KARPAGAM ACADEMY OF HIGHER EDUCATION

(Deemed to be University)
(Established Under Section 3 of UGC Act 1956)
Coimbatore - 641021.
(For the candidates admitted from 2017 onwards)

DEPARTMENT OF COMPUTER SCIENCE, COMPUTER APPLICATION & INFORMATION TECHNOLOGY

SUBJECT : COMPUTER NETWORKS
SEMESTER :III
SUBJECT CODE: 17CTU303 CLASS : II B.sc CT

SCOPE

This course is to master the fundamentals of data communications networks by gaining a working knowledge of data transmission concepts, understanding the operation of all seven layers of OSI Model and the protocols used in each layer.

OBJECTIVES

- Various transmission media, their comparative study, fiber optics and wireless media
- Categories and topologies of networks (LAN and WAN) Layered architecture (OSI and TCP/IP) and protocol suites.
- Channel error detection and correction, MAC protocols, Ethernet and WLAN.
- Details of IP operations in the INTERNET and associated routing principles

UNIT I

Introduction to Computer Networks : Network definition; network topologies; network classifications; network protocol; 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

Digital to analog modulation-; multiplexing techniques- FDM, TDM; transmission media. **Networks Switching Techniques and Access mechanisms:** Circuit switching; packetswitching - 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. B. A Forouzan (2012). Data Communications and Networking(4th ed.). THM.
2. A. S.Tanenbaum, (2002). Computer Networks (4th ed.). 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.w3school.

Continuous Internal Assessment

S.No	Category	Marks
1	Assignment	5
2	Attendance	5
3	Seminar	5
4	CIA I	8
5	CIA II	8
6	CIA III	9
Total Marks		**40**

End Semester Examination –Marks Allocation

1	**Part A** 20 X 1 = 20 Online Examination	20
2	**Part B** 5 X 2 = 10	10
3	**Part C** 5 X 6 = 30 Either '**A**' OR '**B**' Choice	30
	Total Marks	**60**

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

SUBJECT NAME:COMPUTER NETWORKS

SUBJECT CODE:17CTU303 **SEMESTER: III**

STAFF: B.BRINDHA **CLASS: III B.Sc. CT**

LECTURE PLAN

S. No	Lecture Duration (Hr)	Topics to be Covered	Support Materials
		UNIT – I	
1.	1	Introduction to Computer Networks • Definition, Criteria • Physical Structure Network topologies	S1 : 4 – 8, W2 S1 : 9 - 16
2.	1	Network classifications Network protocol Layered network architecture	S2:18-23 S1 : 9-27
3.	1	Overview of OSI reference model	S1:29-42
4.	1	Overview of TCP/IP protocol suite	S2:34-37,S1:42-51
5.	1	Data Communication Fundamentals and Techniques • Analog and digital signal • Data-rate-limits	S1:58-80
6.	1	• Digital to digital line encoding schemes	S1:101-120
7.	1	• Pulse code modulation	S1:121-131
8.	1	• Parallel and serial transmission	S1:131-135
9.	1	Recapitulation and discussion of important questions	
	Total no. of Hours planned for Unit – I		9
		UNIT II	
1.	1	Digital to analog modulation Multiplexing techniques • Frequency-Division Multiplexing	S1 : 141-146 S1:161-167
2.	1	• Time-Division Multiplexing	S1:169-180
3.	1	Transmission media • Guided Media • Unguided Media	S1:191-192 S1:193-202 S1:204-207.W2

4.	1	Networks Switching Techniques and Access mechanisms • Introduction • Circuit switching	S1 : 213 – 230 S2:: 110 – 112, W3
5.	1	• Packet switching • A comparison of circuit-switched and packet-switched networks	S1 : 233 – 235 S2 : 112 – 113, W3
6.	1	• Connectionless datagram switching	S1 : 218 – 221
7.	1	• Connection-oriented virtual circuit switching	S1 : 222 - 227
8.	1	Dial-up modems • Digital subscriber line • Cable TV for data transfer	S1 : 248 – 261, W3
9.	1	Recapitulation and discussion of important questions.	
	Total no. of Hours planned for Unit-II		9
UNIT - III			
1.	1	Data Link Layer Functions and Protocol • Types of Error	S1 : 267 - 271
2.	1	• Error detection and error correction	S1:272-277
3.	1	Error detection and error correction techniques • Cyclic Redundancy Check with example	S1:284-297 S2:143-144
4.	1	Data-link control • Introduction to data link control functions • Framing • Flow control	S1:307-310 S1:311-314
5.	1	Introduction to Protocol	W1
6.	1	Stop-and-Wait Protocol • Automatic Repeat Request	S1 : 315 – 322 S2 : 151 - 155
7.	1	Go-Back-N Protocol • Automatic Repeat Request	S1 : 324 – 331 S2 : 158 - 161
8.	1	Point to Point Protocol on Internet • Framing • Transition Phases	S1 : 346 - 350
9.	1	• Multiplexing • Multilink PPP	T1 : 350 - 355
10.	1	Recapitulation and discussion of important questions	
	Total no. of Hours planned for Unit – III		10
UNIT - IV			
1.	1	Multiple Access Protocol and Networks	S1 : 370 - 378

		• CSMA/CD protocols • Carrier Sense Multiple Access with Collision Detection • Carrier Sense Multiple Access with Collision Avoidance	
2.	1	Ethernet LANS • Standard Ethernet	S1 : 395 – 419
3.	1	Connecting LAN and back-bone networks • Repeaters • Hubs • Switches • Bridges • Router and Gateways	S1 : 445 - 456
4.	1	Networks Layer Functions and Protocols • Distance Vector Routing Network layer protocol of Internet • Internet Working • Addressing and routing	S1 : 660 – 673 S1 : 579 – 581, W4 S2 : 339 - 345
5.	1	• IVP4	S1 : 582 – 584
6.	1	• IVP6	S1 : 596 – 600
7.	1	Internet control protocols	T1 : 621 - 626
8.	1	Internet control message protocols (ICMP)	W2
9.	1	Internet Group Management protocols (IGMP)	T1 : 630 - 637
10.	1	Recapitulation and discussion of important questions	
	Total no. of Hours planned for Unit – IV		**10**
UNIT - V			
1.	1	Transport Layer Functions and Protocols • Transport services • Process-to-Process Communication • Stream Delivery Service • Full-Duplex Communication	S1 : 707 - 715
2.	1	• Flow Control • Error Control Connection establishment and release • Three way handshake	S1 : 728 – 735 S2 : 409 - 411
3.	1	Overview of Application layer protocol Overview of DNS protocol	S1 : 797 – 809 S2 : 441 - 447
4.	1	DNS Messages	S1 : 810 - 812

		• Types of records Registrars	
5.	1	Overview of WWW &HTTP protocol • Architecture • Web Documents	S1 : 851 - 860
6.	1	HTTP • HTTP Transaction • Persistent Versus Nonpersistent Connection • Proxy Server	S1 : 861 – 868 S2 : 499 - 504
7.	1	Recapitulation and discussion of important questions	
8.	1	Previous ESE Question Paper Discussion	
9.	1	Previous ESE Question Paper Discussion	
10.	1	Previous ESE Question Paper Discussion	
	Total no. of Hours planned for Unit – V		**10**
	Total no. of Hours planned:		**48 hours**

Suggested readings

S1: 1. B. A Forouzan (2012). Data Communications and Networking(4th ed.). THM.

S2: 2. A. S.Tanenbaum, (2002). Computer Networks (4th ed.). PHI.

Web Sites

W1: https://www.tutorialspoint.com/data_communication_computer_network
W2: https://en.wikipedia.org/wiki/Computer_network
W3: https://en.wikipedia.org/wiki/Network_switch
W4: https://en.wikipedia.org/wiki/Internet_Protocol

FACULTY **HOD**

UNIT I
SYLLABUS

Introduction to Computer Networks : Network definition; network topologies; network classifications; network protocol; 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;

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

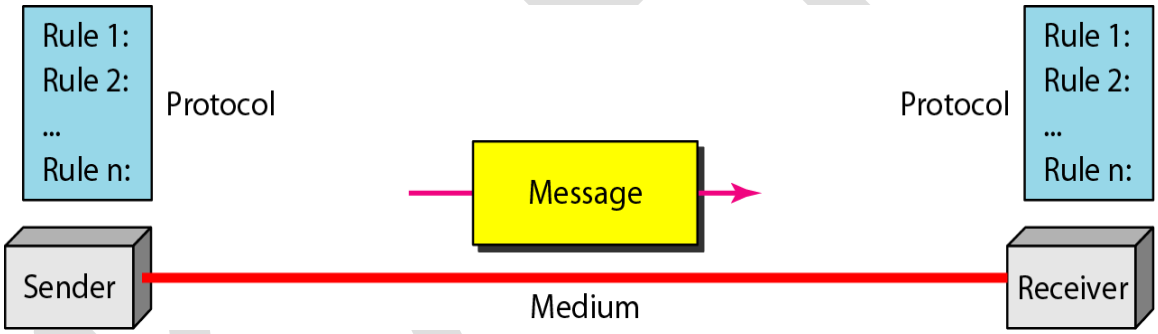
Networks exist so that data may be sent from one place to another. It is the exchange of data between two devices via some form of transmission medium such as a wire cable.

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

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



Data representation

• Text: bit pattern

• ASCII: 128 different symbols (7 bits)

• Extended ASCII: size of each pattern is 1 byte (8 bits)

• Unicode: 65.536 symbols (16 bits)

• ISO: 4.294.967.296 symbols (32 bits)

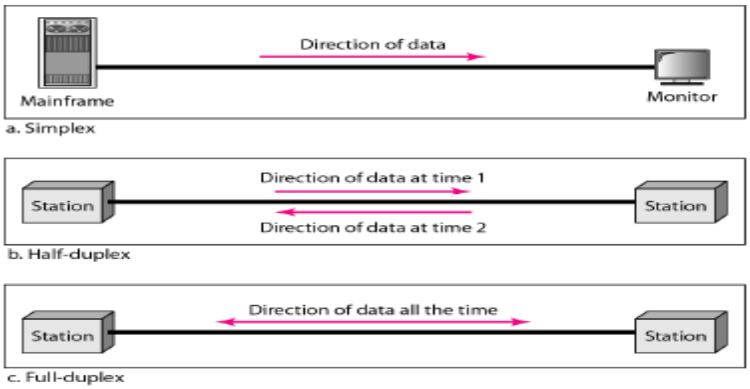
• Numbers: decimal numbers converted directly to binary

• Images: divided into a matrix of pixels

• Audio: representation of sound by an analog or a digital signal

• Video: represented by an analog or digital signal

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

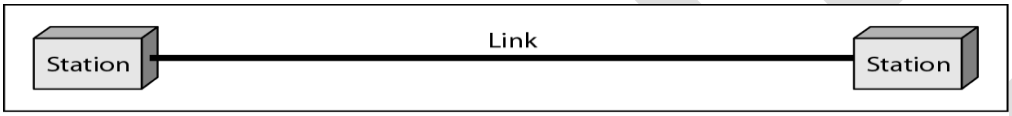
—A measure of frequency of failure and the time needed to recover, network robustness

- Security

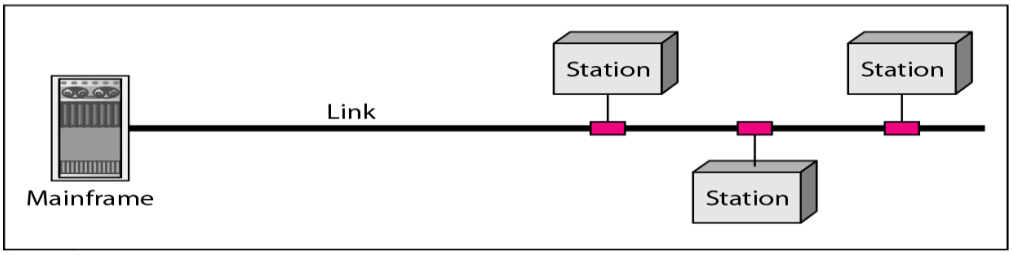
—Protecting of data from unauthorized users

Physical Structures

Types of connections: point-to-point and multipoint



a. Point-to-point



b. 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. When you change television channels by infrared remote control, you are establishing a point-to-point connection between the remote control and the television's control system.

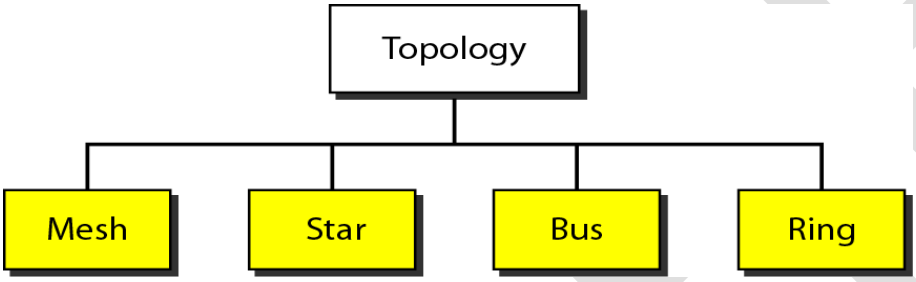
b) Multipoint A multipoint (also called multi drop) connection is one in which more than two specific devices share a single link. In a multipoint environment, the capacity of the channel is shared, either spatially or temporally. If several devices can use the link

simultaneously, it is a *spatially shared* connection. If users must take turns, it is a *timeshared* connection.

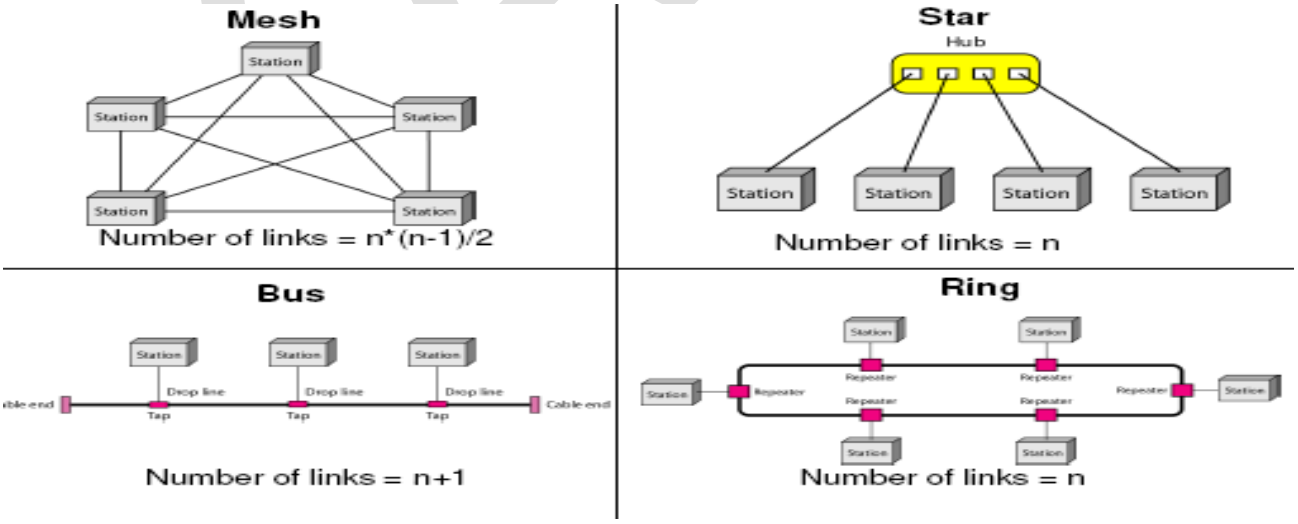
Physical Topology

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)



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.

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.

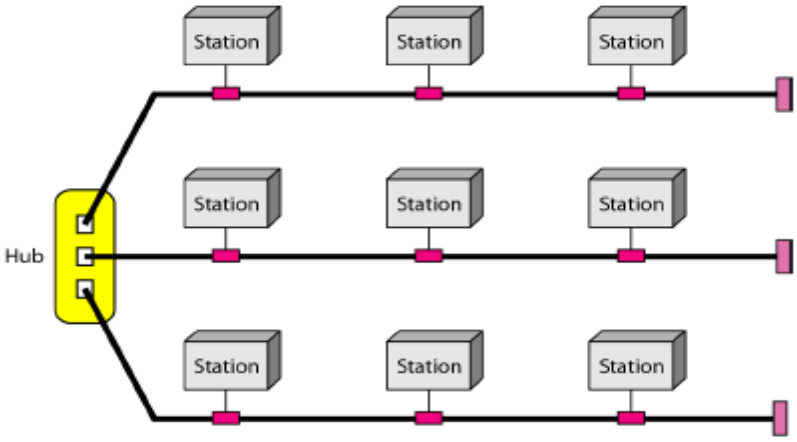
A ring is relatively easy to install and reconfigure. Each device is linked to only its immediate neighbors (either physically or logically). To add or delete a device requires changing only two connections. The only constraints are media and traffic considerations (maximum ring length and number of 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

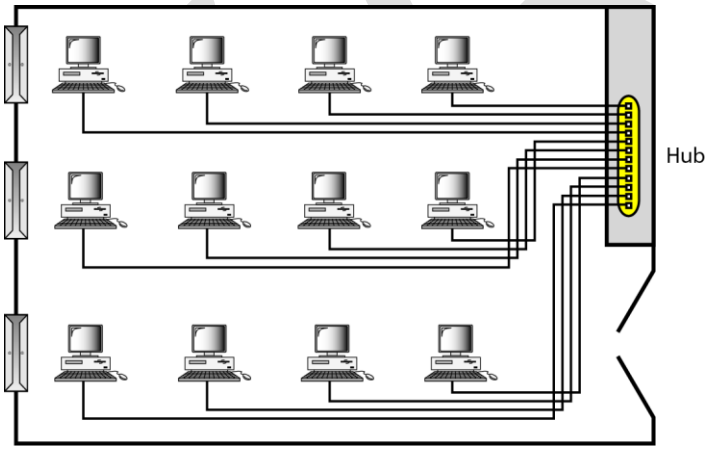
A network can be hybrid. For example, we can have a main star topology with each branch connecting several stations in a bus topology as shown in Figure below.

A star backbone with three bus networks



Categories of networks

• Local Area Networks (LANs)



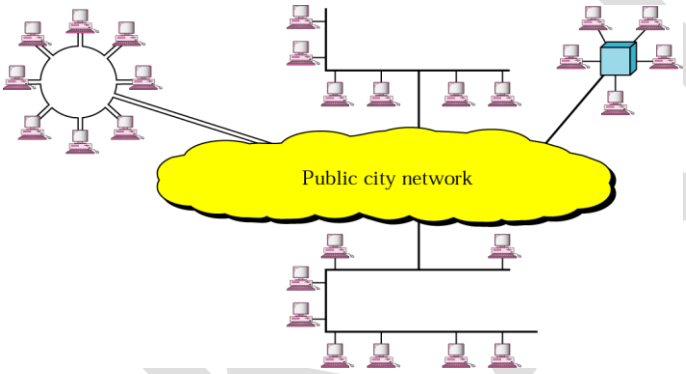
A local area network (LAN) is usually privately owned and links the devices in a single office, building, or campus. Depending on the needs of an organization and the type of technology used, a LAN can be as simple as two PCs and a printer in someone's home office; or it can extend throughout a company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

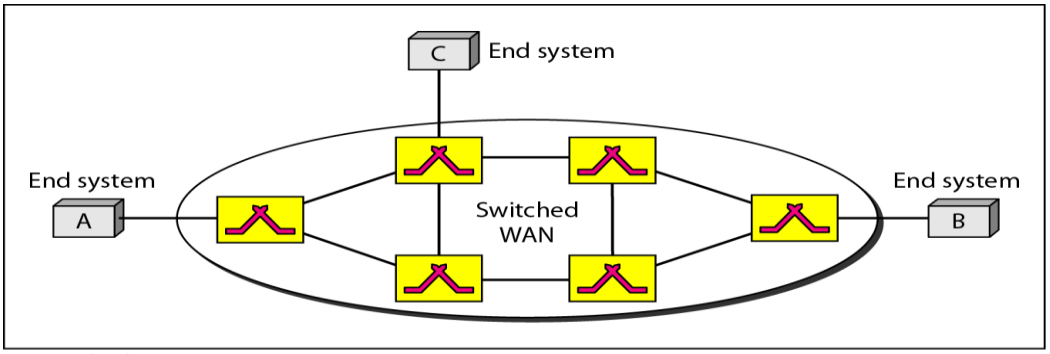
In addition to size, LANs are distinguished from other types of networks by their transmission media and topology. In general, a given LAN will use only one type of transmission medium. The most common LAN topologies are bus, ring, and star. Early LANs had data rates in the 4 to 16 megabits per second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

Metropolitan Area Networks (MANs)

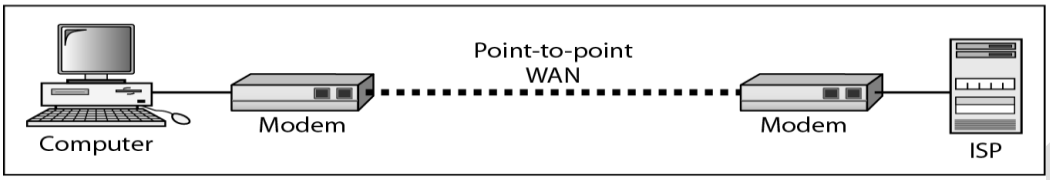


A metropolitan area network (MAN) is a network with a size between a LAN and a WAN. It normally covers the area inside a town or a city. It is designed for customers who need a high-speed connectivity, normally to the Internet, and have endpoints spread over a city or part of city. A good example of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

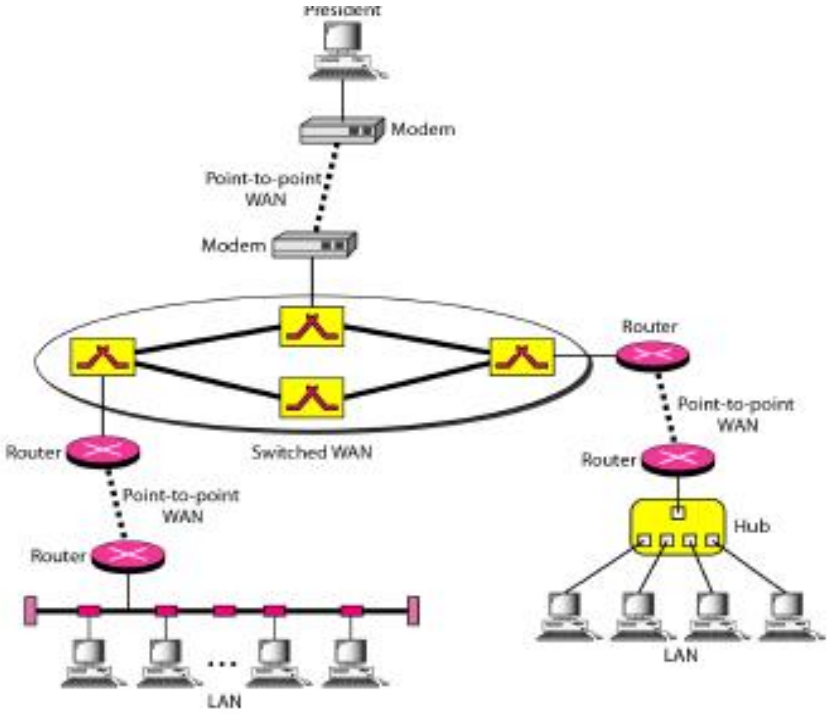
- The switched WAN connects the end systems, which usually comprise a router (internetworking connecting device) that connects to another LAN or WAN.
- The point-to-point WAN is normally a line leased from a telephone or cable TV provider that connects a home computer or a small LAN to an Internet service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

—De facto:

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

—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 worls to another can be broken into several tasks, each performed by a separate software package

• Each piece of software uses the services of another softwarepackage o do its job

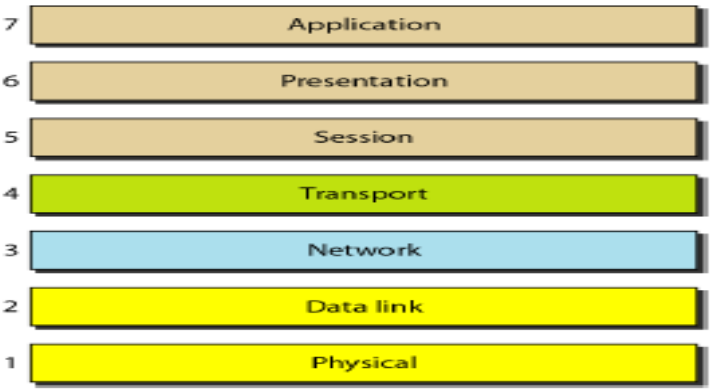
• At the lowest layer, a signal is sent from the source to the destination computer

THE OSI MODEL

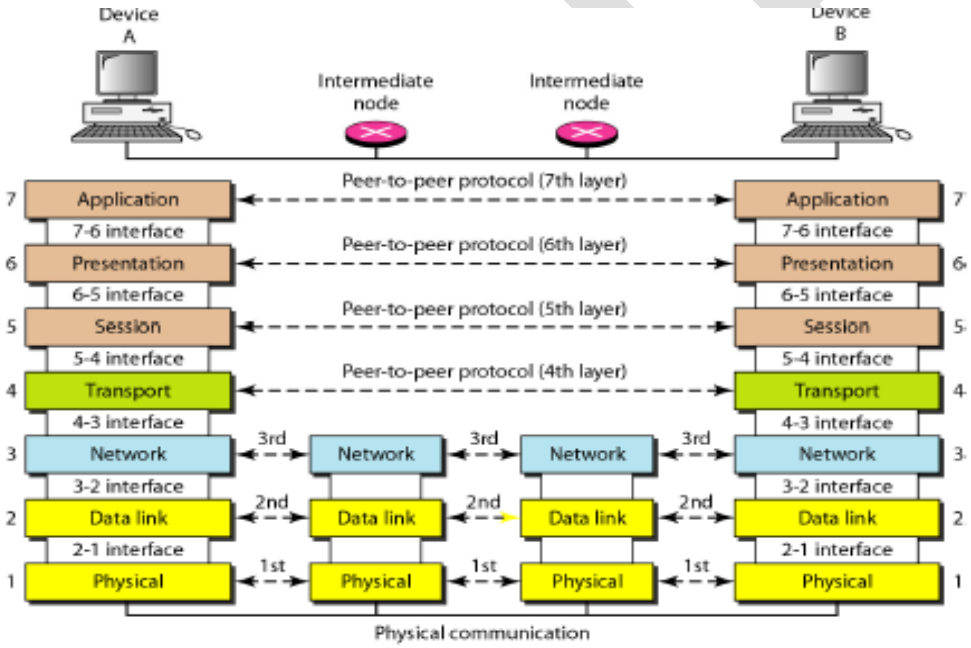
Established in 1947, the International Standards Organization (ISO) is a multinational body dedicated to world wide agreement on international standards.

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.

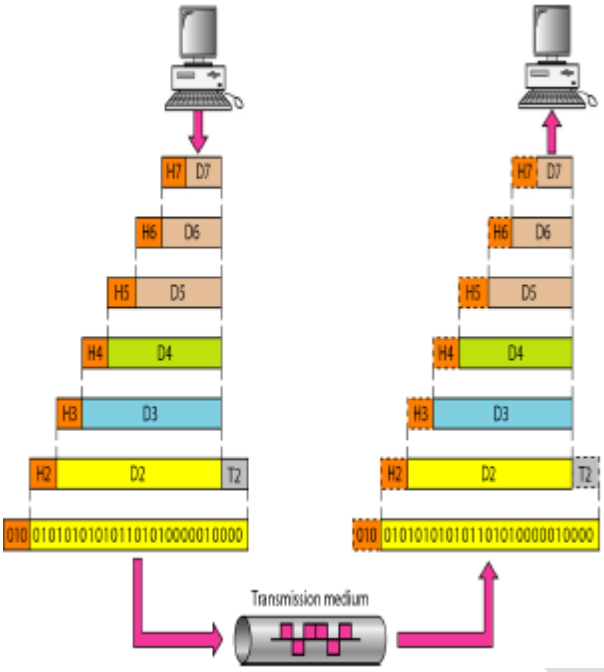
Seven layers of the OSI model



Peer-to-peer processes



Encapsulation

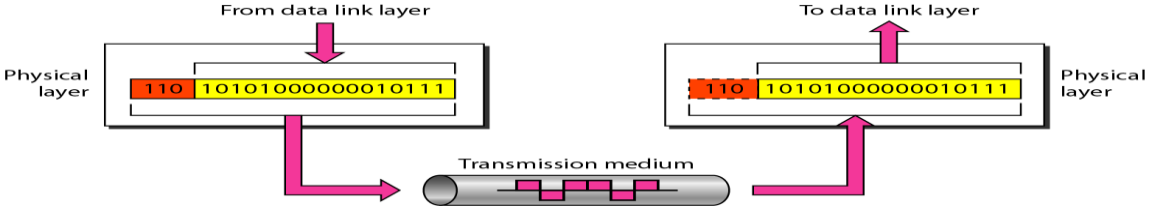


- The process starts at layer 7 (application layer), then moves from layer to layer in descending, sequential order.
- At each layer, a **header** is added to the data unit.
- At layer 2, a **trailer** is added as well.
- When the formatted data unit passes through the physical layer (layer 1) it is 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



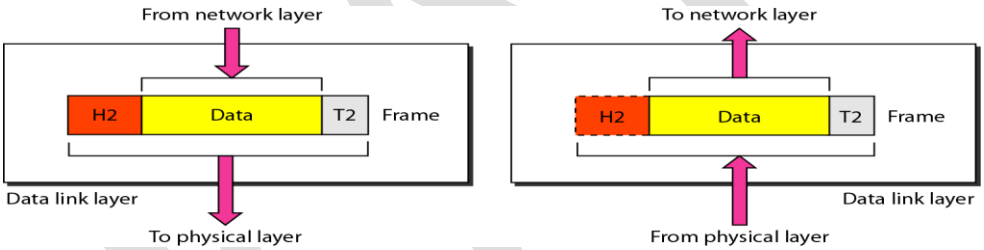
- The physical layer is responsible for movements of individual bits from one hop (node) to the next
- Mechanical and electrical specification, the procedures and functions

Duties:

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

Data link layer

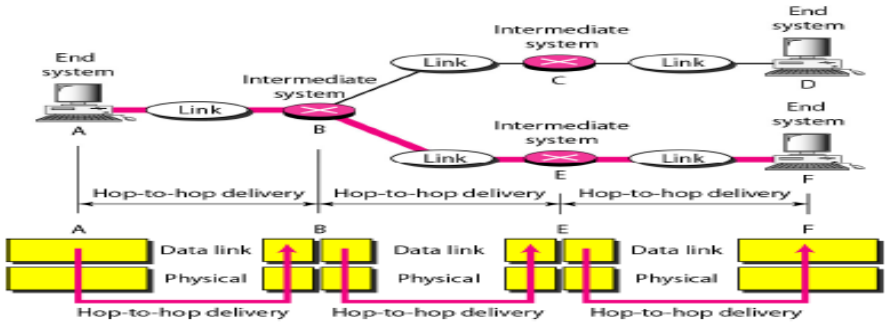
- The data link layer is responsible for moving frames from one hop (node) to the next
- Transform the physical layer to a reliable (error-free) link



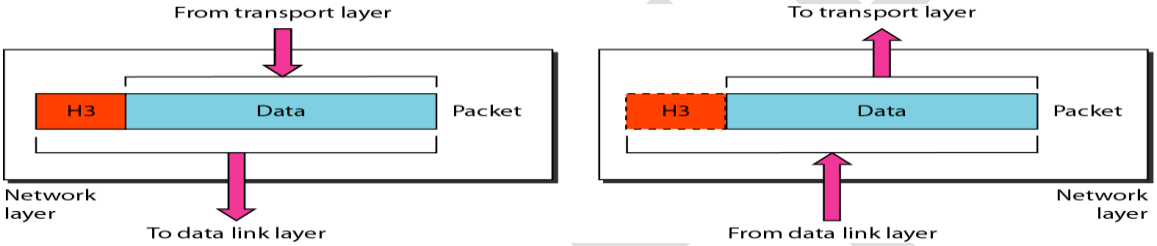
Duties:

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

Hop-to-hop delivery



Network layer

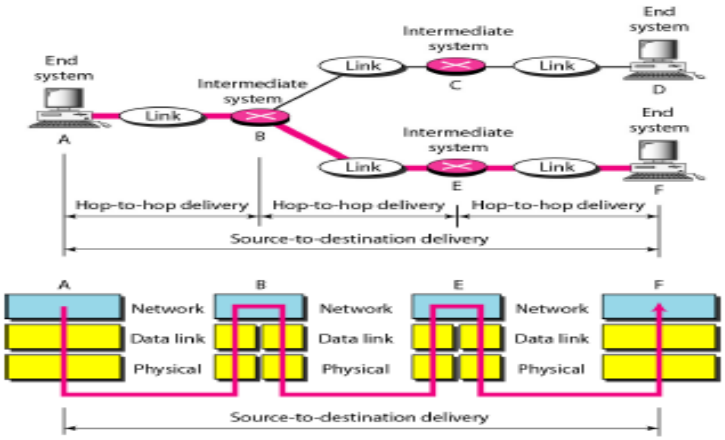


The network layer is responsible for the delivery of individual packets from the source host to the destination host.

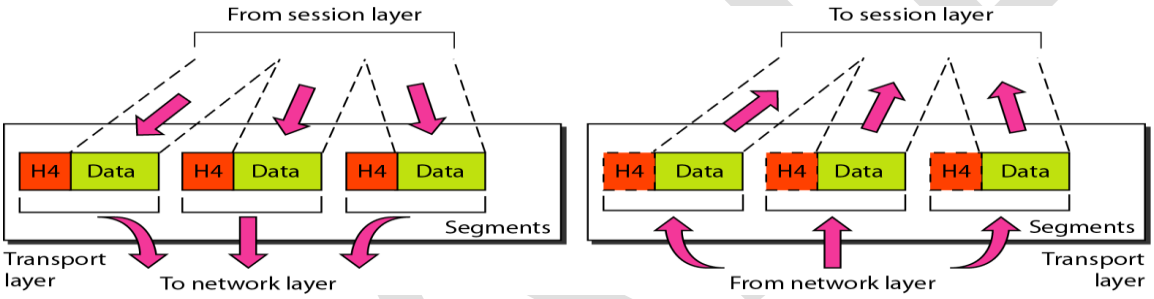
Duties:

- Logical addressing
- Routing

Source-to-destination delivery



Transport layer

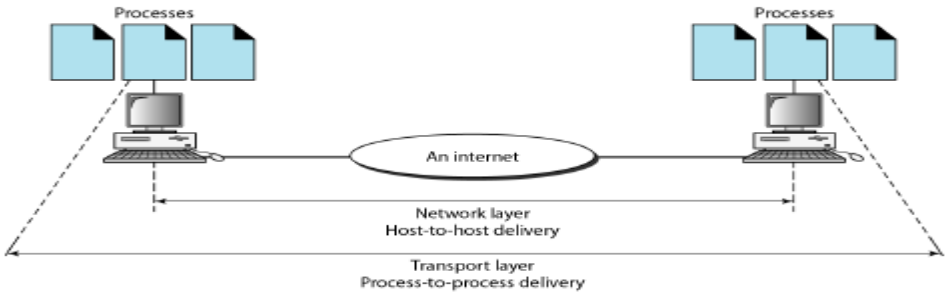


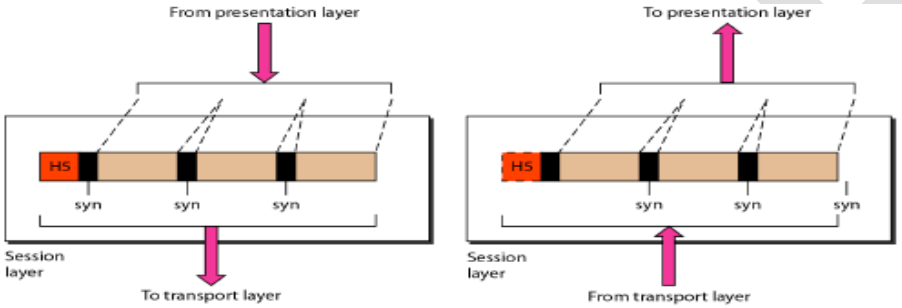
The transport layer is responsible for the delivery of a message from one process to another.

Duties:

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

Reliable process-to-process delivery

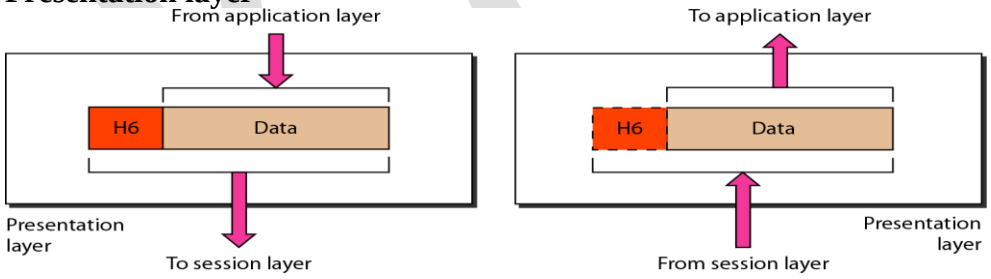




Session layer

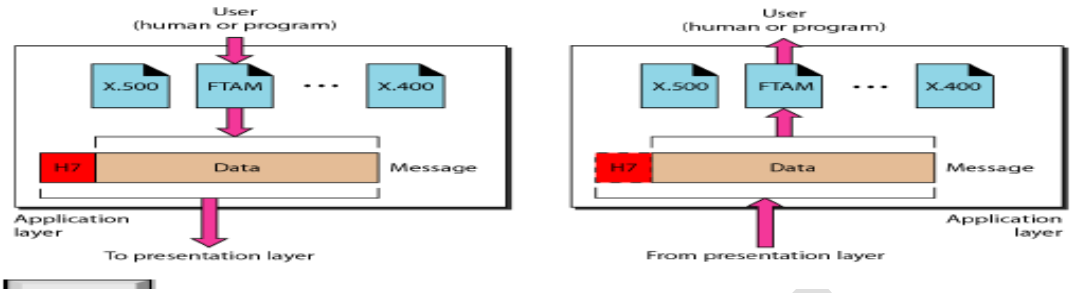
The session layer is responsible for dialog control and synchronization.

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:

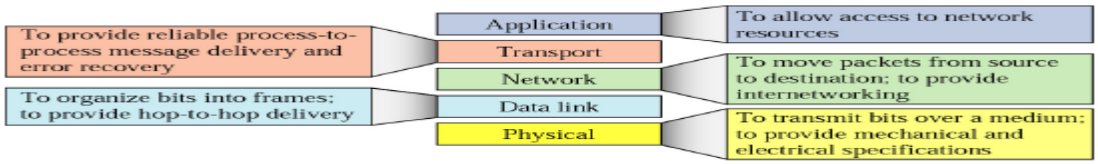
- Network virtual terminal
- Mail services
- File transfer, access, and management
- Directory services

TCP/IP PROTOCOL SUITE

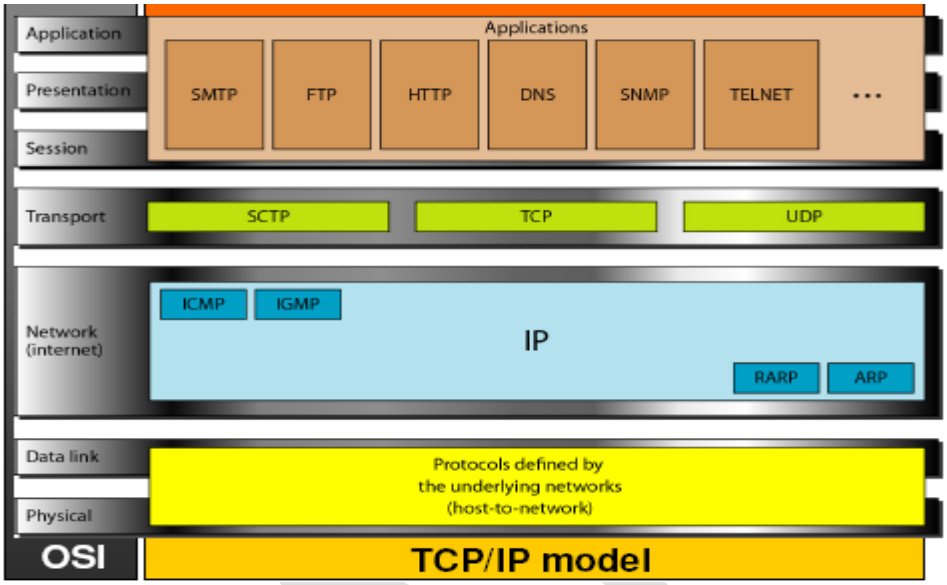
The layers in the TCP/IP protocol suite do not exactly match those in the OSI model. The original TCP//IP protocol suite was defined as having four layers:: host-to-network, internet, transport, and application. However, when TCP/IP is compared to OSI, we can say that the TCP/IP protocol suite is made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

physical, data link, network,, transport, and application.

TCP/IP layers

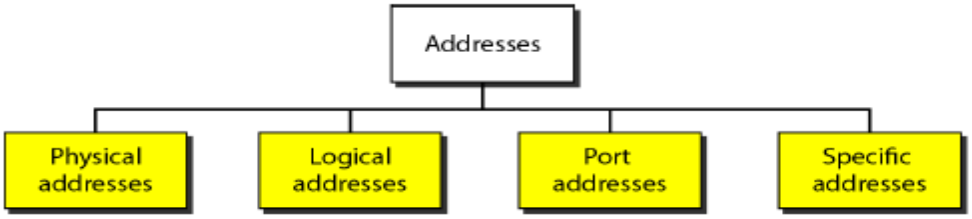


TCP/IP and OSI model



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.

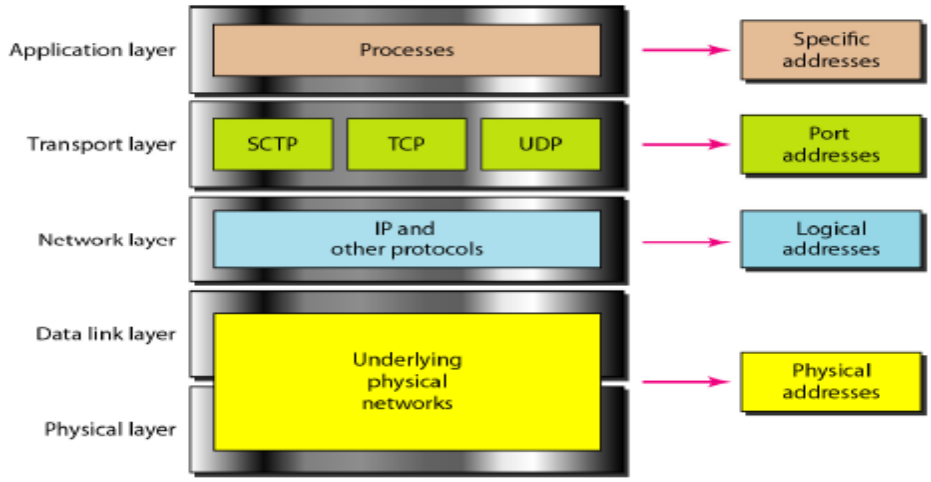
• The Registered Ports are those in the range 1024–49151.

• 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



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.

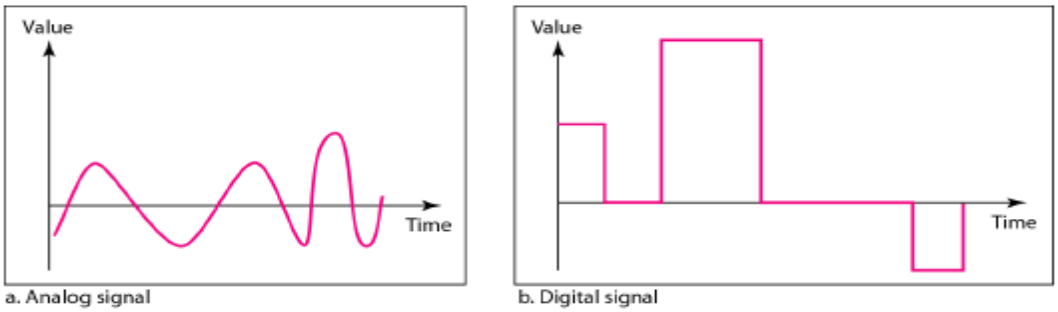
Digital data have discrete states and take discrete values.

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

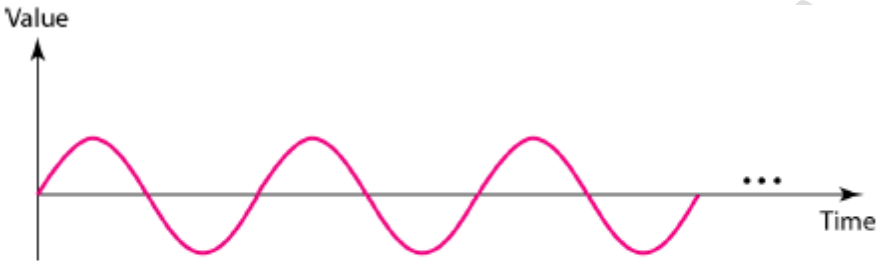
Note

In data communications, we commonly use periodic analog signals and nonperiodic digital signals.

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



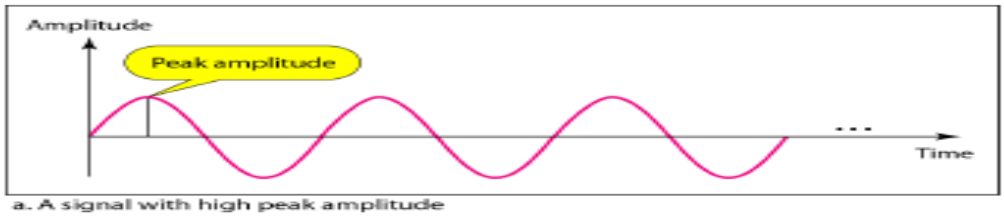
We can mathematically describe the sine wave as

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

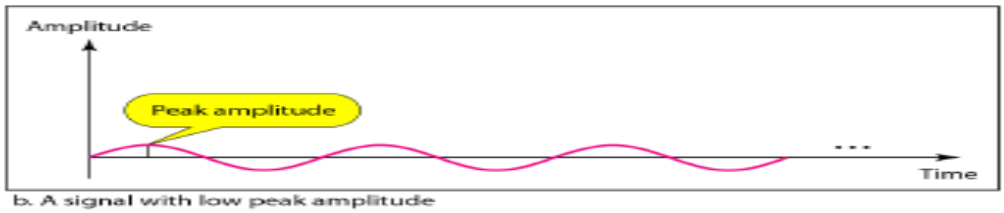
where, s is the instantaneous amplitude
A is the peak amplitude
f is the frequency
φ is the phase
t is the time
π is a constant (~3.14159)

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)

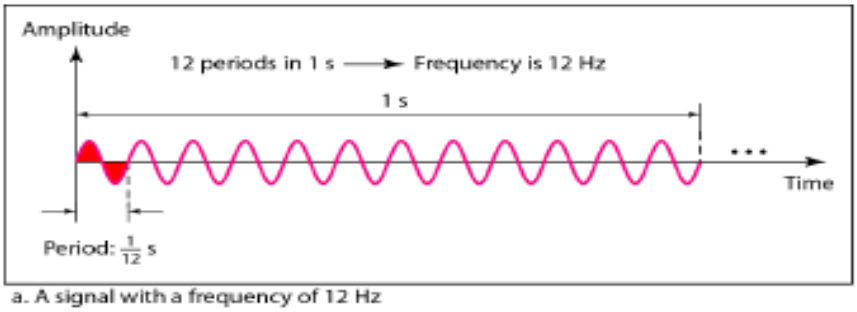
Note

Frequency and period are the inverse of each other.

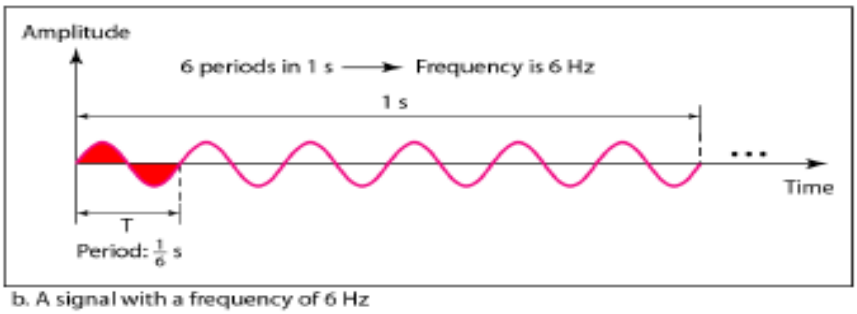
$$f = \frac{1}{T} \qquad \text{and} \qquad T = \frac{1}{f}$$

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.**

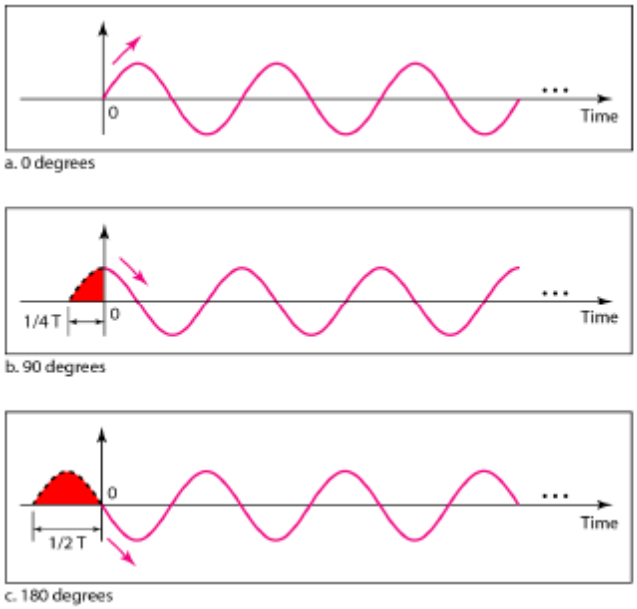
- **If a signal changes instantaneously, its frequency is infinite.**

Phase

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

Three sine waves

Same amplitude and frequency, but different phases

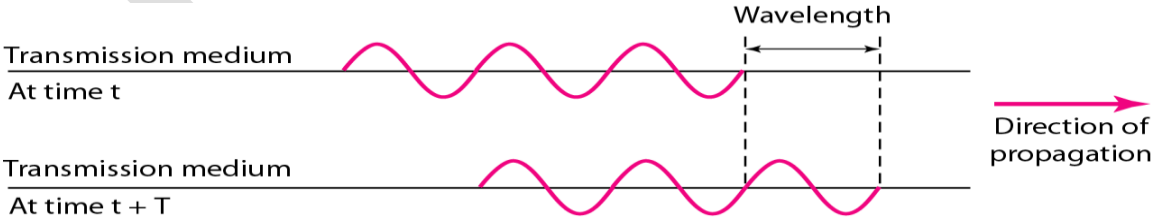


Wavelength and period

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.



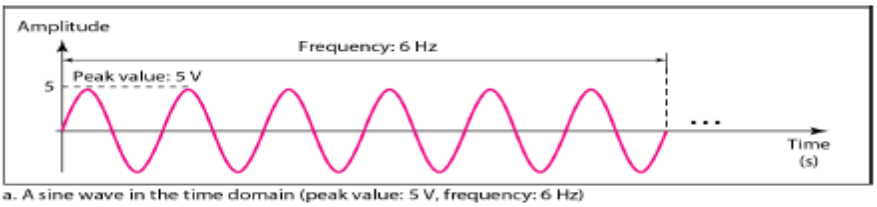
$$\lambda = c/f$$

where, λ is the wavelength

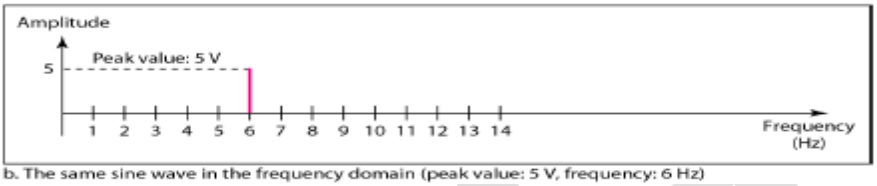
c is the speed of light (~3x108 m/s)

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)

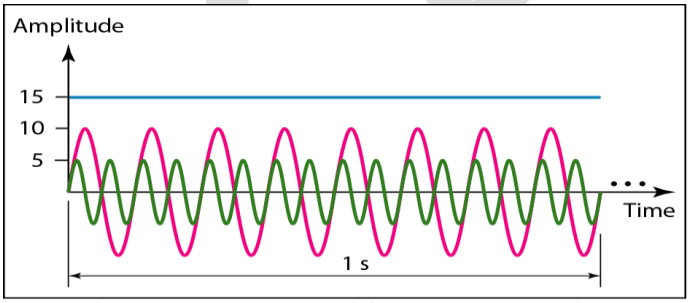


b. The same sine wave in the frequency domain (peak value: 5 V, frequency: 6 Hz)

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**.**

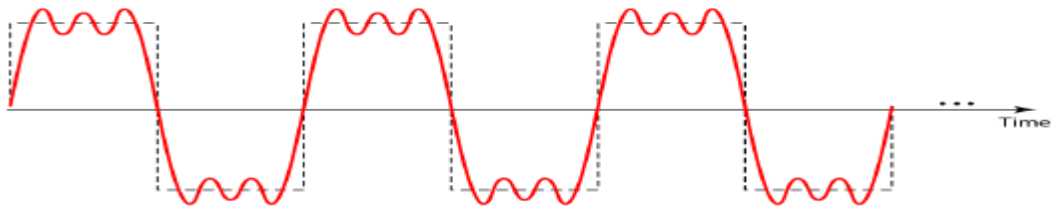
We can use a mathematical technique called **Fourier analysis** to show that any **periodic** signal

is made up of an infinite series of sinusoidal frequency components.

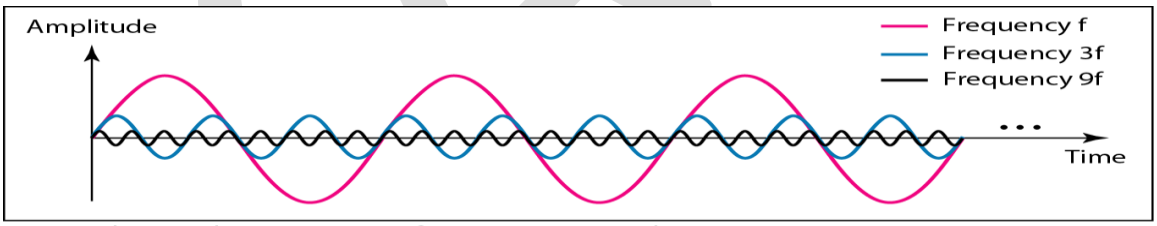
If the composite signal is periodic, the decomposition gives a series of signals with discrete frequencies; if the composite signal is nonperiodic, the decomposition gives a combination of sine waves with continuous frequencies.

Example

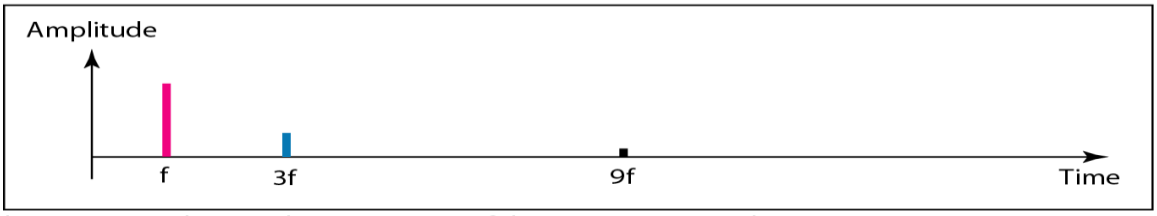
The figure shows a periodic composite signal with frequency ***f***. This type of signal is not typical of those found in data communications. We can consider it to be three alarm systems, each with a different frequency. The analysis of this signal can give us a good understanding of how to decompose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



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



a. Time-domain decomposition of a composite signal

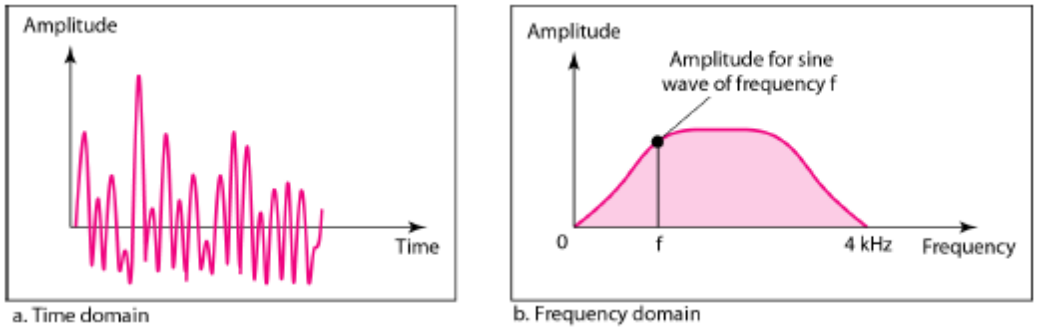


b. Frequency-domain decomposition of the composite signal

Example

The figure shows a nonperiodic composite signal. It can be the signal created by a microphone or

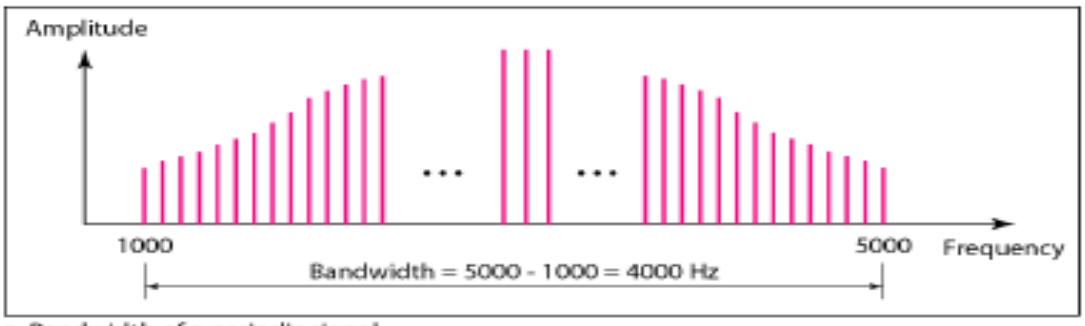
a telephone set when a word or two is pronounced. In this case, the composite signal cannot be periodic, because that implies that we are repeating the same word or words with exactly the same tone.



