PRACTICAL LAB FILE

Computer Networks Lab

(ITC-408)

Submitted To:

Dr. Bhoopesh Singh Bhati

(Assistant Professor)

Submitted By:

Tanish Sharma

Roll no:-12112011

Semester 4th

Branch-IT

INDIAN INSTITUTE OF INFORMATION TECHNOLOGY
SONEPAT

(May,2023)

Index

Experiment#1

Aim: Study of different types of Network cables and practically implement the cross-wired cable and straight through cable using crimping tool.

Apparatus (Components): RJ-45 connector, Crimping Tool, Twisted pair Cable

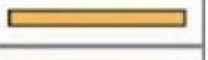
Procedure: To do these practical following steps should be done:

1. Start by stripping off about 2 inches of the plastic jacket off the end of the cable. Be very careful at this point, as to not nick or cut into the wires, which are inside. Doing so could alter the characteristics of your cable, or even worse render is useless. Check the wires, one more time for nicks or cuts. If there are any, just whack the whole end off, and start over.
2. Spread the wires apart, but be sure to hold onto the base of the jacket with your other hand. You do not want the wires to become untwisted down inside the jacket. Category 5 cable must only have 1/2 of an inch of 'untwisted' wire at the end; otherwise it will be 'out of spec'. At this point, you obviously have A LOT more than 1/2 of an inch of un-twisted wire.
3. You have 2 end jacks, which must be installed on your cable. If you are using a premade cable, with one of the ends whacked off, you only have one end to install - the crossed over end. Below are two diagrams, which show how you need to arrange the cables for each type of cableend. Decide at this point which end you are making and examine the associated picture below.

Colour Coding to prepare Cross wired connection

RJ45 Pin # (END 1)	Wire Color	Diagram End #1	RJ45 Pin # (END 2)	Wire Color	Diagram End #2
1	White/Orange		1	White/Green	
2	Orange		2	Green	
3	White/Green		3	White/Orange	
4	Blue		4	White/Brown	
5	White/Blue		5	Brown	
6	Green		6	Orange	
7	White/Brown		7	Blue	
8	Brown		8	White/Blue	

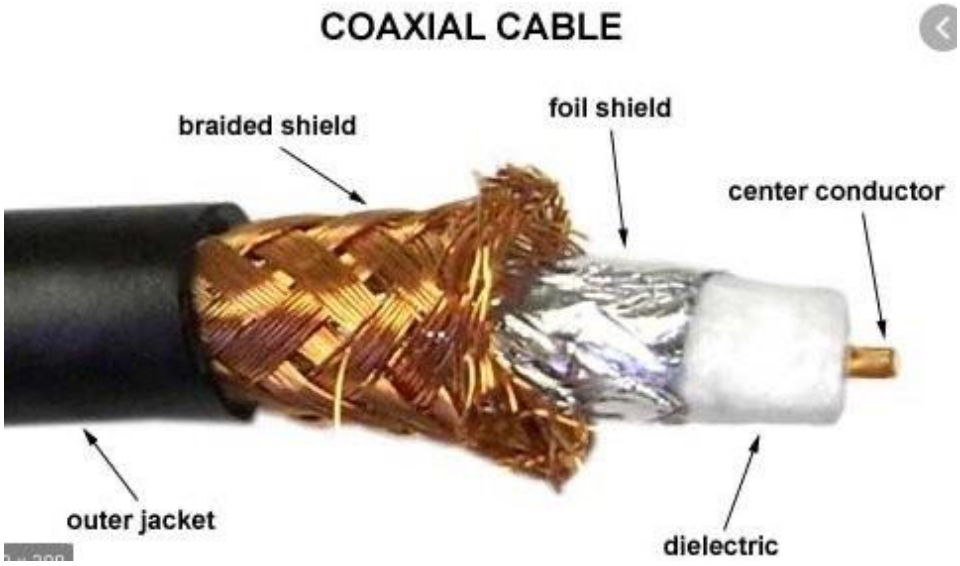
Colour Coding to prepare straight through wired connection

RJ45 Pin # (END 1)	Wire Color	Diagram End #1	RJ45 Pin # (END 2)	Wire Color	Diagram End #2
1	White/Orange		1	White/Green	
2	Orange		2	Green	
3	White/Green		3	White/Orange	
4	Blue		4	White/Brown	
5	White/Blue		5	Brown	
6	Green		6	Orange	
7	White/Brown		7	Blue	
8	Brown		8	White/Blue	

Different types of Network Cables:

(i)Coaxial Cables:

- This cable contains a conductor, insulator, braiding and sheath.The sheath covers the braiding, braiding covers the insulation, and the insulation covers the conductor.
- This cable is used to carry high-frequency electrical signals with low losses. It uses 10Base2 and 10Base5 Ethernetvariants.
- Coaxial cable uses RG rating to measure the materials used in shielding and conducting cores. RG stands for the Radio Guide.
- These wires have a copper conductor in the middle that is surrounded by a dielectric insulator usually made of PVC or Teflon. The dielectric insulator is surrounded by a braided conducting metallic shield which reduces EMI (Electromagnetic Interference) of the metal and outside interference; and finally, the metallic shield is covered by a plastic covering called a sheath usually made of PVC or someother fire-resistant plastic material.
- Its maximum transmission speed is 10 Mbps.
- It is usually used in telephone systems, cable TV, etc.

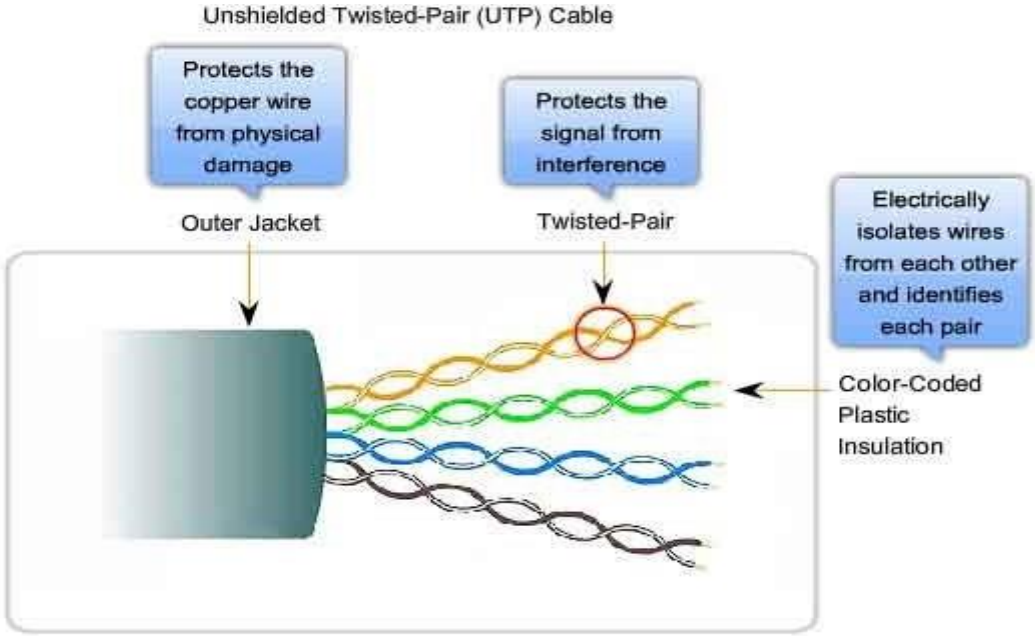


(ii) Twisted-Pair Cables:

- Twisted pair cables have two conductors that are generally made up of copper and each conductor has insulation. Thesetwo conductors are twisted together, thus giving the name twisted pair cables.
- This cable is also known as Ethernet cable. Almost all modernLAN computer networks use this cable.
- Two types of twisted-pair cable:

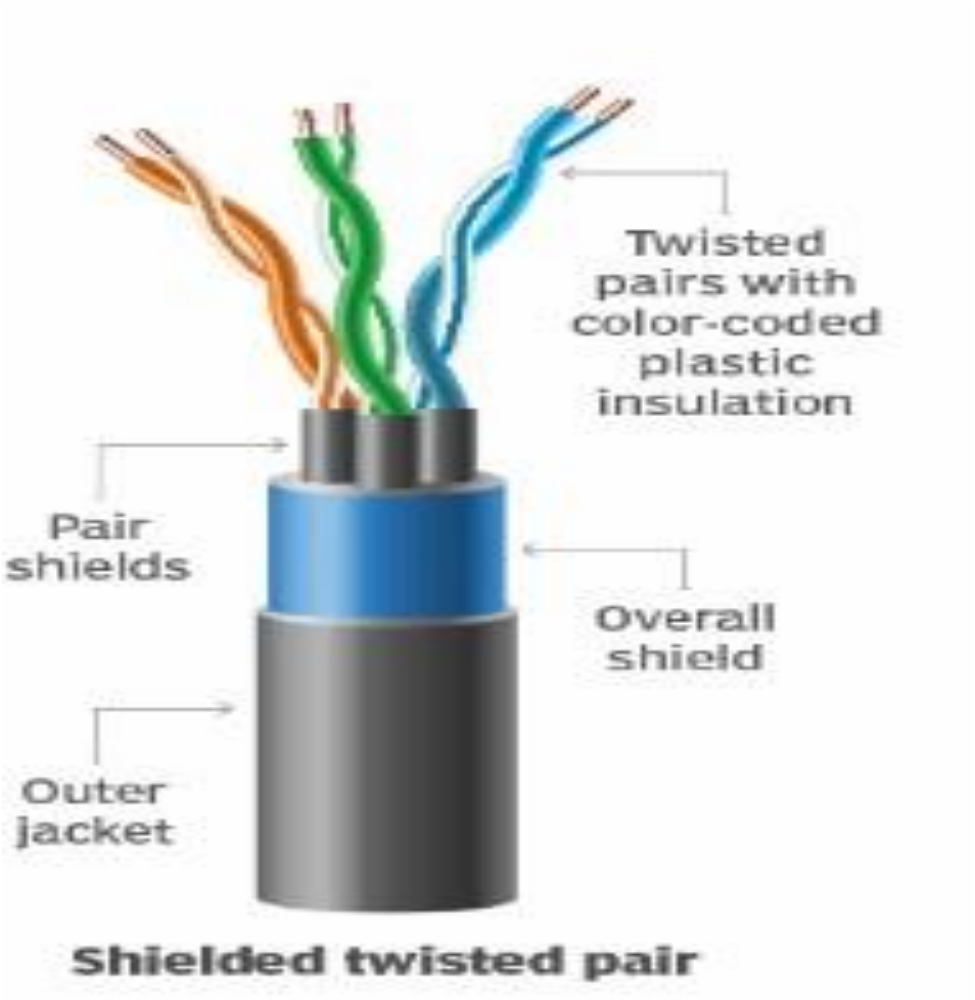
(a)Unshielded Twisted Pair Cables (UTP) :

- These are a pair of two insulated copper wires twisted together without any other insulation or shielding and henceare called unshielded twisted pair cables. They reduce the external interference due to the presence of insulation.
- These cables are cost-effective and easy to install owing totheir compact size.
- The connection established using UTP is not secure.
- They are generally used for short-distance transmission ofboth data and voice.
- These cables have limited bandwidth.



(b) Shielded Twisted Pair Cables (STP) :

- These are the cables that have been twisted together and enclosed in some sort of shield, whether it be foil or mesh.These shields protect the wires from electromagnetic interference.
- They are generally used for long-distance communication and transmission and are installed underground.
- They have a higher bandwidth as compared to UTP.
- These cables are very expensive.



Shielded twisted pair

Crimping Tool:

- Cable crimping is a process of joining wires to another metal terminal. When crimping, the terminal will be compressed to connect to the wire conductor.
- An RJ45 crimping tool is a device used in the networking system. It is a good helper for you to crimp and terminate RJ45 plugs.
- An RJ45 crimping tool is a special device for the installation of different cabling systems. It usually features a compact design that is practical and easy to use.
- It also provides a solid connection between RJ45 connector to the Ethernet cable.

Experiment#2

Aim: To Design Different Types of Topologies in Computer Networks

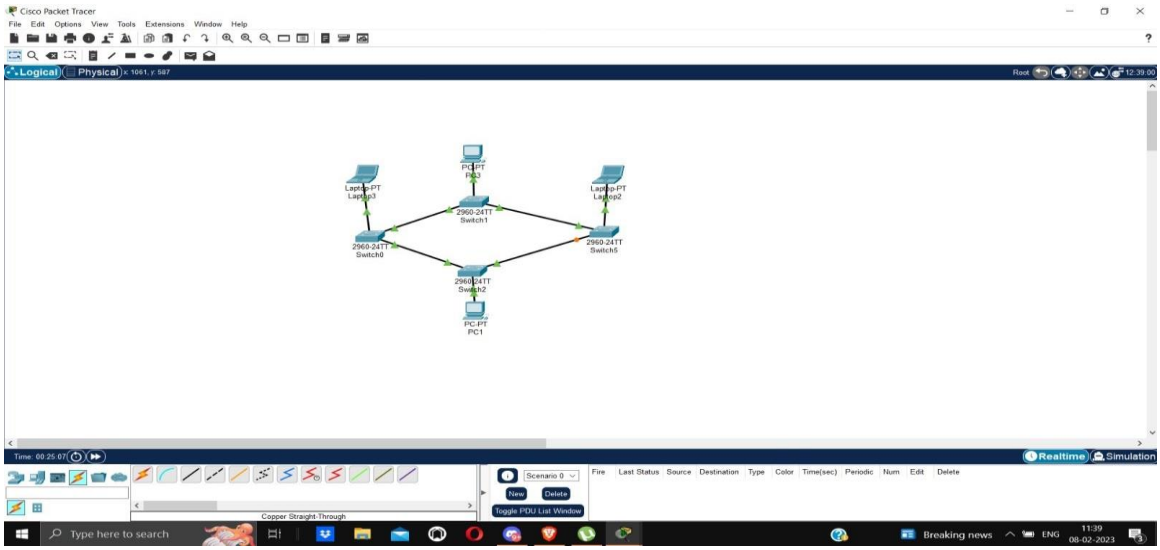
Apparatus (Components): Switch, PC, Laptop, Copper Straight-Through Wire

Different types of Topologies in Computer Network:

(i) Ring Topology:

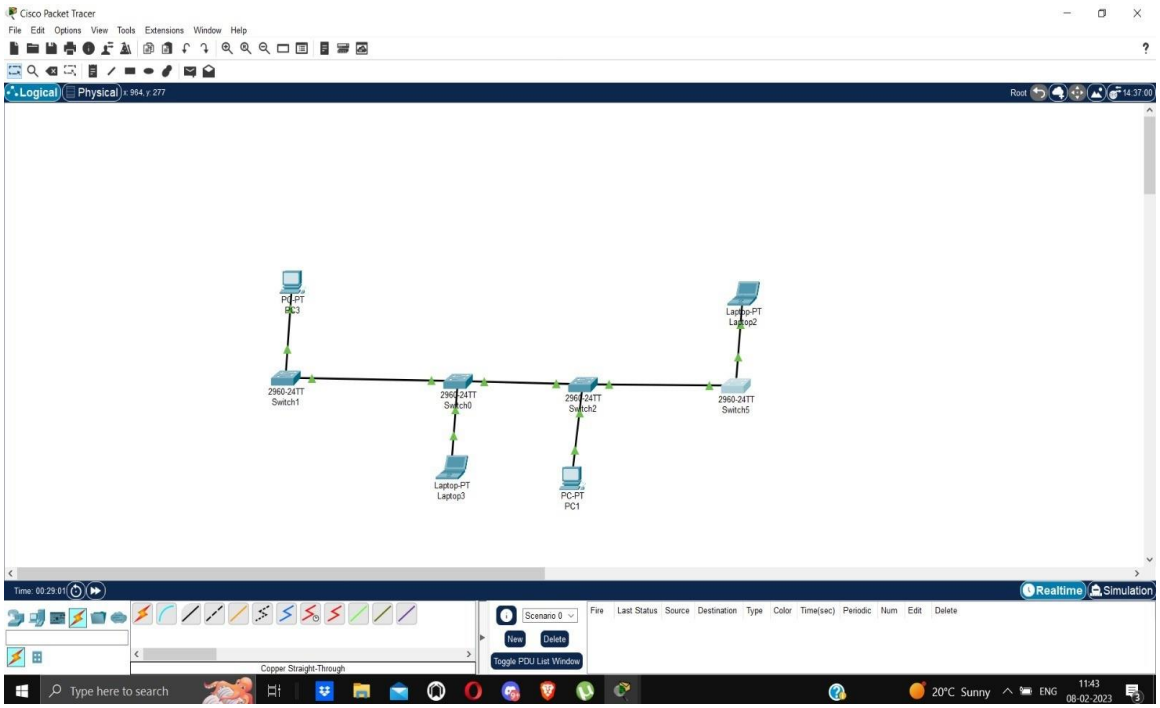
- A ring topology is a network architecture in which devicesare connected in a ring structure and send information to each other based on their ring node's neighboring node.
- Depending on the network card used in each computer, an RJ-45 network cable or a coaxial cable is used to connect computers in a ring topology.
- The advantages of a ring topology include, it does not needa central hub in order to function.
- Installation and troubleshooting with this type of network are also very easy as compared to other networks.
- A ring architecture has the drawback that if one node fails to send data, the entire network suffers.
- In the telecommunications industry, ring topology is commonly utilized in SONET (Synchronous optical network)

fiber networks.



(ii) Bus Topology:

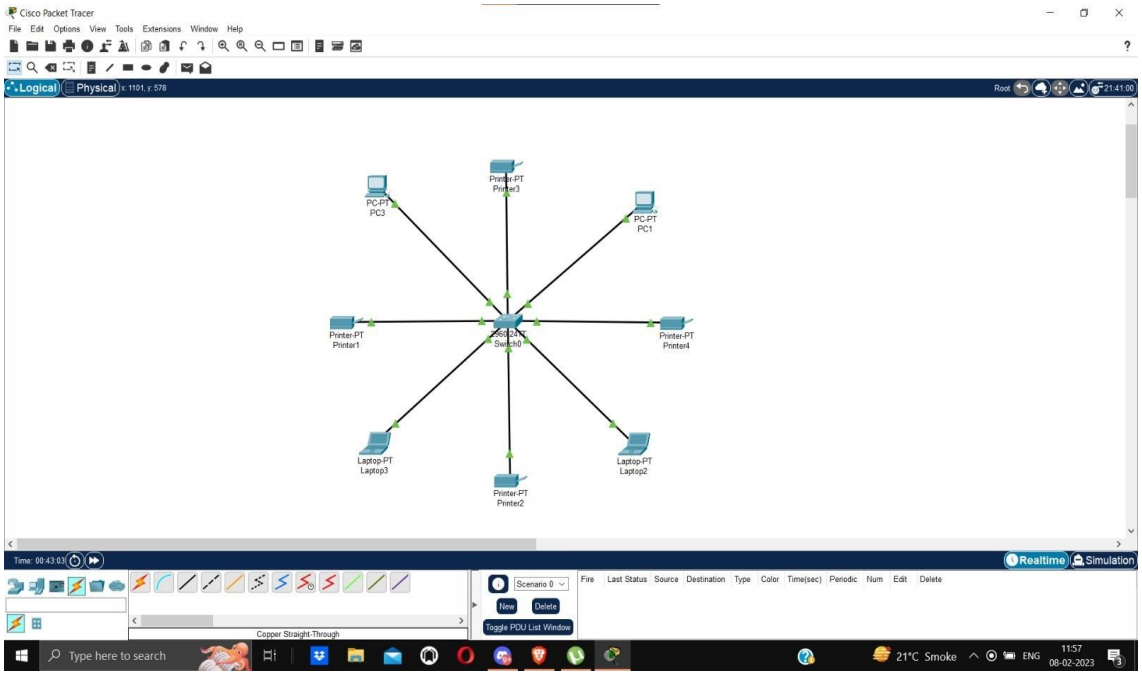
- The bus topology is designed in such a way that all the stations are connected through a single cable known as a **backbone cable**. Each node is either connected to the backbone cable by drop cable or directly connected to the backbone cable.
- When a node wants to send a message over the network, it puts a message over the network. All the stations availablein the network will receive the message whether it has been addressed or not.
- In bus topology, nodes are directly connected to the cable without passing through a hub. Therefore, the initial cost of installation is low.
- Coaxial or twisted pair cables are mainly used in bus-based networks that support upto 10 Mbps.
- It requires specialized test equipment to determine the cable faults. If any fault occurs in the cable, then it would disrupt the communication for all the nodes.
- Adding new devices to the network would slow down the network.



(ii) Star Topology:

- Star topology is an arrangement of the network in which every node is connected to the central hub, switch or acentral computer.
- The central computer is known as a server, and the peripheral devices attached to the server are known as clients.
- Coaxial cable or RJ-45 cables are used to connect the computers.
- As each station is connected to the central hub with its own cable, therefore failure in one cable will not affect the entire network.
- Star topology networks are cost-effective as they use inexpensive coaxial cable.
- It supports a bandwidth of approx 100Mbps. Ethernet 100BaseT is one of the most popular Star topology networks.
- If the central hub or switch goes down, then all the connected nodes will not be able to communicate with each

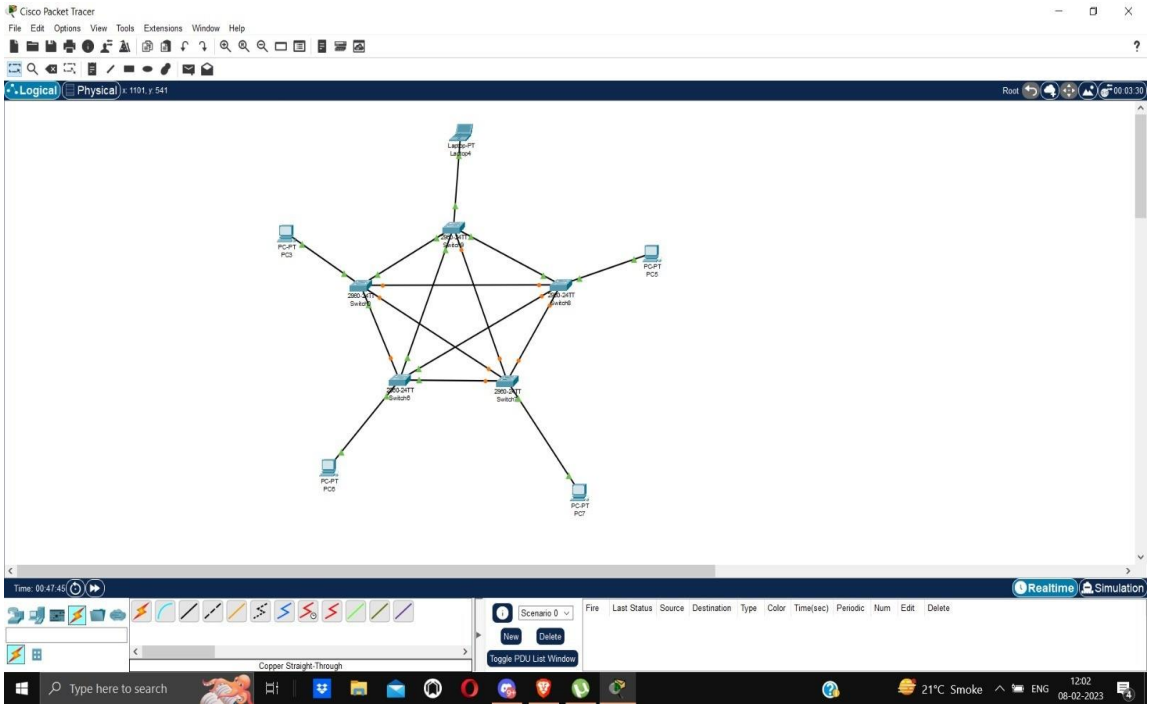
other.



(iv) Mesh Topology:

- Mesh technology is an arrangement of the network in which computers are interconnected with each other through various redundant connections.
- It does not contain the switch, hub or any central computer which acts as a central point of communication.
- The Internet is an example of the mesh topology.
- The mesh topology networks are very reliable as if any link breakdown will not affect the communication betweenconnected computers.
- Communication is very fast between the nodes.
- A mesh topology contains a large number of connected devices such as a router and more transmission media than other topologies.

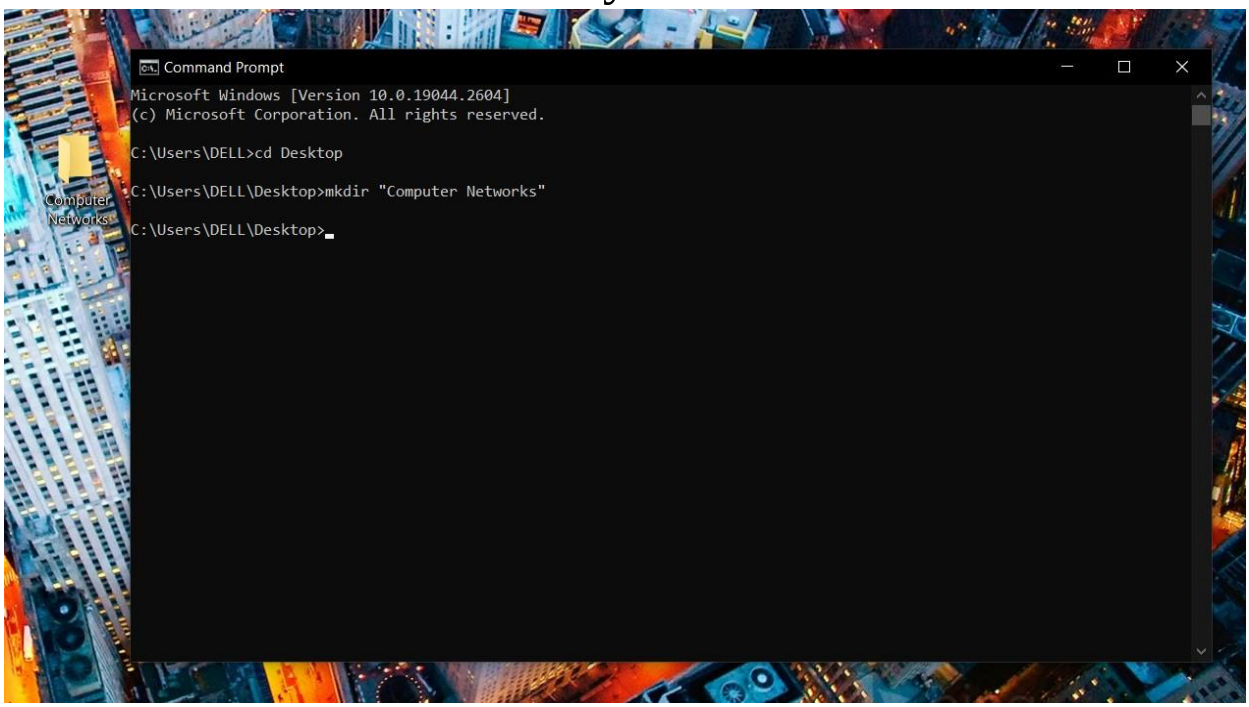
- Mesh topology networks are very large and very difficult to maintain and manage.



