What is Round Trip Time?

Ans. Round Trip Time or RTT is the time taken to send a message from one end of a network to the other and back.

Name the user support layers.

Ans. There are three types of user support layers –

- Session Layer
- Presentation Layer and
- Application Layer

What is OSPF?

Ans. OSPF is an abbreviation for Open Shortest Path First. It is a routing protocol that uses a link-state routing (LSR) algorithm to find out the best possible path for data exchange.

What is SMTP?

Ans. Simple Mail Transfer Protocol (SMTP) is a protocol used to move all internal mail across different networks. It works with Mail Transfer Agent (MTA) and provide the mail transmission on the TCP/IP protocol stack.

What is piggybacking ?
Piggybacking on Internet access is the practice of establishing a wireless Internet connection by using another subscriber's wireless Internet access service without the subscriber's explicit permission or knowledge. It is a legally and ethically controversial practice, with laws that vary by jurisdiction around the world. While completely outlawed or regulated in some places, it is permitted in others.

Name the two sub layers of Data link layer. Specify their protocols.

1. Logical link control(LLC)

2. Media access Control (MAC)

Difference between unacknowledged connection less services and acknowledged connection less services ?
Unacknowledged connectionless service consists of having the source machine send independent frames to the destination machine without having the destination machine acknowledged. Most LAN's use this service.

Acknowledged connectionless service in this service there are no logical connections used but each frame sent individually acknowledged. In this way the sender knows whether a frame has arrived correctly. It is useful on wireless systems

What is frame ?
In computer networking and telecommunication, a frame is a digital data transmission unit or data packet that includes frame synchronization, i.e. a sequence of bits or symbols making it possible for the receiver to detect the beginning and end of the packet in the stream of symbols or bits.

What is bit stuffing?
Ans: Bit stuffing is the insertion of one or more bits into a transmission unit as a way to provide signaling information to a receiver. The receiver knows how to detect and remove or disregard the stuffed bits.

What are the types of errors?

a. Single-Bit errorIn a single-bit error, only one bit in the data unit has changed

b. Burst ErrorA Burst error means that two or more bits in the data have changed

What is CRC?

CRC, is the most powerful of the redundancy checking techniques, is based on binary division

What is Checksum?

Checksum is used by the higher layer protocols (TCP/IP) for error detection

What is Framing?

Framing in the data link layer separates a message from one source to a destination, or from other messages to other destinations, by adding a sender address and a destination address. The destination address defines where the packet has to go and the sender address helps the recipient acknowledge the receipt.

Define Character Stuffing?

In byte stuffing (or character stuffing), a special byte is added to the data section of the frame when there is a character with the same pattern as the flag. The data section is stuffed with an extra byte. This byte is usually called the escape character (ESC), which has a predefined bit pattern. Whenever the receiver encounters the ESC character, it removes it from the data section and treats the next character as data, not a delimiting flag

What is Bit Stuffing?

Bit stuffing is the process of adding one extra 0 whenever five consecutive Is follow a 0 in the data, so that the receiver does not mistake the pattern 0111110 for a flag.

What is Flow Control?

Flow control refers to a set of procedures used to restrict the amount of data that the sender can **send before waiting for acknowledgment**

What is Error Control ?

Error control is both error detection and error correction. It allows the receiver to inform the sender of any frames lost or damaged in transmission and coordinates the retransmission of those frames by the sender. In the data link layer, the term error control refers primarily to methods of error detection and retransmission

What is Stop-and-Wait Protocol?

In Stop and wait protocol, sender sends one frame, waits until it receives confirmation from the receiver (okay to go ahead), and then sends the next frame.

What is Sliding Window?

The sliding window is an abstract concept that defines the range of sequence numbers that is the concern of the sender and receiver. In other words, he sender and receiver need to deal with only part of the possible sequence numbers.

What are the types of Transmission media?

