CCA-102: Data Communications

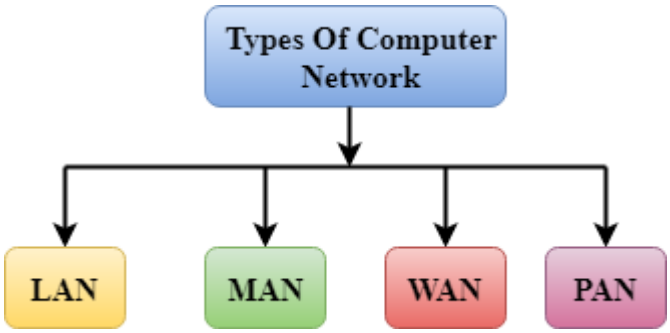
ASSIGNMENT

1. What are the different types of networks?

Ans. *Computer Network Types*

A computer network is a group of computers linked to each other that enables the computer to communicate with another computer and share their resources, data, and applications.

A computer network can be categorized by their size. A **computer network** is mainly of **four types**:



- LAN(Local Area Network)
- PAN(Personal Area Network)
- MAN(Metropolitan Area Network)
- WAN(Wide Area Network)

LAN(Local Area Network)

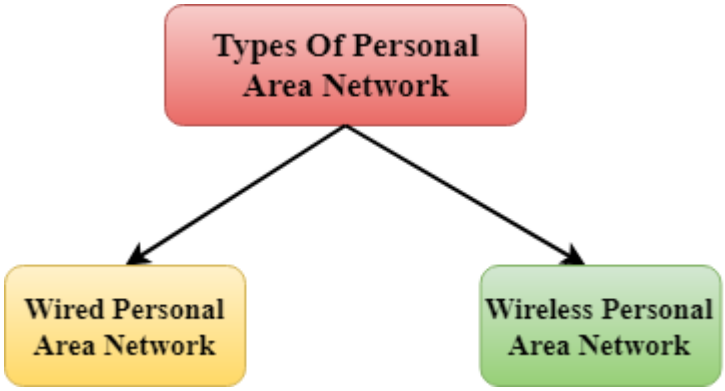
- Local Area Network is a group of computers connected to each other in a small area such as building, office.
- LAN is used for connecting two or more personal computers through a communication medium such as twisted pair, coaxial cable, etc.
- It is less costly as it is built with inexpensive hardware such as hubs, network adapters, and ethernet cables.
- The data is transferred at an extremely faster rate in Local Area Network.

- Local Area Network provides higher security.

PAN(Personal Area Network)

- Personal Area Network is a network arranged within an individual person, typically within a range of 10 meters.
- Personal Area Network is used for connecting the computer devices of personal use is known as Personal Area Network.
- **Thomas Zimmerman** was the first research scientist to bring the idea of the Personal Area Network.
- Personal Area Network covers an area of **30 feet**.
- Personal computer devices that are used to develop the personal area network are the laptop, mobile phones, media player and play stations.

There are two types of Personal Area Network:



- Wired Personal Area Network
- Wireless Personal Area Network

Wireless Personal Area Network: Wireless Personal Area Network is developed by simply using wireless technologies such as WiFi, Bluetooth. It is a low range network.

Wired Personal Area Network: Wired Personal Area Network is created by using the USB.

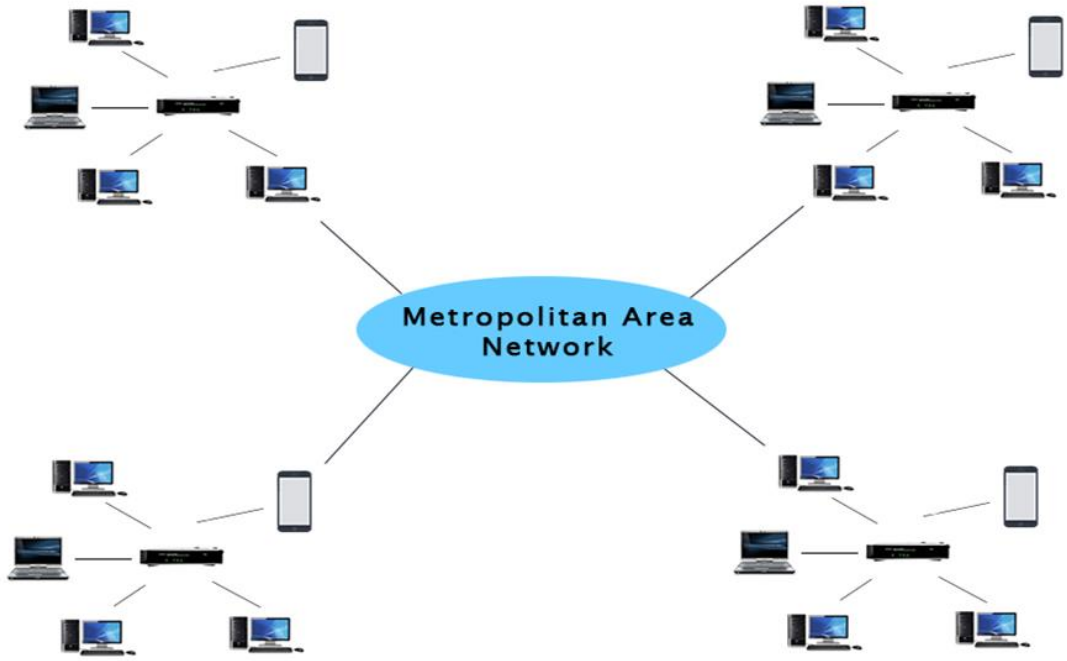
Examples Of Personal Area Network:

- **Body Area Network:** Body Area Network is a network that moves with a person. **For example**, a mobile network moves with a person. Suppose a person establishes a network connection and then creates a connection with another device to share the information.

- **Offline Network:** An offline network can be created inside the home, so it is also known as a **home network**. A home network is designed to integrate the devices such as printers, computer, television but they are not connected to the internet.
- **Small Home Office:** It is used to connect a variety of devices to the internet and to a corporate network using a VPN

MAN(Metropolitan Area Network)

- A metropolitan area network is a network that covers a larger geographic area by interconnecting a different LAN to form a larger network.
- Government agencies use MAN to connect to the citizens and private industries.
- In MAN, various LANs are connected to each other through a telephone exchange line.
- The most widely used protocols in MAN are RS-232, Frame Relay, ATM, ISDN, OC-3, ADSL, etc.
- It has a higher range than Local Area Network(LAN).

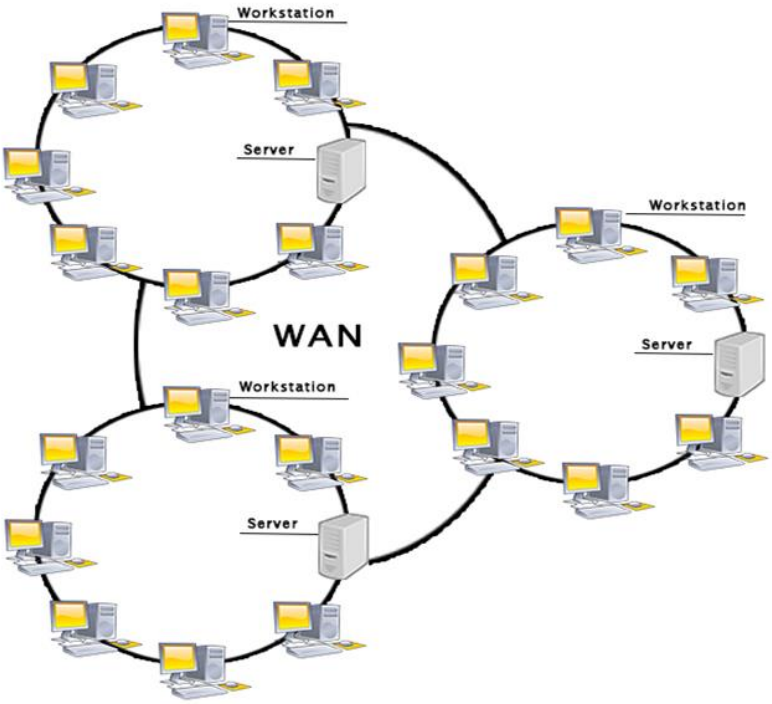


Uses Of Metropolitan Area Network:

- MAN is used in communication between the banks in a city.
- It can be used in an Airline Reservation.
- It can be used in a college within a city.
- It can also be used for communication in the military.

WAN(Wide Area Network)

- A Wide Area Network is a network that extends over a large geographical area such as states or countries.
- A Wide Area Network is quite bigger network than the LAN.
- A Wide Area Network is not limited to a single location, but it spans over a large geographical area through a telephone line, fibre optic cable or satellite links.
- The internet is one of the biggest WAN in the world.
- A Wide Area Network is widely used in the field of Business, government, and education.



Examples Of Wide Area Network:

- **Mobile Broadband:** A 4G network is widely used across a region or country.

- **Last mile:** A telecom company is used to provide the internet services to the customers in hundreds of cities by connecting their home with fiber.
- **Private network:** A bank provides a private network that connects the 44 offices. This network is made by using the telephone leased line provided by the telecom company.

Advantages Of Wide Area Network:

Following are the advantages of the Wide Area Network:

- **Geographical area:** A Wide Area Network provides a large geographical area. Suppose if the branch of our office is in a different city then we can connect with them through WAN. The internet provides a leased line through which we can connect with another branch.
- **Centralized data:** In case of WAN network, data is centralized. Therefore, we do not need to buy the emails, files or back up servers.
- **Get updated files:** Software companies work on the live server. Therefore, the programmers get the updated files within seconds.
- **Exchange messages:** In a WAN network, messages are transmitted fast. The web application like Facebook, Whatsapp, Skype allows you to communicate with friends.
- **Sharing of software and resources:** In WAN network, we can share the software and other resources like a hard drive, RAM.
- **Global business:** We can do the business over the internet globally.
- **High bandwidth:** If we use the leased lines for our company then this gives the high bandwidth. The high bandwidth increases the data transfer rate which in turn increases the productivity of our company.

Disadvantages of Wide Area Network:

The following are the disadvantages of the Wide Area Network:

- **Security issue:** A WAN network has more security issues as compared to LAN and MAN network as all the technologies are combined together that creates the security problem.
- **Needs Firewall & antivirus software:** The data is transferred on the internet which can be changed or hacked by the hackers, so the firewall

needs to be used. Some people can inject the virus in our system so antivirus is needed to protect from such a virus.

- **High Setup cost:** An installation cost of the WAN network is high as it involves the purchasing of routers, switches.
- **Troubleshooting problems:** It covers a large area so fixing the problem is difficult.

Internetwork

- An internetwork is defined as two or more computer network LANs or WAN or computer network segments are connected using devices, and they are configured by a local addressing scheme. This process is known as **internetworking**.
- An interconnection between public, private, commercial, industrial, or government computer networks can also be defined as **internetworking**.
- An internetworking uses the **internet protocol**.
- The reference model used for internetworking is **Open System Interconnection(OSI)**.

Types Of Internetwork:

1. **Extranet:** An extranet is a communication network based on the internet protocol such as **Transmission Control protocol** and **internet protocol**. It is used for information sharing. The access to the extranet is restricted to only those users who have login credentials. An extranet is the lowest level of internetworking. It can be categorized as **MAN**, **WAN** or other computer networks. An extranet cannot have a single **LAN**, atleast it must have one connection to the external network.

2. **Intranet:** An intranet is a private network based on the internet protocol such as **Transmission Control protocol** and **internet protocol**. An intranet belongs to an organization which is only accessible by the **organization's employee** or members. The main aim of the intranet is to share the information and resources among the organization employees. An intranet provides the facility to work in groups and for teleconferences.

Intranet advantages:

- **Communication:** It provides a cheap and easy communication. An employee of the organization can communicate with another employee through email, chat.

- **Time-saving:** Information on the intranet is shared in real time, so it is time-saving.
- **Collaboration:** Collaboration is one of the most important advantage of the intranet. The information is distributed among the employees of the organization and can only be accessed by the authorized user.
- **Platform independency:** It is a neutral architecture as the computer can be connected to another device with different architecture.
- **Cost effective:** People can see the data and documents by using the browser and distributes the duplicate copies over the intranet. This leads to a reduction in the cost.

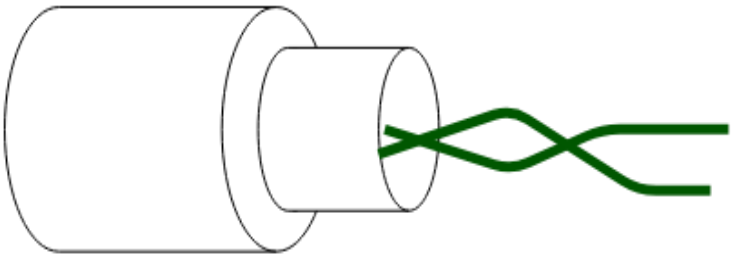
2. Explain the Shielded twisted pair (STP) and Unshielded twisted pair(UTP)

Ans. ***DIFFERENCE BETWEEN UNSHIELDED TWISTED PAIR (UTP) AND SHIELDED TWISTED PAIR (STP) CABLES***

UTP:
UTP is the type of twisted pair cable. It stands for Unshielded twisted pair. Both Data and voice both are transmitted through UTP because its frequency range is suitable. In UTP grounding cable is not necessary also in UTP much more maintenance are not needed therefore it is cost effective.

