Subject: Networking Lab
Department: Electronics and Telecommunication Engineering
Prepared By: Deepika Panda & Shivanee Prusty

Networking Lab Rules

- Students must present a valid ID card before entering the computer lab.
- Playing of games on computer in the lab is strictly prohibited.
- Users are strictly prohibited from downloading, viewing or distributing any offensive
- Before leaving the lab, users must close all programs positively and keep the desktop blank.
- Users are strictly prohibited from modifying or deleting any important files and install any software or settings in the computer
- Based on the prime priority, users may be requested by the lab in-charge, to leave the workstation any time and the compliance is a must.
- Eating and/or drinking inside the computer labs is strictly prohibited.
- Internet facility is only for educational/ study purpose.
- Silence must be maintained in the lab at all times.
- The lab must be kept clean and tidy at all times.
- If any problem arises, please bring the same to the notice of lab in-charge.
- No bags/ hand bags/ rain coats/ casual wears will be allowed inside the computer lab, however note book may be allowed.
- Lab timing will be as per the academic time table of different classes
- Every user must make an entry while entering in the DCCN Lab and also at the time of exit from the lab.
- Each student or visitor must take mobile phones in “Switched Off” mode while entering and or working in Computer Lab.
- Conversation, discussion, loud talking & sleeping are strictly prohibited.
- Students are not allowed to use personal Pen Drives, CDs, DVDs etc., in a Computer Lab. Only prescribed official Pen Drives, CDs, DVDs etc. will be used in the Computer Lab to avoid VIRUS in Computers.
- Users must turn-off the computer before leaving the computer lab.
- In case of theft / destruction of the computers or peripherals, double the cost of the lost will be charged from the student/user.
- Keep your passwords to yourself. Change your password right away if you think someone else may know it.
- The DCCN lab is for academic purposes. Therefore, a quiet atmosphere is required. Noisy students will be asked to leave.
- Food and drink are not permitted in the computer lab.
- The use of cell phones is prohibited in the computer lab. Cell phone usage in the computer lab is distracting to other students and instructors trying to work.

- Please take your calls outside.
- Unauthorized copying and/or installing of unauthorized software is not permitted. This may be a violation of copyright laws.
- Tampering with the hardware or software settings will not be tolerated.
- Students found Internet surfing or chatting for personal reasons may be asked to leave. Preference is given to students doing course work over those engaged in personal computer use.
- Personal files are not to be stored on the local drive C. Students are responsible for providing their own means of digital storage. All lab computers are set up to remove any data stored or any programs installed by users.
- Children and friends of students are not allowed in the computer lab. The computer lab is an adult learning environment, and is not suitable or safe for children.
- DO NOT leave your personal belongings at the computer. The College is not responsible for items left behind.
- Disruptive students will be asked to leave and Public Safety may be called in such situations.
- Sleeping in the lab is not permitted

General Instructions:

An observation note and a fair record are needed to record the experiments conducted in the laboratory. Observation notes are needed to be certified immediately on completion of the experiment. Fair records are due at the beginning of the next lab period. Fair records must be submitted as neat, legible, and complete.

Instructions To Students For Writing The Fair Record: In the fair record, the index page should be filled properly by writing the corresponding experiment number, experiment name , date on which it was done and the page number.

On the right side page of the record following has to be written:

- **Title:** The title of the experiment should be written in the page in capital letters
- In the left top margin, experiment number and date should be written.
- **Aim:** The purpose of the experiment should be written clearly.
- **Apparatus/Tools/Equipments/Components used**: A list of the Apparatus/Tools /Equipments /Components used for doing the experiment should be entered.
- **Theory:** Simple working of the circuit/experimental set up/algorithm should be written.
- **Procedure:** steps for doing the experiment and recording the readings should be briefly described(flow chart/programs in the case of computer/processor related experiments)
- **Results:** The results of the experiment must be summarized in writing and should be fulfilling the aim.
- **Inference:** Inference from the results is to be mentioned.

On the Left side page of the record following has to be recorded:

- **Circuit/Program:** Neatly drawn circuit diagrams/experimental set up.
- **Design:** The design of the circuit/experimental set up for selecting the components should be clearly shown if necessary.
- **Observations:** Data should be clearly recorded using Tabular Columns.
    - Unit of the observed data should be clearly mentioned
    - Relevant calculations should be shown. If repetitive calculations are needed, only show a sample calculation and summarize the others in a table.

- **Graphs:** Graphs can used to present data in a form that show the results obtained, as one or more of the parameters are varied. A graph has the advantage of presenting large amounts of data in a concise visual form. Graph should be in a square format.

INDEX

Experiment - 1

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

Aim: To recognize the i) Physical topology, ii) cabling (coaxial, OFC, UTP, STP) of a network.

Apparatus/Tools/Equipments/Components:

RJ-45 connector, IO Connector, Twisted pair Cable (UTP, STP), Coaxial Cable, Optical Fiber Cable, Computers.

Theory:

i) Physical Topology: The topology of a network is the geometric representation of the relationship of all the links and linking devices (usually called nodes) to one another. It is the schematic description of a network arrangement, connecting various nodes(sender and receiver) through lines of connection.

Types of Network Topology:

1. BUS Topology: Bus topology is a network type in which every computer and network device is connected to single cable. When it has exactly two endpoints, then it is called Linear Bus topology.

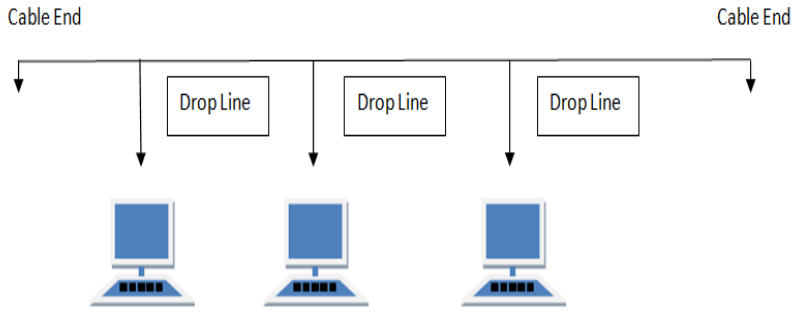


Fig. Bus Topology

Features of Bus Topology:

1. It transmits data only in one direction.
2. Every device is connected to a single cable

2. RING Topology:

It is called ring topology because it forms a ring as each computer is connected to another computer, with the last one connected to the first. Exactly two neighbors for each device.

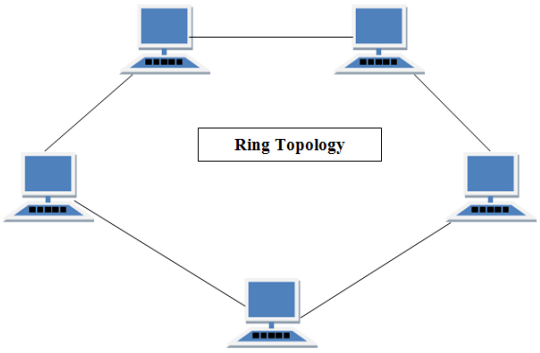


Fig. Ring Topology

Features of Ring Topology:

1. A number of repeaters are used for Ring topology with large number of nodes, because if someone wants to send some data to the 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.
2. The transmission is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called **Dual Ring Topology**.
3. In Dual Ring Topology, two ring networks are formed, and data flow is in opposite direction in them. Also, if one ring fails, the second ring can act as a backup, to keep the network up.
4. Data is transferred in a sequential manner that is bit by bit. Data transmitted, has to pass through each node of the network, till the destination node.

3. STAR Topology:

In this type of topology all the computers are connected to a single hub through a cable. This hub is the central node and all others nodes are connected to the central node.

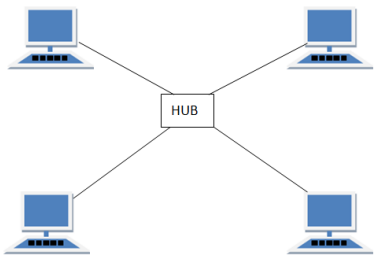


Fig. Star Topology

Features of Star Topology

1. Every node has its own dedicated connection to the hub.
2. Hub acts as a repeater for data flow.
3. Can be used with twisted pair, Optical Fiber or coaxial cable.

4. MESH Topology:

It is a point-to-point connection to other nodes or devices. All the network nodes are connected to each other. Mesh **has n(n-1)/2** physical channels to link n devices.

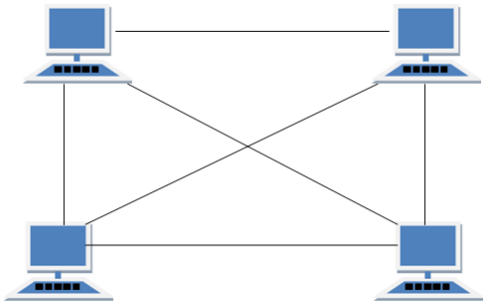


Fig Mesh Topology

Types of Mesh Topology

1. Partial Mesh Topology : In this topology some of the systems are connected in the same fashion as mesh topology but some devices are only connected to two or three devices.
2. Full Mesh Topology : Each and every nodes or devices are connected to each other.

Features of Mesh Topology

1. Fully connected.
2. Robust.
3. Not flexible.

5. TREE Topology:

It has a root node and all other nodes are connected to it forming a hierarchy. It is also called hierarchical topology. It should at least have three levels to the hierarchy.

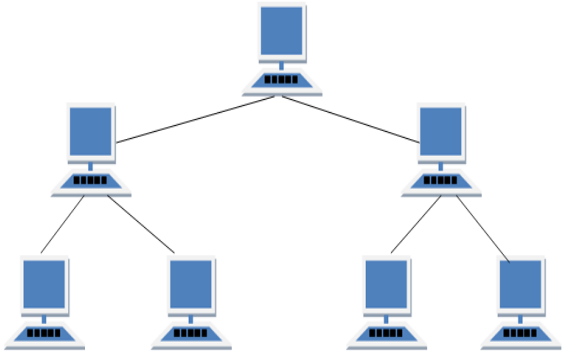


Fig. Tree Topology

Features of Tree Topology

1. Ideal if workstations are located in groups.
2. Used in Wide Area Network.

6. HYBRID Topology:

It is two different types of topologies which is a mixture of two or more topologies. For example if in an office in one department ring topology is used and in another star topology is used, connecting these topologies will result in Hybrid Topology (ring topology and star topology).

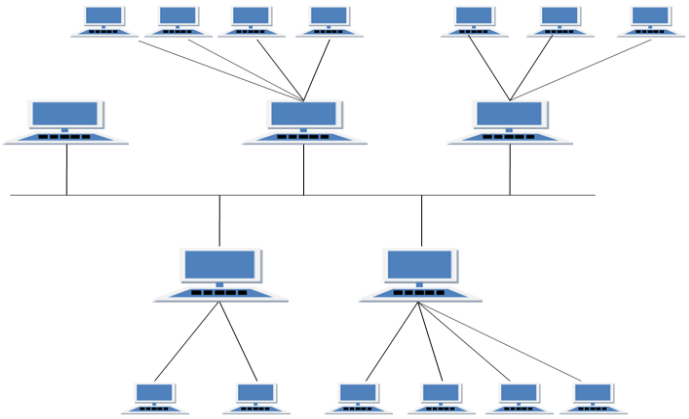


Fig. Hybrid Topology

Features of Hybrid Topology

1. It is a combination of two or topologies
2. Inherits the advantages and disadvantages of the topologies included.

ii) **Cabling of Network:**

Twisted Pair: A twisted pair cable is a type of cable made by putting two separate insulated wires together in a twisted pattern and running them parallel to each other. This type of cable is widely used in different kinds of data and voice infrastructures.

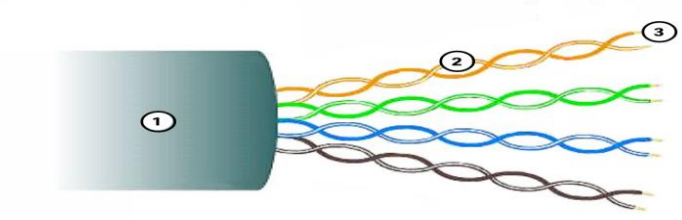
It is further classified into two types. a) UTP, b) STP

a) Unshielded Twisted Pair(UTP):

- UTP is the most common networking media.
- Terminated with RJ-45 connectors
- Interconnects hosts with intermediary network devices.

Key Characteristics of UTP:

1. The outer jacket protects the copper wires from physical damage.
2. Twisted pairs protect the signal from interference.
3. Color-coded plastic insulation electrically isolates the wires from each other and identifies each pair.



UTP has four pairs of color-coded copper wires twisted together and encased in a flexible plastic sheath. No shielding is used. UTP relies on the following properties to limit crosstalk:

- Cancellation - Each wire in a pair of wires uses opposite polarity. One wire is negative, the other wire is positive. They are twisted together and the magnetic fields effectively cancel each other and outside EMI/RFI.

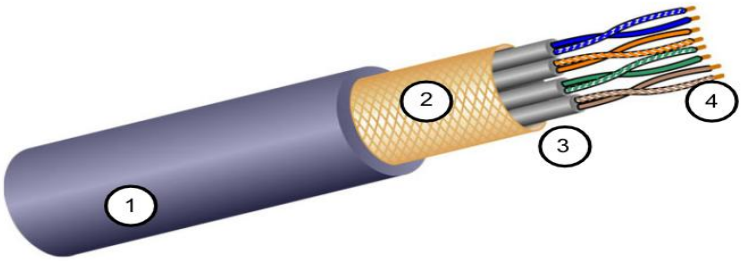
- Variation in twists per foot in each wire - Each wire is twisted a different amount, which helps prevent crosstalk amongst the wires in the cable.

b) Shielded Twisted Pair (STP):

- Better noise protection than UTP
- More expensive than UTP
- Harder to install than UTP
- Terminated with RJ-45 connectors
- Interconnects hosts with intermediary network devices

Key Characteristics of STP

1. The outer jacket protects the copper wires from physical damage
2. Braided or foil shield provides EMI/RFI protection
3. Foil shield for each pair of wires provides EMI/RFI protection
4. Color-coded plastic insulation electrically isolates the wires from each other and identifies each pair.



Coaxial Cable:

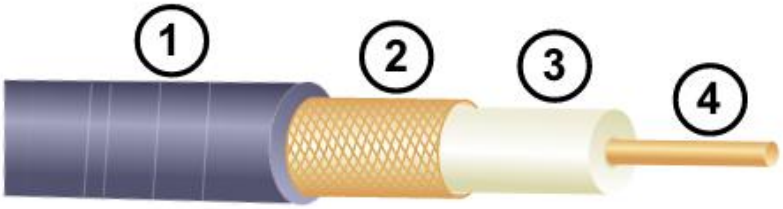
Consists of the following:

1. Outer cable jacket to prevent minor physical damage
2. A woven copper braid, or metallic foil, acts as the second wire in the circuit and as a shield for the inner conductor.
3. A layer of flexible plastic insulation
4. A copper conductor is used to transmit the electronic signals.

There are different types of connectors used with coax cable.

Commonly used in the following situations:

- Wireless installations - attach antennas to wireless devices
- Cable internet installations - customer premises wiring

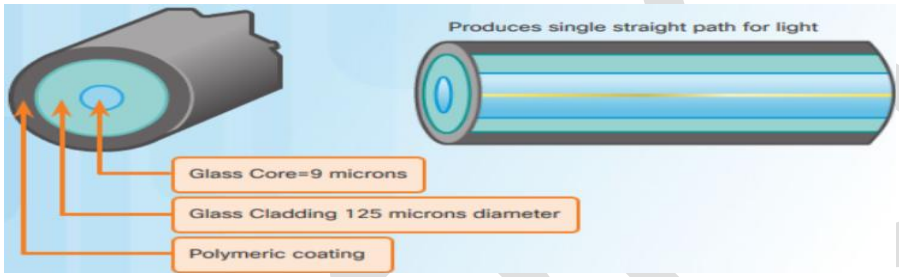


Fiber-Optic Cabling:

Properties of Fiber-Optic Cabling:

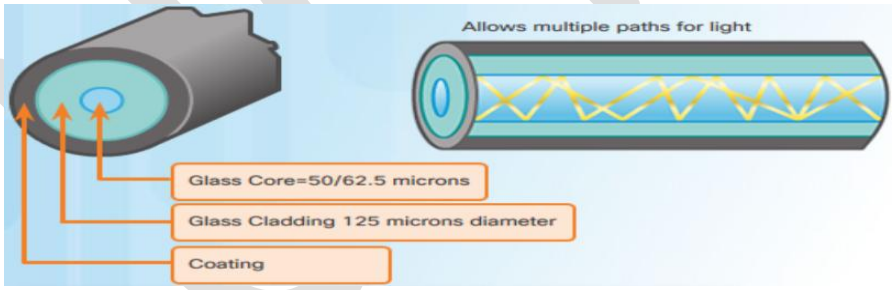
- Not as common as UTP because of the expense involved
- Ideal for some networking scenarios
- Transmits data over longer distances at higher bandwidth than any other networking media
- Less susceptible to attenuation, and completely immune to EMI/RFI
- Made of flexible, extremely thin strands of very pure glass
- Uses a laser or LED to encode bits as pulses of light
- The fiber-optic cable acts as a wave guide to transmit light between the two ends with minimal signal loss

Single-Mode Fiber:



- Very small core
- Uses expensive lasers
- Long-distance applications

Multimode Fiber:



- Larger core
- Uses less expensive LEDs
- LEDs transmit at different angles
- Up to 10 Gbps over 550 meters

Conclusion: In the above experiment we have recognized, observed and studied about different types of topologies and cables in detail.

Experiment-2

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

Aim: To recognize and use of various types of connectors i) RJ-45, ii)RJ-11, iii)BNC and iii) SCST

Apparatus/Tools/Equipments/Components: RJ-45 connector, IO Connector, RJ-11, BNC, SCST .

Theory:

i)RJ-45: RJ45 is a type of connector commonly used for Ethernet networking. It looks similar to a telephone jack, but is slightly wider. Since Ethernet cables have an RJ45 connector on each end, Ethernet cables are sometimes also called RJ45 cables.

The "RJ" in RJ45 stands for "registered jack," since it is a standardized networking interface. The "45" simply refers to the number of the interface standard. Each RJ45 connector has eight pins, which means an RJ45 cable contains eight separate wires. If you look closely at the end of an Ethernet cable, you can actually see the eight wires, which are each a different color. Four of them are solid colors, while the other four are striped.

RJ45 cables can be wired in two different ways. One version is called T-568A and the other is T-568B. These wiring standards are listed below:

T-568A

1. White/Green (Receive +)
2. Green (Receive -)
3. White/Orange (Transmit +)
4. Blue
5. White/Blue
6. Orange (Transmit -)
7. White/Brown
8. Brown

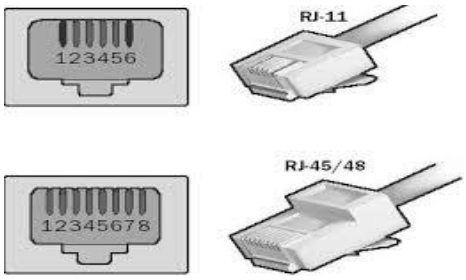
T-568B

1. White/Orange (Transmit +)
2. Orange (Transmit -)
3. White/Green (Receive +)
4. Blue
5. White/Blue
6. Green (Receive -)
7. White/Brown
8. Brown

The T-568B wiring scheme is by far the most common, though many devices support the T-568A wiring scheme as well. Some networking applications require a crossover Ethernet cable, which has a T-568A connector on one end and a T-568B connector on the other. This type of cable is typically used for direct computer-to-computer connections when there is no router, hub, or switch available.

