**CN**

Q1:- What is the difference between physical topology and logical topology?

A physical topology describes how computers are connected with each other’s physically. While a logical topology describes how data is transmitted over the physical topology.

Q2:- What is the cookie?

A cookie is a small piece of information that is stored in user’s browser by a website for various purposes such as tracking, advertising, etc.

Q3:- What is an IP address?

An IP address is a unique identity of an interface in IP network. An IP address consists 32 bits. These bits are divided in four equal sections. Sections are separated by periods and written in a sequence.

Q4:- What is the difference between baseband and broadband technology?

Both technologies are used to transmit the signals in wire. Baseband technology uses bidirectional digital signals for transmission which mean a single channel is used for both sending and receiving data singles. Broadband uses unidirectional analog signals for transmission which means two separate channels are used for sending and receiving the data.

Q5:- What is the Bandwidth?

Bandwidth is the amount of data a cable can carry. Bandwidth is computed by subtracting the lower frequency of data signals from the higher one. For digital signal, it is measured in bps (bits per seconds) and for analog signal it is measured in Hz (Hertz).

Q6:- What is the use of ARP and RARP in network?

In LAN network, a node needs two addresses (IP address and MAC address) to communicate with others. When it has only the one address and needs the other address, it uses ARP and RARP. It uses ARP, when it has IP address and needs MAC address of other node. It uses RARP, when it has MAC address and needs IP address of other node.

Q7:- What is a junk email?

A junk mail is an unsolicited mail. Usually it contains newsletters or advertising contents and it arrives from an address which is not listed in address book.

Q8:- What is the Auto Responder in email system?

In email system, Auto Responder is a service that automatically sends prewritten answer e-mail to the sender as soon as it receives e-mail.

Q9:- What is the Packet Sniffer?

Packet Sniffer is a program or device that captures data packet from wire.

Q10:-What is the Telnet?

Telnet is a program that allows users to remotely access the system or device in which it is running.

Q11:- In OSI model, what is the Encapsulation?

Encapsulation is the process of preparing data for transmission. In this process, first the data is encrypted and compressed. Later this data is packaged through the layers. Each layer adds its own individual information in header. In transmission this information is read and used by various devices and protocols to deliver this package at correct destination.

Q12:- In OSI model, what is the Decapsulation?

Decapsulation is the process of extracting original data from encoded data package. When a data package is received from network, it is wrapped in several headers. In this process, these headers are removed. Once headers are removed, package data is decrypted and decompressed.

Q13:- What is the ANSI?

The ANSI stands for American National Standards Institute. It is an organization that officially defines standards in America. The official website of ANSI is the www.ansi.org.

Q14:- Which layers in OSI model are known as lower layers?

Application, Data Link and Network layers are known as lower layers.

Q15:- Which are the upper layers in OSI model?

The upper layers in OSI model are Application, Presentation, Session and Transport.

Q33:- What do the extensions .com, .net, .org, .info, .biz and .in stand for?

The extensions .com, .net, .org, .info, .biz and .in stand for commercial, network, organization, information, business and India respectively.

Q34:- What is a MAC address?

MAC address is the physical address of a NIC. It is 48 bits in length. It is written in Hexadecimal format. Usually it is stored in ROM of NIC.

Q18:- What does a router use to determine the best path to a destination? Routing table

Q19:- What is used on the Internet to find the numeric address of a computer host that resides on the Internet? DNS server

Q20:- What is a daemon?

A daemon is an application or a process that is running on a server for the purpose of providing client and server access and communication.

Q21:- What functionality can be used to disguise addresses from a private address space to be seen on the Internet? NAT (Network Address Translation)

Q22:- What is the protocol that resolves IP addresses to hardware addresses? ARP (Address Resolution Protocol)

Q23:- What is a proprietary standard?

A proprietary standard is a standard that is developed and owned by a specific vendor.

Q24:- What is a de facto standard?

A de facto standard is a standard that began as a proprietary standard and then grew to a standard that is used by pretty much everyone.

Q25:- What is the maximum rate of collision in a healthy Ethernet LAN?

Collision rate should not be more than 30% in a healthy Ethernet.

Q26:- When a broadcast is made in Ethernet LAN, which devices examine it?

A broadcast message is examined by all devices in network.

Q27:- Is broadcast message intended for a specific device in network?

No, broadcast message is intended for all devices in network.

Q28:- What does OSI stand for?

OSI stands for Open System Interconnection.

Q29:- What does FTP stand for?

FTP stands for File Transfer Protocol.

Q30:- What does DHCP stand for?

DHCP stands for Dynamic host configuration protocol.

Q31:- What is a router?

Router is a device that is used to connect two different networks.

Q32:- What is a MAU?

MAU (Multi-station Access Unit) is a topology specific Hub. In term of functionalities and characteristics, it is same as Hub. But it is only used in token ring.

Q33:- Which is the bottom layer of OSI model?

Physical layer is the bottom layer of OSI model.

Q34:- Which is the top layer of OSI model?

Application layer is the top layer of OSI model.

Q35:- What does the term driver refer in computer networking?

A driver is the software that contains technical information about a specific device. This information includes what that specific device is, how it works in system and what it needs to communicate and coexist with other devices.

Q36:- Are 10Base2 and 10Base5 Ethernet architectures used in modern network?

No, both architectures are used in bus topology which is no longer used to build the networks.

Q37:- In which topology 10BaseT architecture is used?

10BaseT architecture is used in start topology. It provides maximum 10 Mbps speed. It uses Baseband transmission technology and UTP (CAT-3) cable.

Q38:- In Bus topology, to remove a workstation from the network, the T connector is removed from NIC. Will this network work normally?

Yes, this network will work normally because removing T connector does not interrupt the signal flow in main cable.

Q39:- What is a drop cable?

A drop cable is a cable that connects workstation with backbone cable in bus topology.

Q40:- What is the maximum length of Thicknet coaxial cable?

Maximum length of Thicknet coaxial cable is 500 meter.

Q41:- Which cable is known as the RG58 cable?

The Thinnet cable is known as the RG58 cable.

Q42:- Why coaxial cable is no longer used in computer network?

Coaxial cable is used in bus topology. Bus topology is no longer used in computer network.

Q43:- What is the maximum distance of UTP cable?

Maximum distance of UTP cable is 100 meter.

Q44:- Which connector is used to connect UTP cable with NIC?

RJ45 connector is used to connect the UTP cable with NIC.

Q45:- Which cable uses RJ11 connector?

The telephone cable uses RJ11 connector.

Q46:- Can we use Cateogry1 (UTP) cable for data transmission?

No, we can’t use Cateogry1 (UTP) cable for data transmission. It is used in telephone network for voice transmission.

Q47:- Which port does the PING use?

The PING does not use any port. Any application, which operates in layer 4, needs port. Since PING is a layer 3 network management tool, it does not require any port to operate.

Q48:- Which topology uses a centralized device for connectivity?

Star topology uses a centralized device (HUB or Switch) for connectivity.

Q49:- Which topology uses coaxial cable and terminators?

Bus topology uses coaxial cable and terminators.

Q50:- What is the daisy chaining technique and which topology uses this technique?

Star topology uses the daisy chaining technique to extend the network. In this technique, a hub or switch is connected to another hub or switch as the node of the existing topology. Then that hub or switch is used to connect the more devices in network.

Q51:- What is the signal bouncing issue and how it can be solved?

Signal bouncing issue occurs in bus topology. Bus topology uses coaxial cable to connect the computers. In this topology when a computer sends signal, the signal travels in both directions from the sending computer. When this signal reaches at the end of the cable, it bounces back and returns in the original direction. This is known as signal bouncing issue. To solve this issue, terminators are used in both ends of the cable. Terminator absorbs the signals, when they reach to it. This resolves the signal bouncing issue.

Q52:- What is the backbone network?

The network which connects two or more networks together is considered as a backbone network. Usually backbone network contains high speed data transferring devices such as routers and switches. Backbone network should never be used for end user connectivity. The network which provides end user connectivity should be connected through the backbone network.

Q53:- What is the PAN network and how it is different from the LAN network?

A PAN network is the shorter version of LAN network. Unlike LAN networks which are mainly built for a group of users, PAN networks are built for individual users. Usually a PAN network is built to connect multiple personal devices such as smartphone, PDA, laptop and computer together for data sharing.

Q53:- A company has offices in Jaipur and Delhi. What type of computer network it will use to connect these offices?

WAN (Wide Area Network) network is used to connect the networks which are spread over the different geographical location.

Q54:- What is the intranet?

The term intranet refers an IP based network which is administered and controlled by a single entity. In this type of network, only authorized users are allowed to access the network resource.

Q55:- A company does not have sufficient budget for lease line connection. Which cost effective alternate will you suggest for this company?

VPN (Virtual Private Network) is the cost effective alternative for leased line.

Q56:- A company wants to extend its intranet network to certain business partners. What type of network it has to build?

Extranet, when we extend the intranet to external parties, we create Extranet.

Q57:- How many wires does UTP cable contain?

UTP cable contains four pairs of wires. Each pair has two wires which are twisted with each other. This way, there are total eight wires in a UTP cable.

Q58:- How many wires are used for data transmission in UTP cable?

In UTP cable, from eight wires, only four wires are used for data transmission.

Q59:- Which wires are used for data transmission in UTP cable?

In UTP cable, wire 1, 2, 3 and 6 are used for data transmission. The wire 1 and 2 are used to transmit the data while wires 3 and 6 are used to receive the data.

Q60:- What is the maximum data transmission speed of Category 5 UTP cable, Category 5e UTP cable and Category 6 UTP cable?

The maximum transmission speed of Category 5 UTP cable, Category 5e UTP cable and Category 6 UTP cable is 100Mbps, 1000Mbps and 10Gbps respectively.

Q61:- There are two pairs of cables; RG58 & RG8 and RG59 & RG6. From these, which pair is used in computer network and where remaining is used?

RG58 and RG8 cables are used in computer network while RG59 and RG6 cables are used in TV cable network.

Q62:- Can we use RG59 and RG6 cables in computer network?

No, these cables can’t be used in computer network. These cables are built for cable TV network.