Unshielded Twisted Pair

STP:
STP is also the type of twisted pair which stands for Shielded twisted pair. In STP grounding cable is required but in UTP grounding cable is not required. in Shielded Twisted Pair (STP) much more maintenance are needed therefore it is costlier than Unshielded Twisted Pair (UTP).



Shielded Twisted Pair

Difference between Unshielded Twisted Pair (UTP) and Shielded Twisted Pair (STP) cables:

S.NO	UTP	STP
1.	UTP stands for Unshielded twisted pair.	STP stands for Shielded twisted pair.
2.	In UTP grounding cable is not necessary.	While in STP grounding cable is required.
3.	Data rate in UTP is slow compared to STP.	Data rate in STP is high.
4.	The cost of UTP is less.	While STP is costlier than UTP.
5.	In UTP much more maintenance are not needed.	While in STP much more maintenance are needed.
6.	In UTP noise is high compared to STP.	While in STP noise is less.
7.	In UTP the generation of crosstalk is also high compared to STP.	While in STP generation of crosstalk is also less.
8.	In UTP, attenuation is high in comparison to STP.	While in STP attenuation is low.

Attention reader! Don’t stop learning now. Get hold of all the important CS Theory concepts for SDE interviews with the **CS Theory Course** at a student-friendly price and become industry ready.

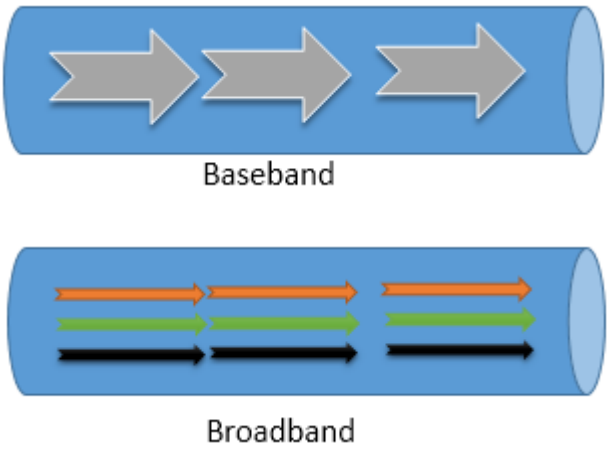
3. What is difference between baseband and broadband transmission?

Ans. *Differences between Baseband and Broadband Explained*

This tutorial explains the differences between the baseband and broadband transmissions in detail. Learn what the baseband and broadband transmissions are and how they differ from each other.

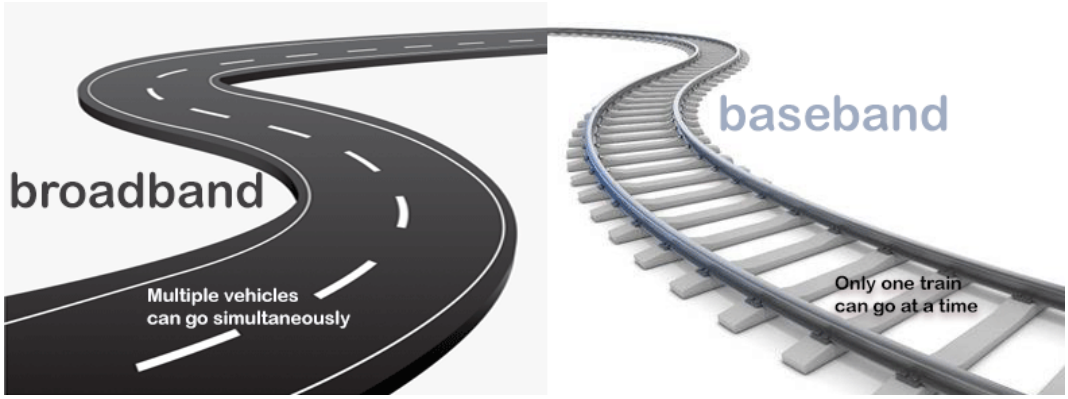
Both baseband and broadband describe how data is transmitted between two nodes. Baseband technology transmits a single data signal/stream/channel at a time while broadband technology transmits multiple data signals/streams/channels simultaneously at the same time.

The following image shows an example of both technologies.



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.

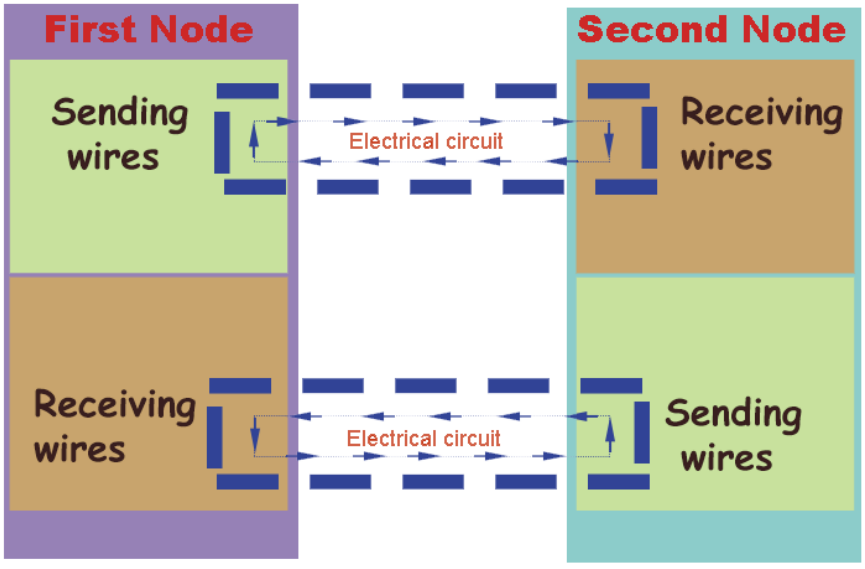


Technical differences between the baseband and broadband transmissions

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

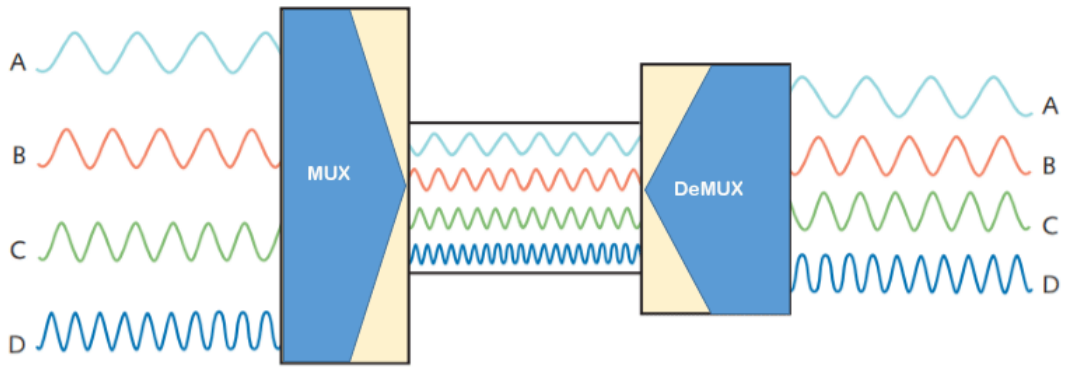
Baseband technology is mainly used in Ethernet networks to exchange data between nodes. This technology can be used on all three popular cable media types of Ethernet; coaxial, twisted-pair, fiber-optic.

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.



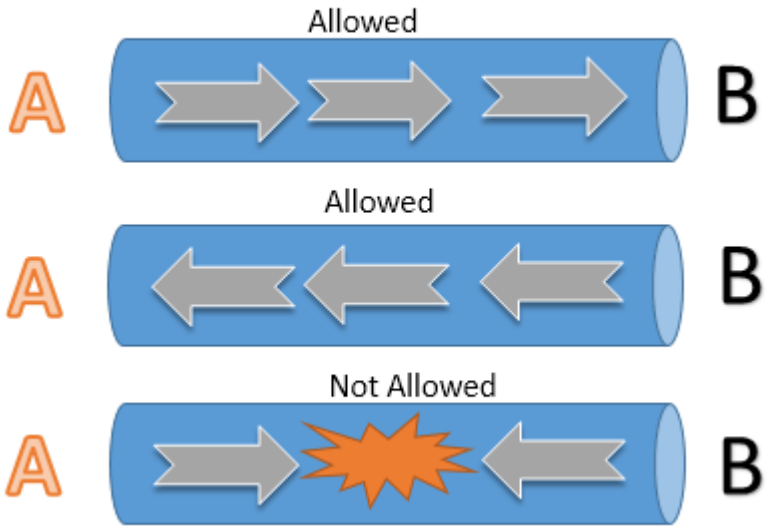
Analog signals can be regenerated using amplifiers in order to travel longer distances.

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 a
Can transmit only a single data stream at a time	Can transmit multiple signal w
Support bidirectional communication simultaneously	Support unidirectional commu
Support TDM based multiplexing	Support FDM based multiplexi
Use coaxial, twisted-pair, and fiber-optic cables	Use radio waves, coaxial cable
Mainly used in Ethernet LAN networks	Mainly used in cable and tele

That's all for this tutorial. If you like this tutorial, please don't forget to share it with friends through your favorite social network.

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

Ans.

Device	What is does
Modem:	Stands for "modulating-demodulating": modems are hardware devices that allow a computer or another device, such as a router or switch, to connect to the Internet. They convert or "modulate" an analog signal from a telephone or cable wire to digital data (1s and 0s) that a computer can recognize. Simply send traffic from point A to piont B without further manipulation.
Routers:	Are responsible for sending data from one network to another. Work at Layer 3 (Network) of the OSI model, which deals with IP addresses. Typically, routers today will perform the functionality of both a router and a switch - that is, the router will have multiple ethernet ports that devices can plug into.
Switches:	They use the MAC address of a device to send data only to the port the destination device is plugged into. Work at Layer 2 (Data Link) of the OSI model, which deals with MAC addresses.
Hubs:	Unlike switches, hubs broadcast data to all ports, which is inefficient, so hubs are basically a multiport repeaters.

Note: it is also useful to know the following terms:

- Default gateway - a piece of software usually located on a router, a firewall, a server, etc, that enables traffic to flow in and out of the network. Gateways act as a junction between multiple networks.

- DHCP (Dynamic Host Configuration Protocol) - a protocol that automatically provides and assigns IP addresses, default gateways, DNS servers and other network parameters to client devices. Most routers/switches have the ability to provide DHCP server support.

  In case you have several devices on your network that support DHCP, you need to make sure that only one of them is configured with DHCP. Having several devices with DHCP enabled will lead to a DHCP Race Condition - also known as Conflicting DHCP Servers.
  Note: modern voice system will require your network to have a router in it. Despite the fact that some modems have integrated router features, they barely capable of maintaining voice systems functionality. You may want to have both modem and router in your network (modem will need to be launched in bridged mode).

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

Ans. 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.

6. *When troubleshooting computer network problems, what common hardware-related problems can occur?*

Ans. **Basic Network Troubleshooting Steps And Tools**

Last Updated:January 18, 2021

An Extensive Study of Network Troubleshooting with the Tools used.
We explored all about **Network Security along with its types** in our previous tutorial. When we run a network or while working in any system there are always chances of failure in the smooth operation owing to technical, physical or any other faults.

For uninterrupted running of the system, we need to resolve the raised issues as soon as possible and for this, we need to detect the cause of the problem first and then fix it.

***Must Read* => Beginner's Guide to Networking**
Thus the process of detection, minimization and resolving the faults that arise in the network while performing the various day to day activities is known as troubleshooting.

Here we will explore the different kinds of troubleshooting steps and the tools we use for fault detection and closure of the same.