Types of cables based on the termination:

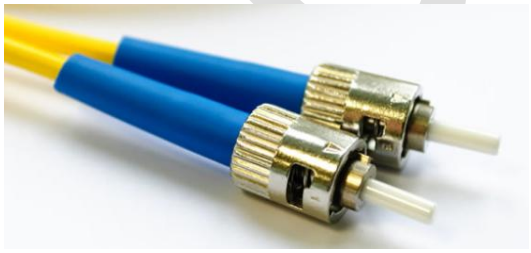
1. Straight-over cable
2. Crossover cable



ii)RJ-11: 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 the center 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.

iii)BNC(*Bayonet **N**eill **C**oncelman connector)*:** It's a type of connector used with coaxial cables such as the RG-58 A/U cable used with the 10Base-2 Ethernet system. The basic BNC connector is a male type mounted at each end of a cable. This connector has a center pin connected to the center cable conductor and a metal tube connected to the outer cable shield. A rotating ring outside the tube locks the cable to any female connector.
BNC T-connectors (used with the 10Base-2 system) are female devices for connecting two cables to a network interface card (NIC). A BNC barrel connector allows connecting two cables together.
BNC connectors can also be used to connect some monitors, which increases the accuracy of the signals sent from the video adapter.

iv) SC-ST: These connectors are used to connect the optical fibers.



Straight-Tip (ST) Connectors

Subscriber Connector (SC) Connectors

Conclusion: In the above experiment we recognized various types of connector such as RJ45,RJ11,BNC and SCST and also learnt how to use them in networking.

Experiment-3

Experiment: Making of cross cable and straight cable.

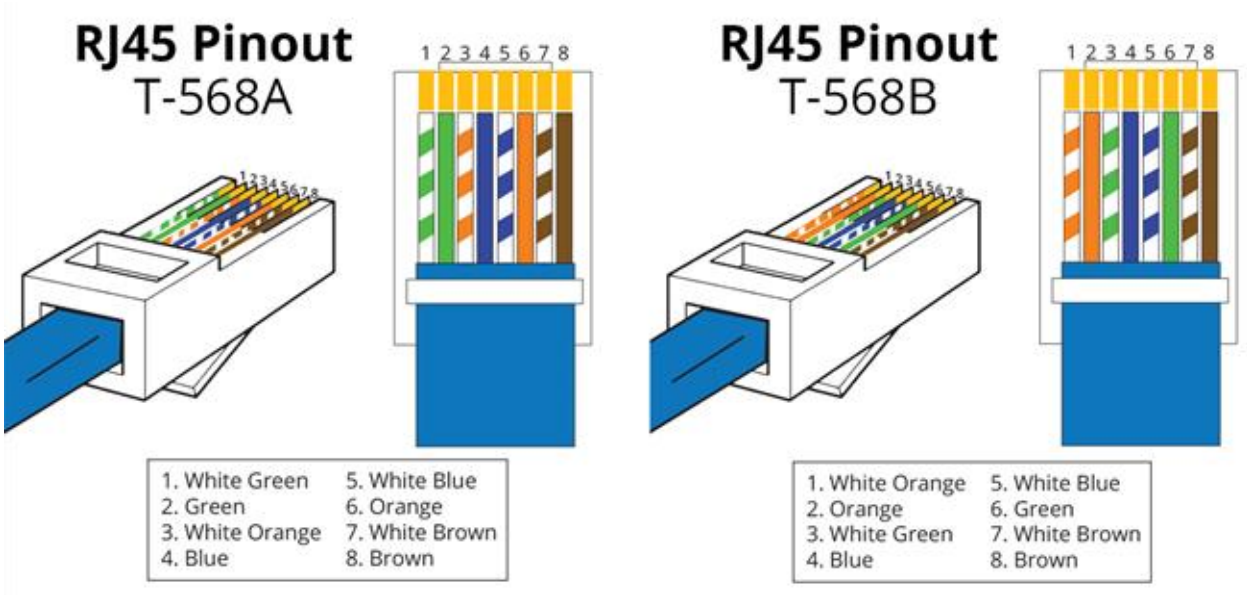
Aim: To make the following a) Cross Cable b) Straight Cable.

Apparatus/Tools/Equipments/Components: RJ-45 connector, IO Connector, Crimping Tool, Twisted pair Cable, Cable Tester

Theory: Ethernet cables can be wired as straight through or crossover. The straight through is the most common type and is used to connect computers to hubs or switches. They are most likely what you will find when you go to your local computer store and buy a patch cable. Crossover Ethernet cable is more commonly used to connect a computer to a computer and may be a little harder to find since they aren't used nearly as much as straight through Ethernet cable. Then, what's the difference between straight through vs crossover cable? Read through this post to find the answer.

T568A And T568B Wiring Standard Basis:

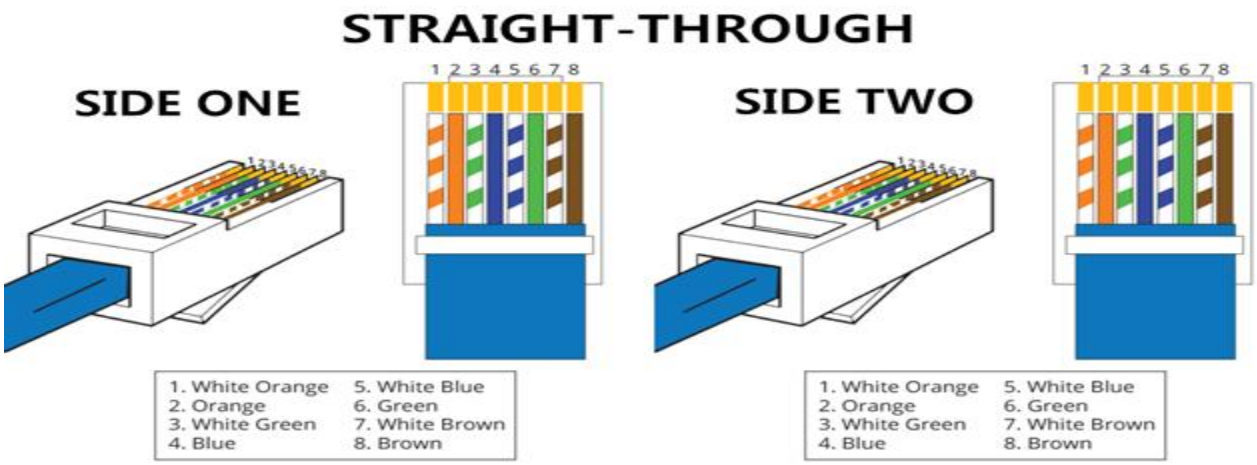
A RJ45 connector is a modular 8 position, 8 pin connector used for terminating Cat5e patch cable or Cat6 cable. A pinout is a specific arrangement of wires that dictate how the connector is terminated. There are two standards recognized by ANSI, TIA and EIA for wiring Ethernet cables. The first is the T568A wiring standard and the second is T568B. T568B has surpassed 568A and is seen as the default wiring scheme for twisted pair structured cabling. If you are unsure of which to use, choose 568B.



Straight Through vs Crossover Cable:

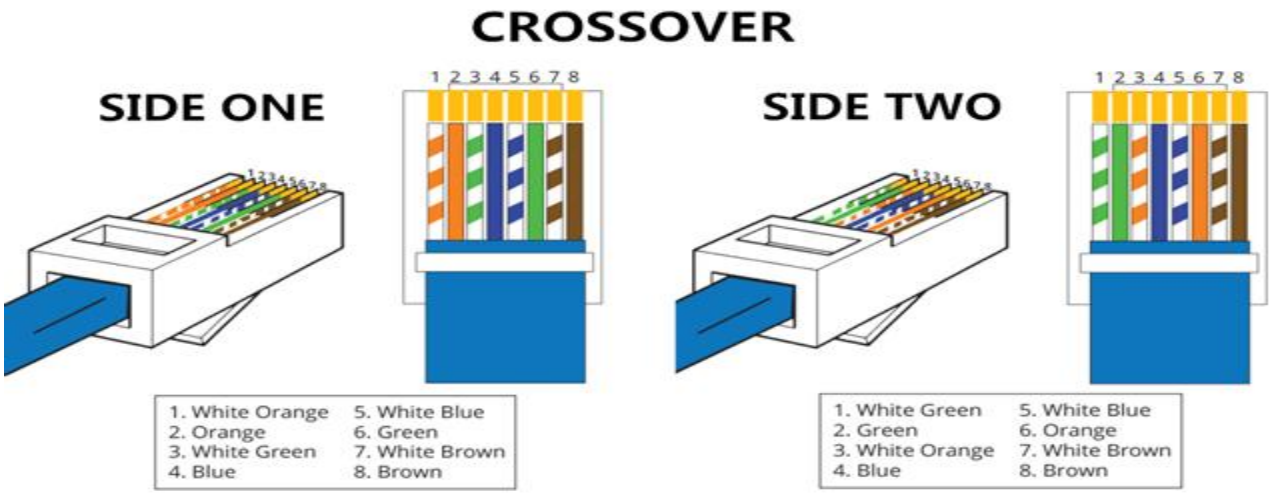
A straight through cable is a type of twisted pair cable that is used in local area networks to connect a computer to a network hub such as a router. This type of cable is also sometimes

called a patch cable and is an alternative to wireless connections where one or more computers access a router through a wireless signal. On a straight through cable, the wired pins match. Straight through cable use one wiring standard: both ends use T568A wiring standard or both ends use T568B wiring standard. The following figure shows a straight through cable of which both ends are wired as the T568B standard.



Crossover Cable:

A crossover Ethernet cable is a type of Ethernet cable used to connect computing devices together directly. Unlike straight through cable, the RJ45 crossover cable uses two different wiring standards: one end uses the T568A wiring standard, and the other end uses the T568B wiring standard. The internal wiring of Ethernet crossover cables reverses the transmit and receive signals. It is most often used to connect two devices of the same type: e.g. two computers (via network interface controller) or two switches to each other.



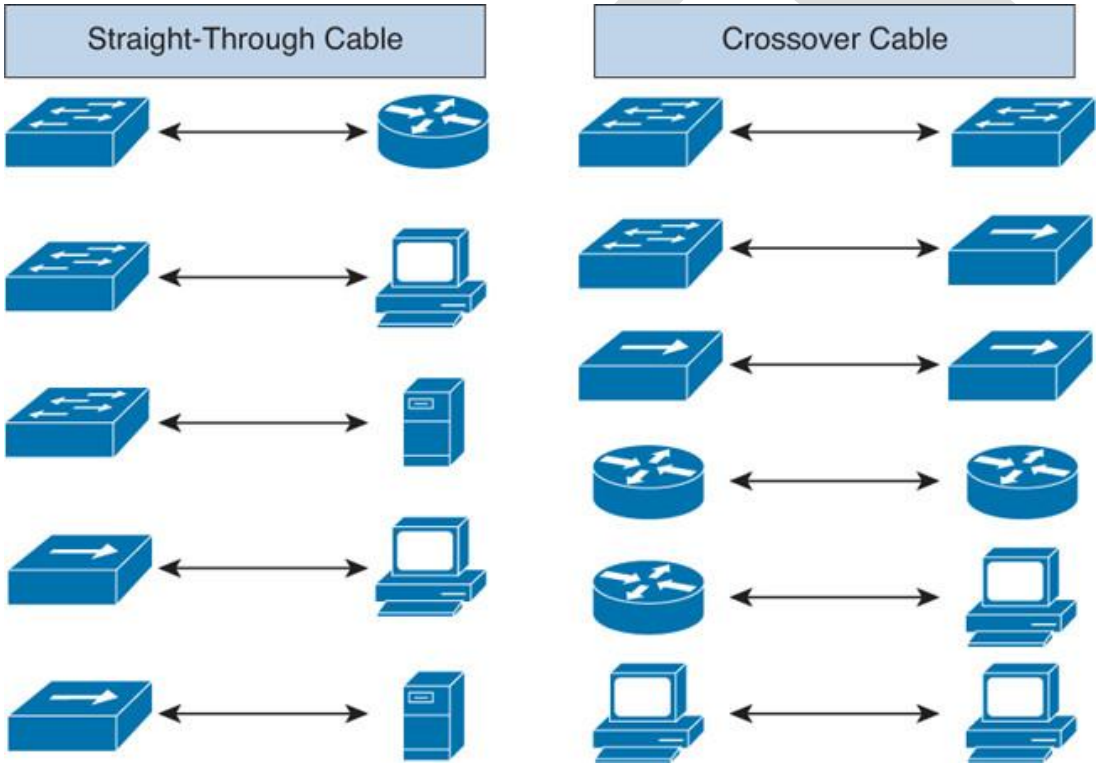
Uses of Straight Through and Crossover Cables: Usually, straight through cables are primarily used for connecting unlike devices. And crossover cables are use for connecting alike devices.

Use straight through Ethernet cable for the following cabling:

- Switch to router
- Switch to PC or server
- Hub to PC or server

Use crossover cables for the following cabling:

- Switch to switch
- Switch to hub
- Hub to hub
- Router to router
- Router Ethernet port to PC NIC
- PC to PC



Procedure:

Step 1: Strip the cable jacket about 1.5 inch down from the end. Ed Rhee

Step 2: Spread the four pairs of twisted wire apart. For Cat 5e, you can use the pull string to strip the jacket farther down if you need to, then cut the pull string. Cat 6 cables have a spine that will also need to be cut. Ed Rhee

Step 3: Untwist the wire pairs and neatly align them in the T568B orientation. Be sure not to untwist them any farther down the cable than where the jacket begins; we want to leave as much of the cable twisted as possible.

Step 4: Cut the wires as straight as possible, about 0.5 inch above the end of the jacket.

Step 5: Carefully insert the wires all the way into the modular connector, making sure that each wire passes through the appropriate guides inside the connector.

Step 6: Push the connector inside the crimping tool and squeeze the crimper all the way down. Ed Rhee

Step 7: Repeat steps 1-6 for the other end of the cable.

Step 8: To make sure you've successfully terminated each end of the cable, use a cable tester to test each pin.

For crossover cables, simply make one end of the cable a T568**A** and the other end a T568**B**. Now you can make Ethernet cables of any length, fix broken connectors, or make yourself a crossover cable.

Conclusion: In the above experiment we have studied about and Straight Through and Crossover cable. Also, we learnt how to make them.

Experiment-4

Experiment: Install and configure a network interface card in a workstation.

Aim: To install and configure a network interface card in a workstation.

Hardware Required: Computer, NIC

Theory:

NICs (Network Interface Card): Network Interface Card, or NIC is a hardware card installed in a computer so it can communicate on a network. The network adapter provides one or more ports for the network cable to connect to, and it transmits and receives data onto the network cable**.**

Procedure to Install the network card:

- Disconnect all cables connected to the computer and open the case.
- Locate an available PCI slot (white slots) and insert the network card and secure the card with the screw that came with it.
- Once the adapter has been installed and secured close the computer case, connect all the cables and turn it on.
- After installing the adapter driver it should be working find, now let's configure the card for use on a network.
- Click on the Start button and select Settings then Control Panel. Double click on the System icon Click on the Hardware tab.
- Click on Device Manager. You will see a list of devices installed in your computer.
- If necessary, click on the + sign next to Network Adapters to expand the list.
- Ensure that there is no yellow exclamation mark (!) next to the Network Adapter. This indicates a possible problem with the card or configuration.
- Double click on your network driver (e.g. NE2000 Compatible).
- In the Device Status box you should see the message: This Device is working correctly.
- If you do not see this message or if there is no Network Adapter displayed, then your Ethernet card will probably need configuring.

Conclusion: Installation and configuration of Wired and Wireless (remotely) NIC and transfer files between systems in LAN and Wireless LAN between two systems in a LAN have been done successfully.

Experiment-5

Experiment: Identify the IP address of a workstation and the class of the address.

Aim:

I. Identify the IP address of a workstation
II. Identify class of the IP address

Equipment Required: Computer

Theory:
Network Classes

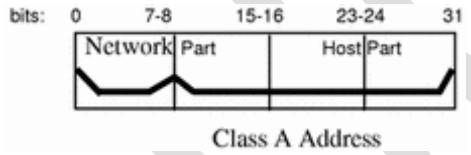
The first step in planning for IP addressing on your network is to determine which network class is appropriate for your network. After you have done this, you can take the crucial second step: obtain the network number from the Inter NIC addressing authority.

Currently there are three classes of TCP/IP networks. Each class uses the 32-bit IP address space differently, providing more or fewer bits for the network part of the address. These classes are class A, class B, and class C.

Class A Network Numbers

A class A network number uses the first eight bits of the IP address as its "network part." The remaining 24 bits comprise the host part of the IP address, as illustrated in Figure 1 below.

Figure 1 Byte Assignment in a Class A Address



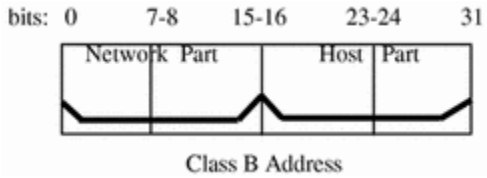
The values assigned to the first byte of class A network numbers fall within the range 0-127. Consider the IP address 75.4.10.4. The value 75 in the first byte indicates that the host is on a class A network. The remaining bytes, 4.10.4, establish the host address. The InterNIC assigns only the first byte of a class A number. Use of the remaining three bytes is left to the discretion of the owner of the network number. Only 127 class A networks can exist. Each one of these numbers can accommodate up to 16,777,214 hosts.

Class B Network Numbers

A class B network number uses 16 bits for the network number and 16 bits for host numbers. The first byte of a class B network number is in the range 128-191. In the number 129.144.50.56, the first two bytes, 129.144, are assigned by the Inter NIC, and comprise the network address. The last two bytes, 50.56, make up the host address, and are assigned at the

discretion of the owner of the network number. Figure 2 graphically illustrates a class B address.

Figure 2 Byte Assignment in a Class B Address

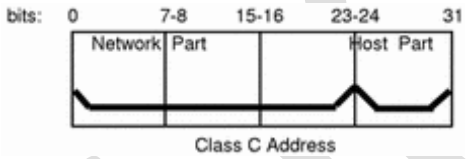


Class B is typically assigned to organizations with many hosts on their networks.

Class C Network Numbers

Class C network numbers use 24 bits for the network number and 8 bits for host numbers. Class C network numbers are appropriate for networks with few hosts--the maximum being 254. A class C network number occupies the first three bytes of an IP address. Only the fourth byte is assigned at the discretion of the network owners. Figure 3 graphically represents the bytes in a class C address.

Figure 3 Byte Assignment in a Class C Address



The first byte of a class C network number covers the range 192-223. The second and third each cover the range 1- 255. A typical class C address might be 192.5.2.5. The first three bytes, 192.5.2, form the network number. The final byte in this example, 5, is the host number.

Administering Network Numbers

If your organization has been assigned more than one network number, or uses subnets, appoint a centralized authority within your organization to assign network numbers. That authority should maintain control of a pool of assigned network numbers, assigning network, subnet, and host numbers as required. To prevent problems, make sure that duplicate or random network numbers do not exist in your organization.

Designing Your IP Addressing Scheme

After you have received your network number, you can then plan how you will assign the host parts of the IP address.

Table 1 shows the division of the IP address space into network and host address spaces. For each class, "range" specifies the range of decimal values for the first byte of the network number. "Network address" indicates the number of bytes of the IP address that are dedicated to the network part of the address, with each byte represented by *xxx*. "Host address" indicates the number of bytes dedicated to the host part of the address. For example, in a class A network address, the first byte is dedicated to the network, and the last three are dedicated to the host. The opposite is true for a class C network.

Table 1 Division of IP Address Space:

Class	**Range**	**Network Address**	**Host Address**
A	0-127	*xxx*	*xxx.xxx.xxx*
B	128-191	*xxx.xxx*	*xxx.xxx*
C	192-223	*xxx.xxx.xxx*	*xxx*

The numbers in the first byte of the IP address define whether the network is class A, B, or C and are always assigned by the Inter NIC. The remaining three bytes have a range from 0-255. The numbers 0 and 255 are reserved; you can assign the numbers 1-254 to each byte **depending on the network number assigned to you**.

