EXPERIMENT NO- 01

AIM: Study of Network media, cables, and devices and Cable Construction.

OBJECTIVE: To study about different types of network media, cables and devices and cable constructions.

DESCRIPTION:

NETWORK MEDIA (TRANSMISSIONMEDIA):

Network media refers to the communication channels used to interconnect nodes on a computer network. Typical examples of network media include copper coaxial cable, copper twisted pair cables and optical fibre cables used in wired networks, and radio waves used in wireless data communications networks.

Network medium is the actual physical path between the transmitter and the receiver i.e., It is the channel through which data is sent from one place to another. It is classified into two types:

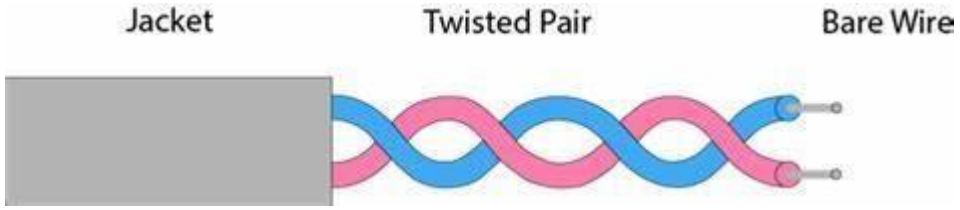
i.Guided media(wired) ii.Unguided media(wireless)

GUIDED MEDIA: Guided media is also called as wired media. It uses a system that guides the data signals along a specific path. Signals being transmitted are directed and confined in a narrow pathway by using physical links.

Features: High speed, secure, used for comparatively shorter distances There

are 3 types of guided media:

a) Twisted pair cable: Twisted pair is a physical media made up of a pair of cables twisted with each other. A twisted pair cable is cheap as compared to other transmission media. Installation of the twisted pair cable is easy, and it is a lightweight cable. The frequency range for twisted pair cable is from 0 to 3. 5KHz.A twisted pair consists of two insulated copper wires arranged in a regular spiral pattern. The degree of reduction in noise interference is determined by the number of turns per foot. Increasing the number of turns per foot decreases noise interference



Twisted pair cable is of two types:

Shielded twisted pair cable:

It consists of special jacket to block external interface. It is used in fast data rate Ethernet and in voice and data channels of telephone lines. It is bulky.

Characteristics of Shielded Twisted Pair:

o The cost of the shielded twisted pair cable is not very high

and not verylow. o An installation of STP is easy. o It has

higher capacity as compared to unshielded twisted pair

cable.

o It has a higher attenuation. o It is shielded that provides the higher data transmission rate. **Disadvantages** o It is more expensive as compared to UTP and coaxial cable.

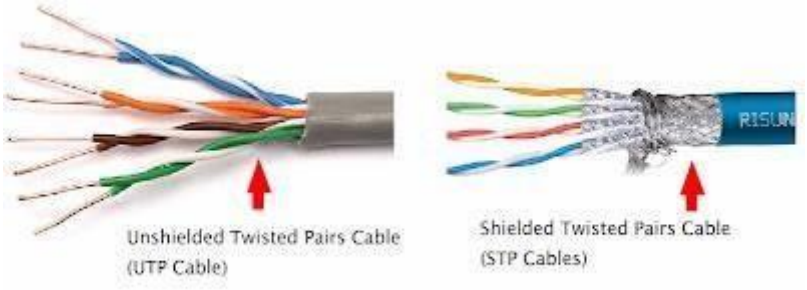
o It has a higher attenuation rate There are 3 types of guided media:

Un Shielded Twisted pair cable:

This type of cable has the ability to block interface and does not depend on a physical shield for this purpose. **Advantages:**

o Least expensive. o Easy to install

o short distance transmission due to attenuation



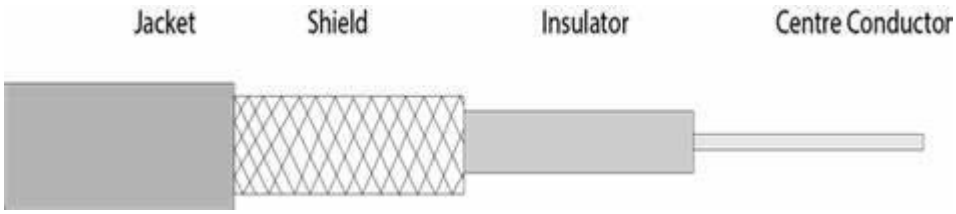
b) Coaxial cable:

It has an outer plastic covering containing 2 parallel conductors each having a separate insulated protection cover. The coaxial cable transmits information in 2 modes:

1) Baseband Mode - dedicated cable bandwidth

2) Broadband mode - bandwidth is split into separate ranges

Cable TV ‘s and analog television networks use coaxial cables. They transmit signals over large distances at higher speed as compared to twisted cables.

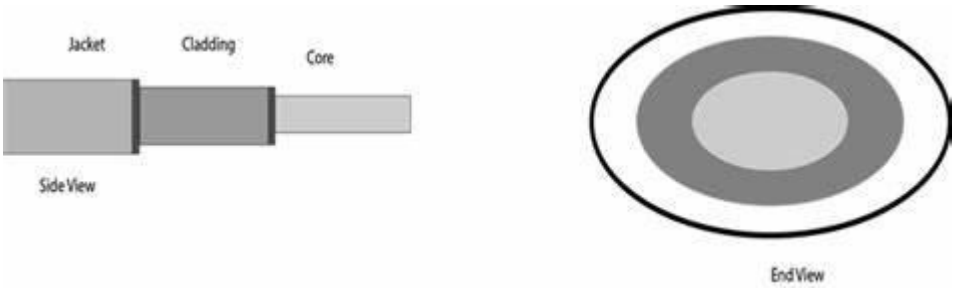


Advantages:

1. High Bandwidth
2. Better noise immunity
3. Easy to install and expand
4. Inexpensive

c) Optical Fiber:

It uses the concept of reflection of light through a core made up of glass or plastic. It is a transparent and flexible fiber made up of glass, which carries information in the form of light pulses from one end to another. Fiber optics is used for long distance and high-performance network. Used in internet, telephone and television. Core is surrounded by less dense glass or plastic covering called the cladding. Used to transfer large volumes of data. It can be uni-directional or bi-directional.



Basic elements of Fiber optic cable:

o Core: The optical fiber consists of a narrow strand of glass or plastic known as a core. A core is a light transmission area of the fiber. The more the area of the core, the more light will be transmitted into thefibre.

o Cladding: The concentric layer of glass is known as cladding. The main functionality of the cladding is to provide the lower refractive index at the core interface as to cause the reflection within the core so that the light waves are transmitted through thefibre.

o Jacket: The protective coating consisting of plastic is known as a jacket. The main purpose of a jacket is to preserve the fiber strength, absorb shock and extra fiberprotection.

Advantages of Optical Fiber

Optical fiber is fast replacing copper wires because of these advantages that it offers:-

- High bandwidth
- Immune to electromagnetic interference
- Suitable for industrial and noisy areas
- Signals carrying data can travel long distances without weakening

Disadvantages of Optical Fibre

Despite long segment lengths and high bandwidth, using optical fibre may not be a viable option for every one due to these disadvantages –

- Optical fibre cables are expensive
- Sophisticated technology required for manufacturing, installing and maintaining optical fibre cables
- Light waves are unidirectional, so two frequencies are required for full duplex transmission **ii)**

UNGUIDEDMEDIA

An unguided transmission transmits the electromagnetic waves without using any physical medium. Therefore, it is also known as wireless transmission. In unguided media, air is the media through which the electromagnetic energy can flow easily. Unguided transmission is broadly classified into three categories:

i) Radio waves: Radio waves are electromagnetic waves and are omnidirectional. When an antenna transports radio waves they are propagated in all directions in free space which means the sending and receiving antennas do not have to be aligned that is any receiving antenna can receive that transmitted

wave. The frequency of radio waves about 30 hertz (Hz) to 300 gigahertz (GHz) and like all other electromagnetic waves radio waves travel at the speed of light in vacuum.

Applications of Radio waves

- These waves are omnidirectional so they are useful for multicasting in which one sender but many receivers.
- Examples of radio waves are television, AM and FM radio, cordless phones and paging.

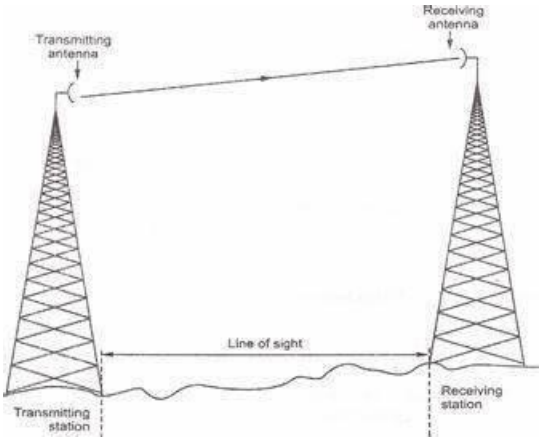
Advantages and disadvantages

- Radio waves are easy to generate and penetrate buildings also can travel long distances.
- Radio waves cover a large area and can penetrate the buildings. By this, an AM radio can receive signals inside a building.
- This can also be disadvantageous because we cannot isolate a communication just inside or outside a building. Cause of this, governments strictly legislate the use of radio transmitters.

ii) Microwaves: Micro Waves includes a line-of-sight transmission that is the sending and receiving antennas that need to be properly aligned with each other. The distance is directly proportional to the height of the antenna which is covered by the signal. In mobile phone communication and television distribution, these are majorly used.

Applications of Micro Waves

Due to the unidirectional properties of Micro Waves, they are very useful when unicast (one-to-one) communication is needed between the sender and the receiver. Cellular phones, satellite networks, and wireless LANs are using Micro Waves.



Two types of Microwave Transmission are as follows,

1. Terrestrial Microwave
2. Satellite Microwave

ii) Infrared waves:

The frequency of Infrared waves is about 300 GHz to 430 THz, which can be used for short-range communication. Infrared waves of high frequencies cannot penetrate walls. This characteristic of Infrared waves prevents interference between one system and another. This means a short-range communication system in a room cannot be affected by another system in the adjacent room.

If we are using the infrared remote control, we do not interfere with the use of the remote by our neighbours. However, by this characteristic, infrared signals become useless for long-range communication. Also, we cannot use infrared waves outside a building because the sun's rays contain infrared waves that can interfere with communication.

Characteristics of infrared waves

- This type of wide bandwidth can be used to transmit digital data with a very high data rate.
- The Infrared Data Association (IrDA) has established standards for using these signals for communication between devices such as keyboards, mouse, PCs, and printers and it is also responsible for sponsoring the use of infrared waves.
- This type of communication provides better security with minimum interference.

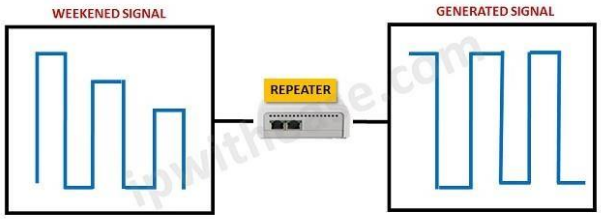
NETWORKDEVICES

Hardware devices that are used to connect computers, printers, fax machines and other electronic devices to a network are called network devices. These devices transfer data in a fast, secure and correct way over same or different networks. Network devices may be inter-network or intra-network. Some devices are installed on the device, like NIC card or RJ45 connector, whereas some are part of the network, like router, switch, etc. Let us explore some of these devices in greater detail.

1. REPEATER

A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network. An important point to be noted about repeaters is that they do not amplify the signal. When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength. It is a 2-port device.

Repeaters are network devices operating at physical layer of the OSI model that amplify or regenerate an incoming signal before retransmitting it. They are incorporated in networks to expand its coverage area. They are also known as signal boosters.



2. HUB

A hub is basically a multiport repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations.

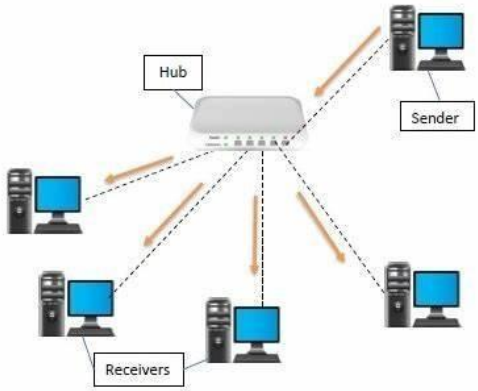
Hubs cannot filter data, so data packets are sent to all connected devices. In other words, collision domain of all hosts connected through Hub remains one. Also, they do not have the intelligence to find out best path for data packets which leads to inefficiencies and wastage.

Types of Hub

- **Active Hub**: -These are the hubs which have their own power supply and can clean, boost, and relay the signal along with the network. It serves both as a repeater as well as wiring centre. These are used to extend the maximum distance between nodes.

- **Passive Hub**: -These are the hubs which collect wiring from nodes and power supply from active hub. These hubs relay signals onto the network without cleaning and boosting them and can‘t be used to extend the distance between nodes.

- **Intelligent Hub**: -It work like active hubs and include remote management capabilities. They also provide flexible data rates to network devices. It also enables an administrator tomonitor the traffic passing through the hub and to configure each port in thehub.



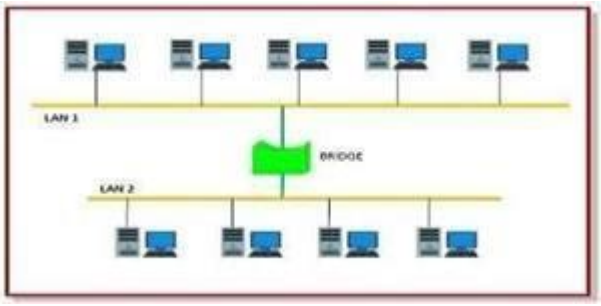
3. BRIDGE

A bridge operates at data link layer. A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of source and destination. It is also used for interconnecting two LANs working on the same protocol. It has a single input and single output port, thus making it a 2-port device.

Types of Bridges

- **Transparent Bridges**: -These are the bridge in which the stations are completely unaware of the bridge ‘s existence i.e., whether or not a bridge is added or deleted from the network, reconfiguration of the stations is unnecessary. These bridges make use of two processes i.e., Bridge forwarding and bridge learning.

- **Source Routing Bridges**: -In these bridges, routing operation is performed by source station and the frame specifies which route to follow. The host can discover frame by sending a special frame called discovery frame, which spreads through the entire network using all possible paths to destination.



4. TWO LAYERSWITCH

A layer 2 switch is a type of network switch or device that works on the data link layer (OSI Layer 2) and utilizes MAC Address to determine the path through where the frames are to be forwarded. It uses hardware-based switching techniques to connect and transmit data in a local area network (LAN).

A layer 2 switch can also be referred to as a multiport bridge. A layer 2 switch is primarily responsible for transporting data on a physical layer and in performing error checking on each transmitted and received frame. A layer 2 switch requires MAC address of NIC on each network node to transmit data. They learn MAC addresses automatically by copying MAC address of each frame received, or listening to devices on the network and maintaining their MAC address in a forwarding table. This also enables a layer 2 switch to send frames quickly to destination nodes. However, like other layer switches (3,4 onwards), a layer 2 switch cannot transmit packet on IP addresses and don‘t have any mechanism to prioritize packets based on sending/receiving application.

5. THREE LAYERSWITCH

A layer 3 switch combines the functionality of a switch and a router. It acts as a switch to connect devices that are on the same subnet or virtual LAN at lightning speeds and has IP routing intelligence built into it to double up as a router. It can support routing protocols, inspect incoming packets, and can even make routing decisions based on the source and destination addresses. This is how a layer 3 switch acts as both a switch and a router. Often referred to as a multilayer switch, a layer 3 switch adds a ton of flexibility to network.

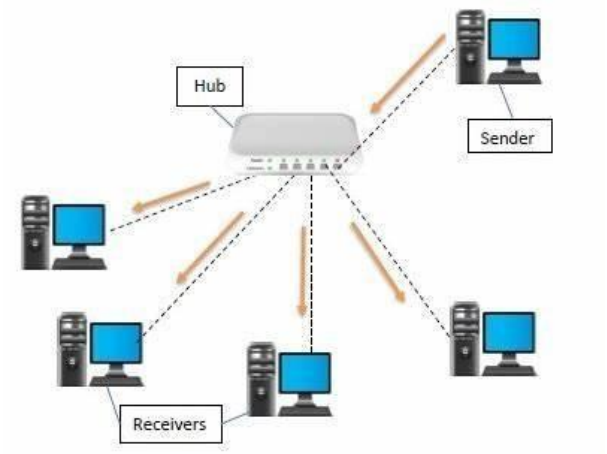
Features of a layer 3 switch

- Comes with 24 Ethernet ports, but no WAN interface.
- Acts as a switch to connect devices within the same subnet.
- Switching algorithm is simple and is the same for most routed protocols.
- Performs on two OSI layers — layer 2 and layer3.

Originally, layer 3 switches were conceived to improve routing performance on large networks, especially corporate intranets. To understand the purpose, let ‘s step back a bit in time to see how these switches evolved.

Layer 2 switches work well when there is low to medium traffic in VLANs. But these switches would hang when traffic increased. So, it became necessary to augment layer 2‘s functionality.

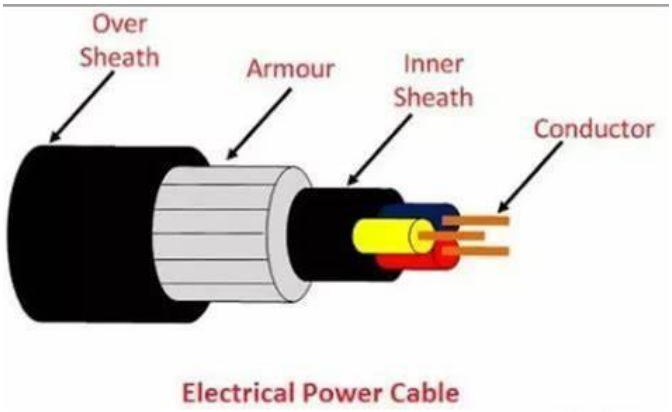
One option was to use a router instead of a switch, but then routers are slower than switches, so this could lead to slower performance.



CABLECONSTRUCTION

A cable used for the transmission and distribution of electrical energy is called electrical power cable. Power cable consists two or more electrical conductors join with an over sheath. It is used for the transmission of extra high voltages in a place where overhead lines are impracticable to use like, the sea, airfield crossing, etc. But underground cable is more costly as compared to aerial cable for the same voltage which is one of the main draws back of electrical power cable.

The power cable mainly consists of three main components, namely, conductor, dielectric, and sheath. The conductor in the cable provides the conducting path for the current. The insulation or dielectric withstands the service voltage and isolates the conductor with other objects. The sheath does not allow the moistures to enter and protects the cables from all external influences like chemical or electrochemical attack, fire, etc. The main components of electrical power cables are explained below in details.



Electrical Power Cable

CONDUCTOR

Coppers and aluminium wires are used as a conductor material in cables because of their high electrical conductivity. Solid or number of bare wires made of either copper or aluminium are used to make a power cable.

For a conductor having more than three wires, the wire is arranged around a centre wire such that there are six in the first layer, twelve in the second, eighteen in the third, and so on. The number of wires in the conductors are 7, 19, 37, 61, 91, etc., The size of the conductor is represented by 7/A, 19/B, 37/C, etc., in which first figures represent the number of strands and the second figure A, B, C ,etc., represents the diameters in cm or mm of the individual wire of the conductors.

INSULATION

The most commonly used dielectric in power cables is impregnated paper, butyl rubber, polyvinyl chloride cable, polyethylene, cross-linked polyethylene. Paper insulated cables are mostly preferred because their current carrying capacity is high, generally reliable and having a long life. The dielectric compound used for the cable should have following properties.

- The insulator must have high insulation resistance.
- It should have high dielectric strength so that it does not allow the leakage current to passthrough it.
- The material must have good mechanical strength.
- The dielectric material should be capable of operating at high temperature.
- It should have low thermal resistance.

- It should have a low power factor. The cables used for submarine and damp soil should use synthetic dielectrics like polyvinyl chloride, polyethylene, etc. These materials are comparatively lighter and have nonmigratory dielectric. Also, such type of dielectric material has good dielectric strength, low power loss, and low thermal resistance.

INNERSHEATH

It is used for protecting the cable from moistures which would affect the insulation. Cable sheath is made up of lead alloy, and these strengths withstand the internal pressures of the pressurized cables. The material used for inner sheath should be nonmagnetic material.

The aluminium sheath is also used in a power cable because it is cheaper, smaller in weight and high mechanical strength than the lead sheath. In oil-filled cables and telephone, cables corrugated seamless aluminium sheath is used because it has better-bending properties, reduced thickness, and lesser weight

PROTECTIVE COVERING

Lead sheath cables when directly laid down on the ground are damaged by corrosion and electrolyte. For protecting the cables against corrosion layers of fibrous material like paper, hessian, etc., or polyvinyl chloride is used. Layers of fibrous material spread with the waterproof compound to the outside of the electrical cable are called serving.

ARMOURING

Armouring is the process in which layers of galvanized steel wires or two layers of metal tape are applied over sheath for protecting it from mechanical damage. The steel wires are normally used for armouring because it has high longitudinal strength. Armouring is also used for earthing the cable. When the fault occurs in the cable (due to insulation failure) the fault current flows through the Armor and get earthed.

OVERSHEATH

It gives the mechanical strength to the cables. It protects the cable from overall damage like moisture, corrosion, dirt, dust, etc. The thermosetting or thermoplastic material is used for making over the sheath.

RESULT: Network media, cables, and devices and Cable Construction are discussed.

EXPERIMENT NO- 02

AIM: Demonstration of basic network commands/utilities in Windows.

OBJECTIVE: To list commands and execute on the CLI to obtain results such as the IP address and ping among many other results.

DESCRIPTION AND EXECUTION:

1) Ipconfig

Ipconfig (Internet Protocol configuration) is among the most common networking tool that allows you to query and show current TCP/IP (Transmission Control Protocol/Internet Protocol) network configuration.

