COMPUTER NETWORK

OLD QUESTION SOLUTION

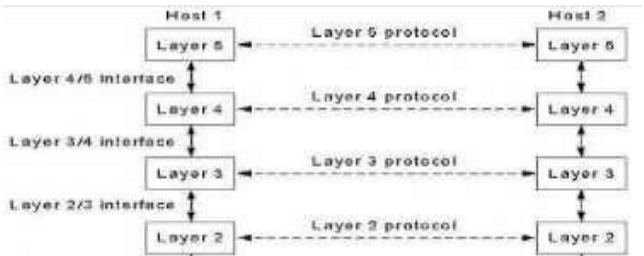
2069 CHAITRA

1. Explain the need of Networking Software in the form of Hierarchy. Mention in which level layer of OSI reference model following tasks are done. [6+2]

(i) Timing and voltage of received signal
(ii) Encryption and decryption of data
(ii) Data framing
(i) Point-to-point connection of socket.

Ans.: Networking software is a foundation element for any network which helps network administrators deploy, manage, and monitor a network. Networking software is invisible to end-users- it is simply used to facilitate the access those users have to network resources, in a seamless way. It allows multiple devices, such as desktops, laptops, mobile phones, tablets, and other systems to connect to one another, as well as other networks. The internet is a prime example of a globally connected system of servers and computers that relies on networking software to ensure accessibility by end users.

The first computer networks were designed with hardware as the main concern and the software as an afterthought. This strategy no longer works due to the advent of software revolution. To reduce the design complexity, most networks are organized as a series or hierarchy of layers or levels. The numbers of layers, the name of each layer, the contents of each layer and the function of each layer differ from network to network. Layer n on one machine communicates with the layer n on another machine on the network using some rules known as the layer n protocol. A protocol is an agreement between the communicating parties on how the communication is to proceed. The entities comprising the corresponding layers on two communicating machines over the network are called peers. In reality, no data is transferred from layer n on any two machines. Instead, each data and control information is passed to the layer below. Additional information including protocol control information may be appended by each layer to data as it travels from higher to lower layers in the form of layer headers. Below layer 1 is the physical medium through which actual communication occurs over communication channels. Network Software is needed to ease the transaction of data through the different hierarchy of protocols between these different layers efficiently.



The level layer in which the given tasks are performed are mentioned below:

1. Timing and voltage of received signal: Physical Layer
2. Encryption and Decryption of data: Presentation Layer
3. Data framing: Data Link Layer
4. Point-to-point connection of socket: Transport Layer

2. Define switching and multiplexing. Differentiate between circuit switching and packet switching. [4+4]

Ans.: Switching is the process that implies that we can dynamically configure a network which is less than fully connected in order to join any two nodes for communication. It is the most valuable asset of computer networking. Every time in computer network, a user access the internet or another computer network outside the user's immediate location, the message requests are sent through a maze of transmission media and connection devices. Simply, switching is the mechanism for exchange of information between different computer networks and network segments. There are basically three types of switching methods available:

2. Circuit Switching

   Circuit Switching maintains the idea of dedicated connections between two endpoints, but allows for sharing of channels within the network, and hence is much more scalable. Circuit switching takes advantage of the fact that while everybody needs t be able to talk to everybody else, the aren't likely to all do so at the same time. The telephone network is based on circuit switching.

3. Message Switching

   Message switching does not set up a dedicated channel (or circuit) between the sender and recipient during the communication session. In message switching each message is treated as an independent block. In this type of networking, each message is then transmitted from first network device to second network device through the internetwork i.e. message is transmitted from the sender to intermediator device.

4. Package Switching

   Package switching alleviates the problems of circuit and message switching. A small upper bound is put on the maximum size of a packet sent through the network. No reserved channel is created ahead of time, each packet belonging to a single message may take a different route through the network. Since there is no reservation of capacity it is possible that congestion becomes a problem. Too many packets trying to get through the same router requires that the router be able to buffer packets. All buffers have finite size, so it is possible that packets are dropped.

Multiplexing is the method by which multiple analog or digital signals are combined into one signal over a shared medium. The aim is to share a scarce resource. In telecommunication, several telephone calls may be carried using one wire. Long distance links use high capacity point-to-point connections with a single physical medium. Some means must be found for the sharing the capacity to enable multiple simultaneous uses

of the medium. The motivation is the same here as for time shared operating systems. There are three wars to divide a channel:

3. Frequency Division Multiplexing

   Frequency Division Multiplexing (FDM) is possible when a single source requires less than the total available bandwidth in the medium. Frequency modulation lets data be moved to any particular part of the frequency spectrum of the channel. Multiple sources can thus share the same medium, by using different parts of the channel simultaneously. FDM allows for full duplex modems, radio, and TV.

4. Time Division Multiplexing

   If the data rate of a medium is larger than the data rate (bps) of a source channel, then multiple channels can be sent by allotting different channels different slices of time. The multiple channels can be interleaved by bit, byte or frame. There are two types of TDM: Synchronous TDM and Asynchronous TDM. The issues of link control are handles per channel, independent of the TDM.

5. Code Division Multiplexing

   Code Division Multiplexing (CDM) is a class of techniques here several channels simultaneously share the same frequency spectrum, and this spectral bandwidth is much higher than the bit rate or symbol rate. One form is frequency hopping, another is direct sequence spread spectrum. In the latter case, each channel transmits its bits as a coded channel-specific sequence of pulses called chips. Number of chips per bit, or chips per symbol is the spreading factor. This coded transmission typically is accomplished by transmitting a unique time-dependent series of short pulses, which are placed within chip times within the larger bit time. All channels, each with a different code, can be transmitted on the same fiber or radio channel or other medium, and asynchronously demultiplexed.

The differences between Circuit switching and packet switching are given below:

Circuit Switching	Packet Switching
It is connection oriented.	It is connectionless oriented.
It was initially designed for voice communication.	It was initially designed for data transmission.
It is inflexible because once a path is set all parts of a transmission follows the same path.	It is flexible because a route is created for each packet to travel to the destination.
The message is received in the order it was sent from the source.	The packets of a message is received out of order and must be assembled at the destination.
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.

Circuit switching is implemented at physical layer.	Packet switching is implemented at Network Layer.

3. Explain the different types of Data link layer framing mechanisms. [8]

Ans.: Frames are the units of digital transmission particularly in computer networks and telecommunications. Frames are comparable to packets of energy called photons in case of light energy. Frame is continuously used in Time Division Multiplexing process.

Framing is a point-to-point connection between two computers or devices consisting of a wire in which data is transmitted as a stream of bits. However, these bits must be framed into discernible blocks of information. Framing is a function of the data link layer. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver. Ethernet, token ring, frame relay, and other data link layer technologies have their own frame structures. Frames have headers that contain information such as error-checking codes.

A frame has the following parts:

- Frame Header: It contains the source and destination addresses of the frame.
- Payload Field: It contains the message to be delivered.
- Trailer: It contains the error detection and error correction bits.
- Flag: It marks the beginning and end of the frame.

There are two types of framing techniques:

1. Fixed Size:

   The frame is of fixed size and there is no need to provide boundaries to the frame, length of the frame itself acts as delimiter. Frames can be of fixed or variable size. In fixed-size framing, there is no need for defining the boundaries of the frames; the size itself can be used as a delimiter. An example of this type of framing is the ATM wide-area network, which uses frames of fixed size called cells.
2. Variable Size:

   In this there is need to define end of frame as well as beginning of next frame to distinguish. In variable-size framing, we need a way to define the end of the frame and the beginning of the next. Historically, two approaches were used for this purpose: a character-oriented approach and a bit-oriented approach. The defining of end and beginning of the frame can be done in two ways:

   1. Length Field: We can introduce a length field in the frame to indicate the length of the frame. it is used in Ethernet. The problem with this is that sometimes the length field might get corrupted.
   2. End Delimiter (ED): We can introduce an ED (pattern) to indicate the end of the frame. it is used in Token Ring. The problem with this is that ED can

occur in the data. This can be solved by : Character/Byte Stuffing and Bit Stuffing.

What is the contribution of sub-netting in IP address management? Show the importance in this case. Banijya bank needs to allocate 15 IPs in HR department, 30 in finance department, 24 in customer care unit and 25 in ATM machines. If you have one network of class C range public IP address, describe how you will manage it. [8]

Ans.: Subnetting is a process of breaking large network in small networks known as subnets. Subnetting happens when we extend default boundary of subnet mask. Basically, we borrow host bits to create networks. The contributions of subnetting in IP address management are given below:

- Subnetting breaks large network in smaller networks and smaller networks which are easier to manage.
- It reduces network traffic by removing collision and broadcast traffic, that overall improves performance.
- Subnetting allows us to apply network security policies at the interconnection between subnets.
- Subnetting allows us to save money by reducing requirement for IP range.

By using subnetting, one single Class A IP address can be used to have smaller sub-networks which provides better network management capabilities.

Solution,

Here,

HR department needs 15 IPs, Finance department needs 30 IPs, Customer Care needs 24 IPs and ATM needs 25 IPs.

Let class C IP address that is allocated to the bank starts from 192.168.0.0

Thus, for HR department:

Total required IP addresses = 15 + 2 = 17 IP addresses

$17 \leq 32 = 2^5$ => hid = 5 and nid = 32-hid => nid=27

Thus:

First Address = 192.168.0.0/27

…… } Usable Range
……

192.168.0.16/27

……

Last Address = 192.168.0.31/27

Subnet Mask = 255.255.255.128

Again, for Finance department:

Total required IP addresses = 30 + 2 = 32 IP addresses

$32 \leq 32 = 2^5$ => hid = 5 and nid = 32-hid => nid=27

Thus:

First Address = 192.168.0.32/27

…… Usable Range
……

Last Address = 192.168.0.63/27

Subnet Mask = 255.255.255.128

Now, for Customer Care:

Total required IP addresses = 24 + 2 = 26 IP addresses $26 \leq 32 = 2^5$ => hid = 5 and nid = 32-hid => nid=27

Thus:

First Address = 192.168.0.64/27

…… Usable Range
……

192.168.0.89/27

……

Last Address = 192.168.0.95/27

Subnet Mask = 255.255.255.128

Finally, for ATMs:

Total required IP addresses = 25 + 2 = 27 IP addresses $27 \leq 32 = 2^5$ => hid = 5 and nid = 32-hid => nid=27 Thus:

First Address = 192.168.0.96/27

…… Usable Range
……

192.168.0.122/27

……

Last Address = 192.168.0.127/27

Subnet Mask = 255.255.255.128

This way, by using subnetting we can divide the allotted IP addresses among the various departments of the Banijya Bank.

5. Why is routing protocol necessary? Explain the working process of routing information protocol (RIP) with example. [3+5]

Ans.: The routing protocol specifies how routers communicate with each other, distributing information that enables them to select routes between any two nodes on a computer network. Routers perform the "traffic directing" function on the Internet; data packets are forwarded through the networks of the internet from router to router until they reach their destination computer. Routing algorithms determine the specific choice of route each router has a prior knowledge only of networks attached to it directly. A routing protocol shares this information first among immediate neighbors, and then throughout the network. This way, routers gain knowledge of the topology of the network. Many routing protocols are defined in documents called RFCs (Request for Comments). The ability of routing protocols to dynamically adjust to changing conditions such as disabled data lines and computers and route data around obstructions is what gives the Internet its survivality and reliability.

The three major classes of widespread routing protocols are:

- Link-state routing protocols
- Distance-vector routing protocols
- Exterior gateway protocols

The Routing Information Protocol (RIP) is one of the oldest distance-vector routing protocols which employs the hop count as a routing metric. RIP prevents routing loops by implementing a limit on the number of hops allowed in a path from source to destination. The largest number of hops allowed for RIP is 15, which limits the size of networks that RIP can support. RIP implements the split horizon, route poisoning and holddown mechanisms to prevent incorrect routing information. There are three standardized versions of the Routing Information Protocol: RIPv1 and RIPv2 for IPv4 and RIPng for IPv6.

The working of RIP is explained below:

Each RIP router maintains a routing table, which is a list of all the destinations (networks) it knows how to reach, along with the distance to that destination. RIP uses a distance vector algorithm to decide which path to put a packet on to get to its destination. It stores in its routing table the distance for each network it knows how to reach, along with the address of the "next hop" router -- another router that is on one of the same networks -- through which a packet has to travel to get to that destination. If it receives an update on a route, and the new path is shorter, it will update its table entry with the length and next-hop address of the shorter path; if the new path is longer, it will wait through a "hold-down" period to see if later updates reflect the higher value as well, and only update the table entry if the new, longer path is stable. Using RIP, each router sends its entire routing table to its closest neighbors every 30 seconds. (The neighbors are the other routers to which this router is connected directly -- that is, the

other routers on the same network segments this router is on.) The neighbors in turn will pass the information on to their nearest neighbors, and so on, until all RIP hosts within the network have the same knowledge of routing paths, a state known as convergence.

Q no 6. Why do you think there exist two protocols in transport layer whereas there exists only one protocol in Internet layer in TCP/IP reference model? Explain token bucket algorithm for congestion control.

Answer:

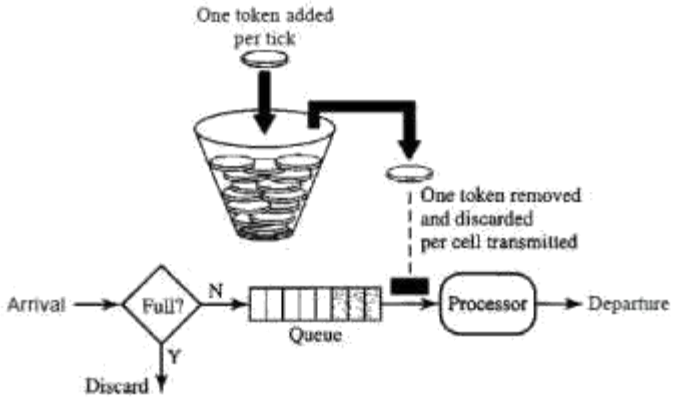
The functionality of the TCP/IP model is divided into four layers, and each includes specific protocols. It is a layered server architecture system in which each layer is defined according to a specific function to perform. All these four layers work collaboratively to transmit the data from one layer to another and the layers are: Application Layer, Transport Layer, Internet Layer and Network Interface.

Transport layer builds on the network layer in order to provide data transport from a process on a source system machine to a process on a destination system. It is hosted using single or multiple networks and maintains the quality of service functions. It determines how much data should be sent where and at what rate. This layer builds on the message which are received from the application layer. It helps ensure that data units are delivered error-free and in sequence. It helps to control the reliability of a link through flow control, error control, and segmentation or de-segmentation.

The transport layer also offers an acknowledgment of the successful data transmission and sends the next data in case no errors occurred. The two main Transport layer protocols are: Transmission Control Protocol (TCP/IP) which provides reliable communication between two hosts and User Datagram Protocol (UDP) which provides unreliable communication between two hosts

Meanwhile an internet layer is the second layer of the TCP/IP model which is also known as a network layer. The main work of this layer is to send the packets from any network, and any computer still they reach the destination irrespective of the route they take. This layer offers the functional and procedural method for transferring variable length data sequences from one node to another with the help of various networks. Message delivery at the network layer does not give any guaranteed to be reliable network layer protocol. So, only one protocol exists in this layer.

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



The token bucket algorithm allows idle hosts to accumulate credit for the future in the form of tokens i.e. for each tick of the clock, the system sends n tokens to the bucket and the system removes one token for every cell (or byte) of data sent. In other words, the host can send bursty data as long as the bucket is not empty. The token bucket can easily be implemented with a counter. The token is initialized to zero where each time a token is added, the counter is incremented by 1. Again, each time a unit of data is sent, the counter is decremented by 1 and when the counter is zero, the host cannot send data.

Q no. 7 What is HTTP protocol? With an example explain how a request initiated by a http client is served by a HTTP server.

Answer:

The Hypertext Transfer Protocol (HTTP) is an application protocol for distributed, collaborative, hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web. Hypertext is structured text that uses logical links (hyperlinks) between nodes containing text. It is a request-response protocol in the client-server computing model. When you enter http:// in front of the address tells the browser to connect over HTTP. For example, when you enter a URL in your web browser, this sends an HTTP command to the Web server to fetch and transfer the requested web page. Here, your web browser is your client and your website host as a server.

Upon interaction with a website, such as trying to retrieve a webpage, data is sent back and forth between you and the web server. The S in HTTPS signals the inclusion of the "Secure Sockets Layer" - more colloquially known as "SSL" - whose function is to encrypt the data that is exchanged between the client and the website so when the client tries to connect to the website,

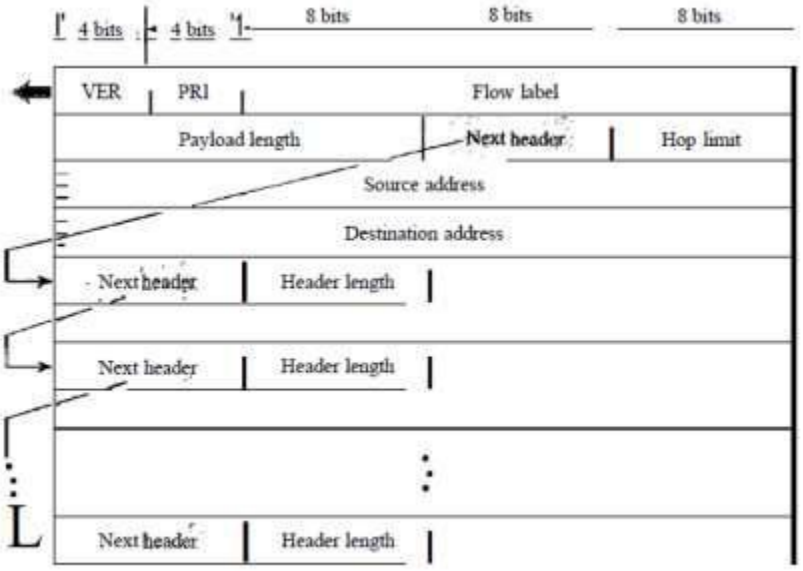
the computer will receive their SSL Certificate and checks it against the server's credentials. The computer and the web server then figure out the best way to encrypt information, exchange special "keys" with one another, and then give it a small test drive to ensure they can properly share encrypted information. Once the two are ready to go, they each give the green light and exchange encrypted information. Because both the Client's computer and the website's server must verify their identities, set up their special way of encoding/decoding that is unique to them, and always transfers information in a secure manner. Also, the method of decryption is unique to each connection.

QNo.8 Explain the IPv6 datagram format and the function of each field with necessary figure.

Answer:

Internet Protocol version 6 (IPv6) is the most recent version of the Internet Protocol (IP), the communications protocol that provides an identification and location system for computers on networks and routes traffic across the Internet. IPv6 was developed by the Internet Engineering Task Force (IETF) to deal with the long-anticipated problem of IPv4 address exhaustion.

Each packet in IPv6 is composed of a mandatory base header followed by the payload which consists of two parts: optional extension headers and data from an upper layer. The base header occupies 40 bytes, whereas the extension headers and data from the upper layer contain up to 65,535 bytes of information.



The base header has eight fields which are as follows:

- Version. This 4-bit field defines the version number of the IP. For IPv6, the value is 6.
- Priority. The 4-bit priority field defines the priority of the packet with respect to traffic congestion.
- Flow label. The flow label is a 3-byte (24-bit) field that is designed to provide special handling for a flow of data.
- Payload length. The 2-byte payload length field defines the length of the IP datagram excluding the base header.
- Next header. The next header is an 8-bit field defining the header that follows the base header in the datagram and is either one of the optional extension headers used by IP or the header of an encapsulated packet such as UDP or TCP. Each extension header also contains this field.
- Hop limit. This 8-bit hop limit field serves the same purpose as the TIL field in IPv4.
- Source address. The source address field is a 16-byte (128-bit) Internet address that identifies the original source of the datagram.
- Destination address. The destination address field is a 16-byte (128-bit) Internet address that usually identifies the final destination of the datagram, But, if source routing is used, this field contains the address of the next router.

Priority

The priority field of the IPv6 packet defines the priority of each packet with respect to other packets from the same source. For example, if one of two consecutive Datagrams must be discarded due to congestion, the datagram with the lower packet priority will be discarded. IPv6 divides traffic into two broad categories: congestion-controlled and noncongestion-controlled.

Flow Label

A sequence of packets sent from a particular source to a particular destination that needs special handling by routers is called a flow of packets. The combination of the source address and the value of the flow label uniquely define a flow of packets. To a router, a flow is a sequence of packets that share the same characteristics, such as traveling the same path, using the same resources, having the same kind of security, and so on and a router that supports the handling of flow labels has a flow label table. In its simplest form, a flow label can be used to speed up the processing of a packet by a router. When a router receives a packet, instead of consulting the routing table and going through a routing algorithm to define the address of the next hop, it can easily look in a flow label table for the next hop.

Qno.9 Compare Symmetric key encryption method with asymmetric key encryption. Describe the operation of RSA algorithm.

Answer:

The comparison of the two encryption methods are:

Symmetric key encryption	Asymmetric key encryption
1. Symmetric encryption uses a single key for both encryption and Decryption. 2. Symmetric encryption is fast in execution. 3. The algorithms include: DES, 3DES, AES, and RC4. 4. The symmetric encryption is used for bulk data transmission.	1. Asymmetric encryption uses a different key for encryption and decryption. 2. Asymmetric Encryption is slow in execution due to the high computational burden. 3. The algorithms include: Diffie-Hellman, RSA. 4. The asymmetric encryption is often used for securely exchanging secret keys.

RSA is named for its inventors Rivest, Shamir, and Adleman (RSA) and it uses two numbers, e and d, as the public and private keys.

The operation of RSA is described below:

Selecting Keys:

We use the following steps to select the private and public keys:

- We choose two very large prime numbers p and q since a prime number is one that can be divided evenly only by 1 and itself.
- We multiply the above two primes to find n, the modulus for encryption and decryption. In other words, n: p X q.
- We calculate another number: (p -1) X (q - 1).
- We choose a random integer e and then calculates d so that d x e: 1 mod
- We announce e and n to the public but keep s and d a secret.

Example:

Bob chooses 7 and 11 as p and q and calculates $n = 7 \cdot 11 = 77$. The value of $\phi = (7 - 1)(11 - 1)$ or 60. Now he chooses two keys, e and d. If he chooses e to be 13, then d is 37. Now imagine Alice sends the plaintext 5 to Bob. She uses the public key 13 to encrypt 5.

Plaintext: 5
$C = 5^{13} = 26 \bmod 77$
Ciphertext: 26

Bob receives the ciphertext 26 and uses the private key 37 to decipher the ciphertext:

Ciphertext: 26
$P = 26^{37} = 5 \bmod 77$
Plaintext: 5 Intended **message sent by Alice**

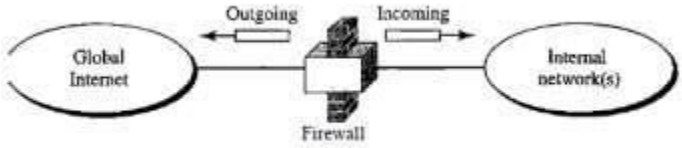
The plaintext 5 sent by Alice is received as plaintext 5 by Bob.

Qno.10 What is network security? How can firewalls enhance network security? Explain how firewalls can protect a system.

Answer:

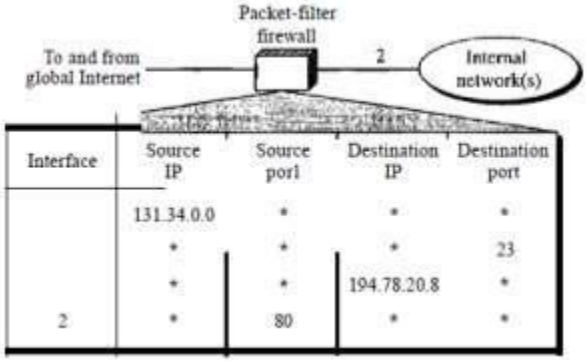
Network security is the practice of preventing and protecting against unauthorized intrusion into corporate networks. As a philosophy, it complements endpoint security, which focuses on individual devices; network security instead focuses on how those devices interact, and on the connective tissue between them.

A firewall is a device (usually a router or a computer) installed between the internal network of an organization and the rest of the Internet. It is designed to forward some packets and filter (not forward) others.



A firewall may filter all incoming packets destined for a specific host or a specific server such as HTTP and can be used to deny access to a specific host or a specific service in the organization. A firewall is usually classified as a packet-filter firewall or a proxy-based firewall.

A firewall can be used as a packet filter and thus can forward or block packets based on the information in the network layer and transport layer headers: source and destination IP addresses, source and destination port addresses, and type of protocol (TCP or UDP). A packet-filter firewall is a router that uses a filtering table to decide which packets must be discarded (not forwarded). Figure shows an example of a filtering table for this kind of a firewall.



1.What do you mean by protocol and interfaces? Write the protocols used in each layer of TCP/IP model.

Network protocols are sets of established rules that dictate how to format, transmit and receive data so computer network devices from servers and routers to endpoints can communicate regardless of the differences in their underlying infrastructures, designs or standards.Standardized network protocols provide a common language for network devices. Without them, computers wouldn't know how to engage with each other.

And a network interface is a software or hardware interface between two pieces of equipment or protocol layers in a computer network.A network interface will usually have some form of network address. This may consist of a node identifier and a port number or may be a unique node ID in its own right.Network interfaces provide standardized functions such as passing messages, connecting and disconnecting, etc.

There are four layers in the TCP/IP model they are:

(a) Host to network layer:
Protocol is used to connect to the host,so that the packets can be sent over it.

(b) Internet layer:
Internet protocol is used in this layer which holds the whole architecture together. It helps the packet to travel independently to the destination.

(c) Transport layer:
Its decides if the data transmission should be on parallel or single path.Functions such as multiplexing, segmenting or splitting on the data is done.

(d) Application layer:
Its have different protocol such as TELNET for two -way communication, FTP for file transfer, SMTP for the transport of electronic mail, DNS for resolving the ip adress into the textual address for the Hosts connected over a network.

2.How do you define network topology?Discuss the types of network topologies based on its size and geographical distributions.

A network topology is the pattern in which nodes (i.e., computers, printers, routers or other devices) are connected to a local area network (LAN) or other network via links (e.g., twisted pair copper wire cable or optical fiber cable). It can also be used to define or describe the arrangement of various types of telecommunication networks, including command and control radio networks,industrial field busses and computer networks.

The different type of network topologies based on size and geographical distribution are as follows:

a) BUS Topology:
Bus topology is a network type in which every computer and network device is connected to single cable. When it has exactly two endpoints, then it is called Linear Bus topology.

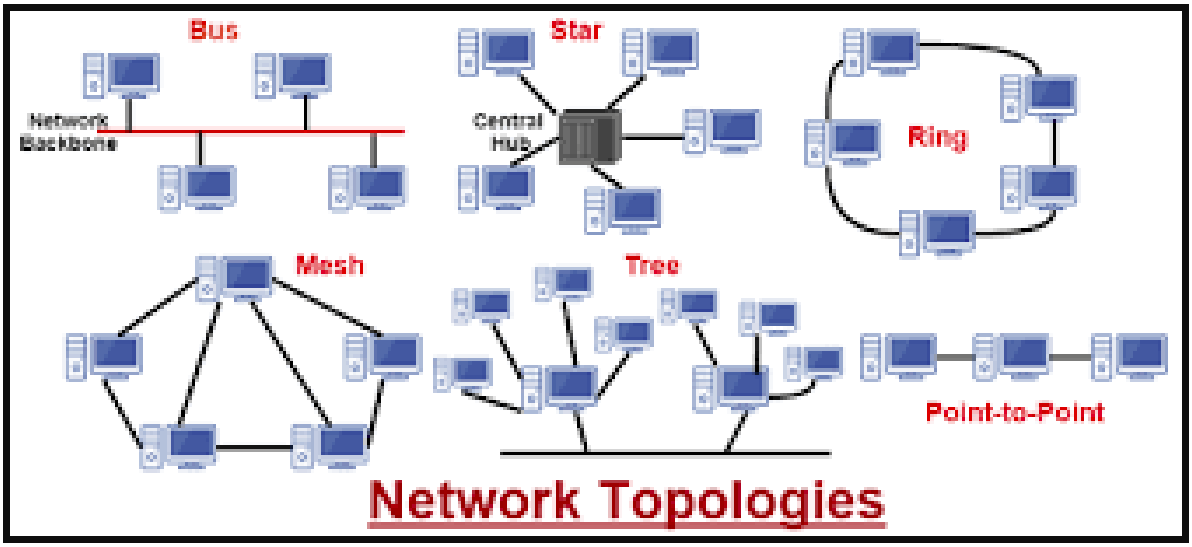
b) RING Topology:
It is called ring topology because it forms a ring as each computer is connected to another computer, with the last one connected to the first. Exactly two neighbours for each device.

c) STAR Topology:
In this type of topology all the computers are connected to a single hub through a cable. This hub is the central node and all others nodes are connected to the central node.

d) MESH Topology:
It is a point-to-point connection to other nodes or devices. All the network nodes are connected to each other. Mesh has n(n-1)/2 physical channels to link n devices.
There are two techniques to transmit data over the Mesh topology, they are :
   i. Routing
   ii. Flooding

e) TREE Topology:
It has a root node and all other nodes are connected to it forming a hierarchy. It is also called hierarchical topology. It should at least have three levels to the hierarchy.

f) HYBRID Topology:
It is two different types of topologies which is a mixture of two or more topologies. For example if in an office in one department ring topology is used and in another star topology is used, connecting these topologies will result in Hybrid Topology (ring topology and star topology).



3.What are the functions of LIC and MAC sub-layer?Discuss different framing approaches used in data link layer.

The function of LIC sub-layer are as follows:

i. To communicates with upper layers of the OSI model.
ii. To transition the packet to the lower layers for delivery.
iii. To gets the network protocol data, which is usually an IPv4 packet.
iv. To add the control information to help deliver the packet to the destination.

And functions of MAC sub-layer are as follows:

i. It provides an abstraction of the physical layer to the LLC and upper layers of the OSI network.
ii. It is responsible for encapsulating frames so that they are suitable for transmission via the physical medium.
iii. It resolves the addressing of source station as well as the destination station, or groups of destination stations.
iv. It performs multiple access resolutions when more than one data frame is to be transmitted. It determines the channel access methods for transmission.

The different type of framing approaches that are used in data link layer are as follows:

1. Character Count

It uses a field in the header to count the number of characters in the frame. On receiver end, the layer sees the character count and knows how many character forms a frame. Count can be changed due to transmission error that results in receiver to be out of synchronization.

2. Flag bytes with byte stuffing
It provides a special byte called FLAG at the beginning and the end of each frame. Two consecutive flag bytes indicate the end of one frame and start of next frame. If error is detected, it looks for flag byte to determine end of current frame. When binary data, object program or numbers are transmitted, the flag byte pattern may occur in the data. It can be resolved by adding special escape byte (ESC) by the sender before every accidental flag byte in the data.

3.Flag with bit stuffing
Each frame begins and ends with a special bit pattern called flag byte. Eg: 01111110.If sender's data link layer encounters five consecutive 1's in the data, it automatically stuffs a 0 bit into outgoing stream. If receiver sees 0 bit following five consecutive 1 bits, it automatically removes 0 bit. This process is called bit stuffing.

4.How data transfer occurs in Ethernet network. Explain?

Modern Ethernet is based on twisted pair wiring. Commonly either CAT5 or CAT6 cabling standards. Twisted pair is nice because it is pretty much immune to noise and allows us to run up to gigabit speeds without too much of a concern. Alternately and for higher speeds up to 100Gb/s, there's fiber (or multi-fiber cables).

Modern Ethernet is point-to-point, with hosts typically connected to switches in a star topology. Each link is used full-duplex, so that each end can transmit at rate without collisions. Switches may be interconnected in a mesh, with loops eliminated by Spanning Tree Protocol or something more clever.

Each host on an Ethernet has an address, known as a MAC Address. This is globally unique, based on manufacturing. Any two hosts on an Ethernet can talk directly to one another just by using the right MAC address. Switches implement multicast and broadcast by flooding the packets across the Ethernet in a loop free manner.

At the link layer, each packet on an Ethernet is prefaced by a preamble. This is a fixed electrical pattern that is used to help the receiver learn what the transmitter's clock looks like. This is followed by an Ethernet frame: a destination MAC address, a source MAC address, an Ethertype, and then the L3 packet body. This is then followed by a CRC-32 checksum of the frame for error detection.

The Ethertype is a 2 byte code that indicates what type of L3 packet is being carried.

5.Discuss how CSMA works?Differentiate it with CSMA-CD. Explain the optical fiber cabling standards with examples.

CSMA works on the principle that only one device can transmit signals on the network, otherwise a collision will occur resulting in the loss of data packets or frames. CSMA works when a device needs to initiate or transfer data over the network. Before transferring, each CSMA must check or listen to the network for any other transmissions that may be in progress. If it senses a transmission, the device will wait for it to end. Once the transmission is completed, the waiting device can transmit its data/signals. However, if multiple devices access it simultaneously and a collision occurs, they both have to wait for a specific time before reinitiating the transmission process.

In CSMA-CD first, the station monitors the transmission medium. As long as this is occupied, the monitoring will continue. Only when the medium is free and for a certain time (in interframe spacing), will the station send a data packet. Meanwhile, the transmitter continues to monitor the transmission medium to see if it detects any data collisions. If no other participant tries to send its data via the medium by the end of transmission, and no collision occurs, the transmission has been a success.

The different types of fiber optics standard for cabling are:

i. Single Mode fiber optics

   A single-mode optical fiber (SMF) is an optical fiber designed to carry only a single mode of light - the transverse mode. Modes are the possible solutions of the Helmholtz equation for waves, which is obtained by combining Maxwell's equations and the boundary conditions. These modes define the way the wave travels through space, i.e. how the wave is distributed in space. Waves can have the same mode but have different frequencies. This is the case in single-mode fibers, where we can have waves with different frequencies, but of the same mode, which means that they are distributed in space in the same way, and that gives us a single ray of light. Although the ray travels parallel to the length of the fiber, it is often called transverse mode since its electromagnetic oscillations occur perpendicular (transverse) to the length of the fiber. The 2009 Nobel Prize in Physics was awarded to Charles K. Kao for his theoretical work on the single-mode optical fiber. The standard G.652 defines the most widely used form of single-mode optical fiber.

ii. Multimode Fiber optics

   Multi-mode optical fiber is a type of optical fiber mostly used for communication over short distances, such as within a building or on a campus. Multi-mode links can be used for data rates up to 100 Gbit/s. Multi-mode fiber has a fairly large core diameter that enables multiple light modes to be propagated and limits the maximum length of a transmission link because of modal dispersion. The equipment used for communications over multi-mode optical fiber is less expensive than that for single-mode optical fiber. Typical transmission speed and distance limits are 100 Mbit/s for distances up to 2 km (100BASE-FX), 1 Gbit/s up to 1000 m, and 10 Gbit/s up to 550 m.

Because of its high capacity and reliability, multi-mode optical fiber generally is used for backbone applications in buildings. An increasing number of users are taking the benefits of fiber closer to the user by running fiber to the desktop or to the zone. Standards-compliant architectures such as Centralized Cabling and fiber to the telecom enclosure offer users the ability to leverage the distance capabilities of fiber by centralizing electronics in telecommunications rooms, rather than having active electronics on each floor.
Multi-mode fiber is used for transporting light signals to and from miniature fiber optic spectroscopy equipment (spectrometers, sources, and sampling accessories) and was instrumental in the development of the first portable spectrometer.
Multi-mode fiber is also used when high optical powers are to be carried through an optical fiber, such as in laser welding

6.What is virtual circuit switching?Describe the operation of frame-relay network.

Virtual circuit switching is a packet switching methodology whereby a path is established between the source and the final destination through which all the packets will be routed during a call. This path is called a virtual circuit because to the user, the connection appears to be a dedicated physical circuit.

Frame Relay is a standardized wide area network technology that specifies the physical and data link layers of digital telecommunications channels using a packet switching methodology. Originally designed for transport across Integrated Services Digital Network (ISDN) infrastructure, it may be used today in the context of many other network interfaces.

It was developed to solve communication problems that other protocols could not the increased need for higher speeds, an increased need for large bandwidth efficiency, particularly for clumping ("bursty" traffic), an increase in intelligent network devices that lower protocol processing, and the need to connect LANs and WANs.Frame Relay is a packet-switched protocol. But the Frame-Relay process is streamlined. There are significant differences that make Frame Relay a faster, more efficient form of networking. A Frame-Relay network doesn't perform error detection, which results in a considerably smaller amount of overhead and faster processing than X.25. Frame Relay is also protocol independent-it accepts data from many different protocols. This data is encapsulated by the Frame-Relay equipment, not the network.

Frame Relay sends information in packets called frames through a shared Frame-Relay network. Each frame contains all the information necessary to route it to the correct destination. So in effect, each endpoint can communicate with many destinations over one access link to the network. And instead of being allocated a fixed amount of bandwidth, Frame-Relay services offer a CIR (committed information rate) at which data is transmitted. But if traffic and your service agreement allow, data can burst above your committed rate.

7. **Differentiate between adaptive and non-adaptive routing. Explain shortest path finding algorithm in link state routing.**

Ans.: The differences between adaptive and non-adaptive routing are given below:

Adaptive	Non-Adaptive

Adaptive routing algorithms are the algorithms that base its decisions on data which reflects the current traffic conditions.	Non adaptive routing algorithms are the algorithms that consult static tables to determine which nodes to send the packet.
Dynamic routing uses adaptive routing algorithms.	Static routing uses non-adaptive routing algorithms.
In adaptive routing algorithms, the basis of routing decisions are the network traffic topology.	In non-adaptive routing algorithms, the basis of routing decisions are static tables.
Centralized, isolated and distributed are the types of adaptive routing algorithms.	Flooding and random walks are the types of non-adaptive algorithms.
Adaptive routing algorithms are more complex.	Non-adaptive routing algorithms are more simple.

Shortest path can be calculated only for the weighted graphs. The edges connecting two vertices can be assigned a nonnegative real number, called the weight of the edge. It is also called Dijkstra's algorithm. It is an algorithm for finding the shortest paths between nodes in a graph, which may represent, for example, road networks. It was conceived by computer scientist Edsger W. Dijkstra in 1956 and published three years later. The algorithm exists in many variants. Dijkstra's original algorithm found the shortest path between two given nodes,[4] but a more common variant fixes a single node as the "source" node and finds shortest paths from the source to all other nodes in the graph, producing a shortest-path tree.

The algorithm is:

1. Initialize the array smallestWeight so that smallestWeight[u] = weights [vertex, u].
2. Set smallestWeight [vertex] = 0.
3. Find the vertex, v that is closest to vertex for which the shortest path has not been determined.
4. Mark v as the (next) vertex for which the smallest weight is found.
5. For each vertex w in G, such that the shortest path from vertex to w has not been determined and an edge (v, w) exists, if the weight of the path to w via v is smaller than its current weight, update the weight of w to the weight of v + the weight of the edge (v, w).

Because there are n vertices, repeat Steps 3 through 5, n – 1 times.

8. Compare between leaky bucket and token bucket algorithm with the operation how token bucket works.

Ans.: The differences between leaky bucket and token bucket are given below:

Leaky Bucket	Token Bucket
Its parameter is rate.	Its parameters are rate and burstiness.
It smooths out traffic by passing packets only when there is a token and doesn't permit burstiness.	Token bucket smooths traffic but permits burstiness which is equivalent to the number of tokens accumulated in the bucket.

It discards packets for which no tokens are available. (No concept of queue)	It discards tokens when bucket is full but never discards packets.
Applications: traffic shaping or traffic policing.	Application: network traffic shaping or rate limiting.

The description of how token bucket works is given below:

The token bucket algorithm is based on an analogy of a fixed capacity bucket into which tokens, normally representing a unit of bytes or a single packet of predetermined size, are added at a fixed rate. When a packet is to be checked for conformance to the defined limits, the bucket is inspected to see if it contains sufficient tokens at that time. If so, the appropriate number of tokens, e.g. equivalent to the length of the packet in bytes, are removed ("cashed in"), and the packet is passed, e.g., for transmission. The packet does not conform if there are insufficient tokens in the bucket, and the contents of the bucket are not changed. Non-conformant packets can be treated in various ways:

- They may be dropped.
- They may be enqueued for subsequent transmission when sufficient tokens have accumulated in the bucket.
- They may be transmitted, but marked as being non-conformant, possibly to be dropped subsequently if the network is overloaded.

A conforming flow can thus contain traffic with an average rate up to the rate at which tokens are added to the bucket, and have a burstiness determined by the depth of the bucket. This burstiness may be expressed in terms of either a jitter tolerance, i.e. how much sooner a packet might conform (e.g. arrive or be transmitted) than would be expected from the limit on the average rate, or a burst tolerance or maximum burst size, i.e. how much more than the average level of traffic might conform in some finite period.

9. What are the major problems with existing IPv4 network? Explain IPv4 addressing and sub-netting with examples.

Ans.: The major problems with the existing IPv4 network is described below:

The network layer protocol in the TCPIIP protocol suite is currently IPv4 (Internetworking Protocol, version 4). IPv4 provides the host-to-host communication between systems in the Internet. Although IPv4 is well designed, data communication has evolved since the inception of IPv4 in the 1970s. IPv4 has some deficiencies (listed below) that make it unsuitable for the fast-growing Internet.

- Despite all short-term solutions, such as subnetting, classless addressing, and NAT, address depletion is still a long-term problem in the Internet.
- The Internet must accommodate real-time audio and video transmission. This type of transmission requires minimum delay strategies and reservation of resources not provided in the IPv4 design.
- The Internet must accommodate encryption and authentication of data for some applications. No encryption or authentication is provided by IPv4.

IP addresses are displayed in dotted decimal notation, and appear as four numbers separated by dots. Each number of an IP address is made from eight individual bits known as octet. Each octet can create number value from 0 to 255. An IP address would be 32

bits long in binary divided into the two components, network component and host component. Network component is used to identify the network that the packet is intended for, and host component is used to identify the individual host on network.
IP addresses are broken into the two components:
Network component: - Defines network segment of device.
Host component: - Defines the specific device on a particular network segment
The practice of dividing a network into multiple subnetworks is called subnetting. Computers that belong to a subnet are addressed with a common, identical, most-significant bit-group in their IP address. Subnetting is a process of breaking large network in small networks known as subnets. Subnetting happens when we extend default boundary of subnet mask. Basically we borrow host bits to create networks. Let's take a example Being a network administrator you are asked to create two networks, each will host 30 systems. Single class C IP range can fulfill this requirement, still you have to purchase 2 class C IP range, one for each network. Single class C range provides 256 total addresses and we need only 30 addresses, this will waste 226 addresses. These unused addresses would make additional route advertisements slowing down the network.
The advantage of Subnetting are given below:

- Subnetting breaks large network in smaller networks and smaller networks are easier to manage.
- Subnetting reduces network traffic by removing collision and broadcast traffic, that overall improve performance.
- Subnetting allows you to apply network security polices at the interconnection between subnets.
- Subnetting allows you to save money by reducing requirement for IP range.

Each IP class is equipped with its own default subnet mask which bounds that IP class to have prefixed number of Networks and prefixed number of Hosts per network. Classful IP addressing does not provide any flexibility of having less number of Hosts per Network or more Networks per IP Class.
CIDR or Classless Inter Domain Routing provides the flexibility of borrowing bits of Host part of the IP address and using them as Network in Network, called Subnet. By using subnetting, one single Class A IP address can be used to have smaller sub-networks which provides better network management capabilities.

10. Write short notes on:

a) ALOHA system

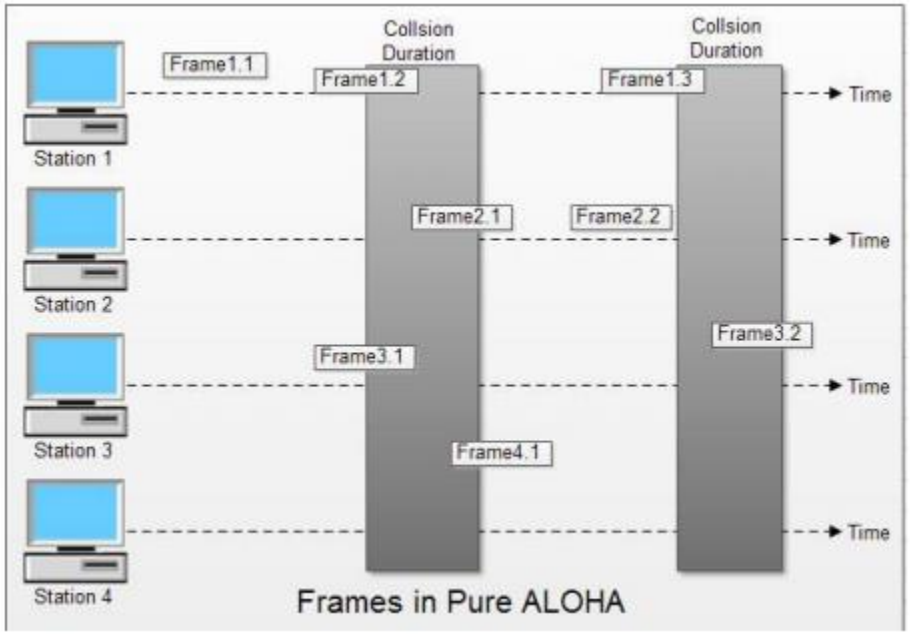
Ans.: ALOHA is a system for coordinating and arbitrating access to a shared communication Networks channel. It was developed in the 1970s by Norman Abramson and his colleagues at the University of Hawaii. The original system used for ground-based radio broadcasting, but the system has been implemented in satellite communication systems. A shared communication system like ALOHA requires a method of handling collisions that occur when two or more systems attempt to transmit on the channel at the same time. In the ALOHA system, a node transmits whenever data is available to send. If another node transmits at the same time, a collision occurs, and the frames that were transmitted

are lost. However, a node can listen to broadcasts on the medium, even its own, and determine whether the frames were transmitted.

There are two different types of ALOHA:

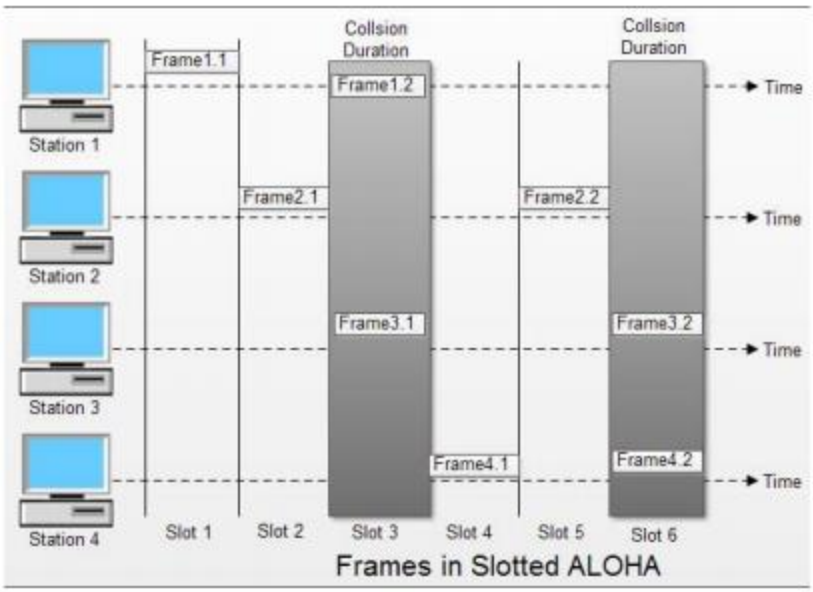
i. Pure ALOHA

In pure ALOHA, the stations transmit frames whenever they have data to send. When two or more stations transmit simultaneously, there is collision and the frames are destroyed. In pure ALOHA, whenever any station transmits a frame, it expects the acknowledgement from the receiver. If acknowledgement is not received within the specified time, the station assumes that the frame (or acknowledgement) has been destroyed. If the frame is destroyed because of collision the station waits for a random amount of time and sends it again. This waiting time must be random otherwise same frames will collide again and again. Therefore, pure ALOHA dictates that when time-out period passes, each station must wait for a random amount of time before resending its frame. this randomness will help avoid more collisions.



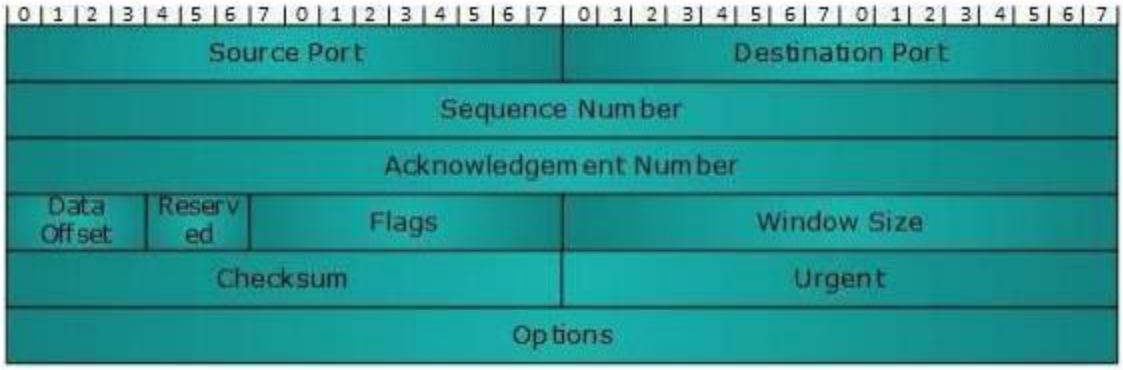
ii. Slotted ALOHA

Slotted ALOHA was invented to improve the efficiency of pure ALOHA as chances of collision in pure ALOHA are very high. In slotted ALOHA, the time of the shared channel is divided into discrete intervals called slots. The stations can send a frame only at the beginning of the slot and only one frame is sent in each slot. In slotted ALOHA, if any station is not able to place the frame onto the channel at the beginning of the slot. i.e. it misses the time slot then the station has to wait until the beginning of the next time slot. There is still chances of collision if two stations try to send at the beginning of the same time slot as shown in figure below. Slotted ALOHA still has an edge over pure ALOHA as chances of collision are reduced to one-half.



b) TCP Header

Ans.: The transmission control protocol (TCP) is one of the most important protocols of internet protocols suite. It is most widely used protocol for data transmission in communication network such as internet. The length of TCP header is minimum 20 bytes long and maximum 60 bytes.



Its different components are described below:

- Source Port (16-bits): It identifies source port of the application process on the sending device.
- Destination Port (16-bits) - It identifies destination port of the application process on the receiving device.
- Sequence Number (32-bits) - Sequence number of data bytes of a segment in a session.
- Acknowledgement Number (32-bits) - When ACK flag is set, this number contains the next sequence number of the data byte expected and works as acknowledgement of the previous data received.
- Data Offset (4-bits) - This field implies both, the size of TCP header (32-bit words) and the offset of data in current packet in the whole TCP segment.

- Reserved (3-bits) - Reserved for future use and all are set zero by default.
- Flags (1-bit each)
    - NS - Nonce Sum bit is used by Explicit Congestion Notification signaling process.
    - CWR - When a host receives packet with ECE bit set, it sets Congestion Windows Reduced to acknowledge that ECE received.
    - ECE -It has two meanings:
        - If SYN bit is clear to 0, then ECE means that the IP packet has its CE (congestion experience) bit set.
        - If SYN bit is set to 1, ECE means that the device is ECT capable.
    - URG - It indicates that Urgent Pointer field has significant data and should be processed.
    - ACK - It indicates that Acknowledgement field has significance. If ACK is cleared to 0, it indicates that packet does not contain any acknowledgement.
    - PSH - When set, it is a request to the receiving station to PUSH data (as soon as it comes) to the receiving application without buffering it.
    - RST - Reset flag has the following features:
        - It is used to refuse an incoming connection.
        - It is used to reject a segment.
        - It is used to restart a connection.
    - SYN - This flag is used to set up a connection between hosts.
    - FIN - This flag is used to release a connection and no more data is exchanged thereafter. Because packets with SYN and FIN flags have sequence numbers, they are processed in correct order.
- Windows Size - This field is used for flow control between two stations and indicates the amount of buffer (in bytes) the receiver has allocated for a segment, i.e. how much data is the receiver expecting.
- Checksum - This field contains the checksum of Header, Data and Pseudo Headers.
- Urgent Pointer - It points to the urgent data byte if URG flag is set to 1.
- Options - It facilitates additional options which are not covered by the regular header. Option field is always described in 32-bit words. If this field contains data less than 32-bit, padding is used to cover the remaining bits to reach 32-bit boundary.

2070 CHAITRA

1.What are the features of client/ Server Architecture? What are headers and trailers and how do they get added and removed? Explain.

Ans: Client-server architecture (client/server) is a network architecture in which each computer or process on the network is either a client or a server. Servers are powerful computers or processes dedicated to managing disk drives (file servers), printers (print servers), or network traffic

(network servers). Clients are PCs or workstations on which users run applications. Clients rely on servers for resources, such as files, devices, and even processing power.
The features of client/server architecture are:

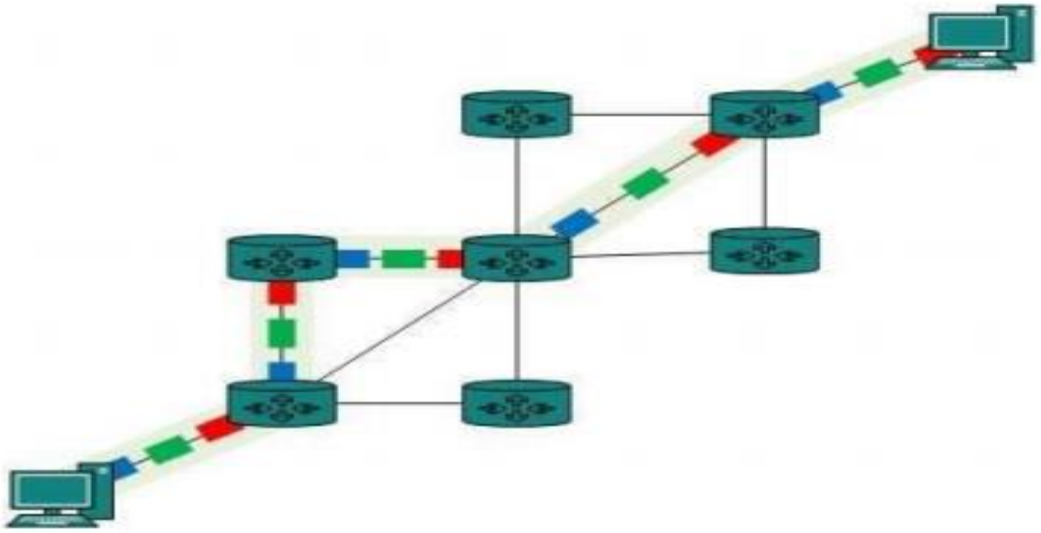
- It is widely used and forms the basis of much network usage.
- This whole arrangement is called the client-server model.
- It is applicable when the client and server are both in the same building but also when they are far apart.
- Under most conditions, one server can handle a large number of clients.
- If we look at the client-server model in detail, we see that two processes are involved, one on the client machine and one on the server machine.
- Communication takes the form of the client process sending a message over the network to the server process.
- The client process then waits for a reply message.
- When the server process gets the request, it performs the requested work or looks up the requested data and sends back a reply.

Headers and trailers are control data added at the beginning and the end of each data unit at each layer of the sender and removed at the corresponding layers of the receiver. They provide source and destination addresses, synchronization points, information for error detection
Adding:
An obvious technique is to allocate memory that can hold what exists plus the piece to be added and to copy each into its proper place. A variation on that is to allocate a block of memory and to place each layer's content in the block such that there is room at the beginning for headers that will be added later lower in the stack

Removing:
Removing without copying is easy. One-layer passes content to the one above as a pointer or two. One pointer can point to a status data area followed by content. With two pointers, one can point to the incoming content, while the other points to status information about the information flow.

2.What do you mean by data switching? Explain about various types of switching with practical implementation example.

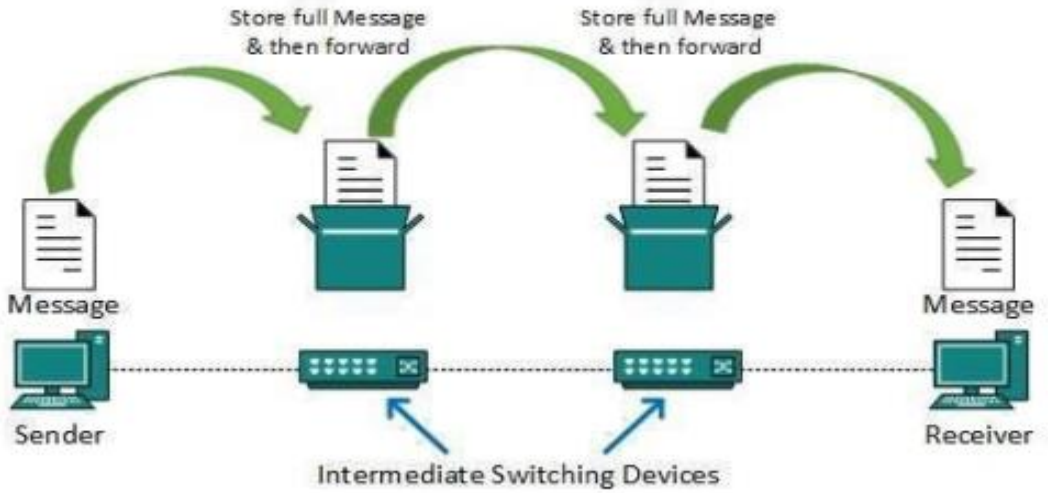
Ans: Switching is process to forward packets coming in from one port to a port leading towards the destination. When data comes on a port it is called ingress, and when data leaves a port or goes out it is called egress. A communication system may include number of switches and nodes.
The types of switching and their implementation in real world are:
Circuit Switching
When two nodes communicate with each other over a dedicated communication path, it is called circuit switching. There 'is a need of pre-specified route from which data will travels and no other data is permitted. In circuit switching, to transfer the data, circuit must be established so that the data transfer can take place.



Telephone is the best suitable example of circuit switching. Before a user can make a call, a virtual path between caller and callee is established over the network.

Message Switching

This technique was somewhere in middle of circuit switching and packet switching. In message switching, the whole message is treated as a data unit and is switching / transferred in its entirety.

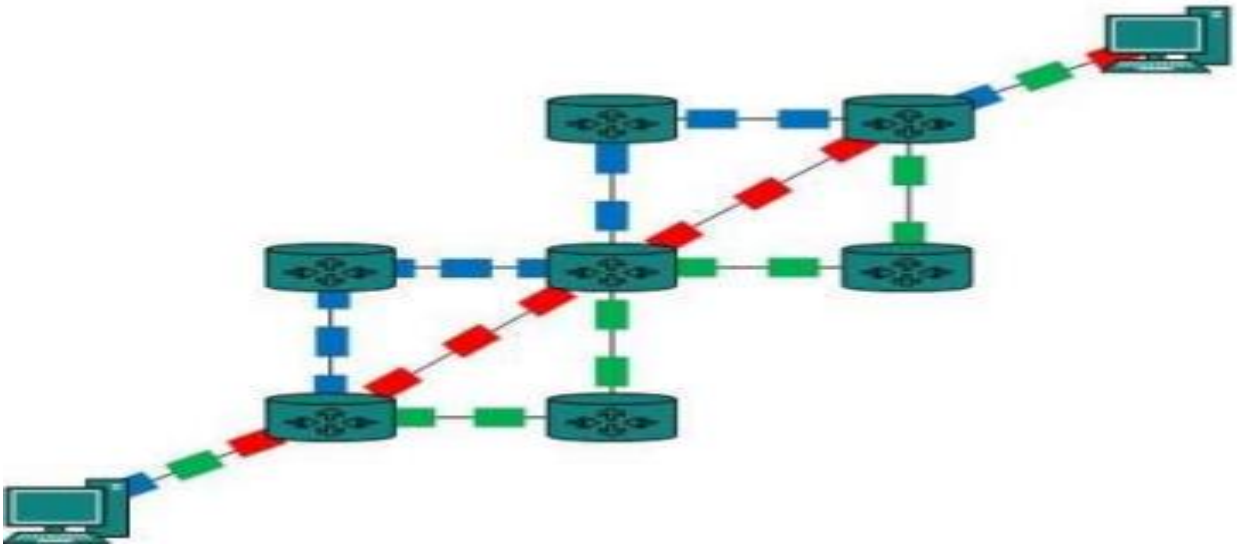


A switch working on message switching, first receives the whole message and buffers it until there are resources available to transfer it to the next hop. If the next hop is not having enough resource to Accommodate large size message, the message is stored and switch waits.

Packet Switching

Shortcomings of message switching gave birth to an idea of packet switching. The entire message is broken down into smaller chunks called packets. The switching information is added in the header of each packet and transmitted independently.

Packet switching enhances line efficiency as packets from multiple applications can be multiplexed over the carrier. The internet uses packet switching technique. Packet switching enables the user to differentiate data streams based on priorities. Packets are stored and forwarded according to their priority to provide quality of service.



3.What are the differences between the error correcting and error detection process? A bit string 01111011111011111110 needs to be transmitted at the data link layer, what is the string actually transmitted after bit suffering, if flag patterns is 0111110.

Ans:

Error Detection

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

Method of detection of error are:
Parity Check
Cyclic Redundancy Check (CRC)
Error Correction
In correction we need to know the exact number of bits that are corrupted and their location in the message.
Method of correcting of error are:

- Backward Error Correction
- Forward Error Correction

4.Explain the working principle of different types of networks devices repeater, hub, bridges, switch and routers.

Ans: Hub

Hub is one of the basic icons of networking devices which works at physical layer and hence connect networking devices physically together. Hubs are fundamentally used in networks that use

twisted pair cabling to connect devices. They are designed to transmit the packets to the other appended devices without altering any of the transmitted packets received. They act as pathways to direct electrical signals to travel along. They transmit the information regardless of the fact if data packet is destined for the device connected or not.

Hub falls in two categories:

Active Hub:

They are smarter than the passive hubs. They not only provide the path for the data signals in fact they regenerate, concentrate and strengthen the signals before sending them to their destinations. Active hubs are also termed as 'repeaters.

Passive Hub:

They are more like point contact for the wires to built in the physical network. They have nothing to do with modifying the signals.

Repeater

A repeater connects two segments of your network cable. It retimes and regenerates the signals to proper amplitudes and sends them to the other segments. When talking about, ethernet topology, you are probably talking about using a hub as a repeater. Repeaters require a small amount of time to regenerate the signal. This can cause a propagation delay which can affect network communication when there are several repeaters in a row. Many network architectures limit the number of repeaters that can be used in a row. Repeaters work only at the physical layer of the OSI network model.

Switches

Switches are the linkage points of an Ethernet network. Just as in hub, devices in switches are connected to them through twisted pair cabling. But the difference shows up in the manner both the devices; hub and a switch treat the data they receive. Hub works by sending the data to all the ports on the device whereas a switch transfers it only to that port which is connected to the destination device. A switch does so by having an in-built learning of the MAC address of the devices connected to it. Since the transmission of data signals are well defined in a switch hence the network performance is consequently enhanced.

Bridges

A bridge is a computer networking device that builds the connection with the other bridge networks which use the same protocol. It works at the Data Link layer of the OSI Model and connects the different networks together and develops communication between them. It connects two local-area networks; two physical LANs into larger logical LAN or two segments of the same LAN that use the same protocol.

Routers

Routers are network layer devices and are particularly identified as Layer- 3 devices of the OSI Model. They process logical addressing information in the Network header of a packet such as IP Addresses. Router is used to create larger complex networks by complex traffic routing.

Static Routing:
In static routing, the routing information is fed into the routing tables manually. It does not only become a time-taking task but gets prone to errors as well. The manual updating is also required in case of statically configured routers when change in the topology of the network or in the layout takes place.
Dynamic Routing:
For larger environment dynamic routing proves to be the practical solution. The process involves use of peculiar routing protocols to hold communication. The purpose of these protocols is to enable the other routers to transfer information about to other routers, so that the other routers can build their own routing tables.

5.Explain UDP segment structures.Illustrate your answer with appropriate figures.

Ans: The User Datagram Protocol (UDP) is simplest Transport Layer communication protocol available of the TCP/IP protocol suite. It involves minimum amount of communication mechanism. UDP is said to be an unreliable transport protocol but it uses IP services which provides best effort delivery mechanism. In UDP, the receiver does not generate an acknowledgement of packet received and in turn, the sender does not wait for any acknowledgement of packet sent. This shortcoming makes this protocol unreliable as well as easier on processing.
Features
• UDP is used when acknowledgement of data does not hold any significance.
• UDP is good protocol for data flowing in one direction.
• UDP is simple and suitable for query based communications.
• UDP is not connection oriented.
• UDP does not provide congestion control mechanism.
• UDP does not guarantee ordered delivery of data.
• UDP is stateless.
• UDP is suitable protocol for streaming applications such as VoIP, multimedia streaming.
UDP Header UDP header is as simple as its function.
UDP header contains four main parameters:
• Source Port - This 16 bits information is used to identify the source port of the packet.
• Destination Port - This 16 bits information, is used identify application level service on destination machine.
• Length - Length field specifies the entire length of UDP packet (including header). It is 16-bits field and minimum value is 8-byte, i.e. the size of UDP header itself.

• Checksum - This field stores the checksum value generated by the sender before sending. IPv4 has this field as optional so when checksum field does not contain any value it is made 0 and all its bits are set to zero.
UDP application
Here are few applications where UDP is used to transmit data:
• Domain Name Services
• Simple Network Management Protocol
• Trivial File Transfer Protocol
• Routing Information Protocol

6.What do you mean by email server? What are the protocols used on it?

Ans: An email server, or simply mail server, is an application or computer in a network whose sole purpose is to act as a virtual post office. The server stores incoming mail for distribution to local users and sends out outgoing messages. This uses a client-server application model to send and receive messages using Simple Mail Transfer Protocol (SMTP).
Mail servers send and receive email using standard email protocols. For example, the SMTP protocol sends messages and handles outgoing mail requests. The IMAP and POP3 protocols receive messages and are used to process incoming mail. When you log on to a mail server using a webmail interface or email client, these protocols handle all the connections behind the scenes.

These are the protocol used on it are they:

Simple Mail Transfer Protocol (SMTP)
SMTP stands for Simple Mail Transfer Protocol. SMTP is used when email is delivered from an email client, such as Outlook Express, to an email server or when email is delivered from one email server to another. SMTP uses port 25.
SMTP provides those codes, and email server software is designed to understand what they mean. As each message travels towards its destination, it sometimes passes through a number of computers as well as their individual MTAs. As it does, it's briefly stored before it moves on to the next computer in the path. Think of it as a letter going through different hands as it winds its way to the right mailbox.

Post Office Protocol (POP)
POP3 stands for Post Office Protocol. POP3 allows an email client to download an email from an email server. The POP3 protocol is simple and does not offer many features except for download. Its design assumes that the email client downloads all available email from the server, deletes them from the server and then disconnects. POP3 normally uses port 110. (1) POP is short for Post Office Protocol, a protocol used to retrieve e-mail from a mail server. Most e-mail applications (sometimes called an e-mail client) use the POP protocol, although some can use the newer IMAP (Internet Message Access Protocol).

8. Explain the IPv6 datagram format with appropriate figures.

Ans.: Internet Protocol version 6 (IPv6) is the most recent version of the internet protocol (IP), the communications protocol that provides an identification and location system for computers on networks and routes traffic across the Internet. IPv6 was developed by the Internet Engineering Task Force (IETF) to deal with the long-anticipated problem of IPv4 address exhaustion. IPv6 is intended to replace IPv4. The IPV6 packet is shown in the figure below. Each packet is composed of a mandatory base header followed by the payload. The payload consists of two parts: optional extension headers and data from an upper layer. The base header occupies 40 bytes, whereas the extension headers and data from the upper layer contains up to 65535 bytes of information.

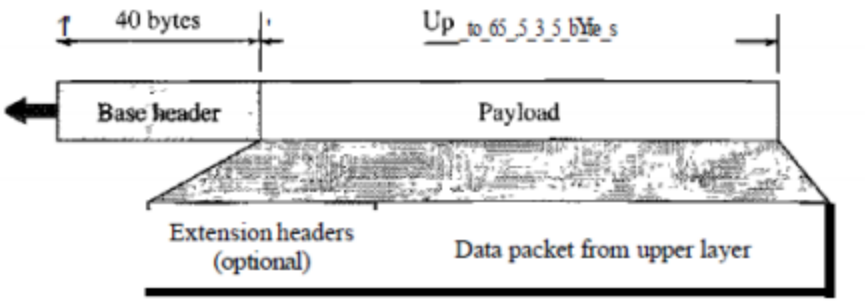


Figure 1 IPv6 datagram header and payload

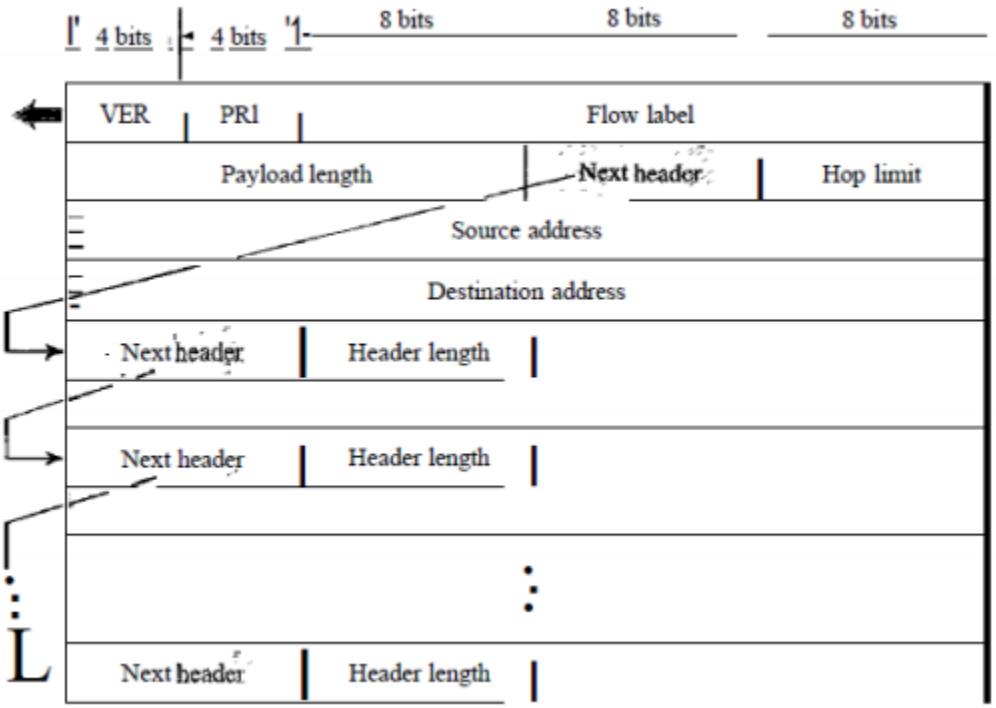


Figure 2 Format of an IPv6 datagram

The figure shows the base header with its eight fields. These fields are as flows:

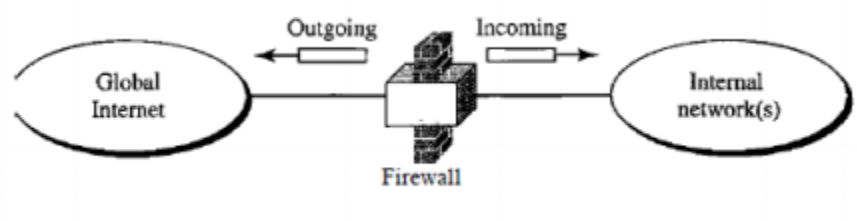
- Version. This 4-bit field defines the version number of the IP. For IPv6, the value is 6.
- Priority. The 4-bit priority field defines the priority of the packet with respect to traffic congestion.
- Flow label. The flow label is a 3-byte (24-bit) field that is designed to provide special handling for a particular flow of data.
- Payload length. The 2-byte payload length field defines the length of the IP datagram excluding the base header.
- Next header. The next header is an 8-bit field defining the header that follows the base header in the datagram. The next header is either one of the optional extension headers used by IP or the header of an encapsulated packet such as UDP or TCP. Each extension

header also contains this field. Table 20.6 shows the values of next headers. Note that this field in version 4 is called the protocol.

- Hop limit. This 8-bit hop limit field serves the same purpose as the TIL field in IPv4.
- Source address. The source address field is a 16-byte (128-bit) Internet address that identifies the original source of the datagram.
- Destination address. The destination address field is a 16-byte (128-bit) Internet address that usually identifies the final destination of the datagram. However, if source routing is used, this field contains the address of the next router.

9. Explain briefly how firewalls protect network and also explain different types of Firewall. Illustrate your answer with appropriate figures.

Ans.: A firewall is a device (usually a router or a computer) installed between the internal network of an organization and the rest of the Internet. It is designed to forward some packets and filter (not forward) others.



