rate at which it is processed. This is essentially the concept of throughput applied to a processing system rather than a communication system.
- The bandwidth of the CPU, itself, is determined by the clock frequency and architectural details (such as the number of cores) that determine how instructions are executed. It turns out, though, that the memory bandwidth can be the limiting factor in processors built around top-of-the-line CPUs.
- Memory bandwidth refers to the speed at which the memory system can move data to the CPU, and apparently technological developments have favored CPU throughput rather than memory performance.
- Perhaps the most important thing to remember about computing bandwidth—measured in, say, bytes per second or instructions per second—is that it is by no means equal to the processor's clock frequency (in cycles per second). Instructions often require more than one clock cycle for execution, even in the relatively simple processors found in microcontrollers. In fact, the original 8051 architecture required at least 12 clock cycles to execute one instruction.

4.7 BANDWIDTH CONSERVATION

One of the goals of mobile agency is to conserve bandwidth, by placing an agent directly at the point of information, rather than sending dozens or even hundreds of queries across the network. This is based on the premise that these queries would have consumed more bandwidth than sending an agent over the network, and bringing it back again.

Bandwidth conservation is an admirable goal, but whether mobile agents will help realize this goal is questionable. For bandwidth to be conserved, the bandwidth consumed by sending across a mobile agent, and waiting for its results, must be less than that of a series of queries sent via a messaging or RPC system. This is a determination that must be made in practice, and cannot be fully verified just by theory.

Many scenarios can be foreseen. Perhaps mobile agents could comb through large amounts of resources on a single site, and bring back a small number of matches, in a similar nature to a search engine. However, some electronic commerce models suggest that mobile agents would be sent out to multiple sites, perhaps to negotiate low prices with vendors (a shopping-bot). This sort of activity has the potential to result in an incredible explosion of bandwidth consumption.

Indeed, searching is a task that many people would like to see mobile agents performing. Currently, a small number of indexing agents collect information for search engines, while millions of queries are made by users. Imagine if the same number of queries were made instead by mobile agents that traveled across the network to sites. Two scenarios are possible. Either a much larger amount of bandwidth (and CPU usage for the agent hosts) will be consumed, or a much lesser amount of bandwidth will be consumed as users receive more accurate search results because their agents have more control over the search process. Instinct suggests, however, that a simple keyword query entered via a web browser will consume less resources and bandwidth than sending an agent with specialised searching algorithms across the network.

Delegate Tasks to Agents when not Connected

The Internet, as it stands today, is made up of many millions of computers, some of which are permanently connected but the majority of which connect via dial-up modem connections for short periods of times. Imagine if you could delegate tasks to mobile agents, that would roam the network for you while not connected. This goal would be extremely desirable in the short term, until permanent connections became more prevalent. Here mobile agents may have found a sound market. This market could potentially be profitable, for the mobile agent technology vendors and the agent hosts that allow offline usage of their network.

Delegation of tasks to mobile agents could also be used as a form of load sharing in distributed systems. Agents could perform tasks on remote systems, moving from system to system as required to balance the load. Mobile agency also gives greater flexibility, because new tasks and new code can be added to the system without the need for a fixed codebase.

Mobile agents enable new types of interaction

The ability of mobile agents to fragment themselves into many pieces that travel to different points across the network sounds promising. It might enable new forms of interaction, such as negotiating agents that travel to vendors seeking the best deal, or meeting places where agents can "get together" and communicate. The attraction of mobile agents for electronic commerce is great, and it might make sense to deploy mobile agents for electronic commerce. However, such uses could also be accomplished by message passing, or direct communication using application protocols like HTTP. Mobile agency is promising, but it is not the only mechanism for new uses of software agents.

Agent privacy

If mobile agents were to become commonplace, serious privacy concerns would be raised. Aside from deliberate attempts to decompile or interrogate an agent (or its encrypted data), agent hosts could also monitor the actions of agents, and create consumer profiles. Even knowledge of the types of queries, or the way in which an agent searched, could reveal information about its owner. When individuals query a search engine, there is some degree of anonymity, but there is less control with mobile agency.

4.8 TRANSMISSION IMPARIMENT

Transmission impairment occurs when the received signal is different from the transmitted signal. As we know, a signal can be transmitted as Analog signal or it can be transmitted as a digital signal.

Notes

In Analog signals due to transmission impairment the resulting received signal gets different amplitude or the shape. In the case of digitally transmitted signals at the receiver side we get changes in bits (0's or 1's).

Causes

There are various causes of transmission impairments:

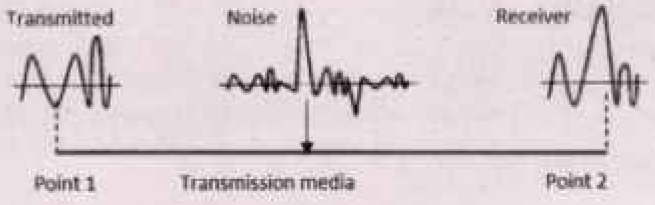
- Noise
- Distortion
- Attenuation

Let us understand them one by one.

Noise

Noise is the major factor for the transmission distortion as any unwanted signal gets added to the transmitted signal by which the resulting transmitted signal gets modified and at the receiver side it is difficult to remove the unwanted noise signal. These noises are various kinds like shot noise, impulse noise, thermal noise etc.

Noise is diagrammatically represented as follows:

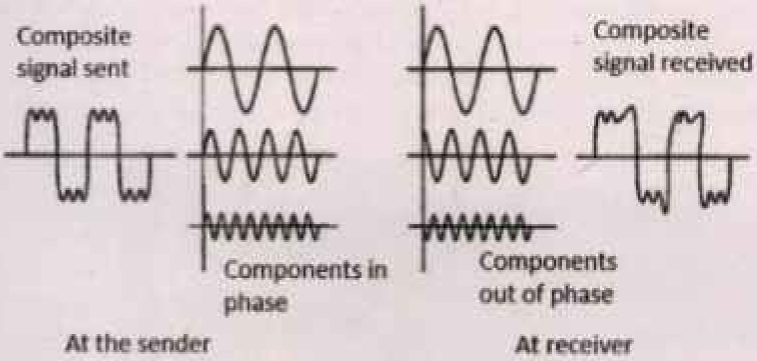


Distortion

This kind of distortion is mainly appearing in case of composite signals in which a composite signal has various frequency components in it and each frequency component has some time constraint which makes a complete signal.

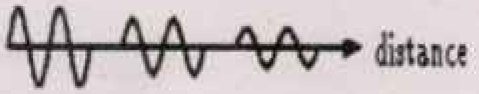
But while transmitting this composite signal, if a certain delay happens between the frequencies components, then there may be the chance that the frequency component will reach the receiver end with a different delay constraint from its original which leads to the change in shape of the signal. The delay happens due to environmental parameters or from the distance between transmitter and receiver etc.

Distortion is diagrammatically represented as follows:



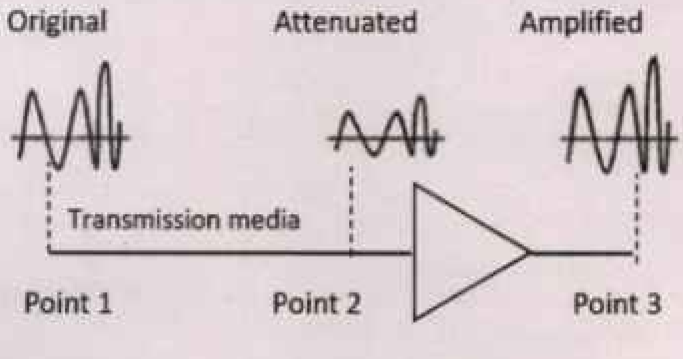
Attenuation

Attenuation is generally decreased in signal strength, by which the received signal will be difficult to receive at the receiver end. This attenuation happens due to the majority factor by environment as environment imposes a lot of resistance and the signal strength decreases as it tries to overcome the resistance imposed.



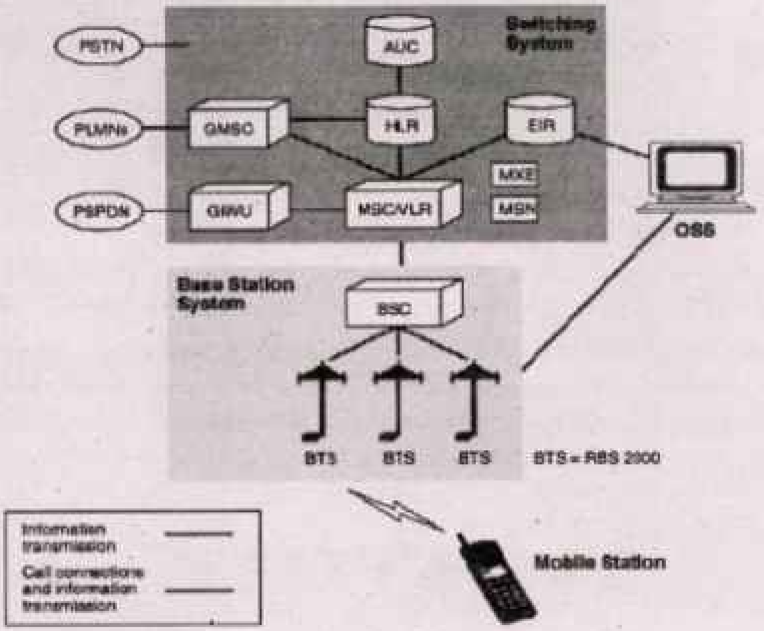
The above picture shows that the signal loses power at its travels time.

Attenuation is diagrammatically represented as follows –



The Operation and Support System

The operations and maintenance center (OMC) is connected to all equipment in the switching system and to the BSC. The implementation of OMC is called the operation and support system (OSS). The OSS is the functional entity from which the network operator monitors and controls the system. The purpose of OSS is to offer the customer cost-effective support for centralized, regional, and local operational and maintenance activities that are required for a GSM network. An important function of OSS is to provide a network overview and support the maintenance activities of different operation and maintenance organizations.



GSM Interfaces

The different interfaces used in GSM listed as follows:

1. GSM radio air interface: This is the interface between MS and BTSs.
2. Abis interface: The one connecting the BTS to a BSC is known as Abis interface. This is responsible for carrying traffic and maintenance data.
3. A interface: This is the interface between a BSC and a MSC.

GSM Channels

There are two types of GSM logical channels:

- Traffic Channels: These channels carry digitally encoded user speech or data.
- Control Channels: Signaling and synchronizing commands between BS and MS are transmitted through these channels.

GSM Services

The GSM services in different spheres are listed as follows:

1. Data services include computer to computer communication and packet switched traffic.
2. Telephone services which include fax services. Videotex and teletex are also supported by GSM.
3. Mobile originated traffic and standard mobile telephony are included in teleservices supported by GSM.
4. Different other services include:
   - call diversion
   - caller line identification
   - call wait
   - SMS services

Speech or voice calls are obviously the primary function for the GSM cellular system. To achieve this the speech is digitally encoded and later decoded using a vocoder. A variety of vocoders are available for use, being aimed at different scenarios.

In addition to the voice services, GSM cellular technology supports a variety of other data services. Although their performance is nowhere near the level of those provided by 3G, they are nevertheless still important and useful. A variety of data services are supported with user data rates up to 9.6 kbps. Services including Group 3 facsimile, videotext and teletex can be supported.

One service that has grown enormously is the short message service. Developed as part of the GSM specification, it has also been incorporated into other cellular technologies. It can be thought of as being similar to the paging service but is far more comprehensive allowing bi-directional messaging, store and forward delivery, and it also allows alphanumeric messages of a reasonable length. This service has become particularly popular, initially with the young as it provided a simple, low fixed cost.

GSM Subscriber Services

There are two basic types of services offered through GSM:

1. Telephony (also referred to as teleservices)
2. Data (also referred to as bearer services).

1. Telephony services: are mainly voice services that provide subscribers with the complete capability (including necessary terminal equipment) to communicate with other subscribers. Telecommunication services that enable voice communication via mobile phones. It offered services mobile telephony and emergency calling.
2. Data services provide: the capacity necessary to transmit appropriate data signals between two access points creating an interface to the network. In addition to normal telephony and emergency calling, the following subscriber services are supported by GSM:

Notes

- dual-tone multifrequency (DTMF): DTMF is a tone signaling scheme often used for various control purposes via the telephone network, such as remote control of an answering machine. GSM supports full-originating DTMF.
- facsimile group III: GSM supports CCITT Group 3 facsimile. As standard fax machines are designed to be connected to a telephone using analog signals, a special fax converter connected to the exchange is used in the GSM system. This enables a GSM-connected fax to communicate with any analog fax in the network.
- short message services: A convenient facility of the GSM network is the short message service. A message consisting of a maximum of 160 alphanumeric characters can be sent to or from a mobile station. This service can be viewed as an advanced form of alphanumeric paging with a number of advantages. If the subscriber's mobile unit is powered off or has left the coverage area, the message is stored and offered back to the subscriber when the mobile is powered on or has reentered the coverage area of the network. This function ensures that the message will be received.
- cell broadcast: A variation of the short message service is the cell broadcast facility. A message of a maximum of 93 characters can be broadcast to all mobile subscribers in a certain geographic area. Typical applications include traffic congestion warnings and reports on accidents.
- voice mail: This service is actually an answering machine within the network, which is controlled by the subscriber. Calls can be forwarded to the subscriber's voice-mail box and the subscriber checks for messages via a personal security code.
- fax mail: With this service, the subscriber can receive fax messages at any fax machine. The messages are stored in a service center from which they can be retrieved by the subscriber via a personal security code to the desired fax number.

