Semester – IV

18ITU401 DATA COMMUNICATION AND NETWORKS 4H – 4C

Instruction Hours / week: L: 4 T: 0 P: 0 **Marks:** Int : **40** Ext : **60** Total: **100**

End Semester Exam : 3 Hours

Course Objectives

- To study the basic taxonomy and terminology of the computer networking and enumerate the layers of OSI model and TCP/IP model.
- To acquire knowledge of Application layer and Presentation layer paradigms and protocols.
- To study Session layer design issues, Transport layer services, and protocols.
- To gain core knowledge of Network layer routing protocols and IP addressing.
- To study data link layer concepts, design issues, and protocols.
- To read the fundamentals and basics of Physical layer, and will apply them in real time applications.

Course Outcomes (COs)

1. Describe the functions of each layer in OSI and TCP/IP model.
2. Explain the functions of Application layer and Presentation layer paradigms and Protocols.
3. Describe the Session layer design issues and Transport layer services.
4. Classify the routing protocols and analyze how to assign the IP addresses for the given network.
5. Describe the functions of data link layer and explain the protocols.
6. Explain the types of transmission media with real time applications

Unit I

Introduction to Data Communication: Network, Protocols & standards and standards organizations - Line Configuration; layered network architecture; overview of OSI reference model; overview of TCP/IP protocol suite. **Data Communication Fundamentals and Techniques**: Analog and digital signal; data-ratelimits; digital to digital line encoding schemes; pulse code modulation; parallel and serial transmission;

Unit II

(cont..)digital to analog modulation-; multiplexing techniques- FDM, TDM; transmission media.

Networks Switching Techniques and Access mechanisms: Circuit switching; packet switching - connectionless datagram switching, connection-oriented virtual circuit switching; dial-up modems; digital subscriber line; cable TV for data transfer.

Unit III

Data Link Layer Functions and Protocol: Error detection and error correction techniques; data-link control- framing and flow control; error recovery protocols- stop and wait ARQ, go-back-n ARQ; Point to Point Protocol on Internet.

Unit IV

Multiple Access Protocol and Networks: CSMA/CD protocols; Ethernet LANS; connecting LAN and back-bone networks- repeaters, hubs, switches, bridges, router and

gateways; **Networks Layer Functions and Protocols**: Routing; routing algorithms; network layer protocol of Internet- IP protocol, Internet control protocols.

Unit V

Transport Layer Functions and Protocols: Transport services- error and flow control, Connection establishment and release- three way handshake; **Overview of Application layer protocol**: Overview of DNS protocol; overview of WWW &HTTP protocol.

Suggested Readings

1. Forouzan, B. A.(2007). Data Communications and Networking(4th ed.). New Delhi: THM.
2. Tanenbaum, A. S. (2002). Computer Networks (4th ed.). New Delhi: PHI.

Web Sites

1. en.wikipedia.org/wiki/Internet_protocol_suite
2. http://docwiki.cisco.com/wiki/Introduction_to_WAN_Technologies
3. www.yale.edu/pclt/COMM/**TCPIP**.HTM
4. www.w3schools.com/**tcpip**/default.asp

KARPAGAM ACADEMY OF HIGHER EDUCATION

(Deemed to be University)
(Established Under Section 3 of UGC Act 1956)
Eachanari (po), Coimbatore-21

DEPARTMENT OF CS, CA & IT

LECTURE PLAN

SUBJECT NAME: DATA COMMUNICATION NETWORKS
SUBJECT CODE: 18ITU402 **SEMESTER: IV**
STAFF : Mrs.HEMAGOWRI.j **CLASS: II B.Sc(IT)**

S.No	Topics Covered	Reference Materials
	Unit I	
1.	**Introduction to Data Communication:** Overview	S1:1-6
2.	Network, Protocols & standards and standards organizations	S1:8-16 , S1:19-21,W2
3.	Line Configuration; layered network architecture	S1:27-29
4.	Overview of OSI reference model	S2 : 32-41
5.	Overview of TCP/IP protocol suite	S1:42-49
6.	**Data Communication Fundamentals and Techniques**: Analog and digital signal	S1:57-74
7.	Data-Rate limits, digital to digital line encoding schemes	S1:85-92
8.	Pulse Code Modulation; Parallel And Serial Transmission	S1:120-129, 131-135, W1
9.	Recapitulation and Possible Questions Discussion	
	Total No of hours for Unit 1: 9	
	Unit II	
1.	Digital To Analog Modulation	S1:141-155 W1
2.	Multiplexing Techniques- FDM, TDM	S1:161-169
3.	Transmission Media - Guided Media- Twisted pair and coaxial cable	S1:191-195
4.	**Networks Switching Techniques and ACS Uses mechanisms:** Circuit switching Packet switching	S1:214-218, 232

5.	Connectionless Datagram Switching Connection-Oriented Virtual Circuit Switching	S1:218-227
6.	Dial-Up Modems; Digital Subscriber Line; Cable TV For Data Transfer	S1:248-256
7.	Recapitulation and Possible Questions Discussion	
Total No of hours for Unit 2: 7		
Unit -III		
1.	**Data Link Layer Functions and Protocol –** Introduction Error detection and error correction techniques	S1:265 S1:272-274
2.	Data-Link Control	S1:307
3.	Framing And Flow Control Error Recovery Protocols	S1:307-308 S1:311
4.	Stop And Wait ARQ	S1:315
5.	Go-Back-N ARQ	S1:324
6.	Point to Point Protocol on Internet.	S1:346-355
7.	Recapitulation and Possible Questions Discussion	
Total No of hours for Unit 3:7		
Unit - IV		
1.	**Multiple Access Protocol And Networks**: CSMA/CD Protocols Ethernet LANS	S1:363-373 S1:395
2.	Connecting LAN And Back-Bone Networks	S1:445-450
3.	Repeaters, Hubs, Switches, Bridges, Router And Gateways	S1:450-457
4.	**Networks Layer Functions And Protocols**: Routing	S1:658-666
5.	Routing Algorithms Network Layer Protocol Of Internet	S1:666-678
6.	IP Protocol, Internet Control Protocols	S1:703-709
7.	Recapitulation and Possible Questions Discussion	
Total No of hours for Unit 4: 7		

Unit - V		
1.	**Transport Layer Functions And Protocols**: Transport Services	S1:761-765
2.	Error And Flow Control	S1:765-768
3.	Connection Establishment And Release	S1:824-834
4.	Three Way Handshake	S1:834-844
5.	**Overview Of Application Layer Protocol**: Introduction Overview Of DNS Protocol	S1:851-868 S1:935-948
6.	Overview Of WWW Overview Of HTTP Protocol	S1:851-868
7.	Recapitulation and Possible Questions Discussion	
8.	Previous year end-semester question paper discussion	
9.	Previous year end-semester question paper discussion	
10.	Previous year end-semester question paper discussion	
Total No of hours for Unit 5:10		

Total hours: 48

Suggested Readings

1. Forouzan, B. A.(2007). Data Communications and Networking (4th ed.). New Delhi: THM.
2. Tanenbaum, A. S. (2002). Computer Networks (4th ed.). New Delhi: PHI.
3. Andrews S. Tanenbaum. 2003. Computer Networks. 4th Edition, Prentice Hall of India, New Delhi.
4. Douglas E. Comer. 2000. Computer Networks and Internets, 2nd Edition. Pearson Education Asia, New Delhi.
5. Stanford H.Rowe and Marsha L. Sehuh. 2005. computer Networking, 1st Edition, Pearson Education
6. William Stallings, 2007, Data and Communication Network, 8th Edition, Tata McGraw Hill, New Delhi.

Web Sites

W1. www.mhhe.com/engcs/compsci/fourouzan/
W2. http://compnetworking.about.com/od/basicnetworkingconcepts/a/network_types.htm
W3. www.amazon.com/Data-communication-Networking-Behrouz-Forouzan/dp/0072923547
W4. highered.mcgraw-hill.com/sites/0072515848/information_center_view0/
W5. en.wikipedia.org/wiki/Internet_protocol_suite
W6. http://docwiki.cisco.com/wiki/Introduction_to_WAN_Technologies
W7. www.yale.edu/pclt/COMM/**TCPIP**.HTM
W8. www.w3schools.com/**tcpip**/default.asp

Class: II BSc IT **Course Name: Data Communication and Networks**
Course Code: 18ITU402 **Unit: I** **Batch-2018-2021**

Data Communication and Networking

Unit I

Data Communication: An Overview – Protocols and Standards. Network Models: The OSI Model and Layers – TCP/IP Protocol Suite – Addressing. Physical Layer: Analog and Digital Signals –Data-Rates Limits , Digital to digital line encoding schemes-pulse code modulation: Parallel and serial transmission.

INTRODUCTION

An Overview of data communication and networking

Data: Data refers to information presented in whatever from is agreed upon by the parties creating and using the data.

Data Communication

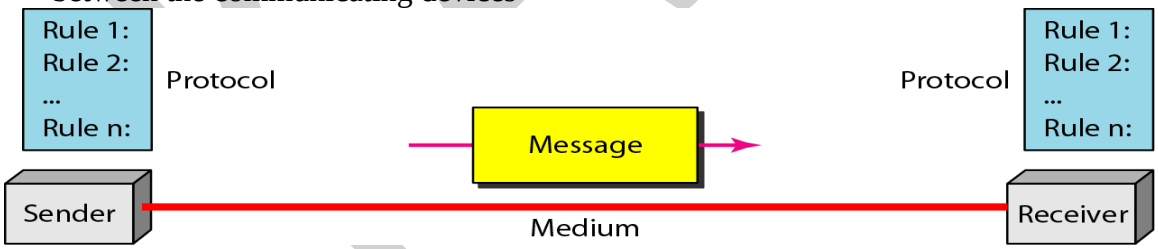
Networks exist so that data may be sent from one place to another. It is the exchange of data between two devices via some form of transmission medium such as a wire cable.

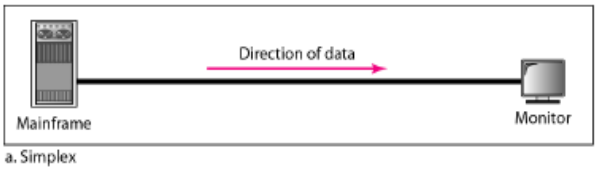
- For a communication to occur the communicating system must be made up of software and hardware
- Three fundamental characteristics for data communication system are
    1. Delivery- deliver data to correct destination
    2. Accuracy-must deliver the data accurately
    3. Timeliness- the system must deliver the data in a timely manner (eg: audio, video – real time transmission.
    4. Jitter- Jitter refers to the variation in the packet arrival time. It is the uneven delay in the delivery of audio or video packets.

Components of data communication:

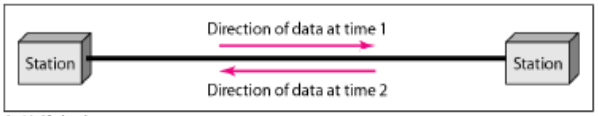
It has 5 components

1. Message: It is the information to be communicated. It consists of text, numbers, pictures, sound, or any combination of these.
2. Sender: it is a device that sends the data message. It can be a computer, workstation, telephone handset, video camera etc.
3. Receiver: it is a device which receives the message. It can be a computer, workstation etc.
4. Medium: The transmission medium is the physical path by which a message travels from sender to receiver. It can be twisted pair wire, coaxial cable, fiber optic cable, or radio waves.
5. Protocols: It is a set of rules that governs data communication. It represents an agreement between the communicating devices

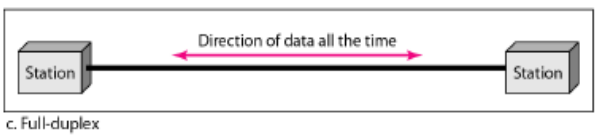




a. Simplex



b. Half-duplex



c. Full-duplex

Direction of data flow

a. Simplex: In this mode the communication is unidirectional eg. Keyboards, monitors

b. Half duplex: Each station can both transmit and receive but not at the same time, when one device is sending the other can only receive. (eg. Walkie talkies)

c. Full duplex: both stations can transmit and receive simultaneously. (eg: telephone networks)

Networks:

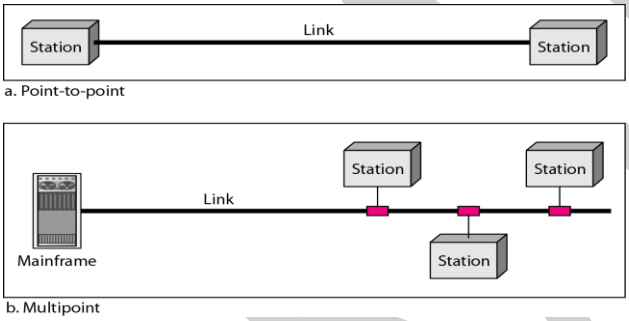
-A network is a set of devices (often referred to as nodes) connected by communication links. A node can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network.

-Data communication between remote parties can be achieved through a process called networking, involving the connection of computers, media and networking devices.

Network criteria

- Performance—Can be measured in may ways
  - transit time: amount of time required for a message to travel from one device to another
  - response time: time elapsed between an inquiry and a response
  - Number of users
  - Type of transmission medium
  - Hardware capabilities and software efficiency
- Reliability—A measure of frequency of failure and the time needed to recover, network robustness
- Security—Protecting of data from unauthorized users

Types of connections: point-to-point and multipoint



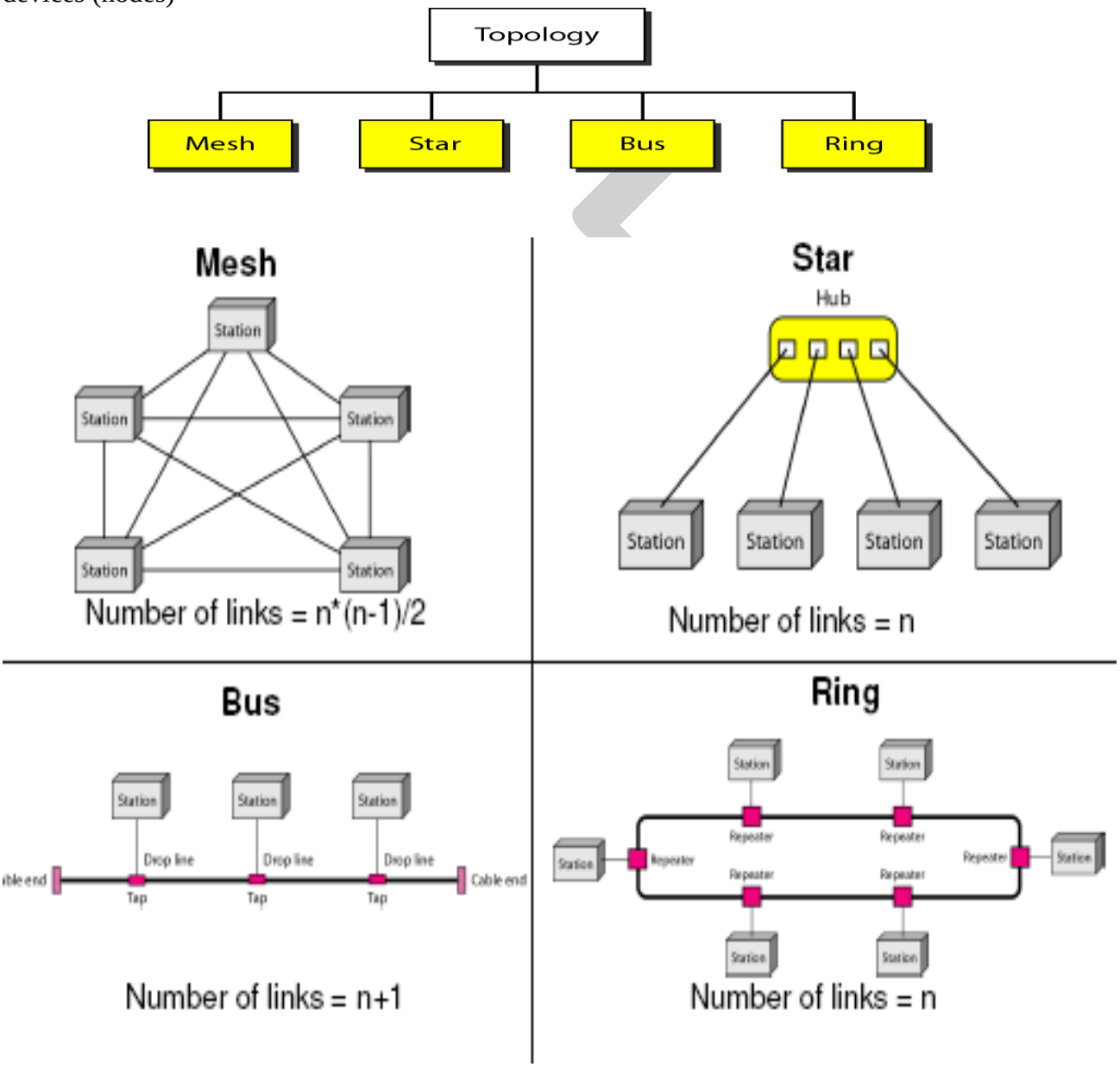
a) Point-to-Point A point-to-point connection provides a dedicated link between two devices. The entire capacity of the link is reserved for transmission between those two devices. Most point-to-point connections use an actual length of wire or cable to connect the two ends, but other options, such as microwave or satellite links, are also possible.

b) Multipoint A multipoint (also called multi drop) connection is one in which more than two specific devices share a single link. In a multipoint environment, the capacity of the channel is shared, either spatially or temporally. If several devices can use the link simultaneously, it is a *spatially shared* connection. If users must take turns, it is a *timeshared* connection.

Physical Topology

Physical topology refers to the way in which a network is laid out physically.

Network topology is the geometric representation of the relationship of all the links and linking devices (nodes)



Mesh Topology: In a mesh topology, every device has a dedicated point-to-point link to every other device. The term dedicated means that the link carries traffic only between the two devices it connects. To find the number of physical links in a fully connected mesh network with n nodes, we first consider that each node must be connected to every other node. Node 1 must be connected to n - I nodes, node 2 must be connected to n – 1 nodes, and finally node n must be connected to n - 1 nodes. We need n(n - 1) physical links. 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.

Advantages of Mesh Topology

- A 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.
- A mesh topology is robust. If one link becomes unusable, it does not incapacitate the entire system.
- There is the 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.
- Finally, point-to-point links make fault identification and fault isolation easy. Traffic can be routed to avoid links with suspected problems. This facility enables the network manager to discover the precise location of the fault and aids in finding its cause and solution.

Disadvantages of Mesh Topology

The main disadvantages of a mesh are related to the amount of cabling and the number of I/O ports required.

- First, because every device must be connected to every other device, installation and reconnection are difficult.
- Second, the sheer bulk of the wiring can be greater than the available space (in walls, ceilings, or floors) can accommodate.
- Finally, the hardware required to connect each link (I/O ports and cable) can be prohibitively expensive.
- For these reasons a mesh topology is usually implemented in a limited fashion, for example, as a backbone connecting the main computers of a hybrid network that can include several other topologies.

One practical example of a mesh topology is the connection of telephone regional offices in which each regional office needs to be connected to every other regional office.

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.

Advantages of Star Topology

- 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 which also makes it easy to install and reconfigure.
- Other advantages include 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.
- As long as the hub is working, it can be used to monitor link problems and bypass defective links.

Disadvantages of Star Topology

- 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.
- 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).

The star topology is used in local-area networks (LANs), High-speed LANs often use a star topology with a central hub.

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

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 of Bus Topology

- Advantages of a bus topology include ease of installation. Backbone cable can be laid along the most efficient path, then connected to the nodes by drop lines of various lengths. In this way, a bus uses less cabling than mesh or star topologies.
- In a star, for example, four network devices in the same room require four lengths of cable reaching all the way to the hub. In a bus, this redundancy is eliminated. Only the backbone cable stretches through the entire facility. Each drop line has to reach only as far as the nearest point on the backbone.

Disadvantages

- Disadvantages include 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. This degradation can be controlled by limiting the number and spacing of devices connected to a given length of cable.
- Adding new devices may therefore require modification or replacement of the backbone.
- In addition, a fault or break in the bus cable stops all transmission, even between devices on the same side of the problem.

Bus topology was the one of the first topologies used in the design of early local area networks. Ethernet LANs can use a bus topology, but they are less popular now.

Ring Topology

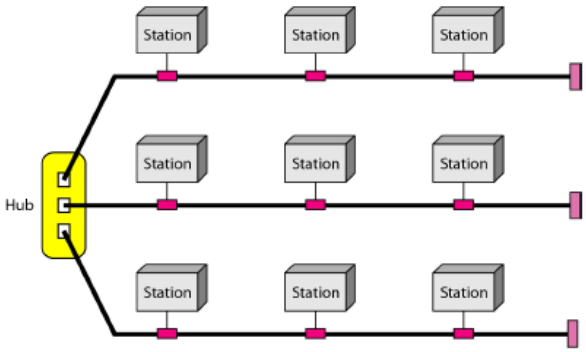
Ring Topology In a ring topology, each device has a dedicated point-to-point connection with only the two devices on either side of it. A signal is passed along the ring in one direction, from device to device, until it reaches its destination. Each device in the ring incorporates a repeater.

When a device receives a signal intended for another device, its repeater regenerates the bits and passes them along.

A 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. The only constraints are media and traffic considerations (maximum ring length and number of devices). In addition, fault isolation is simplified. Generally in a ring, a signal is circulating at all times. If one device does not receive a signal within a specified period, it can issue an alarm. The alarm alerts the network operator to the problem and its location. However, 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. This weakness can be solved by using a dual ring or a switch capable of closing off the break.

Ring topology was prevalent when IBM introduced its local-area network Token Ring. Today, the need for higher-speed LANs has made this topology less popular.

A hybrid topology

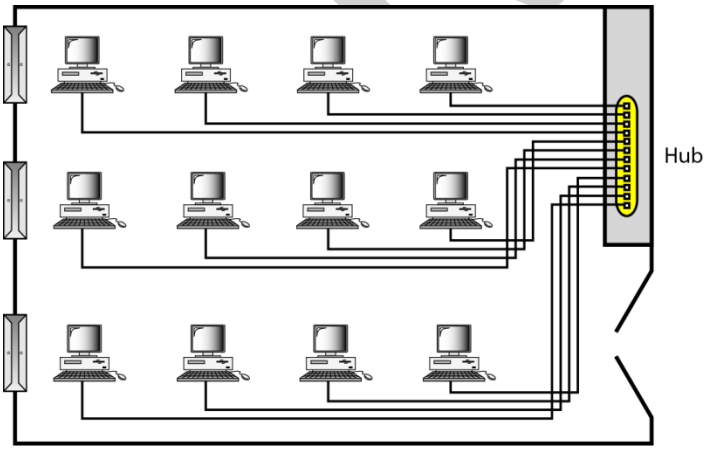


A network can be hybrid. For example, we can have a main star topology with each branch connecting several stations in a bus topology as shown in Figure below. A star backbone with three bus networks

Categories of networks

• Local Area Networks (LANs)

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

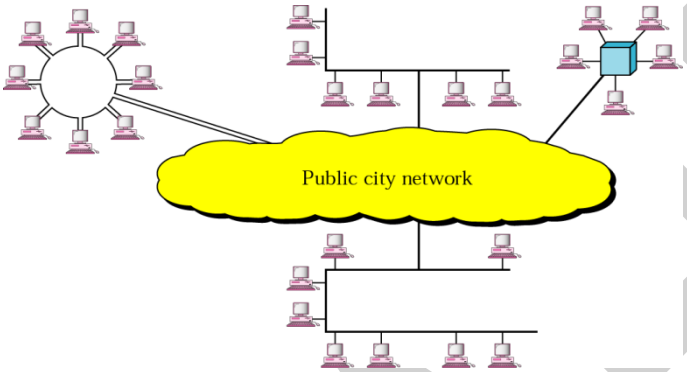


LANs are designed to allow resources to be shared between personal computers or workstations. The resources to be shared can include hardware (e.g., a printer), software (e.g., an application program), or data. A common example of a LAN, found in many business environments, links a workgroup of task-related computers, for example, engineering workstations or accounting PCs. One of the computers may be given a large capacity disk drive and may

become a server to clients. Software can be stored on this central server and used as needed by the whole group. In this example, the size of the LAN may be determined by licensing restrictions on the number of users per copy of software, or by restrictions on the number of users licensed to access the operating system.

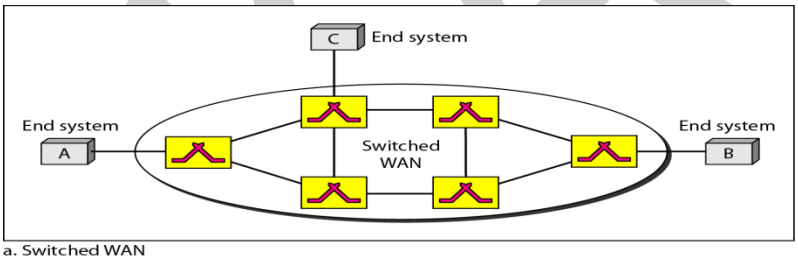
In addition to size, LANs are distinguished from other types of networks by their transmission media and topology. In general, a given LAN will use only one type of transmission medium. The most common LAN topologies are bus, ring, and star. Early LANs had data rates in the 4 to 16 megabits per second (Mbps) range. Today, however, speeds are normally 100 or 1000 Mbps

Metropolitan Area Networks (MANs)

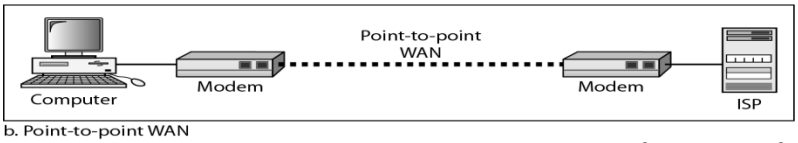


A metropolitan area network (MAN) is a network with a size between a LAN and a WAN. It normally covers the area inside a town or a city. It is designed for customers who need a high-speed connectivity, normally to the Internet, and have endpoints spread over a city or part of city. A good example of a MAN is the part of the telephone company network that can provide a high-speed DSL line to the customer. Another example is the cable TV network that originally was designed for cable TV, but today can also be used for high-speed data connection to the Internet

• Wide Area Networks (WANs)



a. Switched WAN



b. Point-to-point WAN

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

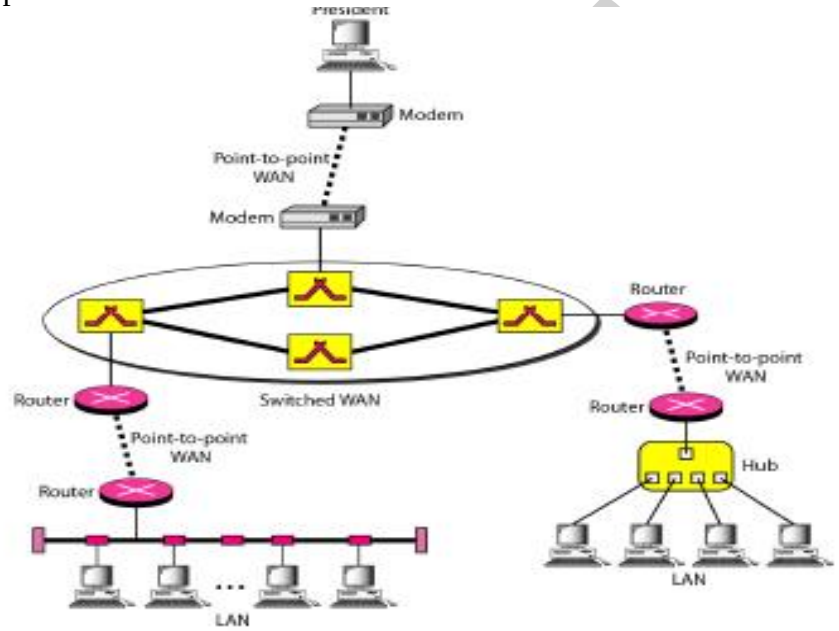
- The switched WAN connects the end systems, which usually comprise a router (internetworking connecting device) that connects to another LAN or WAN.
- The point-to-point WAN is normally a line leased from a telephone or cable TV provider that connects a home computer or a small LAN to an Internet service provider (lSP). This type of WAN is often used to provide Internet access.

• Internetworks

- Internetwork (internet) : two or more networks are connected by internetworking devices
- Internetworking devices: router, gateway, etc.
- The Internet: a specific worldwide network

An heterogeneous network

It is made up of made of four WANs and two LANs



Comparison of LANs, MANs, & WANs

Interprocessor distance	Processors located in same	Example
1 m	Square meter	Personal area network
10 m	Room	Local area network
100 m	Building	
1 km	Campus	
10 km	City	Metropolitan area network
100 km	Country	Wide area network
1000 km	Continent	
10,000 km	Planet	The Internet

LANs: 1 – 1000 Mbps

MANs: 10 – 40 Gbps

WANs: Tbps

THE INTERNET

The Internet has revolutionized many aspects off our daily lives. it has affected the way we do business as well as the way we spend our leisure time..

The Internet is a communication system that has brought a wealth off information to our finger tips and organized it for our use.

A brief history

• Mid-1960s

— Standalone devices

— ARPA (Advanced Research Projects Agency) was interested in finding a way to connect computers to share information

— Backbones: None - Hosts: None

• 1967

— ARPA presented its ideas for ARPANET

— Backbones: None - Hosts: None

• 1969

— The first physical network was constructed

— Backbones: 50Kbps ARPANET - Hosts: 4

• 1972

— The first e-mail program was created by Ray Tomlinson of BBN

— Backbones: 50Kbps ARPANET - Hosts: 23

• 1973

— Development began on the protocol later to be called TCP/IP (by Vint Cerf and Bob Kahn)

— Backbones: 50Kbps ARPANET - Hosts:> 23

PROTOCOLS AND STANDARDS

Protocols and standards. First, we define protocol, which is synonymous with rule. Then we discuss standards, which are agreed-upon rules.

Protocols

• A protocol is a set of rules that governs data communications

• It defines what is communicated, how it is communicated and when it is communicated

• Key elements of a protocol:

- **Syntax:** Structure or format of data, meaning the order in which they are presented
- **Semantics:** Refer to the meaning of each section of bits, how a particular pattern is interpreted and what action to be taken
- **Timing:** Refers to when data should be sent and how fast can they be sent

Standards

• Standards are essential in creating and maintaining an open and competitive market for equipment manufacturers

• Required to guarantee national and international interoperability of data and telecommunications technology and processes

• Categories of data communications standards

1. De facto: Standards that have not been approved by an organizational body but have been adopted through widespread use, eg. model TCP/IP)

2. De jure: Those that have been legislated by an official recognized body, eg. OSI model

Standards organizations

• Standards creation committees

— ISO (International Organization for Standardization)

— ITU-T (International Telecommunications Union – Telecommunications Standards)

• Initially known as CCITT (Consultative Committee for International Telegraphy and Telephony)

— ANSI (American National Standards Institute)

— IEEE (Institute of Electrical and Electronics Engineers)

— EIA (Electronic Industries Association

• Forums:

— Made up of representatives from interested corporations to speed acceptance and use of new technologies in the telecom industry

• Regulatory Agencies

— Governmental agencies: to protect public interest by regulating radio, TV and wire/cable communications

Internet standards

• An Internet standard is a thoroughly tested specification used by those who work with the Internet

• A specification begins with an Internet draft

—Working document with no official status and a 6- month lifetime

—Upon recommendation from the Internet authorities a draft may be published as a Request for Comment(RFC)

NETWORK MODELS

• A network uses a combination of hardware and software to send data from one location to another

—Hardware consists of the physical equipment that carries signals from one point of the network to another

—The task of sending a piece of information from one point in the works to another can be broken into several tasks, each performed by a separate software package

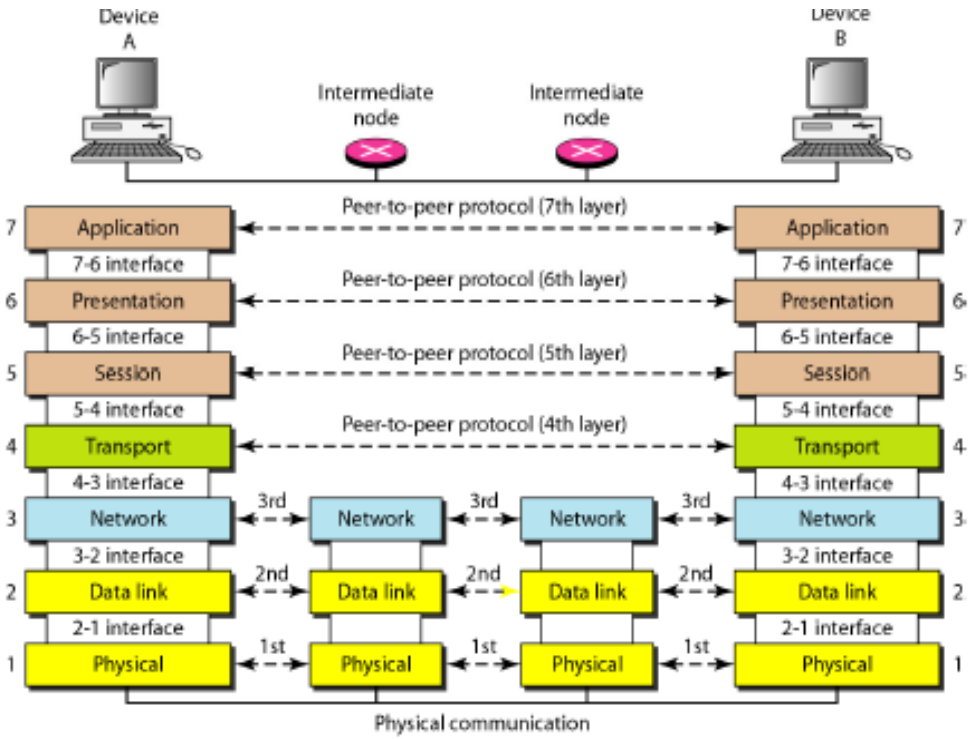
• Each piece of software uses the services of another software package to do its job

• At the lowest layer, a signal is sent from the source to the destination computer.

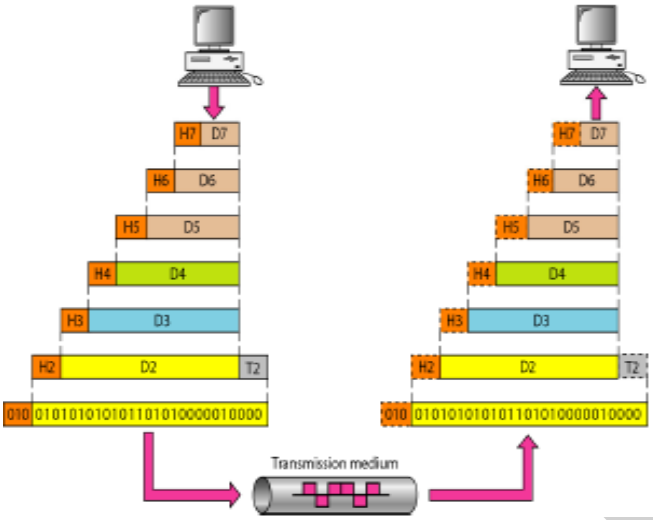
THE OSI MODEL

Established in 1947, the International Standards Organization (ISO) is a multinational body dedicated to world wide agreement on international standards. An ISO standard that covers all aspects of network communications is the Open Systems Interconnection (OSI) model. It was first introduced in the late 1970s.

Peer-to-peer processes



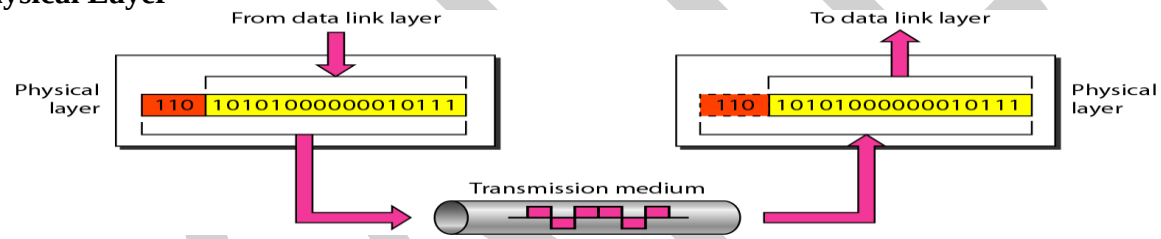
Encapsulation



- The process starts at layer 7 (application layer), then moves from layer to layer in descending, sequential order.
- At each layer, a **header** is added to the data unit.
- At layer 2, a **trailer** is added as well.
- When the formatted data unit passes through the physical layer (layer 1) it is changed into an electromagnetic or optical signal and transported along a physical link
- At the destination the reverse process is performed

THE OSI MODEL AND LAYERS

Physical Layer



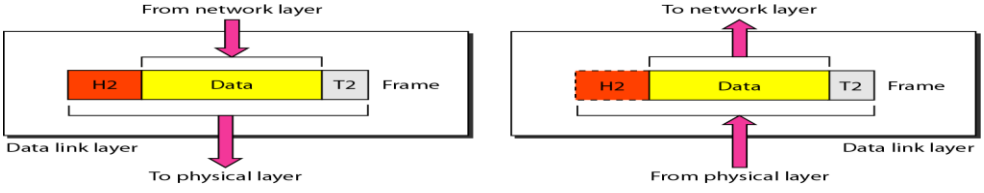
- The physical layer is responsible for movements of individual bits from one hop (node) to the next
- Mechanical and electrical specification, the procedures and functions

Duties:

- Physical characteristics of interfaces and media
- Representation of bits
- Data rate
- Synchronization of bits
- Line configuration
- Physical topology
- Transmission mode

Data link layer

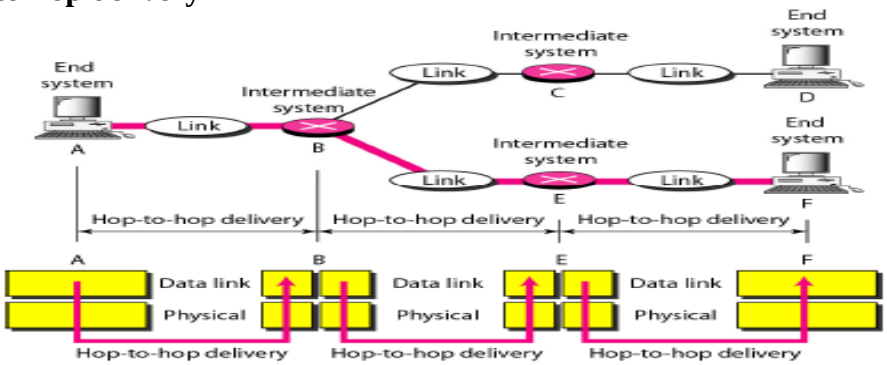
- The data link layer is responsible for moving frames from one hop (node) to the next
- Transform the physical layer to a reliable (error-free) link



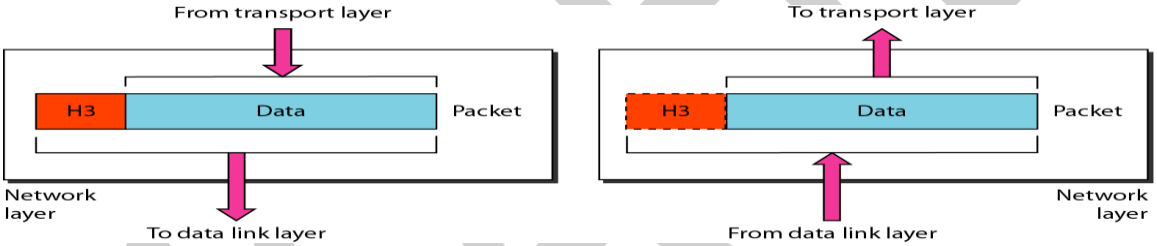
Duties:

- Framing
- Physical addressing
- Flow control
- Error control
- Access control

Hop-to-hop delivery



Network layer

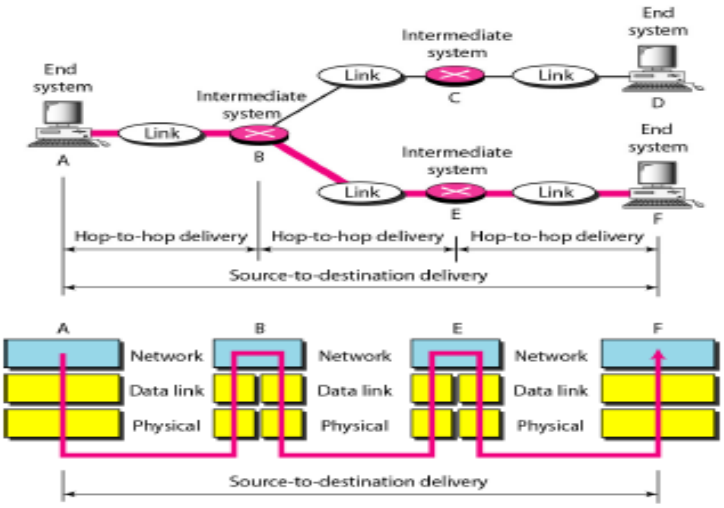


The network layer is responsible for the delivery of individual packets from the source host to the destination host.

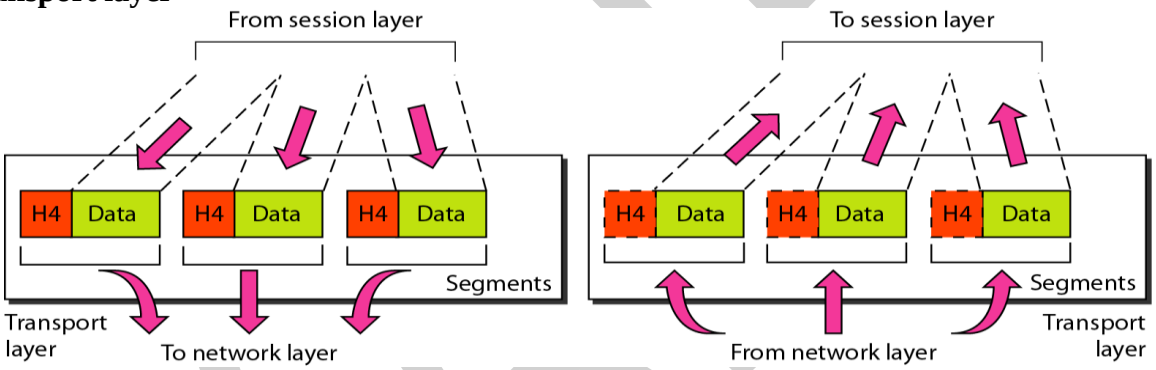
Duties:

- Logical addressing
- Routing

Source-to-destination delivery



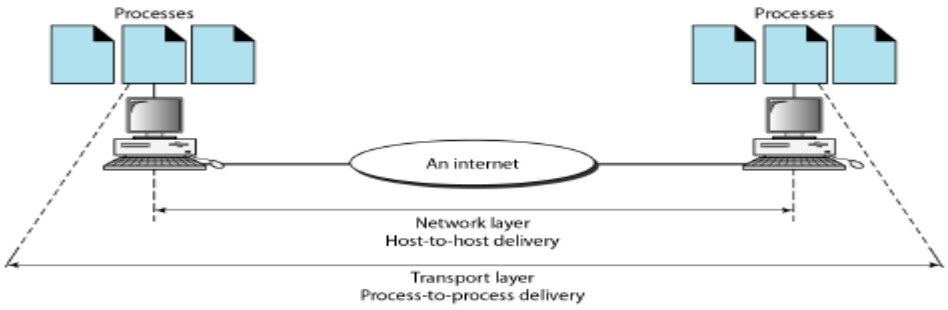
Transport layer



The transport layer is responsible for the delivery of a message from one process to another.
Duties:

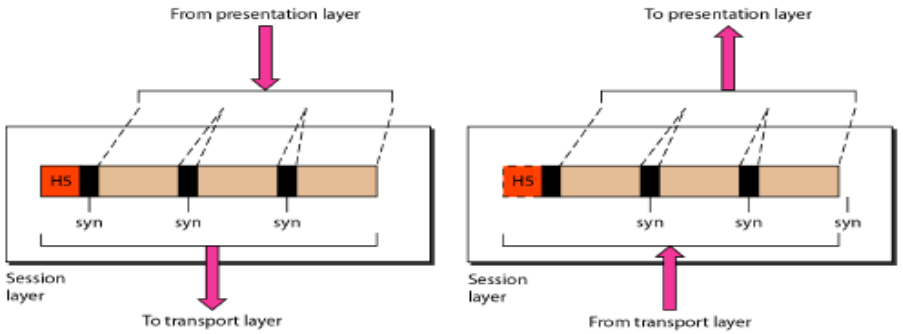
- Service-point (port) addressing
- Segmentation and reassembly
- Connection control
- Flow control
- Error control

Reliable process-to-process delivery



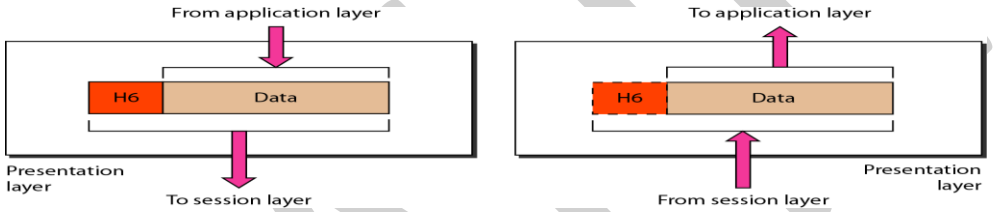
Session layer

The session layer is responsible for dialog control and synchronization.

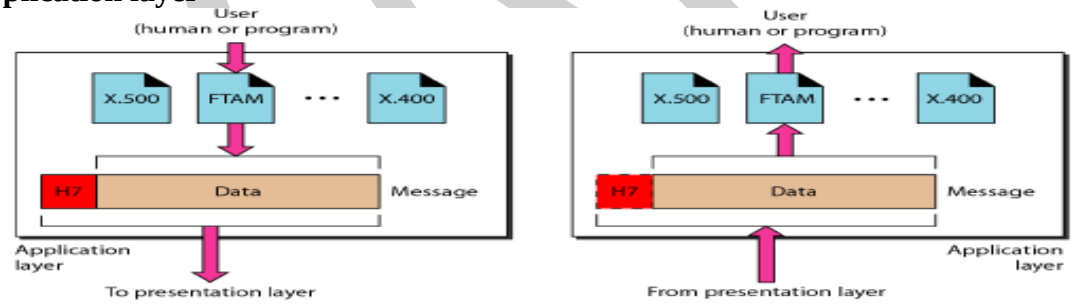


Presentation layer

The presentation layer is responsible for translation, compression, and encryption.



Application layer



The application layer is responsible for providing services to the user.

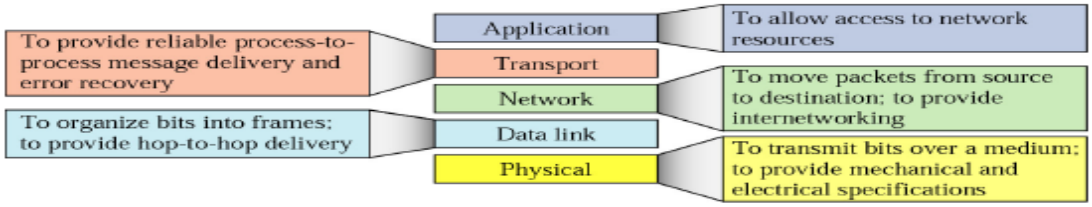
Services:

- Network virtual terminal
- Mail services
- File transfer, access, and management
- Directory services.

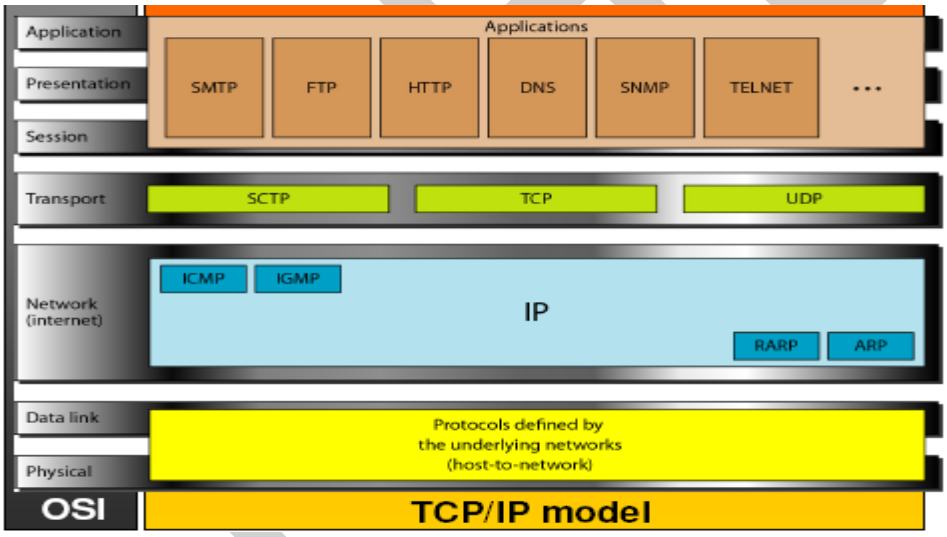
TCP/IP PROTOCOL SUITE

The layers in the TCP/IP protocol suite do not exactly match those in the OSI model. The original TCP//IP protocol suite was defined as having four layers:: host-to-network, internet, transport, and application. However, when TCP/IP is compared to OSI, we can say that the TCP/IP protocol suite is made of five layers: physical, data link, network,, transport, and application.

TCP/IP layers



TCP/IP and OSI model



ADDRESSING

Four levels of addresses are used in an internet employing the TCP/IP protocols: physical, logical, port, and specific.

• Physical address

In computer networks a physical address means a MAC (Medium Access Control) address. Also known as Ethernet Hardware Address (EHA) or hardware address or **adapter address.** It is a number that acts like a name for a particular networkadapter, eg. the network cards

• Logical address

—In computer networks, a logical address refers to a network layer address such as an IP address

—An IP address (Internet Protocol address) is a unique address that certain electronic devices use in order to identify and communicate with each other on a computer network utilizing the Internet Protocol standard (IP)

• **Port address**

—TCP and UDP are transport protocols used for communication between computers via ports

—The port numbers are divided into three ranges.

• The Well Known Ports are those in the range 0–1023.

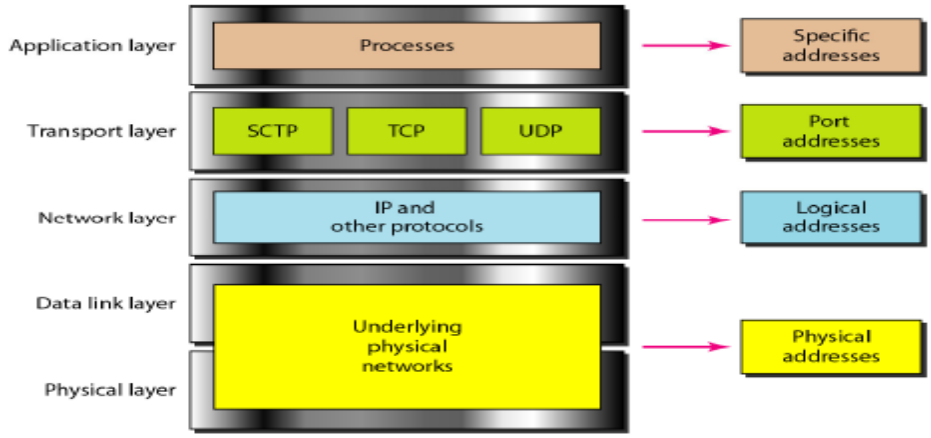
• The Registered Ports are those in the range 1024–49151.

• The Dynamic and/or Private Ports are those in the range 49152–65535. These ports are not used by any defined application.

• **Specific address**

—This address is used by application processes.

Relationship of layers-addresses in TCP/IP



PHYSICAL LAYER- ANALOG AND DIGITAL

Data can be analog or digital. The term analog data refers to information that is continuous; digital data refers to information that has discrete states. Analog data take on continuous values. Digital data take on discrete values.

Note -1

Data can be analog or digital.

Analog data are continuous and take continuous values.

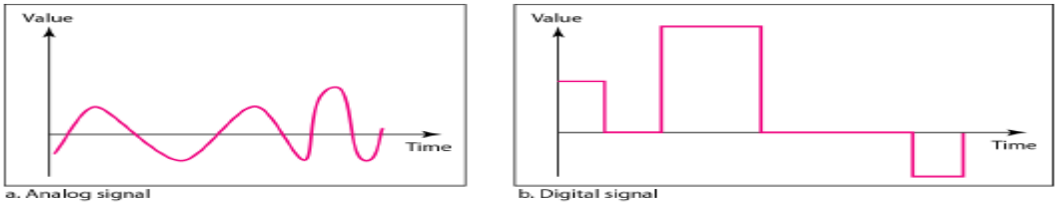
Digital data have discrete states and take discrete values.

Note-2

Signals can be analog or digital.

Analog signals can have an infinite number of values in a range;

Digital signals can have only a limited number of values.



a. Analog signal b. Digital signal

Periodic and Aperiodic signals or NonPeriodic
Both analog and digital signals can take one of two forms

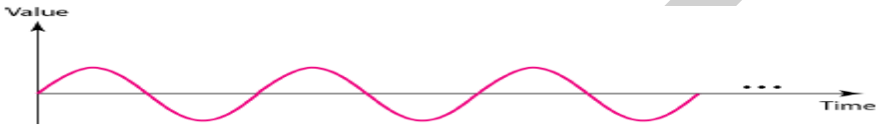
Periodic: completes a pattern within a measurable time frame called a period and repeats that pattern over subsequent identical periods

Nonperiodic: signal changes without exhibiting a pattern or cycle that repeats over time.

PERIODIC ANALOG SIGNALS

Periodic analog signals can be classified as simple or composite. A simple periodic analog signal, a sine wave, cannot be decomposed into simpler signals. A composite periodic analog signal is composed of multiple sine waves

A sine wave



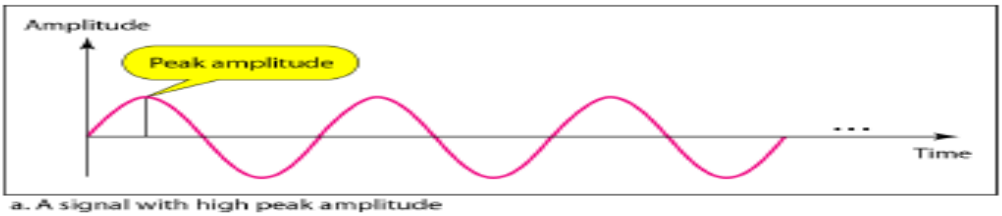
We can mathematically describe the sine wave as

$$s(t) = A\ sin(2\pi ft + \varphi)$$

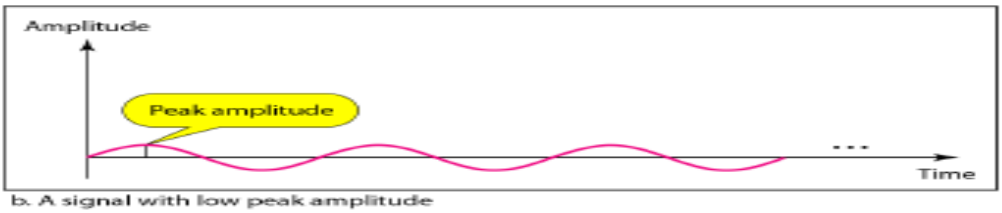
where, s is the instantaneous amplitude
A is the peak amplitude
f is the frequency
φ is the phase
t is the time
π is a constant (~3.14159)

Two signals

Same phase and frequency, but different amplitudes



a. A signal with high peak amplitude



b. A signal with low peak amplitude

Period and frequency

Period refers to the amount of time, in seconds, a signal needs to complete 1 cycle.

• Denoted by ***T***, measured in seconds.

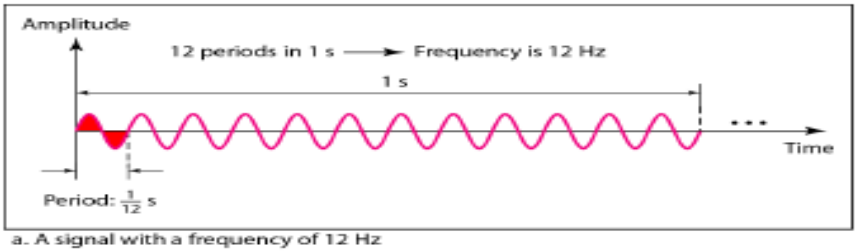
Frequency refers to the number of periods in one second

• Denoted by ***f***, measured in Hertz (Hz)

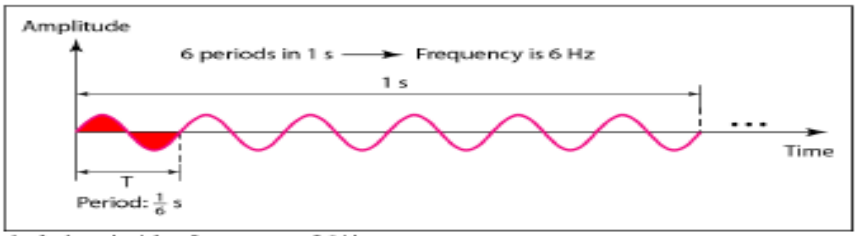
Frequency and period are the inverse of each other.

$$f = \frac{1}{T} \quad \text{and} \quad T = \frac{1}{f}$$

Two signals-Same amplitude and phase, but different frequencies



a. A signal with a frequency of 12 Hz



b. A signal with a frequency of 6 Hz

Units of period and frequency

Unit	*Equivalent*	*Unit*	*Equivalent*
Seconds (s)	1 s	Hertz (Hz)	1 Hz
Milliseconds (ms)	10^{-3} s	Kilohertz (kHz)	10^{3} Hz
Microseconds (µs)	10^{-6} s	Megahertz (MHz)	10^{6} Hz
Nanoseconds (ns)	10^{-9} s	Gigahertz (GHz)	10^{9} Hz
Picoseconds (ps)	10^{-12} s	Terahertz (THz)	10^{12} Hz

More about frequency

- **Frequency is the rate of change with respect to time.**
- **Change in a short span of time means high frequency.**
- **Change over a long span of time means low frequency.**

Two extremes

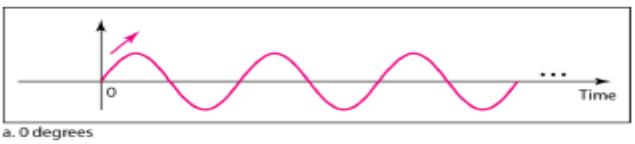
- **If a signal does not change at all, its frequency is zero.**
- **If a signal changes instantaneously, its frequency is infinite.**

Phase

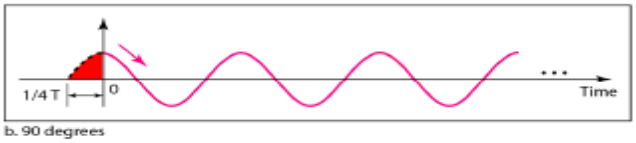
Phase describes the position of the waveform relative to time 0.

Three sine waves

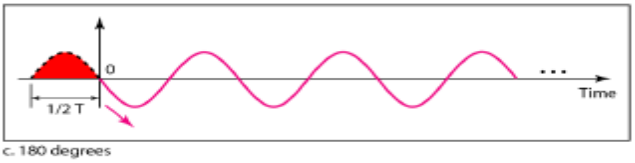
Same amplitude and frequency, but different phases



a. 0 degrees



b. 90 degrees

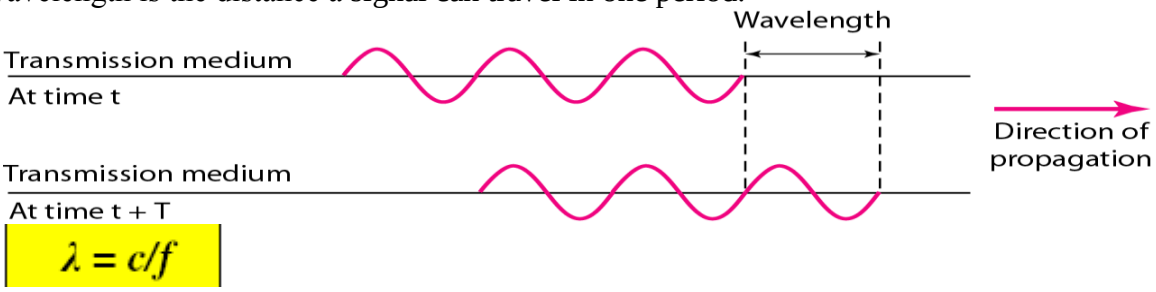


c. 180 degrees

Wavelength and period

Wavelength is another characteristic of a signal traveling through a transmission medium.

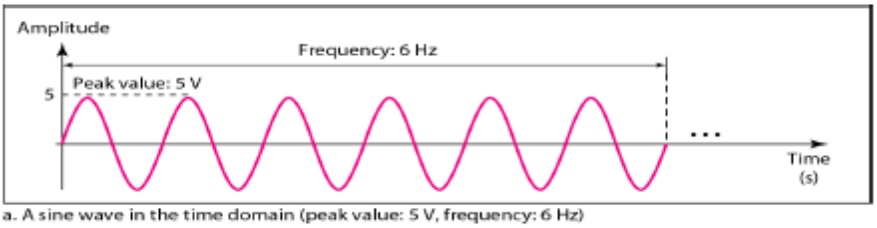
- The wavelength depends on both the frequency and the medium.
- The wavelength is the distance a signal can travel in one period.



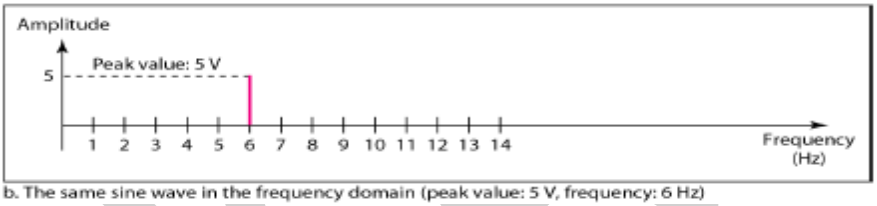
$$\lambda = c/f$$

where, λ is the wavelength
c is the speed of light (~3x108 m/s)
f is the frequency

Time-domain and frequency-domain plots of a sine wave



a. A sine wave in the time domain (peak value: 5 V, frequency: 6 Hz)

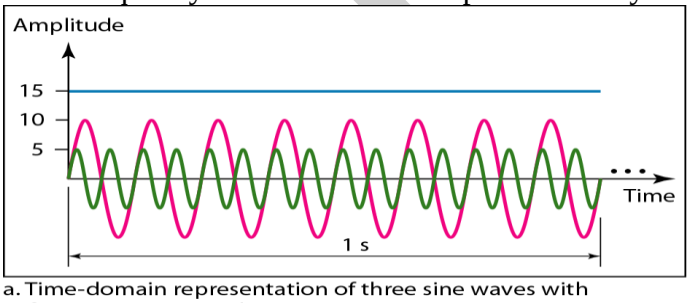


b. The same sine wave in the frequency domain (peak value: 5 V, frequency: 6 Hz)

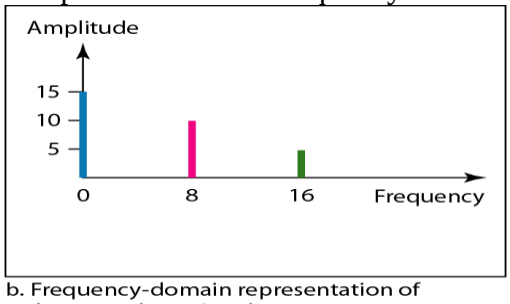
A complete sine wave in the time domain can be represented by one single spike in the frequency domain.

Example

The frequency domain is more compact and useful when we are dealing with more than one sine wave. For example, the following figure shows three sine waves, each with different amplitude and frequency. All can be represented by three spikes in the frequency domain.



a. Time-domain representation of three sine waves with frequencies 0, 8, and 16



b. Frequency-domain representation of the same three signals

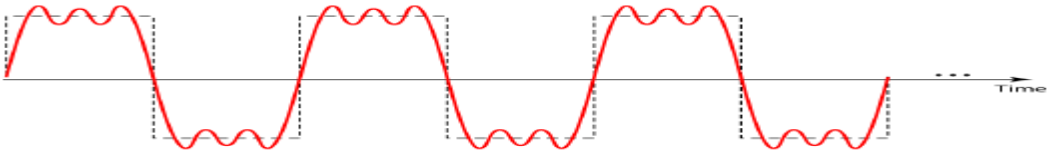
Composite signals

A single-frequency sine wave is not useful in data communications; we need to send a composite signal, a signal made of many simple sine waves**.**

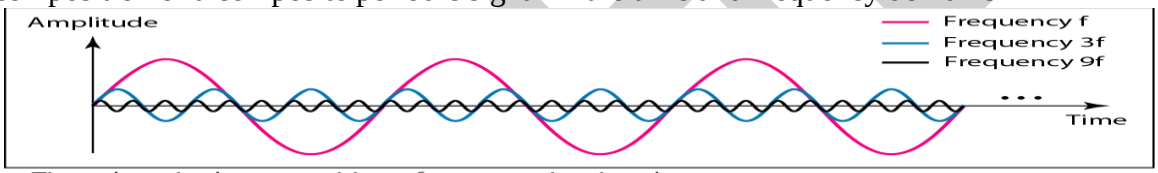
We can use a mathematical technique called **Fourier analysis** to show that any **periodic** signal is made up of an infinite series of sinusoidal frequency components.

If the composite signal is periodic, the decomposition gives a series of signals with discrete frequencies; if the composite signal is non-periodic, the decomposition gives a combination of sine waves with continuous frequencies.

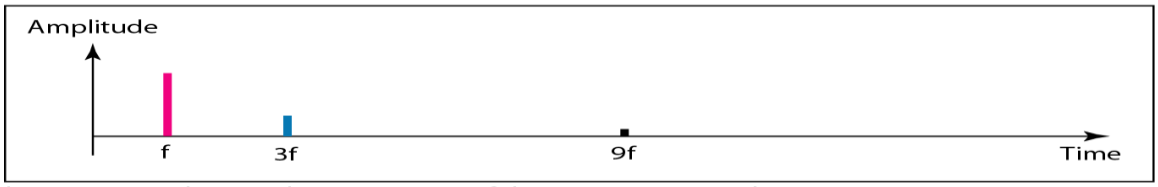
The figure shows a periodic composite signal with frequency ***f***. This type of signal is not typical of those found in data communications. We can consider it to be three alarm systems, each with a different frequency. The analysis of this signal can give us a good understanding of how to decompose signals.



