COMPUTER NETWORKS

Unit-1

What is internet:

Internet is a vast network that connects computers all over the world. Through the Internet, people can share information and communicate from anywhere with an Internet connection.

The Internet is a global network comprised of smaller networks that are interconnected using standardized communication protocols. The Internet standards describe a framework known as the Internet protocol suite. This model divides methods into a layered system of protocol.

These layers are as follows:

- Application layer (highest) – concerned with the data(URL, type, etc.). This is where HTTP, HTTPS, etc., comes in.
- Transport layer – responsible for end-to-end communication over a network.
- Network layer – provides data route.

The Internet provides a variety of information and communication facilities; contains forums, databases, email, hypertext, etc. It consists of private, public, academic, business, and government networks of local to global scope, linked by a broad array of electronic, wireless, and optical networking technologies

It is also known as the Networks of Network.

Ex:BSNL-Public internet service provider.

NUTS & BOLTS DESCRIPTION:

The public Internet is a worldwide computer network, that is, a network that interconnects millions of computing devices throughout the world

In Internet world, all of these devices are called hosts or end systems. Hosts or end systems are connected together by communication links. They are indirectly connected to each other through intermediate switching devices know as packed switches.

Communication links:

Communications link is the communications channel that connects two or more communicating devices. This link may be an actual physical link or it may be a logical link that uses one or more actual physical links.

Different types of communication links:

1. Co-axial cable
2. Fiber optic cable
3. Twisted pair cable

Wireless communication links:

Wireless transmission is a form of unguided media. Wireless communication involves no physical link established between two or more devices, communicating wirelessly. Wireless

signals are spread over in the air and are received and interpreted by appropriate antennas.

Band width:

Network bandwidth is a measurement indicating the maximum capacity of a wired or wireless communications link to transmit data over a network connection in a given amount of time. Typically, bandwidth is represented in the number of bits, kilobits, megabits or gigabits that can be transmitted in 1 second.

INTERNET PROTOCOL:

Internet Protocols are a set of rules that governs the communication and exchange of data over the internet. Both the sender and receiver should follow the same protocols in order to communicate the data.

We have various types of protocals but among them

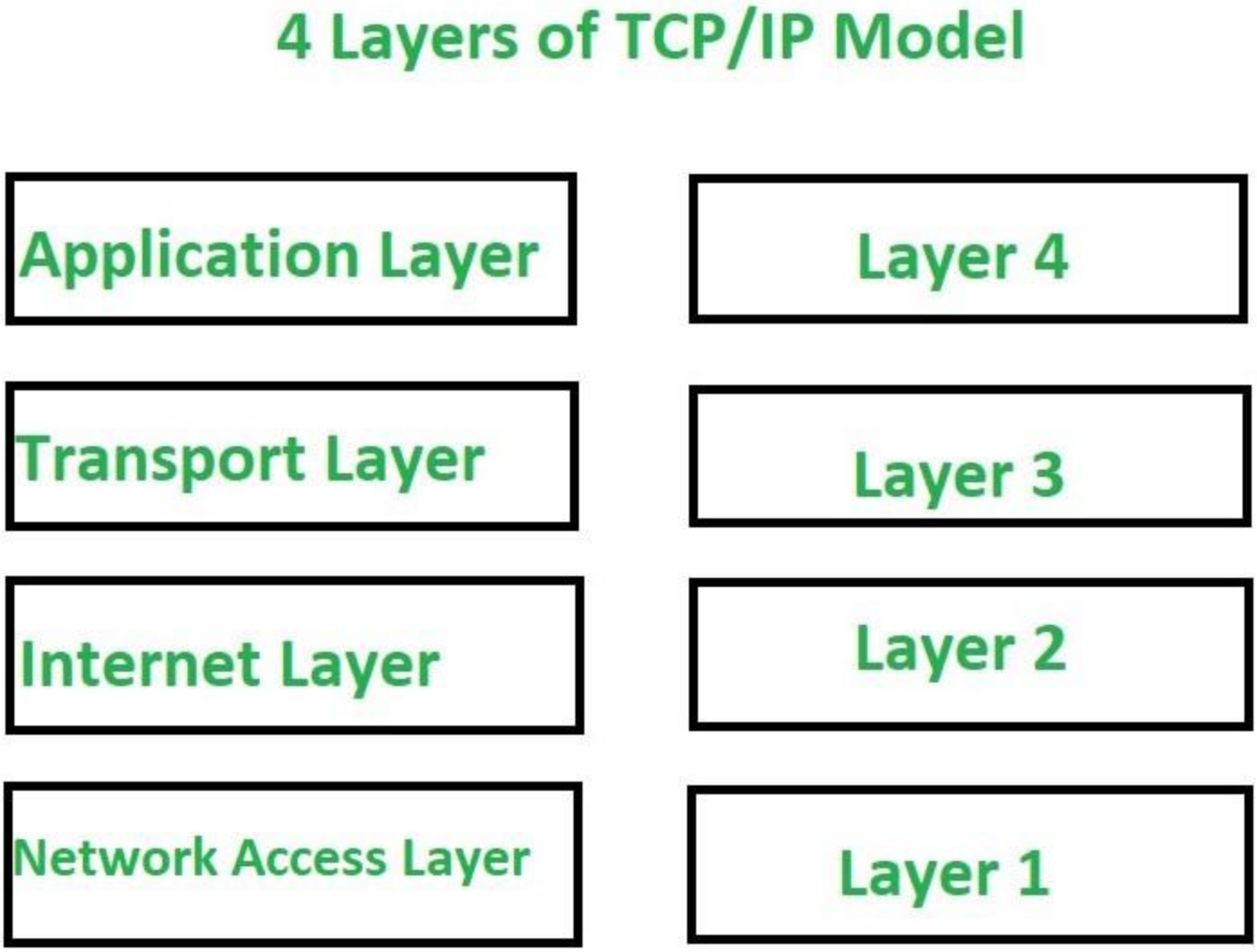
1**.TCP/IP(Transmission Control Protocol/ Internet Protoco**l):

