

Expt.No: 01

Explore all ISP in your area/locality and select best internet ISP/plan based on cost and performance.

Types of ISPs

- Internet Service Providers (ISPs) have several types of connectivity options for the Internet. Each ISP is different in that the company provides a different type of connectivity protocol and speed. Most ISPs are cable or DSL, but other options are available for small, rural areas. It's important to analyze your individual needs before deciding on an ISP.

Dialup

- Although it's painfully slow, dialup access is still a necessity for small, rural areas. ISPs offer dialup access in these areas. A dialup ISP requires the user to have a modem for Internet access. The user dials a phone connection using a telephone number, connects to a remote server, and uses the telephone connection to browse websites.

DSL

- DSL is normally offered by the local phone company. DSL is a technology that uses the "extra" signals not used by telephone signals. These "extra" signals make DSL usage available even during times when the phone is ringing or people are using the telephone access. DSL uses a DSL router that connects using a telephone cable to a phone jack.

Cable

- Cable is offered by the local cable company in the user's neighborhood. Cable Internet access is available by connecting a cable router to the computer and connecting to a designated jack. Cable ISPs are usually faster, especially in areas where there is not much usage. Cable connections are shared by neighbors, which differs from DSL, so cable access speed is dependent on the amount of traffic from other neighborhood users.

Wi-Fi Access

- Wi-Fi is wireless Internet access. It's used by laptops and offered freely by many hotels and coffee shops. Wi-Fi can also be installed in the home for people who have desktops and laptops networked. Wi-Fi is not as quick as DSL or Cable, but it's a more convenient ISP service.

Computer Networks Lab Manual

There are a number of different internet providers in Athani that provide good internet services and the telecom service providers such as Airtel, Jio, BSNL etc also come under this. Since there are so many internet service providers available in Athani, it can be a difficult thing to choose the best one so, we are here to help you in this regard with this list of Best Internet Service Providers in Athani:

The following table is showing the comparison between the top 3 broadband plans.

Internet Speed	JioFiber (Price)	Airtel Fiber (Price)	BSNL Broadband (Price)
30 Mbps	399	Not providing	449
40 Mbps	Not providing	499	Not providing
100 Mbps	699	799	799
150 Mbps	999	Not providing	Not providing
200 Mbps	Not providing	999	999
300 Mbps	1499	1499	1499
1 Gbps	3999	3999	Not providing

Reliance Jio vs Airtel vs Vodafone Idea

Reviews.TrekBook.in

NEW PLAN COMPARISON		PLAN MRP		
Period	Data	JIO	AIRTEL	VODAFONE IDEA
1 Month (28 days)	1.5 GB / Day	199	248	249
	2 GB / Day	249	298	299
	3 GB / Day	349	398	399
2 Month (56 Days)	1.5 GB / Day	399	-	-
	2 GB / Day	444	-	-
3 Month (84 Days)	1.5 GB / Day	555	598	599
	2 GB / Day	599	698	699
	2 GB	129	148	149
Affordable plans	6 GB	329	-	379 (3 months)
	24 GB	1299	1498	1499
12 Months (365 Days)	1.5 GB / Day	2199	2398	1499 (24 GB)

New Recharge Plans Comparison Table

Conclusion: According to above table comparison and research, we conclude that JIO is providing good performance and fastest internet facility for reasonable cost.

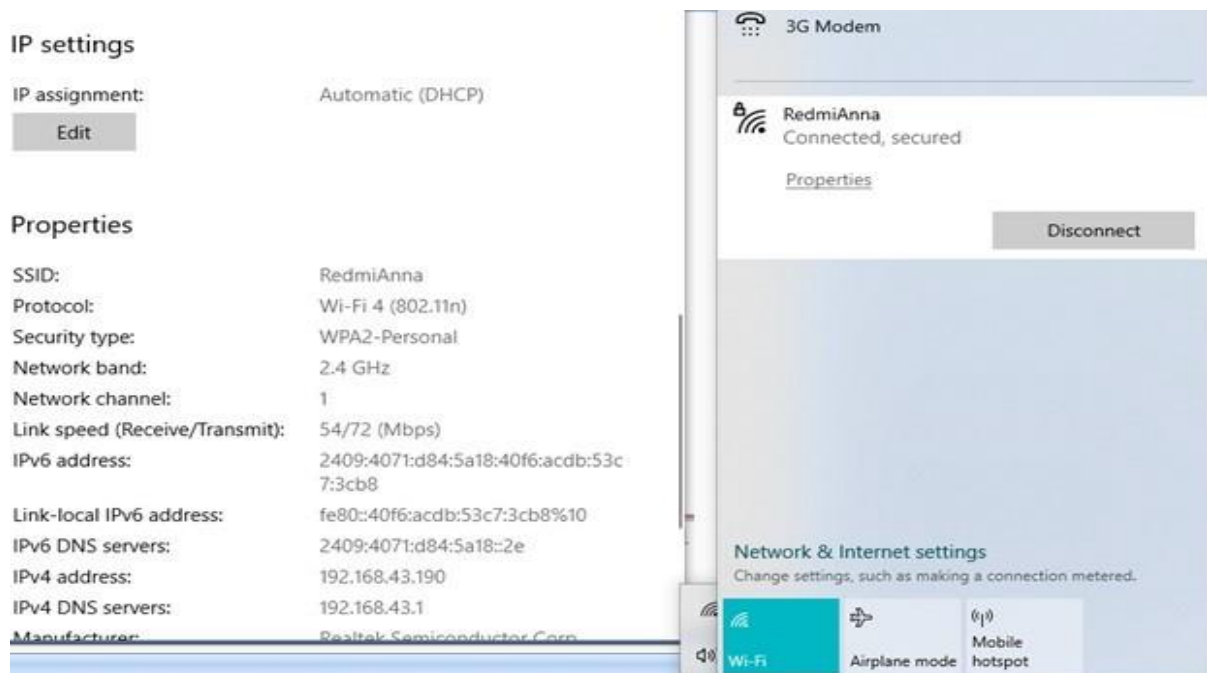
Expt.No: 02

Test the download/upload speed in your computer/mobile phone also check type, bandwidth and ISP.



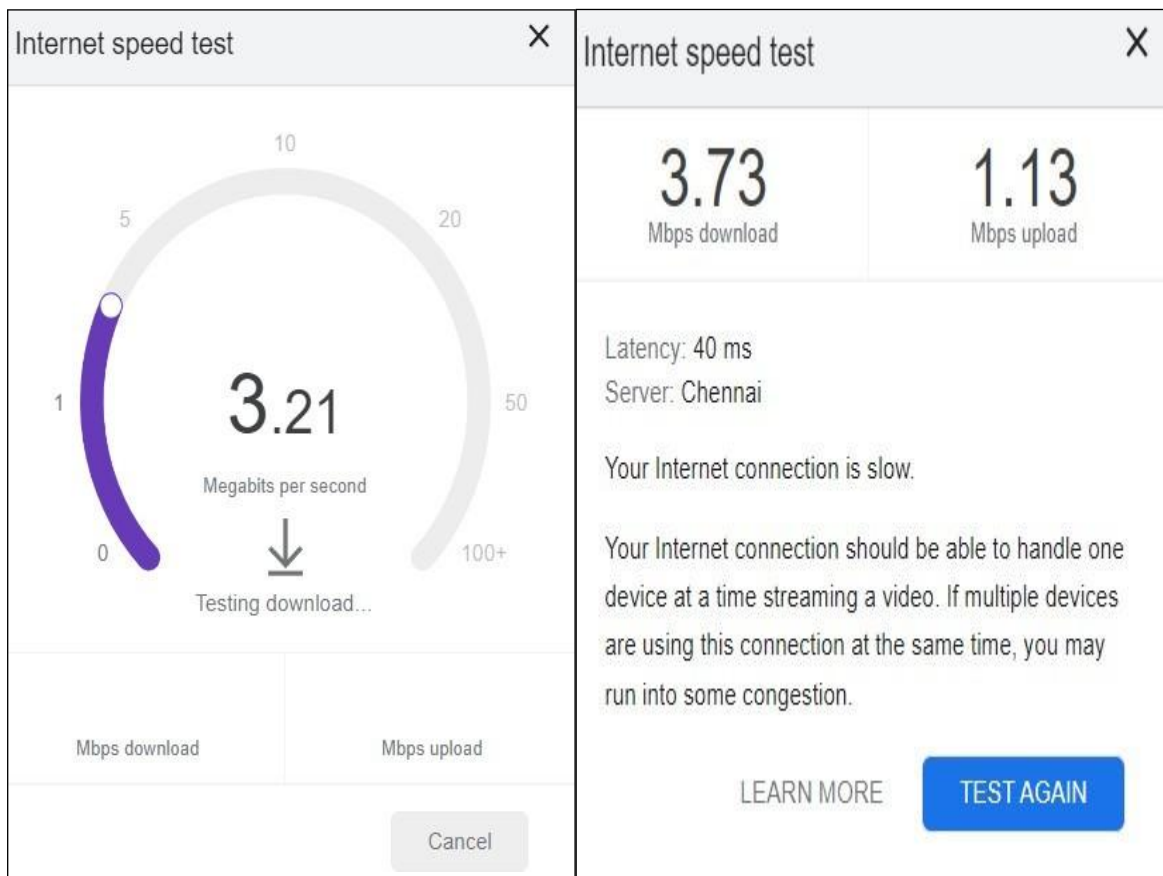
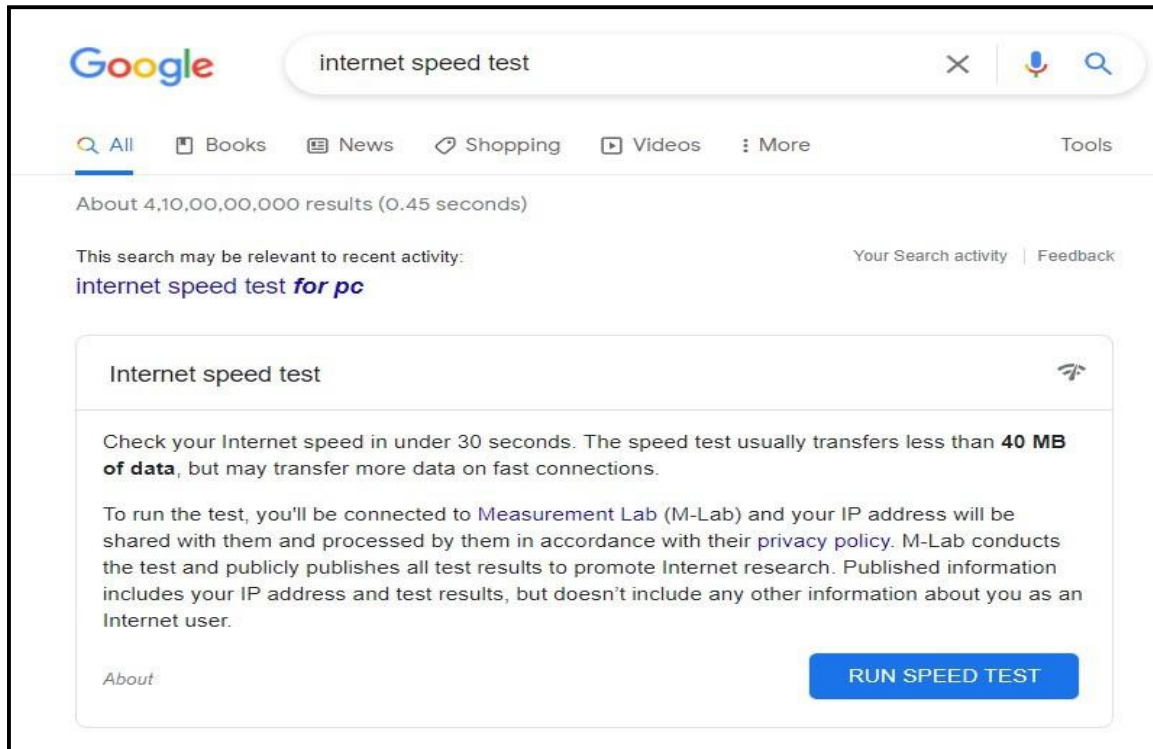
CHECKING INTERNET SPEED ON WINDOWS

