Day1

Q1. OSI Model

OSI stands for Open Systems Interconnection. It has been developed by ISO – ‘International Organization for 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.

1. physical layer

a. commucation using cable

b. frame to light signal / line coding

2. datalink layer

a.error correction

b.flow control

c. packet to frame

d. 2 part

1.LLC logical link control- identify network protocal, perform error chacking , sync frame

2. MAC Media Access Control- Identify device

3. networklayer

a. find best path for routing

b. segment to packet

c. ip assign in this layer

4.transport layer

a. data to segment

b. port work in this layer

5. session layer

a. create a commucation channel.

5. session layer

a. create a commucation channel.

6. presention layer

a. encrypt and dyceret data before sending

7. application layer

a. end use user use it

Q2. TCP/IP Model

Same as OSI but it use 5 layer all application, presentation and session layer are in one layer called application layer.

This layer actually work on internet network.

Q3. What is computer network.

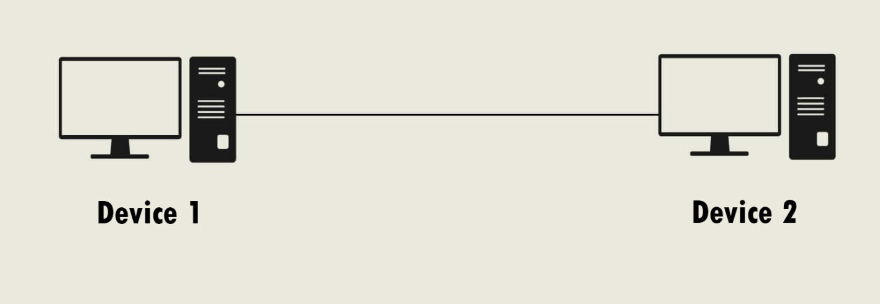
A computer network is a set of computers sharing resources located on or provided by network nodes. Computers use common communication protocols over digital interconnections to communicate with each other.

Q4. Network topology.

Topology defines the structure of the network of how all the components are interconnected to each other.

1. **Point to point**

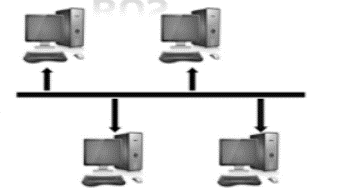
In this network topology one device directly connect with another one device directly with point to point connection.



1. **Bus**

The bus topology is designed in such a way that all the stations are connected through a single cable known as a backbone cable.

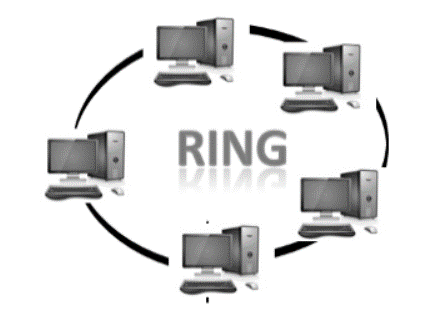
When a node wants to send a message over the network, it puts a message over the network. All the stations available in the network will receive the message whether it has been addressed or not.



1. **Ring**

In ring topology all devices connected with nearest device and make a ring like structure.

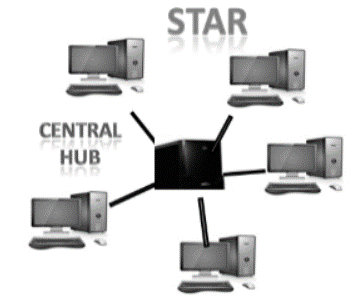
The node that receives the message from the previous computer will retransmit to the next node.



1. **Star**

Star topology is an arrangement of the network in which every node is connected to the central hub, switch or a central computer.

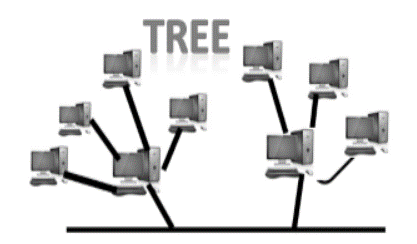
The central computer is known as a server, and the peripheral devices attached to the server are known as clients.



1. **Tree**

Tree topology combines the characteristics of bus topology and star topology.

A tree topology is a type of structure in which all the computers are connected with each other in hierarchical fashion.



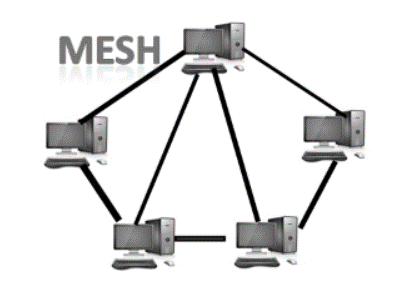
1. **Mesh**

Mesh technology is an arrangement of the network in which computers are interconnected with each other through various redundant connections.

