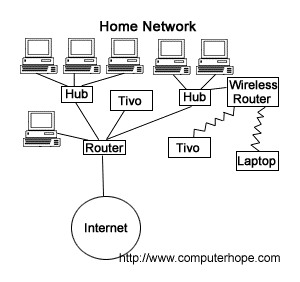
1. What is network?

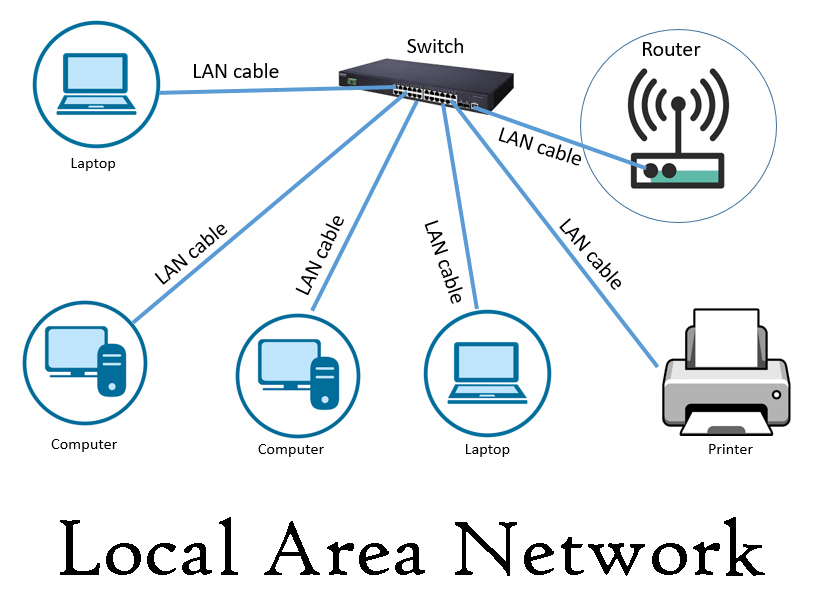
* A network is a collection of computers, servers, mainframes, network devices, peripherals, or other devices connected to allow data sharing. An example of a network is the [Internet](https://www.computerhope.com/jargon/i/internet.htm), which connects millions of people all over the world. To the right is an example image of a home network with multiple computers and other network devices all connected.



1. Explain type of network-- LAN, MAN, WAN?

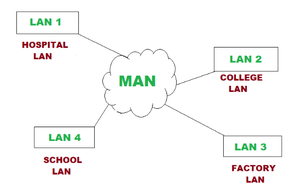
* The **Network** allows computers to **connect and communicate** with different computers via any medium. LAN, MAN, and WAN are the three major types of networks designed to operate over the area they cover. There are some similarities and dissimilarities between them. One of the major differences is the geographical area they cover, i.e. **LAN** covers the smallest area, **MAN** covers an area larger than LAN and **WAN** comprises the largest of all.
* **Local Area Network (LAN) –**

LAN or Local Area Network connects network devices in such a way that personal computers and workstations can share data, tools, and programs. The group of computers and devices are connected together by a switch, or stack of switches, using a private addressing scheme as defined by the TCP/IP protocol. Private addresses are unique in relation to other computers on the local network. Routers are found at the boundary of a LAN, connecting them to the larger WAN.



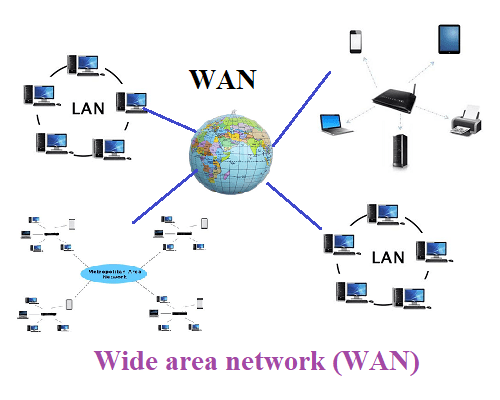
#### Metropolitan Area Network (MAN) –

MAN or Metropolitan area Network covers a larger area than that covered by a LAN and a smaller area as compared to WAN. It connects two or more computers that are apart but reside in the same or different cities. It covers a large geographical area and may serve as an ISP (Internet Service Provider). MAN is designed for customers who need high-speed connectivity. Speeds of MAN range in terms of Mbps. It’s hard to design and maintain a Metropolitan Area Network.



#### Wide Area Network (WAN) –

WAN or Wide Area Network is a computer network that extends over a large geographical area, although it might be confined within the bounds of a state or country. A WAN could be a connection of LAN connecting to other LANs via telephone lines and radio waves and may be limited to an enterprise (a corporation or an organization) or accessible to the public. The technology is high-speed and relatively expensive.



1. What is Internet?

Internet is theforemost important tool and the prominent resource that is being used by almost every person across the globe. It connects millions of computers, webpages, websites, and servers. Using the internet we can send emails, photos, videos, messages to our loved ones. Or in other words, the internet is a widespread interconnected network of computers and electronics devices(that support internet). It creates a communication medium to share and get information online. If your device is connected to the Internet then only you will be able to access all the applications, websites, social media apps, and many more services. Internet nowadays is considered as the fastest medium for sending and receiving information.

1. Define Network Topologies

## Mesh Topology:

In a mesh topology, every device is connected to another device via a particular channel. In Mesh Topology, the protocols used are AHCP (Ad Hoc Configuration Protocols), DHCP (Dynamic Host Configuration Protocol), etc.

Suppose, the N number of devices are connected with each other in a mesh topology, the total number of ports that are required by each device is N-1. In Figure 1, there are 5 devices connected to each other, hence the total number of ports required by each device is 4. The total number of ports required=N\*(N-1).

Suppose, N number of devices are connected with each other in a mesh topology, then the total number of dedicated links required to connect them is NC2 i.e. N(N-1)/2. In Figure 1, there are 5 devices connected to each other, hence the total number of links required is 5\*4/2 = 10.



