CCA-102: DATA COMMUNICATIONS

ASSIGNMENT

1. What are the different types of networks?

WAN(Wide Area Network)

A Wide Area Network is the largest spread network. It spans over very large-distances such as a country, continent or even the whole globe. Two widely separated computers can be connected very easily using WAN. For Example, the Internet.

A WAN may include various Local and Metropolitan Area Network. The mode of communication in a WAN can either be wired or wireless. Telephone lines for wired and satellite links for wireless communication can be used in a wide area network.

In other words, WAN provides long distance transmission of data, voice, image, and video, over a large geographical area. A WAN may span beyond 100km range. It may be privately or publicly owned.

The protocols used in WAN are ISDN(Integrated Service Digital Network), SMDS(Switched Multi-Megabit Data Service), SONET(Synchronous Optical Network), HDLC(High Data Link Control), SDLC(Synchronous Data Link Control), etc.

The advantage of WAN is that it spans over a very large geographical area, and connects a huge mass of people.

Following are the disadvantages of WAN:

1. The propagation delay is more in a WAN
2. The data rate is low
3. The error rate is high

4. It is very complex to design a WAN

These are the types of network according to geographical area.

Following are the types of network, based on functionality:

- **Client-Server Network:** Client-Server network is a network in which a client runs the program and access data that are stored on the server. In this kind of network, one computer becomes the server, serving all other computers called clients.
- **Peer-to-Peer Network:** Peer-to-Peer network facilitates the flow of information from one peer to another without any central server. In other words, each node on a server acts as both client and server.

Following are the types of network, based on Ownership:

- **Private Network:** A private network is a network in which various restrictions are imposed to secure the network, to restrict unauthorized access. This type of network is privately owned by a single or group of people for their personal use. Local Area Network(LAN) can be used as a private network.
- **Public Network:** A public network is a network that has the least or no restrictions on it. It can be freely accessed by anyone, without any restrictions. This type of network is publicly owned by the government or NGOs. Metropolitan Area Network(MAN) and Wide Area Network(WAN) can be used as a public network.

Following are the types of network, based on Transmission Media:

- **Bound/Guided Media Network:** Bounded/Guided media can also be referred to as wired media. This kind of networks provides a physical link between two nodes connected in a network. The physical links are directed towards a particular direction in the network. Co-axial, twisted pair, optical fiber cable, etc. can be used in such networks for connectivity.

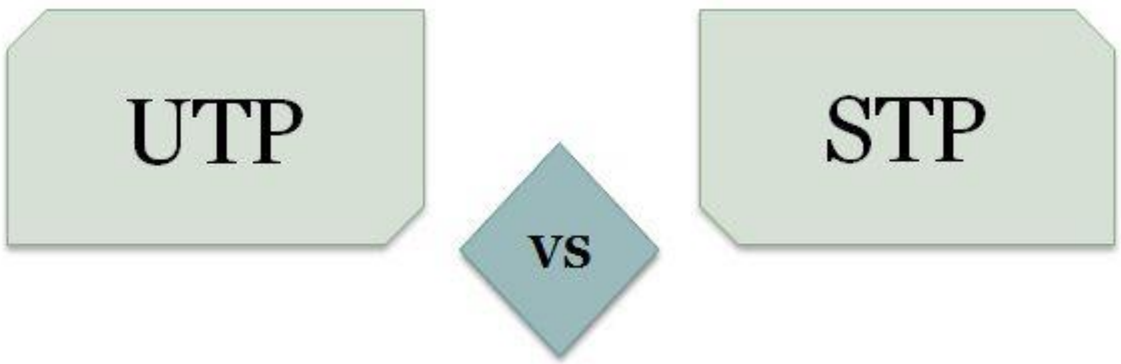
Local Area Network(LAN) and Metropolitan Area Network(MAN) can be used as a Bound/Guided media network.

- **Unbound/Unguided Media Network:** Unbounded/Unguided media can also be referred to as wireless media. This kind of network does not need any physical link for electromagnetic transmission. Radio waves, Microwaves, Infrared, etc. can be used in such networks for connectivity. Metropolitan Area Network(MAN) and Wide Area Network(WAN) can be used as an Unbound/Unguided media network.

This is all about the various types of computer networks.

Q.2 Explain the Shielded twisted pair (STP) and Unshielded twisted pair(UTP)

Ans.2 Difference Between UTP and STP Cables



UTP (Unshielded twisted pair) and STP (Shielded twisted pair) are the types of twisted pair cables which act as a transmission medium and imparts reliable connectivity of electronic equipment. Although the design and manufacture are different but both serve the same purpose.

The basic difference between UTP and STP is **UTP (Unshielded twisted pair)** is a cable with wires that are twisted together to reduce noise and crosstalk. On the contrary, **STP (Shielded twisted pair)** is a twisted pair cable confined in foil or mesh shield that guards the cable against electromagnetic interference.

Content: UTP Cable Vs STP Cable

Comparison Chart

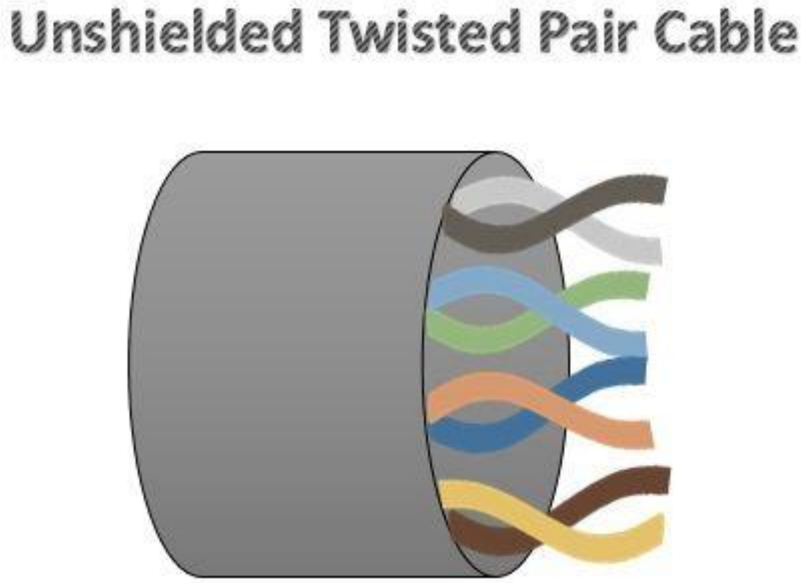
BASIS FOR COMPARISON	**UTP**	**STP**
Basic	UTP (Unshielded twisted pair) is a cable with wires that are twisted	STP (Shielded twisted pair) is a twisted pair cable enclosed in foil or mesh

BASIS FOR COMPARISON	UTP	STP
	together.	shield.
Noise and crosstalk generation	High comparatively.	Less susceptible to noise and crosstalk.
Grounding cable	Not required	Necessarily required
Ease of handling	Easily installed as cables are smaller, lighter, and flexible.	Installation of cables is difficult comparatively.
Cost	Cheaper and does not require much maintenance.	Moderately expensive.
Data Rates	Slow comparatively.	Provides high data rates

Definition of UTP Cable

Unshielded twisted-pair (UTP) cable is the most prevalent type of telecommunication medium in use today. Its frequency range is suitable for transmitting both data and voice. Therefore, these are most commonly used in telephone systems.

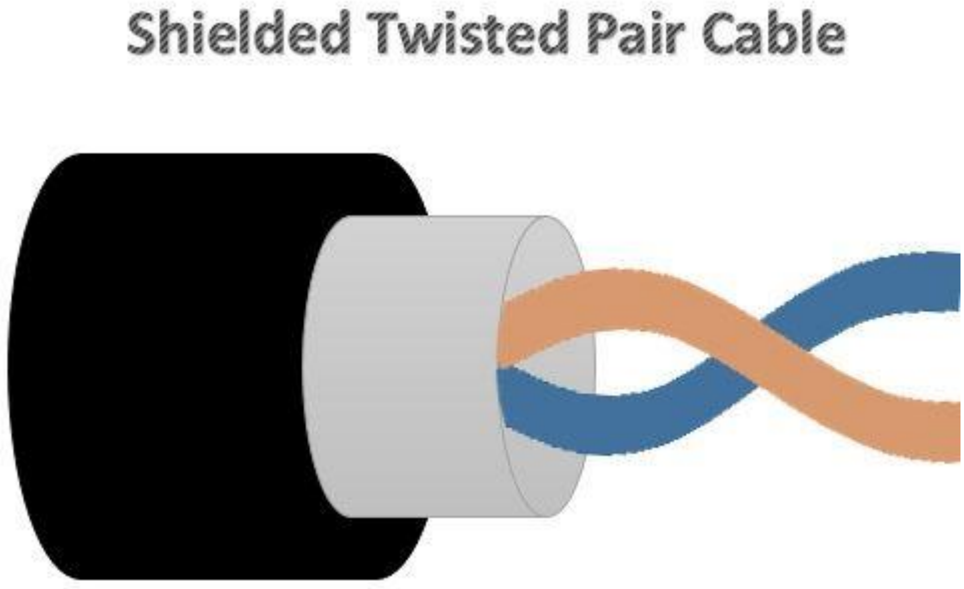
A twisted pair consists of two insulated conductors (usually copper) in a twisted configuration. Color bands are used in plastic insulation for identification. In addition, colors also identify the specific conductors in a cable and to indicate which wires belong in pairs and how they relate to other pairs in a larger bundle.



The two wires are twisted in the twisted pair cable which significantly reduces the noise generated by the external source. The **noise** here we are talking about is generated when two wires are parallel which causes an increase in voltage level in the wire closest to the source and also uneven load and damaged signal.

Definition of STP Cable

Shielded twisted-pair (STP) cable has an additional braided mesh coating or metal foil that wraps each set of insulated conductors. The metal casing intercepts the penetration of **electromagnetic noise**. It also can eradicate a phenomenon called crosstalk, which is the unwanted effect of one circuit (or channel) on another circuit (or channel).



It occurs when one line (acting as a kind of receiving antenna) picks up some of the signals travelling down another line (acting as a kind of sending antenna). This effect can be experienced during telephone conversations when one can hear other conversations in the background. Shielding each pair of a twisted-pair cable can eliminate most crosstalk.

STP has the similar quality factor and uses the same connectors as UTP, but the shield must be connected to the **ground**.

Key Differences Between UTP and STP Cables

1. UTP and STP are the types of twisted pair cable where UTP is the unshielded type whereas STP is shielded, for doing so metal foil or braided mesh is used.
2. UTP reduces the crosstalk and noise as compared to the parallel arrangement of the wires but not at great extent. On the contrary, STP decreases the crosstalk, noise, and electromagnetic interference significantly.
3. UTP cables are easily installed while installation of STP cables is difficult are the cables are bigger, heavier and stiffer.
4. Grounding is not required in UTP cables. As against, STP cables requires grounding.
5. UTP cables are inexpensive whereas STP cables are costly comparatively due to additional material and manufacturing.
6. STP cables incorporate a conducting shield built of metallic foil enclosing the twisted wire pairs, which obstructs out electromagnetic interference, permitting it to carry data at an enhanced rate of speed. In contrast, UTP provides less speed of data transfer.

Conclusion

UTP and STP cables differ in the design and structure where STP cable has an additional metal foil wrapped in insulated conductors.

However, both STP and UTP cables have their respective merits and demerits, when it comes to proper installation and maintenance in a suitable situation for their use, both work finely.

Related Differences:

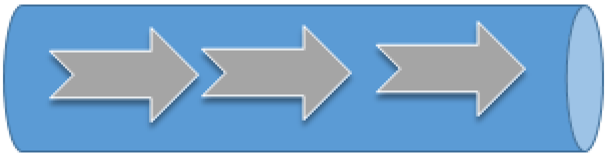
1. **Difference Between Optical Fibre and Coaxial Cable**
2. **Difference Between Guided and Unguided Media**

Q.3 What is difference between baseband and broadband transmission?

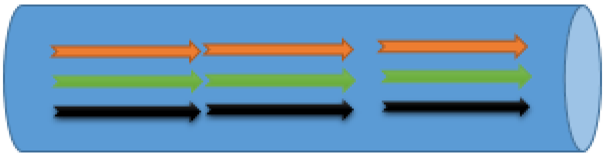
Ans.3

Both baseband and broadband describe how data is transmitted between two nodes. Baseband technology transmits a single data signal/stream/channel at a time while broadband technology transmits multiple data signals/streams/channels simultaneously at the same time.

The following image shows an example of both technologies.



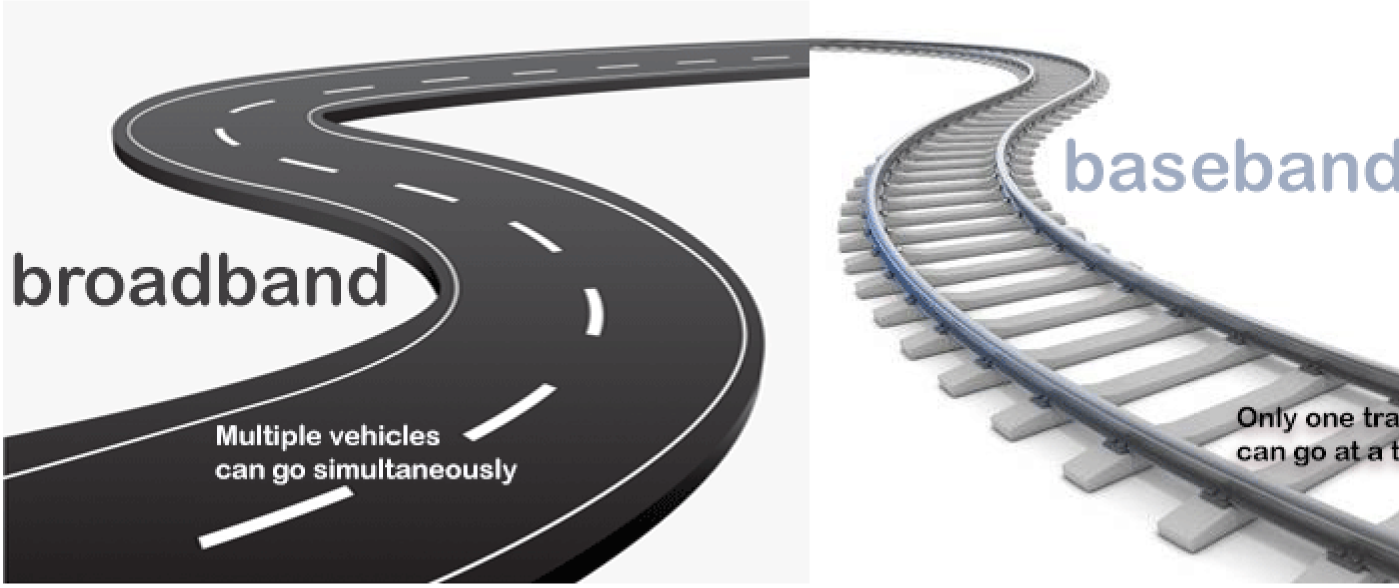
Baseband



Broadband

To understand the basic differences between both technologies, consider the baseband as a railway track and the broadband as a highway. Like, at a time, only one train can go on a railway track, in the baseband transmission only one data signal can be transmitted at a time.

Unlike a railway track on a highway, multiple vehicles can go simultaneously. For example, on a 3 lanes highway, 3 vehicles can go at the same time. Same as a highway, in the broadband transmission, multiple data signals can be transmitted at the same time.

