http://www.careerride.com/Networking-Interview-Questions.aspx

http://www.careerride.com/

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.

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.

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.

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. Whereas my domain is the sub domain or subdivision. A host name is a domain name that has one or more IP addresses associated with it.

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.

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.

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.

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.

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.

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).

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.

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.

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.

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 do you mean by the term ‘routing’? What a router must know to route a packet?

‘Routing’ is used to deliver a packet from one device to another device through communication network. Routing is performed by the router and each router maintains a routing table. A routing table contains the information of the best possible paths from source router to the destination router.

A router must know the following to route a packet:

a. Address of the destination

b. Neighbor routers

c. Routes to all remote networks

d. The best route to each remote network

e. Way to maintain and verify routing information

Comment on Static Routing, Default Routing and Dynamic Routing.

To route a packet over the communication network, a network administrator has to configure a router. These configurations are of three types:

Static Routing: A network administrator manually configures the routes for a router. A static route has higher priority than a dynamic route.

Default Routing: Default routing is used only for the network that has only a single connection to router. Static routes are also manually configured.

Dynamic Routing: Dynamic routing used various routing protocols to route packets. A route is automatically updated as a topology change occurs. Dynamic routing is easier than static and default routing.

How many classes of routing protocols are there. Describe each?

There are three classes of routing protocols: Distance vector, Link State and Hybrid

Distance Vector: This routing protocol discover the best path to a remote network by judging distance. This type of protocols counts the hop; hops are the number of the routers from which a packet goes. The vector points to the direction of remote network.

Example: RIP and IGRP

Link State: A router send updates containing the state of their own link to the other routers. This is also called shortest path first protocol. Three different tables are maintained by the router using this protocol. One is routing table, one of directly attached neighbors and one for the topology of entire internetwork. Link state enables a router to know about internetwork.

Example: OSPF

Hybrid: Hybrid protocols contain the features of both Distance vector and link state protocols.

Example: EIGRP

Why do Routing Loops occur and how to overcome them?

a) Routing loop is common problem of various types of networks. Distance vector routing protocol keeps track of any change to the internetwork by broadcasting periodic updates. This works okay but if a network outage happens then routing loops occurs in the network. The main reason to occur routing loops is that each router is not updated at the same time and the fake information of a router's link broadcasted.

Three rules for distance vector routing protocol are developed to overcome routing loops:

i. Split Horizon: According to this rule, never broadcast a route out of the interface through which it received. It helps to avoid loops between adjacent routers.

ii. Route Poisoning: When a network goes down than the router associated to that network initiates route poisoning. This shows an unreachable network.

iii. Holddown timer: Holddown timer says that if a route advertised as down, do not listen to routing updates from that route for a specified period of time.

Define OSPF and what features are provided by OSPF?

OSPF is abbreviated as Open Shortest Path First. OSPF is an open standard and supported by a large variety of network vendors, including Cisco. OSPF works on the concept of Dijkstra algorithm in which a shortest path is maintained and routing table is populated on that path.

Some features of OSPF are:

i. Minimizes routing update traffic

ii. Open standard routing protocol

iii. Unlimited hop count

iv. Routing update traffic is lesser than any other routing protocol.

Define Routing Information Protocol (RIP) and what is the difference between RIPv1 and RIPv2?

RIP is a distance vector routing protocol which uses hop count to find the best way to a remote network. RIP sends its complete routing table to neighbor router in every 30 seconds. RIP uses maximum 15 hop count and is suitable only for small networks.

RIPv1 uses classful routing that means all the devices in the network must use the same subnet mask and do not send subnet mask information with routing updates. While RIPv2 uses classless routing and subnet mask information is sent with routing update.

What is IGRP? Differentiate between IGRP and RIP.