Decomposition of a composite periodic signal in the time and frequency domains

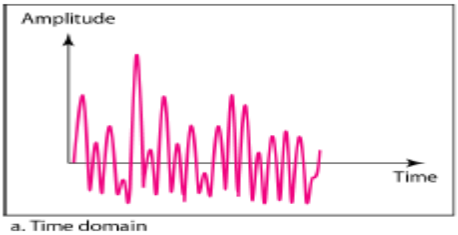


a. Time-domain decomposition of a composite signal

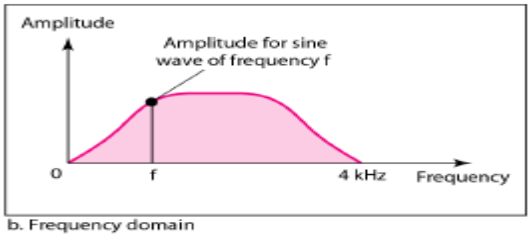


b. Frequency-domain decomposition of the composite signal

Example-The figure shows a non-periodic composite signal. It can be the signal created by a microphone or a telephone set when a word or two is pronounced. In this case, the composite signal cannot be periodic; because that implies that we are repeating the same word or words with exactly the same tone.



a. Time domain

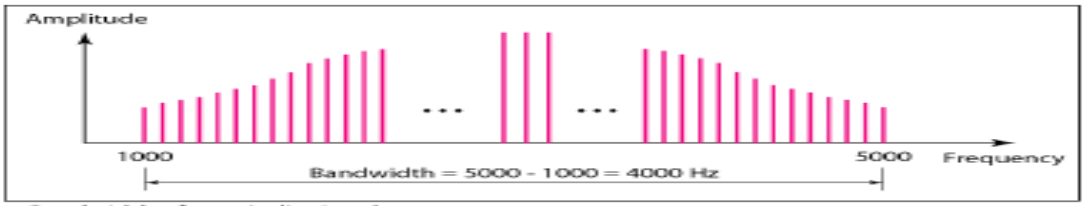


b. Frequency domain

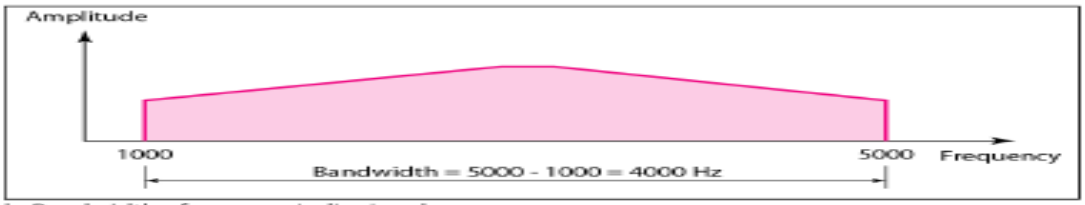
Bandwidth

The bandwidth of a composite signal is the difference between the highest and the lowest frequencies contained in that signal.

The bandwidth of periodic and non-periodic composite signals



a. Bandwidth of a periodic signal

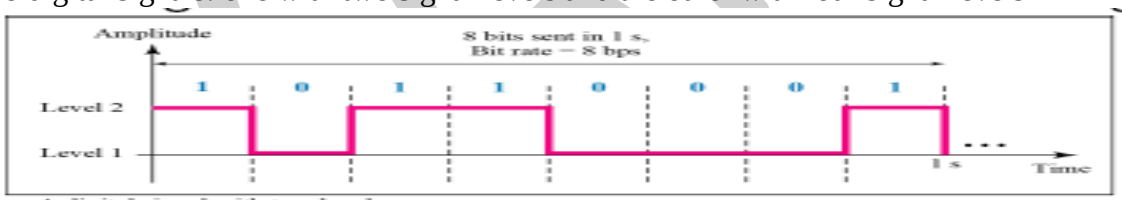


b. Bandwidth of a nonperiodic signal

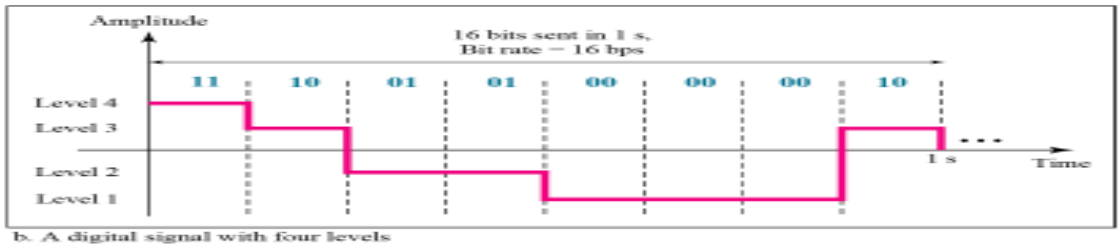
DIGITAL SIGNALS

In addition to being represented by an analog signal information can also be represented by a digital signal. For example, a 1 can be encoded as a positive voltage and a 0 as zero voltage. A digital signal can have more than two levels. In this case,, we can send more than 1 bit for each level.

Two digital signals: one with two signal levels and the other with four signal levels



a. A digital signal with two levels



b. A digital signal with four levels

Bit rate and bit interval

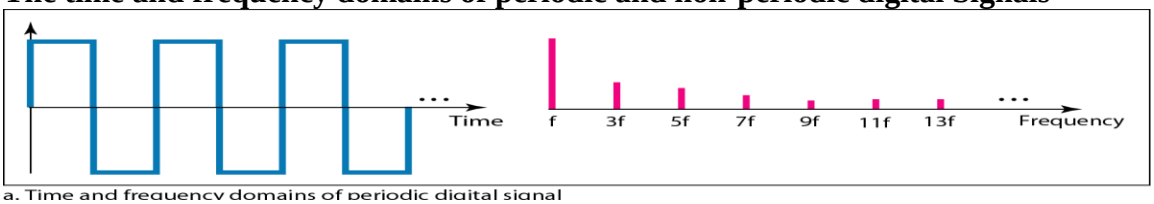
Most digital signals are aperiodic, so the period or frequency are not appropriate.

• Bit interval (instead of period) and bit rate (instead of frequency) are used to describe digital signals.

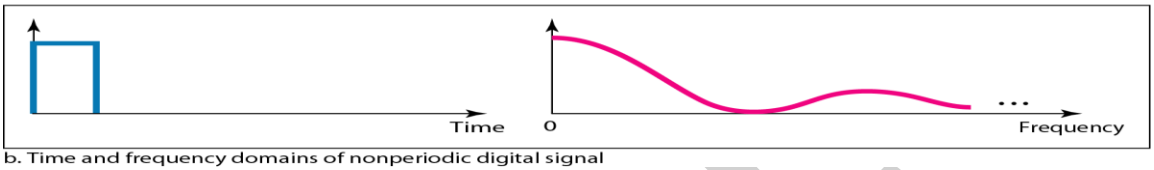
• Bit interval is the time required to send one single bit

• Bit rate is the number of bit intervals per second—Usually expressed as bits per second (bps)

The time and frequency domains of periodic and non-periodic digital Signals



a. Time and frequency domains of periodic digital signal

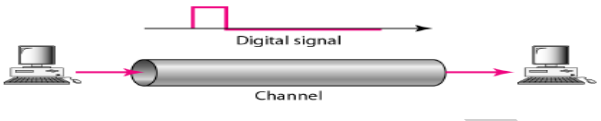


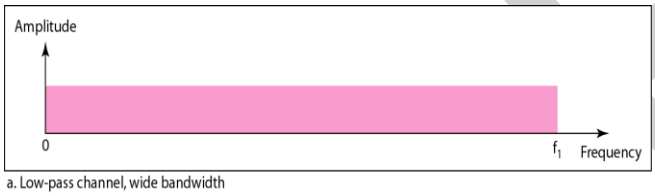
b. Time and frequency domains of nonperiodic digital signal

Baseband transmission

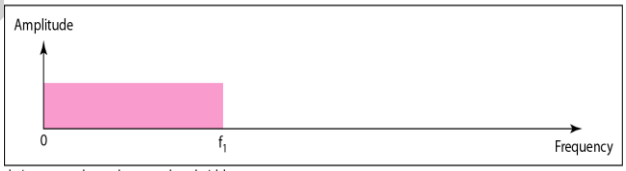
A digital signal is a composite analog signal with an infinite bandwidth.

Bandwidths of two low-pass channels





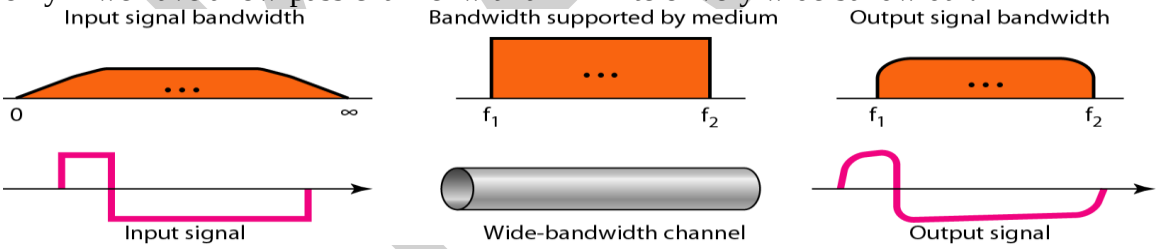
a. Low-pass channel, wide bandwidth



b. Low-pass channel, narrow bandwidth

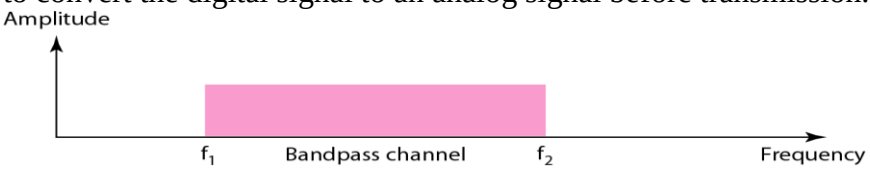
Baseband transmission using a dedicated medium

Baseband transmission of a digital signal that preserves the shape of the digital signal is possible only if we have a low-pass channel with an infinite or very wide bandwidth**.**



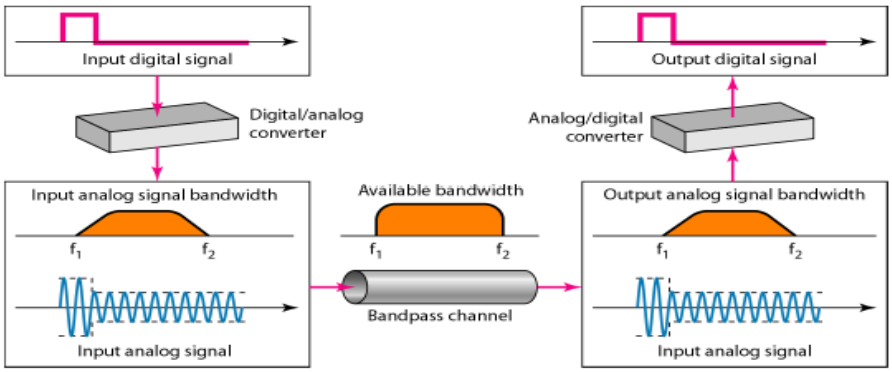
Broadband Transmission :

In broadband transmission the signal is converted to analog for transmission**.** If the available channel is a bandpass channel, we cannot send the digital signal directly to the channel; we need to convert the digital signal to an analog signal before transmission.



Modulation of a digital signal for transmission on a bandpass channel

An example of broadband transmission using modulation is the sending of computer data through a telephone subscriber line, the line connecting a resident to the central telephone office. These lines are designed to carry voice with a limited bandwidth. The channel is considered a bandpass channel. We convert the digital signal from the computer to an analog signal, and send the analog signal. We can install two converters to change the digital signal to analog and vice versa at the receiving end. The converter, in this case, is called a **modem**.



DATA RATE LIMITS

A very important consideration in data communications is how fast we can send data, in bits per second, over a channel.

Data rate depends on three factors:

1. The bandwidth available
2. The level of the signals we use
3. The quality of the channel (the level of noise)

Increasing the levels of a signal may reduce the reliability of the system.

Nyquist Theorem

For noiseless channel,

$$\text{BitRate} = 2 \times \text{Bandwith} \times \log_2 \text{Levels}$$

In baseband transmission, we said the bit rate is 2 times the bandwidth if we use only the first harmonic in the worst case.

However, the Nyquist formula is more general than what we derived intuitively; it can be applied to baseband transmission and modulation.

Also, it can be applied when we have two or more levels of signals.

Examples

Consider a noiseless channel with a bandwidth of 3000 Hz transmitting a signal with two signal levels. What is the maximum bit rate?

$$\text{BitRate} = 2 \times 3000 \times \log_2 2 = 6000 \text{ bps}$$

Consider the same noiseless channel transmitting a signal with four signal levels (for each level, we send 2 bits). What is the maximum bit rate

$$\text{BitRate} = 2 \times 3000 \times \log_2 4 = 12{,}000 \text{ bps}$$

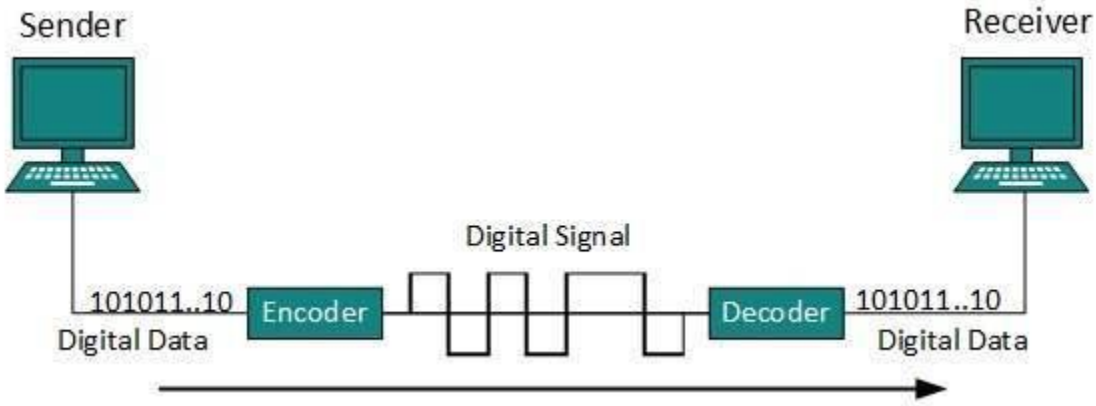
DIGITAL-TO-DIGITAL CONVERSION

Digital-to-Digital Conversion

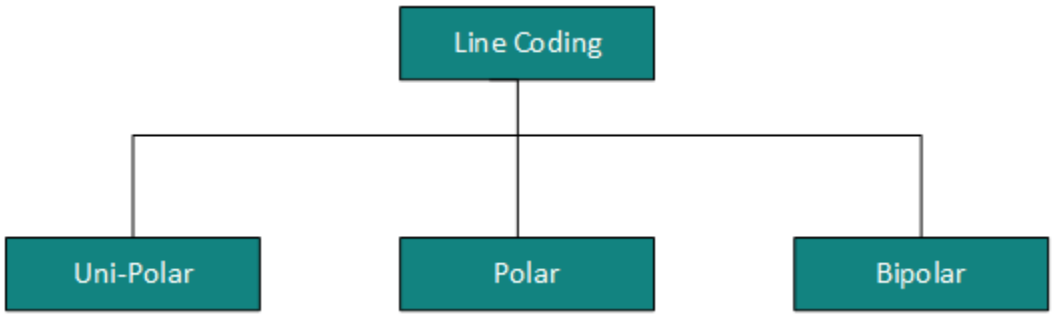
This section explains how to convert digital data into digital signals. It can be done in two ways, line coding and block coding. For all communications, line coding is necessary whereas block coding is optional.

Line Coding

The process for converting digital data into digital signal is said to be Line Coding. Digital data is found in binary format. It is represented (stored) internally as series of 1s and 0s.

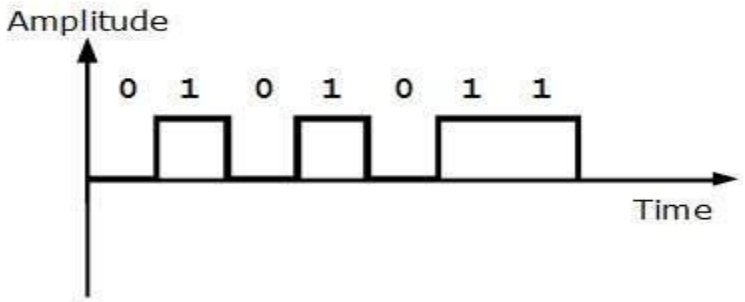


Digital signal is denoted by discreet signal, which represents digital data. There are three types of line coding schemes available:



Uni-polar Encoding

Unipolar encoding schemes use single voltage level to represent data. In this case, to represent binary 1, high voltage is transmitted and to represent 0, no voltage is transmitted. It is also called Unipolar-Non-return-to-zero, because there is no rest condition i.e. it either represents 1 or 0.



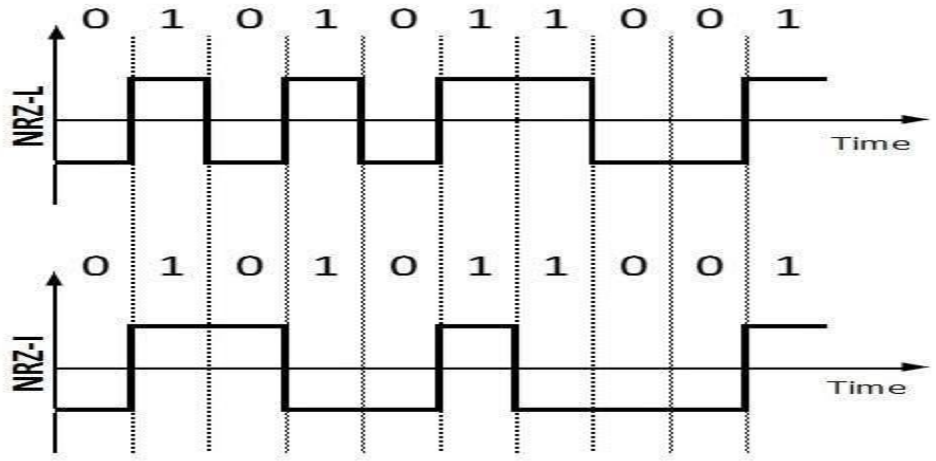
Polar Encoding

Polar encoding scheme uses multiple voltage levels to represent binary values. Polar encodings is available in four types:

- **Polar Non-Return to Zero (Polar NRZ)**

  It uses two different voltage levels to represent binary values. Generally, positive voltage represents 1 and negative value represents 0. It is also NRZ because there is no rest condition.

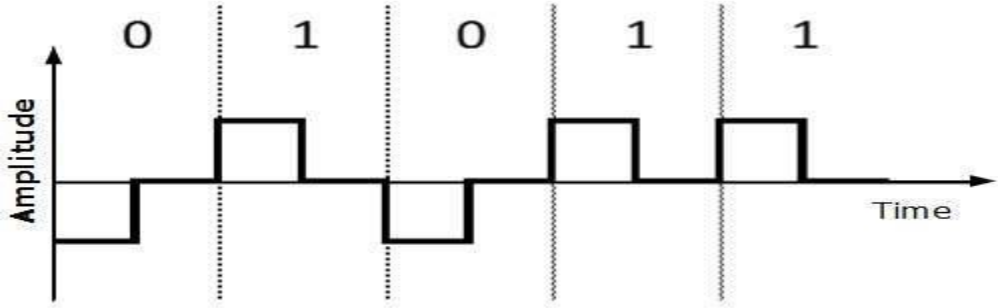
  NRZ scheme has two variants: NRZ-L and NRZ-I.



NRZ-L changes voltage level at when a different bit is encountered whereas NRZ-I changes voltage when a 1 is encountered.

- **Return to Zero (RZ)**

Problem with NRZ is that the receiver cannot conclude when a bit ended and when the next bit is started, in case when sender and receiver's clock are not synchronized.



RZ uses three voltage levels, positive voltage to represent 1, negative voltage to represent 0 and zero voltage for none. Signals change during bits not between bits.

- **Manchester**

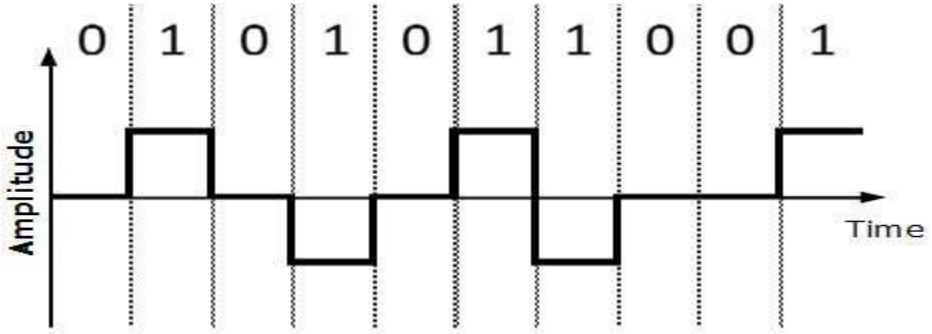
  This encoding scheme is a combination of RZ and NRZ-L. Bit time is divided into two halves. It transits in the middle of the bit and changes phase when a different bit is encountered.

- **Differential Manchester**

  This encoding scheme is a combination of RZ and NRZ-I. It also transit at the middle of the bit but changes phase only when 1 is encountered.

Bipolar Encoding

Bipolar encoding uses three voltage levels, positive, negative and zero. Zero voltage represents binary 0 and bit 1 is represented by altering positive and negative voltages



Block Coding

To ensure accuracy of the received data frame redundant bits are used. For example, in even-parity, one parity bit is added to make the count of 1s in the frame even. This way the original number of bits is increased. It is called Block Coding.

Block coding is represented by slash notation, mB/nB. Means, m-bit block is substituted with n-bit block where n > m. Block coding involves three steps:

- Division,
- Substitution
- Combination.

Analog-to-Digital Conversion

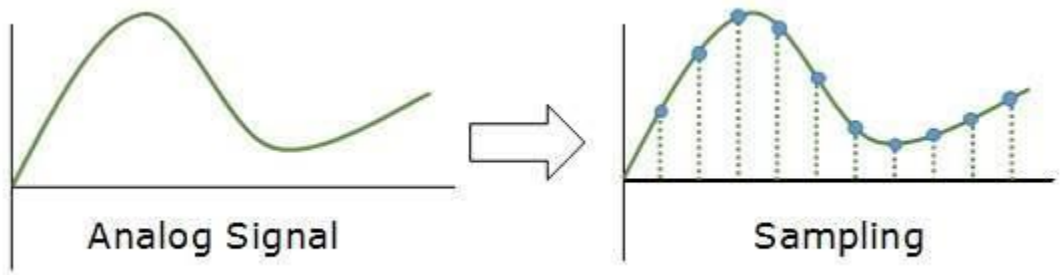
Microphones create analog voice and camera creates analog videos, which are treated is analog data. To transmit this analog data over digital signals, we need analog to digital conversion.

Analog data is a continuous stream of data in the wave form whereas digital data is discrete. To convert analog wave into digital data, we use Pulse Code Modulation (PCM).

PCM is one of the most commonly used method to convert analog data into digital form. It involves three steps:

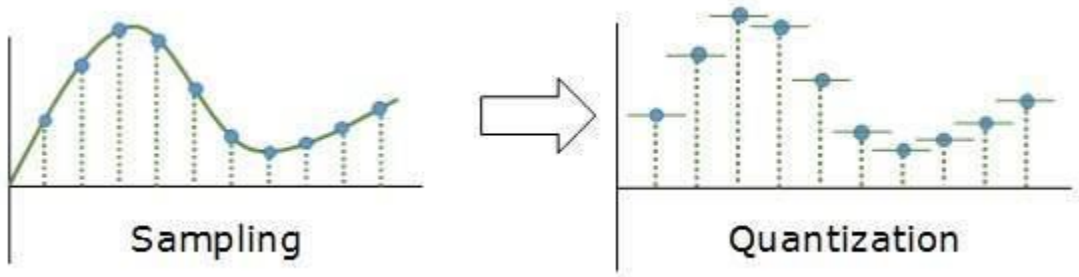
- Sampling
- Quantization

- Encoding.



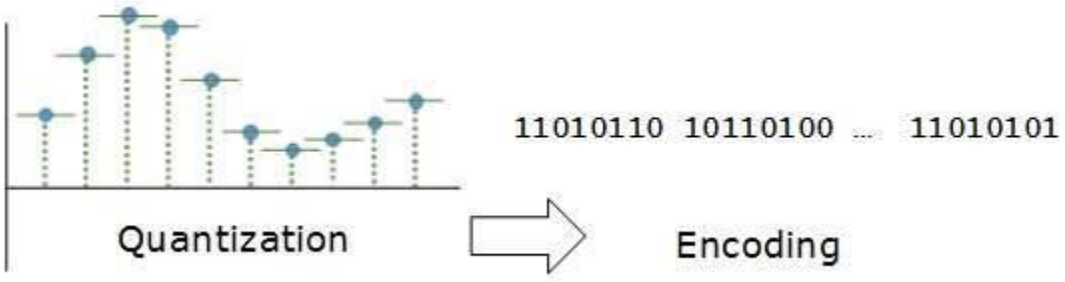
The analog signal is sampled every T interval. Most important factor in sampling is the rate at which analog signal is sampled. According to Nyquist Theorem, the sampling rate must be at least two times of the highest frequency of the signal.

Quantization



Sampling yields discrete form of continuous analog signal. Every discrete pattern shows the amplitude of the analog signal at that instance. The quantization is done between the maximum amplitude value and the minimum amplitude value. Quantization is approximation of the instantaneous analog value.

Encoding

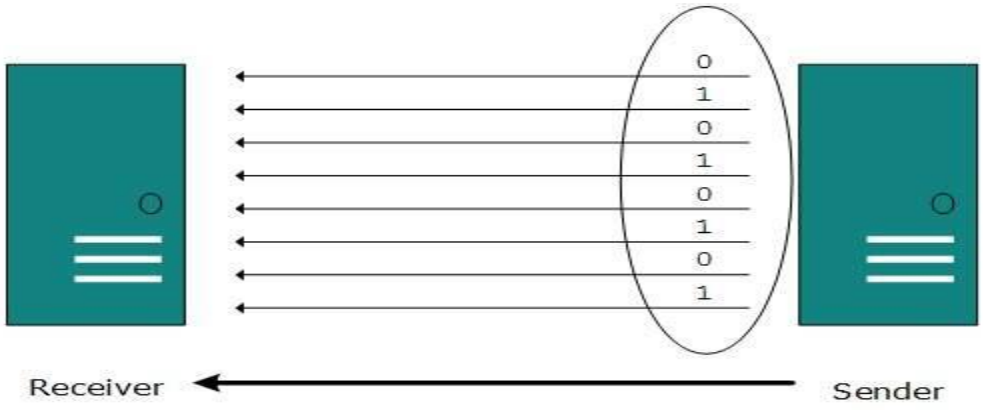


In encoding, each approximated value is then converted into binary format.

Transmission Modes

The transmission mode decides how data is transmitted between two computers. The binary data in the form of 1s and 0s can be sent in two different modes: Parallel and Serial.

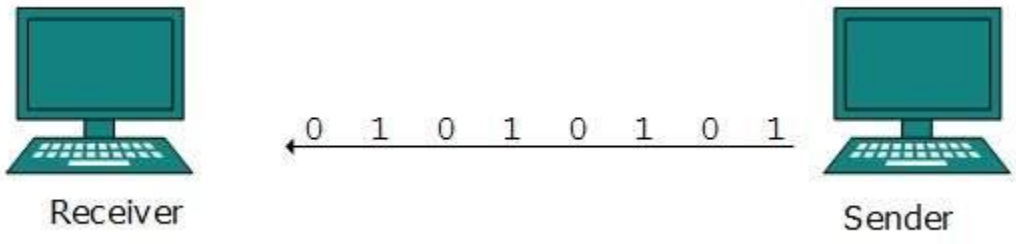
Parallel Transmission



The binary bits are organized in-to groups of fixed length. Both sender and receiver are connected in parallel with the equal number of data lines. Both computers distinguish between high order and low order data lines. The sender sends all the bits at once on all lines. Because the data lines are equal to the number of bits in a group or data frame, a complete group of bits (data frame) is sent in one go. Advantage of Parallel transmission is high speed and disadvantage is the cost of wires, as it is equal to the number of bits sent in parallel.

Serial Transmission

In serial transmission, bits are sent one after another in a queue manner. Serial transmission requires only one communication channel.



Serial transmission can be either asynchronous or synchronous.

Asynchronous Serial Transmission

It is named so because there ’is no importance of timing. Data-bits have specific pattern and they help receiver recognize the start and end data bits. For example, a 0 is prefixed on every data byte and one or more 1s are added at the end.

Two continuous data-frames (bytes) may have a gap between them.

Synchronous Serial Transmission

Timing in synchronous transmission has importance as there is no mechanism followed to recognize start and end data bits. There is no pattern or prefix/suffix method. Data bits are sent in burst mode without maintaining gap between bytes (8-bits). Single burst of data bits may contain a number of bytes. Therefore, timing becomes very important. It is up to the receiver to recognize and separate bits into bytes. The advantage of synchronous transmission is high speed, and it has no overhead of extra header and footer bits as in asynchronous transmission.

QUESTIONS

1) What are the fundamental characteristics and components of data communication
2) Describe protocols and standards
3) Write short note on analog and digital signals
4) Explain types of addressing with neat diagram
5) Discuss in briefly about transmission impairments
6) Describe categories of networks
7) Write short note on network layer in TCP/IP
8) Explain OSI reference model with a neat sketch
9) what are the four levels of addresses used in internet
10) How to measure the network performance explain?
11) Discuss about Analog to Digital Conversion.
12) Discuss about Pulse code Modulation.

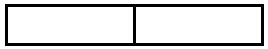
Questions	opt1	opt2	opt3	opt4	Answer
Data communication means exchange of data between _____devices.	one	two	six	four	two
The system must deliver data to the correct destination is called_____	accuracy	jitter	delivery	timeliness	delivery
A_____ is the set of rules.	protocols	transmission medium	networks	ip	protocols
In_____, the communication is unidirection.	duplex mode	full duplex mode	half duplex mode	simplex mode	simplex mode
A_____is a set of devices connected by communication links.	protocols	networks	computer	printer	networks
A_____connection provides a dedicated link between two devices.	point-to-point	multi-point	mesh	physical	point-to-point
One long cable acts as a _____to link all the devices in a network.	bus	mesh	hub	backbone	backbone
MAN stands for _____	metropolitician area network	metropolitan area network	metropolitical area network	macro area network	metropolitan area netwo
The term timing refers to _____ characteristics.	two	three	four	six	two
_____standards are often established originally by manufactures.	de jure	de facto	de fact	semantics	de facto
In physical layer we can transfer data into _____	frame	packet	bit	sp du	bit
Hob to hob delivery is done by the _____	session layer	datalink layer	network layer	transport layer	datalink layer
The _____layer is responsible for process to process delivery.	physical	presentation	networks	transport	transport

The _____layer is responsible for dialog control and synchronization.	transport	session	application	presentation	session
Tcp/Ip is a _____protocol.	hyper text	transfer	internet	hierarchical	hierarchical
Ip is a_____protocol.	hop to hop	node to node	process to process	host to host	host to host
A set of devices connected by a _____links	data	networks	communication	application	communication
Bus topology has a long link called_____	backbone	hub	host	hop	backbone
Periodic analog signals can be classified into _____	simple	composite	simple or composite	simple and composite	simple or composite
Period and frequency has the following formula.	f=1/t and t=1/f	t=1/f or f=1/t	c=t/f	t=c/f	f=1/t and t=1/f
Wavelength is_____	propagation speed	propagation speed * frequency	propagation speed/period	propagation speed/frequency	propagation speed/frequ
Composite signal can be classified into _____types	five	three	four	two	two
The range of frequency contained in a _____ signal is its bandwidth.	simple	composite	periodic	non periodic	composite
The bandwidth of the composite signal is the difference between the _____	highest	highest or lowest	highest and lowest	lowest	highest and lowest
The _____is the number of bits sent in a second.	bit length	bandpass	bandwidth	bit rate	bit rate
Bit length is _____	propagation speed/period	propagation speed * frequency	bit	propagation speed*bit duration	propagation speed*bit d

A_____signal is a composite analog signal with an infinite bandwidth	simple	composite	digital	analog	digital
Decibel (dB) =_____	10 log10 p2/p1	p1/p2	10 log10 p1/p2	2log10 p1/p2	10 log10 p2/p1
Transmission time=_____	message size/birate	distance/bandwidth	message size/distance	message size/bandwidth	message size/bandwidth
_____and star is a point to point device.	bus	ring	mesh	physical	mesh
Protocols can be classified into _____ key elements	one	three	four	two	three
_____is a basic key element.	protocols	standards	topology	protocols and standards	protocols and standards
Bit rate=_____	4*BW*log2L	2*BW*log2L	4*BW/L	2*BW*log 4L	2*BW*log2L
OSI stands for_____	open systems interconnection	open system internetworking	open symantic interconnection	open system internet	open systems interconne
Net work layer delivers data in the form of_____	frame	bits	data	packet	packet
Session layer provides_____ services.	one	two	three	four	two
UDP _____	user data protocol	user datagram protocol	user defined protocol	user dataframe protocol	user datagram protocol
FTP_____	file transmit protocol	file transmission protocol	file transfer protocol	flip transfer protocol	file transfer protocol
SMTP_____	single mail transfer protocol	simple mail transfer protocol	simple mail transmission protocol	single mail transmit protocol	simple mail transfer pro
Complete a cycle is called as _____	period	frequency	non periodic	periodic	period
Jitter is a form of_____	frames	bits	packets	dp tu	packets
Each set is called a _____	node	code	unicode	polar	node

Full duplex also called as_____	simple duplex	single duplex	multiple duplex	duplex	duplex
_____can be measured in transmit time and response time.	performance	frequency	period	non period	performance
A multipoint is also called as_____	multi line	multi drop	multi level	single level	multi drop
Mesh topology we need _____	n(n-1)	n(n+1)	n(n+1)/2	n(n-1)/2	n(n-1)/2
A_____topology on the other hand is multipoint.	star	ring	bus	mesh	bus
A_____can be hybrid	physical	networks	data	link	networks
A MAN is a network with a size between a _____ and _____.	WAN and LAN	WAN or LAN	LAN	WAN	WAN and LAN
When Two or more networks are connected they become an _____	network	inter network	internet connection	interconnection	inter network
The_____layer is responsible for providing services to the user.	presentation	datalink	application	network	application
The _____ layer is responsible for translation, compression encryption.	transport	data link	presentation	application	presentation
The_____layer is responsible for the delivery of a message from one process to another.	data link	transport	presentation	network	transport
A _____layer is responsible for the delivery of packets from the source to destination.	physical	data link	network	session	network
The _____layer is responsible for moving frames from one hop to the next.	data link	physical	network	presentation	data link

The _____layer is responsible for movements of bits from one hop to next.	data link	physical	transport	session	physical
RARP _____	reverse address resolution protocol	reverse address result protocol	reverse addess revolutinized protocol	reverse addess research protocol	reverse address resolutic
_____does not define any specific protocol.	TCP	HTTP	TCP/IP	SMTP	TCP/IP
The TCP/IP protocol suite was developed prior to the_____model.	OSI	ISO	TCP	IP	OSI
The _____layer is responsible for flow control.	session	presentation	application	transport	transport
The term _____ data refers to information continous	analog	digital	physical	analog and digital	analog
The sine wave is the most fundamental form of a _____analog signal.	composite	single	periodic	non periodic	periodic



rk

ency

uration

ection

tocol

ɔn protocol

Data Communication and Networking

Unit II

Multiplexing – Frequency Division Multiplexing-Wavelength Division Multiplexing– Synchronous Time-Division Multiplexing– Statistical Time Division Multiplexing. Transmission Media - Guided Media- Twisted pair and coaxial cable - Fiber optic cable-Unguided Transmission Media Switching – Circuit Switched Networks-Datagram Networks – Virtual Circuit networks.

Unit II

(cont..) Digital to analog modulation-; multiplexing techniques- FDM, TDM; transmission media. **Networks Switching Techniques and Access mechanisms:** Circuit switching; packet switching - connectionless datagram switching, connection-oriented virtual circuit switching; dial-up modems; digital subscriber line; cable TV for data transfer.

Digital to analog modulation

To send the digital data over an analog media, it needs to be converted into analog signal. There can be two cases according to data formatting.

Band pass: The filters are used to filter and pass frequencies of interest. A band pass is a band of frequencies which can pass the filter.

Low-pass: Low-pass is a filter that passes low frequencies signals.

When digital data is converted into a band pass analog signal, it is called digital-to-analog conversion. When low-pass analog signal is converted into band pass analog signal, it is called analog-to-analog conversion.

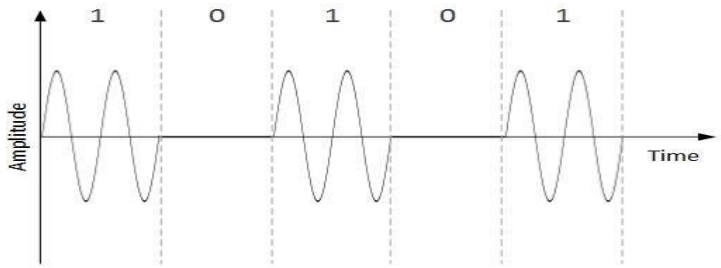
Digital-to-Analog Conversion

When data from one computer is sent to another via some analog carrier, it is first converted into analog signals. Analog signals are modified to reflect digital data.

An analog signal is characterized by its amplitude, frequency, and phase. There are three kinds of digital-to-analog conversions:

- **Amplitude Shift Keying**

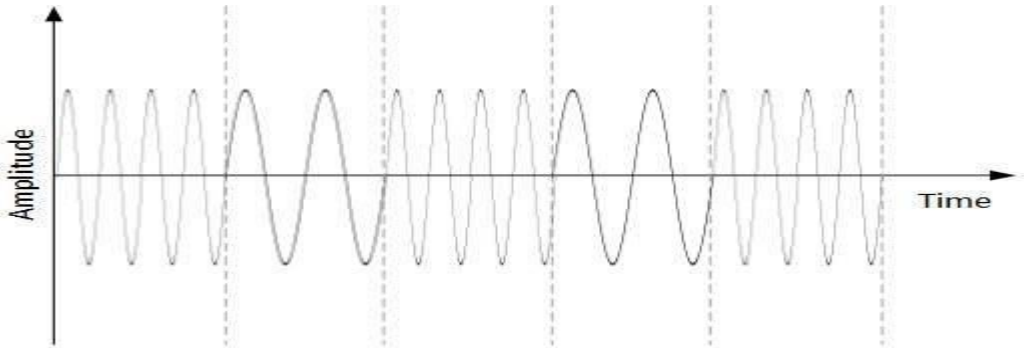
  In this conversion technique, the amplitude of analog carrier signal is modified to reflect binary data.



- When binary data represents digit 1, the amplitude is held; otherwise it is set to 0. Both frequency and phase remain same as in the original carrier signal.

  Frequency Shift Keying

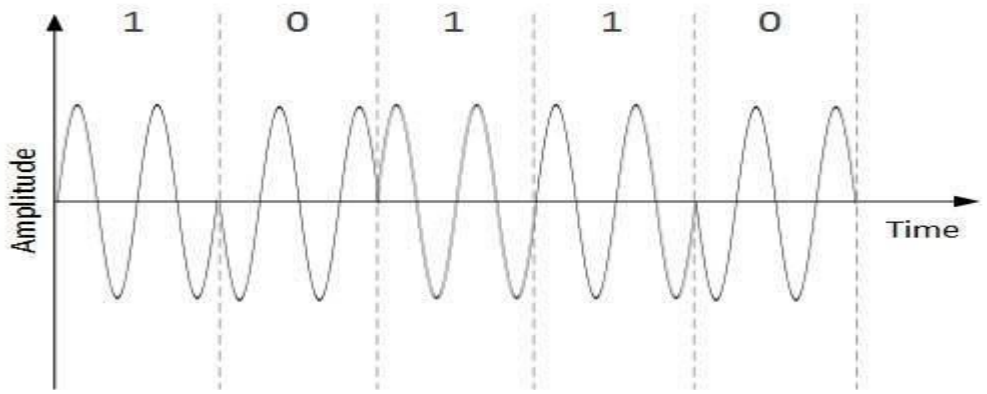
In this conversion technique, the frequency of the analog carrier signal is modified to reflect binary data.



- This technique uses two frequencies, f1 and f2. One of them, for example f1, is chosen to represent binary digit 1 and the other one is used to represent binary digit 0. Both amplitude and phase of the carrier wave are kept intact.

Phase Shift Keying

In this conversion scheme, the phase of the original carrier signal is altered to reflect the binary data.



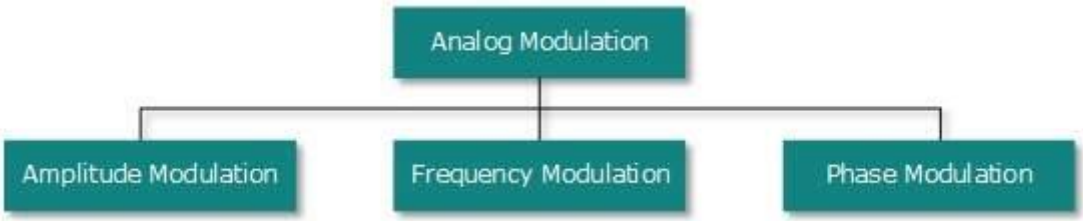
When a new binary symbol is encountered, the phase of the signal is altered. Amplitude and frequency of the original carrier signal is kept intact.

Quadrature Phase Shift Keying

QPSK alters the phase to reflect two binary digits at once. This is done in two different phases. The main stream of binary data is divided equally into two sub-streams. The serial data is converted in to parallel in both sub-streams and then each stream is converted to digital signal using NRZ technique. Later, both the digital signals are merged together.

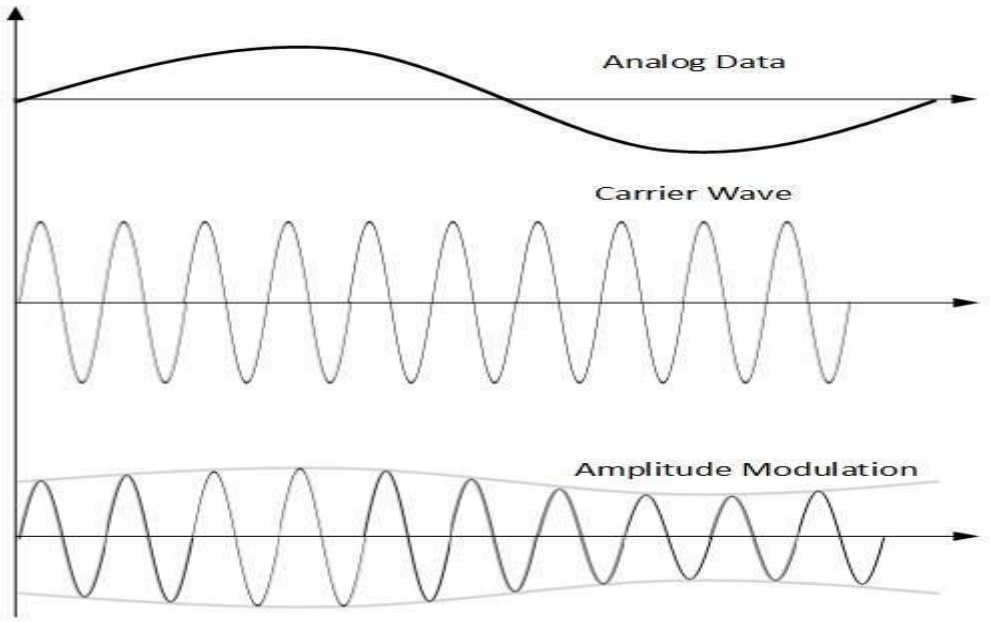
Analog-to-Analog Conversion

Analog signals are modified to represent analog data. This conversion is also known as Analog Modulation. Analog modulation is required when bandpass is used. Analog to analog conversion can be done in three ways:



Amplitude Modulation

In this modulation, the amplitude of the carrier signal is modified to reflect the analog data.

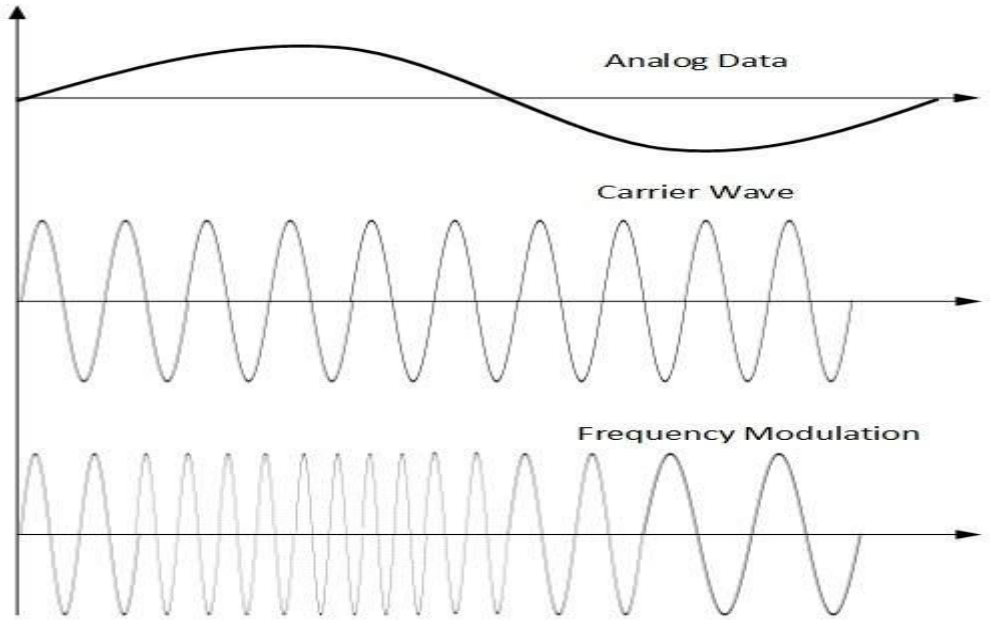


- Amplitude modulation is implemented by means of a multiplier. The amplitude of modulating signal (analog data) is multiplied by the amplitude of carrier frequency, which then reflects analog data.

  The frequency and phase of carrier signal remain unchanged.

Frequency Modulation

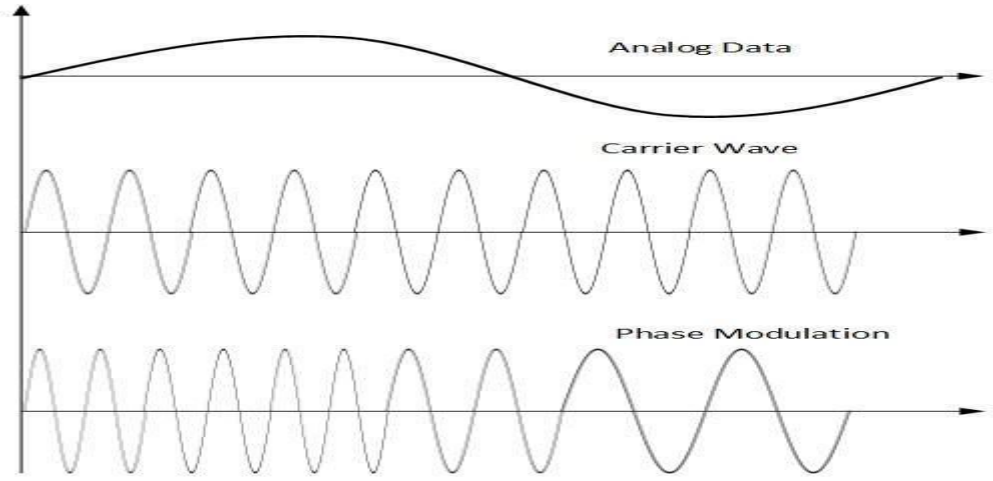
In this modulation technique, the frequency of the carrier signal is modified to reflect the change in the voltage levels of the modulating signal (analog data).



- The amplitude and phase of the carrier signal are not altered.

Phase Modulation

In the modulation technique, the phase of carrier signal is modulated in order to reflect the change in voltage (amplitude) of analog data signal.



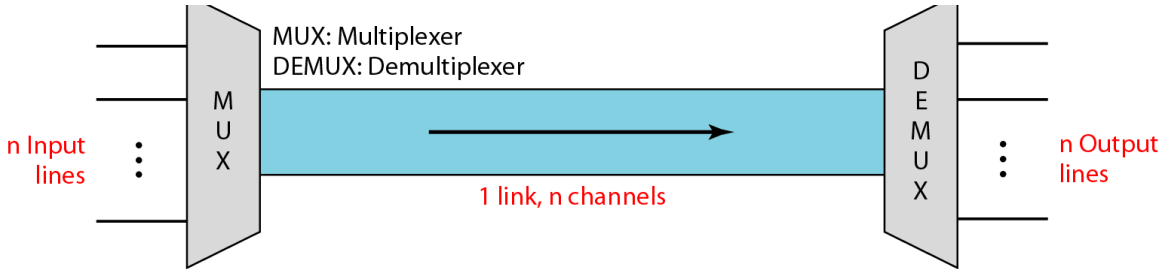
Phase modulation is practically similar to Frequency Modulation, but in Phase modulation frequency of the carrier signal is not increased. Frequency of carrier is signal is changed (made dense and sparse) to reflect voltage change in the amplitude of modulating signal.

MULTIPLEXING

Whenever the bandwidth of a medium linking two devices is greater than the bandwidth needs of the devices, the link can be shared. Multiplexing is the set off techniques that allows the simultaneous transmission of multiple signals across a single data link. As data and telecommunications use increases, so does traffic.

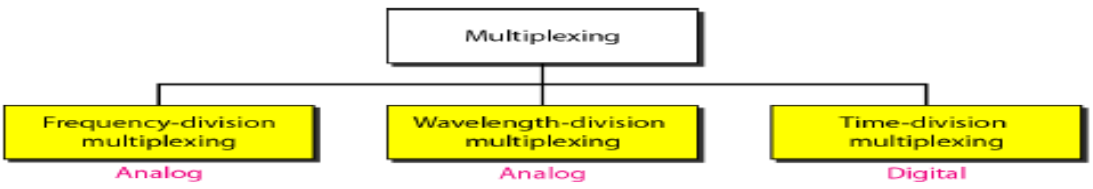
Dividing a link into channels

In a multiplexed system, *n* lines share the bandwidth of one link. 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-to-one). 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. In the figure, the word link refers to the physical path. The word channel refers to the portion of a link that carries a transmission between a given pair of lines. One link can have many *(n)* channels.



Categories of multiplexing

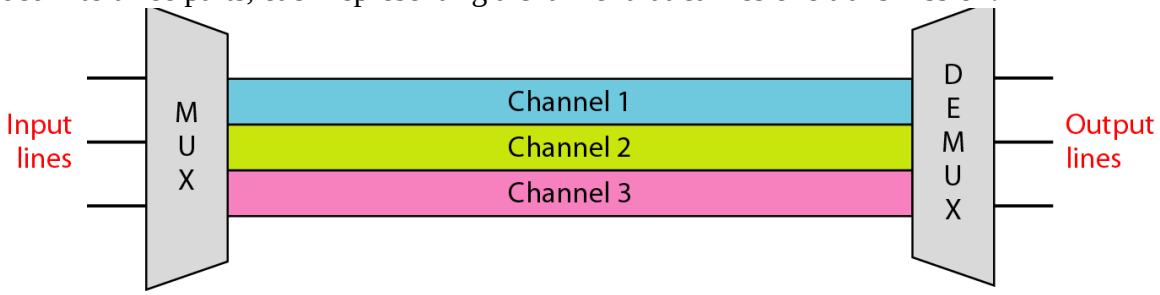
There are three basic multiplexing techniques: frequency-division multiplexing, wavelength-division multiplexing, and time-division multiplexing. The first two are techniques designed for analog signals, the third, for digital signals



Frequency Division Multiplexing (FDM)

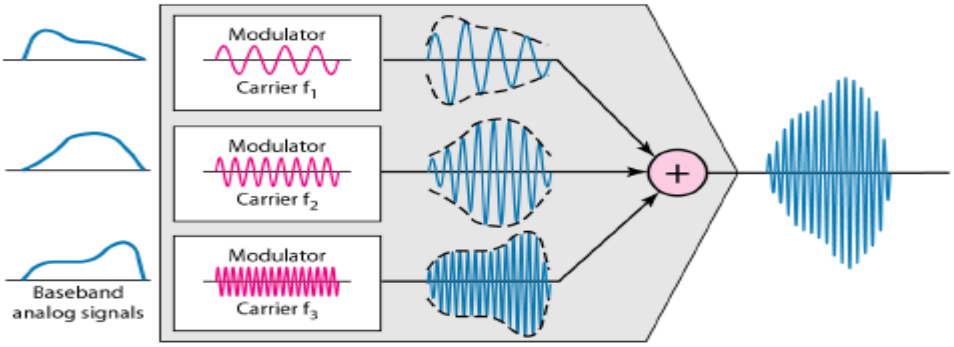
Frequency-division multiplexing (FDM) is an analog technique that can be applied when the bandwidth of a link (in hertz) is greater than the combined bandwidths of the signals to be transmitted. In FDM, signals generated by each sending device modulate different carrier frequencies. These modulated signals 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. In addition, carrier frequencies must not interfere with the original data frequencies. 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.



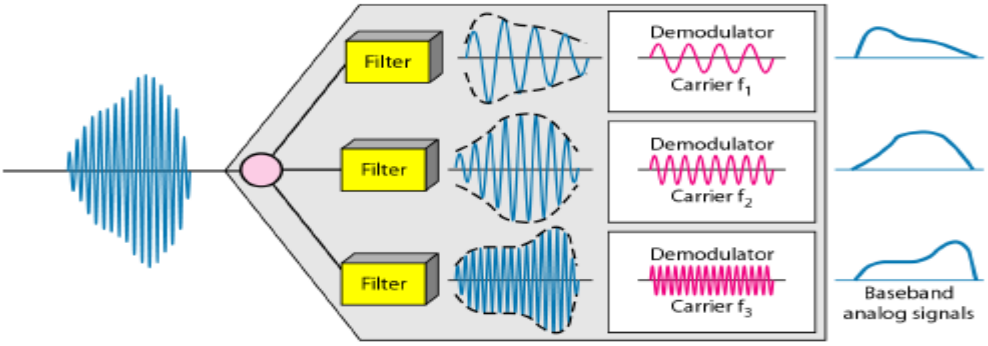
Multiplexing Process

Figure below is a conceptual illustration of the multiplexing process. Each source generates a signal of a similar frequency range. Inside the multiplexer, these similar signals modulates different carrier frequencies. 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.



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.



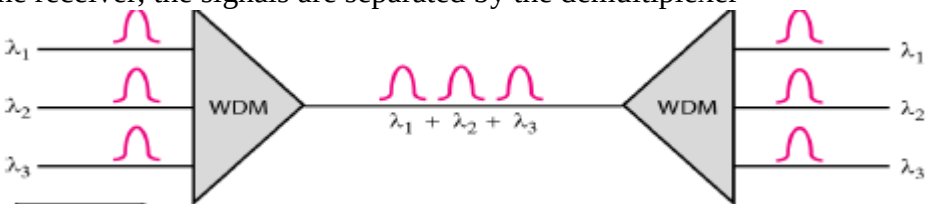
A very common application of FDM is AM and FM radio broadcasting. Radio uses the air as the transmission medium. A special band from 530 to 1700 kHz is assigned to AM radio. All radio stations need to share this band. Each AM station needs 10kHz of bandwidth. Each station uses a

different carrier frequency, which means it is shifting its signal and multiplexing. The signal that goes to the air is a combination of signals. A receiver receives all these signals, but filters (by tuning) only the one which is desired. Without multiplexing, only one AM station could broadcast to the common link, the air. The situation is similar in FM broadcasting. However, FM has a wider band of 88 to 108MHz because each station needs a bandwidth of 200 kHz. Another common use of FDM is in television broadcasting. Each TV channel has its own bandwidth of 6 MHz.

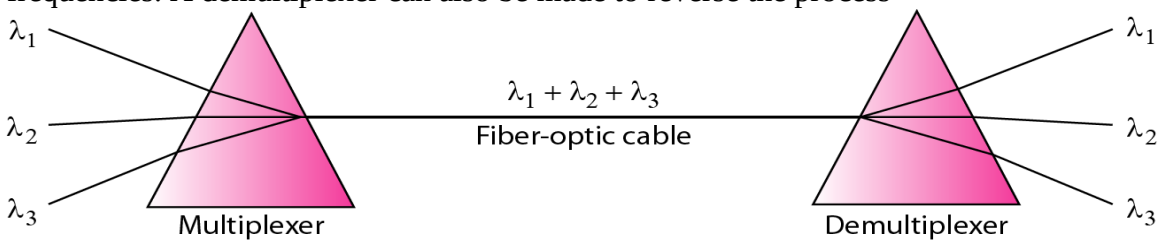
Wavelength Division Multiplexing (WDM)

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 WDM is conceptually the same as FDM, except that the multiplexing and demultiplexing involve optical signals transmitted through fiber-optic channels. The idea is the same: We are combining different signals of different frequencies. The difference is that the frequencies are very high. 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



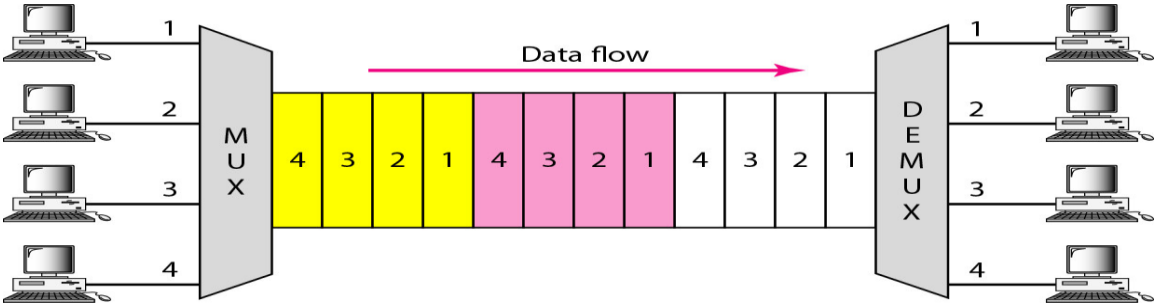
Although WDM technology is very complex, the basic idea is very simple. We want to combine multiple light sources into one single light at the multiplexer and do the reverse at the demultiplexer. The combining and splitting of light sources are easily handled by a prism. Recall from basic physics that 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



Time Division Multiplexing (TDM)

Time-division multiplexing (TDM) is a digital process that allows several connections to share the high bandwidth of a linle Instead of sharing a portion of the bandwidth as in FDM, time is shared. Each connection occupies a portion of time in the link. Figure gives a conceptual view of TDM. Note that the same link is used as in FDM; here, however, the link is shown sectioned by time

rather than by frequency. In the figure, portions of signals 1, 2, 3, and 4 occupy the link sequentially



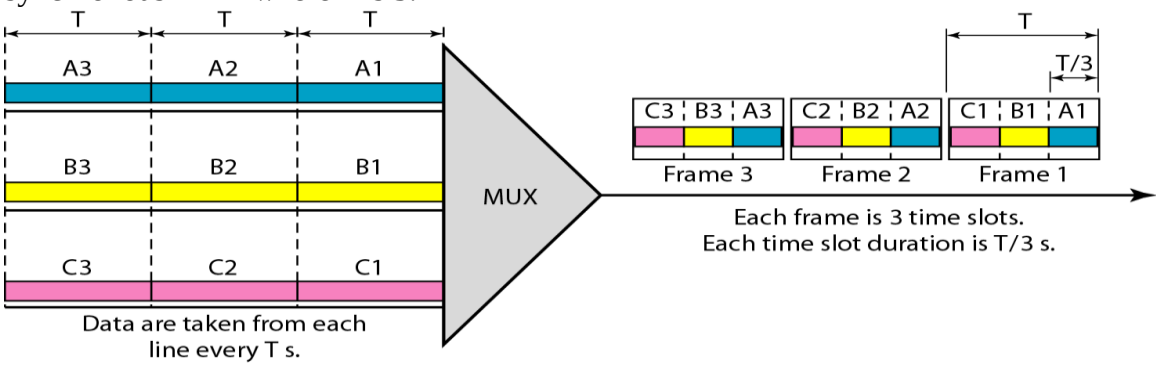
Digital data from different sources are combined into one timeshared link. However, this does not mean that the sources cannot produce analog data; analog data can be sampled, changed to digital data, and then multiplexed by using TDM.

Synchronous Time Division Multiplexing

In synchronous TDM, each input connection has an allotment in the output even if it is not sending data.

Time Slots and Frames

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 Tin s, where n is the number of connections. In other words, a unit in the output connection has a shorter duration; it travels faster. Figure shows an example of synchronous TDM where n is 3.

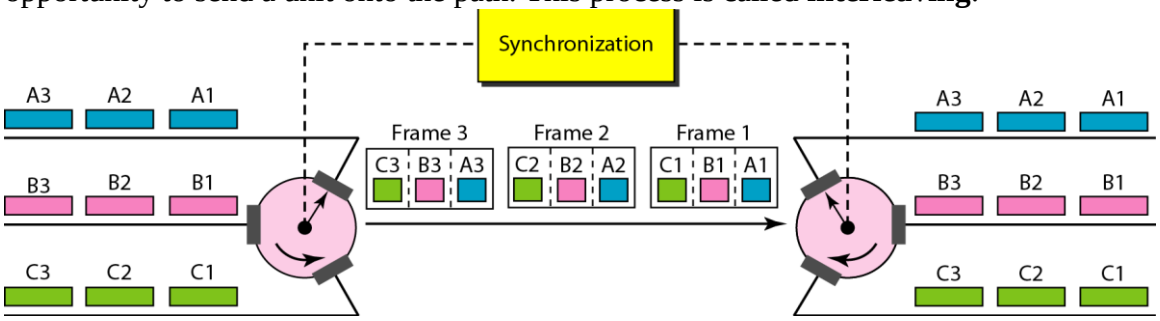


In synchronous TDM, a round of data units from each input connection is collected into a frame. If we have *n* connections, a frame is divided into *n* time slots and one slot is allocated for each unit, one for each input line. If the duration of the input unit is *T*, the duration of each slot is *Tin* and the duration of each frame is *T*. The data rate of the output link must be *n* times the data rate of a connection to guarantee the flow of data. In Figure, the data rate of the link is 3 times the data rate of a connection; likewise, the duration of a unit on a connection is 3 times that of the time slot (duration of a unit on the link). In the figure we represent the data prior to multiplexing as 3 times the size of the data after multiplexing. This is just to convey the idea that each unit is 3 times longer in duration before multiplexing than after.

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 MUX side and the other on the DEMUX side. The switches are synchronized and rotate at the same speed but in opposite directions. On the MUX 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**.



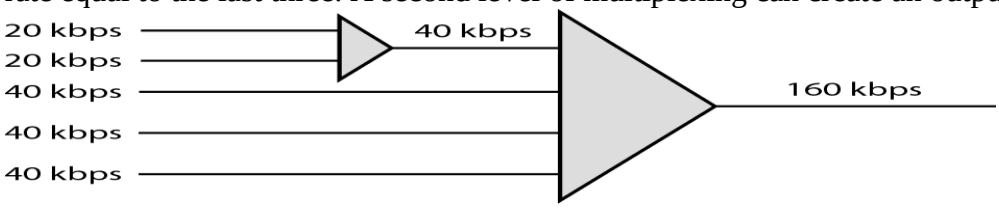
Empty Slots

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. Statistical TDM can improve the efficiency by removing the empty slots from the frame.

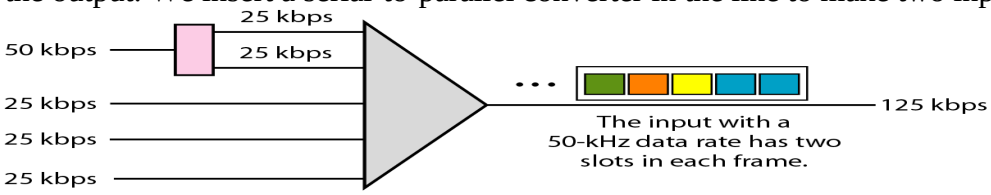
Data Rate Management

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 strategies are **multilevel multiplexing, multiple-slot allocation,** and **pulse stuffing.**

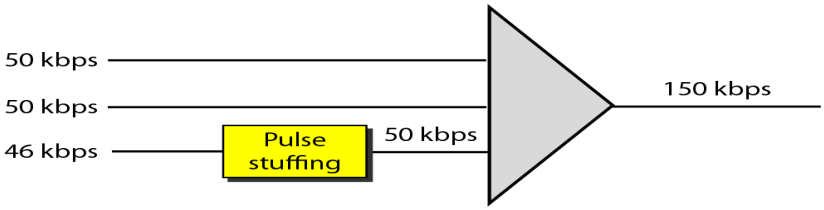
Multilevel Multiplexing Multilevel multiplexing is a technique used when the data rate of an input line is a multiple of others. For example, in Figure below, we have two inputs of 20 kbps and three inputs of 40 kbps. The first two input lines can be multiplexed together to provide a data rate equal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



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 Figure below, the input line with a 50-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.

