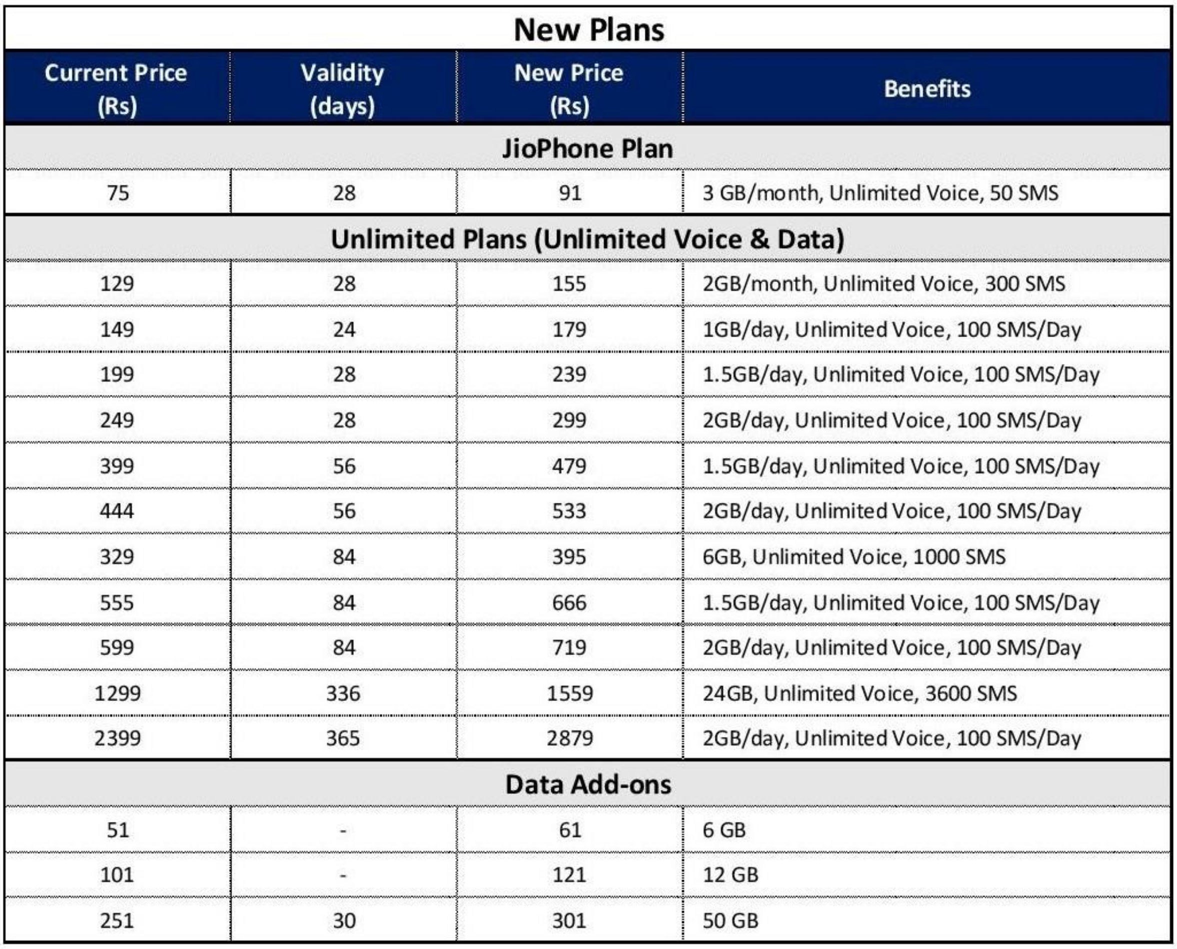
1) Explore all ISP in your area/locality and select best internet ISP/plan based on cost and performance.

An Internet service provider (ISP) is a company or an organization that lets your computer connect to the World Wide Web. It provides customers access to one or more high-speed Internet lines.

ISP across globe: **Xfinity , Version , AT& T , Spectrum , RCN , Cox , Mediacom, HughesNet , Frontier , CenturyLink ,Viasat , Suddenlink Internet .**

ISP in my locality , -Jio , jio fiber , airtel and airtel fibre , BSNL.

Jio plans



New Plans

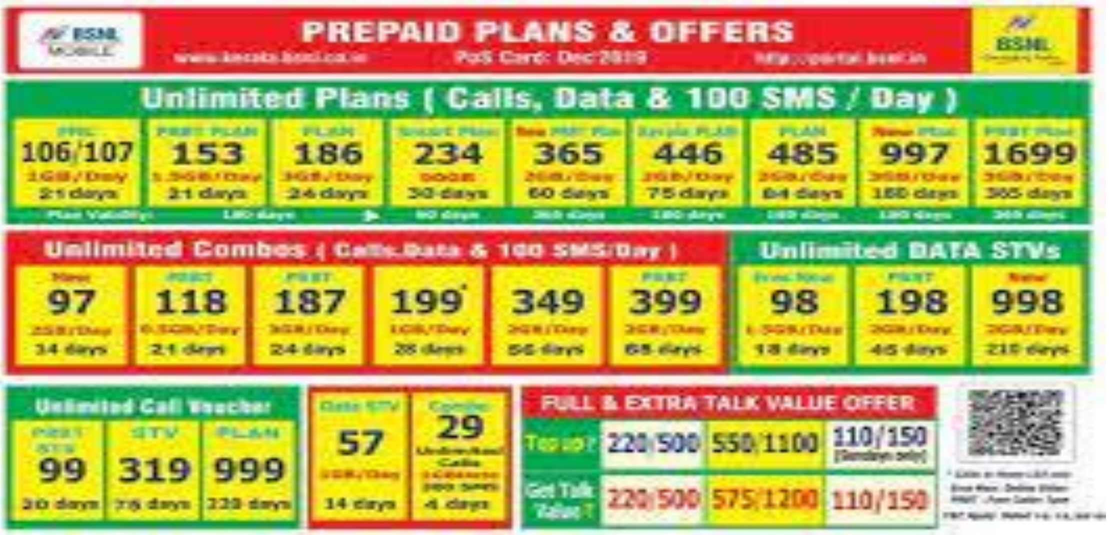
Current Price (Rs)	Validity (days)	New Price (Rs)	Benefits
JioPhone Plan			
75	28	91	3 GB/month, Unlimited Voice, 50 SMS
Unlimited Plans (Unlimited Voice & Data)			
129	28	155	2GB/month, Unlimited Voice, 300 SMS
149	24	179	1GB/day, Unlimited Voice, 100 SMS/Day
199	28	239	1.5GB/day, Unlimited Voice, 100 SMS/Day
249	28	299	2GB/day, Unlimited Voice, 100 SMS/Day
399	56	479	1.5GB/day, Unlimited Voice, 100 SMS/Day
444	56	533	2GB/day, Unlimited Voice, 100 SMS/Day
329	84	395	6GB, Unlimited Voice, 1000 SMS
555	84	666	1.5GB/day, Unlimited Voice, 100 SMS/Day
599	84	719	2GB/day, Unlimited Voice, 100 SMS/Day
1299	336	1559	24GB, Unlimited Voice, 3600 SMS
2399	365	2879	2GB/day, Unlimited Voice, 100 SMS/Day
Data Add-ons			
51	-	61	6 GB
101	-	121	12 GB
251	30	301	50 GB

Airtel plans

Airtel Plans 2021: List of prepaid plans, offers, price, data, validity

Recharge Plan	Data Benefit	Validity	Calling	SMS
Rs 19	200MB	2 Days	Unlimited	NIL
Rs 99	1GB	18 Days	Unlimited	100
Rs 129	1GB	24 Days	Unlimited	300
Rs 149	2GB	28 Days	Unlimited	300
Rs 179	2GB	28 Days	Unlimited	300
Rs 199	1GB per Day	24 Days	Unlimited	100/Day
Rs 219	1GB per Day	28 Days	Unlimited	100/Day
Rs 249	1.5GB per Day	28 Days	Unlimited	100/Day
Rs 279	1.5GB per Day	28 Days	Unlimited	100/Day
Rs 298	2GB per Day	28 Days	Unlimited	100/Day
Rs 349	2GB per Day	28 Days	Unlimited	100/Day
Rs 379	6GB	84 Days	Unlimited	900
Rs 398	3GB per Day	28 Days	Unlimited	100/Day
Rs 399	1.5GB per Day	56 Days	Unlimited	100/Day
Rs 449	2GB per Day	56 Days	Unlimited	100/Day
Rs 558	3GB per Day	56 Days	Unlimited	100/Day
Rs 598	1.5GB per Day	84 Days	Unlimited	100/Day
Rs 698	2GB per Day	84 Days	Unlimited	100/Day
Rs 1498	24GB	365 Days	Unlimited	3600
Rs 2398	1.5GB per Day	365 Days	Unlimited	100/Day

BSNL plans



PREPAID PLANS & OFFERS

www.kerala.bsnl.co.in PoS Card: Dec 2019 http://portal.bsnl.in

Unlimited Plans (Calls, Data & 100 SMS / Day)

106/107	153	186	234	365	446	485	997	1699
1GB/Day	1.5GB/Day	3GB/Day	[illegible]	2GB/Day	2GB/Day	2GB/Day	3GB/Day	3GB/Day
21 days	21 days	24 days	30 days	60 days	75 days	84 days	180 days	365 days

Unlimited Combos (Calls,Data & 100 SMS/Day)

97	118	187	199*	349	399
2GB/Day	0.5GB/Day	3GB/Day	1GB/Day	2GB/Day	2GB/Day
14 days	21 days	24 days	28 days	56 days	68 days

Unlimited DATA STVs

98	198	998
1.5GB/Day	2GB/Day	2GB/Day
18 days	45 days	210 days

Unlimited Call Voucher

99	319	999
20 days	75 days	220 days

Data STV	Combo
57	29
1GB/Day	Unlimited Calls
14 days	4 days

FULL & EXTRA TALK VALUE OFFER

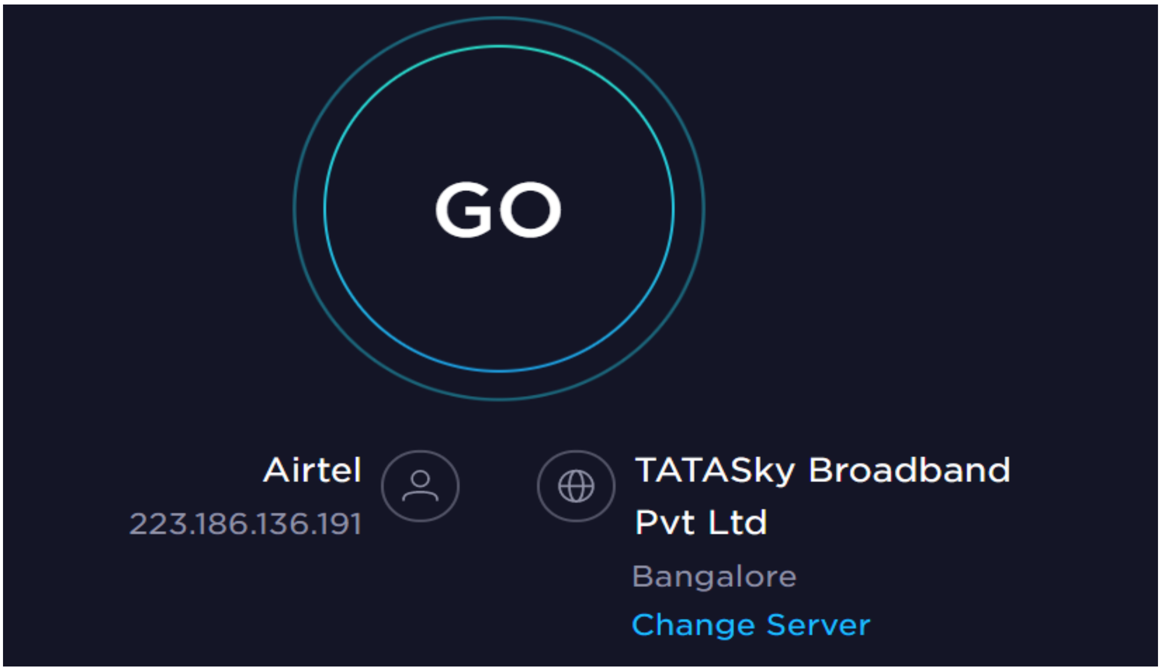
Top up?	220/500	550/1100	110/150 (Sundays only)
Get Talk Value?	220/500	575/1200	110/150

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

An internet speed test is a website or web application that measures a user’s internet connection speed. It reports on:

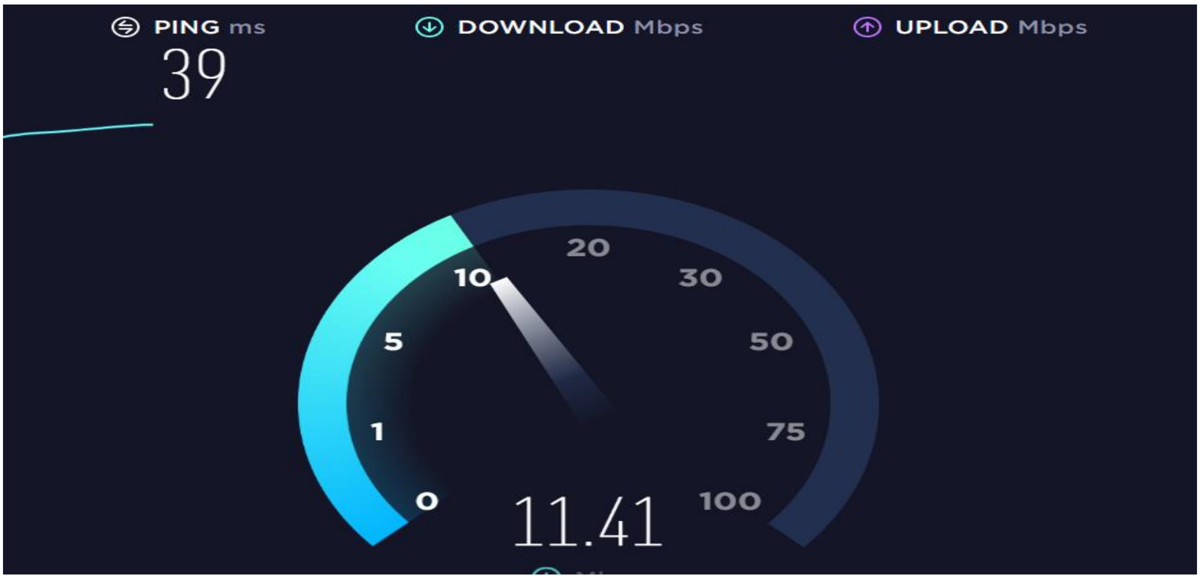
- Upload speed
- Download speed
- Bandwidth
- Ping
- Jitter
- Packet loss

An internet speed test is the process of analyzing broadband connection parameters by sending a small file from the server and measuring the time it takes to download and then upload the file back to the server. Along the way, parameters like jitter and packet loss can also be calculated. Some speed test hosts also measure ping, which is the time for a message to make a round trip from the sender to its destination and back, by sending an Internet Control Message Protocol (ICMP) echo request packet to the host.



Airtel
223.186.136.191

TATASky Broadband Pvt Ltd
Bangalore

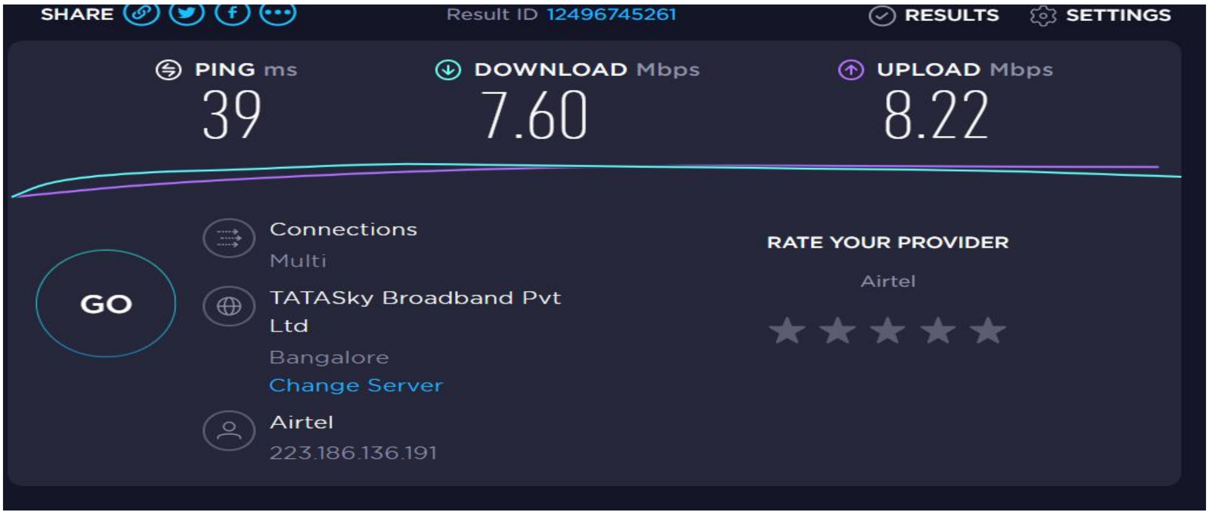


PING ms 39

DOWNLOAD Mbps

UPLOAD Mbps

11.41



Result ID 12496745261

PING ms 39

DOWNLOAD Mbps 7.60

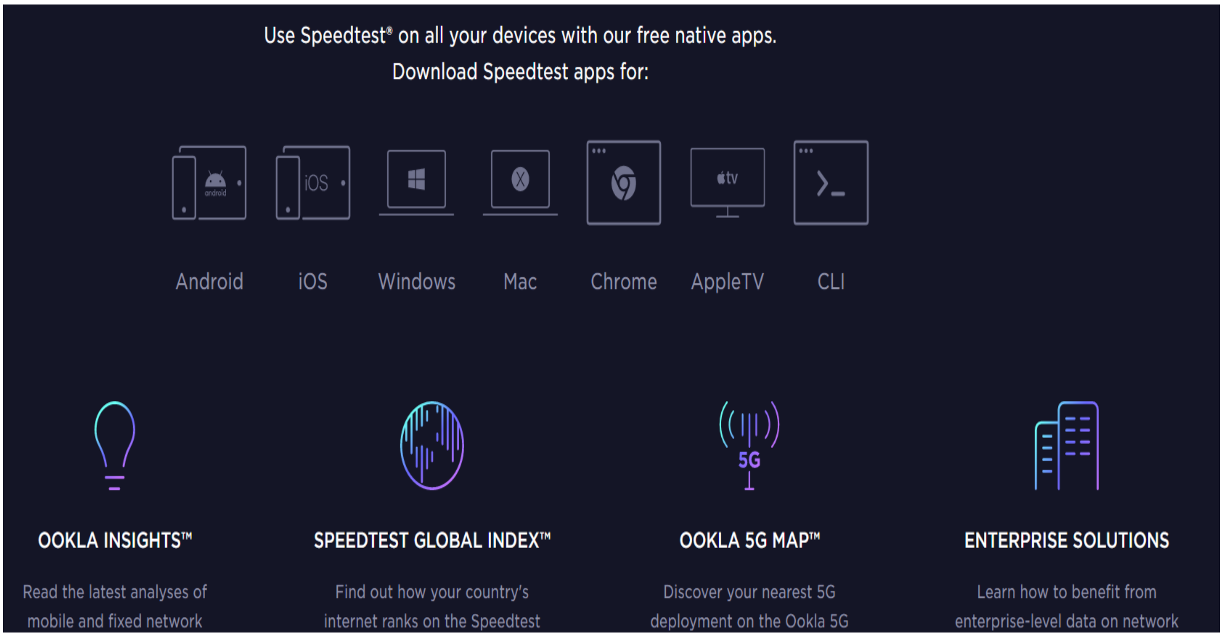
UPLOAD Mbps 8.22

Connections
Multi

TATASky Broadband Pvt Ltd
Bangalore
Change Server

Airtel
223.186.136.191

RATE YOUR PROVIDER
Airtel
★ ★ ★ ★ ★



Use Speedtest® on all your devices with our free native apps.
Download Speedtest apps for:

OOKLA INSIGHTS™
Read the latest analyses of mobile and fixed network

SPEEDTEST GLOBAL INDEX™
Find out how your country's internet ranks on the Speedtest

OOKLA 5G MAP™
Discover your nearest 5G deployment on the Ookla 5G

ENTERPRISE SOLUTIONS
Learn how to benefit from enterprise-level data on network

3. Explore Bluethooth, Wifi, NFC in your smartphone and note their key technical attributes (Radio spectrum band, range, pathloss, throughput, mode etc).

Bluetooth is **a short-range wireless technology standard** that is used for exchanging data between fixed and mobile devices over short distances using UHF radio waves in the ISM bands, from 2.402 GHz to 2.48 GHz, and building personal area networks (PANs).

Bluetooth works by using radio frequencies, rather than the infrared spectrum used by traditional remote controls. As a result, Bluetooth eliminates the need not only for a wire connection but also for maintaining a clear line of sight to communicate between devices.

WIFI

Wi-Fi is similar to Bluetooth in that it also uses radio waves for high-speed data transfer over short distances without the need for a wire connection. Wi-Fi works by breaking a signal into pieces and transmitting those fragments over multiple radio frequencies. This technique enables the signal to be transmitted at a lower power per frequency and also allows multiple devices to use the same Wi-Fi transmitter.

NFC

Near Field Communication (NFC) is a standards-based short-range wireless connectivity technology that makes life easier. NFC is a method of **wireless data transfer** that allows smartphones, laptops, tablets, and other devices to share data when in close proximity. NFC technology powers contactless payments via mobile wallets like Apple Pay, Android Pay, as well as contactless cards.

NFC tends to be more secure than Bluetooth, as it operates on a shorter range allowing for a more stable connection. Therefore, NFC tends to be a better solution for crowded and busy places, where a lot of different devices are trying to communicate with each other, creating signal interference.

WIFI Range

Wi-Fi IEEE 802.11 is used by very many devices from smartphones to laptops and tablets to remote sensors, actuators televisions and many more. It is used as the main wireless communications bearer in wireless LANs as well as for small home WLANs as well.

There are several frequency bands within the radio spectrum that are used for the Wi-Fi and within these there are many channels that have been designated with numbers so they can be identified.

Although many Wi-Fi channels and Wi-Fi bands are normally selected automatically by home Wi-FI routers, for larger wireless LANs and systems it is often necessary to plan the frequencies used. Using many Wi-Fi access points around a large building or area, frequency planning is essential so that the best performance can be obtained from the wireless LAN.

Range of Bluetooth

The range of Bluetooth connection is approximately 30 feet. However, maximum communication range will vary depending on obstacles or electromagnetic environment.

Throughput of WiFi :

That's the measurement of data rate between network devices within your home or small business network, also referred to as your LAN (Local Area Network—different from your Internet bandwidth, or WAN (Wide Area Network) connection speed.

With the 802.11n standard, Wi-Fi became even faster and more reliable. It supported a maximum theoretical transfer rate of **300 Mbps.**

Throughput of Bluetooth :

data throughput represent the maximum amount of data that can be transferred between two applications in a given time.