Experiment#3

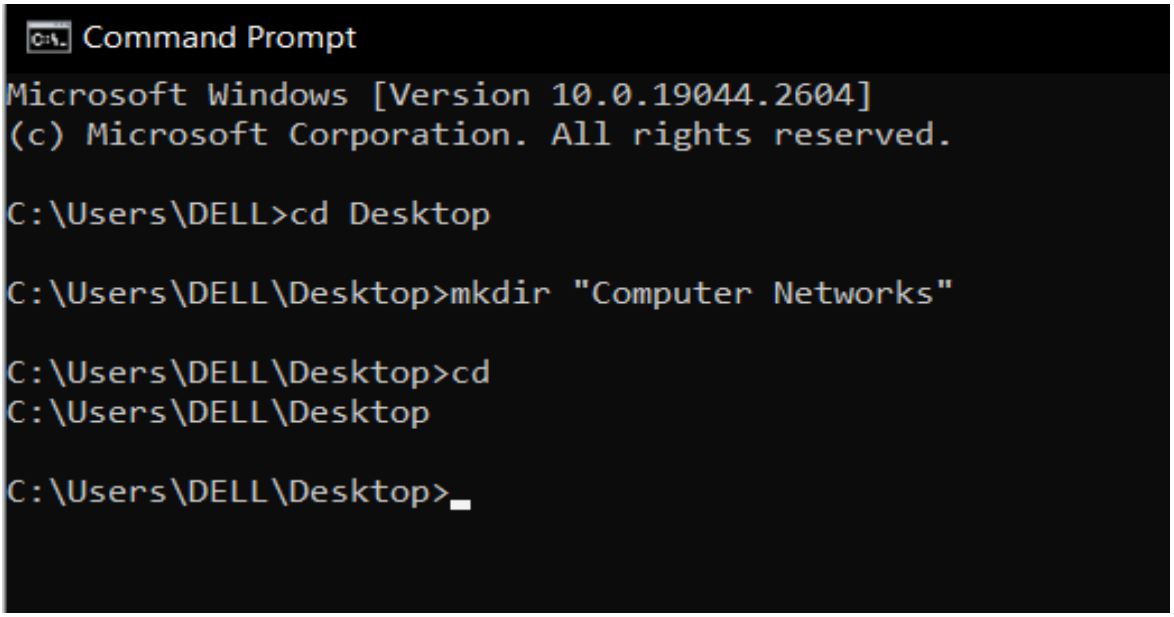
Aim: Study the basic network command and Network configuration commands

1. mkdir
   - Makes a New Directory

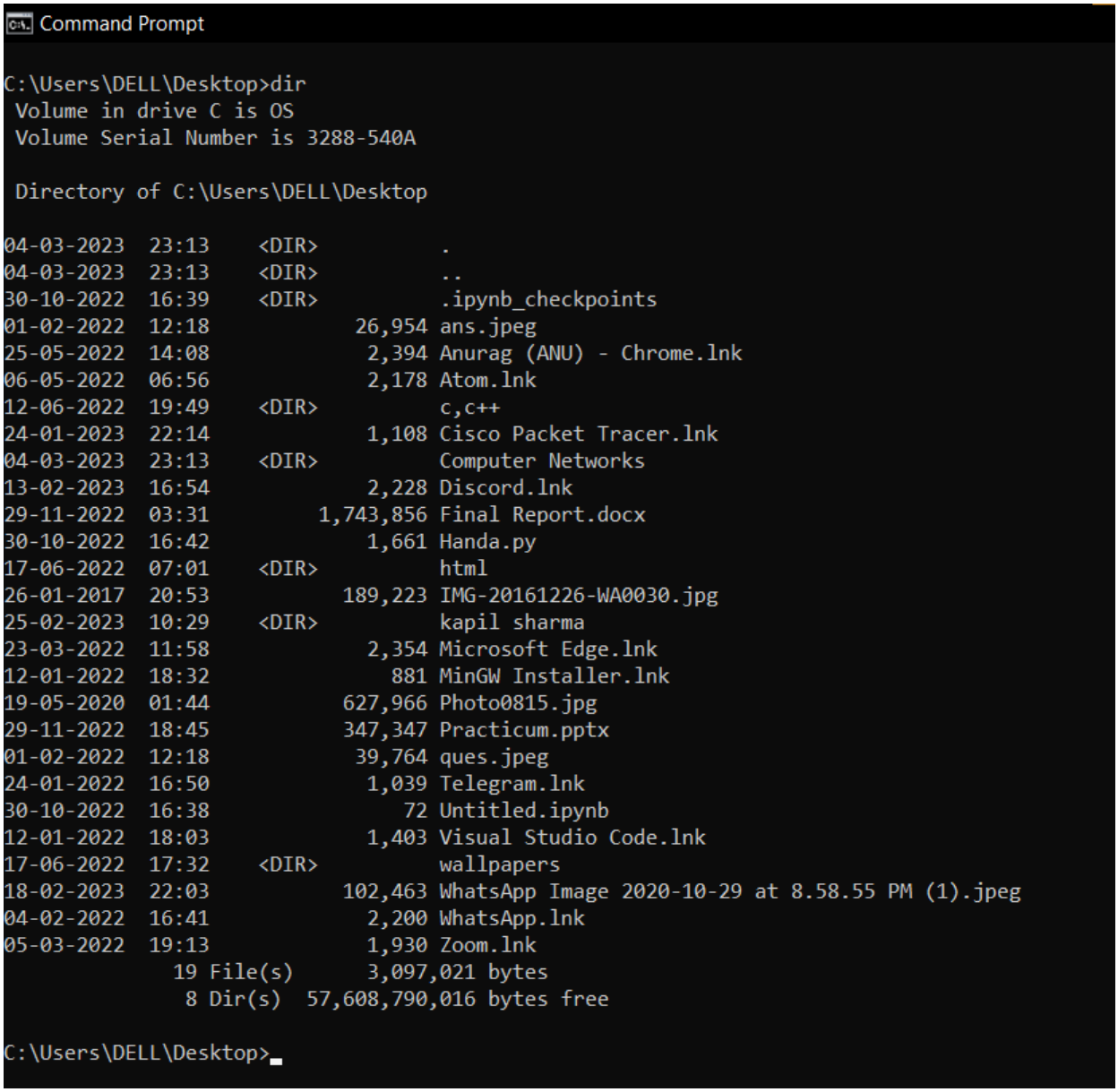


New folder/directory named Computer Networkscreated on desktop.

2. cd (on Windows)
   pwd (on Mac/Linux)
   -prints the current working directory.



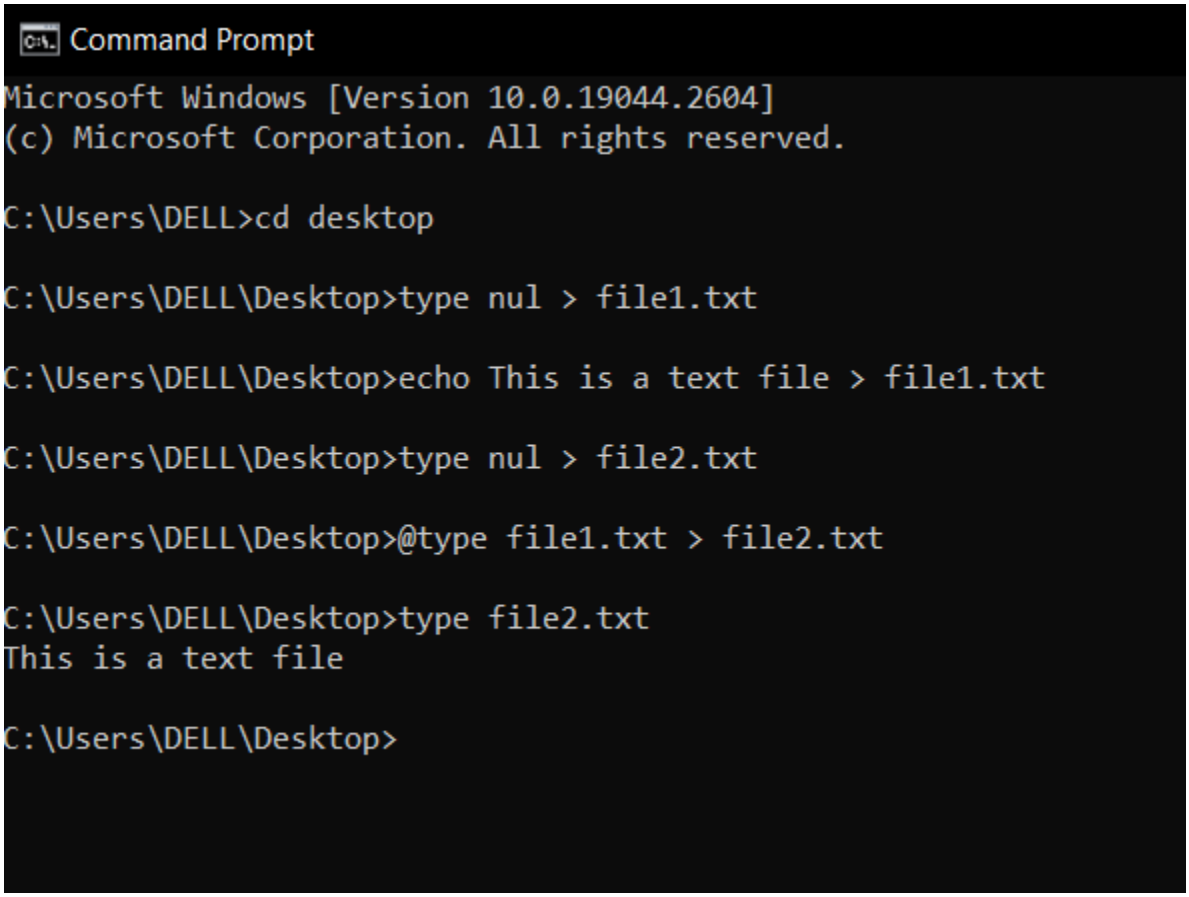
3. dir (on Windows)
   ls (on Mac/Linux)
   -list of files and directory



4. help (on Windows)
   man (on Mac/Linux)
   - Prints man page of provided commands.

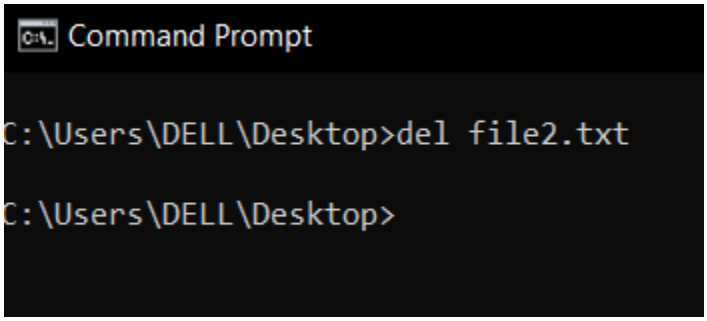

Command Prompt
C:\Users\DELL\Desktop>help
For more information on a specific command, type HELP command-name
ASSOC Displays or modifies file extension associations.
ATTRIB Displays or changes file attributes.
BREAK Sets or clears extended CTRL+C checking.
BCDEDIT Sets properties in boot database to control boot loading.
CACLS Displays or modifies access control lists (ACLs) of files.
CALL Calls one batch program from another.
CD Displays the name of or changes the current directory.
CHCP Displays or sets the active code page number.
CHDIR Displays the name of or changes the current directory.
CHKDSK Checks a disk and displays a status report.
CHKNTFS Displays or modifies the checking of disk at boot time.
CLS Clears the screen.
CMD Starts a new instance of the Windows command interpreter.
COLOR Sets the default console foreground and background colors.
COMP Compares the contents of two files or sets of files.
COMPACT Displays or alters the compression of files on NTFS partitions.
CONVERT Converts FAT volumes to NTFS. You cannot convert the
current drive.
COPY Copies one or more files to another location.
DATE Displays or sets the date.
DEL Deletes one or more files.
DIR Displays a list of files and subdirectories in a directory.
DISKPART Displays or configures Disk Partition properties.
DOSKEY Edits command lines, recalls Windows commands, and
creates macros.
DRIVERQUERY Displays current device driver status and properties.
ECHO Displays messages, or turns command echoing on or off.
ENDLOCAL Ends localization of environment changes in a batch file.
ERASE Deletes one or more files.
EXIT Quits the CMD.EXE program (command interpreter).
FC Compares two files or sets of files, and displays the
differences between them.
FIND Searches for a text string in a file or files.
FINDSTR Searches for strings in files.
FOR Runs a specified command for each file in a set of files.
FORMAT Formats a disk for use with Windows.
FSUTIL Displays or configures the file system properties.
FTYPE Displays or modifies file types used in file extension
associations.
GOTO Directs the Windows command interpreter to a labeled line in
a batch program.
GPRESULT Displays Group Policy information for machine or user.
GRAFTABL Enables Windows to display an extended character set in
graphics mode.
HELP Provides Help information for Windows commands.
ICACLS Display, modify, backup, or restore ACLs for files and
directories.
IF Performs conditional processing in batch programs.

5. @type file1 > file2 (on Windows)
   cp file1 file2(on Mac/Linux)
   - It copies the content of file 1 into file2.

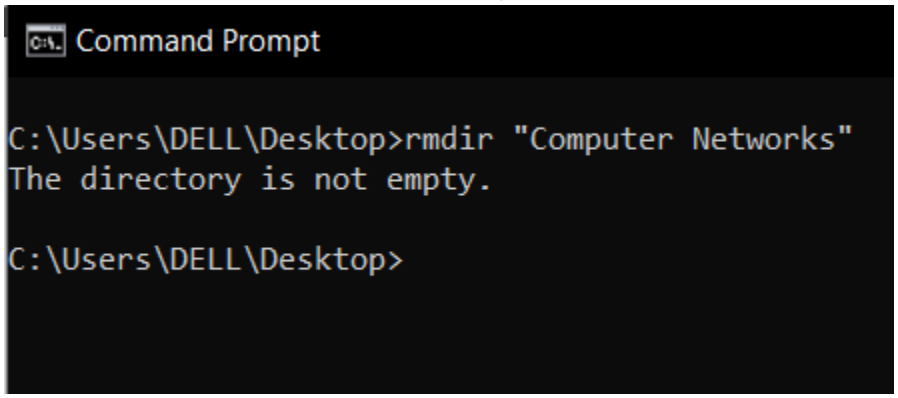


6. move (on Windows)
   mv (on Mac/Linux)
   - It moves the file to other folder and deletes the original file.

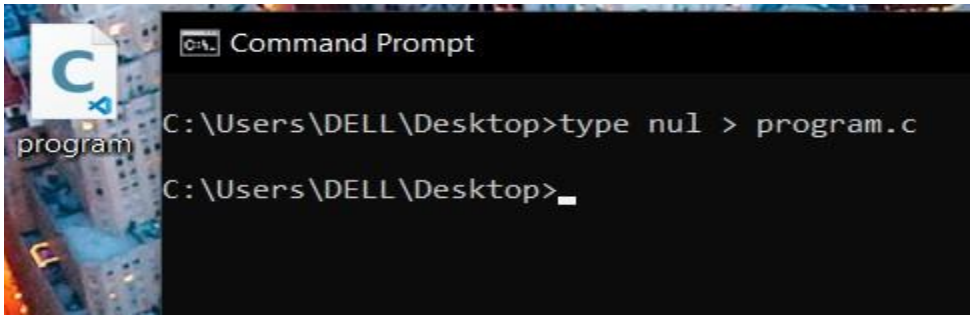
7. del (on Windows)
   rm (on Mac/Linux)
   -It deletes the file.