For example, a firewall may filter all incoming packets destined for a specific host or a specific server such as HTTP. A firewall can be used to deny access to a specific host or a specific service in the organization. A firewall is usually classified as a packet-filter firewall or a proxy-based firewall.

Packet-Filter Firewall

The first reported type of network firewall is called a packet filter. Packet filters act by inspecting packets transferred between computers. When a packet does not match the packet filter's set of filtering rules, the packet filter either drops (silently discards) the packet, or rejects the packet (discards it and generates an Internet Control Message Protocol notification for the sender) else it is allowed to pass.[6] Packets may be filtered by source and destination network addresses, protocol, source and destination port numbers. The bulk of Internet communication in 20th and early 21st century used either Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) in conjunction with well-known ports, enabling firewalls of that era to distinguish between, and thus control, specific types of traffic (such as web browsing, remote printing, email transmission, file transfer), unless the machines on each side of the packet filter used the same non-standard ports. The first paper published on firewall technology was in 1988, when engineers from Digital Equipment Corporation (DEC) developed filter systems known as packet filter firewalls. At AT&T Bell Labs, Bill Cheswick and Steve Bellovin continued their research in packet filtering and developed a working model for their own company based on their original first generation architecture.

Proxy-based Firewall

A proxy firewall is a network security system that protects network resources by filtering messages at the application layer. A proxy firewall may also be called an application

firewall or gateway firewall. Just like a proxy server or cache server, a proxy firewall acts as an intermediary between in-house clients and servers on the Internet. The difference is that in addition to intercepting Internet requests and responses, a proxy firewall also monitors incoming traffic for layer 7 protocols, such as HTTP and FTP. In addition to determining which traffic is allowed and which is denied, a proxy firewall uses stateful inspection technology and deep packet inspection to analyze incoming traffic for signs of attack. Proxy firewalls are considered to be the most secure type of firewall because they prevent direct network contact with other systems. (Because a proxy firewall has its own IP address, an outside network connection will never receive packets from the sending network directly.) Having the ability to examine the entire network packet, rather than just the network address and port number, also means that a proxy firewall will have extensive logging capabilities -- a valuable resource for security administrators who are dealing with security incidents. According to Marcus Ranum, who is credited with conceiving the idea of a proxy firewall, the goal of the proxy approach is to create a single point that allows a security-conscious programmer to assess threat levels represented by application protocols and put error detection, attack detection and validity checking in place. The added security offered by a proxy firewall has its drawbacks, however. Because a proxy firewall establishes an additional connection for each outgoing and incoming packet, the firewall can become a bottleneck, causing a degradation of performance or becoming a single point of failure. Additionally, proxy firewalls may only support certain popular network protocols, thereby limiting which applications the network can support.

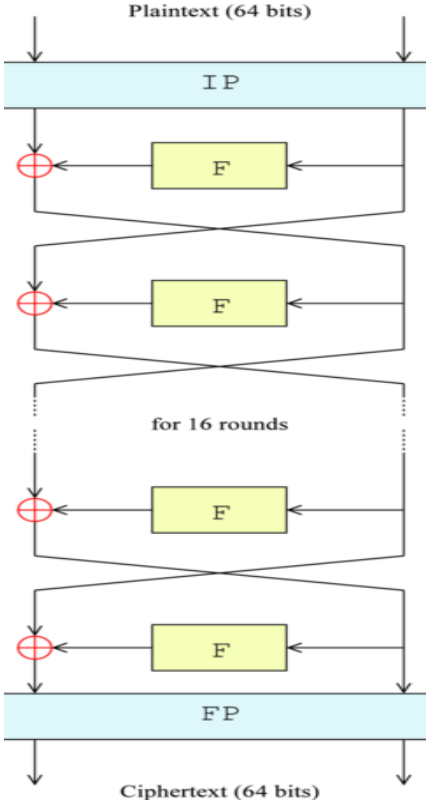
10. What do you mean by Network security? Explain the operation of Data Encryption Standard Algorithm.

Ans.: Network security consists of the policies and practices adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs; conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions. It does as its title explains: it secures the network, as well as protecting and overseeing operations being done. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password.

The operation of Data encryption standard algorithm is described below:

DES is the archetypal block cipher—an algorithm that takes a fixed-length string of plaintext bits and transforms it through a series of complicated operations into another ciphertext bitstring of the same length. In the case of DES, the block size is 64 bits. DES also uses a key to customize the transformation, so that decryption can supposedly only be performed by those who know the particular key used to encrypt. The key ostensibly consists of 64 bits; however, only 56 of these are actually used by the algorithm. Eight

bits are used solely for checking parity, and are thereafter discarded. Hence the effective key length is 56 bits. The key is nominally stored or transmitted as 8 bytes, each with odd parity. Like other block ciphers, DES by itself is not a secure means of encryption, but must instead be used in a mode of operation. Decryption uses the same structure as encryption, but with the keys used in reverse order. (This has the advantage that the same hardware or software can be used in both directions.)



2071 CHAITRA

Question No. 1.

Network Architecture is the complete framework of an organization's computer network. The diagram of the network architecture provides a full picture of the established network with detailed view of all the resources accessible. It includes hardware components used for communication, cabling and device types, network layout and topologies, physical and wireless connections, implemented areas and also the software rules and protocols needed.

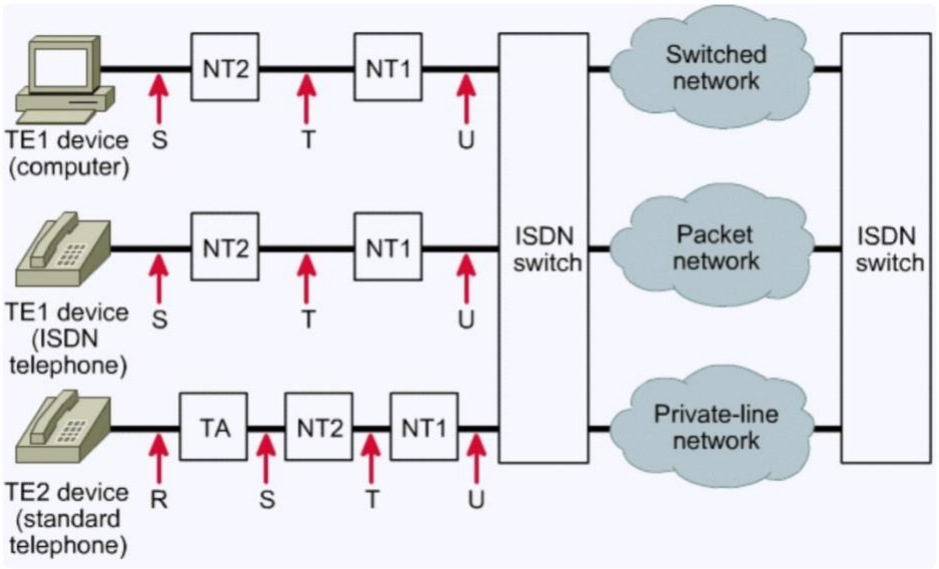
The difference between TCP/IP and OSI reference models:

TCP/IP reference model	OSI reference model
TCP/IP model is a protocol-oriented standard.	OSI model is a generic model that is based upon functionalities of each layer.
TCP/IP does not have a clear distinction between services, interfaces and protocols.	OSI model distinguishes the three concepts, services, interfaces, and protocols.
TCP/IP protocols layout standards on which the Internet was developed.	OSI model gives guidelines on how communication needs to be done.

TCP/IP suite, the protocols were developed first and then the model was developed.	In OSI, the model was developed first and then the protocols in each layer were developed.
TCP/IP has four layers.	The OSI has seven layers.

X.25 is a standard protocol for packet switched WAN communication. It contains packet switching exchange (PSE) nodes as networking hardware and plain old telephone service connection or ISDN connection as physical links. It contains physical, data link and packet layer. It is used for networks for ATMs and credit card verification. It allows multiple logical channels to use the same physical line. It also permits data exchange between terminals with different communication speeds.

Question No. 2

ISDN,  known as

Integrated Services Digital Network, is a digital network which allows digital signals to be sent over existing telephone line. It is a communication standard for simultaneous digital transmission of voice, video and data over the traditional circuits of PSTN. It is a circuit switched telephone network, which also provides access to packet switched network.

Figure: ISDN Architecture

There are three main types of channels used in the ISDN network viz. bearer (B), data (D) and hybrid (H) channels. Different data rates can be obtained by the user with combinations of these channels. One bearer channel supports 64 kbps, one data channel supports between 16 to 64 kbps and one hybrid channel supports 384 or 1536 or 1920 kbps data rates.

The following are the interfaces of ISDN:

Basic Rate Interface (BRI) – There is two data-bearer channels and one data channel in BRI to initiate connections. The B channels operate at a maximum of 64 Kbps while the D channel operates at a maximum of 16 Kbps. The two channels are independent of each other. For example, one channel is used as a TCP/IP connection to a location while the other channel is used to send a fax to a remote location.

Primary Rate Interface (PRI) – Primary Rate Interface service consists of 1 D channel and 23 B channels. Hence, it supports about 1.544 Mbps with 64 kbps B channel, 64 kbps D channel and 8 overhead.

Broadband-ISDN (B-ISDN) – Narrowband ISDN has been designed to operate over the current communications infrastructure, which is heavily dependent on the copper cable however B-ISDN relies mainly on the evolution of fiber optics.

Components of ISDN

- Terminal Equipment-1 or TE1 is used to interface ISDN terminal with the network.
- Terminal Equipment-2 or TE2 is used to interface Non-ISDN terminal with the network such as Plain Old Telephony.
- Terminal Adapter or TA Allows non ISDN devices to be interfaced with ISDN network.
- Network Termination-1 or NT1 is physical layer device which separates user premises from Phone Company.
- Network Termination-2 or NT2 functions as per OSI layers 2 to 3. PBX and LAN are considered as NT-2 devices.

Question No. 3

The multiple access protocols are of three types:

1. Random Access Protocol: All stations have same superiority that is no station has more priority than another station and any station can send data depending on medium's state.
2. Controlled Access Protocol: Here, the data is sent by that station which is approved by all other stations.

3. Channelization protocol: The available bandwidth of the link is shared in time, frequency and code to multiple stations to access channel simultaneously.

The foundation of a token ring is the IEEE 802.5 network. It uses a special three-byte frame called a "token" that travels around a logical "ring" of workstations or servers and whichever node grabs that token will have right to transmit the data.

Whenever a station wants to transmit a frame it inverts a single bit of the 3-byte token which instantaneously changes it into a normal data packet. Because there is only one token, there can at most be one transmission at a time. Since the token rotates in the ring it is guaranteed that every node gets the token with in some specified time. So there is an upper bound on the time of waiting to grab the token so that starvation is avoided. There is also an upper limit of 250 on the number of nodes in the network. To distinguish the normal data packets from token (control packet) a special sequence is assigned to the token packet. When any node gets the token it first sends the data it wants to send, then re-circulates the token.

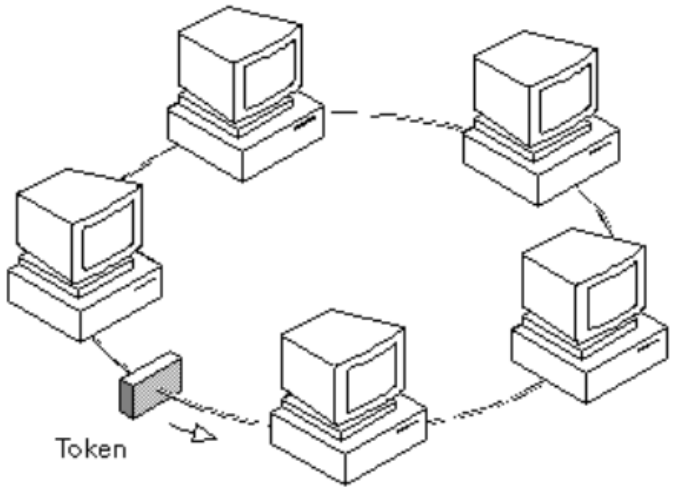


Figure: Token ring

If a node transmits the token and nobody wants to send the data the token comes back to the sender. If the first bit of the token reaches the sender before the transmission of the last bit, then error situation arises. So to avoid this we should have:
Propagation delay + transmission of n-bits (1-bit delay in each node) > transmission of the token time
A station may hold the token for the token-holding time which is 10 ms unless the installation sets a different value. If there is enough time left after the first frame has been transmitted to send more frames, then these frames may be sent as well. After all pending frames have been transmitted or the transmission frame would exceed the token-holding time, the station regenerates the 3-byte token frame and puts it back on the ring.
There are three modes of operation:

- Listen Mode: In this mode the node listens to the data and transmits the data to the next node. In this mode there is a one-bit delay associated with the transmission.
- Transmit Mode: In this mode the node just discards the any data and puts the data onto the network.
- By-pass Mode: In this mode reached when the node is down. Any data is just bypassed. There is no one-bit delay in this mode.

Q.4

1st part

Network security consists of the policies and practices adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs; conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions. It does as its title explains: it secures the network, as well as protecting and overseeing operations being done. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password.

2nd part

Virtual private network (VPN) is a technology that is gaining popularity among large organizations that use the global Internet for both intra- and inter organization communication, but require privacy in their internal communications. We discuss VPN here because it uses the IPSec Protocol to apply security to the IP datagram. A technology called virtual private network allows organizations to use the global Internet for both purposes. VPN creates a network that is private but virtual. It is private because it guarantees privacy inside the organization. It is virtual because it does not use real private WANs; the network is physically public but virtually private. Routers Rl and R2 use VPN technology to guarantee privacy for the organization.

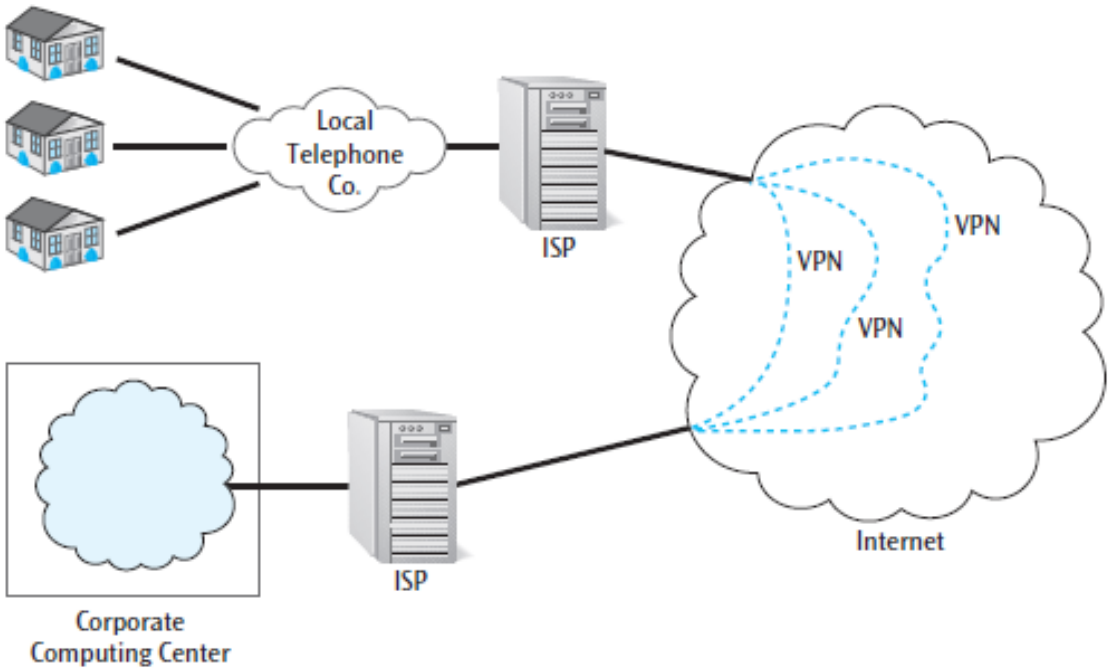


Fig: Virtual Private Network

Applications running on a computing device, e.g., a laptop, desktop, smartphone, across a VPN may therefore benefit from the functionality, security, and management of the private network. Encryption is a common, though not an inherent, part of a VPN connection.

Q.6

1st part

A port number is a way to identify a specific process to which an Internet or other network message is to be forwarded when it arrives at a server. For the Transmission Control Protocol and the User

Datagram Protocol, a port number is a 16-bit integer that is put in the header appended to a message unit. This port number is passed logically between client and server transport layers and physically between the transport layer and the Internet Protocol layer and forwarded on.
So, port number is used in networking.
2nd part
Transport layer services are conveyed to an application via a programming interface to the transport layer protocols. The services may include the following features:

- Connection-oriented communication:

  It is normally easier for an application to interpret a connection as a data stream rather than having to deal with the underlying connection-less models, such as the datagram model of the User Datagram Protocol (UDP) and of the Internet Protocol (IP).
- Same order delivery:

  The network layer doesn't generally guarantee that packets of data will arrive in the same order that they were sent, but often this is a desirable feature. This is usually done through the use of segment numbering, with the receiver passing them to the application in order. This can cause head-of-line blocking.
- Reliability:

  Packets may be lost during transport due to network congestion and errors. By means of an error detection code, such as a checksum, the transport protocol may check that the data is not corrupted, and verify correct receipt by sending an ACK or NACK message to the sender. Automatic repeat request schemes may be used to retransmit lost or corrupted data.
- Flow control:

  The rate of data transmission between two nodes must sometimes be managed to prevent a fast sender from transmitting more data than can be supported by the receiving data buffer, causing a buffer overrun. This can also be used to improve efficiency by reducing buffer underrun.
- Congestion avoidance:

  Congestion control can control traffic entry into a telecommunications network, so as to avoid congestive collapse by attempting to avoid oversubscription of any of the processing

or link capabilities of the intermediate nodes and networks and taking resource reducing steps, such as reducing the rate of sending packets. For example, automatic repeat requests may keep the network in a congested state; this situation can be avoided by adding congestion avoidance to the flow control, including slow-start. This keeps the bandwidth consumption at a low level in the beginning of the transmission, or after packet retransmission.

- Multiplexing:

  Ports can provide multiple endpoints on a single node. For example, the name on a postal address is a kind of multiplexing, and distinguishes between different recipients of the same location. Computer applications will each listen for information on their own ports, which enables the use of more than one network service at the same time. It is part of the transport layer in the TCP/IP model, but of the session layer in the OSI model.

3rd part

Differentiating between TCP and UTP protocol:

Protocol	TCP	UDP
Connection	connection-oriented	connectionless
Usage	high reliability, critical-less transmission time	fast, efficient transmission, small queries, huge numbers of clients
Ordering of data packets	rearranges packets in order	no inherent order
Reliability	yes	no
Streaming of data	read as a byte stream	sent and read individually
Error checking	error checking and recovery	simply error checking, no error recovery
Acknowledgement	acknowledgement segments	no acknowledgment

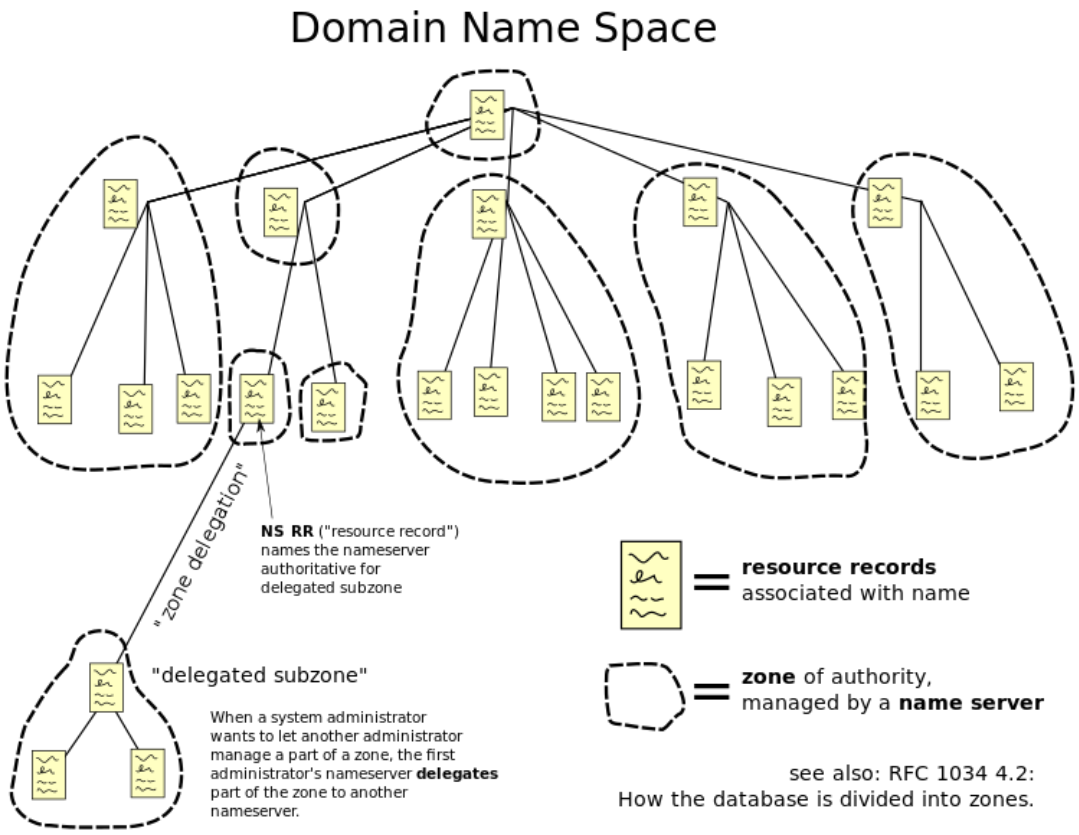
Q.7

1st part

The Domain Name System (DNS) is a hierarchical and decentralized naming system for computers, services, or other resources connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities. Most prominently, it translates more readily memorized domain names to the numerical IP addresses needed for locating and identifying computer services and devices with the underlying network protocols.

2nd part

Structure



Domain name Space

The domain name space consists of a tree data structure. Each node or leaf in the tree has a label and zero or more resource records (RR), which hold information associated with the domain name. The domain name itself consists of the label, concatenated with the name of its parent node on the right, separated by a dot.

The tree sub-divides into zones beginning at the root zone. A DNS zone may consist of only one domain, or may consist of many domains and sub-domains, depending on the administrative choices of the zone manager. DNS can also be partitioned according to class where the separate classes can be thought of as an array of parallel namespace trees.

Domain name syntax, internationalization

The right-most label conveys the top-level domain; for example, the domain name www.example.com belongs to the top-level domain com.

The hierarchy of domains descends from right to left; each label to the left specifies a subdivision, or subdomain of the domain to the right. For example, the label example specifies a subdomain of the com domain, and www is a subdomain of example.com. This tree of subdivisions may have up to 127 levels. A label may contain zero to 63 characters. The null label, of length zero, is reserved for the root zone. The full domain name may not exceed the length of 253 characters in its textual representation.[1] In the internal binary representation of the DNS the maximum length requires 255 octets of storage, as it also stores the length of the name.

Name servers

The Domain Name System is maintained by a distributed database system, which uses the client–server model. The nodes of this database are the name servers. Each domain has at least one authoritative DNS server that publishes information about that domain and the name servers of any domains subordinate to it. The top of the hierarchy is served by the root name servers, the servers to query when looking up (resolving) a TLD.

Authoritative name server

An authoritative name server is a name server that only gives answers to DNS queries from data that has been configured by an original source, for example, the domain administrator or by dynamic DNS methods, in contrast to answers obtained via a query to another name server that only maintains a cache of data.

6. What are the problems of IPV4 ? How IPV6 reduce these problems? Explain different strategies to transit from IPV4 and IPV6.

IPv4 has some deficiencies (listed below) that make it unsuitable for the fast-growing Internet.

o Despite all short-term solutions, such as subnetting, classless addressing, and NAT, address depletion is still a long-term problem in the Internet.

o The Internet must accommodate real-time audio and video transmission. This type of transmission requires minimum delay strategies and reservation of resources not provided in the IPv4 design.

o The Internet must accommodate encryption and authentication of data for some applications. No encryption or authentication is provided by IPv4.

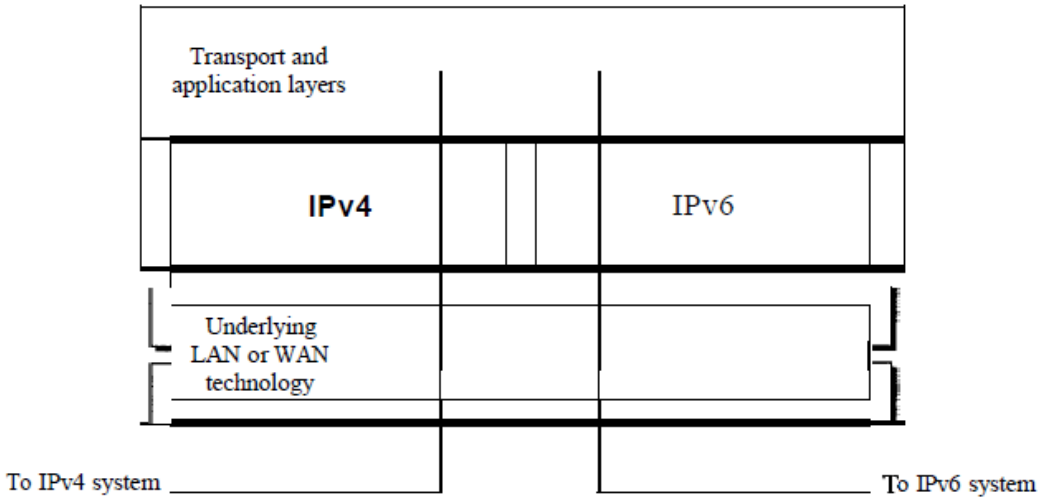
IPV6 reduces the problem by:

- Larger address space. An IPv6 address is 128 bits long, Compared with the 32-bit address of IPv4, this is a huge increase in the address space.
- Better header format. IPv6 uses a new header format in which options are separated from the base header and inserted, when needed, between the base header and the upper-layer data. This simplifies and speeds up the routing process because most of the options do not need to be checked by routers.
- New options. IPv6 has new options to allow for additional functionalities.
- Allowance for extension. IPv6 is designed to allow the extension of the protocol if required by new technologies or applications.
- Support for resource allocation. In IPv6, the type-of-service field has been removed, but a mechanism has been added to enable the source to request special handling of the packet. This mechanism can be used to support traffic such as real-time audio and video.
- Support for more security. The encryption and authentication options in IPv6 provide

Dual Stack

It is recommended that all hosts, before migrating completely to version 6, have a dual stack of protocols. In other words, a station must run IPv4 and IPv6 simultaneously untilall the Internet uses IPv6.

Figure 20.19 *Dual stack*

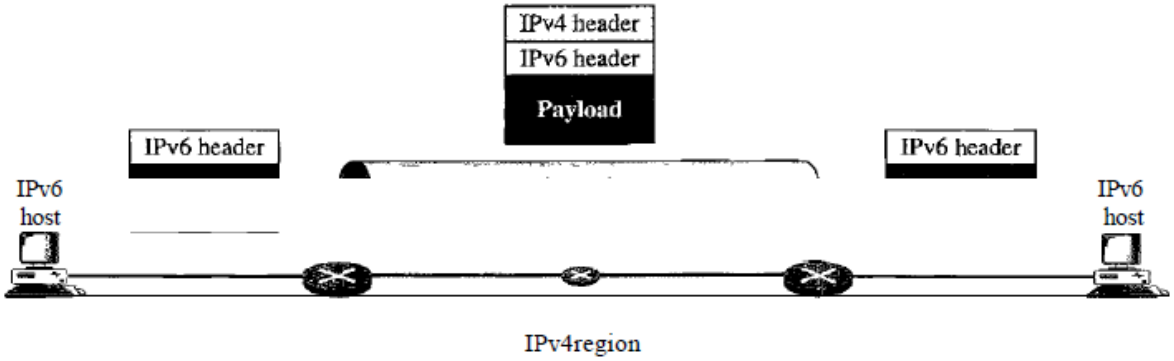


To determine which version to use when sending a packet to a destination, the source host queries the DNS. If the DNS returns an IPv4 address, the source host sends an IPv4 packet. If the DNS returns an IPv6 address, the source host sends an IPv6 packet.

Tunneling

Tunneling is a strategy used when two computers using IPv6 want to communicate with each other and the packet must pass through a region that uses IPv4. To pass through this region, the packet must have an IPv4 address. So the IPv6 packet is encapsulated in an IPv4 packet when it enters the region, and it leaves its capsule when it exits the region. It seems as if the IPv6 packet goes through a tunnel at one end and emerges at the other end. To make it clear that the IPv4 packet is carrying an IPv6 packet as data, the protocol value is set to 41.

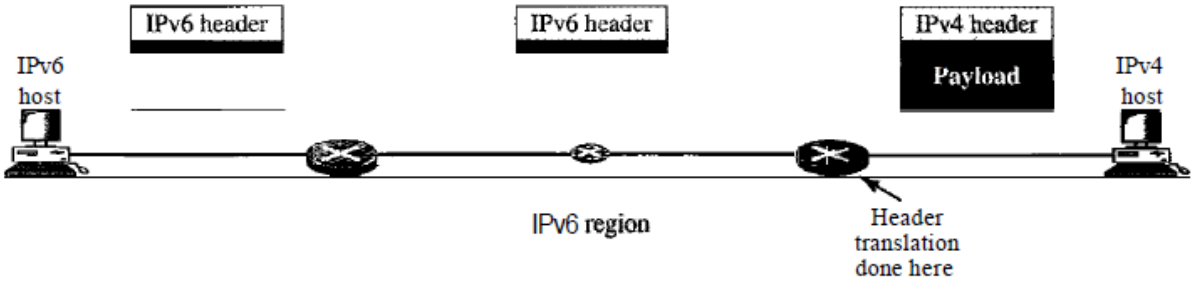
Figure 20.20 *Tunneling strategy*



Header Translation

Header translation is necessary when the majority of the Internet has moved to IPv6 but some systems still use IPv4. The sender wants to use IPv6, but the receiver does not understand IPv6. Tunneling does not work in this situation because the packet must be in the IPv4 format to be understood by the receiver. In this case, the header format must be totally changed through header translation. The header of the IPv6 packet is converted to an IPv4 header

Figure 20.21 *Header translation strategy*



Header translation uses the mapped address to translate an IPv6 address to an IPv4 address.

9. What is public key cryptography? Explain about RSA algorithm in detail.

Public key cryptography (PKC) is an encryption technique that uses a paired public and private key (or asymmetric key) algorithm for secure data communication. A message sender uses a recipient's public key to encrypt a message. To decrypt the sender's message, only the recipient's private key may be used. RSA (Rivest–Shamir–Adleman) is an algorithm used by modern computers to encrypt and decrypt messages. It is an asymmetric cryptographic algorithm. Asymmetric means that there are two different keys. This is also called public key cryptography, because one of the keys can be given to anyone.

RSA Algorithm

Explained above ….

A user of RSA creates and then publishes a public key based on two large prime numbers, along with an auxiliary value. The prime numbers must be kept secret. Anyone can use the public key to encrypt a message, but only someone with knowledge of the prime numbers can decode the message

10. Write short notes on:

a) SSL

SSL (Secure Socket Layer) is a network layer security protocol which is responsible for ensuring security of data or messages in transit through http, ldap, smtp, imap or pop3 application layers and practically ensures a reliable end-to-end secure and authenticated connection between the client and the server over the open Internet.

Objectives of Secure Socket Layer

The key objectives of SSL are listed as follows

1. SSL protocol makes use of standard key cryptographic techniques, mainly public key encryption, to authenticate participants in a communication session at the client and server end. Generally the service client is authenticated by the examination of a digital certificate. Authentication at the client end can also use a similar security mechanism which is offered via SSL protocol.

2. SSL protocol ensures data integrity through encryption during a communication session so that data may not be tampered with by misusing Attack vectors or other techniques.

3. SSL protocol ensures data privacy during transit in a communication session so that it is protected from interception and is reachable and readable only to the real recipient. The key objectives of SSL are served appropriately by its stack-based architecture which comprises a set of protocols within the SSL, sharing different responsibilities.

Architecture of Secure Socket Layer

Architecturally, the SSL protocol is designed as a suite of protocols over TCP/IP. The design of the SSL protocol is often described as the "SSL Protocol Stack".

The first layer of the SSL Protocol Stack over TCP/IP is known as the SSL Record Protocol. The SSL Record protocol is responsible for ensuring data security through encryption, and data integrity. The SSL Record protocol also handles checking of data and encapsulating it with appropriate headers for secure transmission under the TCP protocol.

The second layer of the SSL Protocol Stack is positioned above the SSL Record protocol and is responsible for establishing secured connection with an application protocol like HTTP. The protocols at the second and the top layer of the SSL protocol stack include the SSL Handshake Protocol, the SSL Change Cipher protocol and the SSL Alert Protocol.

These three protocols at the top layer of the SSL protocol stack offer session management, cryptographic parameter management and secure transfer of SSL messages between the client and the server.

b) WEP

Wired Equivalent Privacy (WEP) is a security protocol, specified in the IEEE Wireless Fidelity (Wi-Fi) standard, 802.11b, that is designed to provide a wireless local area network (WLAN) with a level of security and privacy comparable to what is usually expected of a wired LAN.

WEP uses the RC4 algorithm to encrypt the packets of information as they are sent out from the access point or wireless network card. As soon as the access point receives the packets sent by the user's network card it decrypts them. Each byte of data will be encrypted using a different packet key.

WEP (Wired Equivalent Privacy) is an encryption algorithm used to secure wireless networks (such as Wi-Fi). It was the first security measure to be implemented for wireless connections after the original IEEE 802.11 standard was created in 1997

Authentication

Two methods of authentication can be used with WEP: Open System authentication and Shared Key authentication. In Open System authentication, the WLAN client does not provide its credentials to the Access Point during authentication. Any client can authenticate with the Access Point and then attempt to associate. In effect, no authentication occurs. Subsequently, WEP keys can be used for encrypting data frames. At this point, the client must have the correct keys.

In Shared Key authentication, the WEP key is used for authentication in a four-step challenge-response handshake:

1. The client sends an authentication request to the Access Point.
2. The Access Point replies with a clear-text challenge.
3. The client encrypts the challenge-text using the configured WEP key and sends it back in another authentication request.
4. The Access Point decrypts the response. If this matches the challenge text, the Access Point sends back a positive reply.

After the authentication and association, the pre-shared WEP key is also used for encrypting the data frames using RC4.

At first glance, it might seem as though Shared Key authentication is more secure than Open System authentication, since the latter offers no real authentication. However, it is quite the reverse. It is possible to derive the keystream used for the handshake by capturing the challenge frames in Shared Key authentication.[12] Therefore, data can be more easily intercepted and decrypted with Shared Key authentication than with Open System authentication. If privacy is a primary concern, it is more advisable to use Open System authentication for WEP authentication, rather than Shared Key authentication; however, this also means that any WLAN client can connect to the AP. (Both authentication mechanisms are weak; Shared Key WEP is deprecated in favor of WPA/WPA2.)

2072 CHAITRA

1. Compare OSI layer with TCP/IP Layer? Explain in which level of OSI layer following tasks are done.

1. Error detection and correction : Data link layer
2. Encryption and decryption of data : Presentation
3. Logical identification of computer : Network layer
4. Point-to-point connection of socket : Transport layer
5. Dialogue control : Session layer
6. Physical identification of computer :Physical layer

Comparison Chart

BASIS FOR COMPARISON	TCP/IP MODEL	OSI MODEL
Expands To	TCP/IP- Transmission Control Protocol/ Internet Protocol	OSI- Open system Interconnect
Meaning	It is a client server model used for transmission of data over the internet.	It is a theoretical model which is used for computing system.
No. Of Layers	4 Layers	7 Layers
Developed by	Department of Defense (DoD)	ISO (International Standard Organization)
Tangible	Yes	No
Usage	Mostly used	Never used

2. Explain five instances of how network are a part of your life today. Through we have MAC address. Why do we use IP address to represent the host in network? Explain your answer

Solution: Networking allows us to meet like-minded individuals who have a mutual desire to give value to the other person. Networking can happen in the workplace, at school, at the gym or at a networking event. According to the Faced Squared article written by greatbusinessschools.org, “People who got the most results from their networking efforts participate more in "face-to-face" casual contact networks." Of that 72% of those surveyed said they were influenced by looks and handshakes alone.

Here are three reasons why networking is important in your everyday life.

Career Development: Networking is an essential part of career development. Whether you are starting your own business or looking to expand on your career, networking is a gateway to building strong relationships for long term success. According to Forbes,” Around 80% of jobs are not posted online. This is referred to as the “hidden jobs market”. Those who find jobs in this hidden market are individuals who effectively network with other people”

Opportunities: Networking in itself produces a great deal of opportunities. When you network with people and start building connections, those connections also connect you with their connections. The opportunities are endless, from finding a new job, client leads, partnerships and more.

Personal Growth: Networking can help you in not only your business ventures but your personal life as well. You gain skills on how to network, build confidence and obtain a different perspective on your career path. Networking is also a great way to build lifelong friendships!

Networking is not just something people do, its a lifestyle and those that are most successful have adapted to and mastered this lifestyle. Great networks don't grow on trees; you must initiate, build and nourish them to have long lasting relationships.

Mac address cannot be changed. These address are assigned only during the manufacture of hardware. Due to this the network become less secured using it.

3. Briefly explain different types of data link layer framing mechanism. List the features of FDDI.

Solution: Framing can be of two types, fixed sized framing and variable sized framing.

Fixed-sized Framing

Here the size of the frame is fixed and so the frame length acts as delimiter of the frame.

Consequently, it does not require additional boundary bits to identify the start and end of the frame.

Example − ATM cells.

Variable – Sized Framing

Here, the size of each frame to be transmitted may be different. So additional mechanisms are kept to mark the end of one frame and the beginning of the next frame.

It is used in local area networks.

Two ways to define frame delimiters in variable sized framing are −

- Length Field − Here, a length field is used that determines the size of the frame. It is used in Ethernet (IEEE 802.3).
- End Delimiter − Here, a pattern is used as a delimiter to determine the size of frame. It is used in Token Rings. If the pattern occurs in the message, then two approaches are used to avoid the situation −
    - Byte – Stuffing − A byte is stuffed in the message to differentiate from the delimiter. This is also called character-oriented framing.

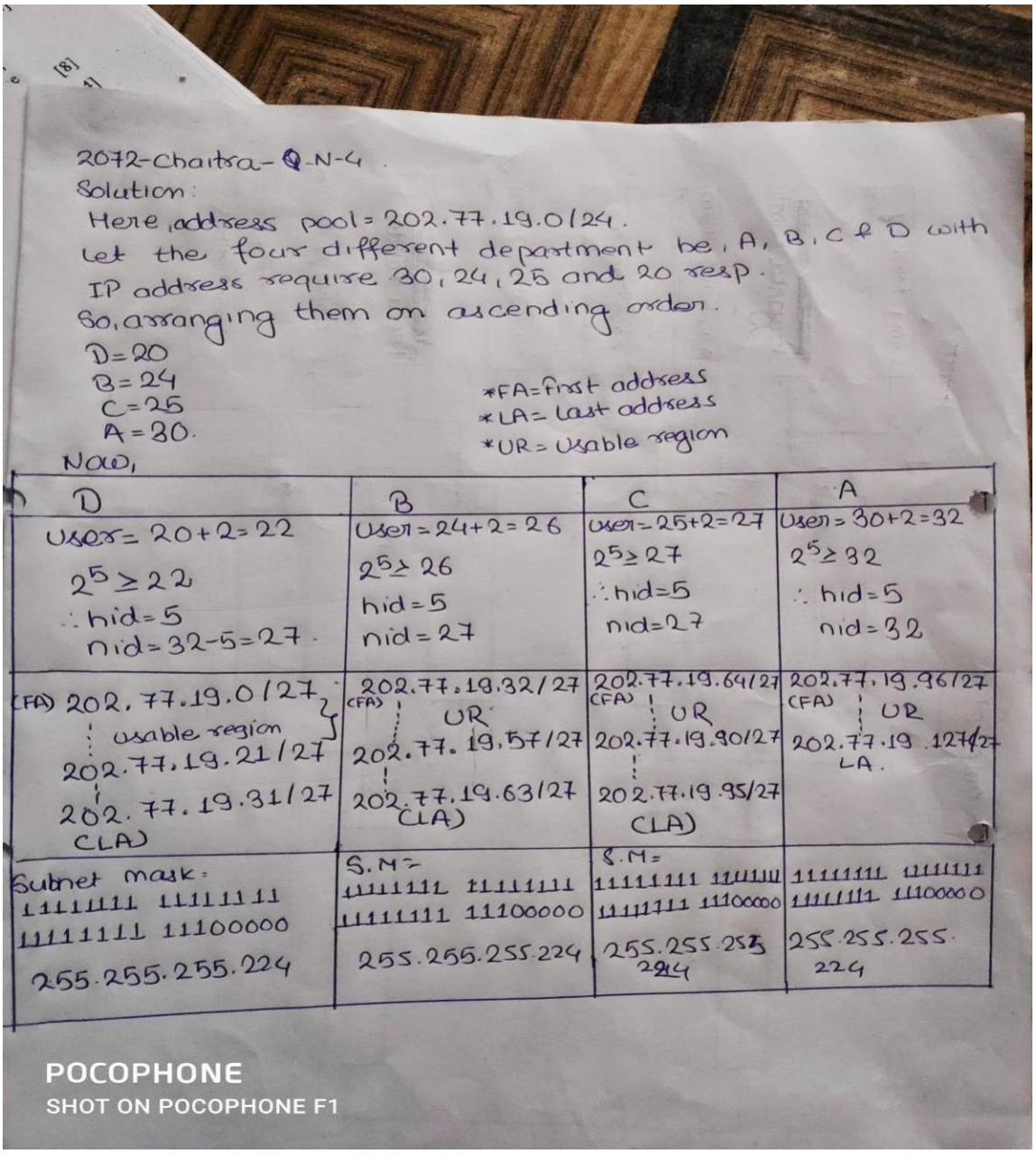
- Bit – Stuffing − A pattern of bits of arbitrary length is stuffed in the message to differentiate from the delimiter. This is also called bit – oriented framing.

FDDI Characteristics:

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

4. Explain how can you allocate 30, 24, 25 and 20 IP address to the four different department of ABC company with minimum wastage. Specify the range of IP address broadcast address,

Network address and subnet mask for each department from given address pool 202.77.19.0/24



2072-Chaitra-Q.N-4

Solution:

Here, address pool = 202.77.19.0/24.

Let the four different department be, A, B, C & D with IP address require 30, 24, 25 and 20 resp.

So, arranging them on ascending order.

D = 20
B = 24
C = 25
A = 30.

*FA = first address
*LA = Last address
*UR = Usable region

Now,

D	B	C	A
User = 20+2 = 22 $2^5 \geq 22$ ∴ hid = 5 nid = 32-5 = 27.	User = 24+2 = 26 $2^5 \geq 26$ hid = 5 nid = 27	User = 25+2 = 27 $2^5 \geq 27$ ∴ hid = 5 nid = 27	User = 30+2 = 32 $2^5 \geq 32$ ∴ hid = 5 nid = 32
(FA) 202.77.19.0/27 usable region 202.77.19.21/27 202.77.19.31/27 (LA)	202.77.19.32/27 (FA) UR 202.77.19.57/27 202.77.19.63/27 (LA)	202.77.19.64/27 (FA) UR 202.77.19.90/27 202.77.19.95/27 (LA)	202.77.19.96/27 (FA) UR 202.77.19.127/27 LA.
Subnet mask: 11111111 11111111 11111111 11100000 255.255.255.224	S.M: 11111111 11111111 11111111 11100000 255.255.255.224	S.M: 11111111 11111111 11111111 11100000 255.255.255.224	11111111 11111111 11111111 11100000 255.255.255.224

POCOPHONE
SHOT ON POCOPHONE F1

5. What is routed and routing protocol? Give example .Explain token bucket algorithm

Solution: A *routed* protocol is a protocol by which data can be routed. Examples of a routed protocol are IP, IPX, and AppleTalk. Required in such a protocol is an addressing scheme. Based on the addressing scheme, you will be able to identify the network to which a host belongs, in addition to identifying that host on that network.

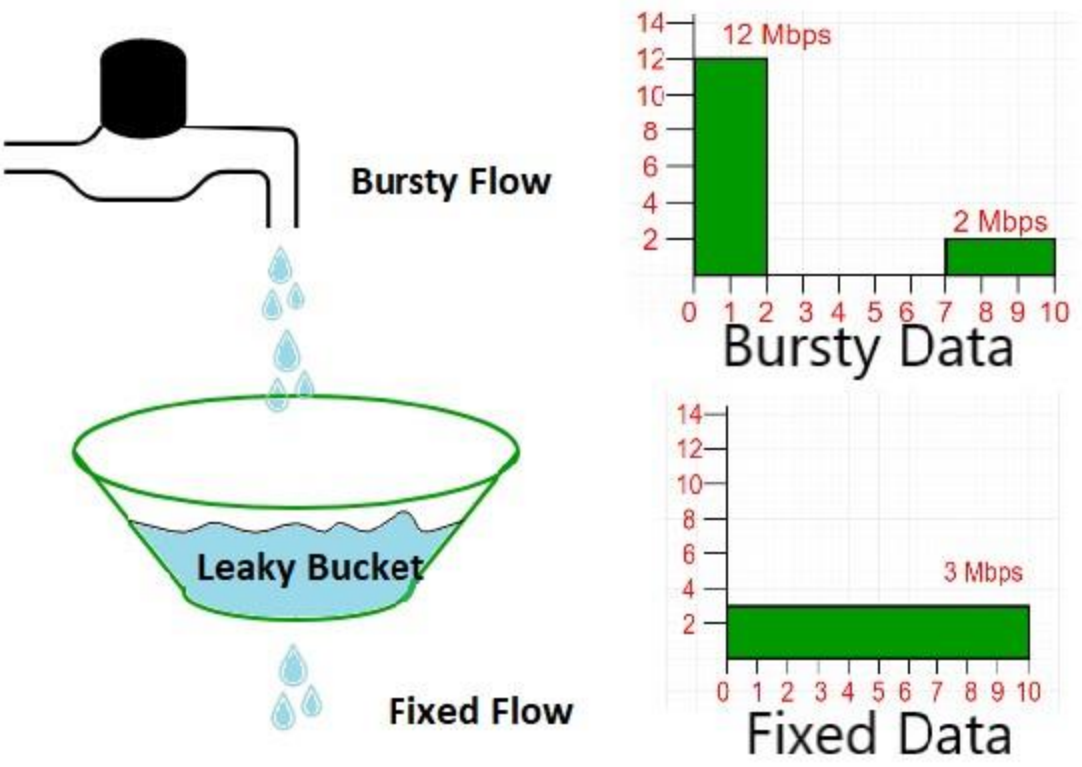
All hosts on an internetwork (routers, servers, and workstations) can utilize the services of a routed protocol.

Routing Protocols

The CCNA objectives only require that you know how to configure RIP and IGRP. However, you do need to know about the three classes of routing protocols (distance vector, link state, and hybrid), and which protocol belongs to which class. OSPF is the only link state protocol with which you need to concern yourself, and EIGRP is the only hybrid protocol. Everything else is belongs to the distance vector category. Know which protocol has a lower administrative distance (RIP is 120 vs. IGRP is 100), and that static routes normally have a lower administrative distance than both (if you use the defaults a static router is 1 and a directly connected router is 0).

The token bucket is an algorithm used in packet switched computer networks and telecommunications networks. It can be used to check that data transmissions, in the form of packets, conform to defined limits on bandwidth and burstiness (a measure of the unevenness or variations in the traffic flow).
The token bucket algorithm can be conceptually understood as follows:

- A token is added to the bucket every seconds.
- The bucket can hold at the most tokens. If a token arrives when the bucket is full, it is discarded.
- When a packet (network layer PDU) of *n* bytes arrives, o if at least *n* tokens are in the bucket, *n* tokens are removed from the bucket, and the packet is sent to the network.
  - o if fewer than *n* tokens are available, no tokens are removed from the bucket, and the packet is considered to be *non-conformant*.



6. For client-server application over TCP, why must the server program be executed before the client program? TCP is known as reliable process how, describe reliability is provided by TCP.

Solution: In a client-server application over TCP (Transmission Control Protocol), the server program must be executed before the client program due to the following reasons: As the TCP is a connection-oriented protocol, a connection must be established between the client and the server before they communicate to each other.

TCP provides for the recovery of segments that get lost, are damaged, duplicated or received out of their correct order. TCP is described as a 'reliable' protocol because it attempts to recover from these errors. ... TCP also requires that an acknowledge message be returned after transmitting data.

7. Compare the header fields of IPV6 and IPV4.Which method do you suggest for the migration of IPV6 and why?

Solution:
IPv6 header is simpler than IPv4 header.
- IPv6 header size is bigger than that of IPv4.

- The source and destination addresses are 32 bit in IPv4 header while 128 bit in IPv6 header.

- IPv4 header is of variable size with minimum of 20 byte in length.

IPv6 header is of fixed size with 40 byte in length IPv6 header is simpler than IPv4 header.
- IPv6 header size is bigger than that of IPv4.

- The source and destination addresses are 32 bit in IPv4 header while 128 bit in IPv6 header.

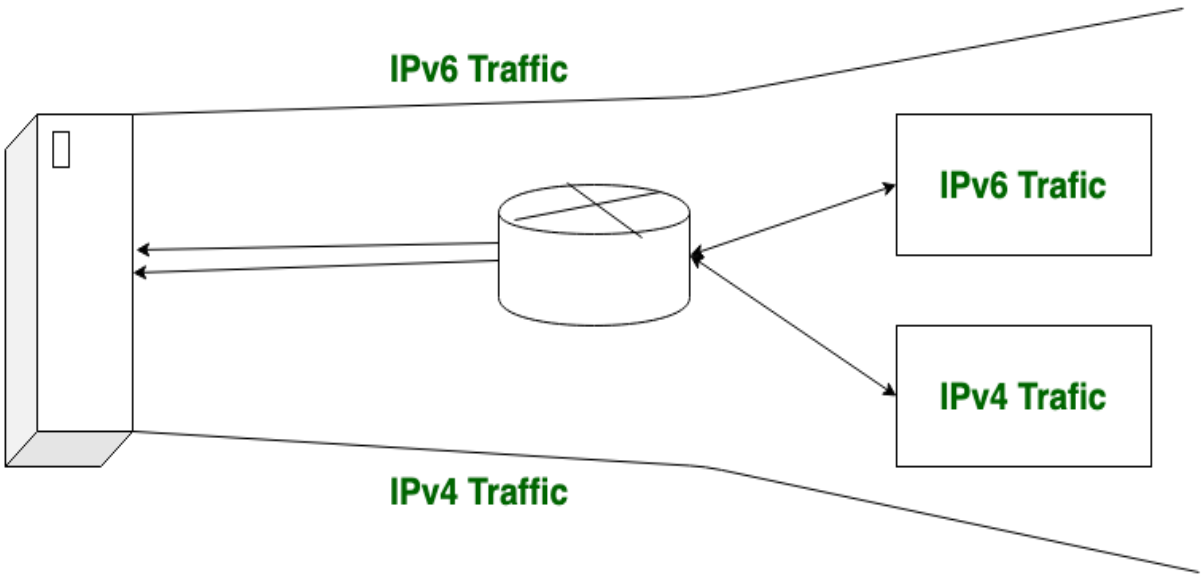
- IPv4 header is of variable size with minimum of 20 byte in length. IPv6 header is of fixed size with 40 byte in length.

Transition from IPv4 to IPv6 address

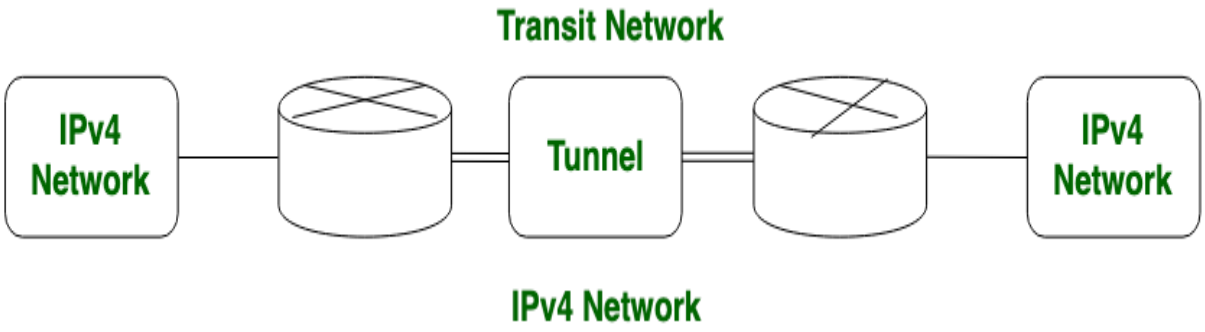
When we want to send a request from an IPv4 address to an IPv6 address but it isn't possible because IPv4 and IPv6 transition is not compatible. For solution to this problem, we use some technologies. These technologies are: *Dual Stack Routers, Tunneling, and NAT Protocol Translation*. These are explained as following below.

Dual Stack Routers:

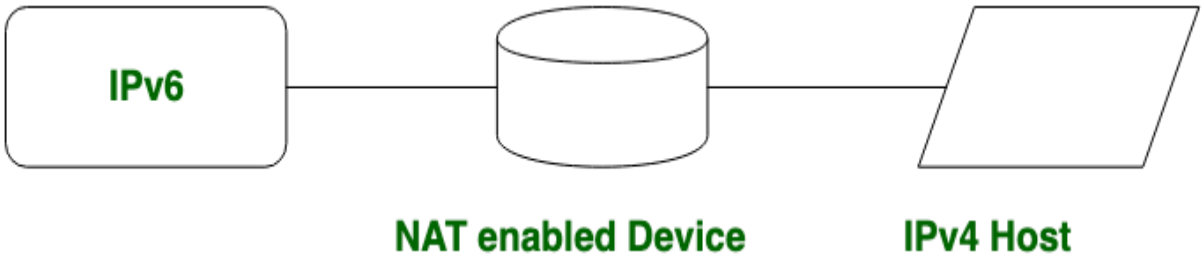
In dual stack router, A router's interface is attached with Ipv4 and IPv6 addresses configured is used in order to transition from IPv4 to IPv6.



In this above diagram, a given server with both IPv4 and IPv6 address configured can communicate with all hosts of IPv4 and IPv6 via dual stack router (DSR). The dual stack router (DSR) gives the path for all the hosts to communicate with server without changing their IP addresses.
Tunneling:
Tunneling is used as a medium to communicate the transit network with the different ip versions.



In this above diagram, the different IP versions such as IPv4 and IPv6 are present. The IPv4 networks can communicate with the transit or intermediate network on IPv6 with the help of Tunnel. It's also possible that the IPv6 network can also communicate with IPv4 networks with the help of Tunnel.
NAT Protocol Translation: By the help of NAT Protocol Translation technique, the IPv4 and IPv6 networks can also communicate with each other which do not understand the address of different IP version. Generally, an IP version doesn't understand the address of different IP version, for the solution of this problem we use NAT-PT device which remove the header of first (sender) IP version address and add the second (receiver) IP version address so that the Receiver IP version address understand that the request is send by the same IP version, and its vice-versa is also possible.



In above diagram, an IPv4 address communicate with the IPv6 address via NAT-PT device to communicate easily. In this situation IPv6 address understand that the request is send by the same IP version (IPv6) and it respond.

8. Explain briefly how firewalls protect network and also explain different types of firewall. Illustrate your answer with appropriate figure.

Solution:

Security is a topic on the minds of most everyone these days so understanding how to best protect your network is naturally a priority. Firewalls are designed as a barricade to keep out untrustworthy entities and traffic. A firewall can be a software or hardware based system that serves as a round the clock traffic cop, prohibiting any traffic that you don't want inside your network. You define the traffic to be permitted into your network. Anything else simply has no access.

A firewall is designed to protect computers from threats. Software-based firewalls are typically part of the operating system or a component of Anti-virus software. It is designed to block some applications that are seen as a potential threat to the user while allowing other approved applications unvented access.

Hardware-based firewalls serve as a physical blockade between the internet and the internal network. A true business-grade firewall should have the following services available to help prevent against malware, ransomware, and viruses: Anti-virus Gateway, Intrusion Prevention, Application Control, Web Reputation, Web Blocker, Spam Blocker, Network Discovery, Data Loss Prevention, and/or Advanced Threat Protection.

Because businesses work with large volumes of sensitive data over their networks, a businessgrade firewall is a must. Intrusion into your network leaves your critical business data available to outsiders/hackers. According to a study completed by the Computer Security Institute (CSI) in conjunction with the FBI, 52% of companies reported system penetration from external sources.

Types of Firewall

Firewall types can be divided into several different categories based on their general structure and method of operation. Here are eight types of firewalls:

Packet-filtering firewalls

Circuit-level gateways

Stateful inspection firewalls

Application-level gateways (a.k.a. proxy firewalls)

Next-gen firewalls

Software firewalls

Hardware firewalls

Cloud firewalls

Packet-Filtering Firewalls

As the most “basic” and oldest type of firewall architecture, packet-filtering firewalls basically create a checkpoint at a traffic router or switch. The firewall performs a simple check of the data packets coming through the router—inspecting information such as the destination and origination IP address, packet type, port number, and other surface-level information without opening up the packet to inspect its contents.

If the information packet doesn’t pass the inspection, it is dropped.

The good thing about these firewalls is that they aren’t very resource-intensive. This means they don’t have a huge impact on system performance and are relatively simple. However, they’re also relatively easy to bypass compared to firewalls with more robust inspection capabilities.

Circuit-Level Gateways

As another simplistic firewall type that is meant to quickly and easily approve or deny traffic without consuming significant computing resources, circuit-level gateways work by verifying the transmission control protocol (TCP) handshake. This TCP handshake check is designed to make sure that the session the packet is from is legitimate.

While extremely resource-efficient, these firewalls do not check the packet itself. So, if a packet held malware, but had the right TCP handshake, it would pass right through. This is why circuitlevel gateways are not enough to protect your business by themselves.

Stateful Inspection Firewalls

These firewalls combine both packet inspection technology and TCP handshake verification to create a level of protection greater than either of the previous two architectures could provide alone.

However, these firewalls do put more of a strain on computing resources as well. This may slow down the transfer of legitimate packets compared to the other solutions.

Proxy Firewalls (Application-Level Gateways/Cloud Firewalls)

Proxy firewalls operate at the application layer to filter incoming traffic between your network and the traffic source—hence, the name "application-level gateway." These firewalls are delivered via a cloud-based solution or another proxy device. Rather than letting traffic connect directly, the proxy firewall first establishes a connection to the source of the traffic and inspects the incoming data packet.

This check is similar to the stateful inspection firewall in that it looks at both the packet and at the TCP handshake protocol. However, proxy firewalls may also perform deep-layer packet inspections, checking the actual contents of the information packet to verify that it contains no malware.

Once the check is complete, and the packet is approved to connect to the destination, the proxy sends it off. This creates an extra layer of separation between the "client" (the system where the packet originated) and the individual devices on your network—obscuring them to create additional anonymity and protection for your network.

If there's one drawback to proxy firewalls, it's that they can create significant slowdown because of the extra steps in the data packet transferal process.

Next-Generation Firewalls

Many of the most recently-released firewall products are being touted as "next-generation" architectures. However, there is not as much consensus on what makes a firewall truly next-gen.

Some common features of next-generation firewall architectures include deep-packet inspection (checking the actual contents of the data packet), TCP handshake checks, and surface-level packet inspection. Next-generation firewalls may include other technologies as well, such as intrusion prevention systems (IPSs) that work to automatically stop attacks against your network.

The issue is that there is no one definition of a next-generation firewall, so it's important to verify what specific capabilities such firewalls have before investing in one.

Software Firewalls

Software firewalls include any type of firewall that is installed on a local device rather than a separate piece of hardware (or a cloud server). The big benefit of a

software firewall is that it's highly useful for creating defense in depth by isolating individual network endpoints from one another.

However, maintaining individual software firewalls on different devices can be difficult and timeconsuming. Furthermore, not every device on a network may be compatible with a single software firewall, which may mean having to use several different software firewalls to cover every asset.

Hardware Firewalls

Hardware firewalls use a physical appliance that acts in a manner similar to a traffic router to intercept data packets and traffic requests before they're connected to the network's servers. Physical appliance-based firewalls like this excel at perimeter security by making sure malicious traffic from outside the network is intercepted before the company's network endpoints are exposed to risk.

The major weakness of a hardware-based firewall, however, is that it is often easy for insider attacks to bypass them. Also, the actual capabilities of a hardware firewall may vary depending on the manufacturer—some may have a more limited capacity to handle simultaneous connections than others, for example.

Cloud Firewalls

Whenever a cloud solution is used to deliver a firewall, it can be called a cloud firewall, or firewallas-a-service (FaaS). Cloud firewalls are considered synonymous with proxy firewalls by many, since a cloud server is often used in a proxy firewall setup (though the proxy doesn't necessarily *have* to be on the cloud, it frequently is).

The big benefit of having cloud-based firewalls is that they are very easy to scale with your organization. As your needs grow, you can add additional capacity to the cloud server to filter larger traffic loads. Cloud firewalls, like hardware firewalls, excel at perimeter security.

9. Write down the steps involved in RSA encryption algorithm. Encrypt the word CAT using RSA algorithm, choose the suitable data for encryption by yourself according to RSA algorithm.

Solution:

The RSA algorithm involves four steps: key generation, key distribution, encryption and decryption.

RSA encrypts messages through the following algorithm, which is divided into 3 steps:

1. Key Generation

I. Choose two distinct prime numbers p and q.

II. Find n such that $n = pq$.

n will be used as the modulus for both the public and private keys.

III. Find the totient of n, $\phi(n)$

$\phi(n)=(p-1)(q-1)$.

IV. Choose an e such that $1 < e < \phi(n)$, and such that e and $\phi(n)$ share no divisors other than 1 (e and $\phi(n)$ are relatively prime). e is kept as the public key exponent.

V. Determine d (using modular arithmetic) which satisfies the congruence relation

$de \equiv 1 \pmod{\phi(n)}$.

In other words, pick d such that de - 1 can be evenly divided by (p-1)(q-1), the totient, or $\phi(n)$. This is often computed using the Extended Euclidean Algorithm, since e and $\phi(n)$ are relatively prime and d is to be the modular multiplicative inverse of e. d is kept as the private key exponent.

The public key has modulus n and the public (or encryption) exponent e. The private key has modulus n and the private (or decryption) exponent d, which is kept secret.

2. Encryption

I. Person A transmits his/her public key (modulus n and exponent e) to Person B, keeping his/her private key secret.

II. When Person B wishes to send the message "M" to Person A, he first converts M to an integer such that $0 < m < n$ by using agreed upon reversible protocol known as a padding scheme.

III. Person B computes, with Person A's public key information, the cipher text c corresponding to

$c \equiv m^e \pmod{n}$.

IV. Person B now sends message "M" in cipher text, or c, to Person A.

In order to understand how encryption works when implemented we will practice an example using small prime factors. Remember the security in encryption relies not on the algorithm but on the difficulty of deciphering the key. Here is an example using the RSA encryption algorithm.

Using RSA, choose p = 5 and q = 7, encode the phrase “cat”. Apply the decryption algorithm to the encrypted version to recover the original plain text message.
Using the RSA encryption method we get the following
Steps:
1) Choose two prime numbers p = 5 and q = 7

2) Compute n = pq and z = (p – 1)(q – 1) a. n = pq = (5)(7) = 35 b. z = (p – 1)(q – 1) = (5 – 1)(7 – 1) = (4)(6) = 24

3) Choose a number e < n such that it has no common factors with z other than 1 a. Let e = 5

4) Find a number d such that ed divided z has a remainder of 1 a. Using the extended Euclidean algorithm to find the inverse modulo 35 find d = 29

5) The public key becomes K+ B or the number pair (n, e) and the private key becomes KB or the number pair (n, d)

Thus, the encrypted value c of the plain text message m is:
c = m^e mod n
Now, using the alphabet such that the letters are numbered 1 through 26 we get
Plain Text Number: 8 5 12
Encrypted value: 8 10 17
8^&5 mod 35 = 8
5^5 mod 35 = 10
12^5 mod 35 = 17

This gives the encrypted value of the word “cat” as 8 10 17
Where: c →8, a →10, t→17,
In order to decrypt the message c, calculate:
m = c^d

mod n

Thus, we

get:

Encrypted value 8 10 17
Number 8 5 12
Plain Text c a t
This gives the encrypted value of 8 10 17 as the word “cat”
Where: 8 →c, 10→a, 17 → t

Which is the word “cat”. Of course if the message was encrypted using the ASII values of the letters for the plain text, the lower and upper case letters could be differentiated.

10. Write short notes on:

a) Simple Mail Transfer Protocol

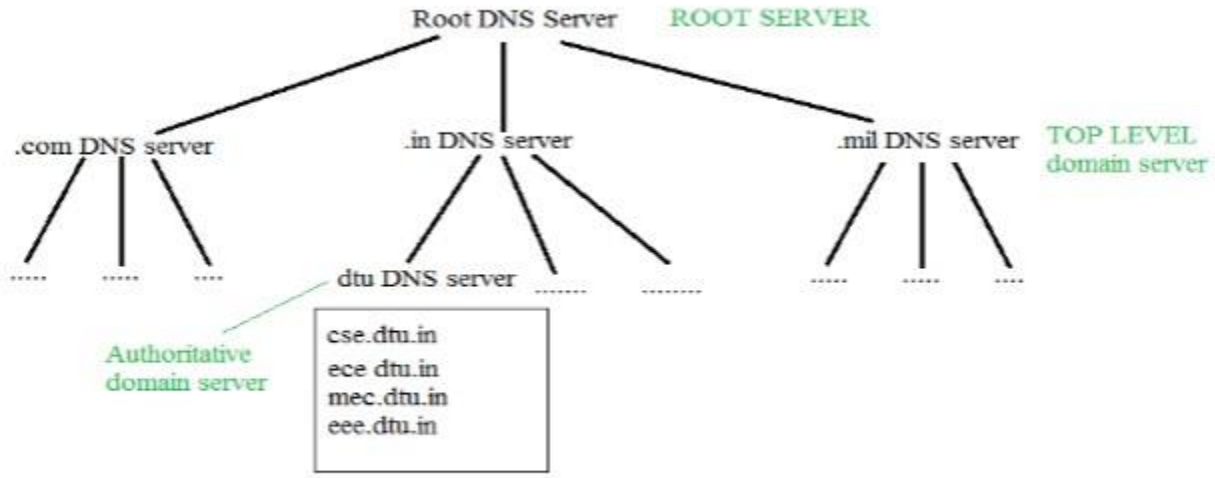
b) Domain Name Server Solution:

Simple Mail Transfer Protocol

SMTP—The Simple Mail Transfer Protocol within the Internet, e-mail is delivered by having the source machine establish a TCP connection to port 25 of the destination machine. Listening to this port is an e-mail daemon that speaks SMTP (Simple Mail Transfer Protocol). This daemon accepts incoming connections and copies messages from them into the appropriate mailboxes. If a message cannot be delivered, an error report containing the first part of the undeliverable message is returned to the sender. SMTP is a simple ASCII protocol. After establishing the TCP connection to port 25, the sending machine, operating as the client, waits for the receiving machine, operating as the server, to talk first. The server starts by sending a line of text giving its identity and telling whether it is prepared to receive mail. If it is not, the client releases the connection and tries again later. If the server is willing to accept e-mail, the client announces whom the e-mail is coming from and whom it is going to. If such a recipient exists at the destination, the server gives the client the go-ahead to send the message. Then the client sends the message and the server acknowledges it. No checksums are needed because TCP provides a reliable byte stream. If there is more e-mail, that is now sent. When all the e-mail has been exchanged in both directions, the connection is released.

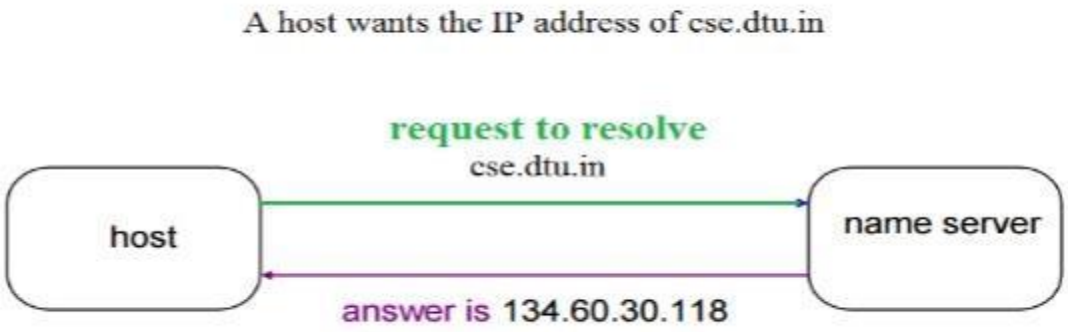
Domain Name Server

DNS is a host name to IP address translation service. DNS is a distributed database implemented in a hierarchy of name servers. It is an application layer protocol for message exchange between clients and servers.
Requirement
Every host is identified by the IP address but remembering numbers is very difficult for the people and also the IP addresses are not static therefore a mapping is required to change the domain name to IP address. So DNS is used to convert the domain name of the websites to their numerical IP address.
Domain:
There are various kinds of DOMAIN:
Generic domain: .com(commercial) .edu(educational) .mil(military) .org(non-profit organization) .net(similar to commercial) all these are generic domain.
Country domain .in (india) .us .uk
Inverse domain if we want to know what is the domain name of the website. Ip to domain name mapping. So DNS can provide both the mapping for example to find the ip addresses of geeksforgeeks.org then we have to type ns lookup www.geeksforgeeks.org.
Organization of Domain



It is Very difficult to find out the ip address associated to a website because there are millions of websites and with all those websites we should be able to generate the ip address immediately, there should not be a lot of delay for that to happen organization of database is very important. DNS record – Domain name, ip address what is the validity?? what is the time to live ?? and all the information related to that domain name. These records are stored in tree like structure.
Namespace – Set of possible names, flat or hierarchical . Naming system maintains a collection of bindings of names to values – given a name, a resolution mechanism returns the corresponding value –
Name server – It is an implementation of the resolution mechanism.. DNS (Domain Name System)
= Name service in Internet – Zone is an administrative unit, domain is a subtree.

Name to Address Resolution



The host request the DNS name server to resolve the domain name. And the name server returns the IP address corresponding to that domain name to the host so that the host can future connect to that IP address.

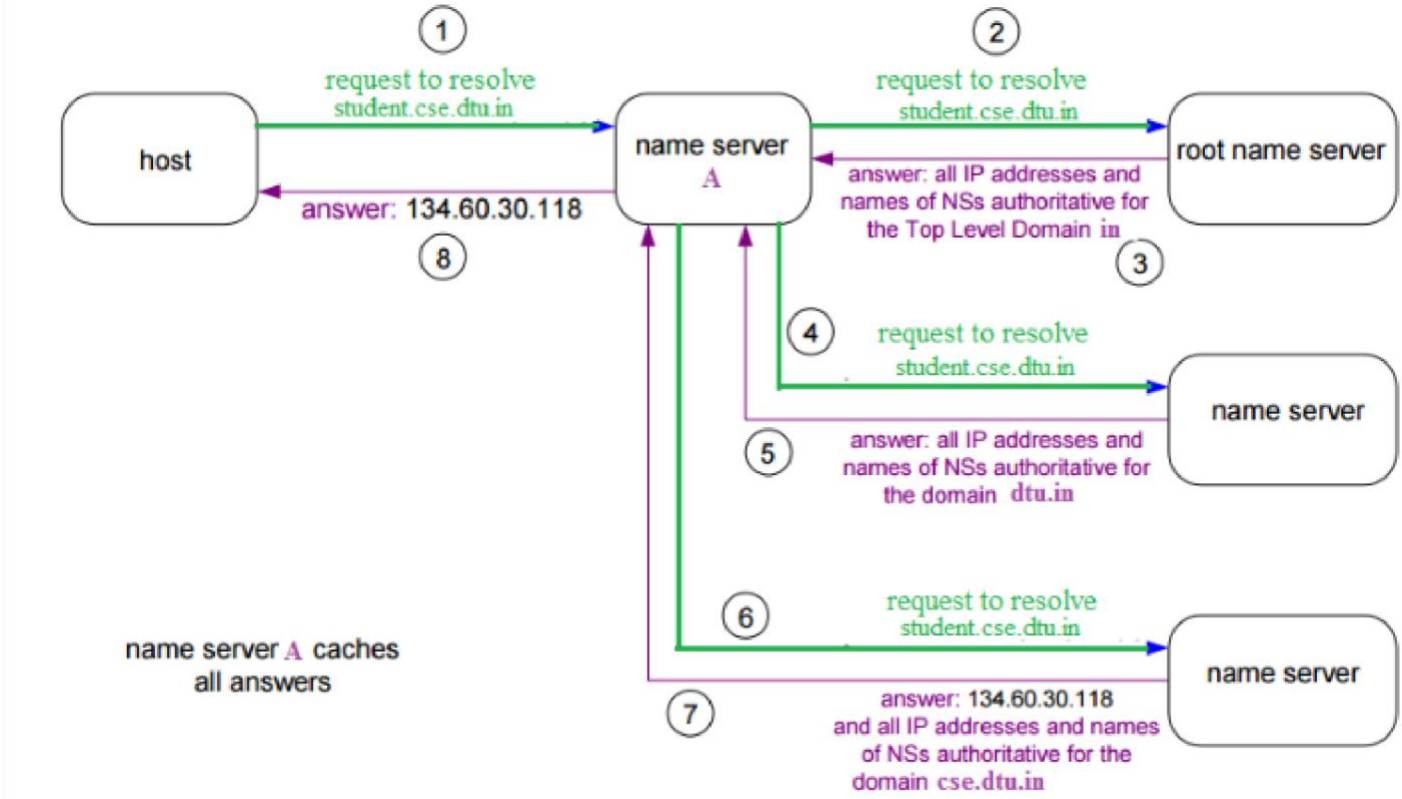
Hierarchy of Name Servers

Root name servers – It is contacted by name servers that can not resolve the name. It contacts authoritative name server if name mapping is not known. It then gets the mapping and return the IP address to the host.