Table 2 shows which bytes of the IP address are assigned to you and the range of numbers within each byte that are available for you to assign to your hosts.

Table 2 Range of Available Numbers:

Network Class	**Byte 1 Range**	**Byte 2 Range**	**Byte 3 Range**	**Byte 4 Range**
A	0-127	1-254	1-254	1-254
B	128-191	Preassigned by Internet	1-254	1-254

Network Class	Byte 1 Range	Byte 2 Range	Byte 3 Range	Byte 4 Range
C	192-223	Preassigned by Internet	Preassigned by Internet	1-254

Procedure:

I. Steps to find workstation's IP address:

1. Click the Start button, then Run
2. In the text box type **cmd** and press the Enter key
3. Type **ipconfig**
4. Under Local Area Connection, to the right of the row labeled “IP Address” you will find the computer's IP Address.

II. Steps to find the class of IP address:

As Mentioned in the theory, once the IP address and subnet mask is known, class can be identified by using the subnet mask.

Observations:
IP address: 192.168.43.140
Subnet Mask:255.255.255.0 – Class C IP address

Conclusion: From the above experiment we have observed the IP address to be 192.168.43.140 which belongs Class C Ipv4 address. We have also learnt to configure IP address to a work station.

Experiment - 6

Experiment- Managing user accounts in windows.

Aim: To study about managing user accounts in windows.

Apparatus Required-

1. A computer with a new installation of Windows 8
2. An account with administrator privileges

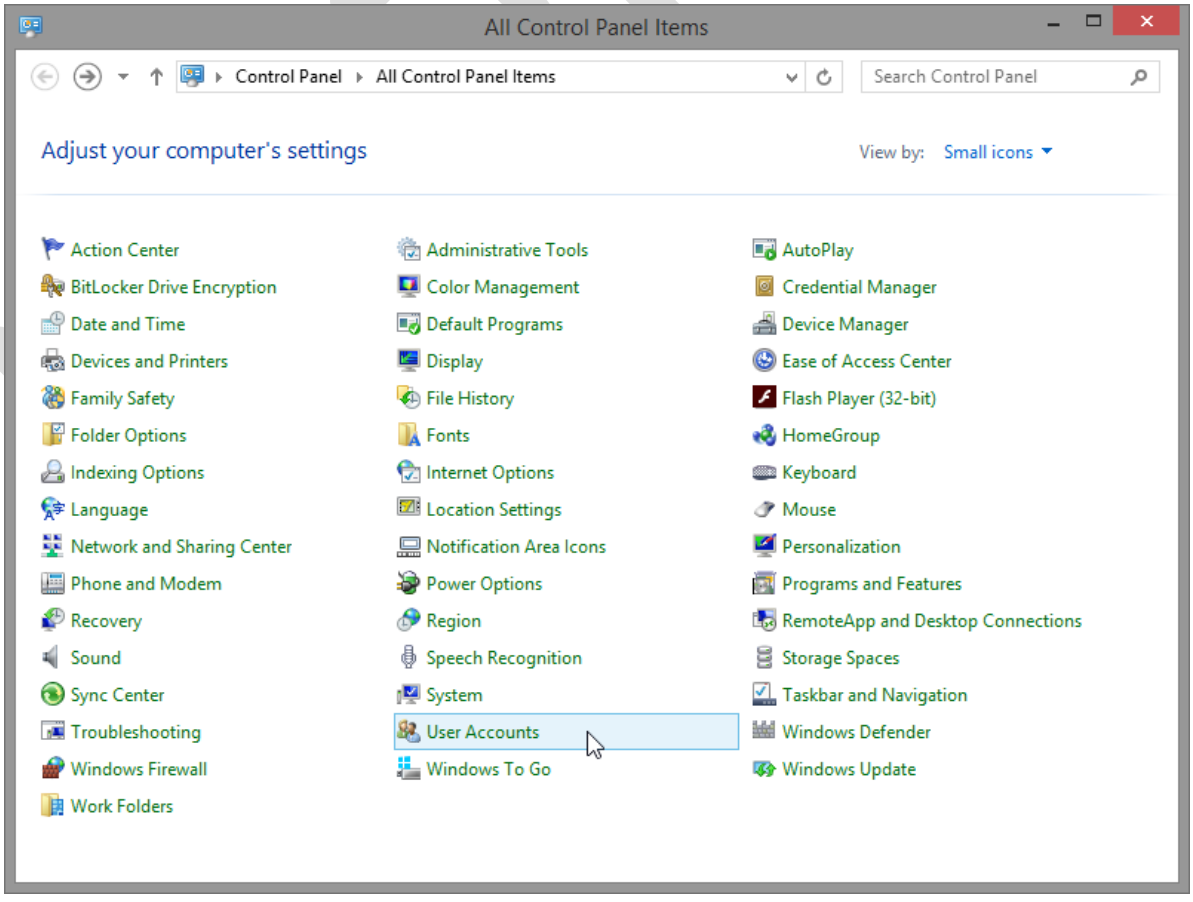
Theory- We can manage user accounts in any OS(Windows and Linux). This implies adding a new user account, editing the user details, removing the user account etc.

Procedure –

Part 1: Windows 8.1

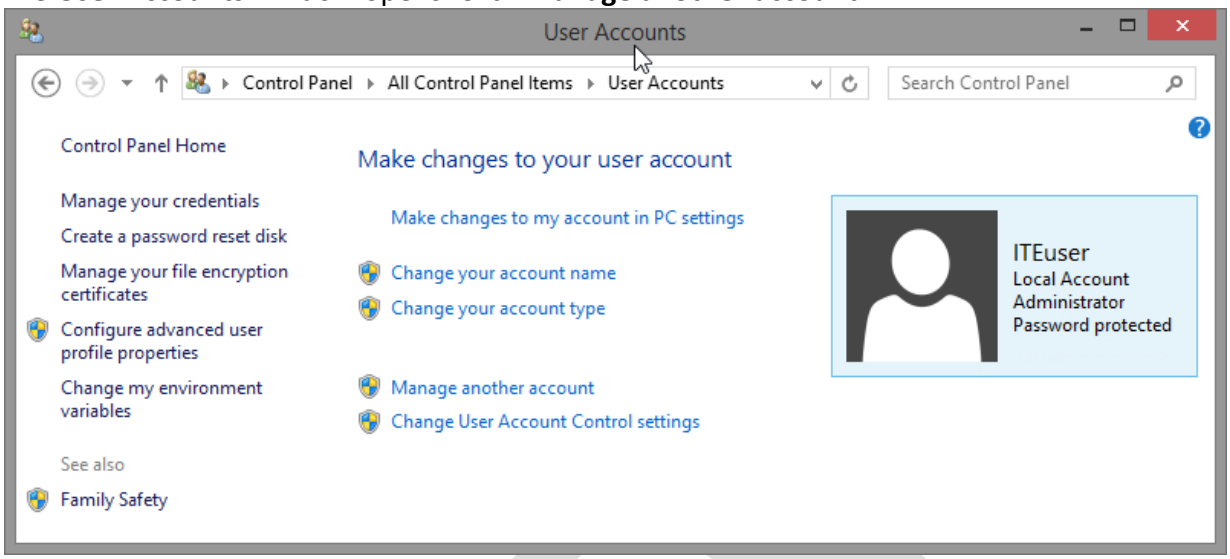
Step 1: Open the User Account Tool

a. Log on to the computer with an Administrator account.
b. Click **Control Panel > User Accounts**.

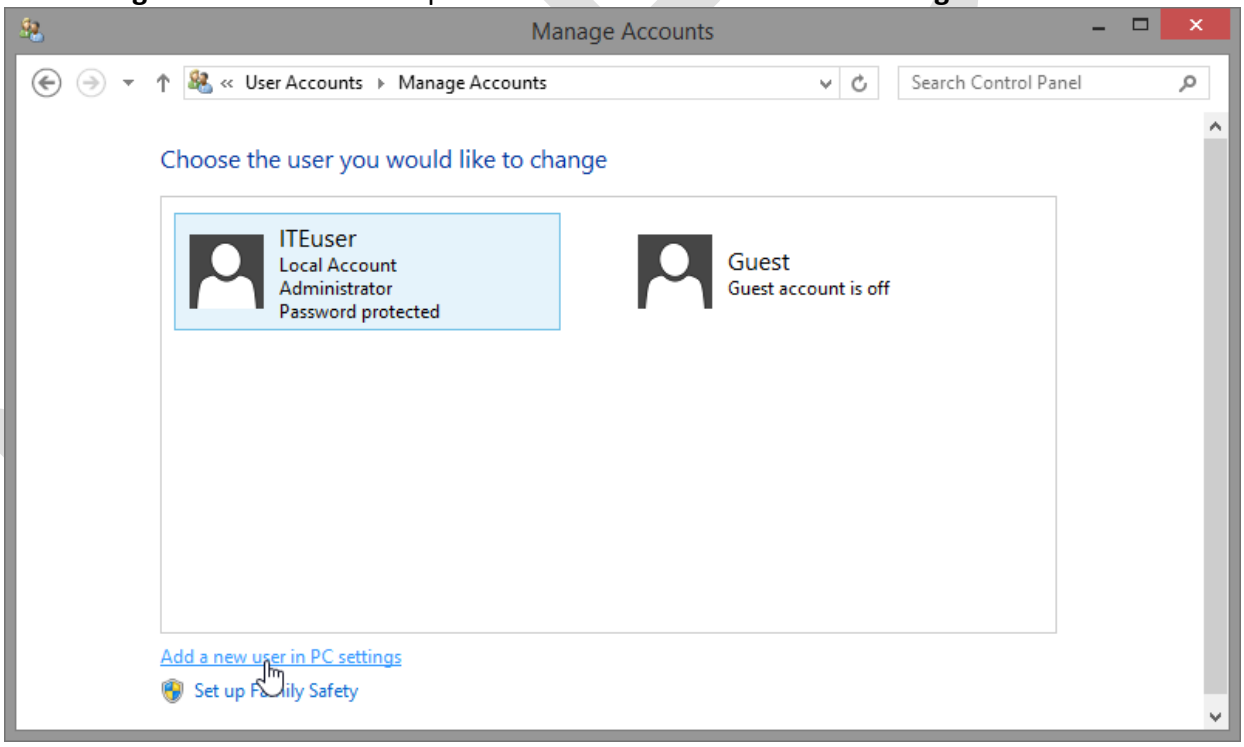


Step 2: Create an Account

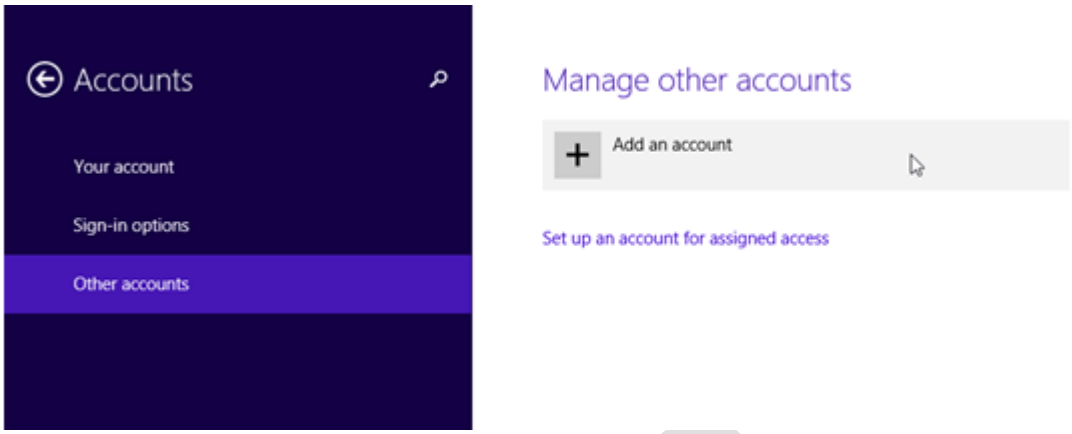
a. The **User Accounts** window opens. Click **Manage another account**.



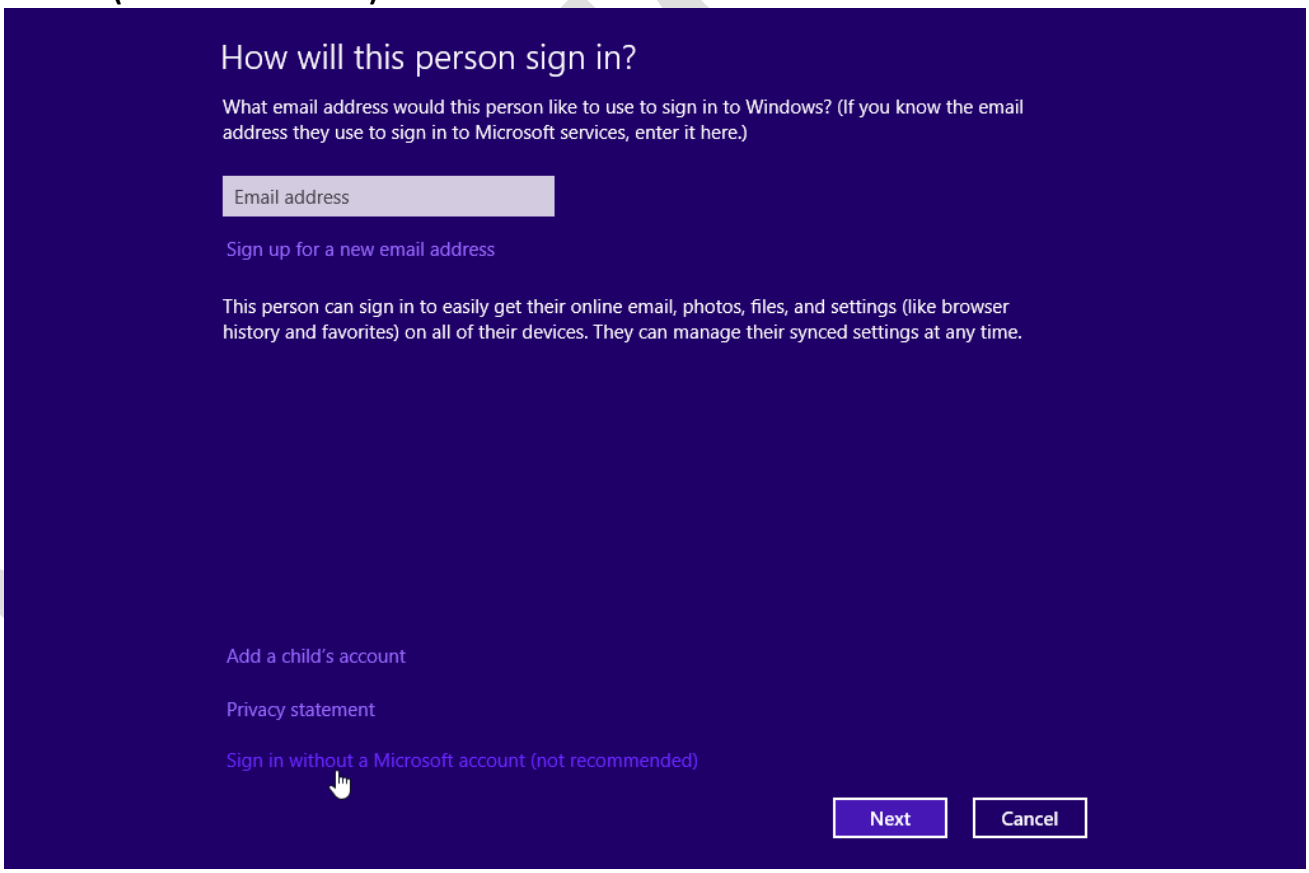
b. The **Manage Accounts** window opens. Click **Add a new user in PC settings**.



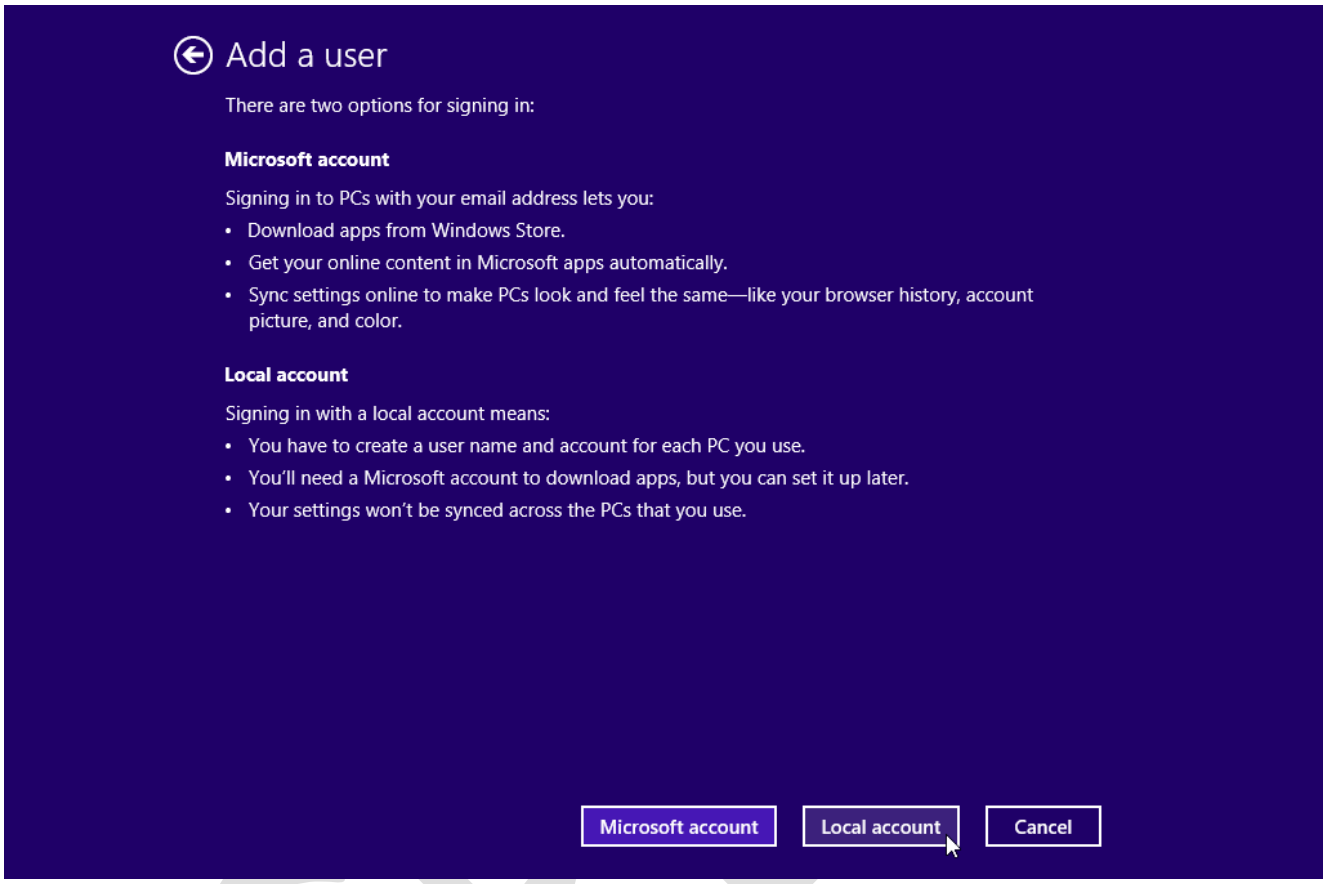
c. The **Manage other accounts** window opens. Click **Add an account.**



d. The **How will this person sign in?** window opens. Click **Sign in without a Microsoft account (not recommended)**.

