Layout - design , state

Date ______
Page ______

Networking / Computer Networks [CN]

VIP :-

Que-1. What is Network ? What are the diffrent types of Networks ? Types of Network Topologies ?

Network :- A network is a set of devices that are connected with a physical media link. In a network, two or more nodes are connected by a physical link or two or more networks are connected by one or more nodes.

A Network is a collection of devices connected to each other to allow the sharing of ~~media~~. data.

Network Topology :- Network topology specifies the layout of a computer network. It shows how devices and cables are connected to each other.

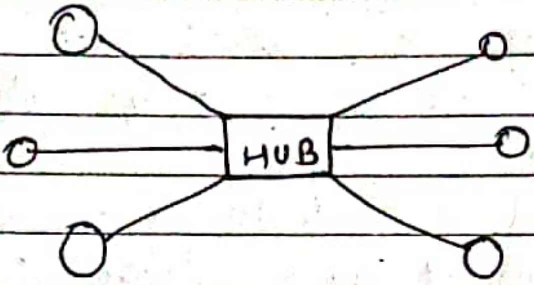
Types of Network Topologies ->

1) Star :- i) Star Topology is a network topology in which all the nodes are connected to a single device known as central device (Hub).

ii) Star topology requires more cable compared to other topologies. Therefore it is more robust as a failure in one cable will only disconnect a specific computer ~~iii)~~ connected to this cable.

iii) If the central device is damaged, then the whole Network fails.

iv) Star topology is easy to install, manage and troubleshoot. It is commonly used in office and home networks.



Star Topology

2) **Ring:-**

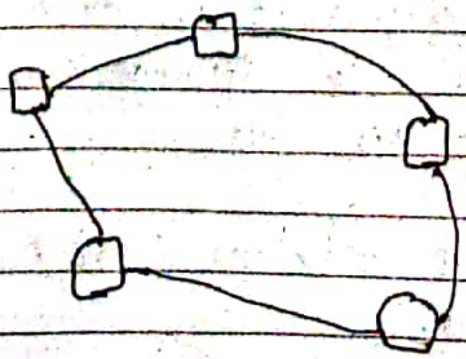
i) Ring topology is a network topology in which nodes are exactly connected to two or more nodes and thus, forming a single continuous path for the transmission.

ii) It does not need any central server to control the connectivity among the nodes.

iii) If the single node is damaged, then the whole network fails.

iv) Ring topology is very rarely used as it is expensive, difficult to install and manage.

v) Example- SONET network, SDH network, etc.



Ring Topology

Date ______
Page ______

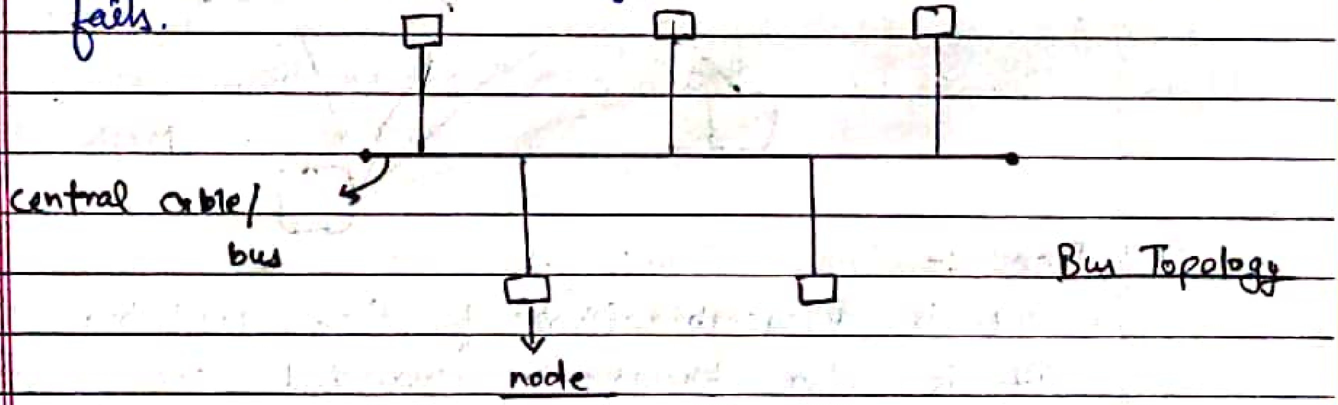
3) Bus -

i) Bus topology is a network topology in which all the nodes are connected to a single cable known as a central cable or bus.

ii) It acts as a shared communication medium, i.e., if any device wants to send the data to the other devices, then it will send the data over the bus which in turn sends the data to all the attached devices.

iii) Bus topology is useful for a small number of devices.

iv) As if the bus is damaged then the whole network fails.