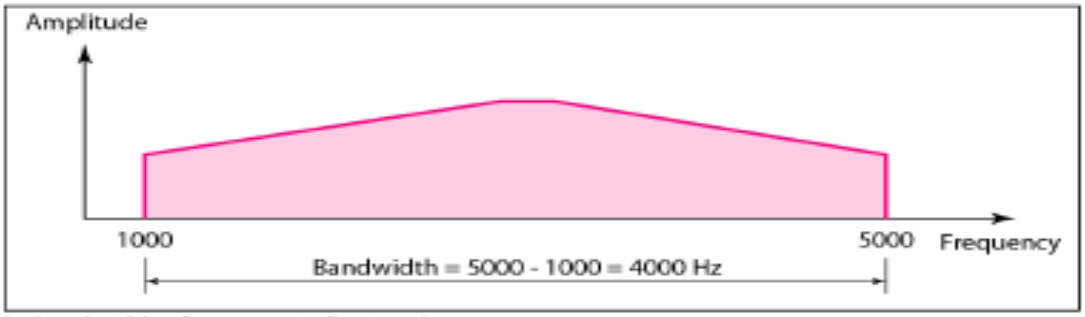
Bandwidth

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

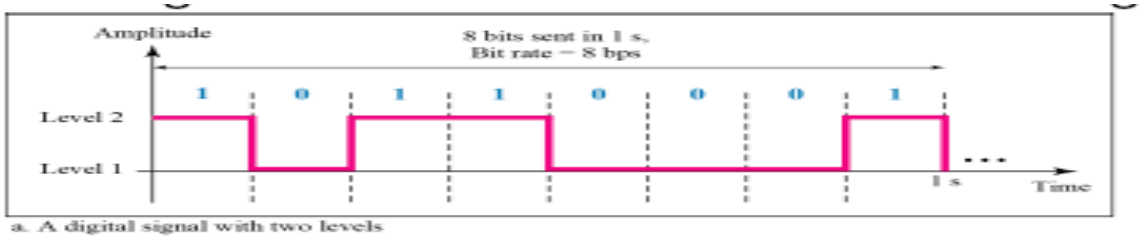


b. Bandwidth of a nonperiodic signal

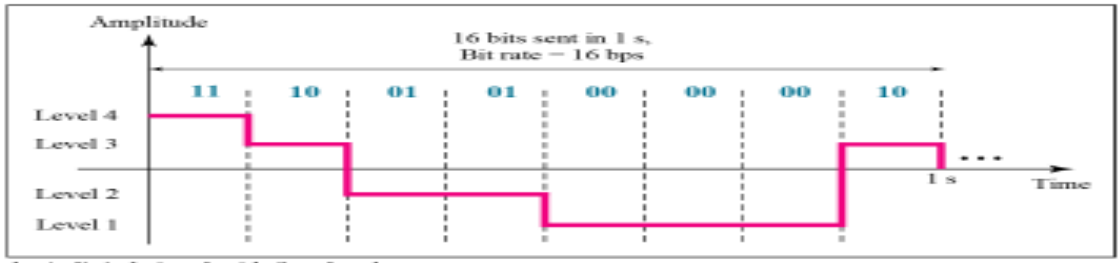
DIGITAL SIGNALS

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.

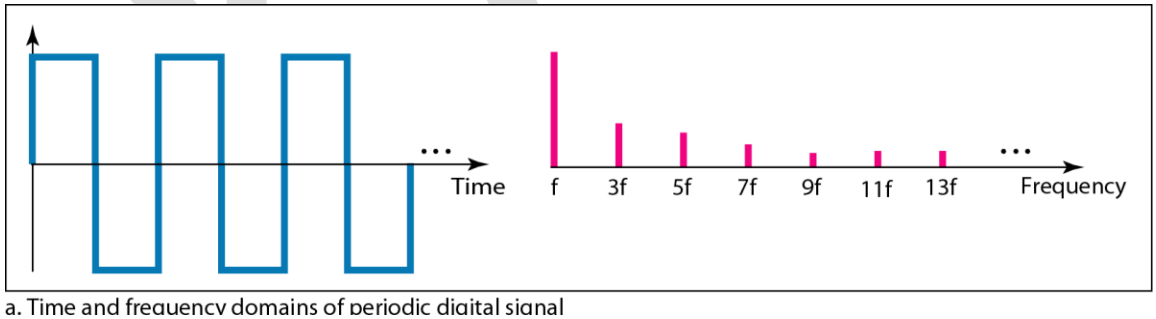
• Bit interval (instead of period) and bit rate (instead of frequency) are used to describe digital signals.

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

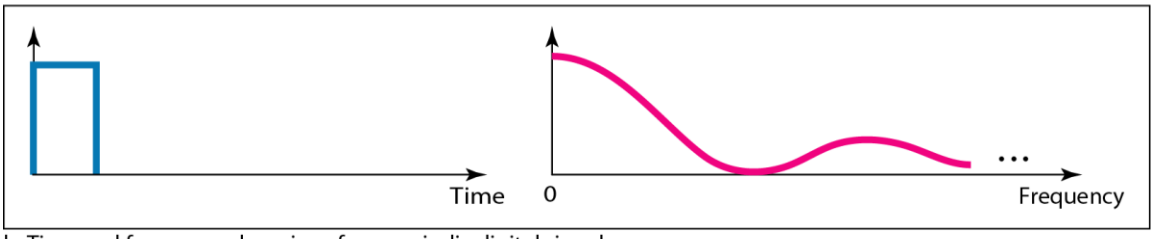
• Bit rate is the number of bit intervals per second

—Usually expressed as bits per second (bps)

The time and frequency domains of periodic and nonperiodic digital Signals

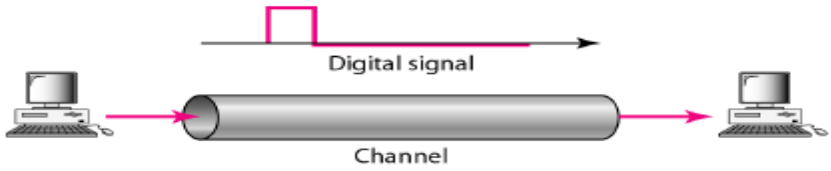


a. Time and frequency domains of periodic digital signal



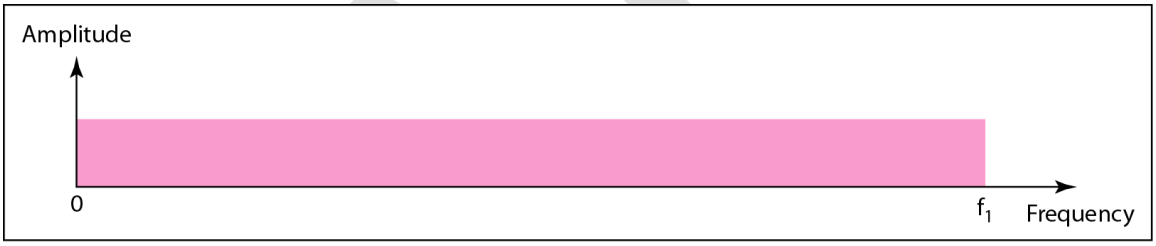
b. Time and frequency domains of nonperiodic digital signal

Baseband transmission



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

Bandwidths of two low-pass channels

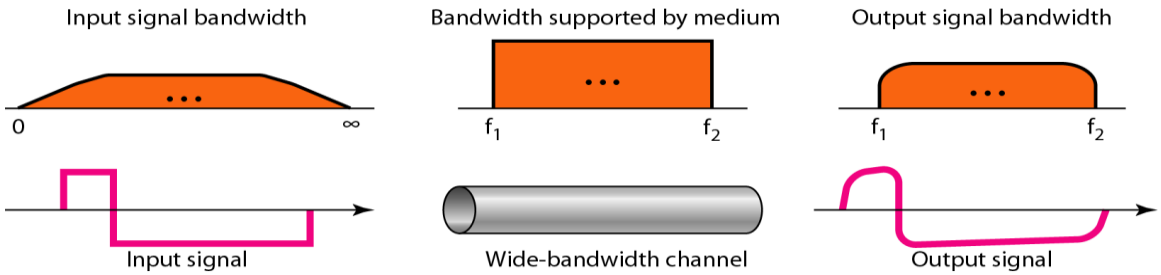


a. Low-pass channel, wide bandwidth

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**.**



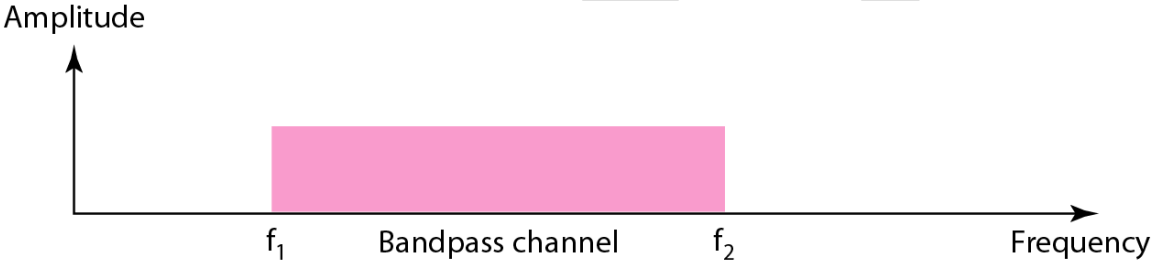
Baseband transmission of a digital signal that preserves the shape of the digital signal is possible only if we have a low-pass channel with an infinite or very wide bandwidth.

Broadband Transmission :

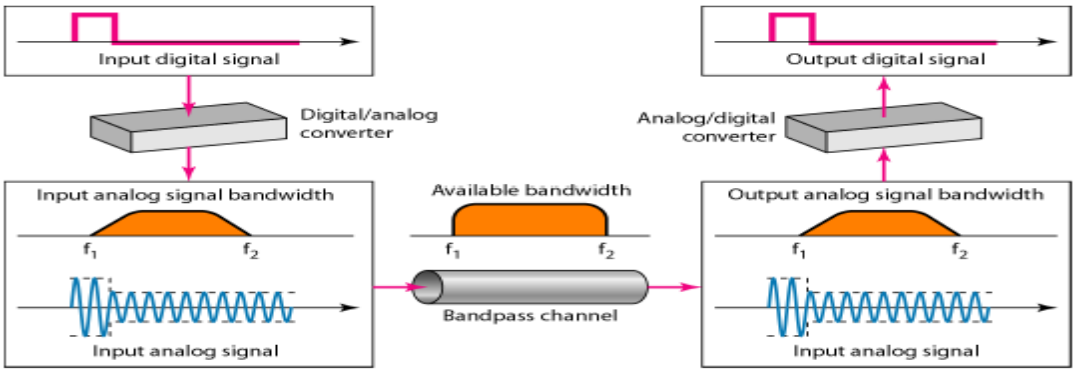
In broadband transmission the signal is converted to analog for transmission.

Bandwidth of a bandpass channel

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



Example

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**.

TRANSMISSION IMPAIRMENT

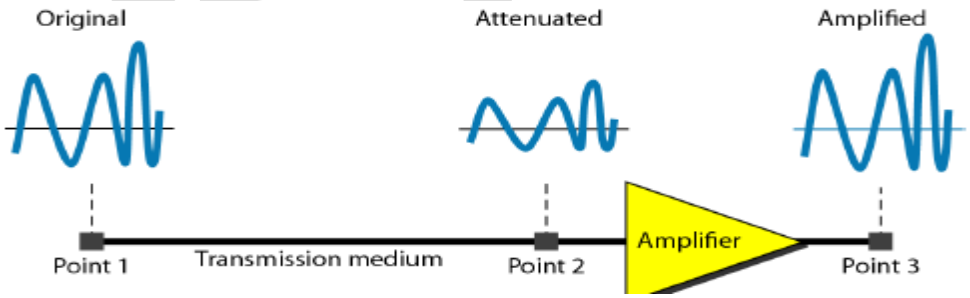
Signals travel through transmission media,, which are not perfect. The imperfection causes signal impairment. This means that the signal at the beginning of the medium is not the same as the signal at the end of the medium.. What is sent is not what is received. Three causes off impairment are attenuation, distortion, and noise.

Attenuation

Attenuation means loss of energy.

When a signal travels through a medium, it looses some of its energy so that it can overcome the resistance of the medium.

To compensate for this loss, amplifiers are used to amplify the signal.



Decibel

To show that a signal has lost or gained strength, we use the concept of the decibel (dB).

• The decibel measures the relative strengths of two signals or a signal at two different points.

• The decibel is negative if a signal is attenuated and positive if a signal is amplified.

$$dB = 10 \log_{10}(P_2/P_1)$$

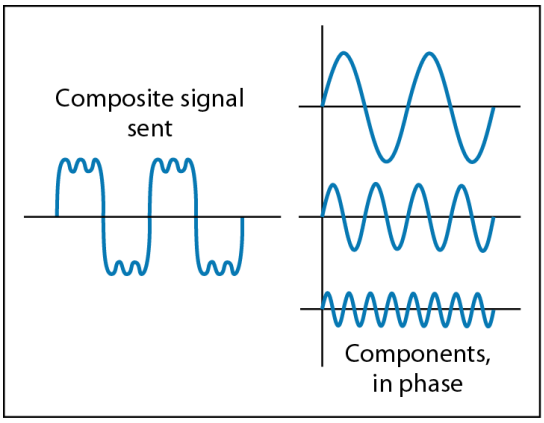
where P1 and P2 are the powers of a signal at points 1and 2, respectively

Distortion

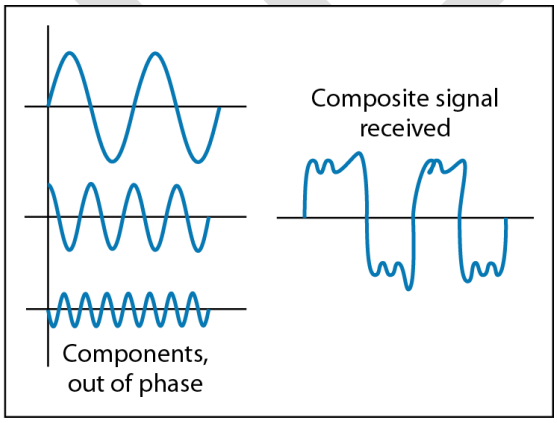
Distortion means that the signal changes its form or shape.

• Distortion occurs in a composite signal made of different frequencies.

• Each signal component has its own propagation speed through a medium and therefore its own delay in arriving at the final destination



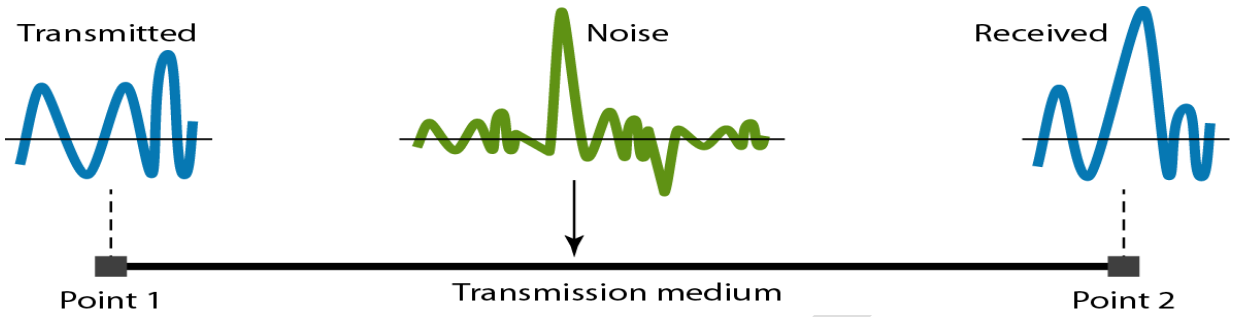
At the sender



At the receiver

Noise

Several types of noise such as thermal noise, induced noise, crosstalk and impulse noise may corrupt the signal.



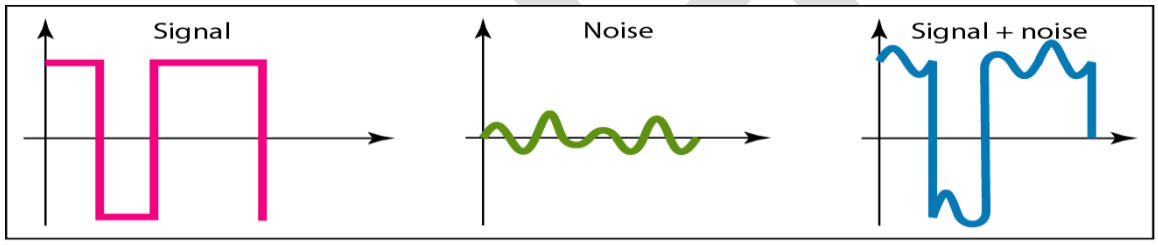
Signal-to-Noise ratio (SNR)

SNR is the statistical ratio of power of the signal to the power of the noise

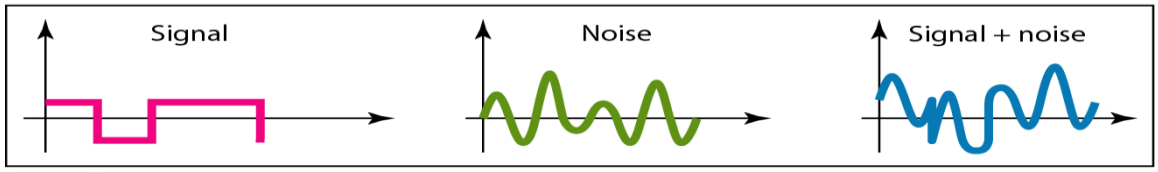
• In decibels it can be expressed as follows:

SNRdB = 10 log10 SNR

Two cases of SNR: a high SNR & a low SNR



a. Large SNR



b. Small SNR

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)

Noiseless channel: Nyquist bit rate

For a noiseless channel, the Nyquist bit rate formula defines the theoretical maximum bit rate

$$C = 2 B \log_2 L$$

where, C is the channel capacity or bit rate in bps

B is the bandwidth in Hz

L is the number of signal levels used to represent data

Noisy channel: Shannon capacity

In reality, we cannot have a noiseless channel; In this case, the Shannon capacity formula is used to determine the theoretical highest data rate for a noisy channel:

$$C = B \log_2 (1+SNR)$$

where, C is the capacity of the channel in bps

B is the bandwidth in Hz

SNR is the signal-to-noise ratio

PERFORMANCE

One important issue in networking is the performance of the network—how good is it? We discuss quality of service, an overall measurement of network performance

Bandwidth

In networking, we use the term bandwidth in two contexts.

- The first, bandwidth in hertz, refers to the range of frequencies in a composite signal or the range of frequencies that a channel can pass.
- The second, bandwidth in bits per second, refers to the speed of bit transmission in a channel or link.

UNIT I

POSSIBLE QUESTIONS

PART-A [20*1=20 Marks]

ONLINE EXAMINATION

PART-B [5*2=10 Marks]

1. What is network and its criteria?
2. Define network topology.
3. Give the network classification.
4. Define protocol.
5. What are the transmission modes?

PART-C [5*6=30 Marks]

1. What is network? Discuss about TCP/IP reference model in detail.
2. Describe about network classification.
3. Discuss in detail about network topology and its types with neat diagrams.
4. Write a detail note on i) LAN ii) MAN
5. Describe about OSI model and its layers with diagrams.
6. Discuss in short about periodic analog signal.
7. Write about the digital signals.

8. Explain in detail about analog signals.
9. Explain in detail about digital to digital conversions.
10. Explain about the transmission modes.

Karpagam Academy of Higher Education

Department of CS, CA & IT

Class: II BSC CT Batch:2017

Subject: COMPUTER NETWORKS

SubCode: 17CTU303

UNIT I

S.NO	QUESTION	CHOICE1	CHOICE2	CHOICE3	CHOICE4	ANSWER
1	Data communication means exchange of data between _____devices.	one	two	six	four	two
2	The combination of two or more networks are called _____	Internetwork	LAN	WAN	MAN	Internetwork
3	A_____ is the set of rules.	protocols	transmission medium	networks	ip	protocols
4	In_____, the communication is unidirection.	duplex mode	full duplex mode	half duplex mode	simplex mode	simplex mode
5	A_____is a set of devices connected by communication links.	protocols	networks	computer	printer	networks
6	A_____connection provides a dedicated link between two devices.	point-to-point	multi-point	mesh	physical	point-to-point
7	One long cable acts as a _____to link all the devices in a network.	bus	mesh	hub	backbone	backbone
8	MAN stands for _____	metropolitician area network	metropolitan area network	metropolitical area network	macro area network	metropolitan area network
9	A _____ can be a device which is capable of sending or receiving data	node	data	bit	link	node
10	The multipoint topology is _____	Bus	Star	Mesh	Ring	Bus
11	In physical layer we can transfer data into _____	frame	packet	bit	sp du	bit
12	A communication path way that transfers data from one point to another is called _____	Link	Node	Medium	Topology	Link

13	The _____layer is responsible for process to process delivery.	physical	presentation	networks	transport	transport
14	The _____layer is responsible for dialog control and synchronization.	transport	session	application	presentation	session
15	Tcp/Ip is a _____protocol.	hyper text	transfer	internet	hierarchical	internet
16	Ip is a_____protocol.	hop to hop	node to node	process to process	host to host	host to host
17	A set of devices connected by a _____links	data	networks	communicatio n	application	communication
18	In _____ topology every device is connected to a single cable	Bus	Star	Ring	Mesh	Bus
19	Periodic analog signals can be classified into _____	simple	composite	simple or composite	simple and composite	simple or composite
20	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
21	Wavelength is_____	propagation speed	propagation speed *	propagation speed/period	propagation speed/frequency	propagation speed/frequenc
22	ISP stands for _____	Internet Service Provider	Internet System	International Service	International System Program	Internet Service Provider
23	The range of frequency contained in a _____ signal is its bandwidth.	simple	composite	periodic	non periodic	composite
24	The bandwidth of the composite signal is the difference between the _____	highest	highest or lowest	highest and lowest	lowest	highest and lowest
25	The _____is the number of bits sent in a second.	bit length	bandpass	bandwidth	bit rate	bit rate
26	Bit length is _____	propagation speed/period	propagation speed *	bit	propagation speed*bit	propagation speed*bit
27	A_____signal is a composite analog signal with an infinite bandwidth	simple	composite	digital	analog	digital
28	Bus topology is also called as_____	Linear Bus Topology	Hybrid Bus Topology	Dual Ring topology	Non Linear Bus Topology	Linear Bus Topology
29	Transmission time=_____	message size/birate	distance/bandw idth	message size/distance	message size/bandwidth	message size/bandwidth

30	_____and star is a point to point device.	bus	ring	mesh	physical	mesh
31	_____ **and** _____ is an example of simplex communication	Keyboard and Monitor	Printer and fax	Mobile and Tab	Bus and ring	Keyboard and Monitor
32	_____is a basic key element.	protocols	standards	topology	protocols and standards	protocols and standards
33	Bit rate=_____	4*BW*log2L	2*BW*log2L	4*BW/L	2*BW*log 4L	2*BW*log2L
34	OSI stands for_____	open systems interconnection	open system internetworkin	open symantic interconnectio	open system internet	open systems interconnection
35	Net work layer delivers data in the form of_____	frame	bits	data	packet	packet
36	Session layer provides_____ services.	one	two	three	four	two
37	UDP stands for _____	user data protocol	user datagram protocol	user defined protocol	user dataframe protocol	user datagram protocol
38	FTP stands for _____	file transmit protocol	file transmission	file transfer protocol	flip transfer protocol	file transfer protocol
39	SMTP stands for _____	single mail transfer protocol	simple mail transfer	simple mail transmission	single mail transmit	simple mail transfer
40	Complete a cycle is called as _____	period	frequency	non periodic	periodic	period
41	_____ generally expands throughout a city such as cable TV network	LAN	WAN	MAN	PAN	MAN
42	_____is reliable and **connection oriented protocol.**	TCP	UDP	FTP	SMTP	TCP
43	Full duplex also called as_____	simple duplex	single duplex	multiple duplex	duplex	duplex
44	_____can be measured in transmit time and response time.	performance	frequency	period	non period	performance
45	A multipoint is also called as_____	multi line	multi drop	multi level	single level	multi drop
46	Mesh has _____ physical channels to link n devices	n(n-1)	n(n+1)	n(n+1)/2	n(n-1)/2	n(n-1)/2

47	A_____topology on the other hand is multipoint.	star	ring	bus	mesh	bus
48	Combination of two or more network topology is called _____	Mesh	Star	Ring	Hybrid	Hybrid
49	A MAN is a network with a size between a _____ and _____.	WAN and LAN	WAN or LAN	LAN	WAN	WAN and LAN
50	_____ refers to information that has discrete states.	Digital data	Analog data	bits	bytes	Digital data
51	The_____layer is responsible for providing services to the user.	presentation	datalink	application	network	application
52	The _____ layer is responsible for translation, compression encryption.	transport	data link	presentation	application	presentation
53	The_____layer is responsible for the delivery of a message from one process to another.	data link	transport	presentation	network	transport
54	A _____layer is responsible for the delivery of packets from the source to destination.	physical	data link	network	session	network
55	The _____layer is responsible for moving frames from one hop to the next.	data link	physical	network	presentation	data link
56	The _____layer is responsible for movements of bits from one hop to next.	data link	physical	transport	session	physical
57	RARP stands for _____	reverse address resolution	reverse address result protocol	reverse addess revolutinized	reverse addess research	reverse address resolution
58	In multicast communication, the relationship is _____	One to one	One to many	Many to one	many to many	One to many
59	The TCP/IP protocol suite was developed prior to the_____model.	OSI	ISO	TCP	IP	OSI
60	The _____layer is responsible for flow control.	session	presentation	application	transport	transport
61	The term _____ data refers to information continous	analog	digital	physical	analog and digital	analog
62	The sine wave is the most fundamental form of a _____analog signal.	composite	single	periodic	non periodic	periodic

UNIT I
SYLLABUS

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

DIGITAL TO ANALOG MODULATION

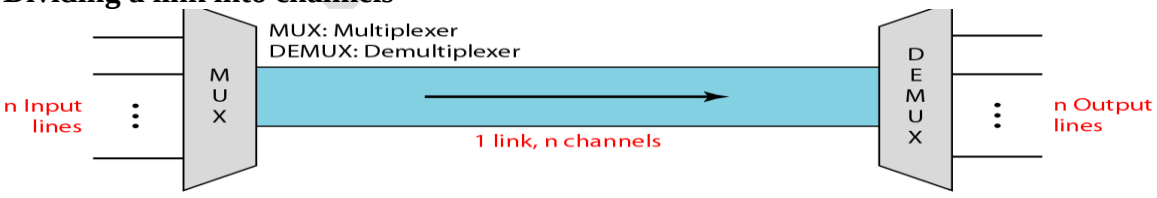
Multiplexing Techniques

Multiplexing is the set of techniques that allows the simultaneous transmission of multiple signals across a single data link.

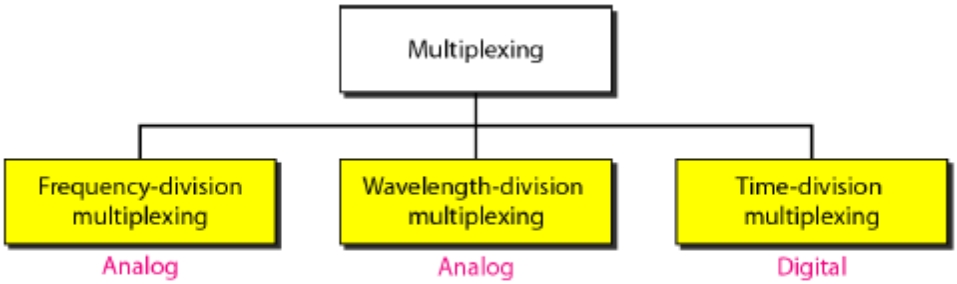
Bandwidth utilization is the wise use of available bandwidth to achieve specific goals. Efficiency can be achieved by multiplexing; privacy and anti-jamming can be achieved by spreading.

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 of techniques that allows the simultaneous transmission of multiple signals across a single data link. As data and telecommunications use increases, so does traffic.
In a multiplexed system, *n* lines share the bandwidth of one link. Figure below 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.

Dividing a link into channels

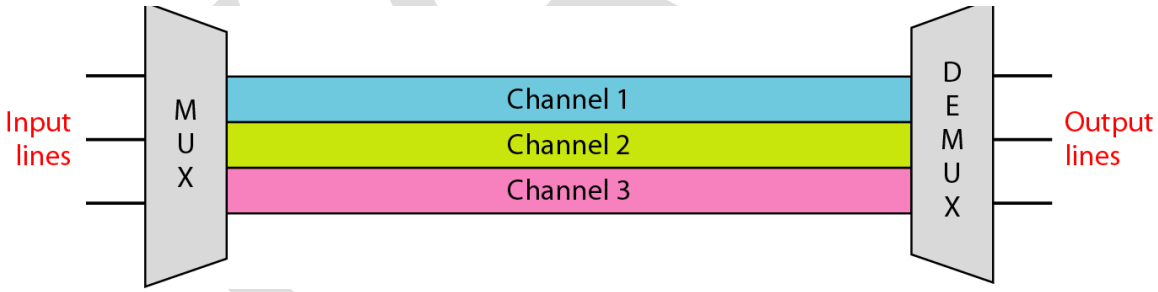


Categories of multiplexing



Frequency Division Multiplexing (FDM)

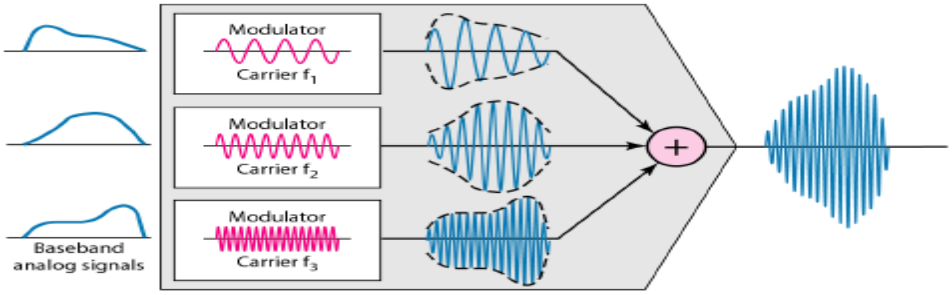
Frequency-division multiplexing (FDM) is an analog technique that can be applied when the bandwidth of a link (in hertz) is greater than the combined bandwidths of the signals to be transmitted. In FOM, signals generated by each sending device modulate different carrier frequencies. These modulated signals 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.



FDM is an analog multiplexing technique that combines analog signals.

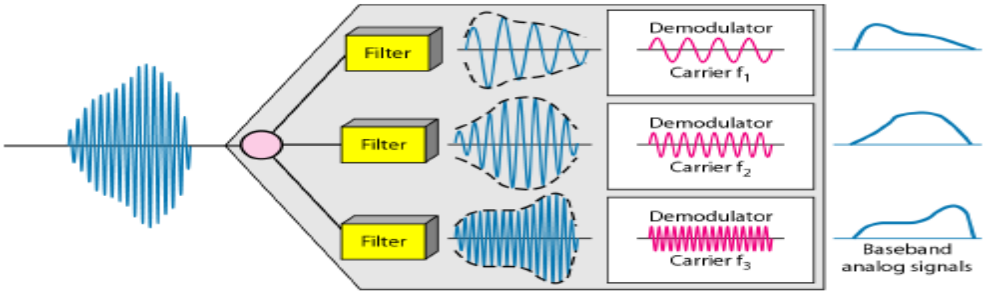
Multiplexing Process

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 *(f1, f2,* and *f3).* The resulting modulated signals are then combined into a single composite signal that is sent out over a media link that has enough bandwidth to accommodate it.



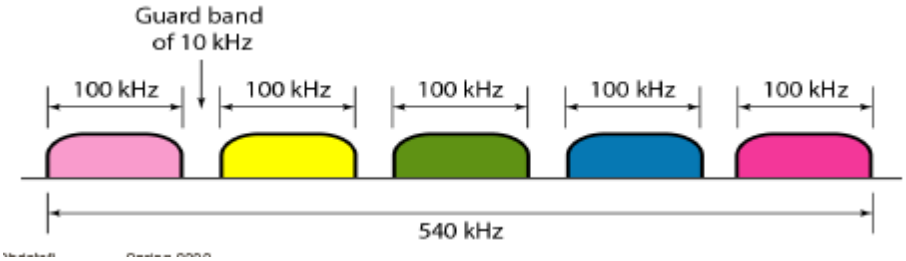
Demultiplexing Process

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. Figure below is a conceptual illustration of demultiplexing process.



Five channels, each with a 100-kHz bandwidth, are to be multiplexed together. What is the minimum bandwidth of the link if there is a need for a guard band of 10 kHz between the channels to prevent interference?

For five channels, we need at least four guard bands. This means that the required bandwidth is at least $5 \times 100 + 4 \times 10 = 540$ kHz as shown in the figure below.



Wavelength Division Multiplexing (WDM)

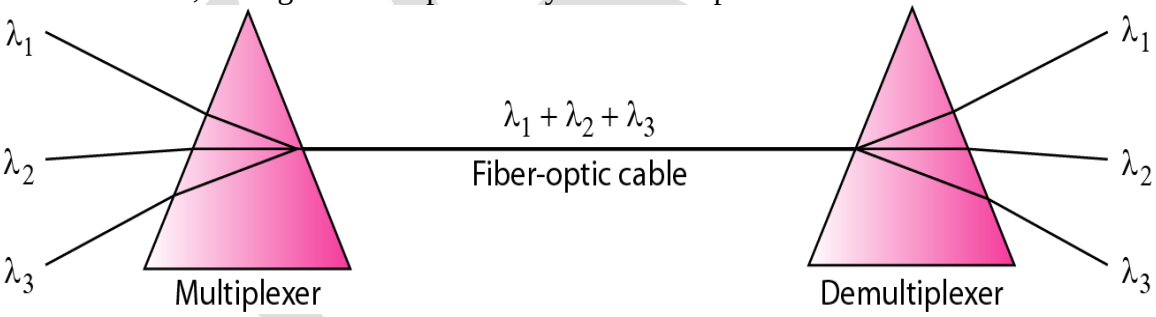
• WDM is designed to use the high data rate capability of fiber optic cable.
• Using a fiber-optic cable for one single line wastes the available bandwidth. Multiplexing allows us to connect several lines into one.
• WDM is conceptually the same as FDM, except that the multiplexing and demultiplexing involve optical signals

Note

WDM is an analog multiplexing technique to combine optical signals.

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

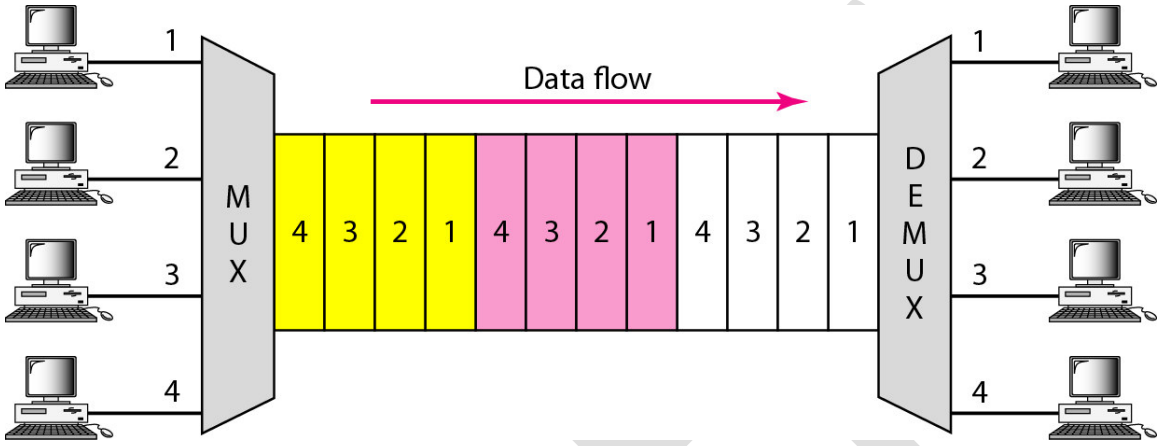
WDM is conceptually the same as FDM, except that the multiplexing and demultiplexing involve optical signals transmitted through fiber-optic channels. The idea is the same: We are combining different signals of different frequencies. The difference is that the frequencies are very high. Figure below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

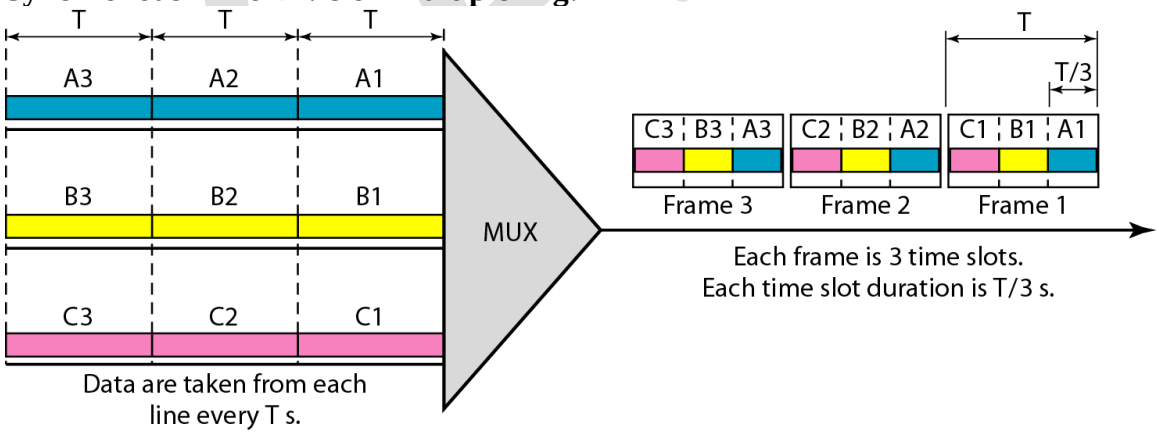
Time Division Multiplexing (TDM)

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 below gives a conceptual view of TDM. 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**.**



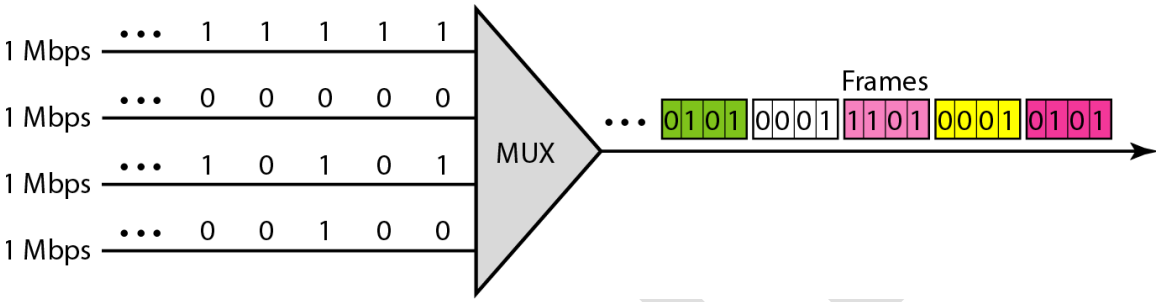
We can divide TDM into two different schemes: synchronous and statistical. We first discuss synchronous TDM and then show how statistical TDM differs. In synchronous TDM, each input connection has an allotment in the output even if it is not sending data. Synchronous Time Division Multiplexing.

Synchronous Time-Division Multiplexing:



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.

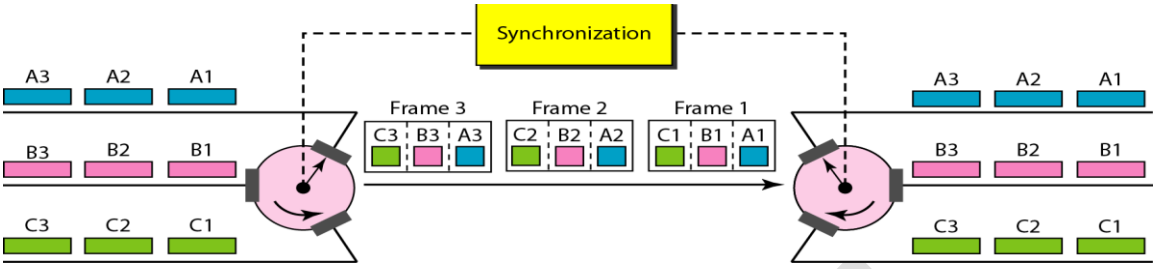


In synchronous TDM, a round of data units from each input connection is collected into a frame. If we have *n* connections, a frame is divided into *n* time slots and one slot is allocated for each unit, one for each input line. If the duration of the input unit is *T*, the duration of each slot is *Tin* 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 6.13, 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.

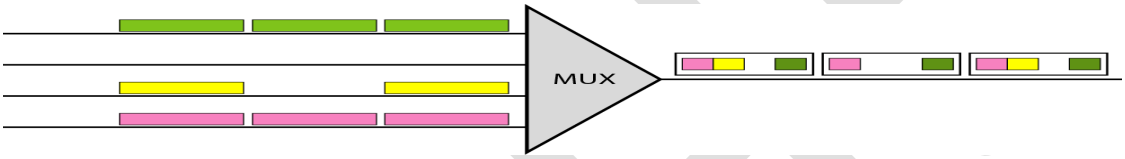
Interleaving

TDM can be visualized as two fast-rotating switches, one on the multiplexing side and the other on the demultiplexing side. The switches are synchronized and rotate at the same speed, but in opposite directions. On the multiplexing side, as the switch opens in front of a connection, that connection has the opportunity to send a unit onto the path. This process is called **interleaving.** On the demultiplexing side, as the switch opens in front of a connection, that connection has the opportunity to receive a unit from the path. Figure shows the interleaving process for the connection. In this figure, we assume that no switching is involved and that the data from the first connection at the multiplexer site go to the first connection at the demultiplexer.



Empty Slots

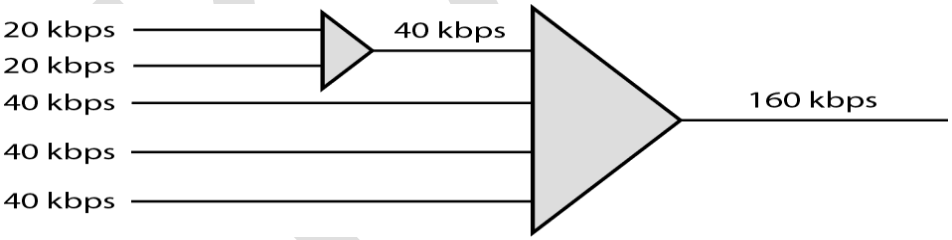
Synchronous TDM is not as efficient as it could be. If a source does not have data to send, the corresponding slot in the output frame is empty. Figure 6.18 shows a case in which one of the input lines has no data to send and one slot in another input line has discontinuous data. The first output frame has three slots filled, the second frame has two slots filled, and the third frame has three slots filled. No frame is full.



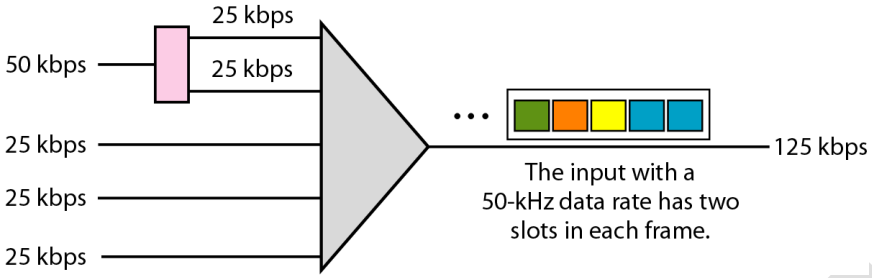
Data Rate Management

One problem with TDM is how to handle a disparity in the input data rates. However, if data rates are not the same, three strategies, or a combination of them, can be used. We call these three strategies **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 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.

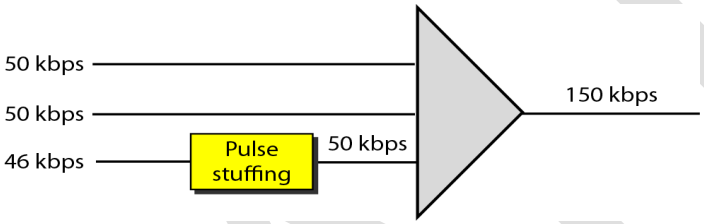


Multiple-Slot Allocation Sometimes it is more efficient to allot more than one slot in a frame to a single input line. For example, we might have an input line that has a data rate that is a multiple of another input. In Figure, the input line with a 50-kbps data rate can be given two slots in the output. We insert a serial-to-parallel converter in the line to make two inputs out of one.



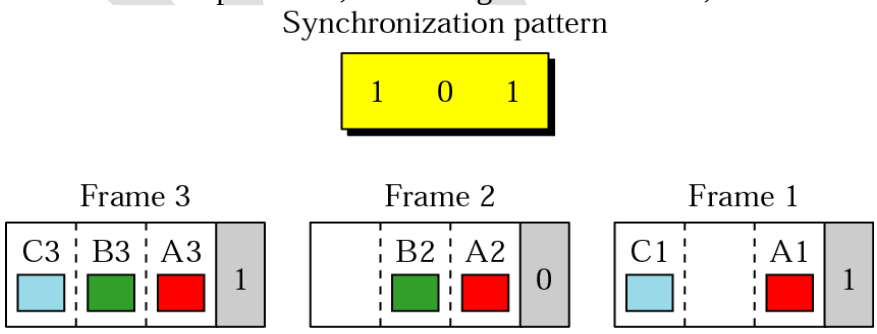
Pulse Stuffing

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 input with a data rate of 46 is pulse-stuffed to increase the rate to 50 kbps. Now multiplexing can take place.



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.

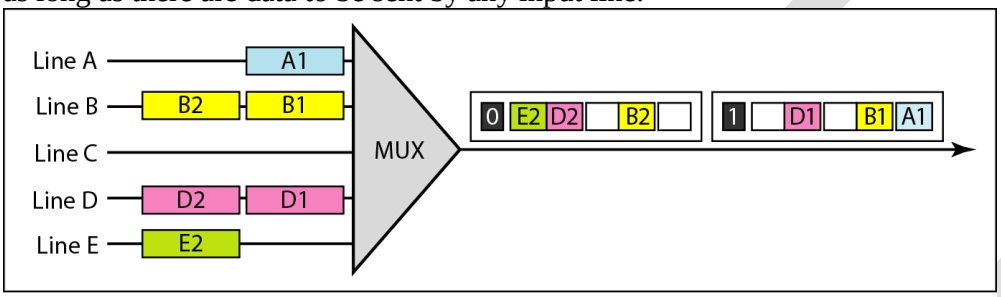


Statistical Time-Division Multiplexing

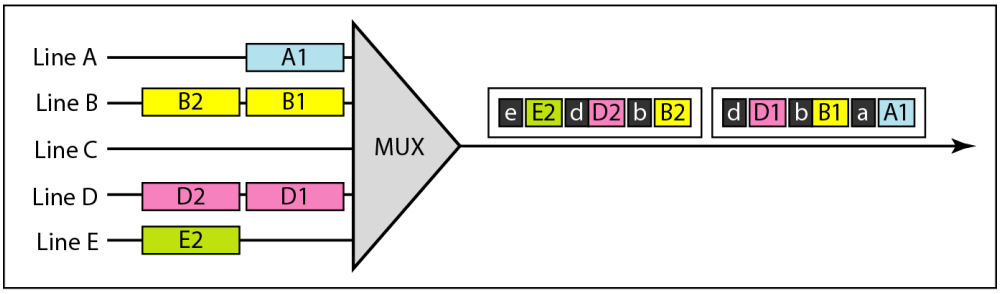
As we saw in the previous section, in synchronous TDM, each input has a reserved slot in the output

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 roundrobin 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 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

Figure also shows a major difference between slots in synchronous TDM and statistical TDM. An output slot in synchronous TDM is totally occupied by data; in statistical TDM, a slot needs to carry data as well as the address of the destination. In synchronous TDM, there is no need for addressing; synchronization and preassigned relationships between the inputs and outputs serve as an address. We know, for example, that input 1 always goes to input 2. If the multiplexer and the demultiplexer are synchronized, this is guaranteed. In statistical multiplexing, there is no fixed relationship between the inputs and outputs because there are no preassigned or reserved slots. We need to include the address of the receiver inside each slot to show where it is to be delivered. The addressing in its simplest form can be *n* bits to define *N* different output lines with $n = 10g2\ N$. 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

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

Bandwidth

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

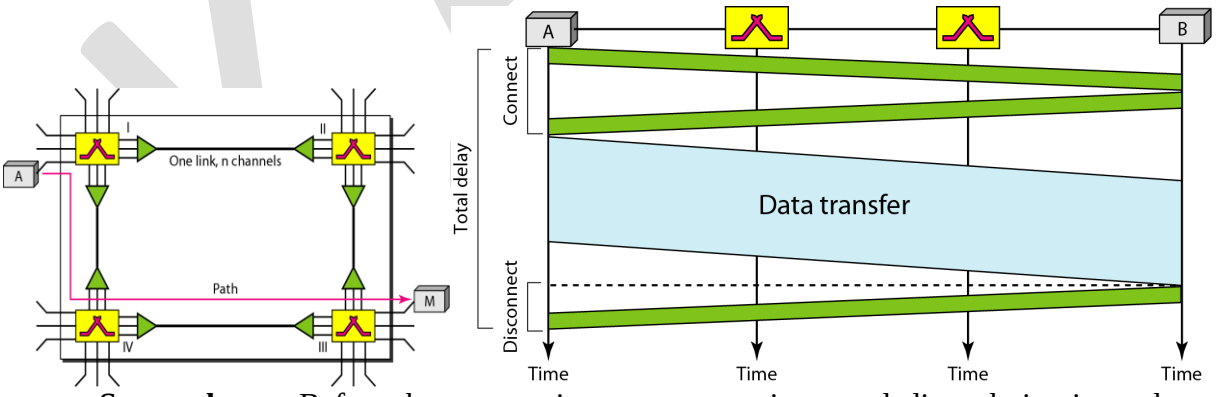
NETWORKS SWITCHING TECHNIQUES AND ACCESS MECHANISMS

There are a number of ways to perform switching:

Different types of switching techniques are employed to provide communication between two computers. These are: Circuit switching, message switching and packet switching.

Circuit Switching

- A circuit-switched network is made of a set of switches connected by physical links, in which each link is divided into *n* channels
- In circuit switching, the resources need to be reserved during the setup phase; the resources remain dedicated for the entire duration of data transfer until the teardown phase.

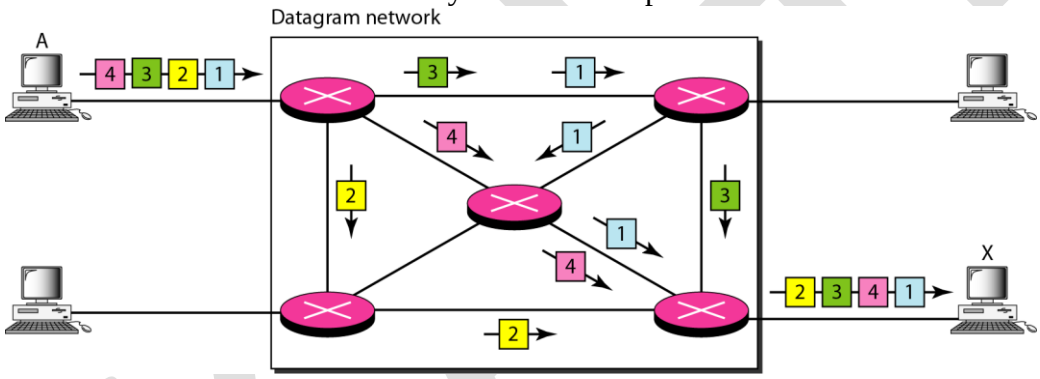


- **Setup phase:** Before the two parties can communicate, a dedicated circuit needs to be established. The end systems are normally connected through dedicated lines to the switches, so connection setup means creating dedicated channels between the switches. end-to-end addressing is required for creating a connection between the two end systems.

- ***Data Transfer Phase:*** After the establishment of the dedicated circuit, 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.
- **Efficiency** is low
- Delay in a circuit-switched network is minimum. It has 4 parts: the propagation time of the source computer request, the request signal transfer time , the propagation time of the acknowledgment from the destination computer, and the signal transfer time of the acknowledgment

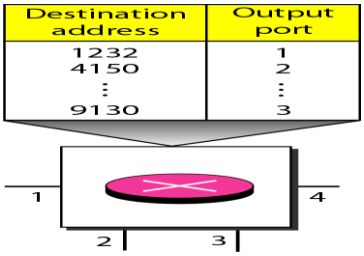
Datagram Networks

- In a packet-switched network, there is no resource reservation; resources are allocated on demand
- In a datagram network, each packet (datagrams) is treated independently of all others.
- Sometimes referred to as connectionless networks
- This approach can cause the datagrams of a transmission to arrive at their destination out of order with different delays between the packets.



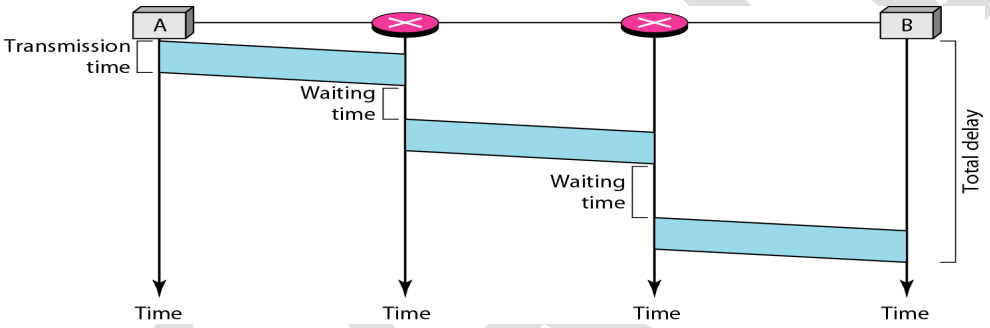
Routing Table

- A switch in a datagram networks uses a routing table that is based on the destination address
- The destination address in the header of a packet in a datagram network remains the same during the entire journey 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 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 in a Datagram Network

- Datagram network may have greater delay than a virtual-circuit network even though no setup and teardown phase
- Delay is not uniform
- 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

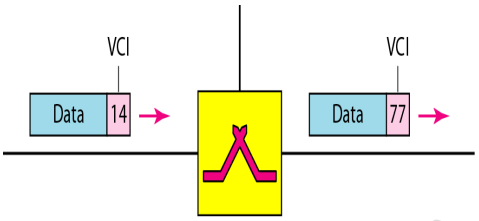


Virtual-Circuit Networks

- Setup, data transfer, and teardown phases as in a circuit-switched network (CSN)
- Resource allocated during setup phase, as in a CSN, or on demand as in a datagram network (DN)
- As in DN, data are packetized and each packet carries an address in the header. The address has local jurisdiction, not end-to-end jurisdiction.
- As in CSN, all packets follow the same path established during the connection
- VCN is normally implemented in the data link layer, while CSN is in physical layer and DN in the network layer

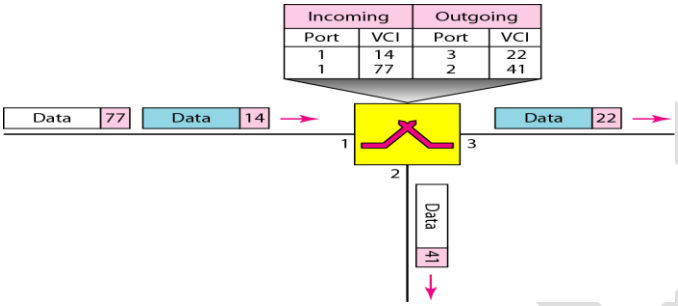
Addressing

- Two types of addressing in a virtual-circuit network: 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.