Signals are usually transmitted over some transmission media that are broadly classified in to two categories.

a.) Guided Media: These are those that provide a conduit from one device to another that include twisted-pair, coaxial cable and fiber-optic cable. A signal traveling along any of these media is directed and is contained by the physical limits of the medium. Twisted-pair and coaxial cable use metallic that accept and transport signals in the form of electrical current. Optical fiber is a glass or plastic cable that accepts and transports signals in the form of light.

b.) Unguided Media: This is the wireless media that transport electromagnetic waves without using a physical conductor. Signals are broadcast either through air. This is done through radio communication, satellite communication and cellular telephony.

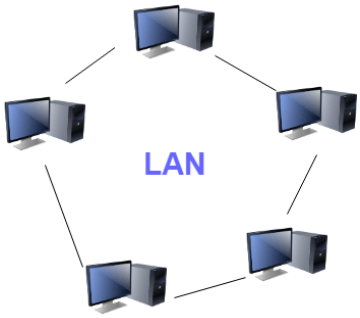
What is a Link?

A link refers to the connectivity between two devices. It includes the type of cables and protocols used for one device to be able to communicate with the other.

What are the layers of the OSI reference model?

There are 7 OSI layers: 1) Physical Layer, 2) Data Link Layer, 3) Network Layer, 4) Transport Layer, 5) Session Layer, 6) Presentation Layer, and 7) Application Layer.

What is a LAN?



LAN stands for Local Area Network. It refers to the connection between computers and other network devices that are located within a small physical location.

What is a node?

A node refers to a point or joint where a connection takes place. It can be a computer or device that is part of a network. Two or more nodes are needed to form a network connection.

What are routers?

Routers can connect two or more network segments. These are intelligent network devices that store information in its routing tables, such as paths, hops, and bottlenecks. With this info, they can determine the best path for data transfer. Routers operate at the OSI Network Layer.

What is a subnet mask?

A subnet mask is combined with an IP address to identify two parts: the extended network address and the host address. Like an IP address, a subnet mask is made up of 32 bits.

What is the maximum length allowed for a UTP cable?

A single segment of UTP cable has an allowable length of 90 to 100 meters. This limitation can be overcome by using repeaters and switches.

What is data encapsulation?

Data encapsulation is the process of breaking down information into smaller, manageable chunks before it is transmitted across the network. In this process that the source and destination addresses are attached to the headers, along with parity checks.

Describe Network Topology

Network Topology refers to the layout of a computer network. It shows how devices and cables are physically laid out, as well as how they connect.

What is a VPN?

VPN means Virtual Private Network, a technology that allows a secure tunnel to be created across a network such as the Internet. For example, VPNs allow you to establish a secure dial-up connection to a remote server.

Briefly describe NAT

NAT is Network Address Translation. This is a protocol that provides a way for multiple computers on a common network to share a single connection to the Internet.

What is the job of the Network Layer under the OSI reference model?

The Network layer is responsible for data routing, packet switching, and control of network congestion. Routers operate under this layer.

What is RIP?

RIP, short for Routing Information Protocol is used by routers to send data from one network to another. It efficiently manages routing data by broadcasting its routing table to all other routers within the network. It determines the network distance in units of hops.

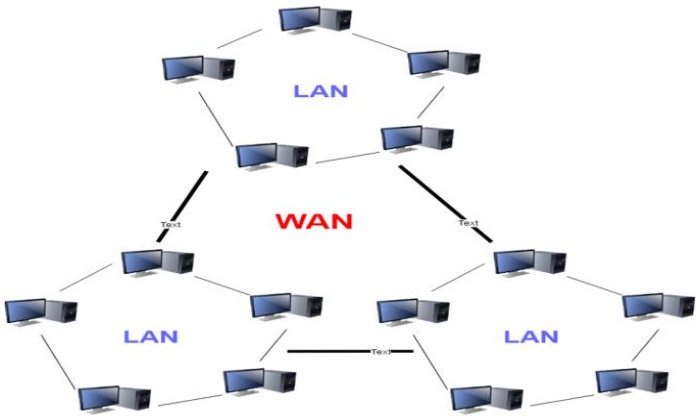
What are the different ways of securing a computer network?

There are several ways to do this. Install a reliable and updated anti-virus program on all computers. Make sure firewalls are setup and configured correctly. User authentication will also help a lot. All these combined would make a highly secured network.

What is NIC?