When you type ipconfig at the Command Prompt. You ‘ll see a list of all the network connections your computer is using. Look under ―Wireless LAN adapter‖ if you ‘re connected to Wi-Fi or ―Ethernet adapter if you‘re connected to a wired network.

```
PS C:\Users\91630> ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

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

Wireless LAN adapter Local Area Connection* 1:

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

Ethernet adapter VMware Network Adapter VMnet1:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::12d:4c0e:2439:291f%3
   IPv4 Address. . . . . . . . . . . : 192.168.40.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::8ca2:ddf0:df72:2b3c%10
   IPv4 Address. . . . . . . . . . . : 192.168.236.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : Dlink
   IPv6 Address. . . . . . . . . . . : fd01::97f7:6ef5:6a05:4e3b
   Temporary IPv6 Address. . . . . . : fd01::f5e0:40b8:83ec:f796
   Link-local IPv6 Address . . . . . : fe80::2976:94bb:8fd3:14cb%4
   IPv4 Address. . . . . . . . . . . : 192.168.0.154
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::e21c:fcff:fe11:409%4
                                       192.168.0.1

Ethernet adapter Bluetooth Network Connection:

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

2) Ipconfig /all

all – Displays additional information for all network adapters

```
Windows IP Configuration

   Host Name . . . . . . . . . . . . : LAPTOP-134K2BDF
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : Dlink

Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek PCIe GbE Family Controller
   Physical Address. . . . . . . . . : BC-E9-2F-BF-F4-A4
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
   Physical Address. . . . . . . . . : 8C-C6-81-96-CB-E4
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Ethernet adapter VMware Network Adapter VMnet1:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : VMware Virtual Ethernet Adapter for VMnet1
   Physical Address. . . . . . . . . : 00-50-56-C0-00-01
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::12d:4c0e:2439:291f%3(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.40.1(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : 08 November 2022 10:06:27
   Lease Expires . . . . . . . . . . : 08 November 2022 20:51:27
   Default Gateway . . . . . . . . . :
   DHCP Server . . . . . . . . . . . : 192.168.40.254
   DHCPv6 IAID . . . . . . . . . . . : 704663638
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-26-8B-C4-7A-BC-E9-2F-BF-F4-A4
   NetBIOS over Tcpip. . . . . . . . : Enabled

Ethernet adapter VMware Network Adapter VMnet8:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : VMware Virtual Ethernet Adapter for VMnet8
   Physical Address. . . . . . . . . : 00-50-56-C0-00-08
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::8ca2:ddf0:df72:2b3c%10(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.236.1(Preferred)
```

```
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : 08 November 2022 10:06:27
   Lease Expires . . . . . . . . . . : 08 November 2022 20:51:27
   Default Gateway . . . . . . . . . :
   DHCP Server . . . . . . . . . . . : 192.168.236.254
   DHCPv6 IAID . . . . . . . . . . . : 721440854
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-26-8B-C4-7A-BC-E9-2F-BF-F4-A4
   Primary WINS Server . . . . . . . : 192.168.236.2
   NetBIOS over Tcpip. . . . . . . . : Enabled

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : Dlink
   Description . . . . . . . . . . . : Intel(R) Wi-Fi 6 AX201 160MHz
   Physical Address. . . . . . . . . : 8C-C6-81-96-CB-E3
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : fd01::97f7:6ef5:6a05:4e3b(Preferred)
   Temporary IPv6 Address. . . . . . : fd01::f5e0:40b8:83ec:f796(Preferred)
   Link-local IPv6 Address . . . . . : fe80::2976:94bb:8fd3:14cb%4(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.0.154(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : 07 November 2022 18:45:54
   Lease Expires . . . . . . . . . . : 09 November 2022 20:21:38
   Default Gateway . . . . . . . . . : fe80::e21c:fcff:fe11:409%4
                                       192.168.0.1
   DHCP Server . . . . . . . . . . . : 192.168.0.1
   DHCPv6 IAID . . . . . . . . . . . : 59557505
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-26-8B-C4-7A-BC-E9-2F-BF-F4-A4
   DNS Servers . . . . . . . . . . . : fe80::e21c:fcff:fe11:409%4
                                       192.168.0.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
   Connection-specific DNS Suffix Search List :
                                       Dlink

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Bluetooth Device (Personal Area Network)
   Physical Address. . . . . . . . . : 8C-C6-81-96-CB-E7
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
```

3) Ping:

Verifies IP-level connectivity to another TCP/IP computer by sending Internet Control Message Protocol (ICMP) Echo Request messages. The receipt of corresponding Echo Reply messages is displayed, along with round-trip times. Ping is the primary TCP/IP command used to troubleshoot connectivity, reachability, and name resolution.

It is one of the most basic yet useful network commands to utilize in the command prompt application. It tells you whether your computer can reach some destination IP address or domain name, and if it can, how long it takes data to travel there and back again.

```
PS C:\Users\91630> ping www.youtube.com

Pinging youtube-ui.l.google.com [142.250.182.46] with 32 bytes of data:
Reply from 142.250.182.46: bytes=32 time=16ms TTL=117
Reply from 142.250.182.46: bytes=32 time=17ms TTL=117
Reply from 142.250.182.46: bytes=32 time=16ms TTL=117
Reply from 142.250.182.46: bytes=32 time=17ms TTL=117

Ping statistics for 142.250.182.46:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 16ms, Maximum = 17ms, Average = 16ms
PS C:\Users\91630>
```

4) Tracert tracert

stands for traceroute like ping it sends out a data packet as a way to troubleshoot any network issues you might have, but instead tracks the route of the packet as it hops from server to server

```
PS C:\Users\91630> tracert www.google.com

Tracing route to www.google.com [142.250.196.4]
over a maximum of 30 hops:

  1     1 ms     1 ms     1 ms  dlinkrouter.Dlink [192.168.0.1]
  2     2 ms     2 ms     2 ms  10.130.96.1
  3     *        *        *     Request timed out.
  4     8 ms    40 ms     3 ms  broadband.actcorp.in [183.82.12.70]
  5    16 ms    15 ms    17 ms  broadband.actcorp.in [183.82.14.78]
```

```
PS C:\Users\91630> tracert -h 10 www.youtube.com

Tracing route to youtube-ui.l.google.com [142.250.183.238]
over a maximum of 10 hops:

  1     1 ms     1 ms     1 ms  dlinkrouter.Dlink [192.168.0.1]
  2     *        2 ms     2 ms  10.130.96.1
  3     *        *        *     Request timed out.
  4     4 ms     *       37 ms  broadband.actcorp.in [183.82.12.70]
  5    16 ms    15 ms    15 ms  broadband.actcorp.in [183.82.14.78]
  6    17 ms    16 ms    17 ms  72.14.243.242
  7    17 ms    17 ms    16 ms  72.14.232.71
  8    16 ms    16 ms    16 ms  209.85.247.251
  9    16 ms    16 ms    16 ms  maa05s23-in-f14.1e100.net [142.250.183.238]

Trace complete.
```

5) nslookup:

The nslookup (Name Server Lookup) tool can show valuable details to troubleshoot and resolve DNSrelated issues. You can use this command to display the default DNS name and address of the local device, determine the domain name of an IP address or the name servers for a specific node.

```
PS C:\Users\91630> nslookup www.gmail.com
Server:  UnKnown
Address:  fe80::e21c:fcff:fe11:409

Non-authoritative answer:
Name:    www.gmail.com
Addresses:  2404:6800:4007:824::2005
          142.250.195.101

PS C:\Users\91630>
```

6) netstat:

The netstat (Network Statistics) tool displays statistics for all network connections. It allows you to understand open and connected ports to monitor and troubleshoot networking problems for Windows 10 and apps. When using the netstat tool, you can list active network connections and listening ports. You can view network adapter and protocols statistics. You can even display the current routing table and much more.

```
PS C:\Users\91630> netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:27060        LAPTOP-134K2BDF:55899  ESTABLISHED
  TCP    127.0.0.1:55899        LAPTOP-134K2BDF:27060  ESTABLISHED
  TCP    192.168.0.154:55077    20.198.118.190:https   ESTABLISHED
  TCP    192.168.0.154:55834    103-10-124-123:27019   ESTABLISHED
  TCP    192.168.0.154:59136    20.198.119.84:https    ESTABLISHED
```

7) Arp:

Windows 10 maintains an arp (Address Resolution Protocol) table, which stores IP to Media Access Control (MAC) entries that the system has resolved. The arp tool lets you view the entire table, modify the entries, and use it to determine a remote computer's MAC address. Type the following command to view the current arp table cache on Windows 10 and press Enter: `arp -a'

```
PS C:\Users\91630> arp -a

Interface: 192.168.40.1 --- 0x3
  Internet Address      Physical Address      Type
  192.168.40.254        00-50-56-ef-b0-80     dynamic
  192.168.40.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  228.8.8.8             01-00-5e-08-08-08     static
  239.255.3.22          01-00-5e-7f-03-16     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  239.255.255.251       01-00-5e-7f-ff-fb     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.0.154 --- 0x4
  Internet Address      Physical Address      Type
  192.168.0.1           e0-1c-fc-11-04-09     dynamic
  192.168.0.116         1c-d6-be-c9-27-22     dynamic
  192.168.0.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  228.8.8.8             01-00-5e-08-08-08     static
  239.255.3.22          01-00-5e-7f-03-16     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  239.255.255.251       01-00-5e-7f-ff-fb     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.236.1 --- 0xa
  Internet Address      Physical Address      Type
  192.168.236.254       00-50-56-ea-ff-d7     dynamic
  192.168.236.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  228.8.8.8             01-00-5e-08-08-08     static
  239.255.3.22          01-00-5e-7f-03-16     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  239.255.255.251       01-00-5e-7f-ff-fb     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

8) net

Used for: Displaying available Net switches Command to enter: net

The net command is definitely a versatile one, allowing you to manage many different aspects of a network and its settings such as network shares, users and print jobs, as just a few examples. Running just net won ‘t do much, but it will present you with a list of all the switches that are available. These include accounts to set password and logon requirements, file to show a list of open files and sessions to list, or even disconnect, sessions on the network.

```
PS C:\Users\91630> net
The syntax of this command is:

NET
    [ ACCOUNTS | COMPUTER | CONFIG | CONTINUE | FILE | GROUP | HELP |
      HELPMSG | LOCALGROUP | PAUSE | SESSION | SHARE | START |
      STATISTICS | STOP | TIME | USE | USER | VIEW ]
PS C:\Users\91630>
```

10) hostname

The hostname command provides you with an easy way of identifying the hostname that has been assigned to your Windows device.

```
PS C:\Users\91630> HOSTNAME
LAPTOP-134K2BDF
PS C:\Users\91630>
```

RESULTS:

Ipconfig, ping, tracert, nslookup, netstat, arp, net, hostname and some other commands have been executed and the results have been displayed

EXPERIMENT NO- 03:

AIM: PC Network Configuration.

OBJECTIVE: To demonstrate PC Network Configuration.

ALGORITHM:

1. Start
2. Connect to the internet
3. Gather TCP/IP configuration information
4. Record IP address, Subnet Mask and Default gateway for the computer
5. Compare TCP/IP information with other computers
6. Check additional TCP/IP information 7. End

DESCRIPTION AND EXECUTION:

IP Address:

An Internet Protocol address (IP address) is a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication. An IP address serves two main functions: host or network interface identification and location addressing.

Internet Protocol version 4 (IPv4) defines an IP address as a 32-bit number.

IPv4 Classes:

There are 5 classes of IPv4 addresses:

1) ClassA:

The first bit of the first octet is always set to 0 (zero). Thus the first octet ranges from 1 – 127. Class A addresses only include IP starting from 1.x.x.x to 126.x.x.x only. The IP range 127.x.x.x is reserved for loopback IP addresses.

The default subnet mask for Class A IP address is 255.0.0.0 which implies that Class A addressing can have 126 networks (27 -2) and 16777214 hosts (224 -2).

2) ClassB:

An IP address which belongs to class B has the first two bits in the first octet set to 10. Class B IP Addresses range from 128.0.x.x to 191.255.x.x. The default subnet mask for Class B is 255.255.x.x. Class B has 16384 (214) Network addresses and 65534 (216 -2) Host addresses.

3) ClassC:

The first octet of Class C IP address has its first 3 bits set to 110.

Class C IP addresses range from 192.0.0.x to 223.255.255.x. The default subnet mask for Class C is 255.255.255.x.

Class C gives 2097152 (221) Network addresses and 254 (28 -2) Host addresses.

4)ClassD:

Very first four bits of the first octet in Class D IP addresses are set to 1110.

Class D has IP address range from 224.0.0.0 to 239.255.255.255. Class D is reserved for Multicasting. In multicasting data is not destined for a particular host, that is why there is no need to extract host address from the IP address, and Class D does not have any subnet mask.

4) ClassE:

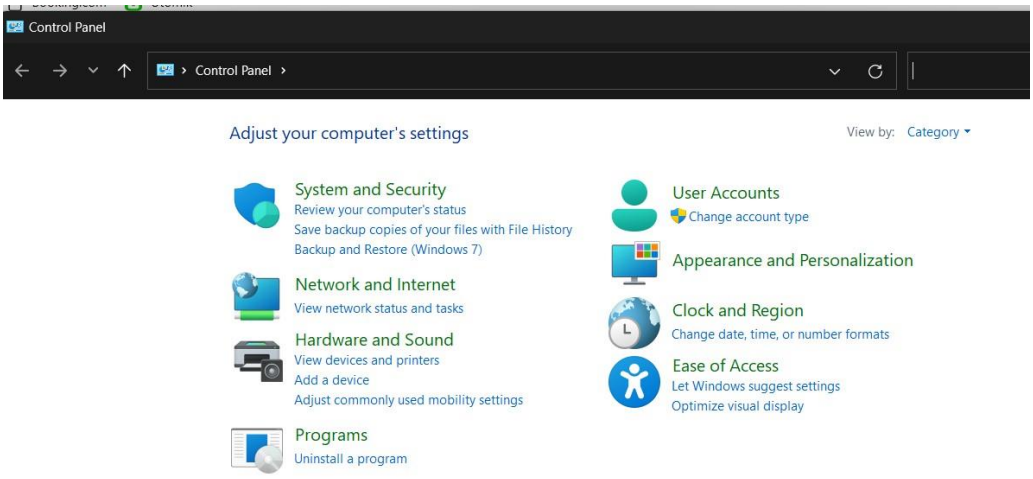
This IP Class is reserved for experimental purposes only for R&D or Study. IP addresses in this class ranges from 240.0.0.0 to 255.255.255.254. Like Class D, this class too is not equipped with any subnet mask.

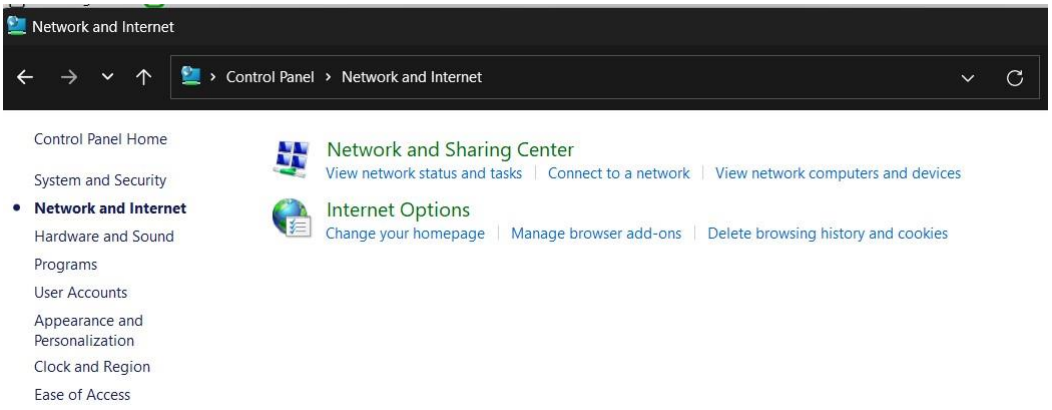
DESCRIPTION AND EXECUTION:

Network Configuration:

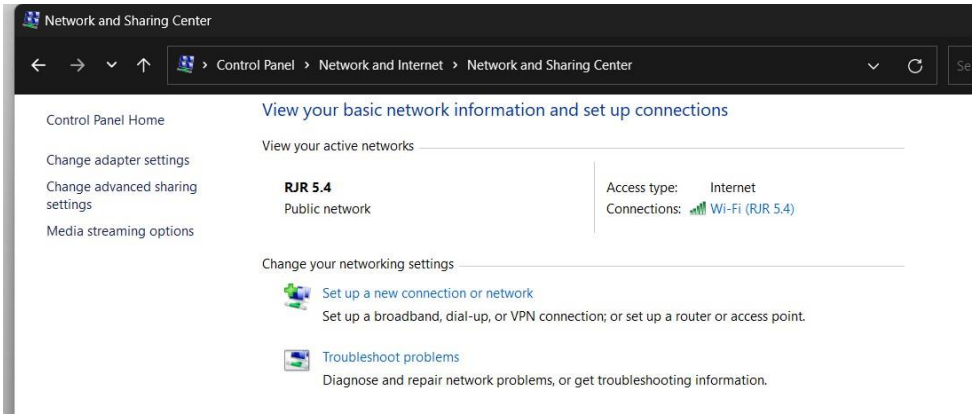
Open Control Panel:

Open Network and Internet:

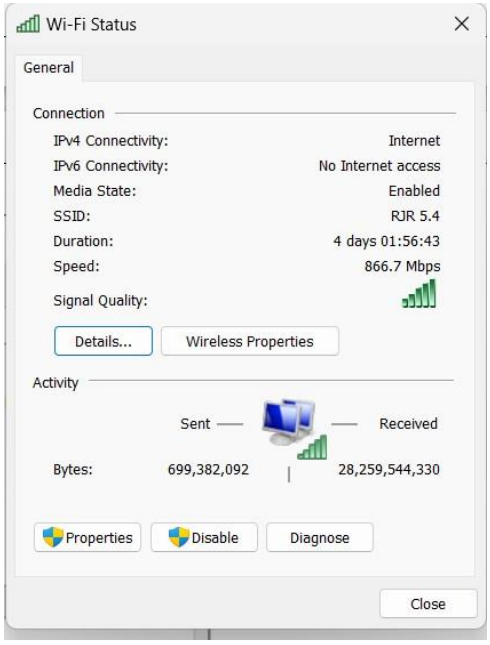




Open Network and Sharing Center:

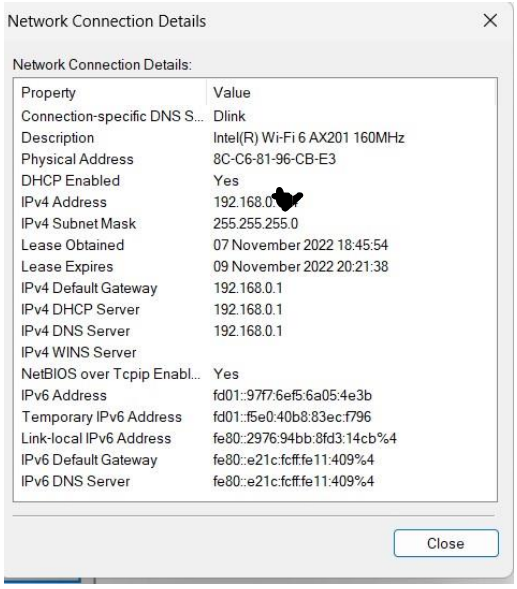


Go to Connection (Wi-Fi or LAN)

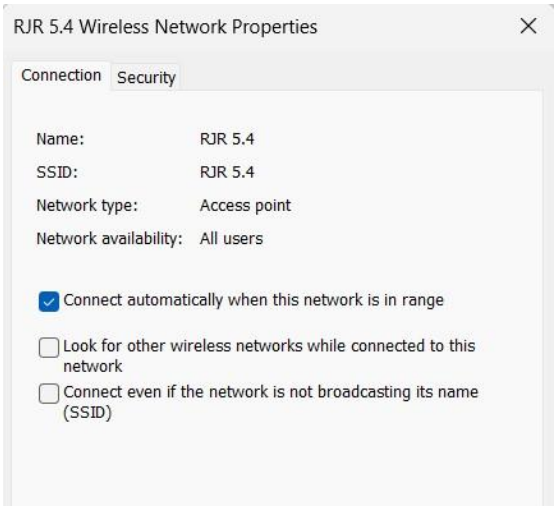


Details:

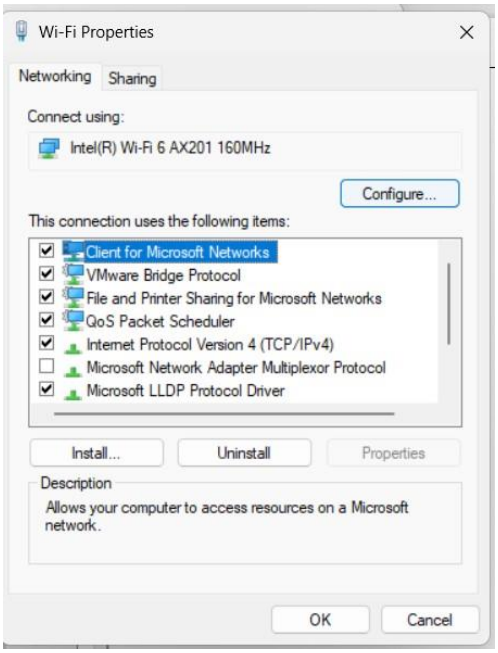
The IP address, Subnet mask and default gateways can be obtained here.



Wireless Properties:

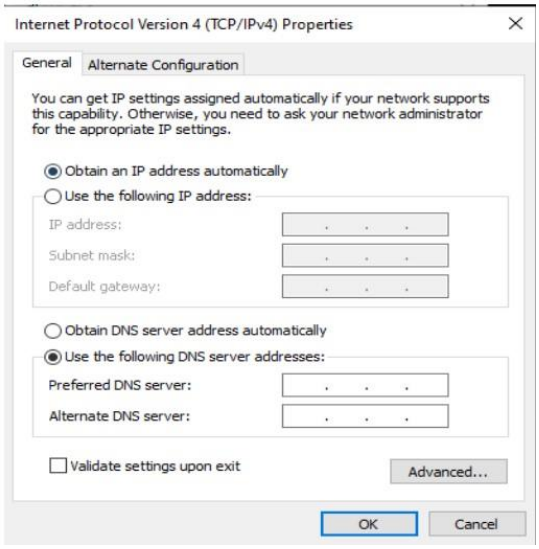


Wi-Fi Properties:



Internet Protocol Version 4 (TCP/IPv4):

The IP address and DNS server addresses can be set manually:



RESULTS: IP classes are studied and PC network configuration info is noted.

EXPERIMENT NO- 04

AIM: Building a switch – based network / Configuration of Cisco Catalyst Switch 3560

OBJECTIVE: To demonstrate building a switch – based network / Configuration Cisco Catalyst Switch3560.

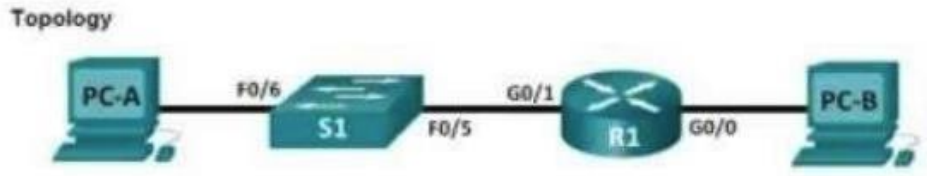
ALGORITHM:

1. Start
2. Setup the Topology and initialize devices
3. Configure Devices and verify connectivity
4. Display Device information
5. End

DESCRIPTION AND EXECUTION:

Resources: 1 Switch, 2 PCs, 1 Router.