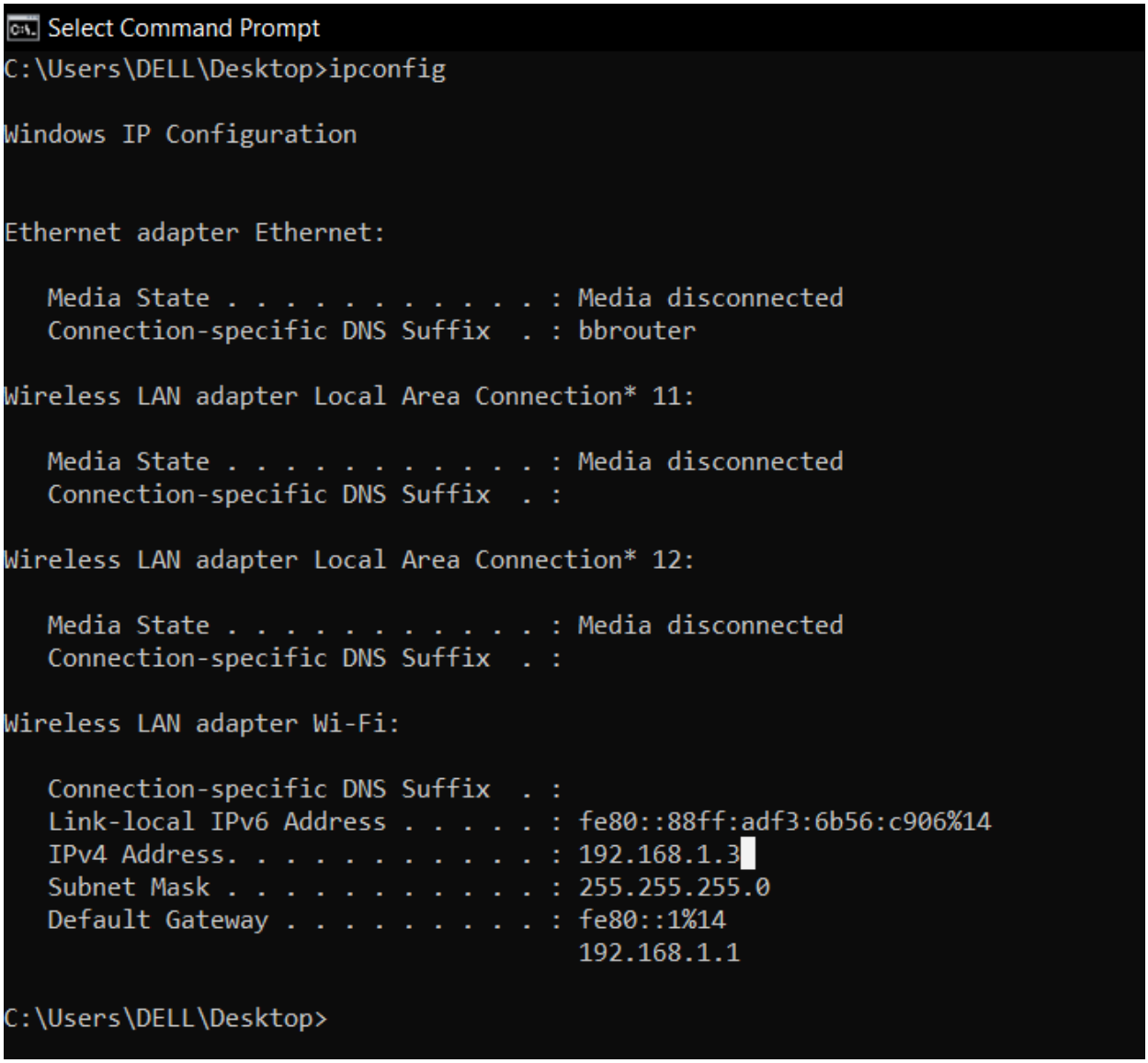
8. rmdir
   -removes the directory.



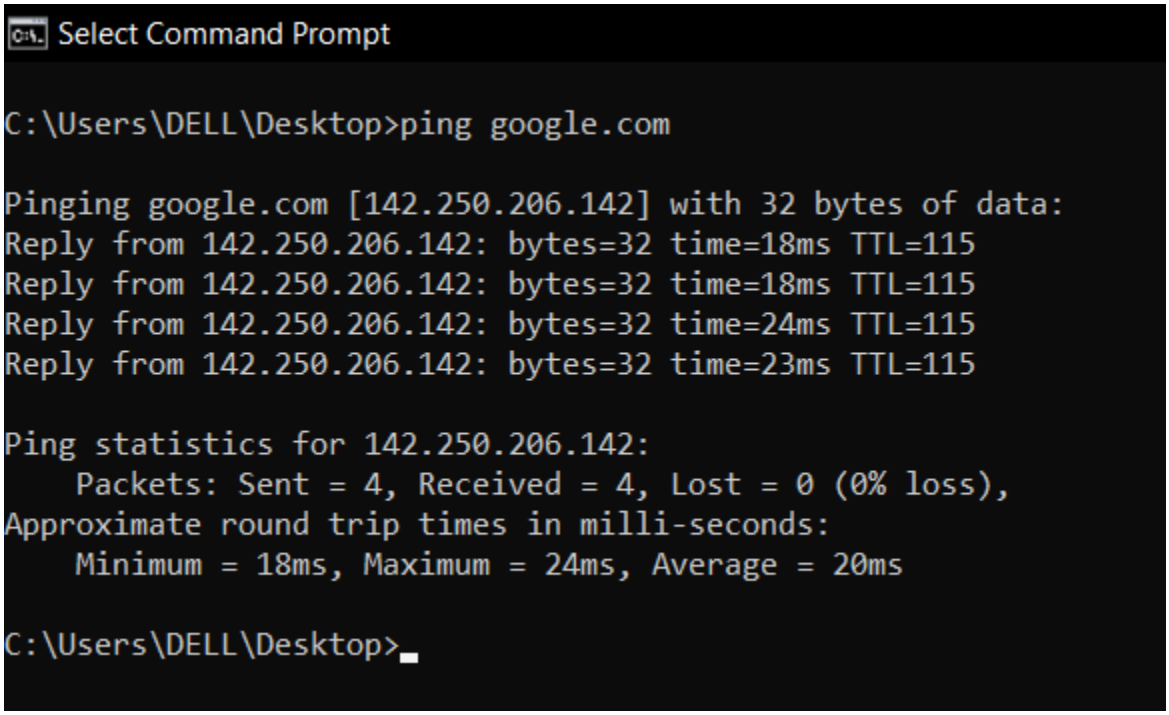
9. type nul > (on Windows)
   vi (on Mac/Linux)
   - It is used to create a new file.



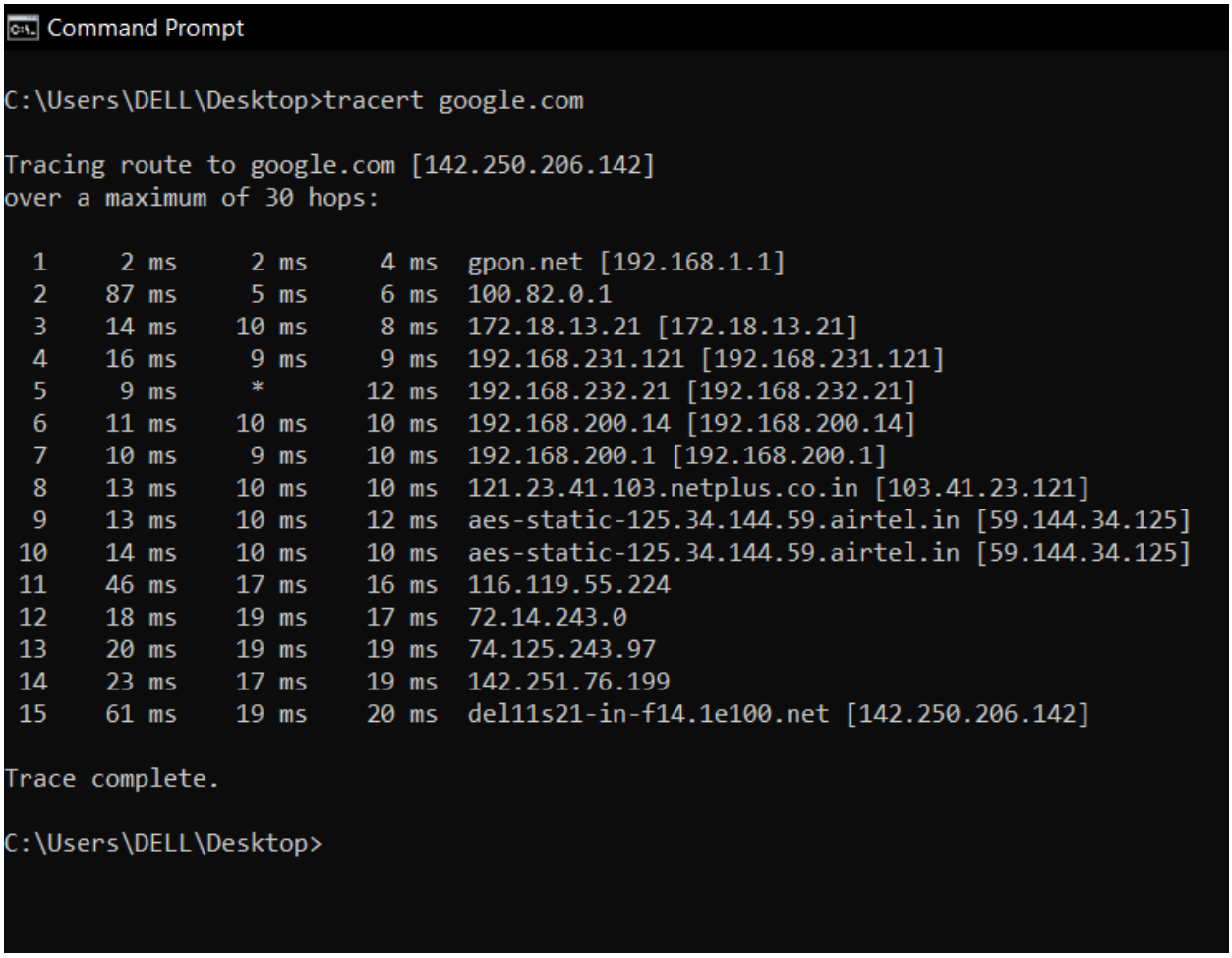
10. ipconfig (on Windows)
    Ifconfig (on Mac/Linux)
    -To know the LAN configuration



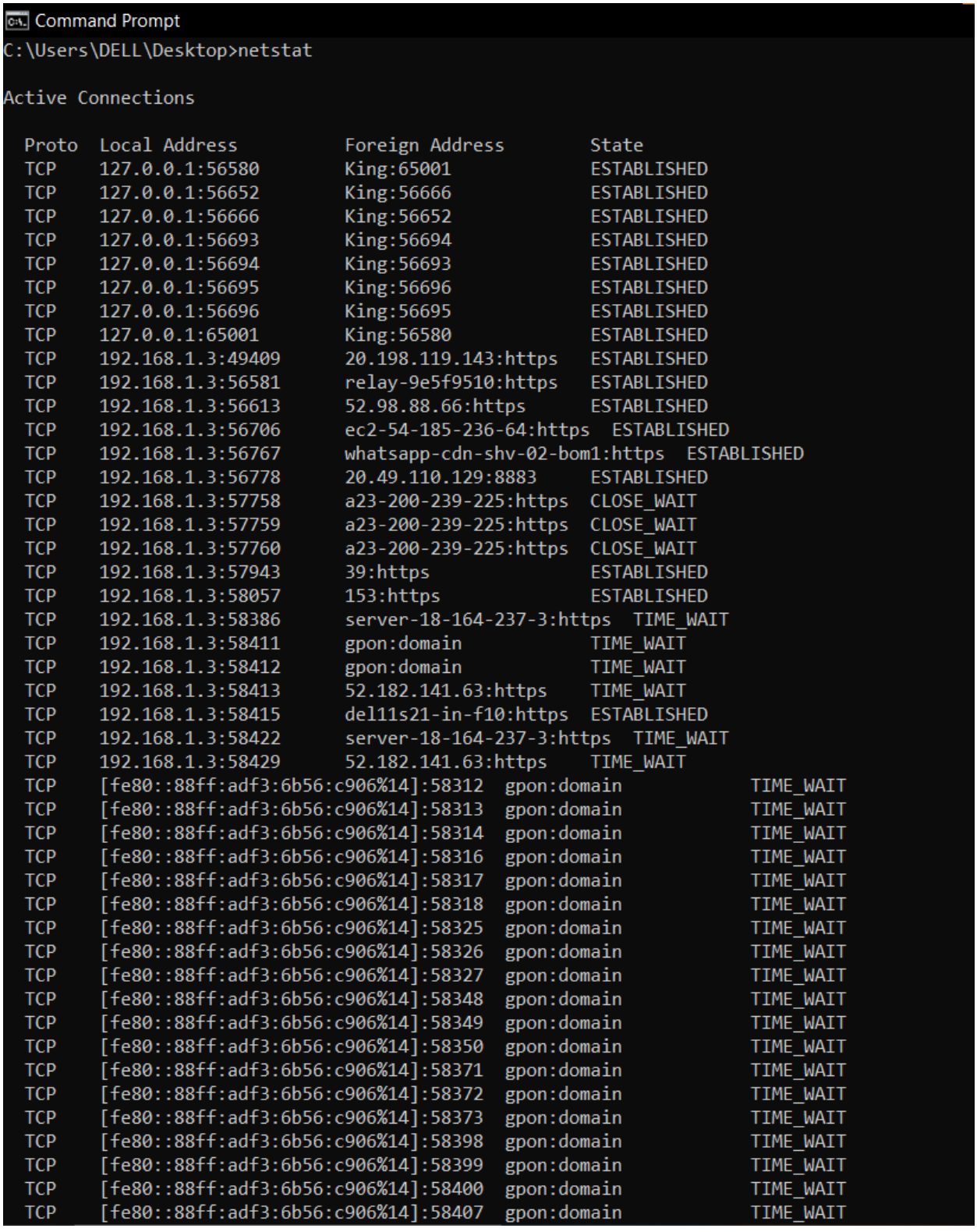
11. ping(packet internet groper)
    - To check the connectivity of network



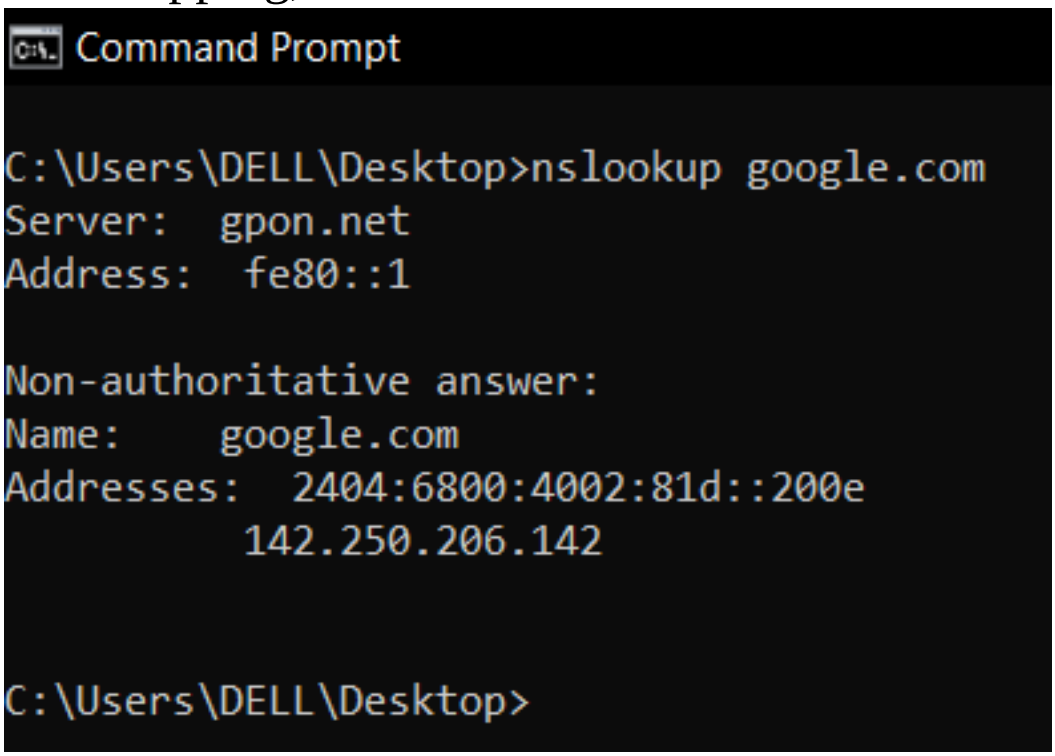
12. tracert (on Windows)
    traceroute (on Mac/Linux)
    -To find path of information from source to Destination



13. nestat
    - It displays all the connections with relevant Protocols.