Network Troubleshooting

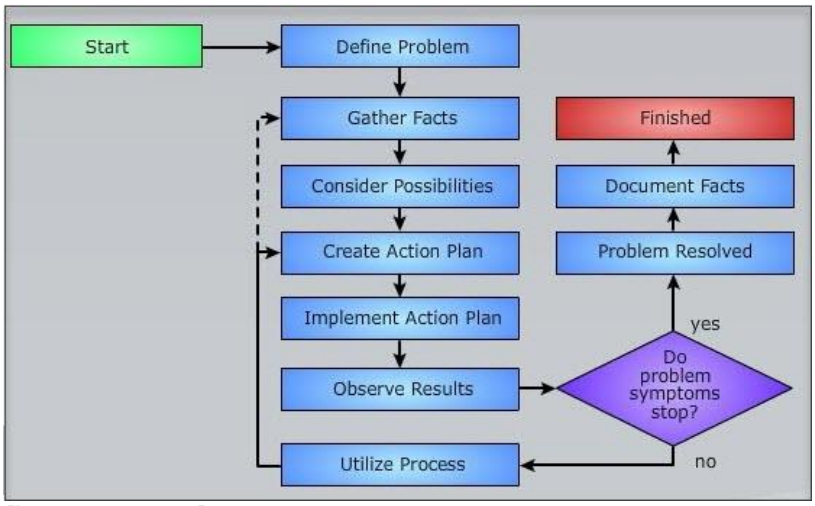
In this tutorial, we are only concerned about the computer networking fault diagnosis and rectification.

Based on the type of issue, we will discuss its troubleshooting steps and tips.

Basic Network Problems

- **Cable Problem**: The cable which is used to connect two devices can get faulty, shortened or can be physically damaged.
- **Connectivity Problem**: The port or interface on which the device is connected or configured can be physically down or faulty due to which the source host will not be able to communicate with the destination host.
- **Configuration Issue**: Due to a wrong configuration, looping the IP, routing problem and other configuration issues, network fault may arise and the services will get affected.
- **Software Issue**: Owing to software compatibility issues and version mismatch, the transmission of IP data packets between the source and destination is interrupted.
- **Traffic overload:** If the link is over utilized then the capacity or traffic on a device is more than the carrying capacity of it and due to overload condition the device will start behaving abnormally.
- **Network IP issue:** Due to improper configuration of IP addresses and subnet mask and routing IP to the next hop, the source will not be able to reach the destination IP through the network.

Network Troubleshooting Flowchart



[image source]

Network Troubleshooting Tools

There are various tools that are used for checking the IP reachability issues and to locate where the packet is lost while communicating with the destination host. These tools make troubleshooting easier and minimize the time for restoration.

Some of the popular tools are mentioned below:

#1) SolarWinds Engineer's Toolset

SolarWinds provides a network software, Engineer's Toolset that contains over 60 tools.

With the help of these tools, you will be able to automate network discovery. For automated network discovery, it has a set of tools like Port Scanner, Switch Port Mapper, SNMP sweep, IP Network Browser, etc.

This software has powerful diagnostic capabilities. It will perform real-time monitoring and alerting. It provides the features of IP address & DHCP scope monitoring, Configuration & log management, and enhanced network security.

Engineer's Toolset can be integrated with SolarWinds Network Performance Monitor. The tool will help you to perform network stress tests with WAN Killer. According to your specifications, it will generate random traffic and will allow you to adjust packet size, bandwidth, and percentage of bandwidth.

SolarWinds offers a fully functional free trial for 14 days. Per seat license of Engineer's Toolset will cost you $1495.

#2) Obkio

Obkio is a simple network performance monitoring solution that provides real-time, end-to-end performance monitoring to help you assess the health of network and core business applications to quickly identify intermittent network problems within minutes!

Obkio's software application is designed for monitoring network performance and web applications and identifies the causes of common network problems like VoIP, video, and application slowdown.

Deploy Network performance monitoring Agents at strategic locations in your company's offices or network destinations to easily identify the source of a system failure so you can quickly apply the corrective measures.

Obkio alerts you as soon as a problem occurs or even if there are signs that a failure is about to happen. Not only does it alert you and pinpoint the source of the issue, but it also allows you to go back in time to complete a diagnosis.

#3) Ping

By using IP ICMP echo request and echo reply messages, the PING tool verifies the reachability to the destination host at the remote end.

It contains two messages, first is, if the data packet is competent to send and receive the messages from the destination IP address and the second is the RTT time for the process (RTT means round trip time and is calculated in milliseconds).

```
CiscoRtr1>ping 10.3.1.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 10.3.1.6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
```

The exclamation shows that ping is successful. If the ping returns saying the destination is unreachable then there are many reasons for this. To find out the cause, we will go for the next tool.

#4) Trace Route

It sends the ICMP echo request messages with a step by step increase in the IP TTL (time to live) values.

The starting value is 1. It sends the data packet in a forward direction and each hop decreases the TTL value by 1 while routing the data and rejects the packet whose TTL value is zero by responding that the message ICMP time has exceeded.

Now again the source host sends the data packet, but this time with a TTL value of 2. In this way, the process will keep going until the packet has arrived at the destination and then the destination host reverts with ICMP echo reply messages.

With the help of traceroute, the router will keep a record of which route is followed by the packets to reach the destination and calculates the latency and other parameters as well.

#5) Protocol Analyzer

It is an advanced tool for finding out the network issues.

It is the software that intercepts and records the data packet flow between the source and the destination. Like, if the system is running slow then it can check for the latency issues and other networking problems which will help in diagnosing the root cause.

Steps Involved In Network Diagnostics

Here steps to troubleshoot and diagnose various network problems like IP, connectivity, wireless connection, etc.

Troubleshooting IP Problems

In the TCP/IP protocol suite, if we are not able to reach at the destination IP address and not able to find the route to reach the next hop at any point in the network, then we will use PING and TRACEROUTE tools for troubleshooting the cause and location of the issue.

The generic steps to troubleshoot the IP related issues in the network include:

- Firstly locate the pair of devices between the source and the destination host between which the connectivity issue has occurred.
- Once you locate the devices using the tools, the fault can be due to a physical connectivity issue. Thus check the physical connections all over the path.
- There can be a fault in the LAN connectivity as well if you are working in a LAN network. So check the LAN connections. The local port can be faulty or down due to which the source cannot be able to reach the destination IP.
- One of the reasons of the fault can be the router connectivity issue while traveling through various paths to reach the destination. Hence check that if the router is defined properly at each of the intermediate hops.
- Check the configuration settings.

Troubleshooting Local Connectivity Issues

Once on the broad level, if you find that there is an issue in the LAN connectivity, then in order to locate the root cause and to resolve it, you should follow the below steps:

- If the destination and the source are of the identical subnet mask, then try to ping the destination IP.

- Else, if the destination is of some other subnet mask then try to ping the gateway IP address of the router.
- Now, if both the ping fails, then first check that in the configuration settings, if both the subnet mask and route to be followed to reach the destination are defined properly in the routing table or not?
- Once you are done with the configuration part and found everything OK, then check if your source host is able to ping some another hop in the LAN network other than the destination host or route to that?
- If you are not able to ping to another device then there can be many reasons for this. It may even be a configuration issue, a physical connectivity issue, and repetitive IP address entry issue.

Correcting the Repetitive IP address Entry Issue

For rectifying the duplicate entry of an IP issue, disconnect the doubtful device from the LAN and also make the interface on which the device was connected shut down.

Now ping the device from some another device of the same subnet or LAN network. If the ping is OK, then it indicates that the IP is being used by some other device as well on the network. From the ARP table of the device, find out its MAC address and modify the IP address according to planning.

But if the problem persists still, then there will be a physical connectivity or configuration issue in it.

Troubleshooting Physical Connectivity Issues

The list of faults that come under this category are:

1. Improper connection of cables
2. Router, switch or hub port is faulty or down.
3. Traffic overload on the link or particular interface.
4. Configuration issue at layer-1.

Let's take a look at the above in detail.

#1) Checking Cable connectivity Issue: The cables are used for connections, based on the type of connectivity. Like, for connectivity between a router and a computer the crossover pair of the cable is used. Thus make sure that the suggested and suitable cable is used to make a physical connection between any two devices**.**
If connections are found ok, then maybe the cable is faulty, so check the connectivity by replacing the existing cable with a newer one. Still, if the problem persists, then check the port or interface on which the link is terminated. There is a possibility for the port to be faulty.

#2) Port Faulty Scenario: Check that the port or interface on which the link is established is not shut down. Verify the duplex mode and speed as well. If the port is up and still the problem persists, then there are indicator lights that are present on each of the device to show the running status of the port.
From the indicator lights, check if the port is physically radiating or down. If the port is physically malfunctioning then it will appear by light status. In this situation, configure the link on some other free port or interface.

#3) Traffic overload: If there is more traffic than the carrying capacity at a link or interface then at some point it will start behaving abnormally. Thus verify these criteria to ensure smooth running.
#4) Configuration Issue: Check the router configuration on the interface by show ip interface and show running-config commands.

Troubleshooting Routing Problems

When we route the data packets in the network, then the chances for occurrences of fault are usual. Thus depending on the type of fault, we will prepare our plan for resolving the faults.

The kind of fault that occurs between the source and destination hosts while floating data packets in a network are listed below:

- The route is not defined in the router between the source and destination.
- A wrong Routing protocol is used to find out the route to the next hop or destination.
- Software related fault at the router.
- Any filter or firewall may be barring the entry of data packets to the destination node.
- There may be configuration faults that arise at the source router end.

How to proceed for resolution:

- To find out the resolution, the first step is to locate the hop between the source and the destination where the problem has occurred.
- The process verifies the IP connectivity and routing protocols connectivity at each hop starting from the source host towards the destination one.
- We can also use the traceroute tool to locate the hop where the problem has arised. But this is not helpful in all the cases. Hence, it is better if we proceed with the first one.
- Once we locate the problematic hop, then login to that router via telnet and then try to ping the source and destination host.
- If the ping is not successful, then verify the routing table for routes between the source and destination. If routes are not defined then configure the IP routes with the subnet mask and default route in the router.
- In condition, if the ping responses with only a few percentages of success, then there may be multiple paths that are defined to reach the destination. But out of multiple paths, one is failing to reach the destination. The cause for this is that a routing loop can occur in the path. To rectify this, trace the looping hop, and correct the configuration.
- After rectification of the above steps, if still, the problem persists, then check the routing protocol used, and change the protocol in accordance with the network.
- The configuration issues at a particular router can be checked using a command like show ip interface for interface related faults, show ip access-group for finding out ant firewall or filter is configured in the network and you can check what is allowed to pass through it, show version for uptime and show running-config for the overall configuration.

Troubleshooting Upper-layer Faults

After checking the physical connectivity, Local connectivity, IP connectivity, and Routing issues, if you are still not finding a resolution for the fault, then there is a possibility for the fault to be the in transport and application layer protocol.

A fault can arise due to the following reasons:

- The data connection is down.

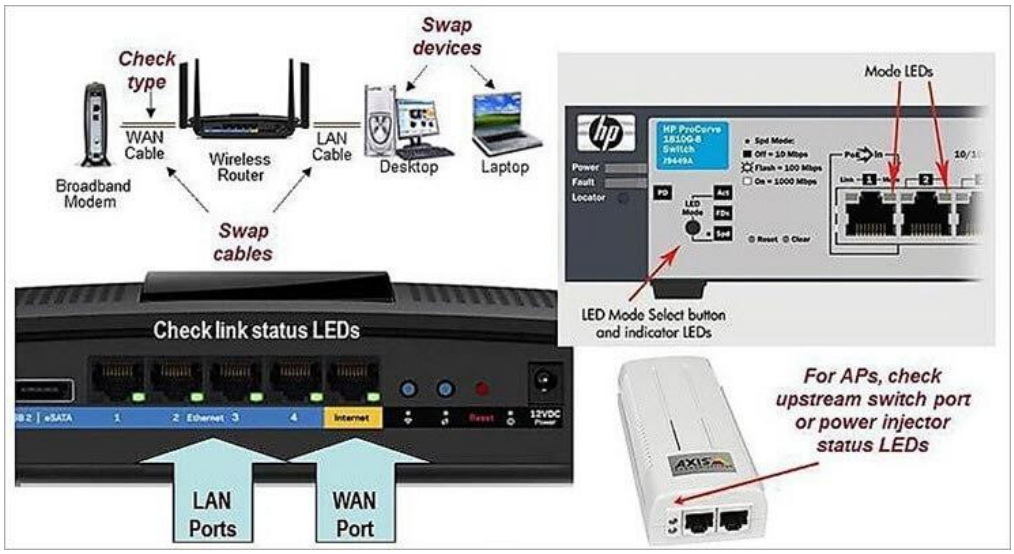
- A packet filter or firewall is blocking the incoming or outgoing traffic.
- Particular service on the server is down.
- There can be an authentication and access issue between the client and the server host.
- Software incompatibility or version mismatch issues between the source and the destination host.

Depending upon the category of fault, we take the rectification steps.

- In the condition of firewall barring the traffic to flow through the network, we look out for a way to move the source host in the network in such a way in which the firewalls can be avoided or bypassed.
- For service down issues, take measures to make it up, or align another server to deliver the service.
- For the authentication process issue, we can deploy checks with the help of the software where the authentication is failing, and then based on the results you can rectify the issue.
- For version mismatch and compatibility issue, upgrade your system so that both will be compatible with each other.