IGRP is abbreviated as Interior Gateway Routing Protocol. This is created by Cisco and all the routers must be of Cisco to run this protocol. IGRP is developed to overcome the problem with RIP. RIP can be used only for small network because it uses maximum 15 hop-counts while IGRP can be used for bigger networks because it uses 255 hop-counts.

i. IGRP uses autonomous system number and supplies this number to all routers while in RIP there is no autonomous number.

ii. IGRP updates its Routing table every 90 seconds and RIP updates its routing table in every 30 seconds.

iii. IGRP has administrative distance of 100 while RIP has 120.

iv. IGRP uses maximum 255 hop-counts while RIP uses 15 maximum hop-counts.

What is EIGRP and what conditions are needed to neighbourship establishment in context to EIGRP?

EIGRP is abbreviated as Enhanced Interior Gateway Routing Protocol. EIGRP is a proprietary Cisco protocol that runs only on Cisco routers. EIGRP is a popular routing protocol now days. EIGRP is a classless, enhanced distance routing protocol.

Before EIGRP routers wants to exchange routes, they have to establish a neighborhood relationship. To establish this neighbourship three conditions must meet:

i. Autonomous System Numbers must match

ii. Hello packet must received

iii. Metrics value must identical

OSPF is supposed to be design in a hierarchical fashion; what are the reasons for creating OSPF in a hierarchical fashion?

OSPF (Open Shortest Path First) is supposed to be design in hierarchical fashion so that a large internetwork could be break into smaller network. These smaller networks are called areas.

Following are some reasons for creating OSPF in hierarchical design:

i. To reduce the routing overhead

ii. To break a bigger internetwork into smaller internetworks caller areas

iii. To accelerate convergence

What do you mean by ‘Switching’? What are the services provided by Switching?

Generally switching refers to the layer 2 switching. Switching is a process which uses the hardware address or MAC address of a device to switch a packet from one device to another.

Services provided by switching are:

i. Switches use Application-Specific Integrated Circuits (ASICs) to make and maintain their filter table.

ii. Time required to transfer a packet is low i.e. low latency
iii. Cost is low

What is Spanning Tree Protocol (STP) and define some STP terms?

The main function of STP is to prevent the network loops occurring in switching network. STP monitors the network to find all links and shut down the redundant links. For this STP uses Spanning tree algorithm.

Some STP terms are:

Root Bridge: To select a root bridge an election is done by all switches in a switching network. All the decisions like- which port is to be blocked and which port is forwarding are made from the viewpoint of Root Bridge.

BPDU: BPDUs (Bridge Protocol Data Unit) are sending from one switch to another to elect a root bridge.

Bridge ID: Bridge ID is an identifier of a Switch.

Three switch functions are address learning, forward/filter decision, loop avoidance. Define these functions.

Address Learning: In Layer 2 switching, each interface of a switch learns the source hardware address (MAC address) and save this into its MAC database table. This table is also known as forward filter table.

Forward/filter decisions: Forward/filter decision is taken by the switch to forward a frame to a specific destination port. The frame which comes on an interface, switch sees its MAC address table and forward this frame to a specific destination port.

Loop Avoidance: Network loops can arise if multiple connections are formed between switches for redundancy purposes. TO prevent network loops STP (Spanning Tree Protocol) is used and redundancy is also maintained.

How STP works and what is the purpose for STP?

Firstly STP elects a Root Bridge and forward to all ports and this root bridge acts as a point of reference for all other devices in STP domain. When all switches agreed on root bridge, every switch must find its one and only allotted root port. Each and every link between switches must have one and only one designated port in such a way that it must provide the highest bandwidth to link.

The main purpose for STP is to prevent the network loops.

Define Spanning-Tree port states.

The port of switches running STP can has five different port state:

- Blocking: A blocking port only listens to BPDUs while cannot forward frames.

- Listening: Listening port only listen to BPDUs and preparing to forward frames.

- Learning: The switch listen to BPDUs and learns all the paths in the LAN network.

- Forwarding: In this port state, switch port can forward and receive the frames.

- Disabled: In disabled state a switch port is administratively down and that port do not participate frame forwarding.

What are Manageable and unmanageable switches? What is the advantage of manageable over unmanageable?

Manageable Switch: Managed switches allows the layer 3 functionality and can be used as a router. It has own IP address and can be easily configured. It also has ability to traffic control, port blocking and VLANs configuration.

