CHAPTER - 1: INTRODUCTION

Q1] Describe the OSI Reference Model with a neat diagram

Ans: **[10M – May15]**

1. The users of a computer network are located all over the world.
2. Therefore International group of standards has been developed to ensure that nationwide and worldwide data communication systems can be developed and are compatible to each other.
3. This standards will fit into a framework which has been developed by the **"International Organization of Standardization (ISO)"**.
4. This framework is called as OSI Model.
5. OSI Model Stands for Open Systems Interconnection Model.
6. OSI Model has **7 Layers**.

OSI REFERENCE MODEL:

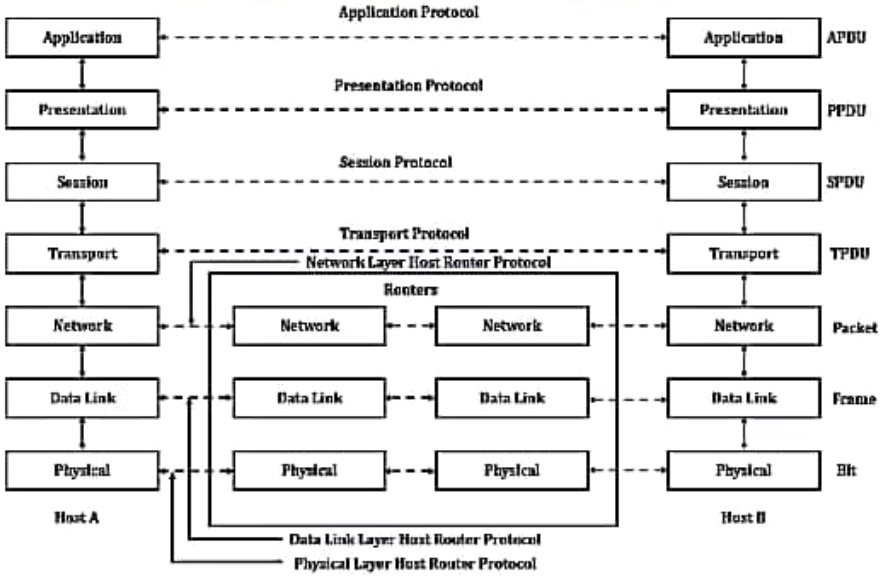


Figure 1.1: OSI Reference Model.

1) Physical Layer:

- It is the bottom layer of OSI Model.
- It is responsible for the actual physical connection between the devices. Such physical connection may be made by **using twisted pair cable**.

- It is concerned with transmitting bits over a communication channel.
- **Functions of Physical Layer:**
  - It defines the transmission rate.
  - Transforming bits into signals.
  - Provides synchronization of bits by a clock.
  - It defines the way in which the devices are connected to the medium.
  - It can use different techniques of multiplexing.

II) Data Link Layer:

- It is responsible for **node-to-node delivery of data.**
- It receives the data from network layer and creates FRAMES, add physical address to these frames & pass them to physical layer.
- It consist of 2 layers:
  - Logical Link Layer (LLC).
  - Medium Access Control (MAC).
- **Functions of Data Link Layer:**
  - It is used for synchronization and error control for the information.
  - It divides the bits received from Network layer into frames.
  - It provides Flow Control.
  - To enable the error detection, it adds error detection bits to the data which is to be transmitted.

III) Network Layer:

- It is responsible for the **source to destination delivery of a packet** across multiple networks.
- If two systems are attached to different networks with devices like routers, then Network layer is used.
- Thus Data Link Layer overseas the delivery of the packet between the two systems on same network and the network layer ensures that the packet gets its point of origin to its final destination.
- **Functions of Network Layer:**
  - It provides Internetworking.
  - Network Layer route the signals through various channels to the other end.
  - It is used in Logical Addressing.
  - It acts as a network controller for routing data.

IV) Transport Layer:

- It is responsible for **process-to-process delivery of the entire message.**

- Transport Layer looks after the delivery of entire message considering all its packets & make sure that all packets are in order.
- At the receiver side, Transport Layer provides services to application layer & takes services form network layer.
- At the source side, Transport Layer receives message from upper layer into packets and reassembles these packets again into message at the destination.
- **Functions of Transport Layer:**
  - It provides Connection Less & Connection Oriented Transmission.
  - It does the functions such as multiplexing, splitting or segmentation on the data.
  - It provides Error Control & Flow Control.
  - It is used for Port Addressing.

V) Session Layer:

- Session layer is the **fifth layer of OSI Model**.
- It has the responsibility of beginning, maintaining and ending the communication between two devices, called session.
- It also provides for orderly communication between devices by regulating the flow of data.
- **Functions of Session Layer:**
  - It manages & synchronizes the conversations between two different applications.
  - It controls logging on and off.
  - It is used for billing, user identification & session management.
  - It provides dialog control & dialog separation.

VI) Presentation Layer:

- Presentation layer is the **sixth layer of OSI Model**.
- It is concerned with the syntax & semantics of the information exchanged between the two devices.
- It works as translating layer.
- **Functions of Presentation Layer:**
  - It is used for data encryption, decryption and compression.
  - It ensures that the information delivered at receiver end is understandable & usable.
  - It is used for data presentation or translation of form and syntax.
  - **Example:** ASCII to EBCDIC and vice versa.

VII) Application Layer:

- It is the topmost i.e. **seventh layer of OSI Model**.
- It enables the user to access the network.

- It provides user interface & supports for services such as e-mail, file transfer, access to the World Wide Web.
- So it provides services to different user applications.
- **Functions of Application Layer:**
  - Application Layer provides various E-mail Services.
  - It allows users to access files in a remote host, to retrieve files from remote computer for use etc.
  - It is provides Remote Login.

Q2] Why there is a need for layered designing for networking and communication? Compare the TCP/IP and OSI reference models.

Ans: **[10M – Dec14]**

NEED FOR LAYERED DESIGNING FOR NETWORKING AND COMMUNICATION:

1. The first computer networks were designed with the hardware as the main concern and the software as an afterthought.
2. This strategy no longer works.
3. Network software is now highly structured.
4. To reduce their design complexity, most networks are organized as a stack of layers or levels, each one built upon the one below it.
5. The number of layers, the name of each layer, the contents of each layer, and the function of each layer differ from network to network.
6. The purpose of each layer is to offer certain services to the higher layers while hiding those layers from the details of how the offered services are actually implemented.
7. In a sense, each layer is a kind of virtual machine, offering certain services to the layer above it.
8. Therefore Layered Architecture provides Flexibility to modify and develop network services.

Example:

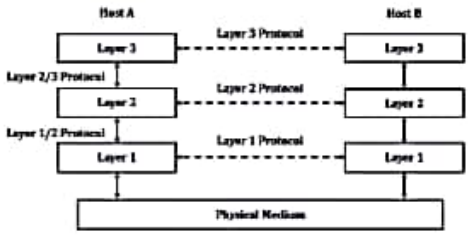


Figure 1.2: Example of 3 Layer Network.

Given in figure 1.2 is a three-layer network. When layer n on one machine carries on a conversation with layer n on another machine, the rules and conventions used in this conversation are collectively known as the layer n protocol.

COMPARISON BETWEEN TCP/IP AND OSI REFERENCE MODELS:

Similarities:

1. Both the model are based on the concept of "Stack" of independent protocols.
2. All layers from bottom till the transport layer provide end to end transport service.
3. All layers above the transport layer are application oriented and use the transport service.

Differences:

Table 1.1: Comparison between OSI & TCP/IP Model.

OSI Model	TCP/IP Model
It has 7 layers.	It has 4 layers.
Transport layer guarantees the delivery of data.	Transport layer does not guarantees the delivery of data.
Follows **horizontal approach**.	Follows **vertical approach**.
It has a separate presentation layer.	No separate presentation layer.
OSI is a general model.	TCP/IP model cannot be used in any other application hence it is not general model.
It is **less reliable**.	It is **more reliable**.
OSI model has a problem of fitting the protocols in the model.	TCP/IP model does not fit any protocol.
Protocols are hidden in OSI model and are easily replaced as the technology changes.	In TCP/IP replacing protocol is not easy.
Network layer of OSI model provide both connection oriented and connectionless service.	The Network layer in TCP/IP model provides connectionless service.
OSI provides layer functioning and also defines functions of all the layers.	TCP/IP model is more based on protocols and protocols are not flexible with other layers.
OSI model defines services, interfaces and protocols very clearly and makes clear distinction between them.	In TCP/IP it is not clearly separated its services, interfaces and protocols.

Q3] What is ISO-OSI reference model? Compare it with TCP/IP reference model. Which layer is used for the following?

(i) To route packets.
(ii) To convert packets to frame.
(iii) To detect and correct errors.
(iv) To run services like FTP, Telnet etc.

Ans: **[10M – May17]**

OSI REFERENCE MODEL:

Refer Q1.

COMPARISON BETWEEN TCP/IP AND OSI REFERENCE MODELS:

Refer Q2 Comparison Part.

LAYERS USED FOR THE FOLLOWING:

(i) **To route packets:** Network Layer.

(ii) **To convert packets to frame:** Data Link Layer.

(iii) **To detect and correct errors:** Transport Layer.

(iv) **To run services like FTP, Telnet etc.:** Application Layer.

Q4] Discuss the design issues for various layers.

Q5] List design issues in OSI layers.

Ans: **[Q4 | 5M – Dec15 & May15] & [Q5 | 5M – Dec16]**

The following are the design issues for the layers:

I) **Addressing:**

- There are multiple processes running on one machine.
- Every layer needs a mechanism to identify senders and receivers.
- Since there are multiple possible destinations, some form of addressing is needed in order to specify a specific destination.

II) **Direction of Transmission:**

- Based on system communication, system are classified as:
  - Simplex Systems.

- Half Duplex Systems.
- Full Duplex Systems.

III) Scalability:

- When network gets large, new problem arises.
- Thus scalability is important so that network can continue to work well when it gets large.

IV) Routing:

- When there are multiple paths between source and destination, only one route must be chosen.
- This decision is made on the basis of several routing algorithms, which chooses optimized route to the destination.

V) Reliability:

- It is a design issue of making a network that operates correctly even when it is made up of unreliable components.

VI) Error Control:

- It is an important issue because physical communication circuits are not perfect.
- Many error detecting and error correcting codes are available.
- Both sending and receiving ends must agree to use any one code.

VII) Flow Control:

- If there is a fast sender at one end sending data to a slow receiver, then there must be flow control mechanism to control the loss of data by slow receivers.
- There are several mechanisms used for flow control such as increasing buffer size at receivers, slow down the fast sender, and so on.
- Some process will not be in position to accept arbitrarily long messages.
- This property leads to mechanisms for disassembling, transmitting and the reassembling messages.

VIII) Multiplexing and De-multiplexing:

- If the data has to be transmitted on transmission media separately, it is inconvenient or expensive to setup separate connection for each pair of communicating processes.
- So, multiplexing is needed in the physical layer at sender end and de-multiplexing is need at the receiver end.

IX) Confidentiality and Integrity:

- Network security is the most important factor.
- Mechanisms that provide confidentiality defend against threats like eavesdropping.
- Mechanisms for integrity prevent faulty changes to messages.

Q6] Compare various types of network topologies.

Ans: **[5M – Dec15]**

***** Note: We have explained the answer in detail. Cut short it for 5 Marks as per understanding.**

1. A connection between two devices are called a link.
2. A topology represents the relationship of all the links and devices.
3. Network topologies describe the ways in which the elements of a network are mapped.
4. They describe the physical and logical arrangement of the network nodes.

I) Bus Topology:

Features:

- Bus Topology is the simplest of network topologies.
- In this topology, no point to point connection exist.
- A long cable acts as the backbone.
- Devices are connected to the backbone using drop lines and taps.
- If device A wants to send data to device B, Device A puts the data on the backbone along with the address of device B.
- All the device receive the data but only Device B can accept the information.

Diagram:

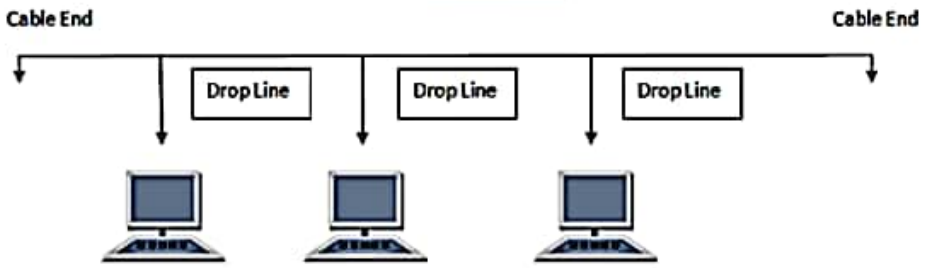


Figure 1.3: Bus Topology.

Advantages:

- It is cost effective.
- Cable required is least compared to other network topology.
- Used in small networks.
- It is easy to understand & Easy to expand joining two cables together.

Disadvantages:

- If the Central Cables fails then whole network fails.
- If network traffic is heavy or nodes are more the performance of the network decreases.
- Cable has a limited length.
- It is slower than the ring topology.

II) Ring Topology:

Features:

- In this topology, each device is connected to the next device; with the last device connected back to the first device.
- Data is passed along the ring from Device to Device until it reaches the destination device.
- Data is passed in one direction only.
- Each device incorporates a repeater.
- Sending and receiving of data takes place by the help of TOKEN.

Diagram:

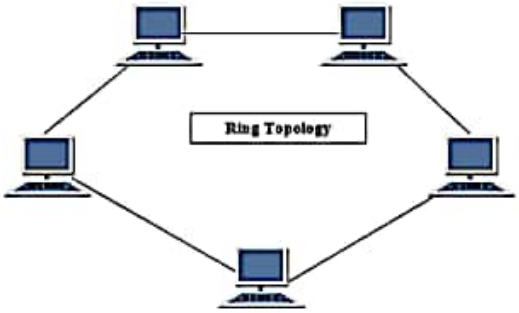


Figure 1.4: Ring Topology.

Advantages:

- Transmitting network is not affected by high traffic or by adding more nodes, as only the nodes having tokens can transmit data.
- Cheap to install and expand.

Disadvantages:

- Troubleshooting is difficult in ring topology.
- Adding or deleting the computers disturbs the network activity.
- Failure of one computer disturbs the whole network.

III) Star Topology:

Features:

- In Star topology, all the components of network are connected to the central device.
- Central Device may be a hub, a router or a switch.
- In Star Topology, all the workstations are connected to central device with a point-to-point connection.
- When the Device A wants to send the data to the Device B, Device A send the data to the central device (Hub) then the central device sends this data to Device B.

Diagram:

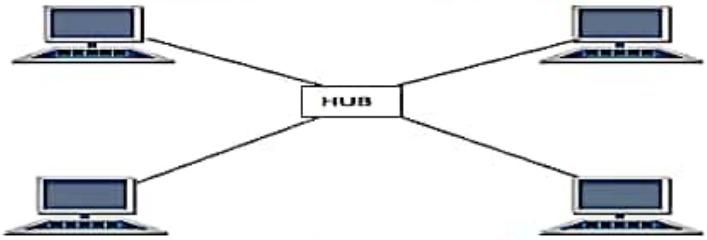


Figure 1.5: Star Topology.

Advantages:

- Fast performance with few nodes and low network traffic.
- Hub can be upgraded easily.
- Easy to troubleshoot, setup and modify.
- Only that node is affected which has failed, rest of the nodes can work smoothly.

Disadvantages:

- Cost of installation is high.
- Expensive to use.
- If the hub fails then the whole network is stopped because all the nodes depend on the hub.
- Performance is based on the hub that is it depends on its capacity.

IV) Mesh Topology:

Features:

- In this topology, every device is connected to every another device via a dedicated point to point link.
- The networks can consist of unidirectional and bidirectional links.
- Every node not only sends its own signals but also relays data from other nodes.
- This type of topology is very expensive as there are many redundant connections, thus it is not mostly used in computer networks.
- It is commonly used in wireless networks.
- Flooding or routing technique is used in mesh topology.

Diagram:

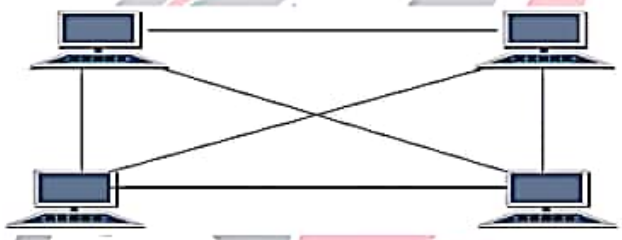


Figure 1.6: Mesh Topology.

Advantages:

- Each connection can carry its own data load.
- It is robust.
- Fault is diagnosed easily.
- Provides security and privacy.

Disadvantages:

- Installation and configuration is difficult.
- Cabling cost is more.
- Bulk wiring is required.

V) Tree Topology:

Features:

- Tree Topology integrates the characteristics of Star and Bus Topology.
- In Tree Topology, the number of Star networks are connected using Bus.
- The central cable seems like a main stem of a tree, and other star networks as the branches.

- It is also called Expanded Star Topology.
- Ethernet protocol is commonly used in this type of topology.

Diagram:

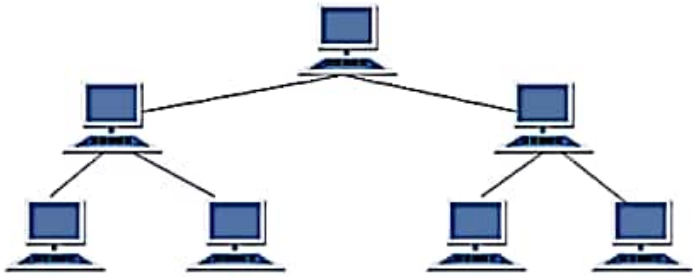


Figure 1.7: Tree Topology.

Advantages:

- Extension of bus and star topologies.
- Expansion of nodes is possible and easy.
- Easily managed and maintained.
- Error detection is easily done.

Disadvantages:

- Heavily cabled.
- Costly.
- If more nodes are added maintenance is difficult.
- Central hub fails, network fails.

Q7] Internetworking Devices.

Ans: **[10M – Dec15]**

1. Internetworking devices move data across a network.
2. Internetworking devices operate at OSI layers above the physical layer.
3. Figure 1.8 shows the different types of internetworking devices.

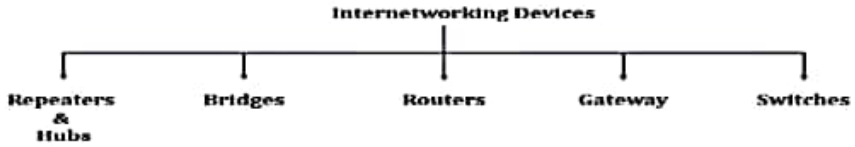


Figure 1.8: Different types of internetworking devices.

I) Repeater:

- It is the electronic device that operates on only physical layer of OSI Model.
- Signals get attenuated as they travel along the time.
- **Process of repeater:**
  - Receive the signal.
  - Regenerate the signal.
  - Transmit the signal.
- Repeater can extend physical length of the LAN.
- Repeater is not the amplifier because amplifier simply amplify the entire incoming signal along with noise.
- Figure 1.9 shows devices interconnection using repeater.

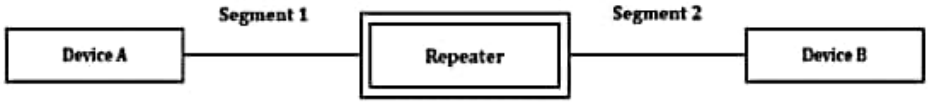


Figure 1.9: Internetworking using Repeater.

II) Hubs:

- It is the device that operates on only physical layer of OSI Model.
- Hub is referred as any connecting device.
- It is called as Multiport Repeater.
- It is normally used for connecting stations in a physical star topology.
- All network require a central location to bring media segments together.
- This central locations are called as Hubs.
- Figure 1.10 shows devices interconnection using hubs.

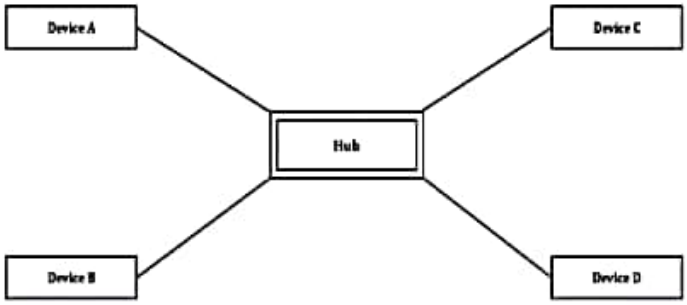


Figure 1.10: Internetworking using Hub.

III) Bridges:

- A bridge operates in the physical layer as well as in the Data Link Layer.
- As a Data Link Layer Device, it can check the MAC Address of source and destination contained in the frame.
- **Process of bridge:**
  - Regenerate the signal.
  - Read the address present on the signal.
  - Find the port number by using the address in the bridge table.
  - Transmit the regenerated signal on the port found in previous step.
- **Example of bridge table is shown below:**

Address	Port
732B134561	1
732B134562	1
642B124651	2
642B124652	2

- Main task of bridge computer is to receive and pass data from one LAN to another.
- Figure 1.11 shows devices interconnection using bridge.

Figure 1.11: Internetworking using Bridge.

IV) Switches:

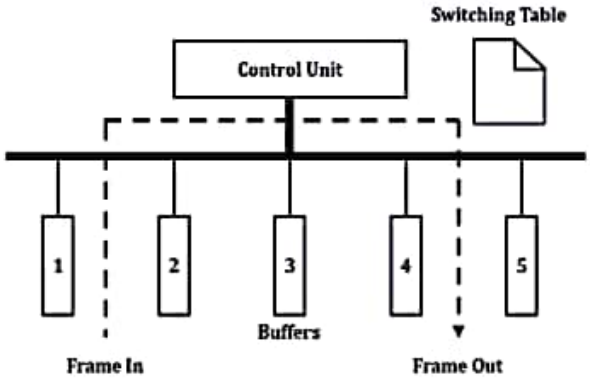


Figure 1.12: Internetworking using Switch.

- Figure 1.12 shows devices interconnection using switch.
- A switch is a device operates in the Physical Layer as well as Data Link Layer.
- It is called as Multiport Bridge.
- It provides bridging functionality with greater efficiently.
- The switch has the buffer for each link to which it is connected.
- When it receives the packet, it stores the packet in the buffer of receiving link and checks the address to find the outgoing link.
- No collision takes place.

V) Routers:

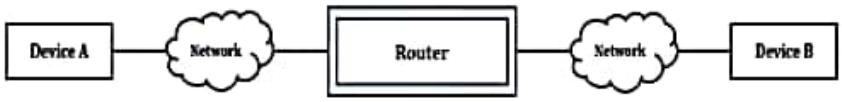


Figure 1.13: Internetworking using Router.

- Figure 1.13 shows devices interconnection using router.
- Router is the device that operates in Network Layer of OSI Model.
- It is used to connect two or more networks.
- They consist of combination of hardware and software.
- The hardware can be network server or a separate computer.
- The software in a router are the operating system and the routing protocol.
- Routers use logical and physical address to convert two or more logically separated networks.

VI) Gateways:

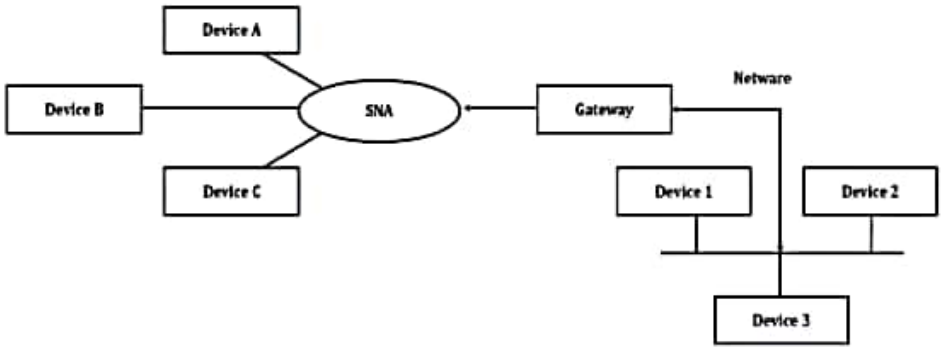


Figure 1.14: Internetworking using Gateway.

- Figure 1.14 shows devices interconnection using gateway.
- Gateway operates on all the layers of OSI Model.
- Gateway is used to connect the network with different protocols.
- Gateway is the device that can interpret and translate the different protocols that are used on two distinct networks.
- Gateways comprise of software, dedicated hardware or combination of both.
- Gateway is the considered as protocol converter.
- A gateway can convert the data so that is works with an application on the computer on the other side of the gateway.

Q8] Explain TCP/IP Model.

Ans: **[4M - May16]**

***** Note: We have explained the answer in detail. Cut short it for 5 Marks as per understanding.**

1. TCP/IP Stands for Transmission Control protocol (TCP) and the Internet Protocol (IP).
2. TCP/IP defines how the data should be processed, transmitted and received on a TCP/IP Network.
3. TCP/IP describe the movement of data between the host computers on Internet.
4. A system of related protocols, such as TCP/IP protocols is called as Protocol Suite.
5. There are four Layers in TCP/IP Protocol Suite.

FEATURES OF TCP/IP:

1. Logical Addressing.
2. Error Checking & Flow Checking.
3. Routing.
4. Application Support.

TCP/IP PROTOCOL SUITE:

Figure 1.15 shows TCP/IP Protocol Suite.

I) Host To Network Layer:

- It is also called as **Network Interface Layer.**
- It is combination of Physical & Data Link Layer of OSI Model.
- TCP/IP Protocol Suite does not define any protocol at these layers.
- In this layer, hardware device reside and it provides support for standard protocols.

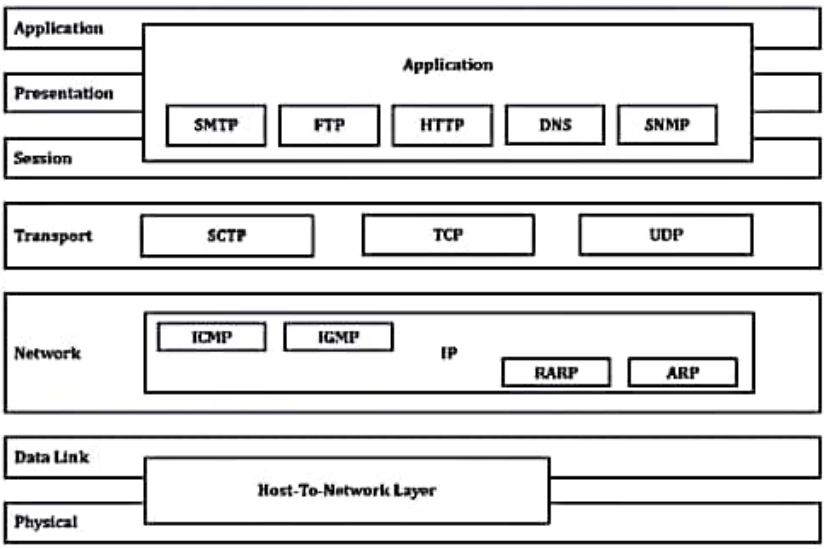


Figure 1.15: TCP/IP Protocol Suite.

II) **Internet Layer:**

- IP is the **primary protocol** in network layer.
- The task of this layer is to deliver the datagram from source host to destination host.
- IP is unreliable and connectionless protocol.
- It provides best effort delivery service.
- It includes:

  - **ICMP:**
    - It stands for Internet Control Message Protocol.
    - ICMP is a mechanism used by routers to send error or control message to other routers or hosts.
  - **IGMP:**
    - IGMP stands for Internet Group Message Protocol.
    - It is used to manage IP Multicast data and enables transmission of messages to a group of recipient simultaneously.
  - **ARP:**
    - ARP stands for Address Resolution Protocol.
    - It is used to convert logical (IP) address to physical address.