- To check the internet speed on your Windows PC, connect your router to PC via the ethernet cable, or you can just check Wi-Fi network also
- Click on connected Wi-fi icon at the bottom right corner of the PC.
- Click on properties and scroll down to see receive/transmit speed:



Computer Networks Lab Manual

OR Search on Google as internet speed test and click on **RUN SPEED TEST** to get download speed and upload speed.



Expt.No: 03

Explore Bluetooth, Wifi, and NFC in your Smartphone and note their key technical attributes (Radio spectrum band, range, path loss, throughput, mode etc)

- Wireless communication is preferred a lot and has replaced wired connections over the years as it is possible to share data even in long range, a faster rate and in a secure way. Wireless communication is possible via technologies such as Bluetooth, NFC and Wi-Fi of which the last one is yet to become mainstream. The technology is chosen based on the purpose. The range plays an important role in choosing a specific wireless technology.
- It is common for users to make use of Bluetooth and Wi-Fi to communication with others and share data between devices. NFC is also used to some extent. Here, you will get to know more details about the different wireless technologies and their major differences.

1) Bluetooth

- Bluetooth is basically used when it is necessary to communicate within a short range.
- It was intended to replace the wired connection. It makes use of short range radio links and operates on FHSS (Frequency Hopping Spread Spectrum) to avoid inference. Bluetooth signals operate at 2.4GHz.
- Bluetooth LE is a recent technology that is aimed at enabling power sensitive devices to connect permanently to the internet.

❖ Technical attributes

- **Radio Spectrum band:** There are several uses of the 2.4 GHz band. Interference may occur between devices operating at 2.4GHz This article details the different users of the 2.4 GHz band, how they cause interference to other users and how they are prone to interference from other users.
- **Range:** Typically less than 10 m (33 ft), up to 100 m (330 ft). Bluetooth 5.0: 40–400 m (100–1,000 ft)
- **Throughput:** 192.0 kbps
- **Mode:** Android.

2) Wifi(Wireless Fidelity)

- Wi-Fi networks are used commonly and these connect every possible device together. Wi-Fi has been developed to facilitate wireless local area networking in the 2.4GHz or 5.2GHZ bands.

- There are issues related to security threat in Wi-Fi, but the same can be prevented using the several security measures that are available. The common security methods include WEP, WPA and WPA2.
- One similarity between Bluetooth and Wi-Fi technologies is that both share a section of the 2.4GHz spectrum. This will pave way for some level of interference.

❖ Technical attributes

- **Radio Spectrum band:** All Spectrum routers support 2.4 and 5 GHz frequencies. If the router has a single WiFi network name, the advanced router will select the correct connection for your device.
- **Range:** A general rule of thumb in home networking says that Wi-Fi routers operating on the 2.4 GHz band can reach up to 150 feet indoors and 300 feet outdoors.
- **Throughput:** 600 mbps
- **Mode:** Router.

1) NFC(Near Field Communication)

- NFC is a standard in many smart phones and other devices. It aims at establishing radio communication between devices by bringing them close to each other or by just touching them. NFC facilitates in contactless transactions and data exchange.

❖ Technical attributes


- **Radio Spectrum band:** NFC operates at **13.56 MHz** on ISO/IEC 18000-3 air interface and at rates ranging from 106 kbit/s to 424 kbit/s. NFC always involves an initiator and a target; the initiator actively generates an RF field that can power a passive target.
- **Range:** NFC operates in a frequency range centered on 13.56 MHz and offers a data transmission rate of up to 424 kbit/s within a distance of approximately 10 centimeters.
- **Throughput:** 106 kbit/s to 424 kbit/s.
- **Mode:** Reader/writer, peer-to-peer, card emulation and wireless charging.

Expt.No: 04 Manual and Automatic address assignment (Windows)

- a) IPv4 address
- b) Subnet mask
- c) DNS

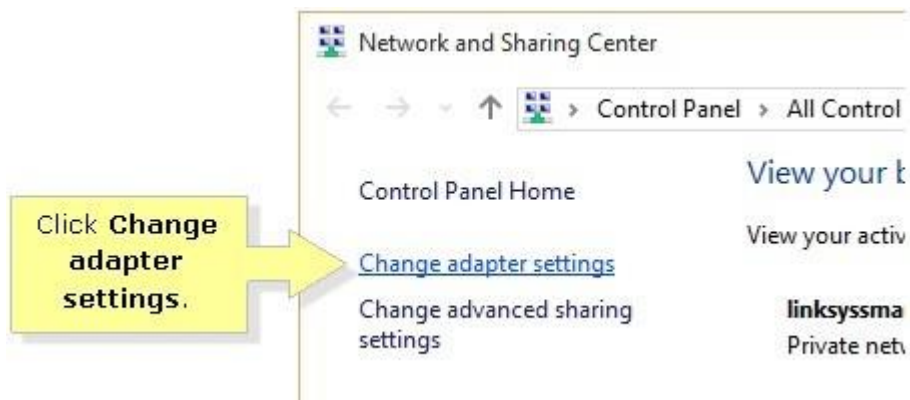
Automatic address assignment:

- Automatically obtaining an IP Address from a **DHCP (Dynamic Host Configuration Protocol)** server such as a router is an easy way to connect computer to the network.
- Instead of manually entering the IP Address, Subnet mask, and Default gateway, these can be automatically assigned by the DHCP server.
- To do this, you need to set the network adapter on your computer to obtain an IP Address automatically.

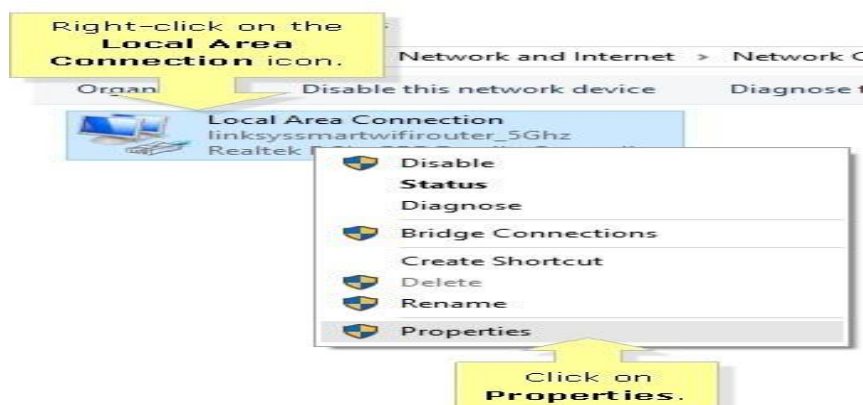
Step1: Right-click the **Network**  icon located on the Desktop screen then click **Open Network and Sharing Center**.



Step 2: Click **Change adapter settings**.

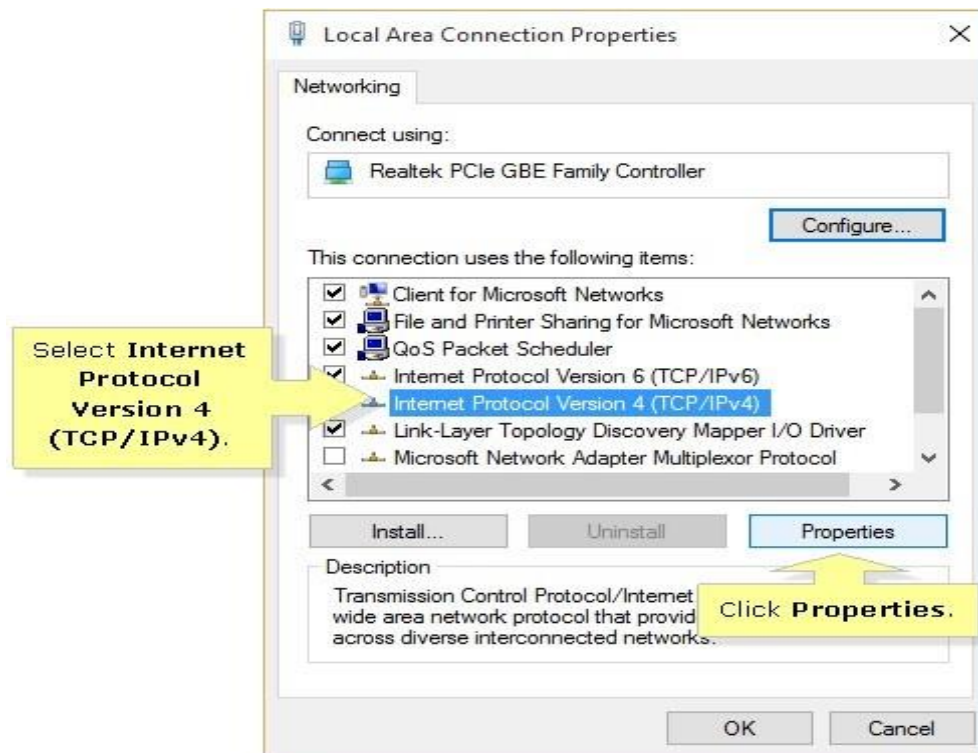


Step 3: Right-click on the **Local Area Connection** icon and click **Properties**.