## Star Topology:

In star topology, all the devices are connected to a single hub through a cable. This hub is the central node and all other nodes are connected to the central node. The hub can be passive in nature i.e., not an intelligent hub such as broadcasting devices, at the same time the hub can be intelligent known as an active hub. Active hubs have repeaters in them. Coaxial cables or RJ-45 cables are used to connect the computers. In Star Topology, many popular Ethernet LAN protocols are used as CD(Collision Detection), CSMA (Carrier Sense Multiple Access), etc.

## Bus Topology:

Bus topology is a network type in which every computer and network device is connected to a single cable. It is bi-directional. It is a multi-point connection and a non-robust topology because if the backbone fails the topology crashes. In Bus Topology, various MAC (Media Access Control) protocols are followed by LAN ethernet connections like TDMA, Pure Aloha, CDMA, Slotted Aloha, etc.



## Ring Topology:

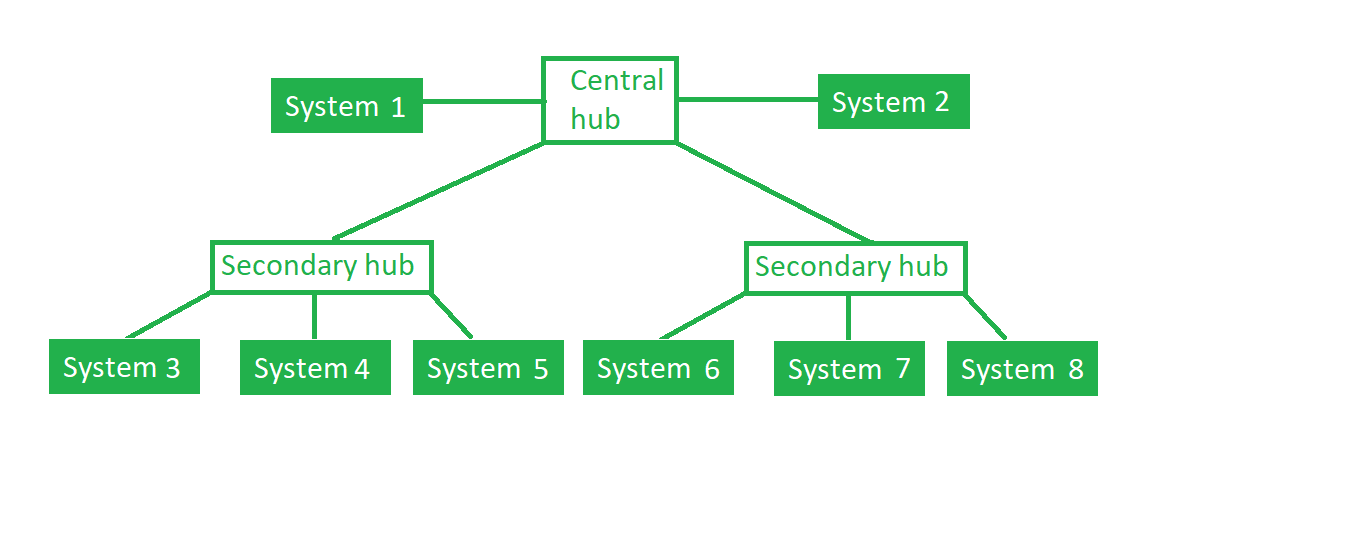
In this topology, it forms a ring connecting devices with exactly two neighboring devices.

A number of repeaters are used for Ring topology with a large number of nodes, because if someone wants to send some data to the last node in the ring topology with 100 nodes, then the data will have to pass through 99 nodes to reach the 100th node. Hence to prevent data loss repeaters are used in the network.

The data flows in one direction, i.e.., it is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called Dual Ring Topology. In-Ring Topology, the Token Ring Passing protocol is used by the workstations to transmit the data.

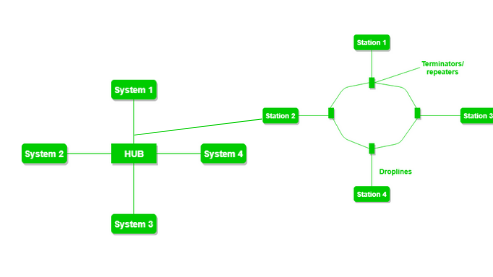
## **Tree Topology :**

This topology is the variation of the Star topology. This topology has a hierarchical flow of data. In Tree Topology, protocols like DHCP and SAC (Standard Automatic Configuration ) are used.

In this, the various secondary hubs are connected to the central hub which contains the repeater. This data flow from top to bottom i.e. from the central hub to the secondary and then to the devices or from bottom to top i.e. devices to the secondary hub and then to the central hub. It is a multi-point connection and a non-robust topology because if the backbone fails the topology crashes.

## Hybrid Topology :

This topological technology is the combination of all the various types of topologies we have studied above. It is used when the nodes are free to take any form. It means these can be individuals such as Ring or Star topology or can be a combination of various types of topologies seen above. Each individual topology uses the protocol that has been discussed earlier.



1. Define list of cables in use of network—Twisted pair , fiber optics

* twisted pair cable

i)Unshilded twisted pair

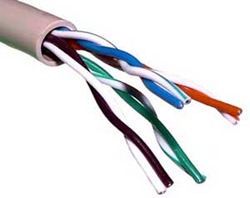
ii)Shilded twisted pair

* coaxial cable
* Fiber optic cable

1)Twisted pair

i)Unshilded twisted pair

UTP stands for Unshielded Twisted Pair cable. UTP cable is a 100 ohm copper cable that consists of 2 to 1800 unshielded twisted pairs surrounded by an outer jacket. They have no metallic shield. This makes the cable small in diameter but unprotected against electrical interference. The twist helps to improve its immunity to electrical noise and EMI.