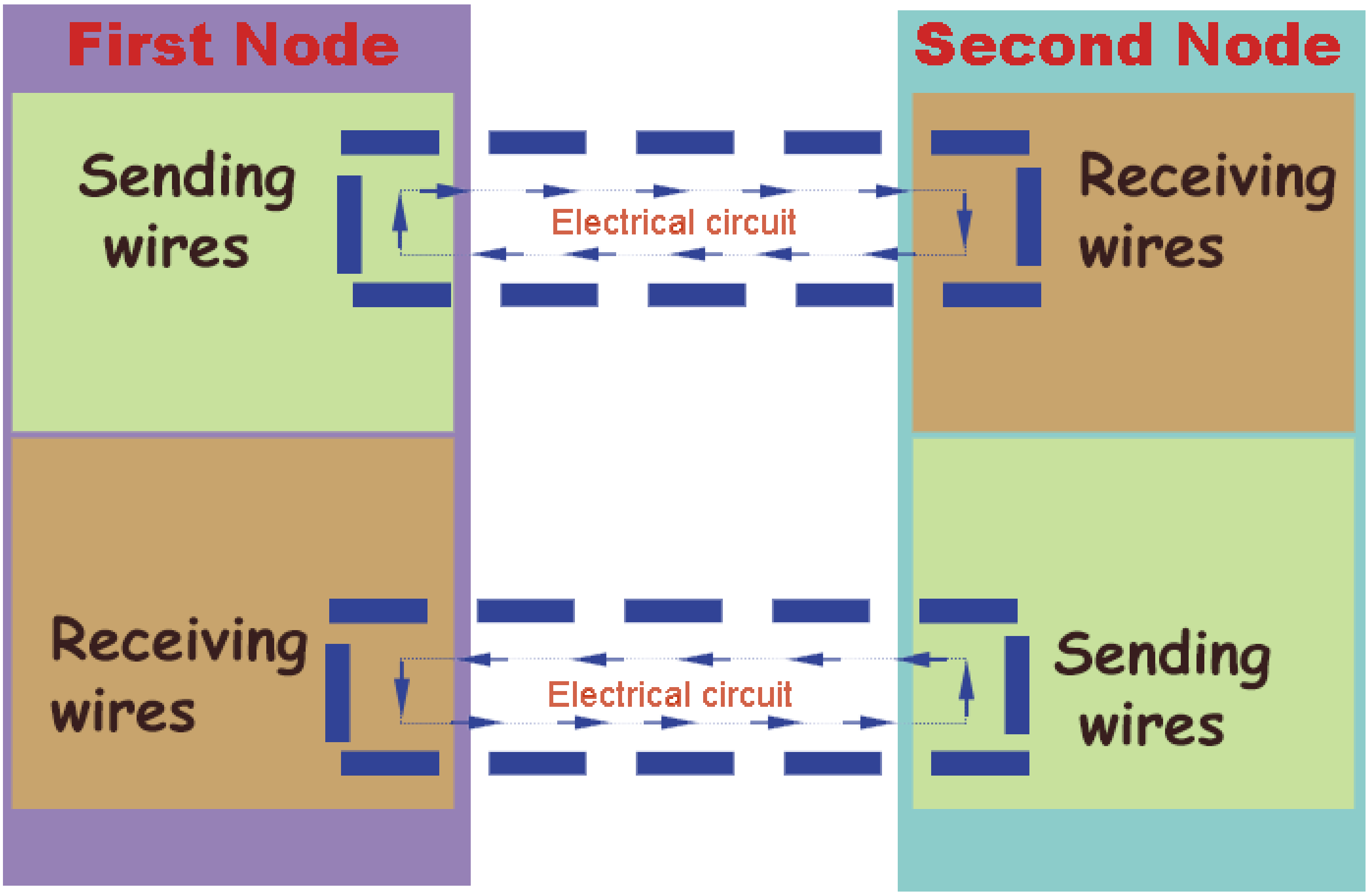


Technical differences between the baseband and broadband transmissions

Baseband technology uses digital signals in data transmission. It sends binary values directly as pulses of different voltage levels. Digital signals can be regenerated using repeaters in order to travel longer distances before weakening and becoming unusable because of attenuation.

Baseband supports bidirectional communication. It means, this technology can send and receive data simultaneously. To support bidirectional communication, this technology uses two separate electric circuits together; one for sending and another for receiving.

The following image shows an example of this.



Although baseband transmits only a single data stream at a time, it is possible to transmit signals of multiple nodes simultaneously. This is done by combining all the signals into a single data stream. To combine the signals of multiple nodes, a technology known as multiplexing is used. Baseband supports the Time Division Multiplexing (TDM).

To learn the types of multiplexing and how the multiplexing is done, you can check this tutorial.

Multiplexing and Demultiplexing Explained with Types

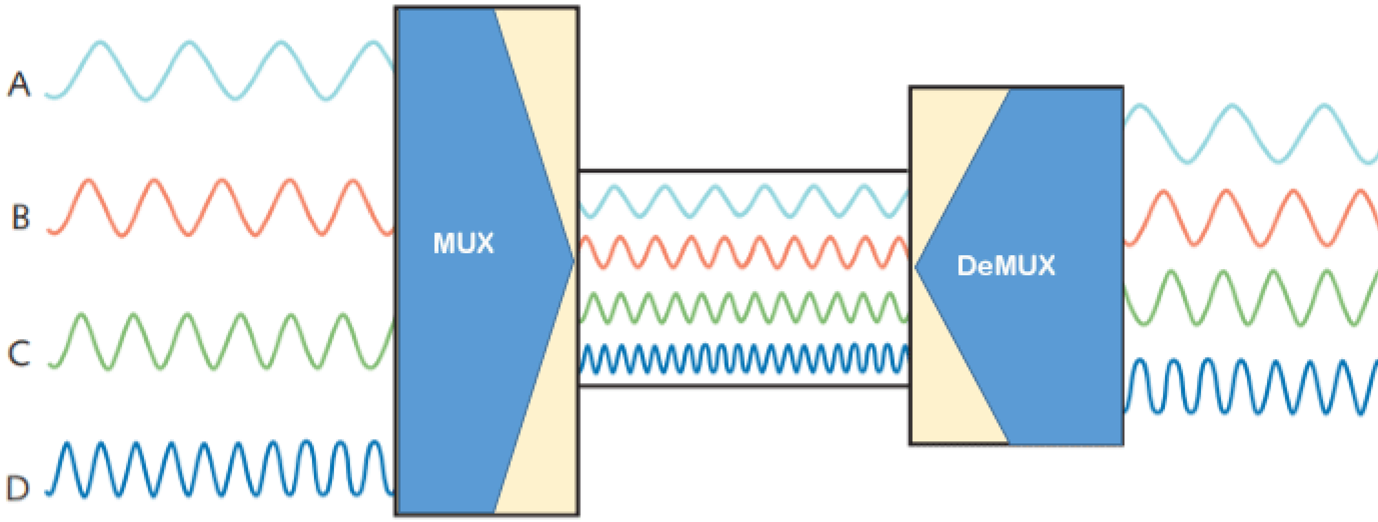
Baseband technology is mainly used in Ethernet networks to exchange data between nodes. This technology can be used on all three popular cable media types of Ethernet; coaxial, twisted-pair, fiber-optic.

Broadband transmission

Broadband technology uses analog signals in data transmission. This technology uses a special analog wave known as the **carrier wave**. A carrier wave does not contain any data but contains all properties of the analog signal. This technology mixes data/digital signal/binary values into the carrier wave and sends the carrier wave across the channel/medium.

To transmit data of multiple nodes simultaneously, this technology supports the Frequency Division Multiplexing. FDM (Frequency Division Multiplexing) divides the channel (medium or path) into several sub-channels and assigns a sub-channel to each node. Each sub-channel can carry a separate carrier wave.

The following image shows an example of this process.

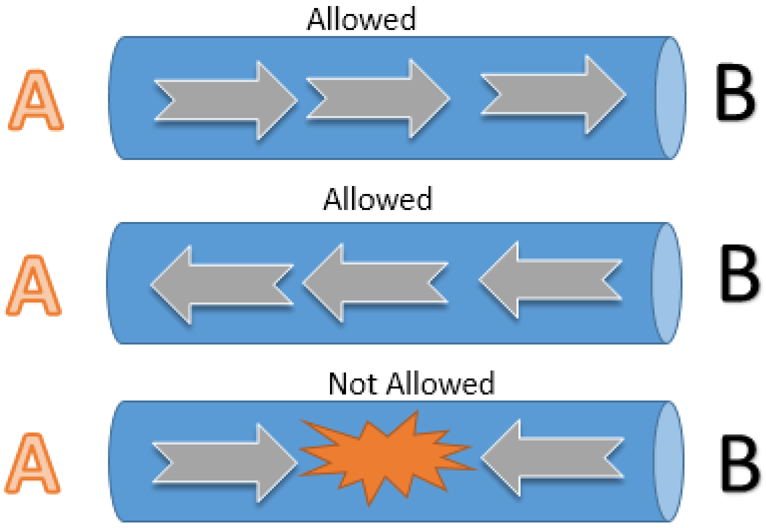


Analog signals can be regenerated using amplifiers in order to travel longer distances.

Broadband supports only unidirectional communication. It means, nodes connected at both ends of a medium can send or receive data but can't perform both actions simultaneously. Only one action is allowed at a time.

For example, two nodes A and B are connected through a cable that uses broadband technology to transmit signals. When node A transmits signals, node B receives the transmitted signals and when node B transmits signals, node A receives the transmitted signals.

The following image shows this example.



Broadband is typically used in an environment that transmits audio, video, and data simultaneously. For example, Cable TV Networks, Radio stations, and Telephone companies. Usually radio waves, coaxial, fiber-optic cables are used for broadband transmission.

Key differences between baseband and broadband transmissions

Baseband transmission	Broadband transmission
Transmit digital signals	Transmit analog signals
To boost signal strength, use repeaters	To boost signal strength, use amplifiers
Can transmit only a single data stream at a time	Can transmit multiple signal waves at a tim
Support bidirectional communication simultaneously	Support unidirectional communication onl
Support TDM based multiplexing	Support FDM based multiplexing
Use coaxial, twisted-pair, and fiber-optic cables	Use radio waves, coaxial cables, and fiber
Mainly used in Ethernet LAN networks	Mainly used in cable and telephone netwo

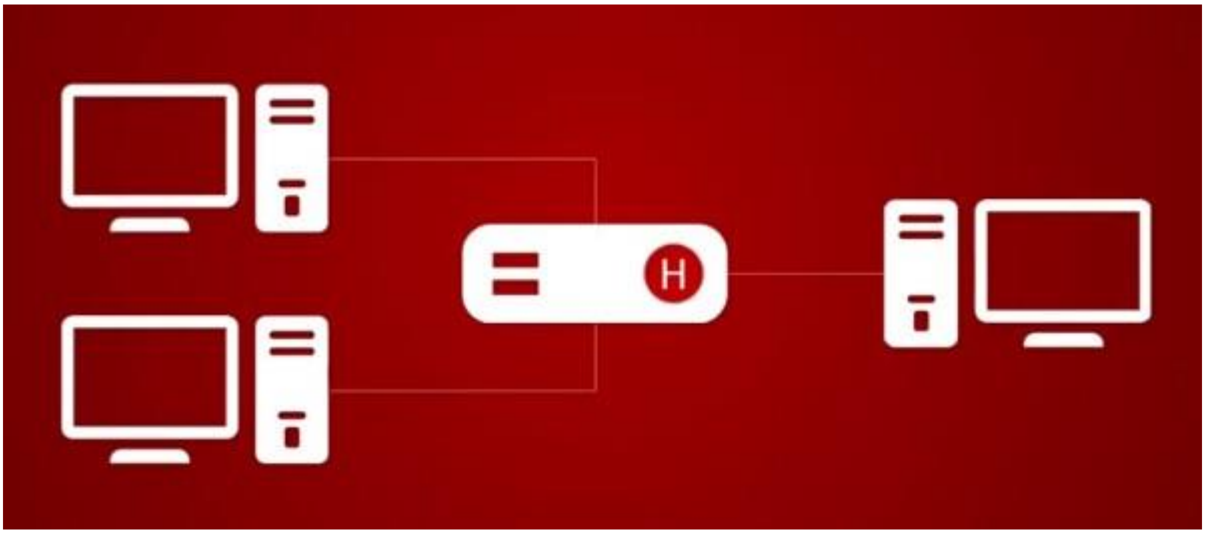
Q.4 What is the difference between a hub, modem, router and a switch?

Ans.4 When computers, network devices or other networks are required to be connected, hubs, **switches** and routers are the bridges to link them together. All the three types of devices can perform the same function, and technicians sometimes may use the terms interchangeably. However, this will make people confuse whether they are the same thing or different from each other. This post is going to explore the actual meanings of hub, switch, router and what they are used for.

Overview of Hub, Switch & Router

Hub

A hub is to sent out a message from one port to other ports. For example, if there are three computers of A, B, C, the message sent by a hub for computer A will also come to the other computers. But only computer A will respond and the response will also go out to every other port on the hub. Therefore, all the computers can receive the message and computers themselves need to decide whether to accept the message.



Switch

A switch is able to handle the data and knows the specific addresses to send the message. It can decide which computer is the message intended for and send the message directly to the right computer. The efficiency of switch has been greatly improved, thus providing a faster network speed.

Different Ports on WDM Mux/Demux

In the WDM (wavelength-division multiplexing) system, CWDM (coarse wavelength-division multiplexing) and DWDM (dense wavelength-division multiplexing) Mux/Demux (multiplexer/demultiplexer) modules are often deployed to join multiple wavelengths onto a single fiber. Multiplexer is for combining signals together, while demultiplexer is for splitting signals apart. On a WDM Mux/Demux, there are many kinds of ports for different applications. This article will discuss the functions of these ports on WDM Mux/Demux.

Necessary Ports on WDM Mux/Demux

Channel port and line port are the necessary ports to support the basic function of WDM Mux/Demux to join or split signals in the data network.

Channel Port

…

Read more · 3 min read

Feb 9, 2017

How Will SDN Change the Future Network?

Traditional networks are usually built with tiers of Ethernet **switches** in a tree structure. However, the development of mobile devices, server virtualization and cloud computing service has driven the need for dynamic computing and storage in data centers. Thus, the concept of software-defined networking (SDN) was put forward to construct a more flexible and agile network. This technology has widely caught people's attention in the industry over the years. In this post, some basic knowledge about SDN will be introduced to help you have better understanding.

Definition of SDN Architecture

SDN is a developing network architecture that aims to directly…

Read more · 3 min read

8

Jan 18, 2017

Have You Chosen the Right Power Cord?

Different cables have particular applications. Some are used for data transmission like fiber optic cable or copper cable, and some are used for the transmission of electrical power. **Power cord** is the assembly widely used as the connection between main electricity supply and the device through a wall socket or extension cord. Power cord is adopted in almost every where when the alternating current power is required. However, have you chosen the right type of power cord for your device? From this article, you may find the answers.

Overview of Power Cord

A power cord set usually has connectors molded...

Read more · 3 min read

Jan 16, 2017

Basic Knowledge of Wireless Access Point

With the rapid development of Ethernet network, cables are widely adopted for wired network connectivity. However, this may also lead to the problem of cable mess when large quantities of cables are deployed. In order to solve this issue, wireless network is now accepted by most network users to reduce the employment of cables. **Wireless access point** is an important device for connecting the wired network with wireless network. This article will talk about the fundamental knowledge about wireless access point.

What Is Wireless Access Point?

Wireless access point (WAP) is also known as access point (AP). It is a...