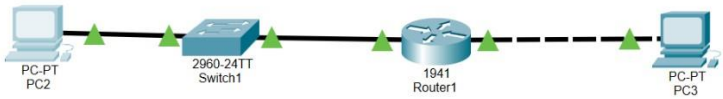
The devices are connected in a star topology:



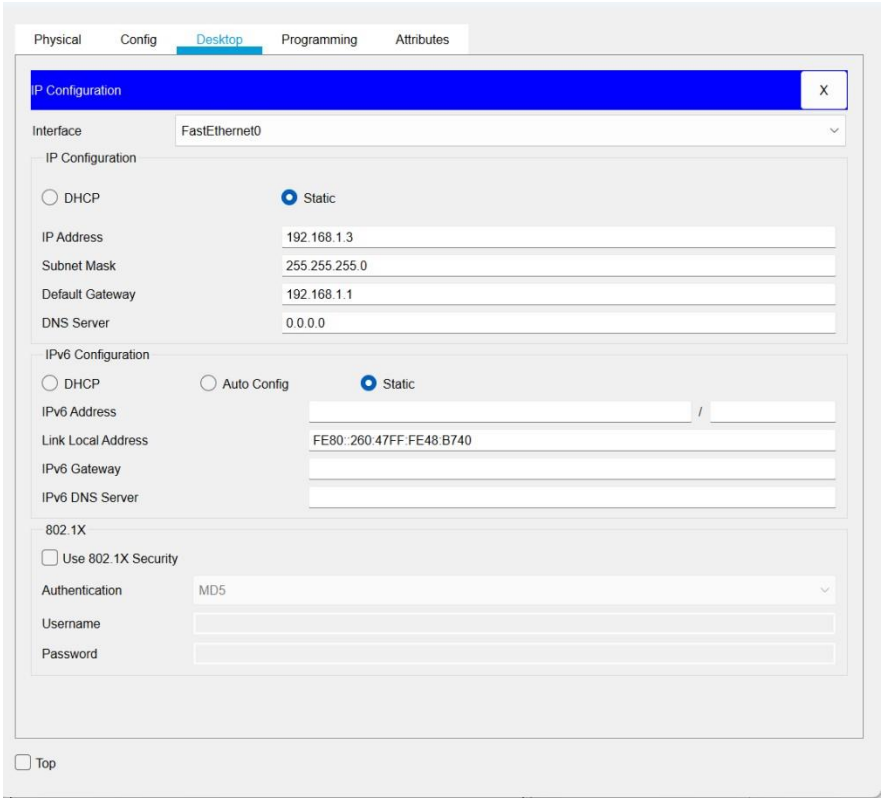
Addressing Table

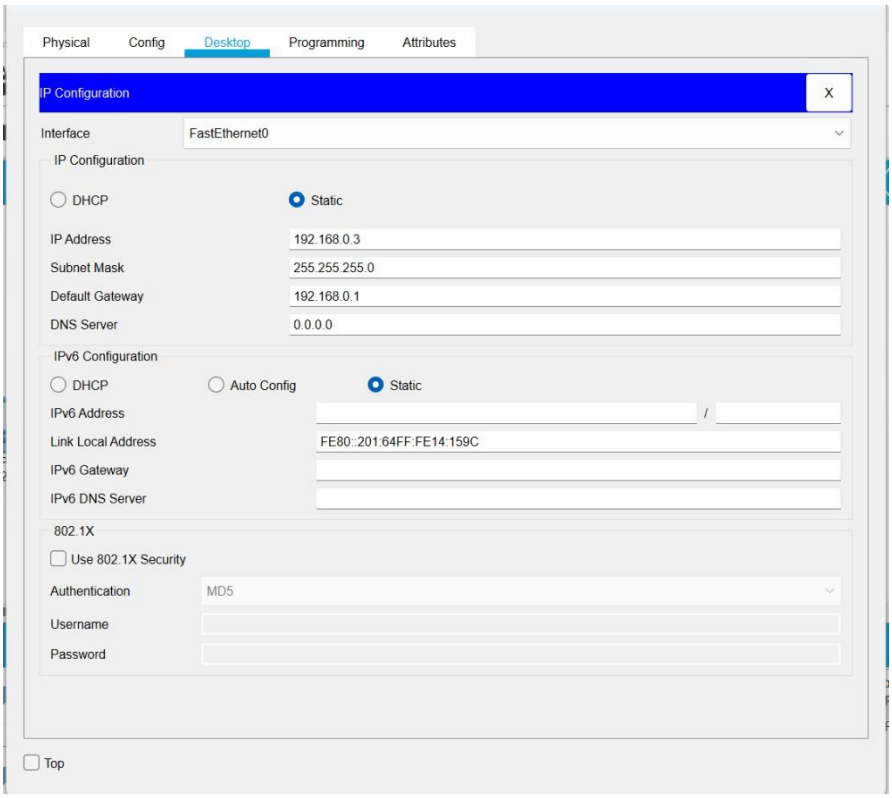
Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	192.168.0.1	255.255.255.0	N/A
	G0/1	192.168.1.1	255.255.255.0	N/A
S1	VLAN 1	N/A	N/A	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.0.3	255.255.255.0	192.168.0.1

Laying out required devices & connecting the devices using cables:

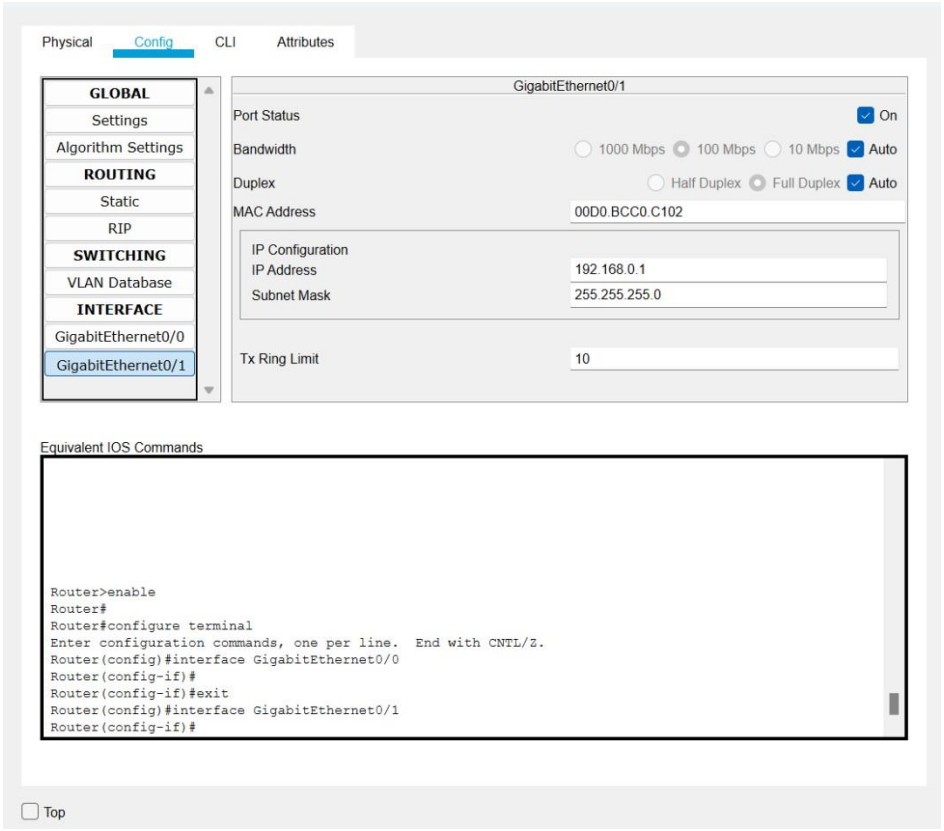


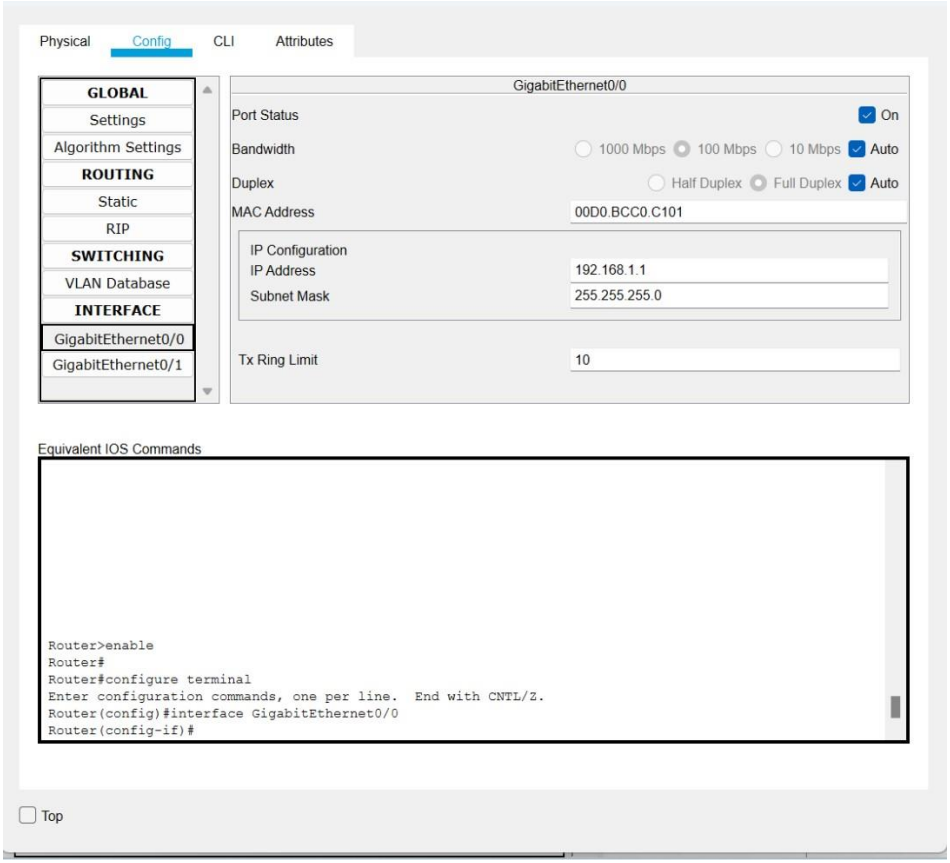
Configuring PC-A and PC-B:

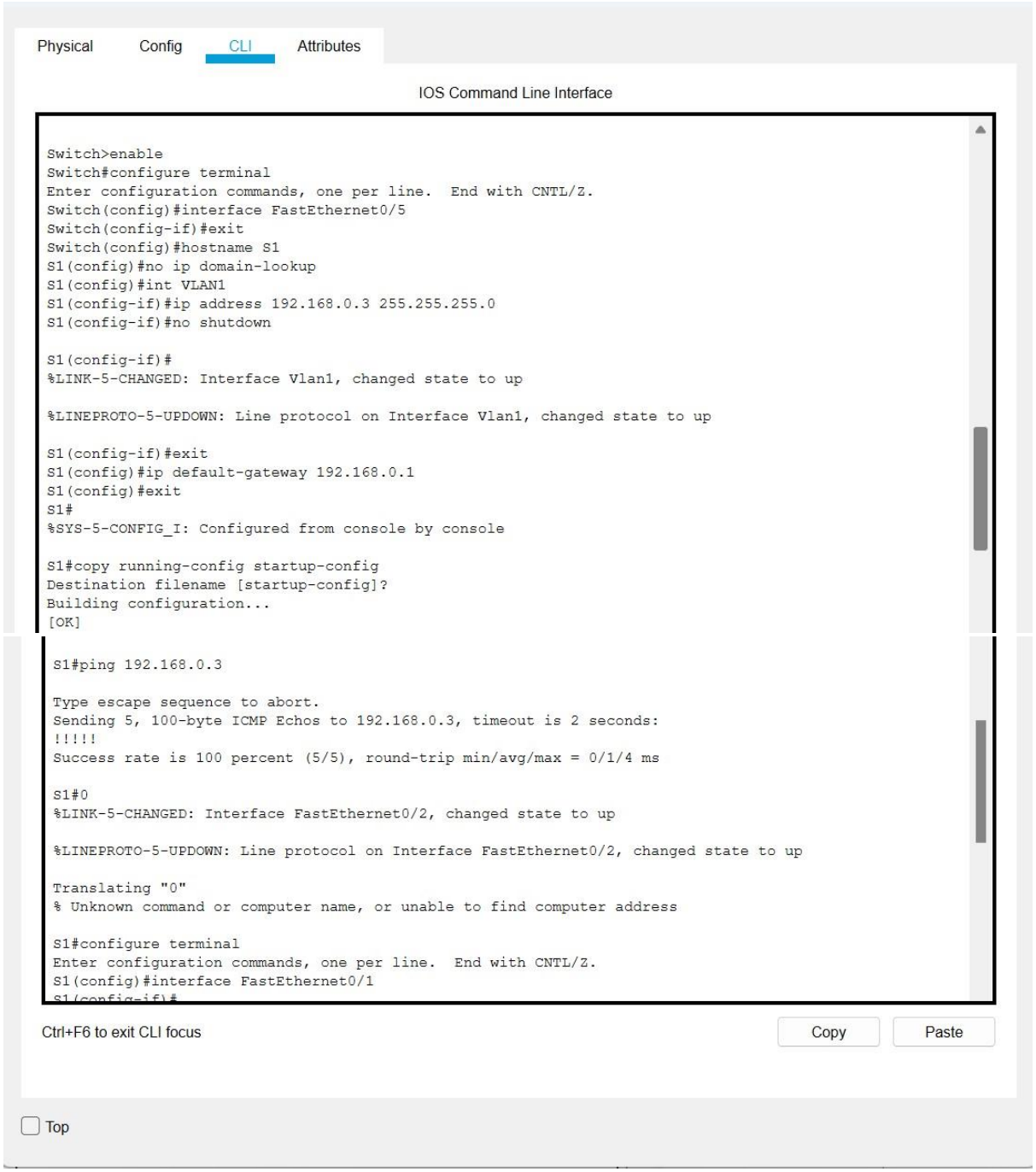




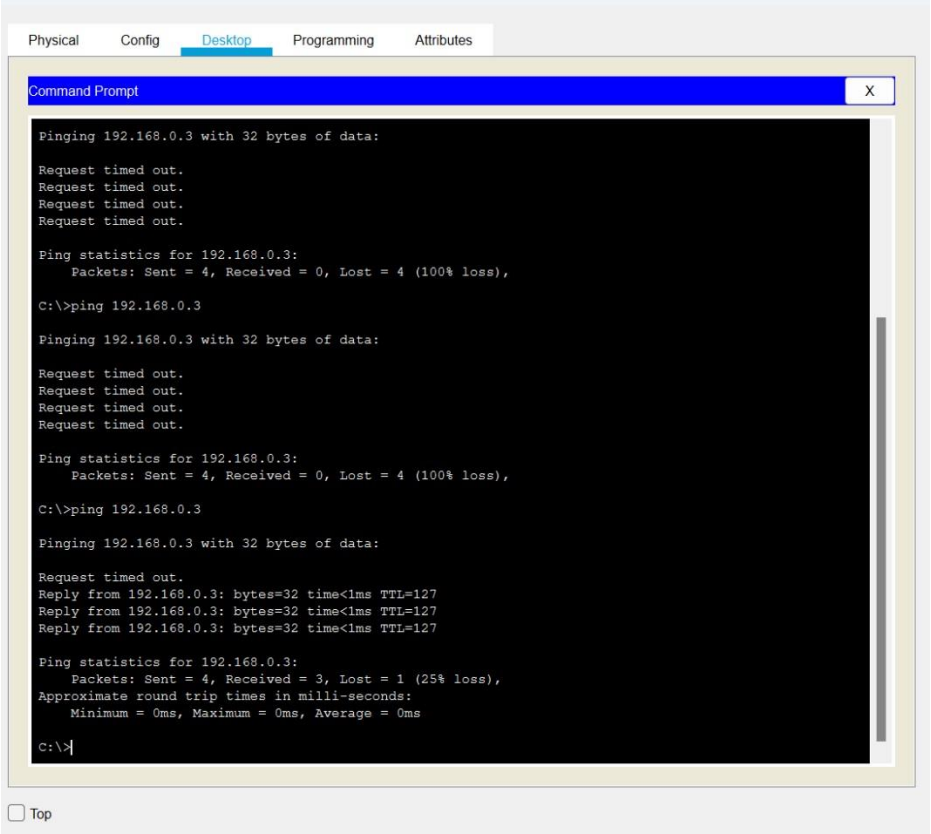
Configuring Switch S1:


Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
GigabitEthernet0/1
Port Status
On
Bandwidth
1000 Mbps
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
00D0.BCC0.C102
IP Configuration
IP Address
192.168.0.1
Subnet Mask
255.255.255.0
Tx Ring Limit
10
Equivalent IOS Commands
Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/1
Router(config-if)#
Top


Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
GigabitEthernet0/0
Port Status
On
Bandwidth
1000 Mbps
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
00D0.BCC0.C101
IP Configuration
IP Address
192.168.1.1
Subnet Mask
255.255.255.0
Tx Ring Limit
10
Equivalent IOS Commands
Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0
Router(config-if)#
Top



Checking ping from PC-A to PC-B:



RESULTS: After the configuration and connection of all devices, the ping is successful from PC-A to PC-B.

EXPERIMENT NO – 5

AIM: Configuration of Cisco Router 2900

OBJECTIVE: To demonstrate Configuration of Cisco Router 2900

ALGORITHM:

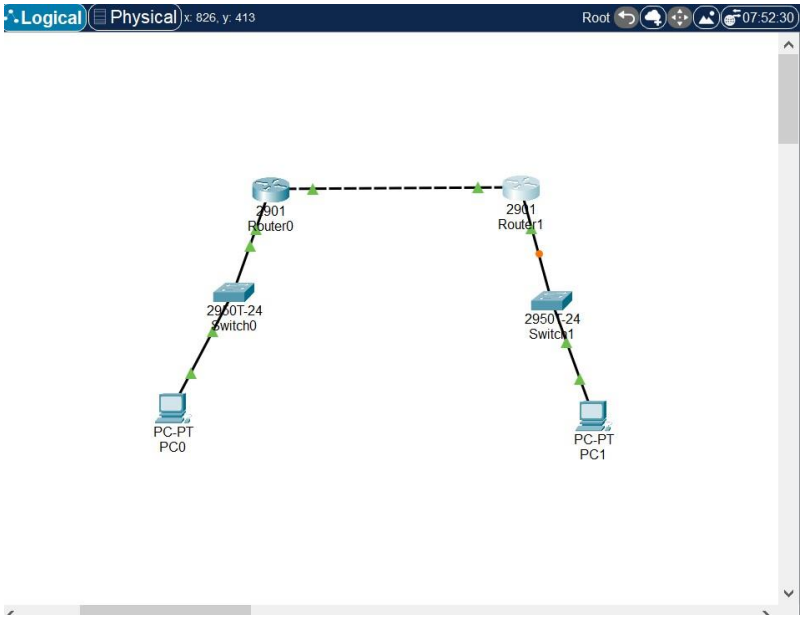
1. Start
2. Setup the Topology and initialize devices
3. Configure Devices and router and verify connectivity
4. Display Device information
5. End

DESCRIPTION AND EXECUTION:

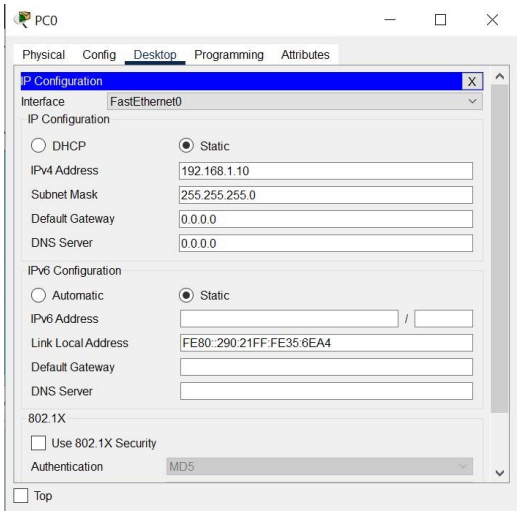
Resources: 2 Switch, 2 PCs, 2 Router.