Top level server – It is responsible for com, org, edu etc and all top level country domains like uk, fr, ca, in etc. They have info about authoritative domain servers and know names and IP addresses of each authoritative name server for the second level domains.

Authoritative name servers This is organization's DNS server, providing authoritative hostName to IP mapping for organization servers. It can be maintained by organization or service provider. In order to reach cse.dtu.in we have to ask the root DNS server, then it will point out to the top level domain server and then to authoritative domain name server which actually contains the IP address. So the authoritative domain server will return the associative ip address.

Domain Name Server



The client machine sends a request to the local name server, which, if root does not find the address in its database, sends a request to the root name server, which in turn, will route the query to an intermediate or authoritative name server. The root name server can also contain some hostName to IP address mappings. The intermediate name server always knows who the authoritative name server is. So finally the IP address is returned to the local name server which in turn returns the IP address to the host.

2072 KARTIK

1. You are assigned to design a network infrastructure for a 3 star-hotel. Recommend a network solution with hardware and software in current trend that can be used in the hotel. Make necessary assumptions and justify your recommendation with logical arguments where possible.

Solution:

A network must be able to meet certain criteria, these are mentioned below:

1. Performance
2. Reliability
3. Scalability

Performance

It can be measured in following ways:

- Transit time: It is the time taken to travel a message from one device to another.
- Response time: It is defined as the time elapsed between enquiry and response.

Other ways to measure performance are:

1. Efficiency of software
2. Number of users
3. Capability of connected hardware

Reliability

It decides the frequency at which network failure takes place. More the failure are, less is the network reliability.

Security

It refers to the protection of data from the unauthorized user or access. While travelling through network, data passes many layers of network, and data can be traced if attempted. Hence security is also a very important characteristic for Networks.

Properties of Good Network

- Interpersonal Communication: We can communicate with each other efficiently and easily example emails, chat rooms, video conferencing etc.
- Resources can be shared: We can use the resources provided by network such as printers etc.
- Sharing files, data: Authorized users are allowed to share the files on the network.

Components of a Network

A computer network comprises the following components:

- A minimum of at least 2 computers.
- Cables that connect the computer to each other's, although wireless communication is becoming more common.
- A network device on each computer (this is called a network interface card or NIC).
- A 'Switch' used to switch the data from one point to another. Hubs are outdated and are little used for new installations.
- Network operating system software

2. List out the functions of physical layer in TCP/IP reference model. Explain different types of transmission media.

Solution:

Physical layer is the lowest layer of the OSI reference model. It is responsible for sending bits from one computer to another. This layer is not concerned with the meaning of the bits and deals with the setup of physical connection to the network and with transmission and reception of signals.

Functions of Physical Layer

Following are the various functions performed by the Physical layer of the OSI model.

Representation of Bits: Data in this layer consists of stream of bits. The bits must be encoded into signals for transmission. It defines the type of encoding i.e. how 0's and 1's are changed to signal.

Data Rate: This layer defines the rate of transmission which is the number of bits per second.

Synchronization: It deals with the synchronization of the transmitter and receiver. The sender and receiver are synchronized at bit level.

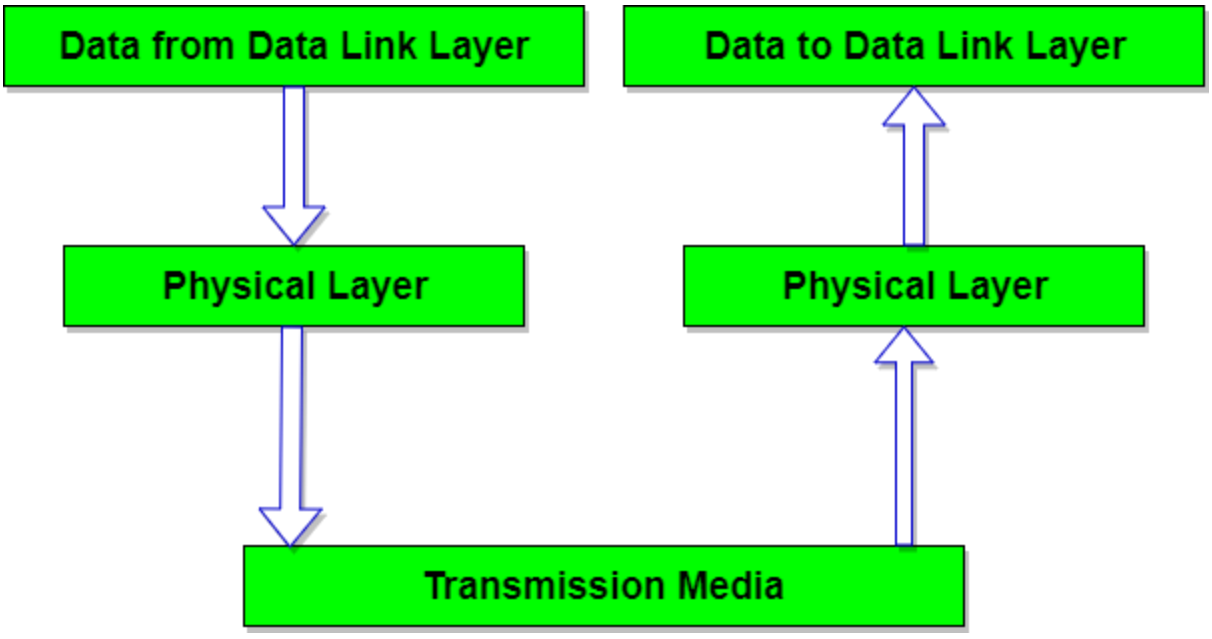
Interface: The physical layer defines the transmission interface between devices and transmission medium.

Line Configuration: This layer connects devices with the medium: Point to Point configuration and Multipoint configuration.

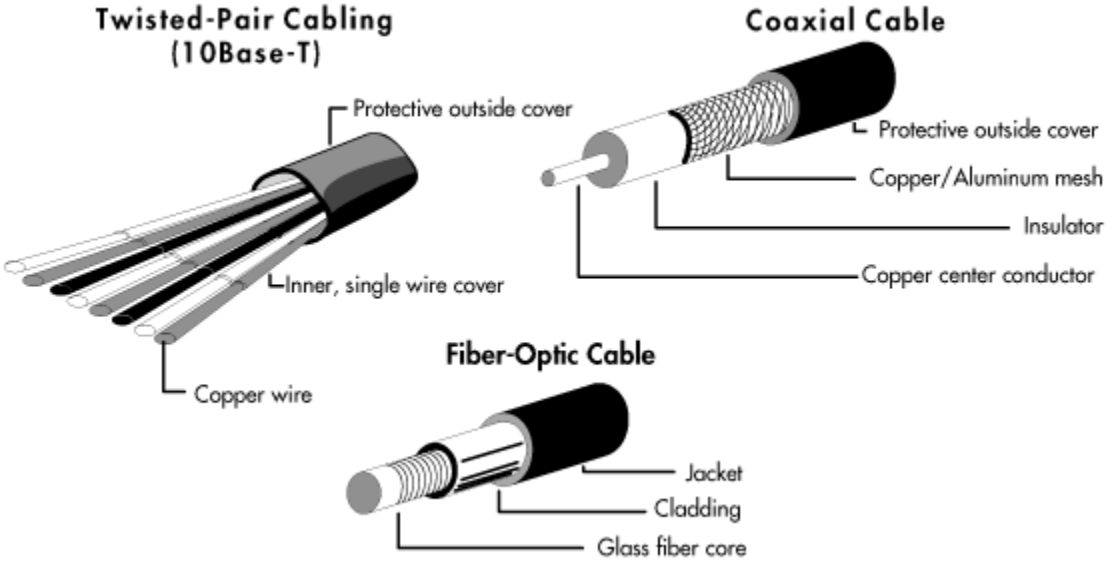
Topologies: Devices must be connected using the following topologies: Mesh, Star, Ring and Bus.

Transmission Modes: Physical Layer defines the direction of transmission between two devices: Simplex, Half Duplex and Full Duplex.

Deals with baseband and broadband transmission.



The different types of transmission media are as follows.



Copper Cable

Well, the copper cable has not much to do with the computer networks, but it is necessary to understand that it is also a significant and a bit traditional type for transmitting data. It is further divided into the twisted pair cable and coaxial paired cable. It is mostly used in telephone lines and as a TV cable. A copper cable is easy to install and less costly and easy to install, but it is not ideal for computer networks, due to its low spectrum and incompatibility with the advance applications like virtual reality and immersion technology.

Wireless Medium

Wireless medium is a more efficient medium. It transmits data through the propagation of electromagnetic waves in the air. In the modern times, wireless media is more common in use. Deployment of a broadcast medium is less expensive and more efficient in the area where implementation of fiber optics or copper cable is a bit complicated. But, there is a drawback, as the signals are spread in the air, in a wireless medium, they are more likely to face interruptions by the obstacles, resulting in lowering of the speed.

Fiber Optics

A Fiber optics cable is the most effective transmission medium in the computer networks. As the name indicates, the cable utilizes the glass fiber for transmission of data. It is also effective against refraction due to a double coating that minimizes the chances of data loss and supports the considerable bandwidth. Well, there are two drawbacks of this medium- First, it is costly than other options and a bit tricky to deploy due to the requirement of expertise and specialized equipment for the process.

3. What are the functions of data link layer? Explain the channel allocation problem with example.

Solution:

Functions of Data Link Layer

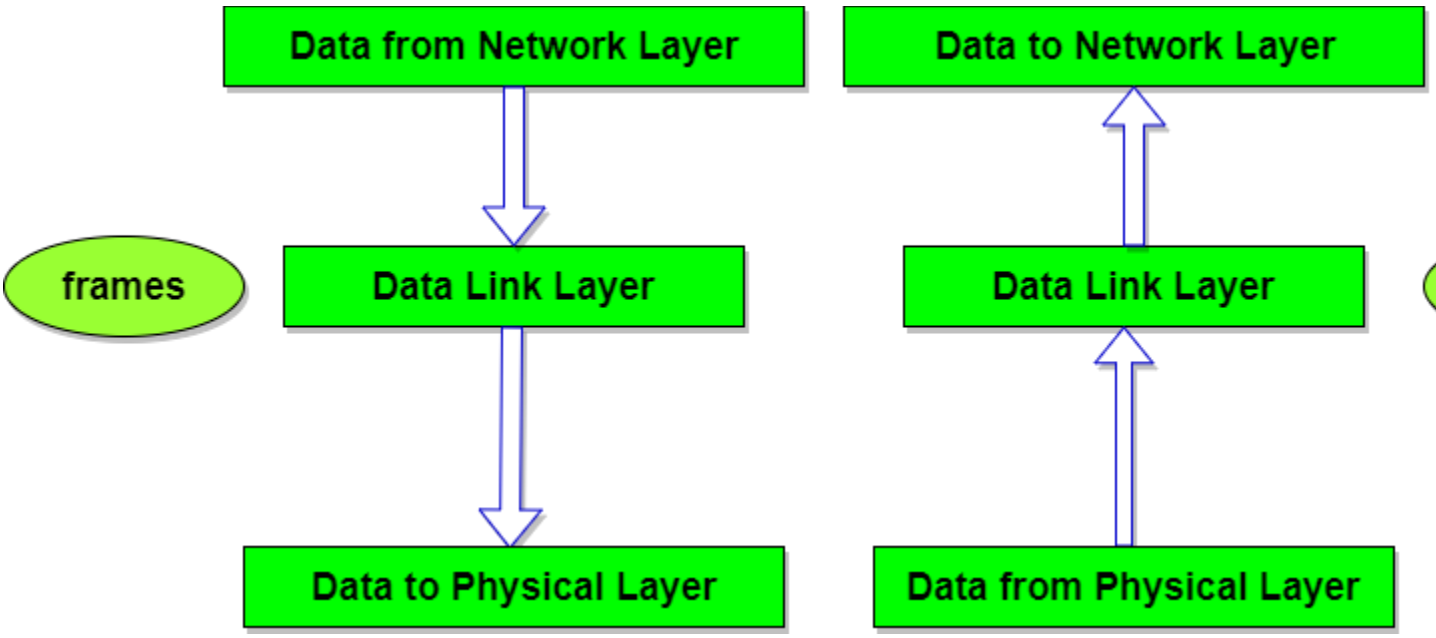
Framing: Frames are the streams of bits received from the network layer into manageable data units. This division of stream of bits is done by Data Link Layer.

Physical Addressing: The Data Link layer adds a header to the frame in order to define physical address of the sender or receiver of the frame, if the frames are to be distributed to different systems on the network.

Flow Control: A flow control mechanism to avoid a fast transmitter from running a slow receiver by buffering the extra bit is provided by flow control. This prevents traffic jam at the receiver side.

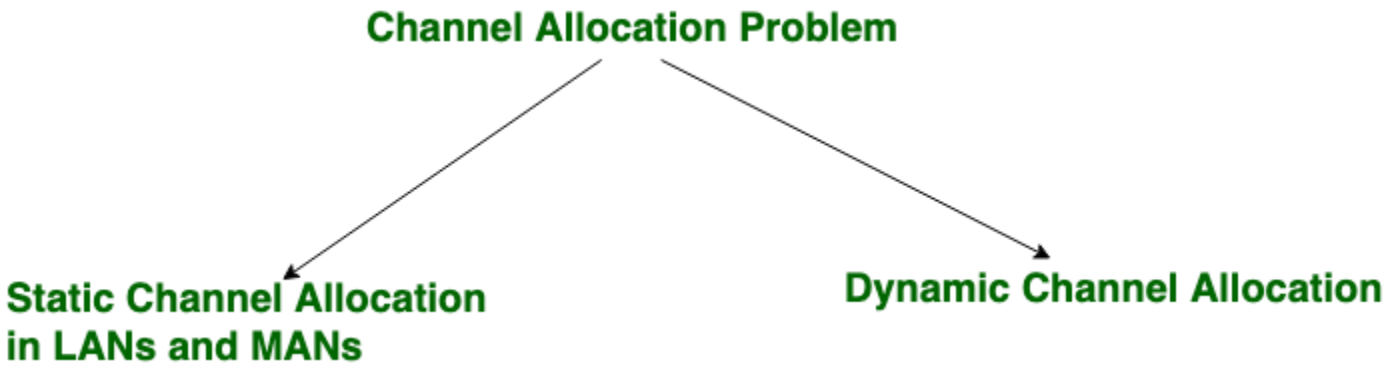
Error Control: Error control is achieved by adding a trailer at the end of the frame. Duplication of frames are also prevented by using this mechanism. Data Link Layers adds mechanism to prevent duplication of frames.

Access Control: Protocols of this layer determine which of the devices has control over the link at any given time, when two or more devices are connected to the same link.



Channel Allocation Problem

Channel allocation is a process in which a single channel is divided and allotted to multiple users in order to carry user specific tasks. There are user's quantity may vary every time the process takes place. If there are N number of users and channel is divided into N equal-sized sub channels, Each user is assigned one portion. If the number of users are small and don't vary at times, than Frequency Division Multiplexing can be used as it is a simple and efficient channel bandwidth allocating technique.
Channel allocation problem can be solved by two schemes: Static Channel Allocation in LANs and MANs, and Dynamic Channel Allocation.



These are explained as following below.

1. Static Channel Allocation in LANs and MANs:
It is the classical or traditional approach of allocating a single channel among multiple competing users Frequency Division Multiplexing (FDM). If there are N users, the bandwidth is divided into N equal sized portions each user being assigned one portion. Since each user has a private frequency band, there is no interface between users.
It is not efficient to divide into fixed number of chunks.

$$T = 1/(U*C-L)$$

$$T(FDM) = N*T(1/U(C/N)-L/N)$$

Where,

T = mean time delay,
C = capacity of channel,
L = arrival rate of frames,
1/U = bits/frame,
N = number of sub channels,
T(FDM) = Frequency Division Multiplexing Time

2.Dynamic Channel Allocation:
Possible assumptions include:

Station Model:
Assumes that each of N stations independently produce frames. The probability of producing a packet in the interval IDt where I is the constant arrival rate of new frames.
Single Channel Assumption:
In this allocation all stations are equivalent and can send and receive on that channel.
Collision Assumption:
If two frames overlap in time-wise, then that's collision. Any collision is an error, and both frames must re-transmitted. Collisions are only possible error.

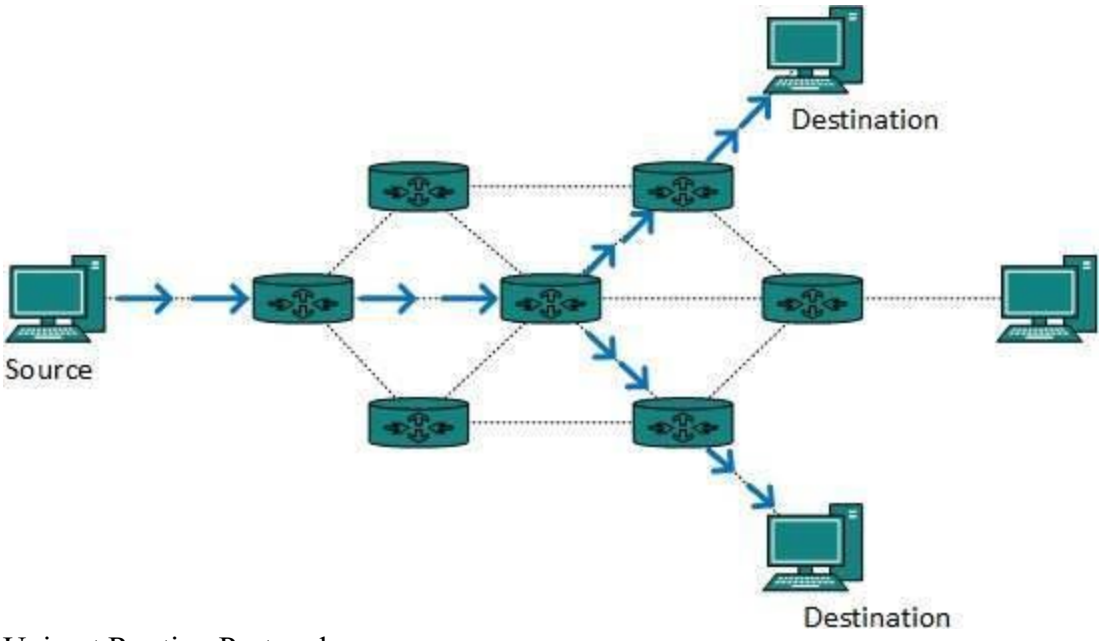
1. Time can be divided into Slotted or Continuous.
2. Stations can sense a channel is busy before they try it.

Protocol Assumption:

- N independent stations.
- A station is blocked until its generated frame is transmitted.
- Probability of a frame being generated in a period of length Dt is IDt where I is the arrival rate of frames.
- Only a single Channel available.
- Time can be either: Continuous or slotted.
- Carrier Sense: A station can sense if a channel is already busy before transmission.
- No Carrier Sense: Time out used to sense loss data.

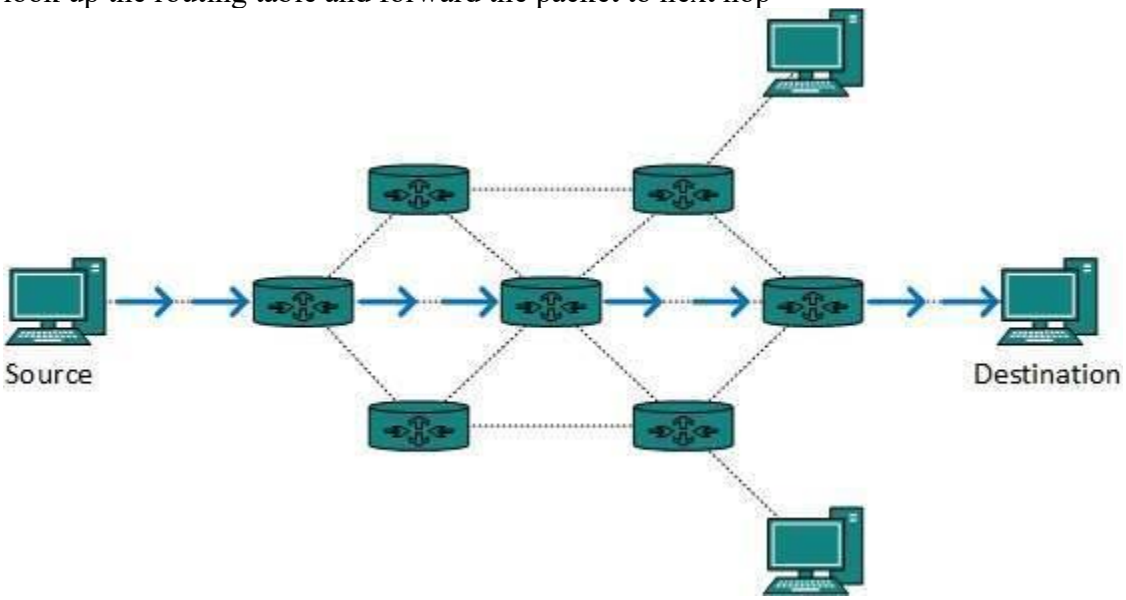
4. What are the functions of network layer? Explain briefly about the multicast routing protocols and unicast routing protocols.

Solution: The main functions of the network layer are:
Routing: When a packet reaches the router's input link, the router will move the packets to the router's output link. For example, a packet from S1 to R1 must be forwarded to the next router on the path to S2.
Logical Addressing: The data link layer implements the physical addressing and network layer implements the logical addressing. Logical addressing is also used to distinguish between source and destination system. The network layer adds a header to the packet which includes the logical addresses of both the sender and the receiver.
Internetworking: This is the main role of the network layer that it provides the logical connection between different types of networks.
Fragmentation: The fragmentation is a process of breaking the packets into the smallest individual data units that travel through different networks.
Multicast Routing Protocols
Multicast routing is special case of broadcast routing with significance difference and challenges. In broadcast routing, packets are sent to all nodes even if they do not want it. But in multicast routing, the data is sent to only nodes which wants to receive the packets. The router must know that there are nodes, which wish to receive multicast packets (or stream) then only it should forward. Multicast routing works spanning tree protocol to avoid looping. Multicast routing also uses reverse path Forwarding technique, to detect and discard duplicates and loops.



Unicast Routing Protocols

Most of the traffic on the internet and intranets known as unicast data or unicast traffic is sent with specified destination. Routing unicast data over the internet is called unicast routing. It is the simplest form of routing because the destination is already known. Hence the router just has to look up the routing table and forward the packet to next hop



5. Network layer is one of the important layers in OSI reference model, why? Differentiate between distance vector routing and static link routing.

Solution: Network layer is a layer 3 that manages device addressing, tracks the location of devices on the network. It determines the best path to move data from source to the destination based on the network conditions, the priority of service, and other factors. The Data link layer is responsible for routing and forwarding the packets. Routers are the layer 3 devices, they are specified in this layer and used to provide the routing services within an internetwork. The protocols used to route the network traffic are known as Network layer protocols. Examples of protocols are IP and Ipv6. So, it is one of the important layer in OSI reference model.

The differences between distance vector routing and static link routing are as follows:

Distance Vector Routing	Link State Routing
--> Bandwidth required is less due to local sharing, small packets and no flooding.	--> Bandwidth required is more due to flooding and sending of large link state packets.
--> Based on local knowledge since it updates table based on information from neighbors.	--> Based on global knowledge i.e. it have knowledge about entire network.
--> Make use of Bellman Ford algo	--> Make use of Dijkastra's algo
--> Traffic is less	--> Traffic is more
--> Converges slowly i.e. good news spread fast and bad news spread slowly.	--> Converges faster.
--> Count to infinity problem.	--> No count to infinity problem.
--> Persistent looping problem i.e. loop will there forever.	--> No persistent loops, only transient loops.
--> Practical implementation is RIP and IGRP.	--> Practical implementation is OSPF and ISIS.

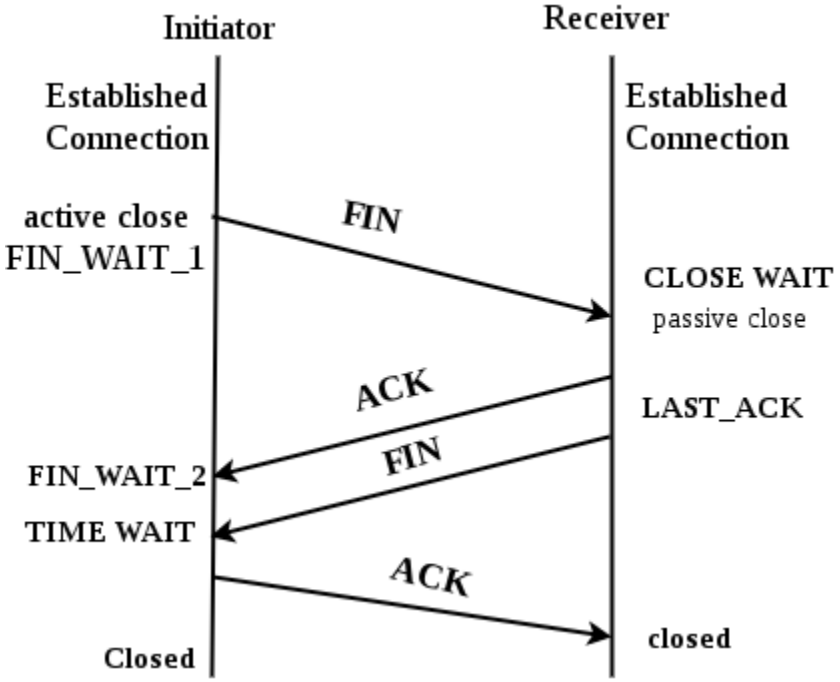
6. What is a TCP connection? Explain how a TCP connection can be gracefully terminated.
Solution: Transmission Control Protocol (TCP) is one of the most important protocols of Internet Protocols suite. It is most widely used protocol for data transmission in communication network such as internet.
There isn't a physical connection from the client to server. Is this connection just the client's socket being linked with the new socket created by the server after the three-way-handshake? Thereafter once the "connection" is set up, the sockets on either ends of the connection then know where to send their packets.

Connection termination in TCP using 3 way handshaking:

1. In a normal situation, the client TCP, after receiving a close command from the client process, sends the first segment, a FIN segment in which the FIN flag is set. Note that a FIN segment can include the last chunk of data sent by the client, or it can be just a control segment. If it is only a control segment, it consumes only one sequence number.
2. The server TCP, after receiving the FIN segment, informs its process of the situation and sends the second segment, a FIN +ACK segment, to confirm the receipt of the FIN segment from the client and at the same time to announce the closing of the connection in the other

direction. This segment can also contain the last chunk of data from the server. If it does not carry data, it consumes only one sequence number.

3. The client TCP sends the last segment, an ACK segment, to confirm the receipt of the FIN segment from the TCP server. This segment contains the acknowledgment number, which is 1 plus the sequence number received in the FIN segment from the server. This segment cannot carry data and consumes no sequence numbers.



7. What are the different components of email server? Explain the different types of electronic mail sending and accessing protocol.

Solution: The different components of email server are:

i. Mail User Agent
ii. Mail Transfer Agent
iii. Mail Host and Mailboxes

The different types of email sending and accessing protocol are:

a. SMTP: SMTP is part of the application layer of the TCP/IP protocol. Using a process called "store and forward," SMTP moves our email on and across networks. It works closely with something called the Mail Transfer Agent (MTA) to send your communication to the right computer and email inbox. SMTP spells out and directs how our email moves from our computer's MTA to an MTA on another computer, and even several computers. Using that "store and forward" feature mentioned before, the message can move in steps from our computer to its destination. At each step, Simple Mail Transfer Protocol is doing its job. Lucky for us, this all takes place behind the scenes, and we don't need to understand or operate SMTP.
b. POP3: POP3, which is an abbreviation for Post Office Protocol 3, is the third version of a widespread method of receiving email. Much like the physical version of a post office

clerk, POP3 receives and holds email for an individual until they pick it up. And, much as the post office does not make copies of the mail it receives, in previous versions of POP3, when an individual downloaded email from the server into their email program, there were no more copies of the email on the server; POP automatically deleted them. POP3 makes it easy for anyone to check their email from any computer in the world, provided they have configured their email program properly to work with the protocol.

c. IMAP: As its name implies, IMAP allows you to access your email messages wherever you are; much of the time, it is accessed via the Internet. Basically, email messages are stored on servers. Whenever you check your inbox, your email client contacts the server to connect you with your messages. When you read an email message using IMAP, you aren't actually downloading or storing it on your computer; instead, you are reading it off of the server. As a result, it's possible to check your email from several different devices without missing a thing. As the world becomes more mobile than ever, IMAP is becoming more and more popular. The proliferation of smartphones, laptops, tablets and other devices is making the demand for IMAP stronger than ever. While POP will remain popular with people who only access their email via one or two devices - and those who have slow connections to the Internet - IMAP is sure to remain the protocol of choice for most of today's busy people.

8. What is IPV6? What methods are used so that IPV6 and IPV4 networks are interoperable?

Solution: Internet Protocol version 6 (IPv6) is the most recent version of the Internet Protocol (IP), the communications protocol that provides an identification and location system for computers on networks and routes traffic across the Internet. IPv6 was developed by the Internet Engineering Task Force (IETF) to deal with the long-anticipated problem of IPv4 address exhaustion. IPv6 is intended to replace IPv4.

9. What is firewall? What are their types? Encrypt and decrypt "OVEL" message using RSA algorithm.

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

The types of firewall are presented below:

i. Packet Filter
ii. Stateful Inspection
iii. Proxy Server Firewall

2072-Kartik

9. Encrypt and decrypt "OVEL" message using RSA algorithm.

i) Let P=3, q=11 (Prime numbers)

ii) $n = P \times q = 33$

iii) Totient, $\phi(n) = (P-1)(q-1) = (3-1) \times (11-1) = 20$

iv) $e = 3$ $(1 < e < \phi(n))$; $\gcd(e, \phi(n)) = 1$

v) $d = \frac{1 + m \times i}{e}$, $i = 0, 1, 2, 3 \ldots$

Also, $de \equiv \text{Mod}\ \phi(n)$

$de \bmod \phi(n) = 1$

$d \times 3 \bmod (20) = 1$

$7 \times 3 \bmod (20) = 1$.

So, $d = 7$.

vi) Public key $(n, e) = (33, 3)$

Private key $(n, d) = (33, 7)$.

Encryption & Decryption is shown below:

Letter	P	P^e	$C = P^e \bmod n$ (Encryption)	d	$P = C^d \bmod n$ (decryption)	Letter
O	15	3375	9	4782696	15	O
V	22	10648	22	2494357888	22	V
E	5	125	26	8031810176	5	E
L	12	1728	12	35831808	12	L

10. Write short notes on:

a) Digital Signature

Digital Signature is a process that guarantees that the contents of a message have not been altered in transit. When you, the server, digitally sign a document, you add a one-way hash (encryption) of the message content using your public and private key pair. Your client can still read it, but the process creates a "signature" that only the server's public key can decrypt. The client, using the server's public key, can then validate the sender as well as the integrity of message contents. Whether it's an email, an online order or a watermarked photograph on eBay, if the transmission arrives but the digital signature does not match the public key in the digital certificate, then the client knows that the message has been altered.

b) IPSec

IPsec (Internet Protocol Security) is a framework that helps us to protect IP traffic on the network layer. IP protocol itself doesn't have any security features at all. IPsec can protect our traffic with the following features:

- Confidentiality: by encrypting our data, nobody except the sender and receiver will be able to read our data.
- Integrity: we want to make sure that nobody changes the data in our packets. By calculating a hash value, the sender and receiver will be able to check if changes have been made to the packet.
- Authentication: the sender and receiver will authenticate each other to make sure that we are really talking with the device we intend to.
- Anti-replay: even if a packet is encrypted and authenticated, an attacker could try to capture these packets and send them again. By using sequence numbers, IPsec will not transmit any duplicate packets.

2073 CHAITRA

1. **What are the reason for using layered protocols? What are headers and trails and how do they get added and removed?**

   The reasons for using layered protocols is because it simplifies the design process as the function of each layers and their interaction are well defined. Some of the reasons are listed below:-

   i. The layered architecture provides flexibility to modify and develop network services.
   ii. Each layer performs different function.
   iii. Redefines the way of convincing networks which leads to cost saving and managerial benefits.
   iv. Addition of new services and management of network infrastructure becomes easy.

   Headers and trailers are the concepts of OSI models. They provide source and destination addresses, synchronization points, information for error detection, etc.
   Headers are the information structure which identifies the information that follows, such as a block of bytes in communication. They are the control data added to the beginning of a data. Headers are added at layer 2,3,4,5, & 6.
   Trailer is the information which occupies several bytes at the end of the block of the data during transmission. They contain error-checking data which is useful for confirming the accuracy and status of the transmission. Trailer is added at layer 2 only.
   At the sending machine, when the message passes through the layers each layers adds the headers or trailers. At the receiving machine, each layers removes the data meant for it and passes the rest to the next layer.

2. Why do you think that static channel assignment is not efficient? Explain about the operation of Carrier Sense Multiple Access with Collision Detection.

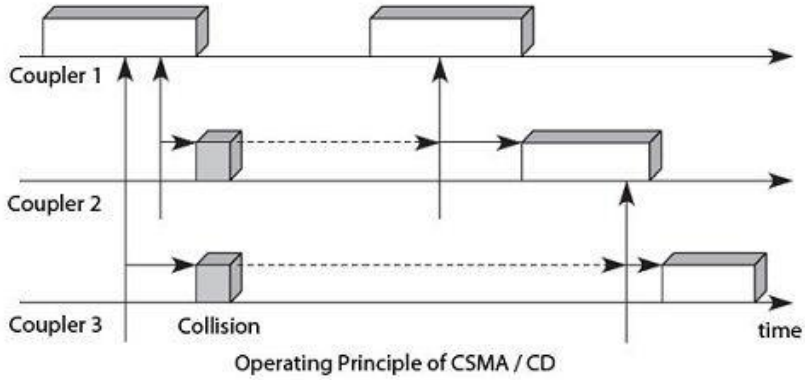
Static channel assignment isn't efficient as in most real-life network situations due to following reasons:

i) There are variable number of users, usually large in number with busty traffic. If the value of N is very large, the bandwidth available for each user will be very less. This will reduce the throughput if the user needs to send a large volume of data once in a while.

ii) Since all of the user are allocated fixed bandwidths, the bandwidth allocated to non-communicating users lies wasted.

iii) If the number of users is more than N, then some of them will be denied service, even if there are unused frequencies.

Operation of Carrier Sense Multiple Access with Collision Detection:
This technique normalized random access by the IEEE 802.3 working group is currently the longer used. At a preliminary listening to the network is added listening during transmission. Coupler to issue a loan that detected free channel transmits and continues to listen the channel. The coupler continues to listen, which is sometimes indicated by the CSMA / CD persistent acronym. If there is a collision, it interrupts its transmission as soon as possible and sends special signals, called padding bits so that all couplers are notified of the collision. He tries again his show later using an algorithm that we present later. Figure shows the CSMA/CD. In this example, the couplers 2 and 3 attempt broadcasting for the coupler 1 transmits its own frame. The couplers 2 and 3 begin to listen and transmit at the same time, the propagation delay around, from the end of the Ethernet frame transmitted by the coupler 1. A collision ensues. Like the couplers 2 and 3 continue to listen to the physical media, they realize the collision, stop their transmission and draw a random time to start retransmission process.



Operating Principle of CSMA / CD

The CS random access because nt transmission. Issuer's with the passing on the line. The collisions are no longer recognized by absence of acknowledgment but by detecting interference. This conflict detection method is relatively simple, but it requires sufficient performance coding techniques to easily recognize a superposition signal. It is generally used for this differential coding technique, such as differential Manchester code.

3. **What is meant by byte stuffing techniques? What is piggy backing? Suppose a bit string, 0111101111101111110 needs to be transmitted at data link layer. What string actually transmitted after the bit stuffing?**

In framing ,a byte is stuffed in the message to differentiate from the delimiter. This is also called byte stuffing technique. That special character is ESC character. ESC character is added just infront of any conflicting character in the data stream.

In two-way communication, wherever a frame is received, the receiver waits and does not send the control frame (acknowledgement or ACK) back to the sender immediately. The receiver waits until its network layer passes in the next data packet. The delayed acknowledgement is then attached to this outgoing data frame. This technique of temporarily delaying the acknowledgement so that it can be hooked with next outgoing data frame is known as piggybacking.

For the input 0111101111101111110 the actual bit transmitted is 011110111110011111010

4. **Why do we think that there arised the need of classless IP address although class based IP address was in used? Show the classless IP with an example.**

Need of classless IP address arised as classfull IP addressing does not provide any flexibility of having less number of hosts per network or more networks per IP class.
Class A with a mask 255.0.0.0 can support 16,777,214 addresses.
Class B with a mask 255.255.0.0 can support 65,534 addresses.
Class C with a mask 255.255.255.0 can support 254 addresses.

But what if someone requires 2000 address? One way to address this situation would be to provide the person with class B network. But that would result in a waste of so many addresses. Another possible way is to provide multiple class C networks, but that too can cause a problem as there would be too many networks to handle. To resolve problems like the one mentioned above CIDR was introduced.

Classless IP example:

In CIDR subnet masks are denoted by /X. For example a subnet of 255.255.255.0 would be denoted by /24. To work a subnet mask in CIDR, we have to first convert each octet into its respective binary value. For example, if the subnet is of 255.255.255.0.

- First octet
  255 has 8 binary 1's when converted to binary.
- Second octet
  255 has 8 binary 1's when converted to binary.
- Third octet
  255 has 8 binary 1's when converted to binary.
- Fourth octet
  0 has 0 binary 1's when converted to binary.

Therefore, in total there are 24 binary 1's, so the subnet mask is /24. While creating a network in CIDR, a person has to make sure that the masks are contagious, i.e. a subnet mask like 10111111.X.X.X can't exist. With CIDR, we can create Variable Length Subnet Masks, leading to less wastage of IP addresses. It is not necessary that the divider between the network and the host portions is at an octet boundary. For example, in CIDR a subnet mask like 255.224.0.0 or 11111111.11100000.00000000.00000000 can exist.

5. Sub netting numerical

For department D (11 host)
D= 11+2=13
2^4 >=13
So , hid=4
Nid=28
1st address=202.70.91.0/24
4th address=202.70.91.3/24
Last address=202.70.91.15/25
Network address is 202.70.91.1
Broadcast address is 202.70.91.0
Subnet mask is 255.255.255.240
For department B(16 host)
B= 16+2=18
2^5 >=18
So , hid=5
Nid=27
1st address=202.70.91.16/24
5th address=202.70.91.20/24
Last address=202.70.91.47/24
Network address is 202.70.91.17
Broadcast address is 202.70.91.16
Subnet mask is 255.255.255.224
For department A(25 host)
B= 25+2=27
2^5 >=27
So , hid=5
Nid=27

1st address=202.70.91.48/24
5th address=202.70.91.52/24
Last address=202.70.91.79/24
Network address is 202.70.91.49
Broadcast address is 202.70.91.48
Subnet mask is 255.255.255.224
For department C(29 host)
B= 29+2=31
2^5 >=31
So , hid=5
Nid=27
1st address=202.70.91.80/24
5th address=202.70.91.84/24
Last address=202.70.91.111/24
Network address is 202.70.91.81
Broadcast address is 202.70.91.80

Subnet mask is 255.255.255.224

6. Explain the difference between TCP and UDP. How congestions can be handled using token bucket? Explain with proper diagram.

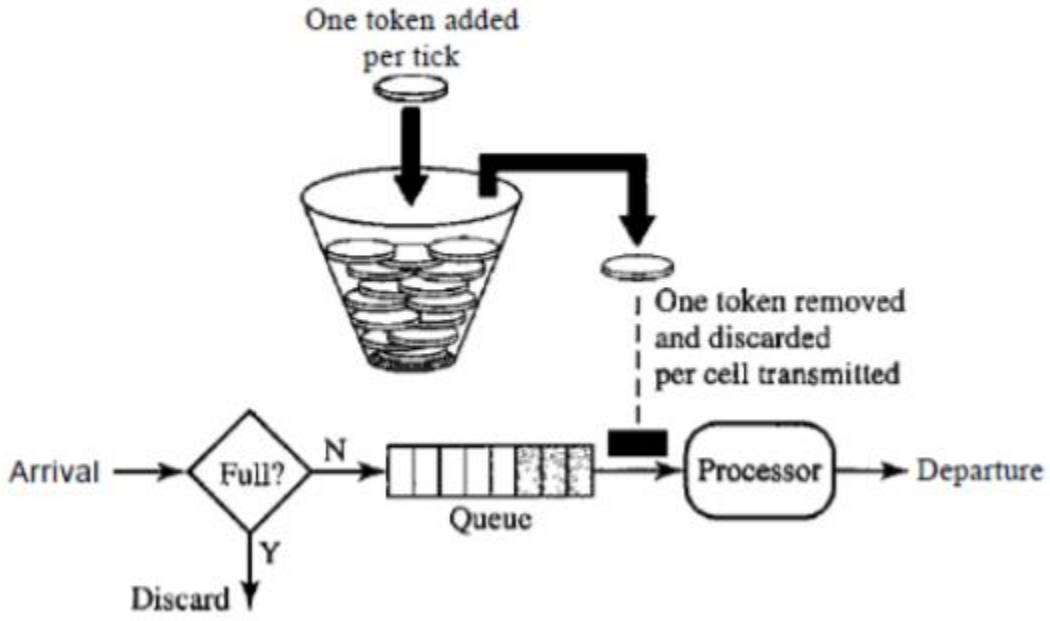
Difference between TCP and UDP is listed below:

S.N	TCP	UDP
1.	TCP is a connection-oriented protocol. Connection-orientation means that the communicating devices should establish a connection before transmitting data and should close the connection after transmitting the data.	UDP is the Datagram oriented protocol. This is because there is no overhead for opening a connection, maintaining a connection, and terminating a connection. UDP is efficient for broadcast and multicast type of network transmission.
2.	TCP is reliable as it guarantees delivery of data to the destination router.	The delivery of data to the destination cannot be guaranteed in UDP.
3.	TCP provides extensive error checking mechanisms. It is because it provides flow control and acknowledgment of data.	UDP has only the basic error checking mechanism using checksums.
4.	Sequencing of data is a feature of Transmission Control Protocol (TCP). this means that packets arrive in-order at the receiver.	There is no sequencing of data in UDP. If ordering is required, it has to be managed by the application layer.
5.	TCP is slower than UPD	UDP is faster, simpler and more efficient than TCP.
6.	TCP has a (20-80) bytes variable length header.	UDP has a 8 bytes fixed length header.
7.	TCP doesn't supports Broadcasting.	UDP supports Broadcasting.
8.	TCP is heavy-weight.	UDP is lightweight.

Congestions handling using token bucket:

Congestion in a network may occur if the load on the network (no. of packet send) is greater that the capacity of the network (no. of packet that can be handle). Congestion control refers to the mechanism and technique to control the congestion and keep the load below the capacity. One of the technique is token bucket which is explained below:

The leaky bucket is very restrictive. It does not credit an idle host. For example, if a host is not sending for a while, its bucket becomes empty. Now if the host has bursty data, the leaky bucket allows only an average rate. The time when the host was idle is not taken into account. On the other hand, the token bucket algorithm allows idle hosts to accumulate credit for the future in the form of tokens. For each tick of the clock, the system sends n tokens to the bucket. The system removes one token for every cell (or byte) of data sent. For example, if n is 100 and the host is idle for 100 ticks, the bucket collects 10,000 tokens. Now the host can consume all these tokens in one tick with 10,000 cells, or the host takes 1000 ticks with 10 cells per tick. In other words, the host can send bursty data as long as the bucket is not empty. Figure 24.21 shows the idea. The token bucket can easily be implemented with a counter. The token is initialized to zero. Each time a token is added, the counter is incremented by 1. Each time a unit of data is sent, the counter is decremented by 1. When the counter is zero, the host cannot send data.



7. **For the client server application over TCP ,why most of server program be executed before the client program? TCP is known as a reliable process describe how reliability is provided by TCP?**

A client-server application run over the TCP, server program is executed first, because the server must accept the request from the client and ready to execute the client's program. If the server is not ready (not running) then the client fails to establish the connection with the server.

TCP is described as a 'reliable' protocol because it attempts to recover from these errors. The sequencing is handled by labling every segment with a sequence number. These sequence numbers permit TCP to detect dropped segments. TCP also requires that an acknowledge message be returned after transmitting data.

TCP provides for the recovery of segments that get lost, are damaged, duplicated or received out of their correct order. TCP is described as a 'reliable' protocol because it attempts to recover from these errors. The sequencing is handled by labling every segment with a sequence number. These sequence numbers permit TCP to detect dropped segments. TCP also requires that an acknowledge message be returned after transmitting data. To verify that the segments are not damaged, a CRC check is performed on every segment that is sent, and every segment that is received. Because every packet has a time to live field, and that field is decremented during each forwarding cycle, TCP must re-calculate the CRC value for the segment at each hop. Segments that do not match the CRC check are discarded.

8. "IPv4 and IPv6 coexist" what does this mean? Explain Dual stack approach with an appropriate figure.

As we know that, IPv6 is not backward compatible with IPv4. Also the time is rapidly approaching when the last of the IPv4 address space will be allocated. We cannot directly replace all IPv4 with IPv6 due to compatible issue. So, there is a concept of coexistence between IPv4 and IPv6. So, the optimal approach for existing network is to focus not on transition but on coexistence. Turn on IPv6 now and start using it and turn off IPv4 off at some point in the future when it is no longer a business requirement. To enable this network administrators should:

- Turn on IPv6 routing in their existing IPv4 network.
- Contract IPv6 service with their upstream, peer, and downstream neighbors.
- Use the IPv6 protocol in addition to IPv4 in their applications and services both on server equipment and on their clients.

The reason to support coexistence of this type should be obvious: If IPv6 isn't working or if another network does not yet support IPv6, the affected applications or services will remain available via IPv4.
Providing coexistence in network layer routing can be accomplished in any one of three ways:

- Enabling IPv6 on routers that carry IPv4.
- Enabling IPv6 on other routers as a parallel network internal to the customer-perceived network.
- Enabling IPv6 on a separate parallel network directly visible to neighboring networks and customers.

Dual Stack Approach for transition from IPv4 to IPv6
The term dual-stack normally refers to a complete duplication of all levels in the protocol stack from applications to the network layer. An example of complete duplication is the OSI and TCP/IP protocols that run on the same system. However, in the context of IPv6 transition, dual-stack means a protocol stack that contains both IPv4 and IPv6. The remainder of the stack is identical. Consequently, the same transport protocols, TCP, UDP, and so on, can run over both IPv4 and IPv6. Also, the same applications can run over both IPv4 and IPv6. It is recommended that all hosts, before migrating completely to version 6, have a dual stack of protocols. In other words, a station must run IPv4 and IPv6 simultaneously until all the Internet uses IPv6.
To determine which version to use when sending a packet to a destination, the source host queries the DNS. If the DNS returns an IPv4 address, the source host sends an IPv4 packet. If the DNS returns an IPv6 address, the source host sends an IPv6 packet. In the dual-stack method, subsets of both hosts and routers are upgraded to support IPv6, in addition to IPv4. The dual-stack approach ensures that the upgraded nodes can always interoperate with IPv4-only nodes by using IPv4.

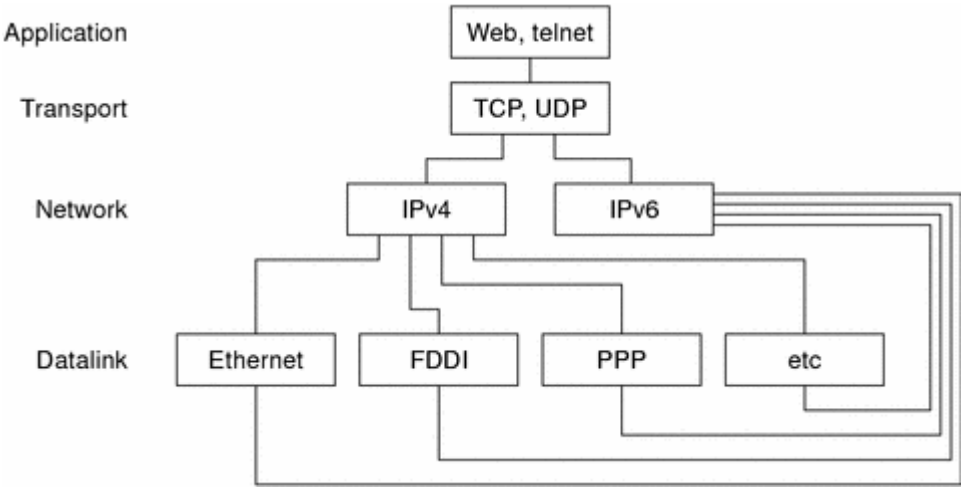


Figure:- Dual Stack Protocal

9. What are the attributes of information security? Explain the RSA algorithm

The attributes of information security are Confidentiality, integrity, and availability
RSA algorithm is a public key encryption technique and is considered as the most secure way of encryption. It was invented by Rivest, Shamir and Adleman in year 1978 and hence name RSA algorithm.
Algorithm
The RSA algorithm holds the following features –

- RSA algorithm is a popular exponentiation in a finite field over integers including prime numbers.
- The integers used by this method are sufficiently large making it difficult to solve.
- There are two sets of keys in this algorithm: private key and public key.

You will have to go through the following steps to work on RSA algorithm –

Step 1: Generate the RSA modulus
The initial procedure begins with selection of two prime numbers namely p and q, and then calculating their product N, as shown –
N=p*q
Here, let N be the specified large number.

Step 2: Derived Number (e)
Consider number e as a derived number which should be greater than 1 and less than (p-1) and (q-1). The primary condition will be that there should be no common factor of (p-1) and (q-1) except 1

Step 3: Public key

The specified pair of numbers n and e forms the RSA public key and it is made public.

Step 4: Private Key
Private Key d is calculated from the numbers p, q and e. The mathematical relationship between the numbers is as follows –
ed = 1 mod (p-1) (q-1)
The above formula is the basic formula for Extended Euclidean Algorithm, which takes p and q as the input parameters.

Encryption Formula
Consider a sender who sends the plain text message to someone whose public key is (n,e). To encrypt the plain text message in the given scenario, use the following syntax –
$C = Pe \bmod n$

Decryption Formula
The decryption process is very straightforward and includes analytics for calculation in a systematic approach. Considering receiver C has the private key d, the result modulus will be calculated as –

$Plaintext = Cd \bmod n$

10. Write short notes on :

a) DHCP

The Dynamic Host Configuration protocol (DHCP) is a network management protocol used on internet protocol networks. DHCP operates based on the client–server model. When a computer or other device connects to a network, the DHCP client software sends a DHCP broadcast query requesting the necessary information. Any DHCP server on the network may service the request. The DHCP server manages a pool of IP addresses and information about client configuration parameters such as default gateway, domain name, the name servers, and time servers. On receiving a DHCP request, the DHCP server may respond with specific information for each client, as previously configured by an administrator, or with a specific address and any other information valid for the entire network and for the time period for which the allocation (lease) is valid. A DHCP client typically queries for this information immediately after booting, and periodically thereafter before the expiration of the information. When a DHCP client refreshes an assignment, it initially requests the same parameter values, but the DHCP server may assign a new address based on the assignment policies set by administrators. Depending on implementation, the DHCP server may have three methods of allocating IP addresses:

- Dynamic allocation:
  A network administrator reserves a range of IP addresses for DHCP, and each DHCP client on the LAN is configured to request an IP address from the DHCP server during network initialization. The request-and-grant process uses a lease concept with a controllable time period, allowing the DHCP server to reclaim and then reallocate IP addresses that are not renewed.
- Automatic allocation:
  The DHCP server permanently assigns an IP address to a requesting client from the range defined by the administrator. This is like dynamic allocation, but the DHCP server keeps a table of past IP address assignments, so that it can preferentially assign to a client the same IP address that the client previously had.
- Manual allocation:
  Also commonly called static allocation and reservations. The DHCP server issues a private IP address dependent upon each client's client id (or, traditionally, the client MAC address), based on a predefined mapping by the administrator.

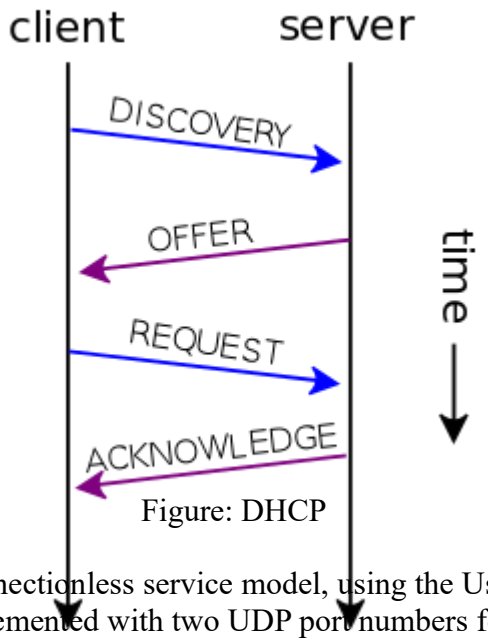


Figure: DHCP

Operation

The DHCP employs a connectionless service model, using the User Datagram Protocol (UDP). It is implemented with two UDP port numbers for its operations which are the same as for the bootstrap protocol (BOOTP). UDP port number 67 is the destination port of a server, and UDP port number 68 is used by the client. DHCP operations fall into four phase:

- Server discovery
- IP lease offer
- IP lease request
- IP lease acknowledgement

b) Firewall

A firewall is a device (usually a router or a computer) installed between the internal network of an organization and the rest of the Internet. It is designed to forward some packets and filter (not forward) others. For example, a firewall may filter all incoming packets destined for a specific host or a specific server such as HTTP. A firewall can be used to deny access to a specific host or a specific service in the organization. A firewall is usually classified as a packet-filter firewall or a proxy based firewall.
A firewall is a type of cybersecurity tool that is used to filter traffic on a network. Firewalls can be used to separate network nodes from external traffic sources, internal traffic sources, or even specific applications. Firewalls can be software, hardware, or cloud-based, with each type of firewall having its own unique pros and cons. The primary goal of a firewall is to block malicious traffic requests and data packets while allowing legitimate traffic through.

5 types of firewalls

- Packet-filtering firewalls
- Circuit-level gateways
- Stateful inspection firewalls
- Application-level gateways (proxy firewall)
- Next-gen firewalls

Packet-filtering firewall:
As the most “basic” and oldest type of firewall architecture, packet-filtering firewalls basically create a checkpoint at a traffic router or switch. The firewall performs a simple check of the data packets coming through the router—inspecting information such as the destination and origination IP address, packet type, port number, and other surface-level information without opening up the packet to inspect its contents. If the information packet doesn’t pass the inspection, it is dropped.
Circuit-level gateways:
As another simplistic firewall type that is meant to quickly and easily approve or deny traffic without consuming significant computing resources, circuit-level gateways work by verifying the transmission control protocol (TCP) handshake. This TCP handshake check is designed to make sure that the session the packet is from is legitimate. While extremely resource-efficient, these firewalls do not check the packet itself. So, if a packet held malware, but had the right TCP handshake, it would pass right through. This is why circuit-level gateways are not enough to protect your business by themselves.
Stateful inspection firewalls
These firewalls combine both packet inspection technology and TCP handshake verification to create a level of protection greater than either of the previous two architectures could provide alone. However, these firewalls do put more of a strain

on computing resources as well. This may slow down the transfer of legitimate packets compared to the other solutions.

Proxy firewalls

Proxy firewalls operate at the application layer to filter incoming traffic between your network and the traffic source—hence, the name "application-level gateway." These firewalls are delivered via a cloud-based solution or another proxy device. Rather than letting traffic connect directly, the proxy firewall first establishes a connection to the source of the traffic and inspects the incoming data packet. If there's one drawback to proxy firewalls, it's that they can create significant slowdown because of the extra steps in the data packet transferal process.

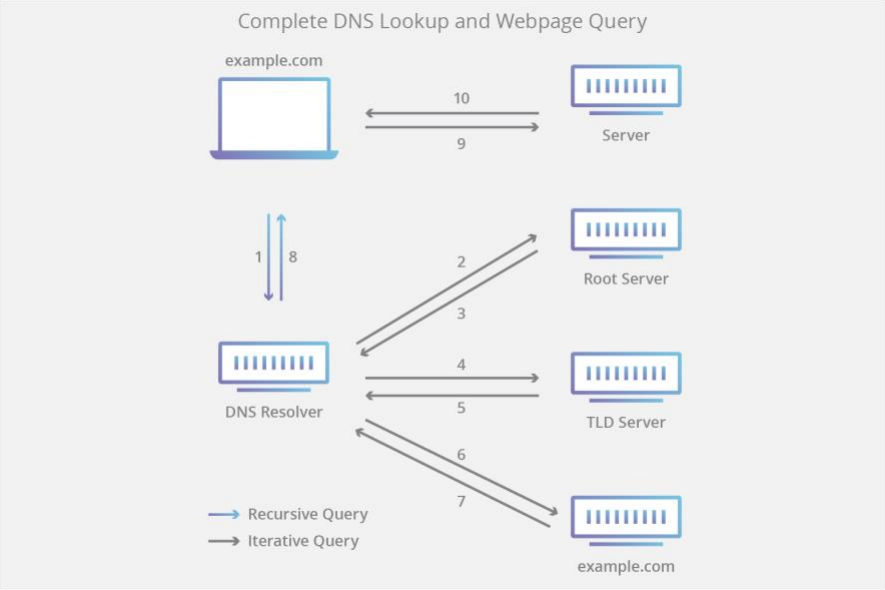
Next-gen firewalls

Some common features of next-generation firewall architectures include deep-packet inspection (checking the actual contents of the data packet), TCP handshake checks, and surface-level packet inspection. Next-generation firewalls may include other technologies as well, such as intrusion prevention systems (IPSs) that work to automatically stop attacks against your network. The issue is that there is no one definition of a next-generation firewall, so it's important to verify what specific capabilities such firewalls have before investing in one.

c) DNS

Domain Name System (DNS) is an internet service that translates domain names into IP addresses, as domain name are alphabetic so easier to remember. Every time you use a domain name, therefore, a DNS service must translate the name into the corresponding IP address. For example, the domain name www.example.com might translate to 198.105.232.4.
Domain names give people a more intuitive way to access content or services than IP addresses: www.techtarget.com instead of 206.19.49.149, for example. Most URLs are built around the domain name of the web server fielding the request: e.g., http://searchnetworking.techtarget.com/definition/DNS-attack. Web browsing and most other internet activity rely on DNS behind the scenes to quickly provide the information necessary to connect users to remote hosts.

Importance of DNS
Having a single DNS server somewhere that maintained a complete central list of domain name or IP address mappings would be impractical. There are too many mappings, they change too often and the number of requests for address or name lookups would overwhelm any system. As a result, DNS is distributed throughout the internet in a hierarchy of authority. Access providers and enterprises, as well as governments, universities and other organizations, typically have their own assigned ranges of IP addresses and an assigned domain name; they also typically run DNS servers to manage the mapping of those names to those addresses.



2073 SHRAWAN

1. Differentiate between TCP/IP and OSI Model. Define Frame Relay in detail.

OSI(Open System Interconnection)	TCP/IP(Transmission Control Protocol / Internet Protocol)
• OSI is a generic, protocol independent standard, acting as a communication gateway between the network and end user.	• TCP/IP model is based on standard protocols around which the internet has developed. It is a communication protocol, which allows connection of hosts over a connection.
• In OSI model the transport layer guarantees the delivery of packets.	• In TCP/IP model the transport layer does not guarantees delivery of packets. Still the TCP/IP model is more reliable.
• Follows vertical approach.	• Follows horizontal approach.
• OSI model has a separate presentation layer and session layer.	• TCP/IP does not have a separate presentation layer or session layer.
• OSI is a reference model around which the networks are built. Generally it is used as a guidance tool.	• TCP/IP model is, in a way implementation of the OSI model.
• Network layer of OSI model provides both connections oriented and connectionless service.	• The network layer in TCP/IP model provides connectionless service.
• OSI model has a problem of fitting the protocols into 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.

• OSI model defines services, interfaces and protocols very clearly and makes clear distinction between them. It is protocol independent.	• In TCP/IP, services, interfaces and protocols are not clearly separated. It is also protocol dependent.
• It has 7 layers.	• It has 4 layers.

The X.25 networks were largely replaced by a new kind of network called frame relay. The essence of frame relay is that it is a connection-oriented network with no error control and no flow control. Because it was connection-oriented, packets were delivered in order. The properties of in-order delivery, no error control, and no flow control make frame relay skin to a wide area LAN. Its most important application is interconnecting LANs at multiple company offices.

2. **What do you mean by switching in communication? Compare switching with multiplexing. Explain the E1 telephone hierarchy system.**

Switching is process to forward packets coming in from one port to a port leading towards the destination. When data comes on a port it is called ingress, and when data leaves a port or goes out it is called egress. A communication system may include number of switches and nodes. Switching is divided into two categories:

Circuit Switching

When two nodes communicate with each other over a dedicated communication path, it is called circuit switching. There 'is a need of pre-specified route from which data will travels and no other data is permitted. In circuit switching, to transfer the data, circuit must be established so that the data transfer can take place. Circuit switching was designed for voice applications. Telephone is the best suitable example of circuit switching. Before a user can make a call, a virtual path between caller and called is established over the network.

Message Switching

This technique was somewhere in middle of circuit switching and packet switching. In message switching, the whole message is treated as a data unit and is switching / transferred in its entirety. A switch working on message switching, first receives the whole message and buffers it until there

are resources available to transfer it to the next hop. If the next hop is not having enough resource to Accommodate large size message, the message is stored and switch waits. This technique was considered substitute to circuit switching. As in circuit switching the whole path is blocked for two entities only. Message switching is replaced by packet switching.

Message switching has the following drawbacks:

- Every switch in transit path needs enough storage to accommodate entire message.
- Because of store-and-forward technique and waits included until resources are available, message switching is very slow.
- Message switching was not a solution for streaming media and real-time applications.

Packet Switching

Shortcomings of message switching gave birth to an idea of packet switching. The entire message is broken down into smaller chunks called packets. The switching information is added in the header of each packet and transmitted independently. It is easier for intermediate networking devices to store small size packets and they do not take many resources either on carrier path or in the internal memory of switches. Packet switching enhances line efficiency as packets from multiple applications can be multiplexed over the carrier. The internet uses packet switching technique. Packet switching enables the user to differentiate data streams based on priorities. Packets are stored and forwarded according to their priority to provide quality of service.

E1 is the European format for DS1 digital transmission. E1 links are similar to T1 links except that they carry signals at 2.048 Mbps. Each signal has 32 channels, and each channel transmits at 64 Kbps. E1 links have higher bandwidth than T1 links because it does not reserve one bit for overhead. Whereas, T1 links use 1 bit in each channel for overhead.

T1 and E1 Signals

T1 and E1 interfaces consist of two pairs of wires—a transmit data pair and a receive data pair. Clock signals, which determine when the transmitted data is sampled, are embedded in the T1 and E1 transmissions. Typical digital signals operate by sending either zeros (0s) or ones (1s), which are usually represented by the absence or presence of a voltage on the line. The receiving device need only detect the presence of the voltage on the line at the particular sampling edge to determine whether the signal is 0 or 1. T1 and E1, however, use bipolar electrical pulses. Signals are

represented by no voltage (0), positive voltage (1), or negative voltage (1). The bipolar signal allows T1 and E1 receivers to detect error conditions in the line, depending on the type of encoding that is being used.

Encoding

The following are common T1 and E1 encoding techniques:

- Alternate mark inversion (AMI)—T1 and E1
- Bipolar with 8-zero substitution (B8ZS)—T1 only
- High-density bipolar 3 code (HDB3)—E1 only

Common Characteristics:-

- Both are having Same Sampling Frequency i.e. 8kHz.
- In both (E1 & T1) Number of samples/telephone signal = 8000/sec.
- In both (E1 & T1) Length of PCM Frame = 1/8000s = 125µs.
- In both (E1 & T1) Number of Bits in each code word = 8.
- In both (E1 & T1) Telephone Channel Bit Rate = 8000/s x 8 Bit = 64 kbit/s.

Differing Characteristics:-

- In E1 Encoding/Decoding is followed by A-Law while in T1 Encoding/Decoding is followed by µ-Law.
- In E1 – 13 Number of Segments in Characteristics while in T1 – 15 Number of Segments in Characteristics.
- In E1 – 32 Number of Timeslots / PCM Frame while in T1 – 24 Number of Timeslots / PCM Frame.
- In E1 – 8 x 32 = 256 number of bits / PCM Frame while in T1 – 8 x 24 + 1* = 193 number of bits / PCM Frame. (* Signifies an additional bit).
- In E1 – (125µs x 8)/256 = approx. 3.9µs is the length of an 8-bit Timeslot while in T1 – (125µs x 8)/193 = approx. 5.2µs is the length of an 8-bit Timeslot.
- In E1 – 8000/s x 256 bits = 2048kbit/s is the Bit Rate of Time-Division Multiplexed Signal while in T1 – 8000/s x 193 bits = 1544kbit/s is the Bit Rate of Time-Division Multiplexed Signal.

3. **What do you mean by Media Access Control? What is its significance in data link layer? Explain why token bus is also called as the token ring.**

A media access control is a network data transfer policy that determines how data is transmitted between two computer terminals through a network cable.

Framing: Data-link layer takes packets from Network Layer and encapsulates them into Frames. Then, it sends each frame bit-by-bit on the hardware. At receiver' end, data link layer picks up signals from hardware and assembles them into frames.

Addressing: Data-link layer provides layer-2 hardware addressing mechanism. Hardware address is assumed to be unique on the link. It is encoded into hardware at the time of manufacturing.

Synchronization: When data frames are sent on the link, both machines must be synchronized in order to transfer to take place.

Error Control: Sometimes signals may have encountered problem in transition and the bits are flipped. These errors are detected and attempted to recover actual data bits. It also provides error reporting mechanism to the sender.

Flow Control: Stations on same link may have different speed or capacity. Data-link layer ensures flow control that enables both machines to exchange data on same speed.

Multi-Access: When host on the shared link tries to transfer the data, it has a high probability of collision. Data-link layer provides mechanism such as CSMA/CD to equip capability of accessing a shared media among multiple Systems.

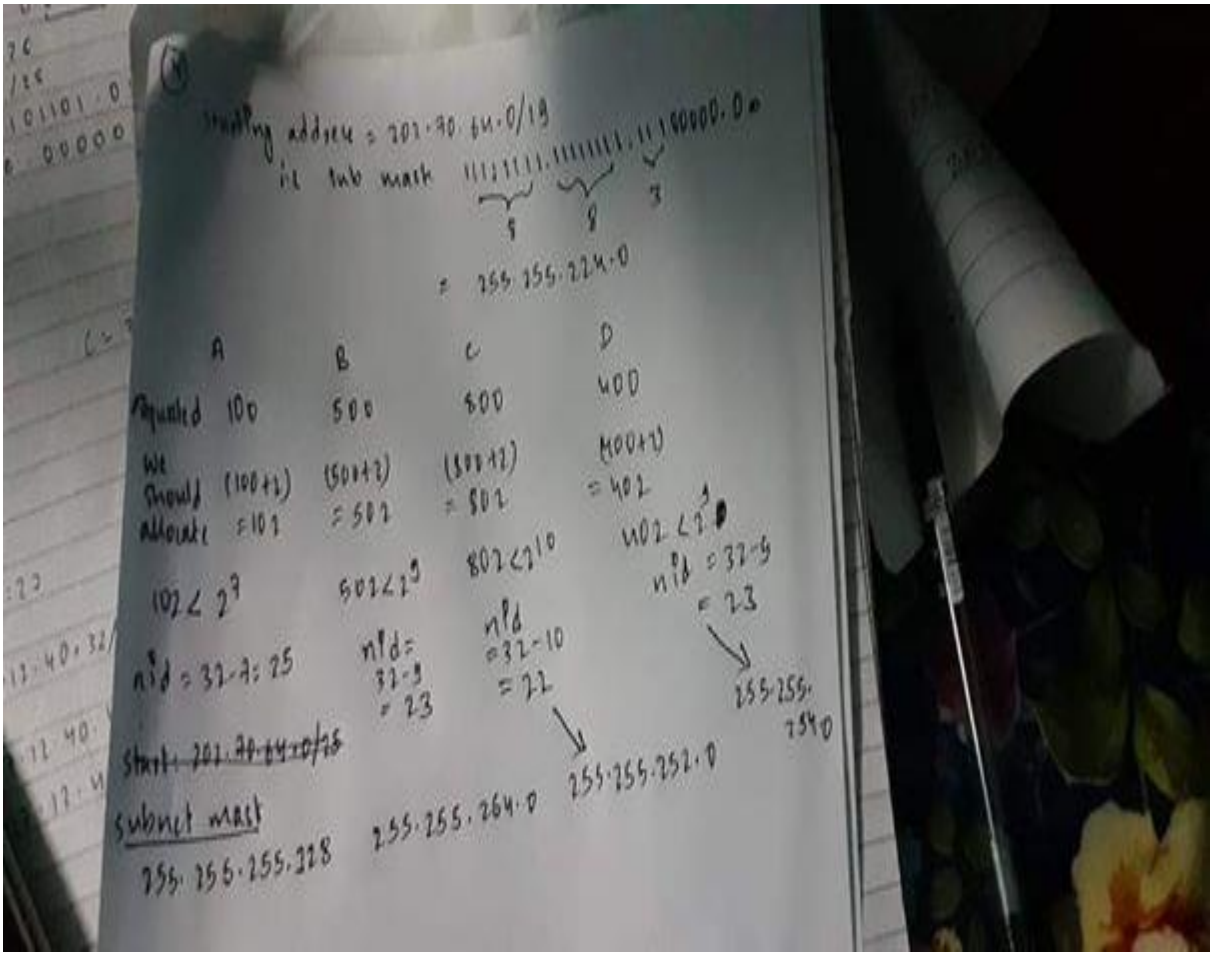
Reliable delivery: When a link-layer protocol provides reliable delivery service, it guarantees to move each network-layer datagram across the link without error.

Token Bus is described in the IEEE 802.4 specification, and is a Local Area Network (LAN) in which the stations on the bus or tree form a logical ring. Each station is assigned a place in an ordered sequence, with the last station in the sequence being followed by the first, as shown below. Each station knows the address of the station to its "left" and "right" in the sequence. This type of network, like a Token Ring network, employs a small data frame only a few bytes in size, known as a token, to grant individual stations exclusive access to the network transmission medium. Token-passing networks are deterministic in the way that they control access to the network, with each node playing an active role in the process. When a station acqires control of the token, it is

allowed to transmit one or more data frames, depending on the time limit imposed by the network. When the station has finished using the token to transmit data, or the time limit has expired, it relinquishes control of the token, which is then available to the next station in the logical sequence. When the ring is initialized, the station with the highest number in the sequence has control of the token.

4. **You are a private contractor hired by the large company to setup the network for their enterprise and you are given a large no. of consecutive IP address starting at 202.70.64.0/19. Suppose that four department A,B,C,D request 100 ,500 ,800 and 400 addresses respectively,how the subnetting can be performed so, that address wastage will be minimum?**

→



5. Discuss about the network congestion? Explain how different parameters effect the congestion.Compare operation of link state routing with the distance vector routing.

→ Network congestion in data networking and queueing theory is the reduced quality of service that occurs when a network node or link is carrying more data than it can handle. Typical effects include queueing delay, packet loss or the blocking of new connections. A consequence of congestion is that an incremental increase in offered load leads either only to a small increase or even a decrease in network throughput.