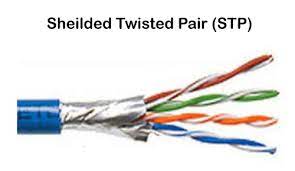


ii) Shilded twisted pair

IBM invented the shielded twisted pair (STP) cable for token ring networks, including two independent wires coated in a foil shielding that prevents electromagnetic interference and speeds up data transmission.

* STP cables are protected with additional foil or copper knitting jackets to help protect cable signals from interference.
* STP cables are more expensive than UTP cables but can transmit data at higher prices over longer distances.
* Electromagnetic interference does not seep out of or into STP cable because of the additional coverage
* Ethernet networks, particularly fast-data-rate Ethernets, frequently use STP cables.
* The efficiency of the additional covering depends on the following features of the shielding substance
  + Frequency
  + Thickness
  + Electromagnetic noise field type
  + Discontinuity in the shield
  + Grounding exercises
* Unlike UTP cables, specific STP cables feature a thick copper braided cover, making the wire thicker, heavier, and thus far more difficult to install.

Other standard STP cables, also known as *foil twisted-pair cables* or *screened twisted-pair cables*, have a minor outer foil barrier. These cables are thinner and less expensive than braided STP cables, but they're also more challenging to install. These thinner cables may be torn during the installation procedure unless the maximum pulling tension and minimum bend radius are appropriately adhered to.



1. Straight cable standard sequence 568 A and 568 B
2. What is fiber optics module and fiber connector

A fiber-optic module is a component that is used to connect a **[fiber-optic cable](https://www.easytechjunkie.com/what-is-a-fiber-optic-cable.htm)** to an electronic device. There are a number of different parts of a fiber-optic module, and different modules are designed with different specifications. The parts of the module are attached to a board which can be installed as a single unit in an electronic device.

The basic parts of a fiber-optic module include a [**transceiver**](https://www.easytechjunkie.com/what-is-a-transceiver.htm), a place for the fiber-optic cable to connect to the module, and a place for the module to connect to the electronic device in which it is being installed. A basic input/output system (BIOS), which is a small computer chip, is standard in a fiber-optic module. The BIOS allows the module to identify its components and transmit information back and forth between the module and the electronic device.

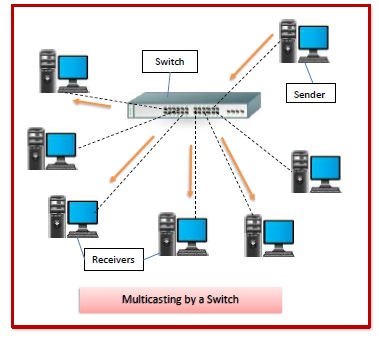
Fiber connector

An optical fiber connector is a flexible device that connects fiber cables requiring a quick connection and disconnection. Optical fibers terminate fiber-optic connections to fiber equipment or join two fiber connections without splicing. Hundreds of optical fiber connector types are available, but the key differentiator is defined by the mechanical coupling techniques and dimensions. Optical fiber connectors ensure stable connections, as they ensure the fiber ends are optically smooth and the end-to-end positions are properly aligned.

An optical fiber connector is also known as a fiber optic connector.

1. Explain Switch

Switches are networking devices operating at layer 2 or a data link layer of the OSI model. They connect devices in a network and use packet switching to send, receive or forward data packets or data frames over the network.

A switch has many ports, to which computers are plugged in. When a data frame arrives at any port of a network switch, it examines the destination address, performs necessary checks and sends the frame to the corresponding device(s).It supports unicast, multicast as well as broadcast communications.

## **Features of Switches**

* A switch operates in the layer 2, i.e. data link layer of the OSI model.
* It is an intelligent network device that can be conceived as a multiport network bridge.
* It uses MAC addresses (addresses of medium access control sublayer) to send data packets to selected destination ports.
* It uses packet switching technique to receive and forward data packets from the source to the destination device.
* It is supports unicast (one-to-one), multicast (one-to-many) and broadcast (one-to-all) communications.
* Transmission mode is full duplex, i.e. communication in the channel occurs in both the directions at the same time. Due to this, collisions do not occur.
* Switches are active devices, equipped with network software and network management capabilities.
* Switches can perform some error checking before forwarding data to the destined port.
* The number of ports is higher – 24/48.

1. Explain Router

A router is a device that connects two or more packet-switched networks or subnetworks. It serves two primary functions: managing traffic between these networks by forwarding [data packets](https://www.cloudflare.com/learning/network-layer/what-is-a-packet/) to their intended [IP addresses](https://www.cloudflare.com/learning/dns/glossary/what-is-my-ip-address/), and allowing multiple devices to use the same Internet connection.

There are several types of routers, but most routers pass data between [LANs (local area networks)](https://www.cloudflare.com/learning/network-layer/what-is-a-lan/) and [WANs (wide area networks)](https://www.cloudflare.com/learning/network-layer/what-is-a-wan/). A LAN is a group of connected devices restricted to a specific geographic area. A LAN usually requires a single router.

A WAN, by contrast, is a large network spread out over a vast geographic area. Large organizations and companies that operate in multiple locations across the country, for instance, will need separate LANs for each location, which then connect to the other LANs to form a WAN. Because a WAN is distributed over a large area, it often necessitates multiple routers and switches\*.

1. Explain MODEM

**modem**, (from “modulator/demodulator”), any of a class of electronic devices that convert [digital](https://www.britannica.com/topic/digital-information) data [signals](https://www.britannica.com/technology/signal) into modulated analog signals suitable for transmission over [analog](https://www.merriam-webster.com/dictionary/analog) telecommunications circuits. A modem also receives modulated signals and demodulates them, recovering the digital signal for use by the [data](https://www.britannica.com/technology/data-transmission) equipment. Modems thus make it possible for established [telecommunications media](https://www.britannica.com/topic/telecommunications-media) to support a wide variety of data [communication](https://www.britannica.com/topic/communication), such as [e-mail](https://www.britannica.com/technology/e-mail) between [personal computers](https://www.britannica.com/technology/personal-computer), facsimile transmission between [fax](https://www.britannica.com/technology/fax) machines, or the downloading of audio-video files from a [World Wide Web](https://www.britannica.com/topic/World-Wide-Web) [server](https://www.britannica.com/technology/server) to a home computer.