These are a set of standard rules that allows different types of computers to communicate with each other. The IP protocol ensures that each computer that is connected to the Internet is having a specific serial number called the IP address. TCP specifies how data is exchanged over the internet and how it should be broken into IP packets. It also makes sure that the packets have the information about the source of the message data, the destination of the message data, the sequence in

which the message data should be re-assembled, and checks if the message has been sent correctly to the specific destination

The functionality of TCP/IP is divided into 4 layers with each one having specific protocols:

- Application Layer: The application layer makes sure that the data from the sending end is received in a format that is acceptable and supported at the receiving end.
- Transport Layer: The transport layer is responsible for the smooth transmission of data from one end to the other. It is also responsible for reliable connectivity, error recovery, and flow control of the data.
- Internet Layer: This Internet Layer moves packets from source to destination by connecting independent networks.
- Network Access Layer: The Network Access Layer sees how a computer connects to a network.



2.**FTP (File Transfer Protocol):**

This protocol is used for transferring files from one system to the other. This works on a client-server model. When a machine requests for file transfer from another machine, the FTO sets up a connection between the two and authenticates

each other using their ID and Password. And, the desired file transfer takes place between the machines.

3.HTTP(HyperText Transfer Protocol):

This protocol is used to transfer hypertexts over the internet and it is defined by the www(world wide web) for information transfer. This protocol defines how the information needs to be formatted and transmitted. And, it also defines the various actions the web browsers should take in response to the calls made to access a particular web page. Whenever a user opens their web browser, the user will indirectly use HTTP as this is the protocol that is being used to share text, images, and other multimedia files on the World Wide Web.

Note: Hypertext refers to the special format of the text that can contain links to other texts.

Types of Protocols

1. Transmission Control Protocol (TCP)
2. Internet Protocol (IP)
3. User Datagram Protocol (UDP)
4. Post office Protocol (POP)
5. Simple mail transport Protocol (SMTP)
6. File Transfer Protocol (FTP)
7. Hyper Text Transfer Protocol (HTTP)
8. Hyper Text Transfer Protocol Secure (HTTPS)

Network edge:

The network edge refers to the area where a device or local network interfaces with the internet. The edge is close to the devices it is communicating with and is the entry point to the network. The network edge is a crucial security boundary that network administrators must provide solutions for.