4) Mesh :-

i) Mesh topology is a network topology in which all the nodes are individually connected to other nodes.

ii) It does not need any central switch or hub to control the connectivity among the nodes

iii) Mesh topology is categorised in two parts :

a) Fully connected - all the nodes are connected to each other.

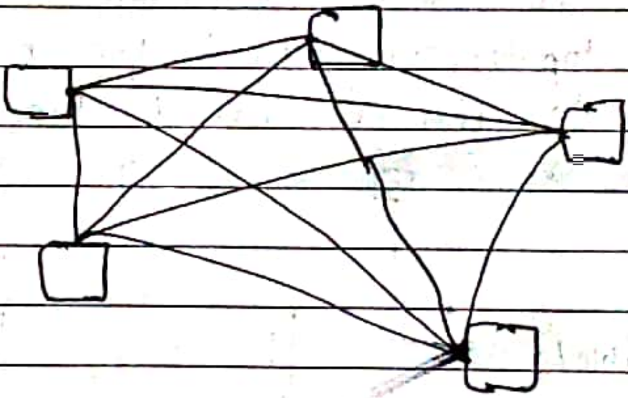
b) Partially connected - all the nodes are not connected to each other.

iv)

iv) It is robust as a failure in one cable will only disconnect the specific computer connected to this cable.

v) Mesh topology is rarely used as installation and configuration are difficult when connectivity gets more.

vi) Cabling cost is high as it requires bulk ~~wiring~~ wiring.



Mesh Topology

5) Tree :-

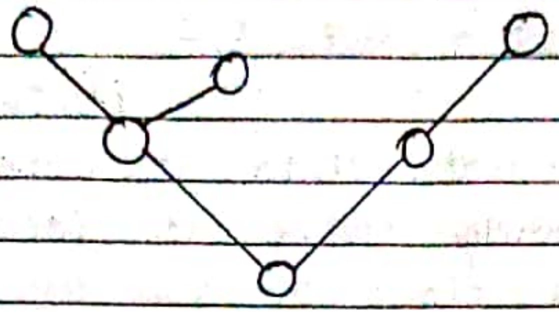
i) It is a combination of star and bus topology. It is also known as expanded star topology.

ii) In tree topology, all the star networks are connected to a single bus.

iii) Ethernet protocol is used in this topology.

iv) In this, the whole network is divided into segments known as star networks which can be easily maintained. If one segment is damaged, there is no effect on other segments.

v) Tree topology depands on the "main bus" and if it breaks, then the whole network got damaged.



Tree topology

6) Hybrid-

i) A Hybrid topology is a combination of diffrent topologies to form a resulting topology.

ii) If star topology is connected to with another star topology, then it remains a star topology. If star topology is connected with diffrent topology, then it becomes a hybrid topology.

iii) It provides flexibility as it can be implemented in a diffrent network environment.

—x—

IMP Different types of Networks-

Network can be divided on the basis of area of distribution. For example-

1) PAN (Personal Area Network)-

its range limit is upto 10 meters. It is created for personal use. Generally personal devices are connected to this network. For example- computers, telephones, fax, printers, etc.

2) LAN (Local Area Network)- It is used for small geographical location like - office, hospital, schools, etc.

Date
Page

3) **HAN (House Area Network)** - It is actually a LAN that is used within a house and used to connect homely devices like personal computers, phones, printers, etc.

4) **CAN (campus Area Network)** - It is a connection of devices within a campus area which links to other departments of the organisation within the same campus.

5) **MAN (Metropoliton Area Network)** - It is used to connect the devices which span to large cities like metropolitan cities over a wide geographical area.

6) **WAN (Wide Area Network)** - It is used over a wide geographical location that may range to connect cities and countries.

7) **GAN (Global Area Network)** - It uses satellites to connect devices over the global area.

Que- 2. What is VPN ? Write down Advantages, disadvantages, and types of VPN.

Date
Page

VPN (Virtual Private Network):-

VPN stands for "Virtual Private Network" and describes the opportunity to establish a protected network connection when using public networks. VPNs encrypt your internet traffic and disguise your online identity. This makes it more difficult for third parties to track your activities online and steal data. The encryption takes place in real time.

Working of VPN -

A VPN hides your IP address by letting the network redirect it through a specially configured remote server run by a VPN host. This means if you surf online with a VPN, the VPN Server becomes the source of your data. That means your Internet Service Provider (ISP) and other third parties cannot see which websites you visit or what data you send and receive online. A VPN works like a filter that turns all your data into "gibberish". Even if someone were to get their hands on your data, it would be useless.

Advantages -

1) VPN is used to connect offices in different geographical locations remotely and is cheaper ~~tha~~ when compared to WAN connections.

2) VPN is used for secure transactions and confidential data transfer between multiple offices located in different geographical locations.