1. Explain DHCP Dynamic host configuration protocol Explain Domain Naming Services What is protocol?

DHCP (Dynamic Host Configuration Protocol) is a network management protocol used to dynamically assign an IP address to any device, or [node](https://www.techtarget.com/searchnetworking/definition/node), on a network so it can communicate using IP. DHCP automates and centrally manages these configurations rather than requiring network administrators to manually assign IP addresses to all network devices. DHCP can be implemented on small local networks, as well as large enterprise networks.

DHCP assigns new IP addresses in each location when devices are moved from place to place, which means network administrators do not have to manually configure each device with a valid IP address or reconfigure the device with a new IP address if it moves to a new location on the network.

Versions of DHCP are available for use in IP version 4 ([IPv4](https://www.techtarget.com/whatis/definition/IPv4-address-class)) and IP version 6 ([IPv6](https://www.techtarget.com/searchnetworking/definition/IPv6-Internet-Protocol-Version-6)). IPv6 became an industry standard in 2017 -- nearly 20 years after its specifications were first published. While the adoption rate of IPv6 was slow, more than 29% of Google users were making inquiries using IPv6 by July 2019.

Domain Name Services: -

Domain Name Services, or DNS, provides addressing help for the Internet. Generally people have a better time remembering and using names, like Google.com, while computers have an easier time using numbers like 173.194.46.19 (one of Google’s addresses). The hierarchical structure of the Internet also makes the use of numbered octets more efficient. This creates a problem where the best addressing scheme for people does not match the best scheme for computers. Name servers help to solve this problem by serving as translators between computers and people.

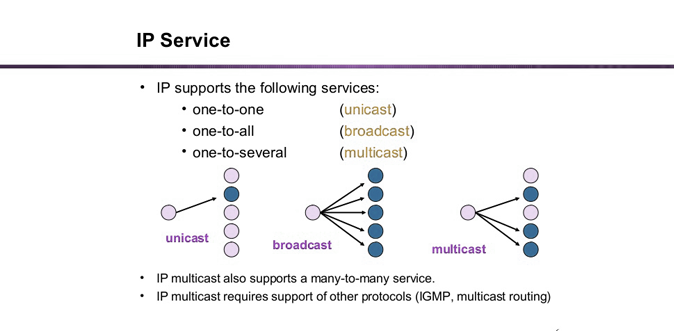
Network Protocol:-

A network protocol is an established set of rules that determine how data is transmitted between different devices in the same network. Essentially, it allows connected devices to communicate with each other, regardless of any differences in their internal processes, structure or design.

1. What is unicast multicast and broadcast?

**Unicast**: from one source to one destination i.e. One-to-One

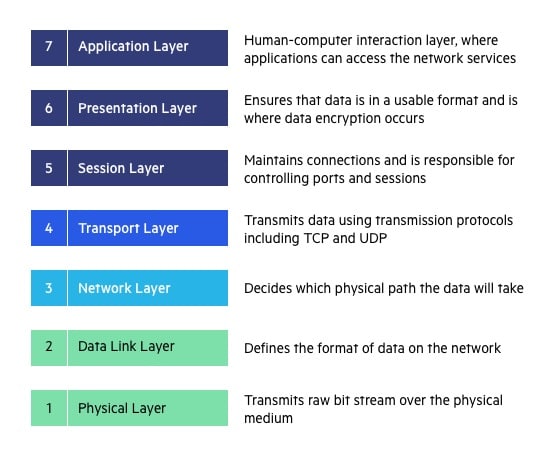
**Broadcast**: from one source to all possible destinations i.e. One-to-All

**Multicast**: from one source to multiple destinations stating an interest in receiving the traffic i.e. One-to-Many

1. What is OSI model?

The Open Systems Interconnection (OSI) model describes seven layers that computer systems use to communicate over a network. It was the first standard model for network communications, adopted by all major computer and telecommunication companies in the early 1980s

The modern Internet is not based on OSI, but on the simpler TCP/IP model. However, the OSI 7-layer model is still widely used, as it helps visualize and communicate how networks operate, and helps isolate and troubleshoot networking problems.

OSI was introduced in 1983 by representatives of the major computer and telecom companies, and was adopted by ISO as an international standard in 1984.

**7. Application Layer**

The application layer is used by end-user software such as web browsers and email clients. It provides protocols that allow software to send and receive information and present meaningful data to users. A few examples of application layer protocols are the [Hypertext Transfer Protocol](https://www.imperva.com/learn/performance/http2/) (HTTP), File Transfer Protocol (FTP), Post Office Protocol (POP), Simple Mail Transfer Protocol (SMTP), and Domain Name System (DNS).

**6. Presentation Layer**

The presentation layer prepares data for the application layer. It defines how two devices should encode, encrypt, and compress data so it is received correctly on the other end. The presentation layer takes any data transmitted by the application layer and prepares it for transmission over the session layer.

**5. Session Layer**

The session layer creates communication channels, called sessions, between devices. It is responsible for opening sessions, ensuring they remain open and functional while data is being transferred, and closing them when communication ends. The session layer can also set checkpoints during a data transfer—if the session is interrupted, devices can resume data transfer from the last checkpoint.

**4. Transport Layer**

The transport layer takes data transferred in the session layer and breaks it into “segments” on the transmitting end. It is responsible for reassembling the segments on the receiving end, turning it back into data that can be used by the session layer. The transport layer carries out flow control, sending data at a rate that matches the connection speed of the receiving device, and error control, checking if data was received incorrectly and if not, requesting it again.

