RAJA JAIT SINGH GOVERNMENT POLYTECHNIC
NEEMKA , HARYANA

LAB MANAUL
on
COMPUTER NETWORK

COMPUTER SCIENCE ENGINEERING

INDEX

#PRACTICAL – 01

AIM: Recognize the physical topology and cabling (coaxial, OFC, UTP, STP) of a network.

Physical Topology:-The arrangement of a network that comprises nodes and connecting lines via sender and receiver is referredto as network topology.

a) Mesh Topology :

In a mesh topology, every device is connected to anotherdevice via a particular channel.

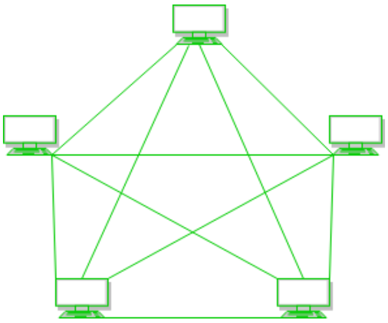


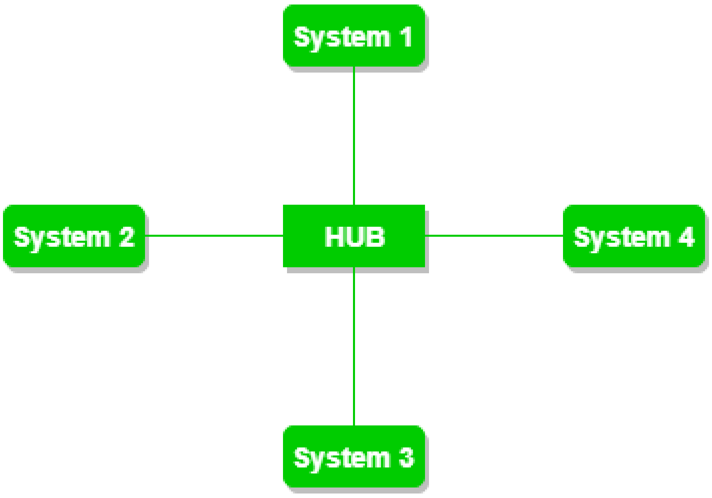
Figure 1: Every device is connected with another via dedicated channels. Thesechannels are known as links.

- Suppose, N number of devices are connected with each other in a mesh topology, the total number of ports that are required by each device is N-1. In Figure 1, there are 5 devices connected to each other, hence the total number of ports required by each device is 4. Total number of ports required=N*(N-1).

- Suppose, N number of devices are connected with each other in a mesh topology, then the total number of dedicated links required to connect them is NC2 i.e. N(N-1)/2. In Figure 1, there are 5 devices connected to each other, hence the total number of links required is5*4/2 = 10.

b) Star Topology :

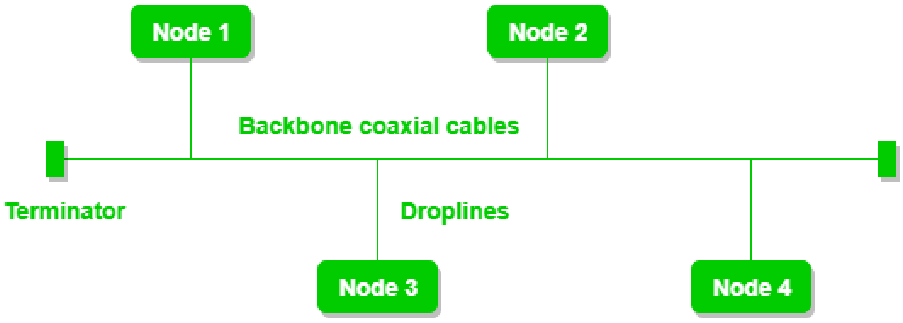
In star topology, all the devices are connected to a single hub through a cable. This hub is the central node and all other nodes are connected to the central node. The hub can be passive in nature i.e., not an intelligent hub such as broadcasting devices, at the same time the hub can be intelligent known as an active hub. Active hubs have repeatersin them.



c) Bus Topology :

Bus topology is a network type in which every computer and network device is connected to a single cable. It transmits the data from one end to another in a single direction. No

bi-directional feature is in bus topology. It is a multi-pointconnection and a non-robust topology because if the backbone fails the topology crashes.

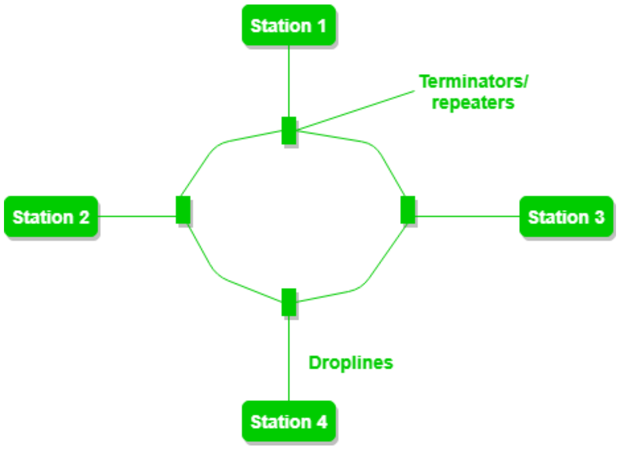


d) Ring Topology :

In this topology, it forms a ring connecting devices with itsexactly two neighboring devices.

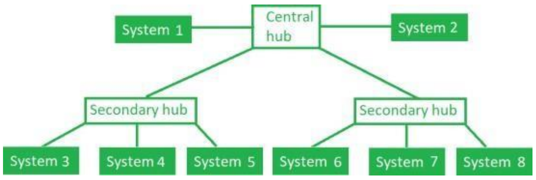
A number of repeaters are used for Ring topology with a large number of nodes, because if someone wants to send some data tothe last node in the ring topology with 100 nodes, then the data will have to pass through 99 nodes to reach the 100th node. Hence to prevent data loss repeaters are used in the network.

The transmission is unidirectional, but it can be made bidirectional by having 2 connections between each NetworkNode, it is called Dual Ring Topology.



e) Tree Topology :

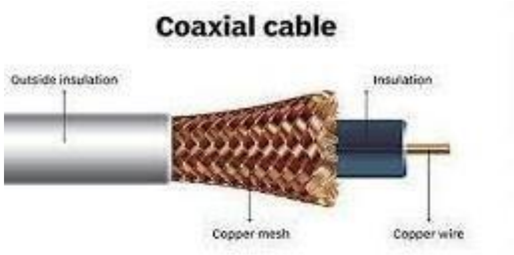
This topology is the variation of Star topology. This topologyhas a hierarchical flow of data.



Cabling (networking)

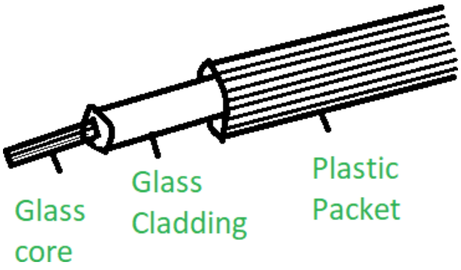
Cabling is the set of wires made of either copper or glass that is used to connect computers and other network componentsto enable them to communicate, thus forming a network of computers.

coaxial→Coaxial cables, commonly called coax, are copper cables with metal shielding designed to provide immunity against noise and greater bandwidth. Coax can transmit signalsover larger distances at a higher speed as compared to twisted pair cables.



Structure of Coaxial Cables
Coax has a central core of stiff copper conductor for transmitting signals. This is covered by an insulating material. The insulator is encased by a closely woven braidedmetal outer conductor that acts as a shield against noise.

Optical Fiber→ An **Optical Fiber** is a cylindrical fiber of glass which is hair thin size or any transparent dielectric medium. The fiber which is used for optical communication iswaveguides made of transparent dielectrics.



Main element of Fiber Optics:

1. **Core:**

   It is the central tube of very thin size made of optically transparent dielectric medium and carries thelight transmitter to receiver and the core diameter mayvary from about 5um to 100 um.

2. Cladding:

It is outer optical material surrounding the core having reflecting index lower than core and cladding helps to keep the light within the core throughout thephenomena of total internal reflection.

3. Buffer Coating:

It is a plastic coating that protects the fibre made ofsilicon rubber. The typical diameter of the fibre afterthe coating is 250-300 um.

UTP (Unshielded Twisted Pair) →UTP is an unshielded twisted pair cable used in computer and telecommunications mediums.Its frequency range is suitable for transmitting both data andvoice via a UTP cable. Therefore, it is widely used in the telephone, computers, etc. It is a pair of insulated copper wires twisted together to reduce noise generated by external interference. It is a wire with no additional shielding, like aluminium foil, to protect its data from the exterior.

STP (Shielded twisted pair):

A shielded twisted pair is a type of twisted pair cable that contains an extra wrapping foil or copper braid jacket to protect the cable from defects like cuts, losing bandwidth, noise, and signal to the interference. It is a cable that is usually used underground, and therefore it is more costly thanUTP. It supports higher data transmission rates across the long distance. We can also say it is a cable with metal sheathor coating that surrounds each pair of the insulated conductorto protect the wire from external users and prevent electromagnetic noise from penetrating.

#PRACTICAL – O2

AIM: Recognition and use of various types of connectors RJ-45, RJ-11,BNC and SCST.

RJ45→RJ45 is newer, modular, self-securing and compact technology used for connecting the ethernet cables to different electronic devices. The RJ45 is an 8 pin connector used to attach the ethernet interfaces. It is known as an 8P8Cconnector.

1. Types of cables based on the termination:Straight-overcable
2. Crossover cable

RJ11→RJ11 is used to terminate the conventional PSTN telephone networks. RJ11 is a four pins connector which is used for terminating the telephone wires. The RJ11 technically uses thecentre 2 contacts of 6 available and is used for wiring a single phone line. It is the common connector for plugging a telephone into the wall and the handset into the telephone.

BNC connector->

BNC connector is a series of connectors used for connecting thinnet coaxial cabling to various networking components. BNC connectors use a twist-and-lock mechanism that provides a secure connection between network cabling and components.

BNC connectors are typically used on 10Base2 Ethernet networks. The different types of BNC connectors include the following:

- **BNC cable connector:** Soldered or crimped to the ends of a thinnet cable
- **BNC T-connector:** Used to connect a network interface card (NIC) to a thinnet cable segment
- **BNC barrel connector:** Used to connect two pieces of thinnet cable
- **BNC terminator:** Provides a 50-ohm termination for the free end of a thinnet cable

BNC Cable Connector

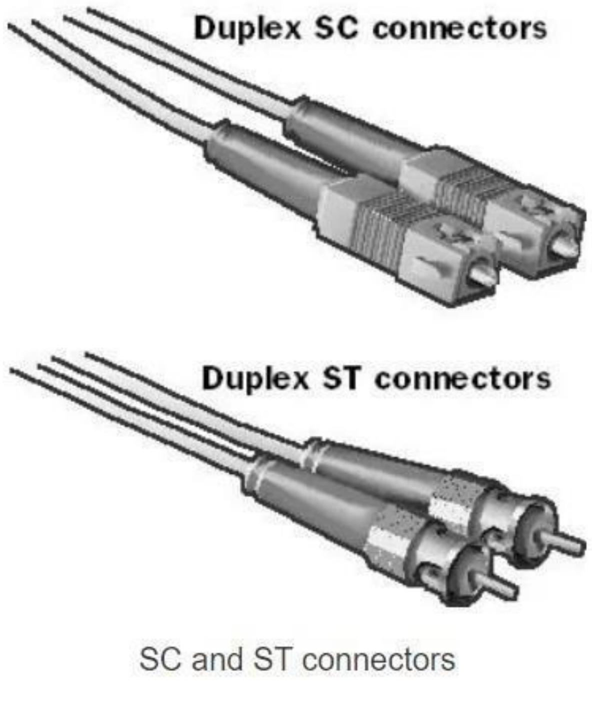
Networks must have two BNC terminators, one BNC T connector per workstation, two BNC cable connector per workstation.

SCST->

SC/ST connectors are used for connecting fiber-optic cabling to networking devices. SC stands for subscriber connector and ST stands for straight tip. See the full article to find more.

Connector types that are generally used for connecting fiber-optic cabling to networking devices. Both are recognized by the Electronic Industries Alliance/Telecommunications Industry Association (EIA/TIA) 568A standard. SC stands for subscriber connector and is a standard-duplex fiber-optic connector with a square molded plastic body and push-pull locking features. SC connectors are typically used in data communication, CATV, and telephony environments. ST stands for straight tip, a high-performance fiber-optic connector with round ceramic ferrules and bayonet locking features. ST connectors are more common than SC connectors.

You can generally use SC and ST connectors with either single-mode or multimode fiber-optic cabling. Coupling receptacles for these connectors come in either panel-mount or free-handing designs. For narrow space installations, you can get 90-degree boot versions instead of straight versions. SC and ST connectors come in both simplex and duplex form.



SC and ST connectors

# PRACTICAL- 03

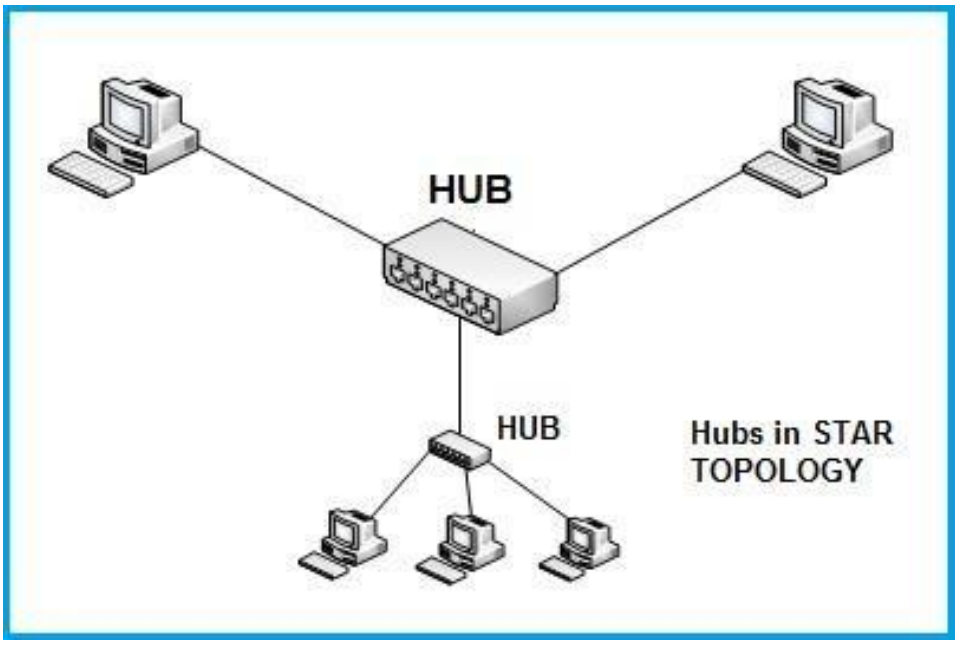
AIM: Recognition of network devices(Switches, Hub, Routers of access point of Wi-Fi)

Network Devices:

Network devices, also known as networking hardware, are physical devices that allow hardware on a computer network to communicate and interact with one another. For example Repeater, Hub, Bridge, Switch, Routers, Gateway, Brouter, and NIC, etc.

Hub –

A hub is a basically multi-port repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations.



Hubs cannot filter data, so data packets are sent to all connected devices. In other words, the collision domain of all hosts connected through Hub remains one. Also, they do not have the intelligence to find out the best path for data packets which leads to inefficiencies and wastage.

Types of Hub:

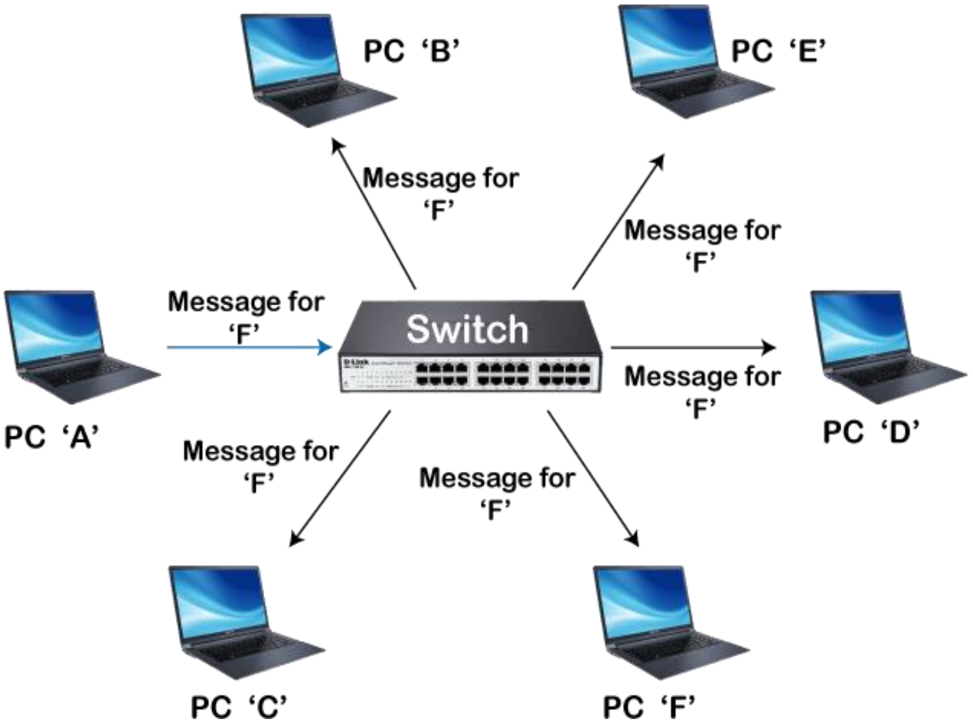
- **Active Hub:-** These are the hubs that have their power supply and can clean, boost, and relay the signal along with the network. It serves both as a repeater as well as a wiring center. These are used to extend the maximum distance between nodes.

- **Passive Hub:-** These are the hubs that collect wiring from nodes and power supply from the active hub. These hubs relay signals onto the network without cleaning and boosting them and can't be used to extend the distance between nodes.

- **Intelligent Hub:-** It works like an active hub and includes remote management capabilities. They also provide flexible data rates to network devices. It also enables an administrator to monitor the traffic passing through the hub and to configure each port in the hub.

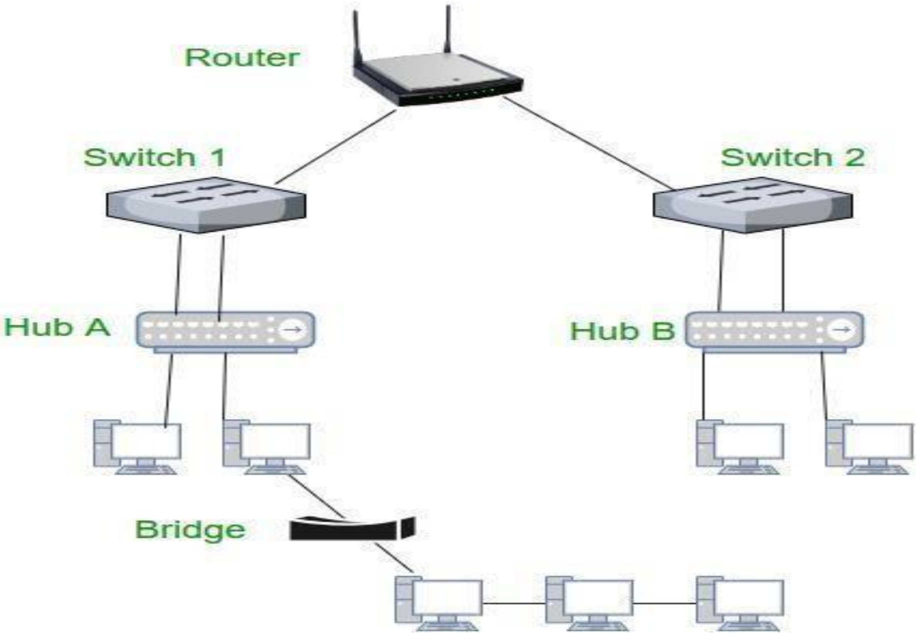
Switch –

A switch is a multiport bridge with a buffer and a design that can boost its efficiency(a large number of ports imply less traffic) and performance. A switch is a data link layer device. The switch can perform error checking before forwarding data, which makes it very efficient as it does not forward packets that have errors and forward good packets selectively to the correct port only. In other words, the switch divides the collision domain of hosts, but the broadcast domain remains the same.

- 

Routers –

A router is a device like a switch that routes data packets based on their IP addresses. The router is mainly a Network Layer device. Routers normally connect LANs and WANs and have a dynamically updating routing table based on which they make decisions on routing the data packets. The router divides the broadcast domains of hosts connected through it.