Protocol	Event length	Method	Maximum data throughput
GATT Client	2.5 ms	Receive Notification	16.0 kbps
		Send Write command	16.0 kbps
		Send Write request	4.0 kbps
		Simultaneous receive Notification and send Write command	8.0 kbps (each direction)
Gatt Server	2.5 ms	Send Notification	16.0 kbps
		Receive Write command	16.0 kbps
		Receive Write request	4.0 kbps
		Simultaneous send Notification and receive Write command	8.0 kbps (each direction)

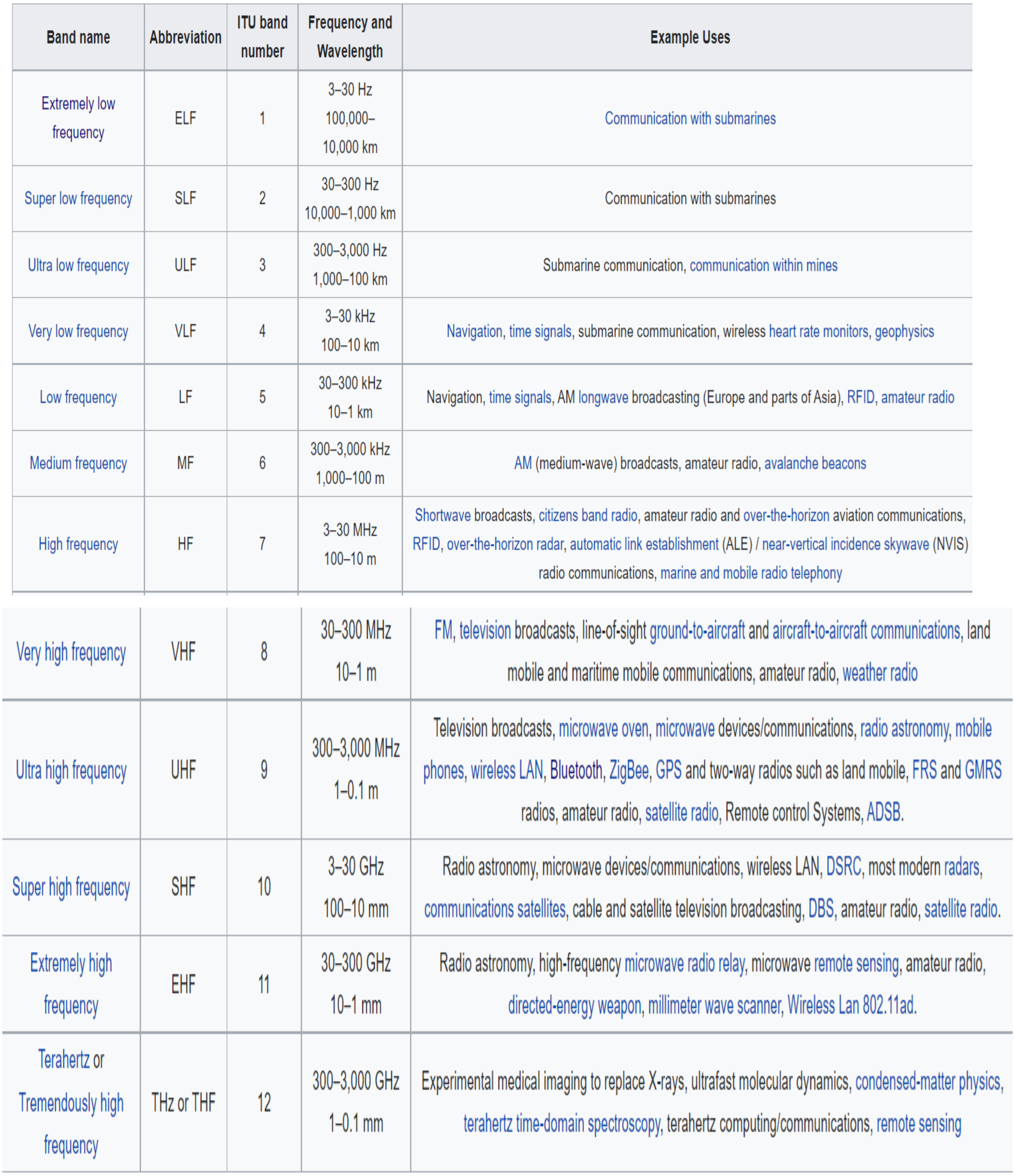
NFC throughput :

NFC operates in unlicensed ISM frequency band of about 13.56 MHz. It supports data rate of **106 Kbps , 212 kbps and 424 Kbps**. NFC uses bandwidth of 14KHz to map data on the RF carrier.

Radio spectrum

The **radio spectrum** is the part of the electromagnetic spectrum with frequencies from 30 Hz to 300 GHz. Electromagnetic waves in this frequency range, called *radio waves*, are widely used in modern technology, particularly in telecommunication. To prevent interference between different users, the generation and transmission of radio waves is strictly regulated by national laws, coordinated by an international body, the International Telecommunication Union (ITU).

A **radio band** is a small contiguous section of the radio spectrum frequencies, in which channels are usually used or set aside for the same purpose. To prevent interference and allow for efficient use of the radio spectrum, similar services are allocated in bands. For example, broadcasting, mobile radio, or navigation devices, will be allocated in non-overlapping ranges of frequencies.



Band name	Abbreviation	ITU band number	Frequency and Wavelength	Example Uses
Extremely low frequency	ELF	1	3–30 Hz 100,000–10,000 km	Communication with submarines
Super low frequency	SLF	2	30–300 Hz 10,000–1,000 km	Communication with submarines
Ultra low frequency	ULF	3	300–3,000 Hz 1,000–100 km	Submarine communication, communication within mines
Very low frequency	VLF	4	3–30 kHz 100–10 km	Navigation, time signals, submarine communication, wireless heart rate monitors, geophysics
Low frequency	LF	5	30–300 kHz 10–1 km	Navigation, time signals, AM longwave broadcasting (Europe and parts of Asia), RFID, amateur radio
Medium frequency	MF	6	300–3,000 kHz 1,000–100 m	AM (medium-wave) broadcasts, amateur radio, avalanche beacons
High frequency	HF	7	3–30 MHz 100–10 m	Shortwave broadcasts, citizens band radio, amateur radio and over-the-horizon aviation communications, RFID, over-the-horizon radar, automatic link establishment (ALE) / near-vertical incidence skywave (NVIS) radio communications, marine and mobile radio telephony
Very high frequency	VHF	8	30–300 MHz 10–1 m	FM, television broadcasts, line-of-sight ground-to-aircraft and aircraft-to-aircraft communications, land mobile and maritime mobile communications, amateur radio, weather radio
Ultra high frequency	UHF	9	300–3,000 MHz 1–0.1 m	Television broadcasts, microwave oven, microwave devices/communications, radio astronomy, mobile phones, wireless LAN, Bluetooth, ZigBee, GPS and two-way radios such as land mobile, FRS and GMRS radios, amateur radio, satellite radio, Remote control Systems, ADSB.
Super high frequency	SHF	10	3–30 GHz 100–10 mm	Radio astronomy, microwave devices/communications, wireless LAN, DSRC, most modern radars, communications satellites, cable and satellite television broadcasting, DBS, amateur radio, satellite radio.
Extremely high frequency	EHF	11	30–300 GHz 10–1 mm	Radio astronomy, high-frequency microwave radio relay, microwave remote sensing, amateur radio, directed-energy weapon, millimeter wave scanner, Wireless Lan 802.11ad.
Terahertz or Tremendously high frequency	THz or THF	12	300–3,000 GHz 1–0.1 mm	Experimental medical imaging to replace X-rays, ultrafast molecular dynamics, condensed-matter physics, terahertz time-domain spectroscopy, terahertz computing/communications, remote sensing

Different modes of WiFi :

The two modes of Wifi are Infrastructure and ad hoc network.

Wireless networks can operate in one of two modes: infrastructure or ad hoc.

In *infrastructure* mode, all devices on a wireless network communicate with each other through an access point (wireless router).

(Infrastructure wireless network is **the wireless network that contains wireless router/access point and enables other computers connect to it wirelessly**. This is the common deployment to build a home wireless network.)

In *ad hoc* mode, a computer with a wireless network adapter communicates directly with a printer equipped with a wireless print server.

	Infrastructure	**Ad hoc**
Characteristics		
Communication	Through an access point	Directly between devices
Security	More security options	WEP or no security
Range	Determined by the range and number of access points	Restricted to the range of individual devices on the network
Speed	Usually faster	Usually slower
Requirements for all devices		
Unique IP address for each device	Yes	Yes
Mode set to	Infrastructure mode	Ad hoc mode
Same SSID	Yes, including the access point	Yes
Same channel	Yes, including the access point	Yes

Infrastructure mode provides:

- Increased network security
- Increased reliability
- Faster performance
- Easier setup

Modes of operation for Bluetooth:

1. SNIFF, HOLD and PARK modes of operation: These are the three power saving modes of operation for Bluetooth devices which are connected to a piconet. These modes are used when no data is to be transmitted.

i. SNIFF mode:

- The slave device listens to the piconet in this mode, but at a reduced rate. Thus reducing its duty cycle.
- The SNIFF interval is programmable and depends on application.

ii. HOLD mode:

- The master unit can put a slave unit into HOLD mode or a slave unit can demand to be put into HOLD mode.
- Data transfer restarts instantly when units transition out of HOLD mode.
- The HOLD is used when connecting several piconets or managing a low-power device such as temperature sensor.

iii. PARK mode:

- The device is still synchronized to the piconet but does not participate in traffic.

PARKED devices have given up their MAC address and occasionally listen to the traffic of the master to resynchronize and check on broadcast messages. In the increasing order of power efficiency, the SNIFF mode has higher duty cycle, followed by HOLD mode with a lower duty cycle, and PARK mode with lowest duty cycle.

Modes of operation for NFC :

NFC devices are unique in that they support **four modes of operation: reader/writer, peer-to-peer, card emulation and wireless charging.**

- In reader/writer mode, the NFC device is capable of reading NFC Forum-mandated tag types, such as a tag embedded in an NFC smart poster. The reader/writer mode on the RF interface is compliant with the ISO 14443 and FeliCa schemes.
- In Peer-to-Peer mode, two NFC devices can exchange data. For example, you can share Bluetooth or WiFi link set-up parameters or you can exchange data such as virtual business cards or digital photos. Peer-to-Peer mode is standardized on the ISO/IEC 18092 standard.
- In Card Emulation mode, the NFC device appears to an external reader much the same as a traditional contactless smart card. This enables contactless payments and ticketing by NFC devices without changing the existing infrastructure.
- In Wireless Charging mode, small IoT devices such as a Bluetooth headset, fitness tracker or smartwatch can be charged with the contact-less transfer of up to1 W of power.

4. How To Fix Wireless Interference with Wi-Fi and Bluetooth

Bluetooth devices suffer their fair share of problems. These issues can be frustrating, especially when you rely on your gadgets to provide a quality connection. Below, we'll discuss how to reduce Bluetooth and Wi-Fi interference.

Interference with Other Devices

Bluetooth technology makes our lives easier, but it doesn't always work as seamlessly as we'd like. Often, Bluetooth gadgets interfere with other devices – especially those that use the same frequency.

Interference can take many forms, making it that much more difficult to determine the source of the problem. The following are among the most common sources of interference:

- Wi-Fi
- Phones with a Processing Speed of 2.4 and 5 GHz
- Satellite Dishes
- Microwaves
- Wireless Speakers
- Baby Monitors

Solutions for Interference

In theory, interference should be rare, as the frequency for most devices is fairly weak. Unfortunately, this phenomenon still occurs regularly. Because a myriad of causes can be at play, it helps to follow a detailed troubleshooting process before declaring the situation hopeless. The following suggestions may help:

- Move Bluetooth devices away from building materials that act as barriers. These include metal, concrete, plaster, and brick.
- Avoid placing Bluetooth gadgets near microwaves or fluorescent lights. These use the same frequency as Bluetooth devices and are therefore best avoided.
- Reboot your router and try a different channel. Depending on your router, channel surfing may occur automatically – or manual selection may be required. If possible, try multiple channels to determine if a particular option is a better fit.
- Move devices closer to your router. By altering your device's placement, you could dramatically improve the strength of your Wi-Fi connection.

5) How to Troubleshoot Bluetooth Issues on Windows

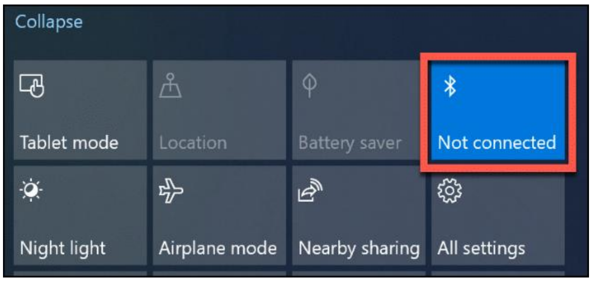
Basic Bluetooth Troubleshooting Steps

Check That Bluetooth Is Turned On

Start by making sure Bluetooth is actually enabled on your Windows PC. Just because the symbol is in the taskbar doesn't mean your Bluetooth radio is actually turned on.

Restart Your Bluetooth Radio

on.



If Bluetooth is enabled, switching it off and on again might resolve some underlying issues of which you're unaware.

To do this, click the notification icon in your Windows taskbar to access your quick settings. Click the "Bluetooth" tile to turn it off. Once it goes gray, click it again to turn it back on.

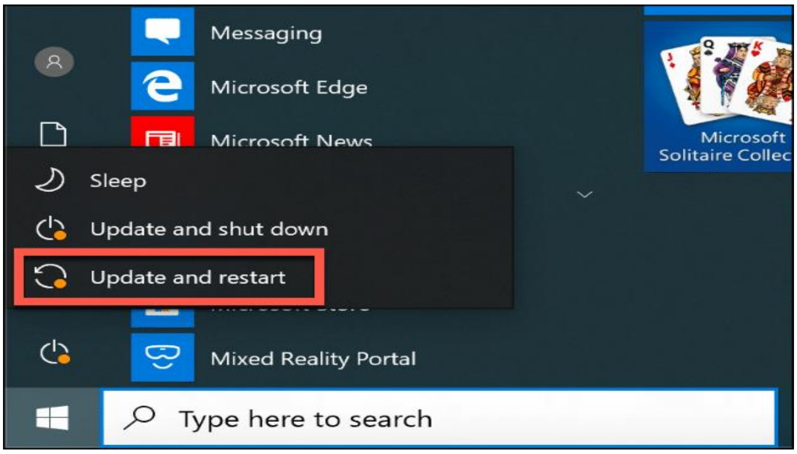
Check the Battery

If you aren't keeping track of the battery level on your Bluetooth device, you might not even be aware when it runs out of power.

Before you try a more serious solution, you might want to replace the batteries in your Bluetooth device or charge it, and then try it again.

Restart Your PC

The best fixes are sometimes the easiest, and if you haven't tried it already, give your PC a quick restart.



When you reboot your PC, you wipe the slate clean, and clear out any idle processes or memory leaks. It's not a miracle fix, but it can rectify some issues with the hardware, so give it a go.

Check Bluetooth Interference and Device Distance

Bluetooth devices communicate wirelessly via radio waves. Just like a Wi-Fi network, interference can affect Bluetooth connections. Other radio signals, physical obstacles (like thick walls), and devices like microwaves can all block or degrade a Bluetooth connection.

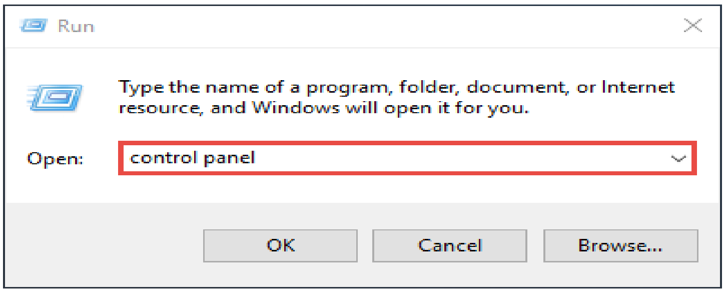
Take a moment to survey the area. How far away is your Bluetooth device from your PC? The bigger the distance, the weaker the signal.

Move your device closer to your PC and see if it impacts the Bluetooth connectivity. If not, try (if possible) to use your Bluetooth device in another location. You can also use third-party apps, like the Bennett Bluetooth Monitor, to check your Bluetooth's signal strength.

6. How to find and manually assign an IP address on Windows 10?

Step 1: Open the Control Panel

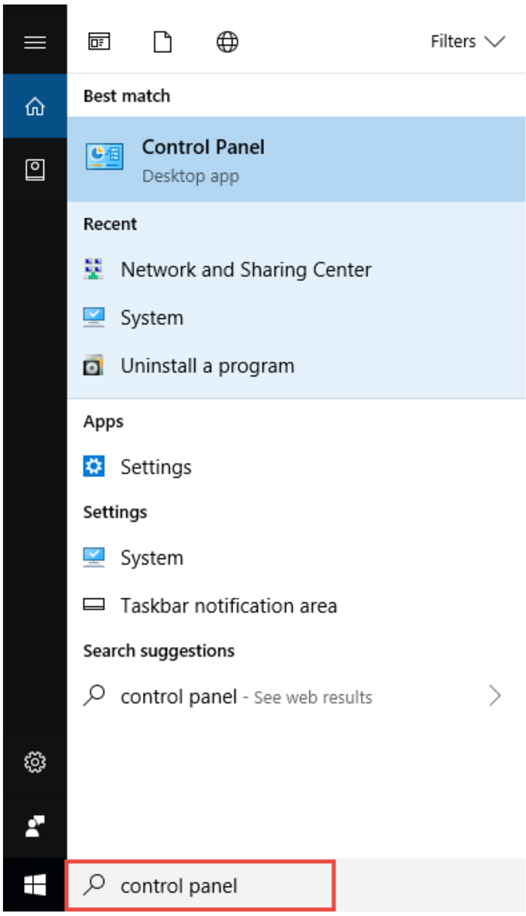
Press "**Windows** + **R**", then a **Run** box comes out. Input **control panel** and press **Enter** to open the control panel.



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

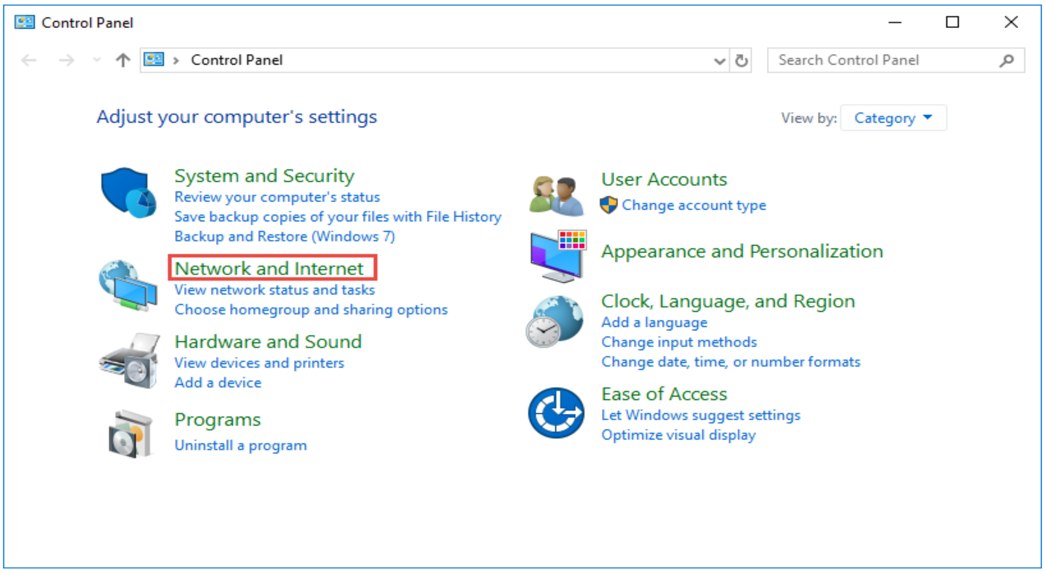
Open: control panel

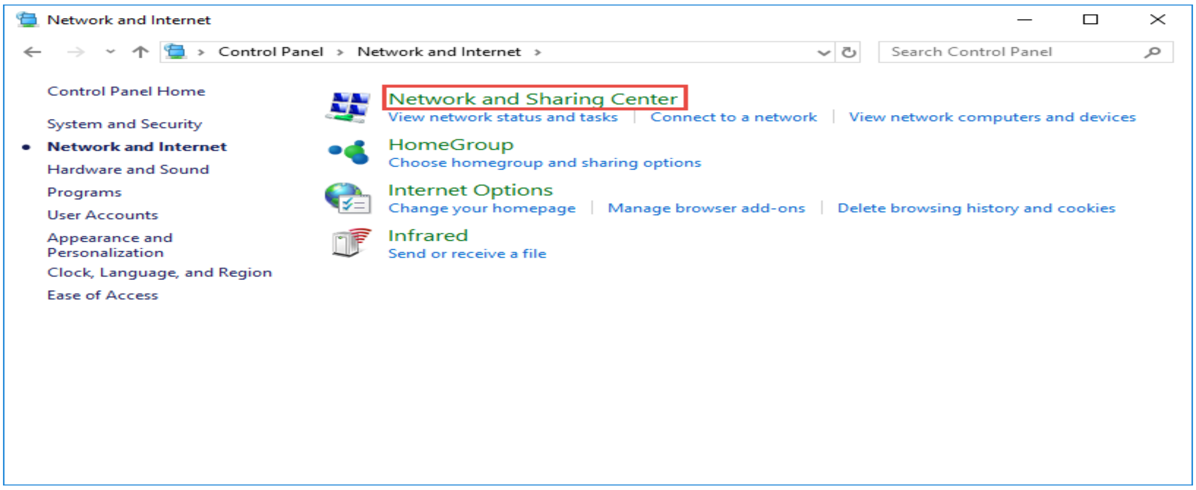
You can also type **control panel** in the search bar at the lower left of the screen and press **Enter** to open the control panel.



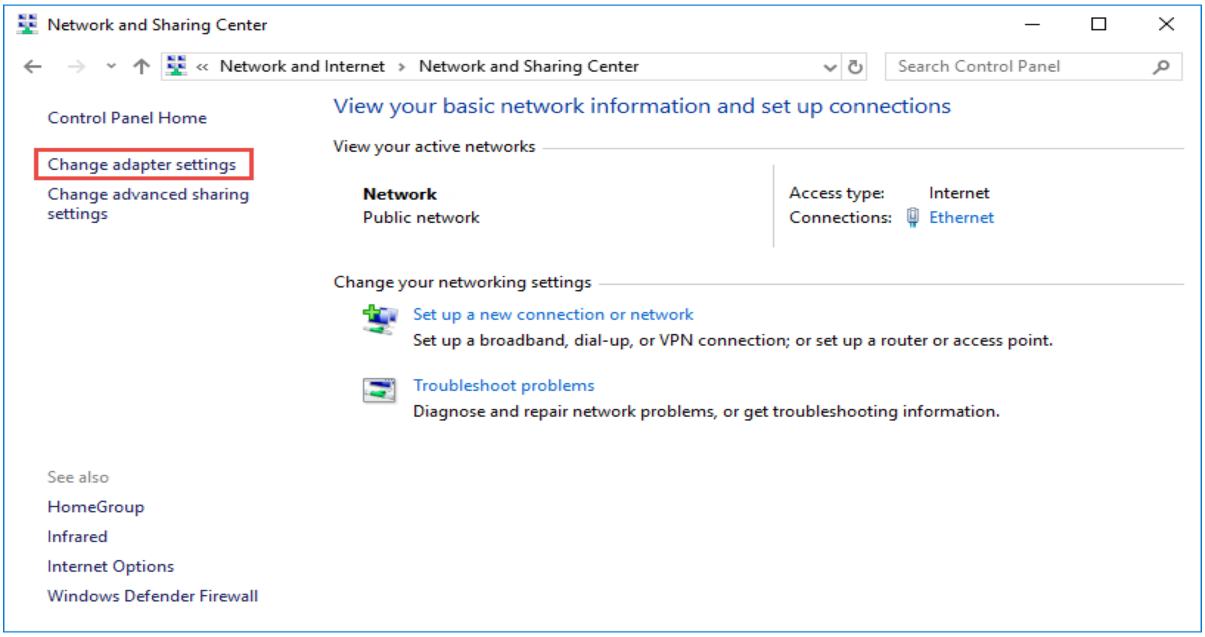
Step 2: Go to Network Connections

Go to **Network and Internet** > **Network and Sharing Center**.


Control Panel
Control Panel
Search Control Panel
Adjust your computer's settings
View by: Category
System and Security
Review your computer's status
Save backup copies of your files with File History
Backup and Restore (Windows 7)
Network and Internet
View network status and tasks
Choose homegroup and sharing options
Hardware and Sound
View devices and printers
Add a device
Programs
Uninstall a program
User Accounts
Change account type
Appearance and Personalization
Clock, Language, and Region
Add a language
Change input methods
Change date, time, or number formats
Ease of Access
Let Windows suggest settings
Optimize visual display



Select **Change adapter settings** on the left.