Q63:- Is coaxial cable still used in computer network? No

Q64:- What is the maximum data transmission speed of Category 2 UTP cable, Category 3 UTP cable and Category 4 UTP cable?

The maximum transmission speed of Category 2 UTP cable, Category 3 UTP cable and Category 4 UTP cable is 4 Mbps, 10 Mbps and 16 Mbps respectively.

Q65:- What is the 802.3 and what it defines?

IEEE 802.3 is a collection of IEEE standards. It defines standards for Physical layer including access methods used in Data Link Layer.

Q66:- What is the 5-4-3 rule and in which architecture it is used?

The 5-4-3 rule is used in 10Base2 and 10Base5 Ethernet architectures. In this rule, there can be maximum five segments in a network, connected with four repeaters. From these five segments, only three segments can be populated with nodes.

Q67:- What does 10Base2 stand for?

In 10Base2 architecture, 10 stands for speed, Base stands for Baseband transmission and 2 stands for 200 meters (Maximum distance it can span).

Q68:- What are the differences between a TCP port and a physical port?

A TCP port is a logical number. Transport layer uses it for the connection multiplexing. In connection multiplexing a local process is mapped with remote node by using the port numbers.

A physical port is the connection point of a node. External device or cable connects with node on this port.

Q68:- Why IP protocol is considered a connectionless protocol?

An IP protocol is considered a connectionless protocol because it does not establish a connection before sending data to endpoint.

Q69:- What is a Link?

A Link is a physical or logical connection between two nodes in network.

Q70:- What is a Node?

In network any device or system that has a NIC and uses an IP address to communicate with others is considered as a node.

Q71:- List any five application which uses TCP port.

Telnet, FTP, SSH, SMTP and POP

Q72:- What are the 2 sub layers of the Data Link layer?

Logical Link Control (LLC) and Media Access Control (MAC)

Q73:- What technology can be used to create a point-to-point network connection over the Internet?

VPN (virtual private network)

Q74:- What does NIC stand for? network interface controller.

Q75:- In which layers of OSI model, does NIC operate?

NIC operates in layer1 and layer2 of OSI model.

Q76:- Which Ethernet architecture uses BNC connector?

10Base2 and 10Base5 Ethernet architectures use BNC connector.

Q77:- Which access method is used in 1000BaseTX network?

CSMA/CD access method is used in 1000BaseTX network.

Q78:- How many network segments can be populated in 10Base2?

Maximum three network segments can be populated in 10Base2.

Q79:- Which cable is used in 10BaseFL network?

Fiber optical cable is used in 10BaseFL network.

Q80:- What is the maximum length of Thinnet cable?

Maximum length of the Thinnet cable is 185 meter.

Q81:- Which cable is known as the RG8 cable?

Thicknet cable is known as the RG8 cable.

Q82:- Which cable is used as the backbone cable in bus topology?

Thicknet (RG8) cable is used as the backbone cable in bus topology.

Q83:- What does ISO stand for?

ISO stands for International Organization for Standardization.

Q84:- What does OSI stand for?

OSI stands for Open System Interconnection.

Q85:- What is the OSI layer model?

OSI Layer model is a logical structure which defines the process of data transmission from one computer to other computer.

Q86:- How many layers are there in OSI model?

There are seven distinct layers in OSI model. The names of layer are Physical, Data link, Network, Transport, Session, Presentation and Application.

Q87:- What is a unicast message?

Unicast message is a message that is sent on a specific address and intended for a specific node in network.

Q88:- What is a multicast message?

Multicast message is a message that is sent on a multicast address and intended for a group of nodes in network.

Q89:- What is a broadcast message?

Broadcast message is a message that is sent on a broadcast address and intended for all nodes of network.

Q90:- What does the standard IEEE802.3ab define?

IEEE802.3ab standard defines 1000BaseTX Ethernet implementation. 1000BaseTX uses UTP (CAT 5e or CAT6) cable. It provides speed of 1000Mbps. It supports a maximum distance of 100 meter.

Q91:- What is a Mail Gateway?

It is a system that performs a protocol translation between different electronic mail delivery protocols.

Q92:- Which network does VPN uses for data transportation?

VPN uses public network such as Internet for data transportation.

Q93:- What is the use of tunneling protocols in VPN?

In VPN, tunneling protocols are used for data encryption and decryption.

Q94:- How many classes are there in IPv4? 5

Q95:- What is the range of each class in IPv4?

|  |  |  |
| --- | --- | --- |
| Class | Starting address | Ending address |
| A | 0.0.0.0 | 127.255.255.255 |
| B | 128.0.0.0 | 191.255.255.255 |
| C | 192.0.0.0 | 223.255.255.255 |
| D | 224.0.0.0 | 239.255.255.255 |
| E | 240.0.0.0 | 255.255.255.255 |

Q96:- What does the term Pipelining describe?

Pipelining describes the sequencing of processes. When an additional task is started before ongoing task is finished, it is known as sequencing.

Q97:- What is difference between Baseband and Broadband transmission?

In Baseband transmission, only one signal is allowed to transmit at a time. While in Broadband transmission, multiple signals are allowed to transmit simultaneously.

Q98:- What does the SLIP stand for?

The SLIP stands for Serial Line Interface Protocol. It is used in WAN technology for transmitting IP datagrams over a serial line.

Q99:- Which measurement unit is used to measure the transmission speed of Ethernet?

The transmission speed of Ethernet is measured in Mbps (millions of bits per second).

Q100:- What are the key elements of a protocol?

A protocol is a set of rules which is used to govern all the aspects of information communication. There are three key elements in a protocol; Syntax, Semantics and Timing. Syntax defines the format in which data is displayed. Semantics describes the data bits of each section. Timing controls what time and how fast data is transmitted.

That’s all for this article. If you have any suggestion, comment or feedback about this article, please mail me. If you like this collection, please do not forget to share it from your favorite social platform.

**Q #1) What is a Network?**

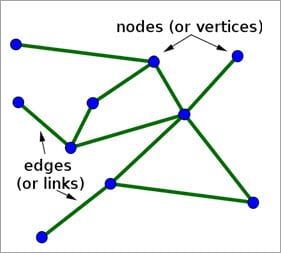
**Answer:** Network is defined as a set of devices connected to each other using a physical transmission medium.

**For Example,** A computer network is a group of computers connected with each other to communicate and share information and resources like hardware, data, and software. In a network, nodes are used to connect two or more networks.

**Q #2) What is a Node?**

**Answer:** Two or more computers are connected directly by an optical fiber or any other cable. A node is a point where a connection is established. It is a network component that is used to send, receive and forward the electronic information.

A device connected to a network is also termed as Node. Let’s consider that in a network there are 2 computers, 2 printers, and a server are connected, then we can say that there are five nodes on the network.

[](https://cdn.softwaretestinghelp.com/wp-content/qa/uploads/2018/01/Nodes.jpg)

**Q #3) What is Network Topology?**

**Answer:** Network topology is a physical layout of the computer network and it defines how the computers, devices, cables, etc are connected to each other.

**Q #4) What are Routers?**

**Answer:** The router is a network device that connects two or more network segments. It is used to transfer information from the source to the destination.

Routers send the information in terms of data packets and when these data packets are forwarded from one router to another router then the router reads the network address in the packets and identifies the destination network.

**Q #5) What is the OSI reference model?**

**Answer:** **O**pen**S**ystem **I**nterconnection, the name itself suggests that it is a reference model that defines how applications can communicate with each other over a networking system.

It also helps to understand the relationship between networks and defines the process of communication in a network.

**Q #6) What are the layers in OSI Reference Models? Describe each layer briefly.**

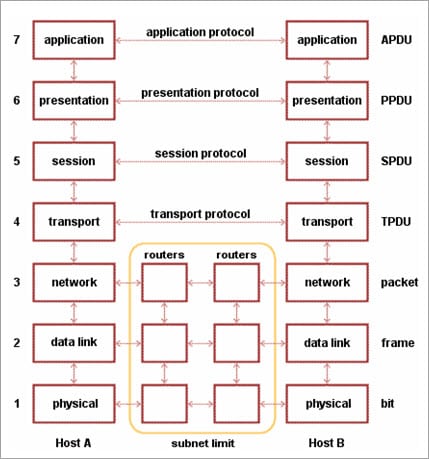
**Answer:** **Given below are the seven layers of OSI Reference Models:**

**a) Physical Layer** **(Layer 1):**It converts data bits into electrical impulses or radio signals. **Example:** Ethernet.

**b) Data Link Layer (Layer 2):** At the Data Link layer, data packets are encoded and decoded into bits and it provides a node to node data transfer. This layer also detects the errors that occurred at Layer 1.

**c) Network Layer** **(Layer 3):** This layer transfers variable length data sequence from one node to another node in the same network. This variable-length data sequence is also known as **“Datagrams”**.

**d) Transport Layer (Layer 4):** It transfers data between nodes and also provides acknowledgment of successful data transmission. It keeps track of transmission and sends the segments again if the transmission fails.

[](https://cdn.softwaretestinghelp.com/wp-content/qa/uploads/2018/01/OSI-Reference-Model.jpg)

*[image*[*source*](http://searchnetworking.techtarget.com/)*]*

**e) Session Layer (Layer 5):** This layer manages and controls the connections between computers. It establishes, coordinates, exchange and terminates the connections between local and remote applications.

**f) Presentation Layer (Layer 6):** It is also called as “Syntax Layer”. Layer 6 transforms the data into the form in which the application layer accepts.

**g) Application Layer** **(Layer 7):** This is the last layer of the OSI Reference Model and is the one that is close to the end-user. Both end-user and application layer interacts with the software application. This layer provides services for email, file transfer, etc.