- 

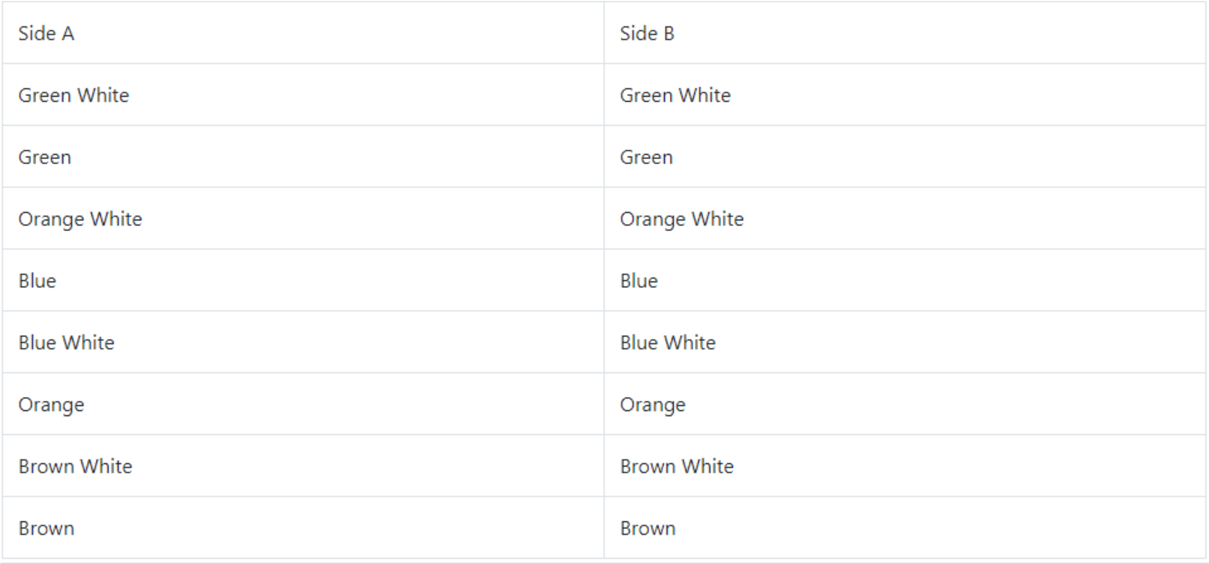
#PRACTICAL – 04

AIM: Making of cross cable and straight cable.

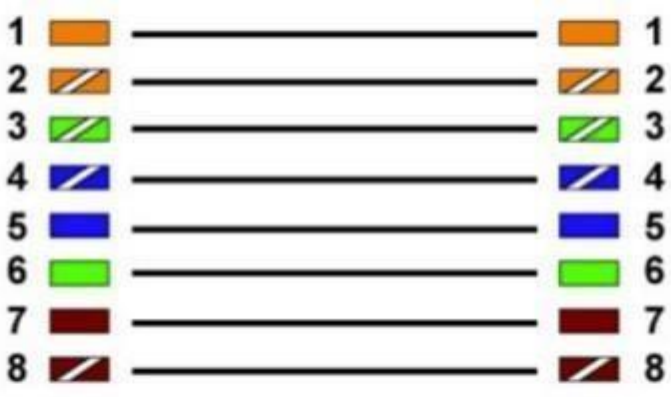
Ethernet straight-through cable

In this cable, wires are placed in the same position at both ends. The wire at pin 1 on one end of the cable connects topin 1 at the other end of the cable. The wire at pin 2 connects to pin 2 on the other end of the cable; and so on.

The following table lists the wire positions of the straight-through cable on both sides.



Side A	Side B
Green White	Green White
Green	Green
Orange White	Orange White
Blue	Blue
Blue White	Blue White
Orange	Orange
Brown White	Brown White
Brown	Brown



The following image shows the straight-through cable.

A straight-through cable is used to connect the followingdevices.

- PC to Switch
- PC to Hub
- Router to Switch
- Switch to Server
- Hub to Server

Ethernet cross-over cable

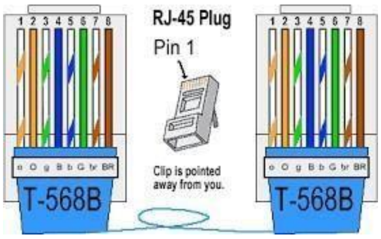
In this cable, transmitting pins of one side connect with thereceiving pins of the other side.

The wire at pin 1 on one end of the cable connects to pin 3 atthe other end of the cable. The wire at pin 2 connects to pin 6 on the other end of the cable. Remaining wires connect inthe same positions at both ends.

The following table lists the wire positions of the cross-overcable on both sides.

Side A	Side B
Green White	Orange White
Green	Orange
Orange White	Green White
Blue	Blue
Blue White	Blue White
Orange	Green
Brown White	Brown White
Brown	Brown

The following image shows the cross-over cable.



The cross-over cable is used to connect the following devices.

- Two computers
- Two hubs
- A hub to a switch
- A cable modem to a router
- Two router interfaces

# PRACTICAL- 05

AIM: Install and configure a network interface card in a workstation

Hardware Installation:

To connect a computer to your network, the computer must havea network interface. Virtually all computers sold in the last 10 years or so have a network interface built-in on themotherboard.

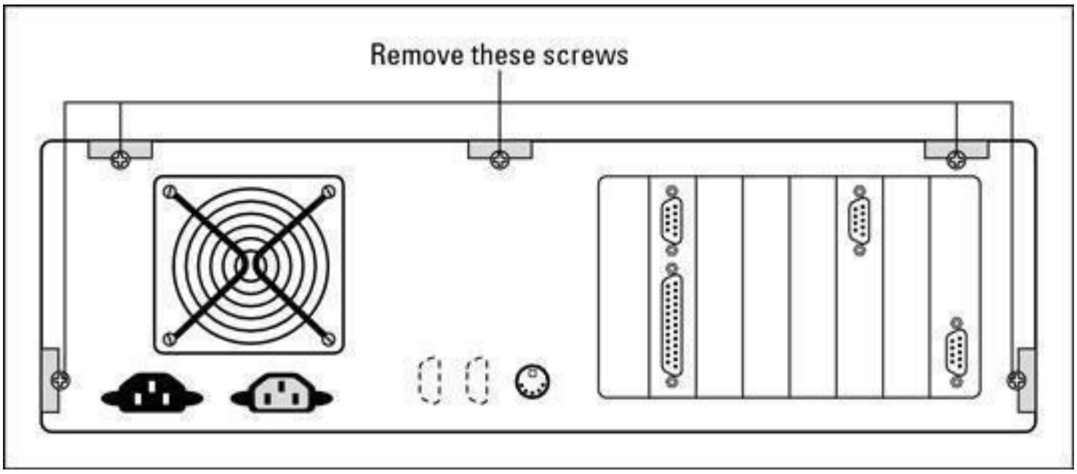
However, you may still encounter the occasional older computerthat doesn’t have a built-in network interface. In that case, you must install a network interface card to enable the computer for your network. Installing a network interface cardis a manageable task, but you have to be willing to roll up your sleeves. If you’ve ever installed one of these cards, youcan probably install a network interface card blindfolded.

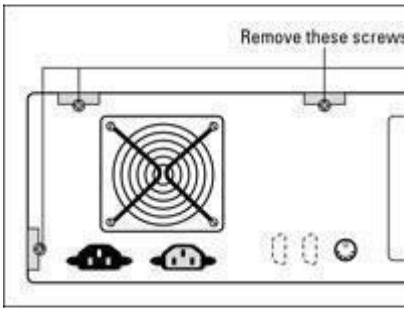
1. Assemble your materials.

   Gather up the network card and the driver disks. Whileyou’re at it, get your Windows installation CD just incase.

2. Shut down Windows, turn off the computer and unplug it. Never work in your computer’s insides with the power on or the power cord plugged in!

3. Remove the cover from your computer.

4. 

5. 

6. You must typically remove a number of screws to open thecover. Put the screws someplace where they won’t wander off.

   If you have a name-brand computer such as a Dell or a Compaq, opening the cover may be trickier than just removing a few screws. You may need to consult the owner’s manual that came with the computer to find outhow to open the case.

7. Find an unused expansion slot inside the computer.

   The expansion slots arelined up in aneat row near theback of the computer; you can’t miss them. Any computerless than five years old should have at least two orthree slots known as *PCI slots.*

8. Remove the metal slot protector from the back of the computer’s chassis.

   If a small retaining screw holds the slot protector inplace, remove the screw and keep it in a safe place because you will need it later. Then pull the slot protector out and discard.

9. Insert the network interface card into the slot.

Line up the connectors on the bottom of the card with theconnectors in the expansion slot and then press the card straight down. Sometimes you have to press uncomfortably hard to get the card to slide into the slot.

10. Secure the network interface card.

Remember that screw you put in a safe place ? Use it tostabilize the network interface card.

11. Put the computer’s case back together.

Watch out for the loose cables inside the computer; you don’t want to pinch them with the case as you slide it back on. Secure the case with the screws that you removedearlier.

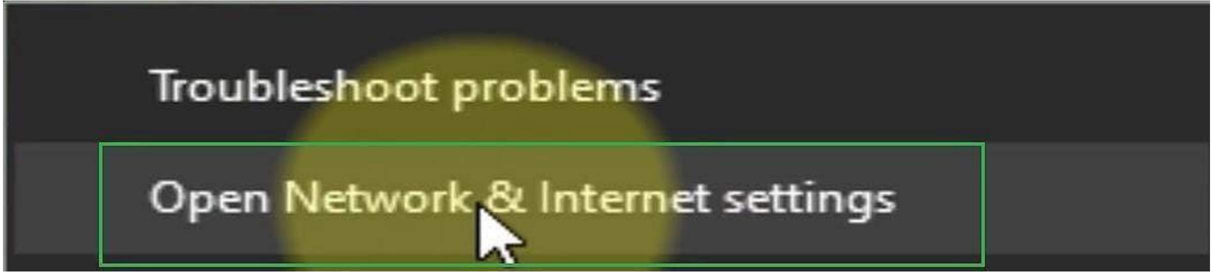
12. Plug in the computer and turn it back on.

If you’re using a Plug and Play card with Windows, the card is automatically configured after you start the computer again. If you’re working with an older computeror an older network interface card, you may need to run an additional software installation program. See the installation instructions that come with the network interface card for details.

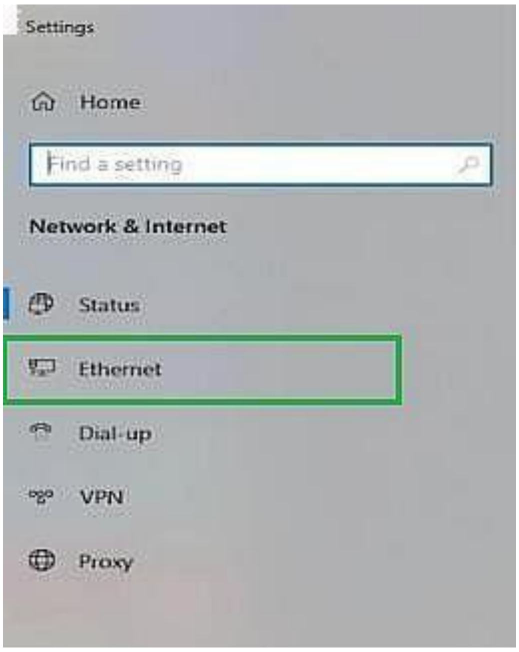
Configuration of Network Interface Card:

Note: Currently, with the Network Interface Card, there is no software provided. As all the cards are now applicable to all the devices. Whatever the operating system is, a Network Interface Card can be used there. As per the user, we need to configure the device. The configuration is simple if it is followed thoroughly.

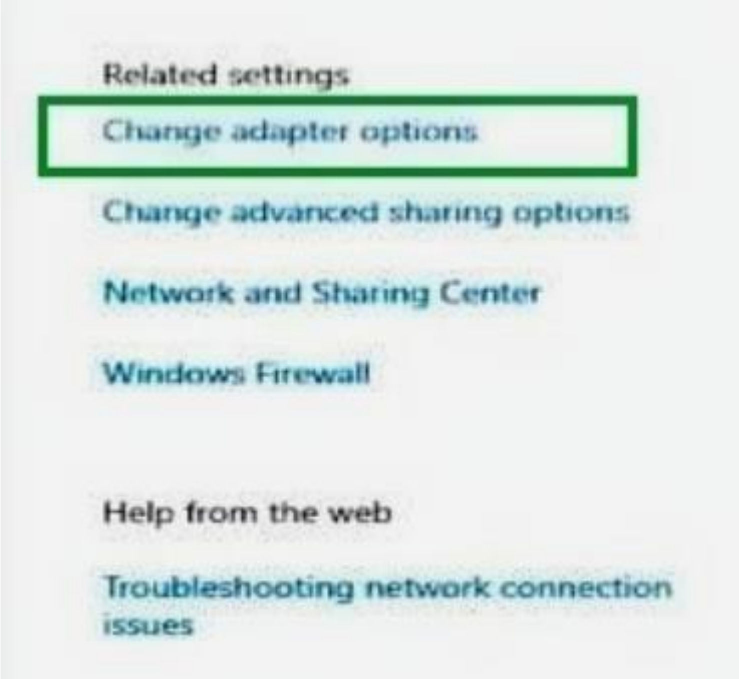
Step 1: After successful hardware installation, you have to click the Internet shortcut sign in the Toolbar. There we have to click on the **Open Network & Internet Settings**. This will help us open more options related to it.



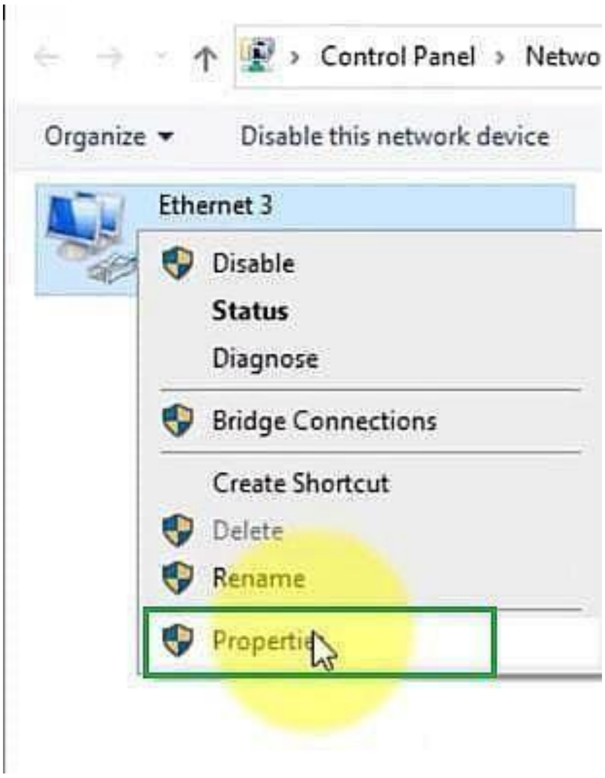
Step 2: There in the settings page, you will find a lot of options present on the left-hand side of the screen. There is an option to present the name Ethernet. You have to click on it.



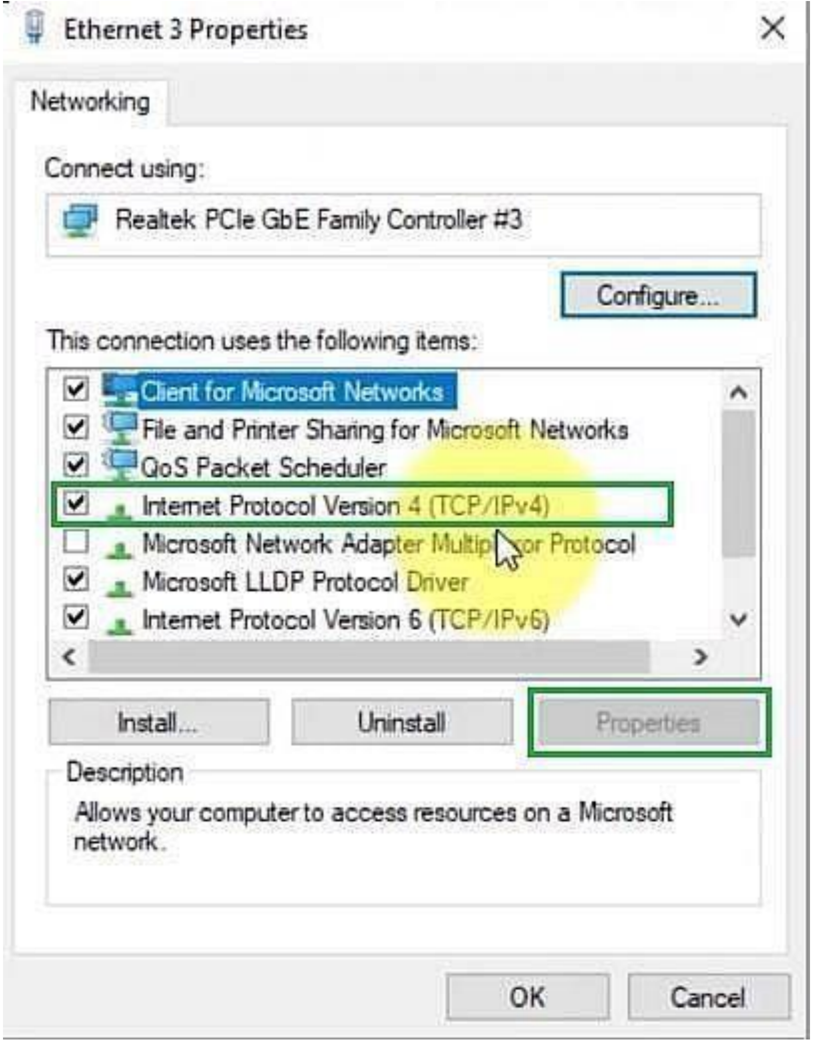
Step 3: After clicking on that, a new window will open. There will be a few more options on the right-hand side of the screen. From there, you will need to click on the **Change Adapter Option.** This will help you get more options.


Related settings
Change adapter options
Change advanced sharing options
Network and Sharing Center
Windows Firewall
Help from the web
Troubleshooting network connection issues

Step 4: There will now be an Ethernet option available. You have to right-click on it. This way, we can see more options related to it. You need to click on the **Properties** option.



Step 5: There will be a lot of options present. For the available option, you need to click on the **Internet Protocol Version**. After clicking on that, you will need to click on the **Properties** option.



Connect using:

Realtek PCIe GbE Family Controller #3

This connection uses the following items:

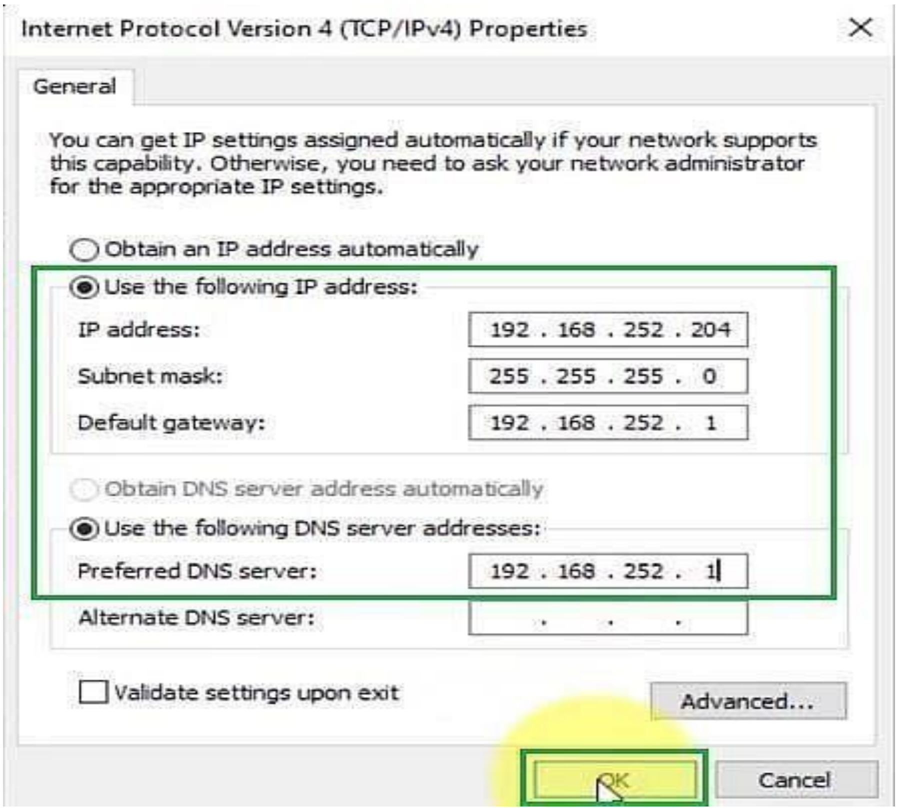
- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☐ Microsoft Network Adapter Multiplexor Protocol
- ☑ Microsoft LLDP Protocol Driver
- ☑ Internet Protocol Version 6 (TCP/IPv6)

Description

Allows your computer to access resources on a Microsoft network.

