EGERTON UNIVERSITY

COLLEGE OF OPEN AND DISTANCE LEARNING

THE E-CAMPUS

E-LEARNING COURSE

ACMP271 : DATA COMMUNICATION AND NETWORKS

By

Peter Kemei

pkemei@egerton.ac.ke or peter.kemei@gmail.com

+254727725372

2021

MAIN INFORMATION PAGE

COURSE PRELIMINARIES

ACMP271: Data Communication and Networks

Is this course for you?

The course is designed to give practical knowledge of the fundamental principles of modern data communications with a focus on physical layer of the network protocol stack. Class discussion complements a series of lab experiments. The course provides practical knowledge of the optical, wireless and wire cable data communication systems relevant to digital data communications, and provides hands-on experience by performing a series of laboratory experiments with a number of important laboratory instruments.

You are expected to complete the course in 45 lecture hours within a period of one semester. The pre-requisites for you to study this course are COMP110, COMP224

Introduction to the course

In this course we aim to provide students with a deeper understanding of foundations of data communication and networks**,** communication concepts. bit and baud rates, synchronous, parallel and serial transmission modes, modulation and demodulation., communication protocols and architecture. Network topologies; bus, star, ring and hierarchical set ups. Basic TCP/IP, Messages, circuit and packet switching. Examples of standard network architecture and Wireless LAN.

Course Outline

There are **Ten (10)** topics in this course, namely:

Topic 1: Concepts & terminology

Topic 2: Protocol Architecture, TCP/IP, and Internet-Based Applications

Topic 3: Analog & Digital signals

Topic 4: Terminal devices i.e. modems, service units etc

Topic 5: OSI model

Topic 6: Protocols

Topic 7: Multiplexing

Topic 8: Network architecture

Topic 9: Packet/Circuit switching

Topic 10: Wireless LAN

Course Learning Outcomes

Upon successful completion of this course, you should be able to:

i. Identify and discuss the basic components of data communications, data networking and the Internet.
ii. Describe protocol architecture, TCP/IP, and Internet-based applications.
iii. Explain data transmission, guided and wireless transmission.
iv. Analyze and describe Local Area Networks and Wide Area Networks.
v. Evaluate communications architecture and protocols.
vi. Describe digital encoding techniques and digital data communication techniques.
vii. Compare packet switching with circuit switching
viii. Basic concepts of Network architecture and wireless LAN

Course Study Skills

As an adult learner your approach to learning will be different to that from your school days: you will choose what you want to study, you will have professional and/or personal motivation for doing so and you will most likely be fitting your study activities around other professional or domestic responsibilities.

Essentially you will be taking control of your learning environment. As a consequence, you will need to consider performance issues related to time management, goal setting, stress management, etc. Perhaps you will also need to reacquaint yourself in areas such as essay planning, coping with exams and using the web as a learning resource.

Your most significant considerations will be time and space, that is, the time you dedicate to your learning and the environment in which you engage in that learning.

We recommend that you take time now - before starting your self-study - to familiarize yourself with these issues. There are a number of excellent resources on the web. A few suggested links are:

http://www.how-to-study.com/

The "How to study" web site is dedicated to study skills resources. You will find links to study preparation (a list of nine essentials for a good study place), taking notes, strategies for reading text books, using reference sources, test anxiety.

http://www.ucc.vt.edu/stdysk/stdyhlp.html

This is the web site of the Virginia Tech, Division of Student Affairs. You will find links to time scheduling (including a "where does time go?" link), a study skill checklist, basic concentration techniques, control of the study environment, note taking, how to read essays for analysis, and memory skills ("remembering").

http://www.howtostudy.org/resources.php

This is another "How to study" web site with useful links to time management, efficient reading, questioning/listening/observing skills, getting the most out of

doing ("hands-on" learning), memory building, tips for staying motivated, developing a learning plan.

Need Help?

This course was developed in April 2020 by Mr. Peter Kemei, **Phone:** +254727725372; **Email:** pkemei@egerton.ac.ke Peter Kemei is a Lecturer of Computer Science in the Department of Computer Science at Egerton University.

This session, the instructor for this course is Mr. Peter Kemei. My office is located in the Department Computer Science, Faculty of Science. You may consult me during the normal working hours between Monday and Friday or contact me through:**Phone:** +254727725372; **Email:** pkemei@egerton.ac.ke Office: Egerton University, Njoro, E-Campus located off the road leading to CMRT opposite the new graduation square.

For technical support e.g. lost passwords, broken links etc. please contact tech-support via e-mail elearning@egerton.ac.ke. You can also reach learner support through elearnersupport@egerton.ac.ke.

Assignments/Activities

Assignments/Activities are provided at the end of each topic. Some assignments/activities will require submission while others will be self-assessments that do not require submission. Ensure you carefully check which assignment require submission and those that do not.

Course Learning Requirements

- Timely submission of the Theory/practicals assignments
- 2 CATs (30%) – CAT 2 marks are derived from assignments.
- Final Examination (70% of total score)

Self-assessment

Self-assessments are provided in order to aid your understanding of the topic and course content. While they may not be graded, you are strongly advised to attempt them whenever they are available in a topic.

TOPIC ONE – DATA COMMUNICATIONS, DATA NETWORKS AND THE INTERNET

Introduction

Welcome to topic one. This topic is aimed at introducing you data communications, data networks, and the internet and defining the terminologies used data communications and networks. You will also contemporary data communication, communications model, communications tasks, data communications model, transmission medium, circuit switching, packet switching frame relay, and asynchronous transfer, types of networking, internet elements and internet architecture. The topic is, therefore, designed to prepare you to have a clear understanding of the data communications and basic concepts and terminologies in data communication and networks.

Topic Time

- Compulsory online reading, activities, self-assessments and practice exercises **[3 hours]**
- Optional further reading **[1.5 hours]**
- Total student input **[4.5 hours]**

Topic Learning Requirements

- Participation in one *chat* (at least 5 entries)
- At least two elaborate contributions to the *discussion* topic. You may also start your own discussion thread.
- Timely submission of the assignments

Learning Outcomes

By the end of this topic you should be able to:

i. State the importance Data Communication and Networks
ii. Define "Data Communication and Networks
iii. Explain Data Communication model

iv. Outline types of networks
v. Explain internet elements and configuration.

Topic Content

1.1 Introduction

Objective of data communication and computer networks:

The fundamental problem of communication is that of reproducing at one point either exactly or approximately a message selected at another point

Data communication refers to the exchange of data between a source and a receiver. Data communication is said to be local if communicating devices are in the same building or a similarly restricted geographical area. The device that transmits the data is known as source and the device that receives the transmitted data is known as receiver. Data communication aims at the transfer of data and maintenance of the data during the process but not the actual generation of the information at the source and receiver

Data communications refers to the transmission of this digital data between two or more computers and a computer network or data network is a telecommunications network that allows computers to exchange data. The physical connection between networked computing devices is established using either cable media or wireless media. The best-known computer network is the Internet.

Data communications is define as exchange of digital information between two digital devices is data communication. Data can exist in a variety of forms such as numbers, text, bits and bytes.

Computer networks: connection of communications devices with the aim of sharing computer resources. Networks exist in various types depend on several factors.

Effective and efficient data communication and networking facilities are vital to any enterprise.

1.1.1 Contemporary Data Communication

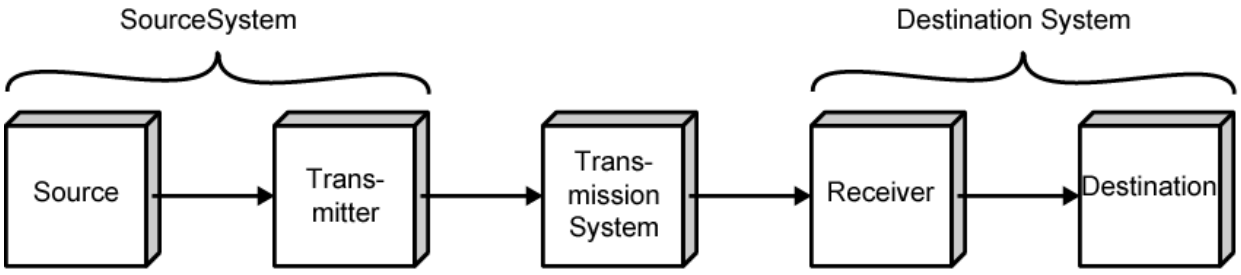
Three different forces have consistently driven the architecture and evolution of data communications and networking facilities: traffic growth, development of new services, and advances in technology.

Momentous changes in the way organizations do business and process information have been driven by changes in networking technology and at the same time have driven those changes. These include a growing need for high-speed LANs in the business environment to support requirements like Centralized server farms, Power workgroups, and High-speed local backbones. Also changes in corporate data traffic patterns are driving the creation of high-speed WANs. Lastly rapid conversion of consumer electronics to digital technology is having an impact on both the Internet and corporate intranets, dramatically increasing the amount of image and video traffic carried by networks.

1.2 A Communications Model

The key elements of this model are:

i. **Source** - generates data to be transmitted
ii. **Transmitter** - converts data into transmittable signals
iii. **Transmission System** - carries data from source to destination
iv. **Receiver** - converts received signal into data
v. **Destination** - takes incoming data



(a) General block diagram

(b) Example

1.3 Communications Tasks

Transmission system utilization	Addressing
Interfacing	Routing
Signal generation	Recovery
Synchronization	Message formatting
Exchange management	Security
Error detection and correction	Network management
Flow control	

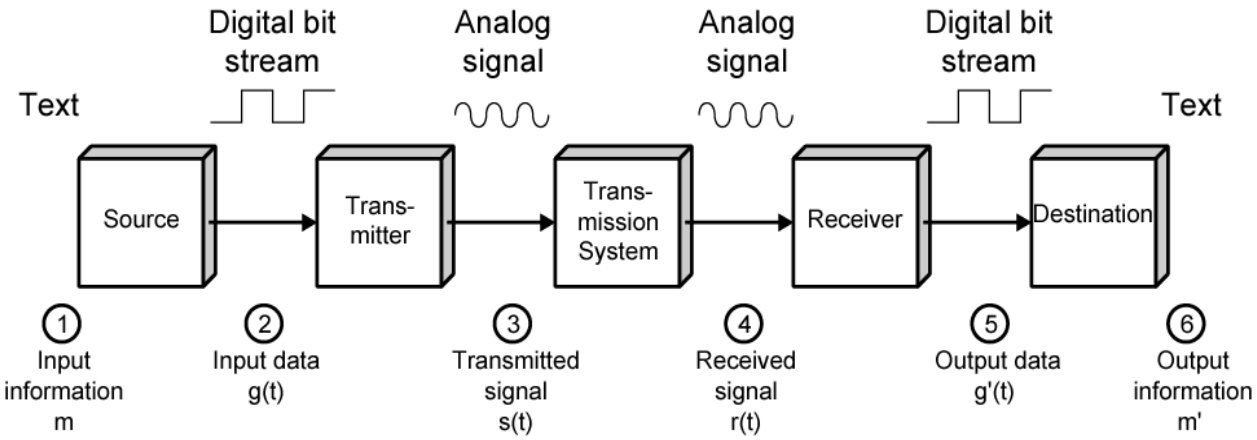
Communicating devices

- Advice must **interface** with the transmission system
- Once an interface is established, **signal generation** is required for communication

- There must be **synchronization** between transmitter and receiver, to determine when a signal begins to arrive and when it ends
- There is a variety of requirements for communication between two parties that might be collected under the term **exchange management**
- **Error detection and correction** are required in circumstances where errors cannot be tolerated
- **Flow control** is required to assure that the source does not overwhelm the destination by sending data faster than they can be processed and absorbed
- **Addressing** and **routing**, so a source system can indicate the identity of the intended destination, and can choose a specific route through this network
- **Recovery** allows an interrupted transaction to resume activity at the point of interruption or to condition prior to the beginning of the exchange
- **Message formatting** has to do with an agreement between two parties as to the form of the data to be exchanged or transmitted
- Frequently need to provide some measure of **security** in a data communications system
- **Network management** capabilities are needed to configure the system, monitor its status, react to failures and overloads, and plan intelligently for future growth

See have gone from the simple idea of data communication between source and destination to a rather formidable list of data communications tasks.

1.4 Data Communications Model

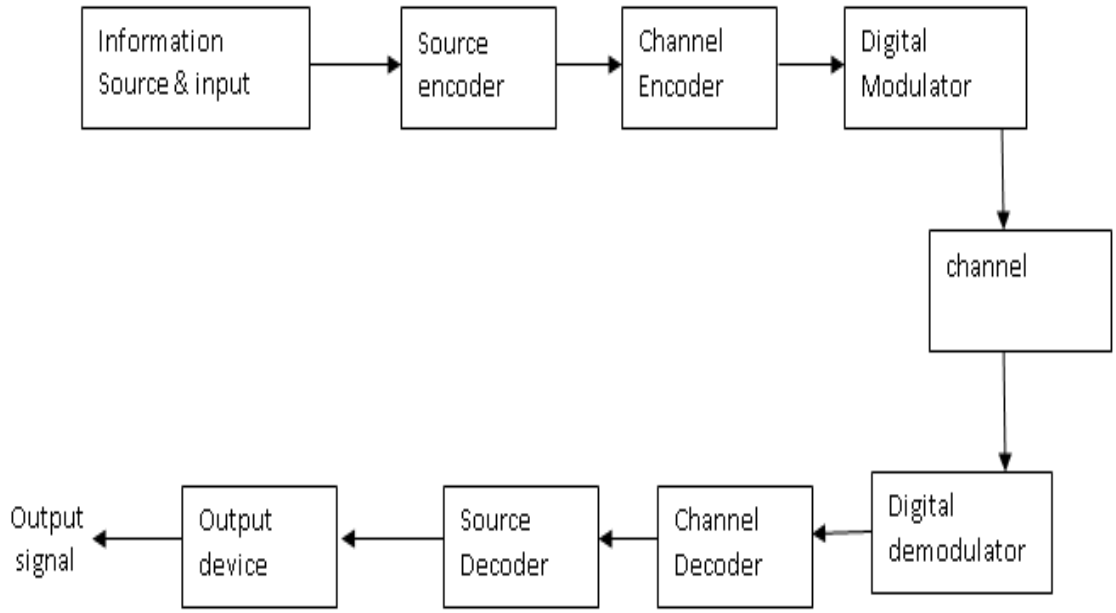


Most fundamental aspects of the communications function, focusing on the transmission of signals in a reliable and efficient manner.

The process is modeled as follows:

- User keys in message m comprising bits g buffered in source PC memory
- Input data is transferred to I/O device (transmitter) as sequence of bits g(t) using voltage shifts
- Transmitter converts these into a signal s(t) suitable for transmission media being used
- Whilst transiting media signal may be impaired so received signal r(t) may differ from s(t)
- Receiver decodes signal recovering g’(t) as estimate of original g(t)
- Which is buffered in destination PC memory as bits g’ being the received message m’

1.4.1 Elements of Data Communication Systems:



Source encoder / Decoder:

The Source encoder (or Source coder) converts the input i.e. symbol sequence into a binary sequence of 0's and 1's by assigning code words to the symbols in the input sequence. For eg. :-If a source set is having hundred symbols, then the number of bits used to represent each symbol will be 7 because 27=128 unique combinations are available. The important parameters of a source encoder are block size, code word lengths, average data rate and the efficiency of the coder (i.e. actual output data rate compared to the minimum achievable rate)

At the receiver, the source decoder converts the binary output of the channel decoder into a symbol sequence. The decoder for a system using fixed – length code words is quite simple, but the decoder for a system using variable – length code words will be very complex.

Channel Encoder / Decoder:

Error control is accomplished by the channel coding operation that consists of systematically adding extra bits to the output of the source coder. These extra

bits do not convey any information but helps the receiver to detect and / or correct some of the errors in the information bearing bits.

The Channel decoder recovers the information bearing bits from the coded binary stream. Error detection and possible correction is also performed by the channel decoder. The important parameters of coder / decoder are: Method of coding, efficiency, error control capabilities and complexity of the circuit

Modulator: The Modulator converts the input bit stream into an electrical waveform suitable for transmission over the communication channel. Modulator can be effectively used to minimize the effects of channel noise, to match the frequency spectrum of transmitted signal with channel characteristics, to provide the capability to multiplex many signals.

Demodulator: The extraction of the message from the information bearing waveform produced by the modulation is accomplished by the demodulator. The output of the demodulator is bit stream. The important parameter is the method of demodulation.

Channel: The Channel provides the electrical connection between the source and destination. The different channels are: Pair of wires, Coaxial cable, Optical fibre, Radio channel, Satellite channel or combination of any of these. The communication channels have only finite Bandwidth, non-ideal frequency response, the signal often suffers amplitude and phase distortion as it travels over the channel. Also, the signal power decreases due to the attenuation of the channel. The signal is corrupted by unwanted, unpredictable electrical signals referred to as noise. The important parameters of the channel are Signal to Noise power Ratio (SNR), usable bandwidth, amplitude and phase response and the statistical properties of noise.

Synchronization: Synchronization involves the estimation of both time and frequency coherent systems need to synchronize their frequency reference with carrier in both frequency and phase.

1.5 Transmission Medium

The basic building block of any communications facility is the transmission line. One of the basic choices facing a business user is the transmission medium. For use within the business premises, this choice is generally completely up to the business. For long-distance communications, the choice is generally but not always made by the long-distance carrier.

In either case, changes in technology are rapidly changing the mix of media used. The ever-increasing capacity of fiber optic channels is making channel capacity a virtually free resource. However, switching is now becoming the bottleneck. The growing use of wireless transmission, is a result of the trend toward universal personal telecommunications and universal access to communications.

Despite the growth in the capacity and the drop in cost of transmission facilities, transmission services remain the most costly component of a communications budget for most businesses. Thus, the manager needs to be aware of techniques that increase the efficiency of the use of these facilities, such as *multiplexing* and *compression.*

1.6 Networking

The number of computers in use worldwide is in the hundreds of millions, with pressure from users of these systems for ways to communicate among all these machines being irresistible. Advances in technology have led to greatly increased capacity and the concept of integration, allowing equipment and networks to deal simultaneously with voice, data, image, and even video.

Have two broad categories of networks: Local Area Networks (LAN) and Wide Area Networks (WAN).

1.6.1 Wide Area Networks (WAN)

Wide area networks generally cover a large geographical area, require the crossing of public right-of-ways, and rely at least in part on circuits provided by a common carrier. Typically, a WAN consists of a number of interconnected switching nodes. Traditionally, WANs have been implemented using one of two

technologies: circuit switching and packet switching. More recently, frame relay and ATM networks have assumed major roles.

Circuit Switching

In a circuit-switching network, a dedicated communications path is established between two stations through the nodes of the network. That path is a connected sequence of physical links between nodes, with a logical channel dedicated to the connection. Data generated by the source station are transmitted along the dedicated path as rapidly as possible. The most common example of circuit switching is the telephone network.

Packet Switching

A packet-switching network uses a quite different approach, without need to dedicate transmission capacity along a path through the network. Rather, data is sent in a sequence of small chunks, called packets. Each packet is passed through the network from node to node along some path leading from source to destination. At each node, the entire packet is received, stored briefly, and then transmitted to the next node. Packet-switching networks are commonly used for terminal-to-computer and computer-to-computer communications.

Frame Relay

Frame relay was developed to take advantage of high data rates and low error rates on modern WAN links. Whereas the original packet-switching networks were designed with a data rate to the end user of about 64 kbps, frame relay networks are designed to operate efficiently at user data rates of up to 2 Mbps. The key to achieving these high data rates is to strip out most of the overhead involved with error control.

Asynchronous Transfer Mode

Asynchronous transfer mode (ATM), is a culmination of developments in circuit switching and packet switching. ATM can be viewed as an evolution from frame relay. ATM uses fixed-length packets, called cells. As with frame relay, ATM provides little overhead for error control, depending on the inherent reliability of the transmission system and on higher layers of logic in the end systems to

catch and correct errors. By using a fixed packet length, the processing overhead is reduced even further for ATM compared to frame relay. The result is that ATM is designed to work in the range of 10s and 100s of Mbps, and in the Gbps range. ATM allows the definition of multiple virtual channels with data rates that are dynamically defined at the time the virtual channel is created.

1.6.2 Local Area Networks (LAN)

A LAN is a communications network that interconnects a variety of devices and provides a means for information exchange among those devices. The scope of the LAN is small, typically a single building or a cluster of buildings. It is usually the case that the LAN is owned by the same organization that owns the attached devices. The internal data rates of LANs are typically much greater than those of WANs.

LANs come in a number of different configurations. The most common are switched LANs and wireless LANs. The most common switched LAN is a switched Ethernet LAN, others are ATM & Fibre Channel LANs. Wireless networks provide advantages in the areas of mobility and ease of installation and configuration.

1.6.3 Metropolitan Area Networks (MAN)

Metropolitan Area Networks provide a middle ground between LANs and WANs, typically spanning a city / metro area e.g private or public network with higher speed connections.

1.7 The Internet

Internet is interconnection of different networks. It evolved from the ARPANET, developed in 1969 by the Advanced Research Projects Agency (ARPA) of the U.S. Department of Defense. It was the first operational packet-switching network. The network was so successful that ARPA applied the same packet-switching technology to tactical radio communication (packet radio) and to satellite communication (SATNET). The need for interworking between these led to Vint Cerf and Bob Kahn of ARPA developing methods and protocols for such *internetworking*, which led eventually to the development of TCP/IP.

1.7.1 Internet Elements

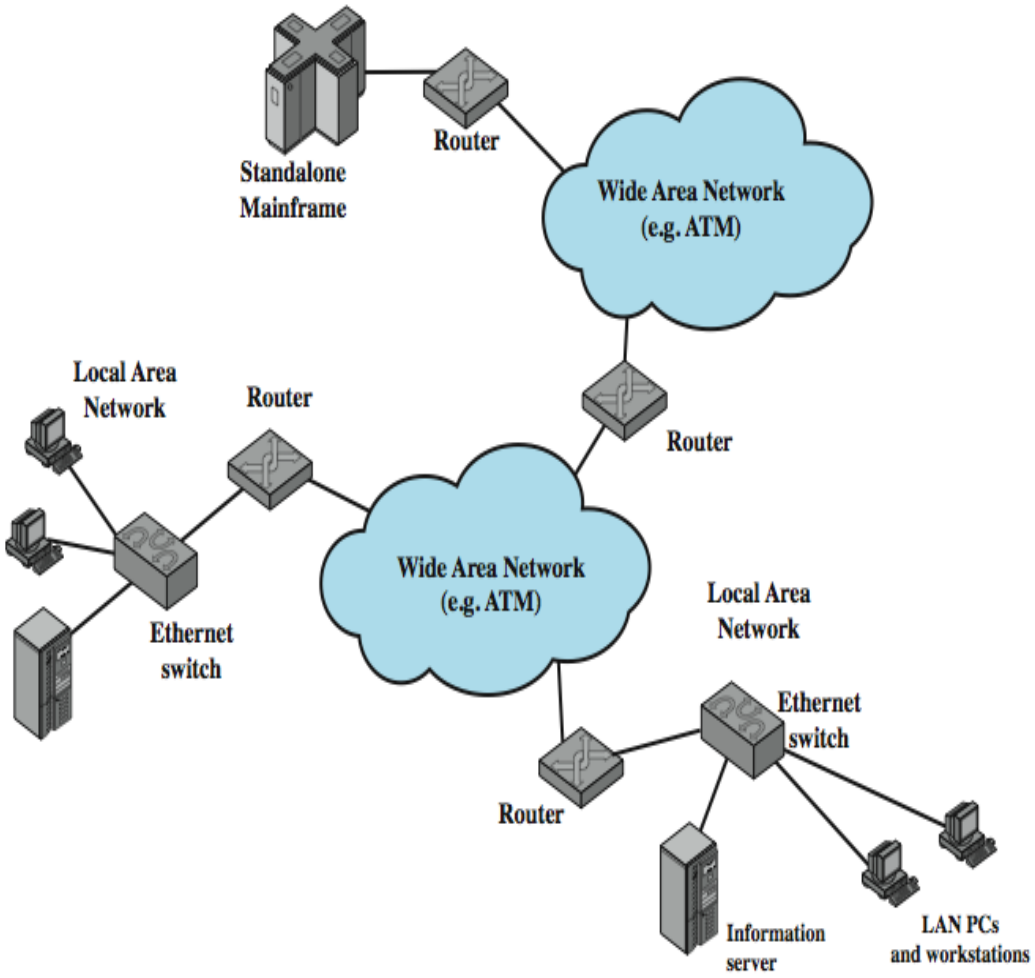
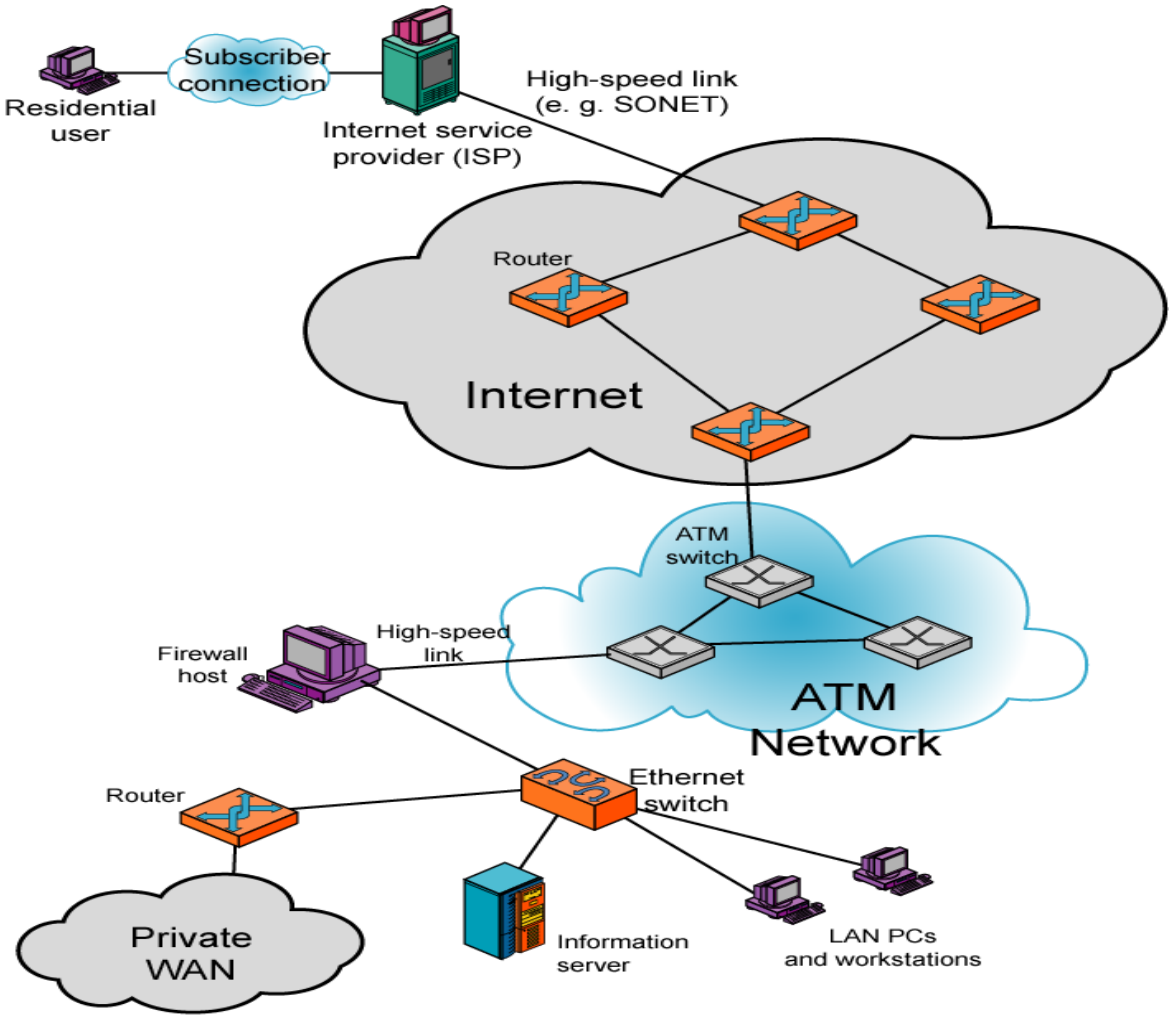


Figure above illustrates the key elements that comprise the Internet, whose purpose is to interconnect end systems, called **hosts**; including PCs, workstations, servers, mainframes, and so on. Most hosts that use the Internet are connected to a **network**, such as a local area network (LAN) or a wide area network (WAN). These networks are in turn connected by **routers**.

Example of Internet Configuration



In summary, you learned that;

i. Importance of data communications needs
ii. Communications model
iii. Definition of data communications
iv. Overview of networks
v. Overview Internet

Glossary

Data communication refers to the exchange of data between a source and a receiver.

Distributed System is a collection of independent computers that appear to the users of the system as a single computer.

Computer networks: connection of communications devices with the aim of sharing computer resources. Networks exist in various types depend on several factors.

Circuit-switching network, a dedicated communications path is established between two stations through the nodes of the network.

A packet-switching network uses a quite different approach, without need to dedicate transmission capacity along a path through the network.

Internet is interconnection of different networks architecture connected globally

Further Reading

Data & Computer networks, Prakash Gupta

William Stallings, Data & Computer networks 10th edition

Any other data communication and networking relevant books, journals, articles e.t.c

TOPIC ACTIVITIES

Activity

In your own opinion list application of network you normally user as describing how data is transferred from your system to another system.

Tips

E.g From your phone to external memory card or from your phone to another

Review

i) Briefly describe with the help of schematic diagram a digital data communication main elements and components.
ii) You want your laptop and cell phone to exchange information. What networking technology might be a requirement as a feature of both your laptop and phone to accomplish this?

iii) What is the principal application that has driven the design of circuit-switching networks?

iv) Use a diagram to review main component of internet configuration

TOPIC TWO – PROTOCOL ARCHITECTURE, TCP/IP, AND INTERNET-BASED APPLICATIONS

Introduction

Welcome to topic one. This topic is aimed at introducing you to need for Protocol architecture, key elements of a protocol, TCP/IP Protocol Architecture, TCP/IP Layers, Operation of TCP and IP. You will learn addressing requirements, operation of TCP/IP, Transmission Control Protocol (TCP), TCP Header, User Datagram Protocol (UDP), UDP Header, IP Header, IPv6 Header and TCP/IP Applications. Also you will learn Layer Specific Standards, Service Primitives and Parameters, Traditional vs Multimedia Applications, Packet structure, subnetting, private and public addressing. The topic is, therefore, designed to prepare you to have a clear understanding of the Protocol Architecture basic concepts, packet structure as well as addressing.

Topic Time

- Compulsory online reading, activities, self-assessments and practice exercises **[3 hours]**
- Optional further reading **[1.5 hours]**
- Total student input **[4.5 hours]**

Topic Learning Requirements

- Participation in one *chat* (at least 5 entries)
- At least two elaborate contributions to the *discussion* topic. You may also start your own discussion thread.
- Timely submission of the assignments

Learning Outcomes

By the end of this topic you should be able to:

vi. State the importance Data Communication and Networks
vii. Define "Data Communication and Networks
viii. Explain Data Communication model
ix. Outline types of networks
x. Explain internet elements and configuration.
xi. Discuss packet structure
xii. Explain network addressing

Topic Content

2.1 Introduction

Need for Protocol Architecture

When computers, terminals, and/or other data processing devices exchange data, the procedures involved can be quite complex. eg. file transfer. There must be a data path between the two computers. But also need:

- Source to activate communications Path or inform network of destination. Source must check destination is prepared to receive.
- File transfer application on source must check destination file management system will accept and store file for his user. May need file format translation. Instead of implementing the complex logic for this as a single module, the task is broken up into subtasks, implemented separately. In a protocol architecture, the modules are arranged in a vertical stack, each layer in the stack performs a related subset of the functions. It relies on the next lower layer to perform more primitive functions. It provides services to the next higher layer. The peer layers communicate using a set of rules or conventions known as a **protocol**.

2.2 Key Elements of a Protocol

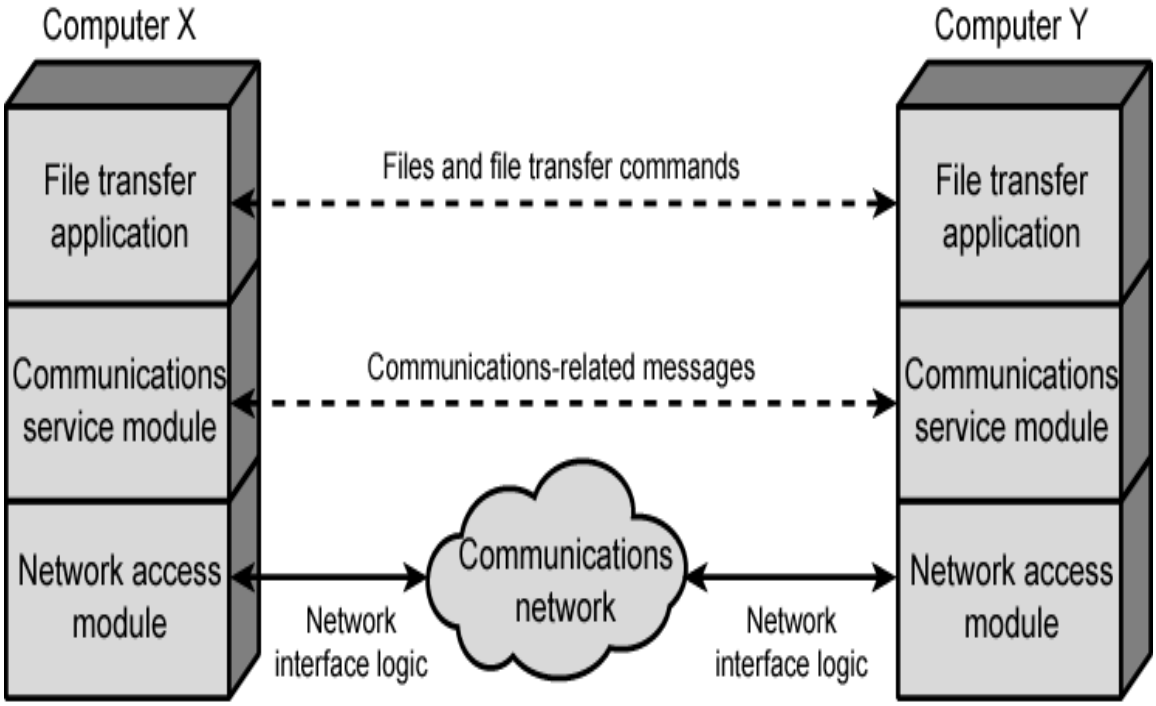
Communication is achieved by having the corresponding, or **peer**, layers in two systems communicate. The peer layers communicate by means of formatted blocks of data that obey a set of rules or conventions known as a **protocol**. The key features of a protocol are:

- **Syntax:** Concerns the format of the data blocks
- **Semantics:** Includes control information for coordination and error handling
- **Timing:** Includes speed matching and sequencing

2.3 TCP/IP Protocol Architecture

The TCP/IP protocol architecture is a result of protocol research and development conducted on the experimental packet-switched network, ARPANET, funded by the Defense Advanced Research Projects Agency (DARPA), and is generally referred to as the TCP/IP protocol suite. This protocol suite consists of a large collection of protocols that have been issued as Internet standards by the Internet Activities Board (IAB).

2.3.1 Simplified Network Architecture



In general terms, communications can be said to involve three agents: applications (eg. file transfer), computers (eg. PCs & servers), and networks. These applications, and others, execute on computers that can often support multiple simultaneous applications. Computers are connected to networks, and the data to be exchanged are transferred by the network from one computer to another. Thus, data transfer involves first getting the data to the computer in

which the application resides and then getting the data to the intended application within the computer. Can think of partitioning these tasks into 3 layers as shown above.

2.4 TCP/IP Layers

TCP/IP have got the following layers

- Application layer
- Host-to-host, or transport layer
- Internet layer
- Network access layer
- Physical layer

2.4.1 Physical Layer

The **physical layer** covers the physical interface between a data transmission device (e.g., workstation, computer) and a transmission medium or network. This layer is concerned with specifying the characteristics of the transmission medium, the nature of the signals, the data rate, and related matters.

2.4.2 Network Access Layer

The network access layer is concerned with the exchange of data between an end system (server, workstation, etc.) and the network to which it is attached. The sending computer must provide the network with the address of the destination computer, so that the network may route the data to the appropriate destination. The sending computer may wish to invoke certain services, such as priority, that might be provided by the network. The specific software used at this layer depends on the type of network to be used; different standards have been developed for circuit switching, packet switching (e.g., frame relay), LANs (e.g., Ethernet), and others. Thus it makes sense to separate those functions having to do with network access into a separate layer.

2.3.3 Internet Layer (IP)

The **internet layer provides** procedures used to allow data to traverse multiple interconnected networks, to provide communications between devices are attached to different networks. The Internet Protocol (IP) is used at this layer

to provide the routing function across multiple networks. This protocol is implemented not only in the end systems but also in routers. A router is a processor that connects two networks and whose primary function is to relay data from one network to the other on its route from the source to the destination end system.

2.3.4 Host-to-Host Layer or Transport Layer

The **host-to-host layer,** or **transport layer**, collects mechanisms in a common layer shared by all applications to provide reliable delivery of data. Regardless of the nature of the applications, there is usually a requirement that data be exchanged reliably, ensuring that all of the data arrives at the destination application and that the data arrives in the same order in which they were sent. These mechanisms for providing reliability are essentially independent of the nature of the applications. The Transmission Control Protocol (TCP) is the most commonly used protocol to provide this functionality.

2.3.5 Application Layer

The **application layer** contains the logic needed to support the various user applications. For each different type of application, such as file transfer, a separate module is needed that is peculiar to that application.

2.4 Operation of TCP and IP

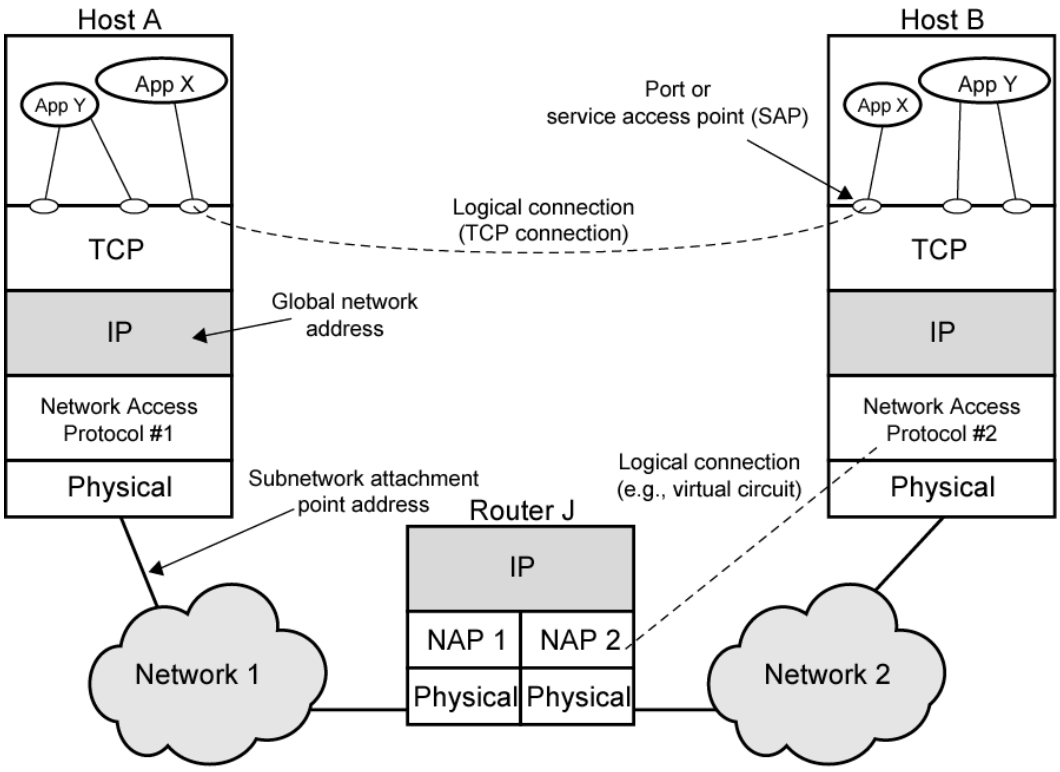
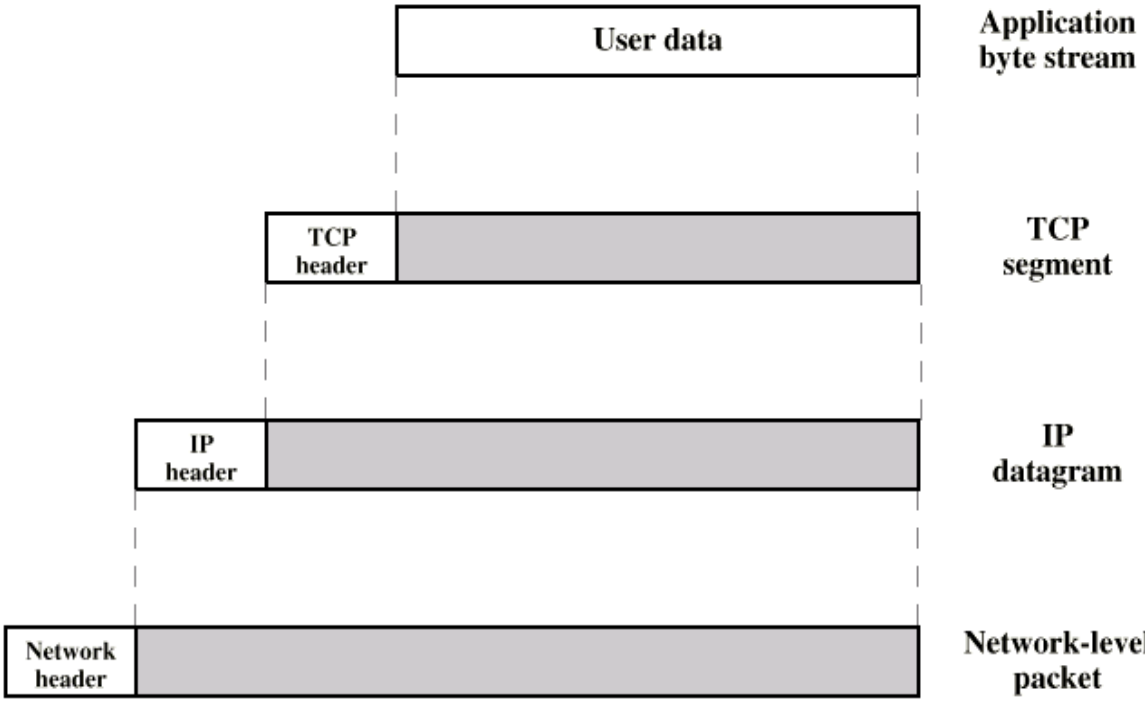


Figure above indicates how these protocols are configured for communications. To make clear that the total communications facility may consist of multiple networks, the constituent networks are usually referred to as **subnetworks**. Some sort of network access protocol, such as the Ethernet logic, is used to connect a computer to a subnetwork. This protocol enables the host to send data across the subnetwork to another host or, if the target host is on another subnetwork, to a router that will forward the data. IP is implemented in all of the end systems and the routers. It acts as a relay to move a block of data from one host, through one or more routers, to another host. TCP is implemented only in the end systems; it keeps track of the blocks of data to assure that all are delivered reliably to the appropriate application.

2.4.1 Operation of TCP/IP



Consider a simple operation where a process on host A, wishes to send a message to another process on host B. The process at A hands the message down to TCP with instructions to send it to host B. TCP hands the message down to IP with instructions to send it to host B. Note that IP need not be told the identity of the destination port. Next, IP hands the message down to the network access layer (e.g., Ethernet logic) with instructions to send it to router J (the first hop on the way to B).

To control this operation, control information as well as user data must be transmitted, The sending process generates a block of data and passes this to TCP. TCP may break this block into smaller pieces to make it more manageable. To each of these pieces, TCP appends control information known as the TCP header, forming a TCP segment.

