CCNA Interview Questions

A list of top frequently asked **CCNA interview questions** and answers are given below.

1) What is the difference between switch and hub?

Basis of Comparison	Hub	Switch
Description	Hub is a networking device that connects the multiple devices to a single network.	A switch is a control unit that turns the flow of electricity on or off in a circuit.
Layer	Hubs are used at the physical layer.	Switches are used at the data link layer.
Transmission type	Transmission type can be unicast, broadcast or multicast.	Initially, the transmission type is broadcast and then is unicast.
Ports	Hub has 4/12 ports.	The switch has 24/48 ports.
Transmission mode	Half duplex	Half/Full duplex.
Collisions	Collisions occur commonly in a Hub.	No collisions occur in a full duplex switch.
Address used for data transmission	Hub uses MAC address for data transmission.	The switch uses a MAC address for data transmission.
Data transmission form	Electrical signal is a data transmission form of a hub.	A Frame is a data transmission form of a switch.

2) What is the difference between Switch and Router?

Basis of Compariso n	Router	Switch
Description	It is a layer 3 device that connects the two different networks and identifies the network devices based on their IP addresses.	It is a layer 2 device and determines the network devices based on their MAC addresses.
Mode of transmission	Router transmits the data in the form of packets.	Switch transmits the data in the form of frames.
Address used	It uses an IP address for the data transmission.	It uses a MAC address to transmit the data.
Layer of OSI model	It uses Layer 3 OSI model and layer is the network layer.	It uses layer 2 OSI model and layer is the data link layer.
Table	It uses a routing table for routes to move to the destination IP.	It uses a Content address memory table for MAC addresses.
Network used	It is used for WAN and LAN networks.	It is used only for LAN networks.
Mode of transmission	Router is used in a full-duplex mode.	A switch is used in half as well as in a full-duplex mode.

3) What are the advantages of using Switches?

Advantages of using Switches:

- Switches are used to receive a signal and create a frame out of the bits from that signal. The signals enable you to get access and read the destination address and after reading that it forward that frame to appropriate frame. So, switches are the significant part of the transmission.

4) What is Routing?

- Routing is a process of finding a path to transfer data from source to destination.
- Routing can be performed in a variety of networks such as circuit switched networks and computer networks.
- In packet switching networks, routing makes a decision that directs the packets from source to the destination.
- Routing makes use of a routing table, which maintains the routes of various destinations.

Types of routing:

1. **Static routing**: Static routing is a routing technique where an administrator manually adds the routes in a routing table. Static routes are used when the route selections are limited. Static routes can also be used in those situations where the devices are fewer and no need to change in the route configuration in future.
2. **Dynamic routing**: Dynamic routing is a routing technique where protocols automatically update the information of a routing table.

---

5) What are Routers?

- The devices known as Routers do the process of routing. Routers are the network layer devices.
- The router is a networking device which is used to transfer the data across the networks, and that can be wired or wireless.
- Routers use headers and routing table to determine the best route for forwarding the packets.
- Router analyzes the data which is being sent over the network, changes how it is packaged and send it over the network.

Examples of routers are:

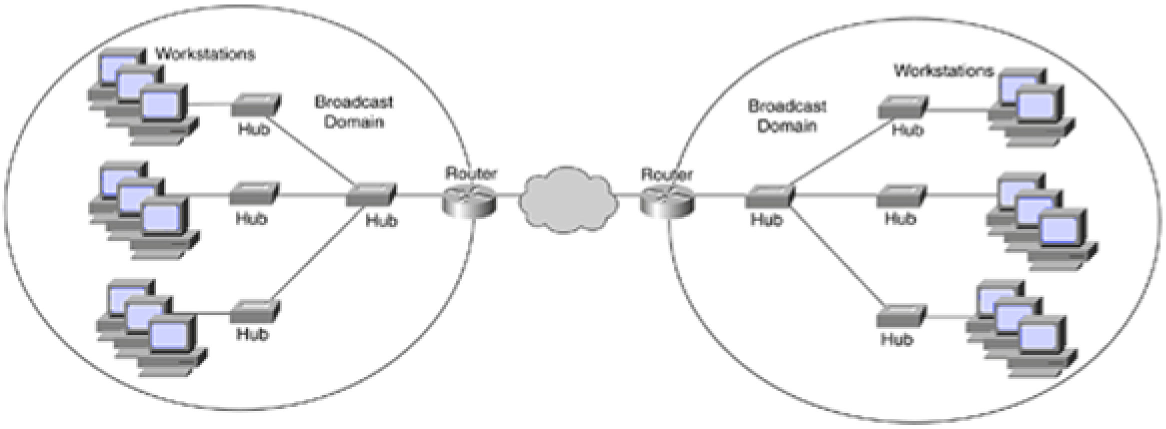
1. **Brouter**: Brouter stands for "Bridge Router". It serves both as a router and bridge.
2. **Core router**: Core router is a router in the computer network that routes the data within a network, but not between the networks.
3. **Edge router**: An edge router is a router that resides at the boundary of a network.
4. **Virtual router**: A virtual router is a software-based router. The virtual router performs the packet routing functionality through a software application. A

Virtual Router Redundancy protocol implements the virtual router to increase the reliability of the network.

5. **Wireless router**: A wireless router is a router that connects the local networks with another local network.

6) What is the advantage of VLAN?

VLAN is a custom network which is created from one or more existing LAN's. VLAN facilitates you to create a collision domain by groups other than just physical location while in conventional LAN domains are always tied to physical location.



Advantage of VLAN:

- **Broadcast control**: A VLAN (Virtual Area Network) removes the physical layer and, it logically separates the networks within networks creating a smaller broadcast domain. It reduces the size of the broadcast domain, therefore, improving the efficiency of the network.
- **Simplified administration**: When a computer is moved to another location, but it stays on the same VLAN without any hardware configuration.
- **Security**:
- **LAN segmentation**: Virtual Area Networks are used to logically separate layer 2 switch networks. Users on different VLAN cannot communicate with each other. Therefore, it's a great way of segmentation and provides security.
- **Dynamic VLANs**: The Dynamic VLAN's are created using the software. The VLAN Management Policy Server (VMPS) is an administrator that dynamically allocates the switch ports based on the information available such as the MAC addresses of the device.

- **Protocol-based VLANs**: The switch that depends on the protocol based VLANs, then the traffic will be segregated by a particular protocol.

---

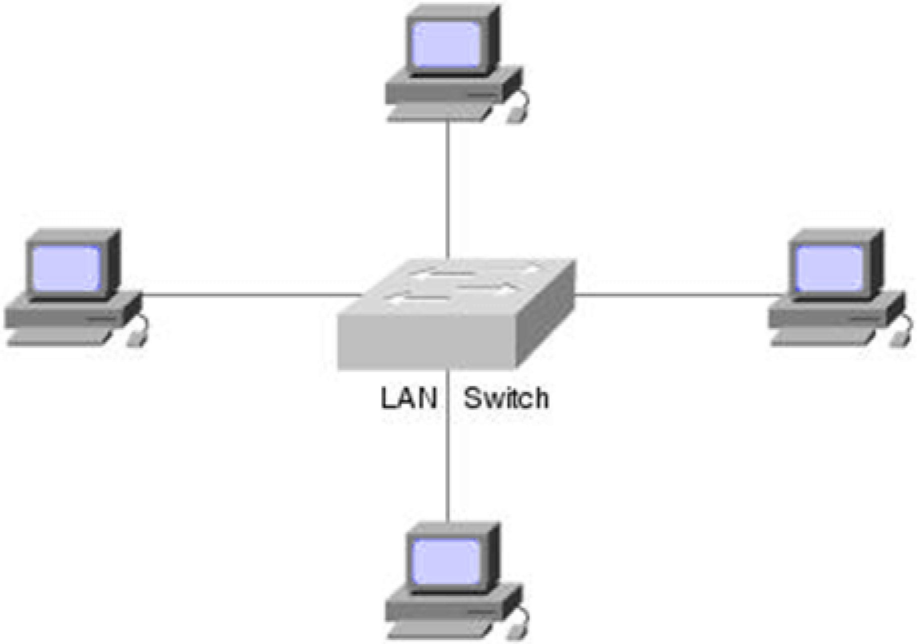
7) What is HDLC?

- HDLC stands for High-Level Data Link Control protocol. It is the property protocol of Cisco which is the default encapsulation operated with Cisco routers.
- HDLC adds the information in a data frame that allows the devices to control the data flow.
- HDLC is a bit-oriented protocol that supports both half and full duplex communication.
- HDLC offers flexibility, adaptability, reliability, and efficiency of operation for synchronous data communication.
- It supports both point-to-point and point-to-multipoint communication.
- It supports synchronous as well as asynchronous communication.
- It provides full data transparency, i.e., the output delivered has the same bit sequence as the input without any restriction.

---

8) What are the advantages of LAN switching?

LAN switching: LAN switching enables the multiple users to communicate with each other directly. LAN switching provides the collision-free network and high-speed networking.



Following are the main advantages of LAN switching:

- **Increased network scalability**: LAN switching can handle the increasing amount of work. Therefore, we can say that when the business grows, the network can expand easily.
- **Improved bandwidth performance**: We require higher bandwidth performance when users operate multimedia applications or some database interactions.
- **Multiple simultaneous connections**: LAN switching allows multiple simultaneous connections, i.e., it can transfer the multiple data at the same time. This cannot be possible in the case of a hub-based network.
- **Reduced congestion and transmission delay**: LAN switching improves the performance of a network as a segmented network consists of fewer hosts per subnetwork and thus, minimizing the local traffic.
- **No single point of failure**: LAN switching provides the proper network designing. Therefore, there are fewer chances of network failure.
- **Allows full duplex data transmission**: LAN switching allows full duplex data transmission, i.e., the data can be transferred in a bidirectional line at the same time.

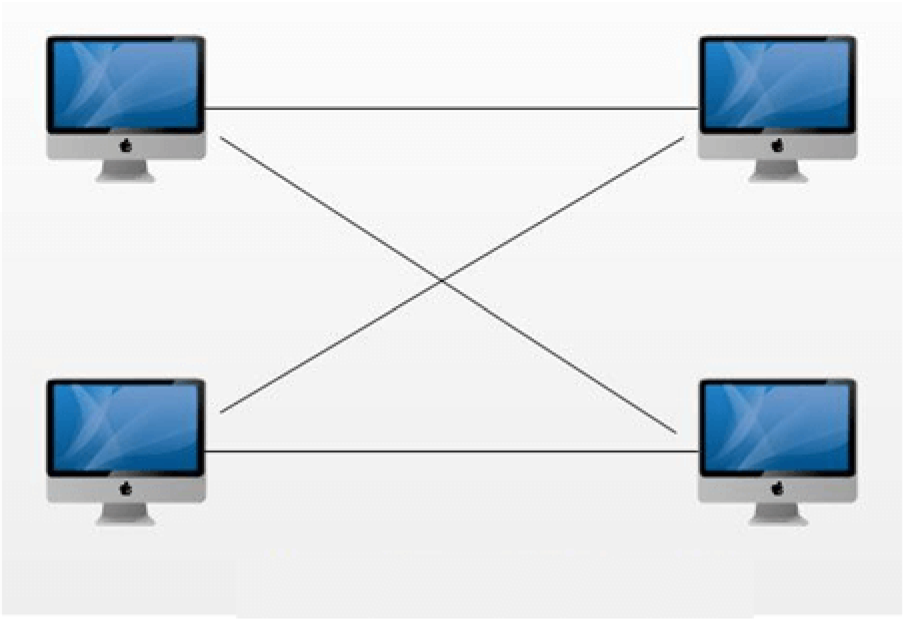
9) What is DLCI?