Network protocols that use aggressive retransmissions to compensate for packet loss due to congestion can increase congestion, even after the initial load has been reduced to a level that would not normally have induced network congestion. Such networks exhibit two stable states under the same level of load. The stable state with low throughput is known as congestive collapse.

The different parameters effecting the congestion are:

• Queuing -- Buffers on network devices are managed with various queuing techniques. And, properly managed queues can minimize dropped packets and network congestion, as well as improve network performance.

• Congestion control in frame relay — implements two congestion avoidance mechanisms: BECN (backward explicit congestion notification), And FECN (forward explicit congestion notification)

• Congestion Control and Avoidance in TCP — designed to prevent overflowing the receiver's buffers, not the buffers of network nodes. Slow start congestion control — a technique that requires a host to start its transmissions slowly and then build up to the point where congestion starts to occur.

• Fast retransmit and fast recovery — algorithms designed to minimize the effect that dropping packets has on network throughput.

• Active queue management (AQM) -- a technique in which routers actively drop packets from queues as a signal to senders that they should slow down

• RED (Random Early Discard) – one of active queues management (AQM) scheme uses statistical methods to drop packets in a "probabilistic" way before queues overflow.

• ECN (explicit congestion notification) —a technique applicable in congestion avoidance mechanism.

Distance Vector Routing	Link State Routing
--> Bandwidth required is less due to local sharing, small packets and no flooding.	--> Bandwidth required is more due to flooding and sending of large link state packets.
--> Based on local knowledge since it updates table based on information from neighbors.	--> Based on global knowledge i.e. it have knowledge about entire network.
--> Make use of Bellman Ford algo	--> Make use of Dijkastra's algo
--> Traffic is less	--> Traffic is more
--> Converges slowly i.e. good news spread fast and bad news spread slowly.	--> Converges faster.
--> Count to infinity problem.	--> No count to infinity problem.
--> Persistent looping problem i.e. loop will there forever.	--> No persistent loops, only transient loops.
--> Practical implementation is RIP and IGRP.	--> Practical implementation is OSPF and ISIS.

6. How web server communicationa and file server communication are possible in network,explain with used protocols.Define socket programming.

→ Common Internet protocols include TCP/IP (Transmission Control Protocol/Internet Protocol), UDP/IP (User Datagram Protocol/Internet Protocol), HTTP (HyperText Transfer Protocol) and FTP (File Transfer Protocol).

- TCP/IP
  TCP/IP is a stream protocol. This means that a connection is negotiated between a client and a server. Any data transmitted between these two endpoints is guaranteed to arrive, thus it is a so-called lossless protocol. Since the TCP protocol (as it is also referred to in short form) can only connect two endpoints, it is also called a peer-to-peer protocol.
- HTTP
  HTTP is the protocol used to transmit all data present on the World Wide Web. This includes text, multimedia and graphics. It is the protocol used to transmit HTML, the language that makes all the fancy decorations in your browser. It works upon TCP/IP.
- FTP
  FTP is the protocol used to transmit files between computers connected to each other by a TCP/IP network, such as the Internet.

File sharing is something which is part of our daily activities. This is also commonly referred to as P2P or Peer-to-Peer sharing. This could be sharing files between two nodes in a network or between a client and a server or between two nodes not within the same network. Any multi-user environment will require a file sharing mechanism.

There are several applications available which cater to file sharing. Some of these are:

- uTorrent
- BitTorrent
- SoulSeek
- eMuke
- Shareaza

The most used file sharing protocols are:

- FTP – FTP stands for File Transfer Protocol. This is a common method used to transfer files between devices and users within a network. You can access, download and upload files using FTP. This is mostly used to transfer files between the host computer and a server or a website. Basic configuration changes with port forwarding enabled can be used to access FTP outside a network. Some of the popular FTP based applications include– Transmit, Cyberduck, FileZilla, WinSCP, Coda.
- SFTP (SSH based) – As the name suggests this is a variant of FTP and is a more secure way of using FTP. SFTP stands for Secure File Transfer Protocol. This is SSH-based file transfer. This has an ability to provide secure connections for file transfer and can be used for local as well as remote systems. In most cases, SFTP is a more favorable choice owing to the added security it provides. Most applications which support FTP also support SFTP.
- SCP – This is commonly referred to as Secure Copy protocol. This works on Secure Shell- SSH protocol and can be used to transfer files between local and remote hosts or between two remote hosts. SCP is based on BSD RCP protocol. Since it works over SSH, SCP uses the same mechanism for authentication. SCP runs over TCP port 22 and using this a client one can either upload or download single or multiple files. There is no RFC that provides specifications of this protocol.
- SMB – SMB stands for Server Message block. This is an application layer network layer protocol. This is a protocol which is mainly used for shared access to printers, files, and ports. Additionally, this also provides an authenticated inter-process communication mechanism. This was mostly used with Windows and was known as Microsoft Windows Network, before the start of Active Directory. SAMBA is an implementation of SMB. CIFS is a specific implementation of SMB and stands for Common Internet File System.

- NFS – NFS stands for Network File System protocol and is a standard protocol used over a distributed file system. This is commonly used in a client-server architecture and allows users to view, store and update files in a remote system. To use this there are a couple of prerequisites and may require the user to be comfortable using Linux based systems. This is a popular file system access protocol which works with Linux, FreeBSD, Apple's macOS, Solaris, AIX. Apart from this, other file system access protocol includes SMB (Server Message Block also called as CIFS), AFP (Apple Filing Protocol), NCP (Network Core Protocol). This is a distributed file system standard for network attached storage-NAS. The protocol allows users to view, store and update files over a remote network. The way SAMBA is closely associated with Windows, NFS is a great choice for Linux or Unix users.

Socket programming is a way of connecting two nodes on a network to communicate with each other. One socket(node) listens on a particular port at an IP, while other socket reaches out to the other to form a connection. Server forms the listener socket while client reaches out to the server.

10. Write short notes on:

a) HDLC:

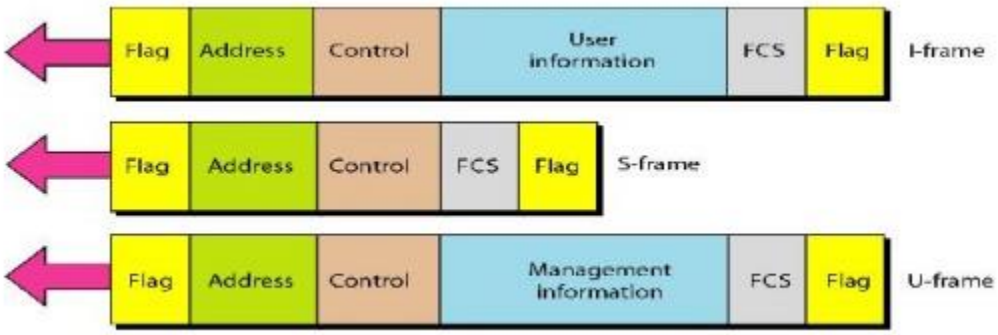
A high-level data link control (HDLC) is a protocol that is a bit-oriented synchronous data link layer. HDLC ensures the error-free transmission of data to the proper destinations and controls the data transmission speed. HDLCs can provide both connection-oriented and connectionless services.

A high-level data link control defines rules for transmitting data between network points. Data in an HDLC is organized into units called frames and is sent across networks to specified destinations. HDLC also manages the pace at which data is transmitted. HDLC is commonly used in the open systems interconnection (OSI) model's layer. HDLC frames are transmitted over synchronous links or asynchronous links, which do not mark the start and end of frames. This is done using a frame delimiter or flag, which contains unique sequence of bits that are not visible inside a frame. There are three types of HDLC frames:

• Information frames/User data (I-frames)
• Supervisory frames/Control data (S-frames)
• Unnumbered frames (U-frames)

The common fields within an HDLC frame are:

• Flag
• Address
• Control information
• Frame check sequence



Flag field : It is a 8-bit sequence with the bit pattern 01111110 that identifies both the beginning and the end of a frame and serves as a synchronization pattern for the receiver.
Address field: It contains the address of the secondary station. If a primary station created the frame, it contains a 'to' address. If a secondary creates the frame, it contains a 'from' address. An address field can be 1 byte or several bytes long, depending on the needs of the network. If the address field is only 1 byte, the last bit is always a 1. If the address is more than 1 byte, all bytes but the last one will end with 0; only the last will end with 1. Ending each intermediate byte with 0 indicates to the receiver that there are more address bytes to come.
Control field: The control field is a 1- or 2-byte segment of the frame used for flow and error control.
Information field: The information field contains the user's data from the network layer or management information
FCS field: The frame check sequence (FCS) is the HDLC error detection field.

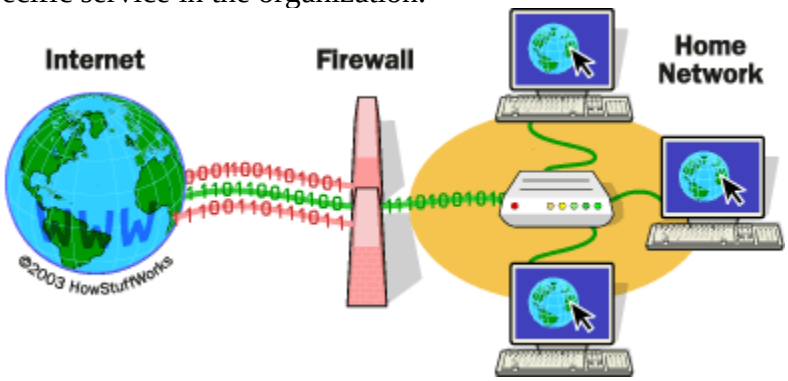
b) Web Server: A web server is server software or hardware dedicated to running said software, that can satisfy world wide web client requests. A web server can, in general, contain one or more websites. The primary function of a web server is to store, process and deliver web pages to clients. The communication between client and server takes place using the HTTP (Hyper text transfer protocol).

Web servers can frequently be found in embedded devices such as printers, routers, webcams and serving only a local network. The web server may then be used as a part of a system for monitoring or administering the device in question. This usually means that no additional software has to be installed on the client computer since only a web browser is required.

A web server can be either incorporated into the OS kernel, or in user space . Web servers that run in user-mode have to ask the system for permission to use more memory or more CPU resources. Not only do these requests to the kernel take time, but they are not always satisfied because the system reserves resources for its own usage and has the responsibility to share hardware resources with all the other running applications. Executing in user mode can also mean useless buffer copies which are another limitation for user-mode web servers.

9. What do you mean by firewall? Explain different types of firewall.

A firewall is a device (usually a router or a computer) installed between the internal network of an organization and the rest of the Internet. It is designed to forward some packets and filter (not forward) others.
For example, a firewall may filter all incoming packets destined for a specific host or a specific server such as HTTP. A firewall can be used to deny access to a specific host or a specific service in the organization.



The different types of firewall are :

I) Packet filter firewall:

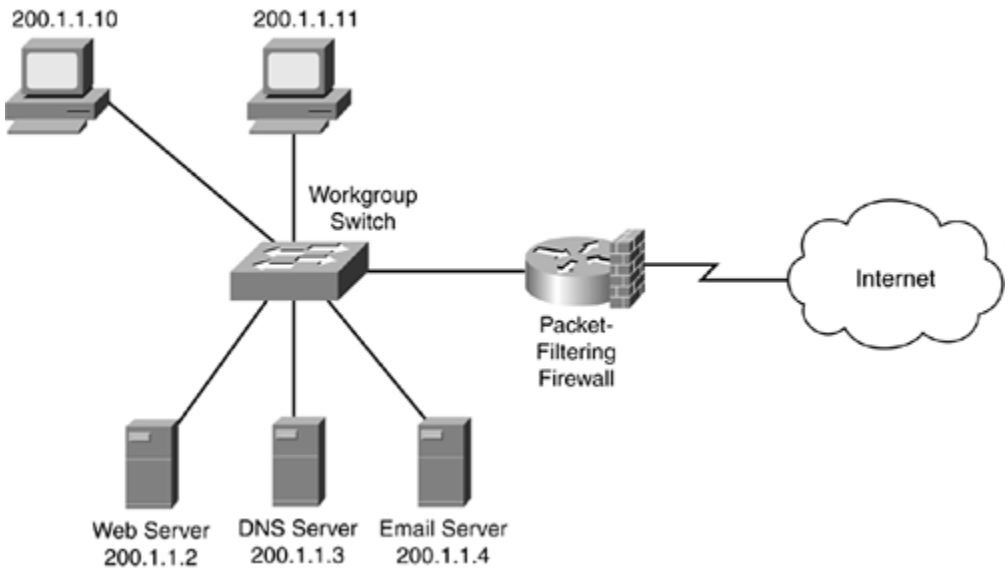
Packet-Filter Firewall A firewall can be used as a packet filter. It can forward or block packets based on the information in the network layer and transport layer headers: source and destination IP addresses, source and destination port addresses, and type of protocol (TCP or UDP). A packet-filter firewall is a router that uses a filtering table to decide which packets must be discarded (not forwarded). Figure shows an example of a filtering table for this kind of a firewall.

A packet-filtering firewall can filter on the following types of information:

- Source and destination Layer 3 address
- Layer 3 protocol information
- Layer 4 protocol information
- Interface of sent or received traffic

Packet filtering table :

Rule	Source Address	Destination Address	IP Protocol	IP Protocol Information	Action
1	Any	200.1.1.2	TCP	Port 80	Allow
2	Any	200.1.1.3	UDP	Port 53	Allow
3	Any	200.1.1.4	TCP	Port 25	Allow
4	Any	Any other address	Any	Any	Drop



In this example, rule 1 states that if traffic from any device on the Internet is sent to TCP port 80 of 200.1.1.2, the packet-filtering firewall should allow it. Likewise, if any traffic is sent to UDP port 53 of 200.1.1.3 or TCP port 25 of 200.1.1.4, the traffic should be allowed. Any other type of traffic should be dropped.

It is important to point out that if you omit rule 4, you might have issues with a packet-filtering firewall. A packet-filtering firewall will make one of two assumptions:

- If there is no match in the rule set, allow the traffic.
- If there is no match in the rule set, drop the traffic.

Packet-filtering firewalls have two main advantages:

- They can process packets at very fast speeds.
- They easily can match on most fields in Layer 3 packets and Layer 4 segment headers, providing a lot of flexibility in implementing security policies.

II) Application Gateway:

An application gateway or application level gateway (ALG) is a firewall proxy which provides network security. It filters incoming node traffic to certain specifications which mean that only transmitted network application data is filtered. Such network applications include File Transfer Protocol (FTP), Telnet, Real Time Streaming Protocol (RTSP) and Bit Torrent.

Application gateways provide high-level secure network system communication. For example, when a client requests access to server resources such as files, Web pages and databases, the client first connects with the proxy server, which then establishes a connection with the main server.

The application gateway resides on the client and server firewall. The proxy server hides Internet Protocol (IP) addresses and other secure information on the client's behalf. A computer's internal system may communicate with an external computer using firewall protection. The application gateway and external computer function without client information or knowledge of the proxy server IP address.

8. Compare symmetric key encryption method with asymmetric key encryption. Explain RSA algorithm with example.

BASIS FOR COMPARISON	SYMMETRIC ENCRYPTION	ASYMMETRIC ENCRYPTION
Basic	Symmetric encryption uses a single key for both encryption and Decryption.	Asymmetric encryption uses a different key for encryption and decryption.
Performance	Symmetric encryption is fast in execution.	Asymmetric Encryption is slow in execution due to the high computational burden.

BASIS FOR COMPARISON	SYMMETRIC ENCRYPTION	ASYMMETRIC ENCRYPTION
Algorithms	DES, 3DES, AES, and RC4.	Diffie-Hellman, RSA.
Purpose	The symmetric encryption is used for bulk data transmission.	The asymmetric encryption is often used for securely exchanging secret keys.

- Rivest, Shamir, and Adleman (RSA) is an algorithm used by modern computers to encrypt and decrypt messages. It is an asymmetric cryptographic algorithm. Asymmetric means that there are two different keys. This is also called public key cryptography, because one of the keys can be given to anyone. The other key must be kept private.
- The algorithm is based on the fact that finding the factors of a large composite number is difficult: when the factors are prime numbers, the problem is called prime factorization. It is also a key pair (public and private key) generator.

It uses two numbers, e and d, as the public and private keys

1. Choose two different large random prime numbers p and q
2. Calculate n = pq
   - n is the modulus for the public key and the private keys
3. Calculate the totient: $\Phi(n) = (p-1)(q-1)$
4. Choose e an integer such that $1 < e < \Phi(n)$, e is co − prime to $\Phi(n)$ i.e.: e and $\Phi(n)$ share no factors other than 1; gcd (e , $\Phi(n)$) = 1.
   - e is released as the public key exponent
5. Simply to say : Calculate d = 1+x $\Phi(n))/e$ to be integer
   - d is kept as the private key exponent

Consider a sender who sends the plain text message to someone whose public key is (n,e). To encrypt the plain text message in the given scenario, use the following syntax −

C = Pe mod n

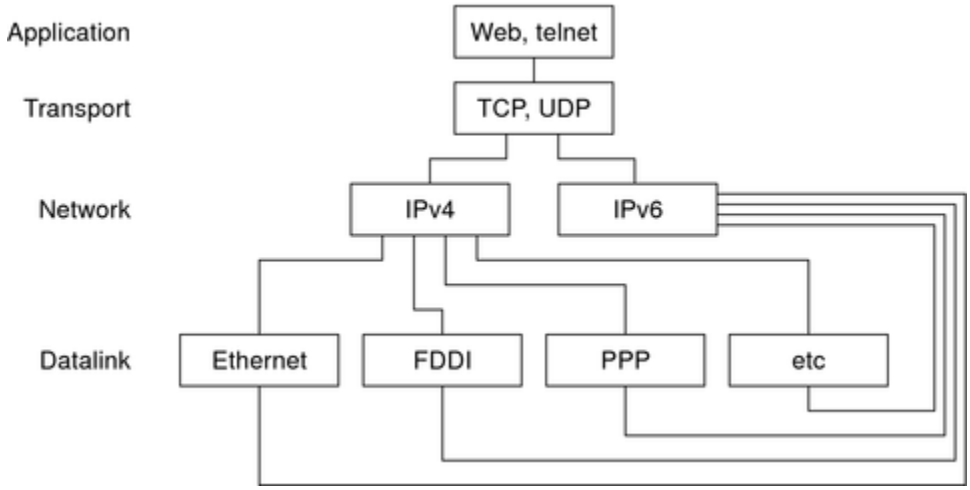
The decryption process is very straightforward and includes analytics for calculation in a systematic approach. Considering receiver C has the private key d, the result modulus will be calculated as −

Plaintext = Cd mod n

7.What are the factors that lead to development of IPv6? Define the process of transition from IPv4 to IPv6.

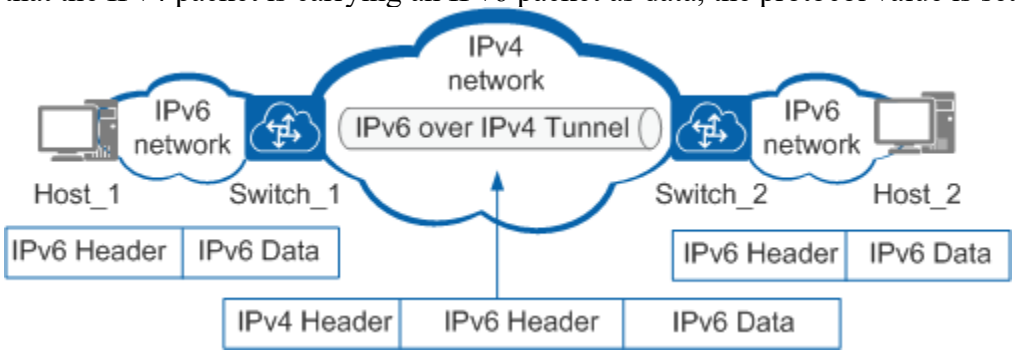
With the rapid growth of the Internet after commercialization in the 1990s, it became evident that far more addresses would be needed to connect devices than the IPv4 address space had available. The IP addresses provided till now would not be sufficient for the future generation and as there are many limitation to IPv4 which need to be overcome in the new version IPv6
IPv4 provides the host-to-host communication between systems in the Internet. Although IPv4 is well designed, data communication has evolved since the inception of IPv4 in the 1970s. IPv4 has some deficiencies (listed below) that make it unsuitable for the fastgrowing Internet.
o Despite all short-term solutions, such as subnetting, classless addressing, and NAT, address depletion is still a long-term problem in the Internet.
o The Internet must accommodate real-time audio and video transmission. This type of transmission requires minimum delay strategies and reservation of resources not provided in the IPv4 design.
o The Internet must accommodate encryption and authentication of data for some applications. No encryption or authentication is provided by IPv4.
The processes needed for the transition from IPv4 to IPv6 are:

Dual Stack :
It is recommended that all hosts, before migrating completely to version 6, have a dual stack of protocols. In other words, a station must run IPv4 and IPv6 simultaneously untilall the Internet uses IPv6.
To determine which version to use when sending a packet to a destination, the source host queries the DNS. If the DNS returns an IPv4 address, the source host sends an IPv4 packet. If the DNS returns an IPv6 address, the source host sends an IPv6 packet.



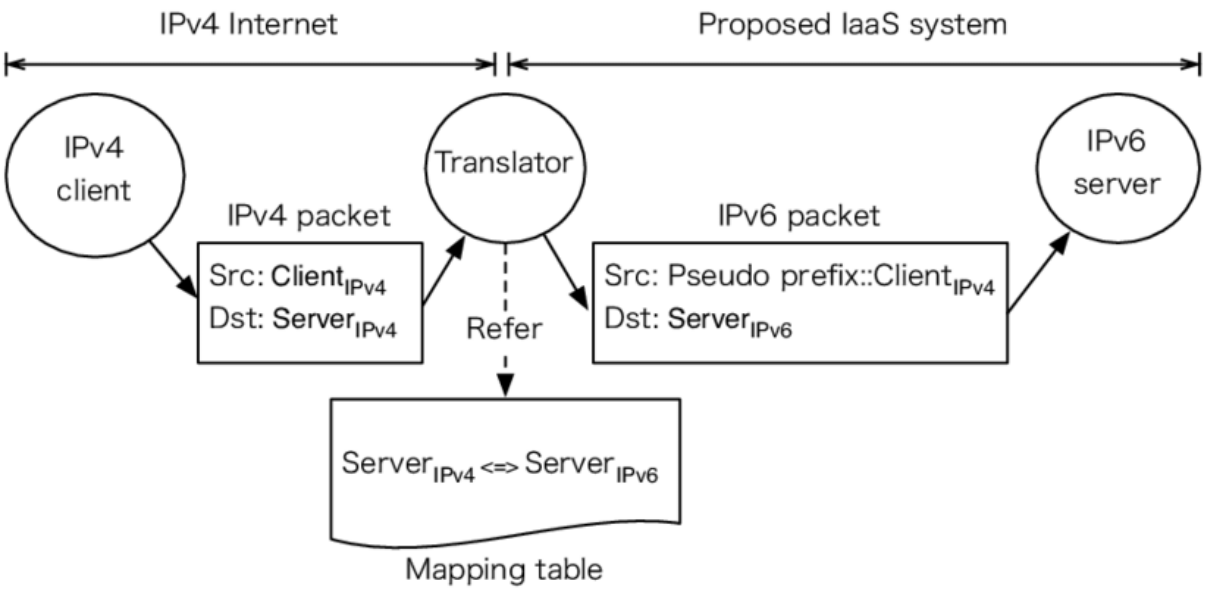
Tunneling:

Tunneling is a strategy used when two computers using IPv6 want to communicate with each other and the packet must pass through a region that uses IPv4. To pass through this region, the packet must have an IPv4 address. So the IPv6 packet is encapsulated in an IPv4 packet when it enters the region, and it leaves its capsule when it exits the region. It seems as if the IPv6 packet goes through a tunnel at one end and emerges at the other end. To make it clear that the IPv4 packet is carrying an IPv6 packet as data, the protocol value is set to 41.



Header Translation :

Header translation is necessary when the majority of the Internet has moved to IPv6 but some systems still use IPv4. The sender wants to use IPv6, but the receiver does not understand IPv6. Tunneling does not work in this situation because the packet must be in the IPv4 format to be understood by the receiver. In this case, the header format must be totally changed through header translation. The header of the IPv6 packet is converted to an IPv4 header.


IPv4 Internet
Proposed IaaS system
IPv4
client
Translator
IPv6
server
IPv4 packet
IPv6 packet
Src: Client$_{IPv4}$
Dst: Server$_{IPv4}$
Refer
Src: Pseudo prefix::Client$_{IPv4}$
Dst: Server$_{IPv6}$
Server$_{IPv4}$ <=> Server$_{IPv6}$
Mapping table

2074 CHAITRA

1.Distinguish between Client-Server Network and Peer-Peer Network. Explain the OSI model

BASIS FOR COMAPAISON	CLIENT-SERVER	PEER-TO-PEER
Basic	There is a specific server and specific clients connected to the server.	Clients and server are not distinguished; each node act as client and server.
Service	The client request for service and server respond with the service.	Each node can request for services and can also provide the services.
Focus	Sharing the information.	Connectivity.
Data	The data is stored in a centralized server.	Each peer has its own data.
Server	When several clients request for the services simultaneously, a server can get bottlenecked.	As the services are provided by several servers distributed in the peer-to-peer system, a server in not bottlenecked.
Expense	The client-server are expensive to implement.	Peer-to-peer are less expensive to implement.
Stability	Client-Server is more stable and scalable.	Peer-to Peer suffers if the number of peers increases in the system.

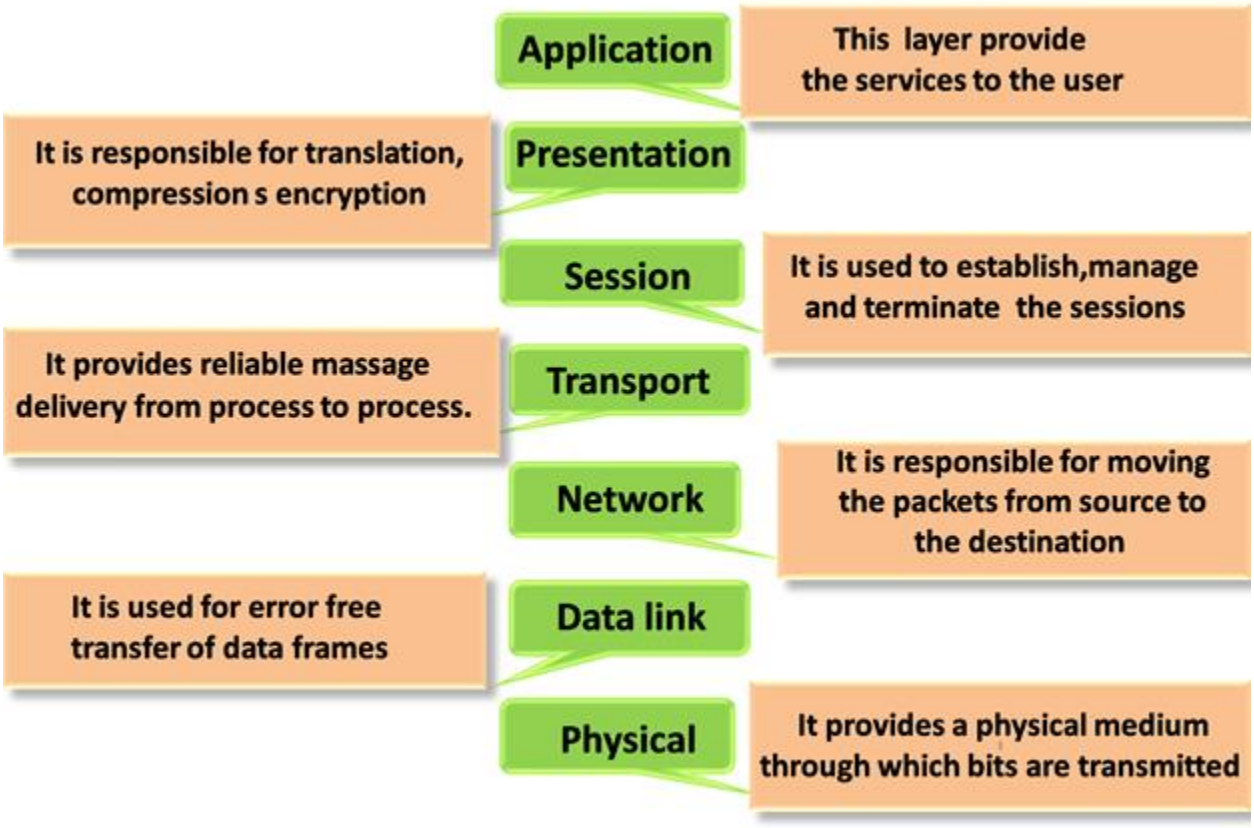


FIG:OSI model layers

- OSI stands for Open System Interconnection is a reference model that describes how information from a software application in one computer moves through a physical medium to the software application in another computer.
- OSI consists of seven layers, and each layer performs a particular network function.
- OSI model was developed by the International Organization for Standardization (ISO) in 1984, and it is now considered as an architectural model for the inter-computer communications.
- OSI model divides the whole task into seven smaller and manageable tasks. Each layer is assigned a particular task.
- Each layer is self-contained, so that task assigned to each layer can be performed independently.
- The OSI model is divided into two layers: upper layers and lower layers.
- The upper layer of the OSI model mainly deals with the application related issues, and they are implemented only in the software. The application layer is closest to the end user. Both the end user and the application layer interact with the software applications. An upper layer refers to the layer just above another layer.

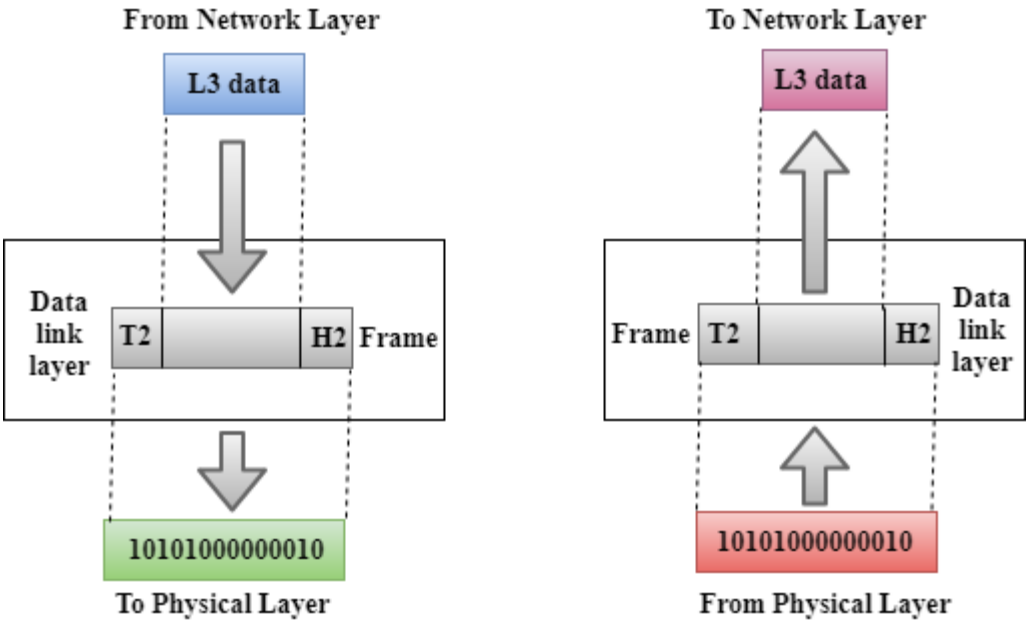
- The lower layer of the OSI model deals with the data transport issues. The data link layer and the physical layer are implemented in hardware and software. The physical layer is the lowest layer of the OSI model and is closest to the physical medium. The physical layer is mainly responsible for placing the information on the physical medium.

2.Define transmission media. Compare among Twisted Pair, Coaxial Cable and Optical fiber

Transmission medium is a physical path between the transmitter and the receiver i.e. it is the channel through which data is sent from one place to another.

Twisted pair cable	Co-axial cable	Optical fiber
1. Transmission of signals takes place in the electrical form over the metallic conducting wires. 2. In this medium the noise immunity is low. 3. Twisted pair cable can be affected due to external magnetic field. 4. Cheapest medium 5. Low Bandwidth 6. Attenuation is very high. 7. Installation is easy.	1. Transmission of signals takes place in the electrical over a form over the inner conductor of the cable. 2. Higher noise immunity than twisted pair cable 3. Less affected by external magnetic field. 4. Moderately Expensive 5. Moderately higher bandwidth 6. Attenuation is low 7. Installation is fairly easy.	1. Transmission of signals takes place takes place in an optical form in a glass fiber. 2. Highest noise immunity. 3. Not affected by external magnetic field. 4. Expensive 5. Very high bandwidth 6. Attenuation is very low 7. Installation is difficult.

3.What is the main functionality of data link layer? Differentiate between circuit switching and packet switching.



- This layer is responsible for the error-free transfer of data frames.
- It defines the format of the data on the network.
- It provides a reliable and efficient communication between two or more devices.
- It is mainly responsible for the unique identification of each device that resides on a local network.
- It contains two sub-layers:
    - Logical Link Control Layer
        - It is responsible for transferring the packets to the Network layer of the receiver that is receiving.
        - It identifies the address of the network layer protocol from the header.
        - It also provides flow control.
    - Media Access Control Layer
        - A Media access control layer is a link between the Logical Link Control layer and the network's physical layer.
        - It is used for transferring the packets over the network.

Functions:

- Framing: The data link layer translates the physical's raw bit stream into packets known as Frames. The Data link layer adds the header and trailer to the frame. The header which is added to the frame contains the hardware destination and source address.

- Physical Addressing: The Data link layer adds a header to the frame that contains a destination address. The frame is transmitted to the destination address mentioned in the header.
- Flow Control: Flow control is the main functionality of the Data-link layer. It is the technique through which the constant data rate is maintained on both the sides so that no data get corrupted. It ensures that the transmitting station such as a server with higher processing speed does not exceed the receiving station, with lower processing speed.
- Error Control: Error control is achieved by adding a calculated value CRC (Cyclic Redundancy Check) that is placed to the Data link layer's trailer which is added to the message frame before it is sent to the physical layer. If any error seems to occur, then the receiver sends the acknowledgment for the retransmission of the corrupted frames.
- Access Control: When two or more devices are connected to the same communication channel, then the data link layer protocols are used to determine which device has control over the link at a given time.

4. Mention the criteria for good routing. Explain RIP, OSPF, BGP, IGRP and EIGRP.

The criteria for routing is

- Hop count
- Delay
- Bandwidth
- Loss rate

RIP

Routing Information Protocol (RIP) is a dynamic routing protocol which uses hop count as a routing metric to find the best path between the source and the destination network. It is a distance vector routing protocol which has AD value 120 and works on the application layer of OSI model. RIP uses port number 520. Hop count is the number of routers occurring in between the source and destination network. The path with the lowest hop count is considered as the best route to reach a network and therefore placed in the routing table. RIP prevents routing loops by limiting the number of hopes allowed in a path from source and destination. The maximum hop count allowed for RIP is 15 and hop count of 16 is considered as network unreachable.

Features of RIP :

1. Updates of the network are exchanged periodically.
2. Updates (routing information) are always broadcast.
3. Full routing tables are sent in updates.
4. Routers always trust on routing information received from neighbor routers. This is also known as Routing on rumors.

OSPF

Open Shortest Path First (OSPF) is a link-state routing protocol which is used to find the best path between the source and the destination router using its own Shortest Path First). OSPF is developed by Internet Engineering Task Force (IETF) as one of the Interior Gateway Protocol (IGP), i.e, the protocol which aims at moving the packet within a large autonomous system or routing domain. It is a network layer protocol which works on the protocol number 89 and uses AD value 110. OSPF uses multicast address 224.0.0.5 for normal communication and 224.0.0.6 for update to designated router(DR)/Backup Designated Router (BDR)

OSPF terms –

Router I'd – It is the highest active IP address present on the router. First, highest loopback address is considered. If no loopback is configured then the highest active IP address on the interface of the router is considered.

Router priority – It is a 8 bit value assigned to a router operating OSPF, used to elect DR and BDR in a broadcast network.

Designated Router (DR) – It is elected to minimize the number of adjacency formed. DR distributes the LSAs to all the other routers. DR is elected in a broadcast network to which all the other routers shares their DBD. In a broadcast network, router requests for an update to DR and DR will respond to that request with an update.

Backup Designated Router (BDR) – BDR is backup to DR in a broadcast network. When DR goes down, BDR becomes DR and performs its functions.

BGP

Border Gateway Protocol (BGP) is used to Exchange routing information for the internet and is the protocol used between ISP which are different ASes.The protocol can connect together any internetwork of autonomous system using an arbitrary topology. The only requirement is that each AS have at least one router that is able to run BGP and that is router connect to at least one other AS's BGP router. BGP's main function is to exchange network reach-ability information with other BGP systems. Border Gateway Protocol constructs an autonomous systems' graph based on the information exchanged between BGP routers. Characteristics of Border Gateway Protocol (BGP):

- Inter-Autonomous System Configuration: The main role of BGP is to provide communication between two autonomous systems.
- BGP supports Next-Hop Paradigm.
- Coordination among multiple BGP speakers within the AS (Autonomous System).
- Path Information: BGP advertisement also include path information, along with the reachable destination and next destination pair.
- Policy Support: BGP can implement policies that can be configured by the administrator. For ex:- a router running BGP can be configured to distinguish between the routes that are known within the AS and that which are known from outside the AS.
- Runs Over TCP.
- BGP conserve network Bandwidth.
- BGP supports CIDR.
- BGP also supports Security.

IGRP

Interior Gateway Routing Protocol (IGRP) is a distance vector interior gateway protocol (IGP) developed by Cisco. It is used by routers to exchange routing data within an autonomous system. IGRP is a proprietary protocol. IGRP was created in part to overcome the limitations of RIP (maximum hop count of only 15, and a single routing metric) when used within large networks. IGRP supports multiple metrics for each route, including bandwidth, delay, load, and reliability; to compare two routes these metrics are combined together into a single metric, using a formula which can be adjusted through the use of pre-set constants. By default, the IGRP composite metric is a sum of the segment delays and the lowest segment bandwidth. The maximum configurable hop count of IGRP-routed packets is 255 (default 100), and routing updates are broadcast every 90 seconds (by default). IGRP uses protocol number 9 for communication. IGRP is considered a classful routing protocol. Because the protocol has no field for a subnet mask, the router assumes that all subnetwork addresses within the same Class A, Class B, or Class C network have the same subnet mask as the subnet mask configured for the interfaces in question. This contrasts with classless routing protocols that can use variable length subnet masks. Classful protocols have become less popular as they are wasteful of IP address space.

EIGRP

Enhanced Interior Gateway Routing Protocol (EIGRP) is a dynamic routing Protocol which is used to find the best path between any two layer 3 device to deliver the packet. EIGRP works on network layer Protocol of osi model and uses the protocol number 88.It uses metric to find out best path between two layer 3 device (router or layer 3 switch) operating EIGRP. It uses some messages to communicate with the neighbour devices that operates EIGRP. These are :-

Hello message- These messages are keep alive messages which are exchanged between two devices operating EIGRP. These messages are used for neighbor discovery/recovery, if there is any device operating EIGRP or if any device(operating EIGRP) coming up again. These messages are used for neighbor discovery if multicast at 224.0.0.10. It contains values like AS number, k values etc. These messages are used as acknowledgment when unicast. A hello with no data is used as the acknowledgment.

NULL update-It is used to calculate SRTT(Smooth Round Trip Timer) and RTO(Retransmission Time Out).

SRTT:The time is taken by a packet to reach neighboring router and the acknowledgment of the packet to reach to the local router.

RTO: If a multicast fails then unicast are being sent to that router. RTO is the time for which the local router waits for an acknowledgment of the packet.

Full Update – After exchanging hello messages or after the neighbourship is formed, these messages are exchanged. This message contains all the best routes.

Partial update-These messages are exchanged when there is a topology change and new links are added. It contains only the new routes, not all the routes. These messages are multicast.

Query message-These messages are multicast when the device is declared dead and it has no routes to it in its topology table.

Reply message – These messages are the acknowledgment of the query message sent to the originator of the query message stating the route to the network which has been asked in the query message.
Acknowledgement message
It is used to acknowledge EIGRP update, queries, and replies. Acks are hello packets that contain no data.
Note:- Hello, and acknowledgment packets do not require any acknowledgment.
Reply, query, update messages are reliable messages i.e requires acknowledgement.

6. How connection is established and released in TCP. Explain Token Bucket algorithm.

Connection establishment:

To establish a connection, TCP uses a three-way handshake. Before a client attempts to connect with a server, the server must first bind to and listen at a port to open it up for connections: this is called a passive open. Once the passive open is established, a client may initiate an active open. To establish a connection, the three-way (or 3-step) handshake occurs:

1. SYN: The active open is performed by the client sending a SYN to the server. The client/host A (see figure below) sets the segment's sequence number to a random value X.
2. SYN-ACK: In response, the server/host B replies with a SYN-ACK. The acknowledgment number is set to one more than the received sequence number (X + 1), and the sequence number that the server/host B chooses for the packet is another random number, Y.
3. ACK: Finally, the client/host A sends an ACK back to the server/host B. The sequence number is set to the received acknowledgement value i.e. X + 1, and the acknowledgement number is set to one more than the received sequence number i.e. Y + 1.

At this point, both the client and server have received an acknowledgment of the connection. The steps 1, 2 establish the connection parameter (sequence number) for one direction and it is acknowledged. The steps 2, 3 establish the connection parameter

(sequence number) for the other direction and it is acknowledged. With these, a full-duplex communication is established.

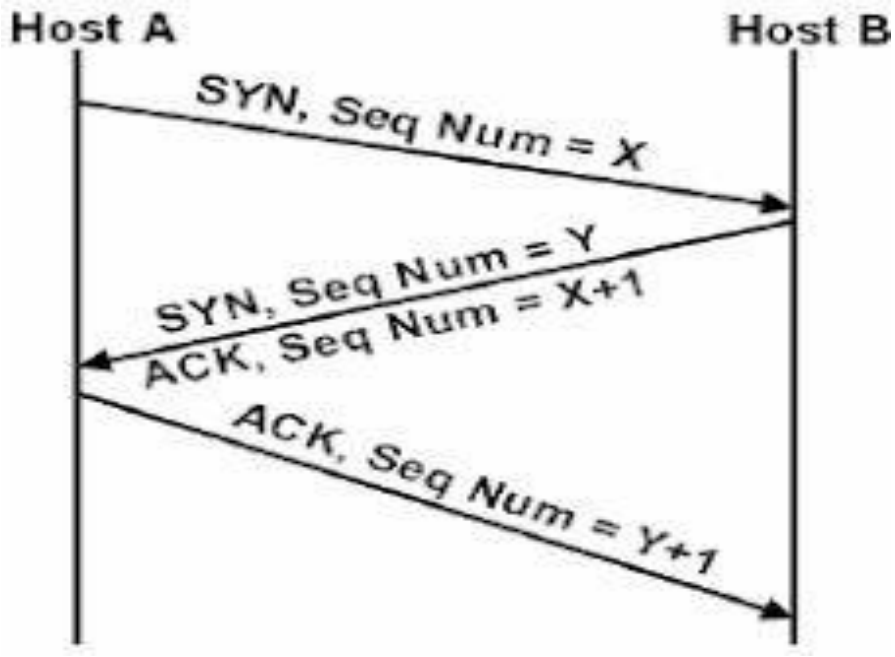


Figure: Tcp connection establishment

Connection termination:

The connection termination phase uses a four-way handshake, with each side of the connection terminating independently. When an endpoint wishes to stop its half of the connection, it transmits a FIN packet, which the other end acknowledges with an ACK. Therefore, a typical tear-down requires a pair of FIN and ACK segments from each TCP endpoint. After both FIN/ACK exchanges are concluded, the side which sent the first FIN before receiving one waits for a timeout before finally closing the connection, during which time the local port is unavailable for new connections; this prevents confusion due to delayed packets being delivered during subsequent connections.

A connection can be “half-open”, in which case one side has terminated its end, but the other has not. The side that has terminated can no longer send any data into the connection, but the other side can. The terminating side should continue reading the data until the other side terminates as well.

It is also possible to terminate the connection by a 3-way handshake, when host A sends a FIN and host B replies with a FIN & ACK (merely combines 2 steps into one) and host A replies with an ACK. This is perhaps the most common method.

It is possible for both hosts to send FINs simultaneously then both just have to ACK. This could possibly be considered a 2-way handshake since the FIN/ACK sequence is done in parallel for both directions.

Some host TCP stacks may implement a half-duplex close sequence, as Linux or HP-UX do. If such a host actively closes a connection but still has not read all the incoming data the stack already received from the link, this host sends a RST instead of a FIN. This allows a TCP application to be sure the remote application has read all the data the former sent—waiting the FIN from the remote side, when it actively closes the connection. However, the remote TCP stack cannot distinguish between a Connection Aborting RST and this Data Loss RST. Both cause the remote stack to throw away all the data it received, but that the application still didn't read.

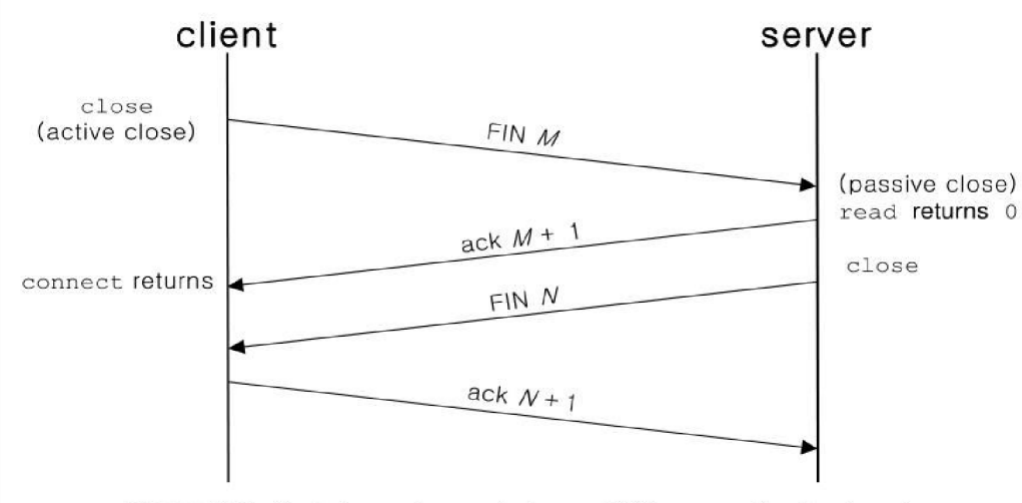


Figure: Tcp connection termination

Token Bucket Algorithm:

- Host is connected to the network by an interface. This interface is actually a bucket. A token is generated in the bucket every ΔT seconds.
- The host sends an unregulated flow to the bucket. For a packet to be transmitted to the network, it must capture and destroy a token present in the bucket.
- If the lost is not sending packets to the bucket the tokens keep getting accumulated in the bucket. Generally there is a maximum amount of tokens that can be accumulated in the bucket.
- Due to this feature of tokens getting accumulated, bursts can be handled better. Therefore in this case the rate increases if tokens are saved in the bucket, whereas in leaky bucket the rate will always be constant (1 packet per clock tick).

Token bucket Algorithm

Need of token bucket Algorithm:-

The leaky bucket algorithm enforces output pattern at the average rate, no matter how bursty the traffic is. So in order to deal with bursty traffic we need a flexible algorithm so that the data is not lost. One such algorithm is token bucket algorithm.

Steps of this algorithm can be described as follows:

1. In regular intervals tokens are thrown into the bucket.
2. The bucket has a maximum capacity.
3. If there is a ready packet, a token is removed from the bucket, and the packet is sent.
4. If there is no token in the bucket, the packet cannot be sent.

For example:

In figure (A) we see a bucket holding three tokens, with five packets waiting to be transmitted. For a packet to be transmitted, it must capture and destroy one token. In figure (B) We see that three of the five packets have gotten through, but the other two are stuck waiting for more tokens to be generated.

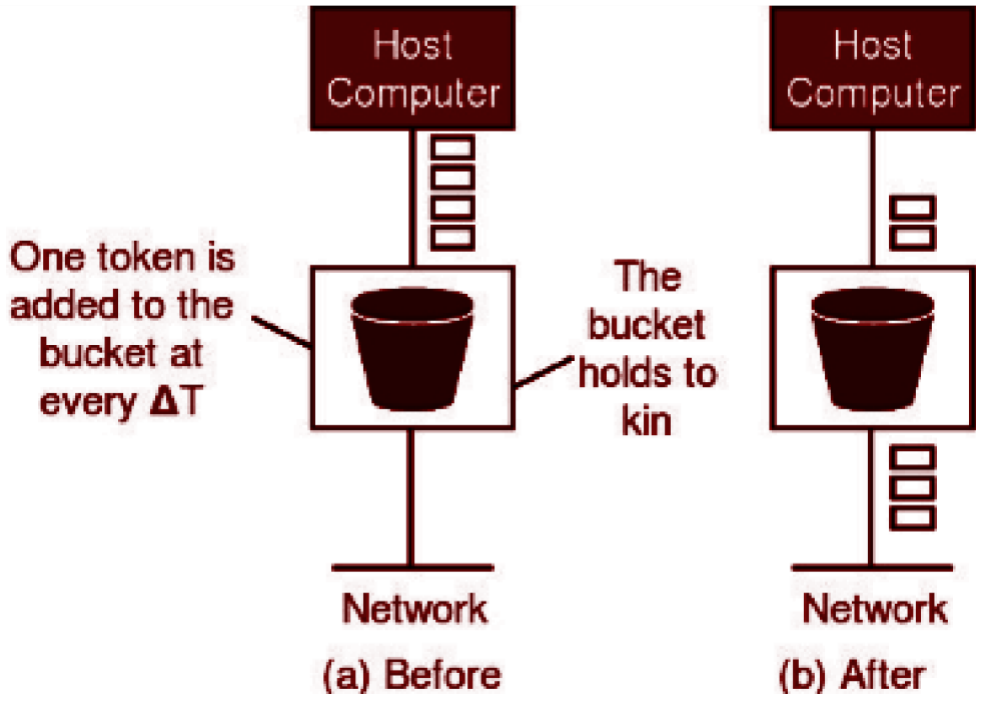


Figure: The token bucket algorithm before and after

7. Which protocols are used in sending and receiving email? Illustrate with necessary figure. Give a comparison of POP3 and IMAP.

For sending and receiving an email, SMTP (Simple Mail Transfer Protocol) is a widely used push protocol.

SMTP Fundamentals

SMTP is an application layer protocol. The client who wants to send the mail opens a TCP connection to the SMTP server and then sends the mail across the connection. The SMTP server is always on listening mode. As soon as it listens for a TCP connection from any client, the SMTP process initiates a connection on that port (25). After successfully establishing the TCP connection the client process sends the mail instantly.

SMTP Protocol

The SMTP model is of two types :

1. End-to- end method
2. Store-and- forward method

The end to end model is used to communicate between different organizations whereas the st

ore and forward method are used within an organization. A SMTP client who wants to send the m

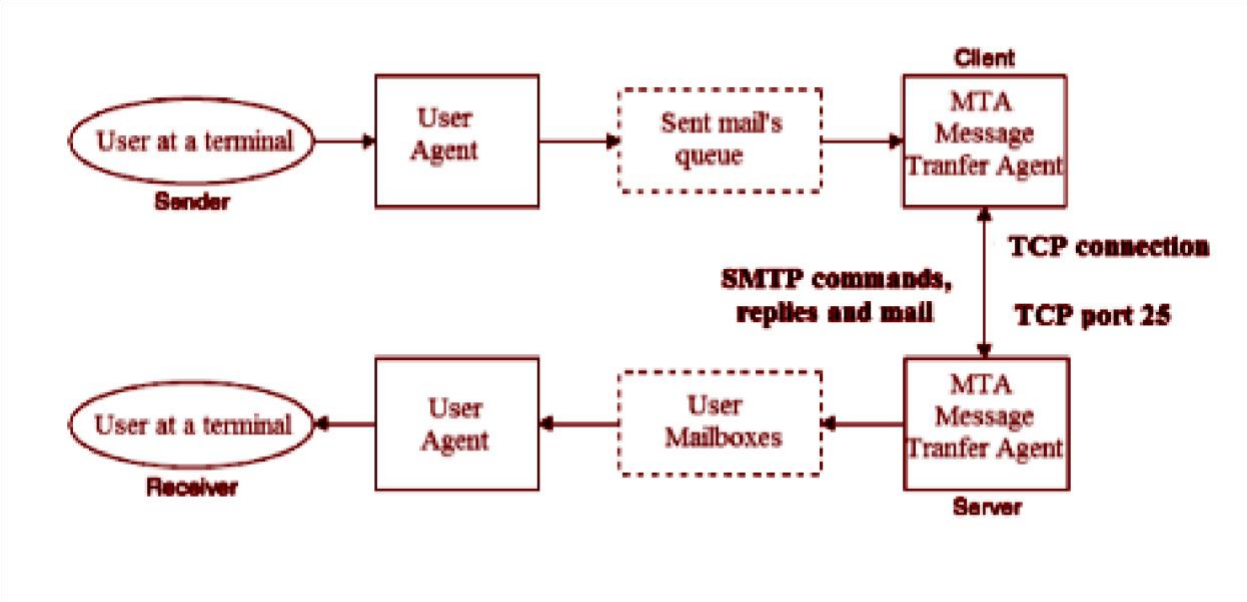
ail will contact the destination's host SMTP directly in order to send mail to the destination. The SMTP server will keep the mail to itself until it is successfully copied to the receiver's SMTP.

The client SMTP is the one which initiates the session let us call it the client- SMTP and the server SMTP is the one which responds to the session request and let us call it receiver-SMTP. The client- SMTP will start the session and the receiver-SMTP will respond to the request.

Model of SMTP system

In the SMTP model, user deals with the user agent (UA) for example Microsoft Outlook, Netscape, Mozilla, etc. In order to exchange the mail using TCP, MTA is used. The users sending the mail do not have to deal with the MTA it is the responsibility of the system admin to set up the local MTA. The MTA maintains a small queue of mails so that it can schedule repeat delivery of mail in case the receiver is not available. The

MTA delivers the mail to the mailboxes and the information can later be downloaded by the user agents.



The difference between IMAP and POP3 is given below:

IMAP VERSUS POP3

IMAP	POP3
IMAP is an acronym for Internet Message Access Protocol.	POP3 is short for Post Office Protocol Version 3.
The first IMAP was developed by Mark Crispin in 1986 as a potential alternative to POP.	The original POP was introduced in 1984 as a simple means to access emails on a remote server.
IMAP is an application layer internet standard protocol used when you need to access your emails from multiple devices.	POP3 is the latest version of the original email protocol used as a standardized method of delivering emails.
Any changes made on one device will be reflected on others.	Any changes made on one device won't be replicated on others.
Ideal for users who use multiple devices to access their emails.	Ideal for those who access their emails from one device and back up their drive regularly.

8. What are the factors that lead to the speedy development of IPv6? Define the process of transition

From IPv4 to IPv6.

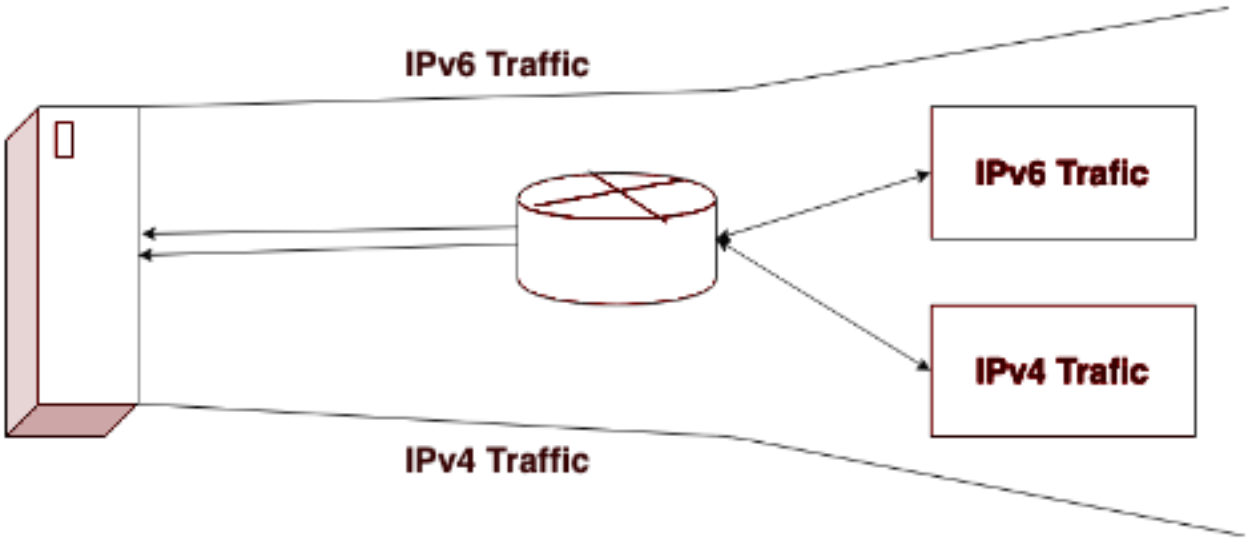
The current version of the Internet Protocol IPv4 was first developed in the 1970s, and the main protocol standard RFC 791 that governs IPv4 functionality was published in 1981. With the unprecedented expansion of Internet usage in recent years – especially by population dense countries like India and China, most of the IPv4 addresses have been used already.

This impending shortage of address space (availability) was recognized by 1992 as a serious limiting factor to the continued usage of the Internet run on IPv4. with this admirable foresight, there was a need of new set of protocol for the internet to continue functioning in future for more devices to come. Since, the old IPv4 protocol has 32 bits address space thus making it eligible to provide over 2^32= 4,294,967,296 unique addresses where first few addresses were already reserved, this reduced the total addresses available even lesser than it already was. The thought of exhaustion was slowly turning into reality when the Internet Engineering Task Force (IETF) initiated as early as in 1994, the design and development of a suite of protocols and standards now known as Internet Protocol Version 6 (IPv6), as a worthy tool to phase out and supplant IPv4 over the coming years. There is an explosion of sorts in the number and range of IP capable devices that are being released in the market and the usage of these by an increasingly tech savvy global population. The new protocol aims to effectively support the ever-expanding Internet usage and functionality, and also address security concerns with its 2^128 addresses which is too large to exhaust provided the address space is 128 bits that is 4 times larger than IPv4.

There are three strategies to map IPv4 to IPv6 : *Dual Stack Routers, Tunneling, and NAT Protocol Translation*. They are:

Dual Stack Routers:

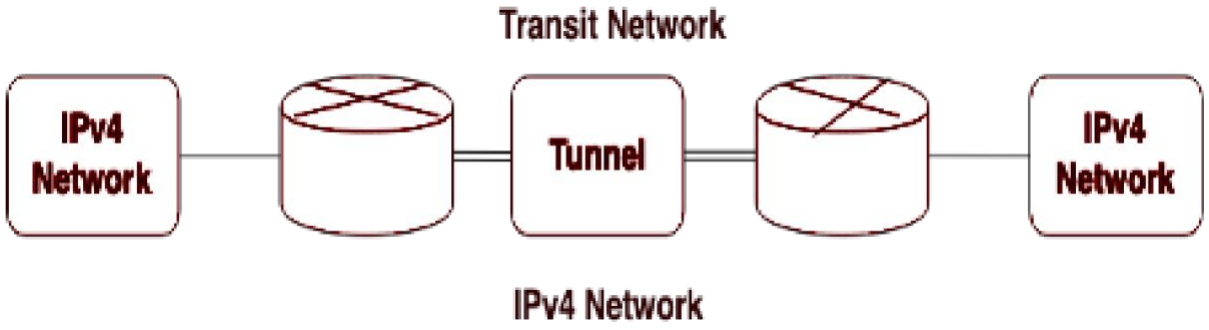
In dual stack router, a router's interface is attached with Ipv4 and IPv6 addresses configured is used in order to transition from IPv4 to IPv6.



In the above diagram, A given server with both IPv4 and IPv6 address configured can communicate with all hosts of IPv4 and IPv6 via dual stack router (DSR). The dual stack router (DSR) gives the path for all the hosts to communicate with server without changing their IP addresses.

Tunneling:

Tunneling is used as a medium to communicate the transit network with the different IP versions.

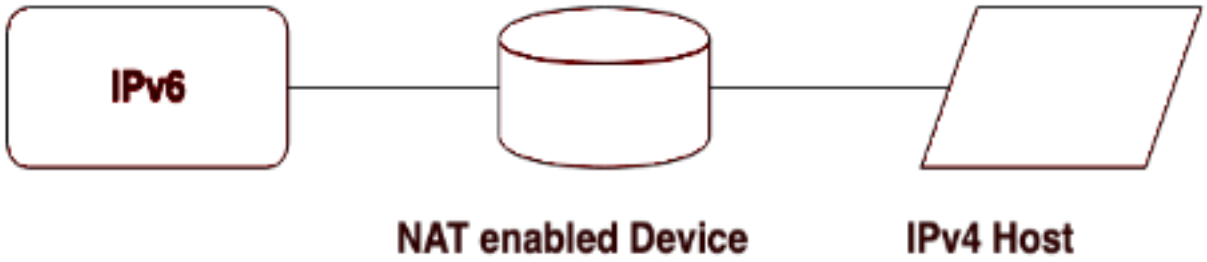


In the above diagram, the different IP versions such as IPv4 and IPv6 are present. The IPv4 networks can communicate with the transit or intermediate network on IPv6 with the help of Tunnel. It's also possible that the IPv6 network can also communicate with IPv4 networks with the help of Tunnel.

NAT Protocol Translation:

By the help of NAT Protocol Translation technique, the IPv4 and IPv6 networks can also communicate with each other which do not understand the address of different IP version.

Generally, an IP version doesn't understand the address of different IP version, for the solution of this problem we use NAT-PT device which remove the header of first (sender) IP version address and add the second (receiver) IP version address so that the Receiver IP version address understand that the request is send by the same IP version, and its vice-versa is also possible.



In the above diagram, an IPv4 address communicates with the IPv6 address via NAT-PT device to communicate easily. In this situation IPv6 address understand that the request is sent by the same IP version (IPv6) and it responds.

9. Define types of Encryption used in security. How PGP can secure email communication?

There are two types of encryption in widespread use : symmetric and asymmetric encryption. The name derives from whether or not the same key is used for encryption and decryption.

Symmetric encryption: -

In symmetric encryption the same key is used for encryption and decryption. It is therefore critical that a secure method is considered to transfer the key between sender and recipient. there is only one key, and all communicating parties use the same key for

encryption and decryption.

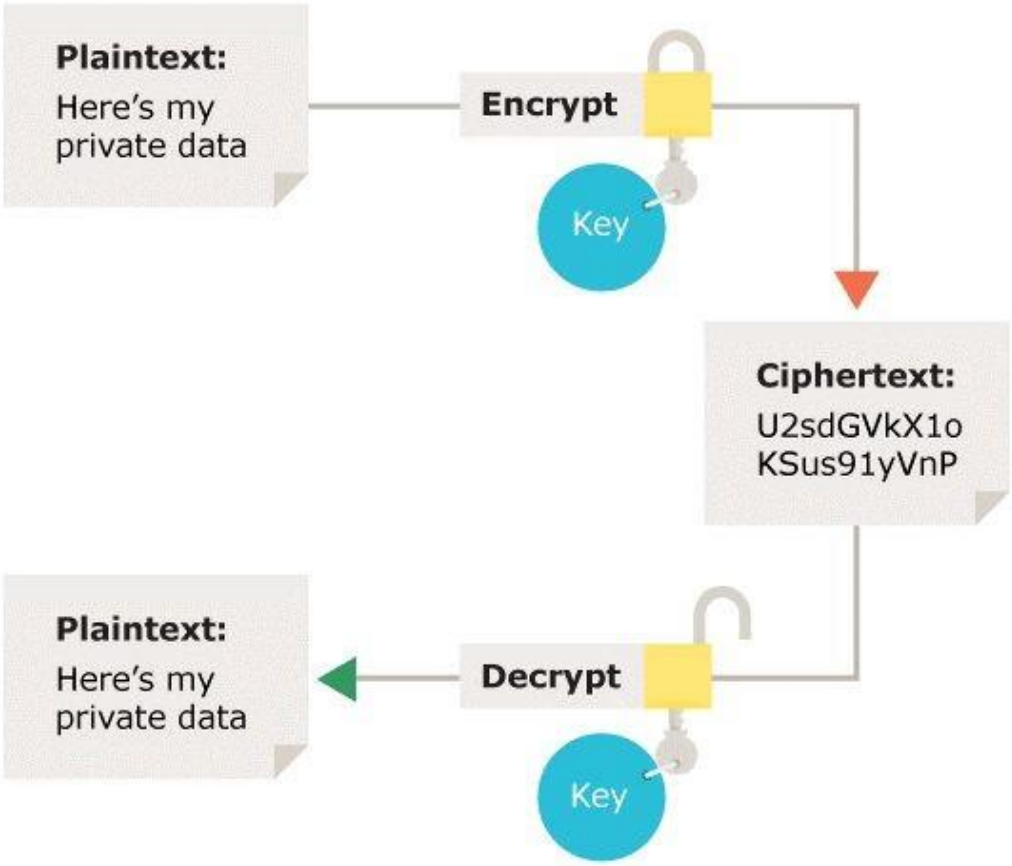


Figure 2: Symmetric encryption – Using the same key for encryption and decryption

Asymmetric encryption: -

Asymmetric encryption uses the notion of a key pair: a different key is used for the encryption and decryption process. One of the keys is typically known as the private key and the other is known as the public key. Either key can be used for either action, but data encrypted with the first key can only be decrypted with the second key, and vice versa. One key is kept private, while one key is shared publicly, for anyone to use – hence the "public key" name.

The private key is kept secret by the owner and the public key is either shared amongst authorised recipients or made available to the public at large.

Data encrypted with the recipient's public key can only be decrypted with the corresponding private key. Data can therefore be transferred without the risk of unauthorised or unlawful access to the data.

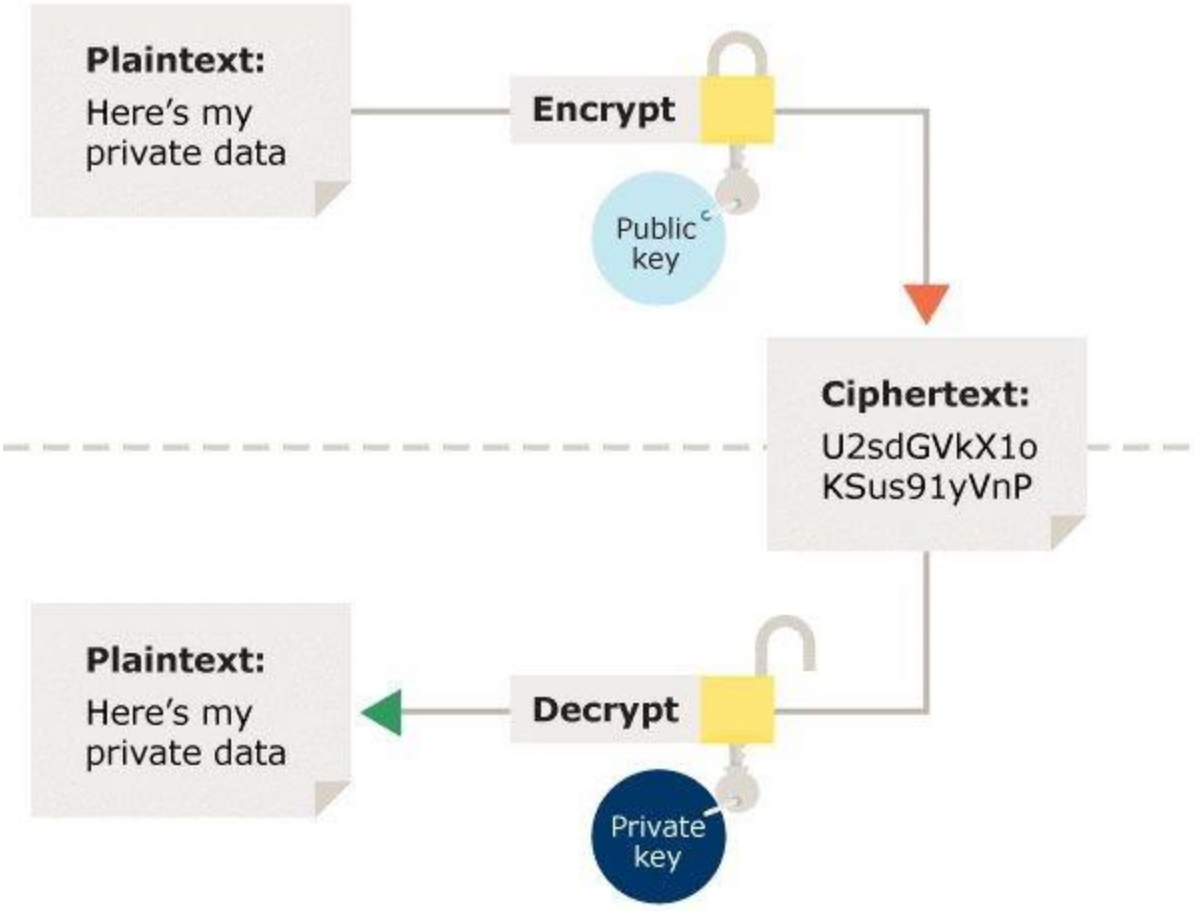


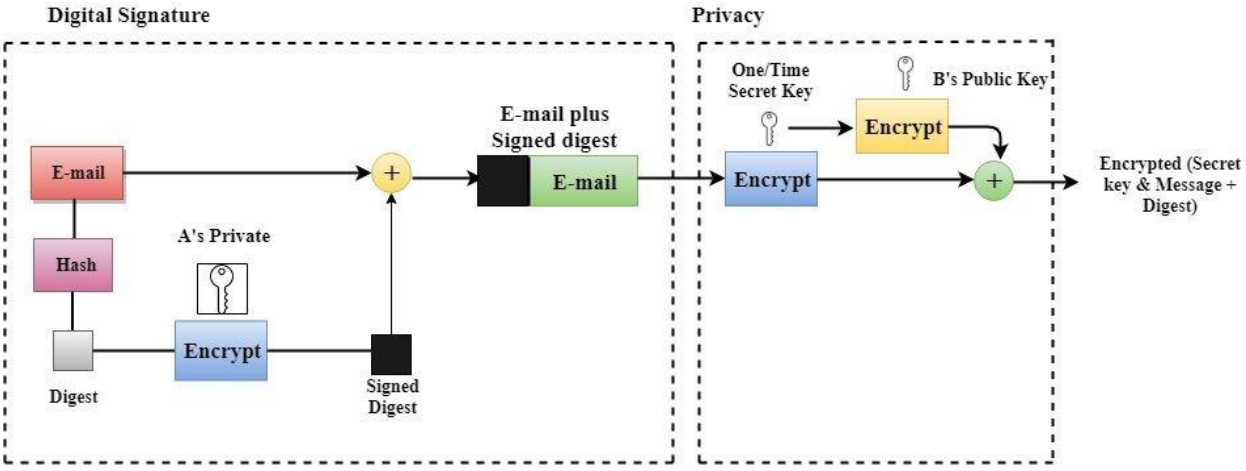
Figure 3: Asymmetric encryption – Using a different key for the encryption and decryption process

Pretty Good Privacy (PGP) was designed to provide all four aspects of security, i.e., privacy, integrity, authentication, and non-repudiation in the sending of email. PGP uses a digital signature (a combination of hashing and public key encryption) to provide integrity, authentication, and non-repudiation. PGP uses a combination of secret key encryption and public key encryption to provide privacy. Therefore, we can say that the digital signature uses one hash function, one secret key, and two private-public key pairs. PGP is an open source and freely available software package for email security. It provides confidentiality through the use of symmetric block encryption. It provides compression by using the ZIP algorithm, and EMAIL compatibility using the radix-64 encoding scheme. steps taken by PGP to create secure email at the sender site:

- The e-mail message is hashed by using a hashing function to create a digest.

- The digest is then encrypted to form a signed digest by using the sender's private key, and then signed digest is added to the original email message.
- The original message and signed digest are encrypted by using a one-time secret key created by the sender.
- The secret key is encrypted by using a receiver's public key.
- Both the encrypted secret key and the encrypted combination of message and digest are sent together.