3) VPN keeps an organisation's information secured against any potential threats or intrusions by using virtualization.

5) .

4) VPN encrypts the internet traffic and disguse the online identity.

Types of VPN:-

1) Access VPN → Access VPN is used to provide connectivity to remote mobile users and telecommuters. It serves as an alternative to dial-up connections or ISDN (Integrated Services Digital Network) connections. It is a low-cost solution and provides a wide range of connectivity.

2) Site-to-Site VPN → A site-to-site or router-to-router VPN is commonly used in large companies having branches in different locations to connect the network of one office to another in different locations.

2 sub categories-

A) Intranet VPN :- It is useful for connecting remote offices in different geographic locations using shared infrastructure (internet connectivity and servers) with the same accessibility policies as a private WAN (Wide Area Network).

B) Extranet VPN :- Extranet VPN uses shared infrastru over an internet, suppliers, customers, partners, and other entities and connect them using dedicated connections.

Disadvantages :-

1) **Slowdown the internet speed :-** Sometimes when you use a VPN you can notice a speed reduction. This is because of the data encryption. Since the data in encrypted in VPN, it has to travel more than usual.

2) **Costs more money :-** Despite there are plenty of free VPN services available. Many of them don't offer the Complete protection needed by the user. Moreover using them is not a reliable option. Hence you need to go for a paid VPN service for enjoying a full complete protection.

3) **Device Compatibility :-** VPNs generally support most of the devices and the operating systems. There are some platforms those are not supported. This is because these platforms are not widely used. In this case if you want to use VPN in such platform, you have to manually setup a VPN connection.

4) **Privacy Issues :-** VPNs are meant to provide you the complete protection but there are some VPN services that can potentially be a threat. Especially the VPN (free VPN) services with no properly configured encryption. Moreover there are chances where these VPNs can sell your data to third party companies.

MAC - Media Access Control
IP - Internet Protocol

IPv4 vs IPv6 ✓
MAC vs IP ✓

What is MAC address & and IP address? What is the difference between them?

07) IP address, Private IP address, Public IP address, APIPA

Que-3 MAC Address :-

MAC Address is the physical address, which uniquely identifies each device on a given network. It is a unique 48-bits hardware number of a computer, which is embedded into network card (Network Interface Card / NIC) during the time of manufacturing.

IP Address :-

i) It is an unique address assigned to each device in an IP network.

ii) ISP assigns IP address to all the devices present on its network.

iii) Computing devices use IP address to identify and communicate with other devices in the IP network.

Difference between private and public IP Address -

i) Private IP address is used to communicate within the same network. Using IP data or information can be sent or received within the same network.

ii) Public IP address is used to communicate outside the network. Public IP address basically assigned by the ISP (Internet Service Provider).

Types → Static and dynamic

Based on Accessibility → Private and Public

Proper differences :-

Private IP Address	Public IP Address
i) Scope is local.	i) Scope is global.
ii) It is used to communicate within the network.	ii) It is used to communicate outside the network.
iii) Private IP addresses of the systems connected in a network	iii) Public IP may differ in uniform or non-uniform manner.
✓iv) It works only in LAN.	iv) It is used to get Internet service.
v) It is used to load network operating system.	v) It is controlled by ISP.
vi) It is available in free of cost.	vi) It is not free of cost.
✓vii) Private IP can be known by entering "ipconfig" on command prompt.	vii) Public IP can be Known by searching "What is my IP" on google.
✓viii) Range : 10.0.0.0 - 10.255.255.255 172.16.0.0 - 172.31.255.255 192.168.0.0 - 192.168.255.255	viii) Range : Besides Private IP addresses rest are Public
✓ix) Example - 192.168.1.10	ix) Example - 17.5.7.8

→ MAC address handles the physical ~~address~~ connection from computer to computer while IP address handles the logical routable connection from both computer to computer and network to network.

Automatic Private IP Addressing (APIPA) :-

APIPA stands for Automatic Private IP Addressing. It is a feature or characteristic in operating systems (eg. windows) which enables computers to self-configure an IP address and subnet mask automatically when their DHCP (Dynamic Host Configuration Protocol) server isn't reachable. The IP address range for APIPA is (169.254.0.1 to 169.254.255.254) having 65, 534 usable IP addresses, with the subnet mask of 255.255.0.0.

Que-4 MAC Address and IP Address :-

i) Both MAC address and IP address are used to uniquely define a device on the internet. NIC Card's manufacturer provides the MAC Address, on the other hand Internet Service Providers Provides IP address.

NIC → MAC
ISP → IP

ii) The main difference between MAC and IP address is that MAC address is used to ensure the physical address of a computer. It uniquely identifies the devices on a network. While IP addresses are used to uniquely ~~identify~~ identify the connection of a network with that device taking part in a network.