Troubleshooting Wireless Network Connection Issue

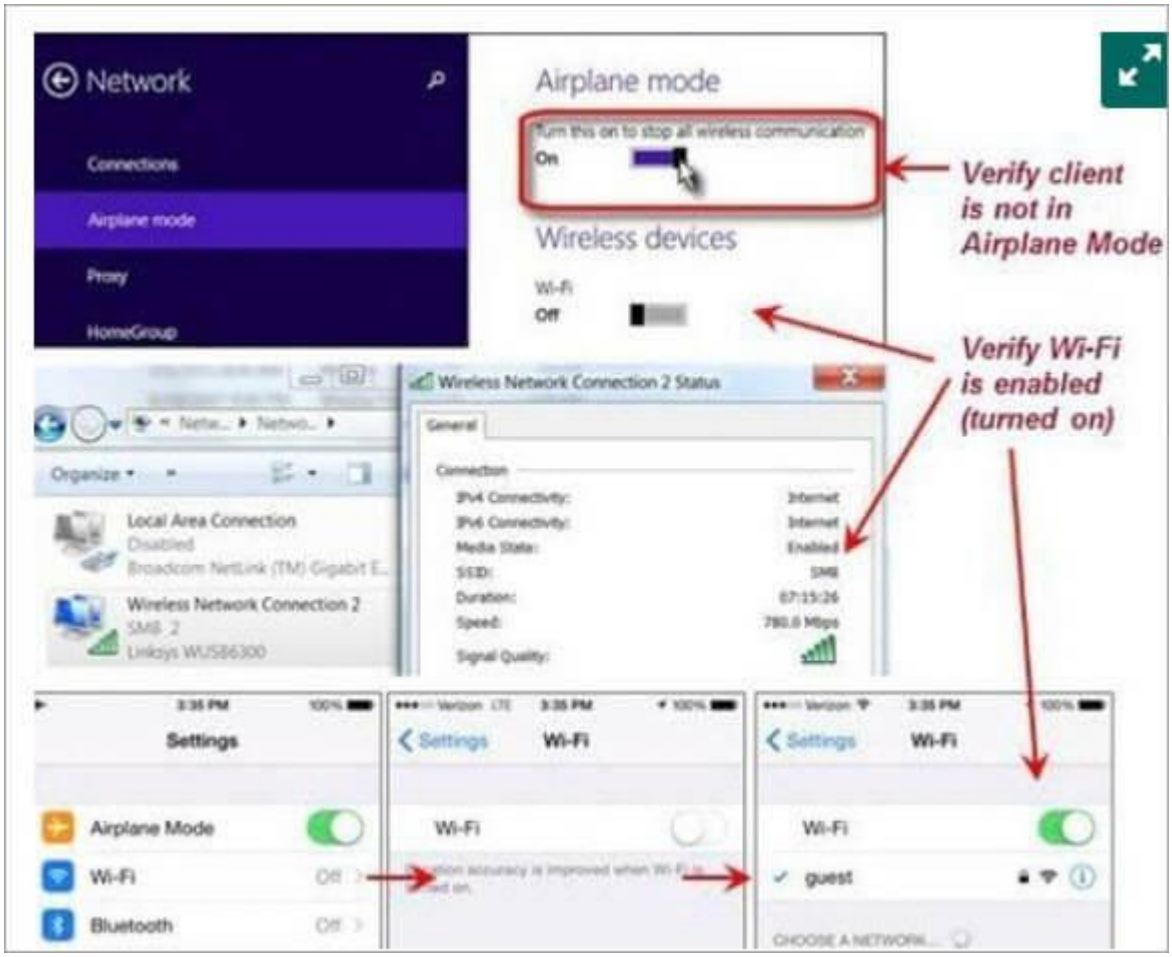
#1) Whenever you connect your Tablet, mobile phone or Laptop with the WI-FI device, and if you are not able to connect then check all the LAN or WAN cable connections. The Ethernet cable should be connected tightly and check the light status on the device. If it is not green then the cable or port may be faulty. Thus change the port and cable connections with a newer one.



#2) After verification of all of the above points, if the connection is still not through, then verify the WI-FI network adaptor settings.
For windows laptop or PC, go to control panel, select the network connections option and check what is the status on the wireless network adaptor? It should be enabled. If it is not enabled then click on the enable key and mark the status as enabled.

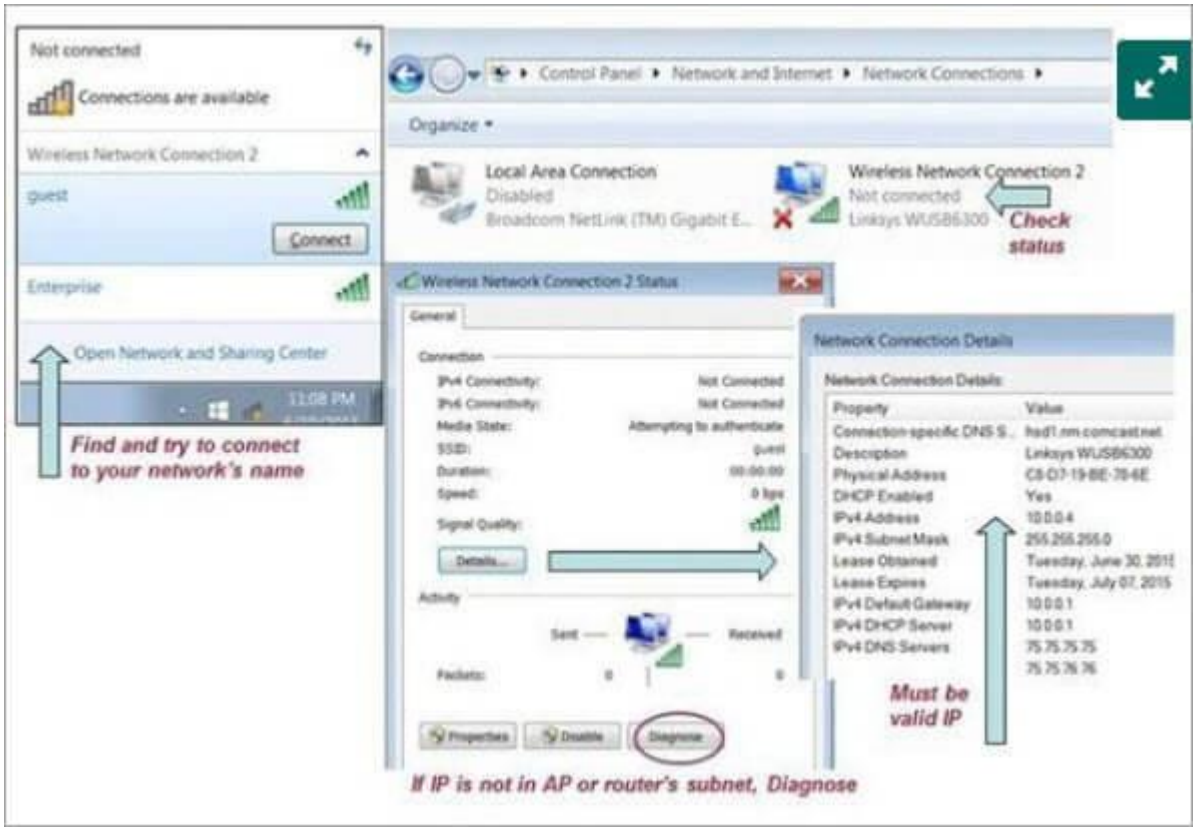
Also, check if the airplane mode on a laptop or PC is disabled. If it is enabled, then it will not allow connecting with a wireless network.

Network Adaptor Settings



#3) After checking all the above settings, if the status is still not connected then check the wireless access point and SSID settings. After correction of the desired settings, the status will change from not connected to acquiring network address to connected. At this point, the client also allocates the IP address to the requesting device.

Network Connection Settings



#4) If still, the problem persists, then click on the diagnose option from the wireless network connection status menu to find out the cause.
#5) After performing all the above troubleshooting steps, if you are not able to connect to the network still, then there may be other reasons like some firewall or packet filter is barring you for using the network, and there could be a problem with the authentication protocol used etc.
#6) To resolve these issues, reconfigure all the network settings and verify the IP reachability by using PING.
These are the basic troubleshooting steps. If you are still not able to connect to the network, then you can restart your system and then try to connect and consult with some network settings expert.

Tips For Network Troubleshooting

Some Tips include:

- Always use a high-level password to protect your network devices such as routers, switches and database servers as they store crucial data within themselves.
- Don't share your router login user ID and password with anyone in the organization or outside the organization.
- Properly log-out from the system once your job is done.
- Keep verifying your configuration **by show running-config command.**
- For assigning IP addresses and subnet mask to the devices for a network, always perform the IP planning first and then make a diagram of the connectivity of devices that you are using in the network.
- It is better if you use the routers or servers in the master-slave mode so that in the worst case if one goes down then the other will take up the load and your network will be kept alive.
- Avoid overloading your device with high traffic.

Conclusion

The different kinds of fault categories that we counter within the networking systems is explained here in this tutorial.

We came to know that an issue can occur from the bottom layer to the top layer of the TCP/IP model and can be due to a physical connectivity issue, LAN issue, IP related issue or any routing related faults.

Based on the category of the issue, we take measures to locate and rectify them. Only the generic and basic troubleshooting steps of the networking system are explained. As it is a very vast topic, several other kinds of faults and newer faults can arise in any network at any time.

But as a beginner, it is important to understand the above-defined troubleshooting steps for ruling out the issue at the ground level.

7**. In a network that contains two servers and twenty workstations, where is the best place to install an Anti-virus program?**

Ans

In a network that contains two servers and twenty workstations, where is the best place to install an anti-virus program? When troubleshooting computer network problems, what common hardware-related problems can occur?

You need AT LEAST three levels of security.

1. A good firewall. This can stop intrusions, malware, unauthorized access, etc. before they reach the workstations.
2. Antivirus software on the servers and at the endpoint workstations. This software should be centrally managed to keep end users updated constantly and to minimize user meddling with the settings. Good antivirus will also protect email clients.
3. Educated and aware users who: do not casually install downloaded programs; don't click on unknown links; don't fall for phishing emails, etc. Establish a strong password policy for all users. You should consider not giving your users Administrative rights on their accounts. They will complain that they cannot install what they need and your workload will increase but, I guarantee you, your entire environment will be more reliable and secure.

Remember: your computing environment is only as secure as your weakest link and non-compliant user.

There is no one simple answer on where to start to troubleshooting network problems. You have to know several things:

1. The first thing I try to find out is if the problem affects one user, a group of users or all users.
2. Is the problem connecting to internal resources or external (internet).

Problems can be physical as in a bad connection; configuration as in ip issues; or software issues.

A good method for troubleshooting is to “divide and conquer”. By that I mean, you go halfway back in your network and see if the problem exists there, then go forward or back halfway and check again.

In order to troubleshoot your network you should have a detailed network map, list of devices, IP address assignments. And remember, you don't know it all: keep a list of associates, help resources and manufacturer references close at hand and don't be afraid to ask for help. We IT folks usually love to help each other because we can all learn something new.

ANTI-VIRUS PROGRAM

Viruses and malware can cripple your computer and destroy your files. Antivirus programs are designed to find and intercept viruses before they do any harm. An antivirus program is essential on a Windows PC, and can be very useful for Mac and Linux users as well. Check out this guide for whichever operating system you use.

Method 1

Windows

1

Understand the need for an antivirus program. Windows is the most virus-prone operating system (OS) out of the three major OSes. It has the most users and the weakest built-in security. Antivirus programs will defend your computer from malware that comes through email, flash drives, downloads, websites and more.

2

Acquire an antivirus program. There are several popular free options available that do a good job of protecting the average user. These programs are updated frequently with new virus definitions that recognize the latest threats.[1]

- If you frequently deal with files or websites that are virus-infected, you may want to opt for more powerful paid protection. Paid antivirus programs are typically available for a yearly subscription fee.
- When downloading free or paid antivirus programs, ensure that you are downloading from a trusted source. There are many programs out there that claim to be antivirus/antimalware but instead install malware themselves. Read reviews and download products from companies that have been around for a long time.[2]
- Windows 10 and 8 have Windows Defender, which is a free anti-malware application provided by Microsoft. It's already built-in.

3

Install the antivirus program. Make sure that no other programs are running while you install the antivirus. You will most likely need to be connected to the internet to download additional files and updates.

- Some free antivirus programs come packaged with toolbars for your web browser. These can add protection but also change your search options and bog down older computers. You have the opportunity to opt out of these changes during the installation process.

4

Update the program. After the installation is complete, reboot your computer and update the program. The file that you downloaded is likely not the most up to date version, so you will need to connect to your antivirus program's servers and download the latest updates. Most antivirus programs allow you to right-click on the icon in the System Tray while it is running and click Update.

- Update your definitions on a weekly basis. Most antivirus programs are set to automatically update. Double check the settings for your program to ensure that you are receiving the necessary updates.