Unmanageable Switch: Unmanageable switches are layer 2 switches and learn only hardware address (MAC address). It learns the MAC address of all the connected devices and when a frame came from some source it broadcast it to all ports and throws frame to destination (by using its MAC table).

Advantages of manageable over unmanageable are:

i. IP address can be assigned to manageable switch and can it can be access through 'telnet' command.

ii. More secure than unmanageable because any port can be block at any time.

iii. Managed switch has router like capabilities.

iv. Managed switch can manage the bandwidth of link.

If your routing table has a static, a RIP, and an IGRP route to the same network, by default which route will be used to route packets?

Administrative distance rates the trustworthiness of the any routing protocol. AD value is an integer from 0 to 255 and trustworthiness increases with the increasing order of the AD value.

Static route will be used to route packets. Static routes have an administrative distance of 1 by default. IGRP has an administrative distance of 100, and RIP has an administrative distance of 120, by default.

If a switch receives a frame and the source MAC address is not in the MAC address table but the destination address is, what will switch do with the frame?

Since the source MAC address is not in the MAC address table, firstly the switch will add the source MAC address and the port it is connected to into its MAC address table and then forward the frame to the outgoing port and frame reached to the right destination address.

If you want to improve switched network performance by increasing the bandwidth available to hosts and limit the size of broadcast domains. Which of the following options will achieve this goal—(i) Bridges, (ii) Switches or (iii) Switches configured with VLANs?

Switches configured with VLANs will improves the network performance. By creating and implementing VLANs in our switched network, we can break up broadcast domain and limit the size of broadcast domain. VLANs greatly enhance network security which also improves the switched network performance.

If two connected routers are configured with RIP routing. What will be the result when a router receives a routing update that contains a higher-cost path to network already in its routing table?

When a routing update is received by a router, the router first checks the administrative distance (AD) value and always choose the route with the lowest administrative distance value. However, if two routes are received and they both have same administrative distance value, then the router will choose the one route with the lowest metrics, or in RIP's case, hop count.

RIP allows a maximum hop-count of 15, so anything that requires 16 hops is consider as unreachable. Hence if a router receives a routing update that contains a higher-cost path but have lower hops than the packet will be transferred through that path.

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 won’t affect the entire LAN.

d. 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.

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.

What is 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.

Define Telnet

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

Define SMTP.

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

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).

MAC vs. IP Addressing

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. Whereas MAC addressing works at the data link layer, IP addressing functions at the network layer (layer 3). 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.

What is VPN?

A VPN is a service that offers secure, reliable connectivity over a shared public network infrastructure such as the Internet. VPN's maintains the same security and management policies as a private network.

VPN supports remote access to computers and allow data to be transmitted over this public network. Even though the data is transmitted over a public network, encryption and decrypting data to ensure security.

How would you define IP address?

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.

Difference between Static and Dynamic IP.

Static IP is also called as permanent address assigned to each device in a network, whereas Dynamic IP, a temporary address assigned to the device via DHCP software. IP address assigned to your service by your cable or DSL Internet provider is typically dynamic IP. In routers and operating systems, the default configuration for clients is dynamic IP

What is Network Address Translation?

Network Address Translation acts as an agent between the Internet and a local network. It is a dynamic method which is used to minimize Internet connectivity needs. Network address translation describes the rewriting of the Internet Protocol (IP) addresses of data packets so that multiple transmissions require only one IP address.

Define IP multicast.

IP multicast technology reduces traffic by sending stream of information to many recipients at one go. Video conferencing, stock quotas are the examples based on IP multicast.

What is subneting?

Subnet adds one level to the way IP address is represented. It logically organizes

Define Address Resolution Protocol.(ARP)

Address Resolution Protocol ARP, is responsible for mapping an IP address to its corresponding physical network address. It is mostly seen on Ethernet network.

Explain Maximum Transfer Unit, MTU.

MTU specifies the largest amount of data that can be transferred across a network.

Describe the basics of internet routing.