MAC → Physical Address → NIC
IP → logical Address → ISP

$$\xleftrightarrow{\text{IP}}$$

$\boxed{\text{Network Id} + \text{Host Id}}$

Que-5

- IPV4 and IPV6 + Difference between them

IPV4 :-

IPV4 is a version 4 of IP Address. It is a current version and the most commonly used IP Address. It is a 32-bit address written in four numbers seperated by 'dot', i.e., periods. This address is unique for each device.

Example- 66.94.24.13

IPV6 :-

IPV4 produces 4 billion addresses, and the developers think that these addresses are enough, but they were wrong. IPV6 is the next generation of IP addresses. It is a 128-bit hexadecimal address. IPV6 provides a large address space, and it contains a simple header as compare to IPV4.

	IPV4	IPV6
i)	32-bit address	i) 128- bit address
ii)	5 different Classes - class A, class B, class C, class D, E	ii) does not contain classes
		US: 1 followed by 36 zero → British: 1 followed by 66 zero
iii)	It generates 4B unique address.	iii) 340 undecillion unique add.
iv)	In IPV4, end-to-end ~~encrypt~~ connection integrity is un achievable.	iv) Achievable
v)	does not provide encryption and authentication.	v) provides encryption and authentication

Date ______
Page ______

Que-6 Q. What is Bandwidth, node, and link

Answer -

Bandwidth :-

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, KBs, MBs or GBs. ~~that can be transmitted ?~~

Node and link :-

A network is a connection setup of two or more computers directly connected by some physical mediums like optical fibre or coaxical cable. This physical medium is known as ~~a~~ link, and the computers that it is connected to are known as nodes.

Que-7 Explain TCP model.

TCP / IP Reference Model :-

It is a compressed version of the OSI model with only 4 layers. It was developed by the US Department of Defence (DoD) in the 1860s. The name of the model is based on 2 standard protocols used i.e, TCP (Transmission Control Protocol) and IP (Internet Protocol).

~~4 Layers:-~~

~~1) Link layer :- Decides which links such as serial lines or classical ethernet must be used to meet the needs of the connectionless internet layers.~~
~~Ex- Sonet, Ethernet.~~

~~2) Internet layer :-~~

✓ It contains 4 layers → ① Host to network ② Internet ③ Transport ④ Application

1) **Host - to - network Layer :-** This is the lowest layer that is concerned with the physical transmission of data. TCP/IP does not specifically define any protocol here but supports all the standard protocols.
Ex- Sonet, Ethernet

2) **Internet layer :-** It defines the protocols for logical transmission of data over the network. The main protocol in this layer is IP (Internet protocol) and it is supported by the protocols ICMP, IGMP, RARP, and ARP.

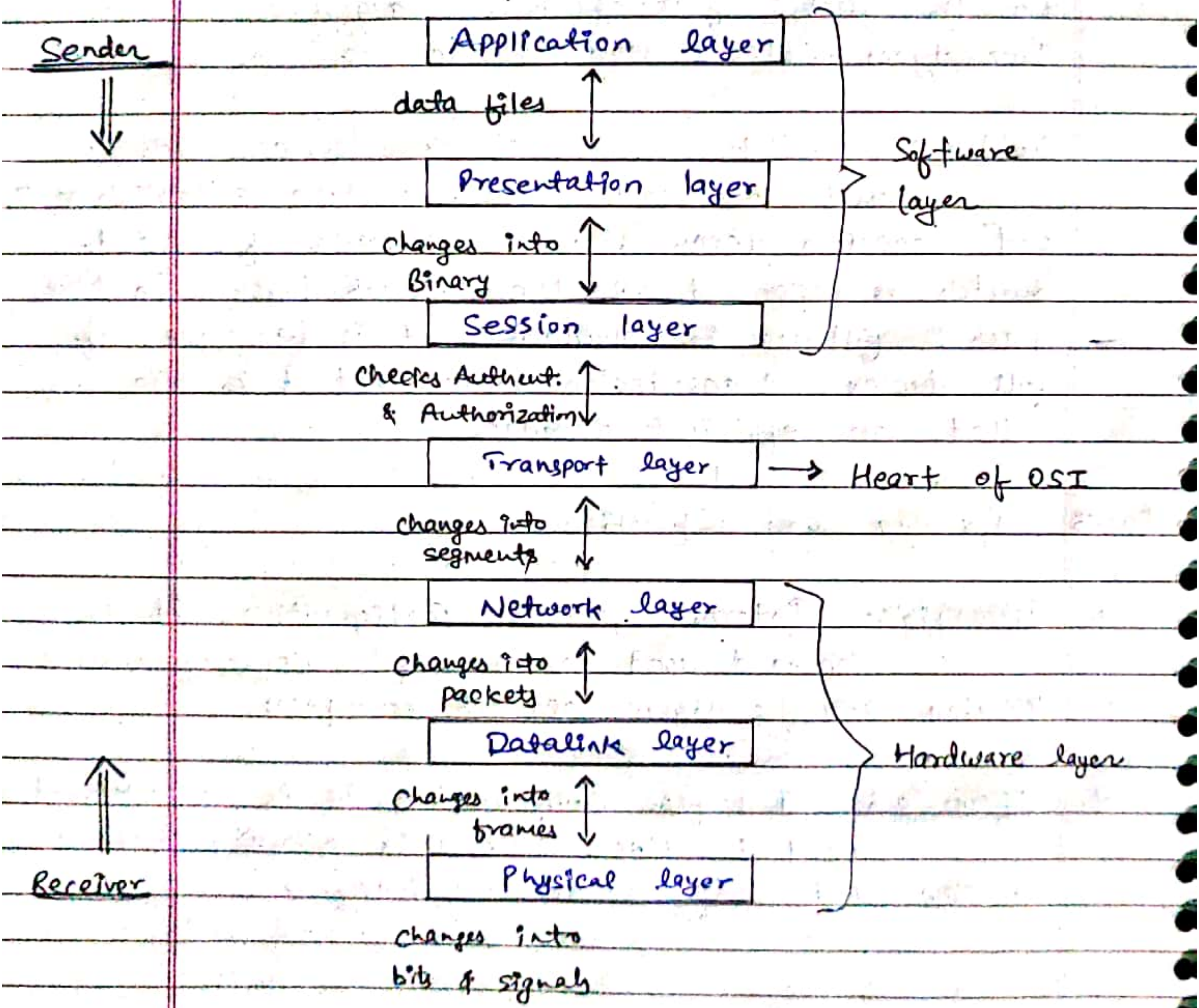
3) **Transport layer :-** It is responsible for error-free and end-to-end delivery of data. The protocols defined here are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).