5

Scan your computer. Once you have the program installed and updated, it's time to scan your computer. This could take several hours, depending on the number of files being scanned and your computer's speed.

6

Set a scan schedule. Antivirus programs are most effective when they are automated. Open your antivirus program's settings and look for the Schedule option. Try to schedule a time when your computer will be on but you won't be using it. Ideally you should be scanning once a week; scan more frequently if you deal with potentially infected files on a regular basis.

7

Keep Windows updated. The best way to keep your computer protected is to always make sure that your copy of Windows is up to date. Microsoft releases security updates for Windows on a regular basis, fixing exploitable areas of Windows.

Method 2

Mac OS X

1

Understand the need for an antivirus program. Mac OS X has long been much more secure than Windows, due to the way that the system software has been designed. In the past, less people used Mac OS, which lead to fewer viruses being developed for Mac. While the population of Mac users has increased dramatically, it is still not as popular as Windows, which is where the majority of virus development happens.

- The most important use for antivirus on Mac is stopping the spread of malware to other computers. Viruses are very easily spread through email, and while you may not get infected yourself, you can spread the virus to other computers that may not have the same protection as your Mac.

2

Acquire an antivirus program. Because of the low chance of infection on your machine, there is little need to get a paid antivirus solution. Instead, download a free option that is designed from the ground up to work with Mac OS X.[3]

3

Install and run the antivirus software. Because the risk of infection is low, you don't necessarily need to constantly scan your system. Instead, use your antivirus program to manually inspect suspicious files and emails.

4

Update Mac OS X. Apple releases security patches on a regular basis to close any exploits that have been discovered. Keep your Mac up to date to ensure that your system is as secure as possible.

Method 3

Linux

1

Understand the need for an antivirus program. Out of the three major OSes, Linux is the most secure when it comes to viruses. This is due to both the low population of users as well as the inherent security of the system software. Because applications are installed directly from the distribution, there is little chance of files being infected.

- The most important use for antivirus on Linux is stopping the spread of malware to other computers. Viruses are very easily spread through email, and while you may not get infected yourself, you can spread the virus to other computers that may not have the same protection as your Linux machine.

2

Acquire an antivirus program. Check with your repository to see what antivirus options are available for your Linux build. Most builds have antivirus programs available as freeware. These programs have been vetted by the Linux community and are designed to take minimal system resources.

3

Install and run the antivirus software. Because the risk of infection is low, you don't necessarily need to constantly scan your system. Instead, use your antivirus program to manually inspect suspicious files and emails.

4

Update your Linux build. Updating system software with Linux updates all of your program builds as well, eradicating any exploits that have been found. The process is mostly automated. Be sure to check your settings to ensure that your Linux installation is updating appropriately.

8. Define Static IP and Dynamic IP? Discuss the difference between IPV4 and IPV6.

Ans. ***Pv4 vs IPv6: What's the Difference?***

What is IP?

An Internet Protocol address is also known as IP address. It is a numerical label which assigned to each device connected to a computer network which uses the IP for communication.

IP address act as an identifier for a specific machine on a particular network. The IP address is also called IP number and internet address. IP address specifies the technical format of the addressing and packets scheme. Most networks combine IP with a TCP (Transmission Control Protocol). It also allows developing a virtual connection between a destination and a source.

What is IPv4?

IPv4 was the first version of IP. It was deployed for production in the ARPANET in 1983. Today it is most widely used IP version. It is used to identify devices on a network using an addressing system.

The IPv4 uses a 32-bit address scheme allowing to store 2^32 addresses which is more than 4 billion addresses. Till date, it is considered the primary Internet Protocol and carries 94% of Internet traffic.

What is IPv6?

It is the most recent version of the Internet Protocol. Internet Engineer Taskforce initiated it in early 1994. The design and development of that suite is now called IPv6.

This new IP address version is being deployed to fulfill the need for more Internet addresses. It was aimed to resolve issues which are associated with IPv4. With 128-bit address space, it allows 340 undecillion unique address space. IPv6 also called IPng (Internet Protocol next generation).

KEY DIFFERENCE

- IPv4 is 32-Bit IP address whereas IPv6 is a 128-Bit IP address.
- IPv4 is a numeric addressing method whereas IPv6 is an alphanumeric addressing method.
- IPv4 binary bits are separated by a dot(.) whereas IPv6 binary bits are separated by a colon(:).
- IPv4 offers 12 header fields whereas IPv6 offers 8 header fields.
- IPv4 supports broadcast whereas IPv6 doesn't support broadcast.
- IPv4 has checksum fields while IPv6 doesn't have checksum fields
- IPv4 supports VLSM (Virtual Length Subnet Mask) whereas IPv6 doesn't support VLSM.
- IPv4 uses ARP (Address Resolution Protocol) to map to MAC address whereas IPv6 uses NDP (Neighbour Discovery Protocol) to map to MAC address.

Features of IPv4

- Connectionless Protocol
- Allow creating a simple virtual communication layer over diversified devices
- It requires less memory, and ease of remembering addresses
- Already supported protocol by millions of devices
- Offers video libraries and conferences

Features of IPv6

- Hierarchical addressing and routing infrastructure
- Stateful and Stateless configuration
- Support for quality of service (QoS)
- An ideal protocol for neighboring node interaction

Difference Between IPv4 and IPv6 Addresses

IPv4 & IPv6 are both IP addresses that are binary numbers. IPv4 is 32 bit binary number while IPv6 is 128 bit binary number address. IPv4 address are separated by periods while IPv6 address are separated by colons.

Both are used to identify machines connected to a network. In principle, they are the same, but they are different in how they work.

Basis for differences	**IPv4**	**IPv6**
Size of IP address	IPv4 is a 32-Bit IP Address.	IPv6 is 128 Bit I P Address.
Addressing metho d	IPv4 is a numeric address, and its binary bits are separated by a dot (.)	IPv6 is an alpha numeric address whose binary bit s are separated b y a colon (:). It a lso contains hexa decimal.
Number of header fields	12	8
Length of header f iled	20	40
Checksum	Has checksum fields	Does not have c hecksum fields
Example	12.244.233.165	2001:0db8:0000: 0000:0000:ff00: 0042:7879
Type of Addresses	Unicast, broadcast, and multicast.	Unicast, multica st, and anycast.
Number of classes	IPv4 offers five different classes of IP Address. Class A to E.	lPv6 allows stori ng an unlimited number of IP Ad dress.
Configuration	You have to configure a newly installed system before it c an communicate with other systems.	In IPv6, the conf iguration is optio nal, depending u pon on functions needed.
VLSM support	IPv4 support VLSM (Virtual Length Subnet Mask).	IPv6 does not of

Basis for differences	IPv4	IPv6
		fer support for V LSM.
Fragmentation	Fragmentation is done by sending and forwarding routes.	Fragmentation is done by the send er.
Routing Informati on Protocol (RIP)	RIP is a routing protocol supported by the routed daemon.	RIP does not sup port IPv6. It uses static routes.
Network Configur ation	Networks need to be configured either manually or with D HCP. IPv4 had several overlays to handle Internet growth, which require more maintenance efforts.	IPv6 support aut oconfiguration c apabilities.
Best feature	Widespread use of NAT (Network address translation) dev ices which allows single NAT address can mask thousands of non-routable addresses, making end-to-end integrity ac hievable.	It allows direct a ddressing becaus e of vast address Space.
Address Mask	Use for the designated network from host portion.	Not used.
SNMP	SNMP is a protocol used for system management.	SNMP does not support IPv6.
Mobility & Intero perability	Relatively constrained network topologies to which move restrict mobility and interoperability capabilities.	IPv6 provides int eroperability and mobility capabili ties which are e mbedded in netw ork devices.
Security	Security is dependent on applications - IPv4 was not desig ned with security in mind.	IPSec(Internet P rotocol Security) is built into the I Pv6 protocol, us able with a prop er key infrastruct ure.
Packet size	Packet size 576 bytes required, fragmentation optional	1208 bytes requi red without frag mentation
Packet fragmentati on	Allows from routers and sending host	Sending hosts on ly
Packet header	Does not identify packet flow for QoS handling which incl udes checksum options.	Packet head cont ains Flow Label field that specifi es packet flow fo r QoS handling
DNS records	Address (A) records, maps hostnames	Address (AAAA) records, maps h ostnames
Address configura tion	Manual or via DHCP	Stateless address autoconfiguratio

Basis for differences	IPv4	IPv6
		n using Internet Control Message Protocol version 6 (ICMPv6) or DHCPv6
IP to MAC resolution	Broadcast ARP	Multicast Neighbour Solicitation
Local subnet Group management	Internet Group Management Protocol GMP)	Multicast Listener Discovery (MLD)
Optional Fields	Has Optional Fields	Does not have optional fields. But Extension headers are available.
IPSec	Internet Protocol Security (IPSec) concerning network security is optional	Internet Protocol Security (IPSec) Concerning network security is mandatory
Dynamic host configuration Server	Clients have approach DHCS (Dynamic Host Configuration server) whenever they want to connect to a network.	A Client does not have to approach any such server as they are given permanent addresses.
Mapping	Uses ARP(Address Resolution Protocol) to map to MAC address	Uses NDP(Neighbour Discovery Protocol) to map to MAC address
Combability with mobile devices	IPv4 address uses the dot-decimal notation. That's why it is not suitable for mobile networks.	IPv6 address is represented in hexadecimal, colon - separated notation. IPv6 is better suited to mobile networks.

IPv4 and IPv6 cannot communicate with other but can exist together on the same network. This is known as **Dual Stack.**

9. Discuss TCP/IP model in detail.

Ans. Introduction to the TCP/IP Model

The TCP/IP model is a part of the Internet Protocol Suite. This model acts as a communication protocol for computer networks and connects hosts on the Internet. It is a concise version of the OSI Model and comprises four layers in its structure.

This concept of TCP/IP is not just important for people in the computer or IT fields but also is an essential part of the Computer Knowledge syllabus, included in major competitive exams.

Before, diving deep into the different aspects of the structure, refer to the table below and know about some basic and introductory features of the model:

Basics of TCP/IP Model	
Full-Form	Transmission Control Protocol/ Internet Protocol
Developed By	Department of Defence (DoD), United States
Developed in	During the 1970s
Year for acknowledgement as a standard protocol by ARPANET	1983
Function of TCP	Collecting and Reassembling Data Packets
Function of IP	Sending the Data Packets to the correct destination
Number of Layers in TCP/IP Model	4 layers

In this article, we shall discuss in detail the different layers of the TCP/IP model along with their functions. Also, a few sample questions based on this topic have been given further below for the reference of Government exam aspirants.

To study in detail about what is a Computer Network and its different types, candidates can visit the linked article.

Interested in learning more about Computer-related terms, applications, and software?? Strengthen your Computer Awareness with the help of links given below:

- **Microsoft Windows**
- **High Level Computer Languages**
- **Input and Output Devices**
- **Web Browsers**
- **Database Management System (DBMS)**
- **Introduction to Operating System**

History and Development of TCP/IP Model

This protocol is a result of the research and development by the Defense Advanced Research Projects Agency (DARPA) during the 1960s. Given below are a few points which had played an important role in the advancement of the TCP/IP model:

- A two-network TCP/IP communications test was conducted between Stanford and University College London in 1975
- An important thing which resulted in promoting this model was when the US Department of Defense declared TCP/IP as the standard for all military computer networking. This was In March 1982
- In 1983, this structured protocol was adopted by ARPANET as a standard protocol
- Later on other Computer and IT companies including IBM, DEC, etc. had also adapted the TCP/IP model as their standard communication protocol
- In 1989, the University of California has accepted the TCP/IP code for public domain

Gradually, this Internet protocol suite or the TCP/IP model was accepted across the globe as a comprehensive framework for computer networking and Internet communication.

The TCP/IP model is considered to be similar to the Open Systems Interconnection Model. However, the framework and the structuring of the two was completely different and Transmission Control Protocol/ Internet Protocol was released prior to the OSI Model. For a detailed difference between the two, candidates can visit the Difference Between TCP/IP and OSI Model page.

Links to a few other fundamental topics and concepts have been given below for people to learn and understand one of the most complex, yet essential devices, which is the Computer:

Computer Abbreviations	Components of Computer
Computer Virus	Important Computer-related Terms
Microsoft Windows	Microsoft Office

Layers of the TCP/IP Model

Unlike the OSI model which comprises seven layers, the TCP/IP model is structured with four different layers. These four layers are:

1. Network Access Layer
2. Internet Layer
3. Host to Host Layer
4. Application Layer

Now, let us discuss each of these four layers in detail along with their functions as a part of the protocol architecture.

