

1What are the different types of networks?

A computer network is a system in which multiple computers are connected to share information and resources. Computer network varies with each other based on their functionality, geography, ownership, and communication media used.

A computer network can be divided into the following types, based on the geographical area that they cover, they are:

- A. LAN(Local Area Network)**
- B. MAN(Metropolitan Area Network)**
- C. WAN(Wide Area Network)**

A]. LAN(Local Area Network)

A local area network is a network, which is designed to operate over a very small geographical or physical area such as an office, building, a group of buildings, etc. Generally, it is used to connect two or more personal computers through a communication medium such as coaxial, twisted-pair cables, etc. A LAN can use either wired or wireless mode of communication. The LAN which entirely uses wireless media for communication can be termed as WLAN(Wireless Local Area Network).

In other words, a LAN connects a relatively small number of machines in a relatively close geographical area. Bus, Ring, and Star topology are generally used in a local area network. In LAN, one computer can become a server in a star topology, serving all other computers called clients. Two different buildings can be connected very easily in LAN using a 'Bridge'.

the advantages of a LAN:

1. File transfer and file access
2. Resource or peripherals sharing
3. Personal computing
4. Document distribution
5. Easy to design and troubleshoot
6. Minimum propagation delay
7. High data rate transfer
8. Low error rate
9. Easily scalable(devices can be added or removed very easily)

Following are the disadvantages of a LAN:

1. Equipment and support may be costly
2. Some hardware devices may not inter-operate properly

B]. MAN(Metropolitan Area Network)

A Metropolitan Area Network is a bigger version of LAN that uses similar technology as LAN. It spans over a larger geographical area such as a town or an entire city.

It can be connected using an optical fiber cable as a communication medium. Two or more LAN's can also be connected using routers to create a MAN. When this type of network is created for a specific campus, then it is termed as CAN(Campus Area Network).

Uses of MAN are as follows:

1. MAN can be used for connecting the various offices of the same organization, spread over the whole city.
2. It can be used for communication in various governmental departments.

Following are the advantages of using MAN:

1. Large geographical area cover as compared to LAN
2. High-speed data connectivity
3. The Propagation delay of MAN is moderate

Following are the disadvantages of MAN:

1. It is hard to design and maintain a MAN
2. MAN is less fault-tolerant
3. It is costlier to implement

C . WAN(Wide Area Network)

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

A WAN may include various Local and Metropolitan Area Network. The mode of communication in a WAN can either be wired or wireless. Telephone lines for wired and satellite links for wireless communication can be used in a wide area n**Following are the disadvantages of WAN:**

1. The propagation delay is more in a WAN
2. The data rate is low
3. The error rate is high
4. It is very complex to design a WAN
etwork.

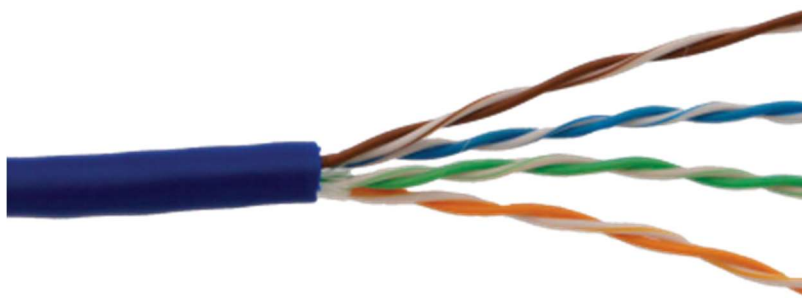
2]. Explain the Shielded twisted pair (STP) and Unshielded twisted pair(UTP)

Unshielded Twisted Pair (UTP) Cable: UTP cable is the most general type of telecommunication medium which is mostly used. Although most familiar

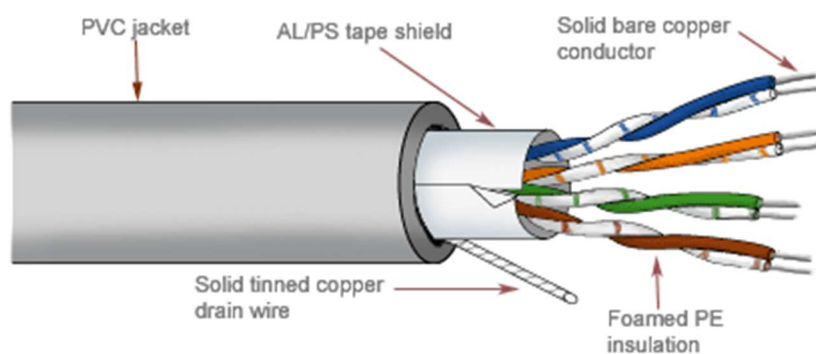
from its use in telephone system, its frequency range is suitable for transmitting both data and voice.



A twisted pair consists of two conductors, generally copper, each with its own coloured plastic insulation. The plastic insulation is colour-banded for identifications shown in fig 1. colors are used both to identify the specific conductors in a cable end to indicate which wires belong in pairs and how they relate to other pairs in a large bundle.