4) **Application layer** :- It is responsible for node-to-node communication and controls user interface specifications. It contains all the higher level protocols. Ex- HTTP, SMTP, RTP, DNS.

Note→ each layer is the packages of some protocols.

OSI model :-

OSI stands for " Open System Interconnection". It has been developed by ISO (International Organization of Standarization). It is a 7 layer architecture by which message transmits from sender to receiver.



→ Please Do Not Tell Secret Password Anyone

Please ↓ physical
Do ↓ datalink
Not ↓ Network
Tell ↓ Transport
Secret ↓ Session
Password ↓ Presentation
Anyone ↓ Application

1) **Application layer :-**

It is a type of layer which consists of application layer protocol which allow network applications (i.e. those application which uses internet) to work correctly in network.

For exomple-

(File Transfer Pro.) FTP → for file transfer

HTTP/ HTTPS → for web surfing

SMTP → for emails

TELNET(Telecommunication network) → for virtual terminals

2) **Presentation layer :-**

Presentation layer receives data from application layer those are in form of characters and numbers. Presentation layer converts those characters and numbers to machine understandable binary format. (EX→ ASCII --- 101110101)

This function of presentation layer is called translation.

Before data is transmitted presentation layer reduces the number of bits that are used to represent the original data. This bit reduction process is called Data compression.

To maintain the integrity of data before transmission, Data is encrypted. SSL (Secure soket layer) is used in presentation layer for data encrption and decryption.

Thus, presentation layer performs three functions-

1. Translation 2. Data Compression
3. Encryption/ Decryption

→ session management

3) Session layer :- → Authentication & Authorization

Session layer helps in setting up and managing connections enabling sending and receiving of data followed by termination of connections or sessions. session layer has its own ~~API~~ helpers called APIs (Application Programming Interfaces). NETBIOS (Network Basic Output System) is an example of APIs which allow application on different computer to communicate ~~to~~ with each - other.

Just before a session/ connection is established with a server, server performs a function called Authentication (It is the process of verifying : who you are?). After authenticating a user, Authorization (It is the process used by server to determine if you have permission to access or not) is checked.

Session layer also helps in session management.

4) Transport layer :-

The layer below session layer is called transport layer. Transport layer controls the reliability of communication through flow control, error control and segmentation.

Tranport layer protocols are TCP and UDP.

Transport layer have 2 types of services

A) Connection - oriented Transmission → TCP

B) Connectionless transmission → UDP

5) Network layer :-

Transport ~~Network~~ layer sends data segments to the network layer. Network layer works for the transmission of the received data segments from one computer to another located in different locations. Data units in Network layer is called Data - Packets.

The function of Network layer are:

A) Logical Addressing → IP addressing done here

B) Routing → method to move data packets source to dest.

C) Path Determination → finds the best optimal path from source to destination for transm.