**Q #7) What is the difference between Hub, Switch, and Router?**

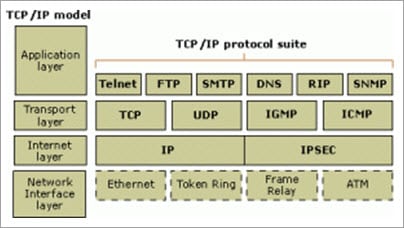
**Answer:**

| **Hub** | **Switch** | **Router** |
| --- | --- | --- |
| Hub is least expensive, least intelligent and least complicated of the three. It broadcast all data to every port which may cause serious security and reliability concern | Switches work similarly like Hubs but in a more efficient manner. It creates connections dynamically and provides information only to the requesting port | The router is smartest and most complicated out of these three. It comes in all shapes and sizes. Routers are similar like little computers dedicated for routing network traffic |
| In a Network, Hub is a common connection point for devices connected to the network. Hub contains multiple ports and is used to connect segments of LAN | Switch is a device in a network which forwards packets in a network | Routers are located at gateway and forwards data packets |

**Q #8) Explain TCP/IP Model**

**Answer:** The most widely used and available protocol is TCP/IP i.e. Transmission Control Protocol and Internet Protocol. TCP/IP specifies how data should be packaged, transmitted and routed in their end to end data communication.

**There are four layers as shown in the below diagram:**

[](https://cdn.softwaretestinghelp.com/wp-content/qa/uploads/2018/01/TCP.jpg)

**Given below is a brief explanation of each layer:**

* **Application Layer**: This is the top layer in the TCP/IP model. It includes processes that use the Transport Layer Protocol to transmit the data to their destination. There are different Application Layer Protocols such as HTTP, FTP, SMTP, SNMP protocols, etc.
* **Transport Layer**: It receives the data from the Application Layer which is above the Transport Layer. It acts as a backbone between the host’s system connected with each other and it mainly concerns about the transmission of data. TCP and UDP are mainly used as Transport Layer protocols.
* **Network or Internet Layer**: This layer sends the packets across the network. Packets mainly contain source & destination IP addresses and actual data to be transmitted.
* **Network Interface Layer**: It is the lowest layer of the TCP/IP model. It transfers the packets between different hosts. It includes encapsulation of IP packets into frames, mapping IP addresses to physical hardware devices, etc.

**Q #9) What is HTTP and what port does it use?**

**Answer:** HTTP is HyperText Transfer Protocol and it is responsible for web content. Many web pages are using HTTP to transmit the web content and allow the display and navigation of HyperText. It is the primary protocol and port used here is TCP port 80.

**Q #10) What is HTTPs and what port does it use?**

**Answer:** HTTPs is a Secure HTTP. HTTPs is used for secure communication over a computer network. HTTPs provides authentication of websites that prevents unwanted attacks.

In bi-directional communication, the HTTPs protocol encrypts the communication so that the tampering of the data gets avoided. With the help of an SSL certificate, it verifies if the requested server connection is a valid connection or not. HTTPs use TCP with port 443.

**Q #11) What are TCP and UDP?**

**Answer:** **Common factors in TCP and UDP are:**

* TCP and UDP are the most widely used protocols that are built on the top of the IP protocol.
* Both protocols TCP and UDP are used to send bits of data over the Internet, which is also known as ‘packets’.
* When packets are transferred using either TCP or UDP, it is sent to an IP address. These packets are traversed through routers to the destination.

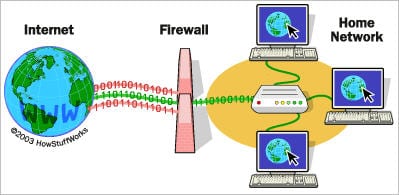
**The difference between TCP and UDP are enlisted in the below table:**

| **TCP** | **UDP** |
| --- | --- |
| TCP stands for Transmission Control Protocol | UDP is stands for User Datagram Protocol or Universal Datagram Protocol |
| Once the connection is setup, data can be sent bi-directional i.e. TCP is a connection oriented protocol | UDP is connectionless, simple protocol. Using UDP, messages are sent as packets |
| The speed of TCP is slower than UDP | UDP is faster compared to TCP |
| TCP is used for the application where time is not critical part of data transmission | UDP is suitable for the applications which require fast transmission of data and time is crucial in this case. |
| TCP transmission occurs in a sequential manner | UDP transmission also occurs in a sequential manner but it does not maintain the same sequence when it reaches the destination |
| It is heavy weight connection | It is lightweight transport layer |
| TCP tracks the data sent to ensure no data loss during data transmission | UDP does not ensure whether receiver receives packets are not. If packets are misses then they are just lost |

**Q #12) What is a Firewall?**

**Answer:** Firewall is a network security system that is used to protect computer networks from unauthorized access. It prevents malicious access from outside to the computer network. A firewall can also be built to grant limited access to outside users.

The firewall consists of a hardware device, software program or a combined configuration of both. All the messages that route through the firewall are examined by specific security criteria and the messages which meet the criteria are successfully traversed through the network or else those messages are blocked.

**[](https://cdn.softwaretestinghelp.com/wp-content/qa/uploads/2017/08/firewall.jpg)**

*[image*[*source*](https://www.comodo.com/)*]*

Firewalls can be installed just like any other computer software and later can be customized as per the need and have some control over the access and security features. “

Windows Firewall” is an inbuilt Microsoft Windows application that comes along with the operating system. This “Windows Firewall” also helps to prevent viruses, worms, etc.

**Q #13) What is DNS?**

**Answer:**Domain Name Server (DNS), in a non-professional language and we can call it an Internet’s phone book. All the public IP addresses and their hostnames are stored in the DNS and later it translates into a corresponding IP address.

For a human being, it is easy to remember and recognize the domain name, however, the computer is a machine that does not understand the human language and they only understand the language of IP addresses for data transfer.

There is a “Central Registry” where all the domain names are stored and it gets updated on a periodic basis. All Internet service providers and different host companies usually interact with this central registry to get the updated DNS details.

**For Example**, When you type a website [www.softwaretestinghelp.com](https://www.softwaretestinghelp.com/), then your Internet service provider looks for the DNS associated with this domain name and translates this website command into a machine language – IP address – 151.144.210.59 (note that, this is the imaginary IP address and not the actual IP for the given website) so that you will get redirected to the appropriate destination.

**This process is explained in the below diagram:**

[](https://cdn.softwaretestinghelp.com/wp-content/qa/uploads/2018/01/DNS.jpg)

*[image*[*source*](https://www.ctrlswitches.com/)*]*

**Q #14) What is the difference between a Domain and a Workgroup?**

**Answer:**In a computer network, different computers are organized in different methods and these methods are – Domains and Workgroups. Usually, computers which run on the home network belong to a Workgroup.

However, computers that are running on an office network or any workplace network belong to the Domain.

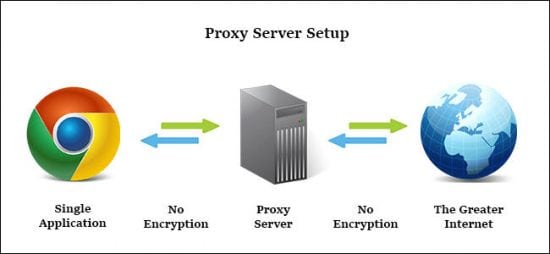
**Their differences are as follows:**

| **Workgroup** | **Domain** |
| --- | --- |
| All computers are peers and no computer has control over another computer | Network admin uses one or more computer as a server and provide all accesses, security permission to all other computers in a network |
| In a Workgroup, each computer maintains their own database | The domain is a form of a computer network in which computers, printers, and user accounts are registered in a central database. |
| Each computer has their own authentication rule for every user account | It has centralized authentication servers which set the rule of authentication |
| Each computer has set of user account. If user has account on that computer then only user able to access the computer | If user has an account in a domain then user can login to any computer in a domain |
| Workgroup does not bind to any security permission or does not require any password | Domain user has to provide security credentials whenever they are accessing the domain network |
| Computer settings need to change manually for each computer in a Workgroup | In a domain, changes made in one computer automatically made same changes to all other computers in a network |
| All computers must be on same local area network | In a domain, computers can be on a different local network |
| In a Workgroup, there can be only 20 computers connected | In a domain, thousands of computers can be connected |

**Q #15) What is a Proxy Server and how do they protect the computer network?**

**Answer:**For data transmission, IP addresses are required and even DNS uses IP addresses to route to the correct website. It means without the knowledge of correct and actual IP addresses it is not possible to identify the physical location of the network.

Proxy servers prevent external users who are unauthorized to access such IP addresses of the internal network. It makes the computer network virtually invisible to external users.

[](https://cdn.softwaretestinghelp.com/wp-content/qa/uploads/2017/08/proxy-server-e1504182916814.jpg)

Proxy Server also maintains the list of blacklisted websites so that the internal user is automatically prevented from getting easily infected by viruses, worms, etc.

**Q #16) What are IP classes and how can you identify the IP class of given an IP address?**

**Answer:**An IP address has 4 sets (octets) of numbers each with a value up to 255.

**For Example**, the range of the home or commercial connection started primarily between 190 x or 10 x. IP classes are differentiated based on the number of hosts it supports on a single network. If IP classes support more networks then very few IP addresses are available for each network.

There are three types of IP classes and are based on the first octet of IP addresses which are classified as Class A, B or C. If the first octet begins with 0 bit then it is of type Class A.

Class A type has a range up to 127.x.x.x (except 127.0.0.1). If it starts with bits 10 then it belongs to Class B. Class B having a range from 128.x to 191.x.  IP class belongs to Class C if the octet starts with bits 110. Class C has a range from 192.x to 223.x.

**Q #17) What is meant by 127.0.0.1 and localhost?**

**Answer:**IP address 127.0.0.1, is reserved for loopback or localhost connections. These networks are usually reserved for the biggest customers or some of the original members of the Internet. To identify any connection issue, the initial step is to ping the server and check if it is responding.

If there is no response from the server then there are various causes like the network is down or the cable needs to be replaced or the network card is not in good condition. 127.0.0.1 is a loopback connection on the Network Interface Card (NIC) and if you are able to ping this server successfully, then it means that the hardware is in a good shape and condition.

127.0.0.1 and localhost are the same things in most of the computer network functioning.

**Q #18) What is NIC?**

**Answer:**NIC stands for Network Interface Card. It is also known as Network Adapter or Ethernet Card. It is in the form of an add-in card and is installed on a computer so that the computer can be connected to a network.

Each NIC has a MAC address which helps in identifying the computer on a network.

**Q #19) What is Data Encapsulation?**

**Answer:** In a computer network, to enable data transmission from one computer to another, the network devices send messages in the form of packets. These packets are then added with the IP header by the OSI reference model layer.