Next, TCP hands each segment over to IP, with instructions to transmit it to B. These segments must be transmitted across one or more subnetworks and relayed through one or more intermediate routers. This operation, too, requires

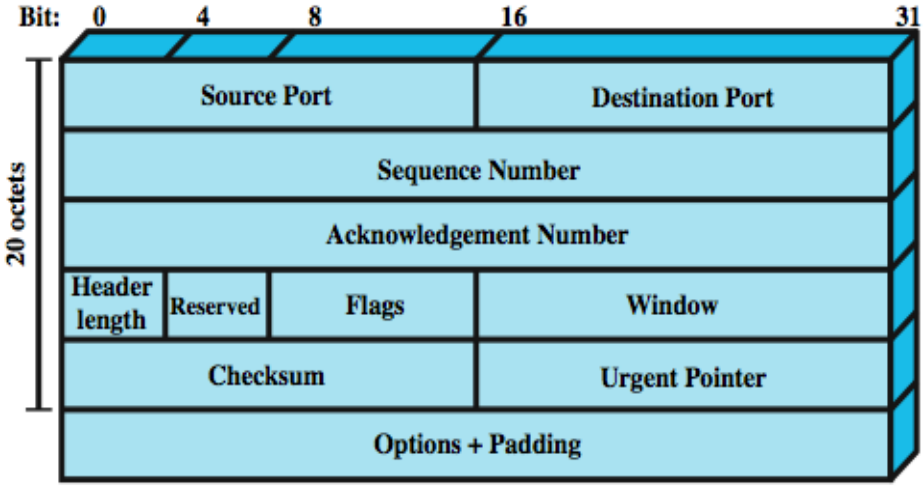
the use of control information. Thus IP appends a header of control information to each segment to form an IP datagram.

Finally, each IP datagram is presented to the network access layer for transmission across the first subnetwork in its journey to the destination. The network access layer appends its own header, creating a packet, or frame. The packet is transmitted across the subnetwork to router J.

2.4.2 Transmission Control Protocol (TCP)

For most applications running as part of the TCP/IP protocol architecture, the transport layer protocol is TCP. TCP provides a reliable connection for the transfer of data between applications. A connection is simply a temporary logical association between two entities in different systems. A logical connection refers to a given pair of port values. For the duration of the connection each entity keeps track of TCP segments coming and going to the other entity, in order to regulate the flow of segments and to recover from lost or damaged segments.

2.4.3 TCP Header



(a) TCP Header

A TCP packet consists of two sections, header and data. All fields may not be used in every transmission. A flag field is used to indicate the type of transmission the packet represents and

how the packet should be interpreted

- **Source port**—identifies the sending application.
- **Destination port**- Identifies the destination application.
- **Sequence number**—Used for assembling segmented data in the proper order at the receiving end
- **Acknowledgement number**—The sequence number the sender (the receiving end) expects next
- **Data offset** or header length —The size of the TCP header, it is also the offset from the start of the TCP packet to the data portion.
- **Reserved**—Reserved for future use, should be set to zero.
- **Flags**(also known as control bits)—contains 6 1-bit flags
    - URG-Urgent pointer field is significant
    - ACK-Acknowledgement field is significant.
    - PSH-Push function.
    - RST-Reset the connection.
    - SYN-Synchronize sequence numbers
    - FIN-No more data from sender.

Window—The number of bytes the sender is willing to receive starting from the acknowledgement field value.

Checksum—used for error-checking of the header and data

Urgent pointer—if the URG flag is set, then this 16-bit field is an offset from the sequence number indicating the last urgent data byte

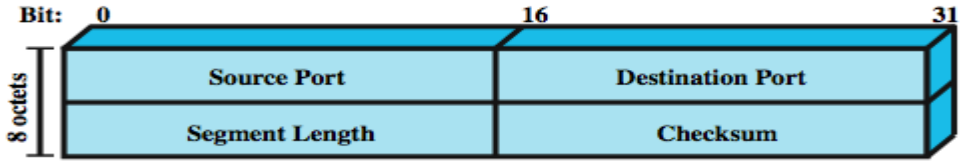
Options—Additional header fields (called options) may follow the urgent pointer

2.4.4 User Datagram Protocol (UDP)

In addition to TCP, there is one other transport-level protocol that is in common use as part of the TCP/IP protocol suite: the User Datagram Protocol (UDP). UDP does not guarantee delivery, preservation of sequence, or protection against duplication. UDP enables a procedure to send messages to other

procedures with a minimum of protocol mechanism. Some transaction-oriented applications make use of UDP; eg SNMP (Simple Network Management Protocol). Because it is connectionless, UDP has very little to do. Essentially, it adds a port addressing capability to IP.

2.4.5 UDP Header



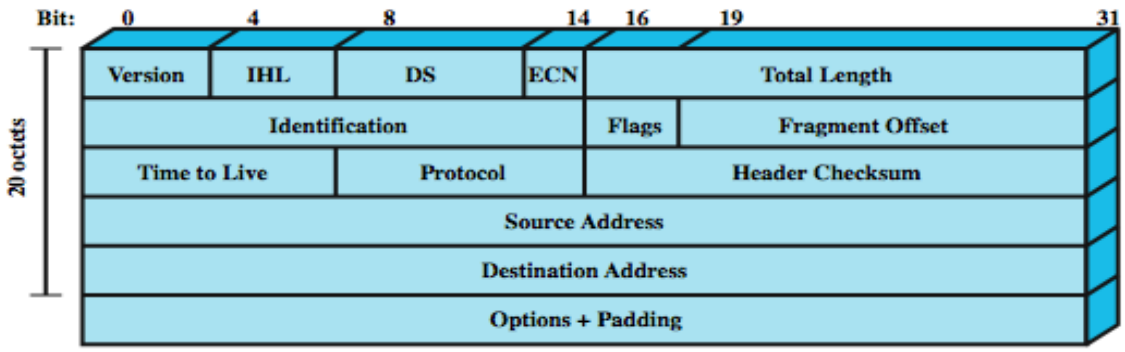
(b) UDP Header

The UDP Packet Structure

The UDP packet structure is illustrated above . It consists of 5 fields, some of which are optional:

- **Source Port-**The sending application. This is an optional field
- **Destination Port-**The target application at the receiving end.
- **Length-**The length of the entire packet.
- **Checksum-**Optional field used to perform basic error correction on the packet.
- **Data-**The user data to be transmitted.

2.4.6 The IPv4 Header



(a) IPv4 Header

The IPv4 Packet Structure (32 bits) by 160 bits

An IP packet consists of two sections; header and data. The header consists of 12 mandatory fields and 1 optional field:

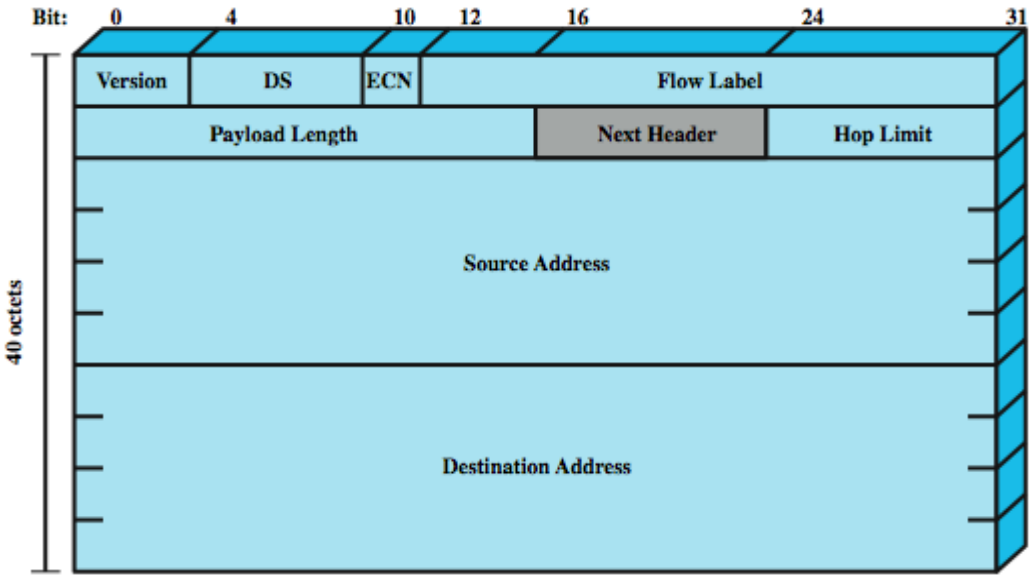
- **Version**—Indicates the IP protocol version being used.
- **Internet Header Length** (IHL)—Indicates the total size of the IP packet header, so the start of the data portion can be determined
- **Type of Service (TOS) or data service (DS)**—Defines delay, throughput and reliability requirement of the IP packet.
- **(ECN) 2** bits are used for Explicit Congestion Notification (ECN).
- **Total Length**—Indicates the entire packet size, including header and data, in bytes.
- **Identification**—Used for uniquely identifying fragments of an original IP datagram.
- **Flags**—Used to control or identify fragments.
- **Fragment Offset**—Allows a receiver to determine the place of a particular fragment in the original IP datagram, measured in units of 8-byte blocks.

Time To Live (TTL): The maximum number of hops a packet can traverse between
the source and destination hosts. Each packet switch (or router) that a packet crosses

decrements the TTL field by one. When the TTL field becomes zero, the packet is
no longer forwarded by a packet switch and is discarded. This mechanism prevents
packets from being trapped in endless routing loops, clogging up a network.

Header Checksum—used for error checking of the header. At each hop, the checksum of the header is compared to the value of this field. If a header checksum is found to be mismatched, the packet is discarded. Because the TTL field is decremented on each hop; the checksum must be recomputed and inserted into the IP packet.

2.4.7 IPv6 Header (32 bits) by 240 bits)



(b) IPv6 Header

IPv6 Packet structure

An IPv6 address is 4 times larger than IPv4, but surprisingly, the header of an IPv6 address is only 2 times larger than that of IPv4. IPv6 headers have one Fixed Header and zero or more Optional (Extension) Headers. All the necessary information that is essential for a router is kept in the Fixed Header. The Extension Header contains optional information that helps routers to understand how to handle a packet/flow.

- **Version** (4-bits): It represents the version of Internet Protocol, i.e. 0110.
- **Traffic Class** (8-bits): These 8 bits are divided into two parts. The most significant 6 bits are used for Type of Service to let the Router Known what services should be provided to this packet. The least significant 2 bits are used for Explicit Congestion Notification (ECN).
- **Flow Label** (20-bits): This label is used to maintain the sequential flow of the packets belonging to a communication. The source labels the sequence to help the router identify that a particular packet belongs to a specific flow of information. This field helps avoid re-ordering of data packets. It is designed for streaming/real-time media.
- **Payload Length** (16-bits): This field is used to tell the routers how much information a particular packet contains in its payload. Payload is composed of Extension Headers and Upper Layer data. With 16 bits, up to 65535 bytes can be indicated; but if the Extension Headers contain Hop-by-Hop Extension Header, then the payload may exceed 65535 bytes and this field is set to 0.

2.4.8 TCP/IP Applications

TCP/IP have a number of standard TCP/IP applications such as cover in topic 6.

- Simple Mail Transfer Protocol (SMTP)
- File Transfer Protocol (FTP)
- Telnet

2.5 Layer Specific Standards

Three elements are key:

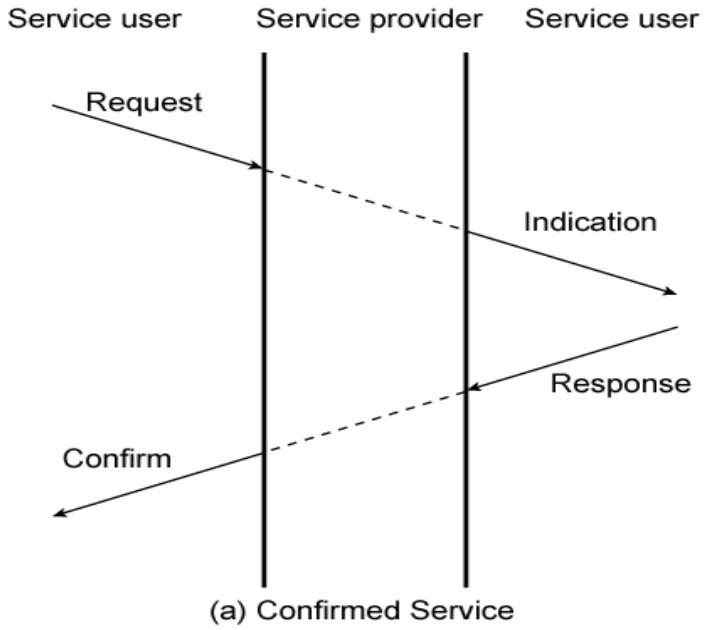
- **Protocol specification**: Two entities at the same layer in different systems cooperate and interact by means of a protocol. Because two different open systems are involved, the protocol must be specified precisely. This includes the format of the protocol data units exchanged, the semantics of all fields, and the allowable sequence of PDUs.
- **Service definition**: In addition to the protocol or protocols that operate at a given layer, standards are needed for the services that each layer

provides to the next higher layer. Typically, the definition of services is equivalent to a functional description that defines what services are provided, but not how the services are to be provided.

- **Addressing**: Each layer provides services to entities at the next higher layer. These entities are referenced by means of a service access point (SAP). Thus, a network service access point (NSAP) indicates a transport entity that is a user of the network service.

2.4.1 Service Primitives and Parameters

i) Define services between adjacent layers using:
ii) Primitives to specify function performed
iii) Parameters to pass data and control information



(a) Confirmed Service

Primitive Types

REQUEST	A primitive issued by a service user to invoke some service and to pass the parameters needed to specify fully the requested service

INDICATION	A primitive issued by a service provider either to: indicate that a procedure has been invoked by the peer service user on the connection and to provide the associated parameters, or notify the service user of a provider-initiated action
RESPONSE	A primitive issued by a service user to acknowledge or complete some procedure previously invoked by an indication to that user
CONFIRM	A primitive issued by a service provider to acknowledge or complete some procedure previously invoked by a request by the service user

2.4.2 Traditional vs Multimedia Applications

The Internet, until recently, has been dominated by information retrieval applications, e-mail, and file transfer, plus Web interfaces that emphasized text and images. Increasingly, the Internet is being used for multimedia applications that involve massive amounts of data for visualization and support of real-time interactivity. Streaming audio and video are perhaps the best known of such applications.

Although traditionally the term *multimedia* has connoted the simultaneous use of multiple media types (e.g., video annotation of a text document), the term has also come to refer to applications that require real-time processing or communication of video or audio alone. Thus, voice over IP (VoIP), streaming audio, and streaming video are considered multimedia applications even though each involves a single media type.

2.4.3 Elastic and Inelastic Traffic

Traffic on a network or internet can be divided into two broad categories: elastic and inelastic.

Elastic traffic can adjust, over wide ranges, to changes in delay and throughput across an internet and still meet the needs of its applications. This is the traditional type of traffic supported on TCP/IP-based internets and is the type of traffic for which internets were designed. Elastic applications include common Internet-based applications, such as file transfer, electronic mail, remote logon, network management, and Web access. But there are differences among the requirements of these applications.

Inelastic traffic does not easily adapt, if at all, to changes in delay and throughput across an internet. The prime example is real-time traffic, such as voice and video. The requirements for inelastic traffic may include the following: minimum throughput may be required, may be delay-sensitive, may require a reasonable upper bound on delay variation, may vary in the amount of packet loss, if any, that they can sustain.

These requirements are difficult to meet in an environment with variable queuing delays and congestion losses. Accordingly, inelastic traffic introduces two new requirements into the internet architecture.

2.5 Packet Structure

A **packet** is one unit of binary data capable of being routed through a computer network.

To improve communication performance and reliability, each message sent between two network devices is often subdivided into packets by the underlying hardware and software.

2.5.1 Packet Structure

Header	Sender's IP address Receiver's IP address Protocol Packet number	96 bits
Payload	Data	896 bits
Trailer	Data to show end of packet Error correction	32 bits

Depending on the protocol(s) they need to support, packets are constructed in some standard **packet format**. Packet formats generally include a header, the body containing the message data (also known as the *payload*), and sometimes a footer (also known as the *trailer*).

- **The header** contains overhead information about the data carried by the packet This information may include:
- **Packet Length**: some packets may be fixed-length, while others rely on the header to contain this information
- **Synchronization:** a few bits that help the packet match up to the network
- **Packet Number**: indicates the position in a sequence of packets
- **Protocol**: defines what type of packet is being transmitted
- **Destination**: indicates where the packet is going
- **Source:** indicates where the packet is coming from
- The header includes:
- An alert signal to indicate that the packet is being transmitted.
- The source address.
- The destination address.
- Clock information to synchronize transmission.

The payload refers to the actual data that the packet is delivering to the destination The payload is sometimes called the body or data of a packet If a

packet is fixed-length, then the payload may be padded with blank information to ensure it is the correct length.

The trailer or footer refers to a set of bits that inform the receiving device that the end of the packet has been reached The trailer is sometimes called the footer of the packet The trailer may also contain some type of error checking The most common error checking used in packets is Cyclic Redundancy Check (CRC).

The receiving device is responsible for re-assembling individual packets into the original message, by stripping off the headers and footers and concatenating packets in the correct sequence.

Example

You send an e-mail to a friend. The e-mail is about 3,500 bits (3.5 kilobits) in size. The network you send it over uses fixed-length packets of 1,024 bits (1 kilobit).

The header of each packet is 96 bits long and the trailer is 32 bits long, leaving 896 bits for the payload.

To break the 3,500 bits of message into packets, you will need four packets (divide 3,500 by 896). Three packets will contain 896 bits of payload and the fourth will have 812 bits. Here is what one of the four packets would contain:

Here is what one of the four packets would contain:

Each packet's header will contain the proper protocols, the originating address (the IP address of your computer), the destination address (the IP address of the computer where you are sending the e-mail) and the packet number (1, 2, 3 or 4 since there are 4 packets).

2.6 Addressing

A core function of IP is to provide logical addressing for hosts. An **IP address** provides a hierarchical structure to both uniquely identify a *host* and what *network* that host exists on.

2.6.1 Addressing Requirements

For successful communication, every entity in the overall system must have a unique address. Actually, two levels of addressing are needed. Each host on a subnetwork must have a unique global internet address; this allows the data to be delivered to the proper host. Each process with a host must have an address that is unique within the host; this allows the host-to-host protocol (TCP) to deliver data to the proper process. These latter addresses are known as ports.

IP addresses

An IP address is a 32-bit number that uniquely identifies a host (computer or other device, such as a printer or router) on a TCP/IP network. IP addresses are normally expressed in dotted-decimal octal format, with four numbers separated by periods, such as 192.168.123.132.

These eight bit sections are known as octets. The example IP address, then, becomes 11000000.10101000.01111011.10000100.

The decimal numbers separated by periods are the octets converted from binary to decimal notation.

an IP address has two parts. The first part of an IP address is used as a network address, the last part as a host address.

For example 192.168.123.132 and divide it into these two parts you get the following:

- 192.168.123. Network
- .132 Host
- 192.168.123.0 - network address. 0.0.0.132 - host address.

Subnet mask

The subnet mask is used by the TCP/IP protocol to determine whether a host is on the local subnet or on a remote network.

In TCP/IP, the parts of the IP address that are used as the network and host addresses are not.

The subnet mask follows two rules:

If a binary bit is set to a **1** (or *on*) in a subnet mask, the corresponding bit in the address identifies the **network**.

If a binary bit is set to a **0** (or *off*) in a subnet mask, the corresponding bit in the address identifies the **host**.

Example 1

- IP Address: 10011110.01010000.10100100.00000011
- Subnet Mask: 11111111.11111111.00000000.00000000

Hosts on the same logical network will have *identical* network addresses b**ut** not same host addresses since the will be IP conflict and can communicate freely. For example, the following two hosts are on the same network:

- **Host A: 158.80.164.100 255.255.0.0**
- **Host B: 158.80.164.101 255.255.0.0**

Both share the same network address (*158.80*), which is determined by the *255.255.0.0* subnet mask.

Example2

Hosts that are on *different* networks cannot communicate without an intermediating device. For example:

- **Host A: 158.80.164.100 255.255.0.0**
- **Host B: 158.85.164.101 255.255.0.0**

The subnet mask has remained the same, but the network addresses are now different (*158.80* and *158.85* respectively). Thus, the two hosts are *not* on the same network, and cannot communicate without a **router** between them.

- **Routing** is the process of forwarding packets from one network to another.

2.7 Network classes

These IP addresses are divided into classes. The most common of these are classes A, B, and C. Classes D and E exist. Each of the address classes has a

different default subnet masks. You can identify the class of an IP address by looking at its first octet.

Class A networks

Class A networks use a default subnet mask of 255.0.0.0 and have 0-127 as their first octet. The address 10.52.36.11 is a class A address. Its first octet is 10, which is between 1 and 126, inclusive.

Class B networks

Class B networks use a default subnet mask of 255.255.0.0 and have 128-191 as their first octet. The address 172.16.52.63 is a class B address. Its first octet is 172, which is between 128 and 191, inclusive.

Class C networks

Class C networks use a default subnet mask of 255.255.255.0 and have 192-223 as their first octet. The address 192.168.123.132 is a class C address. Its first octet is 192, which is between 192 and 223, inclusive.

Default gateways

If a TCP/IP computer needs to communicate with a host on another network, it will usually communicate through a device called a router.

In TCP/IP terms, a router that is specified on a host, which links the host's subnet to other networks, is called a default gateway.

When a host attempts to communicate with another device using TCP/IP, it performs a comparison process using the defined subnet mask and the destination IP address versus the subnet mask and its own IP address.

The result of this comparison tells the computer whether the destination is a local host or a remote host.

If the result of this process determines the destination to be a local host, then the computer will simply send the packet on the local subnet. If the result of the comparison determines the destination to be a remote host, then the computer will forward the packet to the default gateway defined in its TCP/IP properties. It is then the responsibility of the router to forward the packet to the correct subnet.

2.8 CIDR (Classless Inter-Domain Routing)

Classless Inter-Domain Routing (CIDR) is a simplified method of representing a subnet mask. CIDR identifies the number of binary bits set to a **1** (or *on*) in a subnet mask, preceded by a slash.

Example 1

For example, a subnet mask of *255.255.255.240* would be represented as follows in binary:

- 11111111.11111111.11111111.11110000
- The first 28 bits of the above subnet mask are set to *1*. The CIDR notation for this subnet mask would thus be ***/28***.

Address Classes vs. Subnet Mask

Remember the following three rules:

- The **first octet** on an address dictates the *class* of that address.
- The **subnet mask** determines what part of an address identifies the *network*, and what part identifies the *host*.
- Each class has a ***default*** subnet mask. A network using its default subnet mask is referred to as a **classful network**.

Example 2

10.1.1.1 is a Class A address and its default subnet mask is255.0.0.0 (/8 in CIDR).

- Default subnet mask is 10.1.1.1.0

Example 3

- The CIDR mask is often appended to the IP address. An IP address of *192.168.1.1* and a subnet mask of *255.255.255.0* would be represented as follows using CIDR notation:
    - 192.168.1.1 /24

2.8.1 Subnet and Broadcast Addresses

- On each IP network, two host addresses are reserved for special use:

The **subnet** (or **network**) address

The **broadcast** address

Neither of these addresses can be assigned to an actual host.

The **subnet** address is used to identify **the network itself**.

A routing table contains a list of known networks, and each network is identified by its subnet address.

Subnet addresses contain **all 0 bits in the host portion** of the address.

Subnet address example

192.168.1.0/24 is a subnet address. This can be determined by looking at the address and subnet mask in binary:

IP Address: 11000000.10101000.00000001.00000000

Subnet Mask: 11111111.11111111.11111111.00000000

Note that all host bits in the address are set to *0.*

The broadcast address example

The **broadcast** address identifies *all* hosts on a particular network. A packet sent to the broadcast address will be received and processed by every host on that network. Broadcast addresses contain **all 1 bits in the host portion** of the address

- *192.168.1.255/24* is a broadcast address. Note that all host bits are set to *1:*
- IP Address: 11000000.10101000.00000001.11111111
- Subnet Mask: 11111111.11111111.11111111.00000000

Types of IP broadcast packets

- **Unicasts** are packets sent from one host to one other host
- **Multicasts** are packets sent from one host to a *group* of hosts
- **Broadcasts** are packets sent from one host to all other hosts on the local network

2.8.2 Subnetting

Subnetting is the process of creating new networks (or *subnets)* by **stealing bits** from the host portion of a subnet mask. There is one caveat: stealing bits from hosts creates **more** networks but **fewer** hosts per network.

- Consider the following Class C network:
- 192.168.254.0
- The default subnet mask for this network is 255.255.255.0.
- This single network can be segmented, or *subnetted*, into multiple networks.

For example

Assume a minimum of *10* new networks are required. Resolving this is possible using the following magical formula:

- 2^n .The exponent '**n'** identifies the number of bits to steal from the host portion
- The exponent '**n'** identifies the number of bits to steal from the host portion of the subnet mask.
- The default Class C mask (255.255.255.0) looks as follows in binary:
- 11111111.1111111.1111111.00000000

There are a total of 24 bits set to *1*, which are used to identify the network. There are a total of 8 bits set to *0*, which are used to identify the host, and these host bits can be *stolen*

- Stealing bits essentially involves changing host bits (set to *0* or *off*) in the subnet mask to network bits (set to *1* or *on*). Remember, network bits in a subnet mask **must always be contiguous**
- Consider the result if three bits are stolen. Using the above formula:
- $2^n = 2^3 = 8$
- **8 new networks created**

However, a total of 8 new networks *does not* meet the original requirement of at least 10 networks. Consider the result if four bits are stolen:

- $2^n = 2^4 = 16$
- = **16 new networks created**

A total of 16 new networks *does* meet the original requirement. Stealing four host bits results in the following *new* subnet mask:

- **11111111.11111111.11111111.11110000 = 255.255.255.240**

In the previous example, a Class C network was subnetted to create *16* new networks, using a subnet mask of *255.255.255.240* (or */28* in CIDR). Four bits were stolen in the subnet mask, leaving only four bits for hosts.

- for each of the new 16 networks, a slightly modified formula is required:
- $2^n - 2$

Consider the result if four bits are available for hosts:

- $2^n - 2 = 2^4 - 2 = 16 - 2 =$ **14 usable hosts per network**

Thus, subnetting a Class C network with a /28 mask creates 16 new networks, with 14 usable hosts per network.

Why is the formula for calculating usable hosts $2^n - 2$? Because it is **never possible** to assign a host an address with all *0* or all *1* bits in the *host* portion of the address**.**

These are reserved for the **subnet** and **broadcast addresses** respectively. Thus, every time a network is subnetted, useable host addresses are lost.

Example 1

You have been provided with the IP Address range 202.200.10.128/26. Determine the following

i) Subnet mask in dotted quad notation
ii) The maximum number of hosts in the subnet
iii) The available host address (list them)
iv) The subnet address
v) The broadcast address
vi) Network class

Solution

Class C Addressing

Default Subnet mask address for this network using CIDR slash /26 the last quad is

i) 11111111.11111111.11111111.11000000 **= 255.255.255.192**

ii) Maximum Number of Hosts in the subnet, Host bits = 6 hosts Therefore hosts are2^6 - 2 = 64-2= **62 hosts.**

iii) The available host addresses(list them), **202.200.10.129 – 202.200.10.190**

iv) The subnet address , first address is subnet address **= 202.200.10.0**

v) The broadcast address, last address is broadcast address **= 202.200.10.255**

vi) **Class C** first octets range between **192** and **223,**

2.9 Public Address and Private Address

A public IP address, in common parlance, is synonymous with a *globally routable unicast IP address.*

A **public address** can be routed on the Internet. Thus, devices that must be Internet-accessible must be configured with (or *reachable* by) public addresses.

A **private address** is intended for internal use within a home or organization, and can be freely used by anyone.

Private addresses can *never be routed* on the Internet. Three private address ranges for each class are

i) Class A – **10.0.0.0 -10.255.255.255**

ii) Class B - **172.16.0.0- 172.31.0.0**

iii) Class C - **192.168.0.0- 192.168.255.255**

In summary, you learn

- Need for Protocol Architecture
- TCP/IP Protocol Architecture
- Traditional Vs Multimedia Application Needs
- Packet Structure
- Network Addressing

Glossary

Protocol is language used by network systems to communicate using a set of rules or conventions.

TCP/IP is a protocol suite consists of a large collection of protocols that have been issued as Internet standards.

A **packet** is one unit of binary data capable of being routed through a computer network.

An **IP address** is a hierarchical structure to both uniquely identify a *host* and what *network* that host exists on.

Classless Inter-Domain Routing (CIDR) is a simplified method of representing a subnet mask.

Subnetting is the process of creating new networks (or *subnets)* by **stealing bits** from the host portion of a subnet mask.

Further Reading

Data & Computer networks, Prakash Gupta

William Stallings, Data & Computer networks 10th edition

Any other data communication and networking relevant books, journals, articles e.t.c

TOPIC ACTIVITIES

Activity

In own opinion list applications under elastic and inelastic use do using your own mobile phone.

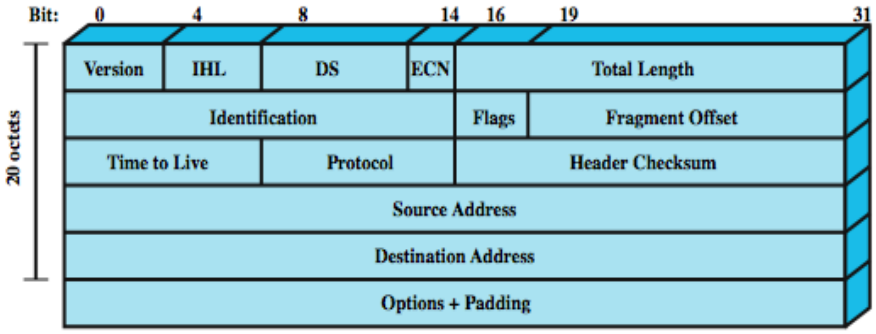
Tips

Identify your mobile specifications, applications and features to guide you appreciate your mobile usability capabilities.

Review

i) Discuss how your mobile phone is able to connect to internet using TCP/IP and UDP provide practical example for each.

ii) The image below depicts the format of the IP header.



Briefly indicate the purpose of the following IPv4 header fields:

a) Version,

b) Time-To-Live,

c) Flags,

d) Header checksum.

iii) Outline the main differences between unicast, broadcast and multicast internet protocol citing real life practical example

iv) Compute the subnet mask, subnet address ad broadcast address for each of the following IP subjects.

a) 196.202.221.16/28

b) 10.10.2.64/30

vii) A host was given the IP addresses 192.168.3.219 /29. Consider this address and indicate:

a) The network address to which the host belongs.

b) The total number of hosts available in the network

TOPIC THREE: ANALOG & DIGITAL SIGNALS

Introduction

Welcome to topic one. This topic is aimed at introducing main concepts of analog & digital signals components, medium, communication links, analog and digital signal, signal main components, wavelength, frequency domain and bandwidth, analog and digital data transmission, transmission impairments, channel capacity, data transmission modes,channel concepts, modulation and demodulation and broadband transmission.

The topic is, therefore, designed to prepare you to have a clear understanding of character encoding techniques and factors that affect performance of the network.

Topic Time

- Compulsory online reading, activities, self-assessments and practice exercises **[3 hours]**
- Optional further reading **[1.5 hours]**
- Total student input **[4.5 hours]**

Topic Learning Requirements

- Participation in one *chat* (at least 5 entries)
- At least two elaborate contributions to the *discussion* topic. You may also start your own discussion thread.
- Timely submission of the assignments

Learning Outcomes

By the end of this topic you should be able to:

i) Explain main concepts of analog & digital signals components,
ii) Discuss medium and communication links,
iii) Describe analog signal ,digital signal and signal main components
iv) Discuss analog and digital data transmission,
v) Explain transmission impairments,
vi) Discuss channel capacity
vii) Describe data transmission modes, and channel concepts,

viii) Discuss modulation and demodulation terminologies and broadband transmission

ix) Discuss character encoding techniques

x) Explain factors that affect performance of the network.

Topic Content

3.1 Introduction

Concepts and terminologies

- **Transmitter:** Converts data into transmittable signals
- **Receiver**: Converts received signal into data
- **Communication** is in the form of electromagnetic waves.
- **Medium**: carries data, may classified as
  - Guided medium: the waves are guided along a physical path. e.g. twisted pair, optical fiber,coxial cable
  - Unguided medium (wireless):provide a means for transmitting electromagnetic waves but do not guide them. e.g. air, water, vacuum (space)

3.2 Communication Links

Direct link: no intermediate devices (no amplifiers or repeaters), the signal propagates directly from transmitter to receiver. This term can apply to both guided an unguided media.

Point-to-point: provides direct link between two devices and those are the only 2 devices sharing the link.

Multi-point guided configuration: more than two devices share the same link

3 .3 Analog and Digital Signals

An analog signal is a continuously varying electromagnetic wave that may be propagated over a variety of media:

A digital signal is a sequence of voltage pulses that can be transmitted over a wire medium: e.g. a constant positive level to represent binary 0 and a constant negative level to represent binary 1.

3.3.1 Time domain concepts:

Time domain concepts: signal viewed as a function of time, an electromagnetic signal can be either analog or digital:

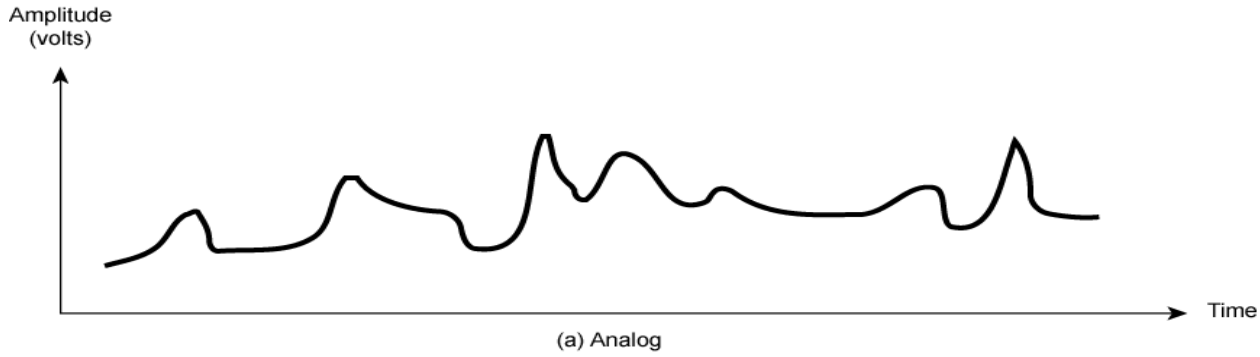
Analog signal: the signal intensity varies in a smooth fashion over time . Continuous signal .No breaks or discontinuities in the signal.

Digital signal: signal intensity maintains a constant level then changes to another constant level. Discrete signal. This is an idealized definition; in fact there is a small transition period.

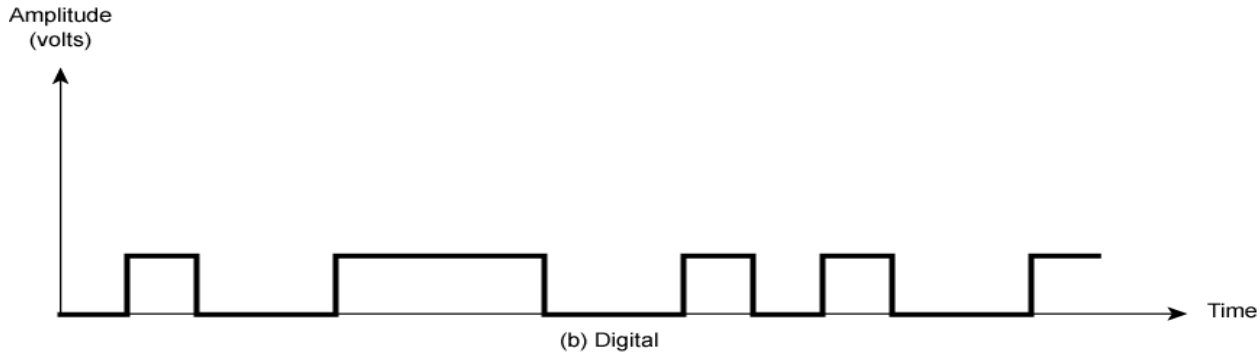
Periodic signal: the same signal pattern repeats over time

A periodic signal: pattern does not repeat over time

Analog and Digital Signals Representation

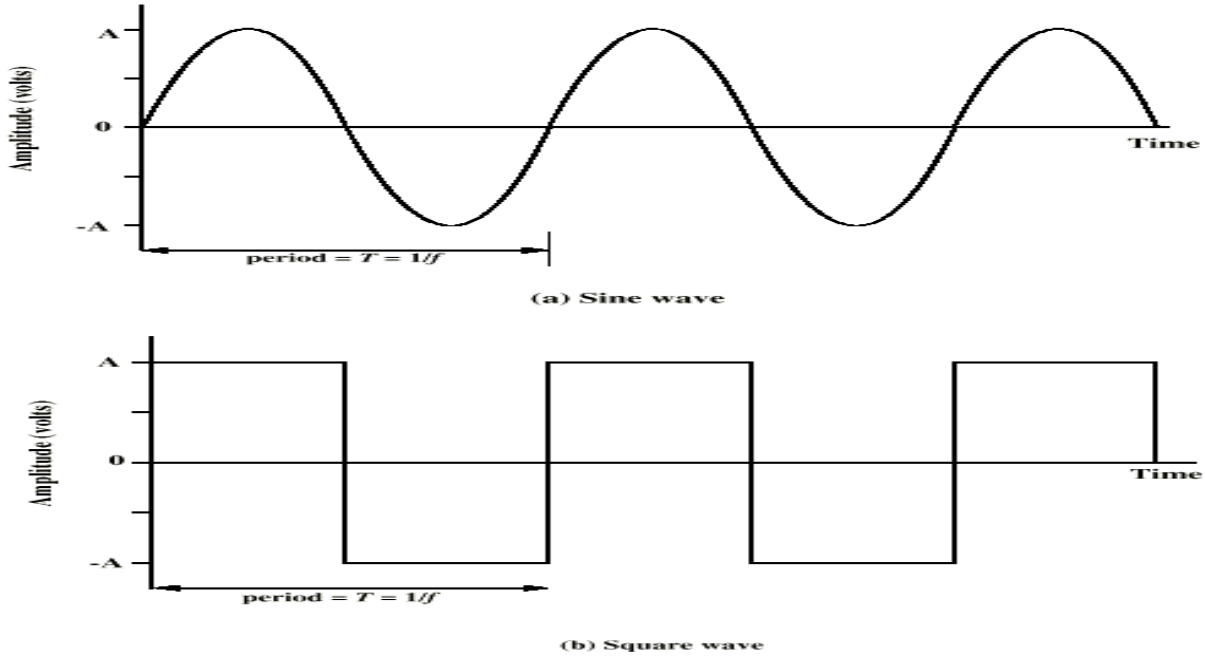


(a) Analog



(b) Digital

3.2.2 Periodic Signals



2.3.3 Signal Main Components

Peak Amplitude (A): Maximum strength of signal, measured in volts.

Frequency (f): Rate at which the signal repeats

Hertz (Hz) or cycles per second

Period = time for one repetition (T)

T = 1/f

Phase (ϕ): Relative position in time within a single

3.3 Wavelength, Frequency Domain and Bandwidth

Wavelength is defined as distance occupied by one cycle or distance between two points of corresponding phase in two consecutive cycles (λ).

Assuming signal velocity *v*

$\lambda = vT$

$\lambda f = v$

$c = 3*10^8\ ms^{-1}$ (speed of light in free space)

For an electromagnetic wave that travels in free space**:**

$\lambda f = c$

Frequency Domain Concepts

An electromagnetic signal is usually made up of many frequencies

signal is made up of components at various frequencies, in which each component is a sinusoid

By adding together enough sinusoidal signals, each with the appropriate amplitude, frequency, and phase, any electromagnetic signal can be constructed.

Spectrum & Bandwidth

Spectrum range of frequencies contained in signal

Bandwidth: The frequency range of a channel, measured as the difference between the highest and lowest frequencies that the channel supports. The maximum transmission speed dependent upon the available bandwidth. The larger the bandwidth, the higher the transmission speed.

Absolute bandwidth: Width of spectrum

Effective bandwidth: Often just *bandwidth*

Narrow band of frequencies containing most of the energy in the signal.

Data Rate and Bandwidth: Any transmission system has a limited band of frequencies. This limits the data rate that can be carried.

3.4 Analog and Digital Data Transmission

Data: Entities that convey meaning, or information.

Signals: Electric or electromagnetic representations of data.

Transmission: Communication of data by propagation and processing of signals

Analog data: Continuous values within some interval (e.g. sound, video)

Digital data: Discrete values (e.g. text, integers**)**

Analog Transmission:

Analog signal transmitted without regard to content.The signals may represent analog data (e.g. voice) or digital data (e.g. binary data pass through modem).The analog signal will become weaker (attenuate) over distance. To

achieve longer distances, analog transmission use amplifiers to boost the energy in the signal. Also amplifies noise. With cascaded amplifiers, the signal becomes more and more distorted

Digital Transmission

Concerned with content. The integrity of the data is not endangered by noise, attenuation and other impairments. Repeaters used

- Repeater receives signal
- Extracts bit pattern
- Retransmits (a new signal is regenerated)
- Attenuation is overcome
- Noise is not amplified

Advantages of Digital Transmission over Analog

i) Digital technology
   - Drop in cost and size of digital circuitry because of the advent of LSI/VLSI technology.

ii) Data integrity
   - With the use of repeaters rather than amplifiers, it is possible to transmit data longer distances over lower quality (less cost) lines.

iii) Capacity utilization
   - High bandwidth links economical. Easier and more efficient multiplexing with digital techniques (time division)

iv) Security & Privacy
   - Encryption techniques can be easily applied to digital data.

v) Integration
   - Can treat analog and digital data similarly, integration of voice, video, and digital data on the same transmission system is possible.

3.4.1 Transmission Impairments

Signal received may differ from signal transmitted. For analog signal these impairments can degrade the signal quality. For digital signals bit errors may be introduced, a binary 1 can be transformed into a binary 0 and vice versa. The most significant impairments are:

i) Attenuation and attenuation distortion
ii) Delay distortion
iii) Noise

Attenuation

Signal strength falls off with distance. Attenuation depends on medium. For guided media: it is exponential and expressed as a constant number of decibels per unit distance. For unguided media: it is a complex function of distance and makeup of the atmosphere. The received signal strength must be: Enough to be detected by the electronic circuitry in the receiver. Sufficiently higher than noise to be received without error. It is important to know that attenuation is an increasing function of frequency.

Delay Distortion

Occurs because the velocity of propagation of a signal through a *guided* medium varies with frequency. The velocity tends to be highest near the center frequency and fall off toward the two edges of the band. Critical for digital data, consider that a sequence of bits is being transmitted. Some of the signal components of one bit position will spill over into other bit positions, causing intersymbol interference. This is a major limitation to maximum bit rate over a transmission channel**.**

Noise

Additional unwanted signals inserted somewhere between transmitter and receiver. It is the major limiting factor in communication system performance. Noise may be divided into four categories:

i) Thermal noise:

- Is due to thermal agitation of electrons.
- Uniformly distributed across the bandwidth and called white noise.
- Cannot be eliminated and therefore places an upper bound on communications system performance

ii) Intermodulation noise

- Signals that are the sum and difference of original frequencies sharing a medium

iii) Crosstalk

- A signal from one line is picked up by another
- e.g. while using telephone, hear another conversation.

iv) Impulse noise

- Irregular pulses or spikes
- e.g. External electromagnetic interference (lightning)
- Short duration and relatively high amplitude

3.5 Channel capacity

Define the channel capacity is the data rate which can be transmitted over a given channel reliably.