Supplementary Services of GSM

GSM supports a comprehensive set of supplementary services that can complement and support both telephony and data services. Supplementary services are defined by GSM and are characterized as revenue-generating features. A partial listing of supplementary services follows.

- call forwarding: This service gives the subscriber the ability to forward incoming calls to another number if the called mobile unit is not reachable, if it is busy, if there is no reply, or if call forwarding is allowed unconditionally.
- barring of outgoing calls: This service makes it possible for a mobile subscriber to prevent all outgoing calls.
- barring of incoming calls: This function allows the subscriber to prevent incoming calls. The following two conditions for incoming call barring exist: baring of all incoming calls and barring of incoming calls when roaming outside the home PLMN.

- advice of charge (AoC): The AoC service provides the mobile subscriber with an estimate of the call charges. There are two types of AoC information: one that provides the subscriber with an estimate of the bill and one that can be used for immediate charging purposes. AoC for data calls is provided on the basis of time measurements.
- call hold: This service enables the subscriber to interrupt an ongoing call and then subsequently reestablish the call. The call hold service is only applicable to normal telephony.
- call waiting: This service enables the mobile subscriber to be notified of an incoming call during a conversation. The subscriber can answer, reject, or ignore the incoming call. Call waiting is applicable to all GSM telecommunications services using a circuit-switched connection.
- multiparty service: The multiparty service enables a mobile subscriber to establish a multiparty conversation: that is, a simultaneous conversation between three and six subscribers. This service is only applicable to normal telephony.
- calling line identification presentation/restriction: These services supply the called party with the integrated services digital network (ISDN) number of the calling party. The restriction service enables the calling party to restrict the presentation. The restriction overrides the presentation.
- closed user groups (CUGs): CUGs are generally comparable to a PBX. They are a group of subscribers who are capable of only calling themselves and certain numbers.

Channel Structure

In GSM the structure and terminology is a bit different:

- mobile stations (MS)
- base transceiver station (BTS): has transmit / receive circuitry and does transcoding / rate-adaptation
- several BTS are managed by a base station controller (BSC): BSC
- allocates channels to BTS, handover management, paging
- several BSC's are under control of a mobile services switching centre
- (MSC): gateway to PSTN, handover.

In GSM there are two types of channels:

1. Traffic channels used for speech and data.
2. Control channels used for network management messages and channel maintenance tasks.

1. Traffic channels (TCH)

Full-rate traffic channels (TCH/F) are defined using a group of 26 TDMA frames called a 26-Multiframe. The 26-Multiframe lasts 120 ms. In this frame group traffic channels for the downlink and uplink are separated by 3 bursts. That implies, the mobiles will not need to transmit and receive at the same time which simplifies considerably the electronics of the system.

Notes

The frames that form the 26-Multiframe structure have different functions:

- 24 frames are reserved to traffic.
- 1 frame is used for the Slow Associated Control Channel (SACCH).
- The last frame is unused. It allows the MN to perform other functions, such as measuring the signal strength of neighboring cells.

Half-rate traffic channels (TCH/H), which double the capacity of the system, are also grouped in a 26-Multiframe but the internal structure is different.

2. *Control channels*

According to their functions, 4 different classes of control channels are defined:

Broadcast channels (BCH) : The BCH channels are used, by BTS to provide the MN with synchronization information from the network. 3 different types of BCHs can be distinguished:

- Broadcast Control Channel (BCCH): gives to the MN the parameters needed to identify and access the network.
- Synchronization Channel (SCH): gives the MN the training symbol sequence to demodulate the information transmitted by BTS.
- Frequency-Correction Channel (FCCH): provides the MN with the frequency reference of the system for the purposes of synchronization.

There are three types of Control Channels :

1. Common Control Channels (CCCH) : The CCCH channels help to establish the calls from the mobile station or the network. These are:

- Paging Channel (PCH): used to alert the MN of an incoming call.
- Random Access Channel (RACH): used by the MN to request network access.
- Access Grant Channel (AGCH): used, by the BTS, to inform the MN about the channel it should use. This channel is the answer of a BTS to a RACH request from the MN.

2. Dedicated Control Channels (DCCH) : The DCCH channels are used for message exchange between several mobiles or a mobile and the network. These are:

- Standalone Dedicated Control Channel (SDCCH): used to exchange signaling in the downlink and uplink.
- Slow Associated Control Channel (SACCH): used for channel maintenance and control.

3. Associated Control Channels (ACCH) : Fast Associated Control Channels (FACCH) replace all or part of a traffic channel when urgent signaling must be transmitted. The FACCH channels carry the same signaling as SDCCH channels.

Channel Allocation in Cellular System

A given radio spectrum can be divided into a set of disjoint or nonintering radio channels. All such channels can be used simultaneously while maintaining on acceptable received radio signal. In order to divide a given radio spectrum into such channels many techniques such

Notes

as frequency decision (PD), time decision (TD), or code decision (CD) can be used. In FD, the spectrum is divided into disjoint frequency bands, whereas in TD, the channel separation is achieved by dividing the usage of the channel into disjoint time periods called time slots. In CD, the channel separation is achieved by using different modelation codes.

Furthermore, more elaborate techniques can be designed to divide a radio spectrum into a set of disjoint channels based on combining the above a set of disjoint channels based on combining the above techniques.

For example, a combination of TD and FD can be used by dividing each frequency based of an FD scheme into time slots.

The major during factor in determining the number of channels with certain quality that can be used for a given wireless spectrum is the level of received signal quality that can be achieved in each channel.

Let Si(K) be denoted as the set (i) of wireless terminals that communicate with each other using the same channel k. By taking advantage of physical characteristics of the radio environment, the same channel k can be reused sinsult aneously by another set j, if the members of sets i or simply co-channels.

The minimum distance at which co-channels can be reused with acceptable interference is called the "co-channel reuse distance."

This is possible because due to propagation path loss in the radio environment, the average power received from a strans mitter at distance d is proportional to PTd-μ where μ is a number in the range of 3-5 depending on the physical environment and PT is the average transmitter power.

For Example

For An indoor environment with μ = 3.5, the average power at a distance 2d is about a percent of the average power received at distance d. thus by adjusting the transmitter power level and/or the distance between co-channels, a channel can be reused by a number of co-channel if the corrier-to-interference ratio (CIR) in each co-channel, and the interference (1) represents the sum of received signal power of all co-channels.

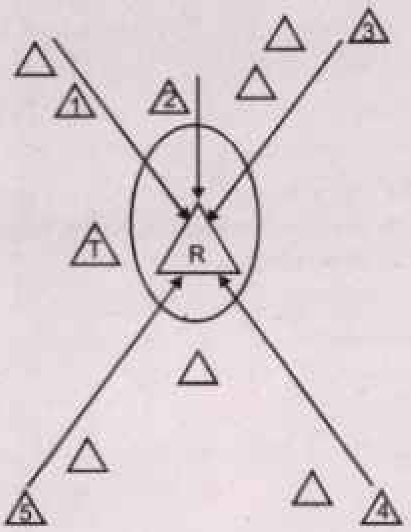
In the following figure where a wireless station labeled R is at distance dt from a transmitter station labeled T using a narrowband radio channel.

Radio channel is used by T to communicate to R as the Reference channel. In this figure, fue other stations labeled 1, 2, ... 5, are also shown which use the same channel as the reference channel to communicate with some other stations.

Denoting the transmitted power of station i by Pi and the distance of station i from R by di, the average CIR at the reference station R is given by :

$$\text{CIR} = \frac{p_1 d_1 - \alpha}{\sum_{i=1}^{5} p_i d_i - \alpha + N_0}$$

Notes



Where No represents the environmental noise. To achieve a certain level of CIR at the reference station R, different methods can be used. For example, the distance between stations 1, 2, ... 5 using the co-channels and the reference station R can be increased to reduce the co-channel interference level many channel allocation schemes are based on this idea of physical separation.

Another solution to reduce the CIR at R is to reduce the interfering power transmitted from fire interfering, stations and/or to increase the desired signal's power level Pt. This is the idea believed power control schemes.

These twomethods present the underlying concept for channel assignment alogrithms in cellular systems. Each of these algorithm uses a different method to achieved a CIR must at each mobile terminal by separating co-channels and/or by adjusting the transmitter power.

Mobile Internet

According to the many sources, one of the major factors of the usage of mobile internet is its speed. Mobile internet has faster connection. Due to this fact, many users tend to use mobile internet. The introduction of the 3G cards has a competitive high speed. All the current service providers and trying to increase their bandwidth to get more customers.

The numbers of mobile phones that are cable of surfing the net have been increasing rapidly. One of the greatest problems when browsing the net on the cell phones is the small size of the screen. Because of this many developers are developing the websites that can easily be seen on the cell phones as well Mobile society.

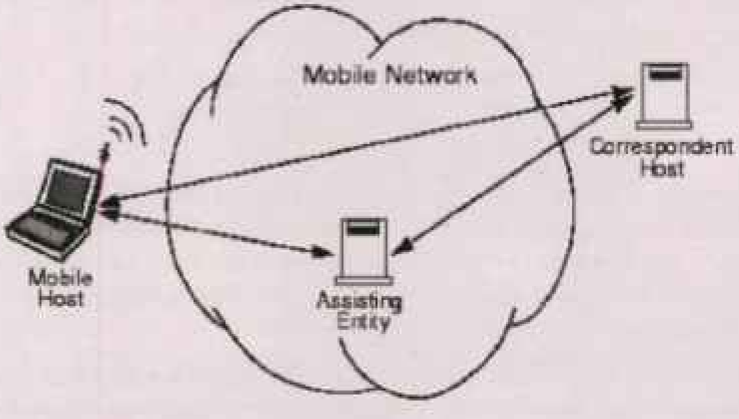
Ongoing debates about the cyberspace, e-computing and E-commerce have suggested that the online world somehow will be dramatically different from the life in the analog world. It is true that E-commerce continues to grow and the specific locations of the persons and businesses do not matter that much anyone. This is also true that now we are seeing forums, blogs, discussion groups and social network to re-socialize and form new tribes on the internet.

It seems that everyday we are increasingly connected via technologies such as email, cellular phones, instant messaging and all of these technologies are increasingly interconnected with each other. When we communicate on our cell phones, we are also mobile in the sense that we can move freely while in the constant communication.

Mobile Data

A mobile host or mobile is a host which can receive network services regardless of its location. The extent to which this host enjoys transparent location-independence is a key concern. Different systems use different terminology for the mobile; CDPD adopts ISO terminology by calling it a Mobile End System (M-ES).

The mobile is an occasionally-connected entity, which means it may or may not be connected at any given moment to a subnet somewhere in the mobile WAN.



Roles in Mobility and Message Flow

The second role necessary in any communications is the opposite side of the correspondence. In this book we refer to this as the correspondent host or correspondent. The correspondent is the location of the opposite side of a mobile's application association; it could be the ultimate source of data destined for the mobile or another entity such as a store-and-forward device.

The correspondent could itself be mobile or fixed in location, but this is generally not material to our analysis. CDPD refers to the correspondent as the Fixed End System (F-ES) when it is fixed in location.

In circuit-switched systems, there will be a maximum of one correspondent per mobile host. However, in the packet-switched systems of greatest interest to us, there can always be multiple correspondents per mobile host.

Associated with the mobile communications is the assisting entity or assistant. The assistant is an enabler of mobility. It could be a network store-and-forward device or mobility-supporting intermediate system (router).

Most likely, it consists of multiple entities in a mobile network infrastructure which collectively support host mobility. In CDPD this role is largely filled by a combination of the Mobile Serving Function and the Mobile Home Function; the Mobile IP Task Force calls this combination the foreign agent and the mobile router or home agent.

Thus, the mobile will generally be the destination host in any mobile system scenario of interest. Consistent with this, we will adopt a system-centric viewpoint by defining the flow of data traffic to a mobile as moving in the forward direction (i.e., mobile network to mobile host).

Likewise, the flow of data traffic from a mobile is said to move in the reverse direction (i.e., mobile host to mobile network). This terminology is consistent with the cellular industry, which is the origin of CDPD, and is displayed, in the above figure.