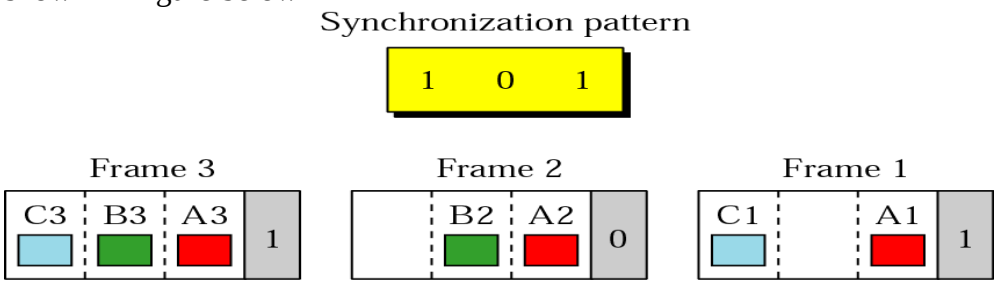


Pulse Stuffing Sometimes the bit rates of sources are not multiple integers of each other. Therefore, neither of the above two techniques can be applied. One solution is to make the highest input data rate the dominant data rate and then add dummy bits to the input lines with lower rates. This will increase their rates. This technique is called pulse stuffing, bit padding, or bit stuffing. The idea is shown in Figure below.



Frame Synchronizing

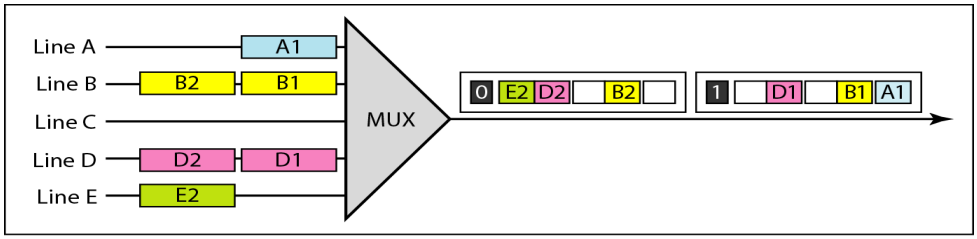
The implementation ofTDM is not as simple as that of FDM. Synchronization between the multiplexer and demultiplexer is a major issue. If the. multiplexer and the demultiplexer are not synchronized, a bit belonging to one channel may be received by the wrong channel. For this reason, one or more synchronization 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 Figure below



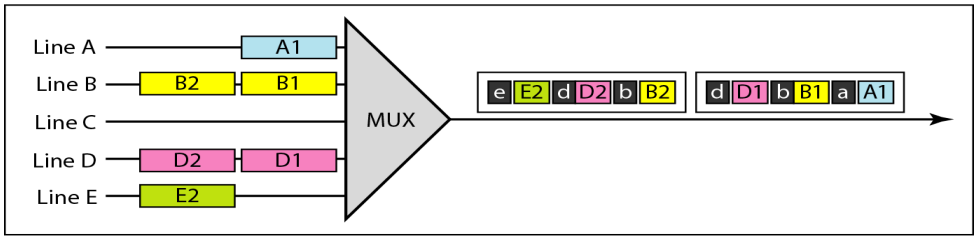
Statistical Time-Division Multiplexing

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.

Figure below 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

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 preassigned relationships between the inputs and outputs serve as an address. In statistical multiplexing, there is no fixed relationship between the inputs and outputs because there are no preassigned or reserved slots. The addressing in its simplest form can be *n* bits to define *N* different output lines with *n* =10g2 *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

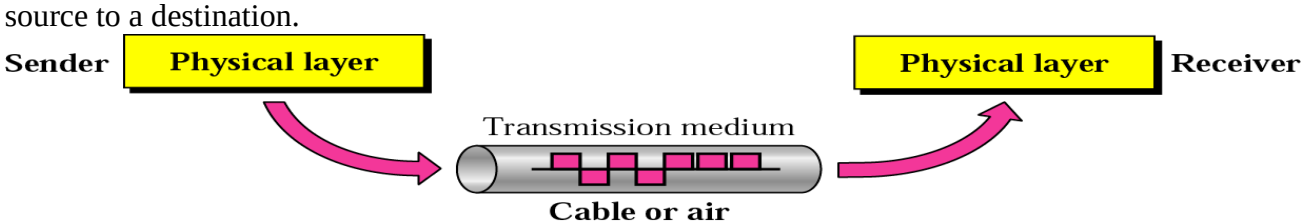
The frames in statistical TDM need not be synchronized, so no need for synchronization bits.

Bandwidth

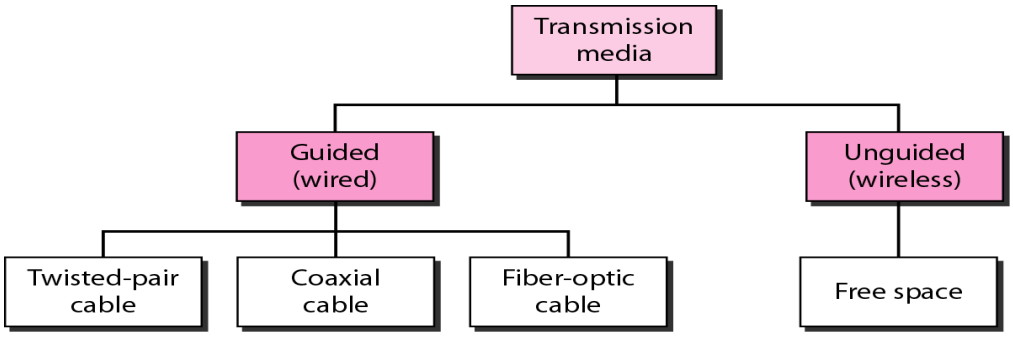
In statistical TDM, the capacity of the link is normally less than the sum of the capacities of each channel.

Transmission Media

A transmission **medium** can be broadly defined as anything that can carry information from a source to a destination.



Transmission media can be divided into two broad categories: guided and unguided. Guided media include twisted-pair cable, coaxial cable, and fiber-optic cable. Unguided medium is free space.

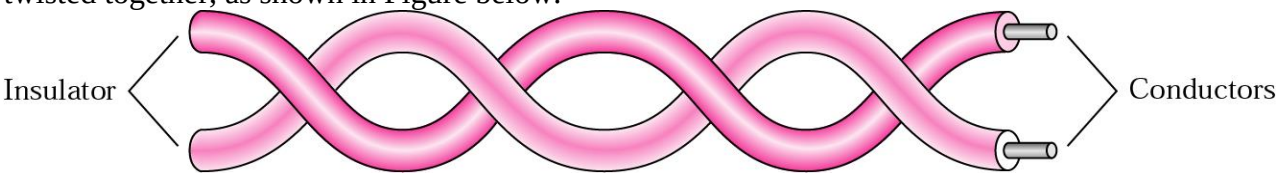


GUIDED MEDIA

Guided media, which are those that provide a conduit 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 Figure below.

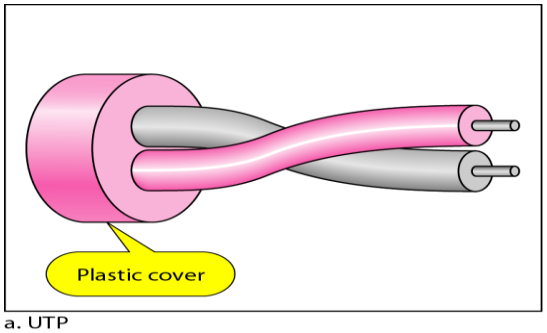


One of the wires is used to carry signals to the receiver, and the other is used only as a ground reference. The receiver uses the difference between the two. In addition to the signal sent by the sender on one of the wires, interference (noise) and crosstalk may affect both wires and create unwanted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

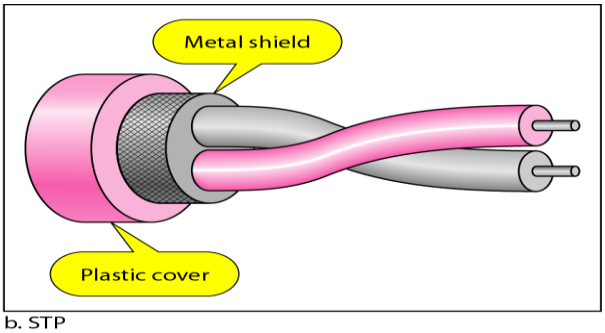
This means that the receiver, which calculates the difference between the two, receives no unwanted signals. The unwanted signals are mostly canceled out. From the above discussion, it is clear that the number of twists per unit of length (e.g., inch) has some effect on the quality of the cable.

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. Although metal casing improves the quality of cable by preventing the penetration of noise or crosstalk, it is bulkier and more expensive. Figure shows the difference between UTP and STP.



a. UTP



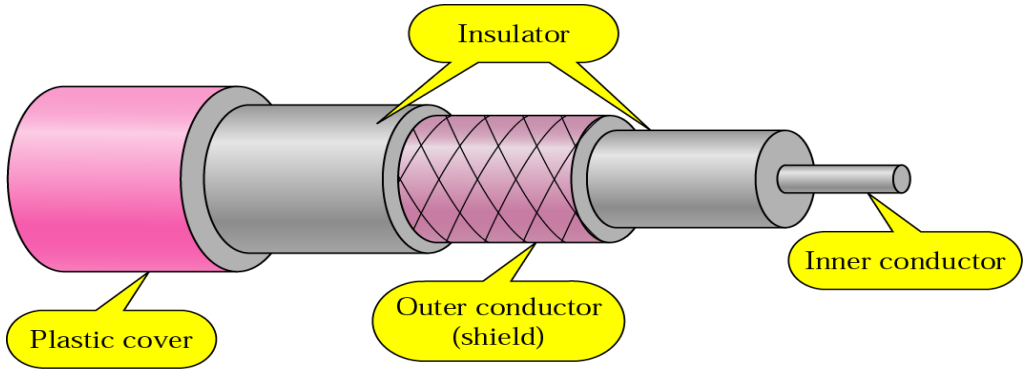
b. STP

Categories of UTP Cables

Category	*Specification*	*Data Rate (Mbps)*	*Use*
1	Unshielded twisted-pair used in telephone	< 0.1	Telephone
2	Unshielded twisted-pair originally used in T-lines	2	T-1 lines
3	Improved CAT 2 used in LANs	10	LANs
4	Improved CAT 3 used in Token Ring networks	20	LANs
5	Cable wire is normally 24 AWG with a jacket and outside sheath	100	LANs
5E	An extension to category 5 that includes extra features to minimize the crosstalk and electromagnetic interference	125	LANs
6	A new category with matched components coming from the same manufacturer. The cable must be tested at a 200-Mbps data rate.	200	LANs
7	Sometimes called SSTP (shielded screen twisted-pair). Each pair is individually wrapped in a helical metallic foil followed by a metallic foil shield in addition to the outside sheath. The shield decreases the effect of crosstalk and increases the data rate.	600	LANs

Coaxial Cable

Coaxial cable (or *coax)* carries signals of higher frequency ranges than those in twisted pair cable, in part because the two media are constructed quite differently. Instead of having two wires, 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.



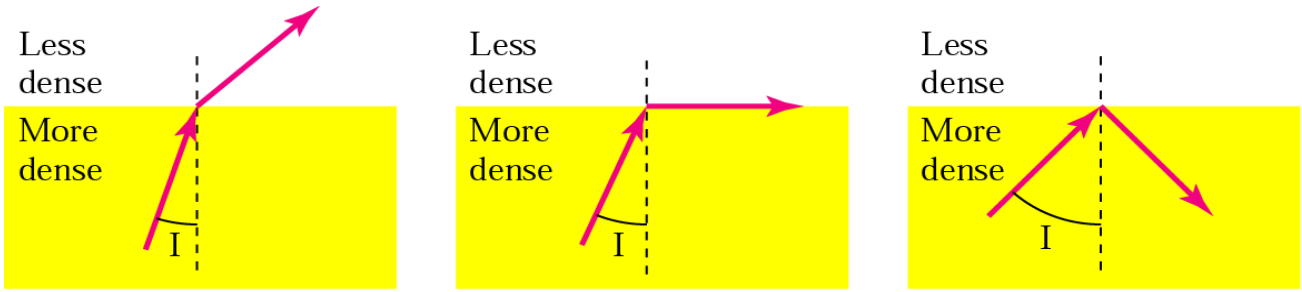
Categories of Coaxial Cables

Category	*Impedance*	*Use*
RG-59	75 Ω	Cable TV
RG-58	50 Ω	Thin Ethernet
RG-11	50 Ω	Thick Ethernet

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. Each cable defined by an RG rating is adapted for a specialized function**,**

Fiber-Optic Cable

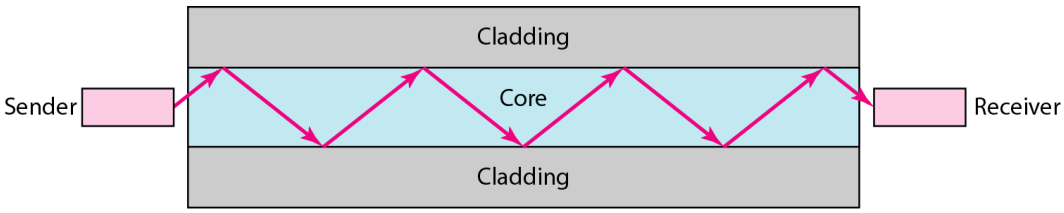
A fiber-optic cable is made of glass or plastic and transmits signals in the form of light. To understand optical fiber, we first need to explore several aspects of the nature of light. Light travels in a straight line as long as it is moving through a single uniform substance. If a ray of light traveling through one substance suddenly enters another substance (of a different density), the ray changes its direction. Figure below shows how a ray of light changes direction when going from a denser 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.

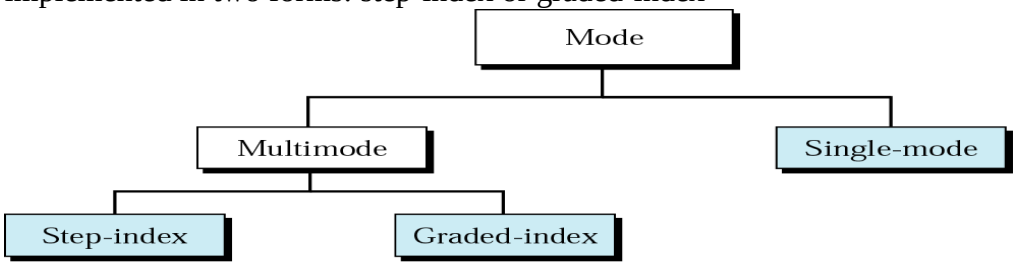
Optical fibers use reflection to guide light through a channel. A glass or plastic core is surrounded by a cladding of less dense glass or plastic. The difference in density of the two materials must be

such that a beam of light moving through the core is reflected off the cladding instead of being refracted into it.



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



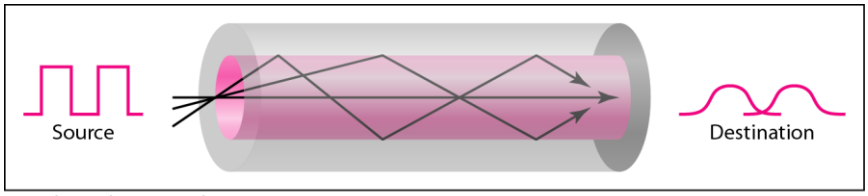
Multimode:

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. 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.

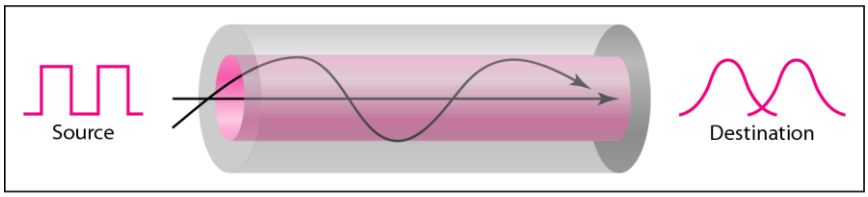
A second type of fiber, called multimode graded-index fiber, decreases this distortion of the signal through the cable. The word *index* here refers to the index of refraction. The index of refraction is related to density. A graded-index fiber, therefore, is one with varying densities. Density is highest at the center of the core and decreases gradually to its lowest at the edge. Figure below shows the impact of this variable density on the propagation of light beams.

Single-Mode:

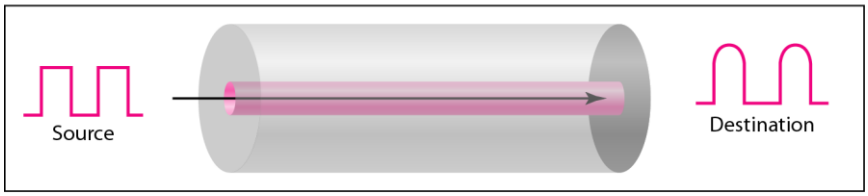
Single-mode uses step-index fiber and a highly focused source of light that limits beams to a small range of angles, all close to the horizontal. The single-mode fiber is manufactured with a much smaller diameter than that of multimode fiber, and with substantially lower density (index of refraction). 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.



a. Multimode, step index



b. Multimode, graded index



c. Single mode

Advantages: Fiber-optic cable has several advantages over metallic cable.

- 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.
- 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.
- Immunity to electromagnetic interference. Electromagnetic noise cannot affect fiber-optic cables.
- Resistance to corrosive materials. Glass is more resistant to corrosive materials than copper.
- Light weight. Fiber-optic cables are much lighter than copper cables.
- 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.

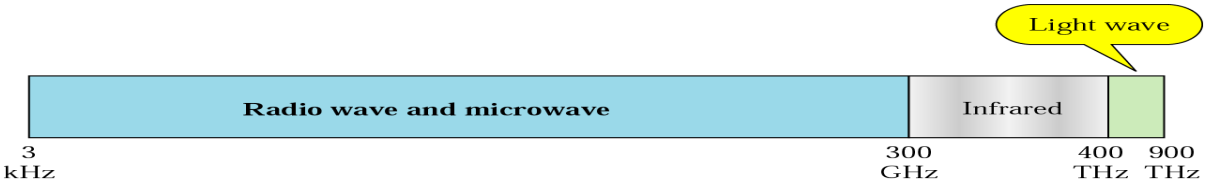
Disadvantages: There are some disadvantages in the use of optical fiber.

- Installation and maintenance. Fiber-optic cable is a relatively new technology. Its installation and maintenance require expertise that is not yet available everywhere.
- Unidirectional light propagation. Propagation of light is unidirectional. If we need bidirectional communication, two fibers are needed.
- 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

UNGUIDED MEDIA: WIRELESS

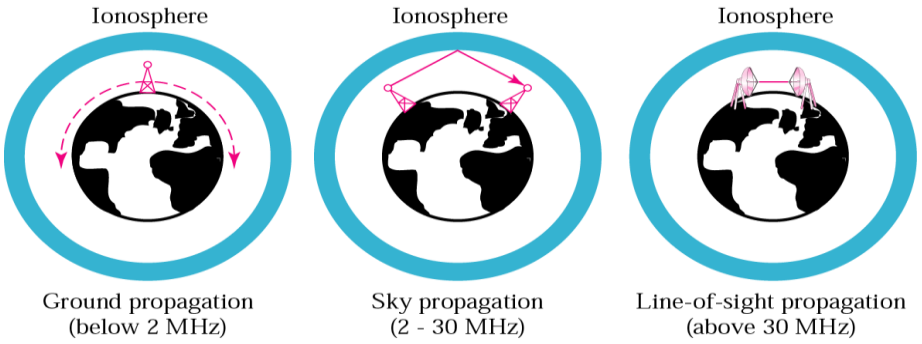
Unguided media transport electromagnetic waves without using a physical conductor. This type of communication is often referred to as wireless communication. Signals are normally broadcast through free space and thus are available to anyone who has a device capable of receiving them.

Figure below shows the part of the electromagnetic spectrum, ranging from 3 kHz to 900 THz, used for wireless communication.



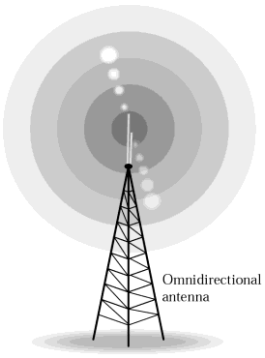
Unguided signals can travel from the source to destination in several ways: ground propagation, sky propagation, and line-of-sight propagation. In ground propagation, radio waves travel through the lowest portion of the atmosphere, hugging the earth. These low-frequency signals emanate in all directions 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. 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. 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.



The section of the electromagnetic spectrum defined as radio waves and microwaves is divided into eight ranges, called *bands*, each regulated by government authorities. These bands are rated from *very low frequency* (VLF) to *extremely highfrequency* (EHF). Table lists these bands, their ranges, propagation methods, and some applications

Band	*Range*	*Propagation*	*Application*
VLF (very low frequency)	3–30 kHz	Ground	Long-range radio navigation
LF (low frequency)	30–300 kHz	Ground	Radio beacons and navigational locators
MF (middle frequency)	300 kHz–3 MHz	Sky	AM radio
HF (high frequency)	3–30 MHz	Sky	Citizens band (CB), ship/aircraft communication
VHF (very high frequency)	30–300 MHz	Sky and line-of-sight	VHF TV, FM radio
UHF (ultrahigh frequency)	300 MHz–3 GHz	Line-of-sight	UHF TV, cellular phones, paging, satellite
SHF (superhigh frequency)	3–30 GHz	Line-of-sight	Satellite communication
EHF (extremely high frequency)	30–300 GHz	Line-of-sight	Radar, satellite



Radio Waves

Electromagnetic waves ranging in frequencies between 3 kHz and 1 GHz are normally called radio waves. Radio waves 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 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. 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

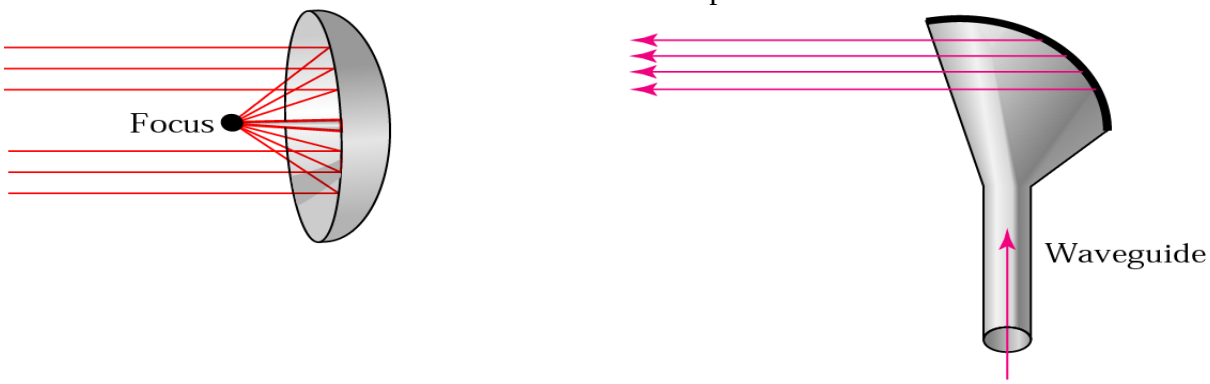
Electromagnetic waves having frequencies between I and 300 GHz are called microwaves. Microwaves are unidirectional. When an antenna transmits microwave waves, they can be narrowly focused. This means that the sending and receiving antennas need to be aligned. The unidirectional property has an obvious 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.

- 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.

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.



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. 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 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.

Infrared

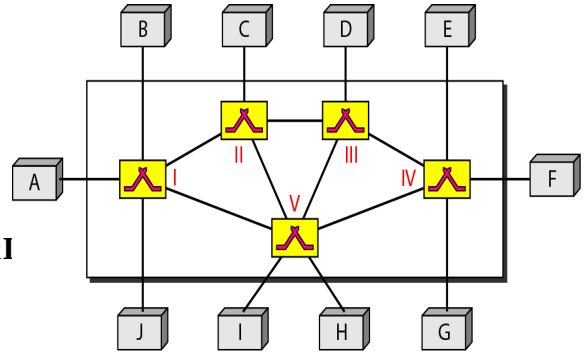
Infrared waves, with frequencies from 300 GHz to 400 THz (wavelengths from 1 mm to 770 nm), can be used for short-range communication. Infrared waves, having high frequencies, cannot penetrate walls. This advantageous characteristic prevents interference between one system and another; a short-range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

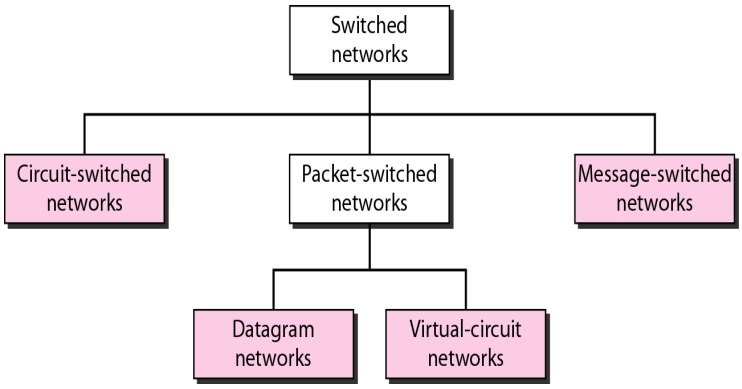
The *Infrared Data Association* (IrDA), an association for sponsoring the use of infrared waves, has established standards for using these signals for communication between devices such as keyboards, mice, PCs, and printers.

Switching

A switched network consists of a series of interlinked nodes, called switches. Switches are devices capable of creating temporary connections between two or more devices linked to the switch. In a switched network, some of these nodes are connected to the end systems



(computers or telephones, for example). Others are used only for routing. Figure shows a switched network.

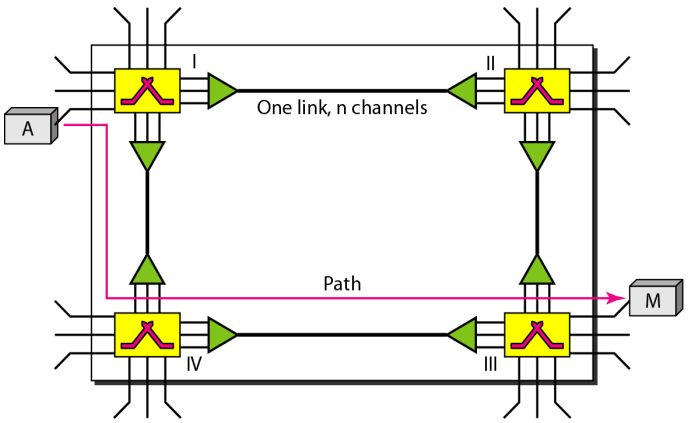


Traditionally, three methods of switching have been important: circuit switching, packet switching, and message switching. Packet-switched networks can further be divided into two subcategories- virtual-circuit networks and datagram networks.

CIRCUIT-SWITCHED NETWORKS

A circuit-switched network consists of a set of switches connected by physical links. A connection between two stations is a dedicated path made of one or more links. However, each connection uses only one dedicated channel on each link. Each link is normally divided into *n* channels by using FDM or TDM.

Figure below shows a trivial circuit-switched network with four switches and four links. Each link is divided into *n (n* is 3 in the figure) channels by using FDM or TDM.



When end system A needs to communicate with end system M, system A needs to request a connection to M that must be accepted by all switches as well as by M itself. This is called the setup phase; a circuit (channel) is reserved on each link, and the combination of circuits or channels defines the dedicated path. After the dedicated path made of connected circuits (channels) is established, data transfer can take place. After all data have been transferred, the circuits are tom down.

- Circuit switching takes place at the physical layer.
- Before starting communication, the stations must make a reservation for the resources to be used during the communication. These resources, such as channels, switch buffers, switch processing time, and switch input/output ports, must remain dedicated during the entire duration of data transfer until the teardown phase.
- Data transferred between the two stations are not packetized (physical layer transfer of the signal). The data are a continuous flow sent by the source station and received by the destination station, although there may be periods of silence.
- There is no addressing involved during data transfer. The switches route the data based on their occupied band (FDM) or time slot (TDM)

Three Phases

The actual communication in a circuit-switched network requires three phases: connection setup, data transfer, and connection teardown.

Setup Phase

Before the two parties can communicate, a dedicated circuit needs to be established. The end systems are normally connected through dedicated lines to the switches, so connection setup means creating dedicated channels between the switches. For example, when system A needs to connect to system M, it sends a setup request that includes the address of system M, to switch I. Switch I finds a channel between itself and switch IV that can be dedicated for this purpose. Switch I then sends the request to switch IV, which finds a dedicated channel between itself and switch III. Switch III informs system M of system A's intention at this time. In the next step to making a connection, an acknowledgment from system M needs to be sent in the opposite direction to system A. Only after system A receives this acknowledgment is the connection established.

Data Transfer Phase

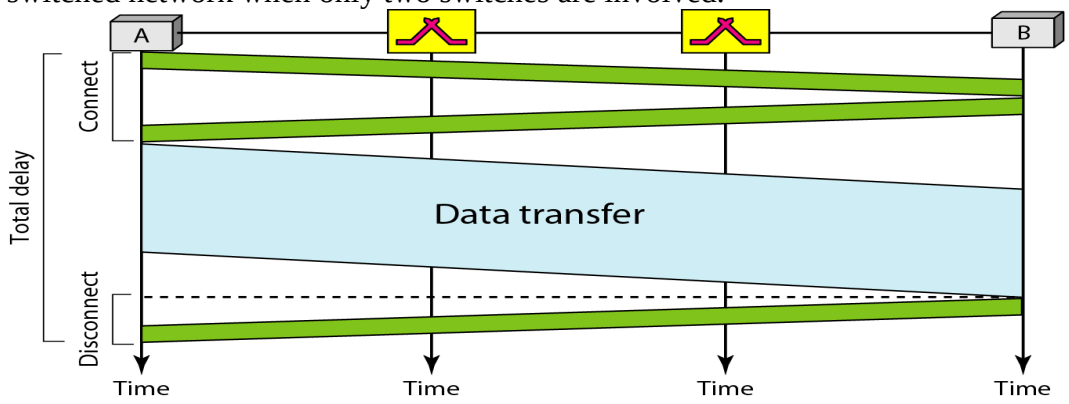
After the establishment of the dedicated circuit (channels), the two parties can transfer data.

Teardown Phase

When one of the parties needs to disconnect, a signal is sent to each switch to release the resources.

Delay

Although a circuit-switched network normally has low efficiency, the delay in this type of network is minimal. During data transfer the data are not delayed at each switch; the resources are allocated for the duration of the connection. Figure shows the idea of delay in a circuit-switched network when only two switches are involved.

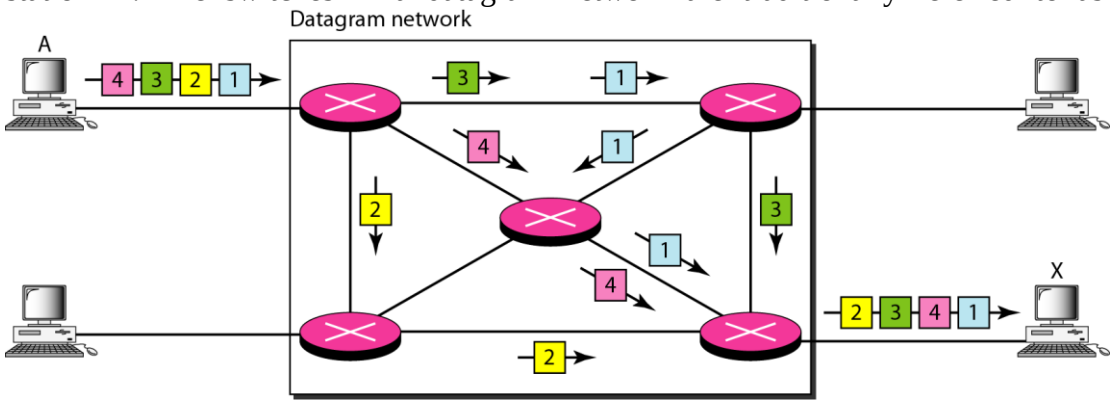


The total delay is due to the time needed to create the connection, transfer data, and disconnect the circuit.

DATAGRAM NETWORKS

If the message is going to pass through a packet-switched network, it needs to be divided into packets of fixed or variable size. The size of the packet is determined by the network and the governing protocol. In packet switching, there is no resource allocation for a packet. This means that there is no reserved bandwidth on the links, and there is no scheduled processing time for each packet. Resources are allocated on demand. The allocation is done on a first-come, first-served basis. In a datagram network, each packet is treated independently of all others. Even if a packet is part of a multipacket transmission, the network treats it as though it existed alone. Packets in this approach are referred to as datagrams. Datagram switching is normally done at the network layer.

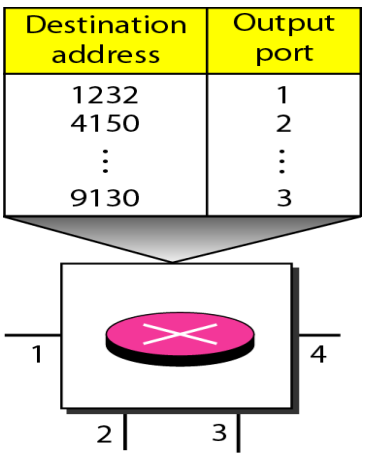
Figure shows how the datagram approach is used to deliver four packets from station A to station X. The switches in a datagram network are traditionally referred to as routers.



In this example, all four packets (or datagrams) belong to the same message, but may travel different paths to reach their destination. This approach can cause the datagrams of a transmission to arrive at their destination out of order with different delays between the packets. Packets may also be lost or dropped because of a lack of resources. In most protocols, it is the responsibility of an upper-layer protocol to reorder the datagrams or ask for lost datagrams before passing them on to the application.

The datagram networks are sometimes referred to as connectionless networks. The term connectionless here means that the switch (packet switch) does not keep information about the connection state. There are no setup or teardown phases. Each packet is treated the same by a switch regardless of its source or destination.

Routing Table



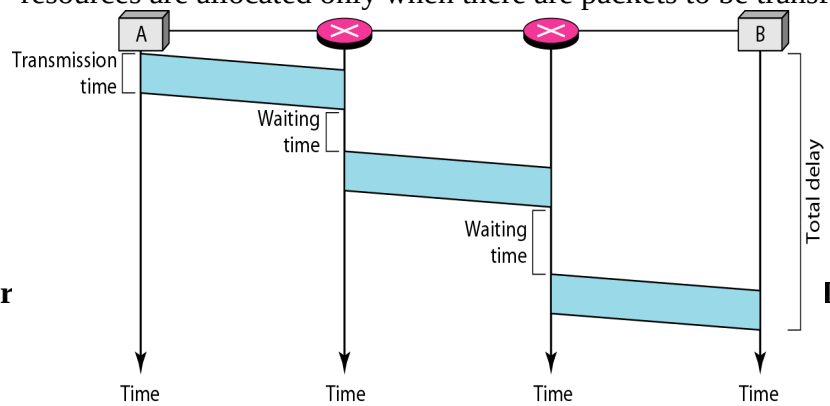
In this type of network, each switch (or packet switch) has a routing table which is based on the destination address. The routing tables are dynamic and are updated periodically. The destination addresses and the corresponding forwarding output ports are recorded in the tables. Figure shows the routing table for a switch.

Every packet in a datagram network carries a header that contains, among other information, the destination address of the packet. When the switch receives the packet, this destination address is examined; the routing table is consulted to find the corresponding

port through which the packet should be forwarded. The destination address in the header of a packet in a datagram network remains the same during the entire journey of the packet.

Efficiency

The efficiency of a datagram network is better than that of a circuit-switched network; resources are allocated only when there are packets to be transferred



Delay

There may be greater delay in a datagram network than in a virtual-circuit network. Although there are no setup and teardown phases, each

Pr **IE.**

packet may experience a wait at a switch before it is forwarded. In addition, since not all packets in a message necessarily travel through the same switches, the delay is not uniform for the packets of a message.

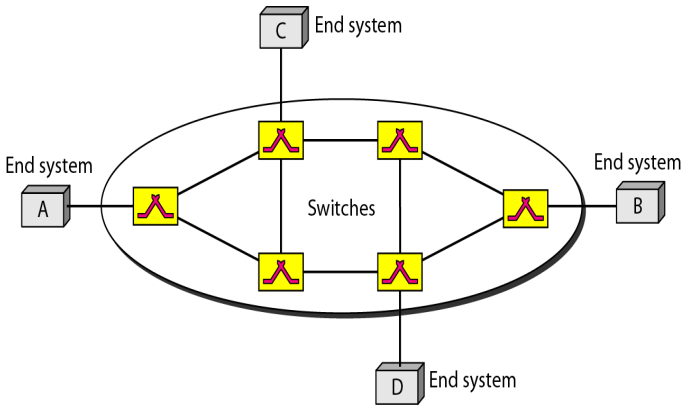
The packet travels through two switches. There are three transmission times (3T),
three propagation delays (slopes 3't of the lines), and two waiting times (WI + w2)' The total delay is Total delay =3T + 3t + WI + W2

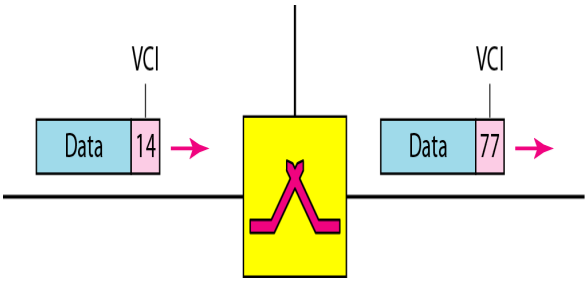
VIRTUAL-CIRCUIT NETWORKS

A virtual-circuit network is a cross between a circuit-switched network and a datagram network. It has some characteristics of both.

1. As in a circuit-switched network, there are setup and teardown phases in addition to the data transfer phase.
2. Resources can be allocated during the setup phase, as in a circuit-switched network, or on demand, as in a datagram network.
3. As in a datagram network, data are packetized and each packet carries an address in the header. However, the address in the header has local jurisdiction (it defines what should be the next switch and the channel on which the packet is being carried), not end-to-end jurisdiction.
4. As in a circuit-switched network, all packets follow the same path established during the connection.
5. A virtual-circuit network is normally implemented in the data link layer, while a circuit-switched network is implemented in the physical layer and a datagram network in the network layer.

Figure is an example of a virtual-circuit network. The network has switches that allow traffic from sources to destinations. A source or destination can be a computer, packet switch, bridge, or any other device that connects other networks.





Addressing

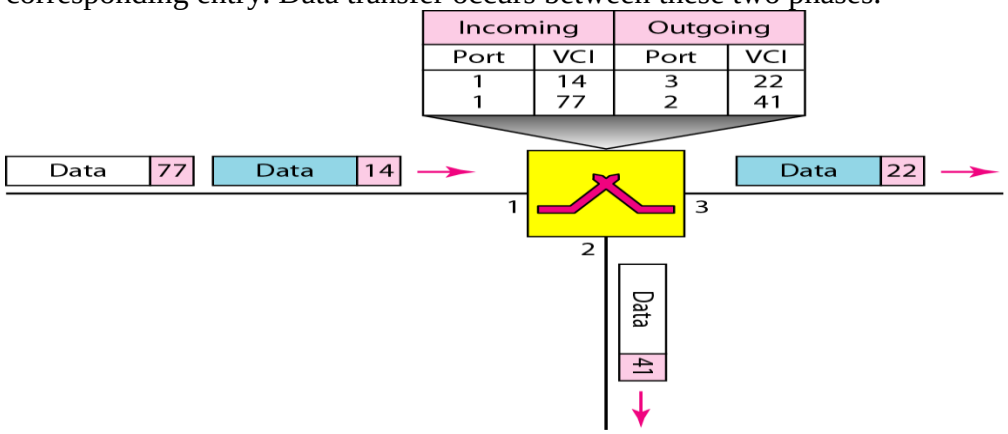
In a virtual-circuit network, two types of addressing are involved: global and local (virtual-circuit identifier-VCI).

- Global address is used only to create a VCI
- Virtual Circuit Identifier is a small number that has only switch scope
- It is used by a frame between two switches.
- When a frame arrives at a switch, it has a VCI; when it leaves, it has a different VCl.

Three Phases

As in a circuit-switched network, a source and destination need to go through three phases in a virtual-circuit network: setup, data transfer, and teardown. In the setup phase, the source and destination use their global addresses to help switches make table entries for the connection.

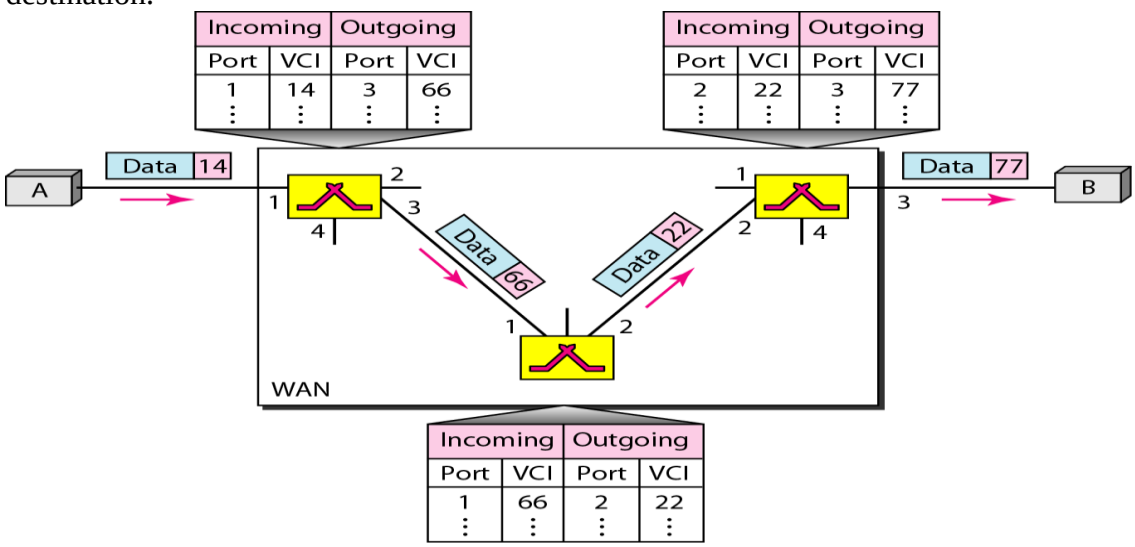
In the teardown phase, the source and destination inform the switches to delete the corresponding entry. Data transfer occurs between these two phases.



Data Transfer Phase

To transfer a frame from a source to its destination, all switches need to have a table entry for this virtual circuit. The table, in its simplest form, has four columns. This means that the switch holds four pieces of information for each virtual circuit that is already set up. Figure 8.12 shows such a switch and its corresponding table.

Figure above shows a frame arriving at port 1 with a VCI of 14. When the frame arrives, the switch looks in its table to find port 1 and a VCI of 14. When it is found, the switch knows to change the VCI to 22 and send out the frame from port 3. Figure below shows how a frame from source A reaches destination B and how its VCI changes during the trip. Each switch changes the VCI and routes the frame. The data transfer phase is active until the source sends all its frames to the destination. The procedure at the switch is the same for each frame of a message. The process creates a virtual circuit, not a real circuit, between the source and destination.



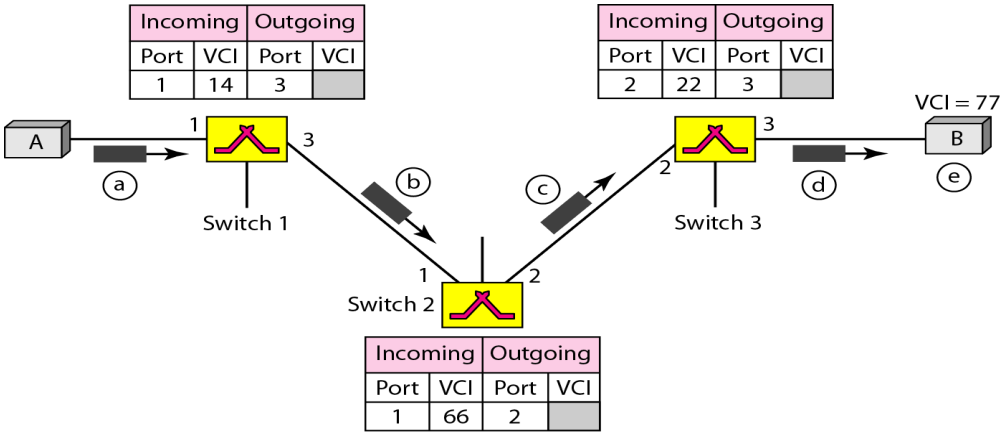
Setup Phase

In the setup phase, a switch creates an entry for a virtual circuit. Two steps are required: the setup request and the acknowledgment.

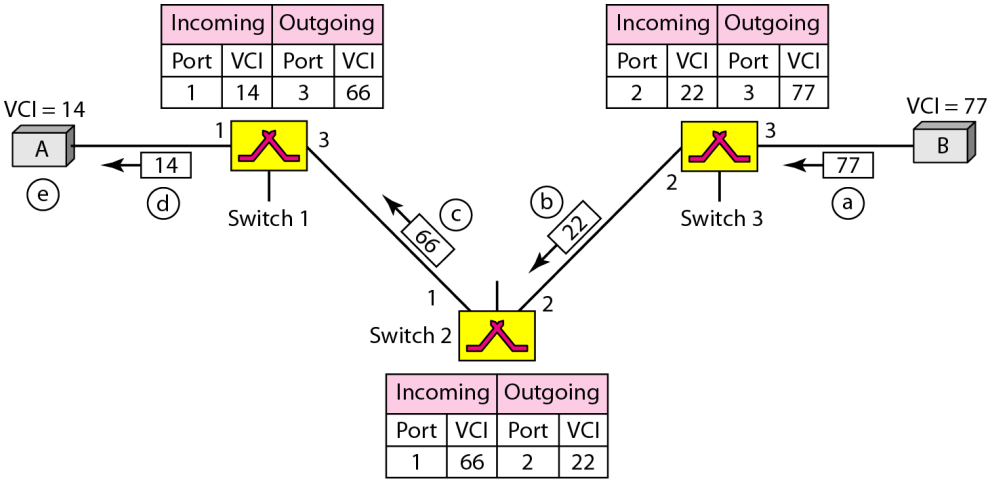
Setup Request: A setup request frame is sent from the source to the destination. Figure shows the process.

a. Source A sends a setup frame to switch 1.

b. Switch 1 receives the setup request frame. The switch assigns the incoming port (1) and chooses an available incoming VCI (14) and the outgoing port (3). It does not yet know the outgoing VCI, which will be found during the acknowledgment step. The switch then forwards the frame through port 3 to switch 2.
c. Switch 2 receives the setup request frame. The same events happen here as at switch 1; three columns of the table are completed: in this case, incoming port (l), incoming VCI (66), and outgoing port (2).
d. Switch 3 receives the setup request frame. Again, three columns are completed: incoming port (2), incoming VCI (22), and outgoing port (3).
e. Destination B receives the setup frame, and if it is ready to receive frames from A, it assigns a VCI to the incoming frames that come from A, in this case 77. This VCI lets the destination know that the frames come from A, and not other sources.



Acknowledgment: A special frame, called the acknowledgment frame, completes the entries in the switching tables. Figure 8.15 shows the process.
a. The destination sends an acknowledgment to switch 3. The acknowledgment carries the global source and destination addresses so the switch knows which entry in the table is to be completed. The frame also carries VCI 77, chosen by the destination as the incoming VCI for frames from A. Switch 3 uses this VCI to complete the outgoing VCI column for this entry. Note that 77 is the incoming VCI for destination B, but the outgoing VCI for switch 3.
b. Switch 3 sends an acknowledgment to switch 2 that contains its incoming VCI in the table, chosen in the previous step. Switch 2 uses this as the outgoing VCI in the table.
c. Switch 2 sends an acknowledgment to switch 1 that contains its incoming VCI in the table, chosen in the previous step. Switch 1 uses this as the outgoing VCI in the table.
d. Finally switch 1 sends an acknowledgment to source A that contains its incoming VCI in the table, chosen in the previous step.
e. The source uses this as the outgoing VCI for the data frames to be sent to destination B.



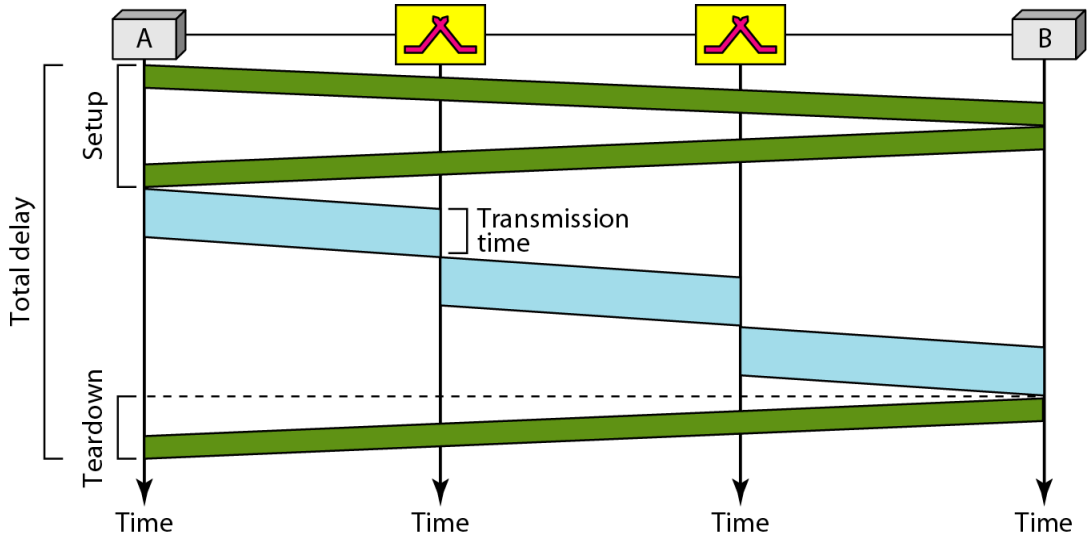
Teardown Phase

In this phase, source A, after sending all frames to B, sends a special frame called a *teardown request.* Destination B responds with a teardown confirmation frame. All switches delete the corresponding entry from their tables.

Delay in Virtual-Circuit Networks

In a virtual-circuit network, there is a one-time delay for setup and a one-time delay for teardown. If resources are allocated during the setup phase, there is no wait time for individual packets. In virtual-circuit switching, all packets belonging to the same source and destination travel the same path; but the packets may arrive at the destination with different delays if resource allocation is on demand**.**

The total delay time is = *3T*+ 3't + setup delay + teardown delay



Questions	opt1	opt2	opt3	opt4	opt5	opt6	answer
Before data can be transmitted, they must be transformed to_____	periodic signals	electromagnetic signals	Aperiodic signals	low frequency sine waves			electromagnetic signals
Which of the following can be determined from a frequency_domain graph of a signal?	frequency	phase	power	amplitude			frequency
Which of the following can be determined from a frequency_domain graph of a signal?	bandwidth	phase	power	frequency			bandwidth
In a frequency_domain plot, the vertical axis measures the_____	peak amplitude	frequency	phase	slope			peak amplitude
In a frequency_domain plot, the horizontal axis measures the_____	peak amplitude	frequency	phase	slope			frequency
As frequency increases, the period_____	dereases	increases	remains the same	doubles			increases
Given two sine waves A and B, if frequency of A is twice that of B, then the period of B is_____ that of A	one_half	twice	the same as	indetermine from			one_half
A sine wave is_____	periodic and continuous	aperiodic and continuous	periodic and discrete	aperiodic and discrete			periodic and continuous
_____is a type of transmission impairment in which the signal loses strength due to the resistance of the transmission medium	attenuation	distortion	noise	decibel			attenuation

_____is a type of transmission impairment in which the signal loses strength due to different propogation speeds of each frequency that makes up the signal	attenuation	distortion	noise	decibel			distortion
_____is a type of transmission impairment in which an outside source such as crosstalk corrupts a signal	attenuation	distortion	noise	decibel			noise
Propogation time is_____ proportional to destance and_____ proportional to propogation speed	inversely; directly	directly; inversely	inversely; inversely	directly; directly			directly; inversely
The wavelength of a signal depend on the_____	frequency of the signal	medium	phase of signal	Frequency and Phase of signal			Frequency and Phase of signal
Unipolar, bipolar and polar encoding are types of_____ encoding	line	block	NRZ	manchester			line
If a symbol is composed of 3bits ther are_____ data levels	2	4	8	16			8
_____ encoding has a transition at the middle of each bit	RZ	manchester	differential manchester	all the above			manchester
_____ encoding has a transition at the begining of each 0 bit	RZ	manchester	differential manchester	all the above			RZ
PCM is an example of_____conversion	digital-to-digital	digital-to-anolog	anolog-to-analog	analog-to-digital			analog-to-digital
The nyquist theorem specifies the minimum sampling rate to be_____	equal to the lowest frequency of signal	equal to the highest frequency of a signal	twice the bandwidth of a signal	twice the highest frequency of signal			twice the highest frequency of signal

Which encoding type always has a nonzero average amplitude?	unipolar	polar	bipolar	multipolar			unipolar
Which of the following encoding methods does not provide for synchronization?	NRZ-L	RZ	NRZ-I	manchester			NRZ-L
Which encoding method uses alternating positive and negative values for 1's?	NRZ-I	RZ	manchester	AMI			AMI
RZ encoding involves_____ signal levels	two	three	four	five			three
Which encoding technique attempts to solve loss of synchronization due to long string of 0's?	BNZS	NRZ	AMI	(a) and (b)			BNZS
Block coding can help is_____ at the receiver	synchronization	error detection	attenuation	Noise			synchronization
_____ transmission, bits are transmitted simultaneously, each across the own wire	asynchronous serial	synchronous serial	parallel	perpendicular			parallel
In_____ transmission, bits are transmitted over a single wire, one at a time	asynchronous serial	synchronous serial	parallel	synchronous and asynchronous serial			(a) and (b)
In_____ transmission, a start bit and a stop bit frame a character byte	asynchronous serial	synchronous serial	parallel	fixed			synchronous serial
In asynchronous transmission, the gap tim between bytes is_____	fixed	variable	a function of the data rate	zero			fixed
Synchronous transmission does not have_____	a start bit	a stop bit	gaps between bytes	all the above			all the above

ASK, PSK, FSK and QAM are examples of_____ modulation	digital-to-digital	digital-to-anolog	anolog-to-analog	analog-to-digital			digital-to-anolog
AM and FM are examples of modulation	digital-to-digital	digital-to-anolog	anolog-to-analog	analog-to-digital			anolog-to-analog
In QAM, both phase and_____ of a carrier frequency are varied	amplitude	frequency	bit rate	baud rate			amplitude
Which of the following is most affected by noise?	PSK	ASK	FSK	QAM			ASK
If the baud rate is 400 for a 4-PSK signal, the baud rate is_____ bps	100	400	800	1600			800
If the bit rate for an ASK signal is 1200bps, the baud rate is	300	400	600	1200			1200
If the bit rate for an FSK signal is 1200bps, the baud rate is_____	300	400	600	1200			1200
If the baud rate for a QAM signal is 3000 and a signal unit is represented by a tribit, what is the bit rate?	300	400	1000	9000			9000
In if-QAM there are 16_____	combintion of phase & amplitude	amplitude	phases	bps			combintion of phase & amplitude
What modulation technique involves tribits, eight different phase shifts and one amplitude?	FSK	8-PSK	ASK	4-PSK			8-PSK
The bandwidth of an FM signalrequires 10 times the bandwidth of the_____ signal	carrier	modulating	bipolar	sampling			modulating

Modulation of an analog signal can be accomplished through changing the_____ of the carrier signal	amplitude	frequency	phase	any of the above			frequency
As the bit rate of an FSK signal increases, the bandwidth_____	dereases	increases	remains the same	doubles			increases
The bit rate always equals the baud rate in which type of signal?	FSK	QAM	4-PSK	all the above			FSK
A modulator converts a(n)_____ signal to a(n)_____ signal	digital; analog	analog; digital	PSK; FSK	FSK; PSK			analog; digital
A 56K modern can download at a rate of_____ kbps and upload at a rate of_____kbps	33.6; 33.6	33.6; 56.6	56.6; 33.6	56.6; 56.6			56.6; 33.6
The sharing of medium and its link by two or more devices is called_____	modulation	encoding	line discipline	multiplexing			multiplexing
Which multiplexing technique transmits analog signals	FDM	TDM	WDM	FDM and WDM			FDM and WDM
Which multiplexing technique transmits digital signals	FDM	TDM	WDM	FDM and WDM			TDM
Which multi plexing technique shifts each signal to a different carrier frequency?	FDM	TDM	WDM	FDM and WDM			FDM
In TDM, for n signal sources of the same data rate, each frame contains_____ slots	n	n+1	n-1	0 to n			n

Guard bands increases the bandwidth for_____	FDM	TDM	WDM	TDM and WDM			FDM
Which multiplexing technique involves signals composed of light beams?	FDM	TDM	WDM	FDM and TDM			WDM
Transmission media are usually categorized as_____	fixed or unfixed	guided of unguided	determinate or indeterminate	metallic or non-metallic			guided of unguided
Transmission media are usually categorized as_____	physical	network	transport	application			physical
Category 1 UTP cable is most often used in_____ networks	fast ethernet	traditional ethernet	infrared	telephone			telephone
BNC connectors are used by_____ cables	UTP	STP	coaxial	fiber-optic			coaxial
In fiber optics, the signal source is_____ waves	light	radio	infrared	very low frequency			light
A parabolic dish contenna is a(n)_____ antenna	omni directional	bi directional	uni directional	horn			omni directional
A telephone network is an example of a_____ network	packet switching	circuit switched	message switched	packet and message switched			circuit switched

UNIT – III

SYLLABUS

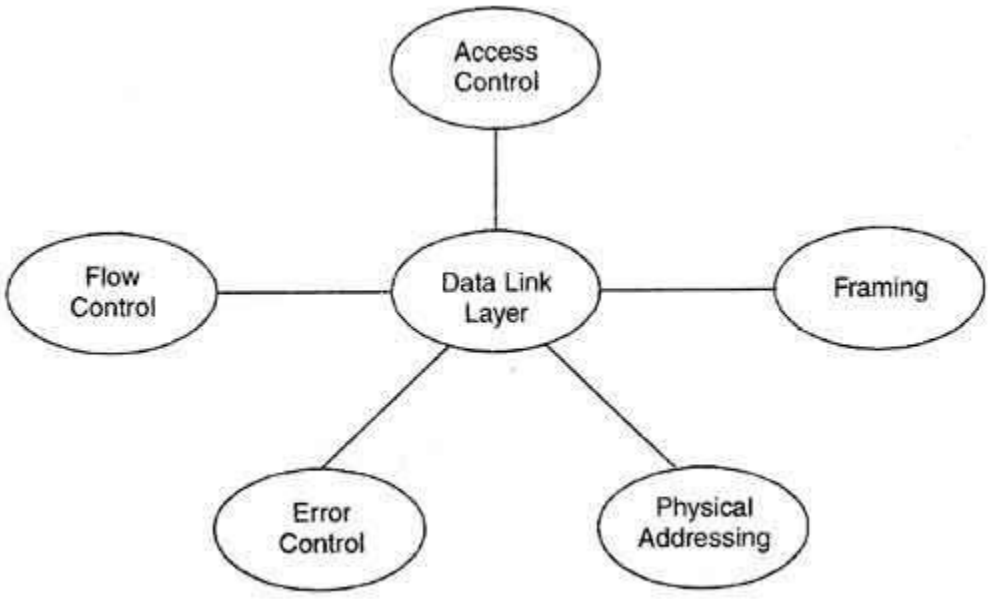
Data Link Layer Functions and Protocol: Error detection and error correction techniques; data-link control- framing and flow control; error recovery protocols- stop and wait ARQ, go-back-n ARQ; Point to Point Protocol on Internet.

DATA LINK LAYER FUNCTIONS AND PROTOCOL:

Data link layer is the second layer in OSI reference model and lies above the physical layer.

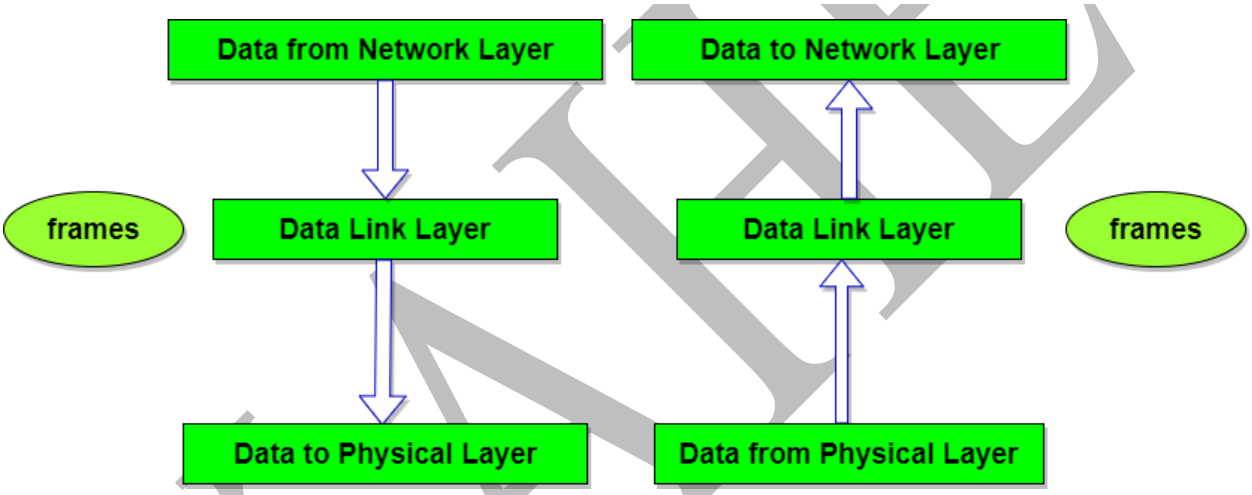
The data link layer performs the following functions.

1. **Framing:** Frames are the streams of bits received from the network layer into manageable data units. This division of stream of bits is done by Data Link Layer.
2. **Physical Addressing:** The Data Link layer adds a header to the frame in order to define physical address of the sender or receiver of the frame, if the frames are to be distributed to different systems on the network.



Functions of data link layer

3. **Flow Control:** A flow control mechanism to avoid a fast transmitter from running a slow receiver by buffering the extra bit is provided by flow control. This prevents traffic jam at the receiver side.
4. **Error Control:** Error control is achieved by adding a trailer at the end of the frame. Duplication of frames is also prevented by using this mechanism. Data Link Layers adds mechanism to prevent duplication of frames.
5. **Access Control:** Protocols of this layer determine which of the devices has control over the link at any given time, when two or more devices are connected to the same link.



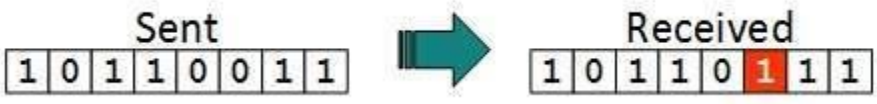
ERROR DETECTION AND ERROR CORRECTION TECHNIQUES:

Data-link layer uses some error control mechanism to ensure that frames (data bit streams) are transmitted with certain level of accuracy. But to understand how errors is controlled, it is essential to know what types of errors may occur.

Types of Errors

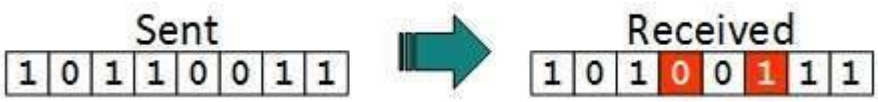
There may be three types of errors:

- **Single bit error**



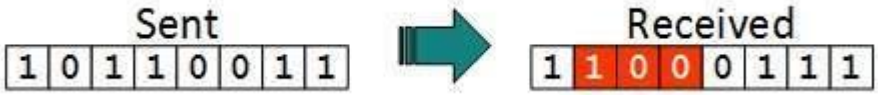
In a frame, there is only one bit, anywhere though, which is corrupt.

- **Multiple bits error**



Frame is received with more than one bit in corrupted state.

- **Burst error**



Frame contains more than1 consecutive bits corrupted.

Error control mechanism may involve two possible ways:

- Error detection
- Error correction

Error Detection

Errors in the received frames are detected by means of Parity Check and Cyclic Redundancy Check (CRC). In both cases, few extra bits are sent along with actual data to confirm that bits received at other end are same as they were sent. If the counter-check at receiver' end fails, the bits are considered corrupted.

Parity Check

One extra bit is sent along with the original bits to make number of 1s either even in case of even parity, or odd in case of odd parity.

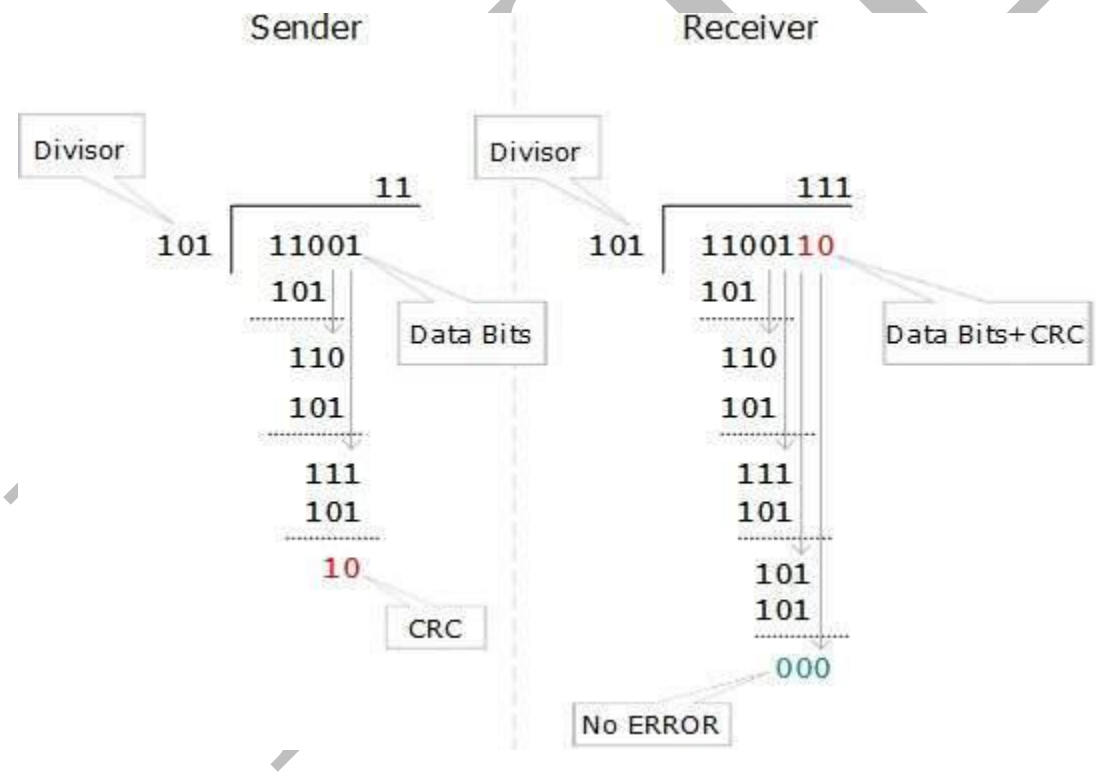
The sender while creating a frame counts the number of 1s in it. For example, if even parity is used and number of 1s is even then one bit with value 0 is added. This way number of 1s remains even. If the number of 1s is odd, to make it even a bit with value 1 is added.