1. Network Access Layer

- This is the bottom-most layer of the TCP/IP model architecture
- It is a combination of the Data Link and Physical Layer of the OSI model
- The physical transmission of data takes place at this layer
- Once the frames are transmitted by a network, encapsulating the IP datagram into these frames is done in this layer
- Also, the mapping of IP address into physical address is done here
- Mainly, the function of this layer is to transmit the data between two devices, connected in a network

2. Internet Layer

- It is the second layer of the TCP/IP model and this layer is parallel to the Network Layer of the OSI Model, in terms of the structure
- Sending the data packets to their destination network is the main function of the Internet layer
- The logical transmission of data takes place at this level
- There are three different protocols used in this layer. These include:
    - **IP:** One of the most important protocols as it detects the IP address of a device which is later used for internetwork connections. It is using this protocol that the path with which the data shall be transmitted is decided. There are two common IP versions which are used, To know the difference between IPv4 and IPv6, visit the linked article.
    - **ARP:** It stands for Address Resolution Protocol. The physical address from the IP address can be determined using ARP.
    - **ICMP:** It stands for Internet Control Message Protocol and notification regarding datagram problems can be sent back to the user using this. Any issue with the network is immediately notified to the user by ICMP. It can only inform the user about the errors and cannot rectify the problem

3. Host-To-Host Layer

- This layer is parallel to the transport layer of the OSI Model
- The error-free delivery of data is the main function of this layer
- There are two main protocols present in this layer:
    - **TCP:** Another integral part, the Transmission Control Protocol is a reliable communication protocol. It manager the flow of data, i.e. the sequence and segmentation of the data
    - **UDP:** It is a connection-free protocol which makes it cost-effective but less reliable.

4. Application Layer

- The topic three layers of the OSI Model: Application, Presentation and Sessions, when combined together, they perform similar functions as the Application Layer of the TCP/IP model
- node-to-node communication based on the user-interface occurs here
- Multiple protocols are present in this layer, a few common ones have been mentioned below in brief:
    - **HTTP:** Hypertext Transfer Protocol is used to manage the communication between the server and web browsers
    - **NTP:** Network Time Protocol can set one standard time source in our computer, which enables sync between the server and the user
    - **TELNET:** Telecommunication Network is used to have access to files present of the Telnet network and manage them on internet
    - **FTP:** File Transfer Protocol, as the name suggests allows easy transferring of files

Other protocols of Application layer include Network File System (NFS), Secure Shell (SSH), Simple Mail Transfer Protocol (SMTP), Trivial File Transfer Protocol (TFTP), etc.

Other Related Articles	
Difference Between Search Engine and Web Browser	Difference Between WWW and Internet
Difference Between MS Excel and MS Word	Difference Between Firewall and Antivirus
Difference Between Virus and Worm	Difference Between Firewall and Antivirus

Sample Questions – TCP/IP Model

Since questions from this topic are asked in the Computer Awareness section of the major Government exams, candidates must be well prepared for the concept from the exam perspective as well.

Thus, to assistant candidates with their preparation, given below are a few sample questions based on the TCP/IP model, in the format of the multiple-choice questions, as asked in the final exam.

Candidates who are looking for study material and preparation strategy for the upcoming exams, they can refer to the links given below and start their preparation now:

Free Online Mock Test Series with Solutions	Previous Year Government Exam Question Papers with Solutions
Preparation Strategy for Competitive Exams	Free Online Govt Exam Quiz
Bank PO Question Papers and Answers	Fundamentals of Computer

Q 1. Which of the following is not a type of protocol under the Application Layer of the TCP/IP model?

1. IP
2. TCP
3. HTTP
4. FTP
5. TELNET

Answer: (1) IP

Solution: IP or Internet Protocol is a type of protocol in the Internet Layer of the TCP/IP model

Q 2. How many layers are there in the Transmission Control Protocol/ Internet Protocol (TCP/IP) model?

1. Six
2. Seven
3. Five
4. Four
5. Nine

Answer: (4) Four

Q 3. Which of the following is not a layer of the TCP/IP model?

1. Application
2. Host to Host
3. Internet
4. Network Access
5. Physical

Answer: (5) Physical Layer

Q 4. Data Link Layer and Physical Layer of the OSI Model combine together to _____ layer of the TCP/IP model.

1. Network Access
2. Internet
3. Host to Host
4. Application
5. None of the above

Answer: (1) Network Access

Q 5. The TCP/IP model was also known as the _____ model.

1. PoP
2. DoD
3. FoF
4. NoN
5. SoS

Answer: (2) DoD

Solutions: It was known as the DoD model based on the Department of Defense which helped in its development

Q 6. _____ is another name for an IP packet.

1. Datagram
2. Segment
3. Protocol
4. Department
5. Address

Answer: (1) Datagram

Questions based on similar format and a bit more complex may be asked in the upcoming competitive exams.

Candidates must go through the information given in this article carefully as it will enhance their knowledge as to how a computer network functions and what is the role of such structured models in networking.

For any further exam updates, study material, preparation notes, etc., candidates can turn to BYJU'S and learn from experts.

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

Ans. *What is a Browser?*

A browser is a software program that is used to explore, retrieve, and display the information available on the World Wide Web. This information may be in the form of pictures, web pages, videos, and other files that all are connected via hyperlinks and categorized with the help of URLs (Uniform Resource Identifiers). For example, you are viewing this page by using a browser.

A browser is a client program as it runs on a user computer or mobile device and contacts the webserver for the information requested by the user. The web server sends the data back to the browser that displays the results on internet supported devices. On behalf of the users, the browser sends requests to web servers all over the internet by using HTTP (Hypertext Transfer Protocol). A browser requires a smartphone, computer, or tablet and internet to work.

History of Web Browser

- The **WorldWideWeb** was the first web browser. It was created by W3C Director Tim Berners-Lee in **1990**. Later, it was renamed **Nexus** to avoid confusion caused by the actual World Wide Web.
- The **Lynx** browser was a text-based browser, which was invented in **1992**. It was not able to display the graphical content.

- Although, the first graphical user interface browser was NCSA Mosaic. It was the first most popular browser in the world, which was introduced in **1993**.
- In **1994**, there were some improvements occurred in Mosaic and came to Netscape Navigator.
- In **1995,** Microsoft introduced the **Internet Explorer** It was the first web browser developed by Microsoft.
- A research project started on Opera in **1994**. Later, it was publicly introduced in 1996.
- **Apple's Safari** browser was introduced in **2003**. It was specifically released for Macintosh computers.
- In **2004**, Mozilla introduced **Firefox** as Netscape Navigator.
- In **2007**, a browser **Mobile Safari** was released as Apple mobile web browser.
- The popular browser **Google Chrome** was launched in **2008**.
- The fast-growing mobile-based browser **Opera Mini** was released in **2011**.
- The Microsoft **Edge** browser was launched in **2015**.

Features of Web Browser

Most Web browsers offer common features such as:

1. **Refresh button:** Refresh button allows the website to reload the contents of the web pages. Most of the web browsers store local copies of visited pages to enhance the performance by using a caching mechanism. Sometimes, it stops you from seeing the updated information; in this case, by clicking on the refresh button, you can see the updated information.
2. **Stop button:** It is used to cancel the communication of the web browser with the server and stops loading the page content. For example, if any malicious site enters the browser accidentally, it helps to save from it by clicking on the stop button.
3. **Home button:** It provides users the option to bring up the predefined home page of the website.
4. **Web address bar:** It allows the users to enter a web address in the address bar and visit the website.
5. **Tabbed browsing:** It provides users the option to open multiple websites on a single window. It helps users to read different websites at the same time.

For example, when you search for anything on the browser, it provides you a list of search results for your query. You can open all the results by right-clicking on each link, staying on the same page.

6. **Bookmarks:** It allows the users to select particular website to save it for the later retrieval of information, which is predefined by the users.

What is the URL (Uniform Resource Locator)?

A **uniform resource locator** is the address of a resource on the internet or the World Wide Web. It is also known as a web address or uniform resource identifier (URI). For example, **https: www.javatpoint.com**, which is the URL or web address for the javatpoint website. A URL represents the address of a resource, including the protocol used to access it.

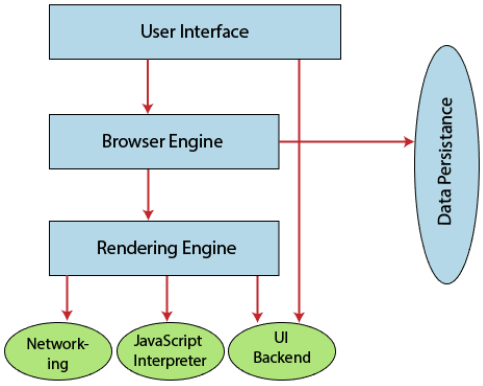
A URL includes the following information:

- It uses the protocol to access the resource.
- It defines the location of a server by IP address or the domain name.
- It includes a fragment identifier, which is optional.
- It contains the location of the resource in the directory of the server.

A URL forwards user to a particular online resource, such as a video, webpage, or other resources. For example, when you search information on Google, the search results display the URL of the relevant resources in response to your search query. The title which appears in the search results is a hyperlink of the URL of the webpage. It is a **Uniform Resource Identifier**, which refers to all kinds of names and addresses of the resources on the webservers. URL's first part is known as a **protocol identifier**, and it specifies the protocol to use, and the second part, which is known as a resource name, represents the IP address or the domain name of a resource. Both parts are differentiated by a colon and two forward slashes like **http://www.javatpoint.com.**

Component of a Web browser

The primary components of a browser are shown in the below image:



1. **User Interface:** The user interface is an area where the user can use several options like address bar, back and forward button, menu, bookmarking, and many other options to interact with the browser.
2. **Browser Engine:** It connects the UI (User Interface) and the rendering engine as a bridge. It queries and manipulates the rendering engine based on inputs from several user interfaces.
3. **Rendering Engine:** It is responsible for displaying the requested content on the browser screen. It translates the HTML, XML files, and images, which are formatted by using the CSS. It generates the layout of the content and displays it on the browser screen. Although it can also display the other types of content by using different types of plugins or extensions. such as:
    - Internet Explorer uses **Trident**
    - Chrome & Opera 15+ use **Blink**
    - Chrome (iPhone) & Safari use **Webkit**
    - Firefox & other Mozilla browsers use **Gecko**
4. **Networking:** It retrieves the URLs by using internet protocols like HTTP or FTP. It is responsible for maintaining all aspects of Internet communication and security. Furthermore, it may be used to cache a retrieved document to reduce network traffic.
5. **JavaScript Interpreter:** As the name suggests, JavaScript Interpreter translates and executes the JavaScript code, which is included in a website. The translated results are sent to the rendering engine to display results on the device screen.
6. **UI Backend:** It is used to draw basic combo boxes and Windows (widgets). It specifies a generic interface, which is not platform-specific.
7. **Data Storage:** The data storage is a persistence layer that is used by the browser to store all sorts of information locally, like cookies. A browser also supports different storage mechanisms such as IndexedDB, WebSQL, localStorage, and FileSystem. It is a database stored on the local drive of your computer where the browser is installed. It handles user data like cache, bookmarks, cookies, and preferences.

How does a browser work?

When a user enters a web address or URL in the search bar like javatpoint.com, the request is passed to a **domain name servers** (DNS). All of these requests are routed via several routers and switches.

The domain name servers hold a list of system names and their corresponding IP addresses. Thus, when you type something in the browser search bar, it gets converted into a number that determines the computers to which the search results are to be displayed.

The browser acts as a part of the client-server model. A browser is a client program that sends the request to the server in response to the user search queries by using Hypertext Transfer Protocol or HTTP. When the server receives the request, it collects information about the requested document and forwards the information back to the browser. Thereafter, the browser translates and displays the information on the user device.

In Brief:

- When a user enters something (like javatpoint.com) in the browser. This request goes to a domain name server.
- The browser sends the user request to the server using an IP address, which is described by the domain name server.
- The domain name server sends an IP address to the web server that hosts the website.
- The server sends the information back to the IP address, which is defined by the browser at the time of the request. The requested page may include links to other files on the same server, like images, for which the browser also requests the server.
- The browser gathers all the information requested by the user, and displays on your device screen in the form of web pages.

List of Internet Browsers

There are various types of internet browsers, which are as follows:

- **Microsoft Edge:** Microsoft Edge is a web browser that comes pre-installed with Windows 10 operating system and Windows Server 2016. It was introduced to replace the Internet Explorer Web browser, and its code name was Spartan. It offers various types of features such as freestyle writing over Web page displays, refined search, and presentations for e-books and other reading resources.
  Microsoft Edge was developed under the **Spartan codename** Project. In April 2015, Microsoft changed the project Spartan name as Microsoft Edge. Although Internet Explorer and Edge are included with Windows 10, Edge act as a default browser. It combines new web technology evaluations and

enhances the speed of browsing.

Although, Internet Explorer 11 was available in Microsoft Windows operating system, Microsoft Edge has become the default browser in Windows 10. It needs at least 1 gigabyte of memory. It offers several types of features, such as annotation features, a new rendering engine, and easy-to-use icons, etc. Furthermore, it also provides better security as compared to Internet Explorer, and it can be combined with Cortana, Microsoft's virtual personal assistant.

