MCSE Questions and Answers: :

1 :: 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 allow a host to inform its local router, that it wants to receive messages.

2 :: 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

3 :: 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.

4 :: 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.

5 :: 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.

6 :: 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.

7 :: 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

8 :: 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

9 :: 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.

10 :: 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

11 :: 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.

12 :: 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.

13 :: 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.

14 :: What is 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.

15 :: 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.

16 :: Define File Transfer Protocol.

File Transfer Protocol (FTP), a standard Internet protocol, is the simplest way to exchange files between computers on the Internet. Like the Hypertext Transfer Protocol (HTTP), which transfers displayable Web pages and related files, and the Simple Mail Transfer Protocol (SMTP), which transfers e-mail, FTP is an application protocol that uses the Internet's TCP/IP protocols. FTP is commonly used to transfer Web page files from their creator to the computer that acts as their server for everyone on the Internet. It's also commonly used to download programs and other files to your computer from other servers.

17 :: 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.

18 :: 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.

19 :: 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.

20 :: 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.

21 :: Explain the different classes of addresses supported by IP addressing.

Computers using the TCP/IP for communication are uniquely identified by a 32 bit address called as an IP address. The routers use the IP address information to forward the packet to the destination computer.

IP addresses are categorized as:

Private address: these IP addresses are used exclusively within a private network and not for public to see.

Public Address: these are registered IP addresses used for public.

Each IP address has a network address and a host address. IP addresses are expressed in four sets of three numbers, separated with dots. Each set is called as an octet because when converted to binary; it denotes eight binary

22 :: 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.

23 :: 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.

24 :: Explain the core naming mechanism, Domain Name System (DNS).

A Domain Name system is used to convert the names of the website on the internet to IP addresses. The domain names for each IP addresses are stored in a database that is distributed across different servers. A domain name space consists of a tree of domain names. The tree has zones. Zones consist of a collection of connected nodes. These nodes are served by a name server. A domain name is usually in the form of mydomain.com. Here, .com is the top level domain. Where as mydomain is the sub domain or subdivision. A host name is a domain name that has one or more IP addresses associated with it.

25 :: Describe Application layer.

The application layer is located at the top of the TCP/IP protocol layers. This one contains the network applications which make it possible to communicate using the lower layers. The software in this layer therefore communicates using one of the two protocols of the layer below (the transport layer), i.e. TCP or UDP. In computer networking, an application layer firewall is a firewall operating at the application layer of a protocol stack.[1] Generally it is a host using various forms of proxy servers to proxy traffic instead of routing it. As it works on the application layer, it may inspect the contents of the traffic, blocking what the firewall administrator views as inappropriate content, such as certain websites, viruses, and attempts to exploit known logical flaws in client software, and so forth. An application layer firewall does not route traffic on the network layer. All traffic stops at the firewall which may initiate its own connections if the traffic satisfies the rules.

26 :: Define DNS

The DNS translates Internet domain and host names to IP addresses. DNS automatically converts the names we type in our Web browser address bar to the IP addresses of Web servers hosting those sites. DNS implements a distributed database to store this name and address information for all public hosts on the Internet.

27 :: Define Telnet

Telnet is the main Internet protocol for creating a connection to a remote server.

28 :: Define SMTP

SMTP - Short for Simple Mail Transfer Protocol, a protocol for sending e-mail messages between servers.

29 :: What Is a MAC Address?

MAC (Media Access Control) addresses are globally unique addressed that are written into hardware at the time of manufacture. The MAC address is a unique value associated with a network adapter. MAC addresses are also known as hardware addresses or physical addresses. They uniquely identify an adapter on a LAN. MAC addresses are 12-digit hexadecimal numbers (48 bits in length).

30 :: MAC vs. IP Addressing

Whereas MAC addressing works at the data link layer, IP addressing functions at the network layer (layer 3). It's a slight oversimplification, but one can think of IP addressing as supporting the software implementation and MAC addresses as supporting the hardware implementation of the network stack. The MAC address generally remains fixed and follows the network device, but the IP address changes as the network device moves from one network to another.

31 :: Define Spanning-Tree Protocol (STP)

Spanning-Tree Protocol (STP) as defined in the IEEE 802.1D is a link management protocol that provides path redundancy while preventing undesirable loops in the network. For an Ethernet network to function properly, only one active path can exist between two stations. Loops occur in networks for a variety of reasons. The most common reason you find loops in networks is the result of a deliberate attempt to provide redundancy - in case one link or switch fails, another link or switch can take over.

32 :: What is VPN?

A VPN is a service that offers secure, reliable connectivity over a shared public network infrastructure such as the Internet. VPNs maintain the same security and management policies as a private network. They are the most cost effective method of establishing a virtual point-to-point connection between remote users and an enterprise customer's network.

33 :: Define broadcast domain.

It is a logical area in a computer network where any computer connected to the network can directly transmit to any other computer in the domain without having to go through a routing device.

34 :: Bridge vs switch.

A bridge connects two different LAN networks. A switch is something like you can connect many computers to a switch and then one computer can connect to another through the switch. Switch is a unicast one to one connection

35 :: What is a Router?

A router is a device or sometimes a software in a computer which decides the next network point to which a packet should be forwarded to reach its destination on Internet. It is usually included as part of the network switch and is located at a gateway, including each point-of-presence on the Internet. The router is connected to at least two networks and determines which way

36 :: Define gateway.

A gateway is a network point that provides entrance into another network. On the Internet, a node or stopping point can be either a gateway node or a host (end-point) node. Both the computers of Internet users and the computers that serve pages to users are host nodes. The computers that control traffic within your company's network or at your local Internet service provider (ISP) are gateway nodes.