The Data Link Layer encapsulates each packet in a frame that contains the hardware address of the source and the destination computer. If a destination computer is on the remote network then the frames are routed through a gateway or router to the destination computer.

**Q #20) What is the difference between the Internet, Intranet, and Extranet?**

**Answer:** The terminologies Internet, Intranet, and Extranet are used to define how the applications in the network can be accessed. They use similar TCP/IP technology but differ in terms of access levels for each user inside the network and outside the network.

* **Internet**: Applications are accessed by anyone from any location using the web.
* **Intranet**: It allows limited access to users in the same organization.
* **Extranet**: External users are allowed or provided with access to use the network application of the organization.

**Q #21) What is a VPN?**

**Answer:** VPN is the Virtual Private Network and is built on the Internet as a private wide area network. Internet-based VPNs are less expensive and can be connected from anywhere in the world.

VPNs are used to connect offices remotely and are less expensive when compared to WAN connections. VPNs are used for secure transactions and confidential data can be transferred between multiple offices. VPN keeps company information secure against any potential intrusion.

**Given below are the 3 types of VPN’s:**

1. **Access VPN**: Access VPN’s provide connectivity to mobile users and telecommuters. It is an alternative option for dial-up connections or ISDN connections. It provides low-cost solutions and a wide range of connectivity.
2. **Intranet VPN**: They are useful for connecting remote offices using shared infrastructure with the same policy as a private network.
3. **Extranet VPN**: Using shared infrastructure over an intranet, suppliers, customers, and partners are connected using dedicated connections.

**Q #22) What are Ipconfig and Ifconfig?**

**Answer: Ipconfig** stands for Internet Protocol Configuration and this command is used on Microsoft Windows to view and configure the network interface.

The command Ipconfig is useful for displaying all TCP/IP network summary information currently available on a network.  It also helps to modify the DHCP protocol and DNS setting.

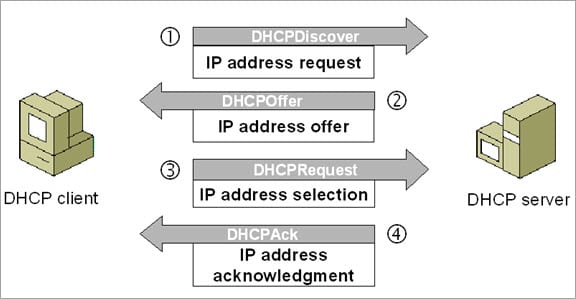
**Ifconfig** (Interface Configuration) is a command that is used on Linux, Mac, and UNIX operating systems. It is used to configure, control the TCP/IP network interface parameters from CLI i.e. Command Line Interface. It allows you to see the IP addresses of these network interfaces.

**Q #23) Explain DHCP briefly?**

**Answer:** DHCP stands for Dynamic Host Configuration Protocol and it automatically assigns IP addresses to the network devices. It completely removes the process of manual allocation of IP addresses and reduces the errors caused due to this.

This entire process is centralized so that the TCP/IP configuration can also be completed from a central location. DHCP has a “pool of IP addresses” from which it allocates the IP address to the network devices. DHCP cannot recognize if any device is configured manually and assigned with the same IP address from the DHCP pool.

In this situation, it throws the “IP address conflict” error.

[](https://cdn.softwaretestinghelp.com/wp-content/qa/uploads/2018/01/DHCP.jpg)

DHCP environment requires DHCP servers to set-up the TCP/IP configuration. These servers then assign, release and renew the IP addresses as there might be a chance that network devices can leave the network and some of them can join back to the network.

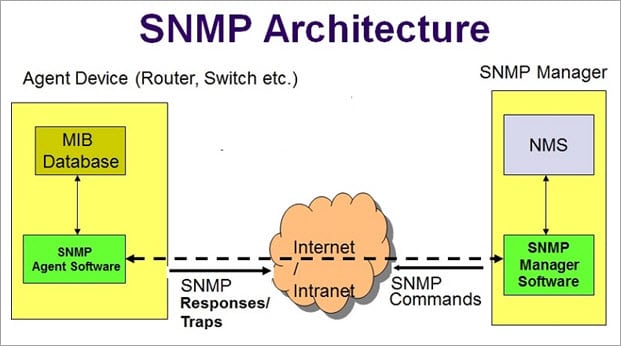
**Q #24) What is SNMP?**

**Answer:** SNMP stands for Simple Network Management Protocol. It is a network protocol used for collecting organizing and exchanging information between network devices. SNMP is widely used in network management for configuring network devices like switches, hubs, routers, printers, servers.

**SNMP consists of the below components:**

* SNMP Manager
* Managed device
* SNMP Agent
* Management Information Base (MIB)

**The below diagram shows how these components are connected with each other in the SNMP architecture:**

[](https://cdn.softwaretestinghelp.com/wp-content/qa/uploads/2018/01/SNMP.jpg)

SNMP is a part of the TCP/IP suite. There are 3 main versions of SNMP which include SNMPv1, SNMPv2, and SNMPv3.

**Q #25) What are the different types of a network? Explain each briefly.**

**Answer:** There are 4 major types of networks.

**Let’s take a look at each of them in detail.**

1. **Personal Area Network (PAN)**: It is the smallest and basic network type that is often used at home. It is a connection between the computer and another device such as phone, printer, modem tablets, etc
2. **Local Area Network (LAN)**: LAN is used in small offices and Internet cafes to connect a small group of computers to each other. Usually, they are used to transfer a file or for playing the game in a network.
3. **Metropolitan Area Network (MAN):**It is a powerful network type than LAN. The area covered by MAN is a small town, city, etc. A huge server is used to cover such a large span of area for connection.
4. **Wide Area Network (WAN)**: It is more complex than LAN and covers a large span of the area typically a large physical distance. The Internet is the largest WAN which is spread across the world. WAN is not owned by any single organization but it has distributed ownership.

**There are some other types of the network as well:**

* Storage Area Network (SAN)
* System Area Network (SAN)
* Enterprise Private Network (EPN)
* Passive Optical Local Area Network (POLAN)

**Q #26) Differentiate Communication and Transmission?**

**Answer:** Through Transmission the data gets transferred from source to destination (only one way). It is treated as the physical movement of data.

Communication means the process of sending and receiving data between two media (data is transferred between source and destination in both ways).

**Q #27) Describe the layers of the OSI model?**

**Answer:** OSI model stands for Open System Interconnection It is a framework that guides the applications on how they can communicate in a network.

**OSI model has seven layers. They are listed below,**

1. **Physical Layer**: Deals with transmission and reception of unstructured data through a physical medium.
2. **Data Link Layer:**Helps in transferring error-free data frames between nodes.
3. **Network Layer:**Decides the physical path that should be taken by the data as per the network conditions.
4. **Transport Layer:**Ensures that the messages are delivered in sequence and without any loss or duplication.
5. **Session Layer:**Helps in establishing a session between processes of different stations.
6. **Presentation Layer:**Formats the data as per the need and presents the same to the Application layer.
7. **Application Layer:**Serves as the mediator between Users and processes of applications.

**Q #28) Explain various types of networks based on their sizes?**

**Answer:** The size of the network is defined as the geographic area and the number of computers covered in it. **Based on the size of the network they are classified as below:**

1. **Local Area Network (LAN):**A network with a minimum of two computers to a maximum of thousands of computers within an office or a building is termed as LAN. Generally, it works for a single site where people can share resources like printers, data storage, etc.
2. **Metropolitan Area Network (MAN):** It is larger than LAN and used to connect various LANs across small regions, a city, campus of colleges or universities, etc which in turn forms a bigger network.
3. **Wide Area Network (WAN):** Multiple LANs and MAN’s connected together form a WAN. It covers a wider area like a whole country or world.

**Q #29) Define various types of Internet connections?**

**Answer:** **There are three types of Internet connections. They are listed below:**

1. **Broadband Connection:**This type of connection gives continuous high-speed Internet. In this type, if we log off from the Internet for any reason then there is no need to log in again. **For Example,** Modems of cables, Fibres, wireless connection, satellite connection, etc.
2. **Wi-Fi:**It is a wireless Internet connection between the devices. It uses radio waves to connect to the devices or gadgets.
3. **WiMAX:** It is the most advanced type of Internet connection which is more featured than Wi-Fi. It is nothing but a high-speed and advanced type of broadband connection.

**Q #30) A few important terminologies we come across networking concepts?**

**Answer:** **Below are a few important terms we need to know in networking:**

* **Network:**A set of computers or devices connected together with a communication path to share data.
* **Networking:** The design and construction of a network are termed as networking.
* **Link:** The physical medium or the communication path through which the devices are connected in a network is called a Link.
* **Node:**The devices or the computers connected to the links are named as nodes.
* **Router/Gateway:**A device/computer/node that is connected to different networks is termed as a Gateway or Router. The basic difference between these two is that Gateway is used to control the traffic of two contradictory networks whereas the router controls the traffic of similar networks.
* **The router**is a switch that processes the signal/traffic using routing protocols.
* **Protocol:**A set of instructions or rules or guidelines that are used in establishing communications between computers of a network is called Protocol.
* **Unicasting:** When a piece of information or a packet is sent from a particular source to a specified destination then it is called Unicasting.
* **Anycasting:** Sending the datagrams from a source to the nearest device among the group of servers that provide the same service as the source is termed as Anycasting.
* **Multicasting:**Sending one copy of data from a single sender to multiple clients or receivers (selected clients) of the networks which are in need of such data.
* **Broadcasting:** Sending a packet to each device of the network is termed as broadcasting.

**Q #31) Explain the characteristics of networking?**

**Answer:** **The main characteristics of networking are** **mentioned below:**

* **Topology:** This deals with how the computers or nodes are arranged in the network. The computers are arranged physically or logically.
* **Protocols:** Deals with the process of how computers communicate with one another.
* **Medium:** This is nothing but the medium used by computers for communication.

**Q #32) How many types of modes are used in data transferring through networks?**

**Answer:** **Data transferring modes in computer networks are of three types. They are listed below,**

1. **Simplex:** Data transferring which takes place only in one direction is called Simplex. In Simplex mode, the data gets transferred either from sender to receiver or from receiver to sender. **For Example,**Radio signal, the print signal given from computer to printer, etc.
2. **Half Duplex:** Data transferring can happen in both directions but not at the same time. Alternatively, the data is sent and received. **For Example,**Browsing through the internet, a user sends the request to the server and later the server processes the request and sends back the web page.
3. **Full Duplex:** Data transferring happens in both directions that too simultaneously. **For Example,** Two-lane roads where traffic flows in both directions, communication through telephone, etc.

