Q1. Differentiate between a router, a hub, and a switch.

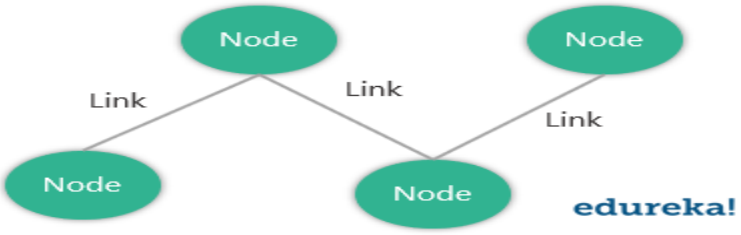
HUB	SWITCH	ROUTER
Connects two or more Ethernet devices	Connects two or more LAN devices	Can connect devices or a LAN and WAN
Does not perform filtering	Filters packets before forwarding them	Highly configured to filter and send packets
Least intelligent, least expensive and least complex	Similar to a hub, but more effective	Extremely smart and complex

Q2. What is a link?

A link basically is the connection between two or more computers or devices. It can be anything depending on whether it is a physical connection or a wireless one. Physical links include cables, hubs, switches, etc and wireless links wireless access points, routers, etc.

Q3. What do you mean by a Node?

The point of intersection in a network is called a Node. Nodes can send or receive data/ information within a network. For example, if two computers are connected to form a network, there are 2 nodes in that network. Similarly, in case there are computers, there will be three nodes and so on. It is not necessary for a node to be a computer, it can be any communicating device such as a printer, servers, modems, etc.



Q4. What does a backbone network mean?

In any system, backbone is the most principle component that supports all other components. Similarly, in networking, a Backbone Network is a Network that interconnects various parts of the network to which it belongs and has a high capacity connectivity infrastructure.

Q5. What is Network Topology?

The physical layout of the computer network is called as Network Topology. It gives the design of how all the devices are connected in a network.

Type	Description
Bus Topology	All the devices share a common communication line
Star Topology	All nodes are connected to a central hub device
Ring Topology	Each node connects to exactly two other nodes
Mesh Topology	Each node is connected to one or more nodes
Tree Topology (Hierarchical Topology)	Similar to star topology and inherits the bus topology
Daisy Chain Topology	All nodes are connected linearly
Hybrid Topology	Nodes are connected in more than one topology styles
Point-to-Point Topology	Connects two hosts such as computers, servers, etc

Q6. Explain what is LAN?

A LAN or Local Area Network the network between devices that are located within a small physical location. It can be either wireless or wired. One LAN differs from another based on the following factors:

- Topology: The arrangement of nodes within the network
- Protocol: Refer to the rules for the transfer of data
- Media: These devices can be connected using optic fibers, twisted-pair wires, etc

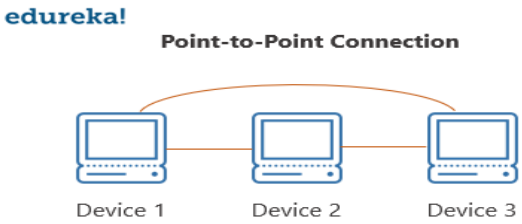
Q7. What are Routers?

A router is some device that transfers the data packets within a network. It basically performs the traffic directing functions within a network. A data packet can be anything such as an email, a web page, etc. Routers are located at the place where two or more networks meet or the gateways.

Routers can either be stand-alone devices or virtual. Stand-alone routers are traditional devices where as virtual routers are actually softwares that act like physical ones.

Q8. What is a Point-to-Point Network?

A Point-to-Point network refers to a physical connection between two nodes. It can be between any device of a network such as a computer, printer, etc.

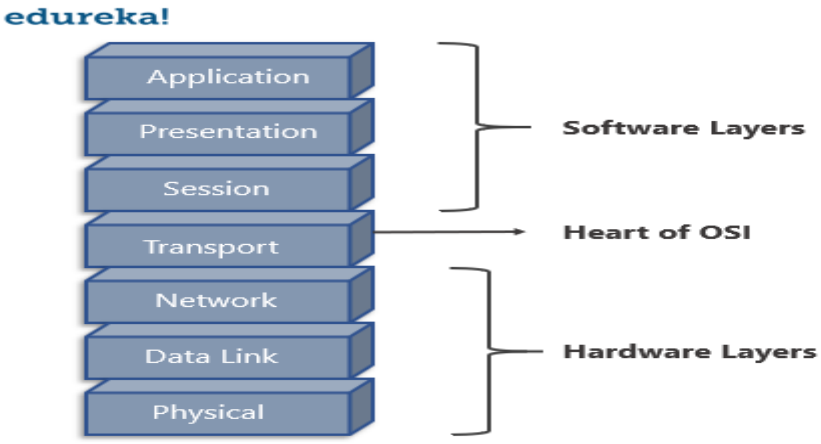


For example, as you can see in the above diagram, all the nodes are connected to each other i.e Device 1 is connected to Device 2 and Device 3 , Device 2 is connected to Device 3 and Device 1 and Device 3 is connected to Device 2 and Device 1 using physical links.