Network and Sharing Center
« Network and Internet > Network and Sharing Center
Search Control Panel
Control Panel Home
Change adapter settings
Change advanced sharing settings
See also
HomeGroup
Infrared
Internet Options
Windows Defender Firewall
View your basic network information and set up connections
View your active networks
Change your networking settings
Set up a new connection or network
Troubleshoot problems

Network
Public network

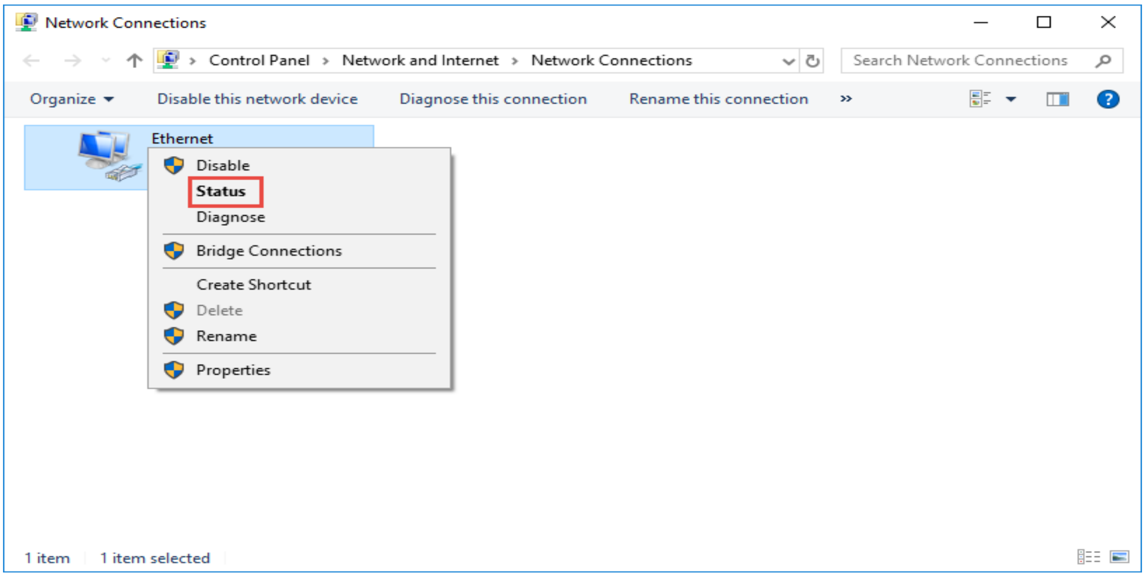
Access type: Internet
Connections: Ethernet

Set up a broadband, dial-up, or VPN connection; or set up a router or access point.

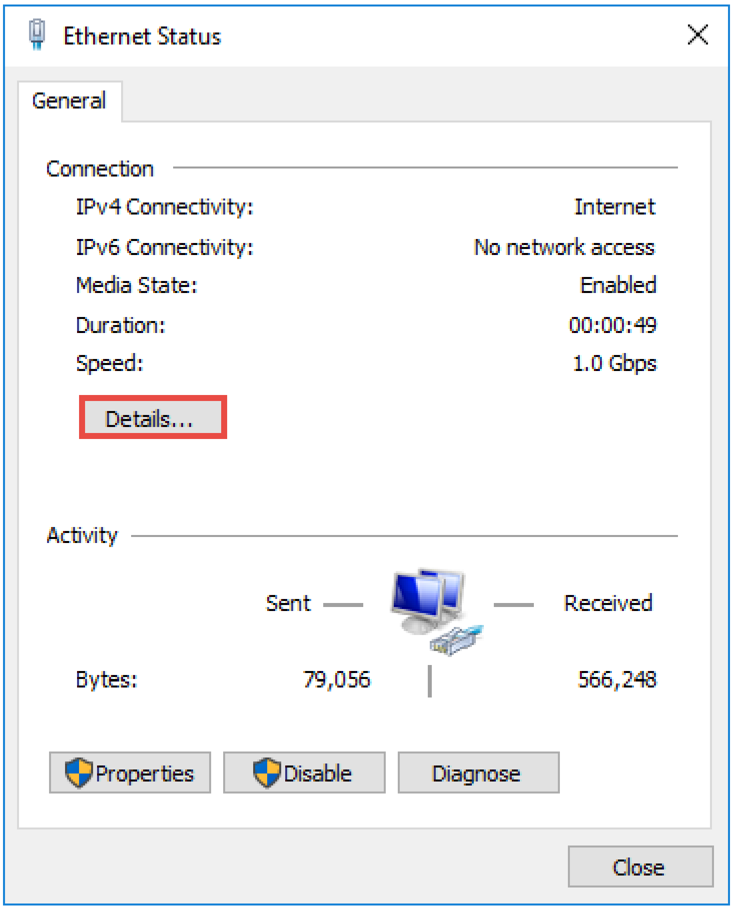
Diagnose and repair network problems, or get troubleshooting information.

Step 3: Find the IP address

Right click the **Ethernet** icon and select **Status** from the context menu.



Then click **Details...** to view all detailed information of network connection.



Connection

IPv4 Connectivity: Internet

IPv6 Connectivity: No network access

Media State: Enabled

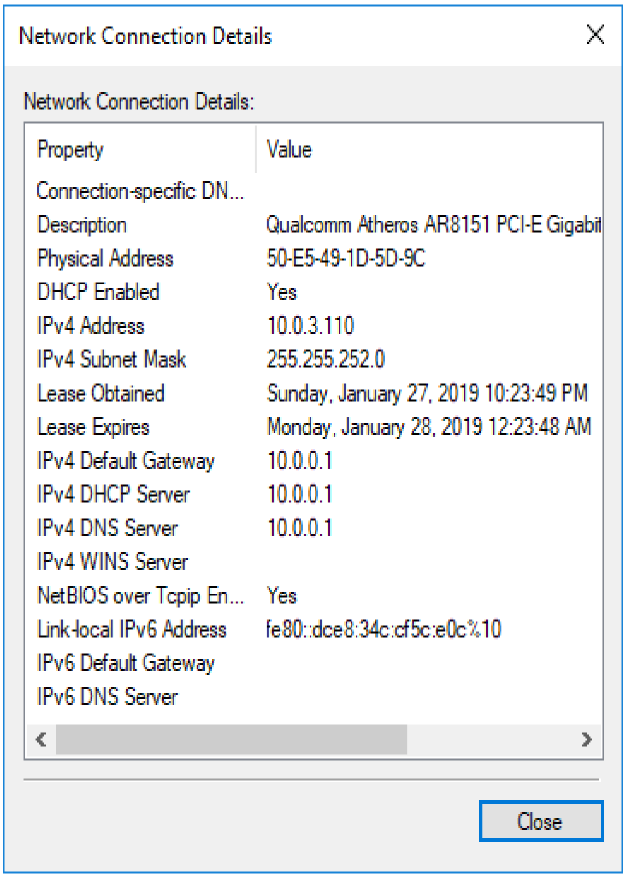
Duration: 00:00:49

Speed: 1.0 Gbps

Activity

Sent — Received

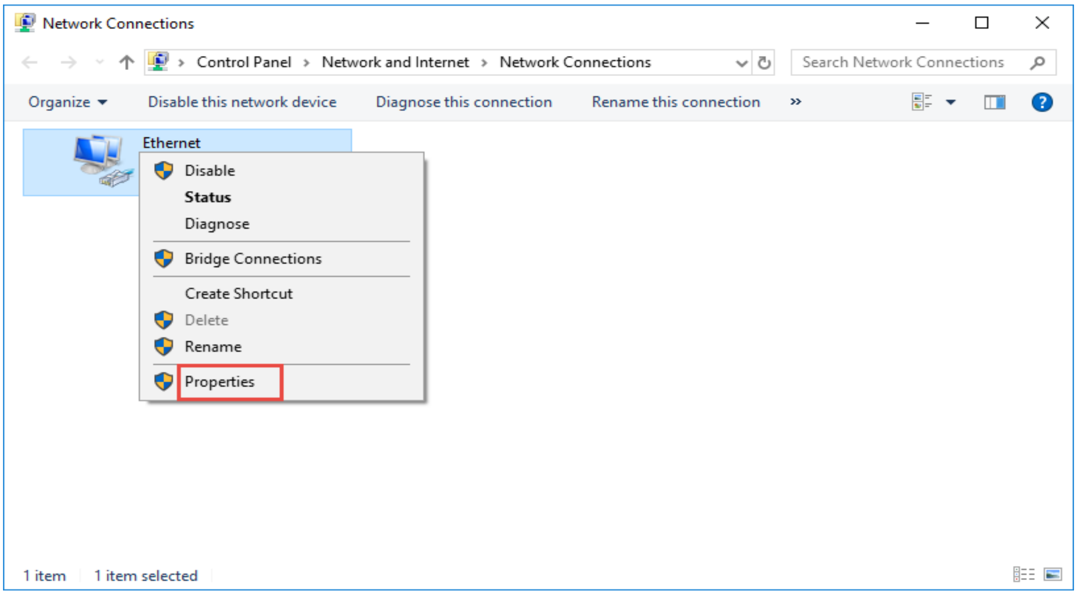
Bytes: 79,056 | 566,248



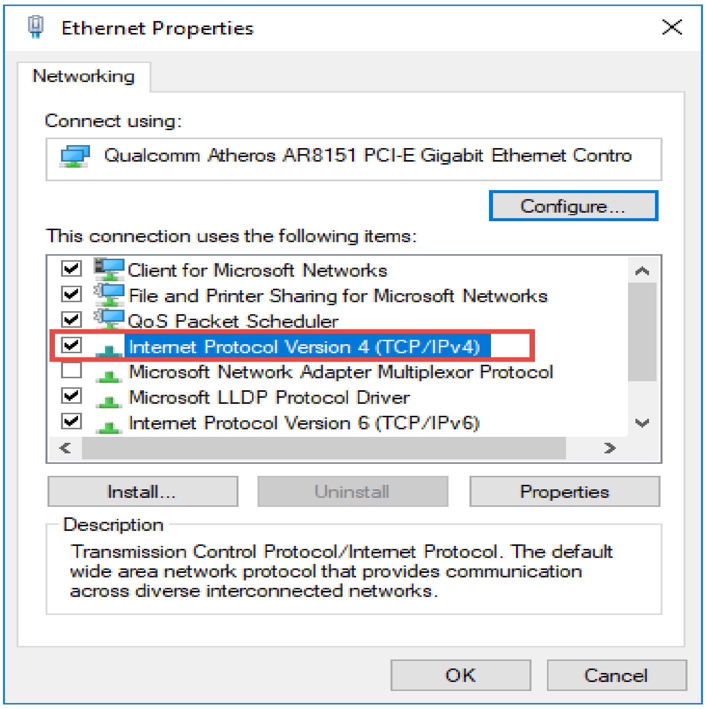
Property	Value
Connection-specific DN...	
Description	Qualcomm Atheros AR8151 PCI-E Gigabit
Physical Address	50-E5-49-1D-5D-9C
DHCP Enabled	Yes
IPv4 Address	10.0.3.110
IPv4 Subnet Mask	255.255.252.0
Lease Obtained	Sunday, January 27, 2019 10:23:49 PM
Lease Expires	Monday, January 28, 2019 12:23:48 AM
IPv4 Default Gateway	10.0.0.1
IPv4 DHCP Server	10.0.0.1
IPv4 DNS Server	10.0.0.1
IPv4 WINS Server	
NetBIOS over Tcpip En...	Yes
Link-local IPv6 Address	fe80::dce8:34c:cf5c:e0c%10
IPv6 Default Gateway	
IPv6 DNS Server	

Step 4: Set the IP address

Right Click **Local Area Connection** and select **Properties**.



Then double click **Internet Protocol Version 4 (TCP/IPv4)**.



Connect using:

Qualcomm Atheros AR8151 PCI-E Gigabit Ethernet Contro

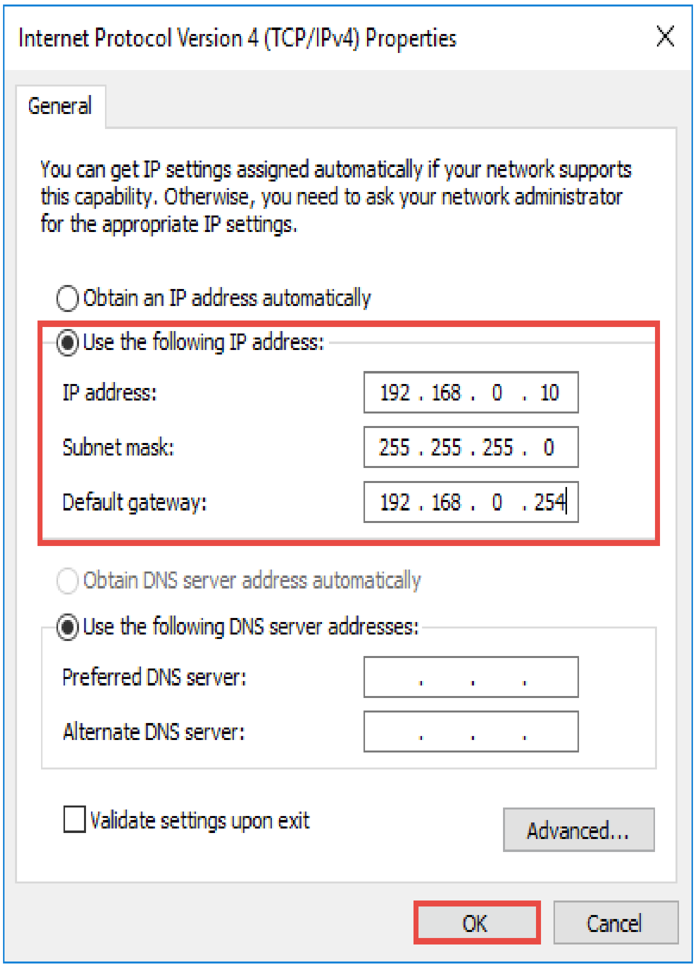
This connection uses the following items:

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

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

Select Use the Following IP address: and type in the IP address, Subnet mask and Default gateway. Click OK to apply the settings.



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 . 0 . 10
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	192 . 168 . 0 . 254

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server:	. . .
Alternate DNS server:	. . .

□ Validate settings upon exit

7. Determine the MAC Address of a Host.

Every computer on an Ethernet local network has a Media Access Control (MAC) address that is burned into the Network Interface Card (NIC). Computer MAC addresses are usually displayed as 6 sets of two hexadecimal numbers separated by dashes or colons (example: 15-EF-A3-45-9B-57). The ipconfig /all command displays the computer MAC address.

Step 1: Display information for the command ipconfig / all

1. Right-click on the **Start** button and select **Command Prompt**.
2. Enter the ipconfig /all command at the command prompt.

Step 2: Locate the MAC (physical) address(es) in the output from the ipconfig /all command

Use the table below to fill in the description of the Ethernet adapter and the Physical (MAC) Address:

Description	Physical Address
Example Answer: Intel(R) Ethernet Connection I219-LM	Example Answer:54-EE-75-C3-2B-33

How many MAC addresses did you discover in your PC ?

Answers will vary depending on the setup of the PC.

Part 2: Analyzing the Parts of a MAC Address

Every Ethernet network interface has a physical address assigned to it when it is manufactured. These addresses are 48 bit (6 bytes) long and are written in hexadecimal notation. MAC addresses are made up of two parts. One part of the MAC address, the first 3 bytes, represents the vendor who manufactured the network interface. This part of the MAC is called the OUI (Organizationally Unique Identifier). Each vendor who wants to make and sell Ethernet network interfaces must register with the IEEE in order to be assigned an OUI .

The second part of the address, the remaining 3 bytes are the unique ID for the interface. All MAC addresses that begin with the same OUI must have unique values in the last 3 bytes.

In this example, the physical MAC address for the Ethernet LAN interface is D4-BE-D9-13-63-00.

Manufacturer OUI	Unique Identifier for the Interface	Vendor Name
D4-BE-D9	13-63-00	Dell Incorporated

8. Identify the NIC types in the PC that you are using. How do you explore different ways to extract information about these NICs and how to activate and deactivate them.

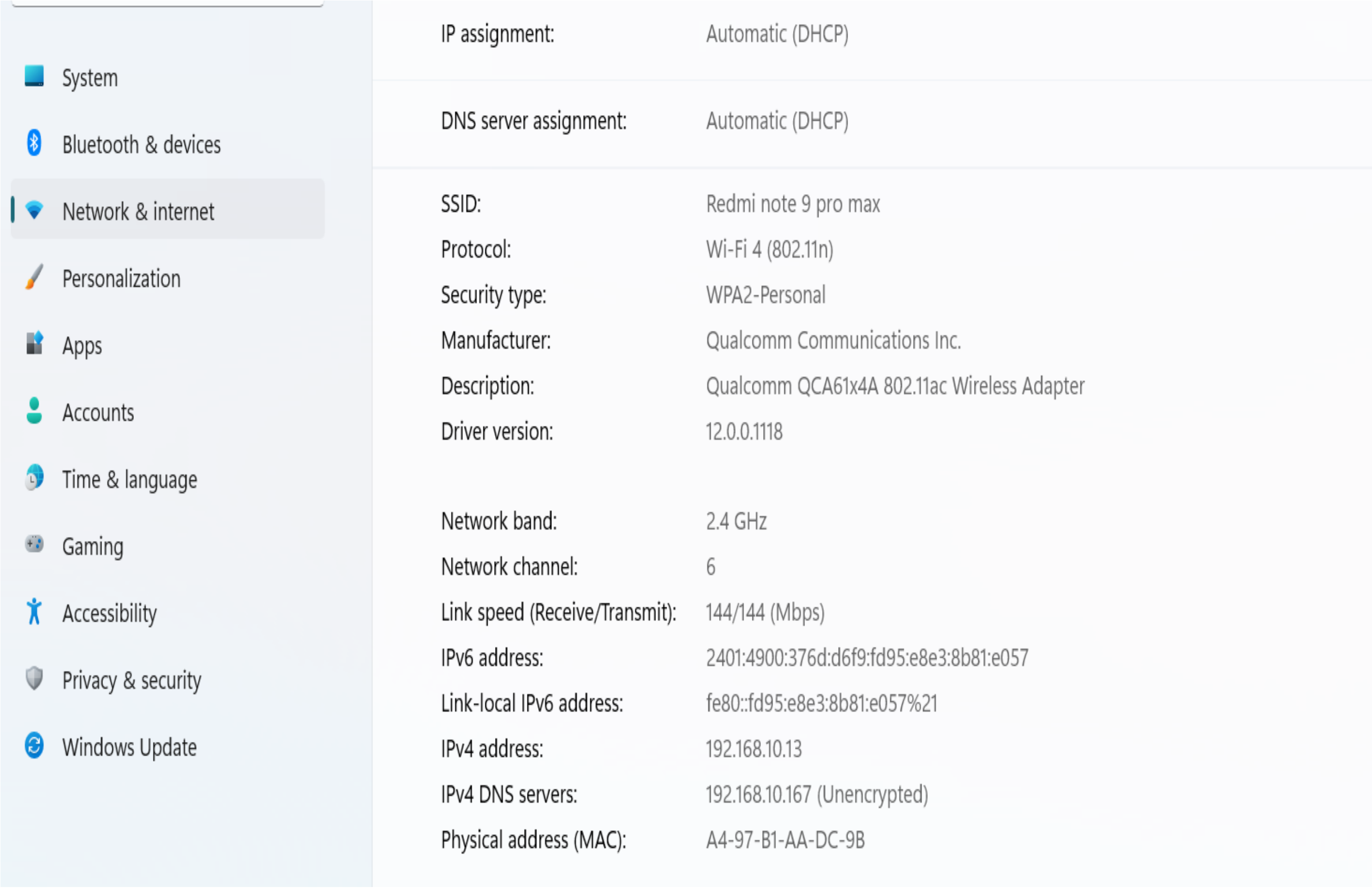
Step 1: Use the Network and Sharing Center.

a. Navigate to the **Control Panel**. Click **View network status and tasks** under Network and Internet heading in the Category View.
b. In the left pane, click the **Change adapter settings**
c. In the Network Connections window, the results provide a list of NICs available on this PC. Look for your Wi-Fi adapters.

Note: Virtual Private Network (VPN) adapters and other types of network connections may also be displayed in this window.

Step 2: Work with your wireless NIC.

a. Locate the wireless network connection. If it is disabled, right-click and select En**a**ble to activate your wireless NIC.
b. If the wireless network connection is not currently connected, right-click and select **Connect/Disconnect** to connect to an SSID that you are authorized to connect to.
c. Right-click a wireless network connection, and then click **Status.**
d. The wireless network connection **Status** window displays where you can view information about your wireless connection.



IP assignment: Automatic (DHCP)

DNS server assignment: Automatic (DHCP)

SSID: Redmi note 9 pro max
Protocol: Wi-Fi 4 (802.11n)
Security type: WPA2-Personal
Manufacturer: Qualcomm Communications Inc.
Description: Qualcomm QCA61x4A 802.11ac Wireless Adapter
Driver version: 12.0.0.1118

Network band: 2.4 GHz
Network channel: 6
Link speed (Receive/Transmit): 144/144 (Mbps)
IPv6 address: 2401:4900:376d:d6f9:fd95:e8e3:8b81:e057
Link-local IPv6 address: fe80::fd95:e8e3:8b81:e057%21
IPv4 address: 192.168.10.13
IPv4 DNS servers: 192.168.10.167 (Unencrypted)
Physical address (MAC): A4-97-B1-AA-DC-9B

9. Wired network vs Wireless network | Difference between Wired network and Wireless network.

Following table compares Wired network vs Wireless network and mentions difference between wired network and wireless network types.

Specifications	Wired network	Wireless network
Speed of operation	Higher	lower compare to wired networks, But advanced wireless technologies such as LTE, LTE-A and WLAN-11ad will make it possible to achieve speed par equivalent to wired network
System Bandwidth	High	Low, as Frequency Spectrum is very scarse resource
Cost	Less as cables are not expensive	More as wireless subscriber stations, wireless routers, wireless access points and adapters are expensive
Installation	Wired network installation is cumbersome and it requires more time	Wireless network installation is easy and it requires less time
Mobility	Limited, as it operates in the area covered by connected systems with the wired network	Not limited, as it operates in the entire wireless network coverage
Transmission medium	copper wires, optical fiber cables, ethernet	EM waves or radiowaves or infrared
Network coverage extension	requires hubs and switches for network coverage limit extension	More area is covered by wireless base stations which are connected to one another.
Applications	LAN (Ethernet), MAN	WLAN, WPAN(Zigbee, bluetooth), Infrared, Cellular(GSM,CDMA, LTE)
Channel Interference and signal power loss	Interference is less as one wired network will not affect the other	Interference is higher due to obstacles between wireless transmitter and receiver e.g. weather conditions, reflection from walls, etc.
QoS (Quality of Service)	Better	Poor due to high value of jitter and delay in connection setup

Reliability	High compare to wireless counterpart, as manufactured cables have higher performance due to existence of wired technology since years.	Reasonably high, This is due to failure of router will affect the entire network.

10. If you want to communicate with the internet which is the most important task to be done ? and how do you accomplish it?

The initial task to be done is to install a NIC .

View of a typical Network Interface Card (NIC)

Short for Network Interface Card, a 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 discuss the process of installing a Network Interface Card/Network Adapter.

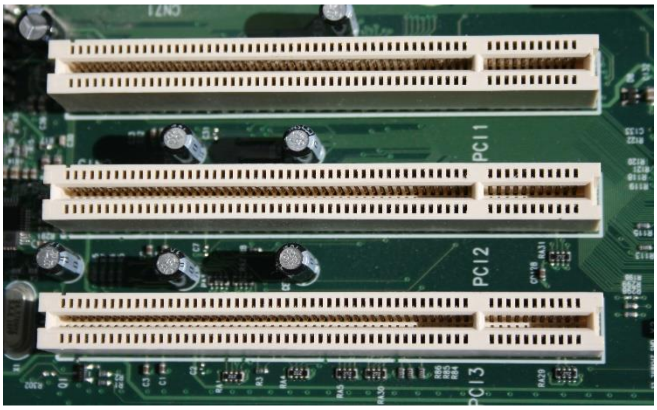
Installation Process in Windows

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.

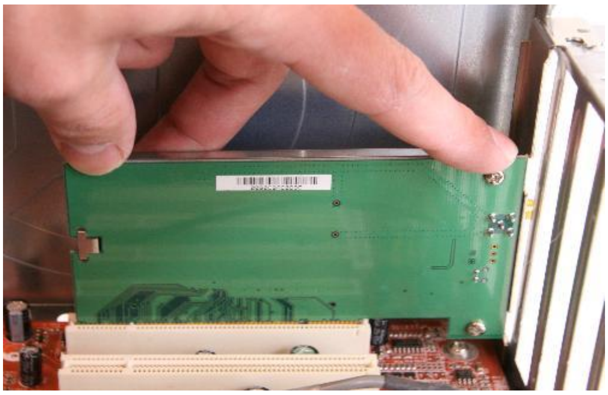
3. Open the computer case.

4. Find an available Peripheral Component Interconnect (PCI) slot on the motherboard and remove slot insert if one exists.



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.