Shielded Twisted –Pair (STP) Cable: Shielded Twisted –Pair (STP) Cable has a metal foil or braided-mesh covering that encases each pair of insulated conductors as shown in

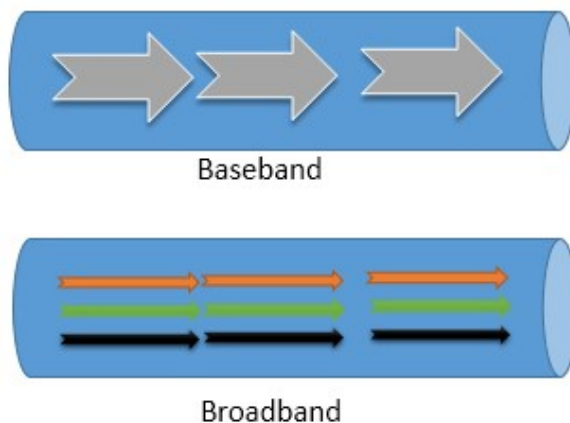


The metal casing prevents the penetration of electromagnetic noise. It also can eliminate the phenomenon called crosstalk. Which is the undesired effect of one circuit (or channel) on another circuit (or channel)? It occurs when one line pickup some of signals travelling down another line. This effect can be experienced during telephone conversations when one can hear other conversations in the background. To eliminate this effect shielding is used for each twisted pair cable. Shielded twisted-pair cable has the same quality consideration and uses the same connectors as unshielded twisted-pair cable, but the shield must be connected to a ground. Materials and manufacturing requirements make STP more expensive than UTP but less Susceptible to noise.

4. What is difference between baseband and broadband transmission?

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.

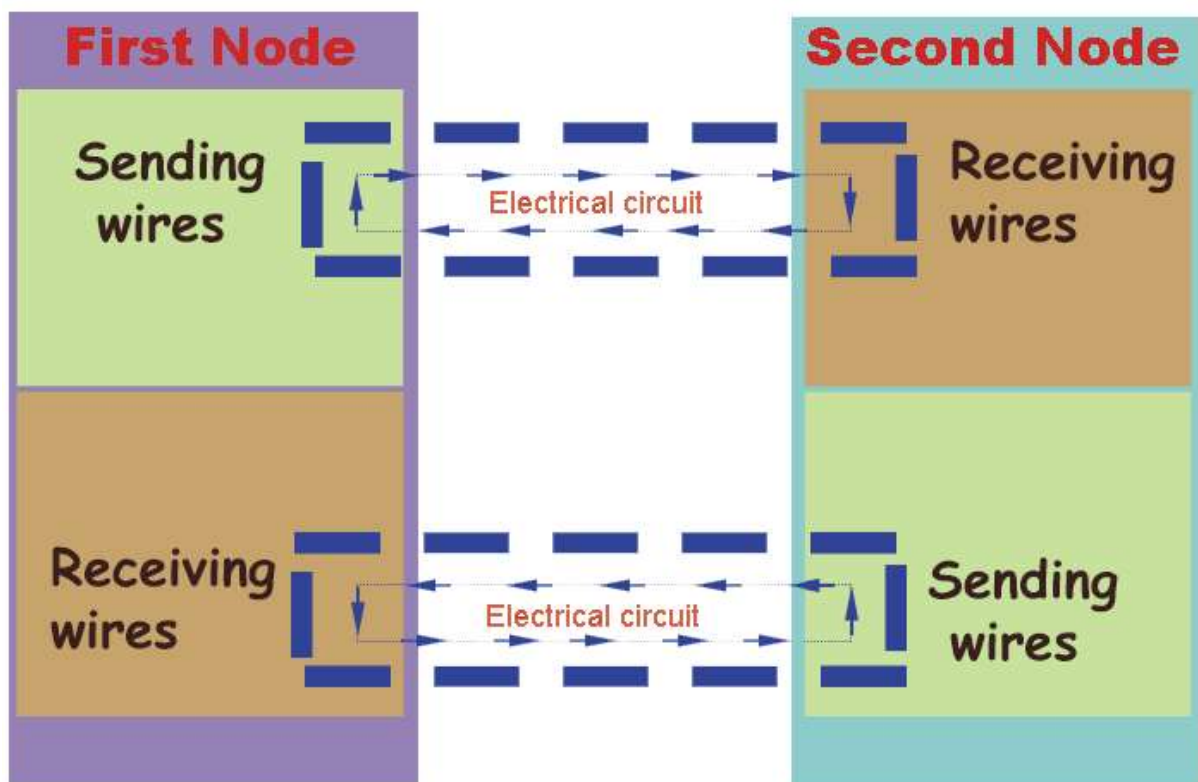


Technical differences between the baseband and broadband transmissions

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



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

What is a Switch?

A switch is a multicast networking device that works under the Datalink layer of the OSI model and connects a bunch of computers or devices in a network. It's mainly used to send a private message and it does not waste data.

A switch can easily identify which device is connected to which port by using a MAC address giving it the ability to deliver the message to a particular machine.

Advantages of using a Switch

- It's secure since it delivers data to the specified node.
- It lowers the chances of frame collisions domains.
- It increases the bandwidth in a network.
- It increases the number of ports needed to connect the nodes available in a network.
- It operates under full-duplex.

Disadvantages of using Switches

- They are more expensive compared to hubs and other devices used in a network.
- To deal with multicast parcels, proper planning is required.
- Problems may arise when broadcasting traffic.

What is a Hub?

A Hub is a simple and cheap networking device that works under the physical layer of the OSI model and connects a bunch of computers in a Local Area Network(LAN). It is considered less intelligent because it does not filter data and does not know where the data is to be sent.

All information sent to a hub is automatically sent to all ports of the devices connected to it. This leads to wastage of bandwidth.