Q9. What is OSI Model?

OSI stands for Open Systems Interconnection. It is a conceptual model that standardizes communication functions of telecommunication. It has 7 layers which are:

1. Physical Layer
2. Data Link Layer
3. Network Layer
4. Transport Layer
5. Session Layer
6. Presentation Layer
7. Application Layer



Q10. Give a brief about each layer in the OSI Model.

Layer Name	Protocol	Description
Physical Layer	Symbol	Transfers raw bits of data over a physical link
Data Link Layer	Frame	Reliable transmission of data frames between nodes connected by the physical layer
Network Layer	Packet	Structures and manages a network with multiple nodes including addressing, routing and traffic control
Transport Layer	Segment, Datagram	Reliable Transmission of data packets between the different points of a network
Session Layer	Data	Manages the communication sessions
Presentation Layer	Data	Transmission of data between the service device and the application
Application Layer	Data	Specifies the shared communication protocols and the interface methods

Q11. What do you mean by anonymous FTP?

An anonymous FTP is a way of allowing a user to access data that is public. The user does not need to identify himself to the server and has to log in as anonymous.So in case you are asked to use anonymous ftp, make sure you add “anonymous” in place of your user id. Anonymous FTPs are very effective while distributing large files to a lot of people, without having to give huge numbers of usernames and password combinations.

Q12. What is the meaning of Network?

A network is a connection between different devices. These devices communicate with each other using physical or wireless connections. Physical connections include twisted pair cables, optic fibers, and coaxial cables..wireless networks can be established with the help of waves such as radio waves infrared waves and microwaves.

Networks basically serve many purposes such as:

- **Sharing hardware devices such as printers, input devices, etc**
- **Help in communications in many ways such as audios videos emails messages etc**
- **Help in sharing data and information using virtual devices**
- **They also help sharing softwares that are installed on other devices**

Q13. What do you mean by a Subnet Mask?

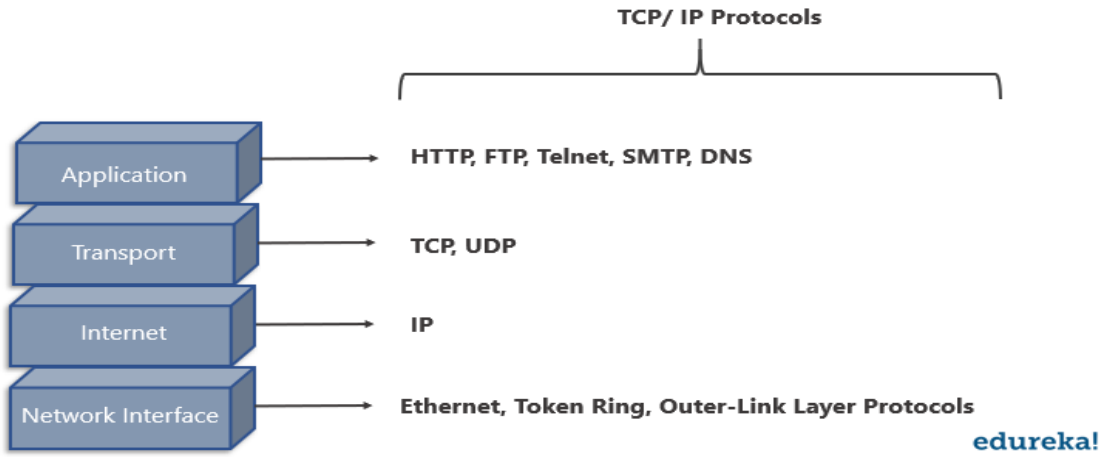
A Subnet Mask is the number describing the range of IP addresses that can be used within a network. They are used to assign subnetworks or subnets. These subnetworks are various LAN's connected to the internet.

This Subnet mask is basically a 32-bit number and it masks the IP address and then divides the IP address into two parts i.e the network address and the host address. Subnet Masks are created by setting all the network bits to "1" and all the host bits to "0"s. There are two network addresses that cannot be assigned to any host on the network i.e The "0" and "255" which are assigned to network and to the broadcast address, and this is why they cannot be assigned to any host.

Q14. Give a brief description of the TCP/ IP Model.

The TCP/ IP Model is a compressed version of the OSI Model. This Model contains 4 layers unlike the OSI Model which are:

1. **Process(Application Layer)**
2. **Host-to-Host(Transport Layer)**
3. **Internet Layer (Network Layer)**
4. **Network Access(Combination of Physical and Data Link Layer)**



Q15. What is the difference between the OSI Model and TCP/ IP Model?