- Client program:

It is one of the system,program running in one system for sending another system

- Server program:

One of the end system

Connection oriented service protocal:

Connection-Oriented Protocol (COP) is a networking protocol used to establish a data communication session in which endpoint devices use preliminary protocols to establish end-to-end connections and then the subsequent data stream is delivered in sequential transfer mode.

It provides two different service.

1. Connection-Oriented Protocols:

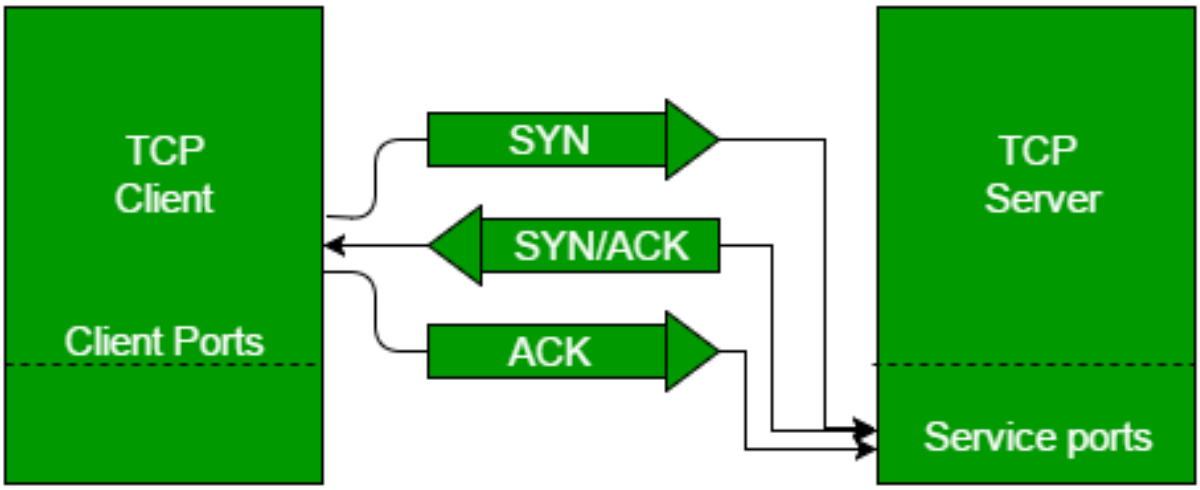
TCP is an example of a connection-oriented protocol. It requires a logical connection to be established between the two processes before data is exchanged. The connection must

be maintained during the entire time that communication is taking place, then released afterwards.

We use **HAND SHAKING MECHANISM** in establishing the connection between 2 or more systems.

HAND SHAKING MECHANISM:

Handshaking is the process that establishes communication between two networking devices. For example, when two computers first connect with each other through modems, the handshaking process determines which protocols, speeds, compression, and error-correction schemes will be used during the communication session



Hand shaking mechanism has 3 variant features:

- Reliable data transfer:
  Reliable data transfer protocols (RDT, RDP) are algorithmic measures to provide assurances of the reliable transfer of

data across a network that may be subject to data loss and/or corruption.

- Flow control:
  Flow control is the management of data flow between computers or devices or between nodes in a network so that the data can be handled at an efficient pace.
- Congestion control:
  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.

2. Connection less services:

A Connectionless Service is technique that is used in data communications to send or transfer data or message at Layer 4 i.e., Transport Layer of Open System Interconnection model. This service does not require session connection among sender or source and receiver or destination. Sender starts transferring or sending data or messages to destination

NETWORK CORE:

Core network is a collection of network hardware, devices, and software that provides the fundamental services for your organization's information technology (IT) needs. A Windows Server core network provides you with many benefits, including the following.