There are multiple paths from one computer to another computer.

It does not contain the switch, hub or any central computer which acts as a central point of communication.

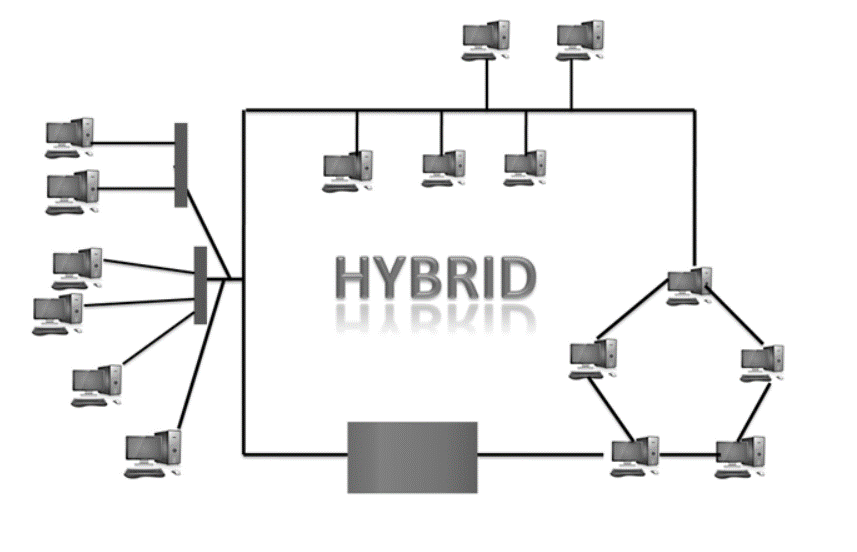
The Internet is an example of the mesh topology.



1. **Hybrid**

The combination of various different topologies is known as Hybrid topology.

A Hybrid topology is a connection between different links and nodes to transfer the data.



Q5. What is LAN, MAN, WAN.

|  |  |  |  |
| --- | --- | --- | --- |
| S No. | LAN | MAN | WAN |
| 1 | LAN is defined as a computer network that links the local areas like schools, universities, organizations, etc. | On the other hand, MAN is defined as a computer network that links the metropolitan areas. | On the other hand, WAN is defined as the telecommunications network that covers a large geographical area. |
| 3 | The full form of the LAN is Local Area Network. | The full form of MAN is Metropolitan Area Network. | The full form of WAN is a Wide Area Network. |
| 4 | LAN is a wired network, i.e., all the computers and printers are connected through wires. | The connections in MAN are connected through modem or cables/ wires. | The network of WAN is connected through broadband services, 3G or 4G internet services, etc. |
| 5 | The ownership of LAN is private | The ownership of MAN might be public or private. | The ownership of WAN might be private or public. |
| 6 | The internet speed of LAN is very high, i.e., 1000 Mbps. | The sped of MAN is moderate, i.e., 44-155 Mbps. | The speed of WAN is relatively less than MAN and LAN, i.e., 150 Mbps. |
| 7 | The maintenance cost of LAN is easy. | The maintenance cost of MAN is difficult. | The maintenance cost of WAN is difficult. |
| 9 | The bandwidth of LAN is high. | The bandwidth of MAN is less | The bandwidth of WAN is relatively low. |

Q6. Class of IP v4

A 1-126 N.H.H.H 126 16777214

B 128-191 N.N.H.H 16.384 65534

C 192-223 N.N.N.H 2097152 254

D 224-239 multicasting

E 240-254 experiment

Note- 127.0.0.0 to 127.255.255.255 canot be use it reserver for loopback testing .

Day 2

**Q1. PORT**

Port 20: FTP (File Transfer Protocol) - Data

Port 21: FTP (File Transfer Protocol) - Control

Port 22: SSH (Secure Shell)

Port 23: Telnet

Port 25: SMTP (Simple Mail Transfer Protocol)

Port 53: DNS (Domain Name System)

Port 67: DHCP (Dynamic Host Configuration Protocol) - Server

Port 68: DHCP (Dynamic Host Configuration Protocol) - Client

Port 69: TFTP (Trivial File Transfer Protocol)

Port 80: HTTP (Hypertext Transfer Protocol)

Port 110: POP3 (Post Office Protocol version 3)

Port 119: NNTP (Network News Transfer Protocol)

Port 123: NTP (Network Time Protocol)

Port 137: NetBIOS Name Service

Port 138: NetBIOS Datagram Service

Port 139: NetBIOS Session Service

Port 143: IMAP (Internet Message Access Protocol)

Port 161: SNMP (Simple Network Management Protocol)

Port 179: BGP (Border Gateway Protocol)

