GATEFLIX

COMPUTER NETWORKS

For
COMPUTER SCIENCE

COMPUTER NETWORKS

Syllabus

Concept of layering. LAN technologies (Ethernet). Flow and error control techniques. IPv4/IPv6, routers and routing algorithms (distance vector, link state). TCP/ UDP and sockets, congestion control. Application layer protocols (DNS, SMTP, POP, FTP, HTTP). Network security: authentication, basics of public key and private key cryptography, digital signatures and certificates, firewalls. Basics of Wifi & switching, Digital signals.

ANALYSIS OF GATE PAPERS

Exam Year	1 Mark Ques.	2 Mark Ques.	Total
2003	2	3	8
2004	3	4	11
2005	5	2	15
2006	1	5	11
2007	2	6	14
2008	1	4	9
2009	-	5	10
2010	2	3	8
2011	2	2	6
2012	3	3	9
2013	3	2	7
2014 Set-1	2	3	8
2014 Set-2	3	2	7
2014 Set-3	3	3	9
2015 Set-1	4	2	8
2015 Set-2	2	3	8
2015 Set-3	2	3	8
2016 Set-1	2	4	10
2016 Set-2	3	4	11
2017 Set-1	2	3	8
2017 Set-2	1	2	5
2018	3	4	7

CONTENTS

Topics		Page No
1.	**ISO OSI PHYSICAL LAYER, LAN TECHNOLOGIES**	
1.1	Introduction	01
1.2	Computer Networks	01
1.3	Design Issues of Layers	01
1.4	Network Hardware	02
1.5	Network Topology	03
1.6	Transmission Mode	07
1.7	Reference Models	**07**
1.8	Functions of the Layer	08
1.9	TCP/IP References Model	10
1.10	Comparison of OSI and TCP/IP Reference Models	12
1.11	Physical Layer	13
1.12	Transmission Media	13
1.13	Coaxial Cable	16
1.14	Optical Fiber	17
1.15	Maximum Date Rate of the Channel	19
1.16	Communication Satellite	19
1.17	Access Algorithms	21
1.18	Manchester Encoding	22
1.19	LMR (Last Minute Revision)	22
	Gate Questions	24
2.	**DATALINK LAYER AND SWP**	
2.1	Introduction	35
2.2	Data Link Layer Design Issue	35
2.3	Error Detection Correction	39
2.4	Error Correcting Codes	40
2.5	Data Link Protocols	50
2.6	IEEE LAN Standards	54
2.7	LLC Protocol	55
2.8	ALOHA	57
2.9	IEEE 802.3 and Ethernet	59
2.10	LMR (Last Minute Revision)	62
	Gate Questions	66
3.	**NETWORK AND TRANSPORT LAYER**	
3.1	Introduction	76
3.2	Switching Networks	76
3.3	Congestion Control	83

3.4	Bridges	87
3.5	Internetworking Devices	89
3.6	IP Addressing	96
3.7	Inter Networking Protocol (IPv4) Format	98
3.8	IPv6 Addressing	99
3.9	Routing Protocol	100
3.10	Introduction to Transport Layer	102
3.11	Duties of the Transport Layer	102
3.12	Connection	105
3.13	OSI Transport Protocol	106
3.14	Addressing	108
3.15	Multihomed Device	111
3.16	Subnetting and Supernetting	113
3.17	IP Datagrams and Routing	114
3.18	Internet Protocol	116
	Gate Questions	129

4. APPLICATION LAYER AND NETWORK SECURITY

4.1	Session Layer	154
4.2	Presentation Layer	155
4.3	Application Layer	163
4.4	Digital Signatures	165
4.5	Firewalls	166
4.6	Standard Common Applications	166
4.7	POP3 (Post Office Protocol)	171
4.8	IMAP (Interactive Mail Access Protocol)	172
4.9	DMSP (Distributed Mail System Protocol)	172
4.10	LMR (Last Minute Revision)	172
	Gate Questions	174

ASSIGNMENT QUESTIONS 190

1 ISO, OSI PHYSICAL LAYER, LAN TECHNOLOGY

1.1 INTRODUCTION

A Network is a set of devices (often referred to as nodes) connected by media links. A node can be a computer, printer, or any other devices capable of sending and / or receiving data generated by other nodes on the network. The links connecting the devices are called communications channels. E.g. fiber optic link, satellite link.

1.2 COMPUTER NETWORKS

Computer network means an interconnected collection of autonomous computers capable of having interconnections with each other. Computer network are generally organized as a series of layers or levels, each one built upon the one below it.

1.2.1 DESIGN ISSUES OF LAYERS

- Every layer needs a mechanism for identifying senders and receivers. A mean should be there for a process on one machine to specify with whom it wants to talk.
- Design decisions should concern the rules for data transfer. It can either be simplex or half- duplex or full – duplex communication.
- Error control is an important issue and any error – detecting or correcting codes must be known on both ends of the connections. Protocol that make explicit for the receiver to allow the pieces to be put back together properly.

An issue that occurs at every level is how to keep, a fast sender from swapping a slow receiver with data. Issue that allows an arbitrarily long message to get accepted by the processes is, when there are multiple paths between source and destination, a route must be chosen. Sometimes this decision spilt over two or more layers.

1.3 NETWORK HARDWARE

The physical devices that are used to establish and maintain the network are said to be Network Hardware. In addition to computers, Network hardware includes NIC, Hub, Switch, Router, Bridge and Gateway.

Network Interface Card: It gives minimum eligibility for the nodes to be in networks. It can exist in either H/w or S/w form. It operates typically at Physical Layer.

Repeater: It works like amplifier, i.e. It convert weak digital signal in to strong digital signal. It Operates at Physical Layer.

Hub: It is a broadcasting device. Hence it stands for Hybrid Universal Broadcast. It operates at Physical and Data link Layers. There are 2 types of hubs: Active and Passive. Passive Hub is Just a Hub but Active hub can do repeater functionality also.

Switch: It is a Uni casting device. There are two switch configurations: 2-layer and 3-layer. 2- Layer switch operates at Data link layer and 3-layer switch operates at Network layer.

Router: It is to calculate the optimal route among network nodes. It operates at network and transport layers.

Bridge: It is a forwarding device, used to connect two or more LANs or network segments. It operates at Data Link Layer. There are 3 types of bridges: Simple, Learning and Multi Port.

Gateway: It is used as intermediate between two or more dissimilar networks. It is capable to convert one protocol format to another. It operates at all the layers.

NOTE: Network Hardware, further discussed in detail in Chapter 4.

1.4 TYPES OF COMPUTER NETWORKS

1.4.1 LOCAL AREA NETWORKS (LAN)

Local area networks (LAN) are privately – owned networks within a single building or campus of up to a few kilo meters in size e.g. Networks within IIT campus.

1.4.2 METROPOLITAN AREA NETWORK (MAN)

Metropolitan area network (MAN) is basically a bigger version of a LAN and can support both data and voice. It covers a group of nearby corporate offices or a city and might be either private or public. E.g. Network connecting all IITs

1.4.3 WIDE AREA NETWORK (WAN)

Wide area network (WAN) spans large geographical area, often a country or continent. It contains a collection of machines intended for running user programs. In most wide area network, the subnet consists of two distinct components: transmission lines and switching elements. Transmission lines move bits between machines. They can be made of copper wire, optical fiber, or even radio links. Switching elements are specialized computers that connect three or more transmission lines. When data arrive on an incoming line, the switching element must choose an outgoing line on which to forward them. These switching computers have been called by various names in the past; the name router is now most commonly used.

1.4.4 SYSTEM AREA NETWORKS (SAN)

Another kind of network that we need to be aware of is SANs (system area networks). SANs are usually confined to a single room and connect the various components of a large computing system. For example, HiPPI (High Performance Parallel Interface) and Fiber Channel are two common SAN technologies used to connect massively parallel processors to scalable storage server and data vaults. (Because they often connect computers to

storage servers, SANs are sometimes defined as storage area network s). e.g. Organization connected worldwide.

1.4.5 LINE CONFIGURATION

Line configuration refers to the way two or more communication devices attach to link. There are two possible line configurations:

i) Point- to - Point

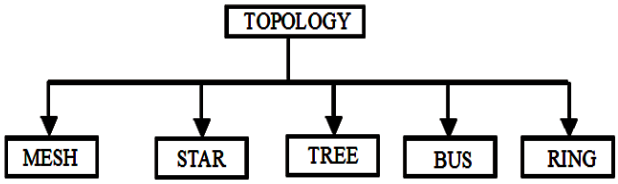
A point–to–point line configuration provides a dedicated link between two devices.

ii) Multi point

A multiport line configuration is one in which more than two specific devices share a single link.

1.5 NETWORK TOPOLOGY

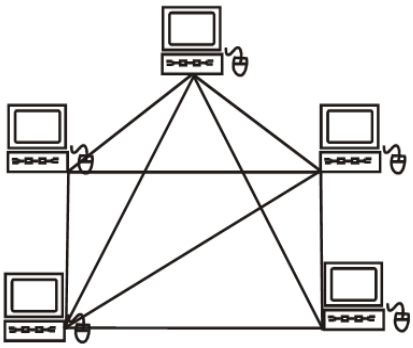
Topology refers to the way a network is laid out, either physically or logically. Two or more devices connect to a link, and then these two or more links form a topology.



The topology of a network is the geometric representation of the relationship of all the links and linking devices (usually called nodes) to each other. Topology is the relative status of the devices to be linked. It can either be peer- to –peer, where the devices share the link equally or primary – secondary, where one devices controls traffic and the others must transmit through it.

1.5.1 MESH

In a mesh topology, every device has a dedicated point – to – point link to every other devices. The term dedicated means that the link carries traffic only between the two devices it connects. Entire bandwidth is utilized by those two nodes. A fully connected mesh network having n devices has n (n-1)/2 physical channels. Thus, every device on the network must have (n-1) input/output (I/O) ports.



Advantages

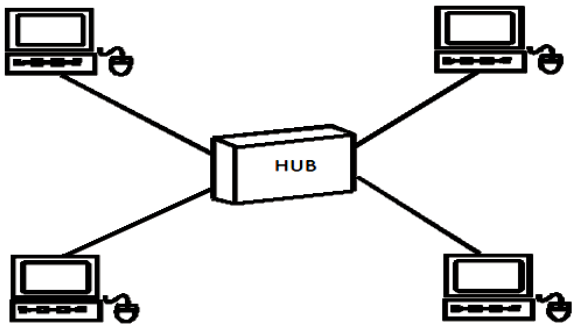
Guarantees that each connection carry its own data load, thus eliminating the traffic problems that can occur when links shared by multiple devices. If one link becomes unusable, it does not affect the entire system. Thus robust It guarantees privacy or security.

Disadvantages

As every device must be connected to every other device, installation and reconfiguration are difficult. The sheer bulk of the wiring can be greater than the available space. The hardware required to connect each link (I/O port and cable) can be prohibitively expensive.

1.5.2 STAR

In star topology, each device has a dedicated point – to – point link only to a central controller, usually called a hub. Thus the devices are not directly linked to each other. If one device wants to send data to another, it sends the data to the controller, and the relay the data to the other connected device.



Advantages

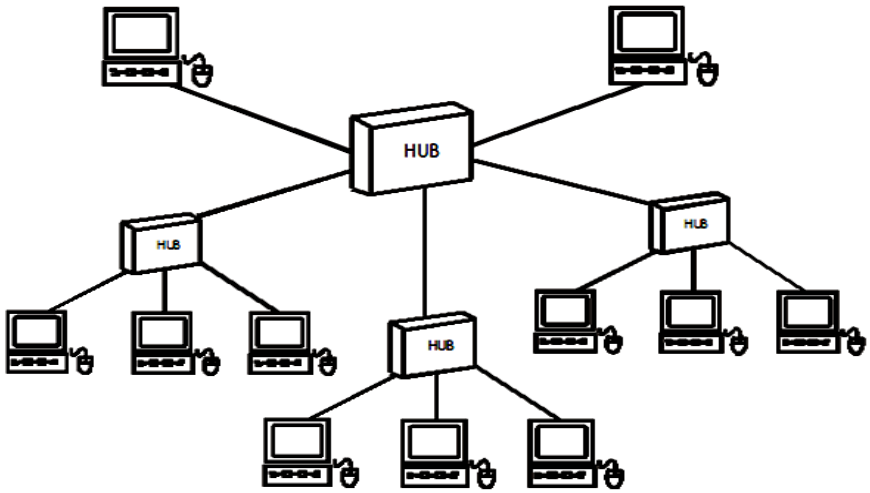
Less expensive
Easy to install and reconfigure
Less cabling
Robustness
Easy fault identification and fault isolation.

Disadvantages

More cabling is required than some other topologies (such as tree, ring or bus)
If hub fails, entire network goes down.

1.5.3 TREE

Nodes in a tree are linked to a central hub that controls the traffic to the network.
Not every devices plug directly into the central hub. The majority of devices cannot to a secondary hub that in turn is connected to the central hub. The central hub in the tree is an active hub, which contains a repeater (a hardware devices that regenerators the received bit pattern before sending them out). The secondary hubs may be active or passive hubs. Passive hub provides a simple physical connection between the attached devices.



Advantages

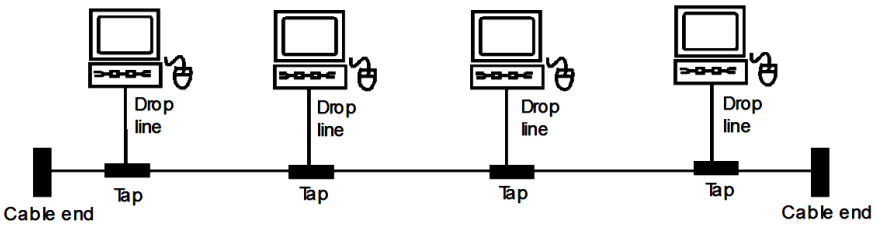
Allow more devices to be attached to a single central hub and therefore increase the distance a signal can travel between devices. It allows the network to isolate and prioritize communication from different computers.

Disadvantage

Not Robust, if central hub goes down whole system will be affected. More cabling required as compared to bus or ring topology.

1.5.4 BUS

In bus topology one long cable acts as a background to link all the devices in the network. Nodes are connected to the bus cable by drop lines or tabs. A drop line is a connection running between the devices and the main cable. As a single travels along the backbone, some of its energy is transformed into heat. (So, it becomes weaker and weaker the faster it has to travel).Thus there is a limit on the number of taps a bus can support and on the distance between those tabs.



Advantages

Ease of installation.
Uses less cabling than mesh, star or other topologies

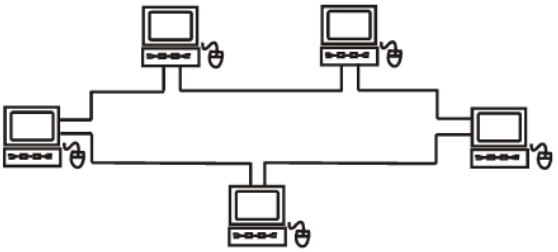
Disadvantages

Difficult reconfiguration and fault isolation. Signal reflection at the taps cause degradation in quality. A fault or break in the bus cable stops all transmission.

1.5.5 RING

Each device has a decided point- to- point line configuration only with the two devices on either side of it. A signal is passed along the ring in one direction, from devices to 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.

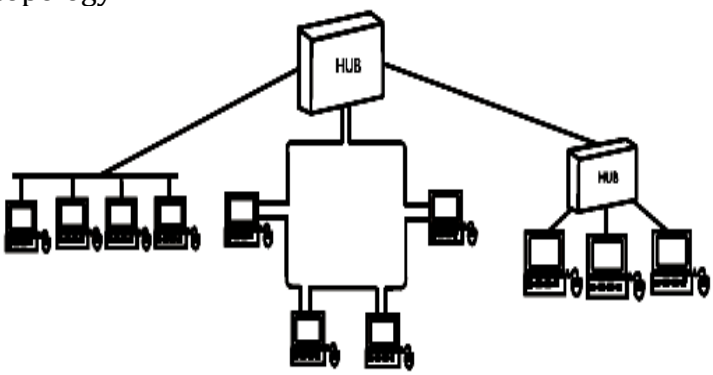


Advantages
Easy to install and reconfigure Fault isolation is simplified.

Disadvantages
A break in the ring can disable the entire network.
Fault identification is difficult.

1.5.6 HYBRID TOPOLOGY

Combination of several topologies of sub networks linked together in the larger topology, forms hybrid topology. Different topologies are connected to each other via a central controller in a star topology.



1.5.7 COMPARISON BETWEEN NETWORK AND RING NETWORK

Comparison Parameters	Bus Network	Ring Network
1.Topology	Broadcast	Point to Point
2. Throughput	Determined by the media and access control mechanism	Determined by media and capability of repeater.
3.Maximum distance	Low, because high bandwidth is require to support virtual channels	Total span is large, even though intermediable length is less.
4.Maximum number of stations	Number of new stations may be added as long as delay and throughput are not affected.	It is determined by system design.
5.Vulnerability to link or equipment failure	Has a signal point of failure, which may take system vulnerability.	It is vulnerable to single break in any node or repeater.
6. Message delay	Increase with no. of stations and volume of traffic.	Increase with number of stations.
7. Cost	Cost per node is higher	Is less compared to bus.

1.6 TRANSMISSION MODE

Transmission mode defines the direction of signal flow between two linked devices. It can either be simplex or half-duplex or full duplex.

1.6.1 SIMPLEX

In a simplex mode, the commutation is unidirectional. Only one of the two stations on a link can transmit, the other can only receive. Keyboards and traditional monitors are simplex deceives. The keyboard can only introduce input; the monitor can only accept output.

1.6.2 HALF-DUPLEX

In half- duplex mode, each stations can both transmit and receive, but not at the same time. When one deceive is sending, the other can only receive, and vice versa.
In a half-duplex transmission, the entire capacity of a channel is taken over by whichever of the two devices is transmitting at the time.

1.6.3 FULL-DUPLEX

Signal going in either direction share the capacity of the link. The sharing can occur in two ways, either the link contain two physically separate transmission paths, one for sending and the other for receiving or the capacity of the channel is divided between signals travelling in opposite directions. In a telephone network, when two people are communicating by a telephone line, both can talk and listen at the same time. Thus, it is Full-Duplex communication.

1.6.4 FULL- FULL DUPLEX

In this Mode, a node may send and receive at a time but from different nodes. i.e. A Node send to one node and receive from another node. Conference communication is example for Full – Full Duplex communication.

1.7 REFERENCE MODELS

1.7.1 THE OSI REFERENCE MODEL

The International Standard Organization (ISO) is a multinational body dedicated to worldwide agreement on international standard. An ISO standard that covers all aspects of network communication is **Open System Interconnection (OSI)** model. The purpose of OSI model is to open communication between different system without requiring change to the logic of the underlying hardware and software.

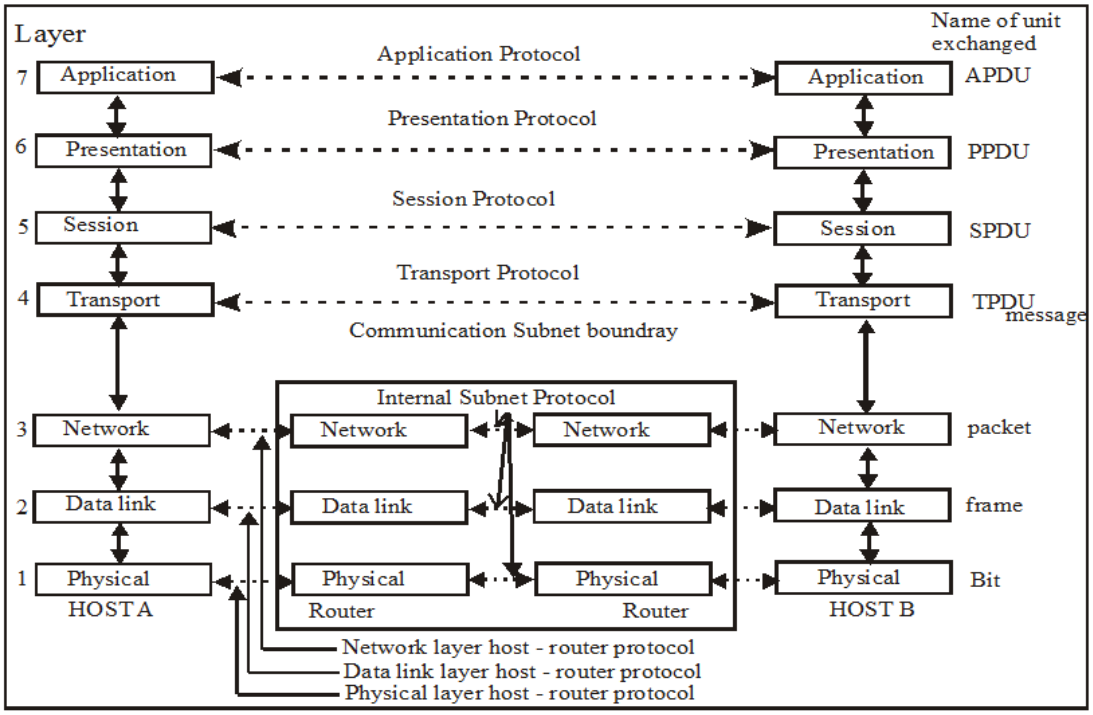
1.7.2 ORGANIZATION OF THE LAYERS

The open system interconnection model in a layered framework for the design of network system that allows communication across all types of computers systems. It consists of

seven separate but related layers each of which defines a segment of the process of moving information across a network.

The OSI model has seven layers. The principles that were applied to arrive at the seven layers can be briefly summarized as follows:

1. A layer should be created where a different abstraction is needed.
2. Each layer should perform a well defined function.
3. The function of each layer should be chosen with an eye toward defining internationally standardized protocols.
4. The layer boundaries should be chosen to minimize the information flow across the internationally.
5. The number of layers should be large enough that distinct functions need not be thrown together in the same layer out of necessity and small enough that the architecture does not become unwieldy.



1.8 FUNCTIONS OF THE LAYER

1.8.1 PHYSICAL LAYER:

The physical layer co-ordinates the functions required to transmit a bit stream over a physical medium. It deals with the mechanical and electrical specifications of the primary connections, such as cables, connections and signalling options that physically link two nodes on a network. It oversees the transmission of raw bits over a communications channel e.g. Hubs, Repeaters

1.8.2 DATA LINK LAYER

It accepts a data unit forms the third layer and adds meaningful bits to the beginning (header) and end (trailer) that contain address and control information. The data unit with this additional information is called a frame. The main task of the link layer is to transform a raw transmission facility into a line that appears free of undetected transmission error to

the network layer. It accomplishes this task by having the sender break up the input data frames (typically a few hundred or a few thousand bytes) and transmit the frames sequentially. If the service is reliable, the receiver confirms correct receipt of each frame by sending back an **acknowledgement frame.**
Another issue that arises in the data link layer (and most of the higher layers as well) is how to keep a fast transmitter from drowning a slow receiver in data. Some traffic regulation mechanism is often to let the transmitter know how much buffer space the receiver has at the moment. It oversees the node–to – node delivery of packets. Hence it provides flow control, error control and synchronization. e.g. Switches, Bridges

1.8.3 NETWORK LAYER

The network layer is concerned with controlling of the subnet.
It oversees source to destination delivery of a packet across multiple network links.
It provides source and destinations address in header.
It provides functions for routing and multiplexing.
It is also responsible for congestion control.
e.g. Routers

1.8.4 TRANSPORT LAYER:

The basic function of transport layer is to accept from session layer, split it up into smaller units if needed and pass these to the network layer.
It is responsible for source to destination delivery of the entire message.
It provides service point addressing i.e. delivery of a message to the appropriate applications on a computer running many applications.
It provides segmentation and reassembly and also responsible for congestion control.

1.8.5 SESSION LAYER

The session layer is the network dialog controller. It establishes maintains and synchronizes the interaction between communicating devices. e.g. It might manage an audio stream and video stream that are being combined in a teleconferencing application.
Specific responsibilities of session layer includes
i) Session management
ii)Synchronization
iii) Dialog control
iv) Graceful close of the session
v) Token management

1.8.6 PRESENTATION LAYER:

The presentation layer ensures interoperability among communication devices. It provides the necessary translation of data needed for the transmission and at receiver changing that format into the one that is understood by the receiver. It provides encryption and decryption for security purpose. It provides compression and decompression to make transmission more efficient. In particular presentation layer is concerned with the syntax and semantics of the information transmitted.

1.8.7 APPLICATION LAYER

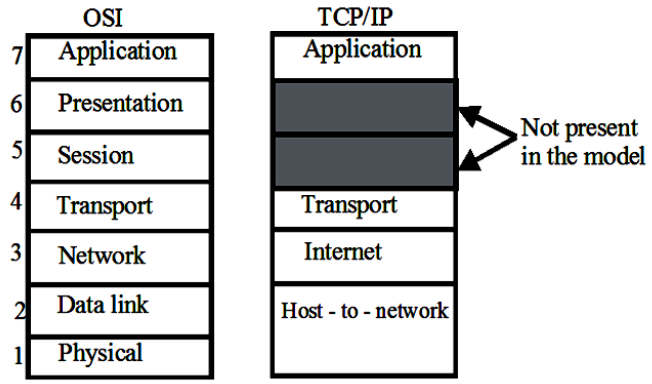
It is responsible to provide an application through which the end user (Sender / Receiver) may send or receive data.

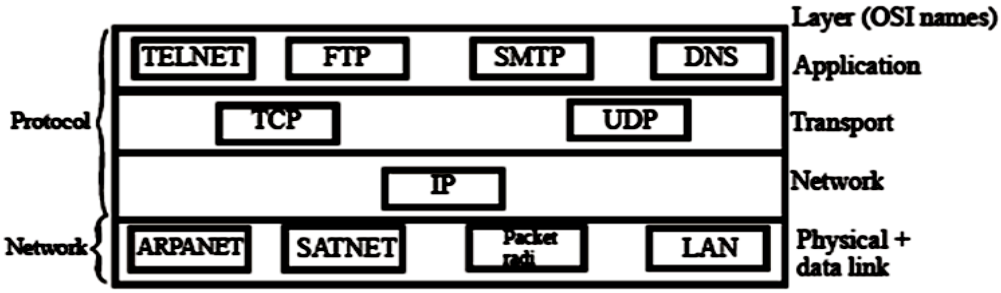
Layer	Layer Name	Header	Protocols/Services	Remember This
7	Application (All)	Protocol Data Unit	Telnet, FTP, SMTP, HTTP, File and Print,Email, (WWW),EDI	Where the user requests network services. This is not the applications, as in a program. This is database and application services.
6	Presentation (People)	Protocol Data Unit	JPEG, GIF, PICT, MIDI, MPEG, Quick Time	Decides how data is represented and translated. Data is formatted for "presentation" to the layers above and below. Encryption, compression and translation take place here.
5	Session (Seem)	Protocol Data Unit	RPC, ZIP, SCP, SQL,X Window, Net BIOS, NFS, ASP, DNA SCP	Establishes, maintains and manages communication sessions between computers. Dialog control occurs here.
4	Transport(To)	Segments	RPC, NBP, UDP, NCP,SPX, ADP, Windowing Flow control, synchronization	Provides reliable data segment transmission. Sets the stage for data disassembly and assembly, before and after transmission. Remember: end- to – end connectivity.
3	Network(Need)	Diagrams or Packets	IP, IPX, BooTP, DHCP, ICMP, BGP, OSPF, RIP.	If it has anything to do with routing to do with routing, this is where it happens. This layer determines how data will be routed across a network. Structure and logical (IP) addressing occurs at this layer. Routers operate here.
2	Data LinkSublayers are MAC and LLC (Data)	Frames	MAC, LLC, Frame Relay, LLPB, PPP, calculating CRC or FCS, controls access to the physical medium.	This layer is concerned with the links and mechanism that move data. Topology (Ether or Token Ring) is defined here. Switches (generally) and all bridges operate here. Remember: Framing.
1	Physical (Processing)	Bits(1s & 0s)	Ethernet, Token Ring, HSSI, 802.3, bit synchronization, physical connector specifications.	If it's on a network and you can touch it, it's here. This layer handles the electrical and physical specifications for network n\media that carry data bits across a network. Hubs, repeaters and multiplexers operate here.

1.9 TCP/IP REFERENCE MODEL

The **Transmission Control Protocol / Inter - networking Protocol (TCP/IP)** is a protocol suite, that defines how all transmission are exchanged across the internet. TCP/IP was designed after OSI model. The layers in the TCP/IP protocol suite do not match exactly with those in the OSI model. The TCP/IP protocol suite is made of five layers: Applications, transport, internet, host to network. Host to network is divided into (i) Data link (ii)

Physical. A network in a TCP/IP internet work can be a local area network (LAN), a metropolitan area network (MAN), or a wide area network (WAN)





1.9.1 FUNCTIONS OF THE LAYERS

1. Host to Network Layer

It consists of physical and Data Link Layer At the physical and DLL, TCP/IP does not define any specific protocols defined by the underlying networks.

2. Internet Layer

At the internet layer, TCP/IP supports the internet protocol (IP). IP contains four supporting protocols: ARP, RARP, ICMP, and IGMP. The Internet Protocol (IP) is the transmission mechanism used by the TCP/IP protocols. It is an unreliable and connectionless datagram protocol. IP transports data in packets called data grams, each of which is transported separately. Address resolution protocol (ARP) is used to translate the protocol address to an equivalent physical hardware address. Reverse address resolution protocol (RARP) is used to find IP address of the stations or node when its physical address is known. Internet control message protocol (ICMP) is a mechanism used by hosts and routes (gate ways) to send modifications of datagram problem back to the sender. Internet group message protocol (IGMP) is used to help simultaneous transmission of a message to a group of recipients.

3. Transport Layer

The transport layer is represented by two protocols: TCP and UDP. Both are responsible for delivery of a message from source applications to destination application. User datagram protocol (UDP) is a process to process protocol that adds only port addresses, checksum error controls. UDP is a connectionless protocol. UDP (User Datagram Protocol), is an unreliable, connectionless protocol for applications that do not want TCP's sequencing or flow control and wish to provide their own. It is also widely used for one-shot, client – server – type request – reply queries and applications in which promote delivery is more

important than accurate delivery, such as transmitting speech or video.The transmission control protocol (TCP) provides full transport layer services to application. TCP (Transmission Control Protocol) is a reliable connections oriented protocol that allows a byte stream originating on one machine to be delivered without error on any other machine in the internet.

It fragments the incoming byte stream into discrete message and passes each one on to the internet layer. At the destination, in the receiving TCP processes reassembles the received message into the output stream. TCP also handle flow control to make sure a fast sender cannot swamp a slow receiver with more messages that it can handle.

4. Applications Layer

Applications layer is equivalent to combined session, presentations and applications layer in the OSI model. It contains all the higher level protocols. The early ones includes virtual terminal (TELENET), file transfer (FTP), and electronic mail (SMTP). The virtual terminal protocol allows a user on one machine to log onto a distant machine and work there. The file transformer protocol provides a way to move data efficiently from one machine to another. Electronic mail was originally just a kind of file transfer, but later a specialized protocol (SMTP) was developed for it.

1.10 COMPARISON OF OSI AND TCP/IP REFERNCE MODLES

1.10.1 SIMILARITIES BETWEEN OSI AND TCP/IP:

Both OSI and TCP/IP reference models are based on the concept of a stack of independent protocols. In both models, the layers above transport are applications oriented users of the transport service. The service definition tells what the layer does, not how entities above it accessed it or how the layer works. Each layer performs some services for the layer above it.

A layer interface tells the processes above it how to access it. It specifies what the parameters are and what result to expect and nothing about how the layer works inside.

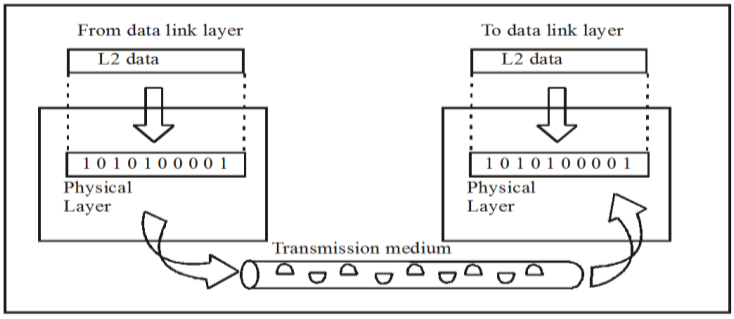
1.10.2 DIFFERENCE BETWEEN OSI AND TCP/IP REFERENCE MODELS:

The OSI reverences model was devised before the protocol were invented with TCP/IP, the protocols came first and the model was just a description of the existing protocols. The OSI model has seven layers and the TCP/IP has five layers. Both have network, transport and applications layers, but the other layers are different. The OSI model supports connection-oriented commutations in the network layer whereas TCP/IP model has only one mode in the network layer i.e. connectionless.

The OSI model has only connection- oriented communication in the transport layer whereas TCP/IP supports both connectionless and connection- oriented modes in the transport layer, giving the user a choice.

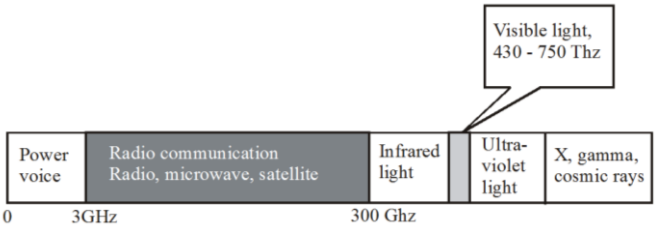
1.11 PHYSICAL LAYER

The physical layer coordinates the functional required to transmit a bit stream over a physical medium. It deals with the mechanical and electrical specifications of the primary connections such as cable, connectors and signalling options that physically link two nodes on a network.
The first layer receives a data unit from the second layer; put it into a format capable of being carried by a communications link.

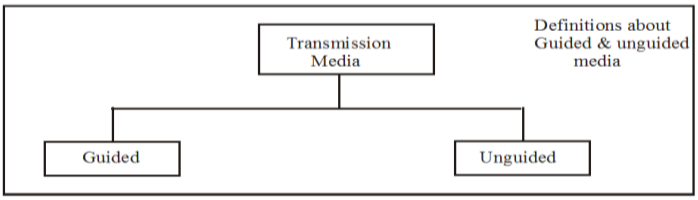


1.12 Transmission Media

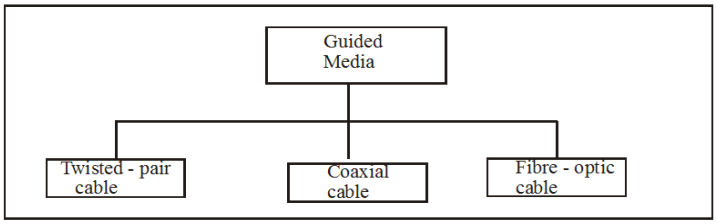
All telecommunication devices use signals to represent data. These signals are transmitted from one device to another in the form of electromagnetic energy.



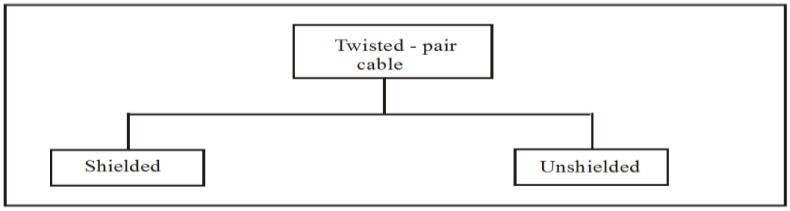
Transmission media can be divided as



1.12.1 Guided Media



1.12.2 Twisted-pair cable



1.12.3 Twisted Pair

The least expensive and most widely used guided transmission medium is twisted pair.

1.12.4 Physical Description

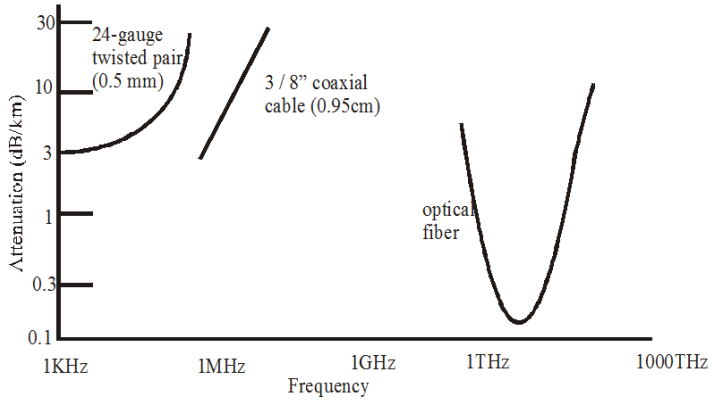
A twisted pair consists of two insulated copper wires arranged in a regular spiral pattern. A wire pair acts as a single communications link. Typically, a number of these pairs are bundled together into a cable by wrapping them in although protective sheath. Over longer distances, cables may contain hundreds of pairs. The twisting tends to decrease the crosstalk interference between adjacent pairs in a cable. Neighbors pairs in a bundle typically have somewhat different twist lengths to reduce the crosstalk interference. On long – distance links, the twist length typically varies from 5 to 15 cm. The wires in pair have thickness of from 0.4 to 0.9 mm.

1.12.4.1 Applications

By far the most common transmission medium for both analog and digital signals is twisted pair. It is the most commonly used medium in the telephone network and is the workhorse for communications within buildings.
In the telephone system, individual residential sets are connected to the local telephone exchange or "end office", by twisted pair wire. These are referred to as subscriber loops.

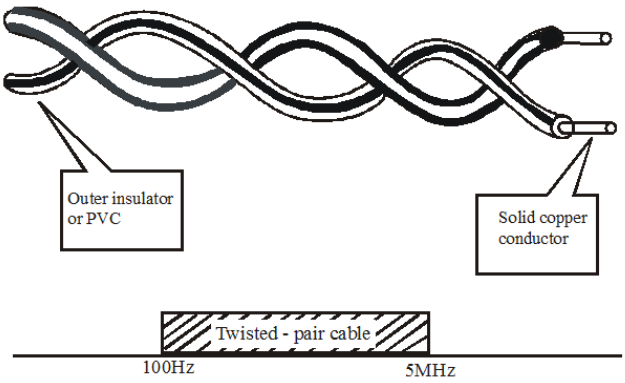
1.12.4.2 Transmission Characteristics

Twisted pair may be used to transmit both analog and digital transmission. For analog signals, amplifiers are required about every 5 to 6 km. For digital transmission (using either analog or digital signals), repeaters are required every 2 or 3 km. Compared to other commonly used guided transmission media (coaxial cable, optical fiber), twisted pair is limited in distance, bandwidth and data rate. As fig. shows, the attenuation for twisted pair is a very strong function of frequency. Twisted pair comes in two varieties
(1) Unshielded Twisted Pair (UTP) Cable
(2) Shielded Twisted Pair (STP) Cable



1.12.4.3 UNSHIELDED TWISTED – PAIR (UTP) CABLE

A twisted pair consists of two conductors (usually copper), each with its own colored plastic insulation. The plastic insulation is color- bundled for identification. Colors are used both to identify the specific conductors in a cable and to indicate which wires belong to pairs and how they relate to others pairs in a larger bundle.
Various categories of UTP cable



Category 1:

→ Used in telephone system

→ Quality is fine for voice but inadequate for all but low-speed data communication.

Category 2:

→ Suitable for voice and for data transmission of up to 4 Mbps

Category 3:

→ Standard cable for most telephone systems

→ Used for data transmission of up to 10Mbps

Category 4:

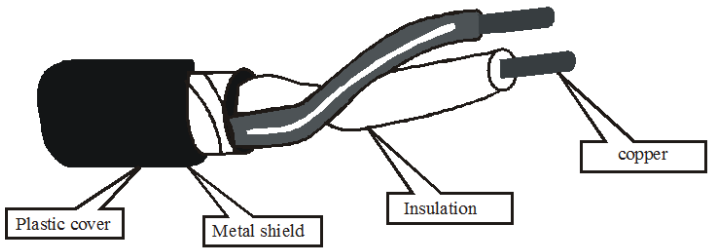
→ Should have at least three twists per foot per as well as other conditions to bring the possible transmission rate to 16 Mbps.

Category5:

→ Used for data transmission up to 100 Mbps

They are data similar to category 3 pairs, but with more twists per centimetre, which results in less crosstalk and a better quality signal over longer distances, making them more suitable for high-speed computer communication.

1.12.4.4 SHIELDED TWISTED-PAIR (STP) CABLE



Shielded twisted – pair (STP) cable has a metal foil covering that encases each pair of insulated conductors. This metal casing prevents the penetration of electronic noise.

1.12.4.5 ADVANTAGES OF TWISTED PAIR CABLE

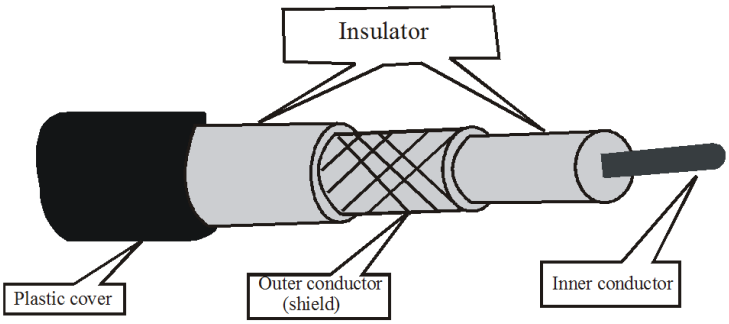
1. Low cost
2. Ease of use
3. Easy to Install
4. Used in LAN Technologies
5. Used on Ethernet and Token ring.

Table: Comparison of Shielded and Unshielded Twisted pair

Frequency (MHz)	Attenuation (dB per 100 m)			Near-end Crosstalk (dB)		
	Category 3 UTP	Category 5 UTP	150-ohm STP	Category 3UTP	Category 5UTP	150-ohm STP
1	2.6	2.0	1.1	41	62	58
4	5.6	4.1	2.2	32	53	58
16	13.1	8.2	4.4	23	44	50.4
25	-	10.4	6.2	-	41	47.5
100	-	22.0	12.3	-	32	38.5
300	-	-	21.4	-	-	31.3

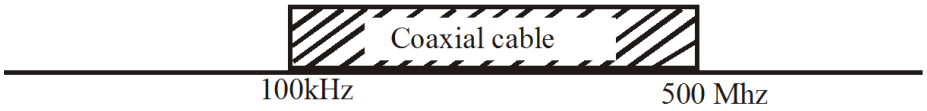
Crosstalk is the undesired effect of one circuit (or channel) on another circuit (or channel). Crosstalk occurs when one line picks up some of the signals travelling down another line.

1.13 COAXIAL CABLE



1.13.1 PHYSICAL DESCRIPTION

Coaxial cable has a central core conductor of solid or wire (usually copper) enclosed in an insulating sheath, which again is encased in an outer conductor of metal foil.



The outer metallic rapping works as
(i) Shield against noise.
(ii) Second conductor is to complete the Circuit. The outer conductor is enclosed in an insulating sheath and the whole cable is protected by a plastic cover.

1.13.2 APPLICATIONS

Coaxial cable is perhaps the most versatile transmission medium and is enjoying widespread use in wide variety of applications. The most important of these are as follows:
Television distribution Long distance telephone transmission Short – run computer system links Local area networks Coaxial Cable is also spreading rapidly as a means of distributing TV signal to individual homes – cable TV.
Coaxial cable is also commonly used for short range connections between devices. Using digital signalling, coaxial cable can be used to provide high-speed I/O channels on computer system.

1.13.4 TRANSMISSION CHARACTERISTICS

Coaxial cable is used to transmit both analog and digital signals. Coaxial cable has frequency characteristic those are superior to those of twisted pair and can hence be used effectively at higher frequencies and data rates. Because of its shielded, concentric construction, coaxial cable is much less susceptible to interfaces and crosstalk than twisted pair. The principal constraints on perform are attenuation, thermal noise, and intermediation noise. The latter is present only when several channels (FDM) or frequency bands are in use on the cable. For long distance transmission of analog signals, amplifiers are needed every few kilometres, with closer spacing required if higher frequencies are used. The usable spectrum for analog signalling extends to about 500 MHz. For digital singling repeaters are needed every kilometre or so, with closer spacing needed for higher data rates.

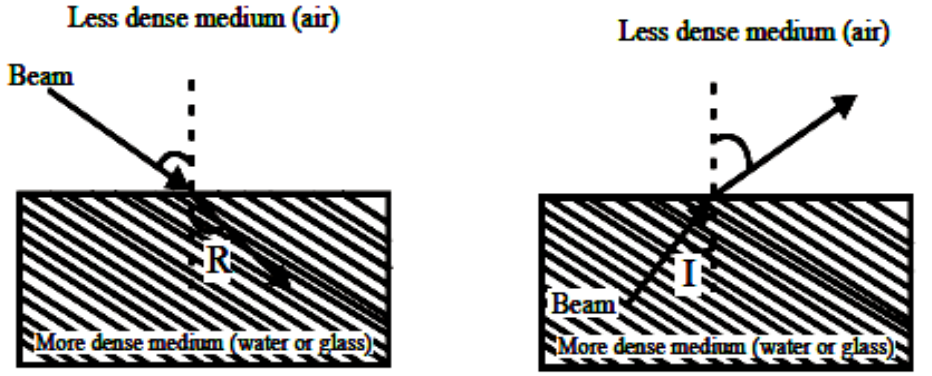
1.13.5 COAXIAL CABLE STANDARDS

Different coaxial cable designs are categorized by their radio government (RG) ratings. Each RG number denotes a unique set of physical specifications, including the wire gauge of the inner conductor, the thickness and type of the inner insulator, the construction of the shield and the size and type of the out casing. Each cable defined by the RG rating is adapted for a specialized function.RG-8 is used in thick Ethernet. RG–58 is used in thin Ethernet. RG-59 is used for TV.

1.13.6 ADVANTAGES

1) Coaxial cable is used for both data transmission i.e. analog and digital data transmission
2) It has higher bandwidth
3) Easy t handle and relativity inexpensive as compared t fiber optic cables.
4) It uses for longer distances at higher data rates.
5) Excellent noise immunity.

1.14 Optical Fiber

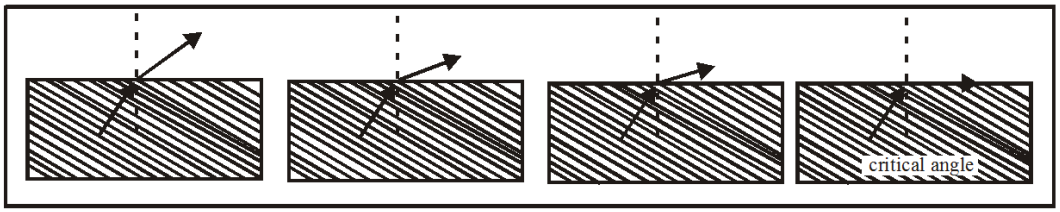


(a) From less dense to more dense medium (b) From more dense to less dense medium

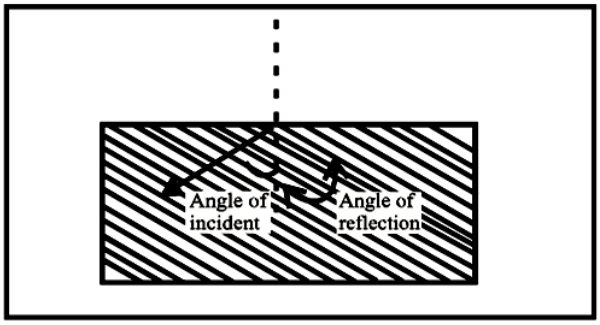
Optical fiber is made of glass or plastic and transmits signals in the form of light. The speed of light depends on the density of the medium through which it is traveling, the higher the density, the slower will be the speed. If a ray of light traveling through one substance suddenly enters into another (less or more dense) substance, its speed changes abruptly, causing the ray to change direction.

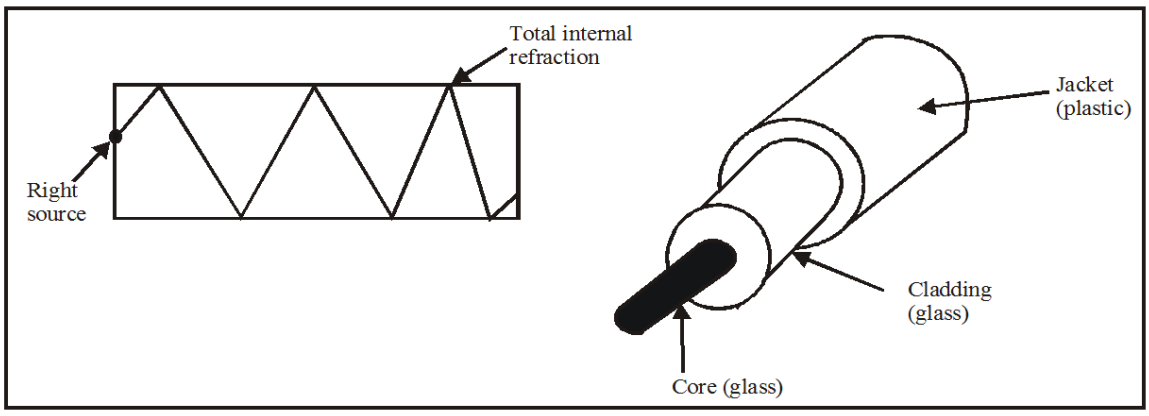
This change is called refraction. When light into a more dense medium, the angle of incidence is greater than the angle of refraction. When light travels into a less dense medium, the angle of incidence is less than angle of refraction. When a beam of light moves from a denser medium and as the angle of incidence increases, so does the angle of

refraction. The change in the incident angle results in a refracted angle of 90°. The incident at this point is known as the critical angle.



When the angle of incidence becomes greater than the critical angle, the angle of incidence is always equal to the angle of reflection. i.e. when the ray of light reflects off a surface, the angle of incidence is equal to the angle of reflection. Optical fiber is made of glass or plastic and transmits signals in the form of light.





1.14.1 PRINCIPAL ON WHICH FIBER CABLES WORK

When a light ray passes from medium to another, for example, from fused silica to air, the ray is reflected at the silica/air boundary. For angles of incidence above a certain critical value, the light is refracted back into the silica, none of it escapes into the air. Thus a light ray incident at or above the critical angle is trapped inside the fiber and can propagates for many kilo meters with virtually no loss.

1.14.2 CONSTRUCTION

At the center is the glass core through with the light propagates. In multimode fibers, the core is 50 microns in diameter and in case of single mode fibers it is 8 to 10 microns. The core is surrounded by a glass cladding with a lower index of reflection than the core, to keep all the light in the core. Next comes a thin plastic jacket to protect the cladding. Optical fibers main applications are long haul trunks, metropolitan trunks, etc.

Total Data Rate	2 gbps
Bandwidth	2 GHz

Repeater Spacing 10 to 100 km

1.15 MAXIMUM DATE RATE OF THE CHANNEL

1.15.1 NYQUIST THEOREM

Henry Nyquist proposed a theorem that has had profound effects on information theory as well as the practical design of data communication techniques involving digitalization of analog signal. Also original theorem was regarding analog signals and noiseless channels and later it was applied t digit signals. Nyquist proved that if an arbitrary signal has been run through a low pass filter of bandwidth H, the filtered signal can be completely reconstructed by making only 2H samples per second. If the signal consist of V discrete levels,
Nyquist's Theorem states:
Maximum data rate = $2\ H \log_2$ bits / sec.
e.g. A noiseless 3KHz channels cannot transmit binary signal at a rate exceeding 6000 bps.

1.15.2 SHANNON'S THEOREM

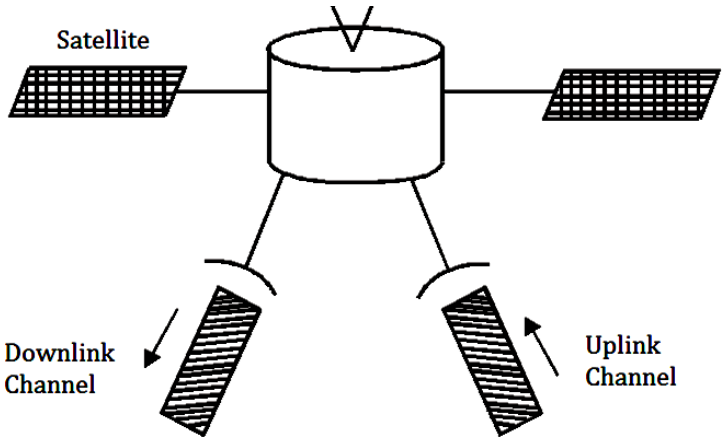
Shannon's major result is that the maximum data rate of a noisy channel whose bandwidth is H Hz, and whose signal – to – ratio is S/N, is given by,
Maximum number of bits/sec.$=H \log_2(1+S/N)$
Shannon's result was derived using information theory arguments and applied to any channel subject to Gaussian (thermal) noise.

1.15.3 TABLE: POINT – POINT TRANSMISSION CHARACTERISTIC OF GUIDED MEDIA

	Frequency Range	**Typically Attenuation**	**Typical Delay**	**Repeater spacing**
Twisted pair (with loading)	0 to 3.5 kHz	0.2 dB/ km @ 1 kHz	50 μs/km	2 km
Twisted pair (multi- pair cables)	0 to 1 MHz	3 dB / km @ 1 kHz	5 μs/km	2 km
Coaxial cable	0 to 500 MHz	7 dB / km @ 10 MHz	4 μs/km	1 to 9 km
Optical fiber	180 to 370 THz	0.2 to 0.5 dB/ km	5 μs/km	40 km

1.16 COMMUNICATION SATELLITE

In satellite based computer networks, communication between the nodes is accomplished using "radio frequencies".
A satellite based networks has a star topology, satellite being the central hub. If the hub fails the entire communication network comes to a standstill. In view of this reliability and redundancy considerations are important when designing satellites.



1.16.1 WORKING OF SATELLITE BASED COMPUTER NETWORKS

Communication satellites generally have up to a dozen or so transponders. Each transponder has a beam that covers some portion of the earth below it, ranging from a wide beam 10,000 km across to a spot beam only 250km across. Stations within the beam area can send frames to the satellite on the uplink frequency.
The satellite then red broadcasts them on the downlink frequency. Different frequencies are used for uplink and downlink to keep the transponder from going into oscillation. Satellites that do no – board processing, but just echo whatever they hear are often called bend-pipe satellite. Each antenna can aim itself at some area, transmit some frames, and then aim to a new area. Aiming is done electronically, but still takes some number of microseconds.

1.16.2 PROTOCOLS: (CHANNELS ALLOCATION ALGORITHMS)

Just as with LAN's one of the key design issue is how to allocate the transponder channels. However, unlike LAN's, carrier sensing is impossible due to the 270 msec propagation delay. Hence the need for other protocols. Five classes of protocols are used on the multiple accesses (up link) channel: polling, ALOHA, TDM, CDMA and FDM.

1.16.3 POLLING

The traditional way to allocate a signal channel among competing users is for somebody to poll them, Having the satellite poll each station in turn to sec if it has a frame is prohibitively expensive, given the 270 m sec time required for each poll / response sequence. However, if all the ground stations are also tied together to a (typically low bandwidth) packet – switching network, a minor variations of this idea is conceivable. The idea is to arrange al the stations in a logical ring, so each station known its successor. Around this terrestrial ring circulates a token. The satellite never sees the token. A station is allowed to transmit on the uplink only when it has captured the token. If the number of stations is small and constant, the token transmission time is short and the burst sent to the uplink channel are much longer than the token rotation time, scheme is moderately efficient.

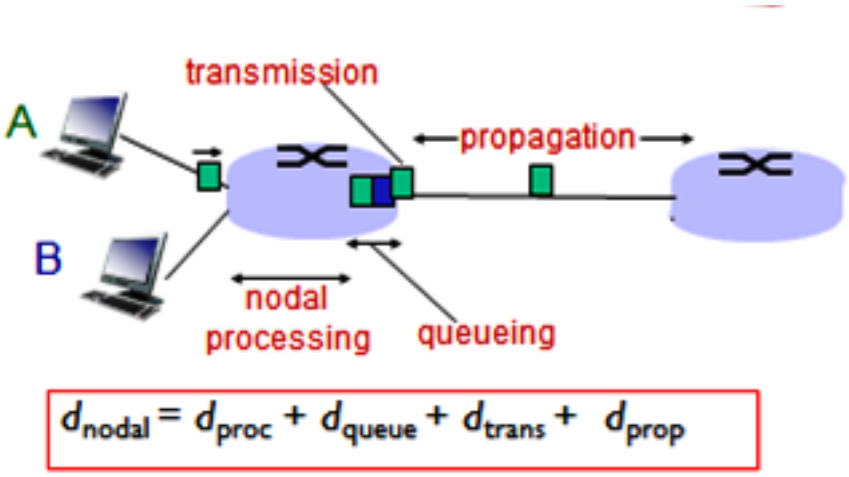
1.16.4 ACCESS ALGORITHMS

ALOHA
Two versions of ALOHA are:
(i) Pure ALOHA
(ii)Slotted ALOHA
Using slotted ALOHA doubles the efficiency but introduces the problem of how synchronize all the stations so they know when each time slot beings. Fortunately, the satellite itself holds the answer, since it is inherently a broadcast medium. One ground station, the reference station, periodically transmits a special signal whose rebroadcast is used by all the stations as the time origin. If the time slots all have length ΔT, each station now knows that time slot k beings at a time $k\Delta T$ after the time origin. Since clocks runs at slightly different rates, periodic resynchronization is necessary to keep everyone in one.

1.17 DELAYS IN NETWORKS

The time required for a packet to send from one node to another is known as network delay. It is Composition of 4 types of delays:

- Queuing Delay : Time to wait in queue
- Processing Delay : Time for appending or verifying control fields
- Transmission Delay: Time to load the packet into channel
- Propagation Delay: Time to reach the destination.



$$d_{nodal} = d_{proc} + d_{queue} + d_{trans} + d_{prop}$$

In the above delays, in general Queuing delay and processing delays are minimum, so, can be neglected.

Hence, **Nodal delay / Network delay=Transmission Delay + Propagation Delay**

Whereas, **Transmission delay = Packet size / bandwidth**
Propagation delay=Length / Speed

In LANs, the distance between the nodes is less and speed of propagation is relatively more. So, Propagation delay will be less than or equal to Transmission Delay.

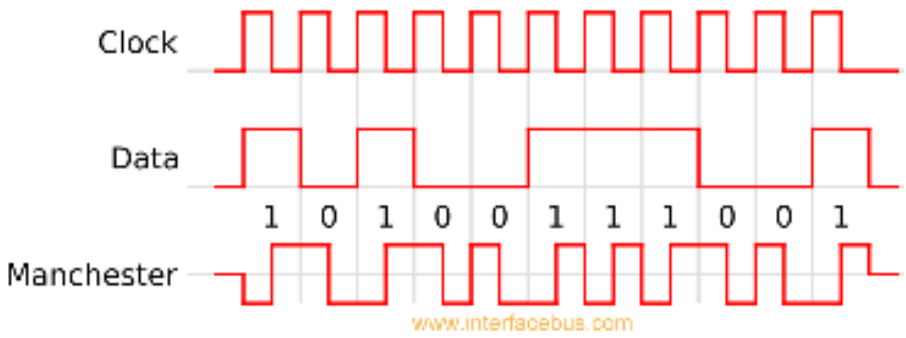
For CSMA/CD based LAN or Ethernet based LAN,

Transmission Delay = 2* Propagation Delay

1.18 Manchester Encoding

Physical Layer represents each individual bit into digital signal, and this process is known as Encoding. Ethernet based LANs follow Manchester encoding scheme for this.

In Manchester encoding, bit '1' is encoded as Low to high transition and a bit '0' is encoded as High to low transition. Here is an example below:



In Manchester encoding, each bit is represented using 2 binary signal voltage levels. Hence,

Baud Rate = 2 * Bit Rate

1.19 LMR (LAST MINUTE REVISION)

- A Network is a set of devices connected by media links. The links connecting the devices are called communications channels.
- LAN is privately-owned networks within a single building or campus of up to a few kilo meters in size.
- MAN is basically a bigger version of LAN and can support both data and voice.
- WAN supports a large geographical area, often a country or continent.
- A line configuration defines the relationship of communication devices to a communication pathway. In a multiport line configuration, three or more devices share a link. Topology refers to the physical or logical arrangement of a network.
- Devices may be arranged in a mesh, star, tree, bus, ring, or hybrid topology.
- Communication between two devices can occur in one of three transmission modes: simplex, half-duplex, full-duplex or full-full duplex. Simplex transmission means that data flows in one direction only. Half-duplex transmission allows data to flow in both directions, but not at the same time. Full-duplex transmission allows data to flow in both directions, at the same time.

- An internet is a network of networks. The transmission control protocol/Internetworking protocol (TCP/IP) is a set of protocols, or a protocol suite, that defines how all transmission are exchanged across the internet.
- The International Standards Organization (ISO) created a model called the Open Systems Interconnection (OSI), which allows diverse systems to communicate. The seven-layer OSI model provides guidelines for the development of universally compatible architecture, hardware and software.
- The physical, data link and network layers are the network support layers. The session, presentation and application layers are the user support layers. The transport layer links the networks support layer and the user support layers.
- Network delay is composition of Queuing delay, processing delay, transmission delay and propagation delay.
- Transmission delay = packet size / bandwidth
- Propagation delay= length/speed
- For CSMA/CD networks, Transmission delay=2*Propagation delay
- In Manchester encoding, Baud Rate=2*Bit Rate
- Crosstalk is the undesired effect of one circuit (or channel) on another circuit (or channel).
- Optical fiber is made up of glass and transmits signals in the form of light.
- Information must be transformed into electromagnetic signals prior to transmission across a network.
- Topology refers to the way a network is laid out, either physically or logically. Two or more devices connect to a link, then these two or more forms a topology.
- A protocol is a set of rules that govern data communication. It also defines what is communicated and when it is communicated.
- A collection of interconnected networks is called an internetwork or just internet.
- An intranet is a private network that is contained within an enterprise.
- It may consist of many interlinked local area networks and also use leased lines in the wide area network.
- In satellite based computer networks, communication between the nodes is accomplished using “radio frequencies”. Satellites that do no on-board processing, but just echo whatever they hear are often called bend-pipe satellite A satellite based network has a star topology, satellite being the central hub.

GATE QUESTIONS

Q.1 A 2 km long broadcast LAN has10^7 bps bandwidth and uses CSMA/CD. The signal travels along the wire at 2×10^8 m/s. What is the minimum packet size that can be used on this network?

a) 50 bytes b) 100 bytes
c) 200 bytes d) None of these

[GATE-2003]

Q.2 A host is connected to a department network which is part of a University network. The University network, in turn, is part of the Internet. The largest network i which the Ethernet address of the host is unique is

a) the subnet to which the host belongs
b) the Department network
c) the University network
d) the Internet

[GATE-2004]

Q.3 Consider a simplified time slotted MAC protocol, where each host always has data to send and transmits with probability p = 0.2 in every slot . There is no backoff and one frame can be transmits in one slot. If more than one host transmits in the same slot, then the transmissions are unsuccessful due to collision. What is the maximum number of hosts which this protocol can support, if each has to be provided a minimum through put of 0.16 frames per time slot?

a) 1 b) 2
c) 3 d) 4

[GATE-2004]

Q.4 A and B are the only two stations on an Ethernet. Each has a steady queue of frames to send. Both A and B attempt to transmit a frame, collide, and A wins the first back off race. At the end of this successful transmission by A, both A and B attempt to transmit and collide. The probability that A wins the second back off race is

a) 0.5 b) 0.625
c) 0.75 d) 1.0

[GATE-2004]

Q.5 Match the List I with List II and select the correct answer by using the codes given below the lists.

List 1	List 2
P. Data Link Layer	1. Ensures reliable transport of data over a physical point to point link
Q. Network Layer	2. Encodes/decodes data for physical transmission
R. Transport Layer	Allows end to end communication between two processes

	4. Routes data from one network node to the next

a) P-1, Q.4, R-3 b) P-2, Q.4, R-1
c) P-2, Q.3, R-1 d) P-1, Q.3, R-2

[GATE-2004]

Q.6 Which of the following statements is TRUE about CSMA/CD
a) IEEE 802.11 wireless LAN runs CSMA/CD protocol
b) Ethernet is not based on CSMA/CD protocol
c) CSMA/CD is not suitable for a high propagation delay network like satellite network
d) There is no contention in a CSMA/CD network

[GATE-2005]

Q.7 Which of the fallowing statements is FALSE regarding a bridge?
a) Bridge is a layer 2 device
b) Bridge reduces collision domain
c) Bridge is used to connect two or more LAN segments
d) Bridge reduces broadcast domain

[GATE-2005]

Q.8 A network with CSMA/CD protocol in the MAC layer is running at 1Gbps over a 1km cable with no repeaters. The signal speed in the cable is 2×10^8 m/sec. The minimum frame size for this net work should be
a) 10000 bits b) 10000 bytes
c) 5000 bits d) 5000 bytes

[GATE-2005]

Q.9 In a TDM medium access control bus LAN, each station is assigned one time slot per cycle for transmission. Assume that the length of each time slot is the time to transmit 100 bits plus the end-to-end propagation delay. Assume a propagation speed of 2×10^8m/sec. The length of the LAN is 1 km with a bandwidth of 10 Mbps. The maximum number of stations that can be allowed in the LAN so that the throughput of each station can be 2/3 Mbps is
a) 3 b) 5
c)10 d) 20

[GATE-2005]

Q.10 A router has two full-duplex Ethernet interfaces each operating at 100 Mb/s. Ethernet frames are at least 84 bytes long (including the preamble and the Inter-Packet -Gap). The maximum packet processing time at the router for wire speed forwarding to be possible is (in micro-seconds)
a) 0.01 b) 3.36
c) 6.72 d) 8

[GATE-2006]

Q.11 There are n stations in a slotted LAN. Each station attempts to transmit with a probability P in each time slot. What is the probability that only one station transmits in a given time slot?
a) $np(1-p)^{n-1}$ b) $(1-p)^{n-1}$
c) $p(1-p)^{n-1}$ d) $1-(1-p)^{n-1}$

[GATE-2007]

Q.12 In Ethernet when Manchester encoding is used, the bit rate is
a) half the baud rate
b) twice the baud rate
c) same as the baud rate
d) None of these

[GATE-2007]

Q.13 A broadcast channel has 10 nodes and total capacity of 10 Mbps. It uses polling for medium access. Once a node finishes transmission, there is a polling delay of 80 is to poll the next node. Whenever a node is polled, it is allowed to transmit a maximum of 1000 bytes. The maximum throughput of the broadcast channel is

a) 1 Mbps b) 100/11 Mbps
c) 10 Mbps d) 100 Mbps

[GATE-2007]

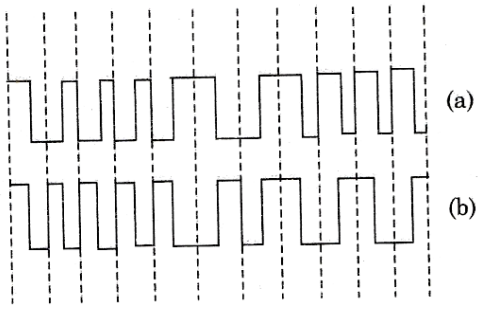
Q.14 Match the List I with List II and select the correct answer by using the codes given below the lists.

List 1	List 2
P : SMTP	1. Application Layer
Q : BGP	2. Transport Layer
R : TCP	3. Data Link Layer
S : PP	4. Network Layer
	5. Physical Layer

a) P-2, Q.1, R-3, S-5
b) P-1, Q.4, R-2, S-3
c) P-1, Q.4, R-2, S-5
d) P-2, Q.4, R-1, S-3

[GATE-2007]

Q.15 In the waveform (a) given below, a bit stream is encoded by Manchester encoding scheme. The same bit stream is encoded in a different coding scheme in wave form (b). The bit stream and the coding scheme are



a) 1000010111 and Differential Manchester respectively
b) 0111101000 and Differential Manchester respectively
c) 1000010111 and Integral Manchester respectively
d) 0111101000 and Integral Manchester respectively

[GATE-2007]

Q.16 The minimum frame size required for a CSMA/CD based computer network running at 1Gbps on a 200m cable with a link speed of 2×10^8m/s is

a) 125 bytes b) 250 bytes
c) 500 bytes d) None of these

[GATE-2008]

Q.17 In serial data transmission, every byte of data is padded with a 0 in the beginning and one or two 1s at the end of byte because

a) receiver is to be synchronized for byte reception
b) receiver recovers lost 0s and 1s from these padded bits
c) padded bits are useful in parity computation
d) None of the above

[GATE-2011]

Q.18 The Protocol Data Unit (PDU) for the application layer in the Internet stack is

a) segment b) datagram
c) message d) frame
[GATE-2012]

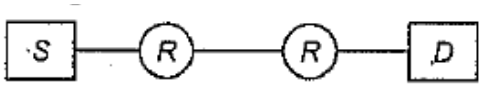
Q.19 Consider a source computer (S) transmitting a file of size 10^6 bit to a destination computer (D) over a network of two routers (R_1 and R_2) and three links (L_1, L_2 and L_3). L_1 connects S to R_1: L_2 connects R_1 to R_2 and L_3 connects R_2 to D. Let each link be of length 100 km. Assume signals travel over each link at a speed of 10^8 m/s. Assume that the link bandwidth on each link is 1Mbit/s. Let the file be broken down into 1000 packets each of size 1000 bits. Find the total sum of transmission and propagation delays in transmitting the file from S to D?

a) 1005 ms b) 1010 ms
c) 3000 ms d) 3003 ms
[GATE-2012]

Q.20 Determine the maximum length of the cable (in km) for transmitting data at a rate of 500 Mbps in an Ethernet LAN with frames of size 10000 bits. Assume the signal speed in the cable to be 200000 km/s.

a) 1 b) 2
c) 2.5 d) 5
[GATE-2013]

Q.21 Assume that source S and destination D are connected. Through two intermediate routers labelled. Determine how many times each packet has to visit the network layer and the data link layer during a transmission from S to D.



a) Network layer - 4 times and Data link layer - 4 times
b) Network layer - 4 times and Data link layer - 3 times
c) Network layer - 4 times and Data link layer - 6 times
d) Network layer - 2 times and Data link layer- 6 times
[GATE-2013]

Q.22 In the following pairs of OSI protocol layer/sub-layer and its functionality, the INCORRECT pair is

a) Network Layer and Routing
b) Data Link Layer and Bit Synchronization
c) Transport Layer and End-to-End process communication
d) Medium Access Control Sub-Layer and Channel Sharing.
[GATE–2014]

Q.23 Consider a CSMA/CD network that transmits data at a rate of 100 Mbps (10^8 bits second) over 1 km cable with no repeaters. If the minimum frame size required for this network is 1250 bytes, what is the signal speed (km/sec) in the cable?

a) 8000 b) 10000
c) 16000 d) 20000
[GATE–2015]

Q.24 Consider a LAN with four nodes S1, S2, S3 and S4. Time is divided into fixed-size slots, and a node can begin its transmission only at the beginning of a slot. A collision is said to have occurred if more

than one node transmit in the same slot. The probabilities of generation of a frame in a time slot by S1, S2, S3 and S4 are 0.1, 0.2, 0.3 and 0.4, respectively. The probability of sending a frame in the first slot without any collision by any of these four stations is _____.