Step 6: Now, we have to input the IP addresses in the following manner. The user needs to carefully put all the data there. We need to keep the last position vacant. After filling in all the data, we need to click on Ok.

Note: With the Network Interface Card, the company provides a proper sequence of IP Addresses there. If the IP Address is available with the product, then the user needs to provide that data only. Sometimes, the IP Address information is not available with the product. In that case, the user can provide the below IP Addresses. There will be no issues.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 252 . 204

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 252 . 1

○ Obtain DNS server address automatically

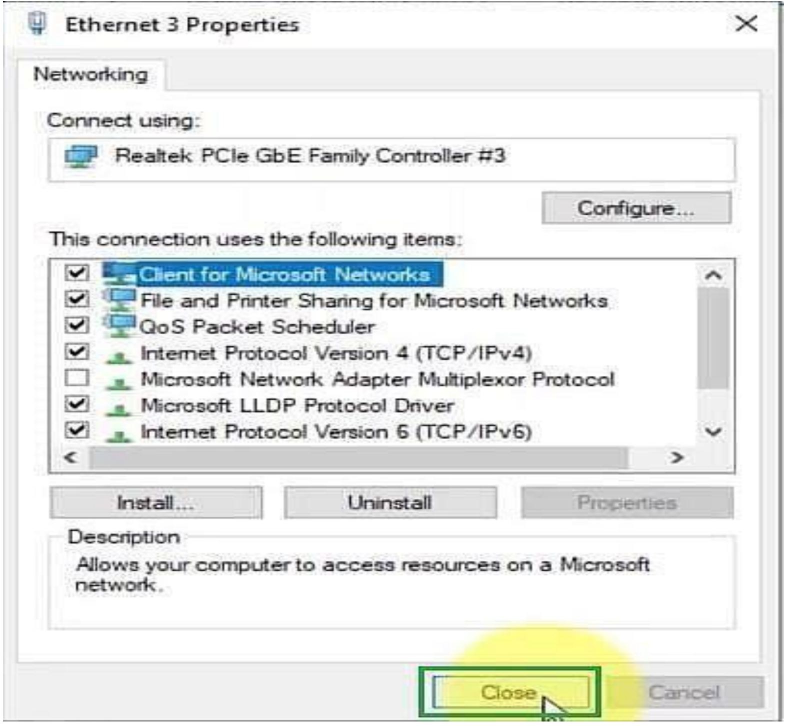
● Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 252 . 1

Alternate DNS server: . . .

□ Validate settings upon exit

Step 7: Now, it will come back to the previous window. From there, you need to press the **Close** button. This will close all the settings.



Ethernet 3 Properties

Networking

Connect using:

Realtek PCIe GbE Family Controller #3

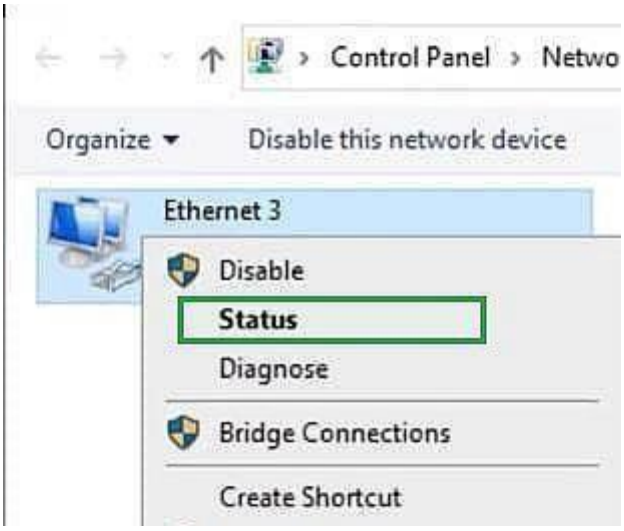
This connection uses the following items:

☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol Version 4 (TCP/IPv4)
□ Microsoft Network Adapter Multiplexor Protocol
☑ Microsoft LLDP Protocol Driver
☑ Internet Protocol Version 6 (TCP/IPv6)

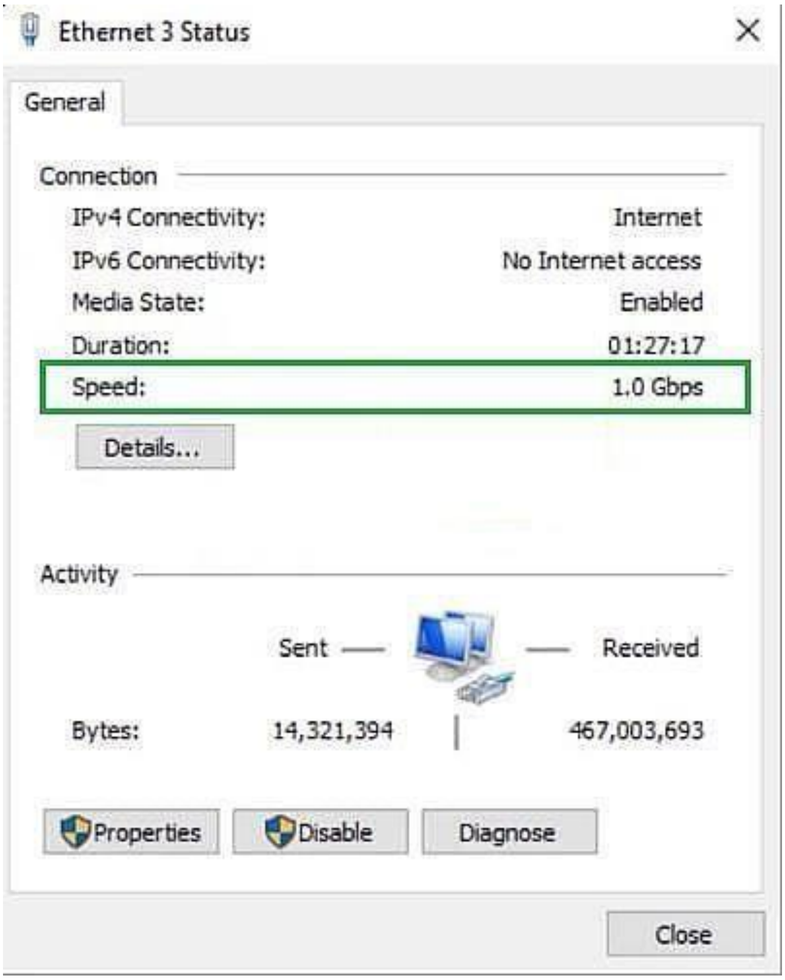
Description

Allows your computer to access resources on a Microsoft network.

Step 8: Now, again, we have to right-click on the Ethernet option. There is an option present called **Status**. You need to click on that.



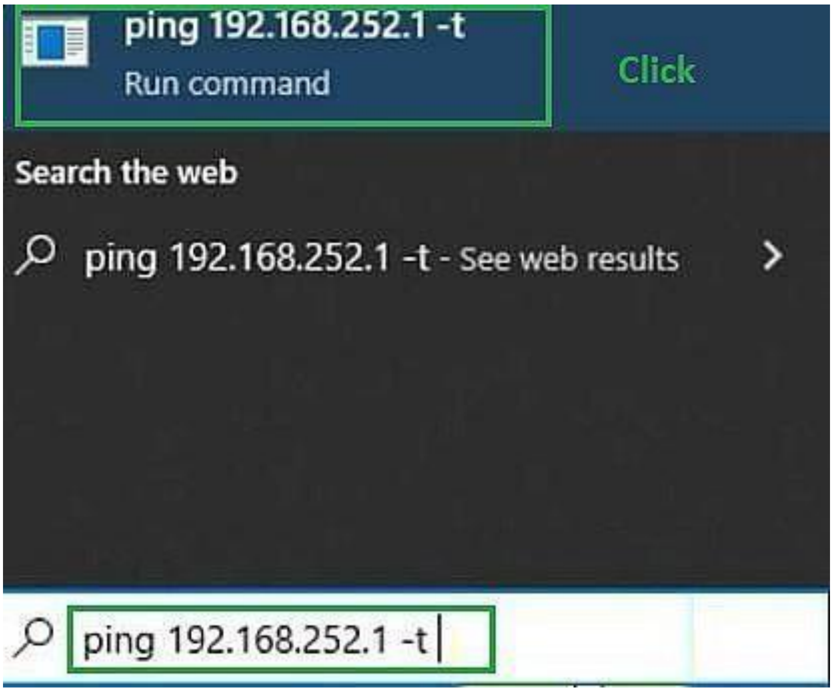
Step 9: There, users will get more information about the internet connection. The internet connection is also available there. We have configured the Network Interface Card.



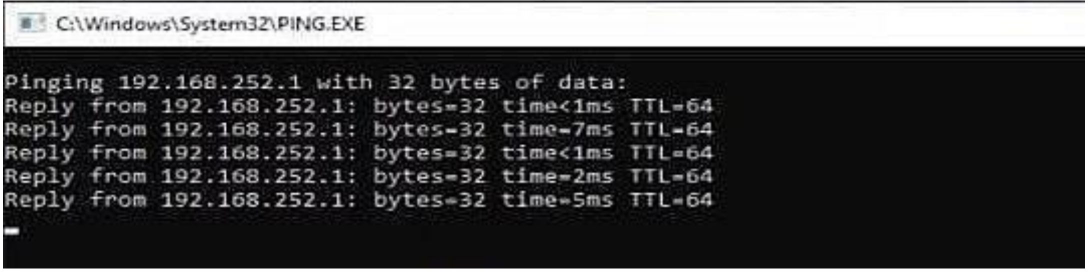
IPv4 Connectivity: Internet
IPv6 Connectivity: No Internet access
Media State: Enabled
Duration: 01:27:17
Speed: 1.0 Gbps
Bytes: 14,321,394 | 467,003,693

Step 10: Now, we have to check the connection status of the Network Interface Card. For that purpose, we can write the below-mentioned command in the search bar of the toolbar. Then you have to click on the command to run inside the Command Prompt. Also, the user can open the Command Prompt & run the same command.

Command: ping 192.168.252.1 -t



Step 11: Then it will open the Command Prompt & provide the output there. This will help us understand the running status of the Network Interface Card.



```
C:\Windows\System32\PING.EXE

Pinging 192.168.252.1 with 32 bytes of data:
Reply from 192.168.252.1: bytes=32 time<1ms TTL=64
Reply from 192.168.252.1: bytes=32 time=7ms TTL=64
Reply from 192.168.252.1: bytes=32 time<1ms TTL=64
Reply from 192.168.252.1: bytes=32 time=2ms TTL=64
Reply from 192.168.252.1: bytes=32 time=5ms TTL=64
```

Hence, we have successfully installed the Network Interface Card on the computer.

#PRACTICAL – 06

AIM: Identify the IP address of a workstation and the class of the address and configure the IP Address ona workstation .

All the computers of the world in the Internet network communicate with each other with underground or underwater cables or wirelessly. If I want to download a file from the internet or load a web page or literally do anything related to the internet, my computer must have an address so that other computers can find and locate mine in order to deliver that particular file or webpage that I am requesting. In technical terms, that address is called **IP Address or InternetProtocol Address**.

Let us understand it with another example, like if someone wants to send you a mail then he/she must have your home address. Similarly, your computer too needs an address so thatother computers on the internet can communicate with each other without the confusion of delivering information to someone else’s computer. And that is why each computer in thisworld has a unique IP Address. Or in other words, an IP address is a unique address that is used to identify computersor nodes on the internet. This address is just a string of numbers written in a certain format. It is generally expressed in the set of numbers for example 192.155.12.1. Here each number in the set is from 0 to 255 range. Or we can say that afull IP address ranges from 0.0.0.0 to 255.255.255.255. And these IP addresses are assign by IANA(known as Internet Corporation For Internet Assigned Numbers Authority).

But what is Internet protocol? This is just a set of rulesthat makes the internetwork. You are able to read this articlebecause your computer or phone has a unique address where the page that you requested (to read this article from GeeksforGeeks) has been delivered successfully.

Working of IP addresses:

The working of IP addresses is similar to other languages. It can also use some set of rules to send information. Using these protocols we can easily send, receive data or files to the connected devices. There are several steps behind the scenes. Let us look at them

- Your device directly requests your Internet Service Provider which then grants your device access to the web.
- And an IP Address is assigned to your device from the given range available.
- Your internet activity goes through your service provider, and that they route it back to you, usingyour IP address.

- Your IP address can change. For example, turning your router on or off can change your IP Address.
- When you are out from your home location your home IP address doesn’t accompany you. It changes as you changethe network of your device.

Types of IP Address

IP Address is of two types:

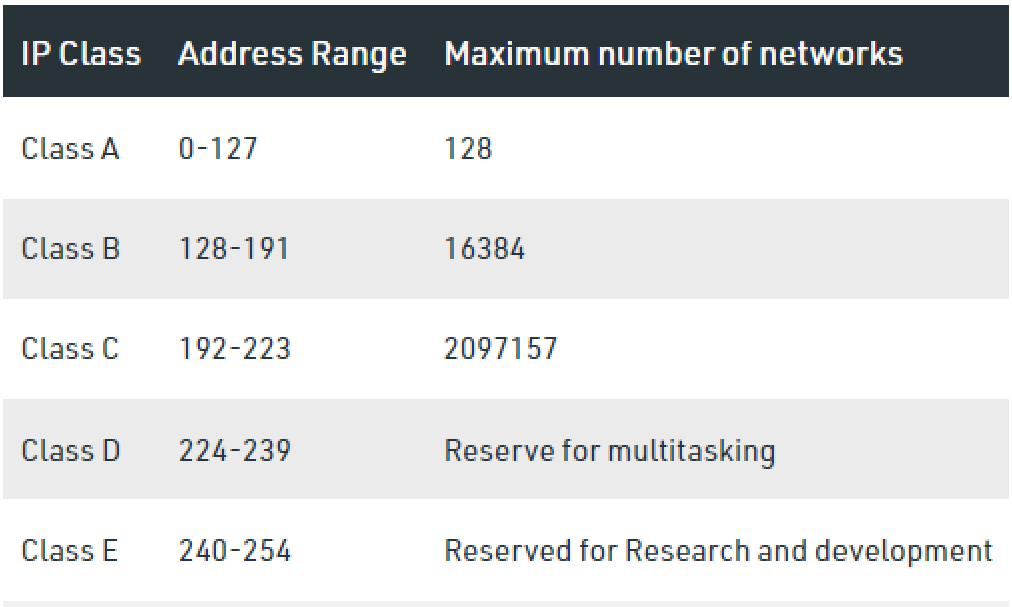
1. IPv4: Internet Protocol version 4. It consists of 4 numbersseparated by the dots. Each number can be from 0-255 in decimal numbers. But computers do not understand decimal numbers, they instead change them to binary numbers which are only 0 and 1. Therefore, in binary, this (0-255) range can be written as (00000000 – 11111111). Since each number N can be represented by a group of 8 digit binary digits. So, a whole IPv4 binary address can be represented by 32-bits of binary digits. In IPv4, a unique sequence of bits is assigned to a computer, so a total of (2^32) devices approximately =4,294,967,296 can be assigned with IPv4.

IPv4 can be written as:

189.123.123.90

Classes of IPv4 Address: There are around 4.3 billion IPv4 addresses and managing all those addresses without any scheme is next to impossible. Let’s understand it with a simple example. If you have to find a word from a language dictionary, how long will you take? Usually, you will takeless than 5 minutes to find that word. You are able to do thisbecause words in the dictionary are organized in alphabetical order. If you have to find out the same word from a dictionarythat doesn’t use any sequence or order to organize the words, it will take an eternity to find the word. If a dictionarywith one billion words without order can be so disastrous,then you can imagine the pain behind finding an address from

4.3 billion addresses. For easier management and assignment IP addresses are organized in numeric order and divided into the following 5 classes :**2. IPv6:** But, there is a problem with theIPv4 address. With IPv4, we can connect only the above number of 4 billion devices uniquely, and apparently, there are much more devices in the world to be connected to the internet. So,gradually we are making our way to **IPv6 Address** which is a 128-bit IP address. In human-friendly form, IPv6 is written asa group of 8 hexadecimal numbers separated with colons(:). Butin the computer-friendly form, it can be written as 128 bitsof 0s and 1s. Since, a unique sequence of binary digits is given to computers, smartphones, and other devices to be connected to the internet. So, via IPv6 a total of (2^128) devices can be assigned with unique addresses which areactually more than enough for upcoming future generations.



IP Class	Address Range	Maximum number of networks
Class A	0-127	128
Class B	128-191	16384
Class C	192-223	2097157
Class D	224-239	Reserve for multitasking
Class E	240-254	Reserved for Research and development

IPv6 can be written as:But, there is a problem with the IPv4 address. With IPv4, we can connect only the above number of 4 billion devices uniquely, and apparently, there are much more devices in the world to be connected to the internet. So, gradually we are making our way to **IPv6 Address** which is a 128-bit IP address. In human-friendly form, IPv6 is written asa group of 8 hexadecimal numbers separated with colons(:).

2011:0bd9:75c5:0000:0000:6b3e:0170:8394

Classification of IP Address

An IP address is classified into the following types:

1. **Public IP Address:** This address is available publicly andit is assigned by your network provider to your router, which further divides it to your devices. Public IP Addresses is of two types :

- **Dynamic IP Address:** When you connect a smartphone or computer to the internet, your Internet Service Provider provides you an IP Address from the range of available IP Addresses. Now, your device has an IP Address and you can simply connect your device to the Internet and send and receive data to and from your device. The very next time when you try to connect to the internet with the same device, your providerprovides you with different IP Addresses to the same device and also from the same available range. Since IPAddress keeps on changing every time when you connect to the internet, it is called Dynamic IP Address.
- **Static IP Address:** Static address never changes. They serve as a permanent internet address. These are usedby DNS servers. What are DNS servers? Actually, these are computers that help you to open a website on your computer. Static IP Address provides information suchas device is located in which continent, which country,which city, and which Internet Service Provider provides internet connection to that particular device. Once, we know who is the ISP, we can trace the locationof the device connected to the internet. Static IP Addresses provide less security than Dynamic IP Addresses because they are easier to track.

2. **Private IP Address:** This is an internal address of yourdevice which are not routed to the internet and no exchange of

data can take place between a private address and theinternet.

3. **Shared IP addresses:** Many websites use shared IP addresses where the traffic is not huge and very much controllable, theydecide to rent it to other similar websites so to make it cost-friendly. Several companies and email sending servers usethe same IP address (within a single mail server) to cut down the cost so that they could save for the time the server is idle.

4. **Dedicated IP addresses:** A dedicated IP Address is an address used by a single company or an individual which gives them certain benefits using a private Secure Sockets Layer (SSL) certificate which is not in the case of a shared IP address. It allows to access the website or log in via File Transfer Protocol (FTP) by IP address instead of its domain name. It increases the performance of the website when the traffic is high. It also protects from a shared IP addressthat is black-listed due to spam.

Lookup IP addresses

To know your public IP, you can simply search “What is my IP?”on google. Other websites will show you equivalent information: they will see your public IP address because, by visiting the location, your router has made an invitation/request and thus revealed the information. the location IP location goes further by showing the name of your Internet Service Provider and your current city.

Finding your device’s private IP Address depends on the OS or platform you are using.

- **On Windows:** Click Start and type “cmd” in the searchbox and run the command prompt. In the black command prompt dialog box type “ipconfig” and press enter. You will be able to see your IP Address there.
- **On Mac:** Go to system preferences and select Network,you will be able to see the information regarding your network which includes your IP Address.

Protect and hide IP address

To secure and hide your IP address from unwanted people alwaysremember the following points:

- Use a proxy server.
- Use a virtual private network (VPN) when using public Wi-Fi, you are traveling, working remotely, or justwant some privacy.
- Change privacy settings on instant messaging applications.
- Create unique passwords.
- Beware of phishing emails and malicious content.
- Use a good and paid antivirus application and keep itup to date.

- When you are using public wifi in a cafe or station or anywhere, you must hide your IP address by using VPN. Getting your IP from public wifi is just a cakewalk forthese hackers and they are very good at stealing all your information while using your computer’s address. There are different phishing techniques in which they email you, call you, SMS you about giving vital information about you. They give links to vicious websites which are pre-rigged. The moment you openthese websites, they steal all your device’s information revealing all the information about you andyour device which are to be kept private. These leaks help the hackers to exploit your device and you and install or download some spyware and malware in your device. But using a good anti-virus gives you web security as well, which will prevent those websites to launch and warn you about the information being passed to these websites.
- It is also not recommended to use torrent or pirated websites which are a threat to your online identity and can compromise your device or mails or any other information about you.