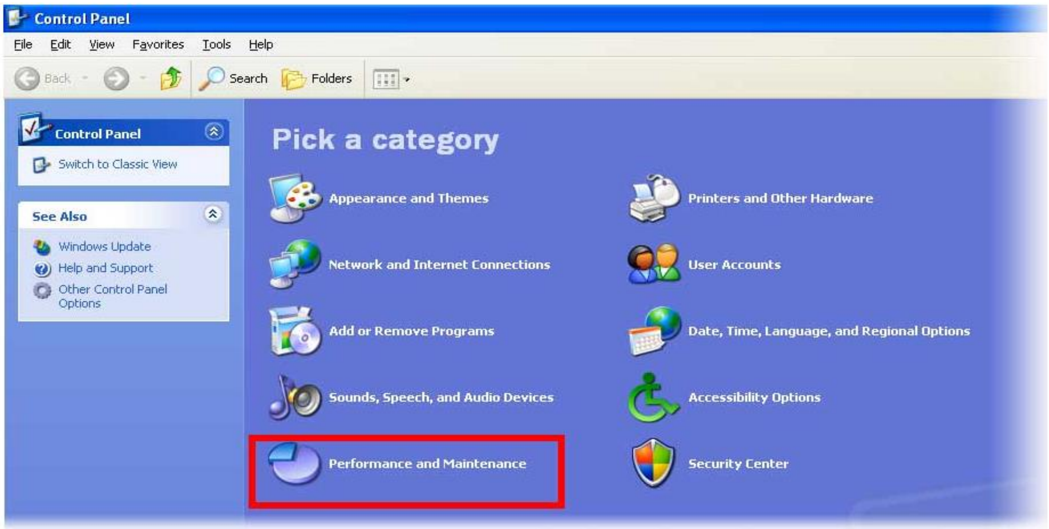
7. Snugly, screw the card to the computer frame, but do not over tighten.

8. Close the computer case.

9. Plug your computer in and power it up.

10. Click Start, then click Control Panel.

11. In Category View (vs. Classic View) click Performance and Maintenance.

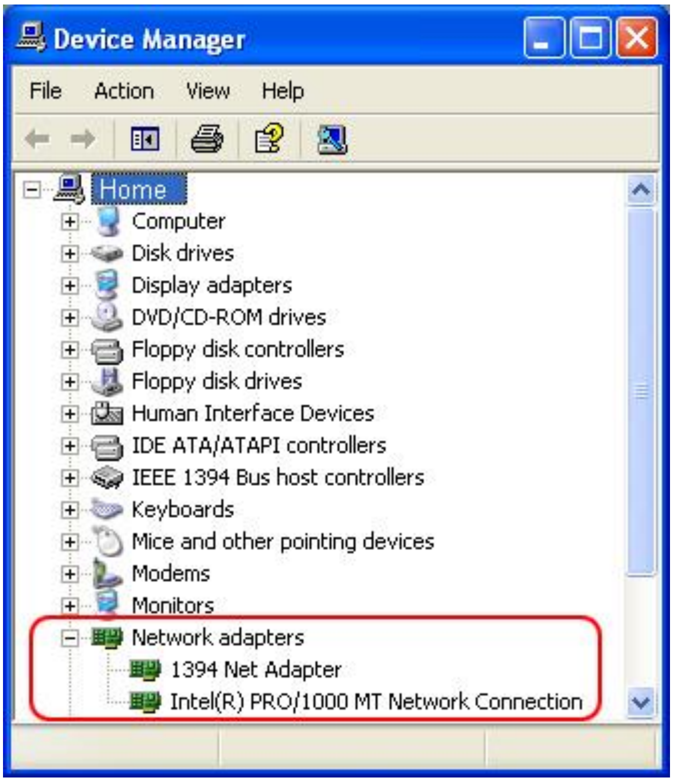

Control Panel
File Edit View Favorites Tools Help
Back Search Folders
Control Panel
Switch to Classic View
See Also
Windows Update
Help and Support
Other Control Panel Options
Pick a category
Appearance and Themes
Printers and Other Hardware
Network and Internet Connections
User Accounts
Add or Remove Programs
Date, Time, Language, and Regional Options
Sounds, Speech, and Audio Devices
Accessibility Options
Performance and Maintenance
Security Center

12. Click "System" icon at bottom of window.

13. Click the Hardware tab.

14. Click the Device Manager button.

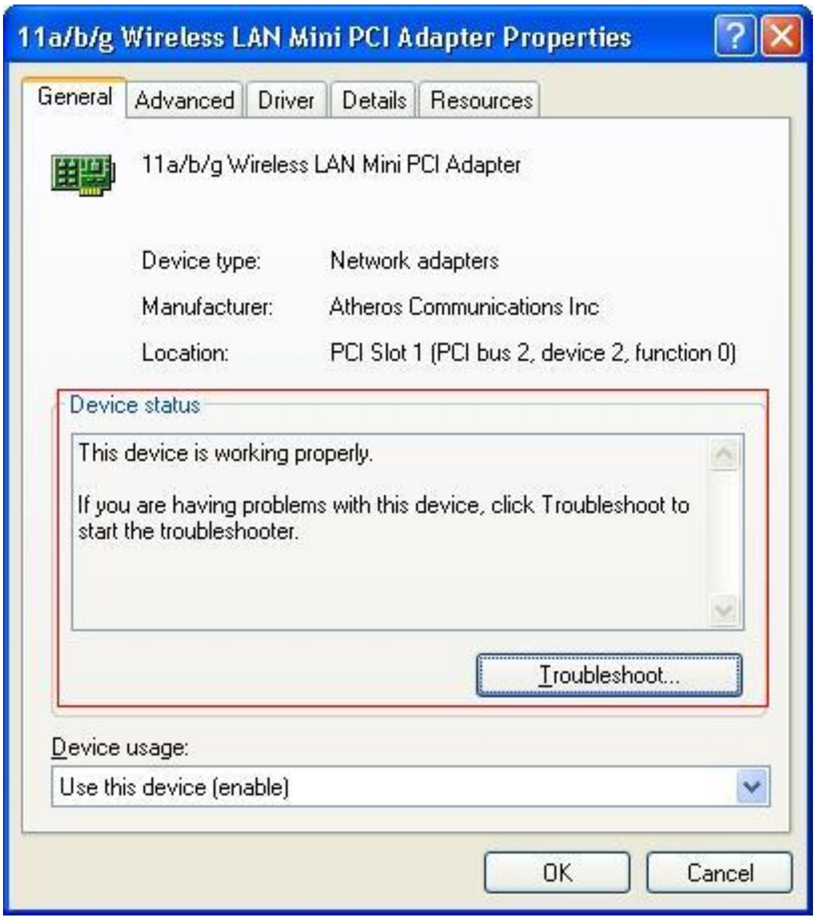
15. Double-click Network Adapters.



16. Beneath it should appear the name of your Ethernet card.

17. Next, double click the name of your Ethernet adapter.

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



11a/b/g Wireless LAN Mini PCI Adapter

Device type: Network adapters

Manufacturer: Atheros Communications Inc

Location: PCI Slot 1 (PCI bus 2, device 2, function 0)

This device is working properly.

If you are having problems with this device, click Troubleshoot to start the troubleshooter.

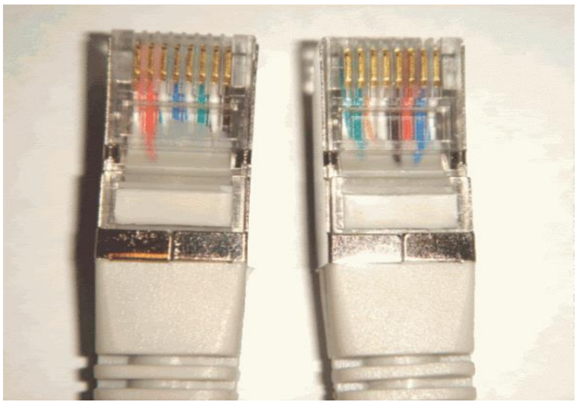
Device usage: Use this device (enable)

19. If the text in the "Device status" box doesn't say "This device is working properly.", then write down on a piece of paper what it says and continue with next step.

20. Click the Troubleshoot. Button and follow instructions. Double check you followed the directions above. Install the most up to date device drivers.

11. Setting up a Simple LAN Connection between 2 PCs

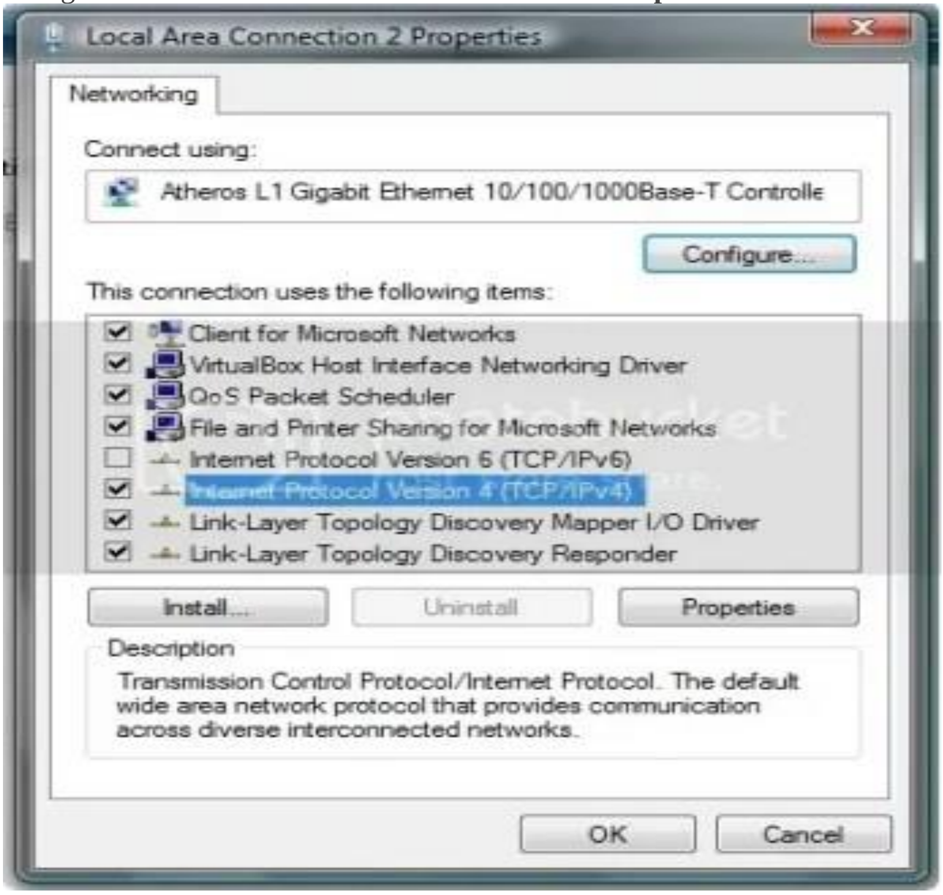
To create a simple LAN connection between two PCs/Laptops, the only hardware requisite is an Ethernet Crossover Cable. Ethernet Crossover Cables are easily available in the market.



Setting up LAN Connection

1. Connect the one end of the cable to your PC/laptop and then the other end to the other PC/laptop and make sure the clips are locked into the Ethernet Port.
2. If it's correctly connected, you should be noticing a computer icon near the clock in the taskbar on both the PCs. Right-click and choose **Network Connections**. Or **Control Panel -> Network Connections**.
Windows Vista & *Windows 7* users, open **Network & Sharing Center** from **Control Panel** and click **Manage Network connections**.

3. Right-click **Local Area Connection** and choose **Properties**



Local Area Connection 2 Properties

Networking

Connect using:

Atheros L1 Gigabit Ethernet 10/100/1000Base-T Controlle

Configure...

This connection uses the following items:

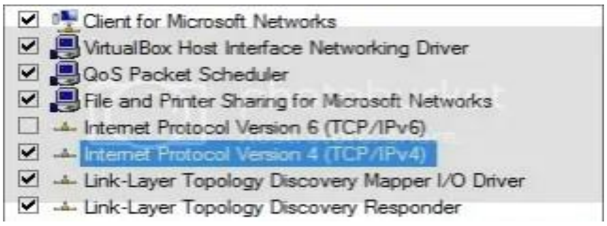
☑ Client for Microsoft Networks
☑ VirtualBox Host Interface Networking Driver
☑ QoS Packet Scheduler
☑ File and Printer Sharing for Microsoft Networks
☐ Internet Protocol Version 6 (TCP/IPv6)
☑ Internet Protocol Version 4 (TCP/IPv4)
☑ Link-Layer Topology Discovery Mapper I/O Driver
☑ Link-Layer Topology Discovery Responder

Install... Uninstall Properties

Description

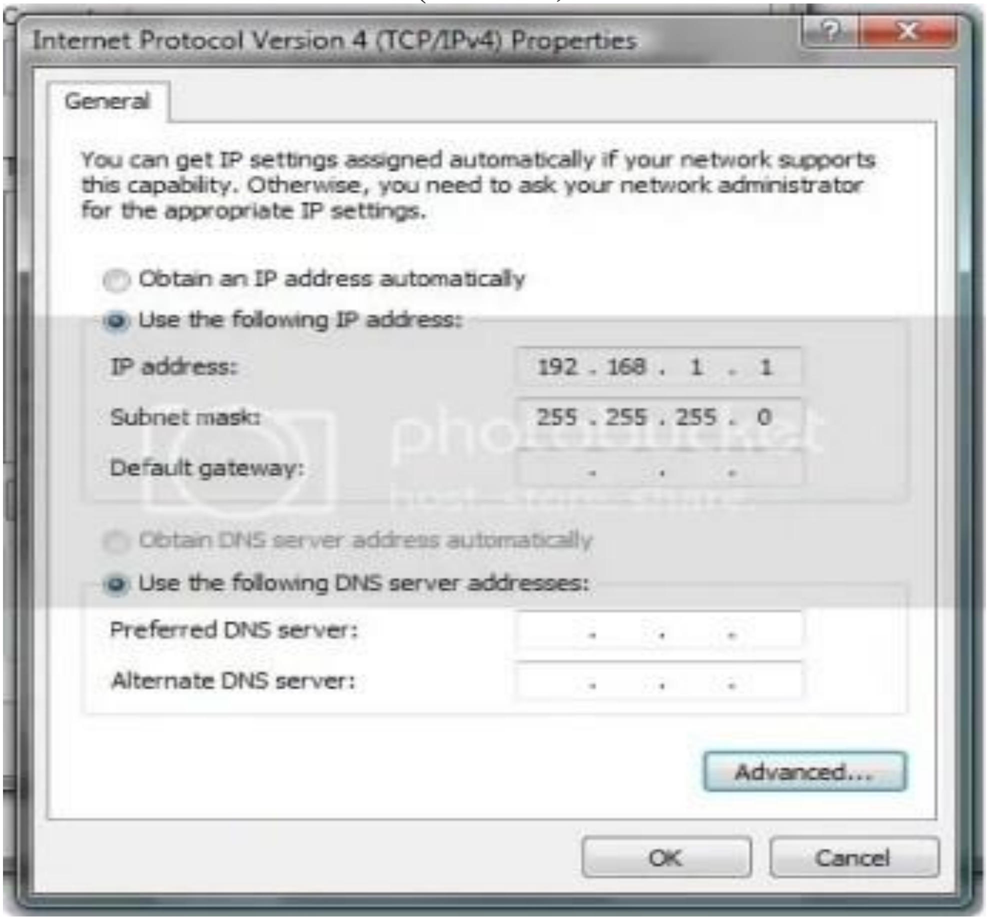
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

OK Cancel



☑ Client for Microsoft Networks
☑ VirtualBox Host Interface Networking Driver
☑ QoS Packet Scheduler
☑ File and Printer Sharing for Microsoft Networks
☐ Internet Protocol Version 6 (TCP/IPv6)
☑ Internet Protocol Version 4 (TCP/IPv4)
☑ Link-Layer Topology Discovery Mapper I/O Driver
☑ Link-Layer Topology Discovery Responder

4. Double-click **Internet Protocol** (Vista users, **Internet Protocol Version 4** – IPv4)



Internet Protocol Version 4 (TCP/IPv4) Properties

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.

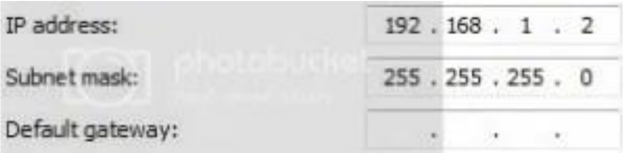
○ Obtain an IP address automatically
● Use the following IP address:

IP address: 192 . 168 . 1 . 1
Subnet mask: 255 . 255 . 255 . 0
Default gateway: . . .

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

Preferred DNS server: . . .
Alternate DNS server: . . .

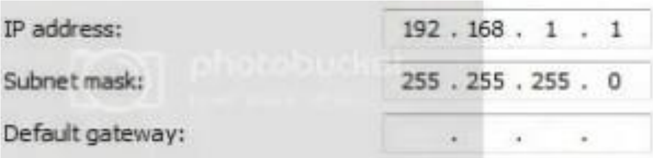
5. Choose “**Use the following IP Address**” radio box and enter the following details



IP address: 192 . 168 . 1 . 2
Subnet mask: 255 . 255 . 255 . 0
Default gateway: . . .

6. Click **OK**

7. Follow steps 1-4 on the other PC, and enter it’s IP & Subnet Mask as:



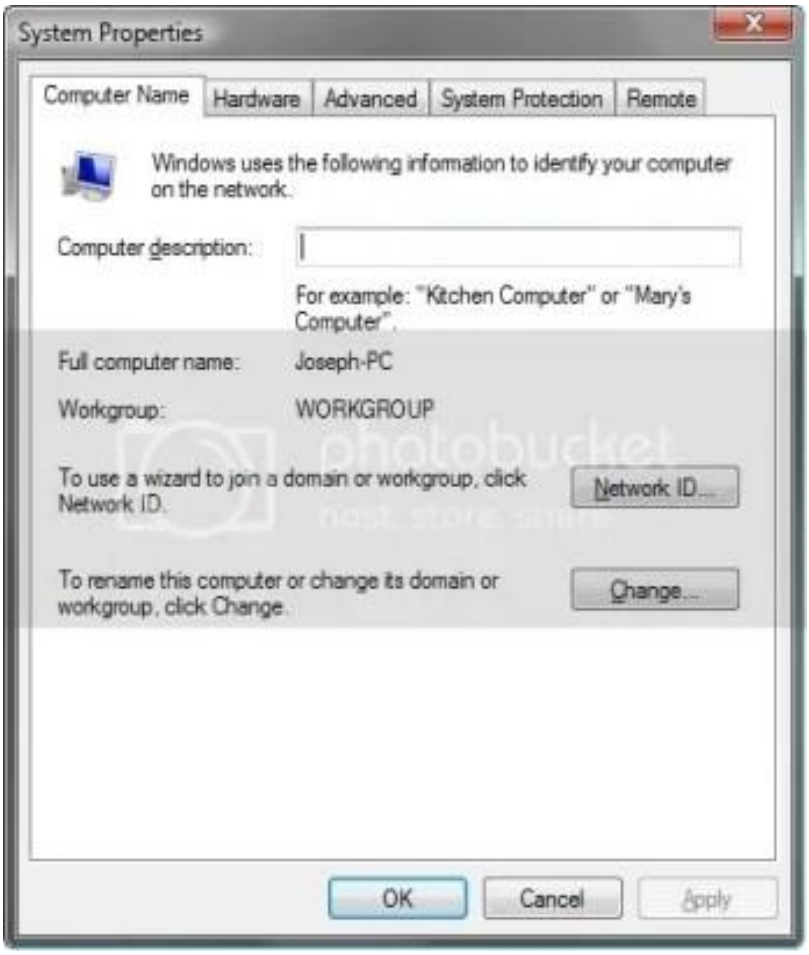
IP address: 192 . 168 . 1 . 1
Subnet mask: 255 . 255 . 255 . 0
Default gateway: . . .

Workgroup Name

If both the PCs use the same Workgroup name “WORKGROUP” (by default), you may leave step 8 and 9.

8. Finally you’ll have set up a Workgroup name on both the PCs/Laptops. To do so, right-click **My Computer**, click Properties, select the **Computer Name** tab and click Change and enter a name. Remember, the name should be the *same* on both PCs.

Vista users, My Computer -> Properties. Under Computer name, click **Change Settings**. Click **Change** button and enter a name. Remember, the name should be the *same* on both PCs.



Windows uses the following information to identify your computer on the network.

Computer description:

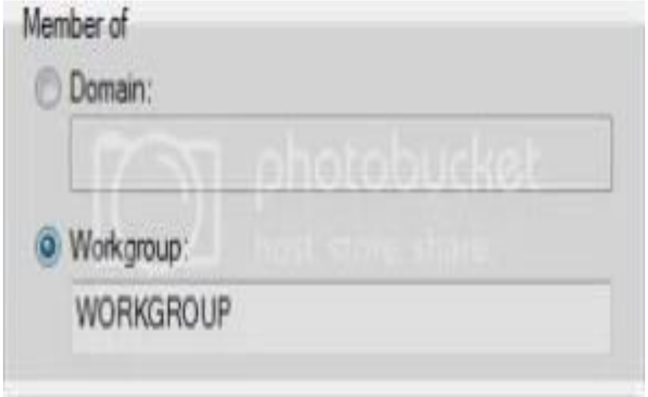
For example: "Kitchen Computer" or "Mary's Computer".

Full computer name: Joseph-PC

Workgroup: WORKGROUP

To use a wizard to join a domain or workgroup, click Network ID.

To rename this computer or change its domain or workgroup, click Change.



Member of

○ Domain:

● Workgroup: WORKGROUP

9. Click OK

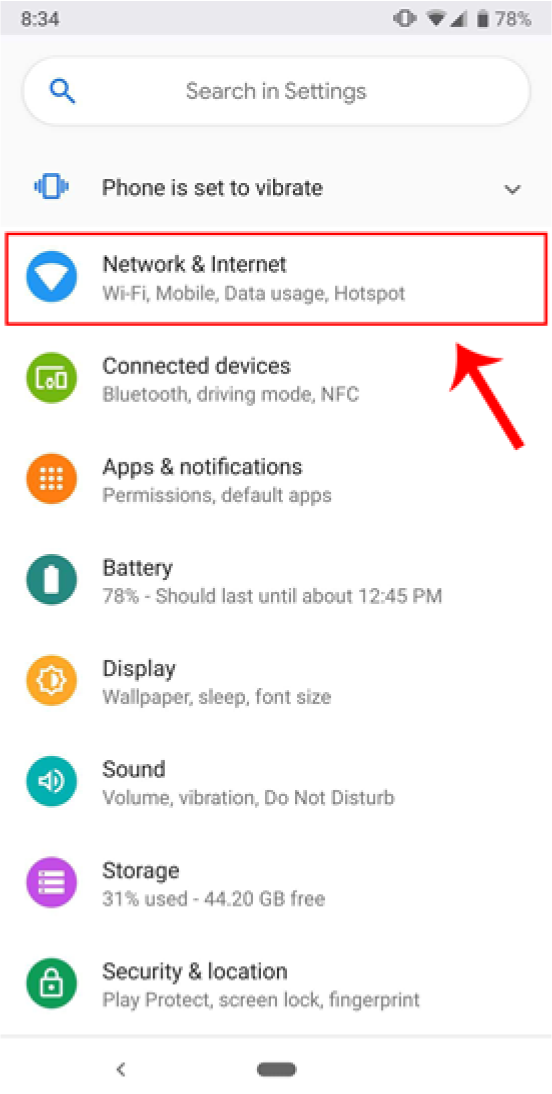
10. Restart both the PCs

You can now share folder or play multiplayer games via LAN. To share a folder, right-click the folder you wish to share and click **Properties**. Select **Sharing** tab and **enable Sharing** for folder. Open **Network** to access the files that are shared by the other PC.