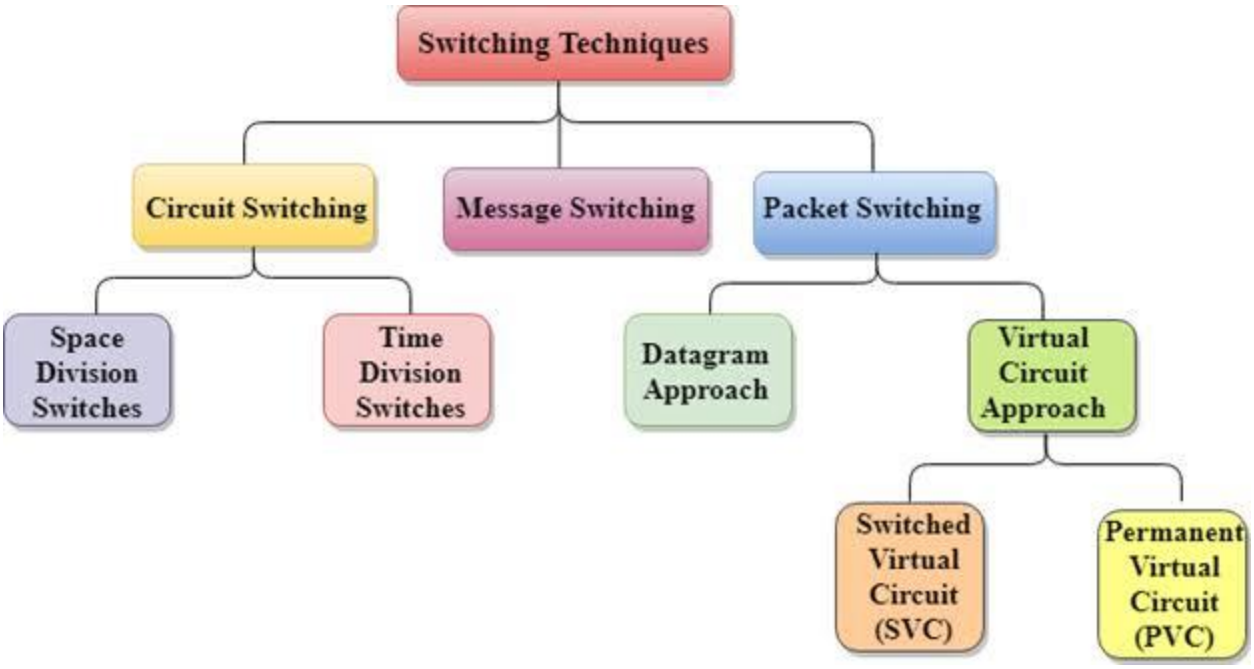
- Switching:

Forwarding the packets that are coming from one part to another part.

- Packets:network packet is a small amount of data sent over Transmission Control Protocol/Internet Protocol (TCP/IP) networks. The packet size is around 1.5 kilobytes for Ethernet and 64 KB for IP payloads.

When a user accesses the internet or another computer network outside their immediate location, messages are sent through the network of transmission media. This technique of transferring the information from one computer network to another network is known as switching.

Switching in a computer network is achieved by using switches. A switch is a small hardware device which is used to join multiple computers together with one local area network (LAN).



1.Circuit Switching:

When a dedicated path is established for data transmission between sender and receiver, it is called circuit switching. When any network node wants to send data, be it audio, video, text or any other type of information, a call request signal is sent to the receiver and acknowledged back to ensure availability of dedicated path. This dedicated path is then used to send data. ARPANET used circuit switching for communication over the network.

Advantages of Circuit Switching:

Circuit switching provides these advantages over other switching techniques –

- Once path is set up, the only delay is in data transmission speed

- No problem of congestion or garbled message

Disadvantages of Circuit Switching:
Circuit switching has its disadvantages too –

- Long set up time is required
- A request token must travel to the receiver and then acknowledged before any transmission can happen
  Line may be held up for a long time

2.Packet Switching:

As we discussed, the major problem with circuit switching is that it needs a dedicated line for transmission. In packet switching, data is broken down into small packets with each packet having source and destination addresses, travelling from one router to the next router.

3.Message Switching :

Message switching was a technique developed as an alternative to circuit switching before packet switching was introduced. In message switching, end-users communicate by sending and receiving messages that included the entire data to be shared. Messages are the smallest individual unit.