[GATE–2015]

Q.25 Two hosts are connected via a packet switch with 10^7 bits per second links. Each link has a propagation delay of 20 microseconds. The switch begins forwarding a packet 35 microseconds after it receives the same. If 1000 bits of data are to be transmitted between the two hosts using a packet size of 5000 bits, the time elapsed between the transmission of the first bit of data and the reception of the last of the data in microsecond is _____.

[GATE–2015]

Q.26 In an Ethernet local area network, which one of the following statements is TRUE?

a) A station stops to sense the channel once it starts transmitting a frame.
b) The purpose of the jamming signal is to pad the frames that are smaller than the minimum frame size.
c) A station continues to transmit the packet even after the collision is detected.
d) The exponential back off mechanism reduces the probability of collision on retransmissions

[GATE–2016]

Q.27 A network has a data transmission bandwidth of 20×106 bits per second. It uses CSMA/CD in the MAC layer. The maximum signal propagation time from one node to another node is 40 microseconds. The minimum size of a frame in the network is _____ bytes.

[GATE–2016]

Q.28 Consider a simple communication system where multiple nodes are connected by a shared broadcast medium (like Ethernet or wireless). The nodes in the system use the following carrier-sense based medium access protocol. A node that receives a packet to transmit will carrier-sense the medium for 5 units of time. If the node does not detect any other transmission in this duration, it starts transmitting its packet in the next time unit. If the node detects another transmission, it waits until this other transmission finishes, and then begins
to carrier-sense for 5 time units again. Once they start to transmit, nodes do not perform any collision detection and continue transmission even if a collision occurs. All transmissions
last for 20 units of time. Assume that the transmission signal travels at the speed of 10 meters per unit time in the medium.

Assume that the system has two nodes P and Q, located at a distance *d* meters from each other. P starts transmitting a packet at time *t=0* after successfully completing its carrier-sense phase. Node Q has a packet to transmit at time *t=0* and begins to carrier-sense the medium.

The maximum distance *d* (in meters, rounded to the closest integer) that allows Q to successfully avoid a collision between its proposed transmission and P's ongoing Transmission is _____.

[GATE–2018]

ANSWER KEY:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
D	C	B	B	A	C	D	A	C	C	A	A	B	B	A
16	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**26**	**27**	**28**		
B	**A**	**C**	**A**	**B**	**C**	**B**	**D**	**0.4404**	**1575**	**D**	**200**	**50**		

EXPLANATIONS

Q.1 **(d)**

Q.2 **(d)**
Ethernet address is nothing but MAC address which is present on NIC and it is unique for every system or host in the internet.

Q.3 **(b)**
Let there be N such hosts.
Then when one host is transmitting then other must be silent.
So the throughput per host:
$0.16=0.2*(0.8)^{(N-1)}$
$0.8=0.8^{(N-1)}$
It implies N-1=1, so N=2.

Q.4 **(b)**
In the first back off race, there are two conditions 0 and 1
In the second back off race there are four conditions 0, 1, 2 and 3
Hence, winning probability of A can be cancelled as

$$\frac{1}{2}\times\frac{3}{4}+\frac{1}{2}\times\frac{1}{2}$$

$$= 3/8 + \frac{1}{4}$$

$$= 5/8$$

$$= 0.625$$

Q.5 **(a)**

Q.6 **(c)**
CSMA/CD was used in early days, 802.3 not in 802.11.
There will be contention in this protocol.
Ethernet is based on CSMA/CD early in 1980s.

Q.7 **(d)**
Bridge does not reduce broadcast domain, it remains same.

Q.8 **(a)**
Let S is minimum packet size.
T_p = (1 km) / (2×10^8 m/s)
$=5\times10^{-6}$ seconds.
Minimum frame size can be found by formula
$T_x = 2\ T_p\ S/1$ Gbps
$S = 10^9\times10^{-5} = 10^4$ bits.

Q.9 **(c)**
Each slot is equal to transmission time of 100 bits + propagation delay.
Propagation delay = 1km/$2*10^8$ms = 5μs.
T_x = 100/10 Mbps = 10 μs.
Let there are maximum N number of station then Length of cycle is = N*(10+5) = 15N μs.
In a whole cycle each user transmit for only 10 μs.
Therefore efficiency is (10/15N).
Throughput of each station is (10/15N)*10Mbps which is given as 2/3 mbps
N = (10*10*3)/(15*2)=10

Q.10 **(c)**
For maintaining the speed of forwarding of wire,
i.e. 100 Mbps.
Processing time should be at most same as minimum transmission time.

84*8 bits/100 Mbps = 6.7 micro seconds.

Q. 11 (a)

It is already given that n stations transmit with a probability p in a slotted LAN.

For this, the stations need to acquire a medium. Let us assume the following

1 be the event when station 1 transmits

2 be the event when station 2 transmits

N be the event when station N transmits

The probability for a station to transmit is represented as

$P(1\bar{2}\bar{3}...\bar{N} \cup \bar{1}2\bar{3}\bar{4}...\bar{N} \cup \bar{1}\bar{2}3\bar{4}\bar{5}...\bar{N} \cup ...)$

As all the events are mutually exclusive. Hence, the probability can be given as

$P(1)P(2)P(3)..P(\bar{N}) + P(\bar{1})P(2)P(\bar{3})$

$P(\bar{4})\ P(\bar{5})...P(\bar{N}) + ...$

As given that all events are independent, hence the probability

$= p(1-p)(1-p)...(1-p) + (1-p)p(1-p)...$

$(1-p) + (1-p)(1-p)p(1-p)...(1-p) + ...$

$= np(1-p)^{n-1}$

Q.12 (a)

Manchester Encoding → 2 signals will be used for sending 1-bit. For sending 10 bits, we have to send 20 signals. Hence baud rate is twice the bandwidth. Bandwidth = Baud rate/2 [Half the baud rate]

Q.13 (b)

T_x =1000 bytes/10Mbps = 800 μs.

Delay because of polling is = 80 μs.

Efficiency of channel e = transmission delay/(total delay) = 800/(800+80) = 10/11) Maximum throughput is

= (10/11)* Mbps = 100/11 Mbps

Q.14 (b)

7. **Application Layer**
   SSI DNS FTP
   Gopher HTTP
   SMPP SMTP SNMP Telnet
6. **PRESENTATION LAYER**
   MIME TLS SSL
5. **SESSION LAYER**
   NetBIOS SAP
4. **TRANSPORT LAYER**
   TCI UDP
3. **NETWORK LAYER**
   IP EGMP IPsec
2. **DATA LINK LAYER**
   ARP CSLIP SLIP Ethernet
1. **PHYSICAL LAYER**
   DSL SONET/SDH
   Ethernet USB Bluetooth

Q.15 (c)

'0'- Low to high.

'1'- High to low

There is a transition at the middle of each bit period.

∴ The bit pattern is 100 00 10111.

Q.16 (a)

The minimum frame size for a CSMA/CD is

= 2 × Pd × BW

$= 2 \times \frac{200}{2 \times 10^8} \times 1\text{Gbps}$

$= 2 \times 10^{-6} \times 10^9$

= 2000 bits = 250 bytes

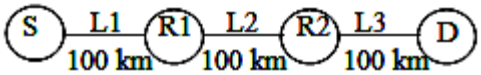
Q.17 (a)

The primary use of padding is to prevent the cryptanalyst from using that predictability to find cribs that aid in breaking the encryption. Hence, Padding bits are used to protect the bits. All the

bytes that are required to be padded are padded with zero.
There are two types of padding methods: Bit Padding/Byte Padding and Zero padding.
Bit Padding Two types of bits are used in the process: Single set bit resented by 1 and Reset Bit 0. A single set (1) bit is added to a message and then as many reset (0) bits as necessary are added to the same message. The total number of reset (0) bits added actually depends on the boundary of the message to which the message needs to be extended. In bit terms this is 1000……. 0000, in hex byte terms this is 80 00 …0000
For example, a message of 23 bit that is padded with 9 bits in order to fill a 32 bit block
…| 11011 1001 1101 0100 001 0 0111 0000 0000 |
Zero Padding In Zero Padding, alI bytes are padded with zero. Example: In the following example the block size is 8 byte and padding is required for 4 byte
…| DD DD DD DD DD DD DD DD | DD DD DD DD 00 00 00 00 |
Zero padding makes it impossible to distinguish between plain text data bytes and padding bytes as it is not reversible in the case when original file ends with one or more zero bytes.

Q.18 **(c)**
The protocol data units are as follows:
For application layer – message
For transport layer – segment
For network layer – data gram
For data link layer – frame

Q.19 **(a)**



Propagation delay to travel from S to R1

$$= \frac{\text{Distance}}{\text{Link Speed}} = \frac{10^5}{10^8} = 1\text{ms}$$

Total propagation delay to travel fromS to D=3*1 ms= 3 ms
Total transmission delay for 1 packet

$$= 3*\frac{(\text{Number of bits})}{\text{Bandwidth}}$$

$$= 3*\frac{(1000)}{10^6} = 3\text{ms}$$

So the forst packet will take 6ms to reach D. While first was reaching D, other packets must have been processing in parallel. So D will receive remaining packets 1 packet per 1 ms from R_2. So remaining 999 packets will take 999 ms and total time will be 999+6=1005 ms

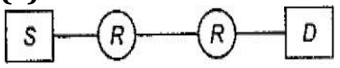
Q.20 **(b)**
Frame size = 10000 bite
Propagation time = transmission time + collision signal

$$\frac{\text{Frame size}}{\text{propagation time}} = \frac{\text{length}}{\text{signal speed}} + \frac{\text{length}}{\text{signalspeed}}$$

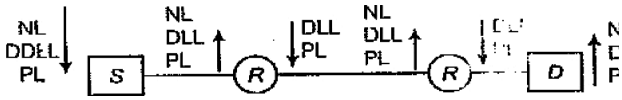
$$\frac{10000\text{bits}}{500\times10^6\text{bits/s}} = \frac{2\times\text{length}}{2\times10^5}$$

Length = 2 km
Hence, the maximum length of the cable (in km) is (b) 2 km

Q.21 **(c)**



The answer is © NL – 4 times and DL – 6 times



Each packet has to visit the network layer 4 times and the data link layer 6 times during a transmission from S to D

Q.22 (b)

(a) One of the main functionality of Network Layer is Routing.

(b) Bit Synchronization is always handled by Physical Layer of OSI model but not Data Link Layer. So Option (b) is INCORRECT.

(c) End to End Process Communication is handled by Transport Layer.

(d) MAC sub layer have 3 types of protocols (Random, Controlled and Channelized Access).

Q.23 (d)

Band width = 100×10^6 bps

d=1000m

For CSMA/CD: $t_d \geq 2P_d$

$$\frac{1250\times8}{100\times10^6} = 2\times\frac{1000}{x\ m/s}$$

$$x = \frac{2\times1000\times100\times10^6}{1250\times8}$$

$= 2\times10^7$=20000(km/sec)

Q.24 0.45

The probability of sending a frame in the first slot without any collision by any of these four stations is sum of following 4 probabilities

Probability that S1 sends a frame and no one else does + Probability thatS2 sends a frame and no one else does + Probability thatS3 sends a frame and no one else does + Probability thatS4 sends a frame and no one else does

=0.1*(1-0.2)*(1-0.3)*(1-0.4)+(1-0.1)* 0.2*(1-0.3)*(1-0.4)+(1-0.1)*(1-0.2)* 0.3*(1-0.4)+(1-0.1)*(1-0.2)*(1-0.3)*0.4

= 0.4404

Q.25 (1575)

Sender host transmits first packet to switch, the transmission time is 5000/107 which is 500 microseconds. After 500 microseconds, the second packet is transmitted. The first packet reaches destination in 500 + 35 + 20 + 20 + 500 = 1075 microseconds.

While the first packet is travelling to destination, the second packet starts its journey after 500 microseconds and rest of the time taken by second packet overlaps with first packet. So over all time is 1075 + 500 = 1575.

Q.26 (d)

The concept of binary exponential backoff algorithm. The exponential backoff mechanism reduces the probability of collision on retransmissions.

Q.27 200

L = ?

B = 20 Mbps

Tp = 40 micro sec

Tx = L/B = 100 ms

Tx = 2Tp

Lmin = 2Tp B = 2(40) (20)/8 = 200 Bytes

Q.28 (50)

Node that receives the packet to transmit, will carrier-sense the medium for 5 units. Any packet which

arrives within 5 units will be sensed and keep the channel busy. Given that Signal speed is 10 meters/time.

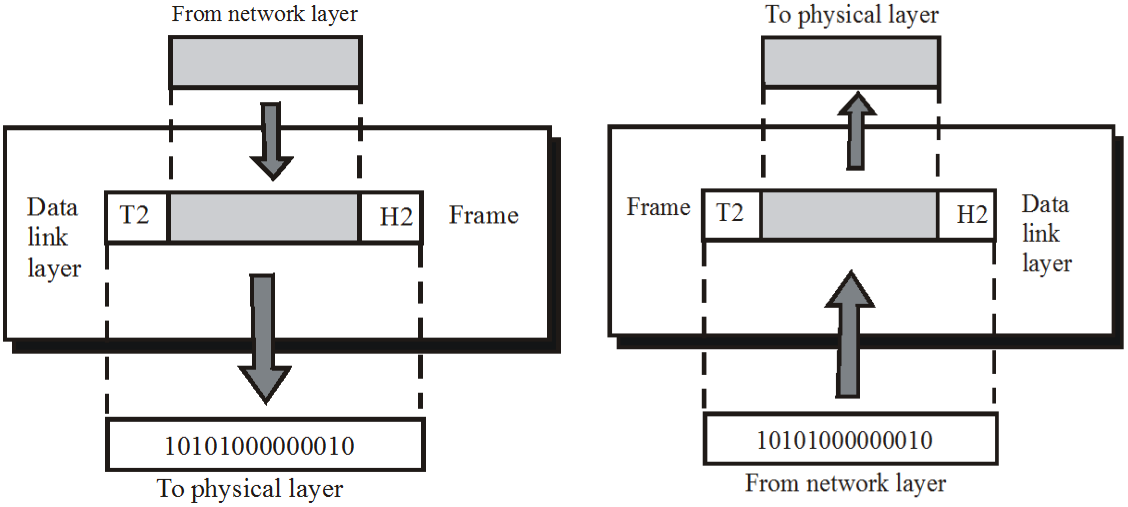
This means in 5 units of time, a packet can travel 50 meters in maximum, which allows Q to successfully avoid the collision.

So Answer is 50.

2 DATALINK LAYER AND SWP

2.1 INTRODUCTION

Data link layer provide interface to the network layer, determine the number of bits of the physical layer to be grouped into frames, delete transmission error and regulate the flow of frames. The data link layer transforms the physical layer to a reliable link and responsible for node-to-node delivery.

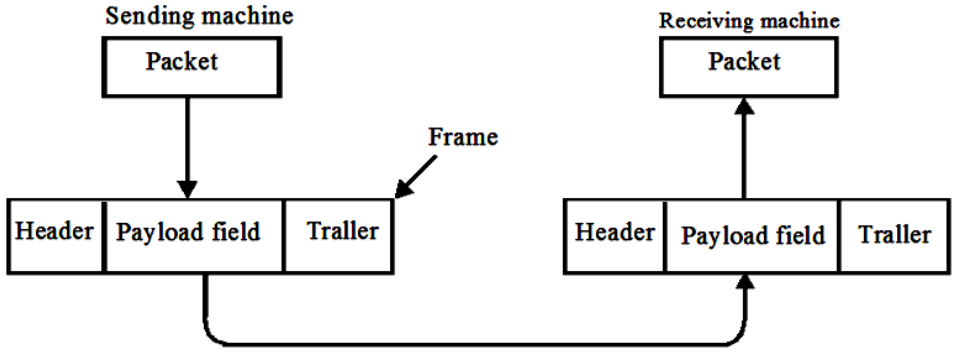


2.2 DATA LINK LAYER DESIGN ISSUES

The data link layer has a number of specific functions it can carry out. These functions include

1. Providing a well-defined service interface to the network layer.
2. Dealing with transmission errors.
2. Regulating the flow of data so that slow receivers are not swamped by fast senders.
4. Framing
5. Physical addressing

To accomplish these goals, the data link layer takes the packets it gets from the network layer and encapsulates then into frames for transmission. Each frame contains a frame header, a payload field for holding the packet, and a frame trailer, as illustrated in fig. Frame management forms the heart of what the data link layer does. In the following sections we will examine all the above mentioned issues in detail.

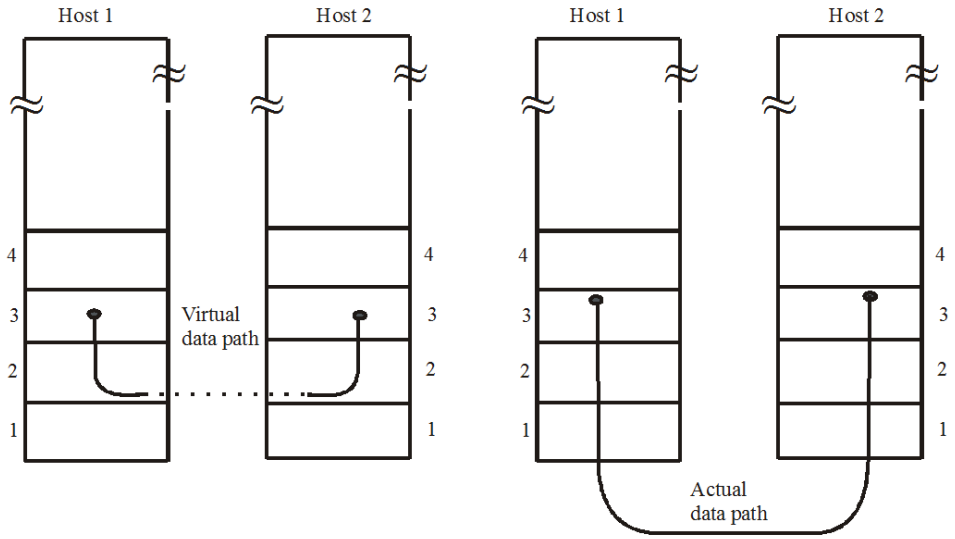


2.2.1 SERVICES PROVIDED TO THE NETWORK LAYER

The function of the data link layer is to provide services 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. One the source machine is an entity, call it a process, in the network layer that 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 there, a shown in Fig.

a) The actual transmission follows the path of Fig.

b) But it is easier to think in terms of two data link layer processes communicating using a data link protocol.



The data link layer can be designed to offer various services. The actual services offered can vary from system to system. There reasonable possibilities that are commonly provided are

1. Unacknowledged connectionless service
2. Acknowledged connectionless service
2. Acknowledged connection-oriented service

An unacknowledged connectionless service consists of having the source machine send independent frames to the destination machine without having the destination machine acknowledged them. No logical connection is established beforehand or released afterward. If a frame is lost due to noise on the line, no attempt is made to detect the loss or recover from it in the data link layer. This class of service is appropriate when the error rate is very low so that recovery is left to higher layers. It is also appropriate for real-time traffic, such as voice, in which late data are worse than bad data. Most LANs use unacknowledged connectionless services in the data link layer. The next step in terms of reliability is **Acknowledged connectionless service.** When this service is offered, there are still no logical connections used, but each frame sent is individually acknowledged. In this way, the sender knows whether a frame has arrived correctly. If it has not arrived correctly. If it has not arrived within a specified time interval, it can be sent again. This service is useful over unreliable channels, such as wireless systems. With **connection –oriented service,** the source 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 indeed received. Furthermore, it guarantees that each frame is received exactly once and that all frames are received in the right order. With connectionless service, in contrast, it is conceivable that a lost acknowledgement causes a packet to be several

times and thus received several times. Connection-oriented service, in constract provides the network layer processes with the equivalent of a reliable bit stream.

2.2.2 FRAMING

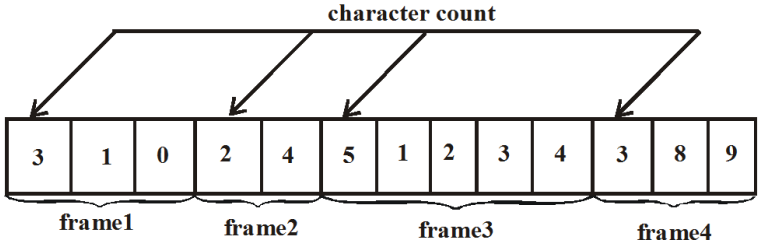
- For providing services to the network layer, the data layer uses the service provided to it by the physical layer.
- If the raw bit stream provided by physical layer is not error free, then it is up to the data link layer to detect and correct errors.
- Bit stream is broken into discrete frames and checksum is calculated for each frame. This checksum is calculated at each destination and if found different from the one contained in the frame, then an error has occurred.
- Various methods of Framing are
  i) Time gaps
  ii) Character count
  iii) Starting and ending characters, with characters stuffing
  iv) Starting and ending flags, with bit stuffing
  v) Physical layer coding violations

2.2.3 TIME GAPS

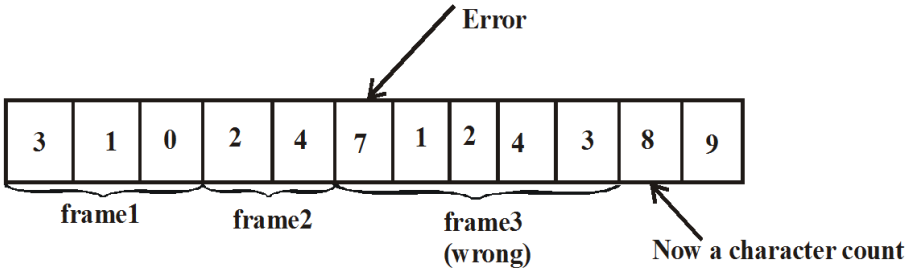
- Framing is done by inserting time gaps between Frames, very similar to the way of spacing between words in ordinary text.
- Network cannot guarantee about timing, so these gaps might be squeezed out or other gaps might be inserted during transmission.
- It is risky to count on timing to mark the start and end of each frame.

2.2.4 CHARACTER COUNT

- It uses a field in the header to specify the number of characters in the frame. Thus at the destination by seeing the character count it knows how many characters follows and where the end of the frame exist.



- **Example**
  Consider the following four frames of sizes 2, 2, 5 and 2.



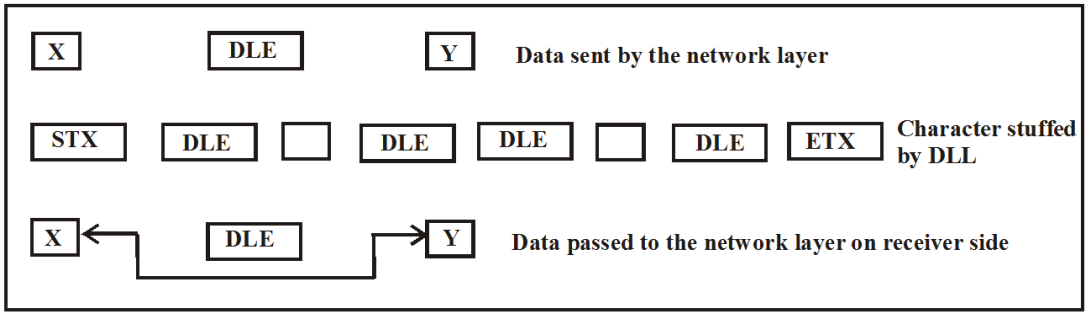
- **Trouble**

→ For the above example if the count of 5 in the third frame becomes 7, then destination will get out of synchronization and unable to locate the start of the next frame.
As the checksum is incorrect and the destination knows that the frame is bad, still it do not know where the next frame starts. Retransmission does not help even, as the destination does not know how many characters to skip over to get to the start of the retransmission.
For this reason, the character count method is rarely used anymore.

2.2.5 STARTING AND ENDING CHARACTERS, WITH CHARACTER STUFFING

- Each frame start with the ASCII character sequence DLESTX and end with the sequence DLE ETX.(DLE-Data Link Escape STX is start of Text, ETX is end of text).
- If the destination loses track of the frame boundaries, all it has to do is to look for DLE STX or DEL ETX character.

Problem:
Binary data such as object programs or floating point numbers, if are transmitted, then they may easily interfere with the framing (as characters for DLE STX or DLE ETX may occur in the data).
Solution:
Insert an ASCII DLE character just before each "accidental" DLE character in the data. The data link layer on the receiver removes the DLE before the data when given to the network layer.



- **Disadvantage**

Closely tied to only 8-bit characters and the ASCII character code. Also embedding the character code in the framing mechanism became more and more obvious. So the new technique had to be developed called bit stuffing to allow arbitrary size characters.

2.2.6 STARTING AND ENDING FLAGS, WITH BIT STUFFING:

- Has arbitrary number of bits and allows character codes with an arbitrary number of bits per character
- Every frame begins and ends with a special bit pattern, 01111110, called a flag byte.
- As soon as the sender`s data link layer encounter five consecutive ones in the data, it stuffs a 0 bit into the outgoing bit stream.
- Receiver dyestuffs the 0 bit of the five consecutive incoming 1 bits, followed by a 0 bit.
- If the user data is 01111110, then it transmitted as 011111010 but stored in receiver as 01111110.

01111111111110010 Original data
0111110111110110010 Bit stuffed data
01111111111110010 Data at receiver

- Flag pattern at the frame boundaries prevent us from loosing track at the receiver.

2.2.7 PHYSICAL LAYER CODLING VIOLATIONS

- Applied to the networks in which the encoding on the physical medium contains some redundancy.
- Example: Encoding of 1 bit of data by using 2 physical bits in some LAN.
- 1 → high-low pair
  0 → low-high pair
  high – high, low – low } Not used for data
- As every data bit has a transition in the middle, thus easy for the receiver to locate the bit boundaries.
- This use of invalid physical code is a part of 802 LAN standards.

2.3 ERROR DETECTION CORRECTION

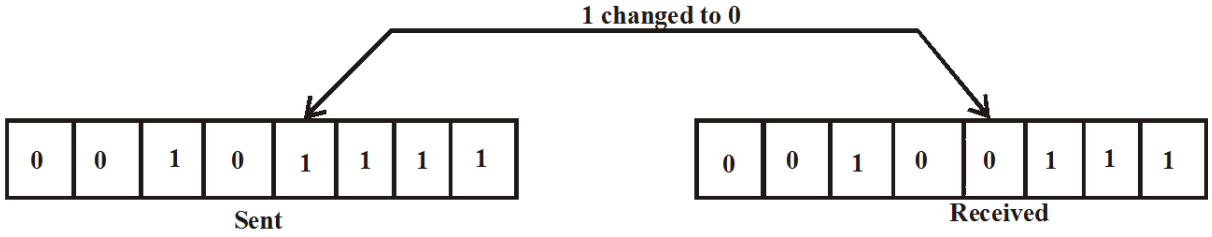
IMP
Data gets corrupted during transmission for reliable and efficient communication; errors must be detected and corrected.

2.3.1 TYPES OF ERRORS

IMP
Unpredictable interference from heat, magnetism and other forms of electricity on signals which may change the shape or timing of it is called errors.

2.3.2 SINGLE-BIT ERROR

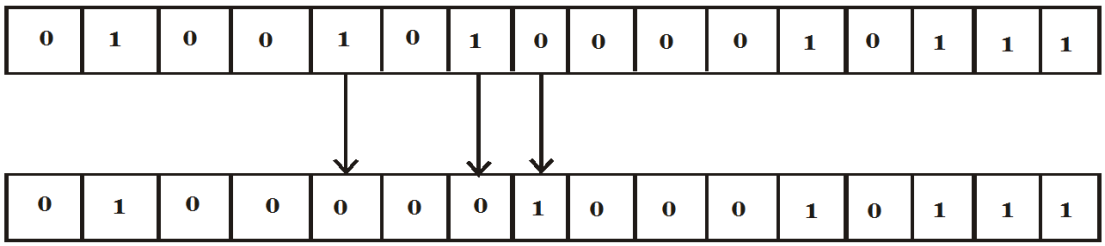
IMP
The term single-bit error means that only one bit in the data unit has changed i.e. it can either be from 1 to 0 or from 0 to 1.
Example



2.3.2 BURST ERROR

IMP
The term burst error means that two or more bits in the data unit have changed i. e. either changed from 1 to 0 or changed from 0 to 1.

Example

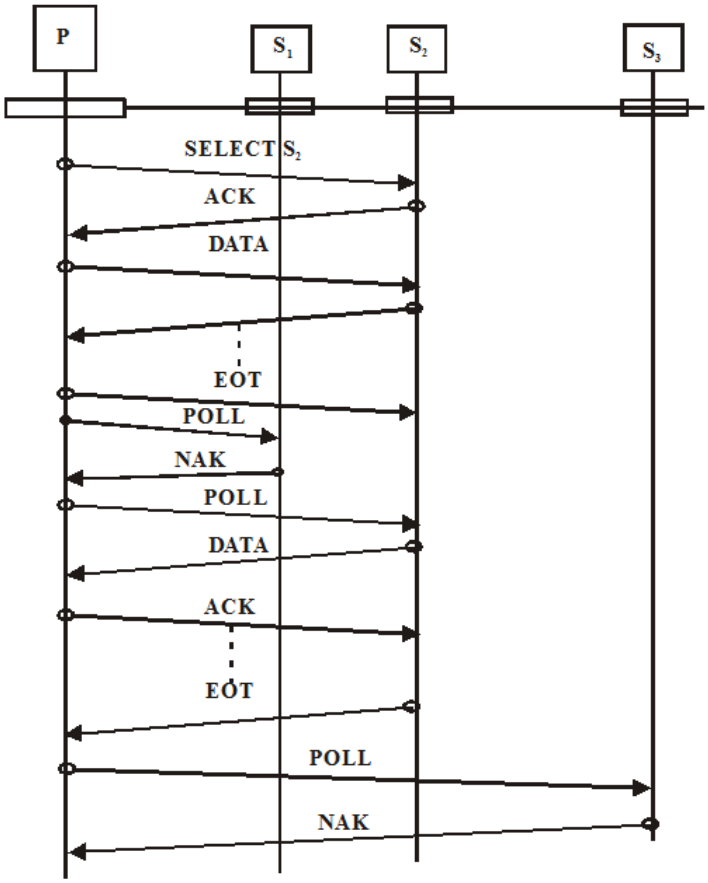


2.4 ERROR CORRECTING CODES

For dealing with errors, one can include enough redundant information along with each block of data sent to enable the receiver to deduce what the transmitted character must have been. This strategy uses error-correcting codes.
For dealing with errors, one can include only enough redundancy to allow the receiver to deduce that and error occurred, but not which error, and has it request a retransmission. The strategy uses error-detecting codes.
When an error is detected, one can do any of following:

i) The receiver can have the sender retransmit The entire data unit.

ii) A receiver can use an error-correcting code, Which automatically corrects certain errors?



2.4.1 ACCESS CONTROL

- Access control methods manage establishment of links.
- Right of a particular device to transmit is given by access control methods.

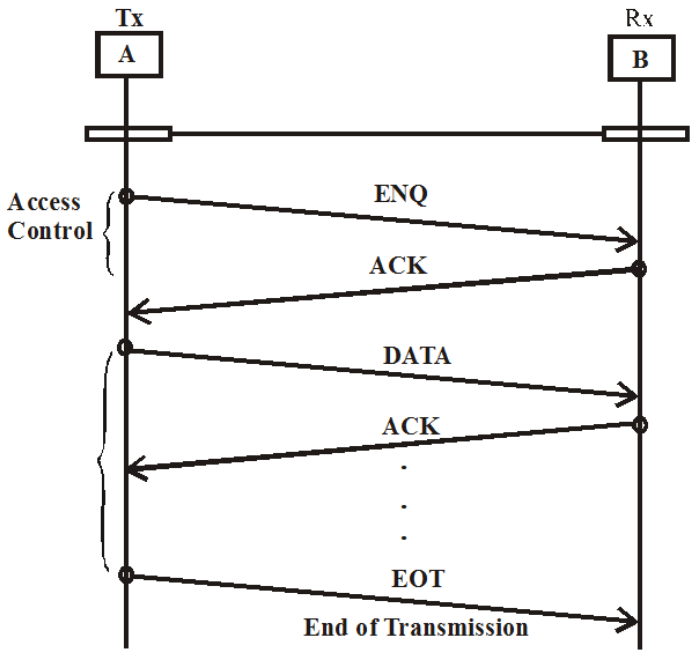


Fig. ENQ-ACK method (Enquiry/Acknowledgement)

1. ENQ-ACK method (Enquiry / Acknowledgement)

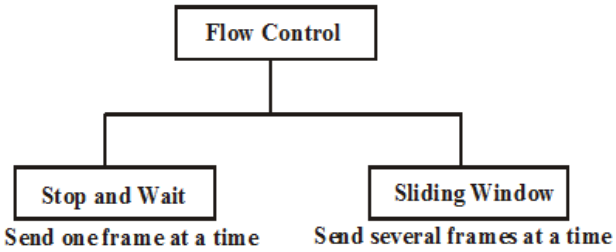
- Used in case of point to point configurations.
- Used for dedicated path.
- 'A' sends an ENQ frame if it wants to initiate data transfer. If 'B' is not ready it sends a NAK else sends ACK.
- If 'B' is not ready or ACK is lost then 'A' will send ENQ frame again. This process repeats 2 times and then it will disconnect if no ACK is received and then try after sometime.

2. POLL/SELECT Method

- Used with multipoint configuration i.e. used in a system where one device works as primary and other as secondary.
- PRIMARY is always initiator of the session. Primary device controls the link and determines which device is allowed to transmit at a given time.
- Whenever multipoint link consists of primary device and multiple secondary devices using a single transmission line all exchange must be made through the primary device even if ultimate destination device is secondary.
- SELECT: Transmission of data from primary to secondary.
  POLL: Transmission of data from secondary to primary.
  POLLING is done by PRIMARY in a sequence.
- Data transmission in POLL mode can be terminated by either 'EOT' from secondary or 'TIME'S UP' by primary which depends on protocol and length of message.

2.4.2 FLOW CONTROL

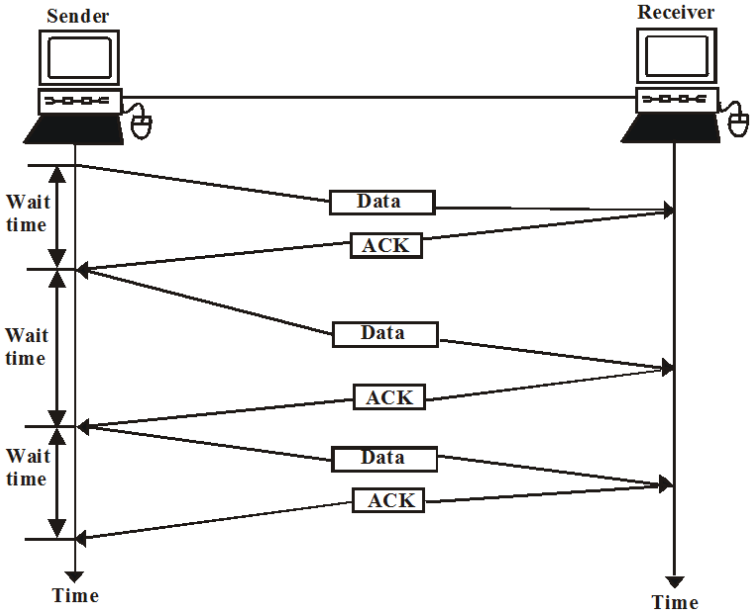
- It regulates the flow of frames so that slow receivers are not affected by the fast sender or vice versa.
- It tells the sender how much data it should transmit before it wait for an acknowledgement from the receiver.



- Incoming data must be checked before they can be used. The rate of processing is often slower than the rate of transmission.
- Each receiving device has a block of memory called a buffer, reserved for storing incoming data until they are processed.
- If the buffer is full, the receiver must be able to tell the sender to halt transmission until it is once again able to receive.
- Frames can be acknowledged frame by frame or several frame at a time. If damaged frame arrives at the receiver, then it should send an error message, a NAK frame.

1. Stop and Wait

- Sender waits for an acknowledgement after every frame it sends. Next frame is sent only after the acknowledgement is received.
- The process of alternately sending and waiting repeats itself until the sender transmits an end of transmission (EOT) frame.



Advantage

Simple as each frame is checked and acknowledged before the next frame is sent.

Disadvantages

i) Extremely slow as each frame must travel all the way to the receiver and an acknowledge must travel all the way back before the next frame can be sent.

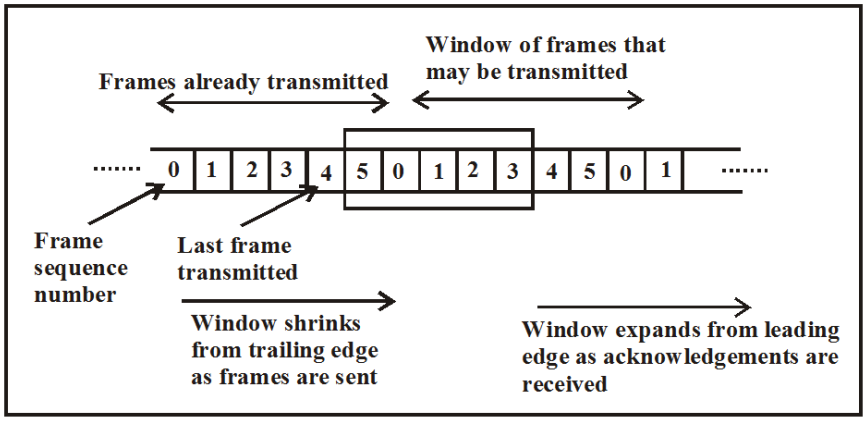
ii) Inefficient as each frame is alone on the line. Each frame sent and received takes the entire time needed to transverse the link.

iii) If the distance between the devices is long then time spent waiting for acknowledgement between each frame add significantly to the total transmission time. Thus, reduction in throughput.

2. Sliding Window

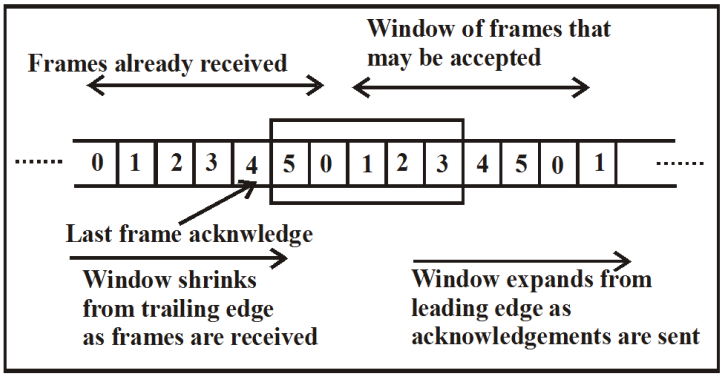
- The sender can transmit several frames without waiting for an acknowledgment. Frames can be sent one after another.
- The receiver every time acknowledges some of the frames using a single acknowledgment frame to confirm the receipt of multiple data frames.
- It uses a window where frames are numbered modulo-n, i.e. they are numbered from 0 to n-1.
- Numbered of next frame a receiver expects to receive is sent along with the acknowledgment frame (ACK).

3. Sender Window



- The sender window contains (n-1) frames in the beginning.
- As soon as the frames are sent out, the left boundary of the window of the moves inward, thus shrinking the size of the window.
- As soon as the acknowledgement frame (ACK) arrives at the transmitter, the window expends to allow in a number of frames equal to the number of frames acknowledged.

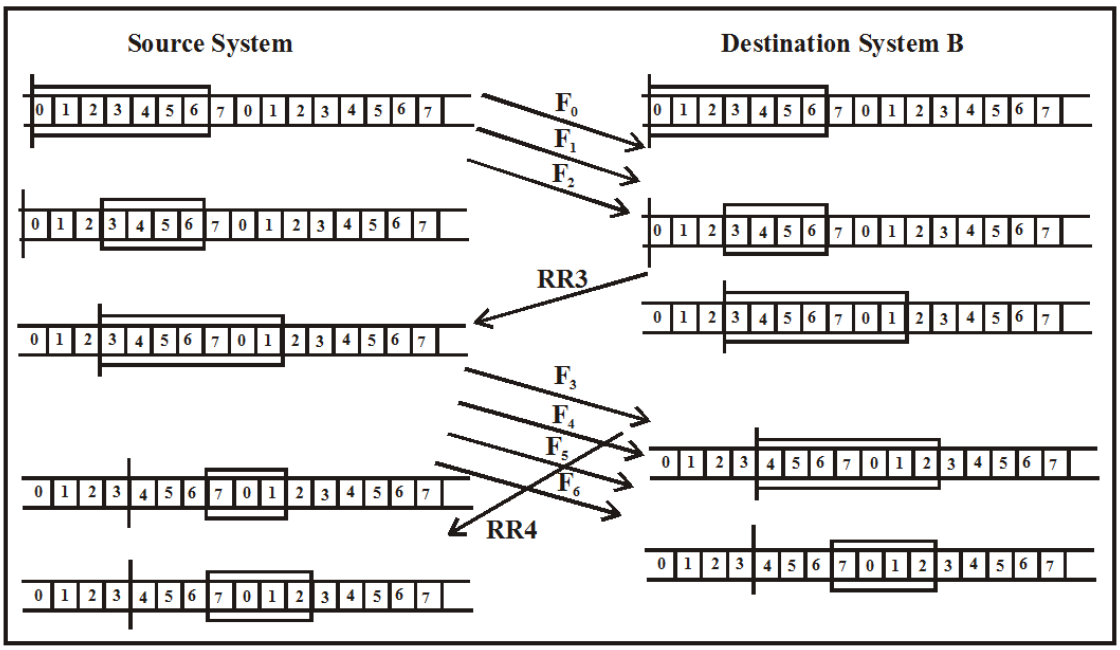
4. Receiver Window



- The receiver window contains (n-1) spaces for frame in the beginning.
- The size of the receiver window shrinks as new frames come in. Thus, the receiver window represents the number of the frames that may still be received before an acknowledge frame (ACK) must be sent.
- When an acknowledge is sent, the window expends to include places for a number of frames equal to the number acknowledged.

An example is shown in Fig. below the example assumes a 2-bit sequence number field and a maximum window size of seven frames. Initially, A and B have windows indicating that A

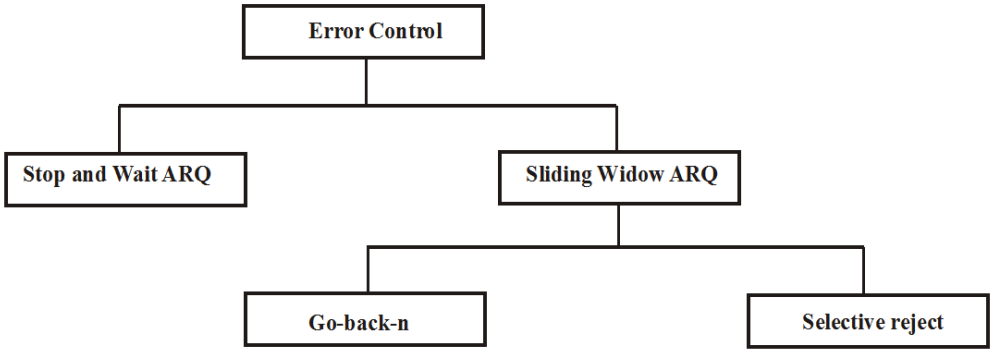
may transmit seven frames, beginning with frame 0 (F0). After transmitting three frames (F0, F1, F2).



Without acknowledgement. A has shrunk its window to four frames and maintains a copy of the three transmitted frames. The window indicates that A may transmit four frames, beginning with frame number 2. B then transmit and RR (receive ready) 2, which means "I have received all frames up through frame number 2 and am ready to receive frame number 2; in fact, I am prepared to receive seven frames, beginning with frame number 2." With this acknowledges F2, and allows transmission of F4 through the next instance of F2. By the time this RR reaches A, it has already transmitted F4, F5, and F6, and therefore A may only open its window to permit sending four frames beginning with F7.

2.4.3 ERROR CONTROL

- It let receiver, to inform the sender about any frame lost or damaged in transmission and thus co-ordinates the re-transmission of those frames by the sender.

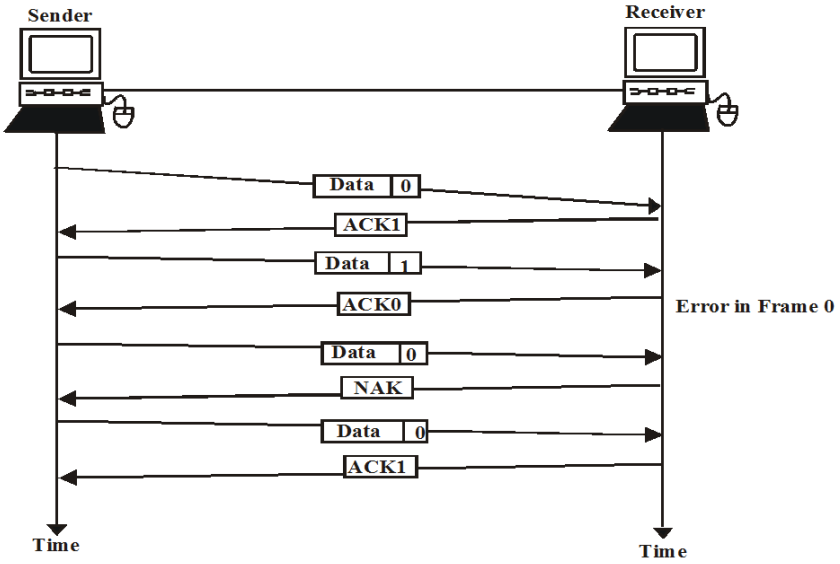


2.4.3.1 STOP AND WAIT ARQ

- It is extended flow control which includes retransmission of data in case of loss or damaged frames.
- The sender keeps a copy of the last frame transmitted unit it receives an acknowledgement for that frame.

- For identification purposes, both data frame and acknowledge frames are numbered. This numbering allows data frames identification in case of duplicate transmission.
- If an error is detected, a NAK frames is sent. NAK frames are not numbered. When the sending device receives a NAK it retransmits the frame transmitted after the last ACK regardless of number.
- The sending device (sender) is equipped with a timer. If an expected acknowledgement is not received within an allotted time period, the sender considers it to be lost data frame and thus sends it again.

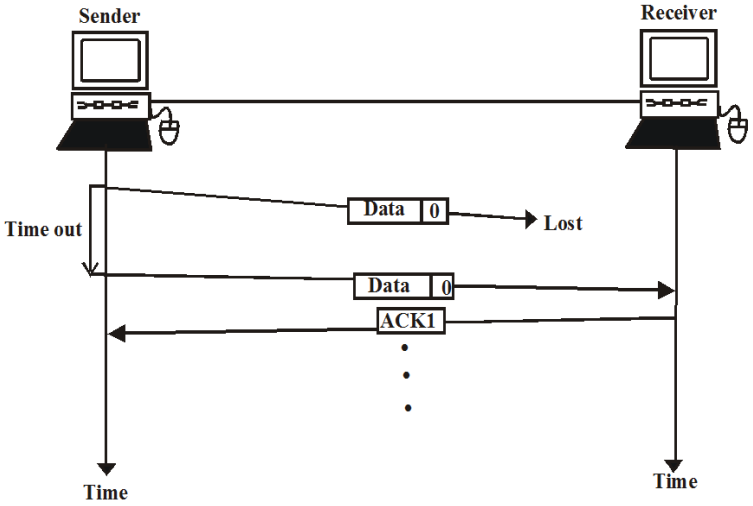
Damaged Frame



- When an error is detected in data frame, NAK is sent and the sender retransmits the last frame.

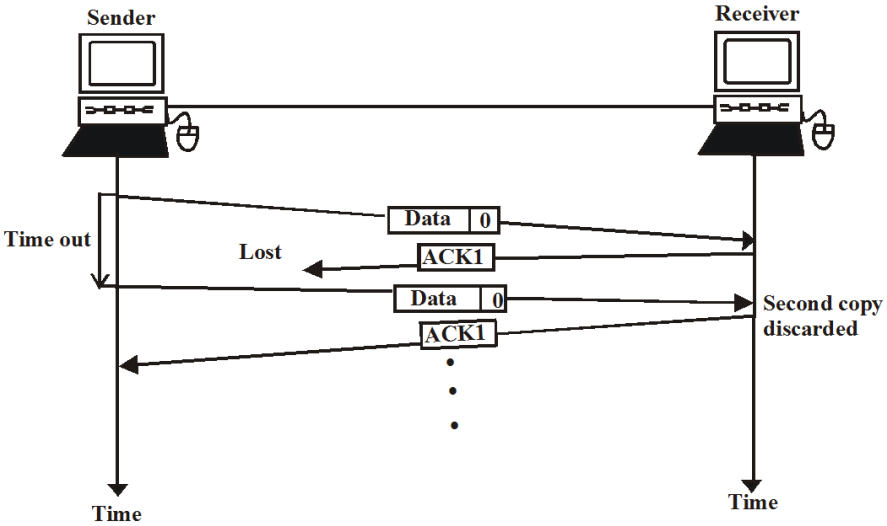
Lost Data Frame

- Every sender is equipped with a timer that starts as soon as a data frame begins to transmit.
- If the frame never make to receiver i.e. if it is lost then the receiver can never acknowledge it (neither ACK nor NAK)
- Sender waits for an ACK/NAK frame until its timer goes off and then it retransmits the last data frame, restart the timer.



Lost acknowledgement

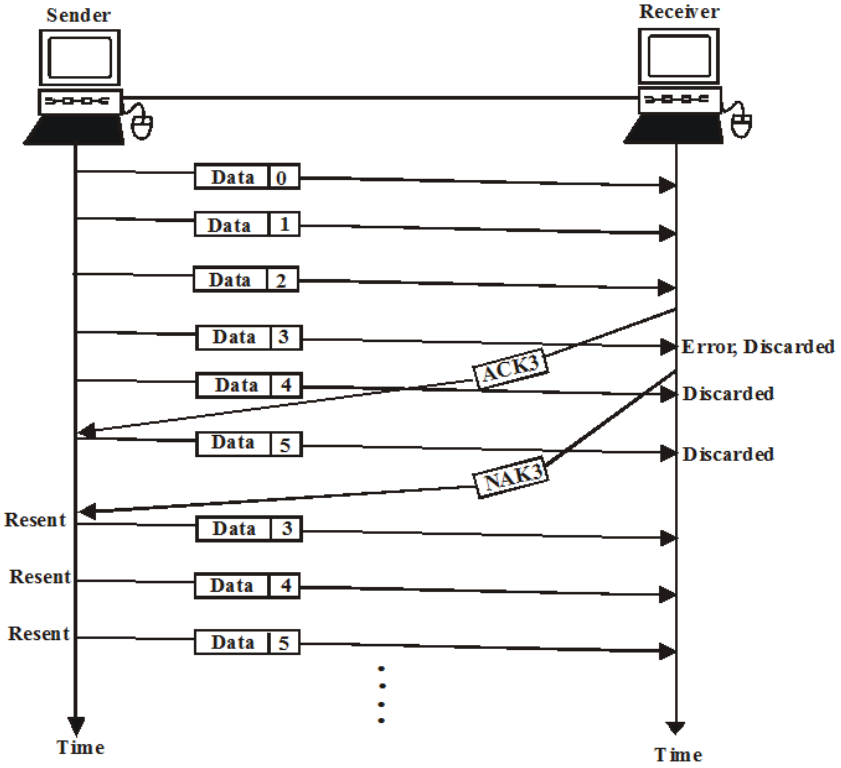
- Data frame received by the receiver can either be acceptable or nor acceptable but the ACK or NAK frame returned by receiver is lost.
- As the timer of the sender goes off, the sender retransmits the data frame. Receiver checks the number of the new data frame.



i) If lost frame was NAK, receiver accepts new copy and returns the appropriate ACK/NAK.

ii) If lost frame was an ACK, receiver recognizes new copy as duplicate and thus discards it and waits for next purpose.

2.4.3.2 SLIDING WINDOW ARQ



- The sending device keeps copies of all transmitted frames until they have been acknowledged.
- For identification purpose both ACK and NAK frames are numbered. ACK frame carry the numbered of the next frame expected and NAK frame carry the number of damaged

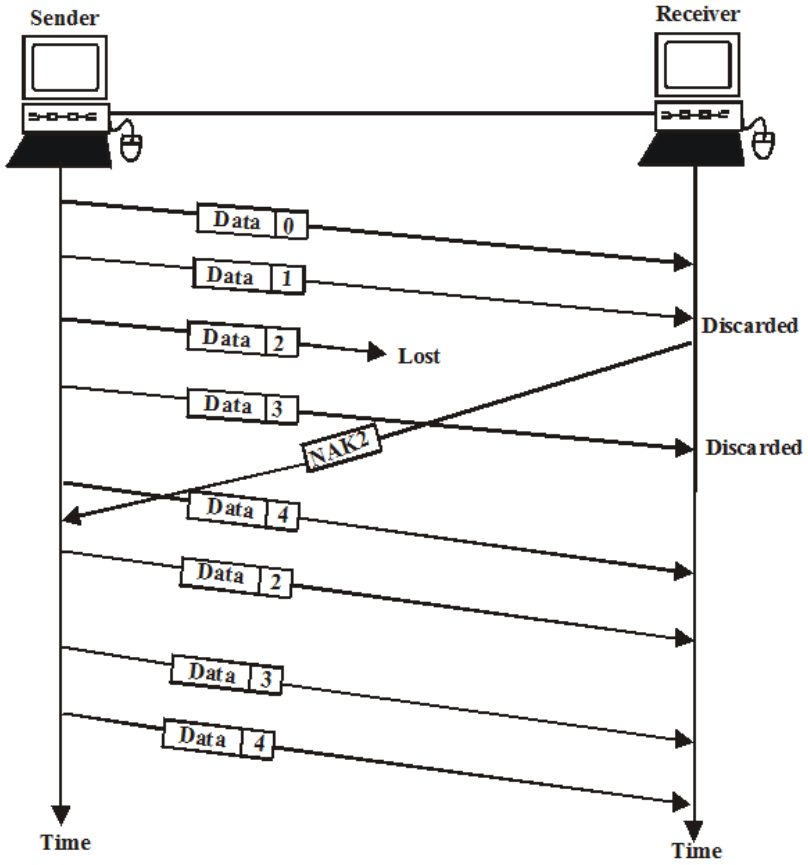
frame itself.
- The sending device is equipped with a timer enable it to handle lost acknowledgements.

Go- Back –n ARQ
- Here if one frame is lost or damaged, all unacknowledged frames are sent.

Damaged Frame
- As soon as the receiver discovers an error, it stops accepting, subsequent frames until the damaged frame is replaced correctly.
- The receiver immediately sends NAK with number of the damaged frame.

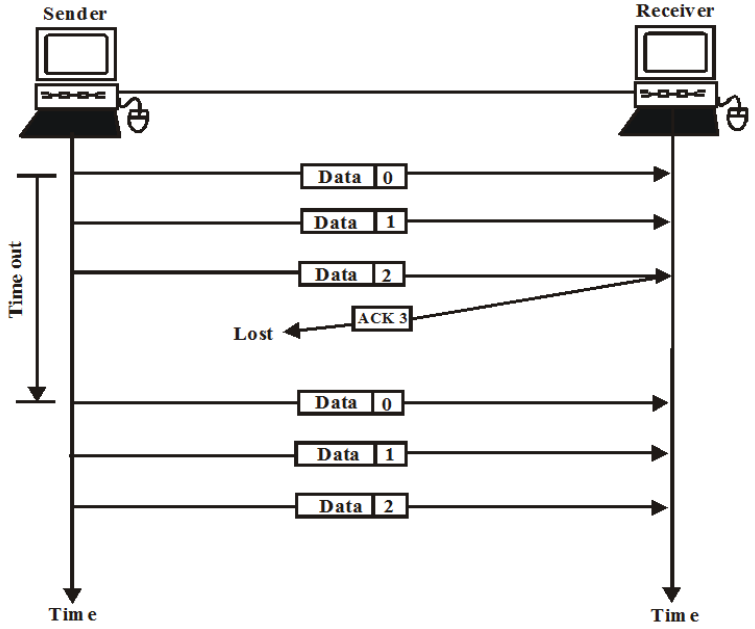
Lost Data Frame

- If frames are lost due to noise, the next frame that arrives at the receiver will be out sequence. The receiver checks the sequence and sends a NAK for the first missing frame.
- A NAK does not indicate whether the frame has lost or damaged, just that it need to be resent.
- The sender then transmits the frame indicated by the NAK and all other frames that it has transmitted after the lost one.



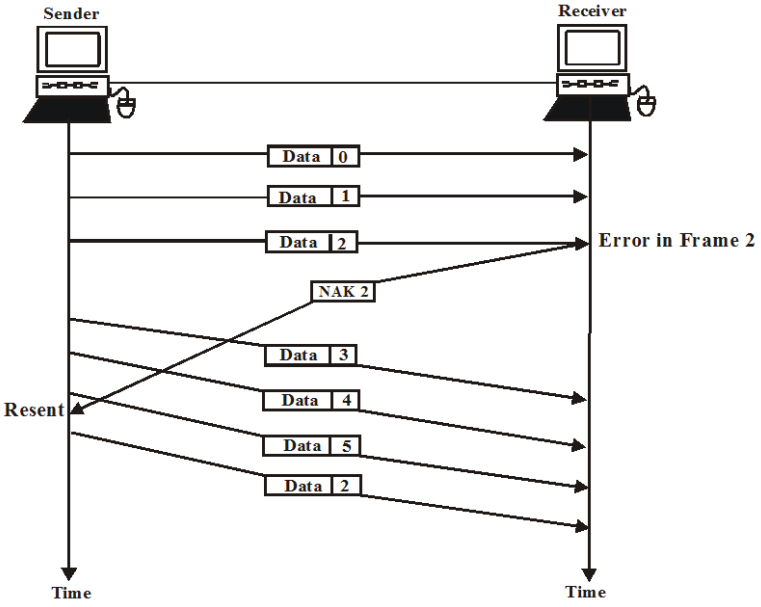
Lost Acknowledgement
- Sender keeps on sending the frames as the window allows before waiting for an acknowledgment.
- Once the limit has been reached for the sender such that no more frames to send, it must wait for an acknowledgment.
- If ACK/NAK sent by the receiver is lost, the senders will never receiver it.

- The sender is equipped with timer that begins that counting whenever the window capacity is reached.
- If no acknowledgment is received within time the sender retransmits every frame transmitted since last acknowledgement received. Selective Reject ARQ
- In selective reject ARQ, only the specific damaged or lost frame is retransmitted



Damage Frame

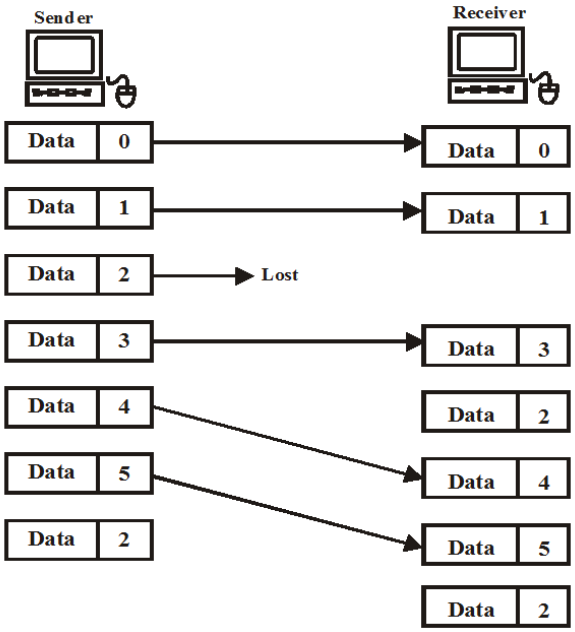
- If a frame is corrupted in corrupted in transit a NAK is returned and the frame is resent out of sequence.
- The receiving device must be able to sort the frames and insert the corrected frame up to its proper place in the sequence.
- The receiving device sorts all the sort frames received after NAK is issued to recorder the frames received out of sequence.



Lost Frame

- In selective –reject ARQ, frames can be accepted out of sequence but cannot be acknowledgment out of sequence.

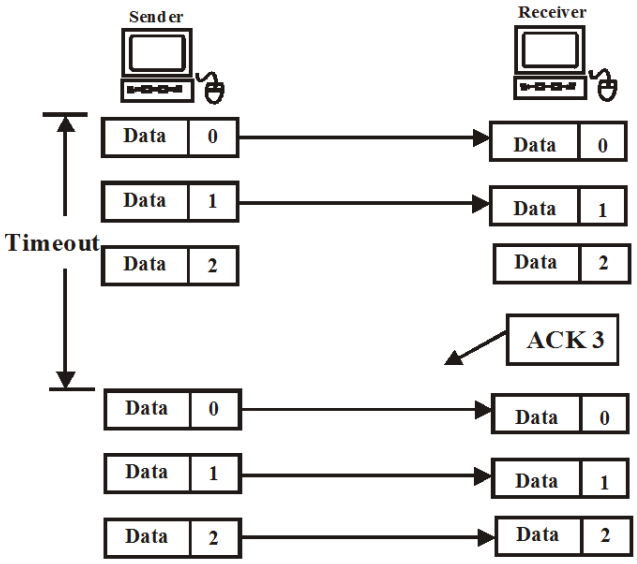
- If a frame is lost, the next frame will arrive out of sequence. Receiver after reordering returns a NAK for the missing frame.
- The NAK frame does not indicate whenever the frame has been lost or damaged; it just needs to be resent. Sender then retransmits the frame indicated by the NAK.



Lost Acknowledgement

If ACK/NAK sent by the receiver is lost, the sender will never receive it. The sender doesn't expect ACK frame for every data frame it sends.

- The sender keeps on sending the frames as many as the window allows before waiting for an acknowledgment.
- Once the limit of window has been reached or the sender has no more frames to send it must wait for an acknowledgment.
- The sender is equipped with a timer that begins counting whenever the window capacity is reached.
- If no acknowledgement is received within time limit, the sender retransmits every frame transmitted since the last ACK.

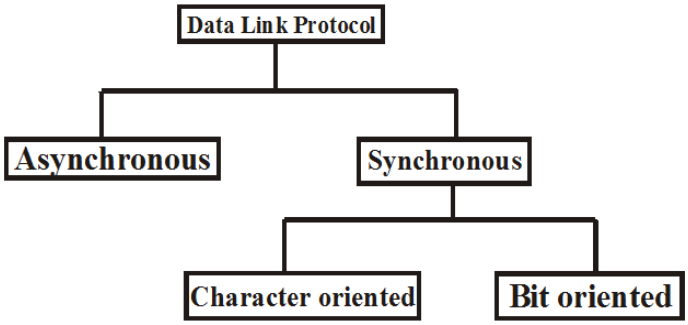


2.4.4 Utilization of Channel

Utilization(U)/ Efficiency of Channel(E)=w/1+2a

Where, w= sliding window size, n= No.of bits required for sequencing frames
W=1 for Stop and Wait ARQ
$W=2^n - 1$ for Go-Back-N ARQ
$W=2^{n-1}$ for Selective Repeat or Selective Reject ARQ
a=Propagation Delay / Transmission Delay

2.5 DATA LINK PROTOCOLS



IMP:
Data link protocols are sets of specifications used to implement the data link layer.
Data link protocols can be divided into two subgroups:
i) Asynchronous protocols
ii) Synchronous protocols

i) Asynchronous Protocols
IMP:
In a asynchronous transmission, a data unit is transmitted with no timing coordination between the sender and receiver. A receiver does not need to know exactly when a data unit is sent, it only needs to recognize the beginning and end of the data unit. This is accomplished by using extra bits i.e. start and stops bits to frame the unit. Due to addition of start and stops bits extends spaces between frames, asynchronous protocols are extremely slow.

Example: XMODEM, YMODEM, ZMODEM, BLAST, KERMIT

ii) Synchronous Protocols
Synchronous protocols can be divided into two classes: (a) Character oriented protocols (b) Bit oriented protocols. In Character oriented protocols, also called as byte oriented protocols, the frame is interpreted as a series of characters. Each character composed of one byte. All control information is in the form of an existing character encoding system.

Example:
ASCII characters
In Bit oriented protocols, the frame is interpreted as a series of bits. Each bit or group of bits have meaning depends on their placement in the frame. Control information in a bit oriented protocol can be one or multiple bits.

Example:
SDLC, HDLC

2.5.1 HIGH LEVEL DATA LINK CONTROL PROTOCOL (HDLC)

HDLC is the most important data link control protocol.
Basic Characteristics:
To satisfy a variety of applications, HDLC defined

- Three types of stations
- Two link configurations
- Three data transfer modes of operation

2.5.2 TYPES OF STATIONS

Primary station	Has the responsibility for controlling the operation of the link. Frames issued by the primary are called commands.
Secondary station	Operates under the control of the primary station. Frames issued by a secondary are called responses. The primary maintains a separate logical link with each secondary station on the line
Combined station	Combines the features of primary and secondary. A combined station may issue both commands and responses.

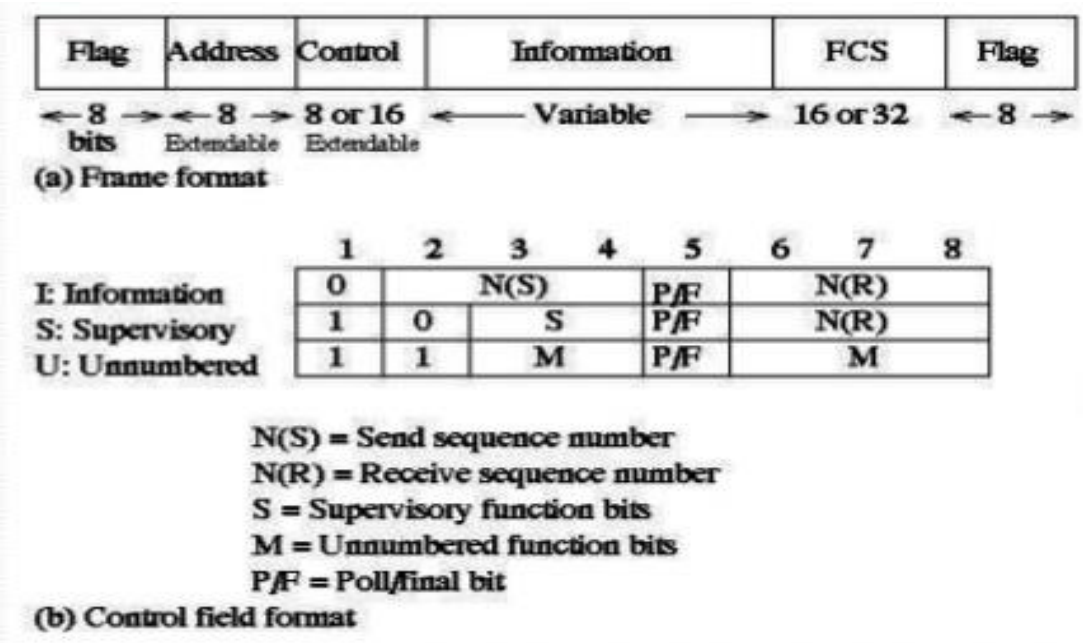
2.5.3 TWO LINK CONFIGURATIONS

Unbalanced Configuration	Consists of one primary and one more secondary and supports both full-duplex and half-duplex transmission.
Balanced Configuration	Consists of two combined stations and supports both full-duplex and half-duplex transmission.

2.5.4 THREE DATA TRANSFER MODES

Normal Response Mode(NRM)	Used with an unbalanced configuration. The primary may initiate data transfer to a secondary, but a secondary may only transmit data in response to a command from the primary
Asynchronous Balanced Mode (ABM)	Used with a balanced configuration. Either combined station may initiate transmission without receiving permission from the other combined station.
Asynchronous Response Mode(ARM)	Used with an unbalanced configuration. The secondary may initiate transmission without explicit permission of the primary. The primary still retains responsibilities for the line, including initialization, error recovery and logical disconnection.

2.5.5 FRAME STRUCTURE



HDLC uses synchronous transmission. All transmission are in the form of frames and a single frame format suffices for all types of data and control exchanges.

Header:
The flag, address and control fields that precede the information field.

Trailer:
The FCS flag fields following the data field.

2.5.6 Flag Fields

Flag fields delimit the frame at both ends with the unique pattern 01111110. The data is bit stuffed at the transmitter and unstuffy at the receiver. While receiving a frame, a station continues to hunt for that sequence to determine the end of the frame. Because the protocol allows the presence of arbitrary bit patterns there is no assurance that the pattern 01111110 will not appear somewhere inside the frame, thus destroying synchronization. To avoid this problem, a procedure known as bit stuffing is used. Between the transmission of the starting and ending flags, the transmitter will always insert an extra 0 bit after each occurrence of five Is in the frame. After detecting a starting flag, the receiver monitors the bit stream. When a pattern of five bit is a 0, the combination is accepted as a flag. If the sixth and seventh bits are both 1, the sender is indicating an abort condition.