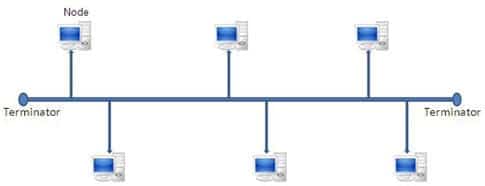
**Q #33) Name the different types of network topologies and brief their advantages?**

**Answer:** Network Topology is nothing but the physical or logical way in which the devices (like nodes, links, and computers) of a network are arranged. Physical Topology means the actual place where the elements of a network are located.

Logical Topology deals with the flow of data over the networks. A link is used to connect more than two devices of a network. And more than two links located nearby form a topology.

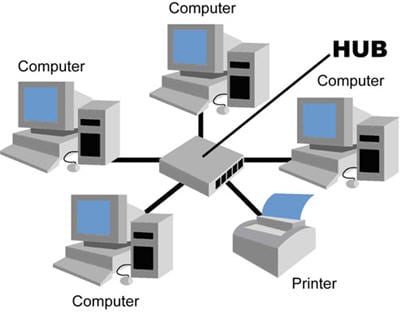
**Network topologies are classified as below:**

**a) Bus Topology:**In Bus Topology, all the devices of the network are connected to a common cable (also called as the backbone). As the devices are connected to a single cable, it is also termed as Linear Bus Topology.

[](https://cdn.softwaretestinghelp.com/wp-content/qa/uploads/2017/03/bus-topology.jpg)

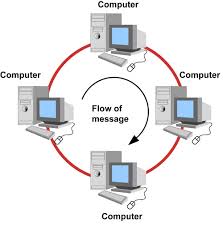
The advantage of bus topology is that it can be installed easily. And the disadvantage is that if the backbone cable breaks then the whole network will be down.

**b) Star Topology:**In Star Topology, there is a central controller or hub to which every node or device is connected through a cable. In this topology, the devices are not linked to each other. If a device needs to communicate with the other, then it has to send the signal or data to the central hub. And then the hub sends the same data to the destination device.

[](https://cdn.softwaretestinghelp.com/wp-content/qa/uploads/2017/03/star-topology.jpg)

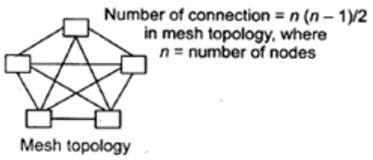
The advantage of the star topology is that if a link breaks then only that particular link is affected. The whole network remains undisturbed. The main disadvantage of the star topology is that all the devices of the network are dependent on a single point (hub). If the central hub gets failed, then the whole network gets down.

**c) Ring Topology:**In Ring Topology, each device of the network is connected to two other devices on either side which in turn forms a loop. Data or Signal in ring topology flow only in a single direction from one device to another and reaches the destination node.

[](https://cdn.softwaretestinghelp.com/wp-content/qa/uploads/2017/03/ring-topology.jpg)

The advantage of ring topology is that it can be installed easily. Adding or deleting devices to the network is also easy. The main disadvantage of ring topology is the data flows only in one direction. And a break at a node in the network can affect the whole network.

**d) Mesh Topology:**In a Mesh Topology, each device of the network is connected to all other devices of the network. Mesh Topology uses Routing and Flooding techniques for data transmission.

[](https://cdn.softwaretestinghelp.com/wp-content/qa/uploads/2017/03/mesh-topology.jpg)

The advantage of mesh topology is if one link breaks then it does not affect the whole network. And the disadvantage is, huge cabling is required and it is expensive.

**Q #34) What is the full form of IDEA?**

**Answer:** IDEA stands for International Data Encryption Algorithm.

**Q #35) Define Piggybacking?**

**Answer:** In data transmission, if the sender sends any data frame to the receiver then the receiver should send the acknowledgment to the sender. The receiver will temporarily delay (waits for the network layer to send the next data packet) the acknowledgment and hooks it to the next outgoing data frame, this process is called Piggybacking.

**Q #36) In how many ways the data is represented and what are they?**

**Answer:** Data transmitted through the networks’ comes in different ways like text, audio, video, images, numbers, etc.

* **Audio:**It is nothing but the continuous sound which is different from text and numbers.
* **Video:** Continuous visual images or a combination of images.
* **Images:** Every image is divided into pixels. And the pixels are represented using bits. Pixels may vary in size based on image resolution.
* **Numbers:**These are converted into binary numbers and are represented using bits.
* **Text:**Text is also represented as bits.

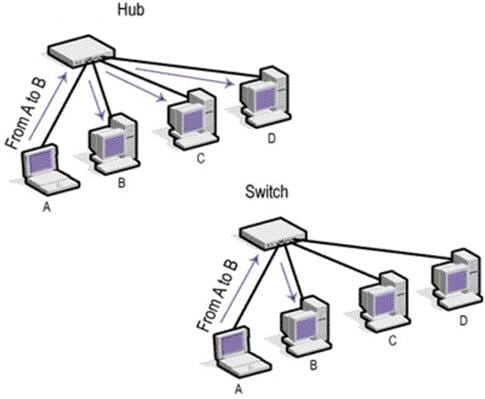
**Q #37) What is the full form of ASCII?**

**Answer:**ASCII stands for American Standard Code for Information Interchange.

**Q #38) How a Switch is different from a Hub?**

**Answer:** Below are the differences between a Switch and a Hub,

**Below given snapshot clearly explains the difference:**

[](https://cdn.softwaretestinghelp.com/wp-content/qa/uploads/2017/03/switch-vs-hub.jpg)

**Q #39) Define Round Trip Time?**

**Answer:** The time taken for a signal to reach the destination and travel back to the sender with the acknowledgment is termed as Round Trip Time (RTT). It is also called Round Trip Delay (RTD).

**Q #40) Define Brouter?**

**Answer:**Brouter or Bridge Router is a device that acts as both a bridge and a router. As a bridge, it forwards data between the networks. And as a router, it routes the data to specified systems within a network.

**Q #41) Define Static IP and Dynamic IP?**

**Answer:** When a device or computer is assigned a specified IP address then it is named as Static IP. It is assigned by the Internet Service Provider as a permanent address.

Dynamic IP is the temporary IP address assigned by the network to a computing device. Dynamic IP is automatically assigned by the server to the network device.

**Q #42) How VPN is used in the corporate world?**

**Answer:**VPN stands for Virtual Private Network. With the help of a VPN, remote users can securely connect to the organization’s network. Corporate companies, educational institutions, government offices, etc use this VPN.

**Q #43) What is the difference between Firewall and Antivirus?**

**Answer:** Firewall and Antivirus are two different security applications used in networking. A firewall acts as a gatekeeper which prevents unauthorized users to access the private networks as intranets. A firewall examines each message and blocks the same which are unsecured.

Antivirus is a software program that protects a computer from any malicious software, any virus, spyware, adware, etc.

**Note:**A Firewall cannot protect the system from viruses, spyware, adware, etc.

**Q #44) Explain Beaconing?**

**Answer:** If a network self-repair its problem then it is termed as Beaconing. Mainly, it is used in the token ring and FDDI (Fiber Distributed Data Interface) networks. If a device in the network is facing any problem, then it notifies the other devices that they are not receiving any signal. Likewise, the problem gets repaired within the network.

**Q #45) Why the standard of an OSI model is termed as 802.xx?**

**Answer:** The OSI model was started in the month of February in 1980. So it is standardized as 802.XX. This ‘80’ stands for the year 1980 and ‘2’ represents the month of February.

**Q #46) Expand DHCP and describe how it works?**

**Answer:**DHCP stands for Dynamic Host Configuration Protocol.

DHCP is used to assign IP addresses automatically to the devices over the network. When a new device is added to the network, it broadcasts a message stating that it is new to the network. Then the message is transmitted to all the devices of the network.

Only the DHCP server will react to the message and assigns a new IP address to the newly added device of the network. With the help of DHCP, IP management became very easy.

**Q #47) How can a network be certified as an effective network? What are the factors affecting them?**

**Answer:** **A network can be certified as an effective network based on below-mentioned factors:**

* **Performance:**A network’s performance is based on its transmitted time and response time. The factors affecting the performance of a network are hardware, software, transmission medium types and the number of users using the network.
* **Reliability:**Reliability is nothing but measuring the probability of failures occurred in a network and the time taken by it to recover from it. The factors affecting the same are the frequency of failure and recovery time from failure.
* **Security:**Protecting the data from viruses and unauthorized users. The factors affecting the security are viruses and users who do not have permission to access the network.

**Q #48) Explain DNS?**

**Answer:**DNS stands for Domain Naming Server. DNS acts as a translator between domain names and IP addresses. As humans remember names, the computer understands only numbers. Generally, we assign names to websites and computers like Gmail.com, Hotmail, etc. When we type such names the DNS translates it into numbers and executes our requests.

Translating the names into numbers or IP address is named as a Forward lookup.

Translating the IP address to names is named as a Reverse lookup.

**Q #49) Define IEEE in the networking world?**

**Answer:**IEEE stands for the Institute of Electrical and Electronic Engineer. This is used to design or develop standards that are used for networking.

**Q #50) What is the use of encryption and decryption?**

**Answer:**Encryption is the process of converting the transmission data into another form that is not read by any other device other than the intended receiver.

Decryption is the process of converting back the encrypted data to its normal form. An algorithm called cipher is used in this conversion process.

**Q #51) Brief Ethernet?**

**Answer:**Ethernet is a technology that is used to connect computers all over the network to transmit the data between each other.

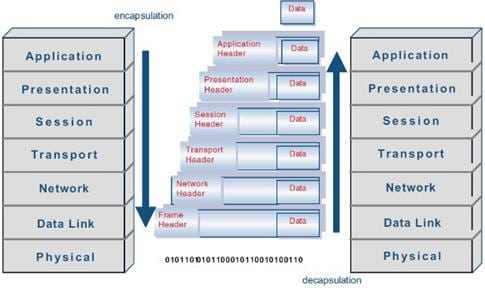
**For Example,** if we connect a computer and laptop to a printer, then we can call it as an Ethernet network. Ethernet acts as the carrier for the Internet within short distance networks like a network in a building.