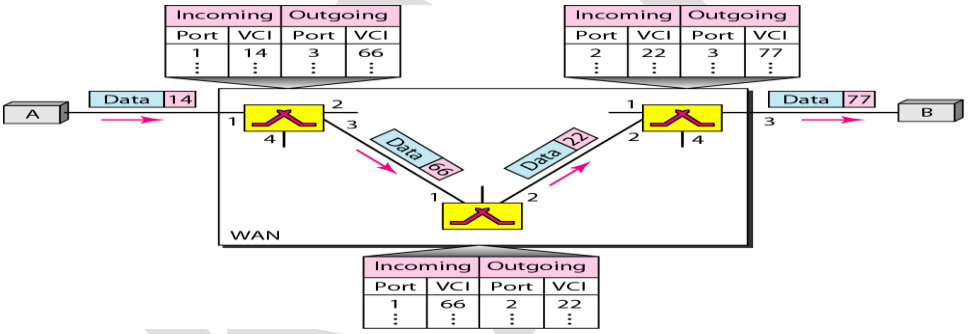
Three Phases

- Data transfer phase, setup phase, teardown phase
- Switch and tables in a virtual-circuit network

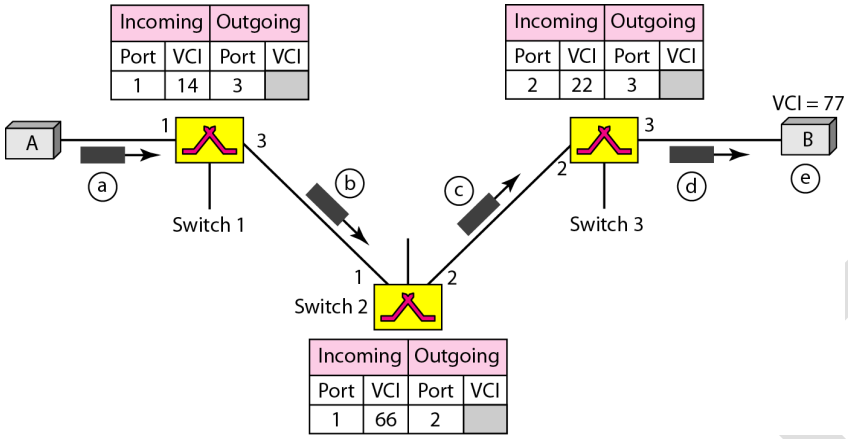


Data Transfer Phases

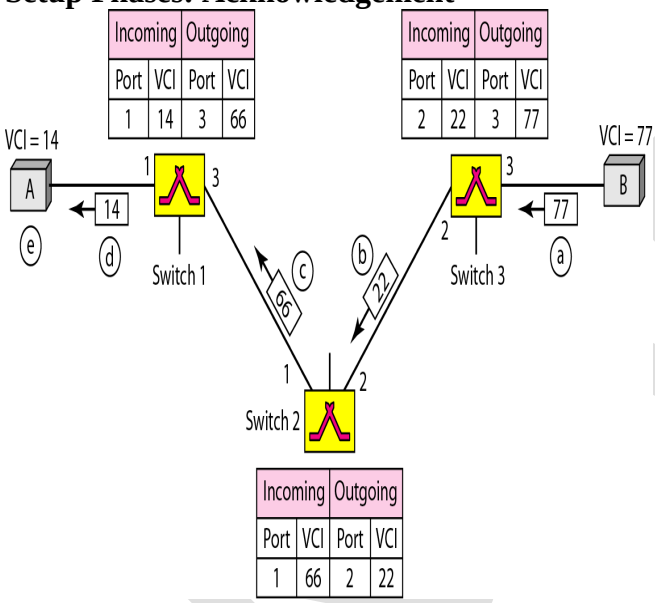
- **Source**-to-destination data transfer in a virtual-circuit network



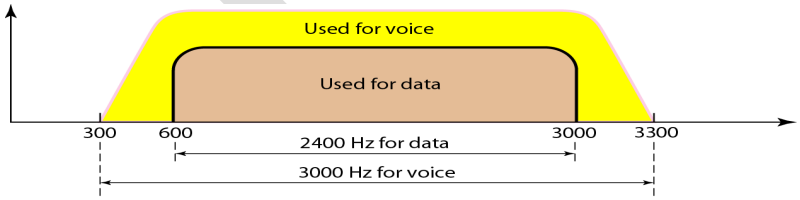
Setup Phases: Setup Request



Setup Phases: Acknowledgement

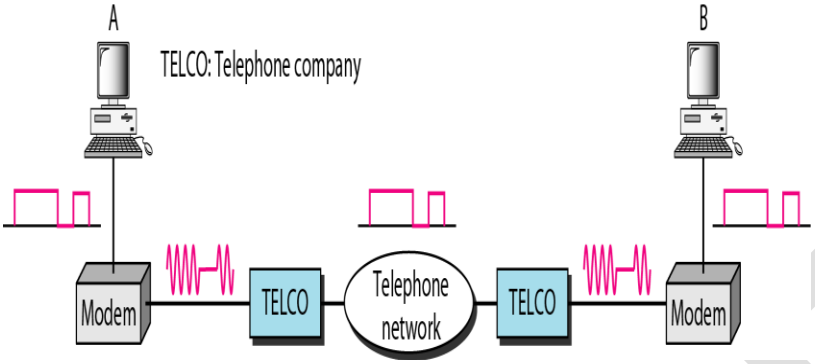


DIAL-UP MODEMS

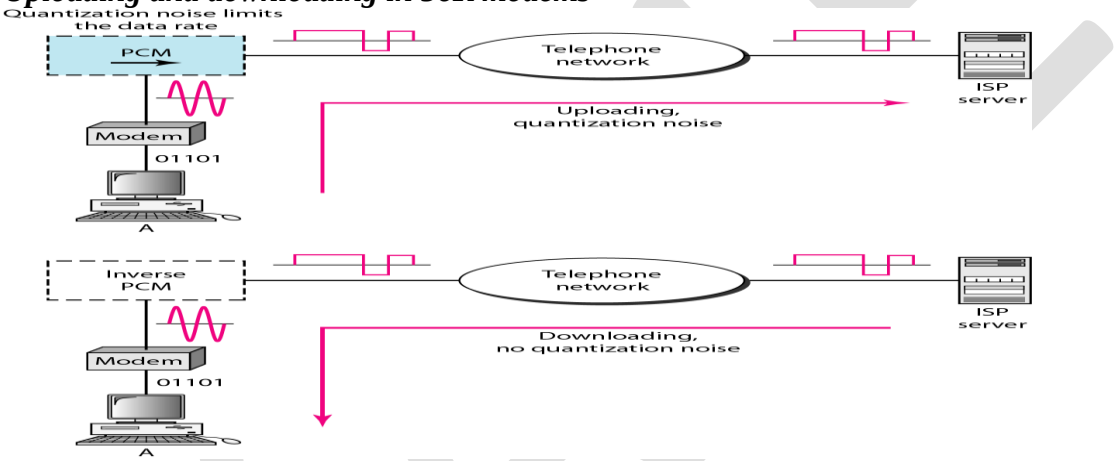


Modem
stands for modulator/demodulator.

Modulation/demodulation



Uploading and downloading in 56K modems



DIGITAL SUBSCRIBER LINE

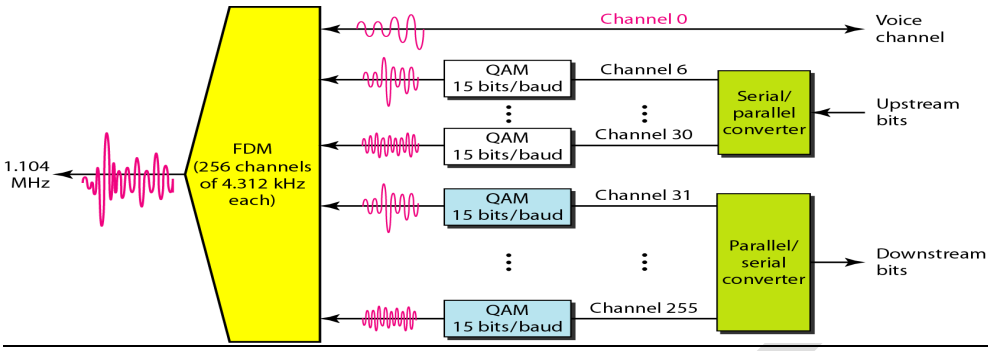
After traditional modems reached their peak data rate, telephone companies developed another technology, DSL, to provide higher-speed access to the Internet. Digital subscriber line (DSL) **technology is one of the most promising for supporting high-speed digital communication over the existing local loops.**

ADSL is an asymmetric communication technology designed for residential users; it is not suitable for businesses.

The existing local loops can handle bandwidths up to 1.1 MHz.

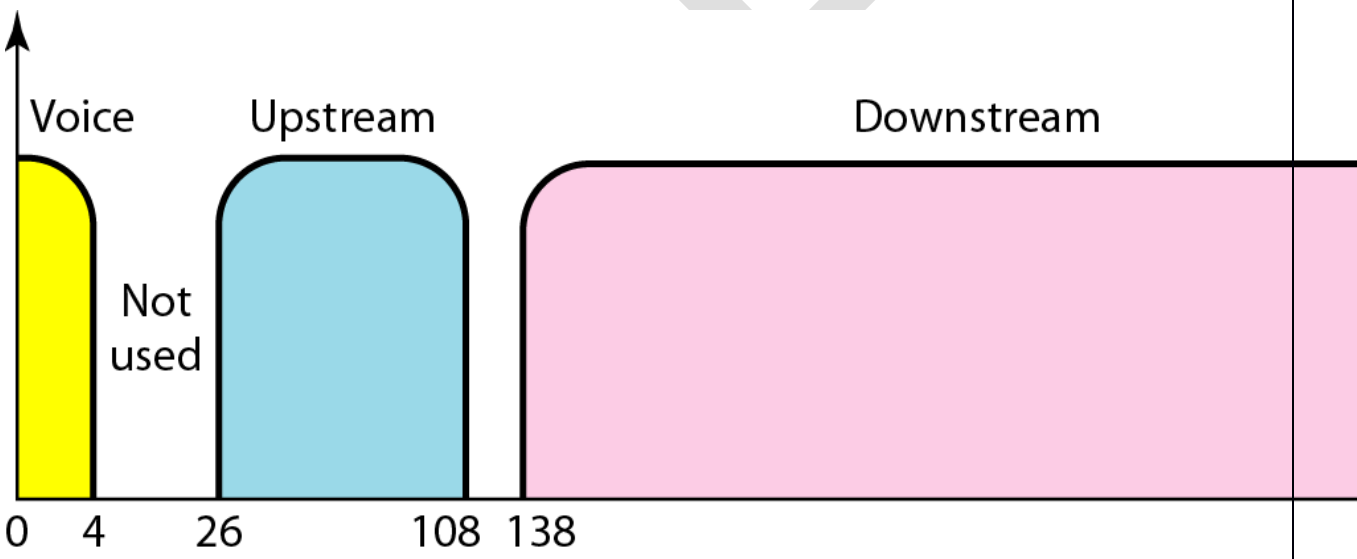
ADSL is an adaptive technology. The system uses a data ratebased on the condition of the local loop line.

Discrete multitone technique



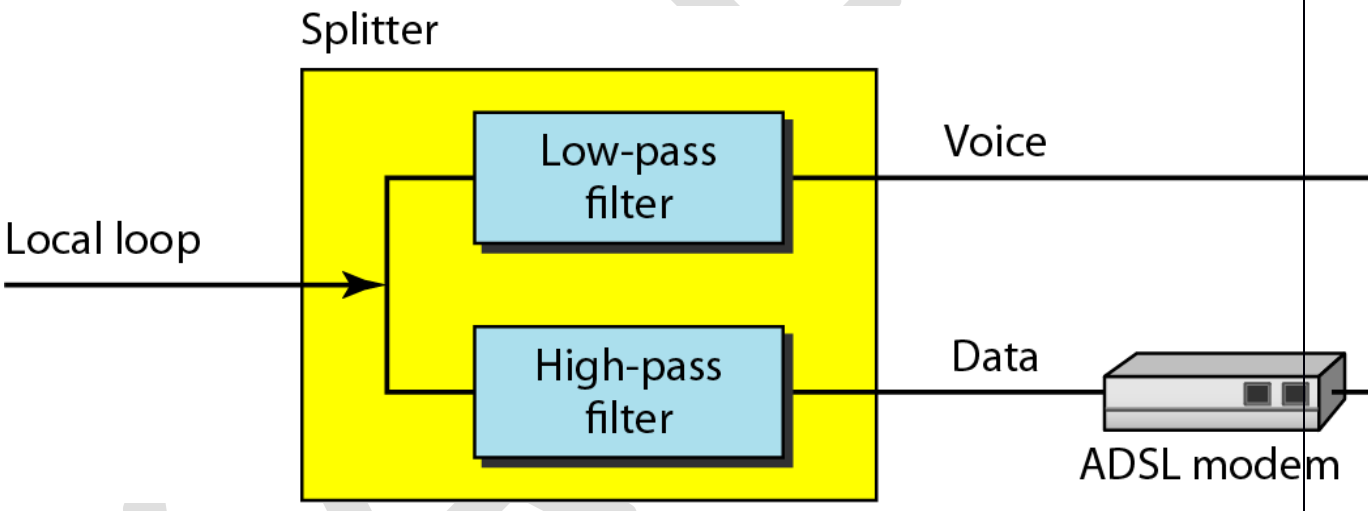
Bandwidth division in ADSL

Figure 9.11 ***Bandwidth division in ADSL***



ADSL modem
DSLAM

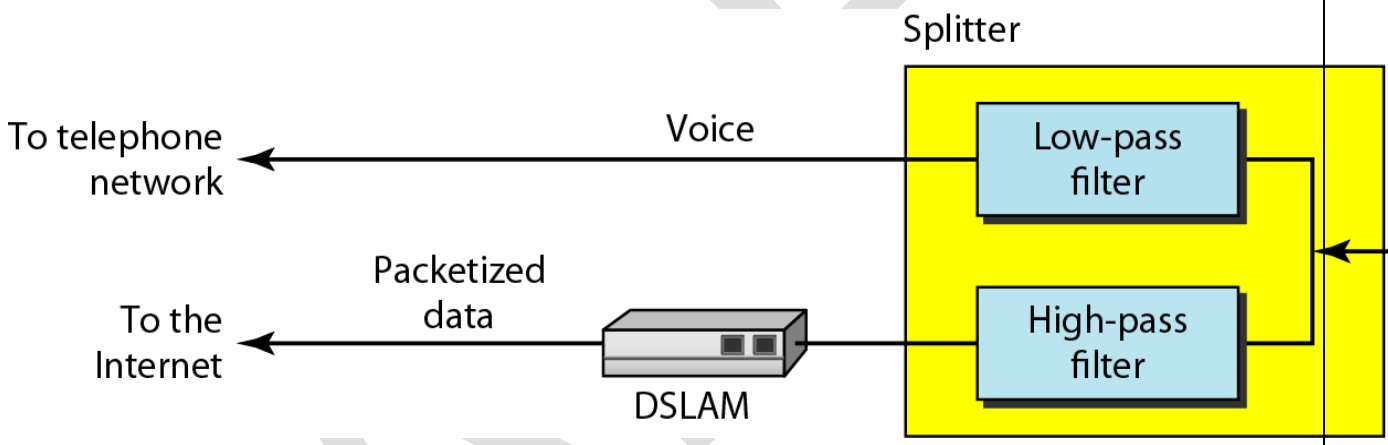
Figure 9.12 *ADSL modem*



9.22

DSLAM

Figure 9.13 *DSLAM*

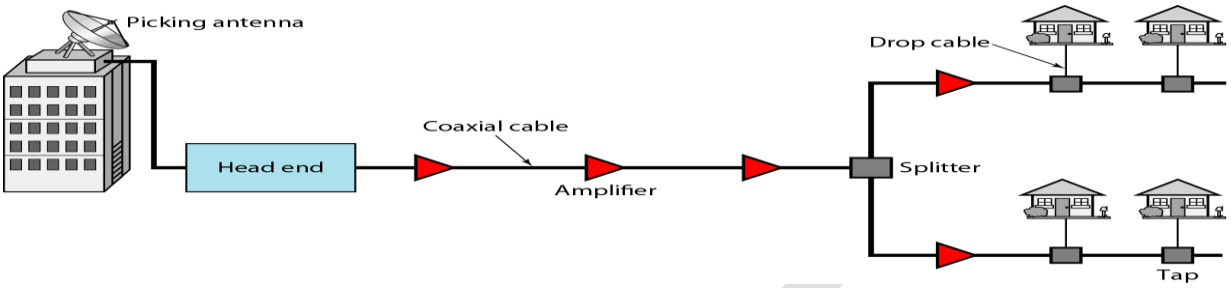


9.23

CABLE TV NETWORKS

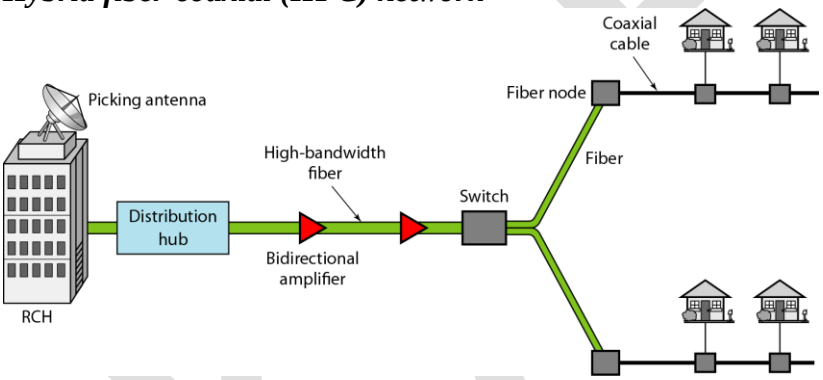
The cable TV network started as a video service provider, but it has moved to the business of Internet access. In this section, we discuss cable TV networks per se; in Section 9.5 we discuss how this network can be used to provide high-speed access to the Internet.

Traditional cable TV network

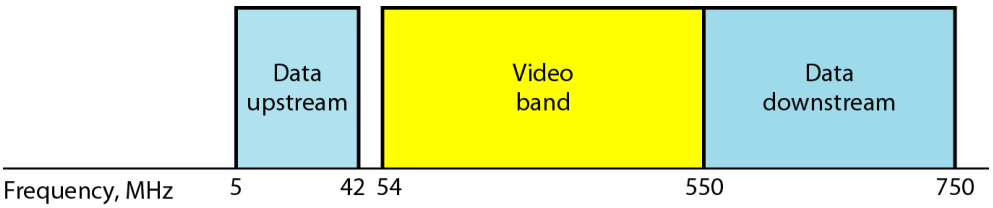


Communication in the traditional cable TV network is unidirectional.
The cable TV office, called the head end, receives video signals from broadcasting stations and feeds the signals into coaxial cables. The signals became weaker and weaker with distance, so amplifiers were installed through the network to renew the signals. There could be up to 35 amplifiers between the head end and the subscriber premises. At the other end, splitters split the cable, and taps and drop cables make the connections to the subscriber premises.

Hybrid fiber-coaxial (HFC) network



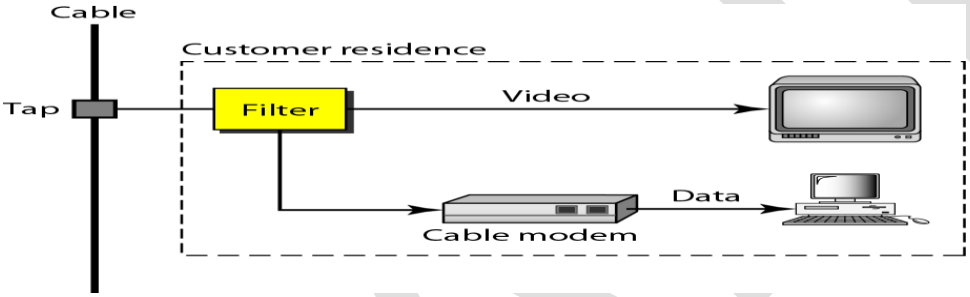
Communication in an HFC cable TV network can be bidirectional.
The second generation of cable networks is called a hybrid fiber-coaxial (HFC) network.
The network uses a combination of fiber-optic and coaxial cable. The transmission medium from the cable TV office to a box, called the fiber node, is optical fiber; from thefiber node through the neighborhood and into the house is still coaxial cable. .
Cable companies are now competing with telephone companies for the residential customer who wants high-speed data transfer. In this section, we briefly discuss this technology.
Division of coaxial cable band by CATV



Downstream data are modulated using the 64-QAM modulation technique.
The theoretical downstream data rate is 30 Mbps.
Upstream data are modulated using the QPSK modulation technique.
The theoretical upstream data rate is 12 Mbps.

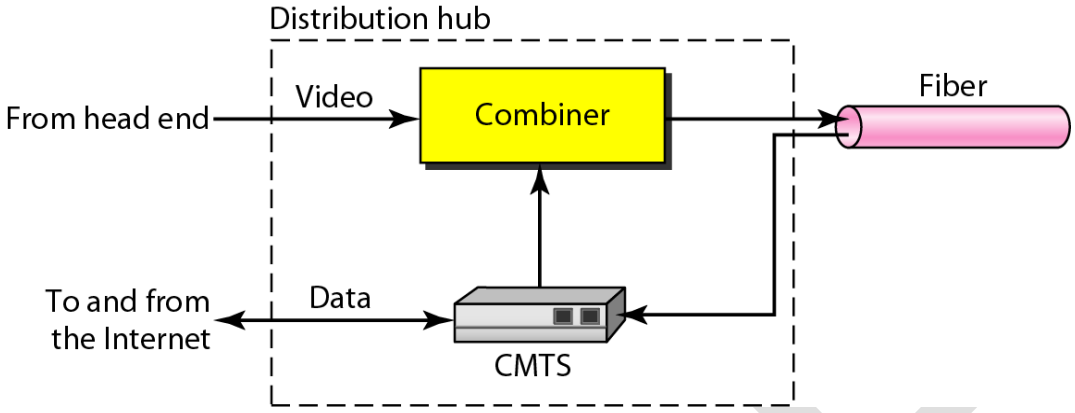
Cable modem (CM)

The cable modem (CM) is installed on the subscriber premises. It is similar to an ADSL modem



Cable modem transmission system (CMTS)

The cable modem transmission system (CMTS) is installed inside the distribution hub by the cable company. It receives data from the Internet and passes them to the combiner, which sends them to the subscriber. The CMTS also receives data from the subscriber and passes them to the Internet.



POSSIBLE QUESTIONS

PART-A [20*1=20 Marks]

ONLINE EXAMINATION

PART-B [5*2=10 Marks]

1. Define multiplexing.
2. List out the three phase used in circuit switched network.
3. What is transmission media?
4. Mention the application for twisted- pair cable.
5. What is DSL?

PART-C [5*6=30 Marks]

1. Discuss in detail about Fiber optics.
2. Discuss about Cable television as a media in detail.

3. What is multiplexing? Discuss about FDM and WDM in detail.
4. Write about guided transmission media.
5. Discuss in detail about virtual- circuit network with diagrams.
6. Explain in detail on unguided media with a neat sketch.
7. What is switched Network? Explain about Circuit-switched network.
8. What is multiplexing? Discuss about WDM in detail.
9. What is multiplexing? Explain about TDM.
10. Discuss in detail on digital subscriber line.

Karpagam Academy of Higher Education

Department of CS, CA & IT

Class: II BSC CT Batch:2017

Subject: COMPUTER NETWORKS

SubCode: 17CTU303

UNIT - II

S.No	Questions	CHOICE 1	CHOICE 2	CHOICE 3	CHOICE 4	ANSWER
1	Before data can be transmitted, they must be transformed to_____	periodic signals	electromagnetic signals	Aperiodic signals	low frequency sine waves	electromagnetic signals
2	Which of the following can be determined from a frequency_domain graph of a signal?	frequency	phase	power	all the above	frequency
3	Which of the following can be determined from a frequency_domain graph of a signal?	bandwidth	phase	power	all the above	bandwidth
4	In a frequency_domain plot, the vertical axis measures the_____	peak amplitude	frequency	phase	slope	peak amplitude
5	In a frequency_domain plot, the horizontal axis measures the_____	peak amplitude	frequency	phase	slope	frequency
6	As frequency increases, the period_____	dereases	increases	remains the same	doubles	increases
7	The last step in Pulse Code Modulation (PCM) is____	Quantization	Sampling	Encoding	Modulation	Encoding
8	A sine wave is_____	periodic and continuous	aperiodic and continuous	periodic and discrete	aperiodic and discrete	periodic and continuous
9	which the signal loses strength due to the resistance of the transmission medium	attenuation	distortion	noise	decibel	attenuation
10	which the signal loses strength due to different propogation speeds of each frequency that makes up	attenuation	distortion	noise	decibel	distortion
11	which an outside source such as crosstalk corrupts a signal	attenuation	distortion	noise	decibel	noise

12	Propogation time is_____ proportional to distance and_____ proportional to propogation speed	inversely; directly	directly; inversely	inversely; inversely	directly; directly	directly; inversely
13	The wavelength of a signal depend on the_____	frequency of the signal	medium	phase of signal	(a) and (b)	(a) and (b)
14	Unipolar, bipolar and polar encoding are types of_____ encoding	line	block	NRZ	manchester	line
15	Guided media provides a conduit from one device to another, includes _____	twisted pair cable	fiber optic cable	coaxial cable	All of the above	All of the above
16	_____ encoding has a transition at the middle of each bit	RZ	manchester	differential manchester	all the above	RZ
17	Optical fibers use reflection to guide light through a _____	channel	metal wire	light	plastic	channel
18	PCM is an example of_____conversion	digital-to-digital	digital-to-anolog	anolog-to-analog	analog-to-digital	analog-to-digital
19	The nyquist theorem specifies the minimum sampling rate to be_____	equal to the lowest frequency of signal	highest frequency of a	bandwidth of a signal	highest frequency of	frequency of signal
20	Which encoding type always has a nonzero average amplitude?	unipolar	polar	bipolar	all the above	unipolar
21	Which of the following encoding methods does not provide for synchronization?	NRZ-L	RZ	NRZ-I	manchester	NRZ-L
22	Which encoding method uses altering positive and negative voltage for bit 1?	NRZ-I	RZ	manchester	Biploar encoding	Biploar encoding
23	RZ encoding involves_____ signal levels	two	three	four	five	three
24	Unguided medium is _____	twisted pair cable	coaxial cable	fiber optic cable	free space	free space
25	Block coding can help is_____ at the receiver	synchronization	error detection	attenuation	(a) and (b)	synchronization
26	_____ transmission, bits are transmitted simultaneously, each across the own wire	asynchronous serial	synchronous serial	parallel	(a) and (b)	parallel

27	In_____ transmission, bits are transmitted over a single wire, one at a time	asynchronous serial	synchronous serial	parallel	(a) and (b)	(a) and (b)
28	In_____ transmission, a start bit and a stop bit frame a character byte	asynchronous serial	synchronous serial	parallel	(a) and (b)	synchronous serial
29	In asynchronous transmission, the gap tim between bytes is_____	fixed	variable	a function of the data rate	zero	fixed
30	synchronous transmission does not have_____	a start bit	a stop bit	gaps between bytes	all the above	all the above
31	ASK, PSK, FSK and QAM are examples of_____ modulation	digital-to-digital	digital-to-anolog	analog-to-analog	analog-to-digital	digital-to-anolog
32	AM and FM are examples of modulation	digital-to-digital	digital-to-anolog	analog-to-analog	analog-to-digital	anolog-to-analog
33	In QAM, both phase and_____ of a carrier frequency are varied	amplitude	frequency	bit rate	baud rate	amplitude
34	Telephone companies implement _____ multiplexing	TDM	FDM	WDM	DWDM	TDM
35	The applications of Frequency-Division Multiplexing (FDM) are_____	broadcasting	AM and FM radio stations	cellular telephones	All of the mentioned	All of the mentioned
36	The Time-Division multiplexing (TDM) is a digital technique of _____	Encoding	Decoding	Multiplexing	Demultiplexing	Multiplexing
37	Wavelength division multiplexing is same as_____	FDM	TDM	DWDM	SDM	FDM
38	The types of multiplexing techniques are _____	one	two	three	four	three
39	Switching in the Internet is done by using the datagram approach to packet switching at the _____	Network Layer	Application Layer	Data link Layer	physical Layer	Network Layer
40	A Circuit-Switched Network is made of a set of switches connected by physical ____	Links	media	nodes	limes	Links
41	A switch in a datagram network uses a ____	destination address	sender address	routing table	header	routing table

42	Time Division Multiplexing inside a switch, is used by _____	Space division switch	crossbar switch	packet switch	switch	switch
43	The identifier that is actually used for data transfer is called the _____	virtual-circuit identifier	global address	local address	header	virtual-circuit identifier
44	Global and local addressing are types of _____	WAN network	local area circuit network	virtual-circuit network	MAN network	virtual-circuit network
45	A modulator converts _____ signal to _____ signal	digital ; analog	analog; digital	PSK; FSK	FSK; PSK	analog; digital
46	analog carrier signal is modified to reflect binary data?	FSK	ASK	PSK	TSK	ASK
47	The sharing of medium and its link by two or more devices is called_____	decoding	encoding	line discipline	multiplexing	multiplexing
48	Which multiplexing technique transmits analog signals	FDM	TDM	WDM	(a) and ©	(a) and ©
49	Which multiplexing technique transmits digital signals?	FDM	TDM	WDM	none of the above	TDM
50	Which multi plexing technique shifts each signal to a different carrier frequency?	FDM	TDM	both(a) and (b)	none of the above	FDM
51	In TDM, for n signal sources of the same data rate, each frame contains_____ slots	n	n+1	n-1	0 to n	n
52	Guard bands increases the bandwidth for_____	FDM	TDM	both(a) and (b)	none of the above	FDM
53	Which multiplexing technique involves signals composed of light beams?	FDM	TDM	WDM	none of the above	WDM
54	Transmission media are usually categorized as_____	fixed or unfixed	guided of unguided	determinate or indeterminate	metallic or non-metallic	guided of unguided
55	Transmission media are usually categorized as_____	physical	network	transport	application	physical
56	Category 1 UTP cable is most often used in_____ networks	fast ethernet	traditional ethernet	infrared	telephone	telephone

57	BNC connectors are used by_____ cables	UTP	STP	coaxial	fiber-optic	coaxial
58	In fiber optics, the signal source is_____ waves	light	radio	infrared	very low frequency	light
59	A parabolic dish Antenna is a(n)_____ antenna	omni directional	bi directional	uni directional	horn	uni directional
60	A telephone network is an example of a_____ network	packet switching	circuit switched	message switched	none of the above	circuit switched
61	Radio waves are _____.	omnidirectional	unidirectional	bidirectional	multidirectional	omnidirectional
62	Microwaves are _____.	omnidirectional	unidirectional	bidirectional	multidirectional	unidirectional
63	_____ are used for short-range communications such as those between a PC and a peripheral device.	Radio waves	Microwaves	Miniwaves	Infrared waves	Infrared waves

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:

- This layer deals with the algorithms for achieving reliable, efficient communication between two adjacent (i.e. physically connected by a communication channel like a wire) machines just above the physical layer.
- Data transfer data rate and error correction are the major concerns of the data link layer.
- Circuit errors, finite data rate and propagation delay have important implications for the efficiency of the data transfer. The protocols used for communications must take all these factors into consideration.

Data Link Layer Design Issues
Functions of the data link layer:

1. Providing a well-defined service interface to the network layer
2. Determining how the bits of the physical layer are grouped into frames
3. Dealing with transmission errors
4. Regulating the flow of frames so that slow receivers are not swamped by fast senders.

Services Provided to the Network Layer

- The function of the data link layer is to provide service to the network layer.
- The principal service is transferring data from the network layer on the source machine to the network layer on the destination machine.
- The network layer hands some bits to the data link layer for transmission to the destination, the job of the data link layer is to transmit the bits to the destination machine, so they can be handed over to the network layer on the destination machine.
- The data link layer can be designed to offer various services.

Three possibilities that are commonly provided are:
1. **Unacknowledged connectionless service.**
2. **Acknowledged connectionless service.**
3. **Acknowledged connection-oriented service**

Unacknowledged connectionless service;

Consists of having the source machine send independent frames to the destination

machine without having the destination machine acknowledge them. No connection is established beforehand or released afterward. Good channels with low eror rates, for real-time traffic, such as speech.

Acknowledged connectionless service:

When this service is offered, there are still no connections used, but each frame sent is individually acknowledged. This way, the sender knows whether or not a frame has arrived safely. Good for unreliable channels, such as wireless.

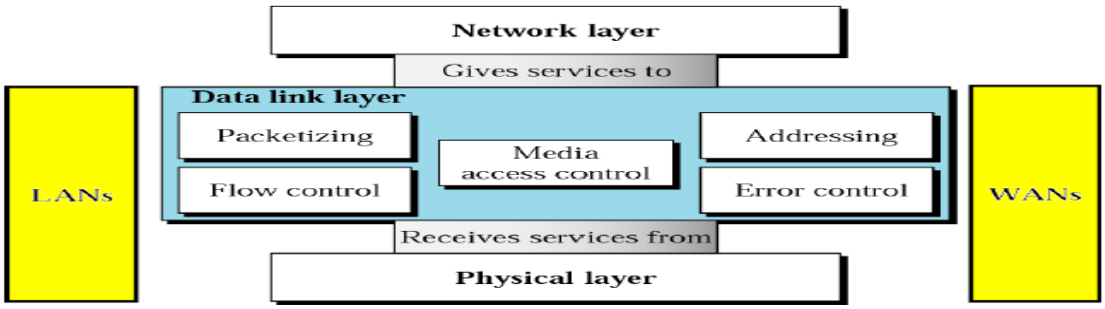
Connection-oriented service:

With this service, the source and destination machines establish a connection before any data are transferred. Each frame sent over the connection is numbered, and the data link layer guarantees that each frame sent is received. Furthermore, it guarantees that each frame is received exactly once and that all frames are received in the right order.

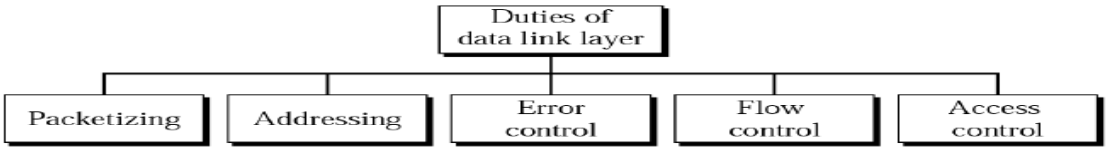
When connection-oriented service is used, transfers have three distinct phases.

1. In the first phase the connection is established by having both sides initialize variable and counter need to keep track of which frames have been received and which ones have not.
2. In the second phase, one or more frames are actually transmitted.
3. In the third phase, the connection is released, freeing up the variables, buffers, and other resources used to maintain the connection.

Position of the Data-Link Layer



Data Link Layer Duties



Data Link Layer Duties

1. **Packetizing:**
   - The packet coming form upper layer must be encapsulated in the appropriate packet defined by the data link layer of the under lying LAN or WAN.
   - Different protocols have different names for the packet.
   - Most LANs/WANs refer to packet as frame.
   - ATM WAN refers as Cell.

2. **Addressing**:
   - The data link layer addresses are called physical addresses or MAC addresses.
   - Next-hop address is used to carry a frame across the LAN.
   - Virtual circuit address is used to carry a frame across WAN.

3. **Error Control:**
   - Network must be able to transfer data from one device to another with complete accuracy.
4. **Flow Control:**
   - The flow of data must not be allowed to overwhelm the receiver.
   - Receiving device must be able to tell the transmitting device to send few frames or stops temporarily.
5. **Medium Access Control:**
   - When computers use a shared medium (cable or air), there must be a method to control the access to the medium.

ERROR DETECTION & CORRECTION

Networks must be able to transfer data from one device to another with acceptable accuracy. For most applications, a system must guarantee that the data received are identical to the data transmitted. Any time data are transmitted from one node to the next, they can become corrupted in passage. Many factors can alter one or more bits of a message. Some applications require a mechanism for detecting and correcting errors.

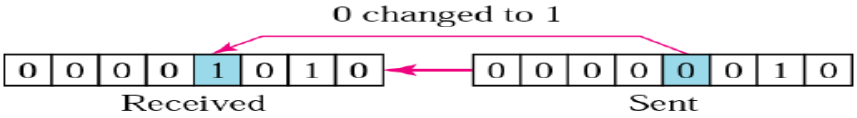
Types of Errors

Whenever bits flow from one point to another, they are subject to unpredictable changes because of interference. This interference can change the shape of the signal. In a single-bit error, a 0 is changed to a 1 or a 1 to a O. In a burst error, multiple bits are changed. For example, a 11100 s

burst of impulse noise on a transmission with a data rate of 1200 bps might change all or some of the12 bits of information.

Single-bit error

Data can be corrupted during transmission. For reliable communication, errors must be detected and corrected.

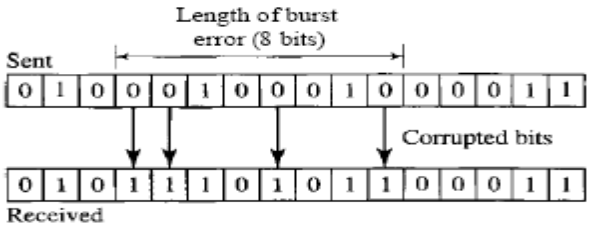


In a single-bit error, only one bit in the data unit has changed.

Burst Error

The term *burst error* means that 2 or more bits in the data unit have changed from 1 to 0 or from 0 to 1.

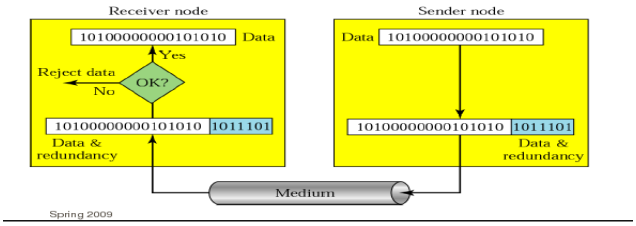
Burst error of length 8



A burst error is more likely to occur than a single-bit error. The duration of noise is normally longer than the duration of 1 bit, which means that when noise affects data, it affects a set of bits. The number of bits affected depends on the data rate and duration of noise.

Redundancy

The central concept in detecting or correcting errors is redundancy. To be able to detect or correct errors, we need to send some extra bits with our data. These redundant bits are added by the sender and removed by the receiver. Their presence allows the receiver to detect or correct corrupted bits.



Detection versus Correction

The correction of errors is more difficult than the detection. In error detection, we are looking only to see if any error has occurred. The answer is a simple yes or no. We are not even

interested in the number of errors. A single-bit error is the same for us as a burst error. In error correction, we need to know the exact number of bits that are corrupted and more importantly, their location in the message. The number of the errors and the size of the message are important factors. If we need to correct one single error in an 8-bit data unit, we need to consider eight possible error locations; if we need to correct two errors in a data unit of the same size, we need to consider 28 possibilities. You can imagine the receiver's difficulty in finding 10 errors in a data unit of 1000 bits.

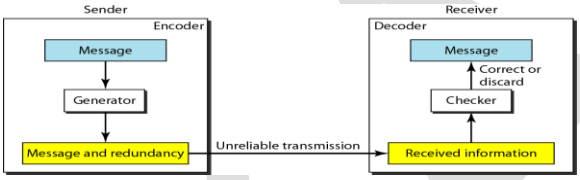
Forward Error Correction Versus Retransmission

There are two main methods of error correction. Forward error correction is the process in which the receiver tries to guess the message by using redundant bits. This is possible, as we see later, if the number of errors is small. Correction by retransmission is a technique in which the receiver detects the occurrence of an error and asks the sender to resend the message. Resending is repeated until a message arrives that the receiver believes is error-free (usually, not all errors can be detected).

Coding

Redundancy is achieved through various coding schemes. The sender adds redundant bits through a process that creates a relationship between the redundant bits and the actual data bits. The receiver checks the relationships between the two sets of bits to detect or correct the errors. The ratio of redundant bits to the data bits and the robustness of the process are important factors in any coding scheme. Figure below shows the general idea of coding.

We can divide coding schemes into two broad categories: block coding and convolution coding.



Modular Arithmetic

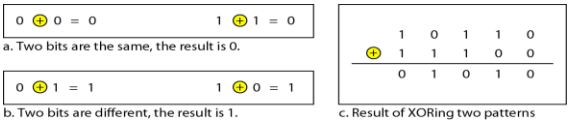
In modular arithmetic, we use only a limited range of integers. We define an upper limit, called a modulus N. We then use only the integers 0 to N - I, inclusive. This is modulo-N arithmetic. For example, if the modulus is 12, we use only the integers 0 to 1, inclusive.

Addition and subtraction in modulo arithmetic are simple. There is no carry when you add or subtract two digits in a column.

Modulo-2 Arithmetic

Operations in this arithmetic are very simple. The following shows how we can add or subtract 2 bits.

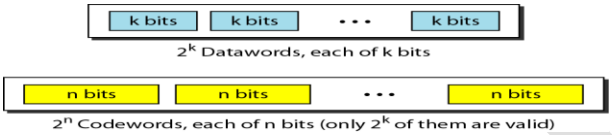
- **Adding: 0 + 0 = 0 0 + 1 = 1 1 + 0 = 1 1 + 1 = 0**
- **Subtracting: 0 – 0 = 0 0 – 1 = 1 1 – 0 = 1 1 – 1 = 0**
- **XORing of two single bits or two words**



BLOCK CODING

In block coding, we divide our message into blocks, each of k bits, called datawords. We add r redundant bits to each block to make the length n = k + r. The resulting n-bit blocks are called codewords.

We have a set of datawords, each of size *k*, and a set of codewords, each of size of *n*. With *k* bits, we can create a combination of 2^k datawords; with *n* bits, we can create a combination of 2^n codewords. Since $n > k$, the number of possible codewords is larger than the number of possible datawords. The block coding process is one-to-one; the same dataword is always encoded as the same codeword. This means that we have $2^n - 2^k$ codewords that are not used. We call these codewords invalid or illegal. Figure below shows the situation.

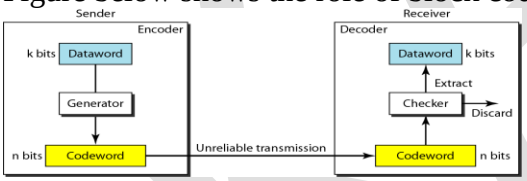


Error Detection

How can errors be detected by using block coding? If the following two conditions are met, the receiver can detect a change in the original codeword.

1. The receiver has (or can find) a list of valid codewords.
2. The original codeword has changed to an invalid one.

Figure below shows the role of block coding in error detection.



- **Example: Assume that k = 2 and n = 3**

Datawords	*Codewords*
00	000
01	011
10	101
11	110

Assume the sender encodes the dataword 01 as 011 and sends it to the receiver. Consider the following cases:

1. The receiver receives 011 which is a valid codeword. The receiver extracts the dataword 01 from it.

2. The codeword is corrupted during transmission, and 111 is received. This is not a valid codeword and is discarded.
3. The codeword is corrupted during transmission, and 000 is received. This is a valid codeword. The receiver incorrectly extracts the dataword 00. Two corrupted bits have made the error undetectable.

An error-detecting code can detect only the types of errors for which it is designed; other types of errors may remain undetected

Error Correction

Error correction is much more difficult than error detection. In error detection, the receiver needs to know only that the received codeword is invalid; in error correction the receiver needs to find (or guess) the original codeword sent. We need more redundant bits for error correction than for error detection. Figure below shows the role of block coding in error correction. The idea is the same as error detection but the checker functions are much more complex.

Dataword	*Codeword*
00	00000
01	01011
10	10101
11	11110

Assume that k = 2 and r = 3 n = 5

Assume the dataword is 01. The sender creates the codeword 01011. The codeword is corrupted during transmission, and 01001 is received. First, the receiver finds that the received codeword is not in the table. This means an error has occurred. The receiver, assuming that there is only 1 bit corrupted, uses the following strategy to guess the correct dataword

1. Comparing the received codeword with the first codeword in the table (01001 versus 00000), the receiver decides that the first codeword is not the one that was sent because there are two different bits. (the same for third or fourth one in the table)
2. The original codeword must be the second one in the table because this is the only one that differs from the received codeword by 1 bit.

Hamming Distance

One of the central concepts in coding for error control is the idea of the Hamming distance. The Hamming distance between two words (of the same size) is the number of differences between the corresponding bits. We show the Hamming distance between two words x and y as d(x, y).

The Hamming distance can easily be found if we apply the XOR operation $(\oplus)$ on the two words and count the number of 1's in the result. Note that the Hamming distance is a value greater than zero.

- Example: Hamming distance d(10101, 11110) is 3

Minimum Hamming Distance

The minimum Hamming distance (d_{min}) is the smallest Hamming distance between all possible

pairs. To find this value, we find the Hamming distances between all words and select the smallest one.

Example

Find the minimum Hamming distance of the coding scheme in Table 10.2.

Solution

We first find all the Hamming distances.

d(00000, 01011) = 3 *d(01011,* 10101) =4 *d(00000,* 10101) =3

d(0l011, 11110) = 3 *d(00000,* 11110) = 4 d(10101, 11110) =3

The *dmin* in this case is 3.

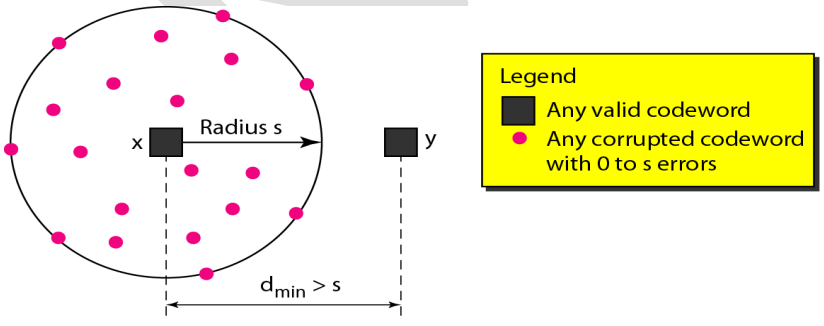
Hamming Distance and Error

When a codeword is corrupted during transmission, the Hamming distance between the sent and received codewords is the number of bits affected by the error. In other words, the Hamming distance between the received codeword and the sent codeword is the number ofbits that are corrupted during transmission. For example, if the codeword 00000 is sent and 01101 is received, 3 bits are in error and the Hamming distance between the two is d(00000, 01101) =3.

Minimum Distance for Error Detection

If s errors occur during transmission, the Hamming distance between the sent codeword and received codeword is s. If our code is to detect up to s errors, the minimum distance between the valid codes must be s + 1, so that the received codeword does not match a valid codeword. In other words, if the minimum distance between all valid codewords is s+1, the received codeword cannot be erroneously mistaken for another codeword. The distances are not enough (s + 1) for the receiver to accept it as valid. The error will be detected. Although a code with dmin =s + 1 may be able to detect more than s errors in some special cases, only s or fewer errors are guaranteed to be detected.

Our second block code scheme has *dmin* = 3. This code can detect up to two errors. Again, we see that when any of the valid codewords is sent, two errors create a codeword which is not in the table of valid codewords. The receiver cannot be fooled. However, some combinations of three errors change a valid codeword to another valid codeword. The receiver accepts the received codeword and the errors are undetected.

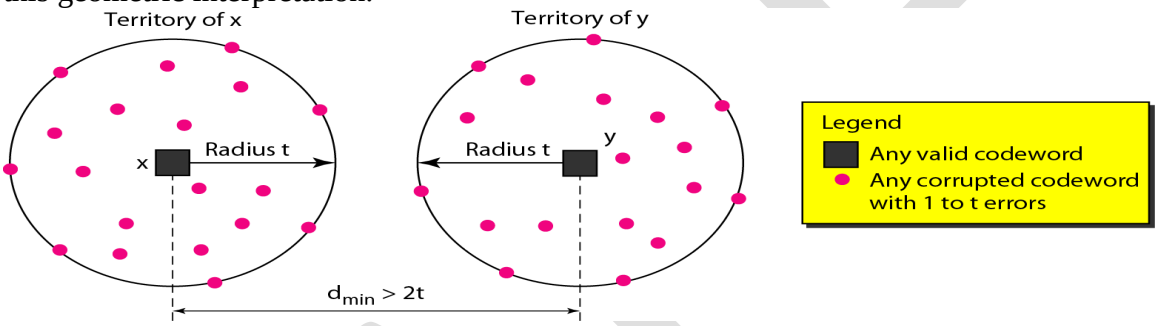


We can look at this geometrically. Let us assume that the sent codeword *x* is at the center of a circle with radius *s*. All other received codewords that are created by 1 to *s* errors are points inside the circle or on the perimeter of the circle. All other valid codewords must be outside the circle, as shown in Figure.

Minimum Distance for Error Correction

Error correction is more complex than error detection; a decision is involved. When a received codeword is not a valid codeword, the receiver needs to decide which valid codeword was actually sent. The decision is based on the concept of territory, an exclusive area surrounding the codeword. Each valid codeword has its own territory.

We use a geometric approach to define each territory. We assume that each valid codeword has a circular territory with a radius of *t* and that the valid codeword is at the center. For example, suppose a codeword *x* is corrupted by *t* bits or less. Then this corrupted codeword is located either inside or on the perimeter of this circle. If the receiver receives a codeword that belongs to this territory, it decides that the original codeword is the one at the center. Note that we assume that only up to *t* errors have occurred; otherwise, the decision is wrong. Figure shows this geometric interpretation.



To guarantee correction of up to t errors in all cases, the minimum Hamming distance in a block code must be dmin = 2t + 1.

LINEAR BLOCK CODES

Almost all block codes used today belong to a subset called linear block codes. The formal definition of linear block codes requires the knowledge of abstract algebra. We therefore give an informal definition. For our purposes, a linear block code is a code in which the exclusive OR (addition modulo-2) of two valid codewords creates another valid codeword.

Example

Let us see if the two codes we defined in Table 10.1 and Table 10.2 belong to the class of linear block codes.

1. The scheme in Table 10.1 is a linear block code because the result of XORing any codeword with any other codeword is a valid codeword. For example, the XORing of the second and third codewords creates the fourth one.
2. The scheme in Table 10.2 is also a linear block code. We can create all four codewords by XORing two other codewords.

Minimum Distance for Linear Block Codes

It is simple to find the minimum Hamming distance for a linear block code. The minimum Hamming distance is the number of 1s in the nonzero valid codeword with the smallest number

of Is.

Example

In our first code (Table 10.1), the numbers of 1s in the nonzero codewords are 2, 2, and 2. So the minimum Hamming distance is dmin =2.

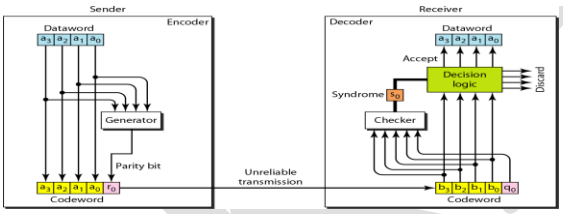
In our second code (Table 10.2), the numbers of 1s in the nonzero codewords are 3, 3, and 4. So in this code we have dmin =3.

Parity Check

In parity check, a parity bit is added to every data unit so that the total number of 1s is even (or odd for odd-parity). In this code, a *k-bit* dataword is changed to an n-bit codeword where $n = k + 1$. The extra bit, called the parity bit, is selected to make the total number of 1s in the codeword even. The minimum Hamming distance for this category is $d_{min} = 2$, which means that the code is a single-bit error-detecting code; it cannot correct any error.

Example: A simple parity-check code is a single-bit error-detecting code in which n= k+1 with dmin = 2.

Datawords	*Codewords*	*Datawords*	*Codewords*
0000	00000	1000	10001
0001	00011	1001	10010
0010	00101	1010	10100
0011	00110	1011	10111
0100	01001	1100	11000
0101	01010	1101	11011
0110	01100	1110	11101
0111	01111	1111	11110



The encoder uses a generator that takes a copy of a 4-bit dataword (a0, a1 a2 and a3) and generates a parity bit r0. The dataword bits and the parity bit create the 5-bit codeword. The parity bit that is added makes the number of 1s in the codeword even. This is normally done by adding the 4 bits of the dataword (modulo-2); the result is the parity bit. In other words,

$$r_0 = a_3 + a_2 + a_1 + a_0 \quad \text{(modulo-2)}$$

If the number of 1s is even, the result is 0; if the number of 1s is odd, the result is 1.In both cases, the total number of 1s in the codeword is even. The sender sends the codeword which may be corrupted during transmission. The receiver receives a 5-bit word. The checker at the receiver does the same thing as the generator in the sender with one exception: The addition is done over all 5 bits. The result, which is called the syndrome, is just 1 bit. The syndrome is 0 when the number of 1s in the received codeword is even; otherwise, it is 1.

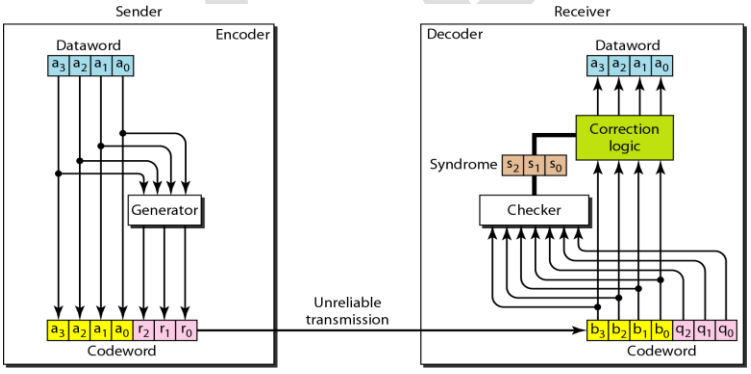
$$s_0 = b_3 + b_2 + b_1 + b_0 + q_0 \qquad \text{(modulo-2)}$$

The syndrome is passed to the decision logic analyzer. If the syndrome is 0, there is no error in the received codeword; the data portion of the received codeword is accepted as the dataword; if the syndrome is 1, the data portion of the received codeword is discarded. The dataword is not created.

Example:

Let us look at some transmission scenarios. Assume the sender sends the dataword 1011. The codeword created from this dataword is 10111, which is sent to the receiver. We examine five cases:

1. No error occurs; the received codeword is 10111. The syndrome is 0. The dataword 1011 is created.
2. One single-bit error changes *a1*. The received codeword is 10011. The syndrome is 1. No dataword is created.
3. One single-bit error changes *roo* The received codeword is 10110. The syndrome is 1. No dataword is created. Note that although none of the dataword bits are corrupted, no dataword is created because the code is not sophisticated enough to show the position of the corrupted bit.
4. An error changes *ro* and a second error changes *a3.* The received codeword is 00110. The syndrome is 0. The dataword 0011 is created at the receiver. Note that here the dataword is wrongly created due to the syndrome value. The simple parity-check decoder cannot detect an even number of errors. The errors cancel each other out and give the syndrome a value of 0.
5. Three bits-a3, a2, and a1-are changed by errors. The received codeword is 01011. The syndrome is 1. The dataword is not created. This shows that the simple parity check, guaranteed to detect one single error, can also find any odd number of errors.



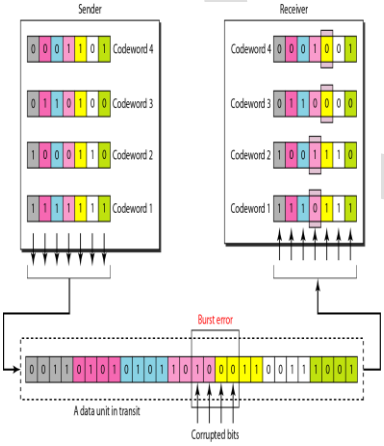
- **r0 = a2 + a1 + a0 modulo-2**
- **r1 = a3 + a2 + a1 modulo-2**
- **r2 = a1 + a0 + a3 modulo-2**
- **s0 = b2 + b1 + b0 + q0 modulo-2**
- **s1 = b3 + b2 + b1 + q1 modulo-2**
- **s2 = b1 + b0 + b3 + q2 modulo-2**

Syndrome	000	001	010	011	100	101	110	111
Error	None	q_0	q_1	b_2	q_2	b_0	b_3	b_1

Let us trace the path of three datawords from the sender to the destination:
1 The dataword 0100 becomes the codeword 0100011. The codeword 0100011 is received. The syndrome is 000, the final dataword is 0100.
2. The dataword 0111 becomes the codeword 0111001. The codeword 0011001 received. The syndrome is 011. After flipping b2 (changing the 1 to 0), the final dataword is 0111.
3. The dataword 1101 becomes the codeword 1101000. The codeword 0001000 received (two errors). The syndrome is 101. After flipping b0, we get 0000, the wrong dataword. This shows that our code cannot correct two errors.

Performance

A Hamming code can only correct a single error or detect a double error. However, there is a way to make it detect a burst error, as shown in Figure. The key is to split a burst error between several codewords, one error for each codeword. In data communications, we normally send a packet or a frame of data. To make the Hamming code respond to a burst error of size *N*, we need to make *N* codewords out of our frame. Then, instead of sending one codeword at a time, we arrange the codewords in a table and send the bits in the table a column at a time. In Figure, the bits are sent column by column (from the left). In each column, the bits are sent from the bottom to the top. In this way, a frame is made out of the four codewords and sent to the receiver. Figure shows that when a burst error of size 4 corrupts the frame, only 1 bit from each codeword is corrupted. The corrupted bit in each codeword can then easily be corrected at the receiver.



CYCLIC CODES

Cyclic codes are special linear block codes with one extra property. In a cyclic code, if a codeword is cyclically shifted (rotated), the result is another codeword. For example, if 1011000 is a codeword and we cyclically left-shift, then 0110001 is also a codeword. In this case, if we

call the bits in the first word *ao* to *a6'* and the bits in the second word *boto b6*, we can shift the bits by using the following:

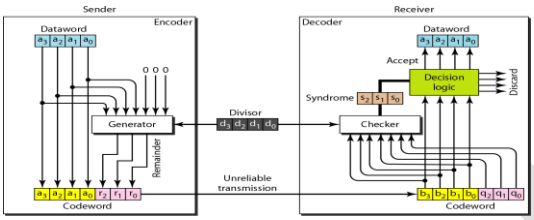
$$b_1 = a_0 \quad b_2 = a_1 \quad b_3 = a_2 \quad b_4 = a_3 \quad b_5 = a_4 \quad b_6 = a_5 \quad b_0 = a_6$$

In the rightmost equation, the last bit of the first word is wrapped around and becomes the first bit of the second word.