Shannon Equation:

Use $R = H \log_2(1+S/N)$

$(S/N)dB = 10\log$ Power-in/Power-out

Example

Given that a copper twisted pair cable link is able to attain a maximum data rate of 56kbps at a bandwidth of 3000Hz estimate the S/N ratio for the cable in dB,

$R = H \log_2(1+S/N)$

Where R =Maximum data rate, S = signal power, N= noise power, H= bandwidth

$R/H = \text{Log}_2 (1+S/N)$

$1+ S/N = 2^{R/H}$

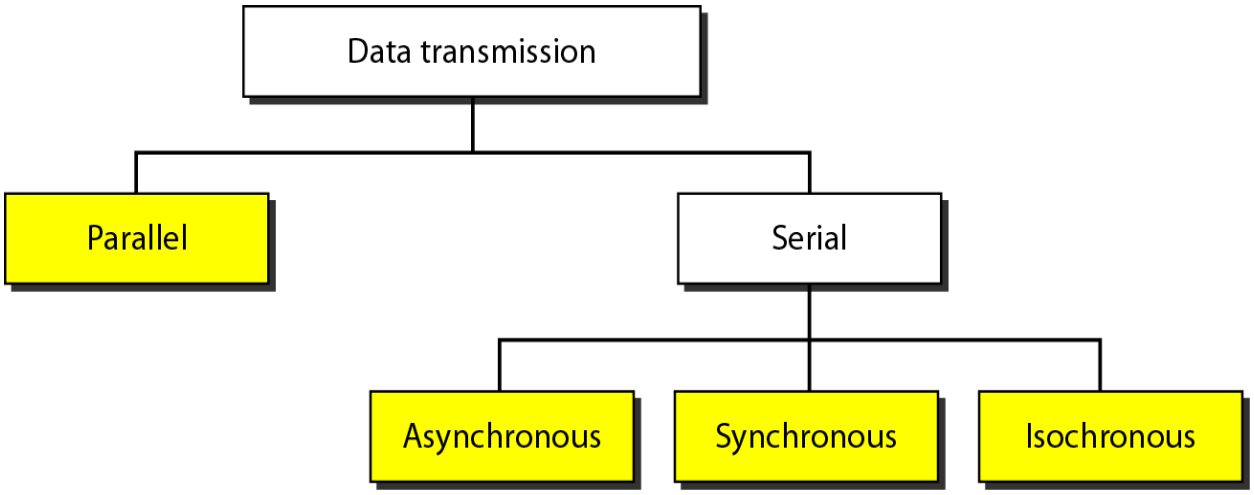
$S/N = 2^{R/H} -1$

$(S/N)_{dB} = 10\log_{10}(2^{R/H} - 1)$ multiply the result by 2 since it is two way communication

$(S/N)_{dB} = 112.4dB$

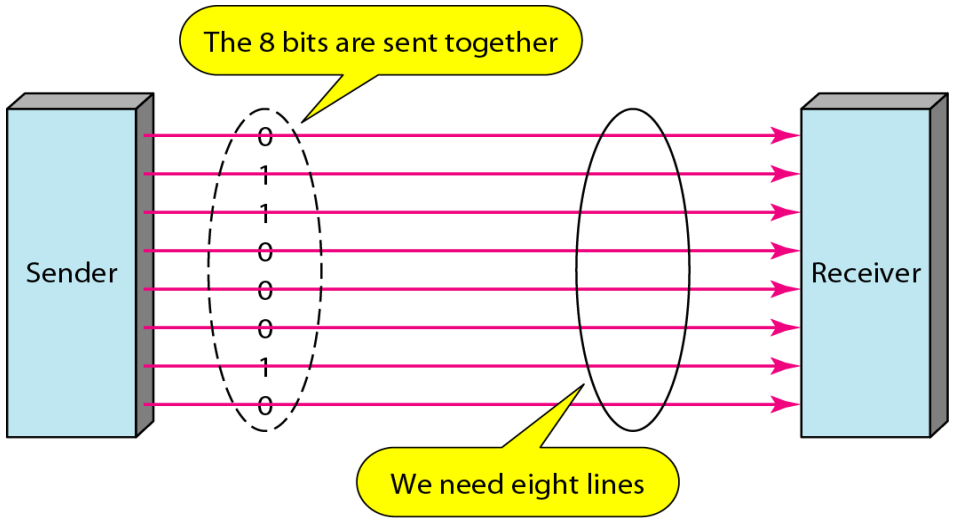
3.6 Data Transmission Modes

The primary concern in the transmission of data from one device to another is the wiring and how to send the data stream. Do we send 1 bit at a time or group bits into larger groups. 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. The different transmission modes are as shown in the following figure.



Parallel Transmission

In Parallel Transmission, data consisting of 1s and 0s, may 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 1bit. This is called parallel transmission. In parallel transmission we use *n* wires to send *n* bits at one time. That way each bit has its own wire, and all *n* bits of one group can be transmitted with each clock tick from one device to another. The following figure shows how parallel transmission works for *n* =8. Typically, the eight wires are bundled in a cable with a connector at each end.

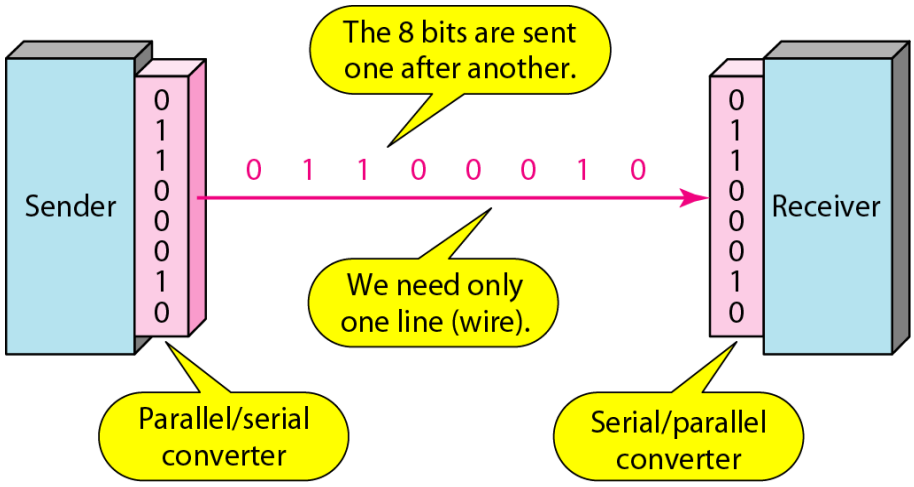


The advantage of parallel transmission is speed. All else being equal, parallel transmission can increase the transfer speed by a factor of n over serial transmission.

But the disadvantage is cost. Parallel transmission requires n communication lines just to transmit the data stream. Because this is expensive, parallel transmission is usually limited to short distances.

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 following figure shows serial transmission.



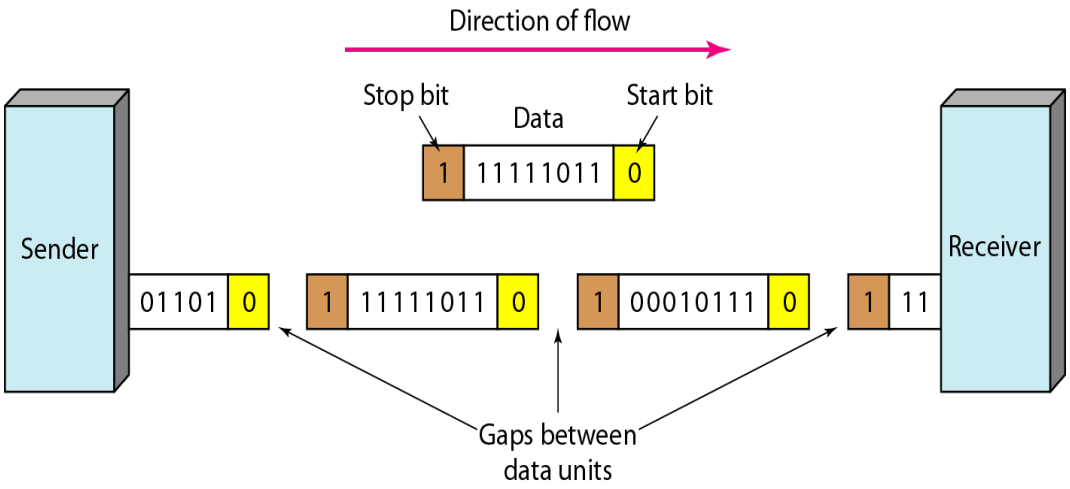
Serial transmission reduces the cost of transmission over parallel by roughly a factor of *n.* Serial transmission occurs in one of three ways: asynchronous, synchronous, and isochronous.

a) **Asynchronous Transmission:**

In Asynchronous transmission, the timing of a signal is unimportant. Instead, information is received and translated by agreed upon patterns. As long as those patterns are followed, the receiving device can retrieve the information without regard to the rhythm in which it is sent. Patterns are based on grouping the bit stream into bytes. Each group, usually 8 bits, is sent along the link as a unit. The sending system handles each group independently, relaying it to the link whenever ready, without regard to a timer.

Without synchronization, the receiver cannot use timing to predict when the next group will arrive. To alert the receiver to the arrival of a new group, therefore, an extra bit is added to the beginning of each byte. This bit, usually a 0, is called the start bit. To let the receiver know that the byte is finished, 1 or more additional bits are appended to the end of the byte. These bits, usually 1 s, are called stop bits.

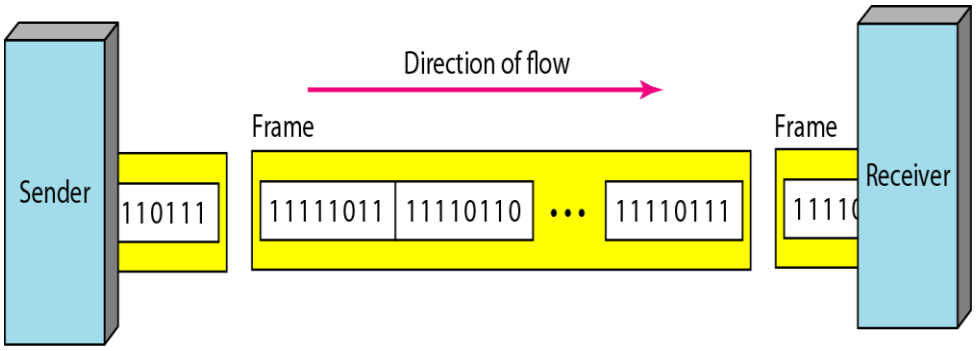
By this method, each byte is increased in size to at least 10 bits, of which 8 bits is information and 2 bits or more are signals to the receiver. In addition, the transmission of each byte may then be followed by a gap of varying duration. This gap can be represented either by an idle channel or by a stream of additional stop bits. The start and stop bits and the gap alert the receiver to the beginning and end of each byte and allow it to synchronize with the data stream. This mechanism is called *asynchronous* because, at the byte level, the sender and receiver do not have to be synchronized. But within each byte, the receiver must still be synchronized with the incoming bit stream. That is, some synchronization is required, but only for the duration of a single byte. The receiving device resynchronizes at the onset of each new byte.



The addition of stop and start bits and the insertion of gaps into the bit stream make asynchronous transmission slower than forms of transmission that can operate without the addition of control information.

b) **Synchronous Transmission*:***

In synchronous transmission, the bit stream is combined into longer "frames," which may contain multiple bytes. Each byte, however, is introduced onto the transmission link without a gap between it and the next one. It is left to the receiver to separate the bit stream into bytes for decoding purposes. The following figure show illustration of synchronous transmission.



The sender puts its data onto the line as one long string. If the sender wishes to send data in separate bursts, the gaps between bursts must be filled with a

special sequence of 0s and 1s that means *idle.* The receiver counts the bits as they arrive and groups them in 8-bit units.

Without gaps and start and stop bits, there is no built-in mechanism to help the receiving device adjust its bit synchronization midstream. Timing becomes very important, therefore, because the accuracy of the received information is completely dependent on the ability of the receiving device to keep an accurate count of the bits as they come in.

The advantage of synchronous transmission is speed. With no extra bits or gaps to introduce at the sending end and remove at the receiving end, and, by extension, with

fewer bits to move across the link, synchronous transmission is faster than asynchronous transmission. For this reason, it is more useful for high-speed applications such as the transmission of data from one computer to another.

c) Isochronous Transmission

In real-time audio and video, in which uneven delays between frames are not acceptable, synchronous transmission fails. For example, TV images are broadcast at the rate of 30 images per second; they must be viewed at the same rate. If each image is sent by using one or more frames, there should be no delays between frames. For this type of application, synchronization between characters is not enough; the entire stream of bits must be synchronized. The isochronous transmission guarantees that the data arrive at a fixed rate.

3.6.1 Channel concepts

i) Channel

- A channel is a portion of the communications medium allocated to the sender and receiver for conveying information between them. The communications medium is often subdivided into a number of separate paths, each of which is used by a sender and receiver for communication purposes.

ii) Baud Rate

- Baud rate is the same as symbol rate and is a measure of the number of line changes which occur every second. Each symbol can represent or convey one (binary encoded signal) or several bits of data. For a binary signal of 20Hz, this is equivalent to 20 baud (there are 20 changes per second).

iii) Bits Per Second

- This is an expression of the number of data bits per second. Where a binary signal is being used, this is the same as the baud rate. When the signal is changed to another form, it will not be equal to the baud rate, as each line change can represent more than one bit (either two or four bits).

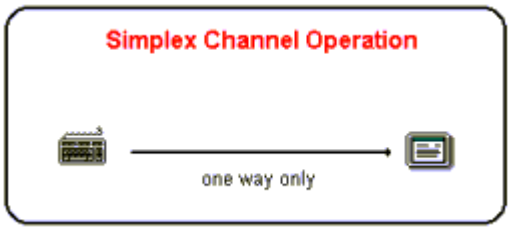
iv) Bandwidth

- Bandwidth is the frequency range of a channel, measured as the difference between the highest and lowest frequencies that the channel supports. The maximum transmission speed is dependant upon the available bandwidth. The larger the bandwidth, the higher the transmission speed.

3.6.2 Data Communication Channels

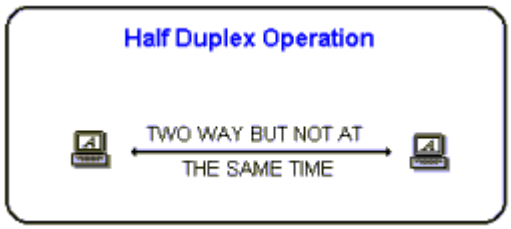
i) Simplex

- Data in a simplex channel is always one way. Simplex channels are not often used because it is not possible to send back error or control signals to the transmit end. An example of a simplex channel in a computer system is the interface between the keyboard and the computer, in that key codes need only be sent one way from the keyboard to the computer system.
- signals are transmitted in only one direction
- Example e.g. Television



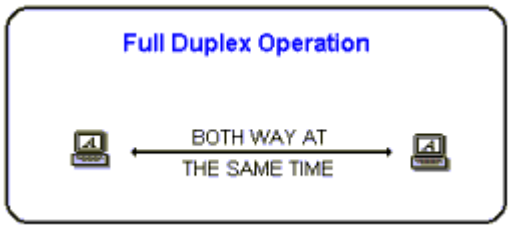
ii) Half Duplex

- A half duplex channel can send and receive, but not at the same time. Its like a one-lane bridge where two way traffic must give way in order to cross. Only one end transmits at a time, the other end receives.
- both stations may transmit but only one way at a time
- Example e.g. police radio



iii) Full Duplex

- Data can travel in both directions simultaneously. There is no need to switch from transmit to receive mode like in half duplex. Its like a two lane bridge on a two-lane highway
- both station may transmit simultaneously
- Example e.g. telephone
-



3.7 Modulation and demodulation

Modulation has been defined as the process of combining an input signal $m(t)$ and a carrier at frequency fc to produce a signal $s(t)$ whose bandwidth is (usually) centered on fc. Reversing the process back to original form signal is demodulation as shown below

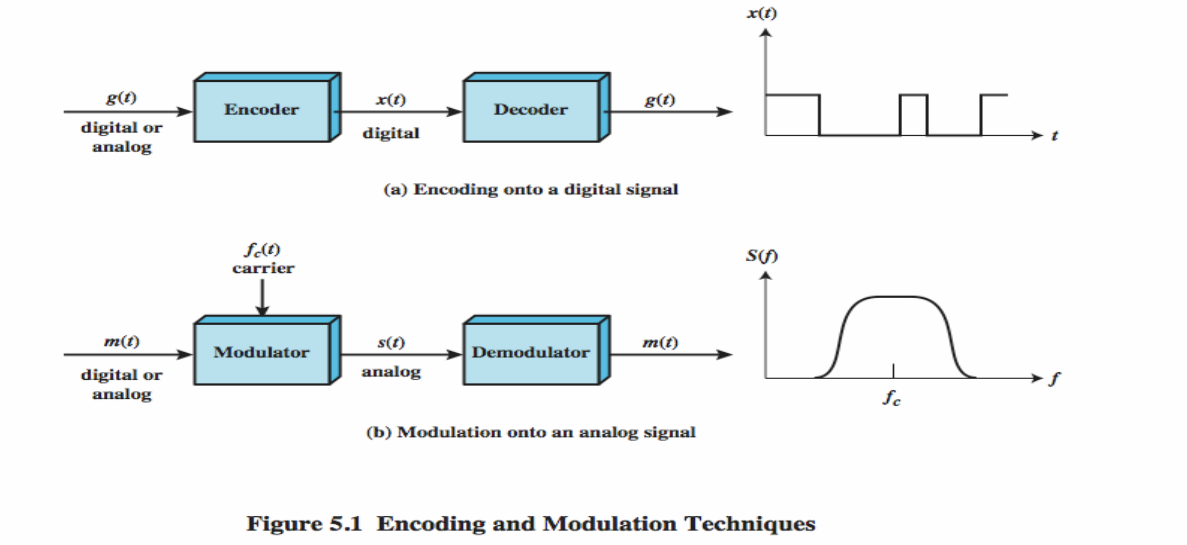


Figure 5.1 Encoding and Modulation Techniques

When only analog transmission facilities are available, modulation is required to convert the digital data to analog form

There are two principal reasons for analog modulation of analog signals:

i) A higher frequency may be needed for effective transmission, since for unguided transmission, it is virtually impossible to transmit baseband signals;
ii) Modulation permits frequency division multiplexing.

As with AM, both FM and PM result in a signal whose bandwidth is centered at fc, but can show that the magnitude of that bandwidth is very different, hence both FM and PM require greater bandwidth than AM. The shapes of the FM and PM signals are very similar.

Modulation techniques are methods used to encode digital information in an analogue world.

Transmission of Digital Signals: A digital signal, periodic or non-periodic, is a composite analog signal with frequencies between zero and infinity. We can

transmit a digital signal by using one of two different approaches: baseband transmission or broadband transmission (using
modulation).

3.7.1 Baseband Transmission

Baseband transmission means sending a digital signal over a channel without changing the digital signal to an analog signal. The following figure shows baseband transmission. Baseband transmission requires a low-pass channel, a channel with a bandwidth that starts from zero. This is the case if we have a dedicated medium with a bandwidth constituting only one channel. For example, the entire bandwidth of a cable connecting two computers is one single channel. As another example, we may connect several computers to a bus, but not allow more than two stations to communicate at a time.

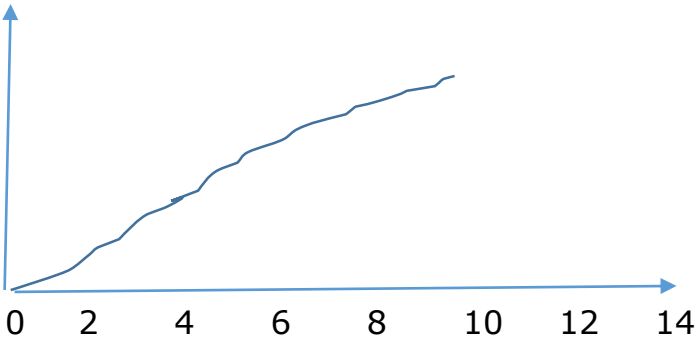


Fig: baseband signal starting from 0Hz

3.7.2 Broadband Transmission (Using Modulation)

Broadband transmission or modulation means changing the digital signal to an analog signal for transmission. Modulation allows us to use a band pass channel- a channel with a bandwidth that does not start from zero. This type of channel is more available than a low-pass channel. The following figure shows a band pass channel.

Fig:

There are three basic modulation techniques

- AM (amplitude modulation)
- FM (frequency modulation)
- PM (phase modulation)

All 3 modulation techniques employ a carrier signal. A carrier signal is a single frequency that is used to carry the intelligence (data).

- For digital, the intelligence is either a 1 or 0.

When we modulate the carrier, we are changing its characteristics to correspond to either a 1 or 0.

Analog and Digital information can be encoded as either analog or digital signals:

1. **Digital data to digital signals:** simplest form of digital encoding of digital data
2. **Digital data to analog signal:** A modem converts digital data to an analog signal so that it can be transmitted over an analog
3. **Analog data to digital signals:** Analog data, such as voice and video, are often digitized to be able to use digital transmission facilities

Analog data to analog signals: Analog data are modulated by a carrier frequency to produce an analog signal in a different frequency band, which can be utilized on an analog transmission system.

For **digital signaling**, a data source $g(t)$, which may be either digital or analog, is encoded into a digital signal $x(t)$. The basis for **analog signaling** is a continuous constant-frequency *fc* signal known as the **carrier** signal or carrier

wave.. Data may be transmitted using a carrier signal or carrier wave by modulation, which is the process of encoding source data onto the carrier signal. All modulation techniques involve operation on one or more of the three fundamental frequency domain parameters: amplitude, frequency, and phase. The input signal $m(t)$ may be analog or digital and is called the modulating signal, and the result of modulating the carrier signal is called the modulated signal $s(t)$.

3.7.3 Character Encoding techniques

1. **Digital data to digital signals**

   A digital signal is a sequence of discrete, discontinuous voltage pulses. Each pulse is a signal element. Binary data are transmitted by encoding each data bit into signal elements. In the simplest case, there is a one-to-one correspondence between bits and signal elements. More complex encoding schemes are used to improve performance, by altering the spectrum of the signal and providing synchronization capability.

   Encoding techniques

   1) Non-return to Zero-Level (NRZ-L)
   2) Nonreturn to Zero Inverted (NRZI)
   3) Bipolar -AMI
   4) Pseudoternary
   5) Manchester
   6) Differential Manchester

Definition of Digital Signal Encoding Format

1. **Non-return to Zero-Level (NRZ-L)**

   0 = high level

   1 = low level

2. **Non-return to Zero Inverted (NRZI)**

   0 = no transition at beginning of interval 1one bit time 2

   1 = transition at beginning of interval

3. **Bipolar-AMI**

0 = no line signal

1 = positive or negative level, alternating for successive ones

4. **Pseudoternary**

   0 = positive or negative level, alternating for successive zeros

   1 = no line signal

5. **Manchester**

   0 = transition from high to low in middle of interval

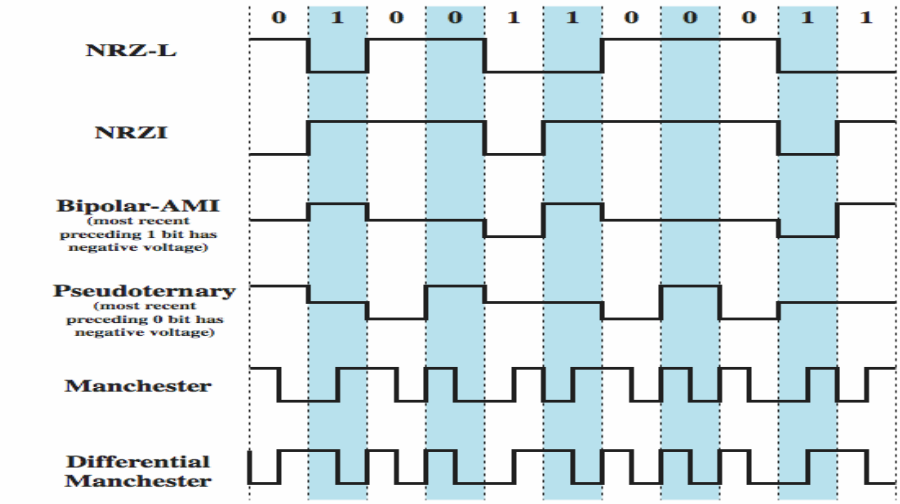
   1 = transition from low to high in middle of interval

6. **Differential Manchester**

   Always a transition in middle of interval

   0 = transition at beginning of interval

   1 = no transition at beginning of interval



2. **Digital Data to Analog Signal modulation**

   Digital devices are attached to the network via a modem (modulator-demodulator), which converts digital data to analog signals, and vice versa.

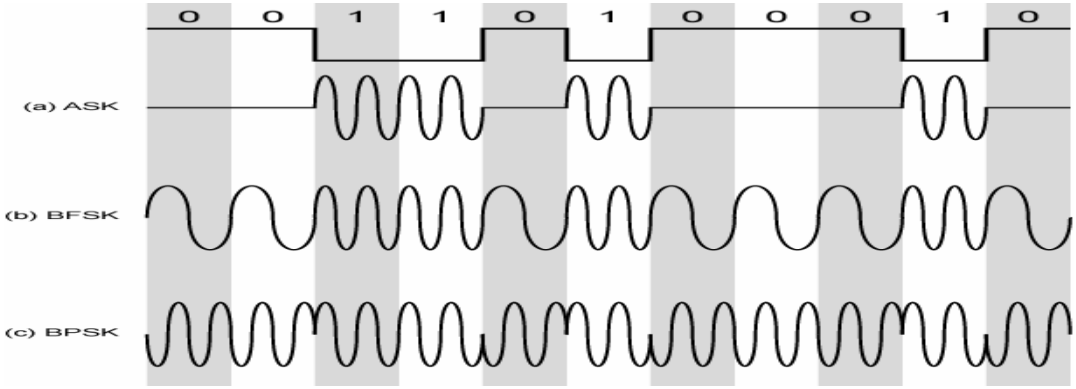
   There are three basic encoding or modulation techniques for transforming digital data into analog signals, as illustrated Figure below:

   1) Amplitude Shift Keying (ASK),

   2) Frequency Shift Keying (FSK), And

3) Phase Shift Keying (PSK).

In all these cases, the resulting signal occupies a bandwidth centered on the carrier frequency.



3. **Analog data to digital signals**

To change an analog signal to digital data we use two techniques,

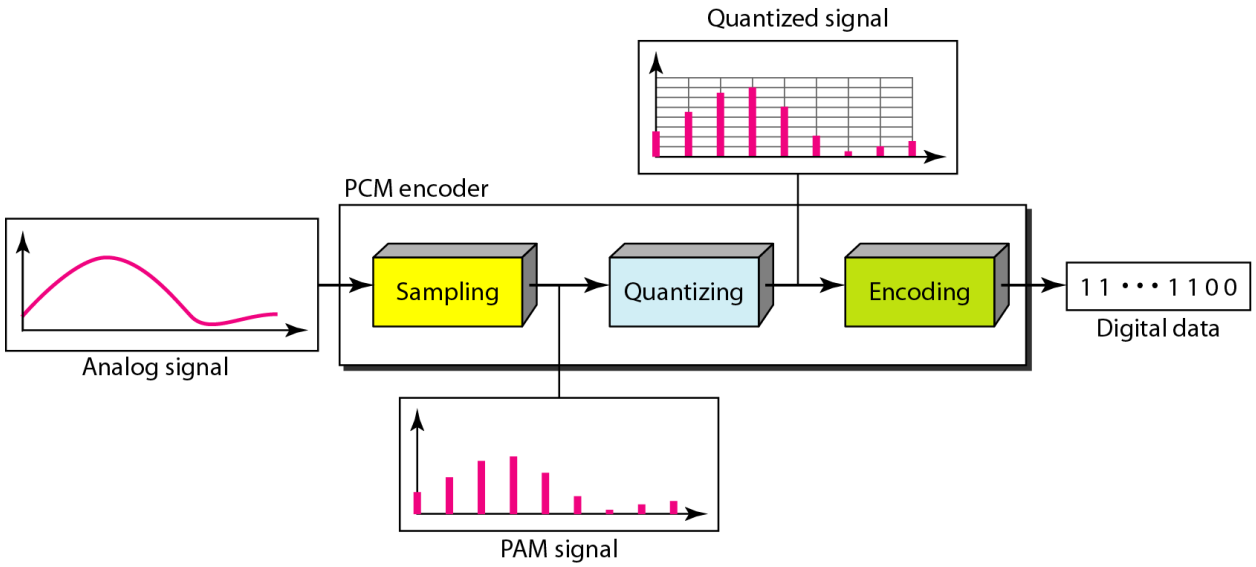
i) pulse code modulation and

ii) Delta modulation.

After the digital data are created (digitization) then we convert the digital data to a digital signal.

Pulse Code Modulation (PCM)

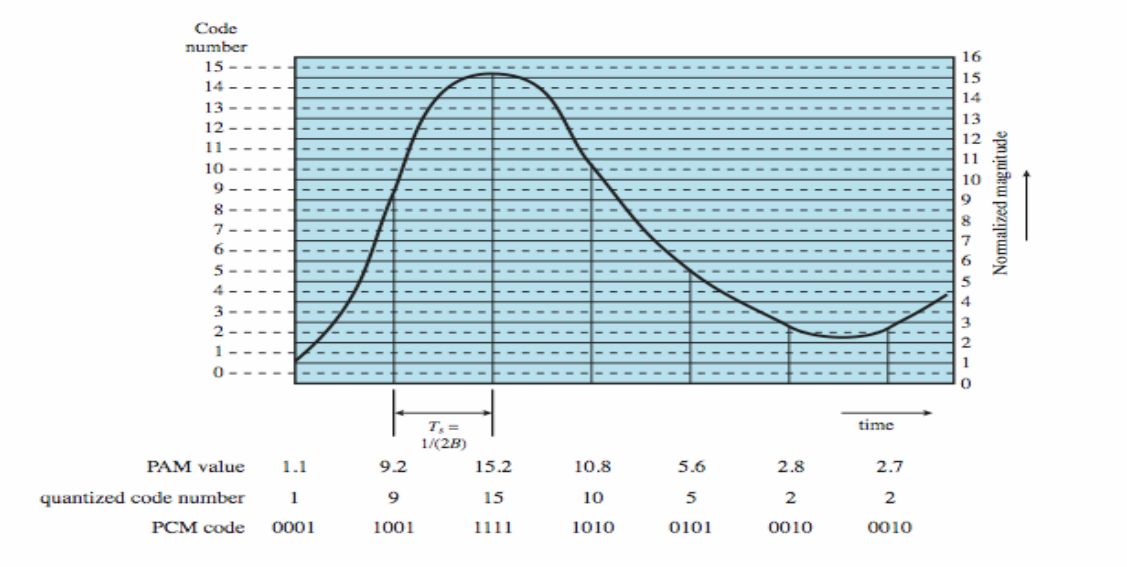
Pulse Code Modulation (PCM) is the most common technique used to change an analog signal to digital data (digitization). A PCM encoder has three processes as shown in the following Figure.



1. The analog signal is sampled
2. The sampled signal is quantized.
3. The quantized values are encoded as streams of bits.

Sampling

The first step in PCM is sampling. The analog signal is sampled every *Ts* s, where *Ts* is the sample interval or period. The inverse of the sampling interval is called the sampling rate or sampling frequency and denoted by *ƒ*s, Where *ƒ*s = 1/ *Ts. As shown below*



Quantization

The result of sampling is a series of pulses with amplitude values between the maximum and minimum amplitudes of the signal. The set of amplitudes can be infinite with non-integral values between the two limits. These values cannot be used in the encoding process. The following are the steps in quantization:

a) We assume that the original analog signal has instantaneous amplitudes between *V*min and *V*max

b) We divide the range into *L* zones, each of height Δ (delta).

Δ (delta) = V max- Vmin/L

c) We assign quantized values of 0 to *L* - I to the midpoint of each zone.

d) We approximate the value of the sample amplitude to the quantized values.

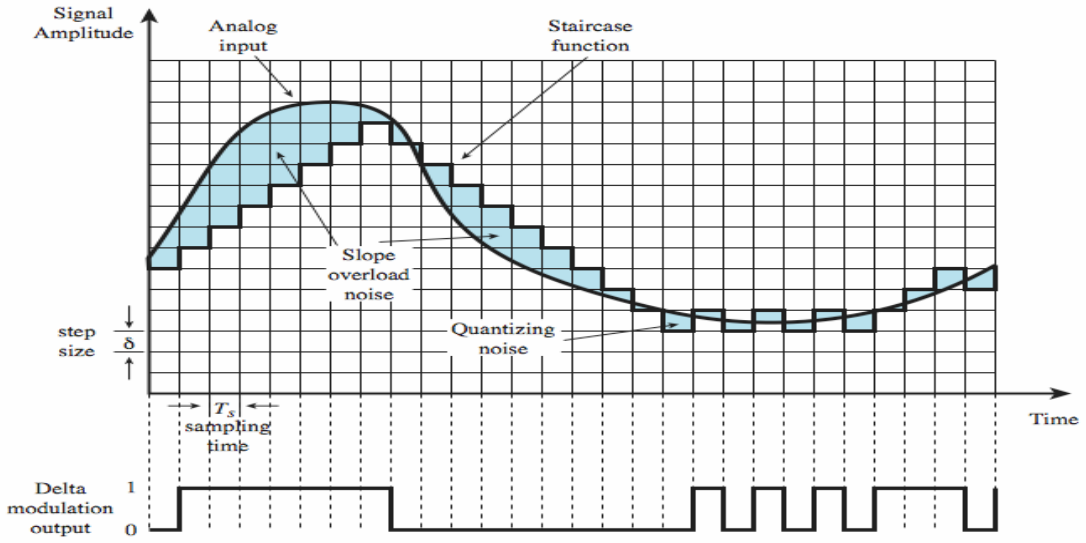


Figure show Delta Modulation where the staircase function is overlaid on the original analog waveform. A 1 is generated if the staircase function is to go up during the next interval; a 0 is generated otherwise. The transition (up or down) that occurs at each sampling interval is chosen so that the staircase function tracks the original analog waveform as closely as possible. There are two

important parameters in a DM scheme: the size of the step assigned to each binary digit, δ, and the sampling rate.

4. **Analog data to analog signals**

Analog data can be modulated by a carrier frequency to produce an analog signal in a different frequency band, which can be utilized on an analog transmission system. The basic techniques are

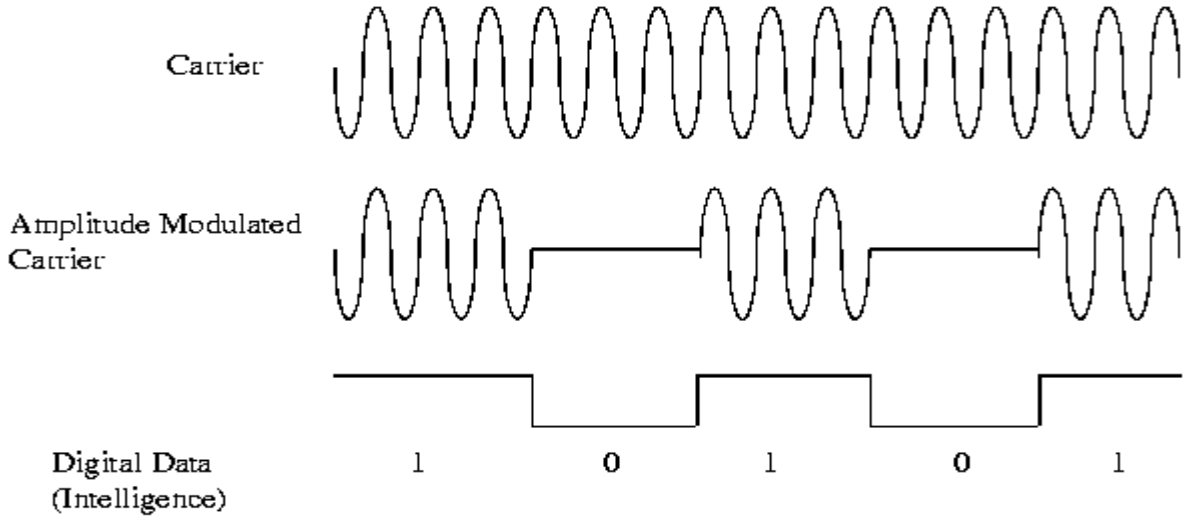
1) **Amplitude modulation (AM):** Amplitude modulation (AM) is the simplest form of modulation, and involves the multiplication of the input signal by the carrier *fc*.

   Modifies the amplitude of the carrier to represent 1s or 0s

   i) A 1 is represented by the presence of the carrier for a predefined period of 3 cycles of carrier.

   ii) Absence or no carrier indicates a 0

- Pros
  - Simple to design and implement
- Cons
  - Noise spikes on transmission medium interfere with the carrier signal.
  - Loss of connection is read as 0s.



2) **Frequency modulation (FM),** for frequency modulation, the derivative of the phase is proportional to the modulating signal.

   Modifies the frequency of the carrier to represent the 1s or 0s.

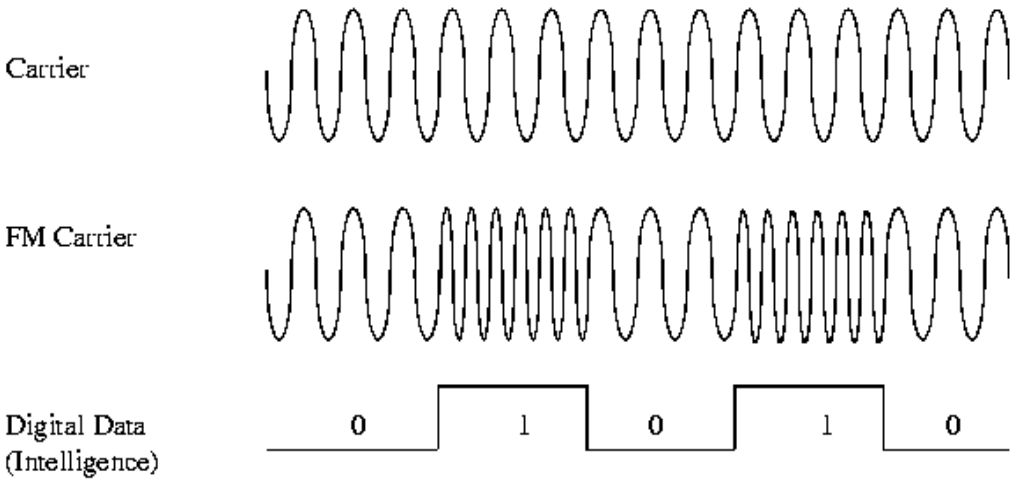
   a. a 0 is represented by the original carrier frequency
   b. a 1 by a much higher frequency (the cycles are spaced closer together)

   Pros

   c. Immunity to noise on transmission medium.
   d. Always a signal present. Loss of signal easily detected

   Cons

   i) Requires 2 frequencies
   ii) Detection circuit needs to recognize both frequencies when signal is lost.



3) **Phase modulation (PM).** Phase modulation, the phase is proportional to the modulating signal

   Phase Modulation modifies the phase of the carrier to represent a 1 or 0.

   i) The carrier phase is switched at every occurrence of a 1 bit but remains unaffected for a 0 bit.

ii) The phase of the signal is measured relative to the phase of the preceding bit. The bits are timed to coincide with a specific number of carrier cycles (3 in this example = 1 bit)

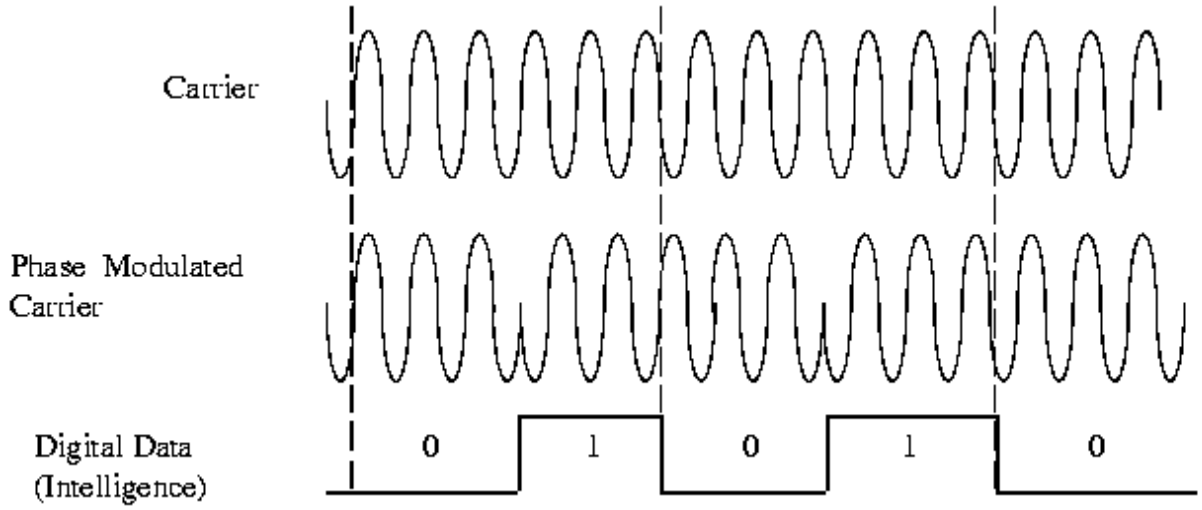
Pros

iii) Only 1 frequency used

iv) Easy to detect loss of carrier

Cons

v) Complex circuitry required to generate and detect phase changes



3.8 Performance of the Network:

One important issue in networking is the performance of the network. The different factors which effects performance of the Network are as follows:

i) **Bandwidth**

One characteristic that measures network performance is bandwidth. However, the term can be used in two different contexts with two different measuring values: bandwidth in hertz and bandwidth in bits per second.

a. Bandwidth in Hertz

Bandwidth in hertz is the range of frequencies contained in a composite signal or the range of frequencies a channel can pass. For example, we can say the bandwidth of a subscriber telephone line is 4 kHz.

b. Bandwidth in Bits per Seconds:

The term *bandwidth* can also refer to the number of bits per second that a channel, a link, or even a network can transmit. For example, one can say the bandwidth of a Fast Ethernet network (or the links in this network) is a maximum of 100 Mbps. This means that this network can send 100 Mbps.

c. Relationship:

There is an explicit relationship between the bandwidth in hertz and bandwidth in bits per seconds. Basically, an increase in bandwidth in hertz means an increase in bandwidth in bits per second. The relationship depends on whether we have baseband transmission or transmission with modulation.

ii) **Throughput :**

The throughput is a measure of how fast we can actually send data through a network. Although, at first glance, bandwidth in bits per second and throughput seem the same, they are different. A link may have a bandwidth of *B* bps, but we can only send *T* bps through this link with *T* always less than *B.* In other words, the bandwidth is a potential measurement of a link; the throughput is an actual measurement of how fast we can send data. For example, we may have a link with a bandwidth of 1 Mbps, but the devices connected to the end of the link may handle only 200 kbps. This means that we cannot send more than 200 kbps through this link.

iii) **Latency (Delay)**

The latency or delay defines how long it takes for an entire message to completely arrive at the destination from the time the first bit is sent out from the source. We can say that latency is made of four components: propagation time, transmission time, queuing time and processing delay.

Latency =propagation time +transmission time +queuing time + processing delay

iv) Propagation Time

Propagation time measures the time required for a bit to travel from the source to the destination. The propagation time is calculated by dividing the distance by the propagation speed.

Propagation time = Distance /Propagation speed

The propagation speed of electromagnetic signals depends on the medium and on the frequency of the signal. For example, in a vacuum, light is propagated with a speed of 3x108mfs. It is lower in air; it is much lower in cable.

v) Transmission time

In data communications we don't send just 1 bit, we send a message. The first bit may take a time equal to the propagation time to reach its destination; the last bit also may take the same amount of time. However, there is a time between the first bit leaving the sender and the last bit arriving at the receiver. The first bit leaves earlier and arrives earlier; the last bit leaves later and arrives later. The time required for transmission of a message depends on the size of the message and the bandwidth of the channel. Transmission time =Message size / Bandwidth

vi) Queuing Time

The third component in latency is the queuing time, the time needed for each intermediate or end device to hold the message before it can be processed. The queuing time is not a fixed factor; it changes with the load imposed on the network. When there is heavy traffic on the network, the queuing time increases. An intermediate device, such as a router, queues the arrived messages and processes them one by one. If there are many messages, each message will have to wait.

vii) **Jitter :**

Another performance issue that is related to delay is **jitter. J**itter is a problem if different packets of data encounter different delays and the application using the data at the receiver site is time- sensitive (audio and video data, for example). **If** the delay for the first packet is 20 ms, for the second is 45 ms, and for the third is 40 ms, then the real-time application that uses the packets endures jitter.

In summary, you learned that;

i) Main concepts of analog & digital signals components,
ii) Types of communication links,
iii) Analog signal, digital signal and signal main components
iv) Analog and digital data transmission,
v) Transmission impairments,
vi) Channel capacity
vii) Data transmission modes, and channel concepts,
viii) Modulation and demodulation concepts
ix) Character encoding techniques
x) Factors that determine performance of the network.

Glossary

An analog signal is a continuously varying electromagnetic wave that may be propagated over a variety of media:

A digital signal is a sequence of voltage pulses that can be transmitted over a wire medium:

Modulation is defined as the process of combining an input signal $m(t)$ and a carrier at frequency fc to produce a signal $s(t)$ whose bandwidth is (usually) centered on fc. Reversing the process is **demodulation.**

Further Reading

Data & Computer networks, Prakash Gupta

William Stallings, Data & Computer networks 10th edition

Any other data communication and networking relevant books, journals, articles e.t.c

TOPIC ACTIVITIES

Activity

In your own place of residence identify communication systems which used full duplex communication modes. At the same time which should communication systems like early TV set were connected through a decoder.