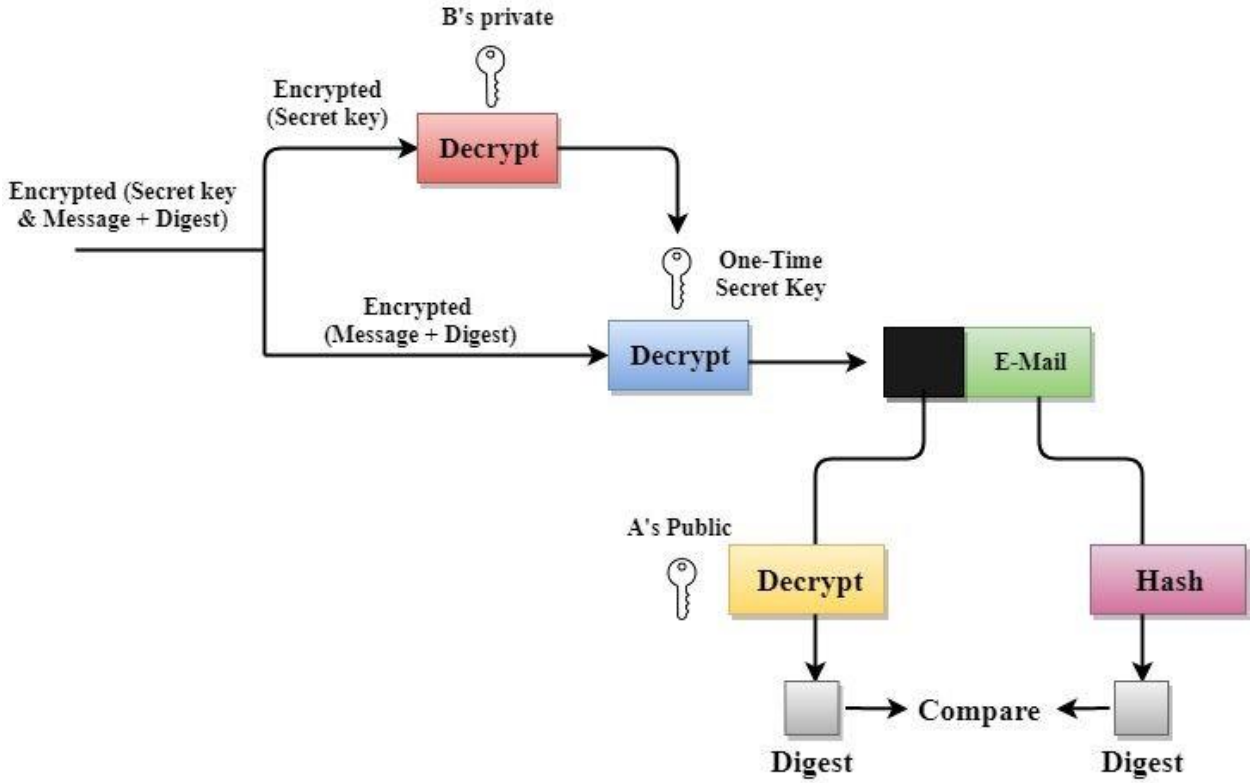
PGP at the Sender site (A)



Steps taken to show how PGP uses hashing and a combination of three keys to generate the original message:

- The receiver receives the combination of encrypted secret key and message digest is received.
- The encrypted secret key is decrypted by using the sender's private key to get the one-time secret key.
- The secret key is then used to decrypt the combination of message and digest.
- The digest is decrypted by using the sender's public key, and the original message is hashed by using a hash function to create a digest.
- Both the digests are compared if both of them are equal means that all the aspects of security are preserved.

PGP at the Receiver site (B)



10. Write short notes on: (any two)

I. Types of firewalls

A firewall is a part of a computer system or a network that is used to filter traffic on a network. Firewalls can be used to separate network nodes from external traffic sources, internal traffic sources, or even specific applications. Firewalls can be software, hardware, or cloud-based, with each type of firewall having its own unique pros and cons. The different types of firewall includes :

A. Packet Filtering Firewall: -

A packet filtering firewall applies a set of rules to each incoming and outgoing IP packetand then forwards or discards the packet. Filtering rules are based on information contained in a network packet. It is the simplest type of firewall. Dealing with each individual packet, the firewall applies its set of rules to determine the packets to be allowed or not.

- Source IP address
- Destination IP address
- Source and destination transport level address
- IP protocol field
- Interface

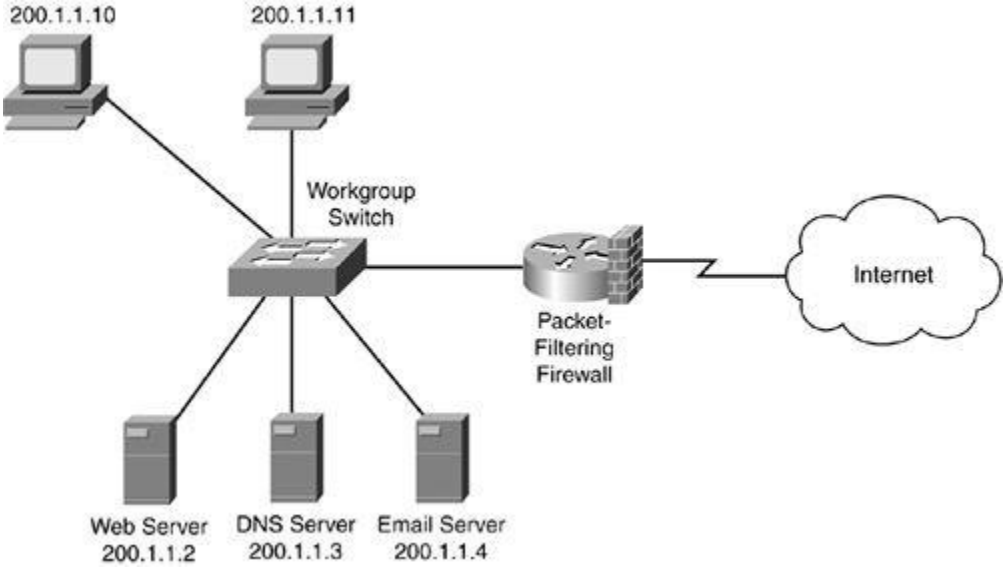


Fig: packet filtering firewall

Two default policies are there to take default action to determine whether to forward or discard the packet. Default = discard Default = forward Some possible attacks on firewall :

- IP address spoofing
- Source routing attacks
- Tiny fragment attacks

B. Application Proxy Firewall: -

In application proxy firewall, filtering is based on specific application data. An application – level gateway, also called an application proxy, acts as a reply of application – level traffic. The user requests service from proxy and the proxy validates request as legal. Then actions request and returns result to user. It can log / audit traffic at application level.

Filtering decision is based on variety of triggers:

- Source or destination address
- Contents of application (content filtering)

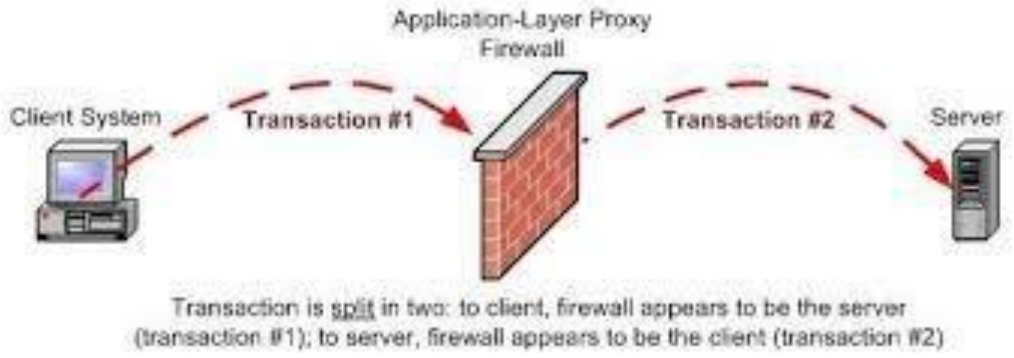


Fig: Application proxy firewall

Application Proxy Firewall Advantage :

- More secure than packet filter firewalls
- Easy to log and audit incoming traffic Disadvantage :

Additional processing overhead on each connection

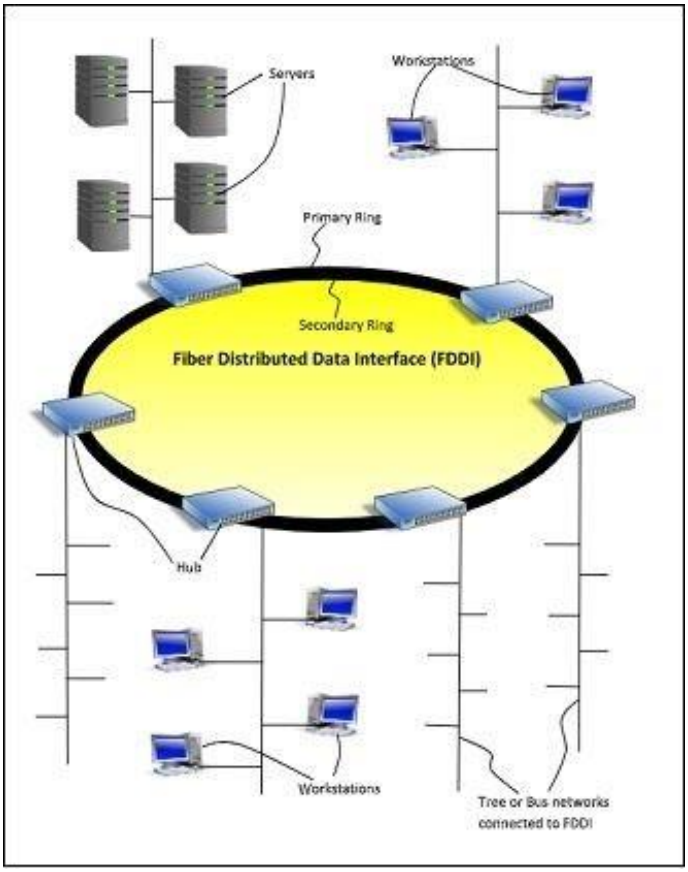
ii. FDDI

Fiber Distributed Data Interface (FDDI) is a set of ANSI and ISO standards for transmission of data in a local area network (LAN) over fiber optic cables. It is applicable in large LANs that can extend up to 200 kilometers in diameter.

Features

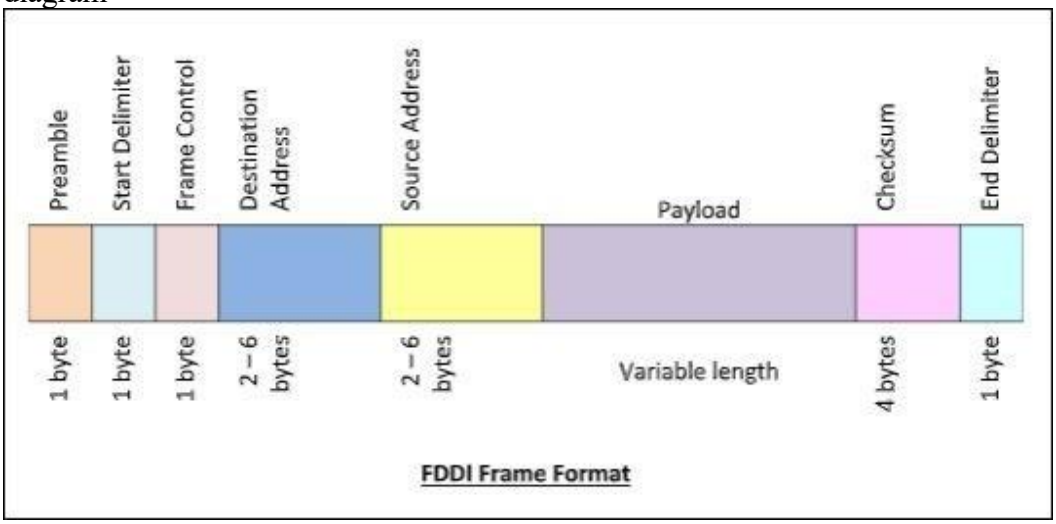
- FDDI uses optical fiber as its physical medium.
- It operates in the physical and medium access control (MAC layer) of the Open Systems Interconnection (OSI) network model.
- It provides high data rate of 100 Mbps and can support thousands of users.
- It is used in LANs up to 200 kilometers for long distance voice and multimedia communication.
- It uses ring based token passing mechanism and is derived from IEEE 802.4 token bus standard.
- It contains two token rings, a primary ring for data and token transmission and a secondary ring that provides backup if the primary ring fails.
- FDDI technology can also be used as a backbone for a wide area network (WAN).

The following diagram shows FDDI −



Frame Format

The frame format of FDDI is similar to that of token bus as shown in the following diagram −



The fields of an FDDI frame are −

- Preamble: 1 byte for synchronization.

- Start Delimiter: 1 byte that marks the beginning of the frame.
- Frame Control: 1 byte that specifies whether this is a data frame or control frame.

- Destination Address: 2-6 bytes that specifies address of destination station.
- Source Address: 2-6 bytes that specifies address of source station.
- Payload: A variable length field that carries the data from the network layer.

- Checksum: 4 bytes frame check sequence for error detection.
- End Delimiter: 1 byte that marks the end of the frame.

2075 ASHWIN

Q.1.Why layering is important? Explain design issues for layers in details. Mention service primitives for implementing connection oriented service.

Ans: The Reasons for a Layering in network are:-

Change: When changes are made to one layer, the impact on the other layers is minimized. If the model consists of a single, all-encompassing layer, any change affects the entire model.

Design: A layered model defines each layer separately. As long as the interconnections between layers remain constant, protocol designers can specialize in one area (layer) without worrying about how any new implementations affect other layers.

Learning: The layered approach reduces a very complex set of topics, activities, and actions into several smaller, interrelated groupings. This makes learning and understanding the actions of each layer and the model generally much easier.

Troubleshooting: The protocols, actions, and data contained in each layer of the model relate only to the purpose of that layer. This enables troubleshooting efforts to be pinpointed on the layer that carries out the suspected cause of the problem.

A number of design issues exist for the layer to layer approach of computer networks. Some of the main design issues are as follows:

Reliability

Network channels and components may be unreliable, resulting in loss of bits while data transfer. So, an important design issue is to make sure that the information transferred is not distorted.

Scalability

Networks are continuously evolving. The sizes are continually increasing leading to congestion. Also, when new technologies are applied to the added components, it may lead to incompatibility issues. Hence, the design should be done so that the networks are scalable and can accommodate such additions and alterations.

Error Control

Unreliable channels introduce a number of errors in the data streams that are communicated. So, the layers need to agree upon common error detection and error correction methods so as to protect data packets while they are transferred.

Resource Allocation

Computer networks provide services in the form of network resources to the end users. The main design issue is to allocate and deallocate resources to processes. The allocation/deallocation should occur so that minimal interference among the hosts occurs and there is optimal usage of the resources.

Routing

There may be multiple paths from the source to the destination. Routing involves choosing an optimal path among all possible paths, in terms of cost and time. There are several routing algorithms that are used in network systems.

Security

A major factor of data communication is to defend it against threats like eavesdropping and surreptitious alteration of messages. So, there should be adequate mechanisms to prevent unauthorized access to data through authentication and cryptography.

There are five types of service primitives for implementing connection oriented service:-

1. LISTEN : When a server is ready to accept an incoming connection it executes the LISTEN primitive. It blocks waiting for an incoming connection.
2. CONNECT : It connects the server by establishing a connection. Response is awaited.
3. RECIEVE: Then the RECIEVE call blocks the server.
4. SEND : Then the client executes SEND primitive to transmit its request followed by the execution of RECIEVE to get the reply. Send the message.
5. DISCONNECT : This primitive is used for terminating the connection. After this primitive one can't send any message. When the client sends DISCONNECT packet then the server also sends the DISCONNECT packet to acknowledge the client.

Q.2. Compare circuit switching and packet switching. Explain ISDN channels with architecture.

Ans:

Circuit Switching	Packet Switching
1. Physical path between source and destination.	1.No physical path.
2. All packets use same path.	2. Packet travels independently.
3. Reserve entire bandwidth in advance.	3.Does not reserve bandwidth.
4. Bandwidth wastage.	4. No Bandwidth wastage.
5. No store and forward transmission.	5.Supports store and forward transmission.
6. Guaranteed capacity.	6. No guarantees.

ISDN Channels with architecture:-

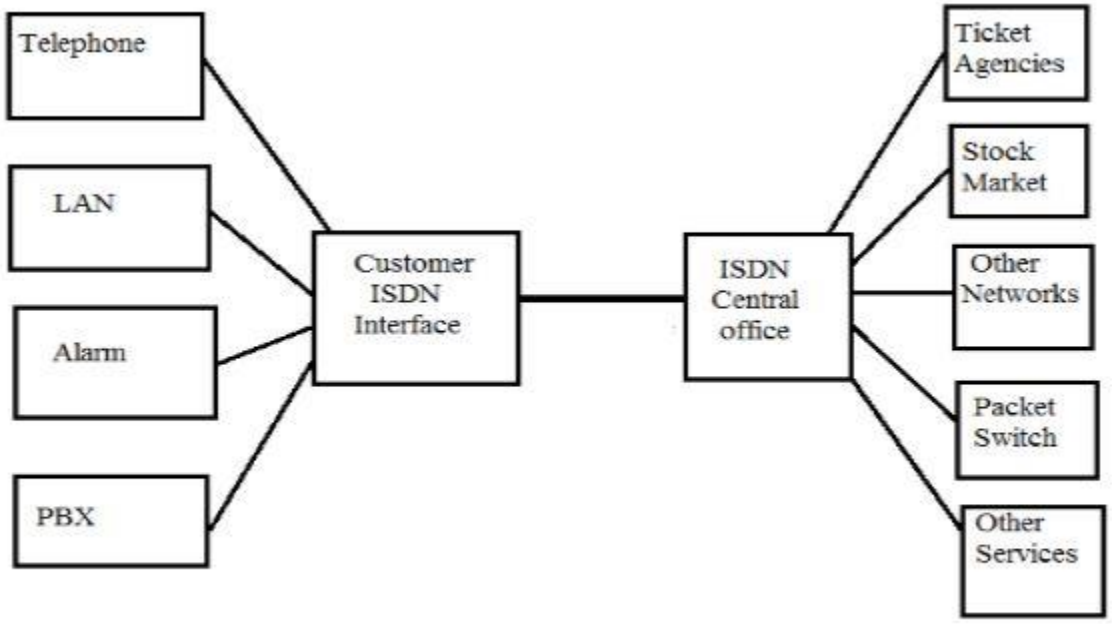


Fig no.2: Architecture of ISDN

ISDN is a network concept providing a integration of data, voice and video. Its based on 64Kbps digital Communication channel. ISDN is a generic term for any network which connects homes and business together with a service companies. Telephone network requires two basic functions:

(i) Signaling –To establish and realize a call.

(ii) End-to-end transmission – To transfer the information between the users

ISDN uses these functions as separate and indeed provide different channels for these services. This is done through proper interface. The purpose is to provide access to various services that are possibly supported by different networks. The base rate interface (BRI) provides the users with two 64Kbps barrier (B) channels and one 16Kbps data (D) channels. The primary data rate interface (PRI) provides users with (23B+1D) channels in North America and Japan and (30B+1D) channels in Europe. Each B channel is bidirectional and provides 64Kbps end –to-end

digital connection that can carry PCM voice or data. The primary function of D channel is to carry information for B channels. Types of ISDN are:

(i) Narrow band ISDN

(ii) Broad band ISDN

Merits:

- An ISDN user can establish two simultaneously independent telecom calls on existing pair of telephone wires.
- Two simultaneously calls may be of any type such as speech, data, image, video.

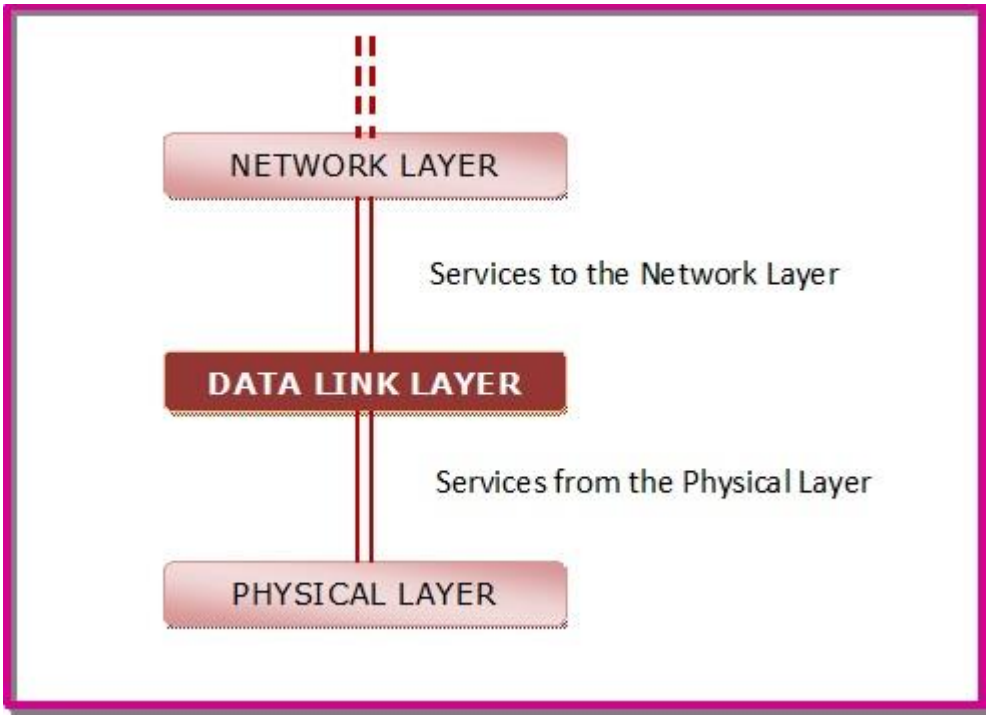
Q.3 State the various design issues for the data link layer. What is piggybacking? A bit string 01111011111101111110 needs to be transmitted at the data link layer. What is the string actually transmitted after bit stuffing?

Ans: The design issues of data link layer are

- Providing services to the network layer
- Framing
- Error Control
- Flow Control

Services to the Network Layer

In the OSI Model, each layer uses the services of the layer below it and provides services to the layer above it. The data link layer uses the services offered by the physical layer.The primary function of this layer is to provide a well defined service interface to network layer above it.



The types of services provided can be of three types −

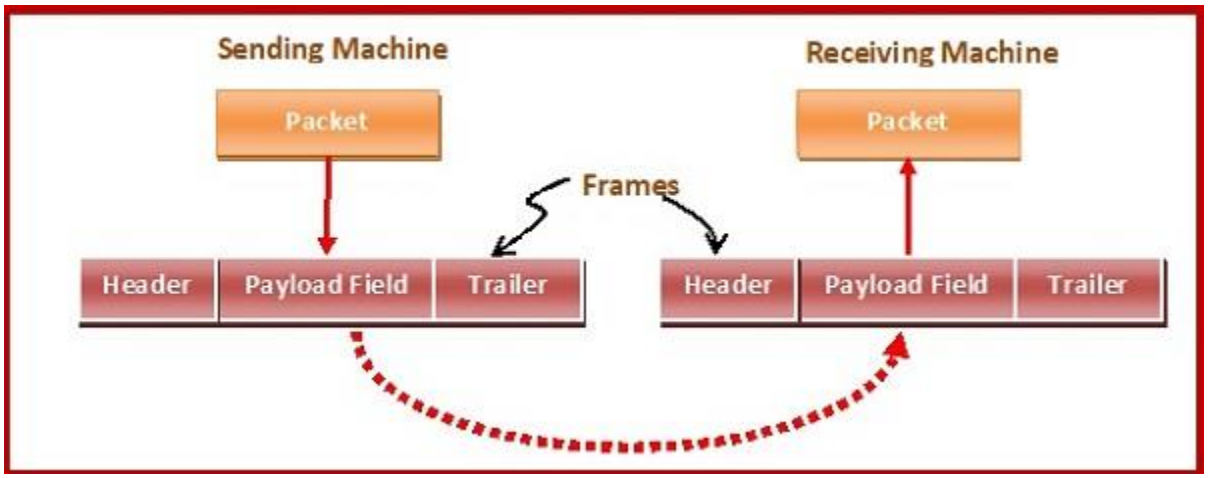
- Unacknowledged connectionless service
- Acknowledged connectionless service
- Acknowledged connection - oriented service

Framing

The data link layer encapsulates each data packet from the network layer into frames that are then transmitted.

A frame has three parts, namely −

- Frame Header
- Payload field that contains the data packet from network layer
- Trailer



Error Control

The data link layer ensures error free link for data transmission. The issues it caters to with respect to error control are −

- Dealing with transmission errors
- Sending acknowledgement frames in reliable connections
- Retransmitting lost frames
- Identifying duplicate frames and deleting them
- Controlling access to shared channels in case of broadcasting

Flow Control

The data link layer regulates flow control so that a fast sender does not drown a slow receiver. When the sender sends frames at very high speeds, a slow receiver may not be able to handle it. There will be frame losses even if the transmission is error-free. The two common approaches for flow control are −

- Feedback based flow control

- Rate based flow control

A technique called piggybacking is used to improve the efficiency of the bidirectional protocols. When a frame is carrying data from A to B, it can also carry control information about arrived (or lost) frames from B; when a frame is carrying data from B to A, it can also carry control information about the arrived (or lost) frames from A.

- The major advantage of piggybacking is better use of available channel bandwidth.
- The major disadvantage of piggybacking Additional complexity and If the data link layer waits too long before transmitting the acknowledgement, then re-transmission of frame would take place.

Here, the given string is as below:

01111011111101111110

After bit stuffing, the transmitted bit is as below:

011110111011011110110

Q.4. Why routing is essential in computer networking? Compare working of distance vector routing algorithm with link state routing algorithm.

Ans: Needs of routing in computer networking:-

- Routing is the hub around which all of IP connectivity revolves.
- At the simplest level, routing establishes basic internetwork communications, implements an addressing structure that uniquely identifies each device, and organizes individual devices into a hierarchical network structure.
- Traditionally, routers have also served as the media adapters that have connected remote offices to the headquarters via a WAN.
- The most recent trend, though, is to see routers as the integration platforms for a wide variety of network enhancements such as security, policy, and services that extend the capabilities of IP to support telephony, video, legacy service integration, and other applications over a converged network.

Comparison between distance vector routing algorithm and link state routing algorithm:-

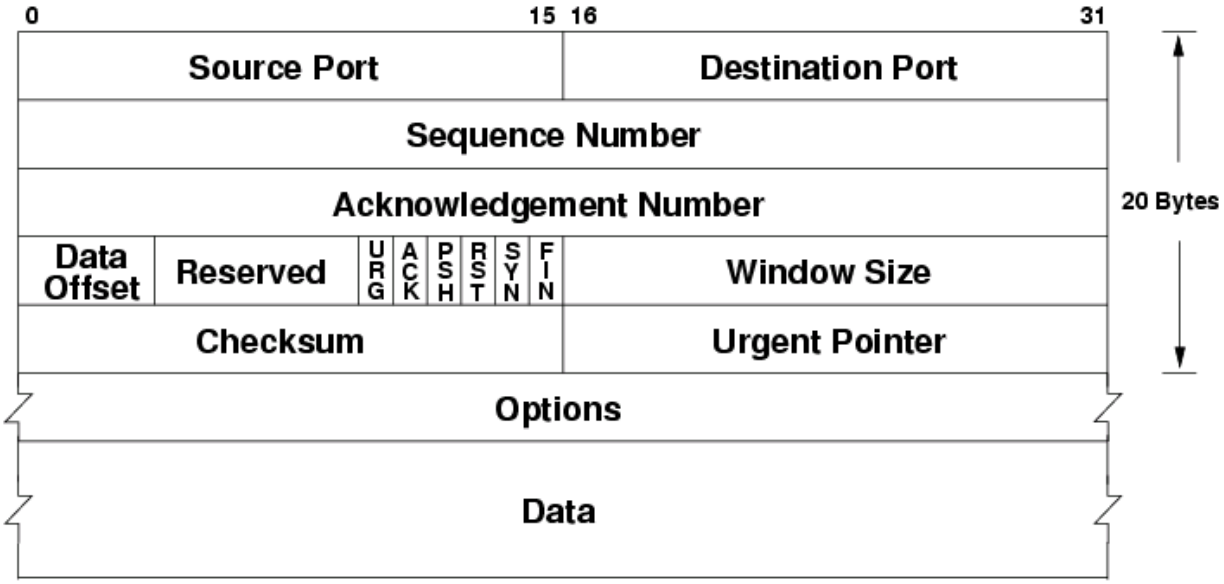
	DVA	LSA
Forwarding Table	A node sends to its neighbors the whole routing table (its distance vector).	A node sends to each the other one the case of the link with the current neighbors by a dependable flooding.
Route Updates	Are sent periodically or when a topological variation is observed.	Are sent periodically or when a topological or when a topological variation is observed.
Path computation	It is established on a distributed version of the classical bellman-ford algorithm (DBF)	A node can then make the chart of the network and can compute the path from itself to each other node independently.
Information generating	A node running a distance vector protocol does not know the network topology.	Because of flooding, all nodes eventually receive each the link-cases from each the other nodes of the network.
Topology Store	All node stores the neighbor's information at the end on the network topology.	
Topology Change	DVA protocols may poorly affect to a topology change ago, it endures from very low convergence (count-to-infinity problem) and may make provisional loops.	LSA converges faster than DVA but it needs a higher overhead.
Example	A well-known example of DVA is RIP	A well-known example of LSAis OOSPF.

Q.6 What are the differences between TCP and UDP services? Explain the TCP datagram format in detail.

Ans:

Transmission Control Protocol (TCP)	User Datagram Protocol (UDP)
TCP is a connection-oriented protocol.	UDP is not connection-oriented protocol.
TCP is reliable as it guarantees delivery of data to the destination router.	The delivery of data to the destination cannot be guaranteed in UDP.
TCP provides extensive error checking mechanisms.	UDP has only the basic error checking mechanism using checksums.
It has sequencing of data.	It doesn't have sequencing of data.
It is comparatively slower.	It is comparatively faster, simper and more efficient than TCP.
Retransmission of lost packets is possible	There is no retransmission of lost packets
TCP doesn't supports Broadcasting.	UDP supports Broadcasting.

The TCP datagram format can be explained as belows:



Header

The length of TCP header is minimum 20 bytes long and maximum 60 bytes.

• Source Port (16-bits) - It identifies source port of the application process on the sending device.

• Destination Port (16-bits) - It identifies destination port of the application process on the receiving device.

• Sequence Number (32-bits) - Sequence number of data bytes of a segment in a session.

• Acknowledgement Number (32-bits) - When ACK flag is set, this number contains the next sequence number of the data byte expected and works as acknowledgement of the previous data received.

- Data Offset (4-bits) - This field implies both, the size of TCP header (32-bit words) and the offset of data in current packet in the whole TCP segment.
- Reserved (3-bits) - Reserved for future use and all are set zero by default

- Flags (1-bit each)
  o NS - Nonce Sum bit is used by Explicit Congestion Notification signaling process.
  o CWR - When a host receives packet with ECE bit set, it sets Congestion Windows Reduced to acknowledge that ECE received.
  o ECE -It has two meanings:
  ▪ If SYN bit is clear to 0, then ECE means that the IP packet has its CE (congestion experience) bit set.

▪ If SYN bit is set to 1, ECE means that the device is ECT capable. o URG - It indicates that Urgent Pointer field has significant data and should be processed.
o ACK - It indicates that Acknowledgement field has significance. If ACK is cleared to 0, it indicates that packet does not contain any acknowledgement.
o PSH - When set, it is a request to the receiving station to PUSH data (as soon as it comes) to the receiving application without buffering it.
o RST - Reset flag has the following features:
▪ It is used to refuse an incoming connection.
▪ It is used to reject a segment. ▪ It is used to restart a connection.
o SYN - This flag is used to set up a connection between hosts.
o FIN - This flag is used to release a connection and no more data is exchanged thereafter. Because packets with SYN and FIN flags have sequence numbers, they are processed in correct order.
• Windows Size - This field is used for flow control between two stations and indicates the amount of buffer (in bytes) the receiver has allocated for a segment, i.e. how much data is the receiver expecting.
• Checksum - This field contains the checksum of Header, Data and Pseudo Headers.
• Urgent Pointer - It points to the urgent data byte if URG flag is set to 1.
• Options - It facilitates additional options which are not covered by the regular header. Option field is always described in 32-bit words. If this field contains data less than 32- bit, padding is used to cover the remaining bits to reach 32-bit boundary.

Q. 7 Define socket programming. How web server communication and file server communication are possible in network. Explain with used protocols.

Ans: Socket programming is a way of connecting two nodes on a network to communicate with each other. One socket(node) listens on a particular port at an IP, while other socket reaches out to the other to form a connection. Server forms the listener socket while client reaches out to the server.
Sockets provide the communication mechanism between two computers using TCP. A client program creates a socket on its end of the communication and attempts to connect that socket to a server. When the connection is made, the server creates a socket object on its end of the communication. The client and the server can now communicate by writing to and reading from the socket. The java.net.Socket class represents a socket, and the java.net.ServerSocket class provides a mechanism for the server program to listen for clients and establish connections with them.
The following steps occur when establishing a TCP connection between two computers using sockets –

• The server instantiates a ServerSocket object, denoting which port number communication is to occur on.

• The server invokes the accept () method of the ServerSocket class. This method waits until a client connects to the server on the given port.

• After the server is waiting, a client instantiates a Socket object, specifying the server name and the port number to connect to.

• The constructor of the Socket class attempts to connect the client to the specified server and the port number. If communication is established, the client now has a Socket object capable of communicating with the server.

• On the server side, the accept() method returns a reference to a new socket on the server that is connected to the client's socket.

After the connections are established, communication can occur using I/O streams. Each socket has both an OutputStream and an InputStream. The client's OutputStream is connected to the server's InputStream, and the client's InputStream is connected to the server's OutputStream. TCP is a two-way communication protocol, hence data can be sent across both streams at the same time. Following are the useful classes providing complete set of methods to implement sockets.

FTP The File Transfer Protocol (FTP) is a standard network protocol used to transfer computer files between a client and server on a computer network. FTP is built on client-server model architecture and uses separate control and data connections between the client and the server. File Transfer Protocol (FTP) is a standard Internet protocol for transmitting files between computers on the Internet over TCP/IP connections.

FTP is a client-server protocol that relies on two communications channels between client and server: a command channel for controlling the conversation and a data channel for transmitting file content. Clients initiate conversations with servers by requesting to download a file. Using FTP, a client can upload, download, delete, and rename, move and copy files on a server. A user typically needs to log on to the FTP server, although some servers make some or all of their content available without login, also known as anonymous FTP.

FTP sessions work in passive or active modes. In active mode, after a client initiates a session via a command channel request, the server initiates a data connection back to the client and begins transferring data. In passive mode, the server instead uses the command channel to send the client the information it needs to open a data channel. Because passive mode has the client initiating all connections, it works well across firewalls and Network Address Translation (NAT) gateways.

Q.8 What are the methods used to interoperate IPv6 and IPv4. Show IPv6 datagram format.

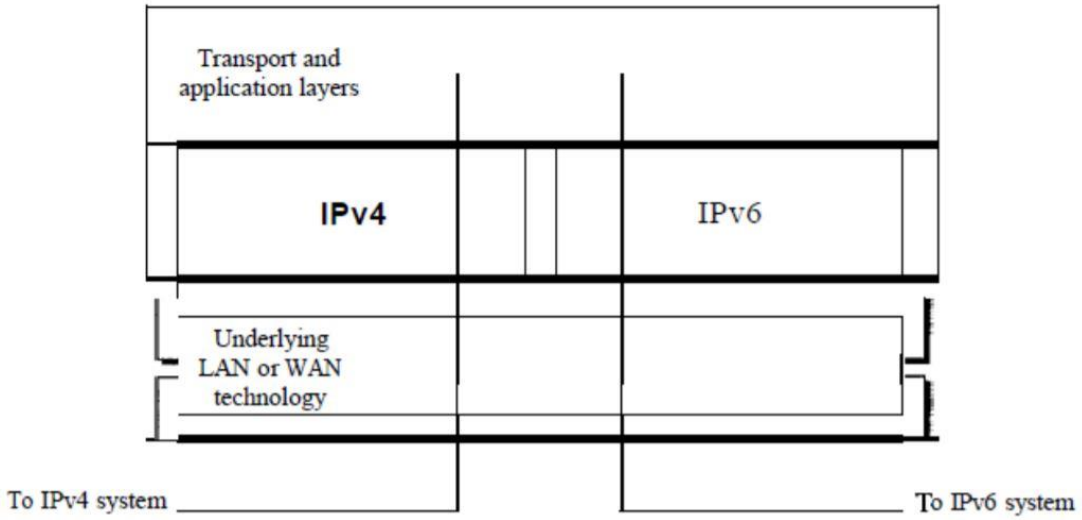
Ans: The methods used to interoperate IPv6 and IPv4 are:

i. Dual Stack

It is recommended that all hosts, before migrating completely to version 6, have a dual stack of protocols. In other words, a station must run IPv4 and IPv6 simultaneously untilall the Internet uses IPv6.

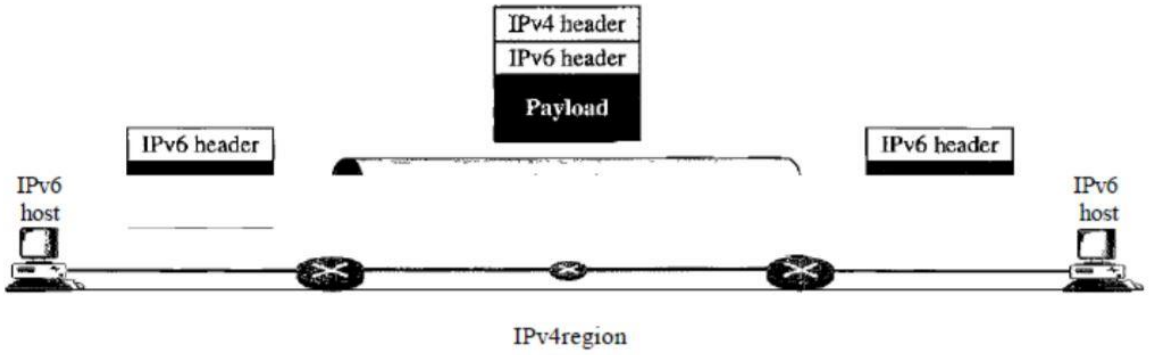
To determine which version to use when sending a packet to a destination, the source host queries the DNS. If the DNS returns an IPv4 address, the source host sends an IPv4

packet. If the DNS returns an IPv6 address, the source host sends an IPv6 packet.



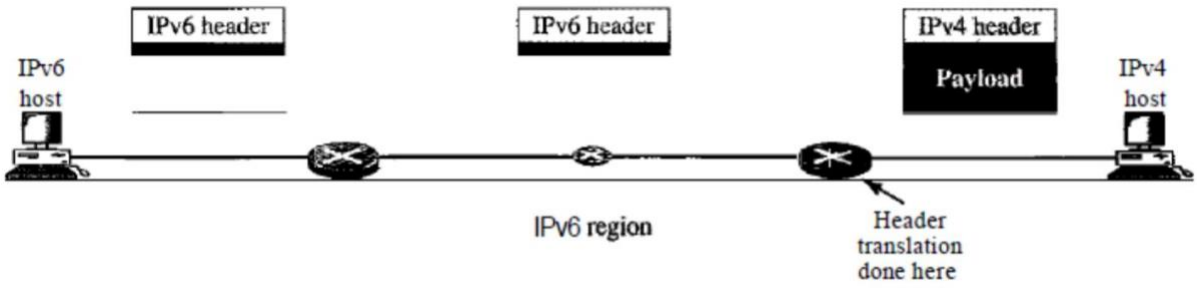
ii. Tunneling

Tunneling is a strategy used when two computers using IPv6 want to communicate with each other and the packet must pass through a region that uses IPv4. To pass through this region, the packet must have an IPv4 address. So the IPv6 packet is encapsulated in an IPv4 packet when it enters the region, and it leaves its capsule when it exits the region. It seems as if the IPv6 packet goes through a tunnel at one end and emerges at the other end. To make it clear that the IPv4 packet is carrying an IPv6 packet as data, the protocol value is set to 41.

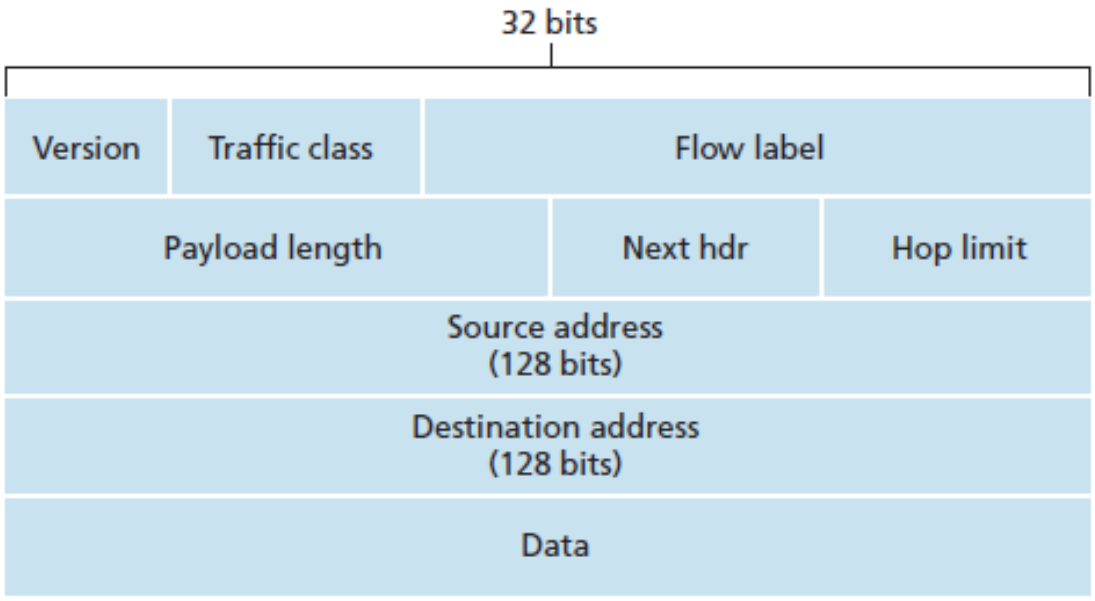


iii. Header Translation

Header translation is necessary when the majority of the Internet has moved to IPv6 but some systems still use IPv4. The sender wants to use IPv6, but the receiver does not understand IPv6. Tunneling does not work in this situation because the packet must be in the IPv4 format to be understood by the receiver. In this case, the header format must be totally changed through header translation. The header of the IPv6 packet is converted to an IPv4 header.



The IPv6 datagram format is as belows:



Q.9. What is VPN? Encrypt a message "network" using RSA algorithm.
Ans: A VPN, or Virtual Private Network, is a private network that encrypts and transmits data while it travels from one place to another on the internet. Using a VPN to connect to the internet allows you to surf websites privately and securely as well as gain access to restricted websites and overcome censorship blocks.
How does a VPN service work?

1. Once you connect to the internet with your VPN service switched on, you will be connected to one of the VPN provider's servers.
2. At the same time they will provide you with the IP address of that particular server. Instead of using your own IP address you are using one that belongs to the VPN provider.
3. Your internet connection is also encrypted between your device and the server you're connected to.
4. Hiding your IP address allows you to access the internet privately and helps to prevent your browsing from being tracked or traced. You are then able to surf the web privately and securely.

→ we got a message "network".

Here is no arithmetic operation we can perform with strings, so the message has to be converted into somethings, so let's say "network" is converted to integer ~~[illegible]~~ "till using some algorithm.

1. Choose 2 prime nos, p & q:

   p = 61 , q = 53

2. Compute: n = p × q = 61 × 53 = 3233

3. $\phi(n) = \phi(p \times q) = \phi(p) \times \phi(q)$
   $= (p-1) \times (q-1)$
   $= 60 \times 52$
   $= 3120$

4. Choose 'e'; $1 \leq e < \phi(n)$, coprime to $\phi(n)$
   Let e = 17

   ∴ (e, n) = publickey(17, 3233)

5. Determine 'd' as $ed = 1 \bmod \phi(n)$
   $d = e^{-1} \bmod \phi(n)$

   ⇒ $17 \times d = 1 \bmod 3120$

Finding d

$ed = 1 \bmod \phi(n)$

$d = \frac{(\phi(n) * i) + 1}{e}$

$d = \frac{(3120 * 1) + 1}{17}$

$= 183.58$

$d = \frac{(3120 * 2) + 1}{17}$

$= 367.11$

$d = \frac{(3120 * 3) + 1}{17}$

$= 550.64$

$d = \frac{(3120 * 4) + 1}{17}$

$= 734.17$

$d = \frac{(3120 * 13) + 1}{17}$

$= 2385.94$

$d = \frac{(3120 * 14) + 1}{17}$

$= 2569.47$

$d = \frac{(3120 * 15) + 1}{17}$

$= 2753$

$(d, n) = (2753, 3233)$

$\therefore$ Cipher text $= p^e \bmod n$

$= (\text{network})^e \bmod n$

$= 4^{17} \bmod 3233$

Plain text $= C^d \bmod n$

$= C^{2753} \bmod 3233$

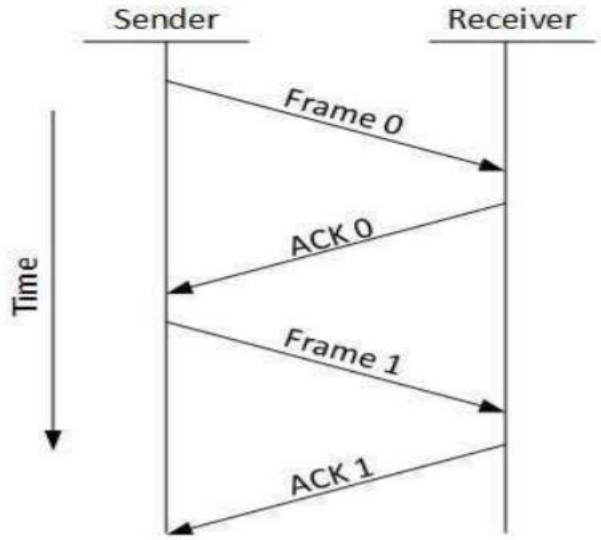
Q.10 Write short notes on:

i. Flow control in DLL

The mechanisms for flow control in DLL are:

a. Stop and Wait

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



b. Sliding Window

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

ii. X.25

A connection-oriented network is X.25, which was the first public data network. It was deployed in the 1970s at a time when telephone service was a monopoly everywhere and the telephone company in each country expected there to be one data network per country — theirs. To use X.25, a computer first established a connection to the remote computer, that is, placed a telephone call. This connection was given a connection number to be used in data transfer packets (because multiple connections could be open at the same time). Data packets were very simple, consisting of a 3-byte header and up to 128 bytes of data. The header consisted of a 12-bit connection number, a packet sequence number, an acknowledgement number, and a few miscellaneous bits. X.25 networks operated for about a decade with mixed success.

It works in 3 layers:

Physical Layer

a. Deals with physical interface between DTE and DCE.

b. Used Standard: X.21, RS232C

Frame Layer

a. Deals with logical transfer of data across the physical layer
b. Used Protocol : LAPB

Packet Layer

a. Deals with end to end communication
b. Used Protocol : X.25 PLP
c.

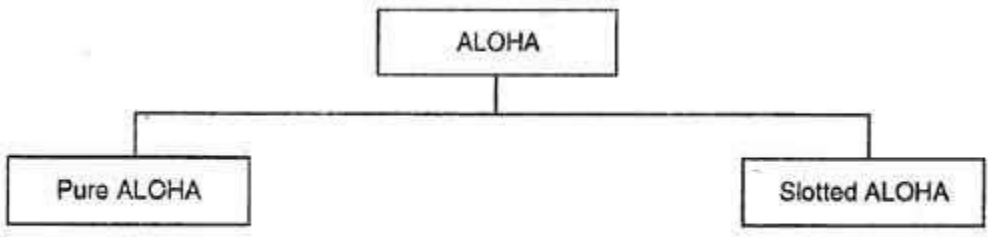
iii. ALOHA

ALOHA is a system for coordinating and arbitrating access to a shared communication Networks channel. It was developed in the 1970s by Norman Abramson and his colleagues at the University of Hawaii. The original system used for ground based radio broadcasting, but the system has been implemented in satellite communication systems.

A shared communication system like ALOHA requires a method of handling collisions that occur when two or more systems attempt to transmit on the channel at the same time. In the ALOHA system, a node transmits whenever data is available to send. If another node transmits at the same time, a collision occurs, and the frames that were transmitted are lost. However, a node can listen to broadcasts on the medium, even its own, and determine whether the frames were transmitted.

Aloha means "Hello". Aloha is a multiple access protocol at the datalink layer and proposes how multiple terminals access the medium without interference or collision. In 1972 Roberts developed a protocol that would increase the capacity of aloha two fold. The Slotted Aloha protocol involves dividing the time interval into discrete slots and each slot interval corresponds to the time period of one frame. This method requires synchronization between the sending nodes to prevent collisions.

There are two different versions of ALOHA



Types of ALOHA

Pure ALOHA

• In pure ALOHA, the stations transmit frames whenever they have data to send.

• When two or more stations transmit simultaneously, there is collision and the frames are destroyed.

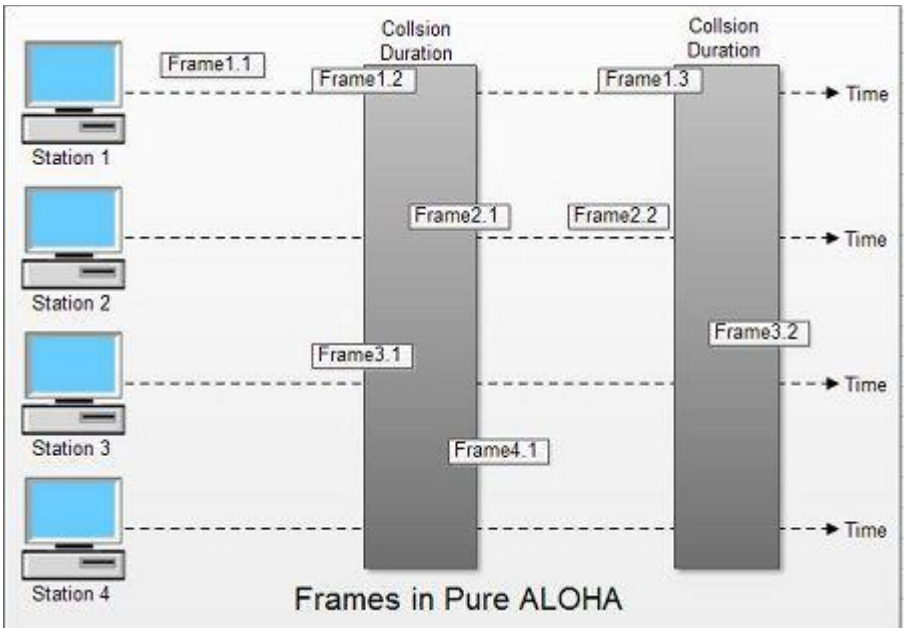
• In pure ALOHA, whenever any station transmits a frame, it expects the acknowledgement from the receiver.

• If acknowledgement is not received within specified time, the station assumes that the frame (or acknowledgement) has been destroyed.

• If the frame is destroyed because of collision the station waits for a random amount of time and sends it again. This waiting time must be random otherwise same frames will collide again and again.

• Therefore pure ALOHA dictates that when time-out period passes, each station must wait for a random amount of time before resending its frame. This randomness will help avoid more collisions.

• Figure shows an example of frame collisions in pure ALOHA.



• In fig there are four stations that .contended with one another for access to shared channel. All these stations are transmitting frames. Some of these frames collide because multiple frames are in contention for the shared channel. Only two frames, frame 1.1 and frame 2.2 survive. All other frames are destroyed.

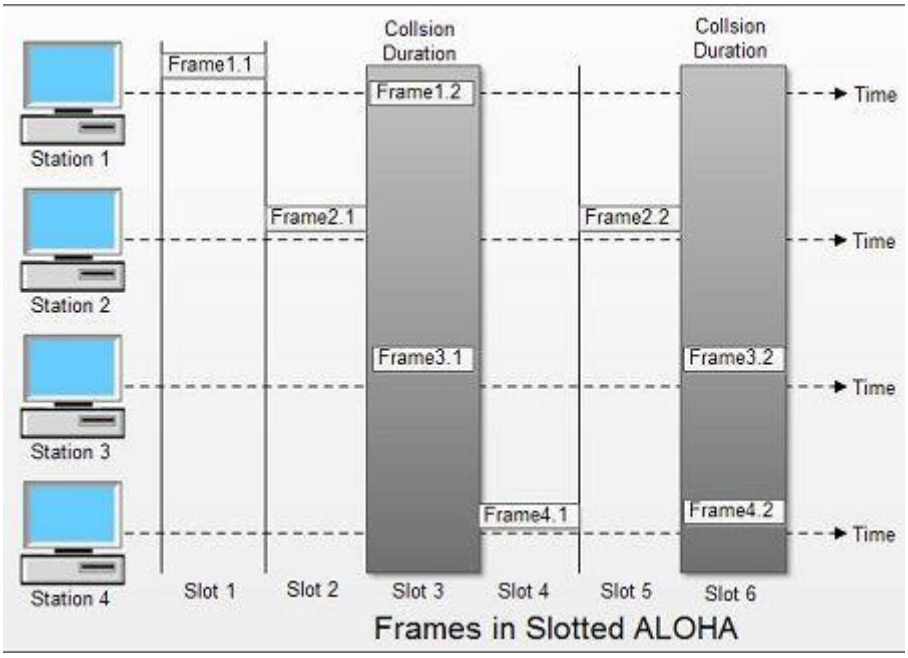
• Whenever two frames try to occupy the channel at the same time, there will be a collision and both will be damaged. If first bit of a new frame overlaps with just the last bit of a frame almost finished, both frames will be totally destroyed and both will have to be retransmitted.

Slotted ALOHA

• Slotted ALOHA was invented to improve the efficiency of pure ALOHA as chances of collision in pure ALOHA are very high.

• In slotted ALOHA, the time of the shared channel is divided into discrete intervals called slots.

• The stations can send a frame only at the beginning of the slot and only one frame is sent in each slot.



• In slotted ALOHA, if any station is not able to place the frame onto the channel at the beginning of the slot *i.e.* it misses the time slot then the station has to wait until the beginning of the next time slot.

• In slotted ALOHA, there is still a possibility of collision if two stations try to send at the beginning of the same time slot as shown in fig.

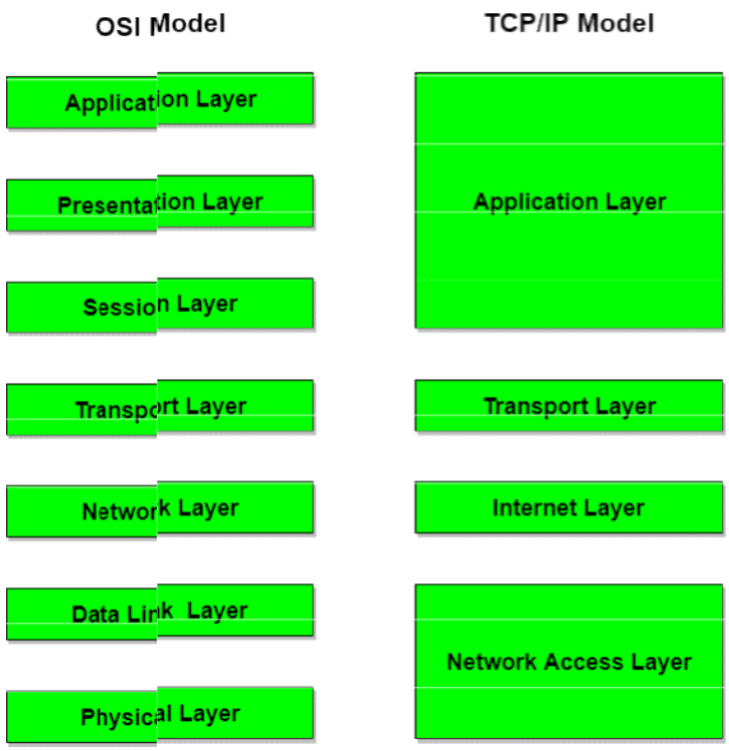
• Slotted ALOHA still has an edge over pure ALOHA as chances of collision are reduced to one-half.

2071 SHRAWAN

Q1) What is computer network? Distinguish between OSI and TCP/IP reference model.

Ans: A computer network is a group of computer systems and other computing hardware devices that are linked together through communication channels to facilitate communication and resource-sharing among a wide range of users. Most common computer networks are Local area network (LAN), Metropolitan area network (MAN), Wide area network (WAN).

Network layer of OSI model p rovides both connection oriented and connectionless service.	8. The Network layer in TCP/IP model provides connectionless service.
7. OSI model has a problem of fitting the protocols into the model.	• TCP/IP model does not fit any protocol
8. Protocols are hidden in OSI model and are easily replaced as the technol ogy changes.	• In TCP/IP replacing protocol is not easy.
9. OSI model defines services, interfaces and protocols very clearly and makes clear distinction between them. It is protocol independent.	• In TCP/IP, services, interface s and protocols are not clearly separated. It is also protocol dependent.
10. It has 7 layers	12. It has 4 layers



Q2. What is transmission media? Explain about any three transmission media in detail.

These are the means by which a communication signal is carried from one system to another. These media can carry information from a source to a destination. The transmission media can usually be free space such as: satellite, microwave, radio and infrared systems, metallic cables such as: twisted pair, or coaxial cable, or fiber-optic cable. In telecommunication, transmission media can be divided into two broad categories:

3. Guided transmission media
4. Unguided transmission media

The three transmission media are explained as follows:

Twisted Pair Cable

Twisted pair cabling is a type of wiring in which two conductors of a single circuit are twisted together for the purposes of canceling out electromagnetic interference (EMI) from external sources; for instance, electromagnetic radiation from unshielded twisted pair (UTP) cables, and crosstalk between neighboring pairs. This cable is the most commonly used and is cheaper than others. It is lightweight, cheap, can be installed easily, and they support many different types of network.

Some important points:

1. Its frequency range is 0 to 3.5 kHz
2. Typical attenuation is 0.2 dB/Km @ 1kHz.
3. Typical delay is 50 μs/km.

- Repeater spacing is 2km.

Twisted Pair is of two types :

1. Unshielded Twisted Pair (UTP)
2. Shielded Twisted Pair (STP)

- Coaxial Cable

Coaxial is called by this name because it contains two conductors that are parallel to each other. Copper is used in this as centre conductor which can be a solid wire or a standard one. It is surrounded by PVC installation, a sheath which is encased in an outer conductor of metal foil, braid or both. Outer metallic wrapping is used as a shield against noise and as the second conductor which completes the circuit. The outer conductor is also encased in an insulating sheath. The outermost part is the plastic cover which protects the whole cable.

Here the most common coaxial standards.

• 50-Ohm RG-7 or RG-11 : used with thick Ethernet.

50-Ohm RG-58 : used with thin Ethernet

- 75-Ohm RG-59 : used with cable television
- 93-Ohm RG-62 : used with ARCNET.

Advantages:

a) Bandwidth is high
b) Used in long distance telephone lines.
c) Transmits digital signals at a very high rate of 10Mbps.
d) Much higher noise immunity
e) Data transmission without distortion
f) The can span to longer distance at higher speeds as they have better shielding when compared to twisted pair cable

Disadvantages:

a) Single cable failure can fail the entire network.
b) Difficult to install and expensive when compared with twisted pair.
c) If the shield is imperfect, it can lead to grounded loop

c) Fiber Optic Cable

These are similar to coaxial cable. It uses electric signals to transmit data. At the centre is the glass core through which light propagates. In multimode fibers, the core is 50microns, and In single mode fibers, the thickness is 8 to 10 microns. The core in fiber optic cable is surrounded by glass cladding with lower index of refraction as compared to core to keep all the light in core. This is covered with a thin plastic jacket to protect the cladding. The fibers are grouped together in bundles protected by an outer shield. Fiber optic cable has bandwidth more than 2 gbps (Gigabytes per Second)

Advantages:

a) Provides high quality transmission of signals at very high speed.
b) These are not affected by electromagnetic interference, so noise and distortion is very less.
c) Used for both analog and digital signals.

Disadvantages:

- It is expensive
- Difficult to install.
- Maintenance is expensive and difficult.
- Do not allow complete routing of light signals.

Q3. What are the major functions of data link layer? Explain about framing in detail.

The major functions of data link layer are:

Data link layer does many tasks on behalf of upper layer. These are:

Framing

Data-link layer takes packets from Network Layer and encapsulates them into Frames. Then, it sends each frame bit-by-bit on the hardware. At receiver' end, data link layer picks up signals from hardware and assembles them into frames.

Addressing

Data-link layer provides layer-2 hardware addressing mechanism. Hardware address is assumed to be unique on the link. It is encoded into hardware at the time of manufacturing.

Synchronization

When data frames are sent on the link, both machines must be synchronized in order to transfer to take place.

Error Control

Sometimes signals may have encountered problem in transition and the bits are flipped. These errors are detected and attempted to recover actual data bits. It also provides error reporting mechanism to the sender.

Flow Control

Stations on same link may have different speed or capacity. Data-link layer ensures flow control that enables both machines to exchange data on same speed.

Multi-Access

When host on the shared link tries to transfer the data, it has a high probability of collision. Data-link layer provides mechanism such as CSMA/CD to equip capability of accessing a shared media among multiple Systems.

Reliable delivery

When a link-layer protocol provides reliable delivery service, it guarantees to move each network-layer datagram across the link without error.

Framing

Framing is a point-to-point connection between two computers or devices consists of a wire in which data is transmitted as a stream of bits. However, these bits must be framed into discernible blocks of information. Framing is a function of the data link layer. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver. A frame has the following parts –

Frame Header − It contains the source and the destination addresses of the frame. Payload field − It contains the message to be delivered.

Trailer − It contains the error detection and error correction bits.

Flag − It marks the beginning and end of the frame.

Encoding Violations

Bit stuffing

Flag byte with Byte

Stuffing Character Count

Q4. What is routing? Differentiate between link state routing and distance vector routing.

When a device has multiple paths to reach a destination, it always selects one path by preferring it over others. This selection process is termed as Routing. Routing is done by special network devices called routers or it can be done by means of software processes. The software based routers have limited functionality and limited scope. A router is always configured with some default route. A default route tells the router where to forward a packet if there is no route found for specific destination.

In case there are multiple path existing to reach the same destination, router can make decision based on the following information:

Hop Count

Bandwidth

Metric

Prefix-

length Delay

Basis of Comparison	Distance vector routing	Link State routing
Algorithm	Bellman ford	Dijsktra
Network view	Topology information from the neighbour point of view	Complete information on the network topology
Best path calculation	Based on the least number of hops	Based on cost.
Updates	Full routing table	Link state updates
Updates frequency	Periodic updates	Triggered updates
CPU and Memory	Low utilization	Intensive

5. Write short notes on:

a) ARP

The address resolution protocol (ARP) is a protocol used by the Internet Protocol (IP) , specifically IPv4, to map IP network addresses to the hardware addresses used by a data link protocol. The protocol operates below the network layer as a part of the interface between the OSI network and OSI link layer. It is used when IPv4 is used over Ethernet. The term address resolution refers to the process of finding an address of a computer in a network. The address is "resolved" using a protocol in which a piece of information is sent by a client process executing on the local computer to a server process executing on a remote computer. The information received by the server allows the server to uniquely identify the network system for which the address was required and therefore to provide the required address. The address resolution procedure is completed when the client receives a response from the server containing the required address. There are four types of ARP messages that may be sent by the ARP protocol. These are identified by four values in the "operation" field of an ARP message. The types of message are: 1. ARP request 2. ARP reply 3. RARP request 4. RARP reply To reduce the number of address resolution requests, a client normally caches resolved addresses for a (short) period of time. The ARP cache is of a finite size, and would become full of incomplete and obsolete entries for computers that are not in use if it was allowed to grow without check. The ARP cache is therefore periodically flushed of all entries. This deletes unused entries and frees space in the cache. It also removes any unsuccessful attempts to contact computers which are not currently running. If a host changes the MAC address it is using, this can be detected by other hosts when the cache entry is deleted and a fresh ARP message is sent to establish the new association. The use of gratuitous ARP (e.g. triggered when the new NIC interface is enabled with an IP address) provides a more rapid update of this information.

b)ICMP

The IP protocol has no error-reporting or error-correcting mechanism. The IP protocol also lacks a mechanism for host and management queries. A host sometimes needs to determine if a router or another host is alive. And sometimes a network administrator needs information from another host or router. The Internet Control Message Protocol (ICMP) has been designed to compensate for the above two deficiencies. It is a companion to the IP protoco1. Types of Messages ICMP messages are divided into two broad categories: error-reporting messages and query messages. The error-reporting messages report problems that a router or a host (destination) may encounter when it processes an IP packet. The query messages, which occur in pairs, help a host or a network manager get specific information from a router or another host. For example, nodes can discover their neighbors. Also, hosts can discover and learn about routers on their network, and routers can help a node redirect its messages.

c)IP

The Internet Protocol (IP) is the principal communications protocol in the Internet protocol suite for relaying datagrams across network boundaries. Its routing function enables internetworking, and essentially establishes the Internet. IP has the task of delivering packets from the source host to the destination host solely based on the IP addresses in

the packet headers. For this purpose, IP defines packet structures that encapsulate the data to be delivered. It also defines addressing methods that are used to label the datagram with source and destination information. Historically, IP was the connectionless datagram service in the original Transmission Control Program introduced by Vint Cerf and Bob Kahn in 1974, which was complemented by a connection-oriented service that became the basis for the Transmission Control Protocol (TCP). The Internet protocol suite is therefore often referred to as TCP/IP. The first major version of IP, Internet Protocol Version 4 (IPv4), is the dominant protocol of the Internet. Its successor is Internet Protocol Version 6 (IPv6), which has been in increasing deployment on the public Internet since c. 2006.

Q6) Distinguish between TCP and UDP. How is TCP connection established? Explain.

Ans:

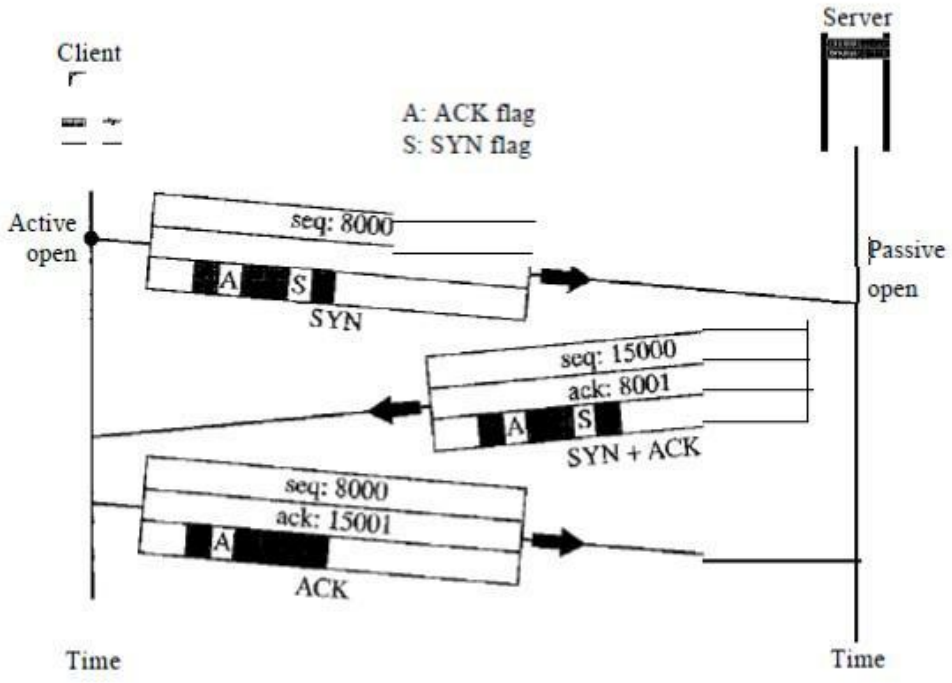
Transmission control protocol (TCP)	User datagram protocol (UDP)
TCP is a connection-oriented protocol. Connection-orientation means that the communicating devices should establish a connection before transmitting data and should close the connection after transmitting the data.	UDP is the Datagram oriented protocol. This is because there is no overhead for opening a connection, maintaining a connection, and terminating a connection. UDP is efficient for broadcast and multicast type of network transmission.
TCP is reliable as it guarantees delivery of data to the destination router.	The delivery of data to the destination cannot be guaranteed in UDP.
TCP provides extensive error checking mechanisms. It is because it provides flow control and acknowledgment of data.	UDP has only the basic error checking mechanism using checksums.
Sequencing of data is a feature of Transmission Control Protocol (TCP). this means that packets arrive in-order at the receiver.	There is no sequencing of data in UDP. If ordering is required, it has to be managed by the application layer.
TCP is comparatively slower than UDP.	UDP is faster, simpler and more efficient than TCP.

Retransmission of lost packets is possible in TCP, but not in UDP.	There is no retransmission of lost packets in User Datagram Protocol (UDP).
TCP has a (20-80) bytes variable length header.	UDP has a 8 bytes fixed length header.

TCP is heavy-weight.	UDP is lightweight.
TCP doesn't supports Broadcasting.	UDP supports Broadcasting.
UDP is used by DNS, DHCP, TFTP, SNMP, RIP, and VoIP.	

TCP connection establishment

TCP communication works in Server/Client model. The client initiates the connection and the server either accepts or rejects it. Three-way handshaking is used for connection management.



Client initiates the connection and sends the segment with a Sequence number. Server acknowledges it back with its own Sequence number and ACK of client's segment which is one more than client's Sequence number. Client after receiving ACK of its segment sends an acknowledgement of Server's response. TCP transmits data in full-duplex mode. When two TCPs in two machines are connected, they can send segments to each other simultaneously. This implies that each party must initialize communication and get approval from the other party before any data are transferred

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

The three steps inthis phase are as follows.

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

Q8) What are the drawbacks in IPV4? Which of these drawbacks do IPV6 solve? Explain.

Ans: Although IPv4 is well designed, data communication has evolved since the inception of IPv4 in the 1970s. IPv4 has some deficiencies (listed below) that make it unsuitable for the fast-growing Internet. Drawbacks of IPV4 are:

Despite all short-term solutions, such as subnetting, classless addressing, and NAT, address depletion is still a long-term problem in the Internet.

The Internet must accommodate real-time audio and video transmission. This type of transmission requires minimum delay strategies and reservation of resources not provided in the IPv4 design.

The Internet must accommodate encryption and authentication of data for some applications. No encryption or authentication is provided by IPv4.

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

Larger address space. An IPv6 address is 128 bits long, compared with the 32-bit address of IPv4, this is a huge increase in the address space.

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

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

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

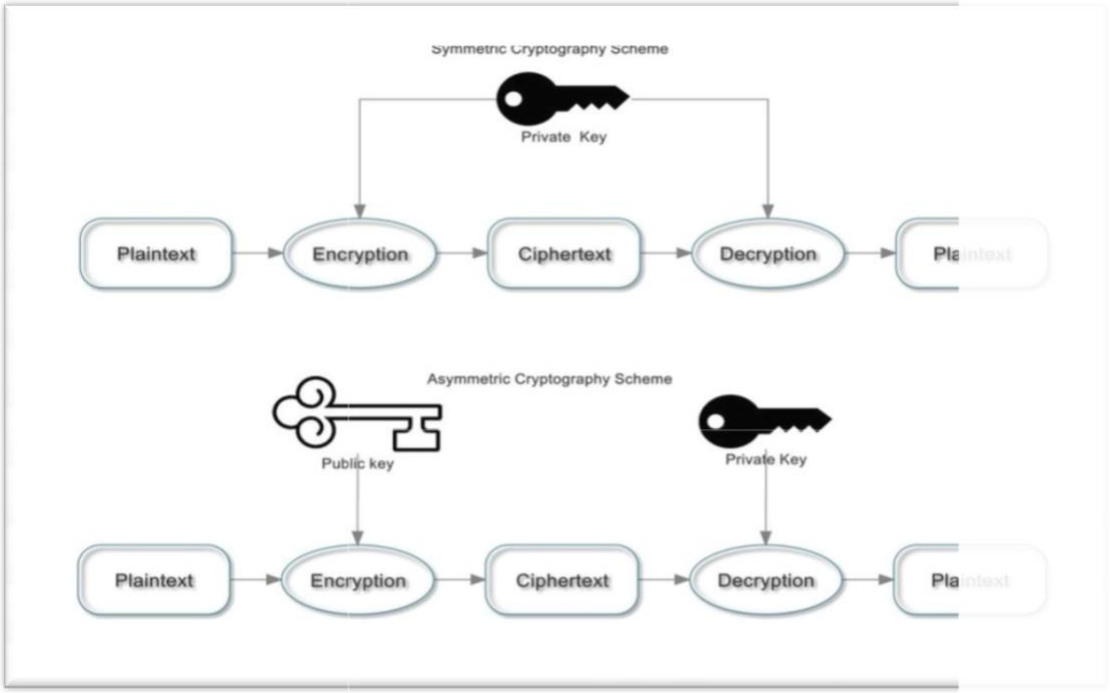
Support for resource allocation. In IPv6, the type-of-service field has been removed, but a mechanism has been added to enable the source to request special handling of the packet. This mechanism can be used to support traffic such as real-time audio and video.