Also, the sender and receiver are not directly connected. There are a number of intermediate nodes that transfer data and ensure that the message reaches its destination. Message switched data networks are hence called hop-by-hop systems

5.1.5 Comparison of Virtual-Circuit and Datagram Networks

Issue	Datagram subnet	Virtual-circuit subnet
Circuit setup	Not needed	Required
Addressing	Each packet contains the full source and destination address	Each packet contains a short VC number
State information	Routers do not hold state information about connections	Each VC requires router table space per connection
Routing	Each packet is routed independently	Route chosen when VC is set up; all packets follow it
Effect of router failures	None, except for packets lost during the crash	All VCs that passed through the failed router are terminated
Quality of service	Difficult	Easy if enough resources can be allocated in advance for each VC
Congestion control	Difficult	Easy if enough resources can be allocated in advance for each VC

Delay & loss of packet in switched networks:

The delays, here, means the time for which the processing of a particular packet takes place. We have the following types of delays in computer networks:

- Propagation delay
- Transmission delay
- Queueing delay
- Processing delay

1. Transmission Delay:

The time taken to transmit a packet from the host to the transmission medium is called Transmission delay.

For example, if bandwidth is 1 bps (every second 1 bit can be transmitted onto the transmission medium) and data size is 20 bits then what is the transmission delay? If in one second, 1 bit can be transmitted. To transmit 20 bits, 20 seconds would be required.

Let B bps is the bandwidth and L bit is the size of the data then transmission delay is,

$Tt = L/B$

This delay depends upon the following factors:

- If there are multiple active sessions, the delay will become significant.
- Increasing bandwidth decreases transmission delay.
- MAC protocol largely influences the delay if the link is shared among multiple devices.
- Sending and receiving a packet involves a context switch in the operating system, which takes a finite time.

2. Propagation delay:

After the packet is transmitted to the transmission medium, it has to go through the medium to reach the destination. Hence the time taken by the last bit of the packet to reach the destination is called propagation delay.

Factors affecting propagation delay:

- Distance – It takes more time to reach the destination if the distance of the medium is longer.
- Velocity – If the velocity(speed) of the signal is higher, the packet will be received faster.

Tp = Distance / Velocity

Note:

Velocity =3 X 10^8 m/s (for air)

Velocity= 2.1 X 10^8 m/s (for optical fibre)

3. Queueing delay:

Let the packet is received by the destination, the packet will not be processed by the destination immediately. It has to wait in a queue in something called a buffer. So the amount of time it waits in queue before being processed is called queueing delay.

In general, we can't calculate queueing delay because we don't have any formula for that.

This delay depends upon the following factors:

- If the size of the queue is large, the queuing delay will be huge. If the queue is empty there will be less or no delay.
- If more packets are arriving in a short or no time interval, queuing delay will be large.
- The less the number of servers/links, the greater is the queuing delay.

4.Processing delay:

Now the packet will be taken for the processing which is called processing delay.

Time is taken to process the data packet by the processor that is the time required by intermediate routers to decide where to forward the packet, update TTL, perform header checksum calculations.

It also doesn't have any formula since it depends upon the speed of the processor and the speed of the processor varies from computer to computer.

Note: Both queueing delay and processing delay doesn't have any formula because they depend on the speed of the processor

This delay depends upon the following factors:

It depends on the speed of the processor.

Ttotal = Tt + Tp + Tq + Tpro

Ttotal = Tt+Tp

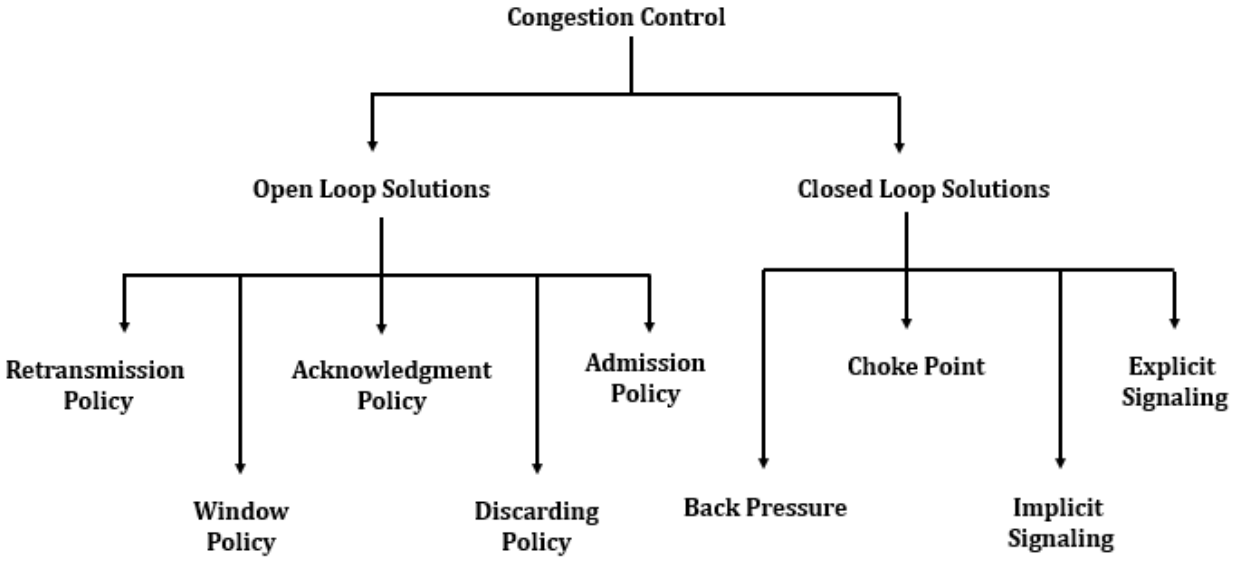
(when taking Tq and Tpro equals to 0)