2.5.6.1 ADDRESS FIELDS

The address fields identify the secondary station that transmitted or is receive the frame. The address field is usually 8 bits long but, by prior agreement, an extended format may be used din which the actual address length is a multiple of 7 bits. The leftmost bit of each octet is 1 or 0 according as it is or is not the last octet of the address field. The remaining 7 bits of each octet form part of the address. The single-octet address of 1111111 is interpreted as the all-stations address in both basic and extended formats. It is used to allow the primary to broadcast a frame for reception by all second aries.

2.5.6.2 CONTROL FIELDS

HLDC defines three types of frames, each with a different control field format.

Information frames (I-frames)	They carry the data to be transmitted for the user. Additionally flow and error control data using the ARQ mechanism are piggybacked on an information frame.
Supervisory frames (S-frames)	They provide the ARQ mechanism when piggybacking is not used.
Unnumbered frames (U-frames)	They provide supplemental link control functions.

2.5.6.3 INFORMATION FIELD

The information field is present only 1-frames and some U-frames. The field can contain any sequence of bits but must consist of an integral number of octets. CRC-CCITT. An optional 22-bit FCS, using CRC-22, may be employed if the frame length or the line reliability dictates this choice.

2.5.6.4 FRAME CHECK SEQUENCE FIELD

FCS is an error-detecting code calculated frame the remaining bits of the flags, exclusive of flags and uses 16-bit CRC

2.5.6.5 OPERATION

The operation of HDLC involves three phases:

1) **Initialization:**
   Initialization may be requested by either side. The command serves three purposes:
   a) it signals the other side that initialization is requested.
   b) It specifies which of the three modes (NRM, ABM, and ARM) is requested.
   c) It specifies whether 2- or 7 bit sequence numbers are to be used.
   If the other sides accept this request, then the HDLC module on that end transmits an unnumbered acknowledged (UA) frame back to the initiating side. If the request is rejected, then a disconnected mode (DM) frame is sent.
2) **Data Transfer**
   When the initialization had been requested and accepted then a logical connection is established both sides may begin to send user data in I-frame, starting with sequence number 0. The N(S) and N(R) fields of the I-frame are sequence numbers that support flow control and error control.
3) **Disconnect**
   Either HDLC module an initiate a disconnect, either on its own initiative if there is some sort of fault, or at the request of its higher-layer user. HDLC issues a disconnected by replying with a UA and informing its layer 2 user that the connection has been terminated. Any outstanding unacknowledged I-frames may be and their recovery is the responsibility of higher layers.

2.6 IEEE LAN STANDARDS

A local area network (LAN) is data communication system that allows a number of independent devices to communicate directly with each other in a limited geographic area.

2.6.1 PROJECT 802

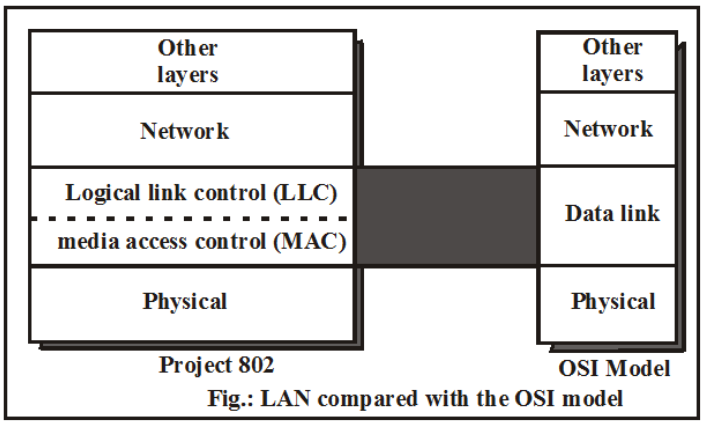


Fig.: LAN compared with the OSI model

In 1985, the computer society of IEEE developed project 802. It covers the first two layers of the OSI model and part of the third level.
The IEEE subdivided the data link layer into two sub layer-logical link controls, media access control

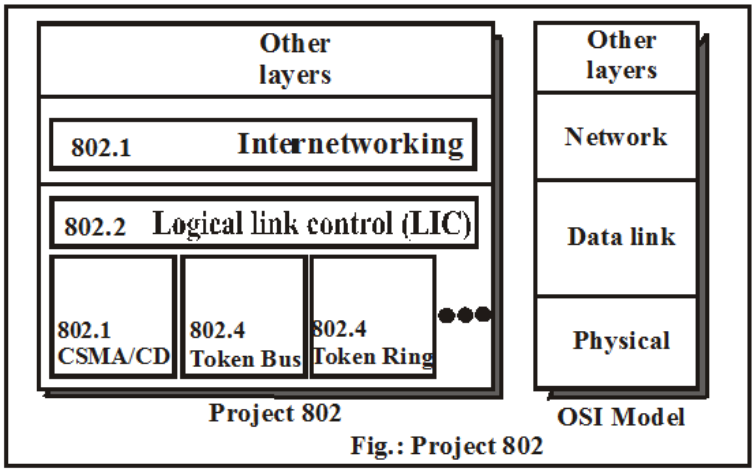


Fig.: Project 802

The IEEE project 802 model takes the structure of HDLC frame and divides it into 2 sets of function.
One set contains the end user portions of the frame
- The logical address
- The control information
- Data

These functions are handled by IEEE 802.2 LIC protocol. LIC is considered the upper layer of the IEEE 802 data link layer and is common LAN protocol.

2.6.2 MEDIUM ACCESS CONTROL (MAC)

MAC sub layer provides an access to the shared media. It contains the synchronization flag flow and error control specifications necessary to move information from one place to another, as well as the physical address of the next station to receive and route a packet.
MAC functions include:

1) At transmitter, assemble data into frame with address and error detecting field.
2) At receiver, dissemble frame, frame perform address recognition and error detection.
2) Govern access to the LAN transmission media.

2.6.3 MAC FRAME FORMAT

The MAC layer receives a block of data from the layer and is responsible for performing functions related to medium access and for transmitting data.

MAC Control	Destination MAC address	Source MAC address	LLU PDU	CRC

Standardized Medium Access Control Techniques Round Robin with Round Robin each station in turn is given the opportunity to transmit. During this time, the station may decline to transmit or may transmit. In any case, the station when it is finished, relinquishes its turn and the right to transmit passes to the next station in logical sequence.

2.6.4 LOGICAL LINK CONTROL

LLC services
LLC specifies the mechanism for addressing stations across the medium and for controlling the exchange of data between two users. The operation and format this standard is based on HDLC.
Some services are provided:

1) **Unacknowledged connectionless service:**
   It is very simple service that does not involve any of the flow and error control mechanism. Thus, the delivery of data is not guaranteed.
2) **Connection – mode service:**
   This service is similar to that offered by HDLC. A logical connection is set up between two users exchanging data and flow control and error controls are provided.
2) **Acknowledged connectionless service:**
   It provides that data are to be acknowledged but no prior logical connections is setup.

Note:

- The unacknowledged connectionless service requires minimum logic.
- The connection mode service could be used in very simple devices such as terminal controller.

2.7 LLC PROTOCOL

The basic LLC protocol is modelled over HDLC and has similar functions and formats.

1) LLC makes use of the asynchronous, balanced mode operation of HDLC in order to support connection mode LLC service. This is type-2 operations.
2) LLC supports a connections service using the unnumbered information PDU. This is type -1 operation.
2) LLC supports an acknowledged connectionless service by using by two Unnumbered PDU's.
   This is type-2 operation.

2.7.1 LLC-PDU

The data unit in the LLC level is called the protocol data unit.

DSAP	SSAP	Control	Information

DSAP – Destination service Access point
SSAP – Source service Access point
Control – The control field of PDU is identical to the control field in HDLC. All the LLC protocols employ the same PDU format. The DSAP and SSAP fields each contain 8 bit addresses which specify the destination and source users of LLC.

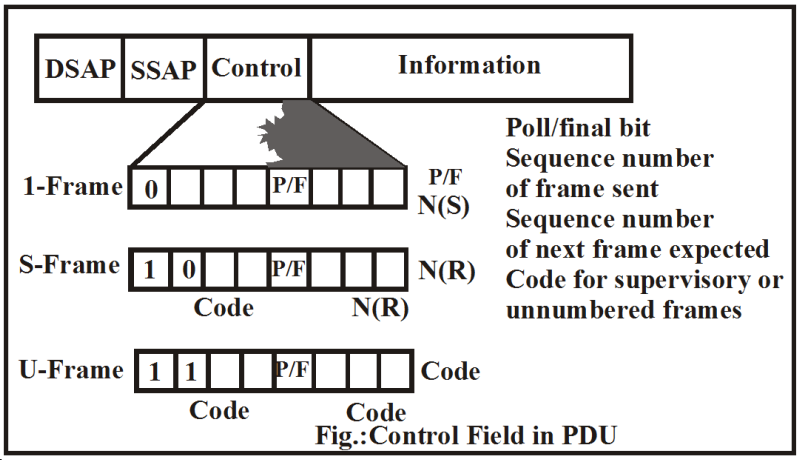


Fig.:Control Field in PDU

- MSB bit of DSAP indicates whether the DSAP is an individual or group address. MSB bit of the SSAP indicates whether the PDU is a command or response PDU.
- For type-1 operation (unacknowledged connectionless service) the unnumbered information (UI) PDU is used for data transfer. There is no acknowledgement flow control or error control. However there is error diction and discard at the receiver.
- For type-2 operation (connection mode) data link connection is established setting two LLC SAP's prior to data exchange. The LLC entity issues a SAMBE PDU to request a logical connection with the other LLC entity. If the connection is accepted by the LLC user designated by the DSAP, then the destination LLC entity returns an unnumbered acknowledgement (UA) PDU. The connection is henceforth uniquely identified by the pair of user SAP's If the destination LLC users rejects the connection request, its LLC entity returns a disconnect mode (DM) PDU.
- Once the connection is established, data is exchanged using the information PDU (I-frame PDU). The information PDU includes send and receives sequence numbers for sequencing and flow control. The supervisory PDU are used as in HDLC for flow control and error control. Either LLC entity can terminate a logical LLC connection by issuing a disconnect (DISC) PDU.
- With type-2 operation (Acknowledged connectionless service) each transmitted PDU is acknowledged. A new unnumbered PDU, the acknowledged connectionless (AC) information PDU is defined. User data are sent in AC command PDU and must be acknowledged using the AC response PDU. To guard against lost PDU, a 1 bit sequence numbered is used. The sender alternative the use of 0 and 1 in its AC command, only one PDU and receiver responds with an AC PDU. With the opposite number of the corresponding command, only one PDU in each direction may be sent at any time.

2.8 ALOHA

ALOHA uses ground based radio broadcasting. The basic idea is applicable to any system in which uncoordinated users are competing for the use of signal shared channel. The ALOHA system was connected to allow radio communication between machines. The two versions of ALOHA
- Pure ALOHA
- Slotted ALOHA

2.8.1 PURE ALOHA

Every station wishing to transmit is allowed to transmit. If more than one device attempt to transmit at the same time, there will be collision and the transmitted frame will be destroyed. A sender waits for a reasonable amount f time for an acknowledgement. If there is no acknowledgment the station assumes that a collision has occurred and retransmits the frame.

Receiving station, examines the frame for address detection. If the address is recognized it checks for error if any. If a received frame is valid then immediately sends an acknowledgment. If a received frame is not valid, it simply ignores the frame because the no. of collisions rises rapidly with increased load. The maximum utilization of the channel is only about 18%. To improve efficiency a modification of ALOHA known as slotted ALOHA was developed.

Whenever two frames try occupying the channel at the same time, there will be a collision and both will garbled. If the first bit of anew frame overlaps with just the last bit of a frame almost finished cannot frames will be totally destroyed and both will have to be retransmitted later. The checksum cannot (and should not) distinguish between a total loss and a near miss.

2.8.2 SLOTTED ALOHA

In this scheme, the time on the channel is divided into discrete intervals, each interval corresponding to frame transmission time. This approach requires the users to agree of slot boundaries. Transmission is permitted to begin only at a slot boundary. Thus continuous pure ALOHA is turned into a discrete one. This increase to the maximum utilization of the channel to about 27%. Both ALOHA exhibit poor utilization. Both fail to take the advantage that the propagation delay between stations is usually very small compared to frame transmission time.

2.8.3 EFFICIENCY OF ALOHA CHANNEL

Let the ‘frame time’ denote the amount of the time needed to transmit the standard fixed length frame. Let S be the average no. of new frames generators / frames time. If $S > 1$, the user is generating frames at a higher rate than the channel can handle and nearly every frame will suffer collision. For reasonable throughput we expect $0<S<1$.In addition to the new frames, the station also generate retransmission of frames that previously suffered collisions.

Let G be the average no. of transmission attempts (old + new) per frame time. Clearly $G \geq S$.

- At low load (i.e. $S \approx 0$) there will be few collisions and here hence retransmission so G =

S.

- At high load, there will be few collisions, so G > S.
- Under all load, S = GP$_0$ where P$_0$ is the probability that a frame does not suffer collision. A frame will not suffer a collision if no other frames are sent within one frame time of its start as shown:

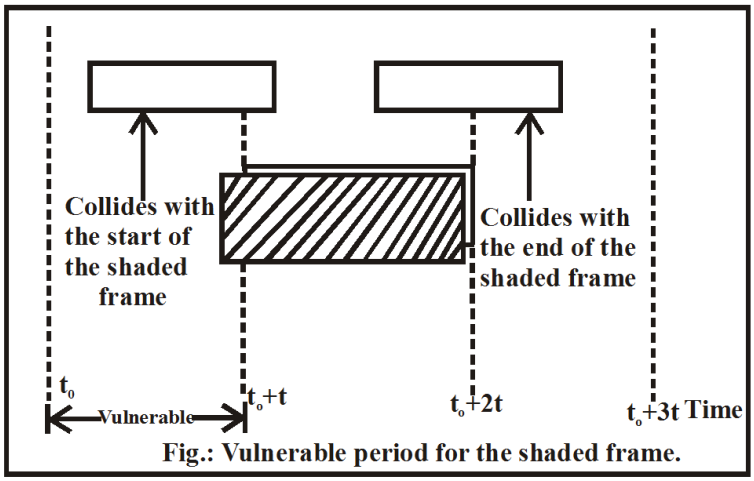


Fig.: Vulnerable period for the shaded frame.

Let t be the time required to send a frame. If any other user has generated a frame between time t$_0$ and t$_0$ + t, the end of that frame will collide with the shaded one. Similarly any other frame started between t$_0$ + t and t$_0$ + 2t will collide with the end of the shaded one. If the frame starts after t$_0$ + 2t time, there given by Poisson distribution

$$P_k = \frac{G^k e^{-G}}{K!}$$

The probability of zero frames is e^{-G}. In an interval two frame times long the average no. of frames generated is 2G. The probability of no other traffic being initiated i.e. zero frame generated during the entire vulnerable period is thus given by

$P_0 = e^{-2G}$

With $S = GP_0$ we get $S = G.e^{-2G}$

The maximum throughput occurs at G = 0.5.

When G = 0.5, $S = (0.5)\, e^{-2(0.5)} = \frac{1}{2e} = 0.184$

That means channel utilization is 18.44.

With slotted ALOHA, station is required to wait for the beginning of the next slot. The probability of no other traffic during the time is thus $P_0 = e^{-G}$ and then

$S = GP_0 = G\, e^{-G}$

Max. Through occurs at G = 1

$S = G\, e^{-G} = e^{-1} = 1/e = 0.268$

That means channel utilization is 26.8% i.e. nearly 27% successes. Operating at higher value of G reduces the number of empties but increase the number of collisions. The probability that it will avoid collision = e^{-G} . Then, the probability of collision is = $(1 - e^{-G})$

The probability of a transmission requiring exactly k attempts i.e. (k – 1) collisions followed by one success is

$P_k = e^{-G}(1 - e^{-G})^{k-1}$

The expected number of transmission E

$$E = \sum_{k=1}^{\infty} k.P_k = \sum_{k=1}^{\infty} k.e^{-G}(1-e^{-G})^{k-1} = e^{G}$$

2.9 IEEE 802.3 AND ETHERNET

IEEE 802 defines two categories
i) Baseband and
ii) Broadband

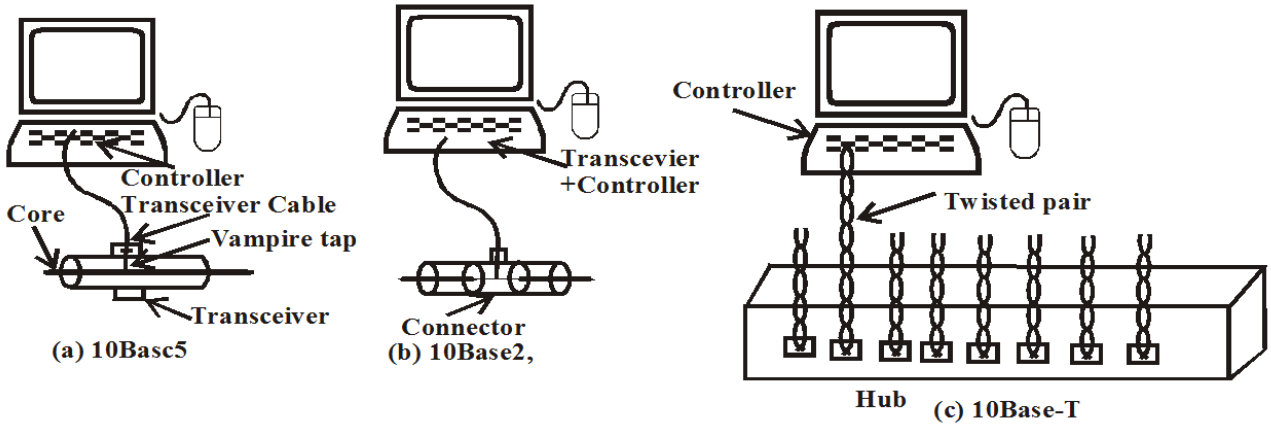
Baseband
IMP:
Baseband uses digital Manchester encoding techniques.

2.9.1 BASEBAND STANDARDS:

Name	Cable	Max. Segment	Nodes / Seg.	Advantages
10 Base 5	Thick coax	500 m	100	Good for background
10 Base 2	Thin coax	200 m	20	Cheapest system
10 Base T	Twisted pair	100 m	1024	Easy maintence
10 Base- F	Fiber optics	2000 m	1024	Best between buildings

2.9.2 CABLING

Five types of caballing are commonly used, as shown in above table. 10 Base5 cabling is called thick Ethernet. Connections to it are generally made using Vampire taps, in which a pin is carefully forced halfway into the coaxial cables core. The notation 10Base5 means that it operate at 10 Mbps, uses baseband signaling, and can support segments of up to 500 meters.
The second cable was **10Base2** or thin Ethernet, bends easily. Connections to it are made using industry standard BNC connectors to form T junction. These are easier to install, but it can run for only 200 meters and can handle only 20 machines per cable segment.
The problem of finding cable breaks require all stations to have a cable running to a central hub. Pairs require the use of label called 10Base- T.



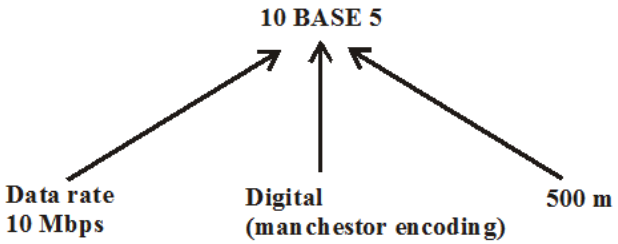
For **10Base5**, a transceiver is clamped securely around the cable so that its tap makes contact with the inner core. The transceiver contains the electronic that handle carrier detection and collision deception. When a collision is detected, the transceiver also puts a special invalid signal on the cable to ensure that all other transceivers also realize that a collision has occurred. With **10Base –T,** there is just the hub. Adding or remove a station is simpler in this configuration, and cable breaks can be detected easily. The disadvantage of

10Base-T is that the maximum cable run form the hub is only 100 meters; the most 150 meters if high quality (category 5) twisted pairs are used. Also a large hub costs thousands of dollars. A fourth cabling option for 802.2 is **10 Base-F,** which uses fiber optics. This alternative is expensive due to the cost of the connectors and terminators, but it has excellent noise immunity and is the method of choice when running between building or widely separated hubs.

Notation

< Date Rate > < Signaling > < Max segment length in hundred of meters >(in Mbps)

Example:



2.9.3 BROADBAND

Broadband uses analog PSK encoding standard.

e.g. 10 BROAD 26

Ethernet LAN consists of co-axial called ether to which multiple computers connect.

Ethernet implements all IEEE 802.2 standards. Ethernet is a bus network in which computers share a signal transmission media. While one computer transmits a frame to another, all other computers must wait. Sharing in LAN technologies does not mean that multiple frames are being sent at the same time. Instead the sending device has exclusive use of the entire cable during the transmission of a given frame, other computers must wait. After one computer finishes transmitting one frame, the shard cable becomes available for other devices to use.

2.9.4 ACCESS METHOD

Carrier sense Multiple Access (CSMA)

With CSMA, a station wishing to transmit first listen to the cable to determine if there is any traffic on the line i.e. if another transmission is in progress. A device listen by checking the voltage on the line (called carrier sense). If the voltage is detected (line is busy) the station must wait. If no voltage is detected (line is idle) the station may transmit. It may happen that two or more station attempt to transmit at about the same time. If this happens, there will be a collision, data from both the station will get corrupted and therefore cannot be received correctly. To account for this, a station waits for a reasonable amount of time after transmitting, for an acknowledgment. If there is no acknowledgement, the stations assume that a collision has occurred and retransmits.

Here the receiving stations must contend in order to respond. Average frames transmission time is much than the propagation time. Collision can occur when more than one user begins transmitting within a short time i.e. during the period of the propagation delay.

If a station begins to transmit a frame, and there is no collision during the time it takes for the leading edge of the packet to propagation to farthest station, then there will be no collision for this frame because all other stations are now aware of the transmission. With CSMA, a station wishing to transmit listens to the medium and obeys the following rules:

i) If the medium is idle, transmit otherwise go to step – ii.
ii) If the medium is busy, continue to listen until the channel is sensed idle, and then transmit immediately.

If two more stations are waiting to transmit, a collision is guaranteed. Things get sorted only after the collision. The max utilization the CSMA is far better than that of ALOHA or slotted ALOHA. The maximum utilization depends on the length of the frame and on the propagation time. The longer the frame or the shorter the propagation time the higher the utilization

2.9.5 PERSISTENT AND NON PERSISTENT CSMA

The first carrier sense protocol is called **1 – persistent CSMA** (Carrier Sense Multiple Access). When a station has data to send, it first to the channel to see if anyone else is transmitting at that moment. If the channel is busy, the stations wait until it becomes idle. When the station detects an idle channel, it transmits a frame. If a collision occurs, the station waits a random amount of time and starts all over again. The protocol is called 1 – persistent because the stations transmit with a probability of 1 when it finds the channel idle. A second carrier sense protocol is **non persistent CSMA** .In this protocol, a conscious attempt is made to be less greedy than in the previous one. Before sending, a station senses the channel. If no one else is sending, the station begins doing so itself. However, if the channel is already in use, the station does not continually sense it for the purpose of seizing it immediately upon detecting the end of the pervious transmission. Instead, it waits a random period of time and then repeats the algorithm. Consequently, this algorithm leads to better channel utilization but longer delay than 1- persistent CSMA. The last protocol is **p–persistent CSMA.** It applies to slotted channels and works as follows. When a station becomes ready to send, it senses the channel. If it is idle, it transmits with a probability p. With a probability q = 1- p, it defers until the next slot. If that slot is also idle, it either transmits or defer again, with probabilities p and q.
This process is repeated until either the frame has been transmitted or another station has begun transmitting. In the latter case, the unlucky stations act as if there has been a collision (i.e., it waits a random time and starts again). If the station initially senses the channel busy, it waits until the next slot and applies the above algorithm. Binary exponential back off means that an Ethernet can recover quickly after collision because each computer agrees to wait longer times between attempts when the cable busy. In the unlikely event that two or more devices choose delay that are approximately equal, exponential back off guarantees that contention for the cable will be reduced after a few collisions.

2.9.6 IEEE 802.3 MAC FRAME

IEEE 802.3 specifies one type of frame containing seven fields.
Ethernet does not provide any mechanism for acknowledging received frames.
Acknowledgement must be implemented at the higher layers. The format of the MAC frame in CSMA/CD is:

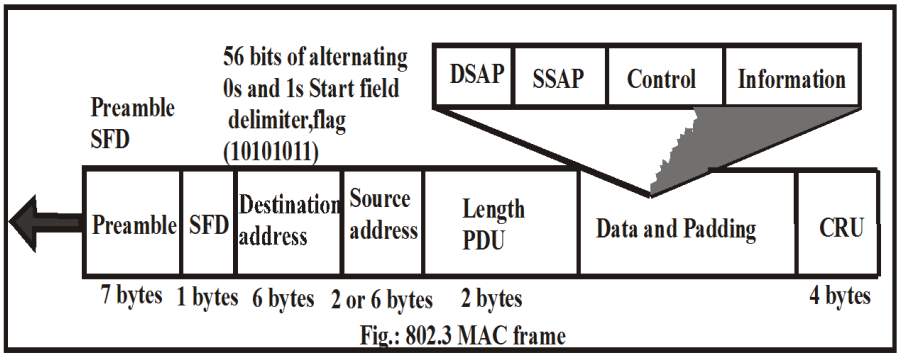


Fig.: 802.3 MAC frame

1. **Preamble:**
   It contains 7 bytes (56 bits) of alternate 0s and 1s that alert the receiving system to the coming frame and enable it to synchronize its input timing.
2. **Start frame Delimiter (SFD):**
   The SFD byte containing the sequence 10101011 indicates the actual start of the frame. The SFD tells receiver that everything that follows is data starting with the addresses.
3. **Destination Address (DA):**
   The DA field is 2 or 6 byte long and contains the physical address of the intended receiver.
4. **Source Address (SA):**
   The SA field is 2 or 6 byte long and specifies the address of the stations that sent the frame.
5. **Length:**
   These 2 bytes indicates the number of bytes in PDU.
6. **LLC data:**
   This is the data unit supplied by LLC PDU can be 46 to 1500 bytes long depending on the type of frame padding and the length of the information field.
7. **CRC:**
   A 22 bit cyclic Redundancy Check.

2.10 LMR (LAST MINUTE REVISION)

- The second layer in the OSI model, the data link layer, has three main functions: line discipline, flow control, and error control.
- Line discipline establishes the status of a device (sender or receiver) on a link.
- ENQ/ACK is a line discipline method used in point – to – point connections.
- The receiving using data or ENQ/ACK line discipline responds with an acknowledged (ACK) if it is ready to receive data or a negative acknowledgement (NAK) if it is not ready.
- Poll/select is a line discipline method. The primary device always initiates communication with either a poll to receive ort (SEL) frame.
- A SEL frame is sent from the primary from the primary device to the secondary device to tell the secondary to prepare to receive data. The secondary responds with an ACK or a NAK.
- Flow control is regulation of data transmission so that the receiver buffer does not become overwhelmed by data.
- There are two main methods of flow control:
  (i) Stop and Wait

(ii) Sliding window

- In stop and wait flow control, each frame must be acknowledged by the receiver before the next frame can be sent. Only one frame can be sent at a time.
- In sliding window flow control, the sending of data is constrained by an imaginary window that expands and contracts according to the acknowledgement received by the sender. Many frames can be sent.
- Utilization(U)/ Efficiency of Channel(E)=w/1+2a
  Where, w= sliding window size, n= No.of bits required for sequencing frames
  W=1 for Stop and Wait ARQ
  $W=2^n - 1$ for Go-Back-N ARQ
  $W=2^{n-1}$ for Selective Repeat or Selective Reject ARQ
  a=Propagation Delay / Transmission Delay

- The receiving of data is constrained by an imaginary window that expands and contracts according to the data received.
- Error control, or how to or damaged data or acknowledges, is simply the retransmission of data.
- A protocol in data communication is a group of specifications used to implement one or more layers of the OSI model.
- Data link protocols can be classified as synchronous or asynchronous.
- Asynchronous protocols such as XMODEM, YMODEM, ZMDOEM, BLAST and Kermit are used in file transfer.
- Synchronous protocol, can be divided in two characters oriented and bit oriented.
- In character oriented protocols, the frame is interpreted as a series of characters.
- All bit – oriented protocols, are related to high – level data link control (HDLC)
- HDLC operates in half or full-duplex mode in a point – to –point or multiport link configuration.
- HDLC stations are categorized as:
  (i) Primary station - sends command
  (ii) Secondary - sends responds
  (iii) Combined station- sends commands and responds
- HDLC stations are configuration as:
  (i) Unbalanced - one primary, one or second daries
  (ii) Symmetrical - two physical stations, each capable of switching from Primary secondary.
  (iii) Balanced - two combined stations,
  each of equal status.
- HDLC stations communication in one of three modes:
  (i) Normal responds mode (NRM) - the secondary station needs permission To transmit
  (ii) Asynchronous response mode (ARM) -the secondary station does not need Permission to transmit.
  (iii) Asynchronous balanced mode (ABM)- either combined station may initiate Transmission.
- HDLC protocol defines three types of frames:
  (i) Information frame (I- frame)-for data transmission and control
  (ii) Supervisory frame (S – frame) -for control
  (iii) Unnumbered frame (U- frame) - for control and management

- HDLC handles data transparency by adding a 0 whenever there are five consecutive 1s following a.0. This is called bit stuffing.
- The purpose of the IEEE's project 802 is to set up standard so that LAN equipment manufactured by different companies is stuffing.
- Project 802 divides the data link layer into sub layers:
  (i) Logical link control
  (ii) Medium access control (MAC)
- Three LANs specified by project 802 are:
  (i) Ethernet (802.3)
  (ii) Token bus (802.4)
  (iii) Token ring (802.5)
- CSMA/CD operators as followings: Any station may listen to the line to determine if the line is clear, transmission can commence. If a collection occurs, a transmission stops the process is repeated.
- Fiber distributed data interface (FDDI) is a LAN protocol using optical fiber as a medium, with a 100 Mbps data rate.
- FDDI consists of a primary ring for data transmission and a secondary ring that assists in failure situations.
- The data link layer transform the physical layer to a reliable link and responsible for node- to- node delivery.
- Data gets corrupted during transmission for reliable and efficient commutation; errors must be detected and corrected.
- Unpredictable interference from heat, magnetism and other forms of electricity on the signals which may change the shape or timing of it is called errors.
- The term single-bit error means that only one bit in the data unit has changed i.e. it can either be from 1 to 0 or form 0 to 1.
- The term burst error means that two or more bits in the data unit have changed i.e. either changed from 1 to 0 or changed from 0 to 1.
- For dealing with errors, one can include enough redundant information along with each bock of data sent to enable the receiver to deduce what the transmitted character must have been. This strategy uses error- correcting codes.
- For dealing with error. One can include only enough redundancy to allow the receiver to deduce that an error occurred, but not which error, and have it request a retransmission. The strategy uses error- detecting codes.
- Data link protocols are sets of specifications used to implement the data link layer.
- In asynchronous transmission, a data unit is transmitted with no timing coordination between the sender and receiver.
- A local area network (LAN) is a data communication system that allows a number coordination between the devices to communicate directly with each other in a limited geographic area.
- Baseband uses analog digital man Chester encoding techniques.
- Broadband uses analog PSK encoding standard.
- Ethernet LAN consists of co-axial called ether to which multiple computers connect. Ethernet implements all IEEE 802.3 standards.
- Monitoring a cable during transmission is known as collision Detect and the mechanism is called CSMA/CD.
- Binary exponential back off means that an Ethernet can be recovered quickly after a collision because each computer aggresses to wait longer times between attempts when

the cable becomes busy.

- The standard 802.4 describes a LAN called Token bus.
- Token bus combines the physical configuration of Ethernet and the collision free feature of token ring. Token bus is a physical bus that operators as a ring using tokens.
- The standard 802.5 describes a LAN called token ring. Synchronous here refers to information that is sensitive. While asynchronous refers to information that is not time sensitive

GATE QUESTIONS

Q.1 Host A is sending data to host B over a full duplex link. A and B are using the sliding window protocol for flow control. The send and receive window sizes are 5 packets each. Data packets (sent only from A to B) are all 1000 byte long and the transmission time for such a packet is 50μs Acknowledgement packets (sent only from B to A) are very small and require negligible transmission time. The propagation delay over the link is 200 μs. What is the maximum achievable throughput in this communication? (Bytes/sec)

a) 7.69×10^6 b) 11.11×10^6
c) 12.33×10^6 d) 15.00×10^6

[GATE-2003]

Q.2 In a data link protocol, the frame delimeter flag is given by 0111. Assuming that bit stuffing is employed, the transmitter sends the data sequence 01110110 as

a) 01101011 b) 011010110
c)011101100 d)0110101100

[GATE-2004]

Q.3 In a sliding window ARQ schemes, the transmitter's window size is N and the receiver's window size is M. The minimum number of distinct sequence numbers required to ensure correct operation of the ARQ scheme is

a) min(M, N) b) max(M, N)
c) M +N d) MN

[GATE-2004]

Q.4 A 20 Kbps satellite link has a propagation delay of 400 ms. The transmitter employs the "go back n ARQ" scheme with n set to 10. Assuming that each frame is 100 bytes long, what is the maximum data rate possible?

a) 5 Kbps b) 10 Kbps
c) 15 Kbps d) 20 Kbps

[GATE-2004]

Q.5 Consider a parity check code with three data bits and four parity check bits. Three of the code words are 0101011,1001101 & 1110001. Which of the following are also code words?

I. 0010111 II. 0110110
III. 1011010 IV. 0111010

a) I and III b) I,II and III
b) II and IV d) I, II, III and IV

[GATE-2004]

Q.6 The maximum window size for data transmission using the selective reject protocol with n-bit frame sequence number is

a) 2^n b) 2^{n-1}
c) $2^n - 1$ d) 2^{n-2}

[GATE-2005]

Q.7 Consider the following message M=1010001101.The cyclic redundancy check (CRC) for this message using the divisor polynomial $x^5 + x^4 + x^2 + 1$ is :

a) 01110 b) 01011
c) 10101 d) 10110

[GATE-2005]

Q.8 A channel has a bit rate of 4 kbps and one-way propagation delay of 20 ms. The channel uses stop and wait protocol. The transmission time of the acknowledgement frame is negligible. To get a channel efficiency of at least 50%, the minimum frame size should be

a) 80 bytes b) 80 bits
c) 160 bytes d) 160 bits

[GATE-2005]

Q.9 On a wireless link, the probability of packet error is 0.2. A stop-and-wait protocol is used to transfer data across the link. The channel condition is assumed to be independent from transmission to transmission. What is the average number of transmission attempts required to transfer 100 packets?

a) 100 b) 125
c) 150 d) 200

[GATE-2006]

Q.10 Station A uses 32 byte packets to transmit messages to Station B using a sliding window protocol. The round trip delay between A and B is 80 ms and the bottleneck bandwidth on the path between A and B is 128 kbps. What is the optimal window size that A should :

a) 20 b) 40
c) 160 d) 320

[GATE-2006]

Q.11 Station A needs to send a message consisting of 9 packets to Station B using a sliding window (window size 3) and go-back-n error control strategy. All packets are ready and immediately available for transmission. If every 5th packet that A transmits gets lost (but no acts from B ever get lost), then what is the number of packets that A will transmit for sending the message to B?

a) 12 b) 14
c) 16 d) 18

[GATE-2006]

Q.12 The message 11001001 is to be transmitted using the CRC polynomial x^3+1 to protect it from errors. The message that should be transmitted is:

a) 11001001000 b) 11001001011
c) 11001010 d) 10010010011

[GATE-2007]

Q.13 An error correcting code has the following code words: 00000000, 00001111,01010101,10101010,11110000. What is the maximum number of bit errors that can be corrected?

a) 0 b) 1
c) 2 d) 3

[GATE-2007]

Q.14 The distance between two stations M nd N is L km. All frames are K bits long. The propagation delay per kilometer is t sec. Let R b/s be the channel capacity. Assuming that processing delay is negligible, the minimum number of bits for the sequence number field in a frame for maximum utilization, when the sliding window protocol is used, is

a) $\log_2 \frac{2LtR+2K}{K}$

b) $\log_2 \frac{2LtR}{K}$

c) $\log_2 \frac{2LtR+K}{K}$

d) $\log_2 \frac{2LtR+K}{2K}$

[GATE-2007]

Q.15 A 1 Mbps satellite link connects two ground stations. The altitude of the satellite is 36,504 km and speed of the signal is 3×10^8 m/s. What should be the packet size for a channel utilization of 25% for a satellite link using go-back-127 sliding window protocol?
Assume that the acknowledgement packets are negligible in size and that there are no errors during communication.
a) 120 bytes b) 60 bytes
c) 240 bytes d) 90 bytes
[GATE-2008]

Q.16 Let G(x) be the generator polynomial used for CRC checking. What is the condition that should be satisfied by G(x) to detect odd number of bits in error?
a) G(x) contain more than two terms
b) G(x) does not devide$1+x^k$, for any k not exceeding the frame length
c) 1+x is a factor of G(x)
d) G(x) has an odd number of terms
[GATE-2009]

Statements for linked answer Questions 17 and 18
Frames of 1000 bits are sent over a 10^6 bps duplex link between two hosts. The propagation time is 25ms. Frames are to be transmitted into this link to maximally pack them in transit (within the link)

Q.17 What is timer minimum number of bits (i) that will be required to represent the sequence numbers distinctly? Assume that no time gap needs to be given between transmission of two frames.
a) i = 2 b) i = 3
c) i = 4 d) i = 5
[GATE-2009]

Q.18 Suppose that the sliding window protocol is used with the sender window size of 2^1, where 1 is the number of bits identified in the earlier part and acknowledgements are always piggy backed. After sending 2^1 frames, what is the minimum time, the sender will have to wait before starting transmission of the next frame? (Identify the closest choice ignoring the frame processing time.)
a) 16 ms b) 18 ms
c) 20 ms d) 22 ms
[GATE-2009]

Q.19 a bit-stuffing based framing protocol uses an 8-bit delimiter pattern of 01111110. If the output bit-string after stuffing is 01111100101, then the input bit-string is
a) 0111110100 b) 0111110101
c) 0111111101 d) 0111111111
[GATE–2014]

Q.20 Consider a selective repeat sliding window protocol that uses a frame size of 1KB to send data on a 1.5 Mbps link with a one-way latency of 50 msec. To achieve a link utilization of 60%, the minimum number of bits required to represent the sequence number field is ___
[GATE–2014]

Q.21 Suppose that the stop-and-wait protocol is used on a link with a bit rate of 64 kilobits per second and 20 milliseconds propagation delay.

Assume that the transmission time for the acknowledgment and the processing time at nodes are negligible. Then the minimum frame size in bytes to achieve a link utilization of at least 50% is _____.

[GATE–2015]

Q.22 A link has a transmission speed of 10^6 bits/sec. It uses data packets of size 1000 bytes each. Assume that the acknowledgement has negligible transmission delay, and that its propagation delay is the same as the data propagation delay. Also assume that the processing delays at the nodes are negligible. The efficiency of the stop-and-wait protocol in this setup is exactly 25%. The value of the one-way propagation delay (in milliseconds) is _____.

[GATE–2015]

Q.23 Consider a network connected two systems located 8000 kilometres apart. The bandwidth of the network is 500×10^6 bits per second. The propagation speed of the media is 4×10^6 meters per second. It is needed to design a Go-Back-N sliding window protocol for this network. The average packet size is 10^7 bits. The network is to be used to its full capacity. Assume that processing delays at nodes are negligible. Then the minimum size in bits of the sequence number field has to be _____.

[GATE–2015]

Q.24 A sender uses the Stop-and-Wait ARQ protocol for reliable transmission of frames. Frames are of size 1000 bytes and the transmission rate at the sender is 80 Kbps (1Kbps = 1000 bits/second).
Size of an acknowledgement is 100 bytes and the transmission rate at the receiver is 8 Kbps. The one-way propagation delay is 100 milliseconds. Assuming no frame is lost, the sender throughput is ____ bytes/second.

[GATE–2016]

Q.25 Consider a 128×10^3 bits/second satellite communication link with one way propagation delay of 150 milliseconds. Selective retransmission (repeat) protocol is used on this link to send data with a frame size of 1 kilobyte. Neglect the transmission time of acknowledgement. The minimum number of bits required for the sequence number field to achieve 100% utilization is _____.

[GATE–2016]

Q.26 The values of parameters for the Stop-and-Wait APQ protocols are as given below:
Bit rate of the transmission channel = 1Mbps.
Propagation delay from sender to receiver = 0.75ms.
Time to process a frame = 0.25 ms.
Number of bytes in the information frame = 1980.
Number of bytes in the acknowledge frame =20.
Number of overhead bytes in the information frame =20. Assume that there are no transmission errors. Then, the transmission efficiency (expressed in percentage) of the stop –and-Wait ARQ protocol for the above

parameters is _____
(correct to 2 decimal places).

[GATE–2017]

ANSWER KEY:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
B	D	C	B	A	B	A	D	B	B	C	B	D	A	A
16	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**26**				
C	D	B	B	4	320	12	8	2500	4	86.5				

EXPLANATIONS

Q. 1 (b)

Now, transmission time for 1 packet = 50 μs

Transmission time for 5 packet =5×50 μs=250μs

Propagation delay = 200μs

Total time = transmission time + propagation

Delay=250+200=450μs=450×10^{-6}μs

Finally, maximum achievable throughput

$$= \frac{\text{size of window}}{\text{total time}} \text{ bps}$$

Q.2 (d)

Three consecutive ones are used for delimiter so whenever in data two consecutive one comes stuff a zero after them. Data is 01110110, After stuffing 0110101100.

Q.3 (c)

M+N: Because $W_s+W_r \leq$ Sequence numbers (because the maximum number of unacknowledged packets at sender will be W_s and at the receiver it will be W_r, similar to the sequence numbering in selective Repeat) where W_s is size of sender window and W_r is receiver window's size.

Q.4 (b)

Tx = 100*8 bits /20 Kbps = 40 ms

Tp = 400 ms,

a = Tp / Tx = 400/40 =10

Efficiency of GBN = W/(1+2a),

Where w=window size = 10

= 10/(1+20)=10/21

BW utilization or throughput or max data rate = efficiency * BW = (10/21)*20

It is nearly 10 Kbps

Q.5 (b)

Q. 6 (b)

Let us assume the following

1) Communication between two stations; station A and station B.
2) The size of window to be 8 (0,1,2, 3,4,5,6,7) Now, the communication between the two stations would be as follows

1) Station A sends frame 0 to station B
2) Station B receive frame 0 and sends an acknowledgement as RR1
3) Station A sends frame 1 to station B
4) Station B receive frame 1 and sends an acknowledge as RR2
5) Station A sends frame 2 to station B
6) Station B received frame 2 and sends an acknowledge as RR3
7) Station A sends frame 3 to station B
8) Station B received frame 3 and sends an acknowledge as RR4
9) Station A sends frame 5 to station B
10) Station B received frame 5 and sends an acknowledge as RR6. (Receive ready 6), i.e., it is ready to receive frame 6

11) Station A sends frame 6 to station B
12) Station B receive frame 6 and sends an acknowledgement(ack) as RR7(Receive ready 7), i.e, it is ready to receive frame 7
13) Now, RR7 is lost in the transmission. Since , station A will send frame 7 only after receiving RR7, so it will Time Out as RR7 is already lost.
14) Now, A times out retransmit frame 0
15) But B was expecting frame 7, so it considers frame 7 as lost and accept frame 0 as a new frame
This problem is overcome by limiting the maximum windows size to 2^{n-1}

Q.7 (a)

Generator polynomial is of degree 5 so append 50's to the end of data and then divide new data by generator polynomial

$x^5 + x^4 + x^3 + x^2 + 1 = 110101$

$$
\begin{array}{r}
110101\overline{)\,101000110100000} \\
\underline{110101} \\
0111011 \\
\underline{110101} \\
0111011 \\
\underline{110101} \\
00111110 \\
\underline{110101} \\
00101100 \\
\underline{110101} \\
0110010 \\
\underline{110101} \\
0001110
\end{array}
$$

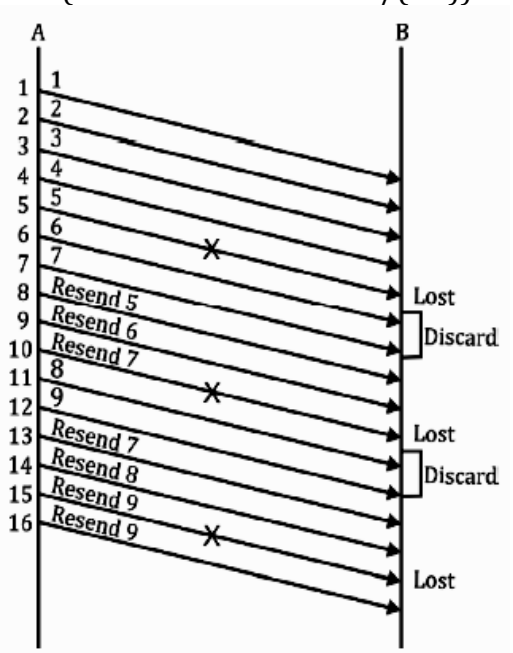
Remainder is 01110

Q.8 (d)

Efficiency of stop and wait
$= 1/(1+2a)$.
If $1/(1+2a) = 0.5$
$\Rightarrow 2*T_p = T_x$
$\Rightarrow L = 2*B*T_p = 160$ bits

Q.9 (b)

Error rate is 0.2
In stop and wait protocol: sender will transmits $100*(1+(0.2)^1 + (0.2)^2 + (0.2)^3 + (0.2)^4 + ...)$packets.
$= 100* (1/(1-0.02)) = 100/0.8$
$= 125$
(sum of infinite G.P. is a/(a-r))



Number of packets = 16

Q.10 (b)

Roundtrip delay × bottleneck bandwidth

$$= 80\times10^{-3} - 3\times128\times1024\,\text{byte}$$

$$= \frac{80\times10^{-3} - 3\times128\times1024}{8}\,\text{bit}$$

[because 1 byte = 8 bit]
Now, optimal size window

$$= \frac{\text{Bandwidth delay production}}{\text{packet size}}$$

$$= \frac{80\times10^{-3} - 3\times128\times1024}{8\times32}\text{ bits} = 40$$

Q. 11 (c)

Q.12 (b)

P(x) = 11001001

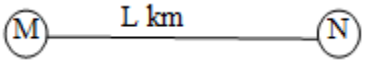
divisor D(x)=1001 and CRC remainder is 011.

So the transmitted message is 11001001011.

Q.13 (d)

The maximum hamming distance among the gives code words.

Q.14 (c)



Frame size K bit long

Propagation delay t sec/km

Channel capacity = R bits/sec

$$U = \frac{w.\frac{K}{R}\sec}{\text{Rsec} + 2Lt}$$

$$1 = \frac{\frac{wK}{R}\sec}{\frac{K + 2LtR}{R}}$$

$$w = \frac{K + 2LtR}{K}$$

$$2^n = \frac{K + 2LtR}{K}$$

$$n = \left\lfloor \log_2 \log_2 \frac{K + 2LtR}{K} \right\rfloor$$

Q.15 (c)

Efficiency for a sliding window protocol is

$$\eta = \frac{N}{1+2a}$$

Where N is the window size.

$\Rightarrow$ N = 127-1=126

Utilization is given as 0.25

$$\therefore 0.25 = \frac{126}{1+2A}$$

Where $a = \frac{t_p}{t_d}$

$$t_d = \frac{x \text{ bytes}}{1\text{Mbps}}$$

$$t_p = \frac{2\times36504\times10^3}{3\times10^3}$$

Q.16 (c)

The polynomial generator used for CRC checking must satisfy at least two condition to detect odd numbers of errors:

1. It should be not divisible by x.
2. It should be not divisible by 1+x.

   Therefore (1+x) is a factor of G(x).

Q.17 (d)

$$\text{Pulse Rate} = \frac{\text{Number of bits}}{\text{Time taken}}$$

$$= \frac{1000}{25\times10^{-3}}$$

$= 4\times10^4$

Now,

Bit rate = Pulse rate $\times 2^1$

$2^1 = 25 \Rightarrow i = 5$

Q.18 (b)

Time taken to send 10^6 bits = 1 s

Now, as 1 frame = 1000 bits

Time taken to send 2^5 frames = 32ms

Also, time taken for first frame to be acknowledged =25 × 2 = 50ms

Hence, the waiting time =50–32=18ms

Q.19 (b)

Input string : 0111110101

Output string : 01111100101
After five consecutive 1's in the input, bit 0 is inserted.

Q.20 (5)

Given L = 1 KB
B = 1.5 Mbps
T_p = 50 ms
η = 60
Efficiency formula for SR protocol is

$$\eta = \frac{W}{1+2a} \Rightarrow \frac{60}{100} = \frac{W}{1+2a}\left(\because a = \frac{T_p}{T_x}\right)$$

$$T_x = \frac{L}{B} = \frac{8\times10^3}{1.5\times10^6} = 5.3\text{ms}$$

$$a = \frac{T_p}{T_x} = \frac{50}{5.3} = \frac{500}{53} = 9.43$$

$$\Rightarrow \frac{60}{100} = \frac{W}{19.86} \Rightarrow W = 11.9 \approx 12$$

$$\Rightarrow W = 2^{n-1} = 12 \Rightarrow 2^n = 24 \Rightarrow 2^n = 24 \approx 2^5 \Rightarrow n = 5$$

Q.21 (320)

Transmission or Link speed = 64 KB per sec
Propagation Delay = 20 millisec
Since stop and wait is used, a packet is sent only
when previous one is acknowledged.
Let x be size of packet, transmission time = x / 64 milisec
Since utilization is at least 50%, minimum possible total time for one packet is twice of transmission delay, which means
x/64 * 2 = x/32
x/32 > x/64 + 2*20
x/64 > 40
x > 2560 bits = 320 bytes

Q.22 (12)

In stop and wait, protocol next packet is sent only when acknowledgement of previous packet is received. This causes poor link utilization.
Tansmission speed = 106
Time to send a packet = (1000 * 8) bits / 106 = 8 millisec
Since link utilization or efficiency is 25%, total time taken for 1 packet is 8 * 100/25 = 32 millisec.
Total time is twice the one way propagation delay plus transmission delay. Propagation delay has to be considered for packet and ack both. Transmission delay is considered only for packet as the question says that transmission time for acknowledgement is negligible.
Let propagation delay be x.
2x + 8 = 32.
x = 12.

Q.23 (8)

Propagation time
= (8000*1000)/(4*10^6)
= 2 seconds
Total round trip propagation time = 4 seconds
Transmission time for one packet
= (packet size) / (bandwidth)
= (10^7) / (500 * 10^6)
= 0.02 seconds
Total number of packets that can be transferred before an acknowledgement comes back = 4 / 0.02 = 200
Maximum possible window size is 200. In Go-Back-N, maximum sequence number should be one more than window size.
So total 201 sequence numbers are needed. 201 different sequence

numbers can be represented using 8 bits.

Q.24 (2500 bytes/sec)

$$\text{Sender throughput} = \frac{\text{Data}}{\text{Total time}}$$

$$= \frac{1000\text{bytes}}{0.1+0.1+0.1+0.1} = 2500 \text{ bytes/sec}$$

Q.25 (4)

$$\text{Transmission time} = \frac{\text{Frame sixe}}{\text{Bandwidth}}$$

$$\text{T.T.} = \frac{1024\times 8}{128\times 10^3} = \frac{1028}{16}\text{msec}$$

= 64 msec [$\because$ 1 K = 2^{10}]

$$\text{Efficiency} = \text{w.s.} \times \frac{\text{T.T.}}{\text{T.T.}+2\text{P.T.}}$$

$$100\% = \text{w.s.} \times \frac{1}{1+2\frac{\text{P.T.}}{\text{T.T.}}}$$

$$1+2\frac{\text{P.T.}}{\text{T.T.}} = \text{w.s.}$$

$$1+2\left\lfloor \frac{150}{64} \right\rfloor = \text{w.s.}$$

1+2[2.34] = w.s.

w.s. = 5.68=6

In selective repeate ARQ.

Total window size ≥ $\log_2$(S.w.s + R.w.s) and Sender w.s.=Reciever w.s.

So, total w.s. ≥ $\log_2$[6 + 6] = $\log_2$[12] =4

Q.26 (89.33)

Processing time of frame=0.25msec

Transmission time of data

$$= \frac{\text{Data size}}{\text{Bandwidth}}$$

$$= \frac{(1980+20)\text{bytes}}{10^6\text{bits/sec}}$$

$$= \frac{2000\times 8\text{bits}}{10^6\text{bits/sec}} = 16\text{msec}$$

Propagation time =0.75msec

Transmission time of ACK

$$= \frac{20\times 8\text{bits}}{10^6\text{bits/sec}} = 0.16\text{msec}$$

Transmission efficiency of stop and wait ARQ

$$= \frac{16}{0.25+16+1.5+0.16}$$

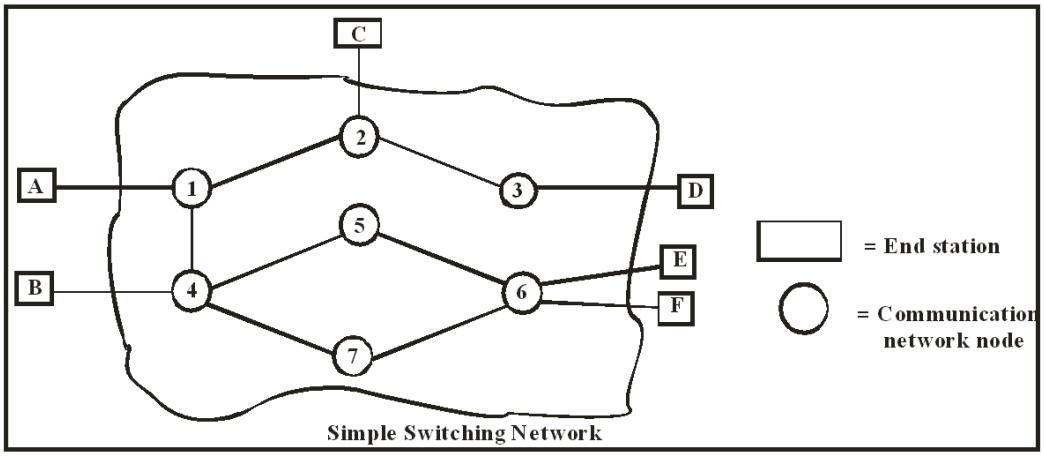
$$= \frac{16}{17.91}\times 100\% = 89.33\%$$

3 NETWORK AND TRANSPORT LAYER

3.1 INTRODUCTION

The network layer is responsible for the source to destination delivery of a packet across multiple network links. To make end to end delivery possible the network layer provides two related services.
Switching and Routing
Switching refers to temporary connections between physical links resulting in larger links for network transmission. A telephone conversation is an example of a switched connection where two lines are temporarily joined into a single dedicated link for the duration of the conversation. In this case packet is sent by the same route to the destination.
Routing means selecting a test path for sending from one point to another when more than one path is available. In this case each packet may take a different route to the destination, where the packets are collected and re- assembled into their original order.

3.2 SWITCHING NETWORKS



Simple Switching Network

A switching network consists of a series of interlinked nodes, called **switching.** Switching are hardware and/or software devices capable of creating temporary connections between two or more devices linked to the switch but not to each other. In a switched network some of these nodes are connected to the communicating devices, others are used for rolling.

3.2.1 SIMPLE SWITCHING NETWORK

Data entering the networks from a station are routed to the destination from node to node. Data from A intended for station F are sent to node 3. That may then be routed via node 5 and 6 or node 7 and 6 to the destination station F.
Note:

- Some nodes connect only to other node. Their task is internal switching of data.
  Other nodes have one or more stations attached as well. In addition to their switching functions, such nodes accept and deliver data to the attached station.
- Node to node links are usually multiplexed using either FDM (Frequency division Multiplexing) or TDM (Time Division Multiplexing).

- Usually, the network is not fully connected, that is there is not a direct link between every possible pair of nodes.
  Traditionally, there methods of switching are used:
- Circuit switching
- Packet switching
- Message switching

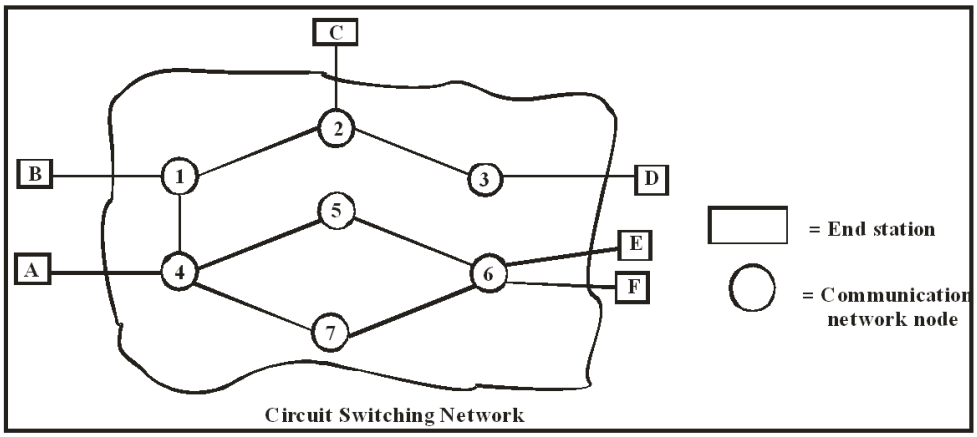
3.2.2 CIRCUIT SWITCHING NETWORKS

Circuit switching creates a direct physical connection between two devices such as phones or computers. There is a dedicated communication path between two stations. That path is connected to sequences of links between nodes. On each physical link, a logical channel is dedicated to the connection.
Commutation via circuit switching involves 3 phases:

- Circuit Establishment
- Data Transfer
- Circuit disconnect

1) Circuit Establishment

Before any signal can be transmitted an end to end circuit must be established.



Example:

Station A sends a request to node 3 requesting a connection to station E. Typically, the link from A to 3 is a decided line, so that part of connection already exists. Node 3 must find a next link in a route leading to node 6. Based on routing information and measure of availability, node 3 selects the link to node 5. It allocates a free channel on that link and sends a message requesting connection to E using FDM and TDM. So far a dedicated path has been establish from A through 3 to 5. Because a number of station may attach to 3, it must be able to establish internal paths from multiple station to multiple nodes. Similarly, node 5 dedicates a channel to node 6. The node 6 completes the connection to E. In completing the connection the is made to determine if E is busy or is prepared to accept the connection.

2) Data Transfer

The information can be transmitted from A through the network to E. The path is A- 3 link, internal switching through 3, 3-5 channel, internal switching through 5, 5-6 channel and internal switching through 6 and finally 6-E link. (Generally, the connection is full duplex).

3) Circuit Disconnect

After some period of data transfer the connection is terminated, usually by the action of one of the two stations. Signals must be propagated to nodes 3, 5, 6 to deallocate the dedicated resources. The connection path is established before data transmission begins. Thus channel capacity must be reserved between each pair of nodes in the path. Once the circuit is established, the network is effectively – transparent to the users. Information is transmitted at a fixed data rate.

Example:
Public telephone networks
Private branch exchange (PBX)
A circuit switch is a device with m inputs and n outputs that creates a temporary connection between an input link and an output link as shown below. The number of inputs does not have to match the no. of outputs.

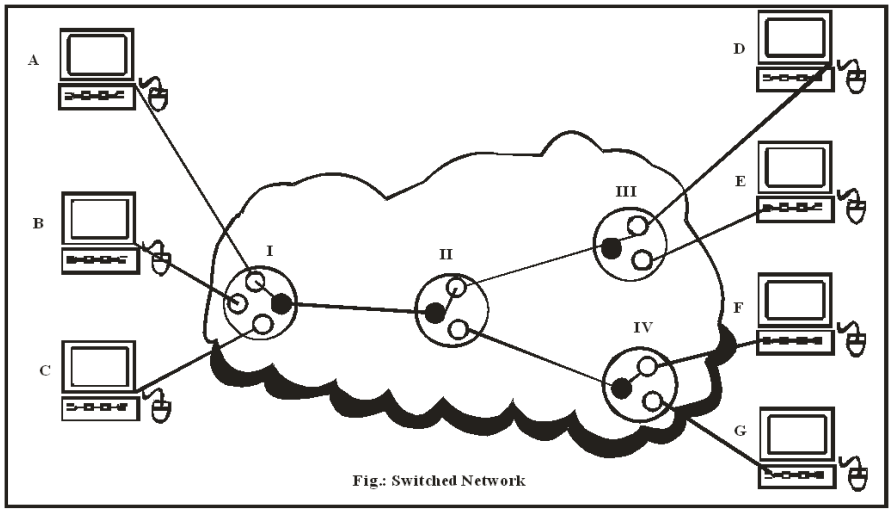


Fig.: Switched Network

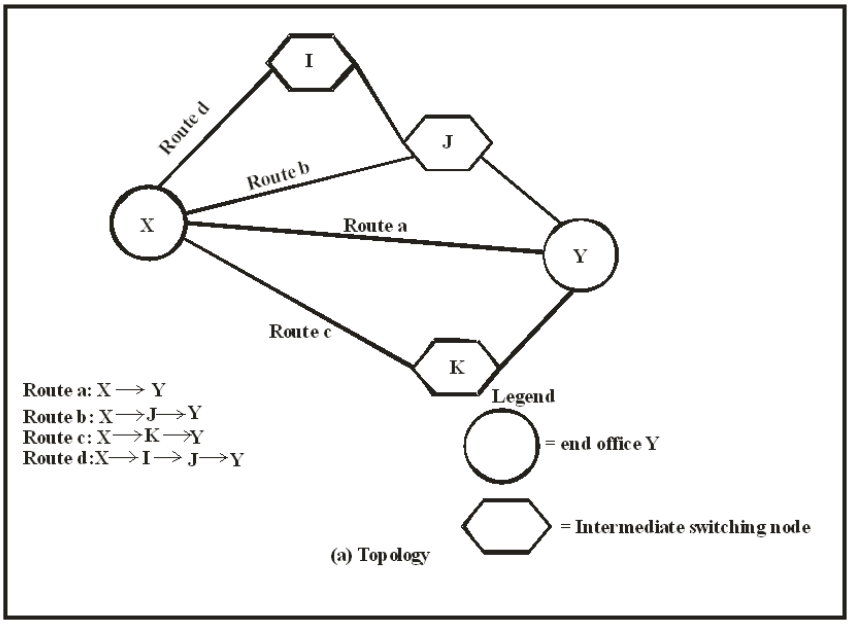
Circuit switching can employ either of two technologies –
(i) Space division switches
(ii) time division switches

3.2.3 ROUTING IN CIRCUIT- SWITCHED NETWORKS

In dynamic routing approach, routing decisions depends on current traffic conditions. The circuit switching network nodes have a peer relationship with other. All nodes are capable of performing the same functions. In such an architecture does not provide a 'natural' path or set of paths, but it is more flexible because more alternative routers are available.
Two broad classes of dynamic routing algorithm have been implemented:
(i) Alternate routing and
(ii) Adaptive routing.

(i) Alternate routing (Also called source routing)
In alternate routing, all the possible routers to be used between two used between two end officers are predefined. It is the responsibility of the originating switch the appropriate router for each call. Each switch is given a set of pre-planned routers for each destination in order of preference.
If there is only one routing sequence defined pair, the scheme is known as a fixed alternative routing scheme. More commonly a dynamic routing scheme is used. In dynamic alternative routing scheme, a different set of pre – planned route is used for different time

periods, so as to take the advantage of different traffic patterns in different time zones and at different times of days.



Time/period	First route	Second route	Third route	Fourth & Final route
Morning	A	b	c	d
Afternoon	A	d	b	C
Evening	A	d	c	B
Weekend	A	c	b	d

As shown in figure the originating switch X has four possible routes to the destination with Y. The direct route (a) will always be tried first. If this trunk is unavailable (busy, out of service) the other providing order, depending in the time period. A form of the dynamic alternative technique is employed by the Bell operating companies for providing companies for providing local and regional telephone service.
This is referred to as Multi Alternative routing (MAR). This approach is also used by AT and T in its long distance network and is referred to as **dynamic nonhierarchical routing (DNHR).**

(ii) Adaptive Routing
In adaptive routing, a central controller is used to find best alternative route depending on the congestion in the network. The central controller collects data from each switch in the network after every 10 second to determine preferred alternative routes. Each call is first attempting on the direct path, if any exists between source and destination. If the path is blocked, it is attempted on a two link alternative path.
Each switch I communicates the following traffic measurements to the central controller:
(i) I_{ij} = The no. of idle trunks on the link to switch j, for all switches in the network.
(ii) CPU_i = The CPU utilization of switch i.
Based on this information, the central controller periodically returns to each switch I for each possible destination switch j.
Note:

- Circuit Switching is designed for voice communication. In a telephone conversation once a circuit is established it remains connected for the duration of the session.

- Circuit switching creates temporary dedicated links that are well suited for this type of communication.
- Circuit switching is less well suited to data and non- conversational transmission. Non voice transmission tends to be busty, meaning data comes in spurts with idle gap between them. When circuit switching links are used for data transmission, the line is often idle.
- In circuit switching network, the connection provides for transmission at constant data rate. Thus each of the two devices that are- connected must transmit and receive at the same data rate as the other, this limits the utility of the network the interconnecting of host computers and terminals.
- Circuit switching sees all transmission is equal. Any request is granted to whatever link is available. e.g. DTM (Dynamic Traffic Management)

3.2.4 PACKET SWITCHING NETWORKS

Principle

In a packet network, data are transmitted in discrete units of potentially variable length blocks called packets. The maximum length of the packet is established by the network. If a source has a longer message to send, the message is broken up into a series of packets. Each packet contains a portion of the user's data plus some control information. The control information, at a minimum include the information that the network requires in order to be able the packet is received, stored briefly and passed on to the next node.

This approach has advantages over circuit switching:

- Line efficiency is greater as a single node to node dynamically shared by many packets over time.
- The packets are queued up and transmitted as rapidly over the link. By contrast, with circuit switching, time of anode – to – node link is pre allocated using synchronous TDM. Much of the time such a link may be able idle because a portion of its time is dedicated to the connection which is idle.
- A packet switching network can perform data rate conversion. Two stations of different data rates can exchange packets because each connects to its proper data rates.
- When traffic becomes heavy on a circuit switching network some calls are blocked i.e. the network refuse to accept additional connection request until the load on the network reduces.
  On a packet switching network, packets are still accepted but delivery delay increases.
- Priority can be used. Thus if a node has number of packets queued for transmission it can transmit the higher priority packet first.
  There are two popular approaches to packet switching:
- Datagram
- Virtual circuit

(i) Datagram Approach

In the datagram approach, each packet is treated independently from all others. Paths in this technology are referred to as data grams.

Figure shows how the datagram approach can be used to delivery four packets from station A to station X. In this example all four packets belong to the same message but may go by different paths to reach their destination.

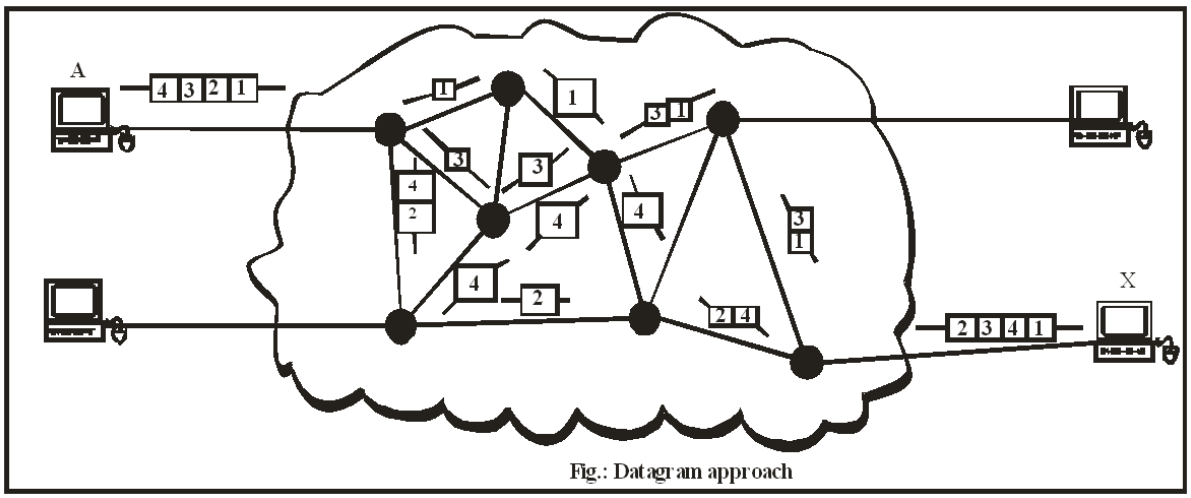


Fig.: Datagram approach

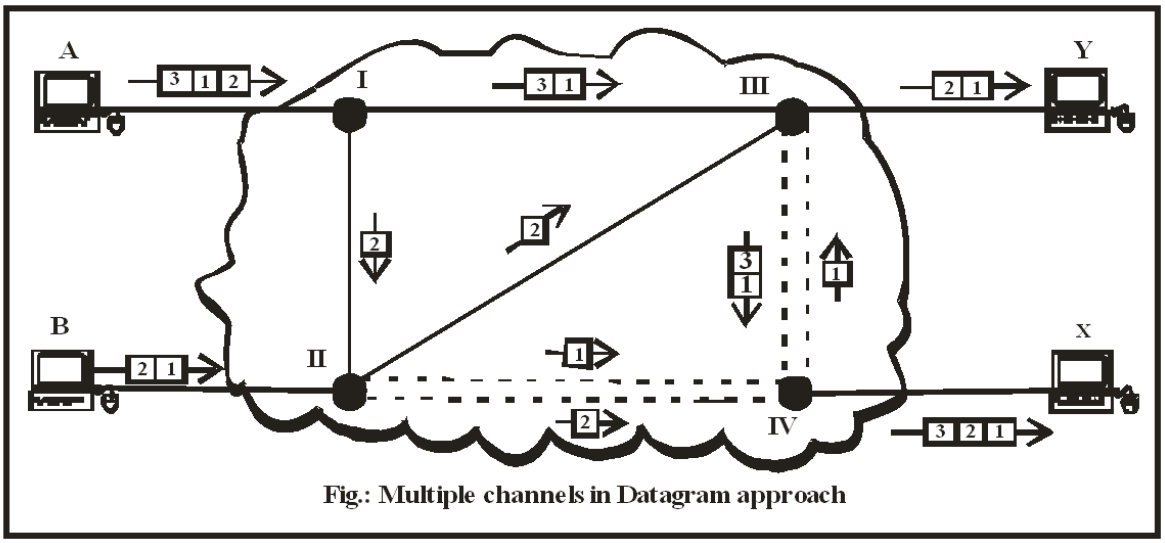


Fig.: Multiple channels in Datagram approach

With this approach datagram arrive to their destination out of order. It is the responsibility of the transport layer to reorder the datagram before passing them on to the destination port. The link joining each pair of nodes can contain multiple channels. Each of these channels is capacity is capable of carrying datagram either from several different sources or from one source simultaneously. Packets can be carried simultaneously by d\either TDM or FDM.