Support for more security. The encryption and authentication options in IPv6 provide.

Q9) What is Cryptography? Differentiate between symmetric key and public key cryptography.

Ans: Cryptography is a method of protecting information and communications using codes so that only those for whom the information is intended can read and process it. The pre-fix "crypt" means "hidden" or "vault" and the suffix "graphy" stands for "writing."

Private Key	Public Key
Private key is faster than public key.	It is slower than private key.
In this, the same key (secret key) and algorithm is used to encrypt and decrypt the message.	In public key cryptography, two keys are used, one key is used for encryption and while the other is used for decryption.
In private key cryptography, the key is kept as a secret.	In public key cryptography, one of the two keys is kept as a secret.
Private key is Symmetrical because there is only one key that is called secret key.	Public key is Asymmetrical because there are two types of key: private and public key.
In this cryptography, sender and receiver need to share the same key.	In this cryptography, sender and receiver does not need to share the same key.
In this cryptography, the key is private.	In this cryptography, public key can be public and private key is private.



Q10)Write short notes on:

WEP

Wired Equivalent Privacy (WEP) is a security protocol, specified in the IEEE Wireless Fidelity (Wi-Fi) standard,802.11b, that is designed to provide a wireless local area network (WLAN) with a level of security and privacy comparable to what is usually expected of a wired LAN. A wired local area network (LA N) is generally protected by physical security mechanisms (controlled access to a buildin g, for example) that are effective for a co ntrolled physical environment, but may be ineffec tive for WLANs because radio waves are not n ecessarily bound by the walls containing the network. WEP seeks to establish similar protection to that offered by the wired network's physical sec urity measures by encrypting data transmitted over the WLAN. Data encryption protects the vul nerable wireless link between clients and access points; once this measure has been taken, other typical LAN security mechanisms such as pass word protection, end-to-end encryption, virtual private networks (VPNs), and authentication can be put in place to ensure privacy.

IDS

An intrusion detection system (IDS) is a device or software application that mo nitors a network or systems for malicious activ ity or policy violations. Any detected activit y or violation is typically reported either to an administrator or collected centrally using a security information and event management (SIEM) s ystem. A SIEM system combines outputs from multiple sources and uses alarm filtering techniqu es to distinguish malicious activity from false alarms. There is a wide spectrum of IDS, varying from antivirus software to hierarchical systems that monitor the traffic

of an entire backbone network. The most common classifications are n etwork intrusion detection systems (NIDS) and host-based intrusion detection systems (HIDS). A system that

monitors important operating system files is an example of a HIDS, while a system that analyzes incoming network traffic is an example of a NIDS. It is also possible to classify IDS by detection approach: the most well-known variants are signature-based detection (recognizing bad patterns, such as malware) and anomaly-based detection (detecting deviations from a model of "good" traffic, which often relies on machine learning). Some IDS can respond to detected intrusions. Systems with response capabilities are typically referred to as an intrusion prevention system

SSL

Secure Sockets Layer (SSL) was the most widely deployed cryptographic protocol to provide security over internet communications before it was preceded by TLS (Transport Layer Security) in 1999. Despite the deprecation of the SSL protocol and the adoption of TLS in its place, most people still refer to this type of technology as 'SSL'. SSL provides a secure channel between two machines or devices operating over the internet or an internal network. One common example is when SSL is used to secure communication between a web browser and a web server. This turns a website's address from HTTP to HTTPS, the 'S' standing for 'secure'.

The authentication process uses public key encryption to validate the digital certificate and to confirm that a server is, in fact, the server it claims to be. Once the server has been authenticated, the client and server establish cipher settings and a shared key to encrypt the information they exchange during the remainder of the session. This provides data confidentiality and integrity. This whole process is invisible to the user. For example, if a webpage requires an SSL connection, the URL will change from HTTP to HTTPS, and a padlock icon will appear in the browser once the server has been authenticated.

Advantages

- To secure online credit card transactions.
- To secure system logins and any sensitive information exchanged online.
- To secure webmail and applications like Outlook Web Access, Exchange and Office Communications Server.
- To secure workflow and virtualization applications like Citrix Delivery Platforms or cloud-based computing platforms.
- To secure the connection between an email client such as Microsoft Outlook and an email server such as Microsoft Exchange.
- To secure the transfer of files over https and FTP(s) services such as website owners updating new pages to their websites or transferring large files.
- To secure hosting control panel logins and activity like Parallels, cPanel, and others. •To secure intranet-based traffic such as internal networks, file sharing, extranets, and database connections.
- To secure network logins and other network traffic with SSL VPNs such as VPN Access Servers or applications like the Citrix Access Gateway.

2073 Chaitra

5. What are the reasons for using layered protocols? What are the headers and trailers and how do they get added and removed?

Ans: The reasons for using layered protocols are as following:

I. It simplifies the design process as the functions of each layers and their interactions are well defined.
II. The layered architecture provides flexibility to modify and develop network services.
III. The number of layers, name of layers and the task assigned to them may change from network to network. But for all the networks, always the lower layer offers certain services to its upper layer.
IV. The concept of layered architecture redefines the way of convincing networks. This leads to a considerable cost savings and managerial benefits.
V. Addition of new services and management of network infrastructure become easy.

The control data added to the beginning of a data is called header. It is an information structure that precedes and identifies the information that follows, such as a block of bytes in communication. The control data added to the end of a data is called trailer. It is an information typically occupying several bytes, at the tail end of a block of transmitted data and often containing a checksum or other error-checking data useful for confirming the accuracy and status of the transmission. In data communication from one device to another the "Sender" appends header and passes it to the lower layer while 'Receiver' removes header and passes it to upper layer. Headers are added at layer 6,5,4,3 & 2 while Trailer is added at layer 2.

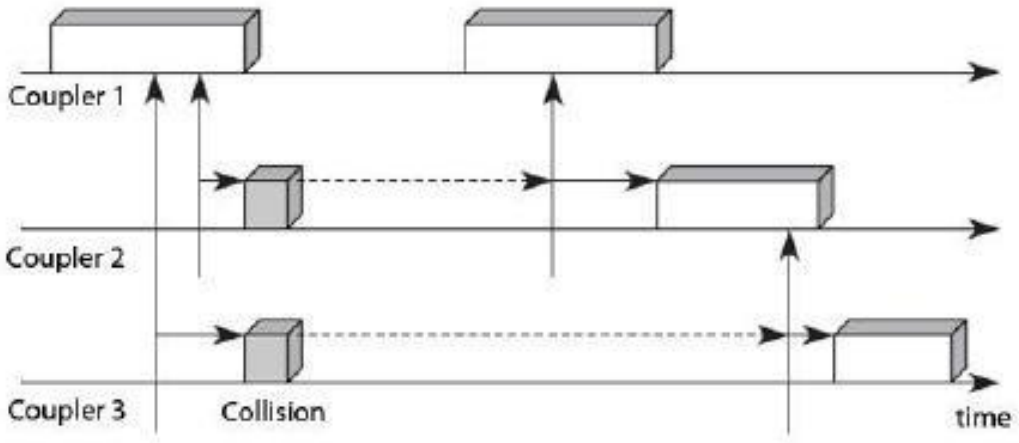
11. Why do you think that static channel assignment is not efficient? Explain about the operation of Carrier Sense Multiple Access with Collision Detection.

Ans: Static channel allocation is a traditional method of channel allocation in which a fixed portion of the frequency channel is allotted to each user, who may be base stations, access points or terminal equipment. In case more static data space is declared than needed, there is waste of space. In case less static space is declared than needed,

then it becomes impossible to expand this fixed size during run time. Hence, static channel assignment is not efficient.

CSMA/CD (Carrier Sense Multiple Access/ Collision Detection) is a media-access control method that was widely used in Early Ethernet technology/LANs, when there used to be shared bus topology and each node were connected by coaxial cables. At a preliminary listening to the network is added listening during transmission. Coupler to issue a loan that detected free channel transmits and continues to listen the channel. The coupler continues to listen, which is sometimes indicated by the CSMA / CD persistent acronym. If there is a collision, it interrupts its transmission as soon as possible and sends special signals, called padding bits so that all couplers are notified of the collision. He tries again his show later using an algorithm that we present later.

Figure shows the CSMA/CD. In this example, the couplers 2 and 3 attempt broadcasting for the coupler 1 transmits its own frame. The couplers 2 and 3 begin to listen and transmit at the same time, the propagation delay around, from the end of the Ethernet frame transmitted by the coupler 1. A collision ensues. Like the couplers 2 and 3 continue to listen to the physical media, they realize the collision, stop their transmission and draw a random time to start retransmission process.



Operating Principle of CSMA / CD

- **What is meant by byte stuffing technique? What is piggy backing? Suppose a bit string, 0111101111101111110, needs to be transmitted at the data link layer. What is the string actually transmitted after bit stuffing?**

Ans: Byte stuffing is a process that transforms a sequence of data bytes that may contain 'illegal' or 'reserved' values (such as packet delimiter) into a potentially longer

sequence that contains no occurrences of those values. In this method, start and end of the frame are recognized with the help of flag bytes. Each frame starts and end with a flag byte. Two consecutive flag bytes indicate the end of one frame and start of the next one. This framing method in only applicable in 8-bit character codes.

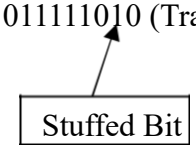
Piggybacking data is a bit different from Sliding Protocol used in the OSI model. In the data frame itself, we incorporate one additional field for acknowledgment (called ACK). Whenever party A wants to send data to party B, it will carry additional ACK information in the PUSH as well. Three rules govern the piggybacking data transfer:

5. If the station A wants to send both data and acknowledgement, it keeps both fields there.
6. If station A wants to send just the acknowledgement, then a separate ACK is sent.
7. If station A wants to send just the data, then the previous acknowledgement field is sent along with the data. Station B simply ignores this duplicate ACK frame upon receiving.

Numerical:

Bit before transmission: 0111101111101111110

Bit after bit stuffing: 01111011111011111010 (Transmitted Bit)



In case of 6 consecutive 1's, after 5 1's a 0 is placed.

Why do we think that there arised the need of classless IP address although class-based IP address was in used? Show the classless IP with an example?
Ans: Classful Addressing, introduced in 1981, with classful routing, IP v4 addresses were divided into 5 classes (A to E).

Disadvantage of Classful Addressing:

- Class A with a mask of 255.0.0.0 can support 16, 777, 214 addresses
- Class B with a mask of 255.255.0.0 can support 65, 534 addresses
- Class C with a mask of 255.255.255.0 can support 254 addresses

But what if someone requires 2000 addresses?

One way to address this situation would be to provide the person with class Bnetwork. But that would result in a waste of so many addresses. Another possible way is to provide multiple class C networks, but that too can cause a problem as there would be too many networks to handle.

To resolve problems like the one mentioned above Classless Inter-Domain Routing (CIDR) was introduced. It allows the user to use Variable Length Subnet Masks.

Example: Allocate 30 and 24 IP addresses to two department with minimum wastage. Specify range of IP address, broadcast address, network address and subnet mask for each department from address pool 202.77.19.0/24.

The starting IP address is : 202.77.19.0/24

The network is of class C.

The subnet mask is 255.255.255.0 (i.e. /24)

Using Variable Length Subnet Mask (VLSM),

For Department A:

To support 30 hosts, it will require 32 IP address such that:

$2^y = 32 \Rightarrow y = 5$

So, we need 5 bits for host field. Hence it requires /27 mask.

IP Address: 202.77.19.0

Network Address: 202.77.19.0

Range of IP for host: 202.77.19.1-202.77.19.30

Broadcast Address: 202.77.19.31

Subnet Mask: 255.255.255.224

For Department B:

To support 24 hosts, it will require at least 2Ss6 IP address such that:

$2^y = 32 \Rightarrow y = 5$

So, we need 5 bits for host field. Hence it requires /27 mask.

IP Address: 202.77.19.32

Network Address: 202.77.19.32

Range of IP for host: 202.77.19.33-202.77.19.62

Broadcast Address: 202.77.19.63

Subnet Mask: 255.255.255.224

- **Suppose we have 4 department A, B, C and D having 25 hosts, 16 hosts, 29 hosts and 11 hosts respectively. You are given a network 202.70.91.0./24. Perform the subnetting in such a way that the IP address wastage in each department is minimum and find out the subnet mask, network address, broadcast address and usable host rang in each department.**

  Ans:

  Network = 202.70.91.0/24

  Using Variable Length Subnet Mask (VLSM)

  For department A:

  User = 25

  To support 25 host, it will require (25+2) = 27 IP address

  i.e.2^5 > 27

  hid = 5

  nid = 32-5 =27

  Network Address = 202.70.91.0

  Usable Host Rang = 202.70.91.1 – 202.70.91.27(1+27-1=27)

  Broadcast Address = 202.70.91.31(0+32=32-1=31)

  Subnet Mask(hid = 0 and nid = 1) = 11111111.11111111.11111111.11100000
  (Binary to Decimal) = 255.255.255.224

  For department B:

  User = 16

  To support 16 host, it will require (16+2) = 18 IP address

  i.e.2^5 > 27

  hid = 5

  nid = 32-5 =27

  Network Address = 202.70.91.32

  Usable Host Rang = 202.70.91.33 – 202.70.91.50(33+18-1=50)

  Broadcast Address = 202.70.91.63(32+32-1=63)

Subnet Mask (hid = 0 and nid = 1) = 11111111.11111111.11111111.11100000
(Binary to Decimal) = 255.255.255.224

For department C:

User = 29

To support 29 host, it will require (29+2) = 31 IP address

i.e.2^5 > 31

hid = 5

nid = 32-5 =27

Network Address = 202.70.91.64

Usable Host Rang = 202.70.91.65 – 202.70.91.95(65+31-1=95)

Broadcast Address = 202.70.91.95(64+32-1=95)

Subnet Mask (hid = 0 and nid = 1) = 11111111.11111111.11111111.11100000
(Binary to Decimal) = 255.255.255.224

For department D:

User = 11

To support 11 host, it will require (11+2) = 13 IP address

i.e.2^4 > 13

hid = 4

nid = 32-4 =28

Network Address = 202.70.91.96

Usable Host Rang = 202.70.91.97 – 202.70.91.109(97+13-1=109)

Broadcast Address = 202.70.91.111(96+16-1=111)

Subnet Mask (hid = 0 and nid = 1) = 11111111.11111111.11111111.11110000
(Binary to Decimal) = 255.255.255.240

• **Explain the difference between TCP and UDP. How congestions can be handled using Token Bucket? Explain with proper diagram.**

Ans:

Characteristics/ Description	UDP	TCP
General Description	Simple High speed low functionality "wrapper" that interface applications to the network layer and does little else	Full-featured protocol that allows applications to send data reliably without worrying about network layer issues.
Protocol connection Setup	Connection less data is sent without setup	Connection-oriented; Connection must be Established prior to transmission.
Data interface to application	Message base-based is sent in discrete packages by the application.	Stream-based; data is sent by the application with no particular structure
Reliability and Acknowledgements	Unreliable best-effort delivery without acknowledgements	Reliable delivery of message all data is acknowledged.
Retransmissions	Not performed. Application must detect lost data and retransmit if needed.	Delivery of all data is managed, and lost data is retransmitted automatically.
Features Provided to Manage flow of Data	None	Flow control using sliding windows; window size adjustment heuristics; congestion avoidance algorithms
Overhead	Very Low	Low, but higher than UDP
Transmission speed	Very High	High but not as high as UDP
Data Quantity Suitability	Small to moderate amounts of data.	Small to very large amounts of data.

Congestion is a state occurring in network layer when the message traffic is so heavy that it slows down network response time.

Effects of Congestion:

- As delay increases, performance decreases.
- If delay increases, retransmission occurs, making situation worse.

Token bucket Algorithm

Need of token bucket algorithm: -

The leaky bucket algorithm enforces output pattern at the average rate, no matter how bursty the traffic is. So, in order to deal with the bursty traffic we need a flexible algorithm so that the data is not lost. One such algorithm is token bucket algorithm.

Steps of this algorithm can be described as follows:

g) In regular intervals tokens are thrown into the bucket. Ƒ

h) The bucket has a maximum capacity. Ƒ

i) If there is a ready packet, a token is removed from the bucket, and the packet is sent.

j) If there is no token in the bucket, the packet cannot be sent.

Let's understand with an example,

In figure (A) we see a bucket holding three tokens, with five packets waiting to be transmitted. For a packet to be transmitted, it must capture and destroy one token. In figure (B) We see that three of the five packets have gotten through, but the other two are stuck waiting for more tokens to be generated.

Ways in which token bucket is superior to leaky bucket:

The leaky bucket algorithm controls the rate at which the packets are introduced in the network, but it is very conservative in nature. Some flexibility is introduced in the token bucket algorithm. In the token bucket, algorithm tokens are generated at each tick (up to a certain limit). For an incoming packet to be transmitted, it must capture a token and the transmission takes place at the same rate. Hence some of the busty packets are transmitted at the same rate if tokens are available and thus introduces some amount of flexibility in the system.

Formula: M * s = C + ρ * s

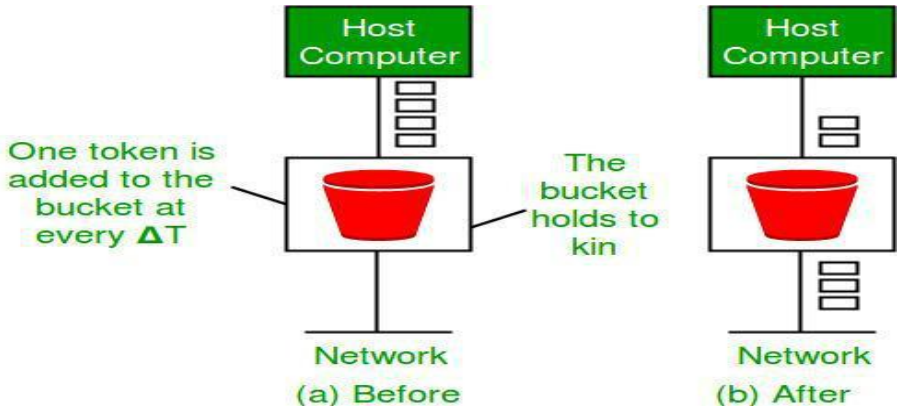
where S – is time taken

M – Maximum output rate

d) – Token arrival rate

C – Capacity of the token bucket in byte

Let's understand with a diagram,



d) For the client-server application over TCP, why must the server program be executed before the client program? TCP is known as reliable process, describe how reliability is provided by TCP.

Ans: In a client-server application over TCP, the server program must be executed before the client program due to the following reasons:

- As the TCP is connection-oriented protocol, a connection must be established between the server and the client before they communicate to each other.
- A client-server run over the TCP, server program is executed first, because the server must accept the request from the client and ready to execute the client's program.
- If the server is not ready (not running) then the client fails to establish the connection with the server.

TCP is known as reliable process. TCP provides for the recovery of segments that get lost, are damaged, duplicated or received out of their correct order. TCP is described as a 'reliable' protocol because it attempts to recover from these errors. The sequencing is handled by labeling every segment with a sequence number. These sequence numbers permit TCP to detect dropped segments. TCP also requires that an acknowledge message be returned after transmitting data.

To verify that the segments are not damaged, a CRC check is performed on every segment that is sent, and every segment that is received. Because every packet has a time to live field, and that field is decremented during each forwarding cycle, TCP must re-calculate the CRC value for the segment at each hop. Segments that do not match the CRC check are discarded. Hence, TCP can be stated as a reliable process.

8. "IPv4 and IPv6 coexists" what does this mean? Explain dual stack approach with an appropriate figure.

Ans: IPv4 IP addresses are 32-bits long while IPv6 addresses are 128-bits long. But IPv6 addresses can (and do) interoperate with IPv4 addresses, through a variety of methods that allow IPv6 to carry along IPv4 addresses. This is achieved through the use of IPv4 mapped IPV6 addresses and IPv4 compatible IPv6 addresses. This allows IPv4 addresses to be represented in IPv6 addresses. There are a variety of ways in which both IPv4 and IPv6 can be made "compatible" from a data center networking point of

view. Tunneling IPv6 via IPv4 to allow individual hosts on an IPv4 network to reach the IPv6 network is one way, but requires that routers are able to be configured to support such encapsulation. Hybrid networking stacks on hosts makes the utilization of IPv6 or IPv4 much simpler, but does not necessarily help routing IPv6 through an IPv4 network. Most methods effectively force configuration and potentially architectural changes to support a dual IP version environment, which for many organizations is exactly what they were trying to avoid in the first place: disruptive, expensive changes in the infrastructure. There is a way to support IPv6 externally while making relatively no changes to the organizational network architecture. An IPv6 gateway can provide the translation necessary to seamlessly support both IPv6 and IPv4. Employing an IPv6 gateway insulates organizations from making changes to internal networks and applications while supporting IPv6 clients and infrastructure externally. The right IPv6-enabled solution can also help with migration internally. For example, an enabled application delivery controller can act as an IPv4 to IPv6 gateway, and vice-versa, by configuring a virtual server using one IP address version and pool members using the other version. This allows organizations to mix and match IP versions within their application infrastructure as they migrate on their own schedule toward a completely IPv6 network architecture, internally and externally.

It is recommended that all the hosts, before migrating completely to version 6, have dual stack of protocols. A station must run IPv4 and IPv6 simultaneously until all the Internet uses IPv6. End nodes and routers/switches run both protocols, and if IPv6 communication is possible that is the preferred protocol. Dual stack routing implements dual IP layers in hosts and routers, supporting both IPv6 and IPv4. A dual stack architecture supports both IPv4 and IPv6 traffic and routes the appropriate traffic as required to any device on the network. Administrators can update network components and applications to IPv6 on their own schedule, and even maintain some IPv4 support indefinitely if that is necessary. Devices that are on this type of network, and connect to the Internet, can query Internet DNS servers for both IPv4 and IPv6 addresses. If the Internet site supports IPv6, the device can easily connect using the IPv6 address. If the Internet site does not support IPv6, then the device can connect using the IPv4 addresses.

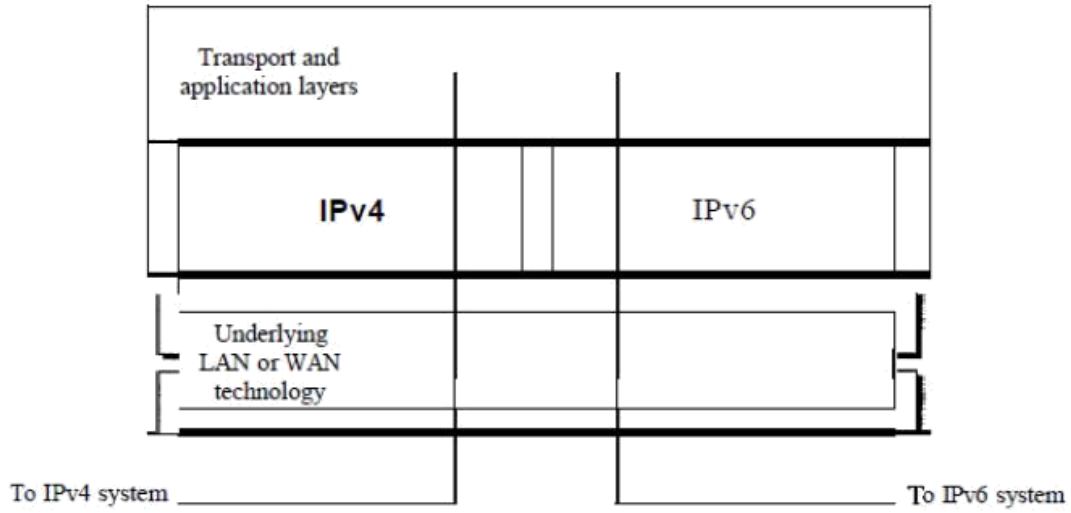


Figure: Dual Stack

9. What are the attributes of information security? Explain the operation of RSA algorithm.

Ans: The term "information security" means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide: Confidentiality, integrity, and availability (CIA) which are the unifying attributes of an information security.

A. Integrity: which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation, accuracy, and authenticity;

B. Confidentiality: which means preserving authorized restrictions on access and disclosure, including a means for protecting personal privacy and proprietary information; and

C. Availability: which means ensuring timely and reliable access to, and use of, information.

RSA (Rivest–Shamir–Adleman) is an algorithm used by modern computers to encrypt and decrypt messages. It is an asymmetric cryptographic algorithm.
Asymmetric means that there are two different keys. This is also called public key cryptography, because one of the keys can be given to anyone. The other key must be kept private. The algorithm is based on the fact that finding the factors of a

large composite number is difficult: when the factors are prime numbers, the problem is called prime factorization. It is also a key pair (public and private key) generator.

RSA involves a public key and private key. The public key can be known to everyone; it is used to encrypt messages. Messages encrypted using the public key can only be decrypted with the private key. The keys for the RSA algorithm are generated the following way:

1. Choose two very large random prime integers. (p and q)
2. Compute n and Ǿ(n) such
   that: n = p * q
   Ǿ(n) = (p-1) * (q-1)
3. Choose an integer e, 1 < e < Ǿ(n), such that:
   gcd(e, Ǿ(n)) = 1
4. Compute d, 1 < d < Ǿ(n), such that:
   e * d = 1 (mod Ǿ(n))

We get, public key = (n, e)
private key = (n, d)
p, q and Ǿ(n) are private
e is public exponent.
d is private exponent.

Encryption and Decryption:

- Cipher (C) = M^e mod n
- Message (M) = C^d mod n

Example:

Key Generation:
1. p = 11 and q = 3
2. n = p * q = 33
   Ǿ(n) = (p-1) * (q-1) = 20
3. Choose e = 3 such that 1 < e < Ǿ(n) and gcd(e, Ǿ(n)) = 1
4. (3) * d = 1 (mod
   20) d = 7

Public key = (33, 3)

Private key = (33, 7)

Let message M = 7.

Encryption:

C = M^e mod n = 7^3 mod 33 = 13

Decryption:

M = C^d mod n = 13^7 mod 33 = 7

10. Write short notes on:

A) DHCP

Dynamic Host Configuration Protocol (DHCP) is an application layer protocol which is used to provide:

- Subnet Mask (Option 1 – e.g., 255.255.255.0)
- Router Address (Option 3 – e.g., 192.168.1.1)
- DNS Address (Option 6 – e.g., 8.8.8.8)
- Vendor Class Identifier (Option 43 – e.g., 'unifi' = 192.168.1.9 ##where unifi = controller)

DHCP is based on a client-server model and based on discovery, offer, request, and ACK.

DHCP port number for server is 67 and for the client is 68. It is a Client server protocol which uses UDP services. IP address is assigned from a pool of addresses. In DHCP, the client and the server exchange mainly 4 DHCP messages in order to make a connection, also called DORA process, but there are 8 DHCP messages in the process. These messages are given as below:

1) DHCP discover message –

This is a first message generated in the communication process between server and client. This message is generated by Client host in order to discover if there is any DHCP server/servers are present in a network or not. This message is broadcasted to all devices present in a network to find the DHCP server. This message is 342 or 576 bytes long.

2) DHCP offer message –

The server will respond to host in this message specifying the unleased IP address and

other TCP configuration information. This message is broadcasted by server. Size of message is 342 bytes. If there are more than one DHCP servers present in the network then client host will accept the first DHCP OFFER message it receives. Also, a server ID is specified in the packet in order to identify the server.

3) DHCP request message –
When a client receives a offer message, it responds by broadcasting a DHCP request message. The client will produce a gratuitous ARP in order to find if there is any other host present in the network with same IP address. If there is no reply by other host, then there is no host with same TCP configuration in the network and the message is broadcasted to server showing the acceptance of IP address. A Client ID is also added in this message.

4) DHCP acknowledgement message –
In response to the request message received, the server will make an entry with specified client ID and bind the IP address offered with lease time. Now, the client will have the IP address provided by server.

5) DHCP negative acknowledgement message –
Whenever a DHCP server receives a request for IP address that is invalid according to the scopes that is configured with, it send DHCP Nak message to client. Eg-when the server has no IP address unused or the pool is empty, then this message is sent by the server to client.

6) DHCP decline –
If DHCP client determines the offered configuration parameters are different or invalid, it sends DHCP decline message to the server .When there is a reply to the gratuitous ARP by any host to the client, the client sends DHCP decline message to the server showing the offered IP address is already in use.

7) DHCP release –
A DHCP client sends DHCP release packet to server to release IP address and cancel any remaining lease time.

8) DHCP inform –
If a client address has obtained IP address manually then the client uses a DHCP inform to obtain other local configuration parameters, such as domain name. In reply to the dhcp inform message, DHCP server generates DHCP ack message with local

configuration suitable for the client without allocating a new IP address. This DHCP ack message is unicast to the client.

Note – All the messages can be unicast also by dhcp relay agent if the server is present in different network.

Advantages –

The advantages of using DHCP include:

- centralized management of IP addresses
- ease of adding new clients to a network
- reuse of IP addresses reducing the total number of IP addresses that are required
- simple reconfiguration of the IP address space on the DHCP server without needing to reconfigure each client

The DHCP protocol gives the network administrator a method to configure the network from a centralised area.
With the help of DHCP, easy handling of new users and reuse of IP address can be achieved

Disadvantages –

Disadvantage of using DHCP is:

- IP conflict can occur

B) Firewall

A firewall is a system designed to prevent unauthorized access to or from a private network. You can implement a firewall in either hardware or software form, or a combination of both. Firewalls prevent unauthorized internet users from accessing private networks connected to the internet, especially intranets. All messages entering or leaving the intranet (the local network to which you are connected) must pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

Types of Firewall

1) Packet Filtering Firewall

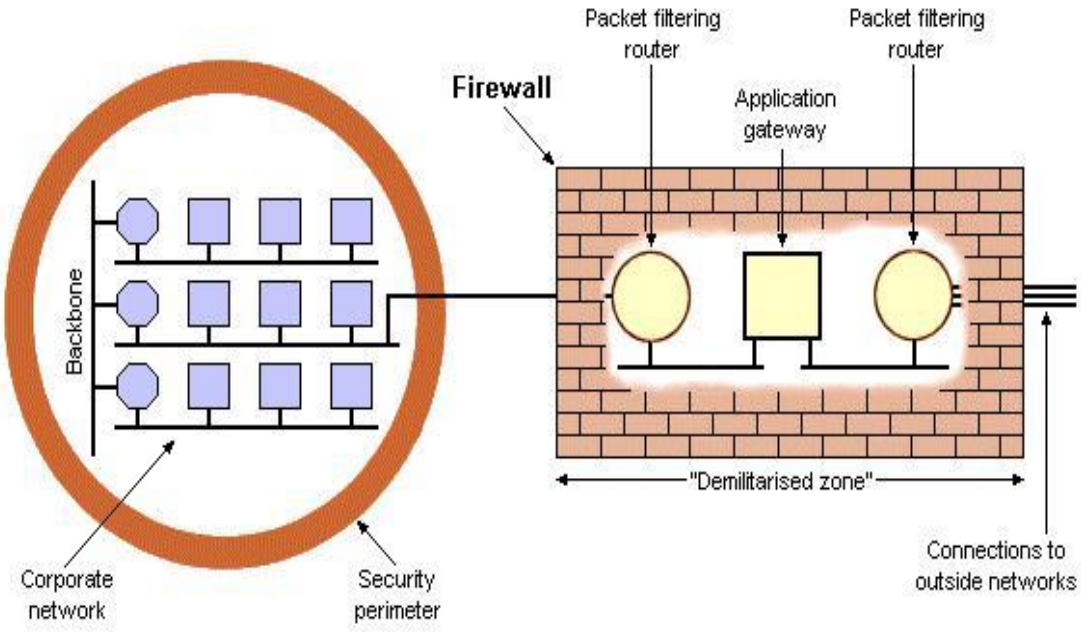
- It protects users from the external network threat
- Packet filtering is the process of passing or blocking packets based on source and destination address, port or protocols at a network interface.
- The header of the packet is analyzed and based on predefined rules, it allows packet to pass or prevents packet from passing.

Methods

-The filter accepts only those packets that it is certain are safe, dropping all others.
- The filter drops only the packets that is certain are unsafe, accepting all others.
- The filter when encounters a packet for which no rule is provided, it query the user for performing what should be done.

2) Application Gateway

6. The gateway operates at the application layer.
7. Application gateway for specific applications can be installed.
8. It filters incoming node traffic to certain rules which mean that only transmitted network application data is filtered.
9. Eg: A mail gateway can be set up to examine each message going in or coming out. For each message, gateway decides whether to transmit of discard the messages.



By: Ankita Karna & Asha Shah

C) DNS

DNS (Domain Name Server) is a host name to IP address translation service. DNS is a distributed database implemented in a hierarchy of name servers. It is an application layer protocol for message exchange between clients and servers.

Requirement:

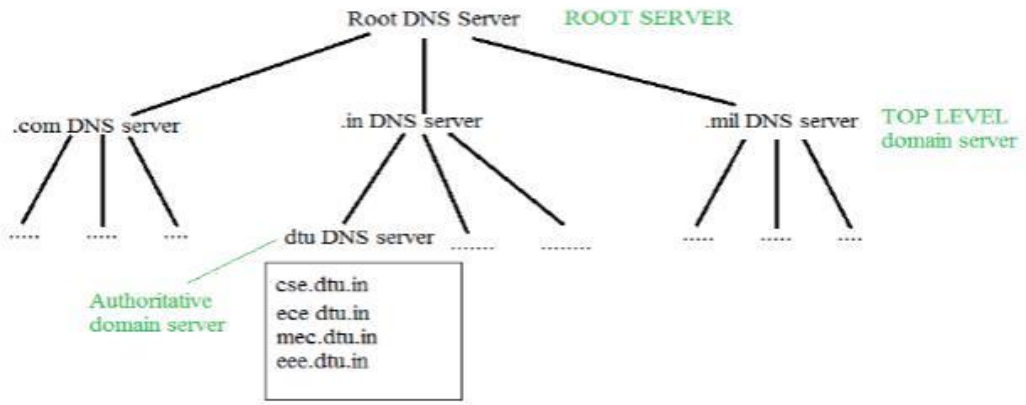
Every host is identified by the IP address but remembering numbers is very difficult for the people and also the IP addresses are not static therefore a mapping is required to change the domain name to IP address. So, DNS is used to convert the domain name of the websites to their numerical IP address.

Domain :

There are various kinds of DOMAIN :

4. Generic domain : .com(commercial) .edu(educational) .mil(military) .org(non profit organization) .net(similar to commercial) all these are generic domain.
5. Country domain .in (india) .us .uk
6. Inverse domain if we want to know what is the domain name of the website. IP to domain name mapping. So, DNS can provide both the mapping for example to find the IP addresses of geeksforgeeks.org then we have to type
   nslookup www.geeksforgeeks.org.

Organization of Domain:



It is very difficult to find out the IP address associated to a website because there are millions of websites and with all those websites we should be able to generate the ip address immediately, there should not be a lot of delay for that to happen organization of database is very important.

DNS record – Domain name, IP address what is the validity?? what is the time to live ?? and all the information related to that domain name. These records are stored in tree like structure.

Namespace – Set of possible names, flat or hierarchical. Naming system maintains a collection of bindings of names to values – given a name, a resolution mechanism returns the corresponding value.

Name server – It is an implementation of the resolution mechanism. DNS (Domain Name System) = Name service in Internet – Zone is an administrative unit, domain is a subtree.
The host request the DNS name server to resolve the domain name. And the name server returns the IP address corresponding to that domain name to the host so that the host can future connect to that IP address.
Hierarchy of Name Servers:
Root name servers – It is contacted by name servers that can not resolve the name. It contacts authoritative name server if name mapping is not known. It then gets the mapping and return the IP address to the host.

Top level server – It is responsible for com, org, edu etc and all top level country domains like uk, fr, ca, in etc. They have info about authoritative domain servers and know names and IP addresses of each authoritative name server for the second level domains.

Authoritative name servers-- This is organization's DNS server, providing authoritative hostName to IP mapping for organization servers. It can be maintained by organization or service provider. In order to reach cse.dtu.in we have to ask the root DNS server, then it will point out to the top level domain server and then to authoritative domain name server which actually contains the IP address. So, the authoritative domain server will return the associative IP address.

The client machine sends a request to the local name server, which , if root does not find the address in its database, sends a request to the root name server , which in turn, will route the query to an intermediate or authoritative name server. The root name server can also contain some hostName to IP address mappings . The intermediate name server always knows who the authoritative name server is. So finally the IP

address is returned to the local name server which in turn returns the IP address to the host.

2075 CHAITRA

Q1. Draw the architecture for Client/Server network model. Explain in details about P2P network model with supportive examples.

Ans: The architecture of Client-Server model is given below:

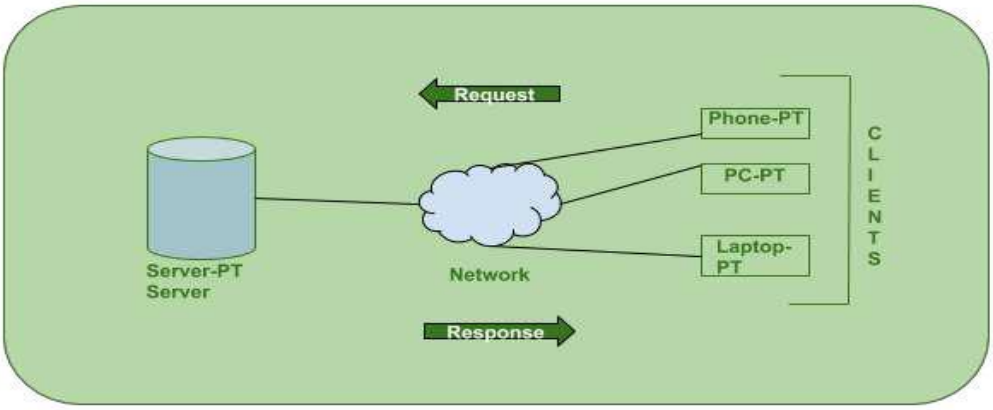


Fig: client-server model architecture

P2P network model:

Peer-to-peer (P2P) is a decentralized communications model in which each party has the same capabilities and either party can initiate a communication session. Unlike the client/server model, in which the client makes a service request and the server fulfills the request, the P2P network model allows each node to function as both a client and server. In its simplest form, a peer-to-peer (P2P) network is created when two or more PCs are connected and share resources without going through a separate server computer. Most P2P programs are focused on media sharing. Peer-to-peer is a feature of, for example, decentralized crypto currency block chains.

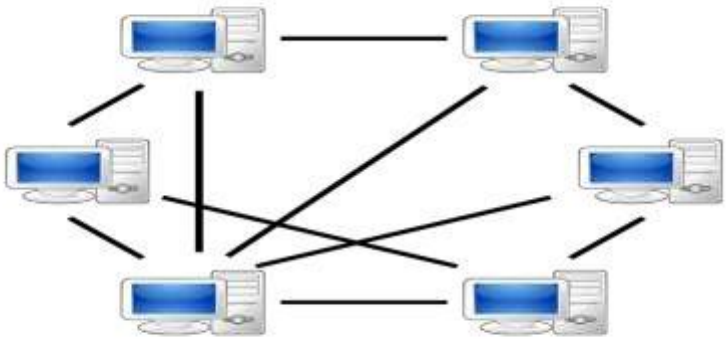


Fig: P2P architecture

Q2. What is switching? What are the various switching techniques? Elaborate packet switching with a proper diagram.

Ans: Switching:

Switching is process to forward packets coming in from one port to a port leading towards the destination. When data comes on a port it is called ingress, and when data leaves a port or goes out it is called egress. A communication system may include number of switches and nodes.

Various switching techniques are:

6. Circuit Switching
7. Message Switching
8. Packet Switching

Packet Switching:

Shortcomings of message switching gave birth to an idea of packet switching. The entire message is broken down into smaller chunks called packets. The switching information is added in the header of each packet and transmitted independently. It is easier for intermediate networking devices to store small size packets and they do not take many resources either on carrier path or in the internal memory of switches. Packet switching enhances line efficiency as packets from multiple applications can be multiplexed over the carrier. The internet uses packet switching technique. Packet switching enables the user to differentiate data streams based on priorities. Packets are stored and forwarded according to their priority to provide quality of service.

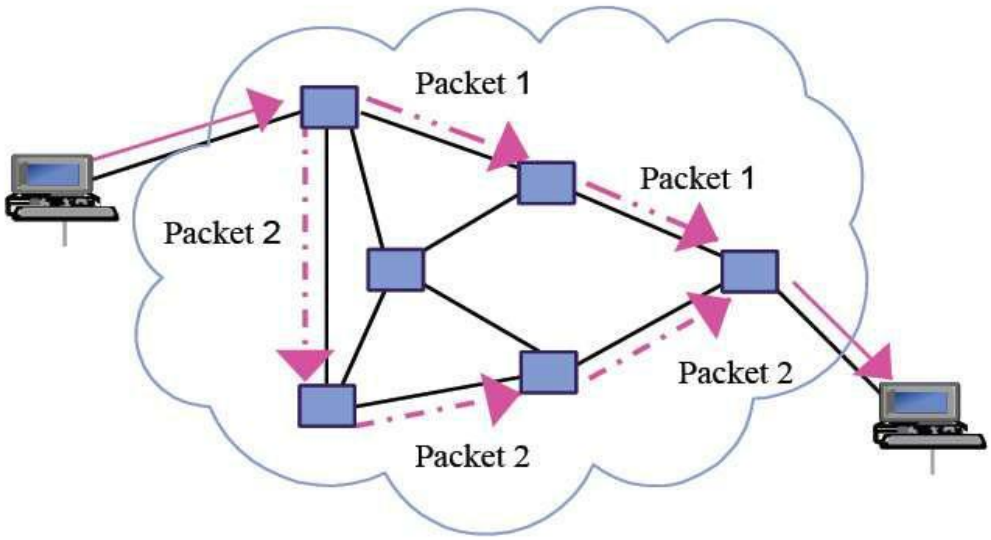
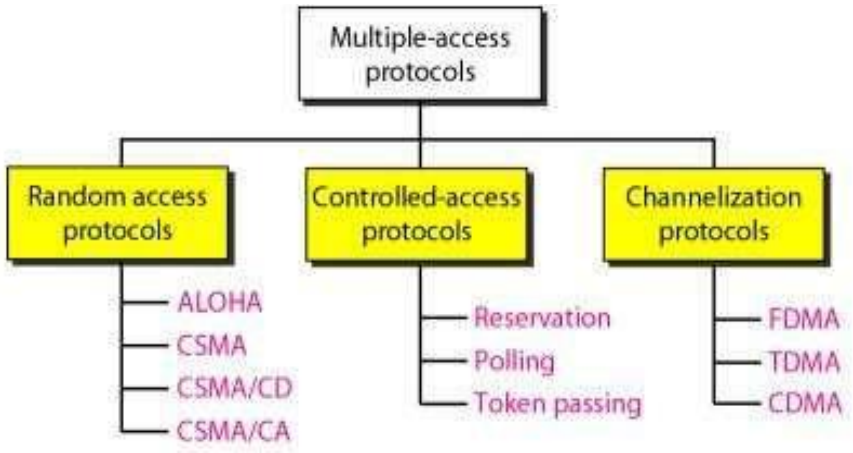


Fig: Packet Switching

Q3. What are multiple access protocols? Describe the various framing techniques at data link layer.

Ans:



Various framing techniques at data link layer are:

5. Encoding Violations
6. Bit stuffing
7. Byte Stuffing
8. Character Count

*Encoding Violations:

This Framing Method is used only in those networks in which Encoding on the Physical Medium contains some redundancy. Some LANs encode each bit of data by using two Physical Bits i.e. Manchester coding is Used. Here, Bit 1 is encoded into high-low (10) pair and Bit 0 is encoded into low-high (01) pair. The scheme means that every data bit has a transition in the middle, making it easy for the receiver to locate the bit boundaries. The combinations high-high and low-low are not used for data but are used for delimiting frames in some protocols.

*Bit Stuffing:

12. Allows frame to contain arbitrary number of bits and arbitrary character size. The frames are separated by separating flag.
13. Each frame begins and ends with a special bit pattern, 01111110 called a flag byte. When five consecutive l's are encountered in the data, it automatically stuffs a '0' bit into outgoing bit stream.

- In this method, frames contain an arbitrary number of bits and allow character codes with an arbitrary number of bits per character. In his case, each frame starts and ends with a special bit pattern, 01111110.
- In the data a 0 bit is automatically stuffed into the outgoing bit stream whenever the sender's data link layer finds five consecutive 1s.
- This bit stuffing is similar to byte stuffing, in which an escape byte is stuffed into the outgoing character stream before a flag byte in the data.
- When the receiver sees five consecutive incoming i bits, followed by a 0 bit, it automatically de stuffs (i.e., deletes) the 0 bit. Bit Stuffing is completely transparent to network layer as byte stuffing. The figure1 below gives an example of bit stuffing.
- This method of framing finds its application in networks in which the change of data into code on the physical medium contains some repeated or duplicate data. For example, some LANs encodes bit of data by using 2 physical bits.

*Byte Stuffing:

8. In this method, start and end of frame are recognized with the help of flag bytes. Each frames starts with and ends with a flag byte. Two consecutive flag bytes indicate the end of one frame and start of the next one. The flag bytes used in the figure 2 used is named as "ESC" flag byte.
9. A frame delimited by flag bytes. This framing method is only applicable in 8-bit character codes which are a major disadvantage of this method as not all character codes use 8-bit characters e.g. Unicode.

*Character Count:

Each frame starts with the ASCII character sequence DLE STX and ends with the sequence DLE ETX. (Where DLE is Data Link Escape, STX is Start of Text and ETX is End of Text.) This method overcomes the drawbacks of the character count method. If the destination ever loses synchronization, it only has to look for DLE STX and DLE ETX characters. If however, binary data is being transmitted then there exists a possibility of the characters DLE STX and DLE ETX occurring in the data. Since this can interfere with the framing, a technique called character stuffing is used. The sender's data link layer inserts an ASCII DLE character just before the DLE character in the data. The receiver's data link layer removes this DLE before this data is given to the network layer. However character stuffing is closely associated with 8-bit characters and this is a major hurdle in transmitting arbitrary sized characters.

Q4. Suppose you are a private consultant hired by the large company to setup the network for their enterprise and you are given large number of consecutive IP address starting at 120.89.96.0/19. Suppose that four departments A, B, C and D requests 100,500,800 and 400

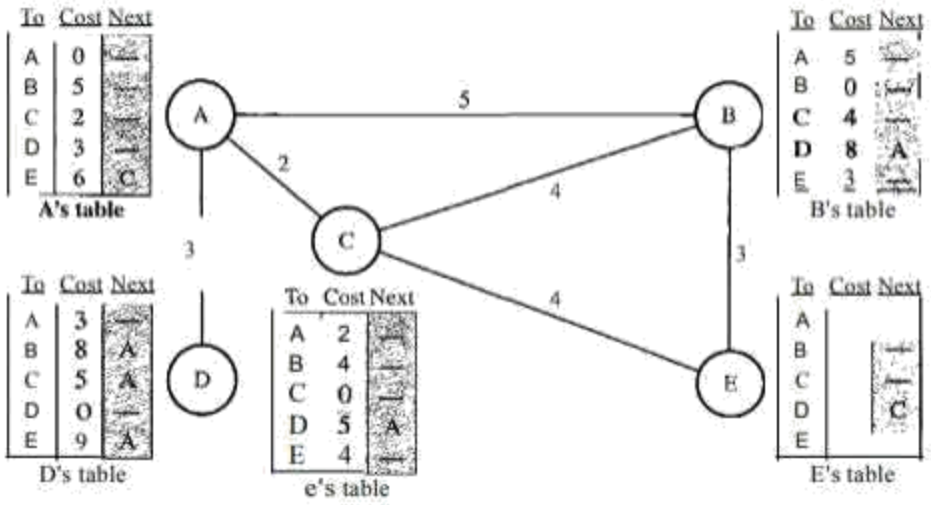
address respectively, how the subnetting can be performed so, that address wastage will be minimum?

Ans:

Class A	Class B	Class C	Class D
User = 100 $100 \leq 128 = 2^7$ Hence, hid = 7 and nid = 32-7 →nid=25 Now, First Address: 120.89.96.0/25 …… <usable addresses> 120.89.96.99/25 …… 120.89.96.127/25 Last Address Subnet Mask: 255.255.255.128	User = 500 $500 \leq 512 = 2^9$ Hence, hid = 9 and nid = 32-9 →nid=23 Now, First Address: 120.89.96.128/23 …… …… <usable addresses> 120.89.98.117/23 …… …… 120.89.98.129/23 Last Address Subnet Mask: 255.255.254.0	User = 800 $800 \leq 1024 = 2^{10}$ Hence, hid = 10 and nid = 32-10 →nid=22 Now, First Address: 120.89.98.130/22 …… …… <usable addresses> 120.89.101.164/22 …… …… 120.89.102.133/22 Last Address Subnet Mask: 255.255.252.0	User = 400 $400 \leq 512 = 2^9$ Hence, hid = 9 and nid = 32-9 →nid=23 Now, First Address: 120.89.102.134/23 …… …… <usable addresses> 120.89.104.24/23 …… …… 120.89.104.136/23 Last Address Subnet Mask: 255.255.254.0

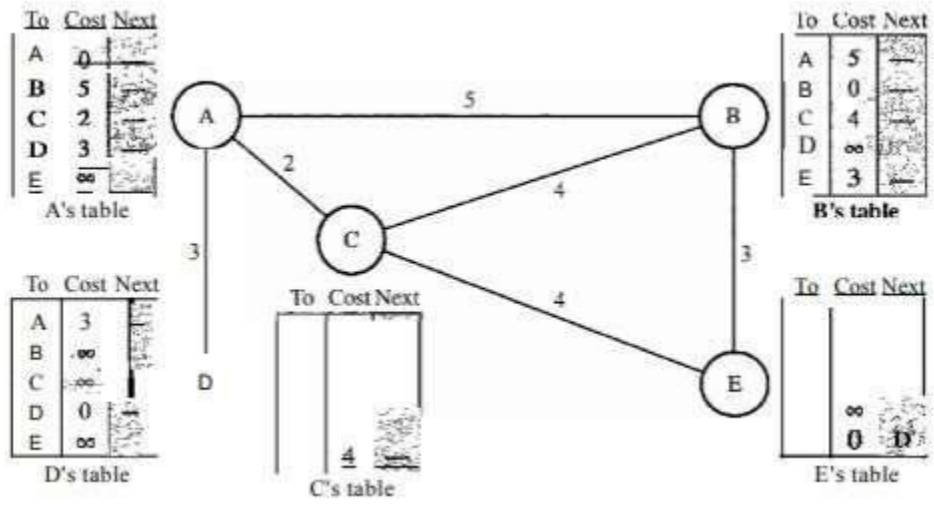
Q5. What do you mean by autonomous system? Explain how routing loops are prevented in Distance Vector Routing with examples.

Ans: In distance vector routing, the least-cost route between any two nodes is the route with minimum distance. In this protocol, as the name implies, each node maintains a vector (table) of minimum distances to every node. The table at each node also guides the packets to the desired node by showing the next stop in the route (next-hop routing). We can think of nodes as the cities in an area and the lines as the roads connecting them. A table can show a tourist the minimum distance between cities. In below Figure, we show a system of five nodes with their corresponding tables.

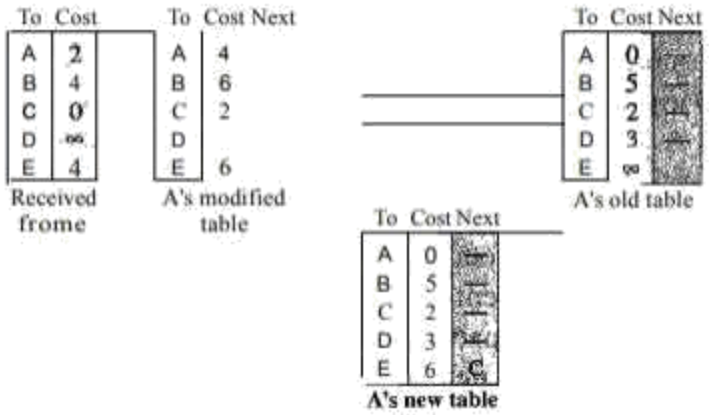


Hence, by sharing the routing table of one node with another the routing loops are prevented in distance vector routing and is calculated as below:

Initialization:

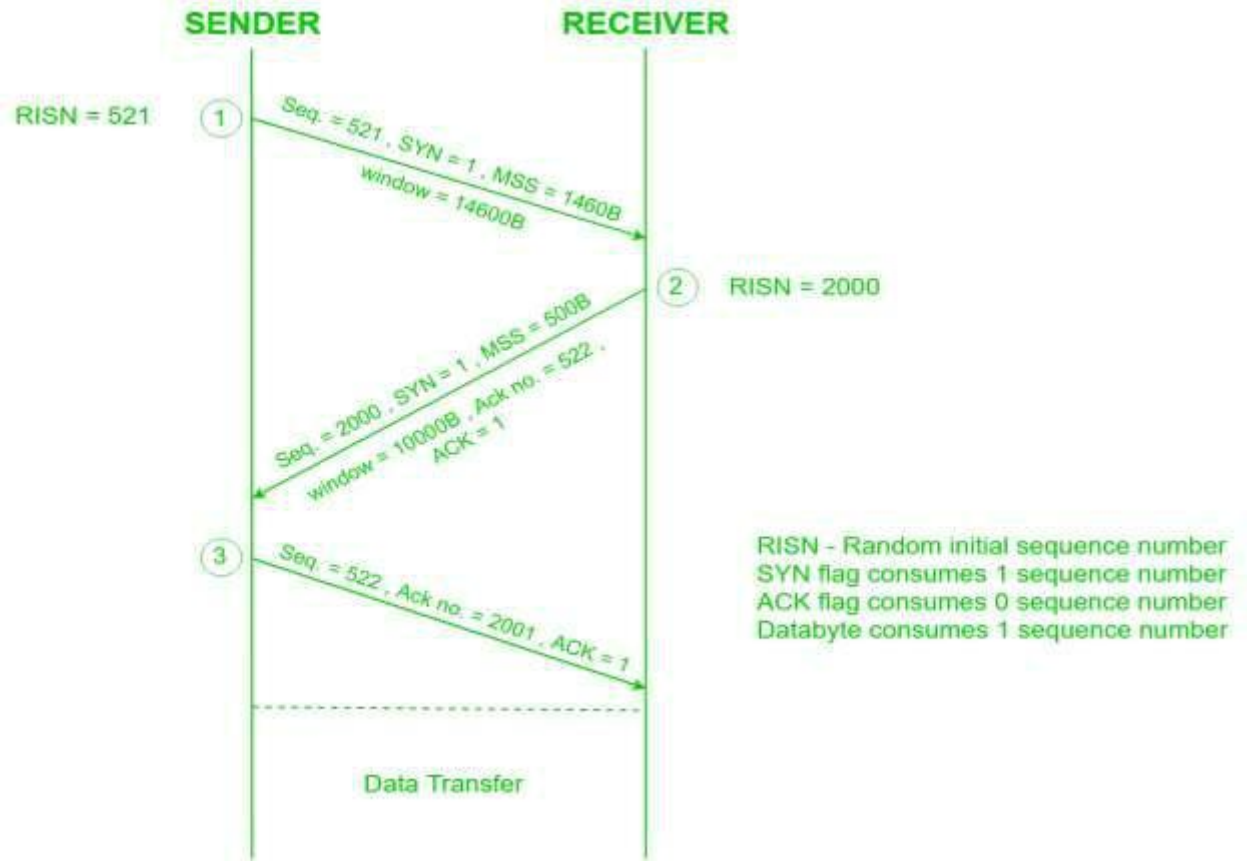


Updating:



Explain connection establishment and termination in TCP. Explain briefly about Leaky-Bucket algorithm for congestion control?

Part1: The connection establishment in TCP is called three way handshaking. In our example, an application program, called the client, wants to make a connection with another application program, called the server, using TCP as the transport layer protocol.



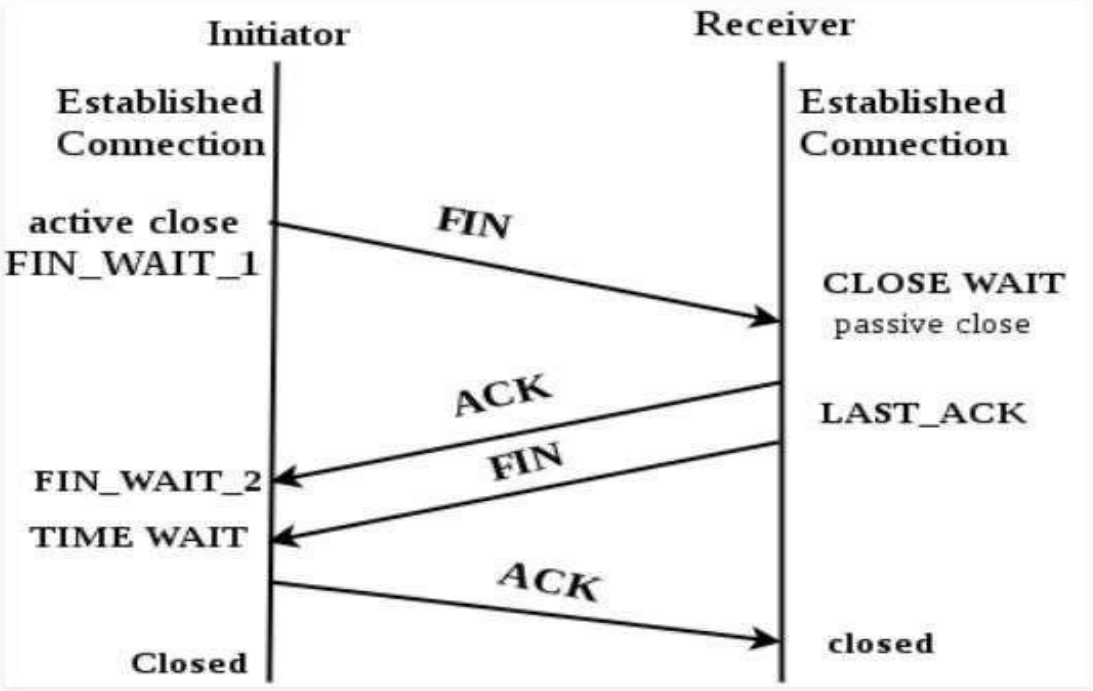
The three steps in this phase are as follows.

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

Connection termination in TCP using three way handshaking:

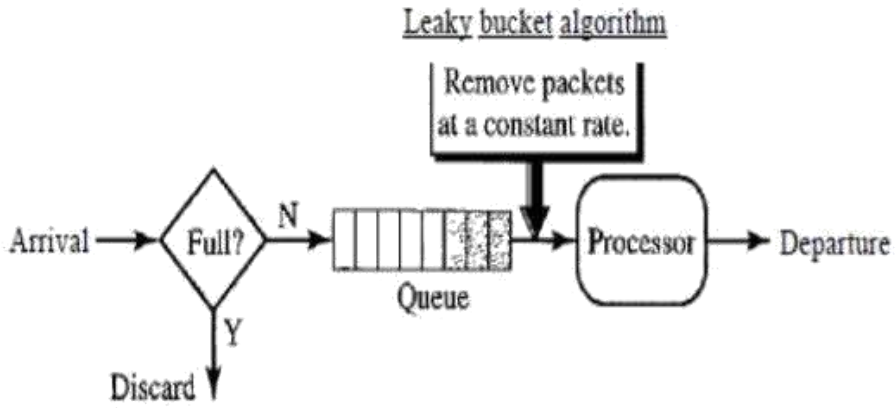
- In a normal situation, the client TCP, after receiving a close command from the client process, sends the first segment, a FIN segment in which the FIN flag is set. Note that a FIN segment can include the last chunk of data sent by the client, or it can be just a control segment. If it is only a control segment, it consumes only one sequence number.
- The server TCP, after receiving the FIN segment, informs its process of the situation and sends the second segment, a FIN +ACK segment, to confirm the receipt of the FIN segment from the client and at the same time to announce the closing of the connection in the other direction. This segment can also contain the last chunk of data from the server. If it does not carry data, it consumes only one sequence number.
- The client TCP sends the last segment, an ACK segment, to confirm the receipt of the FIN segment from the TCP server. This segment contains the acknowledgment number, which is 1 plus the sequence number received in the FIN segment from the server. This segment cannot carry data

and consumes no sequence numbers.



Part2: The following is Leaky Bucket algorithm for congestion control:

- Initialize a counter to n at the tick of the clock.
- If n is greater than the size of the packet, send the packet and decrement the counter by the packet size.
- Repeat this step until n is smaller than the packet size.
- Reset the counter and go to step 1



- **Why we need proxy servers? What are the importance of DNS and HTTP(S) while you are browsing any website?**

Part1: Mainly the proxy server is used for legal documentation and privacy. A proxy act as an intermediary between the user's computer and the Internet to prevent from attack and unexpected access. To implement Internet access control like authentication for Internet connection, bandwidth control, online time control, Internet web filter and content filter etc. An advantage of a proxy server is that its cache can serve all users. If one or more Internet sites are frequently requested, these are likely to be in the proxy's cache, which will improve user response time. A proxy can also log its interactions, which can be helpful for troubleshooting.

Part2: The importance of DNS while browsing any website are as follows:

- Generally DNS is the only system in the entire world that can help us browse the internet. With the internet becoming an integral part of the society, it has increasingly become important that DNS Servers remain maintained. Without them, then the internet would not exist.

- No need for memorizing IP addresses -DNS servers provide a nifty solution of converting domain or sub domain names to IP addresses. Imagine how it would feel having to memorize the IP addresses of twitter, Facebook, Google or any other site that we frequently use on a daily basis. It would definitely be horrific. Its system also makes it easy for search engines to be able to categorize and archive information.

- Security enhancement -DNS servers are an important component for the security of our home or work connections. DNS servers that have been designed for security purposes usually ensure that attempts to hack our server environment are thwarted before entry into our machines.
- However, it’s important to note that the word used is enhanced. This means that we will need other security measures put in place to protect our data, especially if it’s a large organization with tons of sensitive data.

- DNS servers have fast internet connections -People and organizations that use DNS servers can be able to take advantage of high connection speeds that are a key feature in some of these servers.

- DNS servers also have primary and secondary connections. This allows us to have internet uptime even when one of the servers is down for maintenance.

The importance of HTTP(S) while browsing any website are as follows:

- It preserves referrer data.
- It prevents tampering by third parties.
- It makes our site more secure for visitors.
- It encrypts all communication, including URLs, which protects things like browsing history and credit card numbers.

"IPv4 and IPv6 coexistence" what does this mean? Explain what you mean by address family translation in IPv4/IPv6 migration process with an appropriate figure.

Part1: From the IETF's perspective, the optimal approach for existing networks is to focus not on transition but on coexistence. Turn on IPv6 now and start using it; turn IPv4 off at some point in the future when it is no longer a business requirement. Therefore, in the opinion of the IETF, network administrators should:

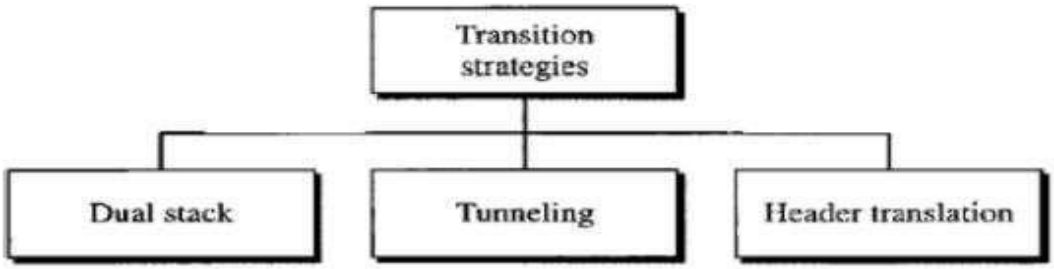
- Turn on IPv6 routing in the existing IPv4 networks.
- Contract IPv6 service with the upstream, peer, and downstream neighbors.
- Use the IPv6 protocol in addition to IPv4 in the applications and services both on server equipment and on their clients.

In doing so, network administrators will likely find software and hardware that are old or for some reason cannot be upgraded. They should schedule those upgrades as their budget allows. The reason to support coexistence of this type should be obvious: If IPv6 isn't working or if another network does not yet support IPv6, the affected applications or services will remain available via IPv4.Providing coexistence in network layer routing can be accomplished in any one of three ways:

- Enabling IPv6 on routers that carry IPv4.
- Enabling IPv6 on other routers as a parallel network internal to the customer-perceived network.
- Enabling IPv6 on a separate parallel network directly visible to neighboring networks and customers.

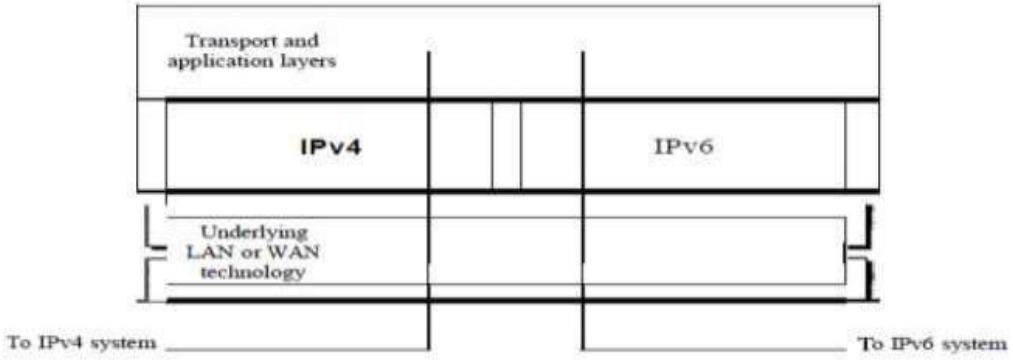
Part2: Because of the huge number of systems on the Internet, the transition from IPv4 to IPv6 cannot happen suddenly. It takes a considerable amount of time before every system in the Internet can move from IPv4 to IPv6. The transition must be smooth to prevent any problems between IPv4

and IPv6 systems. Three strategies have been devised to help the transition



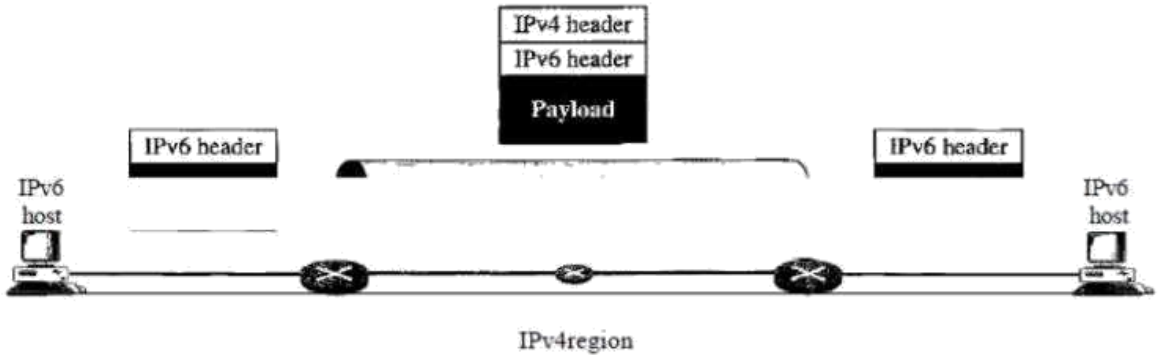
Dual Stack

It is recommended that all hosts, before migrating completely to version 6, have a dual stack of protocols. In other words, a station must run IPv4 and IPv6 simultaneously until all the Internet uses IPv6. To determine which version to use when sending a packet to a destination, the source host queries the DNS. If the DNS returns an IPv4 address, the source host sends an IPv4 packet. If the DNS returns an IPv6 address, the source host sends an IPv6 packet.



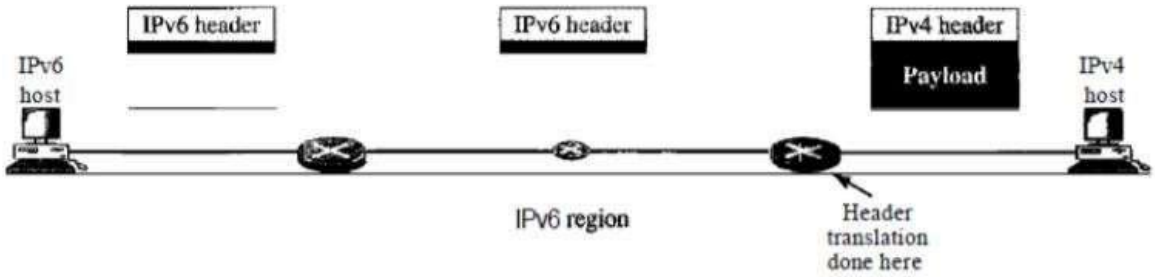
Tunneling

Tunneling is a strategy used when two computers using IPv6 want to communicate with each other and the packet must pass through a region that uses IPv4. To pass through this region, the packet must have an IPv4 address. So the IPv6 packet is encapsulated in an IPv4 packet when it enters the region, and it leaves its capsule when it exits the region. It seems as if the IPv6 packet goes through a tunnel at one end and emerges at the other end. To make it clear that the IPv4 packet is carrying an IPv6 packet as data, the protocol value is set to 41.



Header Translation

Header translation is necessary when the majority of the Internet has moved to IPv6 but some systems still use IPv4. The sender wants to use IPv6, but the receiver does not understand IPv6. Tunneling does not work in this situation because the packet must be in the IPv4 format to be understood by the receiver. In this case, the header format must be totally changed through header translation. The header of the IPv6 packet is converted to an IPv4 header.



- **Explain briefly the desirable properties of secure communication. Explain how packet filtering firewall works.**

Part1: The desirable properties of secure communication are as follows:

Message Confidentiality

Message confidentiality or privacy means that the sender and the receiver expect confidentiality. The transmitted message must make sense to only the intended receiver. To all others, the message must be garbage. When a customer communicates with her bank, she expects that the communication is totally confidential.

Message Integrity

Message integrity means that the data must arrive at the receiver exactly as they were sent. There must be no changes during the transmission, neither accidentally nor maliciously. As more and more monetary exchanges occur over the Internet, integrity is crucial.

Message Authentication

Message authentication is a service beyond message integrity. In message authentication the receiver needs to be sure of the sender's identity and that an imposter has not sent the message.

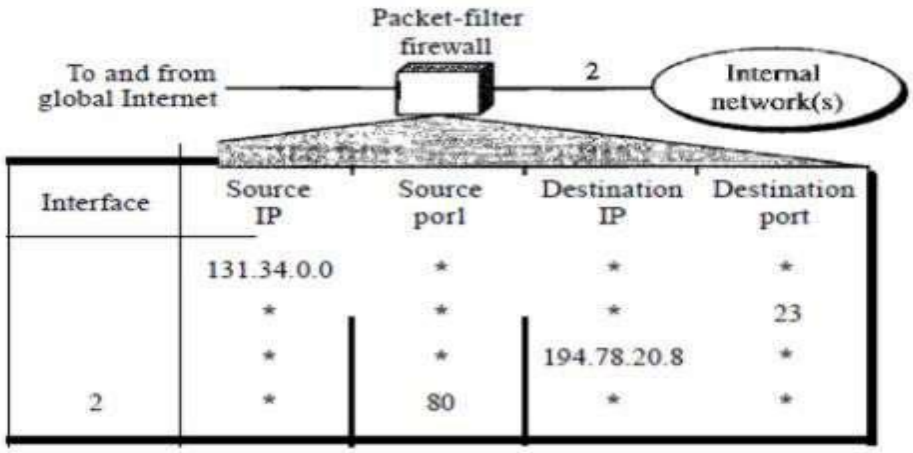
Message Non-repudiation

Message non repudiation means that a sender must not be able to deny sending a message that he or she, in fact, did send. The burden of proof falls on the receiver. For example, when a customer sends a message to transfer money from one account to another, the bank must have proof that the customer actually requested this transaction.

Entity Authentication

In entity authentication (or user identification) the entity or user is verified prior to Access to the system resources (files, for example). For example, a student who needs to access her university resources needs to be authenticated during the logging process. This is to protect the interests of the university and the student.

Part2: A firewall can be used as a packet filter. It can forward or block packets based on the information in the network layer and transport layer headers: source and destination IP addresses, source and destination port addresses, and type of protocol (TCP or UDP). A packet-filter firewall is a router that uses a filtering table to decide which packets must be discarded (not forwarded). Figure shows an example of a filtering table for this kind of a firewall.



Interface	Source IP	Source port	Destination IP	Destination port
	131.34.0.0	*	*	*
	*	*	*	23
	*	*	194.78.20.8	*
2	*	80	*	*

According to Figure, the following packets are filtered:

- Incoming packets from network 131.34.0.0 are blocked (security precaution). Note that the * (asterisk) means "any."
- Incoming packets destined for any internal TELNET server (port 23) are blocked.