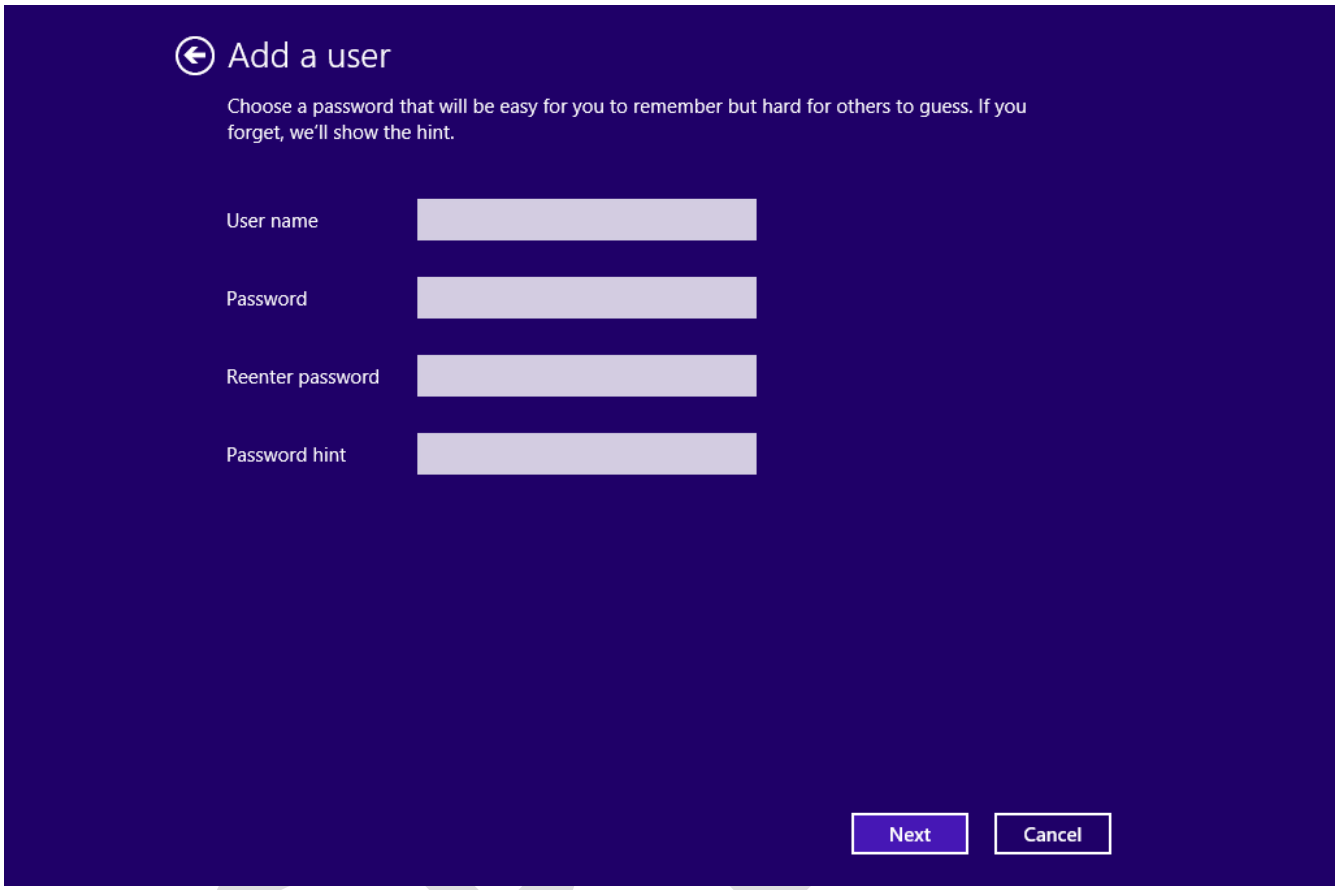


e. The **Add a user** window opens. Click **Local account**.



6.1.2.3 Lab – Create User Accounts in Windows 8 Answers Answers 06

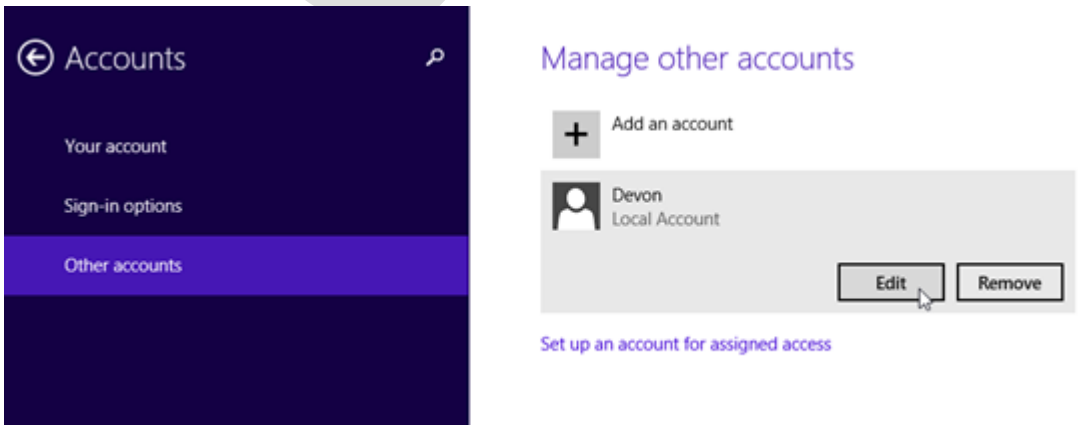
f. The second **Add a user** window opens. Type the name provided by your Answers in the **User name** field.



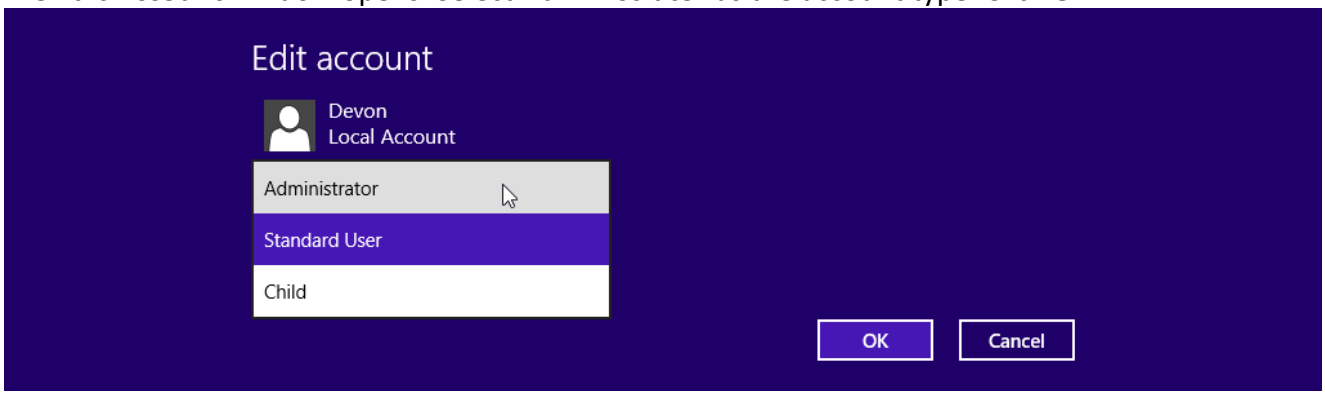
g. Type in the password provided by the Answers in the **Password** field.
h. Reenter the password in the **Reenter password** field.
i. Type a hint to help you remember the password in the **Password hint** field.
j. Click **Next**.
k. The final **Add a user** window opens. Click **Finish**.

Step 3: Change the Account Type

The **Manage other accounts** window opens. Click on the user you just created, and then click **Edit**.

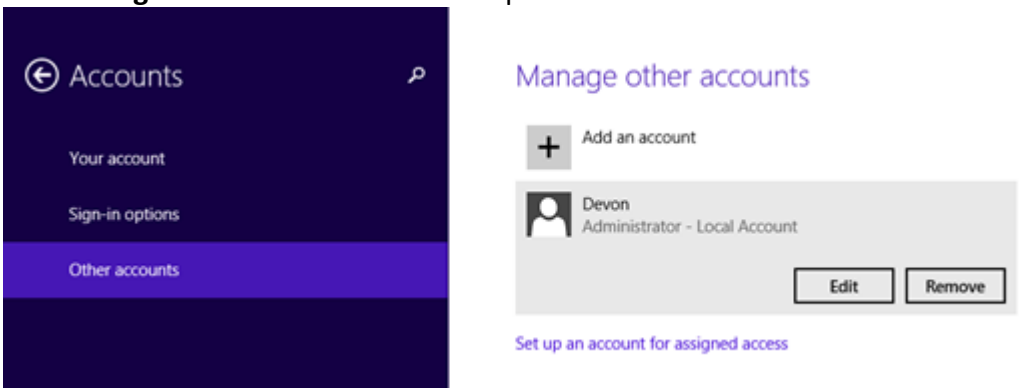


a. The **Edit Account** window opens. Select **Administrator** as the account type. Click **OK**.

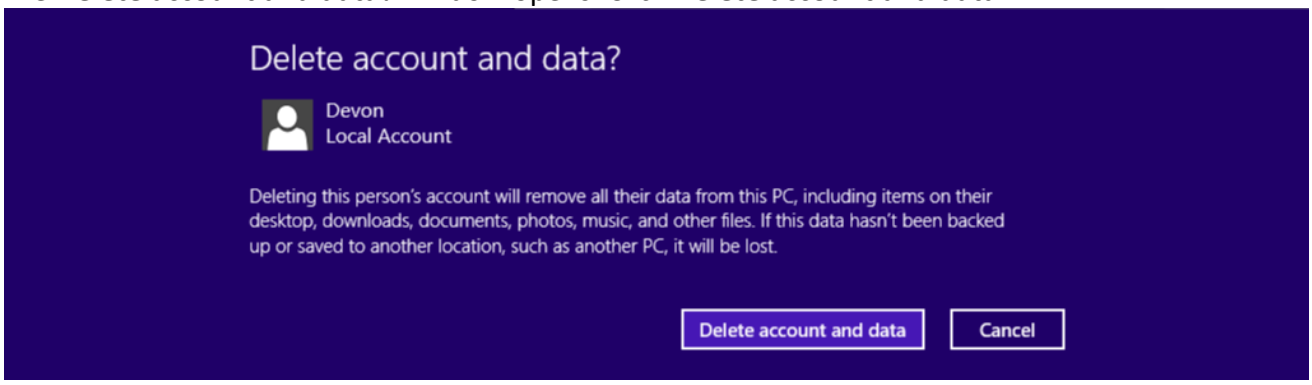


Step 4: Delete the Account

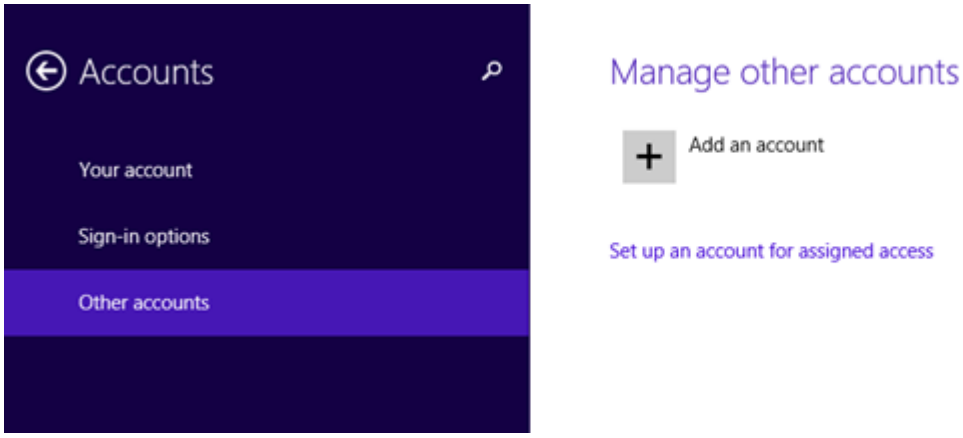
a. The **Manage other accounts** window opens. Click **Remove**.



b. The **Delete account and data?** window opens. Click **Delete account and data**.



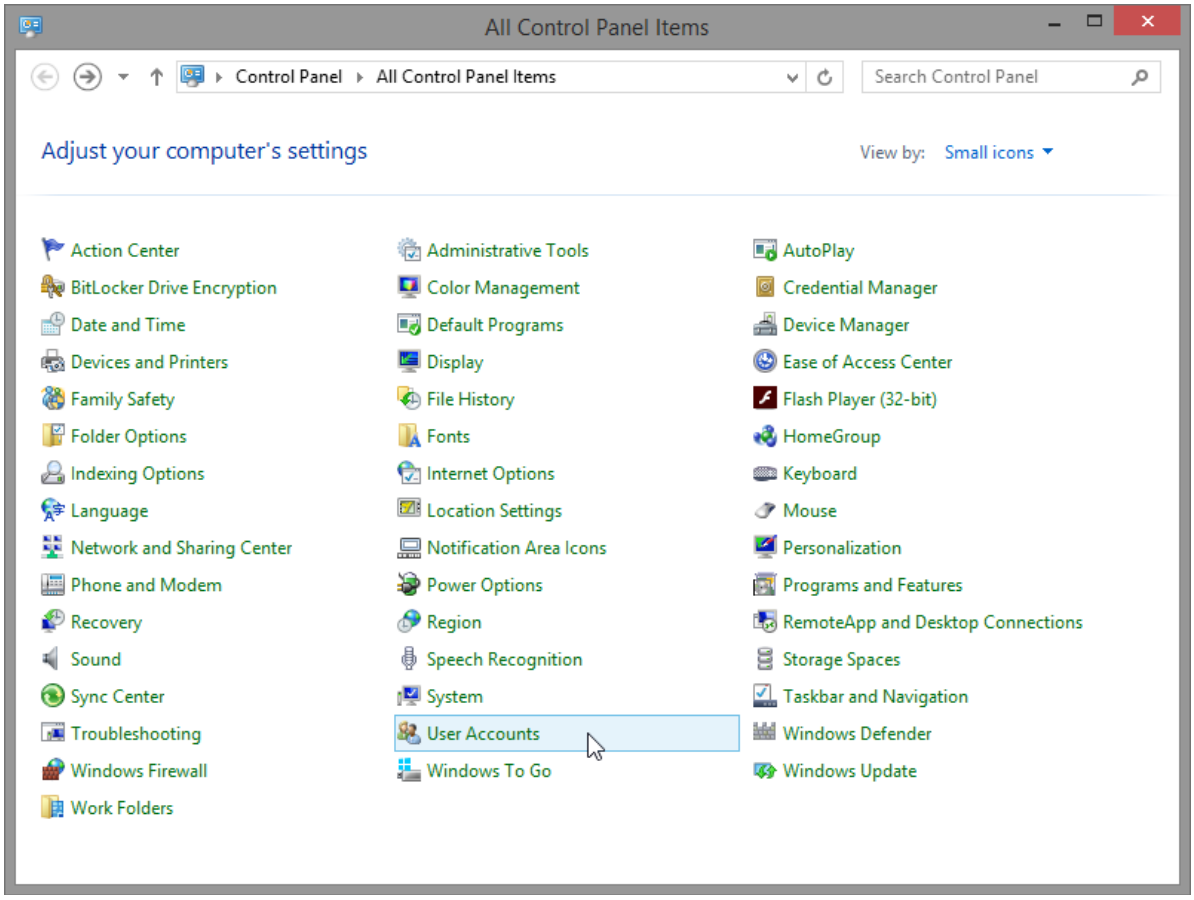
c. Notice the account is no longer listed. Close all open windows.



Part 2: Windows 8.0

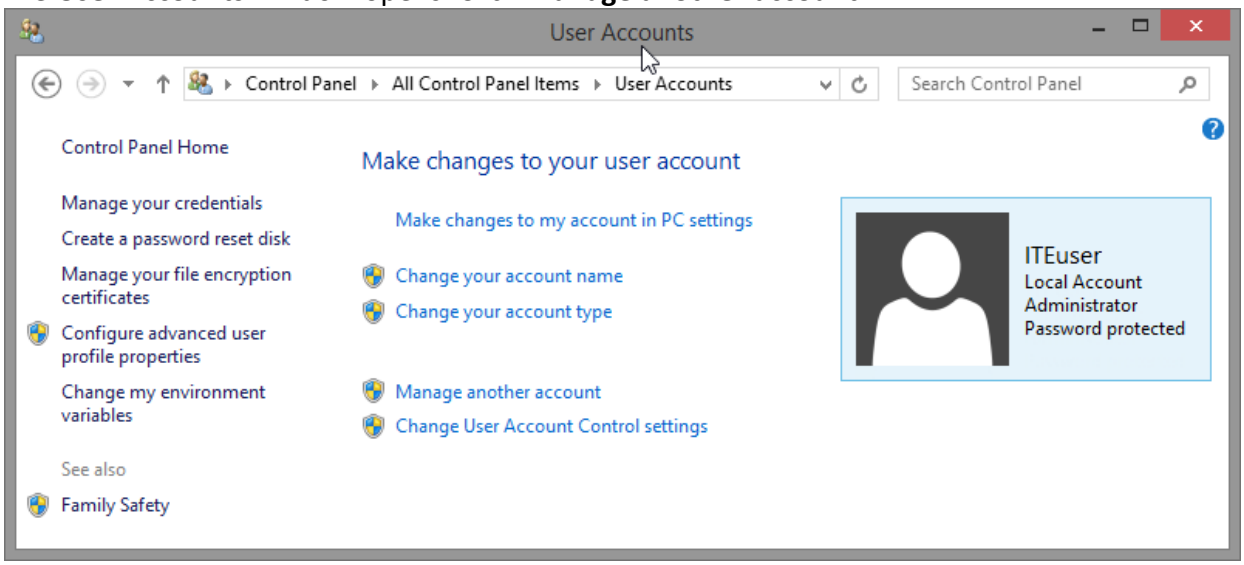
Step 1: Open the User Account Tool

a. Log on to the computer with an Administrator account.
b. Click **Control Panel > User Accounts**.