Packet loss:

Packet loss describes lost packets of data not reaching their destination after being transmitted across a network. Packet loss occurs when network congestion, hardware issues, software bugs, and a number of other factors cause dropped packets during data transmission.

- Congestion:
  Network congestion refers to a reduction in quality of service (QOS) that causes packet loss, queueing delay, or the blocking of new connections. Typically, network congestion occurs in cases of traffic overloading when a

link or network node is handling data in excess of its capacity



Open loop solutions:

1.Retransmission Policy :

If the sender feels that a sent packet is lost or corrupted, the packet needs to be retransmitted. This transmission may increase the congestion in the network. To prevent congestion, retransmission timers must be designed to prevent congestion and also able to optimize efficiency

2.Window Policy :

The type of window at the sender's side may also affect the congestion. Several packets in the Go-back-n window are re-sent, although some packets may be received

successfully at the receiver side. This duplication may increase the congestion in the network and make it worse

3.Acknowledgement Policy :

This policy imposed by the receiver may also affect congestion. If the receiver does not acknowledge every packet it receives, it may slow down the sender and help prevent congestion. A receiver may send an acknowledgment only if it has a packet to be sent or a special timer expires

4.Discarding Policy :

A good discarding policy adopted by the routers is that the routers may prevent congestion and at the same time partially discard the corrupted or less sensitive packages and also be able to maintain the quality of a message

5.Admission Policy :

Switches in a flow should first check the resource requirement of a network flow before transmitting it further. If there is a chance of a congestion or there is a congestion in the network, router should deny establishing a virtual network connection to prevent further congestion

Closed loop solutions (Removal) :

1.Back pressure:

Backpressure is a technique in which a congested node stops receiving packets from upstream node. This may cause the upstream node or nodes to become congested and reject

receiving data from above nodes. Backpressure is a node-to-node congestion control technique that propagate in the opposite direction of data flow.

2.Choke packet:

A choke packet is used in network maintenance and quality management to inform a specific node or transmitter that its transmitted traffic is creating congestion over the network. This forces the node or transmitter to reduce its output rate. Choke packets are used for congestion and flow control over a network.

3.Implicit control/signaling:

In implicit signaling, there is no communication between the congested nodes and the source. The source guesses that there is congestion in a network. For example when sender sends several packets and there is no acknowledgment for a while, one assumption is that there is a congestion.

4.Explicit control/signaling:

The difference between choke packet and explicit signaling is that the signal is included in the packets that carry data rather than creating a different packet as in case of choke packet technique. Explicit signaling can occur in either forward or backward direction.