**3. Network Layer**

The network layer has two main functions. One is breaking up segments into network packets, and reassembling the packets on the receiving end. The other is routing packets by discovering the best path across a physical network. The network layer uses network addresses (typically Internet Protocol addresses) to route packets to a destination node.

**2. Data Link Layer**

The data link layer establishes and terminates a connection between two physically-connected nodes on a network. It breaks up packets into frames and sends them from source to destination. This layer is composed of two parts—Logical Link Control (LLC), which identifies network protocols, performs error checking and synchronizes frames, and Media Access Control (MAC) which uses MAC addresses to connect devices and define permissions to transmit and receive data.

* 1. **Physical Layer**

The physical layer is responsible for the physical cable or wireless connection between network nodes. It defines the connector, the electrical cable or wireless technology connecting the devices, and is responsible for transmission of the raw data, which is simply a series of 0s and 1s, while taking care of bit rate control.

1. What is port number?

A port number is the logical address of each application or process that uses a network or the Internet to communicate. A port number uniquely identifies a network-based application on a computer. Each application/program is allocated a 16-bit integer port number. This number is assigned automatically by the OS, manually by the user or is set as a default for some popular applications.

1. Difference between TCP V/S UDP communications What is session

development?

|  |  |  |
| --- | --- | --- |
| **Feature** | **TCP** | **UDP** |
| **Connection status** | Requires an established connection to transmit data (connection should be closed once transmission is complete) | Connectionless protocol with no requirements for opening, maintaining, or terminating a connection |
| **Data sequencing** | Able to sequence | Unable to sequence |
| **Guaranteed delivery** | Can guarantee delivery of data to the destination router | Cannot guarantee delivery of data to the destination |
| **Retransmission of data** | Retransmission of lost packets is possible | No retransmission of lost packets |
| **Error checking** | Extensive error checking and acknowledgment of data | Basic error checking mechanism using checksums |
| **Method of transfer** | Data is read as a byte stream; messages are transmitted to segment boundaries | UDP packets with defined boundaries; sent individually and checked for integrity on arrival |
| **Speed** | Slower than UDP | Faster than TCP |
| **Broadcasting** | Does not support Broadcasting | Does support Broadcasting |
| **Optimal use** | Used by HTTPS, HTTP, SMTP, POP, FTP, etc | Video conferencing, streaming, DNS, VoIP, etc |

Session Development:-

A **session** is the total time devoted to an activity. In computer systems, a **user session** begins when a user logs in to or accesses a particular computer, network, or software service. It ends when the user logs out of the service, or shuts down the computer. A session can temporarily store information related to the activities of the user while connected.

1. What is flow control?

**Flow control** is [design issue at Data Link Layer](https://www.geeksforgeeks.org/design-issues-in-data-link-layer/). It is a technique that generally observes the proper flow of data from sender to receiver. It is very essential because it is possible for sender to transmit data or information at very fast rate and hence receiver can receive this information and process it. This can happen only if receiver has very high load of traffic as compared to sender, or if receiver has power of processing less as compared to sender. Flow control is basically a technique that gives permission to two of stations that are working and processing at different speeds to just communicate with one another. Flow control in Data Link Layer simply restricts and coordinates number of frames or amount of data sender can send just before it waits for an acknowledgement from receiver. Flow control is actually set of procedures that explains sender about how much data or frames it can transfer or transmit before data overwhelms receiver. The receiving device also contains only limited amount of speed and memory to store data. This is why receiving device should be able to tell or inform the sender about stopping the transmission or transferring of data on temporary basis before it reaches limit. It also needs buffer, large block of memory for just storing data or frames until they are processed.

1. What is the difference between TCP IP model and OSI model?

|  |  |
| --- | --- |
| **Difference  between TCP/IP and OSI Model** | |
| **TCP/IP** | **OSI Model** |
| The full form of TCP/IP is Transmission Control Protocol/ Internet Protocol. | The full form of OSI is Open Systems Interconnection. |
| It is a communication protocol that is based on standard protocols and allows the connection of hosts over a network. | It is a structured model which deals which the functioning of a network. |
| In 1982, the TCP/IP model became the standard language of ARPANET. | In 1984, the OSI model was introduced by the International Organisation of Standardization (ISO). |
| It comprises of four layers:   * Network Interface * Internet * Transport * Application | It comprises seven layers:   * Physical * Data Link * Network * Transport * Session * Presentation * Application |
| It follows a horizontal approach. | It follows a vertical approach. |
| The TCP/IP is the implementation of the OSI Model. | An OSI Model is a reference model, based on which a network is created. |
| It is protocol dependent. | It is protocol independent. |

1. What is arp broadcast?

Most of the computer programs/applications use **logical address (IP address)** to send/receive messages, however, the actual communication happens over the **physical address (MAC address)** i.e from layer 2 of the OSI model. So our mission is to get the destination MAC address which helps in communicating with other devices. This is where ARP comes into the picture, its functionality is to translate IP address to physical addresses. 

The acronym ARP stands for **Address Resolution Protocol** which is one of the most important protocols of the Network layer in the OSI model.

1. What is mac-address?

MAC address is the physical address, which uniquely identifies each device on a given network. To make communication between two networked devices, we need two addresses: **IP address and MAC address.** It is assigned to the NIC (Network Interface card) of each device that can be connected to the internet.

1. What is ip address? Difference between ipv4 address and ipv6

address Assign multiple IPv4 in single network adapter in pc what are network vulnerabilities?

An IP address is a unique address that identifies a device on the internet or a local network. IP stands for "Internet Protocol," which is the set of rules governing the format of data sent via the internet or local network.