DLCI stands for **Data Link Connection Identifiers**. These are normally assigned by a frame relay service provider to identify each virtual circuit that exists on the network uniquely.

10) What are the different types of networks?

These are the two major types of networks:

1. Peer-to-Peer Network:

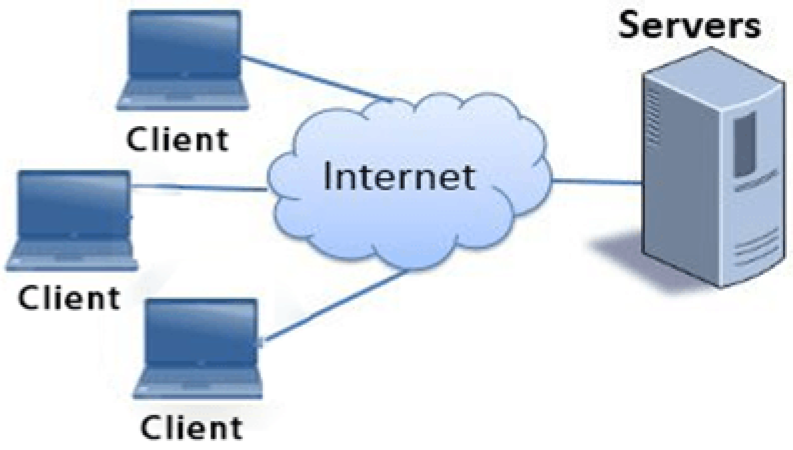


- In a peer-to-peer network, 'peers' are the computers which are connected to each other through an internet connection.
- The computer systems on the network without the need for any computer server.
- Therefore, the computer in P2P is a "computer server" as well as a "client".
- Requirements for a computer to have a peer-to-peer network are the internet connection and P2P software.
- Some of the common P2P software peers include Kazaa, Limewire, BearShare, Morpheus, and Acquisition.
- Once we are connected to the P2P network, then we able to search the files on other people's computer.

Types of a peer-to-peer network:

1. **Pure P2P**: In P2P, peers act as a client and server. There is no central server and central router present in the pure P2P.
2. **Hybrid P2P**: Hybrid P2P has a central server that stores the information and responds to the request for that information. Peers are used for hosting the information as a central server does not store the files. Nasper is an example of Hybrid P2P.
3. **Mixed P2P**: Mixed P2P is a combination of pure P2P and Hybrid P2P.

2. Server-based Network



- In a server-based network, server act as a base for the network known as a central server.
- The central server handles multiple tasks such as authenticating users, storing files, managing printers, and running applications such as database and email programs.
- In case of a server-based network, security is centralized in the system which allows the user to have one login id and password to log on to any computer system.
- Server-based networks are more complex and costly and often requires full- time services for administration.
- In server-based networks, the majority of traffic occurs between the servers.

11) What is the difference between private IP and public IP?

Following are the differences between public IP address and private IP address:

Basis of Comparison	Public IP address	Private IP address
Definition	It is used for the identification of a home network to the outside world.	It is used for the identification of a network device within the home network.
Uniqueness	Public IP address is unique throughout the network.	Private IP address can be the same of two different networks assigned to different computers.
Example	202.60.23.1	192.168.0.3
Usage	It is used over the internet or other WAN.	This type of address can be used on a local area network or for the computers that are not connected to the internet.
Communication	Public IP address is routable. Therefore, communication among different users is possible.	Private IP address is not routable. Thus, communication among different users is not possible.

---

12) What is the difference among straight cable, cross cable and rollover cable?

Straight cable:

- Straight cable is used to connect different group devices. For example Switch-Router.
- Straight cable is a kind of twisted pair cable used in a local area network to connect a computer to a network hub such as a router.
- Straight cables are used for linking different devices.
- It is an 8 wired patch cable.
- It is also used for connecting PC to the switch or router to a hub.
- The main purpose of a straight cable is to connect a host to the client.

Cross cable:

- Cross cable is used to connect the same group devices. For example Switch-Switch.
- Cross cable is a cable used to interconnect two computers by reversing their respective pin contacts.
- Cross cable is a cross-wired cable used to connect the two computers or hosts directly.
- Cross cable is used when two similar devices are to be connected.
- Cross cable crisscross each other, and this makes the communication of two devices at the same time.

Rollover cable:

- Rollover cable is used to connect the console port to the computer.
- Rollover cable is used to connect the computer's terminal to the network's router console port.
- Rollover cable is referred to as a Cisco console cable, and it is flat and light blue in color.
- Another name of a rollover cable is Yost cable.
- Rollover cable is identified by comparing the end of the cable with another cable as rollover cables are beside each other.
- Rollover cable allows the programmer to connect to the network device and can manipulate the programming whenever required.

---

13) What is the difference between tracert and traceroute?

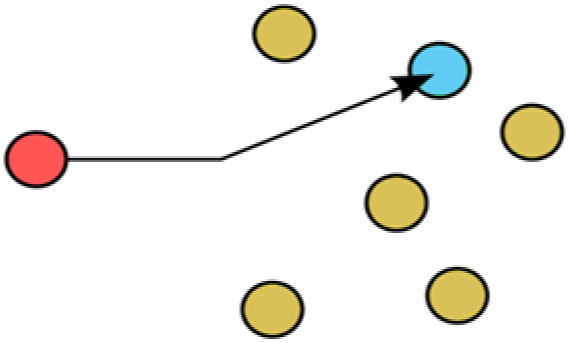
Differences between tracert and traceroute

Basis of Comparison	tracert	traceroute
Description	The tracert command is a command prompt command used to show the route that the packet takes to move from the source to the destination whatever we specify.	The traceroute command is a command used to show the route from your computer to the destination that you specify.

Device used	The tracert command is used on pc.	The traceroute command is used on a router or switch.
Operating system	The tracert command is used in Windows NT based OS.	The traceroute command is used in UNIX OS.

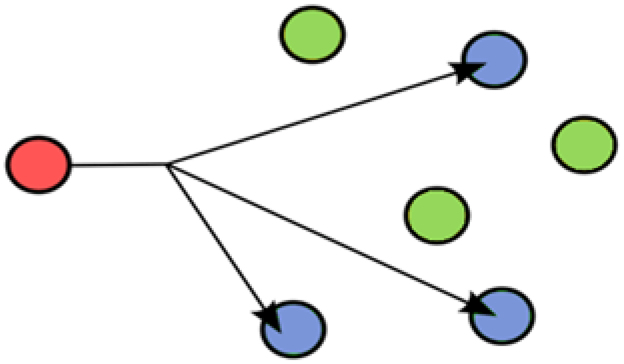
14) Explain the terms Unicast, Multicast, Broadcast.

Unicast:



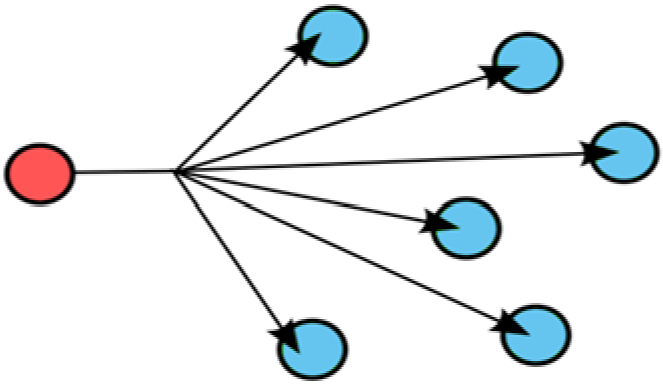
- It specifies one to one communication.
- It is a communication technique in which data communication takes place between two devices present in the network.
- Consider an example of browsing the internet. When we sent a request for some page to the web server, then the request directly goes to the web server to locate the address of a requested page. Therefore, this is one to one communication between client and server.
- Downloading the files from the FTP server is also the best example of unicast communication.

Multicast:



- It specifies one to group communication.
- It is a communication technique in which data communication takes place between a group of devices.
- Multicast uses IGMP(Internet Group Management Protocol) protocol to identify the group.
- Consider an example of video conferencing. If any user in a particular group can initiate the call and the people belongs to this group can participate in this call.
- Sending e-mail to a particular mailing group can also be considered as the example of multicast communication.

Broadcast:



- It specifies one to all communication.
- It is a communication technique in which data communication takes place among all the devices available in the network.
- Broadcasting can be achieved in two ways:

1. By using a high-level standard, i.e., Message passing interface. It is an interface used for exchanging the messages between multiple computers.
2. By using a low-level standard, i.e., broadcasting through an ethernet.

- Network is not secure in broadcasting as it can lead to a data loss if intruders attack the network.

---

15) What is the difference between cross cable and straight cable?

Cross cables are used to connect the same group devices while straight cables are used to connect different group devices.

For example: If you want to connect one PC to another PC, you have to use cross cable while, to connect one switch to a router, you have to use a straight cable.

---

16) What is the difference between static IP addressing and dynamic IP addressing?

Following are the differences between static IP addressing and dynamic IP addressing:

Basis of Comparison	Static IP address	Dynamic IP address
Description	Static IP address is a fixed number assigned to the computer.	The dynamic IP address is a temporary number assigned to the computer.
Provided By	Static IP address is provided by ISP(Internet Service Provider).	The dynamic IP address is provided by DHCP(Dynamic Host Configuration Protocol).
Change requirement	It is static means that IP address does not change.	It is non-static means that IP address changes whenever the user connects to a network.
Security	It is not secure as IP address is constant.	It is secure because each time IP address changes.

Cost	It is costlier than Dynamic IP address.	It is cheaper than the Static IP address.
Device tracking	Static IP address is trackable as IP address is constant.	The dynamic IP address is untraceable as IP address is always changing.

17) What is the difference between CSMA/CD and CSMA/CA?

CSMA/CD stands for **Carrier Sense Multiple Access with Collision Detection**. It is a media access control method used in local area networking using early Ethernet technology to overcome the occurred collision.

CSMA/CA stands for Carrier Sense Multiple Access with Collision Avoidance. It is used in the wireless network to avoid the collision.

Following are the differences between CSMA/CD and CSMA/CA:

CSMA/CD	CSMA/CA
Full form of CSMA/CD is carrier sense multiple access with collision detection.	Full form of CSMA/CA is carrier sense multiple access with carrier avoidance.
CSMA/CD detects the collision, and once the collision is detected, then it stops continuing the data transmission.	CSMA/CA does not deal with the recovery of the collision.
Wired installation is used in a CSMA/CD to detect the collision.	Wireless installation is used in a CSMA/CA as it avoids the collision. Therefore, it does not need a wired network.
An 802.3 Ethernet network uses CSMA/CD.	An 802.11 ethernet network uses CSMA/CA.
CSMA/CD takes effect after the occurrence of a collision.	CSMA/CA takes effect before the occurrence of a collision.

18) What is the purpose of Data Link Layer?

The main purpose of the data link layer is to check that whether messages are sent to the right devices. Another function of the data link layer is framing.

---

19) What is VLAN?