- **RARP:**
  - ARP stands for Reverse Address Resolution Protocol.
  - It is used to convert physical address to logical (IP) address.

III) Transport Layer:

- This is layer above the internet layer.
- Its functions are same as those of a transport layer in OSI Layer.
- It includes:

- **TCP:**
  - It stand for Transmission Control Protocol.
  - It is connection oriented and reliable protocol.
  - It provides the function for reliable transmission of data across the network.
  - It is used to handle error control & flow control.

- **UDP:**
  - It stands for User Datagram Protocol.
  - It is connection less and unreliable protocol.
  - It takes the data from application layer then packages it into datagram and sends it to network layer.
  - It does not provides error control and flow control.

- **SCTP:**
  - It stands for Stream Control Transmission Protocol.
  - It combines the good features of TCP & UDP.

IV) Application Layer:

- The layer on top of transport layer is called as Application Layer.
- The protocols related to this layer are all high level protocols.
- It includes:

- **SMTP:**
  - It stands for Simple Mail Transfer Protocol.
  - It is the protocol for sending E-Mail Message between servers.

- **SNMP:**
  - It stands for Simple Network Management Protocol.
  - It is the framework for managing the devices on the internet using TCP/IP Protocol Suite.
- **HTTP:**
  - It stands for Hyper Text Transfer Protocol.
  - It is used to access data on World Wide Web.
- **FTP:**
  - It stands for File Transfer Protocol.
  - It is used to exchange the files between computers on internet.
- **DNS:**
  - Its stands for Domain Name System.
  - It is used to identify the network and the computer on the network by some Domain Name instead of IP Address.

Q9] Compare Connection-Oriented & Connection-Less Services.

Ans: **[4M – May16]**

Table 1.2: Comparison between Connection-Oriented & Connection-Less Services.

Criteria	Connection-Oriented	Connection-Less
Connection	Prior connection needs to be established.	No prior connection is established.
Resource Allocation	Resources need to be allocated.	No prior allocation of resource is required.
Reliability	It ensures reliable transfer of data.	Reliability is not guaranteed as it is a best effort service.
Congestion	Congestion is not at all possible.	Congestion can occur likely.

Transfer mode	It can be implemented either using Circuit Switching or VCs.	It is implemented using Packet Switching.
Retransmission	It is possible to retransmit the lost data bits.	It is not possible.
Suitability	It is suitable for long and steady communication.	It is suitable for bursty transmissions.
Signaling	Connection is established through process of signaling.	There is no concept of signaling.
Packet travel	In this packets travel to their destination node in a sequential manner.	In this packets reach the destination in a random manner.
Delay	There is more delay in transfer of information, but once connection established faster delivery.	There is no delay due absence of connection establishment phase.

CHAPTER - 2: PHYSICAL LAYER

Q1] Explain the modes of propagating light along optical channels. What are the advantages over other guided media?

Ans: **[10M - Dec14]**

1. Modes refer to the number of paths followed by light rays inside the optical cable.
2. There exist two modes for propagating light all along the optical channels.
   a. Single Mode.
   b. Multiple Mode.
3. In Single mode, light follows a single path through the core.
4. In Multiple mode, the light takes more than one paths through the core.
5. Figure 2.1 shows Propagation Modes in optical Fibers.

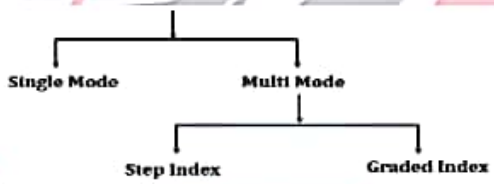


Figure 2.1: Propagation Modes in Optical Fibers.

I) Single Mode:

- Single Mode Fibers **support one mode of propagation.**
- The optical signal which travels inside the fiber has only one group velocity.
- In this mode, the amount of dispersion is less as compared to multimode fibers.
- In this mode, the fiber consist extremely small diameter.
- These small diameter limits the beams to the few angles, which causes almost horizontal beam.
- As the critical angle is close to 90 degree, the propagation of different beams is more or less similar.
- In this mode, the delays are negligible and the signal reconstruction is easier.
- Figure 2.2 shows the Propagation in Single Mode Fiber.

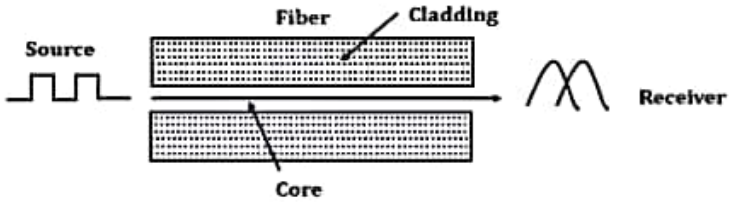


Figure 2.2: Propagation in Single Mode Fiber.

II) **Multi-Mode:**

- Multi-Mode Fibers support simultaneous propagation of many modes.
- Each mode has its own group velocity.
- Each mode follows its own path while travelling from the transmitter to receiver.
- Due to presence of more than one modes, the intermodal dispersion exist.
- Multi-Mode Fibers can have step index or graded index profile.
- They are fabricated using the multicomponent glasses or doped silica.
- Figure 2.3 shows the propagation in multi-mode fiber.

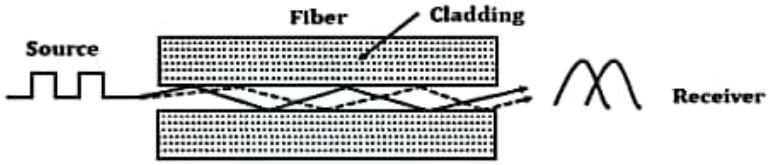


Figure 2.3: Propagation in Multi-Mode Fiber.

ADVANTAGES OVER OTHER GUIDED MEDIA:

1. **Small Size & Light Weight:**

- The size (Diameter) of the optical fibers is very small.
- Therefore a large number of optical fibers can fit into a cable of small diameter.

2. **Easy Available & Low Cost:**

- Silicon glass is used in manufacturing of optical fibers.
- Silicon glass is easily available.
- So the optical fibers cost lower than the cable with metallic conductors.

3. **Higher bandwidth:**

- The bandwidth of optical fibers is extremely large because the light rays have a very high frequency in the GHz range.
- Larger bandwidth offers larger capacity and faster transmission rate.

4. **High security:**

- Using fiber optic cables prevents the emanation of radiation.
- Therefore, radiation-containing signal becomes difficult to tap.
- This makes fiber cable secure against signal leakage and interference.

5. **Free from electrical problems:**

- It does not require electrical ground loop preventing it from short circuit as light waves are being used the carrier of data signal.
- It is also safe in combustible areas (no arching) and offers immunity to lightning and electrical discharges.

6. **Less signal Attenuation:**

- It has transmission distance significantly greater than that of other guided media.

7. **Less number of repeaters:**

- A repeater used to strengthen a signal is always required during the Course of signal transmission.
- Compared to copper media, it requires less number of repeaters.

8. **Other Advantages:**

- Signal can send up to 100 times faster.
- Installation is easy as the optic fiber cables are flexible.
- No cross talk inside the optical fiber cable.

Q2] Write Short Notes on: Virtual LAN.

Ans: **[5M – Dec14, May16 & Dec16]**

1. A Virtual LAN (VLAN) is considered as any broadcast domain.
2. These Broadcast domain is partitioned and isolated in a computer network at the data link layer (OSI layer 2).
3. A VLAN is a set of end stations and the switch ports that connect them.
4. End stations & ports should belong to the same VLAN.
5. To subdivide a network into virtual LANs, we need to configure a network switch or router.
6. Simpler network devices can only partition per physical port.
7. More sophisticated devices can mark packets through tagging, so that a single interconnect may be used to transport data for multiple VLANs.
8. VLAN provides the benefits of both bridging and routing.
9. Like a bridge, a VLAN switch forwards traffic based on the Layer 2 header, which is fast.
10. Like a router, it partitions the network into logical segments, which provides better administration, security, and management of multicast traffic.

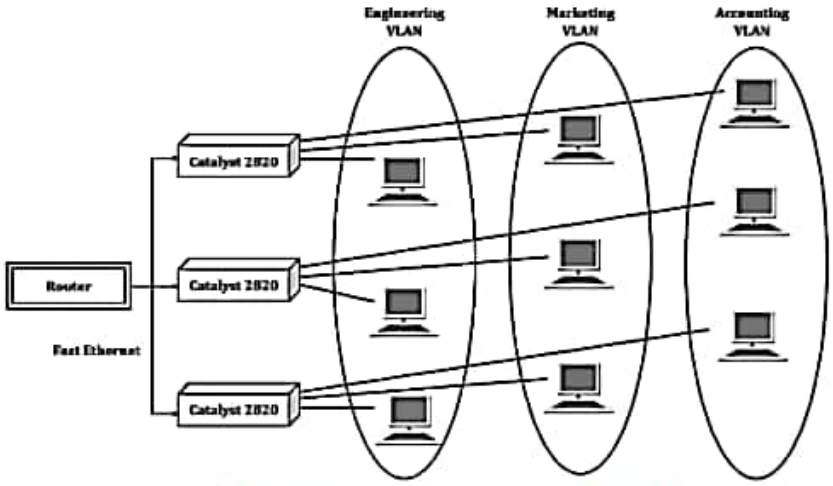


Figure 2.4: Virtual LAN Example.

11. VLANs allow network administrators to group hosts together even if the hosts are not on the same network switch.
12. VLANs can be used to partition a local network into several distinctive segments for example:
    a. Voice over IP.
    b. Network management.
    c. Storage area network. (SAN)
    d. Guest network.
    e. Demilitarized zone. (DMZ)
    f. Client separation.

Q3] List the advantages of fiber optics as a communication medium

Ans: **[SM – Dec16]**

ADVANTAGES:

1. **Wide Bandwidth:**

- **Potential information carrying capacity** increases with the bandwidth of the transmission medium and with the frequency of the carrier.
- The wide bandwidth of a fiber allows signals to be multiplexed through the fiber.

2. **Light Weight:**
- A glass fiber weighs less than a copper conductor.
- A fiber-optic cable with the same information-carrying capacity as a copper cable weighs less than the copper cable since the copper requires more lines than the fiber.

3. **Small Size:**
- A fiber-optic cable is smaller than its copper counterparts.
- A single fiber can replace several copper conductors.
- The small size of fiber-optic cables makes them attractive for applications where space is at a premium.

4. **Safety:**
- A fiber is a dielectric, i.e. it does not carry electricity.
- It presents no spark or fire hazard, so it cannot cause explosions or fires as a faulty copper cable can.
- It does not attract lightning.

5. **Security:**
- Fiber optics is a **highly secure transmission medium.**
- It does not radiate energy that can be received by nearly antenna, and it is extremely difficult to tap a fiber.
- Both government and business consider fiber optics a secure medium for communication.

6. **Ruggedness and Flexibility:**
- Optical fibers have a very high tensile strength.
- The fibers may also be bent to quite small radii or twisted without damage.

7. **Electromagnetic Immunity:**
- Unlike copper cables, optical fibers do not radiate or pickup electromagnetic radiation.
- Optical fibers form a dielectric waveguides and are therefore free from electromagnetic interference (EMI), radio frequency (RF), etc.

8. **Low Transmission Loss:**
- Fibers have been fabricated with losses as low as 0.2dB/km and this feature has become a major advantage of optical fiber communication.

Q4] Bluetooth Architecture

Ans: **[10M – May17]**

BLUETOOTH ARCHITECTURE:

1. Bluetooth is one of the major wireless technologies developed to achieve WPAN.
2. Bluetooth is a wireless LAN technology used to connect devices of different functions such as telephones, computers (laptop or desktop), notebooks, cameras, printers and so on.
3. Bluetooth is used for providing communication between peripheral devices like wireless mouse or keyboard with the computer.
4. It is used by modern healthcare devices to send signals to monitors.
5. It can also be used for file transfer operations from one mobile phone to another.
6. Bluetooth architecture defines two types of networks:

1. Piconet:

- Piconet is a Bluetooth network that consists of one primary (master) node and seven active secondary (slave) nodes.
- Thus, piconet can have upto eight active nodes (1 master and 7 slaves) or stations within the distance of 10 meters.
- There can be only one primary or master station in each piconet.
- The communication between the primary and the secondary can be one-to-one or one-to-many.
- All communication is between master and a slave. Salve-slave communication is not possible.
- In addition to seven active slave station, a piconet can have upto 255 parked nodes.
- These parked nodes are secondary or slave stations and cannot take part in communication until it is moved from parked state to active state.
- Figure 2.5 shows the Piconet Architecture.

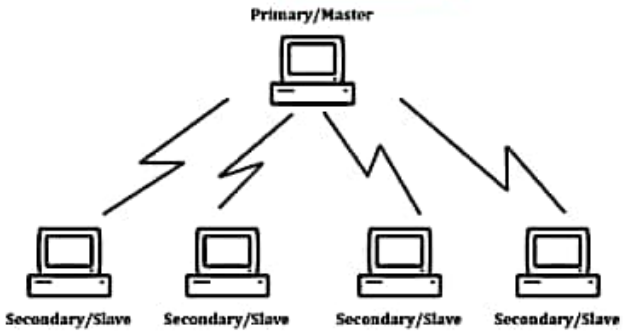


Figure 2.5: Piconet.

2. **Scatternet:**

- Scatternet is formed by combining various piconets.
- A slave in one piconet can act as a master or primary in other piconet.
- Such a station or node can receive messages from the master in the first piconet and deliver the message to its slaves in other piconet where it is acting as master.
- This node is also called **bridge slave.**
- Thus a station can be a member of two piconets.
- A station cannot be a master in two piconets.
- Figure 2.6 shows Scatternet Architecture.

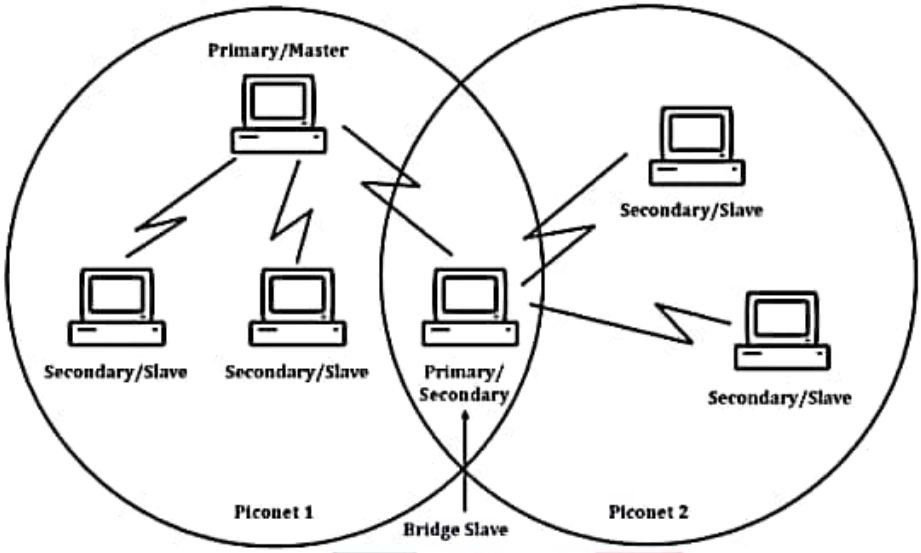


Figure 2.6: Scatternet.

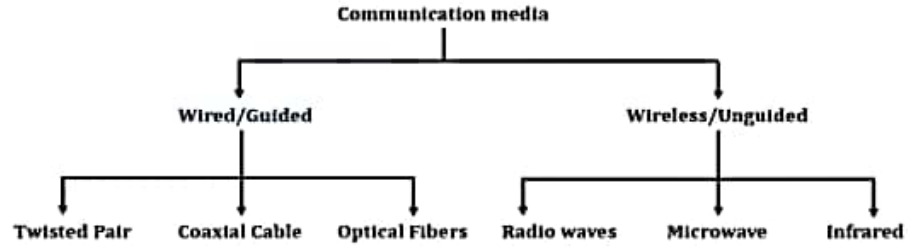
Q5] What are the different guided and unguided transmission media?

Ans: **[5M – May17]**

TRANSMISSION MEDIA:

1. Transmission media is a pathway that carries the information from sender to receiver.
2. We use different types of cables or waves to transmit data.
3. Data is transmitted normally through electrical or electromagnetic signals.
4. Transmission media is also called **Communication channel.**

TYPES OF TRANSMISSION MEDIA:



Transmission media is broadly classified into two groups:

I) **Wired or Guided Media or Bound Transmission Media:**

- Bound transmission media are the cables that are tangible or have physical existence and are limited by the physical geography.
- Popular bound transmission media in use are **twisted pair cable, co-axial cable and fiber optical cable.**
- Each of them has its own characteristics like transmission speed, effect of noise, physical appearance, cost etc.

II) **Wireless or Unguided Media or Unbound Transmission Media:**

- Unbound transmission media are the ways of transmitting data without using any cables.
- These media are not bounded by physical geography.
- This type of transmission is called **Wireless Communication.**
- Nowadays wireless communication is becoming popular.
- Wireless LANs are being installed in office and college campuses.
- This transmission uses **Microwave, Radio wave, Infrared are some of popular unbound transmission media.**

CHAPTER - 3: DATA LINK & MAC LAYER

Q1] Explain CSMA Protocols. Explain how collisions are handled in CSMA/CD.
Q2] Write brief about: CSMA/CD.
Q3] Explain 1-persistent, p-persistent and 0-persistent CSMA giving strong and weak points of each.

Ans: [Q1 | 10M – Dec14, May15 & Dec16], [Q2 | 5M – Dec15] & [Q3 | 10M – May17]

***** Note: Cut short the answer for 5 Marks.**

CSMA:

1. CSMA Protocols stands for **Carrier Sense Multiple Access Protocols.**
2. CSMA is a network access method used on shared network topologies such as Ethernet to control access to the network.
3. Hence, CSMA Protocol operates on the principal of carrier sensing.
4. Devices attached to the network cable listen (carrier sense) before transmitting.
5. If the channel is in use, devices wait before transmitting.
6. MA (Multiple Access) indicates that many devices can connect to and share the same network.
7. All devices have equal access to use the network when it is clear.

TYPES OF CSMA PROTOCOLS:

I) Persistent CSMA:

1. In this method, station that wants to transmit data continuously senses the channel to check whether the channel is idle or busy.
2. If the channel is busy, the station waits until it becomes idle.
3. When the station detects an idle-channel, it immediately transmits the frame with probability
4. Hence it is called **1-persistent CSMA.**
5. This method has the highest chance of collision because two or more stations may find channel to be idle at the same time and transmit their frames.
6. When the collision occurs, the stations wait a random amount of time and start all over again.

Advantages:

Due to carrier sense property 1-persistent CSMA gives better performance than the ALOHA systems.

Disadvantages:

Propagation Delay.

II) Non-Persistent CSMA:

1. In this scheme, if a station wants to transmit a frame and it finds that the channel is busy (some other station is transmitting) then it will wait for fixed interval of time.
2. After this time, it again checks the status of the channel and if the channel is free it will transmit.
3. A station that has a frame to send senses the channel.
4. If the channel is idle, it sends immediately.
5. If the channel is busy, it waits a random amount of time and then senses the channel again.
6. In non-persistent CSMA the station does not continuously sense the channel for the purpose of capturing it when it detects the end of previous transmission.

Advantages:

It reduces the chance of collision and leads to better channel utilization,

Disadvantages:

It reduces the efficiency of network because the channel remains idle and it leads to longer delays than 1-persistent CSMA.

III) P-Persistent CSMA:

1. It is used for **slotted channels.**
2. When a station becomes ready to send, it senses the channel.
3. In this method after the station finds the line idle, it may or may not send.
4. If a station senses an idle channel it transmits with a probability p and refrains from sending by probability (1-p).

CSMA/CD:

1. CSMA/CD stands for **Carrier Sense Multiple Access/Collision Detection.**
2. Ethernet (IEEE 802.3) sends data using CSMA/CD.
3. Persistent and Non-persistent CSMA protocols are clearly an improvement over ALOHA.
4. It is because they ensure that no station begins to transmit when it senses the channel busy.
5. Now a further improvised CSMA, in the form of CSMA/CD has been brought about.
6. In this stations abort their transmission as soon as they detect a collision.

CSMA/CD PROCEDURE:

1. The station that has a ready frame sets the Back off parameter to zero.
2. Then it sense the line using one of the persistent strategies.
3. It then sends the frame.
4. If there is no collision for a period corresponding to one complete frame, then the transmission is successful.

5. Otherwise the station sends the Jam signal to inform the other stations about collision.
6. The station then increments the Back off Time & waits for a random Back off Time and sends the frame again.
7. If the Back off has reached its limit then the station aborts the transmission.
8. CSMA/CD is an important protocol.
9. IEEE 802.3 (Ethernet) is an example of CSMA/CD.
10. It is an International Standard.
11. The MAC Sub layer protocol does not guarantee reliable delivery.
12. Even in absence of collision the receiver may not have copied the frame correctly.
13. Figure 3.1 shows CSMA/CD Procedure.

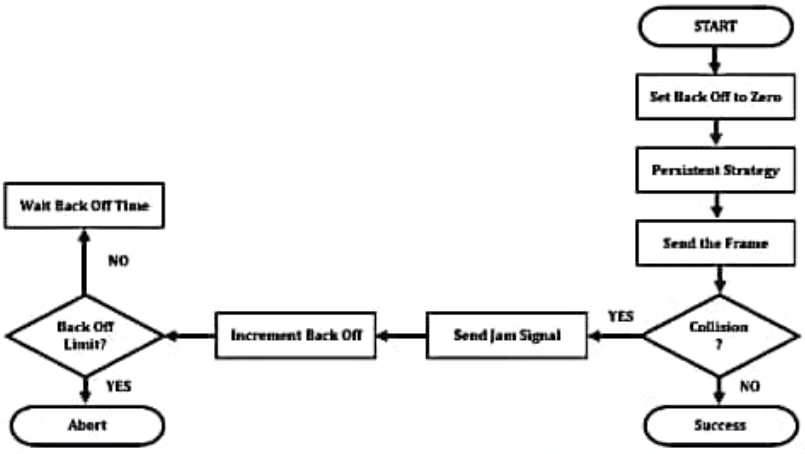


Figure 3.1: CSMA/CD Procedure.

HOW LONG WILL IT TAKE A STATION TO REALIZE THAT A COLLISION HAS TAKEN PLACE?

1. Let the time for a signal to propagate between the two stations be $\tau\tau$.
2. Assume that at time t_0, one station begins transmitting.
3. Let's call the most distant station B.
4. At time $\tau\tau - \varepsilon$, which is an instant before the signal arrives at B, B itself senses an idle channel and begins transmitting.
5. A collision occurs one instant later at time $\tau\tau$.
6. B detects the collision almost instantly and stops, but little noise burst caused by the collision does not get back to the original station until time $\tau\tau + \tau\tau = 2\tau\tau$.
7. In other words, in the worst case a station cannot be sure that it has seized the channel until it has transmitted for $2\ \tau\tau$ without hearing a collision.

Q4] Write Short Notes on: Ethernet.

Ans: **[5M – Dec14]**

ETHERNET:

1. For Wide Area Network, Internet & ATM was designed.
2. But in many applications, a large number of computers are to be connected to each other.
3. For this the Local Area Network (LAN) was introduce.
4. Ethernet is a family of computer networking technologies for local area networks (LANs) and metropolitan area networks (MANs).
5. It is the most popular LAN technology in the world.
6. It is an easy, relatively inexpensive way to provide high-performance networking to all different types of computer equipment.
7. The IEEE 802.3 standard is popularly called as Ethernet.
8. It is bus based broadcast network with decentralized control.
9. Ethernet was invented at Xerox PARC and developed jointly by Digital Equipment Corporation, Intel and Xerox.
10. Ethernet has largely replaced competing wired LAN technologies such as token ring, FDDI, and ARCNET.
11. Ethernet can operate at 10 Mbps or 100 Mbps or above.
12. Computers on an Ethernet can transmit whenever they want to do so.

ARCHITECTURE OF ETHERNET:

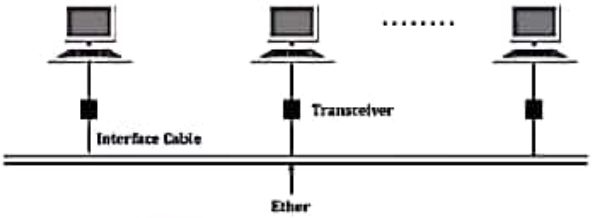


Figure 3.2: Architecture of Ethernet.

GENERATION OF ETHERNET:

1. **Traditional Ethernet:** It has Data Rate of 10 Mbps.
2. **Fast Ethernet:** It has Data Rate of 100 Mbps.
3. **Gigabit Ethernet:** It has Data Rate of 1000 Mbps.

Q5] Write in Brief about: PPP Frame Format

Ans: **[5M – Dec15]**

PPP FRAME FORMAT:

1. PPP stands for **Point-To-Point Protocol.**
2. It is **Data Link Protocol**.
3. This protocol is widely used to connect home computers to the server of an Internet Service Provider.
4. PPP is used to control and manage the data transfer.
5. PPP provides **Error Detection.**
6. It defines how two devices can authenticate each other.
7. It defines link control protocol (LCP) for:
   a. Establishing the link between two devices.
   b. Maintaining this established link.
   c. Configuring this link.
   d. Terminating this link after the transfer.

PPP FRAME FORMAT:

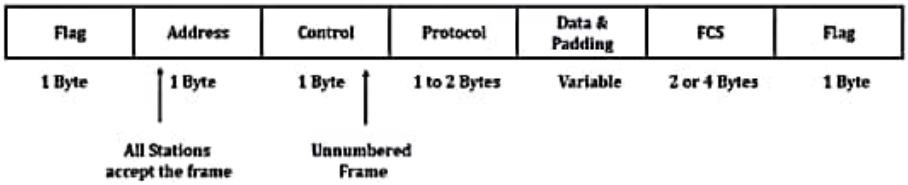


Figure 3.3: PPP Frame Format.

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

I) Flag field:

- PPP Frame always begin & end with the standard HDLC Flag.
- Flag byte is 01111110. (1 byte).

II) Address field:

- This field is of 1 byte and is always 11111111.
- This address is the broadcast address.
- All 1's in the address field indicates that all stations are to accept the frame.

III) Control field:

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

IV) Protocol field:

- This field specifies the kind of packet in the data field i.e. what is being carried in data field.
- The data field can contain the user data or other information.

V) Data field:

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

VI) FCS field:

- FCS stands for **Frame Check Sequence**.
- It is either of 2 bytes or 4 bytes.
- It contains the checksum.

Q6] Differentiate between Aloha & Slotted Aloha.

Ans: **[4M – May15]**

Table 3.1: Comparison between Aloha & Slotted Aloha.

Aloha	Slotted Aloha
Pure ALOHA do not required global time synchronization.	Slotted ALOHA requires the global time synchronization.
In Pure ALOHA, station can send data in continuous time manner.	In Slotted ALOHA, station cannot send data in continuous time manner. It divides the time in slot.
It allow the user whenever they have data.	It do not allow the user whenever they have data.
Vulnerable time for the Pure ALOHA is 2T.	Vulnerable time for Slotted ALOHA is T.
The average successful transmission for Pure ALOHA is Ge^{-2G}	The average successful transmission for Slotted ALOHA is Ge^{-G}
The max throughput is 0.184 when G=1/2.	The max throughput is 0.368 when G= 1.
Throughput Efficiency is Half as compared to Slotted ALOHA.	Throughput Efficiency is Double as compared to Pure ALOHA.

T: Time Required for one transmission.