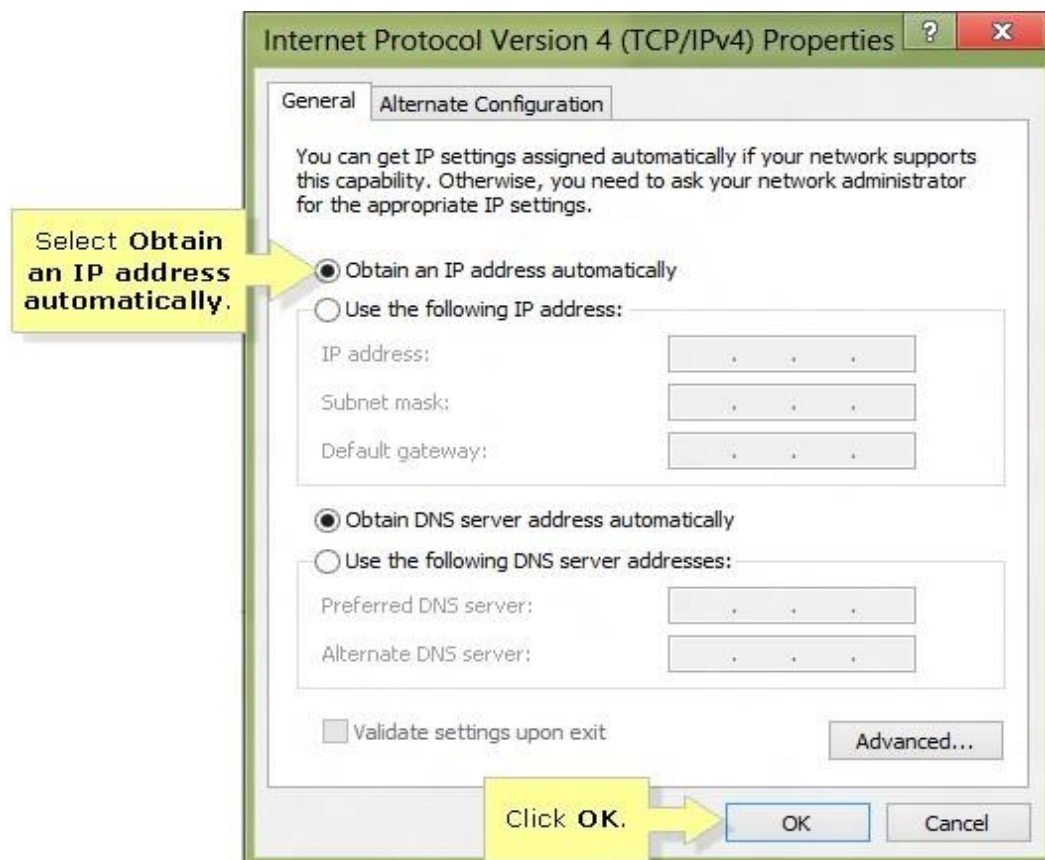


Computer Networks Lab Manual

Step 4: On the **Local Area Connection Properties** window, select **Internet Protocol Version 4 (TCP / IPv4)** then click **Properties**.



Step 5: Select a radio button beside **Obtain an IP address automatically** then click **OK**.



Manual address assignment:

- Repeat the steps 1 to 4 of Automatic address assignment.
- Select the “Use the following IP address” option, and then type in the IP address, subnet mask, and default gateway that corresponds with your network setup.
- Next, type in your preferred and alternate DNS server addresses. Finally, select the “Validate settings upon exit” option so that Windows immediately checks your new IP address and corresponding information to ensure that it works. When you’re ready, click the “OK” button.

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 . 1 . 2

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

Preferred DNS server: 8 . 8 . 8 . 8

Alternate DNS server: 8 . 8 . 4 . 4

☒ Validate settings upon exit

Advanced...

OK Cancel

Expt.No: 05 Manual and Automatic address assignment (Android)

- a) IPv4 address
- b) Subnet mask
- c) DNS

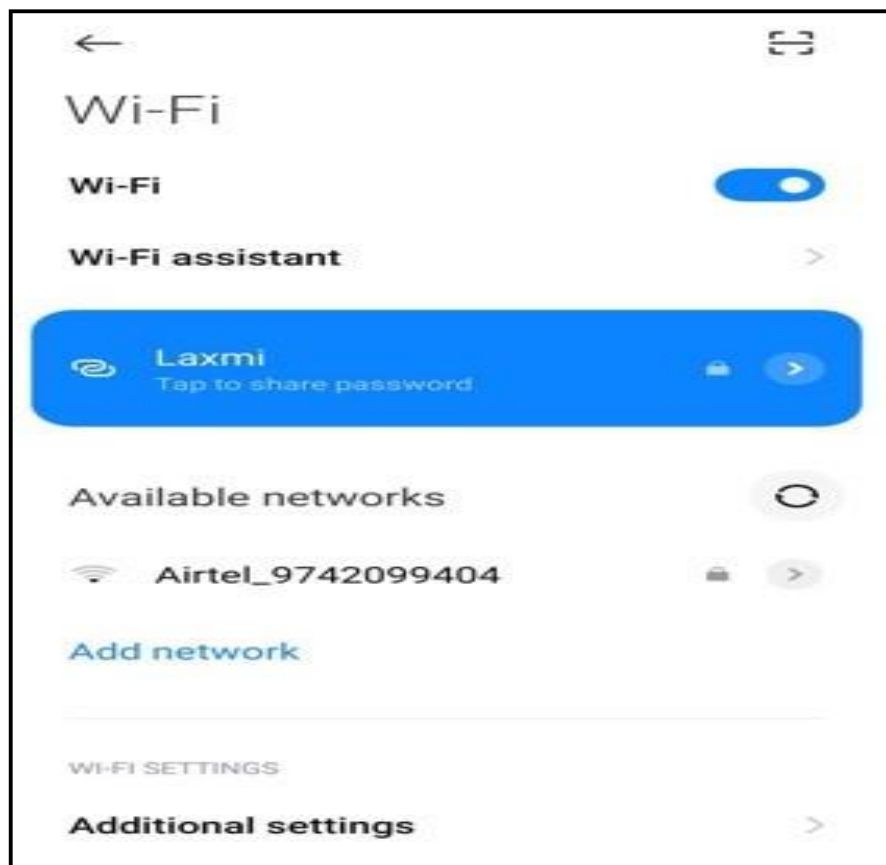
Automatic address assignment:









- Automatically obtaining an IP Address from a **DHCP (Dynamic Host Configuration Protocol)** server such as a router is an easy way to connect mobile to the network.
- Instead of manually entering the IP Address, Default gateway, DNS 1 and DNS 2 these can be automatically assigned by the DHCP server.

Manual address assignment:

How do I setup a static IP Address on my Android device?

- The steps will vary with different versions of Android. This documentation is based on Android version 11.
1. Go to **Settings**.
 2. Select **Network & Internet**, then **Wi-Fi**.
 3. Tap on the network you are currently connected to open the settings menu



 Status Connected	 Technology Wi-Fi 5
 Link speed 96Mbps	 Signal strength Excellent
 Security WPA/WPA2-Personal	 IP address ::4079:da9e:b11f:278e 19
 Subnet mask 255.255.255.0	 Gateway 192.168.43.1
<hr/>	
Proxy	None ↕
IP settings	DHCP ↕
Privacy	Use device MAC ↕
Modify network	

4. Click on DHCP to change to static and set IP address as follows. Then save.

Proxy	None ↕
IP settings	Static ↕
IP address	192.168.43.100
Gateway	192.168.43.1
Prefix length	24
DNS 1	192.168.43.1
DNS 2	8.8.4.4
Privacy	Use device MAC ↕
Modify network	
Forget network	

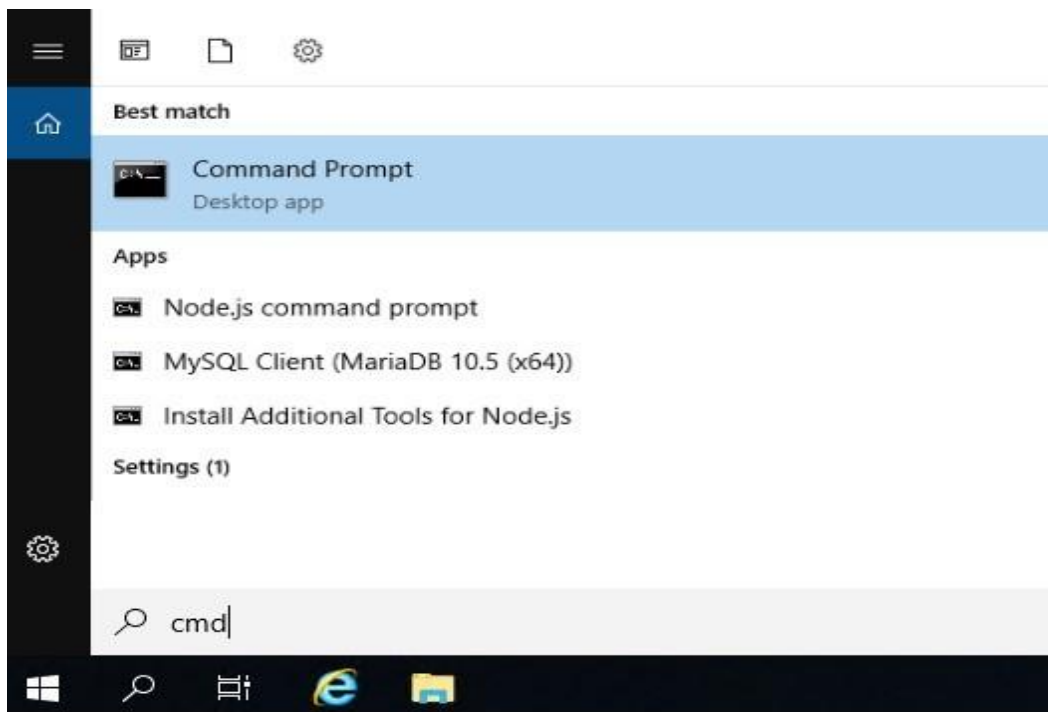
Expt.No: 06 Determine the IP Address Configuration of a Computer (Windows) and Test the Network Interface TCP/IP Stack (Ping).