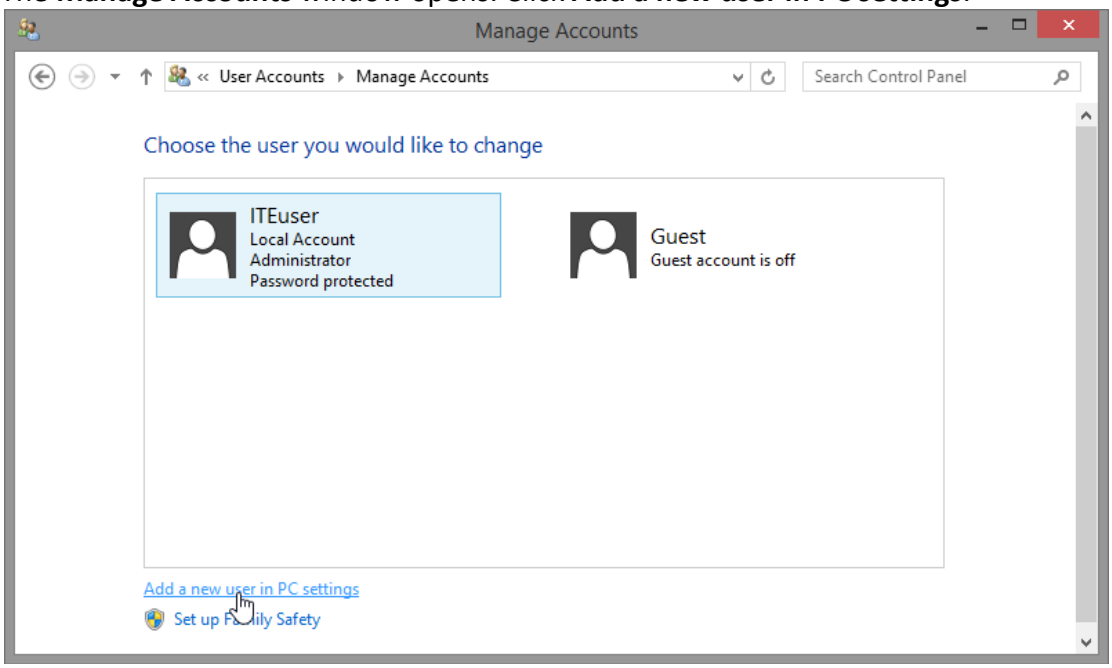


Step 2: Create an Account

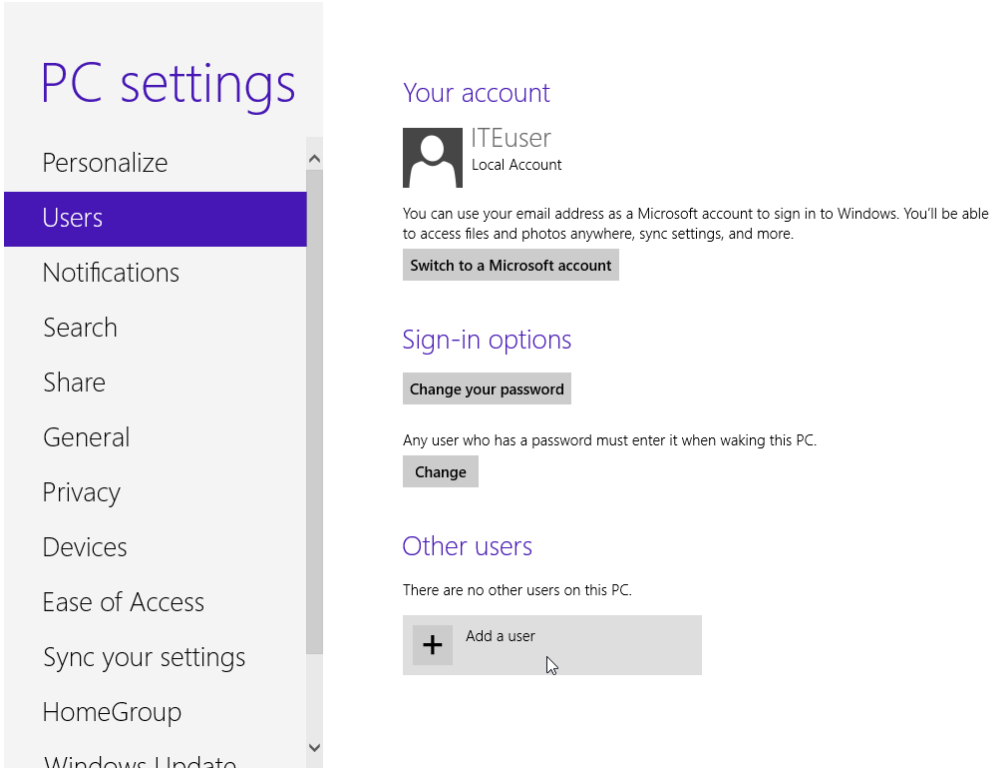
a. The **User Accounts** window opens. Click **Manage another account**.



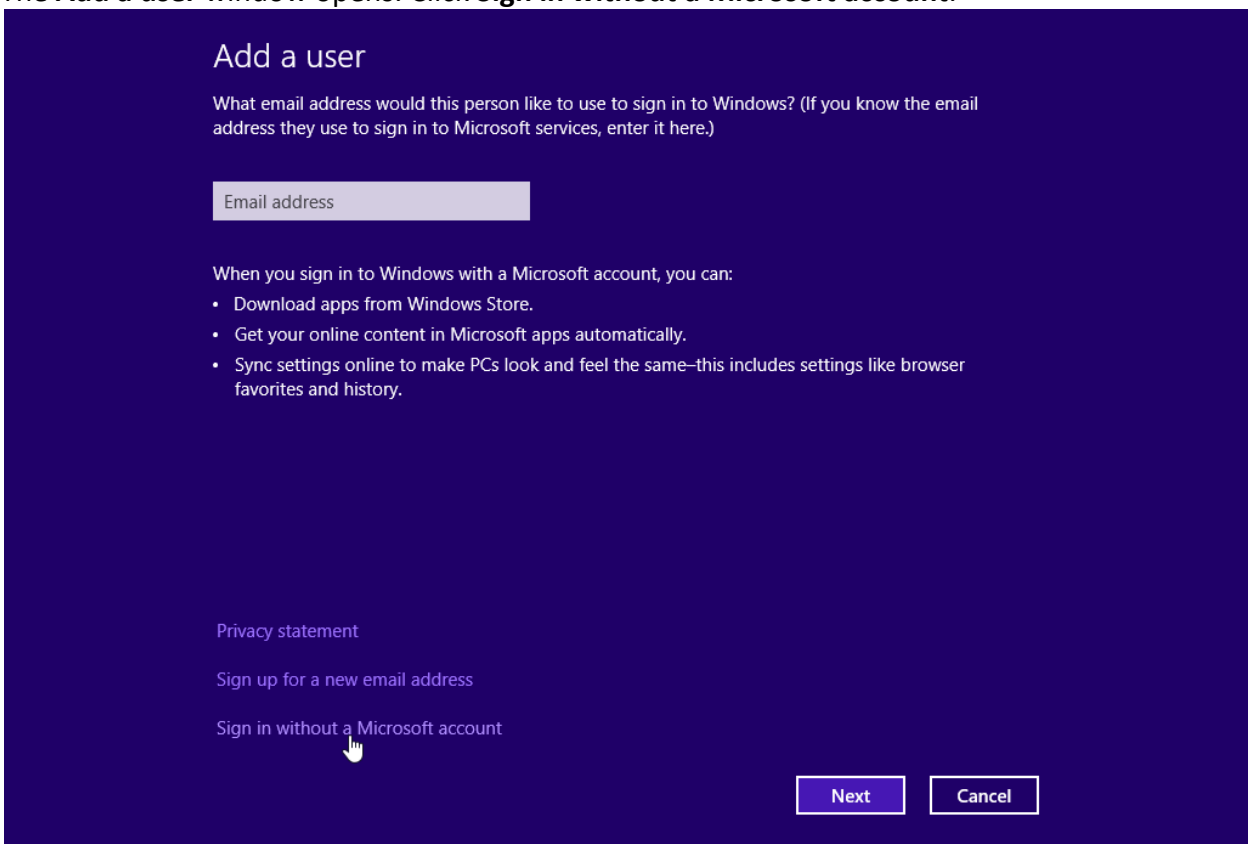
b. The **Manage Accounts** window opens. Click **Add a new user in PC settings**.



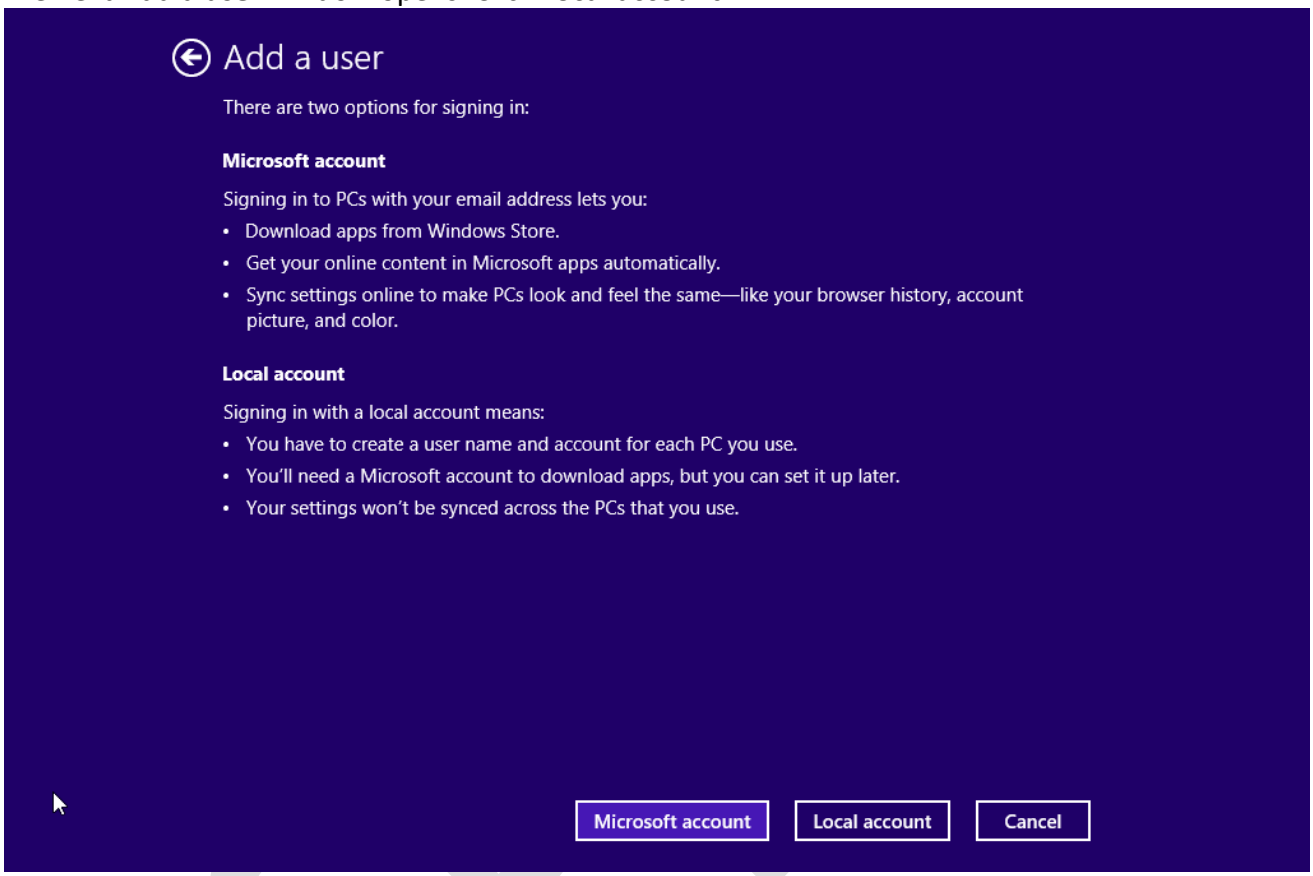
c. The **Manage other accounts** window opens. Click **Add a user**.



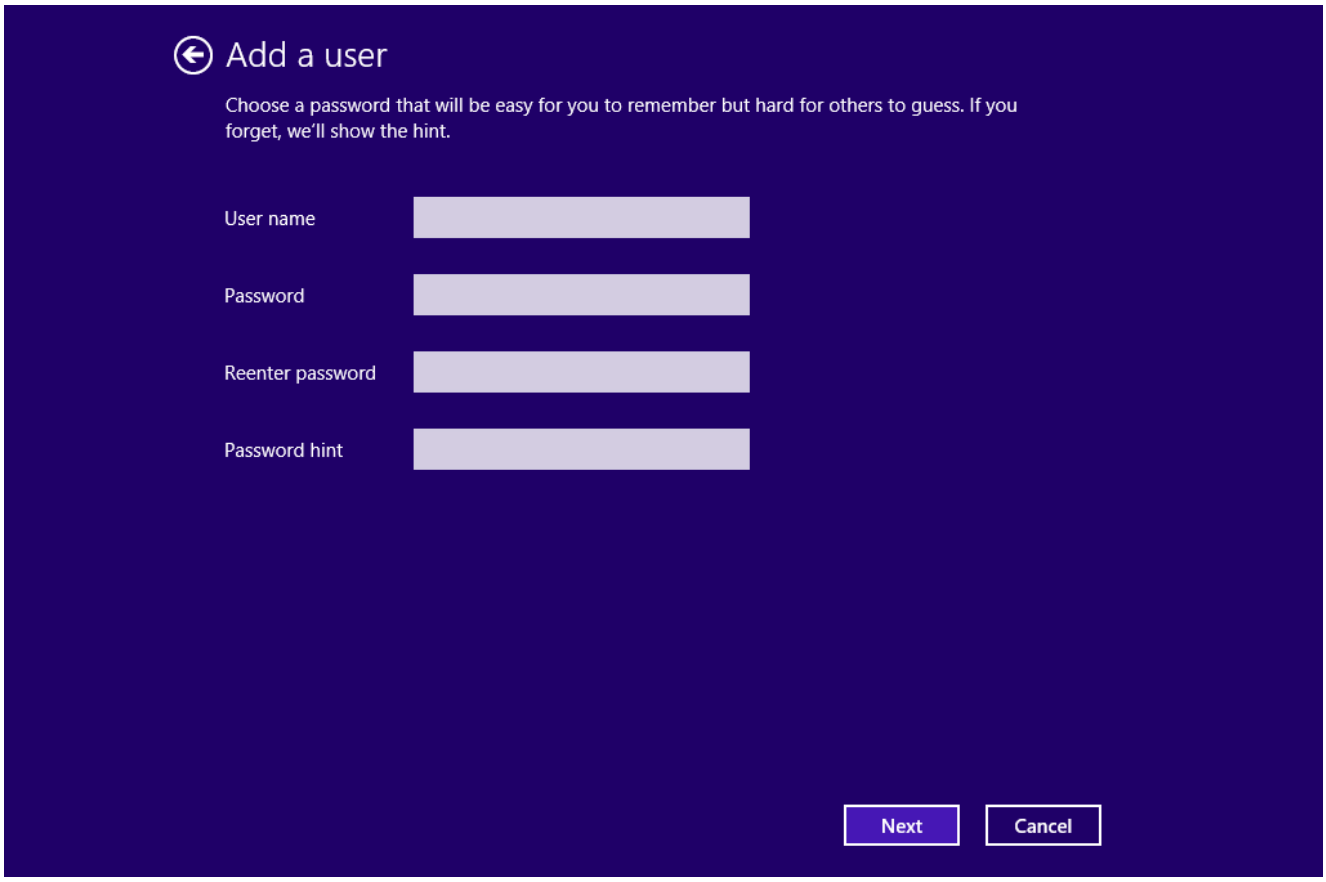
d. The **Add a user** window opens. Click **Sign in without a Microsoft account**.



e. The next **Add a user** window opens. Click **Local account**.

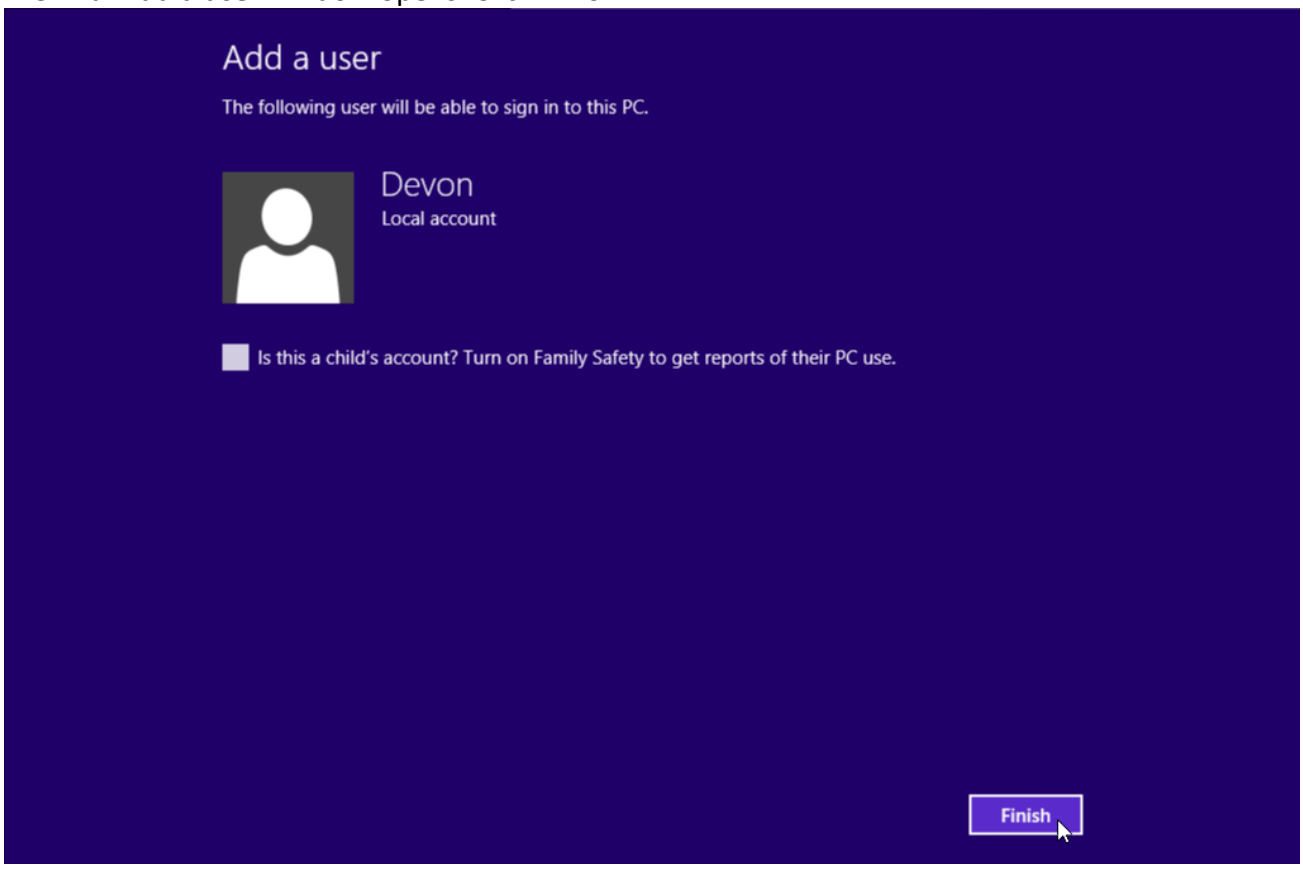


f. The third **Add a user** window opens. Type the name provided by your Answers in the **User name** field.

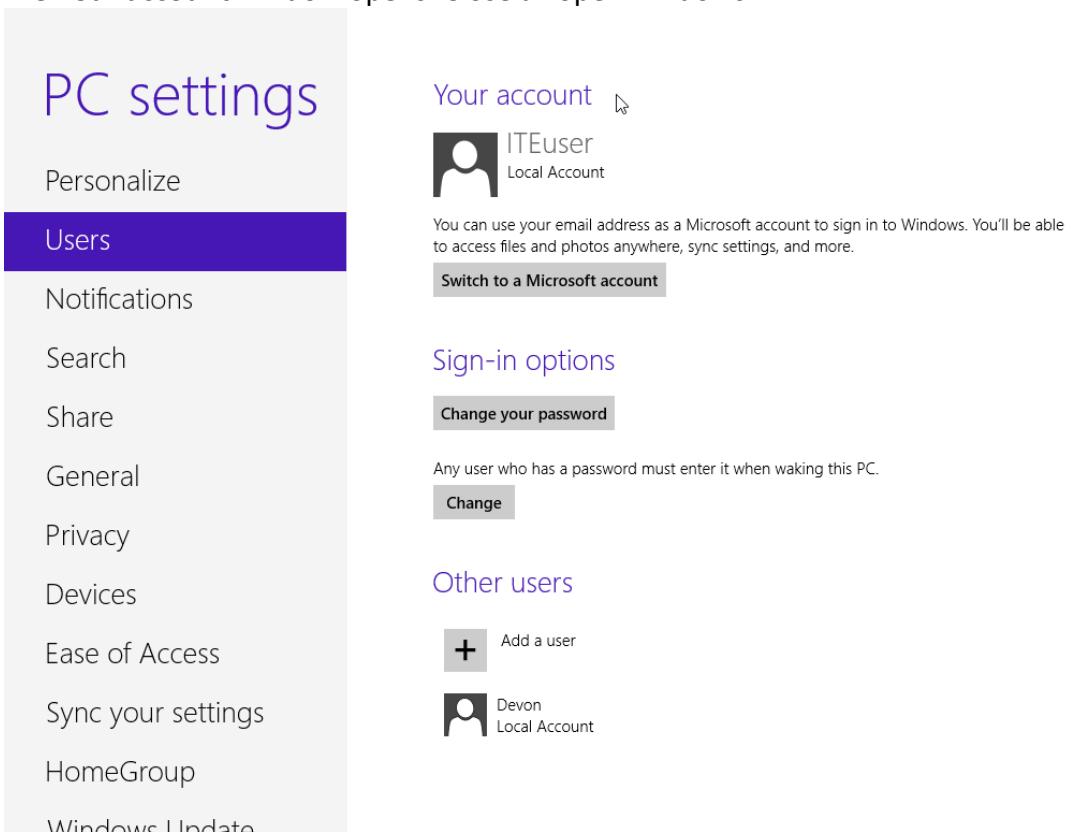


g. Type in the password provided by the Answers in the **Password** field.
h. Reenter the password in the **Reenter password** field.
i. Type a hint to help you remember the password in the **Password hint** field.
j. Click **Next**.

k. The final **Add a user** window opens. Click **Finish**.