The receiver simply counts the number of 1s in a frame. If the count of 1s is even and even parity is used, the frame is considered to be not-corrupted and is accepted. If the count of 1s is odd and odd parity is used, the frame is still not corrupted.

If a single bit flips in transit, the receiver can detect it by counting the number of 1s. But when more than one bit is erroneous, then it is very hard for the receiver to detect the error.

Cyclic Redundancy Check (CRC)

CRC is a different approach to detect if the received frame contains valid data. This technique involves binary division of the data bits being sent. The divisor is generated using polynomials. The sender performs a division operation on the bits being sent and calculates the remainder. Before sending the actual bits, the sender adds the remainder at the end of the actual bits. Actual data bits plus the remainder is called a codeword. The sender transmits data bits as codewords.



At the other end, the receiver performs division operation on codewords using the same CRC divisor. If the remainder contains all zeros the data bits are accepted, otherwise it is considered as there some data corruption occurred in transit.

Error Correction

In the digital world, error correction can be done in two ways:

- **Backward Error Correction** When the receiver detects an error in the data received, it requests back the sender to retransmit the data unit.
- **Forward Error Correction** When the receiver detects some error in the data received, it executes error-correcting code, which helps it to auto-recover and to correct some kinds of errors.

The first one, Backward Error Correction, is simple and can only be efficiently used where retransmitting is not expensive. For example, fiber optics. But in case of wireless transmission retransmitting may cost too much. In the latter case, Forward Error Correction is used.

To correct the error in data frame, the receiver must know exactly which bit in the frame is corrupted. To locate the bit in error, redundant bits are used as parity bits for error detection. For example, we take ASCII words (7 bits data), then there could be 8 kind of information we need: first seven bits to tell us which bit is error and one more bit to tell that there is no error.

For m data bits, r redundant bits are used. r bits can provide 2r combinations of information. In m+r bit codeword, there is possibility that the r bits themselves may get corrupted. So the number of r bits used must inform about m+r bit locations plus no-error information, i.e. m+r+1.

$$2^r >= m+r+1$$

DATA-LINK CONTROL- FRAMING AND FLOW CONTROL:

Data-link layer is responsible for implementation of point-to-point flow and error control mechanism.

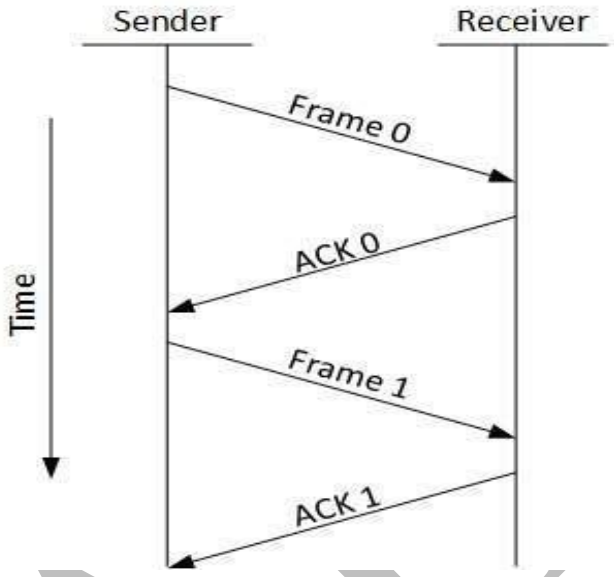
Flow Control

When a data frame (Layer-2 data) is sent from one host to another over a single medium, it is required that the sender and receiver should work at the same speed. That is, sender sends at a speed on which the receiver can process and accept the data. What if the speed (hardware/software) of the sender or receiver differs? If sender is sending too fast the receiver may be overloaded, (swamped) and data may be lost.

Two types of mechanisms can be deployed to control the flow:

- **Stop and Wait**

This flow control mechanism forces the sender after transmitting a data frame to stop and wait until the acknowledgement of the data-frame sent is received.



- **Sliding Window**

In this flow control mechanism, both sender and receiver agree on the number of data-frames after which the acknowledgement should be sent. As we learnt, stop and wait flow control mechanism wastes resources, this protocol tries to make use of underlying resources as much as possible.

Error Control

When data-frame is transmitted, there is a probability that data-frame may be lost in the transit or it is received corrupted. In both cases, the receiver does not receive the correct data-frame and sender does not know anything about any loss. In such case, both sender and receiver are equipped with some protocols which help them to detect transit errors such as loss of data-frame. Hence, either the sender retransmits the data-frame or the receiver may request to resend the previous data-frame.

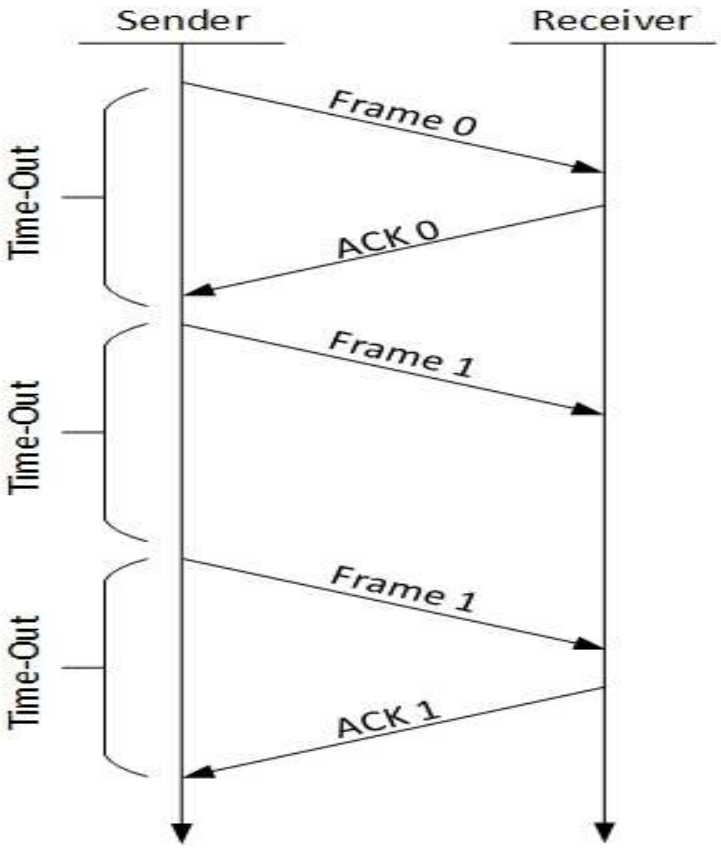
Requirements for error control mechanism:

- **Error detection** - The sender and receiver, either both or any, must ascertain that there is some error in the transit.

- **Positive ACK** - When the receiver receives a correct frame, it should acknowledge it.
- **Negative ACK** - When the receiver receives a damaged frame or a duplicate frame, it sends a NACK back to the sender and the sender must retransmit the correct frame.
- **Retransmission:** The sender maintains a clock and sets a timeout period. If an acknowledgement of a data-frame previously transmitted does not arrive before the timeout the sender retransmits the frame, thinking that the frame or it's acknowledgement is lost in transit.

There are three types of techniques available which Data-link layer may deploy to control the errors by Automatic Repeat Requests (ARQ):

- **Stop-and-wait ARQ**



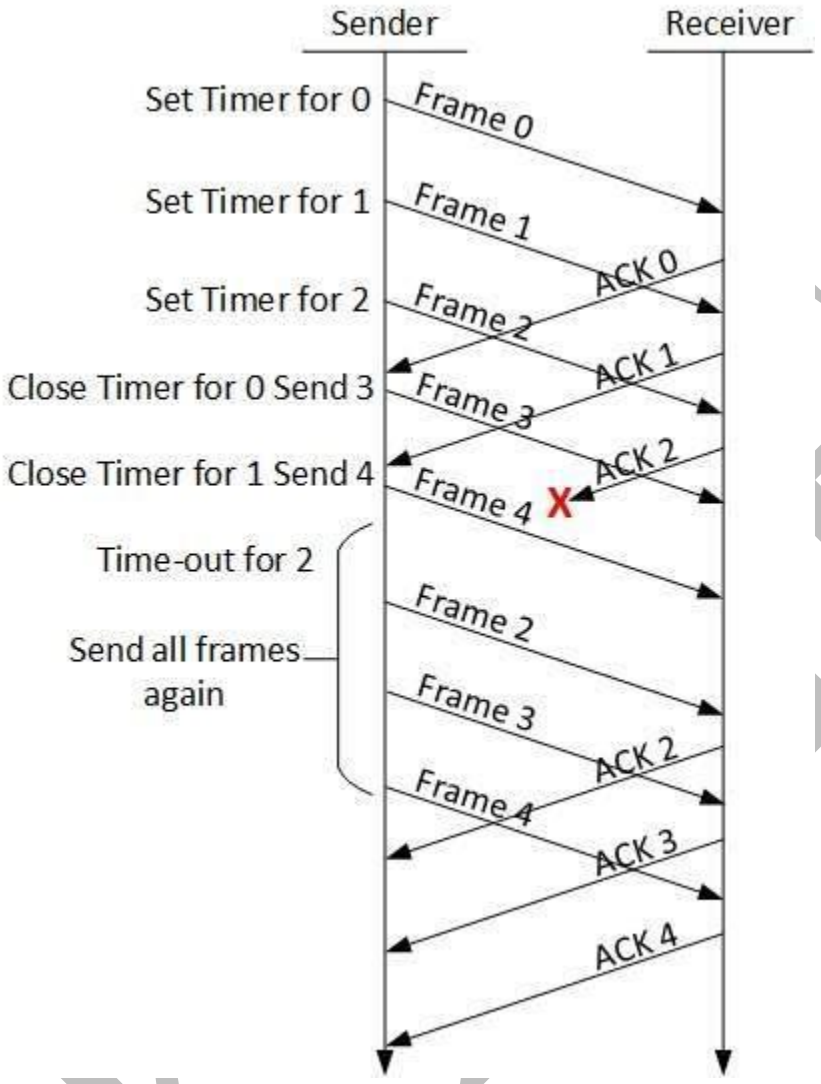
The following transition may occur in Stop-and-Wait ARQ:

- The sender maintains a timeout counter.

- When a frame is sent, the sender starts the timeout counter.
- If acknowledgement of frame comes in time, the sender transmits the next frame in queue.
- If acknowledgement does not come in time, the sender assumes that either the frame or its acknowledgement is lost in transit. Sender retransmits the frame and starts the timeout counter.
- If a negative acknowledgement is received, the sender retransmits the frame.

- **Go-Back-N ARQ**

Stop and wait ARQ mechanism does not utilize the resources at their best. When the acknowledgement is received, the sender sits idle and does nothing. In Go-Back-N ARQ method, both sender and receiver maintain a window.

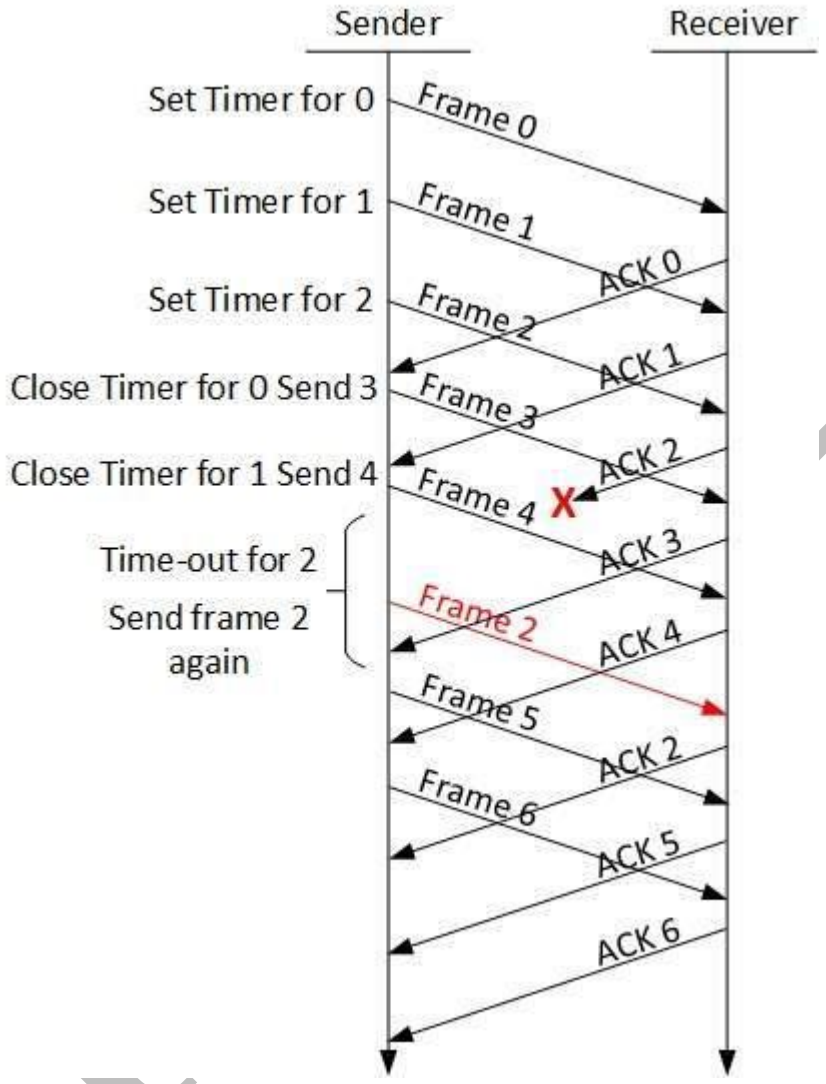


The sending-window size enables the sender to send multiple frames without receiving the acknowledgement of the previous ones. The receiving-window enables the receiver to receive multiple frames and acknowledge them. The receiver keeps track of incoming frame's sequence number.

When the sender sends all the frames in window, it checks up to what sequence number it has received positive acknowledgement. If all frames are positively acknowledged, the sender sends next set of frames. If sender finds that it has received NACK or has not received any ACK for a particular frame, it retransmits all the frames after which it does not receive any positive ACK.

- **Selective Repeat ARQ**

In Go-back-N ARQ, it is assumed that the receiver does not have any buffer space for its window size and has to process each frame as it comes. This enforces the sender to retransmit all the frames which are not acknowledged.



In Selective-Repeat ARQ, the receiver while keeping track of sequence numbers, buffers the frames in memory and sends NACK for only frame which is missing or damaged.

The sender in this case, sends only packet for which NACK is received.

Error Recovery Protocols:

It allows the receiver to inform the sender if a frame is lost or damaged during transmission and coordinates the retransmission of those frames by the sender. Error control in the data link layer is based on automatic repeat request (ARQ). Whenever an error is detected, specified frames are retransmitted.

STOP AND WAIT ARQ:

Characteristics

- Used in Connection-oriented communication.
- It offers error and flow control
- It is used in Data Link and Transport Layers
- Stop and Wait ARQ mainly implements Sliding Window Protocol concept with Window Size 1

Useful Terms:

1. **Propagation Delay:** Amount of time taken by a packet to make a physical journey from one router to another router.
   Propagation Delay = (Distance between routers) / (Velocity of propagation)
2. RoundTripTime (**RTT**) = 2* Propagation Delay
3. TimeOut (**TO**) = 2* RTT
4. Time To Live (**TTL**) = 2* TimeOut. (Maximum TTL is 180 seconds)

Simple Stop and Wait

Sender:

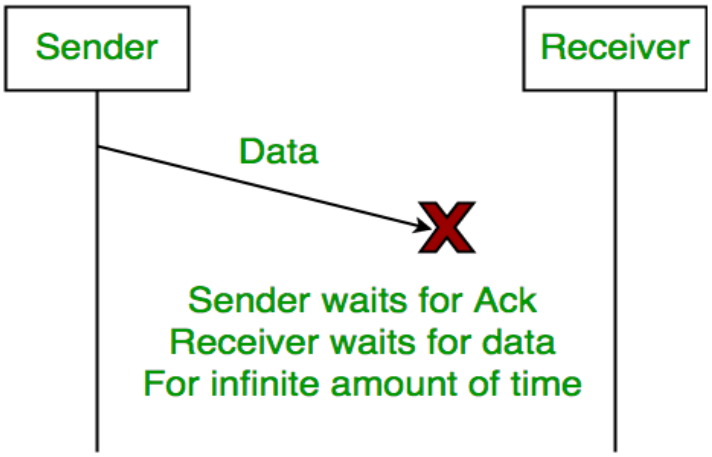
Rule 1) Send one data packet at a time.
Rule 2) send next packet only after receiving acknowledgement for previous.

Receiver:

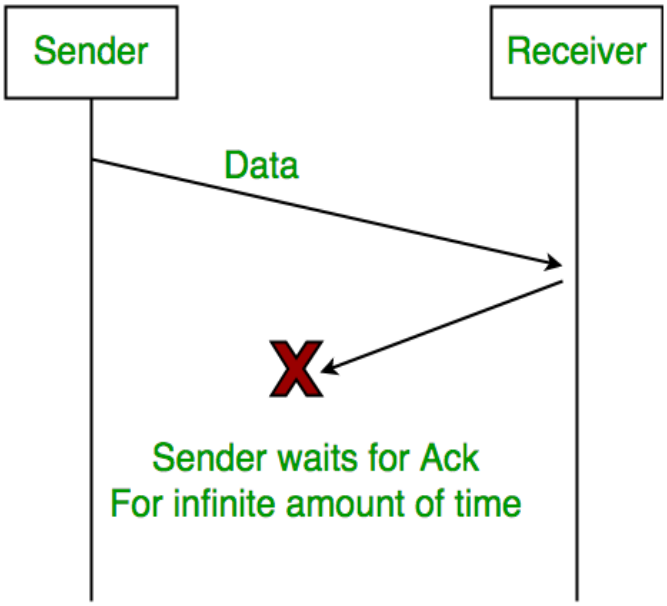
Rule 1) Send acknowledgement after receiving and consuming of data packet.
Rule 2) After consuming packet acknowledgement need to be sent (Flow Control)

Problems:

1. Lost Data



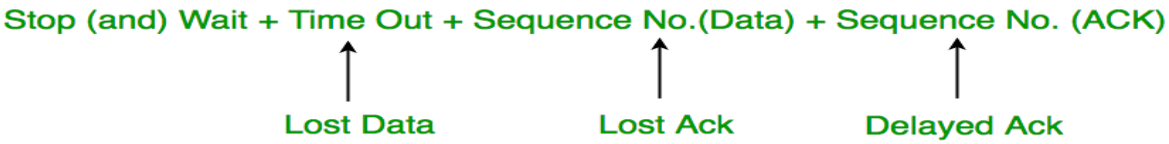
2. Lost Acknowledgement:



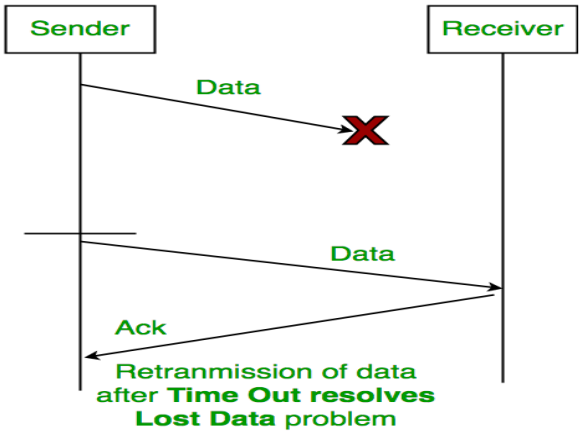
3. Delayed Acknowledgement/Data: After timeout on sender side, a long delayed acknowledgement might be wrongly considered as acknowledgement of some other recent packet.

Stop and Wait ARQ (Automatic Repeat Request)

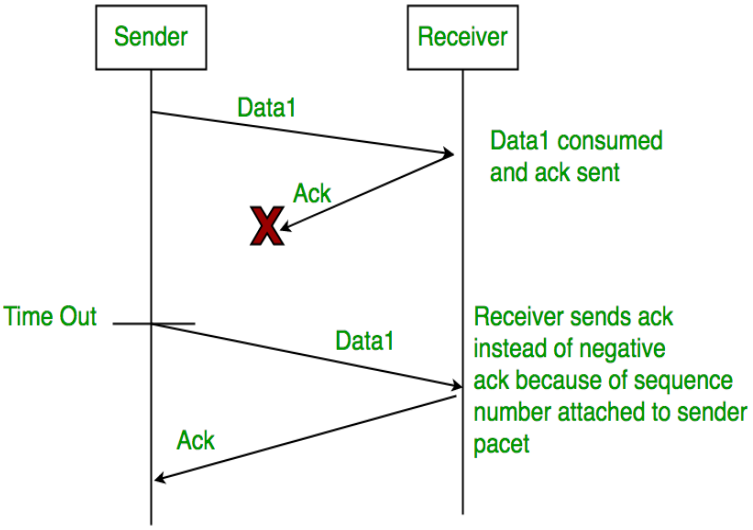
Above 3 problems are resolved by Stop and Wait ARQ (Automatic Repeat Request) that does both error control and flow control.



1. Time Out:



2. Sequence Number (Data)

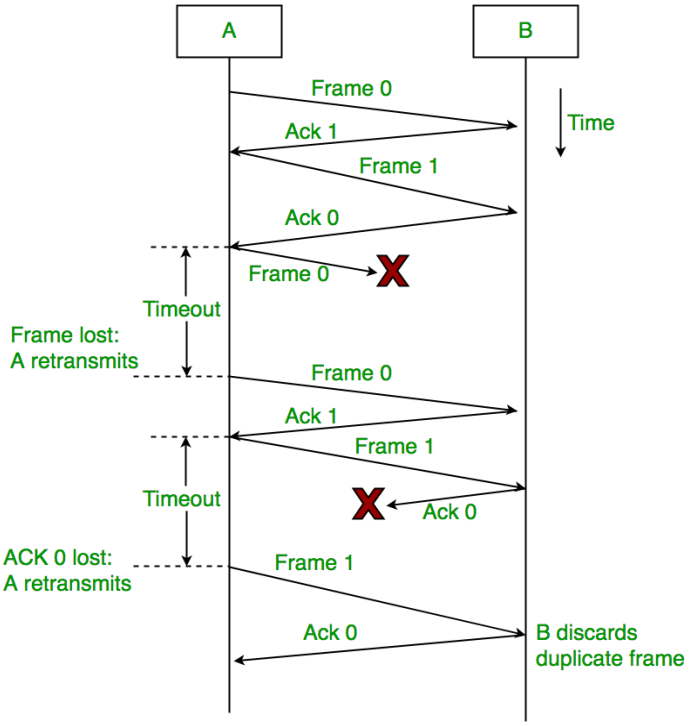


3. Delayed Acknowledgement:

This is resolved by introducing sequence number for acknowledgement also.

Working of Stop and Wait ARQ:

1) Sender A sends a data frame or packet with sequence number 0.
2) Receiver B, after receiving data frame, sends and acknowledgement with sequence number 1 (sequence number of next expected data frame or packet)
There is only one bit sequence number that implies that both sender and receiver have buffer for one frame or packet only.



Characteristics of Stop and Wait ARQ:

- It uses link between sender and receiver as half duplex link
- Throughput = 1 Data packet/frame per RTT
- If Bandwidth*Delay product is very high, then stop and wait protocol is not so useful. The sender has to keep waiting for acknowledgements before sending the processed next packet.
- It is an example for "**Closed Loop OR connection oriented** " protocols
- It is an special category of SWP where its window size is 1
- Irrespective of number of packets sender is having stop and wait protocol requires only 2 sequence numbers 0 and 1

The Stop and Wait ARQ solves main three problems, but may cause big performance issues as sender always waits for acknowledgement even if it has next packet ready to send. Consider a situation where you have a high bandwidth connection and propagation delay is also high (you

are connected to some server in some other country though a high speed connection). To solve this problem, we can send more than one packet at a time with a larger sequence numbers. So Stop and Wait ARQ may work fine where propagation delay is very less for example LAN connections, but performs badly for distant connections like satellite connection.

Sliding Window Protocol | Set 1 (Sender Side)

The Stop and Wait ARQ offers error and flow control, but may cause big performance issues as sender always waits for acknowledgement even if it has next packet ready to send. Consider a situation where you have a high bandwidth connection and propagation delay is also high (you are connected to some server in some other country though a high speed connection); you can't use this full speed due to limitations of stop and wait.

Sliding Window protocol handles this efficiency issue by sending more than one packet at a time with a larger sequence numbers. The idea is same as pipelining in architectures.

Few Terminologies:

Transmission Delay (Tt) – Time to transmit the packet from host to the outgoing link. If B is the Bandwidth of the link and D is the Data Size to transmit

Tt = D/B

Propagation Delay (Tp) – It is the time taken by the first bit transferred by the host onto the outgoing link to reach the destination. It depends on the distance d and the wave propagation speed s (depends on the characteristics of the medium).

Tp = d/s

Efficiency – It is defined as the ratio of total useful time to the total cycle time of a packet. For stop and wait protocol,

Total cycle time = Tt(data) + Tp(data) +

Tt(acknowledgement) + Tp(acknowledgement)

= Tt(data) + Tp(data) + Tp(acknowledgement)

= Tt + 2*Tp

Since acknowledgements are very less in size, their transmission delay can be neglected.

Efficiency = Useful Time / Total Cycle Time

= Tt/(Tt + 2*Tp) (For Stop and Wait)

= 1/(1+2a) [Using a = Tp/Tt]

Effective Bandwidth(EB) or Throughput – Number of bits sent per second.

EB = Data Size(L) / Total Cycle time(Tt + 2*Tp)

Multiplying and dividing by Bandwidth (B),

= (1/(1+2a)) * B [Using a = Tp/Tt]

= Efficiency * Bandwidth

Capacity of link – If a channel is Full Duplex, then bits can be transferred in both the directions and without any collisions. Number of bits a channel/Link can hold at maximum is its capacity.

Capacity = Bandwidth(B) * Propagation(Tp)

For Full Duplex channels,

Capacity = 2*Bandwidth(B) * Propagation(Tp)

Concept of Pipelining

In Stop and Wait protocol, only 1 packet is transmitted onto the link and then sender waits for acknowledgement from the receiver. The problem in this setup is that efficiency is very less as we are not filling the channel with more packets after 1st packet has been put onto the link. Within the total cycle time of Tt + 2*Tp units, we will now calculate the maximum number of packets that sender can transmit on the link before getting an acknowledgement.

In Tt units ----> 1 packet is Transmitted.

In 1 units ----> 1/Tt packet can be Transmitted.

In Tt + 2*Tp units -----> (Tt + 2*Tp)/Tt

packets can be Transmitted

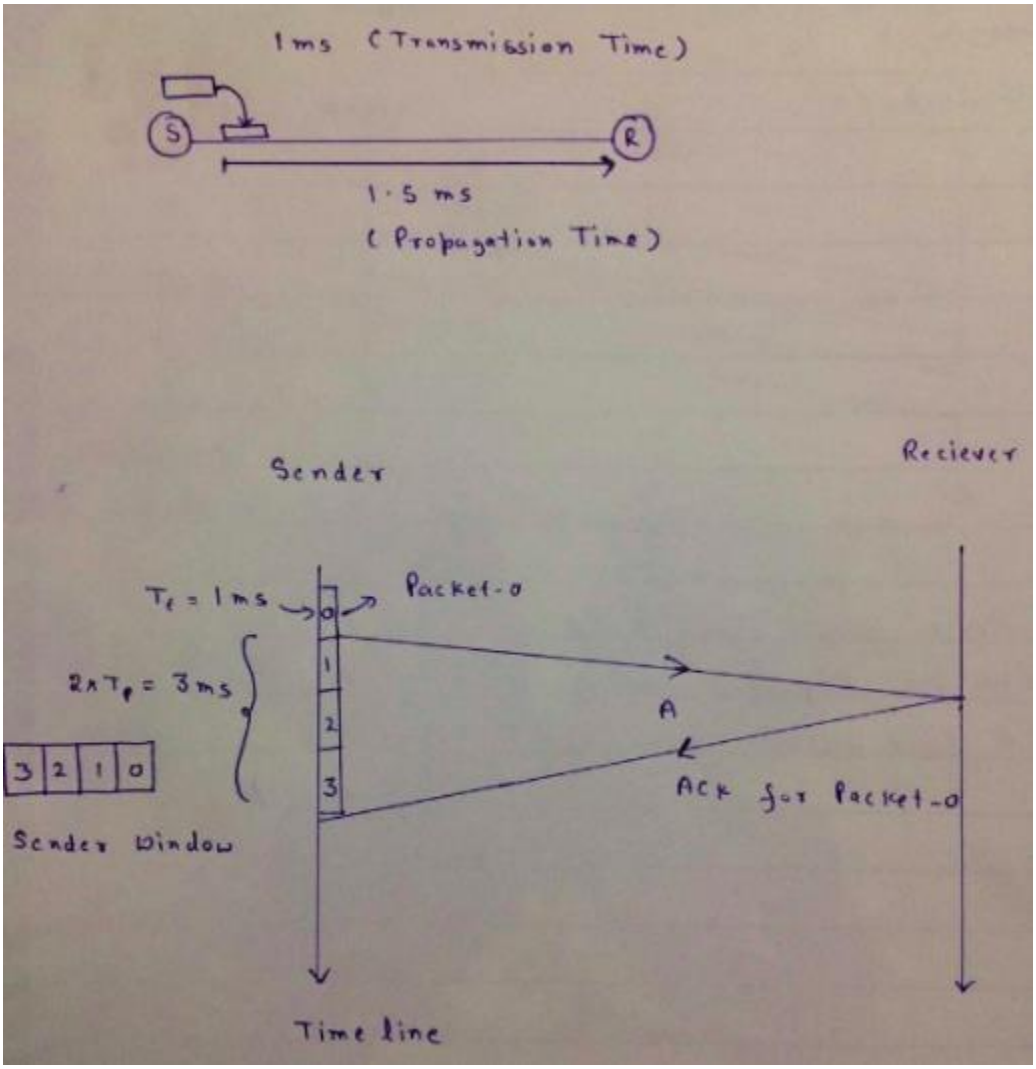
------> 1 + 2a [Using a = Tp/Tt]

Maximum packets That can be Transmitted in total cycle time = 1+2*a

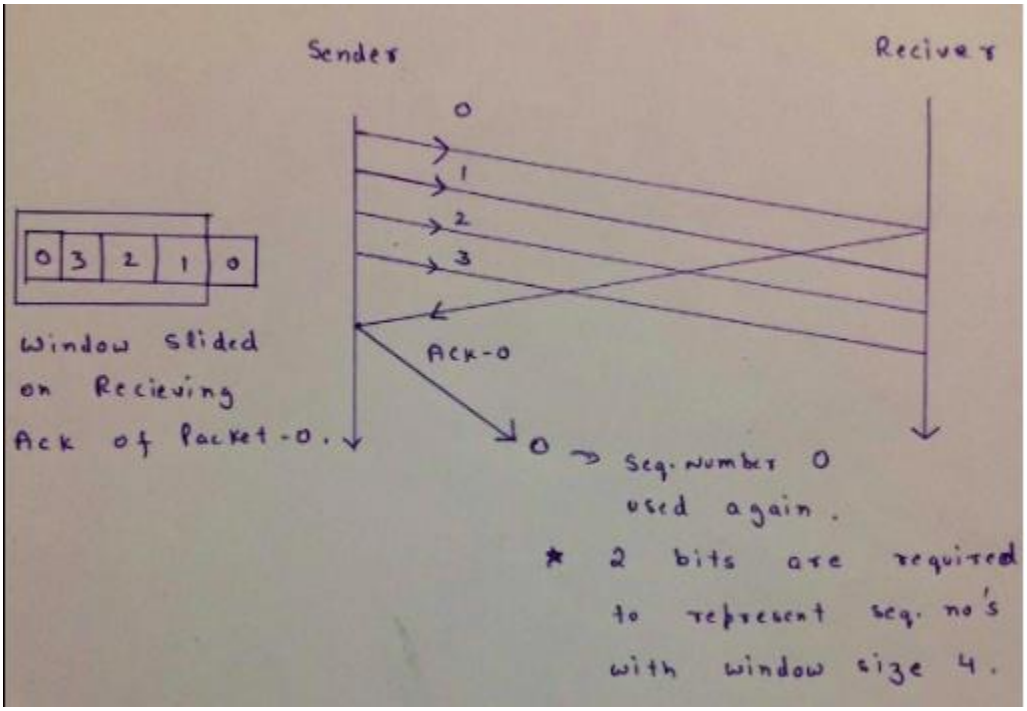
Let me explain now with the help of an example.

Consider Tt = 1ms, Tp = 1.5ms.

In the picture given below, after sender has transmitted packet 0, it will immediately transmit packets 1, 2, 3. Acknowledgement for 0 will arrive after 2*1.5 = 3ms. In Stop and Wait, in time 1 + 2*1.5 = 4ms, we were transferring one packet only. Here we keep a **window of packets which we have transmitted but not yet acknowledged**.



After we have received the Ack for packet 0, window slides and the next packet can be assigned sequence number 0. We reuse the sequence numbers which we have acknowledged so that header size can be kept minimum as shown in the diagram given below.



Minimum Number of Bits for Sender window (Very Important For GATE)

As we have seen above,

Maximum window size = 1 + 2*a where a = Tp/Tt

Minimum sequence numbers required = 1 + 2*a.

All the packets in the current window will be given a sequence number. Number of bits required to represent the sender window = ceil(log2(1+2*a)).

But sometimes number of bits in the protocol headers is pre-defined. Size of sequence number field in header will also determine the maximum number of packets that we can send in total cycle time. If N is the size of sequence number field in the header in bits, then we can have 2^N sequence numbers.

Window Size ws = min(1+2*a, 2^N)

If you want to calculate minimum bits required to represent sequence numbers/sender window, it will be **ceil(log2(ws))**.

SLIDING WINDOW PROTOCOL | SET 2 (RECEIVER SIDE):

Sliding Window Protocol is actually a theoretical concept in which we have only talked about what should be the sender window size (1+2a) in order to increase the efficiency of stop and wait arq. Now we will talk about the practical implementations in which we take care of

what should be the size of receiver window. Practically it is implemented in two protocols namely :

1. Go Back N (GBN)
2. Selective Repeat (SR)

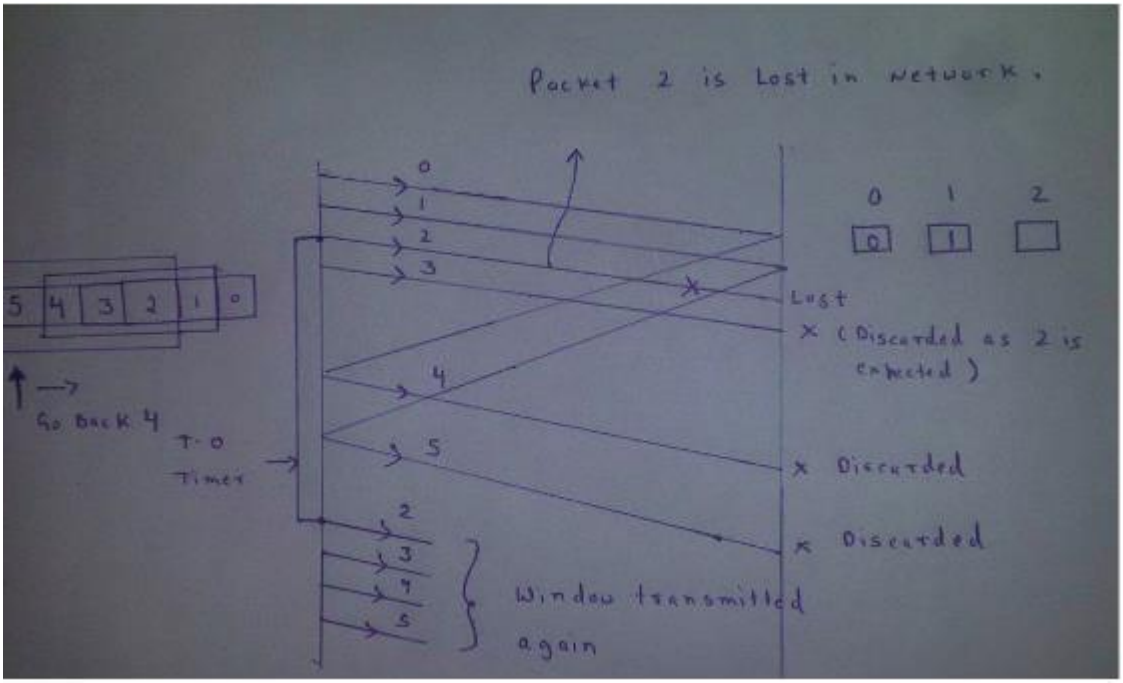
In this article, we will explain you about the first protocol which is GBN in terms of three main characteristic features and in the last part we will be discussing SR as well as comparison of both these protocols

Sender Window Size (WS)
It is N itself. If we say protocol is GB10, then Ws = 10. N should be always greater than 1 in order to implement pipelining. For N = 1, it reduces to Stop and Wait protocol.

Efficiency Of GBN = N/(1+2a) Where a = Tp/Tt

If B is the bandwidth of the channel, then Effective Bandwidth or Throughput = Efficiency * Bandwidth = (N/(1+2a)) * B.

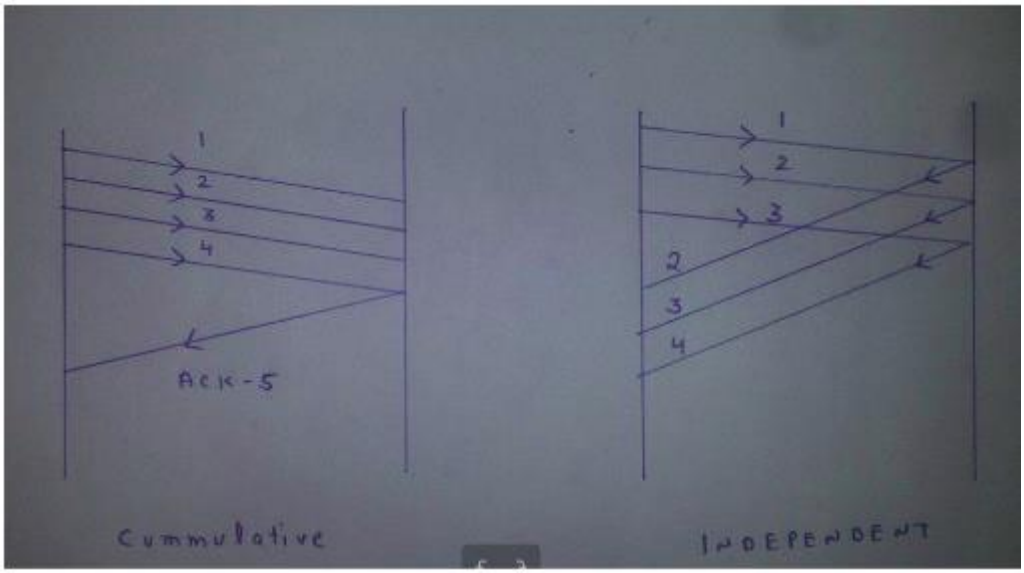
Receiver Window Size (WR)
WR is always 1 in GBN.
Now what exactly happens in GBN, we will explain with a help of example. Consider the diagram given below. We have sender window size of 4. Assume that we have lots of sequence numbers just for the sake of explanation. Now the sender has sent the packets 0, 1, 2 and 3. After acknowledging the packets 0 and 1, receiver is now expecting packet 2 and sender window has also slided to further transmit the packets 4 and 5. Now suppose the packet 2 is lost in the network, Receiver will discard all the packets which sender has transmitted after packet 2 as it is expecting sequence number of 2. On the sender side for every packet send there is a time out timer which will expire for packet number 2. Now from the last transmitted packet 5 senders will go back to the packet number 2 in the current window and transmit all the packets till packet number 5. That's why it is called Go Back N. Go back means sender has to go back N places from the last transmitted packet in the unacknowledged window and not from the point where the packet is lost.



Acknowledgements

There are 2 kinds of acknowledgements namely:

- **Cumulative Ack** – One acknowledgement is used for many packets. Main advantage is traffic is less. Disadvantage is less reliability as if one ack is loss that would mean that all the packets sent are lost.
- **Independent Ack** – If every packet is going to get acknowledgement independently. Reliability is high here but disadvantage is that traffic is also high since for every packet we are receiving independent ack.



GBN uses Cumulative Acknowledgement. At the receiver side, it starts a acknowledgement timer whenever receiver receives any packet which is fixed and when it expires, it is going to send a cumulative Ack for the number of packets received in that interval of timer. If receiver has received N packets, then the Acknowledgement number will be N+1. Important point is Acknowledgement timer will not start after the expiry of first timer but after receiver has received a packet.
Time out timer at the sender side should be greater than Acknowledgement timer.

POINT TO POINT PROTOCOL ON INTERNET:

PPP is most commonly used data link protocol. It is used to connect the Home PC to the server of ISP via a modem.

• This protocol offers several facilities that were not present in SLIP. Some of these facilities are:

1. PPP defines the format of the frame to be exchanged between the devices.

2. It defines link control protocol (LCP) for:-

(a) Establishing the link between two devices.

(b) Maintaining this established link.

(c) Configuring this link.

(d) Terminating this link after the transfer.

3. It defines how network layer data are encapsulated in data link frame.

4. PPP provides error detection.

5. Unlike SLIP that supports only IP, PPP supports multiple protocols.

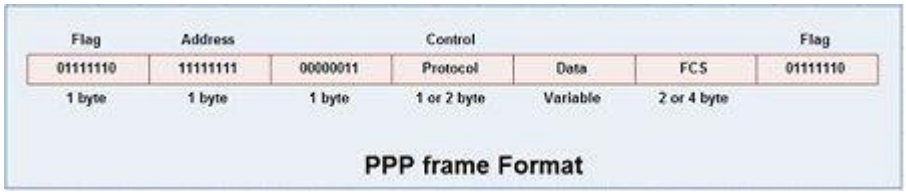
6. PPP allows the IP address to be assigned at the connection time i.e. dynamically. Thus a temporary IP address can be assigned to each host.

7. PPP provides multiple network layer services supporting a variety of network layer protocol. For this PPP uses a protocol called NCP (Network Control Protocol).

8. It also defines how two devices can authenticate each other.

PPP Frame Format

The frame format of PPP resembles HDLC frame. Its various fields are:



PPP frame Format

1. **Flag field**: Flag field marks the beginning and end of the PPP frame. Flag byte is 01111110. (1 byte).

2. **Address field**: This field is of 1 byte and is always 11111111. This address is the broadcast address *i.e.* all the stations accept this frame.

3. **Control field**: This field is also of 1 byte. This field uses the format of the U-frame (unnumbered) in HDLC. The value is always 00000011 to show that the frame does not contain any sequence numbers and there is no flow control or error control.

4. **Protocol field**: This field specifies the kind of packet in the data field *i.e.* what is being carried in data field.

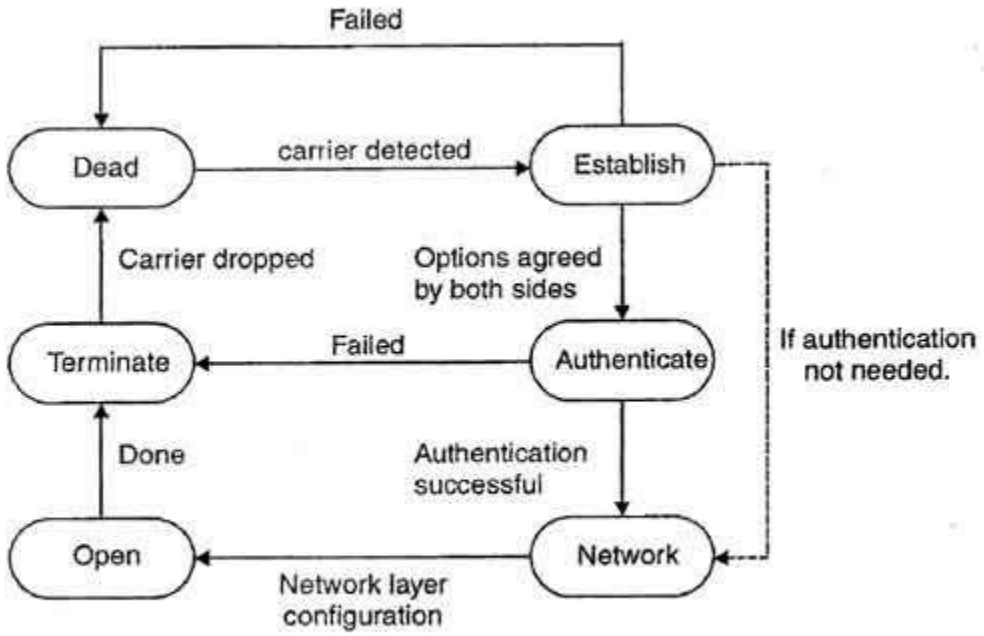
5. **Data field**: Its length is variable. If the length is not negotiated using LCP during line set up, a default length of 1500 bytes is used. It carries user data or other information.

6. **FCS field**: The frame checks sequence. It is either of 2 bytes or 4 bytes. It contains the checksum.

Transition Phases in PPP

The PPP connection goes through different states as shown in fig.

1. **Dead**: In dead phase the link is not used. There is no active carrier and the line is quiet.



Transition phases

2. **Establish**: Connection goes into this phase when one of the nodes start communication. In this phase, two parties negotiate the options. If negotiation is successful, the system goes into authentication phase or directly to networking phase. LCP packets are used for this purpose.

3. **Authenticate**: This phase is optional. The two nodes may decide during the establishment phase, not to skip this phase. However if they decide to proceed with authentication, they send several authentication packets. If the result is successful, the connection goes to the networking phase; otherwise, it goes to the termination phase.

4. **Network**: In network phase, negotiation for the network layer protocols takes place. PPP specifies that two nodes establish a network layer agreement before data at the network layer can be exchanged. This is because PPP supports several protocols at network layer. If a node is running multiple protocols simultaneously at the network layer, the receiving node needs to know which protocol will receive the data.

5. **Open**: In this phase, data transfer takes place. The connection remains in this phase until one of the endpoints wants to end the connection.

6. **Terminate**: In this phase connection is terminated.

Point-to-point protocol Stack

PPP uses several other protocols to establish link, authenticate users and to carry the network layer data.

The various protocols used are:

1. Link Control Protocol

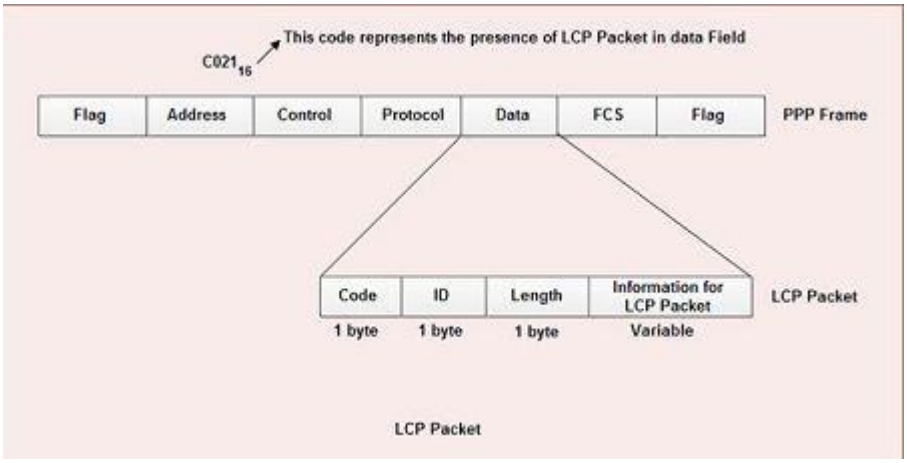
2. Authentication Protocol

3. Network Control Protocol

1. Link Control Protocol

• It is responsible for establishing, maintaining, configuring and terminating the link.

• It provides negotiation mechanism to set options between two endpoints.



• All LCP packets are carried in the data field of the PPP frame.

• The presence of a value $C021_{16}$ in the protocol field of PPP frame indicates that LCP packet is present in the data field.

• The various fields present in LCP packet are:

1. **Code**: 1 byte-specifies the type of LCP packet.

2. I**D**: 1 byte-holds a value used to match a request with the reply.

3. **Length**: 2 byte-specifies the length of entire LCP packet.

4. **Information**: Contains extra information required for some LCP packet.

• There are eleven different type of LCP packets. These are categorized in three groups:

1. **Configuration packet**: These are used to negotiate options between the two ends. For example: configure-request, configure-ack, configure-nak, configure-reject are some configuration packets.

2. **Link termination packets**: These are used to disconnect the link between two end points. For example: terminate-request, terminate-ack, are some link termination packets.

3. **Link monitoring and debugging packets**: These are used to monitor and debug the links. For example: code-reject, protocol-reject, echo-request, echo-reply and discard-request are some link monitoring and debugging packets.

2. Authentication Protocol

Authentication protocols help to validate the identity of a user who needs to access the resources.

There are two authentication protocols:

1. Password Authentication Protocols (PAP)

2. Challenge Handshake Authentication Protocol (CHAP)

1. PAP (Password Authentication Protocol)

This protocol provides two step authentication procedures:

Step 1: User name and password is provided by the user who wants to access a system.

Step 2: The system checks the validity of user name and password and either accepts or denies the connection.

• PAP packets are also carried in the data field of PPP frames.

• The presence of PAP packet is identified by the value $C023_{16}$ in the protocol field of PPP frame.

• There are three PAP packets.

1. **Authenticate-request**: used to send user name & password.

2. **Authenticate-ack**: used by system to allow the access.

3. **Authenticate-nak**: used by system to deny the access.

2. CHAP (Challenge Handshake Authentication Protocol)

• It provides more security than PAP.

• In this method, password is kept secret, it is never sent on-line.

• It is a three-way handshaking authentication protocol:

1. System sends. a challenge packet to the user. This packet contains a value, usually a few bytes.

2. Using a predefined function, a user combines this challenge value with the user password and sends the resultant packet back to the system.

3. System then applies the same function to the password of the user and challenge value and creates a result. If result is same as the result sent in the response packet, access is granted, otherwise, it is denied.

• There are 4 types of CHAP packets:

1. Challenge-used by system to send challenge value.

2. Response-used by the user to return the result of the calculation.

3. Success-used by system to allow access to the system.

4. Failure-used by the system to deny access to the system.

3. Network Control Protocol (NCP)

• After establishing the link and authenticating the user, PPP connects to the network layer. This connection is established by NCP.

• Therefore NCP is a set of control protocols that allow the encapsulation of the data coming from network layer.

• After the network layer configuration is done by one of the NCP protocols, the users can exchange data from the network layer.

• PPP can carry a network layer data packet from protocols defined by the Internet, DECNET, Apple Talk, Novell, OSI, Xerox and so on.

• None of the NCP packets carry networks layer data. They just configure the link at the network layer for the incoming data.

POSSIBLE QUESTIONS

UNIT-III

PART-A (20 MARKS)

(Q.NO 1 TO 20 Online Examination)

PART-B (2 MARKS)

1. What are the responsibilities of Data Link Layer?
2. Define error detection and error correction.
3. What are the error recovery protocols?
4. Define Stop and Wait Protocol.
5. Define Go back and N protocol.
6. What is selective repeat protocol?

PART-C (6 MARKS)

1. Give an account of Error correction and Detections in detail.
2. Explain the concept of cyclic codes error detection and correction.
3. Explain cyclic redundancy check with the help of an example.
4. Elaborate the working of flow control protocols with neat sketches.
5. Illustrate data-link control with proper diagram.
6. Describe the stop and wait ARQ with proper diagram
7. Explain go back n ARQ with neat sketch.
8. Explain Point to Point Protocol on Internet.

Questions	opt1	opt2	opt3
Transmission errors are usually detected at the……..layer of OSI model	physical	datalink	network
Transmission errors are usually corrected at the……..layer of OSI model	network	transport	datalink
Datalink layer imposes a ……mechanism to avoid overwhelming the receiver	flow control	error control	access control
Error control mechanism of datalink layer is achieved through a ……..added to the end of frame.	header	trailer	adress
The datalink layer is responsible for moving……from one hop to next	packets	frames	signals
In a single_bit error,how many bits in a data unit are changed	one	two	four
In a burst error,how many bits in a data unit are changed	less than 2	2 or more than 2	2
The length of the burst error is measured from ……	first bit to last bit	first corrupted bit to last corrupted bit	two
Single bit error will least occur in……data transmissions	serial	parallel	synchronous
To detect errors or correct errors,we need to send …… with data	address	frames	extra bits
Which of the following best describes a single bit error	a single bit is inverted	a single bit is inverted per data unit	a single bit is inverted per transmission
In block coding,we divide our message intp blocks,each of k bits,called	dataword	codeword	integers
In block coding,the length of the block is …….	k	r	k+r
Block coding can detect only ……error	single	burst	multiple
We need ……..redundant bits for error correction than for error detection	less	more	equal
The corresponding codeword for the dataword 01 is…..	011	000	101
The hamming distance can easily be found if we apply the …… operation	XOR	OR	AND

The …… hamming distance is the smallest hamming distance between all possible pairs in a set of words	minimum	maximum	equal
The hamming distance d(000,111) is …….	1	0	2
To guarantee correction of upto t errors in all cases,the minimum hamming distance in a block code must be …..	d(min)=2t+1	d(min)=2t-1	d(min)=2t
To guarantee correction of upto s errors in all cases,the minimum hamming distance in a block code must be …..	d(min)=s-1	d(min)=s+1	d(min)=s
A simple_parity check code is a single bit error detecting code in which n=…… with d(min)=2	K	K*1	K-1
The codeword corresponding to the dataword 1111 is	11110	11111	11101
A simple_parity check code can detect an ……. Number of errors	odd	even	prime
The hamming code is a method of ……..	error detection	error correcton	error encapsulation
To make the hamming code respond to a burst error of size N,we neeed to make …… codewords of our frame	N+1	N-1	N
CRC is used in network such as …….	WAN	LAN and WAN	LAN
In CRC there is no error if the remainder at the receiver is……..	equal to the remainder at the sender	all 0's	non zero
At the CRC checker,…….means that the dataunit is damaged.	string of 0's	string of 1's	a string of alternating 1's and 0's
……. Is a regulation of data transmission so that the receiver buffer do not become overwhelmed	flow control	error control	access control
……..in the datalink layer separates a message from one source ti a destination or from other message to other destinations	packets	address	framing

…….is the process of adding 1 extra byte whenever there is a flag or escape character in text	byte stuffing	redundancy	bit stuffing
…….is the process of adding 1 extra 0 whenever five consecutive 1's follows a 0 in the data.	byte stuffing	redundancy	bit stuffing
……in the data link layer is based on automatic repeat request,which is the retransmission of data	error control	flow control	access control
At any time an error is detected in an exchange specified frames are retransmitted and process is called….	ARQ	ACK	NAK
The datalink layer at the sender side gets data from its……..layer	network	physical	application
ARQ stands for ……..	acknowledge repeat request	automatic repeat request	automatic repeat quantisation
Which of the following is a data link layer function	line discipline	error control	flow control
In protocols the flow and error control information such as ACK and NAK is included in the data frames in a technique called……	stop and wait	go_back	A and B
In stop and wait ARQ ,the sequence of numbers is based on…….	modulo-2-arithmetic	modulo-12-arithmetic	modulo-N-arithmetic
Error correction in …….is done by keeping a copy of the send frames and retransmitting of the frame when time expires	stop and wait ARQ	ARQ	ACK
In the Go_Back N protocol,the sequence numbers are modulo……..	2^m	2^{m-1}	2^{m+1}
In sliding window ,the range which is the concern of the sender is called……..	send sliding window	receive sliding window	piggybacking
Piggypacking is used to improve the efficiency of the ……..protocols.	bidirectional	unidirectional	multidirectional

The send window can slide …….slots when a valid acknowledgment arrive	one or more	one	two
The upper sublayer that is responsible for flow and error control is called…….control	logical	media access	logical and physical
The MAC(media access control)sublayer co-ordinates the datalink task within a specified……..	LAN	MAN	WAN
The lower sublayer that is responsible for multiple access resolution is called ……control	Logical	media access	logical and physical
In the sliding window method or flow control several frame can be be ……..at a time	transit	received	logical and physical
The sliding window of the sender expands to the ……..when acknowledgement are received	left	middle	right
Error detecting codes require ……..nuber of redundant bits.	less	equal	more
The datalink layer transforms the ……,a raw transmission facility to a reliable link and is responsible for node_to_node delivery.	datalink	physical	network
Datalink layer divided into …… functionality oriented sublayer.	one	zero	two
The send window in Go_Back N maximum size can be ……	2^m	2^{m+1}	2
In stop and wait ARQ and Go_Back_N ARQ,the size of the send window is…….	0	3	1
The relationship between m and n in hamming code is ……	n=2m-1	n=m	n=m-1
A simple parity_check code is a single_bit error detecting code in which n=k+1 with d_{min}	3	1	0

……..mechanism of datalink layer is achieved through added to the trailer added to the end of frame.	ARQ	ARC	Error control
In ……,we divide our message into blocks	convolution coding	block coding	linear coding
The …….layer at the sender site gets data from its network layer.	physical	datalink	application
In the …….protocol,the sequence numbers are modulo 2^m	Go_Back N	Simplest	Stop and wait

opt4	opt5	opt6	Answer
transport			physical
physical			transport
none of the above			flow control
frames			trailer
message			frames
five			one
3			2 or more than 2
three			first corrupted bit to last corrupted bit
asynchronous			serial
packets			extra bits
any of the above			a single bit is inverted per data unit
decimal			dataword
k-r			k+r
type			single
less than or equal to			more
110			011
NAND			XOR

not equal			minimum
3			2
d(min)=t+1			d(min)=2t+1
d(min)=0			d(min)=s+1
K+1			K+1
11011			11110
non- prime			odd
error detection and correction			error correcton
0			N
MAN			LAN and WAN
the quotient at the sender			all 0's
a non-zero remainder			a non-zero remainder
connection control			flow control
switching			framing

character stuffing			byte stuffing
character stuffing			bit stuffing
connection control			error control
SEL			ARQ
transport			network
automatic retransmission request			automatic repeat quantisation
all the above			all the above
piggybacking			piggybacking
modulo-1-arithmetic			modulo-2-arithmetic
NAQ			stop and wait ARQ
2			2m
sliding			send sliding window
omnidirectional			bidirectional

two or more			one or more
physical			logical
LAN and MAN			LAN
physical			media access
physical			transit
top			right
less than or equal to			more
transport			physical
three			two
2^{m-1}			2m-1
2			1
n=2m+1			n=2m-1
2			2

Flow control			Error control
A and C			block coding
transport			datalink
ARQ			Go_Back N

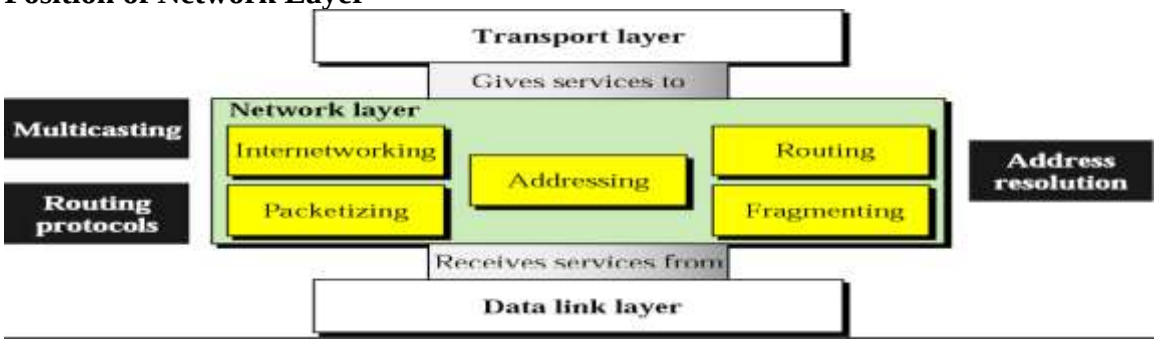
Unit-IV

Network Layer

Network layer functions

- Deliver packets from sending to receiving hosts
- network layer protocols in *every* host, router three important functions:
- *path determination:* route taken by packets from source to dest. *Routing algorithms*
- *forwarding:* move packets from router's input to appropriate router output
- *call setup:* some network architectures require router call setup along path before data flows

Position of Network Layer



Duties of Network Layer

- **Internetworking**

— Logically connecting heterogeneous networks to look like single network to uppertransport and application layers.

• **Addressing**

— Each device (a computer or a router) over the Internet must have unique anduniversally accepted address.

• **Routing**

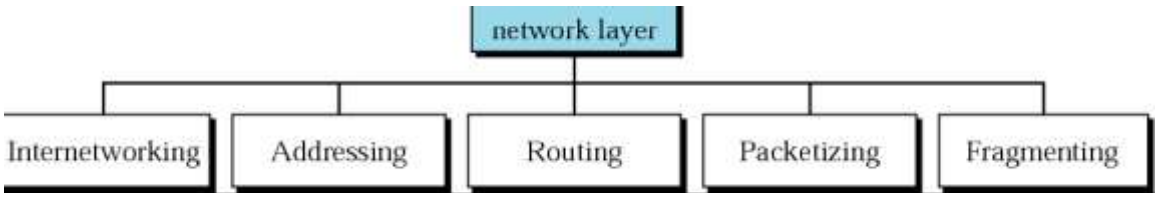
— Packet can not choose its route to the destination. The routers connecting LANsand WANs make this decision.

• **Packetizing**

— The network layer encapsulates datagram/segments received from upper layersand makes packets out of them.

• **Fragmenting**

— Each router de-capsulates the IP datagram from the received frame, process it and encapsulates it into another frame.



IPv4 ADDRESSES

An IPv4 address is a 32-bit address that uniquely and universally defines e connection of a device (for example, a computer or a router) to the Internet.

Address Space

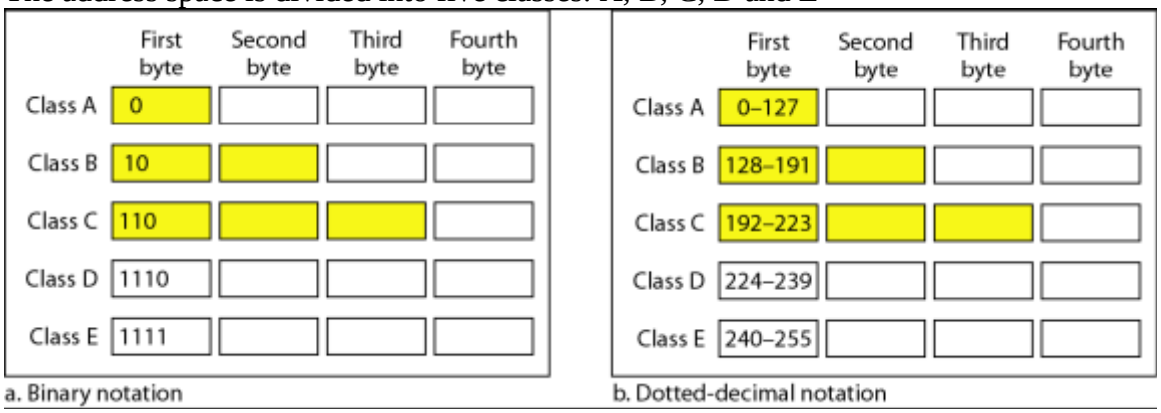
- **An IPv4 address is 32 bits long.**
- **The address space of IPv4 is 232 or 4,294,967,296.**

Note

- The IPv4 addresses are unique and universal**.**
- Dotted-decimal notation and binary notation for an IPv4 address
  - Binary Notation
  - Dotted-Decimal Notation
- Identifier used in network layer to identify each device connected to the Internet
- 32-bit binary address that uniquely and universally defines the connection of a host or a router to the Internet.
- In Internet, no two devices can have the same IP
- Dotted-decimal notation: Each byte is separated by dots.

Classful addressing

The address space is divided into five classes: A, B, C, D and E



Number of blocks and block size in classful IPv4 addressing

Class	*Number of Blocks*	*Block Size*	*Application*
A	128	16,777,216	Unicast
B	16,384	65,536	Unicast
C	2,097,152	256	Unicast
D	1	268,435,456	Multicast
E	1	268,435,456	Reserved

Note

In classful addressing, a large part of the available addresses were wasted.

Default masks for classful addressing

Class	*Binary*	*Dotted-Decimal*	*CIDR*
A	11111111 00000000 00000000 00000000	255.0.0.0	/8
B	11111111 11111111 00000000 00000000	255.255.0.0	/16
C	11111111 11111111 11111111 00000000	255.255.255.0	/24

Note

Classful addressing, which is almost obsolete, is replaced with classless addressing.

- **In IPv4 addressing, a block of addresses can be defined as x.y.z.t /*n* in which x.y.z.t defines one of the addresses and the /*n* defines the mask.**
- **The first address in the block can be found by setting the rightmost 32 − *n* bits to 0s.**
- **The last address in the block can be found by setting the rightmost 32 − n bits to 1s.**
- **The number of addresses in the block can be found by using the formula 232−n.**

Network address

Network address is an address that defines the network itself; it cannot be assigned to a host.

— All hostid bytes are 0s

— Defines the network to the rest of the Internet.

— First address in the block

- Given the network address, we can find the class of the address.

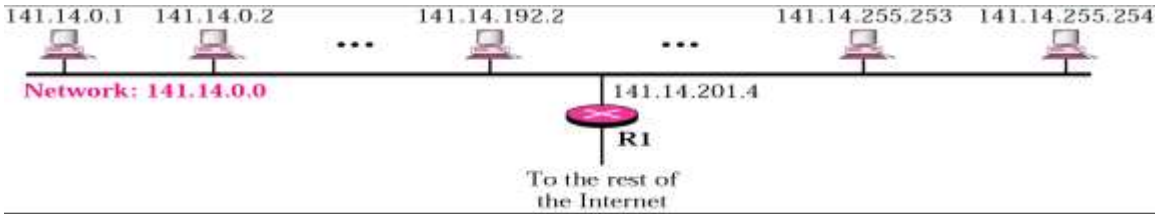
The first address in a block is normally not assigned to any device; it is used as the network address that represents the organization to the rest of the world.