- Internet protocol **configuration (ipconfig)** is one of the most valuable tools used to check and troubleshoot basic TCP/IP settings and this command displays all the IP configuration details of the windows machine.
- The TCP/IP stands for **Transmission Control Protocol/Internet Protocol** and it is a set of networking protocols that allows communicating multiple computers.
- ipconfig is one of the most valuable tool available to check and troubleshoot basic TCP/IP settings.
- **Ipconfig syntax**

```
ipconfig [/parameter]
```

Steps to determine IP address configuration on any computer:

Step 1: Click on the Windows key to open start and search **cmd** and then click on the Command Prompt which is shown in the below image.



Step 2: Type ipconfig command and press enter to get details of IP, subnet mask and default gateway addresses.

```

C:\Users\User>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 1:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 4:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix  . :
    IPv6 Address. . . . . : 2405:204:51a9:dac5:40f6:acdb:53c7:3cb8
    Temporary IPv6 Address. . . . . : 2405:204:51a9:dac5:ccd7:937:ac9b:b993
    Link-local IPv6 Address . . . . . : fe80::40f6:acdb:53c7:3cb8%10
    IPv4 Address. . . . . : 192.168.43.190
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::2c1f:f3ff:fe99:2564%10
                                192.168.43.1

Ethernet adapter Bluetooth Network Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

```

Testing a TCP/IP protocol stack: Using ping

- The **ping** utility provided with many TCP/IP packages is useful for testing the IP network layer.
- **Ping** takes as an argument an IP address and attempts to send a single packet to the named IP protocol stack.
- First, determine if your own protocol stack is operating correctly by “pinging” your own computer. For example, if your IP address is 192.168.43.190, enter **ping 192.168.43.190** at command prompt and wait to see if the packets are routed at all. If they are, the output will appear similar to the following:

```

C:\Users\User>ping 192.168.43.190

Pinging 192.168.43.190 with 32 bytes of data:
Reply from 192.168.43.190: bytes=32 time<1ms TTL=128
Reply from 192.168.43.190: bytes=32 time<1ms TTL=128
Reply from 192.168.43.190: bytes=32 time<1ms TTL=128
Reply from 192.168.43.190: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.43.190:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

```

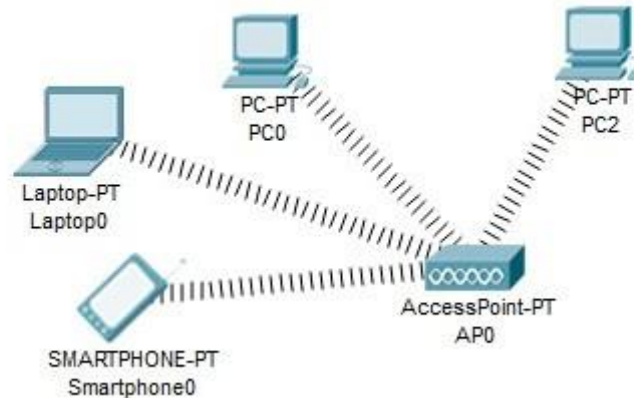
- If the ping works, then the computer is able to route packets to itself. This is reasonable assurance that the IP layer is set up correctly.

Expt.No: 7 Demonstrate working of common network devices.

Access Points:

- While a wired or wireless link is technological in an AP, it usually means a wireless device as shown below.

Access point creating a pure wireless network

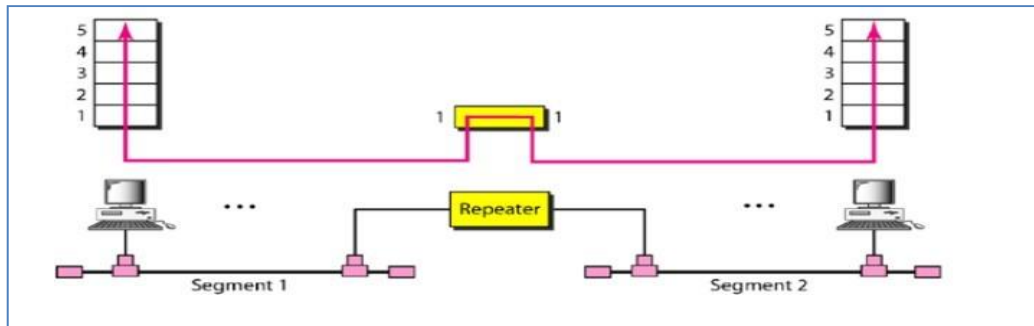


- Access point connects multiple wireless devices together in a single wireless network.
- Access point supports both type of standards; Ethernet and Wi-Fi.
- Access point uses radio signals to provide the connectivity.
- Based on functionality an access point can be categorized in three types; standalone, multifunction and client.
- A standalone access point works in the wireless network exactly as the switch works in the wired network.
- To control the unauthorized access, Access point uses authorization.
- To extend the coverage area, multiple access points are used together under a Wireless LAN Controller.
- An access point which works under the WLC is known as the LWAP (Lightweight Access Point).
- In WLC-LWAPs setup, the WLC controls and manages all LWAPs.
- A LWAP works as the bridge between the WLC and the end device.

Repeaters:

- Repeaters are devices that operate only in the physical layer. Repeaters are used to increase the usable length of the cable.
- Repeaters amplify a weak signal so that the signal stays as strong as the original one.
- Repeaters can also be used to connect two segments of the same network. **Segments refer to logical sections of the same network.**
- Repeaters do not have any capability of directing network traffic or deciding what particular route that certain data should take, **they are simply devices that sit on the network and boost the data signal that they receive.**
- The problem with repeaters is that they amplify the entire signal that they receive, including any line noise.

- Repeaters require a small amount of time to regenerate the signal. This can cause a propagation delay, which can affect network communication when there are several repeaters in a row.
- Repeaters were most commonly associated with coaxial network configurations. Because coaxial networks have now fallen out of favour, and because the functionality of repeaters has been built in to other devices, such as hubs and switches, repeaters are rarely used.
- The role of repeater is shown in the following figure.



Hubs:

- A hub is a centralized device that connects multiple devices in a single LAN network. When a hub receives a data signal from a connected device on one of its ports, except for that port, it forwards those signals from the remaining ports to all other connected devices.
- Typically, a hub has one or more uplink ports that are used to connect it to another hub. Hubs are no longer used in computer networks.
- There are two types of the Hub.
 - **Passive Hub:** - A passive hub forwards data signals as it receives them. It does not change data signals in any manner.
 - **Active Hub:** - An active hub also forwards data signals. But, before forwarding them, it amplifies them. Due to this added feature, an active Hub is also called a repeater.
- The following image shows an active hub and a passive hub.

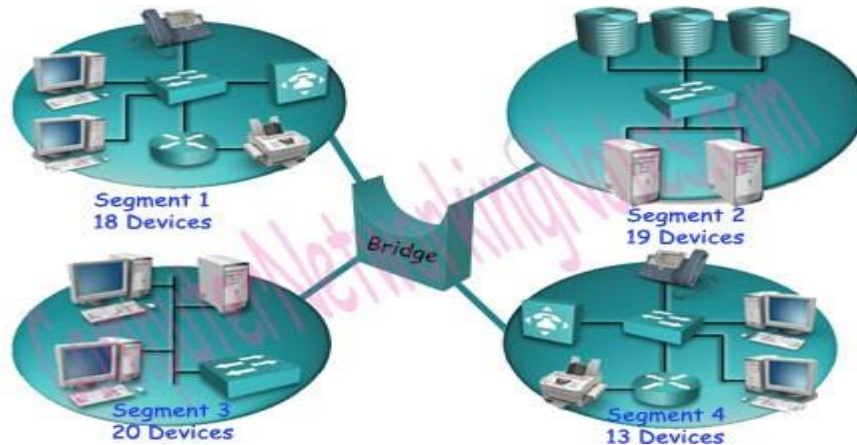


Bridges:

A bridge is used to divide a large network into smaller segments. The basic functions of a bridge are the following: -

- Breaking a large network into smaller segments.
- Connecting different media types such as UTP and fibre optic.
- Connecting different network architectures such as Ethernet and the Token ring.

The following image shows an example of a bridge.



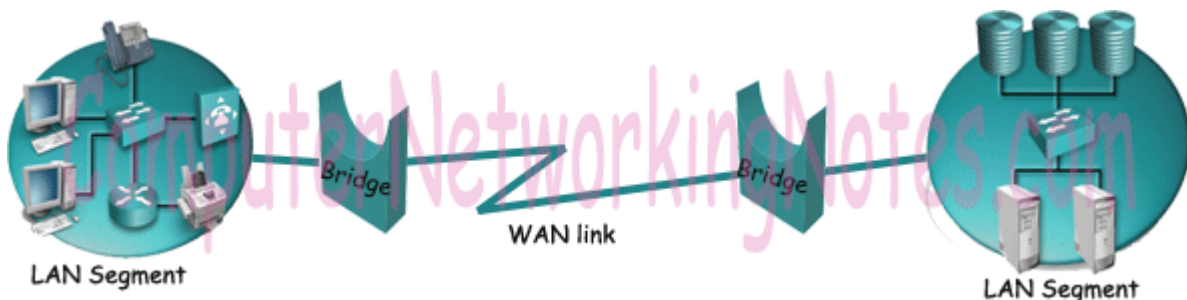
- A bridge can connect two different types of media or network architecture, but it cannot connect two different types of network layer protocols such as TCP/IP or IPX. It requires the same network-layer protocols across all segments.

There are three types of bridge:-

Local Bridge: - The Bridge directly connects two LAN segments. In Ethernet implementations, this is known as a transparent bridge. In the Token Ring network, this is called a source-routed bridge.



Remote Bridge: - This Bridge connects with another Bridge over the WAN link.



Wireless Bridge: - This Bridge connects with another Bridge without using wires. It uses radio signals for connectivity.



- In networking models such as the OSI layers model and TCP/IP model, the functionalities of Bridges are defined in the physical layer and data link layer.
- Just like a Hub, a Bridge is also no longer used in the computer network. Bridges have been replaced by switches.

Switches:

- Like hubs, switches also connect computers in a network or different segments of the same network.
- Switches work at the data link layer of the OSI reference model. Therefore, switches treat data in the form of frames and not as signals,
- The following figure shows an example of a 32-port Ethernet switch.



Figure 4.19 A 32-port Ethernet Switch

- Just as in hub, devices in switches are connected to ports through twisted pair cabling.
- Hub works by sending the data to all the ports on the device whereas a switch transfers it only to that port which is connected to the destination device as shown in figure below.
- A switch does so by having an in-built learning of the MAC address of the devices connected to it. A *MAC address* is a unique number that is stamped into every NIC.
- By forwarding data only to the system to which the data is addressed, the switch decreases the amount of traffic on each network link dramatically.
- In effect, the switch literally channels (or *switches*, if you prefer) data between the ports. For this purpose, switches maintain a list of MAC addresses and the port number associated with each MAC address.