COMPARISON DIAGRAM OF ALOHA & SLOTTED ALOHA:

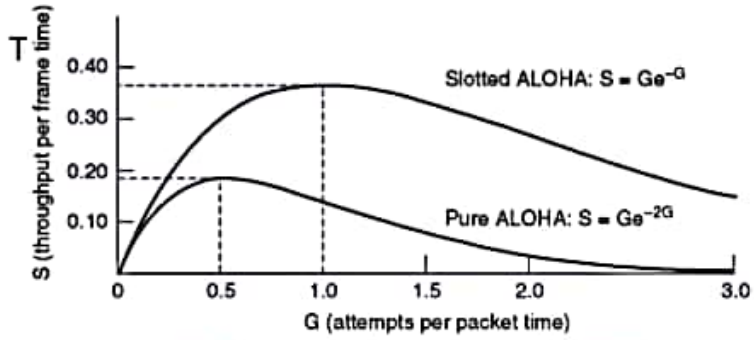


Figure 3.4: Comparison of ALOHA & Slotted ALOHA.

Q7] Why does the data link protocol always put the CRC in a trailer rather than in a header?

Ans: **[4M – May15]**

1. The Data Link Layer is the second layer of OSI Model.
2. It is responsible for node-to-node delivery of data.
3. It receives the data from network layer and creates FRAMES, add physical address to these frames & pass them to physical layer.
4. Data Link Layer delivers the frames using Hardware Address.
5. The CRC is computed while the packet is being transmitted and then incorporated in a trailer.
6. Similarly, the receiver computes the CRC and compares it with the transmitted one.
7. Thus it is more efficient to put CRC in a trailer.
8. Because only one pass needs to be made over the packet as it computes the CRC while scanning the packet, and then outputs it at the end (trailer).
9. If the CRC were in the header, then two passes would be necessary - one to compute the CRC, and one more to append it to the front of the packet.
10. Therefore using the trailer cuts the work in half.

Q8] Explain in short different framing methods.

Ans: **[4M – May15 & May16]**

1. The Data Link Layer takes packets from the Network Layer and converts them into frames.
2. Breaking the bit stream into frames is called as Framing.
3. One way of framing is by inserting the time gap between frames.
4. Figure 3.5 shows the Framing Example using Time gaps.

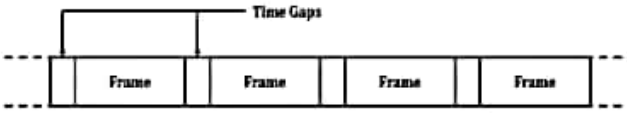


Figure 3.5: Framing Example using Time gaps.

FRAMING METHODS:

I) Character Count:

- The first field in the header specifies the number of characters in the frame.
- This number helps the receiver to know the number of characters in the frame following this count.

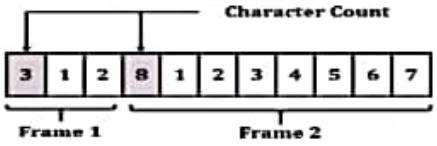


Figure 3.6: Character Count Method.

Disadvantage:

- Count may get garbled by a transmission error.

II) Character Stuffing:

- It is Character Oriented Protocol.
- Each frame starts and ends with a FLAG byte.
- Thus adjacent frames are separated by two flag bytes.
- **Problem:** It is possible that FLAG is actually a part of the data.
- **Solution:**
  - At the sender an ESC character is inserted just before the FLAG byte present in the data.
  - At the receiver the ESC is removed from the data.
  - Now if an ESC is present in the data then an extra ESC is inserted before it in the data.

- This extra ESC is removed at the receiver.

III) Bit Stuffing:

- It is Bit Oriented Protocol.
- Each frame begins and ends with a special bit pattern 01111110 called the flag byte.
- When sender's DLL encounters 5 consecutive 1's in the data it automatically stuffs a '0' bit in the outgoing data stream.
- When the receiver encounters 5 consecutive 1's followed by a '0' it removes the '0' bit.

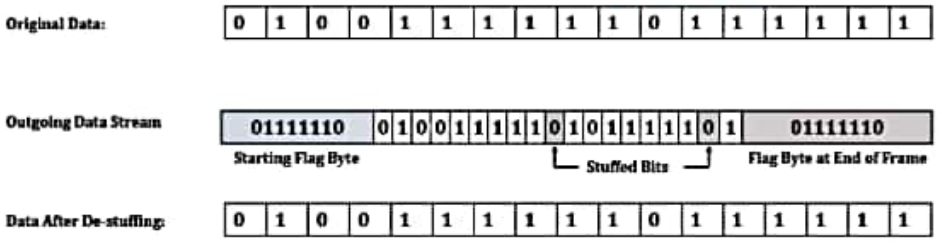


Figure 3.7: Bit Stuffing & De-stuffing.

Q9] Why is flow control needed? What are the mechanisms? Explain how the GO-Back-N and Selective Repeat ARQ differ from each other.

Ans: **[10M – Dec14 & May17]**

FLOW CONTROL:

1. Flow control is the process of managing the rate of data transmission between two nodes to prevent a faster sender from overwhelming a slow receiver
2. Flow control ensures that the receiving device can handle all of the incoming data.
3. Flow control is particularly important where the sending device is capable of sending data much faster than the receiving device can receive it.
4. Flow control can be implemented in hardware and software, or a combination of both.

WHY FLOW CONTROL IS NEEDED:

1. Data Link Layer regulates the flow of data so that receivers are not swamped by fast senders.
2. The receiving entity typically allocates a data buffer of some maximum length for a transfer.
3. When data are received, the receiver must do the certain number of processing before passing the data to higher level software.
4. In the absence of flow control, the receiver's buffer may fill up and over flow while it is processing old data.

5. Flow control allows the receiver to tell the sender to reduce the number of frames it is sending or stop sending completely since it cannot cope with the sender's current sending speed.

FLOW CONTROL MECHANISMS:

I) Stop & Wait:

- It is the simplest form of flow control.
- In Stop-and-Wait flow control, the receiver indicates its readiness to receive data for each frame.
- **Stop & Wait Operations:**
  - **Sender:** Transmit a single frame.
  - **Receiver:** Transmit acknowledgment (ACK)

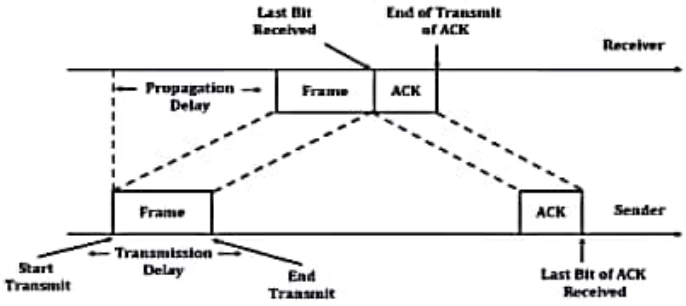


Figure 3.8: Stop & Wait Mechanism.

Disadvantages:

- Only one frame can be in transmission at a time.
- This leads to inefficiency if propagation delay is much longer than the transmission delay.

II) Slidine Window:

- It allows transmission of multiple frames.
- This technique assigns each frame a k-bit sequence number.
- Range of sequence number is 0 to $2^k - 1$.
- **Sliding Window Operation:**
  - **Sending Window:** At any instant, the sender is permitted to send frames with sequence numbers in a certain range.
  - **Receiver Window:** The receiver maintains a receiving window corresponding to the sequence numbers of frames that are accepted.
- If the window size is sufficiently large the sender can continuously transmit packets:

- **N >= 2a+1:** Sender can transmit continuously. (Efficiency = 1)
- **N < 2a+1:** Sender can transmit 'N' frames every 2a+1 time units. (Efficiency = n /(1 + 2a))

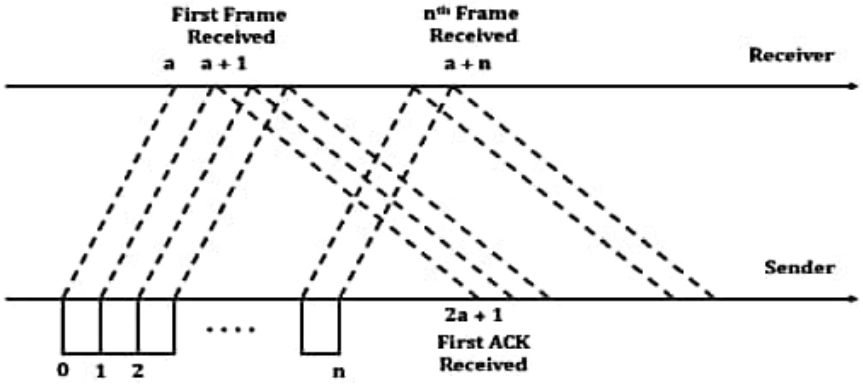


Figure 3.9: Sliding Window Mechanism.

DIFFERENCE BETWEEN GO-BACK-N SELECTIVE REPEAT ARQ:

Table 3.2: Comparison between GO-Back-N Selective Repeat ARQ.

GO-Back-N ARQ	Selective Repeat ARQ
Go Back N ARQ is inefficient for noisy link.	Selective repeat ARQ is efficient for noisy links.
Go Back N ARQ is less complicated than Selective repeat ARQ.	Selective Repeat ARQ is complicated.
In Go Back N ARQ, Sender Window Size is 2^m-1 and receiver window size is 1.	In Selective Repeat ARQ, Sender and receiver Window Size is 2^{m-1}
Go-Back-N ARQ is a specific instance of the automatic repeat request (ARQ) protocol, in which the sending process continues to send a number of frames specified by a window size even without receiving an acknowledgement (ACK) packet from the receiver. It is a special case of the general sliding window protocol with the transmit window size of N and receive window size of 1.	Selective Repeat ARQ / Selective Reject ARQ is a specific instance of the Automatic Repeat-Request (ARQ) protocol used for communications. It may be used as a protocol for the delivery and acknowledgement of message units, or it may be used as a protocol for the delivery of subdivided message sub-units.

Q10] What is the maximum window size allowed for selective repeat ARQ? Explain why with appropriate scenario.

Ans: **[10M – Dec14]**

SELECTIVE REPEAT ARQ:

1. Go-Back-N ARQ simplifies the process at the receiver site.
2. Go-Back-N ARQ protocol is very inefficient for a noisy link.
3. Due to noisy link, there may be possibility of resending of multiple frames which can slow down the transmission.
4. For noisy links, there is another mechanism that does not resend N frames when just one frame is damaged; only the damaged frame is resent.
5. This mechanism is called **Selective Repeat ARQ**.
6. It is more efficient for noisy links, but the processing at the receiver is more complex.
7. Selective Repeat ARQ is a specific instance of the Automatic Repeat-Request (ARQ) protocol used for communications.
8. It may be used as a protocol for the delivery and acknowledgement of message units.

SELECTIVE REPEAT ARQ MECHANISM:

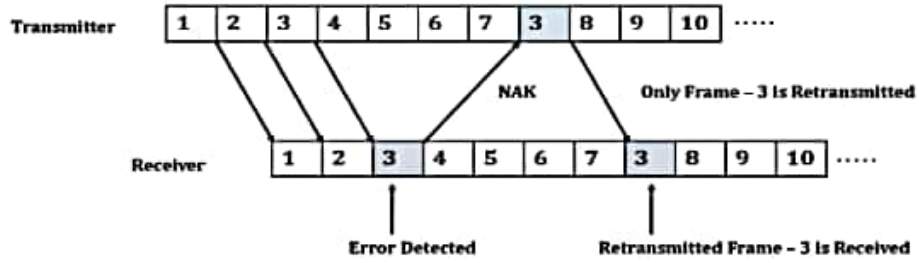


Figure 3.10: Selective Repeat ARQ System.

1. In this system the transmitter does not wait for the ACK signal for the transmission of the next code word.
2. It transmits the code words continuously till it receives the "NAK" signal from the receiver.
3. The receiver sends the NAK signal back to the transmitter when it detects an error in the received frame.
4. For Example the receiver detects an error in the third frame.
5. By the time this NAK signal reaches the transmitter, it had transmitted the frames up to 7 as shown in figure 3.10.

6. On reception of NAK signal, the transmitter will retransmit only frame 3 and then continues with the sequence 8, 9 & so on.
7. The frames 4, 5, 6 & 7 received by the receiver are not discarded by the receiver.
8. The receiver receives the retransmitted frames in between the regular frames.
9. Therefore the receiver will have to maintain the frames sequentially.
10. Hence the Selective Repeat ARQ is the most efficient but the most complex protocol.

MAXIMUM WINDOW SIZES:

1. The size of the sender and receiver windows must be at most one half of 2m.
2. For an example, we choose m = 2, which means the size of the window is $2^m/2$, or 2.
3. Therefore Maximum Window Size allowed for Selective Repeat ARQ is $2^m/2$ or 2.
4. The following figure compares a window size of 2 with a window size of 3.

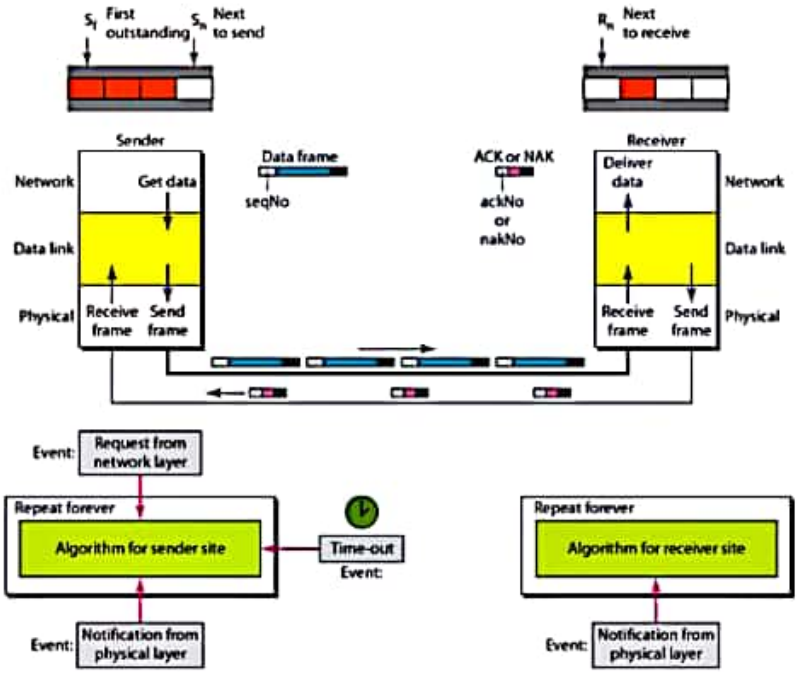


Figure 3.11: Selective Repeat ARQ Window Size Comparison.

5. If the size of the window is 2 and all acknowledgments are lost, the timer for frame 0 expires and frame 0 is resent.

6. However, the window of the receiver is now expecting frame 2, not frame 0, so this duplicate frame is correctly discarded.
7. When the size of the window is 3 and all acknowledgments are lost, the sender sends a duplicate of frame 0.
8. However, this time, the window of the receiver expects to receive frame 0 (0 is part of the window).
9. So it accepts frame 0, not as a duplicate, but as the first frame in the next cycle.
10. This is clearly an error.
11. Hence, the size of window 2 or $2^m/2$ is the maximum window size for Selective Repeat ARQ.

Q11] Explain Sliding Window Protocol using GO-Back-N Technique.

Ans: **[10M – May15]**

SLIDING WINDOW PROTOCOL USING GO-BACK-N TECHNIQUE:

1. It is assumed that in Stop & Wait Protocol, the transmission time required for a frame to arrive at the receiver plus the transmission time required for the acknowledgment to come back is negligible.
2. But this assumption is not correct in some practical situation like satellite system.
3. In satellite system the round trip time can be as long as 500 ms.
4. This means there is a **Propagation Delay.**
5. In order to overcome the inefficiency of Stop & Wait ARQ, Go-Back-N ARQ is used.
6. Go-Back-N ARQ allows the transmitter to continue sending of enough frames, so that the channel is kept busy. While the transmitter waits for the acknowledgment.
7. In this method, if one frame is damaged or lost, all frames are sent since the last frame acknowledgement are transmitted.

PRINCIPLE OF GO-BACK-N ARQ:

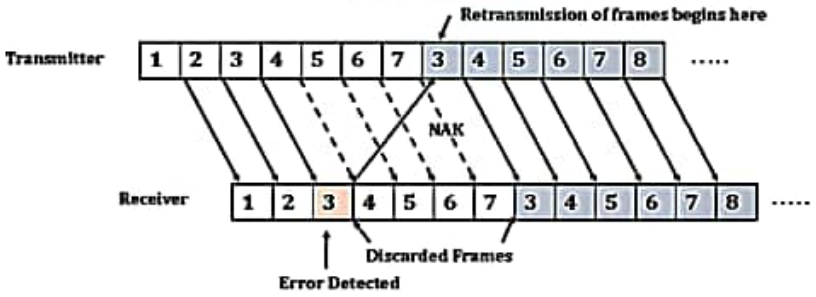


Figure 3.12: Go-Back-N ARQ System.

---

1. In this technique the sender does not waits for ACK Signal for the transmission of next frame.
2. It transmits the frame continuously as long as it does not receive the "NAK" signal.
3. NAK Stands for Negative Acknowledgment Signal, which is send by the receiver to the transmitter.
4. Consider the figure 3.12, when the receiver detects the error in 3rd frame, the receiver sends a NAK signal back to sender.
5. But the signal takes some time to reach the transmitter.
6. By that time the transmitter have transmitted frames up to Frame 7.
7. On reception of NAK signal, the transmitter will retransmit all the frames from 3 onwards.
8. The receiver discards all the frames it has received after 3 i.e. 3 to 7.
9. It will then receive all the frames that are transmitted by the transmitter.

OPERATIONS:

I) Operation When the Frame is Damaged:

- Consider the Figure 3.13 which shows the condition when Frame is Damaged.
- As shown in Figure the 2nd Frame is damaged.
- So the error is detected and receiver send NAK-2 signal back.
- On reception of this signal, the transmitter starts retransmission from Frame 2.
- All the frames received after Frame 2 are discarded by the receiver.

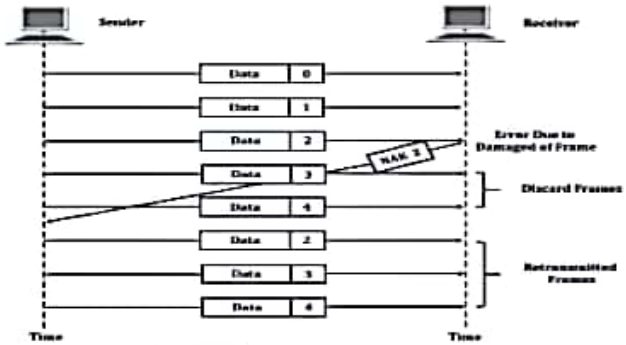


Figure 3.13: Go-Back-N Damaged Frame Condition.

II) Operation When the Frame is Lost:

- Consider the Figure 3.14 which shows the condition when Frame is Lost.
- As shown in Figure the 2nd Frame is Lost.
- This condition is treated in the same manner as that of the damaged frame.
- If the receiver does not receive any particular data frame, then it sends a NAK to the transmitter.
- On reception of the signal, the transmitter starts retransmission all the frames sent since the last frame acknowledged.

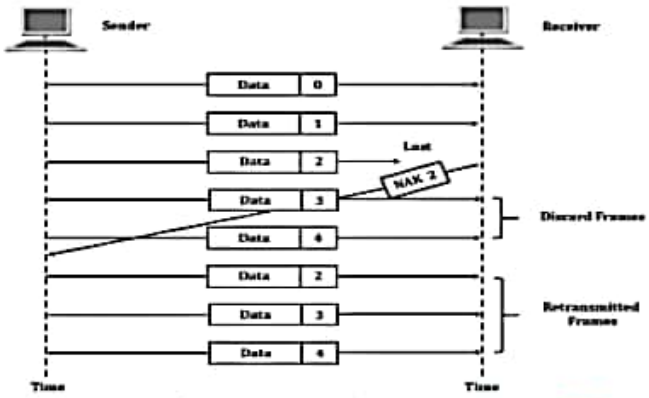


Figure 3.14: Go-Back-N Lost Frame Condition.

III) Operation When the Acknowledgement is Lost:

- Consider the Figure 3.15 which shows the condition when Acknowledgment is Lost.
- In Go-Back-N Method the transmitter does not except an acknowledgment after every data frame.
- It cannot use the absence of sequential ACK number to identify lost ACK or NAK frames.
- It uses a Timer.
- The transmitter can send as many frames as the window allows before waiting for an acknowledgment.
- Once the limit has been reached or the transmitter has no more frames to transmit it must wait till the timer goes off and retransmit all the data frames again.
- The disadvantages of Go-Back-N Technique is that in noisy channels it has poor efficiency. Because of the need to retransmit the frame in error and all the subsequent frames.

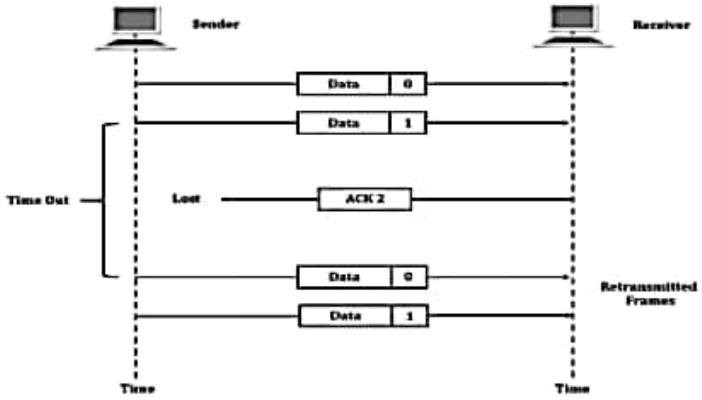


Figure 3.15: Go-Back-N Lost ACK Frame Condition.

Q12] Why there is a need for framing?

The Following encoding is used in a data link protocol:

A: 01000111; B: 11100011; FLAG: 01111110; ESC: 11100000

Show the bit sequence transmitted (in binary) for the four character frame: A B ESC FLAG

When each of the following framing methods are used:

a. **Character count.**
b. **Flag bytes and byte stuffing.**
c. **Starting and Ending flag bytes, with bit stuffing.**

Ans: **[10M – Dec14]**

NEED FOR FRAMING:

1. Data communications is based on the exchange of data units (usually called frames), with a known structure.
2. In general, frames are of variable length.
3. The physical layer simply accepts and transmits a stream of bits without any regard to meaning or structure.
4. Therefore it is the responsibility of Data Link Layer to create and recognize frame boundaries.
5. This can be accomplished by attaching special bit patterns to the beginning and end of the frame.
6. If these bit patterns can accidentally occur in data, special care must be taken to make sure these patterns are not incorrectly interpreted as frame delimiters.

EXAMPLE:

The Following encoding is used in a data link protocol:

A: 01000111; B: 11100011; FLAG: 01111110; ESC: 11100000

This is how the bits will be transmitted for frame A B ESC FLAG:

I) **Character Count:**

00000100	01000111	11100011	11100000	01111110
Count Byte	A	B	ESC	Flag

II) **Flag bytes and byte stuffing:**

01111110	01000111	11100011	11100000	11100000	11100000	01111110	01111110
Start Flag	A	B	ESC to Escape Next Byte	ESC	ESC to Escape Next Byte	Flag	End Flag

III) Starting and Ending flag bytes, with bit stuffing:

01111110	01000111	110100011	11100000	011111010	01111110
Start Flag	A	B with Stuffed Bit (After 5 Continuous 1)	ESC	Flag with Stuffed Bit (After 5 Continuous 1)	ESC to Escape Next Byte

Q13] Explain any four functions of Data Link Layer with Example.

Q14] Enumerate the main responsibilities of the data link layer

Ans: **[Q13 | 10M – May16] & [Q14 | 5M – May17]**

DATA LINK LAYER:

1. Data Link Layer is the second layer of OSI Model.
2. Data Link Layer is responsible for node-to-node delivery of data.
3. It receives the data from network layer and creates FRAMES, add physical address to these frames & pass them to physical layer.
4. It consist of 2 layers:
   - Logical Link Layer (LLC).
   - Medium Access Control (MAC).

FUNCTIONS OF DATA LINK LAYER (DESIGN ISSUES):

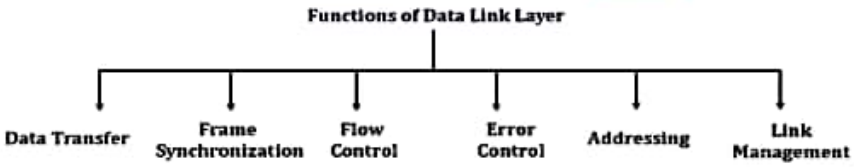


Figure 3.16: Functions of Data Link Layer.

I) Services provided to the network layer:

- Network layer is the layer above the Data Link Layer in OSI Model.
- So Data Link Layer is supposed to provide services to the network layer.
- The main service to be provided is to transfer data from the network layer on the sending machine to the network layer of the receiving machine.

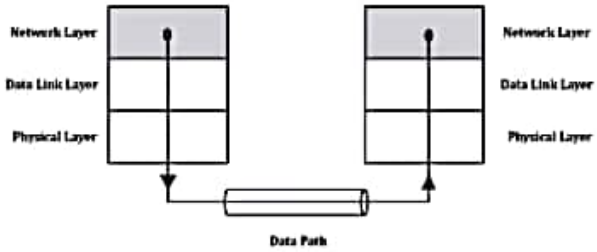


Figure 3.17: Data Path in Data Link Layer.

- Data Link Layer are designed to offer different types of services such as:
  - Unacknowledged Connectionless Service.
  - Acknowledged Connectionless Service.
  - Acknowledged Connection Oriented Service.

II) Frame synchronization:

- DLL divides the bits received from N/W layer into frames.
- Frame contains all the addressing information necessary to travel from Source to Destination.
- For frame synchronization, **Framing** is used.
- Framing methods includes:
  - Character Count.
  - Character Stuffing.
  - Bit Stuffing.

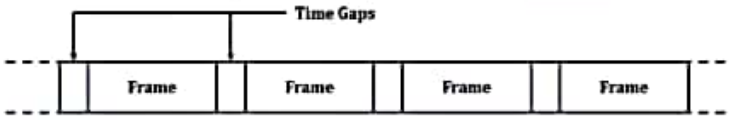


Figure 3.18: Framing.

III) Flow Control:

- If there is a fast sender at one end sending data to a slow receiver, then there must be flow control mechanism to control the loss of data by slow receivers.
- There are several mechanisms used for flow control such as increasing buffer size at receivers, slow down the fast sender, and so on.
- Some process will not be in position to accept arbitrarily long messages.
- This property leads to mechanisms for disassembling, transmitting and the reassembling messages.

IV) Error Control:

- The error made in bits during transmission from source to destination machines must be detected and corrected.
- Many error detecting and error correcting codes are available.
- Both sending and receiving ends must agree to use any one code.

V) Addressing:

- There are multiple processes running on one machine.
- Every layer needs a mechanism to identify senders and receivers.
- Since there are multiple possible destinations, some form of addressing is needed in order to specify a specific destination.
- Data Link Layer provides addressing mechanism to identify the identity of individual machine.

VI) Control & Data on Same Link:

- The data and control information is combined in a frame and transmitted from the source to destination machine.
- The destination machine must be able to recognize control information from the data being transmitted.

VII) Link Management:

- The initiation, maintenance and termination of the link between the source and destination is required for effective exchange of data.
- Protocols & procedures are required for the link management.

Q15] FDDI.

Ans: **[5M – May16]**

FDDI:

1. FDDI stands for **Fiber Distributed Data Interface.**
2. FDDI is a set of ANSI and ISO standards for data transmission on fiber optic lines in a local area network.
3. In addition to being large geographically, an FDDI local area network can support thousands of users.
4. FDDI is frequently used on the backbone for a wide area network (WAN).

FDDI CHARACTERISTICS:

1. FDDI provides 100 Mbps of data throughput.
2. FDDI includes two interfaces.
3. It is used to connect the equipment to the ring over long distances.
4. FDDI is a LAN with Station Management.
5. Allows all stations to have equal amount of time to transmit data.