NIC is short for Network Interface Card. This is a peripheral card that is attached to a PC in order to connect to a network. Every NIC has its own MAC address that identifies the PC on the network.

What is WAN?



WAN stands for Wide Area Network. It is an interconnection of computers and devices that are geographically dispersed. It connects networks that are located in different regions and countries.

What is the importance of the OSI Physical Layer?

The physical layer does the conversion from data bits to the electrical signal, and vice versa. This is where network devices and cable types are considered and setup.

How many layers are there under TCP/IP?

There are four layers: 1) The Network Layer, 2) Internet Layer, 3) Transport Layer, and 4) Application Layer.

What are proxy servers, and how do they protect computer networks?

Proxy servers primarily prevent external users who are identifying the IP addresses of an internal network. Without knowledge of the correct IP address, even the physical location of the network cannot be identified. Proxy servers can make a network virtually invisible to external users.

What is the function of the OSI Session Layer?

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

What is a private IP address?

Private IP addresses are assigned for use on intranets. These addresses are used for internal networks and are not routable on external public networks. These ensure that no conflicts are present among internal networks. At the same time, the same range of private IP addresses is reusable for multiple intranets since they do not "see" each other.

What is OSI, and what role does it play in computer networks?

OSI (Open Systems Interconnect) serves as a reference model for data communication. It is made up of 7 layers, with each layer defining a particular aspect of how network devices connect and communicate with one another. One layer may deal with the physical media used, while another layer dictates how data is transmitted across the network.

What is the purpose of cables being shielded and having twisted pairs?

The primary purpose of this is to prevent crosstalk. Crosstalk's are electromagnetic interferences or noise that can affect data being transmitted across cables.

What is the advantage of address sharing?

By using address translation instead of routing, address sharing provides an inherent security benefit. That's because host PCs on the Internet can only see the public IP address of the external interface on the computer. Instead, it provides address translation and not the private IP addresses on the internal network.

What are MAC addresses?

MAC, or Media Access Control, uniquely identifies a device on the network. It is also known as a physical address or an Ethernet address. A MAC address is made up of 6-byte parts.

What is the equivalent layer or layers of the TCP/IP Application layer in terms of the OSI reference model?

The TCP/IP Application layer has three counterparts on the OSI model: 1) Session Layer, 2) Presentation Layer, and 3) Application Layer.

How can you identify the IP class of a given IP address?

By looking at the first octet of any given IP address, you can identify whether it's Class A, B, or C. If the first octet begins with a 0 bit, that address is Class A. If it begins with bits 10 then that address is a Class B address. If it begins with 110, then it's a Class C network.

What is the main purpose of OSPF?

OSPF, or Open Shortest Path First, is a link-state routing protocol that uses routing tables to determine the best possible path for data exchange.

What are firewalls?

Firewalls serve to protect an internal network from external attacks. These external threats can be hackers who want to steal data or computer viruses that can wipe out data in an instant. It also prevents other users from external networks from gaining access to the private network.

What is tracert?

Tracert is a Windows utility program that can use to trace the route taken by data from the router to the destination network. It also shows the number of hops taken during the entire transmission route.

What are the functions of a network administrator?

A network administrator has many responsibilities that can be summarized into 3 key functions: installation of a network, a configuration of network settings, and maintenance/troubleshooting of networks.

What is DHCP?

DHCP is short for Dynamic Host Configuration Protocol. Its main task is to assign an IP address to devices across the network automatically. It first checks for the next available address not yet taken by any device, then assigns this to a network device.

What is the main job of the ARP?

The main task of the ARP or Address Resolution Protocol is to map a known IP address to a MAC layer address.

What is TCP/IP?

TCP/IP is short for Transmission Control Protocol / Internet Protocol. This is a set of protocol layers that is designed to make data exchange possible on different types of computer networks, also known as a heterogeneous network.

What is the use of a default gateway?

Default gateways provide means for the local networks to connect to the external network. The default gateway for connecting to the external network is usually the address of the external router port.

What is netstat?

Netstat is a command-line utility program. It provides useful information about the current TCP/IP settings of a connection.

What is the number of network IDs in a Class C network?