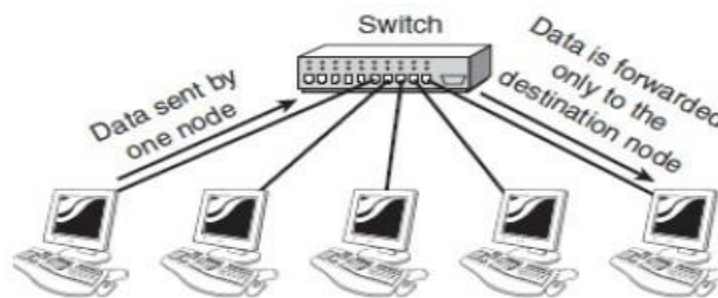


Figure 4.20 How a switch works

Routers:

- Routers allow packets to be transmitted to their destinations by monitoring the sea of networking devices interconnected with different network topologies.
- Routers are smart devices and store data on the networks to which they are connected.
- Most routers can be adjusted as a firewall for packet filters and can use ACLs.
- Routers are also used to convert from LAN to WAN framing in conjunction with the network control unit/data service unit (CSU / DSU). Such routers are called **boundary routers**.
- They serve as a LAN external link to a WAN and run on your network boundaries. Routers interact through the management of destination tables and local connections.
- A router gives data on the linked systems and sends requests if the destination is unknown. Routers are your first protection line, and only the traffic approved by network administrators needs to be enabled to pass.



Network Interface Cards (NICs):

- Network Interface Cards, commonly referred to as NICs, are used to connect a PC to a network. The NIC provides a physical connection between the networking cable and the computer's internal bus.
- Many NIC adapters comply with plug-and-play specifications. On these systems, NICs are automatically configured without user intervention, while on non-plug-and-play systems, configuration is done manually through a set-up program.
- NICs work at both the data link layer and physical layers of the OSI reference model. At the data link layer, NIC converts the data packets into data frames and adds the MAC address to the data frame.

Computer Networks Lab Manual

- At the physical layer, it is responsible for converting the data into signals, and transmitting them across the communication medium. A MAC address is a unique hardware number present on the NIC and is specified by the NIC manufacturer. MAC addresses are globally unique.
- When a computer needs to send data, the NIC receives data packets from the computer, converts them into data frames, and passes them across the cable as signals.
- The role of NIC in most PC environments can be divided into the following tasks:
 - i) Host-to-card communication
 - ii) Buffering
 - iii) Frame Creation
 - iv) Parallel-to-Serial conversion
 - v) Encoding

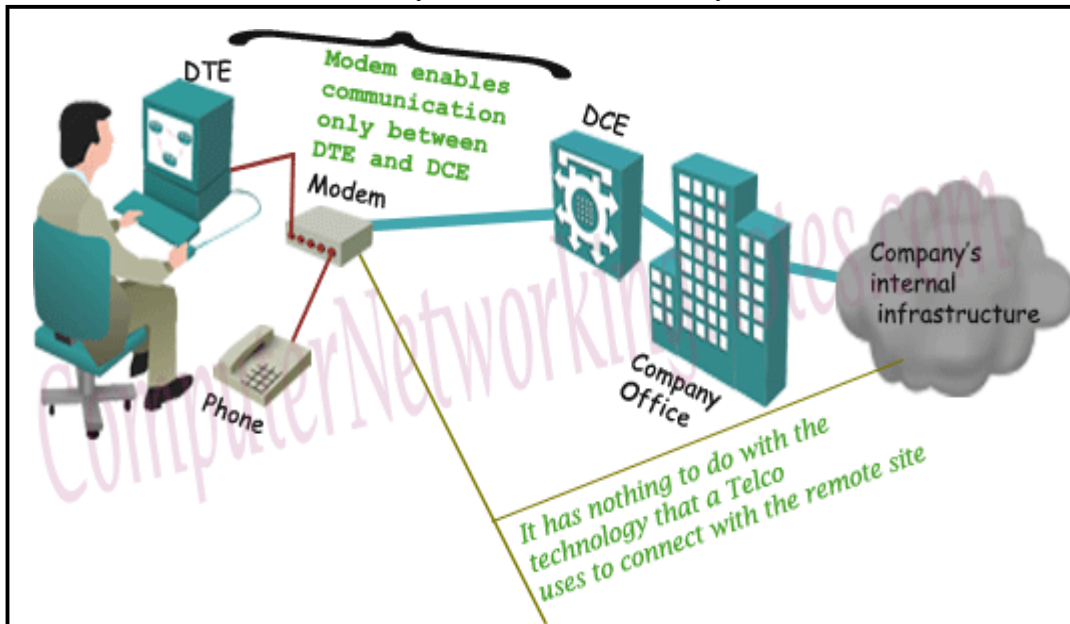


Modems:

- Modems (modulators-demodulators) are used to transmit digital signals over analog telephone lines. Thus, digital signals are converted by the modem into analog signals of different frequencies and transmitted to a modem at the receiving location.
- The receiving modem performs the reverse transformation and provides a digital output to a device connected to a modem, usually a computer.

Computer Networks Lab Manual

- The digital data is usually transferred to or from the modem over a serial line through an industry standard interface, RS-232.
- Many telephone companies offer DSL services, and many cable operators use modems as end terminals for identification and recognition of home and personal users.
- Modems work on both the Physical and Data Link layers.



Expt.No:8 Demonstrate different network cables and connectors.

LAN Cables – Co-axial, twisted pair, optical fibre:

Coaxial Cable

- A coaxial cable consists of two concentric conductors separated by insulation.
- The inner conductor transmits electric signals, and the outer conductor acts as a ground.
- The entire assembly is wrapped in a sheath of Teflon or PVC (polyvinyl chloride).

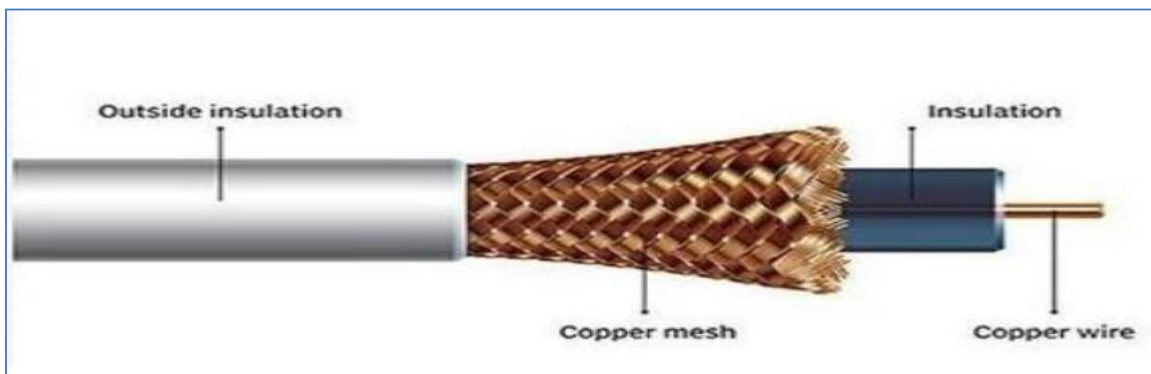


Figure: The cross-section of a typical coaxial cable

- The conductor used in coaxial cables is copper wire. It is used for both the inner and outer conductors.
- Coaxial cable is more resistant to interference and attenuation than twisted-pair cabling. Although coaxial cabling is difficult to install, it is highly resistant to signal interference.
- **The commonly used coaxial cables in Ethernet LANs are:**
 1. **10base2:** It is known as *thin net* supports a data-transfer rate of 10 Mbps and can transmit signals without attenuation over a distance of 185 meters. . Thinnet connects directly to a workstation's network adapter card using a British Naval Connector (BNC).
 2. **10base5:** It is known as *thick net*, supports a data-transfer rate of 10 Mbps over a distance of 500 meters. Thick net has a maximum cable length of 500 meters and usually is used as a backbone to connect several smaller thinnet -based networks.
- There are three categories of coaxial cables namely, RG-59 (Cable TV), RG-58 (Thin Ethernet), and RG-11 (Thick Ethernet). RG stands for Radio Government.

- **Advantages:**

1. Support high bandwidths and can transmit signals up to 10 kilometers.
2. It was relatively inexpensive, and it was light, flexible, and easy to work with.
3. In fact, coaxial cables were the original transmission medium specified by IEEE for use with Ethernet.

- **Disadvantages:** 1. It supports only the bus topology. Coaxial cables do not support star topology, which is the most common topology used in LANs.

Twisted-Pair Cables

- A typical twisted-pair cable consists of four pairs of thin copper wires coated with PVC or Teflon, spiralled (twisted) around one another.
- The spiralling results in radiation between the copper wires and cancels the effect of EMI.
- A pair of wires forms a circuit that can transmit data. The pairs are twisted to provide protection against crosstalk. Crosstalk is the undesired signal noise generated by the Electro-Magnetic fields of the adjacent wires.
- Twisted pair may be used to transmit both analog and digital signals. For analog signals, amplifiers are required about every 5 to 6 km. For digital signals, repeaters are required every 2 or 3 km.

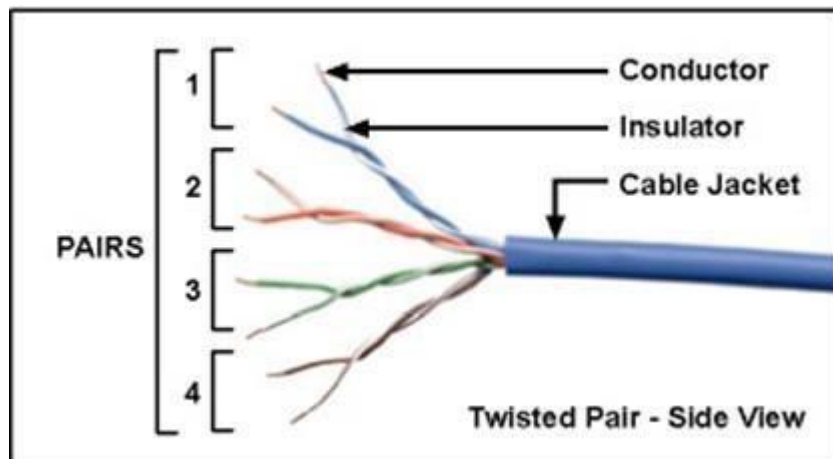


Figure: Cross section of Twisted Pair Cable

- A twisted pair consists of two insulated conductor twisted together in the spiral form. Twisting of wires will reduce the effect of noise or external interference. One of the wires is used to carry signals to the receiver and the other is used only as a ground reference.