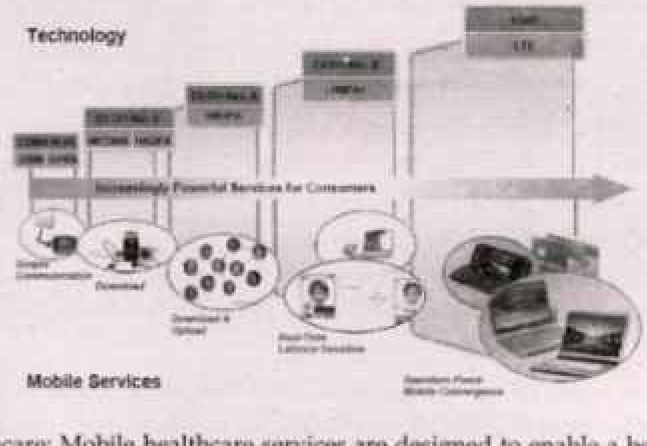
Key Services in Mobile Internet

Mobile Communication: Mobile services are changing the landscape of how we communicate daily; specifically, the why, when, how often, and in what degree we communicate. Today, mobile communication can be ubiquitous (anytime, anywhere, anyplace), personal (instant messaging, picture cards, video messaging) or interactive (push-to-talk [PTT], video telephony, video sharing). Using mobile communication services has never been easier or more entertaining.

Mobile Enterprise: Mobile enterprise services are at the forefront of early wireless-technology service adoption. The implementation of mobile enterprise services provides a competitive advantage to corporations wanting to gain an edge.

Mobile Entertainment: The days of waiting to get home to indulge your passion for entertainment are long gone. Like never before, mobile entertainment has given end users the flexibility and freedom to engage their favorite form of entertainment programming on their terms. Mobile TV (live or cached), videos and movies (streaming or on demand), music (full tracks), gaming (casual and 3D multiplayer), or social networking (user-generated or community-developed content) are all available at your fingertips.

Location-Based Services (LBS): For the enterprise customer, LBS means the efficient tracking of goods and services. For a consumer, LBS enhances the level of comfort by knowing the location of a child or elderly parent. For retail shops and restaurants, LBS provides timely directions for a customer who is lost. Mobile LBS provide end users with location information when and where they need it most.



Mobile Healthcare: Mobile healthcare services are designed to enable a better quality of life 24 hours a day, seven days a week for outpatient treatment and monitoring procedures.

These services allow the capture of patients' medical data at the point of care, enabling faster diagnosis and timelier treatments.

Mobile healthcare services provide freedom, mobility and an enhanced sense of wellness for outpatients, and peace of mind for caregivers.

Mobile Commerce: The old adage "time is money" has never been truer than in today's fast-paced economy. Mobile-commerce services (m-banking, m-payment, e-money, etc.) provide a new level of convenience and safety for managing money transactions.

Mobile and Remote Education: Mobile education services have created new avenues of learning. Never before has the ability to receive live or cached classroom instruction or vocational training in a mobile or distance-learning environment been so accessible.

Emerging Markets: Mobile services in emerging markets are empowering citizens with social and economic choices that many never dreamed of having. People in emerging markets are adopting mobile services where, traditionally, there were no services available to them, notably services such as mobile banking, remote learning and healthcare (e.g., village clinics).

The mobile services just reviewed are but a sampling of the many services currently offered worldwide. As we look into the future, the ways in which we use mobile services will continue to grow, due to our limitless imagination for improvement in the lives of our fellow man.

Business opportunities

- Mobile Business Communications Ltd Established in 1976, operates from a 10,000 sq. foot facility in North York, as well as in Branch Offices in Niagara Falls and Mississauga.
- Authorized Sales Representative and Warranty Service Provider for all major manufacturers and distributors in the wireless industry including Motorola and Kenwood.
- Provides wide-area dispatch solutions and antenna sites, using our independently owned Trunked network, throughout the GTA and Golden Horseshoe regions.
- Additional services include expertise in custom, On-Site system design and implementation.
- Four Trunked Dispatch Networks in operation providing flat-rate airtime on more than 70 channels.
- Mobile also has extensive experience with small, medium, and large, short and long term rental requirements.

There are large efforts being made to make innovative mobile ICT services work. Services like mobile tourist guides or shopping guides for consumers. To join the bandwagon, technology and service providers (contributors) combine their expertise and resources to design these services.

This incorporates designing of several models: the value net (Value network), a Value proposition, a Revenue Model and a Technological architecture.

Notes

A Value Net

A value net is a business design that uses digital supply chains to achieve both superior customer satisfaction and company profitability. It is a fast, flexible system that is aligned with and driven by new customer choice mechanisms. A value net is not what the term supply chain conjures up. It is no longer just about supply, but it is also about creating value for customers, the company and its suppliers.

The value net differs from the traditional value chain in the sense that it is not a sequential, rigid chain. Instead, it is a dynamic, high performance network of customer/supplier partnerships and information flows.

Value Proposition

The Value Proposition model is used to represent the value of the service from the perspective of the end-user (Customer, Consumer). This model is often surprisingly complex for the design of mobile ICT services. This is because the characteristics are very different from physical products. The SHIP-acronym can be used to define four important characteristics of mobile ICT services:

- Simultaneously produced and consumed. This means that the end-user is part of the production of content, and that the producer is also present during the transaction.
- Heterogeneous. This means that there is a (almost) unique instance of the service made for each end-user.
- Intangible. Although the service is intangible, they are often coupled to physical products.
- Perishable. The value of the service disappears after consumption by the end-user.

A value proposition model incorporates the consequences of these characteristics into the development process. This model can be in the form of a textual/graphic model, or even a demonstration version of the proposed service. The composition of the Value Proposition forces the designers to think about different important characteristics of mobile ICT services, the FBBM method addresses the following issues in this context :

1. Context in which the service will operate, e.g., in a 'shopping mall', or at the 'office'.
2. The proposed target group, e.g., 'museum visitors', or 'traveling business people'.
3. Added value in comparison of existing services, 'easier to use', or 'gives more information'.
4. Estimation of its use, e.g., 'how often will consumers use it?', and 'what does it mean to the user?'.

The information about service-characteristics that are gathered in this part of the Method is usually sketched in use-cases diagrams. This illustrates the part how the proposed services would interact with the end-user.

Revenue Model

A Revenue model is used to identify all cash flows concerning the service. These are all costs and revenues that are the result of economic activities. Therefore, the value of each activity must be measured (or approximated) using performance indicators. In the model, the cash flows can be described qualitative at first (high, medium, low) and more in detail at later stages of the development process.

The model uses lines representing in- and outgoing cash flows between the value activities and the actors drawn the model. The meta-model consists of the financial arrangements, which describe the costs and the revenues of a service, using performance indicators.

Technological Architecture

The Technological Architecture model is used to give an overview of the technical functions, and infrastructure needed to provide the service.

For example, the way information is stored, or content is generated and broadcast. Although will be a high-level view of the technological architecture, it can be passed to technical developers who add more detail at a later stage of the development the ICT service.

For Example: Shopping mall

Shop owners in all large shopping mall have a plan to enrich the shopping experience in their mall. They want to develop a wireless application to be used on smart phones or on PDAs, which will be made available for rent at the entrance. The application will have an informative and an entertainment component. This way, the shop owners hope that they will create added value for their customers and improve their competitiveness.

Because there are many contributors to the development of the application (shop owners, (wireless) network provider, hardware provider), the business model is very complex in this case.

The contributors have composed their interpretation of the Value Proposition, the Value Network, the Revenue model and the Technological architecture in a first quick scan. At several more sessions during the pre-product development stage, these work models were compared and balanced.

This process then was repeated until all contributors are satisfied with the resulting business model. The end result is a thought through, and working innovative application that is slowly starting to generate more sales for the participants.

4.9 THE MOBILE INTERNET FUTURE

With the rapid technology advancements in Artificial intellegence, Integrated Circuitry and increases in Computer processor speeds, thw future of mobile computing looksincreasingly exciting. Use of Artificial intellegence may allow mobile units to be the ultimate in personal secretaries, which can receive emails and paging messages, understand what they are about, and change the individuals personal schedule according to the message. This can then be checked by the individual to plan his/her day.

The working lifestyle has changed, with the majority of pepole working from home, rather than computing. This may be beneficial to the environment as less transportation will be utilized. This mobility aspect may be carried further in that, even in social spheres, pepole are interactive via mobile stations, elimating the need to venture outside of the house.

This scary concept of a world full inanimate zombies(company) sitting locked to their mobile stations, accessing every sphere of their lives via the computer screen becomes ever more real as technology, specially in the field of mobile data communications, rapidly improves.

Indeeded, technogies such as interactive television and video image compression already imply a certain degree of mobility in the home, ie home shopping etc.

4.10 IMPLEMENTING OF MOBILE INTERNET SERVICES

1. Data Optimization in Mobile Telecommunication Network

To have high performance of mobile broadband service either 3G, EVDO or WIMAX service, mobile broadband provider should do many efforts on the telecommunication networks. Data optimization is one of the important things need to be executed on the telecommunication networks with many strategies and scenarios. Since mobile broadband service requires high bandwidth utilization, optimization on transport layer will affect to the entire of mobile broadband performance.

Data optimization on transport layer includes replacing the current low capacity of transmission network into higher capacity. Traditional network to serve traditional sendee (voice and SMS) will require several El transmissions to connect one BTS to the BSC.

To meet to requirement on mobile broadband service, this connection should be upgraded to the higher capacity link e.g. optical fiber, SDH/SONET since there will be huge traffic will flow on this transport layer from the mobile broadband customer that may come together at the same time. Data optimization on this transport layer should be planned preciously and detailed. Some areas where mobile broadband customer is very significant should have bigger capacity on transport layer rather than rural area

Another part of telecommunication network which should be optimized to have affordable mobile broadband service is technology platform which serving mobile broadband sendee. Evolution on telecommunication technology should be planned integrated by utilizing current technology. Mobile broadband provider with 3G platform should plan to migrate to the 4G technology as the next platform. Meanwhile mobile broadband provider with EVDO Rev A platform should plan to migrate to the EVDO Rev B to produce high speed internet access than previous platform.

Data optimization in these strategies is very expensive and need long term vision to develop. More over, integrating with current telecommunication network is mandatory to reduce the cost. Actually the cheaper data optimization on mobile broadband sendee is available and some of mobile broadband provider implement it to provide optimum service.

2. Authentication Process in Mobile Broadband Services

While making a session on mobile broadband service, server will check whether the parameters sent by session from mobile broadband subscriber has meet the condition or not. AAA server will reject the session if it does not meet the condition and allowing to the next process if the authentication process is pass.

TheAuthentication, Authorization and Accounting (AAA) call process of mobile broadband session is running on the application layer, mobile broadband subscriber did not aware about the process. Mobile broadband subscriber needs only to make a session while they want to aeeess to internet

Authentication process on mobile broadband service requires several parameters depend on the network platform implemented by telecommunication companies to provide mobile broadband service. The parameters sent to AAA server while mobile broadband subscriber initiate sessions are

1. Useniame and Password

AAA server already specified the unique username and password that should be sent by mobile broadband subscriber while they initiate a session, AAA server is also specifying the domain that those username and password will be classified. Authentication request from subscriber should contain the same value which already specify on the AAA server. In case username or password does not match, then AAA servers will response with authentication reject. A notification will be displayed on the mobile broadband subscriber with certainty value such as "Invalid Username and Password"

2. IMSI (International Mobile Subscriber Identity)

COM A platform will check mobile broadband subscriber's IMSI (International Mobile Subscriber Identity) when authentication process happens. IMSI (International Mobile Subscriber Identity) is 15 digit numbers which divided into digits of MNC (Mobile Network Code), MCC (Mobile Country Code) and MDN (Mobile Directory Number). Authentication process will check whether session from mobile broadband subscriber has valid IMSI or not. In case the IMSI is valid then will go to the next step and if the IMSI is valid the session will be terminated and AAA server will send authentication reject message.

3. Mobile Broadband: EVPO Services

EVDO is one of mobile broadband service which giving high speed internet accesss to mobile telecommunication subscribers. Evolution Data Optimize/Only (EVDO) is the next data service platform of CDMA lx. EVDO service will guarantee single user receiving download speed up to 3,072 Mbps compared to CDMA lx which maximum can reach 164 kbps. By launched EVDO service telecommunication companies need to expand the capacity of network clement such as Base Controller (BSC), Base Transmission Station (BTS) and definitely international Bandwidth internet

Pre-launch EVDO Service

EVDO Rev A has max physical layer throughput 3,072 Mbps unfortunately it is very difficult while testing EVDO Rev through throughput testing tool such as NEMO and QXDM which can test on the application layer, will have throughput less than 3,072 Mbps e.g. 2,99 Mbps etc

Telecommunication companies need to test the throughput on several cell sites before they launch EVDO service. They can do this by doing access to internet directly and get the throughput while downloading huge file and doing FTP to get and put huge file on local network

Poor throughput and handoff

Two things which should be anticipated by telecommunication companies before they launch EVDO service is eliminate the cell sites (BTS) which have poor throughput and hand off process either from one BTS to another one or from EVDO network to CDMA Ix, Poor throughput could come anytime on EVDO service and caused by many things. Usually poor throughput on BTS is caused by RF capacity or high utilization on the BTS. Telecommunication companies should prepare to add more BTS capacity or redirect the close BTS to the BTS which has poor throughput. Meanwhile handoff process is very critical case to make sure that all sessions will have smooth process while mobile telecommunication subscriber move from one BTS to another one or from EVDO network to CDMAIx.