Advantages of using hubs

- They have the ability to connect to the network using different physical media.
- They can be used to increase the network distance.
- Hubs are relatively cheap compared to switches and other devices in the network.

Disadvantages of using a hub

- It increases the chances of collision domains between packets when being transferred from one device to another.
- Hubs operate under half-duplex. Only one device can send or receive data at a time
- Hubs share data to all the devices in a network thus making the network insecure.

- Hubs waste lots of bandwidth when transmitting data.

Switch vs Hub

- A Hub is a broadcast device that sends data from one node to all nodes but a Switch is a multicast device that can send data to a particular node.
- A Hub supports half-duplex i.e., only one device can send or receive data at a time while a switch supports full-duplex i.e., both devices can send and receive data at the same time.
- A switch is located on the second layer of the OSI model while a Hub is located on the first layer.

What is a Router?

A Router is a networking device that operates under the network layer of the OSI model and is used to connect two or more networks. It is a device that establishes a common link between networks to enable data flow between them.

Advantages of Routers

- With the aid of dynamic routing algorithms, it can choose the best path in the internetwork.
- It creates collision domains to reduce network traffic.
- It provides connections between different network architectures.

Disadvantages of Routers

- They are expensive compared to hubs and switches.
- They need to analyze data. This makes them slower.
- They have low bandwidth because of their dynamic router communication.

Let's look at their differences on the OSI model.

The component's layer in the OSI model

The [Open Systems Interconnection Model](#) (OSI Model) is a 7 layer model that is used to describe, in a pictorial way, how computer systems communicate. A switch, a router, and a hub each operate on a different layer.

A switch is located on the OSI model's Data Link layer i.e., the second layer. The link layer is specific to the medium over which the packet is traveling. The Ethernet and Mac Address are part of this layer.

A router resides in the Network Layer of the OSI model i.e., the third layer.

A hub is located in the Physical Layer of the OSI model i.e., the first layer.

Functions of each device

Switch

- It allows various connections of many devices in the same network and the management of port and VLAN security settings.

- **Learning** - This is the process of collecting the MAC address of linked devices.
- **Forwarding** - This is the process of transferring network traffic from one device connected to one port of a network switch to another device connected to another port.
- **Preventing Layer 2 Switching Loops** - In a Local Area Network, redundant connections are built to prevent the entire network from failing if one link fails. Layer 2 switching loops and broadcast storms can be caused by redundant connections. A network switch's job is to prevent layer 2 switching loops and broadcast storms.

Router

- Its major purpose is to connect many types of networks at the same time using adaptive and non-adaptive routing.
- The router is connected to at least two networks and decides how to deliver each data packet depending on its current knowledge of the network status.
- If a packet is traveling to the LAN, the router bounces it back. The packet will be toured depending on the routing table if this is not the case.

Hub

- A hub is a simple and cheap networking device that allows a bunch of computers to be connected to a single network
- When a hub receives a data packet (an Ethernet frame) from a network device at one of its ports, it broadcasts (repeats) the packet to all of its ports, i.e., to all other network devices. A collision occurs when two network devices on the same network try to send packets at the same time.

Applications of each device

Switch

- It is commonly used in local area networks for connecting many nodes.
- **Forwards a message to a specific host** - On each port, a switch, like a bridge, employs the same forwarding or filtering logic. When a host or switch on the network transmits a message to another host or switches on the same network, the switch receives the frames and decodes them to read the physical (MAC) address component of the message.
- **Increase LAN bandwidth** - A switch divides a LAN into many collision domains, each with its broadband connection, considerably improving the LAN's bandwidth.

Router

- It is commonly used in Local Area Network and Metropolitan Area Network (MAN).
- **It manages traffic** by forwarding data packets to their proper IP addresses. Traffic between these networks may be managed.
- It determines the best path to send packets.

Hub

- It is similar to a switch because it is used in the Local Area Network (LAN).

- It is used for network monitoring.
- They are also used in organizations to provide connectivity.
- It can be used to create a device that is available throughout the network.

Modes of data transmission

They define the direction in which data flows between two communicating devices. There are three types of transmission modes:

1. **Simplex** - In this mode of transmission, data can only move to one direction i.e., a device can only send data but cannot receive and the receiver can only receive but cannot send the data.
2. **Half-Duplex** - In this mode, only one device can send or receive data at a time but not both at the same time.
3. **Full-Duplex** - In this mode, a device can send and receive data at the same time.

Read this [documentation](#) for more information on the different modes of data transmission.

Both **switches** and **routers** support full-duplex transmission. Thus, a bunch of computers can send data at the same time.

Hubs support half-duplex transmission. Thus, only one node can send data at a time.

Addresses used in each device

A **switch** stores and uses the MAC address of a device to transfer data while a **router** uses the IP address of the device to transfer data between networks.

A **hub** on the other hand does not store any MAC/IP address to transfer data.

Transmission of data

A **switch** transmits data from one device to another in form of [frames](#) while a **router** transmits data from one network to another in form of [packets](#).

A **hub** transmits data from one device to another in form of binary bits.

Conclusion

In this article, we have looked at hubs, switches, and routers. We have also looked at their functionalities and applications of each device as used in networking.

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

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

the most common network troubleshooting techniques, best practices, and recommended my favorite [network performance monitoring tool](#) you can use to give you a starting point and structure for efficiently resolving network issues as they arise as well as proactively prevent them. I'll be using a bit of technical jargon here, but I'll explain the key terms and hopefully give enough context so anyone can understand what I'm talking about.