(ii) Virtual circuit approach

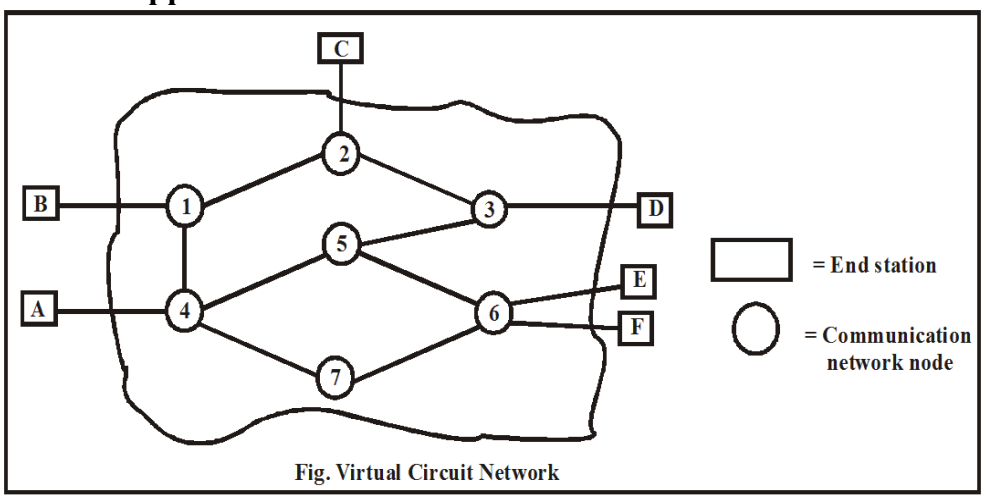


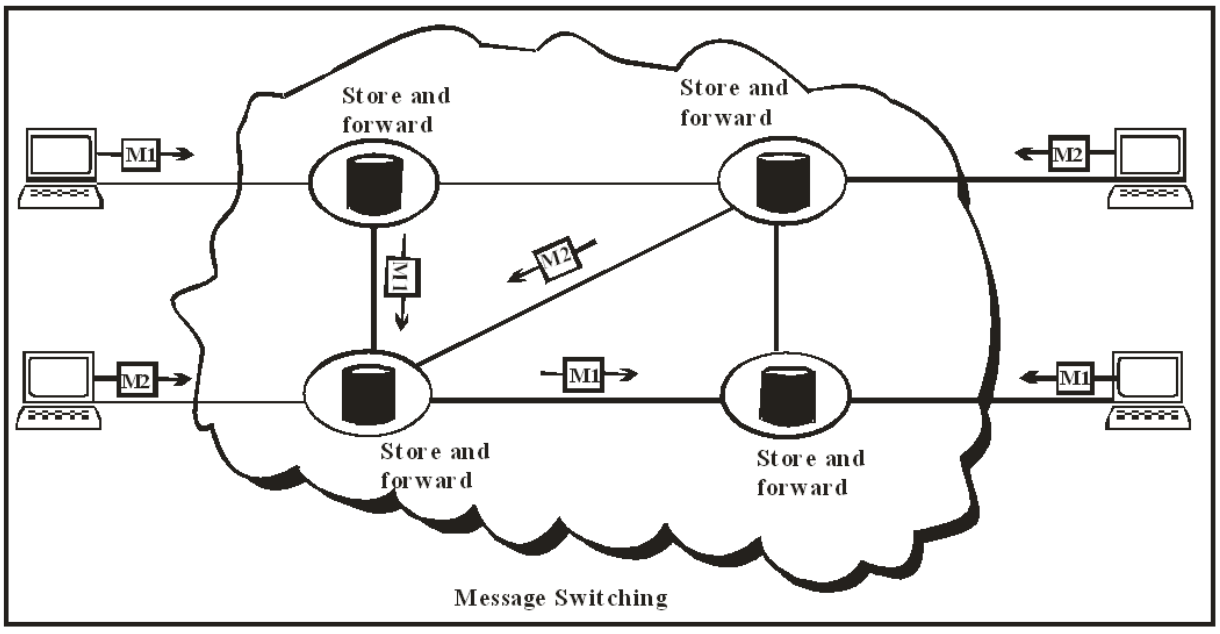
Fig. Virtual Circuit Network

In virtual circuit approach, a route established before are sent. This does not mean that there is a dedicated path as in circuit switching. A packet is still buffered at each node and queued for output over a line.
For example, suppose that A has one or more message to send to E. It first sends a special control packet (call request packet) to 3, requesting s logical connection to E. node 3 decides to route the request and all subsequent packets to 5 which decides to route the request and all connection, it sends a call request accept to 6. This packet is passed back through nodes 5 and 3 to A. Station A and E may now exchange data over the route that that has been established. Each packet contains a virtual identifier and data. Each node on the pre – established route knows where to direct such packets, thus no routing decisions are required. Thus every data packet from E intended for A traverse node 6, 5 and 3. Eventually one of the stations terminates the connection with a clear request packet.
Because the route is fixed for the duration of the logical connection, it is somewhat similar to circuit in a circuit switching network, and is referred to as virtual circuit.

- The network may provide services related to the virtual circuits including sequencing and error control.
- Sequencing refers to the fact that because all packets follow the same route they arrive in the original order.
- Packets arrive more rapidly with virtual circuit, because it is not necessary to make routing decision for each packet at each node.

3.2.5 MESSAGE SWITCHING

Message switching is best known by the term store and Forward. In this mechanism a node receives a message, store it until the appropriate route is free, then sends it along. Node is usually a special computer with a number of disks. In message switching, the message are stored and relayed from the secondary storage (disk), while in packet switching packets are stored and forward from primary storage (RAM).



3.2.6 COMPARISON

Comparison between Circuit switching, datagram packet switching & Virtual circuit packet

Switching

Circuit switching	Datagram packet switching	Virtual circuit packet switching
Dedicated transmission path	No dedicated path	No dedicated path
Continuous transmission of data	Transmission of packets	Transmission of packets
Fast enough for interactive	Fast enough for interactive	Fast enough for interactive
Message are not stored	Packets may be stored until delivered	Packets stored until delivered
The path is established for entire conversation	Route established for each packet	Route established for entire conversation
-Call set up delay negligible - transmission delay	Packet transmission delay	-Call set up delay - Packed transmission delay
Busy signal if called party is busy	Center may be notified if packets not delivered	Center notified of connection denied.
Over may block call set up no delay for establish calls	Overload increases packet delay	May block call set up; increases packet delay.
Electromechanically or computerized switching nodes	Small switching notes	Small switching notes
Responsible for message loss protection	Network may be responsible for individual packets	Network may be responsible for packet sequence
Speed or code convergent	Speed and code convergent	Speed and code convergent
Fixed bandwidth	Dynamic use of bandwidth	Dynamic use of bandwidth
No overhead bits after call set up	Overhead bits in its message	Overhead bits in its packet

3.2.7 COMPARISON OF CIRCUIT SWITCHING AND PACKET SWITCHING

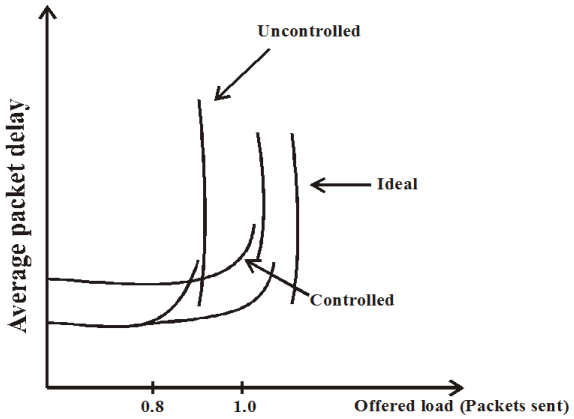
i) For circuit switching, there is a certain amount before the message can be sent. First a call request signal is sent through the network in order to set up a connection to the destination. If the destination if station is not busies a call accepted signal is returned. A processing delay is incurred at each node during the call request; this time is spent at each node setting up the route of the connection. On the return this processing is not needed because the noticeable delay at the switching nodes.

ii) Virtual circuit packet switching appears quite similar to circuit switching. A virtual circuit request using a call request packet which incurs a delay at each node. The virtual circuit is accepted with accepted with a call accept packet. The call acceptances also experiences node delay even though the virtual circuit route is now established. The reason is that this packet is queued at each node and must wait until its turn for retransmission. Once the virtual is established, the message is transmitted in packets. Packets switching involves some delay at each node in the path.

iii) Datagram packet switching does not require a call set up. Thus for short message it will be faster than virtual circuit switching and perhaps circuit switching. Because each individual datagram routed independently, the processing for each datagram at each node may be longer than for virtual circuit packets. Thus for long message the virtual circuit technique may be superior.

3.3 CONGESTION CONTROL

Congestion control maintains the number of packets within the network below the level at which performance falls of dramatically.



- Every node has a queue of packets for each outgoing channel.
- If rate at which packets arrive and queue up, exceeds the rate of packet transmission, then size of queue grows without bound and thus delay experienced by a packet goes to infinity.
  Input buffer accepts arriving packets and output buffer holds packets that are waiting to depart.
- When the packets arrive they are stored in the input buffer of the corresponding link. The node examines each incoming packet to make a routing decision and the moves the packets to the appropriate output buffer. Packets queued up for output in output buffer is transmitted as soon as possible. If packets arrive too fast for the node to process them i.e. to make routing decision or faster than packets can be cleared from the outgoing buffers, than packets will arrive for which for which no memory is available.
  When above saturation point is reached, one can do any of the following:

(i) Discard incoming packet for which there is no available buffer space.

(ii) Node should Exercise some sort of flow control over its neighbors so that the traffic flow remains manageable.

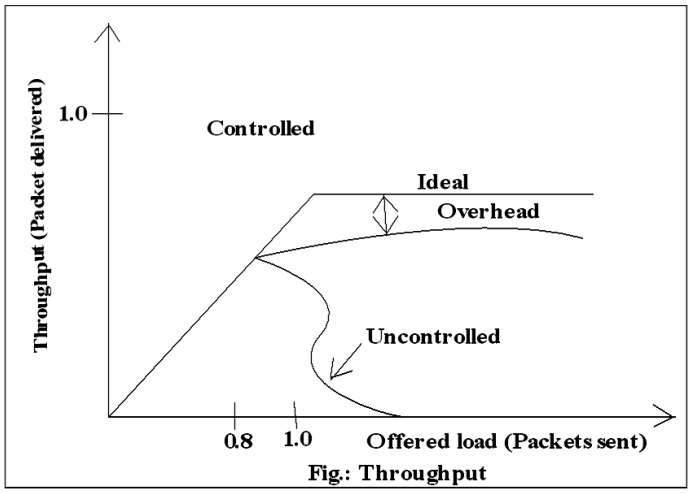


Fig.: Throughput

- Ideally network utilization is 100%. For ideal case all station somehow knows the timing and rate of packets that can be presented to the network which is actually impossible.
- Utilization increase for a while as the load increases. Due to this queue length at the various nodes begin to grow and thus throughput actually drops (as the buffers at each node are of finite size).
- When the buffers are full, it must discard packets. So the source station must retransmit the discarded packets in addition to the new packets.

- As more and more packets are retransmitted, the load on the system grows and more buffers get saturated. While the system is trying to clear buffers, stations are sending old and new packets into the system. Also successfully delivered packets may be transmitted because it takes so long to acknowledgment them. Thus the sender assumes that the packet is lost. Under these circumstances the effective capacity of the system is virtually zero.

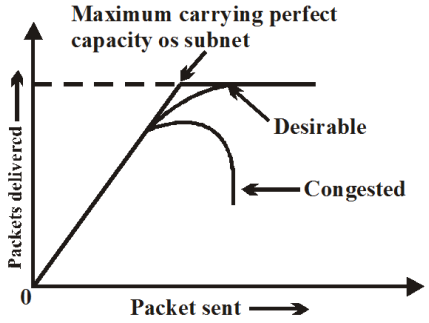
3.3.1 CONGESTION CONTROL TECHNIQUE

Objective of congestion control technique:
Limit queue lengths at the nodes so as to avoid throughput collapse.

1) Send a control packet a congested node to some or all source nodes to stop or slow the rate of transmission from sources and thus limit the total number of packets in the network. This approach requires additional traffic on the network during a period of congestion.
2) Allow packet switching nodes to add congestion information to packets as they pass by. The packets carrying such information can go in both direction i.e. opposite of the congestion and in the same direction as the congestion.
   - Packets in the opposite direction of congestion quickly reach the source node which can reduce the flow of packets into network.
   - Packet going in the same direction as the congestion reaches the destination. The destination asks the source to adjust the load by returning the signal back to the source in the packets.
3) Provide link delay information to other nodes. This information can be used to influence the rate at which new packets are produced. As these delay are influenced by the routing decision, they may vary too rapidly to be used effectively for congestion control.

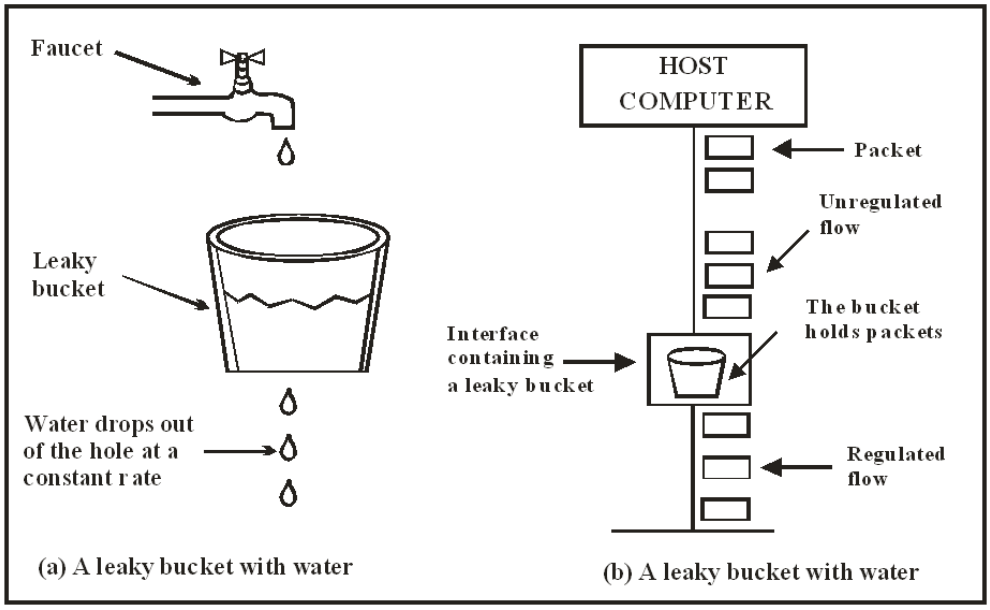
3.3.2 CONGESTION CONTROL ALGORITHM

When too many packets are present in the subnet, performance degrades. This situation is called congestion.



- **Causes of congestion**
  1) If all of a sudden stream of packets begin arriving on three or four input lines and all need the same output line, a queue will build up.
  2) Slow processors
  3) Low bandwidth lines.
- **Traffic shaping**
  (i) One of the main causes of congestion is that traffic is often bursty.
  (ii) If hosts could be made to transmit at uniform rate, congestion would be less common.

3.3.3 LEAKEY BUCKET ALGORITHM



A leaky bucket is with a small hole. No matter at what rate water enters the bucket, the outflow rate, S, when there is any water in the bucket and zero when bucket is empty. Once the bucket is full, any additional water entering it spills over the sides and is lost. Each host is connected to the network by an interface containing a leaky bucket (i.e. a finite internal queue). This arrangement can be built into the network interface or simulated by the host O.S. The host is allowed to put one packet per clock tick on the network.

(i) When the packets are all of the same size at every clock tick, one packet is transmitted.

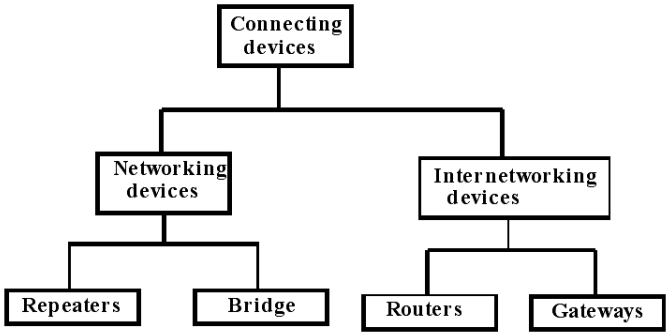
(ii) When variable size packets are used

a. At every tick, a counter is initialized to n.
If the first packet on the queue has fewer bytes than the current value of the counter, it is transmitted and the counter is decremented by that number of bytes.

b. Additional packets may also be sent, as long as the counter is high enough.

c. When the counter drops below the length of the next packet on the queue, transmission stops until the next tick, at which time the residual byte count is overwritten and lost.

3.3.4 CONNECTING DEVICES



3.3.5 NETWORKING DEVICES

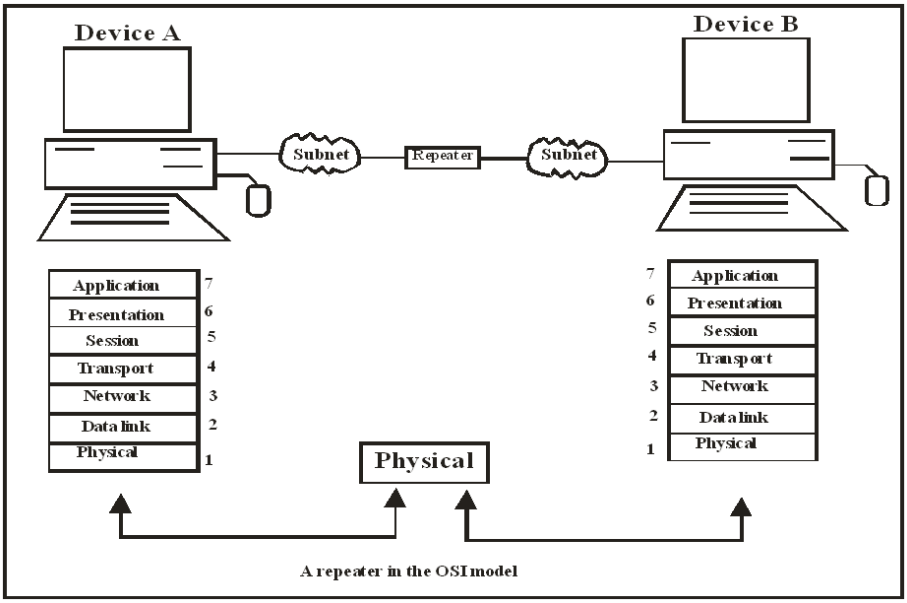
Two or more devices connected for the purpose of sharing data or resources can form a network. A Local area network may need to cover more distance than its media can handle effectively. It may also happen that the number of station may be too great for efficient frame delivery or management of the network and the network may need to be subdivided. Thus for all these purpose, we require networking devices. The two networking device is:

(i) Repeaters
(ii) Bridges

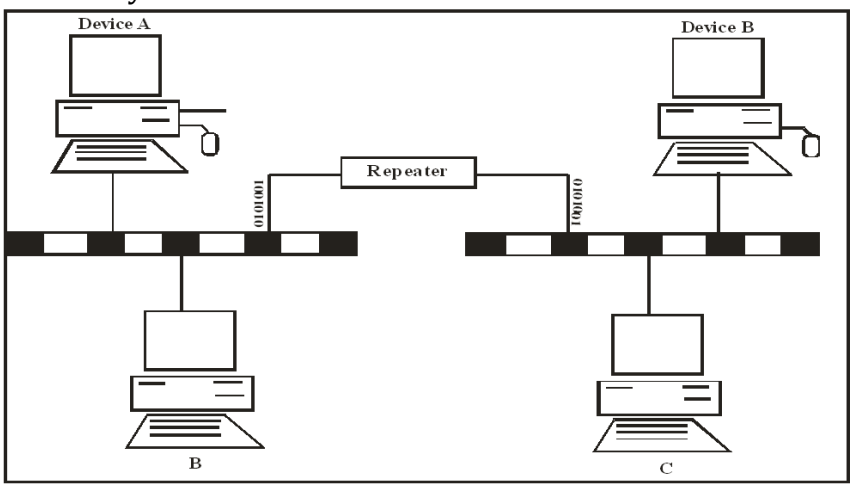
3.3.6 REPEATERS

A repeater (or regenerator) is an electronic device that operates on physical layer of the OSI model.

- A repeater receives the signal before too weak or corrupted, regenerates the original bit pattern and then puts the refreshed copy back onto the link.



- A repeater allows extending the physical length of a network. The repeater does not change the functionality of the network in any way. The two sections connected by the repeater are in reality one network.



- In the above figure, if station A sends a frame to station B, all station will receive the frame, just as they would without the repeater.
- The repeater does not have the intelligence to keep the frame passing to the right side when it is meant for a station on the left.

3.4 BRIDGES

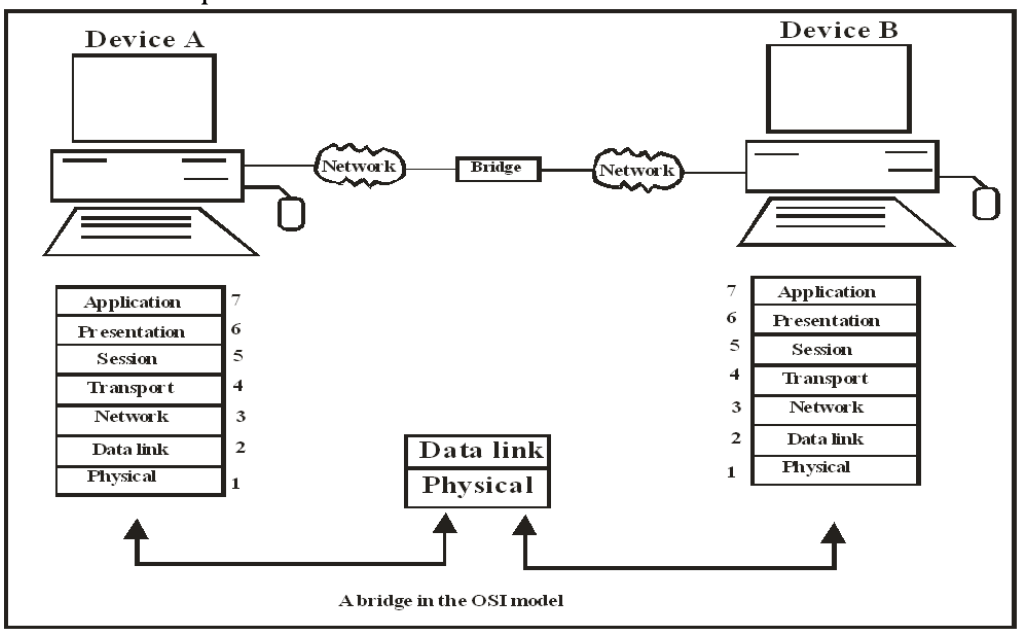
Bridge is an intermediate system used to connect two LANS. They are used at Data link layer.

- Bridge provides an intermediate to LAN that requires no modifications to

communication software in the station attached to the LANs. All the stations are considered as if they are form a single LAN.

Note:

Each station uses a unique address.



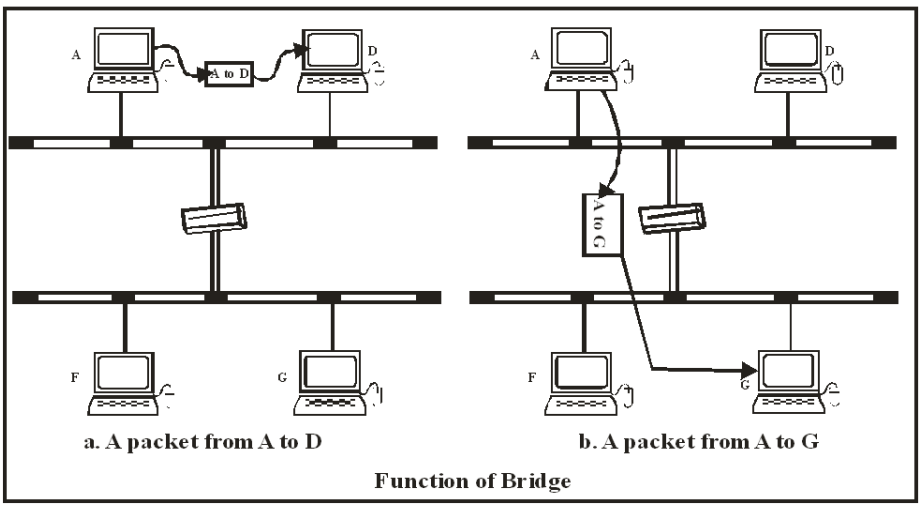
A bridge in the OSI model

- A bridge operator at the data link layer giving it access to the physical address of all stations connected to it.

3.4.1 HOW BRIDGE WORKS

- When a frame enters a bridge, it not only regenerates the signal but checks the address of the destination and forward the new copy only to the segment to which the address belongs.
- When bridge encounters counter a packet it reads the address contained in the frame and compares that address with a table that has name of all the stations on both segments. When it finds a match, it known to which segment the station belongs and forwards the packet only to that segment.

Example



a. A packet from A to D

b. A packet from A to G

Function of Bridge

As shown a packet from station A addressed to station D arrives at the bridge. Station A is on the same segment as station D, therefore the packet is relayed to the upper segment and received by station D. In second part, a packet generated by station A is intended for station G. The bridge allows the packet to cross and relays it to the lower segment, where it is received by station G.

3.4.2 Types of Bridges

To select between segments, a bridge must have a look up contains the physical addresses of every station connected to it. The table
indicates to which segment each station belongs.

There are three types of Bridges

1)Simple
2)Learning
3)Multiport

(i) Simple Bridge

Simple bridges are most primitive and least expensive type of bridge. A simple bridge links two segments and contains a table that lists the addresses of all the stations included in each of them.
Table content must be modified whenever a new station is added. If a station is removed, the invalid must be deleted.

(ii) Learning Bridge:

A learning bridge builds its table addresses on its own as it perform its own as it performs its bridge functions. When the learning bridges are first installed, its table is empty. As it encounters each packet, it looks at both the destination and the source addresses. It checks the destination to decide where to send the packet. Because in the beginning, the table is empty it does not recognize the address and therefore it relay it to all the station on both the segments. It uses the source address to build its table. It copies the source address and the segment to with it belongs into the table. This is the first entry into the table. For e.g. as shown in figure, when station A sends its packet to station G, the bridge learns that the packet coming from A are coming from segment and that station must be located in the upper segment. Now whenever the bridge encounters packet addresses to A, it knows to forward them only to the upper segment. With the first packet transmitted by each station the bridge learn the segment associated with that station. Eventually it has a complete table of station addresses and their respective segment stored in its memory. The logic required to achieve this kind of automation makes a learning bridge more expensive than a simple bridge.

(iii) Multiport Bridges:

A multiport bridge can be either simple or learning and is used to interconnect more than two same type of LAN.

3.5 Internetworking Devices

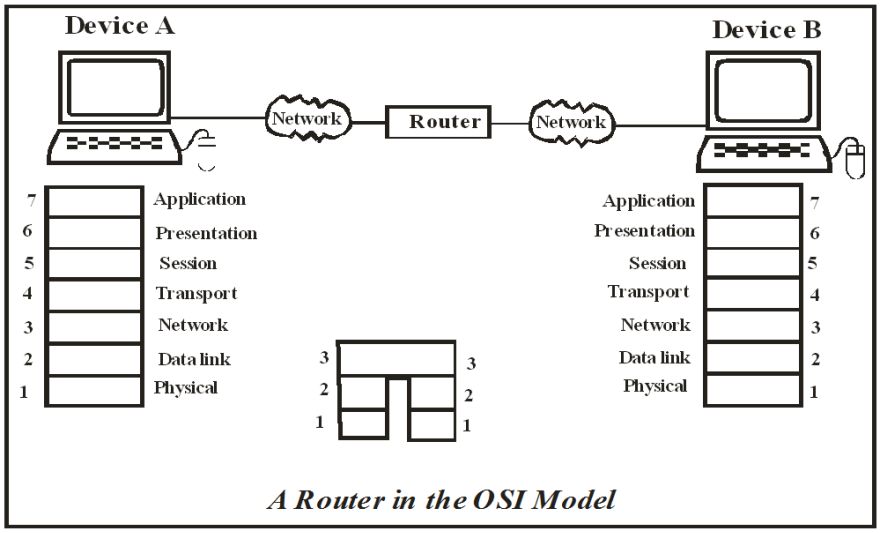
When two or more separate networks are connected for exchanging data or resources, they becomes an inter networking (or internet). Linking a number of LANs into an internet requires additional internetworking devices called routers and gateways. An internet is an interconnection of individual networks. To create an internet, we need internetworking device called routers and gateways. Routers provide links between two separate but same type LANs. Gateways provide links between two incompatible LANs.

3.5.1 ROUTERS

Routers forward the packets among multiple interconnected networks. Routers acts like a station on a network. They receive packets from one connected network and pass them to a second, connected network. If a received packet is addressed to a node on a network of which the router is not a member, the router is capable of determining which of its connected networks the best next point for the packet is. Once a router has identified the best route for a packet to travel, it passes the packet along the appropriate network to another router. That router checks the destination address find what it considers the best route for the packet and passes it to the destination network or across a neigh boring network to the next router on the chosen path.

On the internet, a router is a device or, in some cases, software in a computer, that determines the next network point to which a packet should be forwarded toward its destination. The router is connected to at least two networks and decides which way to send each information packet based on its current understanding of the state of the networks it is connected to. A router is located at any gateway (where one network meet another), including each Internet point – of – presence. A router is often included as part of a network switch.

A router may create or maintain a table of the available routers and their condition and use this information along with distance and cost algorithm to determine the best route for a given packet. Typically, a packet may travel through a number of networking points with routers before arriving at its destination. Routing is a functional associated with the network layer (Layer 3) in the standard model of network programming, the Open system Interconnection (OSI) model. A layer switch is a network. A layer 3 switch is a switch that can perform routing functions. An edge router is a router that interface with asynchronous transfer mode (/a>ATM) network. A router is a network bridge combined with a router.

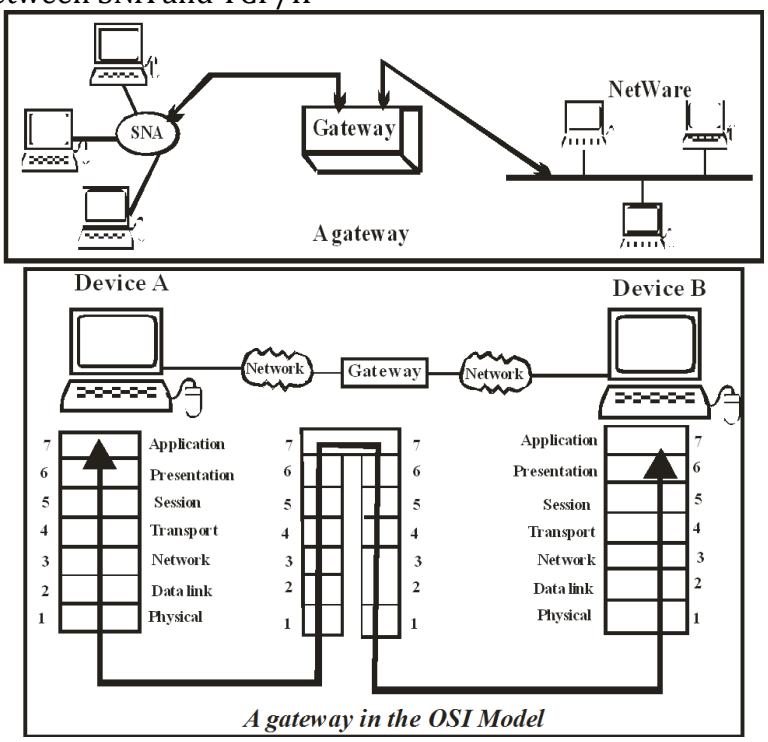


A Router in the OSI Model

3.5.2 GATEWAYS

A gateway is a protocol converter. A router transfers, accepts, and relays packet only across network using similar protocols. A gateway on the other hand, can accept a packet forwarded for one protocol and converter it to packet formatted for another protocol before forwarding it.

A gateway is generally software installed within a router. The gateway understands the protocols used by each network linked into the router and is therefore able to translate from one to another. Gateways potentially operate in all seven layers of the OSI model.
E.g. Connection between SNA and TCP/IP



3.5.3 SWITCHES

A switch is device that providing functionally with greater efficiency.
A switch may act as a multiport bridge to connect devices or segments in a LAN.
The switch normally has a buffer for each link (network) to which it is connected. When it receives the packet, it stores the packet in the buffer of the receiving link and checks the address to find the outgoing link. If the outgoing link is free (no chance of collision) the switch sends the frame to the particular link.
Switching is made based on two different strategies:

- Store – and – forward and
- Cut – through

A store – and – forward switches stores the frame in the input buffer until the whole packet has arrived. A cut –through switch on the other hand forward the packet to the output buffer as the destination address is received.

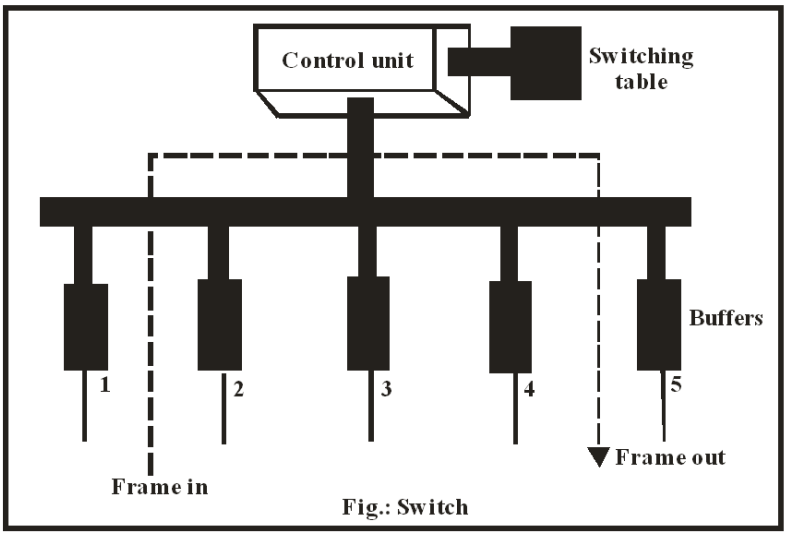


Fig.: Switch

3.5.4 ROUTING SWITCHES

Routing switches are combination of a router and a bridge. These use the network layer destination address to find the output link to which the packet should be forwarded. The process is faster because the network layer software in a regular router finds only the network address of the next station and then passes this information to the data link layer software to find the output link.

3.5.5 ROUTING ALGORITHM

In routing, the pathway with the lowest cost is considered the best. As long as the cost of each link is known, a router can find the optimal combination for any transmission. Several algorithms exist for making this calculation. The most popular are distance vector routing and link state routing.

(i) Distance Vector routing

In distance vector routing each router periodically shares its knowledge about the entire network with its neighbors. It sends whatever knowledge it has about whole network through all of its parts. This information is received and kept by each neigh boring router and used to update that routers own information about the network.

Example

The following figure shows seven LANs interconnected through 6 routers A, B, C, D, E and F. The LANs can be of any type (Ethernet, token ring, FDDI etc.)

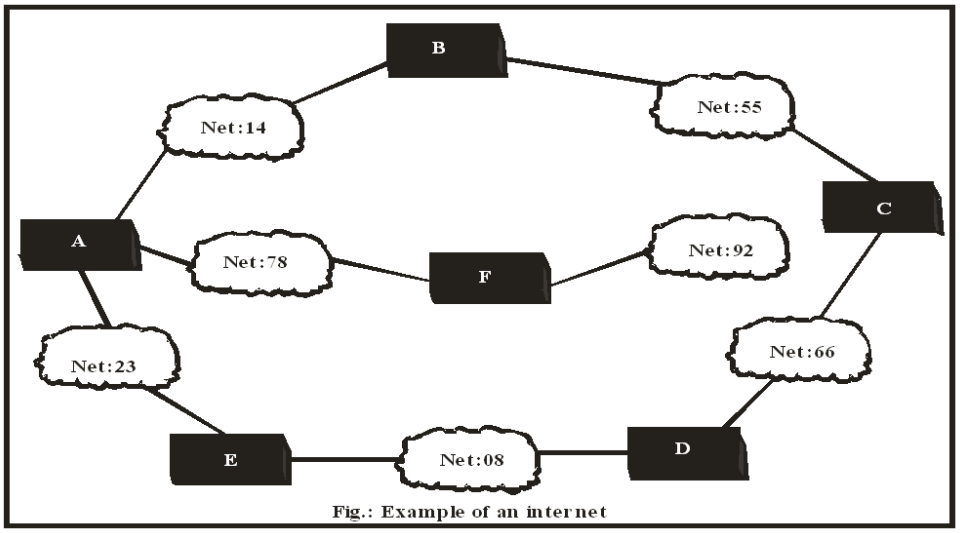


Fig.: Example of an internet

Distance vector routing simplifies the routing process by assuming a cost of 1 unit for every link. In this way the efficiency of transmission is a function of the number of links required to reach a destination. Distance vector routing is therefore based on hop count and not cost count. Each router sends its information about the inter network only to its immediate neighbors. The neighbors add this knowledge to their own knowledge and send the whole table to their own neighbors. In this way the first router gets its own information back plus new information about its neighbor's other neighbors. Each of these neighbors add its knowledge and sends the update table on its own neighbor and so on. Eventually every router knows about every other router in the network.

Example
Bellman- Ford Algorithm

3.5.6 ROUTING TABLE

Every router keeps a **routing table** that has one entry for each destination network of which the router is aware. The entry consists of the destination network address, the shortest distance to reach the destination in hop count, and the next router to which the packet should be delivered to reach its final destination. The hop count is the number of networks that a packet encounters to reach its final destination. The table may contain other information such as the subnet mask or the time this entry was last updated. Table below shows an example of a routing table.

Table: A distance vector routing table

Destination	Hop Count	Next Router	Other Information
163.5.0.0	7	172.6.23.3	
197.5.13.0	5	176.3.6.17	
189.35.0.0	3	200.5.1.6	
115.0.0.0	6	131.3.7.19	

(ii) Link State Routing

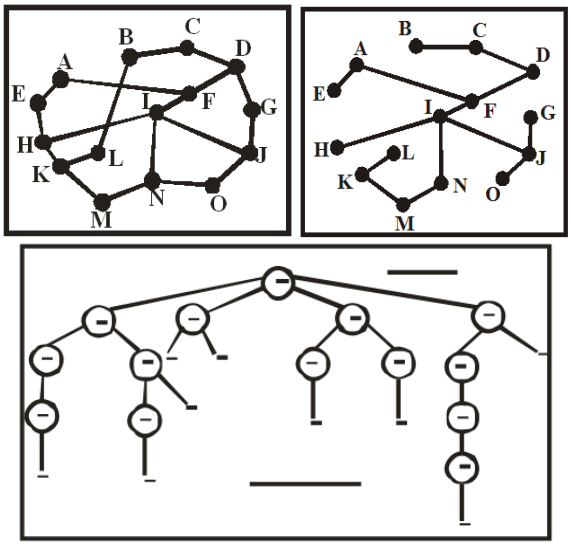
Link –state routing is designed to overcome the drawbacks of distance – vector routing. When a router is initialized, it determines the link cost on each of its network interfaces. The router then advertises this set of link costs to all other routers in the internet topology, not just neighboring routers. From then on, the router monitors its link costs. Whenever there is a significant change (a link cost increase or decreases substantially, a new link is

created, and an existing link becomes unavailable), the router again advertise its se of link costs to all other routers in the configuration.
Because each router receives the link costs of all routers in the configuration, each router can construct the topology of the entire configuration and then calculate the shortest path to each destination network. Having done this, the router can construct its routing table, listing the first hop to each destination. Because the router has a representation of the entire network, it does not use a distributed version of a routing algorithm to determine the shortest paths. In practice, Dijkstra's algorithm is used. The open shortest path first (OSPF) protocol is an example of a routing protocol that uses link-state routing. The second generation routing algorithm for ARPANET also uses this approach.
a) Routing table has entry only for the neighbors.
b) Routing table is sent to all the routers in the network.
c) Routing table is sent only when there is a change in the network.

Each router must:
- Discover its neighbors and learn their network addresses (HELLO packet).
- Measure the delay or cost to each of its has learned.
- Construct a packet telling all it has other routers.
- Compute the shortest path shortest path to all other router.

Example
Dijkstra's algorithm.

(iii) Broadcast Routing
Sending packet to all destinations simultaneously is called broadcasting.
The various broadcasting algorithm are-
(a)Send distinct packet to all destinations
This requires source to have a complete list of destinations.
(b)Flooding
Send the packet on all the outgoing lines expect the line from which it has come.
(c) Multi – destination routing
Each packet contains a list of destination indicating the desired destinations. When a packet arrives at the router, router checks all the destinations to determine the set of output lines that will be needed. The router generates a new copy of the packet for each output line to be used and includes in each packet only those destination that are the line. After sufficient number of hops, each packet will carry only one destination and can be as a normal packet.
Multi destination routing is like separately packets; expect that when several packets must follow the same route, one of them pays full fare and the rest ride free.
(d)Sink tree
A spanning tree is a subnet of the subnet that includes all the routers but contains no loops. When hop count is used as metric, spanning tree is called sink tree. Problem
Each router must have knowledge of some spanning tree for it to be applicable. Sometimes this information is available (e.g. Link state routing) but sometimes it is not (e.g. distance vector routing).
(e)Reverse path forwarding
When a broadcast packet arrives at a router, the router checks to see if the packet arrived on the line that is normally used for sending packets to the source of the broadcast. The router forwards copies of packet arrived on a line other than the one it arrived on. If however the broadcast packet arrived on a line other than the one for reaching the source, the packet is discarded as a likely duplicate.
This is an example of algorithm called path forwarding



Advantage

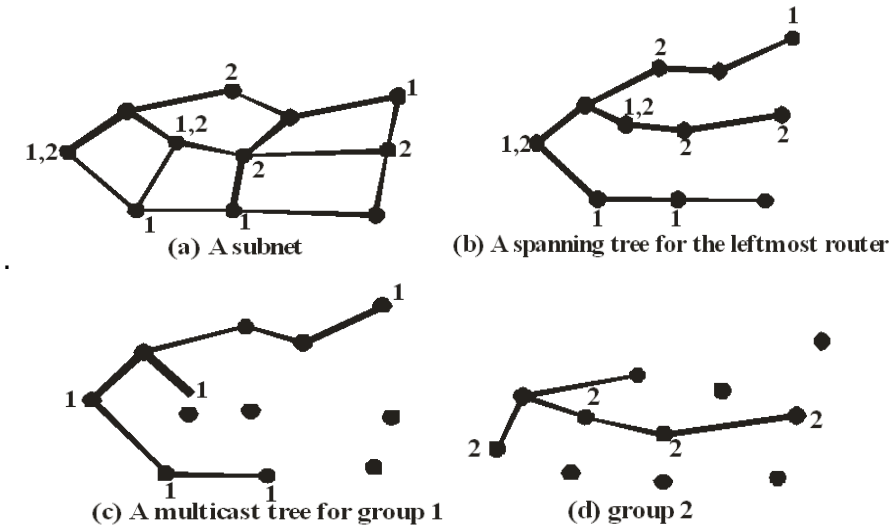
- It does not require routers to know about spanning trees.
- It is efficient and easy to implement.

(iv) Multicasting Routing

- It is frequency necessary to send message to all the other members of a group. If the group is small, point to point messaging is possible. If group is large this is expensive.
- Sending a message to a group is called multicasting and its routing and algorithm is called multicast routing.
- Group management is required, i.e. processes for create, destroy, join and leave group is required. Changes must be informed to the routers.
- To do multicast routing, each router computers a spanning tree covering all other routers in the subnet.
- When a process sends a multicast packet to a group, the first routers examines its spanning tree and prunes it, removing all lines that do not lead to hosts that are members of the group.
- Various ways of pruning a spanning tree are possible:

(i) Link state routing, simple since each router is aware of the complete subnet topology, including which hosts belong to which groups.

(ii) Distance vector routing different pruning strategy has to be used – Reverse path forwarding



3.6 IP ADDRESSING

An IP address is also known as logical address and is used to identify the network in a Wide Area Network (WAN). An IP address is maintained by a protocol Inter- networking protocol (IP). IP is developed in two versions namely Version 3 and Version 6.

3.6.1 IPV4 Addressing

IPV3 address length is 32 bits, represented in dotted decimal notation as follows:

BYTE1. BYTE2. BYTE3. BYTE4

Each Byte is represented in decimal notation, hence in each byte the range of decimal value will be 0 to 255.
Some Special IP addresses include:

First IP address: 0.0.0.0
Last IP address: 255.255.255.255
Loop back IP address: 127.x.x.x

First IP address is used for network interface, Last IP address is used for broadcasting and Loopback IP address is used for self delivery of packets.

Excluding the above, remaining IP addresses are classified into 5 classes as given below:

Class	Subnet Mask decimal	No. of Hosts per Network	No. of Networks	Start -End Address
A	255.0.0.0	16 Million	127	1.0.0.0 - 126.255.255.255
B	255.255.0.0	65000	16000	128.0.0.0 - 191.255.255.255
C	255.255.255.0	254	2 Million	192.0.0.0 - 223.255.255.255
D	Reserved for multicast groups			224.0.0.0 - 239.255.255.255
E	Reserved for future use, or Research and Development Purposes			240.0.0.0 - 254.255.255.254

The numbers of bits for network ID are not sufficient and the numbers of host bits are excess. So, many addresses will be wasted. To reduce the wastage of IP addresses, Sub netting is used.

Private IPv4 addresses:

Class	Private Address Range
A	10.0.0.0 to 10.255.255.255
B	172.16.0.0 to 172.31.255.255
C	192.168.0.0 to 192.168.255

3.6.2 Sub netting

The process of dividing a big network into small networks is called as sub netting. Once sub netting is done, the router needs to compare network ID and Subnet ID both. The number of bits required for subnet ID is borrowed from the Host portion, as the host bits are being excess.

The Subnet Mask for Class A, Class B and Class C is given in above table. According to subnet mask, fixed numbers of bits are allocated for subnet ID, which may cause the wastage or insufficient subnet bits. So, to handle this situation, a class less addressing called, CIDR (Class less Inter Domain Routing) is used.

3.6.3 Super netting (CIDR)

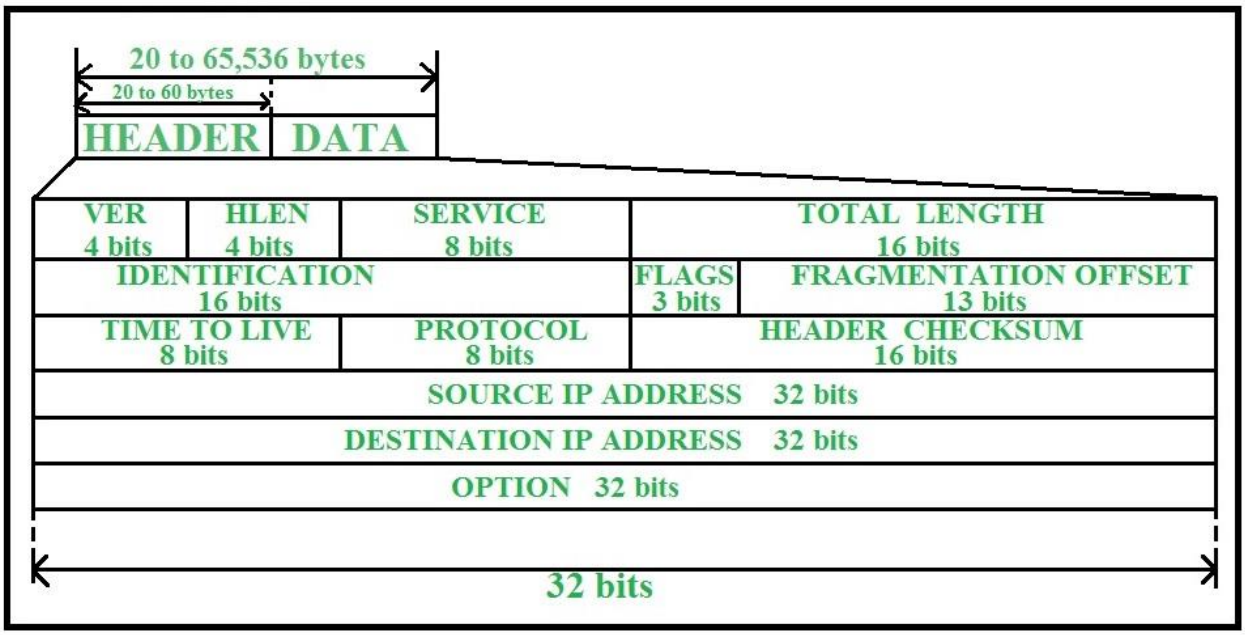
In CIDR notation only network bits are constant and bounded to class restriction, But, subnet bits and host bits are variable according to the network.

For Example, if a class B network is divided into 100 sub networks, then just 7 bits are enough to represent these 100 sub networks, remaining 9 bits are used for host id.

I.e. Network ID = 16 bits, Subnet ID=7 bits, Host ID=9 bits.

CIDR Notation: **W.X.Y.Z/N** is known as CIDR notation, where N represents mask or number of bits required for network ID and subnet ID.

3.7 Inter Networking Protocol (IPv4) format:



1) **Version**
   This four bit defines the version of the IP protocol.
2) **Header length (HLEN)**
   This four bit field defines the total length of the datagram header in four byte words. When the value of field is 5, Header length = 5 × 3 = 20. When the value is 15, the header length is 15 × 3 = 60 bytes.
   are the header and the rest is data upper from layer.

3) Identifier, 4) Flags, Fragmentation Offset

Identifier field indicates to which segment the current datagram belongs to.

DF: Do not Fragment, indicates the intermediate nodes that the current data gram should not be further fragmented.

MF: More Fragments? It indicates, whether the current data gram is last data gram in the respective segment or not. MF=0 indicates, Last fragment.

Fragmentation Offset: It indicates the position of data gram in its respective segment.

5) **Time to live**
   This field is used to control the maximum number of hops (routers) visited by a datagram. When a source host sends the datagram, it stores a number in this field. This value is approximately two times the maximum number of routers between any two hosts. Each router that processes the datagram decrements this number by one. When a

router receives a datagram, it decrements the value of this field by one. If this value becomes zero the router discards the datagram.

6) **Protocol**
This eight bit field defines the higher level protocol that uses the services of the IP layer. An IP datagram may contain data from higher level protocols such as TCP, UDP, ICMP, and IGMP. This field specifies the final destination protocol to which the IP datagram should be delivered.

Value	Protocol
1	IGMP
2	IGMP
6	TCP
17	UDP
31	IPV6

7) **Header Checksum**
The error detection method used by IP is the checksum. The checksum in IP packet covers only the header and not data.
8) **Source address**
The 32- bit field defines the IP address of the destination. This field must remain unchanged during the time the IP datagram travels from the source to destination

3.8 IPv6 ADDRESSING

IPv6 (Internet Protocol version 6) is a set of specifications from the Internet Engineering Task Force (IETF) that's essentially an upgrade of IP version 3 (IPv3). The basics of IPv6 are similar to those of IPv3 -- devices can use IPv6 as source and destination addresses to pass packets over a network, and tools like ping work for network testing as they do in IPv3, with some slight variations.

The length of IPv6 address is 128 bits. An IPv6 address is represented as eight groups of **four** hexadecimal digits, each group representing 16 bits (two octets, a group sometimes also called a hextet). The groups are separated by colons (:).

An example of an IPv6 address is: 2001:0db8:85a3:0000:0000:8a2e:0370:7333.

3.8.1 IPv6 Address Types:

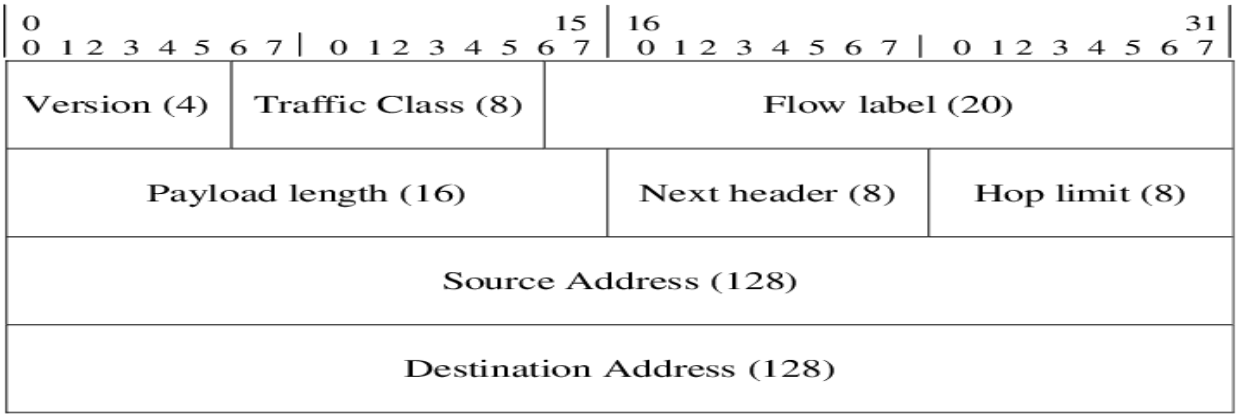
IPv6 has three types of addresses, which can be categorized by type and scope:

- **Unicast addresses.** A packet is delivered to one interface.
- **Multicast addresses.** A packet is delivered to multiple interfaces.
- **Anycast addresses.** A packet is delivered to the nearest of multiple interfaces (in terms of routing distance).

IPv6 does not use broadcast messages.
Unicast and anycast addresses in IPv6 have the following scopes (for multicast addresses, the scope is built into the address structure):

- **Link-local.** The scope is the local link (nodes on the same subnet).
- **Site-local.** The scope is the organization (private site addressing).
- **Global.** The scope is global (IPv6 Internet addresses).

3.8.2 IPv6 Header Format:

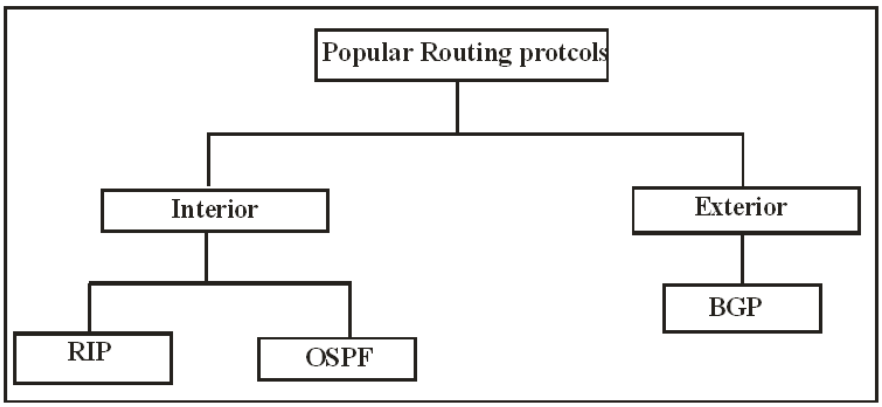


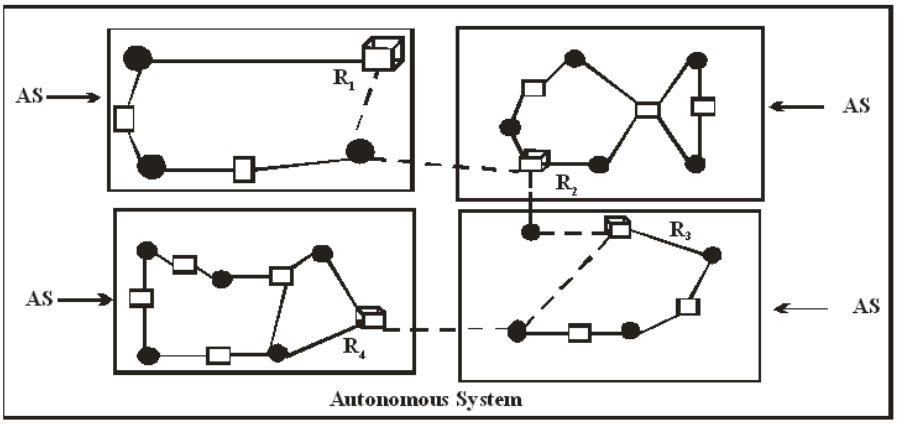
3.9 ROUTING PROTOCOL

Routing tables have been created in response to the demand for the dynamic routing. A routing protocol is a combination of rules and procedures that let routers in the internet inform each other of changes. It allows routers to share whatever they know about the internet or their neighbourhood.

3.9.1 INTERIOR AND EXTERIOR ROUTING

In internet can be so large that one routing protocol cannot handle the track of updating routing tables of all routers. For this reason, an internet is divided into autonomous systems. An autonomous system (AS) is a group of networks and routers under the authority of a single administration. Routing inside an AS is called as interior routing. Routing between autonomous systems is referred to as exterior routing. Each autonomous system can choose an interior routing protocol to handle routing inside the autonomous system and an exterior routing protocol to handle routing between autonomous systems.





3.9.2 RIP

The Routing Information protocol is an interior routing protocol used inside an autonomous system. It is simple protocol based on distance vector routing which uses Bellman – Ford Algorithm for calculating the routing tables.

3.9.3 DISTANCE VECTOR ROUTING

In distance vector routing each router periodically shares its knowledge about the entire internet with its neighbors. The three keys to understand how this algorithm works are-

1) Sharing knowledge about the entire AS: Each router shares its knowledge about the entire autonomous system with its neighbors.

2) Sharing only with neighbors: Each router sends its knowledge only to neighbours. It sends whatever knowledge it has through all of its interfaces.

3) Sharing only with neighbors: Each router its knowledge only to neighbors at fixed intervals Timing in RIP
RIP uses three timers to supports its operator.

- Periodic Timers
- Expiration Timers
- Garbage collection

PERIODIC TIMER

The periodic timer controls the advertising of regular update messages. Although the protocol specifics that this timer must be set to 30 seconds, the working model uses a random number between 25 to 35 seconds. This is to prevent overload on an internet if all routers update simultaneously. Each router has one periodic timer that is set randomly to a number between 25 and 35. It counts down. When zero is reached the update message is sent and the timer is randomly set once again.

EXPIRATION TIMER

The expiration timer governs the validity of a route. When a router receives update information for a route, the expiration timer is set to 180 seconds for that particular route. Every time a new update for the route is received the time is reset. In normal situation this occurs every 30 seconds. If there is a problem on an internet and no update is received within the allowed 180 seconds, the route is considered expired and the hop count of the route is set to 16 which mean the destination is unreachable. Every route has its own expiration timer. Garbage Collection Timer When the information about a route becomes

invalid, the router does not immediately remove it from table. Instead, it continuous too advertises the route with a metric value of 16. At the same time, a timer called the garbage collection timer is set to 120 seconds for that route. When the count reaches zero, the route is removed from the table. This timer allows neighbors to become aware of the invalidity of a route.

3.9.4 OSPF

The Open Shortest First (OSPF) protocol is interior routing protocol used inside an AS. OSPF uses link state routing to update routing tables in an area. An area is a collection of networks, hosts and routers all contained within an autonomous system. An autonomous system in turn, can be divided into much different area. All networks inside the area must be connected. The three keys to understand how this algorithm works:

- Sharing knowledge about the neighborhood: Each router sends the of its neighborhood to every other router in the area.
- Sharing with every other router: Each router sends of its neighborhood to every other router in the area. It does so by flooding. A router sends its information to all of its neighbors (through all of its output ports). Each neighbor sends the packets to all its neighbors and so on. Every router that receives the packet sends copies to each of its neighbors. Eventually every router has received a copy of the same information.
- Sharing when there is a change: Each router shares the state of its neighborhood only when there is a change.

3.9.5 BGP

Border Gateway Protocol (BGP) is an inter – autonomous system routing protocol. BGP is based on routing method called path vector routing. Path vector routing each entry in the routing table contains the destination network, the next router and the path to reach the destination. The path is usually defined as an ordered list of autonomous systems that a packet should travel to reach the destination.

3.10 INTRODUCTION TO TRANSPORT LAYER

The transport layer is responsible for source to destination (end- to –end) delivery of the entire message. Protocols at the layer overseas the delivery of data from an application program on one device to an application program on another device. The transport layer, ensure that the whole message arrives intact and in order overseeing both error control and flow control at the source to destination level.
Examples of transport layer protocols are
i) Transmission control protocol (TCP) and
ii) User Datagram protocol (UDP)

3.11 DUTIES OF THE TRANSPORT LAYER

Transport layer services are implemented by a transport protocol used between entities. The services provided are similar to those of the data link layer. The data link layer is designed to provide its services within a single network, while the transport layer provides these services across an internetwork made of many networks. The data link layer controls the physical layer while the transport layer controls all the lower layers.
The services provided by transport layer protocols can be divided into 5 broad categories.

- End to end delivery

- Addressing
- Reliable delivery
- Flow control and
- Multiplexing

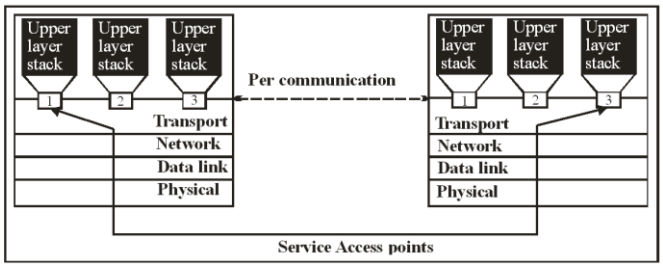
1) End to end delivery

The network layer oversees the end to end delivery packet but does not see any relationship between those packets which belong to a single message. It treats each packet as an independent entity. The transport layer, on the other hand makes sure that the entire message arrives intact and not just a single packet. Thus it oversees the end to end (source to destination) delivery of the entire message.

2) Addressing

Transport layer protocols oversee the delivery of data from an application program on one device to an application program on another device. Let these end points be denoted as Transport Service Access point (TSAP).

- Data Link Layer protocols need to know which two computers within network is communicating.
- Network layer protocols need to know which two computers within an internet are communicating.
- Transport layer protocols need to know which upper layer protocols are communicating.



Note:

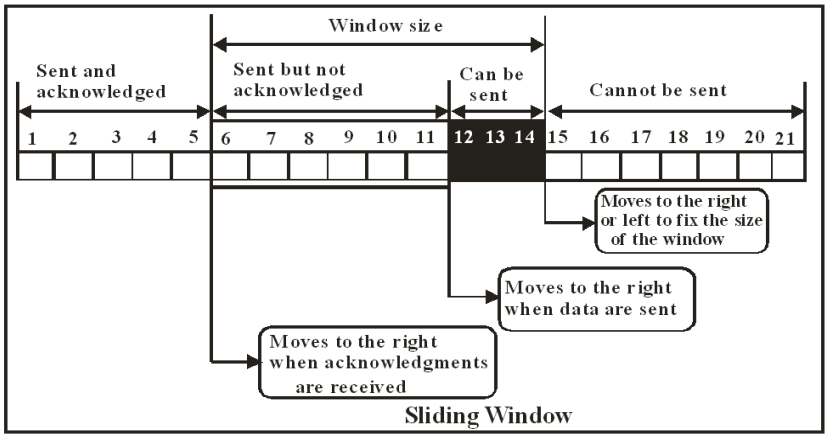
To ensure accurate delivery from TSAP to TSAP another level of addressing is required.

3) Reliable delivery

Aspects of reliable delivery: Error control, Sequence control, Loss control and Duplications control. Error control – This involves error detection and correction, retransmission. Sequence control – Transport layer on the receiving end ensure that whole message arrives intact and order. When the size of the data unit received from the upper layer is too long for the network layer datagram packet or data link layer frame to handle, the transport layer protocols divides it into smaller usable blocks. This dividing process is called segmentation. When on the other hand, the size of the data units belonging to a single session are so small that several can fit together into a single packet or frame, the transport layer combines then into a single data unit. The combining process is called concatenation. Sequence numbers: Transport layer divides a message into transmittable segment called packets and assign a sequence number to each segment. The number indicates the order for reassembly. When several shorter units are concatenated, the number at the end of each subunit is added. This number allows separating them accurately at the destination. Loss control – The transport layer ensure that all pieces of transmission arrives at the destination not just some of them. When data is segmented for delivery, some segment may be loss in transmit Sequence numbers allow the receiver's transport layer protocols to identify any missing segment and request for retransmission. Duplication control – Transport layer ensure that no piece of data arrives at the receiving end duplicated. Sequence numbers allow the receiver's transport layer protocol to identify and discard duplicate segments.

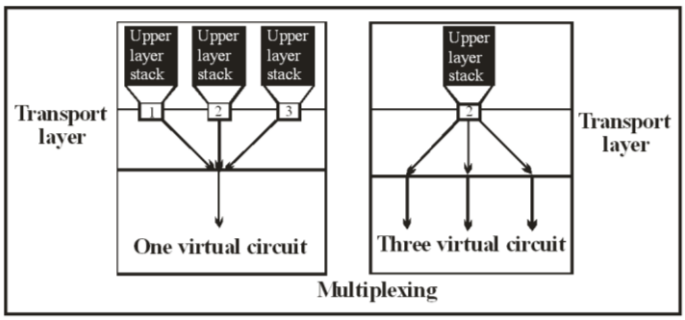
4) Flow Control

Transport layer is responsible for end to end flow control. It is sliding window protocols for flow control. However, the window at the transport layer can vary in size to accommodate buffer occupancy.



With a varying size window the actual amount of data the window can hold is not fixed. The receiver in its acknowledgement packet can specify the size of the window be increased or decreased. In most cases sliding window at the transport layer are based on the number of bytes that the receiver can accommodate. A sliding window is used to make data transmission more efficient as well as to control the flow of data so that the receiver does not become over crowed. To accommodate the variability in size, transport layer sliding windows use three pointers which act as virtual walls to identify the buffers. The left wall moves to the right when ACKs are received. The middle wall moves to the right as data are sent. The right wall moves to the right or left to fix the size of the window. If acknowledgments are received and the size of the window is not changed, the third wall moves to the right keep the size of the window constant.

5)Multiplexing



To improve transmission efficiency, the transport layer has the option of multiplexing. Multiplexing at this layer occurs in two ways:

- **Upward:** Many transport layers use the same network connection.
- **Downward:** One transport layer uses many network connections.

i) Upward:

The transport layer uses virtual circuits based on the lower three layers. Normally the underlying networks charge for each virtual circuit connection. To make it cost effective, the transport layers can send several transmission of the same destination along the same path by multiplexing, by using an already established circuit.

ii) Downward:

Downward multiplexing allows the transport layer to split a single transmission among a number of different paths to improve throughput (speed of delivery). This option is useful when the underlying network have low or slow capacity. For example some network layer

protocols have restrictions on the size of packet sequence numbers that can be handled. If 3 bit sequence numbering code is used, then sequence numbers are restricted to the of 0....7...i.e. only eight packets may be sent before acknowledgment is required. In this case use more throughputs can be unacceptably low. To improve throughput, transport layer protocols can use more than one virtual circuit at the network layer. By sending several data segments at once the delivery can be made much faster.