6) Data-link Layer :-

Data-link layer receives the data from network layer and converts the data into data frames. and then attaches the physical address to these frames which will be further sent to physical layer.

MAC

Functions:

A) Frame synchronization B) Error detection

C) Addressing (physical)

7) Physical Layer :-

It changes the received data from datalink layer to signals and signals to media.

→ { Actual message
file (audio, video, HTML)

Que-9 Define gateway, difference between gateway and router.

A node that is connected to two or more networks is ~~called~~ commonly known as gateway. It is also known as router. It is used to forward messages from one network to another.

Both the gateway and router regulate the traffic in the network. ~~Differences Between gateway~~

Difference between gateway and router :-

A router sends the data between two similar networks while gateway sends the data between two dissimilar networks.

Que-10 What does "Ping" command do ?

The "Ping" command is a Command Prompt command used to test the ability of the source computer to reach a specified destination computer.

It is usually used as a simple way to verify that a computer can communicate over the network with another computer or network devices.

Que-11 What is DNS, DNS forwarder, NIC ?

Imp 1) DNS :-

i) DNS is an acronym that stands for Domain Name systems. DNS was introduced by Paul Mockapetris and Jon Postel in 1983.

~~ii) It is an naming system for all the resources over the internet which includes physical nodes and applications. It is used to locate resources easily over a network.~~

iii) DNS is an internet which maps the domain names to their associated IP addresses.

DNS→ DNS translates human readable domain names (ex- amazon.com) to machine readable IP address (ex- 192.0.2.40)

iv) without DNS, users must know the IP address of the web page that you wanted to access.

IMP

2) **Working of DNS :-**

If you want to visit the website of "Shaurya", then the user will type "https://www.shaurya.com" into the address bar of the web browser. Once the domain name is entered, then the Domain name systems will translate the domain name into the ip address which can be easily interpreted by the computer. Using the IP address, the computer can locate the web page requested by the user.

3) **DNS Forwarder :-** A forwarder is used with a DNS server when it receives DNS queries that cannot be resolved quickly. So it forwards those requests to external DNS servers for resolution. A DNS server which is configured as a forwarder will behave differently than the DNS server which is not configured as a forwarder.

IMP

4) **NIC :-** NIC stands for Network Interface Card. It is a peripheral card attached to the PC to connect to a network. Every NIC has its own MAC address that identifies the PC on the network. It provides a wireless connection to a local area network. NICs were mainly used in desktop computers.

Que-12 What is subnet?

Subnet :-

A subnet is a network inside a network achieved by the process called subnetting which helps divide a network into subnets. It is used for getting a higher routing efficiency and enhances the security of the network. It reduces the time to extract the host address from the routing table.

Que-13 What is firewall?

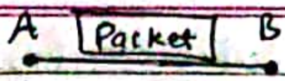
Firewall :-

The firewall is a network security system that is used to monitor the incoming and outgoing traffic and blocks the same based on the firewall security policies. It acts as a wall between the internet (public network) and the networking devices (a private network). It is either a hardware device, software program, or a combination of both. It adds a layer of security to the network.

Que-14 What are the different types of network delays?

Network delay :-

Network delay refers to the amount of time it takes for a packet to go from point A to point B. If point A is source and point B is destination, then the delay is called

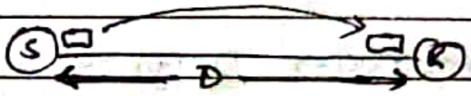


an end to end delay. time = ?

The types of delays encountered in a packet-switched network are:

1) Propagation delay 2) Transmission delay
3) Queuing delay 4) Processing delay

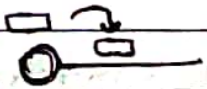
1) Propagation Delay :-



It is the time that it takes for a bit to reach from one end of a link to another. The delay depends on the distance (D) between the sender and the receiver, and the propagation speed (S) of the wave signal. It is calculated as:

$$\text{Propagation delay} = \frac{D}{S} \quad \begin{matrix}(\text{distance}) \\ (\text{speed})\end{matrix}$$

2) Transmission Delay :-

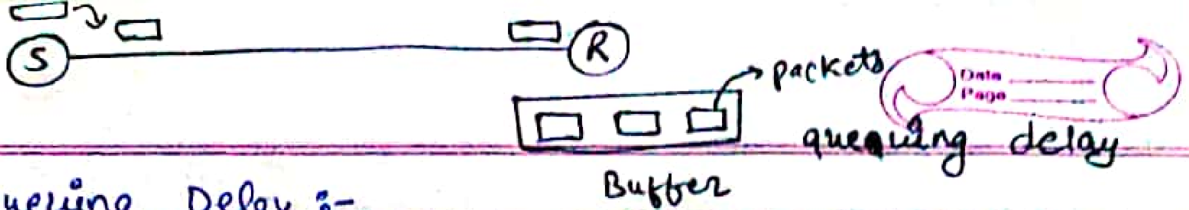


time taken to put packet on outgoing link

[It refers to the time it takes to transmit a data packet onto the outgoing link.] The delay is determined by the size of the packet and the capacity of the outgoing link.