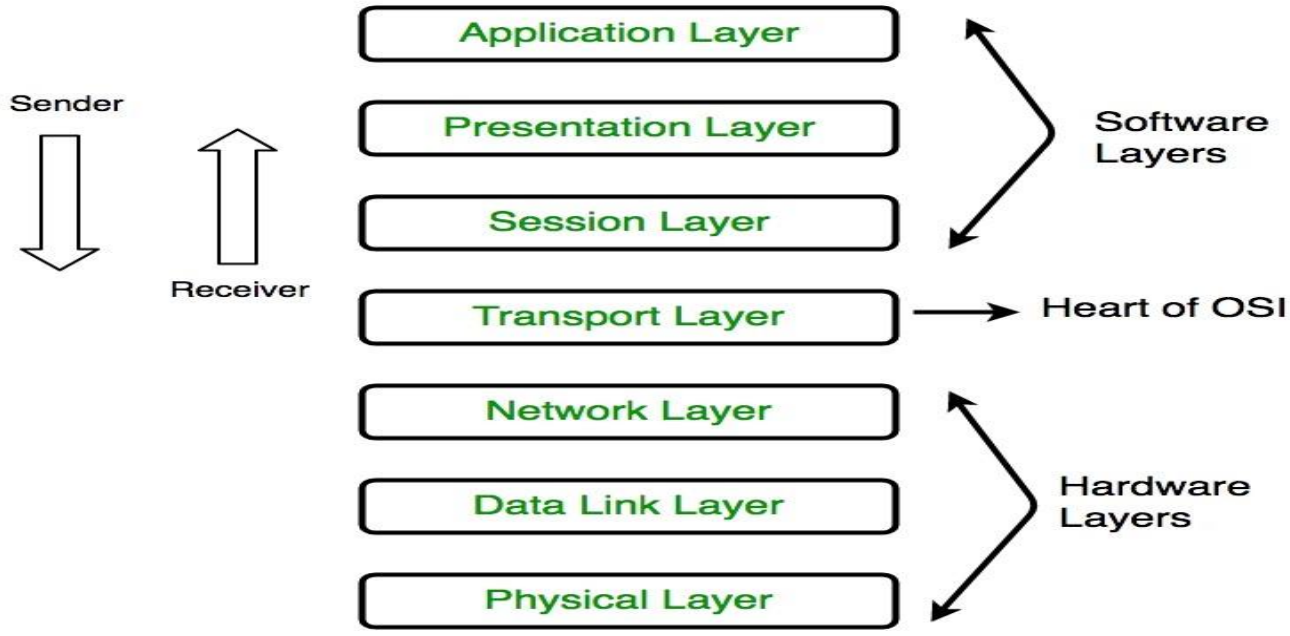
- Software Bugs:

Software bugs are another common cause of packet loss. If rigorous testing has not been carried out or bugs have been introduced following software updates, this could result in unintended or unexpected network behavior. Sometimes rebooting can resolve this issues, but more often than not the software will need to be updated or patched.

Throughout:

In data transmission, network throughput is the amount of data moved successfully from one place to another in a given time period, and typically measured in bits per second (bps), as in megabits per second (Mbps) or gigabits per second (Gbps).

Protocal layers and their service models:



Layered architecture:

Each & every layer had it's own technology and functionality

Totally,it have 7 layers but we consider only 5 among them

1. Application layer
2. Presentation layer
3. Session layer
4. Transport layer
5. Network layer
6. Datalink layer
7. Physical layer

- Application layer(Layer 7) :

At the very top of the OSI Reference Model stack of layers, we find the 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.

Example: Application – Browsers, Skype Messenger, etc.

- Presentation Layer (Layer 6):

The 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 :

Translation: For example, ASCII to EBCDIC.

Encryption/ Decryption: Data encryption translates the data into another form or code. The encrypted data is known as the ciphertext and the decrypted data is known as plain text. A key value is used for encrypting as well as decrypting data.

Compression: Reduces the number of bits that need to be transmitted on the network.

- Session Layer (Layer 5) :

This layer is responsible for the 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 synchronization points into the data. These synchronization points 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

- Transport Layer (Layer 4) :

The transport layer provides services to the application layer and takes services from the 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. The transport layer also provides the acknowledgement of the successful data transmission and re-transmits the data if an error is found.

At sender's side: Transport layer receives the formatted data from the upper layers, performs Segmentation, and also implements Flow & Error control to ensure proper data transmission. It also adds Source and Destination port numbers in its header and forwards the segmented data to the Network Layer.

At receiver's side: Transport Layer reads the port number from its header and forwards the Data which it has received to the respective application. It also performs sequencing and reassembling of the segmented data.