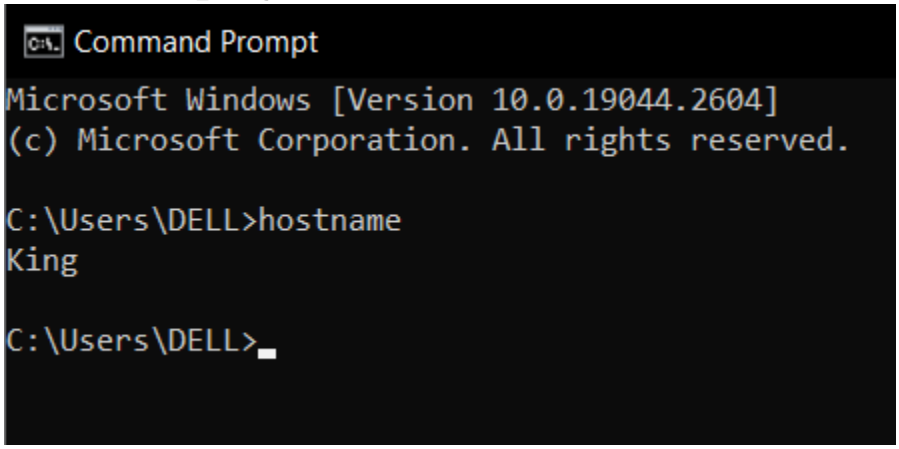

Command Prompt
C:\Users\DELL\Desktop>netstat
Active Connections
Proto Local Address Foreign Address State
TCP 127.0.0.1:56580 King:65001 ESTABLISHED
TCP 127.0.0.1:56652 King:56666 ESTABLISHED
TCP 127.0.0.1:56666 King:56652 ESTABLISHED
TCP 127.0.0.1:56693 King:56694 ESTABLISHED
TCP 127.0.0.1:56694 King:56693 ESTABLISHED
TCP 127.0.0.1:56695 King:56696 ESTABLISHED
TCP 127.0.0.1:56696 King:56695 ESTABLISHED
TCP 127.0.0.1:65001 King:56580 ESTABLISHED
TCP 192.168.1.3:49409 20.198.119.143:https ESTABLISHED
TCP 192.168.1.3:56581 relay-9e5f9510:https ESTABLISHED
TCP 192.168.1.3:56613 52.98.88.66:https ESTABLISHED
TCP 192.168.1.3:56706 ec2-54-185-236-64:https ESTABLISHED
TCP 192.168.1.3:56767 whatsapp-cdn-shv-02-bom1:https ESTABLISHED
TCP 192.168.1.3:56778 20.49.110.129:8883 ESTABLISHED
TCP 192.168.1.3:57758 a23-200-239-225:https CLOSE_WAIT
TCP 192.168.1.3:57759 a23-200-239-225:https CLOSE_WAIT
TCP 192.168.1.3:57760 a23-200-239-225:https CLOSE_WAIT
TCP 192.168.1.3:57943 39:https ESTABLISHED
TCP 192.168.1.3:58057 153:https ESTABLISHED
TCP 192.168.1.3:58386 server-18-164-237-3:https TIME_WAIT
TCP 192.168.1.3:58411 gpon:domain TIME_WAIT
TCP 192.168.1.3:58412 gpon:domain TIME_WAIT
TCP 192.168.1.3:58413 52.182.141.63:https TIME_WAIT
TCP 192.168.1.3:58415 del11s21-in-f10:https ESTABLISHED
TCP 192.168.1.3:58422 server-18-164-237-3:https TIME_WAIT
TCP 192.168.1.3:58429 52.182.141.63:https TIME_WAIT
TCP [fe80::88ff:adf3:6b56:c906%14]:58312 gpon:domain TIME_WAIT
TCP [fe80::88ff:adf3:6b56:c906%14]:58313 gpon:domain TIME_WAIT
TCP [fe80::88ff:adf3:6b56:c906%14]:58314 gpon:domain TIME_WAIT
TCP [fe80::88ff:adf3:6b56:c906%14]:58316 gpon:domain TIME_WAIT
TCP [fe80::88ff:adf3:6b56:c906%14]:58317 gpon:domain TIME_WAIT
TCP [fe80::88ff:adf3:6b56:c906%14]:58318 gpon:domain TIME_WAIT
TCP [fe80::88ff:adf3:6b56:c906%14]:58325 gpon:domain TIME_WAIT
TCP [fe80::88ff:adf3:6b56:c906%14]:58326 gpon:domain TIME_WAIT
TCP [fe80::88ff:adf3:6b56:c906%14]:58327 gpon:domain TIME_WAIT
TCP [fe80::88ff:adf3:6b56:c906%14]:58348 gpon:domain TIME_WAIT
TCP [fe80::88ff:adf3:6b56:c906%14]:58349 gpon:domain TIME_WAIT
TCP [fe80::88ff:adf3:6b56:c906%14]:58350 gpon:domain TIME_WAIT
TCP [fe80::88ff:adf3:6b56:c906%14]:58371 gpon:domain TIME_WAIT
TCP [fe80::88ff:adf3:6b56:c906%14]:58372 gpon:domain TIME_WAIT
TCP [fe80::88ff:adf3:6b56:c906%14]:58373 gpon:domain TIME_WAIT
TCP [fe80::88ff:adf3:6b56:c906%14]:58398 gpon:domain TIME_WAIT
TCP [fe80::88ff:adf3:6b56:c906%14]:58399 gpon:domain TIME_WAIT
TCP [fe80::88ff:adf3:6b56:c906%14]:58400 gpon:domain TIME_WAIT
TCP [fe80::88ff:adf3:6b56:c906%14]:58407 gpon:domain TIME_WAIT

14. dig (Domain Information Groper)
    - Used to search DNS name servers
15. telnet
    - It is a command line interface for communicationwith a remote device or server.
16. whois
    - The whois command displays information abouta website's record.
17. nslookup
    - nslookup is used for querying the Domain Name System to obtain domain name or IP address mapping, or other DNS records.



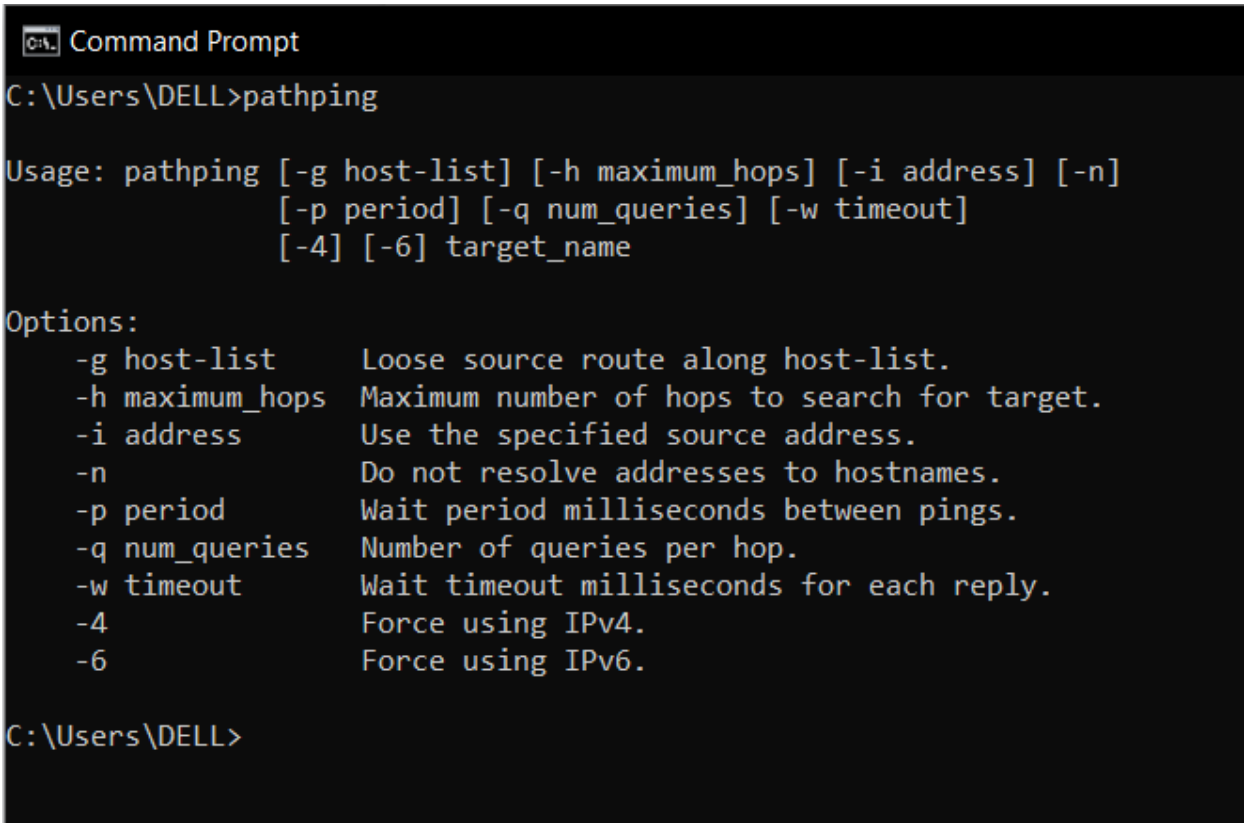
18. scp
    - It copies the files from one system to other system remotely.

19. Enable/Disable Network Interface
    -To enable eth0
     #ifup eht0
    -To disable eth0
     #ifdown eth0
20. Hostname
    -it displays the name of the current host system.



21. pathping

-it sends multiple echo Request messages to each router between a source and destination, Over a period of time, and then computes resultsbased on the packets returned from each router.



Experiment#4

Aim: Verify the connectivity of your workstation to the internet.

Step1: Checking IPV4 Address and Default Gateway are in thesame network or subnet.

```
C:\Users\DELL>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

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

Wireless LAN adapter Local Area Connection* 11:

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

Wireless LAN adapter Local Area Connection* 12:

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

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2409:40d6:101f:8d76:775d:dd8a:3c20:6089
   Temporary IPv6 Address. . . . . . : 2409:40d6:101f:8d76:fcae:f7f9:6b28:6509
   Link-local IPv6 Address . . . . . : fe80::88ff:adf3:6b56:c906%15
   IPv4 Address. . . . . . . . . . . : 192.168.240.241
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::5802:efff:fe0b:5755%15
                                       192.168.240.100
```

Figure 1 :The TCP/IP configuration information of a workstation

IPV4 Address: 192.168.240.241

Default Gateway: 192.168.240.100

The IP address and the default gateway are in the same network or subnet, therefore this host could be able to communicate outside the network. In Figure 1, the subnet mask tells us that thefirst three octets of the IP address and the default gateway must be the same in order to be in the same network.

Step2: Finding DNS and DHCP server addresses using ipconfig/all

```
C:\Users\DELL>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : King
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Mixed
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : bbrouter
   Description . . . . . . . . . . . : Realtek PCIe GbE Family Controller
   Physical Address. . . . . . . . . : B0-7B-25-73-91-E0
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 11:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #3
   Physical Address. . . . . . . . . : A6-97-B1-DC-66-C3
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
```

```
Wireless LAN adapter Local Area Connection* 12:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #4
   Physical Address. . . . . . . . . : B6-97-B1-DC-66-C3
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Qualcomm QCA61x4A 802.11ac Wireless Adapter
   Physical Address. . . . . . . . . : A4-97-B1-DC-66-C3
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2409:40d6:101f:8d76:775d:dd8a:3c20:6089(Preferred)
   Temporary IPv6 Address. . . . . . : 2409:40d6:101f:8d76:fcae:f7f9:6b28:6509(Preferred)
   Link-local IPv6 Address . . . . . : fe80::88ff:adf3:6b56:c906%15(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.240.241(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : 26 April 2023 11:15:54
   Lease Expires . . . . . . . . . . : 26 April 2023 12:26:02
   Default Gateway . . . . . . . . . : fe80::5802:efff:fe0b:5755%15
                                       192.168.240.100
   DHCP Server . . . . . . . . . . . : 192.168.240.100
   DHCPv6 IAID . . . . . . . . . . . : 111450033
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-27-7C-6F-8A-B0-7B-25-73-91-E0
   DNS Servers . . . . . . . . . . . : 192.168.240.100
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

DNS SERVER ADDRESS: 192.168.240.100

DHCP SERVER ADDRESS: 192.168.240.100

A Domain Name System (DNS) server is used to translate domain names to IP Addresses and vice versa whereas DHCP isa client/server protocol that automatically assigns an IP address and other configuration information to an Internet Protocol (IP) host.

- DNS uses User Datagram Protocol (UDP). The DNS service utilizes port 53.

- DHCP is an application layer protocol that provides −
    - Subnet Mask
    - Router Address
    - IP Address

Step3: Ping the IP Address of another computer. (Note that forthe ping and tracert commands to work the PC firewalls have tobe disabled.)

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 198.168.1.1

Pinging 198.168.1.1 with 32 bytes of data:

Reply from 198.168.1.1: bytes=32 time<1ms TTL=128
Reply from 198.168.1.1: bytes=32 time<1ms TTL=128
Reply from 198.168.1.1: bytes=32 time<1ms TTL=128
Reply from 198.168.1.1: bytes=32 time<1ms TTL=128

Ping statistics for 198.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Step4: Ping the Loopback IP address of your computer i.e.127.0.0.1

```
C:\Users\DELL>ping 127.0.0.1

Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

The IP address 127.0.0.1 is reserved for loopback testing. Theping is successful, therefore TCP/IP is properly installed and functioning on this computer.