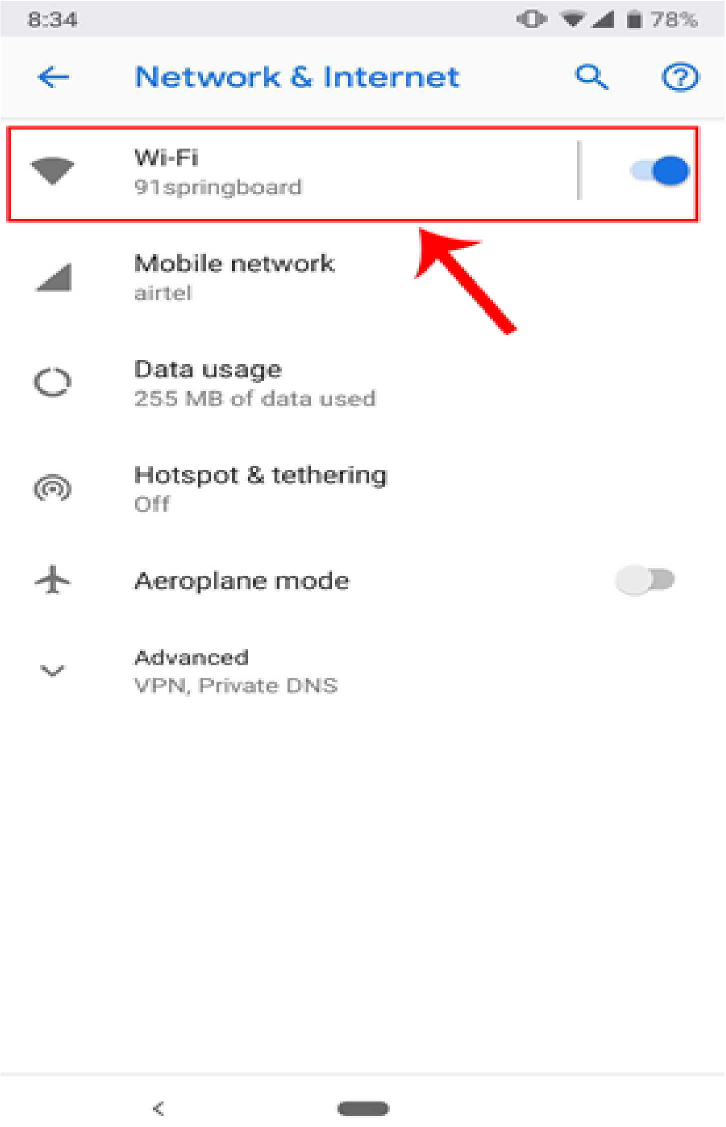
To play multiplayer via LAN, all you need is a game that supports Multiplayer. Proceed with Multiplayer mode, host a game and the other PC should join the game.

12. How to setup static IP on Android

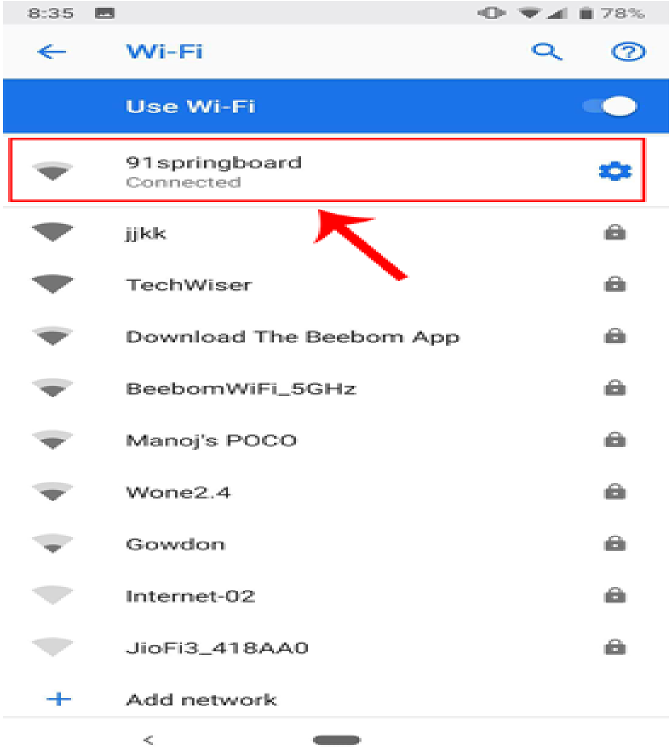
Setting a static IP can be natively done on Android. But the way to do it might be different on every phone due to the manufacturer skin. We will see how to do it on Pixel3 and the process should be similar on other phones as well. So head over to the **Settings** menu and tap on "Network & Internet".


8:34
78%
Search in Settings
Phone is set to vibrate
Network & Internet
Wi-Fi, Mobile, Data usage, Hotspot
Connected devices
Bluetooth, driving mode, NFC
Apps & notifications
Permissions, default apps
Battery
78% - Should last until about 12:45 PM
Display
Wallpaper, sleep, font size
Sound
Volume, vibration, Do Not Disturb
Storage
31% used - 44.20 GB free
Security & location
Play Protect, screen lock, fingerprint

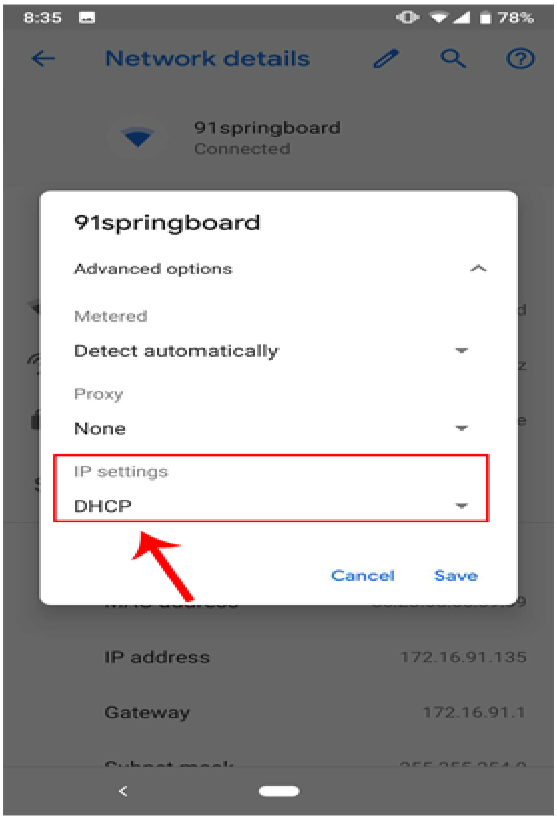
On top of the menu, you will see Wi-Fi, tap on it to get to the Wi-Fi Settings.



The network which you are connected to should be on top of the list. Tap on the settings icon beside the Wi-Fi network name.



Once the pop-up opens, you will see IP settings at the bottom of the menu. The default option is “DHCP”. Tap on it to change the IP configuration.



Metered: Detect automatically

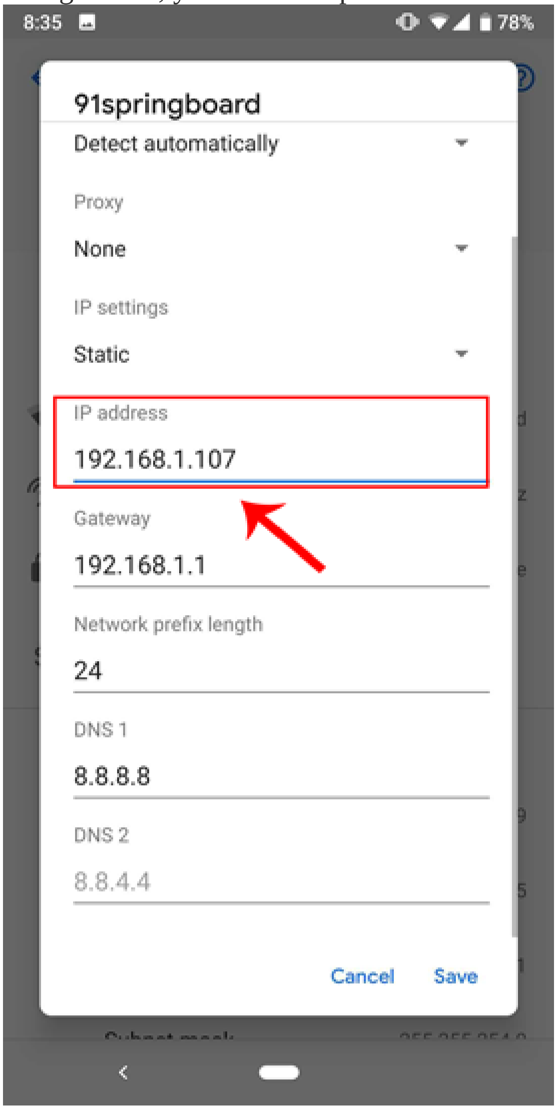
Proxy: None

IP settings: DHCP

IP address 172.16.91.135

Gateway 172.16.91.1

Select “**Static**” from the presented drop-down menu. Enter the **desired IP address** and leave the other options as default. Make sure that other devices are not using the same IP. You can see the IP address of the other devices in your network by using a small utility called Fing. Once you have entered the IP, click on **Save** to register the change. Now, your Android phone should start using the desired IP Address.



91springboard

Detect automatically

Proxy

None

IP settings

Static

IP address

192.168.1.107

Gateway

192.168.1.1

Network prefix length

24

DNS 1

8.8.8.8

DNS 2

8.8.4.4

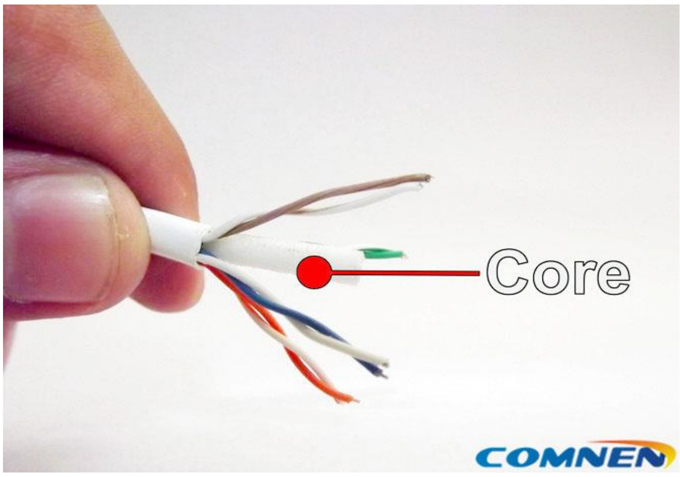
In almost all the Android version, you get the option to set static IP Address. For some rare older Android versions, you can use a third-party app like **WiFi Static**. It's free and it doesn't require ROOT.
To switch back to dynamic IP, repeat the same procedure and select "DHCP" from the IP settings instead.

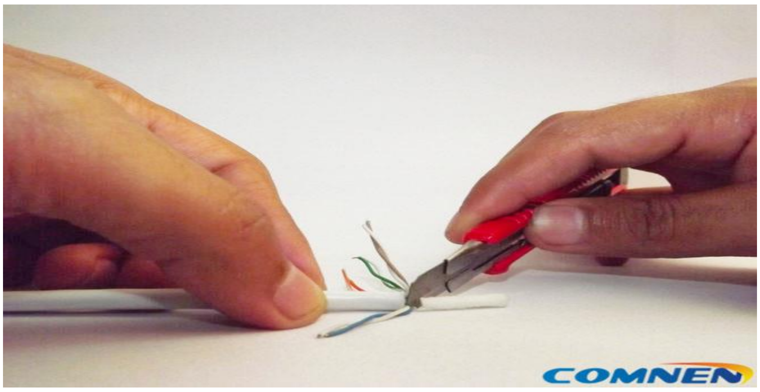
13. How to Crimp Rj45 connectors with a LAN cable.

Step 1
Choose your cable and the right RJ45 connectors
First of all, you should confirm the cable and connectors are the same category, means cat5e cable couple with cat5e rj45 connectors, cat6 cable with cat6 connectors, cat6a cable with cat6a connectors, *cat 7 cables* with cat 7 rj45 connectors. Secondly, the OD of the cable wires must couple with the connectors' wire channel(24AWG – 0.95mm; 26AWG – 0.9mm; 28AWG – 0.75mm; 30AWG – 0.6mm; 32AWG – 0.55mm)

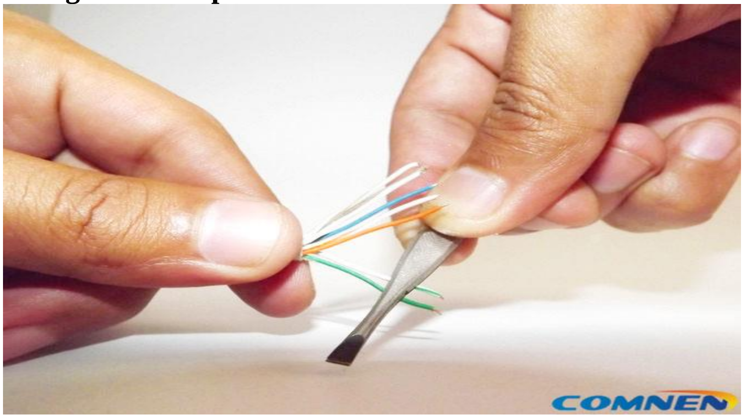
Step 2
Strip 1.8cm to 2cm of the jacket at the end of the cable

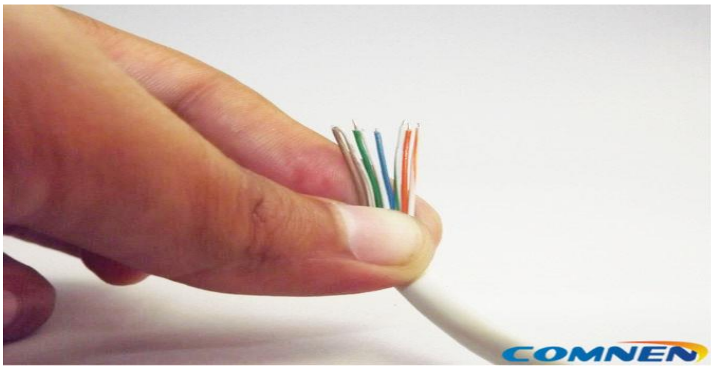
Step3
Cut of the core of the cable and abandon



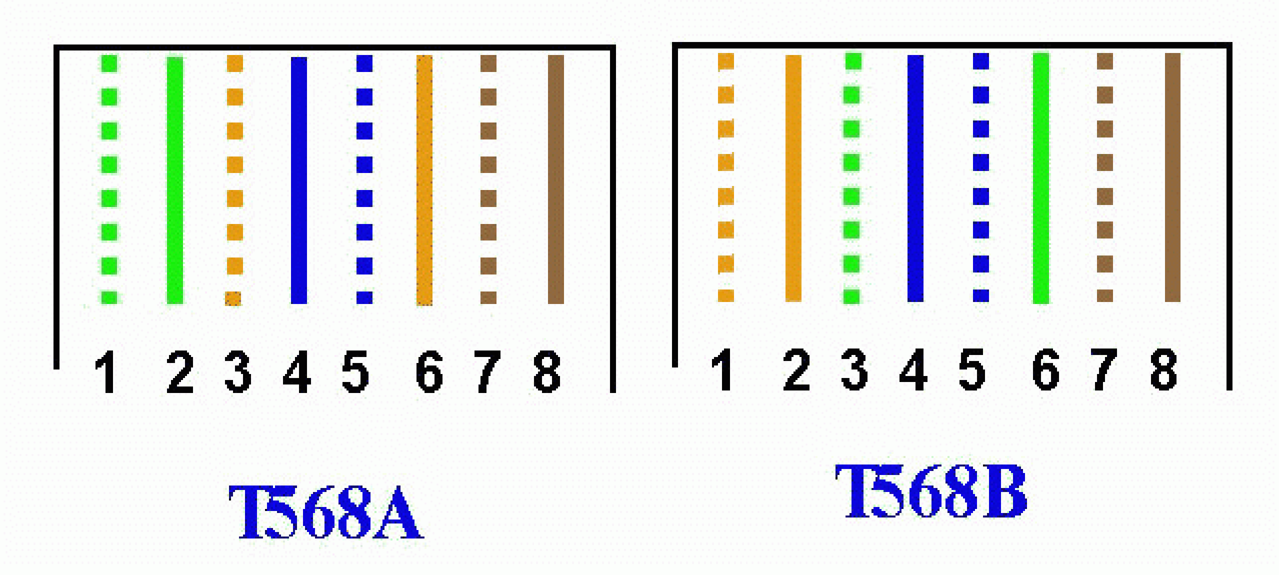


Step 4
Straighten the 4 pairs twisted wires and rank the wires between fingers



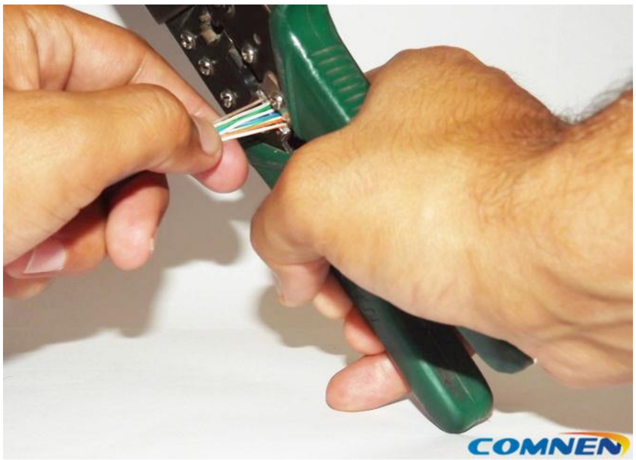


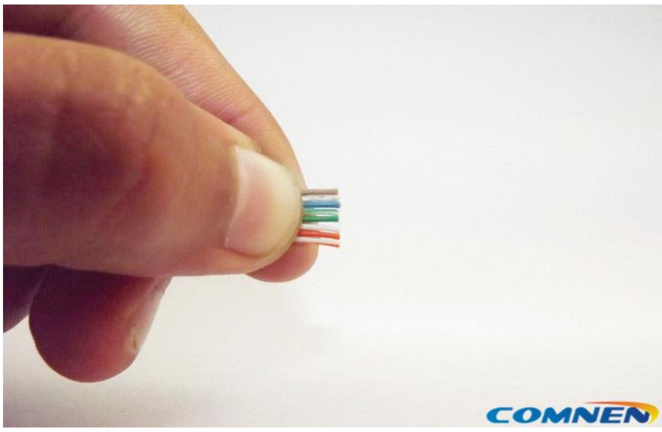
There are 2 kind of orders: T568-A and T568-B



T568-A wires turn(Green-White/Green, Orange-White/Blue, Blue-White/Orange, Brown-White/Brown)
T568-B wires turn(Orange-White/Orange, Green-White/Blue, Blue-white/Green, Brown-White/Brown)

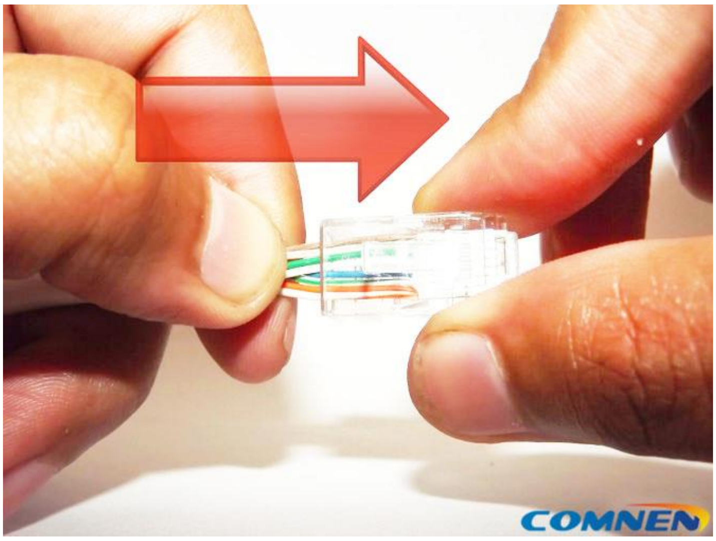
Step 5
Cut off about 0.5cm of the wires and keep the left wires neat



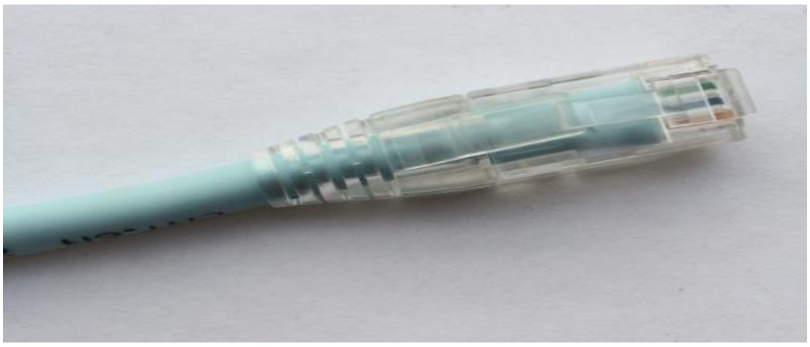


The left wires must be very neat, and easy to wire into the connectors
Step 6

Insert the wires into the RJ45 connectors

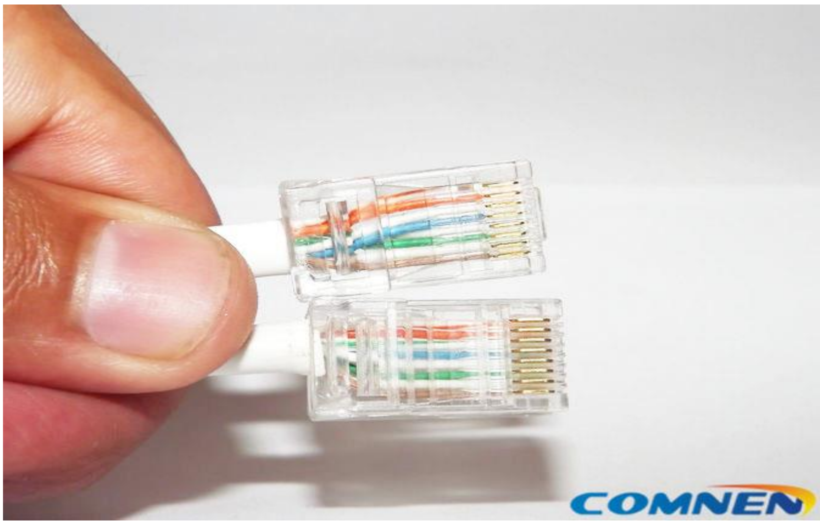


Be careful and make sure that the turns of the wires doesn't misplace
If you have inserted cable into a RJ45 boot, after inserted the wire,please insert RJ45 boot into connector, keep two claw to be inserted in the connector.



Step 7
Crimp the RJ45 connectors to the cable

By using the crimping tool, and press hardly, make sure the contacts of the connectors entirely connected with the wires



also have been crimped into connector.

Step 8

Test the cable using LAN tester.

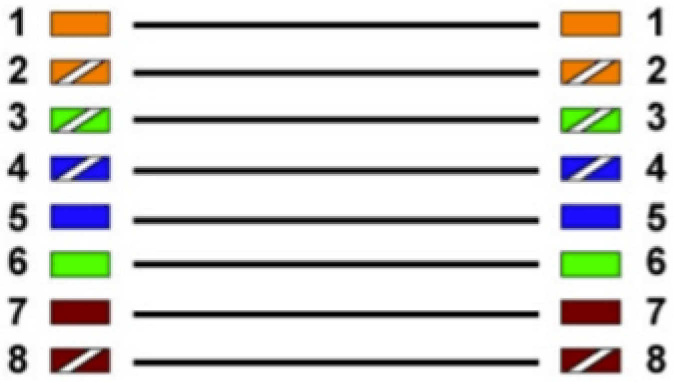
14 . Straight Through Cables vs Crossover Cables: Key Difference.

What is an Ethernet cable?

An Ethernet cable is a network cable used for high-speed wired network connections between two devices. This network cable is made of four-pair cable, which is consists of twisted pair conductors. It is used for data transmission at both ends of the cable, which is called RJ45 connector.

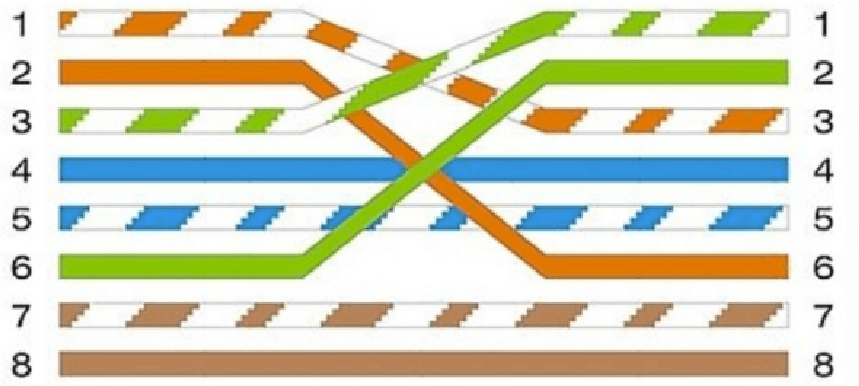
The Ethernet cables are categorized as Cat 5, Cat 5e, Cat 6, and UTP cable. Cat 5 cable can support a 10/100 Mbps Ethernet network while Cat 5e and Cat 6 cable to support Ethernet network running at 10/100/1000 Mbps.

What is Straight Through Cable?



Straight Through Cable :
Straight-through cable is a type of CAT5 with RJ-45 connectors at each end, and each has the same pin out. It is in accordance with either the T568A or T568B standards. It uses the same color code throughout the LAN for consistency. This type of twisted-pair cable is used in LAN to connect a computer or a network hub such as a router. It is one of the most common types of network cable.