FDDI ACCESS METHOD:

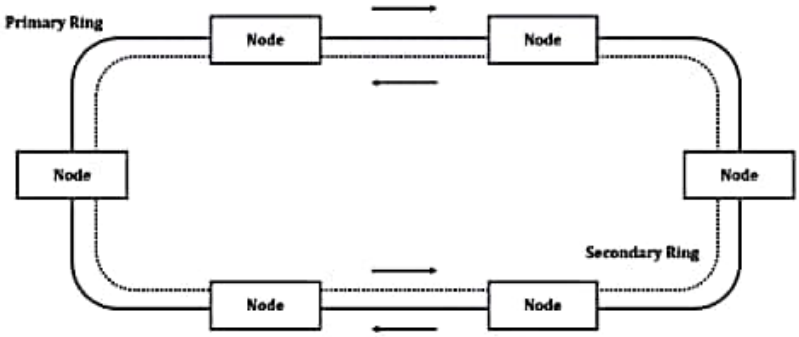


Figure 3.19: FDDI.

1. The FDDI protocol is based on the token ring protocol.
2. An FDDI network contains two token rings, one for possible backup in case the primary ring fails.
3. Any station wants to transmit information holds the token and then transmits the information.
4. When it finish it release the token in the ring.
5. The time a station holds the token is called as Synchronous Allocation Time (SAT).
6. SAT time is variable for each station.
7. The allocation of this time to each station is achieved by Station Management (SMT).
8. The function of SMT are Ring Control, Ring Initialization, Station Insertion and Station Removal.

Q16] HDLC

Ans: **[5M – Dec16]**

HDLC:

1. HDLC stands for **High-level Data Link Control**.
2. HDLC is a **bit-oriented protocol**.

---

3. HDLC is the most important data link control protocol.
4. The HDLC protocol is an international standard that has been defined by ISO for use on both **point-to-point and multi-point data links**.
5. It supports **half-duplex** and **full-duplex communication lines**.
6. It is a group of protocols for transmitting data between network nodes.
7. In HDLC, data is organized into a unit called a **frame** and sent across a network to a destination that verifies its successful arrival.
8. HDLC supports simple **sliding-window mode** for reliable delivery.

TYPES OF FRAMES IN HDLC:

HDLC defines three types of frames:

- **Information frames (I-frame):** I-frames carry user's data and control information about user's data.
- **Supervisory frame (S-frame):** S-frame carries control information, primarily data link layer flow and error controls.
- **Unnumbered frame (U-frame):** U-frames are reserved for system management and information carried by them is used for managing the link.

Q17] What is the throughput of the system both in pure ALOHA and Slotted ALOHA, if the network transmits 200 bit-frames on a shared channel of 200 kbps and the system produces
(a) 1000 frames per second.
(b) 500 frames per second.

Ans: **[SM – Dec16]**

PURE ALOHA:

The frame transmission time is 200/200 kbps or 1ms.

For 1000 frames per second:

- If the system creates 1000 frames per second, this is 1 frame per millisecond.
- The load is 1.
- The throughput for pure ALOHA is

$$S = G \times e^{-2G}$$

- Where G is the average number of frames requested per frame-time.
- The maximum throughput $S_{max} = 0.135$ When G = 1.
- This means that the throughput is **1000 x 0.135 = 135 frames**.
- Therefore, only 135 frames out of 1000 will probably survive.

For 500 frames per second:

- If the system creates 500 frames per second, this is 1/2 frame per millisecond.
- The load is 1/2.
- The throughput for pure ALOHA is

$$S = G \times e^{-2G}$$

- Where G is the average number of frames requested per frame-time.
- The maximum throughput S_{max} = 0.184 When G = 1/2.
- This means that the throughput is **500 x 0.184 = 92 frames**.
- Therefore, only 92 frames out of 1000 will probably survive.

SLOTTED ALOHA:

The frame transmission time is 200/200 kbps or 1ms.

For 1000 frames per second:

- If the system creates 1000 frames per second, this is 1 frame per millisecond.
- The load is 1.
- The throughput for pure ALOHA is

$$S = G \times e^{-G}$$

- Where G is the average number of frames requested per frame-time.
- The maximum throughput S_{max} = 0.368 When G = 1.
- This means that the throughput is **1000 x 0.368 = 368 frames**.
- Therefore, only 368 frames out of 1000 will probably survive.

For 500 frames per second:

- If the system creates 500 frames per second, this is 1/2 frame per millisecond.
- The load is 1/2.
- The throughput for pure ALOHA is

$$S = G \times e^{-G}$$

- Where G is the average number of frames requested per frame-time.
- The maximum throughput S_{max} = 0.184 When G = 1/2.
- This means that the throughput is **500 x 0.303 = 151 frames**.
- Therefore, only 151 frames out of 1000 will probably survive.

Q18] Consider a message represented by a polynomial M (x) = $x^5 + x^4 + x$
Consider a general polynomial G (x) = $x^3 + x^2 + 1$ (1101). Generate a 3 bit CRC and show what will be the transmitted frame. How is error detected by CRC?

Ans: **[10M - May17]**

CRC:

1. CRC Stands for **Cyclic Redundancy Check.**
2. CRC is a technique for detecting errors in digital data, but not for making corrections when errors are detected.
3. It is used primarily in data transmission.
4. In the CRC method, a certain number of check bits, often called a **checksum**, are appended to the message being transmitted.
5. The receiver can determine whether or not the check bits agree with the data, to ascertain with a certain degree of probability whether or not an error occurred in transmission.

TYPES OF ERRORS:

There may be three types of errors:

1. **Single bit error:** In a frame, there is only one bit, anywhere though, which is corrupt.

2. **Multiple bits error:** Frame is received with more than one bits in corrupted state.

3. **Burst error:** Frame contains more than 1 consecutive bits corrupted.

EXAMPLE:

Given:

M(x): $x^5 + x^4 + x$ = 110010

G(x): $x^3 + x^2 + 1$ = 1101

Steps:

1. Multiply M(x) by X3 (highest power in G(x)) i.e. Add 3 zeros = 110010000.
2. Divide the result by G(x). The remainder = C(x).

3. 1101 long division into 110010000 (with subtraction mod 2) = 100100 remainder 100.
4. Transmit 110010000 + 100
5. To be precise, transmit: $T(x) = x^3 M(x) + C(x) = \mathbf{110010100}$.

```
1101 | 110010000
       1101
       ------
       000110000
          1101
          ----
          000100
```

Result is transmitted message followed by remainder. i.e. **110010100**

6. **At Receiver end:** Receive T(x). Divide by G(x), should have remainder 0.

```
1101 | 110010100
       1101
       ------
       000110100
          1101
          ----
          000000
```

7. If the remainder of division is zero, receiver assumes that there is no error in data and it accepts it.
8. If remainder is non-zero then there is an error in data and receiver rejects it.

— EXTRA QUESTION —

Q1] Explain ALOHA in Detail.

Ans:

ALOHA:

1. **ALOHA** was developed at University of Hawaii in early 1970s by Norman Abramson.
2. It was used for ground based radio broadcasting.
3. In this method, stations share a common channel.
4. When two stations transmit simultaneously, collision occurs and frames are lost.
5. There are two different versions of ALOHA: **Pure ALOHA & Slotted ALOHA**.

PURE ALOHA:

1. In pure ALOHA, stations transmit frames whenever they have data to send.
2. When two stations transmit simultaneously, there is collision and frames are lost.
3. In pure ALOHA, whenever any station transmits a frame, it expects an acknowledgement from the receiver.
4. If acknowledgement is not received within specified time, the station assumes that the frame has been lost.
5. If the frame is lost, station waits for a random amount of time and sends it again.
6. This waiting time must be random, otherwise, same frames will collide again and again.
7. Whenever two frames try to occupy the channel at the same time, there will be collision and both the frames will be lost.
8. If first bit of a new frame overlaps with the last bit of a frame almost finished, both frames will be lost and both will have to be retransmitted.

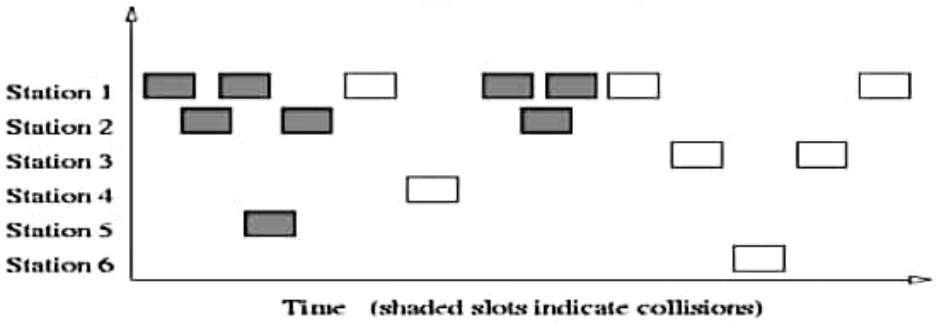


Figure 3.20: Pure ALOHA.

SLOTTED ALOHA:

1. Slotted ALOHA was invented to improve the efficiency of pure ALOHA.
2. In slotted ALOHA, time of the channel is divided into intervals called slots.
3. The station can send a frame only at the beginning of the slot and only one frame is sent in each slot.
4. If any station is not able to place the frame onto the channel at the beginning of the slot, it has to wait until the next time slot.
5. There is still a possibility of collision if two stations try to send at the beginning of the same time slot.

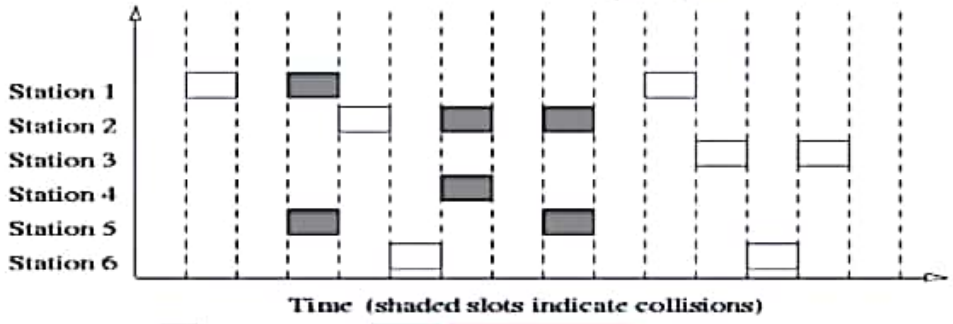


Figure 3.21: Slotted ALOHA.

CHAPTER - 4: NETWORK LAYER

Q1] Border Gateway Protocol.

Q2] Write Short Notes on: BGP.

Ans: **[Q1 | 10M – Dec15 & May17] & [Q2 | 5M – Dec14 & May16]**

BGP:

1. BGP stands for **Border Gateway Protocol**.
2. It is one of the **routing protocol**.
3. BGP is a protocol for exchanging routing information between gateway hosts in a network of autonomous systems.
4. It is an inter-domain routing protocol based on path vector routing.
5. BGP was not built to route within an Autonomous System (AS), but rather to route between AS's.
6. BGP maintains a separate routing table based on shortest AS Path and various other attributes like distance or cost.
7. For communication, BGP uses Classless Inter-domain Routing (CIR) addresses.
8. BGP was mainly developed for a need of efficient Inter-domain unicast routing protocol.

BGP SESSION:

1. BGP establishes a session to exchange information between routers.
2. BGP Session can be Internal BGP or External BGP.
3. When BGP is running inside an autonomous system, it is referred as Internal BGP (IBGP).
4. When BGP runs between autonomous systems, it is referred as External BGP (EBGP).

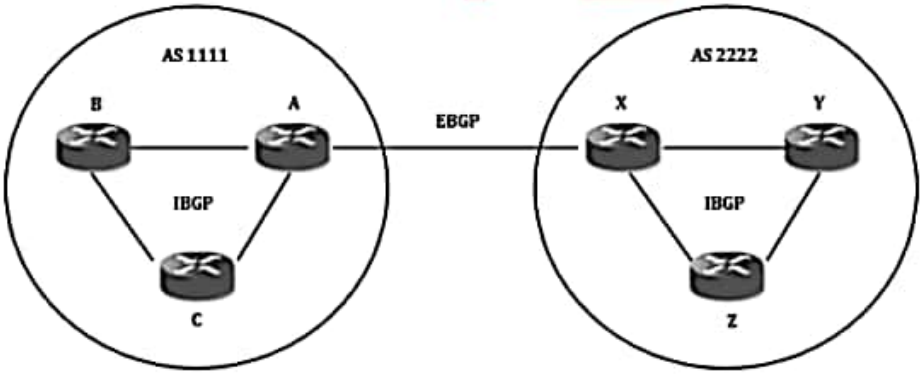


Figure 4.1: BGP Session.

BGP SESSION ESTABLISHMENT:

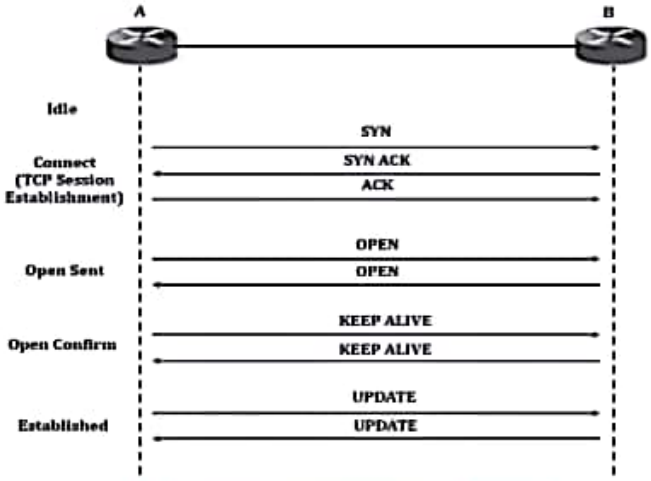


Figure 4.2: BGP Session Establishment.

- **Idle:** No Session is currently active. It is used for configuration of a new BGP Session or Resetting the existing one.
- **Connect:** Attempting to Connect & TCP Session is established.
- **Open Sent:** Open Message is send.
- **Open Confirm:** Response is received.
- **Establishment:** Reception of response & Adjacency Establishment.

BGP MESSAGES:

- **Open:** BGP uses open message to establish a TCP connection with its neighbours.
- **Update:** BGP uses update message to transfer routing information between peers.
- **Keepalive:** BGP use Keep-alive message to notify other routers that they are alive.
- **Notification:** BGP uses notification message whenever it intends to close a connection or an error condition is detected.

BGP PACKET FORMAT:

- **Marker (16 byte):** This field is used for authentication.
- **Length (2 byte):** This field defines the total length of the message (including header).
- **Type (1 byte):** This field indicates the type of packet. The various types of packets are Open, Update, Keepalive, and Notification.

Q3] What is congestion control? Explain various congestion prevention policies.

Q4] Why there is a need for congestion control? What are the different mechanisms? Explain them?

Ans: **[Q3 | 10M – Dec15] & [Q4 | 10M – Dec14]**

CONGESTION:

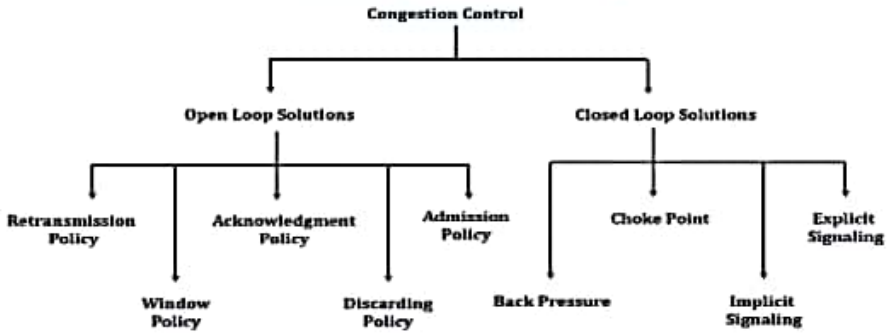
1. Congestion is an important issue that can arise in packet switched network.
2. Congestion is a situation in Communication Networks in which too many packets are present in a part of the subnet.
3. Congestion in a network may occur when the load on the network is greater than the capacity of the network.
4. Due to Congestion the performance degrades.

FACTORS THAT CAUSES THE CONGESTION:

- Packet arrival rate exceeds the outgoing link capacity.
- Insufficient memory to store arriving packets.
- Bursty traffic.
- Slow processor.

CONGESTION CONTROL:

1. Congestion Control is the techniques and mechanisms which can either prevent congestion from happening or remove congestion after it has taken place.
2. Congestion control mechanisms are divided into two categories, one category prevents the congestion from happening and the other category removes congestion after it has taken place.



I) **Open Loop Congestion Control:**

- In Open Loop Congestion Control, policies are used to prevent the congestion before it happens.
- Congestion control is handled either by the source or by the destination.

II) **Closed Loop Congestion Control:**

- Closed loop congestion control mechanisms try to remove the congestion after it happens.
- It uses some kind of feedback.

NEED OF CONGESTION CONTROL:

1. It is not possible to completely avoid the congestion but it is necessary to control it.
2. Congestions leads to a large Queue Length.
3. It results in Buffer Overflow & Loss of Packets.
4. So the congestion control is necessary to ensure that the user gets the negotiated Quality of Services.

CONGESTION PREVENTION POLICIES:

I) **Retransmission Policy:**

- The sender retransmits a packet, if it feels that the packet it has sent is lost or corrupted.
- However retransmission increases the congestion in the network.
- But we need to implement good retransmission policy to prevent congestion.
- The retransmission policy and the retransmission timers need to be designed to optimize efficiency and at the same time prevent the congestion.

II) **Window Policy:**

- To implement window policy, **selective reject window method** is used for congestion control.
- Selective Reject method is preferred over Go-back-n window as in Go-back-n method, when timer for a packet times out, several packets are resent, although some may have arrived safely at the receiver.
- Thus, this duplication may make congestion worse.
- Selective reject method sends only the specific lost or damaged packets.

III) **Acknowledgement Policy:**

- The acknowledgement policy imposed by the receiver may also affect congestion.
- If the receiver does not acknowledge every packet it receives it may slow down the sender and help prevent congestion.
- Acknowledgments also add to the traffic load on the network.
- Thus, by sending fewer acknowledgements we can reduce load on the network.

- To implement it, several approaches can be used:
  - A receiver may send an acknowledgement only if it has a packet to be sent.
  - A receiver may send an acknowledgement when a timer expires.
  - A receiver may also decide to acknowledge only N packets at a time.

IV) Discarding Policy:

- A router may discard less sensitive packets when congestion is likely to happen.
- Such a discarding policy may prevent congestion and at the same time may not harm the integrity of the transmission.

V) Admission Policy:

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

Q5] What are Congestion Prevention Policies? Explain Congestion Control in Virtual Circuit and Datagram Subnets

Ans: **[10M – May17]**

CONGESTION PREVENTION POLICIES:

Refer Q3 Congestion Prevention Policies part.

CONGESTION CONTROL IN VIRTUAL CIRCUIT:

Different approaches are used to control the congestion in virtual-circuit network. Some of them are as follows:

I) Admission control:

- In this approach, once the congestion is signaled, no new connections are set up until the problem is solved.
- This type of approach is often used in normal telephone networks.
- When the exchange is overloaded, then no new calls are established.

II) Allow new virtual connections other than the congested area.

III) Negotiate:

- Negotiate an agreement between the host and the network when the connection is setup.

- This agreement specifies the volume and shape of traffic, quality of service, maximum delay and other parameters.
- The network will reserve resources along the path when the connection is set up.
- Now congestion is unlikely to occur on the new connections because all the necessary resources are guaranteed to be available.
- The disadvantage of this approach is that it may leads to wasted bandwidth because of the some idle connection.

CONGESTION CONTROL IN DATAGRAM SUBNETS:

Congestion control approaches which can be used in the datagram subnets. The techniques are:

I) **Choke Packets:**

- In this approach, the router sends a choke packet back to the source host.
- The original packet is marked so that it would not generate any more choke packets further along the path and is then forwarded in the usual way.
- When the source gets the choke packet, it is required to reduce the traffic by X packets.
- The whole process is illustrated in figure 4.3

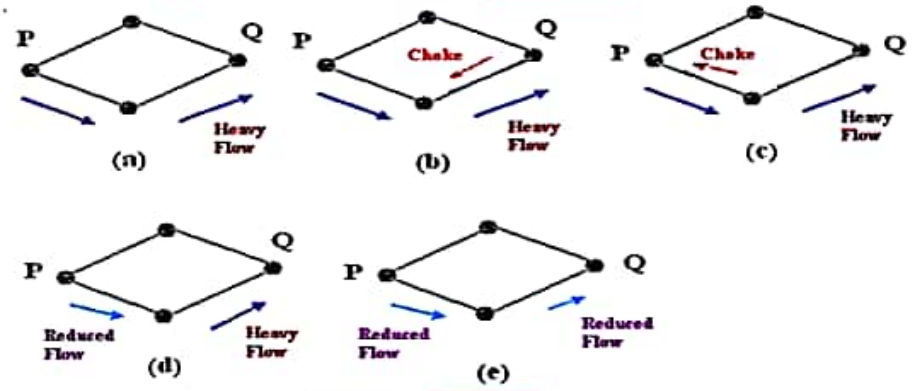


Figure 4.3: Functioning of choke packets.

- (a) Heavy traffic between nodes P and Q
  (b) Node Q sends the Choke packet to P,
  (c) Choke packet reaches P
  (d) P reduces the flow and sends a reduced flow out
  (e) Reduced flow reaches node Q

II) **Load shedding:**

- Admission control, choke packets, fair queuing are the techniques suitable for **light congestion**.
- But if these techniques cannot make the congestion to disappear, then the load shedding technique is to be used.
- In load shedding approach, router just throw packet away.
- In other words, router starts dropping packets.
- Now issue is-which packets to discard? Router may pick packets at random to drop or it may depend on the application running.
- For example, for file transfer, an old packet is important more than a new one and for multimedia application, a new packet is more important than an old one.

III) **Jitter control:**

- Jitter is defined as the variation in delay for the packets belonging to the same flow.
- The real time audio and video cannot tolerate jitter on the other hand the jitter does not matter if the packets are carrying an information contained in a file.
- For the audio and video transmission if the packets take 20 ms to 30ms to reach the destination, it does not matter, provided that the delay remains constant.
- When a packet arrives at a router, the router will check to see whether the packet is behind or ahead and by what time.
- This information is stored in the packet and updated every hop.
- If the packet is ahead of the schedule then the router will hold it for slightly longer time and if the packet is behind the schedule, then the router will try to send it out as quickly as possible.

Q6] What is traffic shaping? Explain Leaky Bucket Algorithm and compare it with Token Bucket Algorithm.

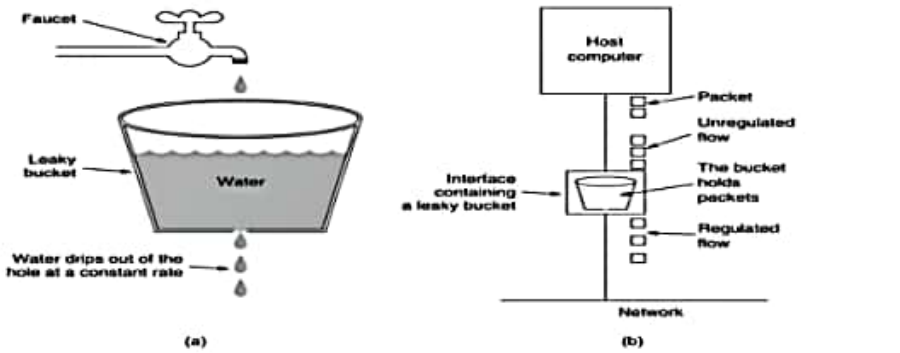
Ans: **[10M – Dec15]**

TRAFFIC SHAPING:

1. One of the reason behind the congestion is **Bursty Traffic.**
2. Traffic Shaping is also known as **Packet Shaping**.
3. It is an **Open Loop Control.**
4. Traffic shaping is the technique of delaying and restricting certain packets traveling through a network to increase the performance of packets that have been given priority.
5. Traffic shaping is a mechanism to control the amount and rate of the traffic sent to the network.
6. The two Traffic Shaping techniques are Leaky Bucket & Token Bucket.

LEAKY BUCKET ALGORITHM:

1. Leaky Bucket is a **traffic shaping mechanism.**
2. A leaky bucket algorithm shapes bursty traffic into fixed rate traffic by averaging the data rate.
3. Imagine a bucket with a small hole at the bottom.
4. The rate at which the water is poured into the bucket is not fixed and can vary but it leaks from the bucket at a constant rate.
5. Thus, the rate at which the water leaks does not depend on the rate at which the water is input to the bucket.
6. Also, when the bucket is full, any additional water that enters into the bucket spills over the sides and is lost.
7. The same concept can be applied to packets in the network.
8. Consider that data is coming from the source at variable speeds.
9. Suppose that a source sends data at 12 Mbps for 4 seconds.
10. Then there is no data for 3 seconds.
11. The source again transmits data at a rate of 10 Mbps for 2 seconds.
12. Thus, in a time span of 9 seconds, 68 Mb data has been transmitted.
13. If a leaky bucket algorithm is used, the data flow will be 8 Mbps for 9 seconds.
14. Thus constant flow is maintained.



(a) A leaky bucket with water. (b) a leaky bucket with packets.

Figure 4.4: Leaky Bucket Principle.

LEAKY BUCKET IMPLEMENTATION:

1. Figure 4.5 shows the implementation of Leaky Bucket Principle.
2. A FIFO Queue is used for holding the packets.
3. Implementation of Leaky Bucket is done under two different operating conditions.

a. **Fixed Size Packets:**
   i. If the arriving packets are of fixed size, then the process removes a fixed number of packets from the queue at each tick of the clock.
   ii. **Example:** Cells in ATM Network.

b. **Packets of variable size:**
   i. If the arriving packets are of different size, then the fixed output rate will not be based on the number of department packets.
   ii. Instead it will be based on the number of departing bytes or bits.

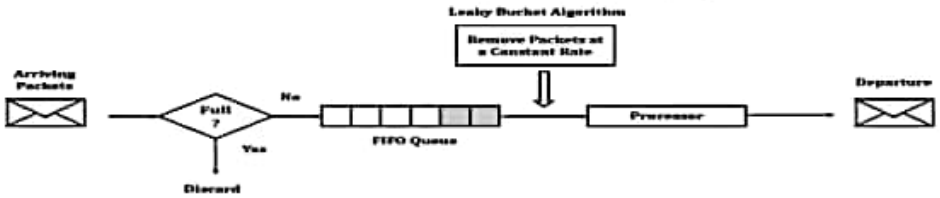


Figure 4.5: Implementation of Leaky Bucket.

LEAKY BUCKET ALGORITHM:

1. Initialize the counter to 'n' at every tick of clock.
2. If n is greater than the size of packet in the front of queue send the packet into the network and decrement the counter by size of packet.
3. Repeat the step until n is less than the size of packet.
4. Reset the counter and go to Step - 1.

COMPARISON OF LEAKY BUCKET ALGORITHM AND TOKEN BUCKET ALGORITHM:

Table 4.1: Comparison of Leaky Bucket Algorithm and Token Bucket Algorithm.

Leaky Bucket	Token Bucket
It is Token Independent.	It is Token dependent.
If bucket is full then packet or data is discarded.	If bucket is full then token are discarded, but not the packet.
Packets are transmitted continuously.	Packets can only transmitted when there are enough token.
It sends the packet at constant rate.	It allows large bursts to be sent faster rate after that constant rate.
It does not save token.	It saves token to send large bursts.

Q7] How does the Token Bucket Algorithm works?