PRACTICAL- 07

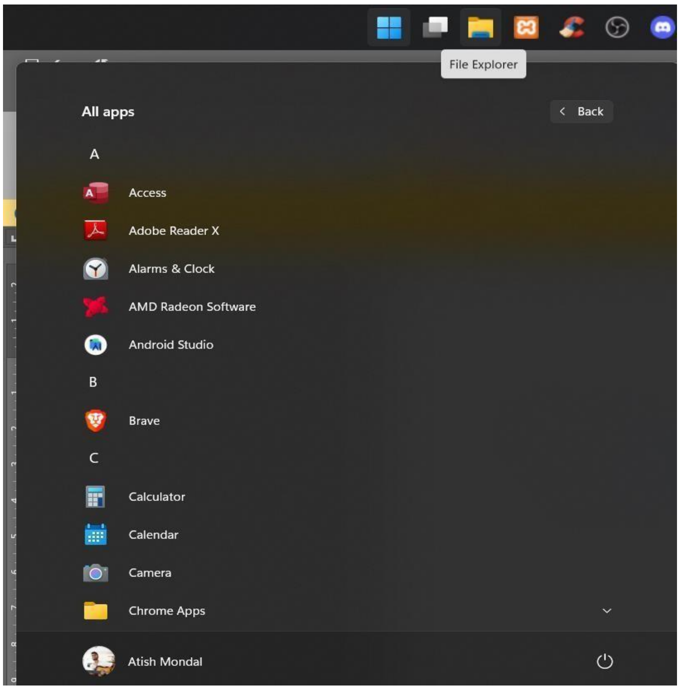
AIM: Managing user account in Windows and linux.

Creating a new user account using windows 10 setting applications you may also create a Microsoft account to be able to transfer account and files between computers

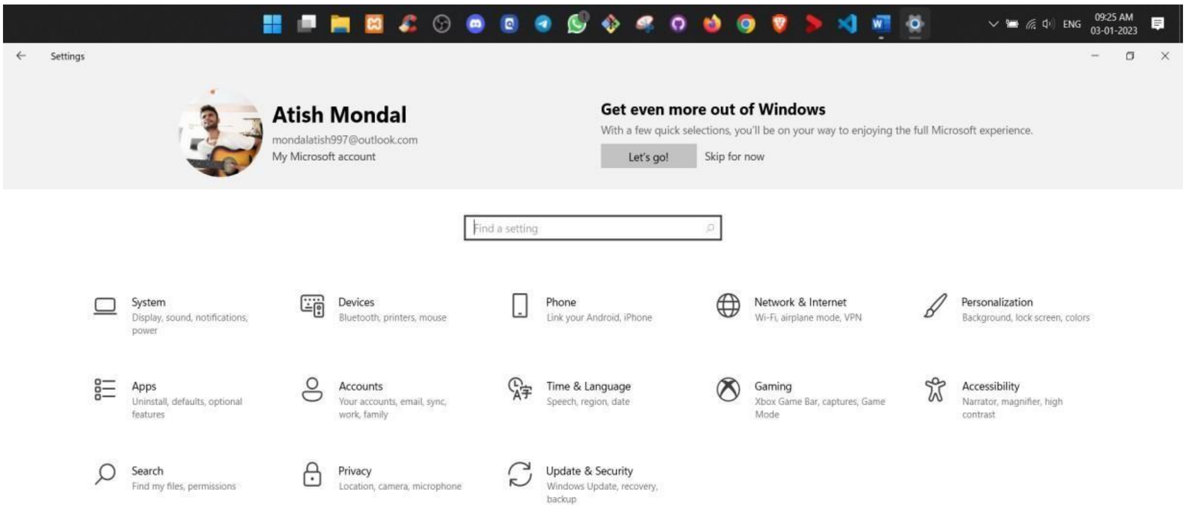
1. Click on the start menu

   In the taskbar

2. Select the settings item integrated by a gear.



3. Click on the accounts



ENG 09:25 AM 03-01-2023

Settings

Atish Mondal
mondalatish997@outlook.com
My Microsoft account

Get even more out of Windows
With a few quick selections, you'll be on your way to enjoying the full Microsoft experience.
Let's go! Skip for now

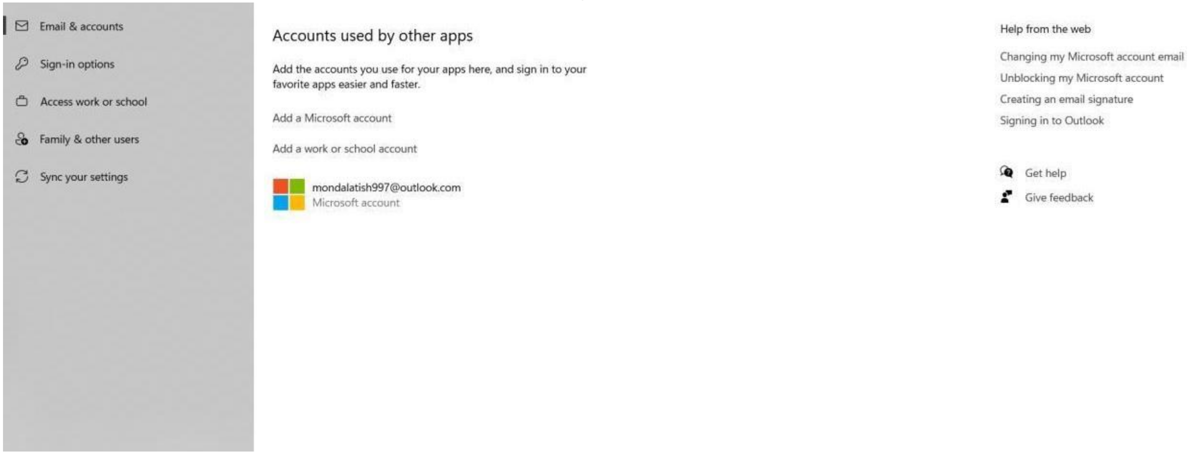
Find a setting

System — Display, sound, notifications, power
Devices — Bluetooth, printers, mouse
Phone — Link your Android, iPhone
Network & Internet — Wi-Fi, airplane mode, VPN
Personalization — Background, lock screen, colors
Apps — Uninstall, defaults, optional features
Accounts — Your accounts, email, sync, work, family
Time & Language — Speech, region, date
Gaming — Xbox Game Bar, captures, Game Mode
Accessibility — Narrator, magnifier, high contrast
Search — Find my files, permissions
Privacy — Location, camera, microphone
Update & Security — Windows Update, recovery, backup

4.

5. Switch to the family and other users category using the panel on the left side of the screen you should see a list of all the current users on the computer

6. Click on the add someone else to the pc button



Email & accounts
Sign-in options
Access work or school
Family & other users
Sync your settings

Accounts used by other apps

Add the accounts you use for your apps here, and sign in to your favorite apps easier and faster.

Add a Microsoft account

Add a work or school account

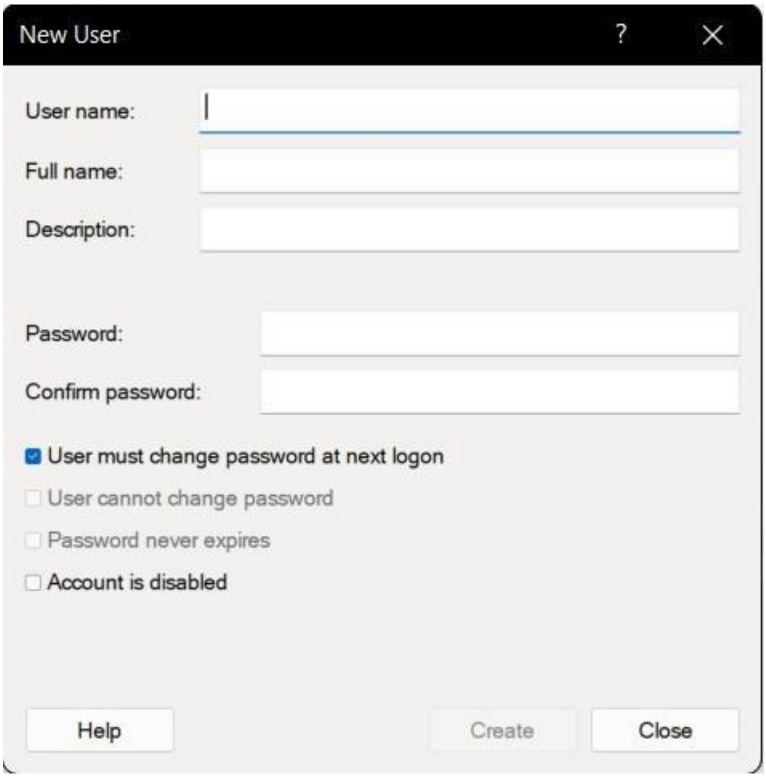
mondalatish997@outlook.com
Microsoft account

Help from the web
Changing my Microsoft account email
Unblocking my Microsoft account
Creating an email signature
Signing in to Outlook

Get help
Give feedback

7.

8. To add a new local user select the I don’t have this person sigh-in option



New User

User name:

Full name:

Description:

Password:

Confirm password:

☑ User must change password at next logon

□ User cannot change password

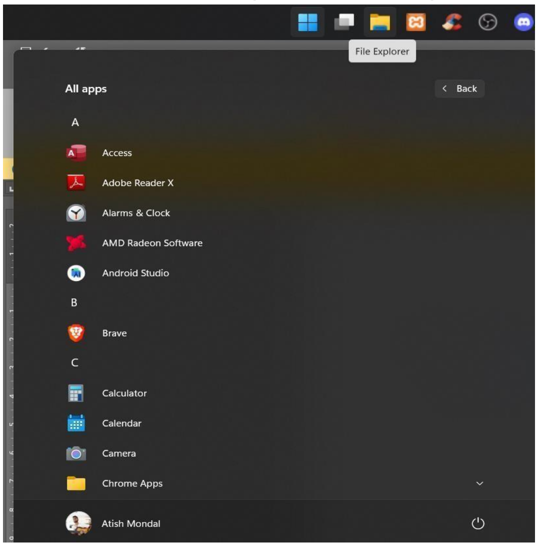
□ Password never expires

□ Account is disabled

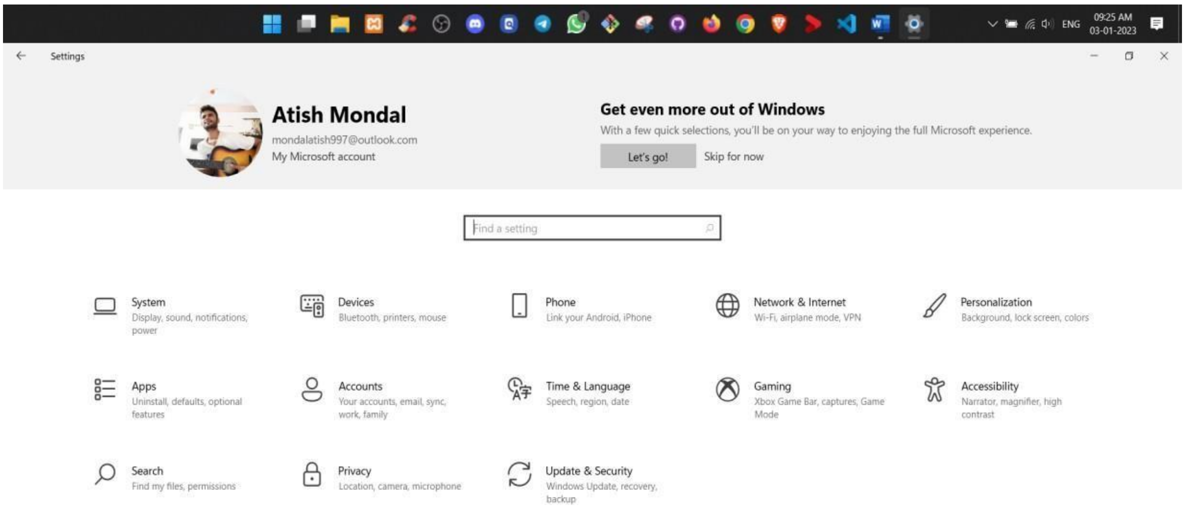
1. Enter the desire user name if needed you can also include a password hint and password. This will give extra privacy to the user in future you are always able to change all of this information
2. Click Next to finalize

How To make local administrator in WINDOWS 10

1. Click on the start menu
   In the taskbar
2. Select the settings item integrated by a gear.



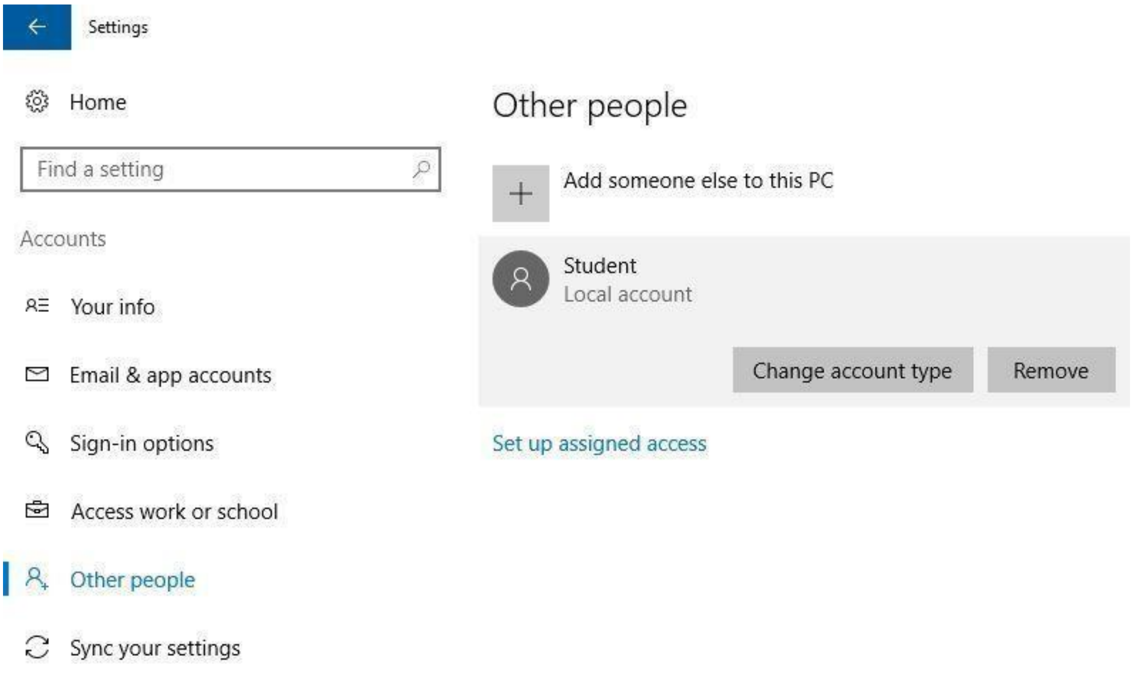
3. Click on the accounts



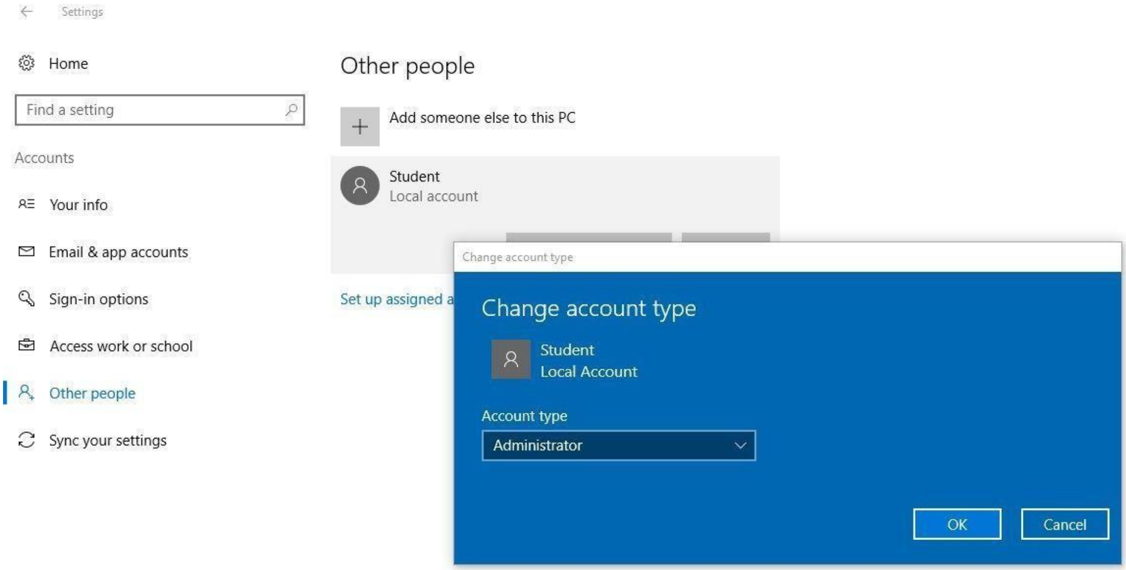
ENG
09:25 AM
03-01-2023
Settings
Atish Mondal
mondalatish997@outlook.com
My Microsoft account
Get even more out of Windows
With a few quick selections, you'll be on your way to enjoying the full Microsoft experience.
Let's go!
Skip for now
Find a setting
System
Display, sound, notifications, power
Devices
Bluetooth, printers, mouse
Phone
Link your Android, iPhone
Network & Internet
Wi-Fi, airplane mode, VPN
Personalization
Background, lock screen, colors
Apps
Uninstall, defaults, optional features
Accounts
Your accounts, email, sync, work, family
Time & Language
Speech, region, date
Gaming
Xbox Game Bar, captures, Game Mode
Accessibility
Narrator, magnifier, high contrast
Search
Find my files, permissions
Privacy
Location, camera, microphone
Update & Security
Windows Update, recovery, backup

4. Switch to the family and other users category using the panel on the left side of the screen you should see a list of all the current users on the computer

5. Select the account you want to modify by clicking on it, once click on it the visible change account type button.



6. Click on the drop down menu and switch from standard user to Administrator

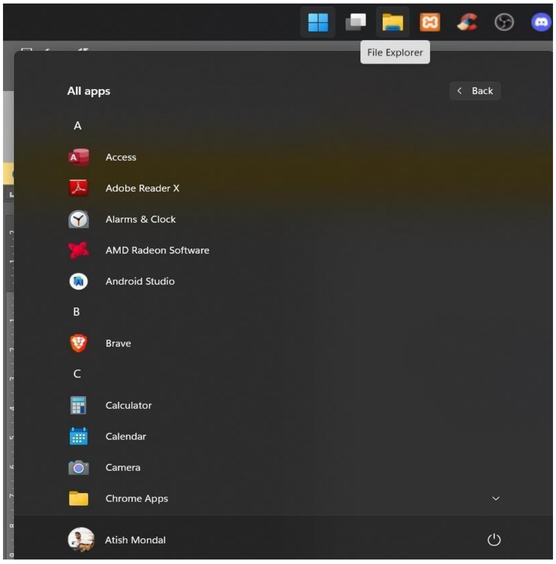


Account type: Administrator

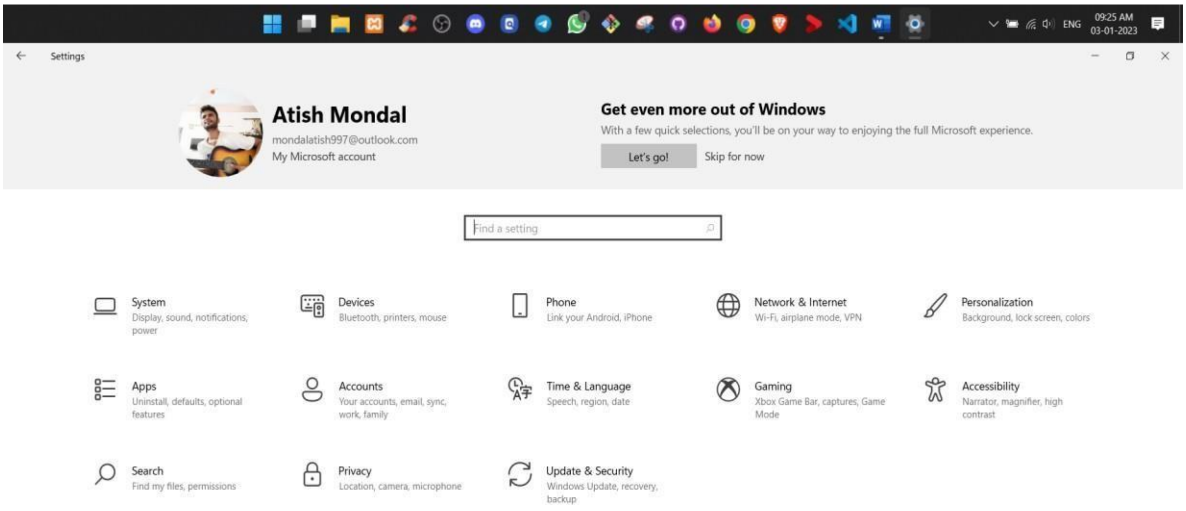
7. Click the Ok button the Account now has full access and administrative permission on the device.