- The number of twists per unit length will determine the quality of the cable. More twists means better quality. It can be shielded or unshielded.
- The twisted-pair cables generally used in LANs are of the following types:

Shielded Twisted Pair (STP)

Unshielded Twisted Pair (UTP)

Shielded Twisted Pair (STP)

- In STP, an extra layer of metal foil is present between the twisted pairs of copper wires and the outer sheath.
- The purpose of this layer is to provide additional protection from EMI and RFI.

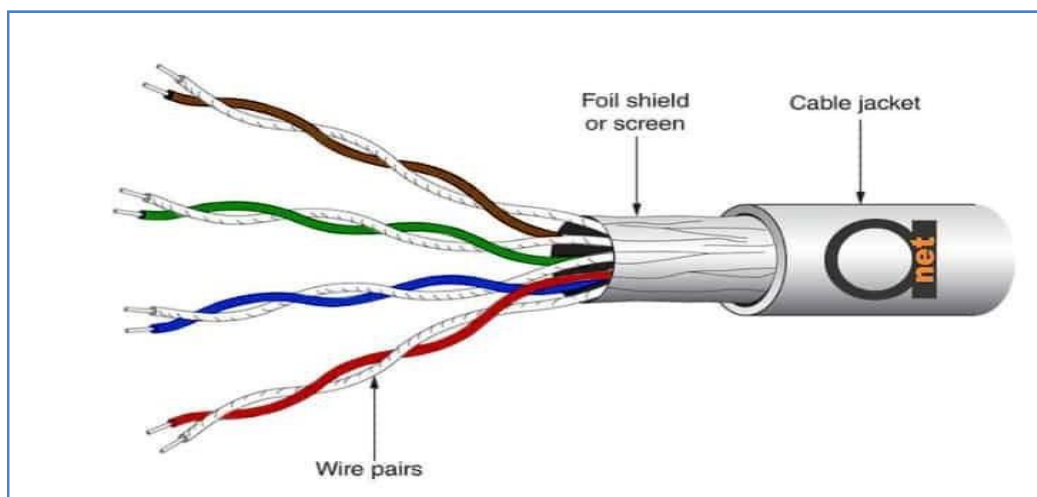


Figure: Cross-section of the STP cable.

- STP is more expensive than UTP and is generally used in networks where cables pass closer to devices that cause high EMI .
- The presence of shielding increases the resistance to the signal and, therefore, restricts the cable length and the throughput offered by STP.
- The following summarizes the features of STP cable:
 - ✓ Speed and throughput—10 to 100 Mbps
 - ✓ Average cost per node—Moderately expensive
 - ✓ Media and connector size—Medium to large
 - ✓ Maximum cable length—100 m (short)

Unshielded Twisted Pair (UTP)

- UTP cables are the most commonly used communication medium in LANs.
- Of the four pairs in a UTP cable, however, only two pairs are actually used for communication in LANs and provide speeds of up to 100 Mbps.

- The wire pairs are then covered with a plastic outer jacket. Each pair is twisted with a different number of twists per inch to help eliminate interference from adjacent pairs and other electrical devices.
- The tighter the twisting, the higher the supported transmission rate and the greater the cost per foot.



Figure: Cross-Section of UTP Cable

- UTP cables are capable of supporting different bandwidths and transmission speeds.
- Depending on the bandwidth offered, the following categories of UTP cables are defined:
- Category 1 (Cat-1), Category 2 (Cat-2), Category 3 (Cat-3), Category 4 (Cat-4), Category-5 (Cat-5)

Advantage:

- UTP cables are inexpensive and are resistant to physical stress.
- They also offer the flexibility to select a particular category of cable depending on the network requirements and resist attenuation over distances that are adequate for most LANs.

Disadvantage:

- UTP cables should not be used if the network is located in an environment with high EMI.

Optical Fibre Cables

- Optical fibre cables transmit data in the form of light. Optical fibre cables contain long thin strands of pure glass, called the fibre, with each strand having a diameter of about 5 microns.
- An optical fibre is a thin (2 to 125 μm), flexible medium capable of conducting an optical ray. Various glasses and plastics can be used to make optical fibres
- A typical optical fibre cable consists of the following three components:
 - **Core:** The core contains the optical fibre conductor (glass) that transmits light.
 - **Cladding:** The core is surrounded by another optical material to prevent any light from escaping the core. The function of cladding is to reflect the light back into the core.
 - **Sheath or Outer jacket:** The core and cladding are covered with a sheath, usually made of plastic, to protect the fibre from damage.

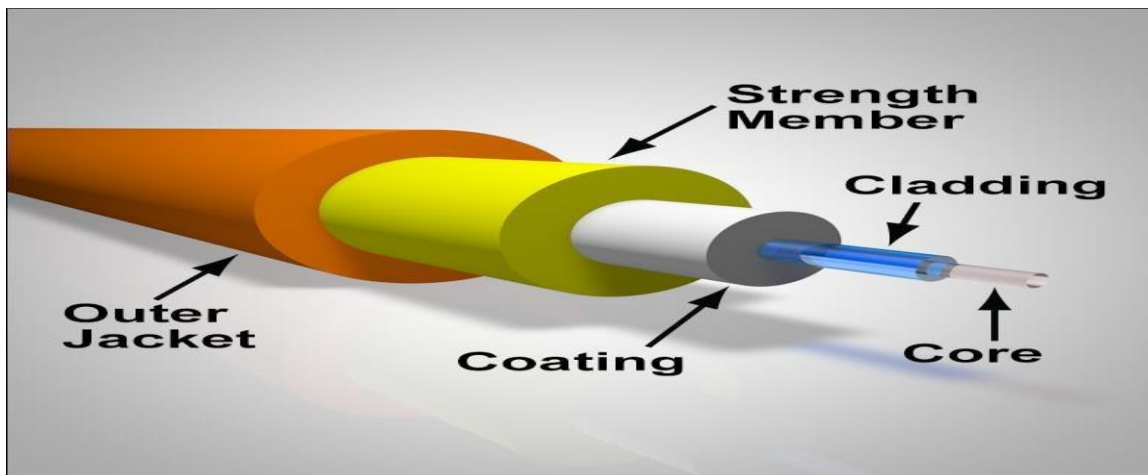


Figure: Cross-Section of Optical Fibre Cable

- The data to be transmitted is converted into light by a codec (coder and decoder) present at each end of the fibre.
- Fibre optic cable transmits light signals which are converted from electrical to light with the help of devices like Light Emitting Diodes (LEDs) or Light Amplification by Stimulated Emitted Radiations (LASERs).
- Each fibre has an inner core of glass or plastic that conducts light. The inner core is surrounded by cladding, a layer of glass or plastic that reflects the light back into the core instead of refraction.
- The codec converts the data from the computer into light, and the light is then transmitted across the cable with the help of either a Light Emitting Diode (LED) or an Injection Laser Diode (ILD).
- At the destination computer, a decoder receives the light beam and converts it into data.

LAN Connectors

- Connectors act as interface between NIC of the computer and the cable that transmits the signals.
- The type of connector depends on type of cable of used to connect computers or devices on the network.

Coaxial Cable Connectors

- To connect coaxial cable to the device, we need coaxial cable connector.
- To connect a coaxial cable to an NIC, the following connectors are required:
 - ✓ BNC connector
 - ✓ T-connector
 - ✓ Terminator

BNC Connectors: (BNC stands for British Naval/Navy Connector or Bayonet Nut Connector or Bayonet Neill Councilman Connector) are available in three different forms:

1. BNC Cable Connector
2. BNC –T Connector
3. BNC Terminator



BNC connector



BNC terminator



BNC T-connector

Figure: Coaxial Cable Connectors in different forms

- The end of the coaxial cable that plugs into a computer is connected to a BNC connector.
- A BNC connector connects the coaxial cable to the T-connector, which is plugged into the NIC of the computer.
- A terminator is required at the end of the coaxial cable in the network to absorb or destroy any signals that are not received by the computers in the network.

Twisted Pair Cable Connectors

- UTP and STP use different connectors to connect with the NIC.
- A UTP cable connects to an NIC with an RJ-45 connector.
- An STP cable uses a D-shell (or DB-9) connector.
- The standard connector for unshielded twisted pair cabling is an RJ-45 connector. This is a plastic connector attached to UTP cable.
- A slot allows the RJ-45 to be inserted only one way. RJ stands for Registered Jack.

- Figure shows the DB-9 connector, which is used with STP and an RJ-45 connector used with UTP.

RJ 45 Connector



Figure: RJ-45 connector

- The connector used on a UTP cable is called as RJ-45 (Registered Jack 45) connector.
- Below picture shows an RJ45 jack, attached to UTP cable. Eight color-coded wires inside Twisted-Pair cable is attached to eight pins in a RJ45 jack as shown above.
- Each wire in the Twisted Pair cable is crimped into 8 pins in the RJ45 jack.
- To prepare a UTP network cable, it is necessary to crimp two RJ45 connectors as shown below.



Figure: UTP network cable

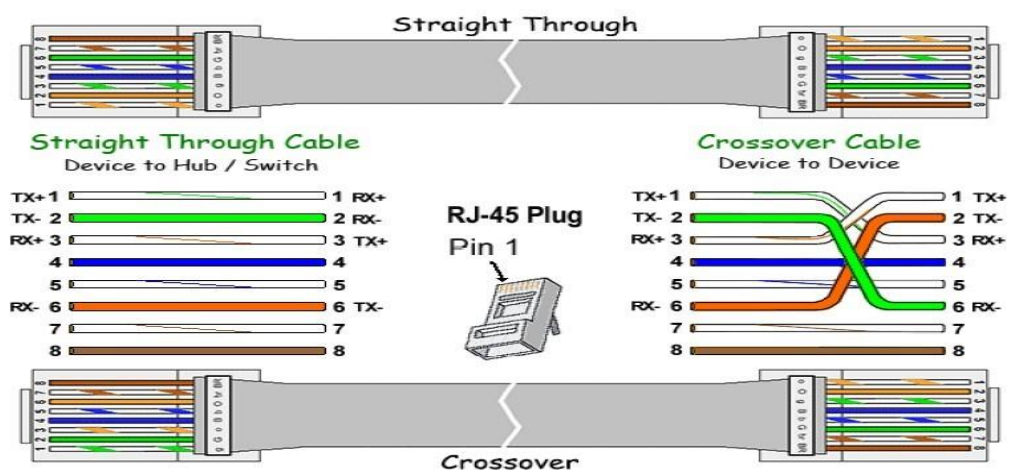
- There are two types of cabling: straight-through cabling and crossover cabling.
- Straight-through cable is used for connecting a computer to the hub/switch.
- Whereas crossover cable is used for connecting two computers or two hubs/switches. Each cable requires two connectors.