Ans: **[4M – May15]**

TOKEN BUCKET ALGORITHM:

1. The leaky bucket algorithm allows only an average (constant) rate of data flow.
2. Its major problem is that it cannot deal with bursty data.
3. A leaky bucket algorithm does not consider the idle time of the host.
4. For example, if the host was idle for 10 seconds and now it is willing to send data at a very high speed for another 10 seconds, the total data transmission will be divided into 20 seconds and average data rate will be maintained.
5. The host is having no advantage of sitting idle for 10 seconds.
6. To overcome this problem, a token bucket algorithm is used.
7. A token bucket algorithm allows bursty data transfers.
8. A token bucket algorithm is a modification of leaky bucket in which leaky bucket contains tokens.
9. In this algorithm, a token(s) are generated at every clock tick.
10. For a packet to be transmitted, system must remove token(s) from the bucket.
11. Thus, a token bucket algorithm allows idle hosts to accumulate credit for the future in form of tokens.
12. For example, if a system generates 100 tokens in one clock tick and the host is idle for 100 ticks. The bucket will contain 10,000 tokens.
13. Now, if the host wants to send bursty data, it can consume all 10,000 tokens at once for sending 10,000 cells or bytes.
14. Thus a host can send bursty data as long as bucket is not empty.

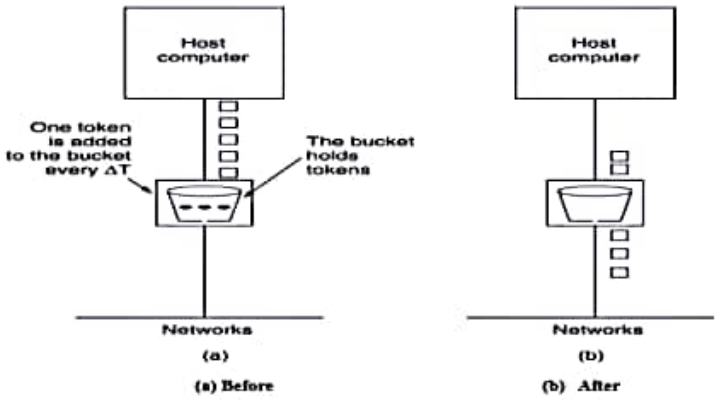


Figure 4.6: Token Bucket Principle.

IMPLEMENTATION OF TOKEN BUCKET:

1. Figure 4.7 shows the implementation of Token Bucket.
2. The token bucket can be easily implemented with a counter.
3. The token is initialized to zero.
4. Each time a token is added, the counter is incremented by 1 and each time a unit of data is dispatched, the counter is decremented by 1.
5. If the counter contains zero, the host cannot send any data.

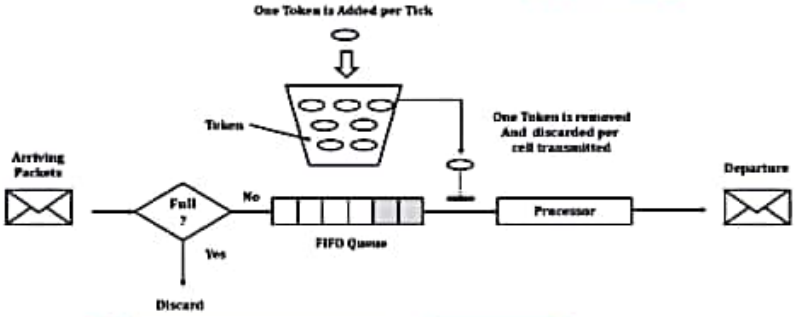


Figure 4.7: Implementation of Token Bucket.

Q8] What are the different types of routing algorithms? When would we prefer to use hierarchical routing over Link State Routing?

Ans: **[10M – Dec15]**

ROUTING:

1. Routing is the process of selecting best paths in a network.
2. It is the process of forwarding of a packet in a network so that it reaches its intended destination.

ROUTING ALGORITHM:

1. Routing Algorithm is the part of network layer software.
2. It is responsible for deciding the output line over which a packet is to be sent.
3. Such decision is dependent on whether the subnet is a virtual circuit or it is datagram switching.

PROPERTIES OF ROUTING ALGORITHM:

1. Correctness.
2. Robustness.
3. Stability.
4. Fairness.
5. Optimality.

TYPES OF ROUTING:

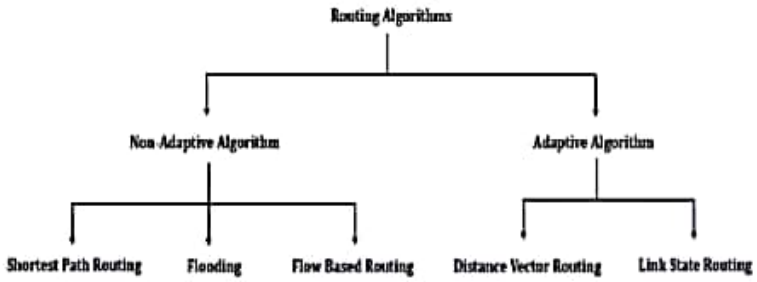


Figure 4.8: Different Types of Routing Algorithm.

I) **Non-Adaptive Algorithm:**

- It is also called as **Static Routing**.
- For this type of routing algorithm, the routing decision is not based on the measurement or estimation of current traffic and topology.
- Instead the route to be taken in going from one node to the other is computed in advance, off-line, and downloaded to the routers when the network is booted.
- **Examples of Static Routing:**
  - Shortest Path Routing.
  - Flooding.
  - Flow Based Routing.

II) **Adaptive Algorithm:**

- It is also called as **Dynamic Routing**.
- These algorithms change their routing decisions to reflect changes in the topology and in traffic as well.
- It gets their routing information from adjacent routers or from all routers.
- **Examples of Dynamic Routing:**
  - Distance Vector Routing.
  - Link State Routing.

HIERARCHICAL ROUTING OVER LINK STATE ROUTING:

1. In Link State Routing, as the size of the network increases, the size of the routing tables of the routers also increases.
2. Due to a large routing tables, a large router memory is consumed.
3. More CPU Time is needed to scan the tables.
4. More bandwidth is required to send status signal report about the tables.

5. Sometime the network becomes so large that the size of the router table become excessively large.
6. Practically it becomes impossible for every router to have an entry for every other router.
7. In order to solve this problem Hierarchical Routing is used.
8. For example: One used in Telephone Networks.
9. In hierarchical routing, the total number of routers are divided into different regions.
10. A router will know everything about the other router in its own region only.
11. Router will have no information about the internal structure of other regions.
12. This reduces the size of the router table.

Q9] What is count to infinity problem in distance vector routing? Discuss in detail.

Ans: **[10M – May15]**

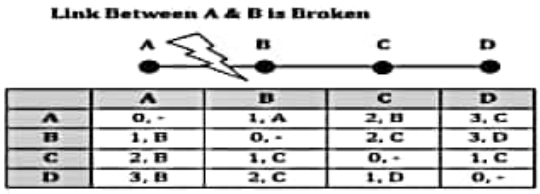
DISTANCE VECTOR ROUTING:

1. Distance Vector Routing is one of the dynamic routing algorithm.
2. It is suitable for **packet switched network.**
3. In distance vector routing, each router maintains a routing table.
4. It contains one entry for each router in the subnet.
5. This entry has two parts:
   a. The first part shows the preferred outgoing line to be used to reach the destination.
   b. Second part gives an estimate of the time or distance to the destination.
6. In distance vector routing, a node tells its neighbor about its distance to every other node in the network.

COUNT TO INFINITY PROBLEM:

1. One of the important issue in Distance Vector Routing is County of Infinity Problem.
2. Counting to infinity is just another name for a routing loop.
3. In distance vector routing, routing loops usually occur when an interface goes down.
4. It can also occur when two routers send updates to each other at the same time.

EXAMPLE:



	A	B	C	D
A	0, -	1, A	2, B	3, C
B	1, B	0, -	2, C	3, D
C	2, B	1, C	0, -	1, C
D	3, B	2, C	1, D	0, -

Figure 4.9: Network Graph & Routing Table.

- Imagine a network with a graph as shown above in figure 4.9.
- As you see in this graph, there is only one link between A and the other parts of the network.
- Now imagine that the link between A and B is cut.
- At this time, B corrects its table.
- After a specific amount of time, routers exchange their tables, and so B receives C's routing table.
- Since C doesn't know what has happened to the link between A and B, it says that it has a link to A with the weight of 2 (1 for C to B, and 1 for B to A -- it doesn't know B has no link to A).
- B receives this table and thinks there is a separate link between C and A, so it corrects its table and changes infinity to 3 (1 for B to C, and 2 for C to A, as C said).
- Once again, routers exchange their tables.
- When C receives B's routing table, it sees that B has changed the weight of its link to A from 1 to 3, so C updates its table and changes the weight of the link to A to 4 (1 for C to B, and 3 for B to A, as B said).
- This process loops until all nodes find out that the weight of link to A is infinity.
- This situation is shown in the table below 4.2.
- In this way, Distance Vector Algorithms have a slow convergence rate.

Table 4.2: Routing Table.

	B	C	D
Sum of Weight to A after link cut	∞, A	2, B	3, C
Sum of Weight to A after 1st updating	3, C	2, B	3, C
Sum of Weight to A after 2nd updating	3, C	4, B	3, C
Sum of Weight to A after 3rd updating	5, C	4, B	5, C
Sum of Weight to A after 4th updating	5, C	6, B	5, C
Sum of Weight to A after 5th updating	7, C	6, B	7, C
Sum of Weight to A after nth updating	....	...	....
∞	∞	∞	∞

- One way to solve this problem is for routers to send information only to the neighbors that are not exclusive links to the destination.
- For example, in this case, C shouldn't send any information to B about A, because B is the only way to A.

Q10] What is the function of IP Protocol? Discuss its Header Format.

Ans: **[10M – May15]**

IP PROTOCOL:

1. IP Protocol Stands for **Internet Protocol**.
2. It is host to host network layer delivery protocol designed for the internet.
3. It is connectionless datagram protocol.
4. It is unreliable protocol because it does not provide any error or flow control.

FUNCTION OF IP PROTOCOL:

I) Addressing:

- IP packet headers contain addresses that identify the sending computer and the receiving computer.
- Routers use this information to guide each packet across communication networks and connect the sending and receiving computers.

II) Reassembly:

- Messages between computers are broken into packets.
- Since most messages are too big to fit in one packet, and since packets aren't sent in any organized order.
- So they must be reassembled as they arrive at the recipient.
- IP dictates how packets are reassembled into usable messages.

III) Timeouts:

- Each IP packet contains a **Time to Live (TTL) Field**.
- Every time when router handles a packet, TTL field is decremented.
- If TTL reaches zero then packet is discarded.
- This prevent the packet from running in circles forever and flooding a network.

IV) Fragmentation:

- IP Packets may be split, or fragmented into smaller packet.
- This permits a large packet to travel across a network which can only handle smaller packets.
- IP Fragments packets transparently.

V) Type of Service:

- IP supports traffic prioritization by allowing packets to be labeled with an abstract type of service.

VI) **Options:**

- IP includes optional features such as allowing the sending computer to decide the path.
- To trace the path they take.
- To include added security in the packets.

Q11] Explain IPv4 header format in detail. If value at HLEN field is 1101 find the size of option and padding field?

Q12] what is IPv4 Protocol? Explain the IPv4 Header Format with Diagram.

Ans: **[Q11 | 10M – Dec15] & [Q12 | 10M – May16]**

IPv4:

1. Internet Protocol Version 4 (IPv4) is the fourth revision of the IP and a widely used protocol in data communication over different kinds of networks.
2. IPv4 is a connectionless protocol used in packet-switched layer networks, such as Ethernet.
3. It provides the logical connection between network devices by providing identification for each device.
4. IPv4 uses a 32-bit Address Scheme.
5. There are many ways to configure IPv4 with all kinds of devices - including manual and automatic configurations - depending on the network type.
6. IPv4 has Dotted Decimal Notation Address Format. For **Example:**192.168.0.1

IP HEADER FORMAT:

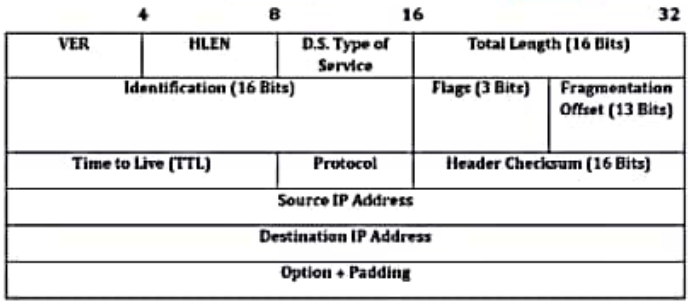


Figure 4.10: IP Header Format.

I) **Version:** This Field defines the version of IP. It is Static 4 bit value.

II) **Header Length:** This Field defines the length of the datagram header. It is 4 bit value.

III) **Type of Service:** It is 8 bit value. It is used tell the network how to treat the IP packet. These bits are generally used to indicate the Quality of Service (QoS) for the IP Packet.

IV) **Packet Length:** 16 bit value indicating the size of the IP Packet in terms of bytes. This gives a maximum packet size of 65536 bytes.

V) **Identification:** 16 bit field used for reassembling the packet at the destination.

VI) **Flags:** It is 3 bits value. It indicates if the IP packet can be further fragmented or not and if the packet is the last fragment or not of a larger transfer.

VII) **Fragment offset:** 13 bit value used in the reassembly process at the destination.

VIII) **Time to Live:** 8 bit value telling the network how long an IP packet can exist in a network before it is destroyed.

IX) **Protocol:** 8 bit value used to indicate the type of protocol being used (TCP, UDP etc.).

X) **Header checksum:** It is 16 bit value. It is used to indicate errors in the header only. Every node in the network has to check and re-insert a new checksum as the header changes at every node.

XI) **Source address:** 32 bit value representing the IP address of the sender of the IP packet.

XII) **Destination address:** 32 bit value representing the IP address of the packets final destination.

XIII) **Options:** Options are not required for every datagram. They are used for network testing and debugging.

XIV) **Padding:** Variable size bit field. These bits are used to ensure a 32 bit boundary for the header is achieved.

EXAMPLE:

If value at HLEN field is 1101 find the size of option and padding field.

HLEN Value = 1101 = 13 Bytes.

Total No. of Bytes in the Header = 13 x 4 = 52 Bytes.

The first 20 bytes are the main header and the next 32 bytes are the options + Padding Field.

Q13] Address Resolution Protocol.

Ans: **[5M – May15]**

ARP:

1. ARP stands for **Address Resolution Protocol**.
2. It is the protocol used by Internet Protocol (IP) specifically IPv4.
3. This protocol operates below the network layer as a part of the interface between the OSI network and OSI link layer.
4. It is used to map Logical Addresses to the Physical Addresses used by a data link protocol.
5. ARP Simply Converts IP Address to Physical Address.
6. It is relatively simple Request-and-Reply Protocol.

ARP REQUEST & REPLY:

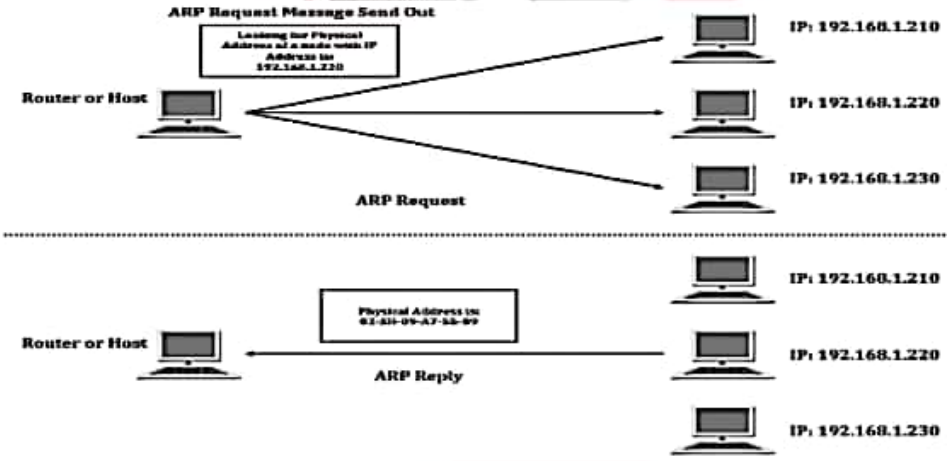


Figure 4.11: ARP Request-Reply.

- ARP maintains the mapping between IP address and MAC address in a table in memory called ARP cache.
- The entries in this table are dynamically added and removed.
- A host will update its ARP cache, only if the ARP request is for its IP address.
- Otherwise, it will discard the ARP request.
- Consider the above figure 4.11, in this a Host sends out the Request Message.
- It is looking for the MAC Address of the node with IP Address 192.168.1.220.
- The Node with the IP Address 192.168.1.220 sends out the Reply Message.
- In reply message it sends its MAC Address to the Host.

Q14] Discuss the quality of service parameters in computer network.

Ans: **[10M – May15, May16 & Dec16]**

QUALITY OF SERVICE:

1. Quality of service (QoS) is the overall performance of a computer network.
2. Particularly it is the performance seen by the users of the network.
3. To measure QoS several aspects are considered such as error rates, bit rate, throughput, transmission delay, availability, jitter, etc.
4. Quality of service is particularly important for the transport of traffic with special requirements.

QUALITY OF SERVICE PARAMETERS:

I) Cell Loss Rate (CLR):

- It is the fraction of cells that are lost during transmission.
- CLR = Cell Lost / Total cells transmitted.

II) Cell Error Ratio (CER):

- This parameter defines the fraction of cells that contained errors.
- CER = Error cells delivered / Total cells delivered.

III) Cell Delay Variation (CDV):

- It defines the difference between the maximum and the minimum cell transfer delay.

IV) Cell Transfer Delay (CTD):

- It is the average time required for cell to travel from source to destination.
- Cell transfer delay is affected by segmentation reassembly and transmission delay.

V) Cell Misinsertion Ratio (CMR):

- It is the number of cells inserted per second that are meant for some other destination.
- It is the ratio of severely error cell blocks to the total transmitted cell blocks.
- SECBR = Severely Error Cell Blocks / Total transmitted cell blocks.

ADDITIONAL PARAMETERS USED TO CHARACTERIZE THE QUALITY OF SERVICE:

I) Reliability:

- Reliability is an important characteristic of QoS.
- Lack of reliability means losing a packet or acknowledgement which then requires retransmission.
- However, the sensitivity of application programs to reliability is not the same.
- For example, it is more important that electronic mail, file transfer, and internet access have reliable transmissions than audio conferencing or telephony.

II) **Delay:**

- Source to destination delay is another flow characteristic.
- Applications can tolerate delay in different degrees.
- In this case, telephony, audio conferencing, video conferencing and remote log in need minimum delay while delay in file transfer or e-mail is less important.

III) **Jitter:**

- Jitter is defined as the variation in delay for packets belonging to the same flow.
- High Jitter means the difference between delays is large and low jitter means the variation is small.
- For example, if four packets depart at times 0, 1, 2 and 3 and arrive at 20, 21, 22 and 23, all have same delay, 20 units of time.
- On the other hand, if the above four packets arrive at 21, 23, 21, and 28 they will have different delays of 21, 22, 19 and 24.

IV) **Bandwidth:**

- Different applications need different bandwidths.
- In video conferencing we need to send millions of bits per second to refresh a color screen while the total number of bits in an email may not reach even a million.

TECHNIQUE TO ACHIEVE GOOD QOS:

I) **Buffering:** Buffering increases delay but its smooth's out jitter and does not affect reliability or bandwidth.

II) **Traffic Shaping:** It forces bursty traffic to be transmitted at a uniform rate.

III) **Over Provisioning:** It provides excess of router capacity, buffer space and bandwidth. So that packets fly through easily.

IV) **Packet Scheduling:** It uses Queuing, so that an aggressive sender does not block all the lines.

V) **Admission Control:** In this a router decides, depending on its current load, whether it should accept or reject a new job.

VI) **Resource Reservation:** Resources such as bandwidth, buffer space and CPU cycles are reserved for further successful transmissions.

VII) **Proportional Routing:** In this, traffic is divided equally amongst all routers so that no single router gets overburdened.

Q15] What is sub-netting? What are the default subnet masks? Find the subnet address if the IP address is 129.31.72.24 and subnet mask is 255.255.192.0

Q16] Explain in short: Subnetting.

Ans: **[Q15 | 5M – Dec15] & [Q16 | 4M – May16]**

SUB-NETTING:

1. Every computer on network has an IP address that represent its location on network.
2. Subnetting is a process of breaking large network in small networks known as subnets.
3. Subnetting happens when we extend default boundary of subnet mask.
4. Basically we borrow host bits to create networks.
5. Subnetting does not give you more hosts, but actually costs you hosts.
6. Subnetting reduces network traffic by removing collision and broadcast traffic, that overall improve performance.

DEFAULT SUBNET MASK:

1. To divide a network address into two or more subnets, you use subnet masks.
2. The default subnet masks for classes:
   a. For Class A networks is 255.0.0.0.
   b. For Class B is 255.255.0.0.
   c. For class C is 255.255.255.0.

Table 4.3: Default Subnet Masks for Class A, Class B and Class C Networks.

IP Address Class	Total # of Bits for Network ID/Host ID	Default Subnet Mask			
		1st Octet	2nd Octet	3rd Octet	4th Octet
Class A	8/24	11111111 (255)	00000000 (0)	00000000 (0)	00000000 (0)
Class B	16/16	11111111 (255)	11111111 (255)	00000000 (0)	00000000 (0)
Class C	24/8	11111111 (255)	11111111 (255)	11111111 (255)	00000000 (0)

EXAMPLE:

IP Address = 129.31.72.24

Subnet Mask = 255.255.192.0

Subnet Address = ?

In order to find Subnet Address we have to AND the IP Address and the Subnet Mask.

IP Address	129.31.72.24	10000001.00011111.01001000.00011000
Subnet Mask	255.255.192.0	11111111.11111111.11000000.00000000
		ANDING
Subnet Address	129.31.64.0	10000001.00011111.01000000.00000000

Q17] What is Subnetting? Given the class C network 192.168.10.0 use the subnet mask 255.255.255.192 to create subnets and answer the following:

(i) What is the number of subnets created?

(ii) How many hosts per subnet?

(iii) Calculate the IP Address of the first host, the last host and the broadcast address of each subnet.

Ans: **[10M – May17]**

SUBNETTING:

Refer Q15.

EXAMPLE:

Given the following:

Network Address: 192.168.10.0

Subnet Mask: 255.255.255.192

Solutions:

Mask	Binary	#Subnet Bits	#Host Bits	Subnet	Hosts
255.255.255.192	11000000	2	6	2	62

What is the number of subnets created?

- Since 192 is 2 bits on (11000000), the answer would be $2^2 - 2 =$ **2 Subnets**.
- The minus 2 is the subnet bits all on or all off, which are not valid by default.

How many hosts per subnet?

- We have 6 host bits off (11000000), so the equation would be $2^6 - 2 =$ **62 hosts**.

Calculate the IP Address of the first host, the last host and the broadcast address of each subnet.

Subnet	Network	First Usable IP	Last Usable IP	Broadcast
1	192.168.10.64	192.168.10.65	192.168.10.126	192.168.10.127
2	192.168.10.128	192.168.10.129	192.168.10.190	192.168.10.191

- First subnet: 256 – 192 = 64
- Second Subnet: 64 + 64 = 128
- The broadcast address is always the number before the next subnet.
- The broadcast address of the 64 subnet is 127 i.e. **192.168.10.127**
- The broadcast address of the 128 subnet is 191 i.e. **192.168.10.191**

Q18] Explain Classless Inter Domain Routing (CIDR).

Ans: **[10M – May16]**

CIDR:

1. CIDR Stands for **Classless Inter-Domain Routing**.
2. It is also called as **Super-netting.**
3. CIDR is an IP addressing scheme that replaces the older system based on classes A, B, and C.
4. With CIDR, a single IP address can be used to designate many unique IP addresses.
5. A CIDR IP address looks like a normal IP address except that it ends with a slash followed by a number, called the *IP* network prefix.
6. **For example:** 172.200.0.0/16.
7. The IP network prefix specifies how many addresses are covered by the CIDR address, with lower numbers covering more addresses.
8. CIDR addresses reduce the size of routing tables and make more IP addresses available within organizations.

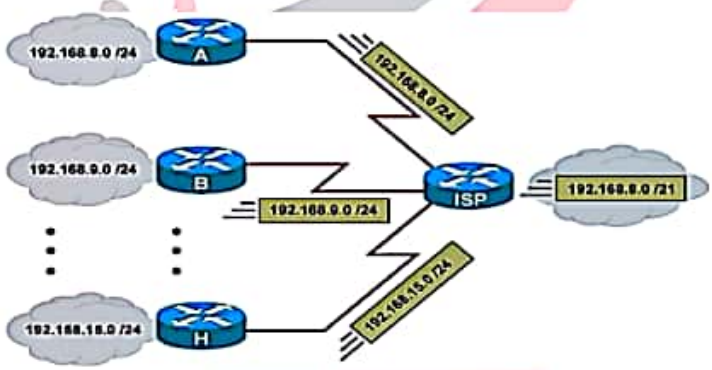


Figure 4.12: CIDR Example.

CIDR NOTATION:

1. CIDR notation is a compact representation of an IP address and its associated routing prefix.
2. The notation is constructed from an IP address, a slash ('/') character, and a decimal number.
3. CIDR Notation of an IP Address: 192.0.2.0/18, here 18 is the prefix length.
4. It states that the first 18 bits are the network prefix of the address & remaining 14 bits are available for specific host Addresses.
5. CIDR notation can replace the use of subnet masks.
6. CIDR Notation allows to drop trailing Zeros of network addresses. For Example: 192.0.2.0/18 can be written as 192.0.2/18

CIDR BLOCK PREFIX:

CIDR Block Prefix	# Equivalent Class C	# of Host Addresses
/27	1/8th of a Class C	32 hosts
/26	1/4th of a Class C	64 hosts
/25	1/2 of a Class C	128 hosts
/24	1 Class C	256 hosts
/23	2 Class C	512 hosts
/22	4 Class C	1,024 hosts
/21	8 Class C	2,048 hosts
/20	16 Class C	4,096 hosts
/19	32 Class C	8,192 hosts
/18	64 Class C	16,384 hosts
/17	128 Class C	32,768 hosts
/16	256 Class C	65,536 hosts
	(= 1 Class B)	
/15	512 Class C	131,072 hosts
/14	1,024 Class C	262,144 hosts
/13	2,048 Class C	524,288 hosts

Figure 4.13: CIDR Block Prefix.

ADVANTAGES:

1. CIDR is now the routing system used by virtually all gateway routers on the Internet's backbone network.
2. Almost Every Internet service provider (ISP) to use CIDR for routing.
3. CIDR is supported by the Border Gateway Protocol & OSPF Interior gateway protocol.
4. CIDR can reduce the number of routing table entries.

Q19] What are the steps involved in Link State Routing. Explain the contents and requirements of Link State Packets.

Ans: **[10M – May16 & Dec16]**

LINK STATE ROUTING:

1. Link state Routing is the **intra-domain routing protocol.**
2. The basic idea behind Link State Protocols is very simple.
3. Link-State routing protocols are more like a road map.
4. They create a topological map of the network and each router uses this map to determine the shortest path to each network.

---

5. Link state protocols are based on Shortest Path First (SPF) algorithm to find the best path to a destination.
6. Shortest Path First (SPF) algorithm is also known as Dijkstra algorithm.

STEPS INVOLVED IN LINK STATE ROUTING:

1. Each router learns about its own directly connected networks.
2. Each router is responsible for contacting its neighbors on directly connected networks.
3. Each router builds a link-state packet (LSP) containing the state of each directly connected link.
4. Each router floods the LSP to all neighbors, who then store all LSPs received in a database.
5. Each router uses the LSPs to construct a database that is a complete map of the topology and computes the best path to each destination network.
6. Figure 4.14 shows Link State Routing Example.