TCP/ IP Model	OSI Model
Has four layers	Has seven layers
More reliable	Less reliable
No strict boundaries	Has strict boundaries
Horizontal Approach	Vertical Approach

Q16. What is a UTP cable?

A UTP cable is a 100 ohms cable made up of copper. It consists of 2-1800 unshielded twisted pairs that are surrounded by a non-metallic case. These twists provide immunity to electrical noise and EMI.

Q17. What is the maximum length allowed for a UTP cable?

The maximum length allowed for a UTP cable is 100m. This includes 90 m of solid cabling and 10m of standard patch cable.

Q18. Explain what is HTTP and which port does it use?

HTTP or HyperText Transfer Protocol allows communication over the Internet. This protocol basically defines how messages are to be transmitted and formatted over the world wide web. HTTP is a TCP/ IP protocol and it uses the port number 80.

Features of HTTP Protocol:

- It is connection-less
- Does not depend on the type of connecting media
- Stateless

Q19. What is NAT?

NAT stands for Network Address Translation. It deals with remapping one IP Address space with another by changing the IP headers of the packets that are being transmitted across a traffic routing device.

Q20. What is TCP?

TCP or Transmission Control Protocol is a connection-oriented protocol that establishes and maintains a connection between communicating devices until both of them are done exchanging messages. This protocol determines how application data can be broken down into packets that can be delivered over a network. It also sends and receives packets to and from the network layer and is in charge of flow control, etc.

Q21. Give a brief explanation about UDP?

UDP or the User Datagram Protocol is used to create a low-latency and loss-tolerating communications between applications connected over the internet. UDP enables process-to-process communication and communicates via datagrams or messages.

Q22. Differentiate between TCP and UDP.

Factor of comparison	TCP	UDP
Connection	Connection made before application messages are exchanged	Connection not made before application messages are exchanged
Use	For applications needing more reliability and less speed	For applications needing more speedy and less reliability
Use by Protocols of the Application Layer	File transfer, e-mail, etc	Multimedia, DNS
Reliability	Messages will be delivered in order and without errors	No guarantee that the messages will be delivered in order and without errors
Data Segments	Data segments rearranged in required order	All segments are independent, therefore has no inherent order specification
Acknowledgment	ACK is received	ACK is not received

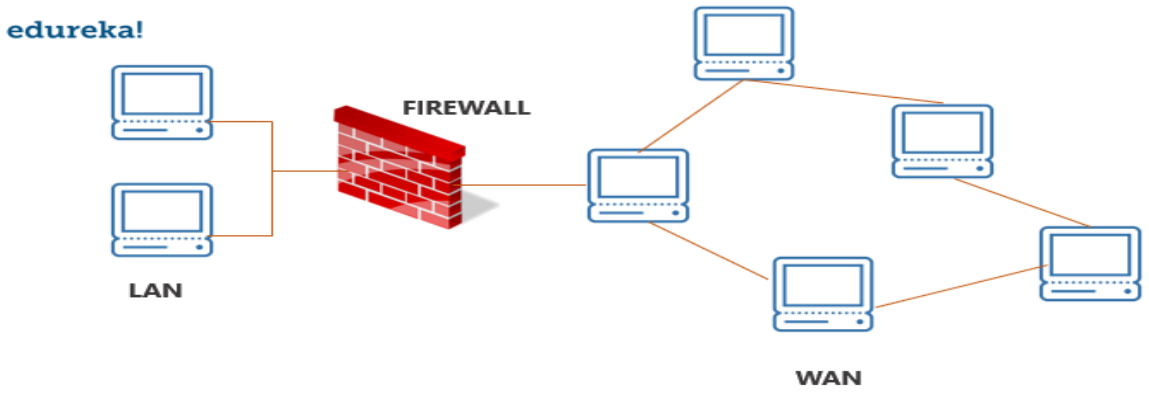
Flow Control	Has the congestion control mechanism	No flow control option
Check for Errors	Resends erroneous segments	Discards Erroneous segments

Q23. What is RIP?

RIP (Routing Information Protocol) is a dynamic routing protocol. It makes use of hop count as its primary metric to find the best path between the source and the destination. It works in the application layer and has an AD (Administrative Distance) value of 120.

Q24. Explain what is a firewall?

A firewall is a network security system which is used to monitor and control the network traffic based on some predefined rules. Firewalls are the first line of defense and establish barriers between the internal and external networks in order to avoid attack from untrusted external networks. Firewalls can be either hardware, software or sometimes both.



Q25. Explain what is NOS?

A Network Operating System (NOS) is an Operating System that is designed to support workstations, databases, personal computers, etc over a network. Some examples of NOS are MAC OS X, Linux, Windows Server 2008, etc. These Operating Systems provide various functionalities such as processor support, multiprocessing support, authentication, Web services, etc.