EXPERIMENT -1

1. Study of Network media, cables, and devices and Cable Construction

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 fiber 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:

- The cost of the shielded twisted pair cable is not very high and not very low.
- An installation of STP is easy.
- It has higher capacity as compared to unshielded twisted pair cable.
- It has a higher attenuation.
- It is shielded that provides the higher data transmission rate.

Disadvantages

- It is more expensive as compared to UTP and coaxial cable.
- It has a higher attenuation rate

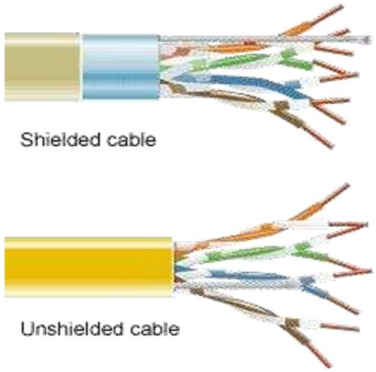
There are 3 types of guided media:

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:

- Least expensive.
- Easy to install
- Short distance transmission due to attenuation



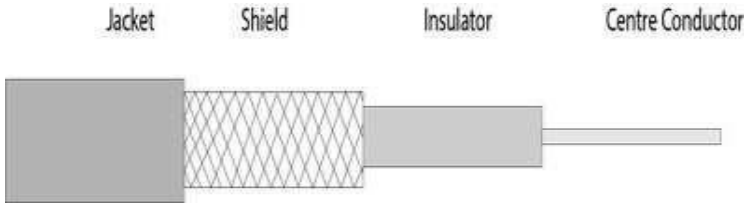
b) Coaxial cable:

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 Band width
2. Better noise immunity
3. Easy to install and expand
4. Inexpensive

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:

- **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 the fibre.

- **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 the fibre.

- **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 fiber protection.

Advantages of Optical Fiber

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

- High band width
- 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

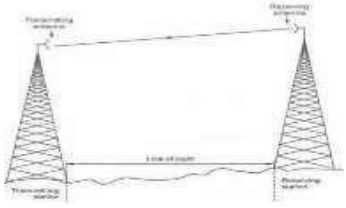
- Radio waves are easy to generate and penetrate buildings also can travel long distances.
- Radio waves cover a large area and can penetrate the buildings. By this, an AM radio can receive signals inside a building.
- This can also be disadvantageous because we cannot isolate a communication just inside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



Microwave Transmission

Two types of Microwave Transmission are as follows,

1. Terrestrial Microwave
2. Satellite Microwave

iii) 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.

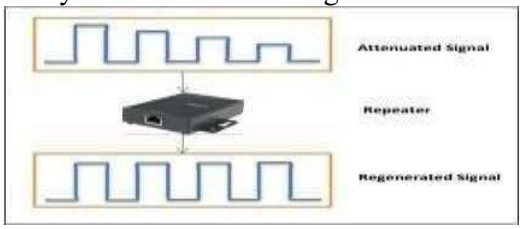
➢ NETWORKDEVICES

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.

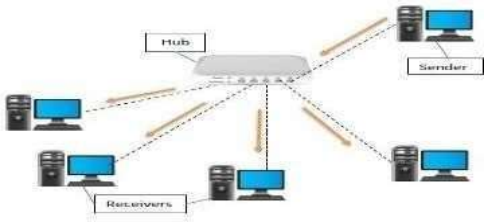


2. HUB

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 to monitor the traffic passing through the hub and to configure each port in the hub.



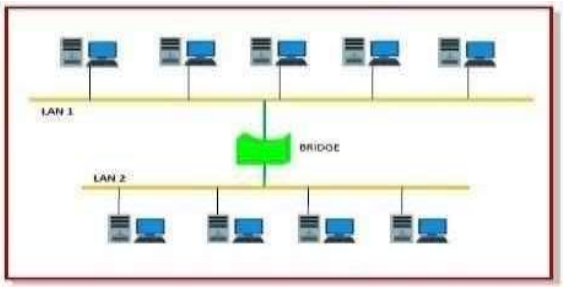
1. BRIDGE

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.



3. 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.

4. THREE LAYERSWITCH

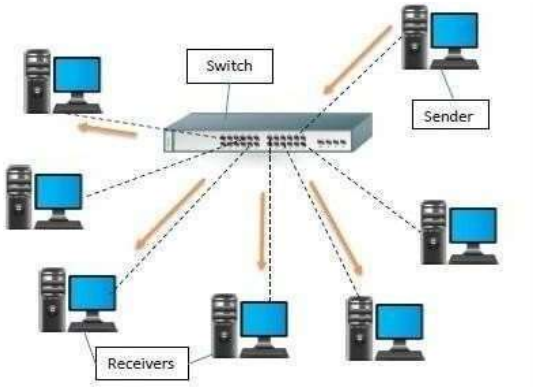
A layer 3 switch combines the functionality of a switch and a router. It acts as a switch to connect devices that are on the same subnet or virtual LAN at lightning speeds and has IP routing intelligence built into it to double up as a router. It can support routing protocols, inspect incoming packets, 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 a 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, lets step back a bit in time to see how these switches evolved.

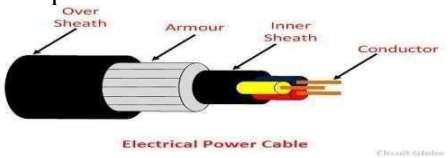
Layer 2 switches work well when there is low to medium traffic in VLANs. But these switches would hang when traffic increased. So, it became necessary to augment layer 2‘s functionality.
One option was to use a router instead of a switch, but then routers are slower than switches, so this could lead to slower performance.



➢ CABLE CONSTRUCTION

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 costlier 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.



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 canter 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 pass through 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 non migratory 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 earthling the cable. When the fault occurs in the cable (due to insulation failure) the fault current flows through the armour 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 -2

2. Demonstration of basic network commands/utilities in Windows.

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

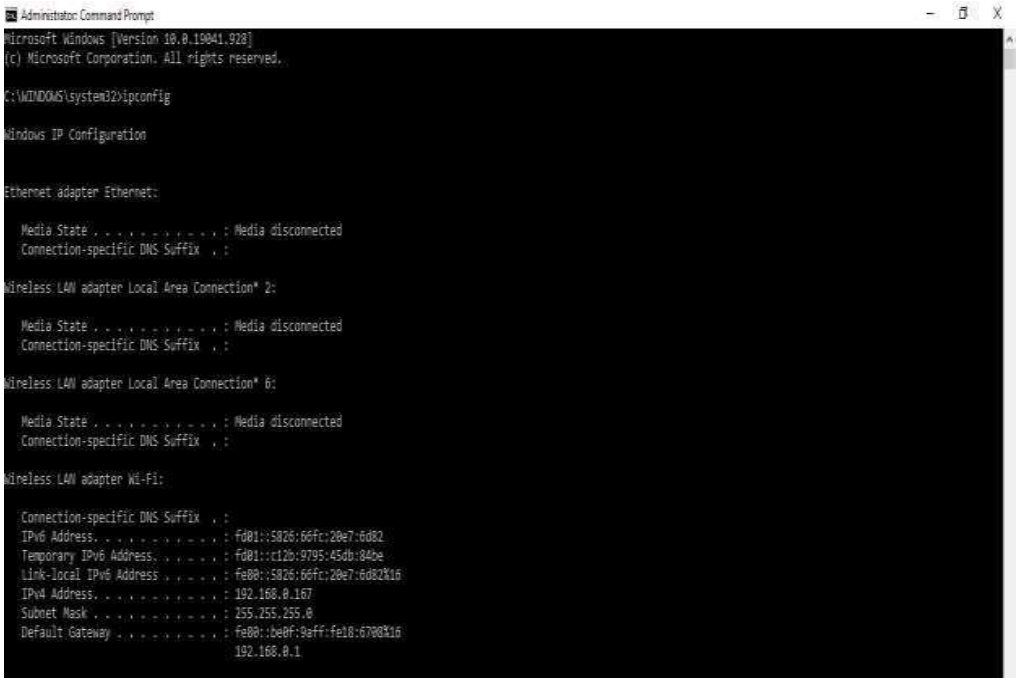
OBJECTIVE: To list commands and execute on the CLI to obtain results such as the IP addressand ping among many other results.

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.



2) Ipconfig/all

all – Displays additional information for all network adapters

```
Windows IP Configuration

   Host Name . . . . . . . . . . . . : Sasank-s-Omen
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : WirelessAP

Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek Gaming GbE Family Controller
   Physical Address. . . . . . . . . : BC-E9-2F-8A-5C-9C
   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. . . . . . . . . : CC-D9-AC-B5-BF-E5
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Local Area Connection* 2:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Microsoft Wi-Fi Direct Virtual Adapter #2
   Physical Address. . . . . . . . . : CE-D9-AC-B5-BF-E4
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::c111:cb5e:a409:cd9e%16(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.137.1(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
   DHCPv6 IAID . . . . . . . . . . . : 248437164
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-26-89-14-91-BC-E9-2F-8A-5C-9C
   DNS Servers . . . . . . . . . . . : fec0:0:0:ffff::1%1
                                       fec0:0:0:ffff::2%1
                                       fec0:0:0:ffff::3%1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : WirelessAP
   Description . . . . . . . . . . . : Intel(R) Wi-Fi 6 AX201 160MHz
   Physical Address. . . . . . . . . : CC-D9-AC-B5-BF-E4
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::d507:5f03:ac24:52ca%12(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.100(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : 26 April 2021 13:26:40
   Lease Expires . . . . . . . . . . : 27 April 2021 19:47:18
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 147642796
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-26-89-14-91-BC-E9-2F-8A-5C-9C
   DNS Servers . . . . . . . . . . . : 49.205.171.194
                                       49.207.34.210
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

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 are 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.

```
C:\WINDOWS\system32>ping www.google.com

Pinging www.google.com [142.250.67.132] with 32 bytes of data:
Reply from 142.250.67.132: bytes=32 time=22ms TTL=117
Reply from 142.250.67.132: bytes=32 time=20ms TTL=117
Reply from 142.250.67.132: bytes=32 time=23ms TTL=117
Request timed out.

Ping statistics for 142.250.67.132:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 20ms, Maximum = 23ms, Average = 21ms
```

4) Tracert

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

```
C:\WINDOWS\system32>tracert www.google.com

Tracing route to www.google.com [142.250.67.132]
over a maximum of 30 hops:

  1     3 ms     2 ms     4 ms  dlinkrouter [192.168.0.1]
  2     2 ms     4 ms     2 ms  10.10.13.1
```

4.1 Tracert

```
C:\WINDOWS\system32>tracert -h 10 www.cbit.ac.in

Tracing route to cbit.ac.in [192.46.212.171]
over a maximum of 10 hops:

  1     2 ms     2 ms     4 ms  dlinkrouter [192.168.0.1]
  2     2 ms     4 ms     2 ms  10.10.13.1
  3     *        6 ms     *     28.69.103-217.in-addr.arpa [103.69.28.217]
  4     *        *        *     Request timed out.
  5     5 ms     5 ms     9 ms  137.59.200.16
  6     7 ms     7 ms     3 ms  14.142.71.253.static-hydrabad.vsnl.net.in [14.142.71.253]
  7    21 ms    19 ms    20 ms  172.25.81.134
  8    94 ms    99 ms   101 ms  172.28.132.237
  9    25 ms    24 ms    33 ms  100.76.112.62
 10    96 ms   101 ms    24 ms  10.214.32.0

Trace complete.
```

5) nslookup:

The nslookup (Name Server Lookup) tool can show valuable details to troubleshoot and resolve DNS-related 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.

```
C:\WINDOWS\system32>nslookup www.hackerrank.com
Server:  UnKnown
Address:  fe80::be0f:9aff:fe18:6708

Non-authoritative answer:
Name:    e8937.dscb.akamaiedge.net
Addresses:  2600:1417:75:cb6::22e9
          2600:1417:75:cab::22e9
          104.122.8.79
Aliases:  www.hackerrank.com
          hackerrank.com.edgekey.net
```

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 Windows10 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.

```
C:\WINDOWS\system32>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:49675        DESKTOP-8FEF7AJ:49676  ESTABLISHED
  TCP    127.0.0.1:49676        DESKTOP-8FEF7AJ:49675  ESTABLISHED
  TCP    192.168.0.167:52086    a23-50-254-60:https    CLOSE_WAIT
  TCP    192.168.0.167:52087    a23-50-254-60:https    CLOSE_WAIT
  TCP    192.168.0.167:52396    40.90.189.152:https    ESTABLISHED
  TCP    192.168.0.167:52988    a-0001:https           ESTABLISHED
  TCP    192.168.0.167:52990    52.113.196.254:https   ESTABLISHED
  TCP    192.168.0.167:52991    13.107.42.254: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'

```
C:\WINDOWS\system32>arp -a

Interface: 192.168.0.167 --- 0x10
  Internet Address      Physical Address      Type
  192.168.0.1           bc-0f-9a-18-67-08     dynamic
  192.168.0.147         1c-d6-be-77-6c-20     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
```

7) 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 anetwork and its settings such as network shares, users and print jobs, as just a few examples.

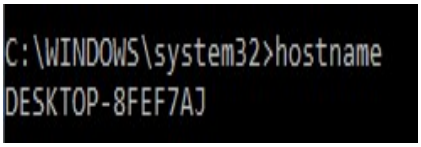
Running just net won‘t do much, but it will present you with a list of all the switches that are available.

These include accounts to set password and logon requirements, file to show a list of open files andsessions to list, or even disconnect, sessions on the network.

```
C:\WINDOWS\system32>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 ]
```

8) hostname

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



RESULTS:

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

EXPERIMENT / PRACTICAL -3

3. PC Network Configuration.

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 mainfunctions: 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) Class A:

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 (2^7-2) and 16777214 hosts (2^{24}-2).

2) Class B:

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 (2^{14}) Network addresses and 65534 (2^{16}-2) Host addresses.

3) Class C:

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 is255.255.255.x.

Class C gives 2097152 (2^{21}) Network addresses and 254 (2^{8}-2) Host

addresses.

Class D:

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

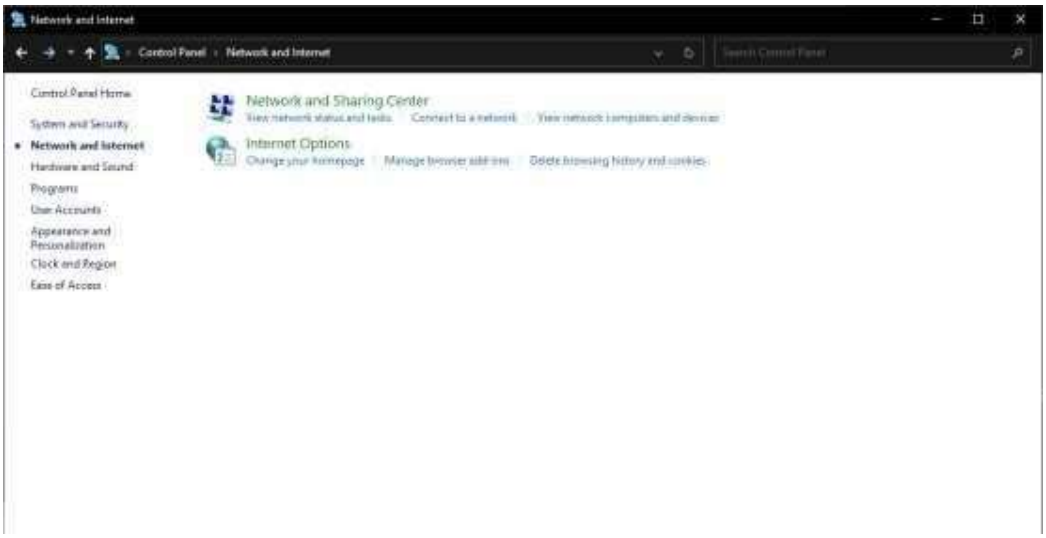
Class D has IP address range from 224.0.0.0 to 239.255.255.255. Class D is reserved for Multicasting. In multicasting data is not destined for a particular host, that is why there is no need to extract host address from the IP address, and Class D does not have any subnet mask.