Difference Between ipv4 and ipv6

| **IPv4** | **IPv6** |
| --- | --- |
| IPv4 has a 32-bit address length | IPv6 has a 128-bit address length |
| It Supports Manual and DHCP address configuration | It supports Auto and renumbering address configuration |
| In IPv4 end to end, connection integrity is Unachievable | In IPv6 end to end, connection integrity is Achievable |
| It can generate 4.29×109 address space | Address space of IPv6 is quite large it can produce 3.4×1038 address space |
| The Security feature is dependent on application | IPSEC is an inbuilt security feature in the IPv6 protocol |
| Address representation of IPv4 is in decimal | Address Representation of IPv6 is in hexadecimal |
| Fragmentation performed by Sender and forwarding routers | In IPv6 fragmentation performed only by the sender |
| In IPv4 Packet flow identification is not available | In IPv6 packet flow identification are Available and uses the flow label field in the header |
| In IPv4 checksum field is available | In IPv6 checksum field is not available |
| It has broadcast Message Transmission Scheme | In IPv6 multicast and anycast message transmission scheme is available |
| In IPv4 Encryption and Authentication facility not provided | In IPv6 Encryption and Authentication are provided |
| IPv4 has a header of 20-60 bytes. | IPv6 has header of 40 bytes fixed |
| IPv4 can be converted to IPv6 | Not all IPv6 can be converted to IPv4 |
| IPv4 consist of 4 fields which are separated by dot (.) | IPv6 consist of 8 fields, which are separated by colon (:) |
| IPv4’s  IP addresses are divided into five different classes. Class A , Class B, Class C , Class D , Class E. | IPv6 does not have any classes of IP address. |
| IPv4 supports VLSM(Variable Length subnet mask). | IPv6 does not support VLSM. |
| Example of IPv4:  66.94.29.13 | Example of IPv6: 2001:0000:3238:DFE1:0063:0000:0000:FEFB |

Network Vulnerability

Network security vulnerabilities are weaknesses or flaws within the system’s software, hardware, or organizational processes. Network vulnerabilities can be either non-physical or physical.

* **Non-Physical:** This weakness refers to anything related to data and software. Vulnerable operating systems that the IT department does not update will leave the entire system susceptible to threat actors. If a virus or malware downloads into the operating system, it could potentially infect the whole network.
* **Physical:** Physical protection for networks includes actions like storing an on-site server in a rack closet and securing it with a lock or requiring a code to access a secure point of entry. Because servers store valuable information such as consumer data or trade secrets, they need tight, physical security controls like biometric scanners or access cards to reduce or eliminate the risk of unauthorized users accessing the area and equipment.

1. What is a firewall to use for?

A Firewall is a network security device that monitors and filters incoming and outgoing network traffic based on an organization’s previously established security policies. At its most basic, a firewall is essentially the barrier that sits between a private internal network and the public Internet. A firewall’s main purpose is to allow non-threatening traffic in and to keep dangerous traffic out.

#### Prevents the Passage of Unwanted Content

#### Prevents Unauthorized Remote Access

#### Prevents Indecent Content

#### Guarantees Security Based on Protocol and IP Address

#### Protects Seamless Operations in Enterprises

#### Protects Conversations and Coordination Contents

#### Prevents Destructive Content from Online Videos and Games

1. Wireless router configures for internet connection and wireless

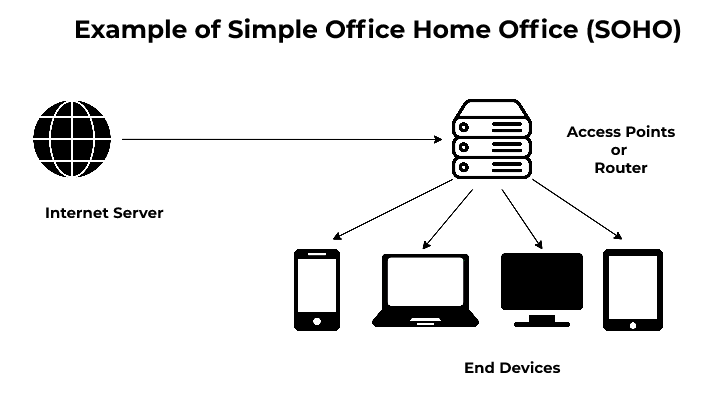
security what is wireless access point? And what is wireless extender?

A wireless access point (WAP) is a hardware device or configured node on a local area network (LAN) that allows wireless capable devices and wired networks to connect through a wireless standard, including Wi-Fi or Bluetooth. WAPs feature radio transmitters and antennae, which facilitate connectivity between devices and the Internet or a network.

A WAP is also known as a hotspot.

**Module – 2**

1. What is SOHO network?

**SOHO** stands for **Small Office and Home Office Networks**. It allows computers in a home office or remote office to connect to a corporate network, or access centralized, shared resources. It is a[LAN (local area network)](https://www.geeksforgeeks.org/local-area-network-lan-technologies/)mainly referred to as a business category involving a small number of workers usually from 01 to 10. SOHO provides a lot of features and benefits such as easy-to-use and setup networks etc. making them an ideal choice for small businesses. A virtual office is another synonym sometimes used for a SOHO network. SOHO networking is mainly used for the purpose of connecting several computing devices on a single network to share information effectively with the multiple connected users in the organization.

1. What is NAT?

To access the Internet, one public IP address is needed, but we can use a private IP address in our private network. The idea of NAT is to allow multiple devices to access the Internet through a single public address. To achieve this, the translation of a private IP address to a public IP address is required. **Network Address Translation (NAT)** is a process in which one or more local IP address is translated into one or more Global IP address and vice versa in order to provide Internet access to the local hosts. Also, it does the translation of port numbers i.e. masks the port number of the host with another port number, in the packet that will be routed to the destination. It then makes the corresponding entries of IP address and port number in the NAT table. NAT generally operates on a router or firewall.

1. What is PAT?

Port address translation (PAT) is a function that allows multiple users within a private network to make use of a minimal number of IP addresses. Its basic function is to share a single IP public address between multiple clients who need to use the Internet publicly. It is an extension of network address translation (NAT).  
  