Tips

Use internet search to review the roles of encoder as well as decoder.

Review

i) Given a channel with an intended capacity of 20 Mbps, the bandwidth of the channel is 3 MHz. Assuming white thermal noise, what signal-to-noise ratio is required to achieve this capacity?

ii) Consider a stream of data consisting of a long sequence digital data equivalent to fifty six decimal value encoded to digital signal. Draw the waveform using the following techniques:-
    a. Manchester
    b. Differential Manchester

iii) In synchronous time division multiplexing, it is possible to interleave bits, one bit from each channel participating in a cycle. If the channel is using a self-clocking code to assist synchronization, might this bit interleaving introduce problems because there is no continuous stream of bits from one source?

iv) Latency or delay defines how long it takes for an entire message to completely arrive at the destination from the time the first bit is sent out from the source. Explain the four main components of latency.

v) What does the sampling theorem states concerning the rate of sampling required for an analog signal? Discuss two techniques used to encode analog data to digital signal briefly.

TOPIC FOUR: TERMINAL DEVICES

Introduction

Welcome to topic one. This topic is aimed at introducing main concepts of Digital Service Unit(DSU), Channel Service Unit (CSU),Ethernet Wiring,Patch Panels,Network interfaces Cards(NIC),Hubs/ concentrators or Repeaters, Switches, Routers, Servers, Gateways, Modem and Firewall

The topic is, therefore designed to prepare you to have a clear understanding of types of transmission media, Network Address Translation (NAT) as well.

Topic Time

- Compulsory online reading, activities, self-assessments and practice exercises **[3 hours]**
- Optional further reading **[1.5 hours]**
- Total student input **[4.5 hours]**

Topic Learning Requirements

- Participation in one *chat* (at least 5 entries)
- At least two elaborate contributions to the *discussion* topic. You may also start your own discussion thread.
- Timely submission of the assignments

Learning Outcomes

By the end of this topic you should be able to:

i) Explain Digital Service Unit (DSU)
ii) Explain Channel Service Unit (CSU)
iii) Explain Data Terminal Equipment (DTE)
iv) Discuss Ethernet Wiring
v) Discuss the roles of Patch Panels and Network interfaces Cards(NIC)
vi) Discuss function Hubs/ concentrators or Repeaters
vii) Explain importance of Switches, Routers and Servers in networks
viii) Describe the functions of Gateways, Modem and Firewall in networks

ix) Explain types of transmission media

x) Roles of Network Address Translation (NAT).

Topic Contents

4.1. Introduction

Network terminal (NT) is device which ends a telecommunications link and is the point at which a signal enters or leaves a network. NT is a device that connects the customer's data or telephone equipment to carrier's line that comes in a building or office. It provide connection for terminal equipment (TE) and terminal adapter (TA) equipment to local loop. Examples of equipment containing network terminations are telephones, fax machines computer terminal and network devices, printers and workstations.

4.2 Data digital services units or digital services units

A data service unit, sometimes called a digital service unit, is a piece of telecommunications circuit terminating equipment that transforms digital data between telephone company lines and local equipment. The device converts bipolar digital signals coming ultimately from a digital circuit and directly from a Channel service unit (CSU), into a format compatible with the piece of data terminal equipment (DTE) (e.g. a router) to which the data is sent.

4.3 Channel Service Unit (CSU)

A channel service unit (CSU) is a line Bridging device for use with T-carrier that:

- Used to perform loopback testing,
- Perform bit stuffing
- Provide a framing and formatting pattern compatible with the network
- Provides a barrier for electrical interference from either side of the unit,
- The last signal regeneration point, on the loop side, coming from the central office before the regenerated signal reaches a multiplexer or data terminal equipment (DTE)

4.4 Data Terminal Equipment (DTE)

(DTE) is an end instrument that converts user information into signals or reconverts received signals. Devices which acts as source or destinations in digital communication and which is capable of converting information to signals and also reconverting received signals.

Features of Data Terminal Equipment

- Provides the data communication control function to the digital data communication.
- It can be single piece equipment or multiple pieces interconnected to perform the required functions.
- In data communication data terminal equipment is the terminal.
- performs error detection and clocking
- Device which uses serial transmission to transmit data, which is done with help of the serial port in the device.
- To connect a data terminal equipment to a communication link, data communication equipment needs to be used.

4.5 Ethernet Wiring

Structured Cabling. A structured cabling system is a complete system of cabling and associated hardware, which provides a comprehensive telecommunications infrastructure. This infrastructure serves a wide range of uses, such as to provide telephone service or transmit data through a computer network.

4.5.1 Vertical and the Horizontal Cabling

The purpose of the **vertical** is to act as the high capacity backbone of the system. This would normally operate between different floors of the building and also main resource centres such as computer rooms and possibly the public service access point to the building.

The **horizontal** element is concerned with the linking of individual access points to the main backbone or vertical element. At the point of transition from vertical to horizontal, there is a requirement for some form of adaptability or conversion.

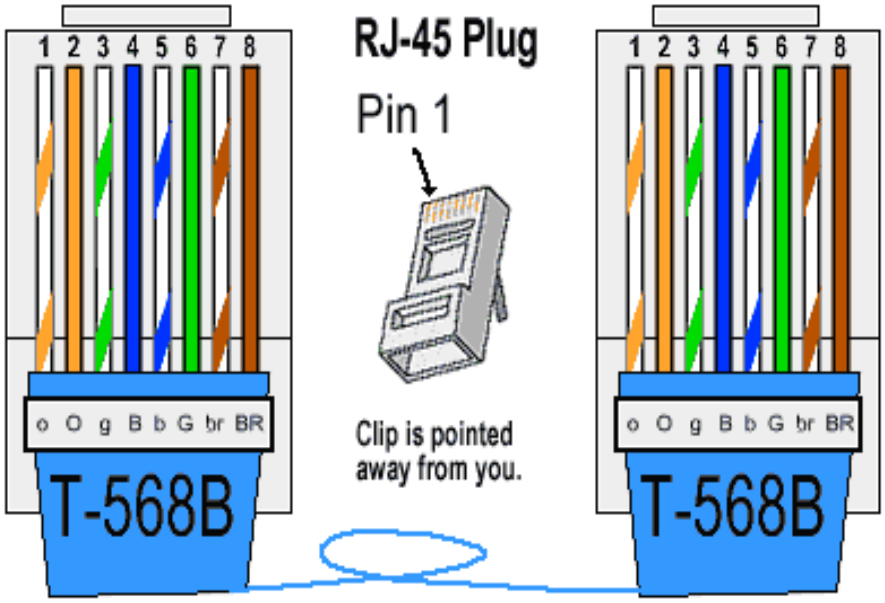
4.5.2 Cable types.

Straight Through Cabling

Straight through cable used to connect dissimilar devices e.g computer to hub, hub to switch, router to switch e.t.c

Both standards define the T-568A and T-568B pin-outs for using Unshielded Twisted Pair cable and RJ-45 connectors for Ethernet connectivity. The standards and pin-out specification appear to be related and interchangeable, but are not the same and should not be used interchangeably.

T-568B Straight-Through Ethernet Cable

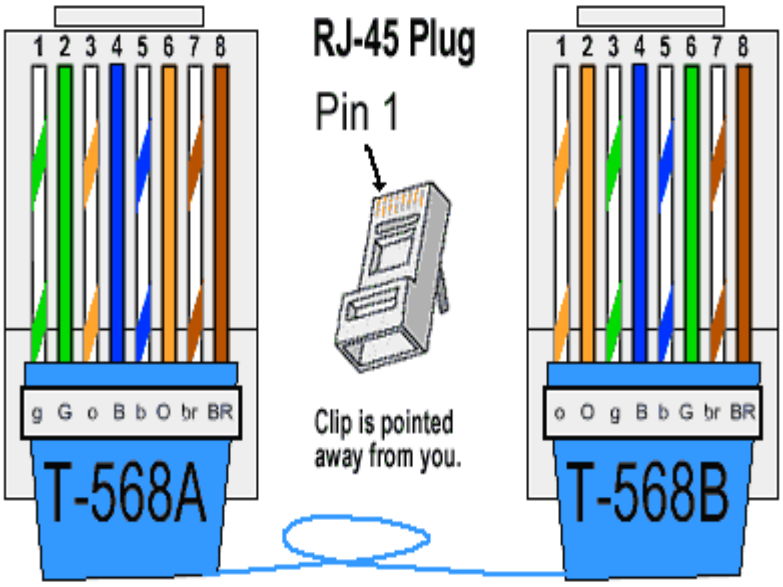


Crossover Ethernet Cable

Cross over cable are used to connect similar device. Each peer to peer, switch to switch, hub to hub,e.t.c

Both the T-568A and the T-568B standard Straight-Through cables are used most often as patch cords for your Ethernet connections. If you require a cable

to connect two Ethernet devices directly together without a hub or when you connect two hubs together, you will need to use a Crossover cable instead.

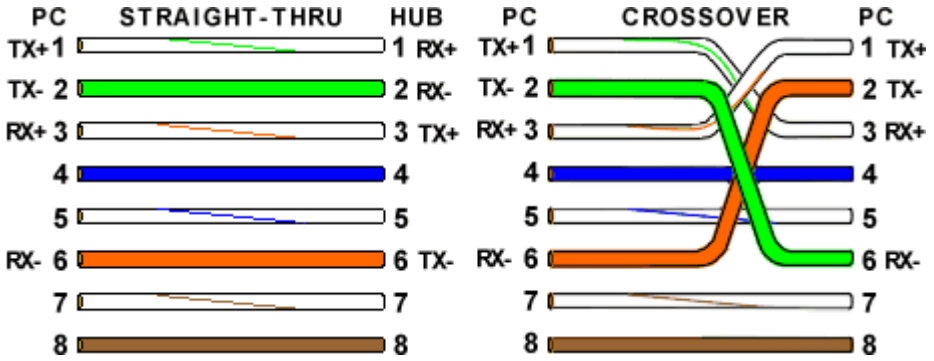


Ethernet Cable Instructions:

- Pull the cable off the reel to the desired length and cut. If you are pulling cables through holes, its easier to attach the RJ-45 plugs after the cable is pulled. The total length of wire segments between a PC and a hub or between two PC's cannot exceed 100 Meters (328 feet) for 100BASE-TX and 300 Meters for 10BASE-T.
- Start on one end and strip the cable jacket off (about 1") using a stripper or a knife. Be extra careful not to nick the wires, otherwise you will need to start over.
- Spread, untwist the pairs, and arrange the wires in the order of the desired cable end. Flatten the end between your thumb and forefinger. Trim the ends of the wires so they are even with one another, leaving only 1/2" in wire length. If it is longer than 1/2" it will be out-of-spec and susceptible to crosstalk. Flatten and insure there are no spaces between wires.
- Hold the RJ-45 plug with the clip facing down or away from you. Push the wires firmly into the plug. Inspect each wire is flat even at the front

of the plug. Check the order of the wires. Double check again. Check that the jacket is fitted right against the stop of the plug. Carefully hold the wire and firmly crimp the RJ-45 with the crimper.

- Check the color orientation, check that the **crimped connection** is not about to come apart, and check to see if the wires are flat against the front of the plug. If even one of these are incorrect, you will have to start over. Test the Ethernet cable.



Ethernet Cable Tips:

- A straight-through cable has identical ends.
- A crossover cable has different ends.
- A straight-thru is used as a patch cord in Ethernet connections.
- A crossover is used to connect two Ethernet devices without a hub or for connecting two hubs.
- A crossover has one end with the Orange set of wires switched with the Green set.
- Odd numbered pins are always striped, even numbered pins are always solid colored.
- Looking at the RJ-45 with the clip facing away from you, Brown is always on the right, and pin 1 is on the left.
- No more than 1/2" of the Ethernet cable should be untwisted otherwise it will be susceptible to crosstalk.
- Do not deform, do not bend, do not stretch, do not staple, do not run parallel with power cables, and do not run Ethernet cables near noise inducing components.

By looking at a T-568A UTP Ethernet straight-thru cable and an Ethernet crossover cable with a T-568B end, we see that the TX (transmitter) pins are connected to the corresponding RX (receiver) pins, plus to plus and minus to minus. Both the blue and brown wire pairs on pins 4, 5, 7, and 8 are not used in either standard. What you may not realize is that, these same pins 4, 5, 7, and 8 are not used or required in 100BASE-TX as well. So why bother using these wires, well for one thing its simply easier to make a connection with all the wires grouped together.

4.6 Patch panels

These are installed in the wiring closet and are designed for the management of cable connections. On the front side of a patch panel there are jacks designed to receive short patch cables, while on the back of the panel there are either jacks or punch down blocks that receive the connections of longer and more permanent cables. This makes it easier to manage 'moves and changes'

4.7 Network Interfaces Cards (NIC)

A network interface is a device that connects a client computer, server, printer or other component to your network. NIC consists of a small electronic circuit board that is inserted into a *slot* inside a computer or printer

NIC provides important services

1. It connects your computer physically to your network,
2. It converts information on your computer to and from electrical signals for your network.
3. Unique MAC (MEDIA Access Control) address helps route information within your local area network and is used by switches and bridges.

4.7.1 Types of NIC

- 10BaseT cards
  - Physical star networks
  - 10 Mbps speed
  - Ethernet standard
  - Twisted pair wiring

- 10base2 cards
  - Physical bus networks
  - 10 Mbps speed
  - Ethernet standard
  - Thin coaxial wiring
- 10Base5
  - 10 Mbps speed
  - Ethernet standard
  - Thick coaxial wiring
- 100BaseTX
  - 100 Mbps speed
  - Fast Ethernet standard
  - Twisted pair
    - Higher quality Category 5 wires are recommended
- Token ring network cards
- Earlier token ring cards
  - 4 Mbps
- Newer token ring cards
  - 16 Mbps

4.7.2 Cable Connections for NICs

- BNC barrel connector
  - Thin coaxial
- RJ 45
  - Twisted pair

4.8 Hubs/ Concentrators or Repeaters:

The hub is a small box that gathers the signals from each individual device, optionally amplifies each signal, and then sends the signal out to all other connected devices. Used for extending the physical span of a network out 10base5 the span is limited to 500 meters.

- Amplification helps to ensure that devices on the network receive reliable information.
- Operates at Physical layer
- Improves the performance by dividing the network into segments thus reducing the numbers of computers per segement.
- Hubs does not support support heavy network traffic
- Does not support uses of different access methods
- Does not filter traffic

Uses

1. Connects two segments of similar or dissimilar media
2. Regenerate the signal to increase the distance transmitted
3. Pass all traffic in both direction
4. Connect two segments in the most cost –effective manner.

Types

- Active hub
- Passive hub

- Passive hubs
  - Simply provides the physical and the electrical connection for the network
- Active hubs
  - Has built-in intelligence
  - Some are manageable hubs

4.9 Switches

A switch is defined as a device that allows a LAN to be segmented .The segments will operate under the same protocol**.** A switch focuses on segmenting a LAN. The device that gathers the signals from devices that are connected to it, and then regenerates a new copy of each signal.

i) Switches operate by learning the MAC addresses of all connected clients, servers, peripherals, and associating each address with one of its ports.

When a switch receives an incoming signal, it creates a temporary circuit between the sender and receiver.

ii) Most switches operate by examining incoming or outgoing signals for information at OSI level 2 the data link level.

4.9.1 Purpose of a Switch

- Performance is improved especially in the case of a bus network
- Multiple bus paths are now available for communication
- Each segment can engage in simultaneous communication within itself
- Easier to isolate a problem to a segment

Switches use three methods to deal with data as it arrives:

i) **Cut-through**—In a cut-through configuration, the switch begins to forward the packet as soon as it is received. No error checking is performed on the packet, so the packet is moved through quickly. The downside of cut-through is that because the integrity of the packet is not checked, the switch can propagate errors.

ii) **Store-and-forward**—In a store-and-forward configuration, the switch waits to receive
the entire packet before beginning to forward it. It also performs basic error checking.

iii) **Fragment-free**—Building on the speed advantages of cut-through switching, fragment free switching works by reading only the part of the packet that enables it to identify fragments of a transmission.

4.9.2 Switches have two benefits:

1. They provide each pair of communicating devices with a fast connection; and
2. They segregate the communication so that it does not enter other portions of the network.

4.10 Routers

Routers are devices whose primary purpose is to connect two or more networks and to filter network signals so that only desired information travels between

them. Routers can inspect a good deal more information than bridges, and they therefore can regulate network traffic more precisely. Routers operate primarily by examining incoming data for its network routing and transport. This information includes the source and destination network routing addresses information

The network routing address provides information on which routers base traffic management decisions Internal tables of network information that it compiles, a router then determines whether or not it knows how to forward the data packet towards its destination.

4.10.1 The Functions of a Router

i) Connect LANs operating under different protocols
ii) The LANs connected are better known as sub-networks instead of network segments
iii) Filtering and isolating traffic
iv) Connecting network segments.
v) A router is connected to two different networks and passes packets between them,

How Routers Work

i) All known networks addresses
ii) Instructions for connections to other networks
iii) The possible paths between routers
iv) The costs of sending data over those paths by choosing the best path (shortest path)

4.10.2 Router Characteristics

i) A router true internetworking device
    - Connects different sub-networks together
ii) Establishes a logical path of communication between the sub-networks
iii) Contributes to the modular construction of a network
    - Network itself is better managed
    - Network resources are better utilized

- Examine and alter the data packets
- Perform protocol conversion
- Operates at Network layer

4.10.3 Router Requirements

i) Requires more processing power compared to switches and hubs
ii) Operations fall within the network layer of the ISO-OSI communication model

4.10.4 Types of Routers

i) **Static routers**: Manually setups and configured the routing table by network administrator by specify each route.
ii) Dynamic router: Designed to discover routes automatically and require a minimal amount of setup and configuration. They examine information from routers and make packet by packet decisions about how to send data across the network.

4.10.5 Servers

A server is a system (software and suitable computer hardware) that responds to requests across a computer network to provide, or help to provide, a network service. Servers operate within a client-server architecture. Servers are computer programs running to serve the requests of other programs, the clients. Thus, the server performs some tasks on behalf of clients. The clients typically connect to the server through the network but may run on the same computer. In the context of Internet Protocol (IP) networking, a server is a program that operates as a socket listener

Servers often provide essential services across a network, either to private users inside a large organization or to public users via the Internet.

4.10.6 Server hardware

i) Hardware redundancy—installing more than one instance of modules such as power supplies and hard disks arranged so that if one fails another is automatically available—is widely used.

ii) Servers may incorporate faster, higher-capacity hard drives, larger computer fans or water cooling to help remove heat, and uninterruptible power supplies that ensure the servers continue to function in the event of a power failure.

iii) ECC memory devices that detect and correct errors are used;

iv) The hard drive controllers and RAID technology is recommend for servers.

4.10.7 Types of servers

i) A **database server** is a computer program that provides database services to other computer programs or computers, as defined by the client–server model. The term may also refer to a computer dedicated to running such a program. Database management systems frequently provide database server functionality, and some DBMSs, file server, mail server, print server, web server, gaming server, and application server.

ii) **File server** is a computer attached to a network that has the primary purpose of providing a location for shared disk access, i.e. shared storage of computer files (such as documents, sound files, photographs, movies, images, databases, etc.) that can be accessed by the workstations that are attached to the same computer network.

iii) **A mail server** is a computer that serves as an electronic post office for email. Mail exchanged across networks is passed between mail servers that run specially designed software. This software is built around agreed-upon, standardized protocols for handling mail messages and any data files (such as images, multimedia or documents) that might be attached to them.

iv) **Printer server**, is a device that connects printers to client computers over a network. It accepts print jobs from the computers and sends the jobs to the appropriate printers, queuing the jobs locally to accommodate the fact that work may arrive more quickly than the printer can actually handle it. Ancillary functions include the ability to inspect the queue of jobs to be processed, the ability to reorder or delete waiting print jobs, or

the ability to do various kinds of accounting (such as counting pages printer, which may involve reading data generated by the printer(s)

v) **Web server**: The primary function of a web server is to store, process and deliver web pages to clients. The communication between client and server takes place using the Hypertext Transfer Protocol (HTTP).

vi) **A proxy server** is a server (a computer system or an application) that acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource available from a different server and the proxy server evaluates the request as a way to simplify and control its complexity.

4.11 Gateways

A gateway device provides communication to a remote network or an autonomous system that is out of bounds for the host network nodes. Gateways serve as the entry and exit point of a network; all data routed inward or outward must first pass through and communicate with the gateway in order to use routing paths. The gateway (or default gateway) is implemented at the boundary of a network to manage all the data communication that is routed internally or externally from that network. Besides routing packets, gateways also possess information about the host network's internal paths and the learned path of different remote networks. If a network node wants to communicate with a foreign network, it will pass the data packet to the gateway, which then routes it to the destination using the best possible path.

4.12 Modem

Modem is a contraction of the terms modulator and demodulator. Modems perform a simple. The main function of modem is translate digital signals from a computer into analog signals that can travel across conventional phone lines. The modem modulates the signal at the sending end and demodulates at the receiving end.

How error detection works between two modems

1. Both Transmitting and receiving modems agree no how error check is to be calculated(via handshaking process)
2. Transmitting modem calculates and transmits the errors check along transmitted data
3. Receiving modem recalculates error check based on received data and compares its newly calculated error check that was calculated and transmitted mode
4. If error checks match transmission is ok – if the transmitted/ received doesn't match, error is detected.

4.13 Firewall

A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.They establish a barrier between secured and controlled internal networks that can be trusted and untrusted outside networks, such as the Internet. A firewall can be hardware, software, or both.

Types of firewalls

i) **Packet Filter firewall (network firewall)**. In Packet filter firewall each packet(incoming or outgoing) is compared to certain set of rules(As defined by the administrator) before it Is forwarded.

ii) **Stateful Inspections or application firewall**. It is a Packet filter firewall with an additional functionality of maintaining state of connections (for each packet) and blocking packets which deviates from their ideal state.

iii) **Application-Level Proxy:** These firewalls contain a proxy agent that acts as an intermediary between two hosts that wish to communicate with each other, and never allows a direct connection between them. Each successful connection attempt actually results in the creation of two separate connections—one between the client and the proxy server, and another between the proxy server and the true destination.

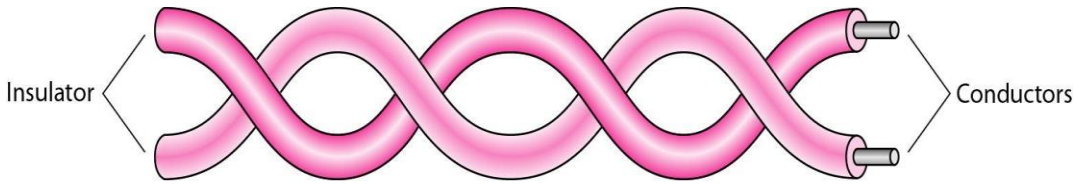
4.14 Types of network media

4.14.1 Guided media:

Guided media, which are those that provide a channel from one device to another, include twisted-pair cable, coaxial cable, and fiber-optic cable. A signal traveling along any of these media is directed and contained by the physical limits of the medium. Twisted-pair and coaxial cable use metallic (copper) conductors that accept and transport signals in the form of electric current. Optical fiber is a cable that accepts and transports signals in the form of light.

Twisted-Pair Cable

A twisted pair consists of two conductors (normally copper), each with its own plastic insulation, twisted together, as shown in the following figure.



One of the wires is used to carry signals to the receiver, and the other is used only as a ground reference. The receiver uses the difference between the two. In addition to the signal sent by the sender on one of the wires, interference (noise) and crosstalk may affect both wires and create unwanted signals.

If the two wires are parallel, the effect of these unwanted signals is not the same in both wires because they are at different locations relative to the noise or crosstalk sources (e,g., one is closer and the other is farther). This results in a difference at the receiver. By twisting the pairs, a balance is maintained.

For example, suppose in one twist, one wire is closer to the noise source and the other is farther; in the next twist, the reverse is true. Twisting makes it probable that both wires are equally affected by external influences (noise or crosstalk).

Unshielded Versus Shielded Twisted-Pair Cable

The most common twisted-pair cable used in communications is referred to as unshielded twisted-pair (UTP). IBM has also produced a version of twisted-pair cable for its use called shielded twisted-pair (STP). STP cable has a metal foil or braided mesh covering that encases each pair of insulated conductors which improves the quality of cable by preventing the penetration of noise or crosstalk, it is bulkier and more expensive.

Categories

The Electronic Industries Association (EIA) has developed standards to classify unshielded twisted-pair cable into seven categories. Categories are determined by cable quality, with 1 as the lowest and 7 as the highest. Each EIA category is suitable for specific uses.

Performance

One way to measure the performance of twisted-pair cable is to compare attenuation versus frequency and distance. A twisted-pair cable can pass a wide range of frequencies. With increasing frequency, the attenuation, measured in decibels per kilometer (dB/km), sharply increases with frequencies above 100 kHz.

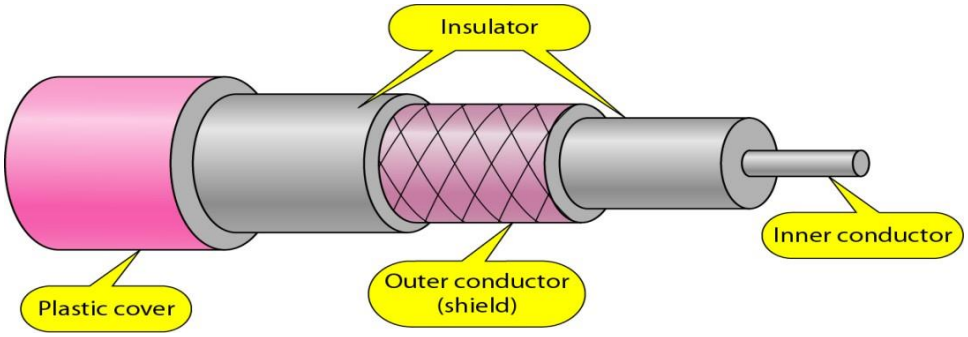
Applications

Twisted-pair cables are used in telephone lines to provide voice and data channels and Local- area networks, such as lOBase-T and lOOBase-T, also use twisted-pair cables.

Coaxial Cable:

Coaxial cable (or coax) carries signals of higher frequency ranges than those in twisted pair cable. Coax has a central core conductor of solid or stranded wire (usually copper) enclosed in an insulating sheath, which is, in turn, encased in an outer conductor of metal foil, braid, or a combination of the two. The outer metallic wrapping serves both as a shield against noise and as the second conductor, which completes the circuit. This outer conductor is

also enclosed in an insulating sheath, and the whole cable is protected by a plastic cover which is shown as follows.



Coaxial Cable Standards:

Coaxial cables are categorized by their Radio Government (RG) ratings. Each RG number denotes a unique set of physical specifications, including the wire gauge of the inner conductor, the thickness and type of the inner insulator, the construction of the shield, and the size and type of the outer casing. Different categories are like RG-59, RG-58 and RG-11.

Performance:

The attenuation is much higher in coaxial cables than in twisted-pair cable. In other words, although coaxial cable has a much higher bandwidth, the signal weakens rapidly and requires the frequent use of repeaters.

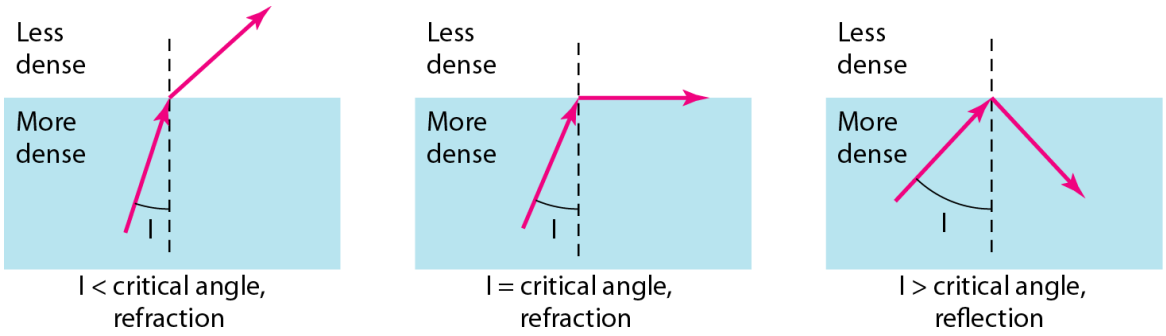
Applications:

The different applications of Coaxial cable are as follows.

i) Coaxial cable was widely used in analog telephone networks where a single coaxial network could carry 10,000 voice signals.
ii) Cable TV networks also use coaxial cables.
iii) Another common application of coaxial cable is in traditional Ethernet LANs

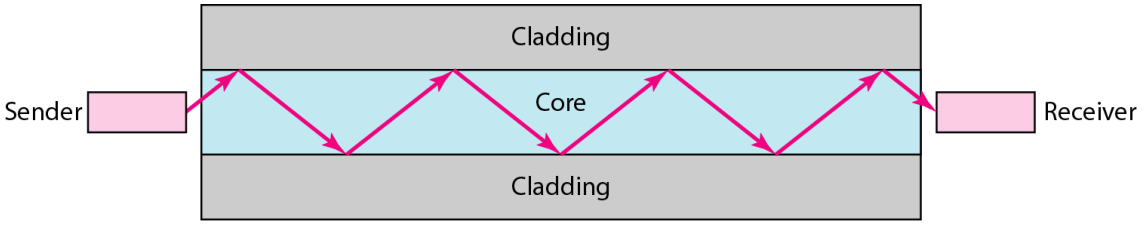
Fiber-Optic Cable:

A fiber-optic cable is made of glass or plastic and transmits signals in the form of light. Light travels in a straight line as long as it is moving through a single uniform substance. If a ray of light traveling through one substance suddenly enters another substance of a different density, the ray changes direction. The following figure shows how a ray of light changes direction when going from a more dense to a less dense substance.



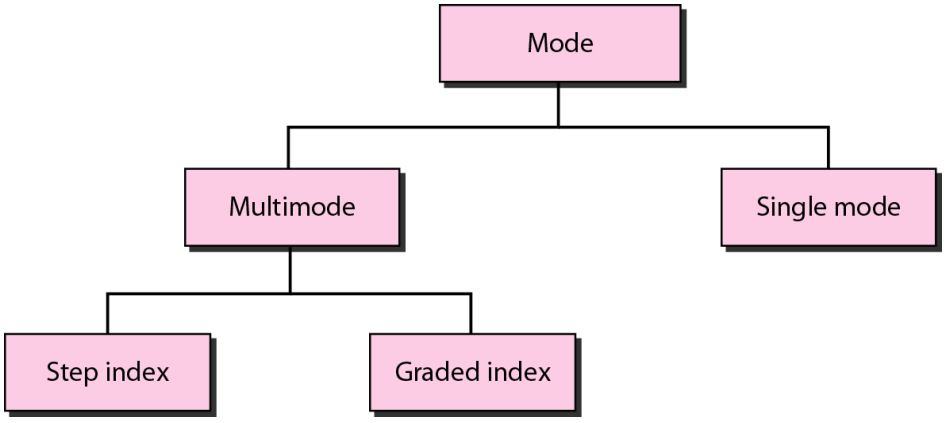
As the figure shows, if the angle of incidence I (the angle the ray makes with the line perpendicular to the interface between the two substances) is less than the critical angle, the ray refracts and moves closer to the surface. If the angle of incidence is equal to the critical angle, the light bends along the interface. If the angle is greater than the critical angle, the ray reflects (makes a turn) and travels again in the denser substance. Note that the critical angle is a property of the substance, and its value differs from one substance to another.

Optical fibers use reflection to guide light through a channel. A glass or plastic core is surrounded by a cladding of less dense glass or plastic. The difference in density of the two materials must be such that a beam of light moving through the core is reflected off the cladding instead of being refracted into it as shown in the following figure.

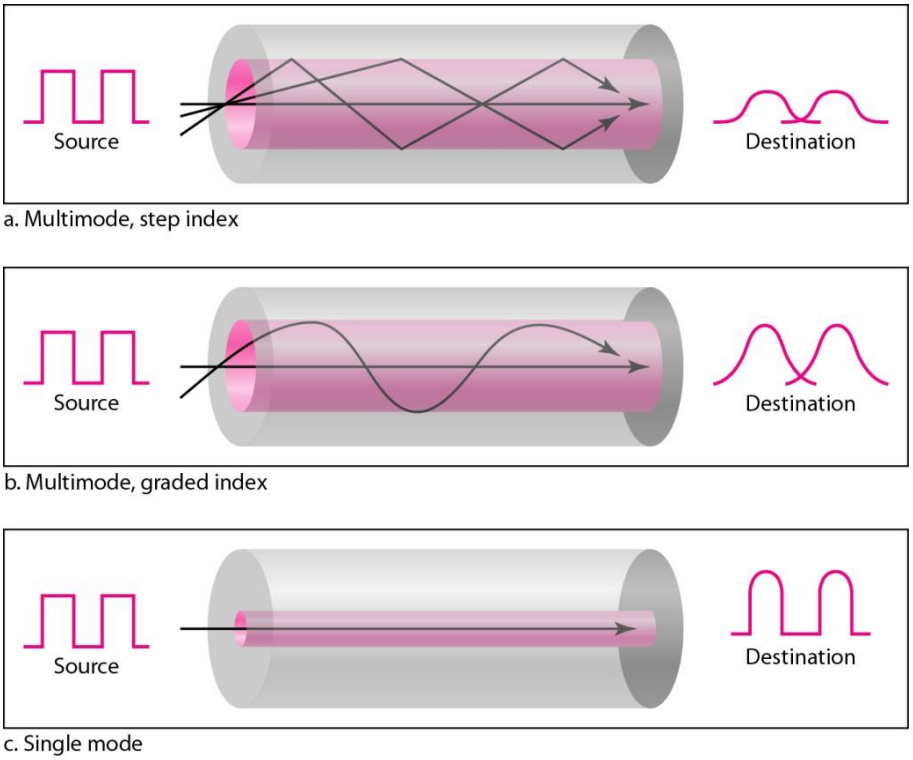


Propagation Modes:

Current technology supports two modes (multimode and single mode) for propagating light along optical channels, each requiring fiber with different physical characteristics. Multimode can be implemented in two forms: step-index or graded-index as shown in the following figure.



i) **Multimode:** Multimode is so named because multiple beams from a light source move through the core in different paths. How these beams move within the cable depends on the structure of the core, as shown in the following figure.



ii) **In multimode step-index fiber**, the density of the core remains constant from the center to the edges. A beam of light moves through this constant density in a straight line until it reaches the interface of the core and the cladding. At the interface, there is an abrupt change due to a lower density; this alters the angle of the beam's motion. The term step index refers to the suddenness of this change, which contributes to the distortion of the signal as it passes through the fiber.

iii) **In multimode graded-index fiber**, decreases this distortion of the signal through the cable. The word index here refers to the index of refraction. As we saw above, the index of refraction is related to density. A graded-index fiber, therefore, is one with varying densities. Density is highest at the center of the core and decreases gradually to its lowest at the edge. The above figure shows the impact of this variable density on the propagation of light beams.

iv) **Single-Mode:** Single-mode uses step-index fiber and a highly focused source of light that limits beams to a small range of angles, all close to the horizontal. The single mode fiber itself is manufactured with a much smaller diameter than that of multimode fiber, and with substantially lowers density (index of refraction). The decrease in density results in a critical angle that is close enough to 90° to make the propagation of beams almost horizontal. In this case, propagation of different beams is almost identical, and delays are negligible. All the beams arrive at the destination "together" and can be recombined with little distortion to the signal.

Performance:

Attenuation is flatter than in the case of twisted-pair cable and coaxial cable. The performance is such that we need fewer (actually 10 times less) repeaters when we use fiber-optic cable.

Applications

- Fiber-optic cable is often found in backbone networks because its wide bandwidth is cost-effective.
- Some cable TV companies use a combination of optical fiber and coaxial cable, thus creating a hybrid network. Optical fiber provides the backbone structure while coaxial cable provides the connection to the user premises. This is a cost-effective configuration since the narrow bandwidth requirement at the user end does not justify the use of optical fiber.
- Local-area networks such as 100Base-FX network (Fast Ethernet) and 1000Base-X also use fiber-optic cable.

Advantages and Disadvantages of Optical Fiber:

Advantages: Fiber-optic cable has several advantages which are as follows.

i) **Higher bandwidth:** Fiber-optic cable can support dramatically higher bandwidths and hence data rates than either twisted-pair or coaxial

cable. Currently, data rates and bandwidth utilization over fiber-optic cable are limited not by the medium but by the signal generation and reception technology available.

ii) **Less signal attenuation:** Fiber-optic transmission distance is significantly greater than that of other guided media. A signal can run for 50 km without requiring regeneration. We need repeaters every 5 km for coaxial or twisted-pair cable.

iii) **Immunity to electromagnetic interference:** Electromagnetic noise cannot affect fiber- optic cables.

iv) **Resistance to corrosive materials:** Glass is more resistant to corrosive materials than copper.

v) **Light weight:** Fiber-optic cables are much lighter than copper cables.

vi) **Greater immunity to tapping:** Fiber-optic cables are more immune to tapping than copper cables. Copper cables create antenna effects that can easily be tapped.

Disadvantages: There are some disadvantages in the use of optical fiber.

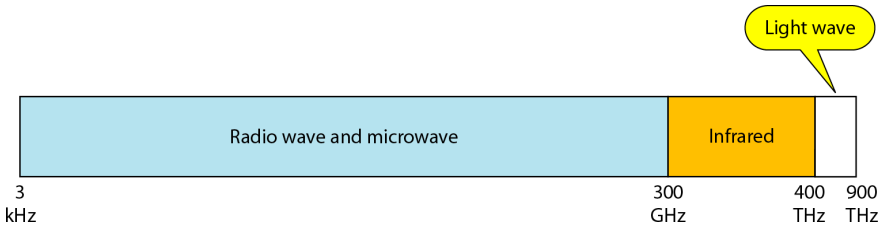
i) **Installation and maintenance:** Fiber-optic cable is a relatively new technology. Its installation and maintenance require expertise that is not yet available everywhere.

ii) **Unidirectional light propagation:** Propagation of light is unidirectional. If we need bidirectional communication, two fibers are needed.

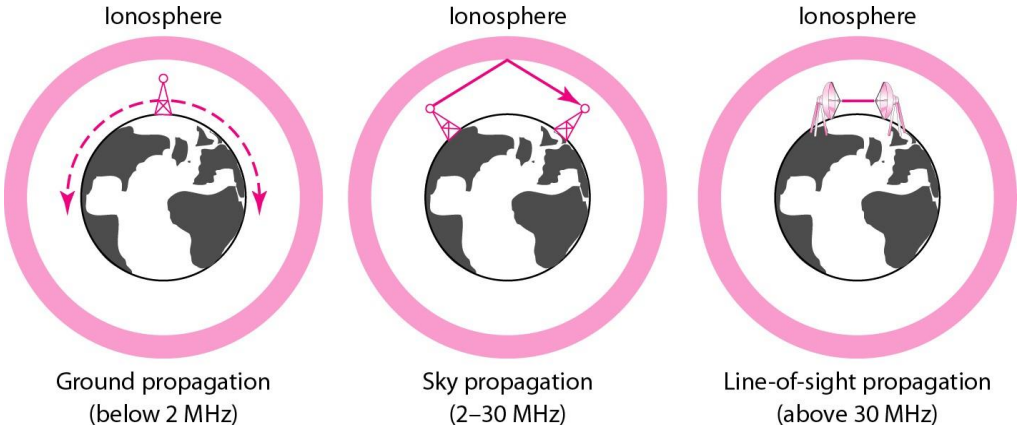
iii) **Cost:** The cable and the interfaces are relatively more expensive than those of other guided media. If the demand for bandwidth is not high, often the use of optical fiber cannot be justified.

4.14.2 Unguided media- Wireless Communication:

Unguided media transport electromagnetic waves without using a physical conductor. This type of communication is often referred to as wireless communication. Signals are normally broadcast through free space and thus are available to anyone who has a device capable of receiving them.



Unguided signals can travel from the source to destination in several ways: ground propagation, sky propagation, and line-of-sight propagation, as shown in the following figure.



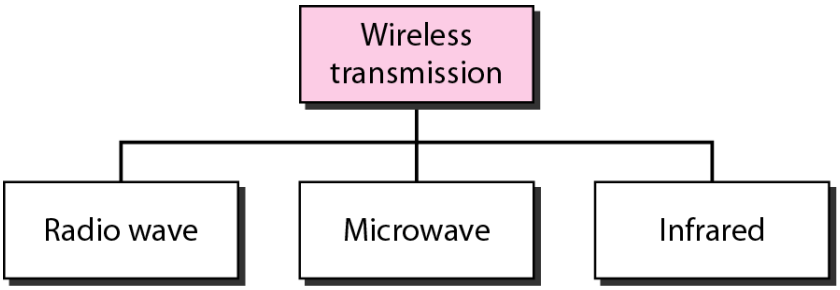
i) **Ground propagation mode:** In ground propagation, radio waves travel through the lowest portion of the atmosphere, hugging the earth. These low-frequency signals emanate in all directions from the transmitting antenna and follow the curvature of the planet. Distance depends on the amount of power in the signal: The greater the power, the greater the distance.

ii) **Sky propagation mode:** In sky propagation, higher-frequency radio waves radiate upward into the ionosphere (the layer of atmosphere where particles exist as ions) where they are reflected back to earth. This type of transmission allows for greater distances with lower output power.

iii) **Line-of-sight propagation mode:** In line-or-sight propagation, very high-frequency signals are transmitted in straight lines directly from

antenna to antenna. Antennas must be directional, facing each other and either tall enough or close enough together not to be affected by the curvature of the earth. Line-of-sight propagation is tricky because radio transmissions cannot be completely focused.

We can divide wireless transmission into three broad groups: radio waves, microwaves, and infrared waves as shown in the following figure.



Radio Waves:

Radio waves, for the most part, are omnidirectional. The electromagnetic waves ranging in frequencies between 3 kHz and 1 GHz are normally called radio waves. Radio waves, for the most part, are omnidirectional. When an antenna transmits radio waves, they are propagated in all directions. This means that the sending and receiving antennas do not have to be aligned. A sending antenna sends waves that can be received by any receiving antenna. The omnidirectional property has a disadvantage, too.

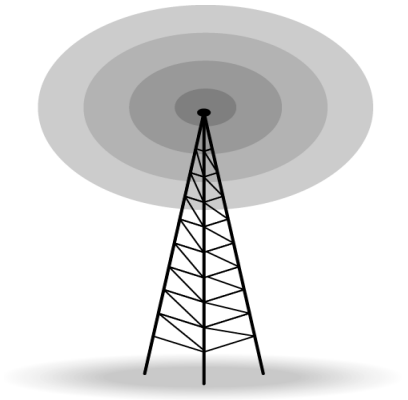
The radio waves transmitted by one antenna are susceptible to interference by another antenna that may send signals using the same frequency or band. Radio waves, particularly those waves that propagate in the sky mode, can travel long distances. This makes radio waves a good candidate for long-distance broadcasting such as AM radio.

Radio waves, particularly those of low and medium frequencies, can penetrate walls. This characteristic can be both an advantage and a disadvantage. It is an advantage because, for example, an AM radio can receive signals inside a building. It is a disadvantage because we cannot isolate a communication to just inside or outside a building.

Omnidirectional Antenna

Radio waves use omnidirectional antennas that send out signals in all directions. Based on the wavelength, strength, and the purpose of

transmission, we can have several types of antennas. The following figure shows an omnidirectional antenna.



Applications

The omnidirectional characteristics of radio waves make them useful for multicasting, in which there is one sender but many receivers. AM and FM radio, television, maritime radio, cordless phones, and paging are examples of multicasting.