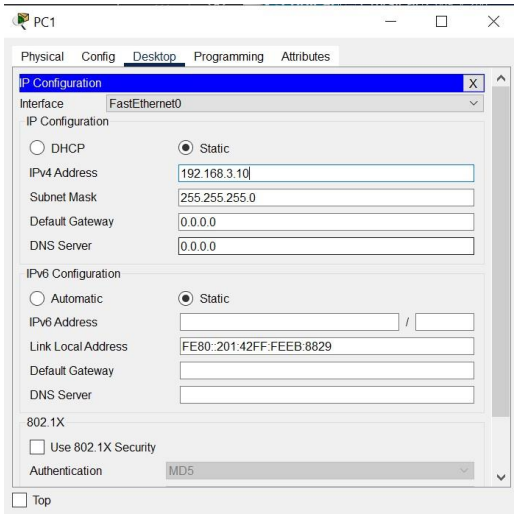
Device	Interface	IP Address	Subnet Mask	Def. Gateway
R1	Fa0/0	192.168.1.1	255.255.255.0	N/A
	S0/0/0	192.168.2.1	255.255.255.0	N/A
R2	Fa0/0	192.168.3.1	255.255.255.0	N/A
	S0/0/0	192.168.2.2	255.255.255.0	N/A
PC1	N/A	192.168.1.10	255.255.255.0	192.168.1.1
PC2	N/A	192.168.3.10	255.255.255.0	192.168.3.1

Connecting the devices using cables:

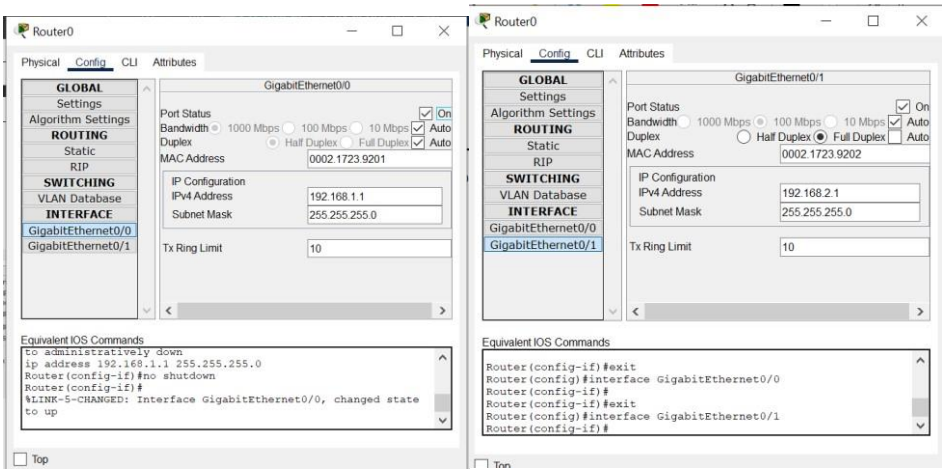


Configuring PC-A and PC-B:

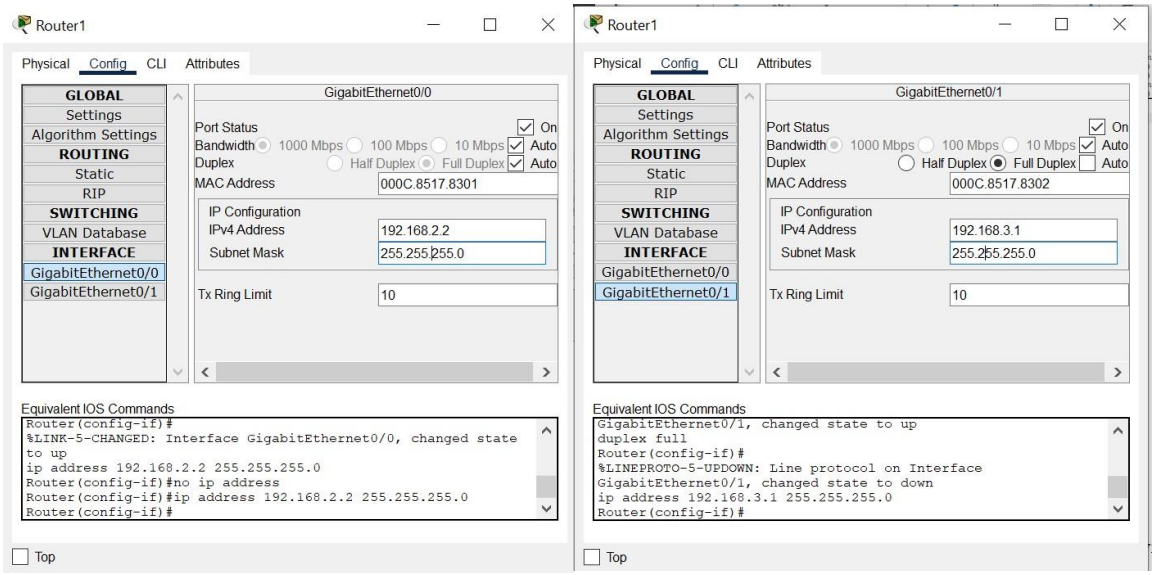




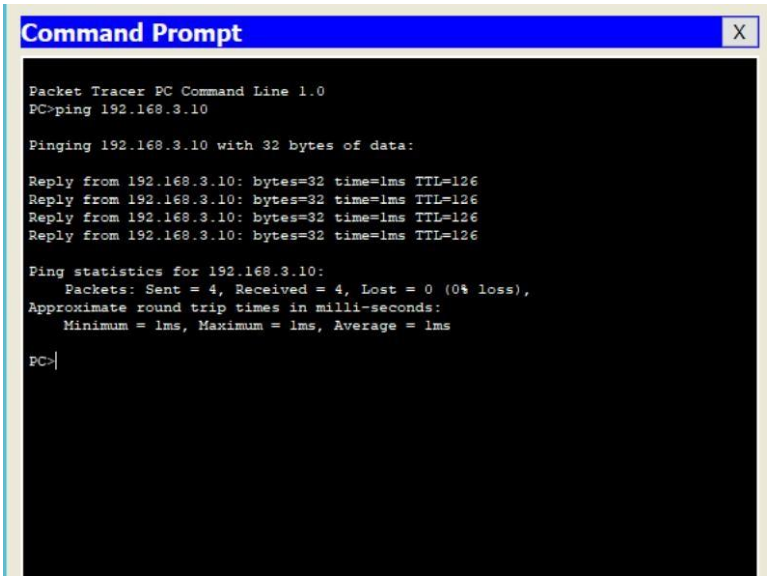
Configuring router 1:



Configuring router 2:



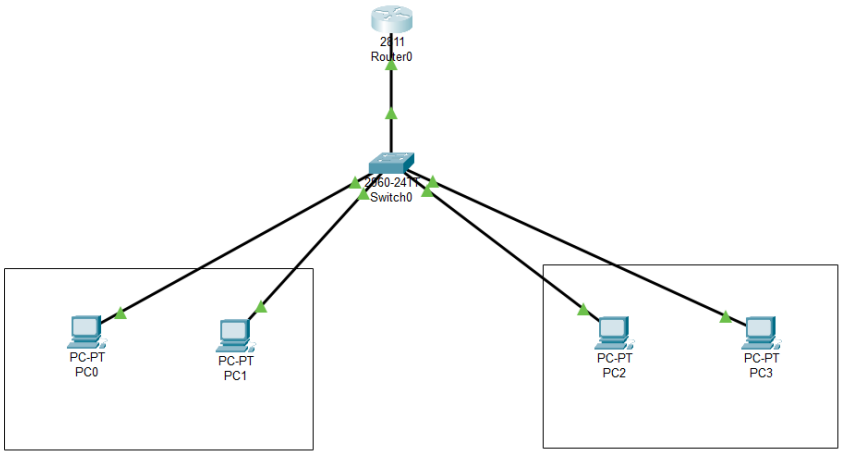
Checking ping from PCA to PCB:



RESULTS: After the configuration and connection of all devices, the ping is successful from PC-A to PC-B

EXPERIMENT-06

AIM: Configuration of Virtual Area Network (VLAN) in Cisco switch.



DESCRIPTION:

- Virtual LAN (VLAN) is a concept in which we can divide the devices logically on layer 2 (data link layer).
- It is a custom network which is created from one or more local area networks.
- It enables a group of devices available in multiple networks to be combined into one logical network.
- The result becomes a virtual LAN that is administered like a physical LAN.
- Network partition allows computers and devices in VLAN to communicate in a stimulated environment as if it is a separate LAN.

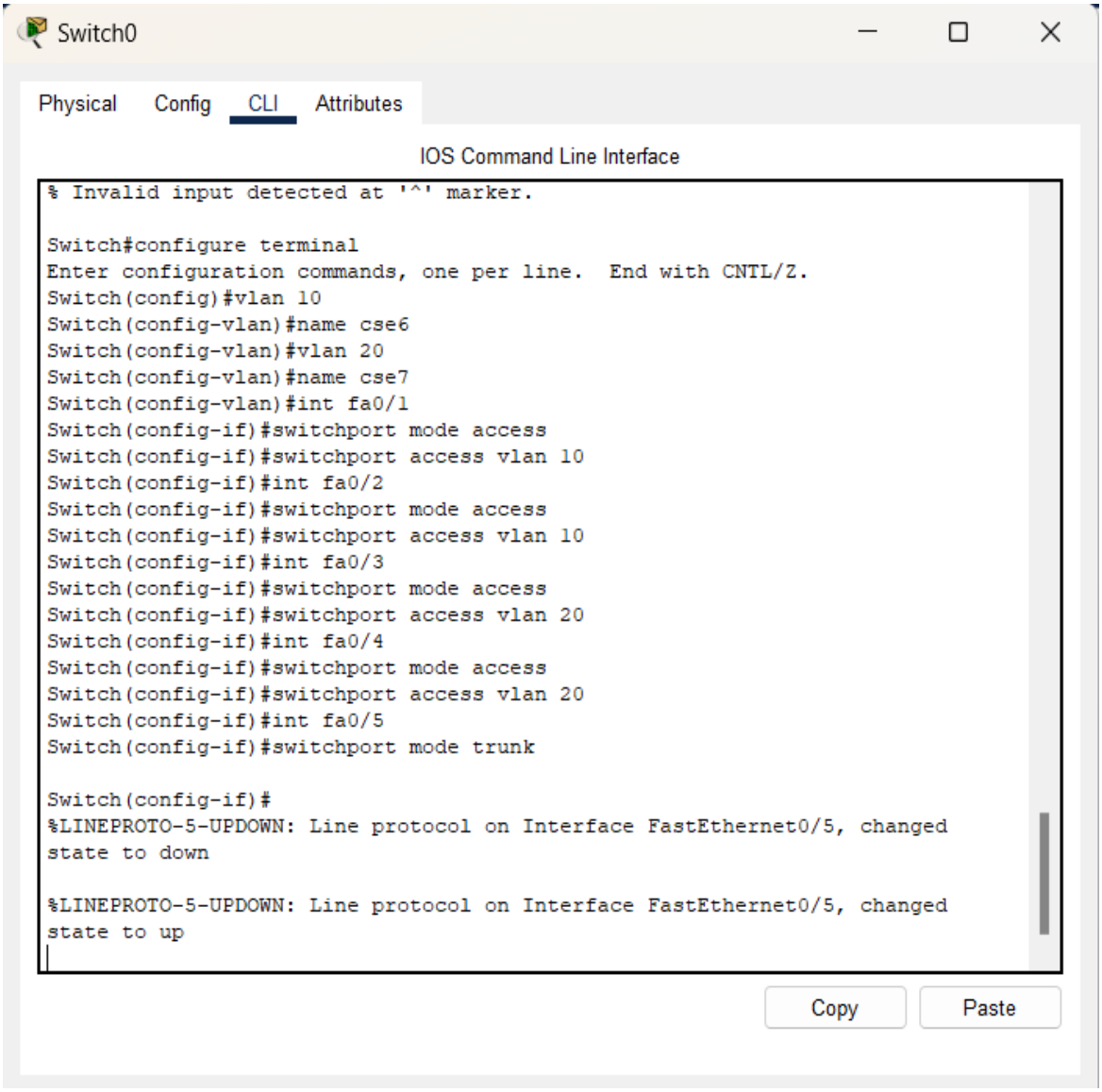
Important characteristics of VLAN:

- Virtual LANs offer structure for making groups of devices, even if their networks are different.
- It increases the broadcast domains possible in a LAN.
- Implementing VLANs reduces the security risks as the number of hosts which are connected to the broadcast domain decreases.
- This is performed by configuring a separate virtual LAN for only the hosts having sensitive information.
- It has a flexible networking model that groups users depending on their departments instead of network location.

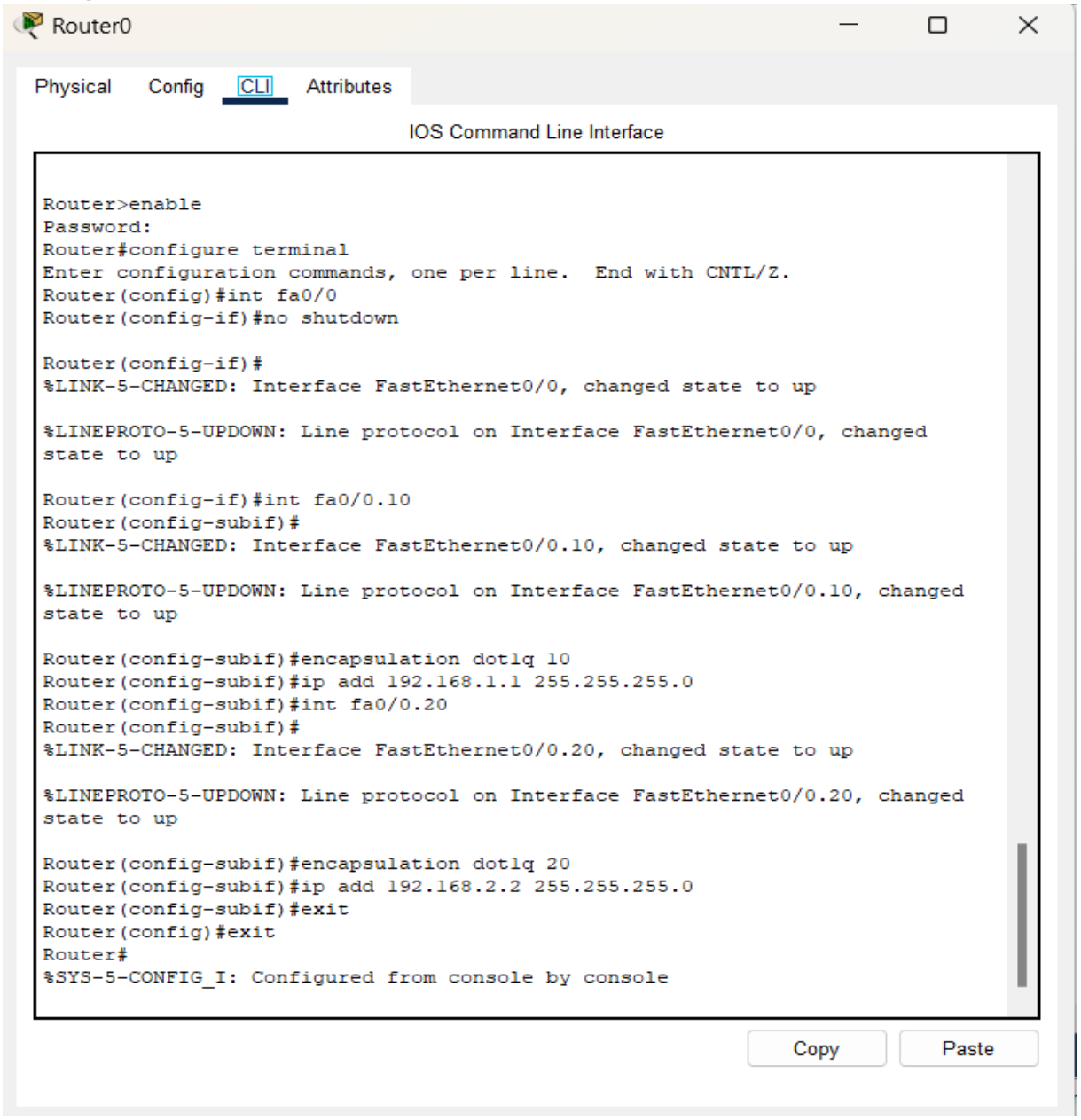
Devices	IP address	Default Gateway
PC-0	192.168.1.10	192.168.1.1
PC-1	192.168.1.20	192.168.1.1
PC-2	192.168.2.10	192.168.2.2
PC-3	192.168.2.20	192.168.2.2
Router	192.168.1.1	PC-0 & PC-1
	192.168.2.2	PC-2 & PC-3

EXECUTION:

Configure Switch:

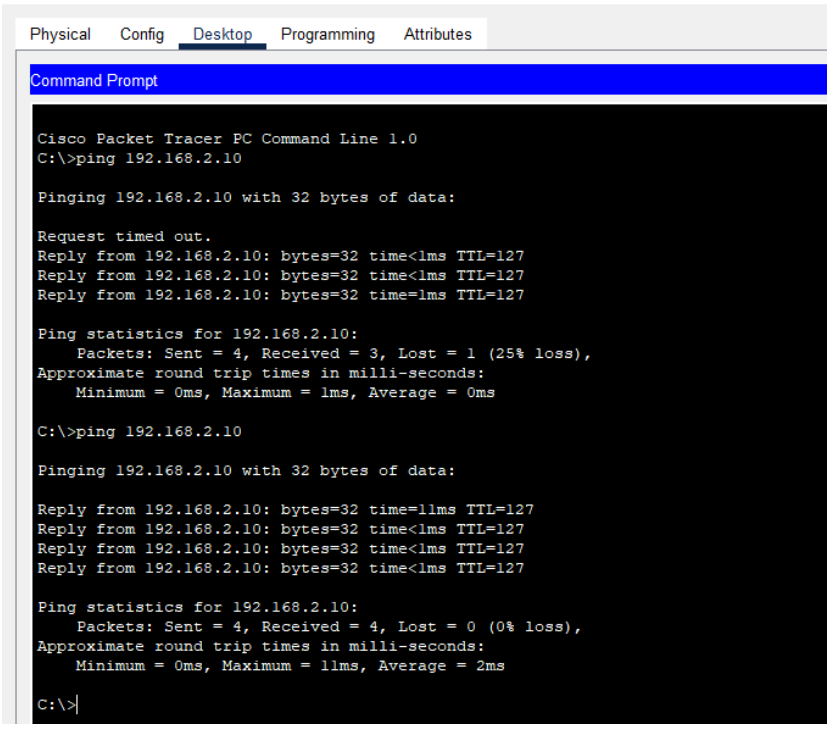


Configure Router:

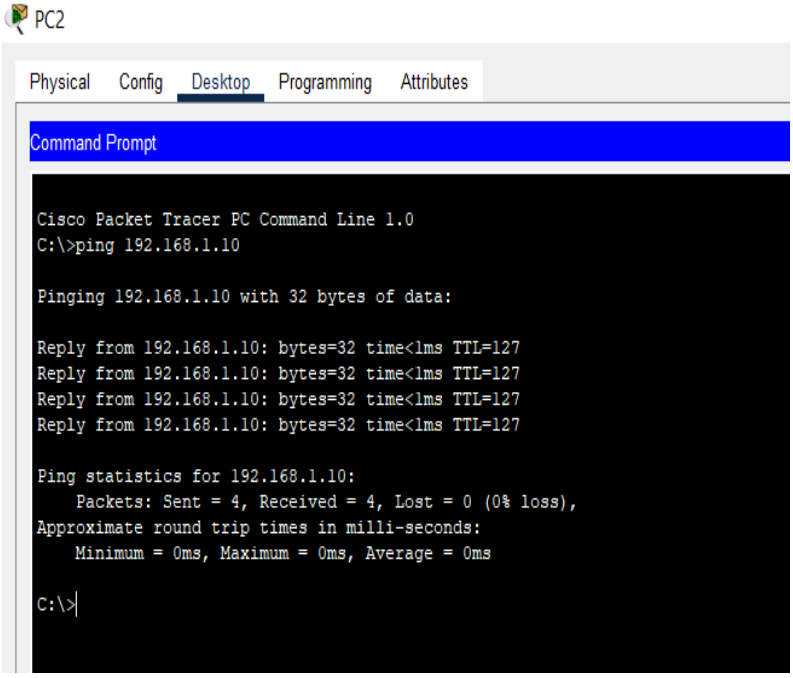


OUTPUT:

PC0



PC2



CONCLUSION:

Hence the VLAN is configured using a switch and connectivity is verified using ping command

EXPERIMENT NO – 7

AIM: Static routing

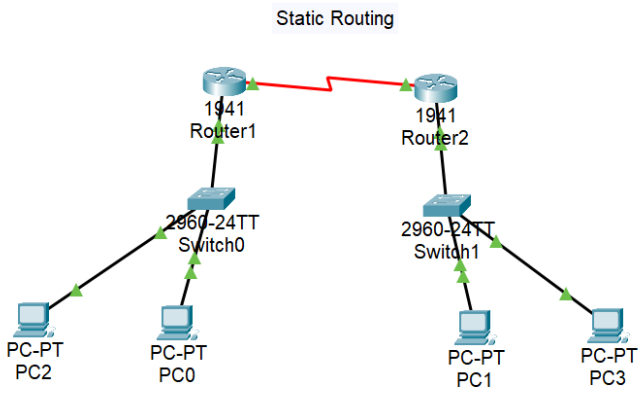
OBJECTIVE: To demonstrate the static routing.

ALGORITHM:

1. Start
2. Setup the Topology and initialize devices
3. Configure Devices and router and verify connectivity
4. Display Device information
5. End

DESCRIPTION AND EXECUTION:

Resources: 2 Switches, 4 PCs, 2 Routers.