Port address translation is also known as overload or port overload.

1. Different between NAT & PAT?

| **Network Address Translation (NAT)** | **Port Address Translation (PAT)** |
| --- | --- |
| [NAT](https://www.geeksforgeeks.org/network-address-translation-nat/) stands for Network Address Translation. | [PAT](https://www.geeksforgeeks.org/port-address-translation-pat-on-adaptive-security-appliance-asa/) stands for Port Address Translation. |
| In NAT, Private IP addresses are translated into the public IP address. | In PAT, [Private IP addresses](https://www.geeksforgeeks.org/private-ip-addresses-in-networking/) are translated into the public IP address via Port numbers. |
| NAT can be considered PAT’s superset. | PAT is a dynamic NAT. |
| NAT uses [IPv4](https://www.geeksforgeeks.org/what-is-ipv4/) address. | PAT also uses IPv4 address but with port number. |
| It have 3 types: Static, Dynamic NAT and PAT/ NAT Overloading/IP masquerading. | It also have two types: Static and Overloaded PAT. |

1. What Is Acl?

A network access control list (ACL) is made up of rules that either allow access to a computer environment or deny it. In a way, an ACL is like a guest list at an exclusive club. Only those on the list are allowed in the doors. This enables administrators to ensure that, unless the proper credentials are presented by the device, it cannot gain access.

There are two basic kinds of ACLs:

1. **Filesystem ACLs**: These work as filters, managing access to directories or files. A filesystem ACL gives the operating system instructions as to the users that are allowed to access the system, as well as the privileges they are entitled to once they are inside.
2. **Networking ACLs**: Networking ACLs manage access to a network. To do this, they provide instructions to switches and routers as to the kinds of traffic that are allowed to interface with the network. They also dictate what each user or device can do once they are inside.

When ACLs were first conceived, they worked like [firewalls](https://www.fortinet.com/resources/cyberglossary/how-does-a-firewall-work), blocking access to unwanted entities. While many firewalls have network access control functions, some organizations still use ACLs with technologies such as [virtual private networks (VPNs)](https://www.fortinet.com/resources/cyberglossary/what-is-a-vpn). In this way, an administrator can dictate which kinds of traffic get encrypted and then sent through the secure tunnel of the VPN.

1. What Are Different Types of Acl? What Is Wildcard Mask?

There are two basic kinds of ACLs:

1. **Filesystem ACLs**: These work as filters, managing access to directories or files. A filesystem ACL gives the operating system instructions as to the users that are allowed to access the system, as well as the privileges they are entitled to once they are inside.
2. **Networking ACLs**: Networking ACLs manage access to a network. To do this, they provide instructions to switches and routers as to the kinds of traffic that are allowed to interface with the network. They also dictate what each user or device can do once they are inside.

Wildcard Mask

A wildcard mask is a sequence of binary bits which helps in streamlining the routing of packets within a subnet of a network. It is shown over the subnet number, providing the router information about which parts of the subnet number to focus on. The use of the wildcard mark helps the router to only focus on the digits chosen by the mask rather than on the entire IP address. Wildcard masks are normally used to specify which IP addresses can be allowed or denied in the access control lists and with router protocols like the Open Shortest Path First.

1. Explain Circuit switching

In circuit switching network resources (bandwidth) are divided into pieces and bit delay is constant during a connection. The dedicated path/circuit established between sender and receiver provides a guaranteed data rate. Data can be transmitted without any delays once the circuit is established.

Telephone system network is one of the examples of Circuit switching. **TDM (Time Division Multiplexing) and FDM (Frequency Division Multiplexing)** are two methods of multiplexing multiple signals into a single carrier.

* **Frequency Division Multiplexing:** *Divides into multiple bands*   
  Frequency Division Multiplexing or FDM is used when multiple data signals are combined for simultaneous transmission via a shared communication medium. It is a technique by which the total bandwidth is divided into a series of non-overlapping frequency sub-bands, where each sub-band carry different signal. Practical use in radio spectrum & optical fibre to share multiple independent signals.
* **Time Division Multiplexing:** *Divides into frames*   
  Time-division multiplexing (TDM) is a method of transmitting and receiving independent signals over a common signal path by means of synchronized switches at each end of the transmission line. TDM is used for long-distance communication links and bears heavy data traffic loads from end user.   
  Time division multiplexing (TDM) is also known as a digital circuit switched.

1. What is difference between leased line and broadband?
2. Difference between a POTS line and a leased line?
3. Practice on printer sharing

The term "IIS" stands for Internet Information Services, which is a general-purpose webserver that runs on the Windows operating system. The IIS accepts and responds to the client's computer requests and enables them to share and deliver information across the [LAN](https://www.javatpoint.com/wireless-lan-introduction) (or Local Area Network) such as a corporate intranet and the WAN (or Wide Area Network) the internet. It hosts the application, websites, and other standard services needed by users and allows developers to make websites, applications and virtual directories to share with their users. A web server provides the users with information in several different forms, such as File exchanges as a download, uploads, Images files, HTML pages, and text documents. The webservers are commonly used as a portal for sophisticated and highly interactive websites, applications that tie middleware and back-end applications together to make enterprise-grade-systems. For example, [AWS](https://www.javatpoint.com/aws-tutorial) enables media services such as Netflix to provide real-time streaming content. Amazon web services also enable public cloud administration all through the webservers. Generally, the IIS is also compared with the Apache, which is also a kind of web server that is freely available for everyone. We can simply say that both works the same except that the apache web server can be used almost on any operating system such as Windows, [Linux](https://www.javatpoint.com/linux-tutorial), and Mac, While the IIS is only available for windows. However, the IIS integrates with Microsoft's other products, such as the [.NET Framework](https://www.javatpoint.com/net-framework), the [ASP](https://www.javatpoint.com/asp-net-tutorial) scripting language. The IIS also has its own helpdesk to manage and solve issues while, on the other hand, the Apache webserver's supports almost come from the user community. Additionally, the IIS has the security features, which makes it a more secure and efficient option than the Apache.