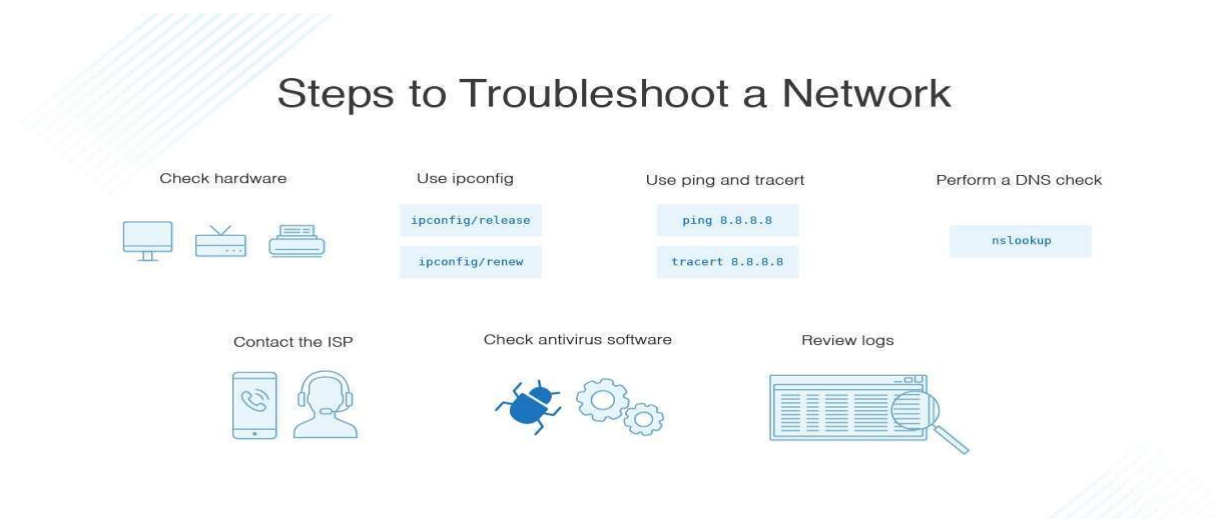
[How to Troubleshoot a Network](#)

[Network Troubleshooting Best Practices](#)

[Best Way to Troubleshoot Network Issues](#)

How to Troubleshoot a Network

Issues can arise at numerous points along the network. Before you start trying to troubleshoot any issue, you want to have a clear understanding of what the problem is, how it came up, who it's affecting, and how long it's been going on. By gathering the right information and clarifying the problem, you'll have a much better chance of resolving the issue quickly, without wasting time trying unnecessary fixes.



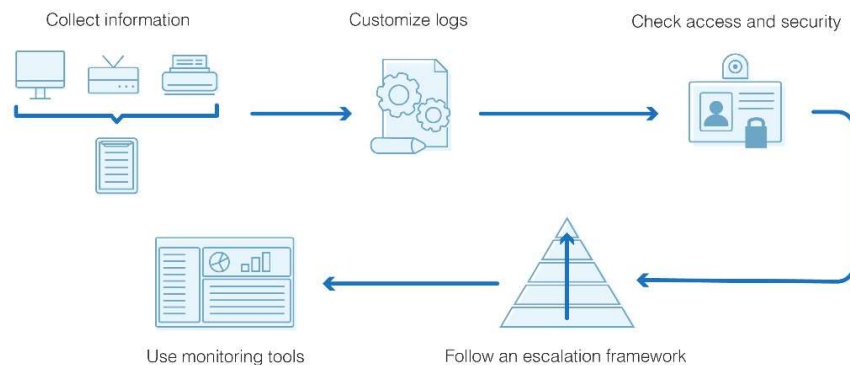
I always start troubleshooting using these simple network troubleshooting steps to help diagnose and refine the issue.

1. **Check the hardware.** When you're beginning the troubleshooting process, check all your hardware to make sure it's connected properly, turned on, and working. If a cord has come loose or somebody has switched off an important router, this could be the problem behind your networking issues. There's no point in going through the process of troubleshooting network issues if all you need to do is plug a cord in. Make sure all switches are in the correct positions and haven't been bumped accidentally.
Next, turn the hardware off and back on again. This is the mainstay of IT troubleshooting, and while it might sound simplistic, often it really does solve the problem. Power cycling

your modem, router, and PC can solve simple issues—just be sure to leave each device off for at least 60 seconds before you turn it back on.