4. Transport technology and mobile internet services

Transport technology means technologies which utilize to carry out the traffic, mobile internet service traffic from mobile internet subscriber to internet gateway. Transport technology responsible to deliver huge traffic which should come from mobile internet service especially on 3G, EVDO and WIMAX services

Types of transport technologies

Telecommunication companies used to used optical fiber, SONET/SDH and satellite as the transport technologies to support high traffic utilization on mobile internet service. Optical fiber, SONET/SDH and satellite used to utilize to deliver the traffic on the core network

Optical Fiber

There are two types of optical fibers, single mode and multi mode fibers. Single mode has a small core rather than multi mode. Single mode fiber forces the light waves to stay on the same path/mode. Single mode fiber keeps the light going farther before they need to be amplified. Meanwhile multi mode fiber has much larger core than single mode, Multi mode fiber signal can not as far before they need to be amplified

SONET/SDH

Synchronous Digital Hierarchy (SDH) and Synchronous Optical Network (SONET) nodes are known as Add Drop Multiplexers (ADMs). SONET was developed at United Stated and SHD in European. SONET can deliver the packet up to 50 Mbps meanwhile SDH ISOMps

Satellite

Telecommunication companies will utilize satellite technology for secondary link and will be delivered the traffic while primary link (optical fiber) goes down. There are two types of satellite technology, active and passive. A passive satellite only reflects received radio signals back to earth. An active satellite acts as a repeater; it amplifies signals received and then retransmits them back to earth.

5. Wireless Internet Services

Wireless internet service includes CDMA and GSM platforms and its next generation network e.g. 3G, 4G and EVDO platforms. In terms of CDMA platform, there are many network elements of wireless internet service on the CDMA platfonn which involve on the data service call flow such AAA (Authentication, Authorization, and Accounting), Public Data Serving Node (PDSN), Home Local Register (HLR) and charging system

Wireless internet service call flow on Radio Frequency level

Mobile internet service session which comes from modern or mobile phone is the first initialization of the wireless internet service call tlow. Radio Frequency will reserve the resource for this session if any resource is available. 1 case, radio frequency resource is full capacity then network busy notification will be sent to mobile internet service session

Wireless internet service call flow on Public Data Serving Node (PDSN)

Public Data Serving Node PDSN will process the entire of wireless internet service call How. Public Data Serving Node PDSN will communicate with the Base Station Controller through the BSC PCF address (interface A10/A11). Public Data Serving Node (PDSN) connects to the AAA (Authentication, Authorization, and Accounting) servers, allocating IP address for the subscriber, maintaining the session including disconnect the session. Session which conies from BSC will be forwarded by PDSN to AAA server for authentication process at the first stage. While authentication process is pass, PDSN will allocate a IP address for the subscriber.

Wireless Internet Service Call flow on AAA (Authentication, Authorization, and Accounting)

Telecommunication companies could implement AAA (Authentication, Authorization, and Accounting) into two stages where authentication and accounting call flow could land into different network element. This mechanism has many benefits and can be implemented for many purpose such as accounting forwarding, proxy accounting etc.

Authentication process will identify several of authentication information while session arrives on authentication server such as nsername, password, domain and IMS! (International Mobile Subscriber Identification). Authentication will acknowledge the authentication process if the session meets the requirement (useraame, password, domain and IMSI is valid). In case one or more of authentication information is not passed then authentication service will reject the session.

4.11 INFERENCE

Distributed in-network inference plays a significant role in large-scale wireless sensor networks (WSNs) in applications for distributed detection and estimation. Belief propagation (BP) holds great potential for forming an essential and powerful underlying mechanism for such distributed inferences in WSNs. However, it has been recognized that many challenges exist

Notes

in the context of WSN distributed inference. One such challenge is how to systematically develop a graphical model of WSN, upon which BP-based distributed inference can be effectively and efficiently performed, rather than ad hoc.

This section investigates this challenge and proposes a general and rigorous data-driven approach to building a solid and practical graphical model of WSN, given prior observations, based on graphical model optimization.

The proposed approach is empirically evaluated using real-world sensor network data. We show that our approach can significantly reduce the energy consumption in BP-based distributed inference in WSNs and also improve the inference accuracy, when compared to the current practice of distributed inference in WSNs.

4.12 TERRESTRIAL MICROWAVE

There are two types of microwaves in computer networks. These are as follows –

- Terrestrial microwave
- Satellite microwave

Let us discuss terrestrial microwaves in detail.

Terrestrial Microwave

It is a technology which transmits the focused beam of a radio signal from one ground-based microwave transmission antenna to another antenna.

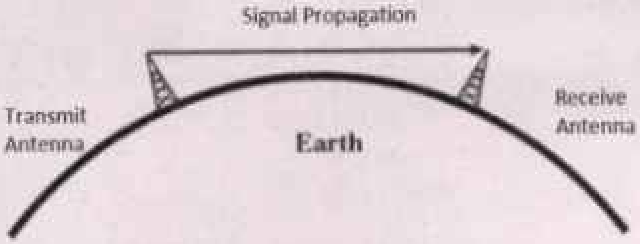
Microwaves are generally an electromagnetic wave which has the frequency in the range from 1GHz to 1000 GHz.

These are unidirectional waves, whereas the sending and receiving antenna is to be aligned which means the antennas are narrowly focused.

Here antennas are mounted on the towers to send a beam to another antenna which is present at km away.

It works on the line-of-sight transmission, which means the antennas mounted on the towers are at the direct sight of each other.

Given below is the diagram of a terrestrial microwave:



Characteristics

The characteristics of a terrestrial microwave are as follows :

- The frequency range of terrestrial microwave is from 4-6 GHz to 21-23 GHz.
- Terrestrial microwaves support the bandwidth from 1 to 10 Mbps.
- These waves are inexpensive for short distances.
- These are expensive as it requires a higher tower for a longer distance.
- The terrestrial microwaves are affected by environmental conditions and antenna size.

Advantages

The advantages of terrestrial microwave are as follows:

- Microwave transmission is cheaper than using cables.
- It is free from land acquisition as it does not require any land for the installation of cables.
- These waves provide easy communication in terrains as the installation of cable in terrain is quite a difficult task.
- Communication over oceans can be achieved by using microwave transmission.

Disadvantages

The disadvantages of terrestrial microwave are as follows:

- Eavesdropping.
- Out of phase signal.
- It is susceptible to weather conditions.
- Bandwidth is limited.

Examples

Some of the examples of terrestrial microwave are as follows:

- Used for long distance telephone services.
- Parabolic dish transmitter mounted high.
- Used for both voice and TV transmission.
- Used by common carriers as well as private networks.

The objects that are tall enough to interface the terrestrial microwaves are as follows –

- Concrete walls (in buildings) can block transmission.
- Electric power transmission lines (in poles) can damage signals.
- Glass (in building windows) can corrupt signals.

Notes

4.13 BROADCAST RADIO

In radio transmission a radiating antenna is used to convert a time-varying electric current into an electromagnetic wave or field, which freely propagates through a nonconducting medium such as air or space. In a broadcast radio channel, an omnidirectional antenna radiates a transmitted signal over a wide service area.

In a point-to-point radio channel, a directional transmitting antenna is used to focus the wave into a narrow beam, which is directed toward a single receiver site. In either case the transmitted electromagnetic wave is picked up by a remote receiving antenna and reconverted to an electric current.

Radio wave propagation is not constrained by any physical conductor or waveguide. This makes radio ideal for mobile communications, satellite and deep-space communications, broadcast communications, and other applications in which the laying of physical connections may be impossible or very costly.

On the other hand, unlike guided channels such as wire or optical fibre, the medium through which radio waves propagate is highly variable, being subject to diurnal, annual, and solar changes in the ionosphere, variations in the density of water droplets in the troposphere, varying moisture gradients, and diverse sources of reflection and diffraction.

Radio-wave Propagation

The range of a radio communications link is defined as the farthest distance that the receiver can be from the transmitter and still maintain a sufficiently high signal-to-noise ratio (SNR) for reliable signal reception. The received SNR is degraded by a combination of two factors: beam divergence loss and atmospheric attenuation. Beam divergence loss is caused by the geometric spreading of the electromagnetic field as it travels through space. As the original signal power is spread over a constantly growing area, only a fraction of the transmitted energy reaches a receiving antenna. For an omnidirectional radiating transmitter, which broadcasts its signal as an expanding spherical wave, beam divergence causes the received field strength to decrease by a factor of 1/r2, where r is the radius of the circle, or the distance between transmitter and receiver.

The other cause of SNR degradation, atmospheric attenuation, depends on the propagation mechanism, or the means by which unguided electromagnetic waves travel from transmitter to receiver. Radio waves are propagated by a combination of three mechanisms: atmospheric wave propagation, surface wave propagation, and reflected wave propagation. They are described below.

Atmospheric propagation

In atmospheric propagation the electromagnetic wave travels through the air along a single path from transmitter to receiver. The propagation path can follow a straight line, or it can curve around edges of objects, such as hills and buildings, by ray diffraction. Diffraction permits mobile phones to work even when there is no line-of-sight transmission path between the phone and the base station.

Atmospheric attenuation is not significant for radio frequencies below 10 gigahertz. Above 10 gigahertz under clear air conditions, attenuation is caused mainly by atmospheric absorption losses; these become large when the transmitted frequency is of the same order as the resonant frequencies of gaseous constituents of the atmosphere, such as oxygen (O_2), water vapour (H_2O), and carbon dioxide (CO_2).

Atmospheric attenuation does not change gradually across the spectrum; there exist short spectral "windows," which specify frequency bands where transmission occurs with minimal clear-air absorption losses. Additional losses due to scattering occur when airborne particles, such as water droplets or dust, present cross-sectional diameters that are of the same order as the signal wavelengths.

Scattering loss due to heavy rainfall is the dominant form of attenuation for radio frequencies ranging from 10 gigahertz to 500 gigahertz (microwave to submillimetre wavelengths), while scattering loss due to fog dominates for frequencies ranging from 103 gigahertz to 106 gigahertz (infrared through visible light range).

Surface propagation

For low radio frequencies, terrestrial antennas radiate electromagnetic waves that travel along the surface of the Earth as if in a waveguide. The attenuation of surface waves increases with distance, ground resistance, and transmitted frequency. Attenuation is lower over seawater, which has high conductivity, than over dry land, which has low conductivity. At frequencies below 3 megahertz, surface waves can propagate over very large distances. Ranges of 100 km (about 60 miles) at 3 megahertz to 10,000 km (6,000 miles) at 1 kilohertz are not uncommon.

Reflected propagation

Sometimes part of the transmitted wave travels to the receiver by reflection off a smooth boundary whose edge irregularities are only a fraction of the transmitted wavelength. When the reflecting boundary is a perfect conductor, total reflection without loss can occur.

However, when the reflecting boundary is a dielectric, or nonconducting material, part of the wave may be reflected while part may be transmitted (refracted) through the medium—leading to a phenomenon known as refractive loss.

When the conductivity of the dielectric is less than that of the atmosphere, total reflection can occur if the angle of incidence (that is, the angle relative to the normal, or a line perpendicular to the surface of the reflecting boundary) is less than a certain critical angle.

Common forms of reflected wave propagation are ground reflection, where the wave is reflected off land or water, and ionospheric reflection, where the wave is reflected off an upper layer of the Earth's ionosphere (as in shortwave radio; see below The radio-frequency spectrum: HF).

Some terrestrial radio links can operate by a combination of atmospheric wave propagation, surface wave propagation, ground reflection, and ionospheric reflection. In some cases this combining of propagation paths can produce severe fading at the receiver. Fading occurs when there are significant variations in received signal amplitude and phase over time or space. Fading can be frequency-selective—that is, different frequency components of a single transmitted signal can undergo different amounts of fading.

A particularly severe form of frequency-selective fading is caused by multipath interference, which occurs when parts of the radio wave travel along many different reflected propagation paths to the receiver.

Each path delivers a signal with a slightly different time delay, creating "ghosts" of the originally transmitted signal at the receiver. A "deep fade" occurs when these ghosts have equal amplitudes but opposite phases—effectively canceling each other through destructive interference.

When the geometry of the reflected propagation path varies rapidly, as for a mobile radio traveling in an urban area with many highly reflective buildings, a phenomenon called fast fading results.