The main difference between the Internet and Ethernet is security. Ethernet is safer than the Internet as Ethernet is a closed-loop and has only limited access.

**Q #52) Explain Data Encapsulation?**

**Answer:** Encapsulation means adding one thing on top of the other thing. When a message or a packet is passed through the communication network (OSI layers), every layer adds its header information to the actual packet. This process is termed as Data Encapsulation.

**Note:** Decapsulation is exactly the opposite of encapsulation. The process of removing the headers added by the OSI layers from the actual packet is termed as Decapsulation.

[](https://cdn.softwaretestinghelp.com/wp-content/qa/uploads/2017/03/encapsulationdecapsulation.jpg)

**Q #53) How are networks classified based on their connections?**

**Answer:** Networks are classified into two categories based on their connection types. **They are mentioned below:**

* **Peer-to-peer networks (P2P):**When two or more computers are connected together to share resources without the use of a central server is termed as a peer-to-peer network. Computers in this type of network act as both server and client. It is generally used in small companies as they are not expensive.
* **Server-based networks:**In this type of network, a central server is located to store the data, applications, etc of the clients. The server computer provides the security and network administration to the network.

**Q #54) Define Pipelining?**

**Answer:** In Networking, when a task is in progress another task gets started before the previous task is finished. This is termed as Pipelining.

**Q #55) What is an Encoder?**

**Answer:** Encoder is a circuit that uses an algorithm to convert any data or compress audio data or video data for transmission purposes. An encoder converts the analog signal into the digital signal.

**Q #56) What is a Decoder?**

**Answer:** Decoder is a circuit that converts the encoded data to its actual format. It converts the digital signal into an analog signal.

**Q #57) How can you recover the data from a system which is infected with a Virus?**

**Answer:** In another system (not infected with a virus) install an OS and antivirus with the latest updates. Then connect the HDD of the infected system as a secondary drive. Now scan the secondary HDD and clean it. Then copy the data into the system.

**Q #58) Describe the key elements of the protocol?**

**Answer:** **Below are the 3 key elements of the protocol:**

* **Syntax:**It is the format of the data. That means in which order the data is displayed.
* **Semantics:**Describes the meaning of the bits in each section.
* **Timing:**At what time the data is to be sent and how fast it is to be sent.

**Q #59) Explain the difference between baseband and broadband transmission?**

**Answer:**

* **Baseband Transmission:** A single signal consumes the whole bandwidth of the cable.
* **Broadband Transmission:** Multiple signals of multiple frequencies are sent simultaneously.

**Q #60) Expand SLIP?**

**Answer:**SLIP stands for Serial Line Interface Protocol. SLIP is a protocol used for transmitting IP datagrams over a serial line.

**1) 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.

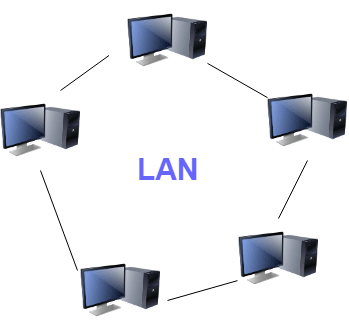
**2) What are the layers of the OSI reference model?**

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.

**3) What is the backbone network?**

A backbone network is a centralized infrastructure that is designed to distribute different routes and data to various networks. It also handles the management of bandwidth and multiple channels.

**4) What is a LAN?**

[](https://www.guru99.com/images/2/041720_1134_Top135Netwo1.png)LAN network

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.

**5) 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.

**6) 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.

**7) What is a point to point link?**

It refers to a direct connection between two computers on a network. A point to point connection does not need any other network devices other than connecting a cable to the NIC cards of both computers.

**8) What is anonymous FTP?**

Anonymous FTP is a way of granting user access to files in public servers. Users that are allowed access to data in these servers do not need to identify themselves, but instead, log in as an anonymous guest.

**9) 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.

**10) 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.

**11) 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.

**12) Describe Network Topology**

[Network Topology](https://www.guru99.com/type-of-network-topology.html) refers to the layout of a computer network. It shows how devices and cables are physically laid out, as well as how they connect.

**13) 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.

**14) 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.

**15) 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.

**16) How does a network topology affect your decision to set a network?**

Network topology dictates what media you must use to interconnect devices. It also serves as a basis on what materials, connectors, and terminations that is applicable for the setup.

**17) 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.

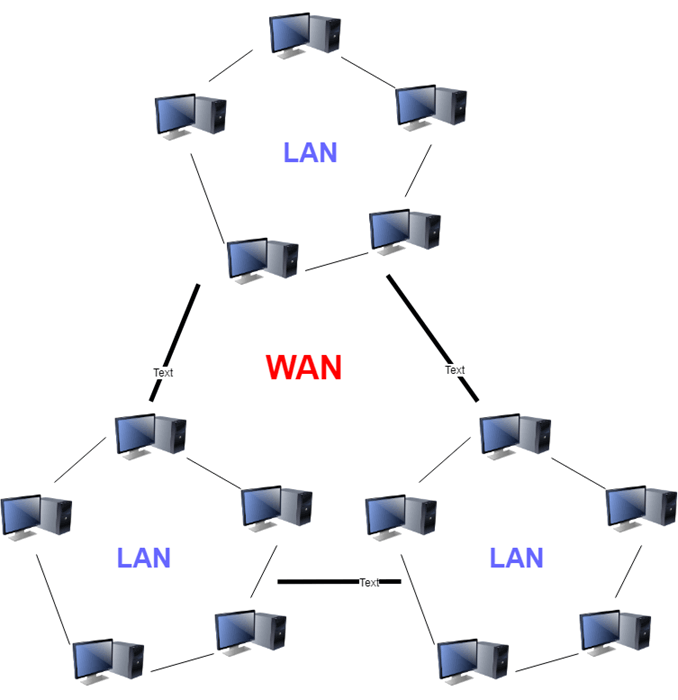
**18) What are the different ways of securing a computer network?**

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.

**19) 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.

**20) What is WAN?**

[](https://www.guru99.com/images/2/041720_1134_Top135Netwo4.png)WAN network

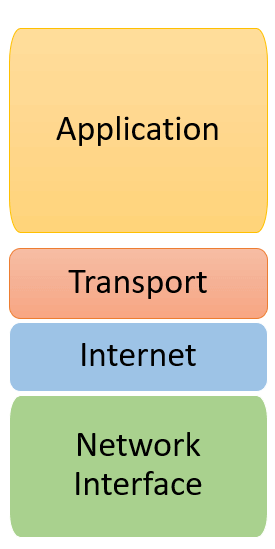
WAN stands for Wide Area Network. It is an interconnection of computers and devices that are geographically dispersed. It connects networks that are located in different regions and countries.

**21) 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.

**22) 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.

[](https://www.guru99.com/images/2/041720_1134_Top135Netwo5.png)TCP/IP Layers

**23) 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.

**24) 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.

**25) What is the importance of implementing a Fault Tolerance System?**

A fault tolerance system ensures continuous data availability. This is done by eliminating a single point of failure.

**26) What does 10Base-T mean?**

The 10 refers to the data transfer rate. In this case, it is 10Mbps. The word Base refers to baseband, as opposed to broadband.

**27) 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.

**28) What is NOS?**

NOS, or Network Operating System, is specialized software. The main task of this software is to provide network connectivity to a computer in order to communicate with other computers and connected devices.

**29) What is DoS?**

DoS, or Denial-of-Service attack, is an attempt to prevent users from being able to access the Internet or any other network services. Such attacks may come in different forms and are done by a group of perpetrators. One common method of doing this is to overload the system server so it cannot anymore process legitimate traffic and will be forced to reset.

**30) 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.

**31) 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.

**32) 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.

**33) 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.

**34) 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.

**35) 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.

**36) 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.

**37) 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.

**38) Describe star topology**

Star topology consists of a central hub that connects to nodes. This is one of the easiest to set up and maintain.

Advantages:

Here are pros/benefits of start topology:

* Easy to troubleshoot, set up, and modify.
* Only those nodes are affected, that has failed. Other nodes still work.
* Fast performance with few nodes and very low network traffic.
* In Star topology, addition, deletion, and moving of the devices are easy.

Disadvantages:

Here are cons/drawbacks of using Star:

* If the Hub or concentrator fails, attached nodes are disabled.
* The cost of installation of star topology is costly.
* Heavy network traffic can sometimes slow the bus considerably.
* Performance depends on the Hub's capacity
* A damaged cable or lack of proper termination may bring the network down.

**39) What are gateways?**

Gateways provide connectivity between two or more network segments. It is usually a computer that runs the gateway software and provides translation services. This translation is key in allowing different systems to communicate on the network.

**40) What is the disadvantage of a star topology?**

One major disadvantage of star topology is that once the central Hub or switch gets damaged, the entire network becomes unusable.

**41) What is SLIP?**

SLIP, or Serial Line Interface Protocol, is an old protocol developed during the early UNIX days. This is one of the protocols that are used for remote access.

**42) Give some examples of private network addresses.**

10.0.0.0 with a subnet mask of 255.0.0.0172.16.0.0 with subnet mask of 255.240.0.0192.168.0.0 with subnet mask of 255.255.0.0

**43) 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.

**44) 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.

**45) What is the main disadvantage of a peer to peer network?**

Accessing the resources that are shared by one of the workstations on the network takes a performance hit.

**46) What is a Hybrid Network?**

A hybrid network is a network setup that makes use of both client-server and peer-to-peer architecture.

**47) 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.

**48) 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.

**49) 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.

**50) How can you manage a network using a router?**

Routers have a built-in console that lets you configure different settings, like security and data logging. You can assign restrictions to computers, such as what resources it is allowed access or what particular time of the day, they can browse the Internet. You can even put restrictions on what websites are not viewable across the entire network.

**51) What protocol can be applied when you want to transfer files between different platforms, such as UNIX systems and Windows servers?**

Use FTP (File Transfer Protocol) for file transfers between such different servers. This is possible because FTP is platform-independent.