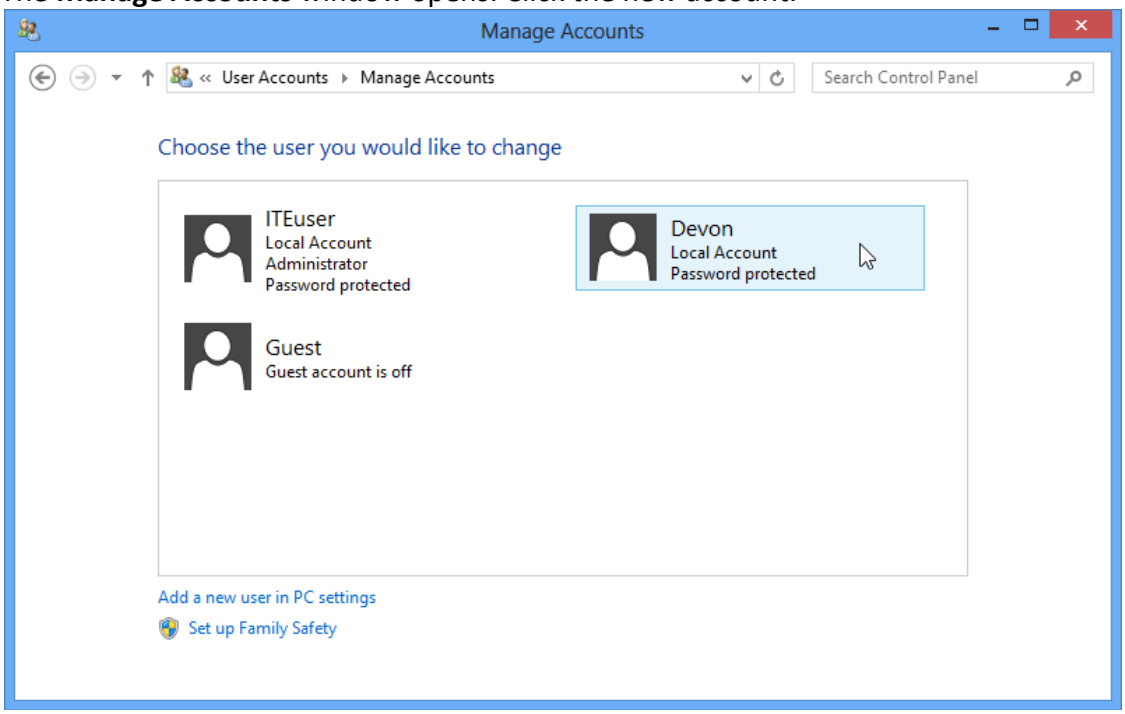


l. The **Your account** window opens. Close all open windows.

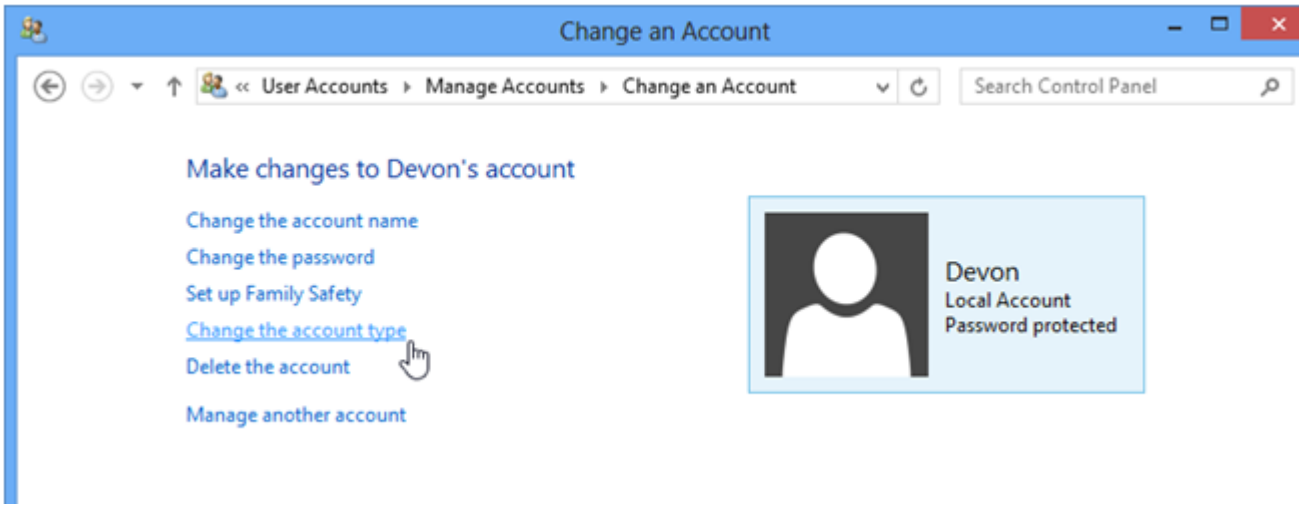


Step 3: Change the Account Type

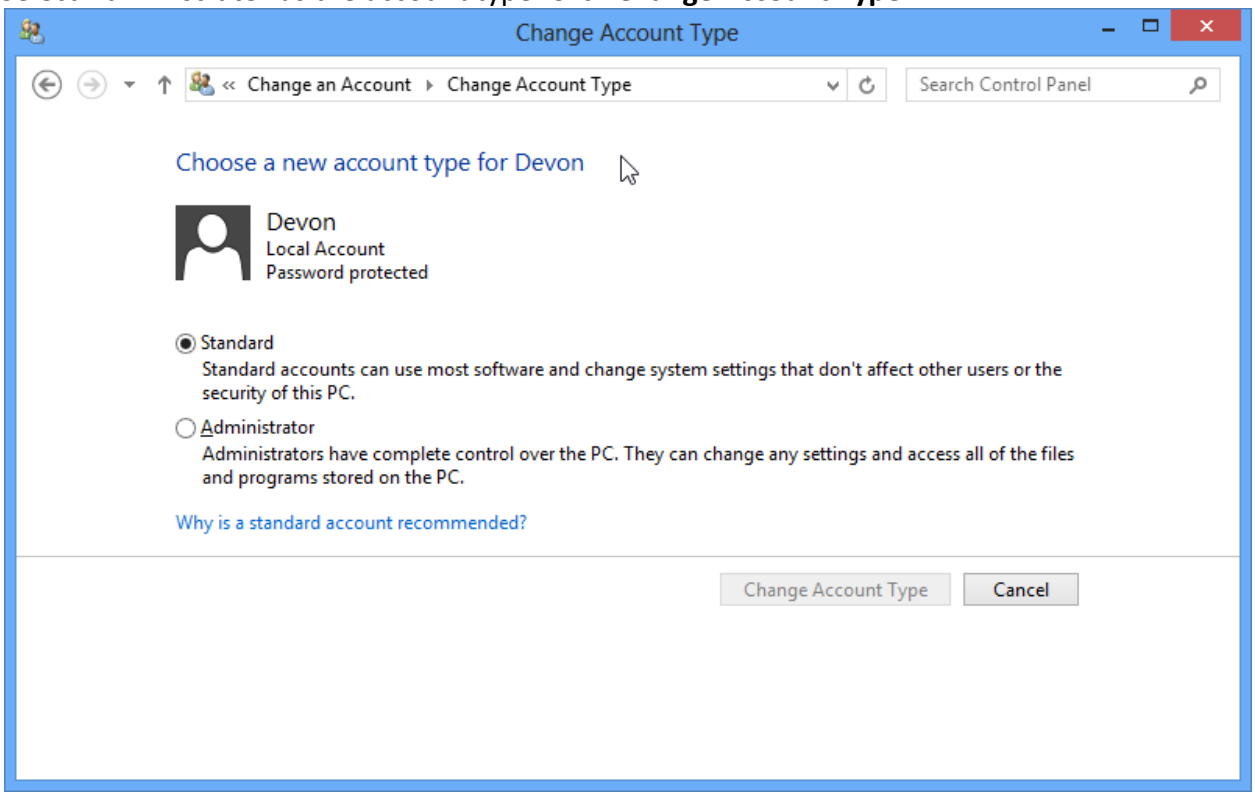
a. Click **Control Panel > User accounts > Manage another account**.
b. The **Manage Accounts** window opens. Click the new account.



c. The **Change an Account** window opens. Click **Change the account type**.



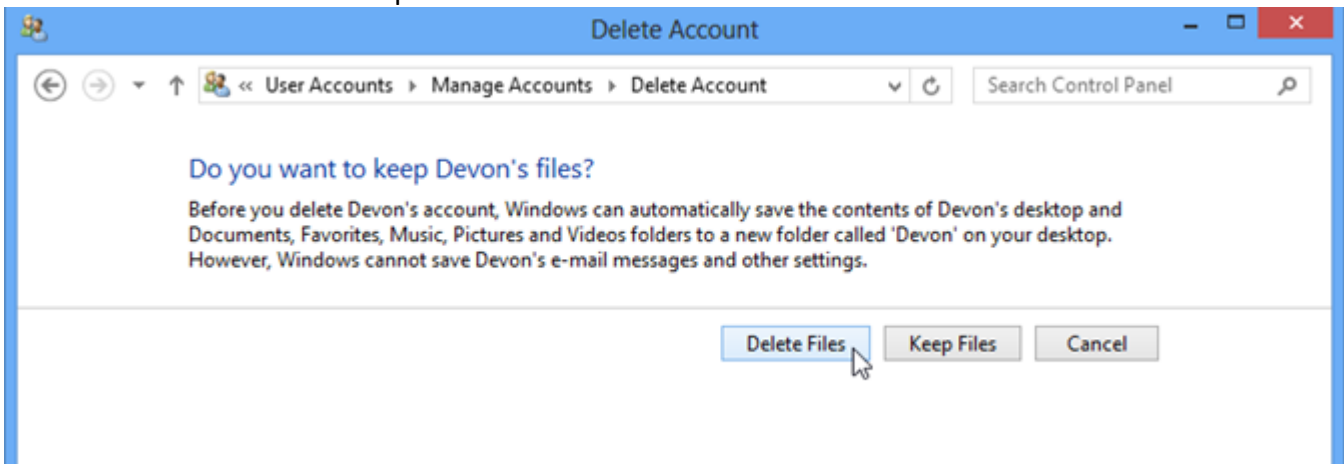
d. Select **Administrator** as the account type. Click **Change Account Type**.



.

Step 4: Delete the Account

a. The **Change an Account** window opens. Click **Delete the Account**.
b. The **Delete Account** window opens. Click **Delete Files**.



c. The **Confirm Deletion** window opens. Click **Delete Account**.
d. Notice the account is no longer listed. Close all opened windows.

Conclusion- In this experiment we learnt about managing user accounts in windows.

Experiment-7

Experiment: Sharing of Hardware resources (Eg:Printer) in the network.

Aim: Install Print server in a LAN and share the between two system in a LAN.

Equipment Required: Computers and Printer

Procedure:

To Install and configure printer:

1. Connect the printer to parallel port of the motherboard and power cable to AC. Switch on the system and printer.
2. Insert the driver disk in the CD drive.
3. Click start >control panel>printers and fax respectively.
4. Then >double click> add a printer>add printer wizard respectively.

Printer sharing:

a) Open Printers and Faxes. Click Start, click Control Panel, click Printers and Other Hardware, and then click Printers and Faxes.
b) Right-click the printer you want to share, and then click Sharing.On the Sharing tab, click Share this printer and then type a share name for the shared printer.
c) If you share the printer with others using different hardware or different operating systems, click Additional Drivers. Click the Environment and operating system for the other computers, and then click OK to install the additional drivers.
d) Click OK, or, if you have installed additional drivers, click Close.

To stop sharing your printer:

a) Open Printers and Faxes. Click Start, click Control Panel, click Printers and Other Hardware, and then click Printers and Faxes.
b) Right-click the printer you want to stop sharing, and then click Sharing.
c) On the Sharing tab, click Do Not share this printer.

To connect to a printer on a network:

1. Open Printers and Faxes. Click Start, click Control Panel, click Printers and Other Hardware, and then click Printers and Faxes.
2. Under Printer Tasks, click Add a printer to open the Add Printer Wizard, and then click Next.
3. Click A network printer, or a printer attached to another computer, and then click Next. Three Ways to Connect to a Printer on a Network:

To search for a printer in Active Directory:

1. Click Find a printer in the directory, and then click Next.
2. Click the Browse button to the right of Location, click the printer location, and then click

OK.

3. Click Find Now.
4. Click the printer you want to connect to, and then click okay

To locate a printer by typing the printer name:

1. Click Connect to this printer.
2. Do one of the following:
   Type the printer name using the following format: **\\printserver_name\share_name**
   Browse for it on the network. Click Next, click the printer in Shared printers.
   1. Click Next.

Conclusion: We have learned how to share printer(hardware resource) in a LAN.

Experiment-8

Experiment: Managing use of NETSTAT and its options

Aim: To study about managing use of NETSTAT and its options

Apparatus Required:

1. A computer with a new installation of Windows 8
2. An account with administrator privileges

Theory:

Netstat is a common command line TCP/IP networking utility available in most versions of Windows, Linux, UNIX and other operating systems. Netstat provides information and statistics about protocols in use and current TCP/IP network connections. (The name derives from the words network and statistics.)

Netstat is a useful tool for checking network and Internet connections. Some useful applications for the average PC user are considered, including checking for malware connections.

When dealing with excessive traffic and malicious software it's advantageous to be informed about the inbound and outbound connections to your computer. These are created via their respective network addresses that indicate which ports were preemptively opened for exchanging data. Once a port is opened, it receives the status "LISTEN" and waits for connection attempts. One problem of having these ports remain open is that your system is then left vulnerable to malware. What's more, there's also a chance that Trojan viruses already found in your system may install a backdoor, opening up a corresponding port in the process. For this reason, you should always regularly check the ports opened by your system, a task for which netstat is particularly well suited. Possible infections can be caught based on unknown opened ports or unknown IP addresses. In order to obtain an informative result, all other programs, such as your internet browser, should be turned off. This is due to the fact that these are often connected with computers that possess unknown IP addresses. Thanks to the detailed statistics, users also receive information on the packets that have been transferred since the last system start as well as notices of any errors that have occurred. The routing table, which delivers information on the paths data packets takes through the net, can be displayed with the help of the system-specific netstat command.

The command syntax is

```
netstat [-a] [-b] [-e] [-f] [-n] [-o] [-p proto] [-r] [-s] [-t] [-x] [-y] [Interval]
```

The combination of the individual options works by stringing the individual parameters together, each separated by a space:

```
netstat [-OPTION1] [-OPTION2] [-OPTION3] …
```

The parameters are typically preceded by a **hyphen (-)**, but if you want to combine several options, you only have to place this hyphen in front of the first element. Instead of the variant shown above, you can also link different parameters as follows:

```
netstat [-OPTION1][OPTION2][OPTION3] …
```

In this case, it is important that you do not leave any spaces between the individual netstat options.

Netstat options and commands for Windows

[OPTION]	Command	Description
	Netstat	Standard listing of all active connections
-a	netstat –a	Displays all active/ listening ports
-b	netstat –b	Displays the executable file of a connection or listening port (requires administrator rights)
-e	netstat –e	Shows statistics about your network connection (received and sent data packets, etc.) Displays Ethernet statistics
-f	netstat –f	Displays the fully qualified domain name (FQDN) of remote/foreign addresses
-i	netstat –i	Brings up the netstat overview menu
-n	netstat –n	Numerical display of addresses and port numbers
-o	netstat –o	Displays the owning process identifier (PID) associated with each displayed connection
-p proto	netstat -p TCP	Displays the connections for the protocol specified by proto, proto may be any of TCP, UDP, TCPv6, or UDPv6
-q	netstat –q	Lists all connections, all listening TCP ports, and all open TCP ports that are not listening

-r	netstat –r	Displays the IP routing table
-s	netstat –s	Retrieves statistics about the important network protocols such as TCP, IP, or UDP
-t	netstat –t	Shows the download status (TCP download to relieve the main processor) of active connections
-x	netstat –x	Informs about all connections, listeners, and shared endpoints for NetworkDirect
-y	netstat –y	Displays which connection templates were used for the active TCP connections
Interval	netstat -p 10	Displays the respective statistics again after a selected number of seconds (here 10); can be combined as required (here with –p), [CTRL] + [C] ends the interval display. Default setting is to display once.
/?	netstat /?	Use the help switch to show details about the netstat command's several options.

Procedure :

In Windows operating systems, you can use the netstat services via the command line (cmd.exe). You can find them in the start menu under "All Programs" -> "Accessories" -> "Command Prompt". Alternatively, you can search directly for "Command Prompt" in the **start menu's search field** or start the command line via "Run" (Windows key + press "R" and enter "cmd").

1. Displaying connections

(a) If you run netstat without specifying any parameters, you get a list of active connections, all the Established and Waiting for TCP connections. something like this:

```
C:\>netstat
Active Connections
  Proto Local Address   Foreign Address                 State
  TCP     Doug:1463     192.168.168.10:1053             ESTABLISHED
  TCP     Doug:1582     192.168.168.9:netbios-ssn       ESTABLISHED
  TCP     Doug:3630     192.168.168.30:9100             SYN_SENT
  TCP     Doug:3716     192.168.168.10:4678             ESTABLISHED
  TCP     Doug:3940     192.168.168.10:netbios-ssn      ESTABLISHED
```

```
C:\>
```

This list shows all the active connections on the computer and indicates the local port used by the connection, as well as the IP address and port number for the remote computer.