Fast fading is especially troublesome at frequencies above one gigahertz, where even a few centimetres of difference in the lengths of the propagation paths can significantly change the relative phases of the multipath signals. Effective compensation for fast fading requires the use of sophisticated diversity combining techniques, such as modulation of the signal onto multiple carrier waves, repeated transmissions over successive time slots, and multiple receiving antennas.

The radio-frequency spectrum

Before 1930 the radio spectrum above 30 megahertz was virtually empty of man-made signals. Today, civilian radio signals populate the radio spectrum in eight frequency bands, ranging from very low frequency (VLF), starting at 3 kilohertz, and extending to extremely high frequency (EHF), ending at 300 gigahertz.

It is frequently convenient to express radio frequencies in terms of wavelength, which is the ratio between the speed of light through a vacuum (approximately 300 million metres per second) and the radio frequency. The wavelength of a VLF radio wave at 3 kilohertz is thus 100 km (about 60 miles), while the wavelength of an EHF radio wave at 300 gigahertz is only 1 mm (about 0.04 inch).

An important measure of the efficiency with which a transmitting antenna delivers its power to a remote receiving antenna is the effective isotropic radiated power (EIRP), measured in watts per metre squared. To achieve high EIRP the antenna dimensions should be several times larger than the largest transmitted wavelength.

For frequencies below the medium frequency (MF) band, where wavelengths range upward from 100 metres (about 330 feet), this is usually not practical; in these cases transmitters must compensate for low EIRP by transmitting at higher power. This makes frequency bands up through high frequency (HF) unsuitable for such applications as handheld personal radios, radio pagers, and satellite transponders, in which small antenna size and power efficiency are essential.

Two radio links can share the same frequency band or the same geographic area of coverage, but they cannot share both without interference. Therefore, international use of the radio spectrum is tightly regulated by the International Telecommunication Union (ITU), while domestic radio links are regulated by national agencies such as the U.S. Federal Communications Commission (FCC). Each radio link is assigned a specific frequency band of operation, a specific transmitter radiation pattern, and a maximum transmitter power.

For example, a broadcast radio or television station may be authorized to broadcast only in certain directions and only at certain times of the day. Frequency bandwidths also are allocated, ranging from 300 hertz for radiotelegraphs to 10 kilohertz for voice-grade radiotelephones to more than 500 megahertz for multichannel digital radio relays in the telephone network to about 850 megahertz for cellular telephones.

VLF-MF

The very low frequency to medium frequency (VLF-MF) bands extend from 3 kilohertz to 3 megahertz, or wavelengths of 100 km to 100 metres. These bands are used for low-bandwidth analog services such as long-distance radio navigation, maritime telegraph and distress channels, and standard AM radio broadcasting.

Owing to insufficient available bandwidth, they are unsuitable for broadband telecommunication services such as television and FM radio. Because of the high conductivity of salt water, maritime radio transmissions at VLF can propagate via surface waves for thousands of kilometres.

HF

High-frequency (HF) radio is in the 100- to 10-metre wavelength band, extending from 3 megahertz to 30 megahertz. Much of the HF band is allocated to mobile and fixed voice communication services requiring transmission bandwidths of less than 12 kilohertz. International (shortwave radio) broadcasting also is conducted in the HF band; it is allocated to seven narrow bands between 5.9 megahertz and 26.1 megahertz.

The primary mode of propagation for HF radio transmissions is reflection off the ionosphere, a series of ionized layers of the atmosphere ranging in altitude from about 50 to 300 km (about 30 to 200 miles) above the Earth. Ionization is caused primarily by radiation from the Sun, so that the layers vary in height and in reflectivity with time. During the day the ionosphere consists of four layers located at average altitudes of 70 km (D layer), 110 km (E layer), 200 km (F1 layer), and 320 km (F2 layer).

At night the D and E layers often disappear, and the F1 and F2 layers combine to form a single layer at an average altitude of 300 km. Reflective conditions thus change with time. During the day an HF radio wave can reflect off the E, F1, or F2 layers. At night, however, it can reflect only off the high-altitude F layer, creating very long transmission ranges. (The D layer is nonreflecting at HF frequencies and merely attenuates the propagating radio wave.) In the lower HF band, transmission ranges of many thousands of kilometres can be achieved by multiple reflections, called skips, between the Earth and layers of the ionosphere.

4.14 INFRARED AND LIGHT WAVES

- Infrared technology uses diffuse light reflected at walls, furniture etc. or a directed light if a line of sight (LOS) exists between sender and receiver.
- Infrared light is the part of the electromagnetic spectrum, and is an electromagnetic form of radiation. It comes from the heat and thermal radiation, and it is not visible to the naked eyes.

- In infrared transmission, senders can be simple light emitting diodes (LEDs) or laser diodes. Photodiodes act as receivers.
- Infrared is used in wireless technology devices or systems that convey data through infrared radiation. Infrared is electromagnetic energy at a wave length or wave lengths somewhat longer than those of red light.
- Infrared wireless is used for medium and short range communications and control. Infrared technology is used in instruction detectors; robot control system, medium range line of sight laser communication, cordless microphone, headsets, modems, and other peripheral devices.
- Infrared radiation is used in scientific, industrial, and medical application. Night vision devices using active near infrared illumination allow people and animals to be observed without the observer being detected.
- Infrared transmission technology refers to energy in the region of the electromagnetic radiation spectrum at wavelength longer than those of visible light but shorter than those of radio waves.
- Infrared technology allows computing devices to communicate via short range wireless signals. With infrared transmission, computers can transfer files and other digital data bidirectional.

Advantages of Infrared

- The main advantage of infrared technology is its simple and extremely cheap senders and receivers which are integrated into nearly all mobile devices available today.
- No licenses are required for infrared and shielding is very simple.
- PDAs, laptops, notebooks, mobile phones etc. have an infrared data association (IrDA) interface.
- Electrical devices cannot interfere with infrared transmission.

Disadvantages of Infrared

Disadvantages of infrared transmission are its low bandwidth compared to other LAN technologies. Limited transfer rates to 115 Kbit/s and we know that even 4 Mbit/s is not a particular high data rate. Their main disadvantage is that infrared is quite easily shielded.

Infrared transmission cannot penetrate walls or other obstacles. Typically, for good transmission quality and high data rates a LOS (Line of site), i.e. direct connection is needed.

Radio Transmission

Almost all networks use radio waves for data transmission, e.g., GSM at 900, 1800, and 1900 MHz, DECT at 1880 MHz etc. Radio transmission technologies can be used to set up ad-hoc connections for work groups, to connect, e.g., a desktop with a printer without a wire, or to support mobility within a small area.

- The two main types of radio transmission are AM (Amplitude Modulation) and (FM) Frequency Modulation.
- FM minimizes noise and provides greater reliability. Both AM and FM process sounds in patterns that are always varying of electrical signals.
- In an AM transmission the carrier wave has a constant frequency, but the strength of the wave varies. The FM transmission is just the opposite; the wave has constant amplitude but a varying frequency.
- Usually the radio transmission is used in the transmission of sounds and pictures. Such as, voice, music and television.
- The images and sounds are converted into electrical signals by a microphone or video camera. The signals are amplified, and transmitted. If the carrier is amplified it can be applied to an antenna.
- The antenna converts the electrical signals into electromagnetic waves and sends them out or they can be received. The antenna consists commonly of a wire or set of wires.

Advantages of Radio Transmission

- Advantages of radio transmission include the long-term experiences made with radio transmission for wide area networks (e.g. microwave links) and mobile cellular phones. Radio transmission can cover larger areas and can penetrate (thinner) walls, plants, furniture etc.
- Additional coverage is gained by reflection.
- Radio typically does not need a LOS (Line of Site) if the frequencies are not too high.
- Higher transmission rates (e.g. 54 Mbit/s) than infrared (directed laser links, which offer data rates well above 100 Mbit/s).

Disadvantages of Radio Transmission

- Radio transmission can be interfered with other senders, or electrical devices can destroy data transmitted via radio.
- Bluetooth is simple than infrared.
- Radio is only permitted in certain frequency bands.
- Shielding is not so simple.
- Very limited ranges of license free bands are available worldwide and those that are available are not the same in all countries.
- A lot harmonization is going on due to market pressure.

Wireless Multiple Access Protocol

Technological advances, coupled with the flexibility and mobility of wireless systems are the driving force behind the anyone, anywhere, anytime paradigm of networking. At the same time, a convergence of the telephone, cable and data networks into a unified network that supports multimedia and real time applications like voice in addition to data.

Notes

Medium access control protocol defines rules for orderly access to the shared wireless bandwidth. The nature of the wireless channel brings new issues like location dependent carrier sensing, time varying channel and burst errors. Low power requirements and half duplex operation of the wireless systems add to the challenge.

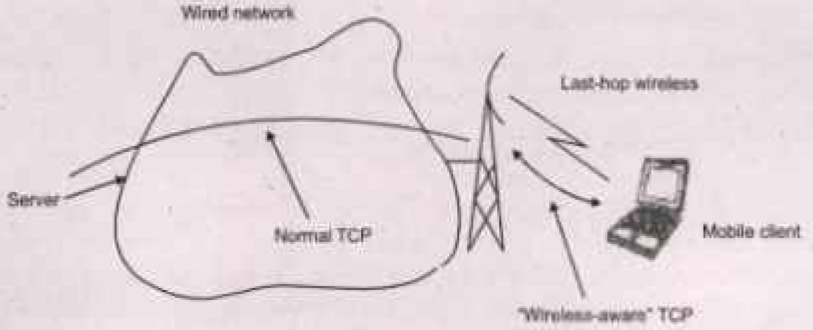
Wireless MAC protocols have been heavily researched and a plethora have been proposed. Protocols have been devised for different types of architectures, different applications and different media.

4.15 TCP OVER WIRELESS

TCP is tuned for wired networks in the sense that packet loss is assumed to be due to congestion only (because error rates in fixed or wired networks are negligible). This assumption fails in wireless networks as error rates in wireless networks may be an order of magnitude larger than in wired networks. Hence, when packets are dropped or corrupted on the wireless link, the congestion control mechanism on the sender kicks in and as a result (of reduction in congestion window size) the throughput decreases drastically.

The increasing popularity of wireless networks indicates that wireless links will play an important role in future internet works. Reliable transport protocols such as TCP have been tuned for traditional networks comprising wired links and stationary hosts. These protocols assume congestion in the network to be the primary cause for packet losses and unusual delays.

TCP performs well over such networks by adapting to end-to-end delays and congestion losses. The TCP sender uses the cumulative acknowledgments it receives to determine which packets have reached the receiver, and provides reliability by retransmitting lost packets. For this purpose, it maintains a running average of the estimated round-trip delay and the mean linear deviation from it. The sender identifies the loss of a packet either by the arrival of several duplicate cumulative acknowledgments or the absence of an acknowledgment for the packet within a timeout interval equal to the sum of the smoothed round-trip delay and four times its mean deviation. TCP reacts to packet losses by dropping its transmission (congestion) window size before retransmitting packets, initiating congestion control or avoidance mechanisms (e.g., slow start and backing off its retransmission timer. These measures result in a reduction in the load on the intermediate links, thereby controlling the congestion in the network.



Wireless Applications

It would be hard to imagine a world without wireless applications and services. Around the globe, mobile services are playing increasingly important roles in many facets of our society. Just a decade ago, mobile services consisted primarily of basic voice communication. Today, we depend on mobile services not only for communication, but also for education, entertainment, healthcare, location and m-commerce. Mobile services have also made significant inroads into developing nations, by improving the quality of life for many of their citizens.

During the past 10 years, mobile services have evolved from basic voice communication to mobile-broadband multimedia services. The mobile-broadband applications and services commercially available around the world owe their existence to the evolution of wireless-technology advancements of yesterday and today.

The technology advancements achieved through air link-performance enhancements higher data rates, optimized quality of service (QoS), reduced latency and increased network capacity—have led to new and enhanced service offerings for mobile operators. As seen in Figure 1, the evolution of wireless technologies has a symbiotic relationship with the evolution of mobile services.

As the evolution of wireless technologies continues to advance, the progression of mobile services will continue to evolve into ever-richer, more compelling mobile and converged services. With end users demanding more and higher-quality multimedia content in all environments, the evolution of device technologies will continue to enhance the increasing consumption of data usage.

Two key beneficiaries of the evolution of wireless technologies, services and devices are mobile operators and consumers. For mobile operators, realized benefits include improved profitability (i.e., lower operating costs and increased ARPU), an increased subscriber base and enhanced customer loyalty. For consumers, benefits include enhanced personal communications, increased convenience and improved entertainment. As mobile services for communication, education, enterprise, entertainment, healthcare, location and retail proliferate, and their consumer adoption increases around the world, one may say that mobile services are indeed becoming the center of life.