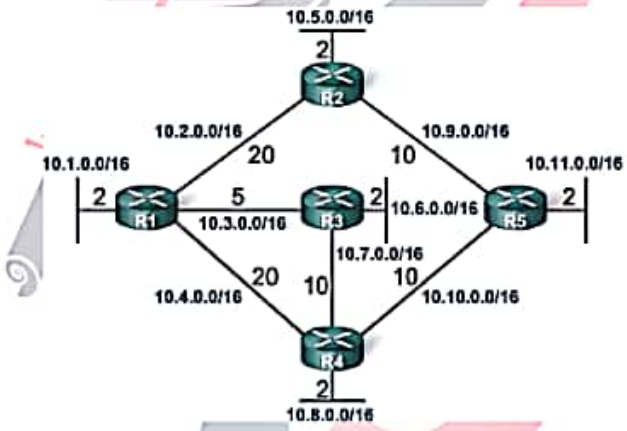


Figure 4.14: Link State Routing Example.

LINK STATE PACKETS FOR ABOVE EXAMPLE:

Table 4.4: Link State Packets for subnet.

R_1		R_2		R_3		R_4		R_5	
Sequence	Age	Sequence	Age	Sequence	Age	Sequence	Age	Sequence	Age
R_2	20	R_1	20	R_1	5	R_1	20	R_2	10
R_3	5	R_5	10	R_4	10	R_3	10	R_4	10
R_4	20					R_5	10		

LINK STATE PACKETS:

1. Link State Packets represent the state of a router and its links to the rest of the network.
2. It Works directly for point to point links.

CONTENTS AND REQUIREMENTS OF LINK STATE PACKETS:

I) Memory Requirements:

- Link-state routing protocols typically require more memory, more CPU processing and, at times, more bandwidth than distance vector routing protocols.
- The memory requirements are because of the use of:
  - Link-state databases.
  - Creation of the SPF tree.

II) Processing Requirements:

- Link-state protocols can also require more CPU processing than distance vector routing protocols.
- The Shortest Path First algorithm requires more CPU time than distance vector algorithms because link-state protocols build a complete map of the topology.

III) Bandwidth Requirements:

- The flooding of link-state packets can adversely affect the available bandwidth on a network.
- This should only occur during initial startup of routers, but it can also be an issue on unstable networks.

IV) Hierarchical Design:

- Link State Routing protocols such as OSPF and IS-IS use the concept of areas.
- Multiple areas create a hierarchical design to networks, allowing better route aggregation (summarization) and the isolation of routing issues within an area.

Q20] What is controlled access for collision control? Explain all the methods of controlled access in details.

Ans: **[10M – Dec15]**

ACCESS CONTROL PROTOCOL:

1. In this method, the stations consult each other to find which station has a right to send.
2. A station cannot send unless it has been authorized by other station.
3. The different controlled access methods are Reservation, Polling & Token Passing.
4. In a controlled access method, either a central authority (in polling) or other stations (in reservation and token passing) control the access.
5. Control Access Protocol avoids the collision because it has Access Control.

I) Reservation:

- In this method, a station needs to make a reservation before sending data.
- The time is divided into intervals.
- In each interval, a reservation frame precedes the data frames sent in that interval.
- If there are N stations, then there are exactly N reservation slots in the reservation frame.
- Each slot belongs to a station.
- When a station needs to send a frame, it makes a reservation in its own slot.
- The stations that have made reservations can send their frames after the reservation frame.
- Figure 4.15 shows the Reservation System.

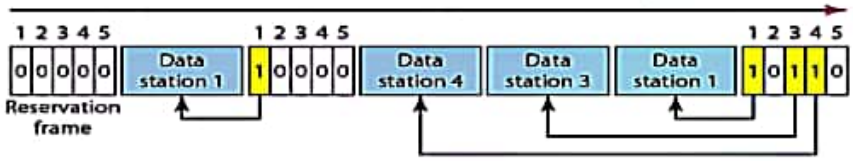


Figure 4.15: Reservation System.

II) Polling:

- Polling method works in those networks where primary and secondary stations exist.
- All data exchanges are made through primary device even when the final destination is a secondary device.
- Primary device controls the link and secondary device follow the instructions.
- Figure 4.16 shows Polling System.

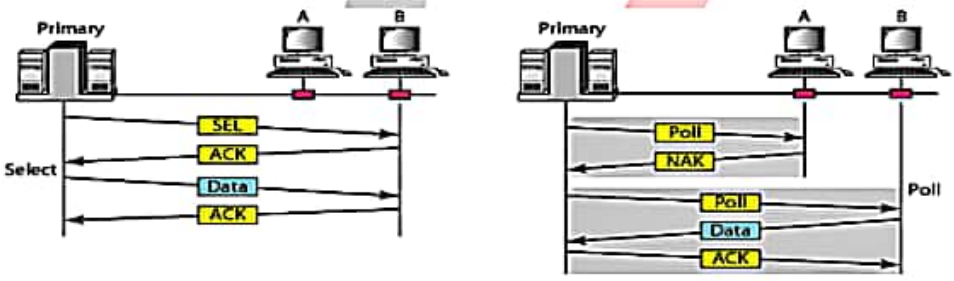


Figure 4.16: Polling System.

III) Token Passing:

- Token passing method is used in those networks where the stations are organized in a logical ring.
- In such networks, a special packet called token is circulated through the ring.
- Station that possesses the token has the right to access the channel.

- Whenever any station has some data to send, it waits for the token.
- It transmits data only after it gets the possession of token.
- After transmitting the data, the station releases the token and passes it to the next station in the ring.
- If any station that receives the token has no data to send, it simply passes the token to the next station in the ring.
- Figure 4.17 shows Token Passing System.

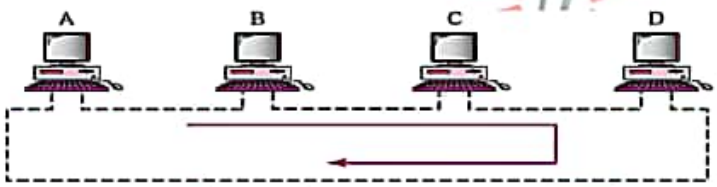


Figure 4.17: Token Passing System.

Q21] Virtual LAN

Ans: **[5M –Dec16]**

VIRTUAL LAN:

1. Virtual LAN is the logical grouping of network nodes.
2. Virtual LAN is defined as a broadcast domain within a switch network.
3. A switch can be configured to support a single or multiple VLANs.
4. Each VLAN becomes its own broadcast domain.
5. VLAN is a solution to divide a single broadcast domain into multiple broadcast domains.
6. Host in one VLAN cannot speak to a host in another.
7. Figure 4.18 shows the example of VLAN.

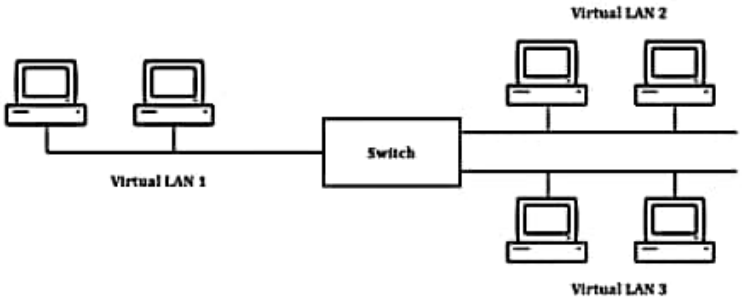


Figure 4.18: Example of VLAN.

BENEFITS OF VLAN:

- It reduces administrative costs.
- It provides segmentation and flexibility.
- It improves bandwidth utilization and reduces network traffic.
- It enforces network security policies.
- Segmenting a large VLAN to smaller VLANs is cheaper than creating a routed network with routers because normally routers costlier than switches.
- VLANs are transparent on the physical topology and medium over which the network is connected.

Q22] What is ICMP protocol? Explain the ICMP Header format with diagram

Ans: **[10M – Dec16]**

ICMP PROTOCOL:

1. ICMP stands for **Internet Control Message Protocol.**
2. ICMP allows routers to send error or control messages to other routers to hosts.
3. ICMP provides communication between the Internet protocol software on one machine and the Internet protocol software on another.
4. ICMP is an **error reporting mechanism.**
5. ICMP messages require two level of encapsulation.
6. Each ICMP message travels across the Internet in the data portion of an IP datagram, which itself travels across each physical network in the data portion of a frame.
7. Figure 4.19 shows the two levels of ICMP encapsulation.

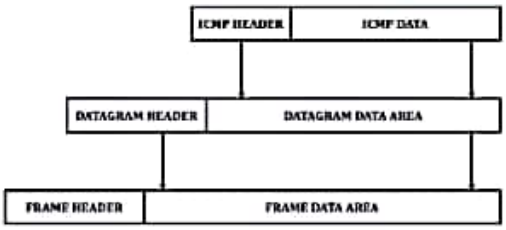


Figure 4.19: Two Levels of ICMP encapsulation.

ICMP HEADER:

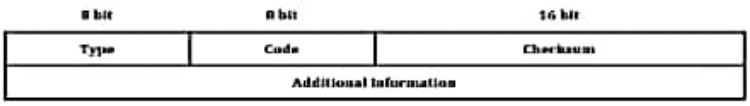


Figure 4.20: ICMP Header Format.

- Figure 4.20 shows ICMP Header Format.
- **Type:** Type field is used to identify the ICMP Message Type.
- **Code:** It provides information of the message type.
- **Checksum:** It is used for error detection.

ICMP MESSAGE TYPE:

Type Field	ICMP Message Type
0	Echo Reply.
3	Destination Unreachable.
4	Source Quench.
5	Redirect.
8	Echo Request.
11	Time Exceeded.
12	Parameter Problem.
13	Timestamp Request.
14	Timestamp Reply.
15	Information Request.
16	Information Reply.
17	Address Mask Request.
18	Address Mask Reply.

ICMP FUNCTIONS:

- Error reporting.
- Reachability testing.
- Congestion control.
- Route change notification.
- Performance measuring.
- Subnet addressing.

Q23] Explain with examples the classification of IPV4 Addresses.

Ans: **[5M – May17]**

1. IPv4 Addressing system is divided into five classes of IP Addresses.
2. Available IP ranges: Class A, Class B, Class C, Class D and Class E.
3. While only A, B, and C are commonly used.

Classification of IPV4 Addresses:

I) Class A Address:

- The first bit of the first octet is always set to 0 (zero). Thus the first octet ranges from 1 – 127, i.e.

  00000001 - **0**1111111
- Class A addresses only include IP starting from 1.x.x.x to 126.x.x.x only.
- The IP range 127.x.x.x is reserved for **loopback IP addresses.**
- The default subnet mask for Class A IP address is 255.0.0.0 which implies that Class A addressing can have 126 networks and 16777214 hosts.
- Class A IP address format is thus: 0NNNNNNN.HHHHHHHH.HHHHHHHH.HHHHHHHH

II) Class B Address:

- An IP address which belongs to class B has the first two bits in the first octet set to 10, i.e.

  10000000 - **10**111111
- Class B IP Addresses range from 128.0.x.x to 191.255.x.x.
- The default subnet mask for Class B is 255.255.x.x.
- Class B has 16384 Network addresses and 65534 Host addresses.
- Class B IP address format is: 10NNNNNN.NNNNNNNN.HHHHHHHH.HHHHHHHH

III) Class C Address:

- The first octet of Class C IP address has its first 3 bits set to 110, that is:

  11000000 - **110**11111
- Class C IP addresses range from 192.0.0.x to 223.255.255.x.
- The default subnet mask for Class C is 255.255.255.x.
- Class C gives 2097152 Network addresses and 254 Host addresses.
- Class C IP address format is: 110NNNNN.NNNNNNNN.NNNNNNNN.HHHHHHHH

IV) Class D Address:

- Very first four bits of the first octet in Class D IP addresses are set to 1110, giving a range of:

  11100000 - **1110**1111
- Class D has IP address rage from 224.0.0.0 to 239.255.255.255.
- Class D is reserved for Multicasting.

- In multicasting data is not destined for a particular host, that is why there is no need to extract host address from the IP address, and Class D does not have any subnet mask.

V) Class E Address:

- This IP Class is reserved for experimental purposes only for R&D or Study.
- IP addresses in this class ranges from 240.0.0.0 to 255.255.255.254.
- Like Class D, this class too is not equipped with any subnet mask.

Q24] Explain distance vector routing. What are its limitations and how they are overcome?

Ans: **[10M – May17]**

DISTANCE VECTOR ROUTING:

1. Distance Vector Routing is one of the dynamic routing algorithm.
2. It is suitable for **packet switched network.**
3. It is used to discover routes on an **interconnected network.**
4. In distance vector routing, each router maintains a routing table.
5. It contains one entry for each router in the subnet.
6. This entry has two parts:
   a. The first part shows the preferred outgoing line to be used to reach the destination.
   b. Second part gives an estimate of the time or distance to the destination.
7. In distance vector routing, a node tells its neighbor about its distance to every other node in the network.
8. Figure 4.21 shows the example of distance vector routing.

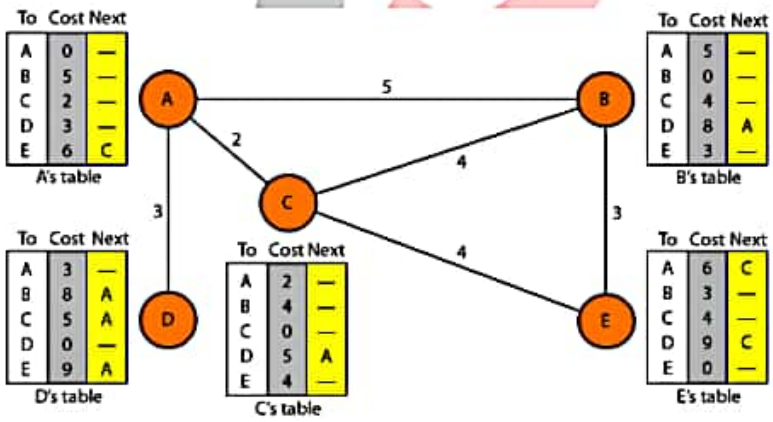
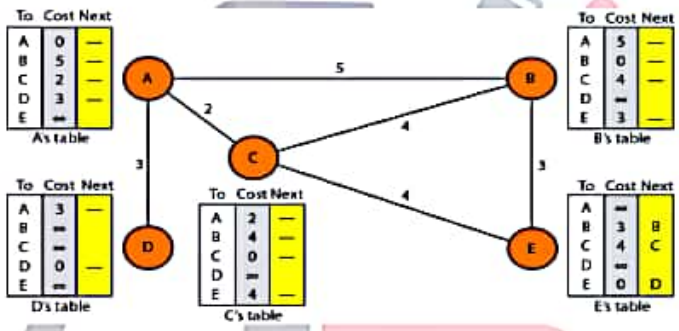


Figure 4.21: Example of Distance Vector Routing.

- Assume each node as the cities.
- Lines as the roads connecting them.

Initialization:

- The table in figure 4.21 are stable.
- Each node knows how to reach any other node and their cost.
- At the beginning, each node know the cost of itself and its immediate neighbor.
- Assume that each node send a message to the immediate neighbors and find the distance between itself and these neighbors.
- The distance of any entry that is not a neighbor is marked as infinite (unreachable).



Sharing

- Idea is to share the information between neighbors.
- The node A does not know the distance about E, but node C does.
- If node C share it routing table with A, node A can also know how to reach node E.
- On the other hand, node C does not know how to reach node D, but node A does.
- If node A share its routing table with C, then node C can also know how to reach node D.
- Node A and C are immediate neighbors, can improve their routing tables if they help each other.

Updating:

- When a node receives a two-column table from a neighbor, it needs to update its routing table.
- Updating takes three steps:
  - The receiving node needs to add the cost between itself and the sending node to each value in the second column. The logic is clear. If node C claims that its distance to a destination is X, and the distance between A and C is Y, then the distance between A and that destination, via C, is X + Y.

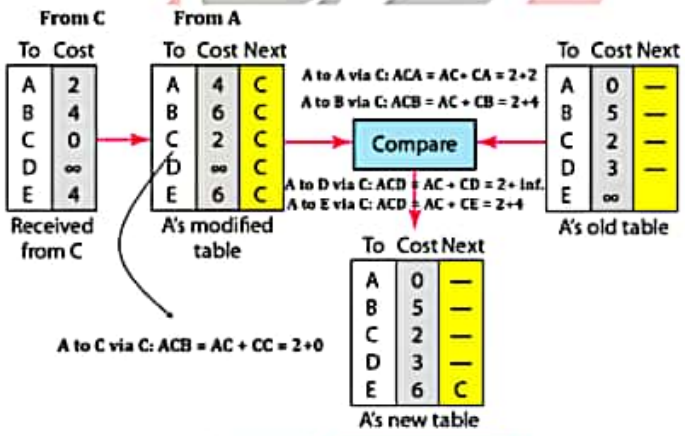
- The receiving node needs to add the name of the sending node to each row as the third column if the receiving node uses information from any row. The sending node is the next node in the route.
- The receiving node needs to compare each row of its old table with the corresponding row of the modified version of the received table.
  - If the next-node entry is different, the receiving node chooses the row with the smaller cost. If there is a tie, the old one is kept.
  - If the next-node entry is the same, the receiving node chooses the new row.

➢ Suppose that now there is no path between C and X; node C now advertises this route with a distance of infinity.

➢ Node A must not ignore this value even though its old entry is smaller.

➢ The old route does not exist anymore.

➢ The new route has a distance of infinity.



LIMITATIONS:

➢ **Slow convergence:** The use of periodic updates can cause slower convergence. Even if some advanced techniques are used like triggered updates, but the overall convergence is still slower compared to link-state routing protocols.

➢ **Limited salability:** Slow convergence can limit the size of the network because larger networks require more time to propagate routing information.

➢ **Routing Loops:** Routing loops can occur when inconsistent routing tables are not updated because of slow convergence in a changing network.

Q25] Differentiate between an IP Address and a MAC or Physical Address. What is the Need to map IP Address to MAC Address? Explain which protocol does this, similarly give a protocol which does reverse mapping.

Ans: **[5M – Dec15]**

COMPARISON BETWEEN IP ADDRESS AND A MAC ADDRESS:

Table 4.5 shows the Comparison between IP Address and a MAC Address

Table 4.5: Comparison between IP Address and a MAC Address.

Points	IP Address	MAC Address
Acronym For	Internet Protocol Address.	Media Access Control Address.
Address Type	It is called as Logical Address.	It is called as Physical Address.
Provided by	It is assigned by User/administrator, DHCP, or ISP.	It is assigned at the time hardware is manufactured.
Length	IPv4 uses 32 bit address in dotted notation, whereas IPv6 uses 128 bit address in hexadecimal notations.	It is 46 bit address which contains 6 group of 2 hexadecimal digits, separated by either hyphens (-) or colons (:)
Use of Classes	IPv4 uses A, B, C, D & E Classes for IP Addressing.	No Classes are used in MAC Addressing.
Spoofing	IP Address Spoofing possible.	MAC Address Spoofing Possible.
Type	It is Software Address.	It is Hardware Address.
Address	Static IP Address: Changeable. Dynamic IP Address: Unchangeable.	Changeable.
Used for	It is Numeric representation of a device that uses TCP/IP.	It is Numeric representation of a device that uses Ethernet.
Subnetting	Subnetting is used.	No Subnetting is used.

NEED TO MAP IP ADDRESS TO MAC ADDRESS:

1. To communicate in a network, there should be some common factor available between the devices.
2. Two machines in a network can communicate only if they know each other's MAC Address.
3. A device that knows only the IP address of another device can use **Address Resolution Protocol** (ARP) to request the physical address of other devices using which they can communicate.
4. Thus ARP is a protocol used for logical to physical address conversation i.e. it converts IP address to MAC address.
5. Similarly, **Reverse Address Resolution Protocol** is used to convert MAC Address back to IP Address.

Q26] Compare Open Loop Congestion Control & Closed Loop Congestion Control.

Ans: **[10M – May16 & Dec16]**

Table 4.6 shows the Comparison between Open Loop & Closed Loop Congestion Control.

Table 4.6: Comparison between Open Loop & Closed Loop Congestion Control.

Points	Open Loop Congestion Control	Closed Loop Congestion Control
Function	In this method, policies are used to prevent the congestion before it happens.	This Method try to remove the congestion after it happens.
Structure	It has simple structure.	It has complex structure.
Stability	It is Stable Method.	This method can cause stability problem.
Cost	Cost is Low.	Cost is High.
Accuracy	Accuracy is Low.	Accuracy is High.
Feedback	This Method does not utilize runtime feedback from the system.	This Method uses the feedback to make corrections at runtime.
Resistance of Disturbance	Resistance of Disturbance is Low.	Resistance of Disturbance is High.
Speed	It has Low Speed.	It has High Speed.
Regulate	It is Easy to Regulate.	It is Complex as compared to Open Loop Congestion Control.
Mechanisms	a. Retransmission Policy. b. Window Policy. c. Acknowledgment Policy. d. Discarding Policy. e. Admission Policy.	a. Back Pressure. b. Choke Point. c. Implicit Signaling. d. Explicit Signaling.

Q27] Compare the network layer protocols IPv4 and IPv6.

Ans: **[10M – Dec14]**

COMPARISON BETWEEN IPV4 & IPV6:

Table 4.7 shows the Comparison between IPv4 & IPv6.

Table 4.7: Comparison between IPv4 & IPv6.

Points	IPv4	IPv6
Deployed	IPv4 was Deployed in 1981.	IPv6 was Deployed in 1999.
Address Size	It has 32 bit address space.	It has 128 bit address space.
Address Format	Dotted Decimal Notation: 192.168.0.1	Hexadecimal Notation: 3FFE:F200:0234:AB00: 0123:4567:8901:ABCD
Checksum	Checksum field is available in Header.	Checksum field is not available in Header.
Packet Size	576 bytes.	1280 bytes.
QoS Support	Provides less Quality of Service.	Provides better Quality of Service.
IP Sec Support	IP Sec Support is optional.	IP Sec Support is required.
Router Discovery	Optional.	Mandatory.
Loopback Address	127.0.0.1	::1
IP Configuration	Manual, DHCP	Automatic, DHCPv6, Manual.
Fragmentation	Host & Router.	Only the Communication Endpoints.
Number of Header Field	12	8
Length of Header Field	20	40
Packet Flow Identification	Not Available.	Available using Flow Label Field.
Communication	It uses both Multicast & Broadcast.	No Broadcast but has different forms of Multicast.
Security	Less	More as compared to IPv4.
Options Field	Options field is available in Header.	Options field is not available in Header.
Link Layer Address Resolution	Address Resolution Protocol (Broadcast).	Multicast Neighbor Discovery Message.

Multicast Membership	IGMP	Multicast Listener Discovery (MLD).
DNS Name Queries	Uses A Records.	Uses AAAA records.
DNS Reverse Queries	Uses IN-ADDR.ARPA	Uses IP6.INT

Q28] Differentiate between OSPF & BGP

Ans: **[5M – May15]**

COMPARISON BETWEEN OSPF & BGP:

Table 4.8 shows the Comparison between OSPF & BGP.

Table 4.8: Comparison between OSPF & BGP.

Points	OSPF	BGP
Acronym For	Open Shortest Path First.	Border Gateway Protocol.
Gateway Protocol	OSPF is an internal gateway protocol.	BGP is an external gateway protocol.
Implementation	Easy to Implement.	Complex to Implement.
Convergence	Fast.	Slow.
Design	Hierarchical Network Possible.	Fully Meshed.
Need of Device Resources	Memory & CPU Intensive.	Depends on the size of the routing table but scales better than OSPF.
Scaled Networks	OSPF is mainly used on smaller scale networks that are centrally administered.	BGP protocol is mainly used on very large-scale networks, like the internet.
Function	OSPF will always search for the fastest route, and not the shortest, in spite of its name.	BGP focuses in determining the best path for a datagram.
Algorithm Used	Dijkstra Algorithm.	Best Path Algorithm.
Protocol	IP Protocol.	TCP Protocol.
Port	89.	179.
Type	Link State.	Path Vector.

Q29] Compare and contrast a circuit switching and a packet switching network.

Ans: **[5M – May17]**

COMPARISON BETWEEN CIRCUIT SWITCHING & PACKET SWITCHING NETWORK:

Table 4.9 shows the Comparison between Circuit Switching & Packet Switching Network.

Table 4.9: Comparison between Circuit Switching & Packet Switching Network.

Points	Circuit Switching Network	Packet Switching Network
Orientation	Connection oriented.	Connectionless.
Purpose	Initially designed for **Voice communication.**	Initially designed for **Data Transmission.**
Dedicated Path	Yes.	No.
Flexibility	**Inflexible**, because once a path is set all parts of a transmission follows the same path.	**Flexible**, because a route is created for each packet to travel to the destination.
Order	Message is received in the order, sent from the source.	Packets of a message are received out of order and assembled at the destination.
Bandwidth	Fixed Bandwidth.	Dynamic Bandwidth.
Technology/Approach	Circuit switching can be achieved using two technologies, either **Space Division Switching** or **Time-Division Switching.**	Packet Switching has two approaches **Datagram Approach** and **Virtual Circuit Approach.**
Delay	Call Setup Delay.	Packet Transmission Delay.
Overhead Bits	No overhead bits after call setup.	Overhead bits in each packets.
Layers	Circuit Switching is implemented at **Physical Layer.**	Packet Switching is implemented at **Network Layer.**

Q30] An ISP is granted a block of address starting with 150.80.0.0/16. The ISP wants to distribute these blocks to 2600 customers as follows.

a. **The First group has 200 medium-size businesses; each needs 128.**
b. **The Second group has 400 small-size businesses; each needs 16.**
c. **The Third group has 2000 households; each needs 4 addresses.**

Design the sub blocks & give the slash notation for each sub block. Find out how many addresses are still available after these allocations.

Ans: **[10M – May16]**

ISP:

1. The total number of addresses in this block is $2^{32-16} = 65536$.
2. The ISP can divide this large block in several ways depending on the predicted needs of its customers in the future.
3. We assume that the future needs follow the present pattern.
4. In other words, we assume that the ISP will have customers that belong to one of the present groups.
5. We design four ranges: group 1, group 2, group 3, and one reserved range of addresses as shown in figure 4.22 below.

Group 1: Addresses 150.80.0.0 to 150.80.127.255
Group 2: Addresses 150.80.128.0 to 150.80.159.255
Group 3: Addresses 150.80.160.0 to 150.80.191.255
Reserved: Addresses 150.80.192.0 to 150.80.255.255

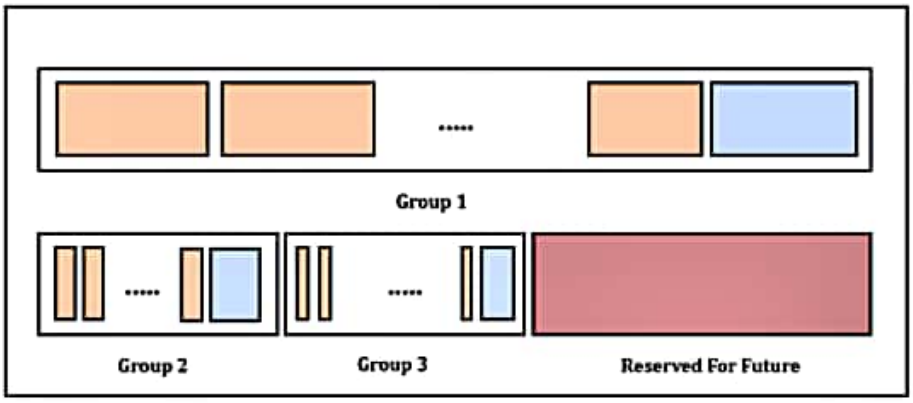


Figure 4.22: One Granted Block of 65,536 Addresses.