When a source sends a packet to a destination, this packet has a specific path or route it follows. Different routing protocols are used to find the shortest path to the destination. The protocols maintain routing tables. Routing tables consist of a set of rules used to determine where these packets will travel. When a packet is received, a network device examines the packet and matches it to the routing table entry providing the best match for its destination. The packet keeps hopping until it reaches its destination.

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.

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.

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.

Define 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.

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.

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).

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.

What is NNTP (Network News Transfer Protocol)?

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.

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.

What is Distance Vector Routing Protocols?

The Distance Vector protocol initially prepares a Routing table which is shared with other routers. This routing table is shared between routers present in the same network. A new routing table is prepared when some new information is received from some other router. Now, the bad routing paths are removed keeping only the smallest hop paths. This new table is then communicated to other routers.

TCP vs. UDP.

TCP guarantees the delivery of data. UDP on the other hand, does not guarantee delivery of data. TCP delivers messages in the order they were sent. UDP has no ordering mechanisms. In TCP data is sent as a stream while UDP sends data as individual packets. UDP is faster than TCP. TCP is a connection oriented protocol while UDP is connectionless.

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.

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.

Working knowledge of Cisco Product (Router 2800, 3800 7200 and 7600, ASR, GSR series & Switch 3750, 4500, 6500, Nexus series.) Certifications

The term loopback (sometimes spelled loop-back) is generally used to describe methods or procedures of routing electronic signals, digital data streams, or other flows of items, from their originating facility quickly back to the same source entity without intentional processing or modification. This is primarily intended as a means of testing the transmission or transportation infrastructure.

Have you ever wondered what a Virtual LAN (or VLAN) is or been unclear as to why you would want one? If so, I have been in your place at one time too. Since then, I have learned a lot about what a VLAN is and how it can help me. In this article, I will share that knowledge with you.

What is a LAN?

Okay, most of you already know what a LAN is but let's give it a definition to make sure. We have to do this because, if you don't know what a LAN is, you can't understand what a VLAN is.

A LAN is a local area network and is defined as all devices in the same broadcast domain. If you remember, routers stop broadcasts, switches just forward them.

What is a VLAN?

As I said, a VLAN is a virtual LAN. In technical terms, a VLAN is a broadcast domain created by switches. Normally, it is a router creating that broadcast domain. With VLAN's, a switch can create the broadcast domain.

This works by, you, the administrator, putting some switch ports in a VLAN other than 1, the default VLAN. All ports in a single VLAN are in a single broadcast domain.

Because switches can talk to each other, some ports on switch A can be in VLAN 10 and other ports on switch B can be in VLAN 10. Broadcasts between these devices will not be seen on any other port in any other VLAN, other than 10. However, these devices can all communicate because they are on the same VLAN. Without additional configuration, they would not be able to communicate with any other devices, not in their VLAN.

Are VLANs required?

It is important to point out that you don't have to configure a VLAN until your network gets so large and has so much traffic that you need one. Many times, people are simply using VLAN's because the network they are working on was already using them. Another important fact is that, on a Cisco switch, VLAN's are enabled by default and ALL devices are already in a VLAN. The VLAN that all devices are already in is VLAN 1. So, by default, you can just use all the ports on a switch and all devices will be able to talk to one another.

When do I need a VLAN?

You need to consider using VLAN's in any of the following situations:

You have more than 200 devices on your LAN

You have a lot of broadcast traffic on your LAN

Groups of users need more security or are being slowed down by too many broadcasts?

Groups of users need to be on the same broadcast domain because they are running the same applications. An example would be a company that has VoIP phones. The users using the phone could be on a different VLAN, not with the regular users.

Or, just to make a single switch into multiple virtual switches.

Why not just subnet my network?

A common question is why not just subnet the network instead of using VLAN's? Each VLAN should be in its own subnet. The benefit that a VLAN provides over a subnetted network is that devices in different physical locations, not going back to the same router, can be on the same network. The limitation of subnetting a network with a router is that all devices on that subnet must be connected to the same switch and that switch must be connected to a port on the router.