Port 194: IRC (Internet Relay Chat)

Port 443: HTTPS (HTTP Secure)

Port 465: SMTP over SSL/TLS

Port 514: Syslog

Port 520: RIP (Routing Information Protocol)

Port 546: DHCPv6 (Dynamic Host Configuration Protocol for IPv6) - Client

Port 547: DHCPv6 (Dynamic Host Configuration Protocol for IPv6) - Server

Port 587: SMTP (Simple Mail Transfer Protocol) - Submission

Port 631: IPP (Internet Printing Protocol)

Port 636: LDAPS (LDAP over SSL/TLS)

Port 993: IMAPS (IMAP over SSL/TLS)

Port 995: POP3S (POP3 over SSL/TLS)

Port 1433: Microsoft SQL Server

Port 1434: Microsoft SQL Server Monitor

Port 1521: Oracle database default listener

Port 1723: PPTP (Point-to-Point Tunneling Protocol)

Port 1812: RADIUS (Remote Authentication Dial-In User Service)

Port 1813: RADIUS Accounting

Port 2049: NFS (Network File System)

Port 2181: ZooKeeper

Port 2222: SSH (Secure Shell) - alternative

Port 3306: MySQL database

Port 3389: RDP (Remote Desktop Protocol)

Port 3690: SVN (Subversion)

Port 4444: Metasploit

Port 5000: UPnP (Universal Plug and Play)

Port 5060: SIP (Session Initiation Protocol)

Port 5432: PostgreSQL database

Port 5900: VNC (Virtual Network Computing)

Port 6667: IRC (Internet Relay Chat) - alternative

Port 8080: HTTP Proxy

Q2. Network Device

Network devices, also known as networking hardware, are physical devices that allow hardware on a computer network to communicate and interact with one another. For example Repeater, Hub, Bridge, Switch, Routers, Gateway, Brouter, and NIC, etc.

**Repeater** – A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted to extend the length to which the signal can be transmitted over the same network. An important point to be noted about repeaters is that they not only amplify the signal but also regenerate it. When the signal becomes weak, they copy it bit by bit and regenerate it at its star topology connectors connecting following the original strength. It is a 2-port device.

**Hub** –  A hub is a basically multi-port repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations.

**Bridge** – A bridge operates at the data link layer. A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of the source and destination. It is also used for interconnecting two LANs working on the same protocol.

**Switch** – A switch is a multiport bridge with a buffer and a design that can boost its efficiency(a large number of ports imply less traffic) and performance. A switch is a data link layer device.

**Gateway** – A gateway, as the name suggests, is a passage to connect two networks that may work upon different networking models. They work as messenger agents that take data from one system, interpret it, and transfer it to another system.

**Brouter** – It is also known as the bridging router is a device that combines features of both bridge and router. It can work either at the data link layer or a network layer.

**NIC**– NIC or network interface card is a network adapter that is used to connect the computer to the network. It is installed in the computer to establish a LAN.

Q3. Network Device Security.

Network security appliances have lots of different jobs. Some manage network traffic, others detect threats, and still others provide secure remote access. Many security devices combine functionality from multiple other devices, especially those that are intended for smaller businesses.

**Firewalls**

Firewalls are one of the most fundamental network security appliances. Like many other security devices, firewalls can come in hardware or software forms.

#### Intrusion Protection Systems (IPS)

Network-based intrusion protection systems proactively monitor all of the traffic going through your network. Using pre-made profiles, signature detection, artificial intelligence, and anomaly detection, IPS systems can detect many kinds of network intrusions, from malware on endpoint devices to denial of service attacks.

#### Network Access Control

Keeping infected or insecurely configured endpoint devices off of the corporate network is critical to security. As a result, network access control devices link network authentication with the state of endpoint devices.

#### Web Application Firewalls (WAF)

Like a regular network firewall, a WAF selectively allows or blocks traffic based on predefined criteria or suspicious activity. Web applications commonly have security vulnerabilities that can be used to compromise a company’s network and leak data. While finding and fixing all of these issues would be the ideal solution, using a web application firewall is a good next layer of defence.

A WAF can block URLs and requests containing suspicious payloads, evidence of SQL injection attempts, and other attacks. They can come in the form of a physical device, a software extension to another network security device, or software installed on a standard reverse proxy server.

#### VPN Gateways

With the rise of remote work, every company needs to ensure that their internal network resources are accessible securely from anywhere. A virtual private network or VPN device can help here. In effect, when employees connect to the VPN, their traffic enters the internal network from the VPN device instead of going straight to the Internet.

In addition to security benefits, VPN gateways give employees access to printers, Intranet sites, and other internal devices, saving time and improving productivity.

Q4. Types of attack.