GROUP 1:

- In the first group, we have 200 businesses.
- We augment this number to 256 (the next number after 200 that is a power of 2) to let 56 more customers of this kind in the future.
- The total number of addresses is 256 × 128 = 32768.
- For this group, each customer needs 128 addresses.
- This means the suffix length is $\log_2 128 = 7$. The prefix length is then 32 – 7 = 25.
- The addresses are:
  - **1st customer:** 150.80.0.0/25 to 150.80.0.127/25
  - **2nd customer:** 150.80.0.128/25 to 150.80.0.255/25
  - ... ...
  - **200th customer:** 150.80.99.128/25 to 150.80.99.255/25
- Unused addresses 150.80.100.0 to 150.80.127.255
- Total Addresses in group 1 = 256 × 128 = 32768
- Used = 200 × 128 = 25600.
- Reserved: 7168, which can be assigned to 56 businesses of this size.

GROUP 2:

- In the second group, we have 400 business.
- We augment this number to 512 (the next number after 400 that is a power of 2) to let 112 more customer of this kind in the future.
- The total number of addresses is = 512 × 16 = 8192.
- For this group, each customer needs 16 addresses.
- This means the suffix length is 4 i.e. $\log_2 16 = 4$. The prefix length is then 32 – 4 = 28.
- The addresses are:
  - **1st customer:** 150.80.128.0/28 to 150.80.128.15/28
  - **2nd customer:** 150.80.128.16/28 to 150.80.128.31/28
  - ... ...
  - **400th customer:** 150.80.152.240/28 to 150.80.152.255/28
- Unused addresses 150.80.153.0 to 150.80.159.255
- Total Addresses in group 2 = 512 × 16 = 8192
- Used = 400 × 16 = 6400
- Reserved: 1792, which can be assigned to 112 businesses of this size.

GROUP 3:

- In the third group, we have 2000 households.
- We augment this number to 2048 (the next number after 2000 that is a power of 2) to let 48 more customer of this kind in the future.
- The total number of addresses is = 2048 × 4 = 8192.
- For this group, each customer needs 4 addresses.
- This means the suffix length is 2 i.e. $\log_2 4 = 2$. The prefix length is then 32 – 2 = 30.
- The addresses are:
  - **1st customer:** 150.80.160.0/30 to 150.80.160.3/30
  - **2nd customer:** 150.80.160.4/30 to 150.80.160.7/30
  - ... ...
  - **2000th customer:** 150.80.191.60/30 to 150.80.191.63/30
- Unused addresses 150.80.191.64 to 150.80.191.255.
- Total Addresses in group 3 = 2048 × 4 = 8192
- Used = 2000 × 4 = 8000
- Reserved: 192, which can be assigned to 48 households.

RESERVED RANGE:

In the reserved range, we have 16384 address that are totally unused.

Q31] An ISP is granted a block of addresses starting with 190.100.0.0/16 (65, 536 addresses). The ISP needs to distribute these addresses to three groups of customers as follows:

(i) The first group has 64 customers; each needs 256 addresses.

(ii) The second group has 128 customers; each needs 128 addresses.

(iii) The third group has 128 customers; each needs 64 addresses.

Design the sub blocks and find out how many addresses are still available after these allocations.

Ans: **[10M – Dec16]**

ISP:

1. The total number of addresses in this block is 65536.
2. The ISP can divide this large block in several ways depending on the predicted needs of its customers in the future.

3. We assume that the future needs follow the present pattern.
4. In other words, we assume that the ISP will have customers that belong to one of the present groups.
5. We design four ranges: group 1, group 2, group 3, and one reserved range of addresses as shown in figure 4.23 below.

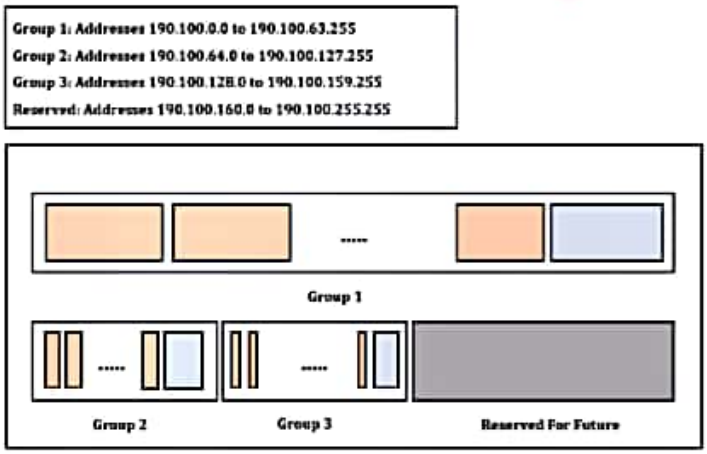


Figure 4.23: One Granted Block of 65,536 Addresses.

GROUP 1:

The suffix length is 8 ($2^8 = 256$).

The prefix length is then 32 - 8 = 24.

The addresses are:

Customer 1: 190.100.0.0/24 → 190.100.0.255/24

Customer 2: 190.100.1.0/24 → 190.100.1.255/24

Customer 64: 190.100.63.0/24 → 190.100.63.255/24

Total = 64 x 256 = 16,384

GROUP 2:

Suffix length is 7 ($2^7 = 128$).

The prefix length is then 32 - 7 = 25.

The addresses are:

Customer 1: 190.100.64.0/25 → 190.100.64.127/25

Customer 2: 190.100.64.128/25 → 190.100.64.255/25

Customer 128: 190.100.127.128/25 → 190.100.127.255/25

Total = 128 x 128 = 16,384

GROUP 3:

Suffix length is 6 ($2^6 = 64$).

The prefix length is then 32 - 6 = 26.

Customer 1: 190.100.128.0/26 → 190.100.128.63/26

Customer 2: 190.100.128.64/26 → 190.100.128.127/26

Customer 128: 190.100.159.192/26 → 190.100.159.255/26

Total = 128 x 64 = 8,192

Therefore,

No. of granted addresses to the ISP: **65,536**

No. of allocated addresses by the ISP: 40,960

No. of available addresses: **24,576**

CHAPTER - 5: TRANSPORT LAYER

Q1] What are transport service primitives? Discuss in brief.

Ans: **[10M – Dec15]**

TRANSPORT SERVICE PRIMITIVES:

1. A service in a computer network consists of a set of primitives.
2. A Primitive is nothing but an operations.
3. Transport Layer Primitives allow the transport user such as application programs to access the transport service.
4. Primitive asks the service to do some action or to report on an action.
5. Primitives can be considered as system calls.
6. The primitive varies for different services.

Table 5.1: Transport Service Primitives.

Primitive	TPDU Sent	Meaning
LISTEN	None	Block until some process tries to connect.
CONNECT	Connect Request	Actively Attempt to Establish Connection.
SEND	Data	Send Data.
RECEIVE	None	Block until a data TPDU Arrives.
DISCONNECT	Disconnect Request	Release the Connection.

NESTING OF TPDU, PACKETS & FRAMES:

1. TPDU Stands for Transport Layer Data Unit.
2. TPDUs are contained in packets.
3. In turn, Packets are contained in frames.
4. TPDUs are exchanged by the transport layer.
5. Packets are exchanged by the network layer.
6. Frames are exchanged by the data link layer.
7. When a frame arrives, the data link layer processes the frame header and passes the contents of the frame payload field up to the network entity.
8. Figure 5.1 shows the Nesting of TPDUs, Packets & Frames.

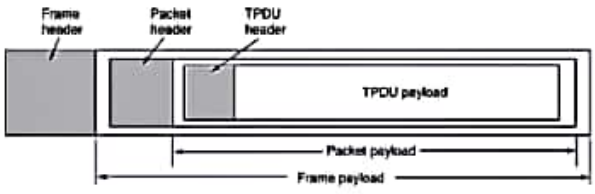


Figure 5.1: Nesting of TPDUs, Packets & Frames.

EXAMPLE OF HOW TRANSPORT SERVICE PRIMITIVE WORKS:

1. Consider an application with a server and a number of remote clients.
2. Now Server executes a LISTEN primitive, by calling a library procedure that makes a system call to block the server until a client turns up.
3. When a client wants to talk to the server, it executes a CONNECT primitive.
4. The transport entity carries out this primitive by blocking the caller and sending a packet to the server.
5. Transport layer message for the server's transport entity is encapsulated in the payload of this packet.
6. Now Client's CONNECT call causes a CONNECTION REQUEST, TPDU to be sent to the server.
7. When it arrives, the transport entity checks to see that the server is blocked on a LISTEN (i.e., is interested in handling requests).
8. It then unblocks the server and sends a CONNECTION ACCEPTED, TPDU back to the client.
9. When this TPDU arrives, the client is unblocked and the connection is established.
10. Data can now be exchanged using the SEND and RECEIVE primitives.
11. As long as both sides can keep track of whose turn it is to send, this scheme works fine.
12. When a connection is no longer needed, it must be released to free up table space within the two transport entities.
13. Disconnection has two variants: asymmetric and symmetric.

Q2] Explain the different elements of transport protocols.

Ans: **[10M – Dec14]**

TRANSPORT LAYER:

1. Transport Layer is responsible for **process-to-process delivery of the entire message.**
2. It looks after the delivery of entire message considering all its packets & make sure that all packets are in order.
3. At the receiver side, Transport Layer provides services to application layer & takes services form network layer.
4. At the source side, Transport Layer receives message from upper layer into packets and reassembles these packets again into message at the destination.

ELEMENTS OF TRANSPORT PROTOCOL:

I) Addressing:

- In order to deliver data from one process to another, address is required.

- Address can be IP Address or MAC Address.
- MAC Address is implemented at Data Link Layer & is called as Physical Addressing.
- Whereas IP Address is implemented at Network Layer & is called as Logical Addressing.
- To deliver data from a process running on source end to process running on destination end, transport layer defines the Service Point Address or Port Numbers.

II) Port Numbers:

- Port Number is the transport layer address.
- Source Port Number is required for reply & Destination Port Number is required for delivery.
- The Port Numbers are the integers between 0 and 65,535.
- Each communicating process is assigned a specific port number.
- In order to select among multiple processes running on a destination host, a port number is required.
- Port numbers are assigned by Internet Assigned Number Authority (IANA).
- IANA has divided the port numbers in three categories:
  - **Well Known Ports:** The ports ranging from 0 to 1023. For e.g.: HTTP: 80, SMTP: 25, FTP: 21.
  - **Registered Ports:** The ports ranging from 1024 to 49,151. These are not controlled by IANA.
  - **Dynamic Ports:** The ports ranging from 49,152 to 65,535. These can be used by any process.

III) Socket Address:

- Socket address is a combination of IP address and Port Number.
- In order to provide communication between two different processes on different networks, both IP address and port number, i.e. socket address is required.
- Figure 5.2 shows Socket Addressing.

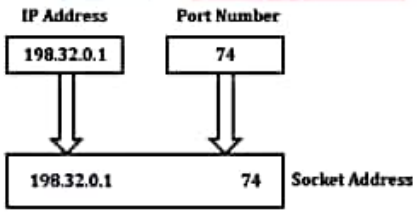


Figure 5.2: Socket Address.

IV) Multiplexing & De-multiplexing:

- A network connection can be shared by various applications running on a system.
- There may be several running processes that want to send data and only one transport layer connection available, then transport layer protocols may perform multiplexing.

- The protocol accepts the messages from different processes having their respective port numbers, and add headers to them.
- The transport layer at the receiver end performs de-multiplexing to separate the messages for different processes.
- After checking for errors, the headers of messages are dropped and each message is handed over to the respective processes based on their port numbers.
- Figure 5.3 shows Multiplexing & De-Multiplexing Process.

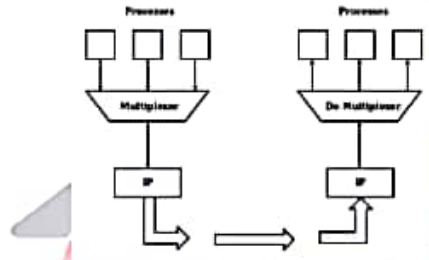


Figure 5.3: Multiplexing & De-Multiplexing.

V) Connection Establishment:

- Before communicating, the source device must first determine the availability of the other to exchange data.
- Path must be found through the network by which the data can be sent.
- This is called Connection Establishment.
- Connection establishment involves Three-Way Handshaking mechanism:
  - The source sends a connection request packet to the destination.
  - The destination returns a confirmation packet back to the source.
  - The source returns a packet acknowledging the confirmation.

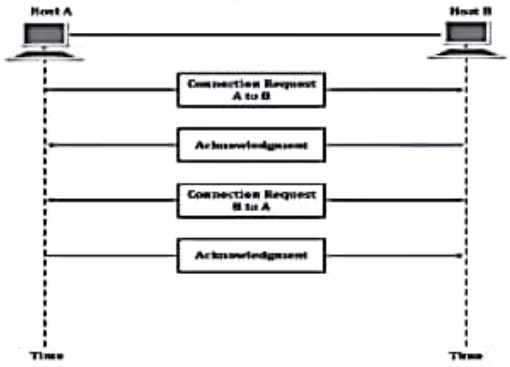


Figure 5.4: Establishing a Connection.

VI) Connection Release:

- Once all of the data has been transferred, the connection must be released.
- Any of the two parties involved in data exchange can close the connection.
- It also requires a **Three-Way Handshaking mechanism**:
  - The source sends a disconnect request packet to the destination.
  - The destination returns a confirmation packet back to the source.
  - The source returns a packet acknowledging the confirmation.

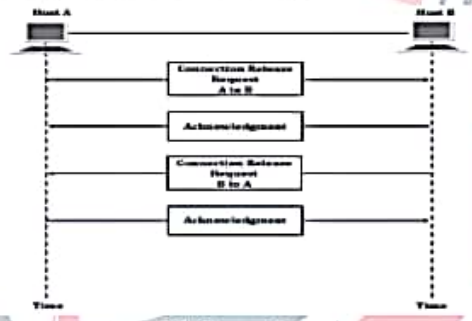


Figure 5.5: Connection Release.

VII) Flow Control & Buffering:

- The sender process may send at much higher speed than the receiver process can handle the data thus causing overflow.
- In order to avoid this Overflow problem, the receiver buffers incoming packets.
- A sliding window mechanism provides a "backpressure" to the sender process when the buffer is imminent to overflow.
- The receiver process continuously tells the sending process how much empty space is left in the receive buffer.
- The sender process never sends more data than can be accommodated in the receive buffer.
- Figure 5.6 shows TCP Flow Control & Buffering

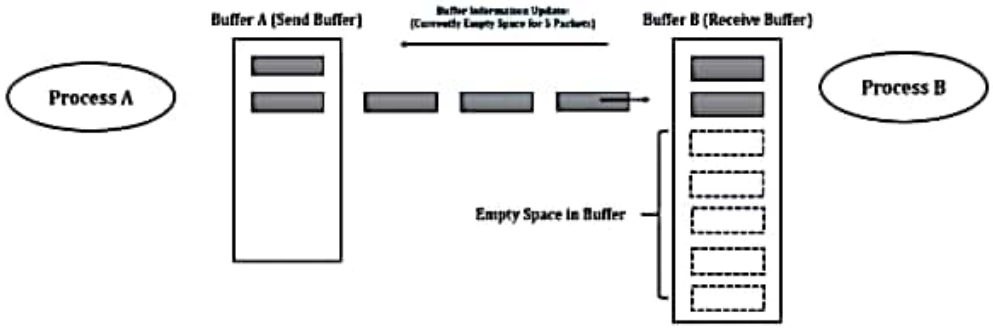


Figure 5.6: TCP Flow Control & Buffering.

VIII) **Cash Recovery:**

- A crash of one host (server) during the transmission leads to a connection loss which results in data loss.
- Proposed Solution is client should retransmits only unacknowledged packets.
- But this solution does not work in all cases because the server sends the ACK and writes the data to the application sequentially.

Q3] Berkeley Socket.

Ans: **[5M – May15]**

SOCKET:

1. Sockets are a service provided by transport layer.
2. A socket is one endpoint of a two-way communication link between two programs running on the network.

BERKELEY SOCKET:

1. Berkeley sockets is an application programming interface (API) for Internet sockets and UNIX domain sockets.
2. It is used for **inter-process communication (IPC).**
3. It is commonly implemented as a library of linkable modules.
4. It originated with the 4.2BSD UNIX released in 1983.

PRIMITIVE USED IN BERKELEY SOCKET:

Table 5.2: List of Primitives used in Berkeley UNIX for TCP.

Primitives	Meaning
SOCKET	Create a New Communication Endpoint.
BIND	Attach a Local Address to a SOCKET.
LISTEN	Shows the Willingness to Accept Connections.
ACCEPT	Block the Caller until a Connection Attempts Arrives.
CONNECT	Actively Attempt to Establish a Connection.
SEND	Send Some Data over Connection.
RECEIVE	Receive Some Data from the Connection.
CLOSE	Release the Connection.

SOCKET PROGRAMMING:

I) **Server side:**

- Server startup executes SOCKET, BIND & LISTEN primitives.

- LISTEN primitive allocate queue for multiple simultaneous clients.
- Then it use ACCEPT to suspend server until request.
- When client request arrives: ACCEPT returns.
- Start new socket (thread or process) with same properties as original, this handles the request, server goes on waiting on original socket.
- If new request arrives while spawning thread for this one, it is queued.
- If queue full it is refused.

II) **Client side:**

- It uses SOCKET primitives to create.
- Then use CONNECT to initiate connection process.
- When this returns the socket is open.
- Both sides can now SEND, RECEIVE.
- Connection not released until both sides do CLOSE.
- Typically client does it, server acknowledges.

Q4] Explain three way handshake technique in TCP.

Ans: **[10M – May15]**

THREE WAY HANDSHAKE TECHNIQUE:

1. A three-way-handshake is a method used in a TCP/IP network to create a connection between a local host/client and server.
2. Therefore it creates a TCP Socket Connection.
3. It is a three-step method that requires both the client and server to exchange SYN and ACK (acknowledgment) packets before actual data communication begins.
4. A three-way-handshake is also known as a TCP handshake.

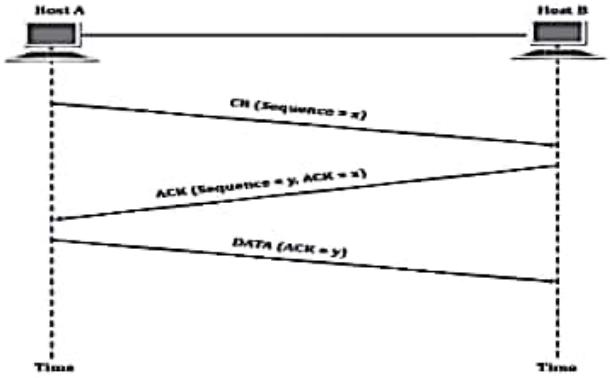


Figure 5.7: Three Way Handshake Technique.

WORKING:

1. Host A choose a sequence number for example 'x' and sends a Connection Request (CR) TPDU containing it to Host B.
2. Host B replies with a connection accepted TPDU to acknowledgment 'x' and announce its own sequence number for example 'y'.
3. Now Host A acknowledges Host B and send the first data TPDU.

OPERATION IN THE ABNORMAL CIRCUMSTANCES:

1. The first TPDU to Host B is a Delayed Duplicate Connection Request from an Old Connection.
2. Host A does not know about it.
3. Host B receives this TPDU and sends Connection Accepted TPDU to Host A.
4. But in this case, Host A is not trying to establish any connection, so it sends a Reject along with Acknowledgment i.e. ACK = y as shown in figure 5.8.
5. So Host B realizes that it was fooled by a Delayed Duplicate and abandons the connection.

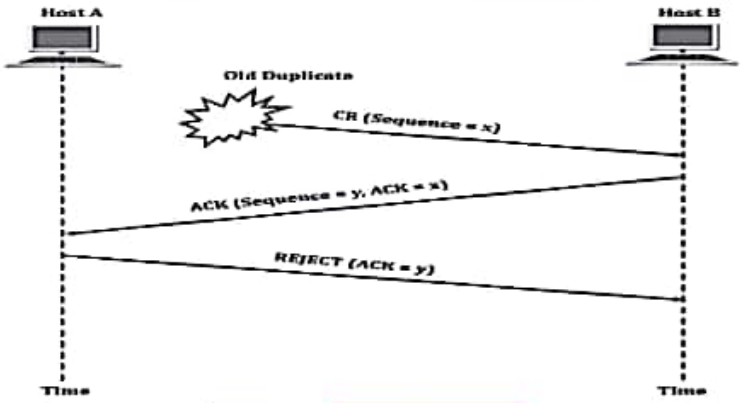


Figure 5.8: Response to an Old Duplicate.

OPERATION WHEN DUPLICATE CR & DUPLICATE ACK:

1. This is another abnormal situation.
2. This is the worst case in which delayed duplicates of Connection Request (CR) and Acknowledgment (ACK) are floating around in the subnet.
3. Host B gets a Connection Request (CR) and it replies to it by sending ACK.
4. By this Host B has proposed a connection with a sequence number say 'y'.
5. When the second delayed TPDU (duplicate) arrives at Host B, it understands that 'z' has been acknowledged and not 'y'.
6. So it understands that this too is an Old Duplicate.

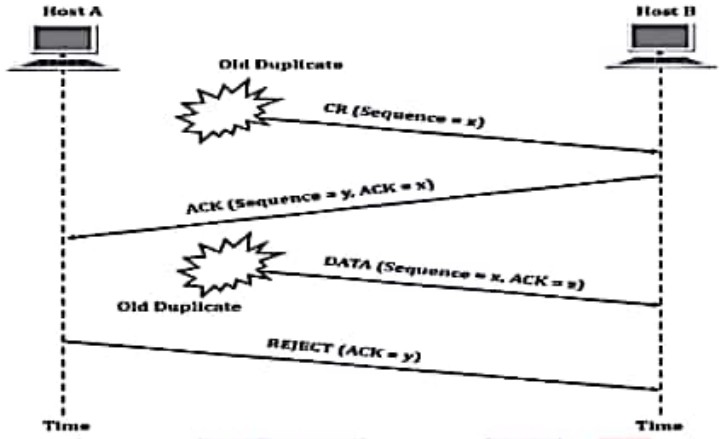


Figure 5.9: Duplicate CR & Duplicate ACK.

Q5] Explain how TCP handles error control and flow control.

Ans: **[10M – Dec14]**

TCP:

1. TCP Stands for **Transmission Control Protocol.**
2. It is used for Process-to-Process communication.
3. It is Connection-oriented service.
4. It is Stream-oriented protocol.
5. TCP provides Full Duplex communication.
6. TCP Provides Segmentation& Utilizes buffers at both ends.

ERROR CONTROL IN TCP:

1. TCP considers a segment as a unit of data for error detection.
2. TCP includes mechanisms for detecting corrupted segments, lost segments, out-of-order segments and duplicated segments.
3. This is achieved through the use of three simple tools:
   a. Checksum.
   b. Acknowledgement.
   c. Retransmission.

I) Checksum:

- TCP uses a 16-bit checksum.
- Each segment in TCP includes a checksum field.
- This Checksum field is used to check for corrupted segment.

- Corrupted segment is discarded by the destination and is considered lost.

II) Acknowledgement:

- In this method, TCP confirms the receipt of data segments.
- Control segments that carry no data but consume a sequence number are also considered as acknowledged.
- ACK segments are never acknowledged.

III) Retransmission:

- A segment is retransmitted on two occasions:
  - When a retransmission timer expires.
  - When the sender receives three duplicate ACKs.
- There is no retransmission for ACK segments.
- Retransmission after Retransmission Timeouts(RTO):
  - TCP maintains one RTO timer for all outstanding (sent, but not acknowledged) segments.
  - When the timer matures, the earliest outstanding segment is retransmitted.
  - Value of RTO is dynamic and is updated based on Round Trip Timer (RTT).

FLOW CONTROL IN TCP:

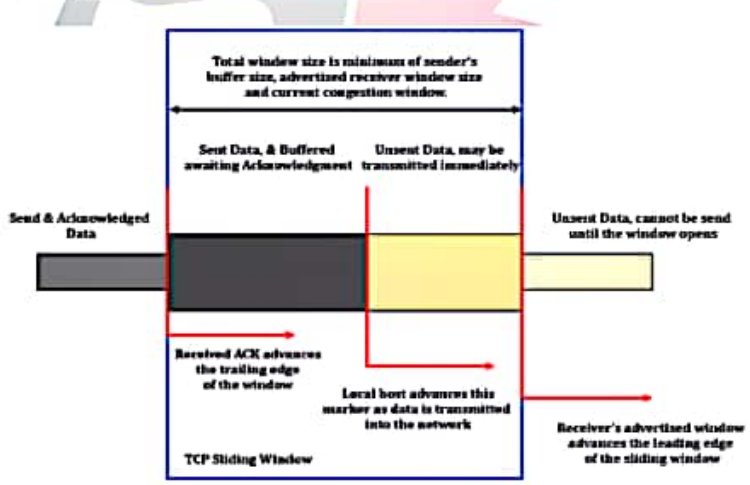


Figure 5.10: Flow Control in TCP using Sliding Window.

1. Figure 5.10 shows Flow Control in TCP using Sliding Window.
2. In TCP Receiver controls the amount of data that are to be sent by the sender.
3. Numbering system allows TCP to use byte-oriented flow control.
4. TCP uses sliding window to handle flow control.

5. The size of the window is determined by the lesser of two values: Receiver Window (rwnd) or Congestion Window (cwnd).
   a. **rwnd:** It is the number of bytes the receiver can accept before its buffer overflows.
   b. **cwnd:** It is the value determined by the network to avoid congestion.
6. The receiver controls most of the aspects.

Q6] TCP Connection Management.

Q7] Explain with the help of suitable diagram TCP connection management and release

Ans: **[Q6 | 10M – Dec15] & [Q7 | 10M – May17]**

1. In TCP, the connections are established using three way handshake technique.
2. TCP Connection Management includes TCP Connection Establishment & TCP Connection Release.

TCP CONNECTION ESTABLISHMENT:

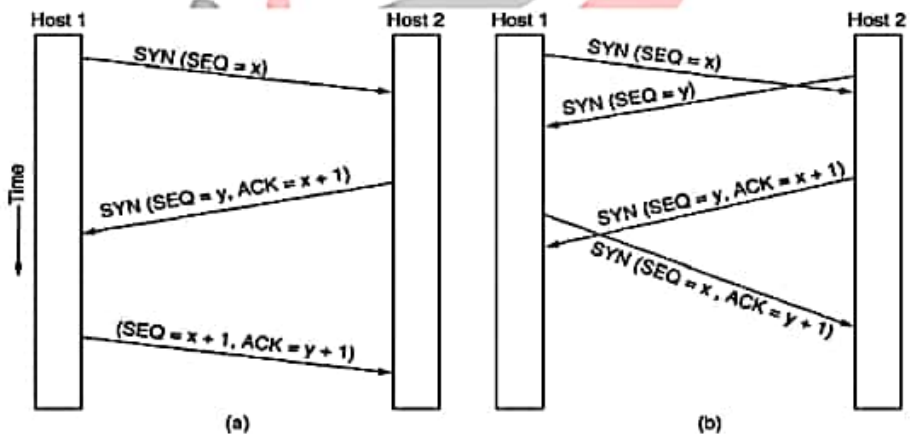


Figure 5.11: (a) Normal Operation & (b) Call Collision Case.

1. To establish a connection, one side, say, the server, passively waits for an incoming connection by executing the LISTEN and ACCEPT primitives, either specifying a specific source or nobody in particular.
2. The other side, say, the client, executes a CONNECT primitive, specifying the IP address and port to which it wants to connect, the maximum TCP segment size it is willing to accept, and optionally some user data (e.g., a password).
3. The CONNECT primitive sends a TCP segment with the SYN bit on and ACK bit off and waits for a response.