4) Class E:

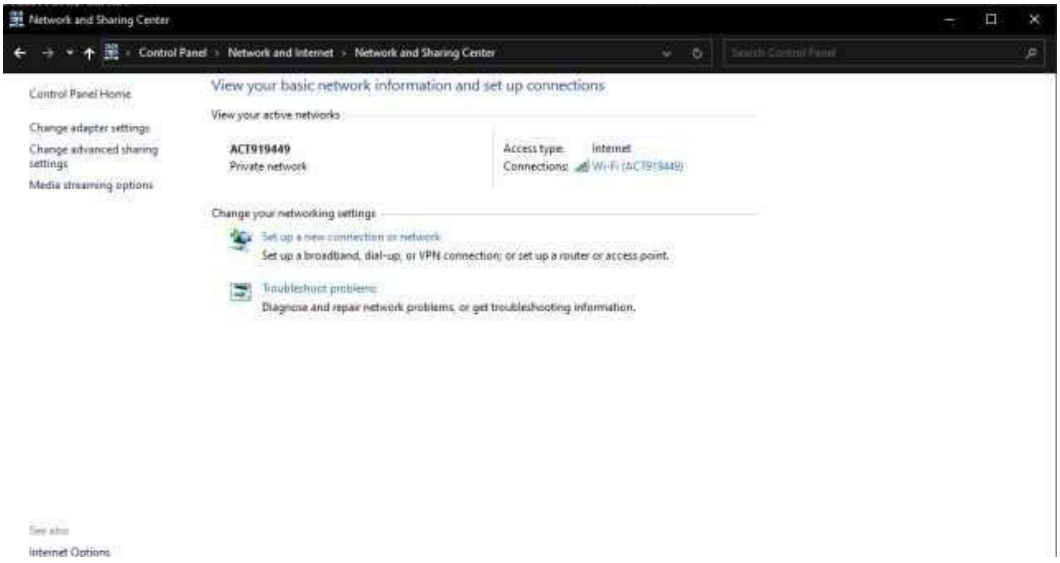
This IP Class is reserved for experimental purposes only for R&D or Study. IP addresses in this class ranges from 240.0.0.0 to 255.255.255.254. Like Class D, this class too is not equipped with any subnet mask.

DESCRIPTION AND EXECUTION:

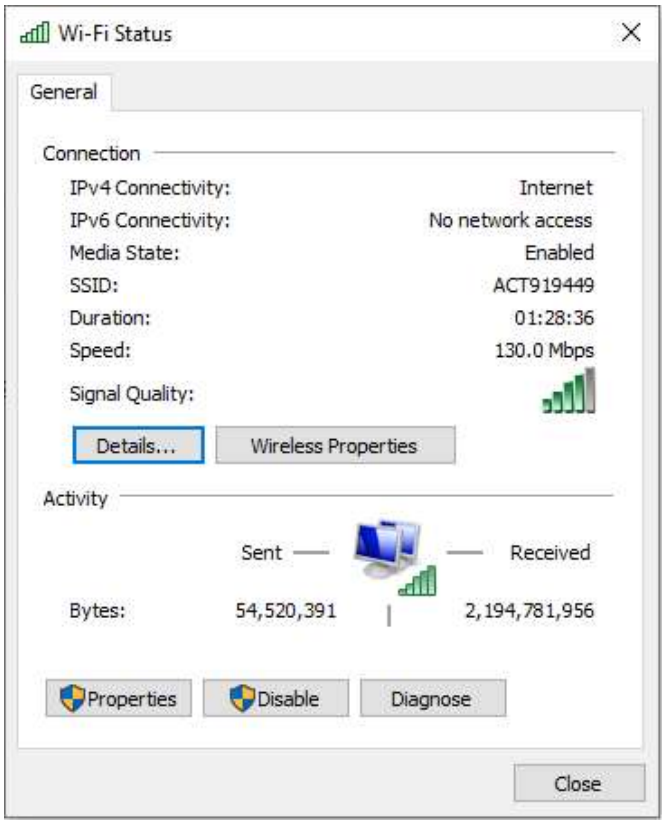
Network Configuration: Open Control Panel: Open Network and Internet:



Open Network and Sharing Center:

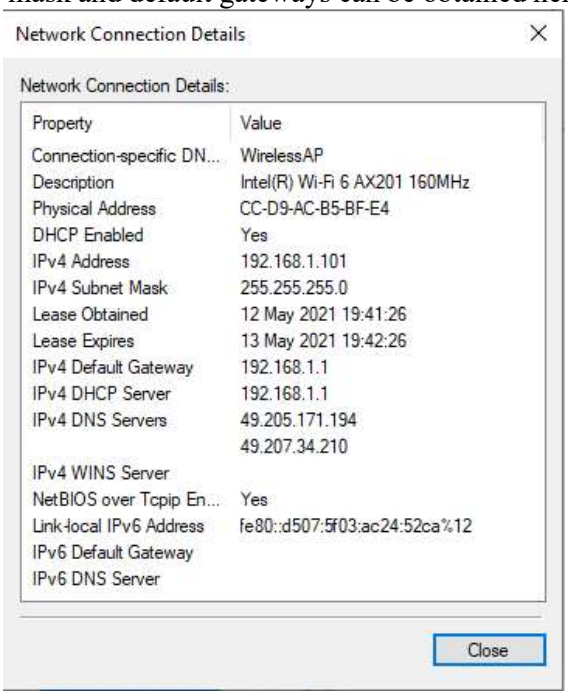


Go to Connection (Wi-Fi or LAN)

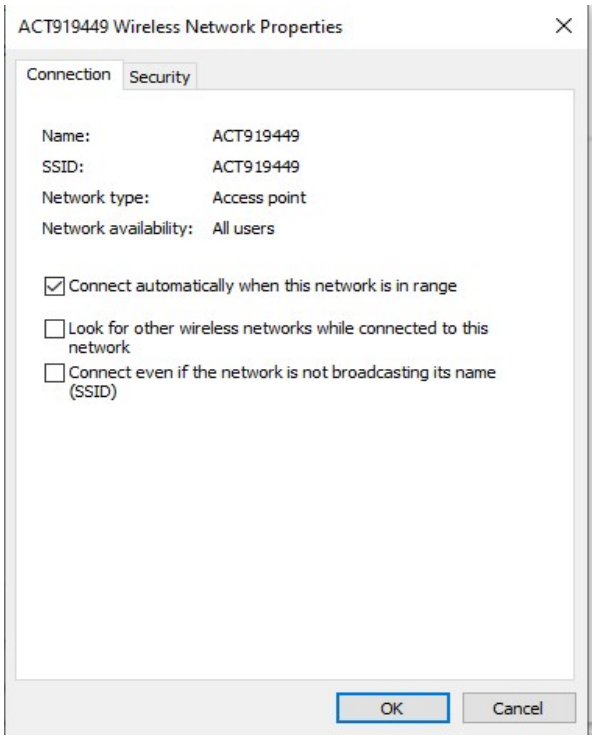


Details:

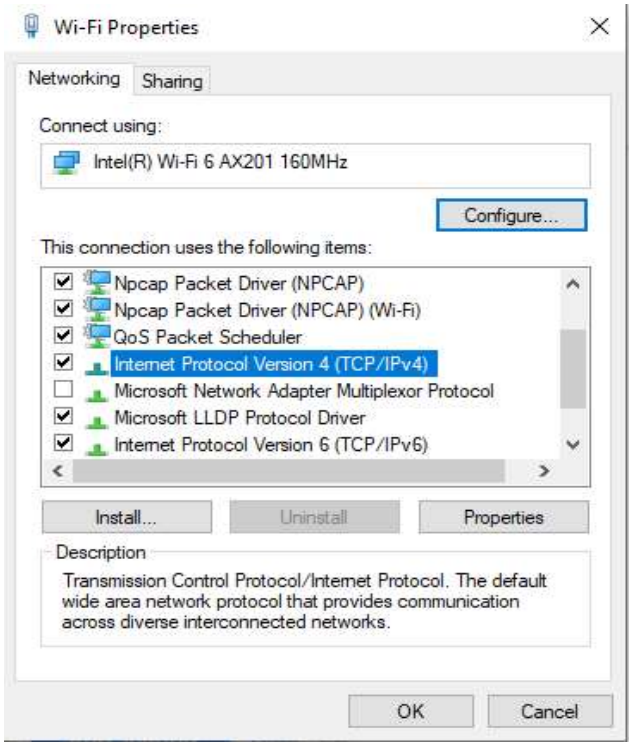
The IP address, Subnet mask and default gateways can be obtained here.



Wireless Properties:

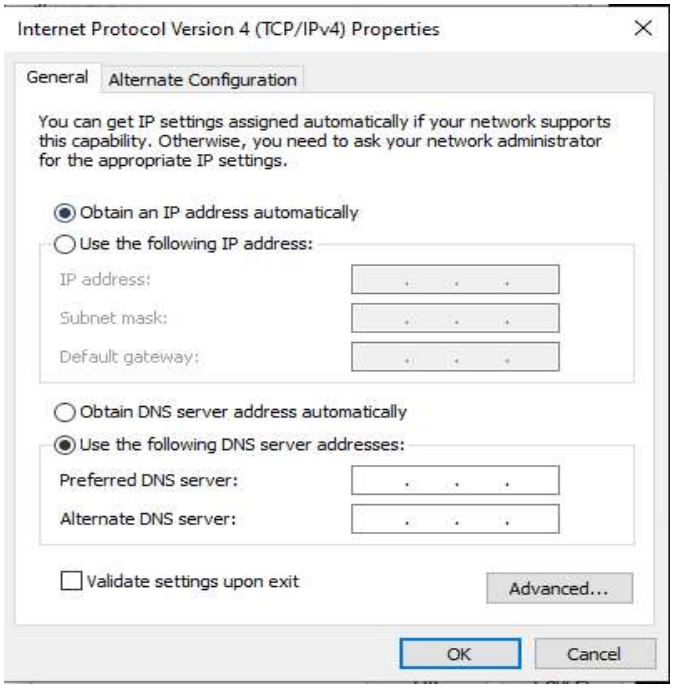


Wi-Fi Properties:



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

EXPERIMENT – 4

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

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

OBJECTIVE: To demonstrate building a switch – based network / ConfigurationCisco Catalyst Switch 3560.

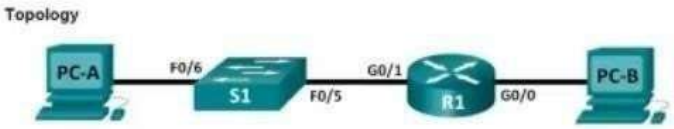
ALGORITHM:

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:



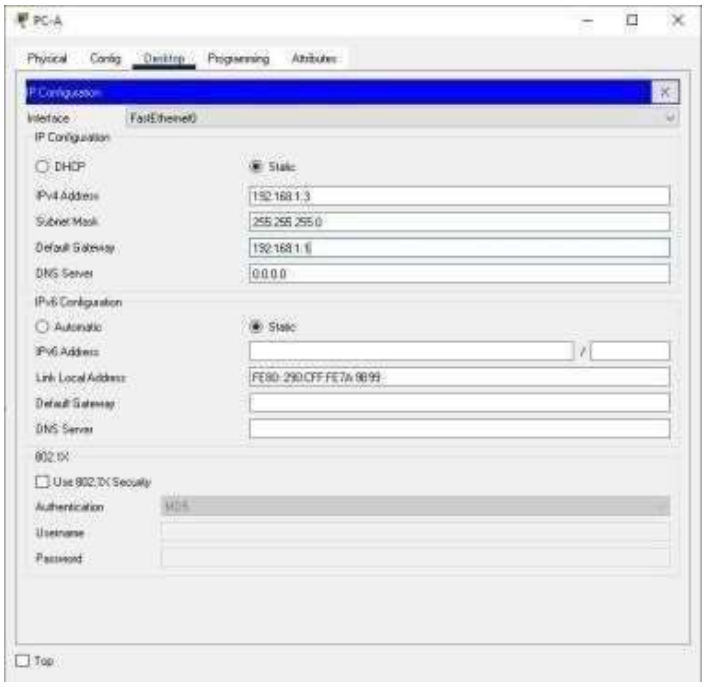
Addressing Table

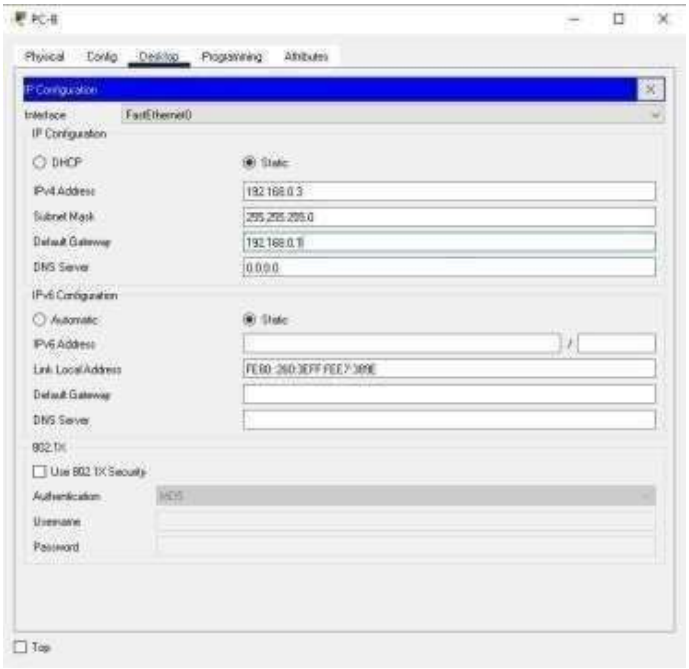
Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	192.168.0.1	255.255.255.0	N/A
	G0/1	192.168.1.1	255.255.255.0	N/A
S1	VLAN 1	N/A	N/A	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.0.3	255.255.255.0	192.168.0.1

Laying out required devices:

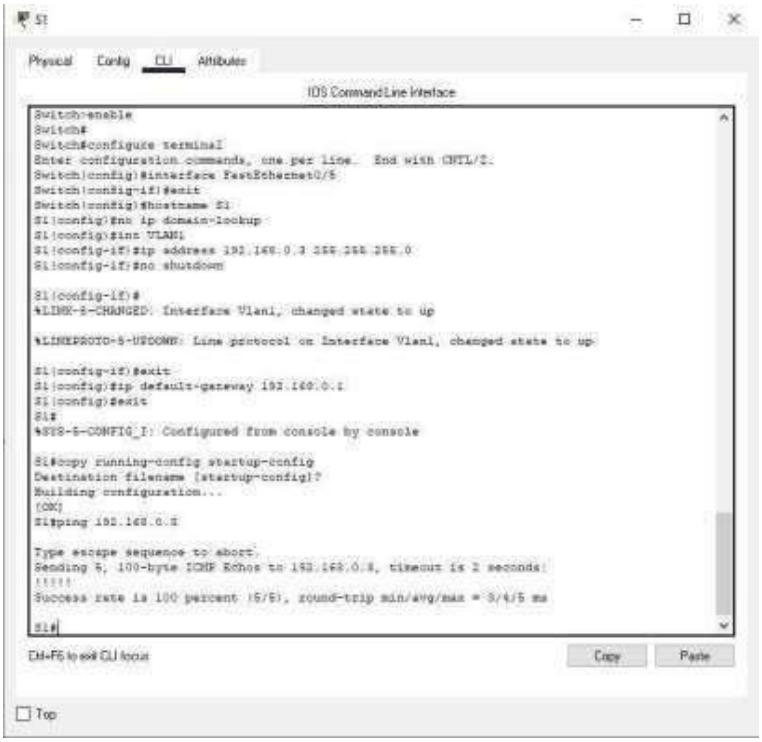
Connecting the devices using cables:

Configuring PC-A and PC-B:

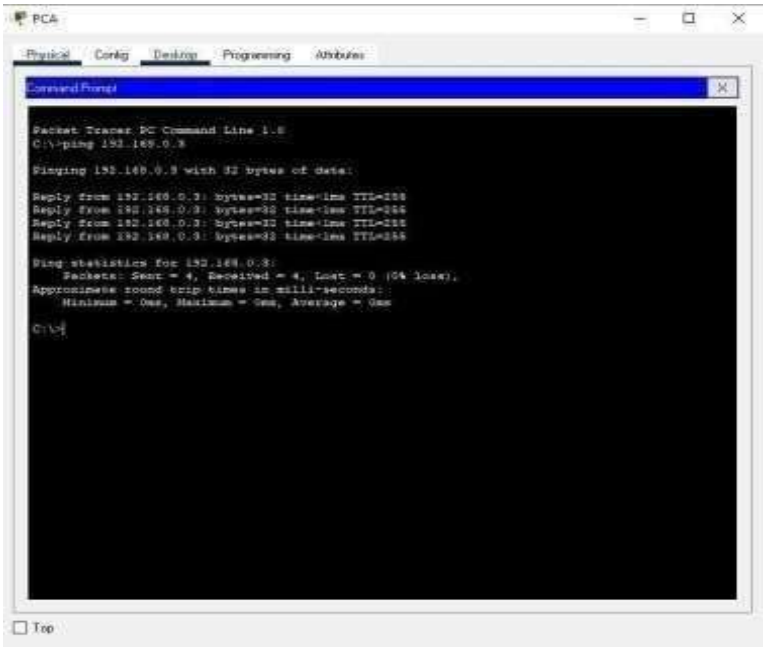




Configuring Switch S1:



Checking ping from PCA to PCB:



RESULTS: Afterthe configuration and connection of all devices, the ping issuccessful from PC-A to PC-B.

EXPERIMENT – 5

5. Configuration of Cisco Router 2900

AIM: Configuration of Cisco Router 2900

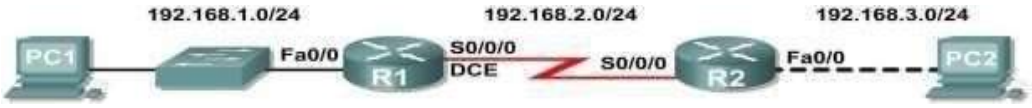
OBJECTIVE: To demonstrate Configuration Of Cisco Router 2900.

ALGORITHM:

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

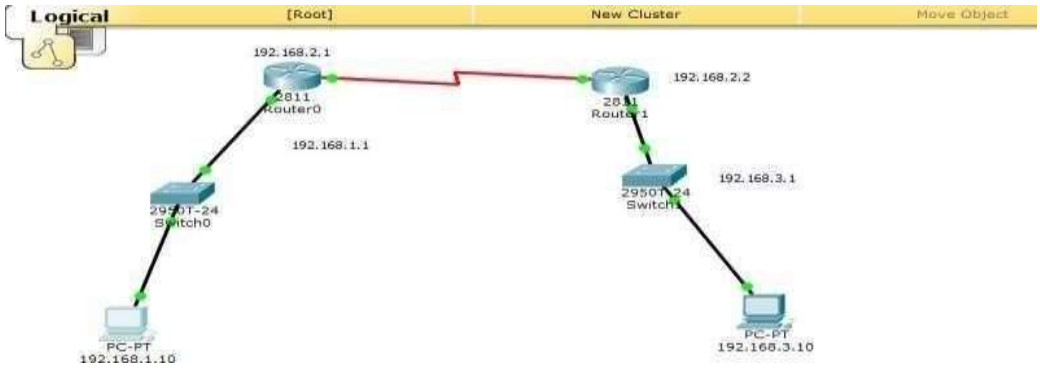
DESCRIPTION AND EXECUTION:

Resources: 2 Switch, 2 PCs, 2 Router.

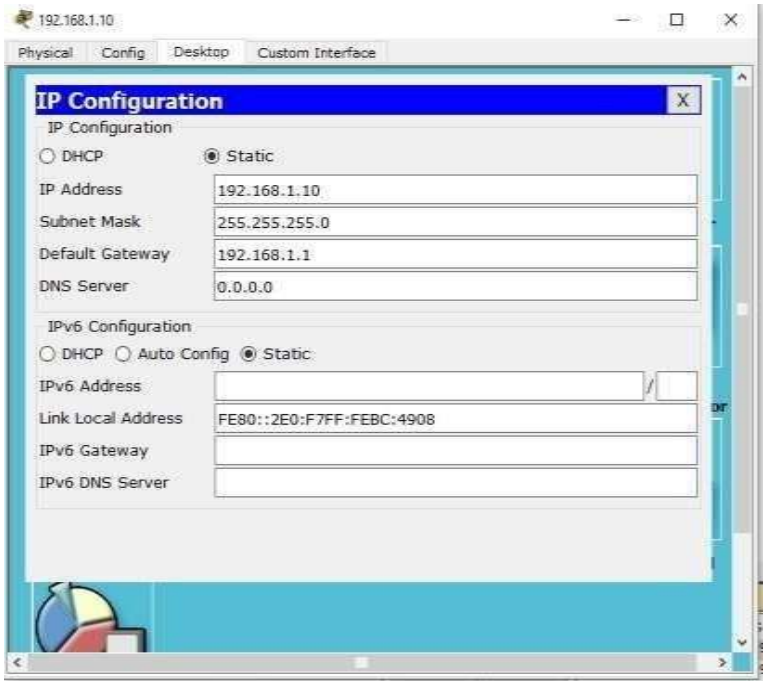


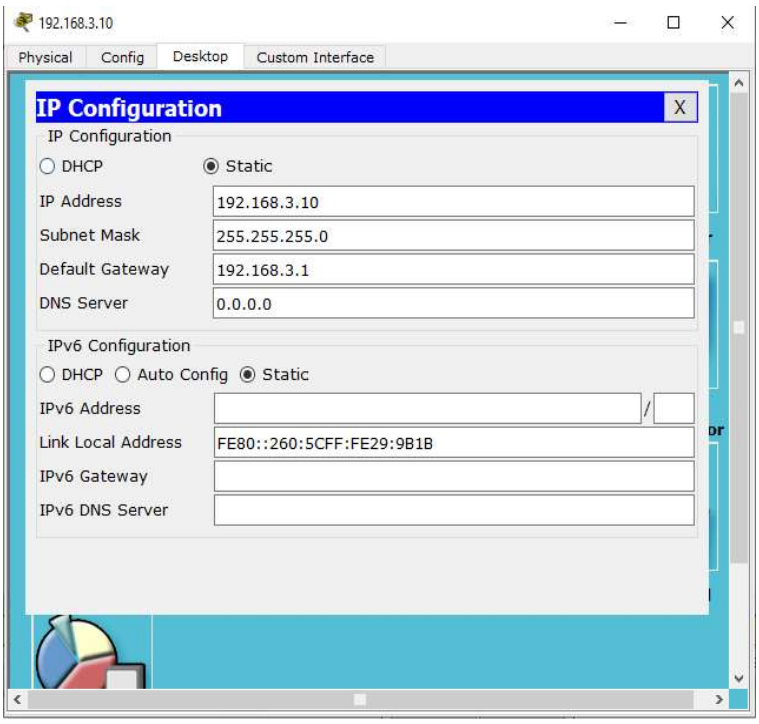
Device	Interface	IP Address	Subnet Mask	Def. Gateway
R1	Fa0/0	192.168.1.1	255.255.255.0	N/A
	S0/0/0	192.168.2.1	255.255.255.0	N/A
R2	Fa0/0	192.168.3.1	255.255.255.0	N/A
	S0/0/0	192.168.2.2	255.255.255.0	N/A
PC1	N/A	192.168.1.10	255.255.255.0	192.168.1.1
PC2	N/A	192.168.3.10	255.255.255.0	192.168.3.1

Connecting the devices using cables:

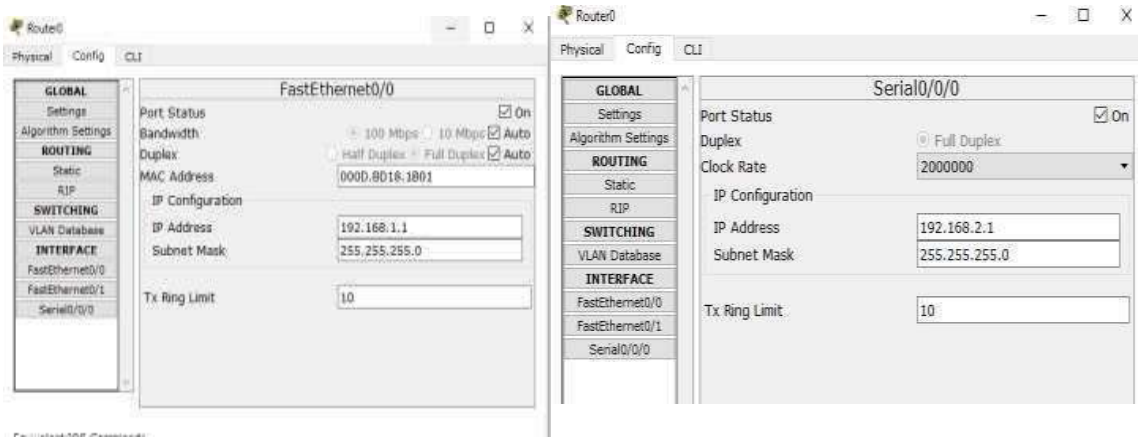


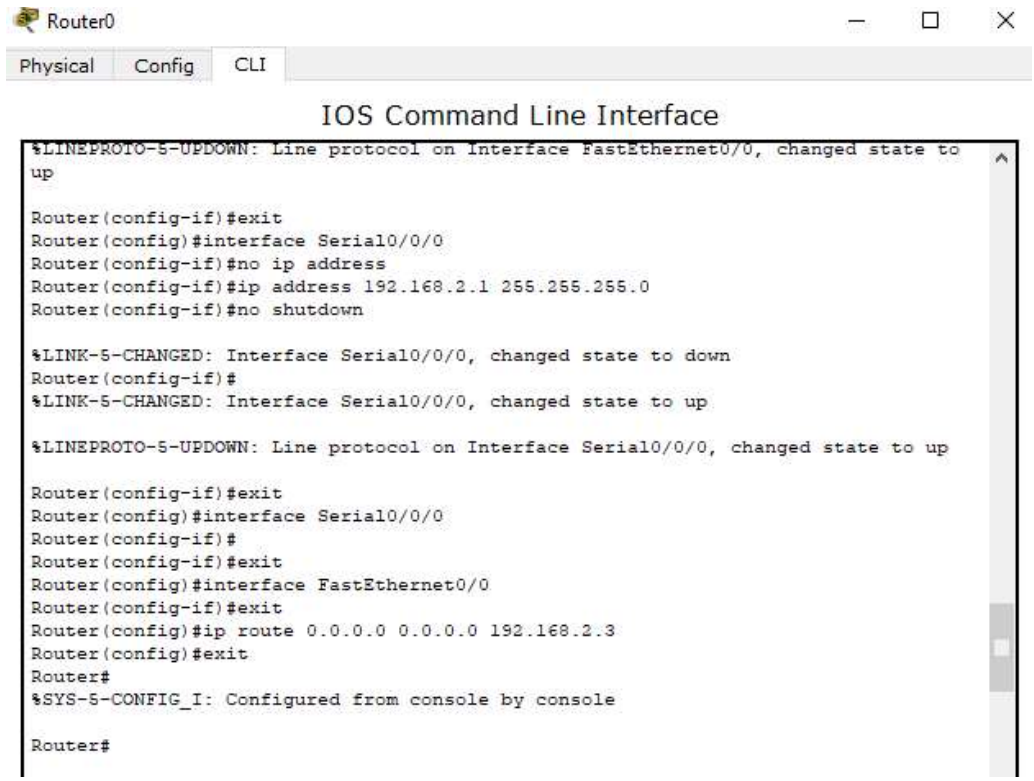
Configuring PC-A and PC-B:



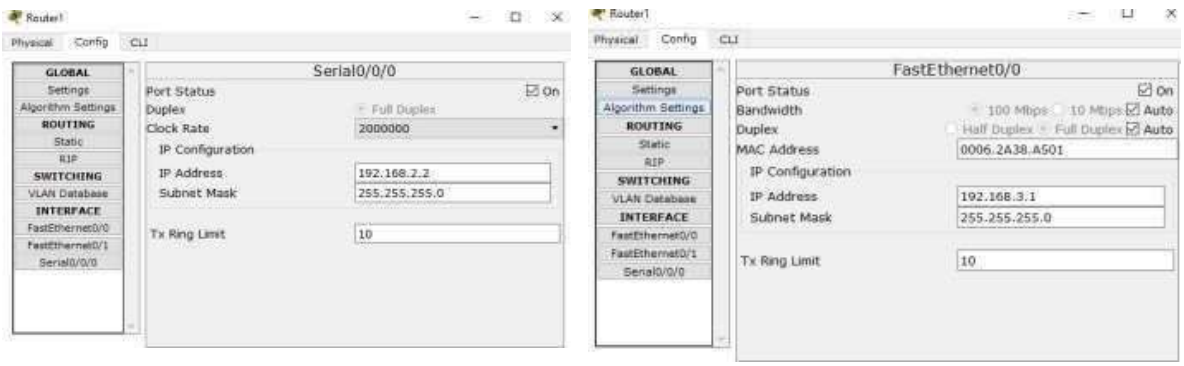


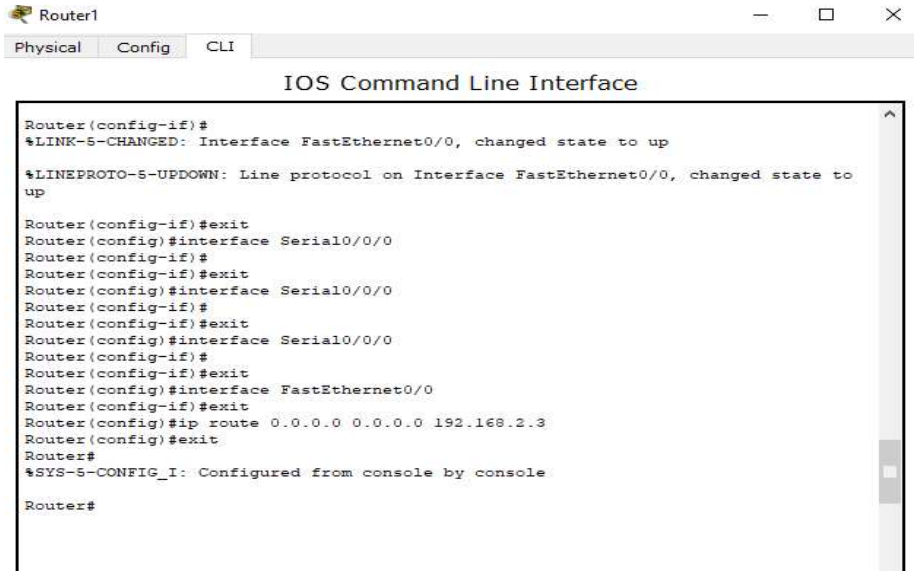
Configuring router 1:



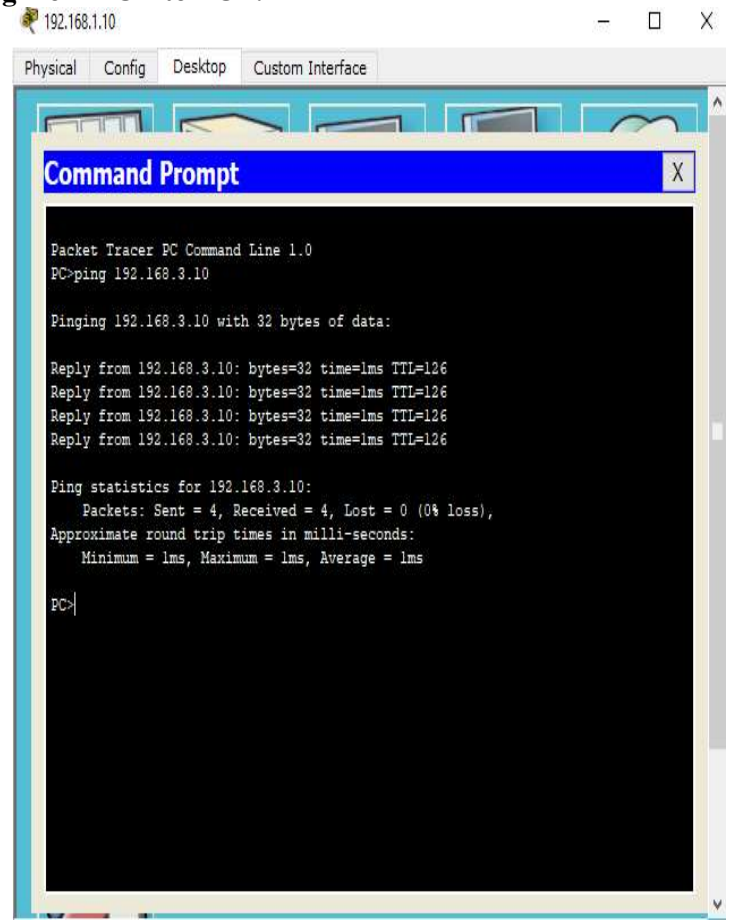


Configuring router 2:





Checking ping from PCA to PCB:



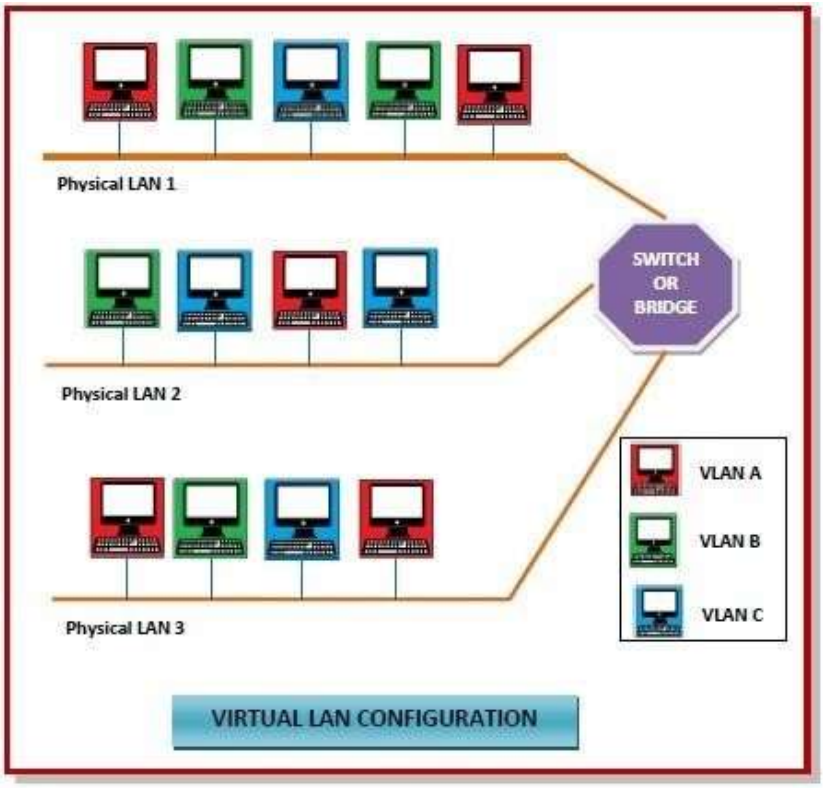
RESULTS: After the configuration and connection of all devices, the ping is successfulfrom PC-A to PC-B.

Experiment-6

AIM: To demonstrate VLAN routing using CISCO Packet tracer.

DESCRIPTION:

- Virtual Local Area Networks or Virtual LANs (VLANs) are a logical group of computers that appear to be on the same LAN irrespective of the configuration of the underlying physical network.
- Network administrators partition the networks to match the functional requirements of the VLANs so that each VLAN comprises a subset of ports on a single or multiple switches or bridges.
- This allows computers and devices in a VLAN to communicate in the simulated environment as if it is a separate LAN.

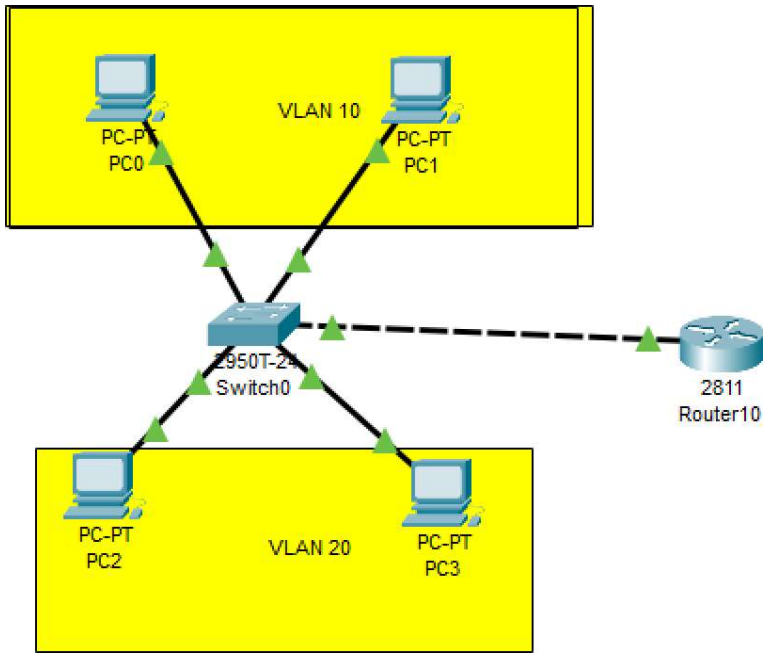


ALGORITHM:

1. Start
2. Setup the Topology and initialise devices
3. Configure Devices and router and verify connectivity
4. Enter the code in CLI.

5. Display Device information
6. End

TOPOLOGY DIAGRAM:



CLI:

Router:

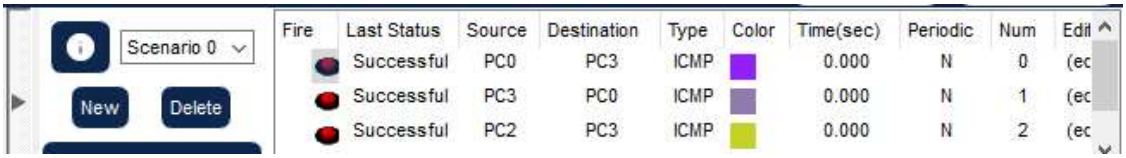
```
R1(config)#interface fastEthernet 0/0
R1(config-if)#no shutdown
R1(config-if)#exit

R1(config)#interface fastEthernet 0/0.10
R1(config-subif)#encapsulation dot1Q 10
R1(config-subif)#ip address 192.168.10.254 255.255.255.0
R1(config-subif)#exit

R1(config)#interface fastEthernet 0/0.20
R1(config-subif)#encapsulation dot1Q 20
R1(config-subif)#ip address 192.168.20.254 255.255.255.0
```

Switch:

```
Switch#config terminal
Switch(config)#vlan 10
Switch(config-vlan)#name SALES
Switch(config-vlan)#vlan 20
Switch(config-vlan)#name IT
```

```
Switch>enable
Switch#config terminal

Switch(config)#int fa0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10

Switch(config-if)#int fa0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10

Switch(config-if)#int fa0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20

Switch(config-if)#int fa0/4
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
```

RESULTS:

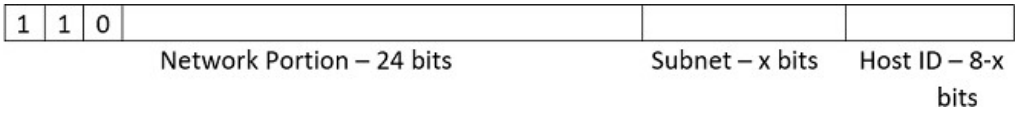


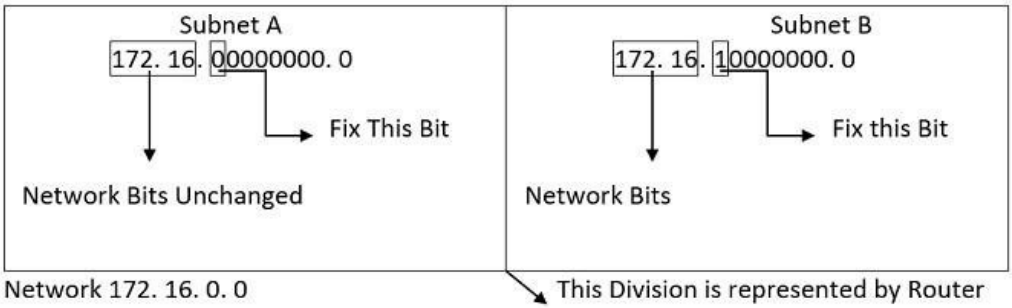
EXPERIMENT – 7

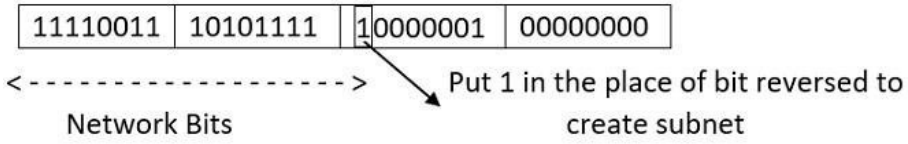
AIM: To demonstrate subnet masking using Cisco Packet tracer.

DESCRIPTION:

- Subnetting is a combination of two words i.e. Sub and Netting. Here Sub word means Substitute and netting word means Network. The Substitute Network created for a function to happen is known as Subnetting.
- Here, Substitute Network does not mean a new network is created. A full piece of the network is broken into small pieces and each piece is assigned a different name.
- Subnet is the name given to a piece of the broken network or can also be called as the Substitute network is known as Subnet.
- Subnets are the legal small parts of IP (Internet Protocol) Addressing process