3.12 CONNECTION

End to end delivery can be accomplished in two modes:

- Connection oriented
- Connectionless

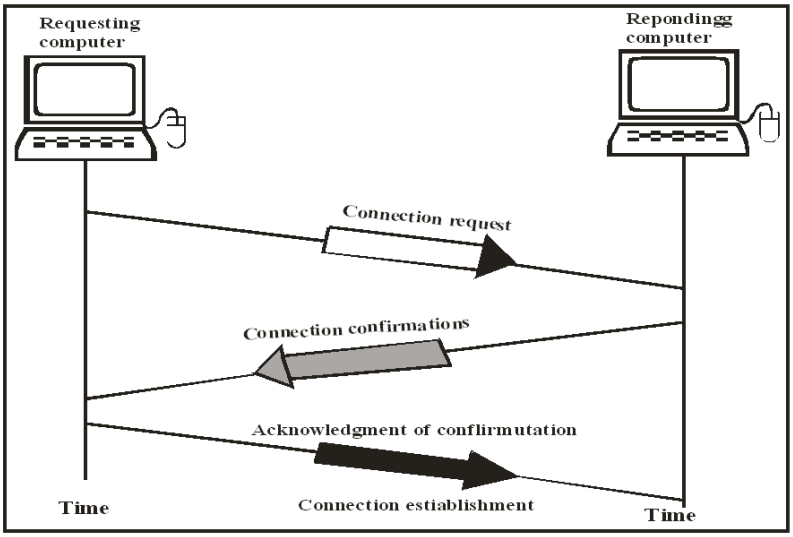
A connection oriented protocols establishes a virtual circuit or pathway through the internet between the sender and receiver. All of the packets belonging to a message are than sent over the same path. Using a single pathway for the entire message facilitates the acknowledgment process and retransmission of damaged or lost frames. Connection oriented services, therefore are generally considered reliable.
Connection oriented transmission has three stages:

- Connection Establishes
- Data transfer and
- Connection Termination

3.12.1 CONNECTION ESTABLISHMENT

It requires three actions, so it is called as three ways Handshake

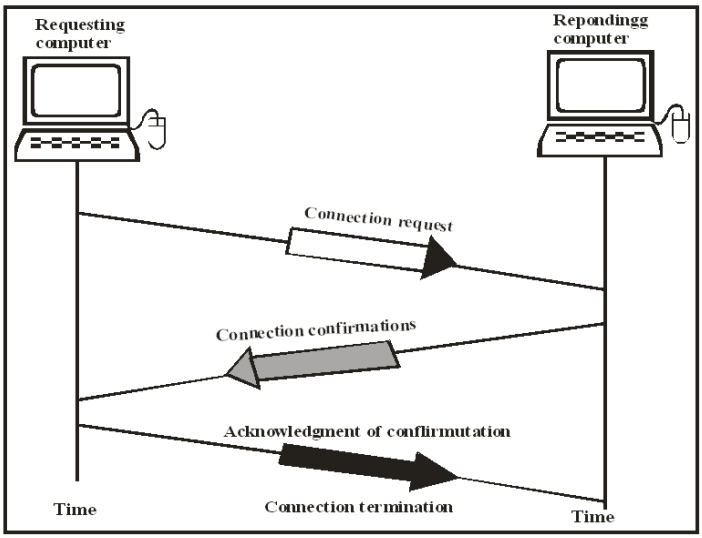
- The computer requesting the connection sends a connection request packet to the intended receiver.
- The responding computers returns connection accepted (confirmation) packet to the requesting computer.
- The requesting computer returns a packet acknowledging the configuration.



3.12.2 CONNECTION TERMINATION

- Connection termination requires three ways Handshake.
- The requesting computers send a disconnection request packet.

- The responding computer confirms the disconnection request by sending disconnection confirmation.
- The requesting computers send Acknowledgment of confirmation.



3.13 OSI TRANSPORT PROTOCOL

3.13.1 Transport Protocols Data unit (TPDU)

Length One byte **length** field indicates the total number of bytes in TPDU.
Fixed Parameters
It consists of five parts:

i) Code: The code identifies the data unit type.
CR: Connection Request
CC: Connection confirm
DR: Disconnect Confirm
DT: Data
ED: Expedited Data
AK: Data Acknowledge
EA: Expedited Data Acknowledge
RJ: Reject TPDU
ER: ERROR TPDU

ii) Source and destination reference:
It contains the address of the original sender and the ultimate destination of the packet.

iii) Sequence number:
Segment sequence number

iv) Credit Allocation:
Credit allocation enables a receiving station to tell the sender how many more data units may be sent before the sender must for an ACK. For example when a receiver returns ACK3 and credit 7, means that the units 0 to 2 have been received successively and the next expected unit is number 3 and that seven more units may be sent before the sender must wait for another acknowledgement.
Variable parameters It contains the control codes used mostly for management.

Data:

The data section contains a regular data or expedited data coming from the upper layers. Expedited Data consist of a high priority message that must be handled out of sequence.

3.13.2 TCP/ IP PROTOCOL SUITE

TCP/ IP were designed prior to the OSI model. Therefore the layers in the TCP/ IP protocols suite do not match exactly with those in the OSI model. The TCP/IP protocols suite is made of five layers, Physical, Data link, Network, Transport and Application.

1)Physical and Data Link Layers

At the Physical and Data link layers TCP/IP does not define any specify protocols. It supports the protocols defined by the underlying networks. A network in TCP/IP internetwork can be a local area network (LAN), a metropolitan area network (MAN) or a wide area network (WAN).

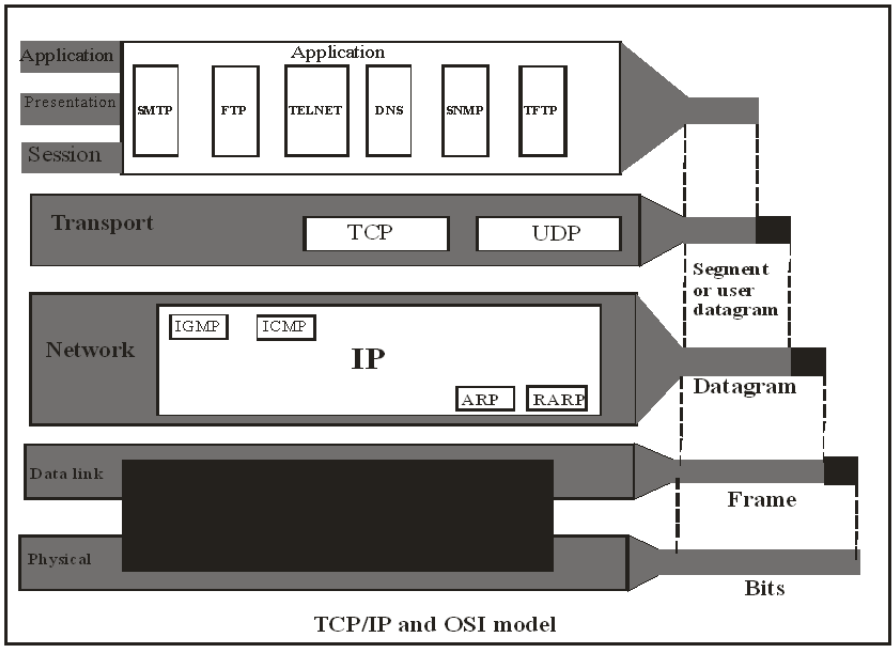
2)Network Layer

At the network layer, TCP/IP supports the internet Protocols (IP). IP contains four supporting protocols: ARP, RARP, ICMP and IGMP.

- Internet protocols (IP): The internet protocol, IP is the transmission, mechanism used by the TCP/IP protocols. It is an unreliable and connectionless datagram protocols – a best effort delivery service. The term best effort means that it provides no error checking or tracking. IP assumes the unreliability of the underlying layers and does its best to get a transmission through to its destination but with no guarantee.
- IP transport data in packets data in packets called datagram each of which is transported separately. Data gram can travel along different routers and can arrive out of sequence or be duplicated. IP does not keep track of the routers has no facility for recording datagram once they arrive at their destination.
- Address Resolution Protocol (ARP): It is used to translate the protocol address to an equivalent physical hardware address. On a physical network each device on a link is identified by a physical address of the node when its IP address is known.
- Reverse Address Resolution Protocol (RARP):
  RARP is used to find IP address of the station or node when it's when its physical address is known.
- Internet Control Message Protocol (ICMP):
  ICMP is a mechanism used by hosts and routers (Gateways) to send notification of datagram problem back to the sender. ICMP sends query and error messages.
- Internet Group Message Protocol (IGMP):
  IGMP is used to help simultaneous transmission of a message to a group of recipients.

3) Transport Layer

The transport layer in TCP/IP is represented by two protocols: TCP and UDP.
TCP and UDP are responsible for delivery of a message form, source application to destination application.



TCP/IP and OSI model

- User datagram Protocols (UDP):
  UDP is a protocol that adds only port addresses, checksum error controls.
  UDP is an unreliable connectionless protocol.
- Transmission Control Protocols (TCP):
  The TCP provides full transport layer services to applications. TCP is a reliable stream transport layer protocol. The term stream means connection oriented. A connection must be establishes between both ends prior to the data exchange.
  At the sending end of each transmission, TCP divides a stream of data into smaller units called segments. Each segment includes a sequence number for reordering. At the receiving end TCP collects each datagram as it comes in and reorders the transmission based on sequence number.

4) Application Layer

It is equivalent to combined Session, Presentation and Application layers in the OSI model.

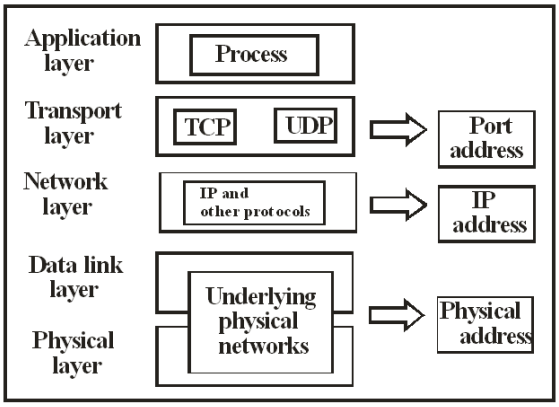
3.14 ADDRESSING

Three different levels of addresses used in an internet using the TCP/IP protocol

- Physical address
- Internet address
- Port address

1) Physical address

The physical address is the address of a node as defined by its LAN or Wan. It is the lowest level address. The physical address have authority over the network (LAN or WAN). The size and format of these addresses vary depending on the network. Physical addresses can be either uncast. i.e. one single recipient, multicast (a group of recipients) or broadcast (to be received by all system in the network).



2) Internet Address

To provide uniform addressing in an internet, TCP/IP protocols define an addressing scheme which is independent of underlying physical address. User, application program and higher layers of protocols software use this address to communicate. Physical addresses are not adequate in an internetworking environment where different network can have different address formats. An internet address is currently 32 bit address which uniquely defines a host connected to the internet. No two devices on the internet can have the same IP addresses.

3) Port Address

The IP address and the physical are necessary for a quantity of data to travel form source to the destination host. However, the end objective of internet communication is a process port address. A port address in TCP/IP is 16 bits long.

3.14.1 IP ADDRESSING

An internet is made of a communication of physical network (LANS or WANS) connected by routers. For a host to communicate with any other host, we need a universal identification system. In other words, we need to name each host uniquely.

- To provide uniform addressing in an internet, TCP/IP protocols software defines an addressing scheme which is independent of underlying physical address. Users, application program and higher layer of protocols software use these addresses to communicate.
- In the TCP/IP protocol, addressing is addressing is specified by the Internet Protocols (IP). The IP standard specifies 32- bit binary address to each host. This address is called Internet Protocols Address or IP Address. Each packet sent across an internet contains 32 bit IP address of the sender (source) as well as the intended recipient (destination). This to transmit information across a TCP / IP internet, a computer must know the IP address of the remote computer to which the information is being sent.
- An IP address is a 32 bit binary address that uniquely defines a host on the internet. The IP addresses are unique. They are unique in the sense that each address defines one and only one device (host or router) on the internet. IP addresses are universal in the sense that the addressing system must be accepted by any host that wants to be connected to the internet.
- Each IP address consists of four bytes, defining two parts: net id host id.
  Net id – identifies a network
  Host id – identifies the host on the network.

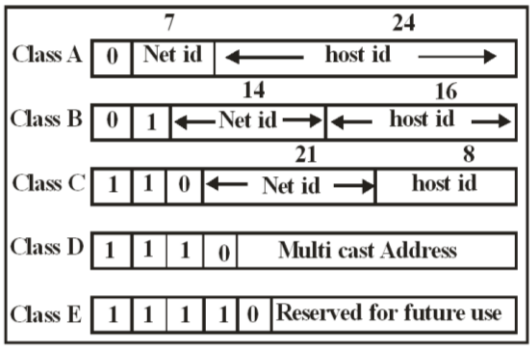
Net id	Host id

- No two networks can be assigned the same net id and no two computers on the same

network can be assigned the same host id.

3.14.2 CLASSES

IP addresses are divided into five different classes: A, B, C, D and E. These are assigned to cover the needs of different types of organizations.



Class A:
Leftmost bit = 0 defines Class A. The remaining 7 bits defines different networks.
Theoretically, we can have 2^7 = 128 networks. Net id = 7 bits + 1 bit class type. Host id = 24 bits i.e. each network can theoretically have 2^{24} hosts. Class A addresses are designed for organization that may have huge number of computer attached to their networks

Class B:
Two left bits = 10 define class B. The next 14 bits define different networks we can have 2^{14} = 16, 384 class B networks.Net id = 14 bits + 2 bits class type.
Host id = 16 bits i.e. each network can theoretically have 2^{16} hosts.
Class B addresses are designed for mid size organization that may have a large number of computers attached to their networks.

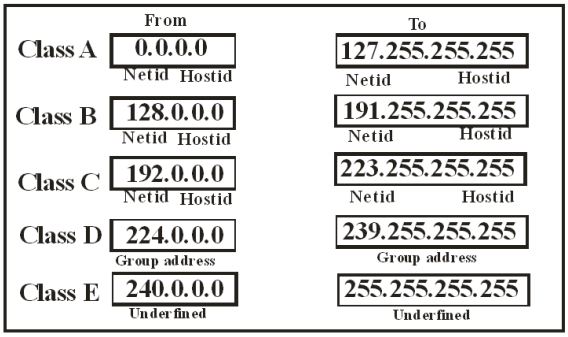
Class C:
Leftmost bits = 110 define class C. The next 21 bits define different networks. We can have 2^{21} networks.
Net id = 21 bits + 3 bits class type.
Host id = 8 bits i.e. network can theoretically have 2^8 hosts.
Class C addresses are defined for small organization that has a small number of computers attached to their networks.

Class D:
The class D address is defined for multicasting. In this case there is no host id, no net id. The whole address is used for multicasting. The first 4 bits (1110) define the class type. The remaining 28 bits define different multicast addresses.
Class E:
Class E is reserved by the Internet for special use: No net id, No host id. The left most 4 bits (1111) define the class.
Decimal Notation:

- If the first number is between 0 and 127, the class is A.
- If the first number is between 128 and 191, the class is B.
- If the first number is between 192 and 223, the class is C.
- If the first number is between 224 and 239, the class is D.

- If the first number is between 240 and 255 the class is E.

Classes using decimal notation:

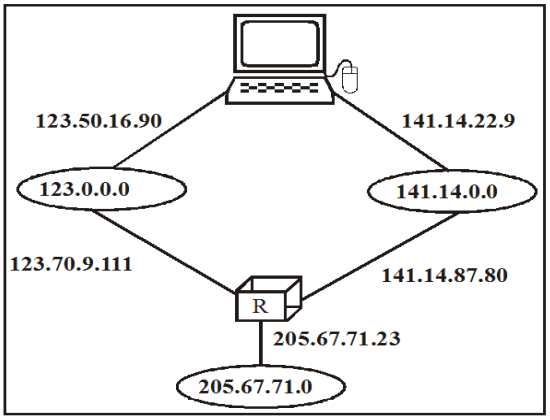


Number of networks and hosts in each class:

Class	No. of network	No. of Hosts
A	126	16,777, 214
B	16384	65, 534
C	2097152	254
D	Not application	Not applicable
E	Not applicable	Not applicable

3.15 MULTIHOMED DEVICE

- An Internet address defines the nodes connected to the network. Any device connected to more than one network must have more than one Internet addresses. In fact a device has a different address for each network it is connected to.
- A computer that is connected to different networks is called multi homed computer and will have more than one address, each possibly belonging to a different class.
- A router is connected to more than one network therefore; a router definitely has more than one IP address one for each interface.

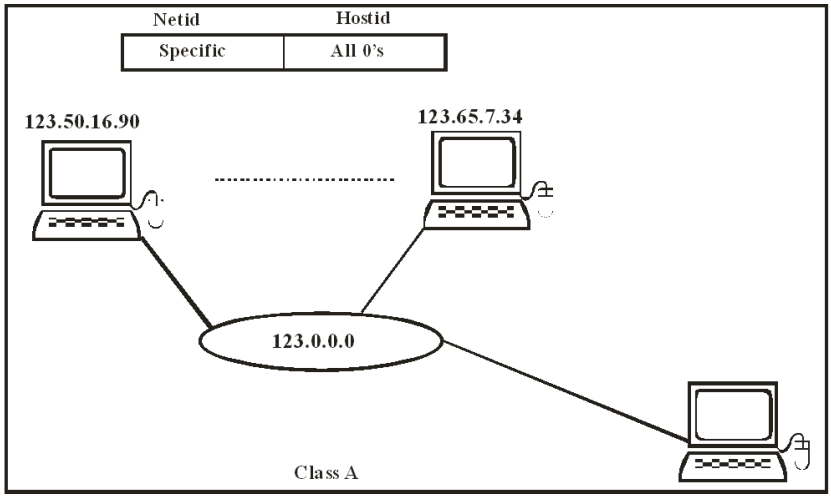


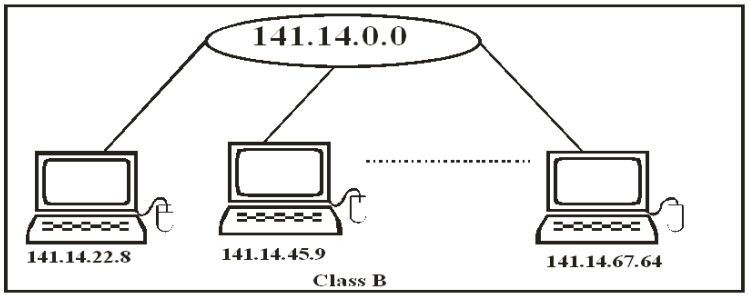
SPECIAL ADDRESS

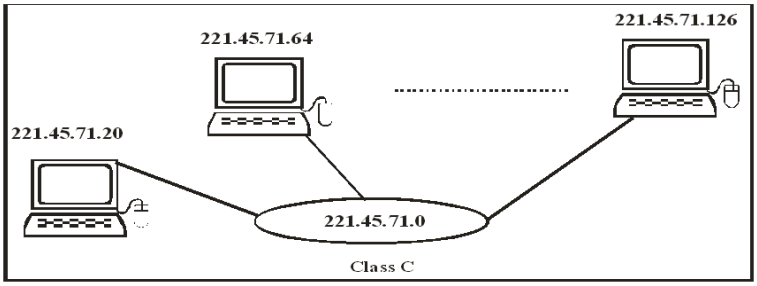
Special address	Net id	Host id
Network Address	Specific	All 0s
Direct Broadcast Address	Specific	All 0s
Limited Broadcast Address	All 1s	All 1s
This host on this network	All 0s	All 0s
Specific host on this network	All 0s	Specific

1) Network address

In classes A, B and C an address with a host id of all zeros is not assigned to any host, it is reversed to define the network itself. This address cannot be used to define a source or destination address in an IP packet.





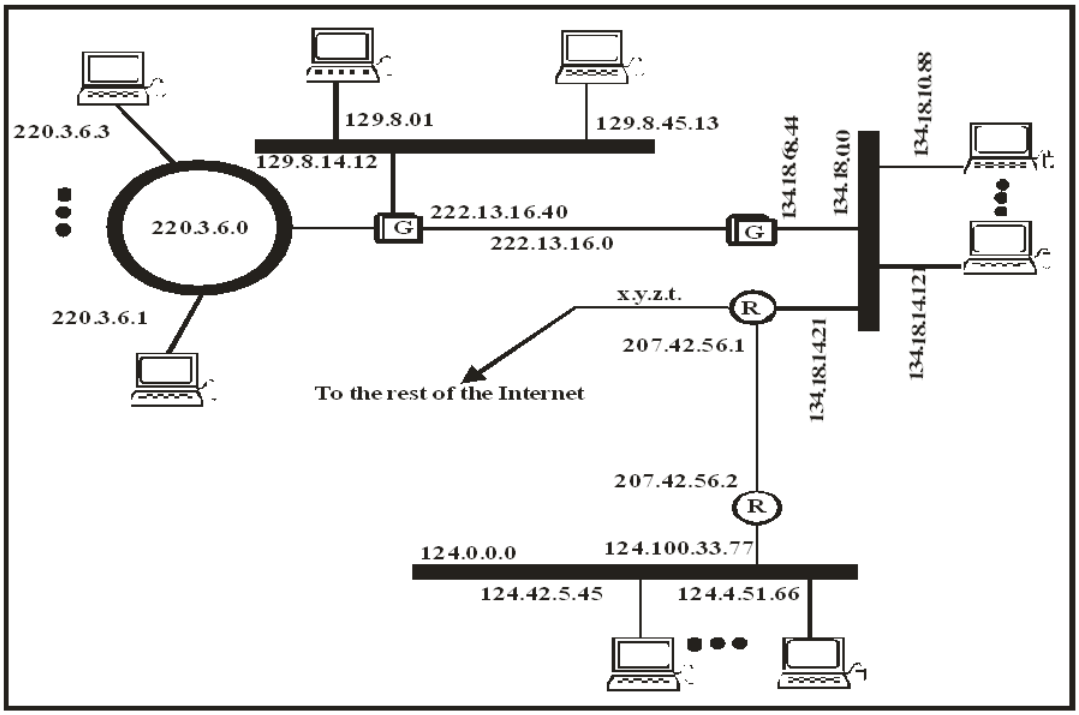


2) Direct broadcast address

It is used by a router to send a packet to all hosts in a specific network. All hosts will accept a packet having this type of destination address.

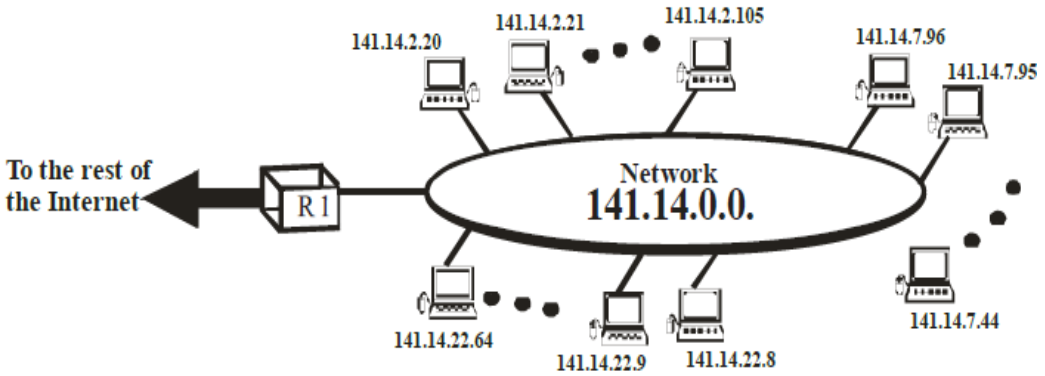
3) Limited broadcast address

An host that wants to send message to every other host in the network can use this address in an IP packet. However, a router will block a packet having this type of address to confine the broadcasting to the local network. This address belong to class E.

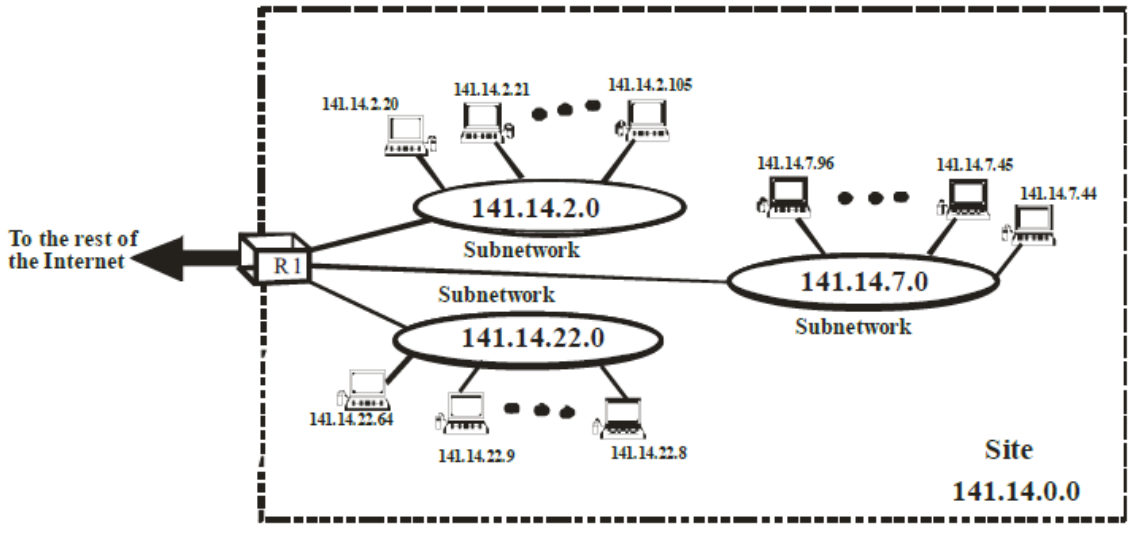


3.16 SUBNETTING AND SUPERNETTING

IMP: Sub netting



A n/w with 2 levels of hierarchy (not subnetted)



A n/w with 3 levels of hierarchy (not subnetted)

In Sub netting a network a network is divided into several smaller sub networks with Each sub network (or subnet) having its own sub network address.

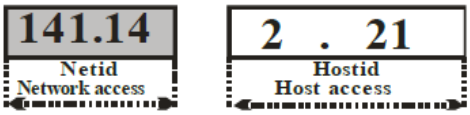
3.16.1 SUPER NETTING

In super netting, an organization can combine several class C addresses to create a Large range of addresses. In other words several networks are combined to create a Super networking.

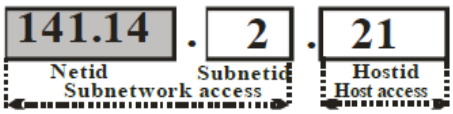
3.16.2 SUB NETTING

The rest of the internet is not aware that network is divided into three physical sub networks. The three sub networks still appear as a single network to the rest of the internet.
IP address is now divided into three levels: net id, subnet id and host id.

- Net id defines site i.e. network.
- Sub net id defines the physical sub network.
- Host id defines the connection of the host to the sub network.



a. Without subnetting



b. With subnetting

When the datagram arrives at router R_1 the interpretation of IP address changes. Router R_1 knows that the network 141.14 is physically divided into three sub networks. It knows that last two octets define two things: Subnet id and host id. Therefore last two octets 2.21must be interpreted as:
Subnet id = 2 host id = 21
Router R_1uses the first two octets (141.14) as net id, the third octet (2) as subnet id and the fourth octet (21) as the host id.

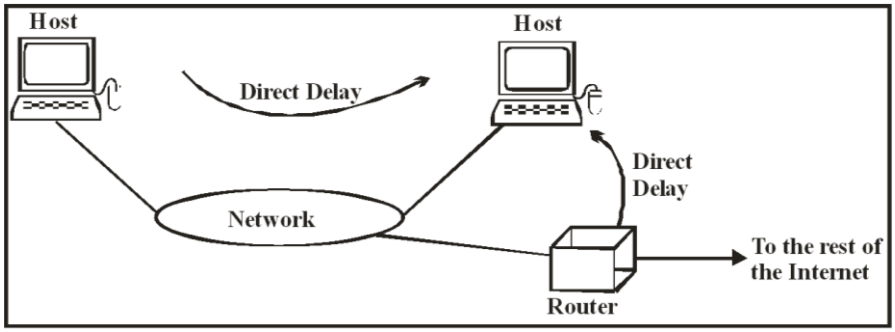
3.17 IP DATAGRAMS AND ROUTING

The IP protocol s a connectionless protocol. It is designed this way because, IP as an internetwork protocol may have to deliver the packets through several heterogeneous networks. If IP were to be connection oriented, all of the networks in the internet should also be connection oriented which is to the case. The delivery of packets to its final destination is accomplished using two different methods of delivery:

- Direct and
- Indirect

3.17.1 Direct Delivery

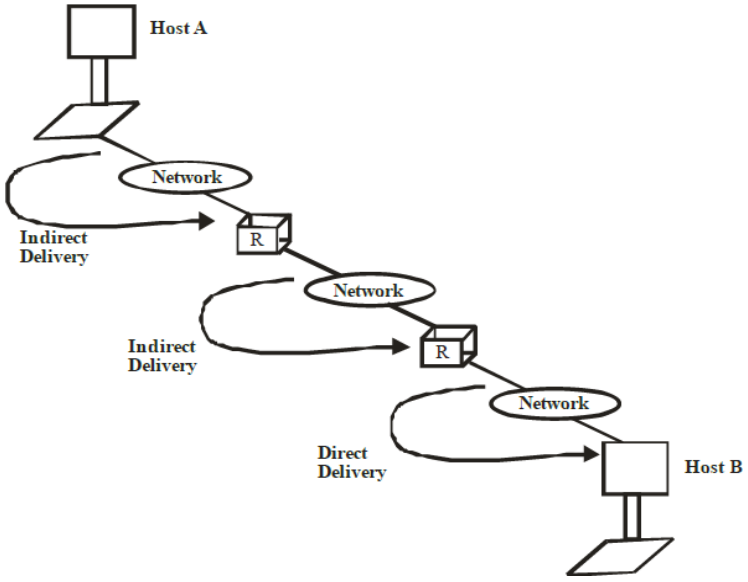
Direct delivery occurs when source and destination of the packet are located on the same physical network or if the delivery is between the last router and the destination host.



The sender can easily determine if the delivery is direct. It can extract the network address of the destination packet and compare this address of the networks to which it is connected. If a match is found, the delivery is direct.

3.17.2 INDIRECT DELIVERY

If the destination host is not on the same network that of the sender, the packet is delivered indirectly. In indirect delivery, the packet goes form router to router until it reaches until it reaches to the router that is connected to the same network to which final destination host is connected. In an indirect delivery, the sender uses the destination IP address and a routing table to find the IP address of the number of routers to which the packets should be delivered. The sender then uses ARP protocol to find the physical addresses of the next router.



3.17.3 FORWARDING IP DATAGRAM

Packets in the IP layer are called Datagram. A source host creates a packet and then sends the packet to a nearly router. When a router receives the packet the router then determines a next hop to which the packet should be sent. The router then forwards the packets to the next hop- either the final destination or another router. Each router maintains a routing table. It contains the set of entries that each specify a destination and the next hop used to each that destination. Each destination in a routing table corresponds to a network, the number of entries in a routing table is proportional to the number of networks in an internet. The routing tables can either static or dynamic. A static table is one that is not changed frequently. A dynamic table on the other hand is updated automatically when there is a changed somewhere in the internet.

3) Service types

This 8 – bit field how the datagram should be handle by the routers.

4) Total length

This is 16 – bit field that defines the total length (header + data) of IP datagram in bytes. Length of data = Total length – Header length. Since the field length is 16 bits, the total length of IP datagram is (2^{16} – 1) bytes i.e. 65535 bytes out of which 20 to 60 bytes

3.18 INTERNET PROTOCOL

The internet protocol (IP) is the transmission mechanism used by TCP / IP protocols. It is an unreliable and connectionless datagram protocol – a best effort delivery service. IP is a connectionless protocol designed for packet switching network hardware, the underlying hardware may misbehave. As a result, IP datagram may be lost, duplicated, delayed delivery out of order or delivered with corrupted data. Higher layers of protocol software are required to handle each of these errors.

3.18.1 DATAGRAM

A datagram is a variable length packet consisting of two parts: header and data. The header can be from 20 to 60 bytes and contains information essential to routing and delivery

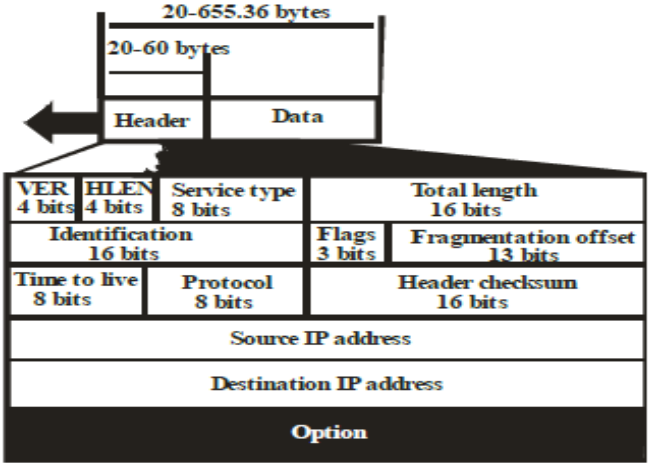
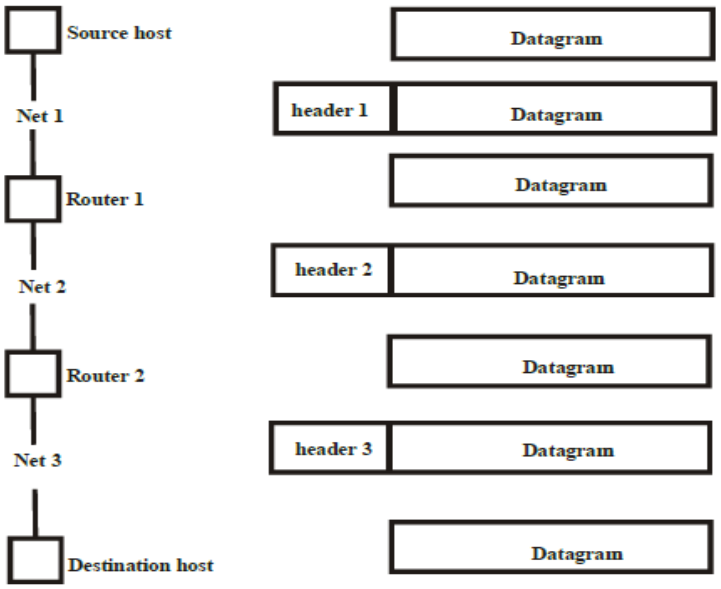


Fig.: IP datagram

3.18.2 IP ENCAPSULATION

3.18.2.1 FRAGMENTATION

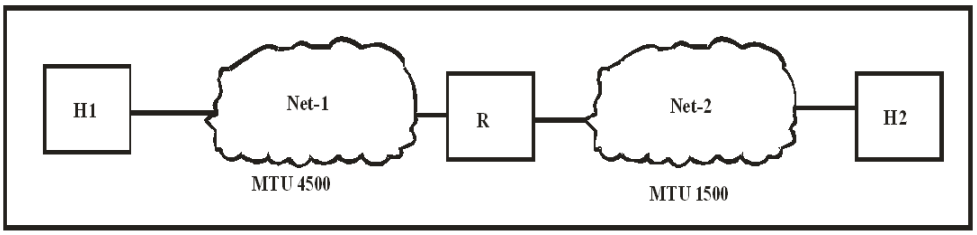
When a host or router handles a datagram, IP software first selects the next hop which the datagram should be sent, then encapsulates the datagram in a frame and transmits the results across the physical network to the next hop.



A datagram can travel through different networks. When the frame reaches the next hop, the receiving software removes the IP datagram and discards the frame. If the datagram is to be forward across another network, a new frame is created.
The following figure illustrates how a datagram appears. Each router encapsulates the IP datagram from the and then encapsulates it in another frame. The format and the size of the received frame depend upon the protocol used by the physical network through which the frame has just traveled. The format and the size of the sent frame depend on the protocol used by the physical network through which the frame is going to travel. For example, if router connects on Ethernet network to a token ring network, it receives a frame in the Ethernet format and sends a frame in the token ring format

3.18.2.2 MAXIMUM TRANSFER UNIT

Each hardware technology specifies the maximum amount of data that a frame can carry. The limit is known as a maximum transmission unit (MTU). The network hardware is not designed to accept or transfer frame s that carries more data than the MTU allows. Thus a datagram must be smaller than or equal to the network MTU. The value of MTU differs from one physical network protocols another. Consider a router that interconnects two networks with MTU values of 4500 and 1500.



If H_1 sends a 4500 byte datagram to H_2, router R will receive the datagram but will not be able to send it across network – 2. When a datagram is larger than the MTU of the network over which it is to be sent, the router divides the datagram into smaller pieces called fragments and sends each fragment and sends each fragment independently. When a datagram is fragmented, each segment has its own header. A fragments datagram may itself be fragmented if it encounters a network with an even smaller MTU. In other words, a datagram can be fragments several times before it reaches the final destination. A datagram can be fragments by the source host or any source host or any router in the path. The

reassembly of the datagram, however, is done only by the destination host because each fragment becomes an independent datagram. Whereas the fragmented datagram can travel through different routes, and we can never control or guarantee which route a fragmented datagram may take, but all the fragments belonging to the same datagram finally arrives at the fragments at the destination host. So it is logical to do fragmentation offset and the length. The rest of the field must be copied. The value of checksum must be recalculated regardless of fragmentation.

3.18.2.3 FIELDS RELATED TO FRAGMENTATION

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

1) Identification:

The 16 bit field identifies a datagram. The combination of the identification and the source IP addresses must uniquely define a datagram as it leaves host. To guarantee unusualness, the IP protocol uses a counter to label the datagram. The counter is initialized to a positive number. When the IP protocol sends a datagram, it copies the current value of the counter in to the identification field and increscent the counter by one. 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 into all fragments. In other words all fragments have the same identification number, which is also the same as he original datagram. The identification number helps the destination in reassembling the datagram. It knows that all fragments having the same identification value should be assembled into one datagram.

2) Flags:

This is three bit field. The first but is reserved. The second but is called the “Do not fragment” 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 error message to the source. If its value is 0, the datagram can be fragmented if necessary. The second 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.

3) 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 measure in units if eight bytes.

3.18.3 REASSEMBLY

The process of creating a copy of the original datagram from fragments is called reassembly. Because each fragment begins with a copy of the original datagram header, all fragments have the same destination address as the original datagram from which they were derived. The internet protocol specifies that ht ultimate destination host should reassemble fragments. All the fragment having same identification number corresponds to the same datagram. Fragments are arranged in the order of offset values. Fragment with 3rd bit of along field = 0 corresponds to the last fragment.

3.18.4 FRAGMENT LOSS

IP does not guarantee datagram delivery. If an underlying network drops packet an encapsulated datagram or fragment can be lost. When all fragments from a datagram arrive

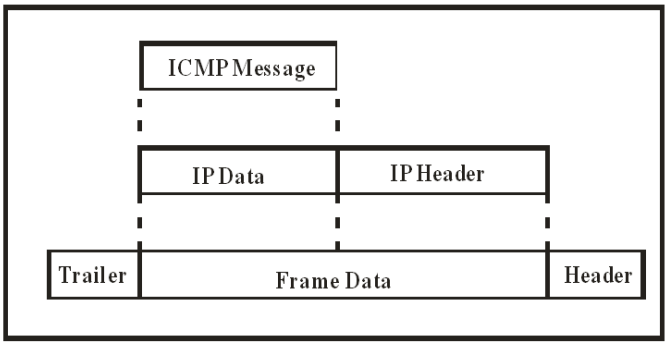
the datagram can be reassembled. A problem arises when one or more fragments from a datagram arrive and some fragments are delayed or lost. Datagram although cannot be reassembled, the receiver must save the fragments. A receiver cannot hold fragments an arbitrarily longtime because fragments occupy space in the receiver's memory. To avoid exhausting memory, IP specifies a max time to hold fragments. When the first fragments arrive from a given datagram, the receiver starts a timer. If all fragments of a datagram arrive before the timer expires, the receiver cancels the timer and reassembles the datagram. However if the timer expires before al fragments arrive, the receiver discards those fragments those fragments that have arrived. The result of IP's reassembly timer is al or nothing, either all fragments arrive and IP reassembles the datagram, or IP discards the complete datagram. In particular, there is no mechanism for a receiver to tell the sender which fragments have arrived. The design makes sense does not know about fragmentation. If the sender did retransmit the datagram, routes may be different, which means retransmission would not necessarily traverse the same route. Hence, there is no guarantee that a retransmitted datagram would not be fragmented in the same way as the original.

3.18.5 INTERNET CONTROL MESSAGE PROTOCOL (ICMP)

(An Error Reporting Mechanism)

The IP provides an unreliable and connectionless datagram delivery. It was designed this way to make efficient use of network resources. Te IP protocol is a best effort delivery service that delivery service that delivers a datagram from its original final destination. However it has two deficiencies: lack of error control and lack of assistance mechanisms. The IP protocol has no error reporting or error correcting mechanism. IP protocol also lacks a mechanism for host and management queries. A network manager needs information from another host or router. The ICMP has been designed to compensate for the above two deficiencies. These two protocols are co- dependent. IP uses ICMP when to send an error message and ICMP uses IP to transport message.

ICMP itself is a network layer protocol. However its message is not passed directly to the data link layer as would be expected. Instead, the messages are first encapsulated inside IP datagram before going to the lower layer as shown in the following figure. The value of the protocol field in the IP datagram header is 1 to indicate that it is ICMP protocol.



3.18.5.1 TYPES OF MESSAGES

ICMP messages are divided into broad categories

- Error reporting messages and
- Query messages.

The error reporting message report problem that a router a host (destination) may encounter when it processes an IP packet. The query messages, which occur in pairs help a

host or a network manager get specific information from a router or another host. Error reporting one of the main responsibilities of ICMP is to report errors. IP is an unreliable protocol. This means that error checking and error control are not a concern of IP. ICMP was designed, in part to compensate for this short coming. However ICMP does not correct errors; it simply reports them. Error correction is left to the higher levels protocols. ICMP message are always sent to the original source because the only information available in the datagram about the route is the source and destination IP address. The ICMP uses the source IP address to send the error message to the source of the datagram.
Five types of Errors are handled:-

- Destination unreachable
- Source quench
- Time exceeded
- Parameter Problem
- Redirection

NO ICMP message will be generated

- In response to a datagram carrying an ICMP error message
- For a fragmented datagram that is not the first fragment
- For a datagram having a multicast address
- For a datagram having a special address such as 127.0.0.0 or 0.0.0.0

3.18.5.2 DESTINATION UNREACHABLE

When a router cannot route a datagram or a host cannot deliver a datagram, the datagram is discarded and the router or the host sends a destination unreachable message back to the source host that initiated the datagram.
The reason for discarding data grams:

1) The network is unreachable, possibly due to hardware failure. This type of message is generated by only router. The host is unreachable possibly due to hardware failure. This type of message can only be generated by a router.
2) The protocols is unreachable. For example if the destination host receives a datagram that must be delivered to the TCP protocol but the TCP protocol is not running at the moment, the error message is sent.
3) The port is unreachable. The application program that the datagram us destined for is not running at the moment.
4) Fragmentation is required but the DF (do not fragment) field of the datagram has been set. In other words, the sender of the datagram has specified that the datagram should not be fragmented but routing is impossible without fragmentation.
5) The destination network is unknown. The router has no information about the destination network. Note that even if a router does not report a destination unreachable message it does not mean that the datagram has been delivered. A router cannot detect all problems that prevent the delivery of packet.

3.18.5.3 SOURCE QUENCH

- The IP protocol is a connectionless protocol. There is no communication between the source host which produces the datagram, the router which forward it and the destination host which processes it. IP does not have flow control mechanism.
- The lack of flow problem can create a major problem in the operation of IP i.e. Congestion. The Source host never knows if the router or the destination host has been

overwhelmed with datagram. The source has never knows, if it producing datagram faster than they can be forwarded by routers or processed by the destination host.

- The lack flow control can create congestion I routers or the destination host. A router or a host has a limited buffer size for incoming datagram. If the datagram faster than they can be forwarded or processed, the buffer may overflow. In this case, the router or the host has no choice but to discard some of the datagram.
- The source quench message in ICMP has been designed to add a kind of flow control to the IP. When a route or a hoist discards a datagram due to congestion, it sends a source quench message to the sender of the datagram. This message has two purposes. First it informs the source that the datagram has been discarded. Second it warns the source that there is congestion somewhere in the path and that the source should slow down the sending process, unit the congestion is relieved.
- The router or destination host that has experienced the congestion should send one source – quench message for each discarded datagram to the source. There is no mechanism to tell the source that the congestion has been relived and the source can resume sending data grams at its previous rate. The source should continue to lower the rate until no more source quench messages are received.

3.18.5.4 TIME EXCEEDED

- Whenever a datagram is received, the router uses a routing table to find the next hop to which datagram should be sent. If there are errors in the routing tables, a packet can travel in a loop or a cycle going from one route to the next or visiting a series of routers endlessly. This problem is solved by time stamping each packet. Each datagram contains a filed called "time to live" in the header.
- Whenever datagram arrives at router, each route decrements contains the value of this field by 1. The route that receives a datagram with a value 0 in this field discards the datagram. When the datagram is discards a time exceeded message must be sent by the router to the source.

→ Whenever a route receives a datagram whose time – to live field has the value of Zero, it discards the datagram and sends a time exceeded message to the original Source.

→ When the final destination does not receive all of the fragments in a set time, it Discards the received fragments sends and sends a time exceeded message to the Original source.

3.18.6 PARAMETERS PROBLEM

If a route or the destination host discovers an ambiguous or missing value in any field of the datagram, it discards and sends a "parameters problem" message back to the source. A parameter problem message can be created by a router or the destination host.

3.18.7 REDIRECTION

When a route needs to sends a packet destined for another network, it must know the IP address of the next appropriate route. The same is true if the sender is a host. Both the route and the host then must have a routing table to find the addresses of the route or the next route. Routers take part in the routing update process and are updated periodically and dynamically, host do not take part in the routing update process because there are

many more hosts in an internet than routers. Hosts usually use static routing. The routing table of host has a limited number of entries. It usually contains the IP address of only one router, the default router, in the beginning. Because of this, the host may send a datagram which is destined for another networks so the wrong router (i.e. to the default router). In this case, the router that receives the datagram forwards the datagram to the correct router. However to update the routing table of the hoist it sends a redirection message to the host. A host usually starts with a small routing table that is gradually augmented and updated. One of the tools to accomplish this is the redirection message.
For example, as shown in the figure, Host A wants to send a datagram to the host B. Router R_2 is obviously the most efficient routing choice, but host sends datagram to R_1. R_1 after referring its table finds that the packet should have gone to R_2. It sends the packet to R_2 and at the same time sends time sends a redirection message to host A. Host A's routing table can now be updated.

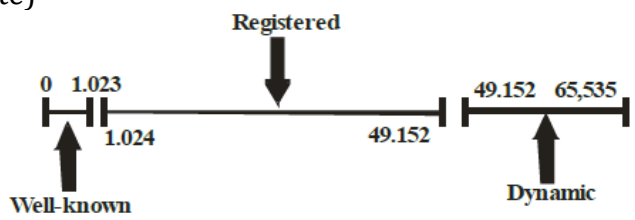
3.18.8 UDP

UDP is connectionless, unreliable transport protocol. It does not add anything to the service of IP expect for providing process to process communication instead of host – to – host communication. Process to process communication The IP is responsible for host to host communication. As a network layer protocol, IP can deliver the message only to the network layer of the destination computer. However this is an incomplete delivery. The message still needs to be handed to the correct process. This is where a transport layer protocol such as UDP takes over. UDP is responsible for delivery of message to the appropriate process.

3.18.9 PORT UMBERS

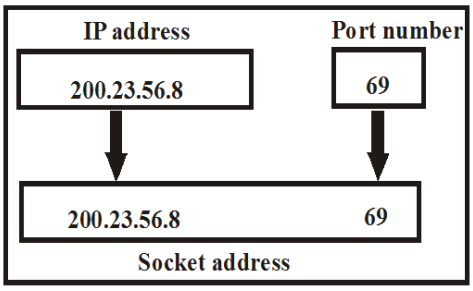
A process running in local host is called client and a process running on the remote host is called server. Both process (client and server) have the same time. However, operating system today support both multiuser and multiprogramming environment. A remote computer can run several server programs at the same time. For communication we define: Local host, Local process, Remote host, and Remote process. The local host and the remote host are defined using IP addresses. To define local processes and remote processes we need second identification which is called port addresses or port number. In the TCP / IP protocol suite, the port number is integers between 0 and 65, 535. The client program defines itself with a port number randomly selected by UDP software running on client host. This is the ephemeral port number. The server process must also be defined with port number. TCP / IP uses universal port numbers for servers; these are called well known port number. The port numbers are numbers are divided into three ranges.

- Well known
- Registered
- Dynamic (or private)



3.18.10 SOCKET ADDRESS

TCP / IP needs two identifiers: IP addressed and port address at each end to make connection. The combination of IP address and port is called socket address.
The client socket address and server socket address define the processes uniquely. To use the services of UDP, we need a pair of socket addresses: the client socket address and the sever socket address. These are part of IP header and UDP header. The IP header contains the IP address, the UDP header contain the port address.



3.18.11 USER DATAGRAM

UDP packet also user datagram have a fixed size header of eight bytes.
Header

1) Source port number
This is the port number used by processing running on the source host. It is 16 bits long which means that the port number can range from 0 to 65535.

Source port number 16 bits	Destination port number 16 bits
Total length 16 bits	Checksum 16 bits

If the source host is client (a client sending request), the port number is an ephemeral port number chosen by UDP software running on the source host. If the source host is server (a server sending a response), the port number is a well – known port number.

2) Destination port number
This is the port number used by processing running on the destination host. It is also 16 bits long. If the destination host is a server the port number is well – known port number. If the destination host is a client the port number is an ephemeral port number. In this case the server copies the ephemeral port number it has received in the request packet.

3) Length
This 16 bit field defines the total length of the user datagram header. It can define a total length of 0 to 656535 bytes.

4) Checksum

This field is used to detect errors over the entire user datagram; header plus data.

3.19 LMR (LAST MINUTE REVISION)

- Internetworking devices connect networks to create an internet.
- Networking and internetworking devices are divided into four categories: repeaters, bridges, routers, and gateways.
- A repeater is a device that operates in the physical layer of the OSI model. Its purpose is regenerators of the signal.
- Routers operate in the physical, data link and network layers of the OSI model. They decide the can therefore connect two dissimilar networks.
- Gateways operate in all seven layers of the OSI model. They convert one protocol to another and can therefore connect two dissimilar networks.
- There are two methods to calculate the shortest path between two routers: distance vector routing and link state routing.
- In distance vector methods to calculate the shortest path between two routers: distance vector routing and link state routing.
- In distance vector routing, each router has a table with information about the networks (ID, cost, and the router to access the particular network).
- In link state routing each router creates its own link state packet (LSP). Every other router receives this LSP through the flooding process. All routers thus have the same information; this is compiled into the link state database. Form this common database, each router finds its shortest paths to the other routers by using the Dijkstra algorithm.
- A cost is assigned to a packet when it leaves the router in link state routing.
- In link state routing, every router has its own unique routing table.
- Switching refers to temporary connection between physical links resulting in larger links for network transmission.
- Routing means selecting a best path for sending a packet from one point to another when more than one path is available.
- Traditionally, three methods of switching are used:
  (i) Circuit switching
  (ii)Packet switching
  (iii) Message switching.
- Communication via circuit switching involves 3 phase:
  (i) Circuit Establishment
  (ii) Data Transfer
  (iii) Circuit Disconnect.
- If there is only routing sequence defined for each source destination pair, the scheme is known as a fixed alternative routing scheme. More commonly a dynamic routing is used.
- In adaptive routing, a central controlled to find the best alternative route depending on the congestion in the network.
- There are two popular approaches to packet switching:
  (i) Datagram
  (ii) Virtual circuit.
- In the datagram approach, each packet is treated independently from all others. Packet in this technology is referred to as datagram.

- The network may provide services related to the virtual circuit including sequencing and error control.
- Sequence refers to the fact that because all packets follow the same route they arrive in the original order.
- Packets arrive more rapidly with virtual circuit, because it is not necessary to make routing decision for each packet at each node.
- Two types of network protocols:
  (i) Connection Oriented Network Service (CONS)
  (ii) Connection less Network Service (CLNS)
- A connection Oriented Network Service (CONS) establishes a virtual circuit for the transmission of data that is active for the entire transmission. All packets belonging to a single transmission are sent in order over the network.
- A route for packet between two stations is defined and labeled. All packets for that virtual circuit follow the same route and arrive in sequence. This forms internal virtual circuit.
- A conception oriented network service follows five general steps:
  (i) Sender transmits a connection– request packet
  (ii) Receiver acknowledgment with a connection confirm packet.
  (iii)Sender transmits data (This step can be repeated)
  (iv)Sender transmits a disconnect request packet
  (v)Receiver acknowledgement with a disconnect confirm packet.
- In a connectionless network service, each packet of a multi packet transmission is treated as an independent unit. Connectionless protocols provide no logical connection.
- Congestion control maintains the number of packets within the network below the level at which performance falls off dramatically.
- Input buffer accept arriving packets and output buffer hold packets that are waiting to depart. If packet arrive arriving too fast for the node to process then i.e. to make routing decision or faster than packets can be cleared form the outgoing buffers, packets will arrive for which no memory is available.
- Objective of congestive control technique: Limit queue at the nodes so as to avoid throughput collapse.
- A repeater (or regenerator) is an electronic device that operates on physical layer of the OSI model.
- Bridge is an intermediate system used to connect two LANS.
- A simple bridge links two segments and contains and contains a table that lists the addresses of all stations included in each of them.
- A learning bridge builds its table of station addresses on its own as it perform its bridge functions.
- A multiport bridge can be either simple or learning and is used to interconnect more than two same type segments.
- When two or more separate network are connected for exchanging data or resources, they become an inter network (or internet).
- Routers forward the packets among multiple interconnected networks. Routers acts like a station on a network. They receive packets from one connected network and pass them to a second connected network.
- A gateway is a protocol converter.
- IPv4 address length is 32 bits and IPv6 is 128 bits.
- IPv4 addresses are divided into five classes as class A, B, C, D and E.

- Class A range is 0 to 127, B is 128 to 191, C is 192 to 223, D is 223 to 239 and E is 240 to 255.
- The subnet mask for class A is 255.0.0.0, class B is 255.255.255.0 and class C is 255.255.255.192
- The notation w.x.y.z/n is known as class less Inter Domain routing addressing, where n represents mask bits.
- 0.0.0.0 and 255.255.255.255 are known as universal IP addresses.
- The IPv4 address 127.0.0.1 is called as Loop back IP address.
- The IPv6 loop back address is : : 1
- IPv6 addresses are 3 types as Uni cast, Multi cast and any cast.
- There is no Broadcast IPv6 address.

- The transport layer, by hiding all of the manipulations necessary to move a message from source to destination, makes data transmission transparent to the upper layers.
- The data link and transport layers perform many of the same duties. The Data link layer functions in a single network, while the transport layer operates across an internet.
- The transport layer needs ports or service access points.
- Reliable delivery requires error control, sequence control, loss control, and duplication control.
- Flow control at the transport level is handled by a three – walled sliding window.
- Multiplexing can be downward or upward in the transport layer.
- Connection establishes and termination is both accomplished through three way handshakes.
- The transport layer is responsible for end – to – end delivery, segmentation and concatenation.
- The transport layer supports two services types:
  a) Connection – oriented transport service (COTS)
  b) Connectionless transport service (CLTS).
- The transport protocols data unit (TPDU) format consists of four fields:
  a) Length
  b) Fixed parameters
  c) Variable parameters
  d) Data
- The five types of transport classes are based on the reliability of the lower layers. Class TP4 is similar to TCP in the TCP / IP suite.
- The service provided by transport layer protocols can be divided into 5 broad categories.
  i) end to end delivery
  ii) addressing
  iii) reliable delivery
  iv) flow control and
  v) Multiplexing

- Aspects of reliable delivery: Error control, Sequence control, Loss control and Duplication control.
- When the size of the data unit received from the upper layer is too long for the network layer datagram packet of data link layer frame to handle, the transport layer protocol divides it into smaller usable blocks. This dividing processing is called segmentation.

- When on the other hand, the size of the data units belonging to a single session are so small that several can fit together into a single packet or frame, the transport layer combines then into a single data unit. The combining process is called concatenation.
- Multiplexing at this layer occurs two ways:
  i) Upward: Many transport layers use the same network connection.
  ii) Downward: One transport layer uses many network connections.
- End to end delivery can be accomplished in two modes:
  i) Connection oriented
  ii) connectionless
- Connection oriented transmission has three stages:
  i) Connection Establishment
  ii) Data transfer
  iii) Connection Termination
- At the network layer, TCP / IP support the Internet Protocol (IP). IP contains four supporting protocols: ARP, RARP, ICMP and IGMP.
- The transport layer in TCP / IP is represented by two protocols: TCP and UDP.
  TCP and UDP are responsible for delivery of a message from source application to destination application.
- Three different levels of addresses used in an internet using the TCP / IP protocols.
  i) Physical address
  ii) Internet address
  iii) Port address
- IP addresses are divided into five different classes: A, B, C, D and E. These are assigned to cover the needs of different types of organization.
- In supporting a network is divided into several smaller subnetwork (or subnet) having own sub network address.
- In super netting, an organization can combine several class C addresses to create a large range of addresses. In other words several networks are combined to create super network.
- IP address is now divided into three levels: net id, subnet id and host id.
  (i) Net id defines site i.e. network.
  (ii) Sub net id defines the physical sub network.
  (iii) Host id defines the connection of the host to the sub network.
- The delivery of packet to its final destination is accomplishes using two different methods of delivery.
  (i) Direct and **(ii)** Indirect.
- A static table is one that is not changed frequently. A dynamic table on the other hand is updated automatically when there is a change somewhere in the internet.
- Definition of AS (Autonomous System)
- Routing inside a AS is called as interior routing. Routing between autonomous systems is referred to as exterior routing.
- ICMP is an error reporting protocol.
- The error reporting messages report problem that a router or a host (destination) may encounter when it processes an IP packet.
- The query messages, which occur in pairs help a host or a network manager get specific information from a router or another host.
- Five types of Error are handled:-
  i) Destination unreachable

ii) Source quench
iii) Time exceeded
iv) Parameter problem
v) Redirection

- No ICMP message will be generated
  i) In response to a datagram carrying an ICMP error message
  ii) For a fragmented datagram that is not the first fragment.
  iii) For a datagram having a multicast address.
  iv) For a datagram having a special such as 127.0.0.0 or 0.0.0.0
- Routers take part in the routing table update process and are periodically dynamically, hosts do not take part in the routing update process because there are many more hosts in an internet than routers. The host usually uses static routing.
- A host usually starts with a small routing table that is gradually augmented and updated. One of the tools to accomplish this is the redirection message.
- UPD is a connectionless, unreliable transport protocol. It does not add anything to the services of IP expect for providing process communication.
- UDP is responsible for delivery of message to the appropriate process.
- A process running on local host is called client and a process running on the remote host is called server.
  The combination of IP addresses and port address is called socket address

GATE QUESTIONS

Q.1 The subnet mask for a particular network is 255.255.31.0. Which of the following pairs of IP addresses could belong to this network?
a) 172.57.88.62 and 172.56.87.233
b) 10.35.28.2 and 10.35.29.4
c) 191.203.31.87 and 191.234.31.88
d) 128.8.129.43 and 128.8.161.55
[GATE-2003]

Q.2 Which of the following functionalities must be implemented by a transport? Protocol over and above the network protocol?
a) Recovery from packet losses
b) Detection of duplicate packets
c) Packet delivery in the correct order
d) End to end connectivity
[GATE-2003]

Q.3 Which of the following assertions is false about the Internet Protocol (IP)?
a) It is possible for a computer to have multiple IP addresses
b) IP packets from the same source to the same destination can take different routes in the network
c) IP ensures that a packet is discarded, if it is unable to reach its destination within a given number of hops
d) The packet source cannot set the route of an outgoing packets; the route is determined only by the routing tables in the routers on the way
[GATE-2003]

Q.4 The routing table of a router is shown below

Destination	Subnet mask	Interface
128.75.43.0	255.255.255.0	Eth0
128.75.43.0	255.255.255.128	Eth1
192.12.17.0	255.255.255.255	Eth2
Default		Eth3

On which interface will the router forward packets addressed to destinations 128.75.43.16 and 192.12.17.10 respectively?
a) Eth1 and Eth2 b) Eth0 and Eth2
c) Eth0 and Eth3 d) Eth1 and Eth3
[GATE-2004]

Q.5 Which of the following is NOT true with respect to a transparent bridge and a router?
a) Both bridge and router selectively forward data packets
b) A bridge uses IP addresses while a router uses MAC addresses
c) A bridge builds up its routing table by inspecting incoming packets
d) A router can connect between a LAN and a WAN
[GATE-2004]

Q.6 Which one of the following statements is FALSE?
a) TCP guarantees a minimum communication rate
b) TCP ensures in-order delivery
c) TCP reacts to congestion by reducing sender window size
d) TCP employs retransmission to compensate for packet loss
[GATE-2004]

Q.7 A subnet has been assigned a subnet mask of 255.255.255.192. What is the maximum number of hosts that can belong to this subnet?
a) 14 b) 30
c) 62 d) 126
[GATE-2004]

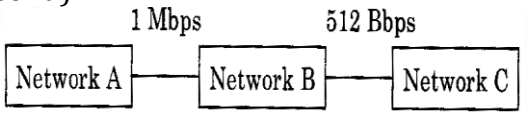
Q.8 In TCP, a unique sequence number assigned to each
a) byte b) word
c) segment d) message
[GATE-2004]

Q.9 In the TCP/IP protocol suite, which one of the following is NOT part of the IP header?
a) Fragment offset
b) Source IP address
c) Destination IP address
d) Destination port number
[GATE-2004]

Q.10 A TCP message consisting of 2100 bytes is passed to IP for delivery across two networks. The first network can carry a maximum payload of 1200 bytes per frame and the second network can carry a maximum payload of 400 bytes per frame excluding network overhead. Assume that IP overhead per packet is 20 bytes. What is the total IP overhead in the second network for this transmission?
a) 40 bytes b) 80 bytes
c) 120 bytes d) 160 bytes
[GATE-2004]

Q.11 Suppose that the maximum transmit window size for a TCP connection is 12000 bytes. Each packets consist of 2000 bytes. At some point of time, the connection is in slow-start phase with a current transmit window of 4000 bytes. Subsequently, the transmitter receives two acknowledgement. Assume that no packets are lost and there are no time-outs. What is the maximum possible value of the current transmit window?
a) 4000 bytes b) 8000 bytes
c) 10000 bytes d)12000 bytes
[GATE-2004]

Common Data Questions Q.12 and Q.13
Consider three IP networks A, B and C. Host H_A in network A sends messages each containing 180 bytes of application data to a host H_C in network C. The TCP layer prefixes a 20 bytes header to the message. This passes through an intermediate network B. The maximum packet size, including 20 bytes IP header, in each network is
A:1000 bytes, B:100 bytes, C:1000 bytes
The network A and B are connected through a 1 Mbps link, while B and C are connected by a 512 Kbps link (bps=bits per second).



Q.12 Assuming that the packets are correctly delivered, how many bytes, including headers, are delivered to the IP layer at the destination for one application message, in the best case? Consider only data packets.
a) 200 b) 220
c) 240 d) 260
[GATE-2004]

Q.13 What is the rate at which application data is transferred to host H_C? Ignore errors, acknowledgements, and other overheads.
a) 325.5 Kbps b) 354.5 Kbps
c) 409.6 Kbps d) 512.0 Kbps
[GATE-2004]

Q.14 In a packet switching network, packets are routed from source to destination along a single path having two intermediate nodes. If the message size is 24 bytes and each packet contains a header of 3 bytes, then the optimum packets size is
a) 4 b) 6
c) 7 d) 9
[GATE-2005]

Q.15 On a TCP connection, current congestion window size is congestion Window=4KB. The window size advertised by the receiver is advertise Window=6 KB. The last byte sent by the sender is Last Byte Sent= 10240 and the last byte acknowledged by the receiver is last byte Acked = 8192.

The current window size at the sender is

a)2048 bytes b) 4096 bytes
c) 6144 bytes d) 8192 bytes

[GATE-2005]

Q.16 In a communication network, a packet of length L bits takes link L1 with a probability of p_1 or link L2 with a probability of p_2. Link L1 and L2 have bit error probability of b_1 and b_2 respectively. The probability that the packet will be a received without error via either L1 or L2 is

a) $(1-b_1)^L p_1 + (1-b_2)^L p_2$
b) $(1- (b_1+ b_2)^L]p_1p_2$
c) $(1-b_1)^L (1-b_2)^L p_1p_2$
d) $1-(b_1^L p_1+b_2^L p_2)$

[GATE-2005]

Q.17 A company has a class C network address of 204.204.204.0. Ti wishes to have three subnets, one with 100 hosts and two with 50 hosts each. Which one of the following options represent a feasible set of subnet address /subnet mask pairs?

a) 204.204.204.128/255.255.255.128
204.204.204.0/255.255.255.128
204.204.204.64/255.255.255.128
b) 204.204.204.0/255.255.255.192
204.204.204.192/255.255.255.128
204.204.204.64/255.255.255.128
c) 204.204.204.128/255.255.255.128
204.204.204.192/255.255.255.192
204.204.204.224/255.255.255.192
d) 204.204.204.128/255.255.255.128
204.204.204.64/255.255.255.192
204.204.204.0/255.255.255.192

[GATE-2005]

Q.18 An organization has a class-B network and wishes to form subnets for 64 departments. The subnet mask would be

a) 255.255.0.0 b) 255.255.64.0
c) 255.255.1.28.0 d)255.255.252.0

[GATE-2005]

Q.19 The Address Resolution Protocol (ARP) is used for

a) finding the IP address from the DNS
b) finding the IP address of the default gateway
c) finding the IP address that corresponds to a MAC address
d) finding the MAC address that corresponds to an IP address

[GATE-2005]

Q.20 Packets of the same session may be routed through different paths in

a) TCP but not UDP
b) TCP and UDP
c) UDP but not TCP
d) Neither TCP nor UDP

[GATE-2005]

Q.21 Which of the following statements is True?

a) Both Ethernet frame and IP packet include checksum fields
b) Ethernet frame includes a checksum field and IP packets includes a CRC field
c) Ethernet frame includes a CRC field and IP packets includes a checksum field
d) Both Ethernet frame and IP packet include CRC fields

[GATE-2006]

Q.22 A router uses the following routing table:

Destination	Mask	Interface
144.16.0.0	255.255.0.0	Eth0
144.16.64.0	255.255.224.0	Eth1
144.16.68.0	255.255.255.0	Eth2
144.16.68.64	255.255.255.244	Eth3

A packet bearing a destination address 144.16.68.117 arrives at the router. On which interface will it be forwarded?

a) eth0 b) eth1
c) eth2 d) eth3

[GATE-2006]

Q.23 Suppose that it takes 1 unit of time to transmit a packet (of fixed size) on a communication link. The link layer uses a window flow control

protocol with a window size of N packets. Each packets causes an ack or a nak to be generated by the receiver , and ack/nak transmission times times are negligible. Further, the round trip time on the kink is equal to N units. Consider time time i>N. If only acks have been received till time i(no naks), then the goodput evaluated at the transmitter at time i(in packets per unit time)is

a) 1-N/i b) i/(N+i)
c) 1 d) $1-e^{(i/N)}$

[GATE-2006]

Q.24 A link of capacity 100 Mbps is carrying traffic from a number of sources. Each sources generates an on-off traffic stream; when the source is on the rate of traffic is 10 Mbps, and when the source is off, the rate of traffic is zero. The duty cycle which is the ratio of on-time to off-time is 1:2. When there is no buffer at the link, the minimum number of sources that can be multiplexed on the link so that link capacity is not wasted and no data loss occurs is S_1. Assuming that all sources are synchronized and that the link is provided with a large buffer, the maximum number of sources that can be multiplexed so that no data loss occurs is S_2. The value of S_1 and S_2 are, respectively.

a) 10 and 30 b) 12 and 25
c) 5 and 33 d) 15 and 22

[GATE-2006]

Q.25 A program on machine X attempts to open a UDP connection to port 5376 on a machine Y, and a TCP connection to port 8632 on machine Z.
However, there are no applications listening at the corresponding ports on y and Z. An ICMP Port Unreachable error will be generated by

a) Y but not Z b) Z but not Y
c) Neither Y nor Z d) Both Y and Z

[GATE-2006]

Q.26 A subnetted Class B network has the following broadcast address: 144.16.95.255. Its subnet mask

a) is necessarily 255.255.224.0
b) is necessarily 255.255.240.0
c) is necessarily 255.255.248.0
d) could be any one of 255.255.224.0, 255.255.240.0, 255.255.248.0

[GATE-2006]

Q.27 For which one of the following reasons does Internet Protocol (IP) use the Time To Live (TTL) field in the IP datagram header?

a) Ensure packets reach destination within that time
b) Discard packets that reach later than that time
c) Prevent packets from looping indefinitely
d) Limit the time for which a packet gets queued in intermediate routers

[GATE-2006]

Q.28 Two computers C_1 and C_2 are configured as follows. C_1 has IP address 203.197.2.53 & netmask 255.255.128.0. C_2 has IP address 203.197.75.201 and netmask 255.255.192.0. Which one of the following statements is true?

a) C_1 and C_2 both assume they are on the same network
b) C_2 assumes C_1 is on same network, but C_1 assumes C_2 is on a different network
c) C_1 assumes C_2 is on same network, but C_2 assumes C_1 is on a different network
d) C_1 and C_2 both assume they are on different networks

[GATE-2006]

Q.29 Consider the following statements about the timeout value used in TCP.

i) The timeout value is set to the RTT (Round Trip Time) measured

during TCP connection establishment for the entire duration of the connection.

ii) Appropriate RTT estimation algorithm is used to set the timeout value of a TCP connection.

iii) Timeout value is set to twice the propagation delay from the sender to the receiver.

Which of the following choices hold?

a) (i) is false, but (ii) and (iii) are true
b) (i) and (iii) are false, but (ii) is true
c) (i) and (ii) are false, but (iii) is true
d) (i), (ii) and (iii) are false

[GATE-2007]

Q.30 Consider a TCP connection in a state where there are no outstanding ACKs. The sender sends two segments back to back. The sequence numbers of the first and second segment are 230 and 290 respectively. The first segment was lost, but the second segment was received correctly by the receiver. Let X be the amount of data carried in the first segment (in bytes), and Y be the ACK number sent by the receiver. The values of X and Y (in that order) are

a) 60 and 290 b) 230 and 291
c) 60 and 231 d) 60 and 230

[GATE-2007]

Q.31 The address of a class B host is to be split into subnets with a 6-bit subnet number. What is the maximum number of subnets and the maximum number of hosts in each subnet?

a) 62 subnets and 262142 hosts
b) 64 subnets and 262142 hosts
c) 62 subnets and 1022 hosts
d) 64 subnets and 1024 hosts

[GATE-2007]

Q.32 Which of the following statements are True?

S1: TCP handles both congestion and flow control

S2: UDP handles congestion but not flow control

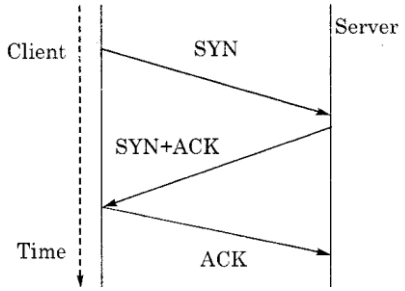
S3: Fast retransmit deals with congestion but not flow control

S4: Slow start mechanism deals with both congestion and flow control

a) S1, S2 and S3 only
b) S1 and S3 only
c) S3 and S4 only
d) S1, S3 and S4 only

[GATE-2008]

Q.33 The three way handshake for TCP connection establishment is shown below.