Microwaves

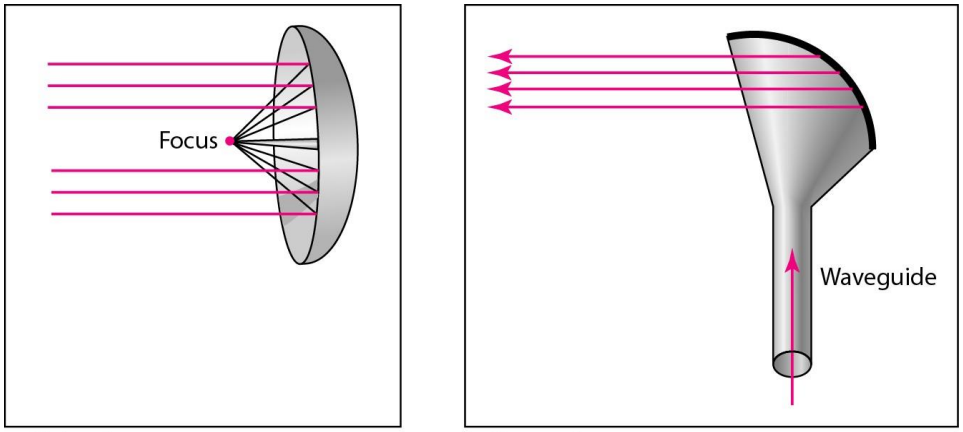
Electromagnetic waves having frequencies between 1 and 300 GHz are called microwaves. Microwaves are unidirectional. When an antenna transmits microwave waves, they can be narrowly focused. This means that the sending and receiving antennas need to be aligned. The unidirectional property has an obvious advantage. A pair of antennas can be aligned without interfering with another pair of aligned antennas. The following describes some characteristics of microwave propagation:

- Microwave propagation is line-of-sight. Since the towers with the mounted antennas need to be in direct sight of each other, towers that are far apart need to be very tall. The curvature of the earth as well as other blocking obstacles does not allow two short towers to communicate by using microwaves. Repeaters are often needed for long distance communication.
- Very high-frequency microwaves cannot penetrate walls. This characteristic can be a disadvantage if receivers are inside buildings.

- The microwave band is relatively wide, almost 299 GHz. Therefore wider sub bands can be assigned, and a high data rate is possible
- Use of certain portions of the band requires permission from authorities.

Unidirectional Antenna

Microwaves need unidirectional antennas that send out signals in one direction. Two types of antennas are used for microwave communications: the parabolic dish and the horn which are shown in the following figure.



a. Dish antenna

b. Horn antenna

A parabolic dish antenna is based on the geometry of a parabola: Every line parallel to the line of symmetry (line of sight) reflects off the curve at angles such that all the lines intersect in a common point called the focus. The parabolic dish works as a funnel, catching a wide range of waves and directing them to a common point. In this way, more of the signal is recovered than would be possible with a single-point receiver.

Outgoing transmissions are broadcast through a horn aimed at the dish. The microwaves hit the dish and are deflected outward in a reversal of the receipt path.

A horn antenna looks like a gigantic scoop. Outgoing transmissions are broadcast up a stem (resembling a handle) and deflected outward in a series of narrow parallel beams by the curved

head. Received transmissions are collected by the scooped shape of the horn, in a manner similar to the parabolic dish, and are deflected down into the stem.

Applications:

Microwaves, due to their unidirectional properties, are very useful when unicast (one-to-one) communication is needed between the sender and the receiver. They are used in cellular phones, satellite networks, and wireless LANs.

Infrared

Infrared waves, with frequencies from 300 GHz to 400 THz (wavelengths from 1 mm to 770 nm), can be used for short-range communication. Infrared waves, having high frequencies, cannot penetrate walls. This advantageous characteristic prevents interference between one system and another; a short-range communication system in one room cannot be affected by another system in the next room.

When we use our infrared remote control, we do not interfere with the use of the remote by our neighbors. However, this same characteristic makes infrared signals useless for long-range communication. In addition, we cannot use infrared waves outside a building because the sun's rays contain infrared waves that can interfere with the communication.

Applications

The infrared band, almost 400 THz, has an excellent potential for data transmission. Such a wide bandwidth can be used to transmit digital data with a very high data rate.

4.15 Network Address Translation(NAT)

Network Address Translation helps improve security by reusing IP addresses. The NAT router translates traffic coming into and leaving the private network. NAT gateways sit between two networks, the *inside* network and the *outside* network. Systems on the inside network are typically assigned IP addresses that cannot be routed to external networks. NAT conserves the number of globally valid IP addresses a company needs, and in combination with Classless Inter-

Domain Routing (CIDR) has done a lot to extend the useful life of IPv4 as a result.

NAT gateways can map IP addresses in several ways:

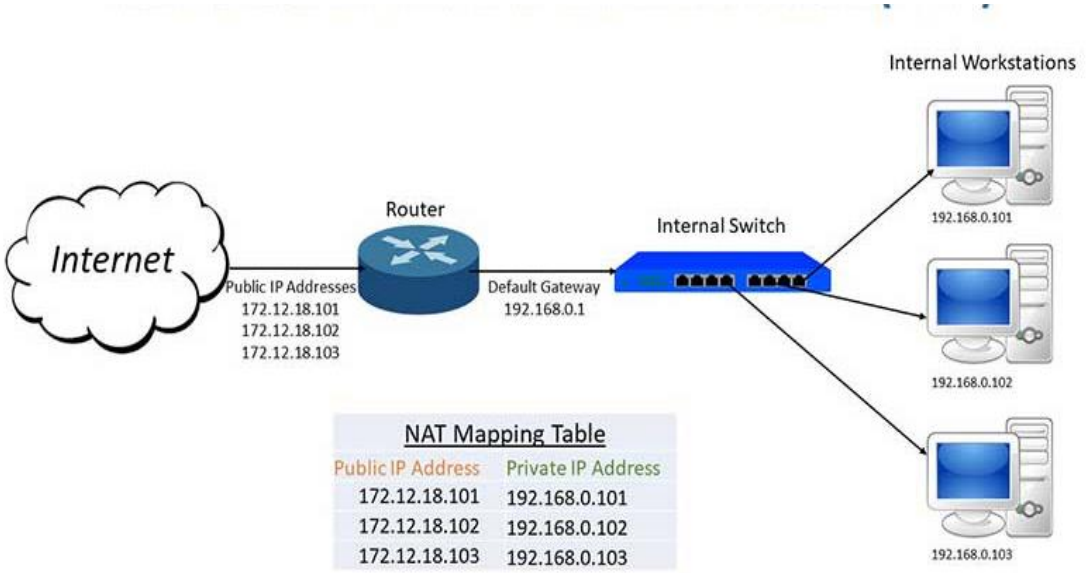
i) From a local IP address to one global IP address statically;

ii) From a local IP address to any of a rotating pool of global IP addresses a company may have;

iii) From a local IP address plus a particular TCP port to a global IP address or one in a pool of ports;

iv) From a global IP address to any of a pool of local IP addresses on a round-robin basis.

Example



In summary, you learned the;

i) Roles of Digital Service Unit (DSU)

ii) Concepts of Channel Service Unit (CSU)

iii) Functions of Data Terminal Equipment (DTE)

iv) Concepts of Ethernet Wiring Technology

v) The roles of Patch Panels and Network interfaces Cards(NIC)

vi) Function Hubs/ concentrators or Repeaters

vii) Importance of Switches, Routers and Servers in networks

viii) The functions of Gateways, Modem and Firewall in networks

ix) Types of transmission media

x) Importance of Network Address Translation (NAT).

Glossary

Network Terminal (NT) devices is device which ends a telecommunications link and is the point at which a signal enters or leaves a network.

Data Terminal Equipment (DTE) (DTE) is an end instrument that converts user information into signals or reconverts received signals.

A channel service unit (CSU) is a line Bridging device for use with T-carrier.

Data Terminal Equipment (DTE) is an end instrument that converts user information into signals or reconverts received signals

Hubs/ concentrators or Repeaters is small box that gathers the signals from each individual device, optionally amplifies each signal, and then sends the signal out to all other connected devices.

Switch is a device that gathers the signals from devices that are connected to it, and then regenerates a new copy of each signal.

Routers are devices whose primary purpose is to connect two or more networks and to filter network signals so that only desired information travels between them.

A **server** is a system (software and suitable computer hardware) that responds to requests across a computer network to provide, or help to provide, a network service.

A gateway device provides communication to a remote network or an autonomous system that is out of bounds for the host network nodes.

Modem (**Mod**ulator and **Dem**odulator) is device that translate digital signals from a computer into analog signals that can travel across conventional phone lines.

A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.

Guided media are those that provide a channel from one device to another.

Unguided media transport electromagnetic waves without using a physical conductor.

Network Address Translation (NAT) is devices used to improve security by reusing IP addresses.

Further Reading

Data & Computer networks, Prakash Gupta

William Stallings, Data & Computer networks 10th edition

Any other data communication and networking relevant books, journals, articles e.t.c

TOPIC ACTIVITIES

Activity

In your own perspective used the skills you have gain from the topic to figure out how Access Point (AP) qualify to be one of the network terminal device if you agree with the statement.

Tips

Use internet search to review the how Access Point (AP) operates as one of Network Terminal Device.

Review/ Assignment1 to be submitted through contact e-mail

i) Explain how error detection works between two modems **(5 Marks)**

ii) Explain any four router characteristics used in accomplishing stated purposes. **(8 Marks)**

iii) A switch is a device that allows a LAN to be segmented and operate under the same protocol**.**

   a) State which OSI layer does a switch operate **(2 Mark)**

   b) How does a switch gather signals from devices that are connected and regenerate a new copy?

c) Recommend the best method used by switches to deal with data giving reason(s). **(3 Marks)**

iv) You have two cell phone and you want to exchange information between this two devices wirelessly. What networking terminal devices might you require as a feature of both cell phone to accomplish this? Explain how the devices operates **(8 Marks)**

v) Illustrate the difference between the following fibre optics propagation methods

i) Multi-Mode Step Index **(2 Marks)**

ii) Multi-Mode Graded Index **(2 Marks)**

TOPIC FIVE: OPEN SYSTEMS INTERCONNECTION (OSI) REFERENCE MODEL

Welcome to topic one. This topic is aimed at introducing main concepts of Open Systems Interconnection (OSI) reference model, roles of OSI and functions of each OSI layer.

The topic is, therefore designed to prepare you to have a clear understanding of responsibilities of each OSI layer as well.

Topic Time

- Compulsory online reading, activities, self-assessments and practice exercises **[3 hours]**
- Optional further reading **[1.5 hours]**
- Total student input **[4.5 hours]**

Topic Learning Requirements

- Participation in one *chat* (at least 5 entries)
- At least two elaborate contributions to the *discussion* topic. You may also start your own discussion thread.
- Timely submission of the assignments

Learning Outcomes

By the end of this topic you should be able to:

i) Explain concepts of Open Systems Interconnection (OSI) Reference Model
ii) Discuss roles of OSI
iii) Explain functions of each OSI layer
iv) Describe responsibilities of each OSI layer

Topic Contents

5.1 Introduction

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 groups communication functions into seven logical layers. A layer serves the layer above it and is served by the layer below it.

5.1.1 Encapsulation and Decapsulation

At each level (N), two entities (layer N peers) exchange protocol data units (PDUs) by means of a layer-N protocol. A service data unit (SDU) is the payload of a PDU, transmitted unchanged to a peer. The SDU is a unit of data that has been passed down from an OSI layer to the next-lower layer, and which the lower layer encapsulates into a PDU. Layer N-1 adds a header or footer, or both, to the SDU, composing a PDU of layer N-1. The added framing makes it possible to get the data from a source to a destination. The PDU at a layer N becomes the SDU of layer N-1 process is refers as decapsulation

2.3 OSI Layers

OSI Model			
	Data unit	Layer	Function
Host layers	Data	7. Application	Network process to application
		6. Presentation	Data representation,encryption and decryption
		5. Session	Interhost communication
	Segments	4. Transport	End-to-end connections and reliability,Flow control
Media layers	Packet	3. Network	Path determination and logical addressing
	Frame	2. Data Link	Physical addressing
	Bit	1. Physical	Media, signal and binary transmission

Advantages and Disadvantages of OSI Model

Advantages

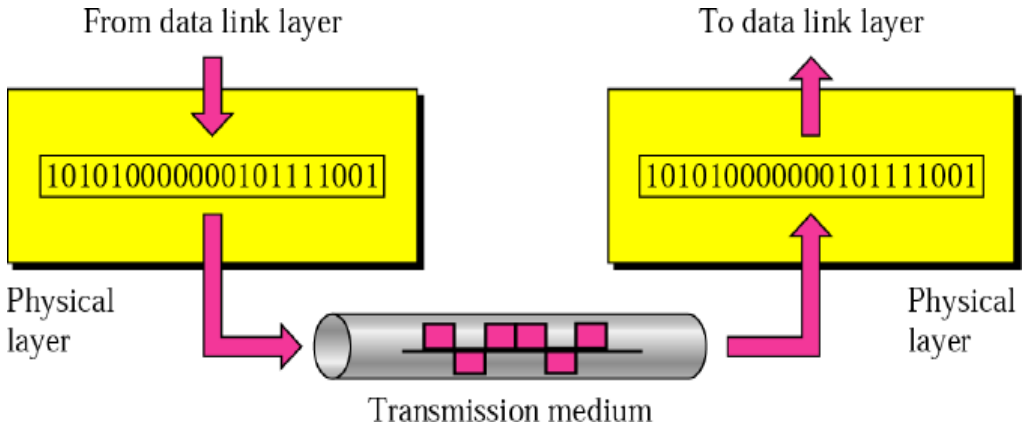
i) Reduces complexity:
ii) Standardizes interfaces:
iii) Facilitates modular engineering
iv) Interoperability between Vendors:
v) Ensures interoperable technology:
vi) Accelerates evolution
vii) Simplifies teaching and learning

Disadvantages

i) Many applications do not need the data integrity provided by OSI
ii) Many LAN applications need very fast setup
iii) The OSI model is too complex
iv) Not adapted at all to telecommunication/Network applications

5.3.1 Physical Layer

The physical layer coordinates the functions required to carry a bit stream over a physical medium. It deals with the mechanical and electrical specifications of the interface and transmission medium. It also defines the procedures and functions that physical devices and interfaces have to perform for transmission to Occur. Figure shows the position of the physical layer with respect to the transmission medium and the data link layer.



The physical layer is also concerned with the following:

i) **Physical characteristics** of interfaces and medium: The physical layer defines the characteristics of the interface between the devices and the transmission medium. It also defines the type of transmission medium.

ii) **Representation of bits**: The physical layer data consists of a stream of bits (sequence of Os or 1s) with no interpretation. To be transmitted, bits must be encoded into signals--electrical or optical. The physical layer defines the type of encoding (how Os and I s are changed to signals).

iii) **Data rate**: The transmission rate-the number of bits sent each second-is also defined by the physical layer.

iv) **Synchronization of bits**: The sender and receiver not only must use the same bit rate but also must be synchronized at the bit level. In other words, the sender and the receiver clocks must be synchronized.

v) **Line configuration**: The physical layer is concerned with the connection of devices to the media. In a point-to-point configuration, two devices are connected through a dedicated link. In a multipoint configuration, a link is shared among several devices.

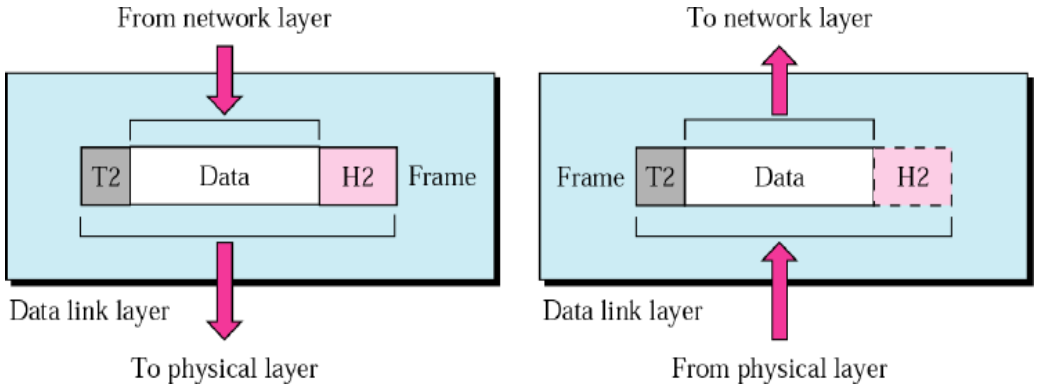
vi) **Physical topology:** The physical topology defines how devices are connected to make a network. Devices can be connected by using a mesh topology (every device is connected to every other device), a star topology (devices are connected through a central device), a ring topology (each device is connected to the next, forming a ring), a bus topology (every device is on a common link), or a hybrid topology (this is a combination of two or more topologies).

vii) **Transmission mode**: The physical layer also defines the direction of transmission between two devices: simplex, half-duplex, or full-duplex.

5.3.2 Data Link Layer:

The data link layer is responsible for moving frames from one hop (node) to the next. It makes the physical layer appear error-free to the upper layer (network

layer). The following Figure shows the relationship of the data link layer to the network and physical layers.



Other responsibilities of the data link layer include the following:

i) **Framing**: The data link layer divides the stream of bits received from the network layer into manageable data units called frames.

ii) **Physical addressing**: If frames are to be distributed to different systems on the network, the data link layer adds a header to the frame to define the sender and/or receiver of the frame. If the frame is intended for a system outside the sender's network, the receiver address is the address of the device that connects the network to the next one.

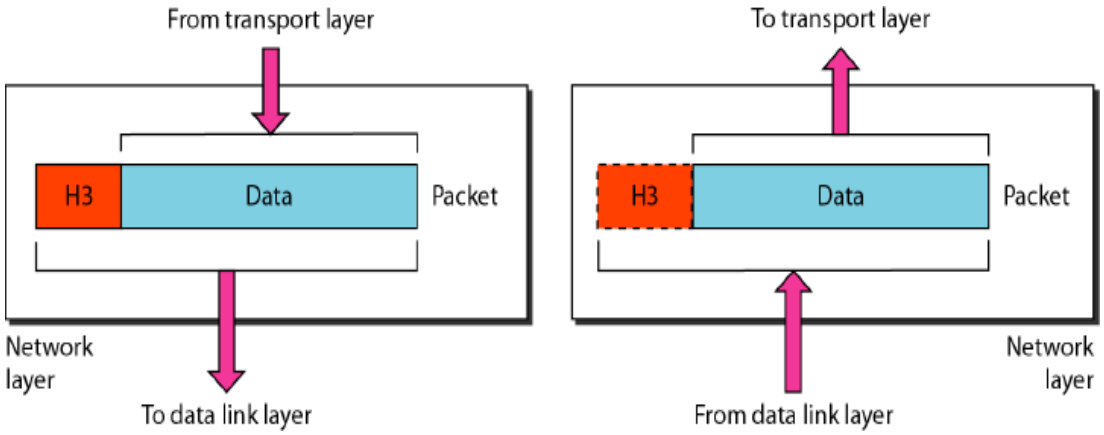
iii) **Flow control:** If the rate at which the data are absorbed by the receiver is less than the rate at which data are produced in the sender, the data link layer imposes a flow control mechanism to avoid overwhelming the receiver.

iv) **Error control:** The data link layer adds reliability to the physical layer by adding mechanisms to detect and retransmit damaged or lost frames. It also uses a mechanism to recognize duplicate frames. Error control is normally achieved through a trailer added to the end of the frame.

v) **Access control**: When two or more devices are connected to the same link, data link layer protocols are necessary to determine which device has control over the link at any given time.

5.3.3 Network Layer:

The network layer is responsible for the delivery of individual packets from the source host to the destination host possibly across multiple networks (links). Whereas the data link layer oversees the delivery of the packet between two systems on the same network (links), the network layer ensures that each packet gets from its point of origin to its final destination. If two systems are connected to the same link, there is usually no need for a network layer. The following shows the relationship of the network layer to the data link and transport layers.



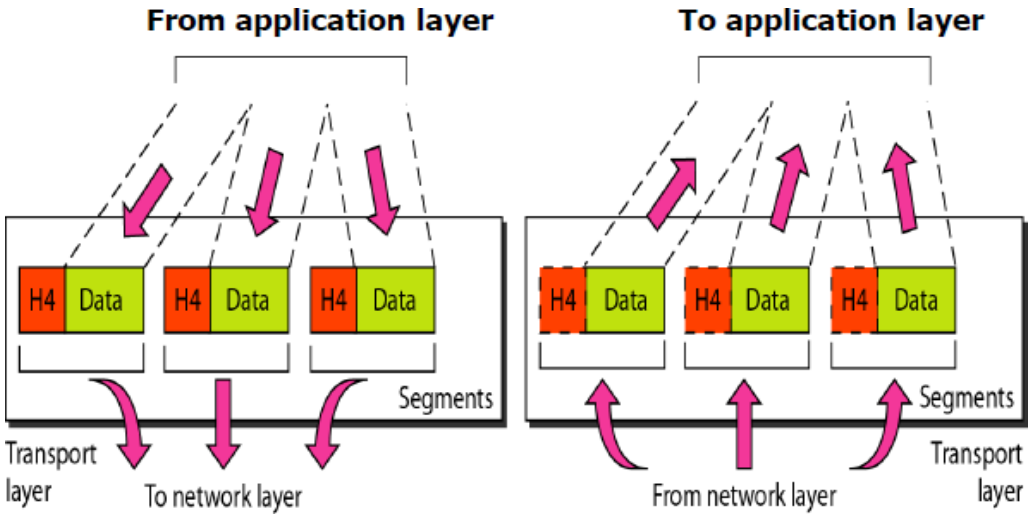
Other responsibilities of the network layer include the following:

i) **Logical addressing**: The physical addressing implemented by the data link layer handles the addressing problem locally. If a packet passes the network boundary, we need another addressing system to help distinguish the source and destination systems. The network layer adds a header to the packet coming from the upper layer that, among other things, includes the logical addresses of the sender and receiver.

ii) **Routing**: When independent networks or links are connected to create internetworks (network of networks) or a large network, the connecting devices (called routers or switches) route or switch the packets to their final destination. One of the functions of the network layer is to provide this mechanism.

5.1.4 Transport Layer:

The transport layer is responsible for process-to-process delivery of the entire message. A process is an application program running on a host. Whereas the network layer oversees source-to-destination delivery of individual packets, it does not recognize any relationship between those packets. It treats each one independently, as though each piece belonged to a separate message, whether or not it does. The transport layer, on the other hand, ensures that the whole message arrives intact and in order, overseeing both error control and flow control at the source-to-destination level. The following Figure shows the relationship of the transport layer to the network and session layers.



Other responsibilities of the transport layer include the following:

i) **Service-point addressing**: Computers often run several programs at the same time. For this reason, source-to-destination delivery means delivery not only from one computer to the next but also from a specific process (running program) on one computer to a specific process (running program) on the other. The transport layer header must therefore include a type of address called a service-point address (or port address). The network layer gets each packet to the correct computer; the transport layer gets the entire message to the correct process on that computer.

ii) **Segmentation and reassembly**: A message is divided into transmittable segments, with each segment containing a sequence number. These numbers enable the transport layer to reassemble the message correctly upon arriving at the destination and to identify and replace packets that were lost in transmission.

iii) **Connection control**: The transport layer can be either connectionless or connection oriented. A connectionless transport layer treats each segment as an independent packet and delivers it to the transport layer at the destination machine. A connection oriented transport layer makes a connection with the transport layer at the destination machine first before delivering the packets. After all the data are transferred, the connection is terminated.

iv) **Flow control**: Like the data link layer, the transport layer is responsible for flow control. However, flow control at this layer is performed end to end rather than across a single link.

v) **Error control**: Like the data link layer, the transport layer is responsible for error control. However, error control at this layer is performed process-to-process rather than across a single link: The sending transport layer makes sure that the entire message arrives at the receiving transport layer without error (damage, loss, or duplication). Error correction is usually achieved through retransmission.

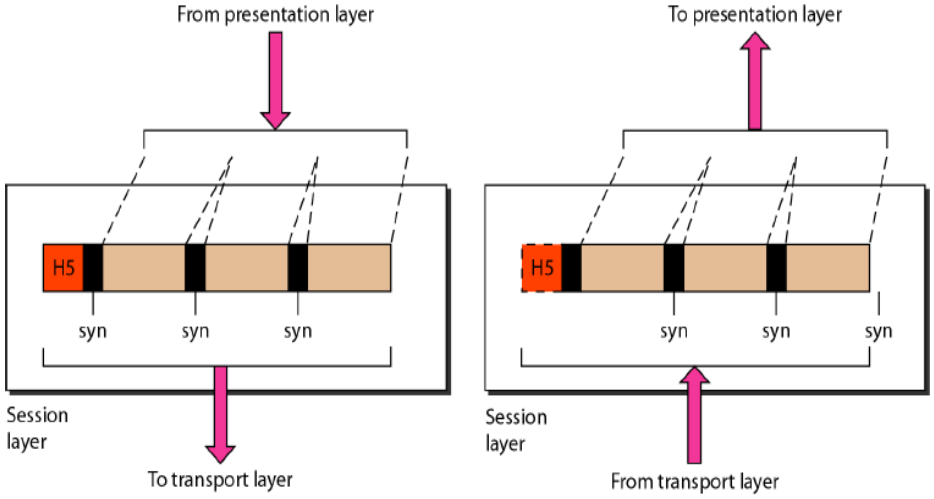
5.1.5 Session Layer:

The services provided by the first three layers (physical, data link, and network) are not sufficient for some processes. The session layer is the network dialog controller. It establishes, maintains, and synchronizes the interaction among communicating systems. Specific responsibilities of the session layer include the following:

i) **Dialog control**: The session layer allows two systems to enter into a dialog. It allows the communication between two processes to take place

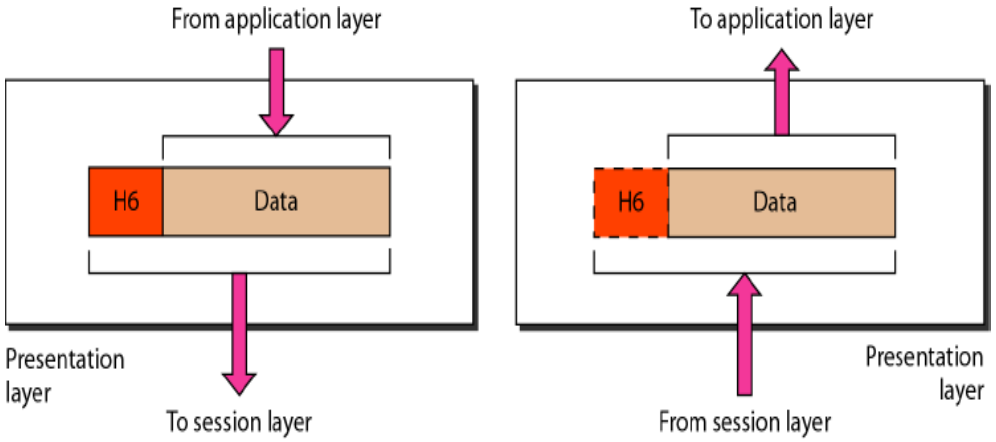
in either half duplex (one way at a time) or full-duplex (two ways at a time) mode.

ii) **Synchronization**: The session layer allows a process to add checkpoints, or synchronization points, to a stream of data. For example, if a system is sending a file of 2000 pages, it is advisable to insert checkpoints after every 100 pages to ensure that each 100-page unit is received and acknowledged independently. In this case, if a crash happens during the transmission of page 523, the only pages that need to be resent after system recovery are pages 501 to 523. Pages previous to 501 need not be resent. The following Figure illustrates the relationship of the session layer to the transport and presentation layers



5.1.6 Presentation Layer:

The presentation layer is concerned with the syntax and semantics of the information exchanged between two systems. The following Figure shows the relationship between the presentation layer and the application and session layers.



Specific responsibilities of the presentation layer include the following:

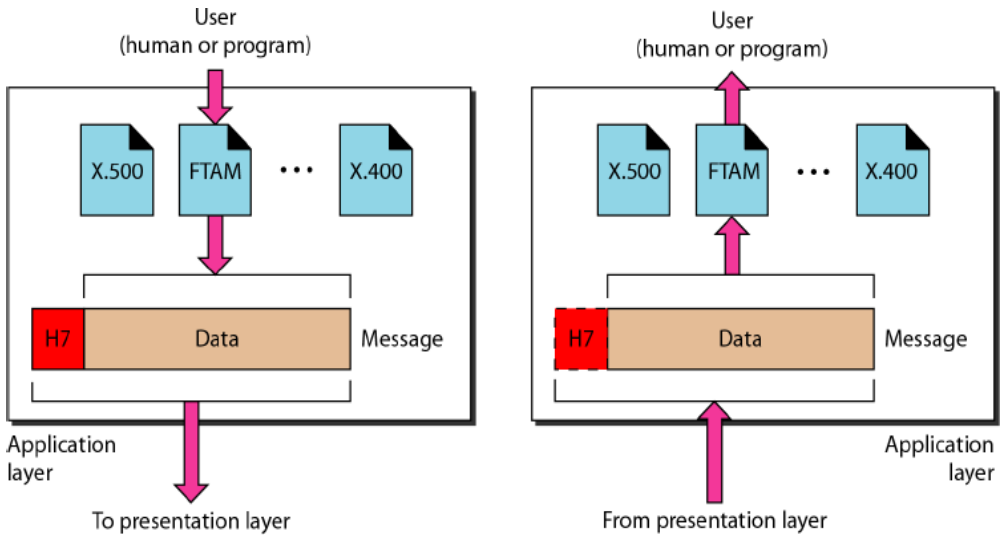
i) **Translation:** The processes (running programs) in two systems are usually exchanging information in the form of character strings, numbers, and so on. The information must be changed to bit streams before being transmitted. Because different computers use different encoding systems, the presentation layer is responsible for interoperability between these different encoding methods. The presentation layer at the sender changes the information from its sender-dependent format into a common format. The presentation layer at the receiving machine changes the common format into its receiver-dependent format.

ii) **Encryption**: To carry sensitive information, a system must be able to ensure privacy. Encryption means that the sender transforms the original information to another form and sends the resulting message out over the network. Decryption reverses the original process to transform the message back to its original form.

iii) **Compression**: Data compression reduces the number of bits contained in the information. Data compression becomes particularly important in the transmission of multimedia such as text, Audio, and video.

5.1.7 Application Layer:

The application layer enables the user, whether human or software, to access the network. It provides user interfaces and support for services such as electronic mail, remote file access and transfer, shared database management, and other types of distributed information services. The following Figure shows the relationship of the application layer to the user and the presentation layer.



Where many application services available, the figure shows only three: XAOO (message-handling services), X.500 (directory services), and file transfer, access, and management (FTAM). The user in this example employs XAOO to send an e-mail message. Specific services provided by the application layer include the following:

i) **Network virtual terminal**: A network virtual terminal is a software version of a physical terminal, and it allows a user to log on to a remote host. To do so, the application creates a software emulation of a terminal at the remote host. The user's computer talks to the software terminal which, in turn, talks to the host, and vice versa. The remote host believes

it is communicating with one of its own terminals and allows the user to log on.

ii) **File transfer, access and management**: This application allows a user to access files in a remote host (to make changes or read data), to retrieve files from a remote computer for use in the local computer, and to manage or control files in a remote computer locally.

iii) **Mail services**: This application provides the basis for e-mail forwarding and storage. Directory services. This application provides distributed database sources and access for global information about various objects and services.

In summary, you learned the;

i) Concepts of Open Systems Interconnection (OSI) Reference Model
ii) Roles of OSI
iii) Functions of each OSI layer
iv) Responsibilities of each OSI layer

Glossary

OSI is a conceptual model that characterizes and standardizes the internal functions of a communication system by partitioning it into abstraction layers.

The physical layer coordinates the functions required to carry a bit stream over a physical medium.

The data link layer is responsible for moving frames from one hop (node) to the next.

The network layer is responsible for the delivery of individual packets from the source host to the destination host possibly across multiple networks (links).

The transport layer is responsible for process-to-process delivery of the entire message.

The session layer is the network dialog controller. It establishes, maintains, and synchronizes the interaction among communicating systems.

The presentation layer is concerned with the syntax and semantics of the information exchanged between two systems.

The application layer enables the user, whether human or software to access the network

Further Reading

Data & Computer networks, Prakash Gupta

William Stallings, Data & Computer networks 10th edition

Any other data communication and networking relevant books, journals, articles e.t.c

TOPIC ACTIVITIES

Activity

Compare the similarities and contrast between TCP/IP model in topic2 and OSI model references.

Tips

Review topic 1 under protocol architecture and related to this topic.

Review

i) Match each of the following functions to the seven layers of the OSI Model.
   a) Physical addressing
   b) Flow control
   c) Inter-host communications
   d) Path determination and logical addressing
   e) Network process to application
   f) Media, signals and binary transmission
   g) Data representation, encryption and decryption

ii) The network layer, or OSI layer 3, provides services to allow end devices to exchange data across the network. To accomplish this end-to-end transport, the network layer uses four basic processes. Briefly describe the purpose of each of these basic processes.
   a) Addressing of end devices,
   b) Encapsulation,
   c) Routing and
   d) De-encapsulation.

TOPIC SIX: PROTOCOLS

Introduction

Welcome to topic one. This topic is aimed at introducing main concepts of protocol, responsibilities of protocol, functions of protocols, ccompare OSI vs. TCP/IP model with respectively protocol and differentiate various types of protocols with their functions.

The topic is, therefore designed to prepare you to have a clear understanding of network security protocols as well.

Topic Time

- Compulsory online reading, activities, self-assessments and practice exercises **[3 hours]**
- Optional further reading **[1.5 hours]**
- Total student input **[4.5 hours]**

Topic Learning Requirements

- Participation in one *chat* (at least 5 entries)
- At least two elaborate contributions to the *discussion* topic. You may also start your own discussion thread.
- Timely submission of the assignments

Learning Outcomes

By the end of this topic you should be able to:

i) Explain the term of protocol
ii) Discuss responsibilities of protocol
iii) Explain functions of protocols
iv) Compare OSI vs. TCP/IP model with respectively protocol
v) Differentiate different protocols
vi) Describe types of protocols
vii) Explain network security protocols

Topic Contents

6.1 Introduction

Protocols are rules or guidelines that regulate the following characteristics of a network: access method, allowed physical topologies, types of cabling and speed of data transfer. Protocols can be implemented either in hardware or software or a mixture of both the lower layers is implemented in hardware, with the higher layers being implemented in software as follows:-

i) Protocols are how computers on a network communicate.
ii) Protocols may determine packet size, information in the headers, and how data is stored in the packet.
iii) Both sides of the conversation must understand these rules for a successful transmission.
iv) Most protocols actually consist of several protocols grouped together in a suite.
v) Protocols are how computers on a network communicate. Rules governing communicate between LAN devices.
vi) Protocols may determine packet size, information in the headers, and how data is stored in the packet.
vii) Both sides of the conversation must understand these rules for a successful transmission.

6.2 Functions of protocols

i) **Data sequencing**. It refers to breaking a long message into smaller packets of fixed size. Data sequencing rules define the method of numbering packets to detect loss or duplication of packets, and to correctly identify packets, which belong to same message.
ii) **Data routing.** Data routing defines the most efficient path between the source and destination.
iii) **Data formatting**. Data formatting rules define which group of bits or characters within packet constitute data, control, addressing, or other information.

iv) **Flow control**. A communication protocol also prevents a fast sender from overwhelming a slow receiver. It ensures resource sharing and protection against traffic congestion by regulating the flow of data on communication lines.

v) **Error control**. These rules are designed to detect errors in messages and to ensure transmission of correct messages. The most common method is to retransmit erroneous message block. In such a case, a block having error is discarded by the receiver and is retransmitted by the sender.

vi) **Precedence and order of transmission**. These rules ensure that all the nodes get a chance to use the communication lines and other resources of the network based on the priorities assigned to them.

vii) **Connection establishment and termination**. These rules define how connections are established, maintained and terminated when two nodes of a network want to communicate with each other.

viii) **Data security**. Providing data security and privacy is also built into most communication software packages. It prevents access of data by unauthorized users.

ix) **Log information**. Several communication software are designed to develop log information, which consists of all jobs and data communications tasks that have taken place. Such information may be used for charging the users of the network based on their usage of the network resources.

6.2.1 Routable Protocols

Many networks today consist of connected LANs. These LANs are often connected using routers. One consideration of connecting LANs is the ability of protocols to work properly across the router to the different networks. A protocol with the ability to communicate across the router is known as a routable protocol. This type of protocol has become increasingly important.

6.2.2 Non-routable Protocols

Some protocols cannot be routed and are limited to smaller LANs. Besides being simpler than routable protocols, non-routable protocols are also usually faster and provide better transfer speeds, due to less overhead.

6.2.3 Connectionless Protocols

Connectionless protocols have no feedback to know whether it arrived safely or not. Connectionless protocols are faster than connection-oriented ones due to less overhead. They are used mainly when there is a need to send data to multiple computers at once when high speed is needed, such as in video or audio.

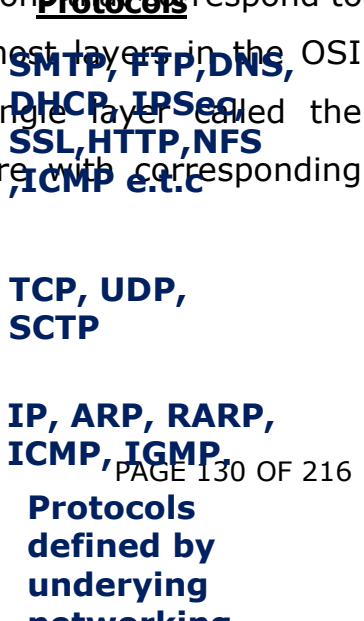
6.2.4 Connection-Oriented Protocols

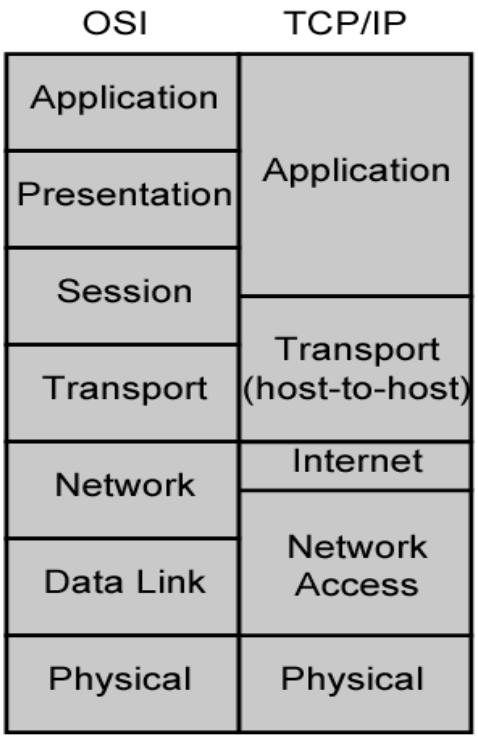
If you need to ensure that certain data arrives at its destination, then a connection oriented protocol can be used. The protocols send acknowledgments to show that data was received successfully.

6.3 TCP/IP Protocol suite

TCPIP is routable, which enables you to connect multiple LANs into one large internetwork. Today it is the main protocol used on the worldwide Internet. TCP/IP has been shown to run over almost any type of network connection from FDDI to radio wave. Almost all devices on a TCP/IP network are considered hosts. TCP/IP Addressing: Every host on a TCP/IP network is given an IP address.

TCP/IP protocol suite is made of five layers: physical, data link, network, transport, and application. The first four layers provide physical standards, network interfaces, internetworking, and transport functions that correspond to the first four layers of the OSI model. The three topmost layers in the OSI model, however, are represented in TCP/IP by a single layer called the application layer which is shown in the following figure with corresponding protocols.





6.3.1 Types of Protocols

i) Network protocols

ii) Transport protocols

iii) Application protocols

6.3.2 Network protocols

Physical/data link Protocols

At the physical and data link layers, TCPIIP does not define any specific protocol. It supports all the standard and proprietary protocols. A network in a TCPI/IP internetwork can be a local-area network or a wide-area network.

6.3.3 Network Layer Protocols

Internetworking Protocol (IP):

(IP) is the transmission mechanism used by the TCP/IP protocols.

It is an unreliable and connectionless protocol-a best-effort delivery service. IP transports data in packets called datagrams, each of which is transported separately. Datagrams can travel along different routes and can arrive out of sequence or be duplicated. Does not keep track of the routes and has no facility for reordering datagrams once they arrive at their destination.IP provides bare-

bones transmission functions that free the user to add only those facilities necessary for a given application and thereby allows for maximum efficiency**.**

Address Resolution Protocol (ARP)

Used to associate a logical address with a physical address. Used to find the physical address of the node when its Internet address is known. Handles the conversion of the address by sending out a discovery packet. To find out the MAC address of a particular IP address. Maintains a list of IP and MAC addresses so a discovery packet is not needed every time communication takes place. ARP is used to find the physical address of the node when its Internet address is known.

Internet Control Message Protocol (ICMP)

Mechanism used by hosts and gateways to send notification of datagram problems back to the sender by sending query and error reporting messages.

The query messages, which occur in pairs, help a host or a network manager get specific information from a router or another host. The error-reporting messages report problems that a router or a host (destination) may encounter when it processes an IP packet.

Internet Group Message Protocol (IGMP)

Used to facilitate the simultaneous transmission of a message to a group of recipients. Gives the multicast routers information about the membership status of hosts (routers) connected to the network as group management protocol. It helps a multicast router create and update a list of loyal members related to each router interface.

6.3.4 Transport protocols

UDP and TCP are transport level protocols responsible for delivery of a message from a process (running program) to another process.

SCTP, has been devised to meet the needs of some newer applications.

User Datagram Protocol (UDP)

The User Datagram Protocol (UDP) is the simpler of the two standard TCP/IP transport protocols. It is a process-to-process protocol that adds only port addresses, checksum error control, and length information to the data from the upper layer.

Transmission Control Protocol:

The Transmission Control Protocol (TCP) provides full transport-layer services to applications. TCP is a reliable stream transport protocol. The term stream, in this context, means connection-oriented: A connection must be established between both ends of a transmission before either can transmit data. At the sending end of each transmission, TCP divides a stream of data into smaller units called segments. Each segment includes a sequence number for reordering after receipt, together with an acknowledgment number for the segments received. Segments are carried across the internet inside of IP datagrams. At the receiving end, TCP collects each datagram as it comes in and reorders the transmission based on sequence numbers.

Services Offered by TCP

TCP Services

i) Provides process-to-process communication using port numbers
ii) TCP allows the sending process to deliver data as a stream of bytes and
iii) Allows the receiving process to obtain data as a stream of bytes
iv) TCP offers full-duplex service, in which data can flow in both directions at the same time.

Connection-Oriented Service

i) The two TCPs establish a connection between them.
ii) Data are exchanged in both directions.
iii) The connection is terminated.
iv) Creates a virtual connection between two TCPs to send data.
v) TCP uses flow and error control mechanisms at the transport level

Reliable Service

i) TCP is a reliable transport protocol

ii) It uses an acknowledgment mechanism to check the safe and sound arrival of data.

TCP/UDP application

- TCP is used in file transfer application between client and server
- UDP provide services to higher layer protocols however multiple higher layer protocols can be multiplexed on to a single UDP layer e.g video streaming application
- UDP no acknowledgement used in audio conferencing

Stream Control Transmission Protocol:

The Stream Control Transmission Protocol (SCTP) provides support for newer applications such as voice over the Internet. It is a transport layer protocol that combines the best features of UDP and TCP. Designed for Internet applications e.g ISDN over IP, telephony signaling, media gateway control, IP telephony. Provides this enhanced performance and reliability. Preserves the message boundaries and at the same time detects lost data, duplicate data, and out-of-order data and has congestion control and flow control mechanisms.

SCTP Services

i) Process-to-Process Communication
   - SCTP uses all well-known ports in the TCP space

ii) Multiple Streams
   - SCTP allows multi-stream service in each connection, which is called association in SCTP terminology

iii) Multi-homing
   - The sending and receiving host can define multiple IP addresses in each end for an association

6.3.5 Application protocols

The application layer in TCP/IP is equivalent to the combined session, presentation, and application layers in the OSI model. Many protocols are defined at this layer some include the following

Simple Mail Transfer Protocol (SMTP)

Simple Mail Transfer Protocol (SMTP) is responsible for making sure that e-mail is delivered. SMTP only handles the delivery of mail to servers and between servers. It does not handle the delivery to the final e-mail client application. Mail transfer is done through message transfer agents (MTA).SMTP simply defines how commands and responses must be sent back and forth.

File Transfer Protocol (FTP)

Mechanism provided by TCP/IP for copying a file from one host to another. Establishes two connections between the hosts. One connection is used for data transfer, the other for control information (commands and responses).

FTP uses the services of TCP. It needs two TCP connections.

i) The well-known port 21 is used for the control connection and

ii) The well-known port 20 for the data connection.

Domain Name System (DNS).

Protocol used to map a name to an IP address or an address to a user friendly name. DNS client program sends a request to a DNS server to map the e-mail address to the corresponding IP address. People prefer to use names instead of numeric addresses.

Name Space

The names assigned to machines must be selected from a name space with complete control over the binding between the names and IP addresses.

Flat Narne Space

A name in this space is a sequence of characters without structure.

Hierarchical Narne Space

Each name is made of several parts. The first part can define the nature of the organization. The second part can define the name of an organization .The third part can define departments in the organization and so on

Simple Network Management Protocol (SNMP).