(b) Running netstat with a number after the command continues to run the command until stopped. In this case, netstat would be refreshed every five seconds. To cancel, press Ctrl+C.

```
C:\>netstat 5
```

An explanation of the different connection states is given in Table –

State	Description
CLOSED	Indicates that the server has received an ACK signal from the client and the connection is closed
CLOSE_WAIT	Indicates that the server has received the first FIN signal from the client and the connection is in the process of being closed
ESTABLISHED	Indicates that the server received the SYN signal from the client and the session is established
FIN_WAIT_1	Indicates that the connection is still active but not currently being used
FIN_WAIT_2	Indicates that the client just received acknowledgment of the first FIN signal from the server
LAST_ACK	Indicates that the server is in the process of sending its own FIN signal
LISTENING	Indicates that the server is ready to accept a connection
SYN_RECEIVED	Indicates that the server just received a SYN signal from the client
SYN_SEND	Indicates that this particular connection is open and active
TIME_WAIT	Indicates that the client recognizes the connection as still active but not currently being used

(c) You can use below syntax to view all **established** connection from/to your Windows server.

```
C:\> netstat | findstr ESTABLISHED
```

Similarly, to view LISTEN, CLOSE_WAIT, TIME_WAIT you can just use as follows.

```
netstat | findstr LISTEN
netstat | findstr CLOSE_WAIT
netstat | findstr TIME_WAIT
```

2. Display connections in both local and foreign addresses in numeric IP form

(a)

```
C:\>netstat -n
Active Connections
Proto  Local Address          Foreign Address        State
TCP    192.168.168.21:1463    192.168.168.10:1053    ESTABLISHED
TCP    192.168.168.21:1582    192.168.168.9:139      ESTABLISHED
TCP    192.168.168.21:3658    192.168.168.30:9100    SYN_SENT
TCP    192.168.168.21:3716    192.168.168.10:4678    ESTABLISHED
TCP    192.168.168.21:3904    207.46.106.78:1863     ESTABLISHED
TCP    192.168.168.21:3940    192.168.168.10:139     ESTABLISHED
```

(b)

```
C:\>netstat -an
```

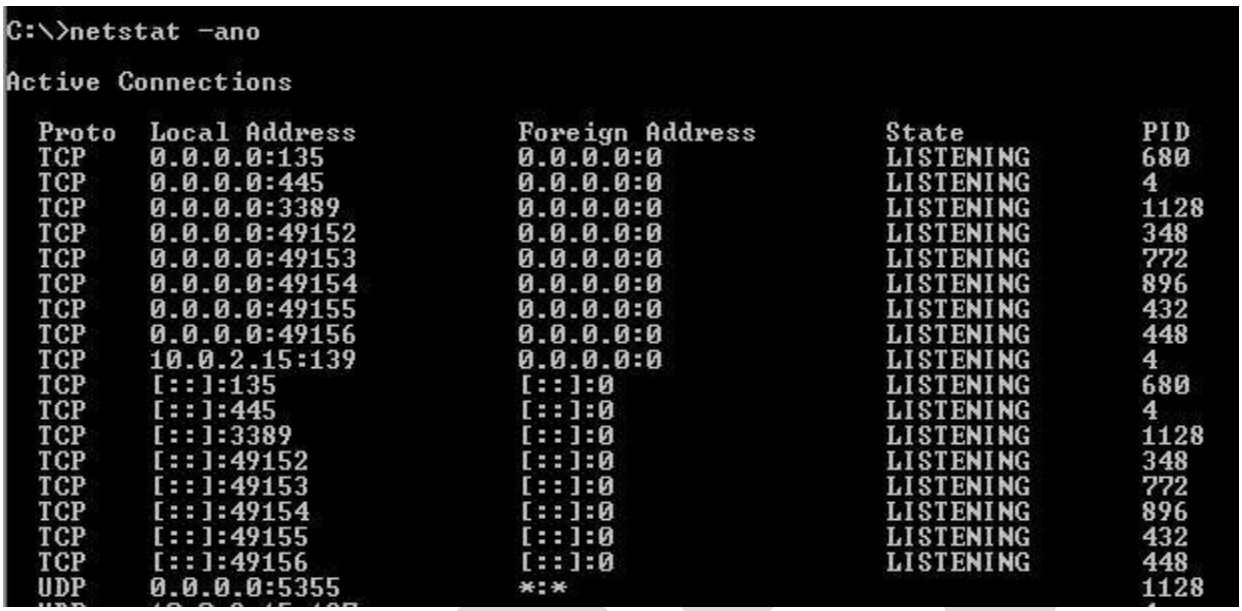
Displays all connections on the computers in numerical format, only displaying the local and foreign IP and port addresses. The information that is displayed includes the protocol, the local address, the remote (foreign) address, and the connection state.

```
C:\Documents and Settings\Owner>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1027         0.0.0.0:0              LISTENING
  TCP    192.168.1.100:139      0.0.0.0:0              LISTENING
  TCP    192.168.1.100:2558     207.68.172.236:80      CLOSE_WAIT
  TCP    192.168.1.100:2916     204.14.90.25:21        CLOSE_WAIT
  TCP    192.168.1.100:2923     69.65.109.55:80        TIME_WAIT
  TCP    192.168.1.100:2924     204.245.162.25:80      ESTABLISHED
  TCP    192.168.1.100:2925     66.150.96.119:80       ESTABLISHED
  TCP    192.168.1.100:2930     204.245.162.27:80      ESTABLISHED
  UDP    0.0.0.0:445            *:*
  UDP    0.0.0.0:500            *:*
  UDP    0.0.0.0:1030           *:*
  UDP    0.0.0.0:1040           *:*
  UDP    0.0.0.0:1155           *:*
  UDP    0.0.0.0:1175           *:*
  UDP    0.0.0.0:4500           *:*
  UDP    127.0.0.1:123          *:*
  UDP    127.0.0.1:1036         *:*
  UDP    127.0.0.1:1900         *:*
  UDP    127.0.0.1:2922         *:*
  UDP    192.168.1.100:123      *:*
  UDP    192.168.1.100:137      *:*
  UDP    192.168.1.100:138      *:*
  UDP    192.168.1.100:1900     *:*
```

3. Display of all open ports and active connections (numeric and process ID included)

One of the most popular netstat commands is undoubtedly to query all open ports and active connections (including process ID) in numeric form:

```
netstat -ano
```



```
C:\>netstat -ano

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       680
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING       1128
  TCP    0.0.0.0:49152          0.0.0.0:0              LISTENING       348
  TCP    0.0.0.0:49153          0.0.0.0:0              LISTENING       772
  TCP    0.0.0.0:49154          0.0.0.0:0              LISTENING       896
  TCP    0.0.0.0:49155          0.0.0.0:0              LISTENING       432
  TCP    0.0.0.0:49156          0.0.0.0:0              LISTENING       448
  TCP    10.0.2.15:139          0.0.0.0:0              LISTENING       4
  TCP    [::]:135               [::]:0                 LISTENING       680
  TCP    [::]:445               [::]:0                 LISTENING       4
  TCP    [::]:3389              [::]:0                 LISTENING       1128
  TCP    [::]:49152             [::]:0                 LISTENING       348
  TCP    [::]:49153             [::]:0                 LISTENING       772
  TCP    [::]:49154             [::]:0                 LISTENING       896
  TCP    [::]:49155             [::]:0                 LISTENING       432
  TCP    [::]:49156             [::]:0                 LISTENING       448
  UDP    0.0.0.0:5355           *:*                                    1128
```

The command netstat -ano lists all open ports and active connections numerically, including process ID.

3. Show PID used by port number

A very handy when you have to find out which PID is using the particular port number..

```
C:\>netstat –o | findstr $portnumber
```

Let’s suppose you want to monitor if a port is listening at a constant interval. Windows netstat command can accept sleep interval.

```
C:\>netstat –abo 5| findstr 8080
```

here the interval is 5 seconds,The `netstat -abo` command would run every 5 seconds until interrupted or stopped with CTRL+C

4. Displaying interface statistics

```
C:\>netstat -e
Interface Statistics

                           Received            Sent
```

```
Bytes                          672932849         417963911
Unicast packets     1981755 1972374
Non-unicast packets            251869            34585
Discards            0                    0
Errors                         0                 0
Unknown protocols              1829
C:\>
```

The items to pay attention to in this output are the Discards and Errors. These numbers should be zero, or at least close to it. If they're not, the network may be carrying too much traffic or the connection may have a physical problem. If no physical problem exists with the connection, try segmenting the network to see whether the error and discard rates drop.

5. **Display Detailed Ethernet and Connection Usage Statistics**

```
C:\>netstat -es
```

Repetitive query of interface statistics (every 20 seconds)

Use the following netstat command for a repeated query of the interface statistics, which returns new values every 20 seconds on received and sent data packets:

```
C:\>netstat -e 20
```

6. Show statistics of all protocols

Useful when you have to find out for any received header error, received address error, discarded packet, etc. It will list out statistics from IPv4, IPv6, ICMPv4, ICMPv6, TCP, UDP, etc.

```
C:\>netstat -s
```

Note: to find out any errors quickly you can use syntax.

```
C:\>netstat -s | findstr Errors
Received Header Errors = 0
 Received Address Errors = 0
 Received Header Errors = 0
 Received Address Errors = 0
 Errors 0 0
 Errors 0 0
 Receive Errors = 0
 Receive Errors = 0
C:\Windows\system32
```

The command findstr Errors is used to find the string or the term “Errors” being displayed in the display list of a command and so it helps out in finding the list of errors if any.

7. List of all connections for the IPv4 protocol

If you don't want to retrieve all active connections, but only all active IPv4 connections, you can do this using the netstat command:

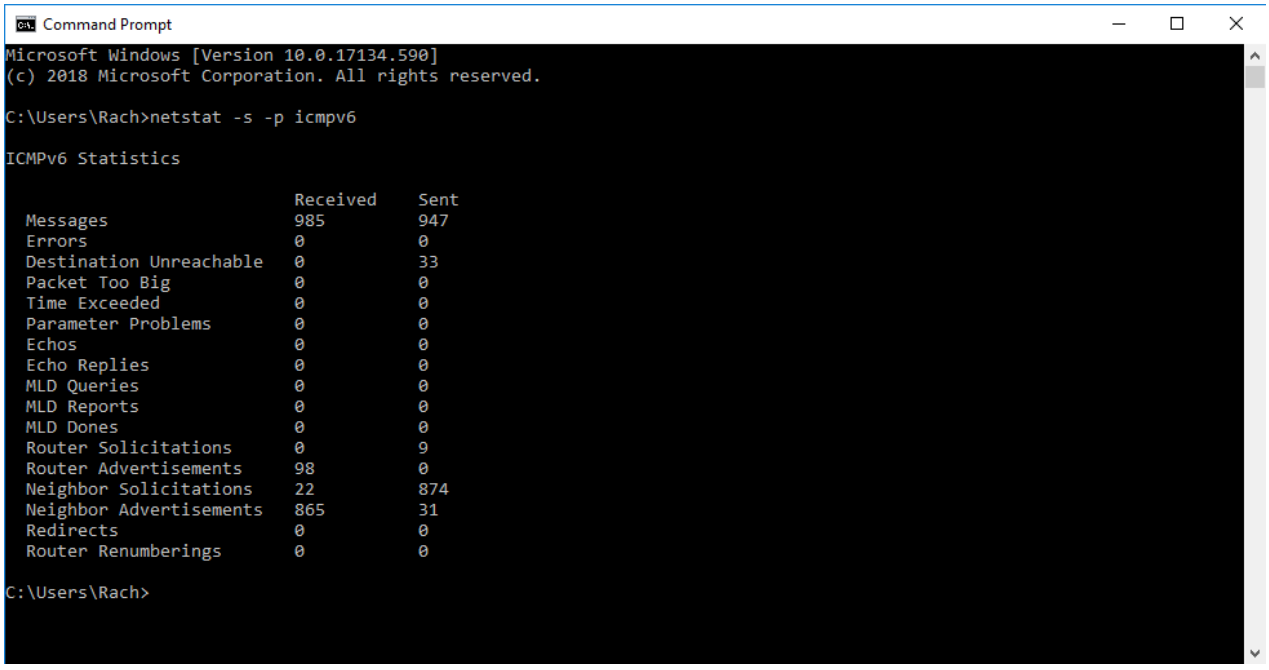
```
C:\>netstat -p IP
```

8. Accessing statistics using the ICMPv6 protocol

If you only want to obtain statistics on the ICMPv6 protocol, enter the following command in the command line:

```
C:\>netstat -s -p icmpv6
```

The output will then look something like this:



To access the statistics for the previous ICMPv6 version 4, replace "icmpv6" with "icmp" in the command shown here.

9. Show routing information

To display Route Table, you can use below syntax. The following syntax will also list all interfaces.

```
C:\>netstat -r
```

Conclusion: In this experiment we have learnt about NETSTAT and its options.

Experiment-9

Experiment: Connectivity troubleshooting using PING, IPCONFIG

Aim: To check connectivity and troubleshooting using PING and IPCONFIG.

Equipment Required: Computer

Procedure:

1. Open Command Prompt, and then type ipconfig. From the display of the ipconfig command, ensure that the network adapter for the TCP/IP configuration you are testing is not in a Media disconnected state.

2. At the command prompt, ping the loopback address by typing ping 127.0.0.1.

3. Ping the IP address of the computer.

4. Ping the IP address of the default gateway. If the ping command fails, verify that the default gateway IP address is correct and that the gateway (router) is operational.

5. Ping the IP address of a remote host (a host that is on a different subnet).
6. If the ping command fails, verify that the remote host IP address is correct, that the remote host is operational, and that all of the gateways (routers) between this computer and the remote host are operational.

7. Ping the IP address of the DNS server.
8. If the ping command fails, verify that the DNS server IP address is correct that the DNS server is operational, and that all of the gateways (routers) between this computer and the DNS server are operational.

Conclusion: In the above experiment we have learnt the usage of ipconfig and ping.

Experiment-10

Experiment - Introduction to Cisco Packet Tracer7.2.2

Aim: To get familiarized with Cisco Packet Tracer 7.2.2

Software used: Cisco Packet Tracer 7.2.2 (for 64-bit machine)

Theory:

Introduction: Packet Tracer is a cross-platform visual simulation tool designed by Cisco Systems that allows users to create network typologies and imitate modern computer networks. The software allows users to simulate the configuration of Cisco routers and switches using a simulated command line interface.

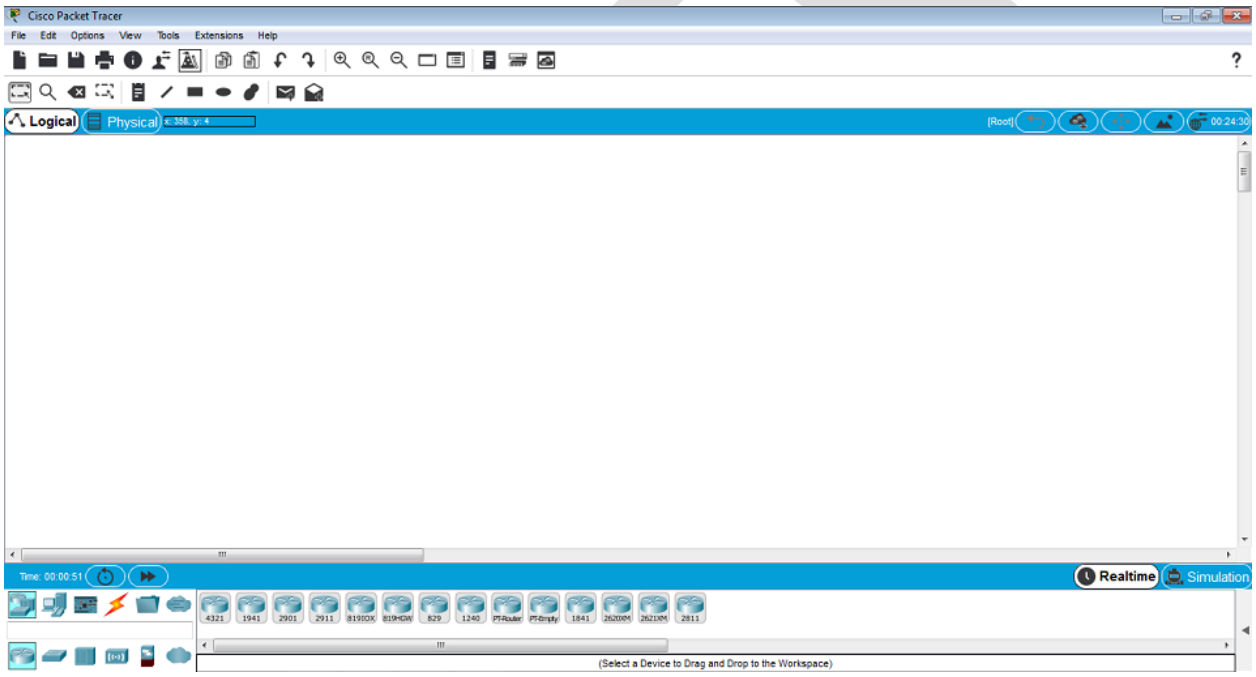


Fig1. Packet tracer Home Screen

Navigating in Cisco Packet Tracer 7.2.2 : Open Packet Tracer. On the lower left corner, there are all the components required for creating our network as shown in fig2. There are routers, switches, End devices, Hubs, Wireless Devices, and Connections etc.

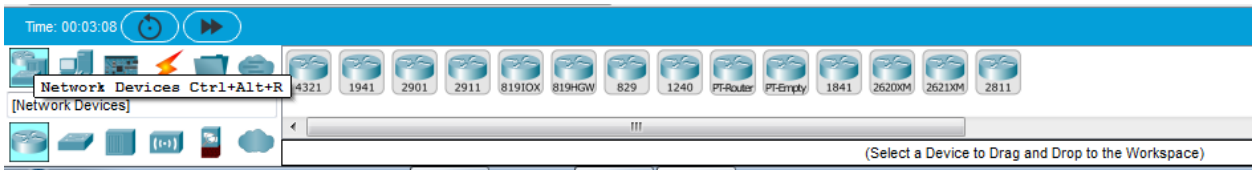


Fig2. List showing Network Devices

Intermediate Devices: Click on “Network Devices” and then a group of Network devices will be displayed as shown in the figure. Click on “Router” to select and place the available routers such as 4312,1941,2901,2911 etc. Likewise to select the switch and hub click on corresponding symbols and select the required intermediate device from the list of available devices and drag to place in the home screen.

End Devices: Click on “End Devices” symbol to select an end device among the available devices such as PC, Laptop, Server etc. Drag it to place the selected end device in the home screen.

Fig 3. List showing End Devices

Connections: The connection icon is used to select different connection media which are used to connect the network devices. The types of connection media available are: Console, Copper straight-through, copper cross-over, fiber, phone, coaxial, Serial DCE, serial DTE, USB etc. When two devices are connected, If the connection end points are **red**, then there is some problem with your wiring. If end points show **green**, then your wiring is alright.

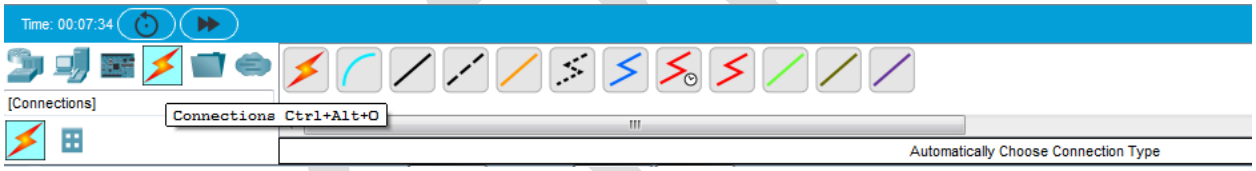


Fig4. List showing types of connections

Packet Tracer Modes: Cisco Packet Tracer provides two operating modes to visualize the behavior of a network—real-time mode and simulation mode. In real-time mode the network behaves as real devices do, with immediate real-time response for all network activities. In simulation mode the user can see and control time intervals, the inner workings of data transfer, and the propagation of data across a network.