VLAN stands for Virtual Local Area Network.

---

20) What is the subnet? Why is it used?

Subnets are used in IP network to break up the larger network into the smaller network. It is used to optimize the performance of the network because it reduces traffic by breaking the larger network into smaller networks. It is also used to identify and isolate network's problem and simplify them.

---

21) What is the difference between communication and transmission?

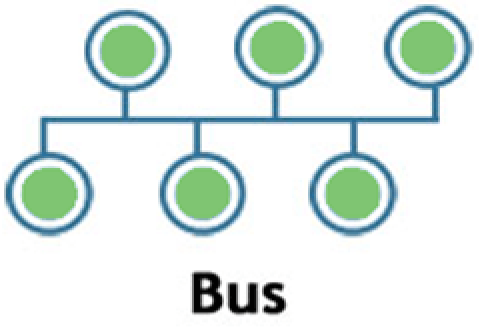
Communication is a process of sending and receiving data from an externally connected data cable whereas transmission is a process of transmitting data from source to destination.

---

22) What is Topology in CCNA?

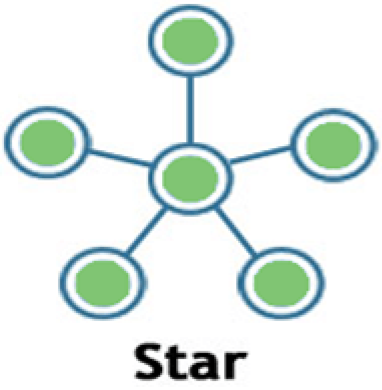
Topology is an arrangement of various elements (links, nodes, etc.) of a computer network in a specific order. These are the different types of topology used in CCNA:

Bus:



- Bus topology is a network topology in which all the nodes are connected to a single cable known as a central cable or bus.
- It acts as a shared communication medium, i.e., if any device wants to send the data to other devices, then it will send the data over the bus which in turn sends the data to all the attached devices.
- Bus topology is useful for a small number of devices. As if the bus is damaged then the whole network fails.

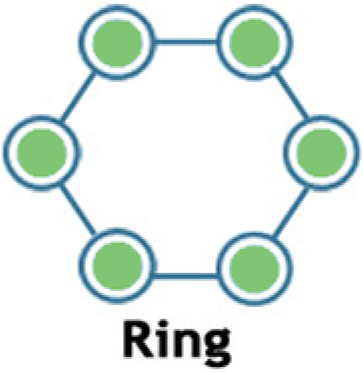
Star:



- Star topology is a network topology in which all the nodes are connected to a single device known as a central device.
- 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 connected to this cable.
- If the central device is damaged, then the whole network fails.
- Star topology is very easy to install, manage and troubleshoot.

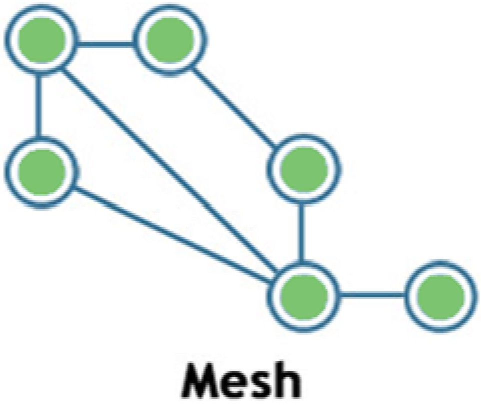
- Star topology is commonly used in office and home networks.

Ring:



- 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.
- It does not need any central server to control the connectivity among the nodes.
- If the single node is damaged, then the whole network fails.
- Ring topology is very rarely used as it is expensive, difficult to install and manage.
- Examples of Ring topology are SONET network, SDH network, etc.

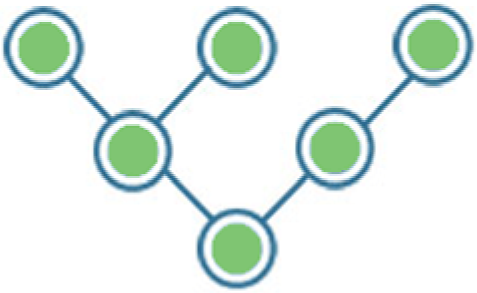
Mesh:



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

- It does not need any central switch or hub to control the connectivity among the nodes.
- Mesh topology is categorized into two parts:
  - **Fully connected mesh topology**: In this topology, all the nodes are connected to each other.
  - **Partially connected mesh topology**: In this topology, all the nodes are not connected to each other.
- It is a robust as a failure in one cable will only disconnect the specified computer connected to this cable.
- Mesh topology is rarely used as installation and configuration are difficult when connectivity gets more.
- Cabling cost is high as it requires bulk wiring.

Tree:



Tree

- Tree topology is a combination of star and bus topology. It is also known as the expanded star topology.
- In tree topology, all the star networks are connected to a single bus.
- Ethernet protocol is used in this topology.
- In this, the whole network is divided into segments known as star networks which can be easily maintained. If one segment is damaged, but there is no effect on other segments.
- Tree topology depends on the "main bus," and if it breaks, then the whole network gets damaged.

Hybrid:

- A hybrid topology is a combination of different topologies to form a resulting topology.
- If star topology is connected with another star topology, then it remains star topology. If star topology is connected with different topology, then it becomes a Hybrid topology.
- It provides flexibility as it can be implemented in a different network environment.
- The weakness of a topology is ignored, and only strength will be taken into consideration.

---

23) What is the passive topology in CCNA?

When the topology enables the computers on the network only to listen and receive the signals, it is known as passive topology because they don't amplify the signals anyway.

---

24) What is RAID in CCNA?

RAID stands for Redundant Array of Independent Disks. RAID is a method which is used to standardize and categorize fault-tolerant disk systems. RAID levels provide various facilities like performance, cost, reliability, etc. These three are the mostly used RAID levels:

- Level 0: (Striping)
- Level 1: (Mirroring)
- Level 5: (Striping and Parity)

---

25) What is the point-to-point protocol in CCNA?

The point-to-point protocol is an industry standard suite of protocols which uses the point-to-point link to transport multiprotocol datagram. The point-to-point protocol is a WAN protocol used at layer 2 to encapsulate the frames for the data transmission over the physical layer.

Following are the features that point-to-point protocol provides:

- **Link quality management**: It is a technique to monitor the quality of a link. If it finds any error in a link, then the link is shut down.

- The point-to-point protocol also provides authentication.
- It provides some essential features such as authentication, error detection, link quality monitoring, load balancing, compression, etc.

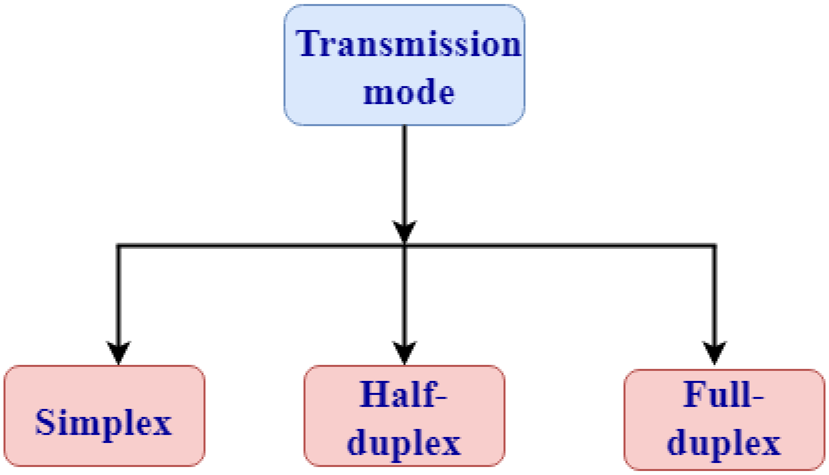
Components of a point-to-point protocol are:

- **Encapsulation**: Point-to-point protocol encapsulates the network packets in its frames using HDLC protocol. This makes the PPP layer three layer independent.
- **Link Control Protocol**: Link Control Protocol is used for establishing, configuring and testing the data link over internet connections.
- **Network Control Protocol**: Point-to-point protocol is used in a data link layer in the OSI reference model. The data comes from the upper layer, i.e., transport layer or network layer is fully compatible with PPP due to the presence of a Network control protocol.

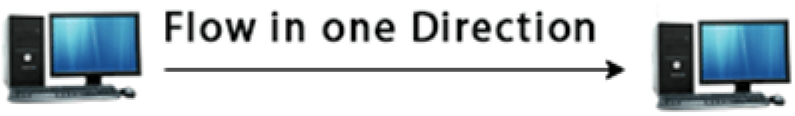
26) What are the possible ways of data transmission in CCNA?

Simplex, half-duplex and full-duplex are the communication channels used to convey the information. Either the communication channel can be a physical medium or logical medium.

These are the three possible ways of data transmission:

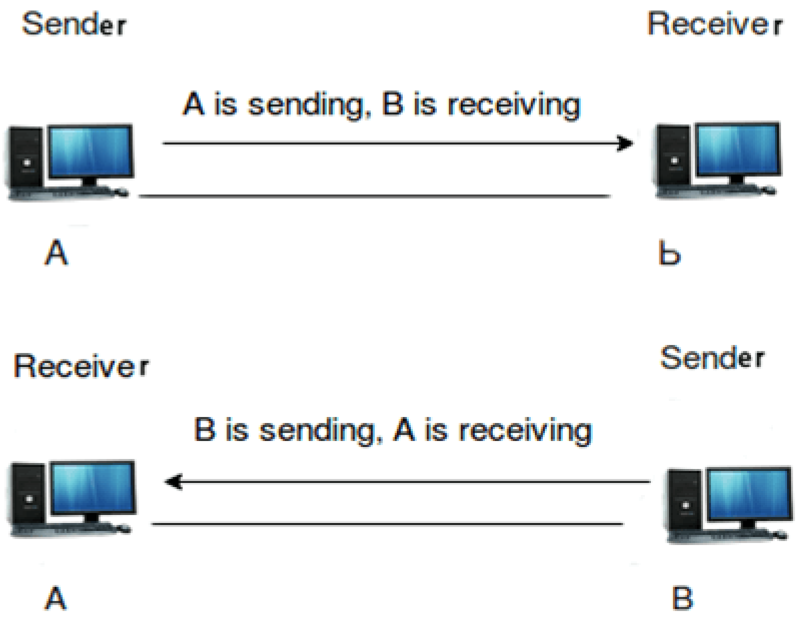


Simplex



- The simplex communication channel sends the data only in one direction.
- Example of the simplex communication channel is a radio station. The radio station transmits the signal while the other receives the signal.
- In simplex mode, entire bandwidth can be utilized for the data transmission as a flow of data is in one direction.

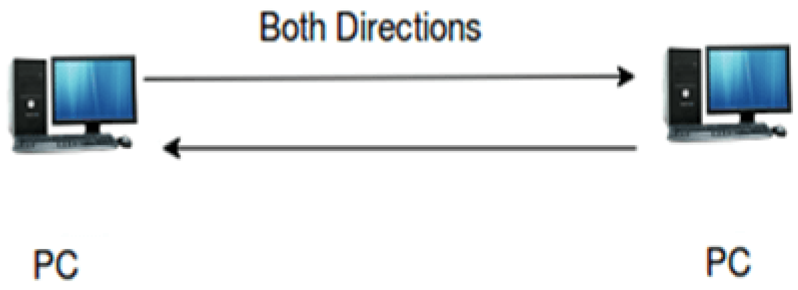
Half-duplex



- The half-duplex communication channel sends the information in both the directions but not at the same time.
- Performance of half-duplex is better than the simplex communication channel as the data flows in both the directions.
- Example of the half-duplex communication channel is "walkie-talkie". In "walkie-talkie", both the transmitter and receiver can communicate with each other on the same channel.