Levels of hierarchy

— To reach a host on the Internet, we must first reach the network by using the first portion of the address (netid)

— Then we must reach the host itself by using the second portion (hostid)

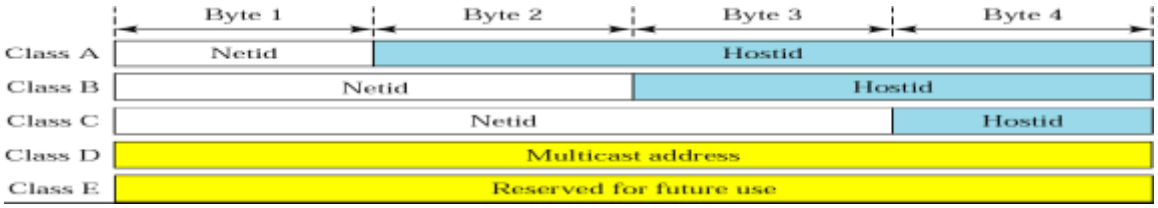
— IP addresses are designed with two levels of hierarchy.



Each address in the block can be considered as a two-level hierarchical structure: the leftmost *n* bits (prefix) define the network;the rightmost 32 − n bits define the host.

Netid, Hostid

- Netid: Network address.
- Hostid: Node address



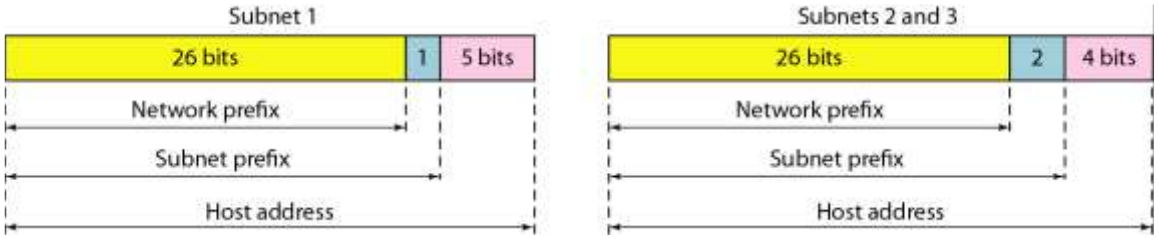
Three-level hierarchy in an IPv4 address

• Adding subnetworks creates an intermediate level of hierarchy in the IP addressing system. Now we have three levels: site, subnet, and host.

• The site is the first level.

• The second level is the subnet.

• The host is the third level.

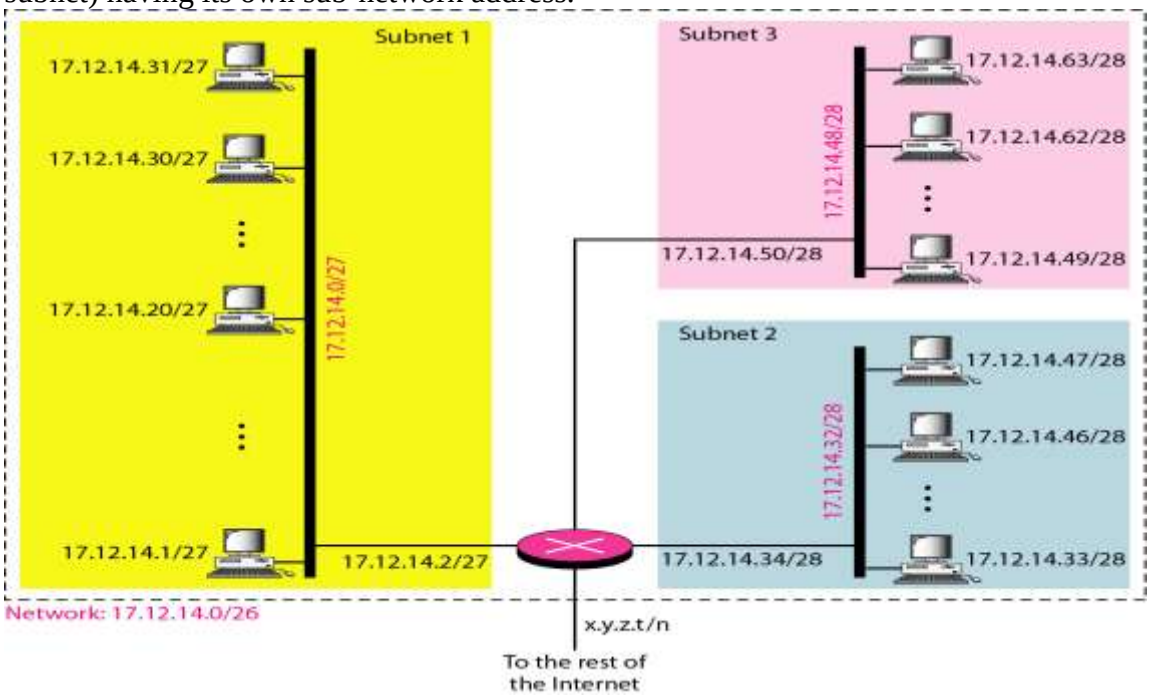


Subnetting

• Sub-netting

—We can divide a network into sub-networks while making the world knows only the main network.

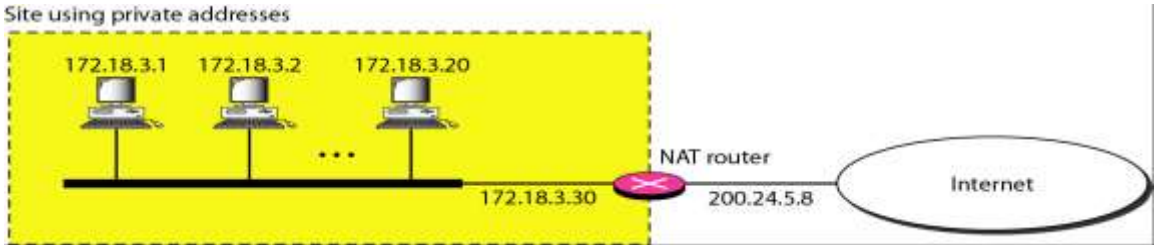
—In sub-netting, a network is divided into several smaller groups with each sub-network (or subnet) having its own sub-network address.



A Network Address Translation (NAT) implementation

• NAT enables a user to have a large set of addresses internally and one address, or a small set of addresses, externally.

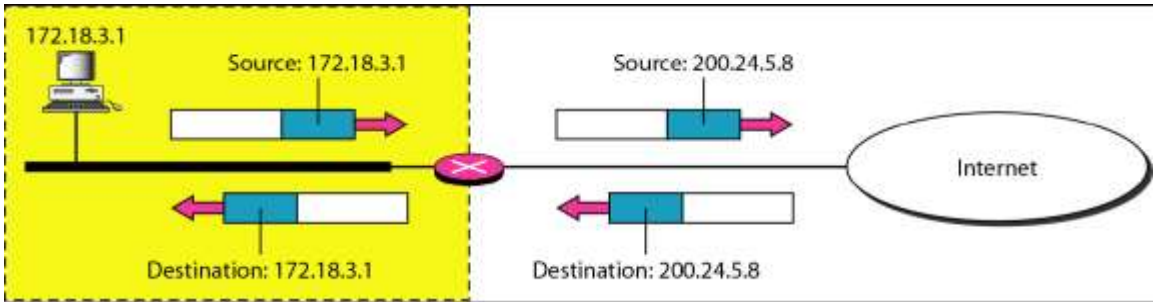
• The traffic inside can use the large set; the traffic outside, the small set.



Address Translation

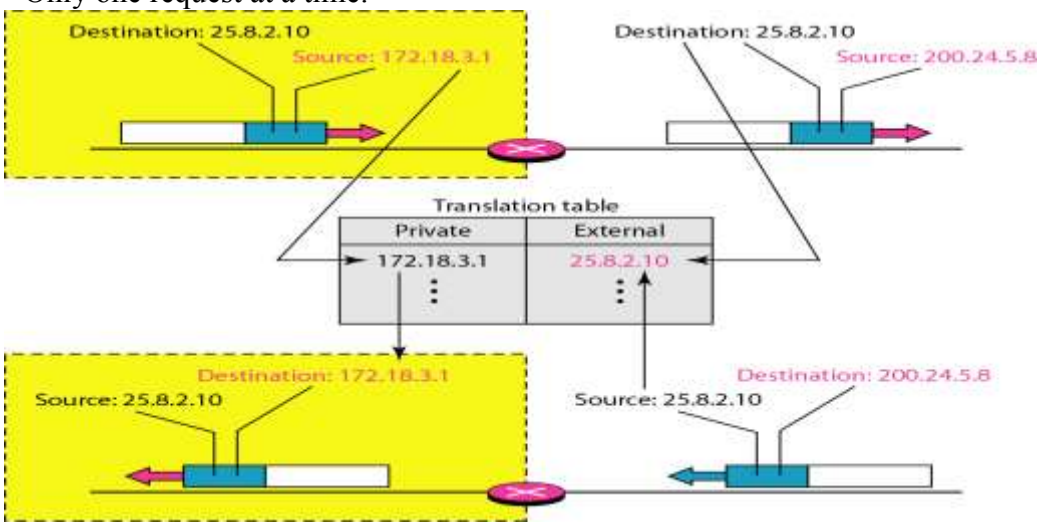
• All the outgoing packets go through the NAT router, which replaces the source address in the packet with the global NAT address.

• All incoming packets also pass through the NAT router, which replaces the destination address in the packet (the NAT router global address) with the appropriate private address.



NAT address translation

• Using one IP address: private address to external address mapping.
• Limitation is that only the private network can initiate a connection and not vice-versa.
• Only one request at a time.

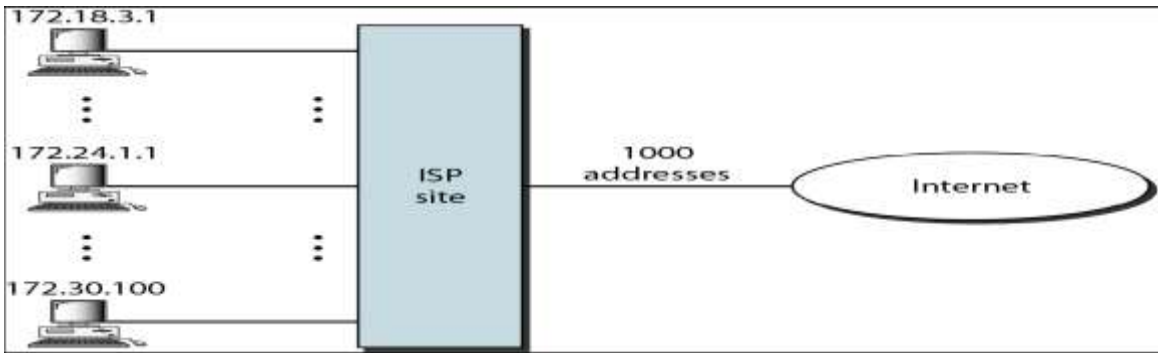


Five-column translation table

• Using a pool of IP addresses
— More than one global address is there and we map to one of them.
— Limited by the number of global IP.
• Using both IP and port numbers
— Mapping with IPs and Port numbers.

Private Address	*Private Port*	*External Address*	*External Port*	*Transport Protocol*
172.18.3.1	1400	25.8.3.2	80	TCP
172.18.3.2	1401	25.8.3.2	80	TCP
. . .	. . .	. . .	. . .	. . .

An ISP and NAT



Routing

Goal: determine a "good" path (sequence of routers) thru network from source to destination.
Graph abstraction for routing algorithms:

- graph nodes are routers m
- graph edges are physical links m link cost: delay, $ cost, or congestion level
- "good" path :typically means minimum cost path other def's possible

Routing Algorithm classification
Global or decentralized information
Global:

- all routers have complete topology, link cost information
- "link state" algorithms

Decentralized:

- router knows physically-connected neighbors, link costs to neighbors
- iterative process of computation, exchange of info with neighbors Static or dynamic?

Static:

- routes change slowly over time

Dynamic:

- routes change more quickly
  - periodic update
  - in response to link cost changes

ROUTING PROTOCOLS
• A routing protocol is a combination of rules and procedures that lets routers in the internet inform one another of changes. It allows routers to share whatever they know about the internet or their neighborhood.

Network Layer: Routing Protocols
There are two types of routing protocols they are:
1 Unicast routing
2 Multicast routing

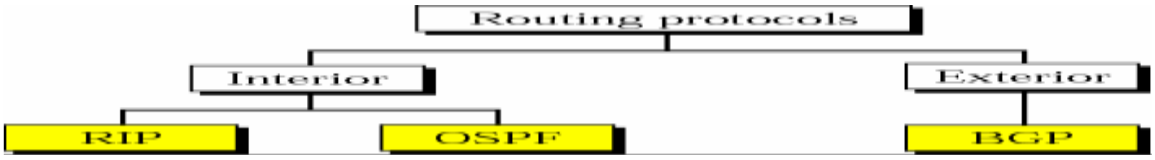
UNICAST ROUTING
• In unicast routing, there is only one source and only one destination.
• When a router receives a packet, it forwards the packet through only one of its ports (the one belonging to the optimum path) as defined in routing table. It discards the packet, if there is no route.

Metric of different protocols
• Metric is the cost assigned for passing through a network.
— The total metric of a particular router is equal to the sum of the metrics of networks that comprise the route.
— A router chooses the route with smallest metric.
• RIP (Routing Information Protocol): Cost of passing each network is same; it is one hop count.
— If a packet passes through 10 networks to reach the destination, the total cost is 10 hop counts.
• OSPF (Open Shortest Path First): Administrator can assign cost for passing a network based on type of service required.
— OSPF allows each router to have more than one routing table based on required type of service.
— Maximum throughput, minimum delay

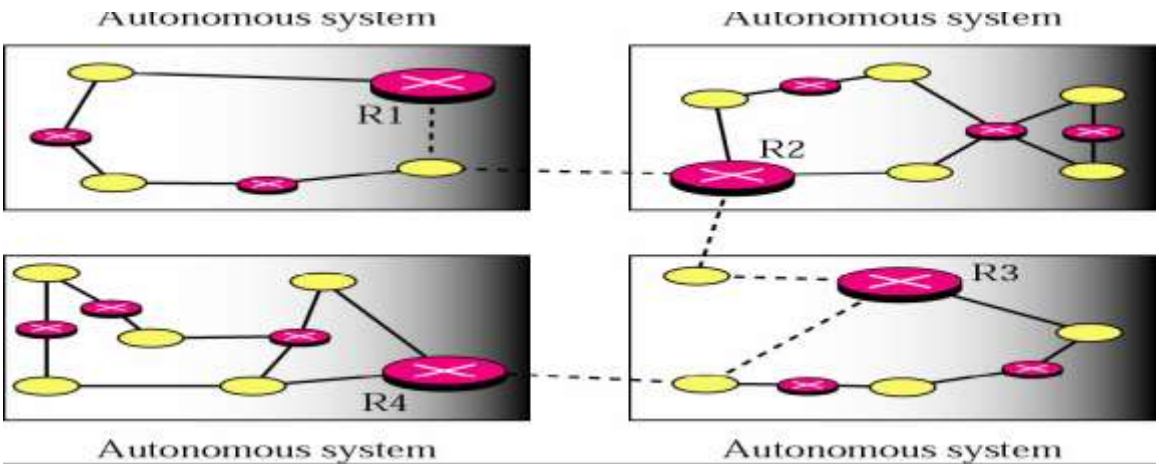
• BGP (Border Gateway Protocol): Criterion is the policy, which is set by the administrator.

Interior and Exterior routing

• Autonomous System: Group of networks and routers under the authority of a single administration.
• Routers inside an autonomous system is referred to as interior routing.
• Routing between autonomous systems is referred to as exterior routing.



Autonomous systems



• Solid lines show the communication between routers that use interior routing protocols.
• Broken lines show the communication between routers that use an exterior routing protocols.

Routing Information Protocol (RIP)

• RIP is based on Distance vector routing.
• Distance vector routing
— Sharing knowledge about the entire autonomous system: Each router periodically shares its knowledge about the entire autonomous system with its neighbours.
— Sharing only with neighbours through all its interfaces.
— Sharing at regular intervals: 30 seconds.
• Routing table
— Has one entry for each destination network of which the router is aware.
— Each entry has destination network address, the shortest distance to reach the destination in hop count, and next router to which the packet should be delivered to reach its final destination.
— Hop count is the number of networks that a packet encounters to reach its final destination.

A distance vector routing table

Destination	Hop Count	Next Router	Other information
163.5.0.0	7	172.6.23.4	
197.5.13.0	5	176.3.6.17	
189.45.0.0	4	200.5.1.6	
115.0.0.0	6	131.4.7.19	

RIP Updating Algorithm

Receive: a response RIP message
1. Add one hop to the hop count for each advertised destination.
2. Repeat the following steps for each advertised destination:
1. If (destination not in the routing table)
1. Add the advertised information to the table.
2. Else
1. If (next-hop field is the same)
1. Replace entry in the table with the advertised one.
2. Else
1. If (advertised hop count smaller than one in the table)
1. Replace entry in the routing table.
3. Return.

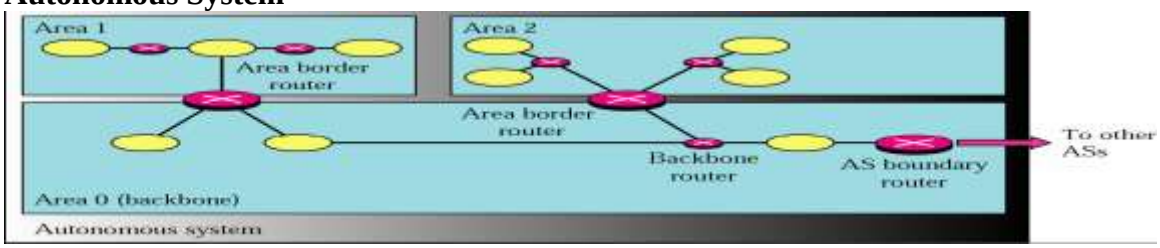
Initial routing tables in a small autonomous system

• When a router is added to a network, it initializes a routing table for itself, using its configuration file.
• The table consists only the directly attached networks and the hop counts, which are initialized to 1.
• The next-hop field, which identifies the next router, is empty.
• Each routing table is updated upon receipt of RIP messages using the RIP updating algorithm.

OSPF

• Open Shortest Path First
• Special routers called autonomous system boundary routers are responsible for dissipating information about other autonomous systems into the current system.
• OSPF divides an autonomous system into areas.

Autonomous System



Areas in an Autonomous System

• Area is a collection of networks, hosts, and routers all contained within an autonomous system.
• Routers inside an area flood the area with routing information.
• Area border routers: Summarize the information about the area and send it to other routers.
• Backbone area [Primary area]: All the areas inside an autonomous system must be connected to the backbone. Routers in this area are called as backbone routers. This area identification number is 0.

• If, due to some problem, the connectivity between a backbone and an area is broken, a virtual link between routers must be created by the administration to allow continuity of the functions of the backbone as the primary area.

OSPF

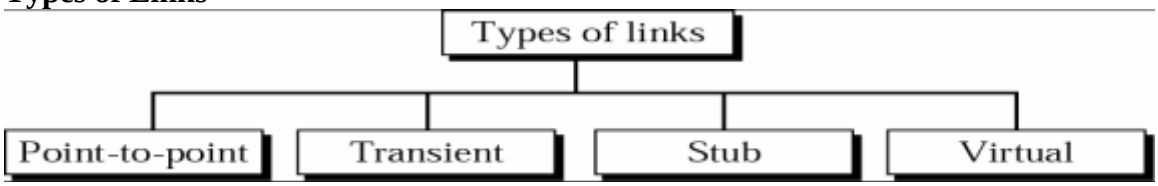
• Metric

— Administrator can assign the cost to each route.
— Based on type of service (minimum delay, maximum throughput, and so on)

• Link state routing

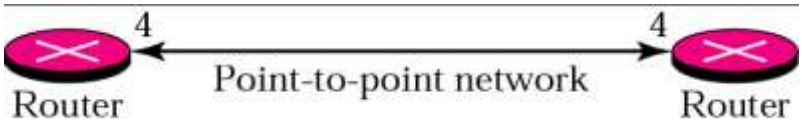
— Sharing knowledge about the neighbourhood: Each router sends the state of its neighbourhood to every other router in the area.
— Sharing with every other router: By flooding, a process whereby a router sends its information to all its neighbours (through all its output ports).
Each neighbour sends the packet to all its neighbours, and so on. Every router that receives the packet sends copies to each of its neighbours.
Eventually, every router (without exception) has received a copy of the same information.
— Sharing when there is a change; Only to its neighbours.
— Each router should have the exact topology of the internet at every moment.
— From this topology, a router can calculate the shortest path between itself and each network.

Types of Links



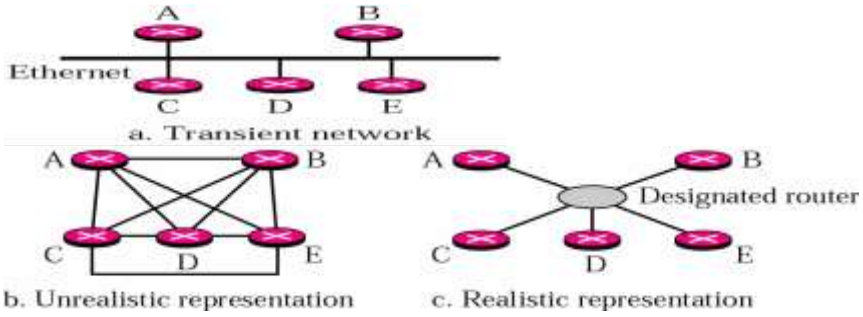
Point-to-Point Link

• Connects two routers without any other router or host in between.
• Directly connected routers using serial line.
• Only one neighbour.



Transient link

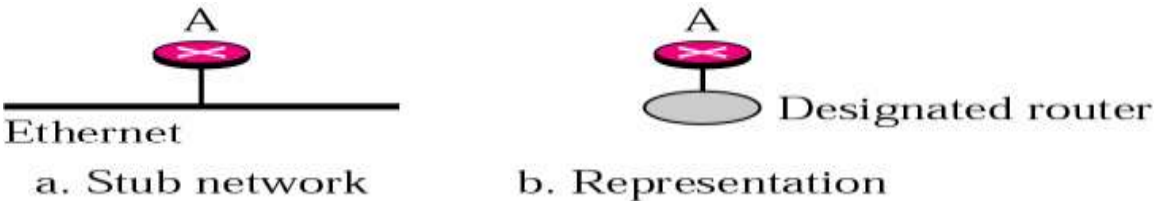
— A network with several routers attached to it.
— Each router has many neighbours.
• Lot of advertisements about their neighbours.
• One of the routers in the network has two duties: true router and designated router because we can not connect each router to every other router through one single network. Each router has only one neighbour, the designated router (network). On the other hand, the designated router (network) has five neighbours.
• Designated router represents a network. There exists a metric between each node to the designated router but there is no metric from the designated router to any other node.



Stub Link

• A network that is connected to only one router.

• The data packets enter the network through this singlerouter and leave the network through this same router.



Dijkstra Algorithm

• Every router in the same area has the same link state database.

• Dijkstra algorithm — calculates the shortest path between two points on a network, using a graph made up of nodes and edges.

— Algorithm divides the nodes into two sets: tentative and permanent. It chooses nodes, makes them tentative, examines them, and if they pass the criteria, makes them permanent.

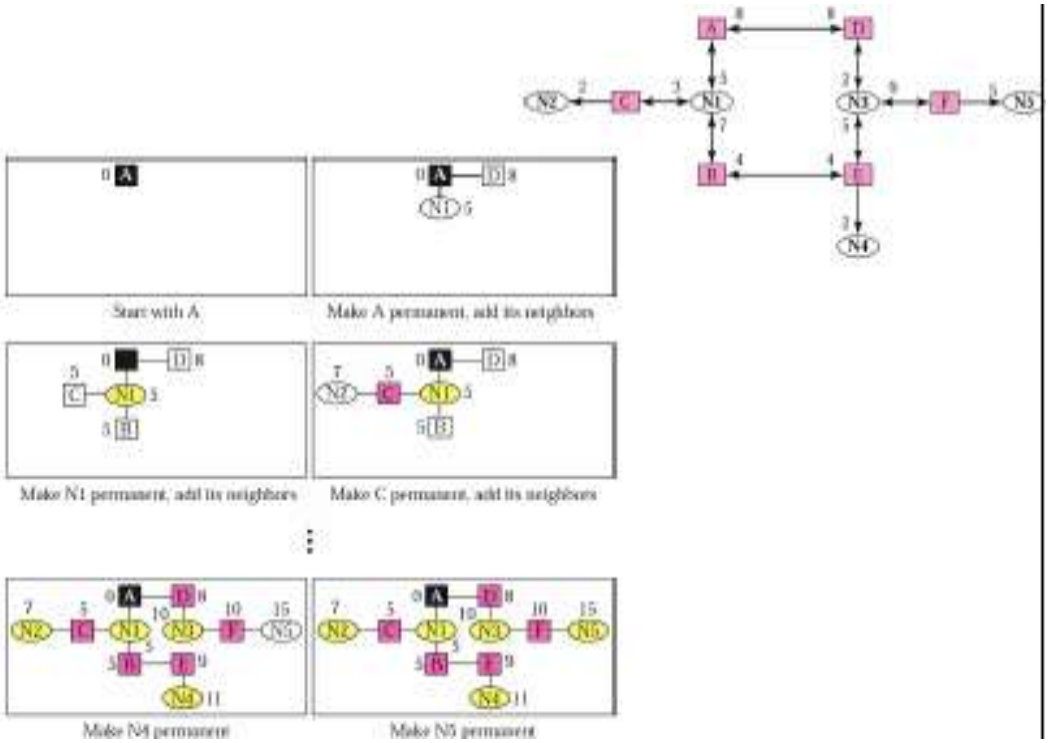
Algorithm

1. Start with the local node (router): the root of the tree.
2. Assign a cost of 0 to this node and make it the first permanent node.
3. Examine each neighbor node of the node that was the last permanent node.
4. Assign a cumulative cost to each node and make it tentative.
5. Among the list of tentative nodes
    1. Find the node with the smallest cumulative cost and make it permanent.
    2. If a node can be reached from more than one direction
        1. Select the direction with the shortest cumulative cost.
6. Repeat steps 3 to 5 until every node becomes permanent.

Shortest-path calculation

• The number next to each node represents the cumulative cost from the root node.

• Note that if a network can be reached through two directions with two cumulative costs, the direction with the smaller cumulative cost is kept, and the other one is deleted.



Link state routing table for router A

Network	Cost	Next Router	Other Information
N1	5	C	
N2	7	D	
N3	10	B	
N4	11	D	
N5	15	C	

BGP

• Border Gateway Protocol
• Inter-autonomous system routing protocol.
• BGP is based on a routing method called path vector routing.
• Path Vector routing

— Each entry in the routing table contains the destination network, the next router, and the path to reach the destination.

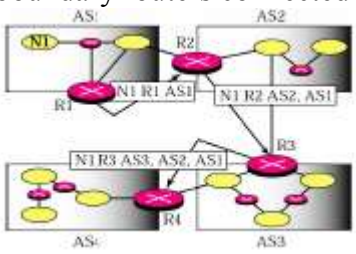
— The path is usually defined as an ordered list of autonomous systems that a packet should travel through to reach the destination.

Path vector routing table

Network	Next Router	Path
N01	R01	AS14, AS23, AS67
N02	R05	AS22, AS67, AS05, AS89
N03	R06	AS67, AS89, AS09, AS34
N04	R12	AS62, AS02, AS09

Path Vector Messages

• Autonomous boundary routers that participate in path vector routing advertise the reach ability of the networks in their own autonomous systems to neighbor autonomous boundary routers.
• Concept of neighborhood here is the same as the one described in the RIP or OSPF protocol.
• Two autonomous boundary routers connected to the same network are neighbours.



AS14, AS23, AS6

Path Vector Messages

• Each router that receives a path vector message verifies that the advertised path is in agreement with its policy (a set of rules imposed by the administrator controlling the routes). If it is, the router updates its routing table and modifies the message before sending it to the next neighbour.
• The modification consists of adding its AS number to the path and replacing the next router entry with its own identification.
• Loop prevention: Path vector avoids this problem by checking the path to see if its own AS is in the list.
• Policy Routing: Check the AS in the path list against a policy. If it is against the policy, the router can ignore that path and that destination. It does not update its routing table with this path, and it does not send this message to its neighbors. So, routing table entry is not based on metric but on policy.

Path Attributes

• Path is a list of attributes
• Each attribute gives some information about the path
• List of attributes help the receiving router make a better decision when applying its policy.
• Two categories: well-known and optional
— Well-known: Every BGP router should recognize
• Mandatory
– ORIGIN: source of routing information [RIP, OSPF, …]
– AS_PATH
– NEXT_HOP
• Discretionary: Not required to be included in every update message.
— Optional: Need not be recognized by every router
• Transitive: One that must be passed to the next router by the router that has not implemented this attribute
• Non-transitive: One that should be discarded if the receiving router has not implemented it.

Types of BGP Messages

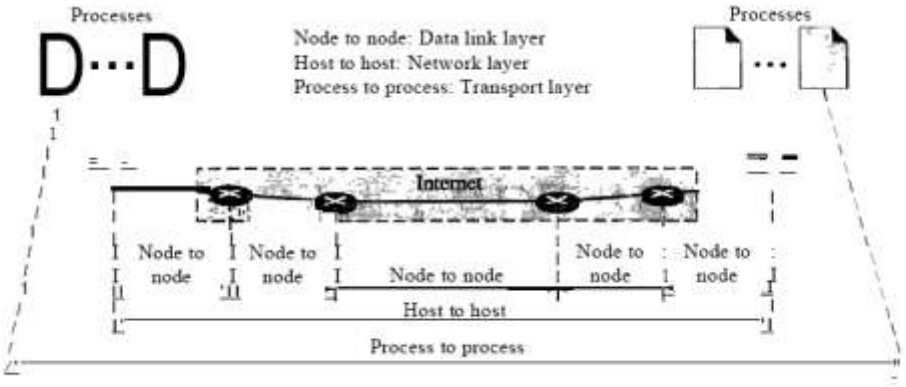
• Open: To create a neighborhood relationship
• If the neighbor accepts the neighborhood relationship, it responds with a keep-alive message, which means that a relationship has been established between two routers
• Update message is used by router to withdraw destinations that have been advertised previously, announce a router to a new destination, or do both.
• Keep-alive: Routers exchange this message regularly (before their hold time expires) to tell each other that they are alive.
• Notification: Sent by a router whenever an error condition is detected or a router wants to close the connection.

Transport Layer

The transport layer is responsible for the delivery of a message from one process to another.
A transport layer protocol 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 is transferred, the connection is terminated. In the transport layer, a message is normally divided into transmittable segments. A connectionless protocol, such as UDP, treats each segment separately. A connection oriented protocol, such as TCP and SCTP, creates a relationship between the segments using sequence numbers

PROCESS-TO-PROCESS DELIVERY

The data link layer is responsible for delivery of frames between two neighboring nodes over a link. This is called *node-to-node delivery.* The network layer is responsible for delivery of datagram between two hosts. This is called *host-to-host delivery.* Communication on the Internet is not defined as the exchange of data between two nodes or between two hosts. Real communication takes place between two processes (application programs). We need process-to-process delivery. However, at any moment, several processes may be running on the source host and several on the destination host. To complete the delivery, we need a mechanism to deliver data from one of these processes running on the source host to the corresponding process running on the destination host. The transport layer is responsible for process-to-process delivery-the delivery of a packet, part of a message, from one process to another. Two processes communication a client/server relationship.



Client/Server Paradigm

A process on the local host, called a client, needs services from a process usually on the remote host, called a server. Both processes (client and server) have the same name. For example, to get the day and time from a remote machine, we need a Daytime client process running on the local host and a Daytime server process running on a remote machine. Operating systems today support both multiuser and multiprogramming environments.

A remote computer can run several server programs at the same time, just as local computers can run one or more client programs at the same time. For communication, we must define the following:

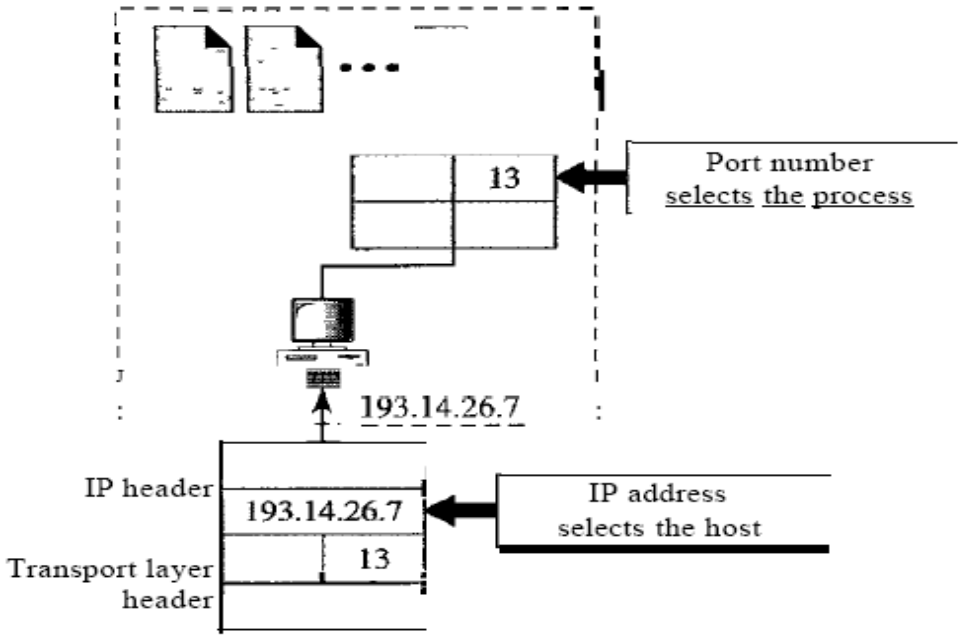
1. Local host
2. Local process
3. Remote host
4. Remote process

Addressing

Whenever we need to deliver something to one specific destination among many, we need an address. At the data link layer, we need a MAC address to choose one node among several nodes if the connection is not point-to-point. A frame in the data link layer needs a destination MAC address for delivery and a source address for the next node's reply.

At the network layer, we need an IP address to choose one host among millions. A datagram in the network layer needs a destination IP address for delivery and a source IP address for the destination's reply. At the transport layer, we need a transport layer address, called a port number, to choose among multiple processes running on the destination host. The destination port number is needed for delivery; the source port number is needed for the reply.

In the Internet model, the port numbers are 16-bit integers between 0 and 65,535. The client program defines itself with a port number, chosen randomly by the transport layer software running on the client host. This is the ephemeral port number.

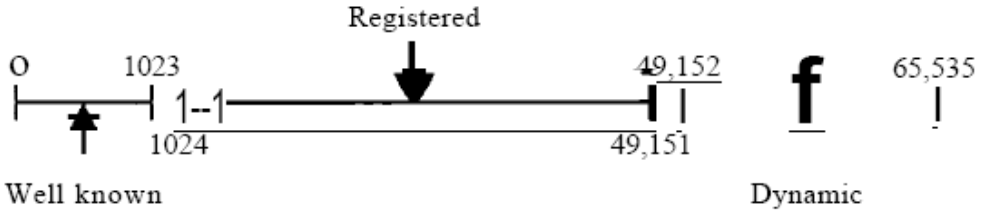


The server process must also define itself with a port number. This port number, however, cannot be chosen randomly. If the computer at the server site runs a server process and assigns a random number as the port number, the process at the client site that wants to access that server and use its services will not know the port number. Of course, one solution would be to send a special packet and request the port number of a specific server, but this requires more overhead. The Internet has decided to use universal
port numbers for servers; these are called well-known port numbers. There are some exceptions to this rule; for example, there are clients that are assigned well-known port numbers. Every client process knows the well-known port number of the corresponding server process.

lANA Ranges

The lANA (Internet Assigned Number Authority) has divided the port numbers into three ranges: well known, registered, and dynamic (or private), as shown in Figure .

o Well-known ports. The ports ranging from 0 to 1023 are assigned and controlled by lANA. These are the well-known ports.

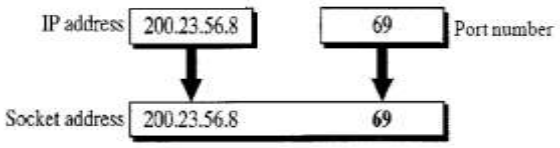


o Registered ports. The ports ranging from 1024 to 49,151 are not assigned or controlled by lANA. They can only be registered with lANA to prevent duplication.

o Dynamic ports. The ports ranging from 49,152 to 65,535 are neither controlled nor registered. They can be used by any process. These are the ephemeral ports.

Socket Addresses

Process-to-process delivery needs two identifiers, IP address and the port number, at each end to make a connection. The combination of an IP address and a port number is called a socket address. The client socket address defines the client process uniquely just as the server socket address defines the server process uniquely.

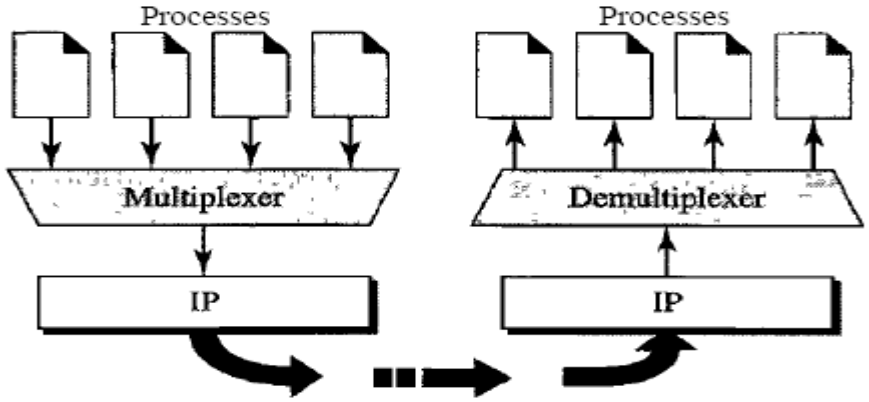


A transport layer protocol needs a pair of socket addresses: the client socket address and the server socket address. These four pieces of information are part of the IP header and the transport layer protocol header. The IP header contains the IP addresses; the UDP or TCP header contains the port numbers.

Multiplexing and Demultiplexing

Multiplexing

At the sender site, there may be several processes that need to send packets. However, there is only one transport layer protocol at any time. This is a many-to-one relationship and requires multiplexing. The protocol accepts messages from different processes, differentiated by their assigned port numbers. After adding the header, the transport layer
passes the packet to the network layer.



Demultiplexing

At the receiver site, the relationship is one-to-many and requires demultiplexing. The transport layer receives datagrams from the network layer. After error checking and dropping of the header, the transport layer delivers each message to the appropriate process based on the port number.

Connectionless Versus Connection-Oriented Service

A transport layer protocol can either be connectionless or connection-oriented.

Connectionless Service

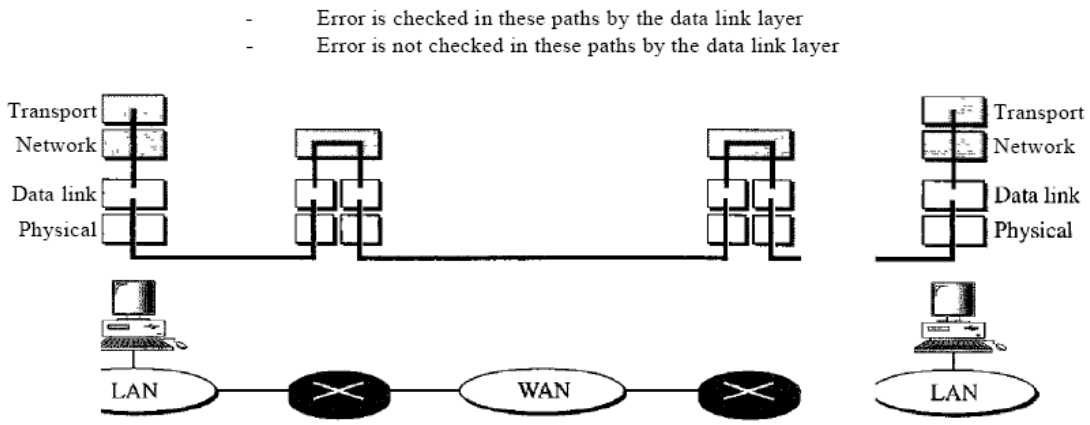
In a connectionless service, the packets are sent from one party to another with no need for connection establishment or connection release. The packets are not numbered; they may be delayed or lost or may arrive out of sequence. There is no acknowledgment either. We will see shortly that one of the transport layer protocols in the Internet model, UDP, is connectionless.

Connection Oriented *Service*

In a connection-oriented service, a connection is first established between the sender and the receiver. Data are transferred. At the end, the connection is released. We will see shortly that TCP and SCTP are connection-oriented protocols.

Reliable Versus Unreliable

The transport layer service can be reliable or unreliable. If the application layer program needs reliability, we use a reliable transport layer protocol by implementing flow and error control at the transport layer. This means a slower and more complex service. On the other hand, if the application program does not need reliability because it uses its own flow and error control mechanism or it needs fast service or the nature of the service does not demand flow and error control (real-time applications), then an unreliable protocol can be used.



In the Internet, there are three common different transport layer protocols, as we have already mentioned. UDP is connectionless and unreliable; TCP and SCTP are connection oriented and reliable. These three can respond to the demands of the application layer programs.

USER DATAGRAM PROTOCOL (UDP)

The User Datagram Protocol (UDP) is called a connectionless, unreliable ransport protocol. It does not add anything to the services of IP except to provide process-toprocess communication instead of host-to-host communication. Also, it performs very limited error checking.

Well-Known Ports for UDP

Table 23.1 shows some well-known port numbers used by UDP. Some port numbers can be used by both UDP and TCP.

Port	*Protocol*	*Description*
7	Echo	Echoes a received datagram back to the sender
9	Discard	Discards any datagram that is received
11	Users	Active users

Port	*Protocol*	*Description*
13	Daytime	Returns the date and the time
17	Quote	Returns a quote of the day
19	Chargen	Returns a string of characters
53	Nameserver	Domain Name Service
67	BOOTPs	Server port to download bootstrap information
68	BOOTPc	Client port to download bootstrap information
69	TFTP	Trivial File Transfer Protocol
III	RPC	Remote Procedure Call
123	NTP	Network Time Protocol
161	SNMP	Simple Network Management Protocol
162	SNMP	Simple Network Management Protocol (trap)

User Datagram

UDP packets, called user datagrams, have a fixed-size header of 8 bytes. Figure below shows the format of a user datagram.

The fields are as follows:

o Source port number. This is the port number used by the process running on the source host. It is 16 bits long, which means that the port number can range from 0 to 65,535. If the source host is the client (a client sending a request), the port number, in most cases, is an ephemeral port number requested by the process and chosen by the UDP software running on the source host. If the source host is the server (a server sending a response), the port number, in most cases, is a well-known port number.

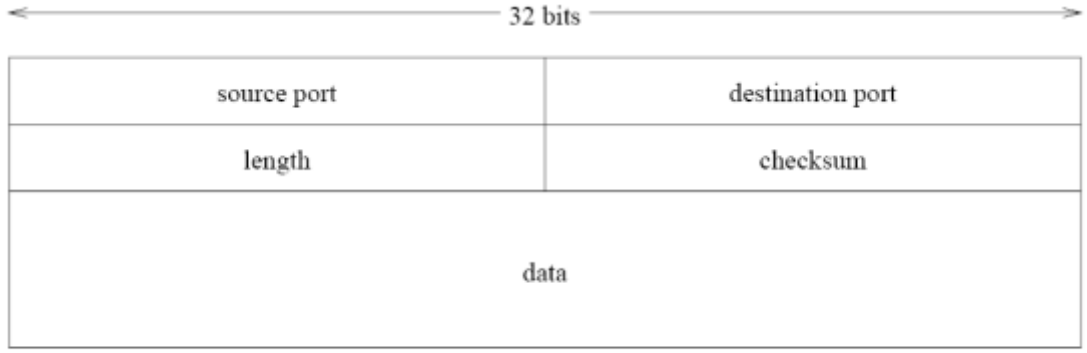


Figure 15.2. UDP header format

o Destination port number. This is the port number used by the process running on the destination host. It is also 16 bits long. If the destination host is the server (a client sending a request), the port number, in most cases, is a well-known port number. If the destination host is the client (a server sending a response), the port number, in most cases, is an ephemeral port number. In this case, the server copies the ephemeral port number it has received in the request packet.

o Length. This is a 16-bit field that defines the total length of the user datagram, header plus data. The 16 bits can define a total length of 0 to 65,535 bytes. However, the total length needs to be much less because a UDP user datagram is stored in an IP datagram with a total length of 65,535 bytes. The length field in a UDP user datagram is actually not necessary. A user datagram is encapsulated in an IP datagram. There is a field in the IP datagram that defines the total length. There is another field in the IP datagram that defines the length of the header. So if we subtract the value of the second field from the first, we can deduce the length of a UDP datagram that is encapsulated in an IP datagram.

UDP length = IP length - IP header's length

However, the designers of the UDP protocol felt that it was more efficient for the destination UDP to calculate the length of the data from the information provided in the UDP user datagram rather than ask the IP software to supply this information.

We should remember that when the IP software delivers the UDP user datagram to the UDP layer, it has already dropped the IP header.

o Checksum. This field is used to detect errors over the entire user datagram (header plus data). The checksum is discussed next. Checksum .We have also shown how to calculate the checksum for the IP and ICMP packet. We now show how this is done for UDP.

UDP Operation

UDP uses concepts common to the transport layer.

Connectionless Services

As mentioned previously, UDP provides a connectionless service. This means that each user datagram sent by UDP is an independent datagram. There is no relationship between the different user datagrams even if they are coming from the same source process and going to the same destination program. The user datagrams are not numbered. Also, there is no connection establishment and no connection termination, as is the case for TCP. This means that each user datagram can travel on a different path. One of the ramifications of being connectionless is that the process that uses UDP cannot send a stream of data to UDP and expect UDP to chop them into different related user datagrams. Instead each request must be small enough to fit into one user datagram. Only those processes sending short messages should use UDP.

Flow and Error Control

UDP is a very simple, unreliable transport protocol. There is no flow control and hence no window mechanism. The receiver may overflow with incoming messages. There is no error control mechanism in UDP except for the checksum. This means that the sender does not know if a message has been lost or duplicated. When the receiver detects an error through the checksum, the user datagram is silently discarded. The lack of flow control and error control means that the process using UDP should provide these mechanisms.

Encapsulation and Decapsulation

To send a message from one process to another, the UDP protocol encapsulates and decapsulates messages in an IP datagram.

Use of UDP

The following lists some uses of the UDP protocol:

- UDP is suitable for a process that requires simple request-response communication with little concern for flow and error control. It is not usually used for a process such as FrP that needs to send bulk data.
- UDP is suitable for a process with internal flow and error control mechanisms. For example, the Trivial File Transfer Protocol (TFTP) process includes flow and error control. It can easily use UDP.
- UDP is a suitable transport protocol for multicasting. Multicasting capability is embedded in the UDP software but not in the TCP software.
- UDP is used for management processes such as SNMP
- UDP is used for some route updating protocols such as Routing Information Protocol

TCP

Transmission Control Protocol (TCP). TCP, like UDP, is a process-to-process (program-to-program) protocol. TCP, therefore, like UDP, uses port numbers. Unlike UDP, TCP is a connection oriented protocol; it creates a virtual connection between two TCPs to send data. In addition, TCP uses flow and error control mechanisms at the transport level.

In brief, TCP is called a *connection-oriented, reliable* transport protocol. It adds connection-oriented and reliability features to the services of IP.

TCP Services

Before we discuss TCP in detail, let us explain the services offered by TCP to the processes at the application layer.

Process-to-Process Communication

Like UDP, TCP provides process-to-process communication using port numbers. able below lists some well-known port numbers used by TCP.The Transmission Control Protocol (TCP) is one of the main transport layer protocols used with IP. It is a connection oriented protocol based on the connectionless IP protocol. Because it is the lowest layer which has end-to-

end communication, it needs to handle things such as lost packets. In this respect it is similar to the data-link layer which must handle errors on an individual link.

Port	*Protocol*	*Description*
7	Echo	Echoes a received datagram back to the sender
9	Discard	Discards any datagram that is received
11	Users	Active users
13	Daytime	Returns the date and the time
17	Quote	Returns a quote of the day
19	Chargen	Returns a string of characters
20	FIP, Data	File Transfer Protocol (data connection)
21	FIP, Control	File Transfer Protocol (control connection)
23	TELNET	Tenninal Network
25	SMTP	Simple Mail Transfer Protocol
53	DNS	Domain Name Server
67	BOOTP	Bootstrap Protocol
79	Finger	Finger
80	HTTP	Hypertext Transfer Protocol
111	RPC	Remote Procedure Call

Segment

Before we discuss TCP in greater detail, let us discuss the TCP packets themselves. A packet in TCP is called a segment.

The format of a TCP segment header is shown in figure below.

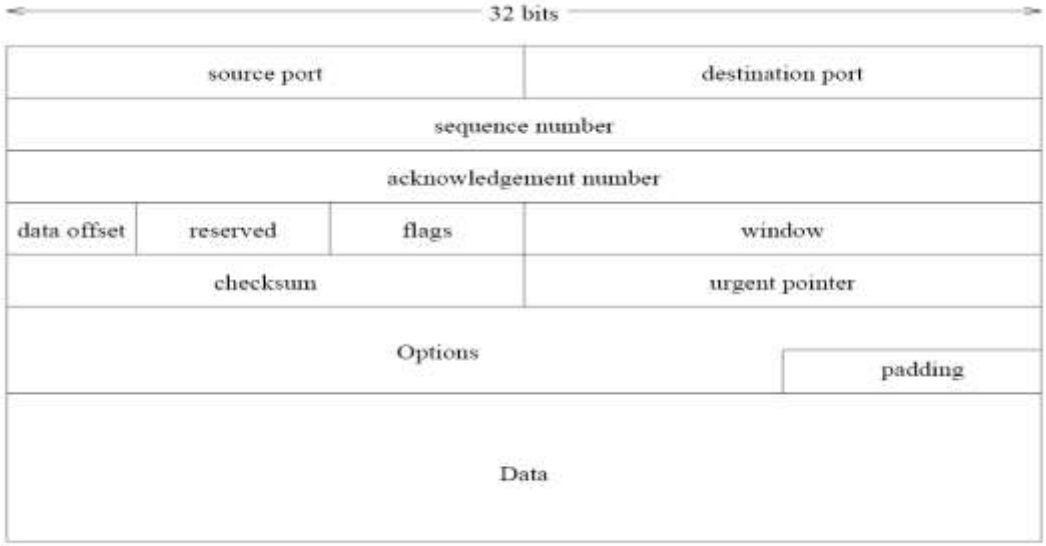


Figure 15.1. TCP header format

Source port

All of the address fields in the lower layer protocols are only concerned with getting the packet to the correct host. Often, however, we want to have multiple connections between two hosts. The source port is simply the number of the outgoing connection from the source host.

Destination port

Similarly, this is the number of the incoming connection on the destination host. There must be a program on the destination host which has somehow told the networking system on that host that it will accept packets destined for this port number.

Sequence number

This is the sequence number of this packet. It differs from the usual data-link layer sequence number in that it is in fact the sequence number of the first byte of information and is incremented

by the number of bytes in this packet for the next message. In other words, it counts the number of bytes transmitted rather than the number of packets.

Acknowledgement number .This is the sequence number of the last byte being acknowledged. This is a piggy-backed acknowledgement. This field is the offset in the packet of the beginning of the data field. (In other words it is the length of the header.)

Flags

This field contains several flags relating to the transfer of the packet. We will not consider them further here.

Window

This field is used in conjunction with the acknowledgement number field. TCPuses a sliding window protocol with a variable window size (often depending on the amount of buffer space available. This field contains the number of bytes which the host is willing to accept from the remote host.

Checksum

This field contains a checksum of the header. It actually uses a modified form of the header which includes some of the information from the IP header to detect some unusual types of errors.

Urgent pointer

There is provision in TCP for some urgent data messages to be sent bypassing the normal sequence number system. This field is used to indicate where such data is stored in the packet.

Options

As with IP, various options may be set. We will not consider them here.

Padding

Padding is added to make the header a multiple of 32 bits long. This is only necessary when options are used.

Data

The data field is passed intact to the program which is receiving packets addressed to this port.

A TCP Connection

TCP is connection-oriented. A connection-oriented transport protocol establishes a virtual path between the source and destination. All the segments belonging to a message are then sent over this virtual path. Using a single virtual pathway for the entire message facilitates the acknowledgment process as well as retransmission of damaged or lost frames. The point is that a TCP connection is virtual, not physical. TCP operates at a higher level. TCP uses the services of IP to deliver individual segments to the receiver, but it controls the connection itself. If a segment is lost or corrupted, it is retransmitted. Unlike TCP, IP is unaware of this retransmission. If a segment arrives out of order, TCP holds it until the missing segments arrive; IP is unaware of this reordering.

In TCP, connection-oriented transmission requires three phases: connection establishment, data transfer, and connection termination.

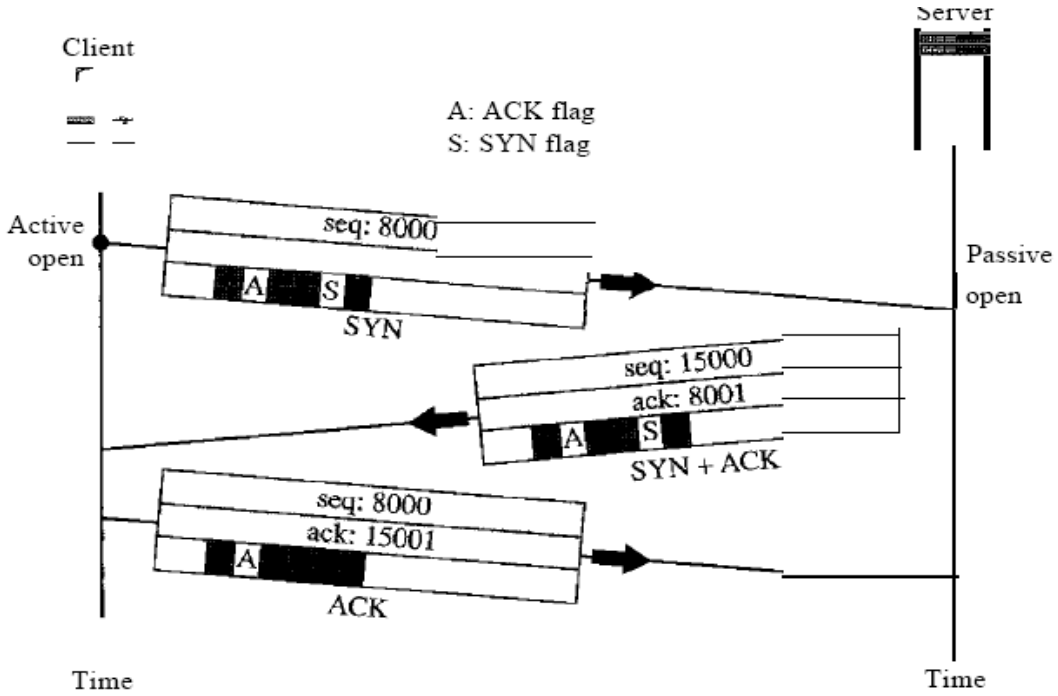
Connection Establishment

TCP transmits data in full-duplex mode. When two TCPs in two machines are connected, they are able to send segments to each other simultaneously. This implies that each party must initialize communication and get approval from the other party before any data are transferred.

Three-Way Handshaking The connection establishment in TCP is called threeway handshaking. In our example, an application program, called the client, wants to make a connection with another application program, called the server, using TCP as the transport layer protocol.

The process starts with the server. The server program tells its TCP that it is ready to accept a connection. This is called a request for a *passive open.* Although the server TCP is ready to accept any connection from any machine in the world, it cannot make the connection itself.

The client program issues a request for an *active open.* A client that wishes to connect to an open server tells its TCP that it needs to be connected to that particular server. TCP can now start the three-way handshaking process as shown in Figure below To show the process, we use two time lines: one at each site. Each segment has values for all its header fields and perhaps for some of its option fields, too. However, we show only the few fields necessary to understand each phase. We show the sequence number, the acknowledgment number, the control flags (only those that are set), and the window size, if not empty. The three steps in this phase are as follows.



1. The client sends the first segment, a SYN segment, in which only the SYN flag is set.
This segment is for synchronization of sequence numbers. It consumes one sequence number. When the data transfer starts, the sequence number is incremented by 1. We can say that the SYN segment carries no real data, but we can think of it as containing 1 imaginary byte.
A SYN segment cannot carry data, but it consumes one sequence number.
2. The server sends the second segment, a SYN +ACK segment, with 2 flag bits set:
SYN and ACK. This segment has a dual purpose. It is a SYN segment for communication in the other direction and serves as the acknowledgment for the SYN segment. It consumes one sequence number. A SYN +ACK segment cannot carry data, but does consume one sequence number.
3. The client sends the third segment. This is just an ACK segment. It acknowledges the receipt of the second segment with the ACK flag and acknowledgment number field. Note that the sequence number in this segment is the same as the one in the SYN segment; the ACK segment does not consume any sequence numbers.
An ACK segment, if carrying no data, consumes no sequence number.
.

Data Transfer

After connection is established, bidirectional data transfer can take place. The client and server can both send data and acknowledgments. We will study the rules of acknowledgment later in the chapter; for the moment, it is enough to know that data traveling in the same direction as an acknowledgment are carried on the same segment.

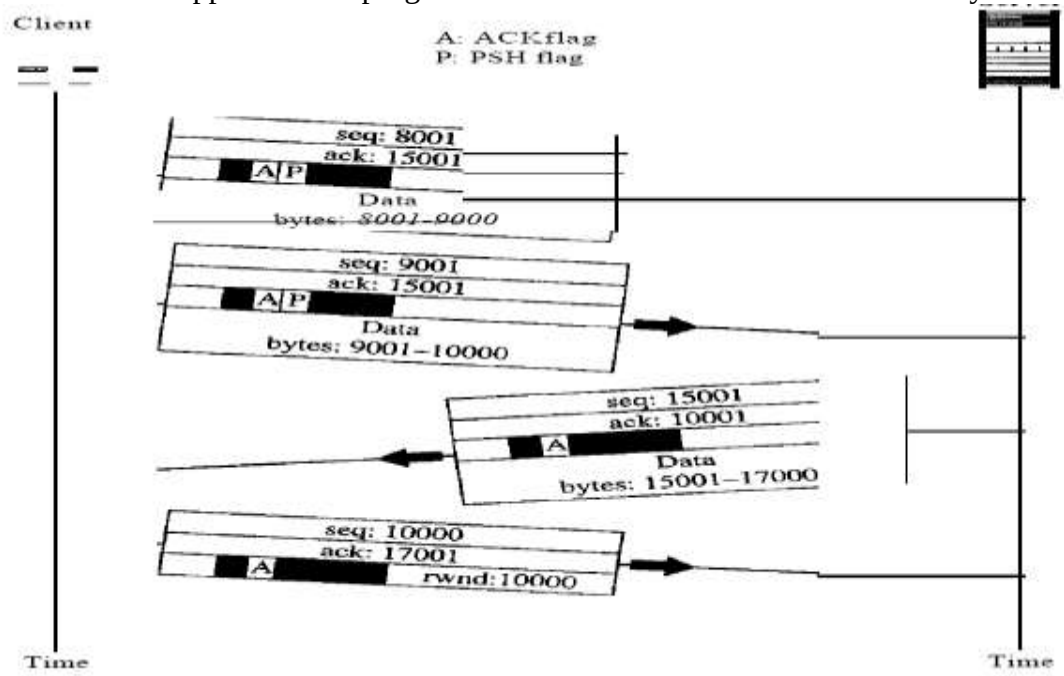
The acknowledgment is piggybacked with the data. Figure Shows an example. In this example, after connection is established (not shown in the figure), the client sends 2000 bytes of data in two segments. The server then sends 2000 bytes in one segment.

The client sends one more segment. The first three segments carry both data and acknowledgment, but the last segment carries only an acknowledgment because there are no more data to be sent. Note the values of the sequence and acknowledgment numbers. The data segments sent by the client have the PSH (push) flag set so that the server TCP knows to deliver data to the server process as soon as they are received.

We discuss the use of this flag in greater detail later. The segment from the server, on the other hand, does not set the push flag. Most TCP implementations have the option to set or not set this flag.

Pushing Data We saw that the sending TCP uses a buffer to store the stream of data coming from the sending application program. The sending TCP can select the segment size. The receiving TCP also buffers the data when they arrive and delivers them to the application program when the application program is ready or when it is convenient for the receiving TCP. This type of flexibility increases the efficiency of TCP.

However, on occasion the application program has no need for this flexibility_ For example, consider an application program that communicates interactively with another



application program on the other end. The application program on one site wants to send a keystroke to the application at the other site and receive an immediate response.

Delayed transmission and delayed delivery of data may not be acceptable by the application program.

TCP can handle such a situation. The application program at the sending site can request a *push* operation. This means that the sending TCP must not wait for the window to be filled. It must create a segment and send it immediately. The sending TCP must also set the push bit (PSH) to let the receiving TCP know that the segment includes data that must be delivered to the receiving application program as soon as possible and not to wait for more data to come. Although the push operation can be requested by the application program, most current implementations ignore such requests. TCP can choose whether or not to use this feature.

Urgent Data

TCP is a stream-oriented protocol. This means that the data are presented from the application program to TCP as a stream of bytes. Each byte of data has a position in the stream. However, on occasion an application program needs to send *urgent* bytes. This means that the sending application program wants a piece of data to be read out of order by the receiving application program.

Connection Termination

Any of the two parties involved in exchanging data (client or server) can close the connection, although it is usually initiated by the client. Most implementations today allow twooptions for connection termination: three-way handshaking and four-way handshaking with a half-close option. Three-Way Handshaking Most implementations today allow *three-way handshaking* for connection termination as shown in Figure below.

1. In a normal situation, the client TCP, after receiving a close command from the client process, sends the first segment, a FIN segment in which the FIN flag is set.

Note that a FIN segment can include the last chunk of data sent by the client, or it can be just a control segment as shown in Figure below. If it is only a control segment, it consumes only one sequence number.

The FIN segment consumes one sequence number ifit does not carry data

2. The server TCP, after receiving the FIN segment, informs its process of the situation and sends the second segment, a FIN +ACK segment, to confirm the receipt of the FIN segment from the client and at the same time to announce the closing of the connection in the other direction. This segment can also contain the last chunk of data from the server. If it does not carry data, it consumes only one sequence number.

The FIN +ACK segment consumes one sequence number if it does not carry data.

3. The client TCP sends the last segment, an ACK segment, to confirm the receipt of the FIN segment from the TCP server. This segment contains the acknowledgment number, which is 1 plus the sequence number received in the FIN segment from the server. This segment cannot carry data and consumes no sequence numbers. In TCP, one end can stop sending data while still receiving data. This is called a half-close.

Flow Control

TCP uses a sliding window, as discussed in Chapter 11, to handle flow control. The sliding window protocol used by TCP, however, is something between the *Go-Back-N* and Selective Repeat sliding window. The sliding window protocol in TCP looks likethe Go-Back-N protocol because it does not use NAKs; it looks like Selective Repeat because the receiver holds the out-of-order segments until the missing ones arrive. There are two big differences between this sliding window and the one we used at the data link layer. First, the sliding window ofTCP is byte-oriented; the one we discussed in the data link layer is frame-oriented. Second, the TCP's sliding window is of variable size; the one we discussed in the data link layer was of fixed size.

Figure below shows the sliding window in TCP. The window spans a portion of the buffer containing bytes received from the process. The bytes inside the window are the bytes that can be in transit; they can be sent without worrying about acknowledgment.

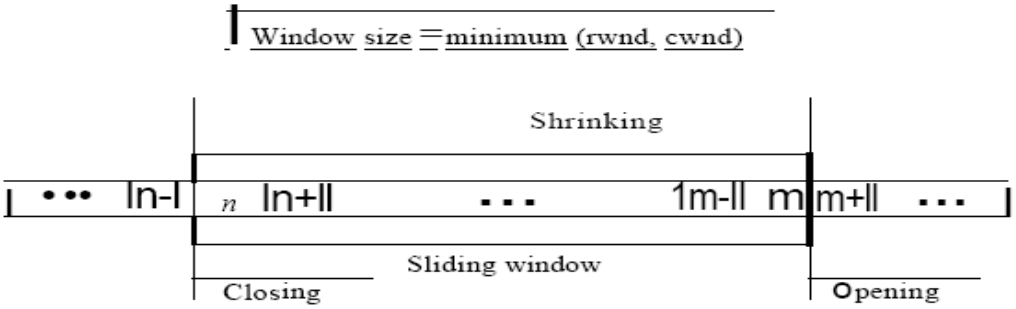
The imaginary window has two walls: one left and one right.

The window is *opened, closed,* or *shrunk.* These three activities, as we will see, are in the control of the receiver (and depend on congestion in the network), not the sender.

The sender must obey the commands of the receiver in this matter.

Opening a window means moving the right wall to the right. This allows more new bytes in the buffer that are eligible for sending. Closing the window means moving the left wall to the right. This means that some bytes have been acknowledged and the sender need not worry about them anymore. Sluinking the window means moving the right wall to the left. This is strongly discouraged and not allowed in some implementations because it means revoking the eligibility of some bytes for sending. This is a problem if the sender has already sent these bytes. Note that the

left wall cannot move to the left because this would revoke some of the previously sent acknowledgments. The size of the window at one end is determined by the lesser of two values: *receiver window (rwnd)* or *congestion window (cwnd).* The *receiver window* is the value advertised by the opposite end in a segment containing acknowledgment. It is the number of bytes the other end can accept before its buffer overflows and data are discarded. The congestion window is a value determined by the network to avoid congestion.