<u>How to remove a local user in windows 10</u>

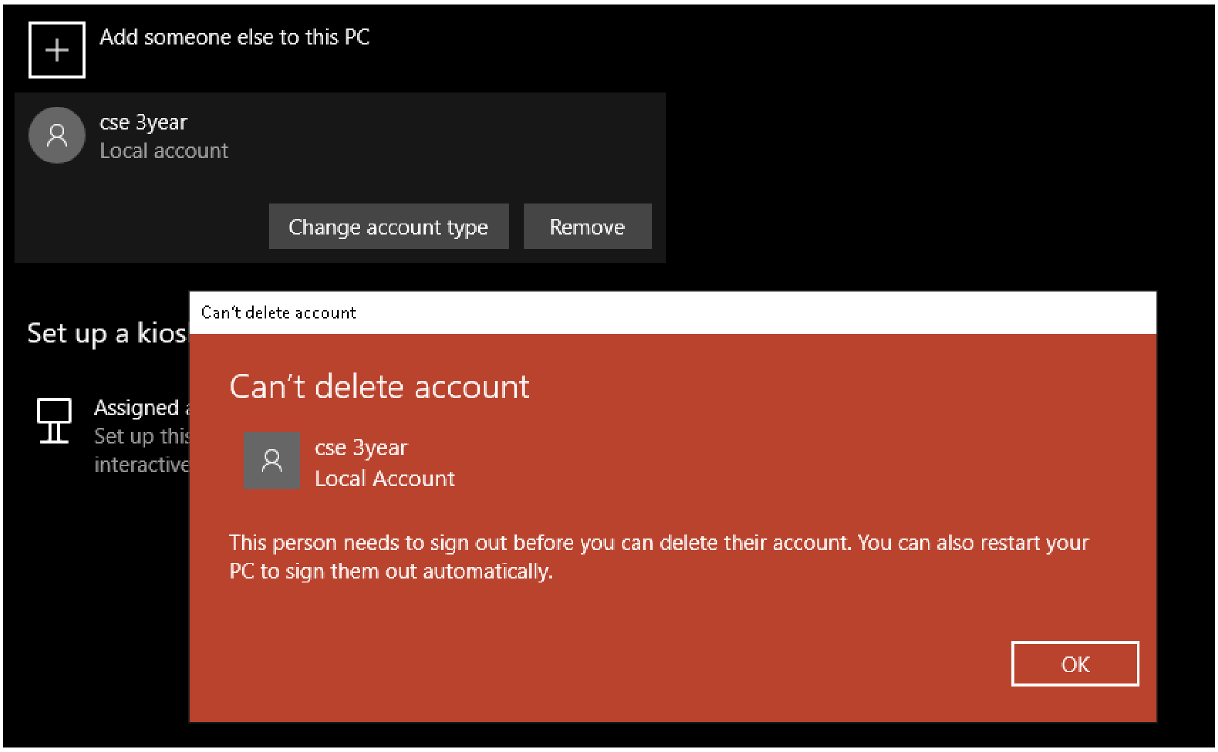
1. Click on the start menu
   In the taskbar
2. Select the settings item integrated by a gear.



3. Click on the accounts


ENG
09:25 AM
03-01-2023
Settings
Atish Mondal
mondalatish997@outlook.com
My Microsoft account
Get even more out of Windows
With a few quick selections, you'll be on your way to enjoying the full Microsoft experience.
Let's go!
Skip for now
Find a setting
System
Display, sound, notifications, power
Devices
Bluetooth, printers, mouse
Phone
Link your Android, iPhone
Network & Internet
Wi-Fi, airplane mode, VPN
Personalization
Background, lock screen, colors
Apps
Uninstall, defaults, optional features
Accounts
Your accounts, email, sync, work, family
Time & Language
Speech, region, date
Gaming
Xbox Game Bar, captures, Game Mode
Accessibility
Narrator, magnifier, high contrast
Search
Find my files, permissions
Privacy
Location, camera, microphone
Update & Security
Windows Update, recovery, backup

4. Switch to the family and other users category using the panel on the left side of the screen you should see a list of all the current users on the computer
5. Select the account you want to delete by clicking on it once click on the now visible remove button



This person needs to sign out before you can delete their account. You can also restart your PC to sign them out automatically.

6. Make sure to remove the warning before clicking the delete account button wait for windows 10 to process your request and remove the local user

User management in linux.

A user is an entity in a linux operating system that can manipulate files and performs several other operations

The commands to manage users in linux are as follows:

1. Use the awk command with –f option we are accessing a file and printing only first column with the help of awk.
2. Using id command you can get the id of any user name every user has an id assign to it and the user is identify with the help of this id.
3. Using passwd command to assign a password to a user after using this command we have to enter the new password for the user and then the password get updated to the new password.
4. The command to change the user id for a user

   Syntax: user mod –u new_id user_name

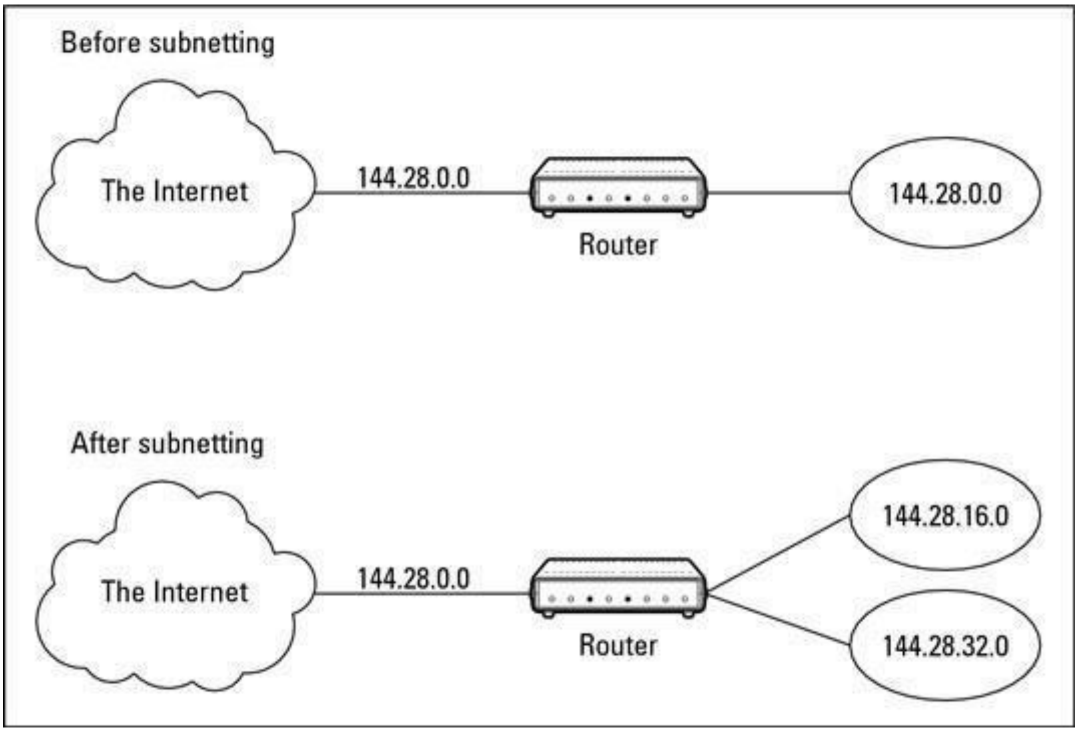
#PRACTICAL – 08

AIM: Study and Demonstration of subnetting of IP address.

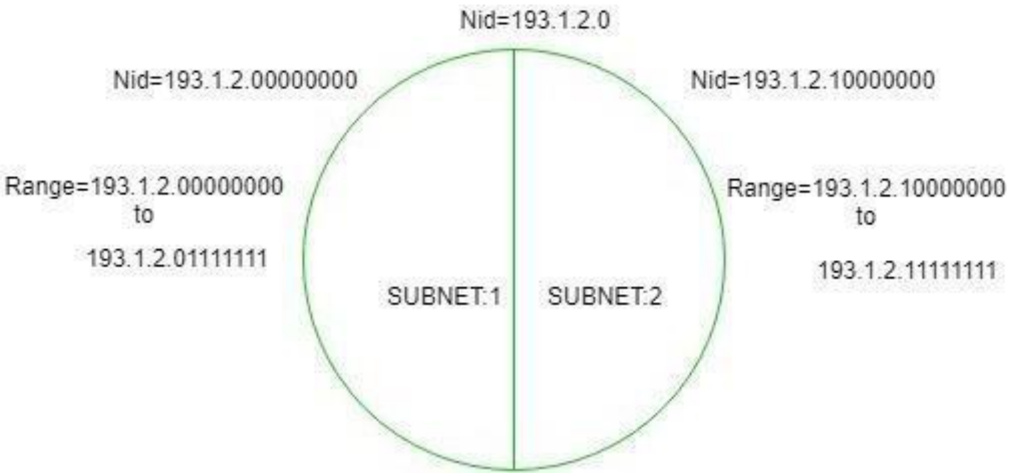
When a bigger network is divided into smaller networks, to maintain security, then that is known as Subnetting.

So, maintenance is easier for smaller networks.

For example, if we consider a class A address, the possible number of hosts is 2^{24} for each network, it is obvious that it is difficult to maintain such a huge number of hosts, but it would be quite easier to maintain if we divide the network into small parts.



Now, let's talk about dividing a network into two parts: To divide a network into two parts, you need to choose one bit for each Subnet from the host ID part.



In the above diagram, there are two Subnets.

Note: It is a class C IP so, there are 24 bits in the network id part and 8 bits in the host id part.

Subnetting for a network should be done in such a way that it does not affect the network bits. In class C the first 3 octets are network bits so it remains as it is.

- **For Subnet-1:** The first bit which is chosen from the host id part is zero and the range will be from (193.1.2.00000000 till you get all 1's in the host ID part i.e, 193.1.2.01111111) except for the first bit which is chosen zero for subnet id part. Thus, the range of subnet-1:

```
193.1.2.0 to 193.1.2.127
```

Subnet id of Subnet-1 is : 193.1.2.0

Direct Broadcast id of Subnet-1 is : 193.1.2.127

Total number of host possible is : 126 (Out of 128, 2 id's are used for Subnet id & Direct Broadcast id)

Subnet mask of Subnet- 1 is : 255.255.255.128

- **For Subnet-2:** The first bit chosen from the host id part is one and the range will be from (193.1.2.100000000 till you get all 1's in the host ID part i.e, 193.1.2.11111111). Thus, the range of subnet-2:

```
193.1.2.128 to 193.1.2.255
```

Subnet id of Subnet-2 is : 193.1.2.128

Direct Broadcast id of Subnet-2 is : 193.1.2.255

Total number of host possible is : 126 (Out of 128, 2 id's are used for Subnet id & Direct Broadcast id)

Subnet mask of Subnet- 2 is : 255.255.255.192

Finally, after using the subnetting the total number of usable hosts are reduced from 254 to 252.

Note:

1. To divide a network into four (2^2) parts you need to choose two bits from the host id part for each subnet i.e, (00, 01, 10, 11).
2. To divide a network into eight (2^3) parts you need to choose three bits from the host id part for each subnet i.e, (000, 001, 010, 011, 100, 101, 110, 111) and so on.
3. We can say that if the total number of subnets in a network increases the total number of usable hosts decreases.

Along with the advantage there is a small disadvantage for subnetting that is, before subnetting to find the IP address first network id is found then host id followed by process id, but after subnetting first network id is found then subnet id then host id and finally process id by this the computation increases.

Example1. An organization is assigned a class C network address of 201.35.2.0. It uses a netmask of 255.255.255.192 to divide this into sub-networks. Which of the following is/are valid host IP addresses?

```
A. 201.35.2.129

B. 201.35.2.191

C. 201.35.2.255

D. Both (A) and (C)
```

Solution:

Converting the last octet of the netmask into the binary form:

255.255.255.**11**000000

Converting the last octet of option A into the binary form: 201.35.2.**10**000001

Converting the last octet of option B into the binary form: 201.35.2.**10**111111

Converting the last octet of option C into the binary form: 201.35.2.**11**111111

From the above, we see that Option B and C is not a valid host IP address (as they are broadcast address of a subnetwork)

and OPTION A is not a broadcast address and it can be assigned to a host IP.

Example 2. An organization has a class C network address of 201.32.64.0. It uses a subnet mask of 255.255.255.248. Which of the following is NOT a valid broadcast address for any subnetworks?

A. 201.32.64.135

B. 201.32.64.240

C. 201.32.64.207

D. 201.32.64.231

Solution:

Converting the last octet of the netmask into the binary form:
255.255.255.**11111**000

Converting the last octet of option A into the binary form:
201.32.64.**10000**111

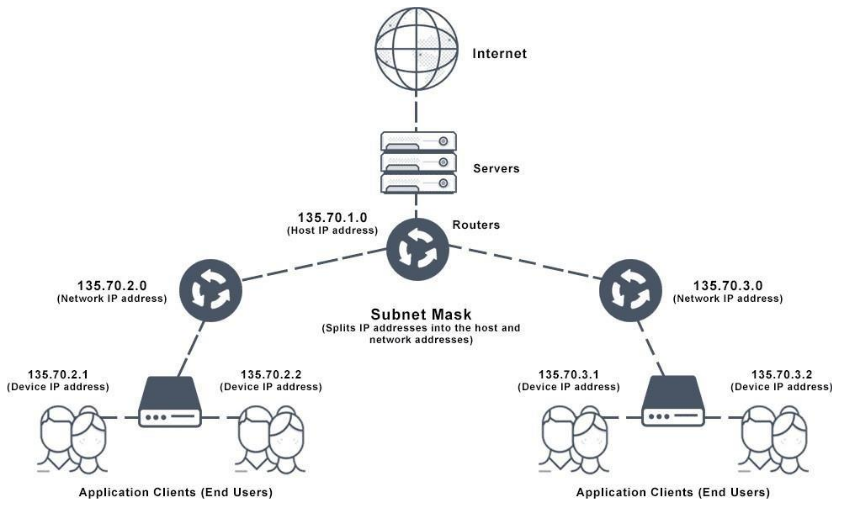
Converting the last octet of option B into the binary form:
201.32.64.**11110**000

Converting the last octet of option C into the binary form:
201.32.64.**11001**111

Converting the last octet of option D into the binary form:
201.32.64.**11100**111

From the above, we can see that, in OPTION A, C, and D all the host bits are 1 and give the valid broadcast address of subnetworks.

and OPTION B the last three bits of the Host address are not 1 therefore it's not a valid broadcast address.

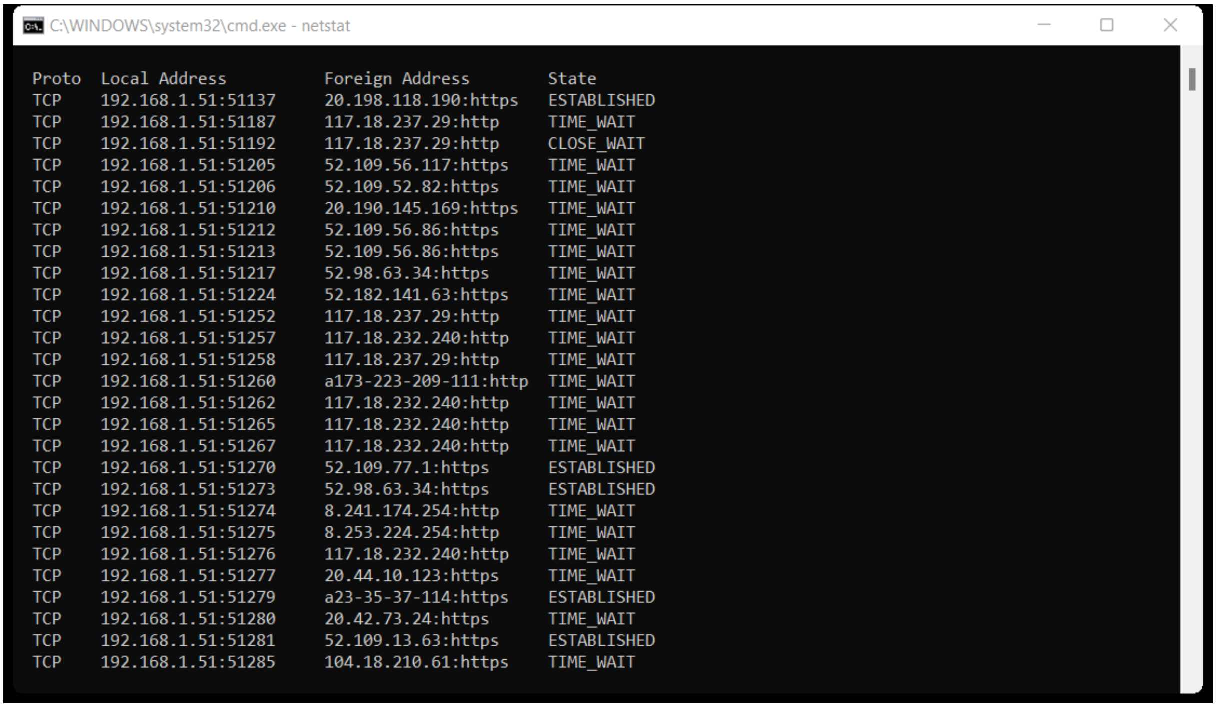


PRACTICAL- 09

Aim :- Use of netstat and its options.

The netstat command is a networking tool used for troubleshooting and configuration that can also serve as monitoring tool for connections over the network both incoming and outgoing connections, routing tables, port listening and usage statics are common use for this command.

It is used to display current network connections and port activity on the computer.