- In half-duplex mode, entire bandwidth can be used by the transmitter when the message is sent over the communication channel.

Full-duplex



- The full-duplex communication channel can send the information in both the directions at the same time.
- Performance of full-duplex is better than the half-duplex communication channel as the data flows in both the direction at the same time.
- Example of a full-duplex communication channel is "telephone". In the case of telephone, one can speak and hear at the same time. Therefore, this channel increases the efficiency of communication.

27) What are the protocol data units (PDU) in CCNA?

Protocol data units (PDU) are the minimum possible units used at different layers of the OSI model to transport data.

Layers	PDU
Transport	Segments
Network	Packets/Datagrams
Data-link	Frames
Physical	Bits

28) What is the difference between RIP and IGRP?

Following are the differences between RIP and IGRP:

Basis of Comparison	RIP	IGRP
Full form	RIP stands for routing information protocol.	IGRP stands for interior gateway routing protocol.
Description	RIP is a distance vector-based routing protocol.	IGRP is a distance vector based interior gateway routing protocol.
Determination of route	RIP depends on the number of hops to determine the best route to the network.	IGRP considers many factors before decides the best route to take, i.e., bandwidth, reliability, MTU and hops count.
Standard	RIP is a industry standard dynamic protocol.	IGRP is a Cisco standard dynamic protocol.
Organization used	RIP is mainly used for smaller sized organizations.	IGRP is mainly used for medium to large-sized organizations.
Maximum routers	It supports maximum 15 routers.	It supports a maximum 255 routers.
Symbol used	RIP is denoted by 'R' in the routing table.	IGRP is denoted by 'I' in the routing table.
Administrative distance	The administrative distance of RIP is 120.	The administrative distance of IGRP is 100.
Algorithm	RIP works on Bellman ford Algorithm.	IGRP works on Bellman ford Algorithm.

29) What are the different memories used in a CISCO router?

Three types of memories are used in a CISCO router:

- **NVRAM**
    - NVRAM stands for Non-volatile random access memory.
    - It is used to store the startup configuration file.
    - NVRAM retains the configuration file even if the router shut down.
- **DRAM**
    - DRAM stands for dynamic random access memory.
    - It stores the configuration file that is being executed.
    - DRAM is used by the processor to access the data directly rather than accessing it from scratch.
    - DRAM is located near the processor that provides the faster access to the data than the storage media such as hard disk.
    - Simple design, low cost, and high speed are the main features of DRAM memory.
    - DRAM is a volatile memory.
- **Flash Memory**
    - It is used to store the system IOS.
    - Flash memory is used to store the ios images.
    - Flash memory is erasable and reprogrammable ROM.
    - The capacity of the flash memory is large enough to accommodate many different IOS versions.

---

30) What is the difference between full-duplex and half-duplex?

Following are the differences between half-duplex and full-duplex

Basis of Comparison	Half-duplex	Full-duplex
Direction of communication	Communication is bi-directional but not at the same time.	Communication is bi-directional and done at the same time.
Send/receive	A sender can send as well as receive the data but not at the same time.	A sender can send as well as receive the data simultaneously.

Performance	Performance of half-duplex mode is not as good as a full-duplex mode.	Performance of full-duplex mode is better than the half-duplex mode.
Example	Example of half-duplex is a walkie-talkie.	Example of full-duplex is a telephone.

31) What is BootP?

BootP is a short form of Boot Program. It is a protocol that is used to boot diskless workstation connected to the network. BootP is also used by diskless workstations to determine its IP address and also the IP addresses of server PC.

32) What is a Frame Relay?

Frame Relay is used to provide connection-oriented communication by creating and maintaining virtual circuits. It is a WAN protocol that is operated at the Data Link and physical layer to sustain high-performance rating.

How frame relay works.

Frame relay multiplexes the traffic coming from different connections over a shared physical medium using special purpose hardware components such as routers, bridges, switch that packages the data into a frame relay messages. It reduces the network latency, i.e., the number of delays. It also supports the variable sized packet for the efficient utilization of network bandwidth.

33) What is Latency?

Latency is the amount of time delay. It is measured as the time difference between at the point of time when a network receives the data, and the time it is sent by another network.

34) What is the MAC address?

MAC address stands for Media Access Control address. This is an address of a device which is identified as the Media Access Control Layer in the network architecture. The MAC address is unique and usually stored in ROM.

35) What is the difference between ARP and RARP?

ARP stands for Address Resolution Protocol. ARP is a protocol that is used to map an IP address to a physical machine address.

RAPR stands for Reverse Address Resolution Protocol. RARP is a protocol that is used to map a MAC address to IP address.

Following are the differences between ARP and RARP:

Basis of Compariso n	ARP	RARP
Full form	Full form of ARP is address resolution protocol.	Full form of RARP is reverse address resolution protocol.
Description	ARP contains the logical address, and it retrieves the physical address of the receiver.	RARP includes the physical address and retrieves the logical address of a computer from the server.
Mapping	ARP is used to map 32-bit logical address to 48-bit physical address.	RARP is used to map 48-bit physical address to 32-bit logical address.

36) What is the size of an IP address?

The size for IPv4 is 32 bits and 128 bits for IPv6.

37) What is Ping? What is the usage of Ping?

PING stands for Packet Internet Groper. It is a computer network tool which is used to test whether a particular host is reachable across an IP address or not.

38) What is the checksum?

The checksum is a simple error detection scheme in which each transmitted message is accompanied by a numerical value based on the number of set bits in the message.

39) What are the different types of the password used in securing a Cisco router?

There are five types of passwords can be set on a Cisco router:

- Consol
- Aux
- VTY
- Enable Password
- Enable Secret

40) What is the usage of Service Password Encryption?

Service Password Encryption command is used to encrypt all passwords on your router to hide from your running config.

Networking Interview Questions

A list of top frequently asked **networking interview questions** and answers are given below

1) What is the network?

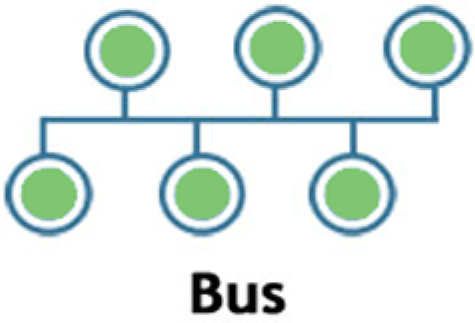
- A network is a set of devices that are connected with a physical media link. In a network, two or more nodes are connected by a physical link or two or more networks are connected by one or more nodes.
- A network is a collection of devices connected to each other to allow the sharing of data.
- Example of a network is an internet. An internet connects the millions of people across the world.

---

2) What do you mean by network topology?

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

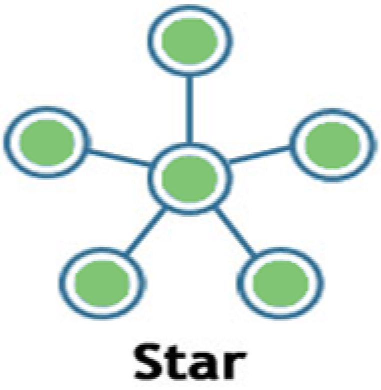
Bus:



- Bus topology is a network topology in which all the nodes are connected to a single cable known as a central cable or bus.
- It acts as a shared communication medium, i.e., if any device wants to send the data to other devices, then it will send the data over the bus which in turn sends the data to all the attached devices.

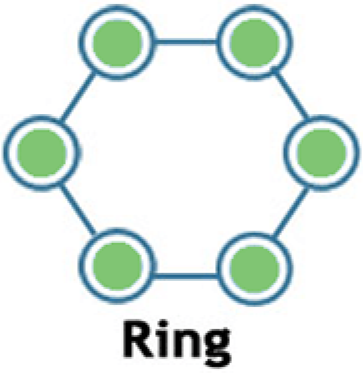
- Bus topology is useful for a small number of devices. As if the bus is damaged then the whole network fails.

Star:



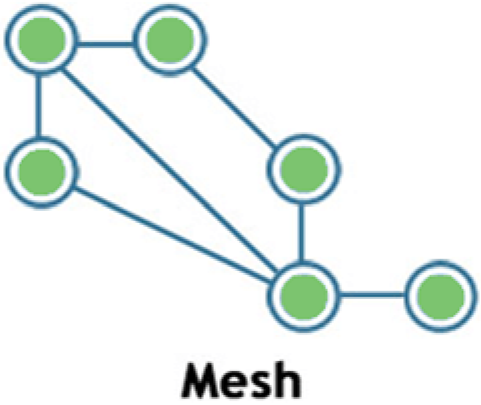
- Star topology is a network topology in which all the nodes are connected to a single device known as a central device.
- Star topology requires more cable compared to other topologies. Therefore, it is more robust as a failure in one cable will only disconnect a specific computer connected to this cable.
- If the central device is damaged, then the whole network fails.
- Star topology is very easy to install, manage and troubleshoot.
- Star topology is commonly used in office and home networks.

Ring



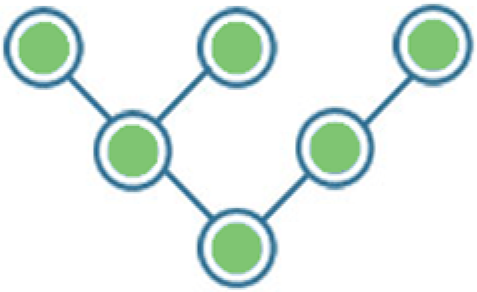
- Ring topology is a network topology in which nodes are exactly connected to two or more nodes and thus, forming a single continuous path for the transmission.
- It does not need any central server to control the connectivity among the nodes.
- If the single node is damaged, then the whole network fails.
- Ring topology is very rarely used as it is expensive, difficult to install and manage.
- Examples of Ring topology are SONET network, SDH network, etc.

Mesh



- Mesh topology is a network topology in which all the nodes are individually connected to other nodes.
- It does not need any central switch or hub to control the connectivity among the nodes.
- Mesh topology is categorized into two parts:
  - **Fully connected mesh topology**: In this topology, all the nodes are connected to each other.
  - **Partially connected mesh topology**: In this topology, all the nodes are not connected to each other.
- It is a robust as a failure in one cable will only disconnect the specified computer connected to this cable.
- Mesh topology is rarely used as installation and configuration are difficult when connectivity gets more.
- Cabling cost is high as it requires bulk wiring.

Tree



Tree

- Tree topology is a combination of star and bus topology. It is also known as the expanded star topology.
- In tree topology, all the star networks are connected to a single bus.
- Ethernet protocol is used in this topology.
- 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.
- Tree topology depends on the "main bus," and if it breaks, then the whole network gets damaged.

Hybrid

- A hybrid topology is a combination of different topologies to form a resulting topology.
- If star topology is connected with another star topology, then it remains a star topology. If star topology is connected with different topology, then it becomes a Hybrid topology.
- It provides flexibility as it can be implemented in a different network environment.
- The weakness of a topology is ignored, and only strength will be taken into consideration.