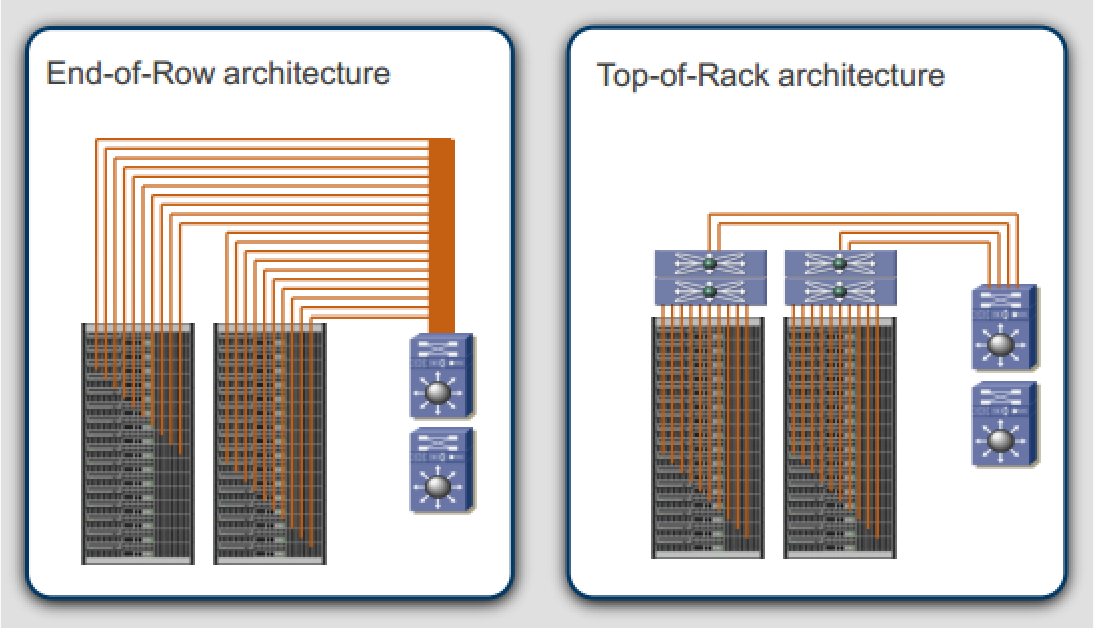
Read more · 3 min read

1

Jan 12, 2017

Data Center Architecture Designs Comparison: ToR Vs. EoR

The interconnection of switches and warranty of data communication are the basic aspects to consider when designing a data center architecture. Today's data centers have been shifted into 1RU and 2RU appliances, thus setting the 1RU and 2RU **switches** into the same-sized **racks** can greatly save space and reduce cabling demands. Typically, Top of Rack (ToR) and End of Row (EoR) are now the common infrastructure designs for data centers. In this article, we will mainly discuss the differences between these two approaches.



Overview of ToR & EoR

What Is ToR?

ToR approach refers to the physical placement of network...

Read more · 4 min read

More From Medium

Solving Minimum Coin Change

Try Khov

Q.5

We have compiled the most frequently asked Networking Interview Questions and Answers that will help you to prepare for the Networking basics interview questions that an interviewer might ask you during your interview. In this list of Networking interview questions, we have covered all commonly asked basic and advanced interview questions on networking with detailed answers to help you clear the job interview.

The below list covers 130+ important interview questions for Networking for freshers candidates as well as Networking interview questions for experienced. This detailed guide of Network Engineer interview questions will help you to crack your Job interview easily.

Network Engineer Interview Questions and Answers

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.

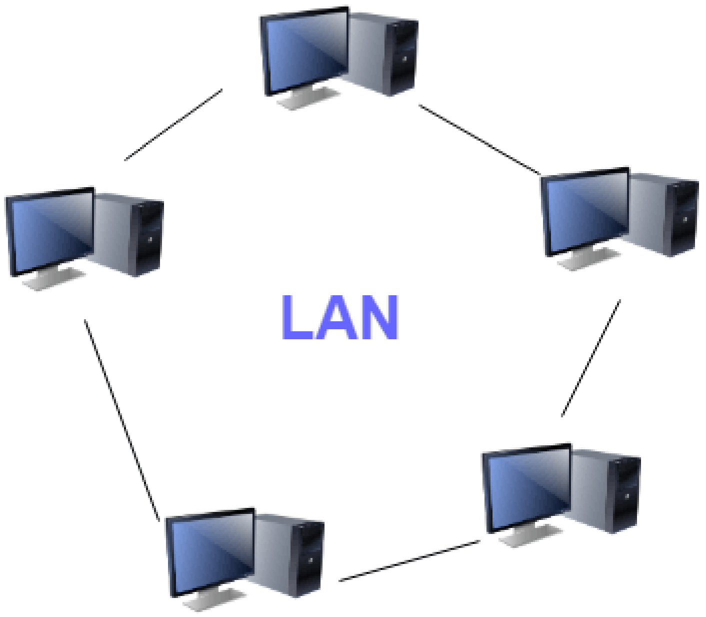
2) What are the layers of the OSI reference model?

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?



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?

Router

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 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.

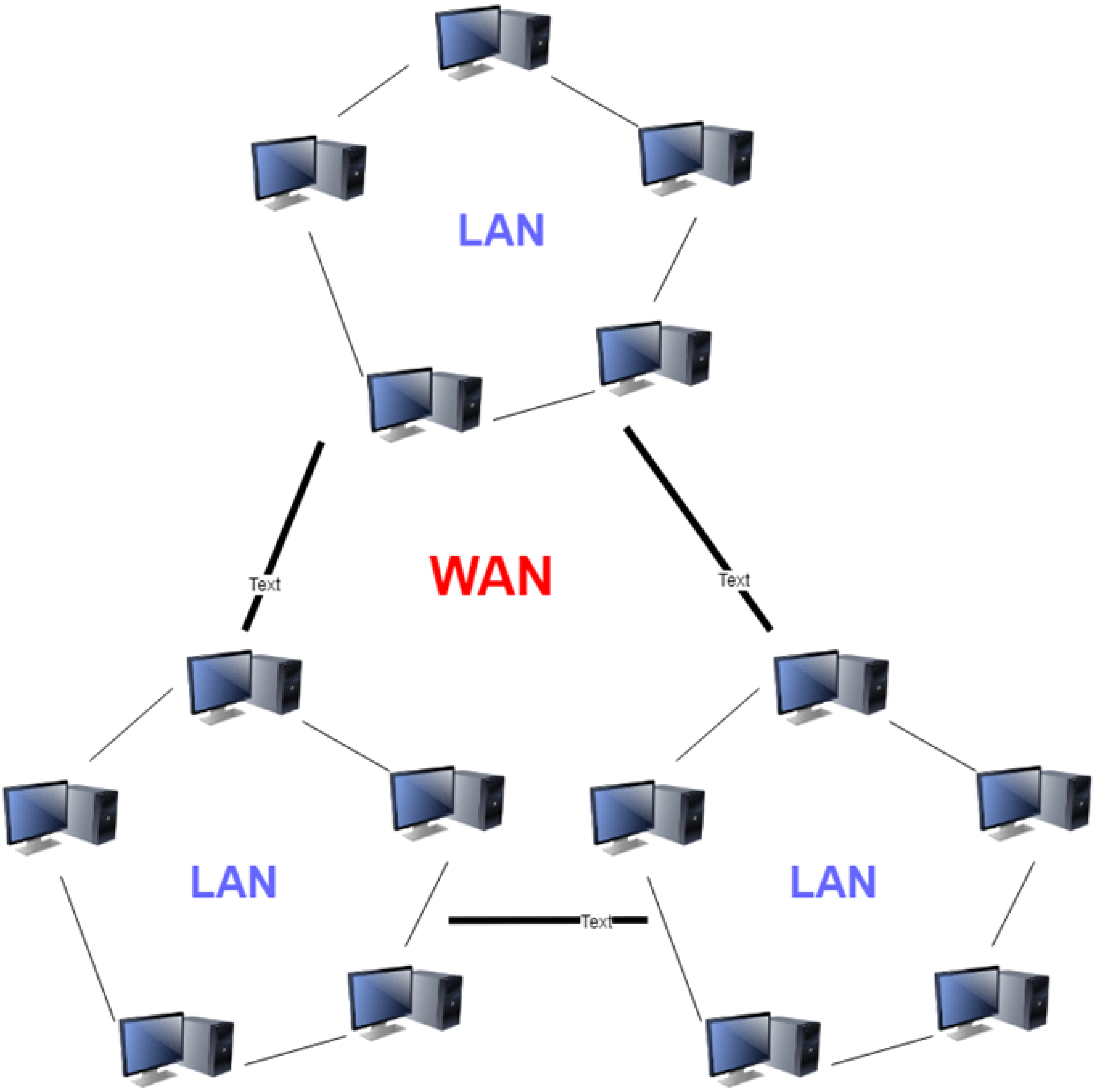
18) What are the different ways of securing a computer network?

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?



WAN network

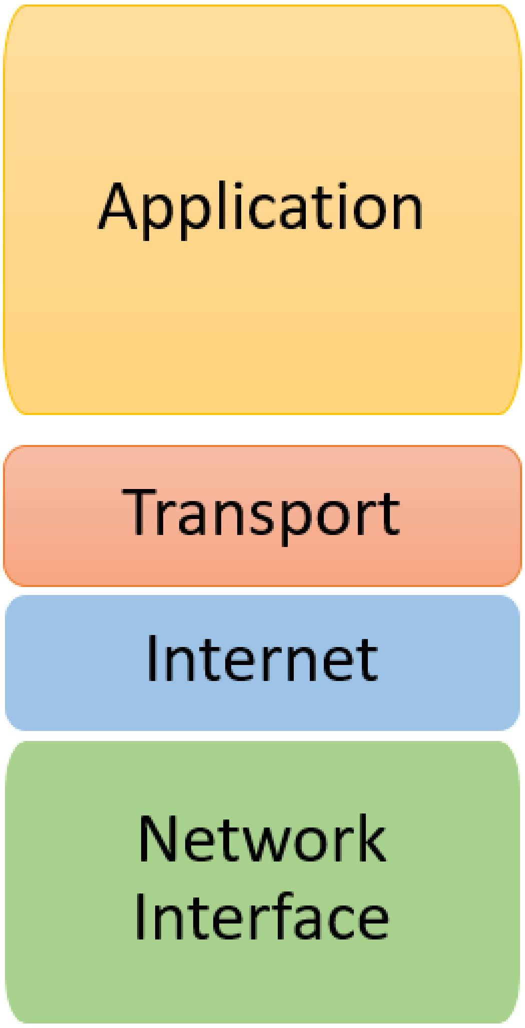
WAN stands for Wide Area Network. It is an interconnection of computers and devices that are geographically dispersed. It connects networks that are located in different regions and countries.

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.



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?

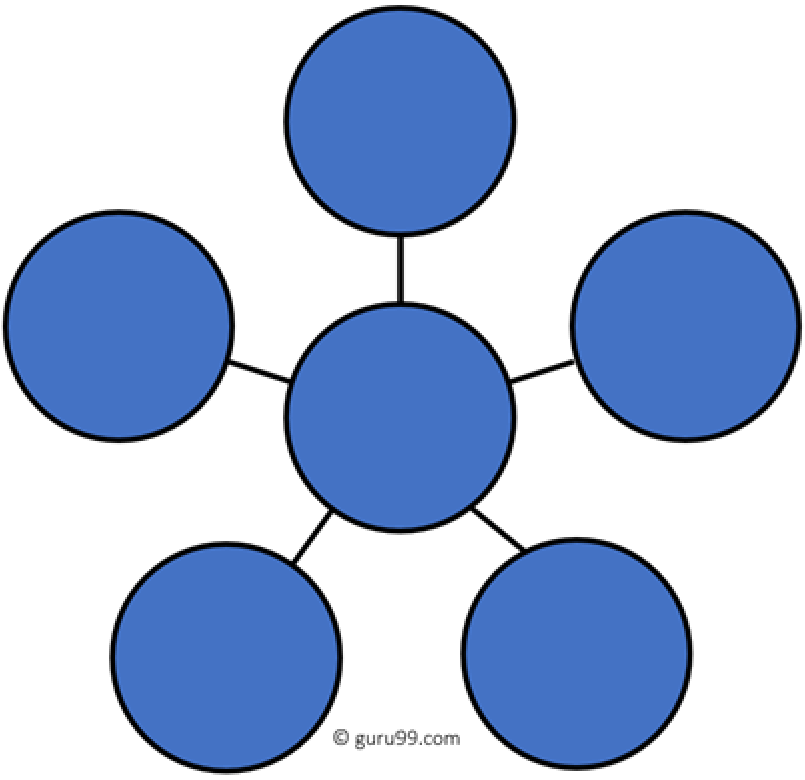
OSPF, or Open Shortest Path First, is a link-state routing protocol that uses routing tables to determine the best possible path for data exchange.

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.



Star Topology

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

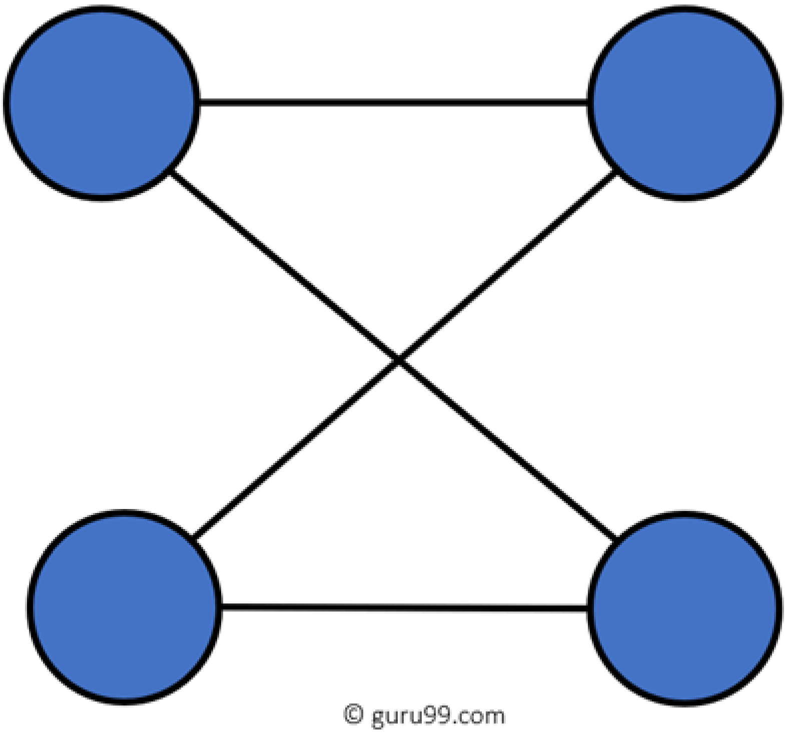
59) What is ICMP?

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?



P2P Network

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?

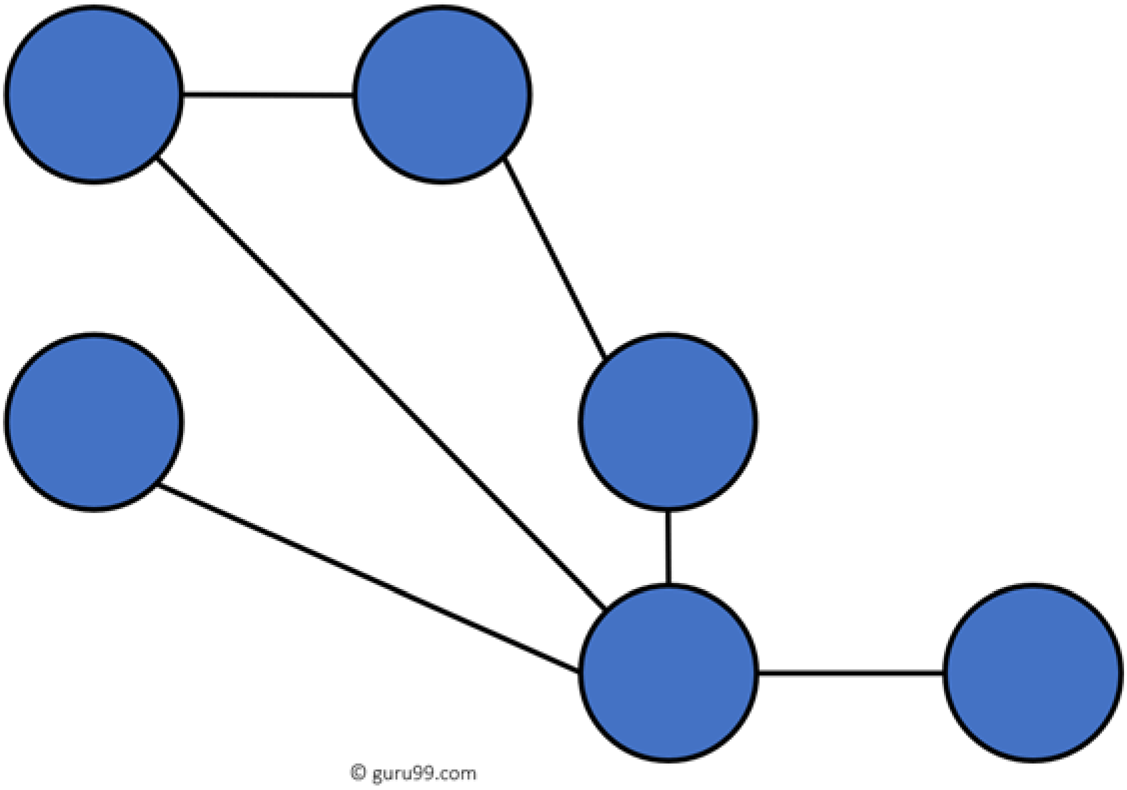
- Analog connections - using conventional telephone lines
- Digital connections - using digital-grade telephone lines
- Switched connections - using multiple sets of links between the sender and receiver to move data.