- Incoming packets destined for internal host 194.78.20.8 are blocked. The organization wants this host for internal use only.
- Outgoing packets destined for an Http server (port 80) are blocked. The organization does not want employees to browse the Internet.

10. Write short notes on:

a) Digital signature

A digital signature is basically a way to ensure that an electronic document (e-mail, spreadsheet, text file, etc.) is authentic. Digital signatures rely on certain types of encryption to ensure authentication. Digital signatures are based on public key cryptography, also known as asymmetric cryptography. Using a public key algorithm such as RSA, one can generate two keys that are mathematically linked: one private and one public. To create a digital signature, signing software (such as an email program) creates a one way hash of the electronic data to be signed. The private key is then used to encrypt the hash. The encrypted hash along with other information, such as the hashing algorithm is the digital signature. Digital signatures, like handwritten signatures, are unique to each signer.

b) VPN

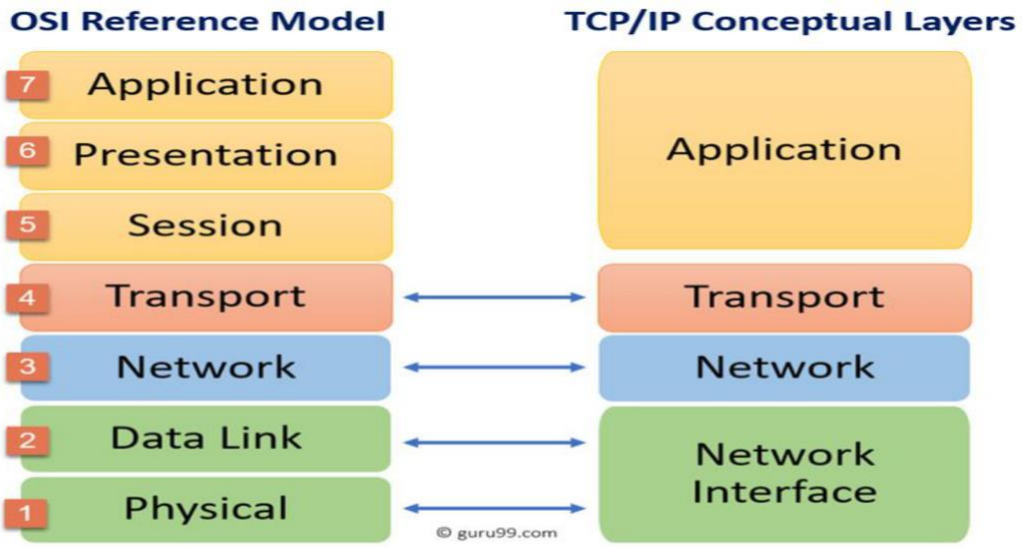
Virtual private network (VPN) is a technology that is gaining popularity among large organizations that use the global Internet for both intra and inter organization communication, but require privacy in their internal communications. We discuss VPN here because it uses the IPsec Protocol to apply security to the IP datagram. A technology called virtual private network allows organizations to use the global Internet for both purposes. VPN creates a network that is private but virtual. It is private because it guarantees privacy inside the organization. It is virtual because it does not use real private WANs; the network is physically public but virtually private.

2073 Shrawan

1. Differentiate between TCP/IP & OSI model. Define Frame Relay in detail.

The OSI Model is a logical and conceptual model that defines network communication used by systems open to interconnection and communication with other systems. The Open System Interconnection (OSI Model) also defines a logical network and effectively describes computer packet transfer by using various layers of protocols.

TCP/IP helps you to determine how a specific computer should be connected to the internet and how you can transmit data between them. It helps you to create a virtual network when multiple computer networks are connected together. TCP/IP stands for Transmission Control Protocol/ Internet Protocol. It is specifically designed as a model to offer highly reliable and end-to-end byte stream over an unreliable internetwork.



BASIS FOR COMPARISON	TCP/IP MODEL	OSI MODEL
Expands To	Transmission Control Protocol/ Internet Protocol	Open system Interconnect
Meaning	It is a client server model used for transmission of data over the internet.	It is a theoretical model which is used for computing system.

Number Of Layers	4 Layers	7 Layers
Developed by	Department of Defense (DoD)	ISO (International Standard Organization)
Tangible	Yes	No
Usage	Mostly used	Never used
Obeys	Horizontal approach	Vertical approach

Frame Relay

Frame relay is a packet-switching telecommunication service designed for cost-efficient data transmission for intermittent traffic between local area networks (LANs) and between endpoints in wide area networks (WANs). Frame relay puts data in a variable-size unit called a frame and leaves any necessary error correction (retransmission of data) up to the endpoints, which speeds up overall data transmission.

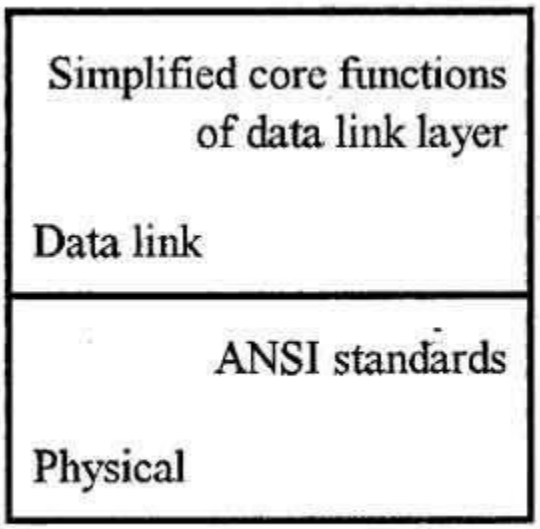
It uses a technology called fast packet in which error checking does not occur in any intermediate node of the transmission but done at the ends. It makes it more efficient than X.25, and a higher process speed achieved (it can transmit over 2,044 Mbps).Another advantage is that you need less powerful switching centers (nodes) and with less memory capacity than those needed by X25 (each X25 switching center uses the receive-store-check-relay method, while Frame Relay does not need checking or correcting errors).

If the traffic is hefty, with a large number of small packages, its performance is more excellent than X25.

Some important features of frame relay are :

- Frame relay operates at a high speed (1.544 Mbps to 44.376 Mbps).

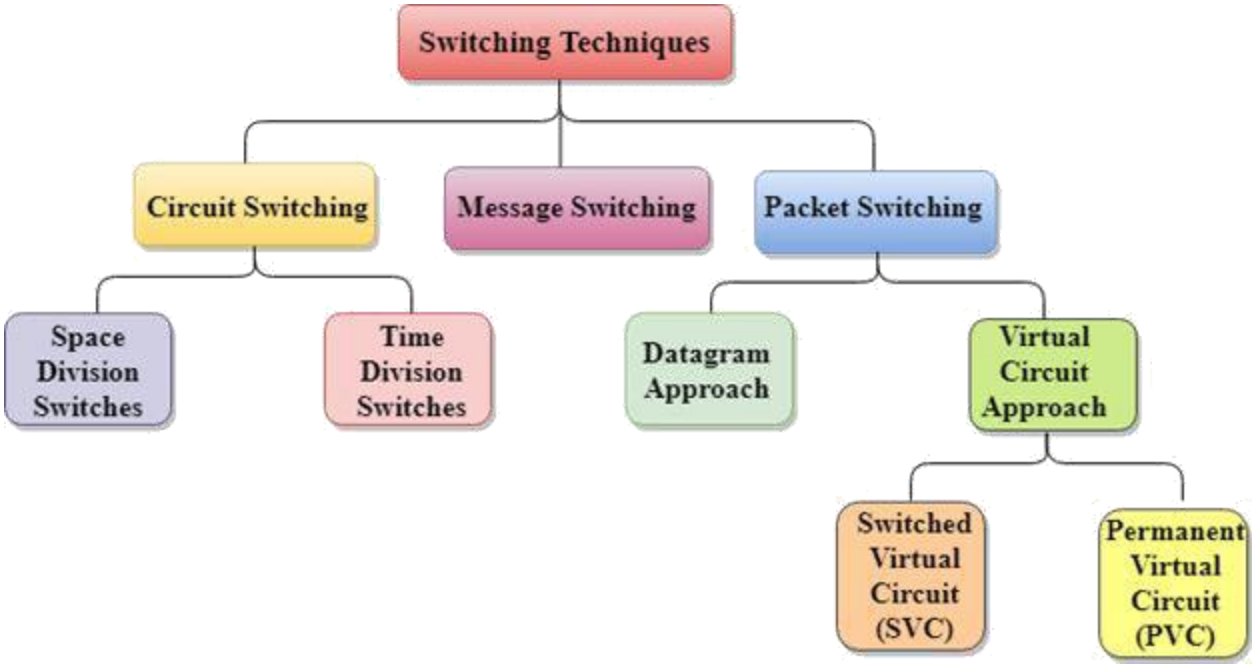
- Frame relay operates only in the physical and data link layers. So it can be easily used in Internet.
- It allows the bursty data.
- It has a large frame size of 9000 bytes. So it can accommodate all local area network frame sizes.
- Frame relay can only detect errors (at the data link layer). But there is no flow control or error control.



Frame relay layers

9. **What do you mean by switching in Communication? Compare switching with multiplexing. Explain the E1 Telephone Hierarchy**
   system.

Switching is the process of channeling data received from any number of input ports to another designated port that will transmit the data to its desired destination. The device through with the input data passes is called a switch. Data entering a port is referred to as ingress, while data leaving the port is referred to as egress. The switch represents the medium through which the data is routed to its final destination.



Switching Vs Multiplexing

- Multiplexing-Combining all the inputs into one output. Switching-Taking one input to the output, at a time/frequency
- Multiplexer sends multiple signals in parallel, while switches only send them in order.

The E-carrier is a member of the series of carrier systems developed for digital transmission of many simultaneous telephone calls by time-division multiplexing. The E carrier telecommunications system and the associated E 1, etc lines has been created by the European Conference of Postal and Telecommunications Administrations (CEPT) as a digital telecommunications carrier scheme for carrying multiple links.

The E-carrier system enables the transmission of several (multiplexed) voice/data channels simultaneously on the same transmission facility or line. Of the various levels of the E-carrier system, the E1 and E3 levels are the only ones that are used.

E CARRIER LINK DESIGNATION	DATA RATE
E0	64 kbps
E1	2.048 Mbps
E2	8.448 Mbps
E3	34.368 Mbps
E4	139.264 Mbps
E5	564.992 Mbps

E1 link operates over two separate sets of wires, usually Unshielded twisted pair (balanced cable) or using coaxial (unbalanced cable). A peak signal is encoded with pulses using a method avoiding long periods without polarity changes. These pulses are further divided into 32 timeslots which are further broken down to 8 bits each. Each time-slot sends and receives a PCM (Pulse Code Modulation) chunk to digitally represent sampled analog signals.

This form of data-transfer allows for a rate of flow useful in voice-over and telecom applications.

- **What do you understand by Media Access Control ? What is its significance in data link layer ? Explain why token bus is also called as the token ring.**

A media access control is a network data transfer policy that determines how data is transmitted between two computer terminals through a network cable. The media access control policy involves sub-layers of the data link layer 2 in the OSI reference model. MAC describes the process that is employed to control the basis on which devices can access the shared network. Some level of control is required to ensure the ability of all devices to access the network within a reasonable period of time, thereby resulting in acceptable access and response times.

This network channel through which data is transmitted between terminal nodes to avoid collision has three various ways of accomplishing this purpose. They include:

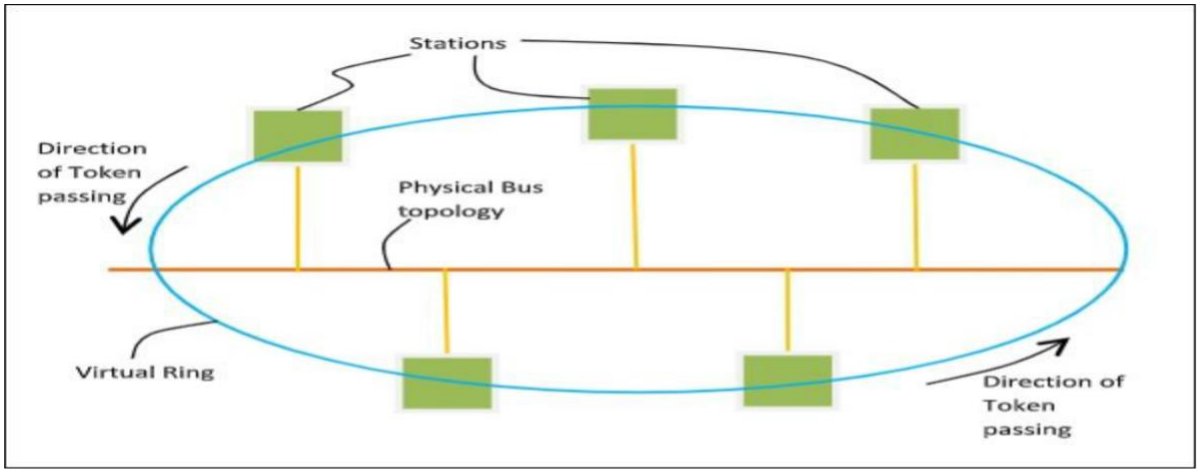
- Carrier sense multiple access with collision avoidance (CSMA/CA)
- Carrier sense multiple access with collision detection (CSMA/CD)
- Demand priority
- Token passing

The essence of the MAC protocol is to ensure non-collision and eases the transfer of data packets between two computer terminals. The basic function of MAC is to provide an addressing mechanism and channel access so that each node available on a network can communicate with other nodes available on the same or other networks. Sometimes people refer to this as the MAC layer.

Token Bus (IEEE 802.4) is a standard for implementing token ring over virtual ring in LANs. The physical media has a bus or a tree topology and uses coaxial cables. A virtual ring is created with the nodes/stations and the token is passed from one node to the next in a sequence along this virtual ring. Each node knows the address of its preceding station and its succeeding station. A station can only transmit data when it has the token. The working principle of token bus is similar to Token Ring.

Token Passing Mechanism in Token Bus

A token is a small message that circulates among the stations of a computer network providing permission to the stations for transmission. If a station has data to transmit when it receives a token, it sends the data and then passes the token to the next station; otherwise, it simply passes the token to the next station. This is depicted in the following diagram −



Differences between Token Ring and Token Bus

Token Ring	Token Bus
The token is passed over the physical ring formed by the stations and the coaxial cable network.	The token is passed along the virtual ring of stations connected to a LAN.
The stations are connected by ring topology, or sometimes star topology.	The underlying topology that connects the stations is either bus or tree topology.
It is defined by IEEE 802.5 standard.	It is defined by IEEE 802.4 standard.
The maximum time for a token to reach a station can be calculated here.	It is not feasible to calculate the time for token transfer.

Discuss about the network congestion? Explain how different network parameters effect the congestion. Compare operation of link state routing with distance vector routing.

Network congestion in data networking and queueing theory is the reduced quality of service that occurs when a network node or link is carrying more data than it can handle. Typical effects include queueing delay, packet loss or the blocking of new connections.

Congestion, in the context of networks, refers to a network state where a node or link carries so much data that it may deteriorate network service quality, resulting in queuing delay, frame or data packet loss and the blocking of new connections. In a congested network, response time slows with reduced network throughput. Congestion occurs when bandwidth is insufficient and network data traffic exceeds capacity.

Data packet loss from congestion is partially countered by aggressive network protocol retransmission, which maintains a network congestion state after reducing the initial data load. This can create two stable states under the same data traffic load - one dealing with the initial load and the other maintaining reduced network throughput.

Effects of Congestion

- As delay increases, performance decreases.
- If delay increases, retransmission occurs, making situation worse.

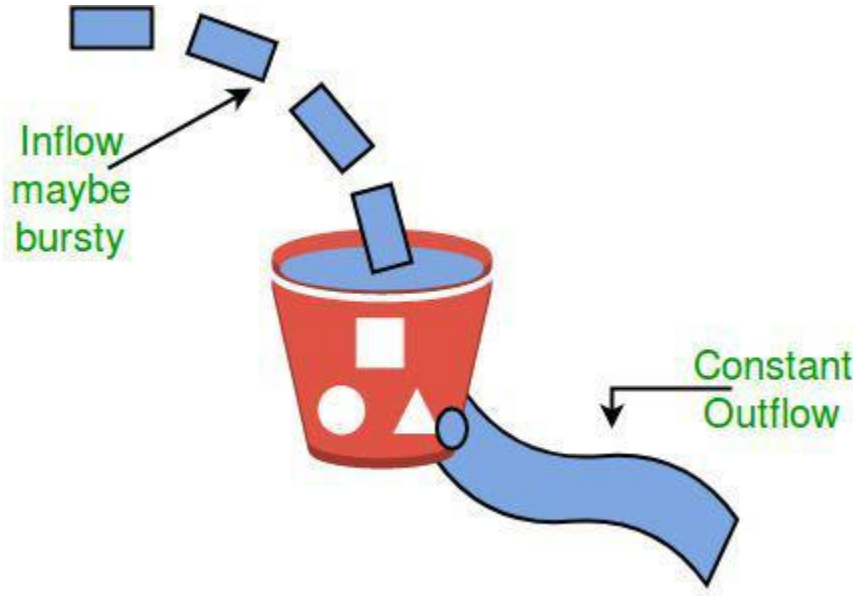
Cause of Congestion

- Over-subscription
- Poor network design/mis-configuration
- Over-utilized devices
- Faulty devices
- Security attack

Congestion control algorithms

1. Leaky Bucket Algorithm

Imagine a bucket with a small hole in the bottom.No matter at what rate water enters the bucket, the outflow is at constant rate.When the bucket is full with water additional water entering spills over the sides and is lost.



Similarly, each network interface contains a leaky bucket and the following steps are involved in leaky bucket algorithm:

- When host wants to send packet, packet is thrown into the bucket.
- The bucket leaks at a constant rate, meaning the network interface transmits packets at a constant rate.
- Bursty traffic is converted to a uniform traffic by the leaky bucket
- In practice the bucket is a finite queue that outputs at a finite rate.

2. Token bucket Algorithm

The leaky bucket algorithm enforces output pattern at the average rate, no matter how bursty the traffic is. So in order to deal with the bursty traffic we need a flexible algorithm so that the data is not lost. One such algorithm is token bucket algorithm. Steps of this algorithm can be described as follows:

- In regular intervals tokens are thrown into the bucket. Ƒ
- The bucket has a maximum capacity. Ƒ
- If there is a ready packet, a token is removed from the bucket, and the packet is sent.
- If there is no token in the bucket, the packet cannot be sent.

Routing

Routing is the mechanism of transferring information from a source to destination across an internetwork. The distance vector routing and link state routing are the two of routing algorithms, categorised depending on the way the routing tables are updated.

The prior difference between Distance vector and link state routing is that in distance vector routing the router share the knowledge of the entire autonomous system whereas in link state routing the router share the knowledge of only their neighbour routers in the autonomous system.

Definition of Distance Vector Routing

In distance vector routing, a router need not know the entire path to every network segment; it only requires to know the direction or vector in which to send the packet. The technique determines the direction (vector) and distance (hop count) to any network in the internetwork.

Distance vector routing algorithms periodically send all or parts of their routing table to their adjacent neighbours. The routers running a distance vector routing protocol will automatically send periodic updates even if there are no changes in the network.

A router can verify all the known routes and alters its local routing table on the basis of the updated information received from neighbouring routing. This process is referred to as “routing

by rumour" because the routing information that a router has of the network topology is based on the perspective of the routing table of the neighbour router.

RIP and IGRP is a commonly used distance vector protocol that uses hop counts or its routing

BASIS FOR COMPARISON	DISTANCE VECTOR ROUTING	LINK STATE ROUTING
Algorithm	Bellman ford	Dijsktra
Network view	Topology information from the neighbour point of view	Complete information on the network topology
Best path calculation	Based on the least number of hops	Based on the cost
Updates	Full routing table	Link state updates
Updates frequency	Periodic updates	Triggered updates
CPU and memory	Low utilisation	Intensive
Simplicity	High simplicity	Requires a trained network administrator
Convergence	Moderate	Fast

metrics.

Definition of Link State Routing

In link-state routing, each router attempt to construct its own internal map of the network topology. At the initial stage of start-up, when a router becomes active, it sends the messages into the network and collects the information from the routers to which it is directly connected. It also provides information about whether the link to reach the router is active or not. This information is used by other routers to build a map of network topology. Then the router uses the map to choose the best path.

The link state routing protocols respond swiftly to the network changes. It sends triggered updates when a network change occurs and sends periodic updates at long time intervals such

as 30 minutes. If the link alters state, the device detected the alteration generates and propagate an update message regarding that link to all routers. Then each router takes a copy of the update message and update its routing table and forwards the message to all neighbouring router.

This flooding of the update message is needed to ensure that all routers update their database before creating an update routing table that reflects the new technology. OSPF protocol is the example link state routing.

How web server communication and file server communication are possible in network ? Explain with protocol used. Define socket programming.

The World Wide Web has a client/server architecture. This means that a client program running on your computer (your Web browser) requests information from a server program running on another computer somewhere on the Internet. That server then sends the requested data back over the Net to your browser program, which interprets and displays the data on your screen. HTTP is a connectionless text based protocol. Clients (web browsers) send requests to web servers for web elements such as web pages and images. After the request is serviced by a server, the connection between client and server across the Internet is disconnected. A new connection must be made for each request. Most protocols are connection oriented. This means that the two computers communicating with each other keep the connection open over the Internet. HTTP does not however. Before an HTTP request can be made by a client, a new connection must be made to the server.

When you type a URL into a web browser, this is what happens:

- If the URL contains a domain name, the browser first connects to a domain name server and retrieves the corresponding IP address for the web server.
- The web browser connects to the web server and sends an HTTP request (via the protocol stack) for the desired web page.
- The web server receives the request and checks for the desired page. If the page exists, the web server sends it. If the server cannot find the requested page, it will send an HTTP 404 error message. (404 means 'Page Not Found' as anyone who has surfed the web probably knows.)
- The web browser receives the page back and the connection is closed.
- The browser then parses through the page and looks for other page elements it needs to complete the web page. These usually include images, applets, etc.
- For each element needed, the browser makes additional connections and HTTP requests to the server for each element.

- When the browser has finished loading all images, applets, etc. the page will be completely loaded in the browser window.

Another commonly used Internet service is electronic mail. E-mail uses an application level protocol called Simple Mail Transfer Protocol or SMTP. SMTP is also a text based protocol, but unlike HTTP, SMTP is connection oriented. SMTP is also more complicated than HTTP. There are many more commands and considerations in SMTP than there are in HTTP. When you open your mail client to read your e-mail, this is what typically happens:

- The mail client (Netscape Mail, Lotus Notes, Microsoft Outlook, etc.) opens a connection to it's default mail server. The mail server's IP address or domain name is typically setup when the mail client is installed.
- The mail server will always transmit the first message to identify itself.
- The client will send an SMTP HELO command to which the server will respond with a 250 OK message.
- Depending on whether the client is checking mail, sending mail, etc. the appropriate SMTP commands will be sent to the server, which will respond accordingly.
- This request/response transaction will continue until the client sends an SMTP QUIT command. The server will then say goodbye and the connection will be closed.

SOCKET PROGRAMMING

Sockets programming is the fundamental technology behind communications on TCP/IP networks. A socket is one endpoint of a two-way link between two programs running on a network. The socket provides a bidirectional communication endpoint to send and receive data with another socket.

Socket connections normally run between two different computers on a local area network (LAN) or across the internet, but they can also be used for interprocess communication on a single computer.

How Server Sockets Work

Typically, a server runs on one computer and accesses a socket that is bound to a specific port. The server waits for a different computer to make a connection request. The client computer knows the hostname of the server computer and the port number on which the server is listening. The client computer identifies itself, and — if everything goes right — the server permits the client computer to connect.

The steps for establishing a TCP socket on the client side are the following:

10. Create a socket using the socket() function;

11. Connect the socket to the address of the server using the connect() function;
12. Send and receive data by means of the read() and write() functions.

The steps involved in establishing a TCP socket on the server side are as follows:

Create a socket with the socket() function;
Bind the socket to an address using the bind() function;
Listen for connections with the listen() function;
Accept a connection with the accept() function system call. This call typically blocks until a client connects with the server.
Send and receive data by means of send() and receive().

5. What are the factors that lead to the development of IPV6 ? Define process of transition from IPV4 to IPV6.

Why IPv6?	IPv4	IPv6
IPv6 has massive address abundance	4.29×10^9 = 4.3 billion addresses - far less than even a single IP address per person on the planet.	3.4×10^{38} = 340 trillion trillion trillion addresses - about 670 quadrillion addresses per square millimetre of the Earth's surface.
IPv6 networks are easier and cheaper to manage	Networks must be configured manually or with DHCP. IPv4 has had many overlays to handle Internet growth, which demand increasing maintenance efforts.	IPv6 networks provide autoconfiguration capabilities. They are simpler, flatter and more manageable, especially for large installations.
IPv6 restores end-to-end transparency	Widespread use of NAT devices means that a single NAT address can mask thousands of non-routable addresses, making end-to-end integrity unachievable.	Direct addressing is possible due to vast address space - the need for network address translation devices is effectively eliminated.
IPv6 has improved security features	Security is dependent on applications - IPv4 was not designed with security in mind.	IPSEC is built into the IPv6 protocol, usable with a suitable key infrastructure.

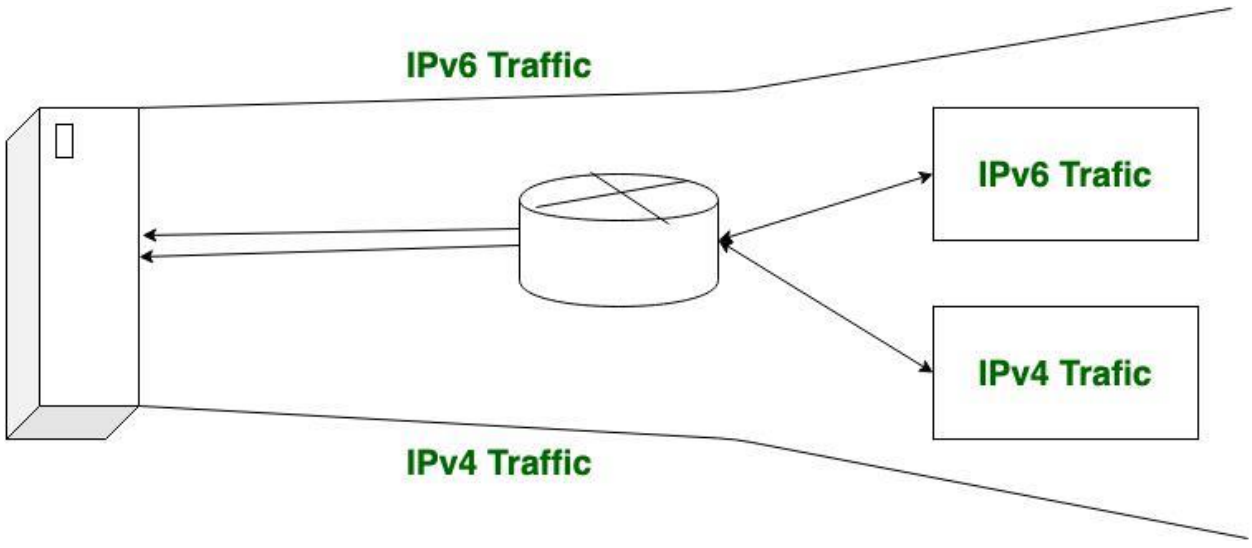
IPv6 has improved mobility capabilities	Relatively constrained network topologies restrict mobility and interoperability capabilities in the IPv4 Internet.	IPv6 provides interoperability and mobility capabilities which are already widely embedded in network devices.
IPv6 encourages innovation	IPv4 was designed as a transport and communications medium, and increasingly any work on IPv4 is to find ways around the constraints.	Given the numbers of addresses, scalability and flexibility of IPv6, its potential for triggering innovation and assisting collaboration is unbounded.

There is an obvious need for IPv6, but it has seen slow adoption. This is due to multiple factors, including cost, the complexity of migrating from IPv4 to IPv6, and existing workarounds that make it possible to postpone the update to IPv6.

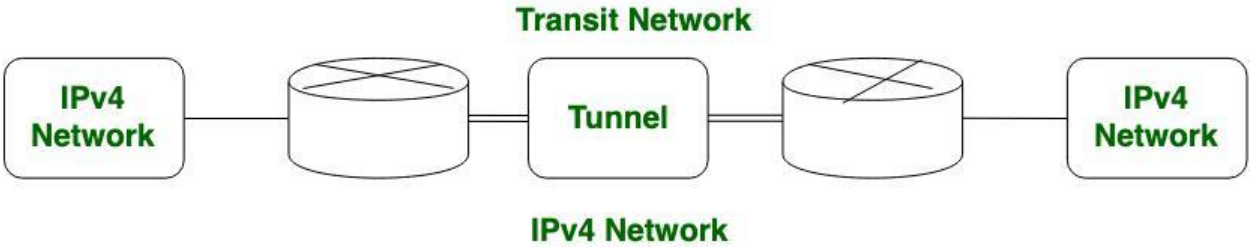
For the reasons above, the transition to IPv6 won't happen overnight, and IPv4 likely isn't going away anytime soon. Instead, applications and ISPs will begin to offer support for both IP versions, a concept known as dual stack support. This allows for internet connected devices to communicate regardless of the IP version used.

Despite the obstacles, the transition to IPv6 is necessary and inevitable. The process of transition from IPV4 to IPV6 are:

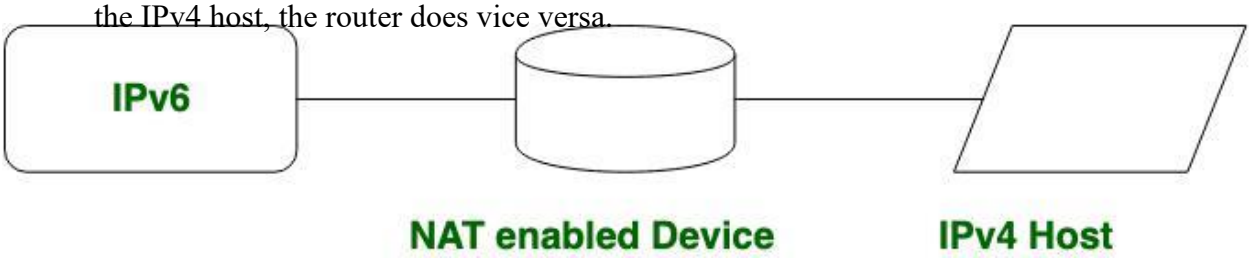
- Dual Stack Routers : In dual stack router, A router's interface is attached with Ipv4 and IPv6 addresses configured is used in order to transition from IPv4 to IPv6.A given server with both IPv4 and IPv6 address configured can communicate with all hosts of IPv4 and IPv6 via dual stack router (DSR). The dual stack router (DSR) gives the path for all the hosts to communicate with server without changing their IP addresses.



5. Tunneling: Tunneling is used as a medium to communicate the transit network with the different ip versions. the different IP versions such as IPv4 and IPv6 are present. The IPv4 networks can communicate with the transit or intermediate network on IPv6 with the help of Tunnel. Its also possible that the IPv6 network can also communicate with IPv4 networks with the help of Tunnel.



B) NAT Protocol Translation :This is another important method of transition to IPv6 by means of a NAT-PT (Network Address Translation – Protocol Translation) enabled device. With the help of a NAT-PT device, actual can take place happens between IPv4 and IPv6 packets and vice versa. A host with IPv4 address sends a request to an IPv6 enabled server on Internet that does not understand IPv4 address. In this scenario, the NAT-PT device can help them communicate. When the IPv4 host sends a request packet to the IPv6 server, the NAT-PT device/router strips down the IPv4 packet, removes IPv4 header, and adds IPv6 header and passes it through the Internet. When a response from the IPv6 server comes for the IPv4 host, the router does vice versa.



11. Compare symmetric key encryption with assymetric key encryption method. Explain RSA algorithm with example.

Definition of Symmetric Encryption

Symmetric encryption is a technique which allows the use of only one key for performing both the encryption and the decryption of the message shared over the internet. It is also known as the conventional method used for encryption.

In symmetric encryption, the plaintext is encrypted and is converted to the ciphertext using a key and an encryption algorithm. While the cipher text is converted back to plain text using the same key that was used for encryption, and the decryption algorithm. Symmetric encryption algorithm executes faster and is less complex hence; they are used for bulk data transmission.

Symmetric Encryption

In symmetric encryption, the host that are participating in the communication already have the secret key that is received through the external means. The sender of the message or information will use the key for encrypting the message, and the receiver will use the key for decrypting the message. The commonly used symmetric encryption algorithms are DES, 3 DES, AES, RC4.

Definition of Asymmetric Encryption

Asymmetric encryption is an encryption technique that uses a pair of key (private key and public key) for encryption and decryption. Asymmetric encryption uses the public key for the encryption of the message and the private key for the decryption of the message.

The public key is freely available to anyone who is interested in sending the message. The private key is kept secret with the receiver of the message. Any message that is encrypted by the public key and the algorithm, is decrypted using the same the algorithm and the matching private key of corresponding public key.

Asymmetric Encryption

The asymmetric encryption algorithm execution is slow. As asymmetric encryption algorithm are complex in nature and have the high computational burden. Hence, the asymmetric encryption is used for securely exchanging the keys instead of the bulk data transmission.

Asymmetric encryption is generally used for establishing a secure channel over the non-secure medium like the internet. The most common asymmetric encryption algorithm are Diffie-Hellman and RSA algorithm.

BASIS FOR COMPARISON	SYMMETRIC ENCRYPTION	ASYMMETRIC ENCRYPTION
Basic	Symmetric encryption uses a single key for both encryption and Decryption.	Asymmetric encryption uses a different key for encryption and decryption.
Performance	Symmetric encryption is fast in execution.	Asymmetric Encryption is slow in execution due to the high computational burden.
Algorithms	DES, 3DES, AES, and RC4.	Diffie-Hellman, RSA.
Purpose	The symmetric encryption is used for bulk data transmission.	The asymmetric encryption is often used for securely exchanging secret keys.

RSA ALGORITHM

RSA algorithm is an asymmetric cryptography algorithm which means, there should be two keys involve while communicating, i.e., public key and private key. There are simple steps to solve problems on the RSA Algorithm.

The idea of RSA is based on the fact that it is difficult to factorize a large integer. The public key consists of two numbers where one number is multiplication of two large prime numbers. And private key is also derived from the same two prime numbers. So if somebody can factorize the large number, the private key is compromised. Therefore encryption strength totally lies on the key size and if we double or triple the key size, the strength of encryption increases exponentially. RSA keys can be typically 1024 or 2048 bits long, but experts believe that 1024 bit keys could be broken in the near future. But till now it seems to be an infeasible task.

Example-1:

- **Step-1: Choose two prime number** p and q
  Lets take $p = 3$ and $q = 11$

- **Step-2: Compute the value of** n and ϕ
  It is given as,

  $n = p \times q$ and $\phi = (p - 1) \times (q - 1)$

  Here in the example,
  $n = 3 \times 11 = 33$
  $\phi = (3 - 1) \times (11 - 1) = 2 \times 10 = 20$

- **Step-3: Find the value of** e **(public key)**
  Choose e, such that e should be co-prime. Co-prime means it should not multiply by factors of ϕ and also not divide by ϕ
  Factors of ϕ are, $20 = 5 \times 4 = 5 \times 2 \times 2$ so e should not multiply by 5 and 2 and should not divide by 20.

  So, primes are 3, 7, 11, 17, 19..., as 3 and 11 are taken choose e as 7

  Therefore, $e = 7$

- **Step-4: Compute the value of** d **(private key)**
  The condition is given as,
  $gcd(\phi, e) = \phi x + ey = 1$ where y is the value of d.
  To compute the value of d,

  1. Form a table with four columns i.e., a, b, d, and k.
  2. Initialize a = 1, b = 0, d = ϕ, k = – in first row.
  3. Initialize a = 0, b = 1, d = e, $k = \frac{\phi}{e}$ in second row.
  4. From the next row, apply following formulas to find the value of next a, b, d, and k, which is given as
     - $a_i = a_{i-2} - (a_{i-1} \times k_{i-1})$
     - $b_i = b_{i-2} - (b_{i-1} \times k_{i-1})$
     - $d_i = d_{i-2} - (d_{i-1} \times k_{i-1})$
     - $k_i = \frac{d_{i-2}}{d_{i-1}}$

  As soon as, $d = 1$, stop the process and check for the below condition

```
if b > ϕ
    b = b mod ϕ
if b < 0
    b = b + ϕ
```

For a given example, the table will be,

A	B	D	K
1	0	20	–
0	1	7	2
1	-2	6	1
-1	3	1	–

As in the above table $d = 1$, stop the process and check for the condition given for the b

$\therefore b = 3$

To verify that b is correct, the above condition should satisfy, i.e. $gcd(\phi, e) = \phi x + ey = (20 \times -1) + (7 \times 3) = 1$. Hence d is correct.

- **Step-5: Do the encryption and decryption**

  Encryption is given as,

  $c = t^e \mod n$

  Decryption is given as,

  $t = c^d \mod n$

  For the given example, suppose $t = 2$, so

  Encryption is $c = 2^7 \mod 33 = 29$

  Decryption is $t = 29^3 \mod 33 = 2$

  Therefore in the final, $p = 3, q = 11, \phi = 20, n = 33, e = 7$ and $d = 3$

[source : https://www.geeksforgeeks.org/rsa-algorithm-cryptography/]

9. What do you mean by Firewall ? Explain different types of firewall.

A firewall is software used to maintain the security of a private network. Firewalls block unauthorized access to or from private networks and are often employed to prevent unauthorized Web users or illicit software from gaining access to private networks connected to the Internet. A firewall may be implemented using hardware, software, or a combination of both.

A firewall is recognized as the first line of defense in securing sensitive information. For better safety, the data can be encrypted. Firewalls generally use two or more of the following methods:

- Packet Filtering: Firewalls filter packets that attempt to enter or leave a network and either accept or reject them depending on the predefined set of filter rules.
- Application Gateway: The application gateway technique employs security methods applied to certain applications such as Telnet and File Transfer Protocol servers.
- Circuit-Level Gateway:A circuit-level gateway applies these methods when a connection such as Transmission Control Protocol is established and packets start to move.
- Proxy Servers: Proxy servers can mask real network addresses and intercept every message that enters or leaves a network.
- Stateful Inspection or Dynamic Packet Filtering: This method compares not just the header information, but also a packet's most important inbound and outbound data parts. These are then compared to a trusted information database for characteristic matches. This determines whether the information is authorized to cross the firewall into the network.
- Software Firewalls : device rather than a separate piece of hardware (or a cloud server). The big benefit of a software firewall is that it's highly useful for creating defense in depth by isolating individual network endpoints from one another.
- Hardware Firewalls : Hardware firewalls use a physical appliance that acts in a manner similar to a traffic router to intercept data packets and traffic requests before they're connected to the network's servers. Physical appliance-based firewalls like this excel at perimeter security by making sure malicious traffic from outside the network is intercepted before the company's network endpoints are exposed to risk.

[source: https://www.compuquip.com/blog/the-different-types-of-firewall-architectures]

- Write Short Notes On:

  HDLC

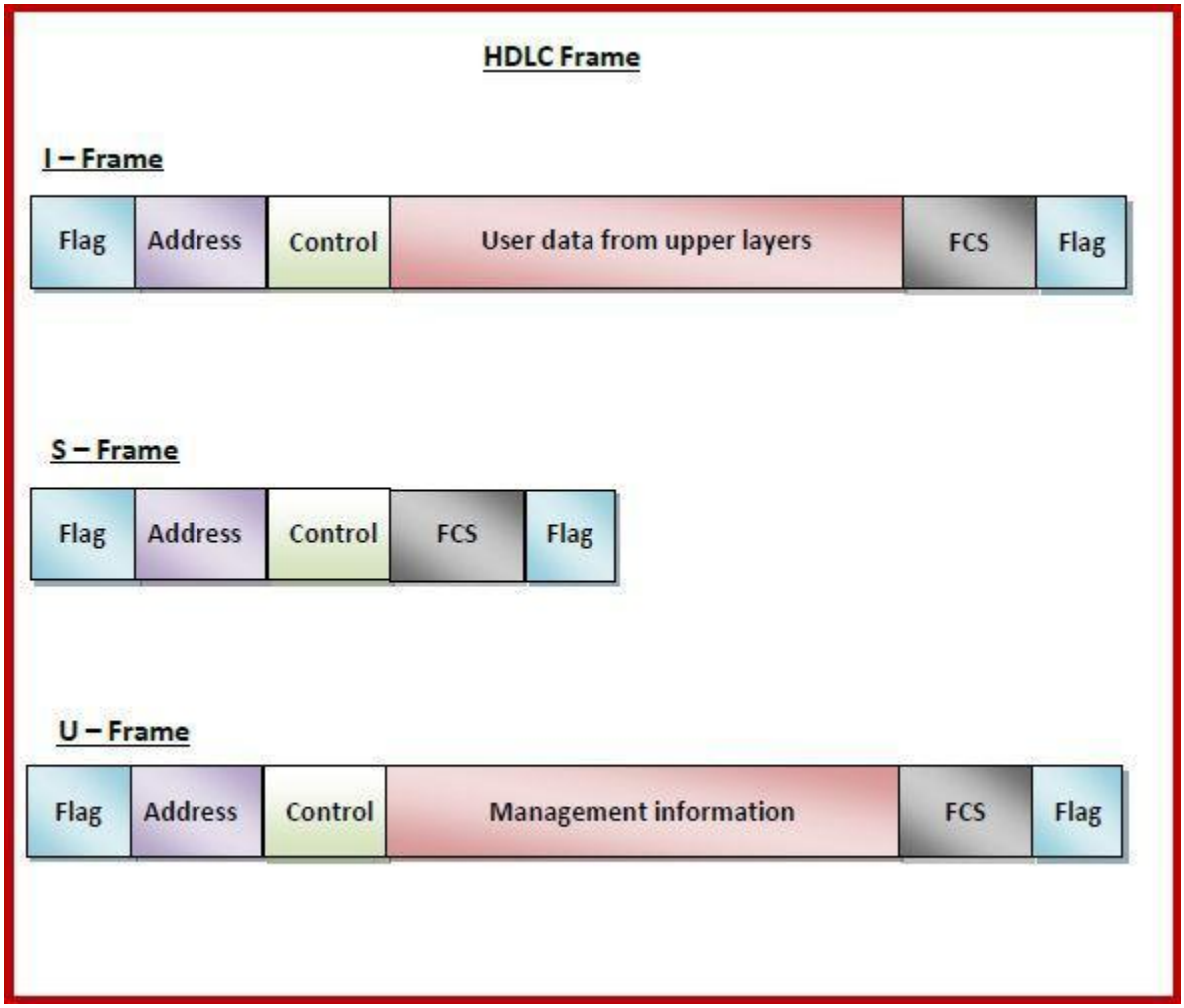
  High-level Data Link Control (HDLC) is a group of communication protocols of the data link layer for transmitting data between network points or nodes. Since it is a data link protocol, data is organized into frames. A frame is transmitted via the network to the

destination that verifies its successful arrival. It is a bit - oriented protocol that is applicable for both point - to - point and multipoint communications.

HDLC supports two types of transfer modes, normal response mode and asynchronous balanced mode.

C) Normal Response Mode (NRM) − Here, two types of stations are there, a primary station that send commands and secondary station that can respond to received commands. It is used for both point - to - point and multipoint communications.

D) Asynchronous Balanced Mode (ABM) − Here, the configuration is balanced, i.e. each station can both send commands and respond to commands. It is used for only point - to - point communications.



b. Web Server

A Web server is software or hardware that uses HTTP (Hypertext Transfer Protocol) and other protocols to respond to client requests made over the World Wide Web (WWW). Web server software controls how a user accesses hosted files. It is accessed through the domain

names of websites and ensures the delivery of the site's content to the requesting user. As hardware, a Web server is a computer that holds web server software and other files related to a website, such as HTML documents, images and JavaScript files. Web server hardware is connected to the internet and allows data to be exchanged with other connected devices.

The Web server process is an example of the client/server model. All computers that host Web sites must have Web server software. Leading Web servers include Apache, Microsoft's Internet Information Server (IIS) and Nginx -- pronounced engine X. Other Web servers include Novell's NetWare server, Google Web Server (GWS) and IBM's family of Domino servers.

Web servers often come as part of a larger package of internet- and intranet-related programs that are used for:

- Sending and receiving emails.
- Downloading requests for File Transfer Protocol (FTP) files.
- Building and publishing Web pages.

Considerations in choosing a Web server include how well it works with the operating system and other servers; its ability to handle server-side programming; security characteristics; and the particular publishing, search engine and site building tools that come with it.

- You are a private contractor hired by the large company to setup the network for their enterprise and you are given a large number of consecutive IP address starting at 202.70.64.0/19. Suppose that four department A, B, C and D request 100, 500, 800 and 400 addresses respectively, how the subnetting can be performed so that wastage will be minimum?

Solution,

Class A	Class D	Class B	Class C
Users = 100+2=102	users = 400+2=402	users = 500+2=502	users = 800+2=802
2^7 >=102	2^9>= 402	2^9>=502	2^10 = 802
hid= 7	hid = 9	hid=9	hid=10
Nid = 128-7=121	nid = 512-9 = 503	nid = 503	nid = 1014
202.70.64.0/121	202.70.64.128/503	202.70.66.128/503	202.70.68.128/1014
To	To	To	To
202.70.64.102/121	202.70.66.17/503	202.70.68.117/503	202.70.71.161/1014
To	To	To	To
202.70.60.127/121	202.70.66.127/503	202.70.68.127/503	202.70.72.127/1014

SM:
255.255.255.128 255.255.255.0 255.255.255.0 255.255.251.0

2076 Ashwin

9. What are the features of Client/Server Architecture? What are headers and trailers and how do they get added and removed?

Ans: The basic features of client/server architectures are:

10. Combination of a client or front-end portion that interacts with the user, and a server or back-end portion that interacts with the shared resource. The client process contains solution-specific logic and provides the interface between the user and the rest of the application system. The server process acts as a software engine that manages shared resources such as databases, printers, modems, or high-powered processors.

11. The front-end task and back-end task have fundamentally different requirements for computing resources such as processor speeds, memory, disk speeds and capacities, and input/output devices.

12. The environment is typically heterogeneous and multivendor. The hardware platform and operating system of client and server are not usually the same. Client and server processes communicate through a well-defined set of standard application program interfaces (API's) and RPC's.

13. An important characteristic of client-server systems is scalability. They can be scaled horizontally or vertically. Horizontal scaling means adding or removing client workstations with only a slight performance impact. Vertical scaling means migrating to a larger and faster server machine or multiservers.

Headers and trailers are the concepts of OSI model. Headers are information structures which identifies the information that follows, such as a block of bytes in communication.

Trailer is the information which occupies several bytes at the end of the block of the data being transmitted. They contain error-checking data which is useful for confirming the accuracy and status of the transmission.

During communication of data the sender appends the header and passes it to the lower layer while the receiver removes header and passes it to upper layer. Headers are added at layer 6,5,4,3 & 2 while Trailer is added at layer 2.

14. Why the telephone companies developed ISDN? Explain the working principle of ISDN with its interface and functional group.

Ans: ISDN or Integrated Services Digital Network is a circuit-switched telephone network system that transmits both data and voice over a digital line. We can also think of it as a set of communication standards to transmit data, voice, and signaling. These digital lines could be copper lines. It was designed to move outdated landline technology to digital.

The telephone companies developed ISDN because of the following reasons:

- It offers multiple digital services that operate through the same copper wire
- Digital signals broadcast through telephone lines.
- ISDN provides a higher data transfer rate.
- Can connect devices and allow them to operate over a single line. This includes credit card readers, fax machines, and other manifold devices.
- It is up and running faster than other modems.

The ISDN works based on the standards defined by ITU-T (formerly CCITT). The Telecommunication Standardization Sector (ITU-T) coordinates standards for telecommunications on behalf of the International Telecommunication Union (ITU) and is based in Geneva, Switzerland. The various principles of ISDN as per ITU-T recommendation are:

10. To support switched and non-switched applications o To support voice and non-voice applications
o Reliance on 64-kbps connections o Intelligence in the network
o Layered protocol architecture o Variety of configurations

The following are the interfaces of ISDN:

i) Basic Rate Interface (BRI) –

There are two data-bearing channels (‘B’ channels) and one signaling channel (‘D’ channel) in BRI to initiate connections. The B channels operate at a maximum of 64 Kbps while the D channel operates at a maximum of 16 Kbps. The two channels are

independent of each other. For example, one channel is used as a TCP/IP connection to a location while the other channel is used to send a fax to a remote location. In iSeries ISDN supports basic rate interface (BRl).

The basic rate interface (BRl) specifies a digital pipe consisting two B channels of 64 Kbps each and one D channel of 16 Kbps. This equals a speed of 144 Kbps. In addition, the BRl service itself requires an operating overhead of 48 Kbps. Therefore, a digital pipe of 192 Kbps is required.

ii) Primary Rate Interface (PRI) –

Primary Rate Interface service consists of a D channel and either 23 or 30 B channels depending on the country you are in. PRI is not supported on the iSeries. A digital pipe with 23 B channels and one 64 Kbps D channel is present in the usual Primary Rate Interface (PRI). Twenty-three B channels of 64 Kbps each and one D channel of 64 Kbps equals 1.536 Mbps. The PRI service uses 8 Kbps of overhead also. Therefore, PRI requires a digital pipe of 1.544 Mbps.

iii) Broadband-ISDN (B-ISDN) –

Narrowband ISDN has been designed to operate over the current communications infrastructure, which is heavily dependent on the copper cable however B-ISDN relies mainly on the evolution of fiber optics. According to CCITT B-ISDN is best described as ‘a service requiring transmission channels capable of supporting rates greater than the primary rate.

3. Explain the working principle of CSMA/CD with appropriate figure.

Ans: CSMA/CD stands for Carrier Sense Multiple Access/Collision Detection, with collision detection being an extension of the CSMA protocol. This creates a procedure that regulates how communication must take place in a network with a shared transmission medium. The extension also regulates how to proceed if collisions occur i.e. when two or more nodes try to send data packets via the transmission medium (bus) simultaneously and they interfere with one other.

Working principle of CSMA/CD:

Step 1: Check if the sender is ready for transmitting data packets.

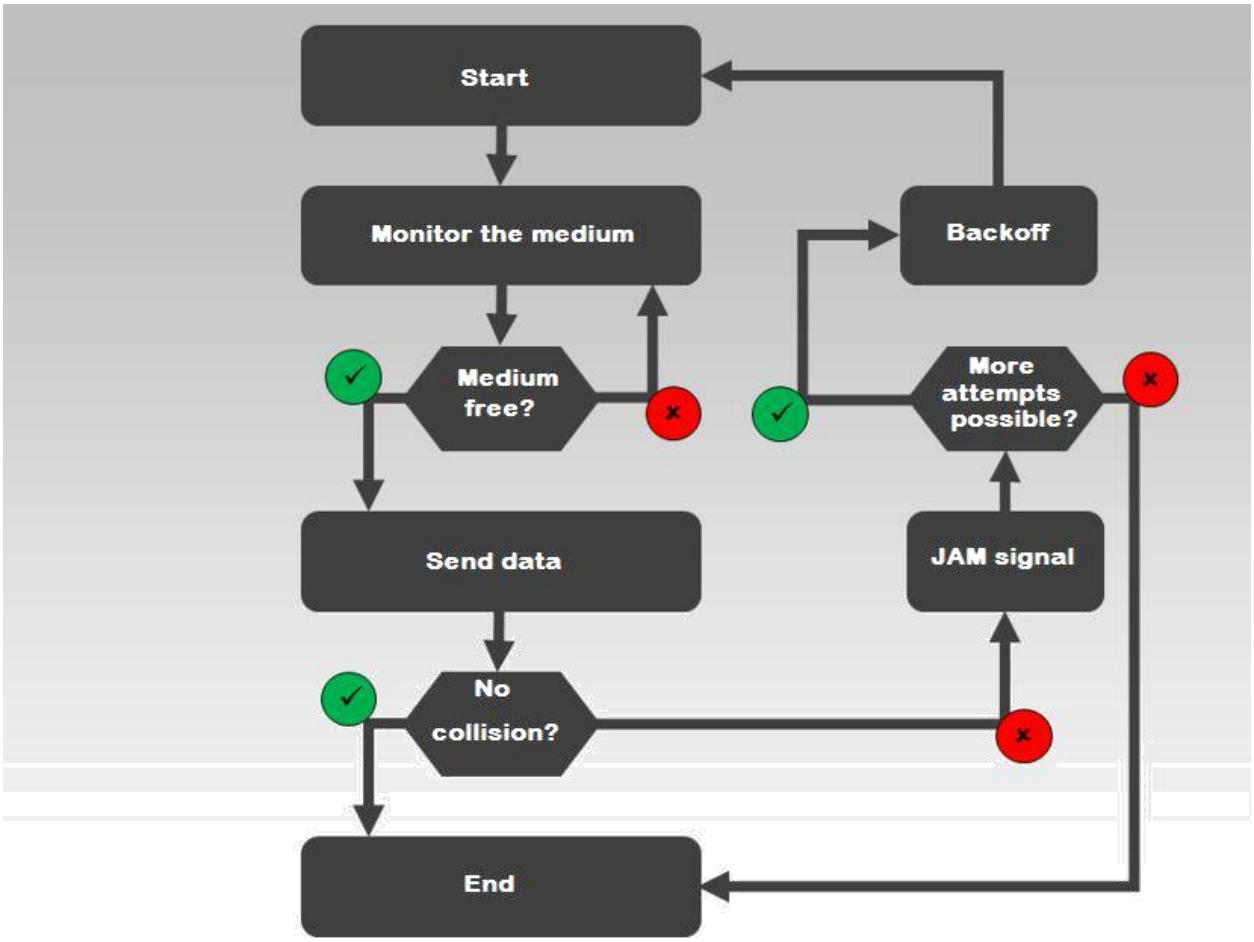
Step 2: Check if the transmission link is idle?

Sender has to keep on checking if the transmission link/medium is idle. For this it continuously senses transmissions from other nodes. Sender sends dummy data on the link. If it does not receive any collision signal, this means the link is idle at the moment. If it senses that the carrier is free and there are no collisions, it sends the data. Otherwise it refrains from sending data.

Step 3: Transmit the data & check for collisions.

Sender transmits its data on the link. CSMA/CD does not use 'acknowledgement' system. It checks for the successful and unsuccessful transmissions through collision signals. During transmission, if collision signal is received by the node, transmission is stopped. The station then transmits a jam signal onto the link and waits for random time interval before it resends the frame. After some random time, it again attempts to transfer the data and repeats above process.

Step 4: If no collision was detected in propagation, the sender completes its frame transmission and resets the counters.



Institute of Engineering has six departments having 16, 32, 61, 8, 6 and 24 computers. Use 192.168.1.0/24 to distribute the network. Find the network address, broadcast address, usable IP range and subnet mask in each department.

SOL

Dep ~~1~~ 16
Dep ~~2~~ 32
Dep 3 =
Dep 1 = 6
Dep 2 = 8
Dep 3 = 16
Dep 4 = 24
Dep 5 = 32
Dep 6 = 61

In ascending order
6, 8, 16, 24, 32, 61

Total

First usable
usable host
least subnet

	Dep 1	Dep 2	Dep 3	Dep 4
	6+2=8	8+2=10	16+2=18	24+2=26
	$\leq 2^3 \Rightarrow$ hid=3	$\leq 2^4 \Rightarrow$ hid=4	$\leq 2^5 \Rightarrow$ hid=5	$\leq 2^5 \Rightarrow$ hid=5
	nid=29	nid=28	nid=27	nid=27
	192.168.1.0/29	192.168.1.8/28	192.168.1.24/27	192.168.1.56/27
	⋮	⋮	⋮	⋮
	192.168.1.7/29	192.168.1.17/28	192.168.1.41/27	192.168.1.81/27
		192.168.1.23/28	192.168.1.55/27	192.168.1.87/27
	255.255.255.248	255.255.255.240	255.255.255.224	255.255.255.224

	Dep 5	Dep 6
	32+2=34	61+2=63
	$\leq 2^6 \Rightarrow$ hid=6	$\leq 2^6 \Rightarrow$ hid=6
	nid=26	nid=26
	192.168.1.88/26	192.168.1.152/26
	⋮	⋮
	192.168.1.121/26	192.168.1.214/26
	⋮	⋮
	192.168.1.151/26	192.168.1.215/26
	255.255.255.192	255.255.255.192

address = 192.168.1.0/2

- What is routing? Differentiate between distance vector and link state routing algorithms.

Ans: Routing is the process of selecting a path for traffic in a network or between or across multiple networks. Broadly, routing is performed in many types of networks, including circuit-switched networks, such as the public switched telephone network (PSTN), and computer networks, such as the Internet.

In packet switching networks, routing is the higher-level decision making that directs network packets from their source toward their destination through intermediate network nodes by specific packet forwarding mechanisms. Packet forwarding is the transit of network packets from one network interface to another. Intermediate nodes are typically network hardware devices such as routers, gateways, firewalls, or switches. General-purpose computers also forward packets and perform routing, although they have no specially optimized hardware for the task.

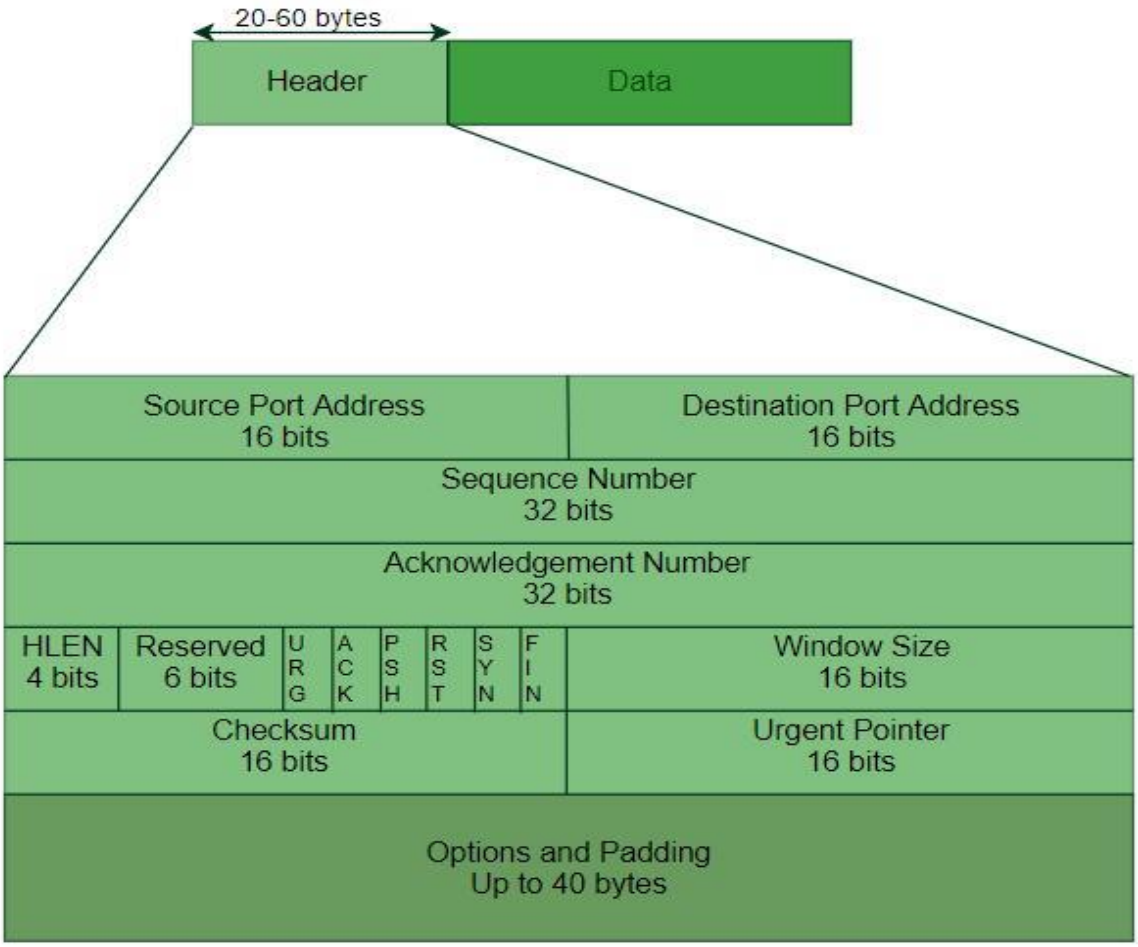
The routing process usually directs forwarding on the basis of routing tables. Routing tables maintain a record of the routes to various network destinations. Routing tables may be specified by an administrator, learned by observing network traffic or built with the assistance of routing protocols.

The difference between distance vector and link state routing algorithms are as tabulated below;

Distance Vector Routing	Link State Routing
--> Bandwidth required is less due to local sharing, small packets and no flooding.	--> Bandwidth required is more due to flooding and sending of large link state packets.
--> Based on local knowledge since it updates table based on information from neighbors.	--> Based on global knowledge i.e. it have knowledge about entire network.
--> Make use of Bellman Ford algo	--> Make use of Dijkastra's algo
--> Traffic is less	--> Traffic is more
--> Converges slowly i.e. good news spread fast and bad news spread slowly.	--> Converges faster.
--> Count to infinity problem.	--> No count to infinity problem.
--> Persistent looping problem i.e. loop will there forever.	--> No persistent loops, only transient loops.
--> Practical implementation is RIP and IGRP.	--> Practical implementation is OSPF and ISIS.

Explain the TCP segment structure. Why TCP is known as reliable protocol and also describe how reliability is provided by TCP?

Ans: TCP segment consists of data bytes to be sent and a header that is added to the data by TCP as shown:



The header of a TCP segment can range from 20-60 bytes. 40 bytes are for options. If there are no options, header is of 20 bytes else it can be of upmost 60-bytes.
Header fields:

- Source Port Address –
  16-bit field that holds the port address of the application that is sending the data segment.
- Destination Port Address –
  16-bit field that holds the port address of the application in the host that is receiving the data segment.

- Sequence Number –
  32-bit field that holds the sequence number, i.e., the byte number of the first byte that is sent in that particular segment. It is used to reassemble the message at the receiving end if the segments are received out of order.
- Acknowledgement Number –
  32-bit field that holds the acknowledgement number, i.e., the byte number that the receiver expects to receive next. It is an acknowledgment for the previous bytes being received successfully.
- Header Length (HLEN) –
  This is a 4 bit field that indicates the length of the TCP header by number of 4-byte words in the header, i.e., if the header is of 20 bytes(min length of TCP header), then this field will hold 5 (because 5 x 4 = 20) and the maximum length: 60 bytes, then it'll hold the value 15(because 15 x 4 = 60). Hence, the value of this field is always between 5 and 15.
- Control flags –
  These are 6 1-bit control bits that control connection establishment, connection termination, connection abortion, flow control, mode of transfer etc. Their function is:
  1. URG: Urgent pointer is valid
  2. ACK: Acknowledgement number is valid (used in case of cumulative acknowledgement)
  3. PSH: Request for push
  4. RST: Reset the connection
  5. SYN: Synchronize sequence numbers
  6. FIN: Terminate the connection

2. Window size –

   This field tells the window size of the sending TCP in bytes.

3. Checksum –

   This field holds the checksum for error control. It is mandatory in TCP as opposed to UDP.

4. Urgent pointer –

   This field (valid only if the URG control flag is set) is used to point to data that is urgently required that needs to reach the receiving process at the earliest. The value of this field is added to the sequence number to get the byte number of the last urgent byte.

2nd part

TCP is reliable as it uses checksum for error detection, attempts to recover lost or corrupted packets by re-transmission, acknowledgement policy and timers. It uses features like byte number and sequence number and acknowledgement number so as to ensure reliability. Also, it uses congestion control mechanisms. So, TCP is known as reliable protocol.

k) What is TFTP? Explain working principle of FTP with data transfer process including proper port connection. Use proper diagram to justify your answer.

Ans: Trivial File Transfer Protocol (TFTP) is a simple lockstep File Transfer Protocol which allows a client to get a file from or put a file onto a remote host. One of its primary uses is in the early stages of nodes booting from a local area network. TFTP has been used for this application because it is very simple to implement.

When files are transferred through FTP, one of two actions is happening – uploading or downloading. Uploading involves transferring files from a personal computer to a server. Downloading involves transferring a file from a server to a personal computer. FTP uses TCP/IP (Transmission Control Protocol/Internet Protocol) to transfer your files. TCP/IP is basically the language that the Internet uses to carry out commands. If you are going to use File Transfer Protocol in order to download files, you should keep security concerns in mind. Files downloaded from the Internet may have viruses that can harm your computer.

One way to use FTP is to go through an FTP client. FTP clients may make it safer for your computer to download/upload files and help you avoid malware and viruses. Some FTP clients are pricey, while some are completely free. Using an FTP client is not a necessary step for transferring folders, but it may make uploading and downloading files easier to do.

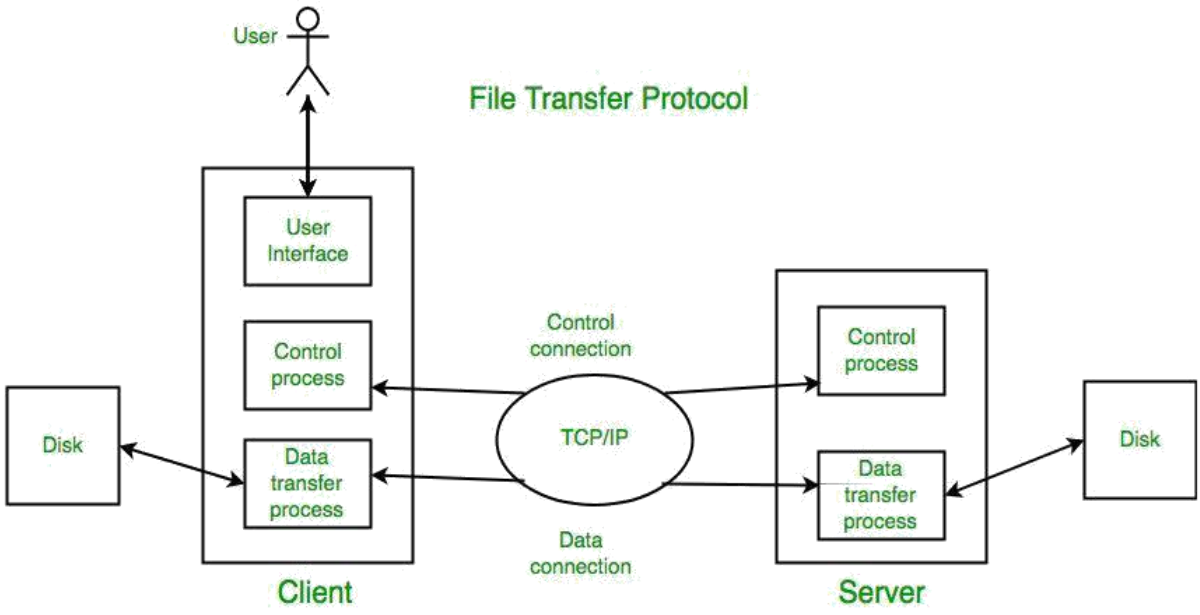


Fig: File transfer protocol in application layer

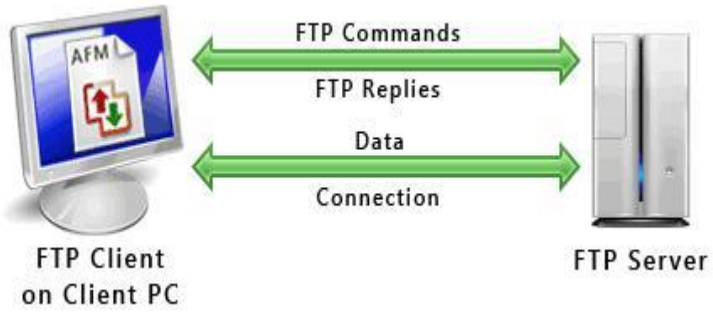


Fig: File transfer protocol

FTP uses one connection for commands and the other for sending and receiving data. FTP has a standard port number on which the FTP server "listens" for connections. A port is a "logical connection point" for communicating using the Internet Protocol (IP). The standard port number used by FTP servers is 21 and is used only for sending commands. Since port 21 is used exclusively for sending commands, this port is referred to as a command port. For example, to get a list of folders and files present on the FTP server, the FTP Client issues a "LIST" command. The FTP server then sends a list of all folders and files back to the FTP Client. So, what about the internet connection used to send and receive data? The port that is used for

transferring data is referred to as a data port. The number of the data port will vary depending on the "mode" of the connection.

Active and Passive Connection Mode-

The FTP server may support Active or Passive connections or both. In an Active FTP connection, the client opens a port and listens and the server actively connects to it. In a Passive FTP connection, the server opens a port and listens (passively) and the client connects to it. You must grant Auto FTP Manager access to the Internet and to choose the right type of FTP Connection Mode.

Most FTP client programs select passive connection mode by default because server administrators prefer it as a safety measure. Firewalls generally block connections that are "initiated" from the outside. Using passive mode, the FTP client (like Auto FTP Manager) is "reaching out" to the server to make the connection. The firewall will allow these outgoing connections, meaning that no special adjustments to firewall settings are required.

If you are connecting to the FTP server using Active mode of connection you must set your firewall to accept connections to the port that your FTP client will open. However, many Internet service providers block incoming connections to all ports above 1024. Active FTP servers generally use port 20 as their data port.

Fig: active mode

It's a good idea to use Passive mode to connect to an FTP server. Most FTP servers support the Passive mode. For Passive FTP connection to succeed, the FTP server administrator must set his / her firewall to accept all connections to any ports that

the FTP server may open. However, this is the server administrator's problem (and standard practice for servers). You can go ahead, make and use FTP connections.

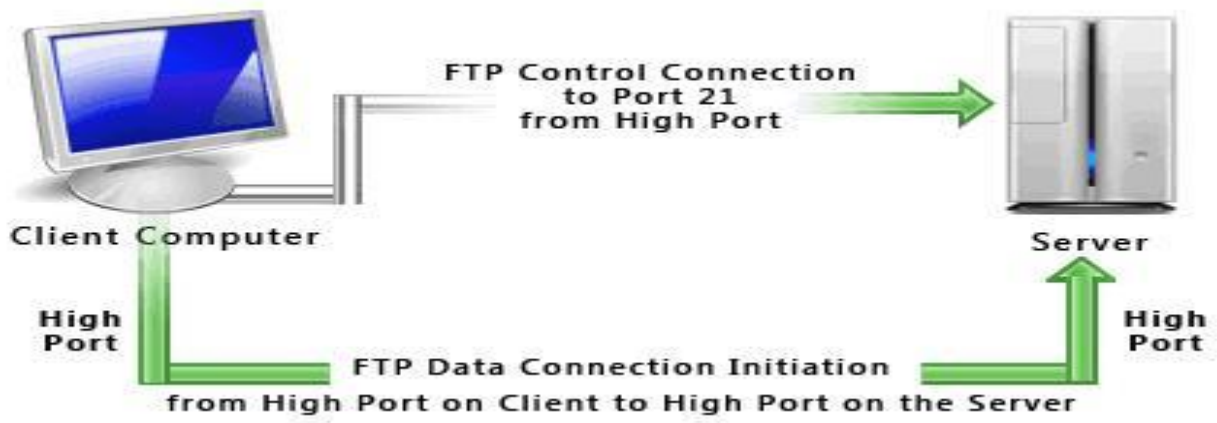


Fig: passive mode

Once the FTP Client manages to open the internet connections, one for command and one for data, it starts communicating with the FTP server. You are now ready to transfer your files and folders between the two connected computers with Auto FTP Manager.

8.List the advantages of IPv6 over IPv4.Explain any two transition strategies for IPv4 to IPv6.

e) The advantages of IPv6 over IPv4 are listed below:

1.Larger address space:An IPv6 address is 128 bits long, Compared with the 32-bit address of IPv4, this is a huge increase in the address space.

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

e) New options:IPv6 has new options to allow for additional functionalities.

f) Allowance for extension: IPv6 is designed to allow the extension of the protocol if required by new technologies or applications.

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

1. Support for more security

- Because of the huge number of systems on the Internet, the transition from IPv4 to IPv6 cannot happen suddenly. It takes a considerable amount of time before every system in the Internet can move from IPv4 to IPv6. The transition must be smooth to prevent any problems between IPv4 and IPv6 systems. The two transition strategies for IPv4 to IPv6 are as follows:

13. Dual Stack:It is recommended that all hosts, before migrating completely to version 6, have a dual stack of protocols. In other words, a station must run IPv4 and IPv6 simultaneously untilall the Internet uses IPv6.