---

3) What are the advantages of Distributed Processing?

A list of advantages of distributed processing:

- Secure
- Support Encapsulation

- Distributed database
- Faster Problem solving
- Security through redundancy
- Collaborative Processing

---

4) What is the criteria to check the network reliability?

Network reliability: Network reliability means the ability of the network to carry out the desired operation through a network such as communication through a network.

Network reliability plays a significant role in the network functionality. The network monitoring systems and devices are the essential requirements for making the network reliable.The network monitoring system identifies the problems that are occurring in the network while the network devices ensure that data should reach the appropriate destination.

The reliability of a network can be measured by the following factors:

- **Downtime**: The downtime is defined as the required time to recover.
- **Failure Frequency**: It is the frequency when it fails to work the way it is intended.
- **Catastrophe**: It indicates that the network has been attacked by some unexpected event such as fire, earthquake.

---

5) Which are the different factors that affect the security of a network?

There are mainly two security affecting factors:

- Unauthorized Access
- Viruses

---

6) Which are the different factors that affect the reliability of a network?

The following factors affect the reliability of a network:

- Frequency of failure
- Recovery time of a network after a failure

7) Which are the different factors that affect the performance of a network?

The following factors affect the performance of a network:

- Large number of users
- Transmission medium types
- Hardware
- Software

8) What makes a network effective and efficient?

There are mainly two criteria which make a network effective and efficient:

- **Performance:** : performance can be measured in many ways like transmit time and response time.
- **Reliability:** reliability is measured by frequency of failure.
- **Robustness:** robustness specifies the quality or condition of being strong and in good condition.
- **Security:** It specifies how to protect data from unauthorized access and viruses.

9) What is bandwidth?

Every signal has a limit of upper range frequency and lower range frequency. The range of limit of network between its upper and lower frequency is called bandwidth.

10) What is a node and link?

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

11) What is a gateway? Is there any difference between a gateway and router?

A node that is connected to two or more networks is commonly known as a gateway. It is also known as a 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 and router:

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

12) What is DNS?

DNS is an acronym stands for Domain Name System.

- DNS was introduced by Paul Mockapetris and Jon Postel in 1983.
- It is a naming system for all the resources over the internet which includes physical nodes and applications. It is used to locate to resource easily over a network.
- DNS is an internet which maps the domain names to their associated IP addresses.
- Without DNS, users must know the IP address of the web page that you wanted to access.

Working of DNS:

If you want to visit the website of "javaTpoint", then the user will type "https://www.javatpoint.com" into the address bar of the web browser. Once the domain name is entered, then the domain name system 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.

13) What is DNS forwarder?

- A forwarder is used with 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.
- **Following are the ways that the DNS server behaves when it is configured as a forwarder**:
  - When the DNS server receives the query, then it resolves the query by using a cache.
  - If the DNS server is not able to resolve the query, then it forwards the query to another DNS server.
  - If the forwarder is not available, then it will try to resolve the query by using root hint.

---

14) What is 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.

---

15) What is the meaning of 10Base-T?

It is used to specify data transfer rate. In 10Base-T, 10 specify the data transfer rate, i.e., 10Mbps. The word Base specifies the baseband as opposed to broadband. T specifies the type of the cable which is a twisted pair.

---

16) What is NOS in computer networking?

- NOS stands for Network Operating System. It is specialized software which is used to provide network connectivity to a computer to make communication possible with other computers and connected devices.
- NOS is the software which allows the device to communicate, share files with other devices.

- The first network operating system was Novel NetWare released in 1983. Some other examples of NOS are Windows 2000, Windows XP, Linux, etc.

---

17) What are the different types of networks?

Networks can be divided on the basis of area of distribution. For example:

- **PAN (Personal Area Network)**: Its range limit is up to 10 meters. It is created for personal use. Generally, personal devices are connected to this network. For example computers, telephones, fax, printers, etc.
- **LAN (Local Area Network)**: It is used for a small geographical location like office, hospital, school, etc.
- **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.
- **CAN (Campus Area Network)**: It is a connection of devices within a campus area which links to other departments of the organization within the same campus.
- **MAN (Metropolitan Area Network)**: It is used to connect the devices which span to large cities like metropolitan cities over a wide geographical area.
- **WAN (Wide Area Network)**: It is used over a wide geographical location that may range to connect cities and countries.
- **GAN (Global Area Network)**: It uses satellites to connect devices over global are.

---

18) What is POP3?

POP3 stands for Post Office Protocol version3. POP is responsible for accessing the mail service on a client machine. POP3 works on two models such as Delete mode and Keep mode.

---

19) What do you understand by MAC address?

MAC stands for Media Access Control. It is the address of the device at the Media Access Control Layer of Network Architecture. It is a unique address means no two devices can have same MAC addresses.

---

20) What is IP address?

IP address is a unique 32 bit software address of a computer in a network system.

---

21) What is private IP address?

There are three ranges of IP addresses that have been reserved for IP addresses. They are not valid for use on the internet. If you want to access internet on these private IPs, you must have to use proxy server or NAT server.

---

22) What is public IP address?

A public IP address is an address taken by the Internet Service Provider which facilitates you to communication on the internet.

---

23) What is APIPA?

APIPA is an acronym stands for Automatic Private IP Addressing. This feature is generally found in Microsoft operating system.

---

24) What is the full form of ADS?

- ADS stands for Active Directory Structure.
- ADS is a microsoft technology used to manage the computers and other devices.
- ADS allows the network administrators to manage the domains, users and objects within the network.
- ADS consists of three main tiers:
    - **Domain**: Users that use the same database will be grouped into a single domain.
    - **Tree**: Multiple domains can be grouped into a single tree.
    - **Forest**: Multiple trees can be grouped into a single forest.

---

25) What is RAID?

RAID is a method to provide Fault Tolerance by using multiple Hard Disc Drives.

26) What is anonymous FTP?

Anonymous FTP is used to grant users access to files in public servers. Users which are allowed access to data in these servers do not need to identify themselves, but instead log in as an anonymous guest.

27) What is protocol?

A protocol is a set of rules which is used to govern all the aspects of information communication.

28) What are the main elements of a protocol?

The main elements of a protocol are:

- **Syntax**: It specifies the structure or format of the data. It also specifies the order in which they are presented.
- **Semantics**: It specifies the meaning of each section of bits.
- **Timing**: Timing specifies two characteristics: When data should be sent and how fast it can be sent.

29 What is the Domain Name System?

There are two types of client/server programs. First is directly used by the users and the second supports application programs.

The Domain Name System is the second type supporting program that is used by other programs such as to find the IP address of an e-mail recipient.

30) What is link?

A link is connectivity between two devices which includes the cables and protocols used in order to make communication between devices.

31) How many layers are in OSI reference model?

OSI reference model: OSI reference model is an ISO standard which defines a networking framework for implementing the protocols in seven layers. These seven layers can be grouped into three categories:

- **Network layer**: Layer 1, Layer 2 and layer 3 are the network layers.
- **Transport layer**: Layer 4 is a transport layer.
- **Application layer**. Layer 5, Layer 6 and Layer 7 are the application layers.

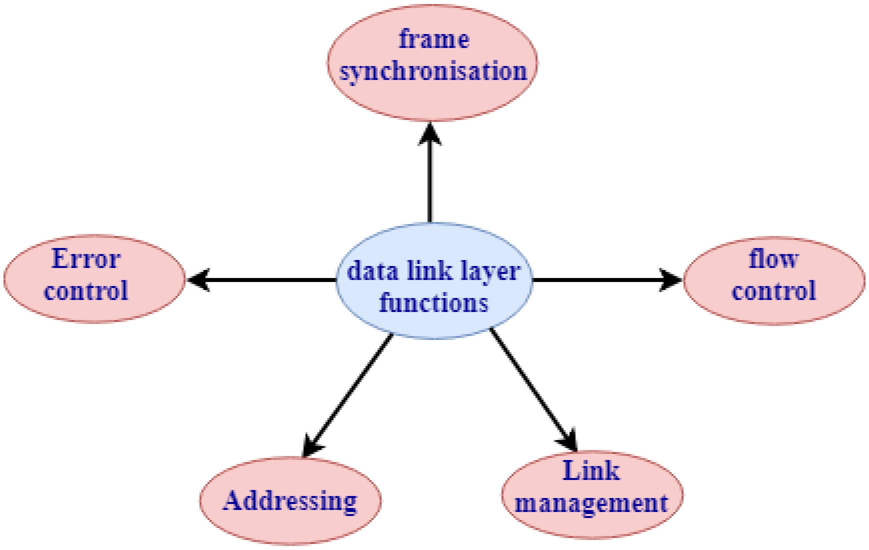
There are 7 layers in the OSI reference model.

1. Physical Layer

- It is the lowest layer of the OSI reference model.
- It is used for the transmission of an unstructured raw bit stream over a physical medium.
- Physical layer transmits the data either in the form of electrical/optical or mechanical form.
- The physical layer is mainly used for the physical connection between the devices, and such physical connection can be made by using twisted-pair cable, fibre-optic or wireless transmission media.

2. DataLink Layer

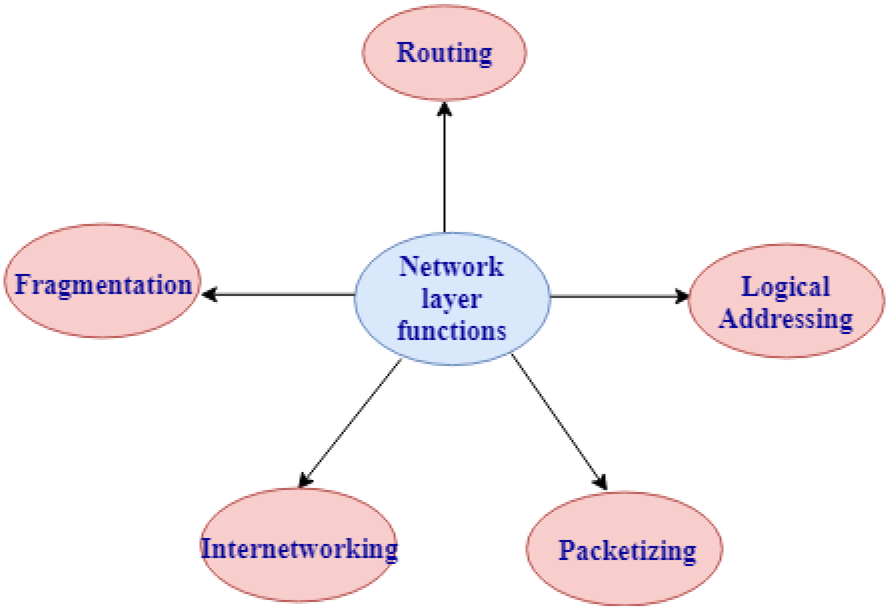
- It is used for transferring the data from one node to another node.
- It receives the data from the network layer and converts the data into data frames and then attach the physical address to these frames which are sent to the physical layer.
- It enables the error-free transfer of data from one node to another node.
  Functions of Data-link layer:



- **Frame synchronization**: Data-link layer converts the data into frames, and it ensures that the destination must recognize the starting and ending of each frame.
- **Flow control**: Data-link layer controls the data flow within the network.
- **Error control**: It detects and corrects the error occurred during the transmission from source to destination.
- **Addressing**: Data-link layer attach the physical address with the data frames so that the individual machines can be easily identified.
- **Link management**: Data-link layer manages the initiation, maintenance and, termination of the link between the source and destination for the effective exchange of data.