Step 5: Ping websites using their domain names

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

Pinging www.google.com [2404:6800:4002:819::2004] with 32 bytes of data:
Reply from 2404:6800:4002:819::2004: time=65ms
Reply from 2404:6800:4002:819::2004: time=82ms
Reply from 2404:6800:4002:819::2004: time=105ms
Reply from 2404:6800:4002:819::2004: time=117ms

Ping statistics for 2404:6800:4002:819::2004:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 65ms, Maximum = 117ms, Average = 92ms
```

Figure 2: Pinging Google

```
C:\Users\DELL>ping www.cisco.com

Pinging e2867.dsca.akamaiedge.net [2600:140f:5:d9d::b33] with 32 bytes of data:
Reply from 2600:140f:5:d9d::b33: time=42ms
Reply from 2600:140f:5:d9d::b33: time=106ms
Reply from 2600:140f:5:d9d::b33: time=87ms
Reply from 2600:140f:5:d9d::b33: time=93ms

Ping statistics for 2600:140f:5:d9d::b33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 42ms, Maximum = 106ms, Average = 82ms
```

Figure 3: Pinging Cisco

We can see that the ping time of both websites are different, thiscan be affected by a variety of variables, including the distance

between the server , the state of the local internet infrastructure,and the volume of network traffic.

Step 6: Trace the route to the google website

```
C:\Users\DELL>tracert www.google.com

Tracing route to www.google.com [142.250.194.100]
over a maximum of 30 hops:

  1     2 ms     4 ms     4 ms  RTK_GW.bbrouter [192.168.1.1]
  2    38 ms     7 ms     8 ms  172.16.32.1
  3     7 ms     *        7 ms  1.199.193.103-gigantic.gtel.in [103.193.199.1]
  4     6 ms     7 ms     7 ms  74.125.147.66
  5     8 ms     8 ms     8 ms  108.170.251.97
  6    10 ms     7 ms    10 ms  142.251.52.223
  7     7 ms     6 ms     7 ms  del12s04-in-f4.1e100.net [142.250.194.100]

Trace complete.
```

Figure 4 : A traceroute Output

Experiment#5

Aim: Transfer of a Message in Cisco Packet Tracer

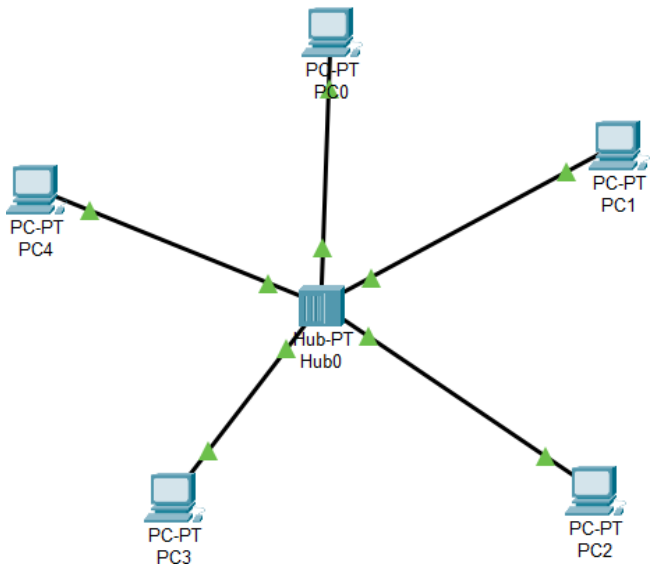
IP Address:

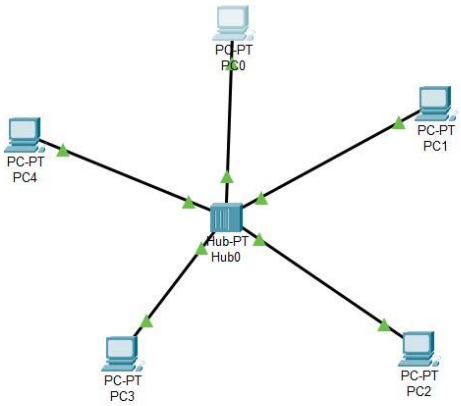
- An IP address is a long string of numbers assigned to every device connected to a network that uses Internet Protocol asthe medium for communication.

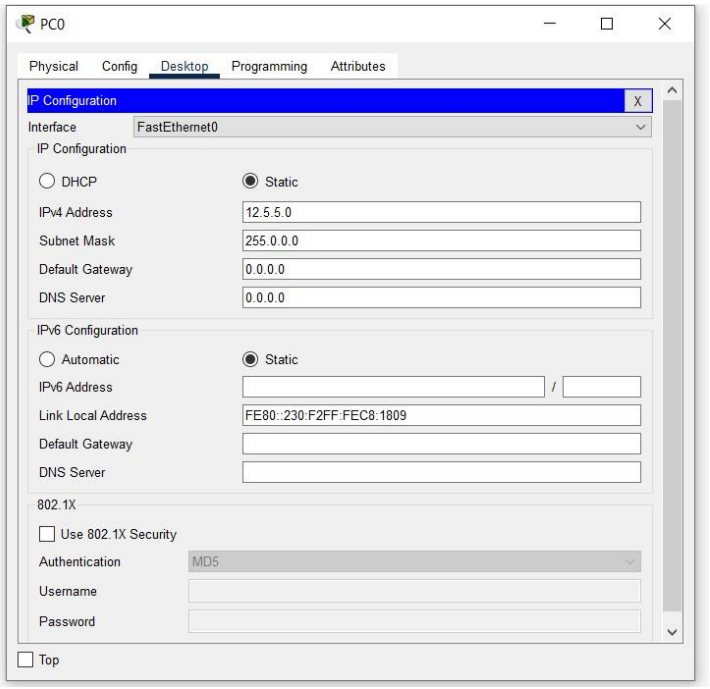
Hub:

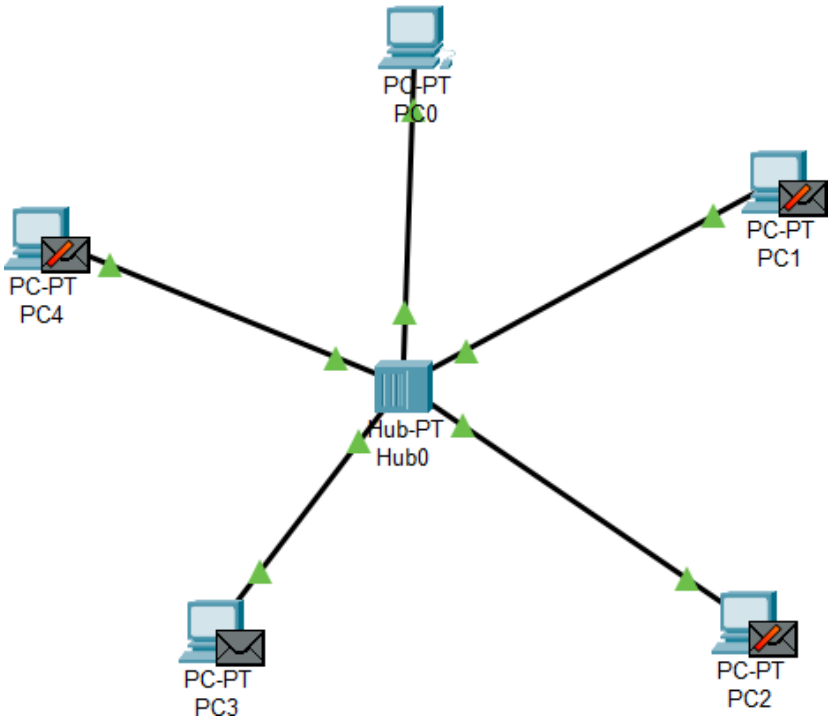
- A hub is a physical layer networking device which is used to connect multiple devices in a network.
- The hub doesn't understand Ethernet, and doesn't know anything about MAC addresses. For the hub, all bits are just bits transmitted over the wire, and these bits should get to allother ends.
- To make Connections we use Cross-Over Wire.

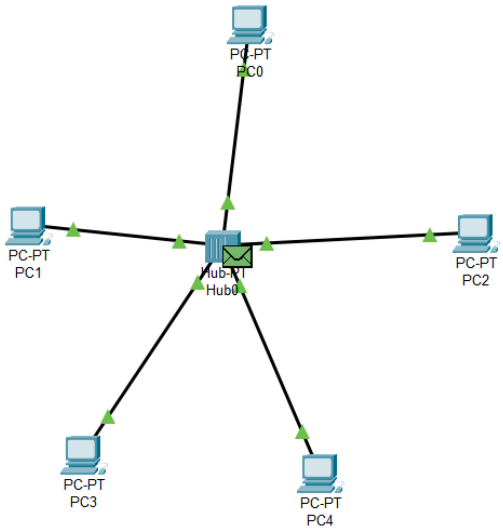
Screenshots:

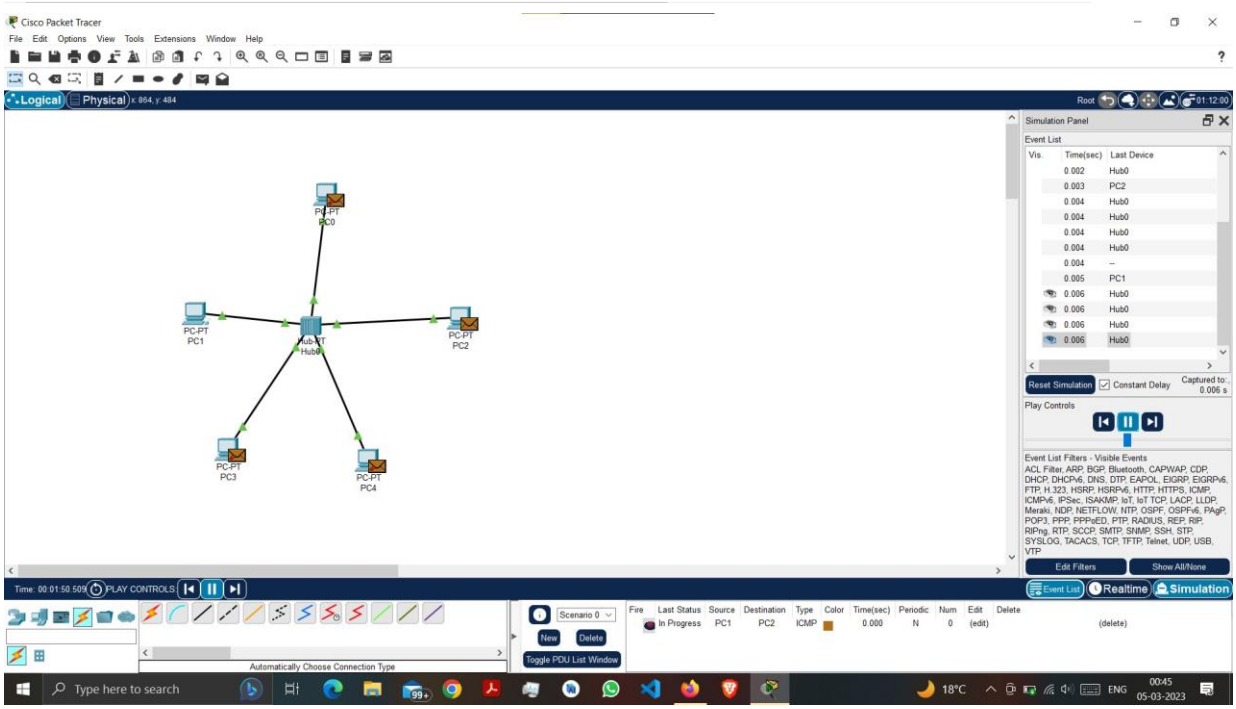


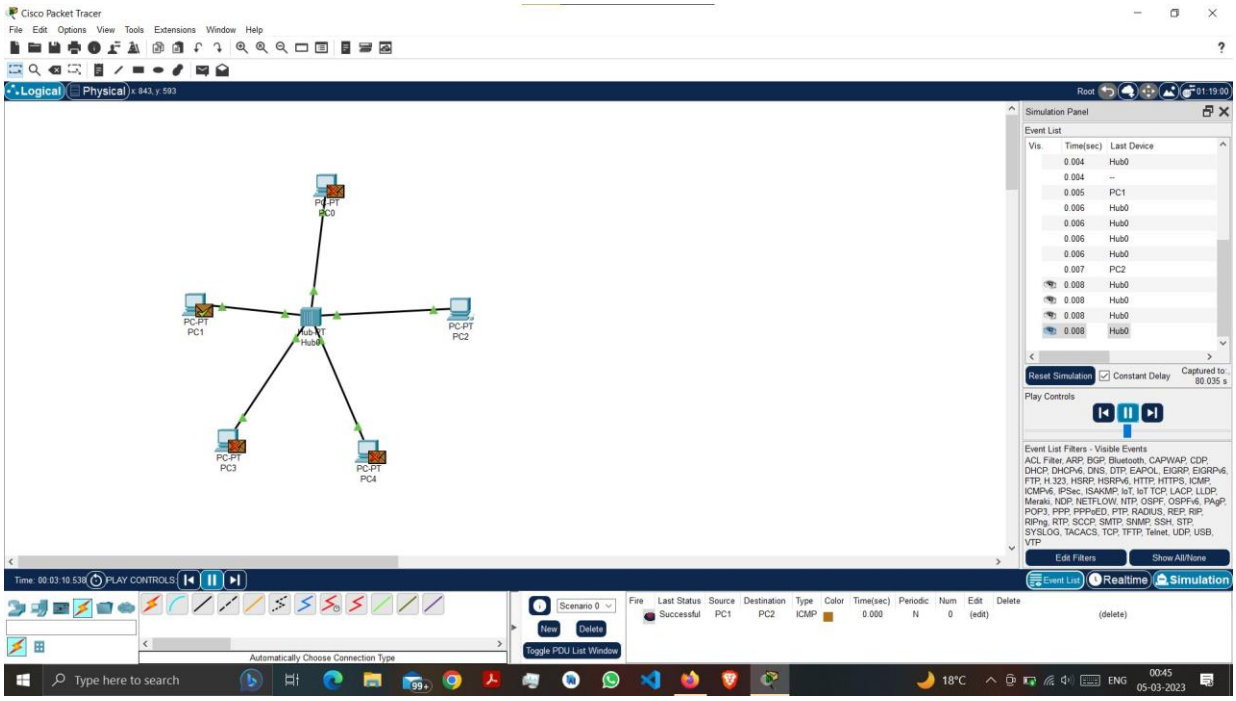

PC-PT
PC0
PC-PT
PC1
PC-PT
PC4
Hub-PT
Hub0
PC-PT
PC3
PC-PT
PC2


PC0
Physical
Config
Desktop
Programming
Attributes
IP Configuration
X
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
12.5.5.0
Subnet Mask
255.0.0.0
Default Gateway
0.0.0.0
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address
FE80::230:F2FF:FEC8:1809
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top


PC-PT
PC0
PC-PT
PC1
PC-PT
PC4
Hub-PT
Hub0
PC-PT
PC3
PC-PT
PC2


PC-PT
PC0
PC-PT
PC1
Hub-PT
Hub0
PC-PT
PC2
PC-PT
PC3
PC-PT
PC4


Cisco Packet Tracer
File Edit Options View Tools Extensions Window Help
Logical Physical
Simulation Panel
Event List
Vis. Time(sec) Last Device
Reset Simulation
Constant Delay
Play Controls
Event List Filters - Visible Events
Edit Filters
Show All/None
Realtime
Simulation
Automatically Choose Connection Type
Toggle PDU List Window
Type here to search
18°C
ENG
00:45
05-03-2023


Cisco Packet Tracer
File Edit Options View Tools Extensions Window Help
Logical Physical
PC-PT PC0
PC-PT PC1
Hub-PT Hub0
PC-PT PC2
PC-PT PC3
PC-PT PC4
Simulation Panel
Event List
Vis. Time(sec) Last Device
0.004 Hub0
0.004 --
0.005 PC1
0.006 Hub0
0.006 Hub0
0.006 Hub0
0.006 Hub0
0.007 PC2
0.008 Hub0
0.008 Hub0
0.008 Hub0
0.008 Hub0
Reset Simulation
Constant Delay
Captured to: 80.035 s
Play Controls
Event List Filters - Visible Events
ACL Filter, ARP, BGP, Bluetooth, CAPWAP, CDP, DHCP, DHCPv6, DNS, DTP, EAPOL, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, IoT, IoT TCP, LACP, LLDP, Meraki, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, PPP, PPPoED, PTP, RADIUS, REP, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, USB, VTP
Edit Filters
Show All/None
Time: 00:03:10.538
PLAY CONTROLS
Event List
Realtime
Simulation
Scenario 0
New
Delete
Toggle PDU List Window
Fire Last Status Source Destination Type Color Time(sec) Periodic Num Edit Delete
Successful PC1 PC2 ICMP 0.000 N 0 (edit) (delete)
Automatically Choose Connection Type
Type here to search
18°C
ENG
00:45
05-03-2023

Experiment#6

Aim: Implementation of the IPCONFIG network command.

(i) IPCONFIG /all:

Display full configuration information.