What Is Crossover Cable?



Crossover Cable

A Crossover cable is a type of CAT 5 where one end isT568A configuration and the other end as T568BConfiguration. In this type of cable connection, Pin 1 is crossed with Pin 3, and Pin 2 is crossed with Pin 6.

Crossover cable is used to connect two or more computing devices. The internal wiring of crossover cables reverses the transmission and receive signals. It is widely used to connect two devices of the same type: e.g., two computers or two switches to each other.

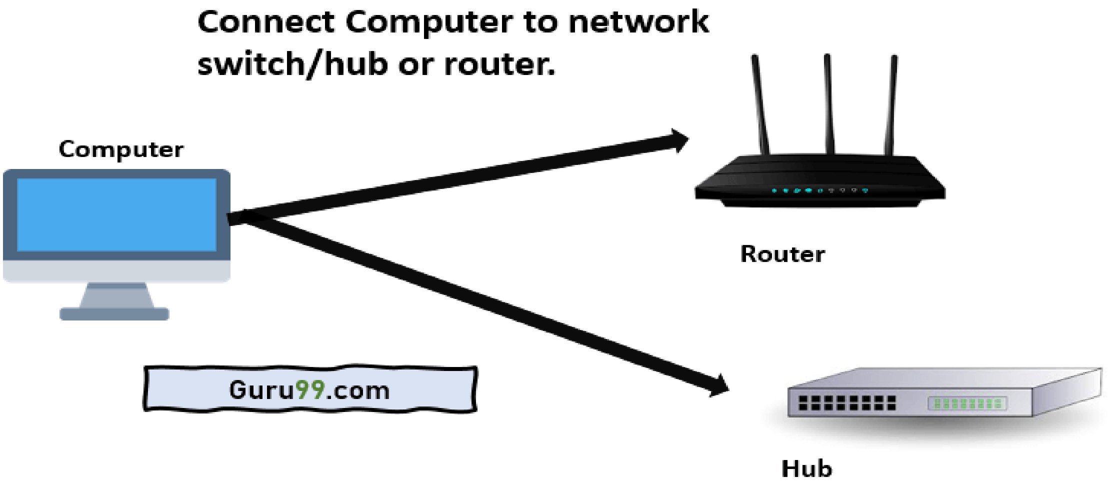
In regard to physical appearance, Crossover Ethernet cables are very much similar to regular Ethernet cables. Still, they are different with regard to the order with which the wires are arranged. This type of Ethernet cable is made to connect to network devices of the same kind over Ethernet directly. Crossover cables are mostly used to connect two hosts directly.

KEY DIFFERENCES:

- Crossover cable, Pin 1 is crossed with Pin 3, and Pin 2 is crossed with Pin 6 while in Straight-through cable Pin connection is one to one.
- Straight-through cables are mainly used for connecting non-similar devices while crossover cables are mostly used for connecting similar devices.

- Straight through cable connects a computer with a DSL modem while Crossover cable connects Router to Router and Computer to Computer.

When to use Straight Through Cable?

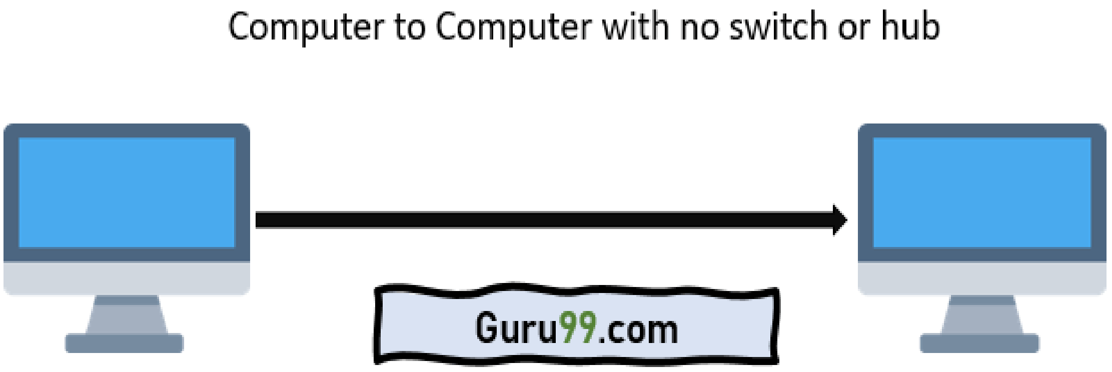


Computer to network switch/hub

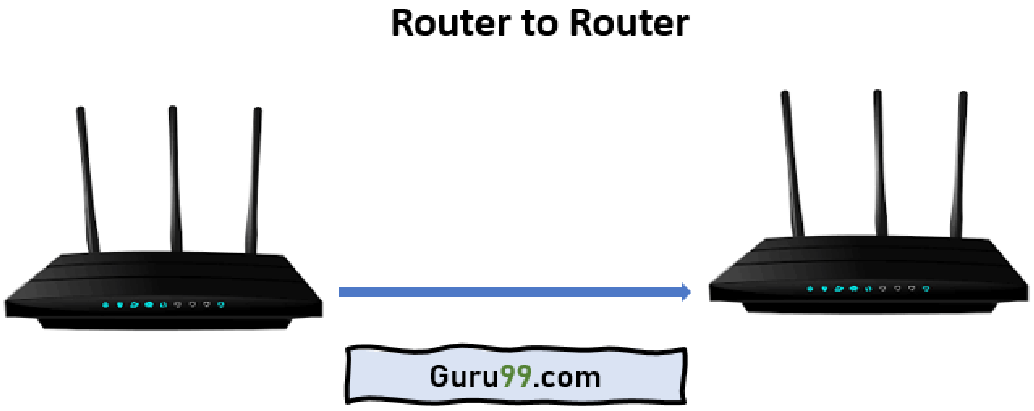
Here are applications where you should use Crossover Cable:

- It helps you to connect a computer to a switch/hub's normal port.
- You can use it to connect a computer to a cable/DSL modem's LAN port.
- It allows you to connect a router's WAN port to a cable/DSL modem's LAN port.
- Connect 2 switches or hubs with one of the hub or switch using an upline port and the other one using a normal port.

When to use Crossover Cable?



Use of Cross over cable- computer to computer



Router to Router
Here is an application where you should use Crossover Cable:

- It can use a computer to a computer with no switch or hub.
- Network devise to the network device. For example, the route to the router.
- Crossover cable enables one to establish a direct connection between two computing devices using Ethernet ports.
- It Connects two computers directly.
- You can connect two hubs/switches by using the normal port in both switches and hubs.

Difference between Crossover and Straight-through cable

Here are the difference between Crossover and straight-through cable

Straight through	**Crossover**
Straight-through cable is a type of CAT5 with RJ-45 connectors at each end, and each has the same pin out.	A Crossover cable is a type of CAT where one end is T568A configuration, and the other end as T568B Configuration.
It is one of the most commonly used cable formats for network cables.	It is used only for certain applications.
You can also connect it to the router's LAN port to a switch/hub's uplink port.	You can connect it to a router's LAN port to a switch or hub's regular port
Straight through cable connects a computer with a cable or DSL modem's LAN port.	Crossover cable connects with a router's LAN port with switch/hub normal port.
You should use straight-through cable when you want to connect two devices of different types.	You should use a crossover cable when you want to connect two devices of the same type.

Straight through	**Crossover**
It helps you connect a router's WAN port to a cable or DSL modem's LAN port.	You can connect two switches/hubs by using the normal port in both switches/hubs.
Straight-through cables are mainly used for connecting, unlike devices.	While crossover cables are mostly used for connecting like devices.

Straight Through vs. Crossover Cable, which one to choose?

The selection or network cable should be done based on your application. If you want your cable to connect to your computer and printer together, you need a crossover cable. If you have several computers and a printer, you should buy a switch**.**

All the computers connected to the switch with a straight–through cable and printer should be connected to the switch with a straight-through cable.

	HUB	**SWITCH**	**ROUTER**	**PC**
Hub	Crossover	Crossover	Straight	Straight
Switch	Crossover	Crossover	Straight	Straight
Router	Straight	Straight	Crossover	Crossover
PC	Straight	Straight	Crossover	Crossover

15 .Configure Network Interface Card (NIC) on a Computer

To connect the Xilinx® Zynq® hardware board to the development computer, you must configure an available network connection on the development computer. Follow the steps outlined for your specific operating system.

Windows

1. Open the **Control Panel**.
2. Set **View by** to Category.
3. Click **Network and Internet**.
4. Click **Network and Sharing Center**.
5. On the left pane, click **Change adapter settings**.
6. Right-click the local area network connection that is connected to the radio hardware and select **Properties**.
   - If an unused network connection is available, the local area connection appears as Unidentified network.
   - If you plan to reuse your network connection, select the local area connection that you plan to use for the radio hardware.
   - If you have only one network connection, check if you can connect wirelessly to the existing local area network. If you can, you can use the network connection for the radio hardware.

- You can use a pluggable USB to Gigabit Ethernet LAN adapter instead of a NIC. The instructions are the same.

7. On the **Networking** tab of the **Properties** dialog box, clear all options except **Internet Protocol Version 4 (TCP/IPv4)**. Other services, particularly antiviral software, can cause intermittent connection problems with the radio hardware.
8. Double-click **Internet Protocol Version 4 (TCP/IPv4)**.
9. On the **General** tab, select **Use the following IP Address**.
10. The default IP address of the Xilinx Zynq hardware board is 192.168.1.101. The development computer network connection must be on the same subnet as the hardware board. To meet this requirement, a compatible IP address must be assigned to the development computer network connection. Set the network IP address to 192.168.1.x, where *x* is any number in the range 1 through 255, apart from 101.

    Note

    Instead of 192.168.1, use the subnet address given by your hardware in the IP address.

11. Leave the subnet mask set to the default value of 255.255.255.0 and click **OK**.

16. A study on Packet tracer, how to install and use it .

Packet Tracer is a cross-platform visual simulation tool designed by Cisco Systems that allows users to create network topologies and imitate modern computer networks. The software allows users to simulate the configuration of routers and switches using a simulated command line interface. Packet Tracer makes use of a drag and drop user interface, allowing users to add and remove simulated network devices as they see fit.

Packet Tracer can be run on Linux, Microsoft Windows, and macOS. Similar Android and iOS apps are also available. Packet Tracer allows users to create simulated network topologies by dragging and dropping routers, switches and various other types of network devices. A physical connection between devices is represented by a 'cable' item. Packet Tracer supports an array of simulated Application Layer protocols, as well as basic routing with RIP, OSPF, EIGRP, BGP,

In addition to simulating certain aspects of computer networks, Packet Tracer can also be used for collaboration. As of Packet Tracer 5.0, Packet Tracer supports a multi-user system that enables multiple users to connect multiple topologies together over a computer network. Packet Tracer also allows instructors to create activities that students have to complete.[2] Packet Tracer is often used in educational settings as a learning aid.

Role in Education :

Packet Tracer allows students to design complex and large networks, which is often not feasible with physical hardware, due to costs. Packet Tracer is commonly used by NetAcad students, since it is available to them for free. However, due to functional limitations, it is intended by Cisco to be used only as a learning aid, not a replacement for Cisco routers and switches.[9] The application itself only has a small number of features found within the actual hardware running a current Cisco IOS version.

Significance of packet tracer:

Packet Tracer offers **an effective, interactive environment for learning networking concepts and protocols**. Most importantly, Packet Tracer helps students and instructors create their own virtual “network worlds” for exploration, experimentation, and explanation of networking concepts and technologies.

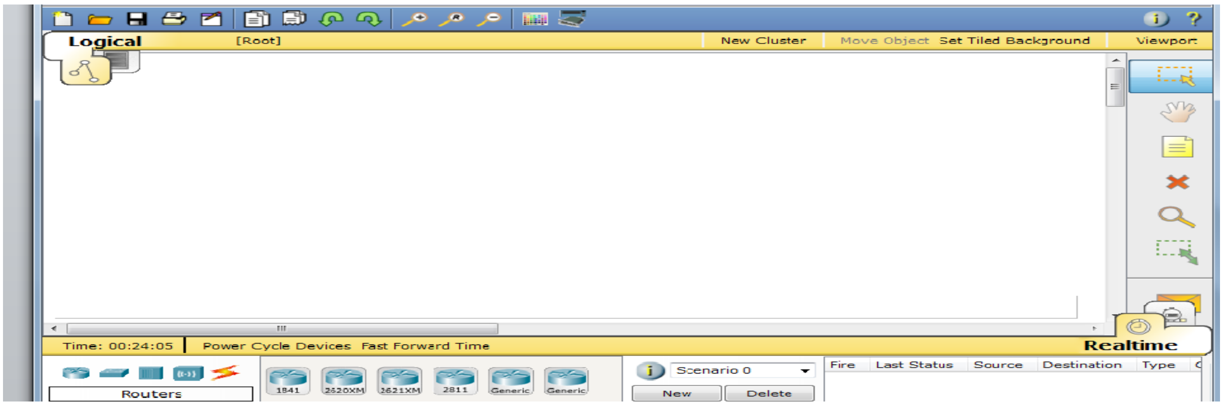
Who uses packet tracer?

It is mostly used by **Networking Curious & Aficionados, CCNA, CCNA Security and CCNP Students along with Engineers, Educators, & Trainers**. Before implementing any protocol, engineers like to test it on Cisco Packet Tracer.

How to use packet tracer to build a sample network.

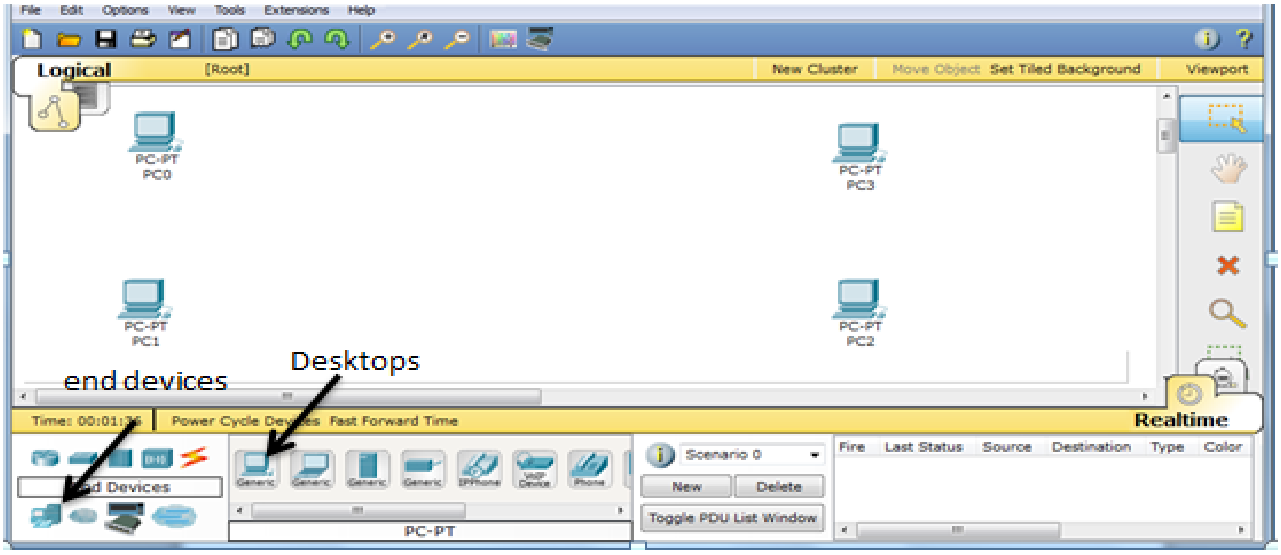
Step 1 Download CISCO Packet Tracer from this website. www.cisco.com

Step 2:



Open the program.
After download and install, the main page should be like this.

Step 3:



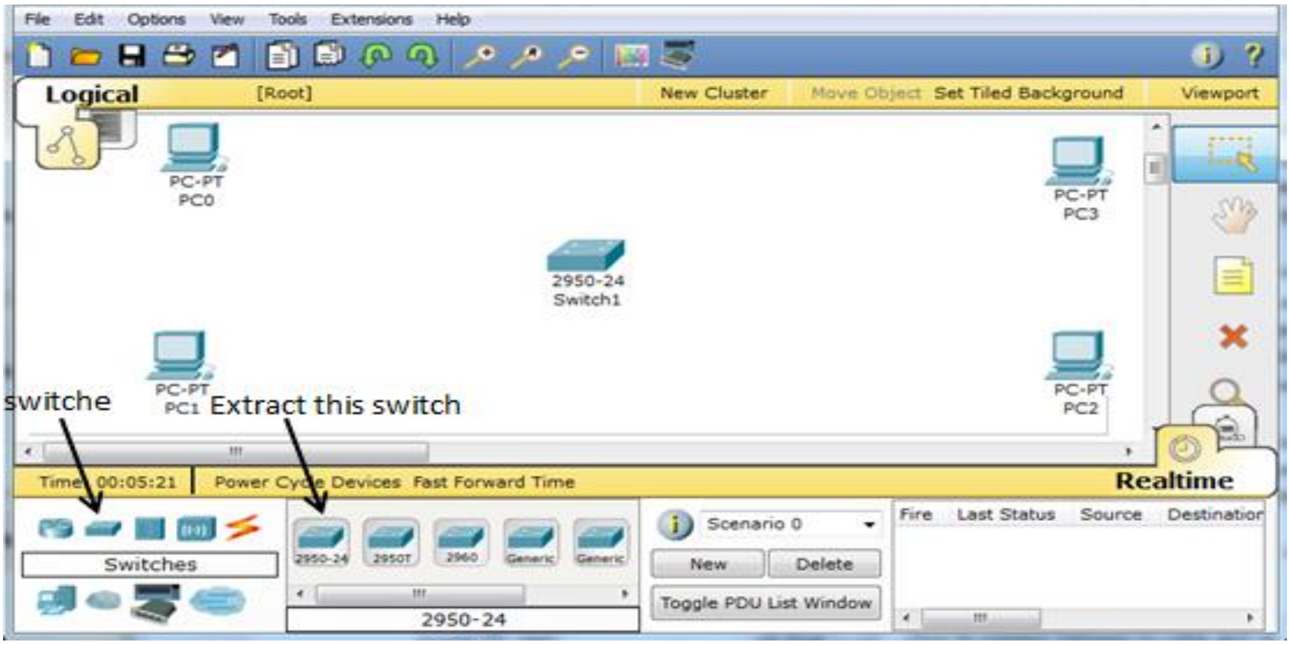
end devices

Desktops

Chose the end devices icon as shown on the Picher, and extract 4 desktops.

Notice: we can extract the devices which we need by click on it, after that drag it at the place which we need.

Step 4:

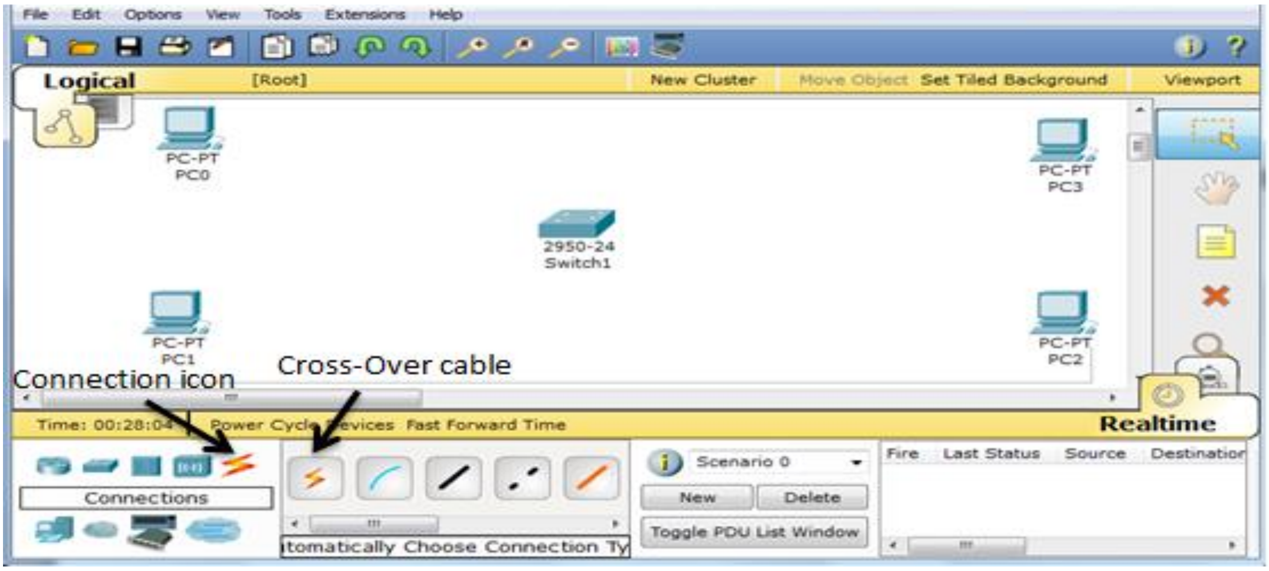


switche

Extract this switch

Add switch device to connect between the desktops. We can extract the switch device from the icon which it shown on the picture.

Step 5:



Connection icon

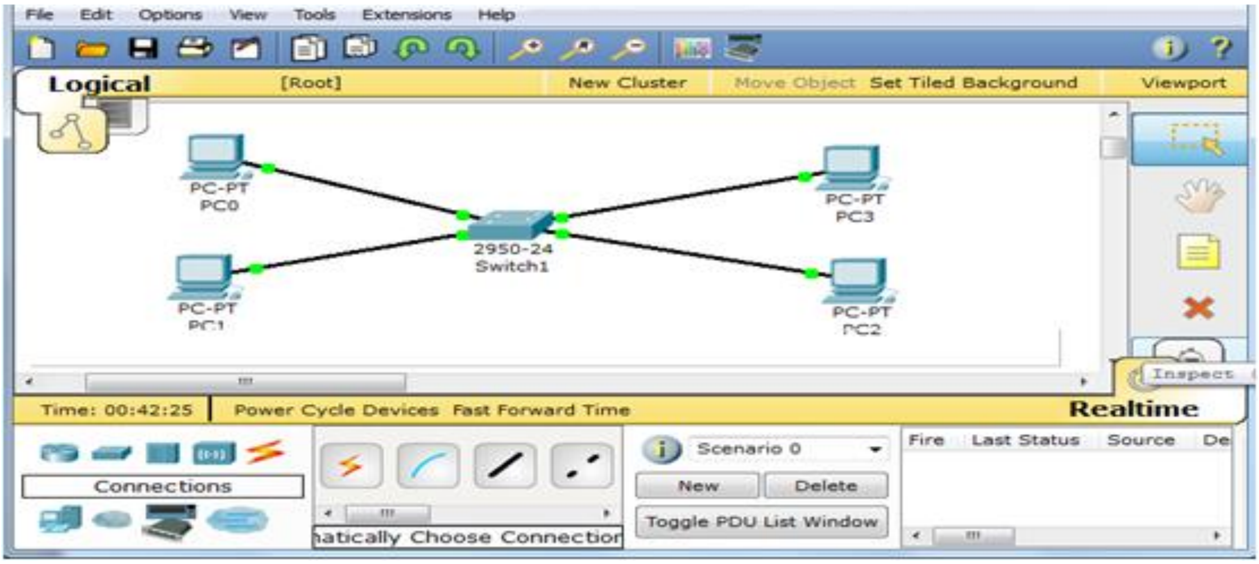
Cross-Over cable

Connecting the desktop via switch using Cross-Over cable .

What is Cross-Over cable?
It is kind of cables we use it to connect the desktops to the switch.