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.

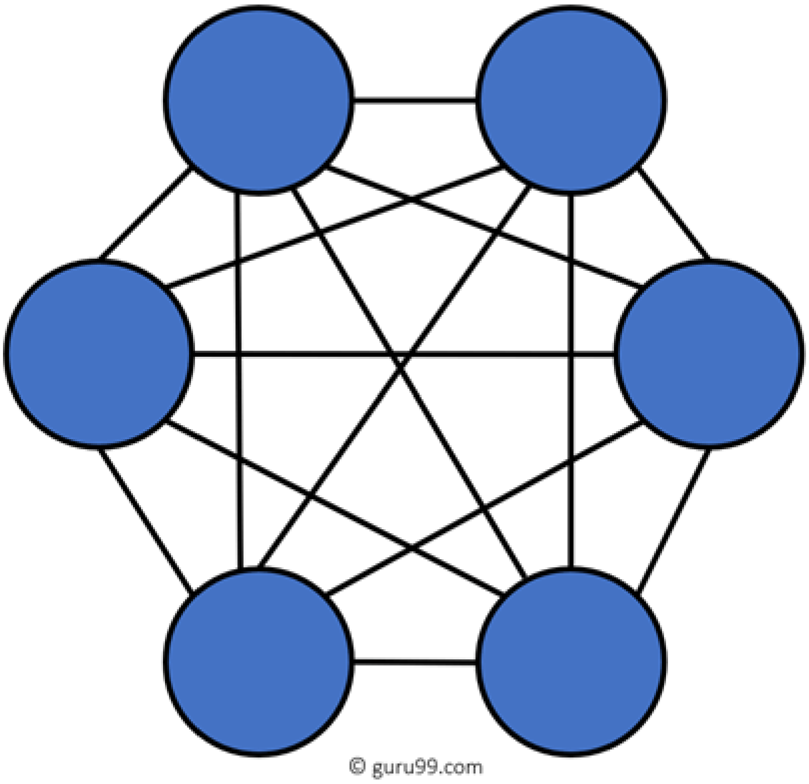
Types of Mesh Topology:

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.


© guru99.com

Partially Connected Mesh Topology

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



Fully Connected Mesh Topology

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?

Here are some major differences between TCP and UDP protocols:

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

destination router.	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.

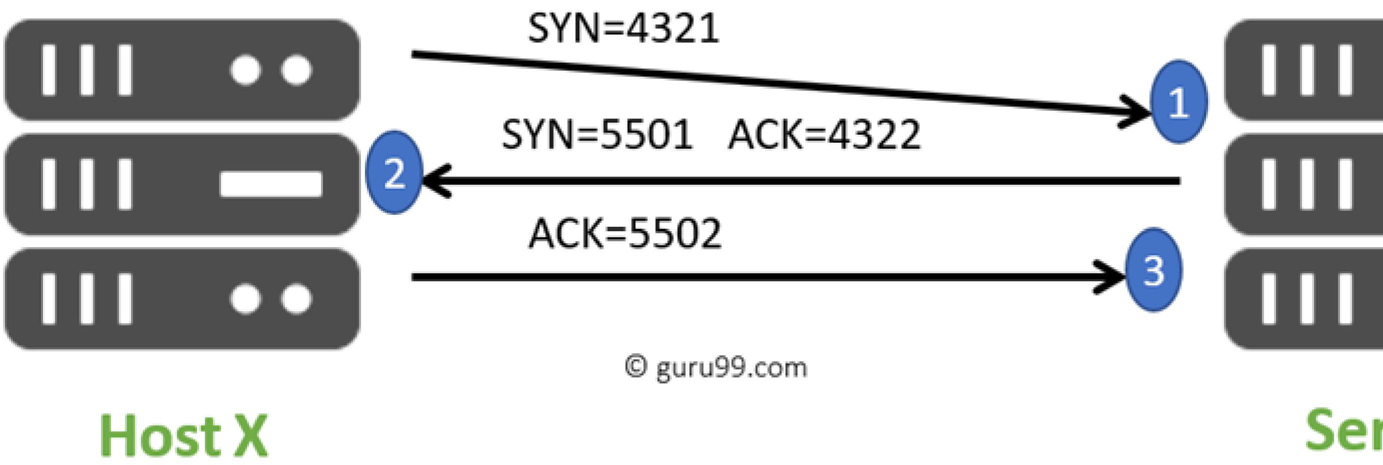
120) What is the use of a Pseudo TTY?

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?



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 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.

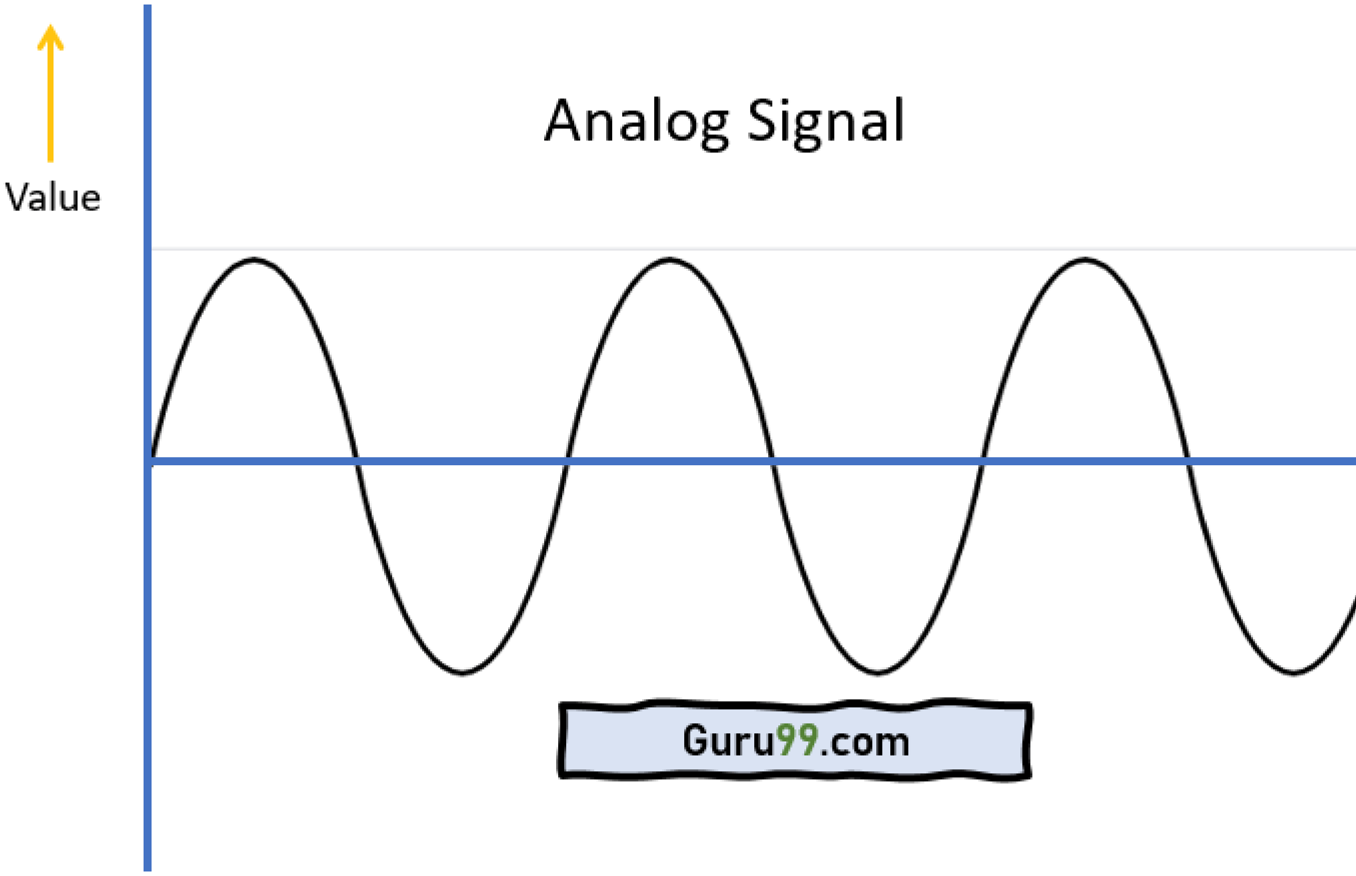
129) What are the important differences between MAC address and IP address

Here, are some difference between MAC and IP 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.

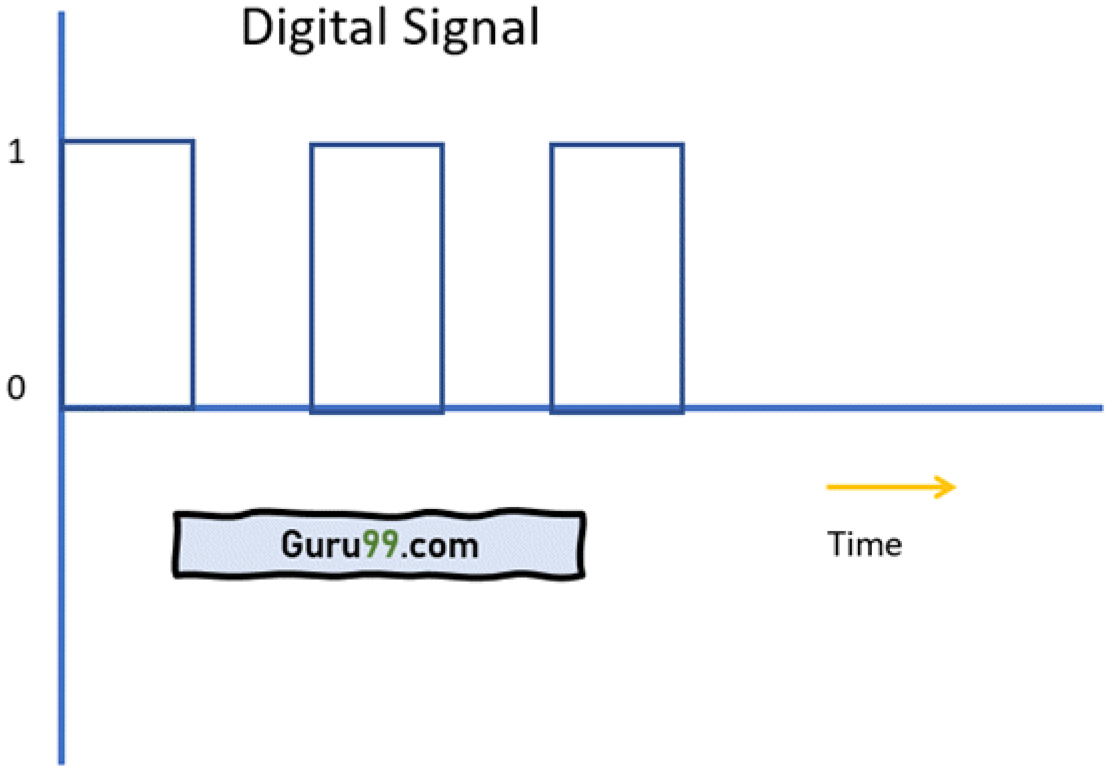
130) What is an Analog Signal?



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?



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.

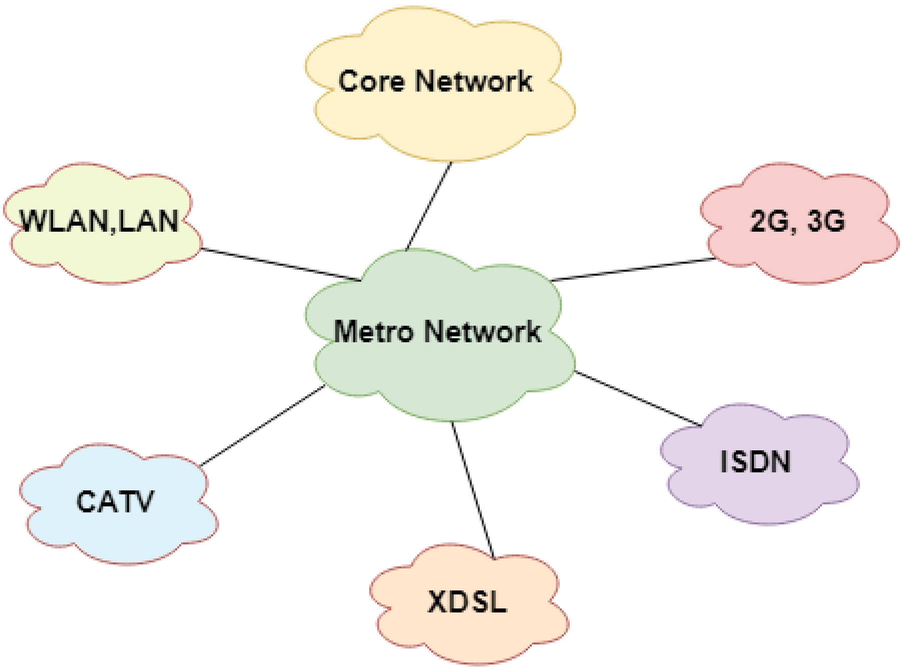
132) What are the differences between analog and digital signal?

Here are the main differences between Analog and Digital 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?



MAN network

A Metropolitan Area Network or MAN is consisting of a computer network 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.

Modem

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.

- Prev

Report a Bug

- Next

Computers communicate using networks. These networks could be on a local area network LAN or...

Read more

ETHICAL HACKING

15 BEST Digital Forensic Tools in 2021 [Free/Paid]

Digital forensic is a process of preservation, identification, extraction, and documentation of...

Read more

ETHICAL HACKING

10 Most Common Web Security Vulnerabilities

OWASP or Open Web Security Project is a non-profit charitable organization focused on improving...

Read more

ETHICAL HACKING

20+ Best FREE Anti Spyware (Malware) Removal Tools

Anti-spyware removes malicious spyware and protects your computer system. They detect and remove...

Read more

ETHICAL HACKING

Top 25 Ethical Hacking Interview Questions and Answers

We have prepared the most important Ethical Hacking interview questions to help you prepare for...

Read more

ETHICAL HACKING

What is Cybercrime? Types, Tools, Examples

What is Cybercrime? Cybercrime is defined as an unlawful action against any person using a...

Read more

Networking Tutorial

- Circuit Vs Packet
- Synchronous Vs Asynchronous
- Networking Interview Q & A
- Computer Network Books

- Computer Networking Cou.

Q.6 When troubleshooting computer network problems, what common hardware-related

problems can occur?

Ans.6

A hardware problem or issue is one of the most dreaded incidences for a computer user. This is due to the fact that such a malfunction can result into complete computer failure. With respect to this, it is considered very important for an individual to be conversant with all the available troubleshooting tools. In addition, one should ensure that he or she is familiar with the indicators or symptoms of a hardware failure so as to curb it in advance. Below is a brief description of some of the most common hardware problems and their resolutions.

Common symptoms

Here are some common symptoms through which one can know if the hardware has got some problems or not;

Unexpected shutdowns

Unexpected shutdowns occur when a computer just turns off without making any notification or giving a message. This is a problem that can be very frustrating since it can lead to loss of unsaved work or even interruption of a session one are logged onto. In most cases, such a problem occurs due to possible system changes such as addition of a new hardware driver. In such an occurrence, the operating system is not completely stopped and one can press the NUM Lock key or Ctrl+Alt+Del to try and get back to the OS for recovery.

In case that fails, one can run some hardware diagnostic tests so as to have a thorough check of anything that could be interrupting one's system. One can perform the Power on Self-Test (POST).