4.16 DATA BROADCASTING

Data broadcasting is the broadcasting of data over a wide area via radio waves. It most often refers to supplemental information sent by television stations along with digital television, but may also be applied to digital signals on analog TV or radio. It generally does not apply to data which is inherent to the medium, such as PSIP data which defines virtual channels for DTV or direct broadcast satellite systems; or to things like cable modem or satellite modem, which use a completely separate channel for data.

Data broad casting often provides news, weather, traffic, stock market, and other information which may or may not relate to the program[s] it is carried with. It may also be interactive, such as gaming, shopping, or education. An electronic program guide is usually included, although this stretches the definition somewhat, as this is often considered inherent to the digital broadcast standard.

Notes

The ATSC, DVB and ISDB standards allow for broadband data broadcasting via DTV, though they do not necessarily define how. The over scan and VBI are used for analog TV, for moderate and low bandwidths (including closed captioning in the VBI) respectively. Direct-Band and RDS/RBDS are medium and narrow sub carriers used for analog FM radio.

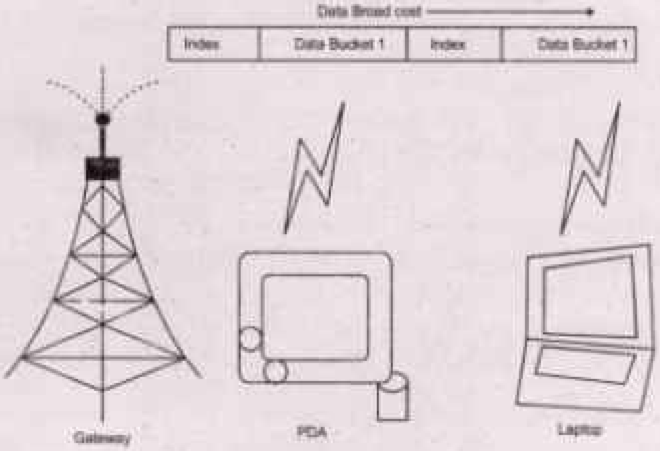
Structure of Broadcast

In broadcast system, there is no traditional network stack. Data is transmitted in the form of buckets. Buckets are also called data blocks or frames. Practically, buckets reside on top of the wireless medium access control (MAC) protocol. In broadcast system, mobile client must wait until the server broadcasts the required information. Therefore, client waiting time is determined by the overall length of broadcast data, which is usually referred to as broadcast cycle.

Clients must keep listenning to the broadcast channel until the arrival of required information. The concept of selective tunning, mobile clients stay in doze mode most of the time and turn into active mode only when the requested information is expected to arrive. Indexing techniques are used to implement selective tunning in wireless environments. Indices are broadcast together with data too help mobile clients locate the required information. In most systems, buckets are classified into index and data buckets.

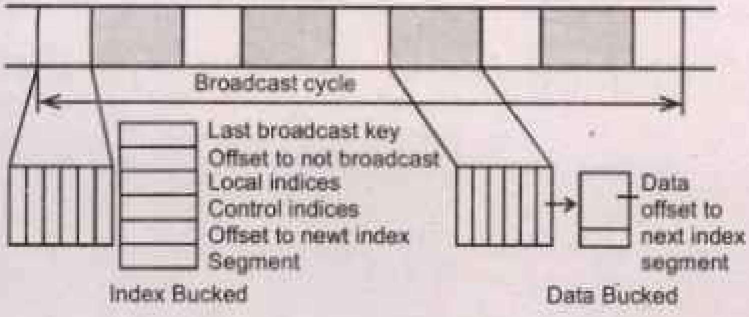
Air indexing is fundamentally different than disk indexing. While disk indices represent a path or an offset in the disk (where accessibility is direct), air indices provide soley a time offset indicating whwrw the pointed item is going to appear in the wireless channel. Therefore, established disk air indexing techniques were accordingly adapted. Most of these indexing schemes are based on three techniques:

- Index Tree
- Signature Indexing
- Hashing



Indexed Broadcast Composition

Hybrid indexing schemes have been proposed as well. The Figure above depicts an example of distributed indexing. The broadcast data is partitioned into several data segments. The index tree precedes each data segment in the broadcast. Users first traverse the index tree to obtain the time offset of the requested data item. After that, they switch to doze mode until the data item arrives.



Index and Data Organization of Distributed Indexing

Services of Data broadcasting

Ambient Information Network

Ambient Information Network, a data broadcasting network owned by Ambient Devices presently hosted by U.S.A. Mobility, a U.S. paging service and focuses on information of interest to the local (or larger) area, such as weather and stock indices, and with a paid subscription Ambient will provide a particular device with more personalized information.

RBDS

A slight variation of the European Radio Data System, RBDS is carried on a 57kHz sub carrier on FM radio stations. While originally intended for program-associated data, it can also be used for data broadcasting purposes including paging and d GPS.

DirectBand

DirectBand, owned by Microsoft, uses the 67.65 kHz sub carrier leased from FM radio stations. This sub carrier delivers about 12 k bit/s (net after error correction) of data per station, for over 100 MB per day per city. Data includes traffic, sports, weather, stocks, news, movie times, calendar appointments, and local time.

Movie Beam

The now-defunct Movie Beam service used NTSC technology by Dot cast to transmit 720p HDTV movies in the lower vestigial sideband of NTSC analog TV. The set-top box stored the movies to be viewed on demand for a fee. This was distributed through PBS's National Data cast.

TV Guide On Screen

TV Guide On Screen is an advertising-supported data cast sent by one local station in each

Notes

media market. It supplements or replaces the limited electronic program guide sent by each TV station, which is already mandated by the U.S. Federal Communications Commission (FCC).

ATSC-M/H

ATSC-M/H is yet another mobile TV standard, although it is transmitted and controlled by the broadcasters instead of a third party, and is therefore mostly free to air (although it can also be subscription-based). From a technical standpoint, it is an IP-encapsulated data cast of MPEG-4 streaming video, alongside the ATSC MPEG transport stream used for over-the-air HDTV/SDTV broadcasting. Heavy error correction, separate from that native to ATSC, compensates for ATSC's poor mobile (and often fixed) reception.

Update TV

Update TV is a service used by some brands of TV sets and other ATSC tuners to update their firmware via over-the-air programming. This is also transmitted on PBS stations via National Data cast.

4.17 MOBILE IP

Mobile IP is the underlying technology for support of various mobile data and wireless networking applications. For example, GPRS depends on mobile IP to enable the relay of messages to a GPRS phone via the SGSN from the GGSN without the sending needing to know the serving node IP address.

Mobile IP can be scan as the least common mobility denominator providing seamless macro mobility solutions among the diversity of accesses. Mobile IP is defining a Home Agent as an anchor point with which the mobile client always has a relationship, and a Foreign Agent, which acts as the local tunnel-endpoint of the access network whose the mobile client is visting. Depending on which network the mobile client is currently visiting; its point of attachement (Foreign Agent) may change. At each point of attachement, Mobile IP either requires the availability of a standaline Foreign Agent or the usage of a co-Located care of address in mobile client itself.

Mobile IP Operation

Mobile IP works by allowing the Mobile Node to be associated with two IP address : a "home address" and a "dynamic case of address". While the home address is fixed, the "care of" address changes at each new point of attachment to the internet. the home IP address assigned to the mobile client makes it logically appear as if the Mobile Node is attached to its home network. It is the IP address where the mobile client seems to be reachable for other Internet clients and services.

For the Correspondent Node, the Mobile Node seems to be attached to the "Home Network" independently of which Network it is currently visiting. A mobile agent (Home Agent) that is provided in a home network receives traffic directed to the mobile client's home IP address even when the mobile client is not physically attached to the home network. When the mobile mode is attached to a foreign netowk a Home Agent routes (tunnels) that traffic to a Foreign Agent using the mobile client's current core of address.

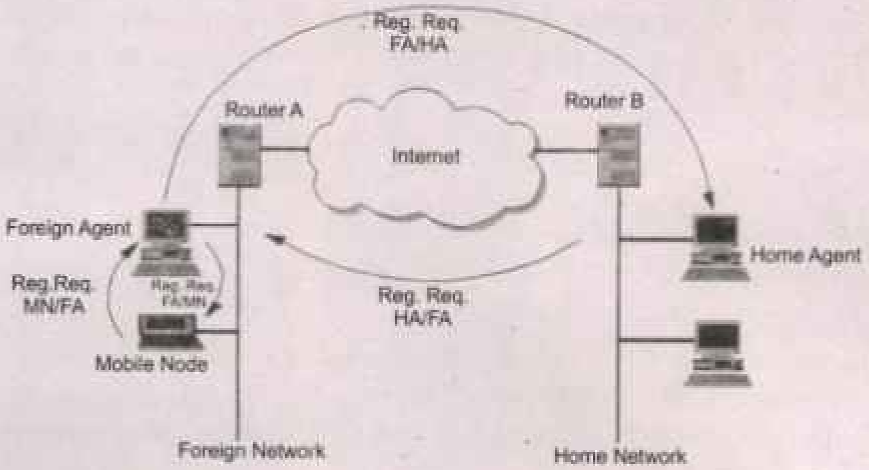
The care of address, which identifies the mobile client's current, topological point of attachment (the Foreign Agent) to the Internet, is used by the Home Agent to route packets to the mobile node. If the Mobile Node is not attached to a foreign network, the Home Agent simply arranges to have the packet data traffic deliered to the mobile client's point of attachement in the home network.

Whenever the Mobile Node moves its point of attachement, it registers a new care of address with its Home Agent. the further delivery by the Home Agent to the Foreign Agent requires that each packet intended for the mobile client be modified/extended so that the care-of address appears as the destination IP address. This modification of the packet is sometimes termed as redirection.

The Home Agent Redirects packets from the home network to the care of address by constructing a new IP header that contains the mobile client's care of address as the packet's destination IP address. This new header "enacapsulates" the original data packet causing the mobile client's home address to have no effect on the encapsulated packet's routing until it arrives at the care of address.

This encapsulation commonly known as tunneling" in the sense that the original data packet is hidden by the new routing "header, while the encapsulated IP header is completly ignored during internet transit.

When the packet arrives at the Foreign Agent the new routing "header is removed and the original packet is sent to the mobile client for properly processing by whatever higher level protocol layer that logically received it from the mobile cleitn's IP layer, processing layer. Tunneling between the agents can be done using IP encapsulation within IP, mechanism specified in. Another encapsulation mechanism is GRE, Generic Routing Encapsulation as specified in.



Basic Mobile IP operation utilizes a technique called triangular routing. Triangular routing means that packets are routed in different paths depending on if the packets are directed to or from the mobile node. Packets from a corresponding node to a mobile client in a visited network are routed from the corresponding node to the Home Agent. The Home

Agent encapsulates. The packets in a Mobile IP tunnel. The tunnel is terminated in the Foreign Agent and the Foreign Agent than Forwards the packet within a layer two technology to the mobile client. In the other direction, from the mobile node to the corresponding node, there is not necessarily a need for tunneling.

In the basic operation packets to the corresponding Node are sent from the mobile node to the Foreign Agent. Since the Corresponding Node is supposed to have a public routable address, it is possible for the Foreign Agent to directly forward the packet to the corresponding node.

In this way, the Home Agent is completely bypassed for corresponding node directly traffic. This technique has some inheait problems though. It cannot support private addressing in a good way since the solution requires unique IP address can every interface. Another problem is that many Internet Routers sterictly filter cut packets that are not orginating from a topologically correct sub-net. The solution for these problems is a technique called "reverse tunneling". Essentially reverse tunneling means that in addition to the "forward tunneling" (become Home Agent to Foreign Agent).

The Foreign Agent also tunnel packets, from the mobile node, back to the Home Agent instead of directly sending them the Corresponding Node. Home Agents and Foreign Agents regularly broadcast agent advertisements (beacans) that include information about one are more corresponding of address when a mobile node receives an agent advertisement. It can obtain IP address of the beacaning Home or Foreign Agent.

The mobile node may also broadcast on advertisement solicitetion that will be answered by any Foreign on Home Agent that receives it. Thus, agent advertisement procedure allaws for the detection of mobility agents (home are foreign). Lets the mobie client determine the network number and status of its link to the Internet, and identifies whether the agent is a Home Agent are a Foreign Agent.