For a Class C network, the number of usable Network ID bits is 21. The number of possible network IDs is 2 raised to 21 or 2,097,152. The number of host IDs per network ID is 2 raised to 8 minus 2, or 254.

What is ICMP?

ICMP is an Internet Control Message Protocol. It provides messaging and communication for protocols within the TCP/IP stack. This is also the protocol that manages error messages that are used by network tools such as PING

What is Ping?

Ping is a utility program that allows you to check connectivity between network devices on the network. You can ping a device by using its IP address or device name, such as a computer name.

What is DNS?

DNS is the Domain Name System. The main function of this network service is to provide host names to TCP/IP address resolution.

What advantages does fiber optics have over other media?

One major advantage of fiber optics is that it is less susceptible to electrical interference. It also supports higher bandwidth, meaning more data can be transmitted and received. Signal degrading is also very minimal over long distances.

What is the difference between a hub and a switch?

Here is the major difference between Hub and switch:

Hub	Switch
A hub operates on the physical layer.	A switch operates on the data link layer.
Hubs perform frame flooding that can be unicast, multicast, or broadcast.	It performs broadcast, then the unicast and multicast as needed.
Just a singular domain of collision is present in a hub.	Varied ports have separate collision domains.
The transmission mode is Half-duplex	The transmission mode is Full duplex
Hubs operate as a Layer 1 device per the OSI model.	Network switches help you to operate at Layer 2 of the OSI model.
To connect a network of personal computers should be joined through a central hub.	Allow connecting multiple devices and ports.
Uses electrical signal orbits	Uses frame & packet
Does not offer Spanning-Tree	Multiple Spanning-Tree is possible
Collisions occur mostly in setups using hubs.	No collisions occur in a full-duplex switch.
Hub is a passive device	A switch is an active device
A network hub can't store MAC addresses.	Switches use CAM (Content Accessible Memory) that can be accessed by ASIC (Application Specific Integrated Chips).
Not an intelligent device	Intelligent device

Its speed is up to 10 Mbps	10/100 Mbps, 1 Gbps, 10 Gbps
Does not use software	Has software for administration

What is ipconfig?

Ipconfig is a utility program that is commonly used to identify the addresses information of a computer on a network. It can show the physical address as well as the IP address.

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

CSMA/CD, or Collision Detect, retransmits data frames whenever a collision occurred. CSMA/CA, or Collision Avoidance, will first broadcast intent to send prior to data transmission.

What is mesh topology?

Mesh topology is a setup wherein each device is connected directly to every other device on the network. Consequently, it requires that each device has at least two network connections.

What is IPv6?

IPv6, or Internet Protocol version 6, was developed to replace IPv4. At present, IPv4 is being used to control internet traffic but is expected to get saturated in the near future. IPv6 was designed to overcome this limitation.

What is the difference between TCP and UDP?

Here are some major differences between TCP and UDP protocols:

TCP	UDP
It is a connection-oriented protocol.	It is a connectionless protocol.
TCP reads data as streams of bytes, and the message is transmitted to segment boundaries.	UDP messages contain packets that were sent one by one. It also checks for integrity at the arrival time.
TCP messages make their way across the Internet from one computer to another.	It is not connection-based, so one program can send lots of packets to another.
TCP rearranges data packets in the specific order.	UDP protocol has no fixed order because all packets are independent of each other.
The speed for TCP is slower.	UDP is faster as error recovery is not attempted.
Header size is 20 bytes	The header size is 8 bytes.
TCP is heavy-weight. TCP needs three packets to set up a socket connection before any user data can be sent.	UDP is lightweight. There are no tracking connections, ordering of messages, etc.
TCP does error checking and also makes error recovery.	UDP performs error checking, but it discards erroneous packets.

Acknowledgment segments	No Acknowledgment segments
Using handshake protocol like SYN, SYN-ACK, ACK	No handshake (so connectionless protocol)
TCP is reliable as it guarantees delivery of data to the destination router.	The delivery of data to the destination can't be guaranteed in UDP.
TCP offers extensive error checking mechanisms because it provides flow control and acknowledgment of data.	UDP has just a single error checking mechanism that is used for checksums.

