Networking interview questions

What is LAN?

LAN is a computer network that spans a relatively small area. Most LANs are confined to a single building or group of buildings. However, one LAN can be connected to other LANs over any distance via telephone lines and radio waves. A system of LANs connected in this way is called a wide-area network (WAN). Most LANs connect workstations and personal computers. Each node (individual computer) in a LAN has its own CPU with which it executes programs, but it also is able to access data and devices anywhere on the LAN. This means that many users can share expensive devices, such as laser printers, as well as data. Users can also use the LAN to communicate with each other, by sending e-mail or engaging in chat sessions.

What's the difference Between an Intranet and the Internet?

There's one major distinction between an intranet and the Internet: The Internet is an open, public space, while an intranet is designed to be a private space. An intranet may be accessible from the Internet, but as a rule it's protected by a password and accessible only to employees or other authorized users.

From within a company, an intranet server may respond much more quickly than a typical Web site. This is because the public Internet is at the mercy of traffic spikes, server breakdowns and other problems that may slow the network. Within a company, however, users have much more bandwidth and network hardware may be more reliable. This makes it easier to serve high-bandwidth content, such as audio and video, over an intranet.

Define the term Protocol.

Protocol is a standard way of communicating across a network. A protocol is the "language" of the network. It is a method by which two dissimilar systems can communicate. TCP is a protocol which runs over a network.

What is FTP (File Transfer Protocol)?

FTP is File Transfer Protocol. It used to exchange files on the internet. To enable the data transfer FTP uses TCP/IP, FTP is most commonly used to upload and download files from the internet. FTP can be invoked from the command prompt or some graphical user interface. FTP also allows to update (delete, rename, move, and copy) files at a server. It uses a reserved port no 21.

Explain the 7 Layers of OSI.

Layer 1: Physical layer
It represents all the electrical and physical specifications for devices.

Layer 2: Data link layer
It provides the functional and procedural means to transfer data between network entities and to detect and possibly correct errors that may occur in the Physical layer.

Layer 3: Network layer
The Network layer provides the functional and procedural means of transferring variable length data sequences from a source to a destination via one or more networks.

Layer 4: Transport layer
It provides transparent transfer of data between end users.

Layer 5: Session layer
It controls the sessions between computers. It connects, manages and terminates the connections between the local and remote application.

Layer 6: Presentation layer
It transforms data to provide a standard interface for the Application layer.

Layer 7: Application layer
It provides a means for the user to access information on the network through an application.

What is a network? What are the different kinds of network? Explain them

A network is a group of computers or nodes connected together. They are connected with each other by communication paths.

Types of Networks:

LAN – Local Area Network connects a group of nodes covering a small physical area. LAN's are most commonly seen in offices, building etc. LAN's enable higher transfer rate of data, smaller coverage of area and hence less wiring.

WAN – Wide Area Network connects a group of nodes covering a wide area. WAN typically connects and allow communication between regions or national boundaries. The most common example of WAN is internet.

VPN – Virtual Private Network connects or links nodes in some larger area by open connections or virtual circuits in some larger network (e.g., the Internet) instead of by physical wires. It is used for secure communication through the public internet. VPN alone may not support explicit security features, such as authentication or content encryption.

Intranet – It is a set of networks under the control of a single administrative person. It can be considered as an internal network of an organization. If it is large, web servers are used to provide information to the users.

Extranet – It is a network that restricts itself within a single organization. It can be categorized as WAN, MAN etc. however; it cannot have a single LAN. It must have a connection (at least one) with external network.

What are network topologies? Explain Ring, Bus and Star topology.

A network topology describes the layout of a network. It describes how different nodes and elements are connected to each other. Different types of topology:

a. Ring:-

All nodes connected with another in a loop.
Each device is connected to one or more another device on either side.

b. Bus

All nodes connected to a central and a common cable called as a back bone.
In bus topology, the server is at one end and the clients are connected at different positions across the network.
Easy to manage and install.
If the backbone fails, the entire communication fails.

c. Star

All nodes connected to a central hub.
The communication between the nodes is through the hub.
Relative requires more cables as compared to BUS. However if any node fails, it wont affect the entire LAN.