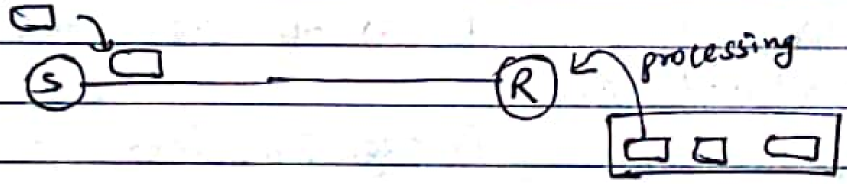
If a packet consists of L bits and the link has a capacity of B bits per second, then the transmission delay is equals to :

$$\frac{L}{B}$$



3) Queuing Delay :- It refers to the time that a packet waits to be processed in the buffer ~~of~~ of a switch. The delay is dependent on the arrival rate of the incoming packets, the transmission capacity of the outgoing link, and the nature of the network's traffic.

4) Processing Delay :- It is the time taken by a switch to process the packet header. The delay depends on the processing speed of the switch.



Que-15 3 way handshaking

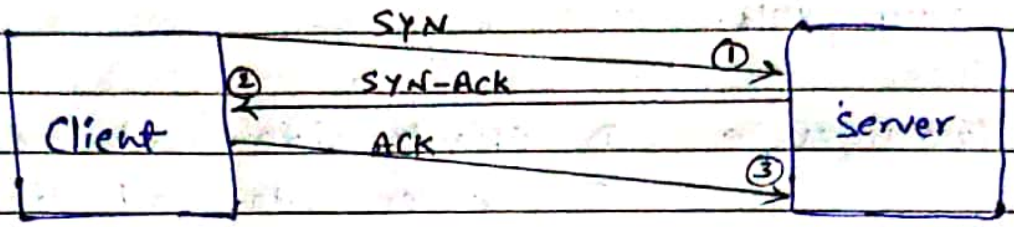
reliable ⊝ TCP 3-way Handshaking (SYN, SYN-ACK, ACK) :-

Three-way handshake or a TCP 3-way handshake is a process which is used in TCP/IP network to make a connection between the server and client.

It is a three-step process that requires both the client and server to exchange synchronization and acknowledgement packets before the real data communication process starts.

TcP three-way handshake process :-

In this TCP - handshake process, a client needs to initiate the conversation by requesting a communication session with the server :



Step-1 (SYN)→ In the first step, client wants to establish a connection with server, so it sends a segment with SYN (synchronize sequence number) which informs server that client is likely to start communication and with what sequence number it starts segments with.

Step-2 (SYN+ACK)→ In the second step, server responds to the client request with SYN-ACK signal set. ACK helps you to signify the response of segment that is received and SYN signifies what sequence number it should able to start with the segments.

Step-3 (ACK)→ In the final step, the client acknowledges the response, and then they both create a stable connection.

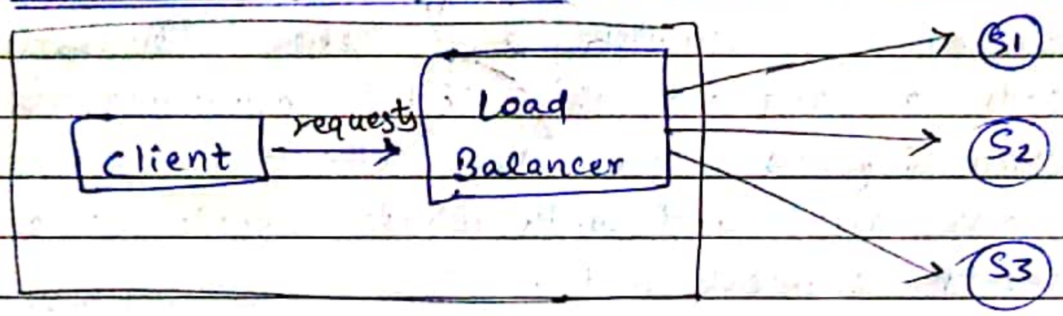
Que-16 Load Balancer ? ~~Client~~ and server side load balancer ?

Date
Page

Load Balancing :- Load balancing refers to efficiently distributing incoming network traffic across a group of backend servers, also known as server farm or server pools.

Two types → ① Client side load balancer
② server side load balancer

② ~~Client~~ side load balancer :-



Server-side load Balancer

Server-side load balancer is a ~~classi~~ classical load balancer. The traffic is distributed by a load distributor placed in front of the servers and distributed to the servers that will perform the main work equally or according to the certain rules.