What are the important differences between MAC address and IP address

Here, are some difference between MAC and IP address:

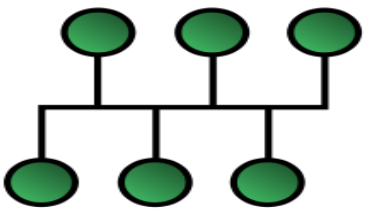
MAC	IP address
The MAC address stands for Media Access Control Address.	IP address stands for Internet Protocol Address.
It consists of a 48-bit address.	It consists of a 32-bit address.
MAC address works at the link layer of the OSI model.	IP address works at the network layer of OSI model.
It is referred to as a physical address.	It is referred to as a logical address.
You can retrieve the MAC address of any device using ARP protocol.	You can retrieve the MAC address of any device RARP protocol.
Classes are not used in MAC address.	In IP, IPv4 uses A, B, C, D, and E classes.

What is Network Topology?

Ans. Network topology is the physical or logical arrangement in which the devices or nodes of a network (e.g. computers, printers, servers, hubs, switches, routers, etc.) are interconnected with each other over a communication medium. It consists of two parts – the physical topology, which is the actual arrangement of the cables (the media), and the logical topology, which defines how the hosts access the media.

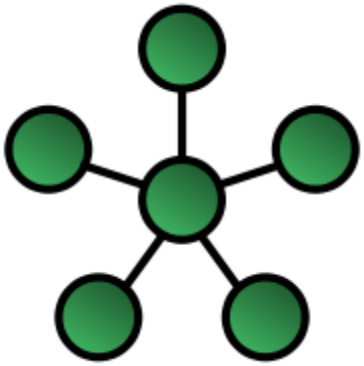
Types of network topologies –

Bus – In the bus network topology, each workstation is connected to a main cable called a bus. Therefore, in effect, each workstation is directly connected to every other workstation on the network.



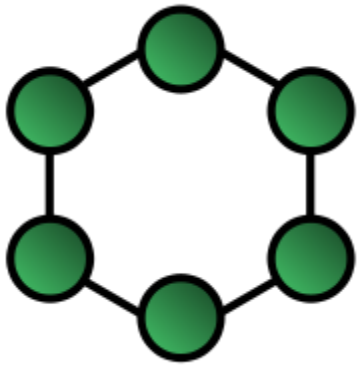
Bus network topology

Star – In the star network topology, there is a central computer or server to which all workstations are directly connected. Each workstation is indirectly connected to each other through the central computer.



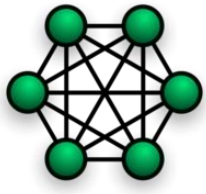
Star network topology

Ring – In the ring network topology, the workstations are connected in a closed loop configuration. Adjacent workstation pairs are directly connected. Other pairs of workstations are indirectly connected, passing data through one or more intermediate nodes.

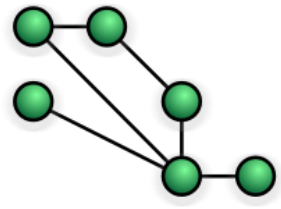


Ring network topology

Mesh – Mesh network topology has two forms – full and partial mesh. In the full mesh topology, each workstation is directly connected to each other. In the partial mesh topology, some workstations are connected to all the others, and some are connected only to the other nodes with which they exchange more data.

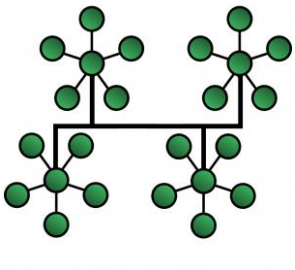


Fully Connected Mesh



Partial Mesh Network Topology

Tree – The tree network topology uses two or more star networks connected to each other. The central computers in star networks are connected to a main bus. Thus, a tree network is a bus network of star networks.



Tree Network Topology

Signal – Signal or Logical topology refers to the nature of the paths that signals follow from node to node. In many cases, the logical topology is the same as the physical topology. But it's not always like this. For example, some networks are physically arranged in a star configuration, but they function logically as bus or ring networks.

What are the different ways to exchange data?

Ans. Following are the different ways to exchange data:

- Simplex
- Half-duplex
- Full-duplex