Which of the following statements are TRUE?

S1: Loss of SYN+ACK from the server will not establish a connection

S2: Loss of ACK from the client cannot establish the connection

S3: The server moves LISTEN→SYN_RCVD→SYN_SENT →ESTABLISHED in the state machine on no packet loss

S4: The server moves LISTEN→SYN_RCVD→ESTABLISHED in the state machine on no packet loss

a) S2 and S3 only b) S1 and S4 only
c) S1 and S3 only d) S2 and S4 only

[GATE-2008]

Direction for Question 34 to 35:

Host X has IP address 192.168.1.97 and is connected through two routers R1 and R2 to another host Y with IP address 192.168.1.80. Router R1 has IP addresses 192.168.1.135 and 192.168.1.110. R2 has IP addresses 192.168.1.67 and 192.168.1.55. The net mask used in the network is 255.255.255.224.

Q.34 Given the information above, how many distinct subnets are guaranteed to ready exist in the network?
a) 1 b) 2
c) 3 d) 6
[GATE-2008]

Q.35 Which IP address should X configure its gateway as?
a) 192.168.1.67 b) 192.168.1.110
c)192.168.1.135 d) 192.168.1.55
[GATE-2008]

Q.36 Which of the following system calls results in the sending of SYN packets?
a) Socket b) Bind
c) Listen d) Connect
[GATE-2008]

Q.37 What is the maximum size of data that the application layer can pass on to the TCP layer below?
a) Any size
b) 2^{16} byte size of TCP header
c) 2^{16} byte
d) 1500 byte
[GATE-2008]

Q.38 A client process P needs to make a TCP connection to a server process S. Consider the following situation. The server process S executes a socket ( ), a bind ( ) and a listen ( ) system call in that order, following which it is pre-empted. Subsequently, the client process P executes a socket ( ) system call followed by connect ( ) system call to connect to the server process S. The server process has not executed any accept ( ) system call. Which one of the following events could take place?
a) Connect ( ) system call returns successfully
b) Connect ( ) system call blocks
c) Connect ( ) system call returns an error
d) Connect ( ) system call results in a core dump
[GATE-2008]

Q.39 If a class B network on the Internet has a subnet mask of 255.255.248.0, what is the maximum number of hosts per subnet?
a) 1022 b) 1023
c) 2046 d) 2047
[GATE-2008]

Q.40 In the slow start phase of the TCP congestion control algorithm, the size of the congestion window
a) does not increase
b) increases linearly
c) increases quadratic ally
d) increases exponentially
[GATE-2008]

Q.41 While opening a TCP connection, the initial sequence number is to be derived using a time-of-day (ToD) clock that keeps running even when the host is down. The low order 32 bits of the counter of the ToD clock is to be used for the initial sequence numbers. The clock counter increments once per millisecond. The maximum packet lifetime is given to be 64s. Which one of the choices given below is closest to the minimum permissible rate at which sequence numbers used for packets of a connection can increase?
a) 0.015/s b) 0.064/s
c) 0.135/s d) 0.327/s
[GATE-2009]

Q.42 One of the header fields in an IP datagram is the Time To Live (TTL) field. Which of the following statements best explains the need for this field?
a) It can be used to prioritize packets
b) It can be used to reduce delays
c) It can be used to optimize throughput
d) It can be used to prevent packet looping

[GATE-2010]

Q.43 Suppose computers A and B have IP addresses 10.105.1.113 and 10.105.1.91 respectively and they both use the same net mask N. Which of the values of N given below should not be used, if A and B should belong to the same network?
a) 255.255.255.0
b) 255.255.255.128
c) 255.255.255.192
d) 255.255.255.224

[GATE-2010]

Q.44 A layer-4 firewall (a device that can look at all protocol headers up to the transport layer) CANNOT
a) block entire HTTP traffic during 9:00 pm and 5:00am
b) block all ICMP traffic
c) stop incoming traffic from a specific IP address but allow outgoing traffic to the same IP address
d) block TCP traffic from a specific user on a multi-user system during 9:00 pm and 5:00 am

[GATE-2011]

Q.45 Which of the following transport layer protocols is used to support electronic mail?
a) SMTP b) IP
c) TCP d) UDP

[GATE-2012]

Q.46 An Internet Service Provider (ISP) has the following chunk of CIDR-based IP addresses available with it; 245.248. 128.0/20. The ISP wants to give half of this chunk of addresses to organization A and a quarter to organization B, while retaining the remaining with itself. Which of the following is a valid allocation of addresses to A and B?
a) 245.248.136.0/21 & 245.248.128.0/022
b) 245.248.128.0/21 & 245.248.128.0/22
c) 245.248.132.0/22 & 245.248.132.0/21
d) 245.248.136.0/24 & 245.248.132.0/21

[GATE-2012]

Q.47 Consider an instance of TCP's Additive Increase Multiplicative Decrease (AIMD) algorithm where the Window size at the start of the slow phase is 2 MSS and the threshold at the start of the first transmission is 8 MSS. Assume that a timeout occurs during the fifth transmission. Find the congestion Window size at the end of the tenth transmission.
a) 8 MSS b) 14 MSS
c) 7 MSS d) 12 MASS

[GATE-2012]

Q.48 In the IPv4 addressing format, the number of networks allowed under Class C addresses is
a) 2^{14} b) 2^{7}
c) 2^{21} d) 2^{24}

[GATE-2012]

Q.49 In an IPv4 datagram, the M bit is 0, the value of HLEN is 10, the value of total length is 400 and the fragment offset value is 300. The position of the datagram, the sequence numbers of the first and the last bytes of the payload, respectively are
a) Last fragment, 2400 and 2789
b) First fragment, 2400 and 2759
c) Last fragment, 2400 and 2759
d) Middle fragment. 300 and 689

[GATE-2013]

Q.50 Let the size of congestion window of a TCP connection be 32 KB when a timeout occurs. The round trip time of the connection is 100 msec and the maximum segment size used is 2 KB. The time taken (in msec) by the

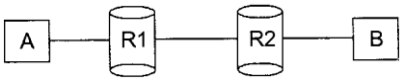
TCP connection to get back to 32 KB congestion window is _____.

[GATE-2014]

Q.51 Consider a selective repeat sliding window protocol that uses a frame size of 1 KB to send data on a 1.5 Mbps link with a one way latency of 50 msec. To achieve a link utilization of 60%, the minimum number of bits required to represent the sequence number field is _____.

[GATE-2014]

Q.52 Consider the store and forward packet switched network given below. Assume that the bandwidth of each link is 10^6 bytes/sec. A user on host A sends a file of size 10^3 bytes to host B through router R1 and R2 in three different ways. In the first case a single packet containing the complete file is transmitted from A to B. In the second case, the file is split into 10 equal parts, and these packets are transmitted from A to B. In the third case, the file is split into 20 equal parts and these packets are sent from A to B. Each packets contains 100 bytes of header information along with the user data. Consider only transmission time and ignore processing, queuing and propagation delays. Also assume that there are no errors during transmission. Let T1, T2 and T3 be the times taken to transmit the file in the first, second and third cse respectively. Which one of the following is CORRECT?



a) T1<T2<T3 b) T1>T2>T3
c) T2=T3, T3<T1 d)T1=T3, T3>T2

[GATE-2014]

Q.53 An IP router implementing Classless Interdomain Routing (CIDR) receives a packet with address 131.23.151.76. The routers routing table has the following entries:

Prefix	Output Interface Identifier
131.16.0.0/12	3
131.28.0.0/14	5
131.19.0.0/16	2
131.22.0.0/15	1

The identifier of the output interface on which this packet will be forwarded is _____.

[GATE-2014(3)]

Q.54 Host A (on TCP/IP v4 network A) sends an IP datagram to host B (also on TCP/ IP v4 network B). Assume that no error occurred during the transmission of D. When D reaches B,which of the following IP header field(s) may be different from that of original datagram D?

TTL
Checksum
Fragment Offset

a) I only b) I and II only
c) II and III only d) I, II, and III

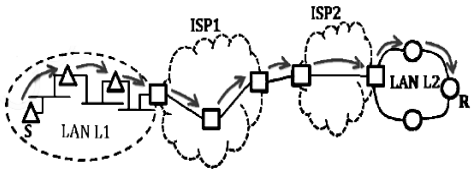
[GATE- 2014]

Q.55 An IP router with a Maximum Transmission Unit [MTU] of 1500 bytes has received an IP packet of size 4404 bytes with an IP header of length 20 bytes. The values of the relevant fileds in the header of the third IP fragment generated by the router for this packet are

MF bit:0, Datagram Length: 1444, Offset: 370
MF bit:1, Datagram Length: 1424, Offset: 185
MF bit:1, Datagram Length: 1500, Offset: 370
MF bit:0, Datagram Length: 1424, Offset: 2960

[GATE-2014]

Q.56 In the diagram shown below, L1 is an Ethernet LAN and L2 is a Token-Ring LAN. An IP packet originates from sender S and traverses to R, as shown. The links within each ISP and across the two ISP's, are all point-to-point optical links. The initial value of the TTL field is 32. The maximum size possible value of the TTL field when R receives the datagram is __



[GATE-2014]

Q.57 Every host in an IPV4 network has a 1-second resolution real-time clock with battery backup. Each host needs to generate up to 1000 unique identifiers per second. Assume that each host bas a globally unique IPv4 address. Design a 50-bit globally unique ID for this purpose. After what period (in seconds) will the identifiers generated by a host wrap around?

[GATE-2014]

Q.58 Which one of the following socket API functions converts an unconnected active TCP socket into a passive socket?

a) Connect b) Bind
c) Listen d) Accept

[GATE-2014]

Q.59 Consider the following routing table at an IP router:

Network No.	Net Mask	Next Hop
128.96.170.0	255.255.254.0	Interface 0
128.96.168.0	255.255.254.0	Interface 1
128.96.166.0	255.255.254.0	R2
128.96.164.0	255.255.252.0	R3
0.0.0.0	Default	R4

For each IP address in Group-I identify the correct choice of the next hop from Group-II using the entries from the routing table above.

LIST-I	**LIST-II**
A. 128.96.171.92	1. Interface 0
B. 128.96.167.151	1. Interface 1
C. 128.96.163.121	1. R2
D. 128.96.165.121	1. R4

Codes:

	A	**B**	**C**	**D**
a)	1	3	5	4
b)	1	4	2	5
c)	2	3	4	5
d)	2	3	5	4

[GATE-2015]

Q.60 Consider the following statements.

I. TCP connections are full duplex.
II. TCP has no option for selective acknowledgment
III. TCP connection are message streams.

a) Only I is correct
b) Only I and II are correct
c) Only II and III are correct
d) All of I, II and III are correct

[GATE-2015]

Q.61 In the network 200.10.11.144/27, the fouth octed (in decimal) of the last IP address of the network which can be assigned to a host is _____.

[GATE-2015]

Q.62 Which one of the following fields of an IP header is NOT modified by a typical IP router?

a) Checksum
b) Source address
c) Time to Live (TTL)
d) Length

[GATE-2015]

Q.63 Host A sends a UDP datagram containing 8880 bytes of user data to host B over an Ethernet LAN. Ethernet frames may carry data up to 1500 bytes (i.e. MTU = 1500 bytes). Size of UDP header is 8 bytes and size of IP header is 20 bytes.

There is no option field in IP header, how many total number of IP fragments will be transmitted and what will be the contents of offset field in the last fragment?

a) 6 and 925 b) 6 and 7400
c) 7 and 1110 d) 7 and 8880

[GATE-2015]

Q.64 Suppose two hosts use a TCP connection to transfer a large file. Which of the following statements is/are FALSE with respect to the TCP connection? If the sequence number of a segment is m, then the sequence number of the subsequent segment is always m+1. If the estimated round trip time at any given point of time is t sec, the value of the retransmission timeout is always set to greater than or equal to t sec. The size of the advertised window never changes during the course of the TCP connection. The number of unacknowledged bytes at the sender is always less than or equal to the advertised window

a) III only b) I and III only
c) I and IV only d) II and IV only

[GATE-2015]

Q.65 Identify the correct order in which a server process must invoke the function calls accept, bind, listen, and recv according to UNIX socket APL

a) listen, accept, bind recv
b) bind, listen, accept, recv
c) bind, accept, listen, recv
d) accept, listen, bind recv

[GATE-2015]

Q.66 Assume that the bandwidth for a TCP connection is 1048560 bits/sec. Let a be the value of RTT in milliseconds (rounded off to the nearest integer) after which the TCP window scale option is needed. Let b be the maximum possible window size the window scale option. Then the values of a and b are

a) 63 milliseconds, 65535×2^{14}
b) 63 milliseconds, 65535×2^{16}
c) 500 milliseconds, 65535×2^{14}
d) 500 milliseconds, 65535×2^{16}

[GATE-2015]

Q.67 An IP datagram of size 1000 bytes arrives at a router. The router has to forward this packet on a link whose MTU (maximum transmission unit) is 100 bytes. Assume that the size of the IP header is 20 bytes. The number of fragments that the IP datagram will be divided into for transmission is ___

[GATE-2016]

Q.68 For a host machine that uses the token bucket algorithm for congestion control, the token bucket has a capacity of 1 megabyte and the maximum output rate is 20 megabytes per second. Tokens arrive at a rate to sustain output at a rate of 10 megabytes per second. The token bucket is currently full and the machine needs to send 12 megabytes of data. The minimum time required to transmit the data is _____seconds.

[GATE-2016]

Q.69 Consider socket API on a Linux machine that supports connected UDP sockets. A connected UDP socket is a UDP socket on which connect function has already been called. Which of the following statement is/are CORRECT?

I. A connected UDP socket can be used to communicate with multiple peers simultaneously.
II. A process can successfully call **connect** function again for an already connected UDP socket.

a) I only b) II only
c) Both I and II d) Neither I nor II

[GATE-2017]

Q.70 Consider a TCP client and a TCP server running on two different machines. After completing data transfer, the TCP client calls **close** to terminate the connection and a FIN segment is sent o the TCP server. Server–side TCP responds by sending an ACK. Which is received by the client-side TCP. As per the TCP connection state diagram(RFC 793). In which sate does the client-side TCP connection wait for the FIN from the server-side TCP ?

a) LAST – ACK b) TIME – WAIT
c)FIN-WAIT d) FIN – WAIT -2

[GATE-2017]

Q.71 The maximum number of IPv4 router addresses that can be listed in the record route (RR) option field of an IPv4 header is _____.

[GATE–2017(2)]

Q.72 Match the following:

Field	Length in bits
P. UDP Header's Port Number	I. 48
Q. Ethernet MAC Address	II. 8
R. IPv6 Next Header	III. 32
S. TCP Header's Sequence no	IV. 16

a) P-III, Q-IV, R-II, S-I
b) P-II, Q-I, R-IV, S-III
c) P-IV, Q-I, R-II, S-III
d) P-IV, Q-I, R-III, S-II

[GATE-2018]

Q.73 Consider the following statements regarding the slow start phase of the TCP congestion control algorithm. Note that *cwnd* stands for the TCP congestion window and MSS denotes the Maximum Segment Size.

(i) The *cwnd* increases by 2 MSS on every successful acknowledgment.

(ii) The *cwnd* approximately doubles on every successful acknowledgement.

(iii) The *cwnd* increases by 1 MSS every round trip time.

(iv) The *cwnd* approximately doubles every round trip time.

Which one of the following is correct?

a) Only (ii) and (iii) are true
b) Only (i) and (iii) are true
c) Only (iv) is true
d) Only (i) and (iv) are true

[GATE-2018]

Q.74 Consider a long-lived TCP session with an end-to-end bandwidth of 1 Gbps (= 10^9 bits-per second). The session starts with a sequence number of 1234. The minimum time (in seconds, rounded to the closest integer) before this sequence number can be used again is _____.

[GATE-2018]

Q.75 Consider an IP packet with a length of 4,500 bytes that includes a 20-byte IPv4 header and a 40-byte TCP header. The packet is forwarded to an IPv4 router that supports a Maximum Transmission Unit (MTU) of 600 bytes. Assume that the length of the IP header in all the outgoing fragments of this packet is 20 bytes. Assume that the fragmentation offset value stored in the first fragment is 0. The fragmentation offset value stored in the third fragment is _____.

[GATE-2018]

ANSWER KEY:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
(d)	(d)	(d)	(c)	(b)	(a)	(c)	(d)	(d)	(c)	(b)	(d)	(b)	(d)	(b)
16	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**26**	**27**	**28**	**29**	**30**
(a)	(d)	(d)	(d)	(b)	(c)	(c)	(a)	(a)	(a)	(d)	(c)	(c)	(c)	(d)
31	**32**	**33**	**34**	**35**	**36**	**37**	**38**	**39**	**40**	**41**	**42**	**43**	**44**	**45**
(c)	(d)	(c)	(b)	(a)	(d)	(a)	(c)	(c)	(d)	(a)	(d)	(d)	(d)	(c)
46	**47**	**48**	**49**	**50**	**51**	**52**	**53**	**54**	**55**	**56**	**57**	**58**	**59**	**60**
(a)	(c)	(c)	(c)	1200	5	(d)		(d)	(a)	26	256	(c)	(a)	(a)
61	**62**	**63**	**64**	**65**	**66**	**67**	**68**	**69**	**70**	**71**	**72**	**73**	**74**	**75**
158	(b)	(c)	(b)	(b)	(c)	13	1.2	(b)	(d)	9	(c)	(c)	34 to 35	144

EXPLANATIONS

Q.1 **(d)**

The subnet mask is 255.255.31.0

The given subnet mask belongs to class B network because first tow octets are all ones which specify the physical network. The third octet also specify the local physical network connection and the fourth octet specify the host computer. The lowest address of class B network is 128.0.0.0 and the highest address is 191.255.0.0. so 191.203.31.87 and 191.234.31.88 belongs to class B network

Q.2 **(d)**

The transport layer of TCP/IP model is very similar to the transport layer of OSI model. The Transport layer is more commonly known as Host to Host protocol layer as it is responsible to setup and maintain (end to end communication) between two hosts. Hence, the transport protocols maintain the end to end connectivity.

Q.3 **(d)**

If source wants, it can set the route by using Options field in IPV4 header. The following are the various options in IPV4 header:-

1. **Record Route :** Used to record Router that a particular datagram visited to reach destination.
2. **Static Source Route :** Sender gives complete path. Datagram should not visit other routers not in the list
3. **Loose Source Route :** Sender gives complete path. Datagram can visit other routers not in the list.
4. **Time Stamp :** Used to record the time of datagram processing by a router. Then we can estimated the time it takes for datagram to go from one router to another.

A computer can have multiple IP addresses → TRUE, since it can have multiple LAN cards

Q.4 **(c)**

Boolean And (Destination Address, Mask) → Must give the Network ID

Given Destination Address = 128.75.43.16 = 128.75.43.00010000

Router always considers the Highest Mask first, then second highest, and so on…

First Highest Mask :-

Mask = 255.255.255.128

Boolean and (128.75.43.16, 255.255.255.2128) = 128.75.43.0→ Matched with Network Id corresponding to the given Mask, So obviously outgoing interface → "Eth1"

Given Destination Address = 192.12.17.10

First Highest Mask :-

Mask = 255.255.255.255

Boolean And (192.12.17.10, 255.255.255.0) =192.12.17.0 → Not Matched with Network ID and it won't match with other mask as well. So outgoing interface = Default → "Eth2"

Q.5 **(b)**

Choice b is not true.

A bridge operates at layer 2 (Data Link Layer) so it use MAC address while routes operates at layer 3 (Network Layer) so it uses IP addresses.

Q.6 **(a)**

Some of the services that TCP does not provide: it does not guarantee a

minimum transmission rate, a sending process is not permitted to transmit at any rate it wishes, the sending rate is regulated by TCP congestion control, or it may force the sender to send at a low average rate. Hence 1st statement is false. All other statements are true.

Q.7 (c)

Since you have 6 subnet bits so we can make (64-2)=62 hosts.

Q.8 (d)

TCP sequences each byte in the packet. Assigning a sequence number to indicate the first byte in a multi-byte packet does this. The second packet will have a sequence number equal to the first sequence number plus the number of bytes in the first packet.

Q.9 (d)

Destination port number is NOT present in IP header.

Because the IP header has nothing to do with the port number. Port number are used by the transport layer to ensure process to process delivery.

Q.10 (c)

In the question they have directly given the payload so 2100 will be divided into 1200 and 904 (900 is not a multiple of 8 so we have to pad 4 bits in order to make it a multiple of 8). Now in second network payload is 400 B.

So 1200 bytes packet will be divided in 400, 400, 400 with each having 20B header, and 900 will be divided into 400, 400 and 104 (4 bits padded) each having 20 B header.

So total overhead is 20*6=120 B

Q.11 (b)

In slow-start phase, for each ACK, the sender increase the current transmit window by Maximum Segment Size (MSS).

In the question it is given a packet consists of 2000 bytes and that can be taken as MSS.

So, after two ACKs, current transmit window = 4000+2000+2000=8000

Q.12 (d)

Network A sends a message of size 180 byte. Network B having the maximum packet size limit is 100 byte including 20 byte header. So the possible combination of sending packet from network A to C is

Header		Header		Header	
20	80	20	80	20	80

So the packet size

= 100+100+60=260 byte

Q.13 (b)

Apply Nyquist theorem

$C=2W\log_2 M$

for H_c=354.5 kbps

Q.14 (d)

Let S denote the source station and D denotes the destination station. X and y are two intermediate nodes between S and D.

Ṡ ẋ ẏ Ḋ

Message size=24bytes, Header (control information)=3 bytes consider the first choice (a).

Packet size = 4 then message size =4-3=1byte so it required 24 messages each containing 3 byte header so the transmission time for header overhead increases. Consider the second, third and fourth choices.

b) Packet size=6 then message size =6–3=3 bytes (required 8 packets)

c) Packet size=7 then message size =7–3=4 bytes (required 6 packets)

d) Packet size=9 then message size =9–3=6 bytes (required 4 packets)

So 4 packet is the optional message size & 9 is the optional packet size.

Q.15 (b)

Current window Size = Min (congestion window, advertised window).

Q.16 (a)

Required probability=Probability of selecting a link L1×(Probability of number of bit errors in L1)^L+ Probability of selecting a link L2× (Probability of number of bit errors in L2)^L

$= p_1(1-b_1)^L + p_2(1-b_2)^L$

Q.17 (d)

In class C network first three octet are reserved for net id, so we have total 8 bits for host and subnets. If we want to distribute addresses in subnets so first we should consider the subnet with maximum host, here which is subnet with 100 hosts. For 100 hosts we require 7 bits for host id, one bit remains for subnet, which we fix ti 1 for this subnet. Subnet mask for this subnet is 255.255.255.10000000=255.255.255.128 and subnet address is 204.204.204.128. For first subnet we have fixed 17th bit to 1 now for second and third subnet 17th bit will be 0. 50 host require 6 bit for host id, two bit remain for subnet id in which one bit is already fixed to zero.

We can configure 18th bit only for these subnets; for second subnet we fix 18th bit to 1 and for third subnet to 0.

Subnet mask for 2nd subnet and 3rd subnet is 255.255.255.11000000=255.255.255.192.

Subnet address for 2nd subnet is 204.204.204.64 and 3rd subnet is 204.204.204.0.

Q.18 (d)

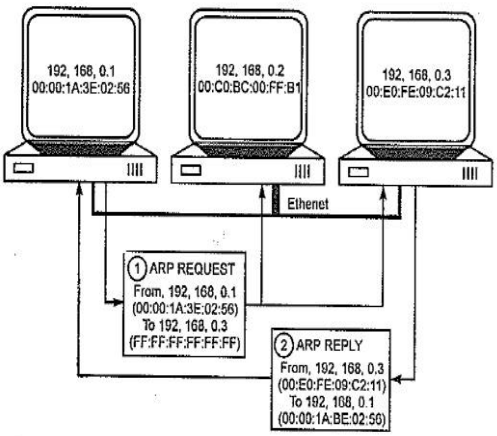
In class B network initial two octets are all 1's but the third octet specifies the physical network for subnet of 64 department or 2^6 so initial 6 bits of third octet are 1's.

11111111.11111111.11111100.00000000

255 . 255 . 252 . 0

Q.19 (d)

Address ReQution Protocol (ARP) is a computer networking protocol used by the Internet protocol (IP) for determining a network host's link layer or hardware address (MAC Address) when only its Internet Layer (IP) or network Layer address is known. The protocol operates as a part of the interface between the OSI network and OSI link layer below the network layer.



As discussed, the term address reQution refers to the process of finding an address of a computer in a network. In this process, a piece of information is sent by a client process executing on the local computer to a server process executing on a remote computer to reQve the address. The information which is received by the server enables it to uniquely identify the network system for which the address was required and hence, to provide the require address. The address reQution procedure is successfully completed when the client receives the required address as the response from the server.

Reverse of ARP is called Reverse Address ReQution Protocol (RARP).

Q.20 (b)

Connection oriented protocol These protocols require that a logical connection be established between two devices before transferring data which is generally accomplished by following a specific set of rules that specify, how a connection should be initiated, negotiated, managed and eventually terminated, e.g., TCP

Connectionless protocol A connectionless protocol is a data communication method in which no previous setup is needed for communication.

The device at one end transmits data to the other device present at other end of communication, irrespective of the fact that the recipient is available and ready to receive the data.

This question may confuse as TCP is connection oriented protocol while UDP is connectionless protocol. Both TCP and UDP protocols work in transport layer and the transport layer is only responsible for end to end communication (refer to OSI model Diag). It is the network layer that is responsible for the path determination.

Q.21 (c)

Ethernet uses cyclic Redundancy Check (CRC) algorithm to detect transmission errors. The Internet Protocol (IP) and mosthigher level protocols of the Internet Protocol Suite (ICMP, IGMP, UDP, UDO-Lite, TCP) use a common checksum algorithm to validate the integrity of the packets that they exchange.

Q.22 (c)

When a packet comes to a router, it matches destination network with those available in routing tables to route the packet.

The route which has longest network address match will be used to route the packet. The longest matching mask is 255.25.255.0 and hence forwarded to eth2.

Q.23 (a)

In computer networks, Goodput is application level throughput, is the number of useful information bits delivered by the network to a certain destination per unit of time. Successful delivery of packet can be assured if ACK has been received for it.

So till time 'i' we would have transmitted 'i' packets but only (i-N) can be acknowledged. Because minimum time for a packet to get Acknowledged is N. So, successfully delivered packets =(i-N)

Time for transmission = i

Goodput=Successfully delivered data/Time=(i-N)/i=1-N/i.

Q.24 (a)

Since there is no buffer, and constraint given, there should not be any data loss and no wastage of capacity as well.

Calculate for the extreme case when all sources are on time (that in transmitting).

10 Mbps * n_station=100 Mbps

n_station=10.

The link is provided with large buffer, so calculate expected value of bandwidth usage:

E=1/3*10+1/3*10+..n_station times

E≤100 Mbps

1/3*10* n_station ≤100 Mbps

Therefore n_station =30.

Q.25 (a)

TCP does not rely on ICMP for error control, but UDP does.

UDP does not have its own Error Control policies.

Q.26 (d)

In the broadcast address for a subnet, all the host bits are set to 1. So as long as all the bits to the right are 1, bits left to it can be taken as possible subnet.
Broadcast address for subnet is 95.255.01011111.11111111 (as in class B, 16 bit each are used for network and host).
So we can take minimum 3 bits (from left) as subnet and make rest as host bits (as they are 1).
.224.011100000.00000000
(leftmost 3 bits for subnet).
.240.011110000.00000000
(leftmost 4 bits for subnet).
.248.011111000.00000000 (….5bits for subnet).

Q.27 (c)
TTL field in IPV4 header →To prevent from packets looping indefinitely

Q.28 (c)
The two computer C_1 and C_2 are configured as following

	C_1	C_2
IPAdress and Network	203.197.2.53	203.197.75.201
	AND	AND
	255.255.128.0	255.255.192.0
	203.197.0.0	203.197.64.0
	Network Adreess	Network Adreess
	203.197.2.53 →	203.197.00000010.00111001
	255.255.192.0 →	255.255.11000000.00000000
	203.197.0.0	203.197.0.0
	203.197.75.201	
	255.255.128.0	
	203.192.0.0	

∴ C_1 assumes C_2 is on same network but C_2 assumes C_1 is one different network.

Q.29 (c)
i) is false because RTT is measured every time an ack is received, because propagation delay changes from time to time depending on the traffic.
ii) Time out value is set to twice the propagation delay from sender to the receiver.
iii) True for same reason.

Q.30 (d)
In TCP sequence number is assign to each data bytes.
Number of bytes in first segment is 290-230=60 bytes
In TCP ACK number send by receiver is next expected sequence number which is 230 here, 230 is first sequence number of first byte in first segment. First segment is lost and second received correctly , but receiver send ACK with sequence number of first byte of first segment until first segment received correctly.

Q.31 (c)
With a class B host. If it is to be split in a 6 bit subnet number (as given), Then,
It would have a 10 bit host number
To understand this ->
It is with a 16 bit host number that it is divided into 6 bit subnet number and 10 bit host number

So 16 bit host number is divided and we can calculate the following,
Maximum of subnets = $2^6 - 2 = 62$
Maximum number of host in each subnet = $2^{10} - 2 = 1022$

Q.32 (d)
S1 is true because TCP has its congestion control and flow control mechanisms.
UDP itself does not have any flow control or congestion control mechanism. Therefore S2 is false.
Fast retransmit and fast recovery are part of TCP congestion control algorithms. Therefore S3 is true.
In slow start algorithm we use congestion and advertised window

and these act as flow control windows.
The congestion windows flow control imposed by the sender while the advertised window is flow control imposed by receiver.
∴ S4 is True.

Q.33 (c)

Initially server is in LISTEN mode when a SYN is received, the server sends SYN+Ack and goes to SYN_RCVD state. Ehen ack from client is received it moves to ESTABLISHED state.
∴S3 is false and S4 is true.
The loss of SYN+Ack from server will not allow the client to move to ESTABLISHED state.
Hence connection cannot be established.

Q.34 (b)

By performing bitwise AND between given IP addresses and subnet mask such as

192.168. 1 .97	192.168. 1 .80
255.255.255.224	255.255.255.224
192.168. 1 .01100001	192.168. 1 .01010000
192.168. 1 .135	192.168. 1 .110
255.255.255.224	255.255.255.224
192.168. 1 .10000111	192.168. 1 .01101110
192.168. 1 .67	192.168. 1 .155
255.255.255.224	255.255.255.224
192.168. 1 .010000011	192.168. 1 .10011011

There are 3 distinct subnet present i.e., 011,010, 100.
So answer should be option (b).

Q.35 (a)

X with IP 192.168.1.97 and subnet mask 255.255.255.224 generate subnet ID to reach the gateway is 192.168.1.96.

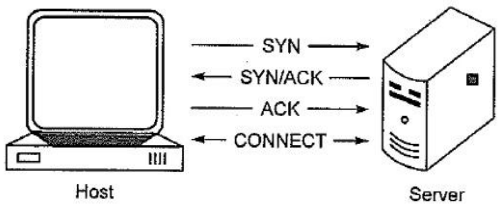
192.168. 1 .97
255.255.255.224
192.168. 1 .01100001

Now, the gateway must also have the same subnet number. We have to check subnet ID from both IP addresses of R1 router and the one which has same subnet ID to X will be its gateway ID.

192.168. 1 .135	192.168. 1 .110
255.255.255.224	255.255.255.224
192.168. 1 .10000111	192.168. 1 .01101110

So IP 192.168.1.110 of R1 router has same subnet ID. So it will be the gateway ID (we can simply check the three MSB of last octet).

Q.36 (d)



Host A sends a TCP synchronize packet to host B
HOST B receives A's SYN
HOST B sends a synchronize-acknowledgement
HOST A receives B's SYN-ACK
HOST A sends acknowledge
HOST B receives ACK. TCP connection is (Established). synchronize and acknowledge messages are indicated by a bit inside the TCP header of the segment. The handshake (TCP handshaking) between sender and receiver is established by connect so that SYN packets could be sent.
TCP knows whether the network connection is opening, synchronizing or established by using the synchronize and acknowledge message when establishing a network connection.
When the communication between two computers ends, another 3-way communication is performed to tear down the TCP connection. This setup and teardown of a TCP connection is part of what qualifies TCP a reliable protocol.

Q.37 (a)

Application layer can pass data of Any Size to Transport Layer. The Transport Layer can send data of any size in multiple segments. Segmentation & Reassembly is the responsibility of Transport Layer to send data of any size given by the application layer.

Q.38 (c)

In a TCP connection the process is
P……Flag →S
P……Sync →S
P<……ACK→S
P……Data Transfer →S
If any error occurs connect 0 system call returns an error.
The handshake (TCP Handshaking) between sender and receiver is established by connect() so that SYN packets could be sent. Now, to send these packets, server should execute accept() in return so that connect() gets an acknowledgement and a handshake could occur. Since, there is no Handshake, error occurs.

Q.39 (c)

Mask = 255.255.248.0
11111111.11111111.11111000.00000000
∴ No. of hosts per subnet=$2^{11}-2=2048-2=2046$

Q.40 (d)

To avoid congestion collapse, TCP uses a multi-faceted congestion control strategy. For each connection, TCP maintains a congestion window, limiting the total number of unacknowledged packets that may be in transit end-to-end. This is somewhat analogous to TCP's sliding window used for flow control TCP uses a mechanism called slow start to increase the congestion window after a connection is initialized and after a timeout. It starts with a window of two times the maximum segment size (MSS). Although the initial rate is low, the rate of increase is very rapid : for every packet unacknowledged, the congestion window increases by 1 MSS so that the congestion window effectively doubles for every round trip time (RTT). When the congestion window exceeds a threshold ss thresh the algorithm enters a new state, called congestion avoidance. In some implementations (e.g. Linux), the initial ss thresh is large, and so the first slow start usually ends after a loss. However, ss thresh is updated at the end of each slow start, and will often affect subsequent slow starts triggered by timeouts.

Congestion avoidance As long as non-duplicate ACKs are received, the congestion window is additively increased by one MSS every round trip time. When a packet is lost, the likelihood of duplicate ACKs being received is very high (it's possible though unlikely that the stream just underwent extreme packet reordering, which would also prompt duplicate ACKs). The behaviour of Tahoe and Reno differ in how they detect and. react to packet loss **Taho** Triple duplicate ACKS are treated the same as a timeout. Tahoe will then reduce congestion window to 1 MSS, and reset to slow-start state.

Reno If three duplicate ACKs are received (i.e., four, ACKs acknowledging the same packet, which are not piggy backed on data, and do not change the receiver's advertised window), Reno will have the congestion window, perform a fast retransmit, and enter a phase called Fast Recovery. If an ACK times out, slow start is used as it is with Tahoe.

Fast recovery (Reno Only) in this state, TCP retransmits, the missing packet that was signaled by three duplicate ACKs, and waits for an

acknowledgement of the entire transmit window before returning to congestion avoidance. If there is no acknowledgement, TCP Reno experiences a timeout and enters the slow-start state. Both algorithms reduce congestion window to 1 MSS on a timeout event.

Q.41 (a)

The maximum packet lifetime is given to be 64 seconds in the question. Thus, a sequence number increments after every 64 seconds. So, the minimum permissible rate= 1/64=0.015per sec.

Q.42 (d)

Time to live (TTL) is a limit on the period of time or transmissions in computer and computer network technology that a unit of data (e.g., a packet) can experience before it should be discarded. If the limit is not defined then the packets can go into an indefinite loop. The packet is discarded when the time to live field reaches 0 to prevent looping.

Q.43 (d)

First of all, let us know what is Net mask. A Netmask is a 32-bit mask used to divide an IP address into subnets and specify the networks available hosts. In a netmask, two bits are always automatically assigned. For example, in 255.255.225.0, 0 is the assigned network address; and in 255.255.255.255.255 is the assigned broadcast address. The 0 and 255 are always assigned and cannot be used. Here, in the problem, both IP Addresses are on same network. To find out the Qution, we have to try out for all four options available. Now, post mask operation, a same ID must come for the both. However it does not come as and when we use 255.255.255.224. Lets see it from the calculation below.

10.105.1.113	10.105. 1.91
255.255.255.224	255.255.255.224
10.105.1.106	10.105.1.64

Here, we can see that both the ID are different from each other.

Q.44 (d)

To block TCP traffic from specific user, requires information of specific user which is done by application layer. To block HTTP data, layer-4, i.e., transport layer can be used because it can block port used by HTTP.

Q.45 (c)

UDP and TCP are transport layer protocol. TCP supports electronic mail.

∴ option 'C' is correct.

Q.46 (a)

It has 20 bit mask, so total number of host are 2^{12}

It wants half of the chunk to A, therefore mask of A should be 21 bit, so it will contain 2^{11} hosts.

∴ Two choices for A

⇒ 245.248.1000 0000.0/21
245.248.1000 1000.0/21

∴ A can be assigned

⇒ 245.248.136.0/21
245.248.128.0/21

Now, one fourth needs to be assigned to B, Hence its mask should be 22 bits. But if we look at choice (b), the host in A and B are conflicting, therefore option (a) is correct.

Q.47 (c)

$$\left.\begin{array}{l}1st \rightarrow 2MSS\\ 2nd \rightarrow 4MSS\end{array}\right\}\text{Slow Start}$$

$$\left.\begin{array}{l}3rd \rightarrow 8MSS\\ 4th \rightarrow 9MSS\\ 5th \rightarrow 10MSS\end{array}\right\}\text{Additive increase}$$

$$\text{Time out} \Rightarrow \text{threshold} = \frac{1}{2}\times 8 = 4$$

$$\left.\begin{array}{l}6th \rightarrow 5MSS\end{array}\right\}\text{multiplicative decrease}$$

$7th \rightarrow 4MSS$

$8th \rightarrow 5MSS$

$9th \rightarrow 6MSS$

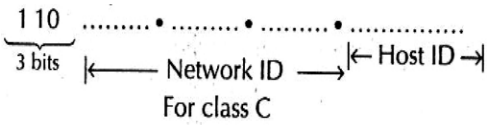
$10th \rightarrow 7MSS$

Q.48 (c)

In class C of IPV4 addressing

$$\left[\underbrace{8bit.8bit.8bit}_{\text{Networn ID}}.\underbrace{8bit}_{\text{Host ID}}\right]$$

So for network there are 24 bits But for class C addressing the first 3 bits are used for represent class C network.



We have 21 bits to generate network for class C. So total number of network in class C = 2^{11}

Q.49 (c)

Since M bit is 0 there would be ni fragment other than this fragment. Hence, this fragment is the "Last fragment". HLEN defines the length of the header in the datagram. The value of HELN is 10 size of the header is 10 * 4 = 40 B.

Length of data = total length – header length

= 400 – 40 = 360 B

The fragment offset of data in the original datagram is measured in units of 8 B. So, to find first byte of

This fragment $\frac{\text{first byte}}{B}$ =fragment offset.

First byte = 300 * 8 = 2400 B.

And hence the length of data is 360 b

So last byte on this datagram is 2759

i.e. 2400 and 2759

Hence, answer is (C) last fragment, 2400 and 2759.

Q.50 (1200 msec)

Congestion window =32 KB.

Threshold = 16 KB

2→4→8→16→18→20→22→24→26 →28→30→32

Time taken to reach 32 KB =12 segments×100 msec=1200 msec.

Q.51 $1RTT=2\times t_{prop}=2\times 50msec=100msec$

Bandwidth = 105×10^6 bps

1.5×10^6 bits→1sec

(1 packet) 1000 bytes→?

⇒ 1 packet transmitted in: $\frac{1000\times 8}{1.5\times 10^6}$ sec

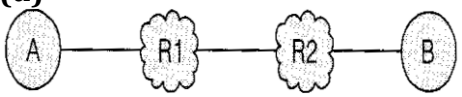
$\frac{1000\times 8}{1.5\times 10^6}$ sec →1 packet transmitted

100 msec→? Number of packets

⇒#packets= $\frac{100msec}{1000\times 8}\times 1.5\times 10^6 = 18.75$

∴ 5- bit are needed for sequence number [i.e., $\log_2 18.75=5$]

Q.52 (d)



Bandwidth : 10^6 bps

Packet size :1000 bytes

1st transmission : 1000+100=1100 bytes transmitted at a time from A

10^6 bits →1 sec

1100 bytes?

Transmission time at A = $1100\times 8/10^6$ = 8.8 msec.

From A, R1 and R2 it takes T1 = 8.8+8.8+8.8=26.4 msec to reach B

2nd transmission : 100+100=200 bytes transmitted 10 times from A

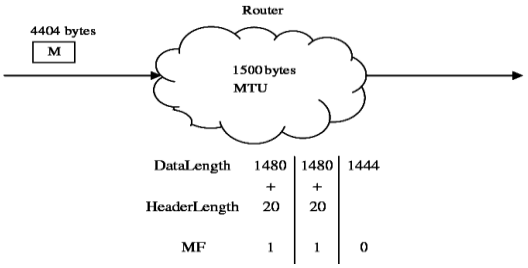
10^6 bits →1 sec

200 bytes?
Transmission time at A for 200 bytes = $200\times8/10^6$ = 1.6 msec.
From A, transmission time for entire packet = 1.6×10 = 16 msec
Note: It uses store and forward so when 10th packet is transmitted from A, B receives 8th packet.
From A, R1 and R2 it takes T2 = 16+1.6+1.6=19.2 msec to reach B
3rd transmission : 50+100=150 bytes transmitted 20 times from A
10^6 bits →1 sec
150 bytes?
Transmission time at A for 150 bytes= $150\times8/10^6$ = 1.2 msec.
From A transmission time for entire packet = 1.2 ×20 = 24 msec
Note: It uses store and forward so when 10th packet is transmitted from A, B receives 8th packet.
From A, R1 and R2 it takes T3 = 24 +1.2 +1.2 = 26.4 msec to reach B.
T1 = T3 = 26.4 msec
T2 = 19.2 msec, T2 < T3.

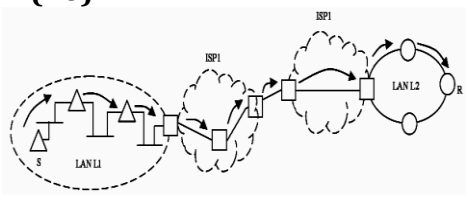
Q.53 131.23.151.76=10000011.000 10111.10010111.01001100
131.16.0.0/12=10000011.0001 0000.0000 0000
131.22.0.0/15=10000011.0001011 0.0000 0000. 0000 0000
Longest prefix match is : 131.22.0.0/15
∴ Interface 1 will be selected to forward the packet.

Q.54 **(d)**
While an IP Datagram is transferring from one host to another host, TTL, Checksum and Fragmentation Offset will be changed

Q.55 **(a)**



Q.56 **(26)**



Q.57 **(256)**
Wrap-around time is nothing but in how many seconds will all the hosts generate all IDs possible. (i.e. TOTAL_IDS / NO. OF IDS PER SEC).
Total IDs possible with 50-bit is 2^50.
One host generating 1000 identifiers per sec. So all hosts will generate 2^{32} * 1000 ----> 2^{32} * 2^{10}-----> 2^{42} unique IDs.
If we Divide them, we get answer (i.e. $2^{50}/2^{42}=2^8$)

Q.58 **(c)**
(a) The **connect function** is used by a TCP client to establish a connection with a TCPserver.
(b) The **bind function** assigns a local protocol address to a socket. With the Internet protocols, the protocol address is the combination of either a 32-bit IPv4 address or a 128-bit IPv6 address, along with a 16-bit TCP or UDP port number.
(c) The **listen function** converts an unconnected socket into a passive socket, indicating that the kernel should accept incoming connection requests directed to this socket.

(d) The **accept function** is called by a TCP server to return the next completed connection from the front of the completed connection queue. If the completed connection queue is empty, the process is put to sleep (assuming the default of a blocking socket).

Q.59 (a)

Network No.	Net Mask	Next Hop	Next Hop
128.96.171.92	255.255.254.0	128.96.170.0	Interface 0
128.96.168.151	255.255.254.0	128.96.166.0	R2
128.96.163.151	Default	0.0.0.0	R4
128.96.165.121	255.255.252.0	128.96.164.0	R3

Q.60 (a)

TCP is a byte stream protocol. Hence III is false. TCP can use both selective ACK and Cumulative Acknowledgement.
Hence II is false.
TCP connection are full duplex.
∴ Statement I is correct.

Q.61 200.10.11.144/27
255.255.255.224
$224 \rightarrow 11100000$

$144 \rightarrow \underset{\text{N/w ID}}{100}\ 10000$

$\text{First IP} \rightarrow 10000001$

$\text{Last IP} \rightarrow 10011110$

i.e. last IP is 200.10.11.158
∴ 158 is the fourth octet of the last IP address.

Q.62 (b)

Length and checksum can be modified when IP fragmentation happens. Time To Live is reduced by every router on the route to destination. Only Source Address is what IP address cannot change.

Q.63 (c)

UDP data = 8880 bytes
UDP header = 8 bytes
IP Header = 20 bytes
Total Size excluding IP Header = 8888 bytes.
Number of fragments= ceil (8888/ 1480) = 7
Refer the Kurose book slides on IP (Offset is always scaled by 8)
Offset of last segment $= (1480*6)/8 = 1110$

Q.64 (b)

TCP sequence number of a segment is the byte number of the first byte in the segment. For example, if the segment contains 500 bytes which are from 1000 to 1499, then sequence number of the segment would be 1000 and sequence number of next segment would be 1500. Receiver window changes when TCP data is processed by application layer of receiver side.

Q.65 (b)

A server must first do bind() to tell operating system the port number on which it would be listing, then it must listen to receive incoming connection requests on the bound port number. Once a connection comes, the server accepts using accept(), then starts receiving data using recv().

Q.66 (c)

Since sequence number in TCP header is limited to 16 bits, the maximum window size is limited. When bandwidth delay product of a link is high, scaling is required to efficiently use link. TCP allows scaling of windows when bandwidth delay product is greater than 65,535 (Refer this).
The bandwidth delay product for given link is 1048560 * α. Window

scaling is needed when this value is more than 65535 bytes, i.e., when α is greater than 65535 * 8 / 1048560 or 0.5 seconds. Scaling is done by specifying a one byte shift count in the header options field. The true receive window size is left shifted by the value in shift count. A maximum value of 14 may be used for the shift count value.
Therefore maximum window size with scaling option is 65535×2^{14}.

Q.67 13

L =1000 bytes
MTU = 100 bytes
IP header = 20 bytes
So MTU payload is 100–20 = 80 bytes
Number of fragments = 1000/80 = 13

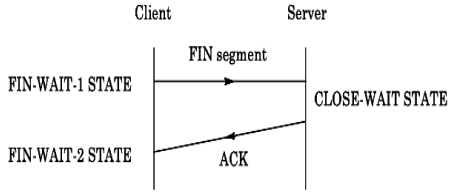
Q.68 1.2

Given, Maximum burst rate, M=20 MB
Token arrival rate, P = 10 MB
Constant rate(bucket o/p), P=10 MB
Bucket capacity, C = 1 MB
Time for 1 MB, S=C/(M–P)=1/(20–10) = 0.1 sec
For the total message of 12 MB is 1.2 sec

Q.69 (b)

Bind () function creates local address. Connect ( ) function is specifying remote address. An unconnected UDP socket is just a bind ( ) function.
A connects UDP socket is one more step above i.e connects ( ) function Just behaves like TCP

Q.70 (d)



Q.71 (9)

In IPv4, options and padding 40 bytes are alloted. Maximum nine routers addresses are allowed. Each IPv4 address is 32 bits or 4 bytes So 4× 9 = 36 bytes Extra bytes are used for the option.

Q.72 (c)

UDP Port address length is 16 bits

Ethernet MAC address is of 48 bits

IPv6 Next header is 8 bits

TCP Sequence number is 32 bits

Q.73 (c)

The value of the Congestion Window will be increased by one with each acknowledgment (ACK) received, effectively doubling the window size each round-trip time.

Q.74 34 or 35

Wrap Around Time = (Possible sequence no. in TCP)/ Given Bandwidth

Note: Bandwidth should be in Byte/Second, so convert if it's given in bits/second. This is because in TCP 1 Byte Consume 1 Sequence no.

WRAP AROUND TIME = (2^32*2^3)/10^9 = 34.35 seconds

Q.75 144

MTU = 600 bytes and IP Header = 20 bytes
So, Payload will be 600 – 20 = 580 bytes

580 is not multiple of 8, but we know fragment size should be

multiple of 8. So fragment size = 576 bytes

K^{th} fragmentation offset value = Fragment Size * (K^{th} fragment – 1) / Scaling Factor
Offset value of 3^{rd} fragment

= 576 * (3 – 1) / 8 = 144

4 APPLICATION LAYER AND NETWORK SECURITY

4.1 SESSION LAYER

The Session Layer establishes maintain and synchronize dialogue between communication upper layers (communication may be between other users or application). The session layer provides a user interface to the transport layer.

4.1.1 SERVICE OF THE SESSION LAYER:

- To – co ordinate connection and disconnection of dialogs between applications.
- To provide synchronization points for data exchange.
- To c0 – ordinate who sends when.
- To ensure that the data exchange is complete before the Session closes.

4.1.2 SESSION LAYER TO TRANSPORT LAYER COMMUNICATION

This communication can be of three types:
i) One to one
ii) Many to one
iii) One too Many

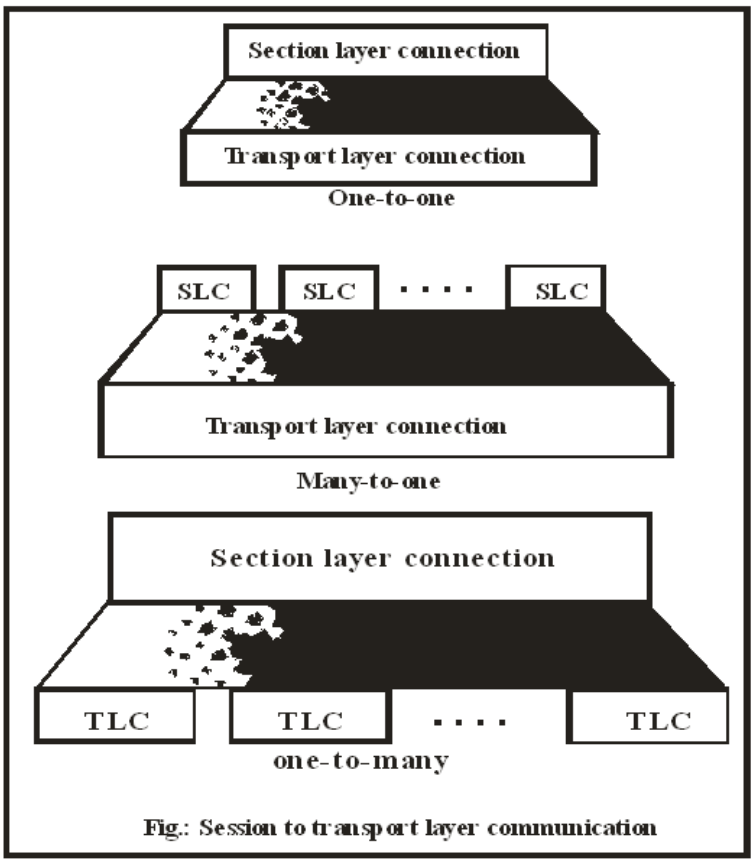


Fig.: Session to transport layer communication

4.1.3 SYNCHRONIZATION POINTS

The transport layer is responsible for delivering a transmission with complete reliability. The session layer provides a mechanism, called synchronous points for recovering data that have been delivered but mishandled. To control the flow of information and allow recovery from software or operate errors the layer allows refund points to be introduction into the data.

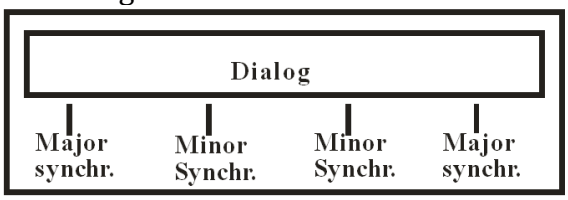
Two types of synchronous points may be used

- Major and
- Minor

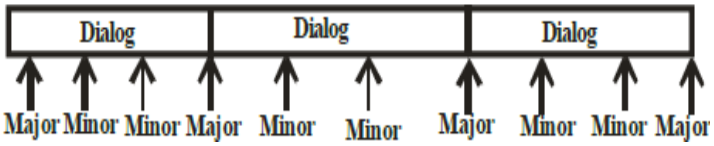
Major synchronous points divided an exchange into a series of dialogs. Each major synchronization point must be acknowledged before the session can continue. If an error occurs, data can be recovered only up to the last major point.

A Session Layer activity can be a single dialog or several dialogues separated by major synchronous points. Minor synchronous points are inserted into the middle of dialogs and may or may not require confirmation depending on the application. They are primary security blankets. If an error occurs the control flow goes back one or more minor synchronous points within a dialog to recover the data.

An activity made of only one dialog.



An activity made of only more than one dialog.

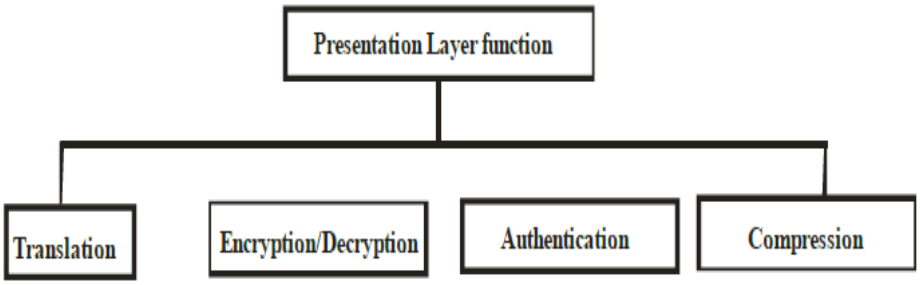


4.1.4 SESSION PROTOCOL DATA UNIT

1) SI (SPDU identifier): It indicates the type of data unit.
2) LI (Length indicator): It indicates the Length of SPDU parameters filed.
3) PGI / PI (Parameter Group Information / parameters information): It includes control information and quality of service specifications.

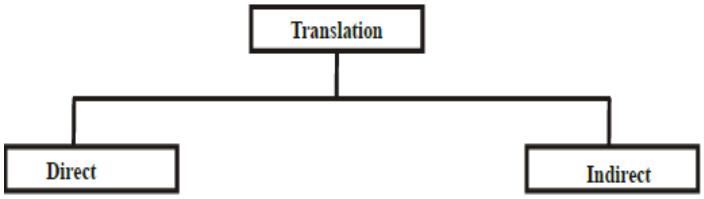
4.2 PRESENTATION LAYER

4.2.1 FUNCTION OF PRESENTATION LAYER



1. Translation

Internet representation of a piece of information might vary from one machine to the other. Transmission handles this problem, so that receiving machine can understand the message sent by the transmitter.



Direct Translation

In direct translation method, sender format is translated into receiver format at the itself.

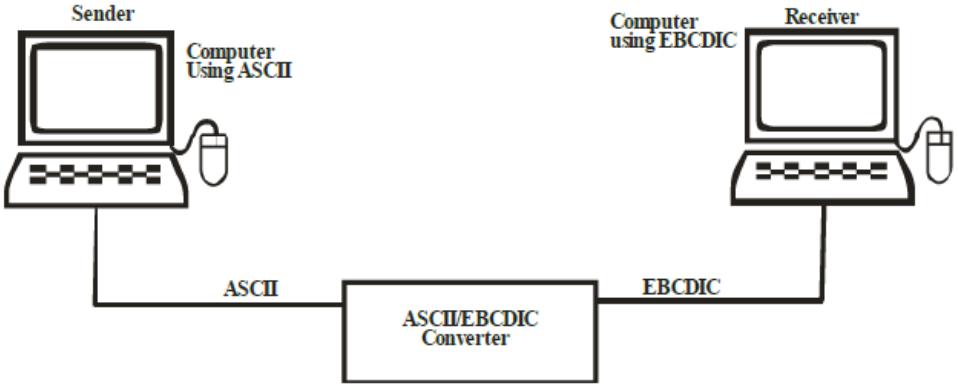
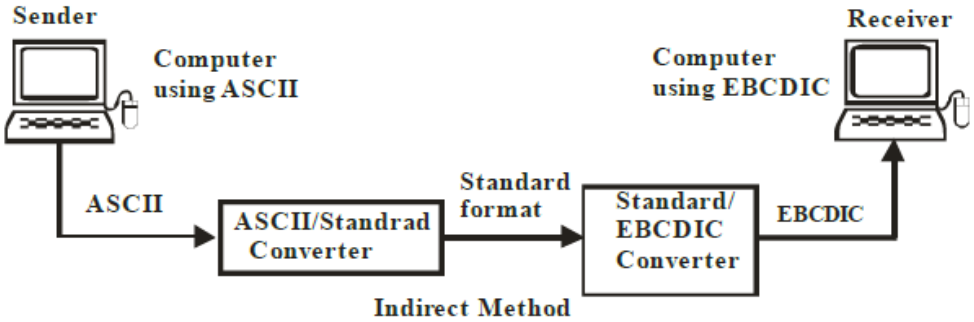


Fig.: Direct Translation

In the given figure ASCII code is transmitted into EBCDIC code at the receiver.

Indirect Translation

In Indirect translation method, transmitter code is transmitted to a standard format at the sender and translated into receiver code at the receiver.

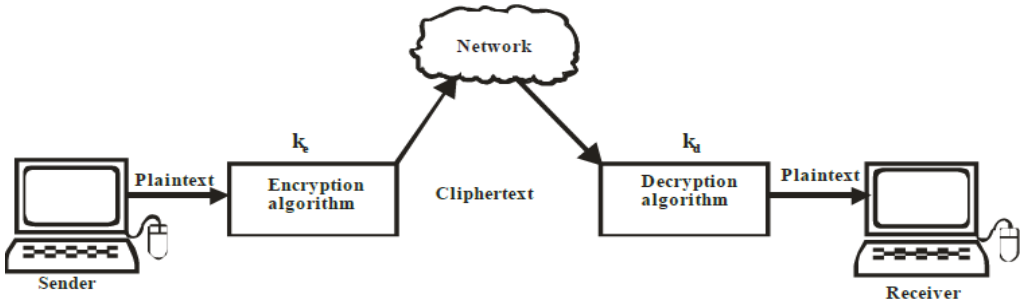


In the given figure ASCII code is translated to a standard format at the sender and translated into EBCDIC at the receiver.

2. Encryption / Decryption

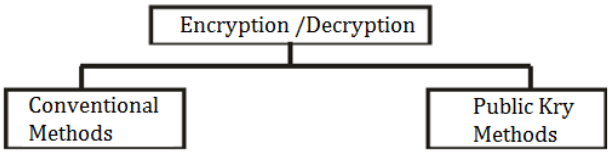
One needs to completely prevent unauthorized access to transmission media. Thus alter information so that only an authorized receiver can understand it. Thus we need to encrypt and decrypt information.

Encryption
Encryption means that the sender transforms the original information to another form and sends the resulting unintelligible message out over the network.
Decryption
Decryption reverses the encryption process in order to transform the message back to its original form.



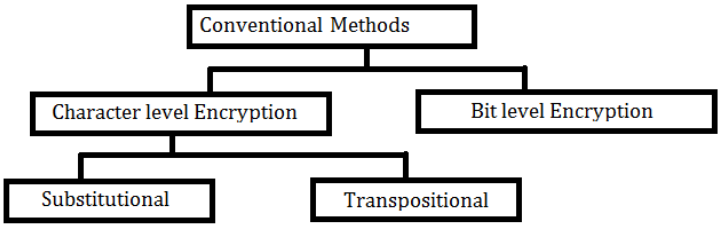
The sender uses an encrypting algorithm and a key to transform the plaintext in to a cipher text. The receiver uses a decryption algorithm and a key transform the cipher text back to the original plaintext.

Categories of Encryption and Decryption methods



Conventional Methods

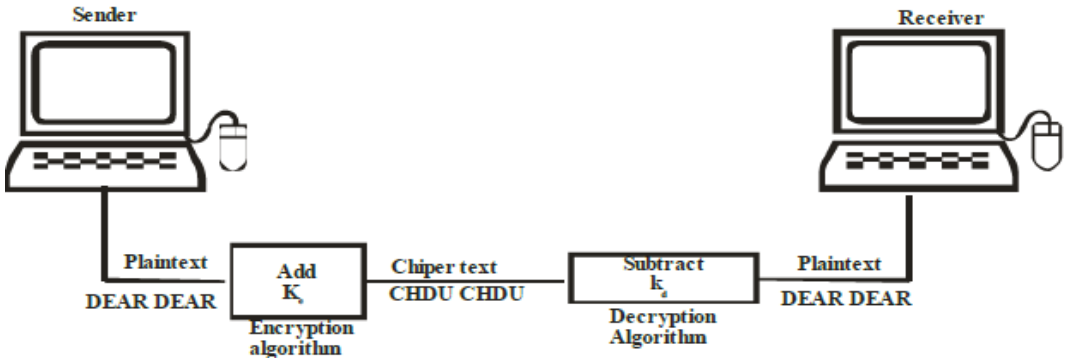
In convergent encryption methods, the encryption key (k_e) and decryption key (k_d) are same and secret.



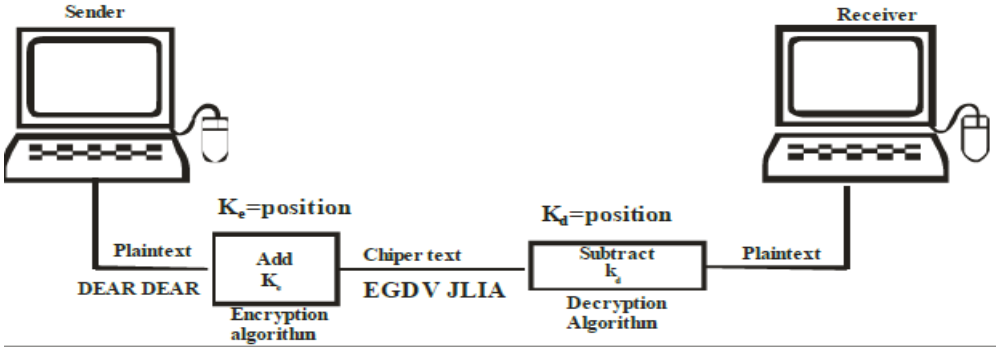
Character Level Encryption

Substitution

(i) In mono alphabetic substitution each character is replaced by another character in the set. The encryption algorithm simply adds a number to the ASCII code of the character. The decryption algorithm simply subs tracks the same number from the ASCII code.

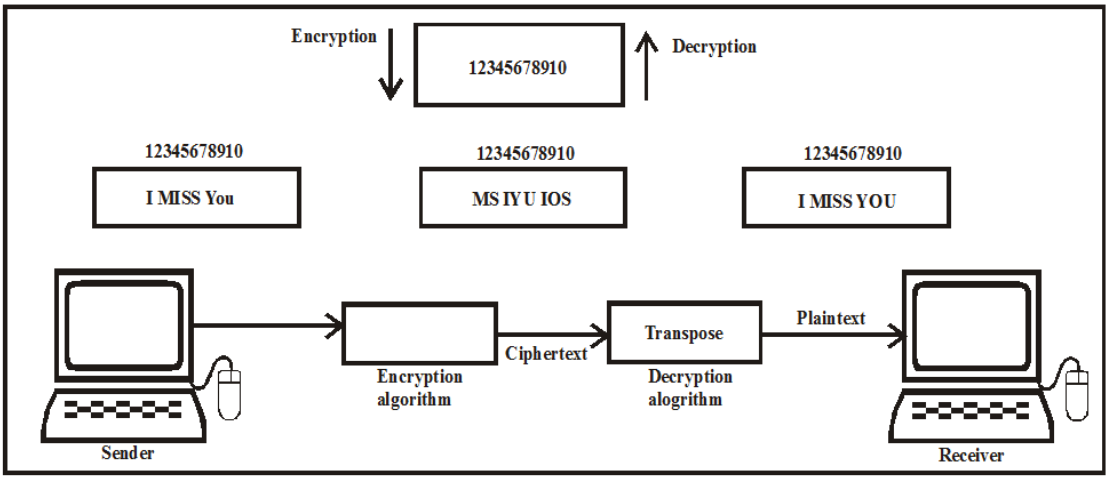


(ii) In poly alphabetic substitution each occurrence of a character can have a different substitute. One possible technique is to find the position of the character in the text and use that value as the key.



Tran positional

In trans positional encryption each character retain their plaintext from but change their positions to create the cipher text. The text is organized into a two – dimensional table, and the columns are interchanged according to a key.

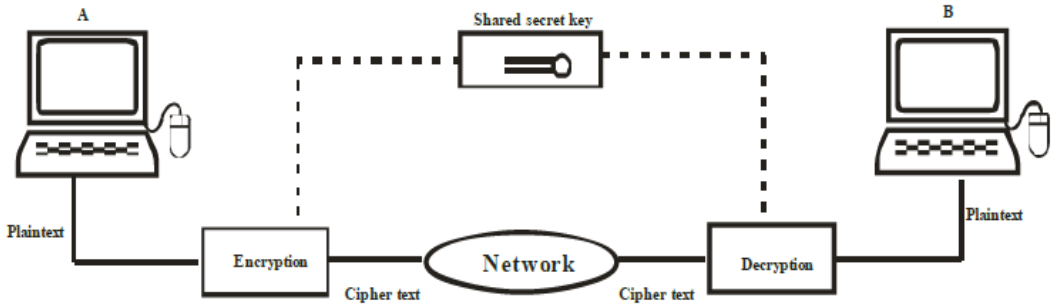


Bit – Level Encryption

Data as text, graphic, audio or video are divided into blocks of bits and then altered by Encoding / Decoding, permutation, substitution, exclusive OR, rotation, and so on.

Secret Key Encryption / Decryption

The same key is used by both parties. The sender uses this key and an encryption algorithm to decrypt the data and the receiver uses the same key and the corresponding decryption algorithm to decrypt the data. The algorithm used for decryption is the inverse of the algorithm used for encryption.



Advantage

i) Efficient as it takes less time to encrypt a message using secret key algorithm.

ii) As key is smaller, thus used to encrypt long messages.

Disadvantages

i) If N people in the world want to use this method, then one need N (N-1) / 2 secret keys.

ii) The distribution of the keys between two parties can be difficult.

Data Encryption Standard (DES)

DES was developed by IBM in the early 1970s. The DES divides a message into 64-bit blocks and uses 56-bit key. It uses a complex combination of transposition (rearrangement of bits), substitution (replacing one bit group with another), exclusive OR operations and few other process on each block to eventually produce 64- bits of encrypted data. In all, the 63-bits block data goes through 19 successive steps, with the output of each step being input to the next step.

The figure (a) shows the primary steps. The first step does a transposition on the 64 data bits and the 56- bit key. The next 16 steps involve many operations. Each step is the except that it uses the different input derived from the first. The second last step swaps the first 32- bit sand the last 32 – bits. The last stage is the exact inverse of the transmission. The algorithm has been designed to allow decryption it be done with the same key as encryption. Decryption algorithm follows the steps of encryption algorithm in reverse order.

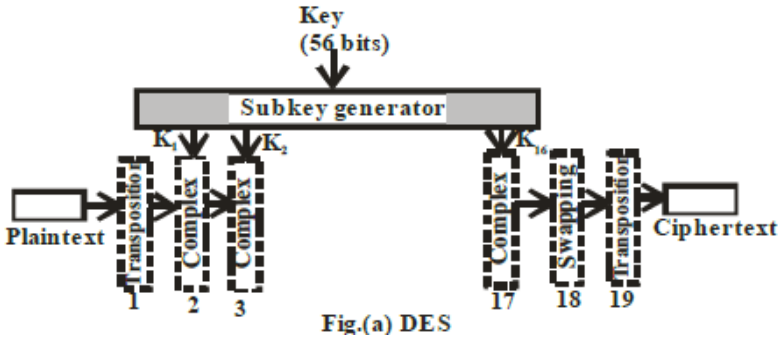
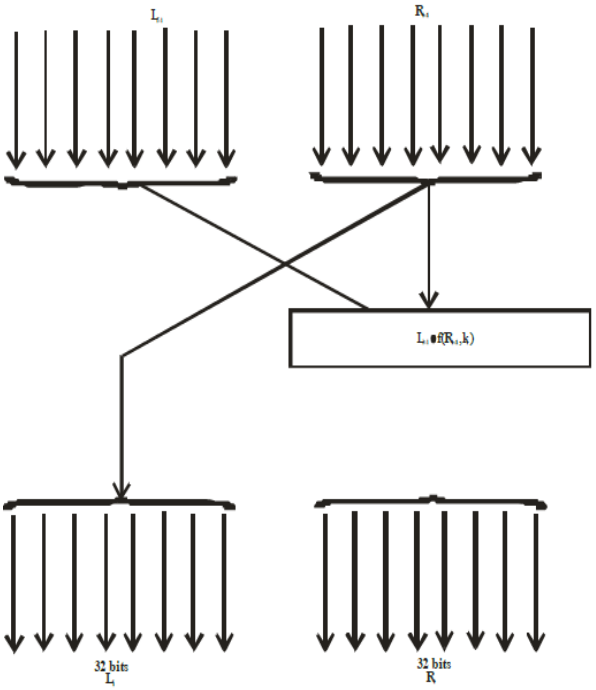


Fig.(a) DES

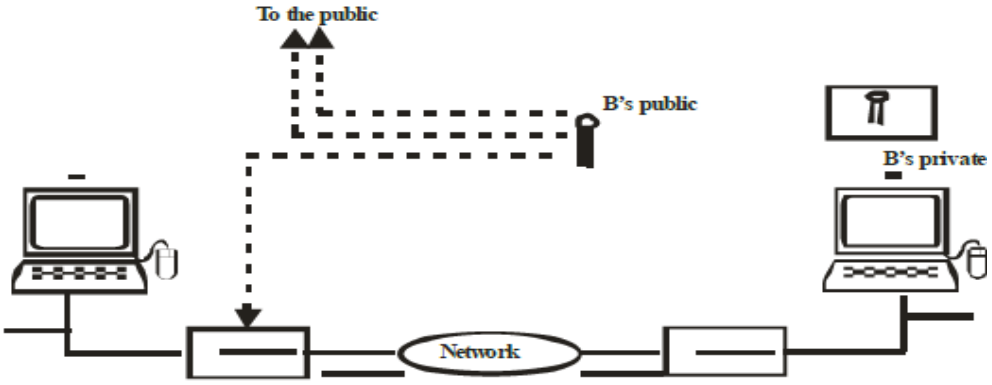


The operation of one of these 16 intermediate stages is illustrated in figure (b). Each stage takes two 32 – bits inputs and produces two 32 – bits outputs. The left output is simply copy of the right input. The right output is the bitwise EXCLUSIVE OR of the left input and a function of the right input and the key for this stage K_i.