Cyclic Redundancy Check

We can create cyclic codes to correct errors. Cyclic codes called the cyclic redundancy check (CRC) that is used in networks such as LANs and WANs.

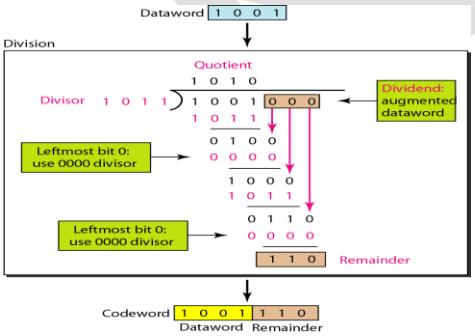
Dataword	Codeword	Dataword	Codeword
0000	0000000	1000	1000101
0001	0001011	1001	1001110
0010	0010110	1010	1010011
0011	0011101	1011	1011000
0100	0100111	1100	1100010
0101	0101100	1101	1101001
0110	0110001	1110	1110100
0111	0111010	1111	1111111



In the encoder, the dataword has *k* bits (4 here); the codeword has *n* bits (7 here). The size of the dataword is augmented by adding *n* - *k* (3 here) Os to the right-hand side of the word. The n-bit result is fed into the generator. The generator uses a divisor of size *n* - *k* + I (4 here), predefined and agreed upon. The generator divides the augmented dataword by the divisor (modulo-2 division). The quotient of the division is discarded; the remainder *(r2rl ro)* is appended to the dataword to create the codeword. The decoder receives the possibly corrupted codeword. A copy of all *n* bits is fed to the checker which is a replica of the generator. The remainder produced by the checker is a syndrome of *n* - *k* (3 here) bits, which is fed to the decision logic analyzer. The analyzer has a simple function. If the syndrome bits are all as, the 4 leftmost bits of the codeword are accepted as the dataword (interpreted as no error); otherwise, the 4 bits are discarded (error).

Encoder

Let us take a closer look at the encoder. The encoder takes the dataword and augments it with *n* - *k* number of as. It then divides the augmented dataword by the divisor, as shown in Figure.

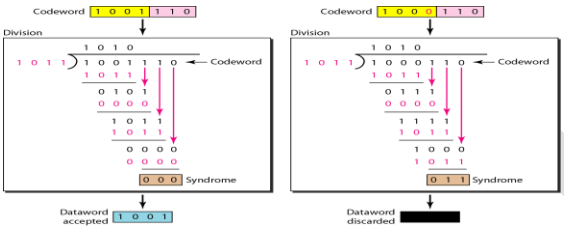


As in decimal division, the process is done step by step. In each step, a copy of the divisor is XORed with the 4 bits of the dividend. The result of the XOR operation (remainder) is 3 bits (in

this case), which is used for the next step after 1 extra bit is pulled down to make it 4 bits long. If the leftmost bit of the dividend (or the part used in each step) is 0, the step cannot use the regular divisor; we need to use an all-Os divisor. When there are no bits left to pull down, we have a result. The 3-bit remainder forms the check bits *(r2' rl'* and *ro).* They are appended to the dataword to create the codeword.

Decoder

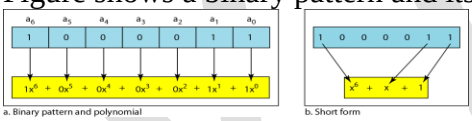
The codeword can change during transmission. The decoder does the same division process as the encoder. The remainder of the division is the syndrome. If the syndrome is all Os, there is no error; the dataword is separated from the received codeword and accepted. Otherwise, everything is discarded. Figure shows two cases: The left hand figure shows the value of syndrome when no error has occurred; the syndrome is 000. The right-hand part of the figure shows the case in which there is one single error. The syndrome is not all 0s (it is 011).



Polynomials

A better way to understand cyclic codes and how they can be analyzed is to represent them as polynomials.

A pattern of 0s and 1s can be represented as a **polynomial** with coefficients of 0 and 1. The power of each term shows the position of the bit; the coefficient shows the value of the bit. Figure shows a binary pattern and its polynomial representation.



Degree of a polynomial: the highest power in the polynomial

Example: $x^6 + x + 1$ -> the degree '6'

Adding and Subtracting Polynomials

Adding and subtracting polynomials in mathematics are done by adding or subtracting the coefficients of terms with the same power.

$(x^5 + x^4 + x^2) + (x^6 + x^4 + x^2) = x^6 + x^5$

- Multiplying two polynomials

Multiplying a polynomial by another is done term by term. Each term of the first polynomial must be multiplied by all terms of the second. The result, of course, is then simplified, and pairs of equal terms are deleted.

$(x^5 + x^3 + x^2 + x)\ (x^2 + x^1 + 1)$

$= x^7 + x^6 + x^5 + x^5 + x^4 + x^3 + x^4 + x^3 + x^2 + x^3 + x^2 + x$
$= x^7 + x^6 + x^3 + x$

- Dividing one polynomial by another- same as encoder
- Shifting

Shifting left 3 bits: 10011 becomes 10011000

Shifting right 3 bits: 10011 becomes 10 ($x^4 + x + 1$, x)

Cyclic Code Encoder Using Polynomials

We show the creation of a codeword from a dataword . The dataword 1001 is represented as $x3$ + 1. The divisor 1011 is represented as $x3 + x + 1$. To find the augmented dataword, we have left-shifted the dataword 3 bits (multiplying by x\ The result is $x6 + x3$. Division is straightforward. We divide the first term of the dividend, $x6$, by the first term of the divisor, $x3$. The first term of the quotient is then $x6/x3$, or $x3$. Then we multiply $x3$ by the divisor and subtract (according to our previous definition of subtraction) the result from the dividend. The result is $x4$, with a degree greater than the divisor's degree; we continue to divide until the degree of the remainder is less than the degree of the divisor.

Cyclic Code Analysis

- $f(x)$ is a polynomial with binary coefficients

Dataword: $d(x)$ Codeword: $c(x)$ Generator: $g(x)$
Syndrome: $s(x)$ Error: $e(x)$

- **In a cyclic code**,
  1. If $s(x) \neq 0$, one or more bits is corrupted.
  2. If $s(x) = 0$, either
     a. No bit is corrupted. Or
     b. Some bits are corrupted, but the decoder failed to detect them
- *Received codeword = c(x) + e(x)*

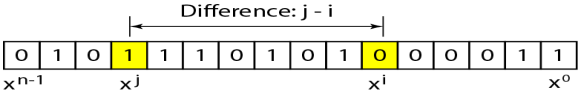
Received codeword/g(x) = c(x)/g(x) + e(x)/g(x)

- In a cyclic code, those $e(x)$ errors that are divisible by $g(x)$ are not caught
- Single-bit error

If the generator has more than one term and the coefficient of x^0 is 1, all single errors can be caught.

- Two isolated single-bit error

If a generator cannot divide $x^t + 1$ (t between 0 and n – 1), then all isolated double errors can be detected



- **Odd numbers of errors**

A generator that contains a factor of $x + 1$ can detect all odd-numbered errors

- **Burst errors**
- All burst errors with $L \leq r$ will be detected.
- All burst errors with $L = r + 1$ will be detected with probability $1 - (1/2)^{r-1}$.
- All burst errors with $L > r + 1$ will be detected with probability $1 - (1/2)^{r}$.

- A good polynomial generator needs to have the following characteristics:
  1. It should have at least two terms.
  2. The coefficient of the term x^0 should be 1.
  3. It should not divide $x^t + 1$, for t between 2 and $n - 1$.
  4. It should have the factor $x + 1$.

Checksum

The checksum is used in the Internet by several protocols although not at the data link layer. Like linear and cyclic codes, the checksum is based on the concept of redundancy. Several protocols still use the checksum for error detection

The concept of the checksum is not difficult. Let us illustrate it with a few examples.

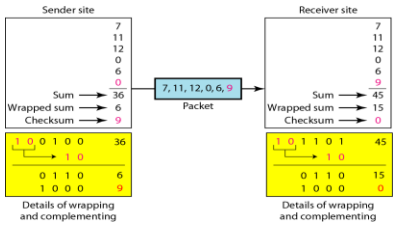
Example: Suppose our data is a list of five 4-bit numbers that we want to send to a destination. In addition to sending these numbers, we send the sum of the numbers. For example, if the set of numbers is (7, 11, 12, 0, 6), we send (7, 11, 12,0,6,36), where 36 is the sum of the original numbers. The receiver adds the five numbers and compares the result with the sum. If the two are the same, the receiver assumes no error, accepts the five numbers, and discards the sum. Otherwise, there is an error somewhere and the data are not accepted.

We can make the job of the receiver easier if we send the negative (complement) of the sum, called the checksum. In this case, we send (7, 11, 12, 0, 6, -36). The receiver can add all the numbers received (including the checksum). If the result is 0, it assumes no error; otherwise, there is an error.

One's Complement

The previous example has one major drawback. All of our data can be written as a 4-bit word (they are less than 15) except for the checksum. One solution is to use one's complement arithmetic. In this arithmetic, we can represent unsigned numbers between 0 and 2n - 1 using only n bits. t If the number has more than n bits, the extra leftmost bits need to be added to the n rightmost bits (wrapping). In one's complement arithmetic, a negative number can be represented by inverting all bits (changing a 0 to a 1 and a 1 to a 0). This is the same as subtracting the number from 2n - 1.

The sender initializes the checksum to 0 and adds all data items and the checksum. However, 36 cannot be expressed in 4 bits. The extra two bits are wrapped and added with the sum to create the wrapped sum value 6. The sum is then complemented, resulting in the checksum value 9 ($15 - 6 = 9$).



Internet Checksum

Traditionally, the Internet has been using a 16-bit checksum. The sender calculates the checksum by following these steps.

Sender site:

1. The message is divided into 16-bit words.
2. The value of the checksum word is set to 0.
3. All words including the checksum are added using one's complement addition.
4. The sum is complemented and becomes the checksum.
5. The checksum is sent with the data.

Receiver site:

1. The message (including checksum) is divided into 16-bit words.
2. All words are added using one's complement addition.
3. The sum is complemented and becomes the new checksum.
4. If the value of checksum is 0, the message is accepted; otherwise, it is rejected.

1	0	1	3	Carries
4	6	6	F	(Fo)
7	2	6	7	(ro)
7	5	7	A	(uz)
6	1	6	E	(an)
0	0	0	0	Checksum (initial)
8	F	C	6	Sum (partial)
			1	
8	F	C	7	Sum
7	0	3	8	Checksum (to send)

a. Checksum at the sender site

1	0	1	3	Carries
4	6	6	F	(Fo)
7	2	6	7	(ro)
7	5	7	A	(uz)
6	1	6	E	(an)
7	0	3	8	Checksum (received)
F	F	F	E	Sum (partial)
			1	
8	F	C	7	Sum
0	0	0	0	Checksum (new)

a. Checksum at the receiver site

Data Link Control

The two main functions of the data link layer are data link control and media access control. The first, data link control, deals with the design and procedures for communication between two adjacent nodes: node-to-node communication.

Data link control functions include framing, flow and error control, and software implemented protocols that provide smooth and reliable transmission of frames between nodes.
To implement data link control, we need protocols. Each protocol is a set of rules that need to be implemented in software and run by the two nodes involved in data exchange at the data link layer. We discuss five protocols: two for noiseless (ideal) channels and three for noisy (real) channels.

FRAMING

Data transmission in the physical layer means moving bits in the form of a signal from the source to the destination. The physical layer provides bit synchronization to ensure that the sender and receiver use the same bit durations and timing. The data link layer, on the other hand, needs to pack bits into frames, so that each frame is distinguishable from another.
Framing in the data link layer separates a message from one source to a destination, or from other messages to other destinations, by adding a sender address and a destination address. The destination address defines where the packet is to go; the sender address helps the recipient acknowledge the receipt.
Although the whole message could be packed in one frame that is not normally done. One reason is that a frame can be very large, making flow and error control very inefficient. When a message is carried in one very large frame, even a single-bit error would require the retransmission of the whole message. When a message is divided into smaller frames, a single-bit error affects only that small frame.

Fixed-Size Framing

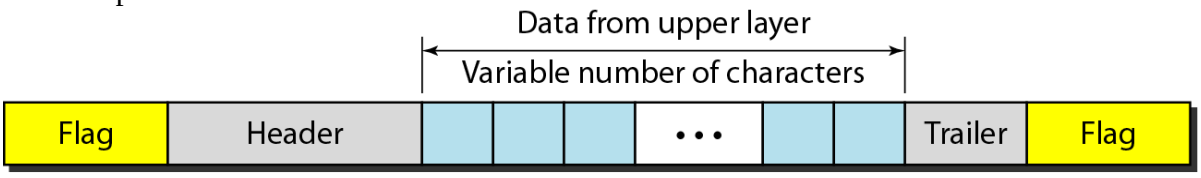
Frames can be of fixed or variable size. In fixed-size framing, there is no need for defining the boundaries of the frames; the size itself can be used as a delimiter

Variable-Size Framing

In variable-size framing, definition of the end of the frame and the beginning of the next is needed. Historically, two approaches were used for this purpose: a character-oriented approach and a bit-oriented approach.

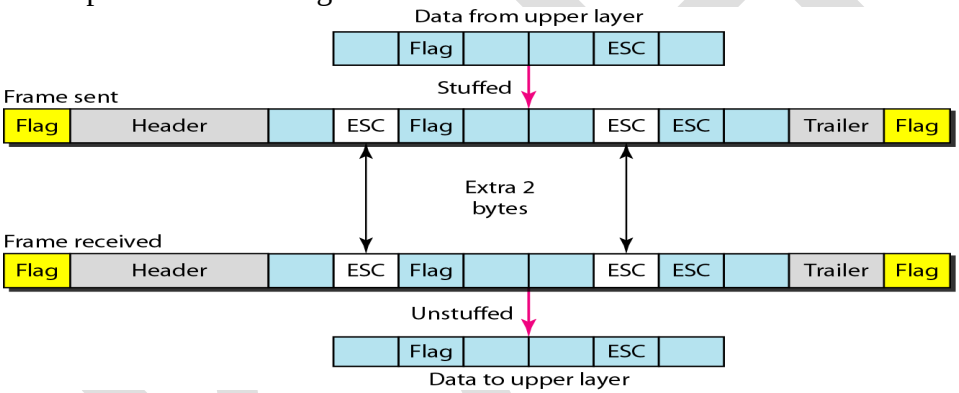
Character-Oriented Protocols

In a character-oriented protocol, data to be carried are 8-bit characters from a coding system such as ASCII. The header, which normally carries the source and destination addresses and other control information, and the trailer, which carries error detection or error correction redundant bits, are also multiples of 8 bits. To separate one frame from the next, an 8-bit (1-byte) flag is added at the beginning and the end of a frame. The flag, composed of protocol-dependent special characters, signals the start or end of a frame. Figure shows the format of a frame in a character-oriented protocol.



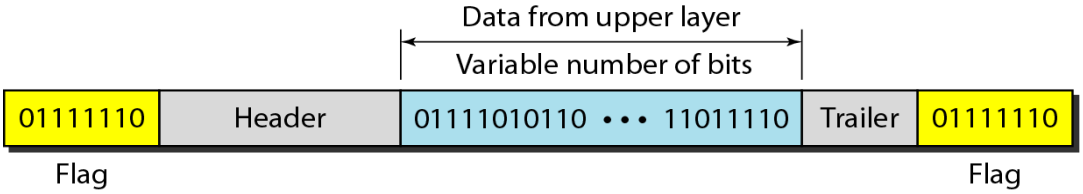
Character-oriented framing was popular when only text was exchanged by the data link layers. The flag could be selected to be any character not used for text communication. Now, however, we send other types of information such as graphs, audio, and video. Any pattern used for the flag could also be part of the information. If this happens, the receiver, when it encounters this pattern in the middle of the data, thinks it has reached the end of the frame. To fix this problem, a byte-stuffing strategy was added to character-oriented framing. In byte stuffing (or character stuffing), a special byte is added to the data section of the frame when there is a character with the same pattern as the flag. The data section is stuffed with an extra byte. This byte is usually called the escape character (ESC), which has a predefined bit pattern. Whenever the receiver encounters the ESC character, it removes it from the data section and treats the next character as data, not a delimiting flag.

Byte stuffing by the escape character allows the presence of the flag in the data section of the frame, but it creates another problem. What happens if the text contains one or more escape characters followed by a flag? The receiver removes the escape character, but keeps the flag, which is incorrectly interpreted as the end of the frame. To solve this problem, the escape characters that are part of the text must also be marked by another escape character. In other words, if the escape character is part of the text, an extra one is added to show that the second one is part of the text. Figure shows the situation.



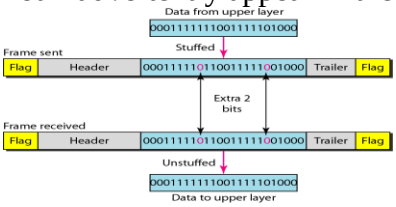
Bit-Oriented Protocols

In a bit-oriented protocol, the data section of a frame is a sequence of bits to be interpreted by the upper layer as text, graphic, audio, video, and so on. However, in addition to headers (and possible trailers), we still need a delimiter to separate one frame from the other. Most protocols use a special 8-bit pattern flag 01111110 as the delimiter to define the beginning and the end of the frame, as shown in Figure.



This flag can create the same type of problem we saw in the byte-oriented protocols. That is, if

the flag pattern appears in the data, we need to somehow inform the receiver that this is not the end of the frame. We do this by stuffing 1 single bit (instead of I byte) to prevent the pattern from looking like a flag. The strategy is called bit stuffing. In bit stuffing, if a 0 and five consecutive I bits are encountered, an extra 0 is added. This extra stuffed bit is eventually removed from the data by the receiver. Note that the extra bit is added after one 0 followed by five 1s regardless of the value of the next bit. This guarantees that the flag field sequence does not inadvertently appear in the frame.



FLOW AND ERROR CONTROL

Data communication requires at least two devices working together, one to send and the other to receive. Even such a basic arrangement requires a great deal of coordination for an intelligible exchange to occur. The most important responsibilities of the data link layer are flow control and error control. Collectively, these functions are known as data link control.

Flow Control

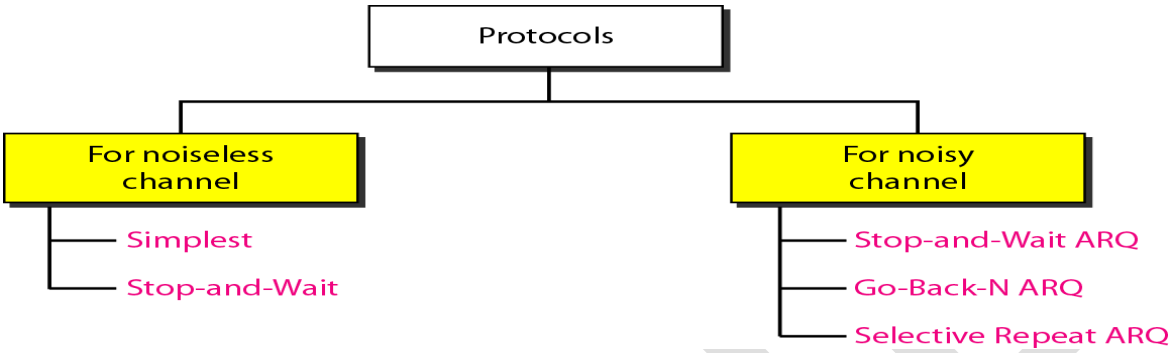
Flow control coordinates the amount of data that can be sent before receiving an acknowledgment and is one of the most important duties of the data link layer. In most protocols, flow control is a set of procedures that tells the sender how much data it can transmit before it must wait for an acknowledgment from the receiver. Any receiving device has a limited speed at which it can process incoming data and a limited amount of memory in which to store incoming data. The receiving device must be able to inform the sending device before those limits are reached and to request that the transmitting device send fewer frames or stop temporarily. Incoming data must be checked and processed before they can be used. The rate of such processing is often slower than the rate of transmission. For this reason, each receiving device has a block of memory, called a *buffer*, reserved for storing incoming data until they are processed. If the buffer begins to fill up, the receiver must be able to tell the sender to halt transmission until it is once again able to receive.

Error Control

Error control is both error detection and error correction. It allows the receiver to inform the sender of any frames lost or damaged in transmission and coordinates the retransmission of those frames by the sender. In the data link layer, the term *error control* refers primarily to methods of error detection and retransmission. Error control in the data link layer is often implemented simply: Any time an error is detected in an exchange, specified frames are retransmitted. This process is called automatic repeat request (ARQ).

PROTOCOLS

Data link layer can combine framing, flow control, and error control to achieve the delivery of data from one node to another. The protocols are normally implemented in software by using one of the common programming languages



All the protocols are unidirectional in the sense that the data frames travel from one node, called the sender, to another node, called the receiver. Although special frames, called acknowledgment (ACK) and negative acknowledgment (NAK) can flow in the opposite direction for flow and error control purposes, data flow in only one direction.

In a real-life network, the data link protocols are implemented as bidirectional; data flow in both directions. In these protocols the flow and error control information such as ACKs and NAKs is included in the data frames in a technique called piggybacking.

NOISELESS CHANNELS

Assume the channel is ideal in which no frames are lost, duplicated, or corrupted. There are two protocols for this type of channel. The first is a protocol that does not use flow control; the second is the one that does. Of course, neither has error control because the channel is a perfect noiseless channel.

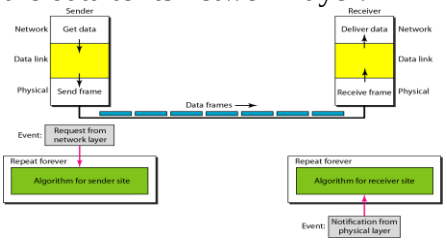
Simplest Protocol

First protocol, the Simplest Protocol, is one that has no flow or en'or control. Like other protocols, it is a unidirectional protocol in which data frames are traveling in only one direction- from the sender to receiver. The receiver can immediately handle any frame it receives with a processing time that is small enough to be negligible. The data link layer of the receiver immediately removes the header from the frame and hands the data packet to its network layer, which can also accept the packet immediately. In other words, the receiver can never be overwhelmed with incoming frames.

Design

There is no need for flow control in this scheme. The data link layer at the sender site gets data from its network layer, makes a frame out of the data, and sends it. The data link layer at the

receiver site receives a frame from its physical layer, extracts data from the frame, and delivers the data to its network layer.



The sender site cannot send a frame until its network layer has a data packet to send. The receiver site cannot deliver a data packet to its network layer until a frame arrives. The procedure at the sender site is constantly running; there is no action until there is a request from the network layer. The procedure at the receiver site is also constantly running, but there is no action until notification from the physical layer arrives. Both procedures are constantly running because they do not know when the corresponding events will occur.

Sender site algorithm

```
1  while(true)                          // Repeat forever
2  {
3    WaitForEvent();                    // Sleep until an event occurs
4    if(Event(RequestToSend))           //There is a packet to send
5    {
6        GetData();
7        MakeFrame();
8        SendFrame();                   //Send the frame
9    }
10 }
```

Receiver site algorithm

```
1  while(true)                          // Repeat forever
2  {
3    WaitForEvent();                    // Sleep until an event occurs
4    if(Event(ArrivalNotification))     //Data frame arrived
5    {
6        ReceiveFrame();
7        ExtractData();
8        DeliverData();                 //Deliver data to network layer
9    }
10 }
```

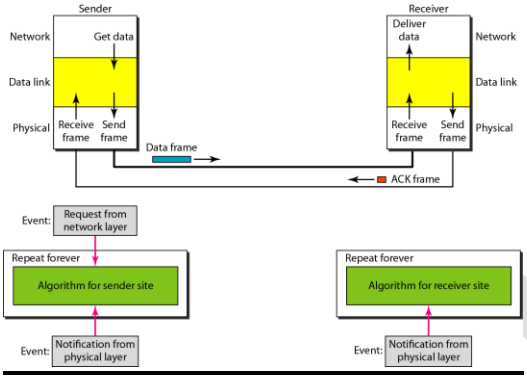
Stop-and-Wait Protocol

If data frames arrive at the receiver site faster than they can be processed, the frames must be stored until their use. Normally, the receiver does not have enough storage space, especially if it is receiving data from many sources. This may result in either the discarding of frames or denial of service. To prevent the receiver from becoming overwhelmed with frames, receiver should tell

the sender to slow down. There must be feedback from the receiver to the sender.
The protocol is called the Stop-and-Wait Protocol because the sender sends one frame, stops until it receives confirmation from the receiver (okay to go ahead), and then sends the next frame. Communication is unidirectional for data frames, but auxiliary ACK frames (simple tokens of acknowledgment) travel from the other direction. Flow control to the previous protocol.

Design

Figure illustrates the mechanism. At any time, there is either one data frame on the forward channel or one ACK frame on the reverse channel, therefore need a half-duplex link.



The sender and receiver side algorithms are given below:

NOISY CHANNELS

Although the Stop-and-Wait Protocol gives an idea of how to add flow control to its predecessor, noiseless channels are nonexistent.

Stop-and-Wait Automatic Repeat Request

The Stop-and-Wait Automatic Repeat Request (Stop-and Wait ARQ), adds a simple error control mechanism to the Stop-and-Wait Protocol.

To detect and correct corrupted frames, redundancy bits are added to data. When the frame arrives at the receiver site, it is checked and if it is corrupted, it is silently discarded. The detection of errors in this protocol is manifested by the silence of the receiver.

Lost frames are more difficult to handle than corrupted ones. In previous protocols, there was no way to identify a frame. The received frame could be the correct one, or a duplicate, or a frame out of order. The solution is to number the frames. When the receiver receives a data frame that is out of order, this means that frames were either lost or duplicated.
The corrupted and lost frames need to be resent in this protocol. If the receiver does not respond when there is an error, how can the sender know which frame to resend? To remedy this problem, the sender keeps a copy of the sent frame. At the same time, it starts
a timer. If the timer expires and there is no ACK for the sent frame, the frame is resent, the copy is held, and the timer is restarted. Since the protocol uses the stop-and-wait mechanism, there is only one specific frame that needs an ACK even though several copies of the same frame can be in the network.

Since an ACK frame can also be corrupted and lost, it too needs redundancy bits and a sequence number. The ACK frame for this protocol has a sequence number field. In this protocol, the sender simply discards a corrupted ACK frame or ignores an out-of-order one

Sequence Numbers
The protocol specifies that frames need to be numbered. This is done by using sequence numbers. A field is added to the data frame to hold the sequence number of that frame.
One important consideration is the range of the sequence numbers. to minimize the frame size, the smallest range that provides unambiguous Communication is considered. The sequence numbers of course can wrap around. For example, if the field is *m* bits long, the sequence numbers start from 0, go to *2m* - 1, and then are repeated.

Assume *x* as a sequence number; only *x* + 1is used after that. There is no need for *x* + 2. To show this, assume that the sender has sent the frame numbered *x.* Three things can happen.
1. The frame arrives safe and sound at the receiver site; the receiver sends an acknowledgment. The acknowledgment arrives at the sender site, causing the sender to send the next frame numbered *x* + 1.
2. The frame arrives safe and sound at the receiver site; the receiver sends an acknowledgment, but the acknowledgment is corrupted or lost. The sender resends the frame (numbered *x)* after the time-out. Note that the frame here is a duplicate. The receiver can recognize this fact because it expects frame *x* + I but frame *x* was received.
3. The frame is corrupted or never arrives at the receiver site; the sender resends the frame (numbered *x)* after the time-out. We can see that there is a need for sequence numbers *x* and *x* + I because the receiver needs to distinguish between case 1 and case 2. But there is no need for a frame to be numbered *x* + 2. In case 1, the frame can be numbered *x* again because frames *x* and *x* + 1 are acknowledged and there is no ambiguity at either site. In cases 2 and 3, the new frame is *x* + I, not *x* + 2. If only *x* and *x* + 1 are needed, we can let *x* = 0 and *x* + I == 1.

Acknowledgment Numbers
Since the sequence numbers must be suitable for both data frames and ACK frames, use this

convention: The acknowledgment numbers always announce the sequence number of the next frame expected by the receiver. For example, if frame 0 has arrived safe and sound, the receiver sends an ACK frame with acknowledgment 1 (meaning frame 1 is expected next). If frame 1 has arrived safe and sound, the receiver sends an ACK frame with acknowledgment 0 (meaning frame 0 is expected).

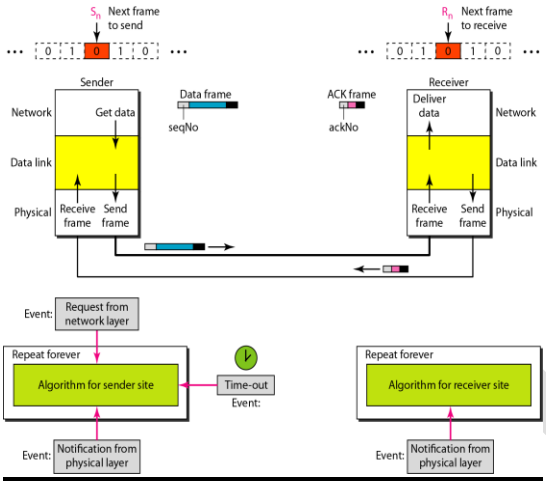


Figure shows the design of the Stop-and-WaitARQ Protocol. The sending device keeps a copy of the last frame transmitted until it receives an acknowledgment for that frame. A data frames uses a seqNo (sequence number); an ACK frame uses an ackNo (acknowledgment number). The sender has a control variable, which we call *Sn* (sender, next frame to send), that holds the sequence number for the next frame to be sent (0 or 1).

The receiver has a control variable, Rn (receiver, next frame expected), that holds the number of the next frame expected. When a frame is sent, the value of Sn is incremented (modulo-2), which means if it is 0, it becomes 1 and vice versa. When a frame is received, the value of Rn is incremented (modulo-2), which means if it is 0, it becomes 1 and vice versa. Three events can happen at the sender site; one event can happen at the receiver site. Variable Sn points to the slot that matches the sequence number of the frame that has been sent, but not acknowledged; Rn points to the slot that matches the sequence number of the expected frame.

Pipelining

In networking and in other areas, a task is often begun before the previous task has ended. This is known as pipelining. Pipelining improves the efficiency of the transmission if the number of bits in transition is large with respect to the bandwidth-delay product

Go-Back-N Automatic Repeat Request

To improve the efficiency of transmission (filling the pipe), multiple frames must be in

transition while waiting for acknowledgment. In other words, more than one frame will be outstanding to keep the channel busy while the sender is waiting for acknowledgment

Go-Back-N Automatic Repeat Request protocol can send several frames before receiving acknowledgments; a copy of these frames is stored until the acknowledgments arrive.

Sequence Numbers

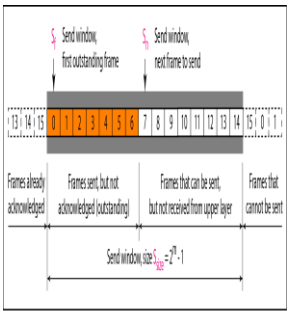
Frames from a sending station are numbered sequentially. If the header of the frame allows *m* bits for the sequence number, the sequence numbers range from 0 to 2^m - 1. For example, if *m* is 4, the only sequence numbers are 0 through 15 inclusive. In other words, the sequence numbers are modulo-2^m

.

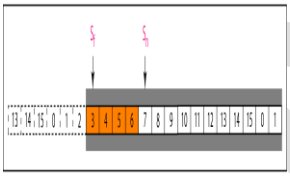
Sliding Window

In this protocol, the sliding window is an abstract concept that defines the range of sequence numbers that is the concern of the sender and receiver. In other words, the sender and receiver need to deal with only part of the possible sequence numbers. The range which is the concern of the sender is called the send sliding window; the range that is the concern of the receiver is called receive sliding window.

The send window is an imaginary box covering the sequence numbers of the data frames which can be in transit. In each window position, some of these sequence numbers define the frames that have been sent; others define those that can be sent. The maximum size of the window is 2^m - 1

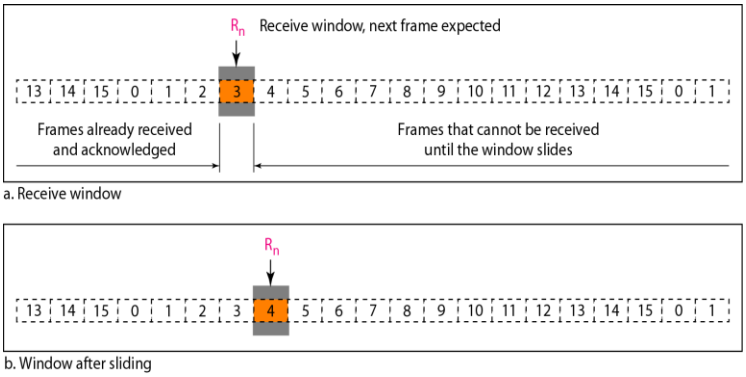


a. Send window before sliding

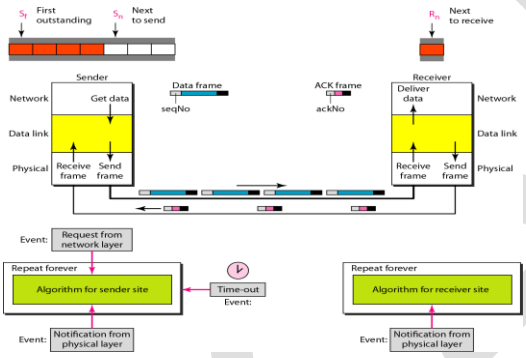


b. Send window after sliding

The receive window makes sure that the correct data frames are received and that the correct acknowledgments are sent. The size of the receive window is always I. The receiver is always looking for the arrival of a specific frame. Any frame arriving out of order is discarded and needs to be resent. Figure shows the receive window.



The sequence numbers to the left of the window belong to the frames already received and acknowledged; the sequence numbers to the right of this window define the frames that cannot be received. Any received frame with a sequence number in these two regions is discarded. Only a frame with a sequence number matching the value of *Rn* is accepted and acknowledged. The receive window also slides, but only one slot at a time.



Timers

The reason is that the only one timer is that, for the first outstanding frame always expires first; all outstanding frames are sent when this timer expires.

Acknowledgment

The receiver sends a positive acknowledgment if a frame has arrived safe and sound and in order. If a frame is damaged or is received out of order, the receiver is silent and will discard all subsequent frames until it receives the one it is expecting. The silence of the receiver causes the timer of the unacknowledged frame at the sender site to expire. This, in turn, causes the sender to go back and resend all frames, beginning with the one with the expired timer. The receiver does not have to acknowledge each frame received. It can send one cumulative acknowledgment for several frames.

Resending a Frame

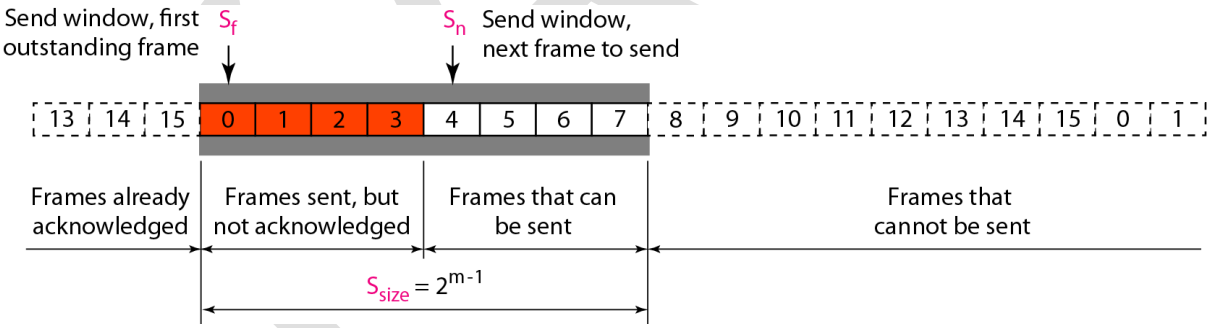
When the timer expires, the sender resends all outstanding frames. For example, suppose the sender has already sent frame 6, but the timer for frame 3 expires. This means that frame 3 has not been acknowledged; the sender goes back and sends frames 3, 4, 5, and 6 again. That is why the protocol is called *Go-Back-N* ARQ.

Selective Repeat Automatic Repeat Request

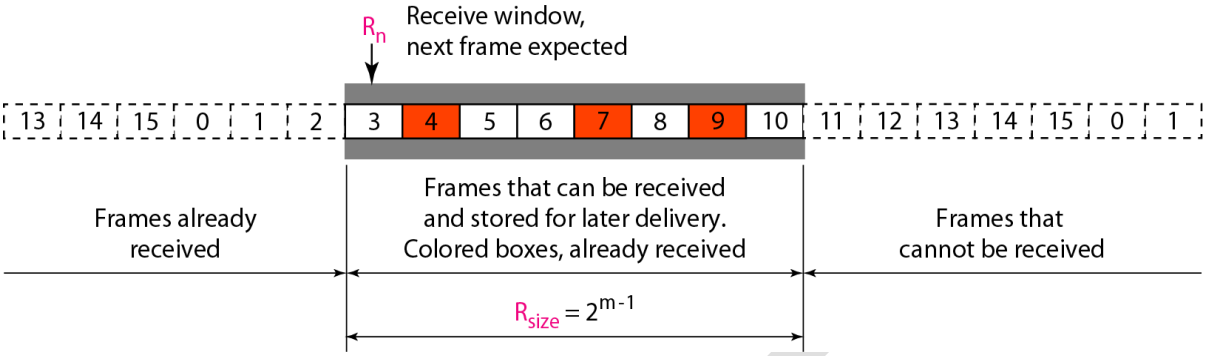
Go-Back-N ARQ simplifies the process at the receiver site. The receiver keeps track of only one variable, and there is no need to buffer out-of-order frames; they are simply discarded. However, this protocol is very inefficient for a noisy link. In a noisy link a frame has a higher probability of damage, which means the resending of multiple frames. This resending uses up the bandwidth and slows down the transmission. For noisy links, there is another mechanism that does not resend *N* frames when just one frame is damaged; only the damaged frame is resent. This mechanism is called Selective Repeat-ARQ. It is more efficient for noisy links, but the processing at the receiver is more complex.

Windows

The Selective Repeat Protocol also uses two windows: a send window and a receive window. However, there are differences between the windows in this protocol and the ones in Go-Back-N. First, the size of the send window is much smaller; it is 2^m-*1*. Second, the receive window is the same size as the send window. The send window maximum size can be 2^m- *1*. For example, if *m* = 4, the sequence numbers go from 0 to 15, but the size of the window is just 8 (it is 15 in the *Go-Back-N* Protocol). The smaller window size means less efficiency in filling the pipe, but the fact that there are fewer duplicate frames can compensate for this. The protocol uses the same variables as Go-Back-N.

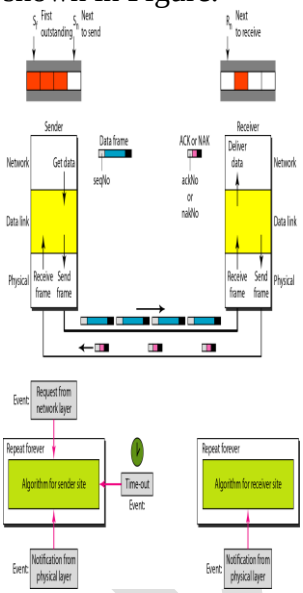


The receive window in Selective Repeat is totally different from the one in Go Back-N. First, the size of the receive window is the same as the size of the send window. The Selective Repeat Protocol allows as many frames as the size of the receive window to arrive out of order and be kept until there is a set of in-order frames to be delivered to the network layer. Because the sizes of the send window and receive window are the same, all the frames in the send frame can arrive out of order and be stored until they can be delivered. However, the receiver never delivers packets out of order to the network layer.



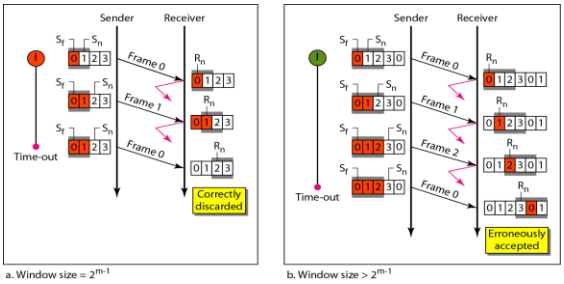
Design

The design in this case is to some extent similar to the Go-Back-N, but more complicated, as shown in Figure.



Window Sizes

The size of the sender and receiver windows must be at most one half of 2^m. For an example, we choose m = 2, which means the size of the window is $2^m/2$or 2. Figure compares a window size of 2 with a window size of 3. If the size of the window is 2 and all acknowledgments are lost, the timer for frame 0 expires and frame 0 is resent. However, the window of the receiver is now expecting frame 2, not frame 0, so this duplicate frame is correctly discarded. When the size of the window is 3 and all acknowledgments are lost, the sender sends a duplicate of frame O. However, this time, the window of the receiver expects to receive frame 0 (0 is part of the window), so it accepts frame 0, not as a duplicate, but as the first frame in the next cycle. This is clearly an error



a. Window size = 2^{m-1} b. Window size > 2^{m-1}

Point to point protocol

HDLC is a general protocol that can be used for both point-to-point and multipoint configurations, one of the most common protocols for point-to-point access is the Point-to-Point Protocol (PPP). The majority of these users have a traditional modem; they are connected to the Internet through a telephone line, which provides the services of the physical layer.

PPP provides several services: 1. PPP defines the format of the frame to be exchanged between devices. 2. PPP defines how two devices can negotiate the establishment of the link and the exchange of data. 3. PPP defines how network layer data are encapsulated in the data link frame. 4. PPP defines how two devices can authenticate each other. 5. PPP provides multiple network layer services supporting a variety of network layer protocols. 6. PPP provides connections over multiple links. 7. PPP provides network address configuration. This is particularly useful when a home user needs a temporary network address to connect to the Internet.

On the other hand, to keep PPP simple, several services are missing: I. PPP does not provide flow control. A sender can send several frames one after another with no concern about overwhelming the receiver. 2. PPP has a very simple mechanism for error control. A CRC field is used to detect errors. If the frame is corrupted, it is silently discarded; the upper-layer protocol needs to take care of the problem. Lack of error control and sequence numbering may cause a packet to be received out of order. 3. PPP does not provide a sophisticated addressing mechanism to handle frames in a multipoint configuration.

Framing

PPP is a byte-oriented protocol. The description of each field follows:

Flag. A PPP frame starts and ends with a I-byte flag with the bit pattern 01111110. Although this pattern is the same as that used in HDLC, there is a big difference. PPP is a byte-oriented protocol; HDLC is a bit-oriented protocol. The flag is treated as a byte, as we will explain later.

- Address. The address field in this protocol is a constant value and set to 11111111 (broadcast address). During negotiation (discussed later), the two parties may agree to omit this byte.

- Control. This field is set to the constant value 11000000 (imitating unnumbered frames in HDLC). As we will discuss later, PPP does not provide any flow control. Error control is also limited to error detection. This means that this field is not needed at all, and again, the two

parties can agree, during negotiation, to omit this byte.

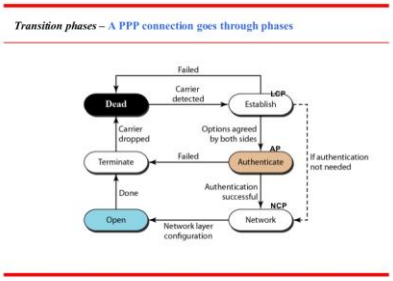
- Protocol. The protocol field defines what is being carried in the data field: either user data or other information. This field is by default 2 bytes long, but the two parties can agree to use only I byte.

- Payload field. This field carries either the user data or other The data field is a sequence of bytes with the default of a maximum of 1500 bytes; but this can be changed during negotiation. The data field is bytestuffed if the flag byte pattern appears in this field. Because there is no field defining the size of the data field, padding is needed if the size is less than the maximum default value or the maximum negotiated value.

- FCS. The frame check sequence (FCS) is simply a 2-byte or 4-byte standard CRe.

Transition Phases

A PPP connection goes through phases which can be shown in a transition phase diagram



11.42

Dead. In the dead phase the link is not being used. There is no active carrier (at the physical layer) and the line is quiet.

Establish. When one of the nodes starts the communication, the connection goes into this phase. In this phase, options are negotiated between the two parties. If the negotiation is successful, the system goes to the authentication phase (if authentication is required) or directly to the networking phase. The link control protocol packets, discussed shortly, are used for this purpose. Several packets may be exchanged here.

Authenticate. The authentication 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, discussed later. If the result is successful, the connection goes to the networking phase; otherwise, it goes to the termination phase.

Network. In the 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. The reason is that PPP supports multiple protocols at the network layer. **Open.** In the open phase, data transfer takes place. When a connection reaches this phase, the exchange of data packets can be started. The connection remains in this phase until one of the endpoints wants to terminate the connection.

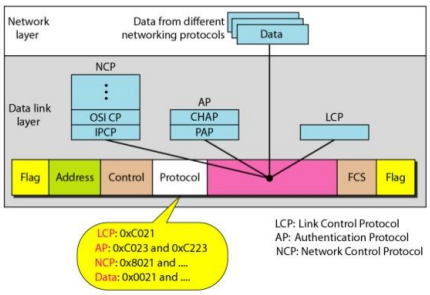
Terminate. In the termination phase the connection is terminated. Several packets are exchanged

between the two ends for house cleaning and closing the link.

Multiplexing

PPP is a data link layer protocol, PPP uses another set of other protocols to establish the link, authenticate the parties involved, and carry the network layer data. Three sets of protocols are defined to make PPP powetful: the Link Control Protocol (LCP), two Authentication Protocols (APs), and several Network Control Protocols (NCPs).

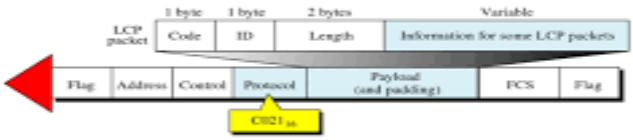
Multiplexing in PPP



Link Control Protocol

The **Link Control Protocol** (LCP) is responsible for establishing, maintaining, configuring, and terminating links. It also provides negotiation mechanisms to set options between the two endpoints. Both endpoints of the link must reach an agreement about the options before the link can be established. All LCP packets are carried in the payload field of the PPP frame with the protocol field set to C021 in hexadecimal.

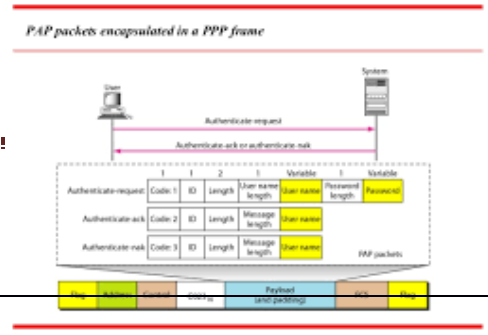
LCP Packet Encapsulated in a Frame



Authentication means validating the identity of a user who needs to access a set of resources.PPP has created two protocols for authentication: Password Authentication Protocol and Challenge Handshake Authentication Protocol.

PAP The **Password Authentication Protocol (PAP)** is a simple authentication procedure with a two-step

PAP packets encapsulated in a PPP frame



11.47

process:

1. The user who wants to access a system sends an authentication identification (usually the user name) and a password.
2. The system checks the validity of the identification and password and either accepts or denies connection.

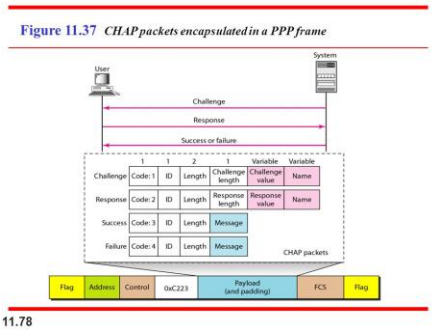
CHAP The **Challenge Handshake Authentication Protocol (CHAP)** is a three-way hand-shaking authentication protocol that provides greater security than PAP. **In** this method, the password is kept secret; it is never sent online.

The system sends the user a challenge packet containing a challenge value, usually a few bytes.

2. The user applies a predefined function that takes the challenge value and the user's own password and creates a result. The user sends the result in the response packet to the system.

3. The system does the same. It applies the same function to the password of the user (known to the system) and the challenge value to create a result. If the result created is the same as the result sent in the response packet, access is granted; otherwise, it is denied. CHAP is more secure than PAP, especially if the system continuously changes

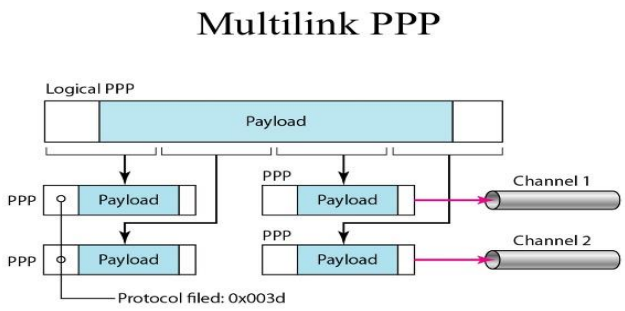
the challenge value. Even if the intruder learns the challenge value and the result, the password is still secret.



11.78

Multilink PPP

PPP was originally designed for a single-channel point-to-point physical link. The availability of multiple channels in a single point-to-point link motivated the development of Multilink PPP. In this case, a logical PPP frame is divided into several actual PPP frames. A segment of the logical frame is carried in the payload of an actual PPP frame.



POSSIBLE QUESTIONS

PART-A [20*1=20 Marks]

ONLINE EXAMINATION

PART-B [5*2=10 Marks]

1. What is single-bit error?
2. What are the functions of data link layer?
3. Define Hamming distance.
4. What is framing?
5. What is cyclic redundancy check?

PART-C [5*6=30 Marks]

1. What is framing? Discuss in short about error control and Flow control.
2. Discuss about Error Correction Methodology in Data-link layer.
3. Write about error detection and error correction in block coding.
4. Describe briefly about point to point protocol.
5. What is check-sum? How it differs from other redundancy methods.
6. Write notes on i) Stop and wait automatic Repeat request ii) Go – back automation repeat request.
7. Explain about the transition phase in ppp protocol.
8. What is framing? Discuss in short about error control and Flow control.
9. What is an Error in data – link layer? Describe Block coding with example.
10. Discuss about Noisy channel in detail.

Karpagam Academy of Higher Education

Department of CS, CA & IT

Class: II BSC CT Batch:2017

Subject: COMPUTER NETWORKS

SubCode: 17CTU303

UNIT III

SL NO	QUESTIONS	OPTION A	OPTION B	OPTION C	OPTION D	ANSWER
1	Transmission errors are usually detected at the……..layer of OSI model	physical	datalink	network	transport	physical
2	Transmission errors are usually corrected at the……..layer of OSI model	network	transport	datalink	physical	transport
3	Datalink layer imposes a ……mechanism to avoid	flow control	error control	access control	none of the above	flow control
4	Error control mechanism of datalink layer is achieved through a ……..added to the end	header	trailer	adress	frames	trailer
5	The datalink layer is responsible for moving……from one hop to next	packets	frames	signals	message	frames
6	In a single_bit error,how many bits in a data unit are changed	one	two	four	five	one
7	In a burst error,how many bits in a data unit are changed	less than 2	2 or more than 2	2	3	2 or more than 2
8	The length of the burst error is measured from ……	first bit to last bit	first corrupted bit to last corrupted	two	three	first corrupted bit to last corrupted
9	Single bit error will least occur in……data transmissions	serial	parallel	synchronous	asynchronous	serial
10	To detect errors or correct errors,we need to send …… with data	address	frames	extra bits	packets	extra bits
11	Which of the following best describes a single bit error	a single bit is inverted	a single bit is inverted per data	a single bit is inverted per	any of the above	a single bit is inverted per data

12	In block coding,we divide our message intp blocks,each of k bits,called	dataword	codeword	integers	none of the above	dataword
13	In block coding,the length of the block is …….	k	r	k+r	k-r	k+r
14	Block coding can detect only ……error	single	burst	multiple	none of the above	single
15	We need ……..redundant bits for error correction than for error detection	less	more	equal	less than or equal to	more
16	The corresponding codeword for the dataword 01 is…..	011	000	101	110	011
17	The hamming distance can easily be found if we apply the …… operation	XOR	OR	AND	NAND	XOR
18	The …… hamming distance is the smallest hamming distance between all	minimum	maximum	equal	none of the above	minimum
19	The hamming distance d(000,111) is …….	1	0	2	3	2
20	To guarantee correction of upto t errors in all cases,the minimum hamming distance in	d(min)=2t+1	d(min)=2t-1	d(min)=2t	d(min)=t+1	d(min)=2t+1
21	To guarantee correction of upto s errors in all cases,the minimum hamming distance in	d(min)=s-1	d(min)=s+1	d(min)=s	none of the above	d(min)=s+1
22	A simple_parity check code is a single bit error detecting code in which n=……	K	K*1	K-1	K+1	K+1
23	The codeword corresponding to the dataword 1111 is	11110	11111	11101	11011	11110
24	A simple_parity check code can detect an ……. Number of errors	odd	even	prime	none of the above	odd
25	The hamming code is a method of ……..	error detection	error correcton	error encapsulation	A and B	error correcton
26	To make the hamming code respond to a burst error of size N,we neeed to make ……	N+1	N-1	N	0	N
27	CRC is used in network such as …….	WAN	LAN and WAN	LAN	MAN	LAN and WAN
28	In CRC there is no error if the remainder at the receiver is……..	equal to the remainder at the	all 0's	non zero	the quotient at the sender	all 0's

29	At the CRC checker,…….means that the dataunit is damaged.	string of 0's	string of 1's	a string of alternating 1's	a non-zero remainder	a non-zero remainder
30	……. Is a regulation of data transmission so that the receiver buffer do not become	flow control	error control	access control	none of the above	flow control
31	……..in the datalink layer separates a message from one source ti a destination or	packets	address	framing	none of the above	framing
32	…….is the process of adding 1 extra byte whenever there is a flag or escape character	byte stuffing	redundancy	bit_stuffing	none of the above	byte stuffing
33	…….is the process of adding 1 extra 0 whenever five consecutive 1's follows a 0 in	byte stuffing	redundancy	bit_stuffing	none of the above	bit_stuffing
34	……in the data link layer is based on automatic repeat request,which is the	error control	flow control	access control	none of the above	error control
35	At any time an error is detected in an exchange specified frames are retransmitted	ARQ	ACK	NAK	SEL	ARQ
36	The datalink layer at the sender side gets data from its……..layer	network	physical	application	transport	network
37	ARQ stands for ……..	acknowledge repeat request	automatic repeat request	automatic repeat	automatic retransmission	automatic repeat quantisation
38	Which of the following is a data link layer function	line discipline	error control	flow control	all the above	all the above
39	In protocols the flow and error control information such as ACK and NAK is	stop and wait	go_back	A and B	piggybacking	piggybacking
40	In stop and wait ARQ ,the sequence of numbers is based on…….	modulo-2-arithmetic	modulo-12-arithmetic	modulo-N-arithmetic	all the above	modulo-2-arithmetic
41	Error correction in …….is done by keeping a copy of the send frames and	stop and wait ARQ	ARQ	ACK	NAQ	stop and wait ARQ
42	In the Go_Back N protocol,the sequence numbers are modulo……..	2^m	2^{m-1}	2^{m+1}	2	2m
43	In sliding window ,the range which is the concern of the sender is called……..	send sliding window	receive sliding window	piggybacking	none of the above	send sliding window
44	Piggypacking is used to improve the efficiency of the ……..protocols.	bidirectional	unidirectional	multidirectional	none of the above	bidirectional
45	The send window can slide …….slots when a valid acknowledgment arrive	one or more	one	two	two or more	one or more

46	The upper sublayer that is responsible for flow and error control is	logical	media access	A and B	all the above	logical
47	The MAC(media access control)sublayer co-ordinates the datalink task within a	LAN	MAN	WAN	LAN and MAN	LAN
48	The lower sublayer that is responsible for multiple access resolution is called	Logical	media access	A and B	all the above	media access
49	In the sliding window method or flow control several frame can be be ……..at a	transit	received	A and B	none of the above	transit
50	The sliding window of the sender expands to the ……..when acknowledgement are	left	middle	right	B and C	right
51	Error detecting codes require ……..nuber of redundant bits.	less	equal	more	less than or equal to	more
52	The datalink layer transforms the ……,a raw transmission facility to a	datalink	physical	network	transport	physical
53	Datalink layer divided into …… functionality oriented sublayer.	one	zero	two	three	two
54	The send window in Go_Back N maximum size can be ……	2^m	2^{m+1}	2	2^{m-1}	2m-1
55	In stop and wait ARQ and Go_Back_N ARQ,the size of the send window	0	3	1	2	1
56	The relationship between m and n in hamming code is ……	n=2m-1	n=m	n=m-1	n=2m+1	n=2m-1
57	A simple parity_check code is a single_bit error detecting code in which n=k+1 with	3	1	0	2	2
58	……..mechanism of datalink layer is achieved through added to the trailer added	ARQ	ARC	Error control	Flow control	Error control
59	In ……,we divide our message into blocks	convolution coding	block coding	linear coding	A and C	block coding
60	The ……layer at the sender site gets data from its network layer.	physical	datalink	application	transport	datalink
61	In the …….protocol,the sequence numbers are modulo 2^m	Go_Back N	Simplest	Stop and wait	all the above	Go_Back N
62	_____ and encapsulates them into frames for transmission.	network layer	physical layer	transport layer	application layer	network layer

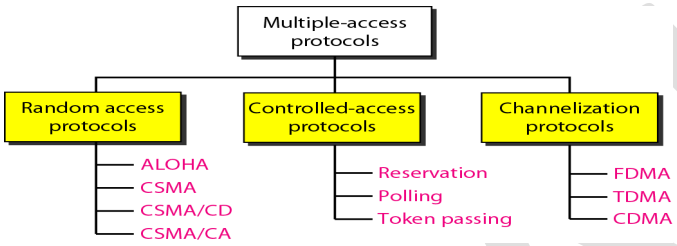
63	Which one of the following task is not done by data link layer?	framing	error control	flow control	channel coding	channel coding
64	CRC stands for_____	cyclic redundancy check	code repeat check	redundancy check	cyclic repeat check	cyclic redundancy check

UNIT IV
SYLLABUS

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.