(SNMP) is a framework for managing devices in an internet using the TCP/IP protocol suite provides a set of fundamental operations for monitoring and maintaining an internet, controls and monitors a set of agents, usually routers SNMP frees management tasks from both the physical characteristics of the managed devices and the underlying networking technology. Used in a heterogeneous internet made of different LANs and WANs connected by routers made by different manufacturers. SNMP uses two other protocols
Structure of Management Information (SMI) and Management Information Base (MIB).

Role of SMI

Defines the general rules for naming objects, defining object types (including range and length), and showing how to encode objects and values

Role of MIB

Creates a collection of named objects, their types, and their relationships to each other in an entity to be managed

Network management protocols are used to

i) Monitoring, testing, configuring, and troubleshooting network components to meet a set of requirements defined by an organization.
ii) Management system protocol is SNMP
iii) Functions performed by a network management system include
    a) Configuration Management,
    b) Fault Management,
    c) Performance Management,
    d) Security Management, And
    e) Accounting Management

Role of SNMP

i) Defines the format of the packet to be sent from a manager to an agent and vice versa.
ii) Interprets the result and creates statistics

iii) It reads and changes the status (values) of objects (variables) in SNMP packets.

Terminal Network (Telnet)

Allows a user to remotely log in to another computer and run applications. User is physically working effectively becomes a dumb terminal — no processing is done on that computer. User wants to access an application program or utility located on a remote machine, she performs remote log-in. TELNET uses only one TCP connection.

Telnet Mode of Operation

Default Mode: User types a character, and the client echoes the character on the screen (or printer) but does not send it until a whole line is completed.

Character mode, each character typed is sent by the client to the server. The server normally echoes the character back to be displayed on the client screen.

Line mode, line editing (echoing, character erasing, line erasing, and so on) is done by the client. The client then sends the whole line to the server.

Dynamic Host Configuration Protocol (DHCP)

DHCP is responsible for providing an IP address from DHCP server offered by Nework operating system. Provide more information when a client host requests an IP address from the DHCP server. Information that a DHCP server can provide to client hosts are

- IP address
- Subnet mask
- DNS server address
- Default gateway

Once network becomes large, keeping up with IP addresses and settings can become an ordeal. (DHCP) takes over the job of assigning addresses and configuring computers on the network. DHCP server is given a range of IP addresses to hand out to network devices. The range of IP addresses must be specified for the network depending on network devices

Network File System (NFS)

NFS is a more advanced protocol used to share files and disk drives than FTP and Telnet. Allows users to connect to network drives and use them as if they were local hard drives.

6.3.6 Network Security Protocols

Secure Sockets Layer (SSL) or Transport Layer Security (TLS).Designed to make use of TCP to provide a reliable end-to-end secure service. Record Protocol provides basic security services to various higher layer protocols defined as part of SSL:

i) The Handshake Protocol,
ii) The Change Cipher Spec Protocol, and
iii) The Alert Protocol

SSL Record Protocol provides two services for SSL connections

i) **Confidentiality:** The Handshake Protocol defines a shared secret key that is used for symmetric encryption of SSL payloads.
ii) **Message integrity**: The Handshake Protocol also defines a shared secret key that is used to form a message authentication code (MAC)

IPV4 and IPV6 Security (IPSec)

Used to secure the network infrastructure from unauthorized monitoring, control of network traffic, secure end user-to-end-user traffic using authentication and encryption mechanisms.

IPSec provides three main facilities:

i) an authentication-only function referred to as Authentication Header (AH),
ii) a combined authentication/encryption function called Encapsulating Security Payload (ESP),
iii) a key exchange function

Applications of IPSec

i) Secure connectivity
ii) Secure remote access

iii) Establishing connectivity

iv) Enhancing electronic security

In summary, you learned the;

i) Main concepts of protocol

i) Responsibilities of protocol

ii) Functions of protocols

iii) Similarities and difference between OSI vs. TCP/IP model with respectively protocol

iv) Different types protocols

v) Network security protocols

Glossary

Protocols are rules or guidelines that regulate the following characteristics of a network: access method, allowed physical topologies, types of cabling and speed of data transfer.

TCP/IP is routable protocol which enables to connect multiple LANs into one large internetwork.

Fiber Distributed Data Interface (FDDI) is a high-performance fibre optic token ring LAN running at 100 Mbps over distances up to 200 km with up to 1000 stations connected

Network Security Protocols: Record protocol provides basic security services to various higher layer protocols.

Further Reading

Data & Computer networks, Prakash Gupta

William Stallings, Data & Computer networks 10th edition

Any other data communication and networking relevant books, journals, articles e.t.c

TOPIC ACTIVITIES

Activity

Read and make brief notes on HTTP and ICMP application protocols.

Tips

Use internet to search HTTP and ICMP application protocols.

Review

i) The Domain Name System (DNS) protocol is chiefly used to translate hostnames into numeric IP addresses. Illustrate how this protocol implements the process.

ii) A local bank just hired you to completely redesign its network. Money is no object but its database transactions are time- critical and PCs throughout the bank must be able to access the databases which are on UNIX systems. Choose and explain the best protocol(s) for this scenario.

iii) Using illustration to show how LAN is connected to internet connectivity labelled all devices and suitable protocol(s).

iv) A switch is a device that allows a LAN to be segmented and operate under the same protocol**.**

   a. State the protocol which a switch uses to achieve the function.
   b. How does a switch implement network security
   c. Which protocol is implemented to achieve network security?

TOPIC SEVEN: MULTIPLEXING

Introduction

Welcome to topic one. This topic is aimed at introducing main concepts of multiplexing, techniques of multiplexing, Frequency-Division Multiplexing, Wavelength-Division Multiplexing and Time-Division Multiplexing

The topic is, therefore designed to prepare you to have a clear understanding multiplexing process, demultiplexing process, interleaving and data rate management.

Topic Time

- Compulsory online reading, activities, self-assessments and practice exercises **[3 hours]**
- Optional further reading **[1.5 hours]**
- Total student input **[4.5 hours]**

Topic Learning Requirements

- Participation in one *chat* (at least 5 entries)
- At least two elaborate contributions to the *discussion* topic. You may also start your own discussion thread.
- Timely submission of the assignments

Learning Outcomes

By the end of this topic you should be able to:

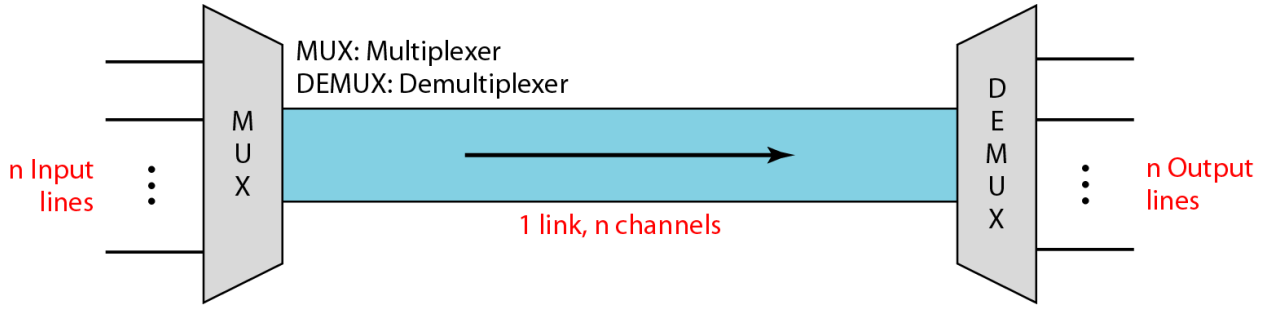
i) Explain the concepts of multiplexing
ii) Differentiate techniques of multiplexing
iii) Describe Frequency-Division Multiplexing
iv) Describe Wavelength-Division Multiplexing
v) Describe Time-Division Multiplexing

Topic Content

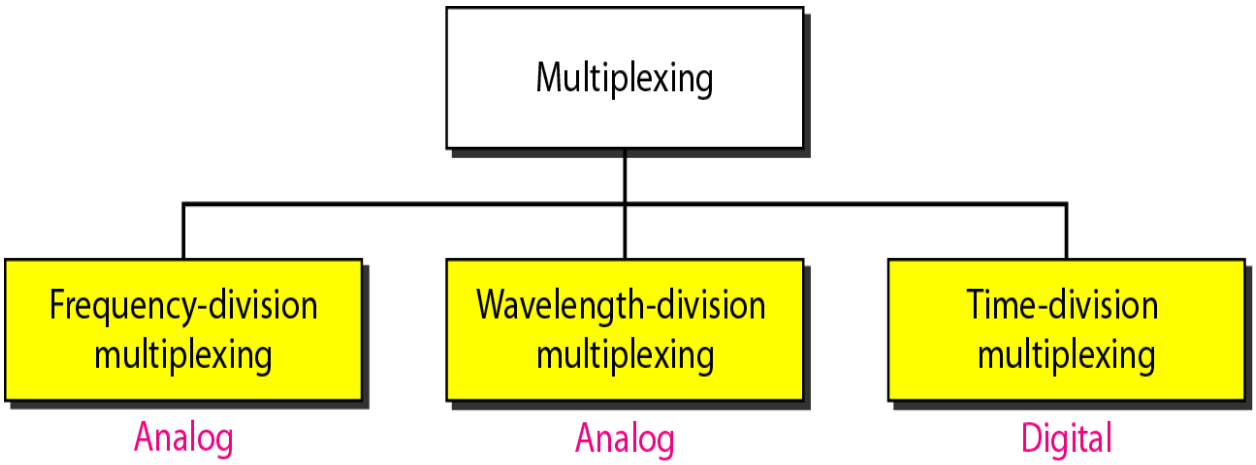
7.1 Introduction

Multiplexing is the set of techniques that allows the simultaneous transmission of multiple signals across a single data link. Whenever the bandwidth of a medium linking two devices is greater than the bandwidth needs of the devices, the link can be shared.

In a multiplexed system, *n* lines share the bandwidth of one link. The following figure shows the basic format of a multiplexed system. The lines on the left direct their transmission streams to a multiplexer (MUX), which combines them into a single stream (many-toone). At the receiving end, that stream is fed into a demultiplexer (DEMUX), which separates the stream back into its component transmissions (one-to-many) and directs them to their corresponding lines.



The following figure shows, the three basic multiplexing techniques: frequency-division multiplexing, wavelength-division multiplexing, and time-division multiplexing. The first two are techniques designed for analog signals, the third, for digital signals.



7.2 Frequency-Division Multiplexing:

Frequency-division multiplexing (FDM) is an analog technique that can be applied when the bandwidth of a link (in hertz) is greater than the combined bandwidths of the signals to be transmitted. In FDM, signals generated by each sending device modulate different carrier frequencies. These modulated signals are then combined into a single composite signal that can be transported by the link. Carrier frequencies are separated by sufficient bandwidth to accommodate the modulated signal. These bandwidth ranges are the channels through which the various signals travel. Channels can be separated by strips of unused bandwidth-guard bands-to prevent signals from overlapping. The following figure gives a conceptual view of FDM. In this illustration, the transmission path

is divided into three parts, each representing a channel that carries one transmission.

7.2.1 Multiplexing Process:

The following figure is a conceptual illustration of the multiplexing process. Each source generates a signal of a similar frequency range. Inside the multiplexer, these similar signals modulate different carrier frequencies (f1, f2 and f3). The resulting modulated signals are then combined into a single composite signal that is sent out over a media link that has enough bandwidth to accommodate it.

7.2.2 Demultiplexing Process*:*

The demultiplexer uses a series of filters to decompose the multiplexed signal into its constituent component signals. The individual signals are then passed to a demodulator that separates them from their carriers and passes them to the output lines.

Applications of FDM:

- To maximize the efficiency of their infrastructure, telephone companies have traditionally multiplexed signals from lower-bandwidth lines onto higher-bandwidth lines.
- A very common application of FDM is AM and FM radio broadcasting.

- The first generation of cellular telephones (still in operation) also uses FDM.

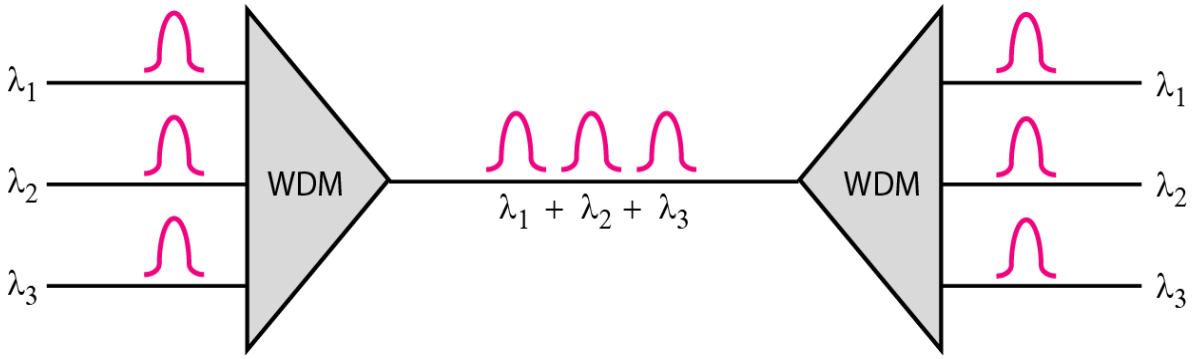
Implementation:

FDM can be implemented very easily. In many cases, such as radio and television broadcasting, there is no need for a physical multiplexer or demultiplexer. As long as the stations agree to send their broadcasts to the air using different carrier frequencies, multiplexing is achieved. In other cases, such as the cellular telephone system, a base station needs to assign a carrier frequency to the telephone user. There is not enough bandwidth in a cell to permanently assign a bandwidth range to every telephone user. When a user hangs up, her or his bandwidth is assigned to another caller.

7.3 Wavelength-Division Multiplexing

Wavelength-division multiplexing (WDM) is designed to use the high-data-rate capability of fiber-optic cable. The optical fiber data rate is higher than the data rate of metallic transmission cable. Using a fiber-optic cable for one single line wastes the available bandwidth. Multiplexing allows us to combine several lines into one.

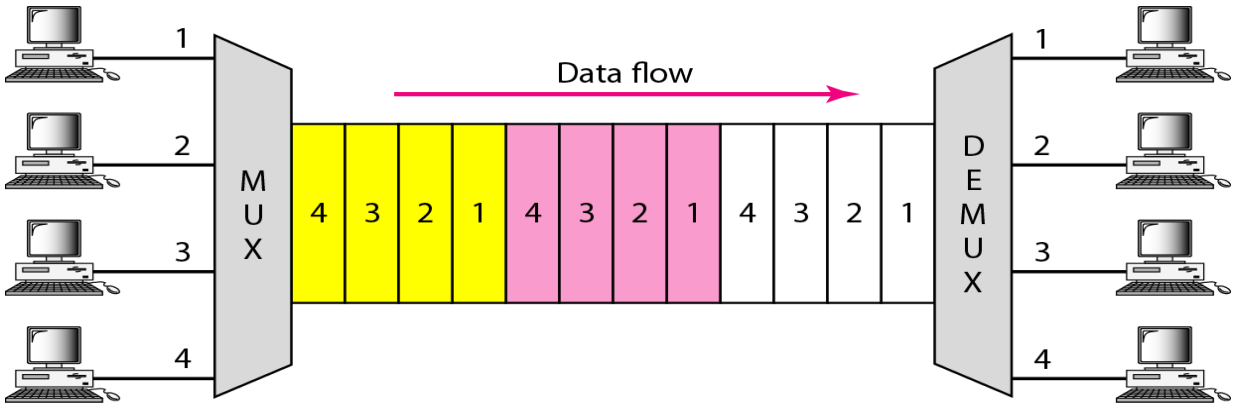
WDM is conceptually the same as FDM, except that the multiplexing and demultiplexing involve optical signals transmitted through fiber-optic channels. The following figure gives a conceptual view of a WDM multiplexer and demultiplexer. Very narrow bands of light from different sources are combined to make a wider band of light. At the receiver, the signals are separated by the demultiplexer.



In this method, we combine multiple light sources into one single light at the multiplexer and do the reverse at the demultiplexer. The combining and splitting of light sources are easily handled by a prism. Recall from basic physics that a prism bends a beam of light based on the angle of incidence and the frequency. Using this technique, a multiplexer can be made to combine several input beams of light, each containing a narrow band of frequencies, into one output beam of a wider band of frequencies. A demultiplexer can also be made to reverse the process.

7.4 Time-Division Multiplexing

Time-division multiplexing (TDM) is a digital process that allows several connections to share the high bandwidth of a link Instead of sharing a portion of the bandwidth as in FDM, time is shared. Each connection occupies a portion of time in the link. The following figure gives a conceptual view of TDM.



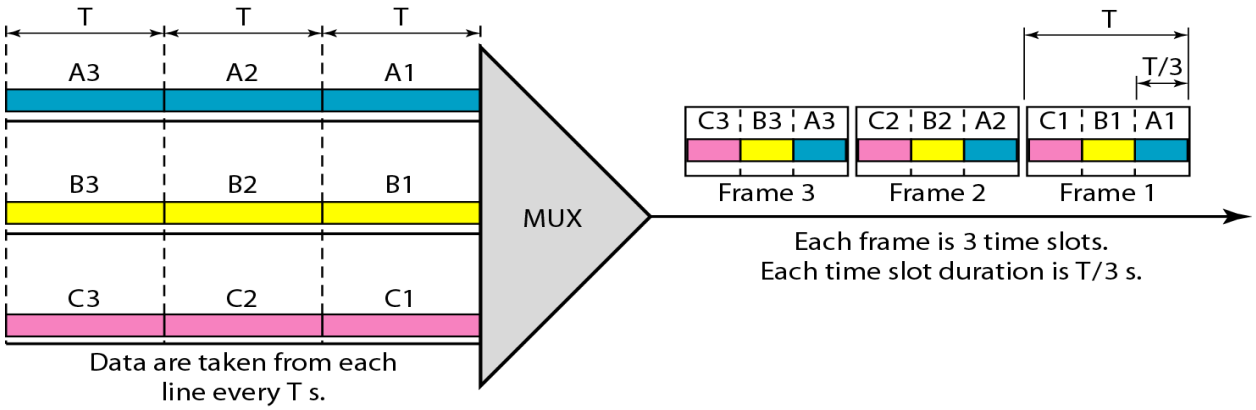
TDM is divided into two different schemes: synchronous and statistical.

a) Synchronous Time-Division Multiplexing:

In synchronous TDM, each input connection has an allotment in the output even if it is not sending data. In synchronous TDM, the data flow of each input connection is divided into units, where each input occupies one input time slot.

A unit can be 1 bit, one character, or one block of data. Each input unit becomes one output unit and occupies one output time slot. However, the duration of an output time slot is n times shorter than the duration of an input time slot. If an input time slot is T s, the output time slot is T/n s, where n is the number of connections. In other words, a unit in the output connection has a shorter

duration; it travels faster. The following figure shows an example of synchronous TDM where n is 3.

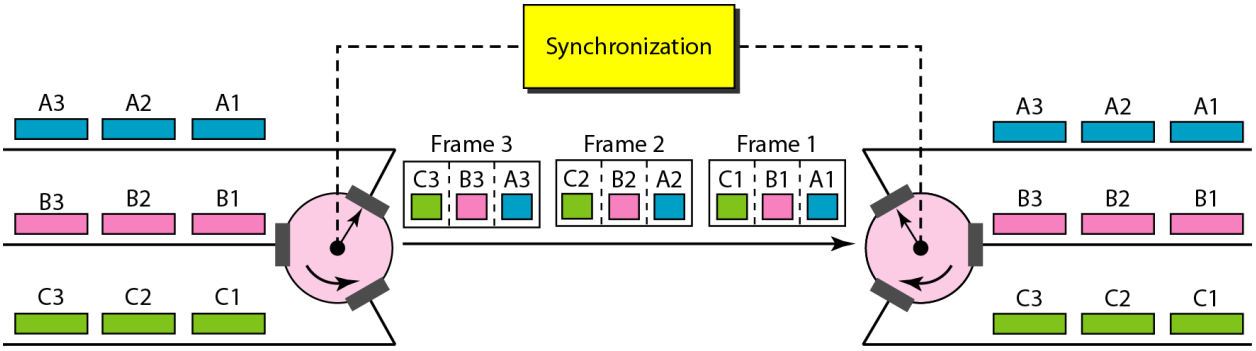


In synchronous TDM, a round of data units from each input connection is collected into a frame. If we have *n* connections, a frame is divided into *n* time slots and one slot is allocated for each unit, one for each input line. If the duration of the input unit is T, the duration of each slot is Tin and the duration of each frame is T.

Time slots are grouped into frames. A frame consists of one complete cycle of time slots, with one slot dedicated to each sending device. In a system with n input lines, each frame has n slots, with each slot allocated to carrying data from a specific input line.

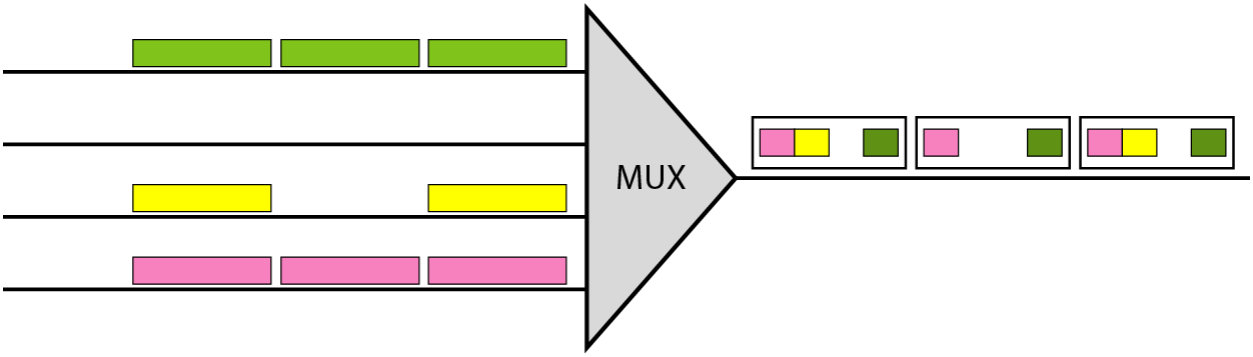
Interleaving

TDM can be visualized as two fast-rotating switches, one on the multiplexing side and the other on the demultiplexing side. The switches are synchronized and rotate at the same speed, but in opposite directions. On the multiplexing side, as the switch opens in front of a connection, that connection has the opportunity to send a unit onto the path. This process is called **interleaving.** On the demultiplexing side, as the switch opens in front of a connection, that connection has the opportunity to receive a unit from the path. The following figure shows the interleaving process.



Empty Slots

Synchronous TDM is not as efficient as it could be. If a source does not have data to send, the corresponding slot in the output frame is empty. The following figure shows a case in which one of the input lines has no data to send and one slot in another input line has discontinuous data.

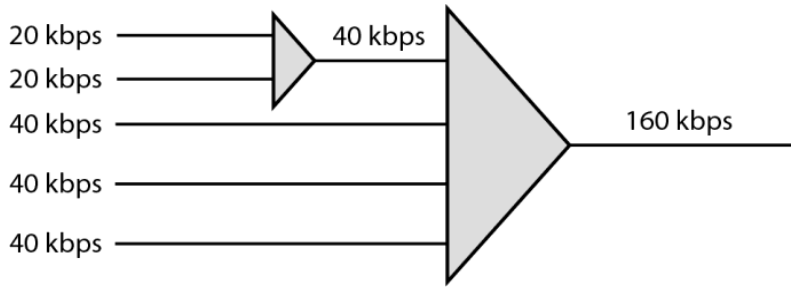


The first output frame has three slots filled, the second frame has two slots filled, and the third frame has three slots filled. No frame is full.

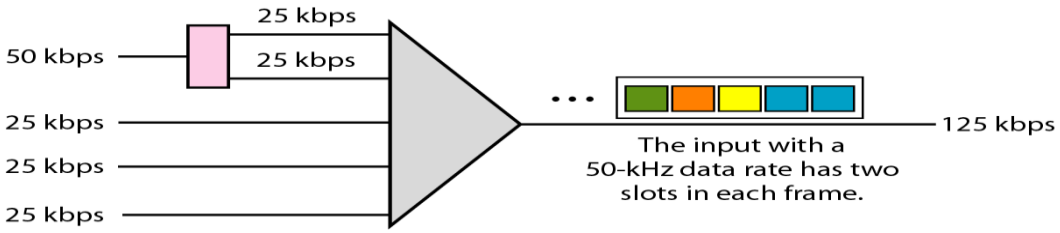
7.4.1 Data Rate Management

One problem with TDM is how to handle a disparity in the input data rates. If data rates are not the same, three strategies, or a combination of them, can be used. The three different strategies are **multilevel multiplexing, multiple-slot allocation,** and **pulse stuffing.**

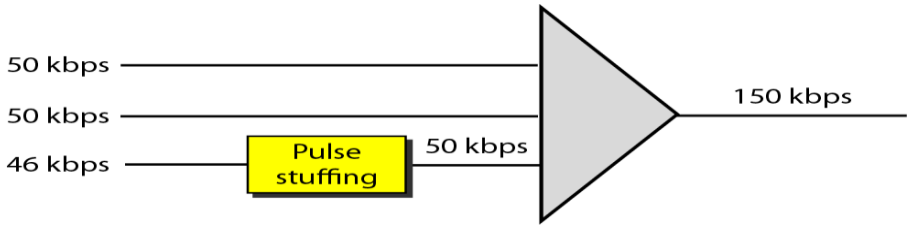
i) **Multilevel Multiplexing:** Multilevel multiplexing is a technique used when the data rate of an input line is a multiple of others. For example, in the following figure, we have two inputs of 20 kbps and three inputs of 40 kbps. The first two input lines can be multiplexed together to provide a data rate equal to the last three. A second level of multiplexing can create an output of 160 kbps.



ii) **Multiple-Slot Allocation:** Sometimes it is more efficient to allot more than one slot in a frame to a single input line. For example, we might have an input line that has a data rate that is a multiple of another input. In the following figure, the input line with a SO-kbps data rate can be given two slots in the output. We insert a serial-to-parallel converter in the line to make two inputs out of one.



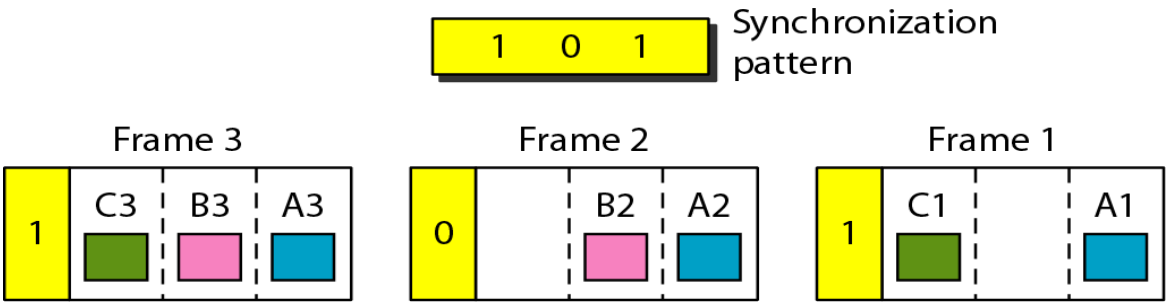
iii) **Pulse Stuffing**: Sometimes the bit rates of sources are not multiple integers of each other. Therefore, neither of the above two techniques can be applied. One solution is to make the highest input data rate the dominant data rate and then add dummy bits to the input lines with lower rates. This will increase their rates. This technique is called pulse stuffing, bit padding, or bit stuffing as shown in the following figure. The input with a data rate of 46 is pulse-stuffed to increase the rate to 50 kbps. Now multiplexing can take place.



7.4.2 Frame Synchronizing

The implementation of TDM is not as simple as that of FDM. Synchronization between the multiplexer and demultiplexer is a major issue. If the, multiplexer and the demultiplexer are not synchronized, a bit belonging to one channel may be received by the wrong channel.

For this reason, one or more synchronization bits are usually added to the beginning of each frame. These bits, called framing bits, follow a pattern, frame to frame, that allows the demultiplexer to synchronize with the incoming stream so that it can separate the time slots accurately. In most cases, this synchronization information consists of 1 bit per frame, alternating between 0 and I, as shown in the following figure.

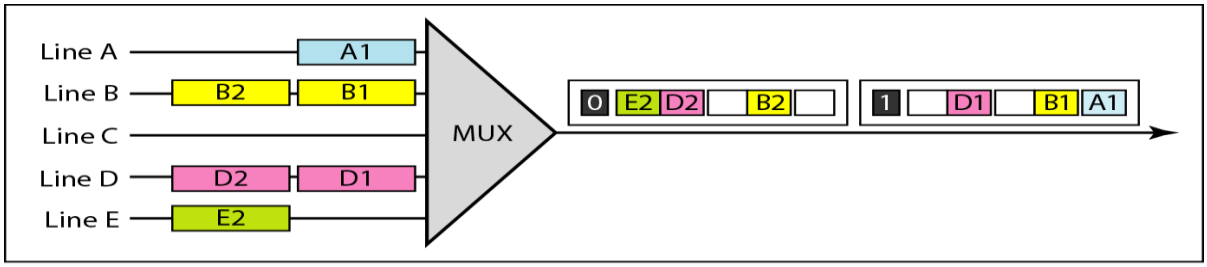


b) Statistical Time-Division Multiplexing:

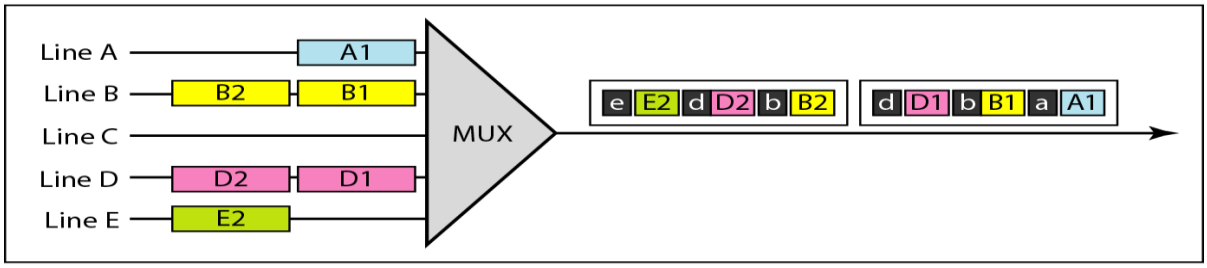
Statistical TDM improve the efficiency by removing the empty slots from the frame. In synchronous TDM, each input has a reserved slot in the output frame. This can be inefficient if some input lines have no data to send. In statistical time-division multiplexing, slots are dynamically allocated to improve bandwidth efficiency. Only when an input line has a slot's worth of data to send is it given a slot in the output frame. In statistical multiplexing, the number of slots in each frame is less than the number of input lines. The multiplexer checks each input line in round robin fashion. It allocates a slot for an input line if the line has data to send otherwise it skips the line and checks the next line.

The following figure shows a synchronous and a statistical TDM example. In the former, some slots are empty because the corresponding line does not have

data to send. In the latter, however, no slot is left empty as long as there are data to be sent by any input line.



a. Synchronous TDM



b. Statistical TDM

Addressing

The above figure also shows a major difference between slots in synchronous TDM and statistical TDM. An output slot in synchronous TDM is totally occupied by data, in statistical TDM; a slot needs to carry data as well as the address of the destination.

In synchronous TDM, there is no need for addressing. Synchronization and reassigned relationships between the inputs and outputs serve as an address. We know, for example, that input 1 always goes to input 1. If the multiplexer and the demultiplexer are synchronized, this is guaranteed. In statistical multiplexing, there is no fixed relationship between the inputs and outputs because there are no pre-assigned or reserved slots. We need to include the address of the receiver inside each slot to show where it is to be delivered.

The addressing in its simplest form can be *n* bits to define *N* different output lines with $n = \log_2 n$. For example, for eight different output lines, we need a 3-bit address.

Slot Size

Since a slot carries both data and an address in statistical TDM, the ratio of the data size to address size must be reasonable to make transmission efficient. For example, it would be inefficient to send 1 bit per slot as data when the address is 3 bits. This would mean an overhead of 300 percent. In statistical TDM, a block of data is usually many bytes while the address is just a few bytes.

No Synchronization Bit

There is another difference between synchronous and statistical TDM, but this time it is at the frame level. The frames in statistical TDM need not be synchronized, so we do not need synchronization bits.

Bandwidth

In statistical TDM, the capacity of the link is normally less than the sum of the capacities of each channel. The designers of statistical TDM define the capacity of the link based on the statistics of the load for each channel. If on average only x percent of the input slots are filled, the capacity of the link reflects this. Of course, during peak times, some slots need to wait.

Glossary

Protocols are rules or guidelines that regulate the following characteristics of a network: access method, allowed physical topologies, types of cabling and speed of data transfer.

TCP/IP is routable protocol which enables to connect multiple LANs into one large internetwork.

Fiber Distributed Data Interface (FDDI) is a high-performance fibre optic token ring LAN running at 100 Mbps over distances up to 200 km with up to 1000 stations connected

Network Security Protocols: Record protocol provides basic security services to various higher layer protocols.

In summary, you learned the;

i) The concepts of multiplexing
ii) Different techniques of multiplexing
iii) Multiplexing and demultiplexing process

iv) Frequency-Division Multiplexing

v) Wavelength-Division Multiplexing

vi) Time-Division Multiplexing

vii) Data management rate and concept of interleaving.

Further Reading

Data & Computer networks, Prakash Gupta

William Stallings, Data & Computer networks 10th edition

Any other data communication and networking relevant books, journals, articles e.t.c

TOPIC ACTIVITIES

Activity

Use the concepts of multiplexing you have learnt figure out which types of multiplexing does mobile telecommucation implement in achieve it main application such as calls, SMS, video streaming, e-mail, what-up, Facebook, twitter e.t.c

Tips

Refer to these multiplexing terms and apply to figure out how to apply in the topic activity:-

a) Frame synchronizing,

b) Addressing,

c) Interleaving and

d) Bandwidth

Review

a) Whenever the bandwidth of a medium linking two devices is greater than the bandwidth needs of the devices, the link can be shared. One approach used is multiplexing.

   i) Describe one goal of multiplexing

   ii) List three main multiplexing techniques

iii) Which of the three multiplexing techniques is (are) used to combine digital signals?

iv) Which of the three multiplexing techniques is common for fiber optic links? Explain the reason**.**

b) Distinguish between multilevel, multiple slot and pulse-stuffed time division multiplexing.

c) In synchronous time division multiplexing, it is possible to interleave bits, one bit from each channel participating in a cycle. If the channel is using a self-clocking code to assist synchronization, might this bit interleaving introduce problems because there is no continuous stream of bits from one source? Discuss briefly

d) Compare statistical and synchronous time division multiplexing using illustration with four inputs.

e) Why is it that the start and stop bits can be eliminated when character interleaving is used in synchronous Time Division Multiplexing (TDM)?

f) Briefly explain how wavelength division multiplexing (WDM) is able to increase the amount of data that can be transmitted along a single fibre optic cable. .

g) Explain in terms of data link control and physical layer concepts how error and flow control are accomplished in synchronous time division multiplexing.

TOPIC EIGHT: NETWORK ARCHITECTURE

Introduction

Welcome to topic eight. This topic is aimed at introducing main concepts of layering of networks as discuss in topic two and five**,** network technologies, network design and network topologies

The topic is, therefore designed to prepare you to have a clear understanding network control access method

Topic Time

- Compulsory online reading, activities, self-assessments and practice exercises **[3 hours]**
- Optional further reading **[1.5 hours]**
- Total student input **[4.5 hours]**

Topic Learning Requirements

- Participation in one *chat* (at least 5 entries)
- At least two elaborate contributions to the *discussion* topic. You may also start your own discussion thread.
- Timely submission of the assignments

Learning Outcomes

By the end of this topic you should be able to:

i) Explain the roles of layering a networks
ii) Discuss existing network technologies
iii) Describe Hierarchical LAN design and converged network
iv) Describe common network topologies
v) Discuss network control access methods

8.1 Introduction

Network architecture is global view of network that describes how various operation are organised in network and data communication. It address the following:-

vi) Layering of networks
- OSI and TCP/IP models

vii) Network technologies
- ISDN, ATM, Ethernet, FDDI, Token ring, SONET, HIPPI e.tc,

viii) Network design
- Hierarchical design and converged network

ix) Network topologies
- Bus, star, ring, mesh and Hybrid.

x) Network control access method.
- Contention methods, token passing, demand priority, polling ad Network switching

xi) Network security
- Security basic concepts, types of threats, security mechanisms, secure channels, security services, message integrity and confidentiality secure channels and access control.

Digital data communication are used in packet switched networks used to transmit data or send data across WAN at

i) High speed,
ii) Convenient and
iii) Reliable
iv) Using different possible paths to package and route data.

8.2 Network Architecture Technologies

The most popular network architecture technologies include

8.2.1 Integrated Services for Digital Network (ISDN)

ISDN is a set of communication standards for simultaneous digital transmission of multimedia and other network services over the public switched telephone network (PSTN).

ISDN elements

i) With ISDN you can have a digital telephone line and a 64 Kbps data line, or one 128 Kbps data line.
ii) 2B (Basic User) Channels – 64Kbps each – digital data and voice
iii) 1D (Data Traffic) Channel – 16Kbps – signalling information for B channels
iv) H (High Speed) Channel – 348Kbps (H0), 1.536Mbps (H11), 1.92Mbps (H12) – high speed apps, fax, video e.t.c

ISDN Services

There are two main ISDN services

i) **The basic rate interface (BRI)** is the service for homes and small businesses. The entry level interface to ISDN is the Basic(s) Rate Interface (BRI), a 128 Kbit/s service delivered over a pair of standard telephone copper wires. The 144 Kbit/s payload rate is broken down into two 64 Kbit/s bearer channels ('B' channels) and one 16 Kbit/s signaling channel ('D' channel or data channel). This is sometimes referred to as 2B+D
ii) **The primary rate interface (PRI)** is the service for larger businesses. The other ISDN access available is the Primary Rate Interface (PRI), which is carried over a T1 (2048 Kbit/s). A T1 is 23 'B' channels of 64 Kbit/s, one 'D' channel of 64 kbit/s and a timing and alarm channel of 64 Kbit/s. used to carry digital data in full duplex mode at rate of 1.544Mbps. A computer connected to a ISDN services can both use B channels together for a combined 128Kbps data stream. If both end stations support compression, much high throughput can be achieved This is sometimes referred to as 23B+D

Example

Compute the full capacity of the following ISDN service types

i) BRI= 2B+D

*= 2*64 + 16 =144Kbps*

ii) PRI=23B+D

= 23*64 +64 =1.54Kbps

iii) What are D and B channels

B= Voice, data, video break down into payload

D= channels use for network management, call setup used to carry tear down data

iv) Which one is equivalent to T1 circuit line? Explain

PRI= 23*B+D

PRI = 23*64 + 64 = 1.536Mbps = 1.544Mbps.

Explanation

1.544 Mbps @ 24 channels each 64Mbps

8.2.2 Asynchrones Transfer Mode (ATM)

ATM is the leased service that can provide a high-speed connection for data transfer between two points either locally or over long distances. Both send packets of data over high speed lines ad require a user to create a circuit with a provider. It is capable of speeds up to 622 Mbps. Data travels over a connection called a virtual channel connection (VCC). VCC is connection between two endpoints. To better manage VCCs, a VCC must travel over a virtual path connection (VPC). One of ATM's strengths (besides its high speeds) is its ability to offer various classes of service.

Types of ATM Bit Rate

i) If a company requires a high-speed, continuous connection, they might consider a **constant bit rate service.**

ii) A less demanding service is **variable bit rate (VBR).** VBR can also support real time applications, as well as non-real time applications, but do not demand a constant bit stream.

iii) **Available bit rate (ABR)** is used for bursty traffic that does not need to be transmitted immediately. ABR traffic may be held up until a transmission opening is available.

iv) **Unspecified bit rate (UBR)** is for lower rate traffic that may get held up, and may even be discarded part way through transmission if congestion occurs.

Advantages and Disadvantages of ATM

- Advantages of ATM include very high speeds and the different classes of service.
- Disadvantages include potentially high costs (both equipment and support) and a high level of complexity.

8.2. 3: Ethernet standards

Ethernet is the most widely-installed local area network (LAN) technology. Specified in a standard, IEEE 802.3 project specification. The standards comprise several wiring and signaling variants of the OSI model. It provides services up to and including the data link layer. An Ethernet LAN typically uses coaxial cable or special grades of twisted pair wires. Ethernet is also used in wireless LANs. An Ethernet LAN typically uses coaxial cable or special grades of twisted pair wires. Ethernet is also used in wireless LANs. The most commonly installed Ethernet systems are called 10BASET and provide transmission speeds up to 10 Mbps. Devices are connected to the cable and compete for access using a Carrier Sense Multiple Access with Collision Detection (CSMA/CD) protocol. Fast Ethernet or 100BASE-T provides transmission speeds up to 100 megabits per second and is typically used for LAN backbone systems, supporting workstations with 10BASET cards. Gigabit Ethernet provides an even higher level of backbone support at 1000 megabits per second (1 gigabit or 1 billion bits per second). 10-Gigabit Ethernet provides up to 10 billion bits per second.

10BASE-T

This designation is an Institute of Electrical and Electronics Engineers (IEEE) shorthand identifier. The "10" in the media type designation refers to the transmission speed of 10 Mbps. The "BASE" refers to baseband signaling, which means that only Ethernet signals are carried on the medium. The "T" represents twisted-pair; the "F" represents fiber optic cable; and the "2", "5", and "36" refer to the coaxial cable segment length (the 185 meter length has been rounded up to "2" for 200). 10BASE-T, one of several physical media specified in the IEEE 802.3 standard for Ethernet local area networks (LANs), is ordinary telephone twisted pair wire. 10BASE-T supports Ethernet's 10 Mbps transmission speed. In addition to 10BASE-T, 10 megabit Ethernet can be implemented with these media types:

i) 10BASE-2 (Thinwire coaxial cable with a maximum segment length of 185 meters)
ii) 10BASE-5 (Thickwire coaxial cable with a maximum segment length of 500 meters)
iii) 10BASE-F (optical fiber cable)
iv) 10BASE-36 (broadband coaxial cable carrying multiple baseband channels for a maximum length of 3,600 meters)
v) 10GB- transmit at 10gabit per second speed at long distance miles way e.g optical fiber cable

8.2.4 Token Ring

Ring topology: every node has exactly two branches connected to it (a succession of point-to-point links). Stations are connected using interfaces (repeaters). Ex: Token Ring LAN. Repeaters joined by point to point links in closed loop. Receive data on one link and retransmit on another and links unidirectional. Data in frames circulate past all stations, destination recognizes address and copies frame. Frame circulates back to source where it is removed. Media access control determines when station can insert frame. Dual ring allows for a second (reserve) ring; data flow has here an opposite direction; not all

stations linked to both rings. The dual ring topology uses a second (auxiliary) ring which operates in the reverse direction compared with the main ring. The second ring is for emergencies only

8.2.5 Fiber distributed data interface (FDDI)

FDDI is a high-performance fiber optic token ring LAN running at 100 Mbps over distances up to 200 km with up to 1000 stations connected. FDDI is used as backbone to connect copper LANs using repeater device to connect many link. It also used token passing access control method to share a common link generated by special token protocol 802.5. FDDI uses a multimode fiber. The FDDI cabling consists of two fiber rings, one transmitting clockwise and the other transmitting counter clockwise. If either one breaks the other If both links break at same time they can be joined to form a new approximately twice as long. This new ring is formed by relays at the two nodes adjoining the broken link. The basic FDDI protocols are modeled on protocol 802.5.The station must first capture a token, transmit a frame and remove it when it comes around. In FDDI the time spent in waiting for a frame to circumnavigate is reduced by allowing the station to put a new token back onto the ring as soon as it has finished transmitting its frames. In a large ring, several frames may be on the ring at the same time.

8.3 LAN design

A properly Network architecture is a fundamental requirement for any organization well designed LAN is and be able to select appropriate devices to support the network specifications of a small- or medium-sized business.

8.3.1 Switched LAN Architecture

Compared to other network designs, a hierarchical network is easier to manage and expand, and problems are solved more quickly. Hierarchical network design involves dividing the network into discrete layers. Each layer provides specific functions that define its role within the overall network. By separating the various functions that exist on a network, the network design becomes modular, which facilitates scalability and performance.

The typical hierarchical design model is broken into three layers:

i) Access
ii) Distribution
iii) Core

8.3.2 Access Layer

The access layer interfaces with end devices, such as PCs, printers, and IP phones, to provide access to the rest of the network. The access layer can include routers, switches, bridges, hubs, and wireless access points. The main purpose of the access layer is to provide a means of connecting devices to the network and controlling which devices are allowed to communicate on the network.