3. Network Layer

- Network layer converts the logical address into the physical address.
- It provides the routing concept means it determines the best route for the packet to travel from source to the destination.
  Functions of network layer:



- **Routing**: The network layer determines the best route from source to destination. This function is known as routing.
- **Logical addressing**: The network layer defines the addressing scheme to identify each device uniquely.
- **Packetizing**: The network layer receives the data from the upper layer and converts the data into packets. This process is known as packetizing.
- **Internetworking**: The network layer provides the logical connection between the different types of networks for forming a bigger network.
- **Fragmentation**: It is a process of dividing the packets into the fragments.

4. Transport Layer

- It delivers the message through the network and provides error checking so that no error occurs during the transfer of data.
- **It provides two kinds of services**:
  - **Connection-oriented transmission**: In this transmission, the receiver sends the acknowledgement to the sender after the packet has been received.
  - **Connectionless transmission**: In this transmission, the receiver does not send the acknowledgement to the sender.

5. Session Layer

- The main responsibility of the session layer is beginning, maintaining and ending the communication between the devices.

- Session layer also reports the error coming from the upper layers.
- Session layer establishes and maintains the session between the two users.

6. Presentation Layer

- The presentation layer is also known as a Translation layer as it translates the data from one format to another format.
- At the sender side, this layer translates the data format used by the application layer to the common format and at the receiver side, this layer translates the common format into a format used by the application layer.
  Functions of presentation layer:
  - Character code translation
  - Data conversion
  - Data compression
  - Data encryption

7. Application Layer

- Application layer enables the user to access the network.
- It is the topmost layer of the OSI reference model.
- Application layer protocols are file transfer protocol, simple mail transfer protocol, domain name system, etc.
- The most widely used application protocol is HTTP(Hypertext transfer protocol). A user sends the request for the web page using HTTP.

---

32) What is the usage of OSI physical layer?

The OSI physical layer is used to convert data bits into electrical signals and vice versa. On this layer, network devices and cable types are considered and setup.

---

33) Explain the functionality of OSI session layer?

OSI session layer provides the protocols and means for two devices on the network to communicate with each other by holding a session. This layer is responsible for setting up the session, managing information exchange during the session, and tear-down process upon termination of the session.

---

34) What is the maximum length allowed for a UTP cable?

The maximum length of UTP cable is 90 to 100 meters.

---

35) What is RIP?

- RIP stands for Routing Information Protocol. It is accessed by the routers to send data from one network to another.
- RIP is a dynamic protocol which is used to find the best route from source to the destination over a network by using the hop count algorithm.
- Routers use this protocol to exchange the network topology information.
- This protocol can be used by small or medium-sized networks.

---

36) What do you understand by TCP/IP?

TCP/IP is short for Transmission Control Protocol /Internet protocol. It is a set of protocol layers that is designed for exchanging data on different types of networks.

---

37) What is netstat?

The "netstat" is a command line utility program. It gives useful information about the current TCP/IP setting of a connection.

---

38) What do you understand by ping command?

The "ping" is a utility program that allows you to check the connectivity between the network devices. You can ping devices using its IP address or name.

---

39) What is Sneakernet?

Sneakernet is the earliest form of networking where the data is physically transported using removable media.

---

40) Explain the peer-peer process.

The processes on each machine that communicate at a given layer are called peer-peer process.

---

41) What is a congested switch?

A switch receives packets faster than the shared link. It can accommodate and stores in its memory, for an extended period of time, then the switch will eventually run out of buffer space, and some packets will have to be dropped. This state is called a congested state.

---

42) What is multiplexing in networking?

In Networking, multiplexing is the set of techniques that is used to allow the simultaneous transmission of multiple signals across a single data link.

---

43) What are the advantages of address sharing?

Address sharing provides security benefit instead of routing. That's because host PCs on the Internet can only see the public IP address of the external interface on the computer that provides address translation and not the private IP addresses on the internal network.

---

44) What is RSA Algorithm?

RSA is short for Rivest-Shamir-Adleman algorithm. It is mostly used for public key encryption.

---

45) How many layers are in TCP/IP?

There are basic 4 layers in TCP/IP:

1. Application Layer
2. Transport Layer

3. Internet Layer
4. Network Layer

46) What is the difference between the TCP/IP model and the OSI model?

Following are the differences between the TCP/IP model and OSI model:

TCP/IP model	OSI model
Full form of TCP is transmission control protocol.	Full form of OSI is Open System Interconnection.
TCP/IP has 4 layers.	OSI has 7 layers.
TCP/IP is more reliable than the OSI model.	OSI model is less reliable as compared to the TCP/IP model.
TCP/IP model uses horizontal approach.	OSI model uses vertical approach.
TCP/IP model uses both session and presentation layer in the application layer.	OSI Reference model uses separate session and presentation layers.
TCP/IP model developed the protocols first and then model.	OSI model developed the model first and then protocols.
In Network layer, TCP/IP model supports only connectionless communication.	In the Network layer, the OSI model supports both connection-oriented and connectionless communication.
TCP/IP model is a protocol dependent.	OSI model is a protocol independent.

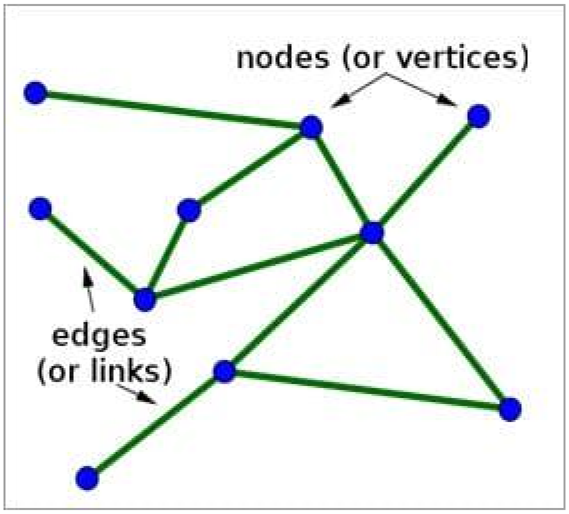
47) What is the difference between domain and workgroup?

Workgroup	Domain
A workgroup is a peer-to-peer computer network.	A domain is a Client/Server network.
A Workgroup can consist of maximum 10 computers.	A domain can consist up to 2000 computers.
Every user can manage the resources individually on their PCs.	There is one administrator to administer the domain and its resources.
All the computers must be on the same local area network.	The computer can be on any network or anywhere in the world.
Each computer must be changed manually.	Any change made to the computer will reflect the changes to all the computers.

Q #2) What is a Node?

Answer: Two or more computers are connected directly by an optical fiber or any other cable. A node is a point where a connection is established. It is a network component that is used to send, receive and forward the electronic information.

A device connected to a network is also termed as Node. Let's consider that in a network there are 2 computers, 2 printers, and a server connected, then we can say that there are five nodes on the network.



[image source]

Q #3) What is Network Topology?

Answer: Network topology is a physical layout of the computer network and it defines how the computers, devices, cables, etc are connected to each other.

Q #4) What are Routers?

Answer: The router is a network device that connects two or more network segments. It is used to transfer information from the source to the destination.

Routers send the information in terms of data packets and when these data packets are forwarded from one router to another router then the router reads the network address in the packets and identifies the destination network.

Q #5) What is the OSI reference model?

Answer: Open **S**ystem **I**nterconnection, the name itself suggests that it is a reference model that defines how applications can communicate with each other over a networking system.

It also helps to understand the relationship between networks and defines the process of communication in a network.

Q #6) What are the layers in OSI Reference Models? Describe each layer briefly.

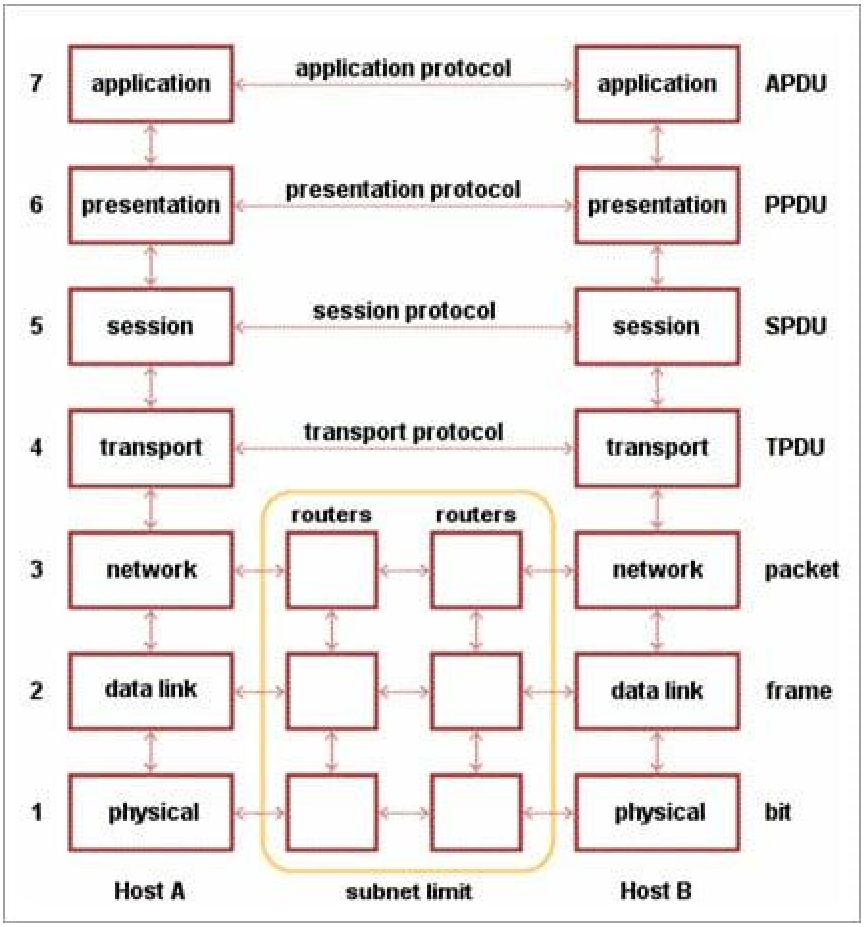
Answer: Given below are the seven layers of OSI Reference Models:

a) Physical Layer (Layer 1): It converts data bits into electrical impulses or radio signals. **<u>Example:</u>** Ethernet.

b) Data Link Layer (Layer 2): At the Data Link layer, data packets are encoded and decoded into bits and it provides a node to node data transfer. This layer also detects the errors that occurred at Layer 1.

c) Network Layer (Layer 3): This layer transfers variable length data sequence from one node to another node in the same network. This variable-length data sequence is also known as **“Datagrams”**.

d) Transport Layer (Layer 4): It transfers data between nodes and also provides acknowledgment of successful data transmission. It keeps track of transmission and sends the segments again if the transmission fails.



e) Session Layer (Layer 5): This layer manages and controls the connections between computers. It establishes, coordinates, exchange and terminates the connections between local and remote applications.

f) Presentation Layer (Layer 6): It is also called as “Syntax Layer”. Layer 6 transforms the data into the form in which the application layer accepts.

g) Application Layer (Layer 7): This is the last layer of the OSI Reference Model and is the one that is close to the end-user. Both end-user and application layer interacts with the software application. This layer provides services for email, file transfer, etc.