- Network Layer (Layer 3) :

The 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 addresses are placed in the header by the network layer.

The functions of the Network layer are :

Routing: The network layer protocols determine which route is suitable from source to destination. This function of the network layer is known as routing.

Logical Addressing: In order to identify each device on internetwork uniquely, the network layer defines an addressing scheme. The sender & receiver's IP addresses are placed in the header by the network layer. Such an address distinguishes each device uniquely and universally.

- 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 sublayers:

- Logical Link Control (LLC)
- Media Access Control (MAC)

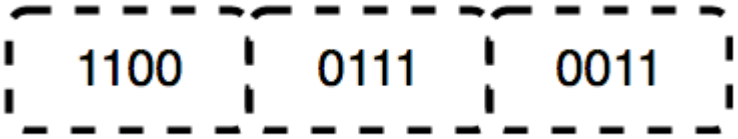
The functions of the Data Link layer are :

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, the Data link layer adds physical addresses (MAC address) of the 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 the amount of data that can be sent before receiving acknowledgement.

5. Access control: When a single communication channel is shared by multiple devices, the MAC sub-layer of the data link layer helps to determine which device has control over the channel at a given time.

- 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 transmitting individual bits from one node to the next. 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.



The functions of the physical layer are as follows:

- 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.

- Bit rate control: The Physical layer also defines the transmission rate i.e. the number of bits sent per second.
- Physical topologies: Physical layer specifies the way in which the different, devices/nodes are arranged in a network i.e. bus, star, or mesh topology.
- 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.
- Hub, Repeater, Modem, Cables are Physical Layer devices.

** Network Layer, Data Link Layer, and Physical Layer are also known as Lower Layers or Hardware Layers.

Network under attack:

Under the network attack method, external parties manipulate forms by submitting malicious codes in place of expected data values. They compromise the network and access sensitive data such as user passwords.

Common types of network attacks:

1. Unauthorized access
2. Distributed Denial of Service (DDoS) attacks
3. Man in the middle attacks

4. Code and SQL injection attacks
5. Privilege escalation
6. Insider threats

These attacks can be prevented by providing some security

Network security:

Network security is a set of technologies that protects the usability and integrity of a company's infrastructure by preventing the entry or proliferation within a network of a wide variety of potential threats.

(Or)

Network security:

It is a protection of the access to files and directories in a computer network against hacking, misuse and unauthorized changes to the system. An example of network security is an anti virus system.

The authorization of access to data in a network, which is controlled by the network administrator.Users are assigned an ID and password that allows them access to information and programs within their authority

History of computer network & Internet:

- Network:

A network is a collection of computers, servers, mainframes, network devices, peripherals, or other devices connected to allow data sharing. An example of a network is the Internet, which connects millions of people all over the world

- Internet:

The Internet is a vast network that connects computers all over the world. Through the Internet, people can share information and communicate from anywhere with an Internet

History:

The First Computer Network is Born:

The history of modern computer networking technology goes back to 1969, when ARPANET (Advanced Research Projects Agency Network) became the first connected computer network. It implemented the TCP/IP protocol suite, which later became the Internet

The period of tremendous growth of the Internet in the latter half of the 1990s. In the 1994-1996 time frame, it changed from a scientific and governmental research network to a commercial and consumer marketplace

To communicate by using internet we follow some kind if protocals,which we had seen before like HTTP,SMTP, TCP, UDP, POP… . etc

Applications of internet:

In modern world we use internet in various fields.some of

them are as

Following are the applications of internet:

- Faster, cheaper and easier medium of communication.
- Information sharing and browsing.
- File transferring facility.
- Reach to the worldwide viewers.
- Effective, easier, faster and cheaper promotion of product or service.

- Better customer support and customer relationship management (CRM).
- Online services like banking, shopping, education, etc.
- E-mail communication for sending and receiving an electronic document.
- Enhanced collaboration between different organizations.
- Effective Supply Chain Management (SCM).
- Electronic payment system using credit /debit cards, ATM, online payment, electronic cheque,Smart card, electronic purse, etc.
- Newsgroups for instant sharing of news and feedback system.
- Creation of new job opportunities related with the internet.
- Source for entertainment.
- Social networking for instant touch with friends and relatives.