Error Control

TCP is a reliable transport layer protocol. This means that an application program that delivers a stream of data to TCP relies on TCP to deliver the entire stream to the application program on the other end in order, without error, and without any part lost or duplicated. TCP provides reliability using error control. Error control includes mechanisms for detecting corrupted segments, lost segments, out-of-order segments, and duplicated segments. Error control also includes a mechanism for correcting errors after they are detected. Error detection and correction in TCP is achieved through the use of three simple tools: checksum, acknowledgment, and time-out.

Checksum

Each segment includes a checksum field which is used to check for a corrupted segment.

If the segment is corrupted, it is discarded by the destination TCP and is considered as lost. TCP uses a 16-bit checksum that is mandatory in every segment.

Acknowledgment

TCP uses acknowledgments to confirm the receipt of data segments. Control segments that carry no data but consume a sequence number are also acknowledged. ACK segments are never acknowledged.

ACK segments do not consume sequence numbers and are not acknowledged layer, SCTP. However, it cannot be changed for TCP because this would involve reconfigurationof the entire header format.

Retransmission

The heart of the error control mechanism is the retransmission of segments. When a segment is corrupted, lost, or delayed, it is retransmitted. In modern implementations, a segment is retransmitted on two occasions: when a retransmission timer expires or when the sender receives three duplicate ACKs.

In modern implementations, a retransmission occurs if the retransmission timer expires or three duplicate ACK segments have arrived. Note that no retransmission occurs for segments that do not consume sequence numbers. In particular, there is no transmission for an ACK segment.

No retransmission timer is set for an ACK segment.

Retransmission After RTO A recent implementation of TCP maintains one retransmission time-out (RTO) timer for all outstanding (sent, but not acknowledged) segments.

When the timer matures, the earliest outstanding segment is retransmitted even

though lack of a received ACK can be due to a delayed segment, a delayed ACK, or a lost acknowledgment. Note that no time-out timer is set for a segment that carries only an

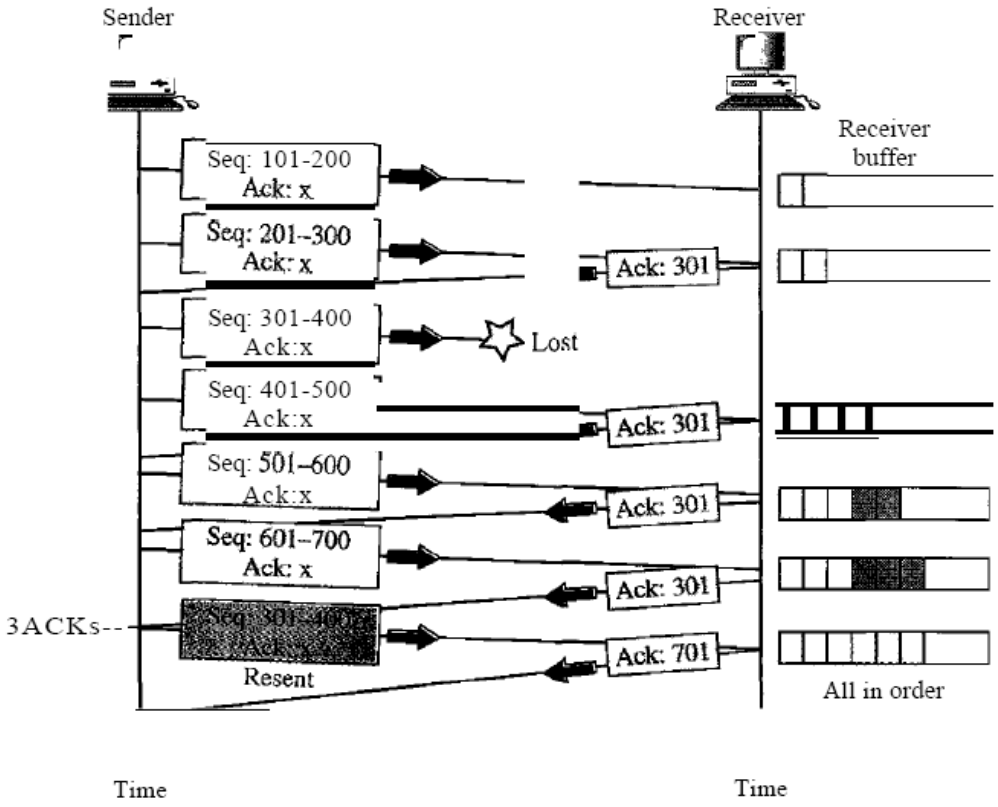
acknowledgment, which means that no such segment is resent. The value of RTO is dynamic in TCP and is updated based on the round-trip time (RTT) of segments. An RTI is the time needed for a segment to reach a destination and for an acknowledgment to be received.

Retransmission After Three Duplicate ACK Segments The previous rule about retransmission of a segment is sufficient if the value ofRTO is not very large. Sometimes, however, one segment is lost and the receiver receives so many out-of-order segments that they cannot be saved (limited buffer size). To alleviate this situation, most implementations today follow the three-duplicate-ACKs rule and retransmit the missing segment immediately. This feature is referred to as fast retransmission, which we will see in an example shortly.

Out-of-Order Segments

When a segment is delayed, lost, or discarded, the segments following that segment arrive out of order. Originally, TCP was designed to discard all out-of-order segments, resulting in the retransmission of the missing segment and the following segments. Most implementations today do not discard the out-of-order segments. They store them temporarily and flag them as out-of-order segments until the missing segment arrives. Note, however, that the out-of-order segments are not delivered to the process. TCP guarantees that data are delivered to the process in order.

Fast Retransmission



When the receiver receives the fourth, fifth, and sixth segments, it triggers an acknowledgment. The sender receives four acknowledgments with the same value (three duplicates). Although the timer for segment 3 has not matured yet, the fast transmission requires that segment 3, the segment that is expected by all these acknowledgments, be resent immediately.

Note that only one segment is retransmitted although four segments are not acknowledged. When the sender receives the retransmitted ACK, it knows that the four segments are safe and sound because acknowledgment is cumulative.

Questions	opt1	opt2	opt3
Data communication means exchange of data between _____devices.	one	two	six
The system must deliver data to the correct destination is called_____	accuracy	jitter	delivery
A_____ is the set of rules.	protocols	transmission medium	networks
In_____, the communication is unidirection.	duplex mode	full duplex mode	half duplex mode
A_____is a set of devices connected by communication links.	protocols	networks	computer
A_____connection provides a dedicated link between two devices.	point-to-point	multi-point	mesh
One long cable acts as a _____to link all the devices in a network.	bus	mesh	hub
MAN stands for _____	metropolitician area network	metropolitan area network	metropolitical area network
The term timing refers to _____ characteristics.	two	three	four
_____standards are often established originally by manufactures.	de jure	de facto	de fact
In physical layer we can transfer data into _____	frame	packet	bit
Hob to hob delivery is done by the _____	session layer	datalink layer	network layer
The _____layer is responsible for process to process delivery.	physical	presentation	networks
The _____layer is responsible for dialog control and synchronization.	transport	session	application
Tcp/Ip is a _____protocol.	hyper text	transfer	internet
Ip is a_____protocol.	hop to hop	node to node	process to process
A set of devices connected by a _____links	data	networks	communication
Bus topology has a long link called_____	backbone	hub	host
Periodic analog signals can be classified into _____	simple	composite	simple or composite
Period and frequency has the following formula.	f=1/t and t=1/f	t=1/f or f=1/t	c=t/f
Wavelength is_____	propagation speed	propagation speed * frequency	propagation speed/period

Composite signal can be classified into _____types	five	three	four
The range of frequency contained in a _____ signal is its bandwidth.	simple	composite	periodic
The bandwidth of the composite signal is the difference between the _____	highest	highest or lowest	highest and lowest
The _____is the number of bits sent in a second.	bit length	bandpass	bandwidth
Bit length is _____	propagation speed/period	propagation speed * frequency	bit
A_____signal is a composite analog signal with an infinite bandwidth	simple	composite	digital
Decibel (dB) =_____	10 log10 p2/p1	p1/p2	10 log10 p1/p2
Transmission time=_____	message size/birate	distance/bandwidth	message size/distance
_____and star is a point to point device.	bus	ring	mesh
Protocols can be classified into _____ key elements	one	three	four
_____is a basic key element.	protocols	standards	topology
Bit rate=_____	4*BW*log2L	2*BW*log2L	4*BW/L
OSI stands for_____	open systems interconnection	open system internetworking	open symantic interconnection
Net work layer delivers data in the form of_____	frame	bits	data
Session layer provides_____ services.	one	two	three
UDP _____	user data protocol	user datagram protocol	user defined protocol
FTP_____	file transmit protocol	file transmission protocol	file transfer protocol
SMTP_____	single mail transfer protocol	simple mail transfer protocol	simple mail transmission protocol
Complete a cycle is called as _____	period	frequency	non periodic
Jitter is a form of_____	frames	bits	packets
Each set is called a _____	node	code	unicode
Full duplex also called as_____	simple duplex	single duplex	multiple duplex

_____can be measured in transmit time and response time.	performance	frequency	period
A multipoint is also called as_____	multi line	multi drop	multi level
Mesh topology we need _____	n(n-1)	n(n+1)	n(n+1)/2
A_____topology on the other hand is multipoint.	star	ring	bus
A_____can be hybrid	physical	networks	data
A MAN is a network with a size between a _____ and _____.	WAN and LAN	WAN or LAN	LAN
When Two or more networks are connected they become an _____	network	inter network	internet connection
The_____layer is responsible for providing services to the user.	presentation	datalink	application
The _____ layer is responsible for translation, compression encryption.	transport	data link	presentation
The_____layer is responsible for the delivery of a message from one process to another.	data link	transport	presentation
A _____layer is responsible for the delivery of packets from the source to destination.	physical	data link	network
The _____layer is responsible for moving frames from one hop to the next.	data link	physical	network
The _____layer is responsible for movements of bits from one hop to next.	data link	physical	transport
RARP _____	reverse address resolution protocol	reverse address result protocol	reverse addess revolutinized protocol
_____does not define any specific protocol.	TCP	HTTP	TCP/IP
The TCP/IP protocol suite was developed prior to the_____model.	OSI	ISO	TCP
The _____layer is responsible for flow control.	session	presentation	application
The term _____ data refers to information continous	analog	digital	physical

The sine wave is the most fundamental form of a _____analog signal.	composite	single	periodic

opt4	opt5	opt6
four		
timeliness		
ip		
simplex mode		
printer		
physical		
backbone		
macro area network		
six		
semantics		
sp du		
transport layer		
transport		
presentation		
hierarchical		
host to host		
application		
hop		
simple and composite		
t=c/f		
propagation speed/frequency		

two		
non periodic		
lowest		
bit rate		
propagation speed*bit duration		
analog		
2log10 p1/p2		
message size/bandwidth		
physical		
two		
protocols and standards		
2*BW*log 4L		
open system internet		
packet		
four		
user dataframe protocol		
flip transfer protocol		
single mail transmit protocol		
periodic		
dp tu		
polar		
duplex		

non period		
single level		
n(n-1)/2		
mesh		
link		
WAN		
interconnection		
network		
application		
network		
session		
presentation		
session		
reverse addess research protocol		
SMTP		
IP		
transport		
analog and digital		

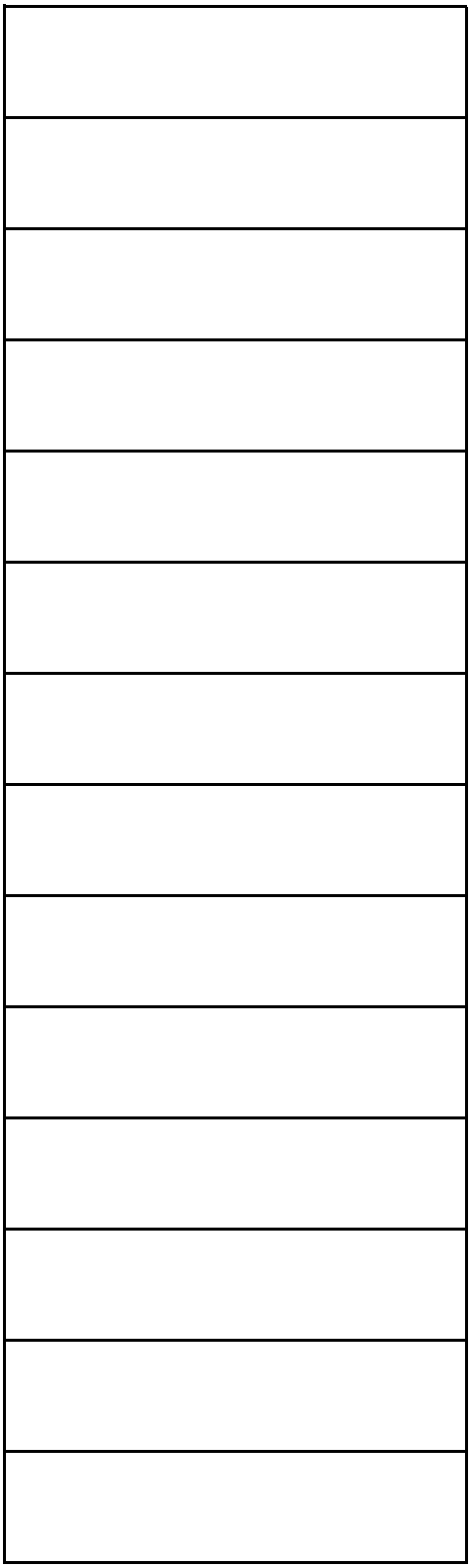
non periodic		

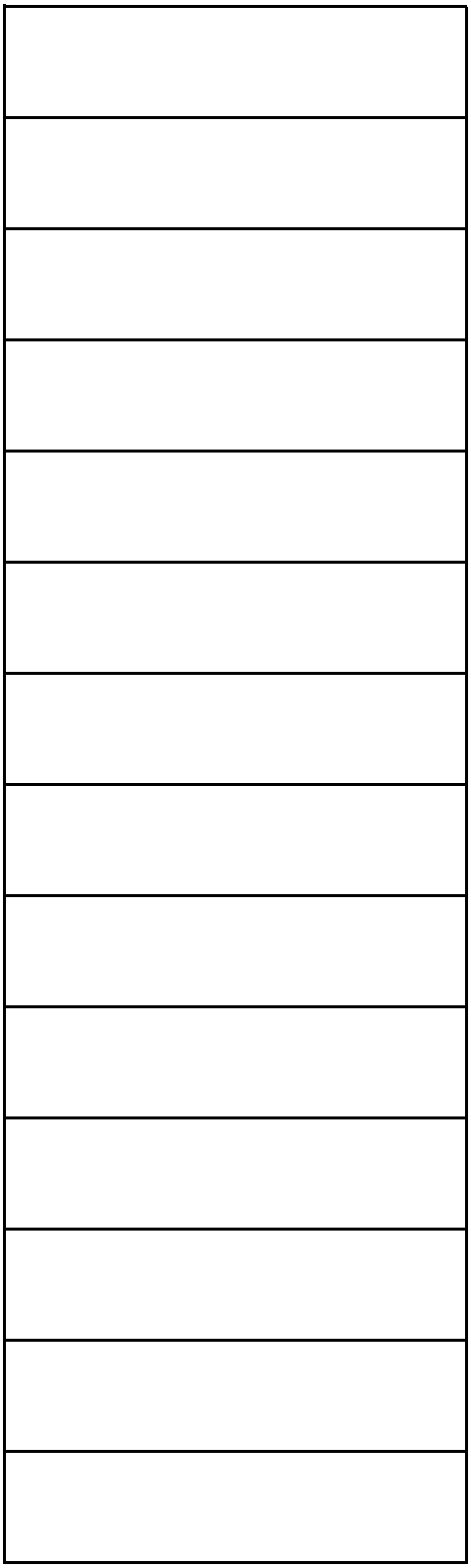
Answer
two
delivery
protocols
simplex mode
networks
point-to-point
backbone
metropolitan area network
two
de facto
bit
datalink layer
transport
session
hierarchical
host to host
communication
backbone
simple or composite
f=1/t and t=1/f
propagation speed/frequency

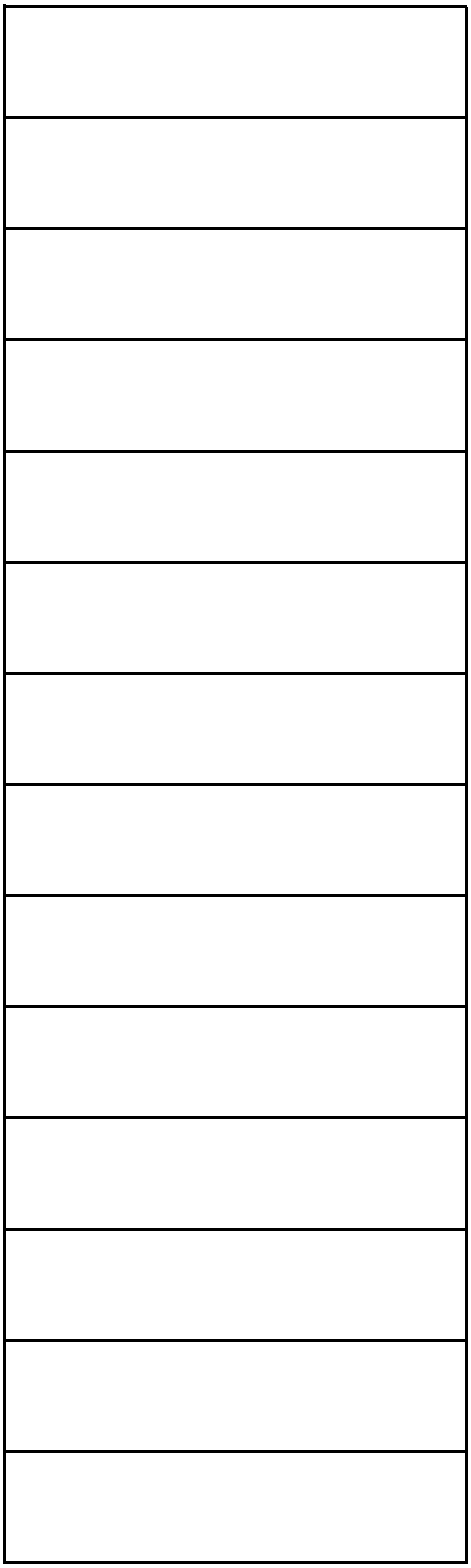
two
composite
highest and lowest
bit rate
propagation speed*bit duration
digital
10 log10 p2/p1
message size/bandwidth
mesh
three
protocols and standards
2*BW*log2L
open systems interconnection
packet
two
user datagram protocol
file transfer protocol
simple mail transfer protocol
period
packets
node
duplex

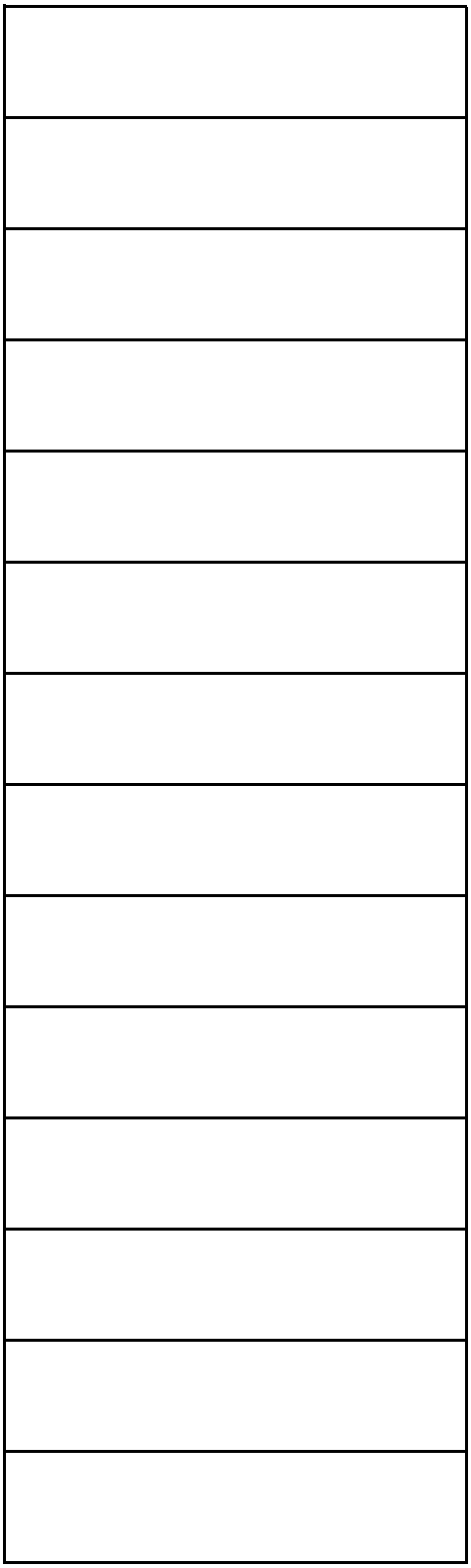
performance
multi drop
n(n-1)/2
bus
networks
WAN and LAN
inter network
application
presentation
transport
network
data link
physical
reverse address resolution protocol
TCP/IP
OSI
transport
analog

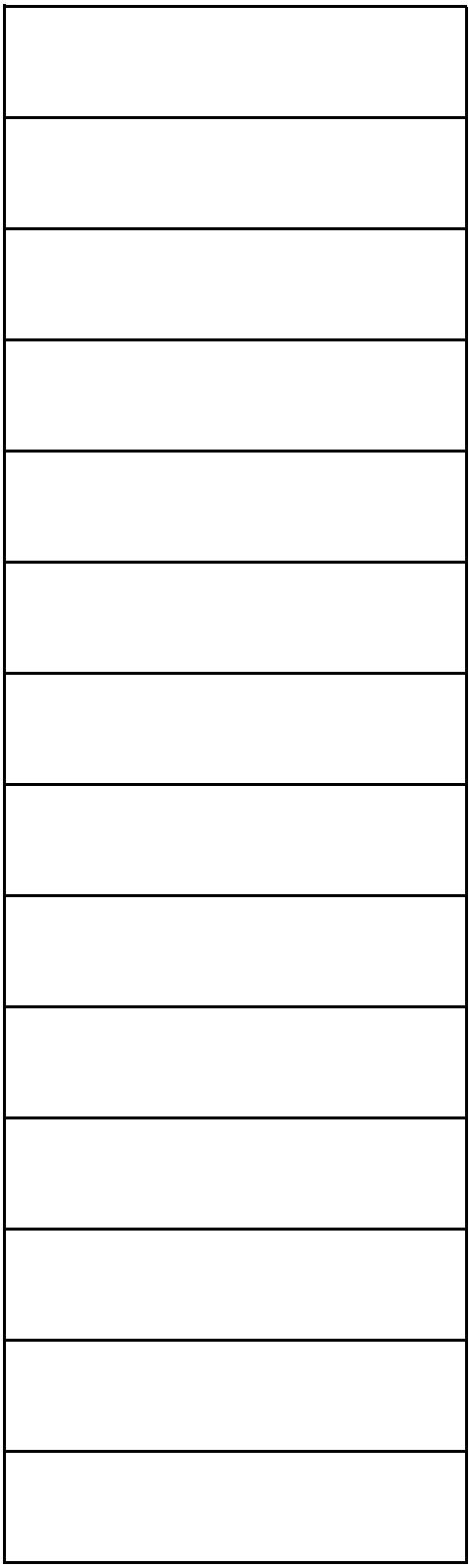
periodic

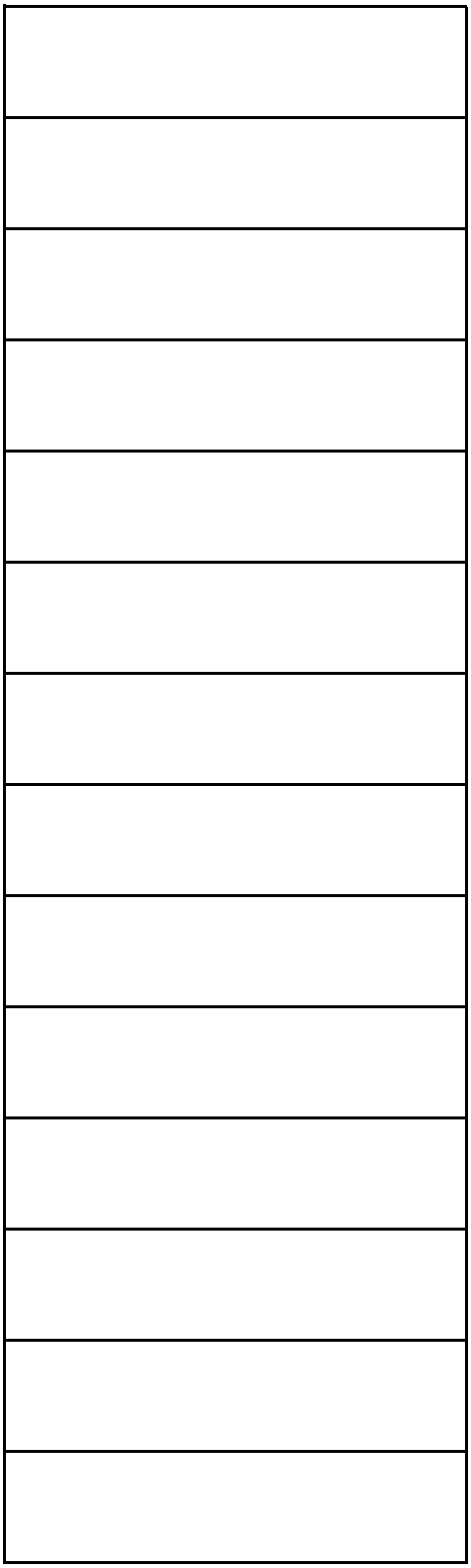


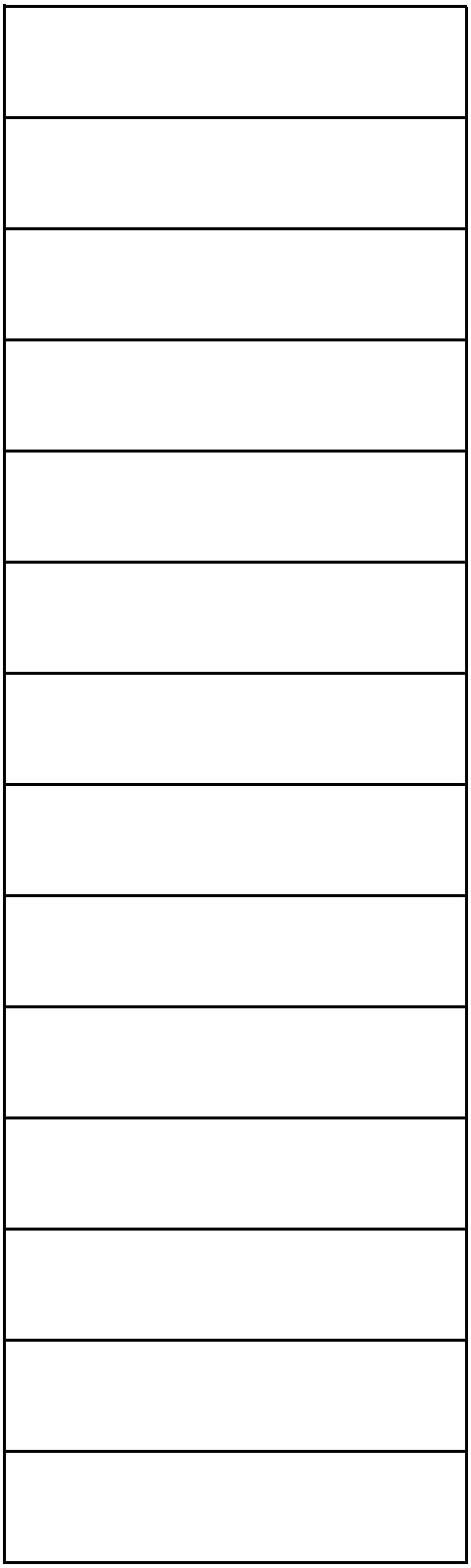


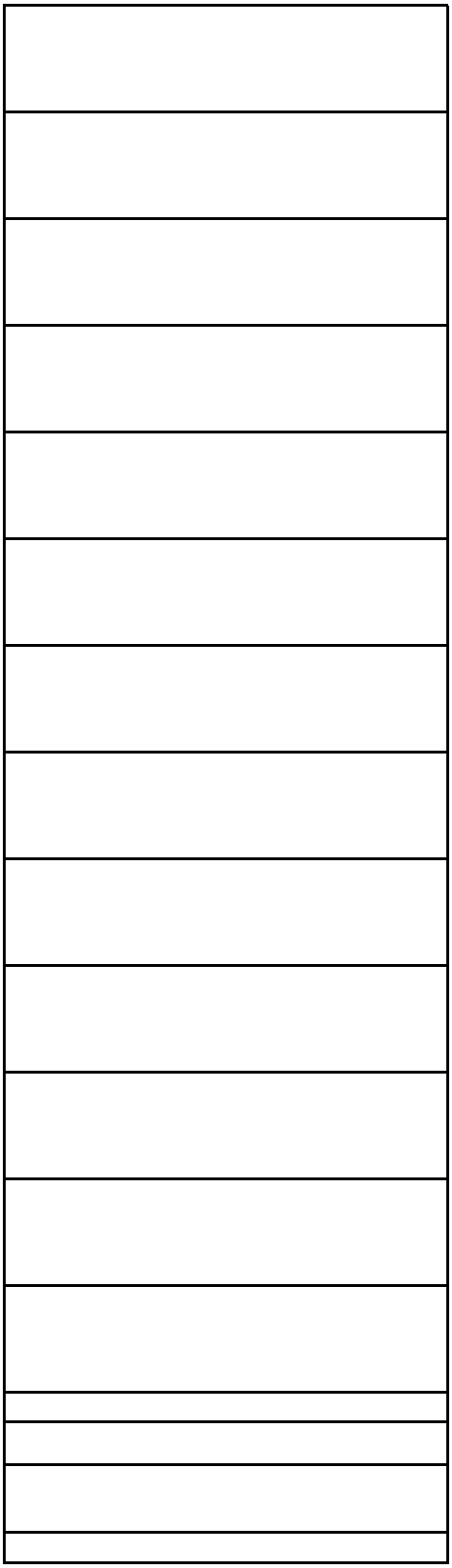


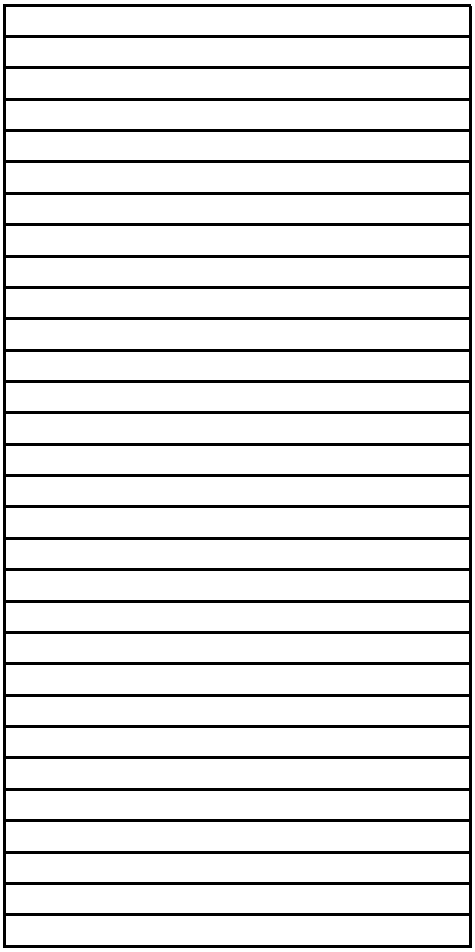












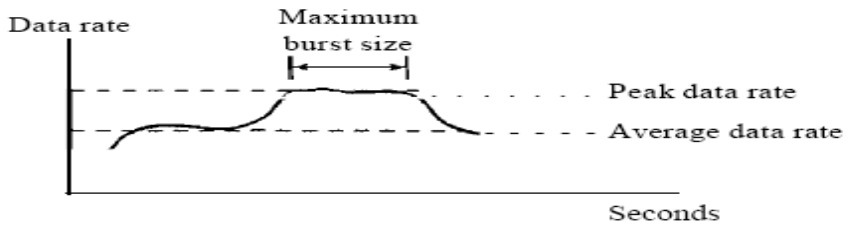
UNIT-V

DATA TRAFFIC

The main focus of congestion control and quality of service is data traffic. In congestion control we try to avoid traffic congestion. In quality of service, we try to create an appropriate environment for the traffic.

Traffic Descriptor

Traffic descriptors are qualitative values that represent a data flow. Figure shows a traffic flow with some of these values.



Average Data Rate

The average data rate is the number of bits sent during a period of time, divided by the number of seconds in that period. We use the following equation:

Average data rate =amount of data time

The average data rate is a very useful characteristic of traffic because it indicates the average bandwidth needed by the traffic.

Peak Data Rate

The peak data rate defines the maximum data rate of the traffic. In the above Figure it is the maximum *y* axis value. The peak data rate is a very important measurement because it indicates the peak bandwidth that the network needs for traffic to pass through without changing its data flow.

Maximum Burst Size

Although the peak data rate is a critical value for the network, it can usually be ignored if the duration of the peak value is very short. For example, if data are flowing steadily at the rate of 1 Mbps with a sudden peak data rate of 2 Mbps for just 1 ms, the network probably can handle the situation. However, if the peak data rate lasts 60 ms, there may be a problem for the network. The maximum burst size normally refers to the maximum length of time the traffic is generated at the peak rate.

Effective Bandwidth

The effective bandwidth is the bandwidth that the network needs to allocate for the flow of traffic. The effective bandwidth is a function of three values: average data rate, peak data rate, and maximum burst size. The calculation of this value is very complex.

Traffic Profiles

For our purposes, a data flow can have one of the following traffic profiles: constant bit rate, variable bit rate, or bursty as shown in above Figure .

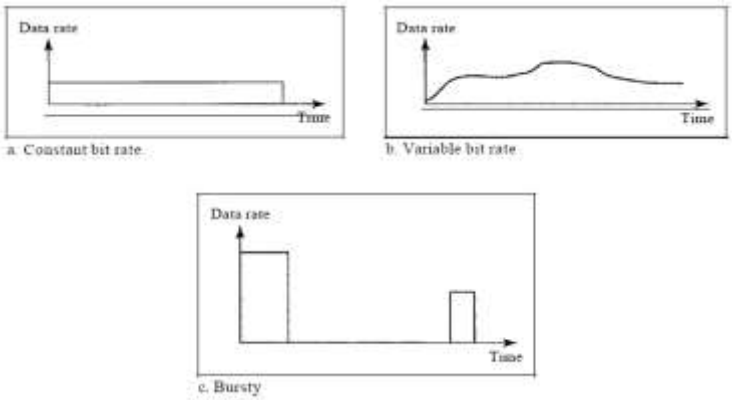
Constant Bit Rate

A constant-bit-rate (CBR), or a fixed-rate, traffic model has a data rate that does not change. In this type of flow, the average data ratc and thc peak data rate are the same.

The maximum burst size is not applicable. This type of traffic is very easy for a network to handle since it is predictable. The network knows in advance how much bandwidth to allocate for this type of flow.

Variable Bit Rate

In the variable-bit-rate (VBR) category, the rate of the data flow changes in time, with the changes smooth instead of sudden and sharp. In this type of flow, the average datarate and the peak data rate are different. The maximum burst size is usually a small value.



Bursty

In the **bursty data** category, the data rate changes suddenly in a very short time. It may jump from zero, for example, to 1 Mbps in a few microseconds and vice versa. It may also remain at this value for a while. The average bit rate and the peak bit rate are very different values in this type of flow. The maximum burst size is significant. This is the most difficult type of traffic for a network to handle because the profile is very unpredictable.

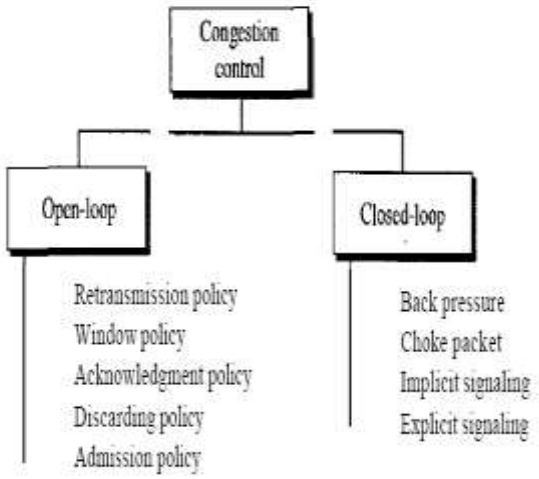
CONGESTION

Congestion in a network may occur if the **load** on the network-the number of packets sent to the network-is greater than the *capacity* of the network-the number of packets a network can handle. **Congestion control** refers to the mechanisms and techniques to control the congestion and keep the load below the capacity.

Congestion in a network or internetwork occurs because routers and switches have queues-buffers that hold the packets before and after processing. A router, for example, has an input queue and an output queue for each interface.

CONGESTION CONTROL

Congestion control refers to techniques and mechanisms that can either prevent congestion, before it happens, or remove congestion, after it has happened.



Open-Loop Congestion Control

In open-loop congestion control, policies are applied to prevent congestion before it happens. In these mechanisms, congestion control is handled by either the source or the destination.

Retransmission Policy

Retransmission is sometimes unavoidable. If the sender feels that a sent packet is lost or corrupted, the packet needs to be retransmitted. Retransmission in general may increase congestion in the network. However, a good retransmission policy can prevent congestion. The retransmission policy and the retransmission timers must be designed to optimize efficiency and at the same time prevent congestion.

Window Policy

The type of window at the sender may also affect congestion. The Selective Repeat window is better than the Go-Back-N window for congestion control. In the *Go-Back-N* window, when the timer for a packet times out, several packets may be resent, although some may have arrived safe and sound at the receiver. This duplication may make the congestion worse. The Selective Repeat window, on the other hand, tries to send the specific packets that have been lost or corrupted.

Acknowledgment Policy

The acknowledgment policy imposed by the receiver may also affect congestion. If the receiver does not acknowledge every packet it receives, it may slow down the sender and help prevent

congestion. Several approaches are used in this case. A receiver may send an acknowledgment only if it has a packet to be sent or a special timer expires. A receiver may decide to acknowledge only *N* packets at a time. We need to know that the acknowledgments are also part of the load in a network. Sending fewer acknowledgments means imposing less load on the network.

Discarding Policy

A good discarding policy by the routers may prevent congestion and at the same time may not harm the integrity of the transmission. For example, in audio transmission, if the policy is to discard less sensitive packets when congestion is likely to happen, the quality of sound is still preserved and congestion is prevented or alleviated.

Admission Policy

An admission policy, which is a quality-of-service mechanism, can also prevent congestion in virtual-circuit networks. Switches in a flow first check the resource requirement of a flow before admitting it to the network. A router can deny establishing a virtual circuit connection if there is congestion in the network or if there is a possibility of future congestion.

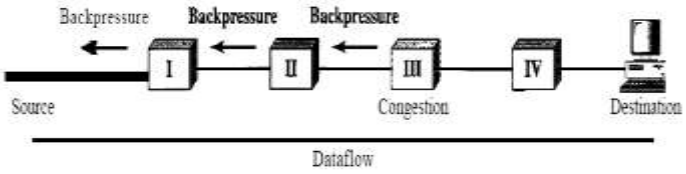
Closed-Loop Congestion Control

Closed-loop congestion control mechanisms try to alleviate congestion after it happens.

Several mechanisms have been used by different protocols. We describe a few of them here.

Backpressure

The technique of *backpressure* refers to a congestion control mechanism in which a congested node stops receiving data from the immediate upstream node or nodes. This may cause the upstream node or nodes to become congested, and they, in turn, reject data from their upstream nodes or nodes. And so on. Backpressure is a node-to-node congestion control that starts with a node and propagates, in the opposite direction of data flow, to the source. The backpressure technique can be applied only to virtual circuit networks, in which each node knows the upstream node from which a flow of data is corning.



Node III in the figure has more input data than it can handle. It drops some packets in its input buffer and informs node II to slow down. Node II, in turn, may be congested because it is slowing down the output flow of data. If node II is congested, it informs node I to slow down, which in turn may create congestion. If so, node I inform the source of data to slow down. This, in time, alleviates the congestion. Note that the *pressure* on node III is moved backward to the source to remove the congestion.

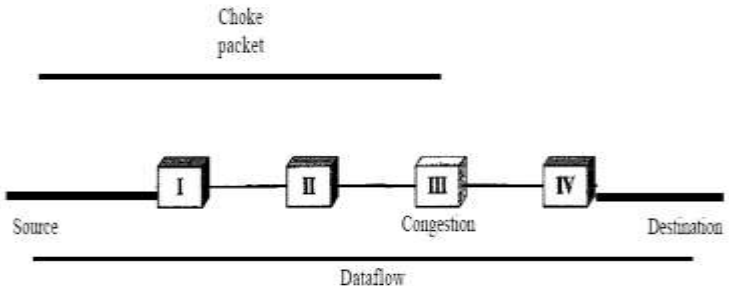
None of the virtual-circuit networks we studied in this book use backpressure. It was, however, implemented in the first virtual-circuit network, X.25. The technique cannot be implemented in a datagram network because in this type of network, a node (router) does not have the slightest knowledge of the upstream router.

Choke Packet

A choke packet is a packet sent by a node to the source to inform it of congestion.

Note the difference between the backpressure and choke packet methods. In backpressure, the warning is from one node to its upstream node, although the warning may eventually reach the source station. In the choke packet method, the warning is from the router, which has encountered congestion, to the source station directly. The intermediate nodes through which the packet has travelled are not warned. We have seen an example of this type of control in ICMP. When a router in the Internet is overwhelmed with IP datagrams, it may discard some of them; but it informs the source host, using a source quench ICMP message. The warning message goes directly to the source station; the intermediate routers, and does not take any action.

This figure shows the idea of a choke packet.



Implicit Signalling

In implicit signalling, there is no communication between the congested node or nodes and the source. The source guesses that there is congestion somewhere in the network from other symptoms. For example, when a source sends several packets and there is no acknowledgment for a while, one assumption is that the network is congested. The delay in receiving an acknowledgment is interpreted as congestion in the network; the source should slow down. We will see this type of signalling when we discuss TCP congestion control later in the chapter.

Explicit Signalling

The node that experiences congestion can explicitly send a signal to the source or destination.

The explicit signalling method, however, is different from the choke packet method. In the choke packet method, a separate packet is used for this purpose; in the explicit signalling method, the signal is included in the packets that carry data. Explicit signalling, as we will see in Frame Relay congestion control, can occur in either the forward or the backward direction.

Backward Signalling A bit can be set in a packet moving in the direction opposite to the congestion. This bit can warn the source that there is congestion and that it needs to slow down to avoid the discarding of packets. Forward Signalling A bit can be set in a packet moving in the direction of the congestion. This bit can warn the destination that there is congestion. The receiver in this case can use policies, such as slowing down the acknowledgments, to alleviate the I congestion.

Application Layer

Electronic Mail

The most heavily used application in virtually any distributed system is electronic mail. The Simple Mail Transfer Protocol (SMTP) has always been the workhorse of the TCP/IP suite. However, SMTP has traditionally been limited to the delivery of simple text messages. In recent years, there has been a demand for the capability to deliver mail containing various types of data, including voice, images, and video clips. To satisfy this requirement, a new electronic mail standard, which builds on SMTP, has been defined: the Multi-Purpose Internet Mail Extension (MIME). In this section, we first examine SMTP, and then look at MIME.

SMTP

SMTP is the standard protocol for transferring mail between hosts in the TCP/IP suite; it is defined in RFC 821. Although messages transferred by SMTP usually follow the format defined in RFC 822, described later, SMTP is not concerned with the format or content of messages themselves, with two exceptions. This concept is often expressed by saying that SMTP uses information written on the *envelope* of the mail (message header), but does not look at the contents (message body) of the envelope. The two exceptions:

1. SMTP standardizes the message character set as 7-bit ASCII.
2. SMTP adds log information to the start of the delivered message that indicates the path the message took.

- RFC 821
- not concerned with format of messages or data
  - covered in RFC 822 (see later)
- SMTP uses info written on envelope of mail
  - message header
- does not look at contents

- message body
- except:
  - standardize message character set to 7 bit ASCII
  - add log info to start of message

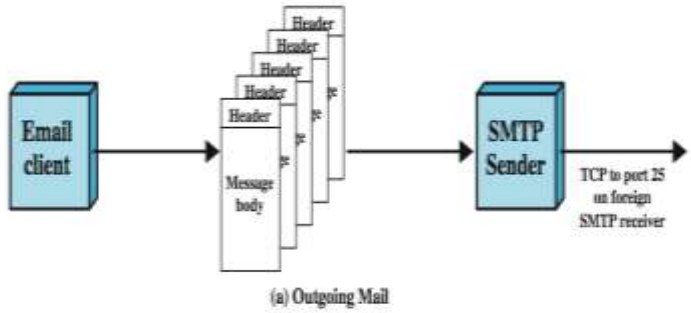
Basic Operation

To begin, mail is created by a user agent program in response to user input. Each created message consists of a header that includes the recipient's e-mail address and other information, and a body containing the message to be sent. These messages are then queued in some fashion and provided as input to an SMTP Sender program, which is typically an always-present server program on the host.

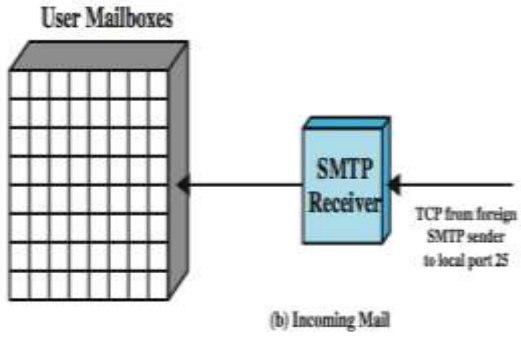
- email message is created by user agent program (mail client), and consists of:
  - header with recipient's address and other info
  - body containing user data
- messages queued and sent as input to SMTP sender program
  - yypically a server process (daemon on UNIX)

SMTP Mail Flow

Figure below illustrates the overall flow of mail in a typical system. Although much of this activity is outside the scope of SMTP, the figure illustrates the context within which SMTP typically operates.



(a) Outgoing Mail



(b) Incoming Mail

Mail Message Contents

Although the structure of the outgoing mail queue will differ depending on the host's operating system, each queued message conceptually has two parts:

1. The message text, consisting ofThe RFC 822 header (constitutes the message envelope and includes an indication of the intended recipient or recipients), andt he body of the message, composed by the user.
2. A list of mail destinations.

The list of mail destinations for the message is derived by the user agent from the 822 message header. In some cases, the destination or destinations are literally specified in the message header. In other cases, the user agent may need to expand mailing list names, remove duplicates, and replace mnemonic names with actual mailbox names. If any blind carbon copies (BCCs) are indicated, the user agent needs to prepare messages that conform to this requirement. The basic idea is that the multiple formats and styles preferred by humans in the user interface are replaced by a standardized list suitable for the SMTP send program.

- each queued message has two parts
- message text
  - RFC 822 header with envelope and list of recipients
  - message body, composed by user
- list of mail destinations
  - derived by user agent from header

- may be listed in header
- may require expansion of mailing lists
- may need replacement of mnemonic names with mailbox names

➢ if BCCs indicated, user agent needs to prepare correct message format

SMTP Sender

The SMTP sender takes messages from the outgoing mail queue and transmits them to the proper destination host via SMTP transactions over one or more TCP connections to port 25 on the target hosts. A host may have multiple SMTP senders active simultaneously if it has a large volume of outgoing mail, and should also have the capability of creating SMTP receivers on demand so that mail from one host cannot delay mail from another. Whenever the SMTP sender completes delivery of a particular message to one or more users on a specific host, it deletes the corresponding destinations from that message's destination list. When all destinations for a particular message are processed, the message is deleted from the queue.

Sending Optimizations

In processing a queue, the SMTP sender can perform a variety of optimizations. If a particular message is sent to multiple users on a single host, the message text need be sent only once. If multiple messages are ready to send to the same host, the SMTP sender can open a TCP connection, transfer the multiple messages, and then close the connection, rather than opening and closing a connection for each message.

Possible Errors

The SMTP sender must deal with a variety of errors. The destination host may be unreachable, out of operation, or the TCP connection may fail while mail is being transferred. The sender can requeue the mail for later delivery, but give up after some period rather than keep the message in the queue indefinitely. A common error is a faulty destination address, which can occur due to user input error or because the intended destination user has a new address on a different host. The SMTP sender must either redirect the message if possible or return an error notification to the message's originator.

SMTP Protocol – Reliability

The SMTP protocol is used to transfer a message from the SMTP sender to the SMTP receiver over a TCP connection. SMTP attempts to provide reliable operation but does not guarantee to recover from lost messages. SMTP does not return an end-to-end acknowledgment to a message's originator to indicate that a message is successfully delivered to the message's recipient. Also, SMTP does not guarantee to return error indications. However, the SMTP-based mail system is generally considered reliable.

SMTP Receiver

The SMTP receiver accepts each arriving message and either places it in the appropriate user mailbox or copies it to the local outgoing mail queue if forwarding is required. The SMTP receiver must be able to verify local mail destinations and deal with errors, including transmission errors and lack of storage capacity.

The SMTP sender is responsible for a message up to the point where the SMTP receiver indicates that the transfer is complete; however, this simply means that the message has arrived at the SMTP receiver, not that the message has been delivered to and retrieved by the intended final recipient. The SMTP receiver's error-handling responsibilities are generally limited to giving up on TCP connections that fail or are inactive for very long periods. Thus, the sender has most of the error recovery responsibility. Errors during completion indication may cause duplicate, but not lost, messages**.**

SMTP Forwarding

In most cases, messages go directly from the mail originator's machine to the destination machine over a single TCP connection. However, mail will occasionally go through intermediate machines via an SMTP forwarding capability, in which case the message must traverse a series of TCP

connections between source and destination. One way for this to happen is for the sender to specify a route to the destination in the form of a sequence of servers. A more common event is forwarding required because a user has moved.

Conversation

It is important to note that the SMTP protocol is limited to the conversation that takes place between the SMTP sender and the SMTP receiver. SMTP's main function is the transfer of messages, although there are some ancillary functions dealing with mail destination verification and handling. The rest of the mail-handling apparatus depicted in Figure below is beyond the scope of SMTP and may differ from one system to another.

SMTP System Overview

The operation of SMTP consists of a series of commands and responses exchanged between the SMTP sender and receiver. The initiative is with the SMTP sender, who establishes the TCP connection. Once the connection is established, the SMTP sender sends commands over the connection to the receiver. Each command generates exactly one reply from the SMTP receiver.

SMTP Commands

Each command consists of a single line of text, beginning with a four-letter command code followed in some cases by an argument field. Most replies are a single-line, although multiple-line replies are possible. The table lists first those commands that all receivers must be able to recognize. The other commands are optional and may be ignored by the receiver.

SMTP Replies

SMTP replies are listed in Stallings DCC8e Table 22.2. Each reply begins with a three-digit code and may be followed by additional information. The leading digit indicates the category of the reply:

• Positive Completion reply: The requested action has been successfully completed. A new request may be initiated.

• Positive Intermediate reply: The command has been accepted, but the requested action is being held in abeyance, pending receipt of further information. The sender-SMTP should send another command specifying this information. This reply is used in command sequence groups.

• Transient Negative Completion reply: The command was not accepted and the requested action did not occur. However, the error condition is temporary and the action may be requested again.

• Permanent Negative Completion reply: The command was not accepted and the requested action did not occur.

Connection Setup

Basic SMTP operation occurs in three phases: connection setup, exchange of one or more command-response pairs, and connection termination.

In the connection setup phase, an SMTP sender will attempt to set up a TCP connection with a target host when it has one or more mail messages to deliver to that host. The sequence is quite simple:

1. The sender opens a TCP connection with the receiver.
2. Once the connection is established, the receiver identifies itself with "220 Service Ready".
3. The sender identifies itself with the HELO command.
4. The receiver accepts the sender's identification with "250 OK".

If the mail service on the destination is unavailable, the destination host returns a "421 Service Not Available" reply in step 2 and the process is terminated.

Mail Transfer

Once a connection has been established, the SMTP sender may send one or more messages to the SMTP receiver. There are three logical phases to the transfer of a message:

1. A MAIL command identifies the originator of the message. The MAIL command gives the reverse path, which can be used to report errors. If the receiver is prepared to accept messages from this originator, it returns a "250 OK" reply. Otherwise the receiver returns a reply indicating failure

to execute the command (codes 451, 452, 552) or an error in the command (codes 421, 500, 501).
2. One or more RCPT commands identify the recipients for this message. The RCPT command identifies an individual recipient of the mail data; multiple recipients are specified by multiple use of this command. A separate reply is returned for each RCPT command. The receiver can accept the destination with a 250 reply; or return an appropriate fail/error response.
3. A DATA command transfers the message text. The advantage of using a separate RCPT phase is that the sender will not send the message until it is assured that the receiver is prepared to receive the message for at least one recipient, thereby avoiding the overhead of sending an entire message only to learn that the destination is unknown. Once the SMTP receiver has agreed to receive the mail message for at least one recipient, the SMTP sender uses the DATA command to initiate the transfer of the message. The end of the message is indicated by a line containing only a period**.**

Example SMTP Transfer

- S: MAIL FROM:<Smith@Alpha.ARPA>
- R: 250 OK
- S: RCPT TO:<Jones@Beta.ARPA>
- R: 250 OK
- S: RCPT TO:<Green@Beta.ARPA>
- R: 550 No such user here
- S: RCPT TO:<Brown@Beta.ARPA>
- R: 250 OK
- S: DATA
- R: 354 Start mail input; end with <CRLF>.<CRLF>
- S: Blah blah blah...
- S: ...etc. etc. etc.
- S: <CRLF>.<CRLF>
- R: 250 OK

This example, taken from RFC 821, illustrates the SMTP mail transfer process. The SMTP sender is transmitting mail that originates with the user Smith@Alpha.ARPA. The message is addressed to three users on machine Beta.ARPA, namely, Jones, Green, and Brown. The SMTP receiver indicates that it has mailboxes for Jones and Brown but does not have information on Green. Because at least one of the intended recipients has been verified, the sender proceeds to send the text message.

Closing Connection

The SMTP sender closes the connection in two steps. First, the sender sends a QUIT command and waits for a reply. The second step is to initiate a TCP close operation for the TCP connection. The receiver initiates its TCP close after sending its reply to the QUIT command

- *two steps*
- *sender sends QUIT and waits for reply*
- *then initiate TCP close operation*
- *receiver initiates TCP close after sending reply to QUIT*

FILE TRANSFER

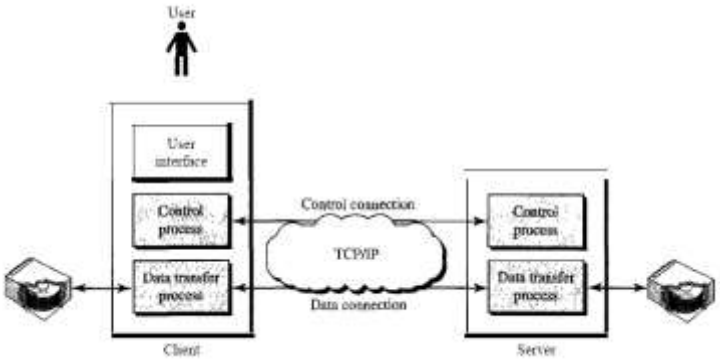
Transferring files from one computer to another is one of the most common tasks expected from a networking or internetworking environment. As a matter of fact, the greatest volume of data exchange in the Internet today is due to file transfer. File ransfer Protocol *(FTP).*

File Transfer Protocol (FTP)

- File Transfer Protocol (FTP) is the standard mechanism provided by *TCP/IP* for copying a file from one host to another. Although transferring files from one system to another seems simple and straightforward, some problems must be dealt with first. For example, two

systems may use different file name conventions. Two systems may have different ways to represent text and data. Two systems may have different directory structures. All these problems have been solved by FTP in a very simple and elegant approach.

- FTP differs from other client/server applications in that it establishes two connections between the hosts. One connection is used for data transfer, the other for control information (commands and responses). Separation of commands and data transfer makes FTP more efficient. The control connection uses very simple rules of communication.We need to transfer only a line of command or a line of response at a time. The data connection, on the other hand, needs more complex rules due to the variety of data types transferred. However, the difference in complexity is at the FTP level, not TCP. For TCP, both connections are treated the same.
- FTP uses two well-known TCP ports: Port 21 is used for the control connection, and port 20 is used for the data connection.
- FTP uses the services of TCP. It needs two TCP connections.
- The well-known port 21 is used for the control connection and the well-known port 20 for the data connection.
- Figure below shows the basic model of FTP. The client has three components: user interface, client control process, and the client data transfer process. The server has two components: the server control process and the server data transfer process. The control connection is made between the control processes. The data connection is made between the data transfer processes.



The control connection remains connected during the entire interactive FTP session.

The data connection is opened and then closed for each file transferred. It opens each time commands that involve transferring files are used, and it closes when the file is transferred. In other words, when a user starts an FTP session, the control connection opens. While the control connection is open, the data connection can be opened and closed multiple times if several files are transferred.

Communication over Control Connection

FTP uses the same approach as SMTP to communicate across the control connection. It uses the 7-bit ASCII character set . Communication is achieved through commands and responses. This simple method is adequate for the control connection because we send one command (or response) at a time. Each command or response is only one short line, so we need not worry about file format or file structure.

Each line is terminated with a two-character (carriage return and line feed) end-of-line token.

Communication over Data Connection

The purpose of the data connection is different from that of the control connection. We want to transfer files through the data connection. File transfer occurs over the data connection under the control of the commands sent over the control connection. However, we should remember that file transfer in FTP means one of three things:

o A file is to be copied from the server to the client. This is called *retrieving aft/e.* It is done under the supervision of the RETR command,

o A file is to be copied from the client to the server. This is called *storing aft/e*. It is done under the supervision of the STOR command.

o A list of directory or file names is to be sent from the server to the client. This is done under the supervision of the LIST command. Note that FTP treats a list of directory or file names as a file. It is sent over the data connection.

The client must define the type of file to be transferred, the structure of the data, and the transmission mode. Before sending the file through the data connection, we prepare for transmission through the control connection. The heterogeneity problem is resolved by defining three attributes of communication: file type, data structure, and transmission mode

File Type FTP can transfer one of the following file types across the data connection:an ASCII file, EBCDIC file, or image file. The ASCII file is the default format for transferring text files. Each character is encoded using 7-bit ASCII. The sender transforms the file from its own representation into ASCII characters, and the receiver transforms the ASCII characters to its own representation. If one or both ends of the connection use EBCDIC encoding (the file format used by IBM), the file can be transferred using EBCDIC encoding. The image file is the default format for transferring binary files. The file is sent as continuous streams of bits without any interpretation or encoding. This is mostly used to transfer binary files such as compiled programs.

Data Structure FTP can transfer a file across the data connection by using one of the following interpretations about the structure of the data: file structure, record structure, and page structure. In the file structure format, the file is a continuous stream of bytes. In the record structure, the file is divided into records. This can be used only with text files. In the page structure, the file is divided into pages, with each page having a page number and a page header. The pages can be stored and accessed randomly or sequentially.

Transmission Mode FTP can transfer a file across the data connection by using one of the following three transmission modes: stream mode, block mode, and compressed mode. The stream mode is the default mode. Data are delivered from FTP to TCP as a continuous stream of bytes. TCP is responsible for chopping data into segments of appropriate size. If the data are simply a stream of bytes (file structure), no end-of-file is needed. End-of-file in this case is the closing of the data connection by the sender. If the data are divided into records (record structure), each record will have a I-byte end of- record (EOR) character and the end of the file will have a I-byte end-of-file (EOF) character. In block mode, data can be delivered from FTP to TCP in blocks. In this case, each block is preceded by a 3-byte header. The first byte is called the *block descriptor;* the next 2 bytes define the size of the block in bytes. In the compressed mode, if the file is big, the data can be compressed. The compression method normally used is run-length encoding. In this method, consecutive appearances of a data unit are replaced by one occurrence and the number of repetitions. In a text file, this is usually spaces (blanks). In a binary file, null characters are usually compressed.

Anonymous FTP

To use FTP, a user needs an account (user name) and a password on the remote server. Some sites have a set of files available for public access, to enable anonymous FTP. To access these files, a user does not need to have an account or password. Instead, the user can use *anonymous* as the user name and *guest* as the password.

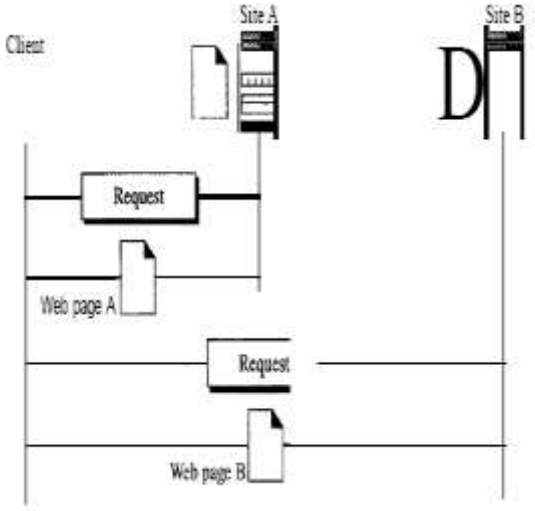
User access to the system is very limited. Some sites allow anonymous users only a subset of commands. For example, most sites allow the user to copy some files, but do not allow navigation through the directories.

WWW and HTTP

The **World Wide Web** (WWW) is a repository of information linked together from points all over the world. The WWW has a unique combination of flexibility, portability, and user-friendly features that distinguish it from other services provided by the Internet. The WWW project was initiated by CERN (European Laboratory for Particle Physics) to create a system to handle distributed resources necessary for scientific research.

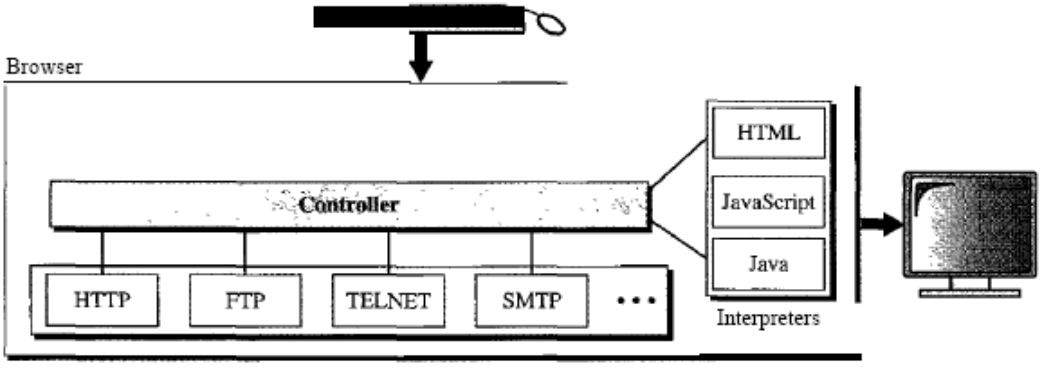
ARCHITECTURE

The WWW today is a distributed clientJserver service, in which a client using a browser can access a service using a server. However, the service provided is distributed over many locations called *sites,* Each site holds one or more documents, referred to as *Web pages.* Each Web page can contain a link to other pages in the same site or at other sites. The pages can be retrieved and viewed by using browsers. Let us go through the scenario shown in Figure below. The client needs to see some information that it knows belongs to site A. It sends a request through its browser, a program that is designed to fetch Web documents. The request, among other information, includes the address of the site and the Web page, called the URL, which we will discuss shortly. The server at site A finds the document and sends it to the client. When the user views the document, she finds some references to other documents, including a Web page at site B. The reference has the URL for the new site. The user is also interested in seeing this document. The client sends another request to the new site, and the new page is retrieved.



Client (Browser)

A variety of vendors offer commercial browsers that interpret and display a Web document, and all use nearly the same architecture. Each browser usually consists of three parts: a controller, client protocol, and interpreters. The controller receives input from the keyboard or the mouse and uses the client programs to access the document. After the document has been accessed, the controller uses one of the interpreters to display the document on the screen. The client protocol can be one of the protocols described previously such as FfP or HTIP (described later in the chapter). The interpreter can be HTML, Java, or JavaScript, depending on the type of document.



Server

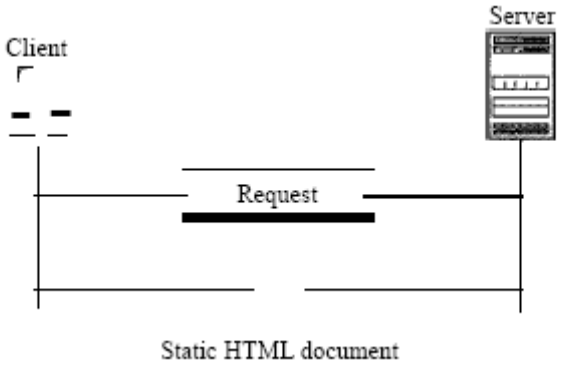
The Web page is stored at the server. Each time a client request arrives, the corresponding document is sent to the client. To improve efficiency, servers normally store requested files in a cache in memory; memory is faster to access than disk. A server can also become more efficient through multithreading or multiprocessing. In this case, a server can answer more than one request at a time.

Uniform Resource Locator

A client that wants to access a Web page needs the address. To facilitate the access of documents distributed throughout the world, HTTP uses locators. The uniform resource locator (URL) is a standard for specifying any kind of information on the Internet. The URL defines four things: protocol, host computer, port, and path The *protocol* is the client/server program used to retrieve the

document. Many different protocols can retrieve a document; among them are FTP or HTTP. The most common today is HTTP. The host is the computer on which the information is located, although the name of the computer can be an alias. Web pages are usually stored in computers, and computers are given alias names that usually begin with the characters "www". This is not mandatory, however, as the host can be any name given to the computer that hosts the Web page. The URL can optionally contain the port number of the server. If the *port* is included, it is inserted between the host and the path, and it is separated from the host by a colon. Path is the pathname of the file where the information is located. Note that the path can itself contain slashes that, in the UNIX operating system, separate the directories from the subdirectories and files.