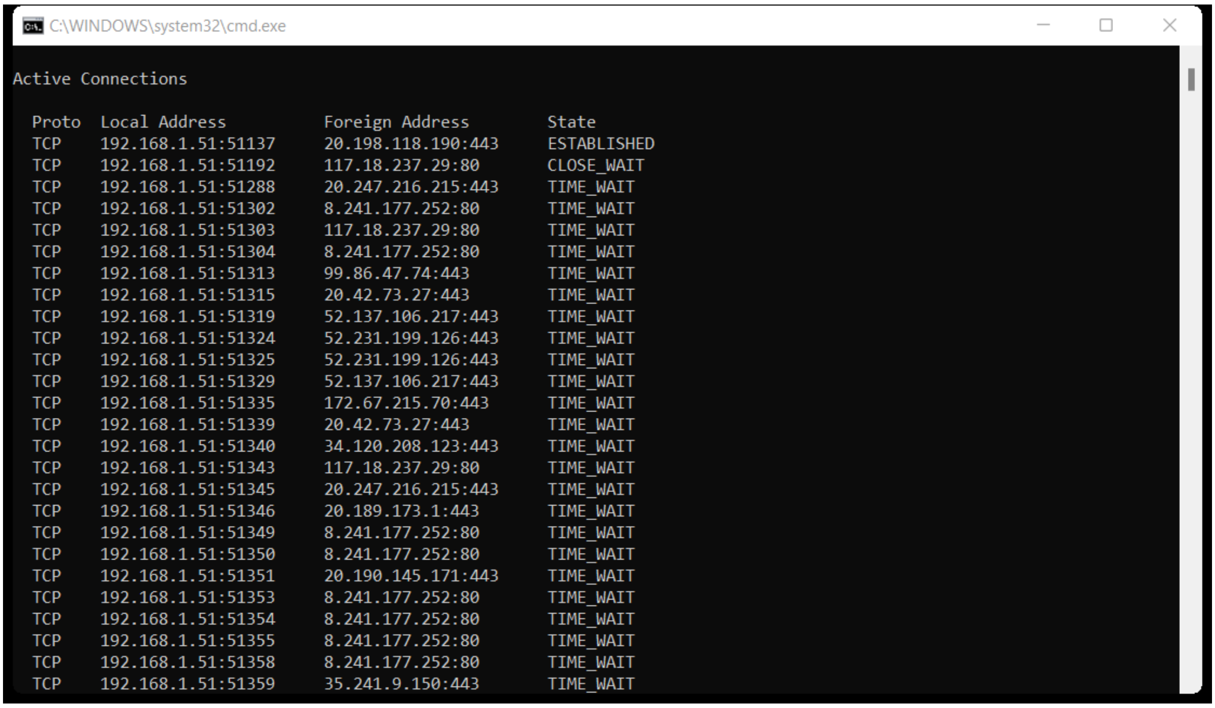


```
  Proto  Local Address          Foreign Address        State
  TCP    192.168.1.51:51137     20.198.118.190:https   ESTABLISHED
  TCP    192.168.1.51:51187     117.18.237.29:http     TIME_WAIT
  TCP    192.168.1.51:51192     117.18.237.29:http     CLOSE_WAIT
  TCP    192.168.1.51:51205     52.109.56.117:https    TIME_WAIT
  TCP    192.168.1.51:51206     52.109.52.82:https     TIME_WAIT
  TCP    192.168.1.51:51210     20.190.145.169:https   TIME_WAIT
  TCP    192.168.1.51:51212     52.109.56.86:https     TIME_WAIT
  TCP    192.168.1.51:51213     52.109.56.86:https     TIME_WAIT
  TCP    192.168.1.51:51217     52.98.63.34:https      TIME_WAIT
  TCP    192.168.1.51:51224     52.182.141.63:https    TIME_WAIT
  TCP    192.168.1.51:51252     117.18.237.29:http     TIME_WAIT
  TCP    192.168.1.51:51257     117.18.232.240:http    TIME_WAIT
  TCP    192.168.1.51:51258     117.18.237.29:http     TIME_WAIT
  TCP    192.168.1.51:51260     a173-223-209-111:http  TIME_WAIT
  TCP    192.168.1.51:51262     117.18.232.240:http    TIME_WAIT
  TCP    192.168.1.51:51265     117.18.232.240:http    TIME_WAIT
  TCP    192.168.1.51:51267     117.18.232.240:http    TIME_WAIT
  TCP    192.168.1.51:51270     52.109.77.1:https      ESTABLISHED
  TCP    192.168.1.51:51273     52.98.63.34:https      ESTABLISHED
  TCP    192.168.1.51:51274     8.241.174.254:http     TIME_WAIT
  TCP    192.168.1.51:51275     8.253.224.254:http     TIME_WAIT
  TCP    192.168.1.51:51276     117.18.232.240:http    TIME_WAIT
  TCP    192.168.1.51:51277     20.44.10.123:https     TIME_WAIT
  TCP    192.168.1.51:51279     a23-35-37-114:https    ESTABLISHED
  TCP    192.168.1.51:51280     20.42.73.24:https      TIME_WAIT
  TCP    192.168.1.51:51281     52.109.13.63:https     ESTABLISHED
  TCP    192.168.1.51:51285     104.18.210.61:https    TIME_WAIT
```

- **TCP** is a protocol.
- **local IP address** of the computer along with the port no. used with that particular network.
- **Foreign address :-** the IP address and the port no. of the remote computer to which the socket is connected. The names that corresponds to the IP address and the port are shown unless the –n

parameter is specified. If the port is not yet established the port no. is shown as an * .\

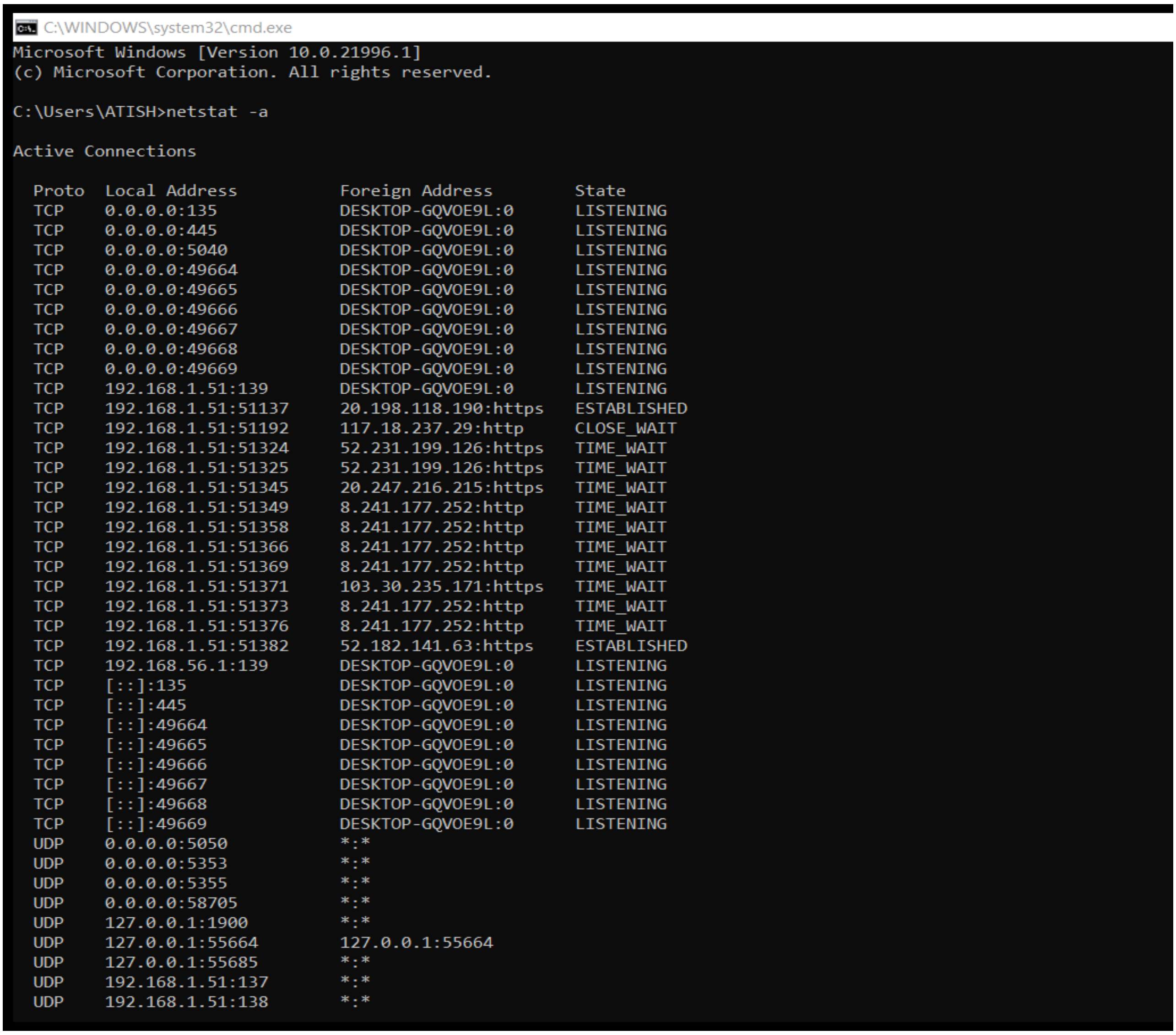
Netstat –n :- netstat can be combine with sub commands or switches to alter the output netstat –n will show only numbers not the name.



```
Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    192.168.1.51:51137     20.198.118.190:443     ESTABLISHED
  TCP    192.168.1.51:51192     117.18.237.29:80       CLOSE_WAIT
  TCP    192.168.1.51:51288     20.247.216.215:443     TIME_WAIT
  TCP    192.168.1.51:51302     8.241.177.252:80       TIME_WAIT
  TCP    192.168.1.51:51303     117.18.237.29:80       TIME_WAIT
  TCP    192.168.1.51:51304     8.241.177.252:80       TIME_WAIT
  TCP    192.168.1.51:51313     99.86.47.74:443        TIME_WAIT
  TCP    192.168.1.51:51315     20.42.73.27:443        TIME_WAIT
  TCP    192.168.1.51:51319     52.137.106.217:443     TIME_WAIT
  TCP    192.168.1.51:51324     52.231.199.126:443     TIME_WAIT
  TCP    192.168.1.51:51325     52.231.199.126:443     TIME_WAIT
  TCP    192.168.1.51:51329     52.137.106.217:443     TIME_WAIT
  TCP    192.168.1.51:51335     172.67.215.70:443      TIME_WAIT
  TCP    192.168.1.51:51339     20.42.73.27:443        TIME_WAIT
  TCP    192.168.1.51:51340     34.120.208.123:443     TIME_WAIT
  TCP    192.168.1.51:51343     117.18.237.29:80       TIME_WAIT
  TCP    192.168.1.51:51345     20.247.216.215:443     TIME_WAIT
  TCP    192.168.1.51:51346     20.189.173.1:443       TIME_WAIT
  TCP    192.168.1.51:51349     8.241.177.252:80       TIME_WAIT
  TCP    192.168.1.51:51350     8.241.177.252:80       TIME_WAIT
  TCP    192.168.1.51:51351     20.190.145.171:443     TIME_WAIT
  TCP    192.168.1.51:51353     8.241.177.252:80       TIME_WAIT
  TCP    192.168.1.51:51354     8.241.177.252:80       TIME_WAIT
  TCP    192.168.1.51:51355     8.241.177.252:80       TIME_WAIT
  TCP    192.168.1.51:51358     8.241.177.252:80       TIME_WAIT
  TCP    192.168.1.51:51359     35.241.9.150:443       TIME_WAIT
```

If we do a netstat with a –n switch the output is very fast in fact its instant this is because it does not use DNS to resolve numbers to names. It only shows numbers instead of showing the names of the computer. It only shows their IP address and same they goes with ports it only shows the port no. and not the port names.

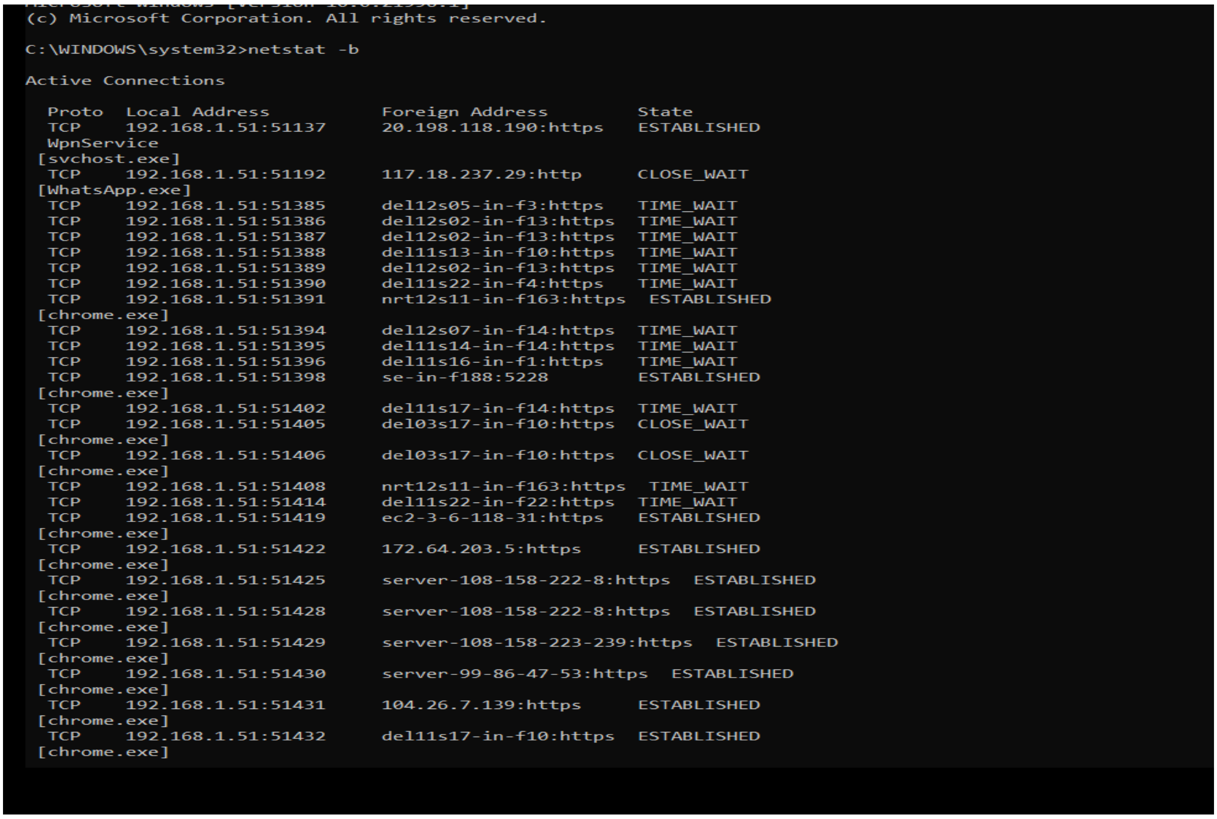
Netstat –a :- It display active connections and which TCP and UDP ports are listening for the connections.



```
Microsoft Windows [Version 10.0.21996.1]
(c) Microsoft Corporation. All rights reserved.

C:\Users\ATISH>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            DESKTOP-GQVOE9L:0      LISTENING
  TCP    0.0.0.0:445            DESKTOP-GQVOE9L:0      LISTENING
  TCP    0.0.0.0:5040           DESKTOP-GQVOE9L:0      LISTENING
  TCP    0.0.0.0:49664          DESKTOP-GQVOE9L:0      LISTENING
  TCP    0.0.0.0:49665          DESKTOP-GQVOE9L:0      LISTENING
  TCP    0.0.0.0:49666          DESKTOP-GQVOE9L:0      LISTENING
  TCP    0.0.0.0:49667          DESKTOP-GQVOE9L:0      LISTENING
  TCP    0.0.0.0:49668          DESKTOP-GQVOE9L:0      LISTENING
  TCP    0.0.0.0:49669          DESKTOP-GQVOE9L:0      LISTENING
  TCP    192.168.1.51:139       DESKTOP-GQVOE9L:0      LISTENING
  TCP    192.168.1.51:51137     20.198.118.190:https   ESTABLISHED
  TCP    192.168.1.51:51192     117.18.237.29:http     CLOSE_WAIT
  TCP    192.168.1.51:51324     52.231.199.126:https   TIME_WAIT
  TCP    192.168.1.51:51325     52.231.199.126:https   TIME_WAIT
  TCP    192.168.1.51:51345     20.247.216.215:https   TIME_WAIT
  TCP    192.168.1.51:51349     8.241.177.252:http     TIME_WAIT
  TCP    192.168.1.51:51358     8.241.177.252:http     TIME_WAIT
  TCP    192.168.1.51:51366     8.241.177.252:http     TIME_WAIT
  TCP    192.168.1.51:51369     8.241.177.252:http     TIME_WAIT
  TCP    192.168.1.51:51371     103.30.235.171:https   TIME_WAIT
  TCP    192.168.1.51:51373     8.241.177.252:http     TIME_WAIT
  TCP    192.168.1.51:51376     8.241.177.252:http     TIME_WAIT
  TCP    192.168.1.51:51382     52.182.141.63:https    ESTABLISHED
  TCP    192.168.56.1:139       DESKTOP-GQVOE9L:0      LISTENING
  TCP    [::]:135               DESKTOP-GQVOE9L:0      LISTENING
  TCP    [::]:445               DESKTOP-GQVOE9L:0      LISTENING
  TCP    [::]:49664             DESKTOP-GQVOE9L:0      LISTENING
  TCP    [::]:49665             DESKTOP-GQVOE9L:0      LISTENING
  TCP    [::]:49666             DESKTOP-GQVOE9L:0      LISTENING
  TCP    [::]:49667             DESKTOP-GQVOE9L:0      LISTENING
  TCP    [::]:49668             DESKTOP-GQVOE9L:0      LISTENING
  TCP    [::]:49669             DESKTOP-GQVOE9L:0      LISTENING
  UDP    0.0.0.0:5050           *:*
  UDP    0.0.0.0:5353           *:*
  UDP    0.0.0.0:5355           *:*
  UDP    0.0.0.0:58705          *:*
  UDP    127.0.0.1:1900         *:*
  UDP    127.0.0.1:55664        127.0.0.1:55664
  UDP    127.0.0.1:55685        *:*
  UDP    192.168.1.51:137       *:*
  UDP    192.168.1.51:138       *:*
```

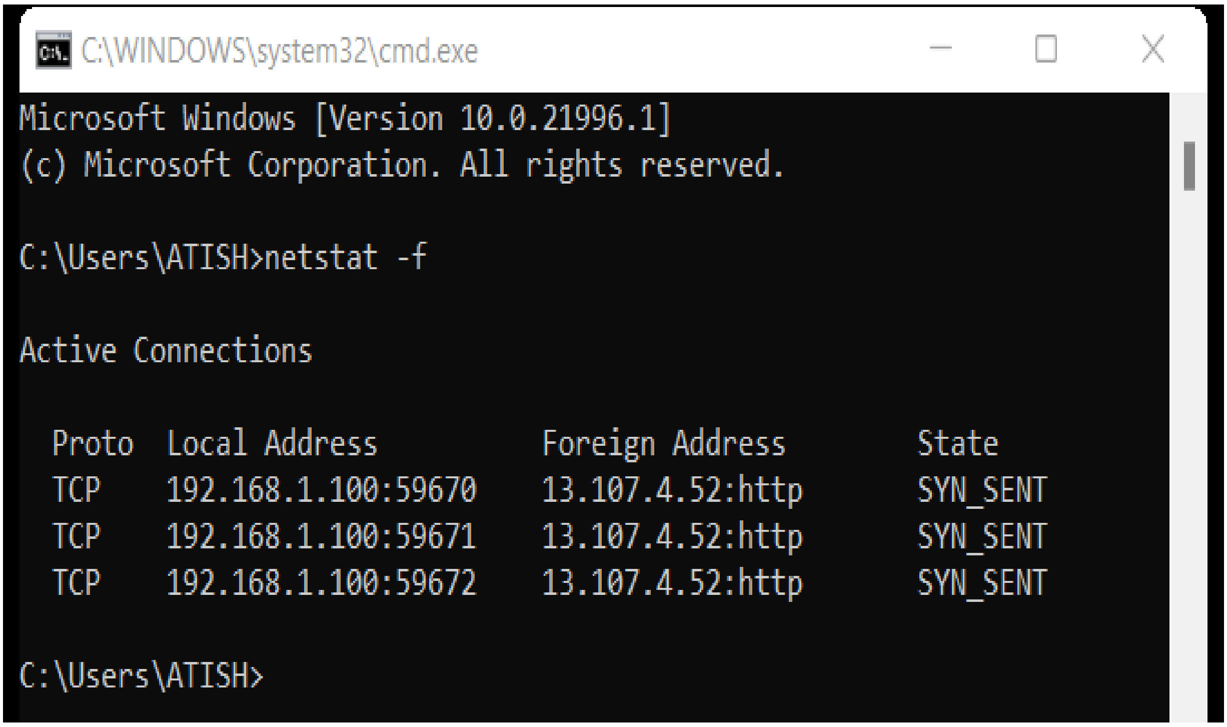
It shows all TCP and UDP ports on the top we see TCP and UDP ports on the bottom . the IP address of all zeros is over computer and the reason while it zero because it means that the port is not listening on a specific IP address. It listening all available IP addresses on all network interface.

Netstat –b :- it display which program is used to make the connection .