2. **Use ipconfig.** Open the command prompt and type “ipconfig” (without the quotes) into the terminal. The Default Gateway (listed last) is your router’s IP. Your computer’s IP address is the number next to “IP Address.” If your computer’s IP address starts with 169, the computer is not receiving a valid IP address. If it starts with anything other than 169, your computer is being allocated a valid IP address from your router.
Try typing in “ipconfig /release” followed by “ipconfig /renew” to get rid of your current IP address and request a new one. This will in some cases solve the problem. If you still can’t get a valid IP from your router, try plugging your computer straight into the modem using an ethernet cable. If it works, the problem lies with the router.
3. **Use ping and tracert.** If your router is working fine, and you have an IP address starting with something other than 169, the problem’s most likely located between your router and the internet. At this point, it’s time to use the **ping** tool. Try sending a ping to a well-known, large server, such as Google, to see if it can connect with your router. You can ping Google DNS servers by opening the command prompt and typing “ping 8.8.8.8”; you can also add “-t” to the end (ping 8.8.8.8 -t) to get it to keep pinging the servers while you troubleshoot. If the pings fail to send, the command prompt will return basic information about the issue. You can use the **tracert** command to do the same thing, by typing “tracert 8.8.8.8”; this will show you each step, or “hop,” between your router and the Google DNS servers. You can see where along the pathway the error is arising. If the error comes up early along the pathway, the issue is more likely somewhere in your local network.
4. **Perform a DNS check.** Use the command “nslookup” to determine whether there’s a problem with the server you’re trying to connect to. If you perform a DNS check on, for example, google.com and receive results such as “Timed Out,” “Server Failure,” “Refused,” “No Response from Server,” or “Network Is Unreachable,” it may indicate the problem originates in the DNS server for your destination. (You can also use nslookup to check your own DNS server.)
5. **Contact the ISP.** If all of the above turn up no problems, try contacting your internet service provider to see if they’re having issues. You can also look up outage maps and related information on a smartphone to see if others in your area are having the same problem.
6. **Check on virus and malware protection.** Next, make sure your virus and malware tools are running correctly, and they haven’t flagged anything that could be affecting part of your network and stopping it from functioning.
7. **Review database logs.** Review all your database logs to make sure the databases are functioning as expected. If your network is working but your database is full or malfunctioning, it could be causing problems that flow on and affect your network performance.

Network Troubleshooting Flowchart



1. **Collect information.** To best support your end users, you first need to make sure you're clear on what the problem is. Collect enough information from both the people who are experiencing network issues and the network itself, so you can replicate or diagnose the problem. Take care not to mistake symptoms for the root cause, as what initially looks like the problem could be part of a larger issue.
2. **Customize logs.** Make sure your event and security logs are customized to provide you with information to support your troubleshooting efforts. Each log should have a clear description of which items or events are being logged, the date and time, and information on the source of the log (MAC or IP address).
3. **Check access and security.** Ensure no access or security issues have come up by checking all access permissions are as they should be, and nobody has accidentally altered a sensitive part of the network they weren't supposed to be able to touch. Check all firewalls, antivirus software, and malware software to ensure they're working correctly, and no security issues are affecting your users' ability to work.
4. **Follow an escalation framework.** There's nothing worse than going to the IT help desk and being directed to another person, who then directs you to another person, who directs you to yet another. Have a clear escalation framework of who is responsible for which issues, including the final person in the chain who can be approached for resolution. All your end users should know who they can go to about a given issue, so time isn't wasted talking to five different people who cannot fix the problem.
5. **Use monitoring tools.** Troubleshooting can be done manually but can become time-consuming if you go through each step. When you have a bunch of people knocking on your office door or sending you frantic emails, it can be overwhelming to try to find the problem, let alone fix it. In business and enterprise situations, it's best to use monitoring tools to make sure you're getting all the relevant network information and aren't missing anything vital, not to mention avoiding exposing the company to unnecessary risk.

My preferred monitoring software is SolarWinds® [Network Performance Monitor](#) (NPM). It's a well-designed tool with features to support network troubleshooting issues in an efficient and thorough

way. It allows you to clearly baseline your network behavior, so you have good data on what your network *should* look like and how it usually performs, and it includes advanced alerting features so you don't receive floods of alerts all the time. You can customize the software to alert you to major issues, choose the timing of alerts, and define the conditions under which alerts occur.

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

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

An Internet Protocol (IP) address is a unique number assigned to every device on a network. Just as a street address determines where a letter should be delivered, an IP address identifies computers on the Internet. Network devices use IP addresses to communicate with each other.

The Internet uses DNS (Domain Name System) to enable people to use words instead of numbers for Internet addresses. You can think of DNS as an Internet address book, mapping domain names to IP addresses.

When you type a URL into your browser, your browser looks up that domain name in DNS. For example, if you type www.google.com into your browser, your browser would ask DNS for Google's IP address. DNS would return the IP address assigned to Google's domain name (74.125.239.35). Your browser then connects to that IP address.

What is the difference between a dynamic and static IP address?

When a device is assigned a *static* IP address, the address does not change. Most devices use *dynamic* IP addresses, which are assigned by the network when they connect and change over time.

When static IPs are needed

Most users don't need static IP addresses. Static IP addresses normally matter more when external devices or websites need to remember your IP address. One example is VPN or other remote access solutions that trust (whitelists) certain IPs for security purposes. A static IP address is not required if you are hosting a server, although it can simplify the setup process. Google Fiber provides two options.

How to get a dynamic IP address

- Use advanced settings for your network to [configure dynamic DNS](#). When your IP address changes, the DNS entry for your server is automatically updated with its new IP address, so outside users can use the same domain name. You can choose the Dynamic DNS provider and don't have to install additional software on your computer.

How to get a static IP address

- Use advanced settings to [reserve an IP address](#) for a device on your local network. Your device keeps the same IP address until you [cancel the reservation](#) or [remove the device from your network](#), even if the device is disconnected.
- When you sign up for Google Fiber for small business, you [can choose to have no static IPs](#) (that is, dynamic IPs for all your devices), one static IP, or multiple static IPs. The number of static IPs available is shown on the screen when you sign up for service. If you sign up for static IPs, we will assign addresses to you when your service is installed and activated.