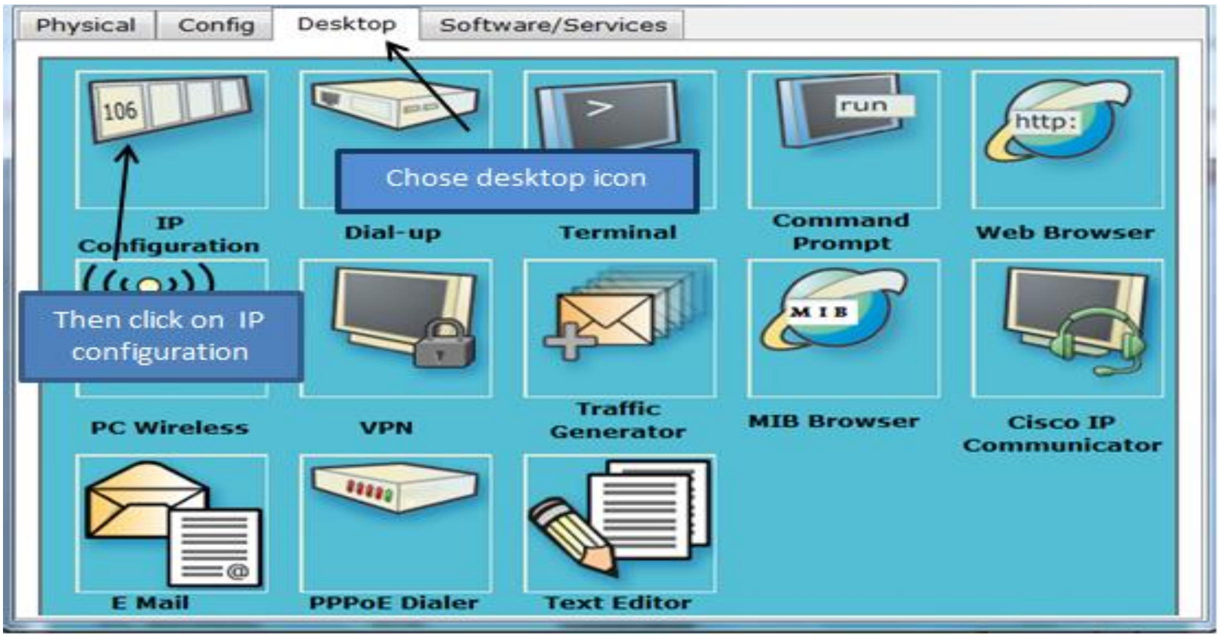
We can use the Cross-Over cable from connection icon, to connect each desktop to the switch.

Step 6:



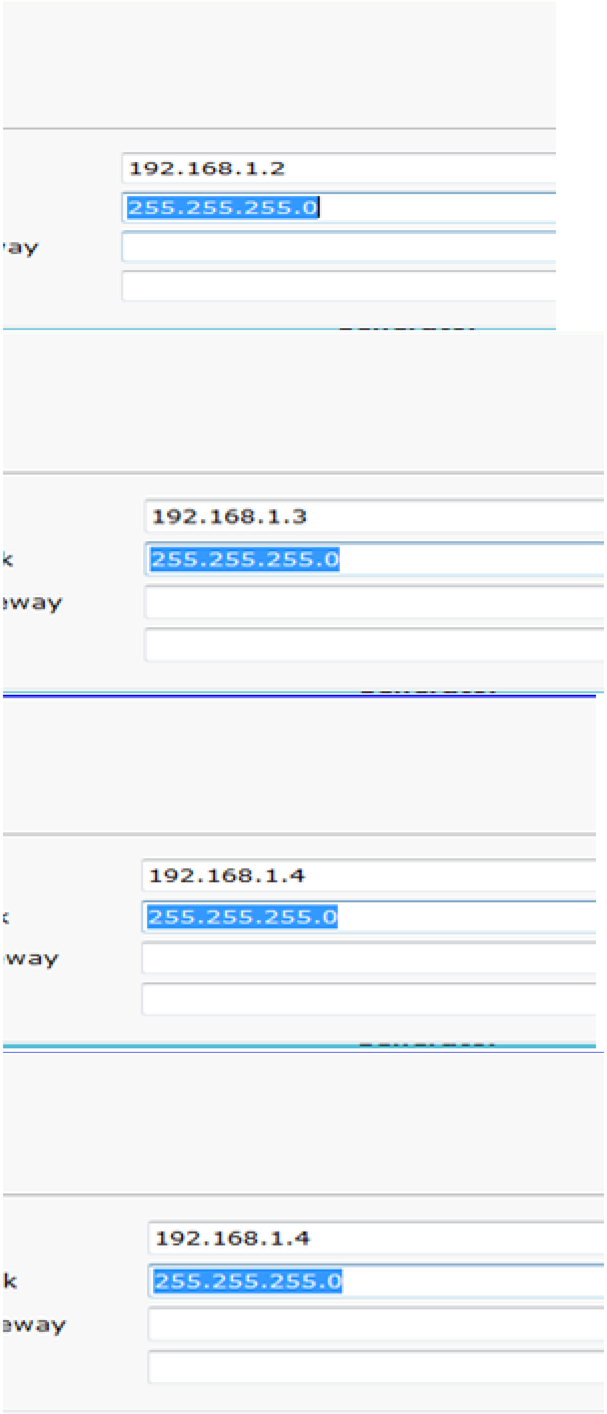
Click on Cross-Over cable, then click on desktop (PC0), after that click on the switch. Do this step with all desktops.

Step 7:



Give an IP address for each desktops.

Step 8:



'ay

192.168.1.2

255.255.255.0

k

eway

192.168.1.3

255.255.255.0

way

192.168.1.4

255.255.255.0

k

eway

192.168.1.4

255.255.255.0

The IP address for (PC0) is 192.168.1.2, and the subnet mask is 255.255.255.0.

The IP address for (PC1) is 192.168.1.3, and the subnet mask is 255.255.255.0.

The IP address for (PC2) is 192.168.1.4, and the subnet mask is 255.255.255.0.

The IP address for (PC3) is 192.168.1.5, and the subnet mask is 255.255.255.0.

17.

Create/Model a simple ethernet network using 3 hosts and a switch, observe traffic behaviour in network and observe data flow of ARP broadcasts and pings.

Objectives

- Develop an understanding of the basic functions of Packet Tracer.
- Create/model a simple Ethernet network using 3 hosts and a switch.
- Observe traffic behavior on the network.
- Observer data flow of ARP broadcasts and pings.

Part 1: Create a logical network diagram with 3 PCs and a switch.

During an activity, to ensure that the instructions always remain visible, click the “top” check box in the instruction box window.

The bottom left-hand corner of the Packet tracer screen displays the icons that represent device categories or groups, such as Routers, Switches, or End Devices.

Moving the cursor over the device categories will show the name of the category in the box. To select a device, first select the device category. When the device category is selected, the options within that category appear in the box next to the category listings. Select the device option that is required.

1. Select **End Devices** from the options in the bottom left-hand corner. Drag and drop 3 generic PCs onto your design area.
2. Select **Switch** from the options in the bottom left-hand corner. Add a 2960 switch to your prototype network by dragging it onto your design area.
3. Select **Connections** from the bottom left-hand corner. Choose a copper straight-through cable type. Click the first host (PC0) and assign the cable to the **FastEthernet0** connector. Click the switch (Switch0) and select a connection FastEthernet0/1 for PC0.
4. Repeat step c for PC1 and PC2. Select FastEthernet0/2 on the Switch0 for PC1 and FastEthernet0/3 for PC2.

There should be green dots at both ends of each cable connection after the network has converged. If not, double check the cable type selected.

Part 2: Configure host names and IP addresses on the PCs.

1. Click **PC0**. Select the **Config** tab. Change the PC Display Name to **PC-A**. Select **FastEthernet** tab on the left and add **192.168.1.1** as the IP address and **255.255.255.0** as the subnet mask. Close PC-A when done.
2. Click **PC1**. Select the **Config** tab. Change the PC Display Name to **PC-B**. Select **FastEthernet** tab on the left and add **192.168.1.2** as the IP address and **255.255.255.0** as the subnet mask. Close PC-B when done.
3. Click **PC2**. Select the **Config** tab. Change the PC Display Name to **PC-C**. Select **FastEthernet** tab on the left and add **192.168.1.3** as the IP address and **255.255.255.0** as the subnet mask. Close PC-C when done.

Part 3: Observe the flow of data from PC-A to PC-C by creating network traffic.

1. Switch to **Simulation Mode** in the bottom right-hand corner.

2. Click **Edit Filter** in the Edit List Filter area. In the event list filter, click **All/None** to deselect every filter. Click **Edit Filter**. Select **ARP** and **ICMP** filters under IPv4 tab.
3. Select a Simple PDU by clicking the closed envelope in the upper toolbar. With the envelop icon, click **PC-A** to establish the source. Click **PC-C** to establish the destination.

Note: Notice that two envelopes are now positioned beside PC-A. One envelop is ICMP, while the other is ARP. The Event List in the Simulation Panel will identify exactly which envelop represents ICMP and which represents ARP.

4. Select **Play** from the Play Controls in the Simulation Panel. You can speed up the simulation using the **Play Speed Slider**. The **Play Speed Slider** is located below **Play** inside the Simulation Panel. Dragging the button to the right will speed up the simulation, while dragging is to the left will slow down the simulation.
5. Observe the path ICMP and ARP envelope. Click **View Previous Event** to continue when the buffer is full.
6. Click **Reset Simulation** in the Simulation Panel. Notice that the ARP envelop is no longer present. This has reset the simulation but has not cleared any configuration changes or dynamic table entries, such as ARP table entries. The ARP request is not necessary to complete the ping because PC-A already has the MAC address in the ARP table.
7. Click **Capture then Forward** inside the Simulation Panel. The ICMP envelop will moved from the source to the switch and stop. The **Capture then Forward** allows you to move the simulation one step at a time. Continue selecting the **Capture then Forward** until you complete the event.
8. Click the **Power Cycle Device** on the bottom left, above the device icons.
9. An error message will appear asking you to confirm reset. Click **Yes**. Now both the ICMP and ARP envelops are present again. The power cycle will clear any configuration changes not saved and will clear all dynamic table entries, such as the ARP and MAC table entries.
10. Exit the simulation mode by clicking **Realtime** a allow the network to converge.
11. After the network has converged, enter the simulation mode.

Part 4: View ARP Tables on each PC.

1. Click **Play** to repopulate the ARP table on the PCs. Click **View Previous Event** when the buffer is full.
2. Click **Inspect** (magnifying glass) in the upper tool bar.
3. With the magnifying glass, click **PC-A**. Select **ARP Table** in the pop-up menu. Notice that PC-A has an ARP entry for PC-C. View the ARP tables for PC-B and PC-C as well. Close all ARP table windows.
4. Click **Select** in the upper tool bar.
5. Click PC-A and select the **Desktop** tab.
6. Select the **Command Prompt** and enter the command **arp -a** to view the ARP table from the desktop view. Close the PC-A configuration window.

```
C:\> arp -a
Internet Address        Physical Address      Type
192.168.1.3             0003.e406.e430        dynamic
```

7. Examine the ARP tables for PC-B and PC-C. Close the **Command Prompt** window when finished.

18. Build a simple peer-to-peer network and verify physical connectivity and Assign various IPv4 addresses to hosts and observe the effects on network communication.

- Go to Cisco Packet Tracer.
- Click on the End Devices and deploy 2PCs.
- Click on the connection category and select the Copper Cross-over cable type to connect PCs
- Click on PC, go to desktop and select IP configuration and assign IP address to all the individual PCs.
- Go to the command prompt and ping all the PCs. Ex: ping 192.168.1.1
- Go to tool bar & take a packet (PDU) & place it into source device and mention the destination device.
- We can start the simulation & we can see the message going from one PC to another PC.

19. Configure IP addresses of a network (real or simulated) and ping across to test and troubleshoot.

- Go to Cisco Packet Tracer.
- Click on the End Devices and deploy 3 PCs.
- Click on the Network Devices and deploy 2960 switch
- Click on the connection category and select the Copper Straight-Through cable type to connect PC to Switch.
- Click on PC, go to desktop and select IP configuration and assign IP address to all the individual PCs.
- Go to the command prompt and ping all the PCs. Ex: ping 192.168.1.1
- Go to tool bar & take a packet (PDU) & place it into source device and mention the destination device.
- We can start the simulation & we can see the message going from one PC to another PC.

20. Subnetting of a network (either using real network or in Simulator).

Subnetting

- It is the process of dividing a network into two or more smaller networks. It increases the network performance and routing efficiency.
- In class C network, the first three octets(24 bits) represents network address and the last octet (8 bits) represents the host address. Therefore the subnet address can be created by modifying the bits of the last octet.
- When subnets are created, the number of subnets is a power of 2. The value of the exponent gives the number of bits that represent the subnet mask.

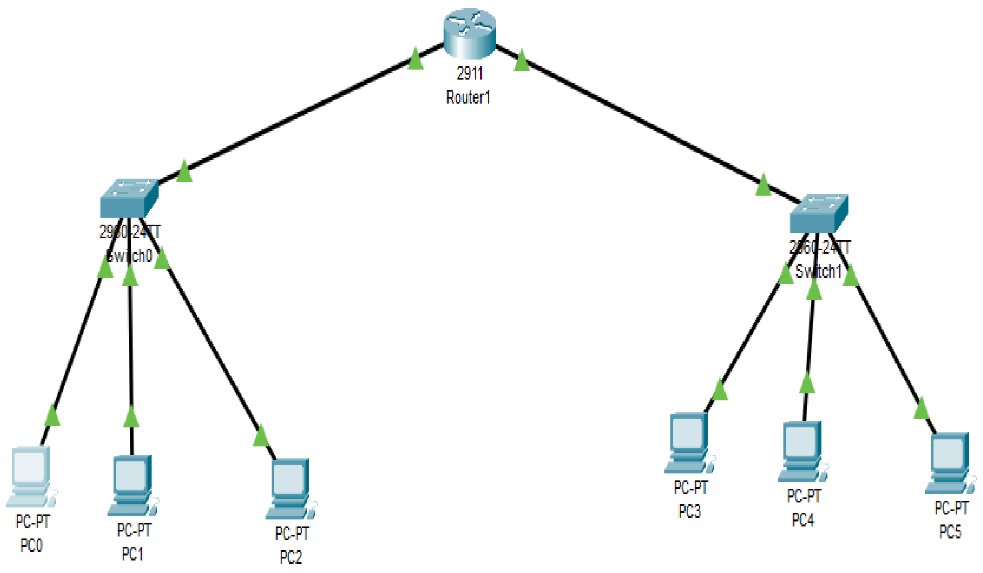
Example: Two subnets

Sl No	Subnet Address (Dotted)	Subnet Address (Binary)
Subnet 0	192.168.1.128	1100000.10101000.00000001.**1**0000000
Subnet 1	192.168.1.255	1100000.10101000. 00000001.**1**1000000

First subnet will have address between 192.168.1.1 and 192.168.1.127

Second subnet will have address between 192.168.1.129 and 192.168.1.255

- Go to Cisco Packet Tracer.
- Click on the End Devices and deploy 6 PCs.
- Click on the Network Devices and deploy two switches (2960) and one router (2911) and design a network as shown in the figure.



- Click on the connection category and select Automatically choose connection type to connect PC to Switch and switch to router
- Click on PC, go to desktop and select IP configuration and assign IP address to all the individual PCs.
- Go to the command prompt and ping all the PCs. Ex: ping 192.168.1.1

For first Network

	PC1	PC2	PC3
IP ADDRESS	192.168.1.1	192.168.1.2	192.168.1.3
SUBNET MASK	255.255.255.128	255.255.255.128	255.255.255.128
DEFAULT GATEWAY	192.168.1.4	192.168.1.4	192.168.1.4

For Second Network

	PC1	PC2	PC3
IP ADDRESS	192.168.1.129	192.168.1.130	192.168.1.131

SUBNET MASK	255.255.255.128	255.255.255.128	255.255.255.128
DEFAULT GATEWAY	192.168.1.132	192.168.1.132	192.168.1.132

For Router

- Click on router
- Go to config
- Click on GigabitEthernet0/0
- Click the on check box in the right corner and assign IP Address : 192.168.1.4

  And subnet mask: 255.255.255.128
- Click on GigabitEthernet0/1
- Click the on check box in the right corner and assign IP Address : 192.168.1.132

  And subnet mask: 255.255.255.128

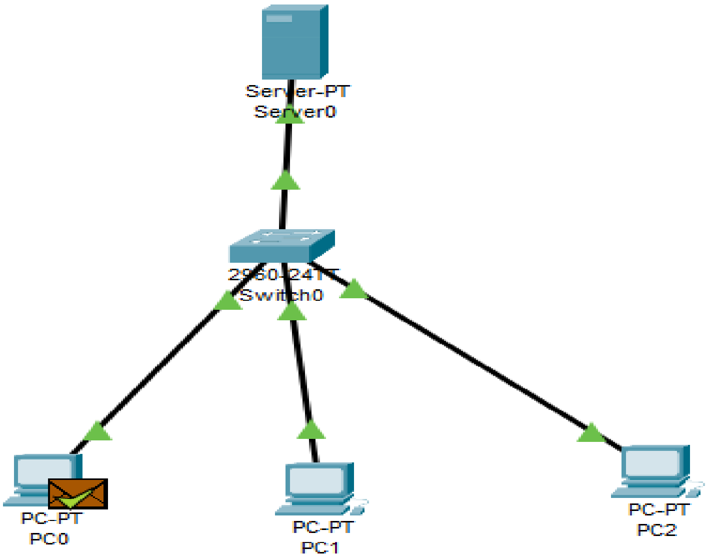
21. Connect to web server using simulator, Observe how packets are sent across the Internet using IP addresses

- Go to Cisco Packet Tracer.
- Deploy 3 PC, one switch and one server as shown in the figure.
- Click on the connection category and select Automatically choose connection type to connect PC to Switch and switch to server
- Click on PC, go to desktop and select IP configuration and assign IP address to all the individual PCs and a server.

-

- Go to tool bar & take a packet (PDU) & place it into source device (PC) and mention the destination device (Server).
- We can start the simulation & we can see the message going from one PC to another Server.

	PC1	PC2	PC3	Server
IP ADDRESS	192.168.1.2	192.168.1.3	192.168.1.4	192.168.1.1
SUBNET MASK	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
DEFAULT GATEWAY	192.168.1.1	192.168.1.1	192.168.1.1	192.168.1.1



22. Implement simple static routing.

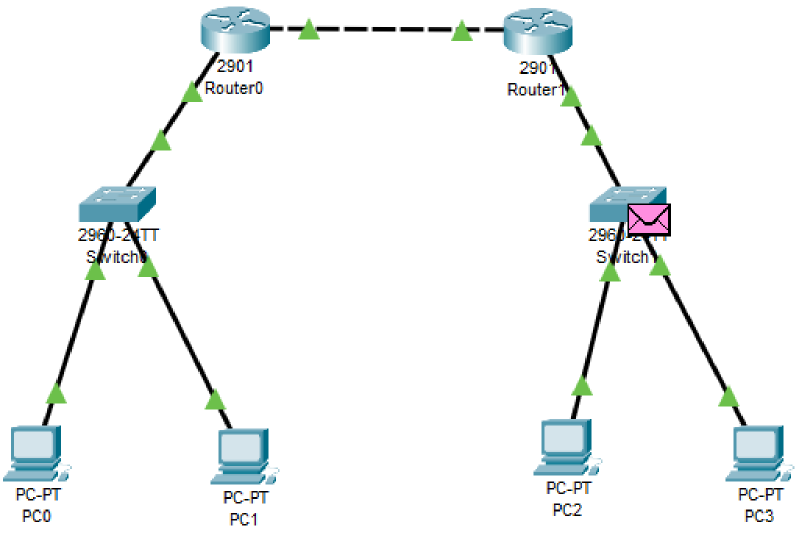
- Go to Cisco Packet Tracer.
- Deploy 4 PC, 2 switch and 2 routers as shown in the figure.
- Click on the connection category and select Automatically choose connection type to connect PC to Switch and switch to router and router to router
- Click on PC, go to desktop and select IP configuration and assign IP address to all the individual PCs and a Routers

-

- Go to tool bar & take a packet (PDU) & place it into source device (PC) and mention the destination device (Server).
- We can start the simulation & we can see the message going from one PC to another Server.

	PC1	PC2	Router1 (Interface 0)	Router1 (Interface 1)
IP ADDRESS	192.168.1.2	192.168.1.3	192.168.1.1	192.168.3.1
SUBNET MASK	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
DEFAULT GATEWAY	192.168.1.1	192.168.1.1		

	PC3	PC4	Router2 (Interface 0)	Router2 (Interface 1)
IP ADDRESS	192.168.2.2	192.168.2.3	192.168.3.2	192.168.2.1
SUBNET MASK	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0
DEFAULT GATEWAY	192.168.2.1	192.168.2.1		



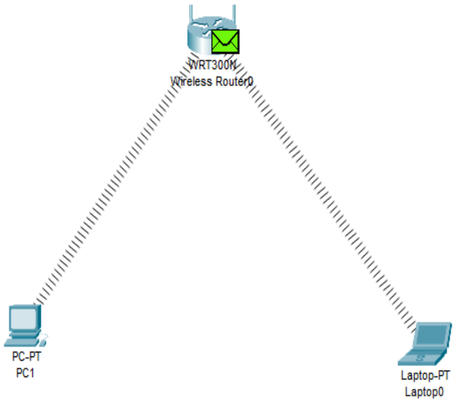
For Router

- Click on router
- Go to config
- Click on Static and mention Network, Mask and Next Hop

	Router1	Router2
Network	192.168.2.0	192.168.1.0
Mask	255.255.255.0	255.255.255.0
Next Hop	192.168.3.2	192.168.3.1

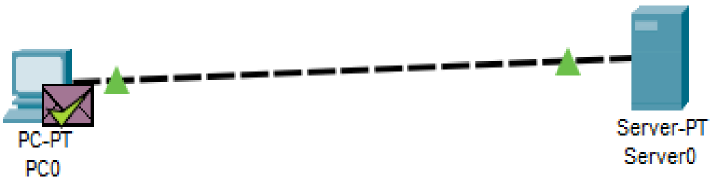
23. Configure and test DHCP on a wireless router (real or simulated)

- Go to Cisco Packet Tracer.
- Click on Wireless Devices
- Deploy a wireless Router, one PC and 1 Laptop as shown in the figure.
- Click on PC/Laptop go to Physical Tab. In physical device view, turnoff the PC, scroll down and remove PT- HOST-NM-1CFE slot (drag and drop to Left Panel) and replace it with WMP300N (drag and drop into slot) and turn on the PC/Laptop.
- Click on PC/Laptop, Go to Desktop Click on IP Configuration Choose DHCP
- Click on PC Select Web Browser Type 192.168.0.1
- Enter admin as User Name and Password
- Go to Wireless Tab, Change Network Name (SSID) and save the changes.
- Click on Router, go to Config tab and choose Wireless and select WEP and set the WEP Key as password(Integer 10 numbers)
- Click on PC/Laptop, select PC Wireless, click on connect, select Wireless Network Name and click on connect and enter WEP Key, click on connect.
- Go to tool bar & take a packet (PDU) & place it into source device (PC) and mention the destination device (Server).
- We can start the simulation & we can see the message going from one PC to another.



24. Ex1: Create a client – server model in simulator and observe the client interaction between the server and PC using packet tracer.

- Go to Cisco Packet Tracer.
  - Deploy and connect a PC and a Server as shown in the figure.
  - Click on server select config tab, click on FastEthernet0, set the IP address 192.168.1.1
  - Click on settings, set default gateway 192.168.1.1
  - Click on Service tab select DHCP, click on Service "On" (Radio Button), set default gateway 192.168.1.1 and Save the Changes
  - Place the PDU and simulate



Ex2: Observe DNS Name Resolution

a) Observe the connection of a URL to an IP address.

- Go to Cisco Packet Tracer.
- Deploy three servers, one switch a PC
- Connect all the devices

	Server1	Server2	Server3 (DNS)	PC
IP Addres	192.168.1.101	192.168.1.102	192.168.1.254	192.168.1.1
DNS Server	192.168.1.254	192.168.1.254	192.168.1.254	192.168.1.254

- Click on first server, select service tab, choose HTTP and edit the index,html file and write welcome to Facebook and save the changes.

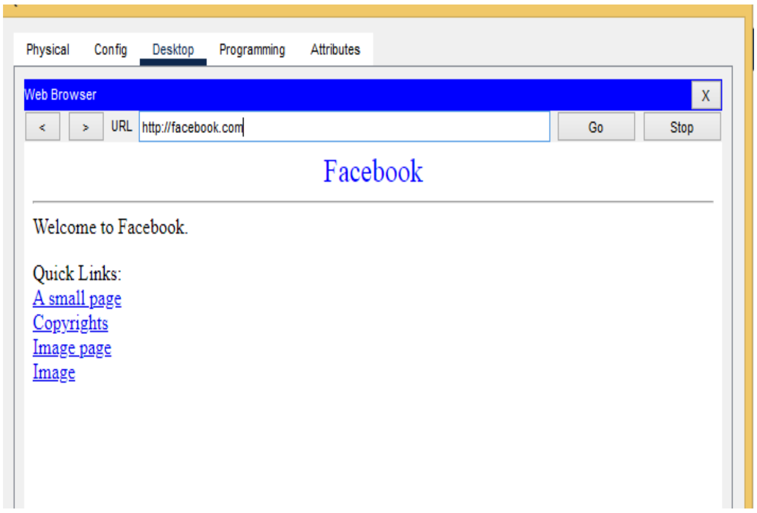
- Click on second server, select service tab, choose HTTP and edit the index,html file and write welcome to Youtube and save the changes.
- Click on PC, goto Command prompt and ping all the IP address.
- Click on Third server (DNS), select service tab, choose DNS, Switch on the DNS Service and Fill Resource Records which includes Name of the server and IP address of all servers and click on add button.