1. What is the difference between cloud and virtualization?

| **S.NO** | **Cloud Computing** | **Virtualization** |
| --- | --- | --- |
| 1. | Cloud computing is used to provide pools and automated resources that can be accessed on-demand. | While It is used to make various simulated environments through a physical hardware system. |
| 2. | Cloud computing setup is tedious, complicated. | While virtualization setup is simple as compared to cloud computing. |
| 3. | Cloud computing is high scalable. | While virtualization is low scalable compared to cloud computing. |
| 4. | Cloud computing is Very flexible. | While virtualization is less flexible than cloud computing. |
| 5. | In the condition of disaster recovery, cloud computing relies on multiple machines. | While it relies on single peripheral device. |
| 6. | In cloud computing, the workload is stateless. | In virtualization, the workload is stateful. |
| 7. | The total cost of cloud computing is higher than virtualization. | The total cost of virtualization is lower than Cloud Computing. |
| 8. | Cloud computing requires many dedicated hardware. | While single dedicated hardware can do a great job in it. |
| 9. | Cloud computing provides unlimited storage space. | While storage space depends on physical server capacity in virtualization. |
| 10. | Cloud computing is of two types : Public cloud and Private cloud. | Virtualization is of two types : Hardware virtualization and Application virtualization. |
| 11. | In Cloud Computing, Configuration is image based. | In Virtualization, Configuration is template based. |
| 12. | In cloud computing, we utilize the entire server capacity and the entire servers are consolidated. | In Virtualization, the entire servers are on-demand. |
| 13. | In cloud computing, the pricing pay as you go model, and consumption is the metric on which billing is done. | In Virtualization, the pricing is totally dependent on infrastructure costs. |

1. Why are network monitoring tools used?

Network monitoring provides the information that network administrators need to determine, in real time, whether a network is running optimally. With tools such as networking monitoring software, administrators can proactively identify deficiencies, optimize efficiency, and more.

1. What is ping ?

Ping (Packet Internet Groper) is a method for determining communication latency between two networks. Simply put, ping is a method of determining latency or the amount of time it takes for data to travel between two devices or across a network. As communication latency decreases, communication effectiveness improves.

1. What is traceroute ?

Traceroute is a simple yet clever command-line tool for tracing the path an IP packet takes across one or many networks. It was originally developed for UNIX-based platforms, but is now included in most operating systems, with the Windows implementation being known as “tracert”. The output of these commands is also frequently referred to as a traceroute. Ask for help with poor streaming video performance, for example, and your ISP might ask you for a traceroute.

1. What is nslookup?

Name server lookup (nslookup) is a command-line tool that lets you find the internet protocol (IP) address or [**domain name system**](https://www.hostinger.com/tutorials/what-is-dns) (DNS) record of a specific hostname. This command also allows [**reverse DNS lookup**](https://www.hostinger.com/tutorials/what-is-a-ptr-record-and-how-to-do-reverse-ip-lookup) by inputting the IP addresses of the corresponding domains.

The nslookup tool is useful for DNS-related tasks, such as server testing or troubleshooting issues. To use this tool, type “nslookup” into a command-line interface (CLI) such as the Command Prompt on Windows or Terminal on Linux and macOS.

1. Explain core switches

A core switch is a high-capacity switch generally positioned within the backbone or physical core of a network. Core switches serve as the gateway to a wide area network (WAN) or the Internet - they provide the final aggregation point for the network and allow multiple aggregation modules to work together.

A core switch is also known as a tandem switch or a backbone switch.

1. What is network management?

Network management is the procedure of administering, managing and working a data network using a network management system. Current network management systems use software and hardware to constantly collect and analyse data and push out configuration changes for increasing performance, reliability, and security.

It involves configuring monitoring and possibly reconfiguring components in a network with the goal of providing optimal performance, minimum downtime, proper security, accountability and flexibility.

## **Features**

There are various features of network management which are as follows −

### **Network automation**

One defining feature of a modern network management system is network automation. This is the procedure of automating the configuring, handling, testing, deploying, and operating of physical and virtual devices inside a network. Network service availability increases when everyday network tasks and functions are automated and repetitive processes are controlled and managed automatically.

### **Network administration**

Network administration encompasses tracking network resources, including switches, routers, and servers. It also includes performance monitoring and software updates.

### **Network Operation**

This contains smooth network functioning as created and intended, including close monitoring of activities to quickly and effectively address and fix problems as they occur and preferably even before users are aware of the problem.

### **Network assurance**

Network assurance features are often included in modern network management systems. These features help improve network performance, customer experience, and security. Assurance systems help network analytics, application analytics, and policy analytics, as well as AI and ML, to achieve full network assurance.

### **Network provisioning**

Network provisioning involves network resource configuration for the purposes of supporting any given service, like voice functions or accommodating additional users.

### **Network maintenance**

Network maintenance covers upgrades and fixes to network resources. It also consists of proactive and remediation activities executed by working with network administrators, such as replacing network gear like routers and switches.

### **Network analytics**

Network analytics is a software tool that compares incoming information against pre-programmed operational models and makes functional decisions for improving network performance.

1. Explain Event Viewer

Microsoft Windows Server Event Viewer is **a monitoring tool that shows a log of events that can be used to troubleshoot issues on a Windows-based system**. The Event Viewer displays information about application, security-related, system and setup events.

1. What are the types of network security attacks?

### 1. Malware Attack

### 2. Phishing Attack

### 3. Password Attack

### 4. Man-in-the-Middle Attack

### 5. SQL Injection Attack

### 6. Denial-of-Service Attack

### 7. Insider Threat

### 8. Crypto jacking

### 9. Zero-Day Exploit

### 10. Watering Hole Attack