Q #7) What is the difference between Hub, Switch, and Router?

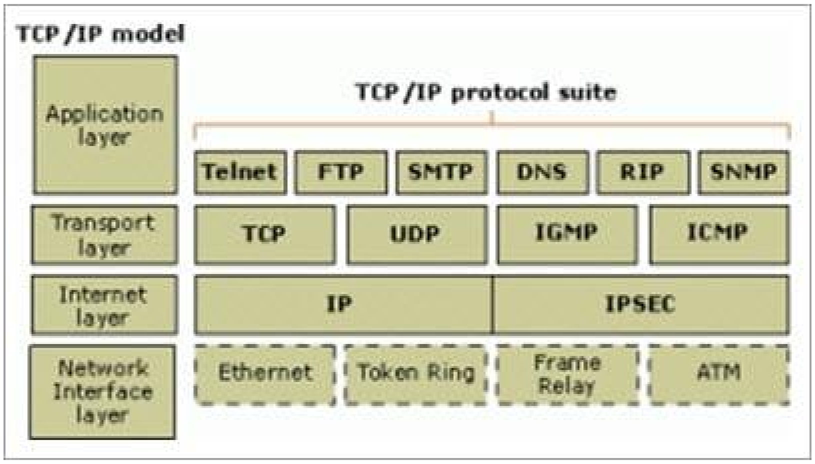
Answer:

Hub	Switch	Router
Hub is least expensive, least intelligent and least complicated of the three. It broadcast all data to every port which may cause serious security and reliability concern	Switches work similarly like Hubs but in a more efficient manner. It creates connections dynamically and provides information only to the requesting port	The router is smartest and most complicated out of these three. It comes in all shapes and sizes. Routers are similar like little computers dedicated for routing network traffic
In a Network, Hub is a common connection point for devices connected to the network. Hub contains multiple ports and is used to connect segments of LAN	Switch is a device in a network which forwards packets in a network	Routers are located at gateway and forwards data packets

Q #8) Explain TCP/IP Model

Answer: The most widely used and available protocol is TCP/IP i.e. Transmission Control Protocol and Internet Protocol. TCP/IP specifies how data should be packaged, transmitted and routed in their end to end data communication.

There are four layers as shown in the below diagram:



Given below is a brief explanation of each layer:

- **Application Layer**: This is the top layer in the TCP/IP model. It includes processes that use the Transport Layer Protocol to transmit the data to their destination. There are different Application Layer Protocols such as HTTP, FTP, SMTP, SNMP protocols, etc.
- **Transport Layer**: It receives the data from the Application Layer which is above the Transport Layer. It acts as a backbone between the host's system connected with each other and it mainly concerns about the transmission of data. TCP and UDP are mainly used as Transport Layer protocols.
- **Network or Internet Layer**: This layer sends the packets across the network. Packets mainly contain source & destination IP addresses and actual data to be transmitted.
- **Network Interface Layer**: It is the lowest layer of the TCP/IP model. It transfers the packets between different hosts. It includes encapsulation of IP packets into frames, mapping IP addresses to physical hardware devices, etc.

Q #9) What is HTTP and what port does it use?

Answer: HTTP is HyperText Transfer Protocol and it is responsible for web content. Many web pages are using HTTP to transmit the web content and allow the display and navigation of HyperText. It is the primary protocol and port used here is TCP port 80.

Q #10) What is HTTPs and what port does it use?

Answer: HTTPs is a Secure HTTP. HTTPs is used for secure communication over a computer network. HTTPs provides authentication of websites that prevents unwanted attacks.

In bi-directional communication, the HTTPs protocol encrypts the communication so that the tampering of the data gets avoided. With the help of an SSL certificate, it verifies if the requested server connection is a valid connection or not. HTTPs use TCP with port 443.

Q #11) What are TCP and UDP?

Answer: Common factors in TCP and UDP are:

- TCP and UDP are the most widely used protocols that are built on the top of the IP protocol.
- Both protocols TCP and UDP are used to send bits of data over the Internet, which is also known as 'packets'.
- When packets are transferred using either TCP or UDP, it is sent to an IP address. These packets are traversed through routers to the destination.

The difference between TCP and UDP are enlisted in the below table:

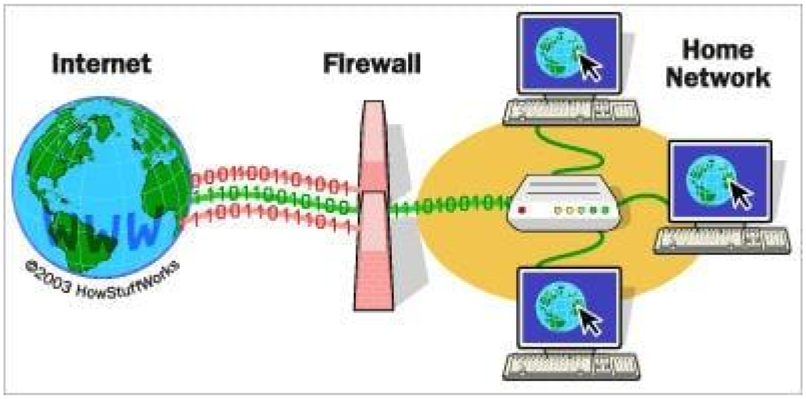
TCP	UDP
TCP stands for Transmission Control Protocol	UDP is stands for User Datagram Protocol or Universal Datagram Protocol
Once the connection is setup, data can be sent bi-directional i.e. TCP is a connection oriented protocol	UDP is connectionless, simple protocol. Using UDP, messages are sent as packets
The speed of TCP is slower than UDP	UDP is faster compared to TCP
TCP is used for the application where time is not critical part of data transmission	UDP is suitable for the applications which require fast transmission of data and time is crucial in this case.
TCP transmission occurs in a sequential manner	UDP transmission also occurs in a sequential manner but it does not maintain the same sequence when it reaches the destination
It is heavy weight connection	It is lightweight transport layer

TCP tracks the data sent to ensure no data loss during data transmission	UDP does not ensure whether receiver receives packets are not. If packets are misses then they are just lost

Q #12) What is a Firewall?

Answer: Firewall is a network security system that is used to protect computer networks from unauthorized access. It prevents malicious access from outside to the computer network. A firewall can also be built to grant limited access to outside users.

The firewall consists of a hardware device, software program or a combined configuration of both. All the messages that route through the firewall are examined by specific security criteria and the messages which meet the criteria are successfully traversed through the network or else those messages are blocked.



[image source]

Firewalls can be installed just like any other computer software and later can be customized as per the need and have some control over the access and security features. “

Windows Firewall” is an inbuilt Microsoft Windows application that comes along with the operating system. This “Windows Firewall” also helps to prevent viruses, worms, etc.

Q #13) What is DNS?

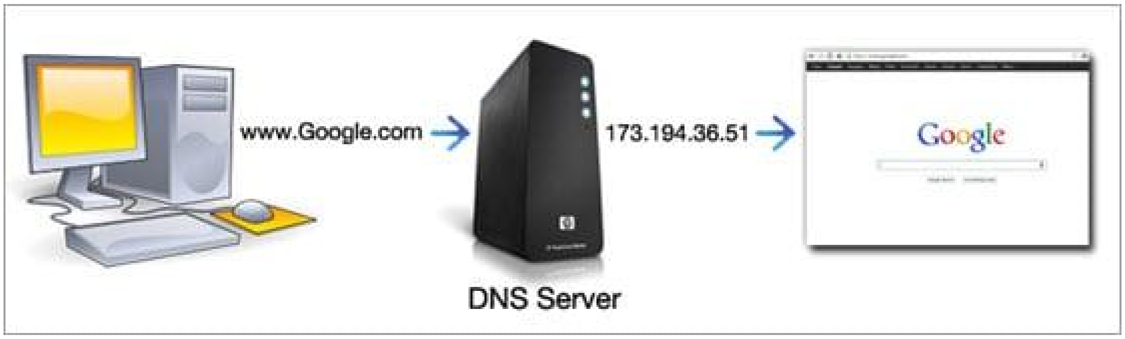
Answer: Domain Name Server (DNS), in a non-professional language and we can call it an Internet’s phone book. All the public IP addresses and their hostnames are stored in the DNS and later it translates into a corresponding IP address.

For a human being, it is easy to remember and recognize the domain name, however, the computer is a machine that does not understand the human language and they only understand the language of IP addresses for data transfer.

There is a “Central Registry” where all the domain names are stored and it gets updated on a periodic basis. All Internet service providers and different host companies usually interact with this central registry to get the updated DNS details.

<u>For Example</u>, When you type a website www.softwaretestinghelp.com, then your Internet service provider looks for the DNS associated with this domain name and translates this website command into a machine language – IP address – 151.144.210.59 (note that, this is the imaginary IP address and not the actual IP for the given website) so that you will get redirected to the appropriate destination.

This process is explained in the below diagram:



[image source]

Q #14) What is the difference between a Domain and a Workgroup?

Answer: In a computer network, different computers are organized in different methods and these methods are – Domains and Workgroups. Usually, computers which run on the home network belong to a Workgroup.

However, computers that are running on an office network or any workplace network belong to the Domain.

Their differences are as follows:

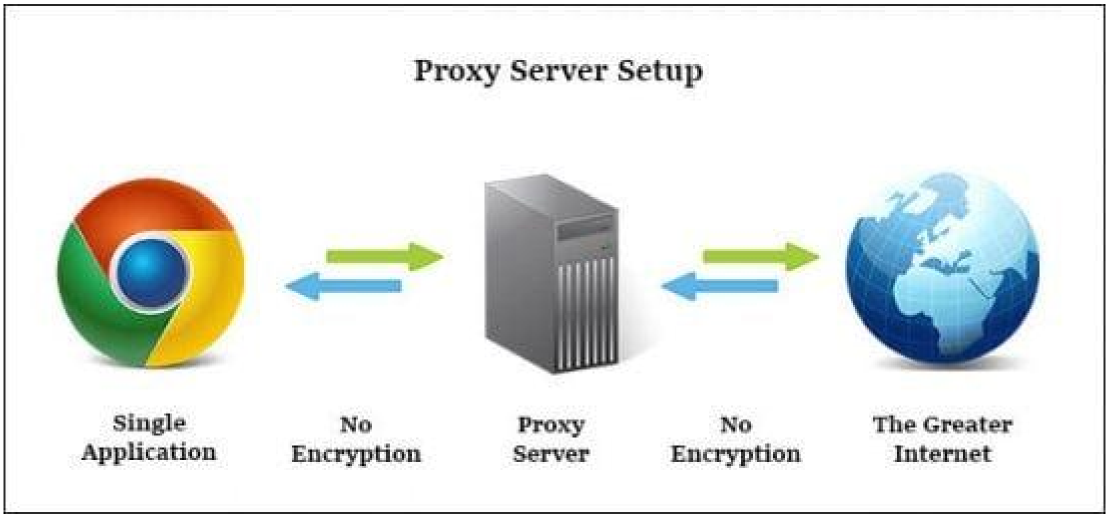
Workgroup	Domain
All computers are peers and no computer has control over another computer	Network admin uses one or more computer as a server and provide all accesses, security permission to all other computers in a network

In a Workgroup, each computer maintains their own database	The domain is a form of a computer network in which computers, printers, and user accounts are registered in a central database.
Each computer has their own authentication rule for every user account	It has centralized authentication servers which set the rule of authentication
Each computer has set of user account. If user has account on that computer then only user able to access the computer	If user has an account in a domain then user can login to any computer in a domain
Workgroup does not bind to any security permission or does not require any password	Domain user has to provide security credentials whenever they are accessing the domain network
Computer settings need to change manually for each computer in a Workgroup	In a domain, changes made in one computer automatically made same changes to all other computers in a network
All computers must be on same local area network	In a domain, computers can be on a different local network
In a Workgroup, there can be only 20 computers connected	In a domain, thousands of computers can be connected

Q #15) What is a Proxy Server and how do they protect the computer network?