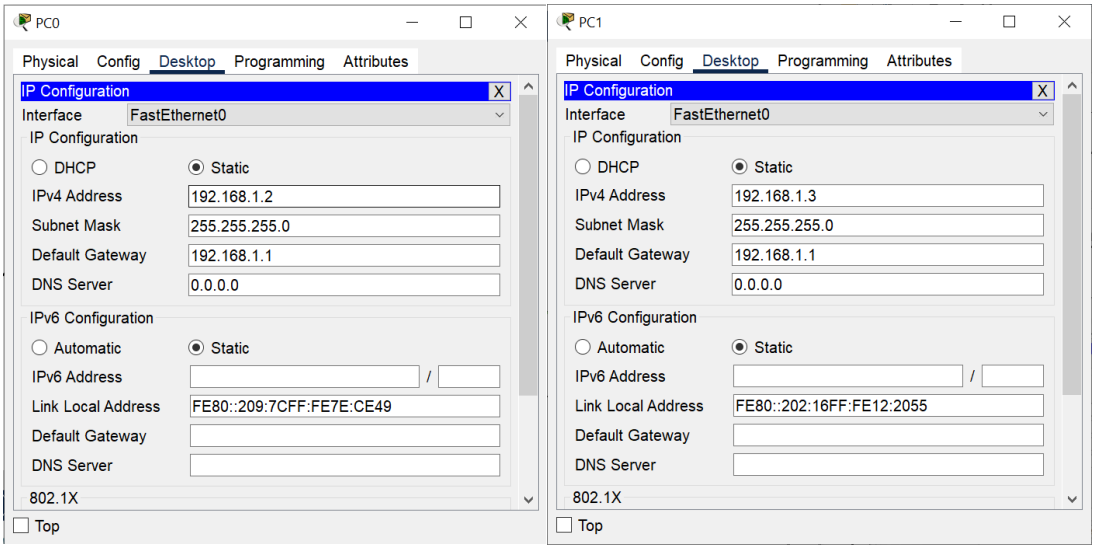


Router no.:1941

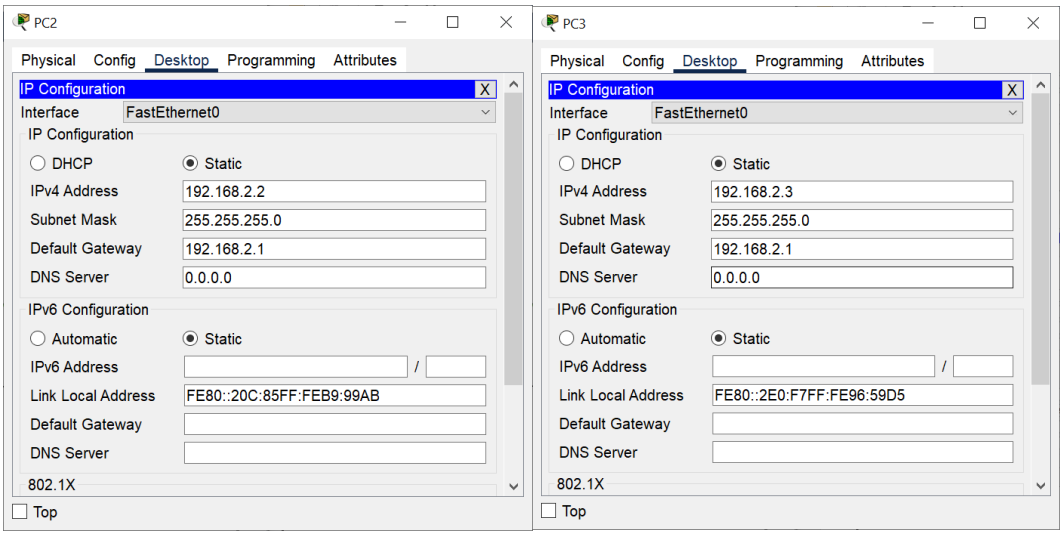
Switch no: 2960 -24

Device	Interface	IP Address	Subnet Mask	Def. Gateway
R1	Fa0/0	192.168.1.1	255.255.255.0	N/A
	S0/0/0	10.10.10.1	255.0.0.0	N/A
R2	Fa0/0	192.168.2.1	255.255.255.0	N/A
	S0/0/0	10.10.11.1	255.0.0.0	N/A
PC0	N/A	192.168.1.2	255.255.255.0	192.168.1.1
PC1	N/A	192.168.1.3	255.255.255.0	192.168.1.1
PC2	N/A	192.168.2.2	255.255.255.0	192.168.2.1
PC3	N/A	192.168.2.3	255.255.255.0	192.168.2.1

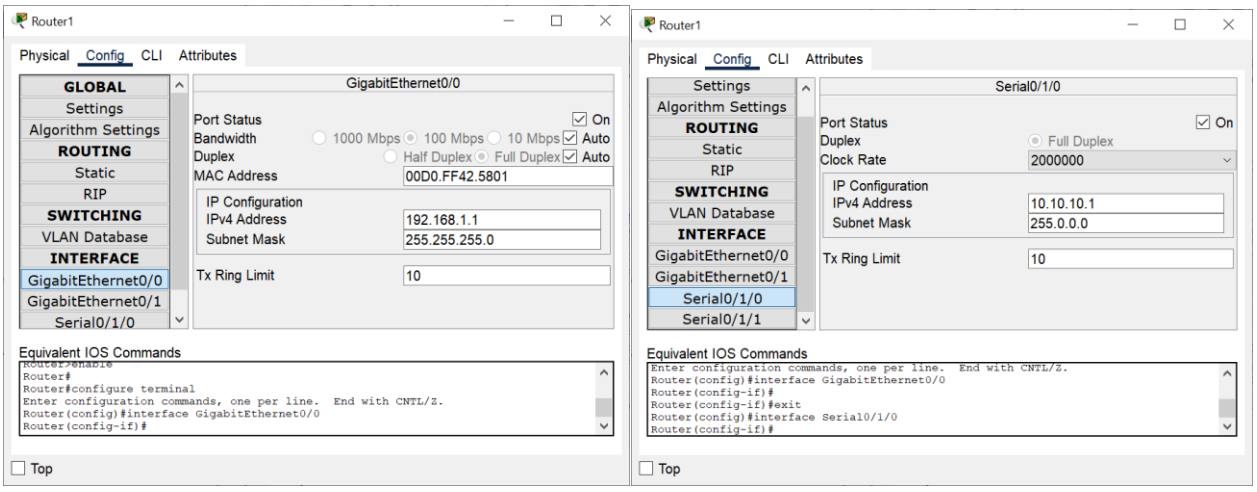
Configuring PC0 and PC1:



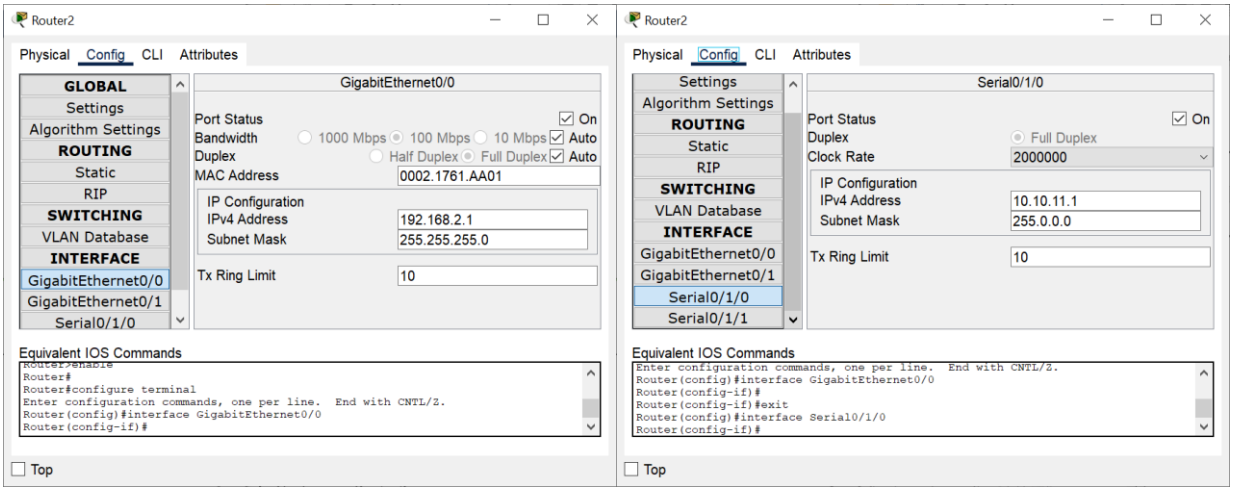
Configuring PC2 and PC3:



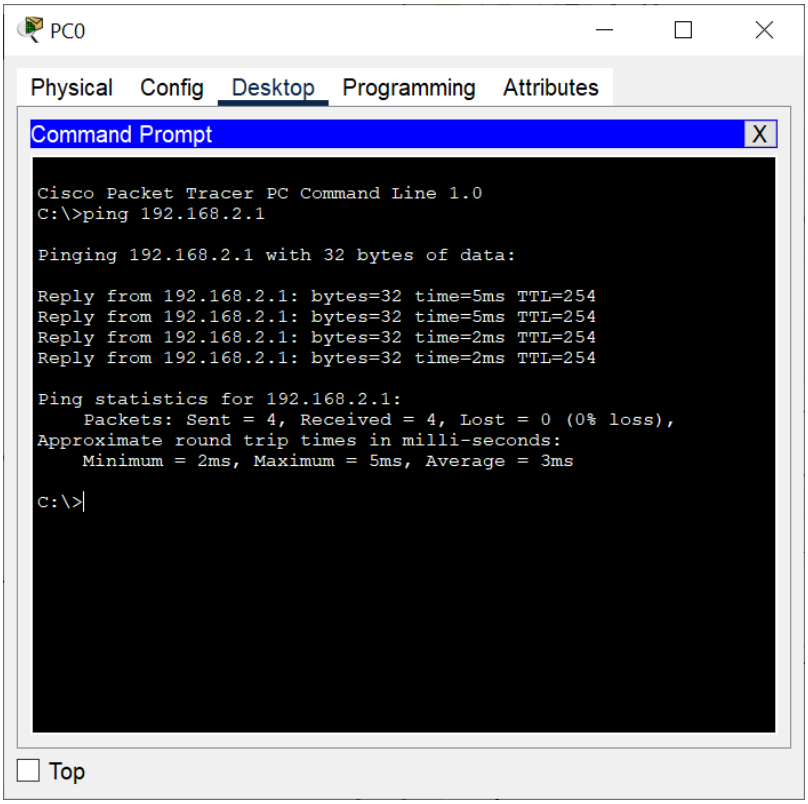
Configuring Router 1:



Configuring Router 2:



Checking connection ping from PC0 to PC2:



RESULTS: After the configuration and connection of all devices, the ping is successful from PC-0(router 1) to PC-2(router 2)

EXPERIMENT NO – 8

AIM: Basic OSPF Configuration

OBJECTIVE: To demonstrate Basic OSPF Configuration.

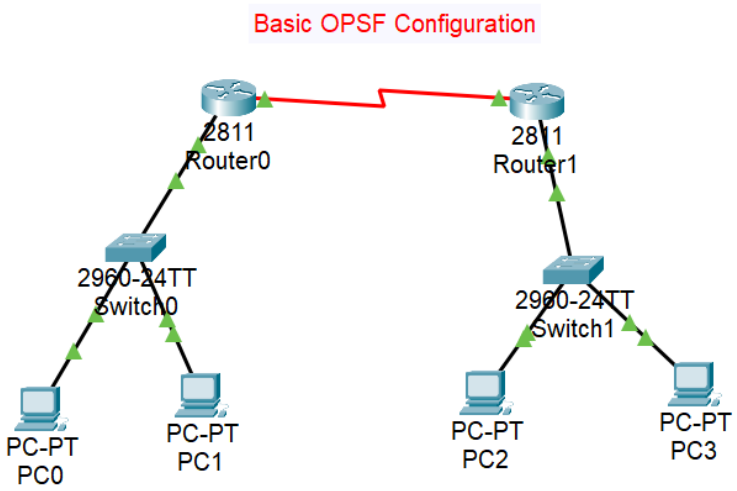
ALGORITHM:

1. Start
2. Setup the Topology and initialize devices
3. Configure Devices and router and verify connectivity
4. Display Device information
5. End

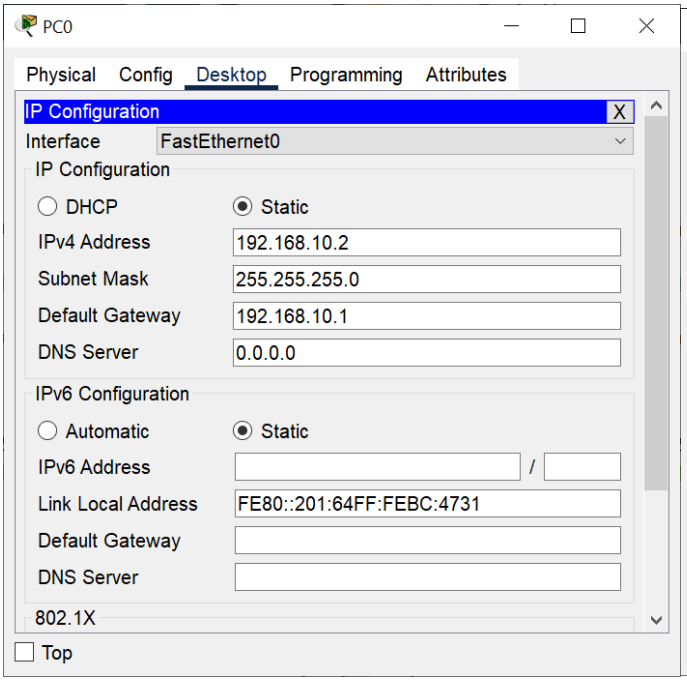
DESCRIPTION AND EXECUTION:

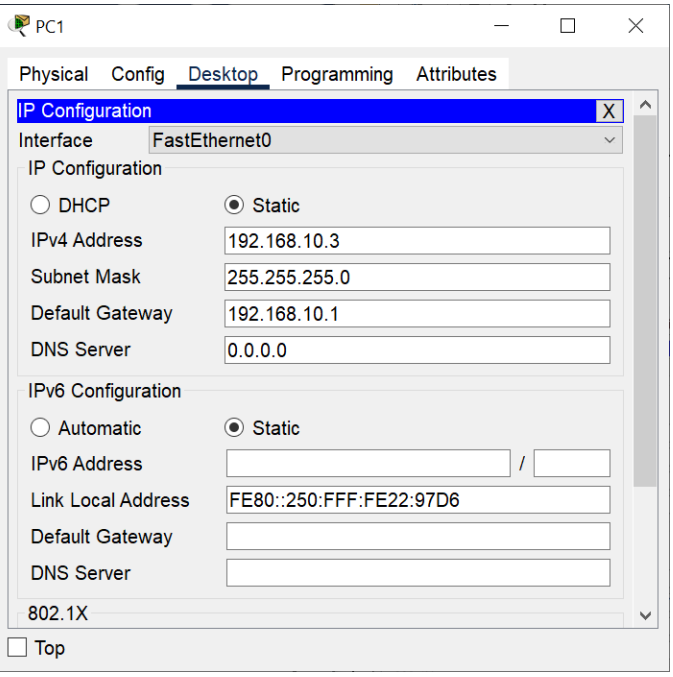
- OSPF is a link-state routing protocol. Link-state protocols use the shortest path first (SPF) algorithm to populate the routing table. OSPF shares information with every router in the network.
- OSPF is considered a difficult protocol to configure and requires a thorough understanding of terms that are commonly used.

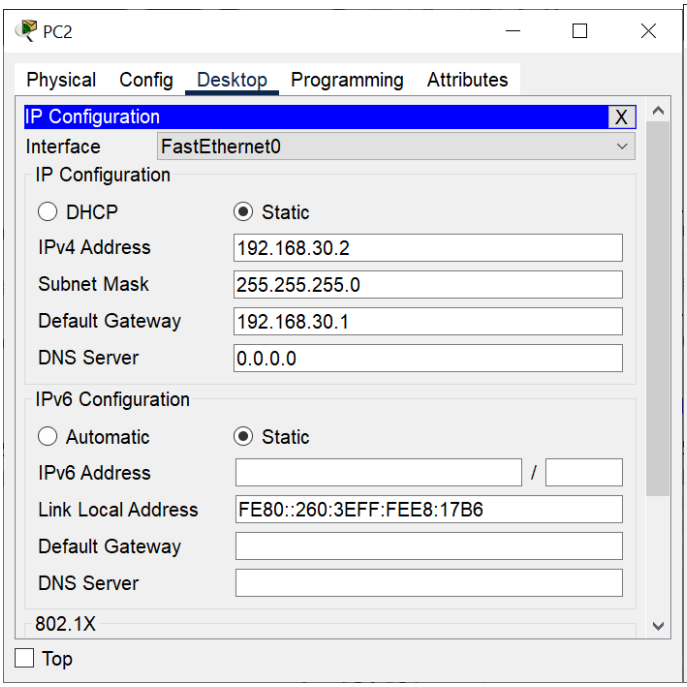
Connecting the devices using cables:

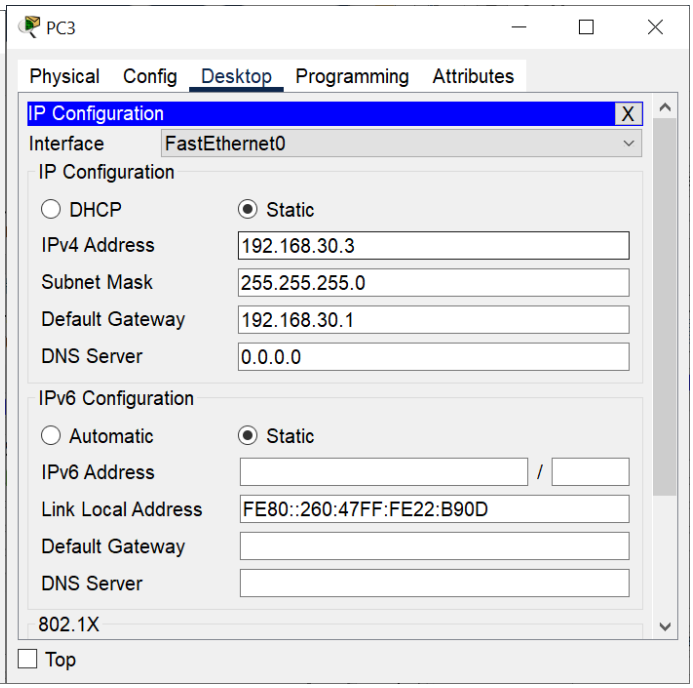


Configuring PCs:



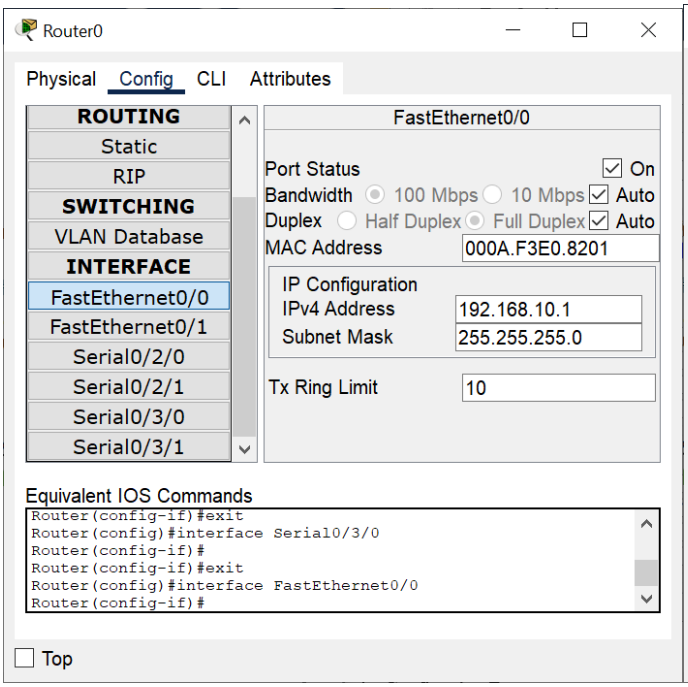


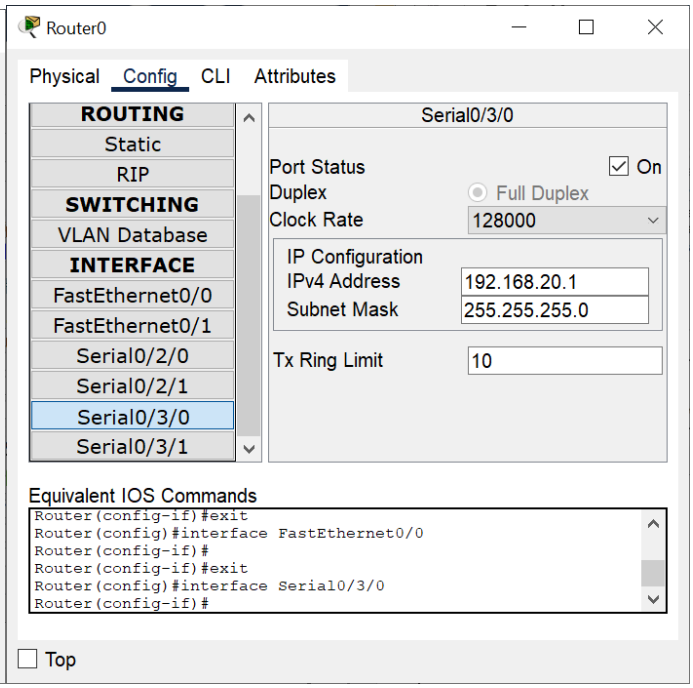




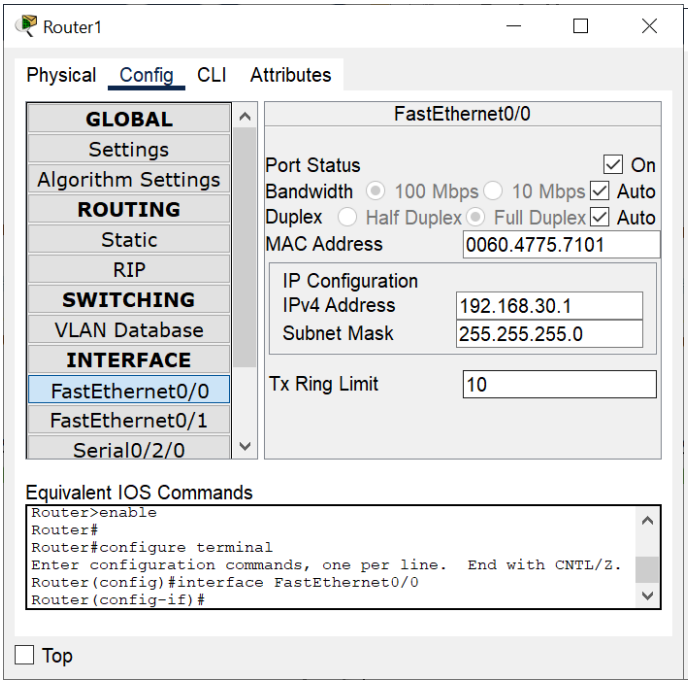
Configuring Routers:

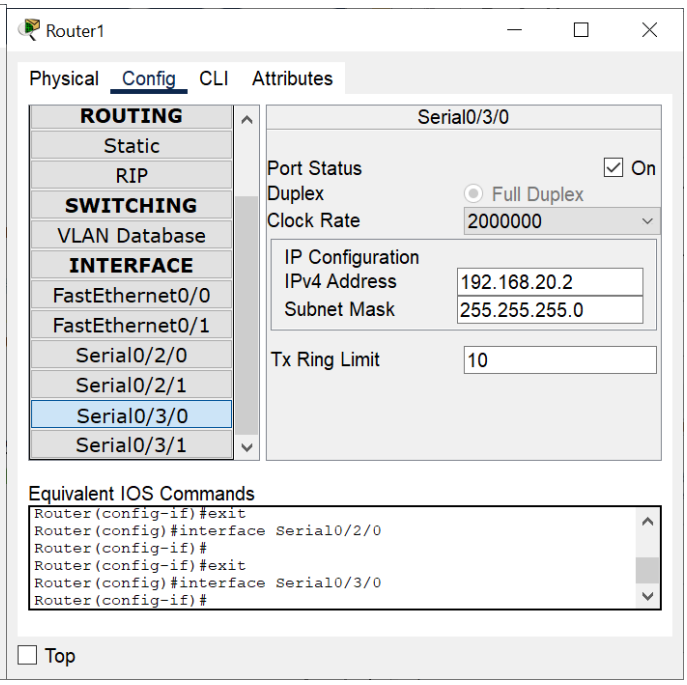
Router 0 : Config



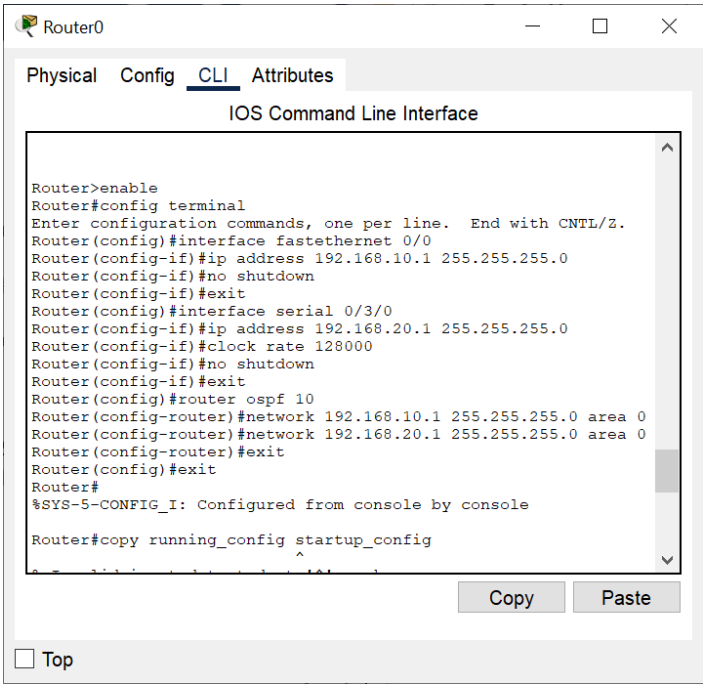


Router 1 : Config

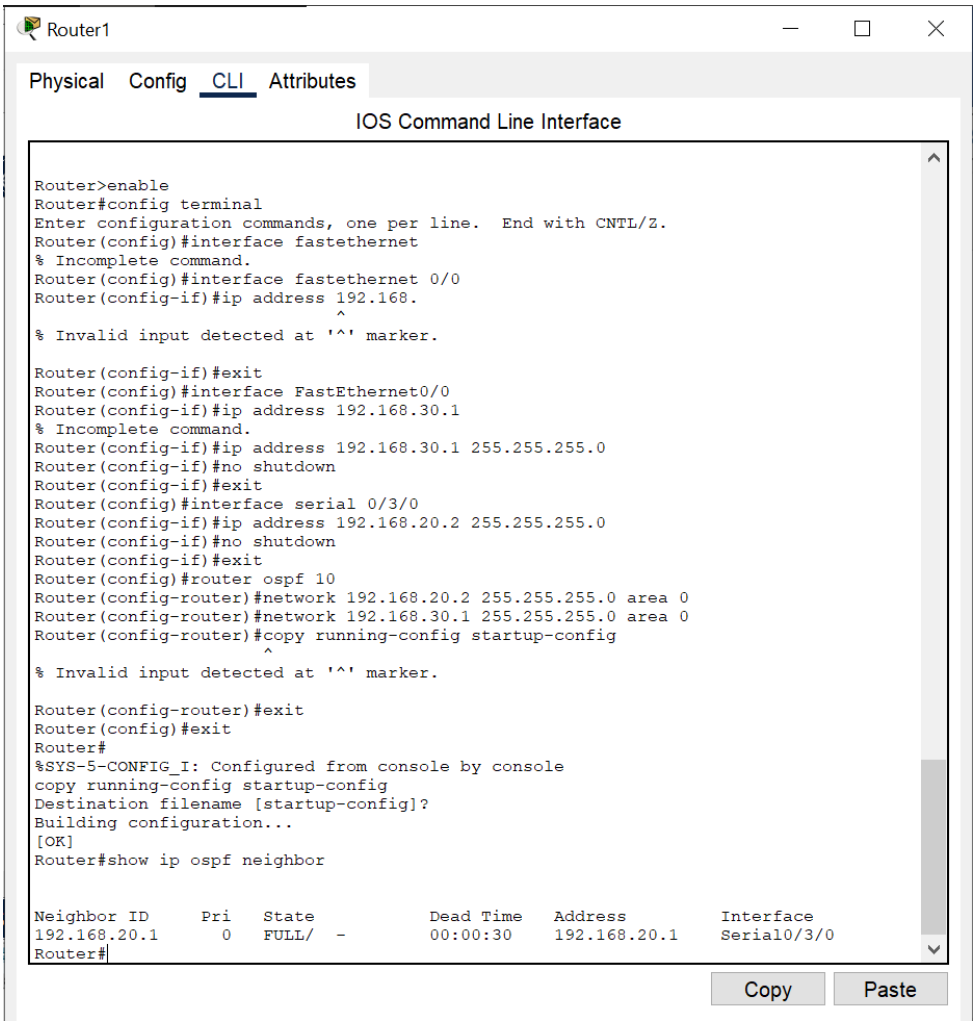




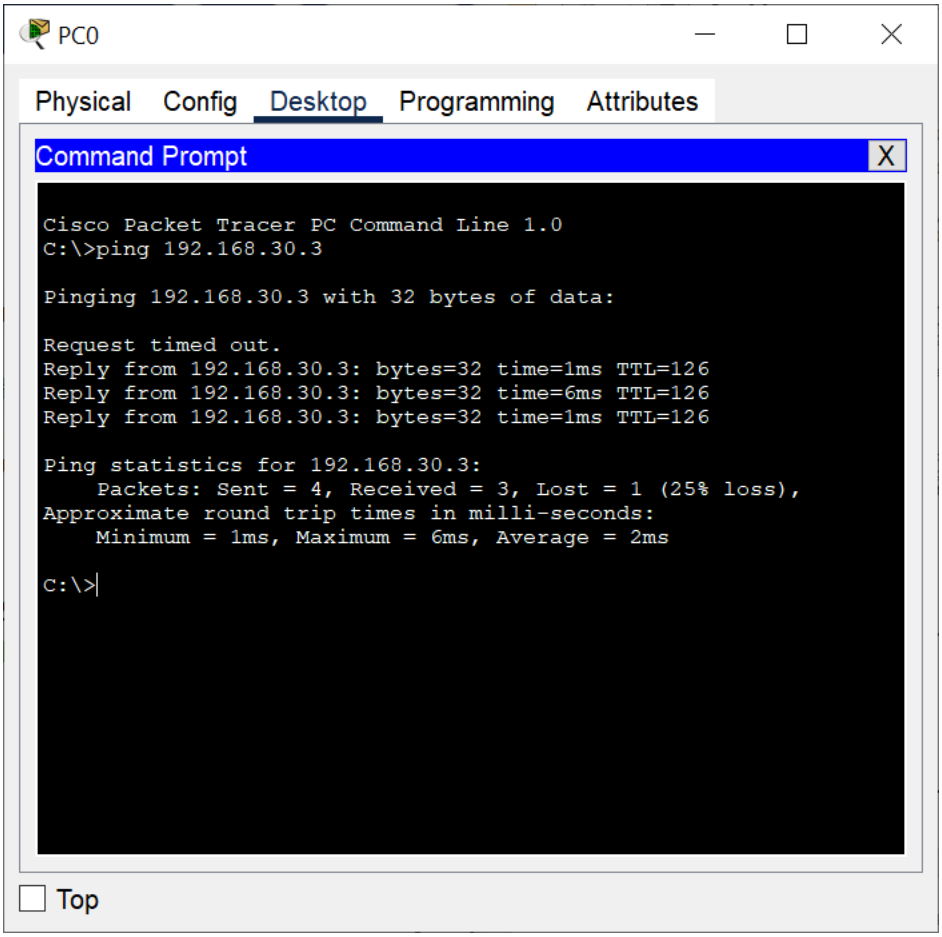
Router 0 : CLI



Router 1: CLI



Checking ping:



RESULT: After the configuration and connection of all devices, the ping is successful from PC-A to PC-B

EXPERIMENT NO – 9

AIM: Basic EIGRP Configuration

OBJECTIVE: To demonstrate Basic EIGRP Configuration and to display EIGRP with a process ID of device.

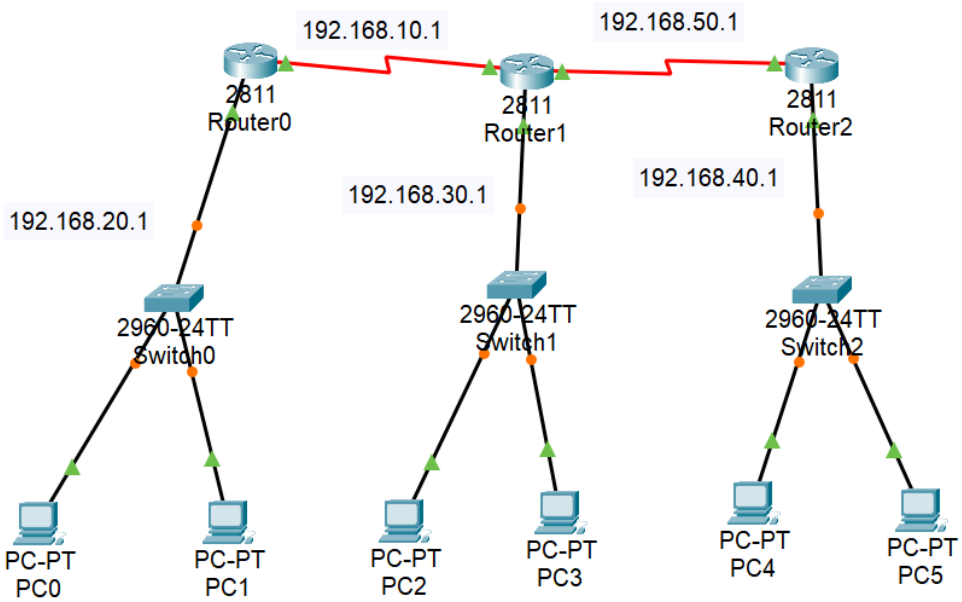
ALGORITHM:

1. Start Cisco Packet tracer application
2. Setup devices and cable them according to the topological diagram
3. Configure fastethernet interface for router 1, 2, and 3
4. Configure serial 0/0/0 interface for router 1 and 3
5. Configure serial 0/1/0 interface for router 2
6. Configure eigrp network for routers.
7. Configure PCs
8. To verify connectivity, ping all PCs through command prompt
9. End

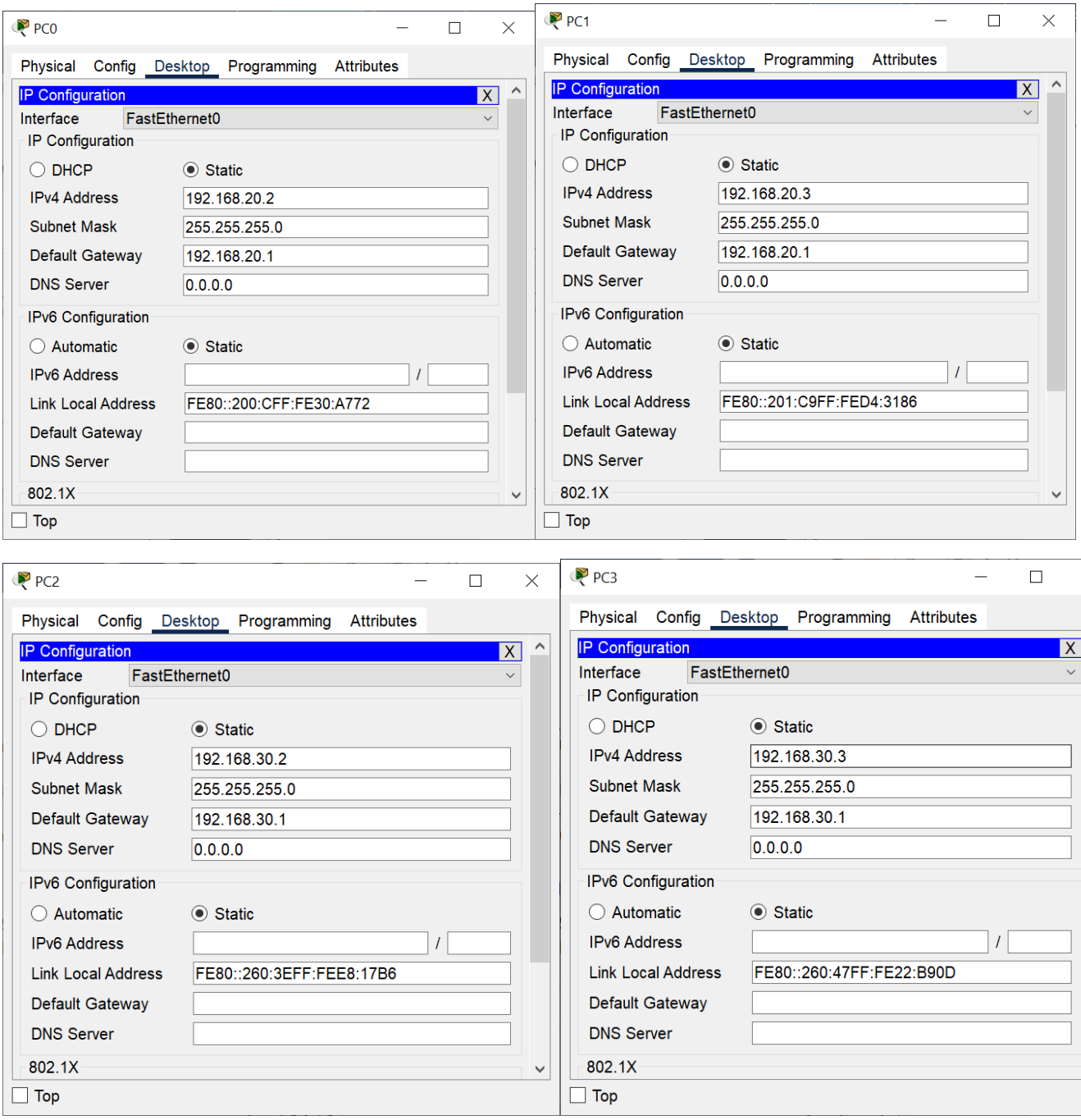
DESCRIPTION AND EXECUTION:

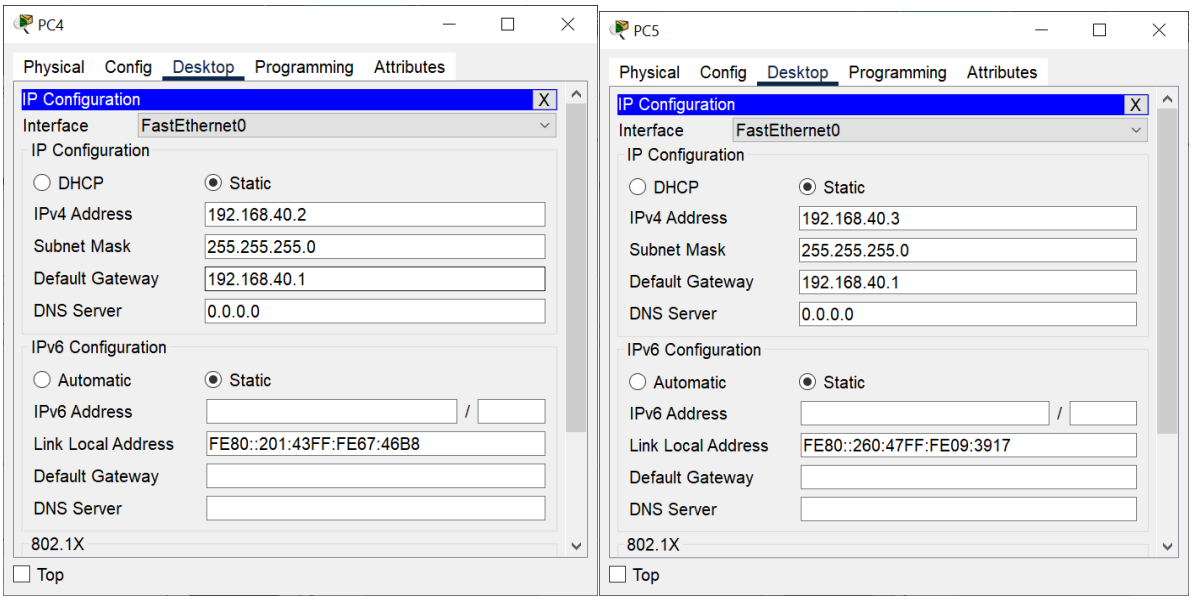
Enhanced Interior Gateway Routing Protocol is an interior gateway protocol suited for many different topologies and media. In a well-designed network, EIGRP scales well and provides extremely quick convergence times with minimal network traffic. It has very low usage of network resources during normal operations; only hello packets are transmitted on a stable network. When a change occurs, only routing table changes are propagated, not the entire routing table; this reduces the load on the routing protocol itself places on the network. It has rapid convergence times for changes in the network topology (in some situations convergence can be almost instantaneous). It is an enhanced distance vector protocol, relying on the Diffused Update Algorithm (DUAL) to calculate the shortest path to a destination within a network.

Setup topological Network:



Configuring PCs:

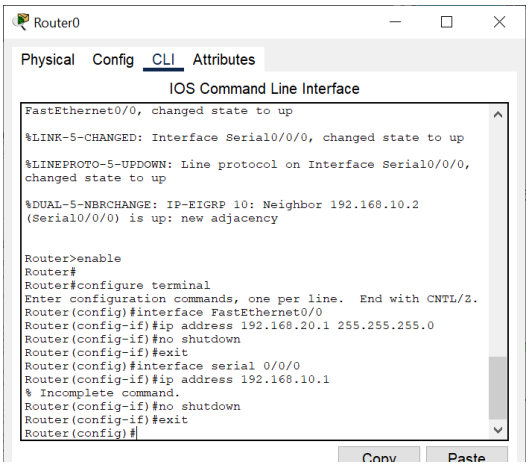




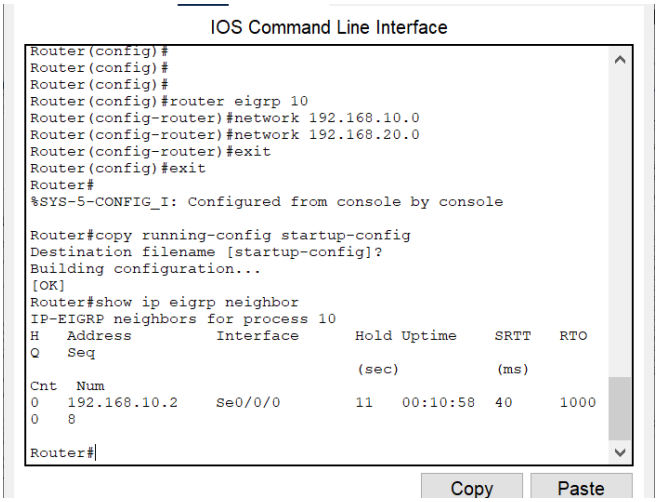
Configuring Routers:

Router 0:

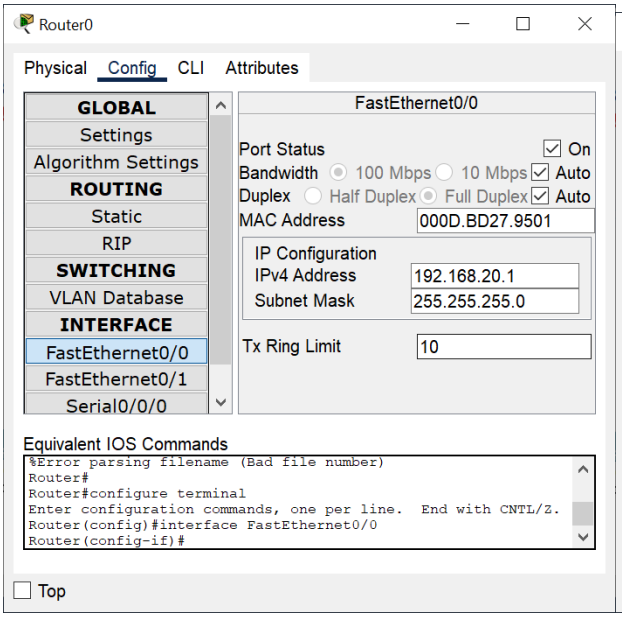
CLI:

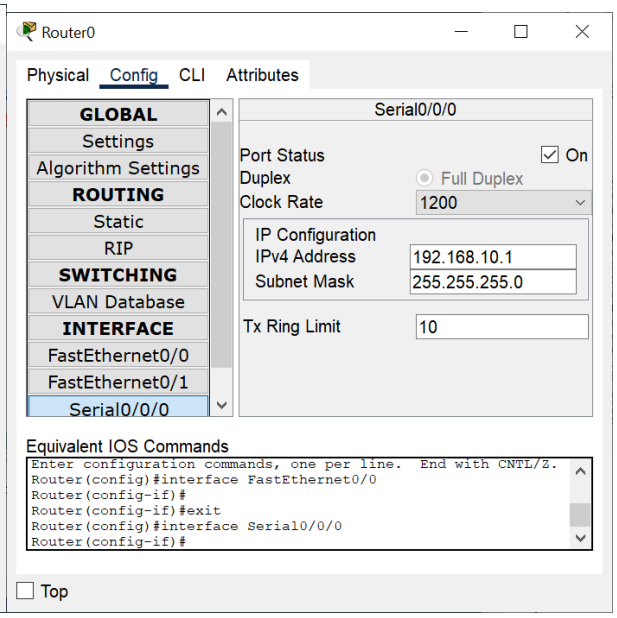


EIGRP:

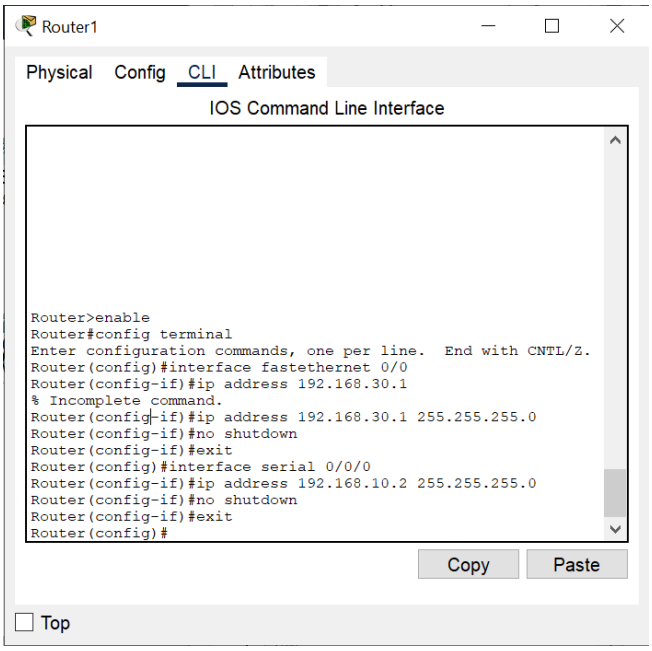


Config:

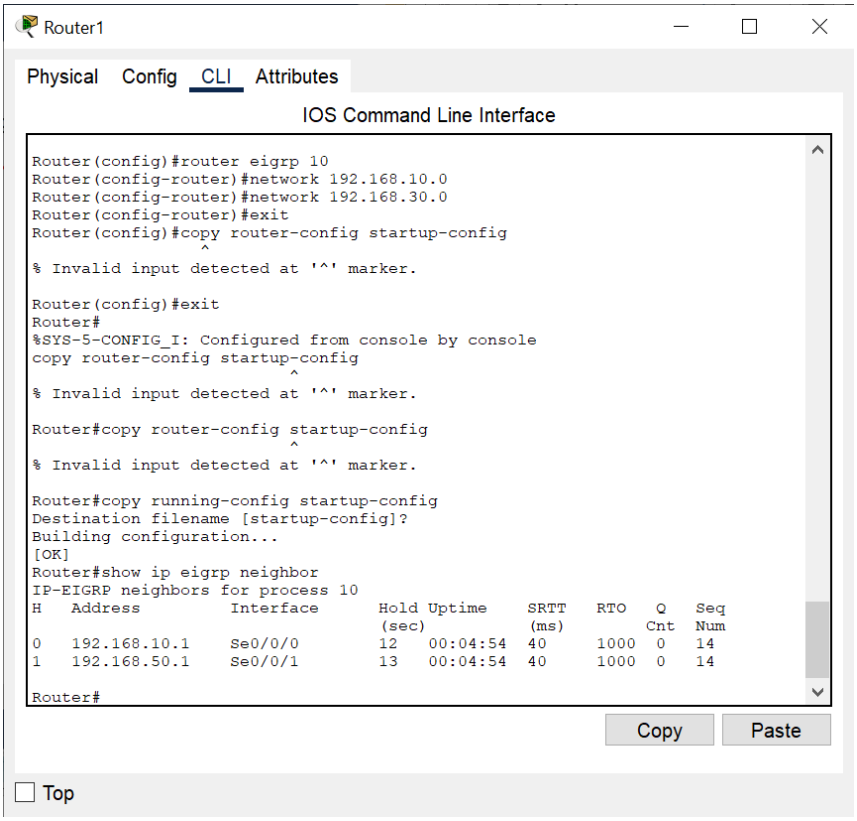




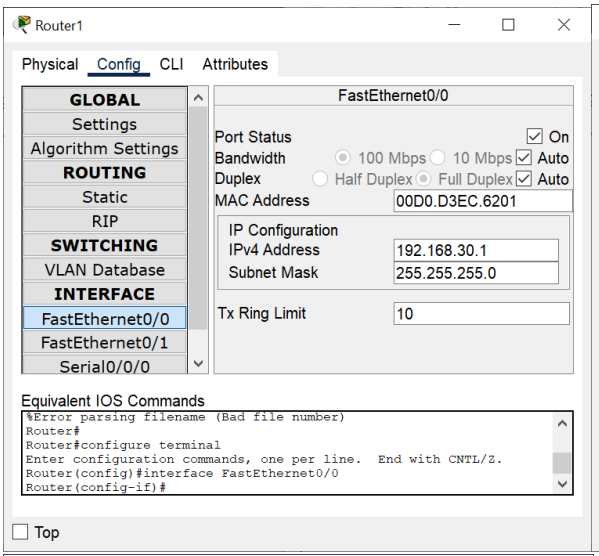
Router 1:

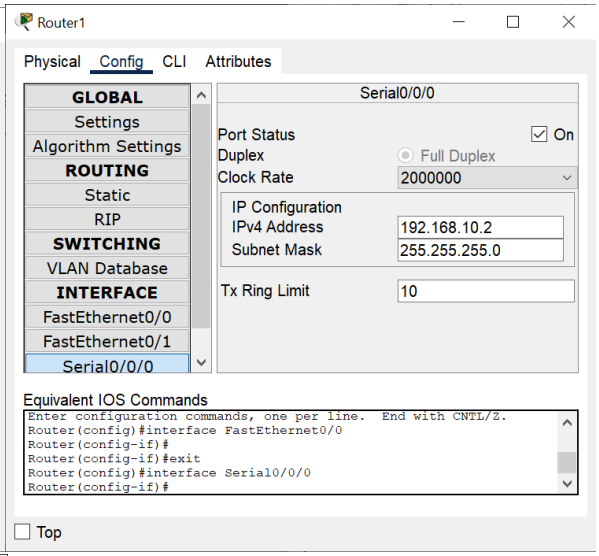


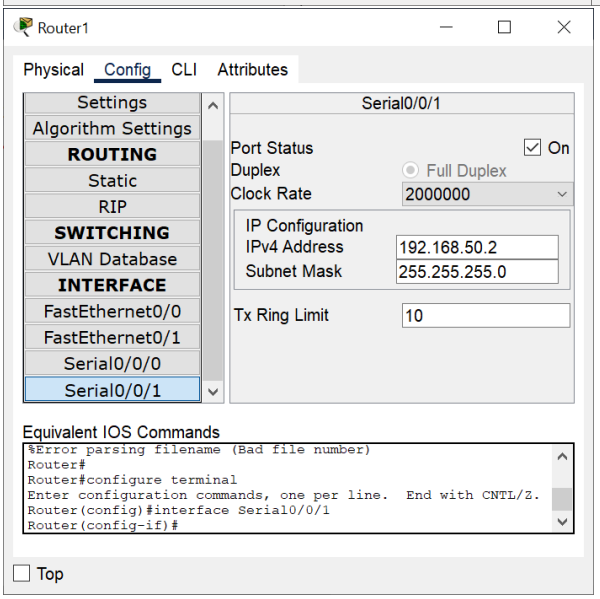
EIGRP:



Config:

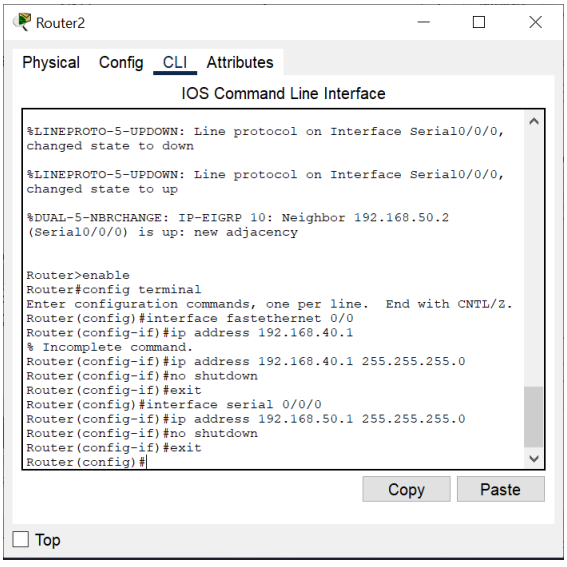

Router1
Physical Config CLI Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Serial0/0/0
FastEthernet0/0
Port Status On
Bandwidth 100 Mbps 10 Mbps Auto
Duplex Half Duplex Full Duplex Auto
MAC Address 00D0.D3EC.6201
IP Configuration
IPv4 Address 192.168.30.1
Subnet Mask 255.255.255.0
Tx Ring Limit 10
Equivalent IOS Commands
%Error parsing filename (Bad file number)
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface FastEthernet0/0
Router(config-if)#
Top


Router1
Physical Config CLI Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Serial0/0/0
Serial0/0/0
Port Status On
Duplex Full Duplex
Clock Rate 2000000
IP Configuration
IPv4 Address 192.168.10.2
Subnet Mask 255.255.255.0
Tx Ring Limit 10
Equivalent IOS Commands
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface FastEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial0/0/0
Router(config-if)#
Top

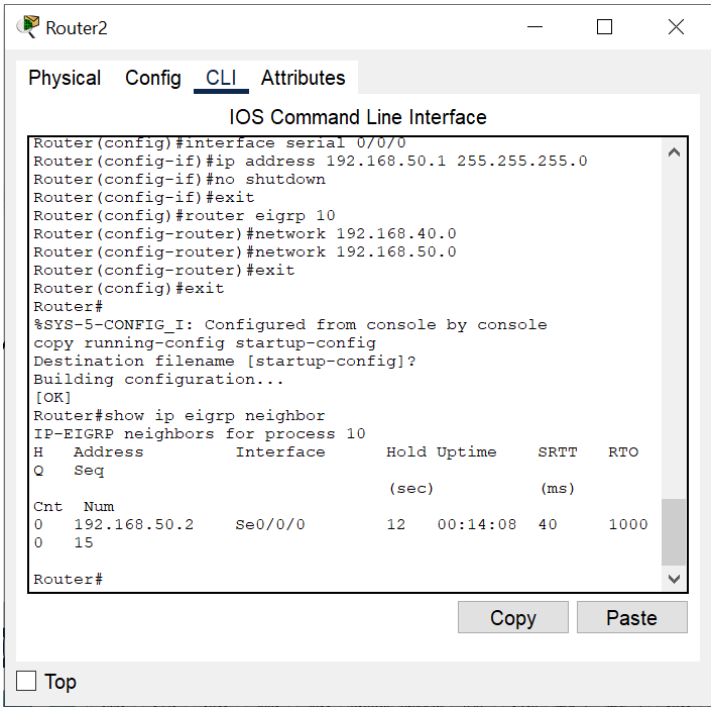

Router1
Physical Config CLI Attributes
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Serial0/0/0
Serial0/0/1
Serial0/0/1
Port Status On
Duplex Full Duplex
Clock Rate 2000000
IP Configuration
IPv4 Address 192.168.50.2
Subnet Mask 255.255.255.0
Tx Ring Limit 10
Equivalent IOS Commands
%Error parsing filename (Bad file number)
Router#
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface Serial0/0/1
Router(config-if)#
Top

Router 2:

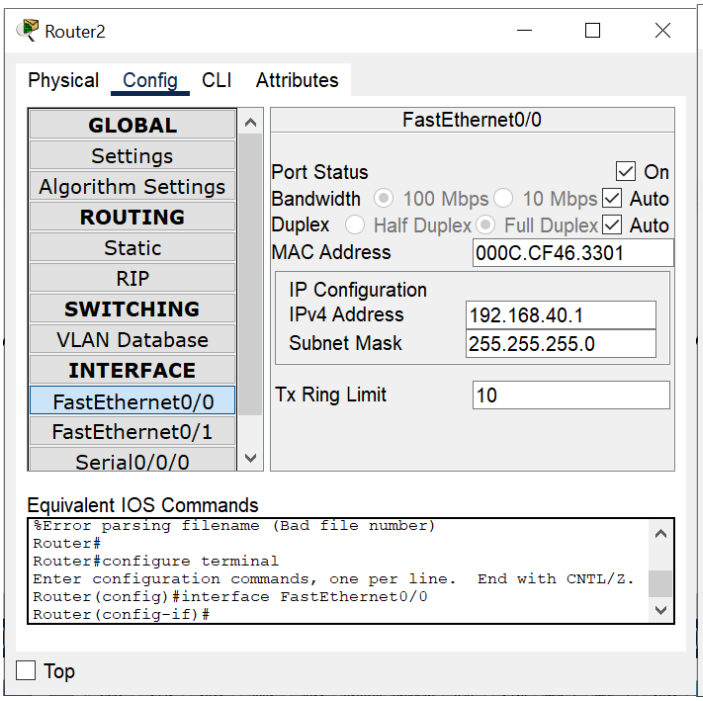
CLI:

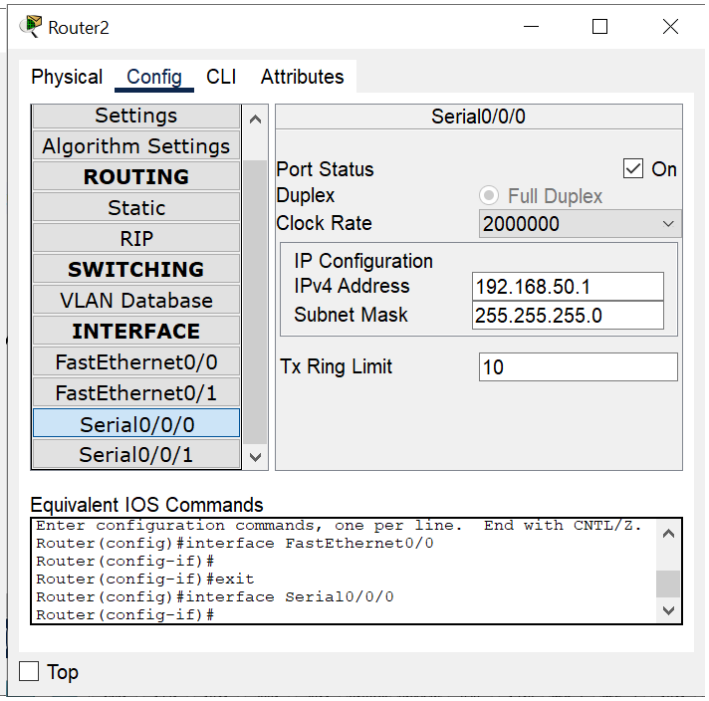

Router2
Physical Config CLI Attributes
IOS Command Line Interface
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
%DUAL-5-NBRCHANGE: IP-EIGRP 10: Neighbor 192.168.50.2 (Serial0/0/0) is up: new adjacency
Router>enable
Router#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface fastethernet 0/0
Router(config-if)#ip address 192.168.40.1
% Incomplete command.
Router(config-if)#ip address 192.168.40.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface serial 0/0/0
Router(config-if)#ip address 192.168.50.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#
Copy
Paste
Top

EIGRP:



Config:





Verification:

Router1

Physical Config CLI Attributes

IOS Command Line Interface

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface Serial0/0/1
Router(config-if)#
?Bad filename
%Error parsing filename (Bad file number)
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#
Router#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.10.0/24 is directly connected, Serial0/0/0
L       192.168.10.2/32 is directly connected, Serial0/0/0
D    192.168.20.0/24 [90/2172416] via 192.168.10.1, 00:16:14, Serial0/0/0
     192.168.30.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.30.0/24 is directly connected, FastEthernet0/0
L       192.168.30.1/32 is directly connected, FastEthernet0/0
D    192.168.40.0/24 [90/2172416] via 192.168.50.1, 00:16:14, Serial0/0/1
     192.168.50.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.50.0/24 is directly connected, Serial0/0/1
L       192.168.50.2/32 is directly connected, Serial0/0/1
```

Copy Paste

Top

Router1

Physical Config CLI Attributes

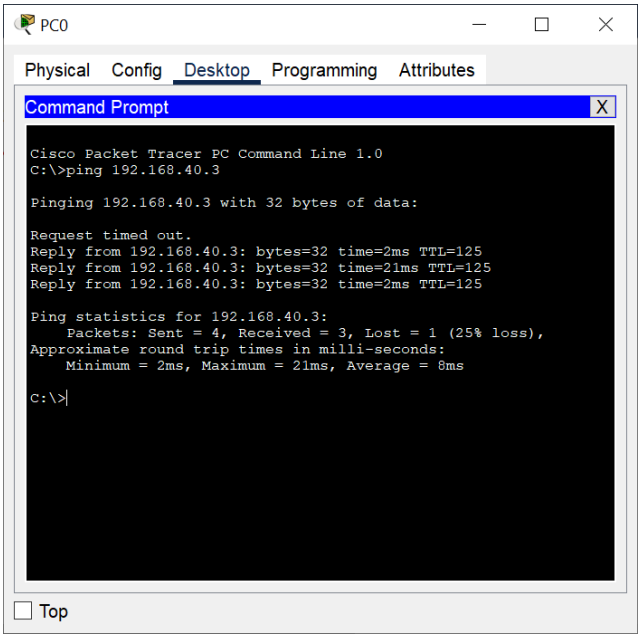
IOS Command Line Interface

```
Router#show ip eigrp neighbor
IP-EIGRP neighbors for process 10
H   Address         Interface       Hold Uptime    SRTT   RTO   Q   Seq
                                    (sec)          (ms)       Cnt  Num
0   192.168.10.1    Se0/0/0         10   00:17:37  40     1000  0   14
1   192.168.50.1    Se0/0/1         11   00:17:37  40     1000  0   14

Router#show ip protocol

Routing Protocol is "eigrp  10 "
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  Redistributing: eigrp 10
  EIGRP-IPv4 Protocol for AS(10)
    Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
    NSF-aware route hold timer is 240
    Router-ID: 192.168.10.2
    Topology : 0 (base)
      Active Timer: 3 min
      Distance: internal 90 external 170
      Maximum path: 4
      Maximum hopcount 100
      Maximum metric variance 1

  Automatic Summarization: disabled
  Automatic address summarization:
  Maximum path: 4
  Routing for Networks:
     192.168.10.0
     192.168.50.0
     192.168.30.0
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.10.1    90            2614037
    192.168.50.1    90            2614058
  Distance: internal 90 external 170
```

Copy Paste

Top

Checking ping:



RESULT: Basic EIGRP Configuration is demonstrated

EXPERIMENT NO – 10

AIM: Analysis of network traces using Tcpdump

OBJECTIVE: To demonstrate Analysis of network traces using Tcpdump

ALGORITHM:

1. Start
2. Open command prompt and run with administrator rights
3. Run windump to locate your network adapter using the command windump -D
4. Run windump to collect packets and write to a file and also run all windump commands.
5. End

DESCRIPTION AND EXECUTION:

Windump prints out a description of the contents of packets on a network interface that match the Boolean expression. It can also be run with the **-w** flag, which causes it to save the packet data to a file for later analysis, and/or with the **-r** flag, which causes it to read from a saved packet file rather than to read packets from a network interface. In all cases, only packets that match expression will be processed bywindump

Windump -D: displays the list of interfaces which are connected to the system. We can use any of the interfaces by specifying its number.

```
Microsoft Windows [Version 10.0.22621.900]
(c) Microsoft Corporation. All rights reserved.

C:\Users\91630>cd /

C:\>cd windump

C:\windump>WinDump.exe
WinDump.exe: listening on \Device\NPF_{CC1D0578-AE27-4F5C-AA29-ED0E582D7439}

0 packets captured
0 packets received by filter
0 packets dropped by kernel

C:\windump>
C:\windump>WinDump.exe -D
1.\Device\NPF_{CC1D0578-AE27-4F5C-AA29-ED0E582D7439} (Microsoft)
2.\Device\NPF_{1D9BA117-6B9D-4FB3-95A2-FFECABFB81DE} (VMware Virtual Ethernet Adapter)
3.\Device\NPF_{20D7F6BB-A568-405A-8F06-3871352FDF4C} (Microsoft)
4.\Device\NPF_{73F64EB4-370F-4FF3-B0D7-B20AA1AB2BB1} (VMware Virtual Ethernet Adapter)
5.\Device\NPF_{F672B3A6-A36C-44ED-80BE-05F0765775C5} (Realtek PCIe GbE Family Controller)
6.\Device\NPF_{A4210DC4-4F56-4DFA-9C03-4AF3306C120C} (Microsoft)

C:\windump>
```

Windump -i 2: By giving this command we will get the list of packets captured from the interface 2.

```
C:\windump>WinDump.exe -i 2
WinDump.exe: listening on \Device\NPF_{1D9BA117-6B9D-4FB3-95A2-FFECABFB81DE}
14:05:11.628328 IP LAPTOP-134K2BDF.64023 > 239.255.255.250.1900: UDP, length 174
14:05:12.637795 IP LAPTOP-134K2BDF.64023 > 239.255.255.250.1900: UDP, length 174
14:05:12.638114 IP6 LAPTOP-134K2BDF.52230 > ff02::1:3.5355: UDP, length 46
14:05:12.638212 IP LAPTOP-134K2BDF.137 > 239.255.255.250.137: UDP, length 50
14:05:12.638379 IP LAPTOP-134K2BDF.52230 > 224.0.0.252.5355: UDP, length 46
14:05:13.650998 IP LAPTOP-134K2BDF.64023 > 239.255.255.250.1900: UDP, length 174
14:05:14.138600 IP LAPTOP-134K2BDF.137 > 239.255.255.250.137: UDP, length 50
14:05:14.661626 IP LAPTOP-134K2BDF.64023 > 239.255.255.250.1900: UDP, length 174
14:05:15.650396 IP LAPTOP-134K2BDF.137 > 239.255.255.250.137: UDP, length 50
14:05:18.577370 IP6 LAPTOP-134K2BDF.52092 > ff02::1:3.5355: UDP, length 90
14:05:18.577591 IP LAPTOP-134K2BDF.52092 > 224.0.0.252.5355: UDP, length 90
14:05:19.424431 IP6 LAPTOP-134K2BDF.61727 > ff02::1:3.5355: UDP, length 42
14:05:19.424526 IP LAPTOP-134K2BDF.137 > 224.0.0.252.137: UDP, length 50
14:05:19.424659 IP LAPTOP-134K2BDF.61727 > 224.0.0.252.5355: UDP, length 42
14:05:20.926470 IP LAPTOP-134K2BDF.137 > 224.0.0.252.137: UDP, length 50
14:05:22.429554 IP LAPTOP-134K2BDF.137 > 224.0.0.252.137: UDP, length 50

16 packets captured
16 packets received by filter
0 packets dropped by kernel
```

Windump -i 2 -c5: By giving this command we will get the list of filters captured from the interface 2 but only limited to 5 filters since, we mentioned count as 5 (-c5).

```
C:\>cd windump

C:\windump>windump -i 2 -c5
windump: listening on \Device\NPF_{1D9BA117-6B9D-4FB3-95A2-FFECABFB81DE}
14:07:21.207978 IP LAPTOP-134K2BDF.5353 > 224.0.0.251.5353:  0 PTR (Cache flush)? _microsoft_mcc._tcp.local. (43
)
14:07:21.208923 IP6 LAPTOP-134K2BDF.5353 > ff02::fb.5353:  0[|domain]
14:07:22.213831 IP LAPTOP-134K2BDF.5353 > 224.0.0.251.5353:  0 PTR? _microsoft_mcc._tcp.local. (43)
14:07:22.214798 IP6 LAPTOP-134K2BDF.5353 > ff02::fb.5353:  0[|domain]
14:07:22.401881 IP6 LAPTOP-134K2BDF.64283 > ff02::1:3.5355: UDP, length 42
5 packets captured
13 packets received by filter
0 packets dropped by kernel
```

Windump -I 2 -c5 -w cap.pcap: this filter is used to write in to a file in which the file nameis cap.pcap .but its limited to only 5packets.

```
C:\windump>windump -i 2 -c5 -w cap.pcap
windump: listening on \Device\NPF_{1D9BA117-6B9D-4FB3-95A2-FFECABFB81DE}

3 packets captured
4 packets received by filter
0 packets dropped by kernel
```

Windump -I 2 -r cap.pcap: this filter is used to read from a file in which the file nameis cap.pcap .but its limited to only 5packets.

```
C:\windump>windump -r cap.pcap
reading from file cap.pcap, link-type EN10MB (Ethernet)
14:09:11.658699 IP LAPTOP-134K2BDF.57779 > 239.255.255.250.1900: UDP, length 174
14:09:12.668695 IP LAPTOP-134K2BDF.57779 > 239.255.255.250.1900: UDP, length 174
14:09:13.673946 IP LAPTOP-134K2BDF.57779 > 239.255.255.250.1900: UDP, length 174
```

Windump -I -nnip: this filter captures the packets and DNS will be converts in to IP address.