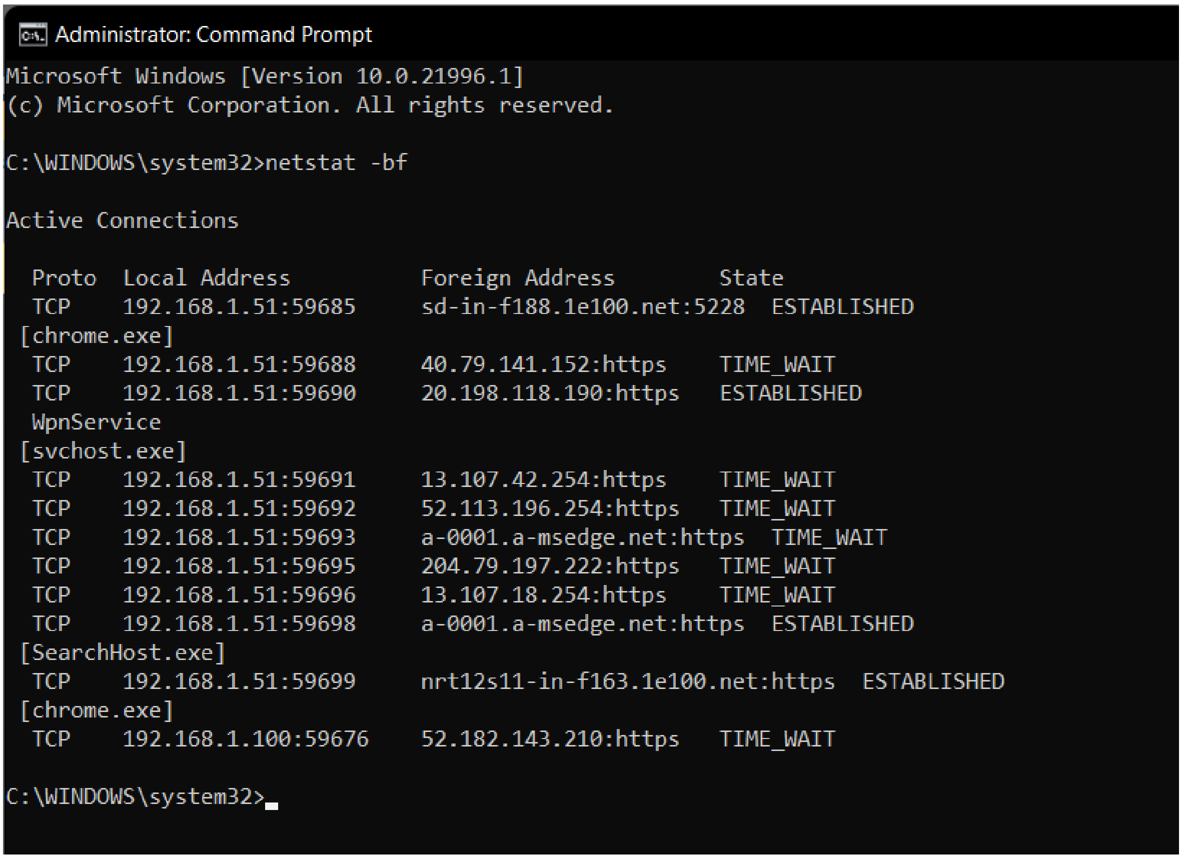
```
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>netstat -b

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    192.168.1.51:51137     20.198.118.190:https   ESTABLISHED
  WpnService
 [svchost.exe]
  TCP    192.168.1.51:51192     117.18.237.29:http     CLOSE_WAIT
 [WhatsApp.exe]
  TCP    192.168.1.51:51385     del12s05-in-f3:https   TIME_WAIT
  TCP    192.168.1.51:51386     del12s02-in-f13:https  TIME_WAIT
  TCP    192.168.1.51:51387     del12s02-in-f13:https  TIME_WAIT
  TCP    192.168.1.51:51388     del11s13-in-f10:https  TIME_WAIT
  TCP    192.168.1.51:51389     del12s02-in-f13:https  TIME_WAIT
  TCP    192.168.1.51:51390     del11s22-in-f4:https   TIME_WAIT
  TCP    192.168.1.51:51391     nrt12s11-in-f163:https  ESTABLISHED
 [chrome.exe]
  TCP    192.168.1.51:51394     del12s07-in-f14:https  TIME_WAIT
  TCP    192.168.1.51:51395     del11s14-in-f14:https  TIME_WAIT
  TCP    192.168.1.51:51396     del11s16-in-f1:https   TIME_WAIT
  TCP    192.168.1.51:51398     se-in-f188:5228        ESTABLISHED
 [chrome.exe]
  TCP    192.168.1.51:51402     del11s17-in-f14:https  TIME_WAIT
  TCP    192.168.1.51:51405     del03s17-in-f10:https  CLOSE_WAIT
 [chrome.exe]
  TCP    192.168.1.51:51406     del03s17-in-f10:https  CLOSE_WAIT
 [chrome.exe]
  TCP    192.168.1.51:51408     nrt12s11-in-f163:https  TIME_WAIT
  TCP    192.168.1.51:51414     del11s22-in-f22:https  TIME_WAIT
  TCP    192.168.1.51:51419     ec2-3-6-118-31:https   ESTABLISHED
 [chrome.exe]
  TCP    192.168.1.51:51422     172.64.203.5:https     ESTABLISHED
 [chrome.exe]
  TCP    192.168.1.51:51425     server-108-158-222-8:https  ESTABLISHED
 [chrome.exe]
  TCP    192.168.1.51:51428     server-108-158-222-8:https  ESTABLISHED
 [chrome.exe]
  TCP    192.168.1.51:51429     server-108-158-223-239:https  ESTABLISHED
 [chrome.exe]
  TCP    192.168.1.51:51430     server-99-86-47-53:https  ESTABLISHED
 [chrome.exe]
  TCP    192.168.1.51:51431     104.26.7.139:https     ESTABLISHED
 [chrome.exe]
  TCP    192.168.1.51:51432     del11s17-in-f10:https  ESTABLISHED
 [chrome.exe]
```

Netstat –f :- It display fully qualified domain name in the foreign address column.



```
Microsoft Windows [Version 10.0.21996.1]
(c) Microsoft Corporation. All rights reserved.

C:\Users\ATISH>netstat -f

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    192.168.1.100:59670    13.107.4.52:http       SYN_SENT
  TCP    192.168.1.100:59671    13.107.4.52:http       SYN_SENT
  TCP    192.168.1.100:59672    13.107.4.52:http       SYN_SENT

C:\Users\ATISH>
```

Netstat -bf :- It shows the details of both the netstat -b and netstat -f.



```
Microsoft Windows [Version 10.0.21996.1]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>netstat -bf

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    192.168.1.51:59685     sd-in-f188.1e100.net:5228  ESTABLISHED
 [chrome.exe]
  TCP    192.168.1.51:59688     40.79.141.152:https    TIME_WAIT
  TCP    192.168.1.51:59690     20.198.118.190:https   ESTABLISHED
  WpnService
 [svchost.exe]
  TCP    192.168.1.51:59691     13.107.42.254:https    TIME_WAIT
  TCP    192.168.1.51:59692     52.113.196.254:https   TIME_WAIT
  TCP    192.168.1.51:59693     a-0001.a-msedge.net:https  TIME_WAIT
  TCP    192.168.1.51:59695     204.79.197.222:https   TIME_WAIT
  TCP    192.168.1.51:59696     13.107.18.254:https    TIME_WAIT
  TCP    192.168.1.51:59698     a-0001.a-msedge.net:https  ESTABLISHED
 [SearchHost.exe]
  TCP    192.168.1.51:59699     nrt12s11-in-f163.1e100.net:https  ESTABLISHED
 [chrome.exe]
  TCP    192.168.1.100:59676    52.182.143.210:https   TIME_WAIT

C:\WINDOWS\system32>
```

#PRACTICAL - 10

AIM: Connectivity troubleshooting using PING, IPCONFIG, IFCONFIG.

Ping (Packet Internet Groper) is a method for determining communication latency between two networks. Simply put, pingis a method of determining latency or the amount of time it takes for data to travel between two devices or across a network. As communication latency decreases, communicationeffectiveness improves.

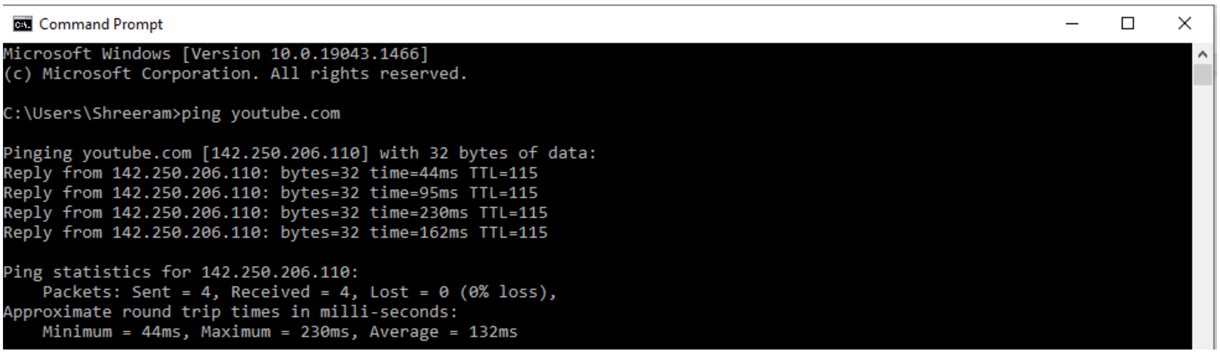
A low ping time is critical in situations where the timely delivery of data is more important than the quantity and quality of the desired information.

How To Get The Ping Value Of Any Site Corresponding To Your Server?

- The ping value represents the strength of a connectionbetween two computers or a network. You can check the ping of any website that corresponds to your computer using a command prompt for Windows or a terminal for Mac.
- Simply type the “ping<space>website name” into the command prompt or terminal to have your system send some data packets to that specific website and then acknowledge you with the value of ping that is occurring within your system and that specific website.

Example –

- As you can see in the image below. I entered “> ping youtube.com”, then my system sent and received four packets of data from YouTube to determine the minimum, maximum, and average ping values, which are 20ms, 22ms,and 21ms, respectively.



```
Microsoft Windows [Version 10.0.19043.1466]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Shreeram>ping youtube.com

Pinging youtube.com [142.250.206.110] with 32 bytes of data:
Reply from 142.250.206.110: bytes=32 time=44ms TTL=115
Reply from 142.250.206.110: bytes=32 time=95ms TTL=115
Reply from 142.250.206.110: bytes=32 time=230ms TTL=115
Reply from 142.250.206.110: bytes=32 time=162ms TTL=115

Ping statistics for 142.250.206.110:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 44ms, Maximum = 230ms, Average = 132ms
```

- So, if an online game streamer has two network options,one with 10ms of ping and 10mbps internet speed, and the other with 100ms of ping and 500mbps internet speed, the gamer will obviously choose the first because he or she wants to interact with the audience in real-time. However, if a person wants to watch YouTube videos and download them, he or she will obviously select the second option in order to speed upthe download process.

ipconfig (standing for "Internet Protocol configuration") is aconsole application program of some computer operating systemsthat displays all current TCP/IP network configuration values and refreshes Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) settings.

The ipconfig command supports the command-line switch /all. This results in more detailed information than ipconfig alone.

An important additional feature of ipconfig is to force refreshing of the DHCP IP address of the host computer to request a different IP address. This is done using two commands in sequence. First, ipconfig /release is executed to force the client to immediately give up its lease by sending the server a DHCP release notification which updates the server's status information and marks the old client's IP address as "available". Then, the command ipconfig /renew is executed to request a new IP address. Where a computer is connected to a cable or DSL modem, it may have to be plugged directly into the modem network port to bypass the router, before using ipconfig /release and turning off the power for aperiod of time, to ensure that the old IP address is taken by another computer.The /flushdns parameter can be used to clear the Domain Name System (DNS) cache to ensure future requests use fresh DNS information by forcing hostnames to be resolved again from scratch.

#PRACTICAL – 11

AIM: Installation of Network Operating System(NOS)

Installation is the most prior to the build server. This installation includes two things, the installation of hardware and software. As a server that will serve the communication between the network, then a minimal server must have two network cards. One for the internal network and the other for external network. Other requirements in the server installation to follow the general installation requirements Operating System, such as:

- The amount of RAM required
- Large hard disk space to be used
- The type and speed of the processor
- Resolution video / screen (required for the operating systemGUI)

This information is normally supplied by the provider of the operating system is concerned. For example, for the OperatingSystem Debian Wheezy with Desktop requires a computer device requirements such as the following.

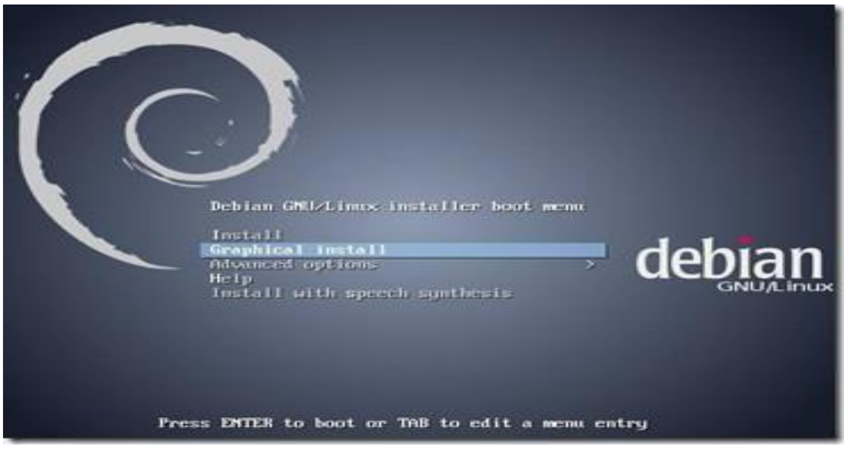
- At least a Pentium IV processor 1 GHz
- A minimum of 128 MB RAM (512 MB is recommended)
- At least 5 GB hard drive

Operating System Installation Methods

The operating system is installed in a particular part of thedisk. This particular location is usually known as a disk partition. There are a number of methods that can be used to install the operating system. The determination of these methods can be based on the condition of the hardware, the operating system’s own requirements and user needs. Here are four choices of operating system installation:

1. **New Installation**

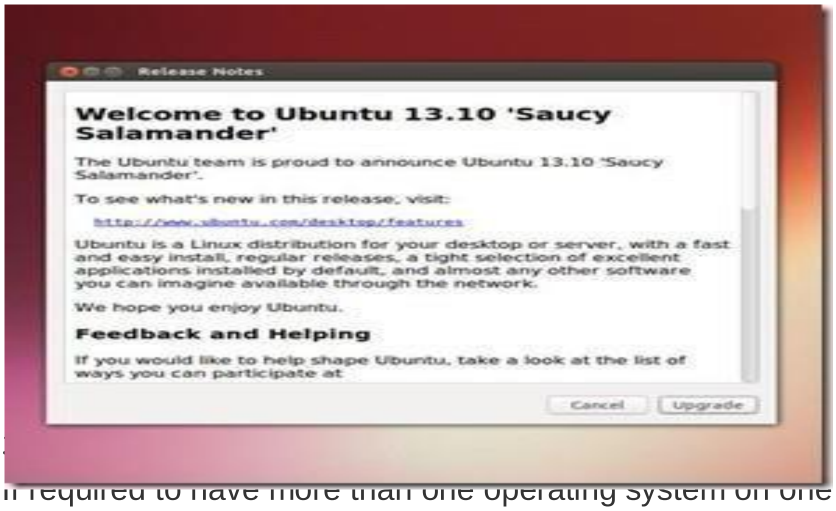
This option can be used when the network to be built is a new network, or the addition of new server hardware that does not support the network operating system available today. If you choose this option then all the data on the selected partition will be deleted. If there are applications that have been installed previously on the old operating system, then later needs to be reinstalled.


Debian GNU/Linux installer boot menu
Install
Graphical install
Advanced options >
Help
Install with speech synthesis
debian
GNU/Linux

Press ENTER to boot or TAB to edit a menu entry

2. Upgrade

This option is widely used in network systems that are alreadyrunning. This option is usually done because of the improvement features of the operating system used, as well as new features that are required. By selecting this option already installed applications that previously would likely still be used after the upgrade. This upgrade option will onlyreplace the files of the previous operating system with a new one.



Welcome to Ubuntu 13.10 'Saucy Salamander'

The Ubuntu team is proud to announce Ubuntu 13.10 'Saucy Salamander'.

To see what's new in this release, visit:

http://www.ubuntu.com/desktop/features

Ubuntu is a Linux distribution for your desktop or server, with a fast and easy install, regular releases, a tight selection of excellent applications installed by default, and almost any other software you can imagine available through the network.

We hope you enjoy Ubuntu.

Feedback and Helping

If you would like to help shape Ubuntu, take a look at the list of ways you can participate at

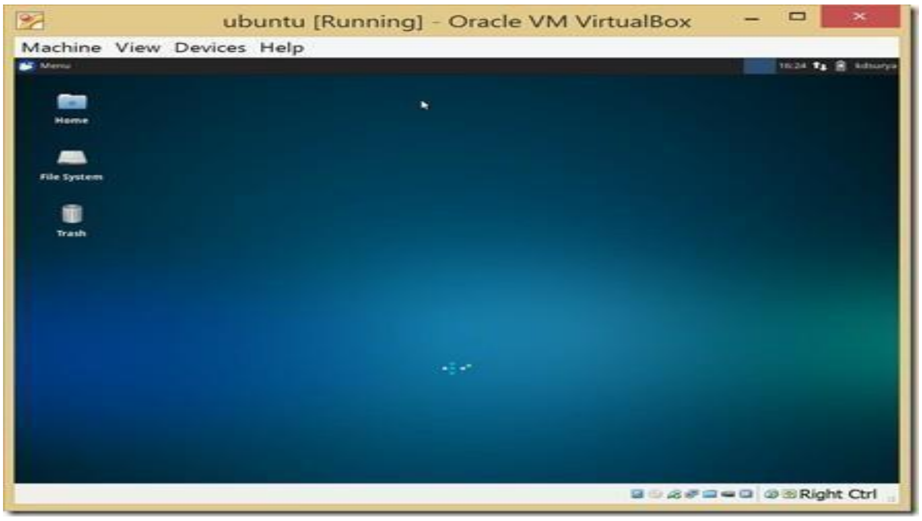
If required to have more than one operating system on one computer, then this option can be selected to allow the use of more than one operating system. Later, each operating system will be placed on their respective partitions. Therefore, there needs to be preparation for a partition before installing a multi-boot it.

4. Virtualization

Virtualization is a technique that allows the operating system installationperformed on the operating system that exists today. Not in a specific partition but in a specific file.

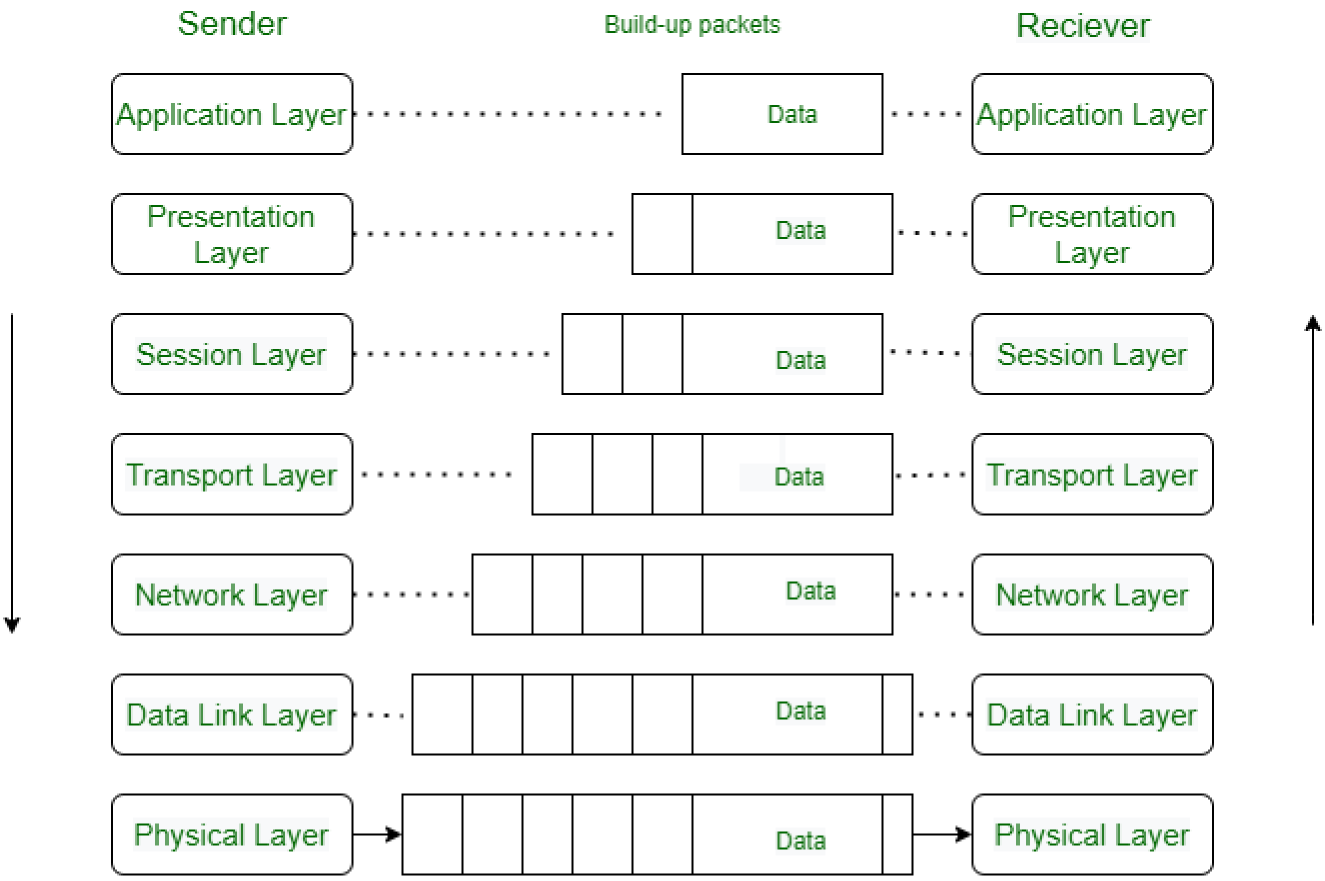
This file is a representation of a virtual computer system.One computer can have more than one virtual computer.

Therefore, the installation of more than one operating systemis also possible with this technique. Some applications whichallow to create virtual system is VirtualBox, VMWare, and Virtual PC.