Answer: For data transmission, IP addresses are required and even DNS uses IP addresses to route to the correct website. It means without the knowledge of correct and actual IP addresses it is not possible to identify the physical location of the network.

Proxy servers prevent external users who are unauthorized to access such IP addresses of the internal network. It makes the computer network virtually invisible to external users.



Proxy Server also maintains the list of blacklisted websites so that the internal user is automatically prevented from getting easily infected by viruses, worms, etc.

Q #16) What are IP classes and how can you identify the IP class of given an IP address?

Answer: An IP address has 4 sets (octets) of numbers each with a value up to 255.

For Example, the range of the home or commercial connection started primarily between 190 x or 10 x. IP classes are differentiated based on the number of hosts it supports on a single network. If IP classes support more networks then very few IP addresses are available for each network.

There are three types of IP classes and are based on the first octet of IP addresses which are classified as Class A, B or C. If the first octet begins with 0 bit then it is of type Class A.

Class A type has a range up to 127.x.x.x (except 127.0.0.1). If it starts with bits 10 then it belongs to Class B. Class B having a range from 128.x to 191.x. IP class belongs to Class C if the octet starts with bits 110. Class C has a range from 192.x to 223.x.

Q #17) What is meant by 127.0.0.1 and localhost?

Answer: IP address 127.0.0.1, is reserved for loopback or localhost connections. These networks are usually reserved for the biggest customers or some of the original members of the Internet. To identify any connection issue, the initial step is to ping the server and check if it is responding.

If there is no response from the server then there are various causes like the network is down or the cable needs to be replaced or the network card is not in good condition. 127.0.0.1 is a loopback connection on the Network Interface Card (NIC) and if you are able to ping this server successfully, then it means that the hardware is in a good shape and condition.

127.0.0.1 and localhost are the same things in most of the computer network functioning.

Q #18) What is NIC?

Answer: NIC stands for Network Interface Card. It is also known as Network Adapter or Ethernet Card. It is in the form of an add-in card and is installed on a computer so that the computer can be connected to a network.

Each NIC has a MAC address which helps in identifying the computer on a network.

Q #19) What is Data Encapsulation?

Answer: In a computer network, to enable data transmission from one computer to another, the network devices send messages in the form of packets. These packets are then added with the IP header by the OSI reference model layer.

The Data Link Layer encapsulates each packet in a frame that contains the hardware address of the source and the destination computer. If a destination computer is on the remote network then the frames are routed through a gateway or router to the destination computer.

Q #20) What is the difference between the Internet, Intranet, and Extranet?

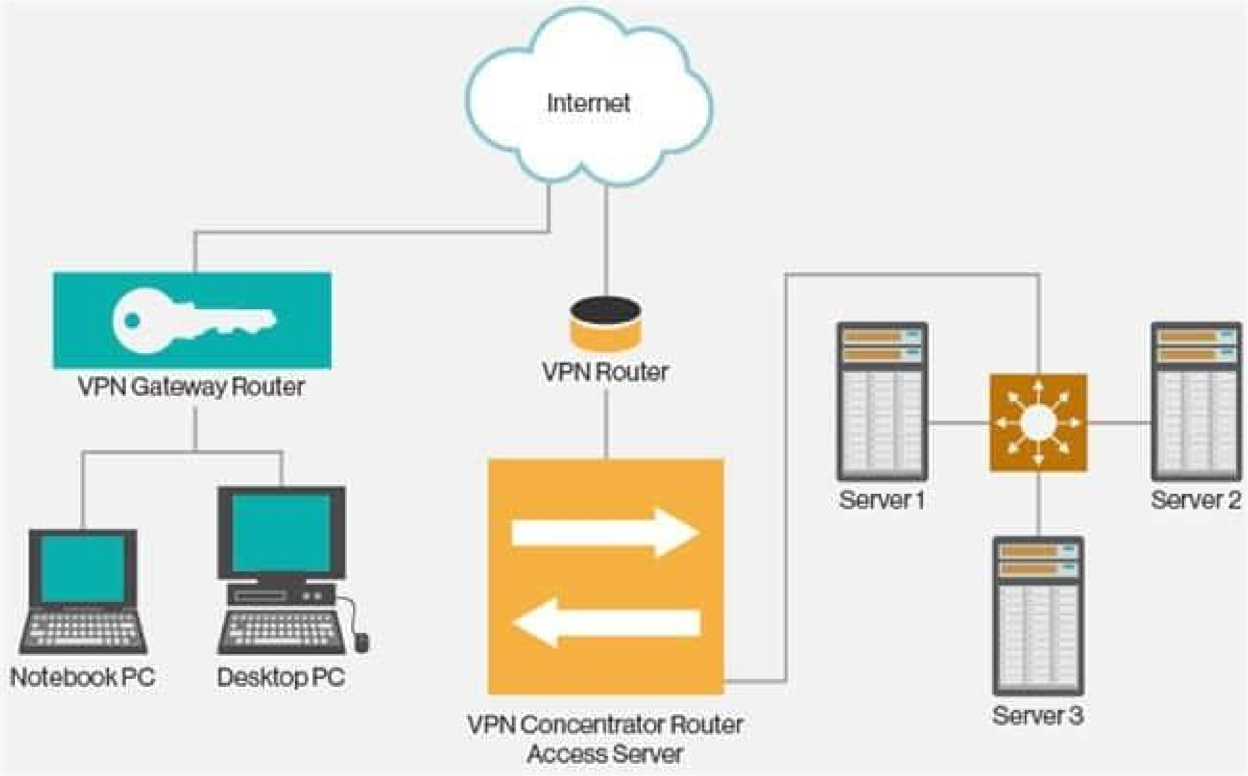
Answer: The terminologies Internet, Intranet, and Extranet are used to define how the applications in the network can be accessed. They use similar TCP/IP technology but differ in terms of access levels for each user inside the network and outside the network.

- **Internet**: Applications are accessed by anyone from any location using the web.
- **Intranet**: It allows limited access to users in the same organization.
- **Extranet**: External users are allowed or provided with access to use the network application of the organization.

Q #21) What is a VPN?

Answer: VPN is the Virtual Private Network and is built on the Internet as a private wide area network. Internet-based VPNs are less expensive and can be connected from anywhere in the world.

VPNs are used to connect offices remotely and are less expensive when compared to WAN connections. VPNs are used for secure transactions and confidential data can be transferred between multiple offices. VPN keeps company information secure against any potential intrusion.



[image source]

Given below are the 3 types of VPN's:

1. **Access VPN**: Access VPN's provide connectivity to mobile users and telecommuters. It is an alternative option for dial-up connections or ISDN connections. It provides low-cost solutions and a wide range of connectivity.
2. **Intranet VPN**: They are useful for connecting remote offices using shared infrastructure with the same policy as a private network.
3. **Extranet VPN**: Using shared infrastructure over an intranet, suppliers, customers, and partners are connected using dedicated connections.

Q #22) What are Ipconfig and Ifconfig?

Answer: Ipconfig stands for Internet Protocol Configuration and this command is used on Microsoft Windows to view and configure the network interface.

The command Ipconfig is useful for displaying all TCP/IP network summary information currently available on a network. It also helps to modify the DHCP protocol and DNS setting.

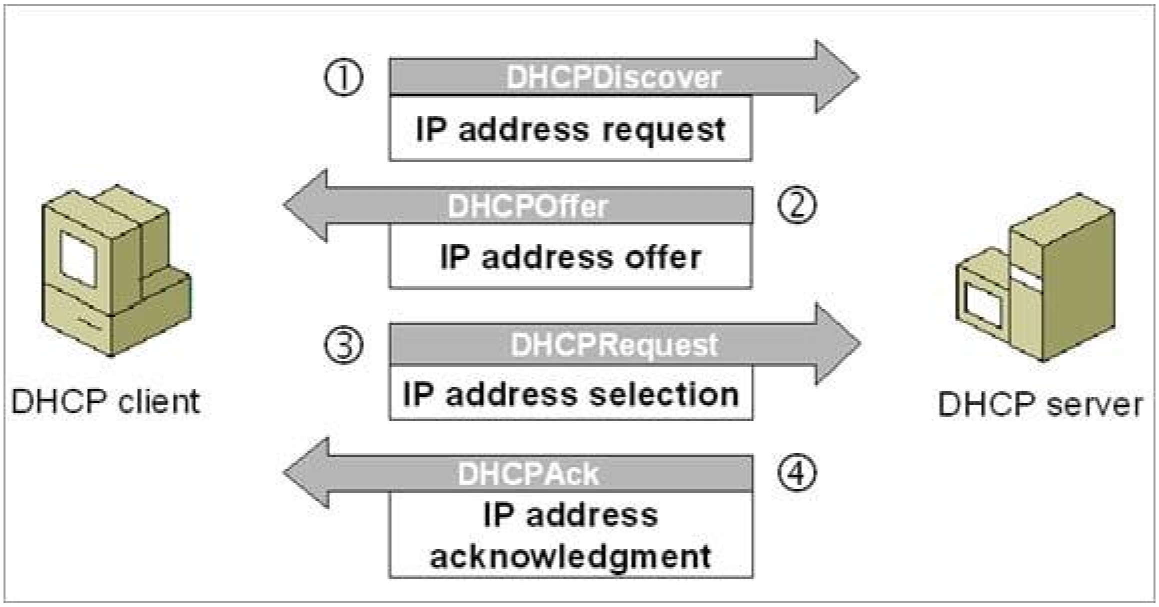
Ifconfig (Interface Configuration) is a command that is used on Linux, Mac, and UNIX operating systems. It is used to configure, control the TCP/IP network interface parameters from CLI i.e. Command Line Interface. It allows you to see the IP addresses of these network interfaces.

Q #23) Explain DHCP briefly?

Answer: DHCP stands for Dynamic Host Configuration Protocol and it automatically assigns IP addresses to the network devices. It completely removes the process of manual allocation of IP addresses and reduces the errors caused due to this.

This entire process is centralized so that the TCP/IP configuration can also be completed from a central location. DHCP has a “pool of IP addresses” from which it allocates the IP address to the network devices. DHCP cannot recognize if any device is configured manually and assigned with the same IP address from the DHCP pool.

In this situation, it throws the “IP address conflict” error.



[image source]

DHCP environment requires DHCP servers to set-up the TCP/IP configuration. These servers then assign, release and renew the IP addresses as there might be a chance that network devices can leave the network and some of them can join back to the network.