Straight-through Cable:

Pin Num.	Connector 1 (T-568A)	Connector 2 (T-568A)
01	White Green	White Green
02	Green	Green
03	White Orange	White Orange
04	Blue	Blue
05	White Blue	White Blue
06	Orange	Orange
07	White Brown	White Brown
08	Brown	Brown

Cross Over Cable:

Pin Num.	Connector 1 (T-568A)	Connector 2 (T-568B)
01	White Green	White Orange
02	Green	Orange
03	White Orange	White Green
04	Blue	Blue
05	White Blue	White Blue
06	Orange	Green
07	White Brown	White Brown
08	Brown	Brown



Optical Fibre Connectors

- There are several types of fibre optic connectors available today.
- The most common are: ST, SC, FC, MT-RJ and LC style connectors.

Straight Tip (ST)

- The ST connector is one of the first connector types widely implemented in fibre optic networking applications.
- ST connections use a 2.5mm ferrule with a round plastic or metal body. Available in single-mode and multimode.
- The connector stays in place with twist-on/twist-off mechanism.
- The ST connector are reliable and durable field installation



Figure 4.11 Straight Tip (ST) Connector

Subscriber Connector (SC)

- SC connectors also use a round 2.5mm ferrule to hold a single fiber.
- They use a push-on/pull-off mating mechanism which is generally easier to use.
- The connector body of an SC connector is square shaped, and two SC connectors are usually held together with a plastic clip (this is referred to as a duplex connection). T
- The Subscriber Connector (SC) can be seen commonly on MMF or SMF.
- Figure below shows an example of an SC connector:



Figure 4.12 Subscriber Connector (SC)

Lucent Connector (LC)

- One popular Small Form Factor (SFF) connector is the LC type. This interface was developed by Lucent Technologies (hence, Lucent Connector).
- It uses a retaining tab mechanism, similar to a phone or RJ45 connector, and the connector body resembles the square shape of SC connector.
- LC connectors are normally held together in a duplex configuration with a plastic clip.
- The ferrule of an LC connector is 1.25mm.
- LC connector is always duplex connecting a pair of fibers at a time.

- Figure below shows an example of a LC connector:



Figure 4.13 Lucent Connector (LC)

Multi-fibre Push On (MPO)

- The Multi-fibre Push On (MPO) connector is another duplex connector that offers an easy option for connection.
- It is often also referred to as Multi-fiber Termination Push-on (MTP); the MTP connector is a brand name (US Conec).
- Figure below shows an example of an MPO connector:



Figure 4.14 Multi-fiber Push On (MPO) Connector

MU Connector

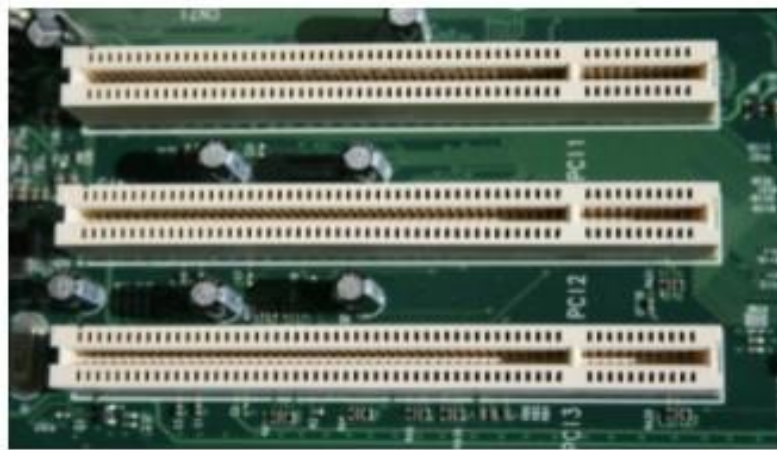
- The MU connector is designed for high-density connections.
- This small single-fiber connector has a high level of performance, providing more than double the packaging density of the SC connector.
- The following Figure shows the MU connector.



Figure 4.15 MU connector

Expt.No: 9 Install and configure NIC.

- The NIC is also commonly referred to as a network adapter and is an expansion card that enables a computer to connect to a network such as a home network and/or the Internet using a Ethernet cable with a RJ-45 connector.
- This section discusses the process of installing a Network Interface Card/Network Adapter.
- Steps:
 1. First step is to read the user's guide and familiarize yourself with the new card.
 2. Power down PC and remove the AC power cord.
 3. Open the computer case.
 4. Find an available Peripheral Component Interconnect (PCI) slot on the motherboard.



5. Carefully remove the network card from its static-proof plastic envelope, and slide it into the slot.
6. Seat the card in the slot firmly with gentle pressure along the length of the card, especially right about the slot itself.



7. Snugly, screw the card to the computer frame, but do not over tighten.
8. Close the computer case.
9. Plug your computer in and power it up.
10. Click Start and then go to control panel.

Computer Networks Lab Manual

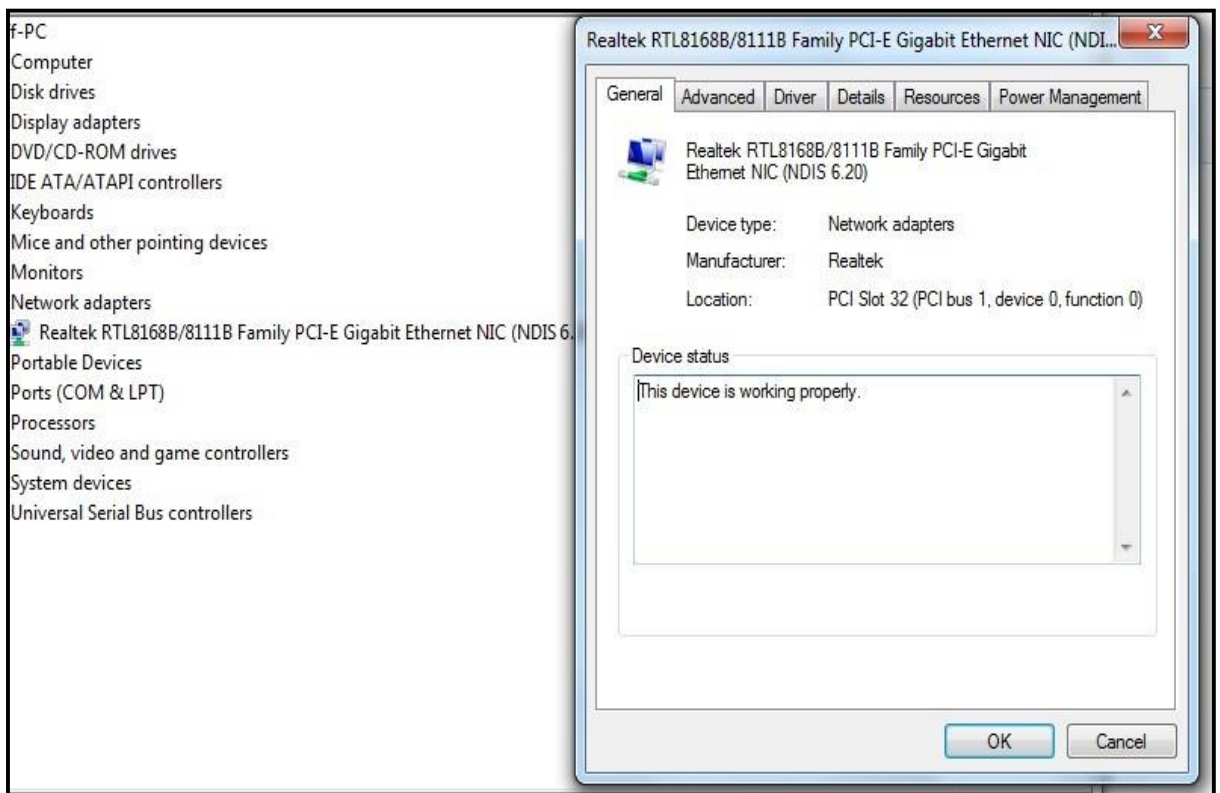
11. Click on hardware and sound and the click on Device Manager.



12. Double click network adapters which shows name of your Ethernet Card.

13. Next, double click the name of the Ethernet Adapter.

14. If the text in the "Device Status" box says **"This device is working properly."**, then you successfully installed the card and are finished.



Expt.No: 10

Crimping of RJ45: Straight and Cross.

a) **Punching Cat 6 cable to I/O Box. Use punching tool.**

b) **Check connectivity using LAN tester.**

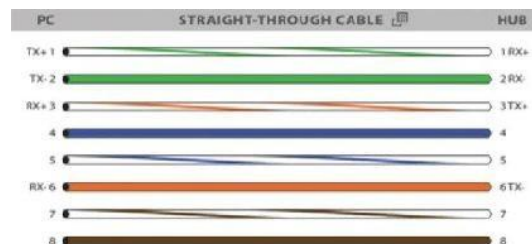
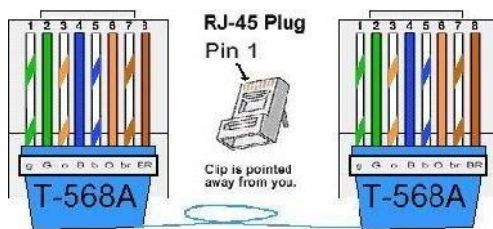
- Crimping is the process of connecting RJ (Registered Jack) 45 connector to the Ethernet cable using crimping tool. Generally there are two types of crimping
 - Straight Through Crimping and
 - Cross Over Crimping
- For connecting two computers to transfer the data we have to use connectors on both ends of a cable. Generally, the connectors are male-female type to ensure reliable connection. The standard connector for unshielded twisted pair cabling is an RJ-45 connector which is made up of plastic and looks like a large telephone-style connector. Although RJ 45 is used for a variety of purposes, but the RJ-45 connector is most commonly used for 10Base-T and 100Base-TX Ethernet connections.

RJ-45 Connector and its Pin Position



Straight Through Crimping

- This type of crimping is used when we want to connect unlike devices i.e., computer to switch, computer to hub, router to switch, switch to computer etc.,
- T-568A Straight Through Crimping and its Pin Connection



T-568A Straight Through Connection

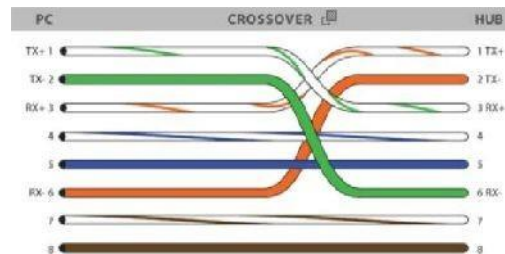
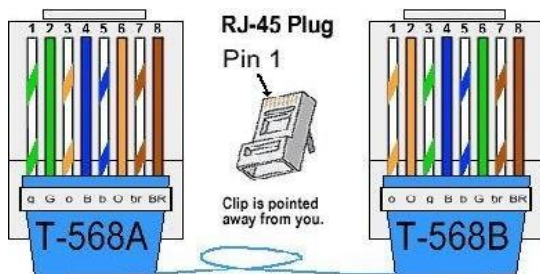
Pin Num.	Connector 1 (T-568A)	Connector 2 (T-568A)
01	White Green	White Green
02	Green	Green
03	White Orange	White Orange
04	Blue	Blue
05	White Blue	White Blue
06	Orange	Orange
07	White Brown	White Brown
08	Brown	Brown

T-568B Straight Through Connection

Pin Num.	Connector 1 (T-568B)	Connector 2 (T-568B)
01	White Orange	White Orange
02	Orange	Orange
03	White Green	White Green
04	Blue	Blue
05	White Blue	White Blue
06	Green	Green
07	White Brown	White Brown
08	Brown	Brown

Cross Over Crimping

- This type of crimping is commonly used when we want to connect like devices i.e., router to router, switch to switch, computer to computer etc.
- T-568A and T-568B Cross Over Crimping and its Pin Connection

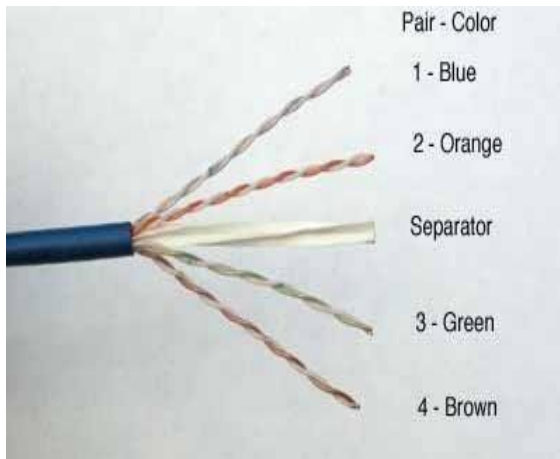


T-568A and T-568B Cross over Connection Categories of UTP cables (Unshielded Twisted Pair)

Pin Num.	Connector 1 (T-568A)	Connector 2 (T-568B)
01	White Green	White Orange
02	Green	Orange
03	White Orange	White Green
04	Blue	Blue
05	White Blue	White Blue
06	Orange	Green
07	White Brown	White Brown
08	Brown	Brown

Type	No of Pairs	Transmission Rate	Implementation
Category 1	1	Voice Grade	<ul style="list-style-type: none">• used in telephone industry• not suitable for long distance data transmission (used only for short distance)
Category 2	2	4 Mbps	<ul style="list-style-type: none">• used for both data and voice transmission
Category 3	4	10 Mbps	<ul style="list-style-type: none">• required 3 twist per foot• used for 10 base networks.• used for voice communication
Category 4	4	16 Mbps	<ul style="list-style-type: none">• required 3 twist per foot• used in IBM token ring networks
Category 5	4	100 Mbps	<ul style="list-style-type: none">• used in Ethernet and 100 Base-X networks
Category 6	4	100 Mbps and higher	<ul style="list-style-type: none">• used in Ethernet and 1000 Base-X networks

Cables and Tools Used for Crimping:



CAT 6 Cable and its internal Twist Pairs connection



Cat 6 cable ready to use for LAN



Crimping and Punching Tool



LAN Tester

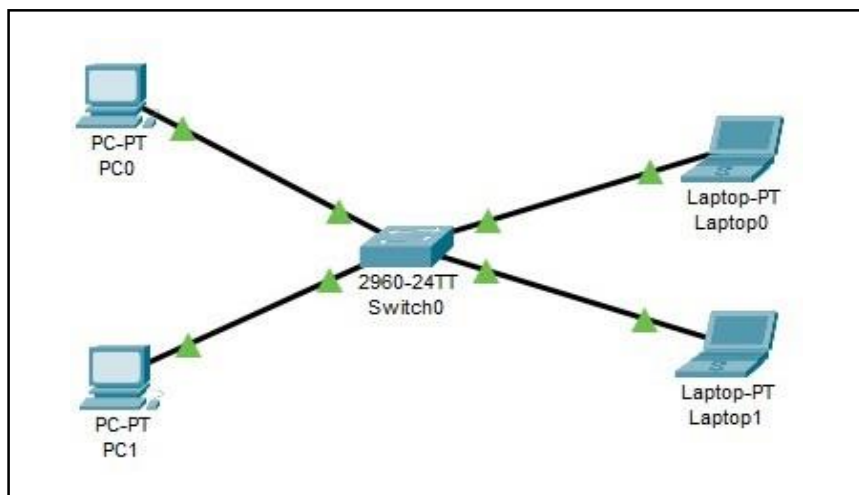
Expt.No: 11. Install Network simulator like Cisco packet tracer. Create simple network in simulator. Create and demonstrate all possible network topologies using simulator.

Installing Packet Tracer:

- Download Packet Tracer which is appropriate for your operating system i.e Windows
- Installation in Windows is pretty simple and straightforward; the setup comes in a single file named Packettracer_Setup 7.3.0.exe.
- Open this file to begin the setup wizard, accept the license agreement, choose a location, and start the installation.

Create simple network in simulator:

- Design and create simple network as shown below.



O/p: Check for successful connection on pinging to any pc through its IP address.

```
Packet Tracer PC Command Line 1.0
C:\>ping 10.1.1.4

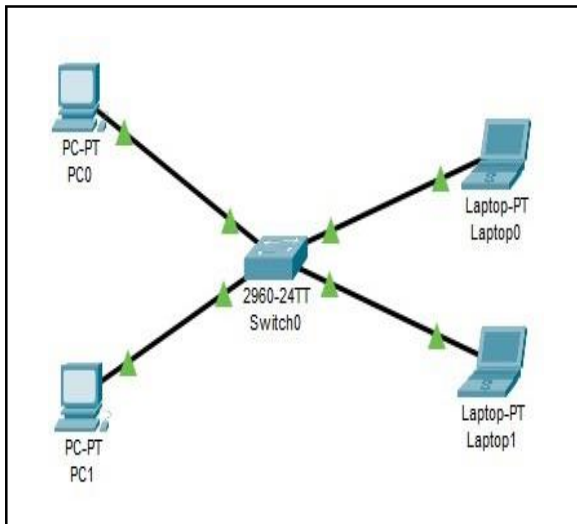
Pinging 10.1.1.4 with 32 bytes of data:

Reply from 10.1.1.4: bytes=32 time=16ms TTL=128
Reply from 10.1.1.4: bytes=32 time=8ms TTL=128
Reply from 10.1.1.4: bytes=32 time=8ms TTL=128
Reply from 10.1.1.4: bytes=32 time=8ms TTL=128

Ping statistics for 10.1.1.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 8ms, Maximum = 16ms, Average = 10ms

C:\>|
```

Network Topologies: Star Topology:



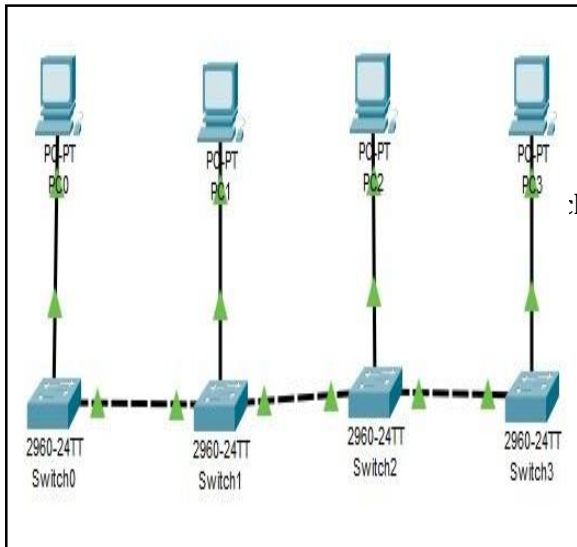
```
PC1
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 10.1.1.4

Pinging 10.1.1.4 with 32 bytes of data:

Reply from 10.1.1.4: bytes=32 time=16ms TTL=128
Reply from 10.1.1.4: bytes=32 time=8ms TTL=128
Reply from 10.1.1.4: bytes=32 time=8ms TTL=128
Reply from 10.1.1.4: bytes=32 time=8ms TTL=128

Ping statistics for 10.1.1.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 8ms, Maximum = 16ms, Average = 10ms
C:\>
```

Bus Topology:



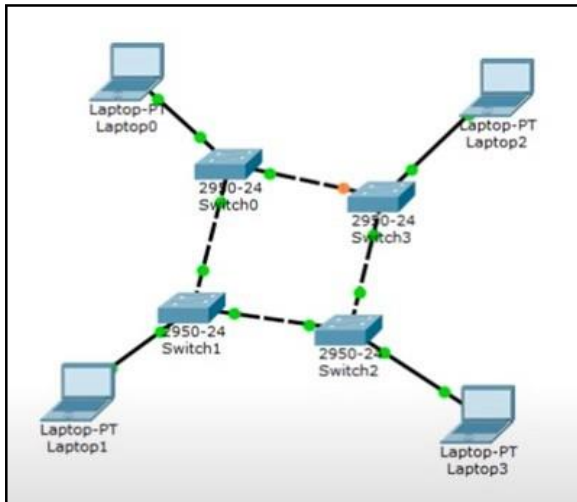
```
PC3
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 10.1.1.1

Pinging 10.1.1.1 with 32 bytes of data:

Reply from 10.1.1.1: bytes=32 time=20ms TTL=128
Reply from 10.1.1.1: bytes=32 time=10ms TTL=128
Reply from 10.1.1.1: bytes=32 time=10ms TTL=128
Reply from 10.1.1.1: bytes=32 time=10ms TTL=128

Ping statistics for 10.1.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 10ms, Maximum = 20ms, Average = 12ms
C:\>
```

Ring Topology:



```
PC3
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 10.1.1.1

Pinging 10.1.1.1 with 32 bytes of data:

Reply from 10.1.1.1: bytes=32 time=20ms TTL=128
Reply from 10.1.1.1: bytes=32 time=10ms TTL=128
Reply from 10.1.1.1: bytes=32 time=10ms TTL=128
Reply from 10.1.1.1: bytes=32 time=10ms TTL=128

Ping statistics for 10.1.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 10ms, Maximum = 20ms, Average = 12ms
C:\>
```