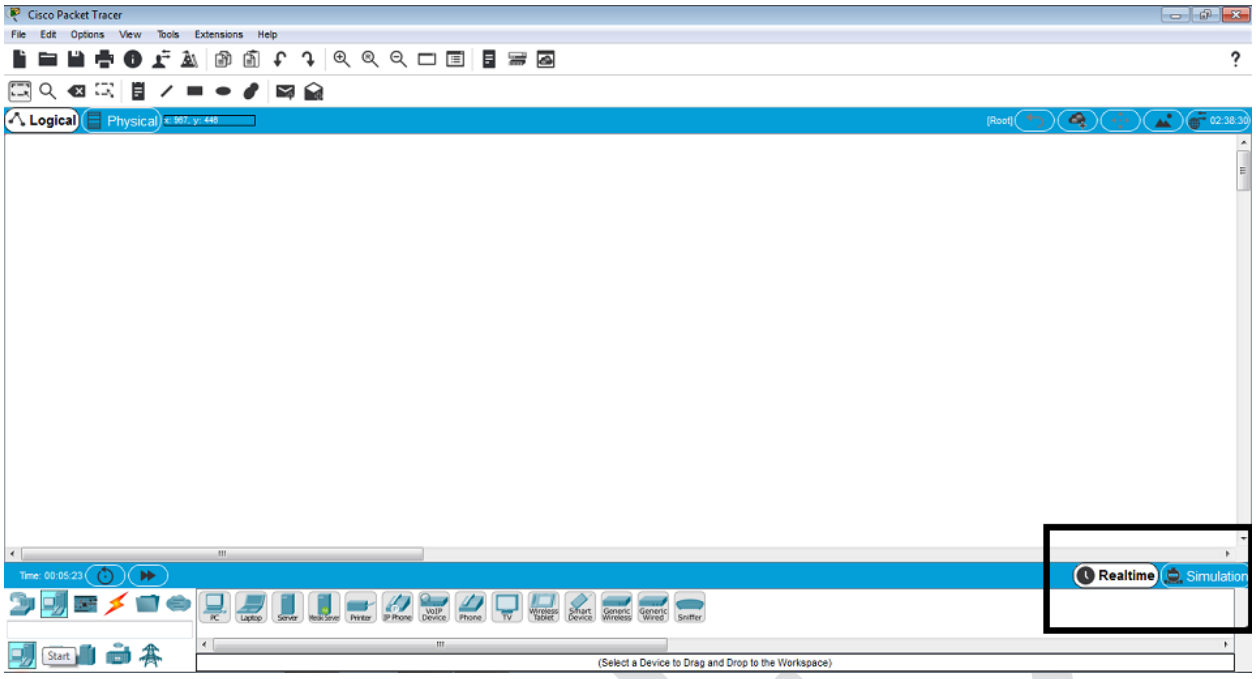


Fig5. Modes in Packet Tracer

A Basic network:

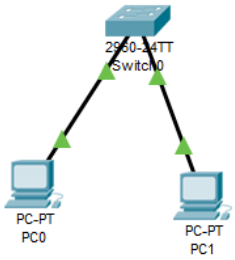


Fig6:Basic Network

Steps to connect the above network:

- Select and place the network devices in the home screen.(Select Switch from “Network Devices” and PCs from “End Devices”).
- Choose appropriate connection media to connect the network devices.(Copper Straigh-through cable is used)

- Connect the cable to the “FastEthernet” port of PC with the ‘FastEthernet’ port of the Switch for successful connection.

Conclusion: From the above experiment we have got familiarized with the Cisco Packet Tracer Software 7.2.2 and learnt how to make a basic network connection.

Experiment – 11

Experiment: Introduction to Cisco IOS

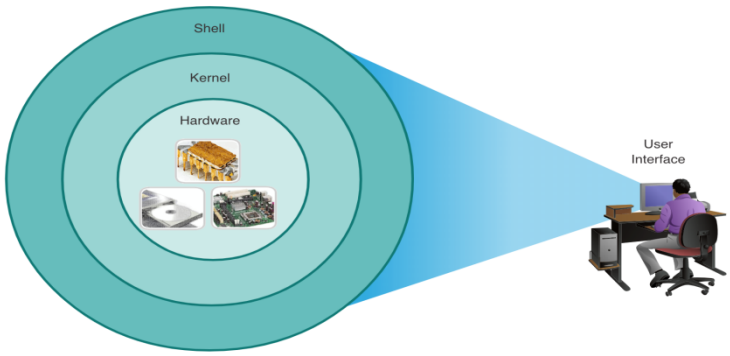
Aim: To get familiarized with Cisco IOS

Software Used: Cisco Packet Tracer

Theory:

Cisco Operating System:

- Shell - The user interface that allows users to request specific tasks from the computer. These requests can be made either through the CLI or GUI interfaces.
- Kernel - Communicates between the hardware and software of a computer and manages how hardware resources are used to meet software requirements.
- Hardware - The physical part of a computer including underlying electronics.



CLI-based network OS:

CLI-based network operating system enables a network technician to do the following:

- Use a keyboard to run CLI-based network programs
- Use a keyboard to enter text and text-based commands
- View output on a monitor

```
analyst@secOps ~]$ ls
Desktop  Downloads  lab.support.files  second_drive
[analyst@secOps ~]$
```

Access Methods:

- **Console** – A physical management port used to access a device in order to provide maintenance, such as performing the initial configurations.
- **Secure Shell (SSH)** – Establishes a secure remote CLI connection to a device, through a virtual interface, over a network. (Note: This is the recommended method for remotely connecting to a device.)
- **Telnet** – Establishes an insecure remote CLI connection to a device over the network. (Note: User authentication, passwords and commands are sent over the network in plaintext.)

IOS Navigation:

Primary Command Modes:

User EXEC Mode:

- Allows access to only a limited number of basic monitoring commands
- Identified by the CLI prompt that ends with the > symbol

```
Switch>
```

```
Router>
```

Privileged EXEC Mode:

- Allows access to all commands and features
- Identified by the CLI prompt that ends with the # symbol

```
Router#
```

```
Switch#
```

Global Configuration Mode:

- Used to access configuration options on the device

```
Switch(config)#
```

Line Configuration Mode:

- Used to configure console, SSH, Telnet or AUX access

```
Switch(config-line)#
```

Interface Configuration Mode:

- Used to configure a switch port or router interface

```
Switch(config-if)#
```

Navigation Between IOS Modes:

- Privileged EXEC Mode:
  - To move from user EXEC mode to privilege EXEC mode, use the enabled command.

```
Switch> enable
Switch#
```

- Global Configuration Mode:
  - To move in and out of global configuration mode, use the configure terminal command. To return to privilege EXEC mode, use the exit command.
  -

```
Switch(config)#
Switch(config)#exit
Switch#
```

- Line Configuration Mode:
  - To move in and out of line configuration mode, use the line command followed by the management line type. To return to global configuration mode, use the exit command.

```
Switch(config)#line console 0
Switch(config-line)#exit
Switch(config)#
```

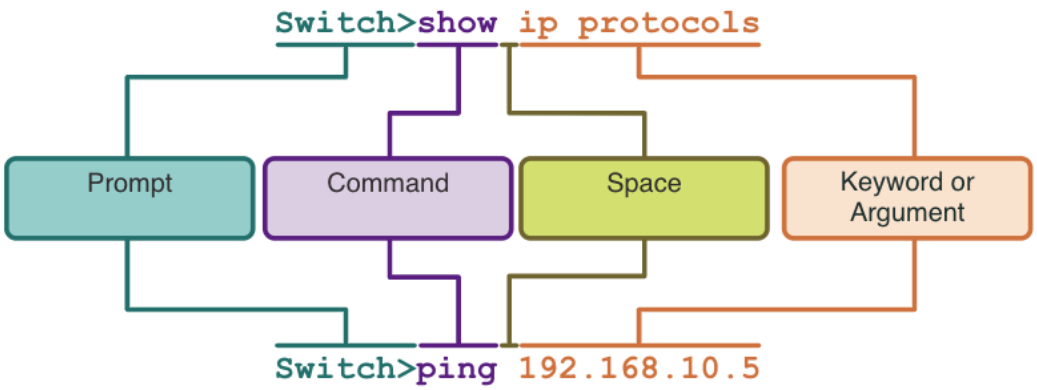
- Subconfiguration Modes:
  - To move out of any subconfiguration mode to get back to global configuration mode, use the **exit** command. To return to privilege EXEC mode, use the **end** command or key combination **Ctrl +Z**.

```
Switch(config)#line console 0
Switch(config-line)#end
Switch#
```

  - To move directly from one subconfiguration mode to another, type in the desired subconfiguration mode command. In the example, the command prompt changes from **(config-line)#** to **(config-if)#**.

```
Switch(config-line)#interface FastEthernet 0/1
Switch(config-if)#
```

The Command Structure:



- Keyword – This is a specific parameter defined in the operating system (in the figure, ip protocols).
- Argument - This is not predefined; it is a value or variable defined by the user (in the figure, 192.168.10.5).

Hot Keys and Shortcuts:

Keystroke	Description
Tab	Completes a partial command name entry.
Backspace	Erases the character to the left of the cursor.
Left Arrow or **Ctrl+B**	Moves the cursor one character to the left.
Right Arrow or **Ctrl+F**	Moves the cursor one character to the right.

Up Arrow or **Ctrl+P**	Recalls the commands in the history buffer, beginning with the most recent commands.

Keystroke	Description
Enter Key	Displays the next line.
Space Bar	Displays the next screen.
Any other key	Ends the display string, returning to privileged EXEC mode.
Keystroke	Description
Ctrl-C	When in any configuration mode, ends the configuration mode and returns to privileged EXEC mode.
Ctrl-Z	When in any configuration mode, ends the configuration mode and returns to privileged EXEC mode.
Ctrl-Shift-6	All-purpose break sequence used to abort DNS lookups, traceroutes, pings, etc.

Conclusion: From the above experiment we have got familiarized with the Cisco IOS and learnt how to make a basic network connection.

Experiment-12

Experiment: Basic Device Configuration in Cisco Packet Tracer

Aim: To configure a basic device (Switch) in Cisco IOS using Cisco Packet Tracer

Software Used: Cisco Packet Tracer

Procedure:

Configure Device Names:

- The first configuration command on any device should be to give it a unique hostname.
- By default, all devices are assigned a factory default name. For example, a Cisco IOS switch is "Switch."

```
Switch# configure terminal
Switch(config)# hostname Sw-Floor-1
Sw-Floor-1(config)#
```

(Note: To return the switch to the default prompt, use the no hostname global config command.)

Configure Passwords:

Securing user EXEC mode access:

- First enter line console configuration mode using the line console 0 command in global configuration mode.
- Next, specify the user EXEC mode password using the password *password* command.
- Finally, enable user EXEC access using the login command.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# line console 0
Sw-Floor-1(config-line)# password cisco
Sw-Floor-1(config-line)# login
Sw-Floor-1(config-line)# end
Sw-Floor-1#
```

Securing privileged EXEC mode access:

- First enter global configuration mode.
- Next, use the enable secret password command.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# enable secret class
Sw-Floor-1(config)# exit
Sw-Floor-1#
```

Save Configurations:

There are two system files that store the device configuration:

- **startup-config -** This is the saved configuration file that is stored in NVRAM. It contains all the commands that will be used by the device upon startup or reboot. Flash does not lose its contents when the device is powered off.

- **running-config -** This is stored in Random Access Memory (RAM). It reflects the current configuration. Modifying a running configuration affects the operation of a Cisco device immediately. RAM is volatile memory. It loses all of its content when the device is powered off or restarted.
- To save changes made to the running configuration to the startup configuration file, use the copy running-config startup-config privileged EXEC mode command.

```
Router#show startup-config
Using 624 bytes
!
version 15.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
```

```
Router#show running-config
Building configuration...

Current configuration : 624 bytes
!
version 15.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
```

Conclusion: From the above experiment we have learnt how to configure name, password of a basic network device and also how to save the configurations.

Experiment - 13

Experiment: Configure IP Addressing of a basic network device in Cisco IOS

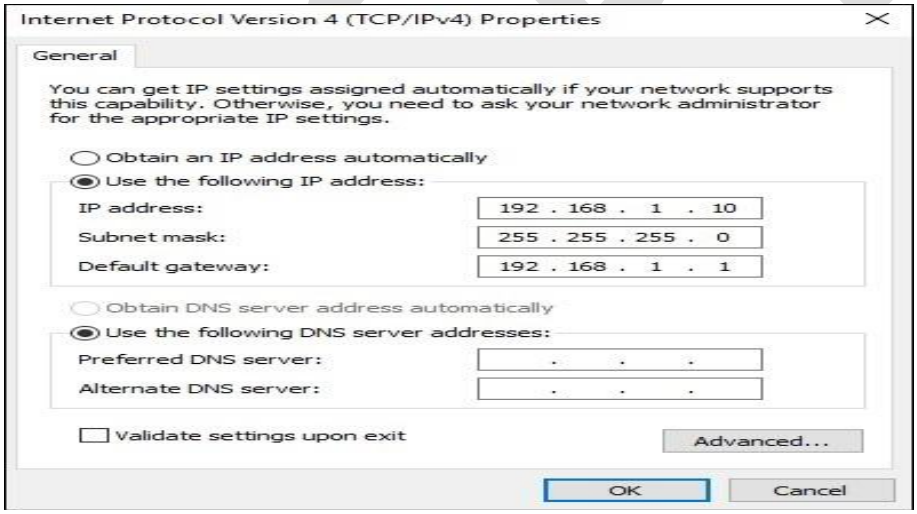
Aim: To configure IP Address of a basic network device in Cisco IOS

Software Used: Cisco Packet Tracer

Procedure:

Manual IP Address Configuration for End Devices:

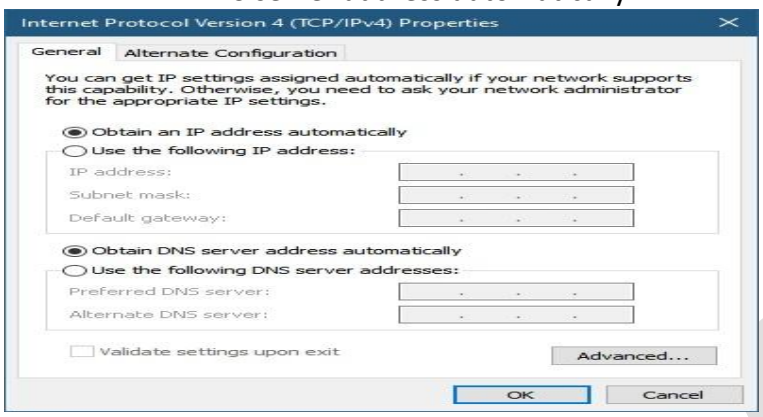
- End devices on the network need an IP address in order to communicate with other devices on the network.
- IPv4 address information can be entered into end devices manually, or automatically using Dynamic Host Configuration Protocol (DHCP).
    - To manually configure an IPv4 address on a Windows PC, open the **Control Panel > Network Sharing Center > Change adapter settings** and choose the adapter. Next right-click and select **Properties** to display the Local Area Connection Properties.
    - Next, click Properties to open **the Internet Protocol Version 4 (TCP/IPv4) Properties** window. Then configure the IPv4 address and subnet mask information, and default gateway.



Automatic IP Address Configuration for End Devices:

- DHCP enables automatic IPv4 address configuration for every end device that is DHCP-enabled.
- End devices are typically by default using DHCP for automatic IPv4 address configuration.
    - To configure DHCP on a Windows PC, open the Control Panel > Network Sharing Center > Change adapter settings and choose the adapter. Next right-click and select Properties to display the Local Area Connection Properties.

- Next, click Properties to open the Internet Protocol Version 4 (TCP/IPv4) Properties window, then select Obtain an IP address automatically and Obtain DNS server address automatically.



Switch Virtual Interface Configuration:

To access the switch remotely, an IP address and a subnet mask must be configured on the SVI. To configure an SVI on a switch:

- Enter the interface vlan 1 command in global configuration mode.
- Next assign an IPv4 address using the ip address *ip-address subnet-mask command.*
- Finally, enable the virtual interface using the no shutdown command.

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip address 192.168.1.20 255.255.255.0
Switch(config-if)# no shutdown
```

Conclusion: In this experiment we have learnt how to configure IP address Manually and Dynamically of a End Device using LAN properties and a of switch using SVI.

Experiment-14

Experiment: Basic Router Configuration

Aim: To perform the following router configurations:

1. Configure Initial Router Settings
2. Configure Interfaces
3. Configure the Default Gateway

Software Required: Cisco Packet Tracer

Procedure:

1. Configure Initial Router Settings:

- Configure the device name.
- Secure privileged EXEC mode.
- Secure user EXEC mode.
- Secure remote Telnet / SSH access.
- Encrypt all plaintext passwords.
- Provide legal notification and save the configuration.

```
Router(config)# hostname hostname
```

```
Router(config)# enable secret password
```

```
Router(config)# line console 0
Router(config-line)# password password
Router(config-line)# login
```

```
Router(config)# line vty 0 4
Router(config-line)# password password
Router(config-line)# login
Router(config-line)# transport input {ssh | telnet}
```

```
Router(config)# service password encryption
```

```
Router(config)# banner motd # message #
Router(config)# end
Router# copy running-config startup-config
```

- Commands for basic router configuration on R1.
- Configuration is saved to NVRAM.

```
R1(config)# hostname R1
R1(config)# enable secret class
R1(config)# line console 0
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# transport input ssh telnet
R1(config-line)# exit
R1(config)# service password encryption
R1(config)# banner motd #
Enter TEXT message. End with a new line and the #
**********************************************
WARNING: Unauthorized access is prohibited!
**********************************************
R1(config)# exit
R1# copy running-config startup-config
```

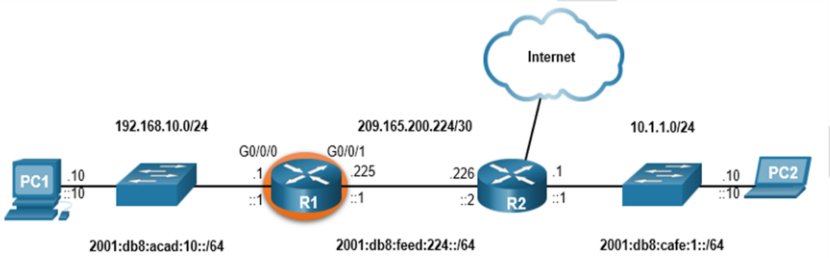
2. Configure Interfaces:

Configuring a router interface includes issuing the following commands:

1.Router(config)# interface *type-and-number*
2.Router(config-if)# description *description-text*
3.Router(config-if)# ip address *ipv4-address subnet-mask*
4.Router(config-if)# ipv6 address *ipv6-address/prefix-length*
5.Router(config-if)# no shutdown

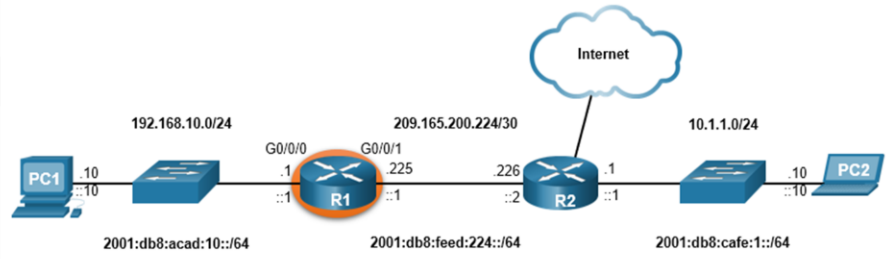
- It is a good practice to use the **description** command to add information about the network connected to the interface.
- The **no shutdown** command activates the interface.

The commands to configure interface G0/0/0 on R1 are shown here:




```
R1(config)# interface gigabitEthernet 0/0/0
R1(config-if)# description Link to LAN
R1(config-if)# ip address 192.168.10.1 255.255.255.0
R1(config-if)# ipv6 address 2001:db8:acad:10::1/64
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)#
*Aug  1 01:43:53.435: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/0, changed state to down
*Aug  1 01:43:56.447: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/0, changed state to up
*Aug  1 01:43:57.447: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0,
changed state to up
```

The commands to configure interface G0/0/1 on R1 are shown here:




```
R1(config)# interface gigabitEthernet 0/0/1
R1(config-if)# description Link to R2
R1(config-if)# ip address 209.165.200.225 255.255.255.252
R1(config-if)# ipv6 address 2001:db8:feed:224::1/64
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)#
*Aug  1 01:46:29.170: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/1, changed state to down
*Aug  1 01:46:32.171: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/1, changed state to up
*Aug  1 01:46:33.171: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1,
changed state to up
```

3. Configure the Default Gateway:

The default gateway address is typically configured on all devices that will communicate beyond their local network.

To configure an IPv4 default gateway on a switch, use the **ip default-gateway** *ip-address* global configuration command. The *ip-address* that is configured is the IPv4 address of the local router interface connected to the switch.

Conclusion: In the above experiment we have performed the basic configurations of the router.