```
Microsoft Windows [Version 10.0.19044.2728]
(c) Microsoft Corporation. All rights reserved.

C:\Users\DELL>IPCONFIG /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : King
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Mixed
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : bbrouter

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : bbrouter
   Description . . . . . . . . . . . : Realtek PCIe GbE Family Controller
   Physical Address. . . . . . . . . : B0-7B-25-73-91-E0
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::1d97:1b69:f71a:639a%17(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.8(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : 05 April 2023 14:19:13
   Lease Expires . . . . . . . . . . : 06 April 2023 14:19:12
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 112229157
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-27-7C-6F-8A-B0-7B-25-73-91-E0
   DNS Servers . . . . . . . . . . . : 192.168.1.1
   NetBIOS over Tcpip. . . . . . . . : Enabled

Wireless LAN adapter Local Area Connection* 11:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #3
   Physical Address. . . . . . . . . : A6-97-B1-DC-66-C3
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
```

```
Wireless LAN adapter Local Area Connection* 12:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #4
   Physical Address. . . . . . . . . : B6-97-B1-DC-66-C3
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Qualcomm QCA61x4A 802.11ac Wireless Adapter
   Physical Address. . . . . . . . . : A4-97-B1-DC-66-C3
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
```

(ii) IPCONFIG /release [adapter]:

Release the IP address for the specified adapter

```
C:\Users\DELL>IPCONFIG /release [adapter]

Windows IP Configuration

The operation failed as no adapter is in the state permissible for
this operation.
```

(iii)IPCONFIG /renew [adapter]:

Renew the IP address for the specified adapter.

```
C:\Users\DELL>IPCONFIG /renew [adapter]

Windows IP Configuration

The operation failed as no adapter is in the state permissible for
this operation.
```

(iv)IPCONFIG /flushdns:

Purge the DNS Resolver cache.

```
C:\Users\DELL>IPCONFIG /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.
```

(v) IPCONFIG /registerdns:

Refresh all DHCP leases and re-register DNS names.

```
C:\Windows\system32>IPCONFIG /registerdns

Windows IP Configuration

Registration of the DNS resource records for all adapters of this computer has been initiated. Any errors will be reported in the Event Viewer in 15 minutes.
```

(vi) IPCONFIG /displaydns:

Display the contents of the DNS Resolver Cache

```
C:\Windows\system32>IPCONFIG /displaydns

Windows IP Configuration

    colab-alv.research.google.com
    ----------------------------------------
    Record Name . . . . . : colab-alv.research.google.com
    Record Type . . . . . : 28
    Time To Live  . . . . : 262
    Data Length . . . . . : 16
    Section . . . . . . . : Answer
    AAAA Record . . . . . : 2001:4860:4802:38::180


    Record Name . . . . . : colab-alv.research.google.com
    Record Type . . . . . : 28
    Time To Live  . . . . : 262
    Data Length . . . . . : 16
    Section . . . . . . . : Answer
    AAAA Record . . . . . : 2001:4860:4802:36::180
```

```
Record Name . . . . . : colab-alv.research.google.com
Record Type . . . . . : 28
Time To Live  . . . . : 262
Data Length . . . . . : 16
Section . . . . . . . : Answer
AAAA Record . . . . . : 2001:4860:4802:34::180


Record Name . . . . . : colab-alv.research.google.com
Record Type . . . . . : 28
Time To Live  . . . . : 262
Data Length . . . . . : 16
Section . . . . . . . : Answer
AAAA Record . . . . . : 2001:4860:4802:32::180


colab-alv.research.google.com
----------------------------------------
Record Name . . . . . : colab-alv.research.google.com
Record Type . . . . . : 1
Time To Live  . . . . : 97
Data Length . . . . . : 4
Section . . . . . . . : Answer
A (Host) Record . . . : 216.239.36.180


Record Name . . . . . : colab-alv.research.google.com
Record Type . . . . . : 1
Time To Live  . . . . : 97
Data Length . . . . . : 4
Section . . . . . . . : Answer
A (Host) Record . . . : 216.239.34.180


Record Name . . . . . : colab-alv.research.google.com
Record Type . . . . . : 1
Time To Live  . . . . : 97
Data Length . . . . . : 4
Section . . . . . . . : Answer
A (Host) Record . . . : 216.239.32.180
```

```
Record Name . . . . . : colab-alv.research.google.com
Record Type . . . . . : 1
Time To Live  . . . . : 97
Data Length . . . . . : 4
Section . . . . . . . : Answer
A (Host) Record . . . : 216.239.38.180


play.google.com
----------------------------------------
Record Name . . . . . : play.google.com
Record Type . . . . . : 28
Time To Live  . . . . : 94
Data Length . . . . . : 16
Section . . . . . . . : Answer
AAAA Record . . . . . : 2404:6800:4002:82d::200e


play.google.com
----------------------------------------
Record Name . . . . . : play.google.com
Record Type . . . . . : 1
Time To Live  . . . . : 180
Data Length . . . . . : 4
Section . . . . . . . : Answer
A (Host) Record . . . : 142.250.206.174


accounts.google.com
----------------------------------------
Record Name . . . . . : accounts.google.com
Record Type . . . . . : 28
Time To Live  . . . . : 95
Data Length . . . . . : 16
Section . . . . . . . : Answer
AAAA Record . . . . . : 2404:6800:4002:809::200d
```

(vii)IPCONFIG /showclassid adapter:

Display all the DHCP class IDs allowed for adapter.

```
C:\Windows\system32>IPCONFIG /showclassid adapter

Windows IP Configuration

The operation failed as no adapter is in the state permissible for
this operation.
```

(viii)IPCONFIG /setclassid adapter [classid]:

Modify the dhcp class id.

```
C:\Windows\system32>IPCONFIG /setclassid adapter [classid]

Windows IP Configuration

The operation failed as no adapter is in the state permissible for
this operation.
```

Experiment#7

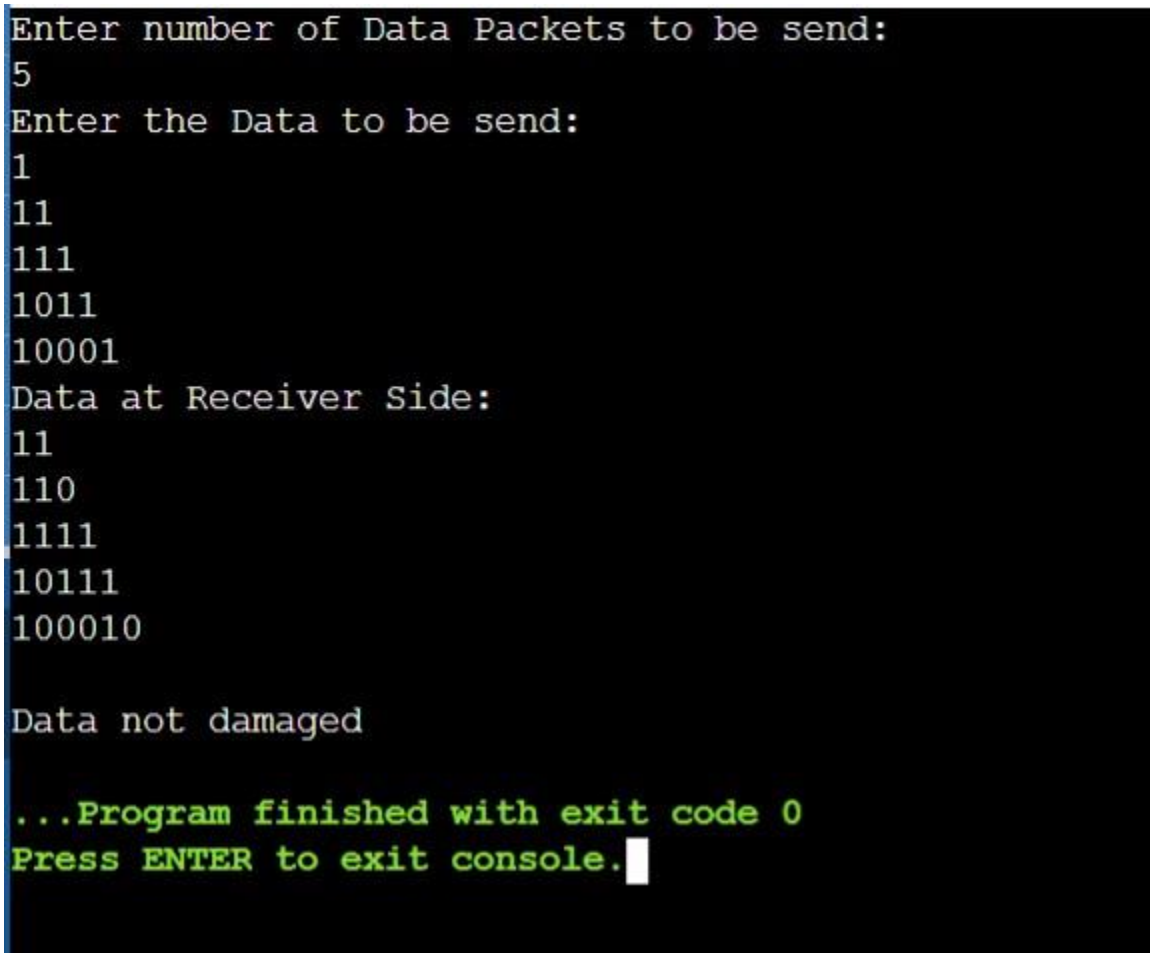
Aim: Program for Error Detection using Even Parity Check

Code:

```
#include <bits/stdc++.h>
using namespace std;

int main(){
    int n,i,j;
    cout<<"Enter number of Data Packets to be send: "<<endl;cin>>n;
    vector<string> v;
    cout<<"Enter the Data to be send: "<<endl;
    for(i=0;i<n;i++){
        string s;

        cin>>s;
        v.push_back(s);
    }

    // Sender Side
    vector<string> data;
    for(i=0;i<n;i++){
        int c=0;
        for(j=0;j<v[i].size();j++){
            if(v[i][j]=='1') c++;
        }
```

```
        if(c & 1) v[i].push_back('1');
        else v[i].push_back('0');
        data.push_back(v[i]);
    }