37 :: What is firewall?

A firewall is a hardware or software installed to provide security to the private networks connected to the internet. They can be implemented in both hardware and software, or a combination of both. All data entering or leaving the Intranet passes through the firewall which allows only the data meeting the administrators' rules to pass through it.

38 :: What are the types of firewalls?

Packet Filtering Firewall:
This type of Firewall detects packets and block unnecessary packets and makes network traffic release.

Screening Router Firewalls:
It's a software base firewall available in Router provides only light filtering.

Computer-based Firewall:
It's a firewall stored in server with an existing Operating System like Windows and UNIX.

Hardware base Firewall:
Its device like box allows strong security from public network. Mostly used by big networks.

Proxy Server:
Proxy server allows all clients to access Internet with different access limits. Proxy server has its own firewall which filters the all packet from web server.

39 :: What is Data encryption?

Data encryption ensures data safety and very important for confidential or critical data. It protect data from being read, altered or forged while transmission.

40 :: What is the Public Key Encryption?

Public key encryption use public and private key for encryption and decryption. In this mechanism, public key is used to encrypt messages and only the corresponding private key can be used to decrypt them. To encrypt a message, a sender has to know recipient's public key.

41 :: What is Digital Signatures?

Digital signature is an attachment to an electronic message used for security purpose. It is used to verify the authenticity of the sender.

42 :: What is Ethernet technology?

Ethernet technology is a high speed broadcast bus technology. In this type, all the station shares a single ether channel and receives every single transmitted signal.

43 :: Explain the use of network interface card, NIC.

NIC is used to connect computer to an Ethernet network.

44 :: Explain token ring technology.

In this technology, all the devices are arranged in a circle. A token moves around the circular network. A device waits for the token before it sends its frame. Once it receives token, it initiates transmission of its frame.

45 :: What is CSMA and CD concept?

In CSDA (carrier sense multiple access), presence of any digital signal in a network is checked before transmission. Data transmission occurs only when no signal is sensed.

CD, Collision detection is responsible for monitoring carrier in order to avoid signal jam.

46 :: What is NetBIOS protocol?

NetBIOS (Network Basic Input/Output System) Protocol allows applications on separate computers to communicate over a LAN. It runs over TCP/IP giving each

computer in the network a NetBIOS name and IP address. E.g. It can be used for computers running Windows 2000 (or before) to join a computer network running Windows 2000 (or later).

47 :: What is IGMP protocol?

Internet Group Management Protocol, allows internet hosts to multicast. i.e. to send messages to a group of computers. There may be a group of internet hosts interested to multicast. IGMP allows router to determine which host groups have members on a given network segment. It helps to establish group memberships. It is commonly used for streamlining videos and gaming. The protocol can be implemented both as a host side and router side. The host side is responsible to notify its membership in a group. The notification is made to a local router. This local router (router side) in turn sends out queries.

48 :: Explain PPP protocol.

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. PPP has a number of phases as below:

* **Link dead:** - takes place when the connection fails.
* **Link Establishment Phase:** - Used to establish connection. If authentication is desired, it moves to next phase.
* **Authentication Phase**: - Allows the nodes to authenticate each other.
* **Network-Layer Protocol Phase**: - here, the network control protocols come into play. Data transport, closing of the protocols takes place in this phase.
* Link Termination Phase: - here, the connection is terminated.

49 :: What is TCP / IP protocol?

Transmission Control Protocol / Internet Protocol: - It is a family of protocols used for communication and connection between hosts on the internet. It is the most widely used standard for transmitting data over the internet. The four layers in the protocol are (from bottom to top):- Physical layer, Data link layer, Network layer, transport layer and application layer, also called as the OSI model. In TCP/IP , IP is responsible for forwarding packets while TCP ensures the correct delivery of data from client to server. TCP detects loss of data as well.

50 :: 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.

51 :: What is HTTP (Hypertext Transfer Protocol)?

HTTP or Hyper Text Transfer Protocol is provides a set of rules to transfer files, videos, images over the world wide web. When the web browser is opened, a HTTP request call is made. A web server contains a HTTP daemon. This daemon is used to wait for HTTP requests and handle them when they arrive. The web browser from where HTTP requests are made is called as a client. These requests are sent to the server. It uses a reserved port no 80.

52 :: What is NNTP (Network News Transfer Protocol)?

NNTP or Network News Transfer Protocol is used to manage the notes posted on Unset newsgroup (a collection of posted notes on a subject posted by different users). NNTP servers are responsible for managing Usenet newsgroup collected globally. A NTTP client is a part of the web browser also called as a news reader. It uses a reserver port no 119.

53 :: What is SMTP (Simple Mail Transfer Protocol)?

SMTP or Simple Mail Transfer Protocol is used to send email messages between servers. The messages are retrieved using email clients. SMTP is more commonly used to send messages from a mail client to a mail server. And hence the email client like POP needs to be configured. Hence, SMTP is used to send emails while POP or IMAP are used to receive messages. It is usually operated on port25 on the internet.

54 :: What is POP3 (Post Office Protocol 3)?

POP3 or Post Office Box 3 is used fro receiving emails. It is a client server protocol which holds the email. Once the email is downloaded from the server, POP3 deletes it from the server. Ordinal numbers are used to identify specific messages.

55 :: What is SNMP (Simple Network Management Protocol)?

SNMP or Simple Network Management Protocol is typically used for managing the network. Managing the network includes managing the nodes present in the network. These nodes may be server, routers, bridges and hubs. SNMP agents are used to achieve this. Managing the network is essential because it helps to monitor network

performance, detect network faults or failures, audit network usage etc. the SNMP messages like TRAP, GET or SET may be invoked by network elements or network management system.