Multiple Access.

When nodes or stations are connected and use a common link, called a multipoint or broadcast link, we need a multiple-access protocol to coordinate access to the link. Many formal protocols have been devised to handle access to a shared link.



RANDOM ACCESS

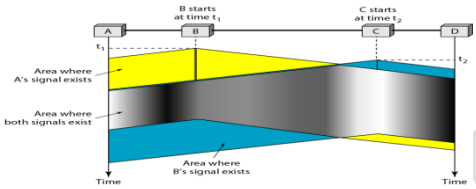
In random access or contention methods, no station is superior to another station and none is assigned the control over another. No station permits, or does not permit, another station to send. At each instance, a station that has data to send uses a procedure defined by the protocol to make a decision on whether or not to send. This decision depends on the state of the medium (idle or busy). In other words, each station can transmit when it desires on the condition that it follows the predefined procedure, including the testing of the state of the medium.

Two features give this method its name. First, there is no scheduled time for a station to transmit. Transmission is random among the stations. That is why these methods are called *random access*. Second, no rules specify which station should send next. Stations compete with one another to access the medium. That is why these methods are also called *contention* methods.

Carrier Sense Multiple Access (CSMA)

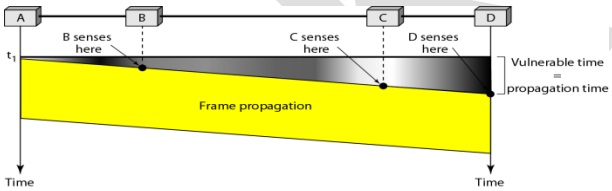
To minimize the chance of collision and, therefore, increase the performance, the CSMA method was developed. The chance of collision can be reduced if a station senses the medium before trying to use it. Carrier sense multiple access (CSMA) requires that each station first listen to the medium (or check the state of the medium) before sending. CSMA can reduce the possibility of collision, but it cannot eliminate it. The reason for this is shown in Figure, a space and time model of a CSMA network. Stations are connected to a shared channel (usually a dedicated medium).

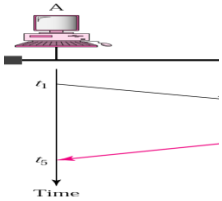
The possibility of collision still exists because of propagation delay; when a station sends a frame, it still takes time (although very short) for the first bit to reach every station and for every station to sense it. In other words, a station may sense the medium and find it idle, only because the first bit sent by another station has not yet been received. At time *t1* station B senses the medium and finds it idle, so it sends a frame. At time *t2 (t2> t1)* station C senses the medium and finds it idle because, at this time, the first bits from station B have not reached station C. Station C also sends a frame. The two signals collide and both frames are destroyed.

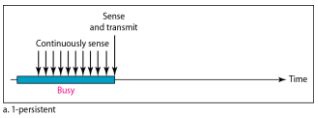


Vulnerable Time

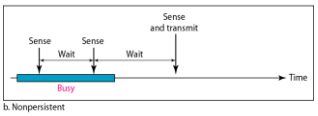
The vulnerable time for CSMA is the propagation time *Tp*. This is the time needed for a signal to propagate from one end of the medium to the other. When a station sends a frame, and any other station tries to send a frame during this time, a collision will result. But if the first bit of the frame reaches the end of the medium, every station will already have heard the bit and will refrain from sending.



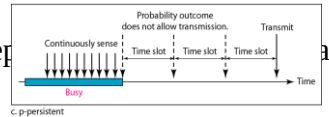




a. 1-persistent



b. Nonpersistent



c. p-persistent

Persistence Methods

I-Persistent: The **I-persistent method** is simple and straightforward. Inthis method, after the station finds the line idle, it sends its frame immediately (with probability I).This method has the highest chance of collision because two or more stations may find the line idle and send their frames immediately.

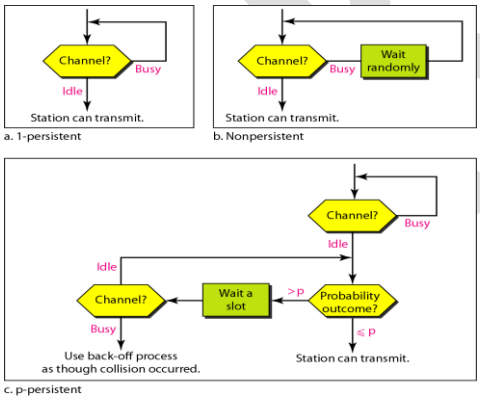
Nonpersistent In the **nonpersistent method,** a station that has a frame to send senses the line. If the line is idle, it sends immediately. If the line is not idle, it waits a random amount of time and then senses the line again. The nonpersistent approach reduces the chance of collision because it is unlikely that two or more stations will wait the same amount of time and retry to send simultaneously. However, this method reduces the efficiency of the network because the medium remains idle when there may be stations with frames to send.

p-PersistentThep-persistent method is used if the channel has time slots with a slot duration equal to or greater than the maximum propagation time. The p-persistent approach combines the advantages of the other two strategies. It reduces the chance of collision and improves efficiency. In this method, after the station finds the line idle it follows these steps:

1. With probability *p*, the station sends its frame.
2. With probability *q* = 1 - *p*, the station waits for the beginning of the next time slotand checks the line again.

a. If the line is idle, it goes to step 1.

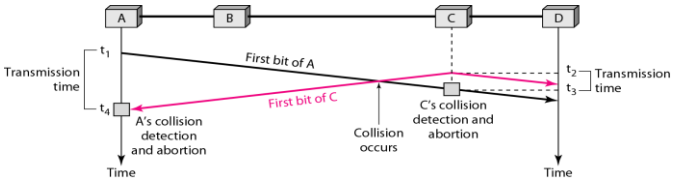
b. If the line is busy, it acts as though a collision has occurred and uses the back off procedure.



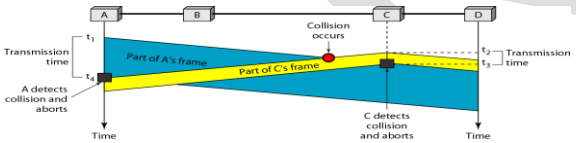
Carrier Sense Multiple Access with Collision Detection (CSMA/CD)

The CSMA method does not specify the procedure following a collision. Carrier sense multiple access with collision detection (CSMA/CD) augments the algorithm to handle the collision. In this method, a station monitors the medium after it sends a frame to see if the transmission was successful. If so, the station is finished. If, however, there is a collision,the frame is sent again.

To better understand CSMA/CD, look at the first bits transmitted by the twostations involved in the collision. Although each station continues to send bits in theframe until it detects the collision, figure shows what happens as the first bits collide. InFigure, stations A and C are involved in the collision.



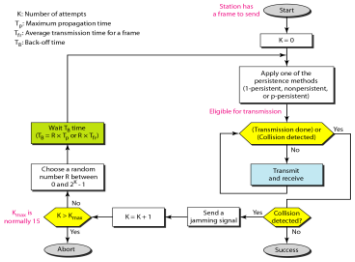
At time *t* 1, station A has executed its persistence procedure and starts sending the bits of its frame. At time *t2,* station C has not yet sensed the first bit sent by A. Station C executes its persistence procedure and starts sending the bits in its frame, which propagate both to the left and to the right. The collision occurs sometime after time *t2'* Station C detects a collision at time *t3* when it receives the first bit of A's frame. Station C immediately (or after a short time, but we assume immediately) aborts transmission. Station A detects collision at time *t4* when it receives the first bit of C's frame; it also immediately aborts transmission. Looking at the figure, we see that A transmits for the duration *t4 - tl;* C transmits for the duration *t3 – t2.* For the protocol to work, the length of any frame divided by the bit rate in this protocol must be more than either of these durations. At time *t4,* the transmission of *A's* frame, though incomplete, is aborted; at time t3, the transmission of B's frame, though incomplete, is aborted. Now that we know the time durations for the two transmissions, we can show a more complete graph in Figure below.



Minimum Frame Size

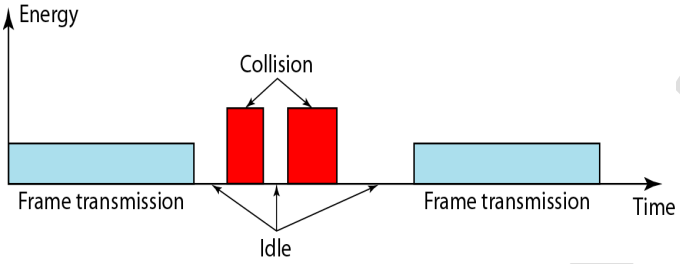
For *CSMAlCD*to work, we need a restriction on the frame size. Before sending the last bit of the frame, the sending station must detect a collision, if any, and abort the transmission. This is so because the station, once the entire frame is sent, does not keep a copy of the frame and does not monitor the line for collision detection. Therefore, the frame transmission time *T*frmust be at least two times the maximum propagation time *Tp.* If the two stations involved in a collision are the maximum distance apart, the signal from the first

takes time *Tp*to reach the second and the effect of the collision takes another time *Tp*to reach the first. So the requirement is that the first station must still be transmitting after *2Tp*



Energy level during transmission, idleness, or collision

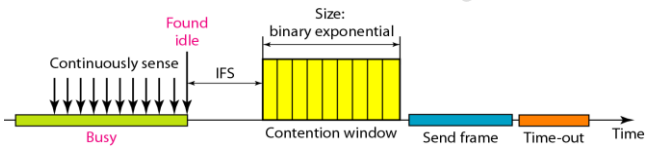
Level of energy in a channel can have three values: zero, normal, and abnormal. At the zero level, the channel is idle. At the normal level, a station has successfully captured the channel and is sending its frame. At the abnormal level, there is a collision and the level of the energy is twice the normal level.



- Throughput of CSMA/CD is greater than that of ALOHA
- The max. throughput occurs at a different value of G and is based on the persistent method and the value of *p* in the *p*-persistent approach
- The max throughput is around 50% when G=1 for 1-persistent, up to 90% when G is between 3 and 8 for non-persistent
- Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)

Carrier sense multiple access with collision avoidance *(CSMAlCA)* was invented for wireless network. Collisions are avoided through the use of CSMA/CA's three strategies: the interframe space, the contention window, and acknowledgments, as shown in Figure.

Interframe Space (IFS)



Collisions are avoided by deferring transmission even if the channel is found idle. When an idle channel is found, the station does not send immediately. It waits for a period of time called the interframe space or IFS.

Even though the channel may appear idle when it is sensed, a distant station may have already started transmitting. The distant station's signal has not yet reached this station. The IFS time allows the front of the transmitted signal by the distant station to reach this station. If after the IFS time the channel is still idle, the station can send.

Contention Window

The contention window is an amount of time divided into slots. A station that is ready to send chooses a random number of slots as its wait time. The number of slots in the window changes according to the binary exponential back-off strategy. This means that it is set to one slot the first time and then doubles each time the station cannot detect an idle channel after the IFS time. This is very similar to the p-persistent method except that a random outcome defines the number of slots taken by the waiting station. One interesting point about the contention window is that the station needs to sense the channel after each time slot. However, if the station finds the channel busy, it does not restart the process; it just stops the timer and restarts it when the channel is sensed as idle. This gives priority to the station with the longest waiting time.

Acknowledgment

With all these precautions, there still may be a collision resulting in destroyed data. In addition, the data may be corrupted during the transmission. The positive acknowledgment and the time-out timer can help guarantee that the receiver has received the frame.

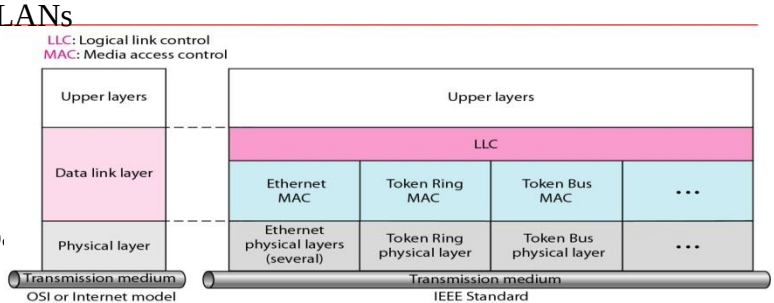
Wired LANs: Ethernet

We learned that a local area network (LAN) is a computer network that is designed for a limited geographic area such as a building or a campus. Although a LAN can be used as an isolated network to connect computers in an organization for the sole purpose of sharing resources, most LANs today are also linked to a wide area network (WAN) or the Internet. The LAN market has several technologies such as Ethernet, Token Ring, Token Bus, FDDI, and ATM LAN. Some of these technologies survived for a while, but Ethernet is by far the dominant technology.

IEEE STANDARDS

In 1985, the Computer Society of the IEEE started a project, called Project 802, to set standards to enable intercommunication among equipment from a variety of manufacturers. Project 802 is a way of specifying functions of the physical layer and the data link layer of major LAN protocols.

IEEE standard for LANs



Data Link Layer:

As we mentioned before, the data link layer in the IEEE standard is divided into two sublayers: LLC and MAC.

 Logical Link Control (LLC) In Chapter 11, we discussed datalink control. We said that data link control handles framing, flow control, and error control. In IEEE Project 802, flow control, error control, and part of the framing duties are collected into one sublayer called the logical link control. Framing is handled in both the LLC sublayer and the MAC sublayer.

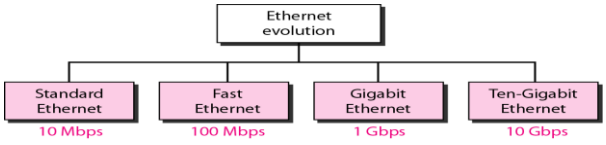
 The LLC provides one single data link control protocol for all IEEE LANs. In this way, the LLC is different from the media access control sublayer MAC, which provides different protocols for different LANs

The purpose of the LLC is to provide flow and error control for the upper-layer protocols that actually demand these services. *Media Access Control (MAC)* In Chapter 12, we discussedmultiple access methods including random access, controlledaccess, and channelization. IEEE Project 802 has created a sublayer called media access control that defines the specific access method for each LAN.Forexample, it defines *CSMA/CD as the media access methodfor Ethernet LANs and the token passing* method forTokenRing and Token Bus LANs. As we discussed in the previous section, part of the framing function is also handled by the MAC layer.In contrast to the LLC sublayer, the MAC sublayer contains a number of distinct modules; each defines the access method and the framing format specific to the corresponding LAN protocol.

STANDARD ETHERNET

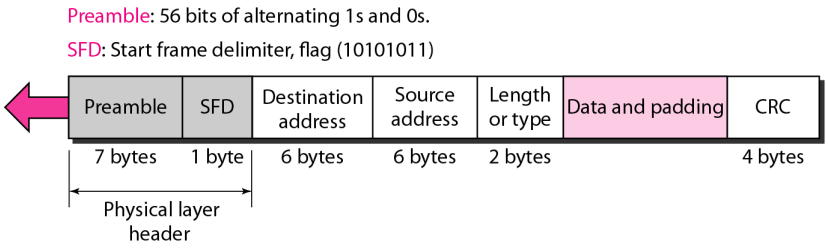
The original Ethernet was created in 1976 at Xerox's Palo Alto Research Center (PARC). Since then, it has gone through four generations.

Ethernet evolution through four generations



MAC Sublayer

In Standard Ethernet, the MAC sublayer governs the operation of the access method. It also frames data received from the upper layer and passes them to the physical layer.



Frame Format

Preamble. The first field of the 802.3 frame contains 7 bytes (56 bits) of alternating Os and 1s that alerts the receiving system to the coming frame and enables it to synchronize its input timing. The pattern provides only an alert and a timing pulse. The 56-bit pattern allows the stations to miss some bits at the beginning of the frame. The preamble is actually added at the physical layer and is not (formally) part of the frame.

Start frame delimiter (SFD).

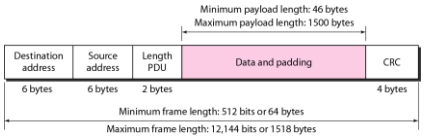
The second field (l byte: 10101011) signals the beginning of the frame. The SFD warns the station or stations that this is the last chance for synchronization. The last 2 bits is 11 and alerts the receiver that the next field is the destination address.

Destination address (DA). The DA field is 6 bytes and contains the physical address of the destination station or stations to receive the packet.

Source address (SA). The SA field is also 6 bytes and contains the physical address of the sender of the packet. Length or type. This field is defined as a type field or length field. The original Ethernet used this field as the type field to define the upper-layer protocol using the MAC frame. The IEEE standard used it as the length field to define the number of bytes in the data field. Both uses are common today.

Data. This field carries data encapsulated from the upper-layer protocols. It is a minimum of 46 and a maximum of 1500 bytes,

CRC. The last field contains error detection information, in this case a CRC-32

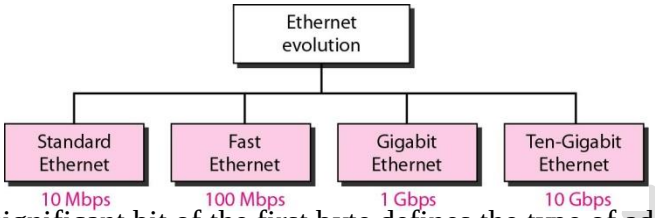


Addressing

- Each station on an Ethernet network (such as a PC, workstation, or printer) has its own network interface card (NIC). The NIC fits inside the station and provides the station with a 6-byte physical address.

As shown in Figure 13.6, the Ethernet address is 6 bytes (48 bits), nonnally written in hexadecimal notation, with a colon between the bytes.

- Unicast, Multicast, and Broadcast Addresses A source address is always a unicast address-the frame comes from only one station. The destination address, however, can be unicast, multicast, or broadcast. Figure 13.7 shows how to distinguish a unicast address from a multicast address. If the least significant bit of the first byte in a destination address is 0, the address is unicast; otherwise, it is multicast.



The least significant bit of the first byte defines the type of address.

If the bit is 0, the address is unicast; otherwise, it is multicast

The broadcast destination address is a special case of the multicast address in which all bits are 1s

Ethernet

Access method: 1-persistent CSMA/CD

Slot time = rount-trip time + time required to send the jam sequence

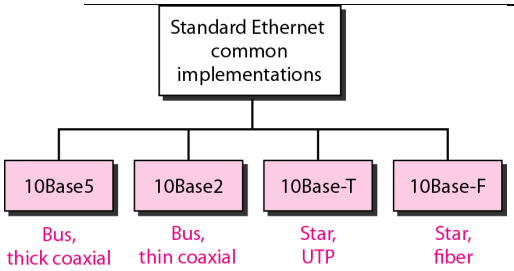
512 bits for Ethernet, 51.2 μs for 10 Mbps Ethernet

Slot time and collision

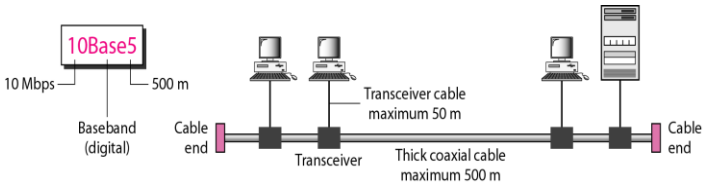
Slot time and maximum network length

- MaxLength = PropagationSpeed x SlotTime/2
- MaxLength = $(2 \times 10^8) \times (51.2 \times 10^{-6}/2) = 5120$ m
- MaxLength = 2500 m 48 % of the theoretical calculation by considering delay times in repeaters and interfaces, and the time required to send the jam sequence

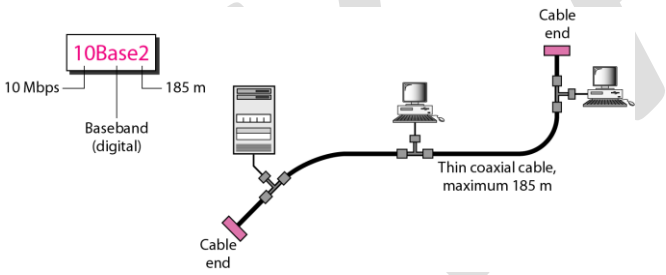
Physical Layer: Ethernet



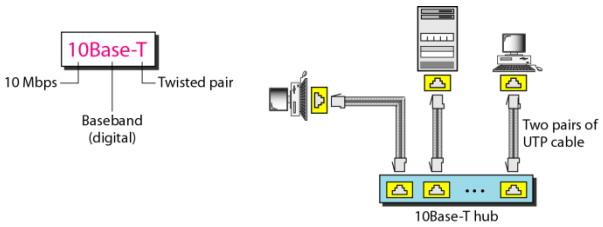
lOBase5: Thick Ethernet The first implementation is called 10Base5, thick Ethernet, or Thicknet. The nickname derives from the size of the cable. lOBase5 was the first Ethernet specification to use a bus topology with an external transceiver (transmitter/receiver) connected via a tap to a thick coaxial cable.



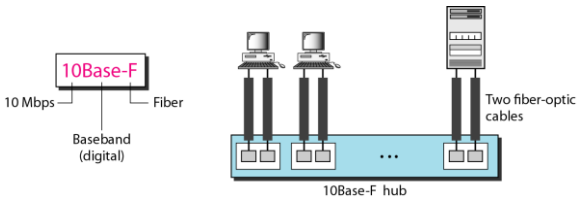
10Base2: Thin Ethernet The second implementation is called lOBase2, thin Ethernet, or Cheapernet. 1OBase2 also uses a bus topology, but the cable is much thinner and more flexible. The cable can be bent to pass very close to the stations. In this case, the transceiver is normally part of the network interface card (NIC), which is installed inside the station. Figure 13.11 shows the schematic diagram of a IOBase2 implementation. ν Note This implementation is more cost effective than 10Base5 because thin coaxial cable is less expensive than thick coaxial and the tee connections are much cheaper than taps. Installation is simpler because the thin coaxial cable is very flexible. However, the length of each segment cannot exceed 185 m (close to 200 m) due to the high level of thin coaxial cable

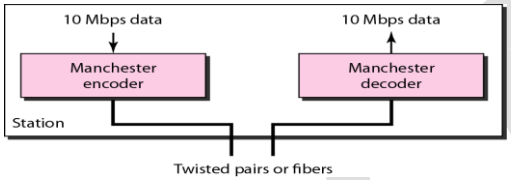


lOBase-T: Twisted-Pair Ethernet The third implementation is called lOBase-T or twisted-pair Ethernet. 1OBase-T uses a physical star topology. The stations are connected to a hub via two pairs of twisted cable, as shown in Figure 13.12. ν Note that two pairs of twisted cable create two paths (one for sending and one for receiving) between the station and the hub. Any collision here happens in the hub. ν The maximum length of the twisted cable here is defined as 100 m, to minimize the effect of attenuation in the twisted cable.



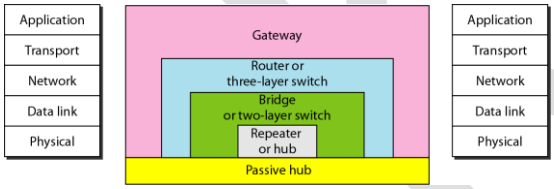
lOBase-F: Fiber Ethernet Although there are several types of optical fiber lO Mbps Ethernet, the most common is called 10Base-F. lOBase-F uses a star topology to connect stations to a hub. The stations are connected to the hub using two fiber-optic cables,



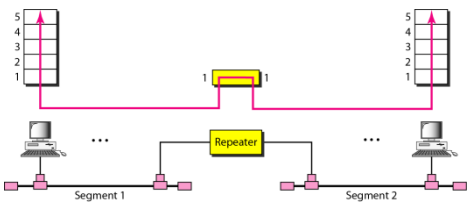


Connecting LANs, Backbone Networks, and Virtual LANs

Five categories of connecting devices



A repeater connecting two segments of a LAN

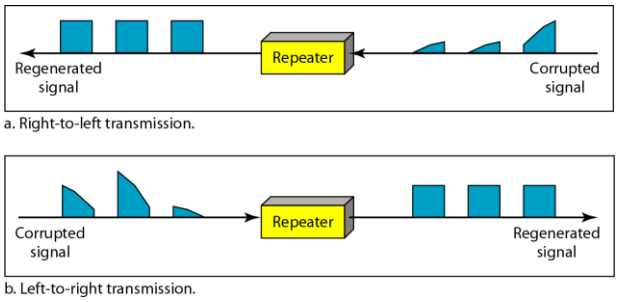


A repeater connects segments of a LAN.

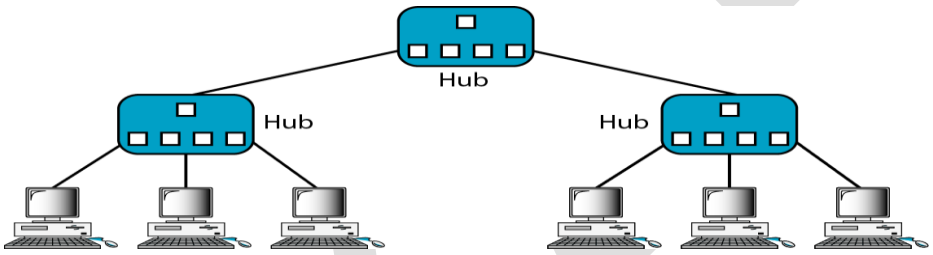
A repeater forwards every frame – there is no filtering.

A repeater is a regenerator, not an amplifier.

Function of a repeater



A hierarchy of hubs

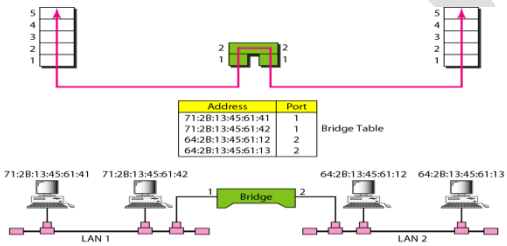


A hub is a multi-port repeater, used in star-wired LANs (Ethernet).

Because of the amount of traffic and collisions, hubs can only be used in small network configurations.

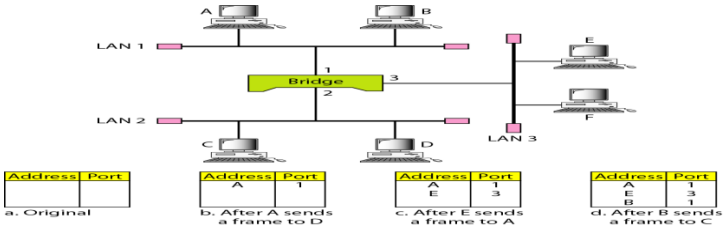
A bridge has a table used in filtering decisions.

A bridge connecting two LANs

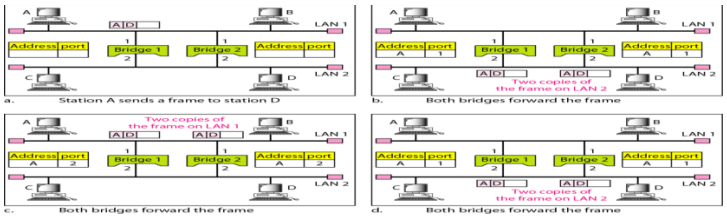


A bridge does not change the physical (MAC) addresses in a frame

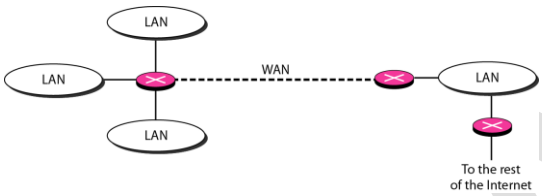
A learning bridge and the process of learning



Loop problem in a learning bridge



Routers connecting independent LANs and WANs



Network layer protocol of Internet

INTERNETWORKING

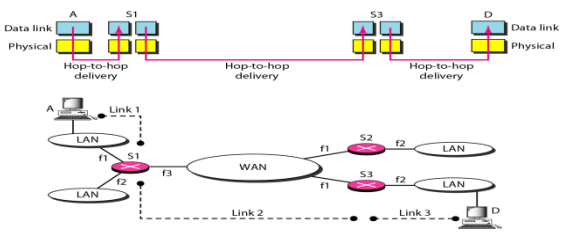
connecting networks together to make an internetwork or an internet.

Network Layer

- Need
  - A frame has no routing info.
  - DL layer has no routing info.
  - For a router with 3+ NIC's,
- how to deliver a packet through multiple links.

- How to find a next hop router
- Responsibility
  - Host-to-host delivery
  - For routing packets through the router and switches.

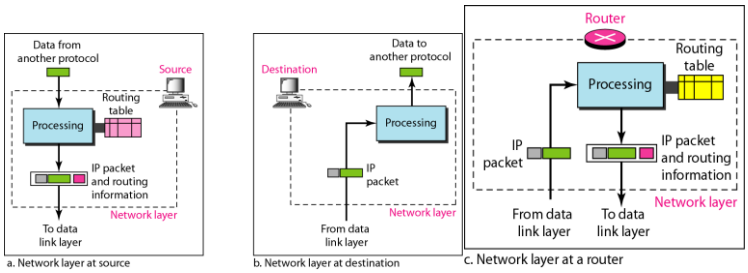
Links between two hosts



- **Source**
  - Creating a packet from the upper layer.
  - The header contains source and destination IP addresses.
  - Checking the routing table to find the routing info (eg. Outgoing interface, or machine address of the next hop)
  - If the packet is larger than MTU, fragment it.
  - Note that it is different from L4 segmentation/reassembly
- **Router**
  - Routing the packet by consulting the routing table for each incoming packet and find the i/f that the packet must be sent to**.**
- **Destination**
  - Address verification.

◦ For fragmented frames, wait for all fragmentations then reassemble them before delivering the packet to the upper layer.

Network layer at the source, router, and destination

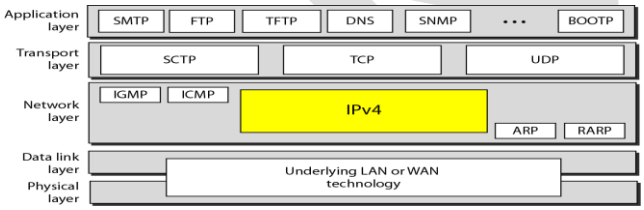


Internet as an L3

- Switching at the network layer in the Internet uses the datagram approach to packet switching.
  - ◦ Use of globally unique address for each packet
- Communication at the network layer in the Internet is connectionless.
  - ◦ Each packet is treated independently by the intermediate routers.
  - ◦ Packets in a message may travel through different paths.

IPv4

The Internet Protocol version 4 (IPv4) is the delivery mechanism used by the TCP/IP protocols. Figure shows the position of IPv4 in the suite.

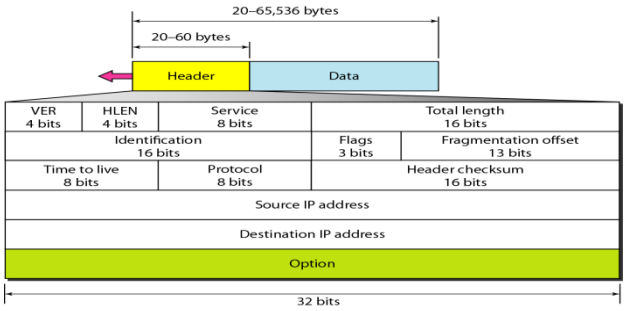


IPv4 is an unreliable and connectionless datagram protocol-a best-effort delivery service. The term *best-effort* means that IPv4 provides no error control or flow control (except for error detection on the header). IPv4 assumes the unreliability of the underlying layers and does its best to get a transmission through to its destination, but with no guarantees.

IPv4 is also a connectionless protocol for a packet-switching network that uses the datagram approach. This means that each datagram is handled independently, and each datagram can follow a different route to the destination. This implies that datagrams sent by the same source to the same destination could arrive out of order. Also, some could be lost or corrupted during transmission. Again, IPv4 relies on a higher-level protocol to take care of all these problems.

Datagram

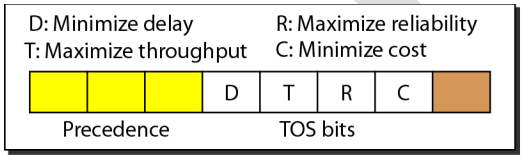
Packets in the IPv4 layer are called datagrams. Figure below shows the IPv4 datagram format.



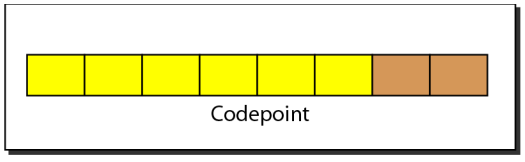
A datagram is a variable-length packet consisting of two parts: header and data.

The header is 20 to 60 bytes in length and contains information essential to routing and delivery. It is customary in *TCP/IP* to show the header in 4-byte sections. A brief description of each field is given below.

- Version (VER). This 4-bit field defines the version of the IPv4 protocol.
- Header length (HLEN). This 4-bit field defines the total length of the datagram header in 4-byte words. This field is needed because the length of the header is variable (between 20 and 60 bytes)
- Services. IETF has changed the interpretation and name of this 8-bit field. This field, previously called service type, is now called differentiated services.



Service type



Differentiated services

1. Service Type

In this interpretation, the first 3 bits are called precedence bits. The next 4 bits are called type of service (TOS) bits, and the last bit is not used.

a. Precedence is a 3-bit subfield ranging from 0 (000 in binary) to 7 (111 in binary). The precedence defines

the priority of the datagram in issues such as congestion.

b. TOS bits is a 4-bit subfield with each bit having a special meaning. Although a bit can be either 0 or 1, one and only one of the bits can have the value of 1 in each datagram. The bit patterns and their interpretations are given in Table

2. Differentiated Services

In this interpretation, the first 6 bits make up the codepoint subfield, and the last 2 bits are not used. The codepoint subfield can be used in two different ways.

a. When the 3 rightmost bits are Os, the 3 leftmost bits are interpreted the same as the precedence bits in the service type interpretation. In other words, it is compatible with the old interpretation.

When the 3 rightmost bits are not all Os, the 6 bits define 64 services based on the priority assignment by the Internet or local authorities according to Table below. The first category contains 32 service types; the second and the third each contain 16. The first category (numbers 0, 2,4, ... ,62) is assigned by the Internet authorities (IETF). The second category (3, 7, 11, 15, , 63) can be used by local authorities (organizations). The third category (1, 5, 9, ,61) is temporary and can be used for experimental purposes.

- Total length. This is a In-bit field that defines the total length (header plus data) of the IPv4 datagram in bytes. To find the length of the data coming from the upper layer, subtract the header length from the total length. The header length can be found by multiplying the value in the HLEN field by 4.

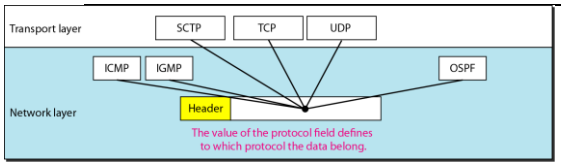
Length of data =total length - header length

Since the field length is 16 bits, the total length of the IPv4 datagram is limited to 65,535 (216 - 1) bytes, of which 20 to 60 bytes are the header and the rest is data from the upper layer.

- Time to live. A datagram has a limited lifetime in its travel through an internet.

This field was originally designed to hold a timestamp, which was decremented by each visited router. The datagram was discarded when the value became zero. Today, this field is used mostly to control the maximum number of hops (routers) visited by the datagram. When a source host sends the datagram, it stores a number in this field. This value is approximately 2 times the maximum number of routes between any two hosts. Each router that processes the datagram decrements this number by 1. If this value, after being decremented, is zero, the router discards the datagram.

- Protocol. This 8-bit field defines the higher-level protocol that uses the services of the IPv4 layer. An IPv4 datagram can encapsulate data from several higher-level protocols such as TCP, UDP, ICMP, and IGMP. This field specifies the final destination protocol to which the IPv4 datagram is delivered.



- Checksum. First, the value of the checksum field is set to O. Then the entire header is divided into 16-bit sections and added together. The result (sum) is complemented and inserted into the checksum field. The checksum in the IPv4 packet covers only the header, not the data.
- Source address. This 32-bit field defines the IPv4 address of the source. This field must remain unchanged during the time the IPv4 datagram travels from the source host to the destination host.
- Destination address. This 32-bit field defines the IPv4 address of the destination. This field must remain unchanged during the time the IPv4 datagram travels from the source host to the destination host.

Fragmentation

A datagram can travel through different networks. Each router decapsulates the IPv4 datagram from the frame it receives, processes it, and then encapsulates it in another frame. The format and size of the received frame depend on the protocol used by the physical network through which the frame has just traveled. The format and size of the sent frame depend on the protocol used by the physical network through which the frame is going to travel.

Maximum Transfer Unit (MTU)

Each data link layer protocol has its own frame format in most protocols. One of the fields defined in the format is the maximum size of the data field. In other words, when a datagram is encapsulated in a frame, the total size of the datagram must be less than this maximum size, which is defined by the restrictions imposed by the hardware and software used in the network The value of the MTU depends on the physical network protocol

To make the IPv4 protocol independent of the physical network, the designers decided to make the maximum length of the IPv4 datagram equal to 65,535 bytes.This is called **fragmentation.**

The source usually does not fragment the IPv4 packet. The transport layer will instead segment the data into a size that can be accommodated by IPv4 and the data link layer in use. When a datagram is fragmented, each fragment has its own header with most of the fields repeated, but with some changed. A fragmented datagram may itself be fragmented if it encounters a network with an even smaller MTU. In other words, a datagram can be fragmented several times before it reaches the final destination. The reassembly of the datagram is done only by the destination host because each fragment becomes an independent datagram

Fields Related to Fragmentation

The fields that are related to fragmentation and reassembly of an IPv4 datagram are the identification, flags, and fragmentation offset fields.

- Identification. This 16-bit field identifies a datagram originating from the source host. The combination of the identification and source IPv4 address must uniquely define a datagram as it leaves the source host. To guarantee uniqueness, the IPv4 protocol uses a counter to label the datagrams. The counter is initialized to a positive number. When the IPv4 protocol sends a datagram, it copies the current value of the counter to the identification field and increments the counter by 1. As long as the counter is kept in the main memory, uniqueness is guaranteed. When a datagram is fragmented, the value in the identification field is copied to all fragments. In other words, all fragments have the same identification number, the same as the original datagram. The identification number helps the destination in reassembling the datagram.
- Flags. This is a 3-bit field. The first bit is reserved. The second bit is called the *donotfragment*bit. If its value is 1, the machine must not fragment the datagram. If it cannot pass the datagram through any available physical network, it discards the datagram and sends an ICMP error message to the source host. If its value is 0, the datagram can be fragmented if necessary. The third bit is called the *more fragment* bit. If its value is 1, it means the datagram is not the last fragment; there are more fragments after this one. If its value is 0, it means this is the last or only fragment
- Fragmentation offset. This 13-bit field shows the relative position of this fragment with respect to the whole datagram. It is the offset of the data in the original datagram measured in units of 8 byte

IPv6

(Internetworking Protocol, version 6), also known as IPng (Internetworking Protocol, next generation), was proposed and is now a standard. In IPv6, the Internet protocol was extensively modified to accommodate the unforeseen growth of the Internet. The format and the length of the IP address were changed along with the packet format. Related protocols, such as ICMP, were also modified. Other protocols in the network layer, such as ARP, RARP, and IGMP. Communications experts predict that IPv6 and its related protocols will soon replace the current IP version. The adoption of IPv6 has been slow. The reason is that the original motivation for its development, depletion of IPv4 addresses, has been remedied by short-term strategies such as classless addressing and NAT. However, the fast-spreading use of the Internet, and new services such as mobile IP, IP telephony, and IP-capable mobile telephony, may eventually require the total replacement of IPv4 with IPv6.

Advantages

The next-generation IP, or IPv6, has some advantages over IPv4 that can be summarized as follows:

O **Larger address space**. An IPv6 address is 128 bits long, as we discussed in Chapter 19. Compared with the 32-bit address of IPv4, this is a huge (296) increase in the address space.

O**Better header format**. IPv6 uses a new header format in which options are separated from the base header and inserted, when needed, between the base header and the upper-layer data. This simplifies and speeds up the routing process because most of the options do not need to be checked by routers.

O**New options**. IPv6 has new options to allow for additional functionalities.

O**Allowance for extension**. IPv6 is designed to allow the extension of the protocol if required by new technologies or applications.

O**Support for resource allocation**. In IPv6, the type-of-service field has been removed, but a mechanism (calledjlow*label)* has been added to enable the source to request special handling of the packet. This mechanism can be used to support traffic such as real-time audio and video.

O**Support for more security**. The encryption and authentication options in IPv6 provide confidentiality and integrity of the packet.

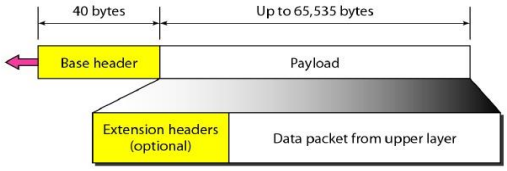
Packet Format

Each packet is composed of a mandatory base header followed by the payload. The payload consists of two parts: optional extension headers and data from an upper layer. The base header occupies 40 bytes, whereas the extension headers and data from the upper layer contain up to 65,535 bytes oinformation. These fields are as follows:

O Version. This 4-bit field defines the version number of the IP. For IPv6, the value is 6.

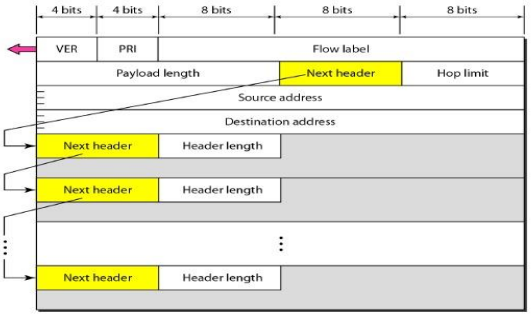
OPriority. The 4-bit priority field defines the priority of the packet with respect to traffic congestion

Figure 20.15 *IPv6 datagram header and payload*



20.39

Figure 20.16 *Format of an IPv6 datagram*



20.40

Flow label. The flow label is a 3-byte (24-bit) field that is designed to provide special handling for a particular flow of data.

Payload length. The 2-byte payload length field defines the length of the IP datagram excluding the base header.

Next header. The next header is an 8-bit field defining the header that follows the base header in the datagram. The next header is either one of the optional extension headers used by IP or the header of an encapsulated packet such as UDP or TCP. Each extension header also contains this field. Table 20.6 shows the values of next headers. Note that this field in version 4 is called the *protocol.*

Hop limit. This 8-bit hop limit field serves the same purpose as the TIL field in IPv4.

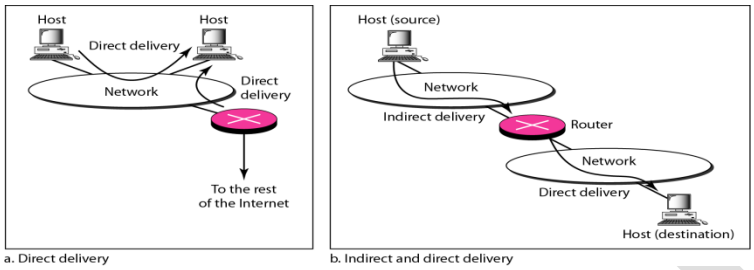
Source address. The source address field is a 16-byte (128-bit) Internet address that identifies the original source of the datagram.

Destination address. The destination address field is a 16-byte (128-bit) Internet address that usually identifies the final destination of the datagram. However, if source routing is used, this field contains the address of the next router.

DELIVERY

The network layer supervises the handling of the packets by the underlying physical networks. We define this handling as the delivery of a packet.

- Direct delivery occurs when the source and destination of the packet are located on the same physical network or when the delivery is between the last router and the destination host.
- If the destination host is not on the same network as the deliverer, the packet is delivered indirectly. The packet goes from router to router until it reaches the one connected to the same physical network as its final destination.



a. Direct delivery
b. Indirect and direct delivery

FORWARDING

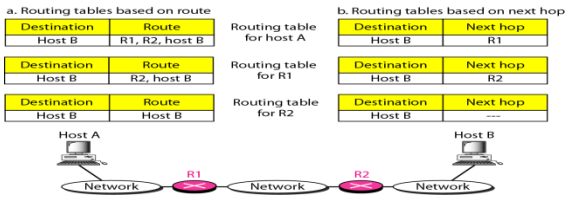
Forwarding means to place the packet in its route to its destination. Forwarding requires a host or a router to have a routing table. When a host has a packet to send or when a router has received a packet to be forwarded, it looks at this table to find the route to the final destination.

Forwarding Techniques

Several techniques can make the size of the routing table manageable and also handle issues such as security.

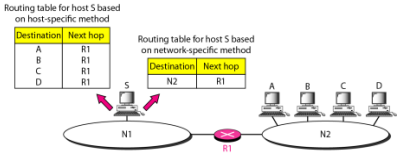
Next-Hop Method Versus Route Method

One technique to reduce the contents of a routing table is called the next-hop method. In this technique, the routing table holds only the address of the next hop instead of information about the complete route (route method). The entries of a routing table must be consistent with one another.



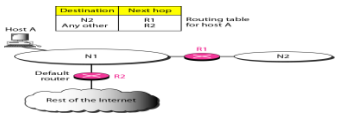
Network-Specific Method Versus Host-Specific Method

A second technique to reduce the routing table and simplify the searching process is called the network-specific method. Here, instead of having an entry for every destination host connected to the same physical network (host-specific method), only one entry that defines the address of the destination network itself. In other words, we treat all hosts connected to the same network as one single entity



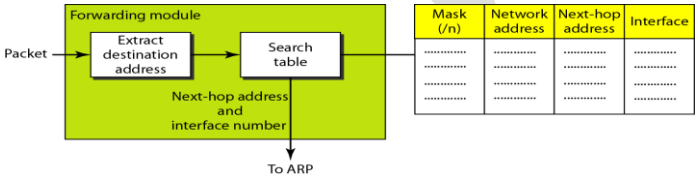
Default Method

Another technique to simplify routing is called the default method. In Figure below host A is connected to a network with two routers. Router Rl routes the packets to hosts connected to network N2. However, for the rest of the Internet, router R2 is used. So instead of listing all networks in the entire Internet, host A can just have one entry called the *default* (normally defined as network address 0.0.0.0).



Forwarding Process

We assume that hosts and routers use classless addressing because classful addressing can be treated as a special case of classless addressing. In classless addressing, the routing table needs to have one row of information for each block involved. The table needs to be searched based on the network address (first address in the block). Unfortunately, the destination address in the packet gives no clue about the network address. To solve the problem, we need to include the mask *(In)* in the table; we need to have an extra column that includes the mask for the corresponding block. Figure shows a simple forwarding module for classless addressing.

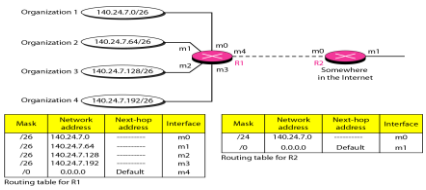


Address Aggregation

When we use classless addressing, it is likely that the number of routing table entries will increase. This is so because the intent of classless addressing is to divide up the whole address space into manageable blocks. The

increased size of the table results in an increase in the amount of time needed to search the table. To alleviate the problem, the idea of address aggregation was designed.

In Figure below we have two routers. Router Rl is connected to networks of four organizations that each use 64 addresses. Router R2 is somewhere far from Rl. Router Rl has a longer routing table because each packet must be correctly routed to the appropriate organization. Router R2, on the other hand, can have a very small routing table. For R2, any packet with destination 140.24.7.0 to 140.24.7.255 is sent out from interface m0 regardless of the organization number. This is called address aggregation because the blocks of addresses for four organizations are aggregated into one larger block. Router R2 would have a longer routing table if each organization had addresses that could not be aggregated into one block.



Mask	Network address	Next-hop address	Interface
/26	140.24.7.0	----------	m0
/26	140.24.7.64	----------	m1
/26	140.24.7.128	----------	m2
/26	140.24.7.192	----------	m3
/0	0.0.0.0	Default	m4

Routing table for R1

Mask	Network address	Next-hop address	Interface
/24	140.24.7.0	----------	m0
/0	0.0.0.0	Default	m1

Routing table for R2

Routing Table

- A static routing table contains information entered manually.
- A dynamic routing table is updated periodically by using one of the dynamic routing protocols such as RIP, OSPF, or BGP. Whenever there is a change in the Internet, such as a shutdown of a router or breaking of a link, the dynamic routing protocols update all the tables in the routers (and eventually in the host) automatically.

Mask	Network address	Next-hop address	Interface	Flags	Reference count	Use
----------	----------	----------	----------	----------	----------	----------

- Mask. This field defines the mask applied for the entry.
- Network address. This field defines the network address to which the packet is finally delivered. In the case of host-specific routing, this field defines the address of the destination host.
- Next-hop address. This field defines the address of the next-hop router to which the packet is delivered.
- Interface. This field shows the name of the interface.
- Flags. This field defines up to five flags.

a. U (up). The U flag indicates the router is up and running. Ifthis flag is not present, it means that the router is down. The packet cannot be forwarded and is discarded.

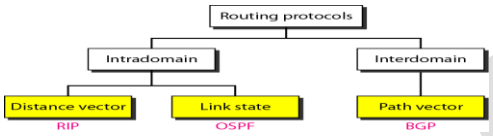
b. G (gateway). The G flag means that the destination is in another network. The packet is delivered to the next-hop router for delivery (indirect delivery). When this flag is missing, it means the destination is in this network (direct delivery).

c. H (host-specific). The H flag indicates that the entry in the network address field is a host-specific address. When it is missing, it means that the address is only the network address of the destination.

d. D (added by redirection). The D flag indicates that routing information for this destination has been added to the host routing table by a redirection message from ICMP.

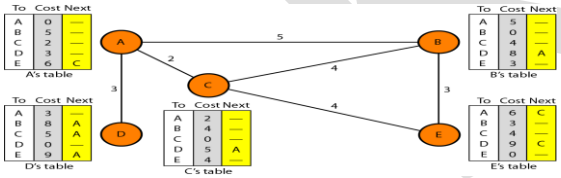
e. M (modified by redirection). The M flag indicates that the routing information for this destination has been modified by a redirection message from ICMP.

- Reference count. This field gives the number of users of this route at the moment.
- Use. This field shows the number of packets transmitted through this router for the corresponding destination.



Distance Vector Routing

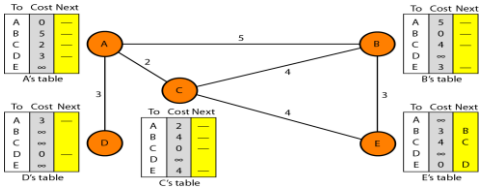
In distance vector routing, the least-cost route between any two nodes is the route with minimum distance. In this protocol, as the name implies, each node maintains a vector (table) of minimum distances to every node. The table at each node also guides the packets to the desired node by showing the next stop in the route (next-hop routing).



Initialization

The tables above are stable; each node knows how to reach any other node and the cost. At the beginning, however, this is not the case. Each node can know only the distance between itself and its immediate neighbors, those directly connected to it. So for the moment, we assume that each node can send a message to the immediate neighbors and find the distance between itself and these neighbors. Figure below shows the initial tables for each node. The distance for any entry that is not a neighbor is marked as infinite

(unreachable).



Sharing

The whole idea of distance vector routing is the sharing of information between neighbors. The best solution for each node is to send its entire table to the neighbor and let the neighbor decide what part to use and what part to discard. However, the third column of a table (next stop) is not useful for the neighbor. When the neighbor receives a table, this column needs to be replaced with the sender's name. If any of the rows can be used, the next node is the sender of the table. A node therefore can send only the first two columns of its table to any neighbor.

- **In distance vector routing, each node shares its routing table with its immediate neighbors periodically and when there is a change.**

Updating takes three steps:

1. The receiving node needs to add the cost between itself and the sending node to each value in the second column.

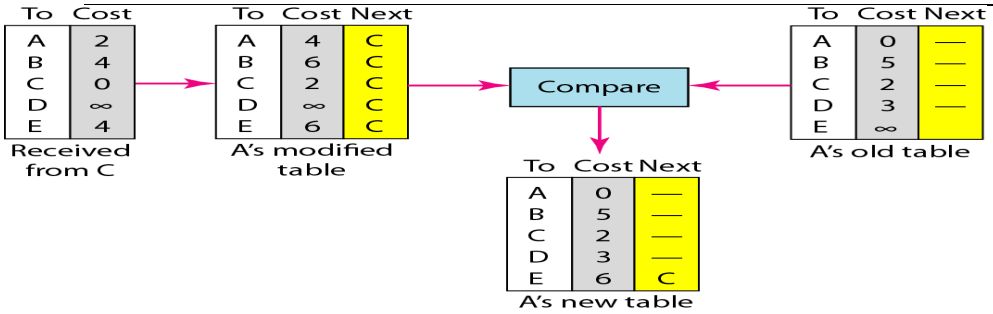
2. The receiving node needs to add the name of the sending node to each row as the third column if the receiving node uses information from any row. The sending node is the next node in the route.

3. The receiving node needs to compare each row of its old table with the corresponding row of the modified version of the received table.

a. If the next-node entry is different, the receiving node chooses the row with the smaller cost. If there is a tie, the old one is kept.

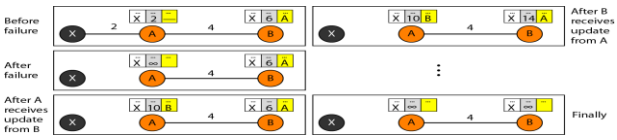
b. If the next-node entry is the same, the receiving node chooses the new row.

Updating in distance vector routing



Two-Node Loop Instability

A problem with distance vector routing is instability, which means that a network using this protocol can become unstable. To understand the problem, let us look at the scenario depicted in Figure below



At the beginning, both nodes A and B know how to reach node X. But suddenly, the link between A and X fails. Node A changes its table. IfA can send its table to B immediately, everything is fine. However, the system becomes unstable if B sends its routing table to A before receiving A's routing table. Node A receives the update and, assuming that B has found a way to reach X, immediately updates its routing table. Based on the triggered update strategy, A sends its new update to B. Now B thinks that something has been changed around A and updates its routing table. The cost of reaching X increases gradually until it reaches infinity. At this moment, both A and B know that X cannot be reached. However, during this time the system is not stable. Node A thinks that the route to X is via B; node B thinks that the route to X is via A. If A receives a packet destined for X, it goes to B and then comes back to A. Similarly, if B receives a packet destined for X, it goes to A and comes back to B. Packets bounce between A and B, creating a two-node loop problem.

RIP

The Routing Information Protocol (RIP) is an intradomain routing protocol used inside an autonomous system. It is a very simple protocol based on distance vector routing. RIP implements distance vector routing directly with some considerations:

1. In an autonomous system, we are dealing with routers and networks (links). The routers have routing tables; networks do not.

2. The destination in a routing table is a network, which means the first column defines a network address.

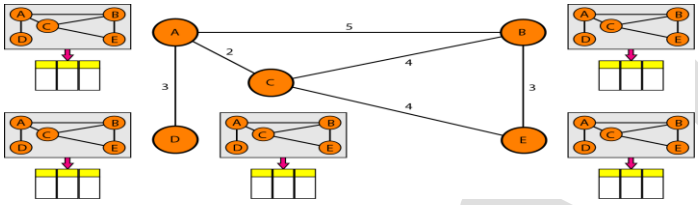
3. The metric used by RIP is very simple; the distance is defined as the number of links (networks) to reach the destination. For this reason, the metric in RIP is called a hop count.

4. Infinity is defined as 16, which means that any route in an autonomous system using RIP cannot have more than 15 hops.

5. The next-node column defines the address of the router to which the packet is to be sent to reach its destination**.**

Link State Routing

Link state routing has a different philosophy from that of distance vector routing. In link state routing, if each node in the domain has the entire topology of the domain the list of nodes and links, how they are connected including the type, cost, and condition of the links (up or down)-the node use Dijkstra's algorithm to build a routing table. Figure below shows the concept.



The figure shows a simple domain with five nodes. Each node uses the same topology to create a routing table, but the routing table for each node is unique because the calculations are based on different interpretations of the topology. The topology must be dynamic, representing the latest state of each node and each link. If there are changes in any point in the network (a link is down, for example), the topology must be updated for each node. Link state routing is based on the assumption that, although the global knowledge about the topology is not clear, each node has partial knowledge: it knows the state (type, condition, and cost) of its links. **In** other words, the whole topology can be compiled from the partial knowledge of each node.

Building Routing Tables

In link state routing, four sets of actions are required to ensure that each node has the routing table showing the least-cost node to every other node.

1. Creation of the states of the links by each node, called the link state packet (LSP).
2. Dissemination of LSPs to every other router, called flooding, in an efficient and reliable way.
3. Formation of a shortest path tree for each node.
4. Calculation of a routing table based on the shortest path tree.