```
C:\windump>windump -i 2 -nn ip
windump: listening on \Device\NPF_{1D9BA117-6B9D-4FB3-95A2-FFECABFB81DE}
14:11:11.675607 IP 192.168.40.1.63420 > 239.255.255.250.1900: UDP, length 174
14:11:12.688740 IP 192.168.40.1.63420 > 239.255.255.250.1900: UDP, length 174
14:11:13.693875 IP 192.168.40.1.63420 > 239.255.255.250.1900: UDP, length 174
14:11:14.707758 IP 192.168.40.1.63420 > 239.255.255.250.1900: UDP, length 174
14:11:57.628794 IP 192.168.40.1.137 > 239.255.255.250.137: UDP, length 50
14:11:57.628808 IP 192.168.40.1.53968 > 224.0.0.252.5355: UDP, length 46
14:11:59.135176 IP 192.168.40.1.137 > 239.255.255.250.137: UDP, length 50
14:11:59.743613 IP 192.168.40.1 > 224.0.0.22: igmp v3 report, 1 group record(s)
14:11:59.764884 IP 192.168.40.1 > 224.0.0.22: igmp v3 report, 1 group record(s)
14:11:59.767322 IP 192.168.40.1.5353 > 224.0.0.251.5353:  0 ANY? LAPTOP-134K2BDF.local. (39)
14:11:59.769636 IP 192.168.40.1.5353 > 224.0.0.251.5353:  0*- [0q] 2/0/0 AAAA[|domain]
14:12:00.106281 IP 192.168.40.1 > 224.0.0.22: igmp v3 report, 1 group record(s)
14:12:00.638690 IP 192.168.40.1.137 > 239.255.255.250.137: UDP, length 50
14:12:04.333124 IP 192.168.40.1.64847 > 239.255.255.250.1900: UDP, length 175
14:12:05.341677 IP 192.168.40.1.64847 > 239.255.255.250.1900: UDP, length 175
14:12:06.342497 IP 192.168.40.1.64847 > 239.255.255.250.1900: UDP, length 175
14:12:07.348216 IP 192.168.40.1.64847 > 239.255.255.250.1900: UDP, length 175
```

Windump -I -c5 -nnip: this filter captures only 5 packets and DNS will be converts in to IP address

```
C:\windump>windump -i 2 -c5 -nn ip
windump: listening on \Device\NPF_{1D9BA117-6B9D-4FB3-95A2-FFECABFB81DE}
14:13:25.737141 IP 192.168.40.1.64853 > 239.255.255.250.3702: UDP, length 656
14:13:25.911994 IP 192.168.40.1.64853 > 239.255.255.250.3702: UDP, length 656
14:13:26.241945 IP 192.168.40.1.64853 > 239.255.255.250.3702: UDP, length 656
14:13:26.882077 IP 192.168.40.1.64853 > 239.255.255.250.3702: UDP, length 656
14:13:28.165915 IP 192.168.40.1.64853 > 239.255.255.250.3702: UDP, length 656
5 packets captured
9 packets received by filter
0 packets dropped by kernel
```

Windump -I port 80: this filter captures the packets whose port number is 80.

```
C:\windump>windump -i 2 port 80
windump: listening on \Device\NPF_{1D9BA117-6B9D-4FB3-95A2-FFECABFB81DE}

0 packets captured
8 packets received by filter
0 packets dropped by kernel
```

Windump -I 2 host 172.20.3.159: this filter is used to connect to the specified host and captures the packets from that host.

```
C:\windump>windump -i 2 host 172.20.3.159
windump: listening on \Device\NPF_{1D9BA117-6B9D-4FB3-95A2-FFECABFB81DE}

0 packets captured
4 packets received by filter
0 packets dropped by kernel
```

```
PS C:\Users\91630> ping 172.20.3.159

Pinging 172.20.3.159 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.20.3.159:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PS C:\Users\91630> ping 172.20.3.159
```

Windump -I 2 tcp: this filter captures all tcp packets.

```
C:\windump>windump -i 2 tcp
windump: listening on \Device\NPF_{1D9BA117-6B9D-4FB3-95A2-FFECABFB81DE}

0 packets captured
4 packets received by filter
0 packets dropped by kernel
```

RESULTS: The network packets received and sent are analyzed using the tcpdump utility.

EXPERIMENT NO – 11

AIM: Analysis of network traces using Wireshark

OBJECTIVE: To demonstrate Analysis of network traces using Wireshark

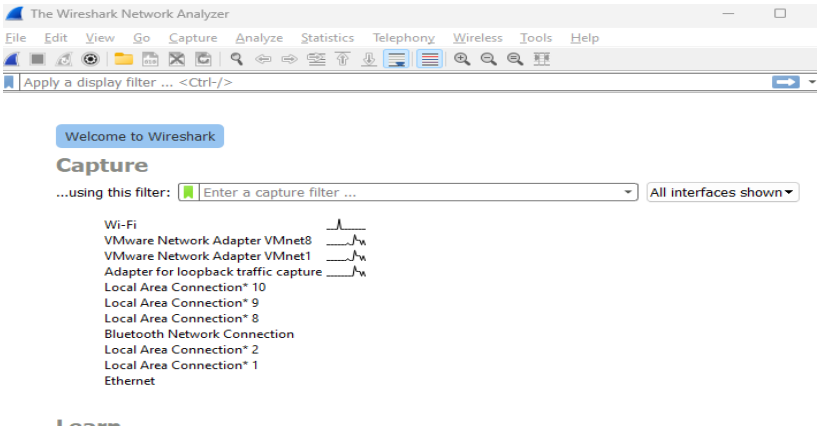
ALGORITHM:

1. Start
2. ip.src == _address'
3. ip.addr == _address'
4. ip.dst == _address'
5. tcp
6. http
7. tcp.port
8. tcp.analysis.flags
9. tcpcontains
10. udpcontains
11. http.response.code
12. End

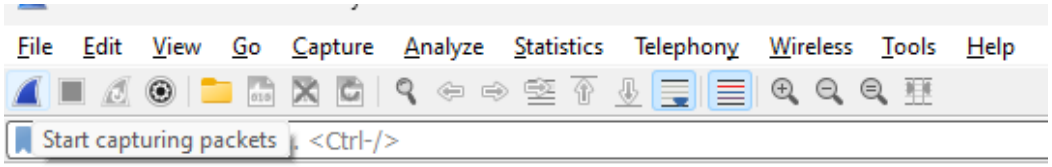
DESCRIPTION AND EXECUTION:

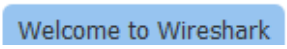
- Several filters such as ip.src, ip.dst are applied to packets on wireshark and the packets are analysed.
- Wireshark is an open-source network protocol analysis software program started by Gerald combs in 1998
- A global organization of network specialists and software developers support Wireshark and continue to make updates for new network technologies and encryption methods.
- Wireshark is a packet sniffer and analysis tool. It captures network traffic on the local network and stores that data for offline analysis
- Wireshark captures network traffic from Ethernet, Bluetooth, Wireless (IEEE 802.11), Token Ring, Frame Relay connections, and more.
- Wireshark allows you to filter the log either before the capture starts or during analysis, so you can narrow down and zero into what you are looking for in the network trace.
- For example, you can set a filter to see TCP traffic between two IP addresses.
- You can set it only to show you the packets sent from one computer. The filters in wireshark are one of the primary reasons it became the standard tool for packet analysis.

➢ When you open Wireshark, you see a screen that shows you a list of all of the network connections you can monitor. You also have a capture filter field, so you only capture the network traffic you want to see



- You can select one or more of the network interfaces using ―shift left-click.‖ Once you have the network interface selected, you can start the capture, and there are several ways todothat.Clickthefirstbuttononthetoolbar,titled―StartCapturingPackets.‖





- Analyzing Data Packets on Wireshark

Wireshark shows you three different panes for inspecting packet data. The Packet List, the top pane, is a list of all the packets in the capture. When you click on a packet, the other two panes change to show you the details about the selected packet. You can also tell if the packet is part of a conversation. Here are some details about each column in the top pane:

▪ No.: This is the number order of the packet that got captured. The bracket indicates that this packet is part of a conversation.

▪ Time: This column shows you how long after you started the capture that this packet got captured. You can change this value in the Settings menu if you need something different displayed.

▪ Source: This is the address of the system that sent the packet.

▪ Destination: This is the address of the destination of that packet.

▪ Protocol: This is the type of packet, for example, TCP, DNS, DHCPv6, or ARP.

▪ Length: This column shows you the length of the packet in bytes.

▪ Info: This column shows you more information about the packet contents, and will vary depending on what kind of packet it is.

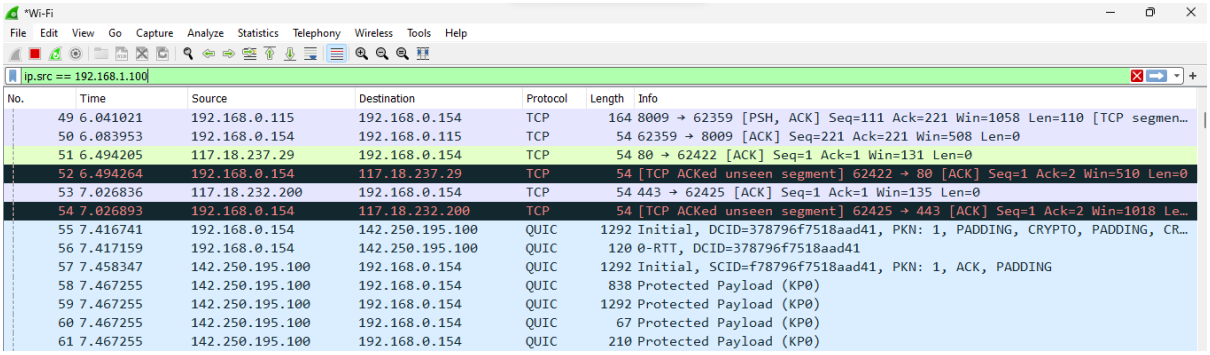
- Wireshark Capture Filters Commands

• Capture filters limit the captured packets by the filter. Meaning if the packets don‘t match the filter, Wireshark won‘t save them. Here are some examples of capture filters:

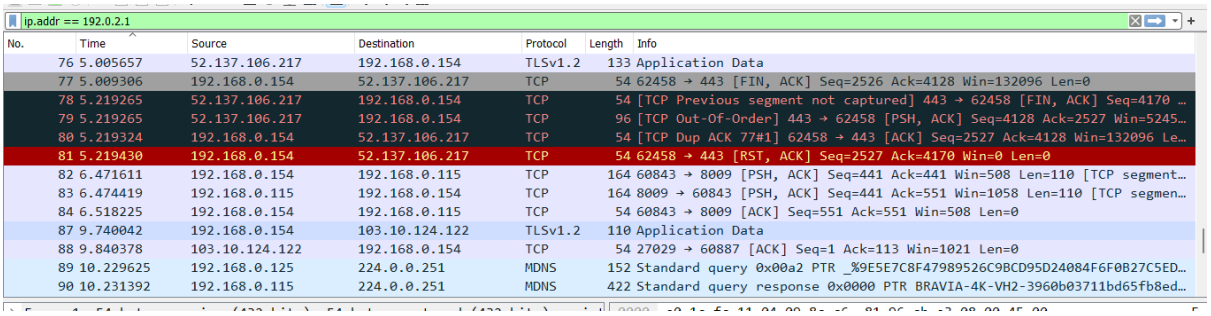
• host IP-address: this filter limits the capture to traffic to and from the IP address net 192.168.0.0/24: this filter captures all traffic on the subnet.

• dst host IP-address: capture packets sent to the specified host. port 53: capture traffic on port 53only.

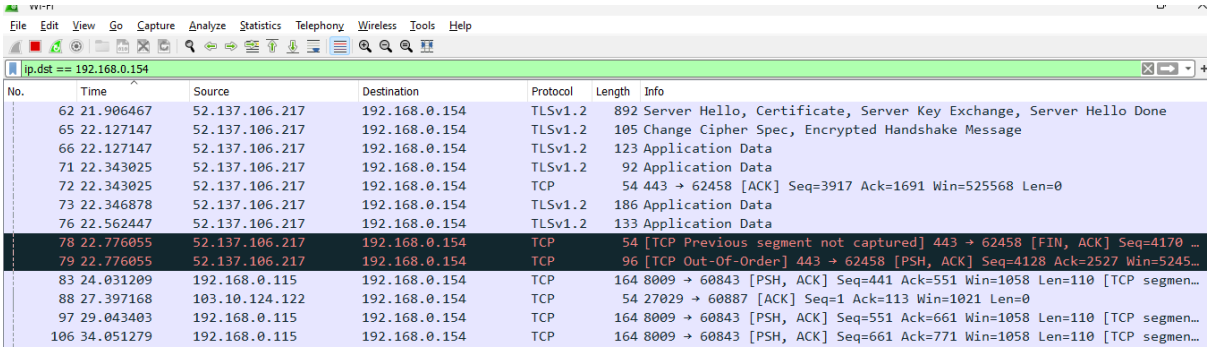
• port not 53 and not arp: capture all traffic except DNS and ARP traffic.



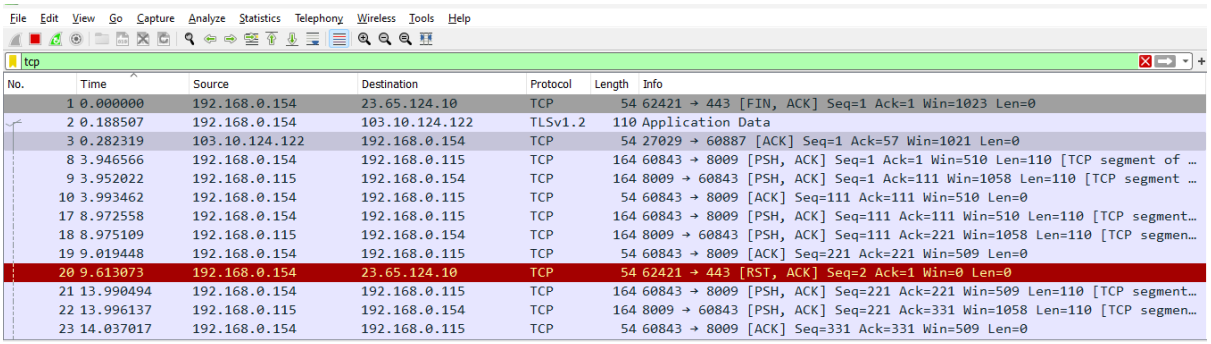
2. ip.addr = =_address‘



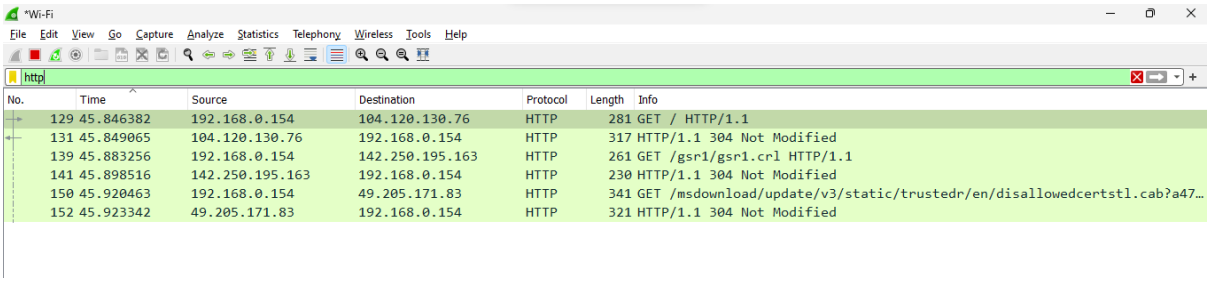
3.ip.dst == _address‘



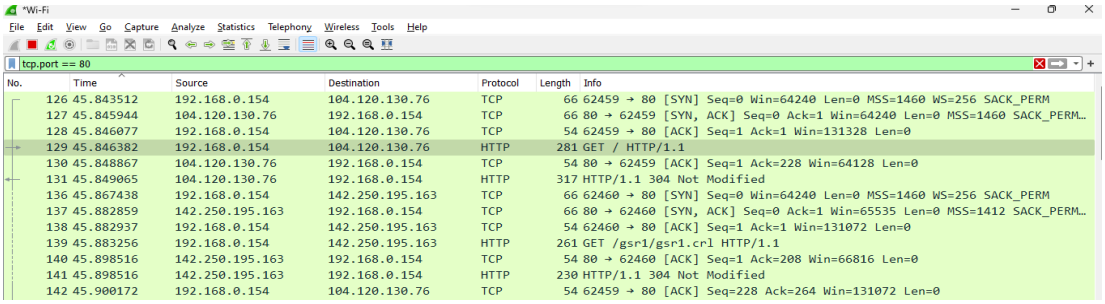
4. tcp



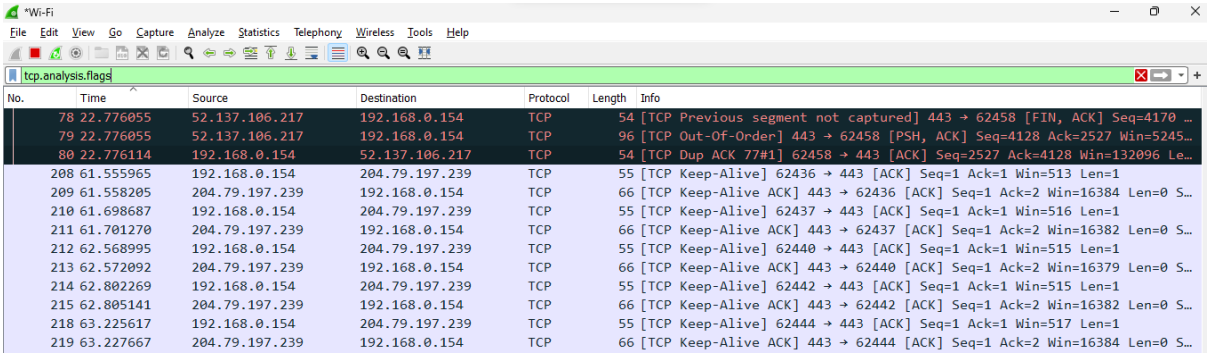
5. http



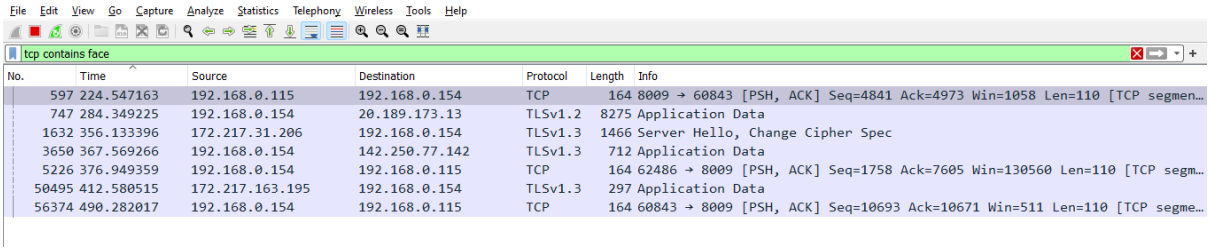
6. tcp.port



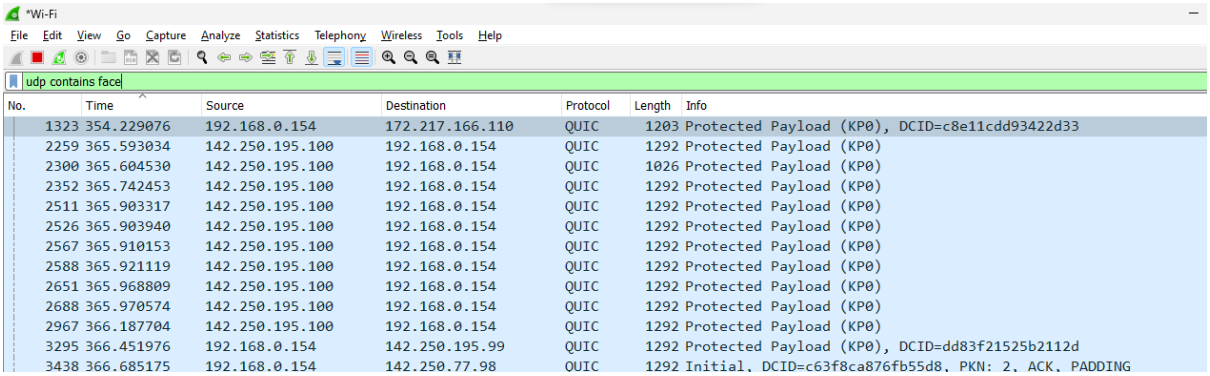
7. tcp.analysis.flags



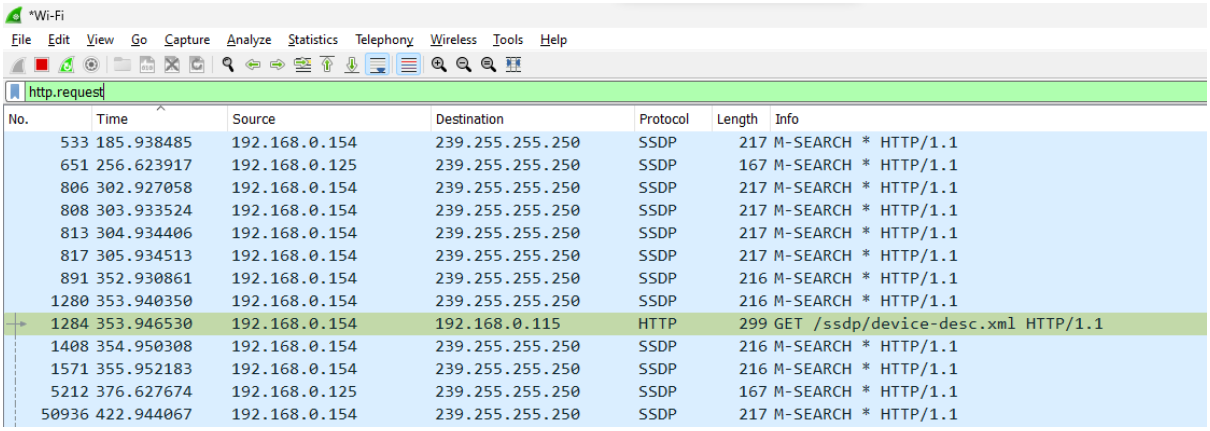
8.tcpcontains



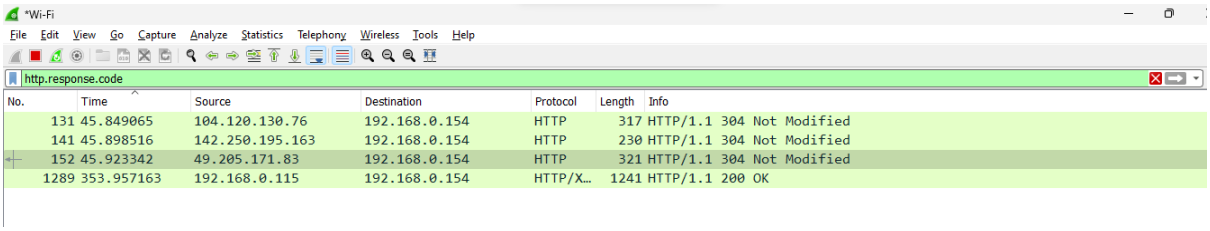
9.udp contains



10. http.request



11. http.response.code



RESULTS: The packets received and sent are analyzed using filters in wireshark.