OSI MODEL

OSI stands for **Open Systems Interconnection**. It has been developed by ISO – '**International Organization for Standardization**', in the year 1984. It is a 7-layer architecture with each layer having specific functionality to perform. All these 7 layers work collaboratively to transmit the data from one person to another across the globe.

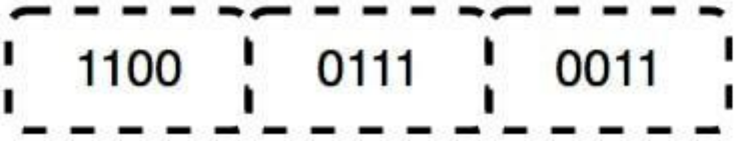


Layers of OSI Model

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

Layer 1- Physical Layer

The lowest layer of the OSI reference model is the physical layer. It is responsible for the actual physical connection between the devices. The physical layer contains information in the form of **bits.** It is responsible for transmitting individual bits from one node to the next. When receiving data, this layer will get the signal received and convert it into 0s and 1s and send them to the Data Link layer, which will put the frame back together.



Data Bits in the Physical Layer

The Functions of the Physical Layer

- **Bit synchronization:** The physical layer provides the synchronization of the bits by providing a clock. This clock controls both sender and receiver thus providing synchronization at the bit level.
- **Bit rate control:** The Physical layer also defines the transmission rate i.e. the number of bits sent per second.
- **Physical topologies:** Physical layer specifies how the different, devices/nodes are arranged in a network i.e. bus, star, or mesh topology.
- **Transmission mode:** Physical layer also defines how the data flows between the two connected devices. The various transmission modes possible are Simplex, half-duplex and full-duplex.

Note: 1. Hub, Repeater, Modem, and Cables are Physical Layer devices.

3. Network Layer, Data Link Layer, and Physical Layer are also known as **Lower Layers** or **Hardware Layers**.

Layer 2- Data Link Layer (DLL)

The data link layer is responsible for the node-to-node delivery of the message. The main function of this layer is to make sure data transfer is error-free from one node to another, over the physical layer. When a packet arrives in a network, it is the responsibility of the DLL to transmit it to the Host using its MAC address. The Data Link Layer is divided into two sublayers:

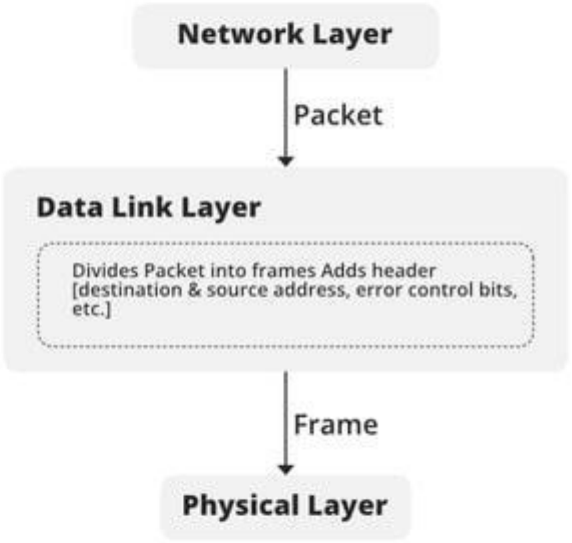
1. Logical Link Control (LLC)
2. Media Access Control (MAC)

The packet received from the Network layer is further divided into frames depending on the frame size of the NIC(Network Interface Card). DLL also encapsulates Sender and Receiver's MAC address in the header.

The Receiver's MAC address is obtained by placing an ARP(Address Resolution Protocol) request onto the wire asking "Who has that IP address?" and the destination host will reply with its MAC address.

The Functions of the Data
Link Layer

- **Framing:** Framing is a function of the data link layer. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver. This can be accomplished by attaching special bit patterns to the beginning and end of the frame.
  - **Physical addressing:** After creating frames, the Data link layer adds physical addresses (MAC addresses) of the sender and/or receiver in the header of each frame.
- **Error control:** The data link layer provides the mechanism of error control in which it detects and retransmits damaged or lost frames.
- **Flow Control:** The data rate must be constant on both sides else the data may get corrupted thus, flow control coordinates the amount of data that can be sent before receiving an acknowledgment.
- **Access control:** When a single communication channel is shared by multiple devices, the MAC sub-layer of the data link layer helps to determine which device has control over the channel at a given time.


Network Layer
Packet
Data Link Layer
Divides Packet into frames Adds header [destination & source address, error control bits, etc.]
Frame
Physical Layer

Function of DLL

Note: 1. Packet in the Data Link layer is referred to as **Frame.**
2. Data Link layer is handled by the NIC (Network Interface Card) and device drivers of host machines.
3. Switch & Bridge are Data Link Layer devices.

Layer 3- Network Layer

The network layer works for the transmission of data from one host to the other located in different networks. It also takes care of packet routing i.e. selection of the shortest path to transmit the packet, from the number of routes available. The sender & receiver's IP addresses are placed in the header by the network layer.

The Functions of the
Network Layer

- **Routing:** The network layer protocols determine which route is suitable from source to destination. This function of the network layer is known as routing.
- **Logical Addressing:** To identify each device on Internetwork uniquely, the network layer defines an addressing scheme. The sender & receiver's IP addresses are placed in the header by the network layer. Such an address distinguishes each device uniquely and universally.

Note: 1. Segment in the Network layer is referred to as **Packet**.
Network layer is implemented by networking devices such as routers and switches.

Layer 4- Transport Layer

The transport layer provides services to the application layer and takes services from the network layer. The data in the transport layer is referred to as *Segments*. It is responsible for the End to End Delivery of the complete message. The transport layer also provides the acknowledgment of the successful data transmission and re-transmits the data if an error is found.

At the sender's side: The transport layer receives the formatted data from the upper layers, performs **Segmentation**, and also implements **Flow & Error control** to ensure proper data transmission. It also adds Source and Destination port numbers in its header and forwards the segmented data to the Network Layer.

Note: The sender needs to know the port number associated with the receiver's application.

Generally, this destination port number is configured, either by default or manually. For example, when a web application requests a web server, it typically uses port number 80, because this is the default port assigned to web applications. Many applications have default ports assigned.

At the receiver's side: Transport Layer reads the port number from its header and forwards the Data which it has received to the respective application. It also performs sequencing and reassembling of the segmented data.

The Functions of the
Transport Layer

- **Segmentation and Reassembly:** This layer accepts the message from the (session) layer, and breaks the message into smaller units. Each of the segments produced has a header associated with it. The transport layer at the destination station reassembles the message.
- **Service Point Addressing:** To deliver the message to the correct process, the transport layer header includes a type of address called service point address or port address. Thus by specifying this address, the transport layer makes sure that the message is delivered to the correct process.

Services Provided by Transport Layer

1. Connection-Oriented Service
2. Connectionless Service

1. Connection-Oriented Service: It is a three-phase process that includes

- Connection Establishment
- Data Transfer
- Termination/disconnection

In this type of transmission, the receiving device sends an acknowledgment, back to the source after a packet or group of packets is received. This type of transmission is reliable and secure.

2. Connectionless service: It is a one-phase process and includes Data Transfer. In this type of transmission, the receiver does not acknowledge receipt of a packet. This approach allows for much faster communication between devices. Connection-oriented service is more reliable than connectionless Service.

Note: 1. Data in the Transport Layer is called **Segments**.

2. Transport layer is operated by the Operating System. It is a part of the OS and communicates with the Application Layer by making system calls.

3. The transport layer is called as **Heart of the OSI** model.

3. **Device or Protocol Use :** TCP, UDP NetBIOS, PPTP

Layer 5- Session Layer

This layer is responsible for the establishment of connection, maintenance of sessions, and authentication, and also ensures security.

The Functions of the
Session Layer

- **Session establishment, maintenance, and termination:** The layer allows the two processes to establish, use and terminate a connection.
- **Synchronization:** This layer allows a process to add checkpoints that are considered synchronization points in the data. These synchronization points help to identify the error so that the data is re-synchronized properly, and ends of the messages are not cut prematurely and data loss is avoided.
- **Dialog Controller:** The session layer allows two systems to start communication with each other in half-duplex or full-duplex.

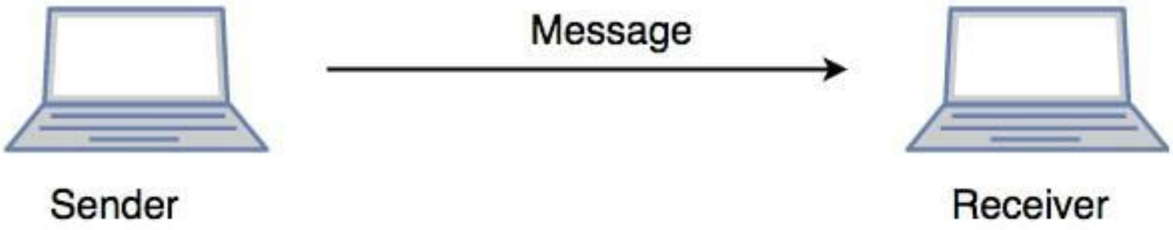
Note: 1. All the below 3 layers(including Session Layer) are integrated as a single layer in the TCP/IP model as the "Application Layer".

2. Implementation of these 3 layers is done by the network application itself. These are also known as **Upper Layers or Software Layers.**

3. **Device or Protocol Use :** NetBIOS, PPTP

Scenario

Let us consider a scenario where a user wants to send a message through some Messenger application running in his browser. The "Messenger" here acts as the application layer which provides the user with an interface to create the data. This message or so-called Data is compressed, encrypted (if any secure data), and converted into bits (0's and 1's) so that it can be transmitted.



Communication in Session Layer

Layer 6- Presentation Layer

The presentation layer is also called the **Translation layer**. The data from the application layer is extracted here and manipulated as per the required format to transmit over the network.

The Functions of the Presentation Layer are

- **Translation:** For example, ASCII to EBCDIC.
- **Encryption/ Decryption:** Data encryption translates the data into another form or code. The encrypted data is known as the ciphertext and the decrypted data is known as plain text. A key value is used for encrypting as well as decrypting data.
- **Compression:** Reduces the number of bits that need to be transmitted on the network.

Note: **Device or Protocol Use :** JPEG, MPEG, GIF

Layer 7- Application Layer

At the very top of the OSI Reference Model stack of layers, we find the Application layer which is implemented by the network applications. These applications produce the data, which has to be transferred over the network. This layer also serves as a window for the application services to access the network and for displaying the received information to the user.

Example: Application – Browsers, Skype Messenger, etc.

Note: 1. The application Layer is also called Desktop Layer.

2. **Device or Protocol Use :** SMTP

The Functions of the Application Layer are

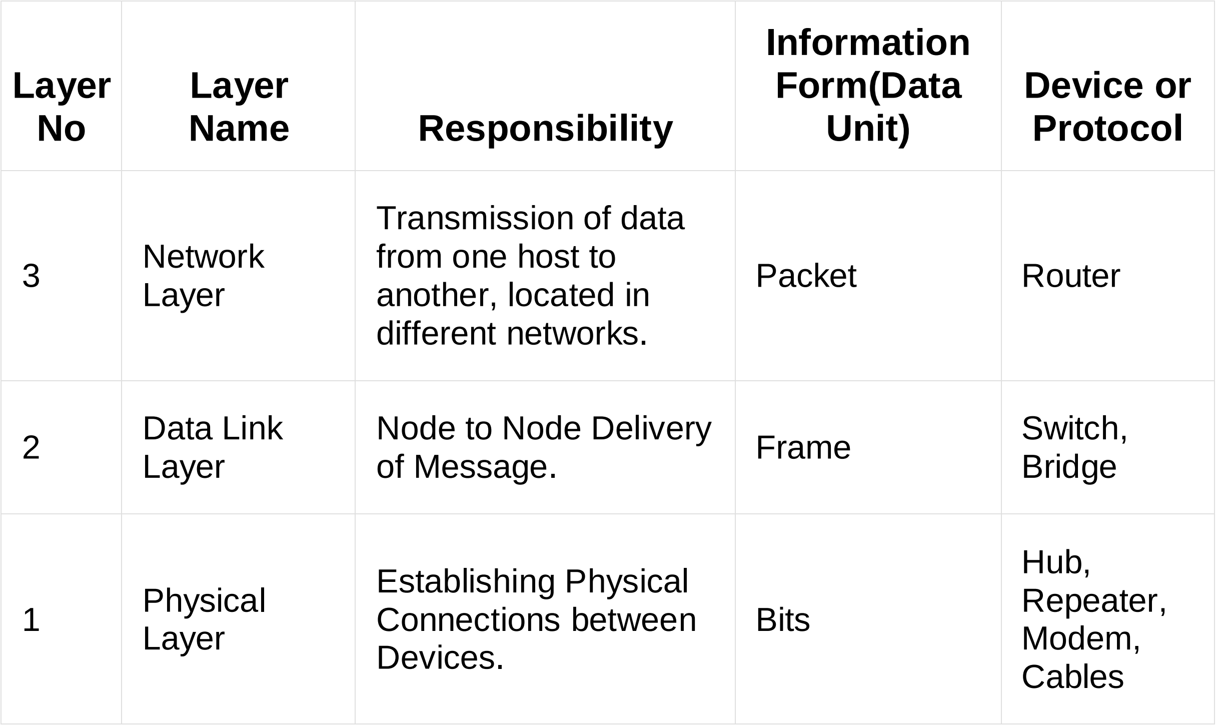
- Network Virtual Terminal: It allows a user to log on to a remote host.
- FTAM- File transfer access and management : This application allows a user to access file in a remote host, retrieve files in remote host and manage or control files from a remote computer.
- Mail Services : Provide email service.
- Directory Services : This application provides distributed database sources and access for global information about various objects and services.

OSI model acts as a reference model and is not implemented on the Internet because of its late invention. The current model being used is the TCP/IP model.

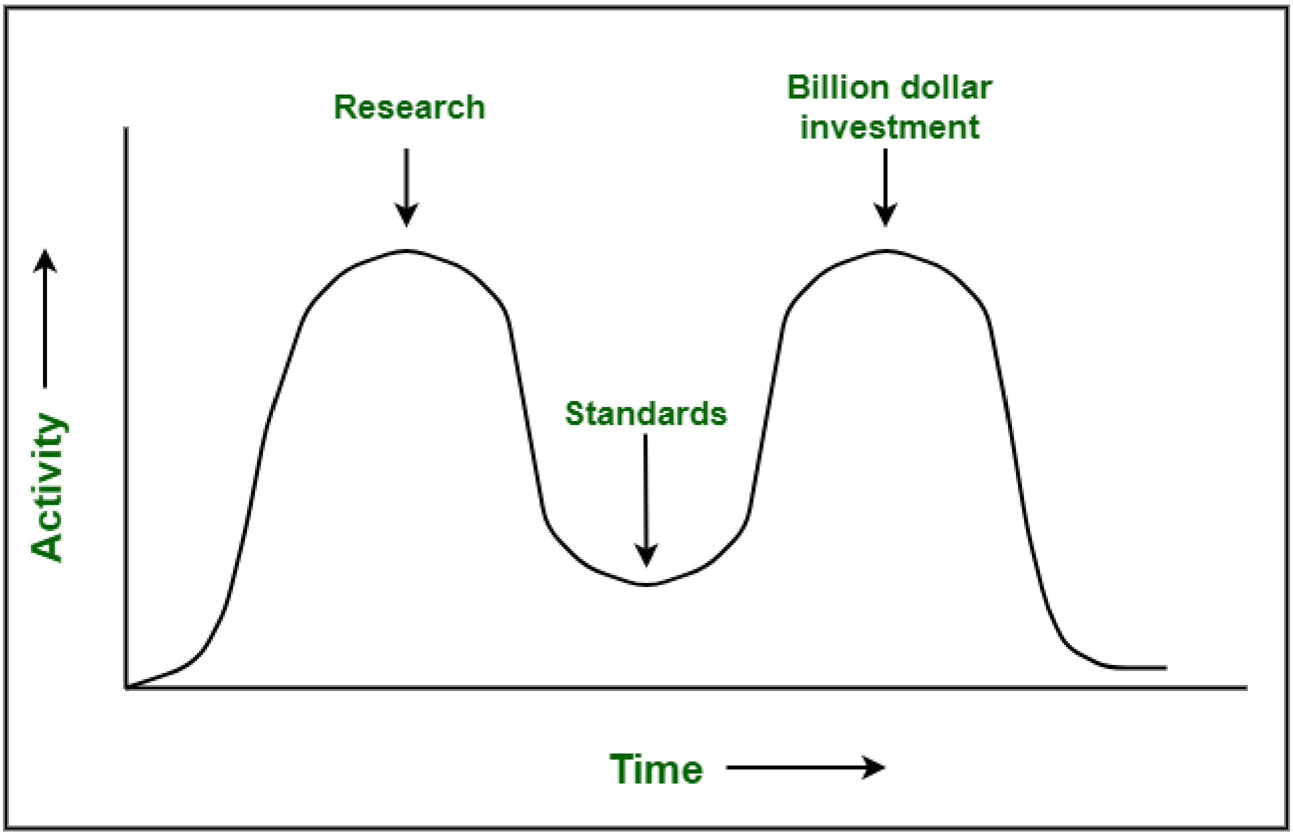
Note:

OSI Model in a Nutshell

Layer No	Layer Name	Responsibility	Information Form(Data Unit)	Device or Protocol
7	Application Layer	Helps in identifying the client and synchronizing communication.	Message	SMTP
6	Presentation Layer	Data from the application layer is extracted and manipulated in the required format for transmission.	Message	JPEG, MPEG, GIF
5	Session Layer	Establishes Connection, Maintenance, Ensures Authentication, and Ensures security.	Message	Gateway
4	Transport Layer	Take Service from Network Layer and provide it to the Application Layer.	Segment	Firewall

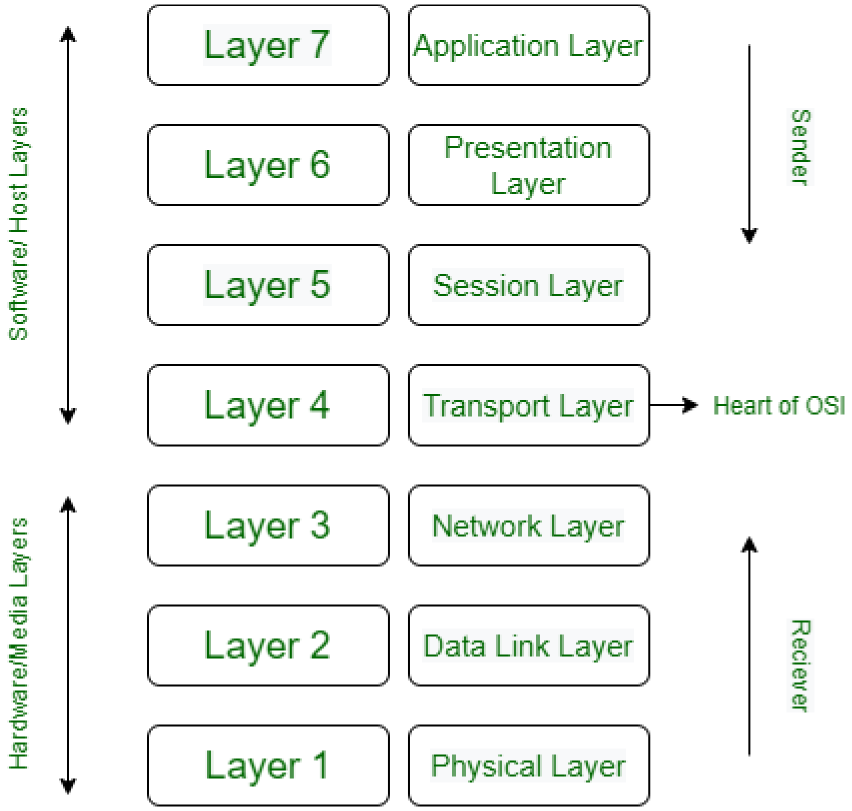


Layer No	Layer Name	Responsibility	Information Form(Data Unit)	Device or Protocol
3	Network Layer	Transmission of data from one host to another, located in different networks.	Packet	Router
2	Data Link Layer	Node to Node Delivery of Message.	Frame	Switch, Bridge
1	Physical Layer	Establishing Physical Connections between Devices.	Bits	Hub, Repeater, Modem, Cables



Apocalypse of the Two Elephants

Critique of OSI Model and Protocols


Software/ Host Layers
Hardware/Media Layers
Layer 7
Application Layer
Layer 6
Presentation Layer
Layer 5
Session Layer
Layer 4
Transport Layer
Heart of OSI
Layer 3
Network Layer
Layer 2
Data Link Layer
Layer 1
Physical Layer
Sender
Reciever