4. When this segment arrives at the destination, the TCP entity there checks to see if there is a process that has done a LISTEN on the port given in the Destination port field.
5. If not, it sends a reply with the (Reset) RST bit on to reject the connection.
6. If some process is listening to the port, that process is given the incoming TCP segment.
7. It can then either accept or reject the connection.
8. Normal case is shown in Figure 5.11 (a).
9. In the event that two hosts simultaneously attempt to establish a connection between the same two sockets, the sequence of events is as illustrated in Figure 5.11 (b).
10. The result of these events is that just one connection is established, not two because connections are identified by their end points.

TCP CONNECTION RELEASE:

1. TCP connections are full duplex.
2. Each simplex connection is released independently of its sibling.
3. To release a connection, either party can send a TCP segment with the FIN bit set, which means that it has no more data to transmit.
4. When the FIN is acknowledged, that direction is shut down for new data.
5. Data may continue to flow indefinitely in the other direction, however.
6. When both directions have been shut down, the connection is released.
7. Normally, four TCP segments are needed to release a connection, one FIN and one ACK for each direction.
8. However, it is possible for the first ACK and the second FIN to be contained in the same segment, reducing the total count to three.
9. To avoid the two-army problem, timers are used.
10. If a response to a FIN is not forthcoming within two maximum packet lifetimes, the sender of the FIN releases the connection.
11. The other side will eventually notice that nobody seems to be listening to it anymore and will time out as well.
12. While this solution is not perfect, given the fact that a perfect solution is theoretically impossible, it will have to do. In practice, problems rarely arise.

FINITE STATE MACHINE FOR CONNECTION ESTABLISH & RELEASE:

Table 5.3: States in TCP Finite State Machine.

State	Description
CLOSED	No Connection is active or pending.
LISTEN	The server is waiting for an incoming call.
SYN RCVD	A connection request has arrived; wait for ACK.

SYN SENT	The application has started to open a connection.
ESTABLISHED	The normal data transfer state.
FIN WAIT 1	The application has said it is finished.
FIN WAIT 2	The other side has agreed to release.
TIMED WAIT	Wait for all packets to die off.
CLOSING	Both sides have tried to close simultaneously.
CLOSE WAIT	The other side has initiated a release.
LAST ACK	Wait for ACK of FIN of last close.

1. In each of the 11 states shown in table 4.3, some specific events are legal.
2. Corresponding to every legal event some action may be taken, but if some other event happens, then error is reported.
3. Each Connection is always in the CLOSED State Initially.
4. It comes out of this state when it does either the passive open (LISTEN) or an active open (CONNECT).
5. A connection is established, if the other side does the opposite and the state becomes ESTABLISHED.
6. When the both the sides initiate a connection release the connection is terminated and the state returns to CLOSED state.

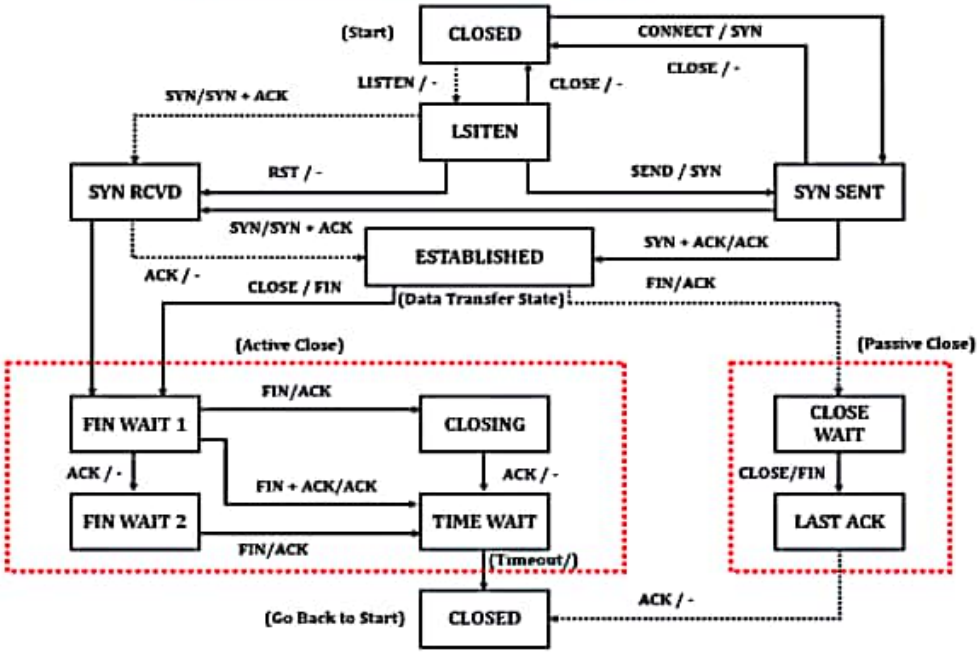


Figure 5.12: TCP Connection Management Finite State Machine.

Q8] Write a Program for Client Server Application using Socket Programming.

Ans: **[10M – May16 & Dec16]**

TCP/IP SOCKET PROGRAMMING:

1. The two key classes from the java.net package used in creation of server and client programs are:
   a. ServerSocket.
   b. Socket.
2. A server program creates a specific type of socket that is used to listen for client requests (server socket).
3. In the case of a connection request, the program creates a new socket through which it will exchange data with the client using input and output streams.
4. The socket abstraction is very similar to the file concept: Developers have to open a socket, perform I/O, and close it.
5. Figure 5.13 illustrates key steps involved in creating socket-based server and client programs.

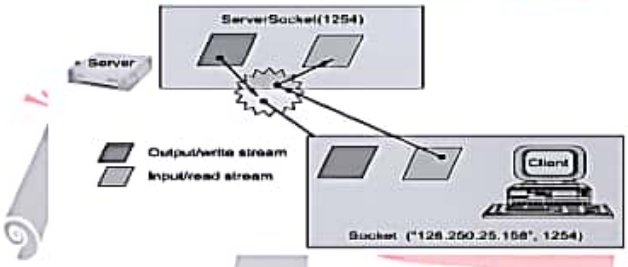


Figure 5.13: Socket Based Client & Server Programming.

SERVER SOCKET PROGRAMMING IN JAVA:

```
// SimpleServer.java: A simple server program.

import java.net.*;
import java.io.*;
public class SimpleServer
{
    public static void main(String args[]) throws IOException
    {
    // REGISTER SERVICE ON PORT 1254

    ServerSocket s = new ServerSocket(1254);
    Socket s1 = s.accept(); // Wait and accept a connection

    // GET A COMMUNICATION STREAM ASSOCIATED WITH THE SOCKET

    OutputStream slout = s1.getOutputStream();
    DataOutputStream dos = new DataOutputStream (slout);

    // SEND A STRING!

    dos.writeUTF("Welcome To Topper's Solutions");

    // CLOSE THE CONNECTION, BUT NOT THE SERVER SOCKET

    dos.close();
    slout.close();
    s1.close();
    }
}
```

CLIENT SOCKET PROGRAMMING IN JAVA:

```
// SIMPLECLIENT.JAVA: A SIMPLE CLIENT PROGRAM.

import java.net.*;
import java.io.*;

public class SimpleClient
{
    public static void main(String args[]) throws IOException
    {

    // OPEN YOUR CONNECTION TO A SERVER, AT PORT 1254

    Socket s1 = new Socket("localhost",1254);

    // GET AN INPUT FILE HANDLE FROM THE SOCKET AND READ THE INPUT

    InputStream s1In = s1.getInputStream();
    DataInputStream dis = new DataInputStream(s1In);
    String st = new String (dis.readUTF());
    System.out.println(st);

    // WHEN DONE, JUST CLOSE THE CONNECTION AND EXIT
    dis.close();
    s1In.close();
    s1.close();
 }
}
```

— EXTRA QUESTIONS —

Q1] Explain how congestion control is achieved in TCP?

Ans:

1. When a connection is established, a suitable window size has to be chosen.
2. The receiver can specify a window based on its buffer size.
3. If the sender sticks to this window size, problems will not occur due to buffer overflow at the receiving end, but they may still occur due to internal congestion within the network.
4. In Figure 5.14 (a), we see a thick pipe leading to a small-capacity receiver.
5. As long as the sender does not send more water than the bucket can contain, no water will be lost.
6. In Figure 5.14 (b), the limiting factor is not the bucket capacity, but the internal carrying capacity of the network.
7. If too much water comes in too fast, it will back up and some will be lost.
8. Each sender maintains two windows: the window the receiver has granted and a second window, the congestion window.
9. Each reflects the number of bytes the sender may transmit.
10. The number of bytes that may be sent is the minimum of the two windows.
11. Thus, the effective window is the minimum of what the sender thinks is all right and what the receiver thinks is all right.

Q2] Compare UDP and TCP.

Ans:

Table 5.4: Comparison between TCP & UDP.

PARAMETER	TCP	UDP
Name	Transmission Control Protocol.	User Datagram Protocol.
Connection	TCP is a connection-oriented protocol.	UDP is a connectionless protocol.
Use by other protocols	HTTP, HTTPs, FTP, SMTP, Telnet.	DNS, DHCP, TFTP, SNMP, RIP, VOIP.
Ordering of data packets	TCP rearranges data packets in the order specified.	UDP has no inherent order as all packets are independent of each other. If ordering is required, it has to be managed by the application layer.
Speed of transfer	The speed for TCP is slower than UDP.	UDP is faster because there is no error-checking for packets.
Header Size	TCP header size is 20 bytes.	UDP Header size is 8 bytes.
Error Checking	TCP does error checking	UDP does error checking, but no recovery options.
Flow Control	TCP Provides Flow Control.	UDP Does not provides Floe Control.
Reliability	Reliability is maintained.	Reliability is not maintained.
Usage	TCP is suited for applications that require high reliability, and transmission time is relatively less critical.	UDP is suitable for applications that need fast, efficient transmission, such as games.

CHAPTER - 6: APPLICATION LAYER

Q1] Explain the need for DNS and describe the protocol functioning.

Ans: **[10M - Dec14 & May15]**

DNS:

1. DNS Stands for **Domain Name System**.
2. DNS is a hierarchical decentralized naming system for computers, services, or any resource connected to the Internet or a private network.
3. DNS is an Internet service that translates domain names into IP addresses.
4. Because domain names are alphabetic, they're easier to remember.
5. The Internet however, is really based on IP addresses.
6. Every time you use a domain name, therefore, a DNS service must translate the name into the corresponding IP address.
7. For example, the domain name www.ToppersSolutions.com might translate to 198.105.232.4.

NEED FOR DNS:

1. One identifier for a host is its hostname.
2. Hostnames are mnemonic and are therefore appreciated by humans. such as:
   a. www.ToppersSolutions.com.
   b. www.Facebook.com.
   c. www.Google.co.in.
   d. surf.eurecom.fr.
3. Hostnames provide little information about the location within the Internet of the host.
4. A hostname such as surf.eurecom.fr, which ends with the country code .fr, tells us that the host is in France, but doesn't say much more.
5. Furthermore, because hostnames can consist of variable-length alpha-numeric characters, they would be difficult to process by routers.
6. For these reasons, hosts are also identified by so-called **IP addresses.**
7. An IP address consists of four bytes and has a rigid hierarchical structure.
8. An IP address looks like 121.7.106.83, where each period separates one of the bytes expressed in decimal notation from 0 to 127.
9. An IP address is hierarchical because as we scan the address from left to right, we obtain more and more specific information about where the host is located in the Internet. (Like a postal address)
10. An IP address is included in the header of each IP datagram.
11. Internet routers use this IP address to route datagram towards its destination.

12. Commonly used suffixes to specify domain names:
    a. com - commercial organization. E.g.: ToppersSolutions.com.
    b. edu – educational organization.
    c. org – non-profit organization.
    d. net – network support group.
    e. gov – government institution.
    f. mil – military group.
    g. int – international organization.

DNS PROTOCOL FUNCTIONING:

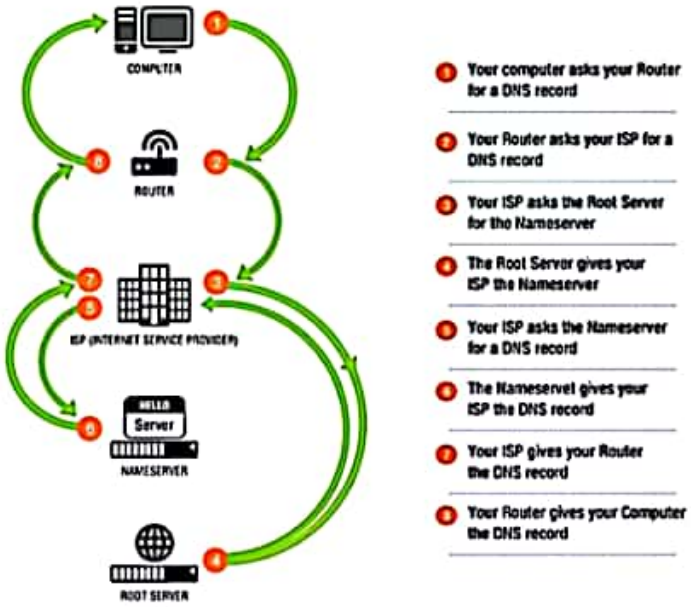


Figure 6.1: DNS Protocol Functioning.

1. Figure 6.1 shows DNS Protocol Functioning.
2. User type a domain name such as '**www.ToppersSolutions.com**' into the browser ("client").
3. The client needs to find the IP address where '**www. ToppersSolutions.com**' content is located.
4. Browser will send this query to the operating system of the computer.
5. Each operating system is configured to query certain DNS servers (Resolving Name Server).
6. The resolving name server is not aware of the location of '**ToppersSolutions.com**', but it does know where the root servers are located.
7. Next, the resolving name server finds the location of the top-level domain name server (In this case COM severs) and sends a query for '**ToppersSolutions.com**'.

8. Each domain on the Internet has an Authoritative name server.
9. Finally, the authoritative name server will give you the exact IP address of **'ToppersSolutions.com'**.
10. This information will come back to the resolving name server, which caches the information and sends backs the information to your browser.
11. And at the end, you would find yourself on **Topper's Solutions** homepage.
12. All these complex task take place in seconds.

Q2] Write Short Notes on: HTTP.

Ans: **[5M – Dec14]**

HTTP:

1. HTTP Stands for **Hyper Text Transfer Protocol**.
2. It is used to access data on World Wide Web.
3. This protocol transfers data in the form of plain text, hypertext, audio, video, and so on.
4. However, it is called the hypertext transfer protocol because its efficiency allows its use in a hypertext environment, where there are rapid jumps from one document to another.
5. HTTP functions like a combination of FTP and SMTP.

FEATURES OF HTTP:

I) HTTP is Connectionless:

- After a request is made, the client disconnects from the server and waits for a response.
- The server must re-establish the connection after it processes the request.

II) HTTP is Media Independent:

- Any type of data can be sent by HTTP as long as both the client and server know how to handle the data content.

III) HTTP is Stateless:

- This is a direct result of HTTP being connectionless.
- The server and client are aware of each other only during a request.
- Afterwards, each forgets the other.
- For this reason neither the client now the browser can retain information between different requests across the web pages.

HTTP WORKING:

1. The idea of HTTP is very simple.
2. A client sends a request, which looks like mail, to the server.
3. The server sends the response, which looks like a mail reply, to the client.
4. The request and response messages carry data in the form of a letter with MIME-like format.

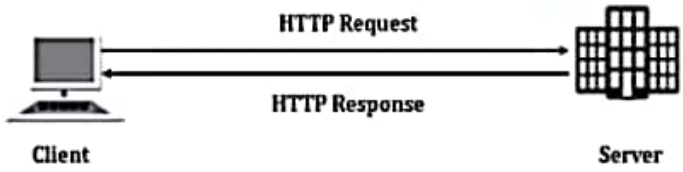


Figure 6.2: HTTP Request & Response.

HTTP MESSAGES:

1. There are two general types of HTTP messages: Request and Response.
2. Both message types follow almost the same format.
   a. **Request Messages:** A request message consists of a request line, headers and sometimes a body.
   b. **Response Messages:** A response message consists of a status line, headers and sometimes, a body.

HTTP COMMANDS:

- **GET:** Request by a client to obtain a web page from the server.
- **PUT:** Request by a client to store a web page on the server.
- **POST:** Request by a client to update contents of a web page on the server.
- **DELETE:** Request by a client to remove a web page from the server.

Q3] What is the use of SSH?

Ans: **[4M – Dec14 & 5M – Dec16]**

SSH:

1. SSH Stands for **Secure Shell.**
2. SSH is a **cryptographic network protocol.**
3. It provides a secure channel over an unsecured network in a client-server architecture, connecting an SSH client application with an SSH server.
4. Common applications include remote command-line login and remote command execution,.
5. Any network service can be secured with SSH.

Figure 6.3: SSH Connection.

USES OF SSH:

1. SSH is used for login to a shell on a remote host (replacing Telnet and rlogin).
2. It is used for executing a single command on a remote host.
3. For setting up automatic (password less) login to a remote server (for example, using OpenSSH).
4. It is also used for secure file transfer.
5. For using as a full-fledged encrypted VPN.
6. For browsing the web through an encrypted proxy connection with SSH clients that support the SOCKS protocol.
7. For securely mounting a directory on a remote server as a file system on a local computer using SSHFS.
8. For development on a mobile or embedded device that supports SSH.

Q4] SMTP

Ans: **[5M – Dec16]**

SMTP:

1. SMTP stands for **Simple Mail Transfer Protocol**.
2. It is a TCP/IP protocol that specifies how computers exchange electronic mail.
3. It works with post office protocol (POP).
4. SMTP is used to upload mail directly from the client to an intermediate host, but only computers constantly connected such as Internet Service Providers (ISP) to the Internet can use SMTP to receive mail.
5. The ISP servers then offload the mail to the users to whom they provide the Internet service.
6. SMTP uses TCP port number 25 for his service.
7. Therefore e-mail is delivered from source to destination by having the source machine established a TCP connection to port 25 of the destination machine.
8. To send a mail, a system must have a client MTA, and to receive a mail, a system must have a server MTA.
9. SMTP transfers this message from client MTA to server MTA.

---

10. SMTP uses commands and responses to transfer the message between an MTA client and MTA server.
11. In order to send a mail, SMTP is used two times: one between the sender and the sender's mail server, and the other between the two mail servers.
12. Each command or response ends with two characters (CR and LF) CR stands for Carriage Return and LF stands for Line Feed.
13. Figure 6.4 shows the example of SMTP.

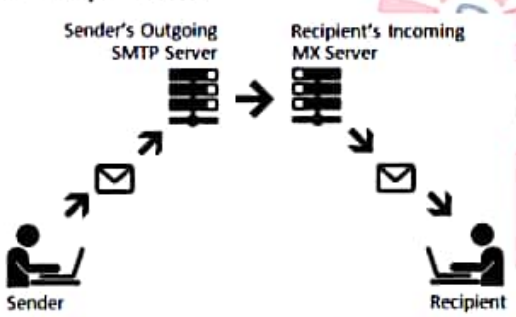


Figure 6.4: Example of SMTP.

— EXTRA QUESTIONS —

Q1] Explain TELNET.

Ans:

TELNET:

1. TELNET stands for **Telecommunication Network.**
2. It is a network protocol used on the Internet or local area network (LAN) connections.
3. It was developed in 1969 beginning with RFC 15 and standardized as IETF STD 8, one of the first Internet standards.
4. It provides bidirectional interactive communications facility.
5. TELNET is used to control information.

Figure 6.5: TELNET Service.

ESTABLISHING TELNET CONNECTION:

1. TELNET Client contacts the host using its internet address.
2. When TELNET Client contact the host, the distant computer and TELNET Client's computer negotiate how they will communicate with each other.
3. They decide which terminal emulation will be used.
4. Telnet emulation determines how TELNET Client's keyboard will transmit information to the distant computer and how information will be displayed on your screen.
5. For example, it determines how a back space key <- will work.
6. When a complete line of data is ready for transmission, the data is sent across the Internet from Network Virtual Terminal (NVT) keyboard.
7. Along with the data is the host's IP address, which makes sure that the packet is sent to the proper location.
8. TELNET Client's IP address is also sent so that information can be routed back to client.
9. After Telnet host receives data, it then processes the data and returns to client and give the results of using the data.

USES OF TELNET:

1. Enterprise networks to access host applications, e.g. on IBM Mainframes.
2. It is used in Administration of network elements.
3. MUD games played over the Internet.
4. Embedded systems.

Q2] Explain Email?

Ans:

E-MAIL:

1. E-mail stands for **Electronic Mail.**
2. It is a mail you can send or receive directly on your computer.
3. Electronic mail is among the most widely available application services.
4. Each user, who intends to participate in email communication, is assigned a mailbox, where out-going and incoming messages are buffered, allowing the transfer to take place in the background.

FEATURES:

- **Composition:** It is process of creating messages and answers.
- **Transfer:** It refers to moving messages from the originator to the recipient.
- **Reporting:** It is the process of telling the originator what happened to the message.
- **Displaying:** It is used to display incoming messages. So people can read their e-mail.

- **Disposition:** It is the final step and concerns what the recipient does with the message after receiving it.

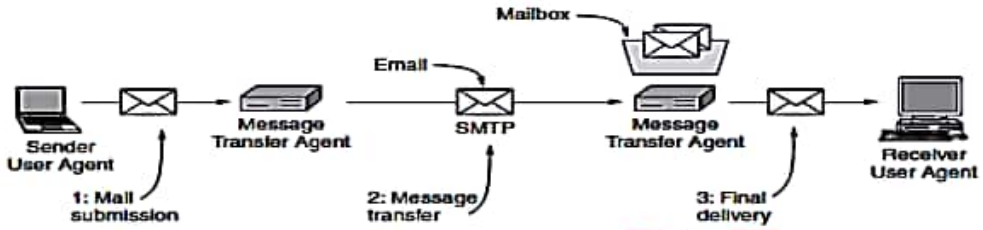


Figure 6.6: Email Architecture.

EMAIL COMPONENTS:

I) User Agents:

- Mail reader.
- Composing, editing, reading mail messages.

II) Mail Servers:

- Mailbox contains incoming messages for user.
- Message queue of outgoing (to be sent) mail messages.

III) Simple Mail Transfer Protocol (SMTP):

- To send email messages between mail servers.

EMAIL MESSAGE FORMAT:

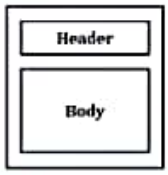


Figure 6.7: Email Message Format.

Header:

- Header Line includes:
  - To:
  - From:
  - Subject:

Body:

- Body includes the Message.
- Only ASCII characters are allowed.

EXAMPLE:

From: ToppersSolutions@gmail.com

To: SagarNarkar123@icloud.com

Subject: Welcome To Topper's Solutions.

Message:

Hi Sagar,

Your Account with Topper's Solutions has been verified & activated successfully. We are pleased to have you here with us. Now you can start exploring Topper's Solutions.

With Regards,
Topper's Solutions Team.

CHAPTER - 7: NETWORK MANAGEMENT

Q1] Write Short Notes on: SNMP.

Ans: **[5M - Dec14, May16 & May17]**

SNMP:

1. SNMP Stands for **Simple Network Management Protocol**.
2. It is a framework for managing devices in an internet using the TCP/IP protocol suite.
3. It is an **Application Level Protocol**.
4. It provides a set of fundamental operations for monitoring and maintaining an internet.
5. SNMP uses the concept of manager and agent.
6. That is, a manager, usually a host, controls and monitors a set of agents, usually routers.

SNMP ARCHITECTURE:

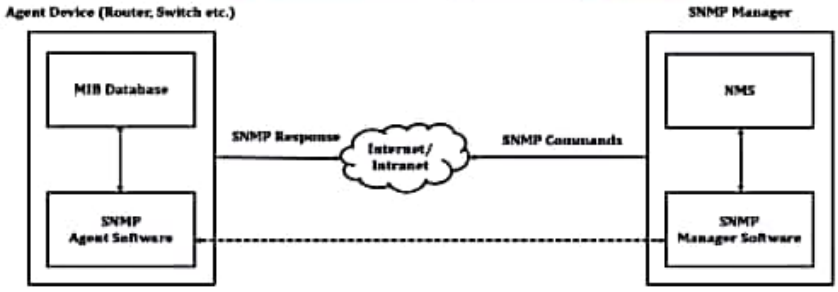


Figure 7.1: SNMP Architecture.

I) SNMP Manager:

- A manager or management system is a separate entity that is responsible to communicate with the SNMP agent implemented network devices.
- This is typically a computer that is used to run one or more network management systems.
- SNMP Manager's key functions:
  - Queries agents.
  - Gets responses from agents.
  - Sets variables in agents.
  - Acknowledges asynchronous events from agents.

II) Managed Devices:

- A managed device or the network element is a part of the network that requires some form of monitoring and management
- **Example:** Routers, Switches, Servers, Workstations, Printers, UPSs, etc.

III) **SNMP Agent:**

- The agent is a program that is packaged within the network element.
- It makes information available to the SNMP manager, when it is queried for.
- These agents could be standard (e.g. Net-SNMP) or specific to a vendor (e.g. HP insight agent)
- SNMP agent's key functions:
  - Collects management information about its local environment.
  - Stores and retrieves management information as defined in the MIB.
  - Signals an event to the manager.
  - Acts as a proxy for some non-SNMP manageable network node.

IV) **Management Information Base (MIB):**

- Every SNMP agent maintains an information database describing the managed device parameters.
- The SNMP manager uses this database to request the agent for specific information and further translates the information as needed for the Network Management System (NMS).
- This commonly shared database between the Agent and the Manager is called Management Information Base (MIB).
- MIB contains standard set of statistical and control values defined for hardware nodes on a network.
- MIB files are the set of questions that a SNMP Manager can ask the agent.
- Agent collects these data locally and stores it, as defined in the MIB.

Q2] Functions of Session Layer.

Q3] Explain any four functions of Session layer with example

Ans: **[Q2 | 5M – May15] & [Q3 | 10M – Dec16]**

SESSION LAYER:

1. Session layer is the fifth layer of OSI Model.
2. It has the responsibility of beginning, maintaining and ending the communication between two devices, called session.
3. Sessions are most commonly implemented on Web browsers using protocols.
4. Session Layer also provides for orderly communication between devices by regulating the flow of data.

FUNCTIONS OF SESSION LAYER:

I) Dialog Control:

- Session Layer allows two systems to start communication with each other in half-duplex or full-duplex.

II) Synchronization:

- Session layer allows a process to add checkpoints which are considered as synchronization points into stream of data.
- **Example:** If a system is sending a file of 800 pages, adding checkpoints after every 50 pages is recommended.
- This ensures that 50 page unit is successfully received and acknowledged.
- This is beneficial at the time of crash as if a crash happens at page number 110; there is no need to retransmit 1 to100 pages.

III) Logging:

- Session Layer controls logging on and off.

IV) Session Management:

- Session Layer is used to Establish, Maintaining & Ending a Session.
- It sends SYN Packet to establish request.
- It receives ACK & SYN.
- To End Session, Sender sends ACK.

V) Billing & User Identification:

- Session Layer is used for billing & user identification.
- Once the user is identified, the session is established.

Q4] MIB

Ans: **[5M – May17]**

MIB:

1. MIB Stands for **Management Information Base.**
2. MIB is a database used for managing the entities in a communication network.
3. Most often MIB is associated with the Simple Network Management Protocol (SNMP).

---

4. MIBs are nothing but the actual set of objects supported by a network device, for controlling and monitoring by the SNMP protocol.
5. These objects are classified and separately maintained in different MIB files.
6. There would be a separate MIB file maintained by the SNMP agent on the network device, for each protocol/entity that can be managed by SNMP
7. Example: System MIB, Chassis MIB, IP MIB, TCP MIB, UDP MIB, ICMP MIB, Interface MIB etc.).
8. MIBs are organized in a tree like structure and each MIB variable has a unique object ID.
9. Each MIB file define three things, namely:
    a. List of objects supported for a specific protocol/entity.
    b. Type of each object.
    c. Hierarchical relationship between all the objects of a given protocol/entity.