8.3.3 Distribution Layer

The distribution layer aggregates the data received from the access layer switches before it is transmitted to the core layer for routing to its final destination. The distribution layer controls the flow of network traffic using policies and delineates broadcast domains by performing routing functions between virtual LANs (VLANs) defined at the access layer. VLANs allow you to segment the traffic on a switch into separate sub-networks. For example, in a university you might separate traffic according to faculty, students, and guests. Distribution layer switches are typically high-performance devices that have high availability and redundancy to ensure reliability.

8.3.4 Core Layer

The core layer of the hierarchical design is the high-speed backbone of the internetwork. The core layer is critical for interconnectivity between distribution layer devices, so it is important for the core to be highly available and redundant. The core area can also connect to Internet resources. The core aggregates the traffic from all the distribution layer devices, so it must be capable of forwarding large amounts of data quickly. E.g. routers

Benefits of a Hierarchical Network

i) **Scalability:** Hierarchical networks scale very well. The modularity of the design allows you to replicate design elements as the network grows. Because each instance of the module is consistent, expansion is easy to plan and implement.

ii) **Redundancy**: As a network grows, availability becomes more important. You can dramatically increase availability through easy redundant implementations with hierarchical networks. Access layer switches are connected to two different distribution layer switches to ensure path redundancy. If one of the distribution layer switches fails, the access layer switch can switch to the other distribution layer switch. If an access layer switch fails, just the devices connected to that one switch would be affected by the outage. The rest of the network would continue to function unaffected.

iii) **Performance**: Communication performance is enhanced by avoiding the transmission of data through low performing, intermediary switches. Data is sent through aggregated switch port links from the access layer to the distribution layer at near wire speed in most cases. The distribution layer then uses its high-performance switching capabilities to forward the traffic up to the core, where it is routed to its final destination. Because the core and distribution layers perform their operations at very high speeds, no contention for network bandwidth occurs. As a result, properly designed hierarchical networks can achieve near wire speed between all devices.

iv) **Security**: Security is improved and easier to manage. Access layer switches can be configured with various port security options that provide control over which devices are allowed to connect to the network. You also have the flexibility to use more advanced security policies at the distribution layer. You may apply access control policies that define which communication protocols are deployed on your network and where they

are permitted to go. Data security has two elements and two models. Data security elements

a. Ensuring that the data is safe from intruders
b. . Ensuring that you can replace destroyed data

Security models

1. Physical model
2. Software model

i) **Physical models** involve keeping intruders way form network devices and transmission media. i.e cables cannot be trap, isolation, devices access e.t.c

ii) **Software models** involves shared oriented and user oriented security Share oriented security the security information is attached to the object and apples to everyone who might access that object User oriented security focuses on the right and permission of each user. A table attached to every object lists who can do what the object permits and keep track of every user. E.g WIN XP and WIN 2000/2003/2007 server security models

v) **Manageability**: Manageability is relatively simple on a hierarchical network. Each layer of the hierarchical design performs specific functions that are consistent throughout that layer. Therefore, if the need to change the functionality of an access layer switch, you could repeat that change across all access layer switches in the network because they presumably perform the same functions at their layer. Deployment of new switches is also simplified because switch configurations can be copied between devices with very few modifications. Consistency between the switches at each layer allows for rapid recovery and simplified troubleshooting. In some special situations, configuration inconsistencies could exist between devices, so you should ensure that configurations are well documented so that you can compare them before deployment.

vi) **Maintainability**: Hierarchical networks are modular in nature and scale very easily, they are easy to maintain. With other network topology designs, maintainability becomes increasingly complicated as the network grows. Also, in some network design models, there is a finite limit to how large the network can grow before it becomes too complicated and expensive to maintain. In the hierarchical design model, switch functions are defined at each layer, making the selection of the correct switch easier. Adding switches to one layer does not necessarily mean there will not be a bottleneck or other limitation at another layer. For a full mesh network topology to achieve maximum performance, all switches need to be high-performance switches because each switch needs to be capable of performing all the functions on the network. In the hierarchical model, switch functions are different at each layer.

8.3.5 Principles of Hierarchical LAN Design

i) **Network Diameter:** When designing a hierarchical network topology, the first thing to consider is network diameter, Network diameter is the number of devices that a packet has to cross before it reaches its destination. Keeping the network diameter low ensures low and predictable latency between devices.

ii) **Bandwidth Aggregation**: Each layer in the hierarchical network model is a possible candidate for bandwidth aggregation. Bandwidth aggregation is the combining of two or more connections to create a logically singular higher bandwidth connection. After bandwidth requirements of the network are known, links between specific switches can be aggregated, which is called link aggregation. Link aggregation allows multiple switch port links to be combined so as to achieve higher throughput between switches.

iii) **Redundancy**: Redundancy is one part of creating a highly available network. Redundancy can be provided in a number of ways .This protects network if one of the distribution switches fails. In case of a failure, the

access layer switch adjusts its transmission path and forwards the traffic through the other distribution switch.

8.4 Converged Network

Convergence is the process of combining voice and video communications on a data network. Converged networks have existed for a while now, but were feasible only in large enterprise organizations because of the network infrastructure requirements and complex management that was involved to make them work seamlessly. High network costs were associated with convergence because more expensive switch hardware was required to support the additional bandwidth requirements. Converged networks also required extensive management in relation to quality of service (QoS), because voice and video data traffic needed to be classified and prioritized on the network.

Benefit of a Converged Network

i) In converged network is that there is just one network to manage. With separate voice, video, and data networks, changes to the network have to be coordinated across networks. 2.

ii) Lower implementation and management costs. It is less expensive to implement a single network infrastructure than three distinct network infrastructures. Managing a single network is also less expensive.

8.5 Considerations of LAN Design

i) **Traffic Flow Analysis:** It is the process of measuring the bandwidth usage on a network and analyzing the data for the purpose of performance tuning, capacity planning, and making hardware improvement decisions

ii) **Analysis Tools**: Many traffic flow analysis tools that automatically record traffic flow data to a database and perform a trend analysis are available. In large networks, software collection solutions are the only effective method for performing traffic flow analysis.

iii) **User Community**: Analysis User community analysis is the process of identifying various groupings of users and their impact on network

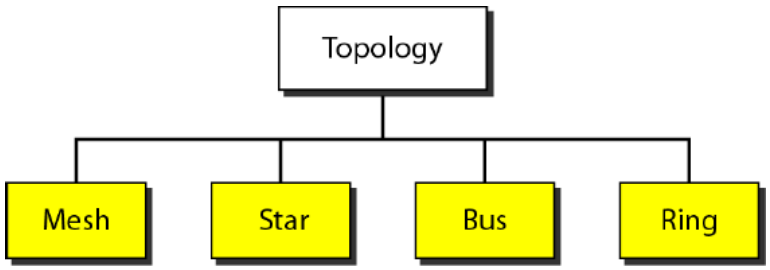
performance. The way users are grouped affects issues related to port density and traffic flow, which, in turn, influence the selection of network switches.

iv) **Data Stores and Data Servers Analysis**: When analyzing traffic on a network, consider where the data stores and servers are located so that you can determine the impact of traffic on the network. Data stores can be servers, storage area networks (SANs), network-attached storage (NAS), tape backup units, or any other device or component where large quantities of data are stored.

v) **Topology Diagrams**: A topology diagram is a graphical representation of a network infrastructure. A topology diagram shows how all switches are interconnected, detailed down to which switch port Interconnects the devices

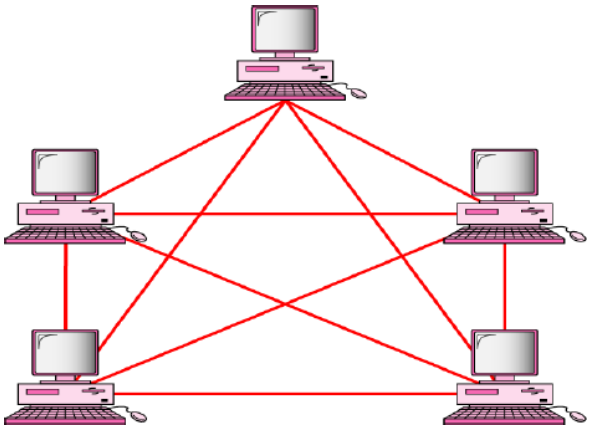
8.6 Network topologies

The term physical topology 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 the links and linking devices (usually called nodes) to one another. There are four basic topologies possible: mesh, star, bus, and ring which are shown in the following figure.



8.6.1 Mesh Topology:

In a mesh topology, every device has a dedicated point-to-point link to every other device. The dedicated link carries traffic only between the two devices it connects. The number of physical links needed in a fully connected mesh network with n nodes are, n(n - 1). However, if each physical link allows communication in both directions (duplex mode), we can divide the number of links by 2. In other words, we can say that in a mesh topology, we need n(n - 1) /2 duplex-mode links. To accommodate that many links, every device on the network must have n – 1 input/output (I/O) ports to be connected to the other n - 1 stations which are shown in the following figure:



Advantages:

The different advantages of Mesh topology are as follows:

i) The dedicated links guarantees that each connection can carry its own data load, thus eliminating the traffic problems that can occur when links must be shared by multiple devices.

ii) A mesh topology is robust. If one link becomes unusable, it does not incapacitate the entire system.

iii) Another advantage of Mesh topology is advantage of privacy or security. When every message travels along a dedicated line, only the intended recipient sees it. Physical boundaries prevent other users from gaining access to messages.

iv) Point-to-point links make fault identification and fault isolation easy. Traffic can be routed to avoid links with suspected problems. This helps to discover the precise location of the fault and aids in finding its cause and solution**.**

Disadvantages: The disadvantages are as follows.

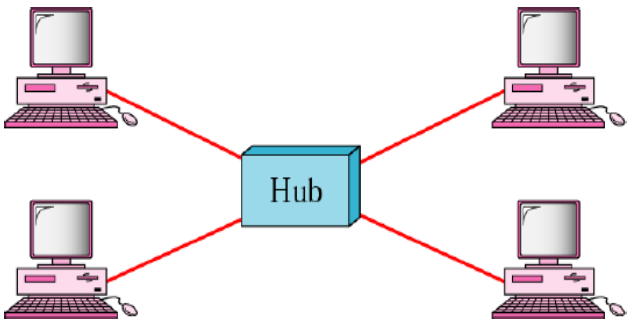
i) Every device must be connected to every other device. So large amount of cabling and the number of I/O ports are required. So, the installation and reconnection are difficult.

ii) The sheer bulk of the wiring can be greater than the available space (in walls, ceilings, or floors) can accommodate.

iii) The hardware required to connect each link (I/O ports and cable) can be prohibitively expensive.

8.6.2 Star Topology:

In a star topology, 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 as shown in the following Figure.



Advantages:

i) A star topology is less expensive than a mesh topology. In a star, each device needs only one link and one I/O port to connect it to any number of others.

ii) A star topology is robust. Robustness. If one link fails, only that link is affected. All other links remain active. This factor also lends itself to easy fault identification and fault isolation.

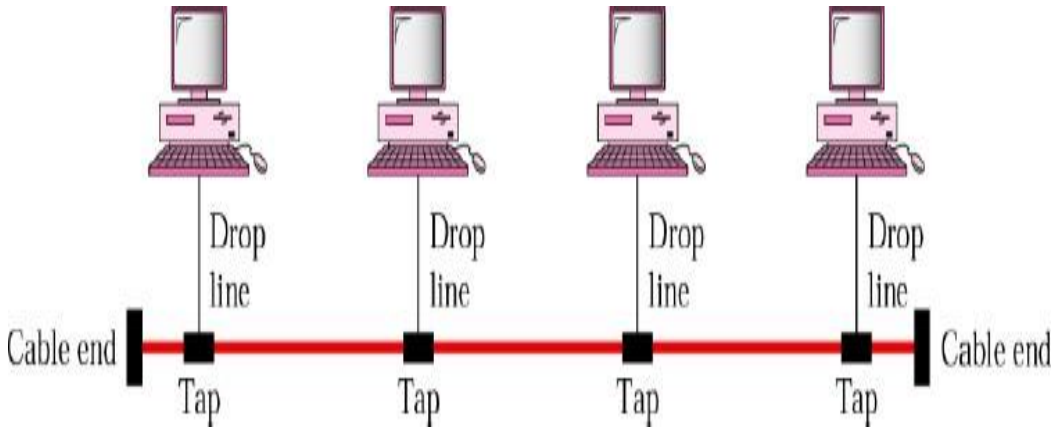
Disadvantages:

i) One big disadvantage of a star topology is the dependency of the whole topology on one single point, the hub. If the hub goes down, the whole system is dead.

ii) Although a star requires far less cable than a mesh, each node must be linked to a central hub. For this reason, often more cabling is required in a star than in some other topologies (such as ring or bus).

8.6.3 Bus Topology:

The preceding examples all describe point-to-point connections. A bus topology, on the other hand, is multipoint. One long cable acts as a backbone to link all the devices in a network which is shown in the following figure.



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.

Advantages:

i) The main advantages of a bus topology is ease of installation. Backbone cable can be laid along the most efficient path, then connected to the nodes by drop lines of various lengths.

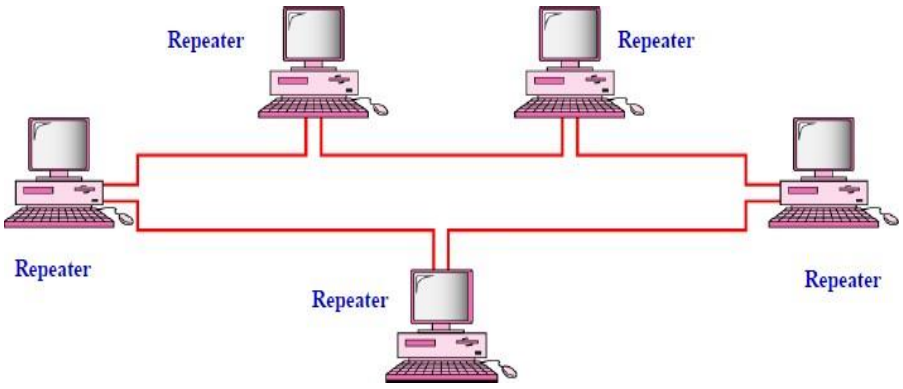
Disadvantages:

i) The disadvantage of bus topology is difficult reconnection and fault isolation. A bus is usually designed to be optimally efficient at installation. It can therefore be difficult to add new devices. Signal reflection at the taps can cause degradation in quality.

ii) A fault or break in the bus cable stops all transmission, even between devices on the same side of the problem. The damaged area reflects signals back in the direction of origin, creating noise in both directions.

8.6.4 Ring Topology:

In a ring topology, each device has a dedicated point-to-point connection with only the two devices on either side of it. A signal is passed along the ring in one direction, from device to device, until it reaches its destination. Each device in the ring incorporates a repeater. When a device receives a signal intended for another device, its repeater regenerates the bits and passes them along. A typical ring topology is as shown in the figure.



Advantages:

i) A ring is relatively easy to install and reconfigure. Each device is linked to only its immediate neighbors (either physically or logically). To add or delete a device requires changing only two connections.

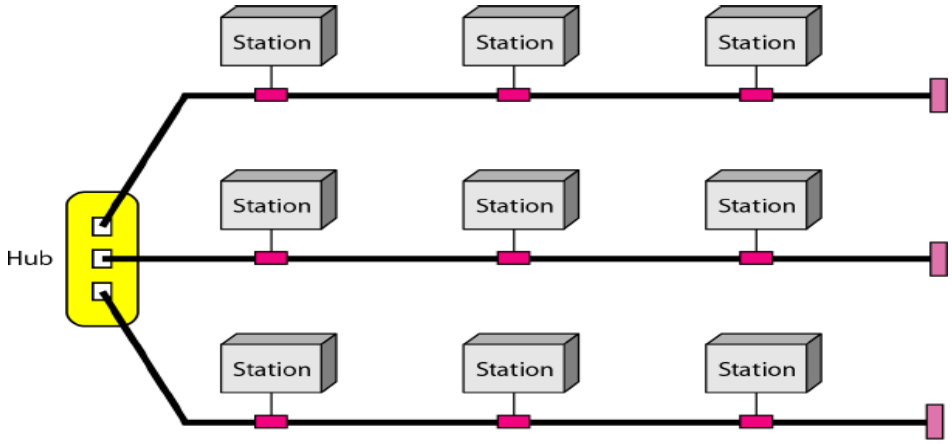
ii) A signal is circulating at all times (token) if one device does not receive a signal within specified period, it can issue an alarm. The alarm alerts the network operator to the problem and its location

Disadvantages:

i) The main disadvantage of ring topology is unidirectional traffic can be a disadvantage. In a simple ring, a break in the ring (such as a disabled station) can disable the entire network.

8.6.5 Hybrid Topology:

A network can be hybrid. It compose of combination of more than one type of topologies. For example, we can have a main star topology with each branch connecting several stations in a bus topology as shown in the following figure.



Mostly this type topology is practically used in real working network. It is impossible to implement only one type of topology in practical working network.

8.7 Network Control Access Method.

In networking, to access a resource is to be able to use that resource. The role of access methods is concerned with how data is put and traffic control on a network cable. Multiple computers must share access to the cable that connects them. However, if two computers were to put data onto the cable at the same time, the data packets from one computer would collide with the packets from the other computer, and both sets of data packets would be destroyed. If data is to be sent over the network from one user to another, or accessed from a server, there must be some way for the data to access the cable without running into other data. And the receiving computer must have reasonable assurance that the data has not been destroyed in a data collision during transmission.

Access methods need to be consistent in the way they handle data. If different computers were to use different access methods, the network would fail because some methods would dominate the cable.

Access methods prevent computers from gaining simultaneous access to the cable. By making sure that only one computer at a time can put data on the network cable, access methods ensure that the sending and receiving of network data is an orderly process.

There are five access methods:

i) Contention Methods
    a. Carrier-Sense Multiple Access with Collision Detection (CSMA/CD) Access Method
    b. Carrier-Sense Multiple Access with Collision Avoidance (CSMA/CA) Access Method
ii) Token passing,
iii) Demand priority.
iv) Polling
v) Switching

The Function of Access Methods

The set of rules that defines how a computer puts data onto the network cable and takes data from the cable is called an *access method*. Once data is moving on the network, access methods help to regulate the flow of network traffic.

8.7.1 CONTENTION METHOD

Carrier-Sense Multiple Access with Collision Detection (CSMA/CD) Access Method

Using the method known as *carrier-sense multiple access with collision detection (CSMA/CD),* each computer on the network, including clients and servers, checks the cable for network traffic. Only when a computer "senses" that the cable is free and that there is no traffic on the cable can it send data. Once the computer has transmitted data on the cable, no other computer can transmit data until the original data has reached its destination and the cable is free again. Remember, if two or more computers happen to send data at exactly the same time, there will be a data collision. When that happens, the two computers involved stop transmitting for a random period of time and then attempt to retransmit. Each computer determines its own waiting period; this reduces the chance that the computers will once again transmit simultaneously. With these points in mind, the name of the access method—carrier-sense multiple access with collision detection (CSMA/CD)—makes sense. Computers

listen to or "sense" the cable (carrier-sense). Commonly, many computers on the network attempt to transmit data (multiple access); each one first listens to detect any possible collisions. If a computer detects a possible collision, it waits for a random period of time before retransmitting (collision detection).

CSMA/CD Considerations

The more computers there are on the network, the more network traffic there will be. With more traffic, collision avoidance and collisions tend to increase, which slows the network down, so CSMA/CD can be a slow-access method.

After each collision, both computers will have to try to retransmit their data. If the network is very busy, there is a chance that the attempts by both computers will result in collisions with packets from other computers on the network. If this happens, four computers (the two original computers and the two computers whose transmitted packets collided with the original computer's retransmitted packets) will have to attempt to retransmit. These proliferating retransmissions can slow the network to a near standstill.

The occurrence of this problem depends on the number of users attempting to use the network and which applications they are using. Database applications tend to put more traffic on the network than word-processing applications do.

Depending on the hardware components, the cabling, and the networking software, using a CSMA/CD network with many users running several database applications can be very frustrating because of heavy network traffic.

Carrier-Sense Multiple Access with Collision Avoidance (CSMA/CA) Access Method

Carrier-sense multiple access with collision avoidance (CSMA/CA) is the least popular of the three major access methods. In CSMA/CA, each computer signals its intent to transmit before it actually transmits data. In this way, computers sense when a collision might occur; this allows them to avoid transmission collisions. Unfortunately, broadcasting the intent to transmit data increases the amount of traffic on the cable and slows down network performance.

8.7.2 Token-Passing Access Method

In the access method known as *token passing*, a special type of packet, called a token, circulates around a cable ring from computer to computer. When any computer on the ring needs to send data across the network, it must wait for a free token. When a free token is detected, the computer will take control of it if the computer has data to send.

The computer can now transmit data. Data is transmitted in frames, and additional information, such as addressing, is attached to the frame in the form of headers and trailers,

While the token is in use by one computer, other computers cannot transmit data. Because only one computer at a time can use the token, no contention and no collision take place, and no time is spent waiting for computers to resend tokens due to network traffic on the cable.

Token-passing is a method that uses an electronic signal called a token. Possession of the token gives a device exclusive use of the transmission channel. The token travels along the channel and stops at each device. A device with a message to send will pick up the token and use it in order to send its message.

When token-passing is used, the device gains access to the transmission channel as follows:

- A network device with a message to send captures the available token as it passes by on the channel.
- The message is attached to the token.
- The message-bearing token continues to circulate on the channel.
- As the token stops at a device, it is checked to see if the message is for the device—this destination device will recognize its address and will read the message.
- The destination device then attaches an acknowledgment of receipt to the token which continues to circulate.
- When the sending device eventually receives the acknowledgment, it clears the
- Token so it may be used by another device.

The token-passing scheme is most commonly used in ring or bus topologies.

8.7.3 Demand Priority Access Method

Demand priority is a relatively new access method designed for the 100-Mbps Ethernet standard known as 100VG-AnyLAN. Standardized by (IEEE) in its 802.12 specification. This access method is based on the fact that repeaters and end nodes are the two components that make up all 100VG-AnyLAN networks. The repeaters manage network access by doing round-robin searches for requests to send from all nodes on the network. The repeater, or hub, is responsible for noting all addresses, links, and end nodes and verifying that they are all functioning. According to the 100VG-AnyLAN definition, an end node can be a computer, bridge, router, or switch.

Demand-Priority Contention

As in CSMA/CD, two computers using the demand-priority access method can cause contention by transmitting at exactly the same time. However, with demand priority, it is possible to implement a scheme in which certain types of data will be given priority if there is contention. If the hub or repeater receives two requests at the same time, the highest priority request is serviced first. If

the two requests are of the same priority, both requests are serviced by alternating between the two.

In a demand-priority network, computers can receive and transmit at the same time because of the cabling scheme defined for this access method. In this method, four pairs of wires are used, which enables quartet signalling, transmitting 25 MHz signals on each of the pairs of wire in the cable.

Demand-Priority Considerations

In a demand-priority network, there is communication only between the sending computer, the hub, and the destination computer. This is more efficient than CSMA/CD, which broadcasts transmissions to the entire network. In demand priority, each hub knows only about the end nodes and repeaters directly connected to it, whereas in a CSMA/CD environment, each hub knows the address of every node in the network.

Demand priority offers several advantages over CSMA/CD including:

- The use of four pairs of wires.
  By using four pairs of wires, computers can transmit and receive at the same time.
- Transmissions through the hub.
  Transmissions are not broadcast to all the other computers on the network. The computers do not contend on their own for access to the cable, but operate under the centralized control of the hub.

Simple LANs generally consist of one or more switches. A switch can be connected to a router, cable modem, or ADSL modem for Internet access. Complex LANs are characterized by their use of redundant links with switches using the spanning tree protocol to prevent loops, their ability to manage differing traffic types via quality of service (QoS), and to segregate traffic with VLANs. A LAN can include a wide variety of network devices such as switches, firewalls, routers, load balancers, and sensors.

8.7.4 Polling

Polling requires that each device on the network be **asked** if it has a message to transmit. To ensure that each device is given an equal opportunity to **speak**, polling must be under central control.

Most commonly found on networks with a central controlling device such as that found in a star topology.

When polling is used, the device gains access to the transmission channels as follows:

- The central controlling device checks with, or polls, each station regularly to see if it has a message to send.
- If the station has a message to send, and the transmission channel is clear, the station receives exclusive use of the channel and sends its message.
- As soon as the station has sent its message, the channel is free for another device to use.

8.7.5 Switching

While not strictly an access control scheme, switching provides a mechanism where a station does not have to share a transmission channel. Switching provides a dedicated transmission channel to each port of a switching hub. Each transmission channel can have multiple stations attached to it, but in high traffic environments, each station can be assigned its own dedicated channel to the switching hub. The switching hub is responsible for providing communications between the channels.

Traditionally, if a network is experiencing excessive traffic—slow performance the network is split into smaller segments, each with its own hub and with fewer attached stations. A switching hub performs this type of segmentation inside a single chassis. It has a number of ports, each of which is a dedicated LAN segment. When switching is used, stations access the transmission channel and communicate as

follows:

- The sending station puts its data onto the transmission channel.

- The switching devices handles the connection to other stations.
- The switching devices handles intersegment traffic via an internal matrix switch.
- When a packet arrives at the switch, its destination address is noted and a connection is made to the destination station.
- The packet is then switched to the destination station.
- Subsequent packets are relayed through the switch automatically

There are two types of switching as discuss in topic 9

i) Packet switching:
ii) Circuit switching :

8.8 Network security

Basic concepts

Security: attempt to protect the services and data it offers against security threats

Confidentiality: the property of a computer system whereby its information is disclosed only to authorized parties.

Integrity: the characteristic that alterations to a system's assets can be made only in an authorized way.

8.8.1 Types of Threats

a) Interception is an unauthorized party has gained access to a service or data!

b) Interruption is services or data become unavailable, unusable, destroyed and so on.

c) Modification is unauthorized changing of data or tampering with a service so that it no longer adheres to its original specifications!

d) Fabrication refers to the situation in which additional data or activity are generated that would normally not exist!

8.8.2 Methods of Attack

a) Eavesdropping is obtaining copies of messages without authority!

b) **Masquerading**: Sending or receiving messages using the identity of another principal without their authority.

c) **Message tampering/Man-in-the-middle attack**: Intercepting messages and altering their contents before passing them on to the intended recipient.

d) **Replaying:** Storing intercepted messages and sending them out at a later time!

e) **Denial of Service** (DoS) is flooding a communication channel or a system resource with messages in order to deny access for others.

8.9 Security Mechanisms

Security mechanisms means of enforcing that policy by

a) **Encryption**:
   i) Transform data into something an attacker cannot understand
   ii) Provides a means to implement confidentiality
   iii) Provides support for integrity

b) **Authentication**: Verify the claimed identity of a user, client, and server and so on!

c) **Authorization:** Check whether the client is authorized to perform the action requested.

d) **Auditing:** Auditing tools are used to trace which clients accessed what, and which way

8.10 Security Services

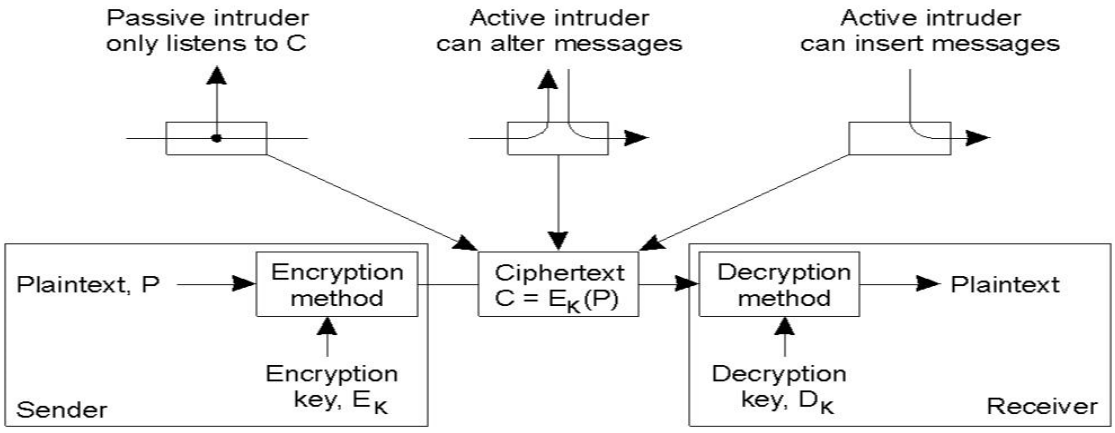
8.10.1 Design Issues

a) **Focus of Control**: Decide the focus of control: data, operations or users

b) **Layering of security mechanisms**: Decide at which level security mechanisms should be placed.

c) **Simplicity**: Simplicity will contribute to the trust that end users will put into the application and, more importantly, will contribute to convincing the designers that the system has no security holes.

8.10.2: Cryptography



The three different attacks(passive intruder ailter messages and active intruder insert messages need to protect against these forms of attacks for which encryption helps by used of **Cryptography**

8.11 Secure Channels

Secure communication requires authentication of the communicating parties, but also ensuring message integrity and possibly confidentiality as well. A secure channel protects senders and receivers against interception, modification, and fabrication of messages. It does not necessarily protect against interruption.Protecting messages against interception is done by ensuring confidentiality. Protecting messages against modification and fabrication is done through protocols for mutual authentication and message integrity.

8.11.1 Authentication

Authentication and message integrity cannot do without each other.

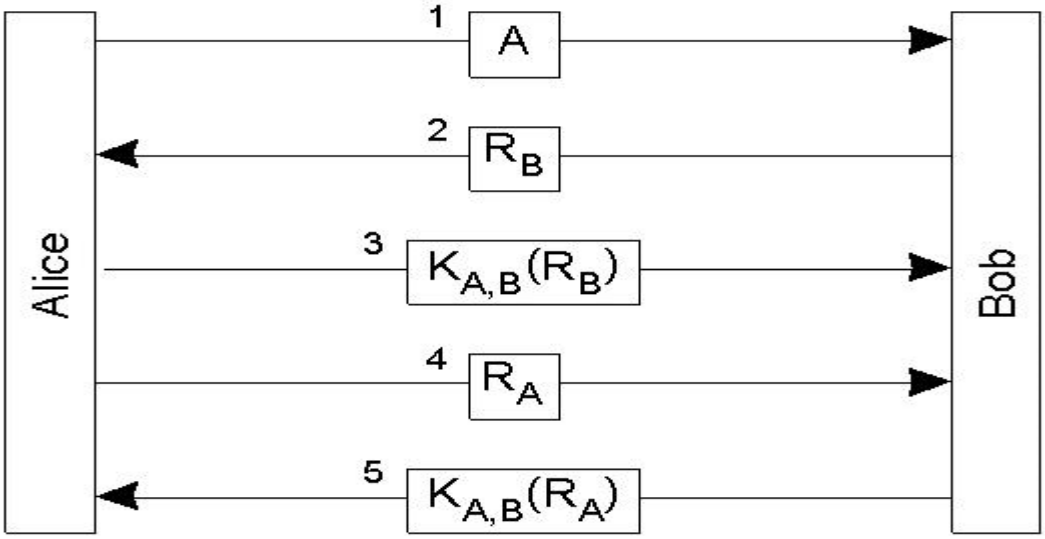
The combination works as follows:-

- Alice starts by sending a message to Bob to set up a channel.
- Once the channel has been set up, Alice knows for sure that she is talking to Bob, and Bob knows for sure that he is talking to Alice, they can exchange messages.

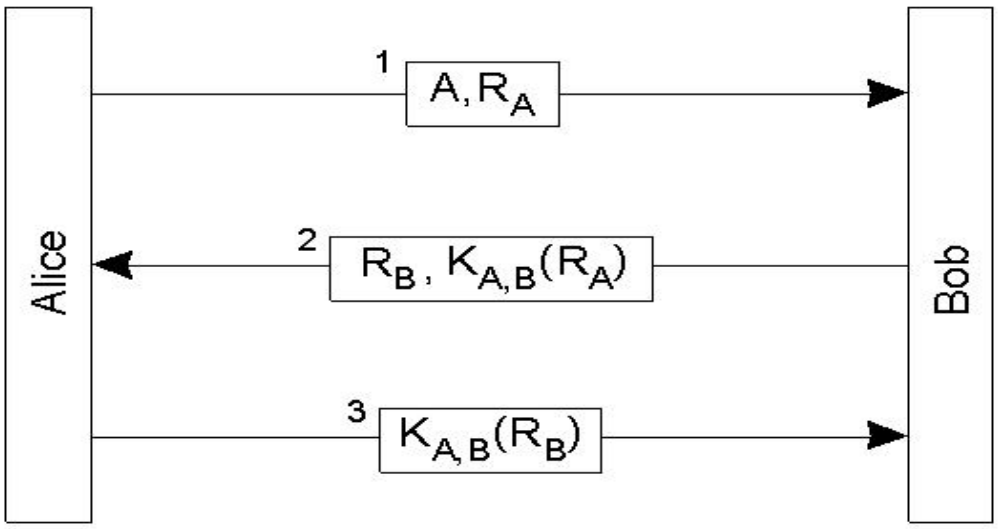
- To subsequently ensure integrity it is common practice to use secret-key cryptography by means of session keys.

Notation!	Description!
$K_{A,B!}$	Secret key shared by A and B!
K_A^+	Public key of A!
K_A^-	Private key of A!

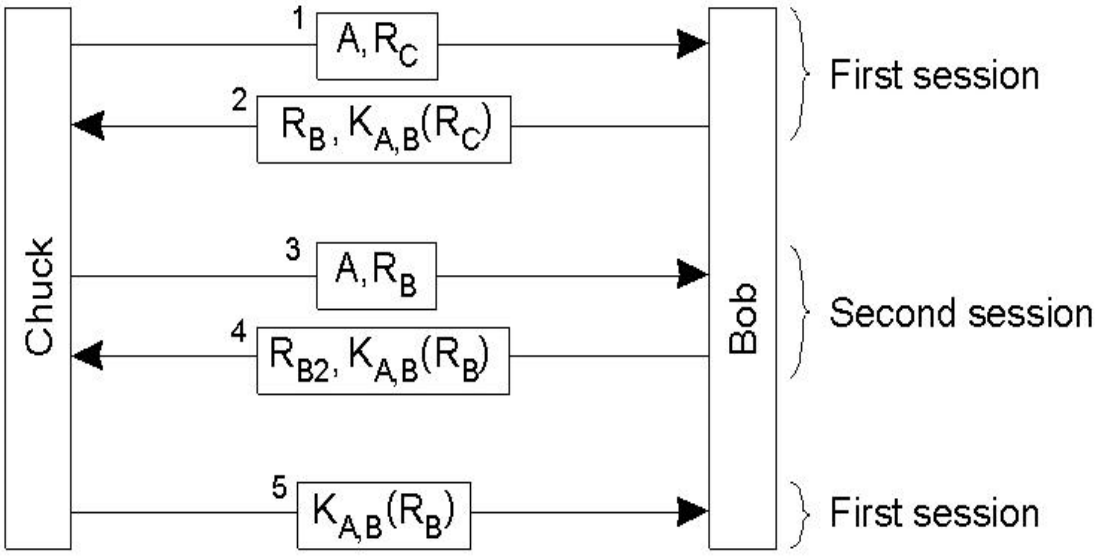
Authentication based on a shared secret key. Also known as challenge-response protocol as shown below



Consider this "optimization": Authentication based on a shared secret key, but using three instead of five messages as shown below.

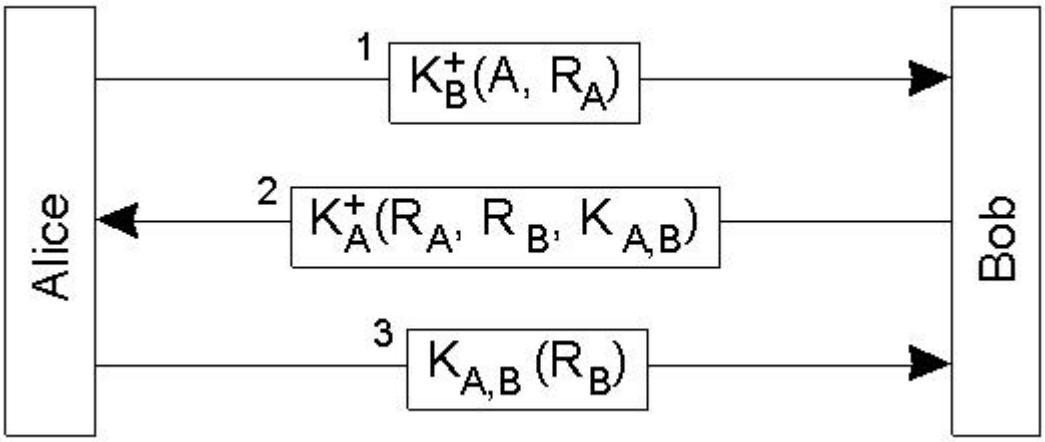


The reflection attack.



Tweaking an existing protocol to improve its performance, can easily affect its correctness

8.11.2 Authentication Using Public-Key Cryptography



8.12 Message Integrity and Confidentiality

Besides authentication, a secure channel should also provide guarantees for message integrity and confidentiality. Confidentiality is easily established by simply encrypting a message before sending it. Protecting a message against modifications is somewhat more complicated.

Digital Signatures: Digitally sign a message in such a way that the signature is uniquely tied to its content.

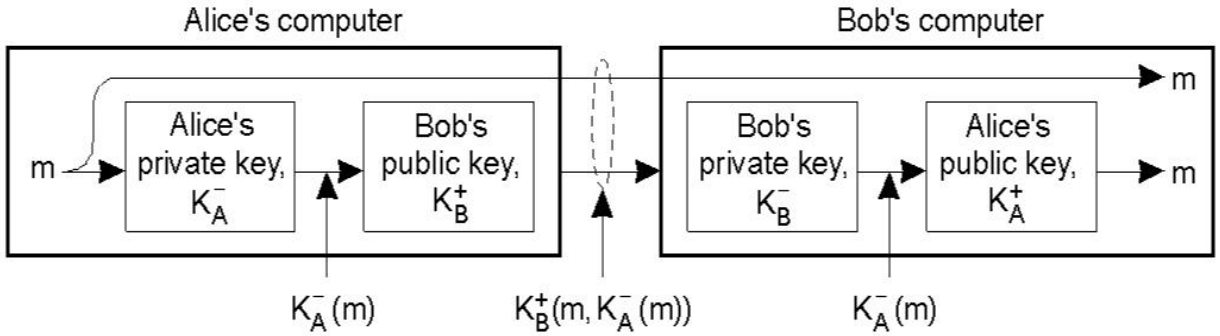
Several ways to place digital signatures:

i) Use a public-key cryptosystem such as RSA.

ii) Use a message digest.

8.12.1 Digital Signatures

a) Digital signing a message using **public-key cryptography.**



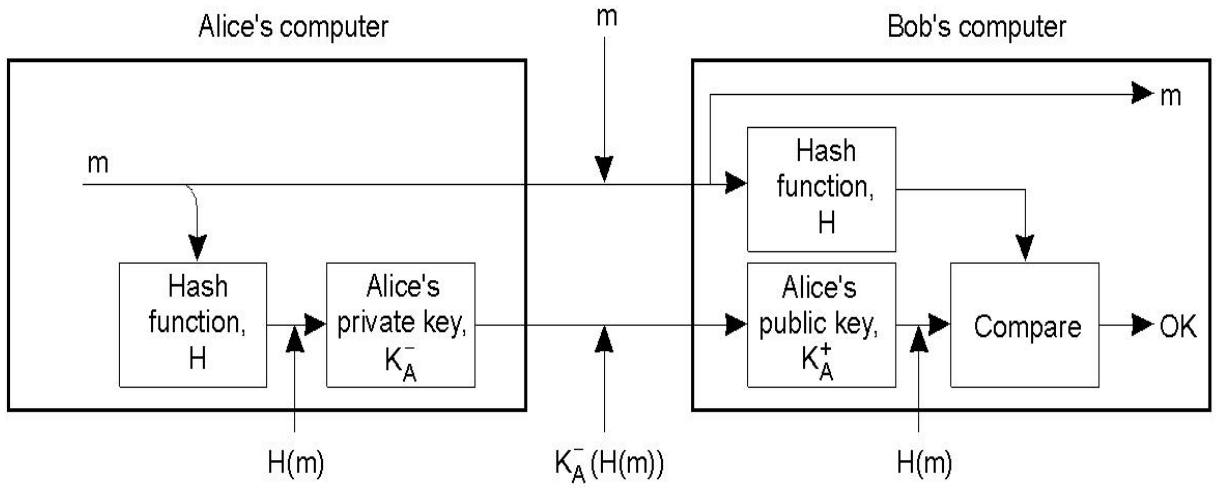
Problems with this scheme**:**

i) The validity of the signature holds only as long as the private key remains secret

ii) What if Alice decides to change her private key

iii) Encryption of the entire message may be costly in terms of processing requirements and is actually unnecessary

b) Digitally signing a message using a **message digest.**



8.12.2 Session Keys

During the establishment of a secure channel, after the authentication phase has completed, the communicating parties generally use a unique shared session key for confidentiality.The session key is safely discarded when the channel is no longer used.

Why not use the same keys for confidentiality as those that are used for setting up the secure channel?

- Cryptographic keys are subject to "wear and tear" just like ordinary keys.
- Protection against replay attacks
- If a key is compromised, only a single session is affected

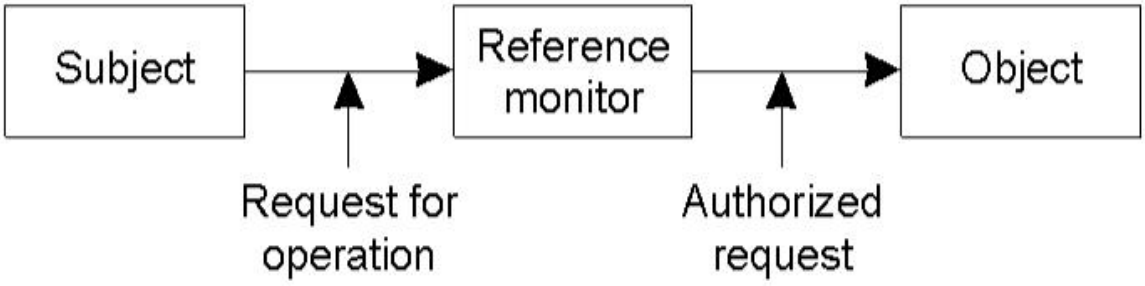
The combination of a long-lasting keys with the much cheaper and more temporary session keys is often a good choice for implementing secure channels for exchanging data.

8.13 Access Control

In the client-server model, once a client and a server have set up a secure channel, the client can issue requests that are to be carried out by the server. A request involve carrying out operations on resources that are controlled by the server. Such a request can be carried out only if the client has sufficient **access rights** for that request. Verifying access rights is referred to as **access control**, whereas **authorization** is about granting access rights.

8.13.1 General Issues in Access Control

General model of controlling access to objects.