WEB DOCUMENTS



Static HTML document

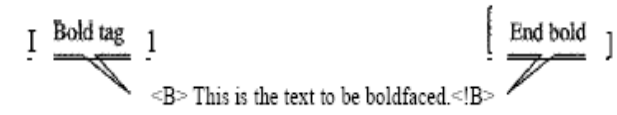
The documents in the WWW can be grouped into three broad categories: static, dynamic, and active. The category is based on the time at which the contents of the document are determined.

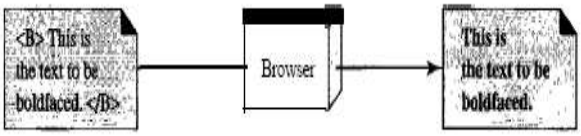
Static Documents

Static documents are fixed-content documents that are created and stored in a server. The client can get only a copy of the document. In other words, the contents of the file are determined when the file is created, not when it is used. Of course, the contents in the server can be changed, but the user cannot change them. When a client accesses the document, a copy of the document is sent. The user can then use a browsing program to display the document

HTML

Hypertext Markup Language (HTML) is a language for creating Web pages. The term *markup language* comes from the book publishing industry. Before a book is typeset and printed, a copy editor reads the manuscript and puts marks on it. These marks tell the compositor how to format the text. For example, if the copy editor wants part of a line to be printed in boldface, he or she draws a wavy line under that part.





The two tags <B> and </B> are instructions for the browser. When the browser sees these two marks, it knows that the text must be boldfaced.

A markup language such as HTML allows us to embed formatting instructions in the file itself. The instructions are included with the text. In this way, any browser can read the instructions and format the text according to the specific workstation. HTML lets us use only ASCII characters for both the main text and formatting instructions. In this way, every computer can receive the whole document as an ASCII document. The main text is the data, and the formatting instructions can be used by the browser to format the data. A Web page is made up of two parts: the head and the body. The head is the first part of a Web page. The head contains the title of the page and other parameters that the browser will use. The actual contents of a page are in the body, which includes the text and the tags. Whereas the text is the actual information contained in a page, the tags define the appearance of the document. Every HTML tag is a name followed by an optional list of attributes, all enclosed between less-than and greater-than symbols « and >).

An attribute, if present, is followed by an equals sign and the value of the attribute. Some tags can be used alone; others must be used in pairs. Those that are used in pairs are called *beginning* and *ending* tags. The beginning tag can have attributes and values and starts with the name of the tag. The ending tag cannot have attributes or values but must have a slash before the name of the tag. The browser makes a decision about the structure of the text based on the tags, which are embedded into the text.

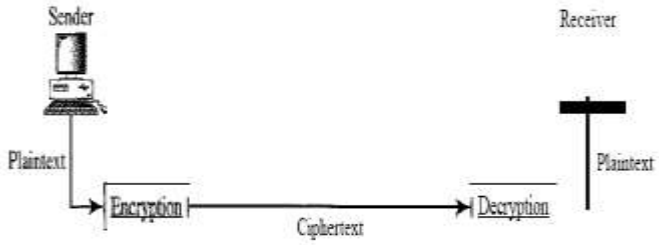
HTML lets us use only ASCII characters for both the main text and formatting instructions. In this way, every computer can receive the whole document as an ASCII document. The main text is the data, and the formatting instructions can be used by the browser to format the data.

A Web page is made up of two parts: the head and the body. The head is the first part of a Web page. The head contains the title of the page and other parameters that the browser will use. The actual contents of a page are in the body, which includes the text and the tags. Whereas the text is the actual information contained in a page, the tags define the appearance of the document. Every HTML tag is a name followed by an optional list of attributes, all enclosed between less-than and greater-than symbols « and >).

An attribute, if present, is followed by an equals sign and the value of the attribute. Some tags can be used alone; others must be used in pairs. Those that are used in pairs are called *beginning* and *ending* tags. The beginning tag can have attributes and values and starts with the name of the tag. The ending tag cannot have attributes or values but must have a slash before the name of the tag. The browser makes a decision about the structure of the text based on the tags, which are embedded into the text.

Cryptography

Cryptography, a word with Greek origins, means "secret writing." However, we use the term to refer to the science and art of transforming messages to make them secure and immune to attacks.



Plaintext and Ciphertext

The original message, before being transformed, is called plaintext. After the message is transformed, it is called ciphertext. An encryption algorithm transforms the plaintext into ciphertext; a decryption algorithm transforms the ciphertext back into plaintext. The sender uses an encryption algorithm, and the receiver uses a decryption algorithm.

Cipher

We refer to encryption and decryption algorithms as ciphers. The term *cipher* is also used to refer to different categories of algorithms in cryptography. This is not to say that every sender-receiver pair needs their very own unique cipher for a secure communication. On the contrary, one cipher can serve millions of communicating pairs.

Key

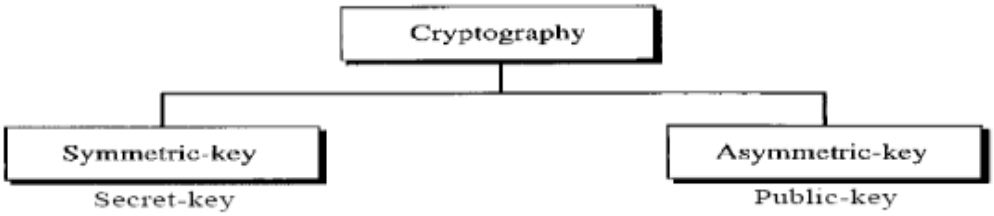
A key is a number (or a set of numbers) that the cipher, as an algorithm, operates on. To encrypt a message, we need an encryption algorithm, an encryption key, and the plaintext. These create the ciphertext. To decrypt a message, we need a decryption algorithm, a decryption key, and the ciphertext. These reveal the original plaintext.

Alice, Bob, and Eve In cryptography, it is customary to use three characters in an information exchange scenario; we use Alice, Bob, and Eve. Alice is the person who needs to send secure data. Bob is the recipient of the data. Eve is the person who somehow disturbs the communication between Alice and Bob by intercepting messages to uncover the data or by sending her own disguised messages. These three names represent computers or processes that actually send or

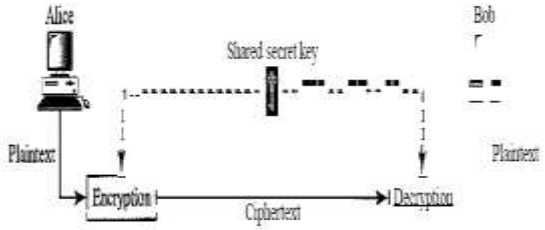
receive data, or intercept or change data.

Two Categories

We can divide all the cryptography algorithms (ciphers) into two groups: symmetrickey (also called secret-key) cryptography algorithms and asymmetric (also called public-key) cryptography algorithms.



Symmetric·Key Cryptography

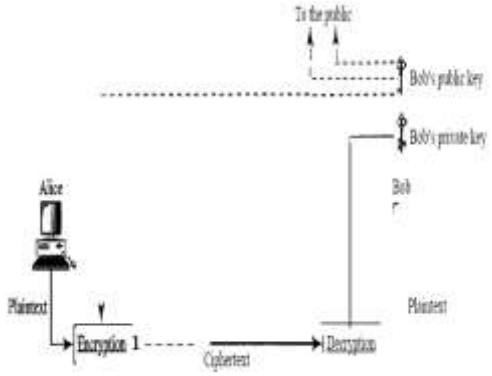


In symmetric-key cryptography, the same key is used by both parties. The sender uses this key and an encryption algorithm to encrypt data; the receiver uses the same key and the corresponding decryption algorithm to decrypt the data

In symmetric·key cryptography, the same key is used by the sender (for encryption) and the receiver (for decryption). The key is shared

Asymmetric-Key Cryptography

In asymmetric or public-key cryptography, there are two keys: a private key and a public key. The private key is kept by the receiver. The public key is announced to the public.

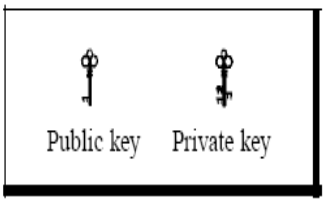


In Figure below, imagine Alice wants to send a message to Bob. Alice uses the public key to encrypt the message. When the message is received by Bob, the private key is used to decrypt the message.

Three Types of Keys

The reader may have noticed that we are dealing with three types of keys in cryptography: the secret key, the public key, and the private key. The first, the secret key, is the shared key used in symmetric-key cryptography. The second and the third are the public and private keys used in asymmetric-key cryptography. We will use three different icons for these keys throughout the book to distinguish one from the others

Symmetric-key cryptography

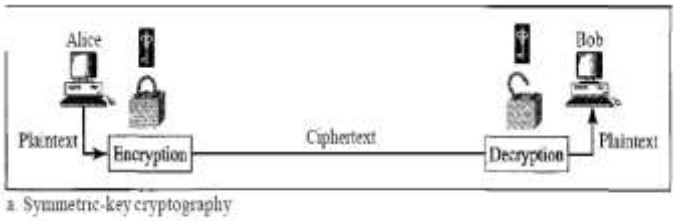


Asymunetric-key cryptography

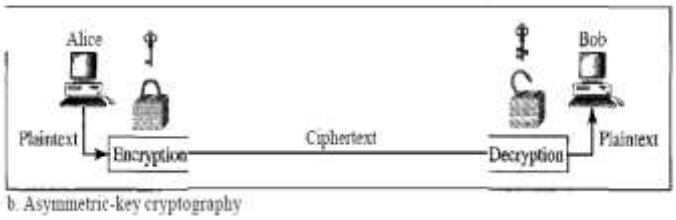
Comparison

Let us compare symmetric-key and asymmetric-key cryptography. Encryption can be thought of as electronic locking; decryption as electronic unlocking. The sender puts the message in a box and locks the box by using a key; the receiver unlocks the box with a key and takes out the message. The difference lies in the mechanism of the locking and unlocking and the type of keys used.

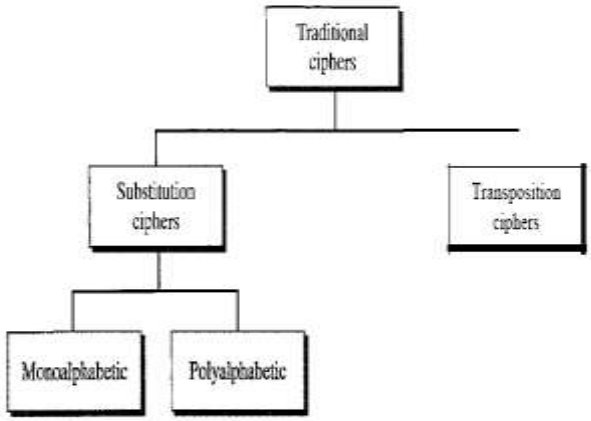
In symmetric-key cryptography, the same key locks and unlocks the box. In asymmetric-key cryptography, one key locks the box, but another key is needed to unlock it.



a. Symmetric-key cryptography



b. Asymmetric-key cryptography



SYMMETRIC-KEY CRYPTOGRAPHY

Symmetric-key cryptography started thousands of years ago when people needed to exchange secrets (for example, in a war).

Traditional Ciphers

We can divide traditional symmetric-key ciphers into two broad categories: substitution ciphers and transposition ciphers

Substitution Cipher

A substitution cipher substitutes one symbol with another. If the symbols in the plaintext are alphabetic characters, we replace one character with another. For example, we can replace character A with D, and character T with Z. If the symbols are digits (0 to 9), we can replace 3 with 7, and 2 with 6. Substitution ciphers can be categorized as either monoalphabetic or polyalphabetic ciphers.

A substitution cipher replaces one symbol with another

In a monoalphabetic cipher, a character (or a symbol) in the plaintext is always changed to the same character (or symbol) in the ciphertext regardless of its position in the text. For example, if the algorithm says that character A in the plaintext is changed to character D, every character A is changed to character D. In other words, the relationship between characters in the plaintext and the ciphertext is a one-to-one relationship.

In a polyalphabetic cipher, each occurrence of a character can have a different substitute. The relationship between a character in the plaintext to a character in the ciphertext is a one-to-many relationship. For example, character A could be changed to D in the beginning of the text, but it could be changed to N at the middle. It is obvious that if the relationship between plaintext characters and ciphertext characters is one-to many, the key must tell us which of the many possible characters can be chosen for encryption. To achieve this goal, we need to divide the text into groups of characters and use a set of keys. For example, we can divide the text "THISISANEASYTASK" into groups of 3 characters and then apply the encryption using a set of 3 keys. We then repeat the procedure for the next 3 characters.

Transposition Ciphers

In a transposition cipher, there is no substitution of characters; instead, their locations change. A character in the first position of the plaintext may appear in the tenth position of the ciphertext. A character in the eighth position may appear in the first position. In other words, a transposition cipher reorders the symbols in a block of symbols

A transposition cipher reorders (permutes) symbols in a block of symbols.

Key In a transposition cipher, the key is a mapping between the position of the symbols in the plaintext and cipher text. For example, the following shows the key using a block of four characters:

Plaintext:

Cipher text:

2 4 1 3

1 2 3 4

In encryption, we move the character at position 2 to position 1, the character at position 4 to position 2, and so on. In decryption, we do the reverse. Note that, to be more effective, the key should be long, which means encryption and decryption of long blocks of data. Figure shows encryption and decryption for our four-characterblock using the above key. The figure shows that the encryption and decryption use the same key. The encryption applies it from downward while decryption applies it upward.

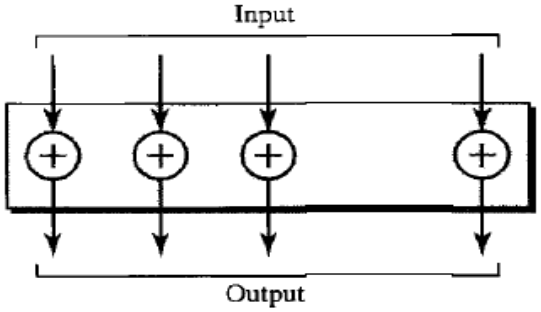
Simple Modern Ciphers

The traditional ciphers we have studied so far are character-oriented. With the advent of the computer, ciphers need to be bit-oriented. This is so because the information to be encrypted is not just text; it can also consist of numbers, graphics, audio, and video data.

It is convenient to convert these types of data into a stream of bits, encrypt the stream, and then send the encrypted stream. In addition, when text is treated at the bit level, each character is replaced by 8 (or 16) bits, which means the number of symbols becomes 8 (or 16). Mingling and mangling bits provides more security than mingling and mangling characters. Modem ciphers use a different strategy than the traditional ones. A modern symmetric cipher is a combination of simple ciphers. In other words, a modern cipher uses several simple ciphers to achieve its goal.

XOR Cipher

Modern ciphers today are normally made of a set of **simple ciphers,** which are simple predefined functions in mathematics or computer science. The first one discussed here is called the **XOR cipher** because it uses the exclusive-or operation as defined in computer science.

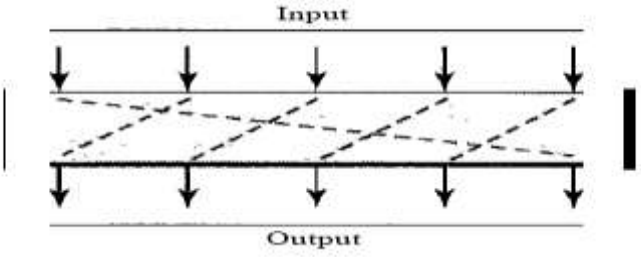


An XOR operation needs two data inputs plaintext, as the first and a key as the second. In other words, one of the inputs is the block to be the encrypted, the other input is a key; the result is the encrypted block. Note that in an XOR cipher, the size of the key, the plaintext, and the ciphertext are all the same. XOR ciphers have a very interesting property: the encryption and decryption are the same.

Rotation Cipher

Another common cipher is the rotation cipher, in which the input bits are rotated to the left or right. The rotation cipher can be keyed or keyless. In keyed rotation, the value of the key defines the number of rotations; in keyless rotation the number of rotations is fixed.

Figure below shows an example of a rotation cipher. Note that the rotation cipher can be considered a special case of the transpositional cipher using bits instead of characters.



The rotation cipher has an interesting property. If the length of the original stream is *N*, after *N* rotations, we get the original input stream. This means that it is useless to apply more than *N* - 1 rotation. In other words, the number of rotations must be between 1 and *N-1*.

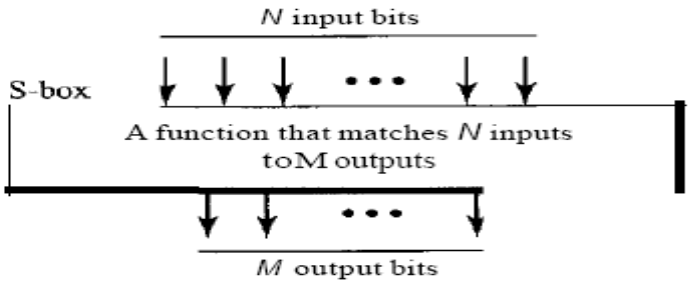
The decryption algorithm for the rotation cipher uses the same key and the opposite rotation direction. If we use a right rotation in the encryption, we use a left rotation in decryption and vice versa.

Substitution Cipher: S-box

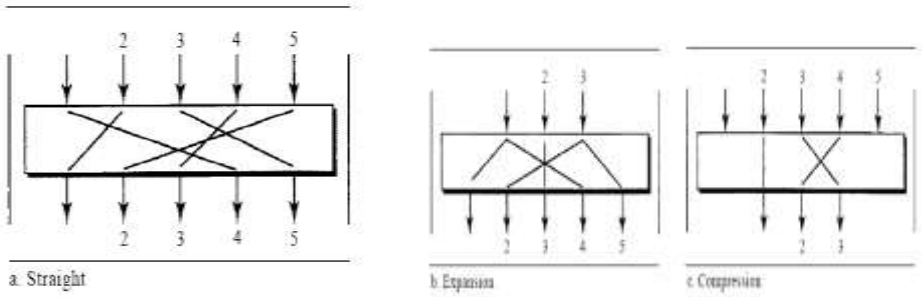
An S-box (substitution box) parallels the traditional substitution cipher for characters. The input to an S-box is a stream of bits with length *N;* the result is another stream of bits with length *M.* And N and *M* are not necessarily the same. Figure shows an S-box. The S-box is normally keyless and is used as an intermediate stage of encryption or decryption. The function that matches the input to the output may be defined mathematically or by a table.

Transposition Cipher: P-box

A P-box (permutation box) for bits parallels the traditional transposition cipher for characters.



It performs a transposition at the bit level; it transposes bits. It can be implemented in software or hardware, but hardware is faster. P-boxes, like S-boxes, are normally keyless. We can have three types of permutations in P-boxes: the **straight permutation, expansion permutation, and compression permutation** as shown in Figure



A straight permutation cipher or a straight P-box has the same number of inputs as outputs. In other words, if the number of inputs is *N,* the number of outputs is also *N.* In an expansion permutation cipher, the number of output ports is greater than the number of n put ports. In a compression permutation cipher, the number of output ports is less than the number of input ports.

Modern Round Ciphers

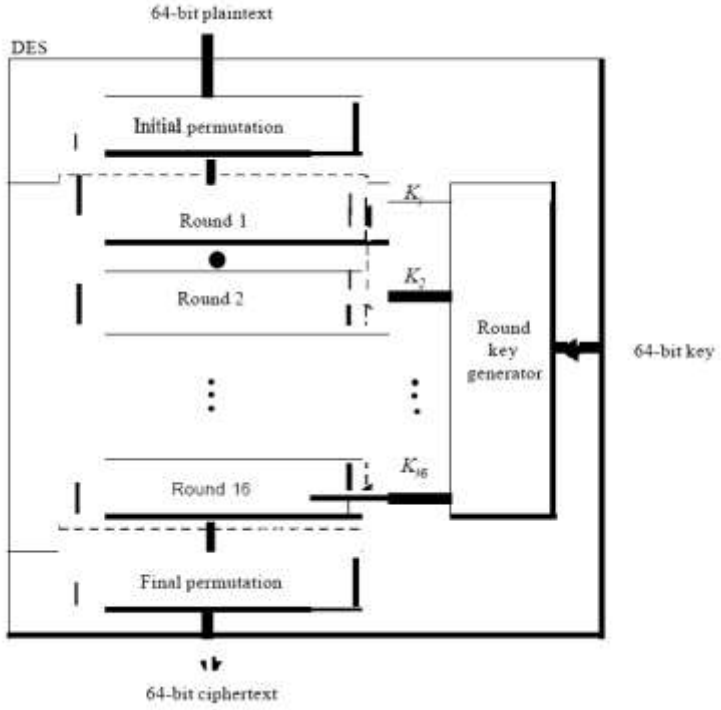
The ciphers of today are called **round ciphers** because they involve multiple **rounds,** where each round is a complex cipher made up of the simple ciphers that we previously described. The key used in each round is a subset or variation of the general key called the round key. If the cipher has *N* rounds, a key generator produces *N* keys, *Kb Kz, ..., KN,* where K1 is used in round 1, *K2* in round 2, and so on.

In this section, we introduce two modem symmetric-key ciphers: DES and AES.

These ciphers are referred to as block ciphers because they divide the plaintext into blocks and use the same key to encrypt and decrypt the blocks. DES has been the de facto standard until recently. AES is the formal standard now.

Data Encryption Standard (DES)

One example of a complex block cipher is the Data Encryption Standard (DES). DES was designed by IBM and adopted by the U.S. government as the standard encryption method for non-military and non classified use. The algorithm encrypts a 64-bit plaintext block using a 64-bit key, as shown in Figure



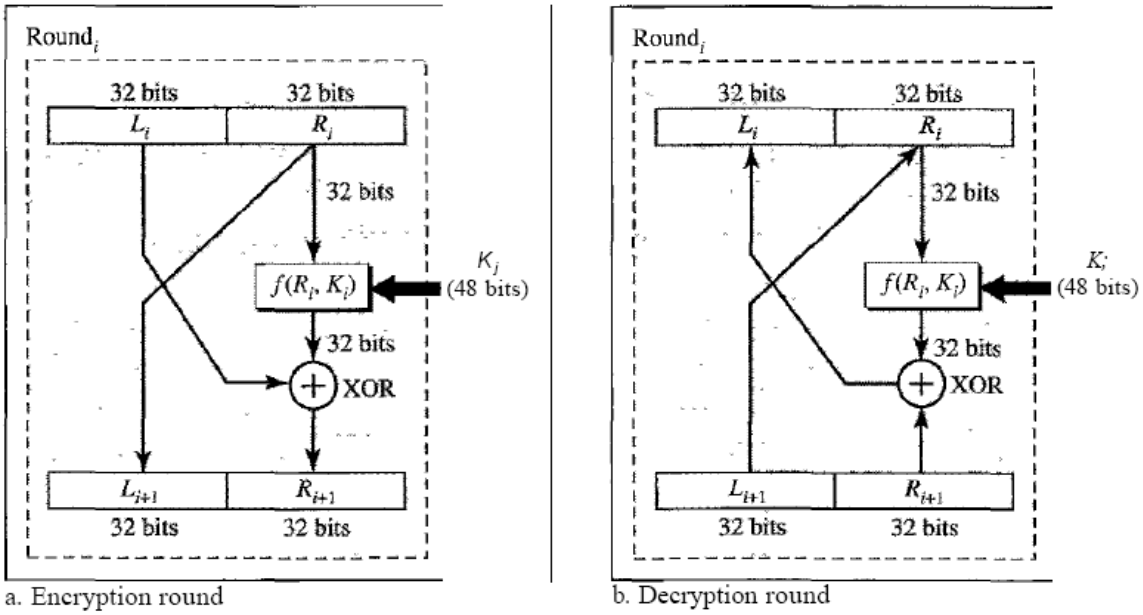
DES has two transposition blocks (P-boxes) and 16 complex round ciphers (they are repeated). Although the 16 iteration round ciphers are conceptually the same, each uses a different key derived from the original key.

The initial and final permutations are keyless straight permutations that are the inverse of each other. The permutation takes a 64-bit input and permutes them according to predefined values.

Each round of DES is a complex round cipher, as shown in Figure below. Note that the structure of the encryption round ciphers is different from that of the decryption one.

DES Function

The heart of DES is the **DES function.** The DES function applies a 48-bit key to the rightmost 32 bits *Ri* to produce a 32-bit output. This function is made up of four operations: an XOR, an expansion permutation, a group of S-boxes, and a straight permutation



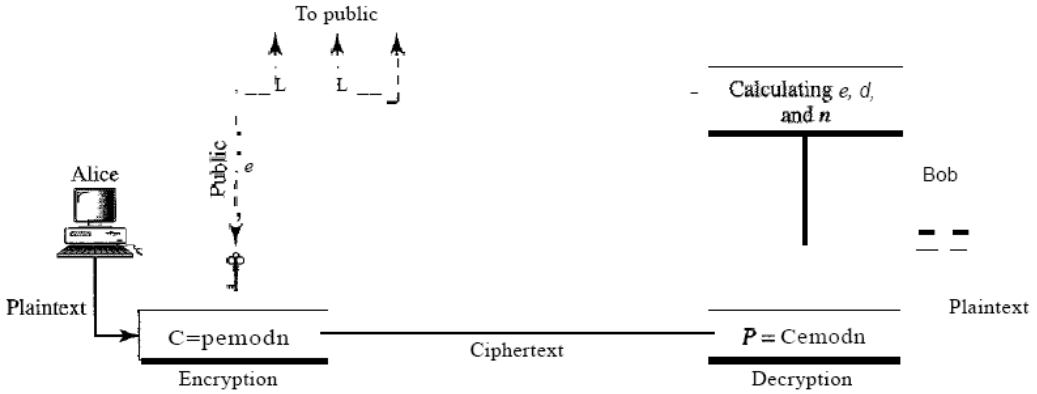
a. Encryption round b. Decryption round

ASYMMETRIC-KEY CRYPTOGRAPHY

An asymmetric-key (or public-key) cipher uses two keys: one private and one public. We discuss two algorithms: RSA and Diffie-Hellman.

RSA

The most common public key algorithm is RSA, named for its inventors Rivest, Shamir, and Adleman (RSA). It uses two numbers, e and d, as the public and private keys.



The two keys, *e* and *d,* have a special relationship to each other, a discussion of this relationship is beyond the scope of this book. We just show how to calculate the keyswithout proof.

Selecting Keys

Bob use the following steps to select the private and public keys:

1. Bob chooses two very large prime numbers *p* and *q.* Remember that a prime number is one that can be divided evenly only by 1 and itself.
2. Bob multiplies the above two primes to find *n,* the modulus for encryption and decryption. In other words, *n* ::: *p* X *q.*
3. Bob calculates another number <1> ::: *(p* -1) X *(q* - 1).
4. Bob chooses a random integer *e.* He then calculates *d* so that *d* x *e::* 1 mod <1>.
5. Bob announces *e* and *n* to the public; he keeps <1> and *d* secret.

Encryption

Anyone who needs to send a message to Bob can use nand *e.* For example, if Alice needs to send a message to Bob, she can change the message, usually a short one, to an integer. This is the plaintext. She then calculates the ciphertext, using *e* and *n.*

C=pt!(modn)

Alice sends C, the ciphertext, to Bob.

Decryption

Bob keeps <p and *d* private. When he receives the ciphertext, he uses his private key *d* to decrypt the message:

P= Cd(modn)

Restriction

For RSA to work, the value of *P* must be less than the value of *n.* If*P* is a large number, the plaintext needs to be divided into blocks to make *P* less than *n.*

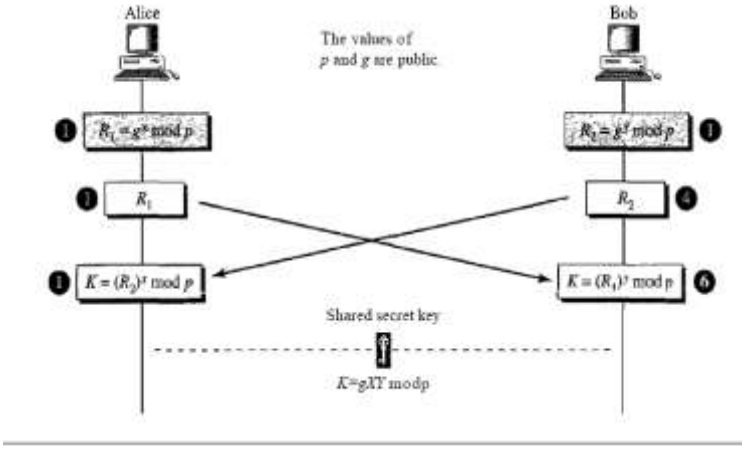
Diffie-Hellman

RSA is a public-key cryptosystem that is often used to encrypt and decrypt symmetric keys. Diffie-Hellman, on the other hand, was originally designed for key exchange. In the

Diffie-Hellman cryptosystem, two parties create a symmetric session key to exchange data without having to remember or store the key for future use. They do not have to meet to agree on the key; it can be done through the Internet. Let us see how the protocol works when Alice and Bob need a symmetric key to communicate. Before establishing a symmetric key, the two parties need to choose two numbers *p* and *g.* The first number, *p,* is a large prime number on the order of 300 decimal digits (1024 bits). The second number is a random number. These two numbers need not be confidential. They can be sent through the Internet; they can be public.

Procedure

Figure below shows the procedure. The steps are as follows:

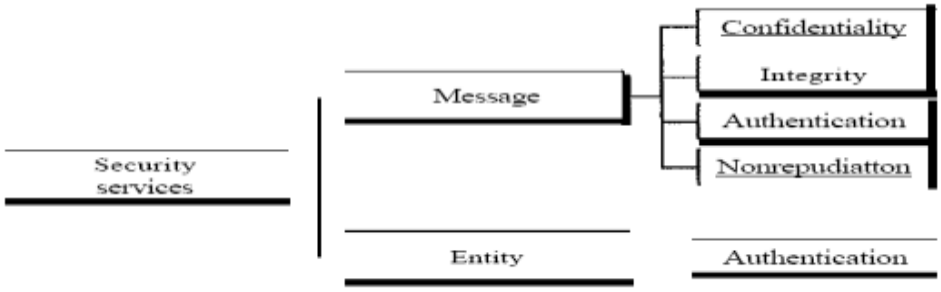


Step 1: Alice chooses a large random number *x* and calculates *R*1=*If* mod *p*.
o Step 2: Bob chooses another large random number *y* and calculates *R2 = gY* mod *p.*
o Step 3: Alice sends *R*1 to Bob. Note that Alice does not send the value of *x;* she sends only *R1-*
o Step 4: Bob sends *R2* to Alice. Again, note that Bob does not send the value of *y,* he sends only *R2.*
o Step 5: Alice calculates *K = (R2l* mod *p.*
o Step 6: Bob also calculates *K = (R1?* mod *p.*
The symmetric key for the session is *K.*
(.f mod *p)Y* mod *p =(gY* mod *p)X* mod *p =.fY* mod *p*
Bob has calculated *K = (R 1?* mod *p =(If* mod *p?* mod *p = lfY* mod *p.* Alice has calculated *K =(R2)X* mod *p =(gY* mod *p)X* mod *=lfY* mod *p.* Both have reached the same value without Bob knowing the value of *x* and without Alice knowing the value of *y.*

SECURITY SERVICES

Security Requirements

- **confidentiality** - protect data content/access .Requires that data only be accessible by authorized parties. This type of access includes printing, displaying, and other forms of disclosure, including simply revealing the existence of an object.
- **integrity** - protect data accuracy. Requires that only authorized parties can modify data. Modification includes writing, changing, changing status, deleting, and creating.
- **availability -** ensure timely service. Requires that data are available to authorized parties**.**
- **authenticity** - protect data origin. Requires that a host or service be able to verify the identity of a user.



Passive Attacks

- A useful means of classifying security attacks (RFC 2828) is in terms of *passive attacks* and *active attacks*. A passive attack attempts to learn or make use of information from the system but does not affect system resources. An active attack attempts to alter system resources or affect their operation.

- Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmitted. Two types of passive attacks are release of message contents (which may contain sensitive or confidential information), and traffic analysis which is subtler. Even with encryption protecting message contents, an opponent might still be able to observe the pattern of these messages. The opponent could determine the location and identity of communicating hosts and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of the communication that was taking place.
- Passive attacks are very difficult to detect because they do not involve any alteration of the data. Typically, the message traffic is sent and received in an apparently normal fashion and neither the sender nor receiver is aware that a third party has read the messages or observed the traffic pattern. However, it is feasible to prevent the success of these attacks, usually by means of encryption. Thus, the emphasis in dealing with passive attacks is on prevention rather than detection.

Active Attacks

Active attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories: masquerade, replay, modification of messages, and denial of service.

- Masquerade attacks take place when one entity pretends to be a different entity. A masquerade attack usually includes some other forms of active attack.
- Replay involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.
- Modification of messages simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect.
- The denial of service prevents or inhibits the normal use or management of communications facilities. This attack may have a specific target. Another form of service denial is the disruption of an entire network or a server.

Active attacks present the opposite characteristics of passive attacks. Whereas passive attacks are difficult to detect, measures are available to prevent their success. On the other hand, it is quite difficult to prevent active attacks absolutely, because to do so would require physical protection of all communications facilities and paths at all times. Instead, the goal is to detect them and to recover from any disruption or delays caused by them. Because the detection has a deterrent effect, it may also contribute to prevention**.**

Data Encryption Standard

DES has been the dominant encryption algorithm since its introduction in 1977. However, because DES uses only a 56-bit key, it was only a matter of time before computer processing speed made DES obsolete. In 1998, the Electronic Frontier Foundation (EFF) announced that it had broken a DES challenge using a special-purpose "DES cracker" machine that was built for less than $250,000. The attack took less than three days. The EFF has published a detailed description of the machine, enabling others to build their own cracker. And, of course, hardware prices will continue to drop as speeds increase, making DES worthless.

Note

- **US standard**
- **64 bit plain text blocks**
- **56 bit key**
- **broken in 1998 by Electronic Frontier Foundation**
  - **special purpose US$250,000 machine**
  - **with detailed published description**

- **less than three days**
- **DES now worthless**

Triple DES

The life of DES was extended by the use of triple DES (3DES), which involves repeating the basic DES algorithm three times, using either two or three unique keys, for a key size of 112 or 168 bits. The principal drawback of 3DES is that the algorithm is relatively sluggish in software. A secondary drawback is that both DES and 3DES use a 64-bit block size. For reasons of both efficiency and security, a larger block size is desirable.

Note

- **ANSI X9.17 (1985)**
- **incorporated in DEA standard 1999**
- **uses 2 or 3 keys**
- **3 executions of DES algorithm**
- **effective key length 112 or 168 bit**
- **slow**
- **block size (64 bit) now too small**

Advanced Encryption Standard

- NIST issued call for proposals for an Advanced Encryption Standard (AES) in 1997
  - security strength equal to or better than 3DES
  - significantly improved efficiency
  - symmetric block cipher with block length 128 bits
  - key lengths 128, 192, and 256 bits
  - evaluation include security, computational efficiency, memory requirements, hardware and software suitability, and flexibility
  - AES issued as FIPS 197 in 2001

AES Description

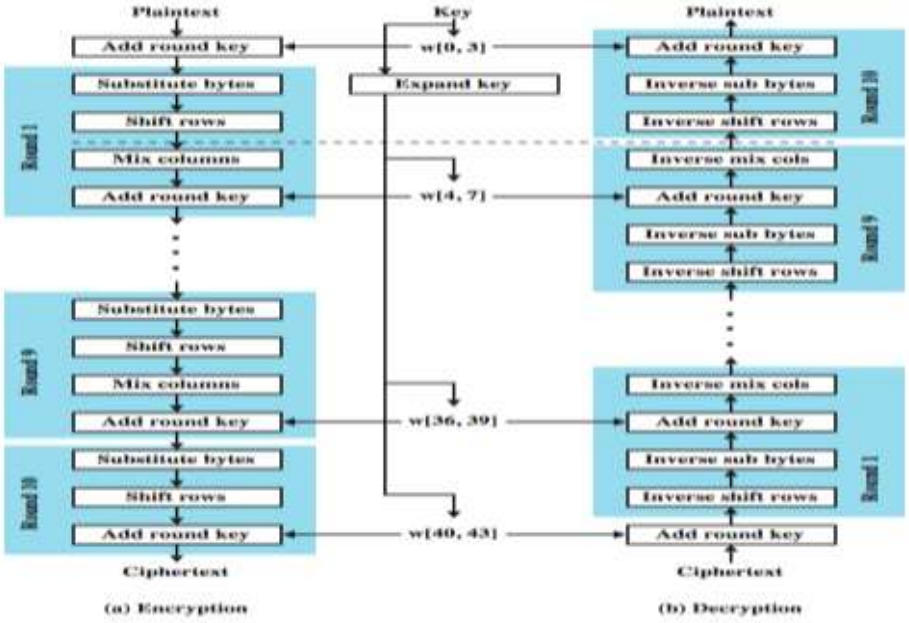
- **assume key length 128 bits**
- **input a 128-bit block (square matrix of bytes)**
  - **copied into state array, modified at each stage**
  - **after final stage, state copied to output**
- **128-bit key (square matrix of bytes)**
  - **expanded into array of 44 32-bit key schedule words**
- **byte ordering by column**
  - **1st 4 bytes of 128-bit input occupy 1st column**
  - **1st 4 bytes of expanded key occupy 1st column**

AES Encryption and Decryption

Stallings DCC8e Figure shows the overall structure of AES. The following comments give some insight into AES:

1. The key that is provided as input is expanded into an array of forty-four 32-bit words. Four distinct words (128 bits) serve as a round key for each round.
2. Four different stages are used, one of permutation and three of substitution:
   - Substitute bytes: Uses a table, referred to as an S-box, to perform a byte-by-byte substitution of the block
   - Shift rows: A simple permutation that is performed row by row
   - Mix columns: A substitution that alters each byte in a column as a function of all of the bytes in the column
   - Add round key: A simple bitwise XOR of the current block with a portion of the expanded key
3. The structure is quite simple. For both encryption and decryption, the cipher begins with an Add

Round Key stage, followed by nine rounds that each includes all four stages, followed by a tenth round of three stages. Figure depicts the structure of a full encryption round.
4. Only the Add Round Key stage makes use of the key. For this reason, the cipher begins and ends with an Add Round Key stage. Any other stage, applied at the beginning or end, is reversible without knowledge of the key and so would add no security.



AES Encryption Round

5. The Add Round Key stage by itself would not be formidable. The other three stages together scramble the bits, but by themselves would provide no security because they do not use the key. We can view the cipher as alternating operations of XOR encryption (Add Round Key) of a block, followed by scrambling of the block (the other three stages), followed by XOR encryption, and so on. This scheme is both efficient and highly secure.
6. Each stage is easily reversible. For the Substitute Byte, Shift Row, and Mix Columns stages, an inverse function is used in the decryption algorithm. For the Add Round Key stage, XOR is its own inverse.
7. As with most block ciphers, the decryption algorithm makes use of the expanded key in reverse order. However, the decryption algorithm is not identical to the encryption algorithm. This is a consequence of the particular structure of AES.
8. Once it is established that all four stages are reversible, it is easy to verify that decryption does recover the plaintext. Figure lays out encryption and decryption going in opposite vertical directions. At each horizontal point State is the same for both encryption and decryption.
9. The final round of both encryption and decryption consists of only three stages. Again, this is a consequence of the particular structure of AES and is required to make the cipher reversible.

Location of Encryption Devices

The most powerful, and most common, approach to countering the threats to network security is encryption. In using encryption, we need to decide what to encrypt and where the encryption gear should be located. As Figure above indicates, there are two fundamental alternatives: link encryption and end-to-end encryption.

Link Encryption

With link encryption, each vulnerable communications link is equipped on both ends with an encryption device. Thus, all traffic over all communications links is secured. Although this requires a lot of encryption devices in a large network, it provides a high level of security. One disadvantage

of this approach is that the message must be decrypted each time it enters a packet switch; this is necessary because the switch must read the address (virtual circuit number) in the packet header to route the packet. Thus, the message is vulnerable at each switch. If this is a public packet-switching network, the user has no control over the security of the nodes.

- each communication link equipped at both ends
- all traffic secure
- high level of security
- requires lots of encryption devices
- message must be decrypted at each switch to read address (virtual circuit number)
- security vulnerable at switches
  - particularly on public switched network

End to End Encryption

With end-to-end encryption, the encryption process is carried out at the two end systems. The source host or terminal encrypts the data. The data, in encrypted form, are then transmitted unaltered across the network to the destination terminal or host. The destination shares a key with the source and so is able to decrypt the data. This approach would seem to secure the transmission against attacks on the network links or switches. There is, however, still a weak spot. The host may only encrypt the user data portion of the packet and must leave the header in the clear, so that the switching nodes in the network can read it in order to route the packet to its destination. Thus, with end-to-end encryption, the user data are secure. However, the traffic pattern is not, because packet headers are transmitted in the clear.

Message Authentication

Encryption protects against passive attack (eavesdropping). A different requirement is to protect against active attack (falsification of data and transactions). Protection against such attacks is known as message authentication which allows communicating parties to verify that received messages are authentic. The two important aspects are to verify that the contents of the message have not been altered and that the source is authentic. We may also wish to verify a message's timeliness (it has not been artificially delayed and replayed) and sequence relative to other messages flowing between two parties.

- protection against active attacks with
  - falsification of data
  - falsification of source
- authentication allows receiver to verify that message is authentic
  - has not been altered
  - is from claimed/authentic source
  - timeliness

Authentication Using Symmetric Encryption

It is possible to perform authentication simply by the use of symmetric encryption. If we assume that only the sender and receiver share a key (which is as it should be), then only the genuine sender would be able successfully to encrypt a message for the other participant. Furthermore, if the message includes an error-detection code and a sequence number, the receiver is assured that no alterations have been made and that sequencing is proper. If the message also includes a timestamp, the receiver is assured that the message has not been delayed beyond that normally expected for network transit.

Authentication Without Encryption

- authentication tag generated and appended to each message
- message not encrypted
- useful when don’t want encryption because:
  - messages broadcast to multiple destinations

- have one destination responsible for authentication
- one side heavily loaded
  - encryption adds to workload
  - can authenticate random messages
- programs authenticated without encryption can be executed without decoding

Secure Hash Functions

- produce a "fingerprint" of message/file
- must have the following properties:
  - can be applied to any size data block
  - produce fixed length output
  - easy to compute
  - not feasible to reverse
  - not feasible to find two messages with the same hash
- giving "weak" & "strong" hash functions
- also used for data integrity

Secure Hash Algorithm

The Secure Hash Algorithm (SHA) was developed by NIST and published as a federal information processing standard (FIPS 180) in 1993; a revised version was issued as FIPS 180-1 in 1995 and is generally referred to as SHA-1. SHA-1 produces a hash value of 160 bits. In 2002, NIST produced a new version of the standard, FIPS 180-2, that defined three new versions of SHA, with hash value lengths of 256, 384, and 512 bits, known as SHA-256, SHA-384, and SHA-512. These new versions have the same underlying structure and use the same types of modular arithmetic and logical binary operations as SHA-1. In 2005, NIST announced the intention to phase out approval of SHA-1 and move to a reliance on the other SHA versions by 2010. Shortly thereafter, a research team described an attack in which two separate messages could be found that deliver the same SHA-1 hash using 2^{69} operations, far fewer than the 2^{80} operations previously thought needed to find a collision with an SHA-1 hash. This result should hasten the transition to the other versions of SHA. The SHA-512 algorithm takes as input a message with a maximum length of less than 2^{128} bits and produces as output a 512-bit message digest. The input is processed in 1024-bit blocks.

- **Secure Hash Algorithm (SHA)**
  - **SHA defined in FIPS 180 (1993), 160-bit hash**
  - **SHA-1 defined in FIPS 180-1 (1995)**
  - **SHA-256, SHA-384, SHA-512 defined in FIPS 180-2 (2002), 256/384/512-bit hashes**
- **SHA-1 being phased out, attack known**
- **SHA-512 processes input message**
  - **with total size less than 2^{128} bits**
  - **in 1024 bit blocks**
  - **to produce a 512-bit digest**

Digital Signatures

Public-key encryption can be used in another way, as illustrated in Stallings DCC8e. Suppose that Bob wants to send a message to Alice and, although it is not important that the message be kept secret, he wants Alice to be certain that the message is indeed from him. In this case Bob uses his own private key to encrypt the message. When Alice receives the ciphertext, she finds that she can decrypt it with Bob's public key, thus proving that the message must have been encrypted by Bob. No one else has Bob's private key and therefore no one else could have created a ciphertext that could be decrypted with Bob's public key. Therefore, the entire encrypted message serves as a digital signature. In addition, it is impossible to alter the message without access to Bob's private key, so the message is authenticated both in terms of source and in terms of data integrity.

- **sender encrypts message with private key**

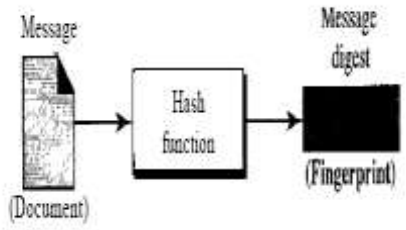
- **receiver decrypts with senders public key**
- **authenticates sender does not give privacy of data must send both original and encrypted copies more efficient to sign authenticator**
- **a secure hash of message send signed hash with message**

MESSAGE INTEGRITY

- Encryption and decryption provide secrecy, or confidentiality, but not **integrity.** However, on occasion we may not even need secrecy, but instead must have integrity. For example, Alice may write a will to distribute her estate upon her death. The will does not need to be encrypted. After her death, anyone can examine the will. The integrity of the will, however, needs to be preserved. Alice does not want the contents of the will tobe changed. As another example, suppose Alice sends a message instructing her banker,
- Bob, to pay Eve for consulting work. The message does not need to be hidden from Eve because she already knows she is to be paid. However, the message does need to be safe from any tampering, especially by Eve.

Message and Message Digest

The electronic equivalent of the document and fingerprint pair is the message and message digest pail: To preserve the integrity of a message, the message is passed through an algorithm called a hash function. The hash function creates a compressed image of the message that can be used as a fingerprint. Figure below shows the message, hash function, and the message digest.



Difference

The two pairs document/fingerprint and message/message digest are similar, with some differences. The document and fingerprint are physically linked together; also, neither needs to be kept secret. The message and message digest can be unlinked (or sent) separately and, most importantly, the message digest needs to be kept secret. The message digest is either kept secret in a safe place or encrypted if we need to send it through a communications channel.

Creating and Checking the Digest

The message digest is created at the sender site and is sent with the message to the receiver. To check the integrity of a message, or document, the receiver creates the hash function again and compares the new message digest with the one received. If both are the same, the receiver is sure that the original message has not been changed. Of course, we are assuming that the digest has been sent secretly.

Hash Function Criteria

To be eligible for a hash, a function needs to meet three criteria: one-wayness, resistance to weak collision, and resistance to strong collision

One-way ness

A hash function must have **one-way ness;** a message digest is created by a one-way hashing function. We must not be able to recreate the message from the digest. Sometimes it is difficult to make a hash function 100 percent one-way; the criteria state that it must be extremely difficult or impossible to create the message if the message digest is given. This is similar to the document/fingerprint case. No one can make a document from a fingerprint

Questions	opt1	opt2	opt3
Data communication means exchange of data between _____devices.	one	two	six
The system must deliver data to the correct destination is called_____	accuracy	jitter	delivery
A_____ is the set of rules.	protocols	transmission medium	networks
In_____, the communication is unidirection.	duplex mode	full duplex mode	half duplex mode
A_____is a set of devices connected by communication links.	protocols	networks	computer
A_____connection provides a dedicated link between two devices.	point-to-point	multi-point	mesh
One long cable acts as a _____to link all the devices in a network.	bus	mesh	hub
MAN stands for _____	metropolitician area network	metropolitan area network	metropolitical area network
The term timing refers to _____ characteristics.	two	three	four
_____standards are often established originally by manufactures.	de jure	de facto	de fact
In physical layer we can transfer data into _____	frame	packet	bit
Hob to hob delivery is done by the _____	session layer	datalink layer	network layer
The _____layer is responsible for process to process delivery.	physical	presentation	networks
The _____layer is responsible for dialog control and synchronization.	transport	session	application
Tcp/Ip is a _____protocol.	hyper text	transfer	internet
Ip is a_____protocol.	hop to hop	node to node	process to process
A set of devices connected by a _____links	data	networks	communication
Bus topology has a long link called_____	backbone	hub	host
Periodic analog signals can be classified into _____	simple	composite	simple or composite
Period and frequency has the following formula.	f=1/t and t=1/f	t=1/f or f=1/t	c=t/f
Wavelength is_____	propagation speed	propagation speed * frequency	propagation speed/period

Composite signal can be classified into _____types	five	three	four
The range of frequency contained in a _____ signal is its bandwidth.	simple	composite	periodic
The bandwidth of the composite signal is the difference between the _____	highest	highest or lowest	highest and lowest
The _____is the number of bits sent in a second.	bit length	bandpass	bandwidth
Bit length is _____	propagation speed/period	propagation speed * frequency	bit
A_____signal is a composite analog signal with an infinite bandwidth	simple	composite	digital
Decibel (dB) =_____	10 log10 p2/p1	p1/p2	10 log10 p1/p2
Transmission time=_____	message size/birate	distance/bandwidth	message size/distance
_____and star is a point to point device.	bus	ring	mesh
Protocols can be classified into _____ key elements	one	three	four
_____is a basic key element.	protocols	standards	topology
Bit rate=_____	4*BW*log2L	2*BW*log2L	4*BW/L
OSI stands for_____	open systems interconnection	open system internetworking	open symantic interconnection
Net work layer delivers data in the form of_____	frame	bits	data
Session layer provides_____ services.	one	two	three
UDP _____	user data protocol	user datagram protocol	user defined protocol
FTP_____	file transmit protocol	file transmission protocol	file transfer protocol
SMTP_____	single mail transfer protocol	simple mail transfer protocol	simple mail transmission protocol
Complete a cycle is called as _____	period	frequency	non periodic
Jitter is a form of_____	frames	bits	packets
Each set is called a _____	node	code	unicode
Full duplex also called as_____	simple duplex	single duplex	multiple duplex

_____can be measured in transmit time and response time.	performance	frequency	period
A multipoint is also called as_____	multi line	multi drop	multi level
Mesh topology we need _____	n(n-1)	n(n+1)	n(n+1)/2
A_____topology on the other hand is multipoint.	star	ring	bus
A_____can be hybrid	physical	networks	data
A MAN is a network with a size between a _____ and _____.	WAN and LAN	WAN or LAN	LAN
When Two or more networks are connected they become an _____	network	inter network	internet connection
The_____layer is responsible for providing services to the user.	presentation	datalink	application
The _____ layer is responsible for translation, compression encryption.	transport	data link	presentation
The_____layer is responsible for the delivery of a message from one process to another.	data link	transport	presentation
A _____layer is responsible for the delivery of packets from the source to destination.	physical	data link	network
The _____layer is responsible for moving frames from one hop to the next.	data link	physical	network
The _____layer is responsible for movements of bits from one hop to next.	data link	physical	transport
RARP _____	reverse address resolution protocol	reverse address result protocol	reverse addess revolutinized protocol
_____does not define any specific protocol.	TCP	HTTP	TCP/IP
The TCP/IP protocol suite was developed prior to the_____model.	OSI	ISO	TCP
The _____layer is responsible for flow control.	session	presentation	application
The term _____ data refers to information continous	analog	digital	physical

The sine wave is the most fundamental form of a _____analog signal.	composite	single	periodic

opt4	opt5	opt6
four		
timeliness		
ip		
simplex mode		
printer		
physical		
backbone		
macro area network		
six		
semantics		
sp du		
transport layer		
transport		
presentation		
hierarchical		
host to host		
application		
hop		
simple and composite		
t=c/f		
propagation speed/frequency		

two		
non periodic		
lowest		
bit rate		
propagation speed*bit duration		
analog		
2log10 p1/p2		
message size/bandwidth		
physical		
two		
protocols and standards		
2*BW*log 4L		
open system internet		
packet		
four		
user dataframe protocol		
flip transfer protocol		
single mail transmit protocol		
periodic		
dp tu		
polar		
duplex		

non period		
single level		
n(n-1)/2		
mesh		
link		
WAN		
interconnection		
network		
application		
network		
session		
presentation		
session		
reverse addess research protocol		
SMTP		
IP		
transport		
analog and digital		

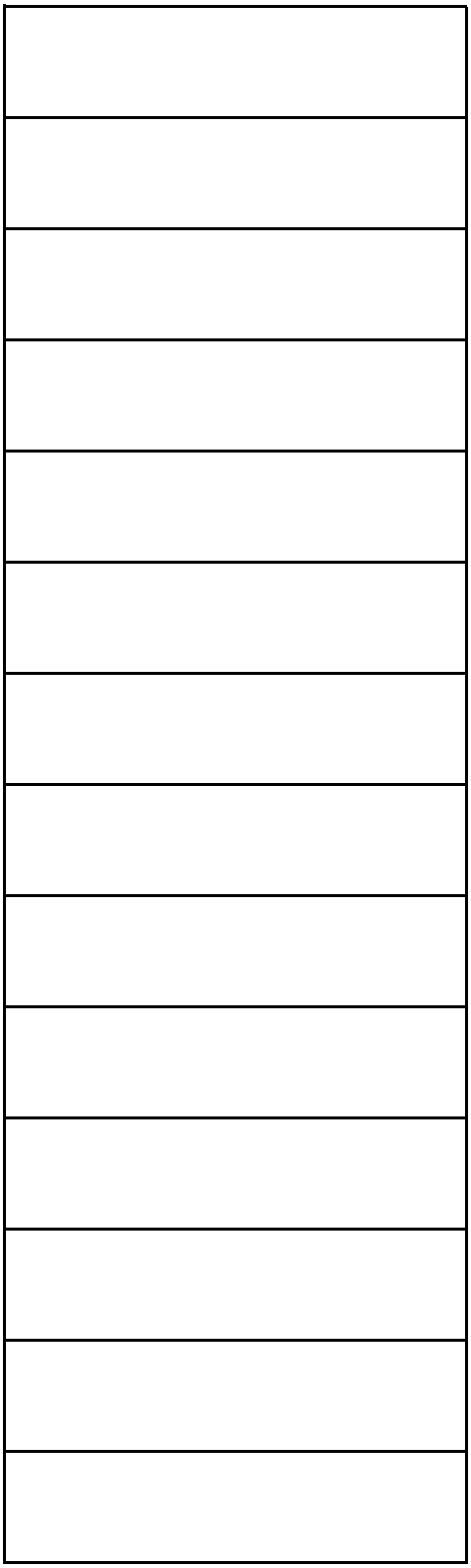
non periodic		

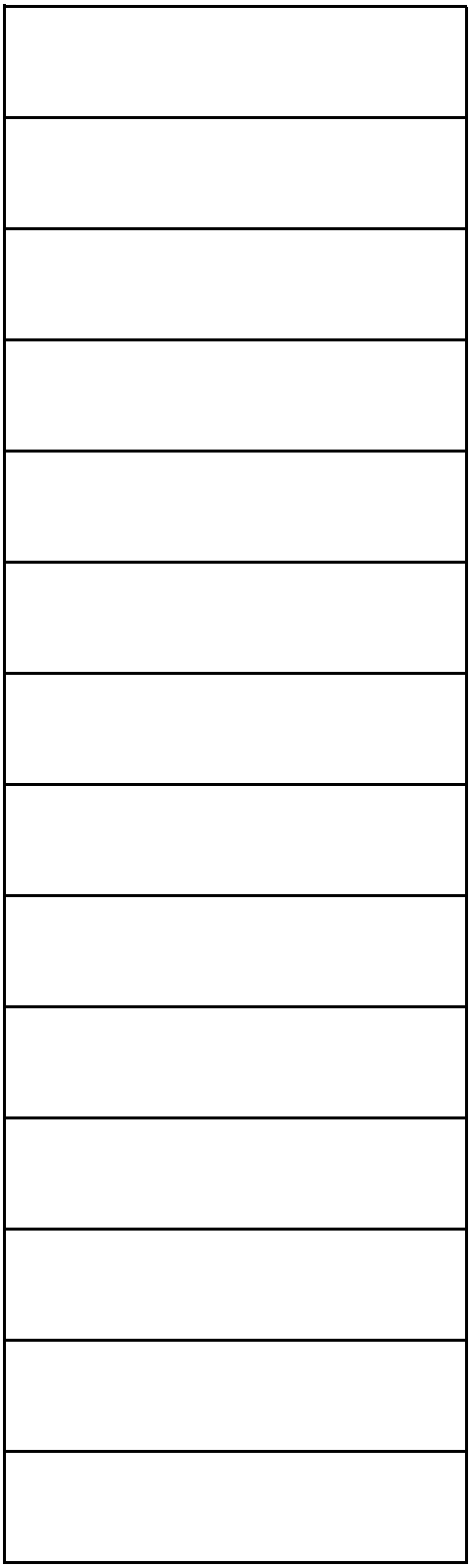
Answer
two
delivery
protocols
simplex mode
networks
point-to-point
backbone
metropolitan area network
two
de facto
bit
datalink layer
transport
session
hierarchical
host to host
communication
backbone
simple or composite
f=1/t and t=1/f
propagation speed/frequency

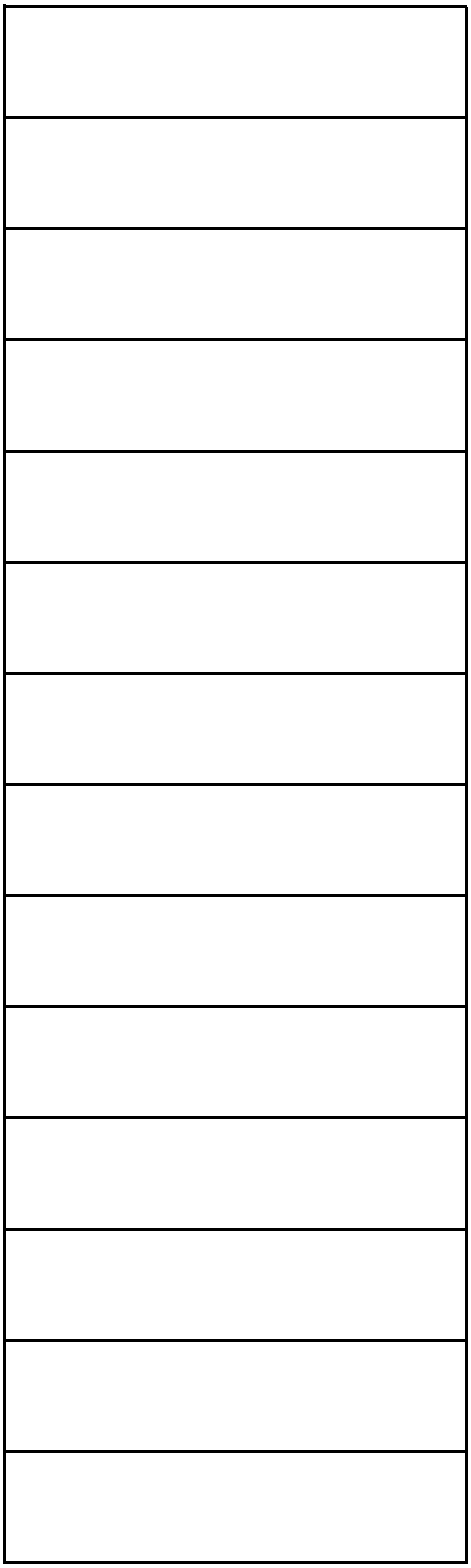
two
composite
highest and lowest
bit rate
propagation speed*bit duration
digital
10 log10 p2/p1
message size/bandwidth
mesh
three
protocols and standards
2*BW*log2L
open systems interconnection
packet
two
user datagram protocol
file transfer protocol
simple mail transfer protocol
period
packets
node
duplex

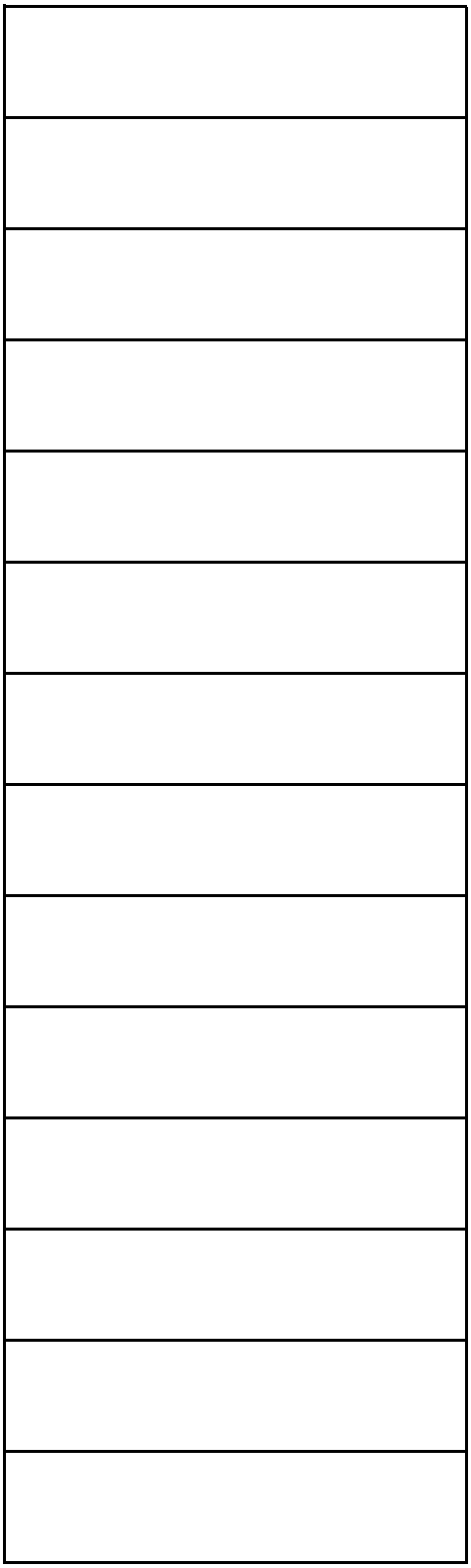
performance
multi drop
n(n-1)/2
bus
networks
WAN and LAN
inter network
application
presentation
transport
network
data link
physical
reverse address resolution protocol
TCP/IP
OSI
transport
analog

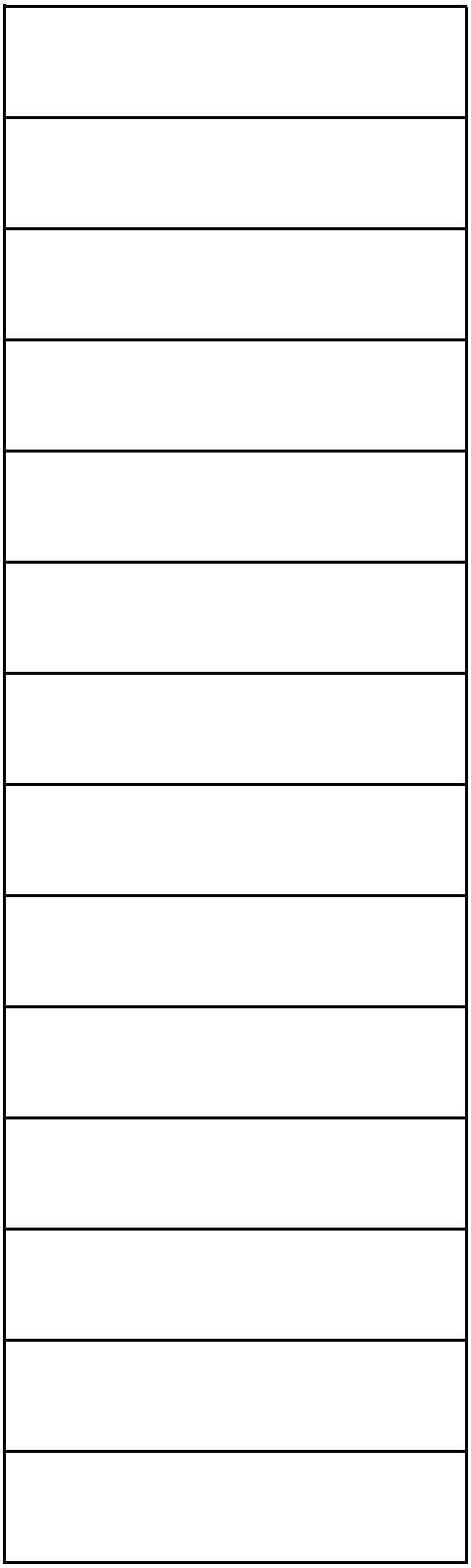
periodic

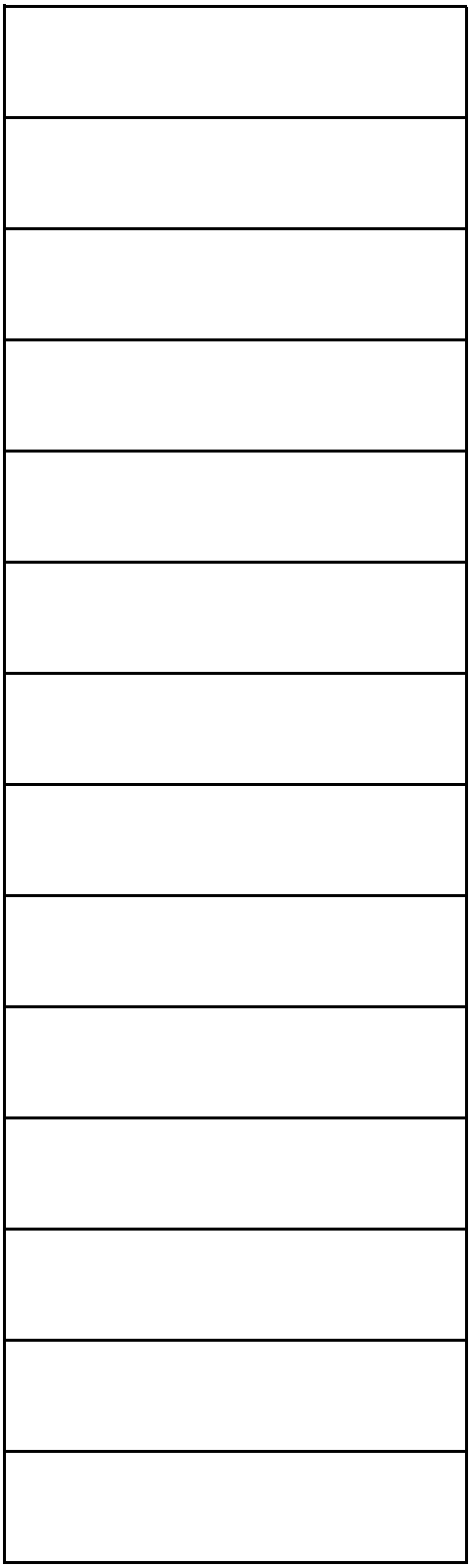


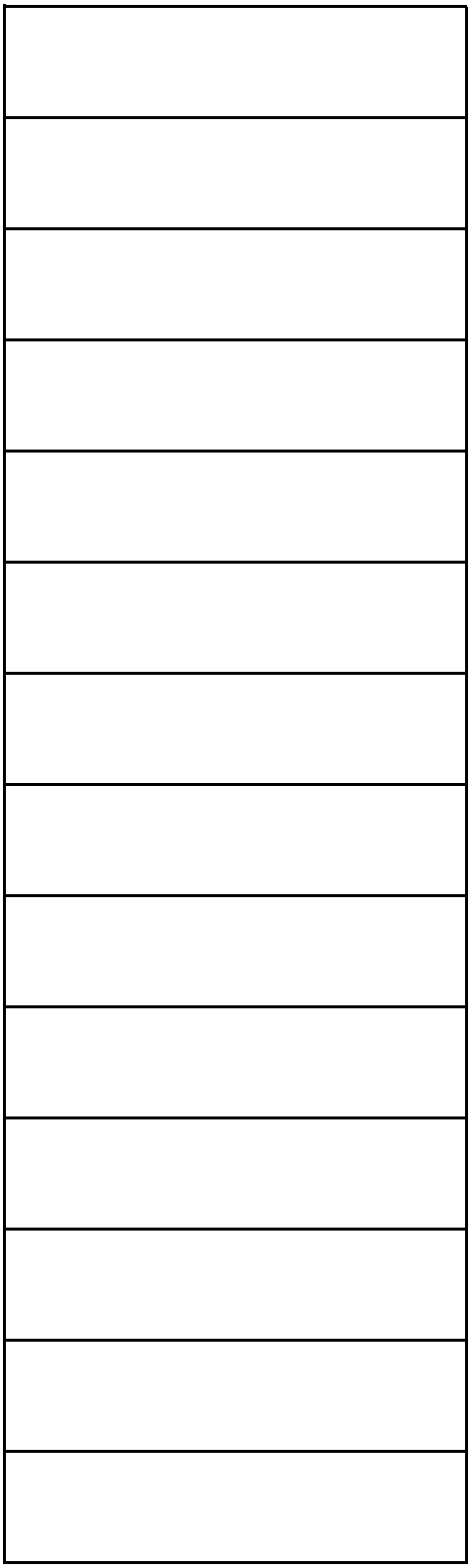


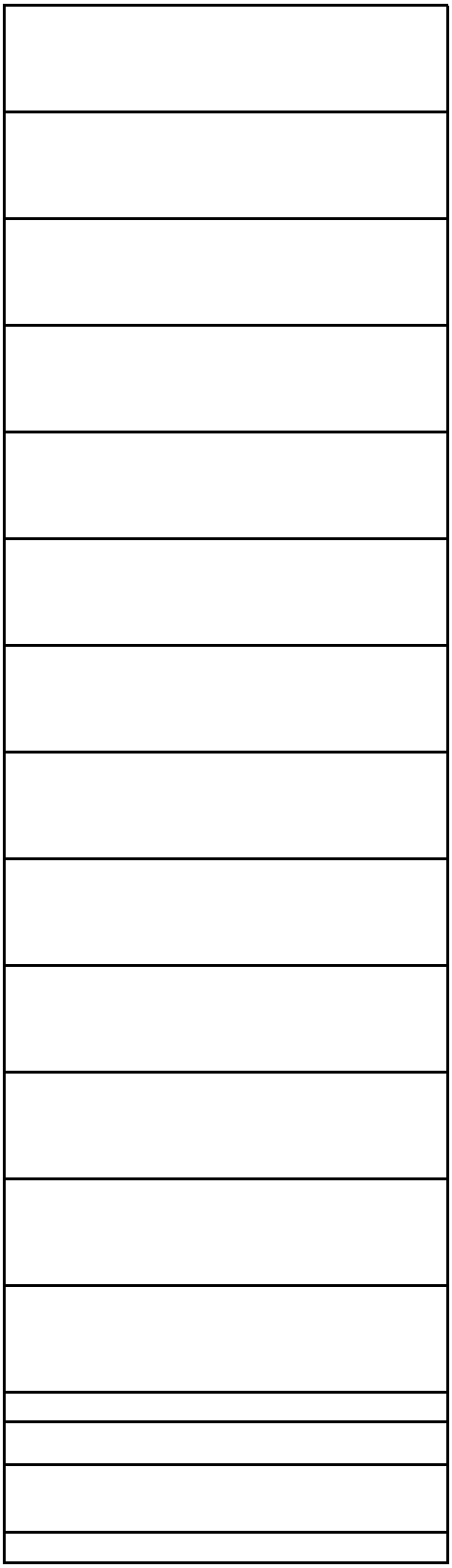


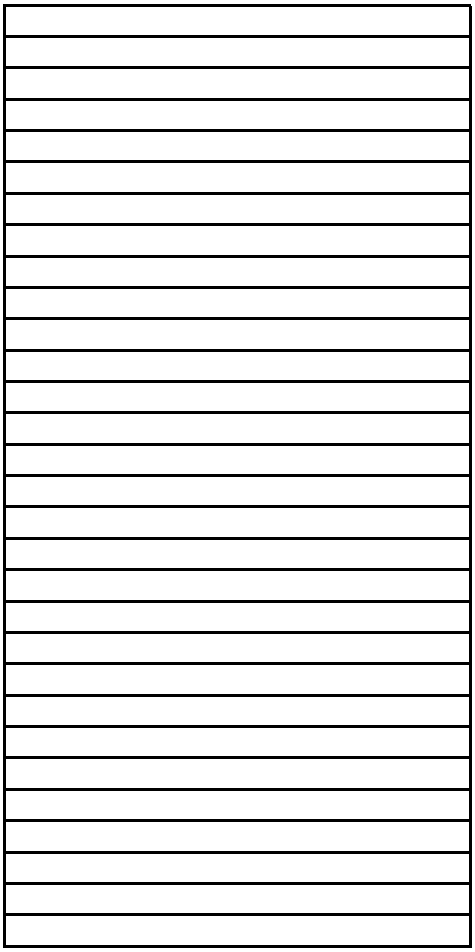












Register Number_____

[18ITU401]

KARPAGAM ACADEMY OF HIGHER EDUCATION

KARPAGAM UNIVERSITY

(Deemed to be University Established under Section 3 of UGC Act 1956)

Information Technology

FIRST INTERNAL EXAMINATION- December 2019

DATA COMMUNICATION NETWORKS

CLASS: II BSc (IT) **Time: 2 hours**

DATE & SESSION: 18.12.2019, FN **Maximum: 50 marks**

PART – A (20 x 1 = 20 Marks)
Answer ALL the Questions

1. The system must deliver data to the correct destination is called_____
   a. **Accuracy** b. jitter c. delivery d. timeliness
2. In_____, the communication is unidirectional.
   a. duplex mode b. full duplex mode c. half duplex mode d. **simplex mode**
3. One long cable acts as a _____to link all the devices in a network.
   a.Bus b. mesh c. hub d. **backbone**
4. MAN stands for _____
   a.Metropolitician area network b. **Metropolitan area network**
   c.Metropolitical area network d. Macro area network
5. In physical layer we can transfer data into _____
   a. Frame b. packet c. **bit** d. byte
6. _____is a type of transmission impairment in which an outside source such as crosstalk corrupts a signal
   a. Attenuation b. distortion c. **noise** d. decibel
7. FTP_____
   a. file transmit protocol b. file transmission protocol
   c. **file transfer protocol** d. flip transfer protocol
8. A multipoint is also called as_____
   a. multi line b. **multi drop** c. multi level d. single level
9. A_____ is the set of rules.
   a. **Protocols** b. transmission medium c. networks d. ip
10. The _____is the number of bits sent in a second.
    a.Bit length b. bandpass c. bandwidth d. **bit rate**
11. _____standards are often established originally by manufactures.
    a.**de jure** b. de facto c. de fact d. Semantics

12. The_____layer is responsible for providing services to the user.

a. Presentation b. data link c. **application** d. network

13. ARP is _____

a. address resolution protocol c. address result protocol

b. address revolutionized protocol d. address research protocol

14. As frequency increases, the period_____

a. **Decreases** b. increases c. remains the same d. doubles

15. Data communication means exchange of data between _____devices.

a. One b**. Two** c. Six d. Four

16. A_____ is the set of rules.

a**. Protocols** b. Modem c. Networks d. Datagram

17. A_____connection provides a dedicated link between two devices.

a. Point-to-point b. **multi-point** c. mesh d. physical

18. The _____layer is responsible for process to process delivery.

a. physical b. presentation c.networks d. **transport**

19. A_____is a set of devices connected by communication links.

a. Protocols b. **networks** c. computer d. printer

20. . The _____layer is responsible for movements of bits from one hop to next.

a.data link b. **physical**

c. transport d. session

PART – B (3 x 8 = 24 Marks)

Answer ALL the Questions

21. **Define Data communication.**

Data communication means exchanging of data between two devices via some form of transmission medium such as a wire cable.