Creation of Link State Packet (LSP)

A link state packet can carry a large amount of information. The node identity, the list of links, a sequence number, and age. The first two, node identity and the list of links, are needed to make the topology. The third, sequence number, facilitates flooding and distinguishes new LSPs from old ones. The fourth, age, prevents old LSPs from remaining in the domain for a long time. LSPs are generated on two occasions:

1. *When there is a change in the topology of the domain.*
2. *On a periodic basis.*

Flooding of LSPs After a node has prepared an LSP, it must be disseminated to all other nodes, not only to its neighbors. The process is called flooding and based on the following:

1. The creating node sends a copy of the LSP out of each interface.

2. A node that receives an LSP compares it with the copy it may already have. If the newly arrived LSP is older than the one it has (found by checking the sequence number), it discards the LSP. If it is newer, the node does the following:

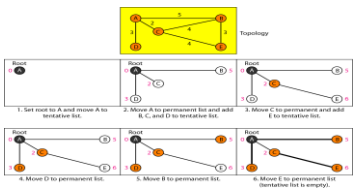
a. It discards the old LSP and keeps the new one.

b. It sends a copy of it out of each interface except the one from which the packet arrived. This guarantees that flooding stops somewhere in the domain (where a node has only one interface).

Formation of Shortest Path Tree:Dijkstra Algorithm

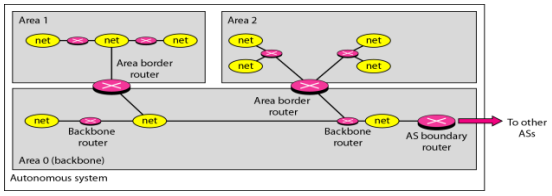
After receiving all LSPs, each node will have a copy of the whole topology. However, the topology is not sufficient to find the shortest path to every other node; a shortest path tree is needed. A tree is a graph of nodes and links; one node is called the root. All other nodes can be reached from the root through only one single route. A shortest path tree is a tree in which the path between the root and every other node is the shortest. What we need for each node is a shortest path tree with that node as the root.

The Dijkstra algorithm creates a shortest path tree from a graph. The algorithm divides the nodes into two sets: tentative and permanent. It finds the neighbors of a current node, makes them tentative, examines them, and if they pass the criteria, makes them permanent. We can informally define the algorithm by using the flowchart.



OSPF -The Open Shortest Path First

- OSPF protocol is an intradomain routing protocol based on link state routing.
- Areas- OSPF divides an autonomous system into areas. An area is a collection of networks, hosts, and routers all contained within an autonomous system.
- At the border of an area, special routers called area border routers summarize the information about the area and send it to other areas.
- Among the areas inside an autonomous system is a special area called the *backbone;* all the areas inside an autonomous system must be connected to the backbone.
- Metric- The OSPF protocol allows the administrator to assign a cost, called the metric, to each route. The metric can be based on a type of service



Types of Links In OSPF terminology, a connection is called a *link.* Four types of links have been defined: point-to-point, transient, stub, and virtual

- A point-to-point link connects two routers without any other host or router in between.
- A transient link is a network with several routers attached to it. The data can enter through any of the routers and leave through any router. All LANs and some WANs with two or more routers are of this type
- A **stub link** is a network that is connected to only one router. The data packets enter the network through this single router and leave the network through this same router. This is a special case of the transient network.
- When the link between two routers is broken, the administration may create a **virtual link** between them, using a longer path that probably goes through several routers.

Path Vector Routing

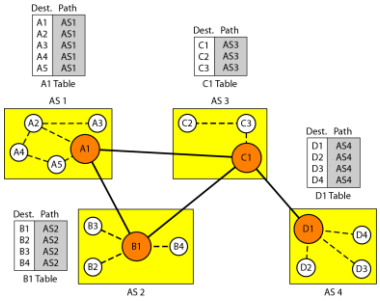
Distance vector and link state routing are not suitable for interdomain routing mostly because of scalability. Both of these routing protocols become intractable when the domain of operation becomes large.

Path vector routing proved to be useful for interdomain routing. The principle of path vector routing is similar to that of distance vector routing. In path vector routing, we assume that there is one node called speaker node

in each autonomous system that acts on behalf of the entire autonomous system. The speaker node in an AS creates a routing table and advertises it to speaker nodes in the neighboring ASs. The idea is the same as for distance vector routing except that only speaker nodes in each AS can communicate with each other. A speaker node advertises the path, not the metric of the nodes, in its autonomous system or other autonomous systems.

Initialization

At the beginning, each speaker node can know only the reachability of nodes inside its autonomous system. Figure below shows the initial tables for each speaker node in a system made of four ASs.



Sharing Just as in distance vector routing, in path vector routing, a speaker in an autonomous system shares its table with immediate neighbors. In Figure above, node Al shares its table with nodes Bl and Cl. Node Cl shares its table with nodes Dl, Bl, andAl. Node Bl shares its table with ClandAl. Node Dl shares its table with Cl.

Updating When a speaker node receives a two-column table from a neighbor, it updates its own table by adding the nodes that are not in its routing table and adding its own autonomous system and the autonomous system that sent the table. After a while each speaker has a table and knows how to reach each node in other ASs. Figure below shows the tables for each speaker node after the system is stabilized.

According to the figure, if router Al receives a packet for nodes A3, it knows that the path is in ASI (the packet is at home); but if it receives a packet for Dl, it knows that the packet should go from ASl, to AS2, and then to AS3. The routing table shows the path completely. On the other hand, if node Dl in AS4 receives a packet for node A2, it knows it should go through AS4, AS3, and AS 1.

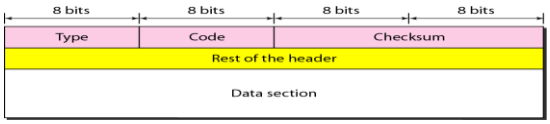
- **Loop prevention**. The instability of distance vector routing and the creation of loops can be avoided in path vector routing. When a router receives a message, it checks to see if its autonomous system is in the path list to the destination. If it is, looping is involved and the message is ignored.

- **Policy routing.** Policy routing can be easily implemented through path vector routing. When a router receives a message, it can check the path. If one of the autonomous systems listed in the path is against its policy, it 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.

ICMP

The IP protocol has no error-reporting or error-correcting mechanism. The IP protocol also lacks a mechanism for host and management queries. The Internet Control Message Protocol (ICMP) has been designed to compensate for the above two deficiencies. It is a companion to the IP protocol.

General format of ICMP messages



ICMP always reports error messages to the original source.

Error-reporting messages

Important points about ICMP error messages:

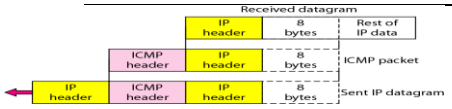
❑No ICMP error message will be generated in response to a datagram carrying an ICMP error message.

❑No ICMP error message will be generated for a fragmented datagram that is not the first fragment.

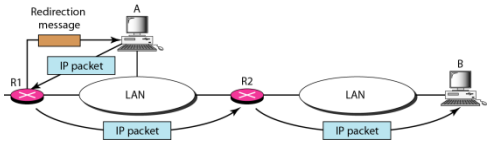
❑No ICMP error message will be generated for a datagram having a multicast address.

❑No ICMP error message will be generated for a datagram having a special address such as 127.0.0.0 or 0.0.0.0.

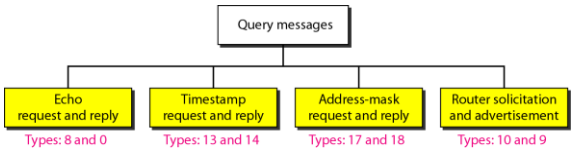
Contents of data field for the error messages



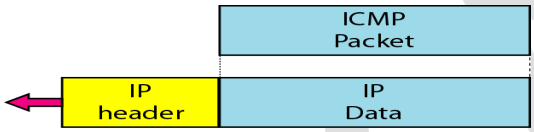
Redirection concept



Query messages

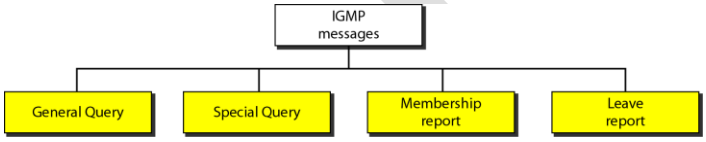


Encapsulation of ICMP query messages



IGMP

The IP protocol can be involved in two types of communication: unicasting and multicasting. The Internet Group Management Protocol (IGMP) is one of the necessary, but not sufficient, protocols that is involved in multicasting. IGMP is a companion to the IP protocol.



IGMP operation

In IGMP, a membership report is sent twice, one after the other.

The general query message does not define a particular group.

POSSIBLE QUESTIONS

PART-A [20*1=20 Marks]

ONLINE EXAMINATION

PART-B [5*2=10 Marks]

1. What is CSMA?
2. What is I-persistent method?
3. What is the difference between a direct and an indirect delivery?
4. What are the two sub layers in data link layer?
5. Define repeater.

PART-C [5*6=30 Marks]

1.What is CSMA? Discuss about it in detail.

2.Write a note on i) Fast Ethernet ii) Switched Ethernet

3.Write about the connecting LANS in detail.

4.Write note on distance vector routing.

5.Discuss in detail about IPv4 protocol.

6.Describe the techniques used for forwarding in detail. Write about the forwarding process with example.

7.Explain in detail about IPV6.

8.Explain about the connecting devices.

Karpagam Academy of Higher Education
Department of CS, CA & IT
Class: II BSC CT Batch:2017
Subject: COMPUTER NETWORKS
SubCode: 17CTU303
UNIT IV

S.NO	QUESTION	OPTION A	OPTION B	OPTION C	OPTION D	ANSWER
1	CSMA/CD stands for _____	Carrier Sense Multiple Access/Collision Detect	Carrier Sense Mono Access/Collision Detect	Control State Multiple Access/Collision Detect	Carrier Sense Multiple Access/Control Data	Carrier Sense Multiple Access/Collision Detect
2	_____ is the protocol for carrier transmission access in Ethernet networks	CSMA/CD	TCP	IP	FTP	CSMA/CD
3	Internet at the network layer is a_____network.	packet-switched	LAN	connection	connetionless	packet-switched
4	Internet has chosen the datagram approach to_____in network layer	routers	packets	switching	protocol	protocol
5	Internet is made of so many_____networks.	homogenous	hetrogeneous	MAN	multipoint	hetrogeneous
6	Communication at network layer in the internet is_____.	connectionless	point-to-point	connection oriented	packet-switched	connectionless
7	What is the abbrevation for IPV4_____.	Inter Protocol Versus 4	Inter Position Version 4	Internet protocol version 4	Internet Position Versus 4	Internet protocol version 4
8	IPV4 provides the term 'best-effort' means that_____.	no error control	error control	error detection	datagram	no error control
9	Packets in the IPV4 layer are called_____.	frames	datagroup	switching	datagrams	datagrams
10	A datagram is a variable length packet consisting of_____parts.	one	six	two	three	two
11	The total length field defines the total length of the datagram including_____.	footer	header	flags	frames	header
12	Abbravation for MTU_____.	Minimum Transfer Unit	Maximum Transfer Unit	Maximum Travel Unit	Minimum Travel Unit	Maximum Transfer Unit
13	_____in the IPV4 packet covers only header,not the data.	Check subtract	Check sum	options	Check product	Check sum

14	Options can be used for network testings and_____.	checking	packets	types	debugging	debugging
15	_____can only used as the last option.	end-of-option	first-of-option	options	no options	end-of-option
16	Record route can list up to_____router address.	fifteen	sixty	nine	ten	nine
17	_____route has less rigid.	loose source	strict source	no route	record	loose source
18	_____is expressed in millisecond,from midnight.	time stand	time stamp	time shot	all the above	time stamp
19	IPv4 also known as_____.	IPNg	IPNG	ipNG	Ipng	Ipng
20	The adoption of IPv6 has been_____.	fast	slow	neuter	quick	slow
21	An IPv6 address is_____bits long.	128	126	125	127	128
22	IPv6 has_____options to allow for additional functionalities.	old	first	new	last	new
23	A_____ is basically a multiport repeater	hub	Repeater	gateway	router	hub
24	Base header with_____fields.	eight	ten	five	none of these	eight
25	The 4bit field defines the_____number of the IP.	versus	header	.footer	version	version
26	A repeater operates at the _____ layer	physical	datalink	application	transport	physical
27	Source and destination of the packet are located on the same physical network called_____.	Indirect delivery	Inward delivery	Direct delivery	Outward delivery	Direct delivery
28	One technique to reduce the content of a routing table is_____.	before-hop	next-hop	first hop	last hop	next-hop
29	The Routing table holds only the address of the next hop_____.	next hop	route method	network method	host method	route method
30	A second technique to reduce the routing table_____.	next hop	default	forward	network specific	network specific
31	All hosts connected to the same network as one single entity_____.	route	next-hop	host specific	d.network specific	host specific
32	In classless addressing,atleast_____columns in a routing table.	5	6	3	4	4
33	In an address aggregation,the network for each organization is_____.	independent	dependent	department	none of these	independent
34	The routing table can be either_____.	static	static and dynamic	static or dynamic	all the above	static or dynamic
35	A static routing table can be used in a_____internet.	big	small	multi	LAN	small

36	Dynamic routing protocols such as_____.	RIP	OSPF	BGP	all the above	all the above
37	A bridge operates at _____layer	data link	physical	application	network	data link
38	_____ is network diagnostic and error reporting protocol	ICMP	FTP	UDP	HTTP	ICMP
39	_____is a device like a switch that routes data packets based on their IP addresses.	router	hub	repeater	bridge	router
40	Routing inside an autonomous system____	Intra	Inter	Inside	all the above	Inside
41	Abbrevation for BGP_____.	Border Gateway Process	Bit Gateway Process	Border Gateway Protocol	Byte Gateway Protocol	Border Gateway Protocol
42	A node sends its routing table,at every_____in a periodic update.	33s	30s	31s	35s	30s
43	_____algorithm creates a shortest path tree from a graph.	data	dakstra	define	dijkstra	dijkstra
44	An area is a collection of_____.	networks	hosts	route	all the above	all the above
45	_____link is a network and is connected to only one router.	stub	point-to-point	transient	none of these	stub
46	Multicasting of the relationship is_____.	one-to-one	many-to-one	one-to-many	many-to-many	one-to-many
47	_____layer is responsible for process-to-process delivery.	transport	physical	application	network	transport
48	Internet has decided to use universal port numbers for severs called_____.	well-unknown port	well-known port	well-known protocol	well-unknown process	well-known port
49	IANA has divided the port numbers into_____ranges.	six	four	five	three	three
50	_____a connection,is first established between the sender and receiver.	connection-oriented	connectionless	token	dialog	connection-oriented
51	UDP is called_____.	connection-oriented	check point	token	connetionless	connetionless
52	UDP length = IP length - _____.	IP length	IP breadth	IP header's length	IP header's breadth	IP header's length
53	UDP is a suitable transport protocol for_____.	unicasting	multicasting	nocasting	none of these	multicasting
54	TCP groups a number of bytes together into a packet called_____.	segment	encapsulation	datagram	data binding	segment
55	The acknowledgement number is _____.	natural	whole	integers	cumulative	cumulative

56	_____ flag is used to terminate the connection.	TER	FIN	URG	PSH	FIN
57	_____ protocol is used to remote procedure call.	DNS	PRC	RPC	RPCC	RPC
58	An ACK segment,if carrying _____data consumes no sequence number.	no	2	3	5	no
59	_____, as the name suggests, is a passage to connect two networks together that may work upon different networking models.	gateway	router	repeater	hub	gateway
60	In _____ routing, the routing table need to recompute the route continuously	static	dynamic	state	none of these	dynamic

UNIT V
SYLLABUS

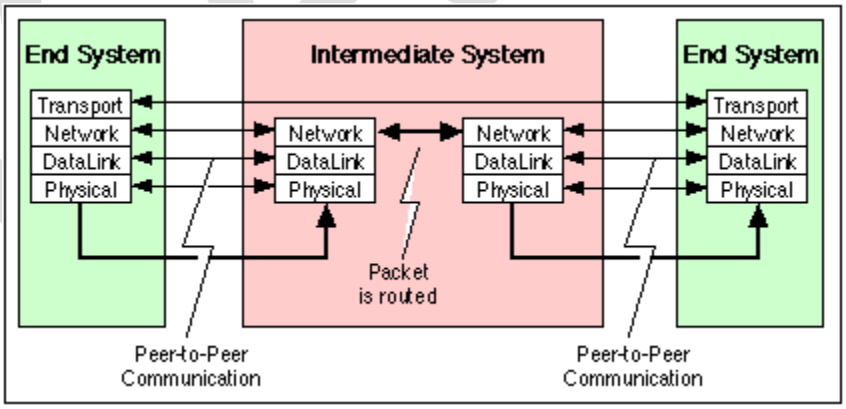
Transport Layer Functions and Protocols: Transport services- error and flow control, Connection establishment and release- three way handshake; **Overview of Application layer protocol**: Overview of DNS protocol; overview of WWW &HTTP protocol.

1). Transport layer functions and protocol

Transport Layer Protocol:

The transport layer is the fourth layer of the OSI reference model. It provides transparent transfer of data between end systems using the services of the network layer (e.g. IP) below to move PDUs of data between the two communicating systems.

The transport service is said to perform "peer to peer" communication, with the remote (peer) transport entity. The data communicated by the transport layer is encapsulated in a transport layer PDU and sent in a network layer SDU. The network layer nodes (i.e. Intermediate Systems (IS)) transfer the transport PDU intact, without decoding or modifying the content of the PDU. In this way, only the peer transport entities actually communicate using the PDUs of the transport protocol.



Two End Systems connected by an Intermediate System (in this case a router) The figure shows the various protocol layers drawn with reference to the OSI reference model

The transport layer relieves the upper layers from any concern with providing reliable and cost effective data transfer. It provides end-to-end control and information transfer with the quality of service needed by the application program. It is the first true end-to-end layer, implemented in all End Systems (ES).

The Internet Protocol (IP) Stack provides a set of transport layer protocols:

Functions of Transport Layer:

The transport layer protocols are primarily responsible for

- **End-to-End application data delivery** between the source and destination computers using the underlying unreliable best-effort IP based networks. It provides either a byte stream or message based service to the application layer protocols. On the sending side, application data is split into a byte stream or into a series of message blocks, a transport layer header added and then transport layer segments are sent to the underlying IP layer in the sending node, to be delivered to the network. Once the IP network delivers the transport layer segments to the receiving machine, the transport layer process at the receiving machine processes the transport headers for reliability, flow and error controls and then hands over the application data to the appropriate application process.

- **Application layer protocol Multiplexing/ Demultiplexing** for multiple applications communicating between end nodes. Multiplexing/ Demultiplexing is provided using transport layer port numbers for providing multiple services like Email, Web browsing, file transfer over the same IP stack implementation on end nodes. For example, HTTP uses the reserved TCP port number 80, SMTP uses the reserved TCP port number 25, FTP control connection uses the reserved port number 21 etc. Similarly, DNS uses the reserved UDP port number 53, SNMP uses the reserved UDP port numbers 161 and 162. Normally, the transport layer header contains fields named as source port number and destination port number to uniquely identify the sending and the receiving processes respectively.

- **End-End Reliability** for making sure that every byte of sender's application data reaches the receiver's application, in order, in spite of travelling over a wide variety of unreliable telecommunication links. Reliability is taken care by

using mechanisms like checksums, sequence numbers, acknowledgement numbers, timeouts and retransmissions.

- **End-End Flow control** for making sure that the sender sends data at a rate that the receiver can process and store**.** This is usually achieved by the receiver advertising its current receiver buffer size continuously to the sender.

- **End-End Congestion control** for making sure that the sender does not introduce congestion in the intermediate network links and router buffers. Mechanisms like feedbacks from intermediate routers/receiver and monitoring receiver packet loss are used for controlling the sender rate so as not to congest the network links and router buffers.

- **Provides unique communication end points in the form of Sockets** for applications to use the Networking stack of the machine to communicate externally

- TCP, UDP are the most popular transport layer protocols

Note: *Reliability, Flow control and congestion control are supported only in TCP and not in UDP.*

Services of transport layer

As layer four of the OSI model, the transport layer is responsible for providing communication services between computers on a network For eg: as the data packets transit between the originating or sending computer and the destination or receiving computer, the transport layer performs error checking and data packet routing services. Additionally, while working with the 3 lower and 3 upper layers, the transport layer continues to provide services, even though different application software processes are running simultaneously on multiple computers.

Services:

- **Connection setup and multiplexing** The sender must contact the receiver before its starts sending data packets. They engage in a three-way handshake operation to establish the connection, then start transmitting data. A single computer can establish multiple connections with multiple computers at the same time, a feature called multiplexing (since the packets for these different connections are transmitted over the same network connection).

- **Flow control mechanisms** While slow start and congestion control are used to avoid network congestion, flow controls help prevent the sender from overflowing the receiver with too much data. These controls are essential because the receiver drops packets when it is overloaded and those packets must be retransmitted, potentially increasing network congestion and reducing system performance."
- **Slow start and congestion control** Once a connection has been made, the sender starts sending packets, slowly at first so it does not overwhelm the network. If congestion is not bad, it picks up the pace. This is called "slow start." Later, congestion controls help the sender scale back if the network gets busy.
- **Reliability services** These services are used to retransmit corrupt, lost, and dropped packets. *Positive acknowledgements* confirm to the sender that the recipient actually received a packet (failure to transmit this acknowledgement means "resend the packet"). Sequencing is used to number packets so that packets can be put back in order and lost packets can be detected. Error checking detects corrupted packets.

listen	Wait till a process wants a connection
connect	Try to setup a connection
send	Send data packet
receive	Wait for arrival of data packet
disconnect	Calling side breaks up the connection

2). Error and Flow control:

Flow Control:

- Flow control coordinates the amount of data that can be sent before receiving acknowledgement
- It is one of the most important functions of data link layer.
- Flow control is a set of procedures that tells the sender how much data it can transmit before it must wait for an acknowledgement from the receiver.

- Receiver has a limited speed at which it can process incoming data and a limited amount of memory in which to store incoming data.
- Receiver must inform the sender before the limits are reached and request that the transmitter to send fewer frames or stop temporarily.
- Since the rate of processing is often slower than the rate of transmission, receiver has a block of memory (buffer) for storing incoming data until they are processed.

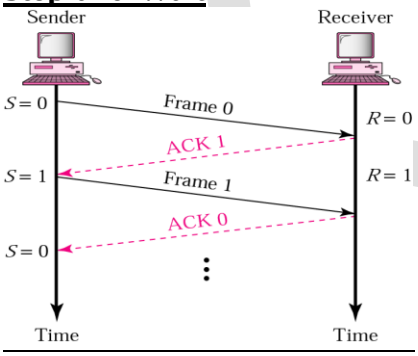
Error Control:

- Error control includes both error detection and error correction.
- 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.

Error and Flow Control Mechanisms:

- Stop-and-Wait
- Go-Back-N ARQ
- Selective-Repeat ARQ

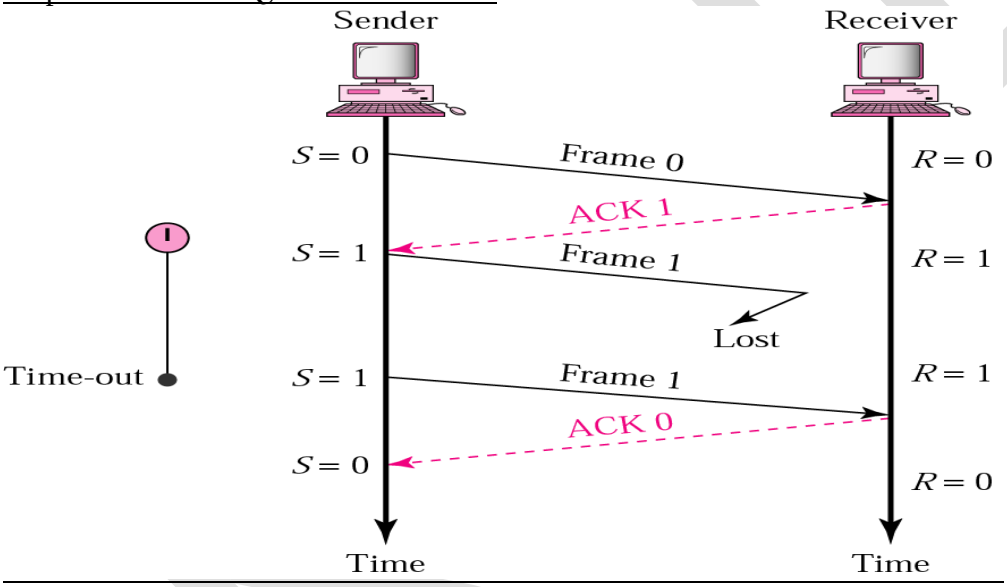
Stop-and-Wait



- Sender keeps a copy of the last frame until it receives an acknowledgement.
- For identification, both data frames and acknowledgements (ACK) frames are numbered alternatively 0 and 1.

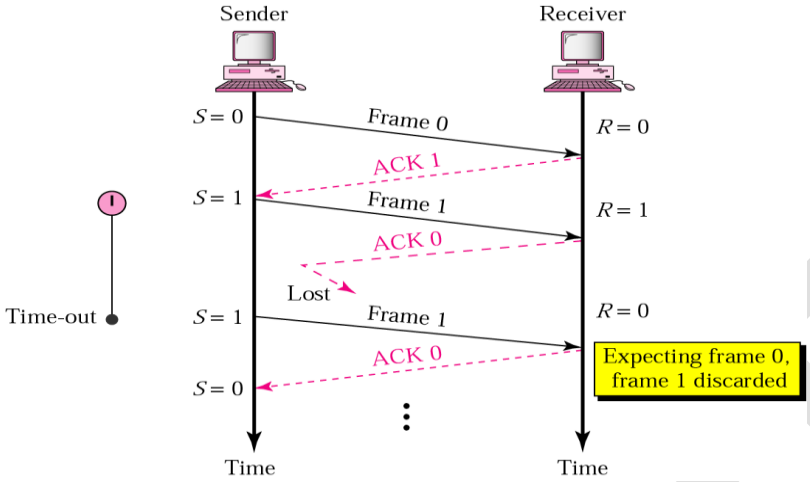
- Sender has a control variable (S) that holds the number of the recently sent frame. (0 or 1)
- Receiver has a control variable ® that holds the number of the next frame expected (0 or 1).
- Sender starts a timer when it sends a frame. If an ACK is not received within a allocated time period, the sender assumes that the frame was lost or damaged and resends it
- Receiver send only positive ACK if the frame is intact.
- ACK number always defines the number of the next expected frame

Stop-and-Wait ARQ, lost ACK frame:



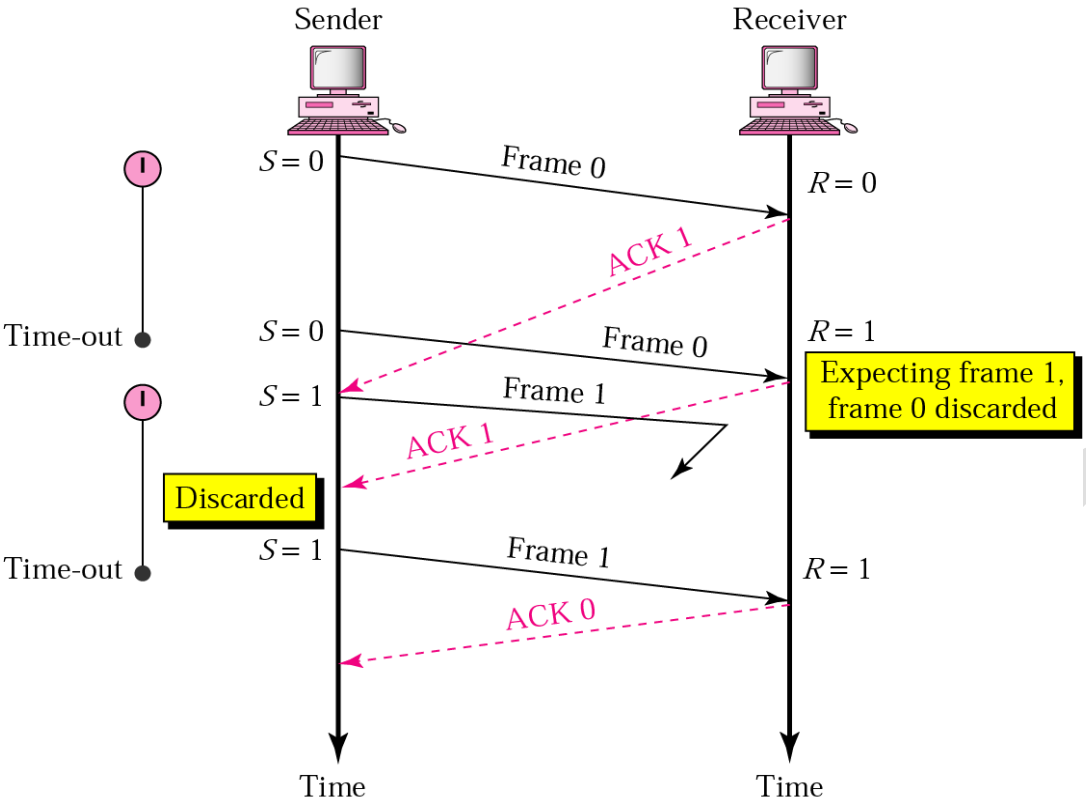
- When a receiver receives a damaged frame, it discards it and keeps its value of R.
- After the timer at the sender expires, another copy of frame 1 is sent.

Stop-and-Wait, lost ACK frame:-



- If the sender receives a damaged ACK, it discards it.
- When the timer of the sender expires, the sender retransmits frame 1.
- Receiver has already received frame 1 and expecting to receive frame 0 (R=0). Therefore it discards the second copy of frame 1.

Stop-and-Wait, delayed ACK frame:



- The ACK can be delayed at the receiver or due to some problem
- It is received after the timer for frame 0 has expired.
- Sender retransmitted a copy of frame 0. However, R =1 means receiver expects to see frame 1. Receiver discards the duplicate frame 0.
- Sender receives 2 ACKs, it discards the second ACK.

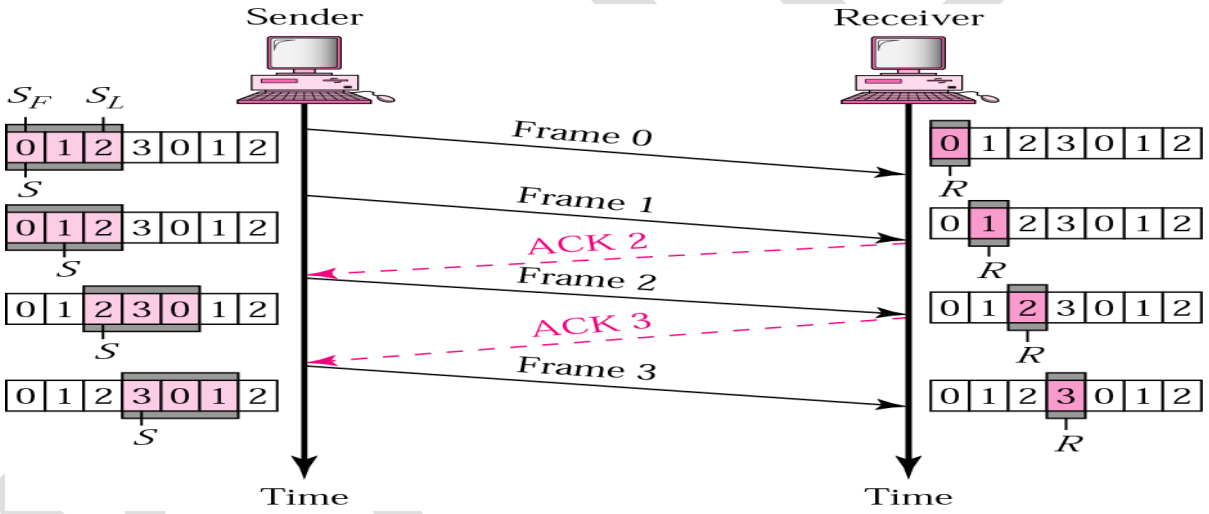
Disadvantage of Stop-and-Wait:

- In stop-and-wait, at any point in time, there is only one frame that is sent and waiting to be acknowledged.
- This is not a good use of transmission medium.
- To improve efficiency, multiple frames should be in transition while waiting for ACK.
- Two protocol use the above concept,

- **Go-Back-N ARQ**
- **Selective Repeat ARQ**

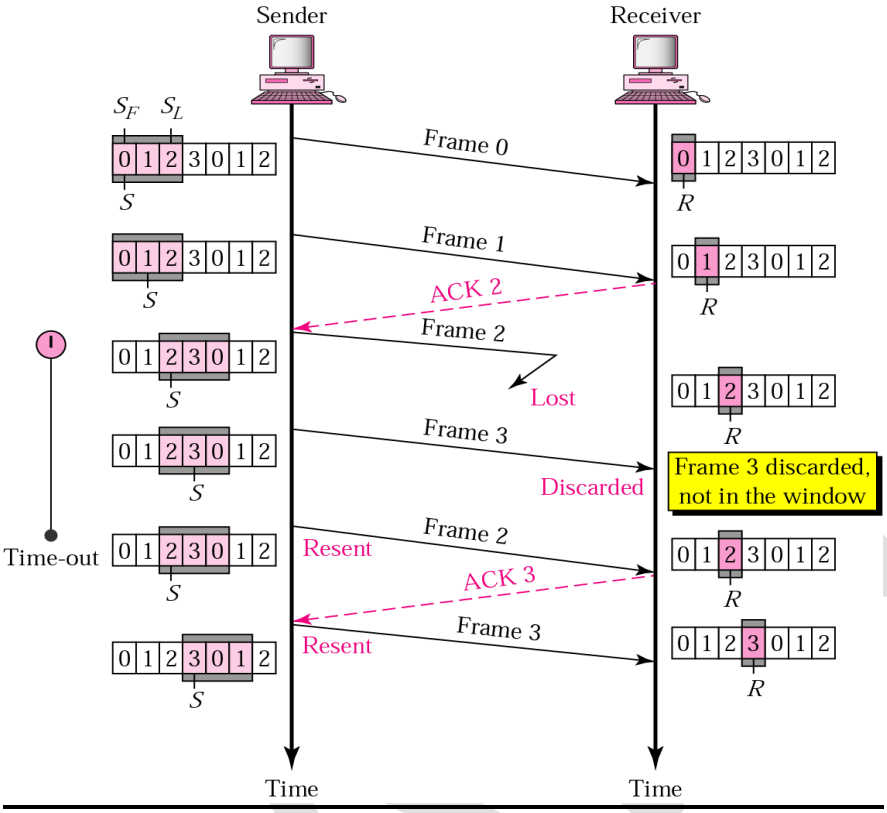
Go-Back-N ARQ:

- We can send up to W frames before worrying about ACKs.
- We keep a copy of these frames until the ACKs arrive.
- This procedure requires additional features to be added to Stop-and-Wait ARQ.
- The sender keeps track of the outstanding frames and updates the variables and windows as the ACKs arrive.



Go-Back-N ARQ, lost frame:

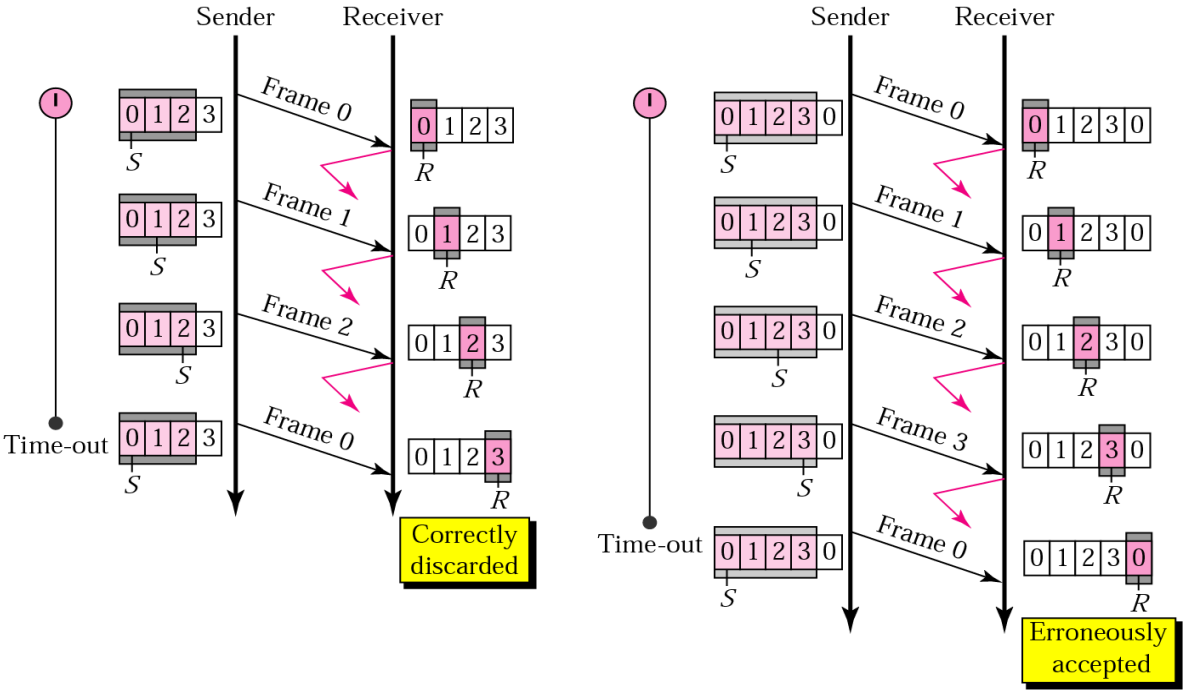
- Frame 2 is lost
- When the receiver receives frame 3, it discards frame 3 as it is expecting frame 2 (according to window).
- After the timer for frame 2 expires at the sender site, the sender sends frame 2 and 3. (go back to 2)



Go-Back-N ARQ, damaged/lost/delayed ACK:

- If an ACK is damaged/lost, we can have two situations:
- If the next ACK arrives before the expiration of any timer, there is no need for retransmission of frames because ACKs are cumulative in this protocol.
- If ACK1, ACK2, and ACk3 are lost, ACK4 covers them if it arrives before the timer expires.
- If ACK4 arrives after time-out, the last frame and all the frames after that are resent.
- Receiver never resends an ACK.
- A delayed ACK also triggers the resending of frames

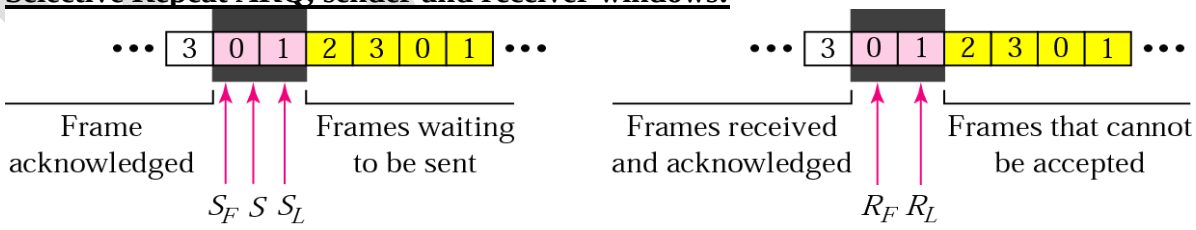
Go-Back-N ARQ, sender window size:



a. Window size < 2^m b. Window size = 2^m

- Size of the sender window must be less than 2^m. Size of the receiver is always 1. If m = 2, window size = $2^m - 1 = 3$.
- Fig compares a window size of 3 and 4.

Selective Repeat ARQ, sender and receiver windows:

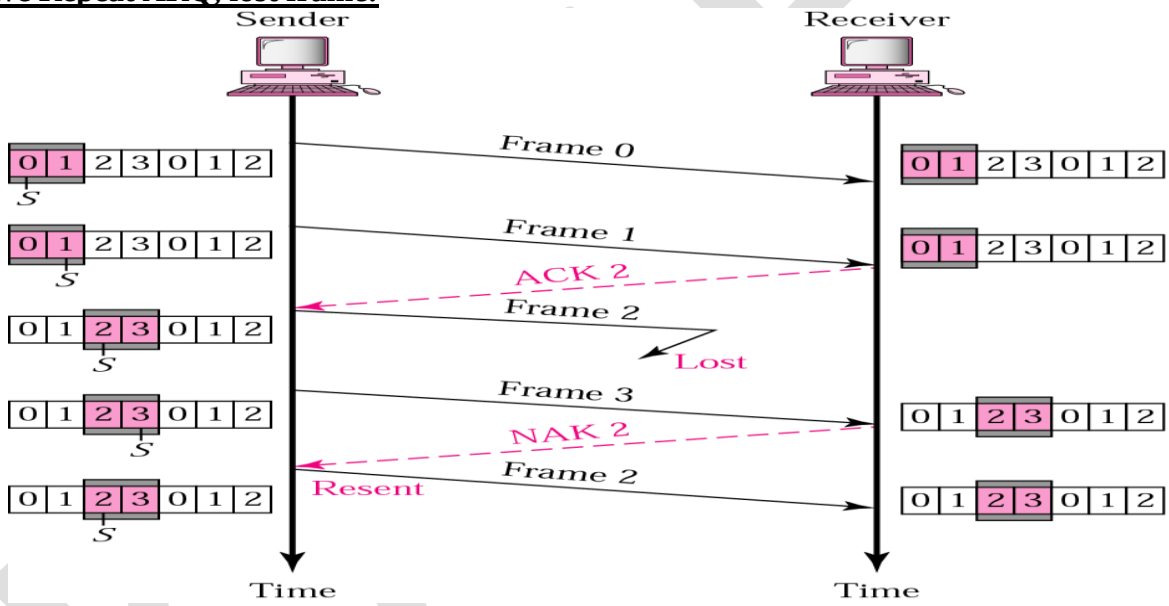


a. Sender window b. Receiver window

- Go-Back-N ARQ simplifies the process at the receiver site. Receiver only keeps track of only one variable, and there is no need to buffer out-of-order frames, they are simply discarded.

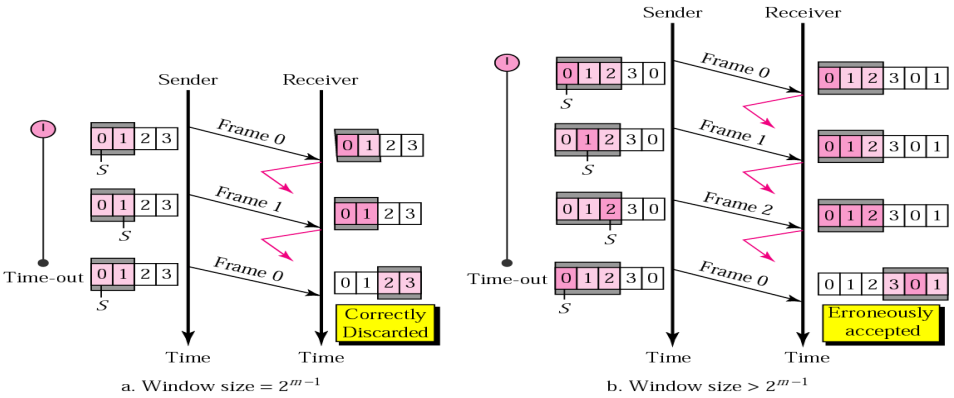
- However, Go-Back-N ARQ protocol is inefficient for noisy link. It bandwidth inefficient and slows down the transmission.
- In Selective Repeat ARQ, only the damaged frame is resent. More bandwidth efficient but more complex processing at receiver.
- It defines a negative ACK (NAK) to report the sequence number of a damaged frame before the timer expires.

Selective Repeat ARQ, lost frame:



- Frames 0 and 1 are accepted when received because they are in the range specified by the receiver window. Same for frame 3.
- Receiver sends a NAK2 to show that frame 2 has not been received and then sender resends only frame 2 and it is accepted as it is in the range of the window.

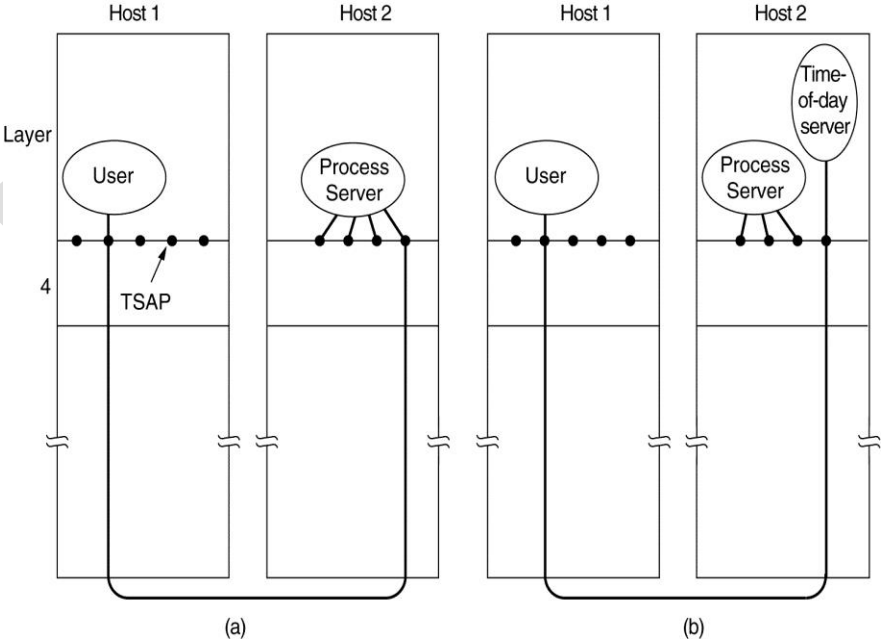
- **Selective Repeat ARQ, sender window size:**

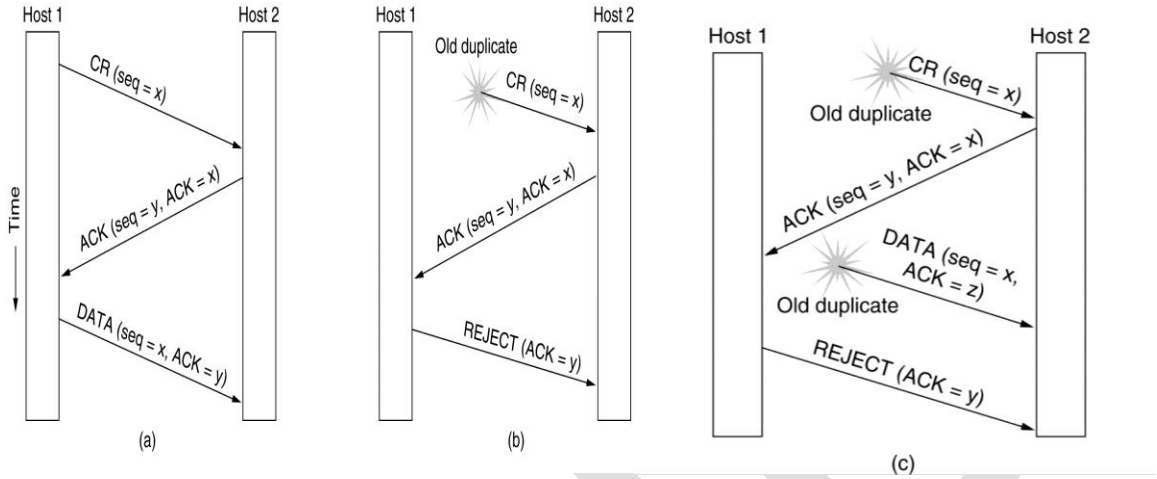


- Size of the sender and receiver windows must be at most one-half of 2^m. If m = 2, window size should be $2^m/2 = 2$. Fig compares a window size of 2 with a window size of 3. Window size is 3 and all ACKs are lost, sender sends duplicate of frame 0, window of the receiver expect to receive frame 0 (part of the window), so accepts frame 0, as the 1st frame of the next cycle – an **error**.

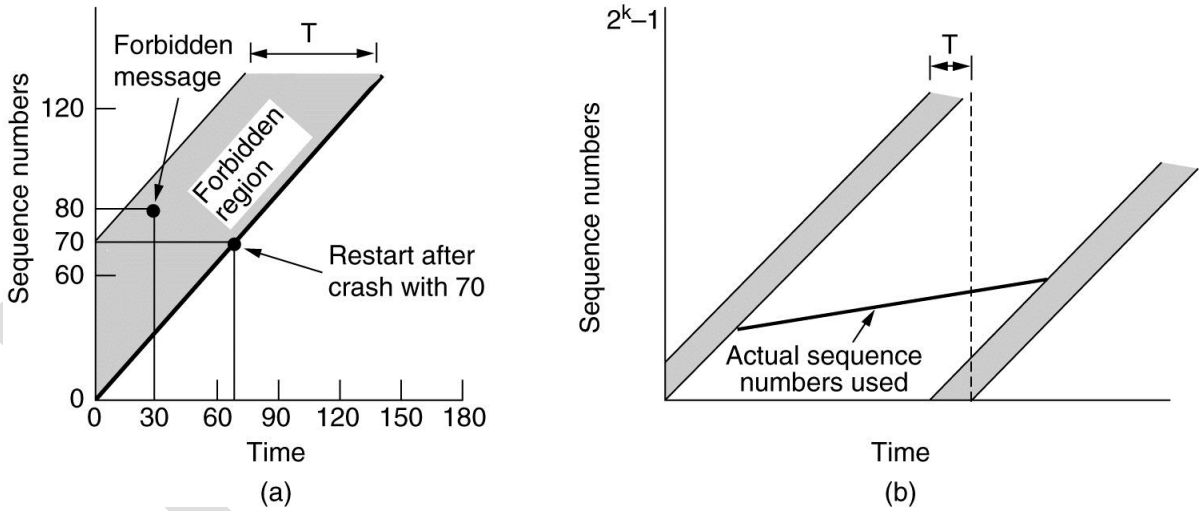
3). Connection Establishment and Release:

Connection Establishment:

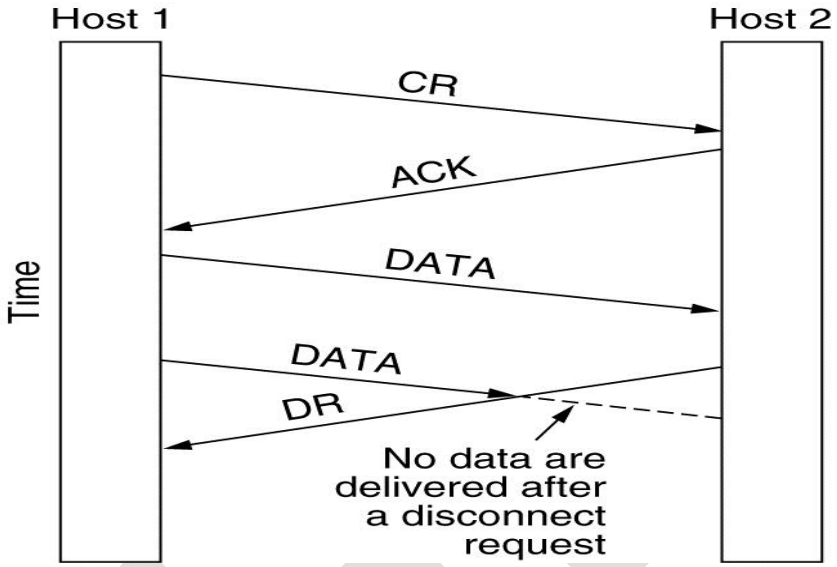




Three protocol scenarios for establishing a connection using a three-way handshake. CR denotes CONNECTION REQUEST.
(a) Normal operation,
(b) Old CONNECTION REQUEST appearing out of nowhere.
(c) Duplicate CONNECTION REQUEST and duplicate ACK

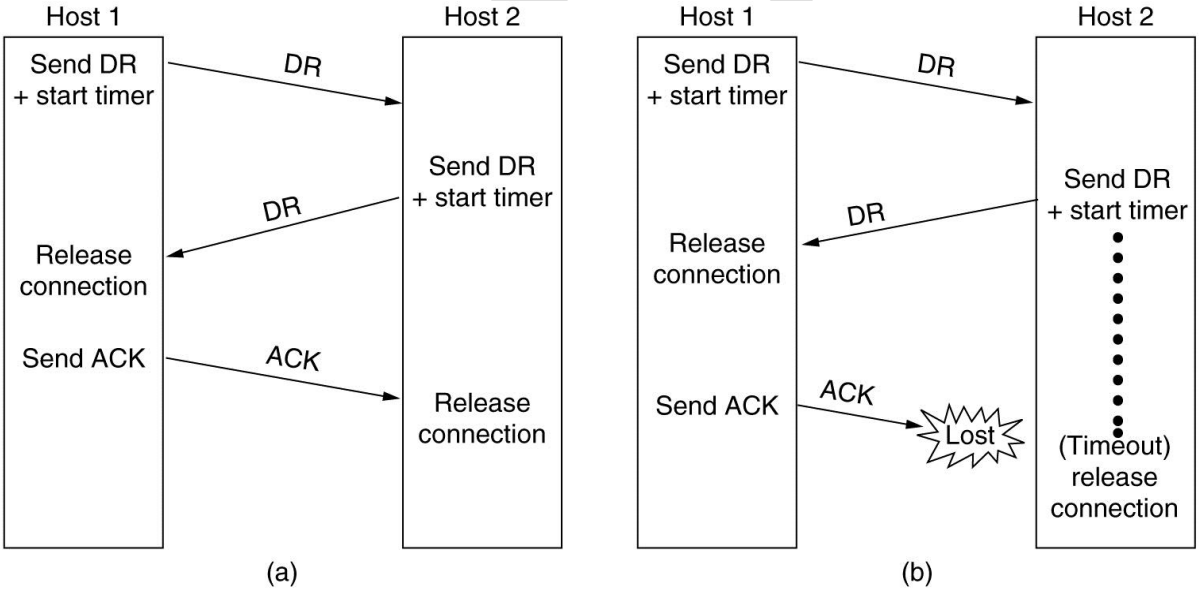


a) TPDUs may not enter the forbidden region.
(b) The resynchronization problem.



Connection Release:

Abrupt disconnection with loss of data.



Four protocol scenarios for releasing a connection. (a) Normal case of a three-way handshake.
(b) final ACK lost.

4). **Three way handshake:**

If a source host wishes to use an IP application such as active FTP for instance, it selects a port number which is greater than 1023 and connects to the destination station on port 21. The TCP connection is set up via three-way handshaking:

- This begins with a **SYN** (Synchronise) segment (as indicated by the code bit) containing a 32-bit **Sequence** number **A** called the **Initial Send Sequence (ISS)**being chosen by, and sent from, host 1. This 32-bit sequence number **A** is the starting sequence number of the data in that packet and increments by **1** for every byte of data sent within the segment, i.e. there is a sequence number for each octet sent. The SYN segment also puts the value **A+1** in the first octet of the data.
- Host 2 receives the **SYN** with the Sequence number **A** and sends a **SYN** segment with its own totally independent ISS number **B** in the Sequence number field. In addition, it sends an increment on the Sequence number of the last received segment (i.e. **A+x** where **x** is the number of octets that make up the data in this segment) in its Acknowledgment field. This **Acknowledgment** number informs the recipient that its data was received at the other end and it expects the next segment of data bytes to be sent, to start at sequence number **A+x**. This stage is aften called the **SYN-ACK**. It is here that the **MSS** is agreed.
- Host 1 receives this **SYN-ACK** segment and sends an **ACK** segment containing the next sequence number (**B+y** where **y** is the number of octets in this particular segment), this is called **Forward Acknowledgement** and is received by Host 2. The **ACK** segment is identified by the fact that the **ACK** field is set. Segments that are not acknowledged within a certain time span, are retransmitted.

TCP peers must not only keep track of their own initiated Sequence numbers but also those Acknowledgment numbers of their peers.
Closing a TCP connection is achieved by the initiator sending a **FIN** packet. The connection only closes when an **ACK** has been sent by the other end and received by the initiator.Maintaining a TCP connection requires the stations to remember a number of different parameters such as port numbers and sequence numbers. Each connection has this set of variables located in

a **Transmission Control Block (TCB)**.

Transmission Timeout

Because every TCP network has its own characteristics, the delay between sending a segment and receiving an acknowledgement varies. Different methods are available for calculating this Transmission Timeout and will depend on the stack. TCP maintains a retransmission timer for each connection. This retransmission timer is used when TCP expects to receive an acknowledgment from the other end. Once data is sent, TCP monitors this **Retransmission Time-Out (RTO)** and also a**Round Trip Time (RTT)**. If an ACK is not received by the time the RTO expires, TCP retransmits the data using an exponentially increasing value for the RTO. This doubling is called an **Exponential Back-Off** The RTO is calculated as a linear function of the RTT and its value changes over time with changes in routing and traffic load.
Typically **RTT+4*mean deviation**.

5). **Overview of application layer protocol:**

An application layer protocol defines how application processes (clients and servers), running on different end systems, pass messages to each other. In particular, an application layer protocol defines:

- The types of messages, e.g., request messages and response messages.
- The syntax of the various message types, i.e., the fields in the message and how the fields are delineated.
- The semantics of the fields, i.e., the meaning of the information that the field is supposed to contain;

  Rules for determining when and how a process sends messages and responds to messages.