Ex- Most common used server side load balancers nginx, netscaler etc.

Que-17 RSA Algorithm and How it works?

Encryption <
- Symmetric → one key for both (Encryp. and decryp.)
- Asymmetric → [public key → encryp. & private → decryp.]

RSA Algorithm :-

The RSA algorithm is an asymmetric cryptography algorithm. This means that it uses a public key and a private key (i.e two different, mathematically linked keys). As their names suggests, a public key is shared publicly, while a private key is secret and must not be shared with anyone.

The RSA algorithm is named after those who invented it in 1978 : Ron Rivest, Adi Shamir, and Leonard Adleman.

How it works :-

1. Generating the keys
2. Encryption
3. Decryption

Que-18 What is HTTP and HTTPS protocol ?

HTTP :-

HTTP is the Hyper Text Transfer Protocol which defines the set of rules and standards on how the information can be transmitted on world wide web (WWW). It helps the web browsers and web servers for communication. It is a 'Stateless Protocol' where each command is independent with respect to the previous command. HTTP is an Application layer protocol built upon the TCP. It uses port 80 by default.

HTTPS :-

HTTPS is the HyperText Transfer Protocol secure or secure HTTP. It is an advanced and secured version of HTTP. On top of HTTP, SSL / TLS protocol is used to provide security. It enables secure transaction by encrypting the communication and also helps identify ~~the~~ network servers securely. It uses port 443 by default.

Que-19 What is SMTP Protocol?

SMTP protocol :- SMTP is the Simple Mail Transfer Protocol. SMTP sets the rule for communication between servers. These set of rules help the software to transmit emails over the internet. It supports both End-to-End and Store-and-Forward methods. It is in always listening mode on port 25.

Que-20 What are TCP and UDP protocol? Prepare differences between TCP and UDP protocol?

3-way handshake

TCP Protocol :- The TCP stands for Transmission Control Protocol. If we want the Communication between two computers and communicatio should be good and reliable then we use TCP protocol.

Ex- If we want to view a web page, then we expect that nothing should be missing on webpage. In this case we should use TCP protocol.

UDP Protocol :-

The UDP stands for User Datagram Protocol. Its working is similar to ~~UDP~~ TCP as it is also used for sending and receiving the message. The main difference is that UDP is a connectionless protocol. Here, connectionless means that no connection establishes prior to communication. It does not guarantee the delivery of data packets. It does not eren care whether the data has been received on the receiver's end or not, so it is also known as the " fire - and - forget" protocol.

UDP is faster than TCP as it does not provide the assurance for the delivery of the packets.

key point differences -> both are transport layer proto.

		TCP	UDP
1.	Type of proto.	connection-oriented	connectionless
2.	Reliability	Reliable	Unreliable
3.	Speed	Slower than UDP	Faster

4. Flow of data]

TCP provides the full-duplex service means data can flow in both directions. On the other hend, UDP is mainly suitable for the unidirectional flow of data.

5. Applications:- TCP is mainly used where a secure and reliable communication process is required, like military service, web browsing and e-mails. whereas UDP is used where fast communication is required and does not care about the reliability like game Streaming, music or video Streaming, etc.

VIP

Que-21 What happens when you enter google.com in the web browser?

steps:-

1) Check the browser cache first if the content is fresh and present in the cache display the same.

2) If not, the browser ~~checks~~ checks if the IP of the URL is present in the cache (browser and OS) if not then requests the OS to do a DNS lookup using UDP to get the corresponding IP address of the URL from the DNS server to establish a new TCP connection.

3) A new TCP connection is set between the browser and the server using three-way handshaking.

4) An HTTP request is ~~sent~~ sent to the server using the TCP connection.

5) The web servers running on the servers handle the incoming HTTP request and sent the HTTP response.

6) The browser processes the HTTP response sent by the server and may close the TCP connection or reuse the same for future requests.

7) If the response data is cacheable then browsers cache the same.

8) Browser decodes the response and renders the content.

Date ____
Page ____

Que-22 Hub vs switch

Hub :- Hub is a networking device which is used to transmit the signal to each port (except one port) to respond from which the signal was received. Hub is operated on a physical layer. In this packet filtering is not available.
Two types - Active Hub, passive hub

Switch :- Switch is a network device which is used to enable the connection establishment and connection termination on the basis of need. Switch is operated on the datalink layer. In this packet filtering is available. It is a type of full duplex transmission mode and it is also called an efficient bridge.

Que-23 Ipconfig and Ifconfig

1. **Ipconfig** :- Internet protocol Configuration, it is a command used in Microsoft operating systems to view and configure network Interfaces.

2. **Ifconfig** :- Interface Configuration, It is a command used in MAC, Linux, Unix operating systems to view and configure network interfaces.