System lockups

System lockups can be very frustrating especially if they occur without the display of an alert message. The screen appears as if it is frozen. Looking at the Event viewer can be good but in such problems with one's hardware, it may not be of much help because the Event Viewer has nothing written on it.

POST code beeps

The Power on self-test occurs when one's computer is immediately powered on to check for one's computer's minimum hardware configurations. POST code beeps are normally delivered via the system speaker and serve as a communication media when the video is not working. Each beep has a correspondence to a specific error message.

Blank screen on boot up

A blank screen on boot up is another dreaded problem that does not necessarily indicate a problem with video but one associated with configurations of the BIOS. In such a case, one may choose to make BIOS modifications so that instead of using a separately installed video card, one can configure the BIOS to utilize the in-built one and identify some of the problems occurring.

BIOS time and settings resets

Unplugging one's computer or powering it off does not lead to lose of computer configurations. At times, the BIOS configurations may keep resetting and getting erased due to the CMOS battery on the motherboard getting spoilt or it no longer being charged. In addition, one may also receive some prompts indicating an invalid configuration or incorrect date and time setting. In case of such a problem, replacing the CMOS battery can be the best way to come up with a resolution for the problem. One can also decide to carry out a complete clearance of the BIOS configuration which should be done in accordance to documentations by the manufacturer.

Attempts to boot to incorrect device

At times, one may see attempts by one's computer to boot from the wrong device for instance when one are using an external USB and the computer system attempts to boot from the USB instead of the internal drive in the computer. The boot order of one's computer can be set at the BIOS where one decide the particular drive to start up or one may alter the order in which the boot process occurs. With such a problem at hand, one should take a look at one's BIOS configurations and possibly modify them in a way that is ideal for one's system.

Continuous reboots

This is a problem that mostly occurs in instances where one's computer keeps looping over the start up process where it appears to be starting and then restarts. In such a case, the first step should be to try and establish the occurrence point of the problem either in the course of the BIOS check where the Power on Self-test is undergoing among some other possible reasons. Once that is established, then one can easily decide if the problem is hardware related or related to the Windows configuration.

No power

At times, one may turn on one's computer and nothing of much significance happens. This should therefore reflect to the possibility of some power related issues in one's computer. Use one's Multimeter check so as to see if there is some power coming from the wall socket. Also ensure that the motherboard is powered which can then help in identification of the problem in one's computer.

Overheating

One's computer tends to emit a lot of heat due to the numerous numbers of components running in it and generating the heat. In case of an overheating problem, then urgent cooling is required. One can induce cooling by using some fans to bring in cool air into one's computer. In this case, the fans can be passed over the warm equipment making the heat to rise up and allow the cool air to pass in much faster.

The HW Monitor is an example of software that one can use to access and determine the level of heat in one's computer

One can also do some troubleshooting or maybe clean one's system. Make an effort to ensure that there is proper spinning of the fans, clear dust and restart one's system to check if such a heat problem occurs. With that, one will be able to accurately determine the occurrence point of one's problem.

Loud noise

A computer should not be a source of too much noise>. The only noise allowed is just a little humming of the fan. Noise inside the computer case could result from some loose components inside it. Such noise can be heard when trying to move one's computer between two different locations. Some scraping noise from the inside case could be an indicator of the hard drive going bad. Some of the odd noises one will hear in such cases call for immediate backup of one's stuff in the drive.

There may also be some clicking noises which relate to fans not working properly or getting spoilt. Such noises can also indicate that the fans spinning rate is too fast. Such noises should be resolved with immediate effect so as to ensure that one's computer's cooling system is in good working condition.

Intermittent device failure

This can be a very frustrating issue whose occurrence is not specific on execution of any activity but just random. Such a problem could translate into the possibility of a hardware problem and therefore a comprehensive hardware check should be the first step to handle this. One should also take a close check at the software drivers since a software driver that is poorly written can be the cause of such a problem. Ensure that all the software drivers are the latest versions.

Fans spin - no power to other devices

Sometimes, one may power on one's computer and the only activity going on is the spinning of the fans and nothing more. Such an incidence should clearly indicate that there is a problem with power supply to the motherboard, either it is just sufficient to drive the fans and not enough for one's motherboard. In addition, it could also mean that one have a problem with one's motherboard. With the fans driving power not relying on the motherboard, a change of the motherboard can be done to try and fix the problem.

Indicator lights

Indicator lights are normally associated with some computer components for instance the network adapter or a sign that the power is on. With these lights, one can easily determine if the component associated with them is working. In case the lights are not working or functional, that should immediately translate into a faulty component.

Smoke

It is said that smoke being emitted by one's computer is what keeps it running. However, the smoke released is not too much to be seen. In some cases, one might smell some smoke or bad odour coming from one's computer. This should be a clear indication that there are some electrical problems in one's computer. This therefore calls for immediate disconnection of the power source but to be much safer, unplug the power cord behind one's computer.

Burning smell

A burning smell from inside one's computer is also another problem to call for alarm. This means that one should open up one's system and check for any blown capacitors. In addition, check for any component on the motherboard that appears to be black or not alright. On completion of a visual check, one should run a hardware diagnosis so as to establish the source of the burning smell. Make a comprehensive check on every hardware component of the computer so as to be sure that such a problem will not arise in future.

BSOD

The blue screen of death also known as the Windows Stop Error is quite dreaded since it completely stops everything and it is only a reboot of the system that can get things back to normal. With the information displayed on the screen being of utmost importance, one should write it on an Event Viewer so as to determine activities that happened in the past. With the Event Viewer tracking down of the exact point the problem occurs becomes quite easy.

Tools:

Here are some tools which can be used for the fixation of hardware;

Multimeter

The multimeter is a special kind of device that one should be well trained to use especially if one are to handle electrical issues with one's hardware. This is a device that can be used to take resistance, current and voltage measurements. One should make sure that the right kind of Multimeter is what one has since this is a tool that must be highly accurate when taking any kind of measurements. One should settle on one that is very easy to use and with a lot of clarity. High levels of accuracy should also be considered. The multimeter can be used to check alternating current voltage. One can also use it to check the direct current so as to ascertain that the voltage to the motherboard is okay and also ensure that the CMOS battery is fully charged.

Power supply tester

A power supply tester is a tool that is very easy to use since it bears a perfect display on its front where power can be plugged directly from the power supply. Plugging other components into this device can give one voltage statistics and information concerning what one have plugged in as well as the voltage they are using.

Loopback plugs

Loopback plugs are mainly used in cases where one is working on network connections either serial or wide area connections. These plugs are used to test physical ports and should be used hand in hand with specific software which will send out information and wait to receive it. The loopback plug for serial ports is RS-232 while for network connections are Ethernet or T1.

POST card

The power on self- test card becomes of much importance the moment one start-up one's computer and one get nothing from it. This card looks at the power and issue detailed error messages to help one discover more concerning one's hardware problems.

It is unarguably true that computer hardware problems can be quite a nuisance and headache especially for an individual not well conversant with the hardware problems and their troubleshooting tools. On the other hand, knowing the hardware problems but not being aware of their troubleshooting tools can be of no use. It is therefore important that one equip one's self with all the important information ranging from hardware problems to their troubleshooting tools. With that in mind, handling hardware related problems becomes very easy and one can even do it by one's self without the need to consult a computer expert.

Q.7

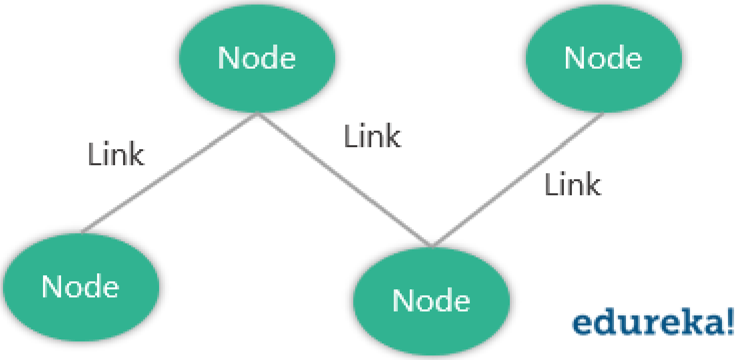
HUB	SWITCH	ROUTER
Connects two or more Ethernet devices	Connects two or more LAN devices	Can connect devices or a LAN and WAN
Does not perform filtering	Filters packets before forwarding them	Highly configured to filter and send packets
Least intelligent, least expensive and least complex	Similar to a hub, but more effective	Extremely smart and complex

Q2. What is a link?

A link basically is the connection between two or more computers or devices. It can be anything depending on whether it is a physical connection or a wireless one. Physical links include cables, hubs, switches, etc and wireless links wireless access points, routers, etc.

Q3. What do you mean by a Node?

The point of intersection in a network is called a Node. Nodes can send or receive data/ information within a network. For example, if two computers are connected to form a network, there are 2 nodes in that network. Similarly, in case there are computers, there will be three nodes and so on. It is not necessary for a node to be a computer, it can be any communicating device such as a printer, servers, modems, etc.



Q4. What does a backbone network mean?

In any system, backbone is the most principle component that supports all other components. Similarly, in networking, a Backbone Network is a Network that interconnects various parts of the network to which it belongs and has a high capacity connectivity infrastructure.

Q5. What is Network Topology?

The physical layout of the computer network is called as Network Topology. It gives the design of how all the devices are connected in a network.

Type	Description
Bus Topology	All the devices share a common communication line
Star Topology	All nodes are connected to a central hub device
Ring Topology	Each node connects to exactly two other nodes
Mesh Topology	Each node is connected to one or more nodes
Tree Topology (Hierarchical Topology)	Similar to star topology and inherits the bus topology
Daisy Chain Topology	All nodes are connected linearly
Hybrid Topology	Nodes are connected in more than one topology styles
Point-to-Point Topology	Connects two hosts such as computers, servers, etc

Q6. Explain what is LAN?

A LAN or Local Area Network the network between devices that are located within a small physical location. It can be either wireless or wired. One LAN differs from another based on the following factors:

- Topology: The arrangement of nodes within the network
- Protocol: Refer to the rules for the transfer of data
- Media: These devices can be connected using optic fibers, twisted-pair wires, etc

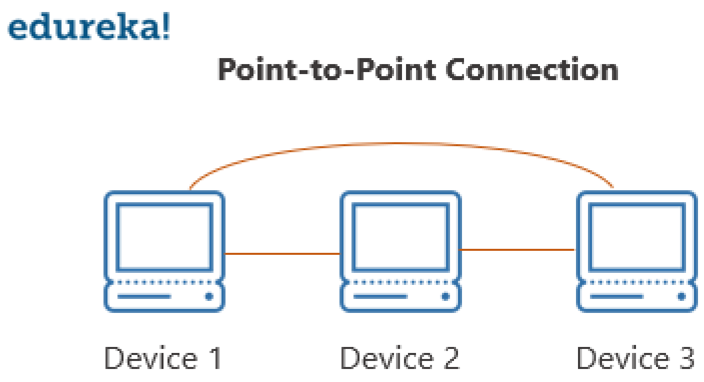
Q7. What are Routers?

A router is some device that transfers the data packets within a network. It basically performs the traffic directing functions within a network. A data packet can be anything such as an email, a web page, etc. Routers are located at the place where two or more networks meet or the gateways.

Routers can either be stand-alone devices or virtual. Stand-alone routers are traditional devices where as virtual routers are actually softwares that act like physical ones.

Q8. What is a Point-to-Point Network?

A Point-to-Point network refers to a physical connection between two nodes. It can be between any device of a network such as a computer, printer, etc.

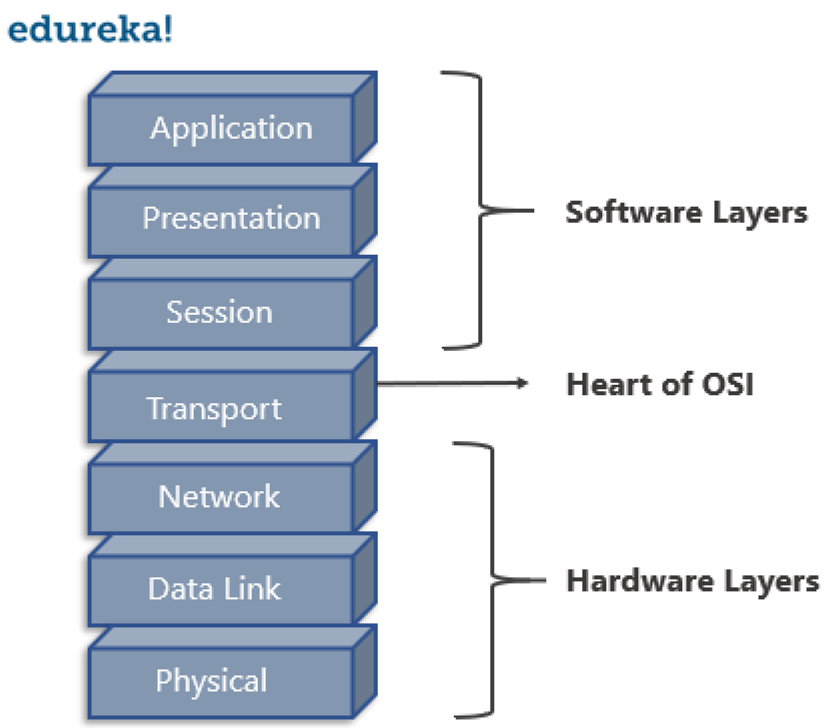


For example, as you can see in the above diagram, all the nodes are connected to each other i.e Device 1 is connected to Device 2 and Device 3 , Device 2 is connected to Device 3 and Device 1 and Device 3 is connected to Device 2 and Device 1 using physical links.

Q9. What is OSI Model?

OSI stands for Open Systems Interconnection. It is a conceptual model that standardizes communication functions of telecommunication. It has 7 layers which are:

1. Physical Layer
2. Data Link Layer
3. Network Layer
4. Transport Layer
5. Session Layer
6. Presentation Layer
7. Application Layer



Q10. Give a brief about each layer in the OSI Model.

Layer Name	Protocol	Description
Physical Layer	Symbol	Transfers raw bits of data over a physical link
Data Link Layer	Frame	Reliable transmission of data frames between nodes connected by the physical layer
Network Layer	Packet	Structures and manages a network with multiple nodes including addressing, routing and traffic control
Transport Layer	Segment, Datagram	Reliable Transmission of data packets between the different points of a network
Session Layer	Data	Manages the communication sessions
Presentation Layer	Data	Transmission of data between the service device and the application

Application Layer	Data	Specifies the shared communication protocols and the interface methods

To learn about Network Programming in Java and Python in detail refer to the following blogs:

- Socket Programming in Java
- Socket Programming in Python

Q11. What do you mean by anonymous FTP?

An anonymous FTP is a way of allowing a user to access data that is public. The user does not need to identify himself to the server and has to log in as anonymous.

So in case you are asked to use anonymous ftp, make sure you add “anonymous” in place of your user id. Anonymous FTPs are very effective while distributing large files to a lot of people, without having to give huge numbers of usernames and password combinations.

Q12. What is the meaning of Network?

A network is a connection between different devices. These devices communicate with each other using physical or wireless connections. Physical connections include twisted pair cables, optic fibers, and coaxial cables..wireless networks can be established with the help of waves such as radio waves infrared waves and microwaves
Networks basically serve many purposes such as:

- Sharing hardware devices such as printers, input devices, etc
- Help in communications in many ways such as audios videos emails messages etc
- Help in sharing data and information using virtual devices
- They also help sharing softwares that are installed on other devices

Q13. What do you mean by a Subnet Mask?

A Subnet Mask is the number describing the range of IP addresses that can be used within a network. They are used to assign subnetworks or subnets. These subnetworks are various LAN’s connected to the internet.