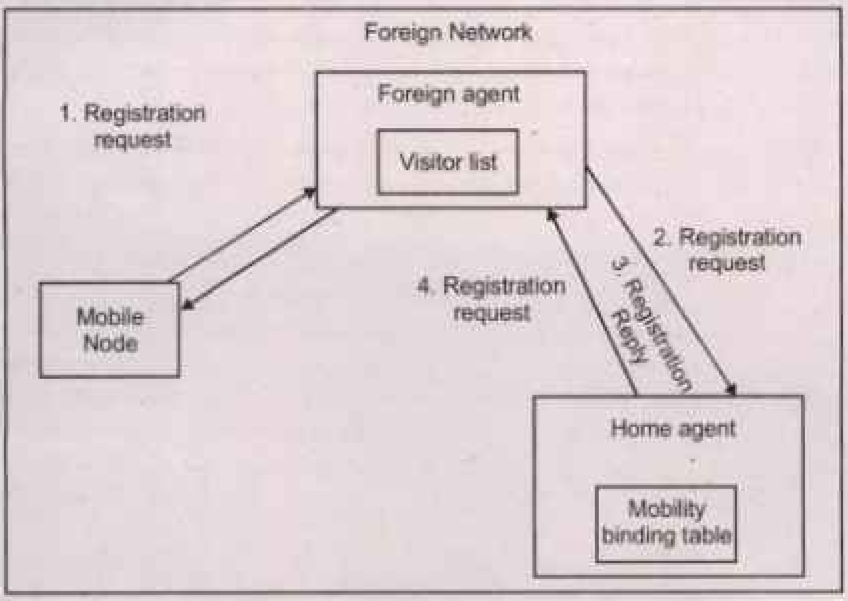
Once a mobile client receives a carve of address, a registeration recaess is used to inform the Home Agent of care of address. The registeration allows the Home Agent :o update its routing table to include the mobile's home address, current care of address and a registeration lifetime.

Capability of Mobile IP

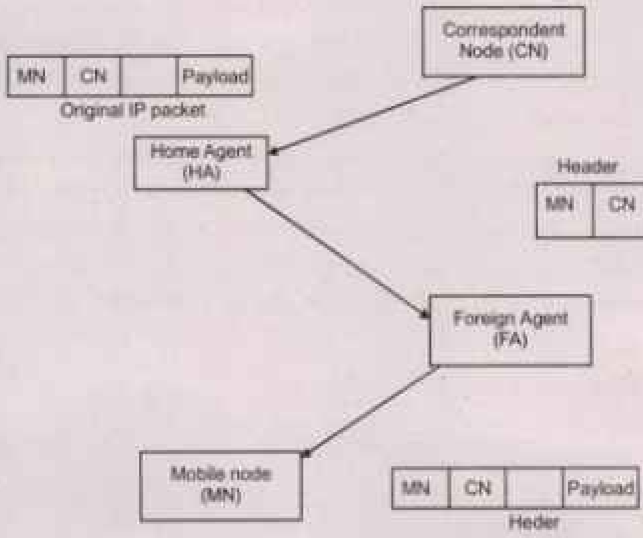
Mobile IP includes three basic capabilities to support the operations:

- Discovery: A mobile nodes uses a discovery procedure to identify prospective home and foreign agents.
- Registration: A mobile node uses an authenticated registration procedure to inform the home agent of its care of address.
- Tunneling: Tunneling is used to forward IP datagram from a home address to a care of address.

Notes



Registration proces in Mobile IP



Tunneling Operation in Mobile IP

4.18 WIRELESS ACCESS PROTOCOL (WAP)

Wireless Access Protocol (WAP) is an open international standard[1] for application-layer network communications in a wireless-communication environment. Most use of WAP involves accessing the mobile web from a mobile phone or from a PDA.

Notes

A WAP browser provides all of the basic services of a computer-based web browser but simplified to operate within the restrictions of a mobile phone, such as its smaller view screen. Users can connect to WAP sites: websites written in, or dynamically converted to, WML (Wireless Markup Language) and accessed via the WAP browser.

Before the introduction of WAP, service providers had extremely limited opportunities to offer interactive data services, but needed interactivity to support now-commonplace activities such as:

- Email by mobile phone
- Tracking of stock-market prices
- Sports results
- News headlines
- Music downloads

The Wireless Application Protocol (WAP) Forum is an industry group dedicated to the goal of enabling sophisticated telephony and information services on hand-held wireless devices such as mobile telephones, pagers, personal digital assistants (PDAs) and other wireless terminals.

Recognizing the value and utility of the World Wide Web architecture, the WAP Forum has chosen to align certain components of its technology very tightly with the Internet and the WWW.

The WAP specifications extend and leverage mobile networking technologies (such as digital data networking standards) and Internet technologies (such as IP, HTTP, XML, URLs, scripting and other content formats).

The WAP specification initiative began in June 1997 and the WAP Forum was founded in December 1997. The WAP Forum has drafted a global wireless protocol specification for all wireless networks and will contribute it to appropriate industry and standards bodies.

WAP will enable manufacturers, network operators, content providers and application developers to offer compatible products and secure services on all devices and networks, resulting in greater economies of scale and universal access to information. WAP Forum membership is open to all industry participants.

The objectives of the WAP Forum are:

- To bring Internet content and advanced data services to digital cellular phones and other wireless terminals.
- To create a global wireless protocol specification that will work across different wireless network technologies.
- To enable the creation of content and applications that scale across a very wide range of wireless bearer networks and wireless device types.
- To embrace and extend existing standards and technology wherever appropriate.

WAP 1.X

The WAP 1.0 standard, released in April 1998, described a complete software stack for mobile internet access.

WAP 2.0

WAP 2.0 released in 2002, a re-engineered WAP, uses a cut-down version of XHTML with end-to-end HTTP (i.e., dropping the gateway and custom protocol suite used to communicate with it). A WAP gateway can be used in conjunction with WAP 2.0; however, in this scenario, it is used as a standard proxy server.

The WAP gateway's role would then shift from one of translation to adding additional information to each request. This would be configured by the operator and could include telephone numbers, location, billing information, and handset information.

4.19 WAP ARCHITECTURE

Wireless Application Protocol (WAP) is a suite of communication protocols for the wireless and mobile devices designed to access the internet independent of manufacturer, vendor, and technology.

The WAP was developed by the WAP Forum, a consortium of device manufacturers, service providers, content providers, and application developers. WAP bridges the gap between the mobile world and the Internet as well as corporate intranets and offers the ability to deliver an unlimited range of mobile value-added services to subscribers—independent of their network, bearer, and terminal.

Mobile subscribers can access the same wealth of information from a pocket-sized device as they can from the desktop. WAP is a global standard and is not controlled by any single company. Ericsson, Nokia, Motorola, and Unwired Planet founded the WAP Forum in the summer of 1997 with the initial purpose of defining an industry-wide specification for developing applications over wireless communications networks.

The WAP specifications define a set of protocols in application, session, transaction, security, and transport layers, which enable operators, manufacturers, and applications providers to meet the challenges in advanced wireless service differentiation and fast/flexible service creation. There are now over one hundred members representing terminal and infrastructure manufacturers, operators, carriers, service providers, software houses, content providers, and companies developing services and applications for mobile devices.

WAP also defines a wireless application environment (WAE) aimed at enabling operators, manufacturers, and content developers to develop advanced differentiating services and applications including a micro browser, scripting facilities, e-mail, World Wide Web (WWW)-to-mobile-handset messaging, and mobile-to-telefax access.

There are three major parts of a WAP-enabled system :

1. WAP Gateway
2. HTTP Web Server
3. WAP Device

WAP Gateway

WAP gateway acts as mediator between Cellular device and HTTP or HTTPS web server. WAP

Notes

gateway routes requests from the client (Cellular Phones) to an HTTP (or Web) server. The WAP gateway can be located either in a telecom network or in a computer network (an ISP).

The HTTP Web Server receive the request from WAP Gateway and process the request and finally sends the output to the WAP Gateway, which in turn the sends this information to the WAP device using it's wireless network.

The WAP Device

Wap device (Cellular phones) is part of wireless network. WAP Device sends the WAP request to the WAP Gateway, which in turn translates WAP requests to WWW requests, so the WAP client is able to submit requests to the Web server. After receiving the response from the the HTTP Web Server, WAP Gateway translates Web responses into WAP responses or a format understood by the WAP client and sends it to the WAP Device.

WAP Protocol Stack

For those of you who want to understand the deep down, nitty-gritty of the WAP, here's a quick summary. The WAP relies on stacked architecture, as does Unix, Windows NT, and most other newer technologies. Because wireless devices have limited memory, some layers of the stack have been offloaded to the WAP gateway (which is part of the service providers" system). The layers, from top to bottom, are:

- the application layer, which relies on the Wireless Application Environment (WAE)
- the session layer, which relies on the Wireless Session Protocol (WSP)
- the transaction layer, which relies on the Wireless Transaction Protocol (WTP)
- the security layer, which relies on the Wireless Transport Layer Security (WLTS)
- the transport layer
- and the network layer.

Overview of WAP

The Wireless Application Protocol (WAP) is a secure specification that allows users to access information instantly via handheld wireless devices such as mobile phones, pagers, two-way radios, smart phones and communicators.

WAP is set of protocols for mobile-internet communication. The Protocol is data transport mechanism or a set of some standard process that allows communication between two or more devices. Devices can be connected with wired or wireless local area network (LAN), Wide Area Network (WAN) and Metropolitan Area Network (MAN). Mobile-Internet communication is a process in which wireless devices, such as cellular phones, pagers, two-way radios, radio transceivers and communicators are used to access the Internet contents. These Internet contents are made visible on mobile devices by WAP.

Wireless devices do not support the existing standard Internet protocols Internet protocols, such as Transmission Control Protocol/Internet Protocols and Hyper Text Transfer Protocols used for computer-to-computer communication over Internet due to usability limitations. Therefore, WAP introduced set of protocols such as Wireless Application Environment and

Wireless Session Protocols for mobile-Internet communication. The set of protocols introduced by WAP protocol stack is developed by WAP forum to access Internet contents through different wireless devices. WAP enabled wireless devices are known as WAP devices.

WAP works across different wireless network environments such LAN and WAN. WAP follows Internet based client/server terminology in which server is a computer that hosts the Web pages and client is computer that access Web pages. However, in WAP, instead of computer, wireless device act as a client and computer act as server.

1. WAP Forum
2. WAP Protocol stack
3. WAP devices.

WAP Forum: AP forum is an organization, founded by Nokia, Ericson, phone.com and Motorola in 1997 to define standards such as WAP protocols stack and WAP architecture for mobile-internet communication. The first version of WAP standards is released. Since them most of the cellular vendors have been developing WAP based components, such as micro browsers and operating systems for WAP devices.

The technologies and protocols that WAP forum used to develop common standards for mobile-Internet communication:-

1. Nokia's Narrow Band Sockets and Tagged Text Markup Language
2. Ericsson's Intelligent Terminal Transfer Protocols
3. Unwired Planet's Handheld Device Markup Language

WAP forum was founded to provide independent wireless network standards for mobile-Internet communicate across different wireless network. WAP forum defined some goals for WAP developers. WAP forum categories goals as follows:-

1. Short-Term Goals
2. Long-Term Goals

WAP Protocol Stack: WAP is a collection of protocols that make complete stack along with the special markup language we say, Wireless Markup Language for WAP application development. The protocols used in WAP are based on Internet protocols such as HTTP and IP.

WAP Devices: WAP enabled wireless devices are called WAP devices. There are so many WAP devices, such as mobile phone, PDAs, pagers and communicators. Each WAP devices consists of two basic characteristics, which as follows:

1. An integrated micro browser that displays information written in WAP supporting mark-up language called WML, on the device screen.
2. A device with user interface such as display screen or touch screen, range of input buttons and scroll buttons.

WAP Benefits

- Operators: New applications can be introduced quickly and easily without the need for additional infrastructure or modifications to the phone. This will allow operators to differentiate themselves from their competitors with new, customized information

Notes

services. WAP is an interoperable framework, enabling the provision of end-to-end turnkey solutions that will create a lasting competitive advantage, build consumer loyalty, and increase revenues.

- Content Providers : Applications will be written in wireless markup language (WML), which is a subset of extensible markup language (XML). Using the same model as the Internet, WAP will enable content and application developers to grasp the tag-based WML that will pave the way for services to be written and deployed within an operator's network quickly and easily. As WAP is a global and interoperable open standard, content providers have immediate access to a wealth of potential customers who will seek such applications to enhance the service offerings given to their own existing and potential subscriber base.
- End Users: End users of WAP will benefit from easy, secure access to relevant Internet information and services such as unified messaging, banking, and entertainment through their mobile devices. Intranet information such as corporate databases can also be accessed via WAP technology. Because a wide range of handset manufacturers already supports the WAP initiative, users will have significant freedom of choice when selecting mobile terminals and the applications they support. Users will be able to receive and request information in a controlled, fast, and low-cost environment, a fact that renders WAP services more attractive to consumers who demand more value and functionality from their mobile terminals.
- Wireless Application Protocol (WAP) is a result of continuous work to define an industry wide standard for developing applications over wireless communication networks. The WAP Forum, originally founded by Ericsson, Motorola, Nokia, and Unwired PlanetWML was formed to create the global wireless protocol specification that works across differing wireless network technology types, for adoption by appropriate industry standards bodies. WML (Wireless Markup Language) is a markup language based on XML, and is intended for use in specifying content and user interface for narrowband devices, including cellular phones and pagers. WML is designed with the constraints of small narrowband devices in mind. These constraints include:

  1. Small display and limited user input facilities;
  2. Narrowband network connection;
  3. Limited memory and computational resources.