22. **What is meant by bandwidth?**

Bandwidth means the amount of data that can be sent from one point to another in a certain period of time. It is measured as a bit rate expressed in bits per second. The bandwidth of a composite signal is the difference between the highest and the lowest frequency contained in that signal.

23. **Write short notes on multiplexing**.

Multiplexing is a set of techniques that allows the simultaneous transmission of multiple signals across single data link.

PART – C (3 x 8 = 24 Marks)
Answer ALL the Questions

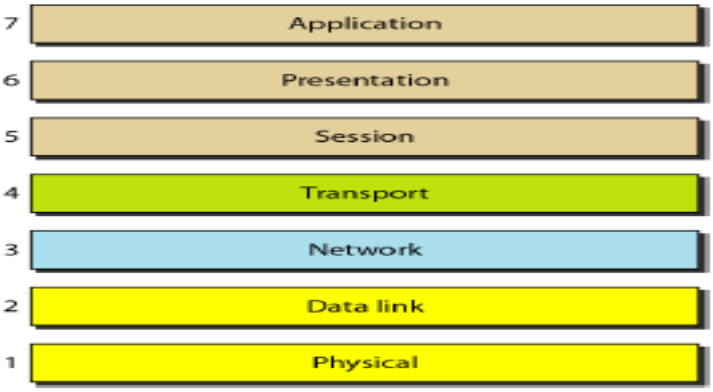
24. a. Elucidate the layered architecture of OSI reference model with a neat diagram.

THE OSI MODEL

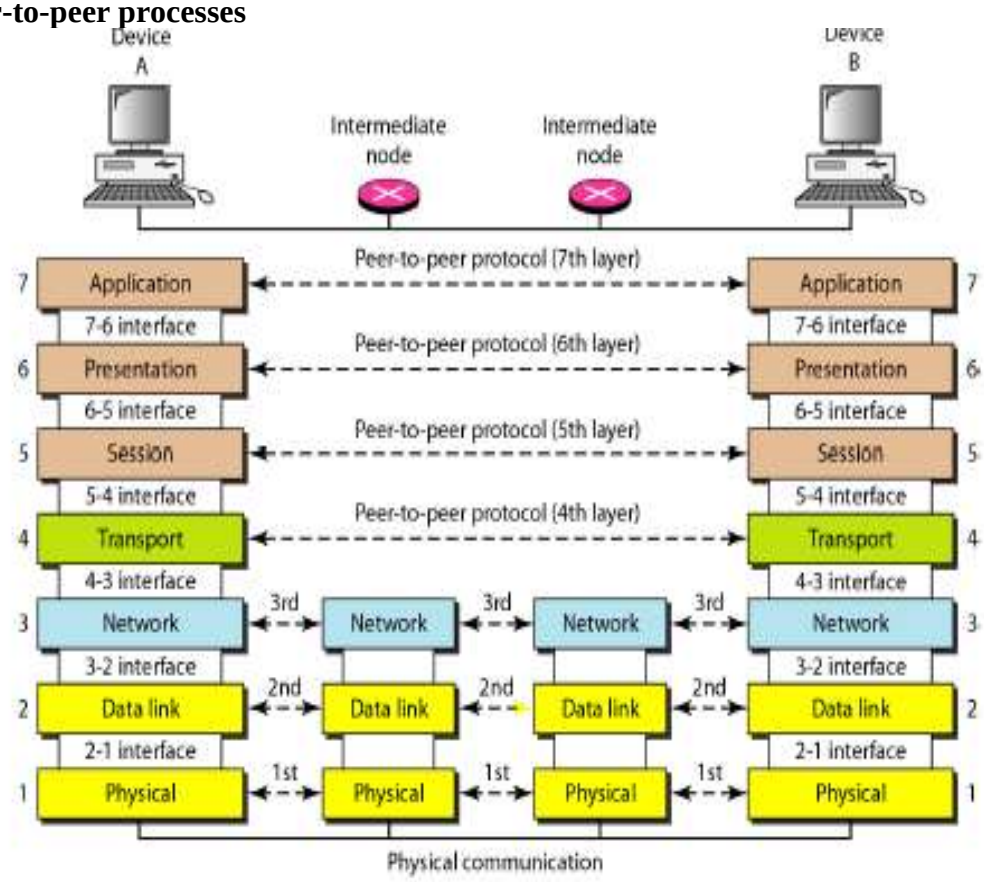
Established in 1947, the International Standards Organization (ISO) is a multinational body dedicated to world wide agreement on international standards.

An ISO standard that covers all aspects of network communications is the Open Systems Interconnection (OSI) model. It was first introduced in the late 1970s.

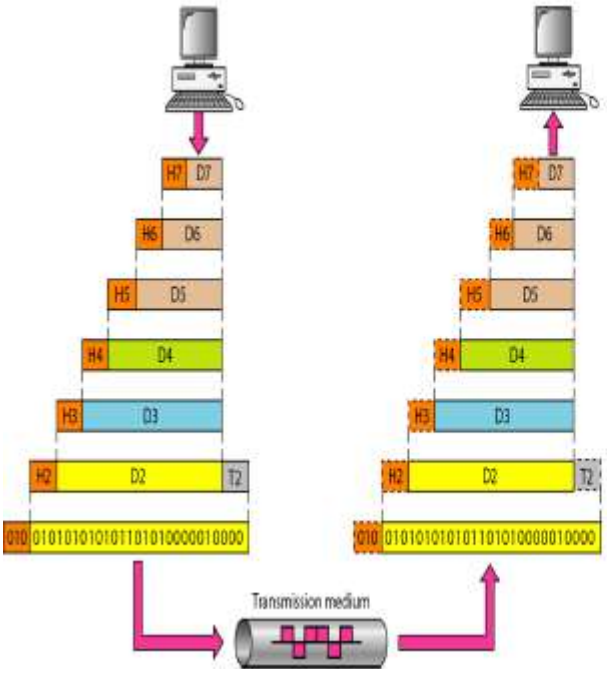
Seven layers of the OSI model



Peer-to-peer processes



Encapsulation

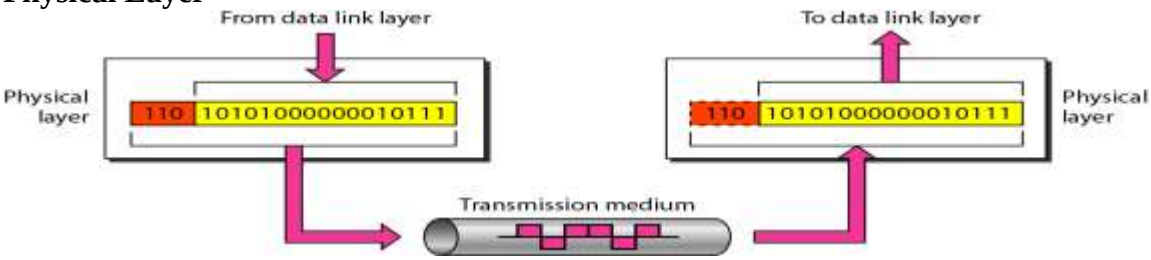


- The process starts at layer 7 (application layer), then moves from layer to layer in descending, sequential order.
- At each layer, a **header** is added to the data unit.
- At layer 2, a **trailer** is added as well.
- When the formatted data unit passes through the physical layer (layer 1) it is changed into an electromagnetic or optical signal and transported along a physical link
- At the destination the reverse process is performed

THE OSI MODEL AND LAYERS

In this section we briefly describe the functions of each layer in the OSI model.

Physical Layer



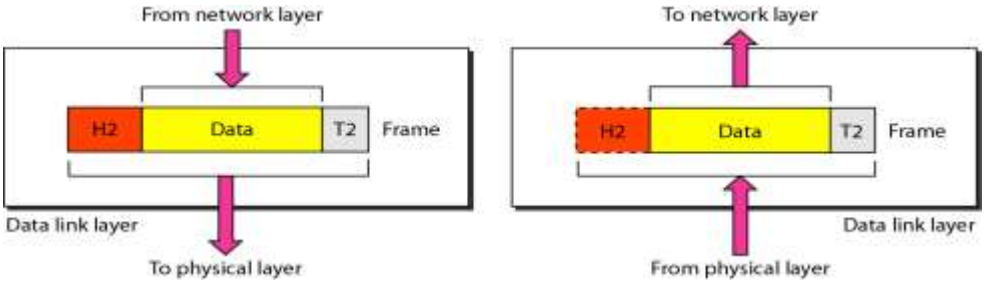
- The physical layer is responsible for movements of individual bits from one hop (node) to the next
- Mechanical and electrical specification, the procedures and functions

Duties:

- Physical characteristics of interfaces and media
- Representation of bits
- Data rate
- Synchronization of bits
- Line configuration
- Physical topology
- Transmission mode

Data link layer

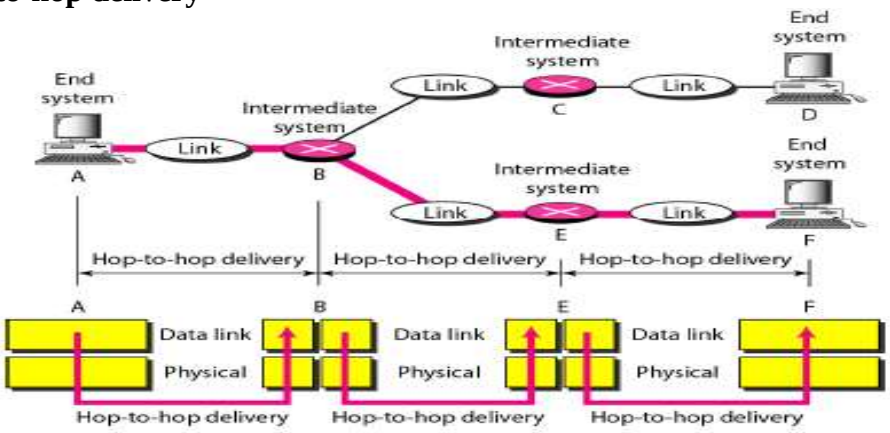
- The data link layer is responsible for moving frames from one hop (node) to the next
- Transform the physical layer to a reliable (error-free) link



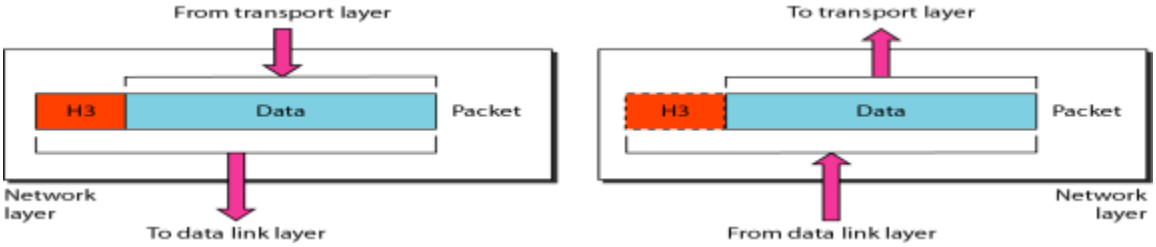
Duties:

- Framing
- Physical addressing
- Flow control
- Error control
- Access control

Hop-to-hop delivery



Network layer

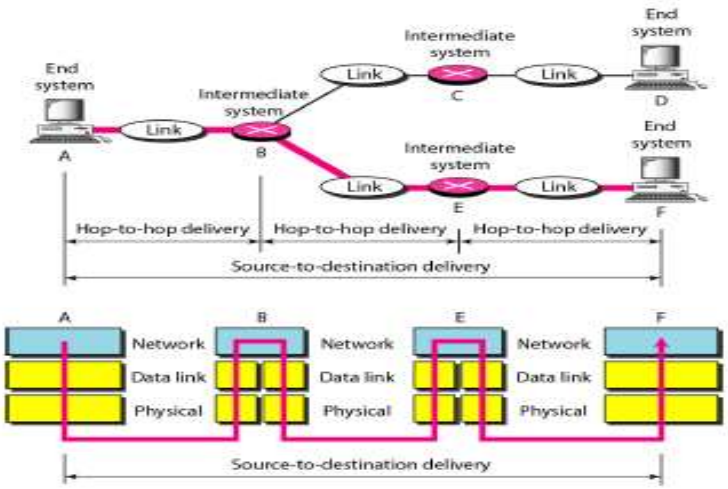


The network layer is responsible for the delivery of individual packets from the source host to the destination host.

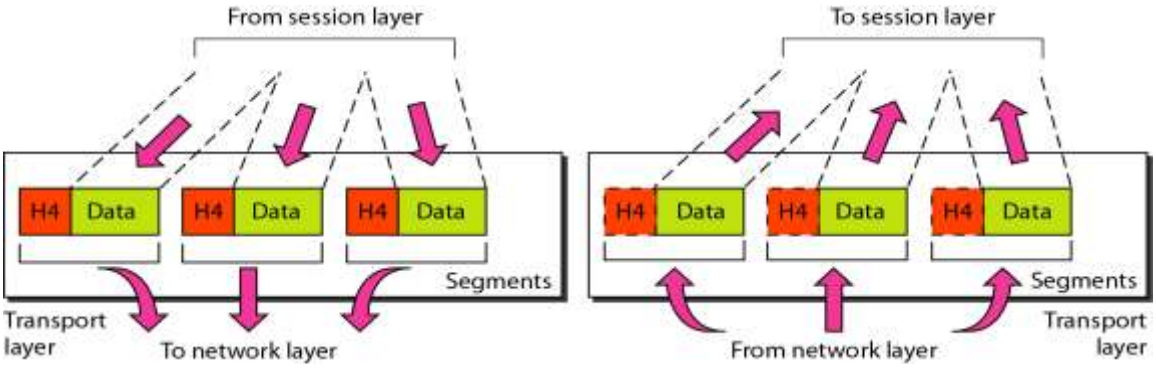
Duties:

- Logical addressing
- Routing

Source-to-destination delivery

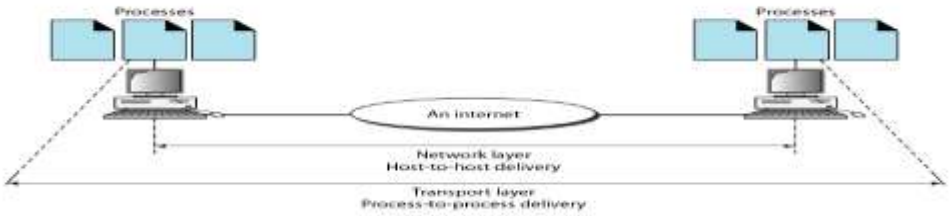


Transport layer



The transport layer is responsible for the delivery of a message from one process to another.
Duties:

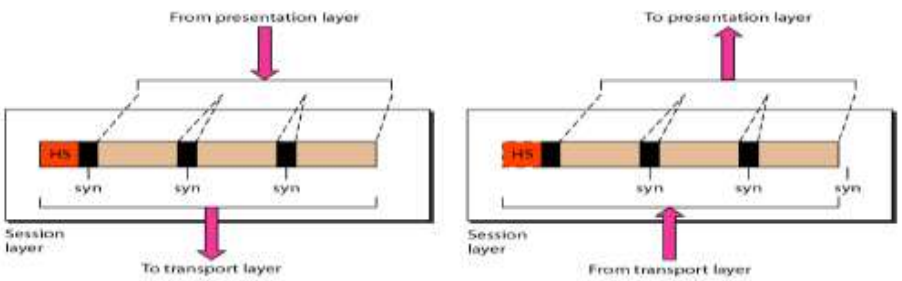
- Service-point (port) addressing
- Segmentation and reassembly
- Connection control
- Flow control
- Error control



Reliable process-to-process delivery

Session layer

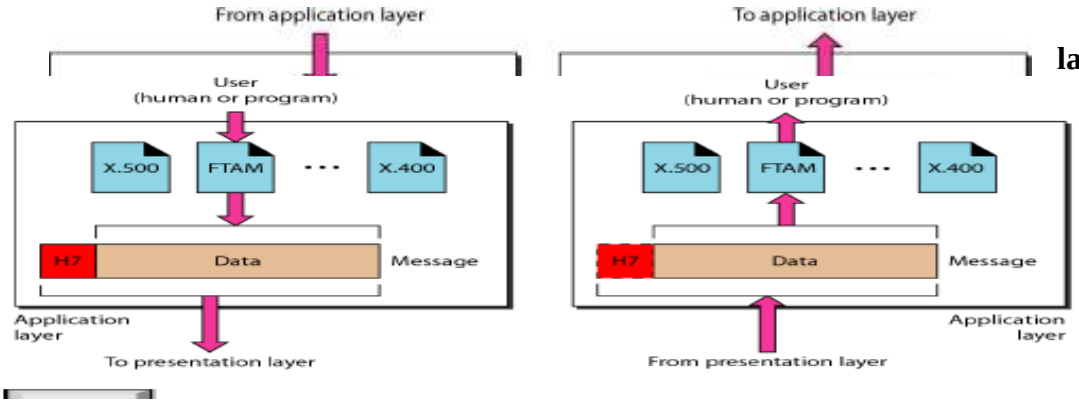
The session layer is responsible for dialog control and synchronization.



Presentation layer

The presentation layer is responsible for translation, compression, and encryption.

Application layer



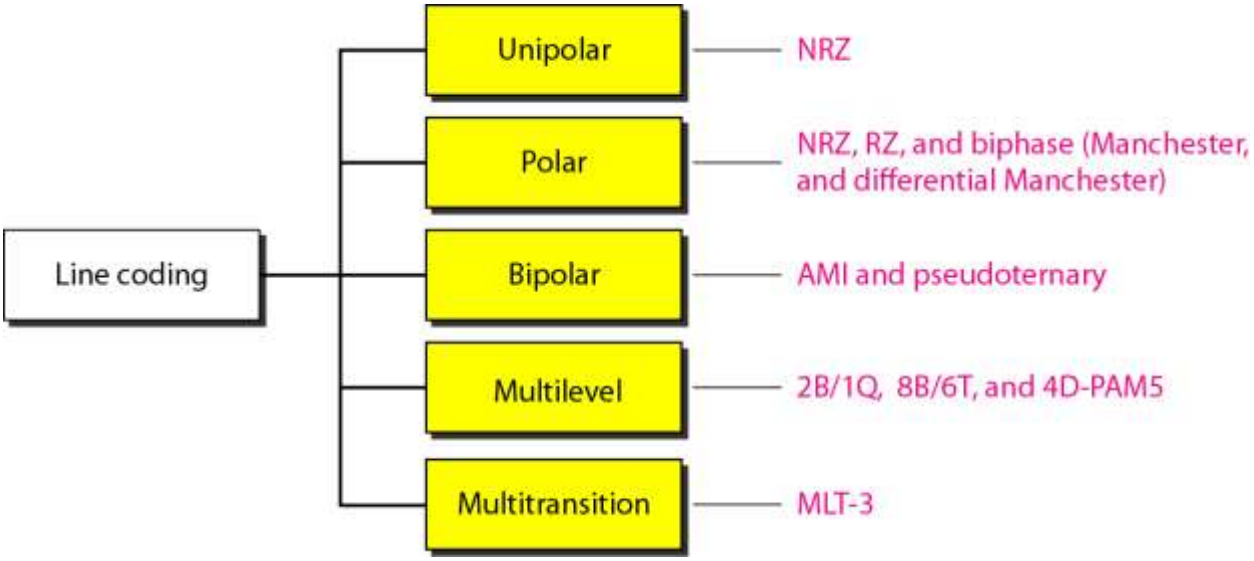
The application layer is responsible for providing services to the user.

Services:

- Network virtual terminal
- Mail services
- File transfer, access, and management
- Directory services

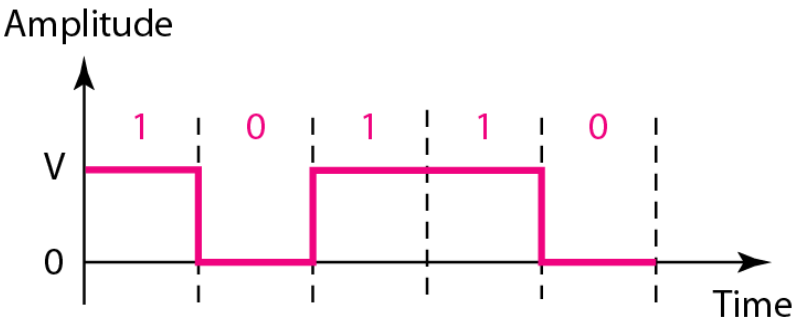
[OR]

b. Explain different categories of line coding scheme with neat sketch.



Unipolar Scheme:

- One polarity: one level of signal voltage
- Unipolar NRZ (None-Return-to-Zero) is simple, but
  - DC component : Cannot travel through microwave or transformer
  - Synchronization : Consecutive 0's and 1's are hard to be synchronized → Separate line for a clock pulse
  - Normalized power is double that for polar NRZ

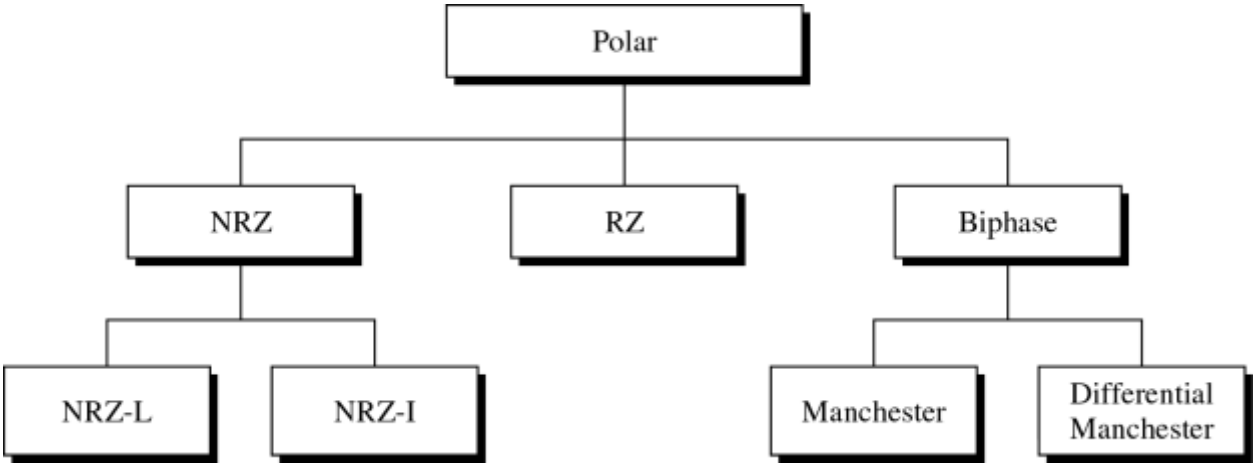


$$\frac{1}{2}V^2 + \frac{1}{2}(0)^2 = \frac{1}{2}V^2$$

Normalized power

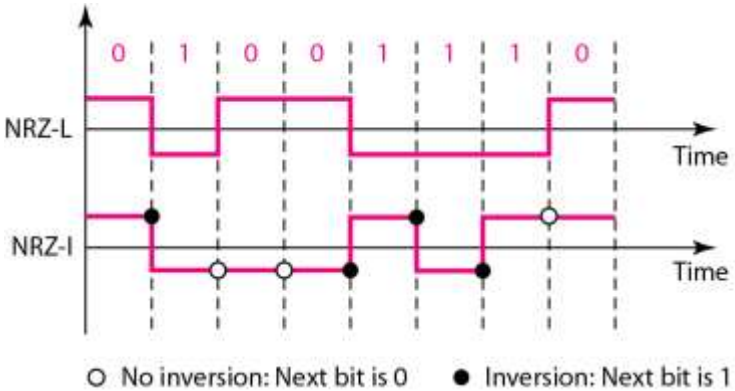
Polar Scheme

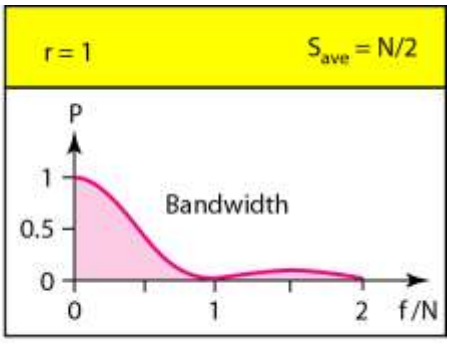
- Two polarity: two levels of voltage
- Problem of DC component is alleviated (NRZ,RZ) or eliminated (Biphaze)



Polar NRZ

- NRZ-L (Non Return to Zero-Level)
  - Level of the voltage determines the value of the bit
- NRZ-I (Non Return to Zero-Invert)
  - Inversion or the lack of inversion determines the value of the bit





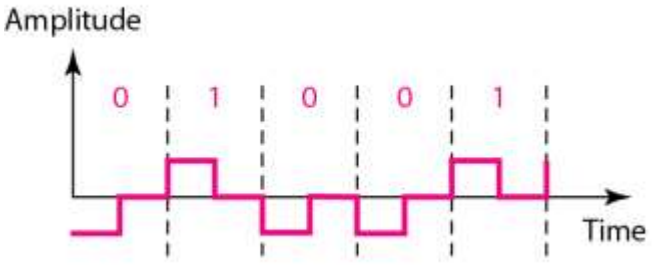
Polar NRZ: NRZ-L and NRZ-I

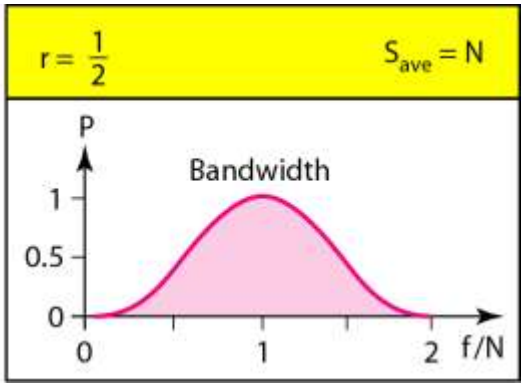
- Baseline wandering problem

  - Both, but NRZ-L is twice severe
- Synchronization Problem
  - Both, but NRZ-L is more serious
- NRZ-L and NRZ-I both have an average signal rate of N/2 Bd
- Both have a DC component problem

RZ

- Provides synchronization for consecutive 0s/1s
- Signal changes during each bit
- Three values (+, -, 0) are used
  - Bit 1: positive-to-zero transition, bit 0: negative-to-zero transition



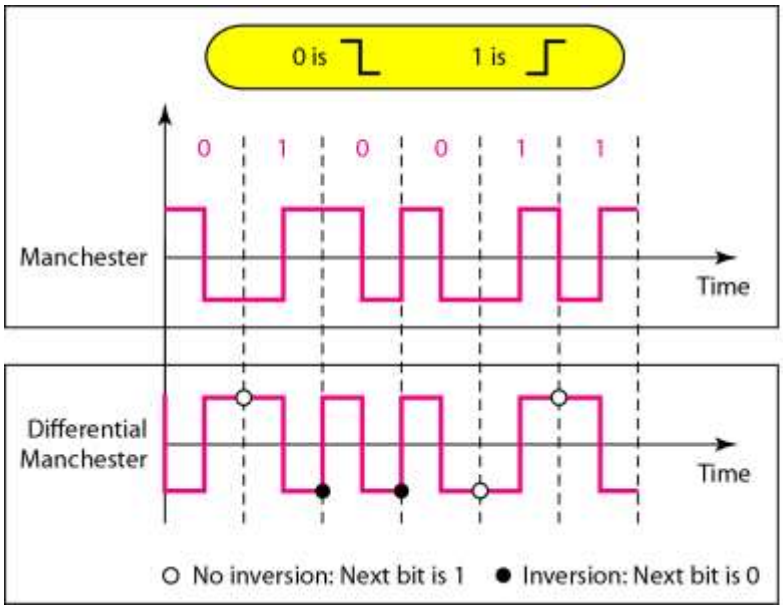


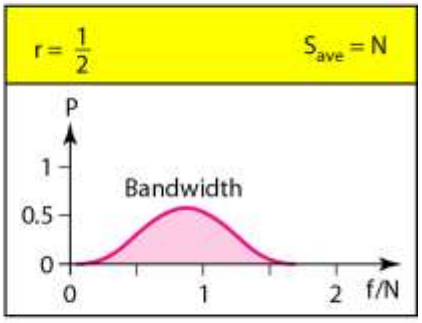
Biphase

- Combination of RZ and NRZ-L ideas
- Signal transition at the middle of the bit is used for synchronization
- Manchester
  - Used for Ethernet LAN
  - Bit 1: negative-to-positive transition
  - Bit 0: positive-to-negative transition
- Differential Manchester
  - Used for Token-ring LAN
  - Bit 1: no transition at the beginning of a bit
  - Bit 0: transition at the beginning of a bit

Polar Biphase

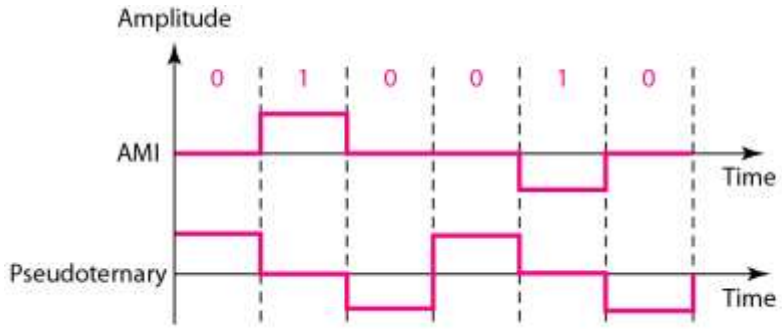
- Minimum bandwidth is 2 times that of NRZ

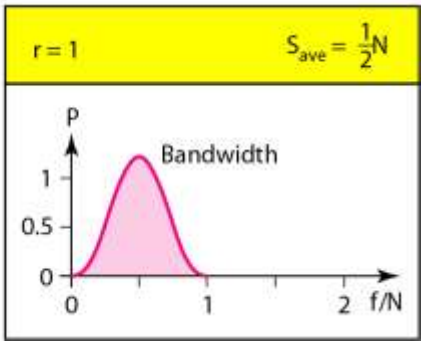




Bipolar Scheme

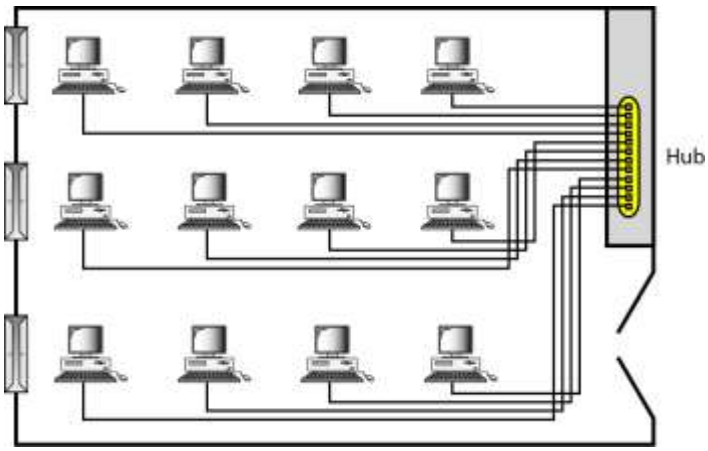
- Three levels of voltage, called "multilevel binary"
- Bit 0: zero voltage, bit 1: alternating +1/-1
  - (Note) In RZ, zero voltage has no meaning
- AMI (Alternate Mark Inversion) and pseudoternary
  - Alternative to NRZ with the same signal rate and no DC component problem





25. a. Describe the architecture of LAN, MAN, WAN and their differences with neat sketches.

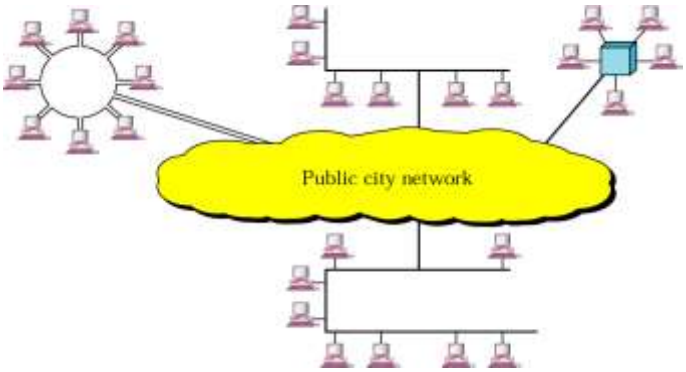
Local Area Networks (LANs)



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

and video peripherals. Currently, LAN size is limited to a few kilometers.
LANs are designed to allow resources to be shared between personal computers or workstations. The resources to be shared can include hardware (e.g., a printer), software (e.g., an application program), or data. A common example of a LAN, found in many business environments, links a workgroup of task-related computers, for example, engineering workstations or accounting PCs. One of the computers may be given a large capacity disk drive and may become a server to clients. Software can be stored on this central server and used as needed by the whole group. In this example, the size of the LAN may be determined by licensing restrictions on the number of users per copy of software, or by restrictions on the number of users licensed to access the operating system.

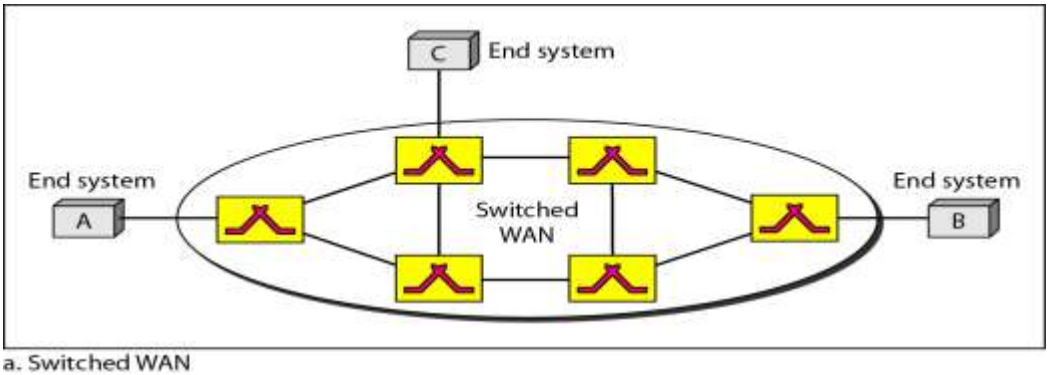
In addition to size, LANs are distinguished from other types of networks by their transmission media and topology. In general, a given LAN will use only one type of transmission medium. The most common LAN topologies are bus, ring, and star. Early LANs had data rates in the 4 to 16 megabits per second (Mbps) range. Today, however, speeds are normally 100 or 1000 Mbps



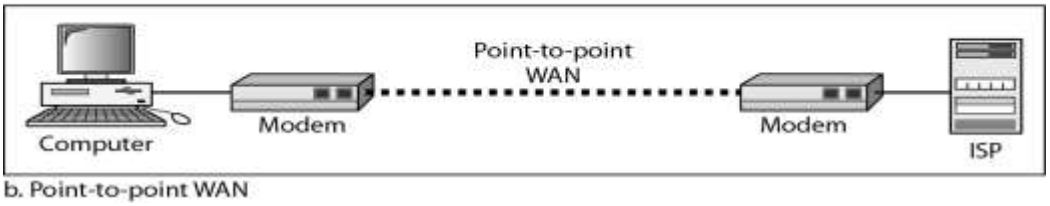
Metropolitan Area Networks (MANs)

A metropolitan area network (MAN) is a network with a size between a LAN and a WAN. It normally covers the area inside a town or a city. It is designed for customers who need a high-speed connectivity, normally to the Internet, and have endpoints spread over a city or part of city. A good example of a MAN is the part of the telephone company network that can provide a high-speed DSL line to the customer. Another example is the cable TV network that originally was designed for cable TV, but today can also be used for high-speed data connection to the Internet

• Wide Area Networks (WANs)



a. Switched WAN



b. Point-to-point WAN

A wide area network (WAN) provides long-distance transmission of data, image, audio, and video information over large geographic areas that may comprise a country, a continent, or even the whole

world. A WAN can be as complex as the backbones that connect the Internet or as simple as a dial-up line that connects a home computer to the Internet. We normally refer to the first as a switched WAN and to the second as a point-to-point WAN.

- The switched WAN connects the end systems, which usually comprise a router (internetworking connecting device) that connects to another LAN or WAN.
- The point-to-point WAN is normally a line leased from a telephone or cable TV provider that connects a home computer or a small LAN to an Internet service provider (lSP). This type of WAN is often used to provide Internet access.

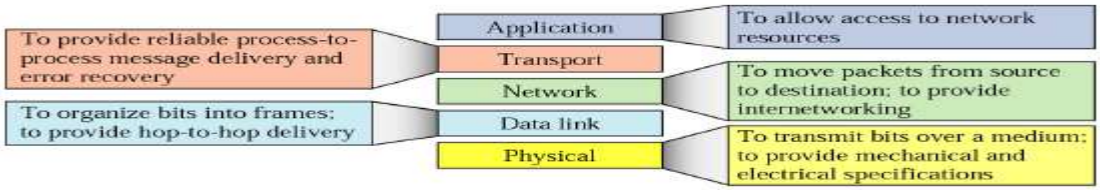
[OR]

b. Explain different types of addresses associated with the layers in TCP/IP protocol suite

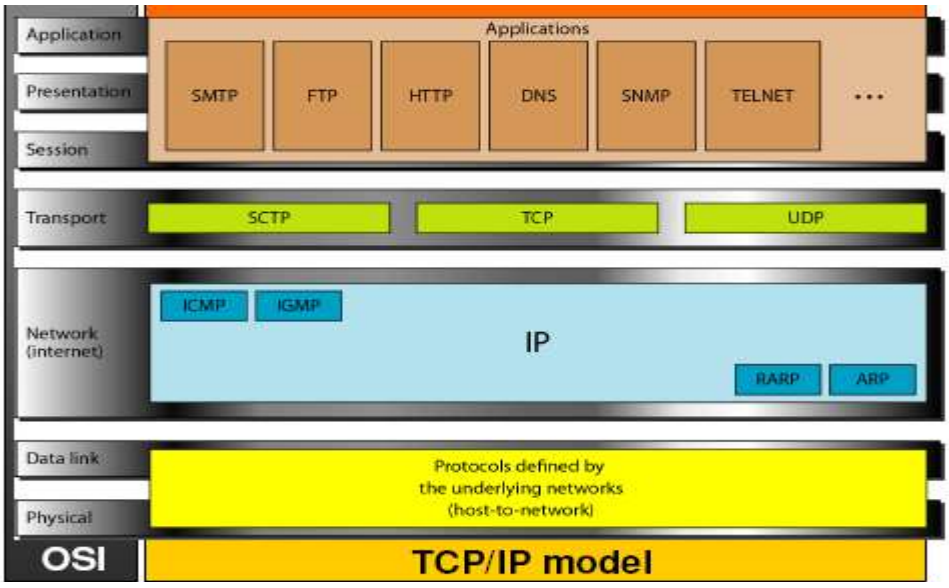
TCP/IP PROTOCOL SUITE

The layers in the TCP/IP protocol suite do not exactly match those in the OSI model. The original TCP//IP protocol suite was defined as having four layers:: host-to-network, internet, transport, and application. However, when TCP/IP is compared to OSI, we can say that the TCP/IP protocol suite is made of five layers:
physical, data link, network,, transport, and application.

TCP/IP layers

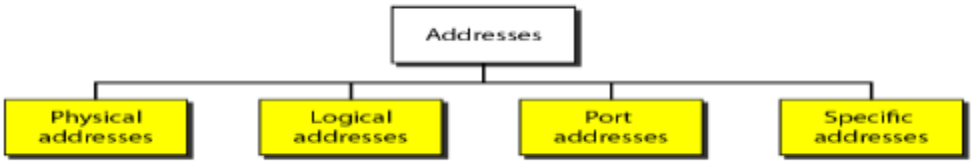


TCP/IP and OSI model



ADDRESSING

Four levels of addresses are used in an internet employing the TCP/IP protocols: physical, logical, port, and specific.



Physical & Logical address

• Physical address

In computer networks a physical address means a MAC (Medium Access Control) address. Also known as Ethernet Hardware Address (EHA) or hardware address or **adapter address.** It is a number that acts like a name for a particular networkadapter, eg. the network cards

• Logical address

—In computer networks, a logical address refers to a network layer address such as an IP address

—An IP address (Internet Protocol address) is a unique address that certain electronic devices use in order to identify and communicate with each other on a computer network utilizing the Internet Protocol standard (IP)

Port & specific address

• Port address

—TCP and UDP are transport protocols used for communication between computers via ports

—The port numbers are divided into three ranges.

• The Well Known Ports are those in the range 0–1023.

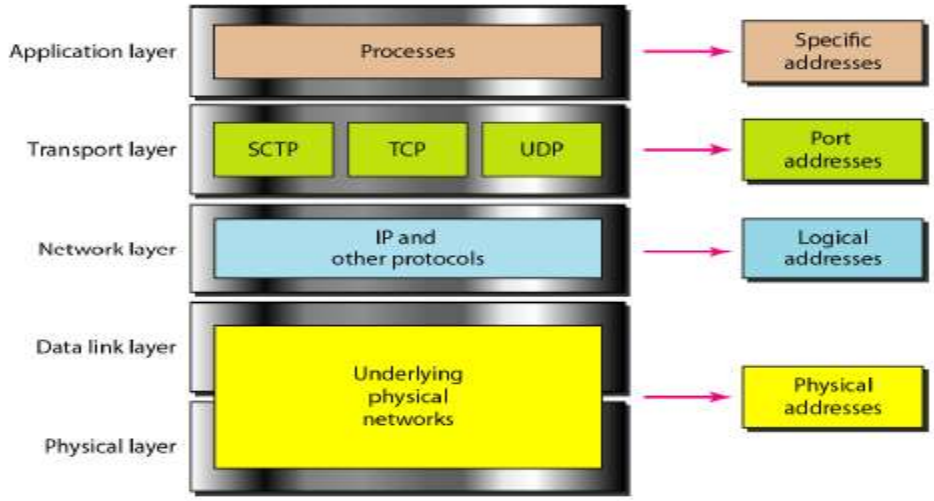
• The Registered Ports are those in the range 1024–49151.

• The Dynamic and/or Private Ports are those in the range 49152–65535. These ports are not used by any defined application.

• Specific address

—This address is used by application processes

Relationship of layers-addresses in TCP/IP

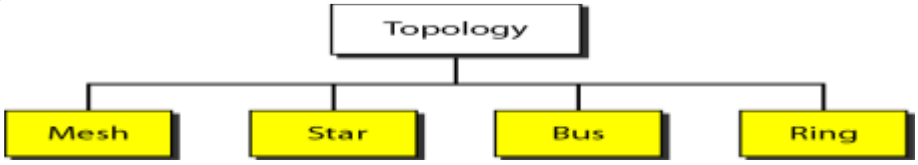


26. a. Explain the various network topologies with a neat diagram

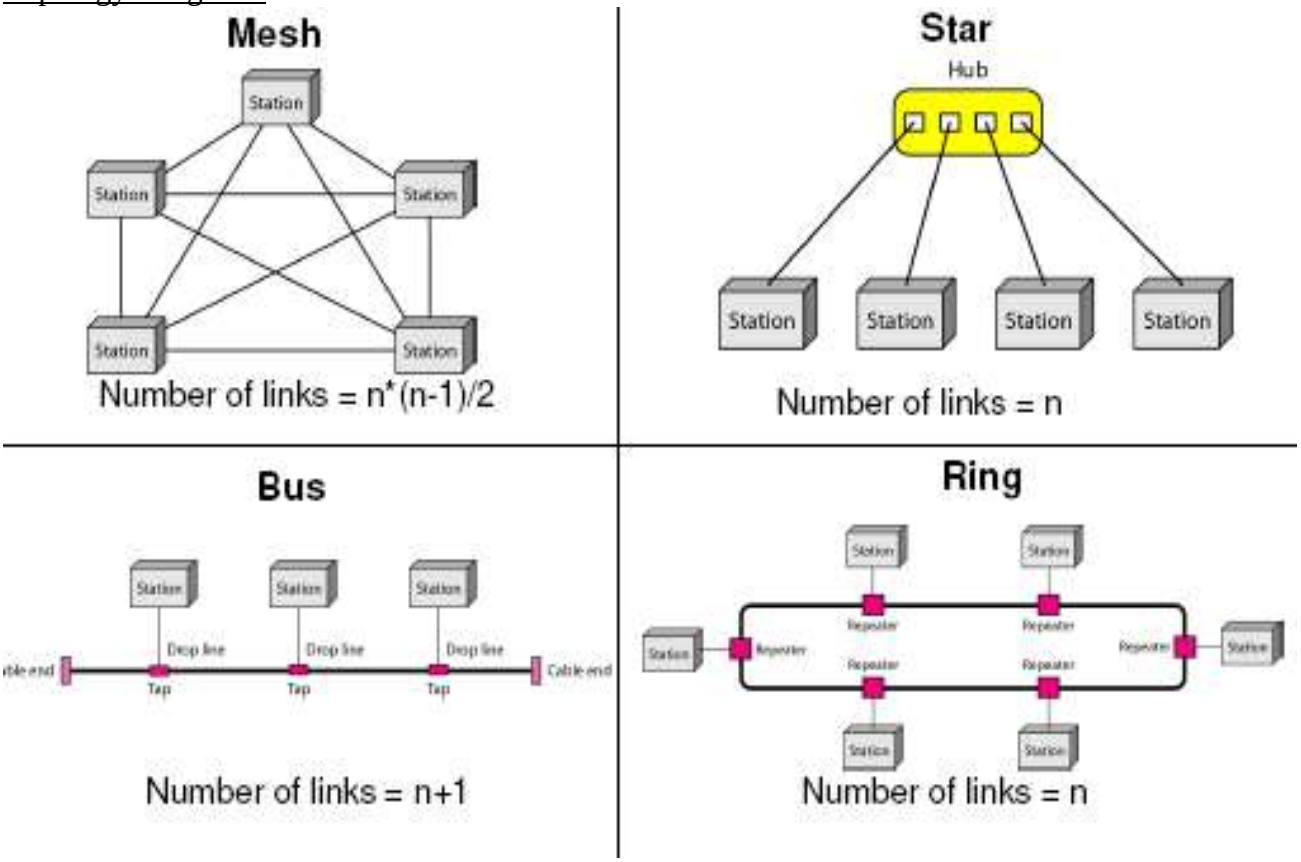
Physical Topology

Physical topology refers to the way in which a network is laid out physically.

Network topology is the geometric representation of the relationship of all the links and linking devices (nodes)



Topology categories



Mesh Topology : In a mesh topology, every device has a dedicated point-to-point link to every other device. The term dedicated means that the link carries traffic only between the two devices it connects. To find the number of physical links in a fully connected mesh network with n nodes, we first consider that each node must be connected to every other node. Node 1 must be connected to n - I nodes, node 2 must be connected to n – 1 nodes, and finally node n must be connected to n - 1 nodes. We need n(n - 1) physical links. 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.

Advantages of Mesh Topology

- A 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.

- A mesh topology is robust. If one link becomes unusable, it does not incapacitate the entire system.
- There is the 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.
- Finally, point-to-point links make fault identification and fault isolation easy. Traffic can be routed to avoid links with suspected problems. This facility enables the network manager to discover the precise location of the fault and aids in finding its cause and solution.

Disadvantages of Mesh Topology

The main disadvantages of a mesh are related to the amount of cabling and the number of I/O ports required.

- First, because every device must be connected to every other device, installation and reconnection are difficult.
- Second, the sheer bulk of the wiring can be greater than the available space (in walls, ceilings, or floors) can accommodate.
- Finally, the hardware required to connect each link (I/O ports and cable) can be prohibitively expensive.
- For these reasons a mesh topology is usually implemented in a limited fashion, for example, as a backbone connecting the main computers of a hybrid network that can include several other topologies.

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.

Advantages of Star Topology

- 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 which also makes it easy to install and reconfigure.
- Other advantages include 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.
- As long as the hub is working, it can be used to monitor link problems and bypass defective links.

Disadvantages of Star Topology

- 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.
- 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).

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

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 of Bus Topology

- Advantages of a bus topology include ease of installation. Backbone cable can be laid along the most efficient path, then connected to the nodes by drop lines of various lengths. In this way, a bus uses less cabling than mesh or star topologies.
- In a star, for example, four network devices in the same room require four lengths of cable reaching all the way to the hub. In a bus, this redundancy is eliminated. Only the backbone cable stretches through the entire facility. Each drop line has to reach only as far as the nearest point on the backbone.

Disadvantages

- Disadvantages include 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. This degradation can be controlled by limiting the number and spacing of devices connected to a given length of cable.
- Adding new devices may therefore require modification or replacement of the backbone.
- In addition, a fault or break in the bus cable stops all transmission, even between devices on the same side of the problem.

Ring Topology

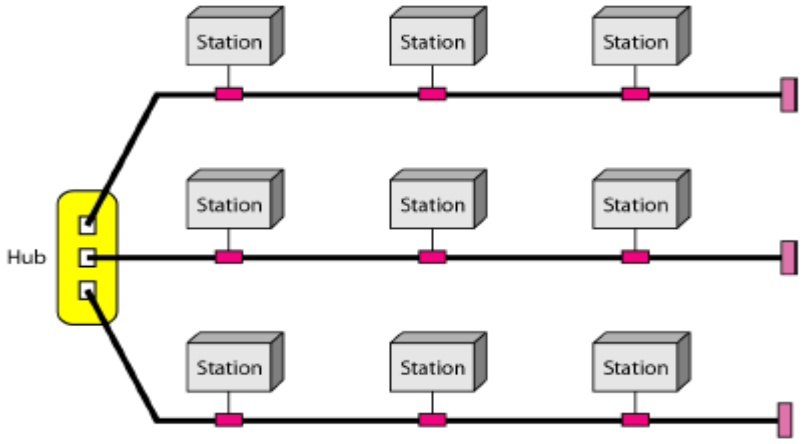
Ring Topology In a ring topology, each device has a dedicated point-to-point connection with only the two devices on either side of it. A signal is passed along the ring in one direction, from device to device, until it reaches its destination. Each device in the ring incorporates a repeater. When a device receives a signal intended for another device, its repeater regenerates the bits and passes them along.

A 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. The only constraints are media and traffic considerations (maximum ring length and number of devices). In addition, fault isolation is simplified. Generally in a ring, a signal is circulating at all times. If one device does not receive a signal within a specified period, it can issue an alarm. The alarm alerts the network operator to the problem and its location. However, 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. This weakness can be solved by using a dual ring or a switch capable of closing off the break.

A hybrid topology

A network can be hybrid. For example, we can have a main star topology with each branch connecting several stations in a bus topology as shown in Figure below.

A star backbone with three bus networks



[OR]

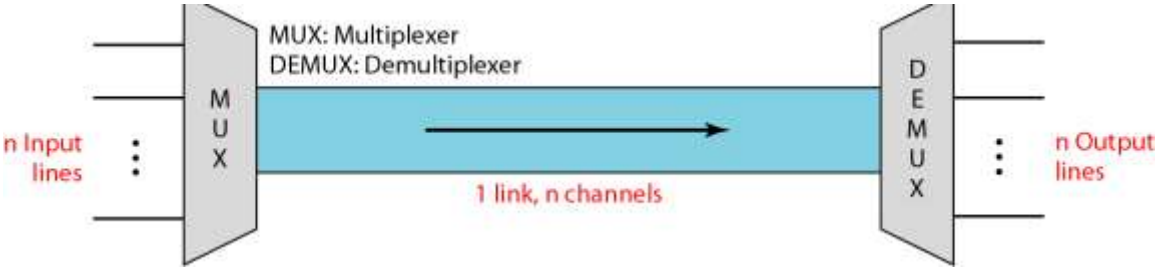
b. Illustrate the working of frequency division multiplexing with a neat diagram.

MULTIPLEXING

Whenever the bandwidth of a medium linking two devices is greater than the bandwidth needs of the devices, the link can be shared. Multiplexing is the set off techniques that allows the simultaneous transmission of multiple signals across a single data link. As data and telecommunications use increases, so does traffic.

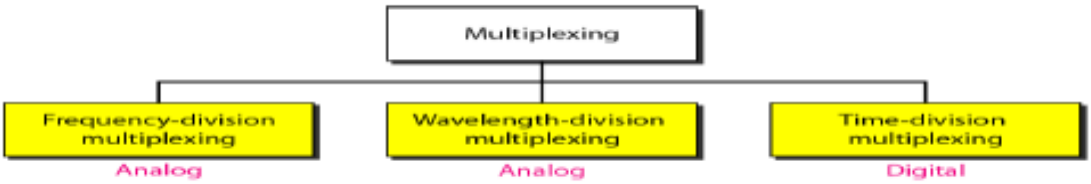
Dividing a link into channels

In a multiplexed system, *n* lines share the bandwidth of one link. 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-to-one). 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. In the figure, the word link refers to the physical path. The word channel refers to the portion of a link that carries a transmission between a given pair of lines. One link can have many *(n)* channels.



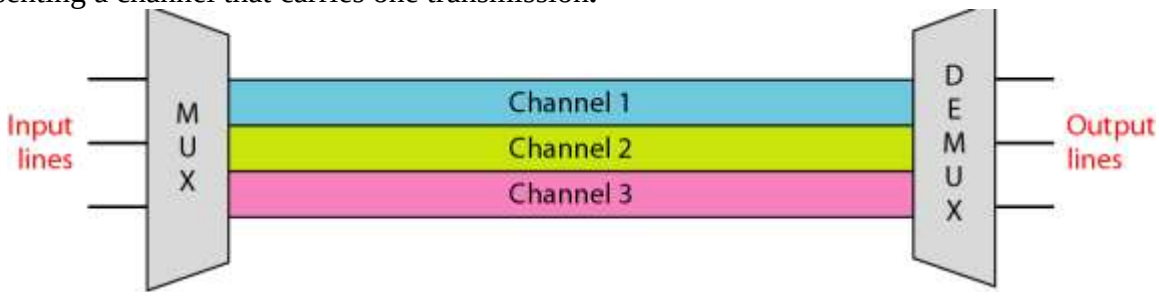
Categories of multiplexing

There are 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



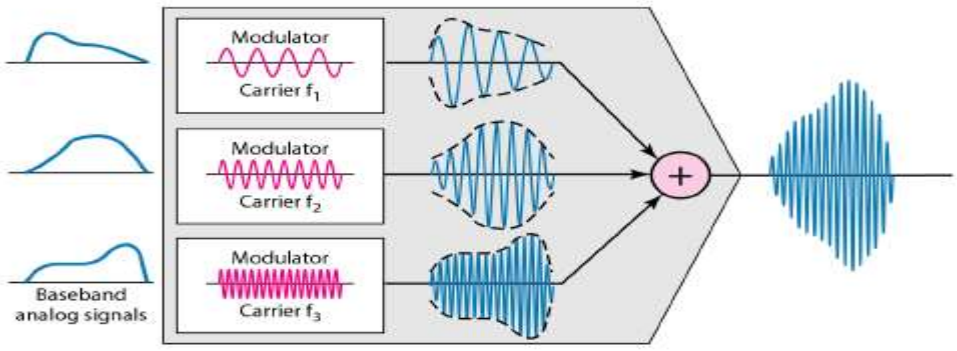
Frequency Division Multiplexing (FDM)

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. In addition, carrier frequencies must not interfere with the original data frequencies. 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**.**



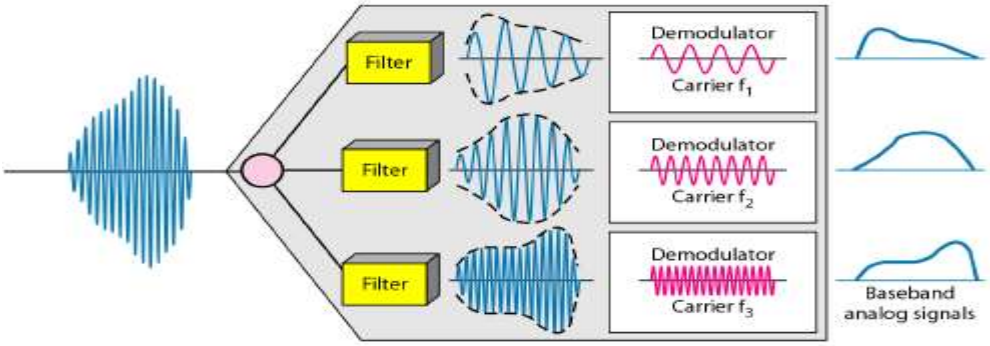
Multiplexing Process

Figure below is a conceptual illustration of the multiplexing process. Each source generates a signal of a similar frequency range. Inside the multiplexer, these similar signals modulates different carrier frequencies. 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.



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.



A very common application of FDM is AM and FM radio broadcasting. Radio uses the air as the transmission medium. A special band from 530 to 1700 kHz is assigned to AM radio. All radio stations need to share this band. Each AM station needs 10kHz of bandwidth. Each station uses a different carrier frequency, which means it is shifting its signal and multiplexing. The signal that goes to the air is a combination of signals. A receiver receives all these signals, but filters (by tuning) only the one which is desired. Without multiplexing, only one AM station could broadcast to the common link, the air. The situation is similar in FM broadcasting. However, FM has a wider band of 88 to 108MHz because each station needs a bandwidth of 200 kHz. Another common use of FDM is in television broadcasting. Each TV channel has its own bandwidth of 6 MHz.