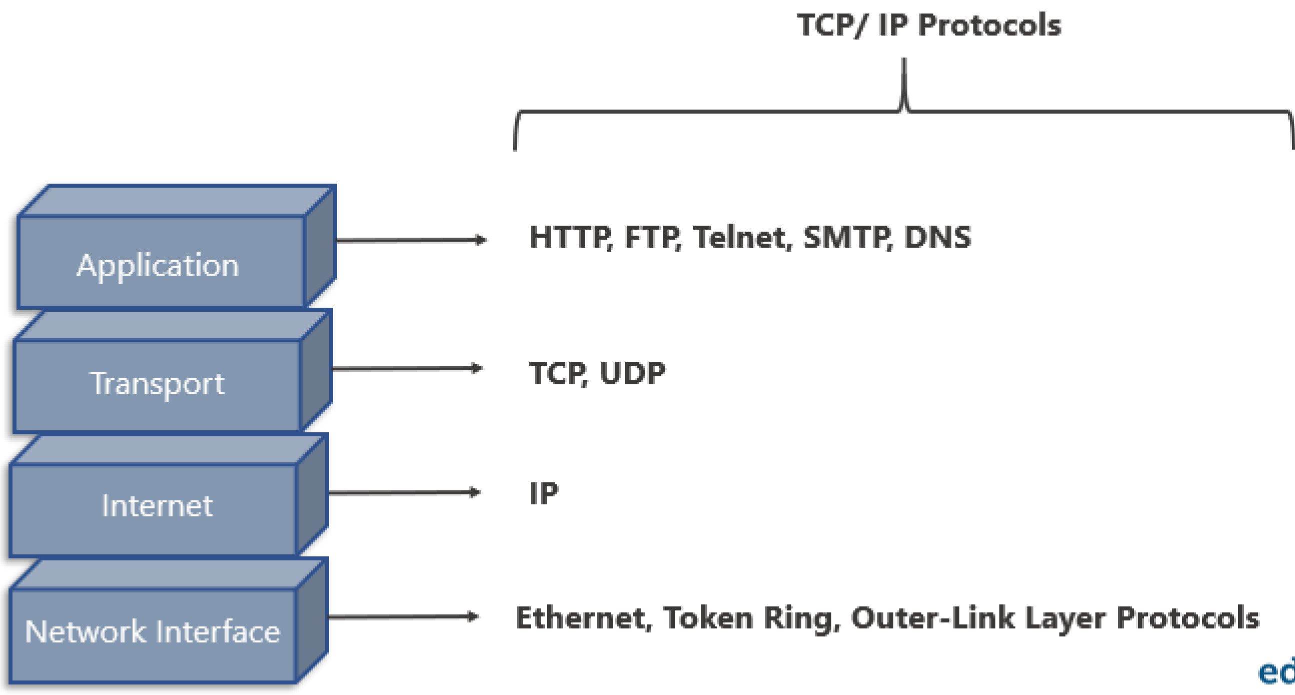
This Subnet mask is basically a 32-bit number and it masks the IP address and then divides the IP address into two parts i.e the network address and the host address. Subnet Masks are created by setting all the network bits to “1” and all the host bits to “0”s. There are two network addresses that cannot be assigned to any host on the network i.e The “0” and “255” which are assigned to network and to the broadcast address, and this is why they cannot be assigned to any host.

Q14. Give a brief description of the TCP/ IP Model.

The TCP/ IP Model is a compressed version of the OSI Model. This Model contains 4 layers unlike the OSI Model which are:

1. Process(Application Layer)
2. Host-to-Host(Transport Layer)

3. Internet Layer (Network Layer)
4. Network Access(Combination of Physical and Data Link Layer)


TCP/ IP Protocols
Application
Transport
Internet
Network Interface
HTTP, FTP, Telnet, SMTP, DNS
TCP, UDP
IP
Ethernet, Token Ring, Outer-Link Layer Protocols
ed

Q15. What is the difference between the OSI Model and TCP/ IP Model?

TCP/ IP Model	OSI Model
Has four layers	Has seven layers
More reliable	Less reliable
No strict boundaries	Has strict boundaries
Horizontal Approach	Vertical Approach

Q16. What is a UTP cable?

A UTP cable is a 100 ohms cable made up of copper. It consists of 2-1800 unshielded twisted pairs that are surrounded by a non-metallic case. These twists provide immunity to electrical noise and EMI.

Q17. What is the maximum length allowed for a UTP cable?

The maximum length allowed for a UTP cable is 100m. This includes 90 m of solid cabling and 10m of standard patch cable.

Q18. Explain what is HTTP and which port does it use?

HTTP or HyperText Transfer Protocol allows communication over the Internet. This protocol basically defines how messages are to be transmitted and formatted over the world wide web. HTTP is a TCP/ IP protocol and it uses the port number 80.

Features of HTTP Protocol:

- It is connection-less
- Does not depend on the type of connecting media
- Stateless

Q19. What is NAT?

NAT stands for Network Address Translation. It deals with remapping one IP Address space with another by changing the IP headers of the packets that are being transmitted across a traffic routing device.

Q20. What is TCP?

TCP or Transmission Control Protocol is a connection-oriented protocol that establishes and maintains a connection between communicating devices until both of them are done exchanging messages. This protocol determines how application data can be broken down into packets that can be delivered over a network. It also sends and receives packets to and from the network layer and is in charge of flow control, etc.

Q21. Give a brief explanation about UDP?

UDP or the User Datagram Protocol is used to create a low-latency and loss-tolerating communications between applications connected over the internet. UDP enables process-to-process communication and communicates via datagrams or messages.

Q22. Differentiate between TCP and UDP.

Factor of comparison	TCP	UDP
Connection	Connection made before application messages are exchanged	Connection not made before application messages are exchanged
Use	For applications needing more reliability and less speed	For applications needing more speedy and less reliability
Use by Protocols of the Application Layer	File transfer, e-mail, etc	Multimedia, DNS
Reliability	Messages will be delivered in order and without errors	No guarantee that the messages will be delivered in order and without errors
Data Segments	Data segments rearranged in required order	All segments are independent, therefore has no inherent order specification
Acknowledgment	ACK is received	ACK is not received

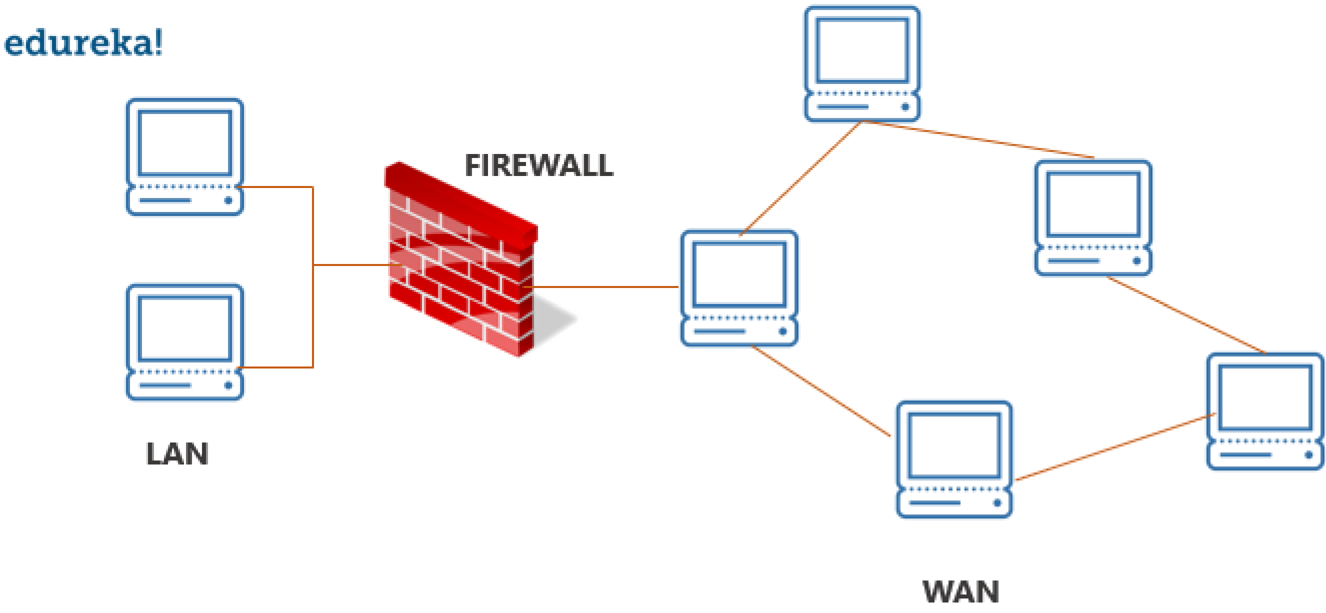
Flow Control	Has the congestion control mechanism	No flow control option
Check for Errors	Resends erroneous segments	Discards Erroneous segments

Q23. What is RIP?

RIP (Routing Information Protocol) is a dynamic routing protocol. It makes use of hop count as its primary metric to find the best path between the source and the destination. It works in the application layer and has an AD (Administrative Distance) value of 120.

Q24. Explain what is a firewall?

A firewall is a network security system which is used to monitor and control the network traffic based on some predefined rules. Firewalls are the first line of defense and establish barriers between the internal and external networks in order to avoid attack from untrusted external networks. Firewalls can be either hardware, software or sometimes both.



Q25. Explain what is NOS?

A Network Operating System (NOS) is an Operating System that is designed to support workstations, databases, personal computers, etc over a network. Some examples of NOS are MAC OS X, Linux, Windows Server 2008, etc. These Operating Systems provide various functionalities such as processor support, multiprocessing support, authentication, Web services, etc.

Q26. Explain what is Denial of Service (DoS)?

Denial of Service (DoS) is a kind of attack that prevents a legitimate user from accessing data over a network by a hacker or an attacker. The attacker floods the server with unnecessary requests in order to overload the server thereby preventing the legitimate users from accessing its services.

Q27. What is the full form of ASCII?

ASCII stands for American Standard Code for Information Interchange. It is a character encoding standard used in the electronic communication field. The ASCII codes basically represent text.

Q28. What is IEEE?

IEEE stands for **I**nstitute of **E**lectrical and **E**lectronics **E**ngineer. It is the world's largest technical professional society and is devoted to advancing innovation and technological excellence.

Q29. What is a MAC address and why is it required?

MAC or Media Access Control address is a computer's unique number assigned to a Network Interface Controller (NIC). It is a 48-bit number that identifies each device on a network and is also referred to as the physical address. MAC addresses are used as a network address for communications within a network such as an Ethernet, Wi-Fi, etc.

Q30. What is piggybacking?

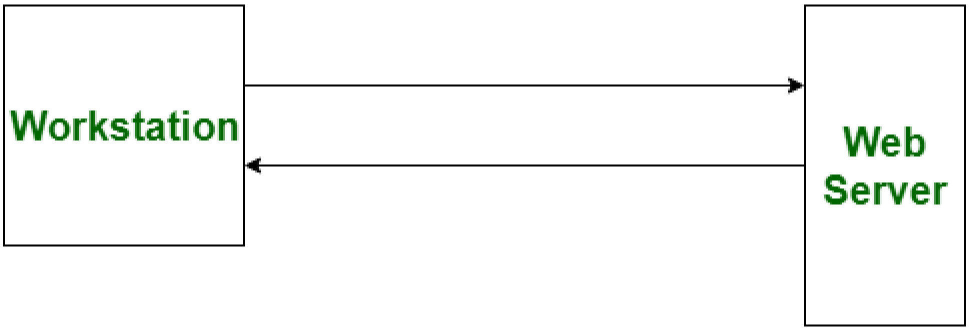
During transmission of data packets in two-way communication, the receiver sends an acknowledgment (control frame or ACK) to the receiver after receiving the data packets. However, the receiver does not send the acknowledgment immediately, but, waits until its network layer passes in the next data packet. Then, the ACK is attached to the outgoing data frame. This process of delaying the ACK and attaching it to the next outgoing data frame is known as piggybacking.

Q31. Explain what is DNS?

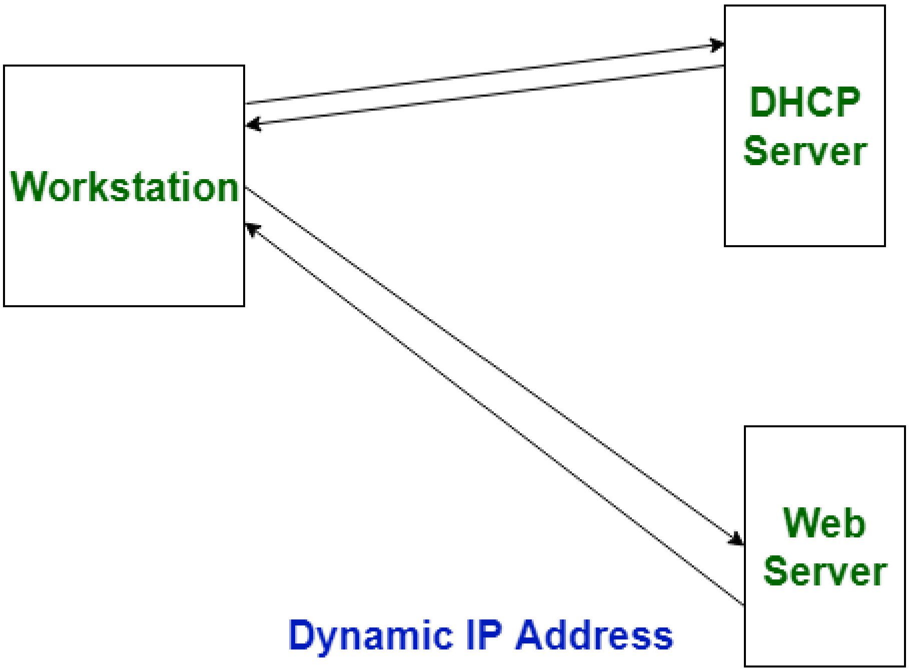
DNS or Domain Name System is a naming system for devices connected over the internet. It is a hierarchical and decentralized system that translates domain names to the numerical IP Addresses which is required to identify and locate devices based on the underlying protocols.

All devices connected to the internet have unique IP addresses which are used to locate them on

Q. 8 **IP** stands for **Internet Protocol**. IP address may be a distinctive numerical symbol allotted to every device on a network to spot each affiliation unambiguously. The distinction between Static and Dynamic IP address lies inside the length of allotted scientific discipline address. The static scientific discipline address is fastened scientific discipline address that is manually allotted to a tool for a protracted amount of your time. On the opposite hand, the Dynamic scientific discipline address oft changes whenever user boots his/her machine, and it's mechanically allotted.



Static IP Address



Dynamic IP Address

Difference between Static and Dynamic IP address:

S.NO	Static IP Address	Dynamic IP address
1.	It is provided by ISP(Internet Service Provider).	While it is provided by DHCP (Dynamic Host Configuration Protocol).
2.	Static ip address does not change any time, it means if a static ip address is provided then it can’t be changed or modified.	While dynamic ip address change any time.
3.	Static ip address is less secure.	While in dynamic ip address, there is low amount of risk than static ip address’s risk.

S.NO	Static IP Address	Dynamic IP address
4.	Static ip address is difficult to designate.	While dynamic ip address is easy to designate.
5.	The device designed by static ip address can be trace.	But the device designed by dynamic ip address can’t be trace.
6.	Static ip address is more stable than dynamic ip address.	While dynamic ip address is less stable than static ip address.
7.	The cost to maintain the static ip address is higher than dynamic ip address.	While the maintaining cost of dynamic ip address is less than static ip address.
8.	It is used where computational data is less confidential.	While it is used where data is more confidential and needs more security.

Q.9. Discuss TCP/IP model in detail.

Ans.

What is the TCP/IP Model?

TCP/IP Model helps you to determine how a specific computer should be connected to the internet and how data should be transmitted between them. It helps you to create a virtual network when multiple computer networks are connected together. The purpose of TCP/IP model is to allow communication over large distances.

TCP/IP stands for Transmission Control Protocol/ Internet Protocol. TCP/IP Protocol Stack is specifically designed as a model to offer highly reliable and end-to-end byte stream over an unreliable internetwork.