WML includes four major functional areas:

1. Text presentation and layout - WML includes text and image support, including a variety of formatting and layout commands;
2. Deck/card organizational metaphor - all information in WML is organized into a collection of cards and decks;
3. Inter-card navigation and linking - WML includes support for explicitly managing the navigation between cards and decks;
4. String parameterization and state management - all WML decks can be parameterized, using a state model."

Advanced WAP

The Wireless Application Protocol (WAP) is an open, global specification that empowers mobile users with wireless devices to easily access and interact with information and services instantly. With more than 300 member companies worldwide, the WAP Forum is the industry association that has developed this de-facto world standard for Internet communications, wireless information and telephony services on digital mobile phones and other wireless terminals.

The primary goal of the WAP Forum is to bring together companies from all segments of the wireless industry value chain to ensure product interoperability and growth of the wireless market. WAP Forum members represent more than 95 percent of the global handset market, carriers with more than 150 million customers, leading infrastructure providers, software developers and other organizations providing solutions to the wireless industry.

WAP Forum Releases Public Review Specifications for Wireless Application Protocol Version 2.0. The WAP Forum has announced the availability of WAP 2.0 for public review. "This next generation of the WAP specification helps content developers deliver a richer and more secure experience to mobile Internet service subscribers. WAP 2.0 is a significant evolutionary step in the worldwide standard and will allow application developers to create compelling mobile content using the same tools and techniques they are already familiar with using for other Internet applications.

As WAP continues convergence with Internet specifications, WAP 2.0 builds upon the latest Internet standards: XHTML, TCP/IP, HyperText Transfer Protocol (HTTP/1.1), and Transport Layer Security (TLS). Utilizing standards developed by the W3C, WAP adopts XHTML and CSS Mobile Profile as part of WML 2.0 (while maintaining backwards compatibility with WML 1.x), to reduce the time necessary to create and test applications and manipulate content for various devices.

At the protocol level WAP 2.0 adopts IETF specifications Supporting XHTML, WAP 2.0 reduces development costs, allowing developers to write applications for both PC and WAP clients, using a common subset of language elements and development tools. XHTML's modular architecture also enables developers to quickly and easily build applications that can adapt to changes in the hardware environment. WAP 2.0 also gives developers the ability to create applications utilizing enhanced style features.

Through the use of Cascading Style Sheets (CSS), developers can separate style attributes for one or more XML documents from the actual code, reducing the size of the markup code in browser memory."

Push Messaging

Push messages are specially formatted messages that give the user the option of connecting directly to a URL via their phone. Push messaging or push technology is a method that allows a server to notify a client when an event occurs. For example, if Twitter is the server, and you are the client, push messaging would involve you getting Tweet notifications. Synchronous conferencing and instant messaging are typical examples of push services. Chat messages and sometimes files are pushed to the user as soon as they are received by the messaging service. Email is also a push system.

Notes

Push Messaging includes audio, short message service (SMS) messages, e-mail, multimedia messaging, cell broadcast, picture messages, surveys, or any other pushed advertising or content.

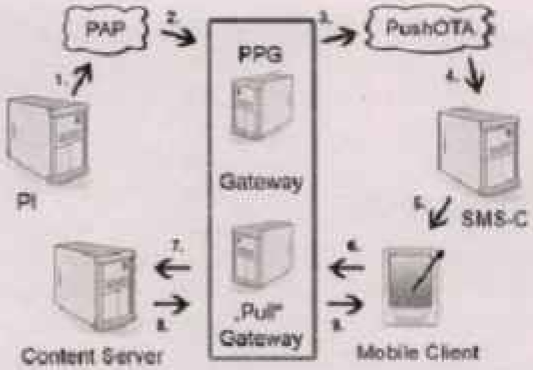
A push message delivers text, XML, and binary content to Windows Mobile Professional and Windows Mobile Standard devices. Push messages always contain a header and body content. For more detailed information about push messages, see the Wireless Application Protocol (WAP) Push Message Specification Version 16-August-1999, available from this Open Mobile Alliance (OMA) Web site.

The following table shows the headers and header extensions used for the Push message.

Header	Description
MSG-010 Generic message headers	Generic message headers identify different features of the message, as described in "Generic Headers" in the WAP Push Message Specification Version 16-August-1999 and the WAP Push Message Specification Information Note Version 11-December-2001. The device accepts the Content-Type header, Content-Location header, and Content-Length header.
MSG-011 Content-Type message header	The Content-Type header identifies the type of content in the message body, as described in "Generic Headers" in the WAP Push Message Specification Version 16-August-1999 and the WAP Push Message Specification Information Note Version 11-December-2001.
MSG-020 WAP message headers	WAP message headers contain WAP-related features of the message, as described in "WAP Headers" in the WAP Push Message Specification Version 16-August-1999 and the WAP Push Message Specification Information Note Version 11-December-2001.
MSG-030 Message header extensions	Message header extensions identify the type of message header, as described in "Header Extensions" in the WAP Push Message Specification Version 16-August-1999 and the WAP Push Message Specification Information Note Version 11-December-2001.

WAP Push Process

WAP Push has been incorporated into the specification to allow WAP content to be pushed to the mobile handset with minimum user intervention. A WAP Push is basically a specially encoded message which includes a link to a WAP address.WAP Push is specified on top of WDP; as such, it can be delivered over any WDP-supported bearer, such as GPRS or SMS. Most GSM networks have a wide range of modified processors, but GPRS activation from the network is not generally supported, so WAP Push messages have to be delivered on top of the SMS bearer.



Process of Push message

On receiving a WAP Push, a WAP 1.2 or later enabled handset will automatically give the user the option to access the WAP content. This is also known as WAP Push SI (Service Indication). The network entity that processes WAP Pushes and delivers them over an IP or SMS Bearer is known as a Push Proxy Gateway (PPG).

End to End WAP services

Such services demand a secured transmission of the packets between the end-user and the server of the service provider. The usual solution recommended by the WAP forum makes use of the WTLS (Wireless Transport Layer Security) protocol layer; this method can, however, only be used to secure the packet transmission between the terminal and the gateway (possibly administered by a mobile network operator).

In this gateway, a conversion of the protocol to the security protocol SSL 3.1 or to the TLS 1.0 is effected.

For example a WAP-enabled GSM (Global System for Mobile Communication) mobile phone that can connect over a digital mobile communication network to a gateway administrated by the operator of this network.

The terminal contains a browser. For example a financial institute or a provider in the field of commerce. This server can access a database where WEB and/or WAP pages are stored. The WEB or WAP pages can contain for example HTML, WML, JAVA-script, WML-script, etc. documents.

In order to access a WEB and/or WAP page in database, a user of terminal has to send a request secured by WTLS services through the gateway to server. This request is decrypted in gateway through all the protocol layers of a converter module, then it is converted into a TLS or SSL-secured request that is sent over a TCP/IP network to the server. In server, another converter module may be provided for converting this request into its own format that can be understood by the database administration system.

The answer of server, for example the contents of a WEB and/or WAP page, is conveyed in the other direction through gateway, where it is converted, to the terminal.This method does not allow for real end-to-end encryption; data and packets need to be decrypted and re-encrypted in gateway to effect is the protocol conversion. For many applications, such a security breach is however not acceptable.

SUMMARY

- Mobile Communication is the use of technology that allows us to communicate with others in different locations without the use of any physical connection (wires or cables). Mobile communication makes our life easier, and it saves time and effort.
- The growth in popularity of new wireless devices continuously increasing day by day. The wireless networks have the ability to start small if necessary, but expand in terms of coverage and capacity as needed - without having to overhaul or build an entirely new network.
- Now a day, wireless networks are much more complex and may consist of hundreds or even thousands of access points, firewalls, switches, managed power and various other components. The wireless networks have a smarter way of managing the entire network from a centralized point.
- Mobile phones are a familiar feature of business life. The traditional telephony features of mobile phones, such as making calls, receiving voicemail, and call diversion, are important to business users.
- Wireless network can also be used to replace wired network. Due to economic reasons it is often impossible to wire remote sensors for weather forecasts, earthquake detection, or to provide environmental information, wireless connections via satellite, can help in this situation.
- Wireless networks utilize radio waves and/or microwaves to maintain communication channels between computers. Wireless networking is a more modern alternative to wired networking that relies on copper and/or fiber optic cabling between network devices.
- A wireless network offers advantages and disadvantages compared to a wired network. Advantages of wireless include mobility and elimination of unsightly cables. Disadvantages of wireless include the potential for radio interference due to weather, other wireless devices, or obstructions like walls.
- Digital technology offers the opportunity for improved transmission in cellular systems. This is due to powerful error detection and recovery techniques, which can be used to counter the debilitating effects of noise, fading and interference. Digital technology also provides the basis for security in the forms of encryption and authentication.

- lobal System for Mobile (GSM) is a second generation cellular standard developed to cater voice services and data delivery using digital modulation.

- Global system for mobile communication (GSM) is a globally accepted standard for digital cellular communication. GSM is developed by Group Special Mobile (founded 1982) which was an initiative of CEPT (Conference of European Post and Telecommunication) to create a common European mobile telephone standard that would formulate specifications for a pan-European mobile cellular radio system operating at 900 MHz. It is estimated that many countries outside of Europe will join the GSM partnership.

- The concept of bandwidth is closely linked to the ability of a system to transmit information. To transfer data, a signal must change in some way and the rate at which these changes occur influences the rate at which information can be transferred.

- Bandwidth conservation is an admirable goal, but whether mobile agents will help realize this goal is questionable. For bandwidth to be conserved, the bandwidth consumed by sending across a mobile agent, and waiting for its results, must be less than that of a series of queries sent via a messaging or RPC system.

- Mobile Communication: Mobile services are changing the landscape of how we communicate daily; specifically, the why, when, how often, and in what degree we communicate. Today, mobile communication can be ubiquitous (anytime, anywhere, anyplace), personal (instant messaging, picture cards, video messaging) or interactive (push-to-talk [PTT], video telephony, video sharing). Using mobile communication services has never been easier or more entertaining

- In radio transmission a radiating antenna is used to convert a time-varying electric current into an electromagnetic wave or field, which freely propagates through a non-conducting medium such as air or space. In a broadcast radio channel, an omnidirectional antenna radiates a transmitted signal over a wide service area.

- TCP is tuned for wired networks in the sense that packet loss is assumed to be due to congestion only (because error rates in fixed or wired networks are negligible). This assumption fails in wireless networks as error rates in wireless networks may be an order of magnitude larger than in wired networks.

- Data broadcasting is the broadcasting of data over a wide area via radio waves. It most often refers to supplemental information sent by television stations along with digital television, but may also be applied to digital signals on analog TV or radio.

- Mobile IP is the underlying technology for support of various mobile data and wireless networking applications. For example, GPRS depends on mobile IP to enable the relay of messages to a GPRS phone via the SGSN from the GGSN without the sending needing to know the serving node IP address.

- Wireless Access Protocol (WAP) is an open international standard[1] for application-layer network communications in a wireless-communication environment. Most use of WAP involves accessing the mobile web from a mobile phone or from a PDA.

- A WAP browser provides all of the basic services of a computer-based web browser but simplified to operate within the restrictions of a mobile phone, such as its smaller view screen. Users can connect to WAP sites: websites written in, or dynamically converted to, WML (Wireless Markup Language) and accessed via the WAP browser.

KEY WORDS

- **Mobile Communication:** It is the use of technology that allows us to communicate with others in different locations without the use of any physical connection (wires or cables).
- **Wireless network :** It can also be used to replace wired network. Due to economic reasons it is often impossible to wire remote sensors for weather forecasts, earthquake detection, or to provide environmental information, wireless connections via satellite, can help in this situation.
- **GSM:** It is global system for mobile communication which is a globally accepted standard for digital cellular communication. GSM is developed by Group Special Mobile (founded 1982) which was an initiative of CEPT (Conference of European Post and Telecommunication) to create a common European mobile telephone standard that would formulate specifications for a pan-European mobile cellular radio system operating at 900 MHz.

REVIEW QUESTIONS

1. What is the fundancental role of mobile computing in wireless communication?
2. What is mobile communication? What are the goals and promises of mobile computing?
3. Explain the view of warless telephony and what are the advantages and disadvantages of it?
4. Describe the applications of mobile communication?
5. Explain wireless communication
6. What are the differences between TCP and Wireless technology?
7. What is broadcasting and how it helps in wireless application?
8. What is WAP? explain functional architecture of WAP.
9. Explain overview of WAP?
10. What is push messaging? What is the process of push message?
11. Write short note on Mobile Internet.

FURTHER READINGS

1. Kurose James F., Ross Keith W. Computer Networking - By Pearson.
2. https://www.javatpoint.com/error-detection-and-correction-code-in-digital-electronics

SWAMI VIVEKANAND

SUBHARTI UNIVERSITY

UGC Approved Meerut

Where Education is a Passion ...

ACCREDITED WITH GRADE A NAAC