The function consists of four steps, carried out in sequence. First, a 48- bit number, E is constructed by expanding the 32- bits R_{i-1} according to a fixed transmission and duplication rule. Second, E and K_i are EXCLUSE O Red together. This output is then partitioned into eight groups of 6 bits each. Each 6 bit group is mapped onto a 4 – bit output resulting $8 \times 4 = 32$ – bits. In each of the 16 operations, a different key is used.

A technique that is sometimes used to make DES stronger is called **whitening.** It consists of XORing a random 64 – bit with each plaintext blocks before feeding it into DES and then XORing a second 64- bit key with the resulting cipher text before feeding it into DES and then XORing a second 64-bit key with the resulting cipher text before transmitting it. Whitening can easily be removed by running the reverse operations (if the receiver has two whitening keys). Since this technique effectively adds more bits to the key length, it makes exhaustive search of the key space much more time consuming.

Public key encryption



It uses two keys: **a private key and a public key.** The private key is kept by the receiver and public key is announced to the public. The public key that is used to encrypt the algorithm is different from the private key that is used to decrypt the algorithm. The public key is available to the public and the private key is kept by each individual.

Advantage

i) Each entity can create a pair of keys , keep the private one, and public distributes the other one.
Each entity is independent and the pair of keys created can be used communicate with any other entity.

ii) The number of keys needed is reduced tremendously.

Disadvantage

This algorithm is very complex. Moreover large number makes this method mote effective. Use of long keys takes a lot of time.

RSA Algorithm (Rivest, Shamir and Aldeman)

For Finding Kp. And N

- Choose two prime numbers as p and q
- Calculate N = p × q
- Select Kp such that it is not a factor of (p-1) × (q-1).
- Select Ks such that "(Kp × Ks) modulo (p-1) × (q-1) = 1"

Encryption Algorithm

- Encode data as number.
- Calculate the cipher text C as C = P^{kp} Modulo N.
- Send C as the cipher text. Decryption Algorithm
- Receive C as the cipher text
- Calculate plaintext P = C^{ks} Modulo N
- Decode P to the original date

A example of how the RSA algorithm works is given in Fig. below, in this example we have chosen p = 3 and q = 3 and q = 11, giving n = 33 and z = 20. A suitable value for d is d = 7, since 7 and 20 have no common factors. With these choice, e can be found by solving the equating 7e = 1 (mod 20), which yields e = 3. The cipher text C, for a plaintext message, P is given by C = p^3 (mod 33).

The cipher text is decryption by the receiver by making use of the rule P = C^7 (mod 33). The figure shows the encryption of the plaintext "SUZANNE" as an example.

Because the primes chosen for this example are so small, P must be less than 33 so each plaintext block can contain only a single character. The result is a mono alphabetic substitution cipher not very impressive. If instead we had chosen p and n ≈ 2^{1024}, so each block could be up to 1024 bits or 128 eight – bit characters, versus 8 characters for DES and 16 characters for AES.

Plaintext(p)			Ciphertext(C)		After decryption	
Symbolic	Numeric	P^3	P^3(mod 33)	C^7	C^7(mod 33)	Symbolic
S	19	6859	28	13492928512	19	S
U	21	9261	21	1801088541	21	U
Z	26	17576	20	1280000000	26	Z
A	01	1	1	1	01	A
N	14	2744	5	78125	14	N
N	14	2744	5	78125	14	N
E	05	125	26	8031810176	05	E

Sender's computation

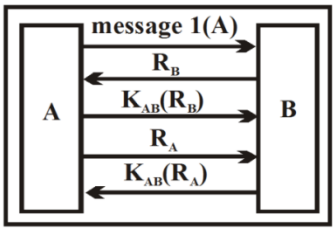
Receiver's computation

3. Authentication

Authentication means verifying the identity of the sender. In other words authentication verifies that a message is coming from an authentic sender.

(i) Authentication based on a Shared Secret key

In this protocol, a secret key is shared with both party i.e. source and destination. One party sends random number to the other; other side transforms it in special way and then returns a result. This type of protocols are challenge response protocols. The working of this protocol is as follows.



First, the party -1 sends a message -1 to party -2 for introducing it. Party -2 needs to find out who has sent this message. So party-2 chooses, a large random number R_B and sends it to party- 2 in plain text format. The party – 1 then encrypts the message with the key which it shares with party – 2 and sends cipher text K_{AB} (R_B) back in message with the key which the key which it shares wit they known that message is from party 1 because of the shared secret key.

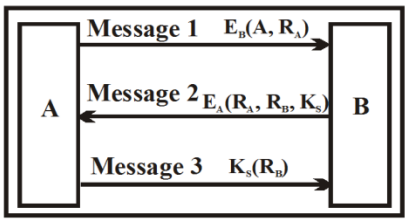
At this point party -2 is sure he is talking to party – 1, but party-1 is not sure of anything. To identify the receiver, Party – 1 sends a random number R_A to party-2 as plain text. Party -2 responds with secret key and sends cipher text K_{AB} (R_A). Party – 1 now knows they are communicating with party-2.

Disadvantage

It is slower and contains extra messages.

(ii) Authentication using public cryptography

In this method, A sends a random, number R_A after encrypting. A uses B' public key E_a for sending message. When B receives this message, B sends a back a message containing A's random numbering, its own random number R_B and a proposed session key K_S. When A gets message 2, A decrypts it using private key.

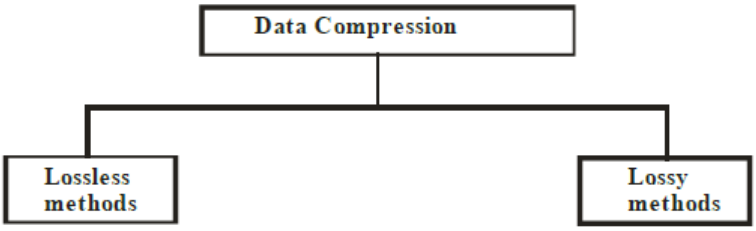


After examining the message 2, A finds out random number R_A. Know message 2 is form B only. Then A agree to the session by sending back message 3 to B. When B reads R_B encrypted with the session key which is generated by B, B knows that A got message 2 and verifying R_A. This protocol assumes that both user A and B already knows each other public key.

4. Data Compression

IMP:

Data compression reduces the number of bits.



Lossless Compression

In each lossless data compression, the compressing and decompressing algorithm are usually the inverse of each other. After decompressing, will get the exact data as they were before compressing. Thus nothing is lost.

For example, Run – length encoding, statistical compression, relative compression.

Lossy Compression

Lossy data compression produces the decompressed information which need not be an exact replica of the original information. The method is lossy compression as one will lose some of the original data in the process. For example, JPEG, MPEG

4.3 APPLICATION LAYER

The application layer enables the user to access the network. It provides user interfaces and support for service such as electronic mail, remote file access and transfer, shared database management and other of distributed information services.

4.3.1 ISSUES IN APPLICATION LAYER

There are three general issues related to this layer: the client server paradigm, addressing, and types of services.

4.3.3 ADDRESSING

A client and a server communicate with each other using addresses. When a client requests a service from a server, it must include the address of the serve as the destination address, as well as its own address as the source address. The source address is required so that the

server where to send the response. When the server responds to the request, it reverses the addresses; it uses its own address as the source and the address of the client as the destination.
However, the addressing mechanism in the application program is not like the ones in other layers; each application its own address format. For example, an email address may look like foruzan@fhda.edu, while an address to access a web page may look http://www.fhda.edu.
The address is related to the port address of the server and the directory structure where the server program is located. The main part, however, is an alias name for the address of the remote host. The application program uses an name instead of an IP address. Although this type of address is very convenient for human begins to remember and use, it is not suitable for the IP protocol when it opens a communication with the server. The alias address must be mapped to the IP address. An application program needs the service of another entity to map the alias address, This entity is an application program, called DNS. In this layer, DNS is not directly used by the user; it is used by other application programs to perform the mapping.

4.3.4 TYPES OF SERVICE

The application layer is designed to give different services to the user or user programs. The most common service, SMTP, allows a user to send a message to another user in the Internet. This service is electronic mail and has many similarities to the traditional postal mail. Another common service is file transfer. A user can transfer a file from its computer to the server or transfer a file from a server to its computer. This application program is called FTP.

4.3.5 SUPPORT

To be useful to the user, an application program must be supported by the services provided by the lower layer, the transport layer. The type of support needed is different for different applications. We can categorize this support into three categories: reliability, throughput, and delay.

4.3.6 RELIABILITY

Some application depends heavily on reliability. Among them is email and file transfer. We do not want to receive a corrupted email or a file that is missing some of its parts. These types of application need either to include reliability as part of their protocol or use the services of a reliable transport- layer protocol such as TCP. Other application programs are not so sensitive to reliability. If a very small part of the music we download from the Internet is missing, it might not even be noticeable.

4.3.7 THROUGHPUT

Maximum throughput, the maximum amount of data that can be transferred in a unity of time is a criteria required by some applications. Multimedia applications need, in general, a high throughput to be effective.

4.3.8 DELAY

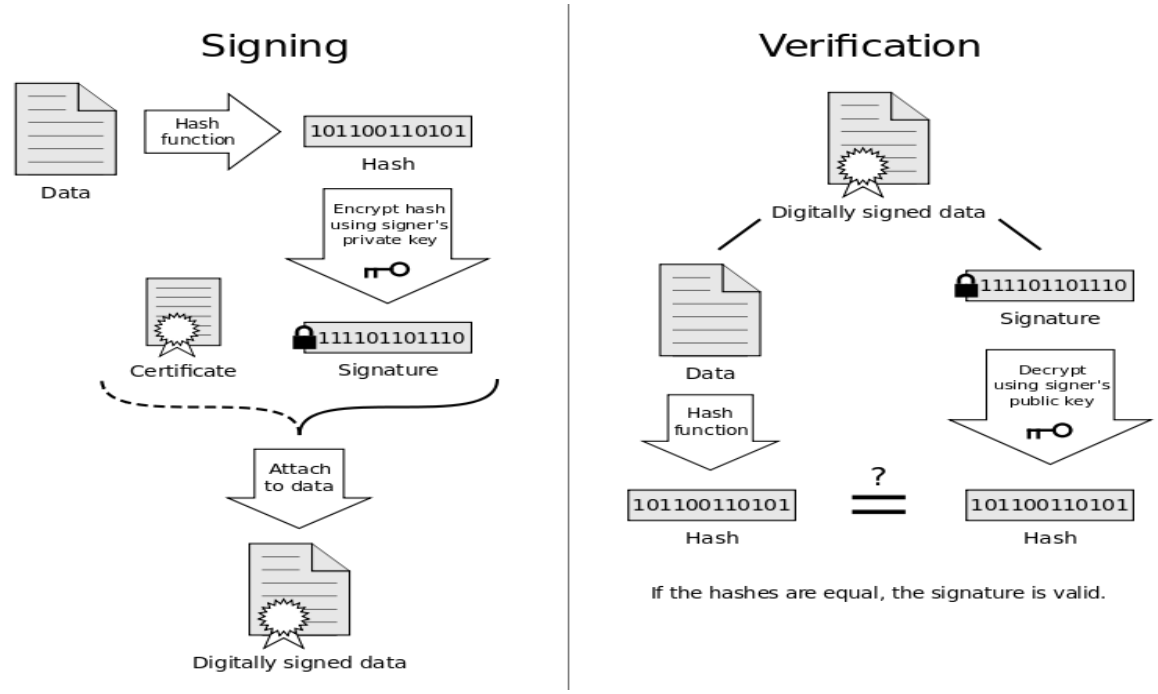
Some applications are very sensitive to delay. An interactive real-time application program cannot tolerate delay. We do not want to use the Internet as a telephone service if there are long delays in the conversation. Some applications, on the other hand are not sensitive to delay. An email can wait for a few seconds or even hours before delivery.

4.4 DIGITAL SIGNATURES:

A digital signature is a mathematical approach for presenting the authenticity of digital messages or documents.

A digital signature scheme meets the security constraints, **authentication, non – repudiation and integrity**. It gives a recipient reason to believe that the message was created by a known sender (authentication), that the sender cannot deny having sent the message (non-repudiation), and that the message was not altered in transit (integrity)

DIGITAL SIGNATURE SCHEME:



A digital signature scheme typically consists of 3 algorithms;

- A **key generation algorithm** that selects a private key uniformly at random from a set of possible private keys. The algorithm outputs the private key and a corresponding public key.
- A **signing algorithm** that, given a message and a private key, produces a signature.
- A **signature verifying algorithm** that, given the message, public key and signature, either accepts or rejects the message's claim to authenticity.

4.5 FIREWALLS

The term *firewall* is a metaphor that compares a type of physical barrier that's put in place to limit the damage a fire can cause, with a virtual barrier that's put in place to limit damage from an external or internal cyber attack. When located at the perimeter of a network, firewalls provide low-level network protection, as well as important logging and auditing functions.
While the two main types of firewalls are host-based and network-based, there are many different types that can be found in different places and controlling different activities. A host-based firewall is installed on individual servers and monitors incoming and outgoing signals. A network-based firewall can be built into the cloud's infrastructure, or it can be a virtual firewall service.

Types of firewalls

Other types of firewalls include packet-filtering firewalls, stateful inspection firewalls, proxy firewalls and next-generation firewalls (NGFWs).

- A packet-filtering firewall examines packets in isolation and does not know the packet's context.
- A stateful inspection firewall examines network traffic to determine whether one packet is related to another packet.
- A proxy firewall inspects packets at the application layer of the Open Systems Interconnection (OSI) reference model.
- An NGFW uses a multilayered approach to integrate enterprise firewall capabilities with an intrusion prevention system (IPS) and application control.

How packet-filtering firewalls work

When a packet passes through a packet-filtering firewall, its source and destination address, protocol and destination port number are checked. The packet is dropped -- it's not forwarded to its destination -- if it does not comply with the firewall's rule set. For example, if a firewall is configured with a rule to block Telnet access, then the firewall will drop packets destined for Transmission Control Protocol (TCP) port number 23, the port where a Telnet server application would be listening.

Packet-filtering firewalls work mainly on the network layer of the OSI reference model, although the transport layer is used to obtain the source and destination port numbers. They examine each packet independently and do not know whether any given packet is part of an existing stream of traffic. Packet-filtering firewalls are effective, but because they process each packet in isolation, they can be vulnerable to IP spoofing attacks and have largely been replaced by stateful inspection firewalls.

4.6 STANDARD COMMON APPLICATIONS

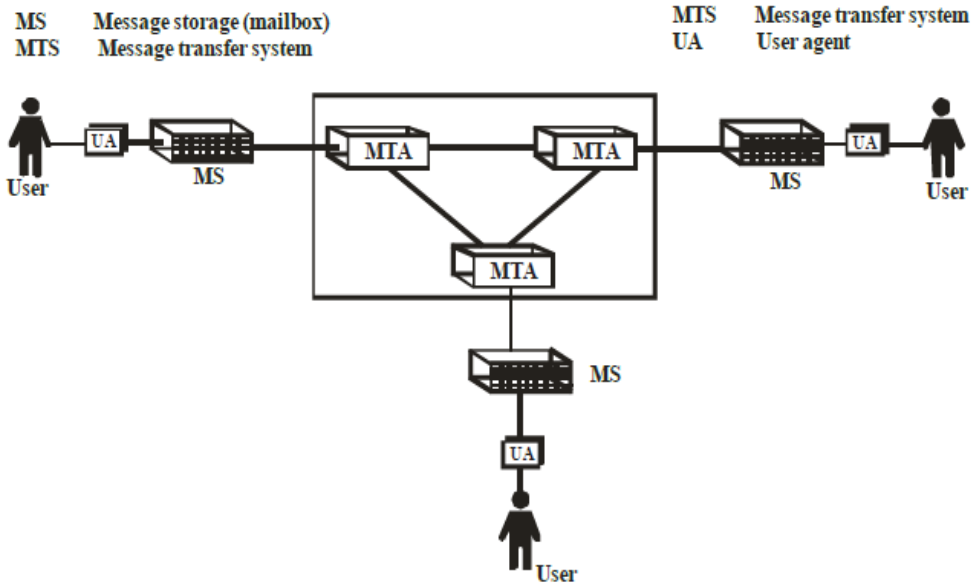
(i) Message Handling System (MHS)

MHS is the OSI protocol that underlines electronic mail and store and forward handling. It is delivered form ITU-T x.400. MHS is the system used to send any message (including copies of data or files) that can be derived in a store and forward manner. Store and forward delivery means that instead of opening an active channel between the sender and receiver,

the protocol provide a delivery service that forward the message when a link a delivery system. The delivery system may not be able to transmit sender the message immediately. When the message is delivered, it is stored in recipient's mailbox.

The Structure of MHS

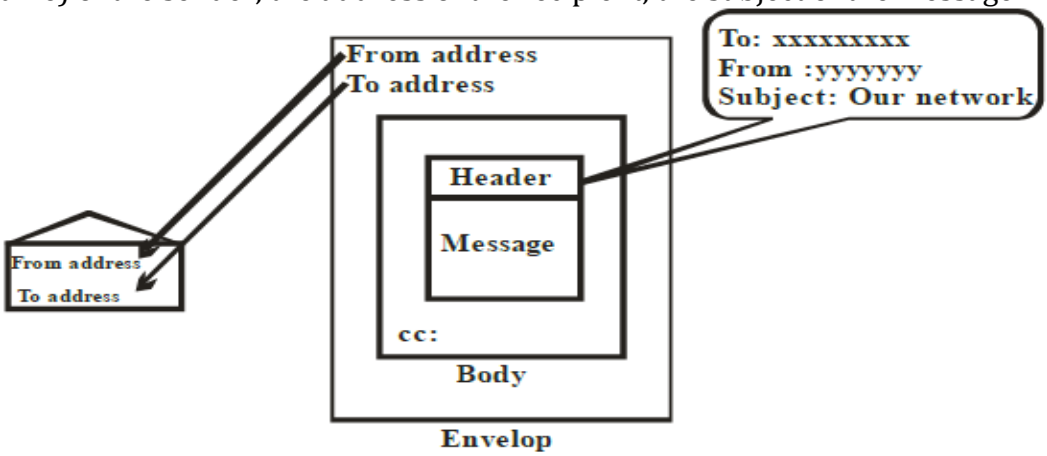
Each user communicates with a program or process called a user agent (UA). The UA is unique mail program associated worth a specific operating system that allows a user to type and edit the message.



Each user has message storage which consists of disk space in a Mail Storage system and is usually referred to as a mail box. Message storage can be use for storing, sending or receiving messages. The message storage communication with a series of process called **Message transfer agents (MTA).** The combined MTA make up the message transfer system (MTS).

Message format

The MHS standard defines the format of a message. Every message can include the address (name) of the sender, the address of the recipient, the subject of the message.

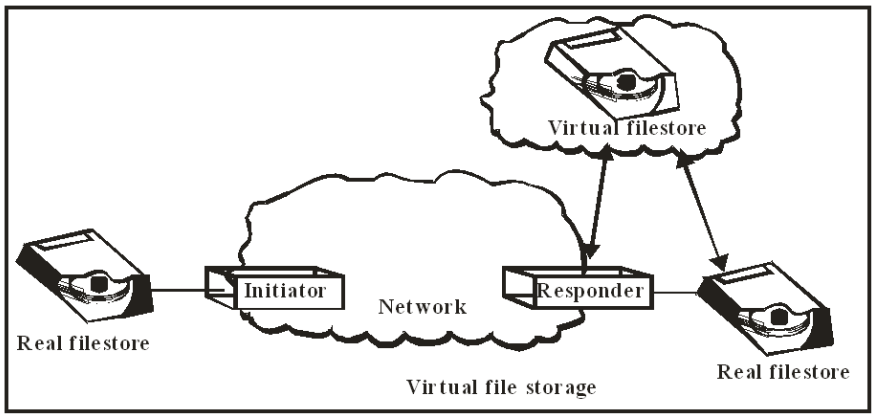


(ii) File Transfer, Access and Managements

The FTAM protocol is used to transfer (copy), access (read, write or modify) and manages (control) files.

Virtual Files and File Stores

To allow the interaction of different file systems, FATM uses the concept of virtual files and virtual file storages. A virtual file stores is a non implementation specific model for files, and database that can be used as an intermediary for file transfer and management.



FTAM is based on asymmetrical access of a virtual file. Each transaction requires an initiator and a responder. The initiator request the transfer of access to or management of a file from responder. The responder creates a virtual file model of its actual file allows the initiator to use virtual model rather than the real file. Because the model is software, it can be designed to be independent of hardware and the operating system constraints.

Attribute and Content

The creation of virtual file store is based on two aspects of the file.

(i) Attribute

(ii)Content

The attributes of a file are a set of properties & security measures used to control either the content or a access. FATM distinguishes between two different types of attributes: per-content and per access.

Per content attributes are those related to the contents of the file. Per- access attributes are security measure that control access to file.

Virtual Terminal

One of the most important applications defined in the OSI model is the virtual terminal (VT).

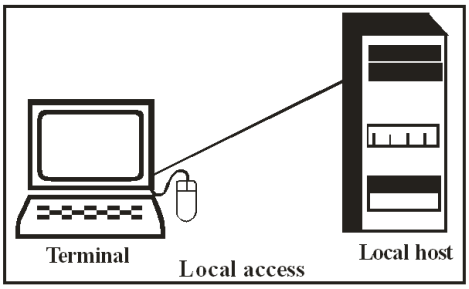
Remote Access

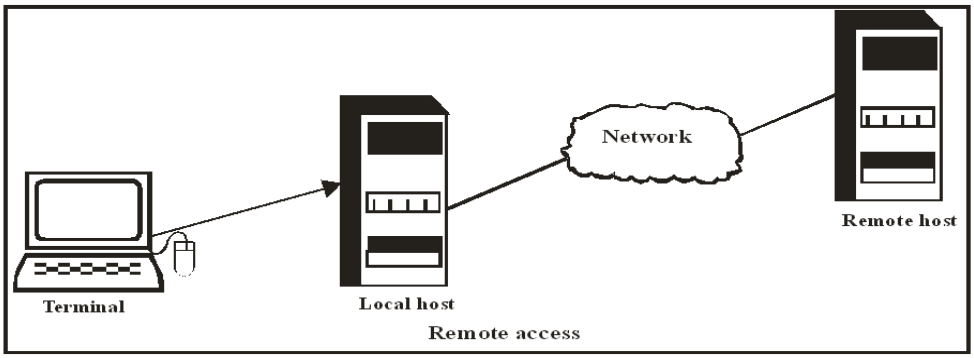
Ordinary, access to a host such as a minicomputer, work station or mainframe is gained through a terminal. Terminals are physically linked to the host. The physical connection is referred to as local access. When the connected to a local host which is in turn connected through a network to a remote host. If the terminal and remote host area of the same type (both 1 BM for ex.) then the network acts as an extra long local link. Problem arise when a

terminal of one type wishes to be connected to a host of another type. The above problem can be eliminated by a virtual terminal.

Virtual Terminal

A virtual terminal is an imaginary terminal with a set of standard characteristic that every host understands. Virtual terminal is a software version of a physical terminal. A terminal that wishes to communicate with a remote host, communications to its local host. The local host contains VT software that translates the request or data received from the actual terminal into the intermediary format used by the VT. The reformatted data travel over the network to the remote host. The remote host passes the transmission to its own VT software which transforms it from its VT format into the format used by the remote host's own terminals. The remote host, therefore receives the input as it is form a local host. After processing the request, the remote host can return a response following the same procedure in reverse.





Directory Services

The OSI directory services are designed according to ITU –T X. 500 standard. A directory is a global source of information about many different objects. An OSI directory service is an application program used to represent locate objects – contained in an OSI directory. The type of information that a directory hold varies according to the types of the object.
The user of a directory service can be either a person or an application. To the user of a directory service all of this information appears to be stored in a single database located in a single host. A directory is distributed database with each host holding only a part. The access mechanism however is structured so that users known only one entry port from which port from which all information may be retrieved.

DIB
The information contained in the directory is called the directory information base (DIB). It is stored as a set of entries each describing one object. An entry may consists of several parts each of which describes a different attributed of the origination a mailing address,

phone no. and so on. The entire structure is organized a tree with different levels of generally at each branch.

Electronic Mail

The attraction of electronic mail or email is that is every very fast. Email has the speed of the telephone without requiring both the parties be available at the same instant. It also leaves a written copy of the message that can be field away or forwarded. Furthermore, a message can be sent to many people at once.
Electronic mail systems are constructed of two distinct but closely related parts:

User Agents

Providing the human interface (e.g. composition, editing and reading mail)

Message transfer Agents

For transporting mail (e.g. managing mailing lists and providing notification of delivery)
Email system supports five basic functions:-

Composition	Refers to the process of creating message and answer
Transfer	Refers to moving message from the originator to the recipient
Reporting	To tell the originator what happened to the message. Was it delivered? Was it rejected? Was it lost?
Displaying	Incoming messages is needed to be displayed so people can read their email
Disposition	Concerned with the recipient does with the message after receiving it

Addition to the basic services is mailbox, mailing list etc…
The user Agent

- **Sending Email**

To send email message, , a user must provide the message, the destination address and possibly some other parameters.

- **Reading Email**

When the user agent is stared up, it will look at the users mailbox for incoming email before displaying anything on the screen. Then it may announce the number of messages in the mailbox or displays onetime summary of each message and wait for a command.

Message Formats

- **RFC 822**

The user agent builds the message and passes it to the message transfer agent which then uses some of the heade4r field to construct the actual envelope.
RFC 822 header fields related to the messages are:
To cc bcc from sender subject return_ path date replay _ to message _id
Reference: keywords
In the message body user can put the text, ascii cartons, political statements an disclaimers of all kinds.

- **MIME- Multipurpose Internet Mail Extensions**

The basic idea of MIME is to continue to use the RFC 822 format, but to add structure to the message body and define the encoding rules for the non-ASCII messages. By not deviating from RFC 822, MIME messages can be send using existing mail programs and protocols.
MIME defines five new message headers:-

Header	**Meaning**
MIME version	Identifications the MIME versions
Content_ Desc.	String telling what is in the message
Content _ Id	Unique Identifier
Content _ transfer _ encoding	How the body is wrapped for Xmssn
Content _ type application,	Nature of the message (Text, image, audio, video, message)

Message Transfer Agent

The message transfer system is connected with relaying messages from originator to the recipient.

- **SMTP(Simple Mail Transfer Protocol)**

SMTP is the standard protocol for transferring mail messages between hosts in the TCP/IP suite; it is defined in RFC821. The messages transferred by SMTP follow the format of RFC822. SMTP is not concerned with the format or content of messages themselves with two exceptions:

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

SMTP uses information written on envelope of the mail (message header) but does not look at the contents (message body) of the envelope.
The SMTP can be used only to send messages that are composed using ASCII character set. MIME can be used to exchange email messages containing non-textual such as graphic, sound and other multimedia files. The MIME encodes these files in a textual form that can be sent using the SMTP.

Final Delivery

Many companies have one or more email servers that can be and receive email. To send or receive messages, a PC must talk to an email server using some kind of delivery protocol.

4.7 POP3 (Post Office Protocol)

- Simple protocol for fetching email from remote mailbox.
- It is defined in RFC1225.
- It has commands for log in, log out, fetch messages and delete messages.
- POP3 is used to fetch email from the remote mailbox and store it on the user's local machine to be read later.
- The protocol itself consists of ASCII text.

4.8 IMAP (INTERACTIVE MAIL ACCESS PROTOCOL)

- Sophisticated delivery protocol defined in RFC 1064.
- IMAP does not copy email to user's personal machine but the email server maintains a central repository that can be accessed from any machine.
- IMAP has the ability mail not by arrival number but using but by using attributes.

4.9 DMSP (DISTRIBUTED MAIL SYSTEM PROTOCOL)

- A part of PCMAIL system and defined in RFC 1056
- It does not assume that all email is on one server (as do POP3 and IMAP). It allows users to download email from the server to a workstation, PC or laptop and then disconnect.
- The email can be read and answered while disconnected. When connection occurs later, email is transferred and the system is re-synchronized.

4.10 LMR (LAST MINTUE REVISION)

- The session layer establishes, maintains and synchronous dialogs between nodes.
- Flow and error control in the session layer use synchronous points, which are reference point introduced into the data.
- The presentation layer handles translation, encryption, authentication and compression.
- Encryption transforms the original message into an resulting unintelligible message.
- Decryption transforms an intentionally unintelligible message (cipher text) in to meaningful information.
- Encryption/ Decryption methods can be broadly classified into the conventionally methods and the public key methods. Conventional methods include character level encryption and Bit Encryption.
- Substitution and transposition encryption are character level encryption methods.
- Bit – level encryption methods include encoding / decoding, permutation, substitution, product, exclusive OR and rotation.
- DES is a bit level encryption method.
- In conventional encryption, the encryption algorithm is known by everyone but the key is secret expect to the sender and receives.
- In public key encryption, both the encryption algorithm and the encryption key are known to everyone but the decryption key is known only the receiver.
- Digital signature is one of the authentication methods.
- The goal of data compression is to reduce the number of transmitted bits.
- Data compression methods are either lossless (all information is recoverable) or lossy (some information is lost).
- Five standard application protocols are:
  - **i)** Mail handling system (MHS) – the protocol for electronic mail and store – and forward handling.
  - **ii)** File transfer, access and management (FTAM)- transfers, accesses and manages files. FTAM uses virtual files.
  - **iii)** Virtual terminal (V.T.) – allows dissimilar terminals or machines to communicate with one another.

iv) Directory service (DS) – an application program that allows users access to database.

v) Common management information protocols (CMIP) – implements and OSI management service.

- Changing the internal representation of data from one to another is called translation.
- Services of the Session Layer:
  i) To co- ordinate connection and disconnection of dialogs between applications.
  ii) To provide synchronous points for data exchange.
  iii) To co- ordinate who sends when.
  iv) To ensure that the data exchange is complete before the Session closes.
- MHS is the OSI protocol that underlines electronic mail and store and forward handling. It is derived from ITU – T X.400 series.
- A virtual file store is non implementation specific model for files, and database that can be used as an intermediary for file transfer access and management.
- Per content attributes are those related to the contents of the file. Per – access attributes are security measures that control access to file.
- The information contained in the directory is called the directory information base(DIB).
- Internal representation of a piece of information might vary from one machine to the other. Translation handles this problem, so that receiving machine can understand the message sent by the transmitter.
- Encryption means that the sender transforms the original information to another from and sends the resulting unintelligible message out over the network.
- Decryption reverses the encryption process in order to transform the message back to its original form.
- Authentication means verifying the identity of the sender. In other words authentication verifies that a message is coming from, an authentic sender

GATE QUESTIONS

Q.1 Which one of the following statements is FALSE?

a) Packet switching leads to better utilization of bandwidth resources than circuit switching
b) Packet switching results in less variation in delay than circuit switching
c) Packet switching requires more per-packet processing than circuit switching
d) Packet switching can lead to reordering unlike in circuit switching.

[GATE-2004]

Q.2 A sender is employing public key cryptography to send a secret message to a receiver. Which one of the following statements is TRUE?

a) Sender encrypts using receiver's public key
b) Sender encrypts using his own public key
c) Receiver decrypts using sender's public key
d) Receiver decrypts using his own public key

[GATE-2004]

Q.3 Consider the three commands LPROMPT, HEAD and RCPT. Which of the following options indicate a correct association of these commands with protocols where these are used?

a) HTTP, SMTP, FTP
b) FTP, HTTP, SMTP
c) HTTP, FTP, SMTP
d) SMTP, HTTP, FTP

[GATE-2005]

Q.4 Trace route reports a possible route that is taken by packets moving from some host A to some other host B. Which of the following options represents the technique used by tracerout to identify these hosts?

a) By progressively querying routers about the next router on the path to B using ICMP packets, starting with the first router
b) By requiring each router to append t he address to the ICMP packet as it is forwarded to B. The list of all routers en-route to B is returned by B in an ICMP reply packet
c) By ensuring that an ICMP reply packet is returned to a by e ach router en-route to B, in the ascending order of their hop distance from A
d) By locally computing the shortest path from A to B

[GATE-2005]

Q.5 Count to infinity is problem associated with

a) Link state routing protocol.
b) Distance vector routing protocol
c) DNS while resolving host name.
d) TCP for congestion control.

[GATE-2005]

Q.6 Assume that "host 1. mydomain.dom" has an IP address of 145.128.16.8. Which of the following options would be most appropriate as a subsequence of steps in performing the reverse lookup of 1455.128.16.8? In the following options "NS" is an abbreviation of "nameserver".

a) Query a NS for the root domain and then NS for the "dom" domains
b) Directly query a NS for ``dom" and then a NS for "mydomain.com" domains

c) Query a NS for in-addr.addr.arpa and then a NS for 128.145.in-addr.arpa domains
d) Directly query a NS for 145.in-addr.arpa and then a NS for 128.145.in-addr.arpa domains

[GATE-2005]

Q.7 Suppose that two parties A and B wish to setup a common secret key (D-H key) between themselves using the Diffie-Hellman key exchange technique. They agree on 7 as the modulus and 3 as the primitive root. Party A chooses 2 and party B chooses 5 as their respective secrets. Their D-H key is

a) 3 b) 4
c) 5 d) 6

[GATE-2005]

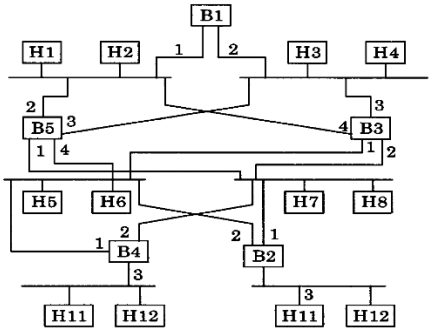
Q.8 HELO and PORT, respectively, are commands from the protocols

a) FTP and HTTP
b) TLENET and POP3
c) HTTP and TELNET
d) SMTP and FTP

[GATE-2006]

Linked Data for Q.9 and Q.10

Consider the diagram shown below where a number of LANs are connected by (transparent) bridges. In order to avoid packets looping through circuits in the graph, the bridges organize themselves in a spanning tree. First, the root bridge is identified as the bridge with the least serial number. Next, the root sends out (one or more)data units to enable the setting up of the spanning tree of shortest paths from the root bridge to each bridge.



Each bridge identifies a port (the root port) through which it will forward frames to the root bridge. Port conflicts are always resolved in favour of the port with the lower index value. When there is a possibility of multiple bridges forwarding to the same LAN (but not through the root port), ties are broken as follows: bridges closest to the root get preference and between such bridges, the one with the lowest serial number is preferred.

Q.9 For the given connection of LANs by bridges, which one of the following choices represents the depth first traversal of the spanning tree of bridges?

a)B1, B5 B3, B4, B2
b)B1, B3, B5, B2, B4
c)B1, B5, B2, B3, B4
d)B1, B3, B4, B5, B2

[GATE-2006]

Q.10 Consider the correct spanning tree for the previous question. Let host H1 send out a broadcast ping packet. Which of the following options represents the correct forwarding table on B3?

(a)

Hosts	Port
H1, H2, H3, H4	3
H5, H6, H9, H10	1
H7, H8, H11, H12	2

(b)

Hosts	Port
H1, H2	3
H3, H4	1
H5, H6	4
H7, H8, H9, H10	2
H11, H12	

(c)

Hosts	Port
H3, H4	3
H5,H6,H9,H10	1
H1, H2	4
H7, H8, H11, H12	2

(d)

Hosts	Port
H1, H2, H3, H4	3

H5, H7, H9, H10	1
H7, H8, H11, H12	4

[GATE-2006]

Q.11 Which one of the following uses UDP as the transport protocol?

a)HTTP b)Telnet
c)DNS d)SMTP

[GATE-2007]

Q.12 Consider the following two statements:

(i) A hash function (these are often used for computing digital signatures) is an injective function.

(ii) An encryption technique such as DES performs a permutation on the elements of its input alphabet.

Which one of the following options is valid for the above two statements?

a) Both are false
b) Statement (i) is true and the other is false
c) Statement (ii) is true and the other is false
d) Both are true

[GATE-2007]

Q.13 The minimum positive integer p such that 3^p modulo 17 = 1 is

a)5 b)8
c)12 d)16

[GATE-2007]

Q.14 Exponentiation is a heavily used operation in public key cryptography. Which of the following options is the tightest upper bound on the number of multiplications required to compute b^n modulo m, $0 \le b,\ n \le m$?

a)O (log n) b)O($\sqrt{n}$)
c)O (n/log n) d)O(n)

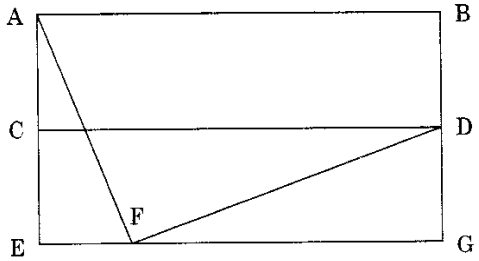
[GATE-2007]

Q.15 A firewall is to be configured to allow hosts in a private network to freely open TCP connections and send packets on open connections. However, it will only allow external hosts to send packets on existing open TCP connections or connections that are being opened (by internal hosts) but not allow them to open TCP connections to hosts in the private network. To achieve this the minimum capability of the firewall should be that of

a) A combinational circuit
b) A finite automaton
c) A pushdown automaton with one stack
d) A pushdown automaton with two stacks

[GATE-2007]

Q.16 For the network given in the figure below, thee routing tables of the four nodes A, E, D and G are shown. Suppose that F has estimated its delay to its neighbours, A, E,D and G as 8, 10, 12 and 6 msecs respectively and updates its routing table using distance vector routing technique.



Routing Table of A	
A	0
B	40
C	14
D	17
E	21
F	9
G	24

Routing Table of E	
A	24
B	27
C	7
D	20
E	0
F	11
G	22

Routing Table of D	
A	20
B	8
C	30
D	0
E	14
F	7
G	22

Routing Table of G	
A	21
B	24
C	22
D	19
E	22
F	10
G	0

a)

A	8
B	20
C	17
D	12
E	10
F	0
G	6

b)

A	21
B	8
C	7
D	19
E	14
F	0
G	22

c)

A	8
B	20
C	17
D	12
E	10
F	16
G	6

d)

A	8
B	8
C	7
D	12
E	10
F	0
G	6

[GATE-2007]

Q.17 A group of 15 routers are interconnected in a centralized complete binary tree with a router at each tree node. Router communicates with router j by sending a message to the root of the tree. The root then sends t he message back down to router j. The mean number of hops per message, assuming all possible router pairs are equally likely is

a) 3 b) 4.26
c) 4.53 d) 5.26

[GATE-2007]

Q.18 Consider the following clauses:

i) Not inherently suitable for client authentication
ii) Not a state sensitive protocol.
iii) Must be operated with more than one server.
iv) Suitable for structured message organization.
v) May need two ports on the serve side for proper operations.

The option that has the maximum number of correct matches is

a) IMAP-(i), FTP-(ii), HTTP-(iii), DNS-(iv), POP3-(v)
b) FTP-(i), POP3-(ii), SMTP-(iii), HTTP- (iv), IMAP-(v)
c) POP3-(i), SMTP-(ii), DNS-(iii), IMAP-(iv), IMAP-(iv), HTTP-(v)
d) SMTP-(i) HTTP-(ii), IMAP-(iii), DNS-(iv), FTP-(v)

[GATE-2007]

Q.19 Match the following:

P. SMTP	1. Application layer
Q. BGP	2. Transport layer
R. TCP	3. Data link layer
S. PPP	4. Network layer
	5. Physical layer

Codes:

a)P-2,Q-1,R-3, S-5 b)P-1, Q-4, R-2, S-3
c)P-1,Q-4,R-2,S-5 d)P-2, Q-4, R-1, S-3

[GATE-2007]

Q.20 Two popular routing algorithm ms are Distance Vector (DV) and Link State (LS) routing. Which of the following are true?

S1:Count to infinity is a problem only with DV and not LS routing

S2:In LS, the shortest path algorithm is run only at one node
S3: In Dv, the shortest path algorithm is run only at one node
S4: DV requires lesser number of network messages than LS

a)S1, S2 and S4 b)S2 and S3 only
c)S1, S2 and S3 only d)S1 and S4 only

[GATE-2008]

Q.21 The total number of keys required for a setoff n individuals to be able to communicate with each other using secret key and public key cryptosystems, respectively are:

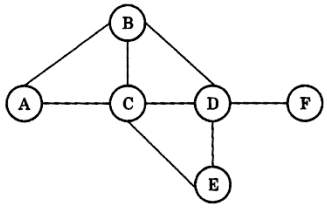
a) n(n-1) and 2n
b)2n and ((n(n-1))/2)
c)((n(n-1))/2) and 2n
d)((n(n-1))/2) and n

[GATE-2008]

Linked Answer Questions 22 and 23

Consider a simple graph with unit edge costs. Each node in the graph represents a router. Each node maintains a routing table indicating the next hop router to be used to relay a packetto its destination and the cost of the path to the destination through that router. Initially, the routing table is empty. The routing table is synchronously updated as follows. In each updated interval, three tasks are performed.

i) A node determines whether its neighbours in the graph are accessible. If so, it sets the tentative cost to each accessible neighbor as 1. Otherwise, the cost is set to ∞.
ii) From each accessible neighbor, it gets the cost to relay to other nodes via that neighbor (as the next hop).
iii) Each node updates its routing table based on the information received in the previous two steps by choosing the minimum cost.



Q.22 For the graph given above, possible routing tables for various nodes after they have stabilized are shown in the following options. Identify the correct table.

a)

Table for node A		
A	-	-
B	B	1
C	C	1
D	B	3
E	C	3
F	C	4

b)

Table for node C		
A	A	1
B	B	1
C	-	-
D	D	1
E	E	1
F	E	3

c)

Table for node B		
A	A	1
B	-	-
C	C	1
D	D	1
E	C	2
F	D	2

d)

Table for node D		
A	B	3
B	B	1
C	C	1
D	-	-
E	E	1
F	F	1

[GATE-2005]

Q.23 Continuing from the earlier problem, suppose at some time t, when the costs have stabilized, node A goes down. The cost from node F to node A at time (t + 100) is:

a)> 100 but finite b)∞
c)3 d)>3 and ≤ 100

[GATE-2005]

Q.24 A computer on a10 Mbps network is regulated by a token bucket. The token bucket is filled at a rate of 2 Mbps. It is initially filled to capacity

with 16 Megabits. What is the maximum duration for which the computer can transmit at the full 10 Mbps?

a)1.6 seconds b)2 seconds
c)5 seconds d)8 seconds

[GATE-2008]

Q.25 In the RSA public key cryptosystem, the private and public keys are (e, n) and (d, n) respectively, where n = p*q and p and q are large primes. Besides, n is public and p and q are private. Let M be an integer such that 0 < M < n and Ø(n)=(p-1)(Q.1). Now consider the following equations.

1. $M' = M^e \bmod n$
   $M = (M')^d \bmod n$
2. $ed = 1 \bmod n$
3. $ed = 1 \bmod Ø\ n$
4. $M' = M^e \bmod Ø n$
   $M = (M')^d \bmod Ø n$

Which of the above equations correctly represent RSA cryptosystem?

a) 1 and 2 b) 1 and 3
c) 2 and 4 d) 3 and 4

[GATE-2009]

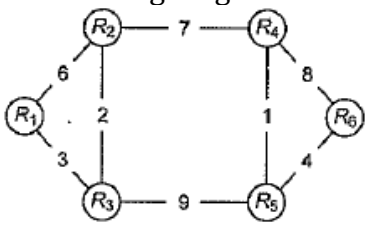
Q.26 Which one of the following is not a client-server application?

a)Internet chat b)Web browsing
c)E-mail d)Ping

[GATE-2010]

Statements for Linked Answer Questions 27 and 28

Consider a network with 6 routers R_1 to R_6 connected with links having weights as shown in the following diagram.



Q.27 All the routers use the distance vector based routing algorithm to update their routing tables. Each router starts with its routing table initialized to contain an entry for each neighbour with the weight of the respective connecting link. After all the routing tables stabilize, how many links in the network will never be used for carrying any data?

a) 4 b) 3
c) 2 d) 1

[GATE-2010]

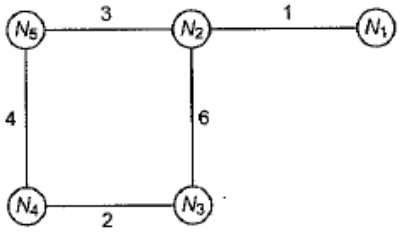
Q.28 Suppose the weights of all unused links in the previous question are changed to 2 and the distance vector algorithm is used again until all routing tables stabilize. How many links will now remain unused?

a) 0 b) 1
c) 2 d) 3

[GATE-2010]

Statements for Linked Answer Questions 29 and 30

Consider a network with five nodes, N_1 to N_5, as shown below:



The network uses a distance vector routing protocol. Once tine routes have stabilized, the distance vectors at different nodes are as following. Each distance vector is the distance of the best known path at that instance to nodes, N_1 to N_5, where the distance to itself is 0. Also, all links are symmetric and the cost is identical in both directions. In each round, all nodes exchange their distance vectors with their respective neighbours, then all nodes update their distance vectors. In between two rounds, any change in cost of a link will cause the

two incident nodes to change only that entry in their distance vectors.

Q.29 The cost of link N_2-N_3 reduces to 2 in (both directions). After the next round of updates, what will be the new distance vector at node N_3?

a) 3, 2, 0, 2, 5 b) 3, 2, 0, 2, 6
c) 7, 2, 0, 2, 5 d) 7, 2, 0, 2, 6

[GATE-2011]

Q.30 After the update in the previous question, the link N_1-N_2 goes down. N_2 will reflect this change immediately in its distance vector as cost ∞. After the next round of update, what will be the cost to N_1 in the distance vector of N_3?

a) 3 b) 9
c) 10 d) ∞

[GATE-2011]

Q.31 Consider the different activities related to email:

M_1: Send an email from a mail client to a mail server.

M_2: Download an email from mailbox server to a mail client.

M_3: Checking email in a web browser.

Which is the application level protocol used in each activity?

a) m_1 : HTTP m_2 : SMTP m_3 : POP
b) m_1 : SMTP m_2 : FTP m_3 : HTTP
c) m_1 : SMTP m_2 : POP m_3 : HTTP
d) m_1 : POP m_2 : SMTP m_3 : IMAP

[GATE-2011]

Q.32 The Protocol Data Unit (PDU) for the application layer in the Internet stack is

a)Segment b)Datagram
c)Message d)Frame

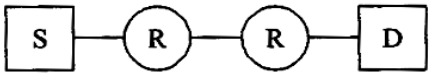
[GATE-2012]

Q.33 The transport layer protocols used for real time multimedia, file transfer, DNS and email respectively are

a)TCP, UDP, UDP and TCP
b)UDP, TCP, TCP, and TCP
c)UDP, TCP, UDP and TCP
d)TCP, UDP, TCP and UDP

[GATE-2013]

Q.34 Assume that source S and destination D are connected through two intermediate routers labels R. Determine how many times each packet has to visit the network layer and the data link layer during a transmission form S to D.



a) Network layer-4 times and Data link layer -4 times
b) Network layer-4 times and Data link layer -3 times
c) Network layer-4 times and Data link layer -6 times
d) Network layer-2 times and Data link layer -6 times

[GATE-2013]

Q.35 Using public key cryptography, X adds a digital signature σ to message M, encrypts <M, σ >, and sends it to γ, where it is decrypted. Which one of the following sequences of keys is used for the operations?

a) Encryptions X's private key followed by Y's private key; Decryption X's public key followed by Y's public
b) Encryption X's private key followed by Y's public key; Decryption X's public key followed by Y's private key
c) Encryption X's public key followed by Y's private key; Decryption Y' spublic key followed by X's private key
d) Encryption X's private key followed by Y's public key; Decryption Y's private key followed by X's public key

[GATE-2013]

Q.36 Consider the following three statements about link state and

distance vector routing protocols, for a large network with 500 network nodes and 4000 links.

S1: The computational overhead in link state protocols is higher than in distance vector protocols.

S2: A distance vector protocol (with split horizon) avoids persistent routing loops, but not a link state protocol.

S3: After a topology change, a link state protocol will converge faster than a distance vector protocol.

Which one of the following is correct about S1, S2, and S3?

a) S1, S2, and S3 are all true.
b) S1, S2, and S3 are all false.
c) S1 and S2 are true, but S3 is false.
d) S1 and S3 are true, but S2 is false.

[GATE-2014]

Q.37 Which of the following are used to generate a message digest by the network security protocols?

(P) RSA (Q) SHA-1
(R) DES (S) MD5

a)P and R only b)Q and R only
c)Q and S only d)R and S only

[GATE-2014]

Q.38 An IP machine Q has a path to another IP machine H via three IP routers R1, R2, and R3.

Q—Ra—R2—R3—H

H acts as an HTTP server, and Q connects to H via HTTP and downloads a file. Session layer encryption is used, with DES as the shared key encryption protocol. Consider the following four pieces of information:

[I1] The URL of the file downloaded by Q
[I2] The TCP port numbers t Q and H
[I3] The IP addresses of Q and H
[I4] The link layer addresses of Q and H

Which of I1, I2, I3, and I4 can an intruder learn through sniffing at R2 alone?

a)Only I1 and I2 b)Only I1
c)Only I2 and I3 d)Only I3 and I4

[GATE-2014]

Q.39 Which one of the following is TRUE about the interior gateway routing protocols—Routing Information Protocol [RIP] and Open Shortest Path First [OSPF]?

a) RIP uses distance vector routing and OSPF uses link state routing
b) OSPF uses distance vector routing and RIP uses link state routing
c) Both RIP and OSPF uses link state routing
d) Both RIP and OSPF uses distance vector routing.

[GATE–2014]

Q.40 In one of the pair s of protocols given below, both the protocols can use multiple TCP connections between the same client and the server. Which one is that?

a)HTTP, FTP b)HTTP,TELNET
c)FTP, SMTP d)HTTP, SMTP

[GATE–2015]

Q.41 Suppose that everyone in a group of N people wants to communicate secretly with (N–1) others using symmetric key cryptographic system. The communication between any two persons should not be decodable by the others in the group. The number of keys required in the system as a whole to satisfy the confidentiality requirement is

a) 2N b) N(N – 1)
c) N(N – 1)/2 d) (N – 1)2

[GATE–2015]

Q.42 The value of the expression 13^{99} (mod 17), in the range 0 to 16, is _____.

[GATE–2016]

Q.43 For the IEEE 802.11 MAC protocol for wireless communication, which

of the following statements is/are TRUE?

I. At least three non-overlapping channels are available for transmission.

II. The RTS-CTS mechanism is used for collision detection.

III. Unicast frames are ACKed

a)All I, II, and III b)I and III only

c)II and III only d)II only

[GATE–2016]

Q.44 Consider that B wants to send a message m that is digitally signed to A. Let the pair of private and public keys for A and B be denoted by K_x^- and K_x^+ for x =A,B respectively. Let Kx(m) represent the operation of encrypting m with a key Kx and H(m) represent the message digest. Which one of the following indicates the **CORRECT** way of sending the message m along with the digital signature to A?

a)$\{m, K_B^+ (H(m))$ b)$\{m, K_B^- (H(m))\}$

c) $\{m, K_A^- (H(m))\}$ d)$\{m, K_A^+ (m)\}$

[GATE–2016]

Q.45 Anarkali digitally signs a message and sends it to Salim. Verification of the signature by Salim requires

a) Anarkali's public key

b) Salim's public key

c) Salim's private key

d) Anarkali's private key

[GATE–2016]

Q.46 Identify the correct sequence in which the following packets are transmitted on the network by a host when a browser requests a webpage from a remote server, assuming that the host has just been restarted.

a) HTTP GET request, DNS query, TCP SYN

b) DNS query, HTTP GET request, TCP SYN

c) DNS query, TCP SYN, HTTP GET request

d) TCP SYN, DNS query, HTTP GET request

[GATE–2016]

Q.47 Which one of the following protocol is not used to resolve one form of address to another one?

a) DNS b) ARP

c) DHCP d) RARP

[GATE–2016]

Q.48 Which of the following is/are example(s) of state full application layer protocols?

(i) HTTP (ii) FTP

(iii) TCP (iv) POP3

a) (i) and (ii) only

b)(ii)and (iii) only

c) (ii) and (iv) only

d) (iv) only

[GATE–2016]

Q.49 Consider the following statements about the routing protocols, Routing Information Protocol (RIP) and Open Shortest Path First (OSPF) in an IPv4 network.

I: RIP uses distance vector routing

II: RIP packets are sent using UDP

III: OSPF packets are sent using TCP

IV: OSPF operation is based on link-state routing. Which of the statements above are **CORRECT**?

a) I and IV only b) I, II and III only

c) I, II and IV only d) II, III and IV only

[GATE–2017]

Q.50 A sender S sender a message m to receiver R. which is the digitally signed by S with its private key .In this scenario, one or more of the following security violations can take place.

I. S can launch a birthday attack to replace m with a fraudulent message.

II. A third party attacker can launch a birthday attack to replace m with a fraudulent message.
III. R can launch a birthday attack to replace m with a fraudulent message.

Which of the following are possible security violations?

a)I and II only b)I only
c)II only d)II and III only

[GATE–2017]

Q.51 In a RSA cryptosystem, a participant A uses two prime numbers p = 13 and q = 17 to generate her public and private keys. If the public key of A is 35, then the private key of A is _____.

[GATE–2017]

ANSWER KEY:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
B	A	B	A	B	C	B	D	A	A	C	C	D	A	D
16	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**26**	**27**	**28**	**29**	**30**
A		D	B	D	C	C	A	B	B	D	C	B	A	C
31	**32**	**33**	**34**	**35**	**36**	**37**	**38**	**39**	**40**	**41**	**42**	**43**	**44**	**45**
C	C	C	C	D	D	C	C	A	A	C	4	B	B	A
46	**47**	**48**	**49**	**50**	**51**									
C	C	C	C	B	11									

EXPLANATIONS

Q.1 **(c)**

Q.2 **(a)**

In public key cryptography if sender used receiver's public key for encryption then the decryption of message I s possible only by using private key of receiver.

Hence 1st is true and remaining are false.

If sender encrypts using his own public key then no one except the sender can decrypt it and only sender knows his private key on one else.

Q.3 **(a)**

RCPT: Recipient to, As the name suggest it is used in SMTP (Simple Mail Transfer protocol).

HEAD: This is used in HTTP to get the meta-information, to decide the category of packet.

Prompt: Turns off prompting for individual files when using the mget or mput commands.

Q.4 **(a)**

Traceroute works by sending packets with gradually increasing TTL value, starting with TTL value of 1.

The first router receives the packet, decrements the TTL value and drops the packet because it then has TTL value zero.

The router sends an ICMP Time Exceeded message back to the source.

The next st of packets are given a TTL value of 2, so the first router forwards the packet s, but the second router drops them and replies with CIMP Time Exceeded.

Proceeding in this way, traceroute used the returned ICMP Time Exceeded messages to build a list of routers that packets traverse, until the destination is reached and returns an ICMP Echo Reply message.

Q.5 **(b)**

In distance vector routing the count-to-infinity problem happens when a router is unable to reach an adjoining network. A second router, 1 hop away from the first route, thinks that the unreachable network is 2 hops a way. Meanwhile, the first router then updates its records to say it is 3 hops away from the unreachable network based on the fact it is 1hop from t he second router, which says it is 2 hops from the unreachable network. The routers continue incrementing their hop count until the maximum (15, ``infinity''), is reached.

Q.6 **(c)**

The appropriate sequences of steps performing the reverse lookup of 145.128.16.8 are:

Step-1: Query a Name server for in-addr.arpa. Because information regarding the IP address 145.128.16.8 is located at domain name.

145.128.16.8 in -addr.arpa.

Step-2: Second setup is request Name server for128.45 in-addr.arpa.domain. This is because the query is for PTR records. The resolver reverses the address and appends the in-addr.arpa to the end of the reversed address. This forms the fully qualified domain name for which to be searched is reverse lookup zone.

Q.7 **(b)**

D-H key : $g^{AB} \bmod n = 3^{2\times5} \bmod 7 = 3^{10} \bmod 7 = 4$.

Q.8 (d)

HELO: Initiates a conversation with the mail server. When using this command your can specify your domain name so that the mail server known who you are. The PORT command is sent by an FTP client to establish a secondary connection (address and port) for data to travel over.

Q.9 (c)

B1-B5-B2-B3-B4

Q.10 (a)

Use spanning tree generated in previous question.

Q.11 (c)

Domain Name System (DNS) maps a name onto an IP address, an application program calls a library procedure called the resolver, passing name as a parameter. The resolver sends a UDP packet to a load DNS server, which then looks up the name and returns the IP address to the resolver, which then returns it to caller. So DNS used transport layer protocol UDP.

Q.12 (c)

During hash generation more than one message may generate the same HASH value. So hash function is Many-to-One.

Q.13 (d)

By Fermat's theorem, 3^{17-1} modulo 17=1. So p = 16.

Q.14 (a)

One can compute b, b^2, b^4, b^8,... and combine them to the extent possible.

This means a continuous division of n by 2 and so gives a complexity of O (log n).

Q.15 (d)

A pushdown automata with two stacks can simulate a general purpose computer.

The number of internal hosts and external hosts is not bounded, and we need comparison so (a) and (b) cannot help as they deal with bounded numbers.

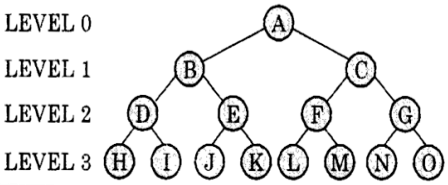
Q.16 (a)

Based on the given options only (a) matches correct.

	A	B	C	D	E	F	G
F via A	8	48	22	25	29	0	32
F via B							
F via C							
F via D	32	20	42	12	226	0	34
F via E	34	37	17	30	10	0	32
F via G	27	30	28	25	28	0	6
Min values	≤8	≤20	≤17	≤12	≤10	0	≤6

Q.17 (c)

Consider Complete tree:



Forward packet to the router at Level 3: Total 6 hops are required if A wants to communicate with any level 3 node. Similarly, 5 hops are required if H wants to communicate with any level 2 node, 4 hops are required if H wants to communicate with any level 1 node and 3 hops are required if H wants to communicate with any level 0 node.

Hops required if H wants to communicates with all other nodes

$= (8-1)*6+4*5+2*4+1*3 = 73.$

If all 8 nodes of level 3 communicates with all other nodes then hops required =73*8=584. Similarly. Hops required if D wants to communicates with all other nodes

$= 8*5+(4-1)*4+2*3+1*2 = 60.$

If all 4 nodes of level 2 communicates with all other nodes then hops required $=60*4=240$.
Hops required if B wants to communicates with all other nodes
$=8*4+4*3+(2-1)*2+1*1=47$.

If all 2 nodes of level 1 communicates with all other nodes then hops required $=47*2=94$.
Hops required if A wants to communicates with all other nodes
$=8*3+4*2+2*1=34$.
Total hops required when all nodes communicate with all other nodes
$=584+240+94+34=952$.
Total number of messages
$=2^{*15}C_2=2*(15*14/2)=2*105=210$

(Here 2 is multiplied with $^{15}C_2$, because in communication between A and B, A sends message to B and B sends message to A)
Mean number of hops per message
=952/210 = 4.53

Q.18 (d)

IMAP: It distributes mail boxes across multiple servers.
FTP : Requires two ports: 20 and 21 for FTP- data and FTP-control respectively.
HTTP: HTTP is stateless protocol. Hence not a state sensitive protocol.
DNS : This protocol maintains it's database is structured an hierarchial manner.
SMTP: Intersect standard for e-mail transmission and not suitable for client server communication.

Q.19 (b)

P. SMTP = Application Layer protocol
Q. BGP = Network Layer protocol
R. TCP = Transport Layer protocol
S. PPP = Data Link Layer protocol

Q.20 (d)

Count to infinity problem accurs only in distance vector algorithm.
Hence S1 is true.
In link state we use flooding to share updates hence S4 is true.
S2 and S3 are both false because routing algorithm need to be executed at each and every node.

Q.21 (c)

For private key cryptography for communication between each pair of individuals on secret key will be required.
If an individual wants to communicate with other n-1 individuals he should have n-1 secret keys, so the total number of secret keys for private encryption is $(n*(n-1))/2$.
For public key encryption each individual needs to have a public and private key, the total keys required in 2*n.

Q.22 (c)

Q.23 (b)

Q.24 (b)

Data transfer rate of token bucket = 10 Mbps
Initially filled to capacity 16 Megabits Maximum duration=16/18 = 2 seconds

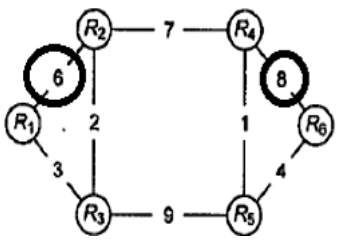
Q.25 (b)

The RSA laboratories define RSA cryptosystems as the following
The RSA cryptosystem is a public-key cryptosystem that offers both encryption and digital signatures (authentication). Ronald Rivest, Adi Shamir and Leonard Adleman developed the RSA system in 1977; RSA stands for the first letter in each of its, inventors' last 'names. The RSA algorithm works as follows: take two large primes, p and q, and compute their product n = pq, n is called the modulus. Choose a number,

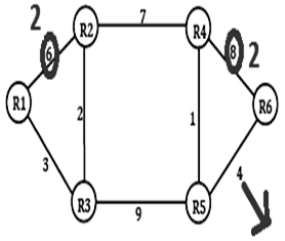
e, less than n and relatively prime to (p-1) (q-1), which means e and (p-1) (q-1) have no common factors except 1. Find another number d such that (ed-1) is divisible by (p-1) (q-1). The values e and d are called the public and private exponents, respectively. The public key is the pair (n, e); the private key is (n, d). The factors p and q may be destroyed or kept with the private key.
It is currently difficult to obtain the private key d from the public key (n, e). However, if one could factor n into p and q, then one could obtain the private key d. Thus, the security of the RSA system is based on the assumption that factoring is difficult. The RSA cryptosystem in the problem is correctly represented by the equation 1 and 3.

Q.26 (d)
Internet chat, web browsing and E-mail all are client- server application. Ping is a utility. It is mainly used to check the connection between two computers, there is a chance both are client or one is client and another server. In chat system first user authentication required and it requires server.

Q.27 (c)
After routing table stability, only 2 link will be unused "R1→R2" and "R4→R6"

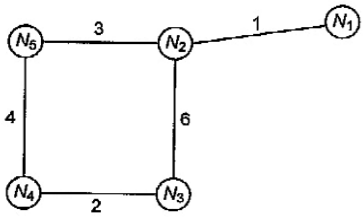


Q.28 (b)
After changing the weights of unused links R1→R2 and R4→R6 to 2. Then the no of unused links are only one [R5 →R6]



Link R5-R6 will be used

Q.29 (a)



Distance vector for N_3 will be
N_3 : (N_1, N_2, N_3, N_4, N_5)
N_3 : (3, 2, 0, 2, 5)

Q.30 (c)
In the next ground, N3 will receive distance from N2 to N1 as infinite. It will receive distance from N4 to N1 as 8. So it will update distance to N1 as 8+2 =10.

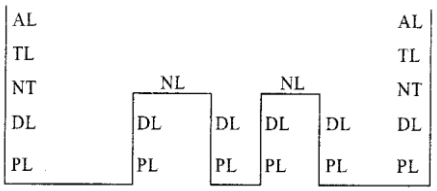
Q.31 (c)
Sending an email will be done through user agent and message transfer agent by SMTP, downloading an email from mail box is done through POP, checking email in a web browser is done through HTTP.

Q.32 (c)
Message ⟶ Application layer
Segment ⟶ Transport layer
Datagram ⟶ Network layer
Frame ⟶ Data link layer

Q.33 (c)
UDP: Transport layer protocol which is unreliable but fast.
TCP: Transport layer connection oriented protocol which is secure and reliable but comparatively slow.
So for real time multimedia we need fast processing so UDP is suitable for it.

For file transfer we need security so TCP is suitable for file transfer.
DNS always use UDP
For email we need security so used TCP.
Option (c) is correct.

Q.34 (c)
In the layered architecture sender and receiver uses all the 5 layers and router do procession upto the network layer.



So network layer is visited 4 times and data link

Q.35 (d)
As stated X adds a digital signature σ to message M encrypts < M, σ > and transmits it to Y. In order to the make sure that Y receives the message and is able to decrypt it the following sequence and is able to decrypt it the following sequence of keys is used for the operations.
(D) Encryption X's private key followed by Y's public key the message needs to be encrypted by the sender's private key and receiver's public key in order to maintain authenticity and confidentiality.
Decryption Y's private key followed by X's public key on receiving the encrypted message, receiver Y will have to decrypt it using his own private key and by using sender X's public key.

Q.36 (d)
S1 is TRUE: Processing time in link state protocol in high because of link state database.
S2 is **FALSE:** Link state protocol is a loop free protocol avoids persistent routing loops.
S3 is **TRUE**: Link state protocol is fast convergence because of link state database i.e., it contains complete information of the network. This information is given to the router by the link state packets.

Q.37 (c)
SHA-1 and MD5 are used to generate a message digest.

Q.38 (c)
Given R_1,R_2 and R_3 are routers
At R_2 intruder can learn the TCP port numbers and IP address of Q and H.

Q.39 (a)
RIP Uses Distance Vector Routing and OSPF uses Link State Routing.

Q.40 (a)
HTTP and FTP protocols can use multiple TCP connections between the same client and the server. FTP used data and control connections used with two separate TCP connection.

Q.41 (c)
In Symmetric Key Cryptography, access of key is with both the parties. It implies every person needs to communicate N-1 other users using different keys i.e 1+2+3...N-2+N-1. This is like number of edges needed in a complete graph with N vertices is N(N-1)/2.

Q.42 (4)

$$13^{99} \bmod 17 \Rightarrow \left(13^3 \bmod 17\right)^{33}$$

$$\Rightarrow \left(4 \bmod 17\right)^{33}$$

$$\Rightarrow \left(4^3 \bmod 17\right)^{11}$$

$\Rightarrow \left(4^{11} \bmod 17\right)^3$

$\Rightarrow 4$

Q.43 (b)

RTS-CTS is used for collision avoidance but not for collision detection.

Q.44 (b)

The concept of digital signature.
Message is digested: h(m) and cryptographically protected with sender's private key to become sign and sent along with the message.

Q.45 (a)

Sign is sender's private key and the receiver side the verification is done with sender public key.

Q.46 (c)

The concept to be followed

Step 1:

The client(browser) initiates a DNS query for remote server. It may be that they already have this server in their DNS cache, in which case the client may simply send a TCP SYN directly to the application server.

Step 2:

The client will next send a connection request to the application server. This will be a TCP SYN packet, the first in the TCP three-way handshake.

Step 3:

Next, after the TCP connection has been established, the client will request data from the server. In the web-based application, the client performs an HTTP GET.

Q.47 (c)

Q.48 (c)

Q.49 (c)

RIP uses distance vector routing. OSPF uses link- state routing protocols. OSPF neither uses TCP nor UDP. [Link state packet should be given to all routers in subnet so it's not possible with TCP. These link state packets should be reliable at that same time which is not possible with UDP].

Q.50 (a)

Q.51 (11)

P = 13,q=17
n = p × q
=13×17=221
$\Phi(n)=(p-1) \times (q-1)$
=12×16=192
$(d \times e) \bmod \Phi(n)=1$
$(d \times 35) \bmod 192=1$
d=11

ASSIGNMENT QUESTIONS

Q.1 Protocols are
a) Agreements on how communication components and DTE's are to communicate
b) Logical communication channels used for transferring data
c) Physical communication used for transferring data
d) None of the above

Q.2 The method of communication in which transmission takes place in both directions, but only in one direction at a time is called
a) Simplex b) four wire circuit
c) Full duplex d) half duplex

Q.3 Error detection at the data link level is achieved by
a) bit stuffing
b) cyclic redundancy codes
c) Hamming codes
d) equalization

Q.4 Which of the following is a wrong example of a network layer?
a) Internet protocol (IP)-ARPANET
b) X.25 packet level protocol (PLP)-ISO
c) Source routing & domain USENET
d) X.25 level 2-ISO

Q.5 The topology with highest reliability is
a) bus topology b) star topology
c) ring topology d)mesh topology

Q.6 Baud means?
a) the number of bits transmitted per unit time
b) the number of bytes transmitted per unit time
c) the rate at which the signal changes
d) none of the above

Q.7 Star and stop bits are used in serial communication for
a) error detection
b) error correction
c) Synchronization
d) slowing down the communication

Q.8 Unmodulated signal coming from a transmitter is known as
a) Error signal
b) baseband signal
c) primary signal
d) none of the above

Q.9 Manchester code is a
a) BI-polar
b)non return to zero code
c) polar code
d) none of the above

Q.10 Pick the incorrect abatements.
a) Another name for primary/ secondary protocol is master /slave.
b) Peer to peer protocol provides equal status to all sites on the channel.
c) Priority, no –priority types come under master/slave protocol.
d) TDM is a primary/secondary non-priority system

Q.11 Pick the correct statement.
a) A switched circuit is a dial-up circuit that may encounter blockage (busy signal)
b) Non switched leased line supports higher data volume and quality than switched lines.
c) Non switched lines are expensive for high volume data.
d) Switched circuit provides time .