Features of Microsoft Edge

- It provides support for Firefox and Chrome add-ons.
- It has the ability to fill the form automatically.
- It can be integrated with Cortana.
- It provides faster page rendering.
- It has more security features and also allows private browsing.
- It is modern, lightweight, and reduces resource consumption.

Latest versions of Edge browser

Platform	Versions	Release Date
Window 10	79.0.309.71	22-01-2020
Window 10 Mobile	40.15254.603	21-01-2020
Xbox One	40.15063.0	30-08-2018

- **Amazon Silk:** Amazon silk is a proprietary Internet browser. It was released for Fire OS devices on 15 November 2011. It is based on the open-source Chromium project and derives most of the features from the Google Chrome browser. It divides the task of loading webpages between Amazon's servers and Fire.

Silk is the default browser on most Amazon hardware devices as well as on app-based Kindle devices, TV, Fire, and compatible Echo devices. Furthermore, it is the first new mass-market, client software delivery mechanism, which should be built from the base of the cloud, not only the web.

How does Silk Work?

Silk browser works through Amazon EC2 (Elastic cloud computing). EC2 acts as the middleman between devices and webpages and simplify them for examined mobile consumption. Then, it includes the whole host of processes like page caching, file compression, and local file storage.

It tries to guess your browsing habits. Accordingly, it predicts the pages that you may like to visit, and then pre-loads those pages in advance. These background processes use lower bandwidth and promote speed of page loading. If EC2 is offline, the silk browser switches to a backup mode where it translates all information on the Kindle Fire itself.

Rendering pages on EC2

When the all contents of a page have been fetched on EC2, it renders the pages for display in the client's browser window. It depends on the amount of load and the client's network conditions.

The components that can be handed off to EC2 to speed up browsing are: HTML, CSS, Networking, JavaScript, Block building, Marshaling, Native OM, etc.

- **Opera:** An Opera web browser was first conceived at Telenor company in 1994, later bought by the Opera Software on 1 April 1995. It was designed for desktop and mobile interfaces, but it is more popular now for mobile phones. It is based on Chromium, and it uses the blink layout engine. An

opera mini was released for smartphones on 10 August 2005 that could run standard web browsers. It can be downloaded from the google play store or Apple play store.

- **Apple Safari:** Safari is an internet browser available for the Macintosh, and Windows operating systems included the iPhone, iPad, and iPod Touch. It was developed by Apple, Inc. on 30 June 2003. It is the default browser for the operating system in its products, such as OS X for the MacBook and Mac computers and iOS for the iPad and iPhone mobile devices. It is at number four in the browser market after Microsoft Internet Explorer, Mozilla Firefox, and Google Chrome. It uses the WebKit engine, which is used for rendering fonts, displays graphics, determining page layout, and running JavaScript.
- **Google Chrome:** Google Chrome is an open-source internet browser. It is developed by Google on 11 December 2008 for Windows, Linux, Mac OS X, Android, and iOS operating systems. **Read more**
- **Mozilla Firefox:** The Mozilla Firefox web browser is developed by the Mozilla Foundation and its subordinate company, Mozilla Corporation. It was first released was beta on 23 September 2002. Although it was released as the Mozilla Browser, it was internally code-named Phoenix. The First version 1.0 of Firefox was introduced on 9 November 2004. **Read more**
- **Internet Explorer:** It is a web browser that is manufactured by Microsoft Corporation, and it is included with the Microsoft Windows operating system. But It was removed in Window 10 in support of Microsoft's new Edge Browser. **Read more**

How to download different type of browsers

Follow below links to download the different browsers:

Google Chrome: https://www.google.com/chrome/

Mozilla Firefox: https://www.mozilla.org/en-US/firefox/

Opera: https://www.opera.com/

Apple Safari: https://support.apple.com/downloads/safari

11. What is a search engine? Give example.

Ans. **search engine** is software accessed on the Internet that searches a database of

information according to the user's query. The engine provides a list of results that best match what the user is trying to find. Today, there are many different search engines available on the Internet, each with its own abilities and features. The first search engine ever developed is considered Archie, which was used to search for FTP files, and the first text-based search engine is considered Veronica. Currently, the most popular and well-known search engine is Google. Other popular search engines include AOL, Ask.com, Baidu, Bing, DuckDuck Go, and Yahoo.

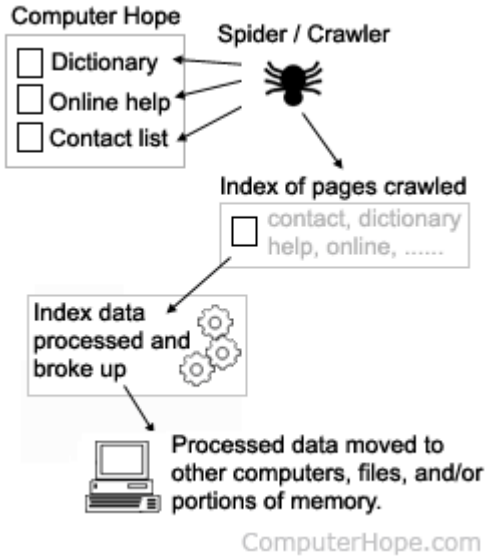
How to access a search engine

For users, a search engine is accessed through a browser on their computer, smartphone, tablet, or another device. Today, most new browsers use an omnibox, which is a text box at the top of the browser. The omnibox allows users to type in a URL or a search query. You can also visit one of the major search engines' home page to perform a search.

- How to find information on the Internet.

How a search engine works

Because large search engines contain millions and sometimes billions of pages, many search engines display the results depending on their importance. This importance is commonly determined by using various algorithms.



As illustrated, the source of all search engine data is collected using a spider or crawler that visits each page on the Internet and collects its information.

Once a page is crawled, the data contained in the page is processed and indexed. Often, this can involve the steps below.

- Strip out stop words.
- Record the remaining words on the page and the frequency they occur.
- Record links to other pages.

- Record information about any images, audio, and embedded media on the page.

The data collected is used to rank each page. These rankings then determine which pages to show in the search results and in what order.

Finally, once the data is processed, it's broken up into files, inserted into a database, or loaded into memory where it's accessed when a search is performed.

Do all search engines give the same results?

Not necessarily. Search engines use proprietary algorithms to index and correlate data, so every search engine has its own approach to finding what you're trying to find. Its results may be based on where you're located, what else you've searched for, and what results were preferred by other users searching for the same thing. Each search engine uniquely weights these and offers you different results.

What is the best search engine?

There isn't one search engine that is better than all the others. Many people could argue that Google's search engine is the best, and it is the most popular and well-known. It's so popular that people often

use it as a verb when telling someone to search for their question.

Microsoft's Bing search engine is also popular and used by many people. Bing does an excellent job of finding information and answering questions. Bing is also what powers the search in Windows 10 and the Yahoo search engine.

Users concerned with privacy, enjoy using Duck Duck Go. This search engine makes its users anonymous and is an excellent solution for users concerned with how much information Google and Bing collect on its users.

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

Ans. ***IMPORTANCE OF INTERNET TECHNOLOGY FOR EASY LIF***

Today, the internet has become unavoidable in our daily life. Appropriate use of the internet makes our life easy, fast and simple. The internet helps us with facts and figures, information and knowledge for personal, social and economic development. There are many uses of the internet, however, the use of the internet in our daily life depends on individual requirements and goals.

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

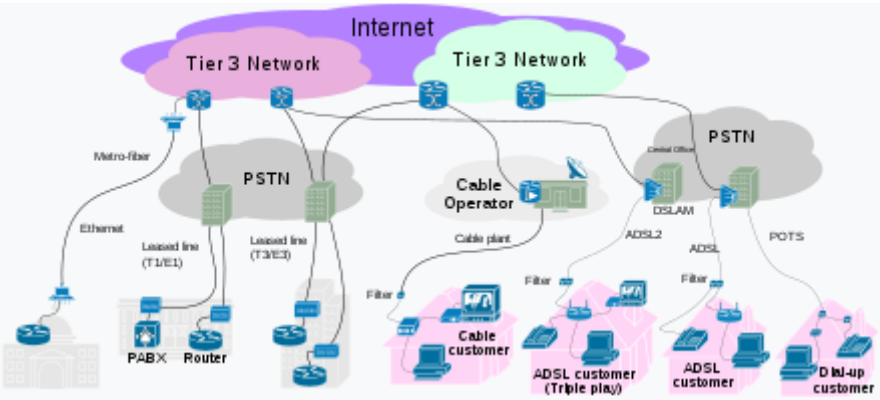
internet. Considering its scope and importance, it would be hard to imagine a world without the internet.

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

Ans. *Internet service provider*

*"ISP" redirects here. For other uses, see **ISP (disambiguation)**.*

*"Internet service" redirects here. It is not to be confused with **Web service**.*



Internet connectivity options from end-user to tier 3/2 ISPs

An **Internet service provider (ISP)** is an organization that provides a myriad of services for accessing, using, or participating in the **Internet.** Internet service providers can be organized in various forms, such as commercial, **community-owned, non-profit**, or otherwise **privately owned.**

Internet services typically provided by ISPs can include Internet access, **Internet transit, domain name** registration, **web hosting, Usenet** service, and **colocation.**

An ISP typically serves as the **access** point or the **gateway t**hat provides a user, access to everything available on the Internet.[1]

Local ISP in Manhattan installing fiber for provisioning Internet access

Contents

History

The Internet (originally **ARPAnet)** was developed as a network between government research laboratories and participating departments of universities. Other companies and organizations joined by direct connection to the **backbone,** or by arrangements through other connected companies, sometimes using dialup tools such as **UUCP.** By the late 1980s, a process was set in place towards public, commercial use of the Internet. Some restrictions were removed by 1991,[2] shortly after the introduction of the **World Wide Web**.[3]

During the 1980s, **online service providers** such as **CompuServe** and **America On** Line (AOL) began to offer limited capabilities to access the Internet, such as e-mail interchange, but full access to the Internet was not readily available to the general public.

In 1989, the first Internet service providers, companies offering the public direct access to the Internet for a monthly fee, were established in Australia[4] and the United States. In Brookline, Massachusetts, **The World** became the first commercial ISP in the US. Its first customer was served in November 1989.[5] These companies generally offered **dial-up** connections, using the public telephone network to provide last-mile connections to their customers. The **barriers to entry** for dial-up ISPs were low and many providers emerged.

However, cable television companies and the telephone carriers already had wired connections to their customers and could offer Internet connections at much higher speeds than dial-up using **broadband** technology such as **cable modems** and digital subscriber line (DSL). As a result, these companies often became the dominant ISPs in their service areas, and what was once a highly competitive ISP market became effectively a monopoly or **duopoly** in countries with a commercial telecommunications market, such as the United States.

In 1995, NSFNET was decommissioned removing the last restrictions on the use of the Internet to carry commercial traffic and **network access points** were created to allow peering arrangements between commercial ISPs.

Net neutrality[

*Main article: **Net neutrality in the United States***

On 23 April 2014, the U.S. **Federal Communications Commission** (FCC) was reported to be considering a new rule permitting ISPs to offer content providers a faster track to send content, thus reversing their earlier **net neutrality** position.[6][7][8] A possible solution to net neutrality concerns may be **municipal broadband**, according to **Professor Susan Crawford,** a legal and technology expert at Harvard **Law School**.[9] On 15 May 2014, the FCC decided to consider two options regarding Internet services: first, permit fast and slow broadband lanes, thereby compromising net neutrality; and second, reclassify broadband as a **telecommunication** service, thereby preserving net neutrality.[10][11] On 10 November 2014, President **Barack Obama** recommended that the FCC reclassify broadband Internet service as a telecommunications service in order to preserve **net neutrality.**[12][13][14] On 16 January 2015, **Republicans** presented legislation, in the form of a **U.S. Congress H.R. discussion draft bill,** that makes concessions to net neutrality but prohibits the FCC from accomplishing the goal or enacting any further regulation affecting Internet service providers.[15][16] On 31 January 2015, **AP News** reported that the FCC will present the notion of applying ("with some caveats") **Title II (common carrier) of the Communications Act of 1934** to the Internet in a vote expected on 26 February 2015.[17][18][19][20][21] Adoption of this notion would reclassify Internet service from one of information to one of the telecommunications[22] and, according to **Tom Wheeler,** chairman of the FCC, ensure net neutrality.[23][24] The FCC was expected to enforce net neutrality in its vote, according to ***The New York Times*.**[25][26]

On 26 February 2015, the FCC ruled in favor of net neutrality by adopting **Title II (common carrier)** of the **Communications Act of 1934** and **Section 706 in the Telecommunications Act of 1996** to the Internet.[27][28][29] The FCC Chairman, **Tom Wheeler**, commented, "This is no more a plan to regulate the Internet than the **First Amendment** is a plan to regulate free speech. They both stand for the same concept."[30] On 12 March 2015, the FCC released the specific details of the net neutrality rules.[31][32][33] On 13 April 2015, the FCC published the final rule on its new "**Net Neutrality**" regulations.[34][35] These rules went into effect on 12 June 2015.[36]

Upon becoming FCC chairman in April 2017, **Ajit Pai** proposed an end to net neutrality, awaiting votes from the commission.[37][38] On 21 November 2017, Pai announced that a vote will be held by FCC members on 14 December 2017 on whether to repeal the policy.[39] On 11 June 2018, the repeal of the FCC's network neutrality rules took effect.[40]

Classifications

Access providers

Access provider ISPs provide Internet access, employing a range of technologies to connect users to their network.[41] Available technologies have ranged from computer modems with **acoustic couplers t**o telephone lines, to television cable (CATV), **Wi-Fi,** and fiber optics.