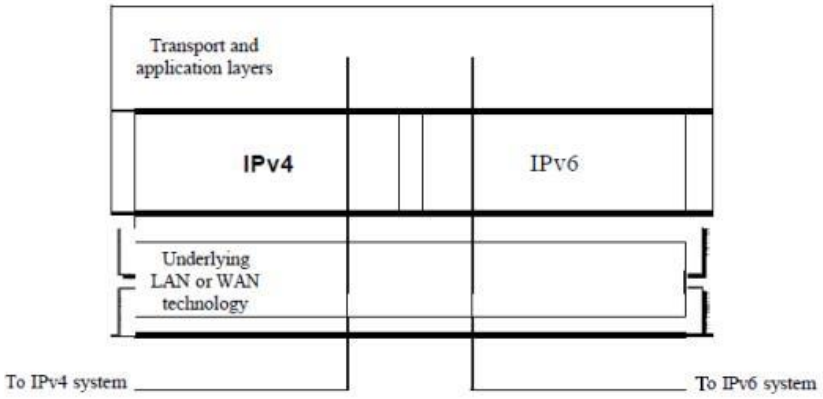


Fig:Dual Stack

To determine which version to use when sending a packet to a destination, the source host queries the DNS. If the DNS returns an IPv4 address, the source host sends an IPv4 packet. If the DNS returns an IPv6 address, the source host sends an IPv6 packet.

6. Tunneling: Tunneling is a strategy used when two computers using IPv6 want to communicate with each other and the packet must pass through a region that uses IPv4. To pass through this region, the packet must have an IPv4 address. So the IPv6 packet is encapsulated in an IPv4 packet when it enters the region, and it leaves its capsule when it exits the region. It seems as if the IPv6 packet goes through a tunnel at one end and emerges at the other end. To make it clear that the IPv4 packet is carrying an IPv6 packet as data, the protocol value is set to 41.

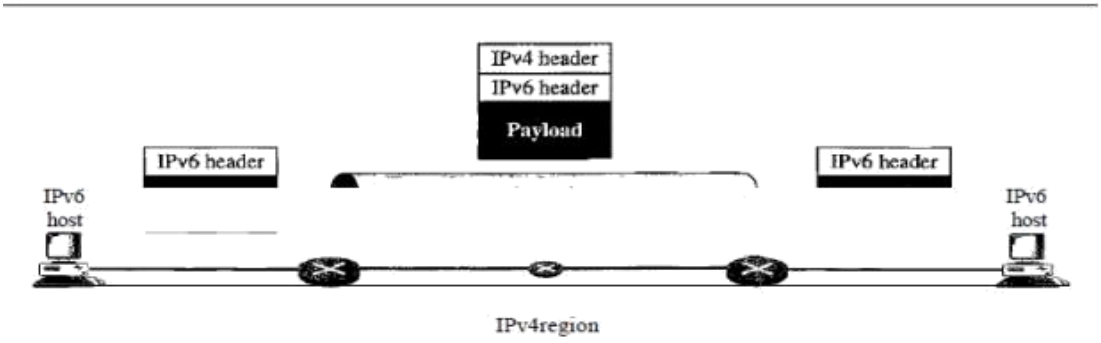


Fig: Tunneling strategy

9.List the properties of secure communication. Encrypt and decrypt “ROSE” using RSA algorithm.

- The properties of secure communication are as follows:

6. Message Confidentiality: Message confidentiality or privacy means that the sender and the receiver expect confidentiality. The transmitted message must make sense to only the intended receiver. To all others, the message must be garbage. When a customer communicates with her bank, she expects that the communication is totally confidential.

7. Message Integrity: Message integrity means that the data must arrive at the receiver exactly as they were sent. There must be no changes during the transmission, neither accidentally nor maliciously. As more and more monetary exchanges occur over the Internet, integrity is crucial. For example, it would be disastrous if a request for transferring $100 changed to a request for $10,000 or $100,000. The integrity of the message must be preserved in a secure communication.

8. Message Authentication: Message authentication is a service beyond message integrity. In message authentication the receiver needs to be sure of the sender's identity and that an imposter has not sent the message.

Message Nonrepudiation: Message nonrepudiation means that a sender must not be able to deny sending a message that he or she, in fact, did send. The burden of proof falls on the receiver. For example, when a customer sends a message to transfer money from one account to another, the bank must have proof that the customer actually requested this transaction.

A) Entity Authentication: In entity authentication (or user identification) the entity or user is verified prior to Access to the system resources (files, for example). For example, a student who needs to access her university resources needs to be authenticated during the logging process. This is to protect the interests of the university and the student.

12. The Encryption and decryption of "ROSE'using RSA algorithm is shown below:

Step1: Let us consider two prime numbers p and q i.e. p=3 and q=11.

Step2: Let n=p*q=3*11=33.

Step3:Let m=(p-1) (q-1)=(3-1)*(11-1)=20,where m is co-prime.

Step4:Choose a small number e (1<e<m),co-prime to m such that greatest common divider GCD(e,m)=1.

So, the best value of e will be 3.

Therefore,e=3.

Step5:Here,we have to find d.So, (d*e mod(m))=1 and d=(1+m*i)/e.where,i=1,2,3,4……..

So, For i=1,

d=7.

Step6:Hence,Public key(n,e)=(33,3) and Private key(n,d)=(33,7).

Encryption and Decryption is as shown in the table below.

Letters	P	P^e	$C=P^e \bmod (n)$ [Encryption]	C^d	$P=C^d \bmod (n)$ [Decryption]	Letters
R	18	5832	24	4586471424	18	R
O	15	3375	9	4782969	15	O
S	19	6859	28	13492928512	19	S
E	5	125	26	8031810176	5	E

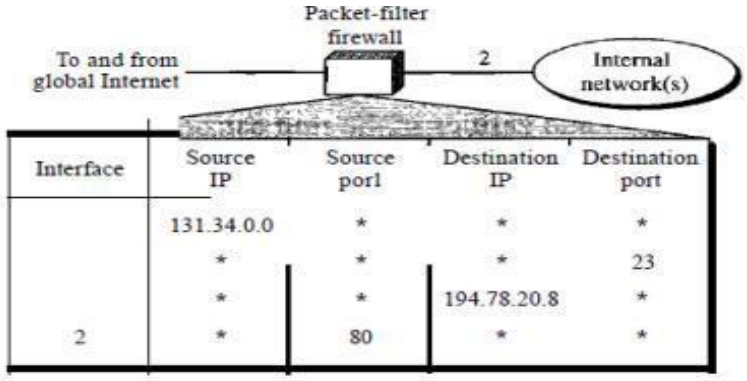
10.Write short notes on:

a) Firewall and their types

→All previous security measures cannot prevent Eve from sending a harmful message to a system. To control access to a system, we need firewalls. A firewall is a device (usually a router or a computer) installed between the internal network of an organization and the rest of the Internet. It is designed to forward some packets and filter (not forward) others.A Firewall is usually classified as a packet-filter firewall or a proxy-based firewall.

Packet_Filter Firewall

A firewall can be used as a packet filter. It can forward or block packets based on the information in the network layer and transport layer headers: source and destination IP addresses, source and destination port addresses, and type of protocol (TCP or UDP). A packet-filter firewall is a router that uses a filtering table to decide which packets must be discarded (not forwarded). Figure shows an example of a filtering table for this kind of a firewall.



Interface	Source IP	Source port	Destination IP	Destination port
	131.34.0.0	*	*	*
	*	*	*	23
	*	*	194.78.20.8	*
2	*	80	*	*

According to Figure , the following packets are filtered:

1. Incoming packets from network 131.34.0.0 are blocked (security precaution). Note that the * (asterisk) means "any."

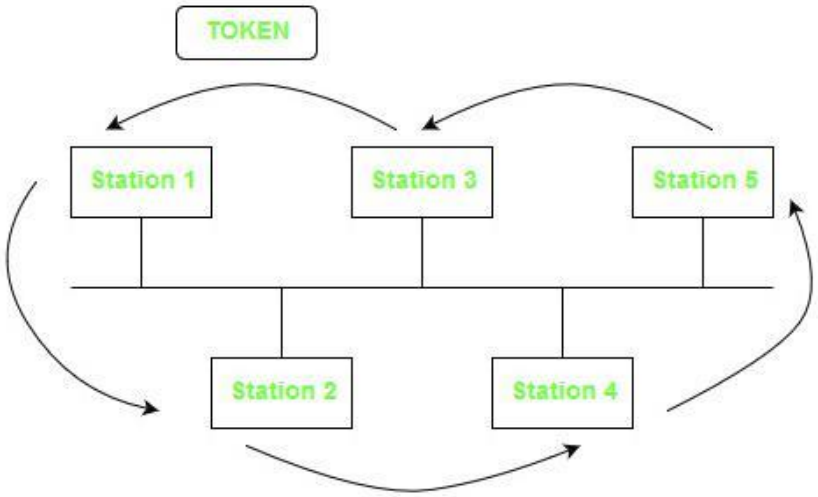
- Incoming packets destined for any internal TELNET server (port 23) are blocked.

Incoming packets destined for internal host 194.78.20.8 are blocked. The organization wants this host for internal use only.

E) Outgoing packets destined for an Http server (port 80) are blocked. The organization does not want employees to browse the Internet.

b)803 Token Bus

→Token Bus is a popular standard for the token passing LANs. In a token bus LAN, the physical media is a bus or a tree and a logical ring is created using coaxial cable. The token is passed from one user to other in a sequence (clockwise or anticlockwise). Each station knows the address of the station to its "left" and "right" as per the sequence in the logical ring. A station can only transmit data when it has the token. The working of token bus is somewhat similar to token ring.



c)Virtual circuit switching

→Virtual circuit (VC) is a means of transporting data over a switched computer in such a way that it appears as though there is a dedicated layer link between the source and destination end systems of this data. The term virtual circuit is synonymous with virtual connection and virtual channel. Before a connection or virtual circuit may be used, it has to be established, between two or more nodes or software applications, by configuring the relevant parts of the interconnecting network. After that, a bit stream or byte stream may be delivered between the nodes; hence, a virtual circuit protocol allows higher level protocols to avoid dealing with the division of data into segments, packets, or frames. Virtual circuit communication resembles circuit switching, since both are connection oriented, meaning that in both cases data is delivered in correct order, and signaling overhead is required during a connection
establishment phase. However, circuit switching provides a constant bit rate and latency, while these may vary in a virtual circuit service due to factors such as: • varying packet queue lengths in the network nodes, • varying bit rate generated by the application, • varying load from other users sharing the same network resources by means of statistical multiplexing, etc. Many virtual circuit protocols, but not all, provide reliable communication service through the use of data retransmissions because of error detection and automatic repeat request (ARQ).

2067 ASHAD

1. Why network software should be in hierarchical form? Explain in detail about OSI layers.

Network software should be in hierarchical form as it simplifies the design process as the functions of each layers and their interactions are well defined. The layered architecture provides flexibility to modify and develop network services. The number of layers, name of layers and the tasks assigned to them may change from network to network. But for all the networks, always the lower layer offers certain services to its upper layer. The concept of layered architecture redefines the way of convincing networks. This leads to a considerable cost savings and managerial benefits. Addition of new services and management of network infrastructure become easy.

OSI stands for Open Systems Interconnection. It has been developed by ISO – 'International Organization of Standardization', in the year 1984. It is a 7 layer architecture with each layer having specific functionality to perform. All these 7 layers work collaboratively to transmit the data from one person to another across the globe.

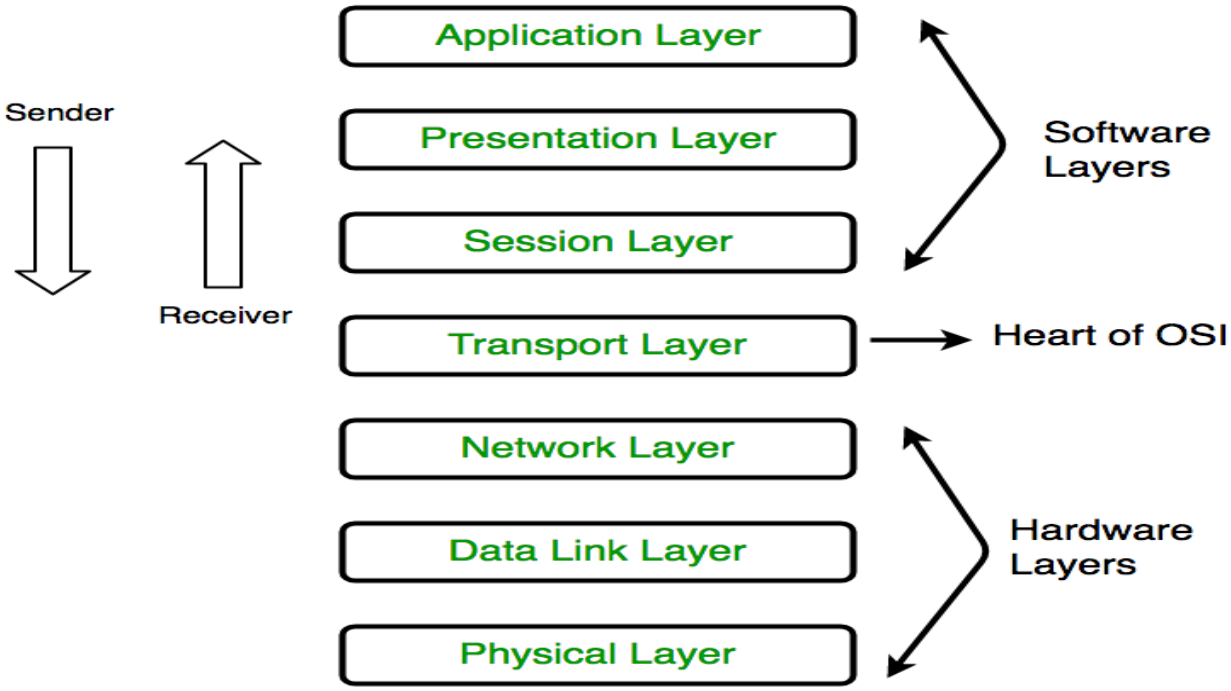


Figure: - OSI Layer

(Explain each layer briefly from below, no need to write all)

1. Physical Layer (Layer 1):

The lowest layer of the OSI reference model is the physical layer. It is responsible for the actual physical connection between the devices. The physical layer contains information in the form of bits. It is responsible for the actual physical connection between the devices. When receiving

data, this layer will get the signal received and convert it into 0s and 1s and send them to the Data Link layer, which will put the frame back together.
Hub, Repeater, Modem, Cables are Physical Layer devices.
The functions of the physical layer are :

1. Bit synchronization: The physical layer provides the synchronization of the bits by providing a clock. This clock controls both sender and receiver thus providing synchronization at bit level.
2. Bit rate control: The Physical layer also defines the transmission rate i.e. the number of bits sent per second.
3. Physical topologies: Physical layer specifies the way in which the different, devices/nodes are arranged in a network i.e. bus, star or mesh topolgy.
4. Transmission mode: Physical layer also defines the way in which the data flows between the two connected devices. The various transmission modes possible are: Simplex, half-duplex and full-duplex.

2. Data Link Layer (DLL) (Layer 2):

The data link layer is responsible for the node to node delivery of the message. The main function of this layer is to make sure data transfer is error free from one node to another, over the physical layer. When a packet arrives in a network, it is the responsibility of DLL to transmit it to the Host using its MAC address.
Data Link Layer is divided into two sub layers:

1. Logical Link Control (LLC)
2. Media Access Control (MAC)

Packet in Data Link layer is referred as Frame. The packet received from Network layer is further divided into frames depending on the frame size of NIC(Network Interface Card). DLL also encapsulates Sender and Receiver's MAC address in the header.

The Receiver's MAC address is obtained by placing an ARP(Address Resolution Protocol) request onto the wire asking "Who has that IP address?" and the destination host will reply with its MAC address.

The functions of the data Link layer are :

1. Framing: Framing is a function of the data link layer. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver. This can be accomplished by attaching special bit patterns to the beginning and end of the frame.
2. Physical addressing: After creating frames, Data link layer adds physical addresses (MAC address) of sender and/or receiver in the header of each frame.
3. Error control: Data link layer provides the mechanism of error control in which it detects and retransmits damaged or lost frames.
4. Flow Control: The data rate must be constant on both sides else the data may get corrupted thus , flow control coordinates that amount of data that can be sent before receiving acknowledgement.

5. Access control: When a single communication channel is shared by multiple devices, MAC sub-layer of data link layer helps to determine which device has control over the channel at a given time.

3. Network Layer (Layer 3) :

Network layer works for the transmission of data from one host to the other located in different networks. It also takes care of packet routing i.e. selection of the shortest path to transmit the packet, from the number of routes available. The sender & receiver's IP address are placed in the header by network layer. Segment in Network layer is referred as Packet. Network layer is implemented by networking devices such as routers.

The functions of the Network layer are :

1. Routing: The network layer protocols determine which route is suitable from source to destination. This function of network layer is known as routing.
2. Logical Addressing: In order to identify each device on internetwork uniquely, network layer defines an addressing scheme. The sender & receiver's IP address are placed in the header by network layer. Such an address distinguishes each device uniquely and universally.

4. Transport Layer (Layer 4) :

Transport layer provides services to application layer and takes services from network layer. The data in the transport layer is referred to as *Segments*. It is responsible for the End to End delivery of the complete message. Transport layer also provides the acknowledgment of the successful data transmission and re-transmits the data if an error is found.

Transport Layer is called as Heart of OSI model.

The functions of the transport layer are:

1. Segmentation and Reassembly: This layer accepts the message from the (session) layer , breaks the message into smaller units . Each of the segment produced has a header associated with it. The transport layer at the destination station reassembles the message.
2. Service Point Addressing: In order to deliver the message to correct process, transport layer header includes a type of address called service point address or port address. Thus by specifying this address, transport layer makes sure that the message is delivered to the correct process.

The services provided by transport layer :

1. Connection Oriented Service: It is a three-phase process which include
   – Connection Establishment
   – Data Transfer
   – Termination / disconnection
   In this type of transmission, the receiving device sends an acknowledgment, back to the source after a packet or group of packet is received. This type of transmission is reliable and secure.

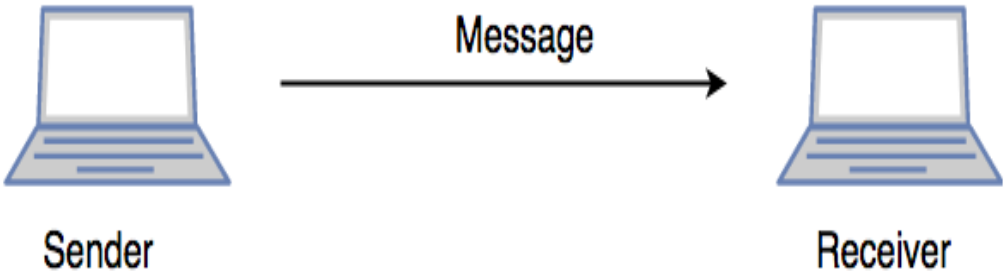
2. Connection less service: It is a one phase process and includes Data Transfer. In this type of transmission, the receiver does not acknowledge receipt of a packet. This approach allows for much faster communication between devices. Connection oriented Service is more reliable than connection less Service.

5. Session Layer (Layer 5) :

This layer is responsible for establishment of connection, maintenance of sessions, authentication and also ensures security.
The functions of the session layer are :

1. Session establishment, maintenance and termination: The layer allows the two processes to establish, use and terminate a connection.
2. Synchronization : This layer allows a process to add checkpoints which are considered as synchronization points into the data. These synchronization point help to identify the error so that the data is re-synchronized properly, and ends of the messages are not cut prematurely and data loss is avoided.
3. Dialog Controller : The session layer allows two systems to start communication with each other in half-duplex or full-duplex.

SCENARIO:
Let's consider a scenario where a user wants to send a message through some Messenger application running in his browser. The "Messenger" here acts as the application layer which provides the user with an interface to create the data. This message or so-called Data is compressed, encrypted (if any secure data) and converted into bits (0's and 1's) so that it can be transmitted.



6. Presentation Layer (Layer 6) :

Presentation layer is also called the Translation layer.The data from the application layer is extracted here and manipulated as per the required format to transmit over the network.
The functions of the presentation layer are :

1. Translation : For example, ASCII to EBCDIC.
2. Encryption/ Decryption : Data encryption translates the data into another form or code. The encrypted data is known as the cipher text and the decrypted data is known as plain text. A key value is used for encrypting as well as decrypting data.
3. Compression: Reduces the number of bits that need to be transmitted on the network.

7. Application Layer (Layer 7) :

At the very top of the OSI Reference Model stack of layers, we find Application layer which is implemented by the network applications. These applications produce the data, which has to be transferred over the network. This layer also serves as a window for the application services to access the network and for displaying the received information to the user.
Ex: Application – Browsers, Skype Messenger etc.

The functions of the Application layer are :

1. Network Virtual Terminal
2. FTAM-File transfer access and management
3. Mail Services
4. Directory Services

OSI model acts as a reference model and is not implemented in Internet because of its late invention. Current model being used is the TCP/IP model.

3. What do you mean by ISDN and what is it contribution in the field of data communication? Explain various types of multiplexing mechanism used in communication.

Integrated Services Digital Network (ISDN) is a set of communication standards for simultaneous digital transmission of voice, video, data, and other network services over the traditional circuits of the public switched telephone network. Prior to ISDN, the telephone system was viewed as a way to transport voice, with some special services available for data. The key feature of ISDN is that it integrates speech and data on the same lines, adding features that were not available in the classic telephone system. The ISDN standards define several kinds of access interfaces, such as Basic Rate Interface (BRI), Primary Rate Interface (PRI), Narrowband ISDN (N-ISDN), and Broadband ISDN (B-ISDN).
ISDN is a circuit-switched telephone network system, but it also provides access to packet switched networks that allows digital transmission of voice and data. This results in potentially better voice or data quality than an analog phone can provide. It provides a packet-switched connection for data in increments of 64 kilobit/s. It provided a maximum of 128 kbit/s bandwidth in both upstream and downstream directions. A greater data rate was achieved through channel bonding. Generally ISDN B-channels of three or four BRIs (six to eight 64 kbit/s channels) are bonded.

The contribution of ISDN in the field of data communication is that ISDN provides a fully

integrated digital service to users. These services fall into 3 categories- bearer services, teleservices and supplementary services.

1. Bearer Service
   Transfer of information (voice, data and video) between users without the network manipulating the content of that information is provided by the bearer network. There is no need for the network to process the information and therefore does not change the content. Bearer services belong to the first three layers of the OSI model. They are well defined in the ISDN standard. They can be provided using circuit-switched, packet-switched, frame-switched, or cell-switched networks.
2. Teleservices Service
   In this the network may change or process the contents of the data. These services corresponds to layers 4-7 of the OSI model. Teleservices relay on the facilities of the bearer services and are designed to accommodate complex user needs. The user need not to be aware of the details of the process. Teleservices include telephony, teletex, telefax, videotex, telex and teleconferencing. Though the ISDN defines these services by name yet they have not yet become standards.
3. Supplementary Service
   Additional functionality to the bearer services and teleservices are provided by supplementary services. Reverse charging, call waiting, and message handling are examples of supplementary services which are all familiar with today's telephone company services.

Multiplexing is a technique by which different analog and digital streams of transmission can be simultaneously processed over a shared link. Multiplexing divides the high capacity medium into low capacity logical medium which is then shared by different streams. When multiple senders try to send over a single medium, a device called Multiplexer divides the physical channel and allocates one to each. On the other end of communication, a De-multiplexer receives data from a single medium, identifies each, and sends to different receivers.

Multiplexing techniques are mainly used in communication, and these are classified into three types. The 3 types of multiplexing techniques include the following.

- Frequency Division Multiplexing (FDM)
- Wavelength Division Multiplexing (WDM)
- Time Division Multiplexing (TDM)

1). Frequency Division Multiplexing (FDM)

The FDM is used in telephone companies in the 20th century in long-distance connections for multiplexing number of voice signals using a system like a coaxial cable. For small distances, low-cost cables were utilized for different systems such as bell systems, K-and N-carrier, however, they don't let huge bandwidths. This is analog multiplexing used to unite analog signals. This type of multiplexing is useful when the link's bandwidth is better than the United bandwidth of the transmitted signals.

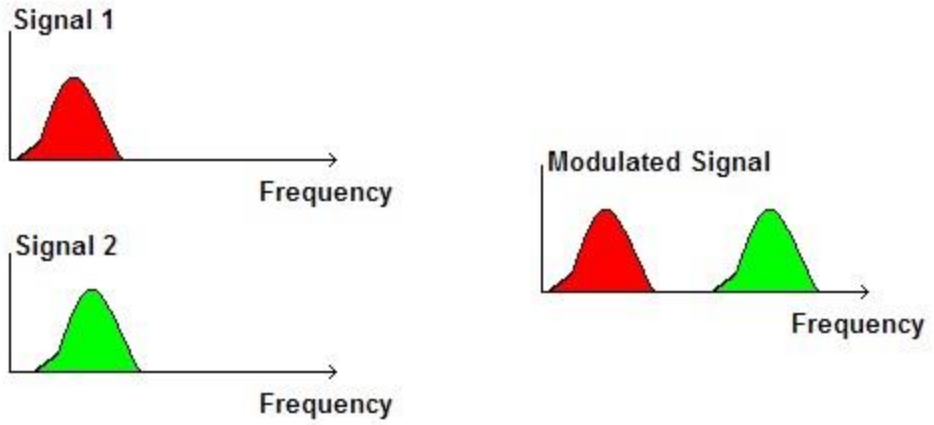


Figure: -Frequency Division Multiplexing

In FDM, signals are produced by transmitting various device modulated carrier frequencies, and then these are united into a solo signal which can be moved by the connection. To hold the adapted signal, the carrier frequencies are divided by sufficient bandwidth, & these ranges of bandwidths are the channels through the different traveling signals. These can be divided by bandwidth which is not used. The best examples of the FDM comprise signal transmission in TV and radio.

2). Wavelength Division Multiplexing (WDM)

In fiber communications, the WDM (Wavelength Division Multiplexing) is one type of technology. This is the most useful concept in high-capacity communication systems. At the end of the transmitter section, the multiplexer is used to combine the signals as well as at the end of receiver section, de-multiplexer for dividing the signals separately. The main function of WDM at the multiplexer is for uniting various light sources into an only light source, and this light can be changed into numerous light sources at the de-multiplexer.

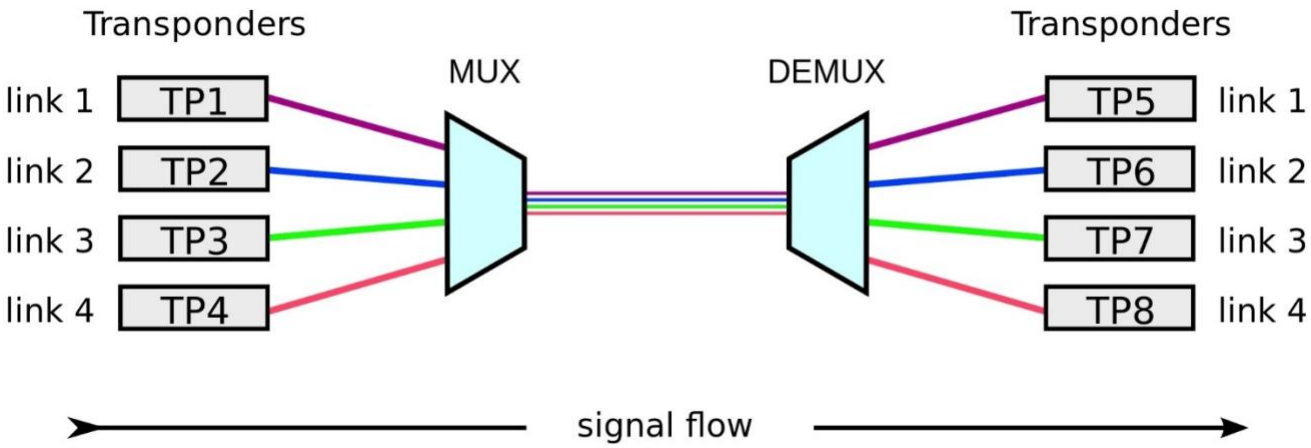


Figure: -Wavelength Division Multiplexing

The main intention of WDM is to utilize the high data rate capacity of the FOC (fiber optic cable). The high data rate of this FOC cable is superior to the data rate of the metallic transmission cable. Theoretically, the WDM is similar to the FDM, apart from the data transmission through the FOC in which the multiplexing & de-multiplexing occupies optical signals. Please refer the link to know more about Wavelength Division Multiplexing (WDM) Working and Applications

3). Time Division Multiplexing (TDM)

The Time division multiplexing (or) TDM is one kind of method for transmitting a signal over a channel of particular communication with separating the time edge into slots. Like single slot is used for each message signal.

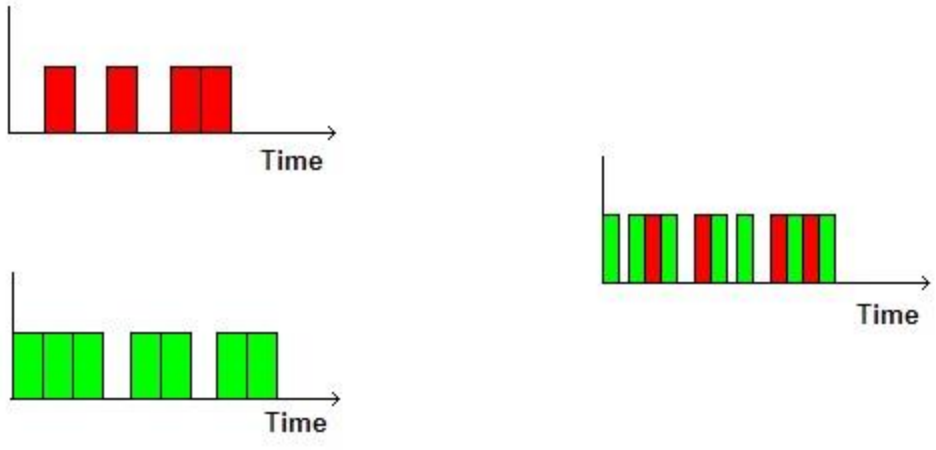


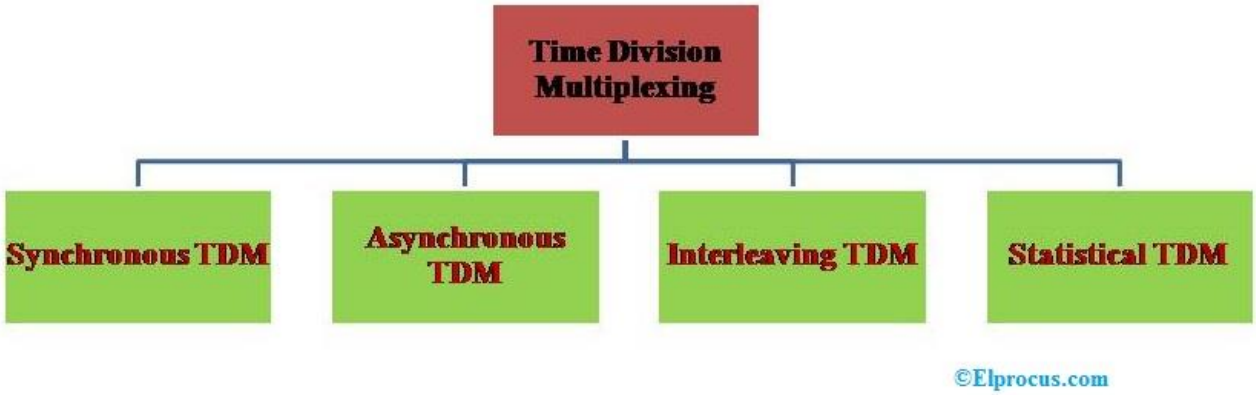
Figure: -Time Division Multiplexing

TDM is mainly useful for analog and digital signals, in which several channels with low speed are multiplexed into high-speed channels used for transmission. Depending on the time, every low-speed channel will be assigned to an exact position, wherever it works in the mode of synchronized. Both the ends of MUX and DEMUX are synchronized timely & at the same time switch toward the next channel.

Types of Time Division Multiplexing

The different types of TDM include the following.

- Synchronous TDM
- Asynchronous TDM
- Interleaving TDM
- Statistical TDM



Types of TDM

1). Synchronous TDM

The synchronous TDM is very useful in both analog as well as digital signals. In this type of TDM, the connection of input is allied to a frame. For example, if there are n-connections in the frame, then a frame will be separated into n-time slots, and for every unit, each slot is assigned to every input line.

In the sampling of synchronous TDM, the speed is similar for every signal, as well as this sampling needs a clock (CLK) signal at both the ends of sender & receiver. In this type of TDM, the multiplexer assigns the similar slot for each device at every time.

2). Asynchronous TDM

In asynchronous TDM, for different signals, the rate of sampling is also different, and it doesn't need a general clock (CLK). If the device has nothing for transmitting, then the time slot is assigned to a new device. The design of a commutator otherwise de-commutator is not easy & the bandwidth is low for this type of multiplexing, and it is applicable for not synchronous transmit form network.

3). Interleaving TDM

The TDM can be imagined like two speedy rotary switches on the multiplexing & demultiplexing surface. These switches can be rotated & synchronized in reverse directions. Once the switch releases at the surface of multiplexer ahead of a connection, then it has a chance of sending a unit into the lane. Similarly, once the switch releases at the surface of de-multiplexer ahead of a connection a chance to receiving a unit from the lane. This procedure is named as interleaving.

4). Statistical TDM

The statistical TDM is applicable to transmit different types of data simultaneously across a single cable. This is frequently used to handle data being transmitted through the network like LAN (or) WAN. The transmission of data can be done from the input devices which are connected to networks like computers, fax machines, printers, etc. The statistical TDM can be used in the settings of telephone switchboards to control the calls. This type of multiplexing is comparable to dynamic bandwidth distribution, and a communication channel is separated into a random data stream number.

4). Code Division Multiplexing (CDM)

Code division multiplexing (CDM) is a multiplexing technique that uses spread spectrum communication. In spread spectrum communications, a narrowband signal is spread over a larger band of frequency or across multiple channels via division. It does not constrict bandwidth's digital signals or frequencies. It is less susceptible to interference, thus providing better data communication capability and a more secure private line.

4. Describe what do you understand by switching along with various type of switching mechanism. Explain the fault tolerance mechanism of FDDI.

Switching is process to forward packets coming in from one port to a port leading towards the destination. When data comes on a port it is called ingress, and when data leaves a port or goes out it is called egress.

There are three types of switching methods: -

1) Circuit Switching
2) Packet Switching
3) Message Switching

1). Circuit Switching

- Circuit switching is a switching technique that establishes a dedicated path between sender and receiver.
- In the Circuit Switching Technique, once the connection is established then the dedicated path will remain to exist until the connection is terminated.
- Circuit switching in a network operates in a similar way as the telephone works.
- A complete end-to-end path must exist before the communication takes place.
- In case of circuit switching technique, when any user wants to send the data, voice, video, a request signal is sent to the receiver then the receiver sends back the acknowledgment to ensure the availability of the dedicated path. After receiving the acknowledgment, dedicated path transfers the data.
- Circuit switching is used in public telephone network. It is used for voice transmission.
- Fixed data can be transferred at a time in circuit switching technology.

Communication through circuit switching has 3 phases:

- Circuit establishment
- Data transfer
- Circuit Disconnect

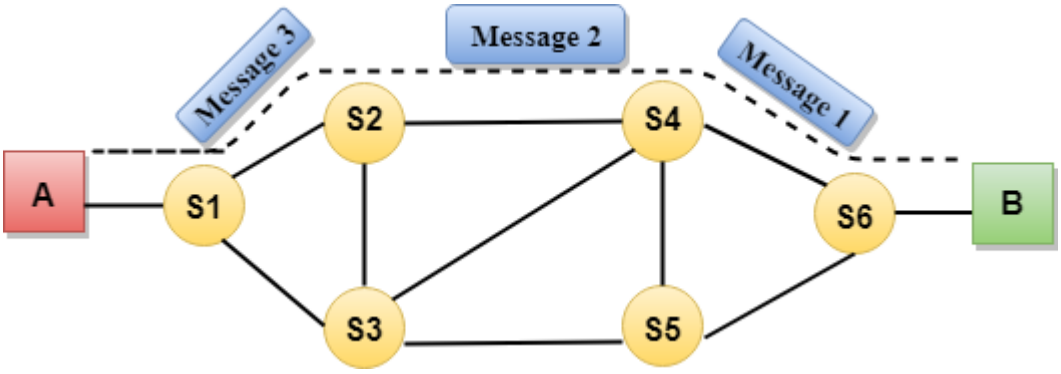


Figure: - Circuit Switching

2). Packet Switching

- The packet switching is a switching technique in which the message is sent in one go, but it is divided into smaller pieces, and they are sent individually.
- The message splits into smaller pieces known as packets and packets are given a unique number to identify their order at the receiving end.
- Every packet contains some information in its headers such as source address, destination address and sequence number.
- Packets will travel across the network, taking the shortest path as possible.
- All the packets are reassembled at the receiving end in correct order.
- If any packet is missing or corrupted, then the message will be sent to resend the message.
- If the correct order of the packets is reached, then the acknowledgment message will be sent.

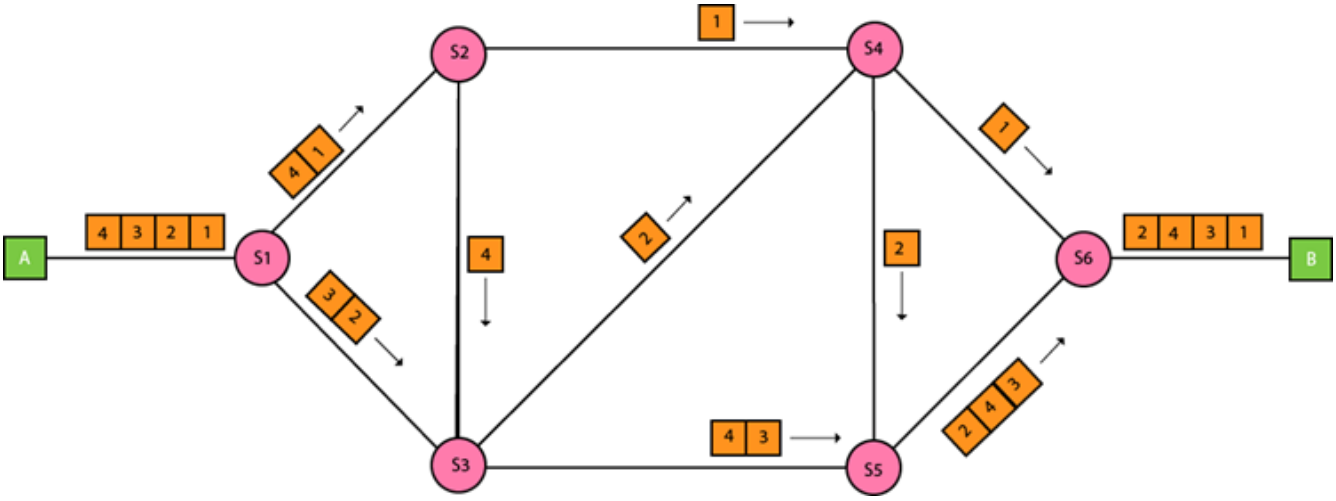


Figure: - Packet Switching

There are two of Packet Switching:

Datagram Packet switching:

- It is a packet switching technology in which packet is known as a datagram, is considered as an independent entity. Each packet contains the information about the destination and switch uses this information to forward the packet to the correct destination.
- The packets are reassembled at the receiving end in correct order.
- In Datagram Packet Switching technique, the path is not fixed.
- Intermediate nodes take the routing decisions to forward the packets.
- Datagram Packet Switching is also known as connectionless switching.

Virtual Circuit Switching

- Virtual Circuit Switching is also known as connection-oriented switching.
- In the case of Virtual circuit switching, a preplanned route is established before the messages are sent.
- Call request and call accept packets are used to establish the connection between sender and receiver.
- In this case, the path is fixed for the duration of a logical connection.

3). Message Switching

- Message Switching is a switching technique in which a message is transferred as a complete unit and routed through intermediate nodes at which it is stored and forwarded.
- In Message Switching technique, there is no establishment of a dedicated path between the sender and receiver.
- The destination address is appended to the message. Message Switching provides a dynamic routing as the message is routed through the intermediate nodes based on the information available in the message.
- Message switches are programmed in such a way so that they can provide the most efficient routes.
- Each and every node stores the entire message and then forward it to the next node. This type of network is known as store and forward network.
- Message switching treats each message as an independent entity.

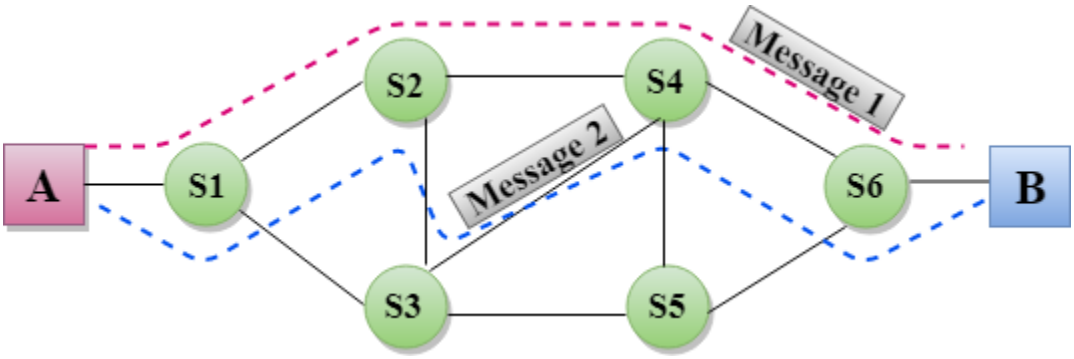


Figure: - Message Switching

5. Why access control of channel is essential? Compare operating details of IEEE 802.4 and IEEE 802.5.

Access control is to minimize the risk of unauthorized access to physical and logical systems. Access control is a fundamental component of security compliance programs that ensures security technology and access control policies are in place to protect confidential information,

such as customer data. In a channel the data and information of different user are send and received some of the information passed might be confidential and can no be provided to everyone so access control of channel is essential such that the user appointed can only access the channel for the information. This helps in the privacy of the channel and provides security to the channel.

S.N.	IEEE 802.4	IEEE 802.5.
1.	Topology used in IEEE 802.4 is Bus or Tree Topology.	Topology used in IEEE 802.5 is Ring Topology.
2.	Size of the frame format in IEEE 802.4 standard is 8202 bytes.	Frame format in IEEE 802.5 standard is of the variable size.
3.	It supports priorities to stations.	In IEEE 802.5 priorities are possible
4.	Size of the data field is 0 to 8182 bytes.	No limit is of the size of the data field.
5.	It can handle short minimum frames.	It supports both short and large frames.
6.	Throughput & efficiency at very high loads are outstanding.	Throughput & efficiency at very high loads are outstanding.
7.	Modems are required in this standard.	Like IEEE 802.4, modems are also required in it.
8	Protocol is extremely complex.	Protocol is moderately complex.
9.	It is applicable to Real time traffic.	It can be applied for Real time applications and interactive applications because there is no limitation on the size of data.

6. Explain along with the packet form about the virtual circuit connection of X.25.

• X.25 is a standard used by many older public networks specially outside the U.S.
• This was developed in 1970s by CCITT for providing an interface between public packet-switched network and their customers.
• The packet switching networks use X.25 protocol. The X.25 recommendations were first prepared in1976 and then revised in1978,1980 and 1984.

• X.25 was developed for computer connections, used for terminal/timesharing connection.
• This protocol is based on the protocols used in early packet switching networks such as ARPANET, DATAPAC, and TRANSPAC etc.

• X.25 Packet Switched networks allows remote devices to communicate with each other across high speed digital links without the expense of individual leased lines.
• A protocol X.21 which is a physical layer protocol is used to specify the physical electrical and procedural interface between the host and network.
• The problem with this standard is that it needs digital signal rather than analog signals on telephone lines.
• So not many networks support this standard. Instead RS 232 standard is defined.
• The data link layer standard has a number of variations. It is designed for error detection and

corrections.

• The network layer protocol performs the addressing, flow control, delivery confirmation etc.

• It allows the user to establish virtual circuits and send packets on them. These packets are delivered to the destination reliably and in order.

• X.25 is a connection oriented service. It supports switched virtual circuits as well as the permanent circuits.

• Packet Switching is a technique whereby the network routes individual packets of HDLC data between different destinations based on addressing within each packet.

• A switched virtual circuit is established between a computer and network when the computer sends a packet to the network requesting to make a call to other computer.

• Packets can then be sent over this connection from sender to receiver.

• X.25 provides the flow control, to avoid a fast sender overriding a slow or busy receiver.

• A permanent virtual circuit is analogous to-a leased line. It is set up in advance with a mutual agreement between the users.

• Since it is always present, no call set up is required for its use.

• In order to allow the computers which do not use the X.25 to communicate with the X.25 network a packet assembler disassembler (PAD) is used.

• PAD is required to be installed along with each computer which does not use X.25.

• X.25 defines the interface for exchange of packets between a DTE and switch data subnetwork node.

Three Layers of X.25:

The X.25 interface is defined at three levels:

The three levels are:

(i) Physical layer (level 1)

(ii) Data link layer (level 2)

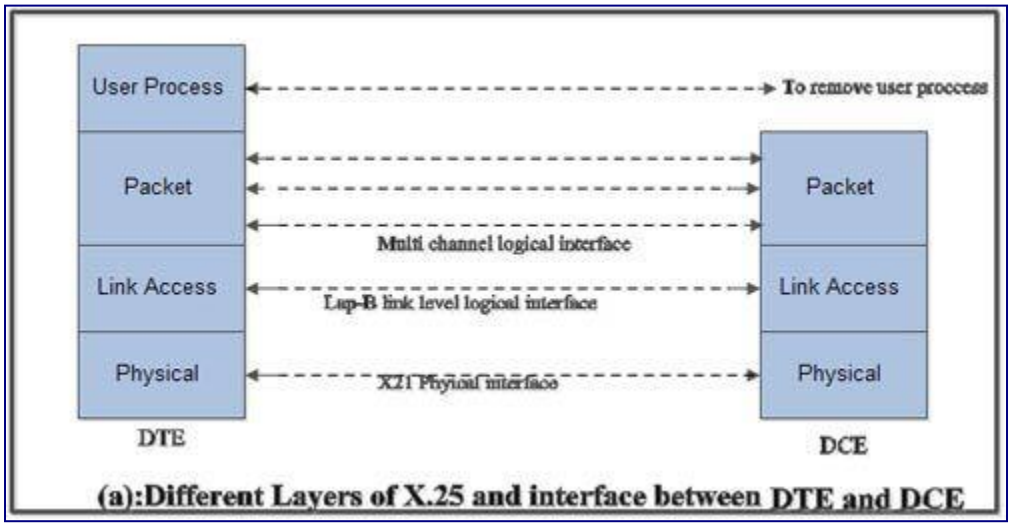
(iii) Packet layer (level 3).

• These three layers correspond to the three lower most layers of the ISO-OSI reference model. The physical layer takes care of the interface between a computer terminal and the link which attaches it to the packet switching node.

• The X.25 defines the interface for exchange of packets between the user's machine (DTE) and the packet switching node to which this DTE is attached which is called as DCE.

• The three layers of X.25 interface are as shown in Fig.(a).

• At the physical level X.21 physical interface is being used which is defined for circuit switched data network. At the data link level, X.25 specifies the link access procedure-B (LAP-B) protocol which is a subset of HDLC protocol.



(a):Different Layers of X.25 and interface between DTE and DCE

• At the network level (3rd level), X.25 defines a protocol for an access to packet data subnetwork.

• This protocol defines the format, content and procedures for exchange of control and data transfer packets. The packet layer provides an external virtual circuit service.

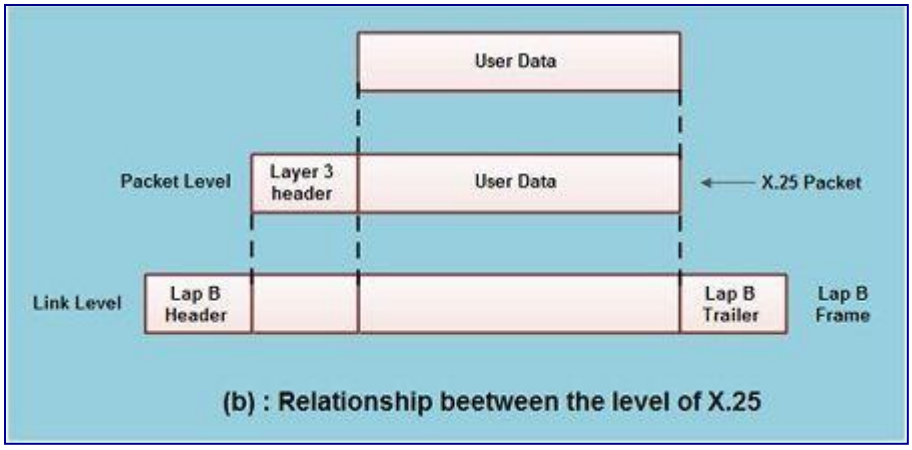
• Fig.(b) shows the relationship between the levels of x'25. User data is passed down to X.25 level 3.

• This data then appends the control information as a header to form a packet. This control .information is then used in the operation of the protocol.

• The entire X.25 packet formed at the packet level is then passed down to the second layer i.e. the data link layer.

• The control information is appended at the front and back of the packet forming a LAP-B frame. The control information in LAP-B frame is needed for the operation of the LAP-B protocol.

• This frame is then passed to the physical layer for transmission.



(b) : Relationship beetween the level of X.25

Virtual Circuit Service

• With the X25 packet layer, data are transmitted in packets over external virtual circuits, The virtual circuit service of X25 provides for two types of virtual circuits,

• The virtual circuit service of X25 provides for two types of virtual circuits i.e. "virtual call" and "permanent virtual circuit".

• A virtual call is a dynamically established virtual circuit using a call set up and call clearing procedure.

• A permanent virtual circuit is a fixed, network assigned virtual circuit. Data transfer takes place as with virtual calls, but no call set up or clearing is required.

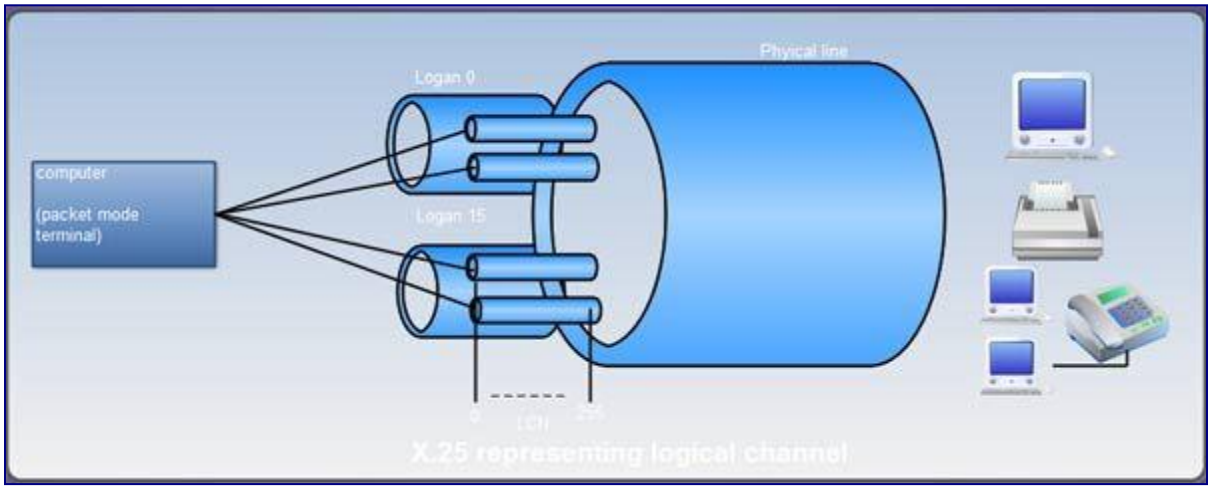
Characteristics of X.25

In addition to the characteristics of the packet switched network, X.25 has the following characteristics:

10. Multiple logical channels can be set on a single physical line
14. Terminals of different communication speeds can communicate
15. The procedure for transmission controls can be changed.

Multiple Logical Channels can be set on a Single Physical Line

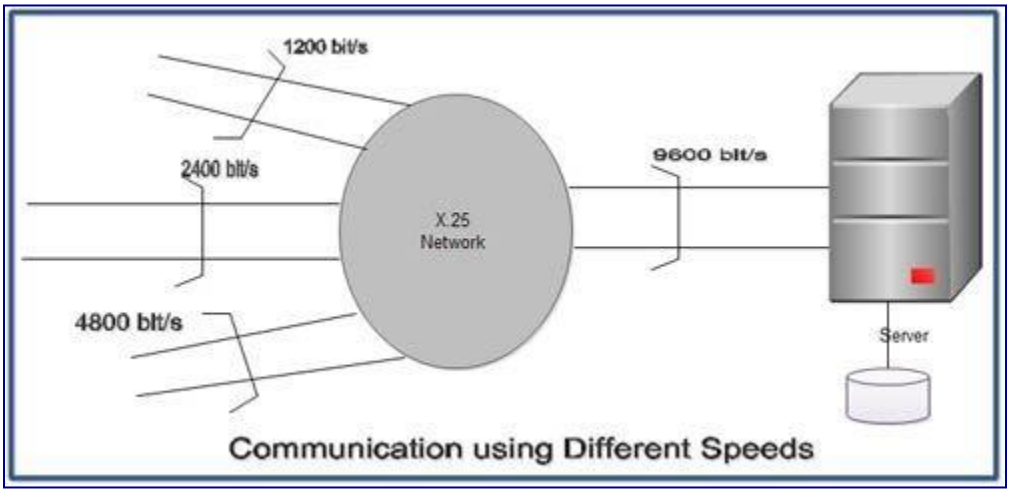
The terminal connected to the packet switched network can communicate with multiple terminals at the same time using a single physical line. This makes it possible to set multiple logical paths called logical channels on a single physical line. Multiple communications thus takes place through these logical channels. Based on the X.25 rules, 4096 logical channel can be set on a single physical line. To enable control of 4096 logical channels there are 16 logical channel groups. Each logical channel group is divided into 256 logical channels. These channel groups are known as LCGN (Logical Channel Group Number) and LCN (Logical Channel Number).



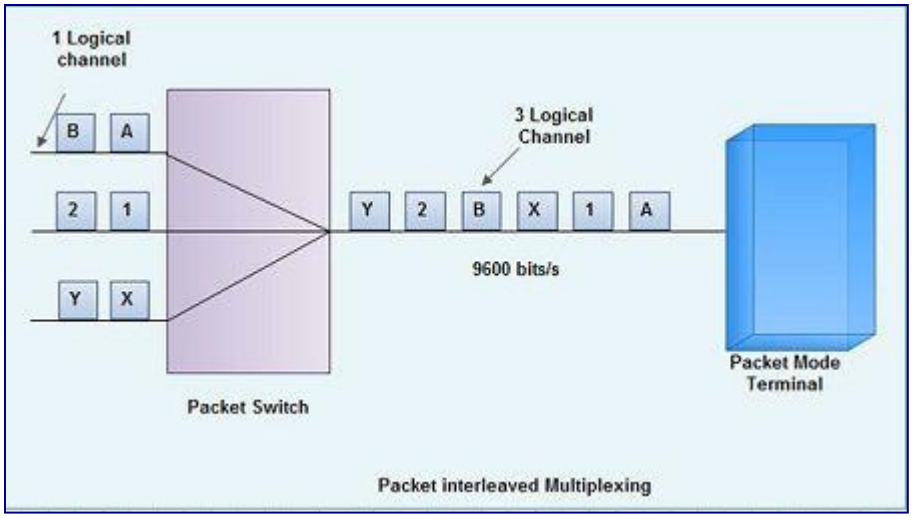
Terminals of Different Communication Speeds can communicate

As X.25 uses the store and forward method, therefore, the communication is possible. In other words, a terminal of 1.2 Kbits/s can communicate with a host computer at 9600 bits/s through the packet switched network. When the 'telephone network or a leased line is used, this type of communication cannot be established. In other words, in these environments, the transmission speed of the sender should be the same as that of the receiver.

The reason that communication between terminals with different communication speeds is possible is that the senders and the receivers are not physically connected. Data transmission from a 1.2 Kbits/s terminal is temporarily stored in the receiving buffer of the packet switched network and the data is then passed through the network and transmitted to the host computer at 9600 bits/s.

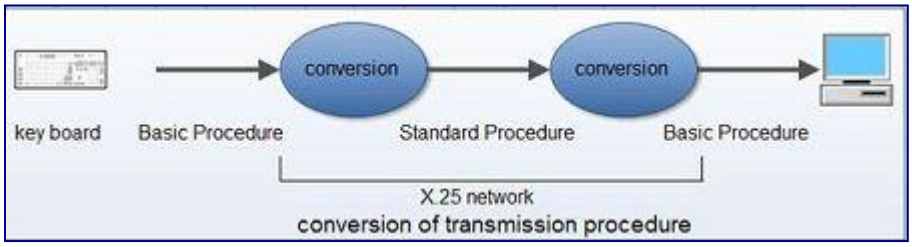


By using the above 2 features the network can be established. By applying a higher line speed to the host computer than the terminal and setting multiple logical channels, the number of lines at the computer can be reduced.



The Procedure for Transmission Controls can be changed

It is possible to change the procedure for transmission control. As we know that X.25 uses the store and forward method, therefore, all data must be once stored in the packet switched unit. By implementing a protocol conversion function to the packet switched unit can connect the devices with different transmission control (basic procedure and X.25 protocol).With the help of this method, any terminal that cannot handle packets cannot be connected to the packet switched network. A terminal that cannot handle packets is called an NPT (Non-packet mode terminal).



OSI and X.25

The X.25 standards appeared well before the OSI reference model. Hence, it was not following the 7-layer model. X.25 describes three layers, as shown in Figure.

X.21: Physical Layer

In the X.25terminology, the physical layer is called X.21interface. This interface specifies the electrical, procedural interface between the data terminal equipment and the X.25network. The RS232-C or V.35 can be used as a substitute for X.21 interface.

Link Access Layer

Link access layer of X.25 is similar to the data link layer of OSI reference model. It provides the basic point-to-point connections between the terminal and X.25 network. It also describes the data

transmission and frame composition methods that X.25supports. It also provides various error control methods and flow control techniques. It defines the basic HDLC LAP-B (Link Access Procedure-B). This protocol is used for establishing virtual connections, handling flow control and releasing the connections. It also includes a mechanism for acknowledging the receipt of packets at the destination.

Packet Layer

This layer is used to setup reliable virtual connections throughout the packet-switched network and a short discussion on packet networks are given for the sake of better understanding of X.25 protocol. The following are a few components of a packet-switched network.

Packet: Packet is a unit of information that can travel independently from the source to the destination. It is packed and addressed so that no additional information is needed to deliver it. Similar to a postal envelope in the postal system, the packet travels through several devices through the network. A packet can convey many different types of information, such as commands, applications, etc.

Packet Assembler or Disassembler (PAD) In packet switching, a single block of information is broken down into many small, individually addressed packets of data. The sending station performs this and transmits them to the destination through the network. The packets are reassembled at the destination to form the original message. The device that performs this is known as a packet assembler or disassembler or PAD. The mechanism by which communication is done between two PCs, using PAD, is illustrated in Figure.

Suppose a station in LAN A is willing to send information to another station in LAN B, the following procedure is adopted. The sending station calls the local PAD and requests a virtual circuit to the remote LAN. The PAD takes data from the sending station, forming it into packets and forwards it to the X.25 network. The network-switching device routes the packets to their destination. The functions of the PAD are governed by three additional protocols. They are:

X.3: Specifies how the PAD actually assembles and disassembles the data.

X.28: Defines the interface between data terminal equipment and the PAD.

X.29: Defines the interface between data communication equipment and PAD.

Packet dispatching method Each packet in the X.25 network carries the destination address. The method by which the packet reaches its destination needs the following three components.

- • Router
- • Bridges
- • Switches

Each packet in the X.25 network contains two addresses. They are MAC address and the network address. Bridges and switches in the network use MAC address. They transmit the packet to the

correct segment on the network in which the destination is present. The complete set of addresses in each network segment is available at each bridge for this purpose. Router sends the packet over predefined routes to the destination address. There are several routing algorithms used for this. Routers on the X.25 network can determine data transmission path, using connection oriented or connectionless communication method.

X.25 is a connection-oriented protocol. It establishes a connection between the sending and receiving stations before data is transmitted. However, for each connection, only one packet is transmitted, thereby, one of the major problems associated with the connection-oriented protocol is overcome. At the same time, X.25 retains the reliability of connection-oriented protocol.

Packet-switched network As the X.25 network transmits data at the rate of one packet per connection. For transmitting a complete block of data, thousands of connections are made rapidly and released. Hence, the X.25 network is known as a packet-switched network. A packet-switched network consists of a dense mesh of point-to-point connections. At a very high level, it behaves like a circuit switched network. A virtual connection is established between the sending station and the receiving station. The sending station then transmits the data to the receiving station. When the transmission is complete, the virtual circuit is cleared. The packet-switched network is similar to the one shown in Figure.

The main difference between circuit-switched and the packet-switched network is that in a circuit switched network, once a connection is established, the entire data is transmitted through that connection. But in a packet-switched network, each packet of a single message may take a different virtual circuit.

Uses of public and private X.25 networks X.25 networks provide effective solutions to many applications. They work very well, when users are willing to connect to multiple hosts for a shorter duration of time. One good example is processing of credit cards. Special card readers are used to read the information from the credit cards. The electronic transaction from the card reader is frequently carried out over an X.25 network. This permits very short messages (which include the account number, store ID, and the amount to be charged) to be sent to the concerned bank and the receipt of the transaction to be acknowledged by the bank. The X.25protocol allows this to occur without the use of costly, dedicated connections from each store to each bank that issues the credit card.

Packet-switching services can be obtained through private or public networks. Private networks are networks, whose resources (access circuits, interfaces between users' equipments and packet switching nodes (PSNs), and the trunk circuit that connects them) are dedicated to a small group of users. Private network access is done through dedicated circuits.

Resources of a public network are owned by someone and leased on a usage basis by many users. For example, the telephone network is a public network. It is owned by DOT and leased by many subscribers under a rented basis. Access to public network is done through dial-up circuits. The tariff for usage of a public network is estimated from the amount of time the user is connected or

the number of packets the user sends and receives. The choice of private and public network is based on the cost and the desired network performance.

Switched and permanent virtual circuits A virtual circuit is an end-to-end logical transmission path, through which data packets can be transmitted. Each station maintains a virtual circuit table, which contains all the virtual circuits passing through it. Virtual circuits can be established in two ways. They are permanent virtual circuit (PVC) and switched virtual circuit (SVC). The network manager can manually configure a permanent virtual circuit. Hence, at the time of transmission, no set up time is needed. The PVC provides dedicated bandwidth to a particular station. The second type of virtual circuit, switched virtual circuit (SVC) is a temporary virtual circuit set up between the sending and the receiving stations. The SVC is maintained until the transmission has been completed. It is cleared when the transmission session is over. SVC is established every time before the start of data transfer, by either the network manager or by the application. X.25 supports both types of virtual circuits.

X.25 Performance During 1976, when the X.25standard was released, it was capable of supporting a transmission speed of 64 Kbps. Unfortunately most of this bandwidth was used only for error checking. During 1992, ITU revised and issued a new X.25version, which was able to support a speed of 2.048Mbps. The France Telecom has been offering 2.08Mbps X.25 for many years. The packet based nature of the X.25 affect the performance very badly. During times when the traffic is extremely heavy, packet delivery delay is inevitable. Even though the routers are directing the packets around the congested areas, users still experience a poor performance. On the other hand packet-switching can accommodate burst of traffic over and above the maximum bandwidth however, circuit switching can accommodate inflexible and finite amount of traffic only.

X.25 protocol is highly reliable than any other protocol of this kind. Every router in the network, on receiving the packet, performs a complete check-up for the presence of errors before sending it to the next router. As a result, each node maintains a table, containing management, flow control, and error checking information against which, each packet is checked. In addition to this, the destination stations take responsibility to detect the lost or damaged packet and requests for a retransmission.

For every transmission of a packet to the next node, an acknowledgment is received from the next node in the data link layer. At the network layer, acknowledgment is sent back by the destination station to the source station as soon as the packet is received.

7. Why routing is essential in computer networking? Compare working of distance vector routing algorithm with link state routing algorithm.

The routing algorithms are used for routing the packets. The routing algorithm is nothing but a software responsible for deciding the optimal path through which packet can be transmitted. The routing protocols use the metric to determine the best path for the packet delivery. The metric is the standard of measurement such as hop count, bandwidth, delay, current load on the path, etc.

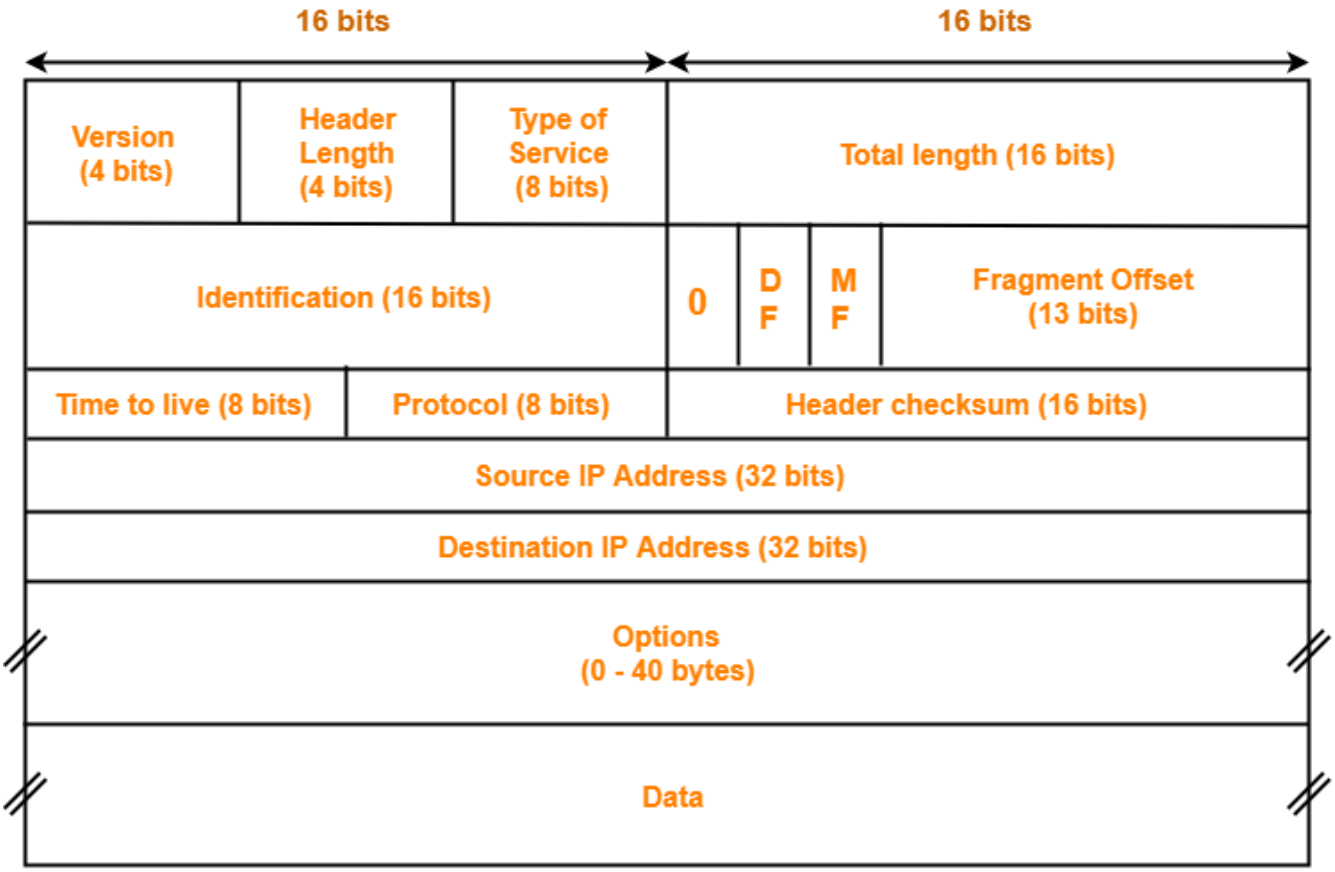
used by the routing algorithm to determine the optimal path to the destination. The routing algorithm initializes and maintains the routing table for the process of path determination.

Key Differences Between Distance Vector Routing and Link State Routing: -

11. Bellman-Ford algorithm is used for performing distance vector routing whereas Dijsktra is used for performing the link state routing.
12. In distance vector routing the routers receive the topological information from the neighbour point of view. On the contrary, in link state routing the router receive complete information on the network topology.
13. Distance vector routing calculates the best route based on the distance (fewest number of hops). As against, Link state routing calculates the best route on the basis of least cost.
14. Link state routing updates only the link state while Distance vector routing updates full routing table.
15. The frequency of update in both routing technique is different distance vector update periodically whereas link state update frequency employs triggered updates.
16. The utilization of CPU and memory in distance vector routing is lower than the link state routing.
17. The distance vector routing is simple to implement and manage. In contrast, the link state routing is complex and requires trained network administrator.
18. The convergence time in distance vector routing is slow, and it usually suffers from count to infinity problem. Conversely, the convergence time in link state routing is fast, and it is more reliable.
19. Distance vector doesn't have hierarchical structure while in link state routing the nodes can have a hierarchical structure.

8. Explain in detail about IP frame format.

The IPv6 packet is shown in Figure. Each packet is composed of a mandatory base header followed by the payload. The payload consists of two parts: optional extension headers and data from an upper layer. The base header occupies 40 bytes, whereas the extension headers and data from the upper layer contain up to 65,535 bytes of information.Base HeaderFigure shows the base header with its eight fields. These fields are as follows:o Version. This 4-bit field defines the version number of the IP. For IPv6, the value is 6.o Priority. The 4-bit priority field defines the priority of the packet with respect to traffic congestion.



IPv4 Header

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

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

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

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

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

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

10. How does the protocol SMTP operate? Explain the procedures to make your network secured.

SMTP provides a set of codes that simplify the communication of email messages between email servers (the network computer that handles email coming to you and going out). It's a kind of shorthand that allows a server to break up different parts of a message into categories the other server can understand. When you send a message out, it's turned into strings of text that are separated by the code words (or numbers) that identify the purpose of each section.

SMTP provides those codes, and email server software is designed to understand what they mean. As each message travels towards its destination, it sometimes passes through a number of computers as well as their individual MTAs. As it does, it's briefly stored before it moves on to the next computer in the path. Think of it as a letter going through different hands as it winds its way to the right mailbox.

1. Put In And Monitor Firewall Performance

A firewall is a piece or set of software or hardware designed to block unauthorized access to computers and networks. In very simple terms, a firewall is a series of rules that control incoming and outgoing network traffic; computers and networks that “follow the rules” are allowed into access points, and those that don’t are prevented from accessing your system.

Firewalls are becoming more and more sophisticated (right along with hackers) and the latest are integrated network security platforms that consist of a variety of approaches and encryption methods, all working in tandem to prevent breaches.

2. Update Passwords At Least Every Quarter

Hopefully, by now your employees know to avoid default passwords or phrases like “password,” “12345” and their dates of birth. In addition to using passwords that feature both letters, symbols and numbers — and some uppercase letters — for added security, require employees to regularly change any personal passwords used on systems that have access to business networks (your business will have its own, but many computers also allow personal passwords).

Let employees know that when choosing passwords, substituting letters with similarly shaped characters, like “pa$$w0rd” for “password,” is a bad idea. Hackers are onto that trick!

Every quarter is the recommended frequency, but more often is better. However, there is a fine line: changing passwords too often can cause confusion, leading employees to reach out to IT for reminders of their username and passwords.

3. Maintain Your Anti-Virus Software

If you're not performing regular updates of your anti-virus software, you're putting your network at greater risk and creating potential cybersecurity issues, as hackers find ways to "crack" these tools and can deploy new viruses. Staying ahead of them by using the latest versions of software is critical.

It's also a good idea to help employees identify the signs to look for to know if their computer has been hacked. Cybercriminals are increasingly cunning, and even the most vigilant efforts to secure your network could be compromised by an equally vigilant hacker.

4. Create A Virtual Private Network (VPN)

VPNs create a far more secure connection between remote computers (home networks or computers used by people on the road) and other "local" computers and servers. These networks are essentially only available to people who should have access to your systems, including your wireless network, and to equipment that's been authorized in your network settings. A VPN can dramatically decrease the likelihood that hackers can find a wireless access point and wreak havoc on your system.

5. Training Your Employees

All the tools and tricks in the book won't do much good if the people using your system aren't following computer security best practices. Frequent reminders about the risks and the steps to mitigate them will help keep network security top of mind; some organizations work these kinds of updates into mandatory meetings to help communicate the importance. Educating employees about how to avoid major security risks is possibly the greatest weapon you have in combating cybercrime.