Explain IP, TCP and UDP.

TCP – Transmission control Protocol is used to establish communication between nodes or networks and exchange data packets. It guarantees delivery of data packets in the order they were sent. Hence it is most commonly used in all applications that require guaranteed delivery of data. It can handle both timeouts (if packets were delayed) and retransmission (if packets were lost). The stream of data is transmitted in segments. The segment header is 32 bit. it is a connectionless communication protocol at the third level (network) of the OSI model.

IP – Internet protocol is used for transmission of data over the internet. IP uses IP addresses to identity each machine uniquely. Message is sent using small packets. The packet contains both the sender and receivers address. IP does not guarantee the delivery in the same order as sent. This is because the packets are sent via different routes. It is a connectionless communication protocol at the third level (network) of the OSI model.

UDP – User Data Protocol is a communication protocol. It is normally used as an alternative for TCP/IP. However there are a number of differences between them. UDP does not divide data into packets. Also, UDP does not send data packets in sequence. Hence, the application program must ensure the sequencing. UDP uses port numbers to distinguish user requests. It also has a checksum capability to verify the data.

What is multicasting?

Multicasting allows a single message to be sent to a group of recipients. Emailing, teleconferencing, are examples of multicasting. It uses the network infrastructure and standards to send messages.

Explain the functionality of PING.

Ping Is particularly used to check if the system is in network or not. It also gives packet lost information. In windows ping command is written as ping ip_address. The output returns the data packets information. The number of packets sent, received and lost is returned by PING.

What is a MAC address?

A Media Access Control address is a unique identifier that is assigned to the network adapters or NICs by the manufacturers for the purpose of identification and used in the Media Access Control protocol sub layer. It is a 12 digit hexadecimal number. A MAC address usually encodes the registered identification of the manufacturer, if the address is assigned by the manufacturer. It some times also called as Ethernet Hardware Address / physical address/ adapter address.

Explain Spanning-Tree protocols.

Spanning Trees are a standard technique implemented in LAN connections. On a mesh topology, a set of spanning tree algorithms were developed for prevention of redundant transmission of data along intermediate hops between a source and a destination host. In the absence of spanning trees, a mesh network is flooded and rendered unusable by messages by circulating within a loop that is infinite, between hosts. An algorithm used in transparent bridges which determines the best path from source to destination to avoid bridge loops.

At the time of STP initialization in a network, its first action is to utilize the Spanning Tree Algorithm for selection of a root bridge and a root port. The root bridge is the network which has lowest-value bridge identifier. All the switches on the network use Bridge Protocol Data Units to broadcast the bridge IDs to the other switches in that network. Soon after selection of the root bridge, determination of the root ports on all other bridges is done.

What is the use of IGMP protocol?

Internet Group Management Protocol: - It allows internet hosts to participate in multicasting. The IGMP messages are used to learn which hosts is part of which multicast groups. The mechanism also allows a host to inform its local router that it wants to receive messages.

What are Ping and Tracert?

Ping and tracert are the commands used to send information to some remote computers to receive some information. Information is sent and received by

packets.

Ping I particularly used to check if the system is in network or not. It also gives packet lost information. In windows ping command is written as ping ip_address
Tracert is called as trace route. It is used to track or trace the path the packet takes from the computer where the command is given until the destination. In windows ping command is written as tracert ip_address

Explain RSVP. How does it work?

Resource Reservation protocol is used to reserve resources across a network. It is used for requesting a specific Quality of Service (QoS) from the network.

This is done by carrying the request (that needs a reservation of the resource) of the host throughout the network. It visits each node in the network. RSVP used two local modules for reservation of resources. Admission control module confirms if there are sufficient available resources while policy module checks for the permission of making a reservation. RSVP offers scalability. On a successful completion of both checks RSVP uses the packet classifier and packet scheduler for the desired Qos requested.

Explain the concept of DHCP.