9. Discuss TCP/IP model in detail.

TCP/IP Reference Model is a four-layered suite of communication protocols. It was developed by the DoD (Department of Defence) in the 1960s. It is named after the two main protocols that are used in the model, namely, TCP and IP. TCP stands for Transmission Control Protocol and IP stands for Internet Protocol.

The four layers in the TCP/IP protocol suite are –

- **Host-to- Network Layer** –It is the lowest layer that is concerned with the physical transmission of data. TCP/IP does not specifically define any protocol here but supports all the standard protocols.

- **Internet Layer** – It defines the protocols for logical transmission of data over the network. The main protocol in this layer is Internet Protocol (IP) and it is supported by the protocols ICMP, IGMP, RARP, and ARP.
- **Transport Layer** – It is responsible for error-free end-to-end delivery of data. The protocols defined here are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).
- **Application Layer** – This is the topmost layer and defines the interface of host programs with the transport layer services. This layer includes all high-level protocols like Telnet, DNS, HTTP, FTP, SMTP, etc.

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

What Is a Browser?

A web browser, or browser for short, is a computer software application that enables a person to locate, retrieve, and display content such as webpages, images, video, as well as other files on the World Wide Web.

Browsers work because every web page, image, and video on the web has its own unique Uniform Resource Locator (URL), allowing the browser to identify the resource and retrieve it from the web server.

What Is the Difference Between a Search Engine and a Browser?

Some people confuse web browsers and search engines, but they are not the same and perform different roles. A search engine is essentially a type of website that stores searchable information about other websites (common examples of search engines are Google, Bing, Yahoo, and Baidu). However, to connect to a website's server and display its webpages requires a browser. Some examples of browsers can be found below.

5 Popular Browsers

1. Google Chrome

Chrome, created by internet giant Google, is the most popular browser in the USA, perceived by its computer and smartphone users as fast, secure, and reliable. There are also many options for customization in the shape of useful extensions and apps that can be downloaded for free from the Chrome Store.

Chrome also allows easy integration with other Google services, such as Gmail. Due to the success of the "Chrome" brand name, Google has now extended it to other products, for example, Chromebook, Chromebox, Chromecast, and Chrome OS.

2. Apple Safari

Safari is the default on Apple computers and phones, as well as other Apple devices. It's generally considered to be an efficient browser, its slick design being in keeping with the ethos of Apple. Originally developed for Macs, Safari has become a significant force in the mobile market due to the domination of iPhones and iPads.

Unlike some of the other browsers listed, Safari is exclusive to Apple, it doesn't run on Android devices, and the Windows version of Safari is no longer supported by important security updates from Apple.

3. Microsoft Internet Explorer and Edge

Although it has been discontinued, Internet Explorer is worthy of mention as it was the go-to browser in the early days of the internet revolution, with usage share rising to 95% in 2003. However, its relatively slow start-up speed meant that many users turned to Chrome and Firefox in the years that followed.

10. What is a search engine? Give example.

What Is a Search Engine?

Also known as a web search engine and an internet search engine, a search engine is a (usually web-based) computer program that collects and organizes content from all over the internet.

The user enters a query composed of keywords or phrases, and the search engine responds by providing a list of results that best match the user's query. The results can take the form of links to websites, images, videos, or other online data.

How Do Search Engines Work?

The work of a search engine can be broken down into three stages. Firstly, there is the process of discovering the information. Secondly, there is the organization of the information so that it can be effectively accessed and presented when users search for something. Thirdly, the information must be assessed to present search engine

Crawling

Search engines use pieces of software called web crawlers to locate publicly available information from the internet, which is why this process is known as crawling. Web crawlers can also sometimes be referred to as search engine spiders. The process is complicated, but essentially the crawlers/spiders find the web servers (also known as just servers for short) which host the websites and then proceed to investigate them.

A list of all the servers is created, and it is established how many websites are hosted on each server. The number of pages each website has, as well as the nature of the content, for example, text, images, audio, video, is also ascertained. The crawlers also follow any links that the website has, whether internal ones that point to pages within the site, or external ones that point to other websites and use them to discover more pages.

Indexing

Information found by the crawlers is organized, sorted, and stored so that it can later be processed by the algorithms for presentation to the search engine user. This is known as indexing. Not all the page information is stored by the search engine, instead, it's just the essential information needed by the algorithms to assess the relevance of the page for ranking purposes.

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

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. That is why we have internet plans that

suit those needs, whether that be [Xfinity internet plans](#) for the home or business internet, each one has a part to play.

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. With multiple choices ranging from online home décor stores to buying [coats and jackets from Gym King](#) or similar companies, the options are endless. Moreover, 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. It is also great for small businesses who are potentially looking at [florida business banking](#) services, or ones closer depending on

the location of their business, so they can do everything remotely that can help them with keeping it running.

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. With the growing popularity of digital currency, it could be said that the internet is the necessity of this century. Cryptocurrency is one of the major platforms for trading digital assets or digital money through blockchain technology. If you want to learn more about how to invest in crypto, you can check out [Bitcoin Prime review](#) or other similar blogs.

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.