In this TCP/IP tutorial, you will learn:

- TCP Characteristics
- Four Layers of TCP/IP model
- Application Layer
- Transport Layer

TCP Characteristics

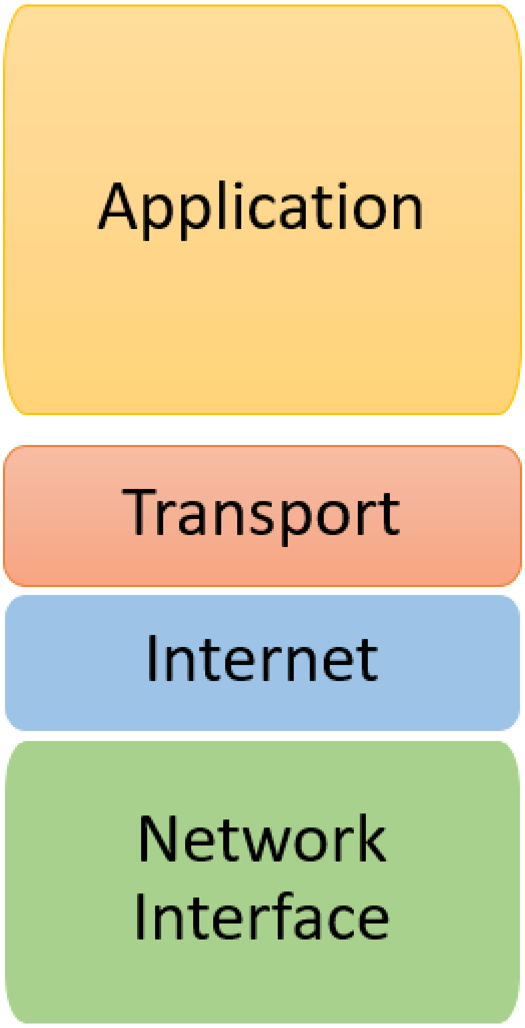
Here, are the essential characteristics of TCP/IP protocol

- Support for a flexible TCP/IP architecture
- Adding more system to a network is easy.
- In TCP/IP, the network remains intact until the source, and destination machines were functioning properly.
- TCP is a connection-oriented protocol.
- TCP offers reliability and ensures that data which arrives out of sequence should put back into order.

- TCP allows you to implement flow control, so sender never overpowers a receiver with data.

Four Layers of TCP/IP model

In this TCP/IP tutorial, we will learn about different TCP/IP layers and their functions



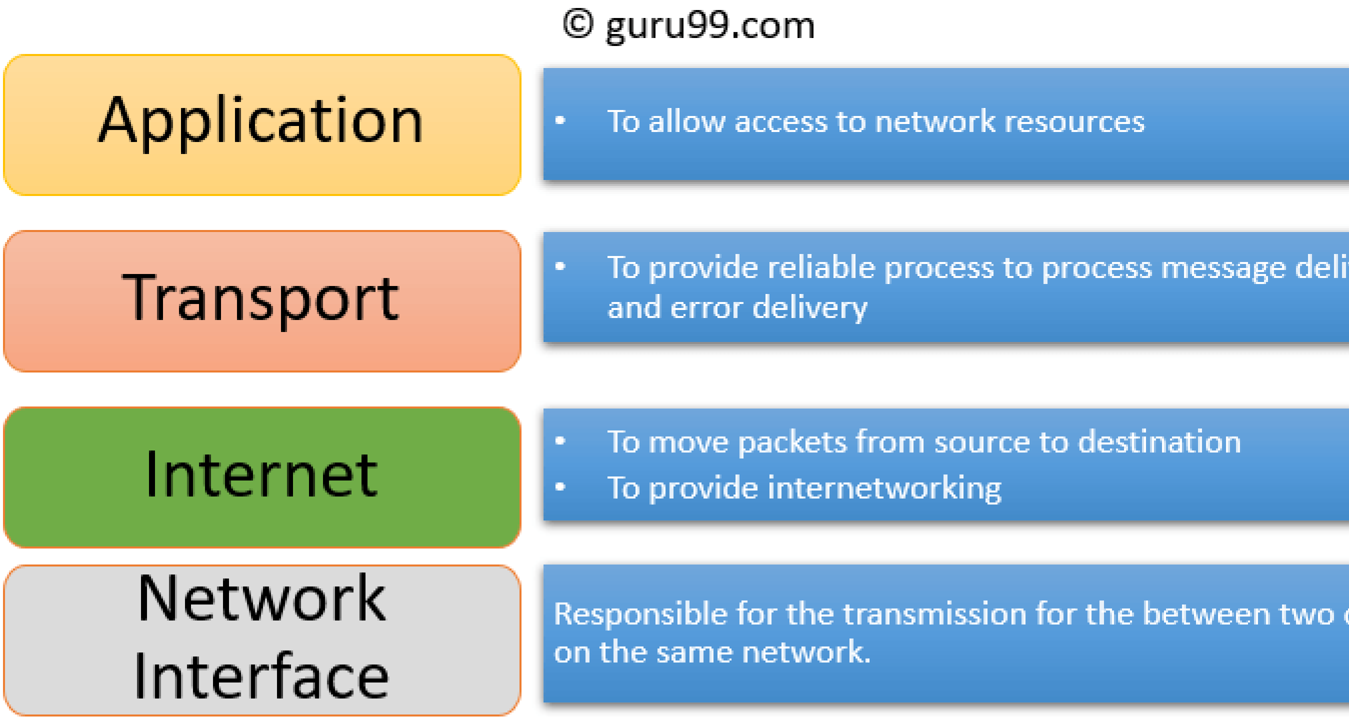
TCP/IP Conceptual Layers

The functionality of the TCP IP model is divided into four layers, and each includes specific protocols.

TCP/IP is a layered server architecture system in which each layer is defined according to a specific function to perform. All these four TCP/IP layers work collaboratively to transmit the data from one layer to another.

- Application Layer
- Transport Layer

- Internet Layer
- Network Interface


© guru99.com

- To allow access to network resources
- To provide reliable process to process message deli
and error delivery
- To move packets from source to destination
- To provide internetworking

Responsible for the transmission for the between two
on the same network.

Application Layer

Application layer interacts with an application program, which is the highest level of OSI model. The application layer is the OSI layer, which is closest to the end-user. It means the OSI application layer allows users to interact with other software application.

Application layer interacts with software applications to implement a communicating component. The interpretation of data by the application program is always outside the scope of the OSI model.

Example of the application layer is an application such as file transfer, email, remote login, etc.

The function of the Application Layers are:

- Application-layer helps you to identify communication partners, determining resource availability, and synchronizing communication.
- It allows users to log on to a remote host
- This layer provides various e-mail services
- This application offers distributed database sources and access for global information about various objects and services.

Transport Layer

Transport layer builds on the network layer in order to provide data transport from a process on a source system machine to a process on a destination system. It is hosted using single or multiple networks, and also maintains the quality of service functions.

It determines how much data should be sent where and at what rate. This layer builds on the message which are received from the application layer. It helps ensure that data units are delivered error-free and in sequence.

Transport layer helps you to control the reliability of a link through flow control, error control, and segmentation or de-segmentation.

The transport layer also offers an acknowledgment of the successful data transmission and sends the next data in case no errors occurred. TCP is the best-known example of the transport layer.

Important functions of Transport Layers:

- It divides the message received from the session layer into segments and numbers them to make a sequence.
- Transport layer makes sure that the message is delivered to the correct process on the destination machine.
- It also makes sure that the entire message arrives without any error else it should be retransmitted.

Internet Layer

An internet layer is a second layer of TCP/IP layes of the TCP/IP model. It is also known as a network layer. The main work of this layer is to send the packets from any network, and any computer still they reach the destination irrespective of the route they take.

The Internet layer offers the functional and procedural method for transferring variable length data sequences from one node to another with the help of various networks.

Message delivery at the network layer does not give any guaranteed to be reliable network layer protocol.

Layer-management protocols that belong to the network layer are:

1. Routing protocols
2. Multicast group management

3. Network-layer address assignment.

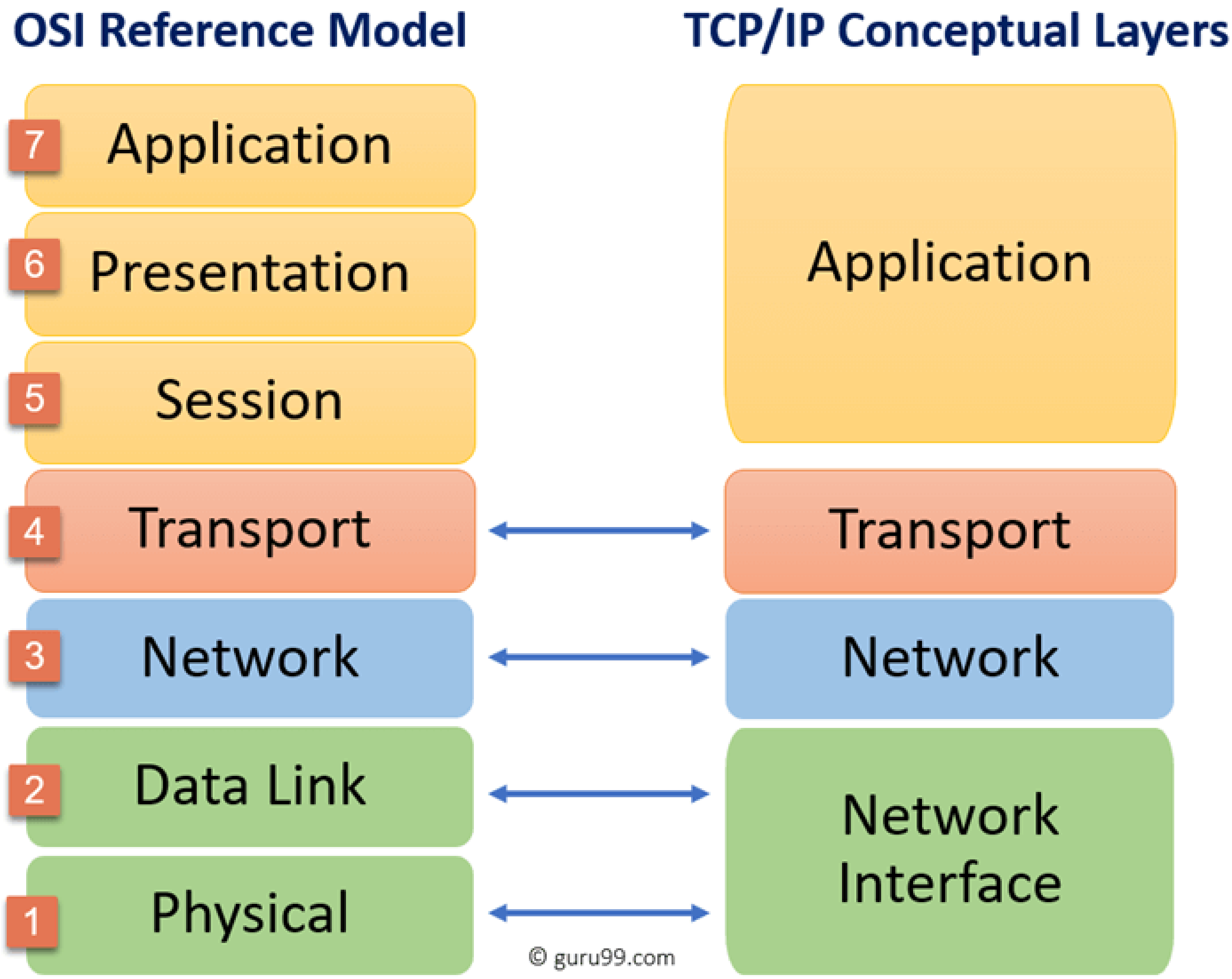
The Network Interface Layer

Network Interface Layer is this layer of the four-layer TCP/IP model. This layer is also called a network access layer. It helps you to defines details of how data should be sent using the network.

It also includes how bits should optically be signaled by hardware devices which directly interfaces with a network medium, like coaxial, optical, coaxial, fiber, or twisted-pair cables.

A network layer is a combination of the data line and defined in the article of OSI reference model. This layer defines how the data should be sent physically through the network. This layer is responsible for the transmission of the data between two devices on the same network.

Differences between OSI and TCP/IP models



Here, are some important differences between the OSI and TCP/IP model:

OSI Model	TCP/IP model
It is developed by ISO (International Standard Organization)	It is developed by ARPANET (Advanced Research Project Agency Network).
OSI model provides a clear distinction between interfaces, services, and protocols.	TCP/IP doesn't have any clear distinguishing points between services, interfaces, and protocols.

OSI refers to Open Systems Interconnection.	TCP refers to Transmission Control Protocol.
OSI uses the network layer to define routing standards and protocols.	TCP/IP uses only the Internet layer.
OSI follows a vertical approach.	TCP/IP follows a horizontal approach.
OSI model use two separate layers physical and data link to define the functionality of the bottom layers.	TCP/IP uses only one layer (link).
OSI layers have seven layers.	TCP/IP has four layers.
OSI model, the transport layer is only connection-oriented.	A layer of the TCP/IP model is both connection-oriented and connectionless.
In the OSI model, the data link layer and physical are separate layers.	In TCP, physical and data link are both combined as a single host-to-network layer.
Session and presentation layers are not a part of the TCP model.	There is no session and presentation layer in TCP model.
It is defined after the advent of the Internet.	It is defined before the advent of the internet.
The minimum size of the OSI header is 5 bytes.	Minimum header size is 20 bytes.

Most Common TCP/IP Protocols

Some widely used most common TCP/IP protocol are:

TCP:

Transmission Control Protocol is an internet protocol suite which breaks up the message into TCP Segments and reassembling them at the receiving side.

IP:

An Internet Protocol address that is also known as an IP address is a numerical label. It is assigned to each device that is connected to a computer network which uses the IP for communication. Its routing function allows internetworking and essentially establishes the Internet. Combination of IP with a TCP allows developing a virtual connection between a destination and a source.

HTTP:

The Hypertext Transfer Protocol is a foundation of the World Wide Web. It is used for transferring webpages and other such resources from the HTTP server or web server to the web client or the HTTP client. Whenever you use a web browser like Google Chrome or Firefox, you are using a web client. It helps HTTP to transfer web pages that you request from the remote servers.

SMTP:

SMTP stands for Simple mail transfer protocol. This protocol supports the e-mail is known as a simple mail transfer protocol. This protocol helps you to send the data to another e-mail address.

SNMP:

SNMP stands for Simple Network Management Protocol. It is a framework which is used for managing the devices on the internet by using the TCP/IP protocol.

DNS:

DNS stands for Domain Name System. An IP address that is used to identify the connection of a host to the internet uniquely. However, users prefer to use names instead of addresses for that DNS.

TELNET:

TELNET stands for Terminal Network. It establishes the connection between the local and remote computer. It established connection in such a manner that you can simulate your local system at the remote system.

FTP:

FTP stands for File Transfer Protocol. It is a mostly used standard protocol for transmitting the files from one machine to another.

Advantages of the TCP/IP model

Here, are pros/benefits of using the TCP/IP model:

- It helps you to establish/set up a connection between different types of computers.
- It operates independently of the operating system.
- It supports many routing-protocols.
- It enables the internetworking between the organizations.
- TCP/IP model has a highly scalable client-server architecture.
- It can be operated independently.
- Supports a number of routing protocols.
- It can be used to establish a connection between two computers.

Disadvantages of the TCP/IP model

Here, are few drawbacks of using the TCP/IP model:

- TCP/IP is a complicated model to set up and manage.
- The shallow/overhead of TCP/IP is higher-than IPX (Internetwork Packet Exchange).
- In this, model the transport layer does not guarantee delivery of packets.
- Replacing protocol in TCP/IP is not easy.
- It has no clear separation from its services, interfaces, and protocols.

Summary:

- The full form or TCP/IP model explained as Transmission Control Protocol/ Internet Protocol.
- TCP supports flexible architecture
- Four layers of TCP/IP model are 1) Application Layer 2) Transport Layer 3) Internet Layer 4) Network Interface
- Application layer interacts with an application program, which is the highest level of OSI model.
- Internet layer is a second layer of the TCP/IP model. It is also known as a network layer.