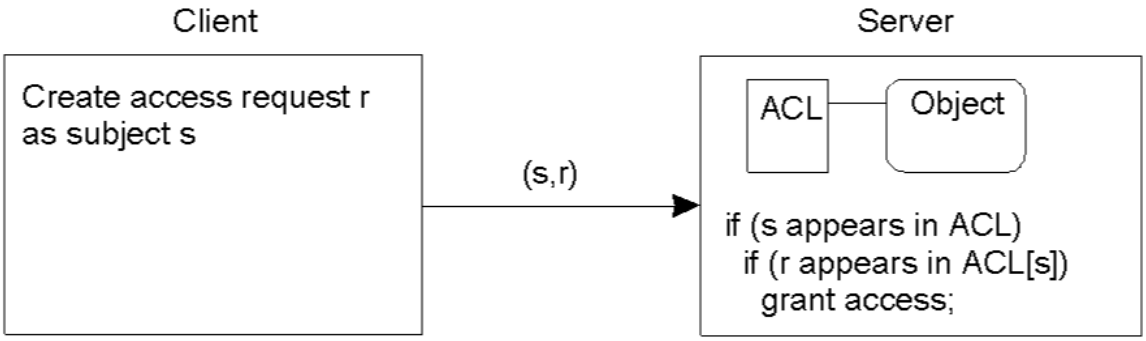
- Controlling the access to an object is all about protecting the object against invocations by subjects that are not allowed to have specific methods carried out
- Also, protection may include object management issues

8.13.2 Access Control Matrix

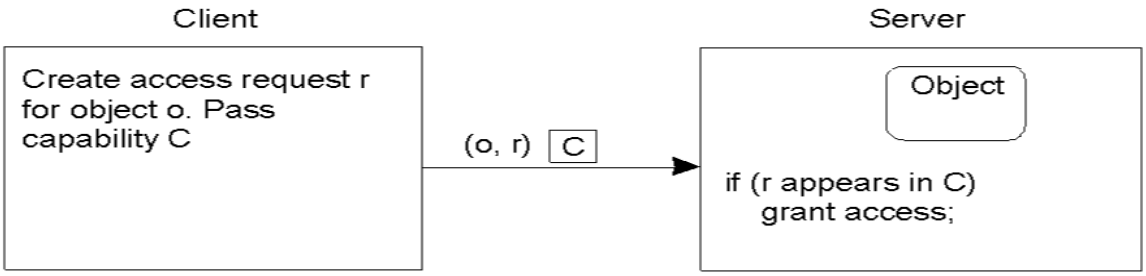
A common approach to modeling the access rights of subjects with respect to objects, is to construct an access control matrix M[s,o]={m1,m2,…}

- **Access Control List**: The matrix is distributed columnwise
- **Capabilities:** The matrix is distributed row-wise

The two access control matrix are shown below (a) Access Control List (b) Capabilities



(a) Access Control List



(b) Capabilities

8.13.2 Role-Based Access Control

Related to having groups as protection domains, it is also possible to implement protection domains as roles. In role-based access control, a user always logs into the system with a specific role, which is often associated with a function the user has in an organization.

A user may have several functions. Depending on the role the user takes when logging in, he may be assigned different privileges (i.e. his role determines the protection domain in which he will operate).

In summary, you learned the following concepts on this topic

i) Network technologies
   - ISDN, ATM, Ethernet, FDDI, Token ring, SONET, HIPPI e.tc,

ii) Network design
   - Hierarchical design and converged network

iii) Network topologies

- Bus, star, ring, mesh and Hybrid.

iv) Network control access method.

- Contention Methods, Token passing, Demand priority, Polling and Switching

v) Network security

- Security basic concepts, types of threats, security mechanisms, secure channels, security services ,message integrity and confidentiality secure channels and access control.

Further Reading

Data & Computer networks, Prakash Gupta

William Stallings, Data & Computer networks 10th edition

Any other data communication and networking relevant books, journals, articles e.t.c

Glossary

Network architecture is global view of network that describes how various operation are organised in network and data communication.

ISDN is a set of communication standards for simultaneous digital transmission of multimedia and other network services over the public switched telephone network (PSTN).

ATM is the leased service that can provide a high-speed connection for data transfer between two points either locally or over long distances.

FDDI is high-performance fiber optic token ring LAN running at 100 Mbps over distances up to 200 km with up to 1000 stations connected.

Hierarchical network design involves dividing the network into discrete layers

Convergence network is the process of combining voice and video communications on a data network.

TOPIC ACTIVITIES

Activity

Read and make briefly on

i) **SONET** network architecture, define, implementation, protocol use, access control method, application

ii) **HIPPI** network architecture define, implementation, protocol use, access control method, application.

TIPS

Refer to these network architecture terms and apply to figure out how to apply in the topic activity:-

i) Network architecture

ii) Protocol

iii) Access control method

Review

i) The basic rate interface (BRI) is the service for homes and small businesses, while the primary rate interface (PRI) is the service for larger businesses. Compute the full capacity of the following service types.

   i) BRI= 2B+D

   ii) PRI=23B+D

ii) Fibre distributed data interface (FDDI) is used as backbone to connect copper LANs to connect many link. Explain which network topology, network access control and network device is used to share a common link.

iii) An airline seat reservation system is being designed in a new airport. One problem that existed in the old location is that some of fast computers on the network could monopolize the bandwidth, causing agents with slower computer to miss seating opportunities Recommend and explain network topology could you use that creates a far environment in which all computer have equal access to the available bandwidth?

iv) Discuss types of connection that ATM utilizes to implement connectivity and manage data transfer between two endpoints either locally or over long distances.

v) A properly designed LAN is a fundamental requirement for any organization well designed LAN is and be able to select appropriate devices to support the network specifications of a small- or medium-sized business. The typical hierarchical design model is broken into three layers namely;

- Access layer
- Distributed layer
- Core layer

a) Write short notes on each hierarchical layer above

b) State three key principles of hierarchical LAN Design

iv) A secure channel protects senders and receivers against the types of threats. Discuss types of security threats

v) Explain mechanisms use to build secure channels

vi) Discuss main protocols used in securing traffic

vii) Describe approaches used by the receiver to verify the sender traffic.

TOPIC NINE: PACKET AND CIRCUIT SWITCHING

Introduction

Welcome to topic nine. This topic is aimed an overview packet and circuit switching and packet switching techniques.

The topic is, therefore designed to prepare you to have a clear understanding of circuit switching, packet switching, datagram and virtual circuit approaches.

Topic Time

- Compulsory online reading, activities, self-assessments and practice exercises **[3 hours]**
- Optional further reading **[1.5 hours]**
- Total student input **[4.5 hours]**

Topic Learning Requirements

- Participation in one *chat* (at least 5 entries)
- At least two elaborate contributions to the *discussion* topic. You may also start your own discussion thread.
- Timely submission of the assignments

Learning Outcomes

By the end of this topic you should be able to:

i) Explain concepts of circuit switching
ii) Explain concepts of packet switching
iii) Describe switched communications networks
iv) Discuss packet switching techniques
v) Explain datagram approach
vi) Explain virtual circuit approach

Topic contents

9.1 Introduction

Networks are used to interconnect many devices. We have discussed with Local Area Networks. Now will shall discuss wide area networks

Since the invention of the telephone, **circuit switching** has been the dominant technology for voice communications.

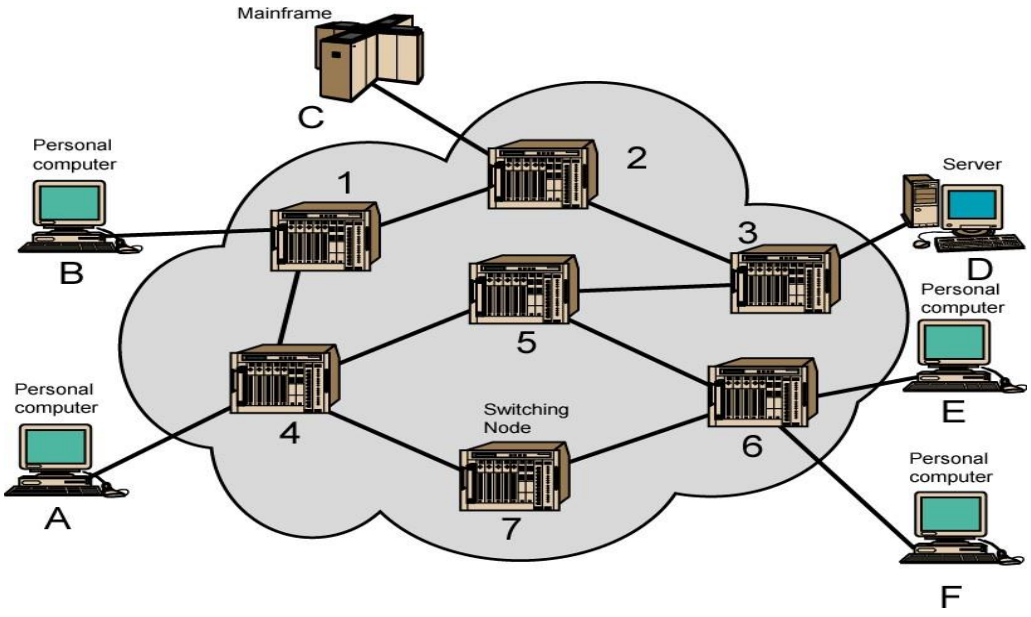
Since 1970, **packet switching** has evolved substantially for digital data communications. It was designed to provide a more efficient facility than circuit switching for bursty data traffic.Two types of packet switching:

i) Datagram (such as today's Internet)
ii) Virtual circuit (such as Frame Relay, ATM)

9.2 Switched Communications Networks

Long distance transmission between stations (called—end devices) is typically done over a network of **switching nodes**. Switching nodes do not concern with content of data. Their purpose is to provide a switching facility that will move the data from node to node until they reach their destination (the end device).A collection of nodes and connections forms a communications network. In a switched communications network, data entering the network from a station are **routed** to the destination by being switched from node to node.

Simple Switching Network



Switching nodes

Nodes may connect to other nodes, or to some stations. Network is usually partially connected. However, some redundant connections are desirable for reliability. Two different switching technologies

i) Circuit switching
ii) Packet switching

9.3 Circuit switching

In circuit switching there is a dedicated communication path between two stations (end-to-end).The path is a connected sequence of links between network nodes. On each physical link, a logical channel is dedicated to the connection. Communication via circuit switching has three phases:

i) Circuit establishment (link by link)

- Routing & resource allocation (FDM or TDM)

ii) Data transfer

iii) Circuit disconnect

- De-allocate the dedicated resources

The switches must know how to find the route to the destination and how to allocate bandwidth (channel) to establish a connection.

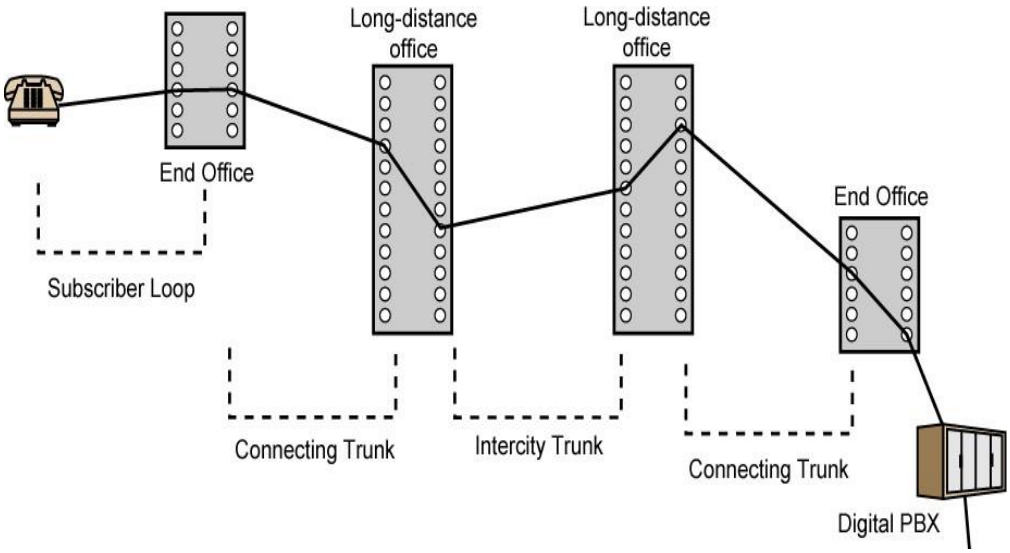
Circuit switching properties

i) Inefficiency
   - Channel capacity is dedicated for the whole duration of a connection
   - If no data, capacity is wasted

ii) Delay
   - Long initial delay: circuit establishment takes time
   - Low data delay: after the circuit establishment, information is transmitted at a fixed data rate with no delay other than the propagation delay. The delay at each node is negligible.

iii) Developed for voice traffic (public telephone network) but can also applied to data traffic.
   - For voice connections, the resulting circuit will enjoy a high percentage of utilization because most of the time one party or the other is talking.
   - But how about data connections?

Public Circuit Switched Network



Public Circuit Switched Network operations

- Subscribers: the device that attach to the network
- Subscriber loop: the link between the subscriber and the network. Exchanges: the switching centers in the network.
- End office: the switching center that directly supports subscribers.
- Trunks: the branches between exchanges. They carry multiple voice-frequency circuits using either FDM or synchronous TDM

Disadvantages of circuit switching

i) Designed for voice service
ii) Resources dedicated to a particular call
iii) For data transmission, much of the time the connection is idle (say, web browsing)
iv) Data rate is fixed
    - Both ends must operate at the same rate during the entire period of connection

9.4 Packet switching

Packet switching is designed to address disadvantages of circuit switching

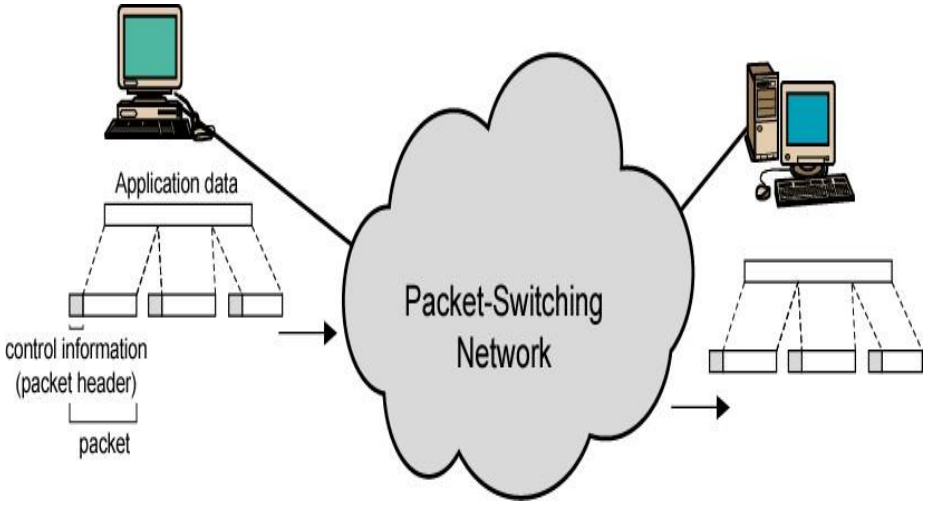
Basic operations of packet switching

i) Data are transmitted in short packets
   - Typically at the order of 1000 bytes
   - Longer messages are split into series of packets
   - Each packet contains a portion of user data plus some control info

ii) Control info contains at least
   - Routing (addressing) info, so as to be routed to the intended destination
   - Recall the content of an IP header!

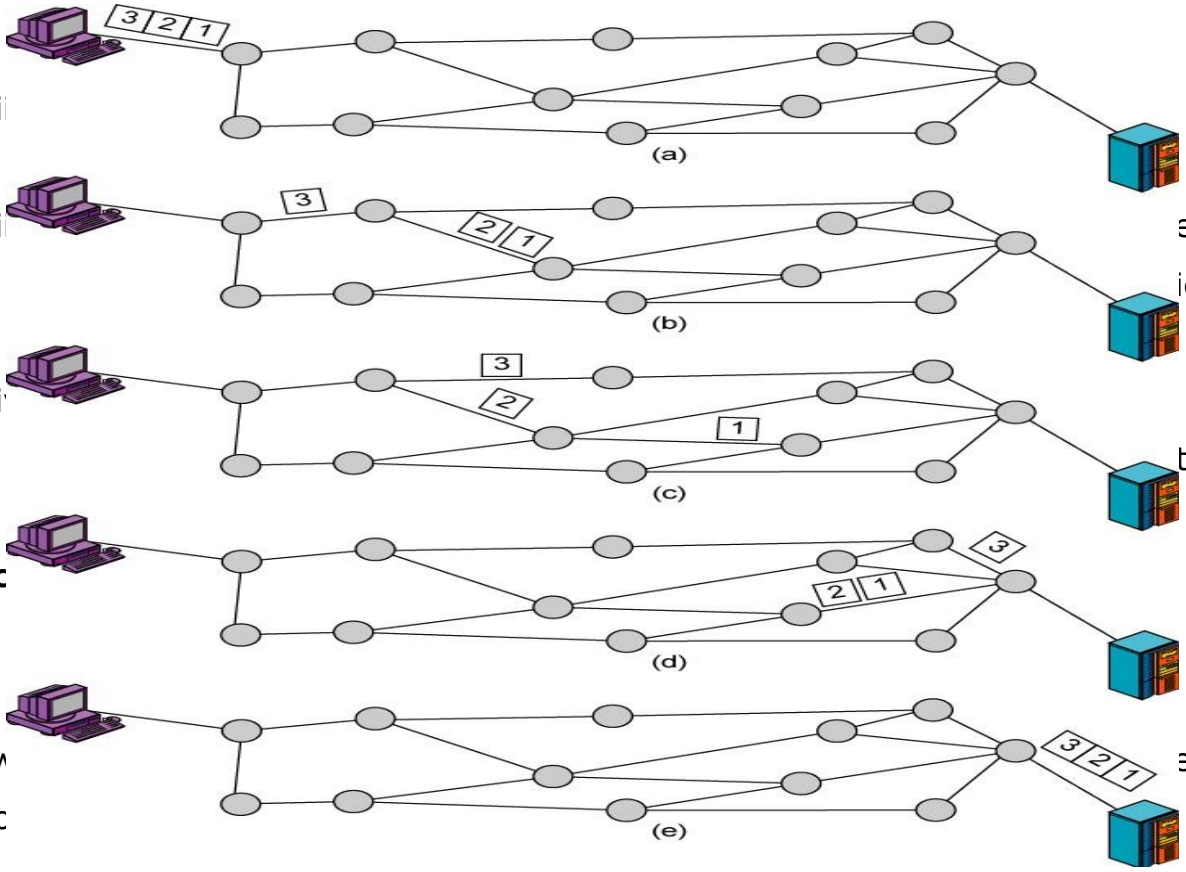
iii) Store and forward
   - On each switching node, packets are received, stored briefly (buffered) and passed on to the next node.

Use of Packets



Advantages of Packet Switching

i) Line efficiency
   - Single node-to-node link can be dynamically shared by many packets over time
   - Packets are queued up and transmitted as fast as possible



i

i ee

ic,

i t.

Pac

How em

thro

Two approaches

i) **Datagram** approach
ii) **Virtual circuit** approach

9.4.1 Datagram

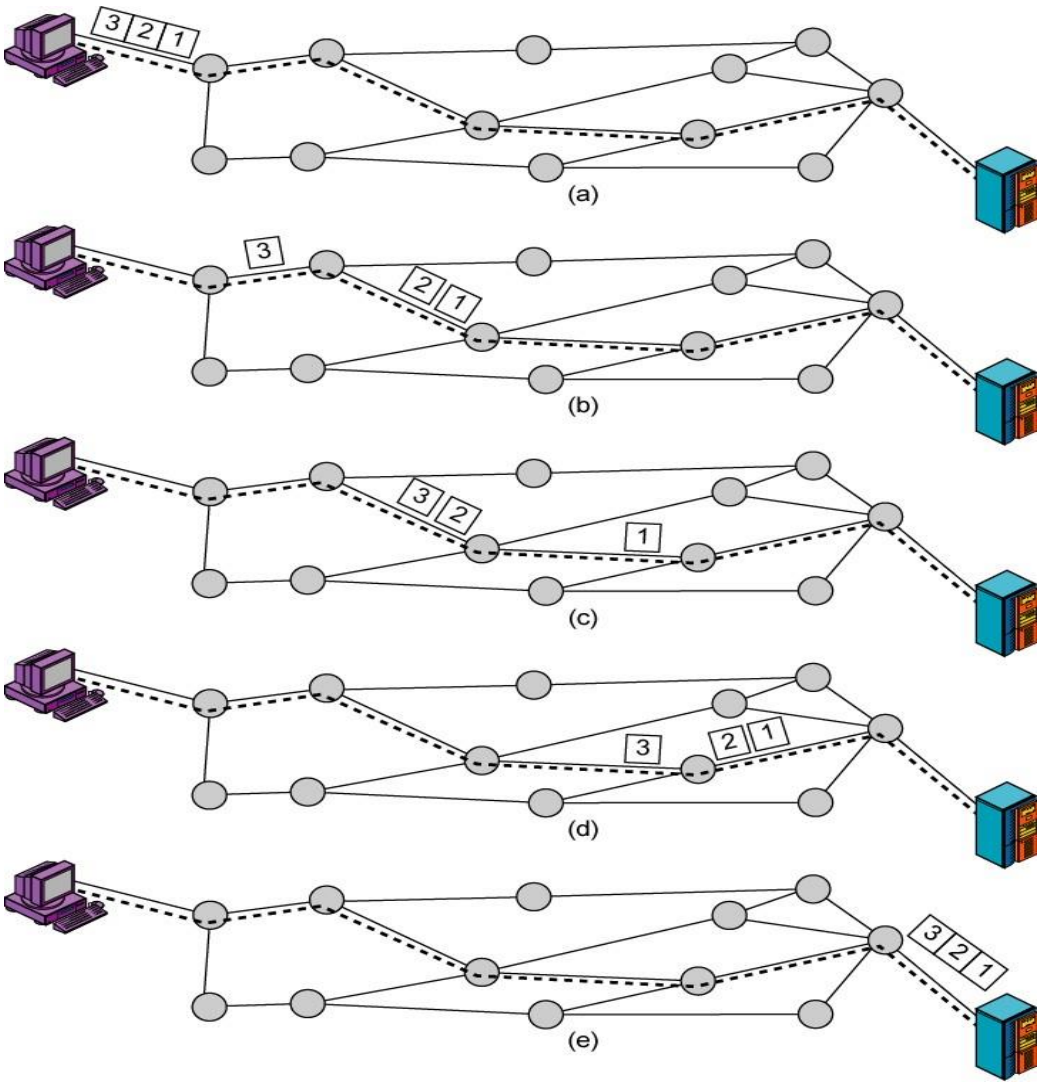
Each packet is treated independently, with no reference to packets that have gone before. Each node chooses the next node on a packet's path. Packets can take any possible route and may arrive at the receiver out of order. Also packets may go missing. It is up to the receiver to re-order packets and recover from missing packets. Good example of this approach of switching is Internet.

Example of datagram illustrations of how 3 packets are sent over network

9.4.2 Virtual Circuit

In virtual circuit, a preplanned route is established before any packets are sent, then all packets follow the same route. Each packet contains a virtual circuit identifier instead of destination address, and each node on the pre-established route knows where to forward such packets.The node need not make a routing decision for each packet. Example: X.25, Frame Relay, ATM e.t.c

Example of Virtual Circuit illustrations of how 3 packets are sent over network



Virtual Circuit Vs. Datagram

Virtual circuits

i) Network can provide sequencing (packets arrive at the same order) and error control (retransmission between two nodes).

ii) Packets are forwarded more quickly

- Based on the virtual circuit identifier
- No routing decisions to make

iii) Less reliable

- If a node fails, all virtual circuits that pass through that node fail.

Datagram

i) No call setup phase

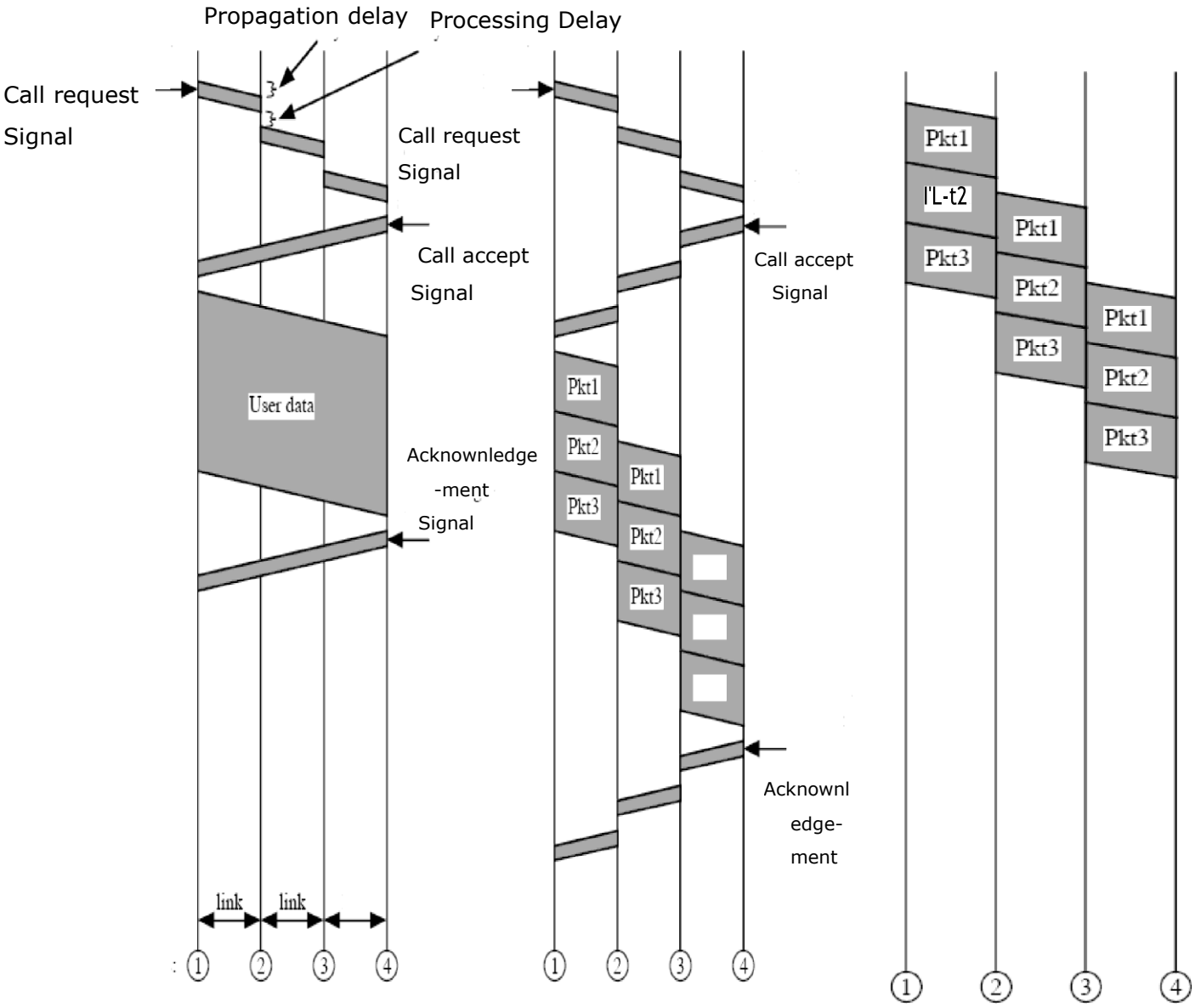
- Good for bursty data, such as Web applications

ii) More flexible

- If a node fails, packets may find an alternate route
- Routing can be used to avoid congested parts of the network

The diagram below illustrates an event timing of circuit switching and packet switching

a) Circuit switching b)Virtual circuit switching c) Datagram packet switching



Comparison of Communication Switching Techniques

Circuit Switching	Datagram Packet Switching	Virtual Circuit Packet Switching
Dedicated transmission path	No dedicated path	No dedicated path
Continuous transmission of data	Transmission of packets	Transmission of packets
Fast enough for interactive	Fast enough for interactive	Fast enough for interactive
Messages are not stored	Packets may be stored until delivered	Packets stored until delivered
The path is established for entire conversation	Route established for each packet	Route established for entire conversation
Call setup delay; negligible transmission delay	Packet transmission delay	Call setup delay; packet transmission delay
Busy signal if called party busy	Sender may be notified if packet not delivered	Sender notified of connection denial
Overload may block call setup; no delay for established calls	Overload increases packet delay	Overload may block call setup; increases packet delay
Electromechanical or computerized switching nodes	Small switching nodes	Small switching nodes
User responsible for message loss protection	Network may be responsible for individual packets	Network may be responsible for packet sequences
Usually no speed or code conversion	Speed and code conversion	Speed and code conversion
Fixed bandwidth	Dynamic use of bandwidth	Dynamic use of bandwidth
No overhead bits after call setup	Overhead bits in each packet	Overhead bits in each packet

In summary, you learned the following concepts on this topic

i) Circuit switching
ii) Packet switching
iii) Switched communications networks
iv) Packet switching techniques
v) Datagram approach
vi) Virtual circuit approach
vii) Comparison between the network switching approaches

Further Reading

Data & Computer networks, Prakash Gupta

William Stallings, Data & Computer networks 10th edition

Any other data communication and networking relevant books, journals, articles e.t.c

Glossary

Circuit switching: is a dedicated communication path between two stations (end-to-end)

Circuit switching is a connected sequence of links between network nodes. On each physical link, a logical channel is dedicated to the connection.

Packet switching is switching where data are transmitted in short packets, routing (addressing) info, so as to be routed to the intended destination and On each switching node, packets are received, stored briefly (buffered) and passed on to the next node.

Datagram approach each packet is treated independently, with no reference to packets that have gone before.

Virtual circuit is preplanned route is established before any packets are sent, then all packets follow the same route.

TOPIC ACTIVITIES

Activity

Transmission of information in any network involves end-to-end addressing and sometimes local addressing .The table below shows the types of networks and the addressing mechanism used in each of them.

Network	Setup	Data Transfer	Teardown
Circuit-switched	End-to-end		End-to-end
Datagram		End-to-end	

Using the table above for the following activities

i) Does a circuit-switched network need end-to-end addressing during the setup and teardown phases? Why are no addresses needed during the data transfer phase for this type of network?
ii) Does a datagram network need only end-to-end addressing during the data transfer phase, but no addressing during the setup and teardown phases?
iii) Does a virtual-circuit network need addresses during all three phases?

TIPS

Review the three switching techniques

Review

i) Compare and contrast a circuit-switched network and a packet-switched network.
ii) What is the principal application that has driven the design of circuit-switching networks?
iii) Datagram and virtual-circuit are packet switching techniques. There need a routing or switching table to find the output port from which the information belonging to a destination should be sent out, but a circuit-

switched network has no need for such a table. Give reasons as to why there is this difference between the two switching techniques.

TOPIC TEN: WIRELESS LAN

Introduction

Welcome to topic ten. This topic is aimed introducing main goals of wireless LAN, concept of IEEE 802.11 and standards, architecture of wireless LAN, Wireless LAN standard services and Wireless LAN station types

The topic is, therefore designed to prepare you to have a clear understanding Impacts of Wireless LAN and Application of wireless LAN.

Topic Time

- Compulsory online reading, activities, self-assessments and practice exercises **[3 hours]**
- Optional further reading **[1.5 hours]**
- Total student input **[4.5 hours]**

Topic Learning Requirements

- Participation in one *chat* (at least 5 entries)
- At least two elaborate contributions to the *discussion* topic. You may also start your own discussion thread.
- Timely submission of the assignments

Learning Outcomes

By the end of this topic you should be able to outline:-

i) Main goals of Wireless LAN
ii) Concept of IEEE 802.11 and standards
iii) Architecture of Wireless LAN
iv) Wireless LAN standard services
v) Wireless LAN station types
vi) Impacts of Wireless LAN
vii) Application of wireless LAN

Topic Concepts

10.1 Introduction

The demand for connecting devices without the use of cables is increasing everywhere.

Goals

i) To deliver services in wired networks
ii) To achieve high throughput
iii) To achieve highly reliable data delivery
iv) To achieve continuous network connection

Two promising wireless technologies for LANs: IEEE 802.11 wireless LANs, sometimes called wireless Ethernet, and Bluetooth, a technology for small wireless LANs.

10.2 IEEE 802.11

IEEE has defined the specifications for a wireless LAN, called IEEE 802.11, which covers the physical and data link layers.

Architecture

i) IEEE 802.11 is devoted to wireless LANs.
    — Consists of MAC and physical layer protocols for wireless LANs
ii) The Wi-Fi Alliance (Wi-Fi: Wireless Fidelity)
    — An industry consortium
    — To certify interoperability for 802.11 products
iii) IEEE 802.11 Architecture
    — The smallest building block is Basic Service Set (BSS)
        • A number of stations executing the same MAC protocol
        • Shared wireless medium
        • BSS corresponds to a cell
    — A BSS may be isolated, or may connect to a Backbone Distribution System (DS) through an Access Point (AP)
        • AP functions as a bridge and a relay point

- AP could be a station which has the logic to provide DS services
- AP corresponds to a Control Module (CM)
- DS can be a switch, wired network, or wireless network

— An Extended Service Set (ESS) consists of two or more BSSs interconnected by a DS.

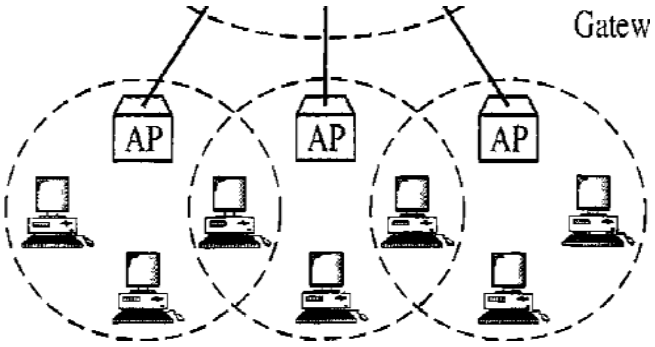
The standard defines two kinds of services: the basic service set (BSS) and the extended Service set (ESS).

10.3 Basic Service Set

IEEE 802.11 defines the basic service set (BSS) as the building block of a wireless LAN. A basic service set is made of stationary or mobile wireless stations and an optional central base station, known as the access point (AP). The BSS without an AP is a stand-alone network and cannot send data to other BSSs. It is called an *ad hoc architecture.* In this architecture, stations can form a network without the need of an AP; they can locate one another and agree to be part of a BSS. A BSS with an AP is sometimes referred to as an *infrastructure* network.

10.4 Extended Service Set

An extended service set (ESS) is made up of two or more BSSs with APs. In this case, the BSSs are connected through a *distribution system,* which is usually a wired LAN. The distribution system connects the APs in the BSSs. IEEE 802.11 does not restrict the distribution system; it can be any IEEE LAN such as an Ethernet. Note that the extended service set uses two types of stations: mobile and stationary. The mobile stations are normal stations inside a BSS. The stationary stations are AP stations that are part of a wired LAN. Figure below shows an ESS.



BSS BSS BSS

When BSSs are connected, the stations within reach of one another can communicate without the use of an AP. However, communication between two stations in two different BSSs usually occurs via two APs. The idea is similar to communication in a cellular network if we consider each BSS to be a cell and each AP to be a base station. Note that a mobile station can belong to more than one BSS at the same time.

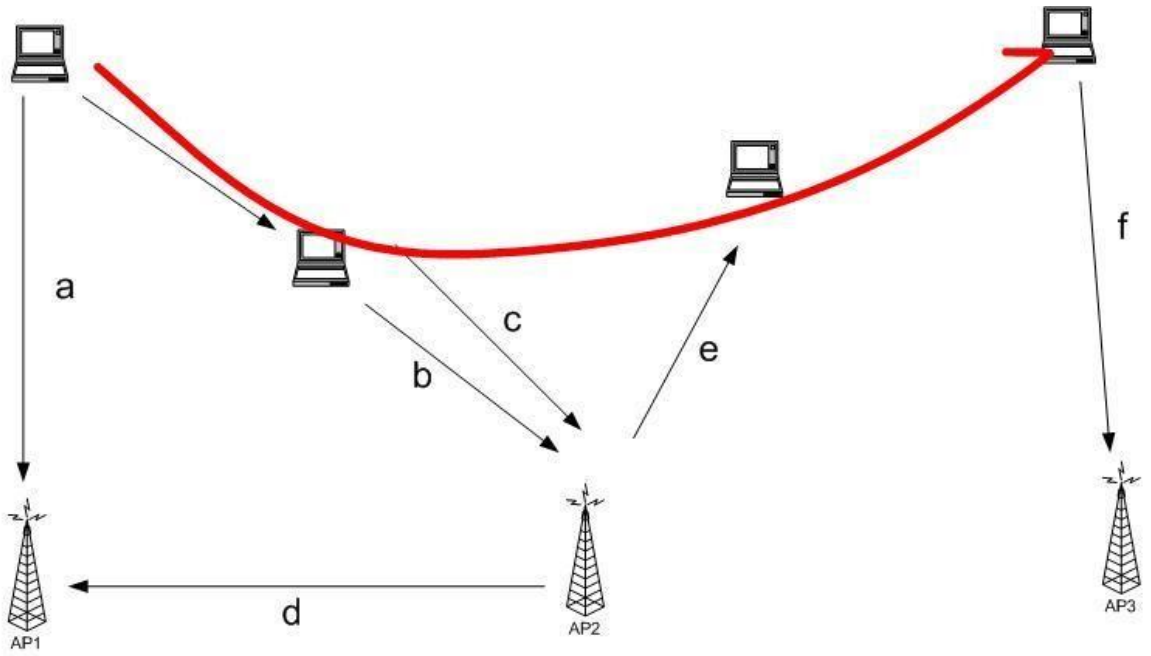
10.5 Station Types

IEEE 802.11 defines three types of stations based on their mobility in a wireless LAN: no transition, BSS· transition, and ESS-transition mobility. A station with no-transition mobility is either stationary (not moving) or moving only inside a BSS. A station with BSS-transition mobility can move from one BSS to another, but the movement is confined inside one ESS. A station with ESS-transition mobility can move from one ESS to another. However, IEEE 802.11 does not guarantee that communication is continuous during the move.

Services

- Station services:
  - authentication,
  - de-authentication,
  - privacy,
  - delivery of data
- Distribution Services *(A thin layer between MAC and LLC sublayer)*

- association
- disassociation
- re-association
- distribution
- Integration



(a) ---- The station finds AP1, it will authenticate and associate.

(b) ---- As the station moves, it may pre-authenticate with AP2.

(c) ---- When the association with AP1 is no longer desirable, it may reassociate with AP2.

(d) ---- AP2 notify AP1 of the new location of the station, terminates the previous association with AP1.

(e) ---- At some point, AP2 may be taken out of service. AP2 would disassociate the associated stations.

(f) ---- The station find another access point and authenticate and associate.

The following are among the most important requirements for wireless LANs:

i) **Throughput:** The medium access control protocol should make as efficient use as possible of the wireless medium to maximize capacity.

ii) **Number of nodes:** Wireless LANs may need to support hundreds of nodes across multiple cells

iii) **Connection to backbone LAN:** In most cases, interconnection with stations on a wired backbone LAN is required. For infrastructure wireless LANs, this is easily accomplished through the use of control modules that connect to both types of LANs. There may also need to be accommodation for mobile users and ad hoc wireless networks.

iv) **Service area:** A typical coverage area for a wireless LAN has a diameter of 100 to 300 m.

v) **Battery power consumption:** Mobile workers use battery-powered workstations that need to have a long battery life when used with wireless adapters. This suggests that a MAC protocol that requires mobile nodes to monitor access points constantly or engage in frequent handshakes with a base station is inappropriate. Typical wireless LAN implementations have features to reduce power consumption while not using the network, such as a sleep mode.

vi) **Transmission robustness and security:** Unless properly designed, a wireless LAN may be especially vulnerable to interference and eavesdropping. The design of a wireless LAN must permit reliable transmission even in a noisy environment and should provide some level of security from eavesdropping.

vii) **Collocated network operation:** As wireless LANs become more popular, it is quite likely for two or more wireless LANs to operate in the same area or in some area where interference between the LANs is possible. Such interference may thwart the normal operation of a

MAC algorithm and may allow unauthorized access to a particular LAN.

viii) **License-free operation:** Users would prefer to buy and operate wireless LAN products without having to secure a license for the frequency band used by the LAN.

ix) **Handoff/roaming:** The MAC protocol used in the wireless LAN should enable mobile stations to move from one cell to another.

x) **Dynamic configuration:** The MAC addressing and network management aspects of the LAN should permit dynamic and automated addition, deletion, and relocation of end systems without disruption to other users.

10.6 IEEE 802.11 Standards

Standard Scope

Medium access control (MAC): One common MAC for WLAN applications as follows:-

IEEE 802.11 Physical layer: Infrared at 1 and 2 Mbps

IEEE 802.11 Physical layer: 2.4-GHz FHSS at 1and 2 Mbps

IEEE 802.11 Physical layer: 2.4-GHz DSSS at 1 and 2 Mbps

There are categories based on data rate as well as services as follows:-

i) IEEE 802.11a Physical layer: 5-GHz OFDM at rates from 6 to 54 Mbps

ii) IEEE 802.11b Physical layer: 2.4-GHz DSSS at 5.5 and 11 Mbps

iii) IEEE 802.11c Bridge operation at 802.11 MAC layer

iv) IEEE 802.11d Physical layer: Extend operation of 802.11 WLANs to new regulatory domains (countries)

v) IEEE 802.11e MAC: Enhance to improve quality of service and enhance security mechanisms

vi) IEEE 802.11f Recommended practices for multivendor access point interoperability

vii) IEEE 802.11g Physical layer: Extend 802.11b to data rates>20 Mbps

10.7 Impact of wireless environment on networks

i) **The wireless spectrum**: Different frequency ranges i.e *Wireless LAN (IEEE 802.11b/g),* 2.4 GHz, *Wireless LAN (IEEE 802.11a)* 5 GHz, *Bluetooth* 2.45 GHz *Local Multipoint Distribution Services (LMDS)* 27.5-31.3 GHz e.t.c

ii) **Physical impairments**: Noise, Interference, fading **-** Unwanted signals added to the message signal

iii) **Diversity:** A diversity scheme extracts information from multiple signals transmitted over different fading paths

iv) **Contention for the shared medium**: Need for medium access control mechanisms to establish what to do in this case (also, to maximize aggregate utilization of available capacity

v) **Effects of mobility**: Resource management and QoS are directly affected by route changes

vi) **Restrictions on terminal equipment**: Form factors (size, power dissipation, ergonomics, etc.) play an important part in mobility and nomadicity

vii) **Security:** Safeguards for physical security must be even greater in wireless communications: Encryption: intercepted communications must not be easily interpreted

10.8 Application of wireless LAN

i) Wireless LAN Applications: wireless LAN saves the cost of the installation of LAN cabling and eases the task of relocation and other modifications to network structure.

ii) **Cross-Building Interconnect** Another use of wireless LAN technology is to connect LANs in nearby buildings, be they wired or wireless LANs. In this case, a point-to-point wireless link is used between two buildings.The devices so connected are typically bridges or routers. This single point-to-point link is not a LAN per se,but it is usual to include this application under the heading of wireless LAN.

iii) **Nomadic access**: provides a wireless link between a LAN hub and a mobile data terminal equipped with an antenna, such as a laptop computer or notepad computer. One example of the utility of such a connection is to enable an employee returning from a trip to transfer data from a personal portable computer to a server in the office. Nomadic access is also useful in an extended environment such as a campus or a business operating out of a cluster of buildings. In both of these cases, users may move around with their portable computers and may wish access to the servers on a wired LAN from various locations.

iv) **Ad Hoc Networking** An ad hoc network is a peer-to-peer network (no centralized server) set up temporarily to meet some immediate need. For example, a group of employees, each with a laptop or palmtop computer, may convene in a conference room for a business or classroom meeting. The employees link their computers in a temporary network just for the duration of the meeting.

In summary, you learned the following concepts on this topic

i) Main goals of Wireless LAN
ii) Concept of IEEE 802.11 and standards
iii) Architecture of Wireless LAN
iv) Wireless LAN standard services
v) Wireless LAN station types
vi) Impacts of Wireless LAN

vii) Application of wireless LAN

Further Reading

Data & Computer networks, Prakash Gupta

William Stallings, Data & Computer networks 10th edition

Any other data communication and networking relevant books, journals, articles e.t.c

Glossary

Wireless LAN connecting devices without the use of cables

A basic service set (BSS) is made of stationary or mobile wireless stations and an optional central base station, known as the access point (AP).

An extended service set (ESS) is made up of two or more BSSs with APs. In this case, the BSSs are connected through a distribution system, which is usually a wired LAN.

A station with **no-transition** mobility is either stationary (not moving) or moving only inside a BSS

A station with **BSS-transition mobility** can move from one BSS to another, but the movement is confined inside one ESS,

A station with **ESS-transition mobility** can move from one ESS to another

TOPIC ACTIVITIES

Activity

Use the knowledge you have acquired from the topic to figure out how your normally access internet using you mobile phone or laptop without connecting physical cable. Determine the phone/labtop standard services

TIPS

Review Wireless LAN standard services and how the mobile services providers offer internet services to their clients.

Review

i) You want your laptop and cell phone to exchange information wireless. What networking technology might you want as a feature of both your laptop and phone to accomplish this?

ii) Explain two main goals of IEEE 802.11 and one impact of wireless environment as mode of channel data communication and networks.

iii) IEEE has defined the specifications for a wireless LAN, called IEEE 802.11.

   a) State two main OSI layers which covers wireless LAN technology
   b) What is the difference between a BSS and an ESS?
   c) Discuss any two types of mobility in a wireless LAN.

iv) A broadcast network is one in which a transmission from any one attached station is received by all other attached stations over a shared medium. Examples are a bus-topology local area network, such as Ethernet and a wireless radio network. Discuss the need or lack of need for a network layer and in a broadcast network.

END

THANKS