For users and small businesses, traditional options include copper wires to provide **dial-up,** DSL, typically **asymmetric digital subscriber lin**e (ADSL), cable modem or **Integrated Services Digital Network** (ISDN) (typically **basic rate interface**). Using **fiber-optics** to end users is called **Fiber To The Home** or similar names.[42]

Customers with more demanding requirements (such as medium-to-large businesses, or other ISPs) can use higher-speed DSL (such as **single-pair high-speed digital subscriber line**), **Ethernet**, **metropolitan Ethernet**, **gigabit Ethernet**, **Frame Relay**, ISDN **Primary Rate Interface**, **ATM (Asynchronous Transfer Mode)** and **synchronous optical networking** (SONET).[43]

Wireless access is another option, including **cellular** and **satellite Internet access**.

Mailbox providers

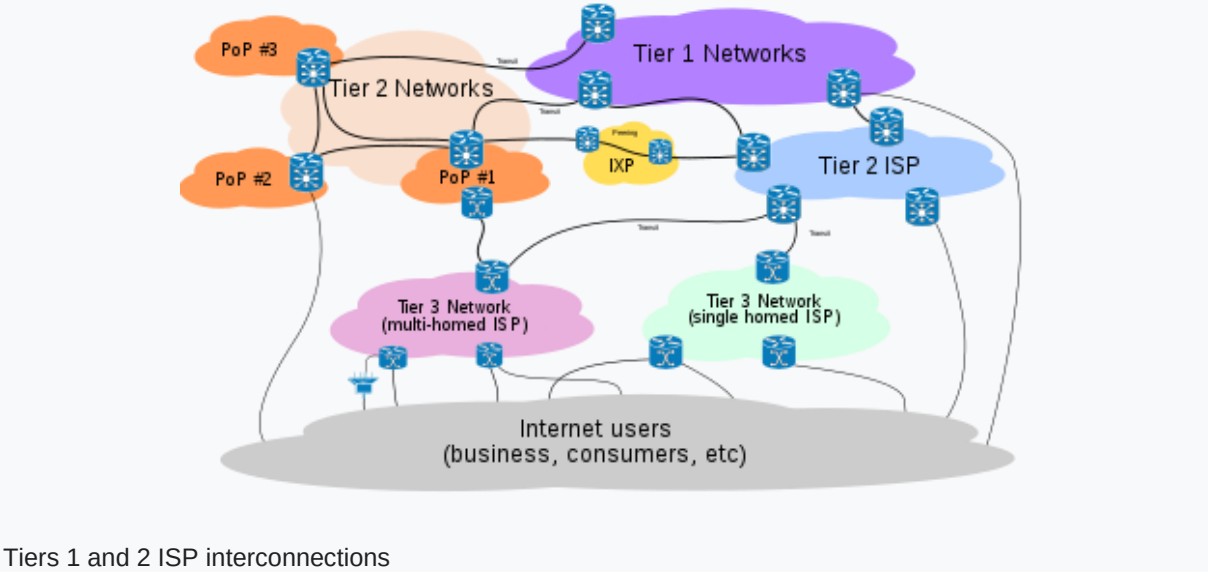
A **mailbox provider** is an organization that provides services for hosting electronic mail domains with access to storage for mail boxes. It provides **email servers** to send, receive, accept, and store email for **end users** or other organizations.

Many mailbox providers are also access providers,[44] while others are not (e.g., **Gmail**, **Yahoo! Mail**, **Outlook.com**, **AOL Mail**, **Po box**). The definition given in **RFC 6650** covers email hosting services, as well as the relevant department of companies, universities, organizations, groups, and individuals that manage their mail servers themselves. The task is typically accomplished by implementing **Simple Mail Transfer Protocol** (SMTP) and possibly providing access to messages through **Internet Message Access Protocol** (IMAP), the **Post Office Protocol**, **Webmail**, or a proprietary protocol.[45]

Hosting ISPs

Internet hosting services provide email, web-hosting, or online storage services. Other services include **virtual server**, cloud services, or physical server operation.[46]

Transit ISPs



Tiers 1 and 2 ISP interconnections

Just as their customers pay them for Internet access, ISPs themselves pay upstream ISPs for Internet access. An upstream ISP usually has a larger network than the contracting ISP or is able to provide the contracting ISP with access to parts of the Internet the contracting ISP by itself has no access to.[47]

In the simplest case, a single connection is established to an upstream ISP and is used to transmit data to or from areas of the Internet beyond the home network; this mode of interconnection is often cascaded multiple times until reaching a **tier 1 carrier**. In reality, the situation is often more complex. ISPs with more than

one **point of presence** (PoP) may have separate connections to an upstream ISP at multiple PoPs, or they may be customers of multiple upstream ISPs and may have connections to each one of them at one or more point of presence.[47] Transit ISPs provide large amounts of **bandwidth** for connecting hosting ISPs and access ISPs.[48]

Virtual ISP

A **virtual ISP** (VISP) is an operation that purchases services from another ISP, sometimes called a *wholesale ISP* in this context,[49] which allow the VISP's customers to access the Internet using services and infrastructure owned and operated by the wholesale ISP. VISPs resemble **mobile virtual network operators** and **competitive local exchange carriers** for voice communications.

Free ISPs

Free ISPs are Internet service providers that provide service free of charge. Many free ISPs display advertisements while the user is connected; like commercial **television**, in a sense they are selling the user's attention to the advertiser. Other free ISPs, sometimes called **freenets**, are run on a nonprofit basis, usually with volunteer staff.[50]

Wireless ISP

A **wireless Internet service provider** (WISP) is an Internet service provider with a network based on wireless networking. Technology may include commonplace Wi-Fi wireless mesh networking, or proprietary equipment designed to operate over open 900 MHz, 2.4 GHz, 4.9, 5.2, 5.4, 5.7, and 5.8 GHz bands or licensed frequencies such as 2.5 GHz (EBS/BRS), 3.65 GHz (NN) and in the UHF band (including the MMDS frequency band) and **LMDS**.[51]

Peering

ISPs may engage **in peering**, where multiple ISPs interconnect at **peering points** or **Internet exchange points (**IXPs), allowing routing of data between each network, without charging one another for the data transmitted—data that would otherwise have passed through a third upstream ISP, incurring charges from the upstream ISP.[47]

ISPs requiring no upstream and having only customers (end customers or peer ISPs) are called **Tier 1 ISPs.**

Network hardware, software and specifications, as well as the expertise of network management personnel are important in ensuring that data follows the most efficient route, and upstream connections work reliably. A tradeoff between cost and efficiency is possible.[50]

Law enforcement and intelligence assistance

Internet service providers in many countries are legally required (e.g., via **Communications Assistance for Law Enforcement Act** (CALEA) in the U.S.) to allow law enforcement agencies to monitor some or all of the information transmitted by the ISP, or even store the browsing history of users to allow government access if needed (e.g. via the **Investigatory Powers Act 2016** in the **United Kingdom).** Furthermore, in some countries ISPs are subject to

monitoring by intelligence agencies. In the U.S., a controversial National Security Agency program known as **PRISM** provides for broad monitoring of Internet users traffic and has raised concerns about potential violation of the privacy protections in the **Fourth Amendment to the United States Constitution**.[52][53] Modern ISPs integrate a wide array of **surveillance** and **packet sniffing** equipment into their networks, which then feeds the data to law-enforcement/intelligence networks (such as **DCSNet** in the United States, or **SORM**[54] in Russia) allowing monitoring of Internet traffic in real time.

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

Ans. ***Difference between MAC Address and IP Address***

Both MAC Address and IP Address are used to uniquely identify a machine on the internet. MAC address is provided by the chip maker while IP Address is provided by the Internet Service Provider.

Following are the important differences between MAC Address and IP Address.

Sr. No.	Key	MAC Address	IP Address
1	Definition	MAC Address stands for Media Access Control Address.	IP Address stands for Internet Protocol Address.
2	Usage	MAC Address ensure that physical address of the computer is unique.	IP Address is a logical address of the computer and is used to uniquely locate computer connected via a network.
3	Format	MAC Address is of six byte hexadecimal address.	IP Address is of 4 bytes or of 16 bytes.
4	Access Protocol	MAC Address can be retrieved using ARP protocol.	IP Address can be retrieved using RARP protocol.
5	Provider	Chip maker manufacturer	Internet Service Provider, ISP provides

Sr. No.	Key	MAC Address	IP Address
		provides the MAC Address.	the IP Address.

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

Ans. 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.

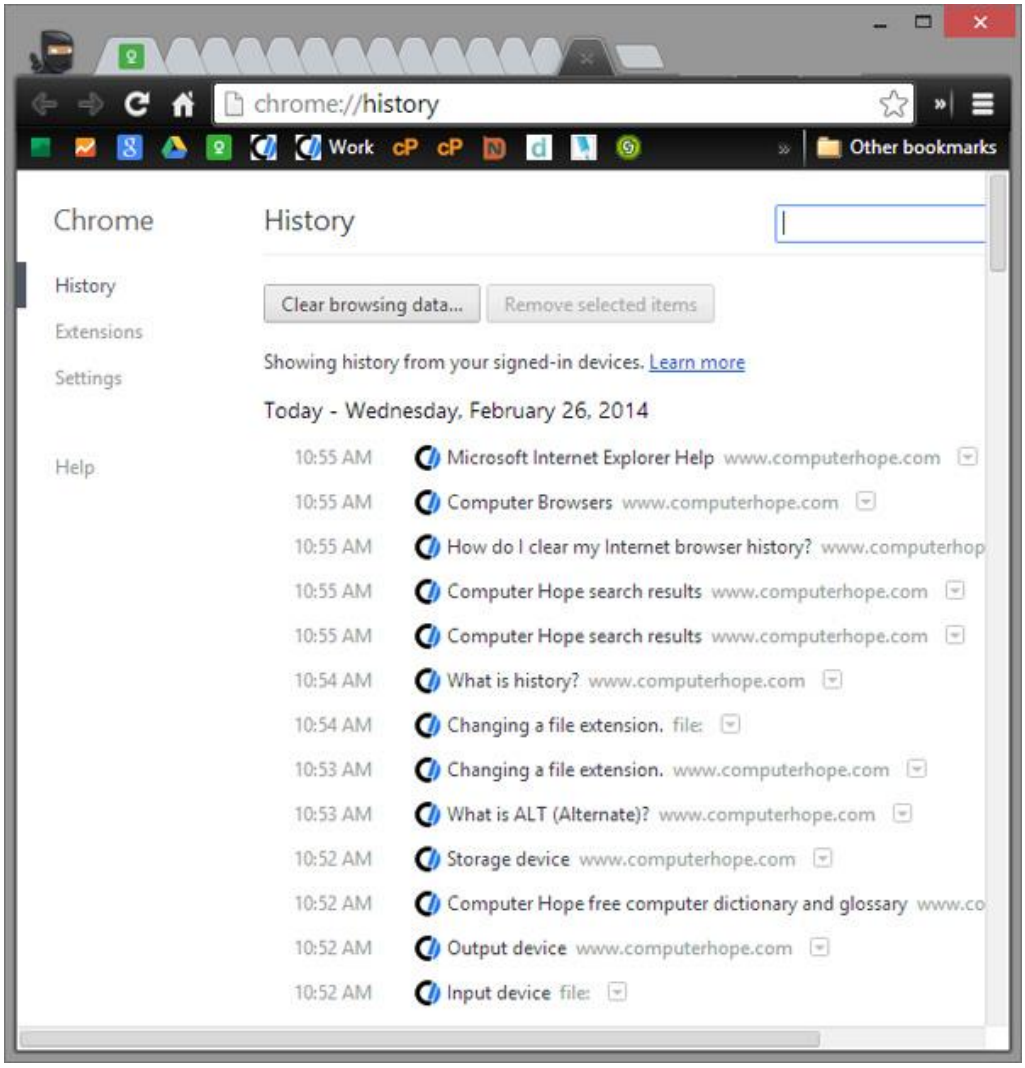
Desktop or laptop computer

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.


chrome://history
Work
cP
cP
Other bookmarks
Chrome
History
Extensions
Settings
Help
History
Clear browsing data...
Remove selected items
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: