Expt.No: 02
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.

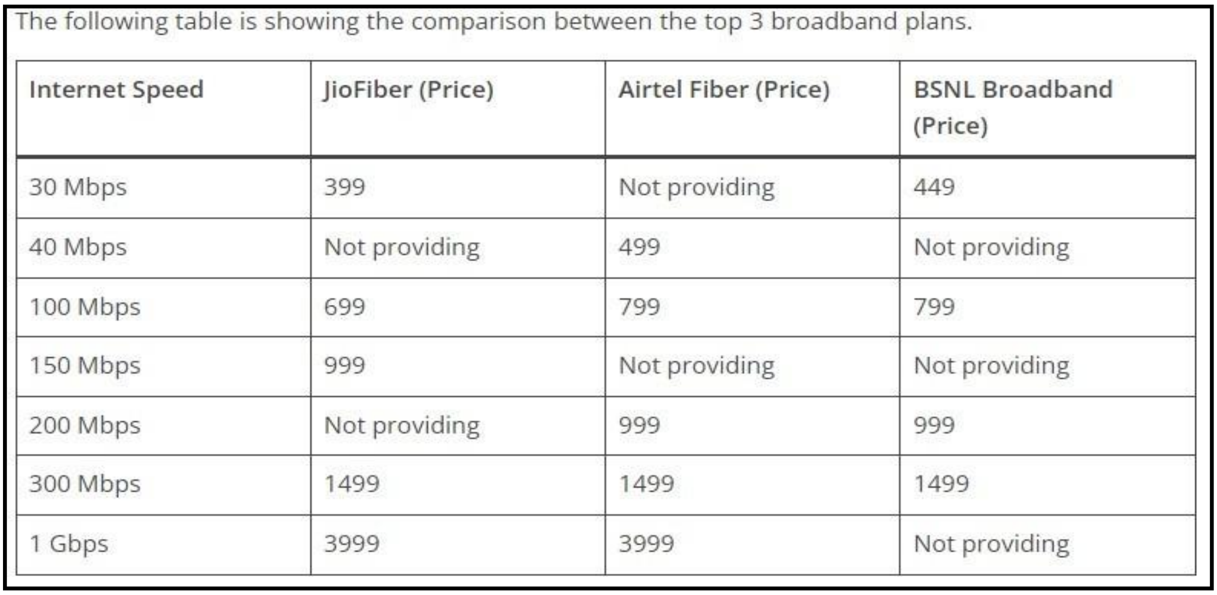
Cable

- 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

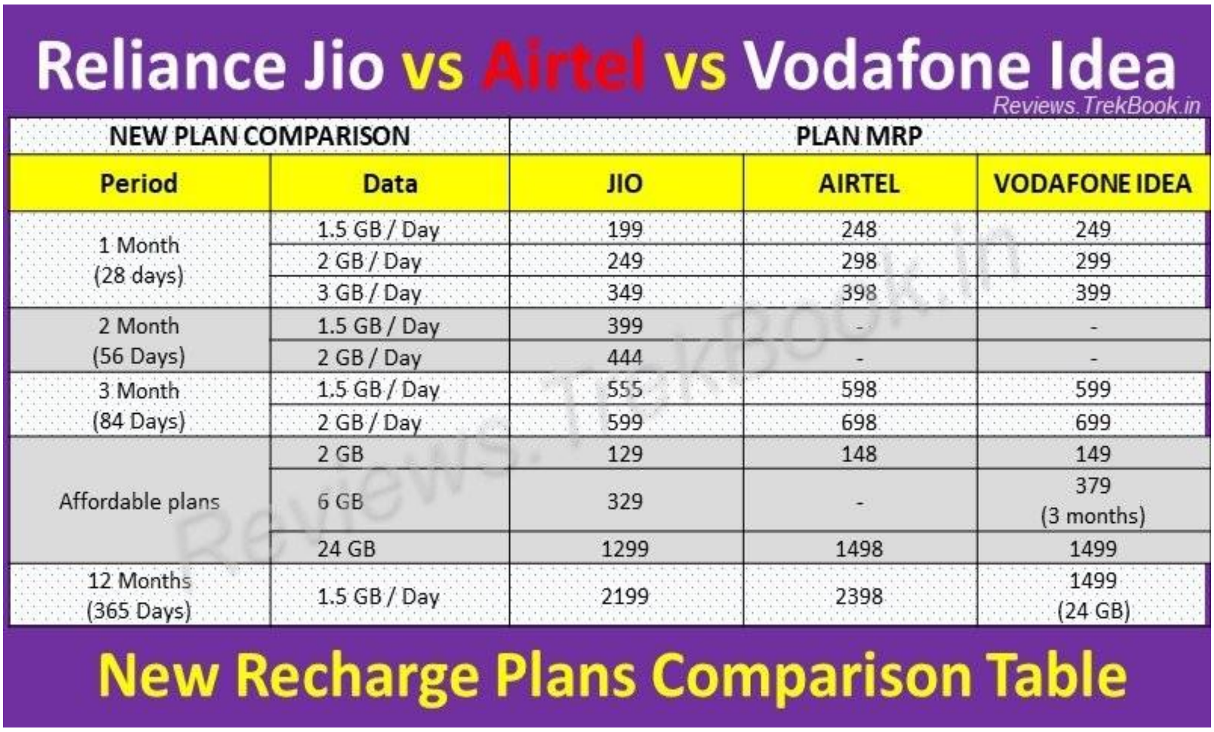
- Wi-Fi is wireless Internet access. It's used by laptops and offered freely by many hotels and coffee shops. Wi-Fi can also be installed in the home for people who have desktops and laptops networked. Wi-Fi is not as quick as DSL or Cable, but it's a more convenient ISP service.

There are a number of different internet providers



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

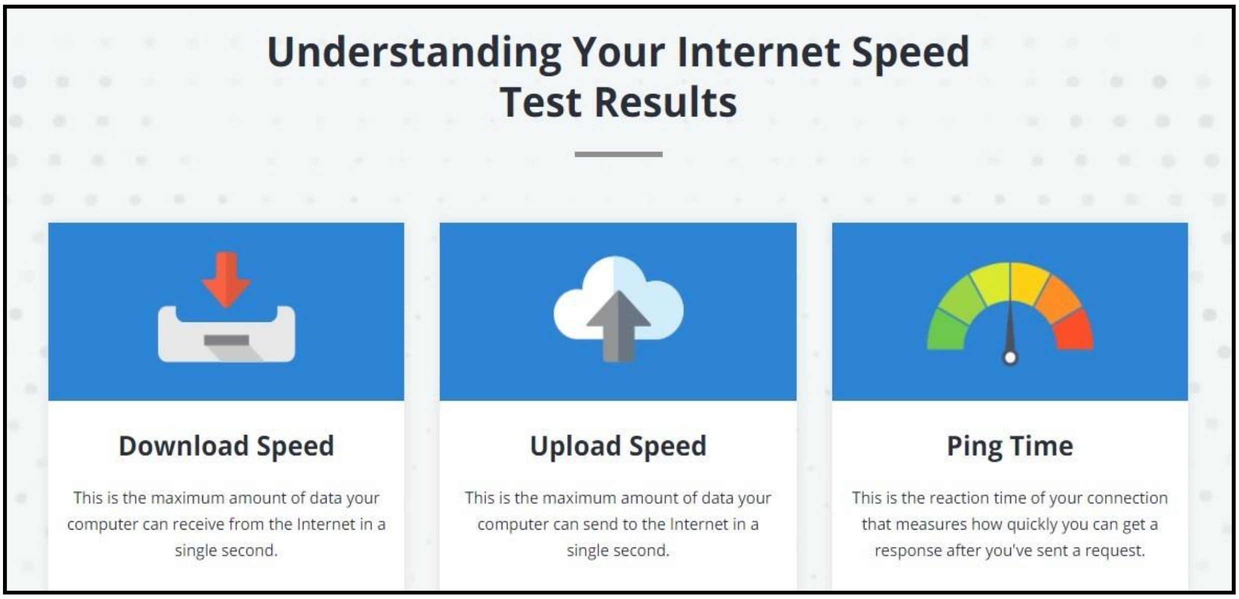
NEW PLAN COMPARISON		PLAN MRP		
Period	Data	JIO	AIRTEL	VODAFONE IDEA
1 Month (28 days)	1.5 GB / Day	199	248	249
	2 GB / Day	249	298	299
	3 GB / Day	349	398	399
2 Month (56 Days)	1.5 GB / Day	399	-	-
	2 GB / Day	444	-	-
3 Month (84 Days)	1.5 GB / Day	555	598	599
	2 GB / Day	599	698	699
Affordable plans	2 GB	129	148	149
	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: 03

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



Understanding Your Internet Speed Test Results

Download Speed

This is the maximum amount of data your computer can receive from the Internet in a single second.

Upload Speed

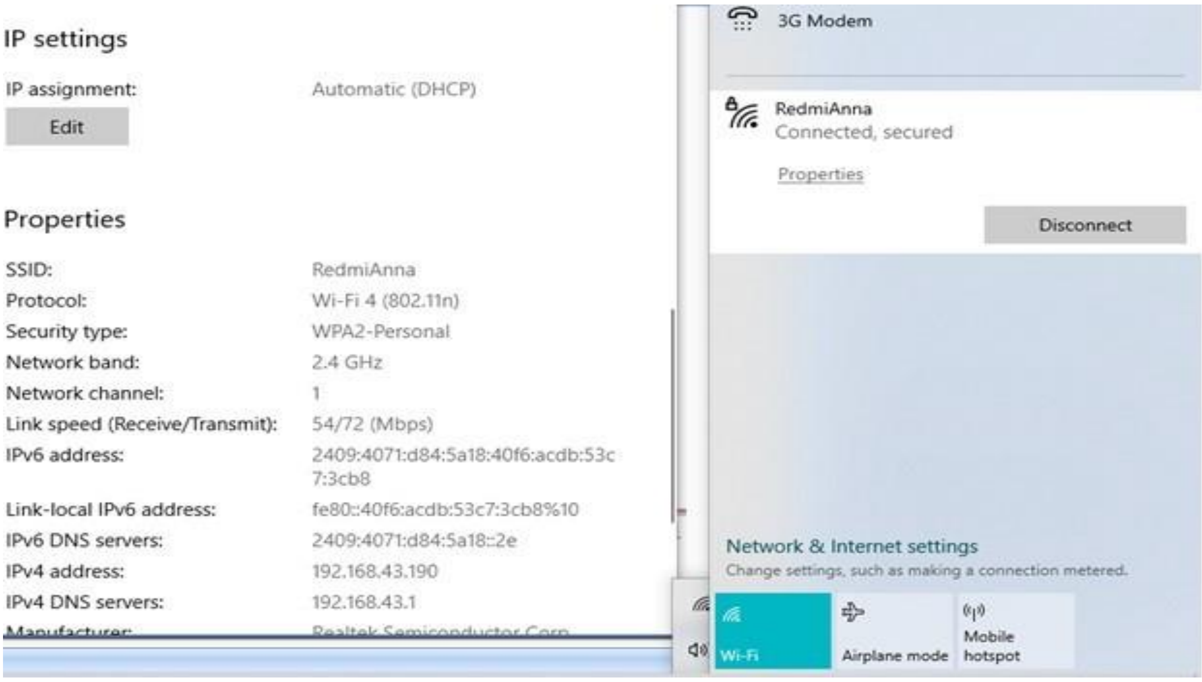
This is the maximum amount of data your computer can send to the Internet in a single second.

Ping Time

This is the reaction time of your connection that measures how quickly you can get a response after you've sent a request.

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:



IP settings

IP assignment: Automatic (DHCP)

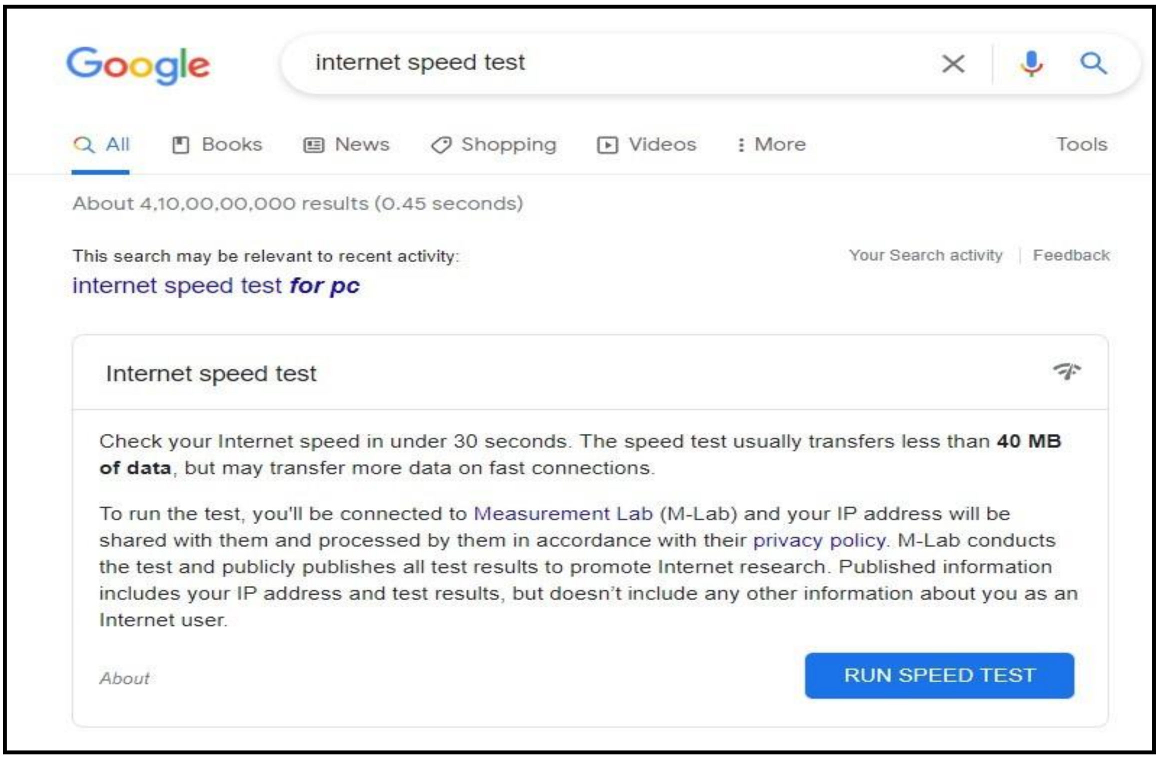
Properties

SSID:	RedmiAnna
Protocol:	Wi-Fi 4 (802.11n)
Security type:	WPA2-Personal
Network band:	2.4 GHz
Network channel:	1
Link speed (Receive/Transmit):	54/72 (Mbps)
IPv6 address:	2409:4071:d84:5a18:40f6:acdb:53c7:3cb8
Link-local IPv6 address:	fe80::40f6:acdb:53c7:3cb8%10
IPv6 DNS servers:	2409:4071:d84:5a18::2e
IPv4 address:	192.168.43.190
IPv4 DNS servers:	192.168.43.1
Manufacturer:	Realtek Semiconductor Corp.

RedmiAnna
Connected, secured

Network & Internet settings
Change settings, such as making a connection metered.

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



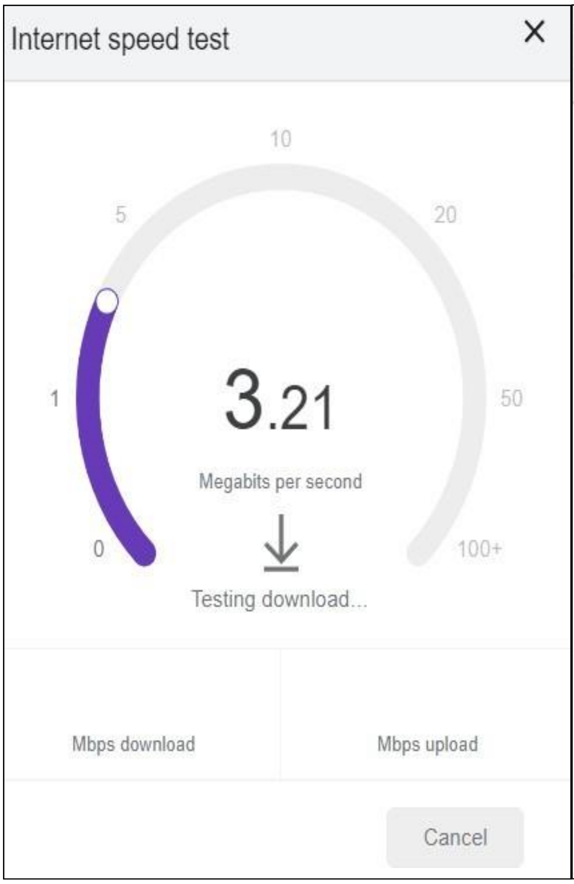
About 4,10,00,00,000 results (0.45 seconds)

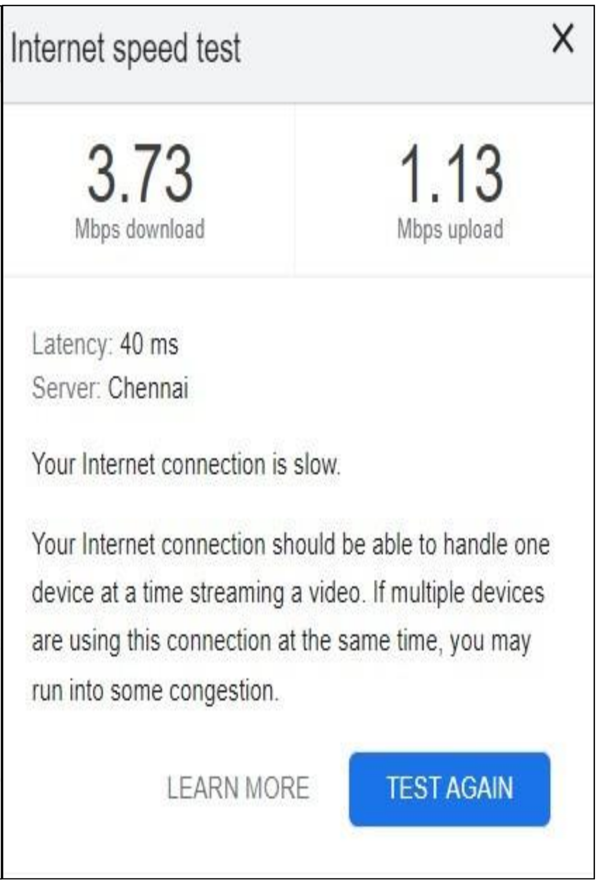
This search may be relevant to recent activity:
internet speed test ***for pc***

Internet speed test

Check your Internet speed in under 30 seconds. The speed test usually transfers less than **40 MB of data**, but may transfer more data on fast connections.

To run the test, you'll be connected to Measurement Lab (M-Lab) and your IP address will be shared with them and processed by them in accordance with their privacy policy. M-Lab conducts the test and publicly publishes all test results to promote Internet research. Published information includes your IP address and test results, but doesn't include any other information about you as an Internet user.





Latency: 40 ms
Server: Chennai

Your Internet connection is slow.

Your Internet connection should be able to handle one device at a time streaming a video. If multiple devices are using this connection at the same time, you may run into some congestion.

Expt.No: 04

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:**Andriod.

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: 05. My Protocol rules objectives.

Objectives

i. Relate computer network protocols to the rules that you use every day for various forms of communication.

ii. Define the rules that govern how you send and interpret text messages.

iii. Explain what would happen if the sender and receiver did not agree on the details of the protocol.

iv. Play the communication game.

Background / Scenario:

- Before beginning to communicate with each other, we establish rules or agreements to govern the conversation. These rules, or protocols, must be followed for the message to be successfully delivered and understood. Among the protocol characteristics that govern successful human communication are:
  - ➢ An identified sender and receiver
  - ➢ Agreed upon method of communicating
  - ➢ Common language and grammar
  - ➢ Speed and timing of delivery
  - ➢ Confirmation or acknowledgement requirements
- The techniques that are used in network communications share these fundamentals with human conversations.

Instructions

- Think about the commonly accepted protocol standards for sending text messages to your friends. Fill out the chart on the next page with some of the rules that you follow when texting with friends and others.

Reflection

1. Now that you have documented the protocols that you use when sending and reading text messages, do you think that these protocols would be the same if you were texting with friends or with your parents and teachers? Explain your answer.

____

____

____

2. What do you think that the consequences would be if there was no agreed upon protocol standards for different methods of communications?____

____

3. Share your protocol rules with your classmates. Are there differences between your protocols and theirs? If so, could these differences result in misunderstanding of the messages?____

____

Your Text Messaging Protocol

Protocol Requirement	What does this mean?	How is it implemented in your protocol?
An identified sender and receiver	How do you know who the text message is from? How does the person on the other end know the message is delivered to you? Is it going to an individual or a group?	In text messaging, the sender and receiver are usually identified by telephone number, username, or nickname. Group texts can be sent to a predefined group or new groups created on demand.
Agreed upon method of communicating	Do we send text only? Do we send pictures back & forth? What about using smileys and emoji?	**It can be a mix of text, pictures, smileys and emoji. Depending on your device and mobile OS, you may even be able to send videos.**
Common language and grammar	Do we use acronyms? Is slang acceptable? What is the native language of the participants?	**The sender and receiver can use acronyms and languages that are understood by both sides.**
Speed and timing of delivery	What determines how soon the recipient gets the message? How quickly to we expect to receive a response?	**The speed of the delivery depends on the speed of the network and amount delay and latency in the network. A response is received when the recipient sends a response.**
Confirmation or acknowledgement requirements	How do you know that the message was received? How do you know that the conversation is finished?	**The intended recipient sends a response and the recipient indicates the end of the conversation.**

- Play the communication game (Telephone Game)-Dogs dig holes for big bones

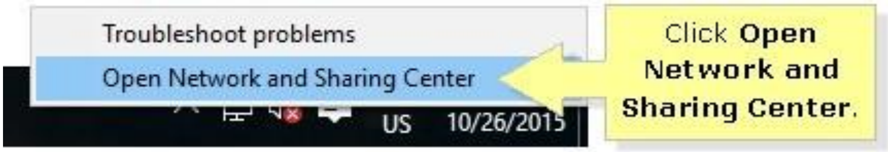
Expt.No: 06 Manual and Automatic address assignment (Windows)

a) IPv4 address
b) Subnet mask
c) DNS

Automatic address assignment:

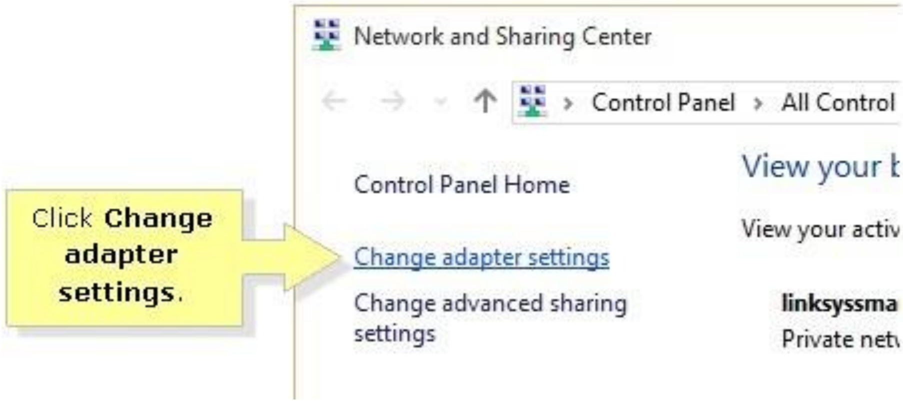
- Automatically obtaining an IP Address from a **DHCP (Dynamic Host Configuration Protocol)** server such as a router is an easy way to connect computer to the network.
- Instead of manually entering the IP Address, Subnet mask, and Default gateway, these can be automatically assigned by the DHCP server.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



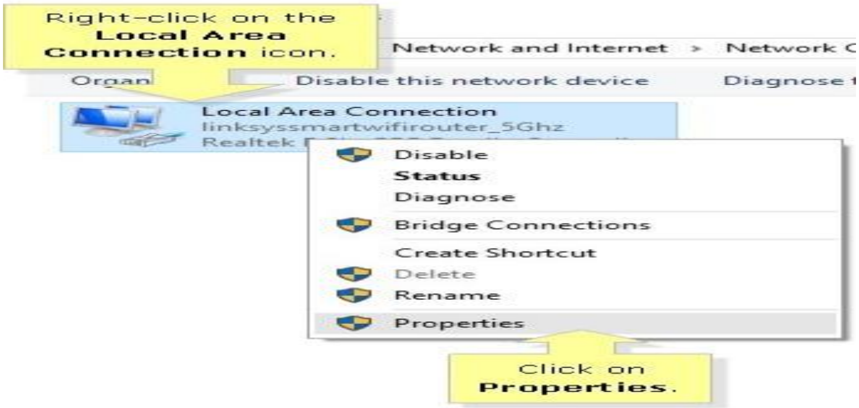
Click **Open Network and Sharing Center.**

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



Click **Change adapter settings.**

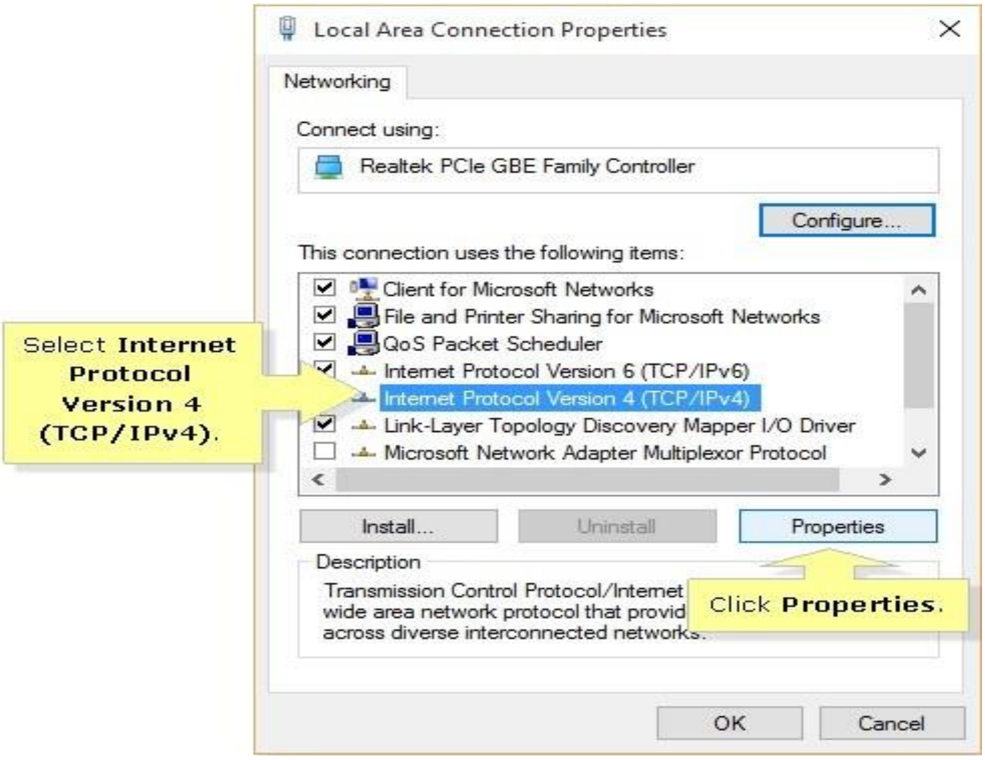
Step 3: Right-click on the **Local Area Connection** icon and click **Properties**.



Right-click on the **Local Area Connection** icon.

Click on **Properties.**

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



Local Area Connection Properties

Networking

Connect using:

Realtek PCIe GBE Family Controller

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- □ Microsoft Network Adapter Multiplexor Protocol

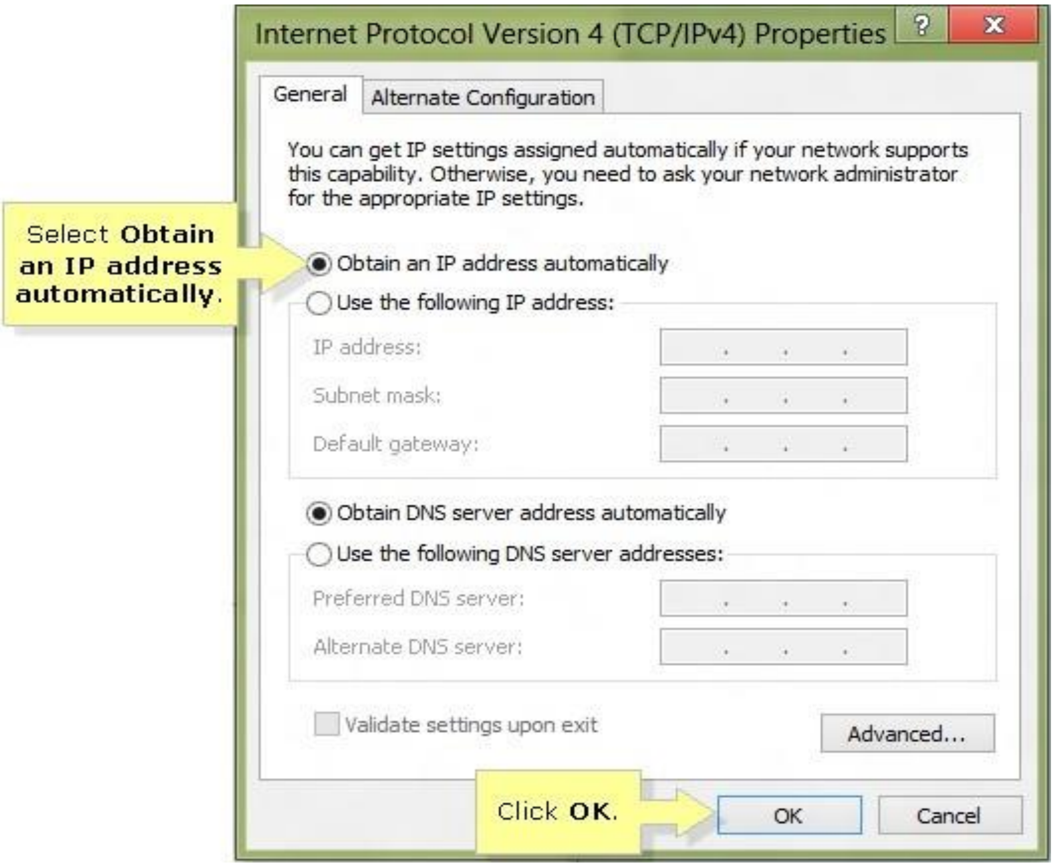
Description

Transmission Control Protocol/Internet wide area network protocol that provid across diverse interconnected networks.

Select **Internet Protocol Version 4 (TCP/IPv4)**.

Click **Properties**.

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



Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

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: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

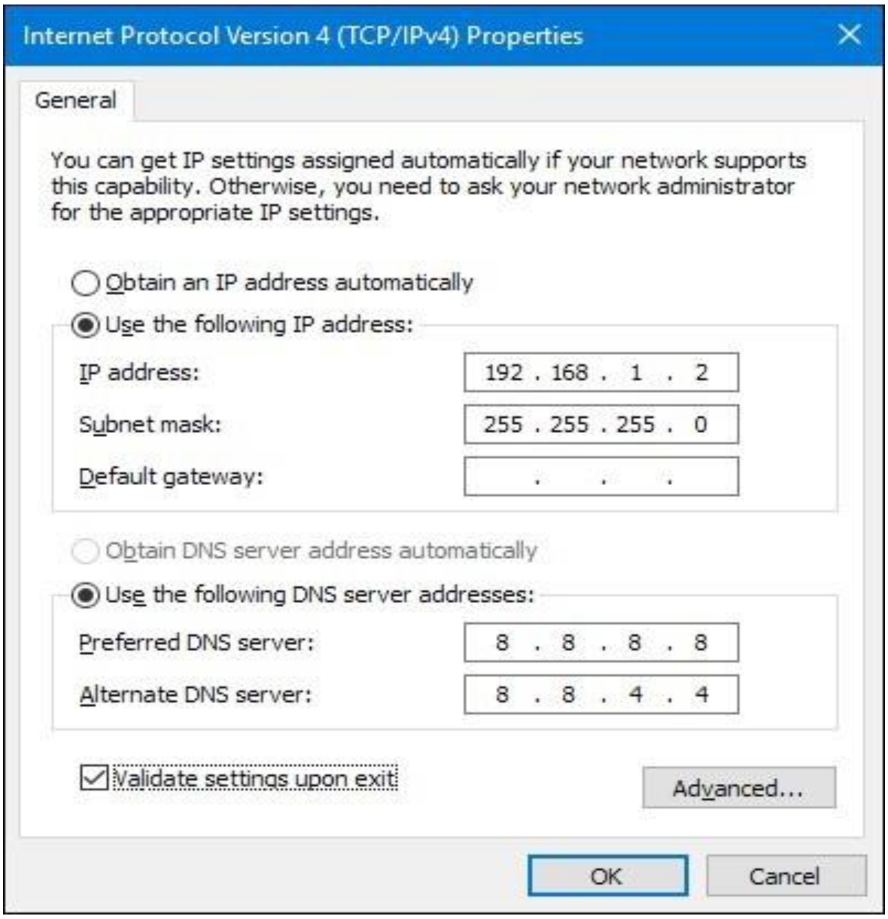
□ Validate settings upon exit

Select **Obtain an IP address automatically**.

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

Expt.No: 07 Manual and Automatic address assignment (Android)

a) IPv4 address

b) Subnet mask

c) DNS

Automatic address assignment:

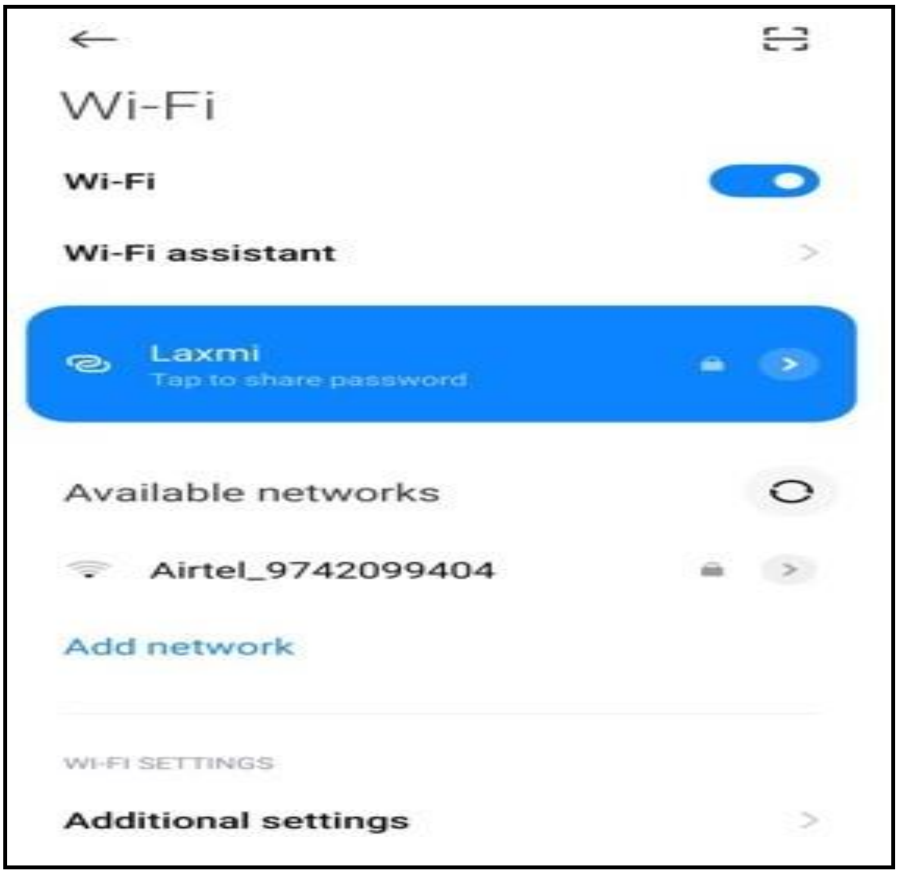
- Automatically obtaining an IP Address from a **DHCP (Dynamic Host Configuration Protocol)** server such as a router is an easy way to connect mobile to the network.
- Instead of manually entering the IP Address, Default gateway, DNS 1 and DNS 2 these can be automatically assigned by the DHCP server.

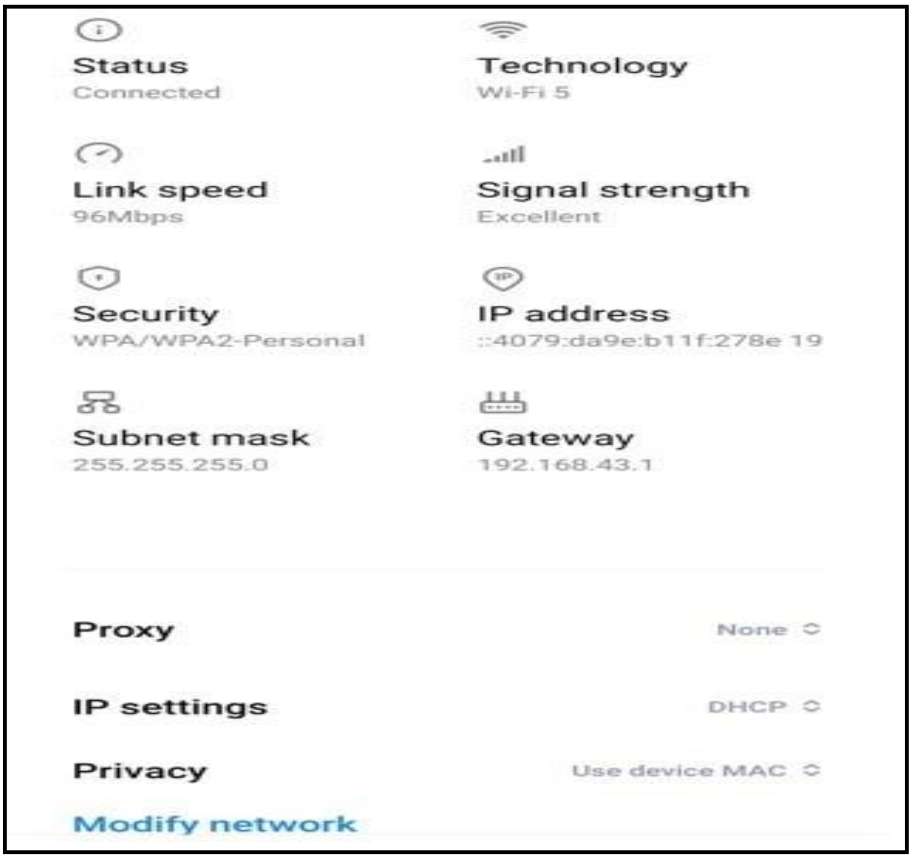
Manual address assignment:

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

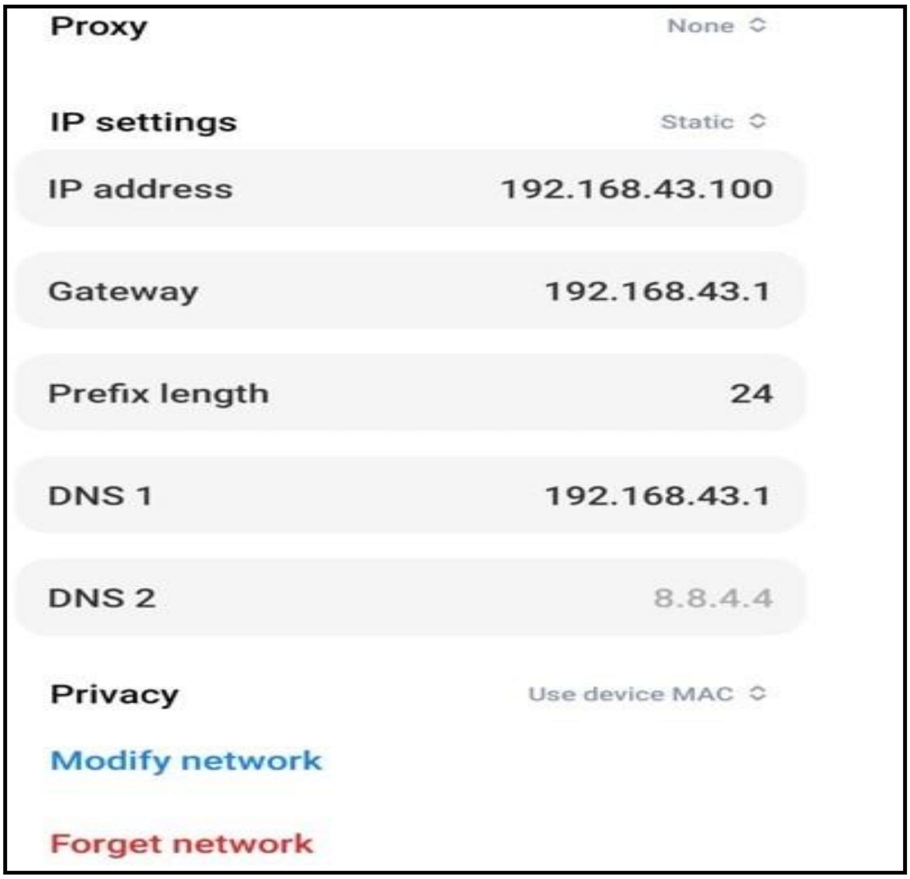
Gateway
192.168.43.1

Proxy None

IP settings DHCP

Privacy Use device MAC

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

Expt.No:08

i) Organize and play games to understand working of TCP/IP like: Create 2 groups of students, each playing role of layers of TCP/IP (intermediate network devices roles can also be considered). Start the communication between two with a sender and receiver.

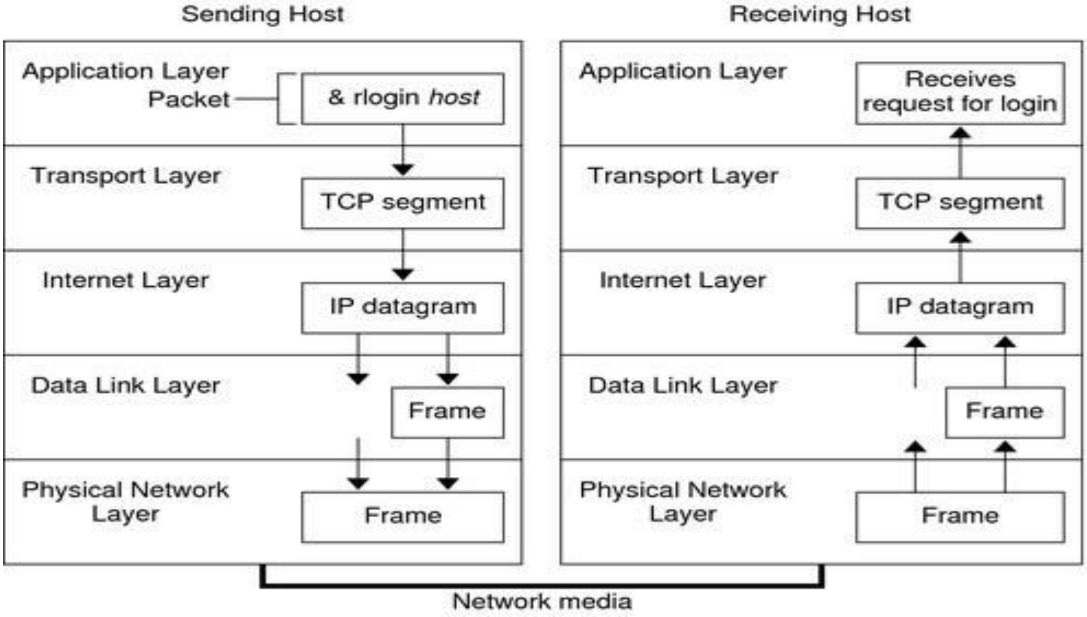
How the TCP/IP Protocols Handle Data Communications

- When a user issues a command that uses a TCP/IP application layer protocol, a series of events is initiated. The user's command or message passes through the TCP/IP protocol stack on the local system. Then, the command or message passes across the network media to the protocols on the remote system. The protocols at each layer on the sending host add information to the original data.
- Protocols on each layer of the sending host also interact with their peers on the receiving host. Figure shows this interaction.

Data Encapsulation and the TCP/IP Protocol Stack

- The packet is the basic unit of information that is transferred across a network. The basic packet consists of a header with the sending and receiving systems' addresses, and a body, or **payload**, with the data to be transferred. As the packet travels through the TCP/IP protocol stack, the protocols at each layer either add or remove fields from the basic header. When a protocol on the sending system adds data to the packet header, the process is called **data encapsulation**. Moreover, each layer has a different term for the altered packet, as shown in the following figure.

Figure : How a Packet Travels Through the TCP/IP Stack



- This section summarizes the life cycle of a packet. The life cycle starts when you issue a command or send a message. The life cycle finishes when the appropriate application on the receiving system receives the packet.

Application Layer: Where a Communication Originates

- The packet's history begins when a user on one system sends a message or issues a command that must access a remote system. The application protocol formats the packet so that the appropriate transport layer protocol, TCP or UDP, can handle the packet.
- Suppose the user issues an **rlogin** command to log in to the remote system, as shown in Figure. The **rlogin** command uses the TCP transport layer protocol. TCP expects to receive data in the form of a stream of bytes that contain the information in the command. Therefore, **rlogin** sends this data as a TCP stream.

Transport Layer: Where Data Encapsulation Begins

- When the data arrives at the transport layer, the protocols at the layer start the process of data encapsulation. The transport layer encapsulates the application data into transport protocol data units.
- The transport layer protocol creates a virtual flow of data between the sending and receiving application, differentiated by the transport port number. The port number identifies a **port**, a dedicated location in memory for receiving or sending data. In addition, the transport protocol layer might provide other services, such as reliable, in order data delivery. The end result depends on whether TCP, SCTP, or UDP handles the information.

TCP Segmentation

- TCP is often called a “connection-oriented” protocol because TCP ensures the successful delivery of data to the receiving host. Figure :Shows how the TCP protocol receives the stream from the **rlogin** command. TCP then divides the data that is received from the application layer into segments and attaches a header to each segment.
- Segment headers contain sending and receiving ports, segment ordering information, and a data field that is known as a **checksum**. The TCP protocols on both hosts use the checksum data to determine if the data transfers without error.

Establishing a TCP Connection

- TCP uses segments to determine whether the receiving system is ready to receive the data. When the sending TCP wants to establish connections, TCP sends a segment that is called a **SYN** to the TCP protocol on the receiving host. The receiving TCP returns a segment that is called an **ACK** to acknowledge the successful receipt of the segment. The sending TCP sends another ACK segment, and then proceeds to send the data. This exchange of control information is referred to as a **three-way handshake**.

UDP Packets

- UDP is a “connectionless” protocol. Unlike TCP, UDP does not check that data arrived at the receiving host. Instead, UDP formats the message that is received from the application layer into **UDP packets**. UDP attaches a header to each packet. The header contains the sending and receiving ports, a field with the length of the packet, and a checksum.
- The sending UDP process attempts to send the packet to its peer UDP process on the receiving host. The application layer determines whether the receiving UDP process acknowledges the reception of the packet. UDP requires no notification of receipt. UDP does not use the three-way handshake.

Internet Layer: Where Packets Are Prepared for Delivery

- The transport protocols TCP, UDP, and SCTP pass their segments and packets down to the Internet layer, where the IP protocol handles the segments and packets. IP prepares them for delivery by formatting them into units called **IP datagrams**. IP then determines the IP addresses for the datagrams, so that they can be delivered effectively to the receiving host.

IP Datagrams

- IP attaches an **IP header** to the segment or packet's header, in addition to the information that is added by TCP or UDP. Information in the IP header includes the IP addresses of the sending and receiving hosts, the datagram length, and the datagram sequence order. This information is provided if the datagram exceeds the allowable byte size for network packets and must be fragmented.

Data-Link Layer: Where Framing Takes Place

- Data-link layer protocols, such as PPP, format the IP datagram into a **frame**. These protocols attach a third header and a footer to “frame” the datagram. The frame header includes a **cyclic redundancy check** (CRC) field that checks for errors as the frame travels over the network media. Then, the data-link layer passes the frame to the physical layer.

Physical Network Layer: Where Frames Are Sent and Received

- The physical network layer on the sending host receives the frames and converts the IP addresses into the hardware addresses appropriate to the network media. The physical network layer then sends the frame out over the network media.

How the Receiving Host Handles the Packet

- When the packet arrives on the receiving host, the packet travels through the TCP/IP protocol stack in the reverse order from which it was sent. Figure :Illustrates this path. Moreover, each protocol on the receiving host strips off header information that is attached to the packet by its peer on the sending host. The following process occurs:

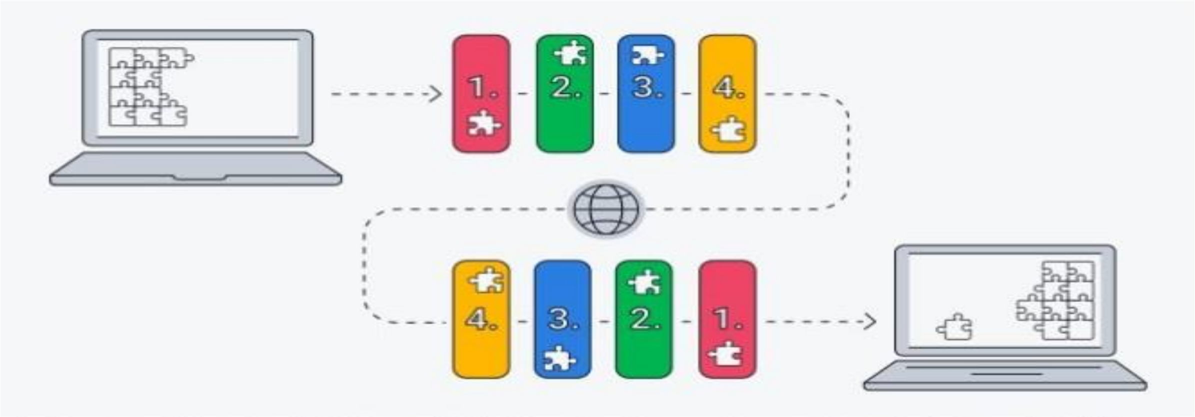
i) The physical network layer receives the packet in its frame form. The physical network layer computes the CRC of the packet, and then sends the frame to the data link layer.

ii) The data-link layer verifies that the CRC for the frame is correct and strips off the frame header and the CRC. Finally, the data-link protocol sends the frame to the Internet layer.

iii) The Internet layer reads information in the header to identify the transmission. Then, the Internet layer determines if the packet is a fragment. If the transmission is fragmented, IP reassembles the fragments into the original datagram. IP then strips off the IP header and passes the datagram on to transport layer protocols.

iv) The transport layer (TCP, SCTP, and UDP) reads the header to determine which application layer protocol must receive the data. Then, TCP, SCTP, or UDP strips off its related header. TCP, SCTP, or UDP sends the message or stream to the receiving application.

v) The application layer receives the message. The application layer then performs the operation that the sending host requested.



A diagram of how the TCP/IP model divides data into packets and sends it through 4 different layers.

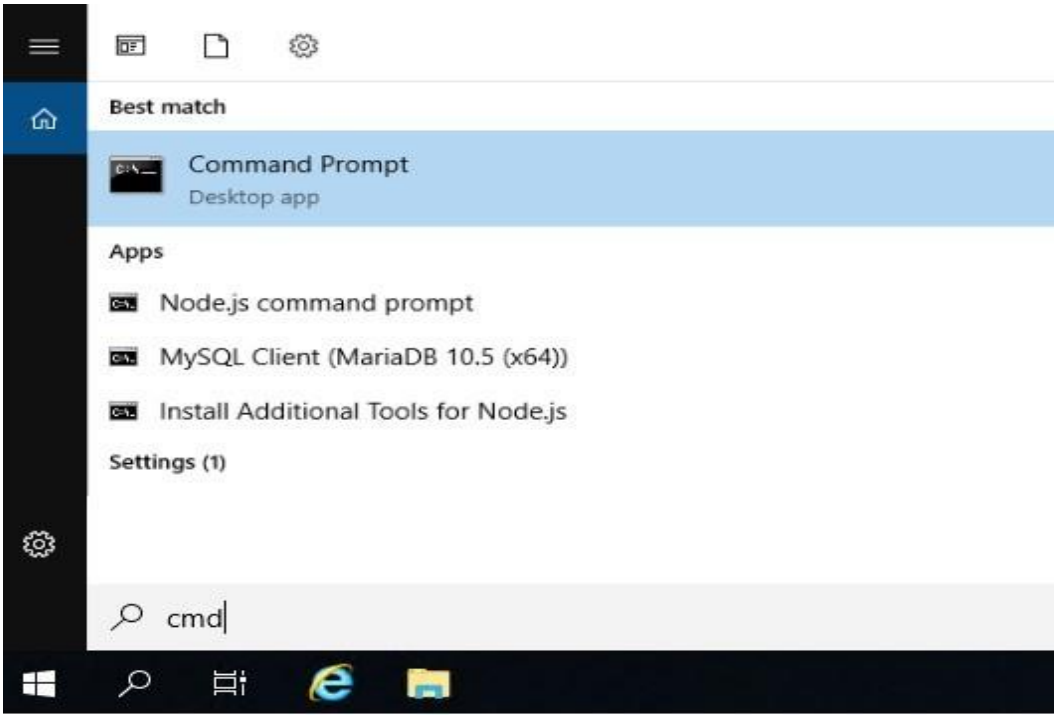
Expt.No: 09 Determine the IP Address Configuration of a Computer (Windows) and Test the Network Interface TCP/IP Stack (Ping).

- **I**nternet **p**rotocol **config**uration **(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**

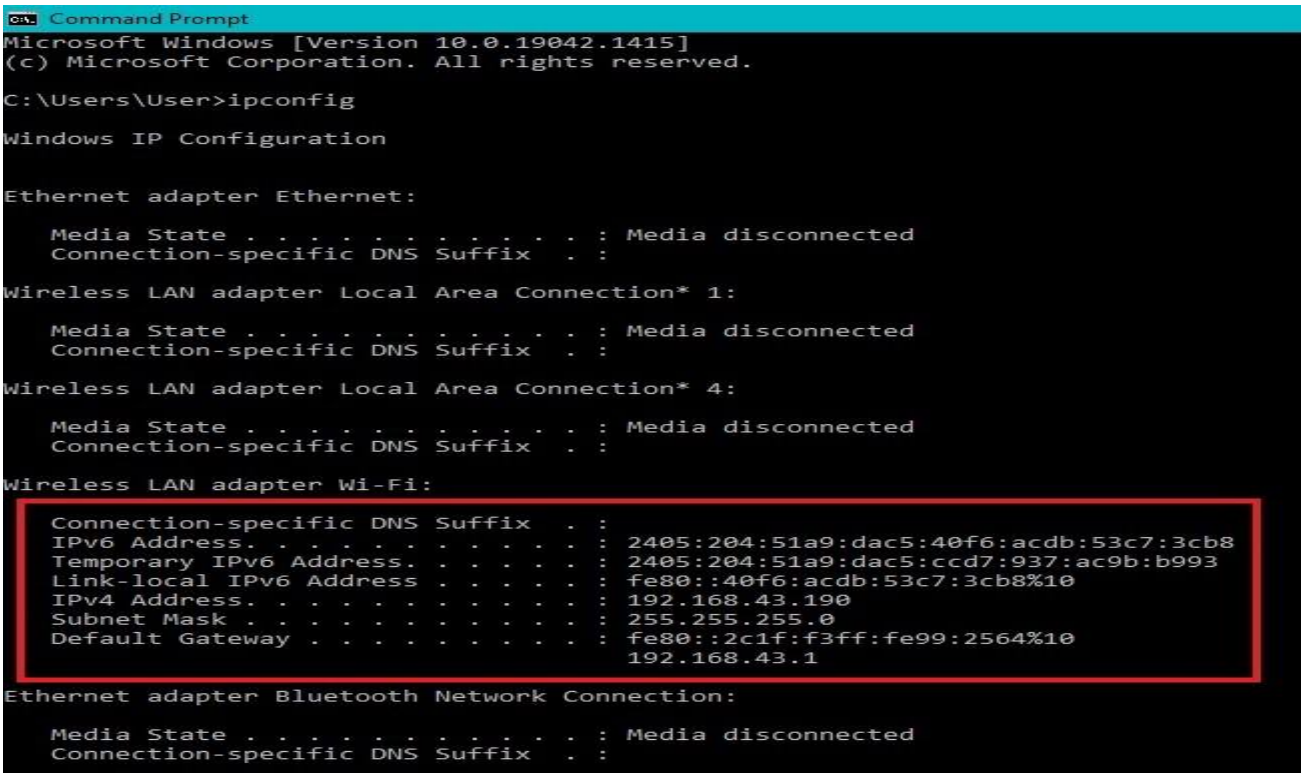
```
ipconfig [/parameter]
```

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.

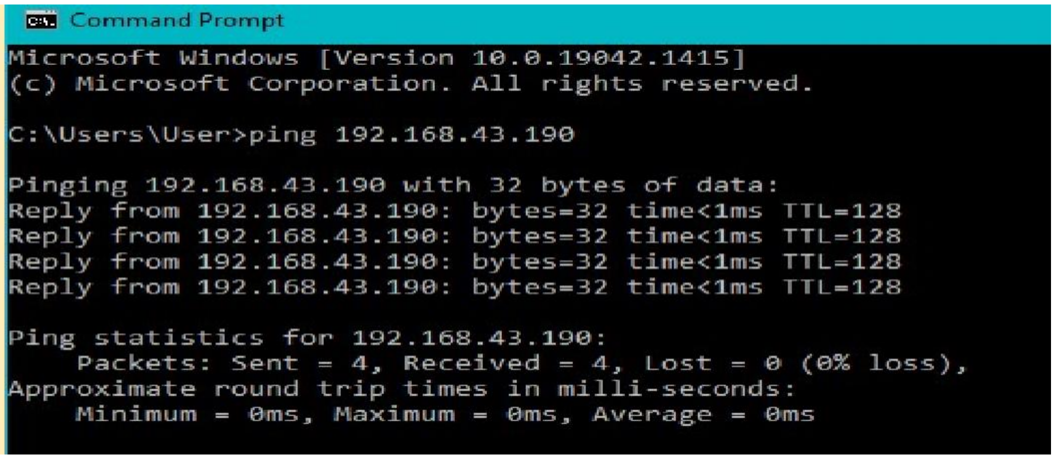


```
Command Prompt
Microsoft Windows [Version 10.0.19042.1415]
(c) Microsoft Corporation. All rights reserved.

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:



```
Command Prompt
Microsoft Windows [Version 10.0.19042.1415]
(c) Microsoft Corporation. All rights reserved.

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