Q.12 Pick the incorrect statements that pertain to error retransmission used in continuous ARQ method.

a) Go-back-N method requires more storage at the receiving site.
b) Selective repeat involves complex login than Go-back-N.
c) Go-back-N has better line utilization
d) Selective Report has better line utilization.

Q.13 In the carrier sense network if the prevailing condition is a 'channel busy' then which of the Following are correct?
a) If the technique used is non-persistent than it result in randomized wait and sense
b) If the technique used is 1-parsistent than the channel is continually sense.
c) If the technique used is p-persistent than randomized retransmission is done.
d) If the method used is non-persistent then continuous sensing results.

Q.14 Which of the following are non-polling systems?
a) TDMA b) Stop and Wait
c) Xon/Xoff d) Continuous ARQ

Q.15 Pick the systems that can be used in both priority & non-priority modes.
a) TDM
b) Register insertion
c) Carrier sense systems
d) Token passing

Q.16 How many characters per sec (7 bits + 1 parity) can transmitted over 2400 bps line if transfer is synchronous (1 start and 1 stop bit)?
a)300 b) 240
c) 250 d) 275

Q.17 Match the Following

1. session layer	(i)connects DCE into physical channel
2. transport layer	(ii) provides end to end accountability
3. Application	(iii) provides organized means to exchange data Between users and (like synchronization Points)
4.MDI (medium Dependent Interface)	(iv) support an end user process and Performs Required file transfer.

a)1-(iii), 2-(iv), 3(ii), 4-(i)
b)1-(ii), 2-(ii), 3(iv), 4-(i)
c)1-(ii), 2-(iv), 3(i), 4-(iii)
d)1-(iv), 2-(iii), 3(ii), 4-(i)

Q.18 The Hamming distance between 001111 and 010011 is
a) 1 b) 2
c) 3 d) 4

Q.19 BSC Is a
a) Character oriented protocol
b) bit- oriented protocol
c) full-duplex protocol
d) help-duplex protocol

Q.20 HDLC is
a) Bit oriented
b) code transparent
c) Code dependent
d) none of the above

Q.21 Bit stuffing refers to
a) Inserting a '0' in user data stream to avoid ambiguity
b) Inserting a '0' in flag stream to avoid ambiguity
c) Appending a nibble to the flat sequence
d) Appending a nibble to the user data stream

Q.22 Choose the correct statement (S)
a) Baseband network used analog technology.
b) Baseband network is time Division multiplexed.
c) Broadband network used digital technology.
d) In broadband network, the career signal operates at lower Frequency.

Q.23 In Ethernet CSMS/CD, the sequence transmitted by media access management for collision handling is called as

a) Preamble b) post amble
c) jam d) none of the above

Q.24 Adaptive or dynamic directory used in packet routing changes
a) Within each user session
b) With each user session
c) at system generation time only
d) both (a) and (b)

Q.25 The method of network routing where every possible path between transmitting and receiving DTE is used is called
a) RANDOM routing
b) packet flooding
c) directory routing
d) message switching

Q.26 Which on the following network used dynamic or adaptive routing
a) TYMNET
b) ARPANET
c) SNA (ISBM's System Network Architecture)
d) Nome of the above

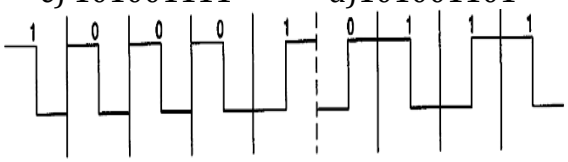
Q.27 The number of cross point needed for 10 lines in a cross point switch is full duplex in nature and there are no self-connection is
a) 100 b) 45
c) 50 d) 90

Q.28 A terminal multiplexer has six 1200 bps terminals and 'n' 300 bps terminals connected to it. The outgoing line is 9600 bps. What is the maximum Value of 'n'?
a) 4 b) 16
c) 8 d) 28

Q.29 The difference between a multiplexer and a statistical multiplexer is.
a) a multiplexer use TDM (time division multiplexing), While statistical a Multiplexer use the ALOHA protocol
b) a multiplexer often waste the output link capacity ,while statistical a multiplexer optimize its use.
c) Statistical a multiplexer need buffer s while multiplexers do not need buffers.
d) Multiplexers use the X.25 protocol, while statistical a multiplexers use the ALOHA protocol.

Q.30 A modem constellation diagram has data points at (0,1,) and (0,2) What type of modulation does the modem use?
a) Phase modulation
b) Amplitude modulation
c) Both (a) and (b)
d) None of the above

Q.31 Write the differential Manchester code for the given sketch
a) 111100101 b) 100010111
c) 101001111 d)101001101



Q.32 Maximum data rate of a channel for a noises 3-KHz binary channel is
a) 3000bps b) 6000 bps
c) 1500bps d) none of the above

Q.33 The maximum data rate of a 3000-Hz bandwidth and SNR of 30 dB is
a) 15,000 bps b) 60,000bps
c) 30,000bps d) 3,000bps

Q.34 In time division switches if each memory access takes 100 ns and one frame period is 125 μs, Then the maximum number of lines that can be supported is
a) 625 line b) 1250 line
c) 2300 line d) 318 line

Q.35 if the **bit** string 0111101111101111110 is subjected to bit stuffing for the flag string 01111110, the output string is
a) 011110111110011111010
b) 01111011111011111100

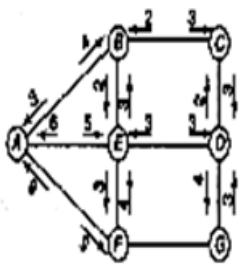
c) 01111011111011111010
d) 01111011111101111110

Q.36 End-to-end connectivity is provided from host-to host in
a) The network layer
b) The transport layer
c) The session layer
d) It is a combined functionality of the network and the data link later.

Q.37 Pick the correct statement
a) In connection-oriented service, the destination address is to be specified only During the setup.
b) Initial setup is not possible in connectionless service.
c) Packet sequencing is not guaranteed in connection-oriented service.
d) Initial setup is required for connectionless service.

The next 3 questions are based on the following diagram that represents shortest path adaptive routing.

FD	NN	OD
A		
B		
C		
D		
F		
G		



the final destination: NN is the next mode; OD is the overall delay.

Q.38 The entry for NN if FD is nod B is
a) E b) C
c) G d) None of the above

Q.39 The entry of OD for the above case is
a) 6 b) 14
c) 4 d) 3

Q.40 The OD if FD is node A is
a) 6 b) 9
c) 13 d) 7

Q.41 Pick the correct statements about flowing.
a) It is a type of isolated routing.
b) It is a method in which every incoming packet is sent out on every outgoing line except the one by which it arrived.
c) Flooding does not always select the shortest path
d) Selective flooding is a type in which the packets are sent to those line that are going approximately in the right direction.

Q.42 The parameter which is giving the probability of the transport layer itself spontaneously terminating a connection due to internal problems is called
a) Protection b) resilience
c)negotiation d) transfer failure

Q.43 The _____ measures the number of lost or garbled messages as a Fraction of the Total sent in the sampling period.
a) Residual Error rate
b) Transfer Failure Probability
c) Connection Release failure Probability
d) Connection establishment failure Probability

Q.44 In session layer, during data transfer,the data stream responsible for the control purpose (i.e. control of the session layer itself) is
a) Regular data b) Typed data
c) Capability data d) Expedited data

Q.45 The minimum number of bits required to represent all the symbols together is
a) 14 b) 11
c) 12 d) 15

Q.46 The average code length of the giving problem is
a) 2 b) 2.25
c) 2.45 d) 3

Q.47 The minimum number of bits required to represent **B** is
a) 1 b) 2
c) 3 d) 4

Q.48 In cryptography, the following uses transposition ciphers and the keyword
Is **LAYER. EN-**crypt the following message. (Spaces are omitted during encryption) WELCOME TO NETWORK SECURITY '
a) MEKREETSILTWETCOOCYONRU
b) EETSICOOYWMEKRONRU'TWET
c)LTWETONRU;WMEKRCOOCYEETST
d)ONRU; COOCYLTVETEETSIWMEKR

Q.49 Encrypt NEKEWNINRROGTTI using the above keyword in transposition cipher Method
a) INTERWORKINGNET
b) INTRERNETWORKING
c) WORKINGINTERNET
d) NON OF THE ABOVE

Q.50 Assuming that for given network layer implementation, connection establishment Overhead is 100 bytes and disconnection overhead is 28 bytes. What would be the minimum size of a packet the transport layer needs to keep up, if it wishes to Implement a datagram service above the network later and needs to keep its overhead to a maximum of 12.5% (Ignore transport layer overhead.)
a) 512 bytes b) 768 bytes
c) 1152 bytes d) 1024bytes

Q.51 Which of the following is not a standard RS-23C signal?
a) RTS b) CTS
c) DSR d) VDR

Q.52 A high speed communication equipment typically would not be need for
a) E-mail
b) Transferring large volume of data
c) Supporting communication between nodes in a LAN
d) all of the above

Q.53 Which of the following ISO level is more closely related to the physical Communications facilities?
a) Application b) session
c) Network d) data link

Q.54 Which of the following is not a field in the ethernet message packet?
a) Type b) data
c) Pin-code d) address

Q.55 The network topology that supports bi-directional links between each possible node is
a)Ring b) star
c) Tree d) mesh

Q.56 In A brand sense, a railway track is an
example of
a) Simplex b) half-duplex
c) full- duplex d) all of the above

Q.57 The frequency range at which the lend coaxial cables will be used is
a) 10^6 to 10^8 Hz b) $10^{10}$to 10^{11} Hz
c) 10^3 to 10^4 Hz d)10^{14} to 10^{15}Hz

Q.58 The data rate of the ring is 20 Mbps, signal propagation speed is 200m/μs then the number of Bits that can be placed on the channel of 200 km is
a)2000 bps b) 20,000 bps
c) 1,000 bps d) none of the above

Q.59 **ICI** (interface control information) is
a) Used to transfer user data from layer to layer
b) Used to exchange information by peer entities at different sites on the network to Instruct an entity

to perform a service function c) A combination of service data unit (SDU) and protocol control information (PCI)

d) A temporary parameter passed between N and N-1 layers to involve service Functions between two layers

Q.60 Match the following

1. Data link layer	i)The lowest later whose function is to activate deactivate & maintain the circuit between DTE & DCE
2. Physical Payer	ii) Performs, routing & communication
3. Presentation Layer	iii) Detection and recovery from error in the transmitted data
4. Network Layer	iv) Provides for the syntax of the data

a) 1-(iii , 2-(i), 3-(iv), 4-(ii)
b) 1-(ii), 2-(i), 3-(iv), 4-(iii)
c) 1-(iv), 2-(i), 3-(ii), 4-(iii)
d) 1-(ii), 2-(i), 3-(iii), 4-(iv)

Q.61 Which of the following category of noise is also called white noise:
a) Thermal noise
b) Intermodulation noise
c) Crosstalk
d) Impulse noise.

Q.62 A cable TV system has 100 commercial channels, all of them alternating programs with advertisements. This is
a) Time division multiplexing (TDM)
b) Frequency division multiplexing (FDM)
c) Both a) and b)
d) None of the above.

Q.63 Television channels are 6 MHz wide. How many bits/sec can be sent if four-level digital signals are used? Assume a noiseless channel.
a) 8 Mbps b) 16 Mbps
c) 22 Mbps d) 24 Mbps.

Q.64 A signal is measured at two different points. The power is Pt at the first point and P2 at the second point. The dB is 0. This implies
a) P2 is zero
b) P2 is equal to PI
c) P2 is much larger than Pt
d) P2 is much smaller than Pi.

Q.65 Which of the following is a type of transmission impairment in which the signal looses strength due to the different propagation speed of each frequency that makes up the signal.
a) Attenuation b) Distortion
c) Noise d) Decibel.

Q.66 Using the Shannon formula to calculate the data rate for a given channel, if C = B, then this implies where C is channel capacity and B is bandwidth
a) Signal is less than noise
b) Signal is greater than the noise
c) Signal is equal to the noise
d) Not enough information is given to answer the question.

Q.67 If a signal doesn't change at all, its frequency is
a) Infinity
b) Zero
c) One
d) Information insufficient to answer the question.

Q.68 If a signal changes instantaneously, its frequency is
a) 0
b) 10
c) Infinity
d) Information not enough to answer the question.

Q.69 If the bandwidth of a signal is 5 kHz and the lowest frequency is 52 kHz, what is the highest frequency ?
a) 55 kHz b) 60 kHz
c) 67 kHz d) 57 kHz.

Q.70 n networking, UTP stands for

a) Unshielded T-connector port
b) Unshielded twisted pair
c) Unshielded terminating pair
d) No such term exists.

Q.71 Nyquist theorem is true for
a) Optical fibre only
c) Coaxial cable only
b) Copper wire only
d) All media.

Q.72 A modem constellation diagram has data points at (0, 1) and (0, 2). The modem uses
a) Phase modulation
b) Frequency modulation
c) Amplitude modulation
d) None of the above.

Q.73 How many bits of RAM buffer does a time switch interchanger need if the input line samples are 10 bits and there are 80 input lines ?
a) 10 bits b) 800 bits
c) 80 bits d) 8 bits.

Q.74 Layered protocols offers following advantages :
a) It breaks the design problem into more manageable and smaller pieces
b) It allows protocols to be changed without affecting higher or lower ones
c) Both a) and b)
d) None of the above.

Q.75 Breaking the transmitted bit stream into frames is handled by the following OSI layer :
a) Data link layer b) Physical layer
c) Transport layer d) Network layer

Q.76 Determining which route through the subnet to use is handled by the following OSI layer:
a) Transport layer b) Physical layer
c) Network layer d) Data link layer

Q.77 Which agency created the V series standards (V. 32, V. 33, V. 42) which define data trans- mission over phone lines
a) ATT b) ITU-T
c) ANSI d) ISO.

Q.78 Which agency -developed standards for electrical connections and the physical transfer of data between devices
a) EIA b) ITU-T
c) FCC d) IEEE.

Q.79 Which organisation has authority over interstate and international commerce in the telecommunications field ?
a) ITU-T b) IEEE
c) ATT d) FCC.

Q.80 FDDI is a
a) ring network
b) star network
c) mesh network
d) bus based network

Q.81 Which of the following TCP/IP protocol is used for file transfer with minimal capability and minimal overhead :
a) RARP b) FTP
c) TELNET d)IP.

Q.82 How many class A, B and C network Ids can exist
a) 126, 16382, 2000000
b) 256, 65764, 1000000
c) 64, 8191, 2500000
d) 512, 32764, 3000000.

Q.83 Which of the following item is not used in local area network (LAN) :
a) computer b) modem
c) printer d) cable.

Q.84 Working of the WAN generally involves.
a) telephone lines b) microwaves
c) satellites d) all of the above

Q.85 Bit stuffing refers to

a) Inserting a '0' in user stream to differentiate it with a flag
b) Inserting a '0' in flag stream to avoid ambiguity
c) Appending a nibble to the flag sequence
d) Appending a nibble to the data stream.

Q.86 How many character per sec (7 bits + 1 parity) can be transmitted over a 2400 bps line if the transfer is synchronous (1 start & 1 stop bit).
a) 300 b) 240
c) 250 d) 275.

Q.87 Continuous flow control with a window size of 127?
a) 23.18% b) 23.28%
c) 23.38% d) 23.48%

Q.88 What is the minimum number of wires, needed to send data over a serial communication link layer ?
a) 1 b) 2
c) 3 . d) 4.

Q.89 The area of coverage of a satellite radio beam is called its.
a) beam width
b) circular polarization
c) footprint
d) identity.

Q.90 Which data communication method is used to send data over a serial communication link.
a) simplex b) half duplex
c) full duplex d) all of the above.

Q.91 What is the main difference between synchronous and asynchronous transmission ?
a) the bandwidth required is different
b) the pulse height is different
c) the clocking is derived from the data in synchronous transmission
d) the clocking is mixed with data in asynchronous transmission.

Q.92 Four bits are used for packet sequence in a computer network. What is the maximum window size?
a) 4 b) 8
c) 15 d) 16.

Q.93 Which of the following is possible in a token passing bus network :
a) in-service expansion
b) unlimited number of stations
c) both a) and b) above
d) unlimited distance.

Q.94 A geostationary satellite used for communication systems
a) rotates with the earth
b) remains stationary relative to the earth
c) is positioned over equator
d) all the above.

Q.95 Which of the following network access standard, disassemble is used for connecting station to a packet switched network :
a) X.3 b) X.21
c) X.25 d) X.75.

Q.96 The amount of uncertainty in a system of symbol is called.
a) bandwidth b) entropy
c) loss d) quantum.

Q.97 Which of the following network access standard is used for connecting station to a circuit switched network ?
a) X.3 b) X .21
c) X.25 d) X .75

Q.98 ARP (Address resolution protocol) is
a) a TCP/IP protocol used to dynamically bind a higher level IP address to a low level physical address
b) a TCP/IP high level protocols for transferring files from one machine to another

c) a protocol used to monitor computers
d) a protocol that handles error and control messages.

Q.99 Class A network can have following number of hosts.
a) 16-million hosts b) 64000 hosts
c) 32000 hosts d) 254 hosts.

Q.100 ALOHA
a) is used for channel allocation problem
b) is a mechanism used for buffering
c) is used for data transfer
d) all of the above.

Q.101 PURE ALOHA
a) Does not require global time synchronization
b) Divides time into discrete intervals
c) Requires global time synchronization
d) none of these.

Q.102 Class-B network can have following number of hosts :
a)128000 hosts b) 64000hosts
c) 254 hosts d) 1024 hosts.

Q.103 Error detection at the data link level is achieved by
a) bit stuffing
b) cyclic redundancy codes
c) hamming codes
d) equalization.

Q.104 Baud means the
a) Number of bits transmitted per unit time
b) Number of bytes transmitted per unit time
c) Rate at which the signal changes
d) Signal elements per second.

Q.105 Class-C network can have at the maximum, following number of hosts:
a) 254 hosts b) 1024 hosts
c) 512 hosts d) 4096 hosts.

Q.106 HF radio waves follow how many basic paths on leaving the transmitter ?
a) Two b) Four
c) One d) Many.

Q.107 What frequency range is most affected by fog and precipitation ?
a) 4 GHz to 6 GHz b) 6 GHz to 10 GHz
c) 2 GHz to 4 GHz d) Above 10 GHz.

Q.108 If the data rate of ring is 20 Mbps, signal propagation speed is 200 bpμs , then the number of bits that can be placed on the channel of 200 km is
a) 2000 bits b) 20000 bits
c) 1000 bits d) None of these.

Q.109 Adaptive or dynamic directory used in packet routing changes
a) within each user session
b) with each user session
c) at system generation time only
d) none of these.

Q.110 A terminal multiplexer has six 1200 bps terminals and n 300 bps terminals connected to it. The outgoing line is 9600 bps. The maximum value of n is.
a) 4 b) 16
c) 8 d) 28.

Q.111 End-to-end connectivity is provided from host-to-host in the
a) Network layer b) Transport layer
c) Session layer d) None of these.

Q.112 An example of a network layer protocol is
a) Internet protocol (IP)
b) X-25 packet level protocol
c) Source routing & domain naming
d) All of these.

Q.113 Unmodulated signal coming from a transmitter is known as
a) Carrier signal b) Baseband signal
c) Primary signal d) None of these.

Q.114 Non-polling system is
a) TDMA
b) Stop and wait
c) Continuous ARQ
d) None of these

Q.115 In the carrier sense protocol if the prevailing condition is channel busy, and if the technique used is
a) Non-persistent then it results in randomized wait and sense
b) 1-persistent then the channel is continually sensed.
c) P-persistent then randomized retransmission is done
d) Both a) and b).

Q.116 Hamming distance between 001111 and 010011 is
a) 1 b) 2
c) 3 d) 4.

Q.117 How many characters per sec (7 bit + 1 parity) can be _transmitted over a 2400 bps line, if the transfer is asynchronous (1 start & 1 stop bit)
a) 300 b) 240
c) 250 d) 275.

Q.118 In Ethernet CSMS/CD, the special bit sequence transmitted by media access management for collision handling is called as
a) Preamble b) Postamble
c) Jam d)None of above

Q.119 FDDI is a
a) ring network
b) start network
c) mesh network
d)bus based network

Q.120 No. of pairs of stations that can simultaneously communicate on Ethernet LAN
a) 1 b) 2
c) 3 d) multiple.

Q.121 Which of the following is a wrong example of a network layer :
a) Internet protocol (IP)-ARPANET
b) X.25 Packet level protocol (PLP)-ISO
c) Source routing and domain naming - USE NET
d) X.25 level 2–ISO.

Q.122 Which of the following are non-polling system :
a) TDMA
b) Stop and wait
c) Carrier sense system
d) Continous ARQ.

Q.123 Match the description to term :

P. Based on representing most commonly used characters with fewest number of bits	1. Run length encoding
Q. Based on slight difference between values	2. Huffman encoding
R. Based on occurence of one special character	3. Diatomic encoding
S. Based on data streams in which same characters occur frequentlyy.	4. Relational encoding.

a) P-4, Q-2, R-3, S-1
b) P-3, Q-1, R-4, S-2
c) P-2, Q-3, R-4, S-1
d) P-2, Q-4, R-3, S-1

Q.124 How many class A, B and C network IDs can exist ?
a) 2,113,658 b) 16,382
c) 126 d) 128.

Q.125 The Internet control message protocol (ICMP)
a) Allows gateways to send error a control messages to other gateways or hosts
b) Provides communications between the Internet protocol software on one machine and the Internet protocol software on another
c) Only reports error conditions to the original source, the source must relate errors to individual

application programs and take action to correct the problem
d) All of the above.

Q.126 Working of the WAN generally involves
a) telephone lines b) microwaves
c) satellites d) All of the above

Q.127 Many large organizations with their offices in different countries of the world connect their computers through telecommunication satellites and telephone lines. Such a communication network is called
a) LAN b) WAN
c) ECONET d) EITHERNET.

Q.128 A network which is used for sharing data, software and hardware among several users owning microcomputers is called
a) WAN b) MAN
c) LAN d) VAN.

Q.129 When a group of computers is connected together in a small area without the help of telephone lines, it is called
a) Remote communication network (RCN)
b) Local area network (LAN)
c) Wide area network (WAN)
d) Value added network (VAN)

Q.130 Standard of the Electronic Industries Association of America. What do the letters 'RS' stand for?
a) Recognised standard
b) Random sequence
c) Recommended standard
d) Registered source. 3

Q.131 An example of digital, rather than analog, communication is
a) DDD b) DDS
c) WATS d) DDT.

Q.132 Terminals are used to
a) Collect data from the physical system
b) Provide information for the manager
c) Communicate management decisions to the physical system
d) All of the above.

Q.133 Communication circuits that transmit data in both directions but not at the same time at operating in
a) a simplex mode
b) a half-duplex mode
c) a full-duplex mode
d) an asynchronous mode.

Q.134 A required characteristic of an online real-time system is
a) more than one CPU
b) offline batch processing
c) no delay in processing
d) All of the above.

Q.135 BSC ENQ code perform the following function
a) Select b) Bids
c) Polls d) All of these.

Q.136 HDLC is a
a) Network access standard for connecting station to a circuit switched network
b) A very common bit oriented data link protocol issused by ISO
c) A method of determining which device has access to the transmission medium at any time
d) A method access control technique for multiple access transmission media.

Q.137 ARP is a
a) A protocol used to monitor computers
b) A protocol that handles error and control message
c) A TCP/IP high level protocol for transferring files from one machine to another

d) A TCP/IP protocol used to dynamically bind a high level IP address to a low level physical address.

Q.138 TDMA stands for
a) Time distribution multiple access
b) Typical division multiple access
c) Time division multiple access
d) None of above.

Q.139 X 21 is a
a) Network access standard for connecting station to a circuit switched network
b) A method access control technique for multiple access transmission media
c) A method of determining which device has access to the transmission medium at any time
d) A very common bit oriented data link protocol.

Q.140 The 32 bit internet address 10000000000101000000010000111 10 will be written in dotted decimal notation is
a) 128.10.2.30 b) 210.28.2.64
c) 148.24.2.32 d) 168.102.8.61

Q.141 Which of the following layer protocol are responsible for user and the application program support such as password resource sharing, file transfer and network management ?
a) Layer 4 protocol
b) Layer 6 protocol
c) Layer 5 protocol
d) Layer 7 protocol

Q.142 The simultaneous transmission of data to a number of station is known as
a) Bandwidth
b) Aloha
c) Analog transmission
d) Broadcast.

Q.143 What is the bit rate for transmitting VGA colour with 8 bits/pixel of 40 frames/sec ?
a) 92.75 Mbps b) 93.75 Mbps
c) 94.75 Mpbs d) 95.75 Mbps.

Q.144 What is the maximum data rate of a noiseless 4 kHz channel that is sampled every 1 m-sec.

Q.145 Television channels are 6 MHz wide. How many bits/sec can be sent if four-level digital signals are used ? Assume a noiseless channel.
a) 20 Mpbps b)22 Mbps
c) 24 Mbps d) 26 Mbps.

Q.146 If a binary signal is sent over a 3 kHz channel whose signal-to-noise ratio is 20 dB, what is the maximum achievable data rate ?
a) 19.5 Kbps b) 6 Kbps
c) 3 Mbps d) None of the above

Q.147 How much bandwidth is needed, and how many microns of wavelength are needed
a) 400 Mbps b) 410 Mbps
c) 420 Mbps d) 422 Mbps.

Q.148 For this band at 1.30 microns.
a) 105×10^{-6} microns
b) 2.0×10^{-6} microns
c) 2.5×10^{-6} microns
d) 3.0×10^{-6} microns.

Q.149 What signal-to-noise ratio is needed to put a T1 carrier on a 50 kHz line?
a) 90 db b) 93 db
c) 96 db d) 99 db.

Q.150 Radio antennas often work best when the diameter of the antenna is equal to the wavelength of the ratio wave. Reasonable antennas range from 1 cm to 5 meters in diameter. What frequency range does this cover?
a) 60 GHz to 300 GHz

b) 60 MHz to 80 MHz
c) 60 MHz to 30 GHz
d) 30 GHz to 60 GHz.

Q.151 How much bandwidth is there in 0.1 micron of spectrum at a wavelength of 1 micron ?
a) 3^3 GHz b) 3^4 GHz
c) 3^5 GHz d) 3^6 GHz.

Q.152 A modem constellation diagram has data points at the following co-ordinates : (1,1), (1,-1), (1,1) and (-1,1). How many bps can a modem with these parameters achieve at 1200 band
a) 2000 bps b) 2100 bps
c) 2300 bps d) 2400 bps.

Q.153 For S/N = 30 dB, what is the number of uniform quantization levels needed? Assume a = 0.1.
a) 8 b) 16
c) 32 d) 64

Q.154 Imagine that you have trained your Dog to carry a box of three 8 mm Exabyte tapes instead of a flask of brandy (when your disk fills up, fills up, you consider that an emergency). These tapes each contain 7 gigabytes. The dog can travel to your side, wherever you by be, at 18 km/hour. For what rage of distances does your dog have a higher data rate than a 155-Mbps ATM line?
a) Less than 5.4 km
b) Less than 6 km
c) Less than 6.6 km
d) Less than 7.2 km

Q.155 The Internet is roughly doubling in size every 18 months .Although no one really knows for sure, one estimate put the number of hosts on it at 7 million in January , 1996. Use these data to compute the expected number of internet hosts in the year 2008
a) 1.5billion b) 1.8 billion
c) 2.0 billion d) 2.4 billion

Q.156 A system has an n-layer protocol hierarchy. Applications generate messages of length M bytes. At each of the layer, an h-byte header is added. What fraction of the network band width is filled with headers?
a) h/m b) hn/m
c) h/mm d) n/m

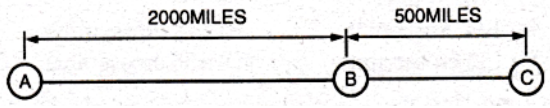
Q.157 A channel has a data rate of 4 Kbps and a propagation delay of 20ms. For what rage of frame sizes does stop-and-wait give an efficiency of atleast 50%.
a) 120 bits b) 140bits
c) 160 bits d) 180 bits

Q.158 Stop-and-wait flow control?
a) 0.2% b) 0.1%
c) 0.3% d) 0.4%

Q.159 Continuous flow control with a window size of 7?
a) 1.1% b) 1.2%
c) 1.3% d) 1.4 %

Q.160 Continuous flow control with a window size of 255?
a) 47.10% b) 47.13%
c) 47.16% d) 47.19%

Q.161 In the following figures frames are generated at node A and sent to node C through node B. Determine the minimum transmission rate required between nodes B and C, so that the buffers of node B are not floaded, based on the following :



(i) The data rate between A and B is 100 kbps.
(ii) The propagation delay is 10μ sec/mile for both lines .

(iii) There are full duplex lines between the nodes
(iv) All data frames are 1000 bits long; ACK frames are separate frames of negligible length.
(v) Between A and B, a sliding window protocol with a window size of Z is used.
(vi) Between B and C, stop – and – wait is used
(vii) There are no errors

a) 140 Kbps b) 160 Kbps
c) 160 Kbps d) 170 Kbps

Q.162 A channel has a data rate of R bps and a propagation delay of t second per kilometer. The distance between the sending and receiving nodes is L kilometers. Nodes exchange fixed-size frame of B bits Find a formula that gives the minimum sequence filed size of the frame as a function of R, t, B & L (considering maximum utilization). Assume that ACK frames are negligible in size and the processing at nodes is instantaneous

a) $\lceil \log_2 N \rceil$ b) $\lceil 2\log_2 N \rceil$
c) $\lceil 8\log_2 N \rceil$ d) $\lceil 10\log_2 N \rceil$

Q.163 Let M=11100011 be the message, which is to be transmitted and let P=110011 be the predetermined divisor. You are required to compute the Cyclic redundancy check (CRC) code.

a) 11010 b) 10101
c) 10011 d) 10110

Q.164 Assume that the velocity of propagation on a Time division multiplexing bus is 0.8 C, its length is 10m and the data rate is 500Mbps. How many bits should be transmitted in a time slot to achieve a bus efficiency of 99%

a) 2020 bits b) 2040 bits
c) 2060 bits d) 2080 bits

Q.165 You are assigned the tasks to design a Time division multiplexing carrier to support 30 voice channels using 6 bit samples and a structure similar to DS-1. Determine the required bit rate.

a) 1662 Kbps b) 1664 Kbps
c) 1666 Kbps d) 1668 Kbps

Q.166 Compute the end–to end delay for circuit switching.

a) 0.540sec b) 0.541sec
c) 0.542sec d) 0.543sec

Q.167 Compute the end to end delay for datagram packet switching.

a) 0.749sec b) 750 sec
c) 0.751sec d) 0.752 sec

Q.168 Compute the end to end delay for virtual circuit packet switching

a) 0.950 sec b) 0.951sec
c) 0.952sec d) 0.953sec

Q.169 What is the remainder obtained by dividing $x^7 + x^5 + 1$ by the generator polynomial $x^3 + 1$?

a) $x^3 + 1$ b) $x^3 + x^2$
c) x^3 d) $x^3 + x^2 + 1$

Q.170 A channel has a bit rate of 4 Kbps and a propagation delay of 20m-sec. For what rage of frame size does stop and wait give an efficiency of at least 80 percent?

a) 3200 bits b) 3600 bits
c) 4800 bits d) 6400 bits

Q.171 A 3000 km long T1 truck is used to transmit 64 – byte frames using a sliding window protocol along with go back n. If the propagation speed is 6 μ-sec/km, how many bits should the sequence number be?

a) 7 bits b) 8bits
c) 9 bits d) 10 bits

Q.172 A 100 km long cable runs at T1 data rate. The propagation speed in the cable is 2/3 the speed of light. How many bits fit in the cable?

a) 770 bits b) 771 bits
c) 772 bits d) 773 bits

Q.173 Following data fragment occurs in the middle of a data steam for which the character stuffing algorithm is used
DLE,STX,A,DLE.B,DLE,ETX
What is the output after stuffing ?
Here DLE is data line escape,
STX is start of Text
ETX is End of Text.

Q.174 What is the baud rate of the standard 10-mbps 802.3 LAN.
a) 10 Megabaud b) 20 Megabaud
c) 30 Megabaud d) 40 Megabaud

Q.175 A group of n stations share a 56 Kbps pure ALOHA channel. Each station outputs a 1000 –bit frame on an average of once every 100 sec, even if the previous one has not yet been sent (e.g., he stations are buffered.)
What is the maximum value of N?
a) 1000 stations b) 1010 stations
c) 1020 stations d) 1030 stations

Q.176 A sine wave has a frequency of 6 Hz. What is its period?
a) 0.17 second b) 0.18 second
c) 0.19 second d) 0.20 second

Q.177 A sine wave has a frequency of 8 kHz. A What is its period ?
a) 100µs b) 120 µs
c) 125 µs d) 135 µs

Q.178 A sine wave completes one cycle in 4 seconds. What is its frequency ?
a) 0.10Hz b) 0.25 Hz
c) 0.45 Hz d) 0.90 Hz

Q.179 A sine wave completes one cycle in 25 µs. What is its frequency ?
a) 10kHz b) 10Hz
c) 20kHz d) 40 kHz

Q.180 A sine wave is offset 1/6 of a cycle zero with respect to time zero. What is its phase ?
a) 30 degrees b) 45 degrees
c) 60 degrees d) 90 degrees

Q.181 A signal has a bandwidth of 20 Hz. The highest frequency is 60 Hz. What is the lowest frequency?
a) 40Hz b) 80 Hz
c) 30 Hz d) 50 Hz

Q.182 If a periodic signal id decomposed into five sine waves with frequencies of 100, 500, 700 and 900 Hz, What is the band width?
a) 500Hz b) 600 Hz
c) 700 Hz d) 800 Hz

Q.183 A digital signal has bit rate of 2000 bps. What is the duration of each bit (bit interval)?
a) 300µs b) 800 µs
c) 500 µs d) 200 µs

Q.184 A digital signal has bit interval of 40 microseconds . What is the bit rate ?
a) 20 Kbps b) 25 Kbps
c) 30 Kbps d) 35 Kbps

Q.185 A signal has 1000Hz as its lowest frequency and 11000 Hz as it highest frequency (thus the single has a bandwidth of 10000 Hz). What sampling rate is needed for this signal
a) 20,000 samples /second
b) 22,000 samples /second
c) 24,000 samples /second
d) 2,000 samples /second

Q.186 A signal is sampled. Each sample requires at least 12 levels of precision (+0 to + 5 and -0 to -5). How many bits should be sent for each sample?
a) 2 bits b) 3 bits
c) 4 bits d) 5 bits

Q.187 We want to digitize the human voice. What is the bit rate assuming eight bits per sample?

a) 64 Kbps b) 60 Kbps
c) 80 Kbps d) 66 Kbps

Q.188 An analog signal carries four bits in each signal elements. If 1000 signal elements are sent per second find the baud rate and bit rate.
a) 1000 baud per second, 4000 bps
b) 2000 baud per second, 4000bps
c) 2000 baud per second, 8000bps
d) 3000 baud per second, 6000bps

Q.189 It is given that bit rate of a signal is 6000. If each signal elements carries 10 bits, what is the baud rate?
a) 500 baud per second
b) 600 baud per second
c) 700 baud per second
d) 800 baud per second

Q.190 We have a Frequency Shift Keying (FSK) signal transmitting at 2000 bps. The transmission is in half duplex mode and the carriers must be departed by 3000 Hz. What will be minimum bandwidth of the signal.
a) 4000 Hz b) 4500 Hz
c) 5000 Hz d) 5500 Hz

Q.191 We have an amplitude shift keying signal transmitting at 200 bps. The mode of transmission is half – duplex the bandwidth required is
a) 1000 Hz b) 1250 Hz
c) 1750 Hz d) 2000 Hz

Q.192 In 4-PSK (Phase Shift Keying), a phase of 0 degrees represents 00; 90degrees represents 01; 180 degrees represents 10; & 270 degrees represent 11. What will be the band width for a 4-PSK signal transmitting at 2000 bps. Transmission is in half-duplex mode.
a) 1000Hz b) 2000Hz
c) 3000 Hz d) 4000 Hz

Q.193 For a transmission media the minimum frequency is 1000Hz and the maximum frequency is 11,000 Hz. For a full duplex Amplitude Shift keying(ASK). Fid the bandwidth for each direction.
a) 10000 Hz b) 8000 Hz
c) 6000 Hz d) 5000 Hz

Q.194 With the data given in the previous question what will be carrier frequency in forward direction and backward direction respectively .
a) 5000 Hz, 10000Hz
b) 0 Hz, 5000 Hz
c) 3500 Hz,8500Hz
d) None of the above

Q.195 The bandwidth of the transmission media is 12000 Hz. The modulation scheme to be used is Frequency Shift Keying (FSK). The difference between the two carriers must be at least 2000 Hz and transmission is in full duplex mode . What will be the maximum bit rates:
a) 2000bps b) 3000 bps
(C) 4000 bps d) 5000 bps

Q.196 What is the baud rate to f an 8- PSK
a) 12000 baud b) 13000 baud
c) 14000 baud d) 15000 baud

Q.197 At a transmission rate of 5 Mbps and a propagation speed of 200 m/μ-sec, to how many meters of cable is the 1- bit delay in a token ring interface equivalent ?
a) 40 meters b) 45 meters
c) 50 meters d) 55 meters

ANSWER KEY:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
(a)	(d)	(b)	(d)	(d)	(c)	(c)	(b)	(b)	(c)	(a)	(a)	(a)	(a)	(c)
16	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**26**	**27**	**28**	**29**	**30**
(a)	(b)	(c)	(a)	(a)	(a)	(b)	(c)	(a)	(b)	(b)	(b)	(c)	(c)	(b)
31	**32**	**33**	**34**	**35**	**36**	**37**	**38**	**39**	**40**	**41**	**42**	**43**	**44**	**45**
(b)	(b)	(c)	(a)	(a)	(b)	(a)	(b)	(c)	(d)	(a)	(b)	(a)	(c)	(c)
46	**47**	**48**	**49**	**50**	**51**	**52**	**53**	**54**	**55**	**56**	**57**	**58**	**59**	**60**
(c)	(b)	(b)	(b)	(d)	(d)	(a)	(d)	(c)	(d)	(b)	(a)	(b)	(d)	(a)
61	**62**	**63**	**64**	**65**	**66**	**67**	**68**	**69**	**70**	**71**	**72**	**73**	**74**	**75**
(a)	(c)	(d)	(b)	(b)	(c)	(b)	(c)	(d)	(b)	(d)	(c)	(b)	(c)	(a)
76	**77**	**78**	**79**	**80**	**81**	**82**	**83**	**84**	**85**	**86**	**87**	**88**	**89**	**90**
(c)	(b)	(a)	(d)	(a)	(a)	(a)	(c)	(d)	(a)	(a)	(d)	(b)	(c)	(c)
91	**92**	**93**	**94**	**95**	**96**	**97**	**98**	**99**	**100**	**101**	**102**	**103**	**104**	**105**
(d)	(c)	(a)	(d)	(c)	(b)	(b)	(c)	(a)	(a)	(a)	(b)	(b)	(d)	(a)
106	**107**	**108**	**109**	**110**	**111**	**112**	**113**	**114**	**115**	**116**	**117**	**118**	**119**	**120**
(a)	(d)	(b)	(a)	(c)	(b)	(d)	(b)	(a)	(b)	(c)	(b)	(c)	(a)	(a)
121	**122**	**123**	**124**	**125**	**126**	**127**	**128**	**129**	**130**	**131**	**132**	**133**	**134**	**135**
(d)	(A)	(d)	(a)	(d)	(d)	(b)	(c)	(b)	(c)	(b)	(d)	(b)	(c)	(d)
136	**137**	**138**	**139**	**140**	**141**	**142**	**143**	**144**	**145**	**146**	**147**	**148**	**149**	**150**
(b)	(d)	(b)	(a)	(a)	(d)	(d)	(b)	-	(c)	(b)	(d)	(c)	(b)	(c)
151	**152**	**153**	**154**	**155**	**156**	**157**	**158**	**159**	**160**	**161**	**162**	**163**	**164**	**165**
(b)	(d)	(c)	(a)	(b)	(b)	(c)	(a)	(c)	(b)	(b)	(d)	(a)	(c)	(d)
166	**167**	**168**	**169**	**170**	**171**	**172**	**173**	**174**	**175**	**176**	**177**	**178**	**179**	**180**
(b)	(d)	(c)	(d)	(d)	(a)	(c)	-	(b)	(d)	(a)	(c)	(b)	(d)	(c)
181	**182**	**183**	**184**	**185**	**186**	**187**	**188**	**189**	**190**	**191**	**192**	**193**	**194**	**195**
(a)	(d)	(c)	(b)	(b)	(c)	(a)	(a)	(b)	(c)	(d)	(a)	(d)	(c)	(c)
196	**197**													
(a)	(a)													

EXPLANATIONS

Q.9 (b)
In bipolar code the signal varies among three levels. In non-return to zero code the signal remains the same throughout the bit cell. In unipolar code, there will be no signal either below zero or above zero. In Manchester code the signal level will not vary in the middle and is unipolar.

Q.16 (a)
Start and stop bits are not needed in synchronous transfer of data. So, it is 2400/8=300

Q.21 (a)
Bit stuffing is required when there is a flag of bit to represent one of the incidents, like start of frame, end of frame, etc., if the same flag of bits appear in the data stream, a zero can be inserted. The receiver deletes this zero from the data stream.

Q.27 (b)
As all lines are full-duplex and there are no self-connections, only the cross points above the diagonal needed. Hence formula for the number of cross points needed is n(n-1)/2

Q.28 (c)
Since there are six 1200 bps terminals 6×1200 + n×300=9600. Solving, n=8.

Q.32 (b)
Maximum data rate = $2H\log_2 V$ bps, where H is the bandwidth, V is the discrete levels. Here H is 3 kHz and V is 2

Q.33 (c)
Maximum number of the bps = $H\log_2 (1+ SNR)$.

Q.34 (a)
In time division switches 2nT=1 frame period, where T is the memory access
time.

Q.45 (c)
The Huffman code for A will have 2 digits, B-3 digit, C-3 digits,D-2 digits and E-2 digits. This can be obtained by constructing the binary tree corresponding to the given probabilities.

Q.46 (c)
Refer to the explanation of the previous questions.

Q.47 (b)
Average code length is the sum of product of the length and probability of the occurrence of the symbols.
Here it is,
2×0.3+3×0.15+3×0.1+2×0.25+2×0.2=2.25.

Q.86 (a)
In synchronous transfer start and stop bits are never used.
Hence 240018 = 300 bits per sec.

Q.87 (d)
Consider the use of 1000 bit frames on a 1 Mbps satellite channel with a 270 ms delay. What is the maximum link utilization for ?
Given that the window size is 127
a = 270
So, $127 < 541 \quad (N < 2a+1)$

$$\Rightarrow \text{Efficiency} = \frac{127}{541}$$

$$= 0.2348 = 23.48\%$$

Q.92 (c)

With n bits number of combinations possible is 2^n. Therefore with 4 bits number of combinations = 2^4 = 16. As numbering starts from 0, maximum packet number is 15.

Q.143 (b)

The GVA resolution is given as 640 ×480 pixels with each pixel requiring 8 bits, total number of bits become 460 ×480×8 bits.

This is the number of bits in one frame. Now to transmit 40 such frames, number of bits to be transmitted in one second is

$640 \times 480 \times 8 \times 40 \text{ bits/sec} = 93.75$

Q.144

A noiseless channel can carry on arbitrarily large amount of information, no matter how often it is sampled . Just send a lot of data per sample. As per Nyquist theorem, we can make 8000 samples/sec for a 4 kHz channel.

1. If each sample is 16 bits, the channel can send 128 Kbps.
2. If each sample is 1024 bits, the channel can send 8.2 Mbps.

The keyword here is ``noiseless", with a normal 4 kHz channel, the Shannon limit would not allow this .

Q.145 (c)

The Nyquist theorem states that, on a noiseless channel, if signal cansists of V discrete levels, then

Maximum data rate

$= 2H \log_2 V \text{ bits/sec}$

Where

H = bandwidth of the channel.

∴ Maximum data rate

$= 2 \times 6 \times \log_2 4 = 2 \times 6 \times 2 = 24 \text{ Mbps.}$

Q.146 (b)

The Shannon's theorem states:

For a noisy channel:

Maximum data rate

$= H \log_2(1 + s/N)$

H = bandwidth

S/N = signal-to-noise ratio

$\therefore \quad 1 \text{ dB} = 10 \log_{10} S/N$

$\therefore \quad 20 \text{ dB} \Rightarrow S/N = 100$

Maximum data rate $= 3 \log_2(1 + 100)$

$= 19.5 \text{ Kbps.}$

Thus we can say that Shannon's limit is 19.5 Kbps.

The Nyquist theorem states:

For a noisy channel:

Maximum data rate

$= 2H \log_2 V \text{ bits/sec}$

Since V is not specified, we will assume $\log_2 V = 1$

Maximum data rate

$= 2 \times 3 = 6 \text{ Kbps.}$

Thus we can say that Nyquist limit is 6 Kbps. The bottleneck is therefore the Nyquist limit, giving a maximum channel capacity of 6 Kps.

Q.147 (d)

The data rate can be easily calculated as

$= 480 \times 640 \times 24 \times 60 = 422 \text{ Mbps.}$

The fundamental relation between f, λ and C (in vacuum) is

$\lambda f = C$

Where

$\lambda =$ wavelength,

f = frequency,

c = speed of light.

If we solve this equation for f and differentiate with respect to λ we get,

$$\frac{df}{d\lambda} = \frac{C}{\lambda^2}$$

If we now go to finite differences instead of differentials and only look at absolute values , we get,

$$\Delta f = \frac{c \Delta \lambda}{\lambda^2}$$

Where $\Delta f =$ bandwidth or frequency band

$\Delta\lambda =$ wavelength band

$\Rightarrow \Delta\lambda = \dfrac{\Delta f \lambda^2}{C}$

We know, $\Delta f = 442 \text{Mbps}$

$C = 3\times10^8$ m/sec

$$\Delta\lambda = \frac{4.42\times10^8 \times \left(1.3\times10^{-6}\right)^2}{3\times10^8} = 205\times10^{-6}$$

microns

Thus bandwidth required

= 422 Mbps.

Wave length needed

$= 2.5\times10^{-6}$ microns.

Q.148 (c)

The data rate can be easily calculated as

$= 480\times640\times24\times60 = 422$ Mbps.

The fundamental relation between f, λ and C (in vacuum) is

$\lambda f = C$

Where

$\lambda =$ wavelength,

f = frequency,

c = speed of light.

If we solve this equation for f and differentiate with respect to λ we get,

$$\frac{df}{d\lambda} = \frac{C}{\lambda^2}$$

If we now go to finite differences instead of differentials and only look at absolute values , we get,

$$\Delta f = \frac{c\Delta\lambda}{\lambda^2}$$

Where $\Delta f =$ bandwidth or frequency band

$\Delta\lambda =$ wavelength band

$\Rightarrow \Delta\lambda = \dfrac{\Delta f \lambda^2}{C}$

We know, $\Delta f = 442 \text{Mbps}$

$C = 3\times10^8$ m/sec

$$\Delta\lambda = \frac{4.42\times10^8 \times \left(1.3\times10^{-6}\right)^2}{3\times10^8} = 205\times10^{-6}$$

microns

Thus bandwidth required = 422 Mbps.

Wave length needed

$= 2.5\times10^{-6}$ microns.

Q.149 (b)

We know that the data rate of T1 carrier is 1.544 Mbps.

Now as per Shannon's theorem:

Maximum data rate

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

$\Rightarrow H \log_2(1+s/N) = 1.544$ Mbps.

Given that, H = 50000

$50000\log_2(1+S/N) = 1.544\times10^6$

$\log_2(1+S/N) = 30.88$

$\Rightarrow \quad (1+S/N) = 2^{30.88}$

Expressing the result in dB.

Taking log on both sides

$\log_{10} S/N = 30.88\log_{10} 2 - \log_{10} 1 = 9.2958$

Multiplying both side by 10

$10\log_{10} S/N = 92.958 = 93$ db.

Q.150 (c)

We know, $\lambda f = C$

Where

$\lambda =$ wavelength,

f = frequency,

C = speed of light

When diameter = 1 cm $\Rightarrow \lambda = 1$ cm

$\lambda = 1\times10^{-2}$ m

$$f = \frac{3\times10^8}{1\times10^{-2}} = 30 \text{ GHz}$$

When diameter = 5 m $\Rightarrow \lambda = 5$m

$$f = \frac{3\times10^8}{5} = 60 \text{ MHz}$$

Thus the band covered is 60 MHz to 30 GHz.

Q.151 (b)

We know $\Delta f = \dfrac{C\Delta\lambda}{\lambda^2}$

where

$\Delta f =$ frequency band,

$\Delta\lambda =$ wavelength band,

C = speed of light
Given :
$\Delta\lambda = 10^{-7}$ microns
$\lambda = 10^{-6}$
$\Delta f = \frac{3\times10^{8}\times10^{-7}}{10^{-6}\times10^{-6}} = 3\times10^{13}$
Bandwidth,
$(\Delta f) = 3^{4}$ GHz or 30000 GHz

Q.152 (d)

We know, $D = \frac{R}{b}$
Where
D = modulation rate, baud,
R = data rate, bps,
b = Number of bits per signal element.
As per the constellation diagram, there are 4 different legal values. Thus number of bits per signal element is 2.
Data rate $= 2\times1200 = 2400$ bps.

Q.153 (c)

The signal-to-noise ratio for quantizing noise can be expressed as
$\frac{S}{N} = (6n - a)\,dB$
Where a is a constant on the order of 0 to 1.
$\Rightarrow 30 = 6n - 0.1$
$6n = 30 + 0.1$
$n = 4.98$
Rounding off, $n = 5$ bits.
This gives $2^{5} = 32$ Quantization levels.
(b) Data rate = Number of samples per sec × Number of bits per sample
$= 7000\times5 = 35$ Kbps.

Q.154 (a)

Dog can carry 3 tapes.
The data in each tape is 7 gigabytes
Thus dog can carry 21gigbytes
or21 × 8 = 168 gagabits.
The speed of dog is 18 km/hour, which is equal to
$= \frac{18}{60\times60} = 0.005$ km/sec
The time to travel x km is
$\frac{x}{0.005} = 200x$ sec
Thus dog can cover x km in 200x second
This will give us a data rate of $\frac{168}{200x}$ Gbps or $\frac{840}{x}$ mbps.
Now $\frac{840}{x}$ Mbps > 155 Mbps For the dog to beat the AIM line
$\Rightarrow \frac{840}{155} > x$
$5.4 > x$
For x < 5.4 km, the dog has a higher rate than an ATM line.

Q.155 (b)

Douling in size every 18 months signifies a growth factor rate of four in 3 years.
In 12 years the gain factor will be
1st three years 4x
2nd three years $4\times4x$
3rd three years $4\times4\times4x$
4th three years $4\times4x\times4\times4x$
Thus in 12 years the gain factor will be 4^{4} or 256.
Thus the number of hosts in year 2008 will be 256 × 7 million
= 1792 millions
= 1.8 billion

Q.156 (b)

Given that the system has n-layers.
Number of bytes added per layer is h.
Total number of header bytes per message is hn
Given that the applications generate message of length M bytes.

Q.157 (c)

The efficiency of stop-and-wait

Protocol is determined using the following formula:

$$\text{Efficiency} = \frac{1}{1+2a}$$

$$\text{Where} \quad a = \frac{\text{Propagation time}}{\text{Transimission time}}$$

$$\text{Propagation time} = \frac{\text{Distance of the link(d)}}{\text{Velocity of progatation(V)}}$$

$$\text{Transmission time} = \frac{\text{Length of frame in bits(L)}}{\text{Data rate(R)}}$$

$$\Rightarrow a = \frac{d/V}{L/R}$$

$$\Rightarrow a = \frac{dR}{LV}$$

$$\text{Thus,} \quad a = \frac{20\times10^{-3}}{L/\left(4\times10^{3}\right)}$$

$$a = \frac{80}{L}$$

Substituting in (1),

$$\text{Efficiency} = \frac{1}{1+(160/L)} = \frac{50}{100}$$

$$1 = 0.5 + 0.5(160/L) = 0.5 + 80/L \Rightarrow L = 160.$$

An efficiency of atleast 50% requires a frame size of atleast 160 Bits.

Q.158 (a)

Consider the use of 1000 bit frames on a 1 Mbps satellite channel with a 270 ms delay. What is the maximum link utilization for ?

The efficiency of stop-and-wait protocol is determined using the following formula:

$$\text{Efficiency} = \frac{1}{1+2a}$$

$$\text{Where } a = \frac{\text{Propagation time}}{\text{Transmission time}}$$

$$a = \frac{270\times10-3}{10^{3}/10^{6}} = 270$$

Efficiency

$$= \frac{1}{(1+2\times270)} = \frac{1}{541} = 0.0018$$

$$= 0.002 \text{ or } 0.2\%$$

Q.159 (c)

Consider the use of 1000 bit frames on a 1 Mbps satellite channel with a 270 ms delay. What is the maximum link utilization for ?

The efficiency of sliding window protocol is determined using the following formula:

$$\text{Efficiency} = \begin{cases} 1 & N > 2a+1 \\ \dfrac{N}{2a+1} & N < 2a+1 \end{cases}$$

Where N is the size of window.

Typically, the sequence number is provided for in an n-bit

Field, and the maximum window size is $N = 2^{n} - 1$.

Given that the window size is 7

$a = 270$

So, $7 < 541 \quad (N < 2a+1)$

$$\Rightarrow \text{Efficiency} = \frac{7}{541} = 0.0129 = 1.3\%$$

Q.160 (b)

Consider the use of 1000 bit frames on a 1 Mbps satellite channel with a 270 ms delay. What is the maximum link utilization for ?

Given that the window size is 255

$a = 270$

So, $255 < 541 \quad (N < 2a+1)$

$$\Rightarrow \text{Efficiency} = \frac{255}{541}$$

$$= 0.4713 = 47.13\%$$

Q.161 (b)

Case-I.

Frames are sent from node A to B

Round trip propagation time

$$= 2\times2000\times10\ \mu\text{sec} = 40\text{m}-\text{sec}$$

Transmission time per fram

$$= \frac{1000}{100\times10^{3}}$$

$$= 10\ \text{m}-\text{sec}$$

Case-II.

Frames are sent from node B to C

Round trip propagation time $= 2 \times 500 \times 10\ \mu - \text{sec} = 10\ \text{m} - \text{sec}$

Transmission time per fram $= x = \dfrac{1000}{R}$

Where R is the data rate between B and C and R has not been provided to us.

A can transmit three frames t o B and then must wait for the acknowledgement of the first frame b before transmitting additional frames. The first frame takes 10 m-sec to transmit ; the last bit fo the first frame arrives at B 20m-sec after it was transmitted, and therefore, 30 m-sec after the frame transmission began. It will take an additional 20 msec. For B's acknowledgement to return to A. Thus, A can transmit 3 frames in 50 m-sec. B can transmit one frame to C and an additional 5 m –sec for C's acknowledgement to return to A. The us, B can transmit one frame every 10 + x msec or3 frames every 30+3x m-sec. Thus,

$30 + 3x = 50$

$x = 6.66\ \text{m} - \text{sec}$

R(Data rate) $= \dfrac{1000}{x} = 150\ \text{Kbps.}$

Q.162 (d)

Round trip propagation delay of the link is given as

$2 \times L \times t$

Time to transmit a frame (Transmission time)

$= \dfrac{B}{R}\left(\dfrac{\text{Frame size}}{\text{Data rate}}\right)$

To reach 100% utilization, transmitter should be able to transmit frames continuously during a round trip propagation time. Thus, total number of frames transmitted without an ACK is

$N = \dfrac{2 \times L \times t}{B/R} + 1$ ...(1)

Reason.

We know the formula for determining the efficiency of a sliding window protocol is

$U = \dfrac{N}{2a + 1}$ ...(2)

Where $a = \dfrac{\text{Propagation delay}}{\text{Transmission time}}$

In our case, $a = \dfrac{L \times t}{B/R}$

We want efficiency to be 100%

$\Rightarrow \quad U = 1$

Substituting the above values in (2).

$1 = \dfrac{N}{\left(\dfrac{2 \times L \times t}{B/R} + 1\right)} \Rightarrow N = \dfrac{2 \times L \times t}{B/R} + 1$

For a window size to accommodate N frames, M-bit sequence number will be generated,

$M = [10 \log_2 N]$

Q.163 (a)

Given : M = 11100011 (8 bits)

Pattern P = 110011 (6 bits)

FCS, R = ? (5 bits)

No. of bits in FCS is always one less than the number of bits in pattern P.

Now, the message M is multiplied by 2_1^5 yielding

1110001100000

This product is divided by `P'

$$
\begin{array}{r}
1010110 \\
110011 \overline{)1110001100000} \\
\underline{110011} \\
101111 \\
\underline{110011} \\
111000 \\
\underline{110011} \\
101100 \\
\underline{110011} \\
111110 \\
\underline{110011} \\
\text{CRC} = \quad 11010
\end{array}
$$

Note.
We have used Modulo 2. Arithmetic, which uses binary additional with no carries, which is just the exclusive or operation.
CRC = 11010 Ans.

Q.164 (c)

$$\text{Propagation delay} = \frac{\text{Length of the link}}{\text{Velocity of propagation}}$$

$$\text{Propagation delay} = \frac{10\text{m}}{0.8\times 3\times 10^8 \text{ m/sec}}$$

$= 4.17\times 10^{-8}$ sec.

Now to achieve an efficiency of 99%, the transmission time perslot should be 99 times the propagation delay.

∴ Transmission time

$= 99\times 4.17\times 10^{-8}$

$= 4.12\times 10^{-6}$ sec

Number of bits/slot

$= 4.12\times 10^{-6}\times 500\times 10^6 = 2060$ bits

Q.165 (d)

The basis of the TDM hierarchy (in North America and Japan) is the DS-1 transmission format, which multiplexes 24 channels. Each frame contains 8 bits per channel plus a framing bit for $24\times 8+1=193$ bits

The most significant frequency of voice channels (telephone lines) is 4 kHz.

As per sampling theorem,

Voice sampling rate $= 2\times 4\text{kHz}$

$= 8000$ sample/sec.

Thus, 30 voice channels

$\Longrightarrow 30\times 8\times 6$ = 1440 Kbps.

1 synchronous bit/channel

$\Longrightarrow 30\times 8$ = 240 Kbps.

1 synchronous bit/frame

$\Longrightarrow 1\times 8$ = 8 kbps

Total = 1668 Kbps

Thus, the required bit rate is 1668 kbps.

Q.166 (b)

N = Number of hops between two given end system

L = Message length in bits

B = Data rate, in bits per seonc (bps) on all links

P = Packet size

H = Overhead (header) bits per packet

S = call setup time (circuit switching or virtual circuit) in seconds

D = propagation delay per hop in seconds.

Given : N =4, := 3200, B = 9600, P = 1024, H =16,

S = 0.2 and D =0.001.

Let, T denote the end-to end delay

$T = C_1 + C_2$

Where C_1 = call set-up time,

C_2 = Message delivery time,

$C_1 = S = 0.2(\text{Given})$

C_2 = Propagation delay + Transmission time

$$= N\times D + \frac{L}{B} = 4\times 0.001 + \frac{3200}{9600}$$

$= 0.004 + 0.337 = 0.341$

$\Longrightarrow \quad T = 0.2 + 0.341 = 0.541\text{sec.}$

Q.167 (d)

N = Number of hops between two given end system

L = Message length in bits

B = Data rate, in bits per seonc (bps) on all links

P = Packet size

H = Overhead (header) bits per packet

S = call setup time (circuit switching or virtual circuit) in seconds

D = propagation delay per hop in seconds.

Given : N =4, := 3200, B = 9600, P = 1024, H =16,

S = 0.2 and D =0.001.

Let, T denote the end-to-end delay.

$T = D_1 + D_2 + D_3 + D_4$

Where D_1 = Time to transmit and deliver all packets through first hop

D_2 = Time to deliver last packet across second hop

D_3 = Time to deliver last packet across third hop

D_4 = Time to deliver last packet across fourth hop

Let us determine the number of packets.

Total length of the message = 3200 bits

Size of the packet = 1024

Number of data bits in the packet

= Size of packet – Header bits

= 1024 -16

= 108 data bits packet.

For a message of size = 3200 bits.

Number of packets required is $\frac{3200}{1008} = 4.$

$D_1 = 4 \times t + p$

t = transmission time for one packet

p = propagation delay for one hop.

$$D_1 = 4 \times \left(\frac{P}{B}\right) + D = 4 \times \frac{1024}{9600} + 0.001 = 0.428$$

$$D_2 = D_3 = D_4 = t + p = \left(\frac{P}{B}\right) + D$$

$$= \left(\frac{1024}{9600}\right) + 0.001 = 0.108$$

$$T = 0.428 + 0.108 + 0.108 + 0.108 = 0.752 \text{sec}.$$

Q.168 (c)

N = Number of hops between two given end system

L = Message length in bits

B = Data rate, in bits per seonc (bps) on all links

P = Packet size

H = Overhead (header) bits per packet

S = call setup time (circuit switching or virtual circuit) in seconds

D = propagation delay per hop in seconds.

Given : N =4, := 3200, B = 9600, P = 1024, H =16,

S = 0.2 and D =0.001.

$T = V_1 + V_2$

where V_1 = Call setup time,

V_2 = Datagram packet switching time

$T = S + 0.752 = 0.2 + 0.752 = 0.952 \text{sec}.$

Q.169 (d)

$x^7 + x^5 + 1$ can be written as $10100001 = M$

$x^3 + 1$ can be writes as 1001 = P

$\Longrightarrow$ M = 10100001 (8 bits)

P = 1001 (4 bits)

Multiplying M by 2^3

$\Longrightarrow$ M = 10100001000

This product will not be divided by P as shown below :

```
1001 | 10100001000 | 10110111
       1001
       ----
        1100
        1001
        ----
         1010
         1001
         ----
          1110
          1001
          ----
          1110
          1001
          ----
          1110
          1001
          ----
           111
           111
```

Thus the remainder is 111

In polynomial notation, this can be written as

$x^3 + x^2 + 1.$

Q.170 (d)

$$\text{Efficiency} = \frac{1}{1+2a}$$

Where $a = \frac{\text{Propagation time}}{\text{Transmission time}}$

$$a = \frac{\text{Distanceoflink / Velocity of propagation}}{\text{Datarate / Size of frame}}$$

$$= \frac{20\times10^{-3}\times4000}{\text{Size of frame}}$$

$S = \frac{80}{s}$ where S ddenotes s size of frame.

$$\text{Efficiency} = \frac{1}{1+\frac{160}{S}}$$

$$\frac{80}{100} = \frac{S}{(S+160)}$$

$80*(S+160) = 100\ S.$

$80\ S + 12800 = 100S$

$12800 = 20\ S$

$\Rightarrow$ S = 6400 bits

Q.171 (a)

In order to operate efficiently, the s ending window size must be large enough to keep transmitting until the first acknowledgement has been received.

Propagation time is 18 ms.

Given that it is a T1 trunk.

$\Rightarrow$ Transmission speed is 1.536 Mbps.

$\Rightarrow$ A 64-bytes frame will take 0.300 m-sec.

Therefore, the first frame fully arrives 18.3 m-sec after its transmission was started.

The acknowledgement takes another 18 m-sec to get back, plus a small (negligible) time for the acknowledgement to arrive fully.

In all, this time is 36.3 m-sec.

The transmitter must have enough window space to keep going for 36.3 m-sec. A frame takes 0.3 ms, so it takes 121 frames to fill the pipe.

7-bit sequence numbers are needed.

Q.172 (c)

Propagation speed in the cable

$$= \frac{2}{3}\times\text{Speed of light}$$

$$= \frac{2}{3}\times3\times10^{8}\text{m} = 2\times10^{5}\text{km/sec}$$

Or = 200 km/sec.

$\Rightarrow$ A 100 km cable will be filled in 500 μ-sec.

This corresponds to four 193 bit frames.

or $4\times193 = 772$ bits on the cable.

Q.173

It may easily happen that the characters for DLE STX or DLE ETX occur in the data, which will interfere with the framing. One way to solve this problem is to have the sender's data link layer insert an ASCII DLE character just before each "accidental" DLE character in the data. The data link layeron the receiving end removes the DLE before the data are given to the network layer. This technique is called character stuffing. Thus a framing DLE SIX or DLE ETX can be distinguished from one in data by the absence or presence of a single DLE.

Thus after stuffing the bytes are DLES, STX, A, DLE, DLE, B, DLE, ETX.

Q.174 (b)

The Ethernet uses Manchester encoding.

$\Rightarrow$ It has two signal period per bit sit.

The data rate of standard Ethernet is 10 Mbps. So the baud rate is twice i.e., 20 Megabaud.

Q.175 (d)

We know that the efficiency of pure ALOHA is 1.84%

Thus, the usable bandwidth is 18.4% off 56 Kbps

$\Rightarrow$ 0.184×56 Kbps $= 10.3$ Kbps

With a 1000-bit frame each station requires 10 bps.

$\Rightarrow \quad N = \frac{10300}{10} = 1030$ stations.

Q.176 (a)

Let T be the period and f be the frequency. Then

$T = \frac{1}{f} = \frac{1}{6} = 0.17$ second.

Q.177 (c)

Let T be the period and f be the frequency.

Then

$T = \frac{1}{f} = \frac{1}{8000} = 0.000125$ second

$= 125 \times 10^{-6}$ second

= 125 μs.

Q.178 (b)

Let T be period and f be the frequency. Then $f = \frac{1}{T} = \frac{1}{4} = 0.25Hz$

Q.179 (d)

Let T be the period o and f be the frequency

Then, $f = \frac{1}{T} = \frac{1}{(25 \times 10^6)} = 40,000Hz$

= 40 kHz

Q.180 (c)

We know that one complete cycle is 360 degrees.

$\frac{1}{6}$ of a cycle is equivalent to

$\frac{1}{6}$ of 360 = 60 degrees.

Q.181 (a)

Let fight be the highest frequency .

Let flow be the lowest frequency

Let H denote the bandwidth

$\Rightarrow f_{high} - f_{low}$

$\Rightarrow 20 = 60 - f_{low}$

$f_{low} = 60 - 20 = 40$ Hz

Q.182 (d)

Let f_{high} be the highest frequency

Let f_{low} be the lowest frequency

Let B be the Bandwidth

$B = f_{high} - f_{low} = 900 - 100 = 800Hz$

Q.183 (c)

We know that the bit integral is inverse of bit rate.

$\text{Bit Interval} = \frac{1}{\text{bit rate}} = \frac{1}{2000} = 0.000500\,\text{sec}$

$= 500 \times 10^{-6}$ bit per second $= 25 \times 10^3$ bits per second

=500μs

Q.184 (b)

We know that the bit integral is inverse of bit rate.

$\text{bit rate} = \frac{1}{(\text{bit interval})} = \frac{1}{(40 \times 10^{-6})}$

=25000 bit per second $= 25 \times 10^3$ bits per second

=25 Kbps

Q.185 (b)

As per sampling theorem, the sampling rate must be twice the highest frequency in the signal. Sampling rate=2×11,00

=22,000 samples /second.

Q.186 (c)

We will be needing four bits;

One bit for the sign

Three bits for the value .

A 3- bit value can represent 2^3-=8 levels which is more that what we need. (0 to 5 is six levels).

Q.187 (a)

The human voice normally contains frequencies from 0 to 4000 Hz. So the sampling rate, as per sampling theorem is

2×4000=8000 sample /second

The bit rate can be calculated as

Bit rate = sampling rate × Number of bits per sample

8000×8=64000 bits/second
=64 Kbps

Q.188 (a)

Baud rate = Number of bits per signal element 1000 ×4=4000 bps

Q.189 (b)

We can calculate baud rate using

$$\text{Baud rate} = \frac{\text{Bit rate}}{\text{Number of bits per signal element}}$$

Q.190 (c)

Let f_{c1} and f_{c0} are the carrier frequencies , then, Bandwidth = B +Rate + $(f_{c1} - f_{c0})$

We know that the baud rate here is same as the bit rate

∴ Bandwidth = Bit rate + $(f_{c1} - f_{c0})$

=2000+3000=5000 Hz

Q.191 (d)

In amplitude shift keying , the baud rate and bit rate are the same.

Note. An amplitude shift keying signal requires a minimum bandwidth equal to its baud rate.

∴ Baud rate is2000

⟹ Minimum bandwidth is 2000 Hz.

Q.192 (a)

A PSK signal requires a bandwidth equal to its baud rate

For 4 –PSK the baud rate is half of the bit rate

$$\Longrightarrow \text{Baud rate } \frac{1}{2}\times 2000 = 1000$$

⟹ Bandwidth =1000

Q.193 (d)

The effective bandwidth is 11000-1000 =10000Hz.

For a full – duplex transmission , this bandwidth will be divided into half, one for each direction.

$$\text{Bandwidth} = \frac{10000}{2} = 5000\text{Hz}$$

Q.194 (c)

The carrier frequencies can be taken at the middle of each band.

∴ f_c (forward direction)

$$= \frac{1000+5000}{2} = 3500\text{Hz}$$

Similarly f_c (backward direction)

$$= \frac{1000-3000}{2} = 8500\text{Hz}$$

Q.195 (c)

As transmission is full – duplex

⇒ Bandwidth for each direction =

$$\frac{1}{2}\times 12000 = 6000\text{Hz}$$

Let f_{c1} and f_{c0} be the carrier frequencies

We know, bandwidth

= Baud rate +(f_{c1} - f_{c0})

= 6000-2000 = 4000 bps

Q.196 (a)

Recall that for PSK the baud rate is same as bandwidth.

Q.197 (a)

Given, transmission rate is 5 Mbps.

⟹ Bit time is 20 ns.

In 200 ns, the signal travels 40 meters.

Insertion of one new station adds as much delay as insertion of 40 meters of cable.