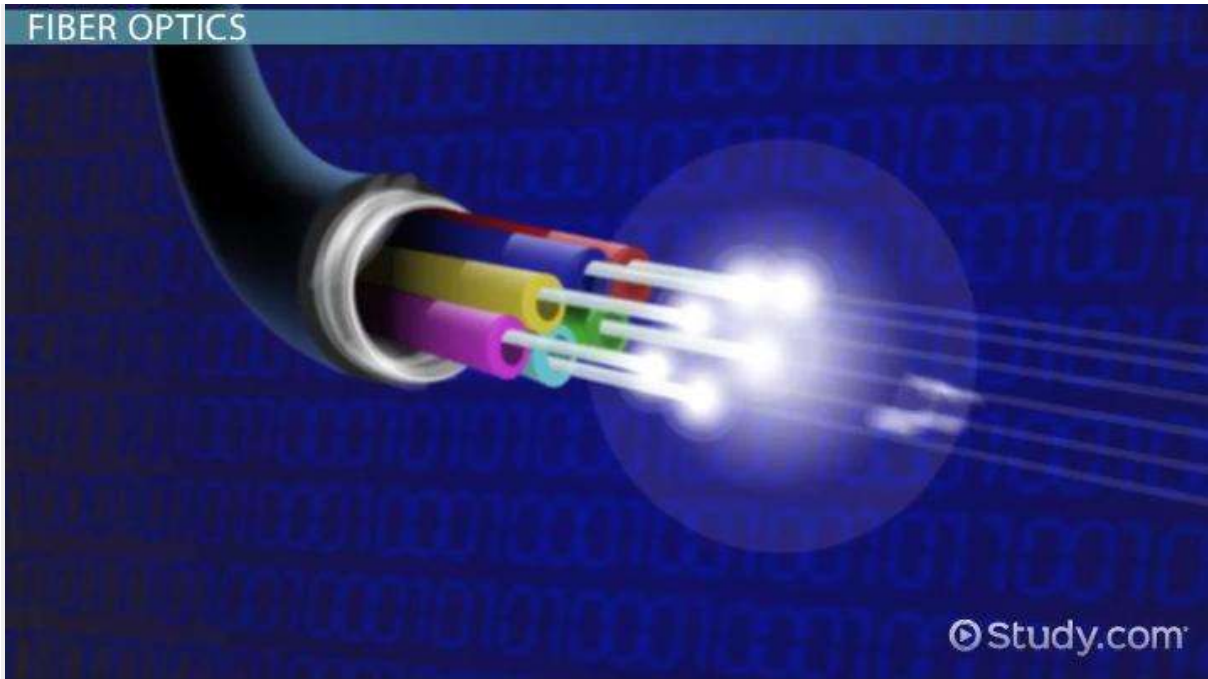
12. What is an Internet Service Provider? Give some example of ISP in India.

Definition

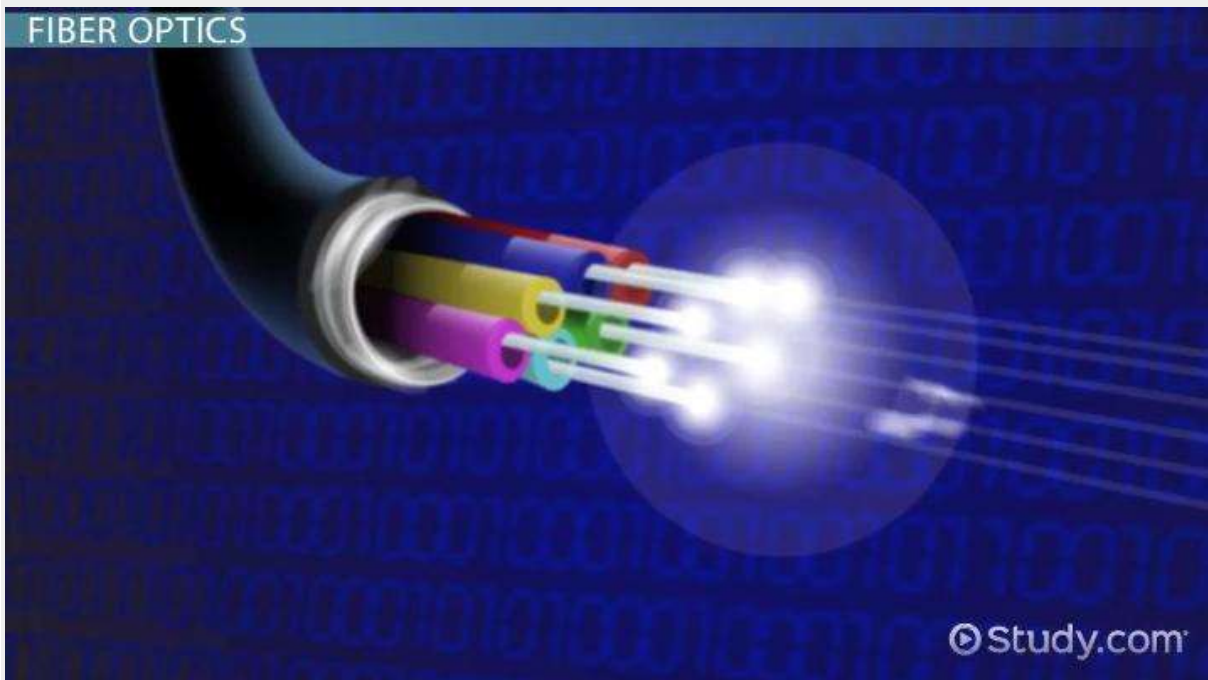
An **Internet Service Provider (ISP)** is a company such as AT&T, Verizon, Comcast, or Spectrum that provides Internet access to companies, families, and even mobile users. ISPs use fiber-optics, satellite, copper wire, and other forms to provide Internet access to its customers.