  Ex: Name: facebook.com

  IP address: 192.168.1.101

  Name: youtube.com

  IP address: 192.168.1.102
- Click on PC go to web browser, in the URL type facebook.com or youtube.com and observe the response



URL: http://facebook.com

Facebook

Welcome to Facebook.

Quick Links:
A small page
Copyrights
Image page
Image

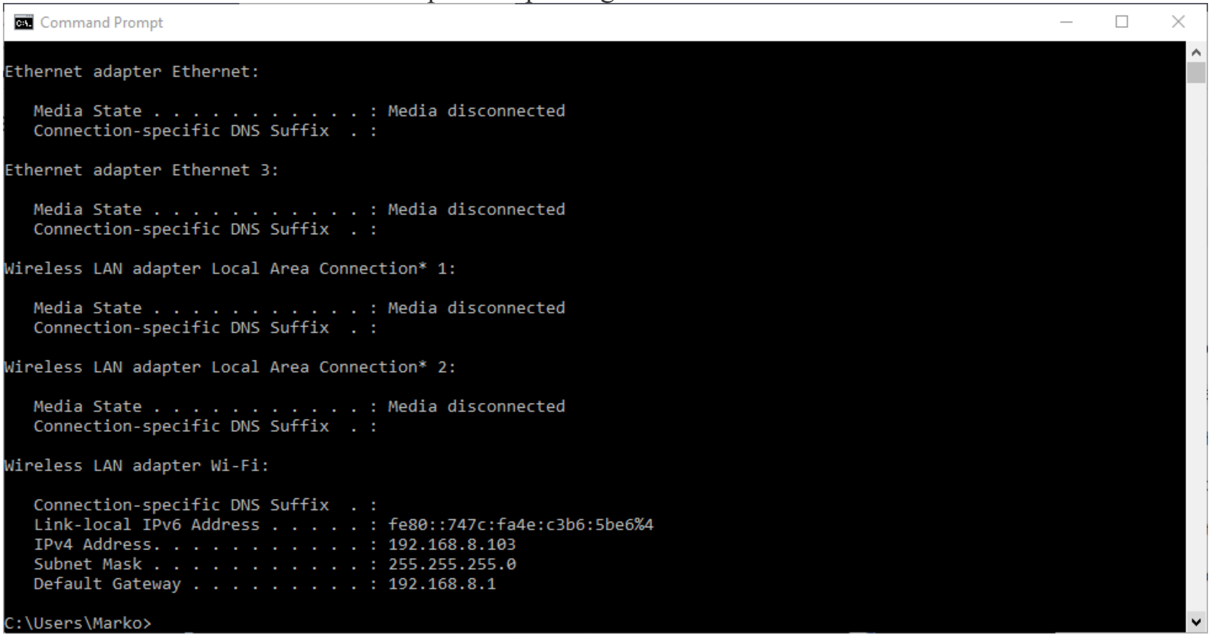
b) Observe DNS lookup using the nslookup command.

- Click on PC, go to Command prompt and type nslookup, press enter and Check the sever and its address

25 . Demonstrate troubleshooting Commands with a scenario-ipconfig, ping , netstat, tracert, nslookup.

A) ipconfig

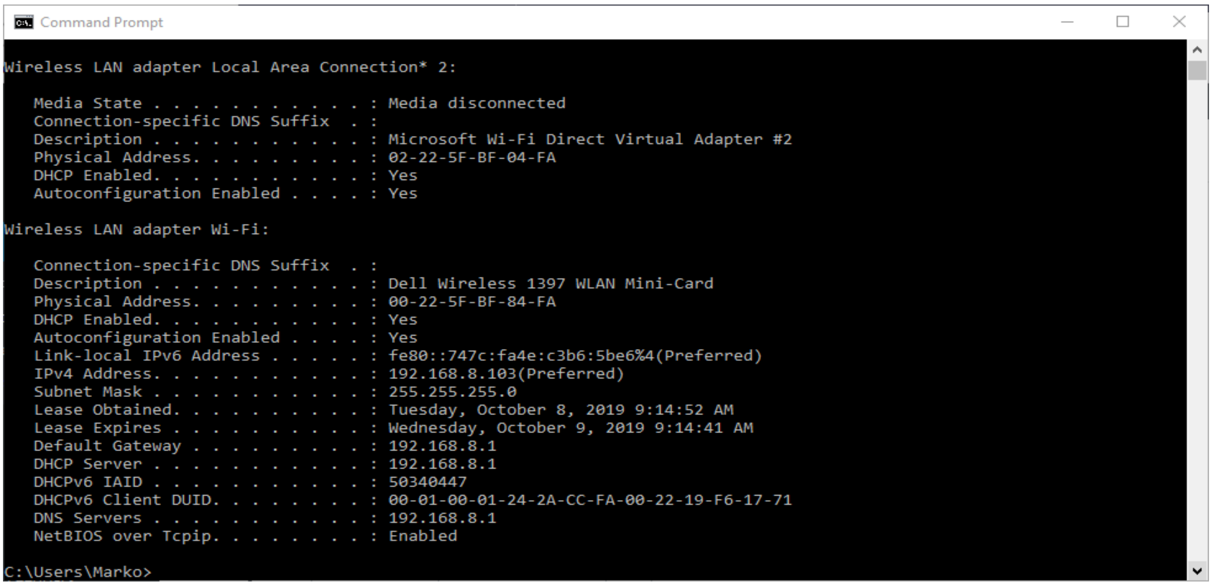
The “ipconfig” displays the current information about your network such as your your IP and MAC address, and the IP address of your router. It can also display information about your DHCP and DNS servers. Let’s see the basic output of “ipconfig”:



```
Ethernet adapter Ethernet:

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

Ethernet adapter Ethernet 3:

   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* 2:

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

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::747c:fa4e:c3b6:5be6%4
   IPv4 Address. . . . . . . . . . . : 192.168.8.103
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.8.1

C:\Users\Marko>
```

Depending on your network connection type, you may see different output for different connection. For example, if you are connected to the network using Ethernet (you plug in your network cable to the RJ45 jack), you’ll see IP information in the “Ethernet adapter” section. In our case we are connected to the WIFI (wireless) connection so we our information there. In our case, the local IP (IPv4) of our computer is 192.168.8.103. We also see the Subnet Mask (255.255.255.0) which we can use to find the network address. We also see the Default Gateway IP (192.168.8.1), which is our router

However, we don’t see DHCP and DNS information. To see detailed IP information we can use the “/all” switch together with “ipconfig” command (ipconfig /all).



```
Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
   Physical Address. . . . . . . . . : 02-22-5F-BF-04-FA
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Dell Wireless 1397 WLAN Mini-Card
   Physical Address. . . . . . . . . : 00-22-5F-BF-84-FA
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::747c:fa4e:c3b6:5be6%4(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.8.103(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Tuesday, October 8, 2019 9:14:52 AM
   Lease Expires . . . . . . . . . . : Wednesday, October 9, 2019 9:14:41 AM
   Default Gateway . . . . . . . . . : 192.168.8.1
   DHCP Server . . . . . . . . . . . : 192.168.8.1
   DHCPv6 IAID . . . . . . . . . . . : 50340447
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-24-2A-CC-FA-00-22-19-F6-17-71
   DNS Servers . . . . . . . . . . . : 192.168.8.1
   NetBIOS over Tcpip. . . . . . . . : Enabled

C:\Users\Marko>
```

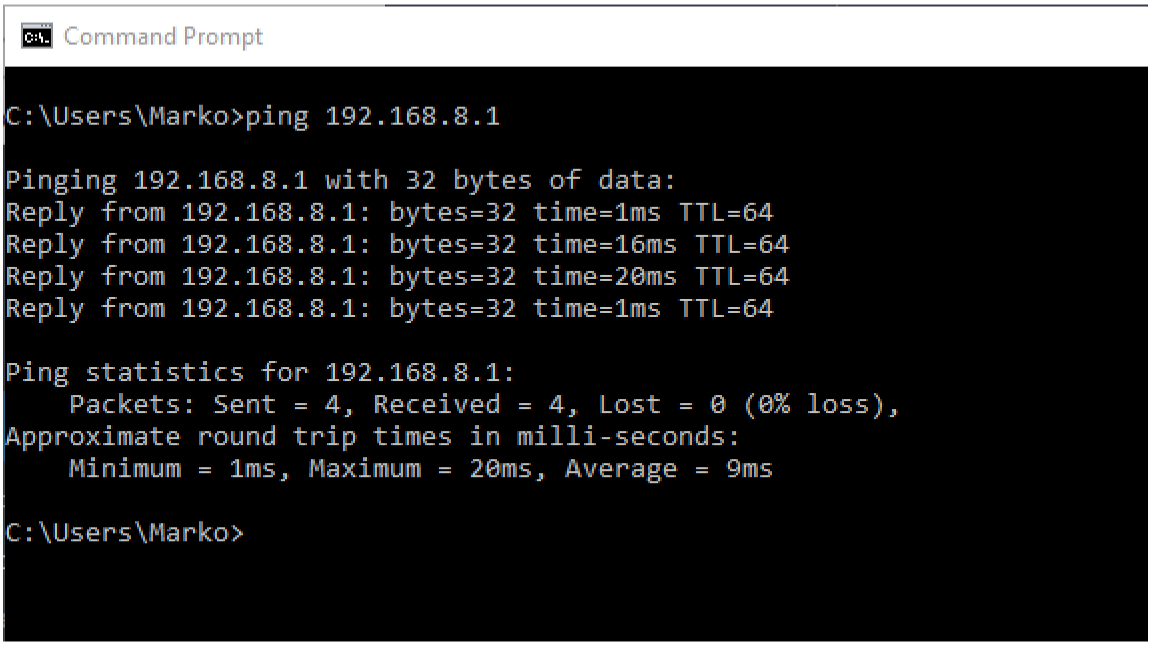
This time there’s much more information present. The IP address, the Subnet Mask and and the Default Gateway address is still here, but this time you can also see your DHCP server and DNS server. In our case the DHCP IP address is the same as the router address, which means that DHCP server is currently residing on the router. DNS server is also the same as router address which means it is also DNS server.

Information gathering is a part of troubleshooting. For example, if you’re trying to troubleshoot the DNS server, you can beforehand type in the “ipconfig” command and find where the DNS server is.

Network troubleshooting with ping

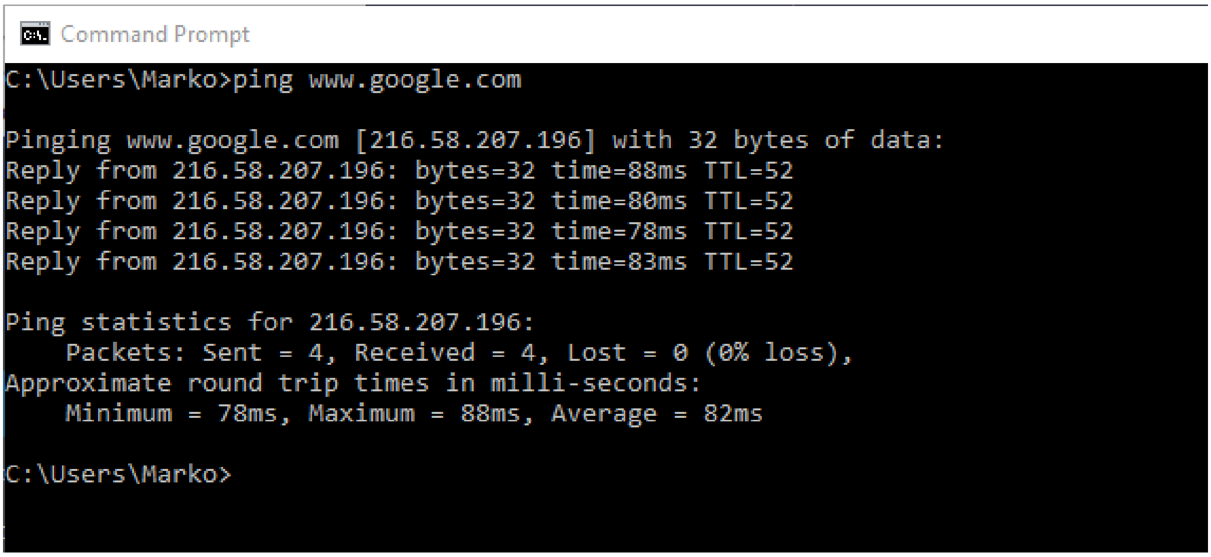
The “ping” command ping command allows you to send a signal to another device, and if that device is active, it will send a response back to the sender. The “ping” command is a subset of the ICMP (Internet Control Message Protocol), and it uses what is called an “echo request”. So, when you ping a device you send out an echo request, and if the device you pinged is active or online, you get an echo response.

For example, if your local computer has Internet connectivity issues, you can try to ping your router. If you get no response then you know that the router is what is giving you problems. Let’s ping our router IP, which is 192.168.8.1 in our example, and let’s analyze the the printout.



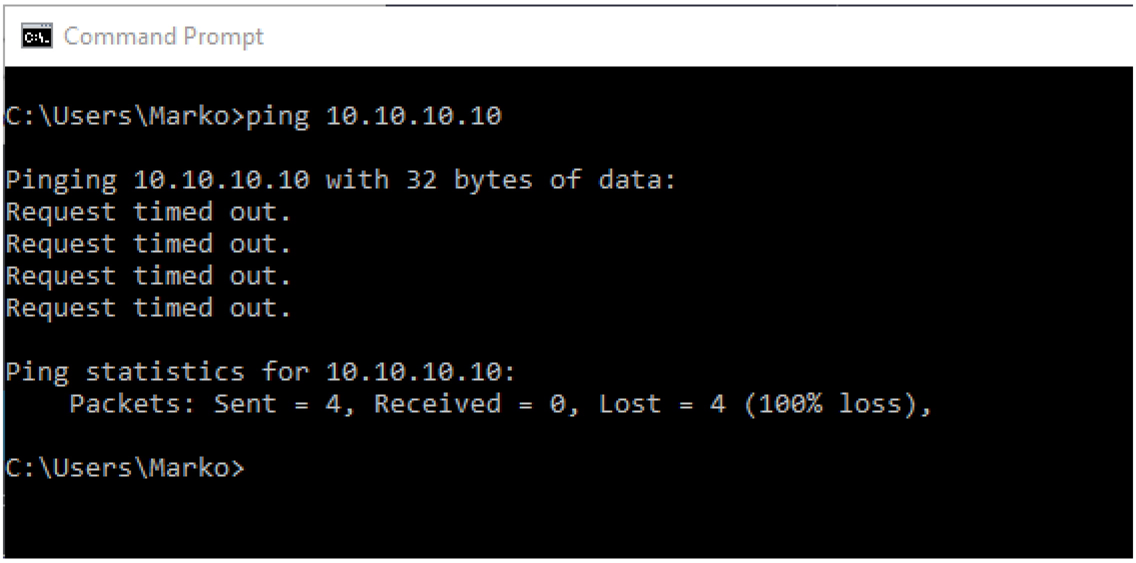
```
C:\Users\Marko>ping 192.168.8.1

Pinging 192.168.8.1 with 32 bytes of data:
Reply from 192.168.8.1: bytes=32 time=1ms TTL=64
Reply from 192.168.8.1: bytes=32 time=16ms TTL=64
Reply from 192.168.8.1: bytes=32 time=20ms TTL=64
Reply from 192.168.8.1: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.8.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 20ms, Average = 9ms

C:\Users\Marko>
```

What happens is we send out four packets to the destination and the destination responds back with the same four packets. We sent out 32 bytes of data and we got back 32 bytes of data, and we got it back in 9 milliseconds average. From this we see that the device is alive and see the connection stability (4 of 4 packets received). Let us ping www.google.com and see what happens.



```
C:\Users\Marko>ping www.google.com

Pinging www.google.com [216.58.207.196] with 32 bytes of data:
Reply from 216.58.207.196: bytes=32 time=88ms TTL=52
Reply from 216.58.207.196: bytes=32 time=80ms TTL=52
Reply from 216.58.207.196: bytes=32 time=78ms TTL=52
Reply from 216.58.207.196: bytes=32 time=83ms TTL=52

Ping statistics for 216.58.207.196:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 78ms, Maximum = 88ms, Average = 82ms

C:\Users\Marko>
```

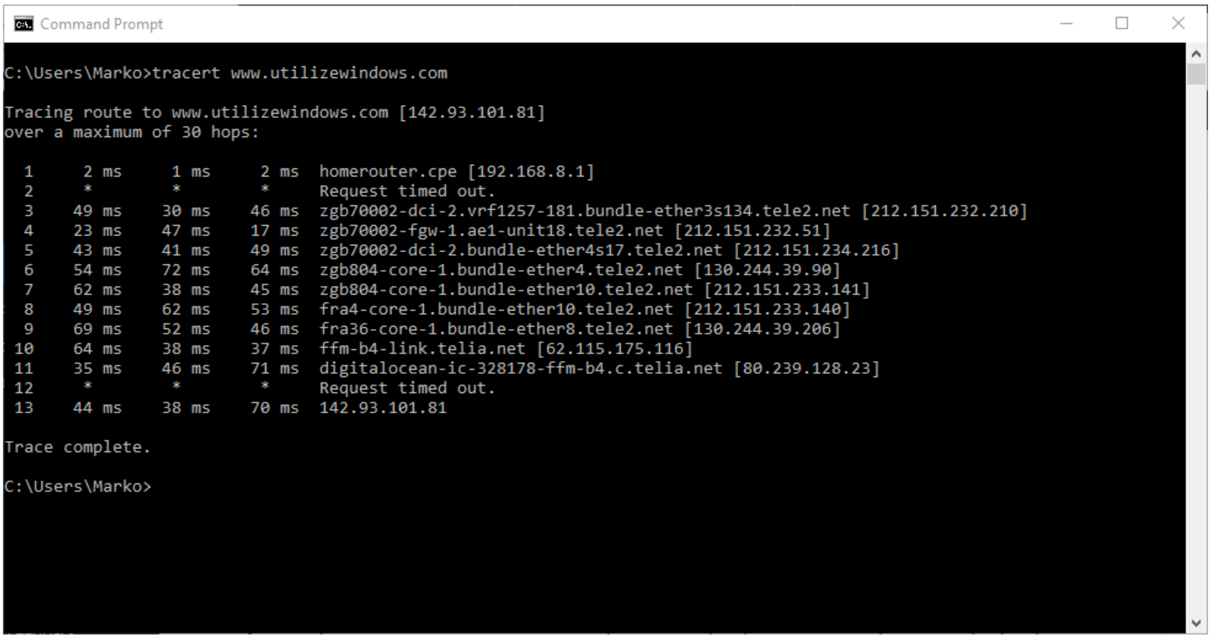
We got a similar printout, however, since we used domain name, we now see the resolved IP address of www.google.com. We sent out 32 bytes of data but, because Google server is far away it took 82 milliseconds to send and receive 4 packets from Google. We sent and received 4 packets so the connection was stable. Finally let’s ping a device that doesn’t exist.



```
C:\Users\Marko>ping 10.10.10.10

Pinging 10.10.10.10 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.10.10.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Marko>
```

Tracert

This command lets you see all steps a packet takes to the destination. For example, if we send a packet to www.google.com, it actually goes through a couple of routers to reach the destination. The packet will first go to your router, and then it will go to all kinds of different routers before it reaches Google servers. We can also use the term “hops” instead of routers. Let’s run the command and see what kind of results we get.



```
C:\Users\Marko>tracert www.utilizewindows.com

Tracing route to www.utilizewindows.com [142.93.101.81]
over a maximum of 30 hops:

  1     2 ms     1 ms     2 ms  homerouter.cpe [192.168.8.1]
  2     *        *        *     Request timed out.
  3    49 ms    30 ms    46 ms  zgb70002-dci-2.vrf1257-181.bundle-ether3s134.tele2.net [212.151.232.210]
  4    23 ms    47 ms    17 ms  zgb70002-fgw-1.ae1-unit18.tele2.net [212.151.232.51]
  5    43 ms    41 ms    49 ms  zgb70002-dci-2.bundle-ether4s17.tele2.net [212.151.234.216]
  6    54 ms    72 ms    64 ms  zgb804-core-1.bundle-ether4.tele2.net [130.244.39.90]
  7    62 ms    38 ms    45 ms  zgb804-core-1.bundle-ether10.tele2.net [212.151.233.141]
  8    49 ms    62 ms    53 ms  fra4-core-1.bundle-ether10.tele2.net [212.151.233.140]
  9    69 ms    52 ms    46 ms  fra36-core-1.bundle-ether8.tele2.net [130.244.39.206]
 10    64 ms    38 ms    37 ms  ffm-b4-link.telia.net [62.115.175.116]
 11    35 ms    46 ms    71 ms  digitalocean-ic-328178-ffm-b4.c.telia.net [80.239.128.23]
 12     *        *        *     Request timed out.
 13    44 ms    38 ms    70 ms  142.93.101.81

Trace complete.

C:\Users\Marko>
```

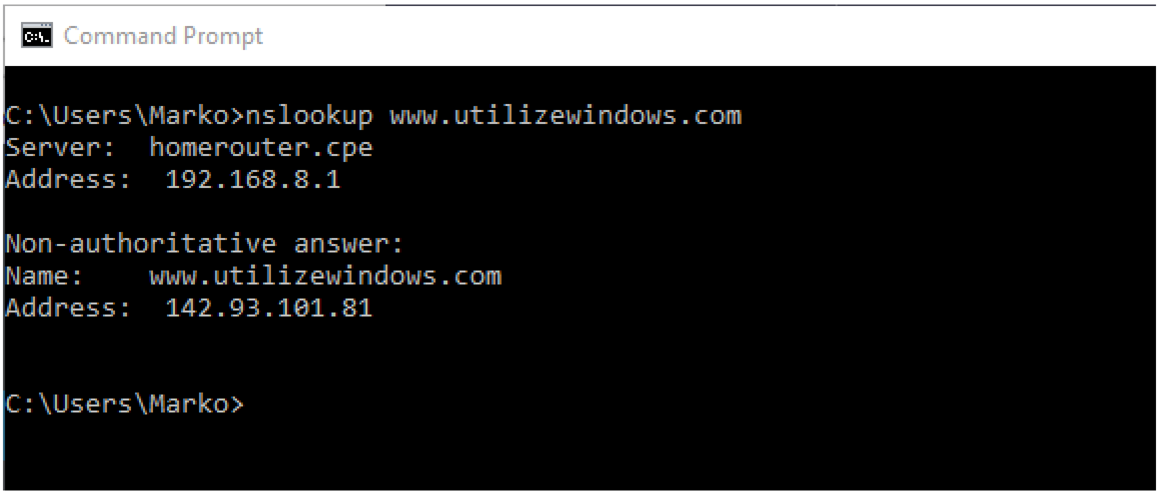
We have traced the route to www.utilizewindows.com, and we’re getting a list of each of the routers that we’re hitting. At the end we see the IP address for utilizewindows.com server so the trace is complete. In our case we have 13 hops before we actually reached the intended server. The first router that we hit was our own router (we can tell by the IP address 192.168.8.1). So what is the significance of this? Let’s say your home network was perfectly fine but there was a problem with some router in the between, for example with your ISP router. If there’s any problems it will try to indicate what the problem is. It could say things like “request timed out”, “destination unreachable” or similar. However, different messages don’t necessarily mean that there is a real problem with the device. There are several reasons why a “Request timed out” message may appear at the end of a trace route.

This is typically because a device doesn't respond to ICMP or traceroute requests. Also, the device firewall or other security device could be blocking the request.

nslookup :

The nslookup command will fetch the DNS records for a given domain name or an IP address. Remember the IP addresses and domain names are stored in DNS servers, so the nslookup command lets you query the DNS records to gather information.

Let's say you wanted to know the IP address of www.utilizewindows.com. You could simply type in nslookup and type in www.utilizewindows.com. Let's analyze this printout.



```
C:\Users\Marko>nslookup www.utilizewindows.com
Server:  homerouter.cpe
Address:  192.168.8.1

Non-authoritative answer:
Name:    www.utilizewindows.com
Address:  142.93.101.81


C:\Users\Marko>
```

The first two lines show you which DNS server was used to get these results. Our DNS server happens to reside on our router, so our router is also our DNS server. The answer that we got was the IP address of the www.utilizewindows.com server.