- Transport layer builds on the network layer in order to provide data transport from a process on a source system machine to a process on a destination system.
- Network Interface Layer is this layer of the four-layer TCP/IP model. This layer is also called a network access layer.
- OSI model is developed by ISO (International Standard Organization) whereas TCP/IP model is developed by ARPANET (Advanced Research Project Agency Network).
- An Internet Protocol address that is also known as an IP address is a numerical label.
- HTTP is a foundation of the World Wide Web.
- SMTP stands for Simple mail transfer protocol which supports the e-mail is known as a simple mail transfer
- SNMP stands for Simple Network Management Protocol.
- DNS stands for Domain Name System.
- TELNET stands for Terminal Network. It establishes the connection between the local and remote computer
- FTP stands for File Transfer Protocol. It is a mostly used standard protocol for transmitting the files from one machine to another.
- The biggest benefit of TCP/IP model is that it helps you to establish/set up a connection between different types of computers.
- TCP/IP is a complicated model to set up and manage.

Q.10 What is a Web Browser (Browser)? Give some example of browsers.

Ans. 10. A web browser, or simply "browser," is an application used to access and view websites. Common web browsers include Microsoft Internet Explorer, Google Chrome, Mozilla Firefox, and Apple Safari.

The primary function of a web browser is to render HTML, the code used to design or "mark up" webpages. Each time a browser loads a web page, it processes the HTML, which may include text, links, and references to images and other items, such as cascading style sheets and JavaScript functions. The browser processes these items, then renders them in the browser window.

Early web browsers, such as Mosaic and Netscape Navigator, were simple applications that rendered HTML, processed form input, and supported bookmarks. As websites have evolved, so have web browser requirements. Today's browsers are far more advanced, supporting multiple types of HTML (such as XHTML and HTML 5), dynamic JavaScript, and encryption used by secure websites.

The capabilities of modern web browsers allow web developers to create highly interactive websites. For example, Ajax enables a browser to dynamically update information on a webpage without the need to reload the page. Advances in CSS allow browsers to display a responsive website layouts and a wide array of visual effects. Cookies allow browsers to remember your settings for specific websites.

While web browser technology has come a long way since Netscape, browser compatibility issues remain a problem. Since browsers use different rendering engines, websites may not appear the same across multiple browsers. In some cases, a website may work fine in one browser, but not function properly in another. Therefore, it is smart to install multiple browsers on your computer so you can use

an alternate browser if necessary.
Updated: February 28, 2014

Cite this definition:

APAMLAChicagoHTMLLink

TechTerms - The Tech Terms Computer Dictionary

This page contains a technical definition of Web Browser. It explains in computing terminology what Web Browser means and is one of many software terms in the TechTerms dictionary.

All definitions on the TechTerms website are written to be technically accurate but also easy to understand. If you find this Web Browser definition to be helpful, you can reference it using the citation links above. If you think a term should be updated or added to the TechTerms dictionary, please email TechTerms!

Subscribe to the TechTerms Newsletter to get featured terms and quizzes right in your inbox. You can choose to receive either a daily or weekly email.

Q.11. What is a search engine? Give example.

Ans. What is a search engine?

A search engine is a web-based tool that enables users to locate information on the World Wide Web. Popular examples of search engines are Google, Yahoo!, and MSN Search. Search engines utilize automated software applications (referred to as robots, bots, or spiders) that travel along the Web, following links from page to page, site to site. The information gathered by the spiders is used to create a searchable index of the Web.

cHow do search engines work?

Every search engine uses different complex mathematical formulas to generate search results. The results for a specific query are then displayed on the SERP. Search engine algorithms take the key elements of a web page, including the page title, content and keyword density, and come up with a ranking for where to place the results on the pages. Each search engine's algorithm is unique, so a top ranking on Yahoo! does not guarantee a prominent ranking on Google, and vice versa. To make things more complicated, the algorithms used by search engines are not only closely guarded secrets, they are also constantly undergoing modification and revision. This means that the criteria to best optimize a site with must be surmised through observation, as well as trial and error — and not just once, but continuously.

Gimmicks less reputable SEO firms tout as the answer to better site rankings may work at best for only a short period before the search engine's developers become wise to the tactics and change their algorithm. More likely, sites using these tricks will be labeled as spam by the search engines and their rankings will plummet.

Search engines only "see" the text on web pages, and use the underlying HTML structure to determine relevance. Large photos, or dynamic Flash animation mean nothing to search engines, but the actual text on your pages does. It is difficult to build a Flash site that is as friendly to search engines; as a result, Flash sites will tend not to rank as high as sites developed with well coded HTML and CSS (Cascading Style Sheets — a complex mechanism for adding styles to website pages above and beyond regular HTML). If the terms you want to be found by do not appear in the text of your website, it will be very difficult for your website to yield high placement in the SERPs.

Q.12

What is the Internet & WWW? What are the uses of internet in our daily life?

Ans 1. Uses of the Internet in Education

The Internet is a great platform for students to learn throughout their lifetime. They can use the internet to learn new things and even acquire degrees through online education programs. Teachers can also use the internet to teach students around the world.

2. Internet Use to Speed Up Daily Tasks

The Internet is very much useful in our daily routine tasks. For example, it helps us to see our notifications and emails. Apart from this, people can use the internet for money transfers, shopping order online food, etc.

3. Use of the Internet for Shopping

With the help of the internet, anybody can order products online. The increase in online shopping has also resulted in companies offering a huge discount for their customers.

4. Internet for Research & Development

The Internet plays a pivotal role in research and development as it is propelled through internet research. The benefit of the internet is enjoyed by small businessmen to big universities.

5.Business Promotion and Innovation

The Internet is also used to sell products by using various e-Commerce solutions. The result is new services and businesses starting every day thereby creating job opportunities and reducing unemployment.

6.Communication

Without a doubt, the internet is the most powerful medium of communication at present. It connects people across different parts of the world free and fast.

7. Digital Transactions

The internet facilitates internet banking, mobile banking, and e-wallets. Since all digital transactions are stored in a database, it helps the government to track income tax details or income reports in the ITR.

8. Money Management

The internet can also be used to manage money. Now, there are many websites, applications, and other tools that help us in daily transactions, transfers, management, budget, etc.

9. Tour & Travel

During tour and travel, the use of the internet is highly effective as it serves as a guide. People browse the internet before they start visiting the places. Tour bookings can also be done using the internet.

The influence of the internet in our daily life is huge. It has opened us a magical world of information and we would have never seen the world as it is without the internet. Considering its scope and importance, it would be hard to imagine a world without the internet.

Q.13 What is an Internet Service Provider? Give some example of ISP in India.

Ans.13 The following table shows the top 10 ISPs in India by total subscriber base as of 31 March 2020. Broadband is defined as "an always-on Internet connection with download speed of 512 kbit/s or above." The number of internet users is 743.19 million, out of which 55.75 million are narrow band subscribers and 687.44 million are broadband subscribers.[2]

Rank	ISP	Narrowband	Broadband	Total
1	Reliance Jio	0	388,390,116	388,390,116
2	Airtel	27,111,012	148,569,937	175,680,949
3	Vodafone Idea	22,019,406	117,451,416	139,470,822
4	BSNL	6,400,380	24,507,496	30,907,876
5	ACT Fibernet	0	1,607,015	1,607,015
6	APSFL	0	970,270	970,270

Rank	ISP	Narrowband	Broadband	Total
7	MTNL	170,697	855,744	1,026,441
8	Excitel	0	1,350,783	1,350,783
9	Hathway	0	969,157	969,157
10	You Broadband	14,660	778,584	793,244
11	GTPL Broadband	0	359,347	359,347

Note:

1. On 28 February 2018 Aircel filed for bankruptcy at NCLT and a substantial number of customers have migrated to other services due to closing down of most of the consumer services.[3][4]
2. The services of Telenor India has been merged with Airtel on 14 May 2018.[5]
3. On 31 August 2018, Vodafone India has been merged with Idea Cellular and renamed as Vodafone Idea Limited.[6]

Other notable ISPs[edit]

ISP	Coverage area
RailTel Corporation of India	State-owned ISP with pan-India optic fiber network along Railway track

Q.14 Discuss the difference between MAC address, IP address and Port address.

Ans. Both MAC Address and IP Address are used to uniquely defines a device on the internet. NIC Card’s Manufacturer provides the MAC Address, on the other hand Internet Service Provider provides IP Address.

The main difference between MAC and IP address is that, MAC Address is used to ensure the physical address of computer. It uniquely identifies the devices on a network. While IP address are used to uniquely identifies the connection of network with that device take part in a network.

Let’s see the difference between MAC Address and IP Address:

S.NO	MAC Address	IP Address
1.	MAC Address stands for Media Access Control Address.	IP Address stands for Internet Protocol Address.
2.	MAC Address is a six byte hexadecimal address.	IP Address is either four byte (IPv4) or eight byte (IPv6) address.
3.	A device attached with MAC Address can retrieve by ARP protocol.	A device attached with IP Address can retrieve by RARP protocol.
4.	NIC Card’s Manufacturer provides the MAC Address.	Internet Service Provider provides IP Address.
5.	MAC Address is used to ensure the physical address of computer.	IP Address is the logical address of the computer.
6.	MAC Address operates in the data link layer.	IP Address operates in the network layer.
7.	MAC Address helps in simply identifying the device.	IP Address identifies the connection of the device on the network.
8.	MAC Address of computer cannot be changed with time and environment.	IP Address modifies with the time and environment.
9.	MAC Address can’t be found easily by third party.	IP Address can be found by third party.

favorite_border**Like**0

Nextlast_page
Layers of OSI Model

RECOMMENDED ARTICLES

Page :
1

Q.15 How do we view my Internet browser's history?

Ans.15 Today, all major browsers have functionality that allows you to quickly and easily view your Internet browser's history. However, as multiple devices contain browser history, there are multiple ways to view as well. To proceed, choose your devices from the section below and follow the instructions.

- Desktop or laptop computer.
- Android phone or tablet running Google Chrome.
- iPhone or iPad running Safari.

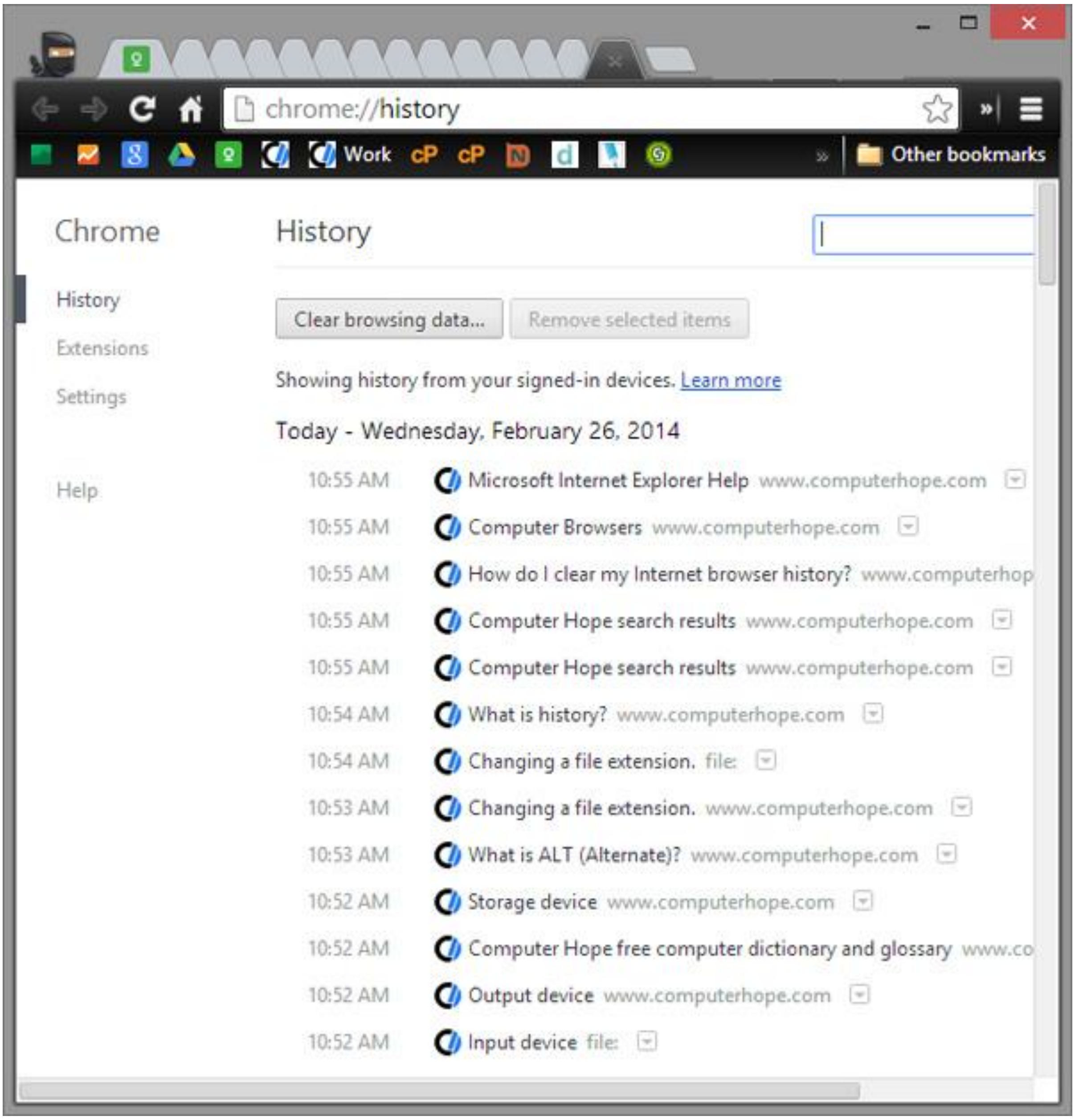
Desktop or laptop computer

If you are using Windows, Linux, or macOS, there are quick shortcut key combinations that allow you to view your history.

Windows and Linux users: Ctrl+H

Apple users: Command + Shift + H

Once one of the above shortcut keys is pressed, a history section similar to the example below should appear. In the following screenshot, browsing history is being viewed in Google Chrome.



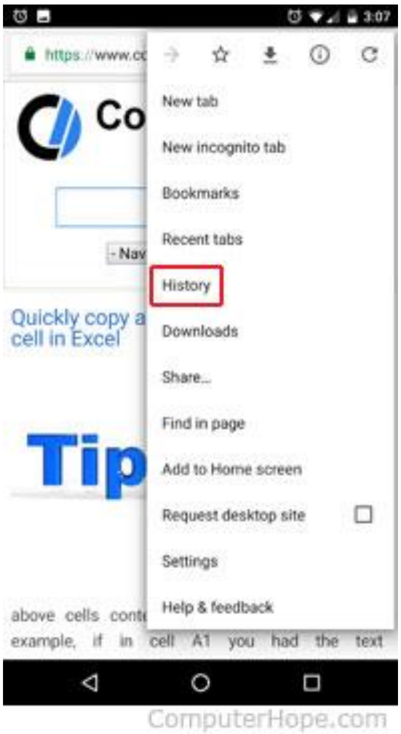
History

Showing history from your signed-in devices. Learn more

Today - Wednesday, February 26, 2014

10:55 AM Microsoft Internet Explorer Help www.computerhope.com
10:55 AM Computer Browsers www.computerhope.com
10:55 AM How do I clear my Internet browser history? www.computerhop
10:55 AM Computer Hope search results www.computerhope.com
10:55 AM Computer Hope search results www.computerhope.com
10:54 AM What is history? www.computerhope.com
10:54 AM Changing a file extension. file:
10:53 AM Changing a file extension. www.computerhope.com
10:53 AM What is ALT (Alternate)? www.computerhope.com
10:52 AM Storage device www.computerhope.com
10:52 AM Computer Hope free computer dictionary and glossary www.co
10:52 AM Output device www.computerhope.com
10:52 AM Input device file:

Android phone or tablet running Google Chrome



Users who are running Google Chrome on their Android phone or tablet can view their history with the following steps.

1. Open the Google Chrome Internet browser.
2. In the upper-right corner of the screen **tap the** ⋮ **icon**.
3. In the drop-down menu that appears, select **history** and shown in the image.
4. The following page contains your device's history.

iPhone or iPad running Safari

Users who are running Safari for iOS on their iPhone or iPad can view their history with the following steps.

1. On your device, open the Safari Internet browser.