Application Type	Application-layer protocol	Transport Protocol
Electronic mail	Send: Simple Mail Transfer Protocol SMTP [RFC 821]	TCP 25
	Receive: Post Office Protocol v3 POP3 [RCF 1939]	TCP 110
Remote terminal access	Telnet [RFC 854]	TCP 23
World Wide Web (WWW)	HyperText Transfer Protocol 1.1 HTTP 1.1 [RFC 2068]	TCP 80
File Transfer	File Transfer Protocol FTP [RFC 959]	TCP 21
	Trivial File Transfer Protocol TFTP [RFC 1350]	UDP 69
Remote file server	NFS [McKusik 1996]	UDP or TCP
Streaming multimedia	Proprietary (e.g., Real Networks)	UDP or TCP
Internet telephony	Proprietary (e.g., Vocaltec)	Usually UDP

SMTP (Simple Mail Transfer Protocol):

- One of the most popular network service is electronic mail (e-mail).
- The TCP/IP protocol that supports electronic mail on the Internet is called Simple Mail Transfer Protocol (SMTP).
- SMTP transfers messages from senders' mail servers to the recipients' mail servers using TCP connections.
- Users based on e-mail addresses.
- SMTP provides services for mail exchange between users on the same or different computers.
- Following the client/server model:
    - SMTP has two sides: a client side which executes on a sender's mail server, and server side which executes on recipient's mail server.
    - Both the client and server sides of SMTP run on every mail server.

- When a mail server sends mail (to other mail servers), it acts as an SMTP client.
- When a mail server receives mail (from other mail servers) it acts as an SMTP server.

TELNET (Terminal Network):

- TELNET is client-server application that allows a user to log onto remote machine and lets the user to access any application program on a remote computer.
- TELNET uses the NVT (Network Virtual Terminal) system to encode characters on the local system.
- On the server (remote) machine, NVT decodes the characters to a form acceptable to the remote machine.
- TELNET is a protocol that provides a general, bi-directional, eight-bit byte oriented communications facility.
- Many application protocols are built upon the TELNET protocol

FTP (File Transfer Protocol):

- FTP is the standard mechanism provided by TCP/IP for copying a file from one host to another.
- FTP differs form other client-server applications because it establishes 2 connections between hosts.
- FTP is built on a client-server architecture and uses separate control and data connections between the client and the server.
- One connection is used for data transfer, the other for control information (commands and responses).
- It transfer data reliably and efficiently.

Multipurpose Internet Mail Extensions (MIME):

- It is an extension of SMTP that allows the transfer of multimedia messages.
- If binary data is included in a message MIME headers are used to inform the receiving mail agent:
  - Content-Transfer-Encoding: Header alerts the receiving user agent that the message body has been ASCII encoded and the type of encoding used.
  - Content-Type: Header informs the receiving mail agent about the type of data included in the message.

POP (Post Office Protocol):

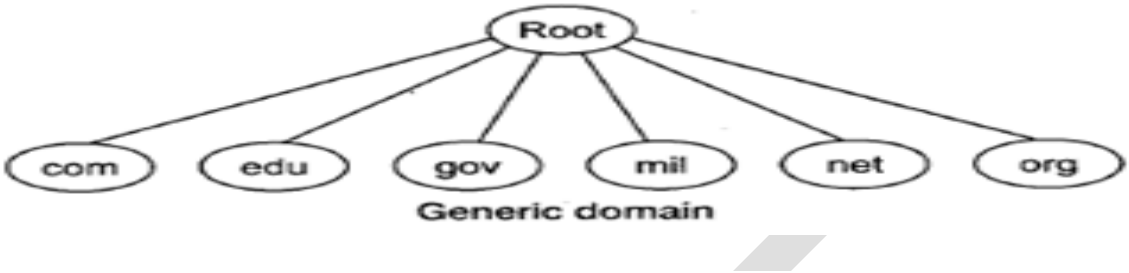
- POP is also called as POP3 protocol.
- This is a protocol used by a mail server in conjunction with SMTP to receive and holds mail for hosts.
- POP3 mail server receives e-mails and filters them into the appropriate user folders. When a user connects to the mail server to retrieve his mail, the messages are downloaded from mail server to the user's hard disk.

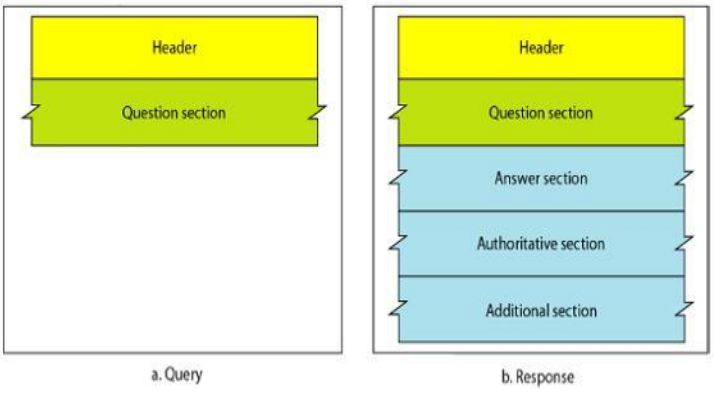
HTTP (Hypertext Transfer Protocol):

- This is a protocol used mainly to access data on the World Wide Web (www).
- The Hypertext Transfer Protocol (HTTP) the Web's main application-layer protocol although current browsers can access other types of servers
- A respository of information spread all over the world and linked together.
- The HTIP protocol transfer data in the form of plain text, hyper text, audio, video and so on.
- HTTP utilizes TCP connections to send client requests and server replies.

Overview of Domain Name System (DNS) protocol:

- To identify an entity, TCP/IP protocol uses the IP address which uniquely identifies the connection of a host to the Internet.
- DNS is a hierarchical system, based on a distributed database, that uses a hierarchy of Name Servers to resolve Internet host names into the corresponding IP addresses required for packet routing by issuing a DNS query to a name server.
- However, people refer to use names instead of address. Therefore, we need a system that can map a name to an address and conversely an address to name.
- In TCP/IP, this is the domain name system.
- DNS in the Internet: DNS is protocol that can be used in different platforms.
- Domain name space is divided into three categories.
- **Generic Domain:** The generic domain defines registered hosts according, to their generic behaviour. Each node in the tree defines a domain which is an index to the domain name space database.



- **Country Domain:** The country domain section follows the same format as the generic domain but uses 2 characters country abbreviations (e.g., US for United States) in place of 3 characters.
- **Inverse Domain:** The inverse domain is used to map an address to a name.
- **DNS MESSAGES**
- DNS has two types of messages: query and response. Both types have the same format. The query message consists of a header and question records; the response message consists of a header, question records, answer records, authoritative records, and additional records**Header**
- Both query and response messages have the same header format with some fields set to zero for the query messages. The header is 12 bytes, and its format is shown below. The *identification* subfield is used by the client to match the response with the query. The client uses a different identification number each time it sends a query. The server duplicates this number in the corresponding response. The *flags* subfield is a collection of
- 

subfields that define the type of the message, the type of answer requested, the type of desired resolution (recursive or iterative), and so on. The *number ofquestion records* subfield contains the number of queries in the question section of the message. The *number*
ofanswer records subfield contains the number of answer records in the answer section of the response message. Its value is zero in the query message. The *number of authoritative records* subfield contains the number of authoritative records in the authoritative section of a response message. Its value is zero in the query message. Finally, the *number of*
additional records subfield contains the number additional records in the additional section of a response message. Its value is zero in the query message.

Question Section

This is a section consisting of one or more question records. It is present on both query and response messages. We will discuss the question records in a following section.

Answer Section

This is a section consisting of one or more resource records. It is present only on response messages. This section includes the answer from the server to the client (resolver).

Authoritative Section

This is a section consisting of one or more resource records. It is present only on response messages. This section gives information (domain name) about one or more authoritative servers for the query.

Additional Information Section

This is a section consisting of one or more resource records. It is present only on response messages. This section provides additionalinformation that may help the resolver. For example, a server may give the domain name of an authoritative server to the resolver in the authoritative section, and include the IP address of the same authoritative server in the additional information section.

REGISTRARS

A registrar first verifies that the requested domain name is unique and then enters it into the DNS database. A fee is charged.Today, there are many registrars; their names and addresses can be found at

http://www.intenic.net

To register, the organization needs to give the name of its server and the IP address of the server. For example, a new commercial organization named *wonderful* with a server named *ws*and IP address 200.200.200.5 needs to give the following information to one of the registrars:

Domain name: ws.**wonderful.com**

IP address: 200.200.200.5

WWWandHTTP

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

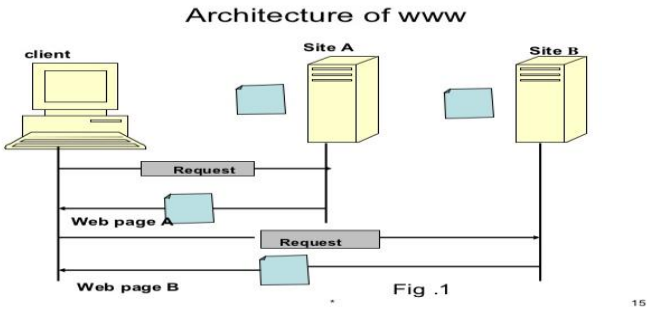


Fig .1

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.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 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.

PROTOCOL://HOST:PORT/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.

Cookies

The World Wide Web was originally designed as a stateless entity. A client sends a request; a server responds. Their relationship is over. The original design of WWW, retrieving publicly available documents, exactly fits this purpose. Today the Web has other functions; some are listed here.

I. Some websites need to allow access to registered clients only. 2. Websites are being used as electronic stores that allow users to browse through the store, select wanted items,

put them in an electronic cart, and pay at the end with a credit card. 3. Some websites are used as portals: the user selects the Web pages he wants to see. 4. Some websites are just advertising.

WEB DOCUMENTS

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. 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 .

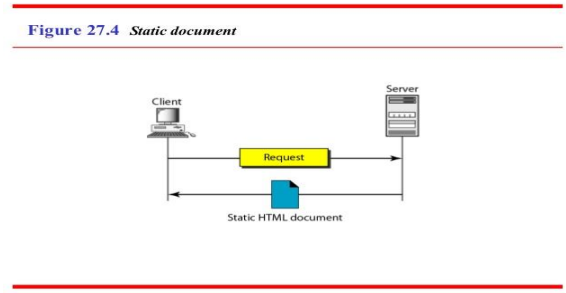


Figure 27.4 *Static document*

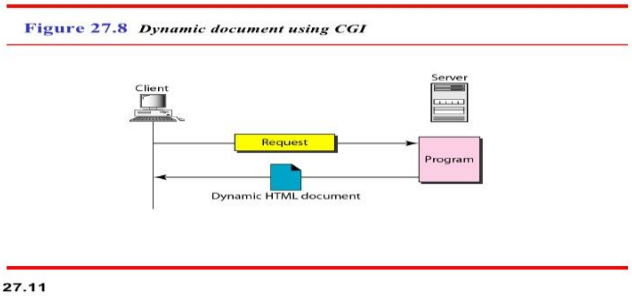
27.7

Dynamic Documents A **dynamic document** is created by a Web server whenever a browser requests the document. When a request arrives, the Web server runs an application program or a script that creates the dynamic document. The server returns the output of the program or script as a response to the browser that requested the document.

Because a fresh document is created for each request, the contents of a dynamic document can vary from one request to another. The client can ask the server to run a program such as the *date* program in UNIX and send the result of the program to the client.

Common Gateway Interface (CGI)

The **Common** Gateway **Interface** (CGI) is a technology that creates and handles dynamic documents. CGI is a set of standards that defines how a dynamic document is written, how data are input to the program, and how the output result is used.



27.11

Active Documents

For many applications, we need a program or a script to be run at the client site. These are called active documents. For example, suppose we want to run a program that creates animated graphics on the screen or a program that interacts with the user. The program definitely needs to be run at the client site where the animation or interaction takes place. When a browser requests an active document, the server sends a copy of the document or a script. The document is then run at the client (browser) site

Overview of Services:-

Service	Type	Direction
DNS	UDP	Out
HTTP/HTTPS	TCP	Out
FTP	TCP/UDP	Out
TELNET	TCP/UDP	Out
POP3	TCP	Out
SMTP	TCP	Out
IRCU	TCP/UDP	Out
IDENT	TCP	In
Private File Service	TCP/UDP	In/Out
NNTP	TCP/UDP	Out
NTP	TCP/UDP	Out
Remote Desktop	TCP/UDP	In/Out

Overview of http:-

The Hypertext Transfer Protocol (HTTP) is an application-level protocol for distributed, collaborative, hypermedia information systems. This is the foundation for data communication for the World Wide Web . HTTP is a generic and stateless protocol which can be used for other purposes as well using extensions of its request methods, error codes, and headers.

Basically, HTTP is a TCP/IP based communication protocol, that is used to deliver data (HTML files, image files, query results, etc.) .

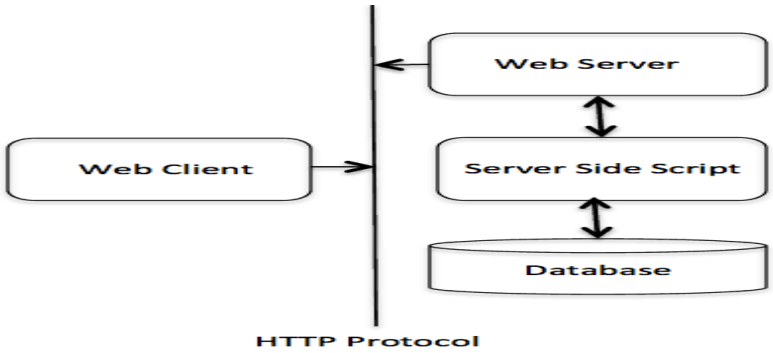
Basic Features

There are three basic features that make HTTP a simple but powerful protocol:

- **HTTP is connectionless:** The HTTP client, i.e., a browser initiates an HTTP request and after a request is made, the client disconnects from the server and waits for a response. The server processes the request and re-establishes the connection with the client to send a response back.
- **HTTP is media independent:** It means, any type of data can be sent by HTTP as long as both the client and the server know how to handle the data content. It is required for the client as well as the server to specify the content type using appropriate MIME-type.
- **HTTP is stateless:** As mentioned above, HTTP is connectionless and it is a direct result of HTTP being a stateless protocol. The server and client are aware of each other only during a current request. Afterwards, both of them forget about each other. Due to this nature of the protocol, neither the client nor the browser can retain information between different requests across the web pages.

Basic Architecture:-

The following diagram shows a very basic architecture of a web application and depicts where HTTP sits:



The HTTP protocol is a request/response protocol based on the client/server based architecture where web browsers, robots and search engines, etc. act like HTTP clients, and the Web server acts as a server.

Client:-

The HTTP client sends a request to the server in the form of a request method, URI, and protocol version, followed by a MIME-like message containing request modifiers, client information, and possible body content over a TCP/IP connection.

Server:-

The HTTP server responds with a status line, including the message's protocol version and a success or error code, followed by a MIME-like message containing server information, entity meta information, and possible entity-body content.

POSSIBLE QUESTIONS

PART-A [20*1=20 Marks]

ONLINE EXAMINATION

PART-B [5*2=10 Marks]

1. What is transport layer?
2. Define WWW.
3. What are the components of an URL?
4. Define SMTP.
5. What is HTTP?

PART-C [5*6=30 Marks]

1. Write about transport layer functions.
2. Write about overview of DNS
3. Write about the architecture of WWW.
4. Write note on DNS protocol.
5. Explain in detail about HTTP and describe how it is used to access data on World Wide Web.
6. Write about Web Documents.
7. Explain about error and flow control mechanisms in transport layer.
8. Discuss about connection establishment and release.

Karpagam Academy of Higher Education
Department of CS, CA & IT
Class: II BSC CS Batch:2017
Subject: COMPUTER NETWORKS
SubCode: 17CSU303
UNIT V

S.NO	QUESTION	OPTION A	OPTION B	OPTION C	OPTION D	ANSWER
1	In the transport layer, a message is normally divided into transmittable _____	Segments	Signals	Networks	Frames	Segments
2	The transport layer may be responsible for flow and error Control, like the _____	Physical Layer	Data Link Layer	Subnet Layer	Application Layer	Data Link Layer
3	The transport layer is responsible for process-to-process delivery of the _____	Message	Address of Message	Few Packets of Message	Partial Message	Address of Message
4	Transport layer aggregates data from different applications into a single stream before passing it to _____	network layer	data link layer	application layer	physical layer	network layer
5	Which one of the following is a transport layer protocol used in networking?	TCP	UDP	Both TCP and UDP	None of the mentioned	Both TCP and UDP
6	Which one of the following is a transport layer protocol?	stream control transmission protocol	internet control message protocol	neighbor discovery protocol	dynamic host configuration protocol	stream control transmission protocol
7	Transmission control protocol is _____	connection oriented protocol	uses a three way handshake to establish a connection	recievs data from application as a single stream	all of the mentioned	all of the mentioned
8	An endpoint of an inter-process communication flow across a computer network is called _____	socket	pipe	port	none of the mentioned	socket
9	Transport layer protocols deals with _____	application to application communication	process to process communication	node to node communication	none of the mentioned	process to process communication
10	Congestion control is divided into--------types	1	2	3	4	2

11	A ----------is mechanism that can prevent before and after it happens	open-loop	closed-loop	congestion control	none	congestion control
12	In---------- control ,policies are applied to prevent congestion before it happens	open-loop congestion	closed-loop congestion	both a & b	congestion control	open-loop congestion
13	If the sender feels that a sent packets is lost ,the packet needs to ----------	transmission	delete	retransmission	none	retransmission
14	The name of the domain is the domain name of the node at the top of the _____	Sub Tree	Main Tree	Leaf Node	Bottom Tree	Sub Tree
15	The domain, which is used to map an address to a name is called _____	Generic Domains	Inverse Domain	Main Domains	Sub-Domains	Inverse Domain
16	The term that define registered hosts according to their generic behavior, is called _____	Generic Domains	Main Domains	Super-Domains	Sub-Domains	Generic Domains
17	The DNS client adds the suffix atc.jhda.edu. before passing the address to the _____	DNS Client	DNS Server	DNS Label	DNS Recipient	DNS Server
18	New domains can be added to DNS through a _____	Query	Registrar	Domain	Response	Registrar
19	The country domains section uses two-character country _____	Generations	Abbreviations	Notations	Zones	Abbreviations
20	Hyper Text Transfer Protocol (HTTP) support	Proxy Domain	Proxy Documents	Proxy Server	Proxy IP	Proxy Server
21	Nontextual information such as digitized photos or graphic images is not a physical part of an _____	WebPage	WebData	HTML	Web-document	HTML
22	The documents in the WWW can be grouped into three broad categories _____	Static, double, active	Stateless, dynamic, archive	Static, domain, architecture	Static, dynamic, active	Static, dynamic, active
23	To use proxy server, the client must be configured to access the proxy instead of the _____	Proxy Server	Target Server	Domain Server	Original Server	Target Server
24	In WWW and HTTP. a technology that creates and handles dynamic documents is called _____	Common Gateway Interface	Common Gateway Integrate	Common Gateway IP	Common Gateway Internet	Common Gateway Interface
25	HTTP is _____ protocol.	application layer	transport layer	network layer	none of the mentioned	application layer

26	. In the network HTTP resources are located by	uniform resource identifier	unique resource locator	unique resource identifier	none of the mentioned	uniform resource identifier
27	The default connection type used by HTTP is _____	Persistent	Non-persistent	Can be either persistent or non-persistent depending on connection request	None of the mentioned	Persistent
28	The HTTP request message is sent in _____ part of three-way handshake.	First	Second	Third	None of the mentioned	Third
29	The values GET, POST, HEAD etc are specified in _____ of HTTP message	Request line	Header line	Status line	Entity body	Request line
30	Find the oddly matched HTTP status codes	200 OK	400 Bad Request	301 Moved permanently	304 Not Found	400 Bad Request
31	the service provider is distrubuted over many location called _____	internet	sites	www	http	sites
32	The web page is stored at the _____	hard disk	disk	client	server	server
33	The _____ is the computer on which the information is located	path	sites	host	cookies	host
34	_____is the pathname of the file where the information is located	host	path	server	sites	path
35	_____ is language for creating web pages	HTML	C	C++	java	HTML
36	A_____ is created by a web server whenever a browser request the document	common gate way	dynamic document	script	all the above	dynamic document
37	_____ is the protocol used mainly to access data on the world wide web	communicatio	network	WWW	HTTP	HTTP
38	In _____each segment is considered as an i	Connectionless	Connection Oriente	static	dynamic	Connectionless
39	In _____ before delivering packets, connecti	Connectionless	Connection Oriente	static	dynamic	Connectionless
40	_____ provides reliable communication between two hosts.	TCP	UDP	FTP	SMTP	TCP
41	_____ provides unreliable comm	TCP	UDP	FTP	SMTP	UDP
42	Three way handshake is referred by _____	SYN, SYN-ACK, A	SYN, ACK	SYN-ACK, ACK	ACK	SYN, SYN-ACK,

43	_____ is used to link web pages on different Websites	Absolute URL	Relative URL	dynamic URL	static URL	Absolute URL
44	_____ is used to link web pages within the s	Absolute URL	Relative URL	dynamic URL	static URL	Relative URL
45	_____ server contains the DNS database	Name	Web	Mail	Data	Name
46	The HTTP uses a TCP connection to	Establishment of se	Transfer whole data	Client server conne	Transfer files	Transfer files
47	In Hyper Text Transfer Protocol (HTTP), a client	Web-based connect	Domain	TELNET	Linear Connection	TELNET
48	The Uniform Resource Locator (URL), is a stand	Server-End	Client-End	WebPage	Internet	Internet
49	_____allows us to send message include text,auido and video .	mail	internet	E-mail	all the above	E-mail
50	The_____client established a connection with MTA server on the system	MTA	alice	UA	system server	MTA
51	The first component of an electrionic mail system is the_____	alice	server	user agent	services provider	user agent
52	_____is the example of user agents are mail,pine,and elm	user agent	command driven	GUI-based	E-mail	command driven
53	_____ define the names of aspecial files	local part	domain name	mime	both a & b	local part
54	The second part of address is_____	system server	internet	domain name	local part	domain name
55	MIME is_____	multiple internet mail extensions	multipurpose interface mail extensions	multipurpose internet mail exchange	multipurpose internet mail extensions	multipurpose internet mail extensions
56	_____ has delete and keep mode	pop	pop2	pop3	none	pop3
57	_____is the mechanism provided by TCP/IP for copying a file from one host to another	FTP	MIME	UA	pop3	FTP
58	_____ is the default format for transferring text files	image	ASCII	data structure	record structure	ASCII
59	_____ is the default format for transferring binary files	image	data structure	record structure	ASCII	image
60	In the _____ format, the file is a continuous stream of byte	file structure	record structure	data structure	image	file structure

ACK

Reg.No ----------

[17CTU303]

KARPAGAM ACADEMY OF HIGHER EDUCATION

(Deemed University Established Under Section 3 of UGC Act 1956)

COIMBATORE – 641 021

(For the candidates admitted in 2016 onwards)

I -INTERNAL EXAMINATION ,JULY 2018

Third Semester

COMPUTER TECHNOLOGY

Computer Networks

CLASS :II Bsc CT Maximum marks:50

DATE:

PART-A [20*1= 20 Marks]

1. Which of the following is a telecommunication device?
   a) digital watch b)telephone c)micro phone d)data card
2. Star Topology uses ____ as a Connection Device.
   a) Hub b) Repeater c) Switch d) Router.
3. Which of the following are the components of the network
   a)message b)receiver c)sender d)all the above
4. A_____is a set of rules for governing data communication
   a) program b)algorithm c)pseudo code d)protocol
5. Unicode used to represent _____
   a)text b)image c)video d)audio
6. ISP is a kind of _____
   a) MAN b) PAN c) WAN d) LAN
7. If communication between devices are unidirectional it is referred as_____
   a)simplex b)duplex c)half duplex d)full duplex
8. If both the devices in telecommunication can transmit and receive data simultaneously it Is referred as_____
   a)simplex b)duplex c)full duplex d)semi duplex
9. LAN cover_____miles
   a)5 b)6 c)10 d)2
10. Which of the following is not a topology?
    a)mesh b)star c)bus d)LAN
11. If all the device in the topology are provided dedicated line,the topology known as
    a)mesh b)star c)bus d)ring
12. HUB is used in _____topology
    a)mesh b)star c)bus d)ring

13. Repeaters are used in _____topology
a)star b)mesh c)bus d)ring

14. Protocols deals with _____
a)semantics b)syntax c)timing d)all the above
15. TCP/IP have _____layers
a)4 b)5 c)7 d)8
16.OSI reference model has _____layers
a) 7 b) 6 c)8 d)5
17. The transmission of data in satellite is of the _____form
a) electro-magnetic b) radio-wave c)light d)analog
18. Twisted cable transmit data in _____form
a) electro-magnetic b) radio-wave c) light d) analog
19. OSI is a _____
a) model b)protocol c)protocol and model d)network type
20._____is a device to transfer data between networks
a) Switch b) hub c) router d) repeater

Part-B **[3*2=6 Marks]**

Answer all the questions

21. Define computer network
22. List out network classification.
23. What is transmission medium?

Part-C **[3*8=24Marks]**

Answer all the questions

24. a) Explain in detail about OSI reference model with neat diagram.

(Or)

b) Discuss about network classification.

25. a) Explain about TCP/IP suite.

(Or)

b) Explain about network topologies.

26. a) Explain in detail about FDM with a neat diagram.

(Or)

b) Discuss about Transmission media.

Reg.No ----------

[17CTU303**]**

KARPAGAM ACADEMY OF HIGHER EDUCATION

(Deemed to be University)

(Established Under Section 3 of UGC Act 1956)

COIMBATORE – 641 021

(For the candidates admitted in 2016 onwards)

I -INTERNAL EXAMINATION ,July 2018

Third Semester

COMPUTER TECHNOLOGY

Computer Networks

CLASS :II Bsc CT Maximum marks:50

DATE:

PART-A **[20*1= 20 Marks]**

ANSWER ALL QUESTIONS

1. Which of the following is a telecommunication device?
   a) digital watch **b)telephone** c)micro phone d)data card
2. Data communication generally deals with_____
   a)analog signal b)voice c)digital data d)both a and b
3. Which of the following are the components of the network
   a)message b)receiver c)sender **d)all the above**
4. A_____is a set of rules for governing data communication
   a) program b)algorithm c)pseudo code **d)protocol**
5. Unicode used to represent _____
   a)text b)image c)video d)audio
6. Image colors can be represented in____formats
   a)RGP b)black and white c)YCM d)all the above
7. If communication between devices are unidirectional it is referred as_____
   a)simplex b)duplex c)half duplex d)full duplex
8. If both the devices in telecommunication can transmit and receive data simultaneously it is referred as_____
   a)simplex **b)duplex** c)full duplex d)semi duplex
9. LAN cover_____miles
   a)5 b)6 c)10 **d)2**
10. Which of the following is not a topology?
    a)mesh b)star c)bus **d)LAN**
11. If all the device in the topology are provided dedicated line,the topology known as
    a)mesh b)star c)bus d)ring
12. HUB is used in _____topology
    a)mesh **b)star** c)bus d)ring
13. Repeaters are used in _____topology

a)star b)mesh c)bus **d)ring**

14. Protocols deals with _____

a)semantics b)syntax c)timing **d)all the above**

15. TCP/IP have _____layers

a)4 b)5 c)7 d)8

16.OSI reference model has _____layers

a) 7 b) 6 c)8 d)5

17. The transmission of data in satellite is of the _____form

a) electro-magnetic b) radio-wave c)light **d)analog**

18. Twisted cable transmit data in _____form

a) electro-magnetic **b) radio-wave** c) light d) analog

19. OSI is a _____

a) model b)protocol c)protocol and model d)network type

20._____is a device to transfer data between networks

a) Switch b) hub **c) router** d) repeater

Part-B **[3*2=6 Marks]**

Answer all the questions

21. Define computer network

-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.

22. Write short notes on LAN

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.

23. What is point to point and multi point connection

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.

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.

Part-C **[3*8=24Marks]**

Answer all the questions

24. a) Explain about network topologies

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

Topology Catagories:

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. 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 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

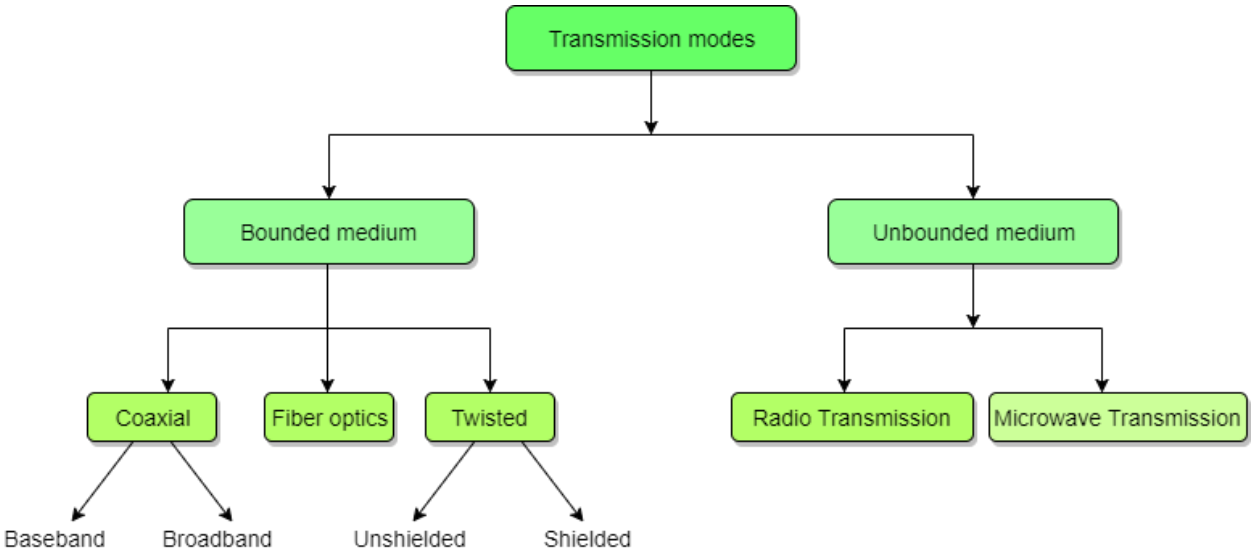
(Or)

b) Discuss about transmission modes

Data is represented by computers and other telecommunication devices using signals. Signals are transmitted in the form of electromagnetic energy from one device to another. Electromagnetic signals travel through vacuum, air or other transmission mediums to move from one point to another(from sender to receiver).

Electromagnetic energy (includes electrical and magnetic fields) consists of power, voice, visible light, radio waves, ultraviolet light, gamma rays etc.

Transmission medium is the means through which we send our data from one place to another. The first layer (physical layer) of Communication Networks OSI Seven layer model is dedicated to the transmission media.



Factors to be considered while selecting a Transmission Medium

1. Transmission Rate
2. Cost and Ease of Installation
3. Resistance to Environmental Conditions
4. Distances

   Twisted Pair Cable

   This cable is the most commonly used and is cheaper than others. It is lightweight, cheap, can be installed easily, and they support many different types of network. Some important points :

   Its frequency range is 0 to 3.5 kHz.
   Typical attenuation is 0.2 dB/Km @ 1kHz.
   Typical delay is 50 μs/km.
   Repeater spacing is 2km.
   A twisted pair consists of two conductors(normally copper), each with its own plastic insulation, twisted together. One of these wires is used to carry signals to the receiver, and the other is used only as 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. This results in a difference at the receiver.

Twisted Pair is of two types:

- Unshielded Twisted Pair (UTP)
- Shielded Twisted Pair (STP)
- Unshielded Twisted Pair Cable
- It is the most common type of telecommunication when compared with Shielded Twisted Pair Cable which consists of two conductors usually copper, each with its own colour plastic insulator. Identification is the reason behind coloured plastic insulation.

UTP cables consist of 2 or 4 pairs of twisted cable. Cable with 2 pair use RJ-11 connector and 4 pair cable use RJ-45 connector.

25. a) Discuss about network classification

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 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 in detail about OSI reference model with neat diagram

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

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

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

26. a) Explain in detail about 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 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

(Or)

b) Discuss about analog signals in detail.

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

Two signals

Same phase and frequency, but different amplitudes

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)

Note

Frequency and period are the inverse of each other.

Two signals

Same amplitude and phase, but different frequencies

Units of period and frequency

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

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.
where, 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 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.

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 nonperiodic, the decomposition gives a combination of sine waves with continuous frequencies.
Example
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
Example
The figure shows a nonperiodic 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.

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

REG NO_____

KARPAGAM ACADEMY OF HIGHER EDUCATION
(Deemed to be University)
(Established Under Section 3 of UGC Act 1956)
COIMBATORE – 641 021

Department of CS,CA & IT
Third Semester
SECOND INTERNAL EXAMINATION - AUGUST 2018

COMPUTER NETWORKS

Class & Section: II B.Sc (CT) **Duration: 2 hours**
Date & Session : .8.18(FN) **Maximum marks: 50 marks**
Subj.Code: 17CTU303

PART-A [20 * 1=20Marks]

Answer ALL the Questions

1. The following is the guided Transmission media where data is transmitted as Waves.
   a)Twisted Cable b) Fiber Optics c) UST d) Co-axial
2. FDM Stands for _____
   a) Frequency Divider Multiplier b) Frequency Division Multiplier
   c) Frequency Division Multiplexing d) Frequency Divider Multiplexing
3. The segmentation of data is done in ____layer.
   a)Presentation b) Session c) Application d) Network
4. Which of the following converts Analog into Digital and vice-versa?
   a)Hub b) Port c) Switch d) Modem
5. The process of making frame out of raw bit is called _____.
   a) Flooding b) Framing c) Switching d) Normalizing
6. The special byte used as a starting and ending of a frame is called _____.
   a)Identifier Byte b) Entry-Exit Byte c) Flag Byte d) Unique Byte
7. The process of removing the escape bytes in data link layer before forward to Network layer is called _____.
   a) Cleaner b) Optimizer c) Remover d) Stuffing
8. PPP refers to _____.
   a) Peer to Peer protocol b) Point to point Protocol
   c) Peer with Peer Protocol d) Point with point Protocol
9. The segmentation of data is done in ____layer.
   a) Presentation b) Session c) Application d) Network
10. Protocol in which sender sends one frame and waits for the Acknowledgement before proceeding are called as _____.
    a) Procedure b) stop and wait c) wait and Stop d) Stop and Proceed
11. FEC stands for _____
    a) Forward Efficiency Correction b) Forward Error Constraint
    c) Forward Error Code d) Forward Error Correction

12. If 1100 is forwarded and received as 1101 it is of which error?
    a) Burst error b) Bit error c) Byte error d) all
13. The Size of a frame in data-link layer is _____.
    a) 32 bit b) 64 bit c) 16 Bit d) not Fixed
14. ARQ refers to _____.
    a) Admitted Repeat Query b) Automatic Repeat request
    b) c) Auto Repeater Query d) None
15. An *n*-bit unit containing data and check bits is referred to as an _____
    a) Data code b) Byte Code c) Code Word d) Liner code
16. If a bit of data is being modified it is referred as _____
    a) Burst error b) Bit Error c) Byte Error d) All
17. CRC refers to _____.
    a) Circular Redundancy Check b) Cyclic Redundancy Cross
    c) Circular Repeater Checking d) Cyclic Redundancy Check
18. The number of bit positions in which two code-words differ is called_____
    a) Hamming Code b) Byte Code c) Sampling Code d) Hammer code
19._____ is a technique in which every incoming packet is sent out on every outgoing line except the one it arrived on.
    a) Routing b) Flooding c) Compressing d) Diverting
20. The special byte used as a starting and ending of a frame is called _____.
    a) Identifier Byte b) Entry-Exit Byte c) Flag Byte d) Unique Byte

PART-B **[3 * 2 = 6 Marks]**

Answer all the questions

21. List out the three phases used in circuit switched network.

22. Define Hamming distance.

23. What is single-bit error?

PART-C **[3 * 8 = 24 Marks]**

Answer all the questions

24. a)What is switched Network? Explain about Circuit-switched network.

[OR]

b) Discuss about Cable television as a media in detail.

25. a) What is framing? Discuss in short about error control and Flow control.

[OR]

b)Write note on i)Simplest Protocol ii)Stop and Wait protocol.

26. a) Explain about the transition phase in ppp protocol.

[OR]

b)Explain about error detection and error correction.

REG NO_____

[17CTU303]

KARPAGAM ACADEMY OF HIGHER EDUCATION
(Deemed to be University)
(Established Under Section 3 of UGC Act 1956)
COIMBATORE – 641 021

Department of CS,CA & IT
Third Semester
SECOND INTERNAL EXAMINATION - AUGUST 2018

COMPUTER NETWORKS

Class & Section: II B.Sc (CT) **Duration: 2 hours**
Date & Session :16.8.18(FN) **Maximum marks: 50 marks**

PART-A **[20 * 1=20Marks]**

Answer all the questions

1. The following is the guided Transmission media where data is transmitted as Waves.
   a)Twisted Cable **b) Fiber Optics** c) UST d) Co-axial
2. FDM Stands for _____
   a) Frequency Divider Multiplier b) Frequency Division Multiplier
   c) Frequency Division Multiplexing d) Frequency Divider Multiplexing
3. The segmentation of data is done in ____layer.
   a)Presentation **b) Session** c) Application d) Network
4. Which of the following converts Analog into Digital and vice-versa?
   a)Hub b) Port c) Switch **d) Modem**
5. The process of making frame out of raw bit is called _____.
   a) Flooding **b) Framing** c) Switching d) Normalizing
6. The special byte used as a starting and ending of a frame is called _____.
   a)Identifier Byte b) Entry-Exit Byte **c) Flag Byte** d) Unique Byte
7. The process of removing the escape bytes in data link layer before forward to Network layer is called _____.
   a) Cleaner b) Optimizer c) Remover **d) Stuffing**
8. PPP refers to _____.
   a) Peer to Peer protocol **b) Point to point Protocol**
   c) Peer with Peer Protocol d) Point with point Protocol
9. The segmentation of data is done in ____layer.
   a) Presentation **b) Session** c) Application d) Network
10. Protocol in which sender sends one frame and waits for the Acknowledgement before proceeding are called as _____.
    a) Procedure **b) stop and wait** c) wait and Stop d) Stop and Proceed
11. FEC stands for _____
    a) Forward Efficiency Correction b) Forward Error Constraint
    c) Forward Error Code **d) Forward Error Correction**
12. If 1100 is forwarded and received as 1101 it is of which error?
    a) Burst error **b) Bit error** c) Byte error d) all

13. The Size of a frame in data-link layer is _____.
    a) 32 bit b) 64 bit c) 16 Bit **d) not Fixed**
14. ARQ refers to _____.
    a) Admitted Repeat Query **b) Automatic Repeat request**
    b) Auto Repeater Query d) None
15. An *n*-bit unit containing data and check bits is referred to as an _____
    a) Data code b) Byte Code **c) Code Word** d) Liner code
16. If a bit of data is being modified it is referred as _____
    a) Burst error **b) Bit Error** c) Byte Error d) All
17. CRC refers to _____.
    Circular Redundancy Check b) Cyclic Redundancy Cross
    c) Circular Repeater Checking **d) Cyclic Redundancy Check**
18. The number of bit positions in which two code-words differ is called_____
    a) Hamming Code b) Byte Code c) Sampling Code d) Hammer code
19._____ is a technique in which every incoming packet is sent out on every outgoing line except the one it arrived on.
    a) Routing **b) Flooding** c) Compressing d) Diverting
20. ACK refers to_____
    a)Acknowledge b) Automation **c) Acknowledgement** d)None

PART-B **[3 * 2 = 6 Marks]**

Answer all the questions

21. List out the three phases used in circuit switched network.

The three phases used in circuit switched network are

i)Setup phase

ii)Data transfer phase

iii)Teardown phase

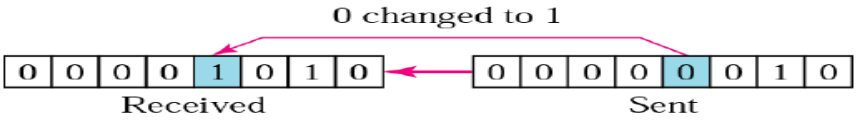
22. Define Hamming distance.

Hamming distance between two words (of the same size) is the number of differences between the corresponding bits. Hamming distance is a value greater than zero.

- Example: Hamming distance d(10101, 11110) is 3

23. What is single-bit error?

Data can be corrupted during transmission. For reliable communication, errors must be detected and corrected.



In a single-bit error, only one bit in the data unit has changed.

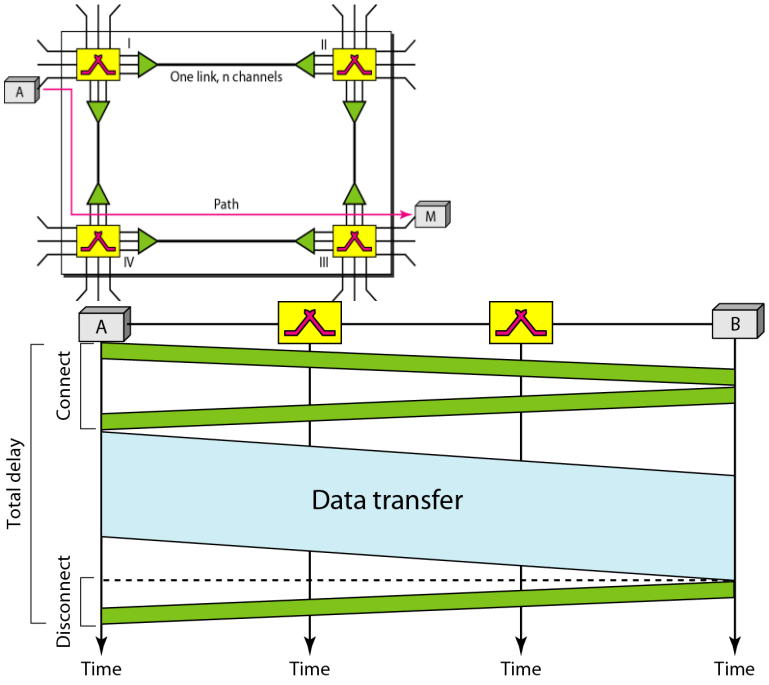
PART-C **[3 * 8 = 24 Marks]**

Answer all the questions

24. a)What is switched Network? Explain about Circuit-switched network.

A circuit-switched network is made of a set of switches connected by physical links, in which each link is divided into n channels.

- A circuit-switched network is made of a set of switches connected by physical links, in which each link is divided into n channels
- In circuit switching, the resources need to be reserved during the setup phase; the resources remain dedicated for the entire duration of data transfer until the teardown phase.



- 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. end-to-end addressing is required for creating a connection between the two end systems.

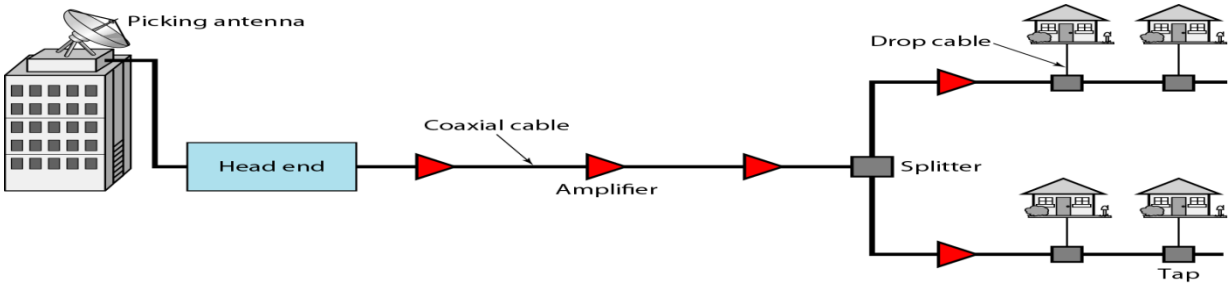
- Data Transfer Phase: After the establishment of the dedicated circuit, the two parties can transfer data.
- Teardown Phase When one of the parties needs to disconnect, a signal is sent to each switch to release the resources.
- Efficiency is low
- Delay in a circuit-switched network is minimum. It has 4 parts: the propagation time of the source computer request, the request signal transfer time , the propagation time of the acknowledgment from the destination computer, and the signal transfer time of the acknowledgment

[OR]

b)Discuss about Cable television as a media in detail.

The cable TV network started as a video service provider, but it has moved to the business of Internet access. In this section, we discuss cable TV networks per se; in Section 9.5 we discuss how this network can be used to provide high-speed access to the Internet.

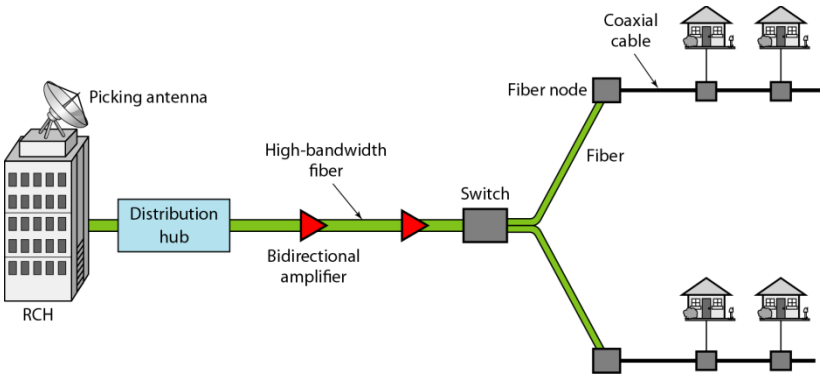
Traditional cable TV network



Communication in the traditional cable TV network is unidirectional.

The cable TV office, called the head end, receives video signals from broadcasting stations and feeds the signals into coaxial cables. The signals became weaker and weaker with distance, so amplifiers were installed through the network to renew the signals. There could be up to 35 amplifiers between the head end and the subscriber premises. At the other end, splitters split the cable, and taps and drop cables make the connections to the subscriber premises.

Hybrid fiber-coaxial (HFC) network



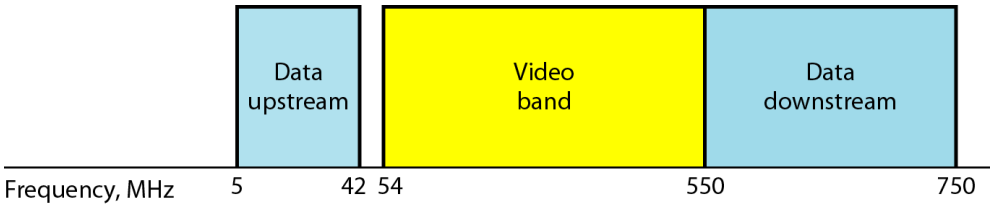
Communication in an HFC cable TV network can be bidirectional.

The second generation of cable networks is called a hybrid fiber-coaxial (HFC) network.

The network uses a combination of fiber-optic and coaxial cable. The transmission medium from the cable TV office to a box, called the fiber node, is optical fiber; from thefiber node through the neighborhood and into the house is still coaxial cable. .

Cable companies are now competing with telephone companies for the residential customer who wants high-speed data transfer. In this section, we briefly discuss this technology.

Division of coaxial cable band by CATV



Downstream data are modulated using the 64-QAM modulation technique.

The theoretical downstream data rate is 30 Mbps.

Upstream data are modulated using the QPSK modulation technique.

The theoretical upstream data rate is 12 Mbps.

25. a) What is framing? Discuss in short about error control and Flow control.

FRAMING

Data transmission in the physical layer means moving bits in the form of a signal from the source to the destination. The physical layer provides bit synchronization to ensure that the sender and receiver use the same bit durations and timing. The data link layer, on the other hand, needs to pack bits into frames, so that each frame is distinguishable from another.

Framing in the data link layer separates a message from one source to a destination, or from other messages to other destinations, by adding a sender address and a destination address. The destination address defines where the packet is to go; the sender address helps the recipient acknowledge the receipt.

Flow Control

Flow control coordinates the amount of data that can be sent before receiving an acknowledgment and is one of the most important duties of the data link layer. In most protocols, flow control is a set of procedures that tells the sender how much data it can transmit before it must wait for an acknowledgment from the receiver. Any receiving device has a limited speed at which it can process incoming data and a limited amount of memory in which to store incoming data. The receiving device must be able to inform the sending device before those limits are reached and to request that the transmitting device send fewer frames or stop temporarily. Incoming data must be checked and processed before they can be used. The rate of such processing is often slower than the rate of transmission. For this reason, each receiving device has a block of memory, called a *buffer,* reserved for storing incoming data until they are processed. If the buffer begins to fill up, the receiver must be able to tell the sender to halt transmission until it is once again able to receive.

Error Control

Error control is both error detection and error correction. It allows the receiver to inform the sender of any frames lost or damaged in transmission and coordinates the retransmission of those frames by the sender. In the data link layer, the term *error control* refers primarily to methods of error detection and retransmission. Error control in the data link layer is often implemented simply: Any time an error is detected in an exchange, specified frames are retransmitted. This process is called automatic repeat request (ARQ).

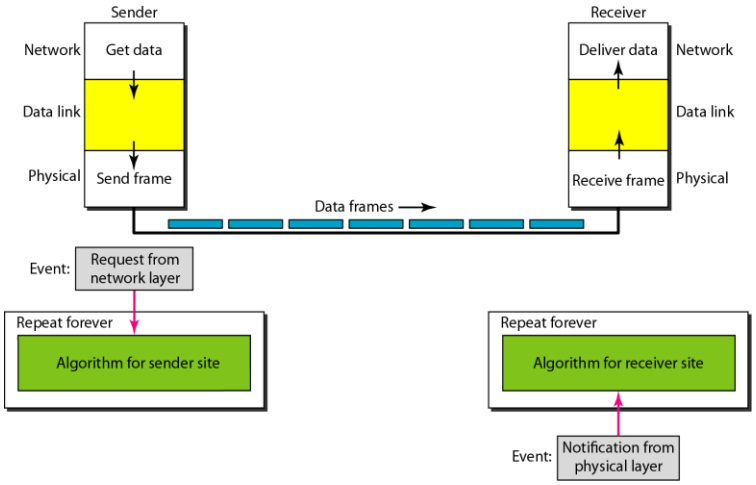
[OR]

b)Write note on i)Simplest Protocol ii)Stop and Wait protocol.

First protocol, the Simplest Protocol, is one that has no flow or en'or control. Like other protocols, it is a unidirectional protocol in which data frames are traveling in only one direction-from the sender to receiver. The receiver can immediately handle any frame it receives with a processing time that is small enough to be negligible. The data link layer of the receiver immediately removes the header from the frame and hands the data packet to its network layer, which can also accept the packet immediately. In other words, the receiver can never be overwhelmed with incoming frames.

Design

There is no need for flow control in this scheme. The data link layer at the sender site gets data from its network layer, makes a frame out of the data, and sends it. The data link layer at the receiver site receives a frame from its physical layer, extracts data from the frame, and delivers the data to its network layer.



The sender site cannot send a frame until its network layer has a data packet to send. The receiver site cannot deliver a data packet to its network layer until a frame arrives. The procedure at the sender site is constantly running; there is no action until there is a request from the network layer. The procedure at the receiver site is also constantly running, but there is no action until notification from the physical layer arrives. Both procedures are constantly running because they do not know when the corresponding events will occur.

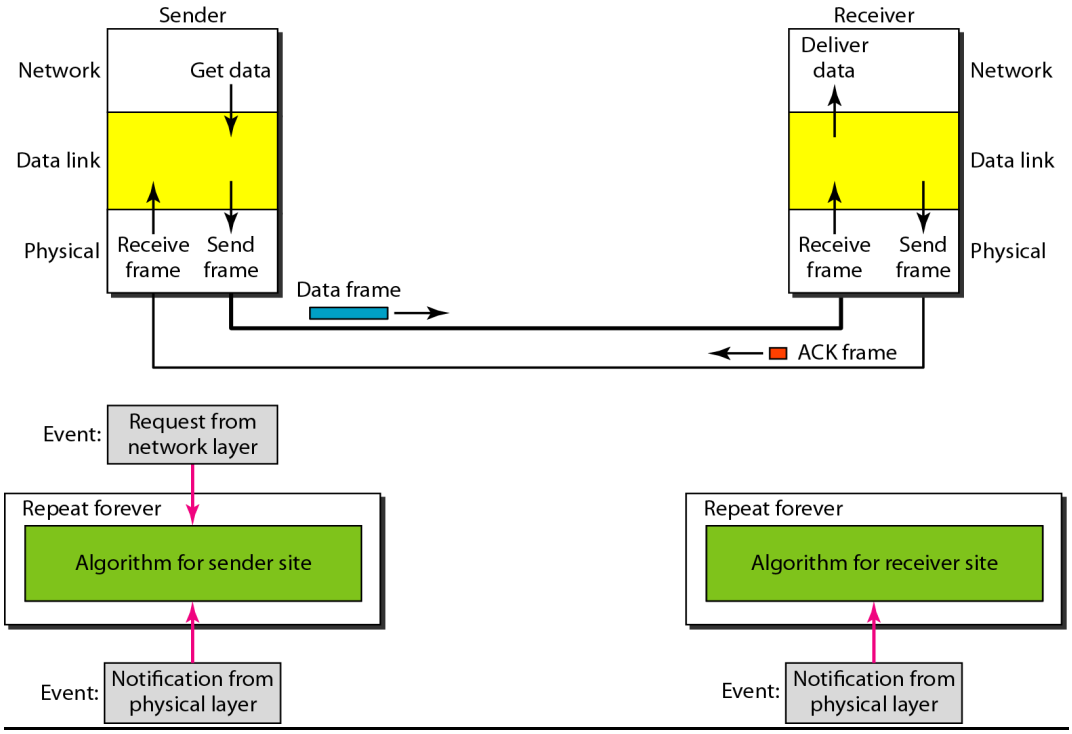
Stop-and-Wait Protocol

If data frames arrive at the receiver site faster than they can be processed, the frames must be stored until their use. Normally, the receiver does not have enough storage space, especially if it is receiving data from many sources. This may result in either the discarding of frames or denial of service. To prevent the receiver from becoming overwhelmed with frames, receiver should tell the sender to slow down. There must be feedback from the receiver to the sender.

The protocol is called the Stop-and-Wait Protocol because the sender sends one frame, stops until it receives confirmation from the receiver (okay to go ahead), and then sends the next frame. Communication is unidirectional for data frames, but auxiliary ACK frames (simple tokens of acknowledgment) travel from the other direction. Flow control to the previous protocol.

Design

Figure illustrates the mechanism. At any time, there is either one data frame on the forward channel or one ACK frame on the reverse channel, therefore need a half-duplex link.



26. a) Explain about the transition phase in ppp protocol.

A PPP connection goes through phases which can be shown in a transition phase

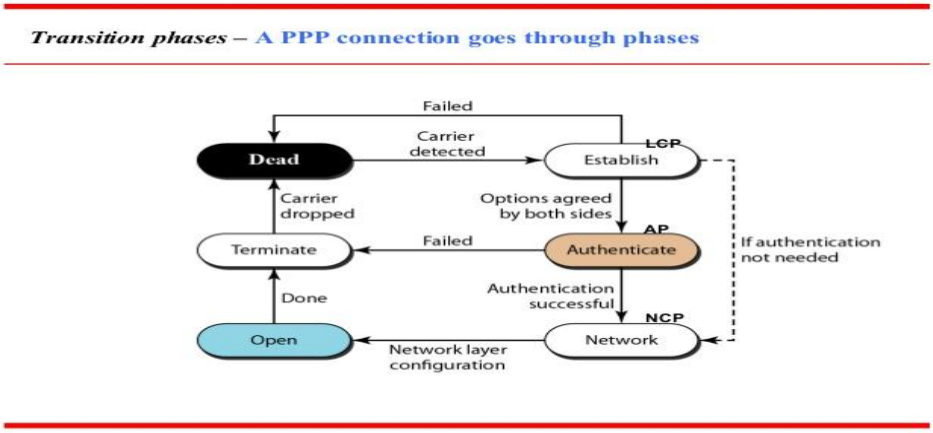


diagram11.42

Dead. In the dead phase the link is not being used. There is no active carrier (at the physical layer) and the line is quiet.
Establish. When one of the nodes starts the communication, the connection goes into this phase. In this phase, options are negotiated between the two parties. If the negotiation is successful, the system goes to the authentication phase (if authentication is required) or directly to the networking phase. The link control protocol packets, discussed shortly, are used for this purpose. Several packets may be exchanged here.
Authenticate. The authentication 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, discussed later. If the result is successful, the connection goes to the networking phase; otherwise, it goes to the termination phase.
Network. In the 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. The reason is that PPP supports multiple protocols at the network layer.

Open. In the open phase, data transfer takes place. When a connection reaches this phase, the exchange of data packets can be started. The connection remains in this phase until one of the endpoints wants to terminate the connection.
Terminate. In the termination phase the connection is terminated. Several packets are exchanged between the two ends for house cleaning and closing the link.

[OR]

b) Explain about error detection and 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.