Dynamic Host Configuration Protocol is used assigning IP addresses to computers in a network. The IP addresses are assigned dynamically. Certainly, using DHCP, the computer will have a different IP address every time it is connected to the network. In some cases the IP address may change even when the computer is in network. This means that DHCP leases out the IP address to the computer for sometime. Clear advantage of DHCP is that the software can be used to manage IP address rather than the administrator.

What are the differences between a domain and a workgroup?

In a domain, one or more computer can be a server to manage the network. On the other hand in a workgroup all computers are peers having no control on each other.

In a domain, user doesn't need an account to logon on a specific computer if an account is available on the domain. In a work group user needs to have an account for every computer.

In a domain, Computers can be on different local networks. In a work group all computers needs to be a part of the same local network.

Explain how NAT works

Network Address Translation translates and IP address used in a network to another IP address known within another network. A NAT table is maintained for global to local and local to mapping of IP's. NAT can be statically defined or dynamically translate from a pool of addresses. The NAT router is responsible for translating traffic coming and leaving the network. NAT prevents malicious

activity initiated by outside hosts from reaching local hosts by being dependent on a machine on the local network to initiate any connection to hosts on the other side of the router.

What is PPP protocol? Explain PPP packet format.

Point to Point protocol helps communication between 2 computers over a serial cable, phone line or other fiber optic lines, e.g. Connection between an Internet Service Provider and a host. PPP also provides authentication. PPP operates by sending Request packets and waiting for Acknowledge packets that accept, reject or try to change the request. The protocol is also used to negotiate on network address or compression options between the nodes.

Packet format

Flag field: 1 byte: - Indicates frames beginning or end

Address field: 1 byte: - Used for broadcast address (destination address)

Control field: 1 byte: - Used as a control byte

Protocol field: - 1 or 2 bytes: - Setting of protocol in information field (of datagram)

Information: - 0 or more bytes: - Datagram (whether it contains data or control information)

Padding: - 0 or more bytes: - optional padding

FCS: - 2 or more bytes: - error check sum

What is IP Spoofing and how can it be prevented?

IP spoofing is a mechanism used by attackers to gain unauthorized access to a system. Here, the intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted host. This is done by forging the header so it contains a different address and make it appear that the packet was sent by a different machine.

Prevention
Packet filtering: - to allow packets with recognized formats to enter the network using special routers and firewalls.
Encrypting the session

Explain IP datagram, Fragmentation and MTU.

IP datagram can be used to describe a portion of IP data. Each IP datagram has set of fields arranged in an order. The order is specific which helps to decode and read the stream easily. IP datagram has fields like Version, header length, Type

of service, Total length, checksum, flag, protocol, Time to live, Identification, source and destination ip address, padding, options and payload.

MTU: Maximum Transmission Unit is the size of the largest packet that a communication protocol can pass. The size can be fixed by some standard or decided at the time of connection

Fragmentation is a process of breaking the IP packets into smaller pieces. Fragmentation is needed when the datagram is larger than the MTU. Each fragment becomes a datagram in itself and transmitted independently from source. When received by destination they are reassembled.

What is an application gateway?

An application gateway is an application program that runs on a firewall between two networks. An application gateway is used for establishing connection between client program and destination service. The client negotiates with the gateway to communicate with the service of destination. Here, gateway can be called as a proxy. Hence, two connections are made; One between client and proxy; other between proxy and destination service. Connections take place behind the firewall.

Explain Circuit Level Gateway.

A circuit level gateway is used to find if a session in TCP handshaking is legitimate or not. It can be considered as a layer between application layer and transport layer. They protect the information of the private network they protect. Circuit level gateways do not filter packets.

What is 'Gateway of Last Resort'?

A Gateway of Last Resort or Default gateway is a route used by the router when no other known route exists to transmit the IP packet. Known routes are present in the routing table. Hence, any route not known by the routing table is forwarded to the default route. Each router which receives this packet will treat the packet the same way, if the route is known, packet will be forwarded to the known route.