**52) 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.

**53) What can be considered as good passwords?**

Good passwords are made up of not just letters, but by combining letters and numbers. A password that combines uppercase and lowercase letters is favorable than one that uses all upper case or all lower-case letters. Passwords must be not words that can easily be guessed by hackers, such as dates, names, favorites, etc. Longer passwords are also better than short ones.

**54) What is the proper termination rate for UTP cables?**

The proper termination for unshielded twisted pair network cable is 100 ohms.

**55) What is netstat?**

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

**56) 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.

**57) What happens when you use cables longer than the prescribed length?**

Cables that are too long would result in signal loss. It means that data transmission and reception would be affected because the signal degrades over length.

**58) What common software problems can lead to network defects?**

Software related problems can be any or a combination of the following:

* Client-server problems
* Application conflicts
* Error in configuration
* Protocol mismatch
* Security issues
* User policy and rights issues

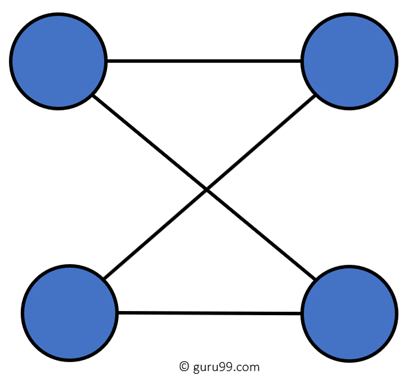
**59) What is ICMP?**

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.

**60) 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.

**61) What is peer to peer?**

[](https://www.guru99.com/images/2/041720_1134_Top135Netwo7.png)

Peer to peer (P2P) are networks that do not rely on a server. All PCs on this network act as individual workstations.

**62) 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.

**63) 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.

**64) 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 |

**65) What are the different network protocols that are supported by Windows RRAS services?**

There are three main network protocols supported: NetBEUI, TCP/IP, and IPX.

**66) What are the maximum networks and hosts in class A, B, and C network?**

For Class A, there are 126 possible networks and 16,777,214 hosts. For Class B, there are 16,384 possible networks and 65,534 hosts. For Class C, there are 2,097,152 possible networks and 254 hosts

**67) What is the standard color sequence of a straight-through cable?**

Orange/white, orange, green/white, blue, blue/white, green, brown/white, brown.

**68) What protocols fall under the Application layer of the TCP/IP stack?**

The following are the protocols under the TCP/IP Application layer: FTP, TFTP, Telnet, and SMTP.

**69) You need to connect two computers for file sharing. Is it possible to do this without using a hub or a router?**

Yes, you can connect two computers, using only one cable. A crossover type cable can be used in this scenario. In this setup, the data transmit pin of one cable is connected to the data receive pin of the other cable, and vice versa.

**70) 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.

**71) What is the difference between a straight-through and crossover cable?**

A straight-through cable is used to connect computers to a switch, hub, or router. A crossover cable is used to connect two similar devices, such as a PC to PC or Hub, to the Hub.

**72) What is the client/server?**

Client/server is a type of network wherein one or more computers act as servers. Servers provide a centralized repository of resources such as printers and files. Clients refer to a workstation that accesses the server.

**73) Describe networking.**

Networking refers to the interconnection between computers and peripherals for data communication. Networking can be done using wired cabling or through a wireless link.

**74) When you move the NIC cards from one PC to another PC, does the MAC address gets transferred as well?**

Yes, that's because MAC addresses are hard-wired into the NIC circuitry, not the PC. This also means that a PC can have a different MAC address when another one replaced the NIC card.

**75) Explain clustering support**

Clustering support refers to the ability of a network operating system to connect multiple servers in a fault-tolerant group. The main purpose of this is the if one server fails, all processing will continue with the next server in the cluster.

**76) Where is the best place to install an Anti-virus program?**

An anti-virus program must be installed on all servers and workstations to ensure protection. That's because individual users can access any workstation and introduce a computer virus. You can plug in their removable hard drives or flash drives.

**77) Describe Ethernet**.

Ethernet is one of the popular networking technologies used these days. It was developed during the early 1970s and is based on specifications, as stated in the IEEE. Ethernet is used in local area networks.

**78) What are some drawbacks of implementing a ring topology?**

In case one workstation on the network suffers a malfunction, it can bring down the entire network. Another drawback is that when there are adjustments and reconfigurations needed to be performed on a particular network, the entire network must be temporarily brought down.

**79) 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.

**80) What is SMTP?**

SMTP is short for Simple Mail Transfer Protocol. This protocol deals with all internal mail and provides the necessary mail delivery services on the TCP/IP protocol stack.

**81) What is multicast routing?**

Multicast routing is a targeted form of broadcasting that sends a message to a selected group of the user instead of sending it to all users on a subnet.

**82) What is the importance of Encryption on a network?**

Encryption is the process of translating information into a code that is unreadable by the user. It is then translated back or decrypted back to its normal readable format using a secret key or password. Encryption ensures that information that is intercepted halfway would remain unreadable because the user must have the correct password or key for it.

**83) How are IP addresses arranged and displayed?**

IP addresses are displayed as a series of four decimal numbers that are separated by period or dots. Another term for this arrangement is the dotted-decimal format. An example is 192.168.101.2

**84) Explain the importance of authentication.**

Authentication is the process of verifying a user's credentials before he can log into the network. It is normally performed using a username and password. This provides a secure means of limiting access from unwanted intruders on the network.

**85) What is meaning by tunnel mode?**

This is a mode of data exchange wherein two communicating computers do not use IPsec themselves. Instead, the gateway that is connecting their LANs to the transit network creates a virtual tunnel. So, it uses the IPsec protocol to secure all communication that passes through it.

**86) What are the different technologies involved in establishing WAN links?**

* Analog connections - using conventional telephone lines
* Digital connections - using digital-grade telephone lines
* Switched connections - using multiple sets of links between the sender and receiver to move data.

**87) Explain Mesh Topology**

The mesh topology has a unique network design in which each computer on the network connects to every other. It is developing a P2P (point-to-point) connection between all the devices of the network. It offers a high level of redundancy, so even if one network cable fails, data still has an alternative path to reach its destination.

**Types of Mesh Topology:**

**Partial Mesh Topology:**In this type of topology, most of the devices are connected almost similarly as full topology. The only difference is that few devices are connected with just two or three devices.

**Full Mesh Topology:**In this topology, every node or device are directly connected with each other.

**88) When troubleshooting computer network problems, what common hardware-related problems can occur?**

A large percentage of a network is made up of hardware. Problems in these areas can range from malfunctioning hard drives, broken NICs, and even hardware startups. Incorrect hardware configuration is also one of those culprits to look into.

**89) How can you fix signal attenuation problems?**

A common way of dealing with such a problem is to use repeaters and hubs because it will help regenerate the signal and therefore prevent signal loss. Checking if cables are properly terminated is also a must.

**90) How does dynamic host configuration protocol aid in network administration?**

Instead of having to visit each client computer to configure a static IP address, the network administrator can apply dynamic host configuration protocol to create a pool of IP addresses known as scopes that can be dynamically assigned to clients.

**91) Explain profile in terms of networking concepts**

Profiles are the configuration settings made for each user. A profile may be created that puts a user in a group, for example.

**92) What is sneakernet?**

Sneakernet is believed to be the earliest form of networking wherein data is physically transported using removable media, such as disk, tapes.

**93) What is the role of the IEEE in computer networking?**

IEEE, or the Institute of Electrical and Electronics Engineers, is an organization composed of engineers that issues and manages standards for electrical and electronic devices. This includes networking devices, network interfaces, cablings, and connectors.

**94) What protocols fall under the TCP/IP Internet Layer?**

There are 4 protocols that are being managed by this layer. These are ICMP, IGMP, IP, and ARP.

**95) When it comes to networking, what are rights?**

Rights refer to the authorized permission to perform specific actions on the network. Each user on the network can be assigned individual rights, depending on what must be allowed for that user.

**96) What is one basic requirement for establishing VLANs?**

A VLAN is required because at the switch level. There is only one broadcast domain. It means whenever a new user is connected to switch. This information is spread throughout the network. VLAN on switch helps to create a separate broadcast domain at the switch level. It is used for security purposes.

**97) 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.

**98) What is the RSA algorithm?**

RSA is short for the Rivest-Shamir-Adleman algorithm. It is the most commonly used public-key encryption algorithm in use today.

**99) 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.

**100) what is the maximum segment length of a 100Base-FX network?**

The maximum allowable length for a network segment using 100Base-FX is 412 meters. The maximum length for the entire network is 5 kilometers.

**101) What is the 5-4-3 rule, and in which architecture is it used?**

The 5-4-3 rule is used in 10Base2 and 10Base5 Ethernet architectures. In this rule, there can be a maximum of five segments in a network connected with four repeaters. Out of these five segments, only three segments can be populated with nodes.

**102) What is the difference between TCP and UDP?**

|  |  |
| --- | --- |
| **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. |

**103) What are the important elements of the protocol?**

Here, are three most important elements of the protocol:

* **Syntax:** It is the format of the data. It is an order the data is displayed.
* **Semantics:** It describes the meaning of the bits in each section.
* **Timing:** What time the data is to be sent and how fast it is to be sent.

**104) What is the maximum segment length of a 100Base-FX network?**

The maximum length for a network segment using 100Base-FX is 412 meters.

**105) What is a Decoder?**

The decoder is a type of circuit that converts the encoded data to its original format. It also converts the digital signal into an analog signal.

**106) What is Brouter?**

Brouter is also known as Bridge Router. It is a device that acts as both a bridge and a router. As a bridge can forwards data between the networks. It also routes the data to specified systems within a network.

**107) How to use VPN?**

By using a Virtual Private Network (VPN), users can connect to the organization's network. Corporate companies, educational institutions, government offices.

**108) Why the standard OSI model is known as 802.xx?**

The OSI model was started in February 1980. In 802.XX, '80' stands for the year 1980, and '2' represents the month of February.

**109) What is NVT (Network Virtual Terminal)?**

NVT is a set of pre-defined rules to very simple virtual terminal interaction. This terminal helps you to start a Telnet session.