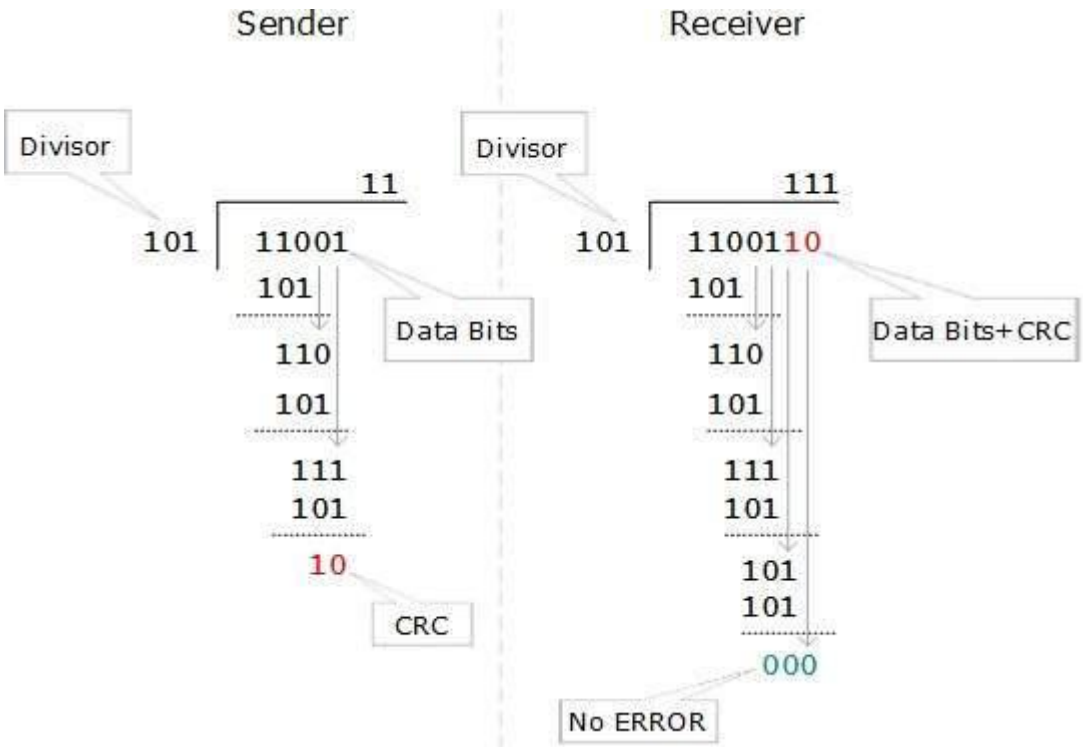
The sender while creating a frame counts the number of 1s in it. For example, if even parity is used and number of 1s is even then one bit with value 0 is added. This way number of 1s remains even. If the number of 1s is odd, to make it even a bit with value 1 is added.

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.

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

REG NO_____

[17CTU303]

KARPAGAM ACADEMY OF HIGHER EDUCATION
(Deemed to be University)
(Established Under Section 3 of UGC Act 1956)
COIMBATORE – 641 021

Department of CS, CA & IT
Third Semester
THIRD INTERNAL EXAMINATION - AUGUST 2018

COMPUTER NETWORKS

Class & Section: II B.Sc (CT) **Duration: 2 hours**
Date & Session : 09.10.2018 (FN) **Maximum marks: 50 marks**

PART-A (20 * 1=20Marks)

Answer all the questions

1. Web pages are written in a language called ____
   a) MIME b) HTML c) Http d) URL
2. The____ protocol is used to establish an online connection to a remote machine.
   a) TELNET b) HTML c) Http d) URL
3. The hardware or software within the transport layer that does the work is called the ___.
   a) Network entity b) Transport entity c) Physical entity d) None
4. TPDU stands for____
   a) Transport protocol data unit b) Transport protocol datagram unit
   c) Terminal protocol data unit d) Transfer protocol data unit
5. Each socket has a 16-bit number local to that host called a_____.
   a) Well known ports b) ports c) TCP d) None
6. The transport service is implemented by a _____ used between the two transport entities.
   a) Network protocol b) transport protocol c) application protocol d) All
7. Each socket has a socket number consisting of the IP address of the host and a 16 bit number local to that host called a _____
   a) Port b) UDP c) IP d) Hub
8. The Bottom Four layers of OSI can be treated as _____
   a) Transport Service Users b) Transport Service Providers
   c) Transport Service Helpers d) Transport Service Clients
9. A _____consists of a fixed 20 byte header followed by zero or more data bytes
   a) UDP segment b) TCP segment c) Port segment d) Datagram Segment
10. _____refers to moving messages from the originator to the recipient
    a) Composition b) Transfer c) disposition d) reported
11. The message inside the envelope contains _____parts
    a) 3 b) 2 c) 4 d) 1
12. Network management is done from _____
    a) Stations b) management systems c) management nodes d) management protocols
13. If more than a bit of data is being modified it is referred as _____
    a) Burst error b) Bit Error c) Byte Error d) All
14. DNS stands for_____

a) Digital Name Server b) Domain Name Serve c) Domain name System d) None

15. ARP stands for____
    a) Address resolution protocol b) Automatic resolution protocol
    c) Address Resolver protocol d) arrived resolver protocol
16. RARP stands for_____.
    a) Redirect address resolution protocol b) Reverse address resolution protocol
    c) Reverse automatic resolver protocol d) none
17. The ___ tells where in the current datagram this fragment belongs
    a) Fragment off set b) type of service c) time to live d) Source Address
18. Which layer handles data in the form of frame?
    a) Network b) Session c) Physical d) Data-link
19. The mechanism of delivering acknowledgement with the next set of data is called___
    a) Piggy Backing b) Resolver c) Acknowledgement d) Retriever
20. The Process to Process Communication is _____layer.
    a) Session b) Transport c) Presentation d) Application

PART-B **(3*2=6 Marks)**

Answer ALL the questions.

21. Define a hub.
22. Define WWW.
23. What are the types of an URL?

PART –C **(3x 8 =24 Marks)**

Answer ALL the questions.

24. a) What is CSMA? Discuss about it in detail.

(OR)

b) Write a note on IPV4.

25. a) Write about transport layer functions.

(OR)

b) Explain about overview of DNS

26. a) Discuss about the connecting LANS in detail.

(OR)

b) Explain in detail about the architecture of WWW.

s

Reg.No ----------

[17CTU303**]**

KARPAGAM ACADEMY OF HIGHER EDUCATION

(Deemed to be University)

(Established Under Section 3 of UGC Act 1956)

COIMBATORE – 641 021

(For the candidates admitted in 2017 onwards)

III -INTERNAL EXAMINATION ,SEPTEMBER 2018

Third Semester

COMPUTER TECHNOLOGY

Computer Networks

CLASS :II Bsc CT Maximum marks:50

DATE:

PART-A (20*1= 20 Marks)

1. Web pages are written in a language called ____

   a) MIME b**) HTML** c) Http d) URL

2. The____ protocol is used to establish an online connection to a remote machine.

   a) **TELNET** b) HTML c) Http d) URL

3. The hardware or software within the transport layer that does the work is called the ___.

   a) **Network entity** b) Transport entity c) Physical entity d) None

4. TPDU stands for____

   a) **Transport protocol data unit** b) Transport protocol datagram unit

   c) Terminal protocol data unit d) Transfer protocol data unit

5. Each socket has a 16-bit number local to that host called a_____.

   a) **Well known ports** b) ports c) TCP d) None

6. The transport service is implemented by a _____ used between the two transport entities.

   a) Network protocol b**) transport protocol** c) application protocol d) All

7. Each socket has a socket number consisting of the IP address of the host and a 16 bit number local

   to that host called a _____

   a) **Port** b) UDP c) IP d) Hub

8. The Bottom Four layers of OSI can be treated as _____

   a) Transport Service Users b) **Transport Service Providers** c) Transport Service Helpers

   d) Transport Service Clients

9. A _____consists of a fixed 20 byte header followed by zero or more data bytes

   a) UDP segment b) TCP segment c) **Port segment** d) Datagram Segment

10._____refers to moving messages from the originator to the receipier

   a) Composition b) **Transfer** c) disposition d) reported

11. The message inside the envelope contains _____parts
    a) 3 b) **2** c) 4 d) 1
12. Network management is done from _____
    a) Stations b) **management systems** c) management nodes d) management protocols

13. If more than a bit of data is being modified it is referred as _____
    a) Burst error b) Bit Error c) Byte Error d) All
14. DNS stands for_____
    a) Digital Name Server b) Domain Name Serve c) **Domain name System** d) None
15. ARP stands for____
    a) **Address resolution protocol** b) Automatic resolution protocol
    c) Address Resolver protocol d) arrived resolver protocol
16. RARP stands for_____.
    a) Redirect address resolution protocol b) **Reverse address resolution protocol**
    c) Reverse automatic resolver protocol d) none
17. The ___ tells where in the current datagram this fragment belongs
    a) **Fragment off set** b) type of service c) time to live d) Source Address
18. Which layer handles data in the form of frame?
    a) Network b) Session c) Physical d) **Data-link**
19. The mechanism of delivering acknowledgement with the next set of data is called___
    a) **Piggy Backing** b) Resolver c) Acknowledgement d) Retriever
20. The Process to Process Communication is _____layer.
    a) Session b) **Transport** c) Presentation d) Application

PART-B (3*2=6 Marks)

Answer ALL of the following

21. What are the components of an URL?

ANS: A Uniform Resource Locator(URL) colloquially tremed a Web address,is a reference to a web resource that specifies its location on a computer network and a mechanism of retrieving it.

22. Define WWW.

ANS: The World Wide Web(WWW) is a network of online content that is formatted in HTML and accessed via HTTP. The term refer to all the interlinked HTML pages that can accessed over the internet.

23. What is the difference between a direct and an indirect delivery?

ANS: Forwarded IP packets used at least one of two types of delivery based on whether the IP packet is forwarded to the final destination or whether it is forwarded to an IP router. These two types of delivery are known as direct and indirect delivery

DIRECT : Direct delivery occurs when the IP node forwards a packet to the final destination on a direct delivery attached network**.**

INDIRECT: Indirect delivery occurs when the IP node forwards a packet to an intermediate node because the final destination is not a directly attached network.

PART –C **(3x 8 =24Marks)**

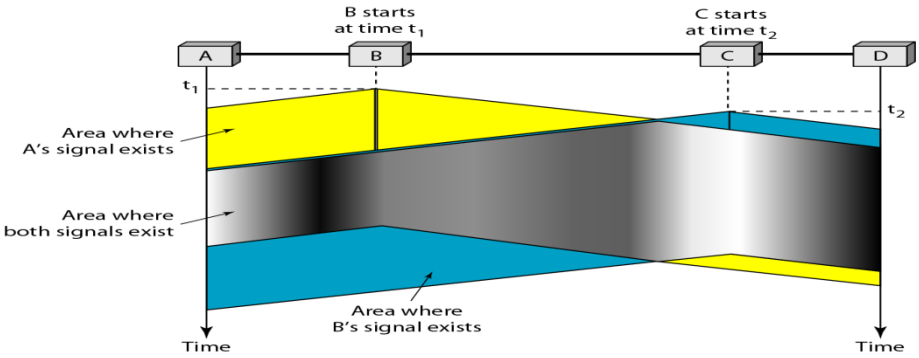
Answer ALL the questions.

24. a) What is CSMA? Discuss about it in detail.

ANS: Carrier Sense Multiple Access (CSMA)

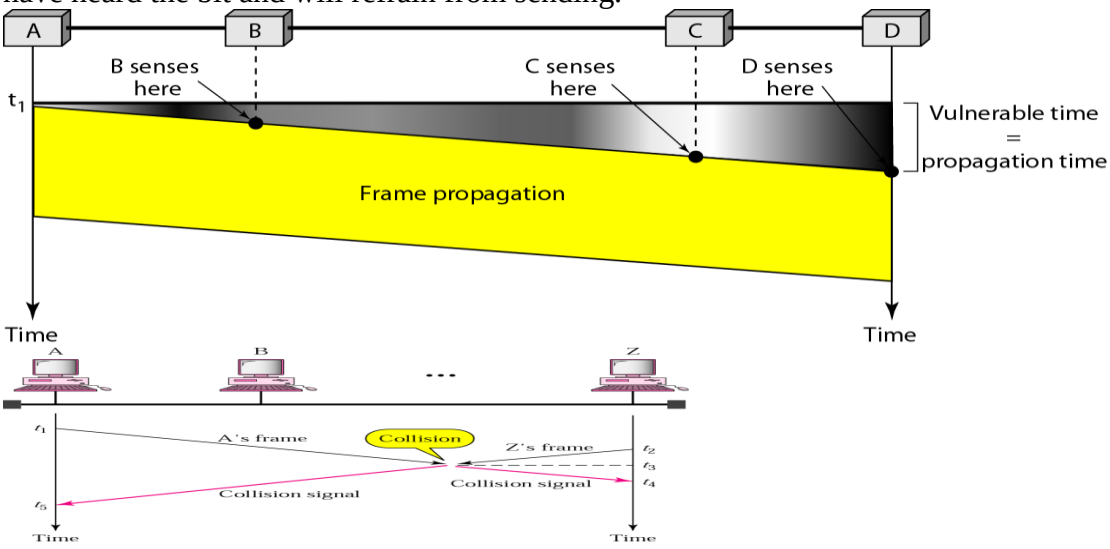
To minimize the chance of collision and, therefore, increase the performance, the CSMA method was developed. The chance of collision can be reduced if a station senses the medium before trying to use it. Carrier sense multiple access (CSMA) requires that each station first listen to the medium (or check the state of the medium) before sending. CSMA can reduce the possibility of collision, but it cannot eliminate it. The reason for this is shown in Figure, a space and time model of a CSMA network. Stations are connected to a shared channel (usually a dedicated medium).

The possibility of collision still exists because of propagation delay; when a station sends a frame, it still takes time (although very short) for the first bit to reach every station and for every station to sense it. In other words, a station may sense the medium and find it idle, only because the first bit sent by another station has not yet been received. At time *t1* station B senses the medium and finds it idle, so it sends a frame. At time *t2 (t2> t1)* station C senses the medium and finds it idle because, at this time, the first bits from station B have not reached station C. Station C also sends a frame. The two signals collide and both frames are destroyed.



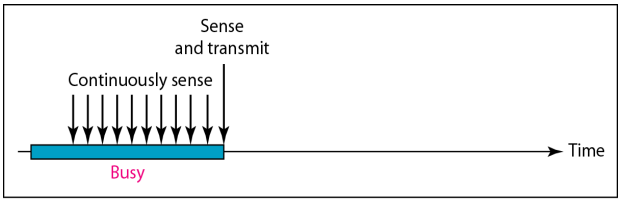
Vulnerable Time:

The vulnerable time for CSMA is the propagation time *Tp*. This is the time needed for a signal to propagate from one end of the medium to the other. When a station sends a frame, and any other station tries to send a frame during this time, a collision will result. But if the first bit of the frame reaches the end of the medium, every station will already have heard the bit and will refrain from sending.

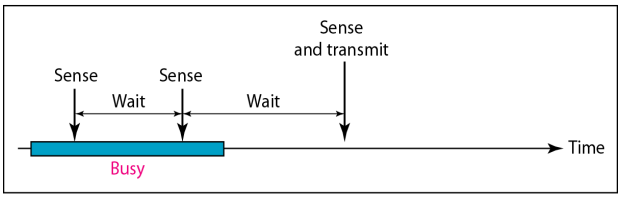


Persistence Methods

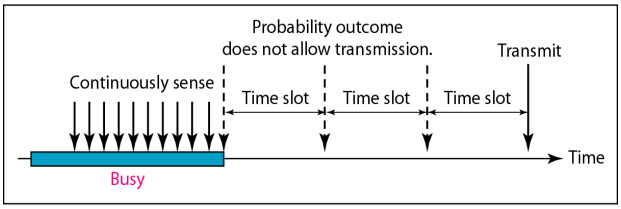
I-Persistent: The **I-persistent method** is simple and straightforward. Inthis method, after the station finds the line idle, sends its frame immediately (with probability I).This method has the highest chance of collision because two or more stations may find the line idle and send their frames immediately.



a. 1-persistent



b. Nonpersistent



c. p-persistent

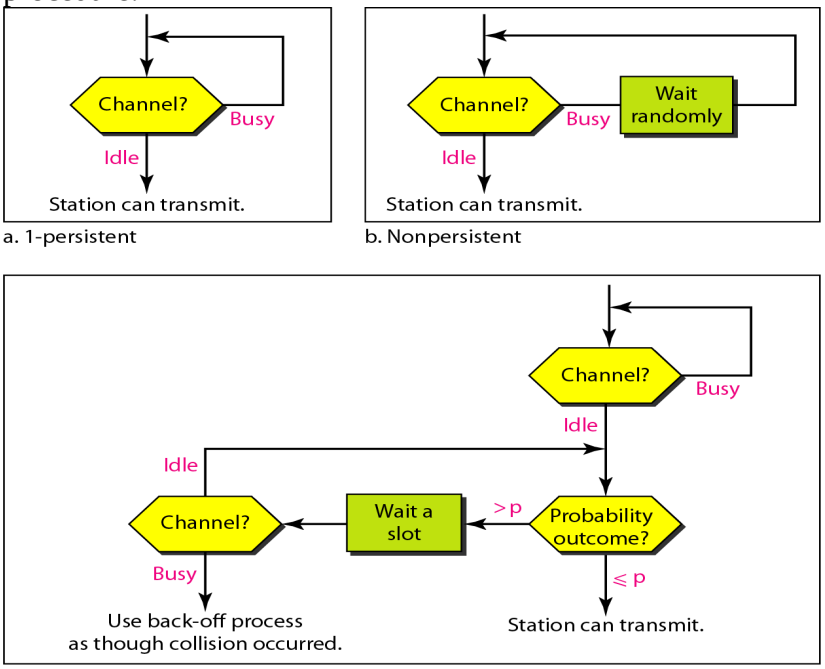
Nonpersistent In the **nonpersistent method,** a station that has a frame to send senses the line. If the line is idle, it sends immediately. If the line is not idle, it waits a random amount of time and then senses the line again. The nonpersistent approach reduces the chance of collision because it is unlikely that two or more stations will wait the same amount of time and retry to send simultaneously. However, this method reduces the efficiency of the network because the medium remains idle when there may be stations with frames to send.

p-PersistentThep-persistent method is used if the channel has time slots with a slot duration equal to or greater than the maximum propagation time. The p-persistent approach combines the advantages of the other two strategies. It reduces the chance of collision and improves efficiency. In this method, after the station finds the line idle it follows these steps:

1. With probability *p*, the station sends its frame.
2. With probability $q = 1 - p$, the station waits for the beginning of the next time slotand checks the line again.

a. If the line is idle, it goes to step 1.

b. If the line is busy, it acts as though a collision has occurred and uses the back off procedure.

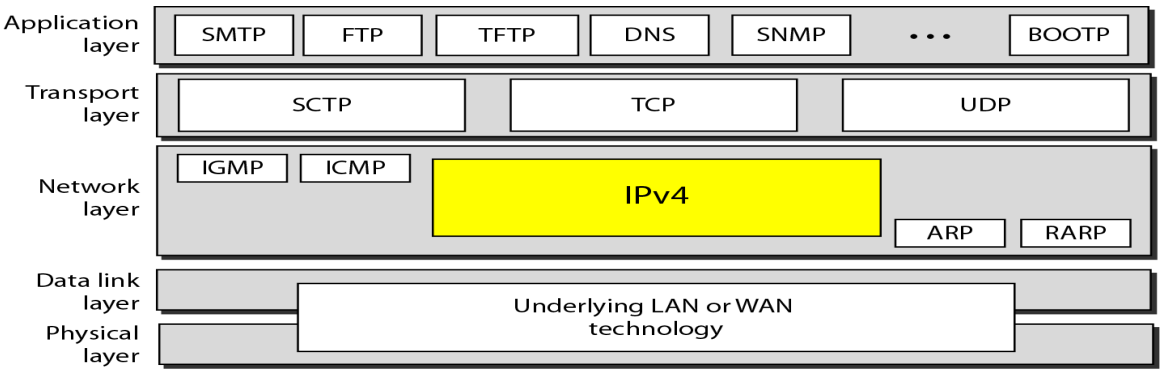


(OR)

b)Write a note on IPV4.

ANS: IPv4

The Internet Protocol version 4 (IPv4) is the delivery mechanism used by the TCP/IP protocols. Figure shows the position of IPv4 in the suite.

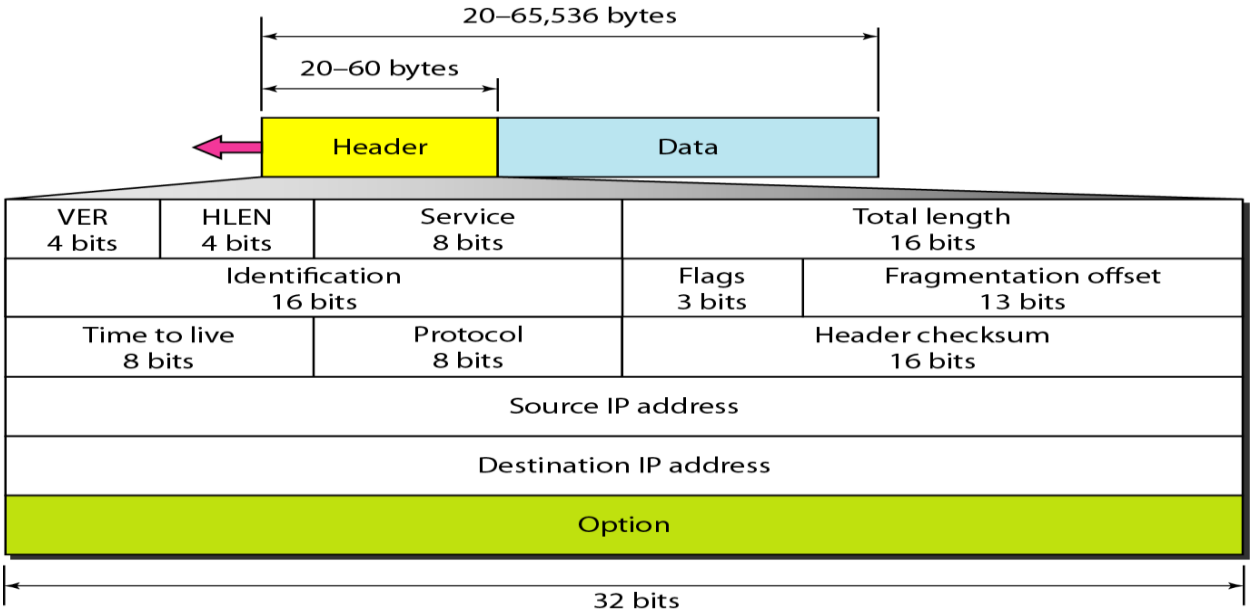


IPv4 is an unreliable and connectionless datagram protocol-a best-effort delivery service. The term *best-effort* means that IPv4 provides no error control or flow control (except for error detection on the header). IPv4 assumes the unreliability of the underlying layers and does its best to get a transmission through to its destination, but with no guarantees.

IPv4 is also a connectionless protocol for a packet-switching network that uses the datagram approach. This means that each datagram is handled independently, and each datagram can follow a different route to the destination. This implies that datagrams sent by the same source to the same destination could arrive out of order. Also, some could be lost or corrupted during transmission. Again, IPv4 relies on a higher-level protocol to take care of all these problems.

Datagram

Packets in the IPv4 layer are called datagrams. Figure below shows the IPv4 datagram format.

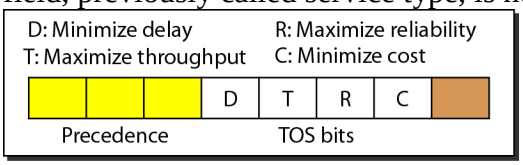


A datagram is a variable-length packet consisting of two parts: header and data.

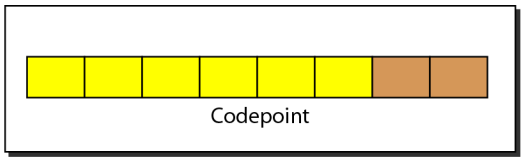
The header is 20 to 60 bytes in length and contains information essential to routing and delivery. It is customary in *TCP/IP* to show the header in 4-byte sections. A brief description of each field is given below.

- Version (VER). This 4-bit field defines the version of the IPv4 protocol.

- Header length (HLEN). This 4-bit field defines the total length of the datagram header in 4-byte words. This field is needed because the length of the header is variable (between 20 and 60 bytes)
- Services. IETF has changed the interpretation and name of this 8-bit field. This field, previously called service type, is now called differentiated services.



Service type



Differentiated services

1. Service Type

In this interpretation, the first 3 bits are called precedence bits. The next 4 bits are called type of service (TOS) bits, and the last bit is not used.

a. Precedence is a 3-bit subfield ranging from 0 (000 in binary) to 7 (111 in binary). The precedence defines the priority of the datagram in issues such as congestion.

b. TOS bits is a 4-bit subfield with each bit having a special meaning. Although a bit can be either 0 or 1, one and only one of the bits can have the value of 1 in each datagram. The bit patterns and their interpretations are given in Table

TOS Bits	*Description*
0000	Normal (default)
0001	Minimize cost
0010	Maximize reliability
0100	Maximize throughput
1000	Minimize delay

2. Differentiated Services

In this interpretation, the first 6 bits make up the codepoint subfield, and the last 2 bits are not used. The codepoint subfield can be used in two different ways.

a. When the 3 rightmost bits are Os, the 3 leftmost bits are interpreted the same as the precedence bits in the service type interpretation. In other words, it is compatible with the old interpretation.

When the 3 rightmost bits are not all Os, the 6 bits define 64 services based on the priority assignment by the Internet or local authorities according to Table below. The first category contains 32 service types; the second and the third each contain 16. The first category (numbers 0, 2,4, ... ,62) is assigned by the Internet authorities (IETF). The second category (3, 7, 11, 15, , 63) can be used by local authorities (organizations). The third category (1, 5, 9, ,61) is temporary and can be used for experimental purposes.

Value	*Protocol*
1	ICMP
2	IGMP
6	TCP
17	UDP
89	OSPF

- Total length. This is a In-bit field that defines the total length (header plus data) of the IPv4 datagram in bytes. To find the length of the data coming from the upper layer, subtract the header length from the total length. The header length can be found by multiplying the value in the HLEN field by 4.

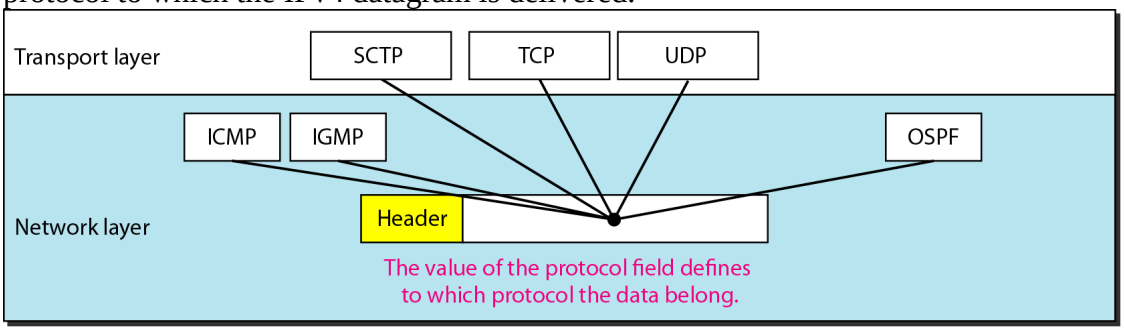
Length of data =total length - header length

Since the field length is 16 bits, the total length of the IPv4 datagram is limited to 65,535 (216 - 1) bytes, of which 20 to 60 bytes are the header and the rest is data from the upper layer.

- Time to live. A datagram has a limited lifetime in its travel through an internet.

This field was originally designed to hold a timestamp, which was decremented by each visited router. The datagram was discarded when the value became zero. Today, this field is used mostly to control the maximum number of hops (routers) visited by the datagram. When a source host sends the datagram, it stores a number in this field. This value is approximately 2 times the maximum number of routes between any two hosts. Each router that processes the datagram decrements this number by 1. If this value, after being decremented, is zero, the router discards the datagram.

- Protocol. This 8-bit field defines the higher-level protocol that uses the services of the IPv4 layer. An IPv4 datagram can encapsulate data from several higher-level protocols such as TCP, UDP, ICMP, and IGMP. This field specifies the final destination protocol to which the IPv4 datagram is delivered.



- Checksum. First, the value of the checksum field is set to O. Then the entire header is divided into 16-bit sections and added together. The result (sum) is complemented and inserted into the checksum field. The checksum in the IPv4 packet covers only the header, not the data.
- Source address. This 32-bit field defines the IPv4 address of the source. This field must remain unchanged during the time the IPv4 datagram travels from the source host to the destination host.
- Destination address. This 32-bit field defines the IPv4 address of the destination. This field must remain unchanged during the time the IPv4 datagram travels from the source host to the destination host.

Fragmentation

A datagram can travel through different networks. Each router decapsulates the IPv4 datagram from the frame it receives, processes it, and then encapsulates it in another frame. The format and size of the received frame depend on the protocol used by the physical network through which the frame has just traveled. The format and size of the sent frame depend on the protocol used by the physical network through which the frame is going to travel.

Maximum Transfer Unit (MTU)

Each data link layer protocol has its own frame format in most protocols. One of the fields defined

Protocol	*MTU*
Hyperchannel	65,535
Token Ring (16 Mbps)	17,914
Token Ring (4 Mbps)	4,464
FDDI	4,352
Ethernet	1,500
X.25	576
PPP	296

in the format is the maximum size of the data field. In other words, when a datagram is encapsulated in a frame, the total size of the datagram must be less than this maximum size, which is defined by the restrictions imposed by the hardware and software used in the network The value of the MTU depends on the physical network protocol

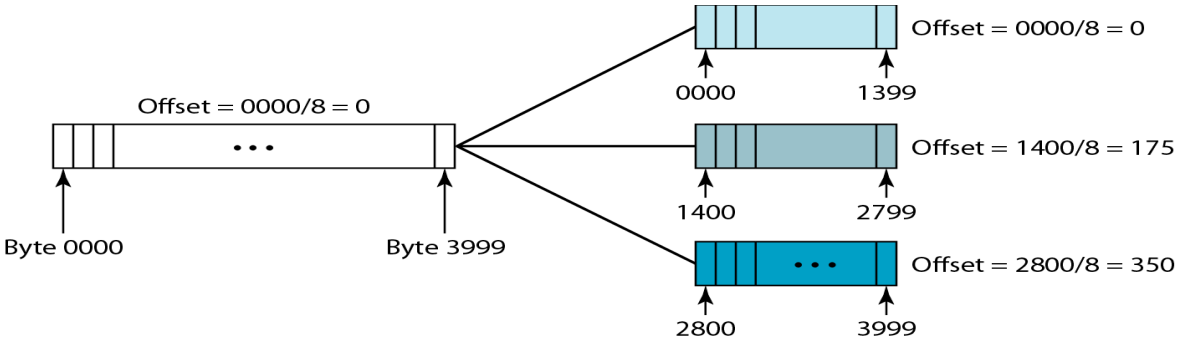
To make the IPv4 protocol independent of the physical network, the designers decided to make the maximum length of the IPv4 datagram equal to 65,535 bytes.This is called **fragmentation.**

The source usually does not fragment the IPv4 packet. The transport layer will instead segment the data into a size that can be accommodated by IPv4 and the data link layer in use. When a datagram is fragmented, each fragment has its own header with most of the fields repeated, but with some changed. A fragmented datagram may itself be fragmented if it encounters a network with an even smaller MTU. In other words, a datagram can be fragmented several times before it reaches the final destination. The reassembly of the datagram is done only by the destination host because each fragment becomes an independent datagram

Fields Related to Fragmentation

The fields that are related to fragmentation and reassembly of an IPv4 datagram are the identification, flags, and fragmentation offset fields.

- Identification. This 16-bit field identifies a datagram originating from the source host. The combination of the identification and source IPv4 address must uniquely define a datagram as it leaves the source host. To guarantee uniqueness, the IPv4 protocol uses a counter to label the datagrams. The counter is initialized to a positive number. When the IPv4 protocol sends a datagram, it copies the current value of the counter to the identification field and increments the counter by 1. As long as the counter is kept in the main memory, uniqueness is guaranteed. When a datagram is fragmented, the value in the identification field is copied to all fragments. In other words, all fragments have the same identification number, the same as the original datagram. The identification number helps the destination in reassembling the datagram.
- Flags. This is a 3-bit field. The first bit is reserved. The second bit is called the *donotfragment*bit. If its value is 1, the machine must not fragment the datagram. If it cannot pass the datagram through any available physical network, it discards the datagram and sends an ICMP error message to the source host. If its value is 0, the datagram can be fragmented if necessary. The third bit is called the *more fragment* bit. If its value is 1, it means the datagram is not the last fragment; there are more fragments after this one. If its value is 0, it means this is the last or only fragment
- Fragmentation offset. This 13-bit field shows the relative position of this fragment with respect to the whole datagram. It is the offset of the data in the original datagram measured in units of 8 byte



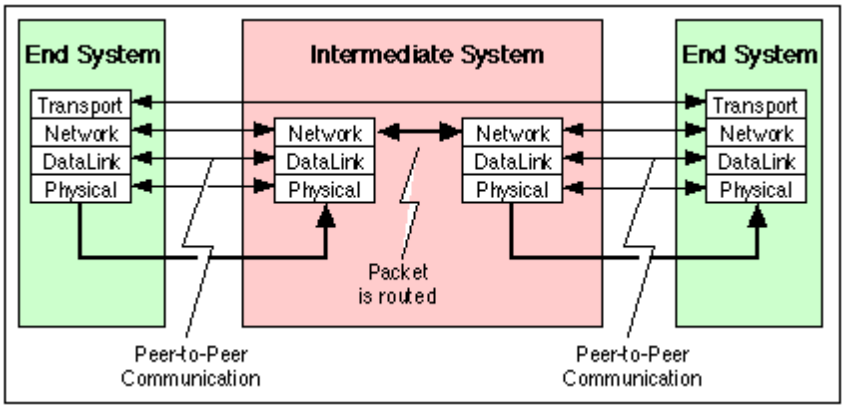
25. a) Write about transport layer fuctions.

ANS: Transport layer functions and protocol

Transport Layer Protocol:

The transport layer is the fourth layer of the OSI reference model. It provides transparent transfer of data between end systems using the services of the network layer (e.g. IP) below to move PDUs of data between the two communicating systems.

The transport service is said to perform "peer to peer" communication, with the remote (peer) transport entity. The data communicated by the transport layer is encapsulated in a transport layer PDU and sent in a network layer SDU. The network layer nodes (i.e. Intermediate Systems (IS)) transfer the transport PDU intact, without decoding or modifying the content of the PDU. In this way, only the peer transport entities actually communicate using the PDUs of the transport protocol.



Two End Systems connected by an Intermediate System (in this case a router) The figure shows the various protocol layers drawn with reference to the OSI reference model

The transport layer relieves the upper layers from any concern with providing reliable and cost effective data transfer. It provides end-to-end control and information transfer

with the quality of service needed by the application program. It is the first true end-to-end layer, implemented in all End Systems (ES).

The Internet Protocol (IP) Stack provides a set of transport layer protocols:

Functions of Transport Layer:

The transport layer protocols are primarily responsible for

- **End-to-End application data delivery** between the source and destination computers using the underlying unreliable best-effort IP based networks. It provides either a byte stream or message based service to the application layer protocols. On the sending side, application data is split into a byte stream or into a series of message blocks, a transport layer header added and then transport layer segments are sent to the underlying IP layer in the sending node, to be delivered to the network. Once the IP network delivers the transport layer segments to the receiving machine, the transport layer process at the receiving machine processes the transport headers for reliability, flow and error controls and then hands over the application data to the appropriate application process.

- **Application layer protocol Multiplexing/ Demultiplexing** for multiple applications communicating between end nodes. Multiplexing/ Demultiplexing is provided using transport layer port numbers for providing multiple services like Email, Web browsing, file transfer over the same IP stack implementation on end nodes. For example, HTTP uses the reserved TCP port number 80, SMTP uses the reserved TCP port number 25, FTP control connection uses the reserved port number 21 etc. Similarly, DNS uses the reserved UDP port number 53, SNMP uses the reserved UDP port numbers 161 and 162. Normally, the transport layer header contains fields named as source port number and destination port number to uniquely identify the sending and the receiving processes respectively.

- **End-End Reliability** for making sure that every byte of sender's application data reaches the receiver's application, in order, in spite of travelling over a wide variety of unreliable telecommunication links. Reliability is taken care by using mechanisms like checksums, sequence numbers, acknowledgement numbers, timeouts and retransmissions.

- **End-End Flow control** for making sure that the sender sends data at a rate that the receiver can process and store**.** This is usually achieved by the receiver advertising its current receiver buffer size continuously to the sender.

- **End-End Congestion control** for making sure that the sender does not introduce congestion in the intermediate network links and router buffers. Mechanisms like feedbacks from intermediate routers/receiver and monitoring receiver packet loss are used for controlling the sender rate so as not to congest the network links and router buffers.

- **Provides unique communication end points in the form of Sockets** for applications to use the Networking stack of the machine to communicate externally

- TCP, UDP are the most popular transport layer protocols

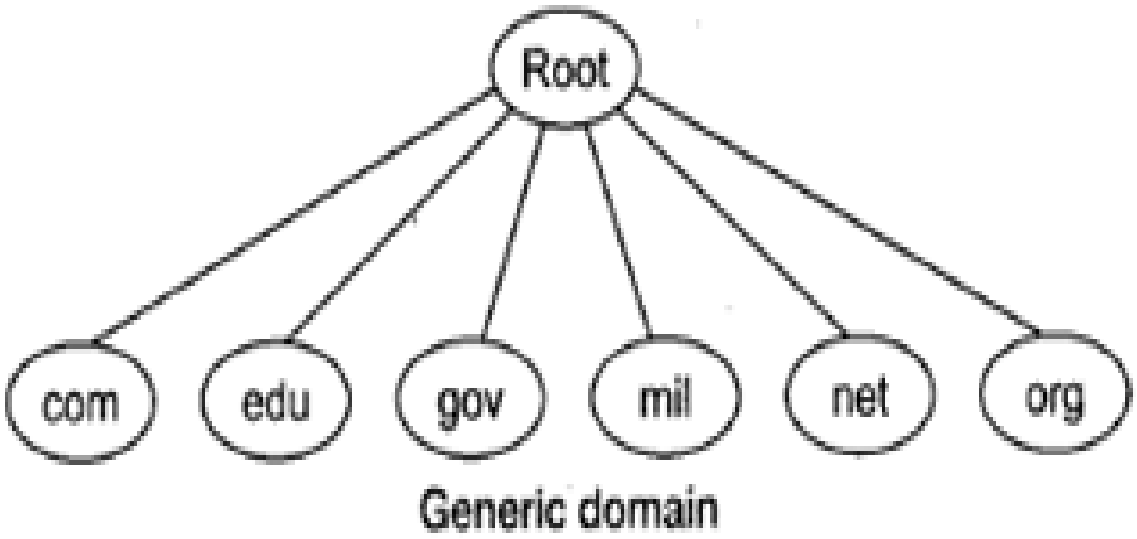
Note: Reliability, Flow control and congestion control are supported only in TCP and not in UDP.

(OR)

b)Write about overview of DNS

ANS: Domain Name System (DNS):

- To identify an entity, TCP/IP protocol uses the IP address which uniquely identifies the connection of a host to the Internet.
- DNS is a hierarchical system, based on a distributed database, that uses a hierarchy of Name Servers to resolve Internet host names into the corresponding IP addresses required for packet routing by issuing a DNS query to a name server.
- However, people refer to use names instead of address. Therefore, we need a system that can map a name to an address and conversely an address to name.
- In TCP/IP, this is the domain name system.
- DNS in the Internet: DNS is protocol that can be used in different platforms.
- Domain name space is divided into three categories.
- **Generic Domain:** The generic domain defines registered hosts according, to their generic behaviour. Each node in the tree defines a domain which is an index to the domain name space database.



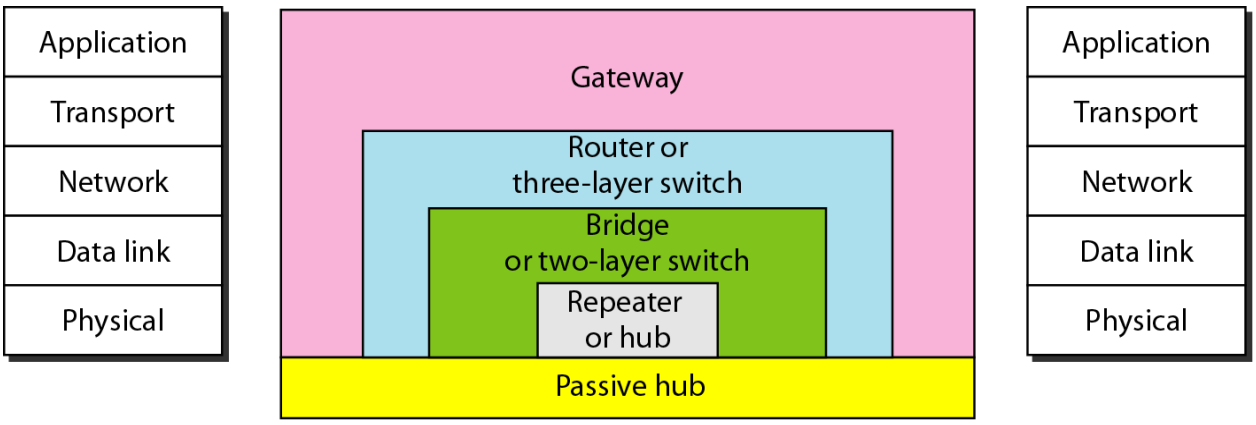
- **Country Domain:** The country domain section follows the same format as the generic domain but uses 2 characters country abbreviations (e.g., US for United States) in place of 3 characters.

Inverse Domain: The inverse domain is used to map an address to a name

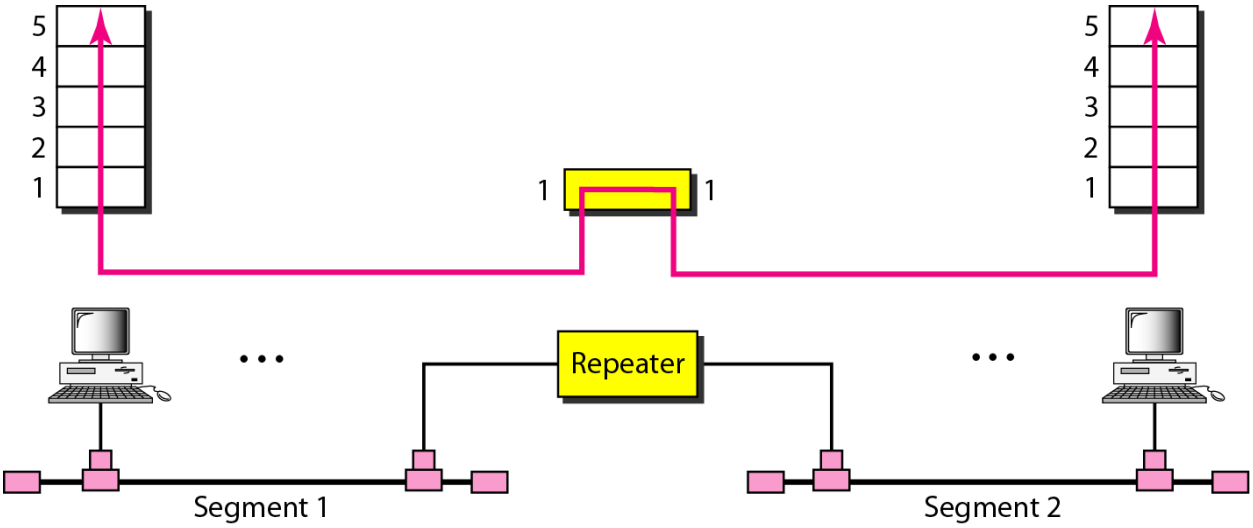
26. a) Write about the connecting LANS in detail

ANS: Connecting LANs, Backbone Networks, and Virtual LANs

Five categories of connecting devices

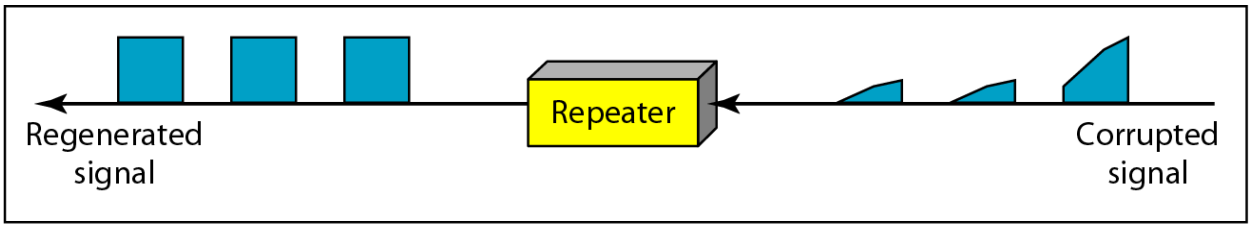


A repeater connecting two segments of a LAN

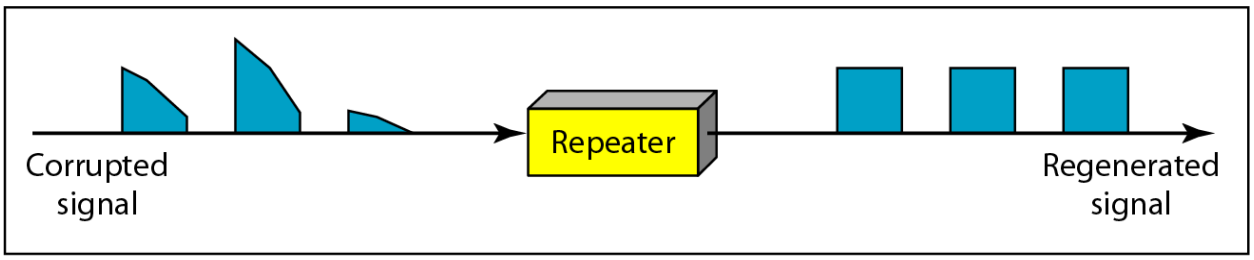


A repeater connects segments of a LAN.
A repeater forwards every frame – there is no filtering.
A repeater is a regenerator, not an amplifier.

Function of a repeater

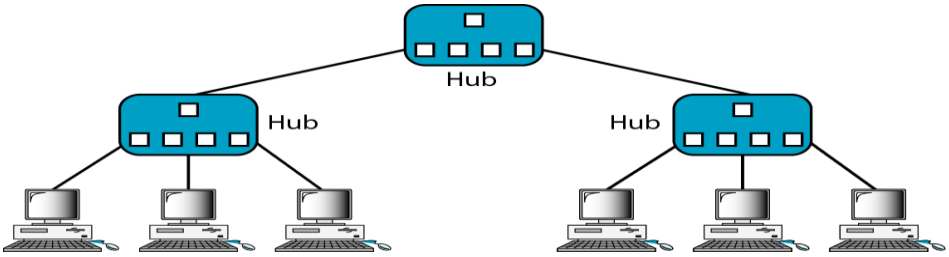


a. Right-to-left transmission.



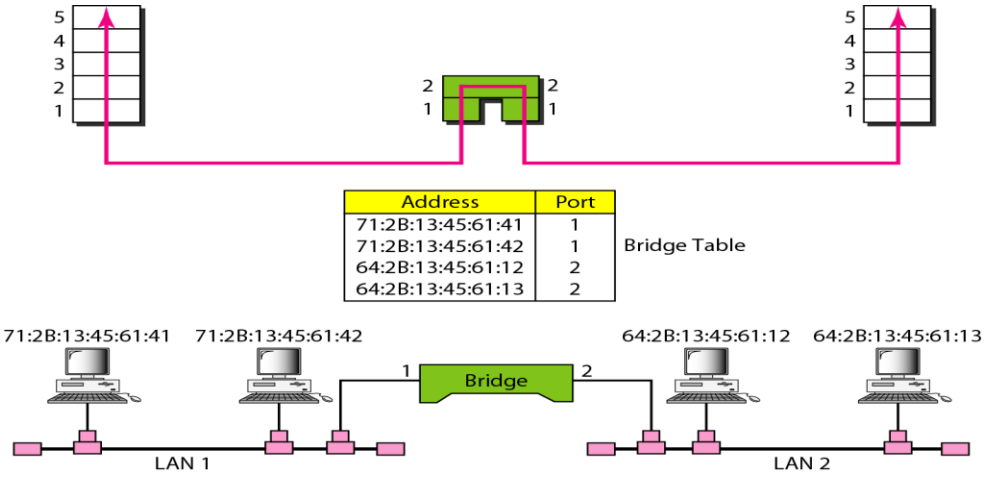
b. Left-to-right transmission.

A hierarchy of hubs



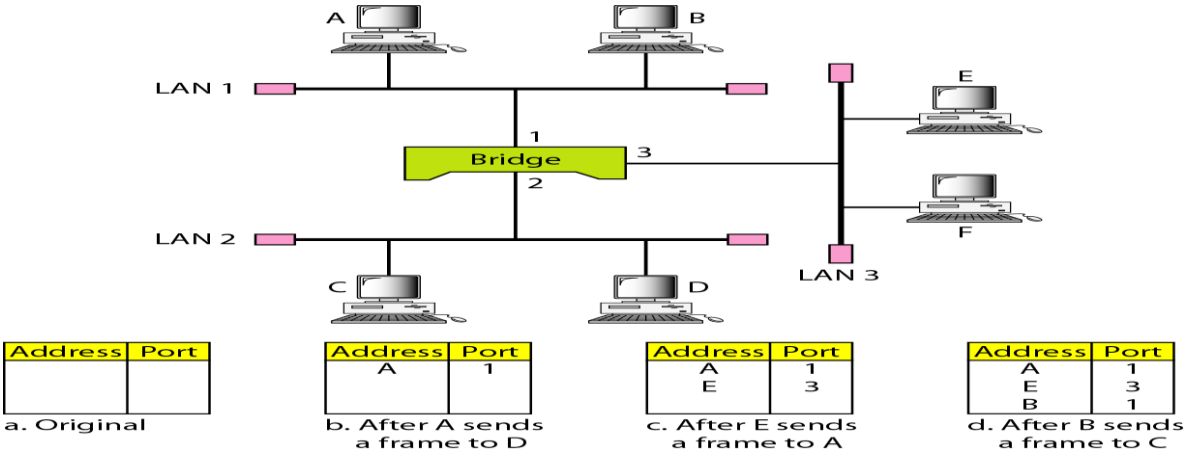
A hub is a multi-port repeater, used in star-wired LANs (Ethernet).
Because of the amount of traffic and collisions, hubs can only be used in small network configurations.
A bridge has a table used in filtering decisions.

A bridge connecting two LANs

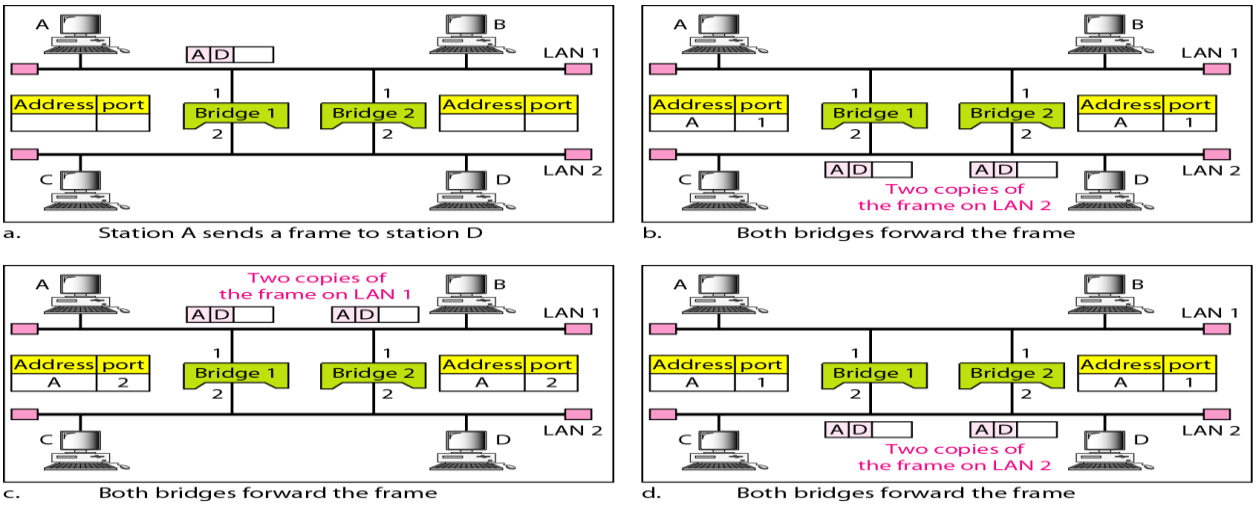


A bridge does not change the physical (MAC) addresses in a frame

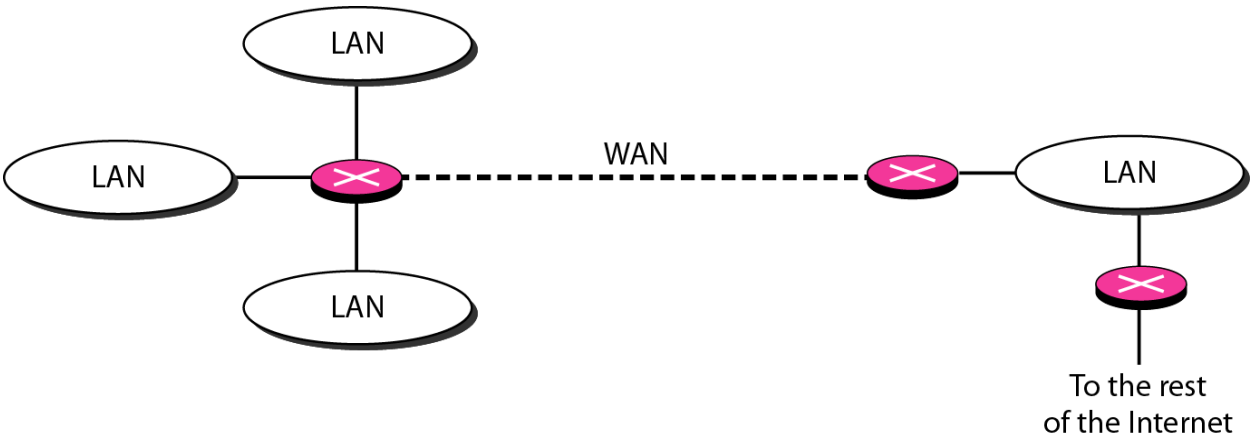
A learning bridge and the process of learning



Loop problem in a learning bridge



Routers connecting independent LANs and WANs



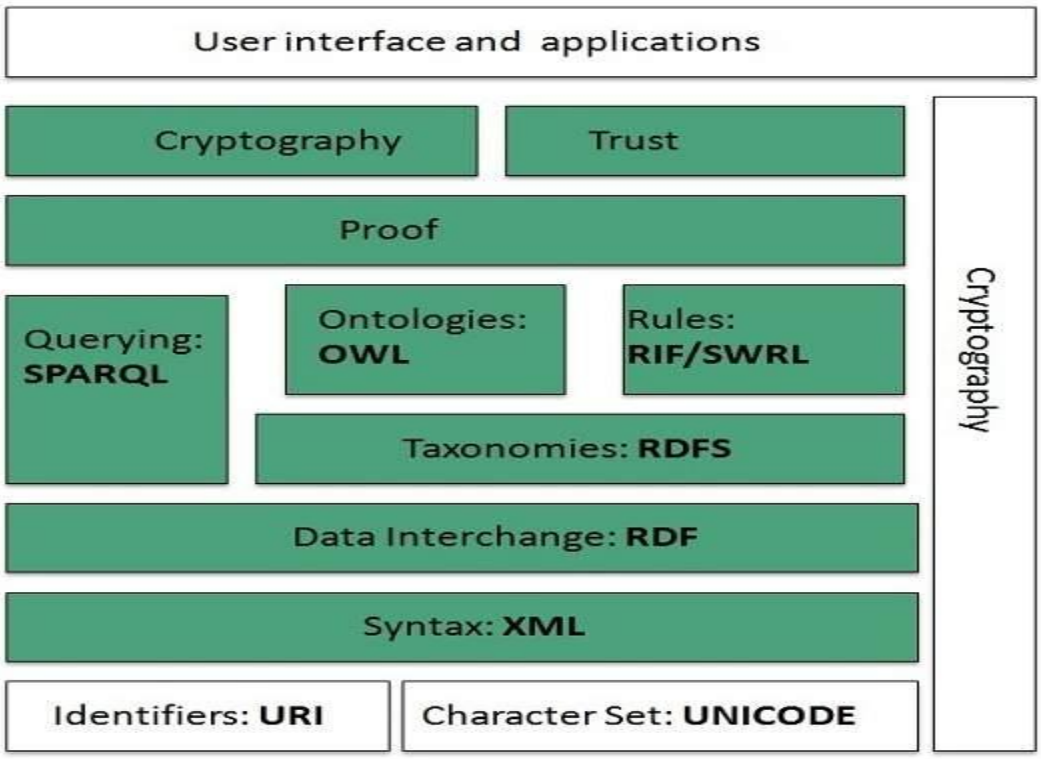
.(OR)

b) Write about the architecture of WWW.

ANS:

WWW Architecture

WWW architecture is divided into several layers as shown in the following diagram:



Identifiers and Character Set:-

Uniform Resource Identifier (URI) is used to uniquely identify resources on the web and **UNICODE** makes it possible to built web pages that can be read and write in human languages.

WWW Operation:-

WWW works on client- server approach. Following steps explains how the web works:

1. User enters the URL of the web page in the address bar of web browser.
2. Then browser requests the Domain Name Server for the IP address corresponding to www.tutorialspoint.com.

3. After receiving IP address, browser sends the request for web page to the web server using HTTP protocol which specifies the way the browser and web server communicates.

4. Then web server receives request using HTTP protocol and checks its search for the requested web page. If found it returns it back to the web browser and close the HTTP connection.

5. Now the web browser receives the web page, It interprets it and display the contents of web page in web browser's window.