    // Receiver Side
    cout<<"Data at Receiver Side:"<<endl;for(i=0;i<n;i++){
        cout<<data[i]<<endl;
    }
    int f=0;
    for(i=0;i<n;i++)
    {
        int c=0;
        for(j=0;j<data[i].size();j++){
                if(data[i][j]=='1') c++;
        }
        if(c & 1){
                f=1;
                break;
        }
    }

    if(f){
        cout<<endl<<"Data damaged or lost";
    }
    else{
        cout<<endl<<"Data not damaged";
    }
}
```

Output:


Enter number of Data Packets to be send:
5
Enter the Data to be send:
1
11
111
1011
10001
Data at Receiver Side:
11
110
1111
10111
100010
Data not damaged
...Program finished with exit code 0
Press ENTER to exit console.

Experiment#8

Aim: Study of network IP

- Classification of IP address
- Subnetting
- Super netting

Procedure: Following is required to be studied under thispractical.

- Classification of IP address

As shown in figure we teach how the ip addresses are classifiedand when they are used.

Class	Address Range	Supports
Class A	1.0.0.1 to 126.255.255.254	Supports 16 million hosts on each of 127 networks.
Class B	128.1.0.1 to 191.255.255.254	Supports 65,000 hosts on each of 16,000 networks.
Class C	192.0.1.1 to 223.255.254.254	Supports 254 hosts on each of 2 million networks.
Class D	224.0.0.0 to 239.255.255.255	Reserved for multicast groups.
Class E	240.0.0.0 to 254.255.255.254	Reserved.

Subnetting: Subnetting is a process of dividing a single networkinto multiple sub networks.

Why do we Develop Subnetting?

1. Improved Network Security
2. Better Network Performance and Speed
3. Administration is a Breeze
4. Easier to Control Growth of Network
5. Less Network Congestion

How to calculate Subnet Mask?

Subnet mask is a 32 bit number which is a sequence of 1's followedby a sequence of 0's where-

- 1's represent the global network ID part and the subnet ID part.
- 0's represent the host ID part.

For any given IP Address, the subnet mask is calculated-

- By setting all the bits reserved for network ID part and subnet IDpart to 1.
- By setting all the bits reserved for the host ID part to 0.

For example:

Consider we have a network having IP Address 200.1.2.0.Clearly, this IP Address belongs to class C.

In class C-

- 24 bits are reserved for the Network ID part.
- 8 bits are reserved for the Host ID part.

Subnet mask is obtained-

- By setting the first 24 bits to 1.
- By setting the remaining 8 bits to 0.

So, Subnet mask
= 11111111.11111111.11111111.00000000
= 255.255.255.0

How to identify Subnet Address?

To calculate the IP Address Subnet you need to perform a bitwise AND operation on the host IP address and subnet mask. The result isthe subnet address in which the host is situated.

IP Address (Decimal)	192.	168.	10.	44
IP Address (Binary)	11000000	10101000	00001010	00101100
Subnet Mask (Binary)	11111111	11111111	11111111	11111000
Subnet Address (Binary)	11000000	10101000	00001010	00101000
Subnet Address (Decimal)	192.	168.	10.	40

Supernetting: Supernetting is the opposite of Subnetting. In subnetting, a single big network is divided into multiple smaller subnetworks. In Supernetting, multiple networks are combined into abigger network termed as a Supernetwork or Supernet.

Why we develop Supernetting?

1. It saves memory and processing resources on routing devices. Basically, they need less space to store their routing table andless processing power to search through the routing table.
2. It provides stability on the network because fluctuations in one part of the network are not propagated to all parts of the network i.e. fluctuations can be isolated.

How to calculate Supernet Mask and How to identify Supernet Address?

Combining these networks into one network: (A summarized route)

- 192.168.0.0/24
- 192.168.1.0/24
- 192.168.2.0/24
- 192.168.3.0/24

Step 1: Write all the IP Addresses in binary like so:

• 192.168.0.0/24
11000000.10101000.00000000.00000000
• 192.168.1.0/24
11000000.10101000.00000001.00000000
• 192.168.2.0/24
11000000.10101000.00000010.00000000
• 192.168.3.0/24
11000000.10101000.00000011.00000000
Step 2: Find matching bits from left to right
11000000.10101000.00000000.00000000
11000000.10101000.00000001.00000000
11000000.10101000.00000010.00000000
11000000.10101000.00000011.00000000
Step 3: Re-write the matching numbers and add the remaining zeros,because you are converting network bits into host bits. This will be your NEW NETWORK ID, the route that you will be
advertising. (A summarized route) 11000000.10101000.00000000.00000000 = 192.168.0.0
Step 4: Find the new subnet mask. Put “1s” in the matchingnetworking part, and all zeros in the host part.
11111111.11111111.11111100.00000000
This your new subnet mask 255.255.252.0
• Your new summarized route is 192.168.0.0/22

Experiment#9

Program to implement Cyclic Redundancy Check (CRC).

Code:

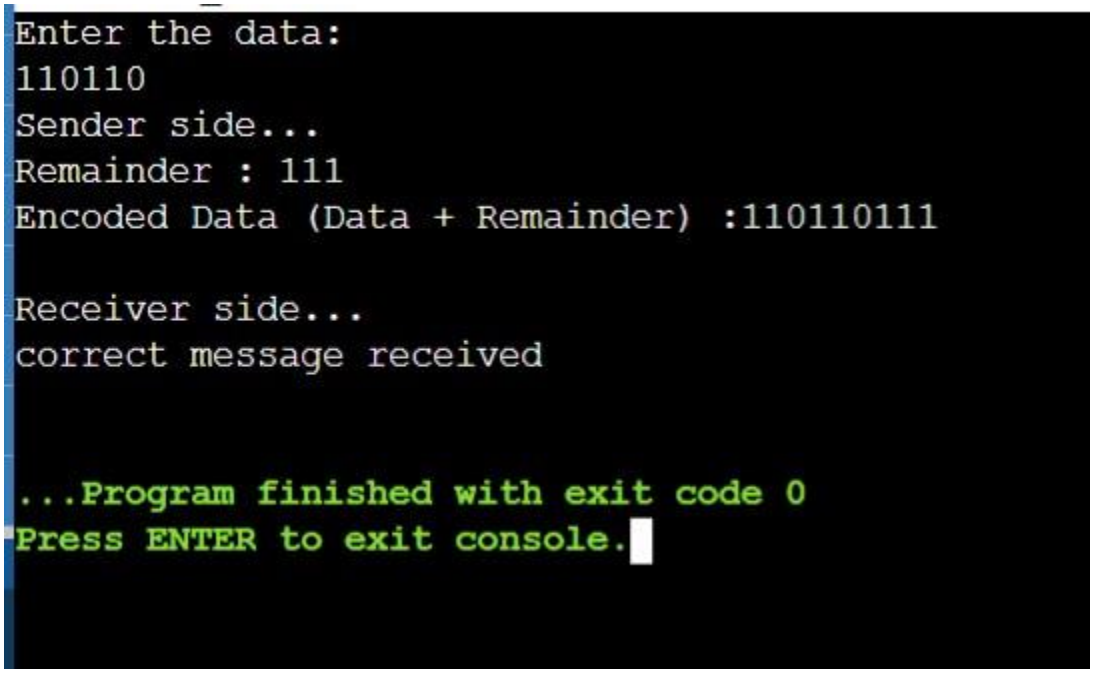
```
#include <bits/stdc++.h>
using namespace std;

string xor1(string a, string b)
{
    string result = "";

    int n = b.length();
    for (int i = 1; i < n; i++) {
        if (a[i] == b[i])
            result += "0";
        else
            result += "1";
    }

    return result;
}

string mod2div(string dividend, string divisor)
{
    int pick = divisor.length();
    string tmp = dividend.substr(0, pick);int
    n = dividend.length();
```

```
    while (pick < n) {
        if (tmp[0] == '1')
            tmp = xor1(divisor, tmp) + dividend[pick];
        else
            tmp = xor1(std::string(pick, '0'), tmp)
                + dividend[pick];
        pick += 1;
    }
    if (tmp[0] == '1')
        tmp = xor1(divisor, tmp);
    else
        tmp = xor1(std::string(pick, '0'), tmp);

    return tmp;
}

void encodeData(string data, string key)
{
    int l_key = key.length();

    string appended_data
        = (data + std::string(l_key - 1, '0'));

    string remainder = mod2div(appended_data, key);string
    codeword = data + remainder;
    cout << "Remainder : " << remainder << "\n";
    cout << "Encoded Data (Data + Remainder) :" << codeword<<"\n";
}
```

```
void receiver(string data, string key)
{
    string currxor
        = mod2div(data.substr(0, key.size()), key);int
    curr = key.size();
    while (curr != data.size()) {
        if (currxor.size() != key.size()) {
                currxor.push_back(data[curr++]);
        }
        else {
                currxor = mod2div(currxor, key);
        }
    }
    if (currxor.size() == key.size()) {
        currxor = mod2div(currxor, key);
    }
    if (currxor.find('1') != string::npos) {
        cout << "there is some error in data" << endl;
    }
    else {
        cout << "correct message received" << endl;
    }
}

int main()
{
    string data;
    cout<<"Enter the data: "<<endl;
    cin>>data;
    string key = "1101";
```

```
    cout << "Sender side..." << endl;
    encodeData(data, key);

    cout << "\nReceiver side..." << endl;
    receiver(data+mod2div(data+std::string(key.size() - 1, '0'),key),
key);

    return 0;
}
```

Output:



Experiment#10

Aim: Perform an initial configuration of a Cisco Catalyst 2960switch.

Procedure:

In this activity, you will configure these settings on the customerCisco Catalyst 2960 switch:

- Host name
- Console password
- vty password
- Privileged EXEC mode password
- Privileged EXEC mode secret
- IP address on VLAN1 interface
- Default gateway

Step 1: Configure the switch host name.

a. From the Customer PC, use a console cable and terminal emulation software to connect to the console

of the customer Cisco Catalyst 2960 switch.

b. Set the host name on the switch to **CustomerSwitch** using these commands.

Switch>enable

Switch#configure terminal

Switch(config)#hostname CustomerSwitch

Step 2: Configure the privileged mode password and secret.

a. From global configuration mode, configure the password as **cisco**.

CustomerSwitch(config)#enable password cisco

b. From global configuration mode, configure the secret as **cisco123**.

CustomerSwitch(config)#enable secret cisco123

Step 3: Configure the console password.

a. From global configuration mode, switch to configuration modeto configure the console line.

CustomerSwitch(config)#line console 0

b. From line configuration mode, set the password to cisco and require the password to be entered at login.

CustomerSwitch(config-line)#password cisco

CustomerSwitch(config-line)#login

CustomerSwitch(config-line)#exit

Step 4: Configure the vty password.

a. From global configuration mode, switch to the configuration mode for the vty lines 0 through 15.

```
CustomerSwitch(config)#line vty 0 15
```

b. From line configuration mode, set the password to cisco and require the password to be entered at Login.

```
CustomerSwitch(config-line)#password cisco
CustomerSwitch(config-line)#login
CustomerSwitch(config-line)#exit
```

Step 5: Configure an IP address on interface VLAN1.

From global configuration mode, switch to interface configurationmode for VLAN1, and assign the IP address 192.168.1.5 with thesubnet mask of 255.255.255.0.

```
CustomerSwitch(config)#interface vlan 1
CustomerSwitch(config-if)#ip address 192.168.1.5 255.255.255.0
CustomerSwitch(config-if)#no shutdown
CustomerSwitch(config-if)#exit
```

Step 6: Configure the default gateway.

a. From global configuration mode, assign the default gateway to 192.168.1.1.

CustomerSwitch(config)#ip default-gateway 192.168.1.1

b. Click the Check Results button at the bottom of this instruction window to check your work.

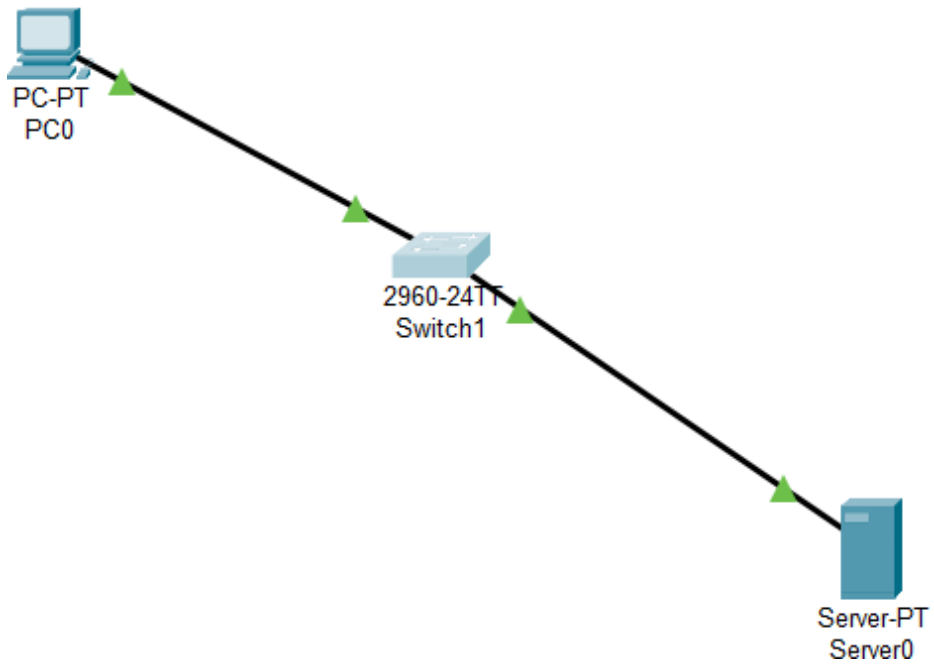
Step 7: Verify the configuration.

The Customer Switch should now be able to ping the ISP Serverat 192.168.1.7 The first one or two pings may fail while ARP converges.

CustomerSwitch(config)#end

CustomerSwitch#ping 192.168.1.7

Screenshots:



Physical Config CLI Attributes

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname CustomerSwitch
CustomerSwitch(config)#enable password cisco
CustomerSwitch(config)#enable secret cisco123
CustomerSwitch(config)#line console 0
CustomerSwitch(config-line)#password cisco
CustomerSwitch(config-line)#login
CustomerSwitch(config-line)#exit
CustomerSwitch(config)#line vty 0 15
CustomerSwitch(config-line)#password cisco
CustomerSwitch(config-line)#login
CustomerSwitch(config-line)#exit
CustomerSwitch(config)#interface vlan 1
CustomerSwitch(config-if)#ip address 192.168.1.5 255.255.255.0
CustomerSwitch(config-if)#no shutdown

CustomerSwitch(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up

CustomerSwitch(config-if)#exit
CustomerSwitch(config)#ip default-gateway 192.168.1.1
CustomerSwitch(config)#end
CustomerSwitch#
%SYS-5-CONFIG_I: Configured from console by console
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.7, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/7 ms
```