The type of Internet access varies depending on what the customer requires. For home use, cable or DSL (digital subscriber line) is the perfect, affordable choice. The price of home use can range anywhere from free to roughly \$120 a month. The amount of bandwidth is usually what drives the price. **Bandwidth** is the amount of data that can be sent through an internet connection in a given amount of time. The speed for home use usually varies from 14 kilobits per second to 100 megabits per second. For large companies and organizations, their bandwidth requirements may be 1 to 10 gigabits per second, which is both insanely fast and expensive!

FIBER OPTICS



FIBER OPTICS



[Save](#)

Timeline

Autoplay

Speed **Normal**

- **Video**

- [Quiz](#)

- [Course](#)

172K views

The Internet Highway

ISPs connect to one another by forming backbones, which is another way of saying a main highway of communications. Backbones usually consist of satellite, copper wire, or even fiber-optic media. **Media** is a term that means cables or lines, and it's the physical means of connecting your home to the internet.

Now, imagine these 'main highways' are like the major arteries that we have in our bodies. These major arteries push an extreme amount of blood (or data) to our smaller blood arteries (cities). Those smaller arteries then feed into blood vessels (neighborhoods) and then into tiny capillaries (our individual homes).

ISPs provide the same service, except that they use different types of media to do so. ISPs bridge distant locations between cities, states, and countries. Because of these high speed backbone systems, we are able to receive an email within seconds, stream our favorite movie without interruption, and play online games with no lag whatsoever.

Satellites

Let's go over the different types of media that are used in order to give you a broader understanding of how ISPs work.

Customers who live in remote locations, such as farms, deserts, and mountainous areas, may require a **satellite Internet service**. This involves transmitting and receiving data from a satellite orbiting about 22,000 miles above the earth. Although satellite communication is not as fast as other mediums, it does provide flexibility with limited environmental impact, and there is not as much need for support from the local telecommunications company.

These satellite terminals can also be used when setting up natural disaster recovery centers. For example, FEMA used a satellite terminal during Hurricane Katrina, since the public telecommunication infrastructure was severely damaged.

Fiber Optics

Fiber optics, or fiber, is a transmission medium used to transmit light instead of electrical voltage, like copper. The great thing about fiber is that it transmits Internet traffic at the speed of light!

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

Difference between MAC Address and IP Address

- Difficulty Level : [Easy](#)
- Last Updated : 23 Feb, 2022

Both [MAC Address](#) and [IP Address](#) are used to uniquely define a device on the internet. NIC Card's Manufacturer provides the MAC Address, on the other hand, Internet Service Provider provides IP Address.

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

MAC
Address
stands for
Media
Access
Control
Address.

IP Address stands for
Internet Protocol Address.

- | | | |
|----|---|---|
| 2. | MAC Address is a six byte hexadecimal address. | IP Address is either a four-byte (IPv4) or a sixteen-byte (IPv6) address. |
| 3. | A device attached with MAC Address can retrieve by ARP protocol. | A device attached with IP Address can retrieve by RARP protocol. |
| 4. | NIC Card's Manufacturer provides the MAC Address. | Internet Service Provider provides IP Address. |
| 5. | MAC Address is used to ensure the physical address of a computer. | IP Address is the logical address of the computer. |
| 6. | MAC Address operates in the data link layer. | IP Address operates in the network layer. |
| 7. | MAC Address helps in simply identifying the device. | IP Address identifies the connection of the device on the network. |

8.	MAC Address of computer cannot be changed with time and environment.	IP Address modifies with the time and environment.
9.	MAC Addresses can't be found easily by a third party.	IP Addresses can be found by a third party.
10.	<p>It is a 48-bit address that contains 6 groups of 2 hexadecimal digits, separated by either hyphens (-) or colons(.).</p> <p>Example:</p> <p>00:FF:FF:AB:BB:AA</p> <p>or</p> <p>00-FF-FF-AB-BB-AA</p>	<p>IPv4 uses 32-bit addresses in dotted notations, whereas IPv6 uses 128-bit addresses in hexadecimal notations.</p> <p>Example:</p> <p>IPv4 192.168.1.1</p> <p>IPv6 FFFF:F200:3204:0B00</p>
11.	No classes are used for MAC addressing.	IPv4 uses A, B, C, D, and E classes for IP addressing.
12.	MAC Address sharing is not allowed.	In IP address multiple client devices can share the IP address.

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


Today, all major browsers, including [Firefox](#), [Safari](#), [Edge](#), and [Chrome](#), have functionality that allows you to quickly and easily view your search and destination history. However, as different devices contain browser history, there are multiple ways to view it as well. To proceed, choose your desired device from the section below and follow the instructions.

When one of these [keyboard shortcuts](#) is pressed, a history section similar to the example below should appear. In the following screenshot, browsing history is being viewed in Google Chrome.

Android phone or tablet running Google Chrome



Users running Google Chrome on their [Android](#) phone or tablet can view their history with the following steps.

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

iPhone or iPad running Safari

Users running [Safari](#) for [iOS](#) on their [iPhone](#) or [iPad](#) can view their history with the following steps.

1. On your device, open the [Safari](#) Internet browser.
2. In the lower-left corner of the browser window, tap and hold the back arrow.
3. The page that opens contains your browser's history.