**110) What is the source route?**

The source route is a sequence of IP addresses that helps you to identify the route a datagram. You can include the source route in the IP datagram header.

**111) Explain the term Pipelining**

Pipelining describes the sequencing of processes. When any new task begins before an ongoing task is finished, it is called sequencing.

**112) Which measurement unit is used to measure the transmission speed of Ethernet?**

The transmission speed of Ethernet is mostly measured in Mbps.

**113)** **What is the maximum length of Thinnet cable?**

The length of the Thinnet cable is 185 meters.

**114) Which cable is also called as the RG8 cable?**

Thicknet cable is also called as the RG8 cable.

**115)** **Is coaxial cable still used in the computer network?**

No, Nowadays, coaxial cable no longer used in a computer network.

**116)** **Which cable uses the RJ11 connector?**

Most of the telephone cable uses the RJ11 connector.

**117) Explain Multi-homed Host**

It is a host that has multiple network interfaces that multiple IP addresses is called a Multi-homed Host.

**118) Explain EGP**

The full form of EGP is Exterior Gateway Protocol. It is the protocol of the routers. It is the neighboring autonomous systems that help you to identify the set of networks that you will able to reach within or via each independent system.

**119)** **Explain the term Passive Topology**

When a computer in the network listen and receive the signal, they are called passive topology.

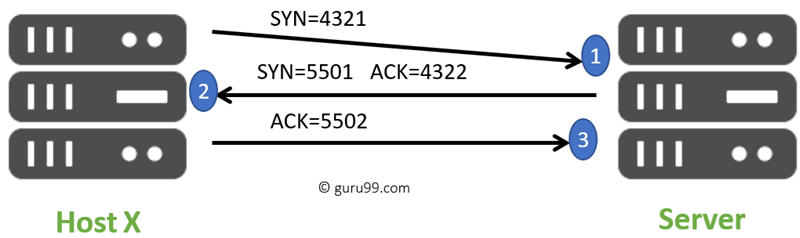
**120)** **What is the use of a Pseudo TTY?**

It is a false terminal which allows you external machines to connect through Telnet or log in. Without this, no connection can take place.

**121)** **Explain Redirector**

Redirector is a kind of software which intercepts file or prints I/O requests and translates them into network requests. This component comes under the presentation layer.

**122) What Is TCP Three-Way Handshake?**

[](https://www.guru99.com/images/2/041720_1134_Top135Netwo10.png)TCP Three-Way Handshake

THREE-WAY handshake or a TCP 3-way handshake is a process that is used in a TCP/IP network to make a connection between the server and client. It is a three-step process that requires both the client and server to exchange synchronization and acknowledgment packets before the real data communication process starts.

**123) What is a Hamming code?**

[Hamming code](https://www.guru99.com/hamming-code-error-correction-example.html) is a liner code that is useful for error detection up to two immediate bit errors. It is capable of single-bit errors.

In Hamming code, the source encodes the message by adding redundant bits in the message. These redundant bits are mostly inserted and generated at certain positions in the message to accomplish the error detection and correction process.

**124) What is the Application of Hamming code?**

Here are some common applications of using Hemming code:

* Satellites
* Computer Memory
* Modems
* PlasmaCAM
* Open connectors
* Shielding wire
* Embedded Processor

**125)** **What are the benefits of the Hamming code?**

Here, are important benefits of Hamming code

* The Hamming code method is effective on networks where the data streams are given for the single-bit errors.
* Hamming code not only provides the detection of a bit error but also helps you to indent bit containing error so that it can be corrected.
* The ease of use of hamming codes makes it suitable for use in computer memory and single-error correction.

**126)** **What is a MAC Address?**

MAC address is a unique identifier that is assigned to a NIC (Network Interface Controller/ Card). It consists of a 48 bit or 64-bit address, which is associated with the network adapter. MAC address can be in hexadecimal format. The full form of MAC address is Media Access Control address.

**127)** **Why Use MAC Address?**

Here are the important reasons for using MAC address:

* It provides a secure way to find senders or receivers in the network.
* MAC address helps you to prevent unwanted network access.
* MAC address is a unique number. Hence it can be used to track the device.
* Wi-Fi networks at the airport use the MAC address of a specific device in order to identify it.

**128) What are the types of MAC Addresses?**

Here are the important types of MAC addresses:

* Universally Administered Address

UAA(Universally Administered Address) is the most used type of MAC address. It is given to the network adapter at the time of manufacturing.

* Locally Administered Address

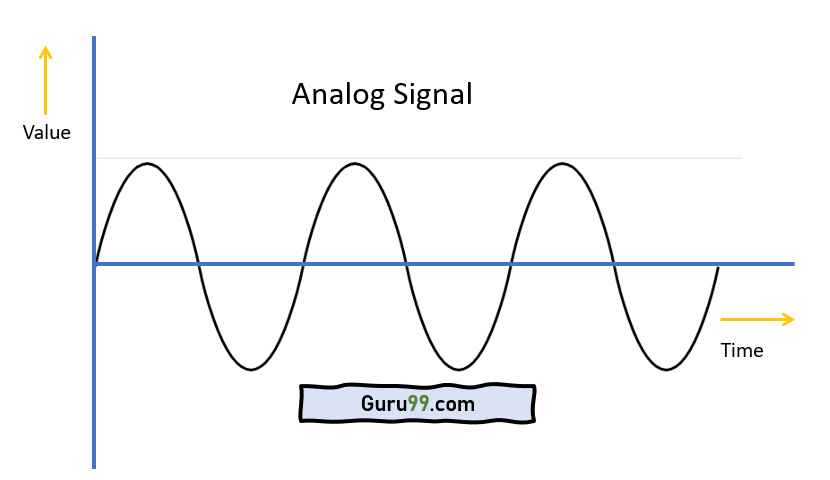
LAA (Locally Administered Address) is an address that changes the MAC address of the adapter. You may assign this address to a device used by network administrator.

**129) What are the important differences between MAC address and IP address**

Here, are some difference between [MAC and IP](https://www.guru99.com/difference-between-mac-address-and-ip-address.html) address:

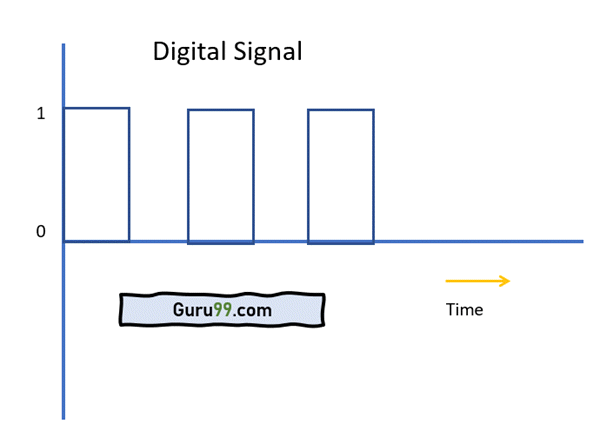
|  |  |
| --- | --- |
| **MAC** | **IP address** |
| The MAC address stands for Media Access Control Address. | IP address stands for Internet Protocol Address. |
| It consists of a 48-bit address. | It consists of a 32-bit address. |
| MAC address works at the link layer of the OSI model. | IP address 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. |

**130) What is an Analog Signal?**

[](https://www.guru99.com/images/2/030720_0729_AnalogvsDig1.png)Analog Signal

Analog signal is a continuous signal in which one time-varying quantity represents another time-based variable. These kind of signals works with physical values and natural phenomena such as earthquake, frequency, volcano, speed of wind, weight, lighting, etc.

**131) What is a Digital Signal?**

[](https://www.guru99.com/images/2/041720_1134_Top135Netwo12.png)Digital Signal

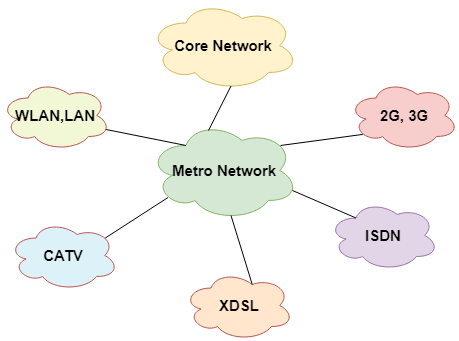
A digital signal is a signal that is used to represent data as a sequence of separate values at any point in time. It can only take on one of a fixed number of values. This type of signal represents a real number within a constant range of values.

**132) What are the differences between analog and digital signal?**

Here are the main differences between [Analog and Digital](https://www.guru99.com/analog-vs-digital.html) Signal:

|  |  |
| --- | --- |
| **Analog** | **Digital** |
| An analog signal is a continuous signal that represents physical measurements. | Digital signals are time separated signals which are generated using digital modulation. |
| It is denoted by sine waves | It is denoted by square waves. |
| It uses a continuous range of values that help you to represent information. | The Digital signal uses discrete 0 and 1 to represent information. |
| The analog signal bandwidth is low | The digital signal bandwidth is high. |
| Analog hardware never offers flexible implementation. | Digital hardware offers flexibility in implementation. |
| It is suited for audio and video transmission. | It is suited for Computing and digital electronics. |
| The Analog signal doesn't offer any fixed range. | Digital signal has a finite number, i.e., 0 and 1. |

**133)** **What is MAN?**

[](https://www.guru99.com/images/2/041720_1134_Top135Netwo13.png)MAN network

A Metropolitan Area Network or MAN is consisting of a [computer network](https://www.guru99.com/types-of-computer-network.html) across an entire city, college campus, or a small region. This type of network is large than a LAN, which is mostly limited to a single building or site. Depending upon the type of configuration, this type of network allows you to cover an area from several miles to tens of miles.

**134) What is Modem?**

A modem (modulator-demodulator) is a device that modulates an analog signal to digital information. It also decodes carrier signals to demodulates the transmitted information.

The main aim of the Modem is to produce a signal that can be transmitted easily and decoded to reproduce the digital data in its original form. Modems are also used for transmitting analog signals, from Light Emitting Diodes (LED) to radio.

**135) What are the advantages of a Modem?**

Here, are pros/advantage of Modem:

* More useful in connecting LAN with the Internet
* Speed depends on the cost
* The Modem is the most widely used data communication roadway.