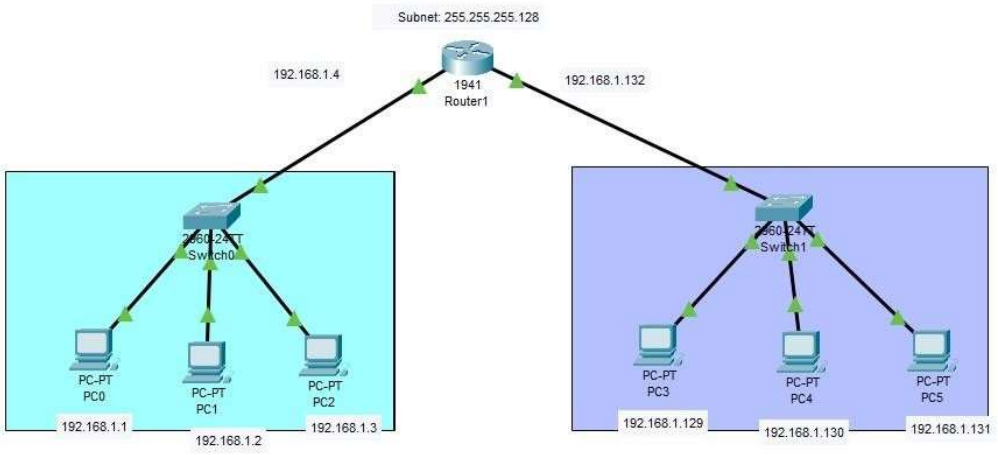




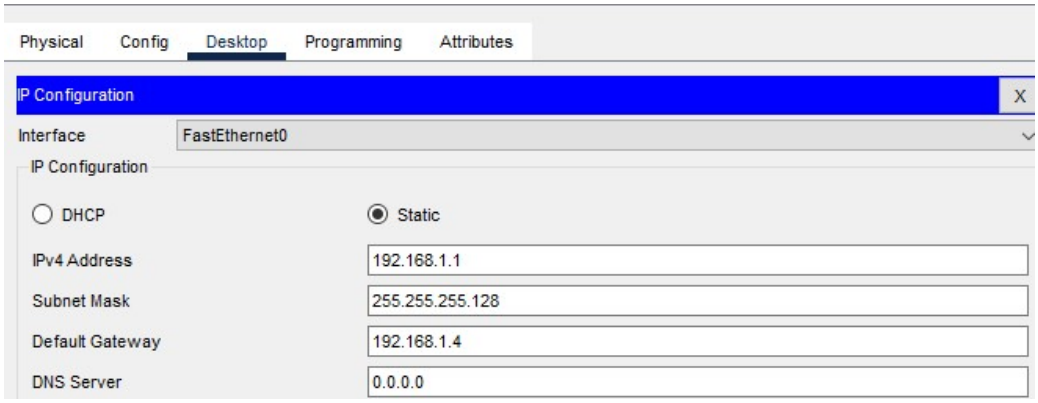


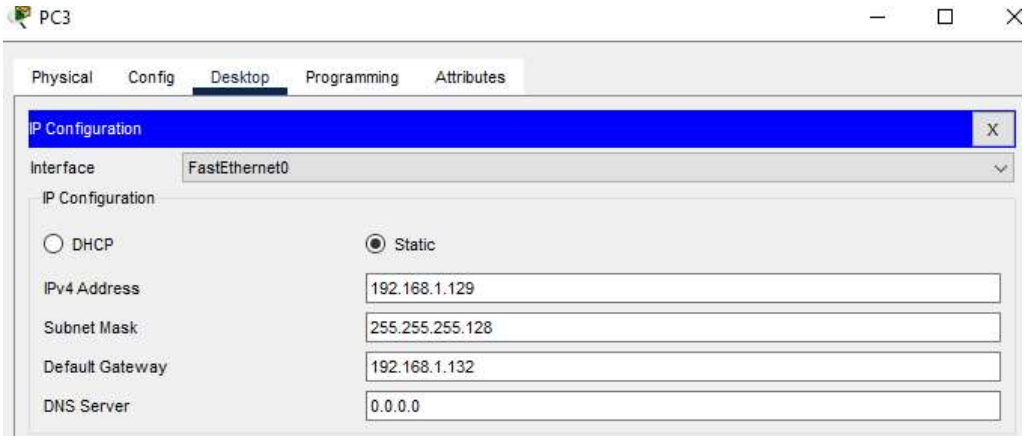
Subnet Mask = 243. 175. 129. 0

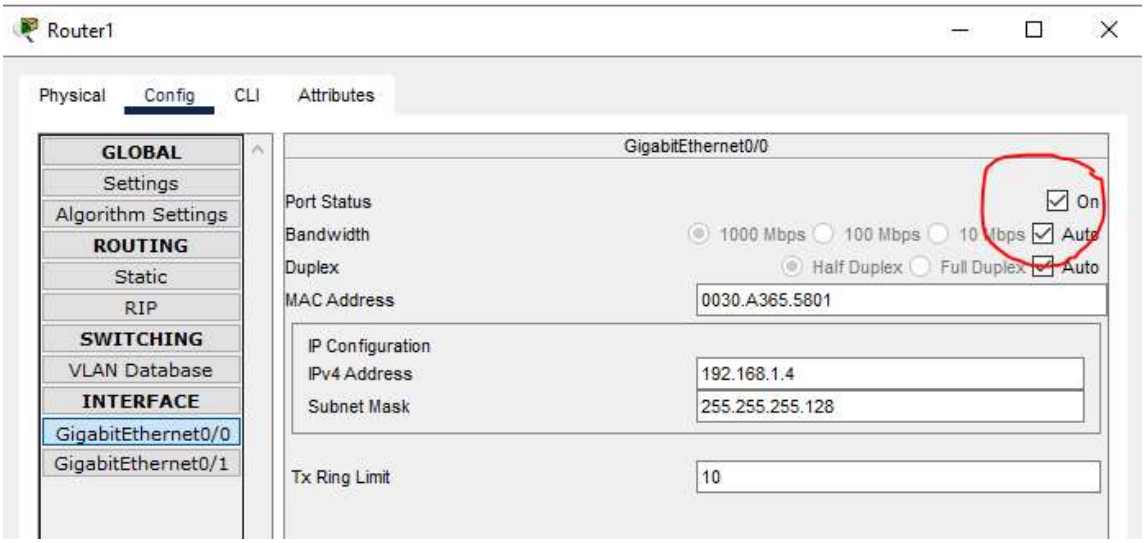
TOPOLOGY DIAGRAM:



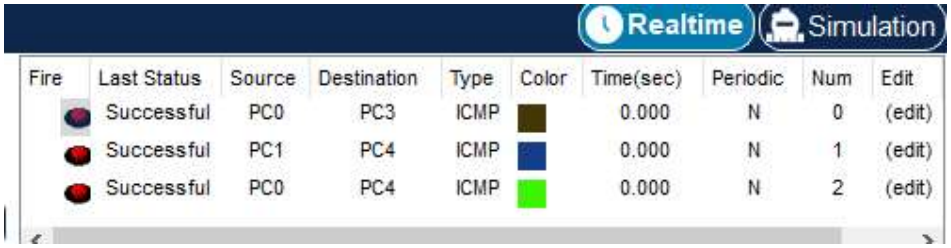
CONFIGURATION:






Router1
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
0030.A365.5801
IP Configuration
IPv4 Address
192.168.1.4
Subnet Mask
255.255.255.128
Tx Ring Limit
10

RESULTS:


Realtime
Simulation
Fire
Last Status
Source
Destination
Type
Color
Time(sec)
Periodic
Num
Edit
Successful PC0 PC3 ICMP 0.000 N 0 (edit)
Successful PC1 PC4 ICMP 0.000 N 1 (edit)
Successful PC0 PC4 ICMP 0.000 N 2 (edit)

EXPERIMENT – 8

AIM: To demonstrate static routing using a Cisco Packet tracer.

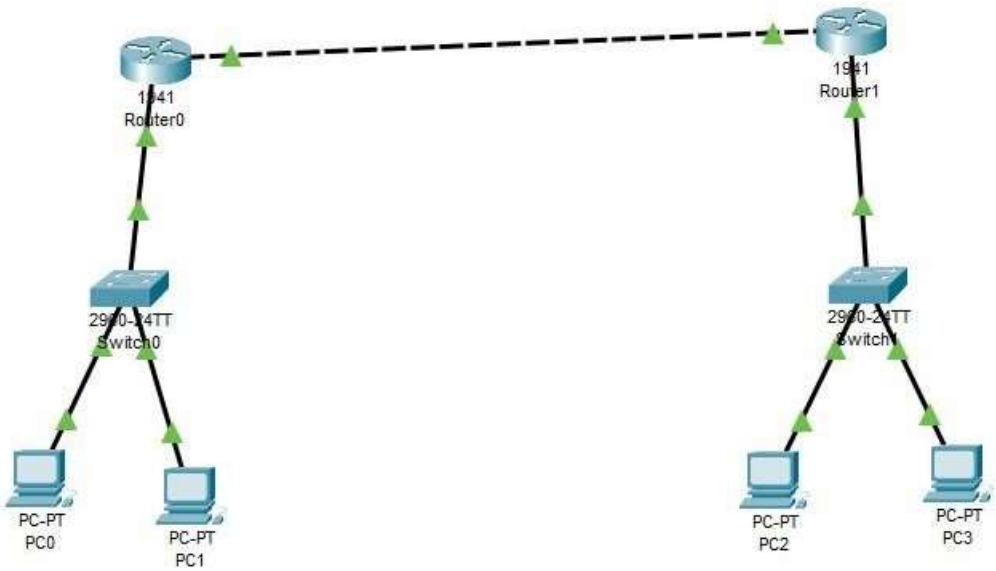
DESCRIPTION:

- Static routing is a form of routing that occurs when a router uses a manually-configured routing entry, rather than information from dynamic routing traffic.
- In many cases, static routes are manually configured by a network administrator byadding entries into a routing table, though this may not always be the case
- .Unlike dynamic routing, static routes are fixed and do not change if the network ischanged or reconfigured.
- Static routing and dynamic routing are not mutually exclusive. Both dynamic routingand static routing are usually used on a router to maximize routing efficiency
- and to provide backups in case dynamic routing information fails to be exchanged. Static routing can also be used in stub networks, or to provide a gateway of last resort

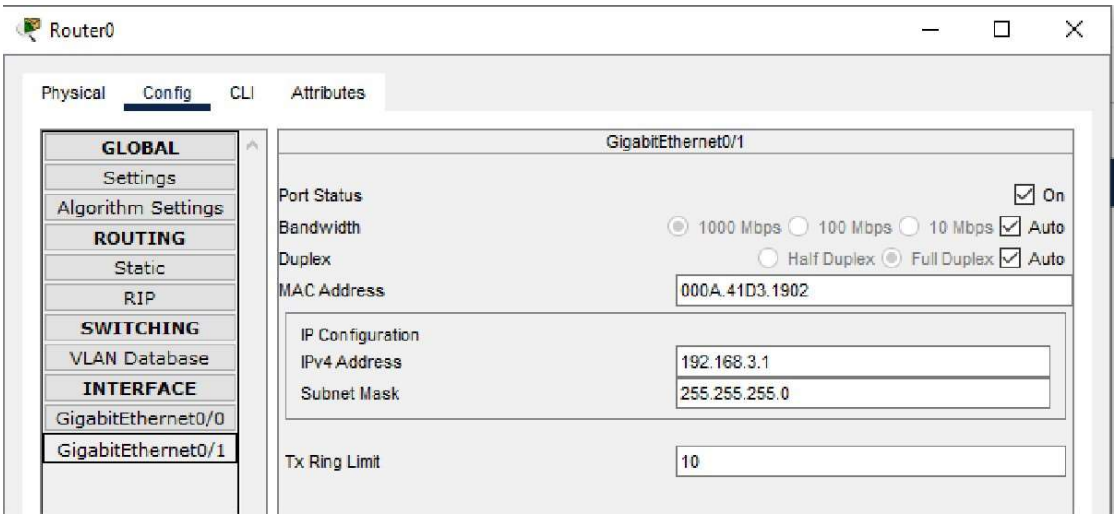
ALGORITHM:

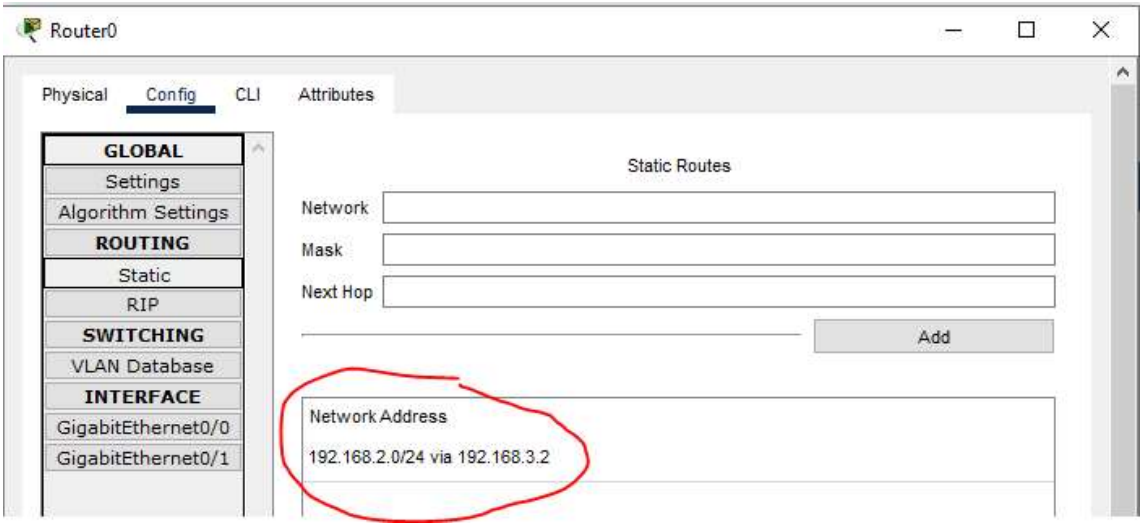
1. Start
2. Setup the Topology and initialize devices
3. Configure Devices and routers and verify connectivity
4. Enter the configuration in the static space in the router
5. Display Device information
6. End

TOPOLOGY DIAGRAM:

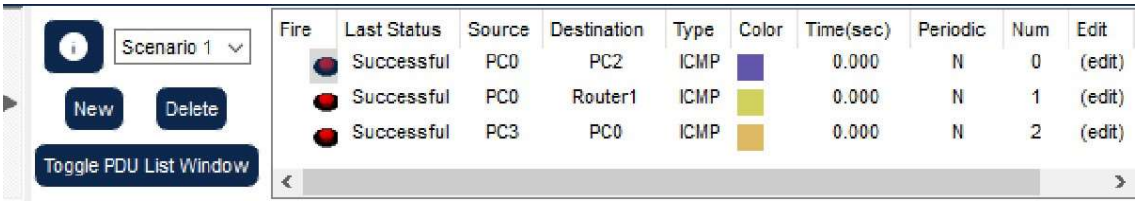


CONFIGURATION:


Router0
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
000A.41D3.1902
IP Configuration
IPv4 Address
192.168.3.1
Subnet Mask
255.255.255.0
Tx Ring Limit
10


Router0
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0
GigabitEthernet0/1
Static Routes
Network
Mask
Next Hop
Add
Network Address
192.168.2.0/24 via 192.168.3.2

RESULTS:


Scenario 1
New
Delete
Toggle PDU List Window
Fire
Last Status
Source
Destination
Type
Color
Time(sec)
Periodic
Num
Edit
Successful PC0 PC2 ICMP 0.000 N 0 (edit)
Successful PC0 Router1 ICMP 0.000 N 1 (edit)
Successful PC3 PC0 ICMP 0.000 N 2 (edit)

EXPERIMENT – 9

9. Basic OSPF Configuration

AIM: Basic OSPF Configuration

OBJECTIVE: To demonstrate Basic OPSF Configuration.

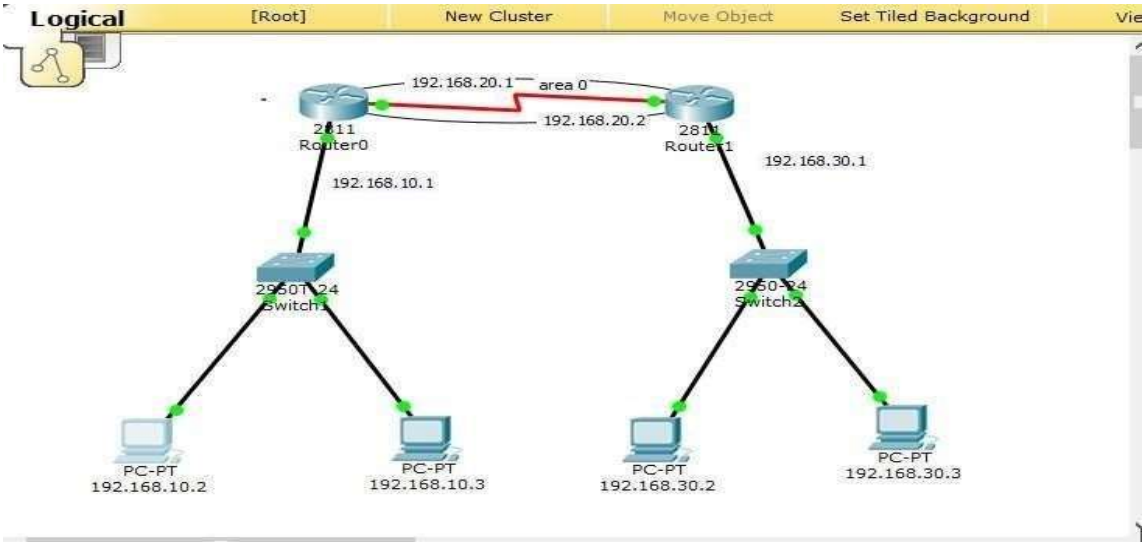
ALGORITHM:

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

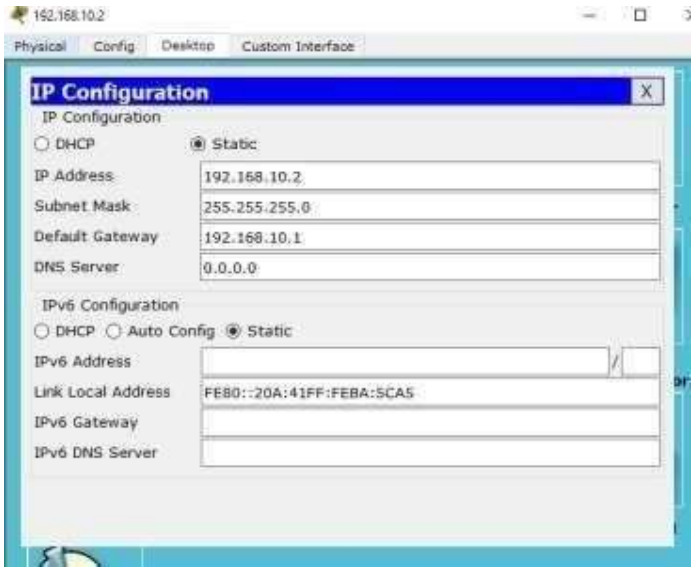
DESCRIPTION AND EXECUTION:

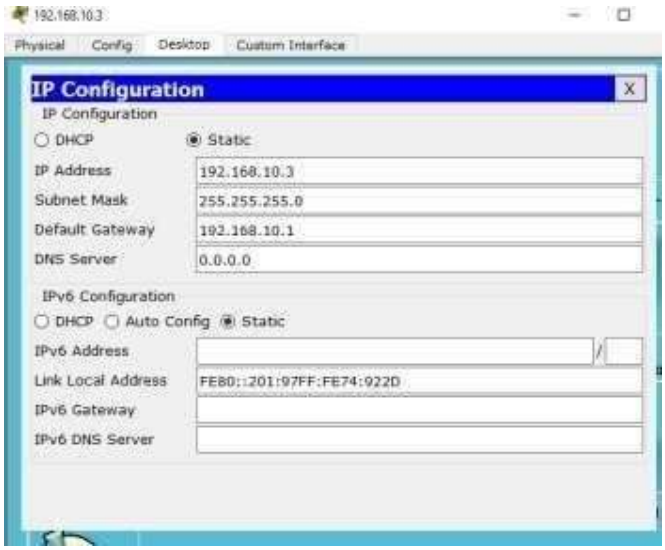
- OSPF is a link-state routing protocol. Link-state protocols use the shortest path first (SPF)algorithm to populate the routing table. OSPF shares information with every router in the network.
- OSPF is considered a difficult protocol to configure and requires a thorough understanding ofterms that are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

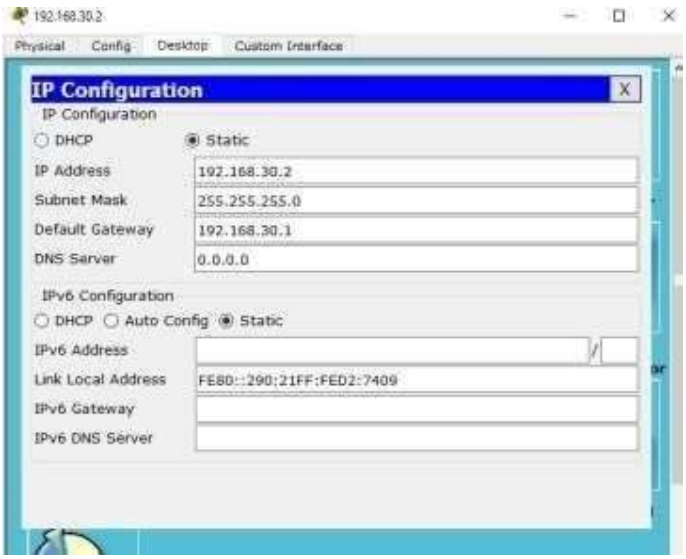
Connecting the devices using cables:

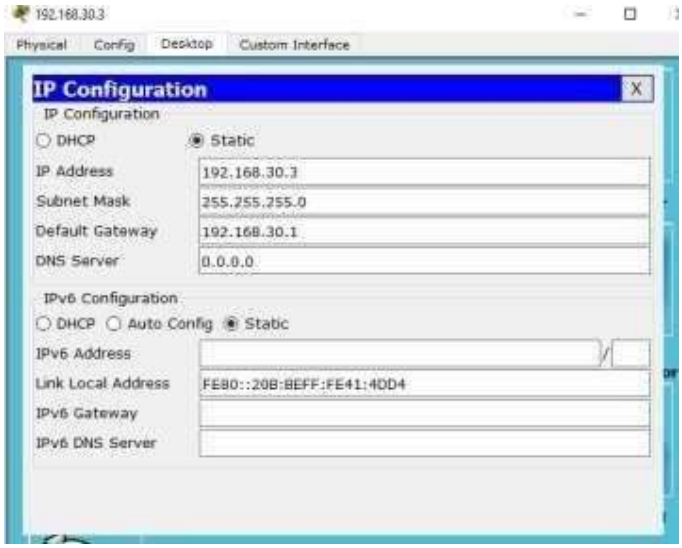


Configuring PC‘s:



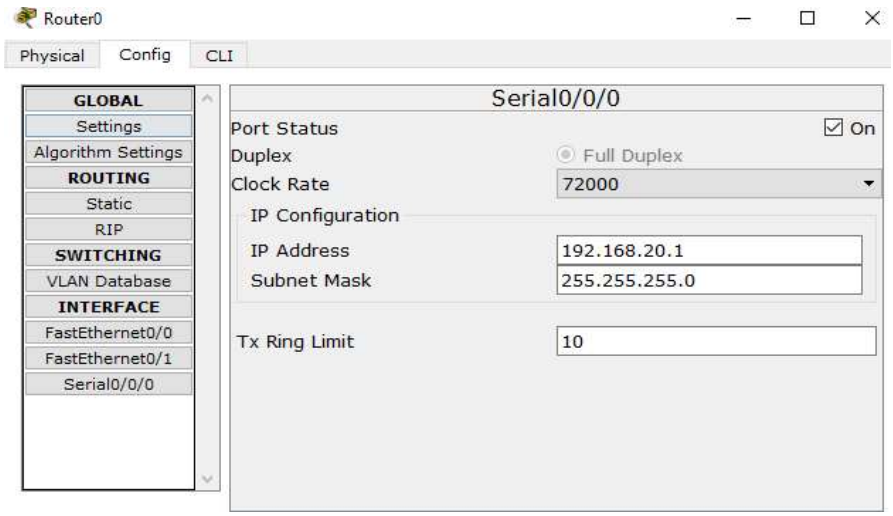


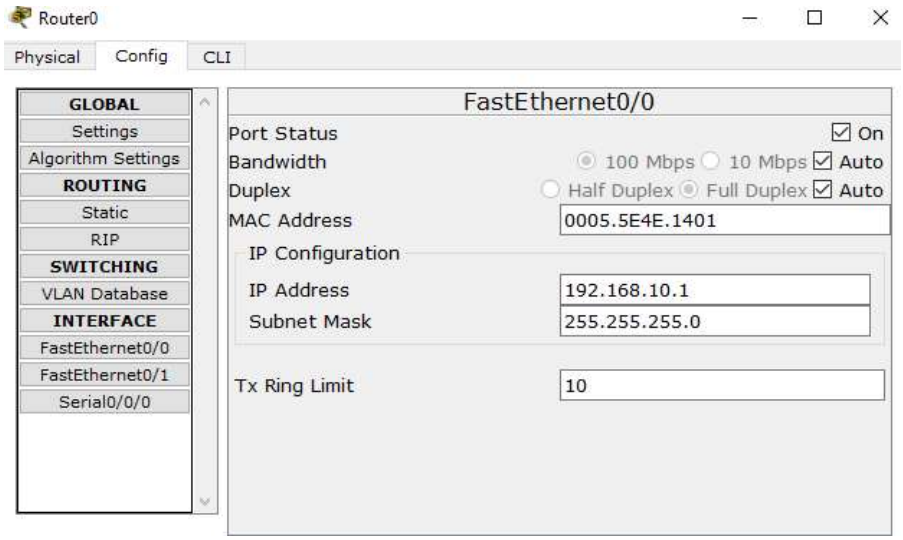




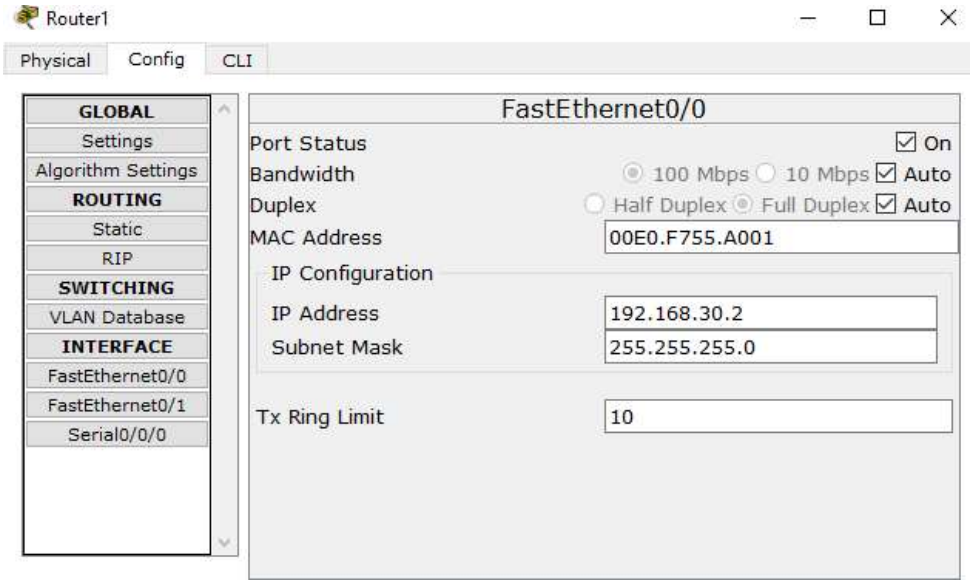
Configuring Routers:

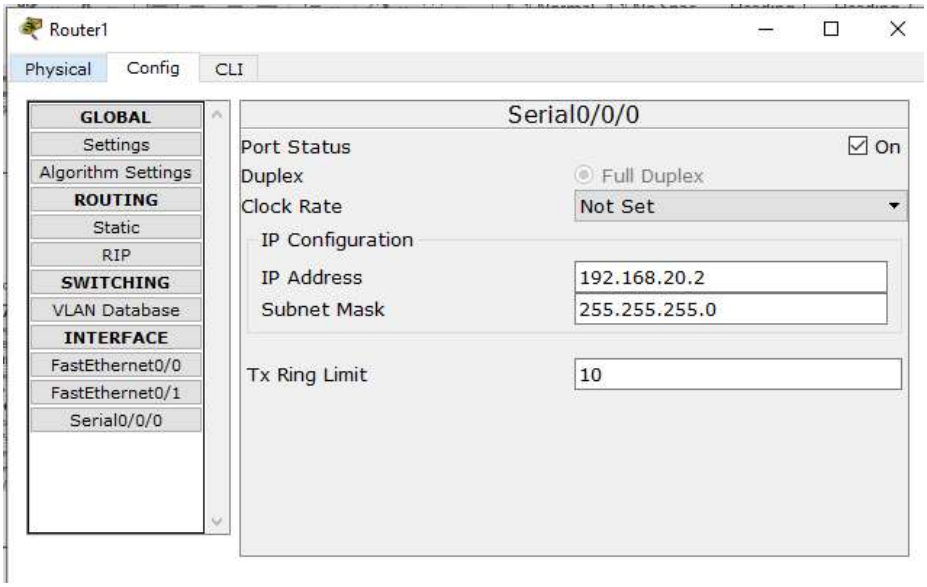
Router 0: Config



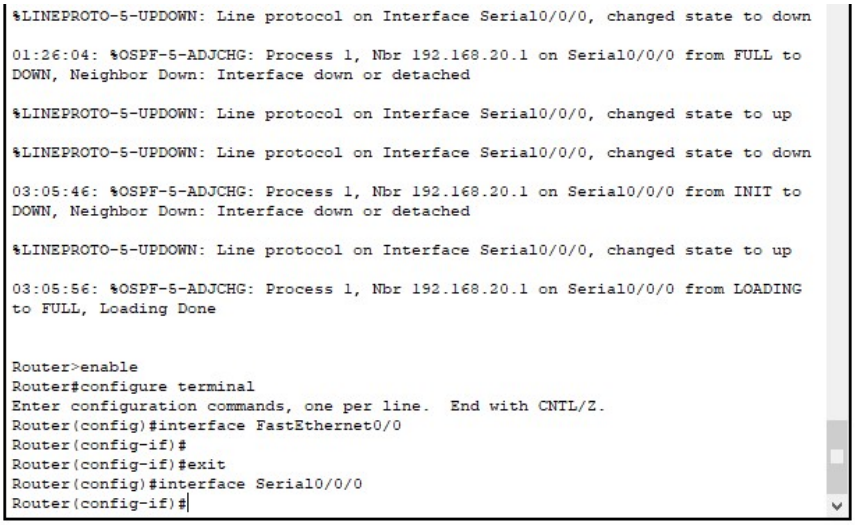


Router 1: config

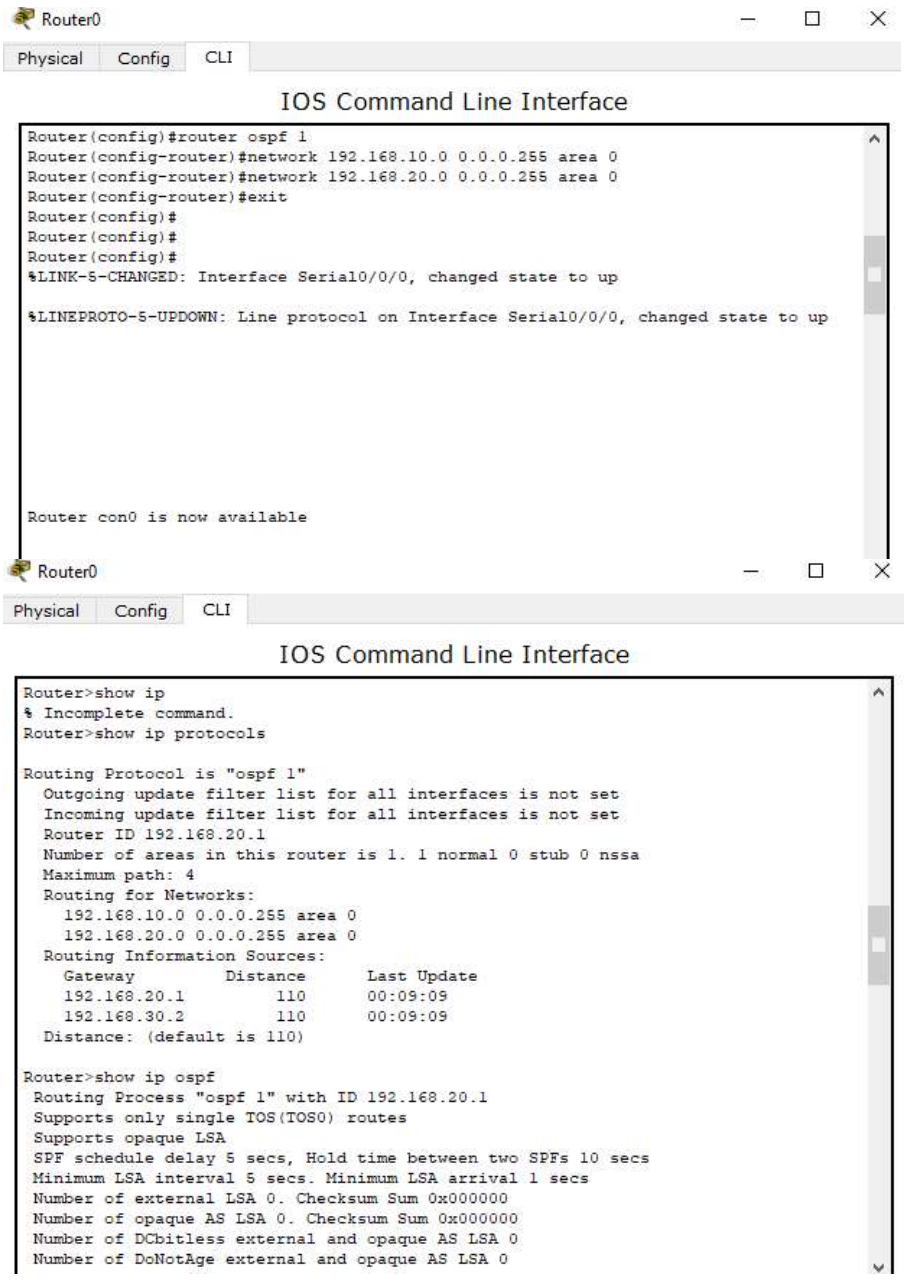




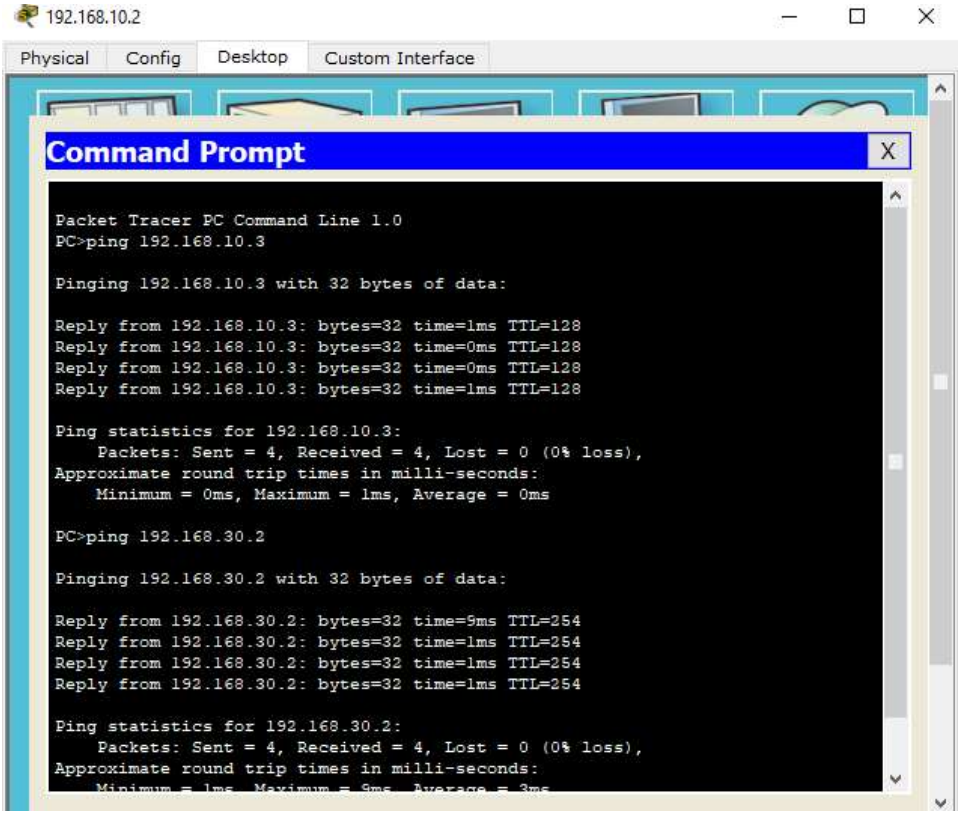
Router 1: CLI



Router 0: CLI


Router0
Physical
Config
CLI
IOS Command Line Interface
Router(config)#router ospf 1
Router(config-router)#network 192.168.10.0 0.0.0.255 area 0
Router(config-router)#network 192.168.20.0 0.0.0.255 area 0
Router(config-router)#exit
Router(config)#
Router(config)#
Router(config)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
Router con0 is now available
Router0
Physical
Config
CLI
IOS Command Line Interface
Router>show ip
% Incomplete command.
Router>show ip protocols
Routing Protocol is "ospf 1"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Router ID 192.168.20.1
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Maximum path: 4
Routing for Networks:
192.168.10.0 0.0.0.255 area 0
192.168.20.0 0.0.0.255 area 0
Routing Information Sources:
Gateway Distance Last Update
192.168.20.1 110 00:09:09
192.168.30.2 110 00:09:09
Distance: (default is 110)
Router>show ip ospf
Routing Process "ospf 1" with ID 192.168.20.1
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
Number of external LSA 0. Checksum Sum 0x000000
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0

Checking Ping:



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

EXPERIMENT / PRACTICAL - 10

10. Basic EIGRP Configuration

AIM: Basic EIGRP Configuration

OBJECTIVE: To demonstrate Basic EIGRP Configuration and To display EIGRP with aprocess ID of1.

ALGORITHM:

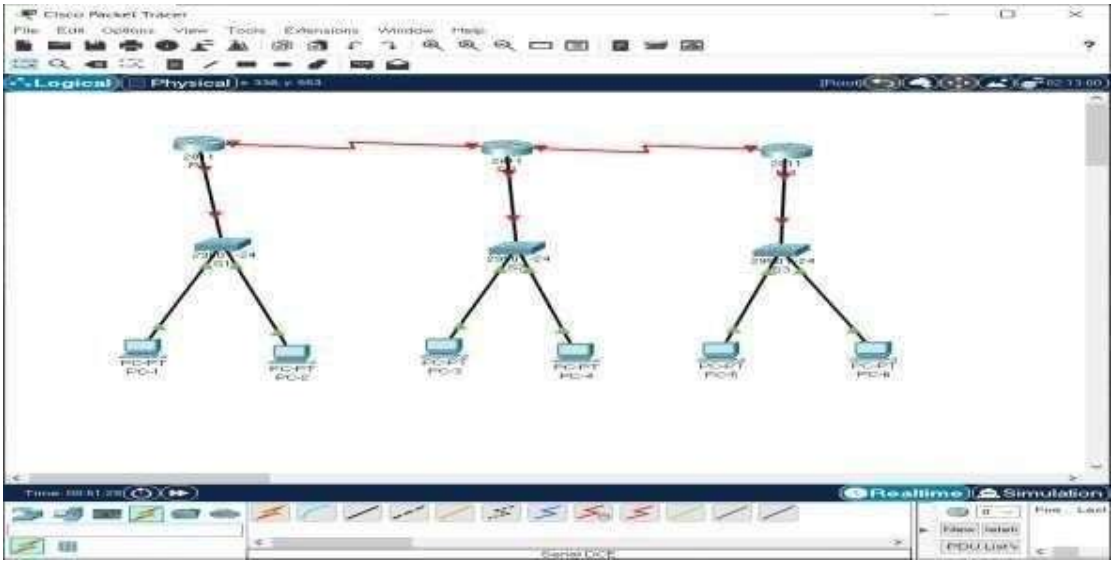
1. Start Cisco Packet Tracer application.
2. Setup devices and cable them according to the topo logical diagram.
3. Configure fast ethernet interface for router 1, 2 and3.
4. Configure serial 0/0/0 interface for router 1 and3.
5. Configure serial 0/1/0 interface for router2.
6. Configure eigrp network for routers.
7. Configure PC‘s.
8. To verify connectivity, ping all PC‘s through command prompt.
9. Exit.

DESCRIPTION AND EXECUTION:

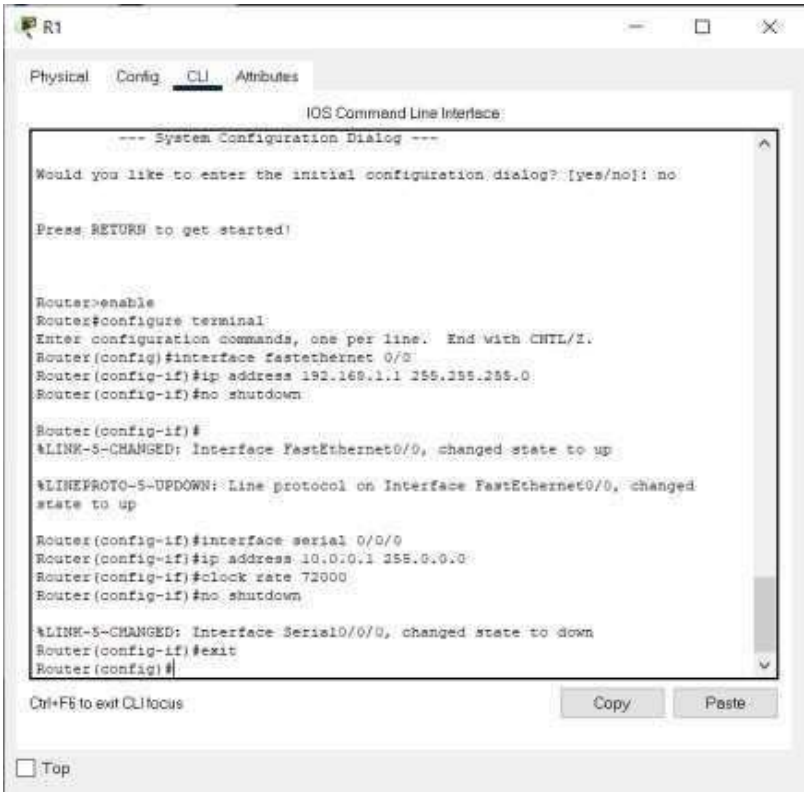
Enhanced Interior Gateway Routing Protocol is an interior gateway protocol suited for many different topologies and media. In a well-designed network, EIGRP scales well and provides extremely quick convergence times with minimal network traffic. It has very low usage of network resources during normal 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 anetwork.

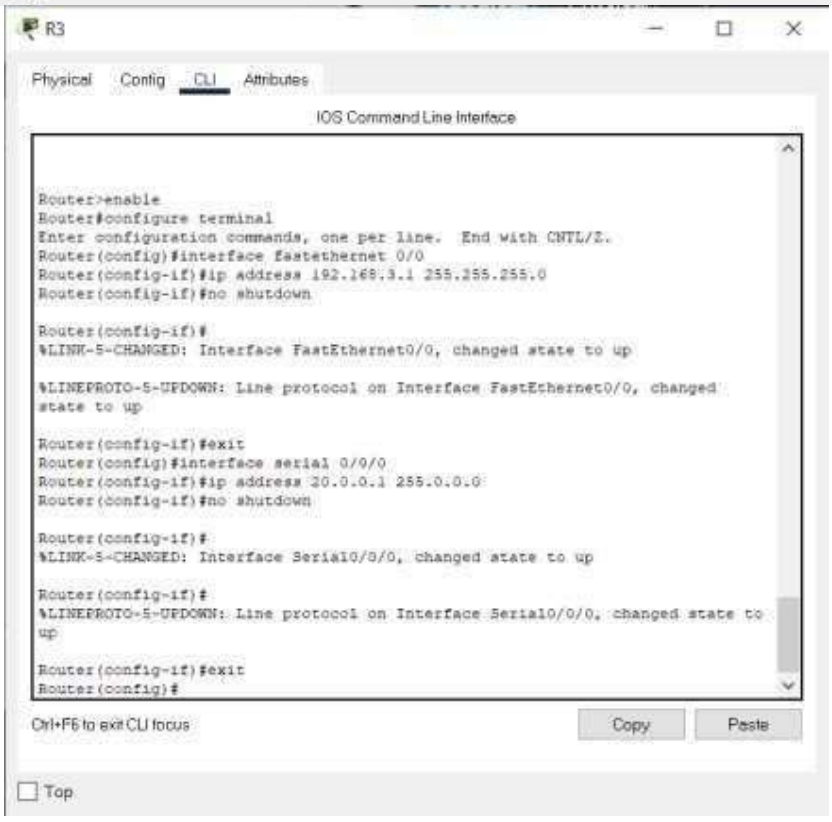
Setup topological network:

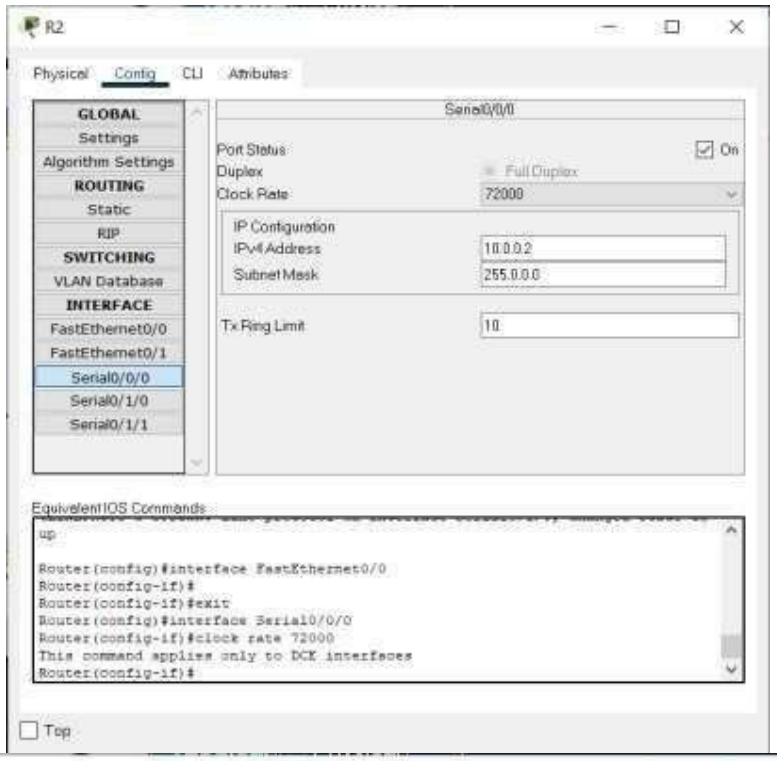


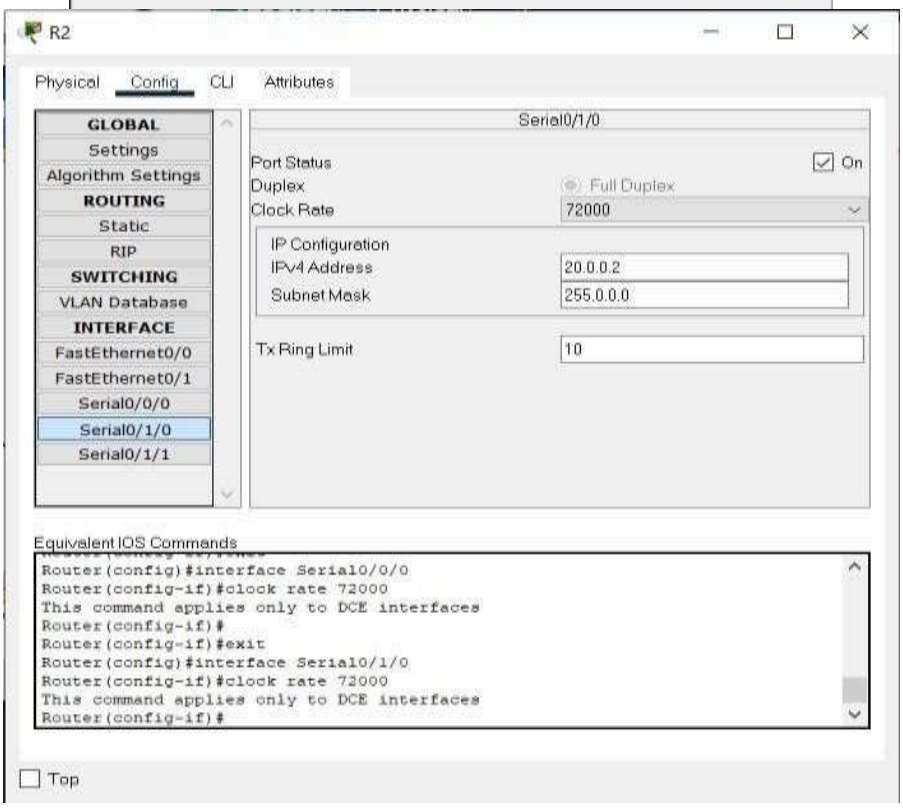
Router configuration:

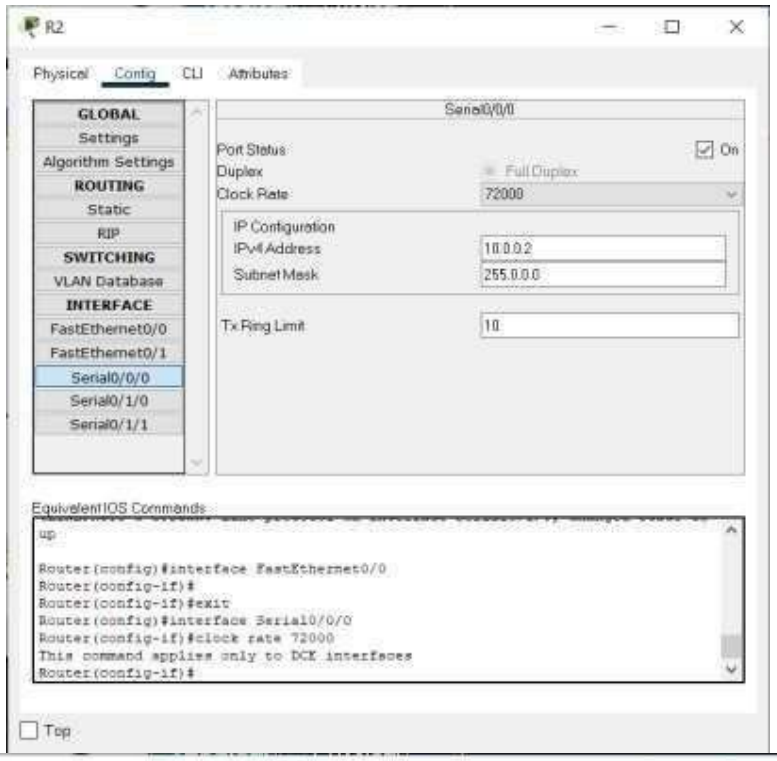


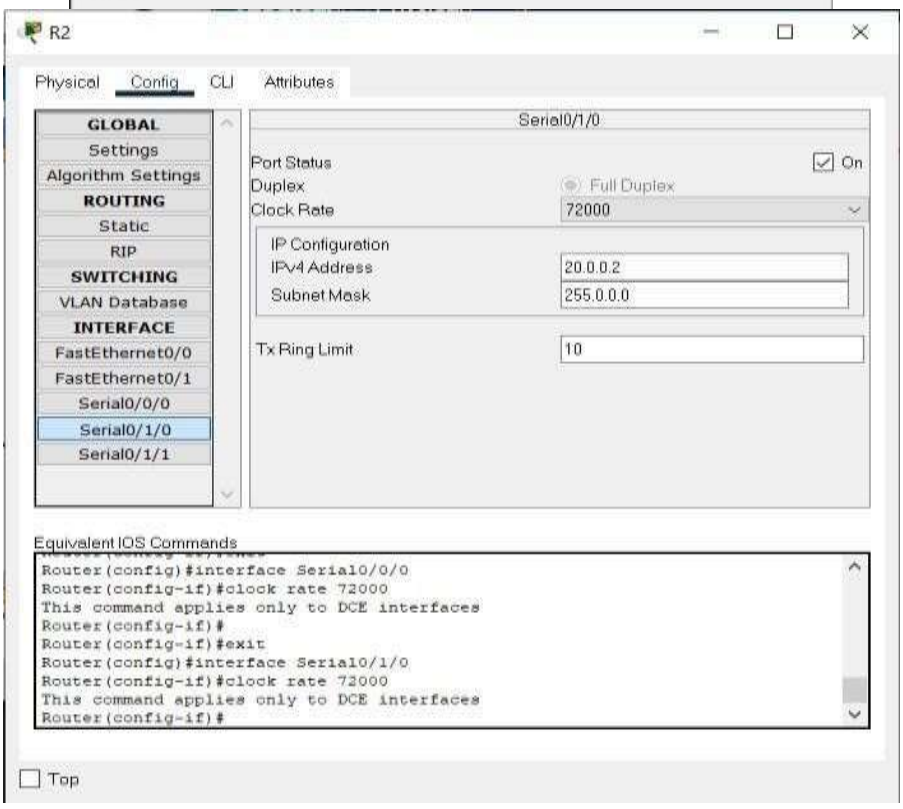

R2
Physical
Config
CLI
Attributes
3 Low-speed serial(sync/async) network interface(s)
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
2490368K bytes of ATA System CompactFlash 0 (Read/Write)
--- System Configuration Dialog ---
Would you like to enter the initial configuration dialog? [yes/no]: no
Press RETURN to get started!
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface fastethernet 0/0
Router(config-if)#ip address 192.168.2.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
Router(config-if)#exit
Router(config)#interface serial 0/0/0
Router(config-if)#ip address 10.0.0.2 255.0.0.0
Router(config-if)#clock rate 72000
This command applies only to DCE interfaces
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
Router(config-if)#exit
Router(config)#interfa
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
% Incomplete command.
Router(config)#interface serial 0/1/0
Router(config-if)#ip address 20.0.0.2 255.0.0.0
Router(config-if)#clock rate 72000
This command applies only to DCE interfaces
Router(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/1/0, changed state to down
Router(config-if)#exit
Router(config)#
Ctrl+F6 to exit CLI focus
Top

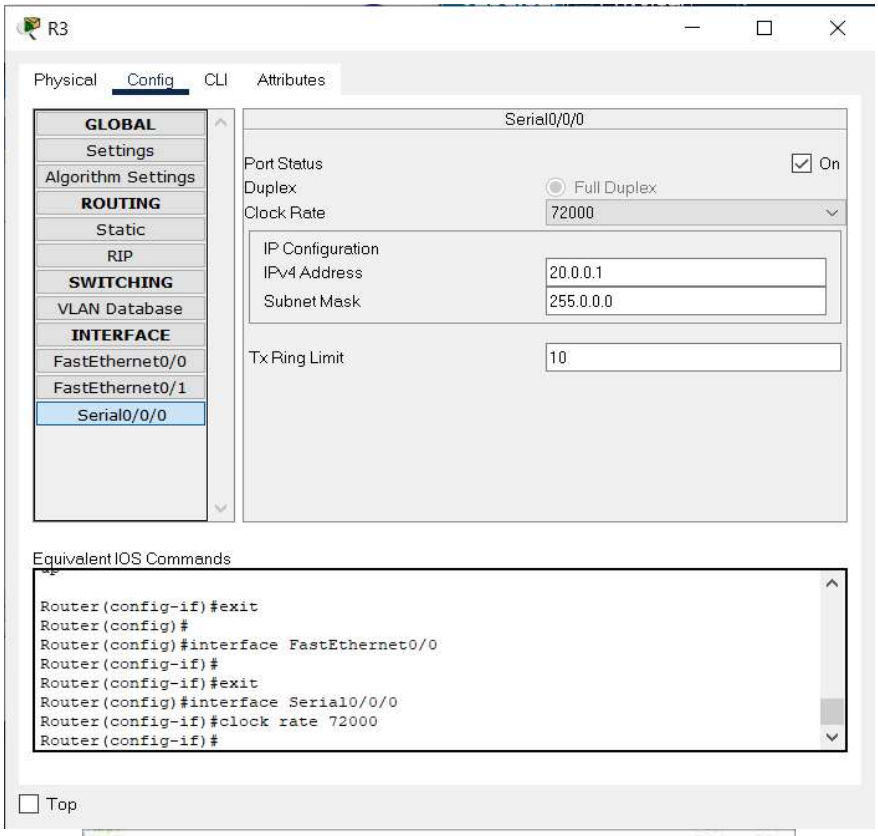

R3
Physical
Config
CLI
Attributes
IOS Command Line Interface
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface fastethernet 0/0
Router(config-if)#ip address 192.168.3.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
Router(config-if)#exit
Router(config)#interface serial 0/0/0
Router(config-if)#ip address 20.0.0.1 255.0.0.0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
Router(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
Router(config-if)#exit
Router(config)#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top

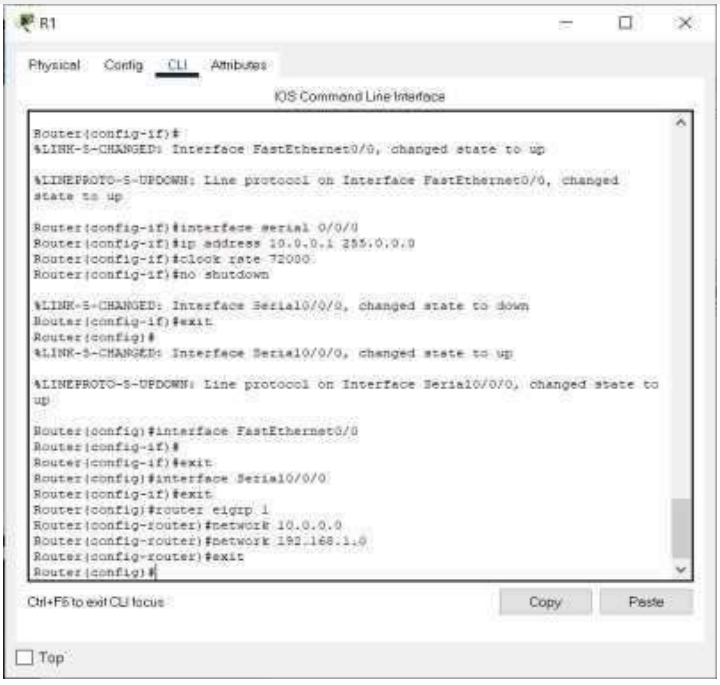

R2
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Serial0/0/0
Serial0/1/0
Serial0/1/1
Serial0/0/0
Port Status
On
Duplex
Full Duplex
Clock Rate
72000
IP Configuration
IPv4 Address
10.0.0.2
Subnet Mask
255.0.0.0
Tx Ring Limit
10
Equivalent IOS Commands
up
Router(config)#interface FastEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial0/0/0
Router(config-if)#clock rate 72000
This command applies only to DCE interfaces
Router(config-if)#
Top

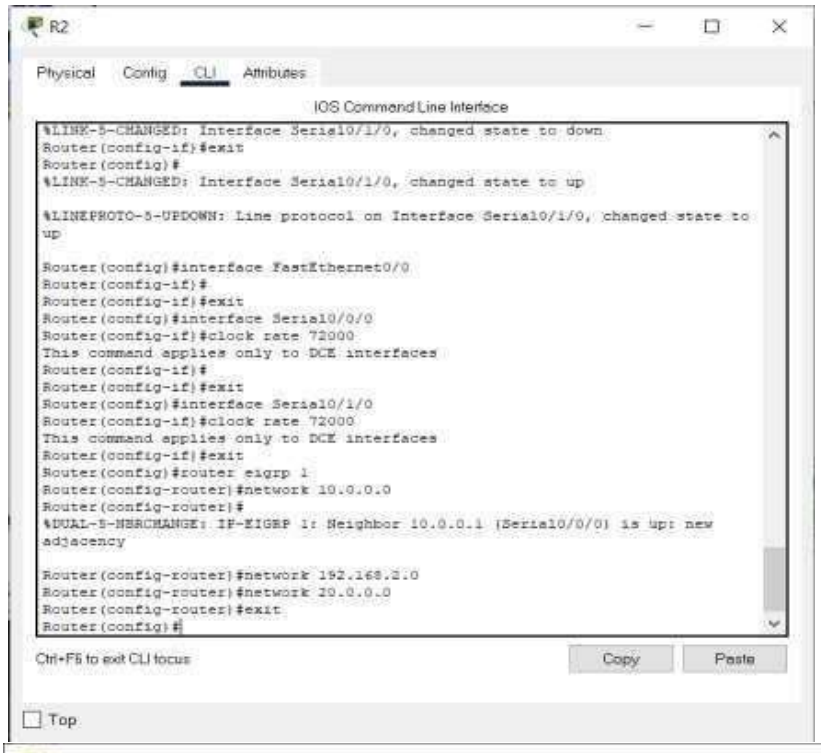

R2
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Serial0/0/0
Serial0/1/0
Serial0/1/1
Serial0/1/0
Port Status
On
Duplex
Full Duplex
Clock Rate
72000
IP Configuration
IPv4 Address
20.0.0.2
Subnet Mask
255.0.0.0
Tx Ring Limit
10
Equivalent IOS Commands
Router(config)#interface Serial0/0/0
Router(config-if)#clock rate 72000
This command applies only to DCE interfaces
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial0/1/0
Router(config-if)#clock rate 72000
This command applies only to DCE interfaces
Router(config-if)#
Top

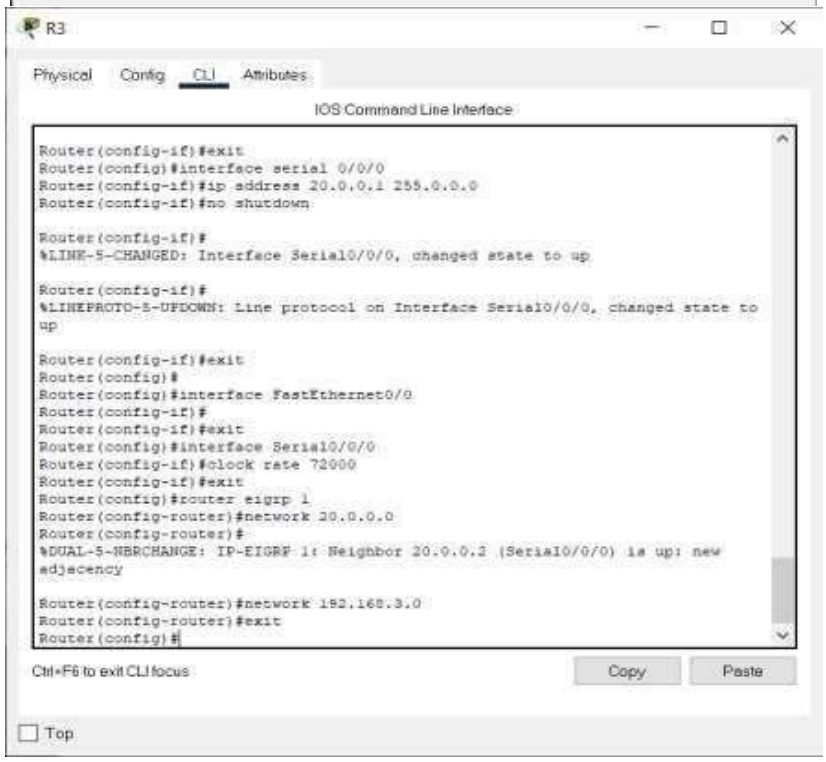

R2
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Serial0/0/0
Serial0/1/0
Serial0/1/1
Serial0/0/0
Port Status
On
Duplex
Full Duplex
Clock Rate
72000
IP Configuration
IPv4 Address
10.0.0.2
Subnet Mask
255.0.0.0
Tx Ring Limit
10
Equivalent IOS Commands
up
Router(config)#interface FastEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial0/0/0
Router(config-if)#clock rate 72000
This command applies only to DCE interfaces
Router(config-if)#
Top


R2
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Serial0/0/0
Serial0/1/0
Serial0/1/1
Serial0/1/0
Port Status
On
Duplex
Full Duplex
Clock Rate
72000
IP Configuration
IPv4 Address
20.0.0.2
Subnet Mask
255.0.0.0
Tx Ring Limit
10
Equivalent IOS Commands
Router(config)#interface Serial0/0/0
Router(config-if)#clock rate 72000
This command applies only to DCE interfaces
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial0/1/0
Router(config-if)#clock rate 72000
This command applies only to DCE interfaces
Router(config-if)#
Top

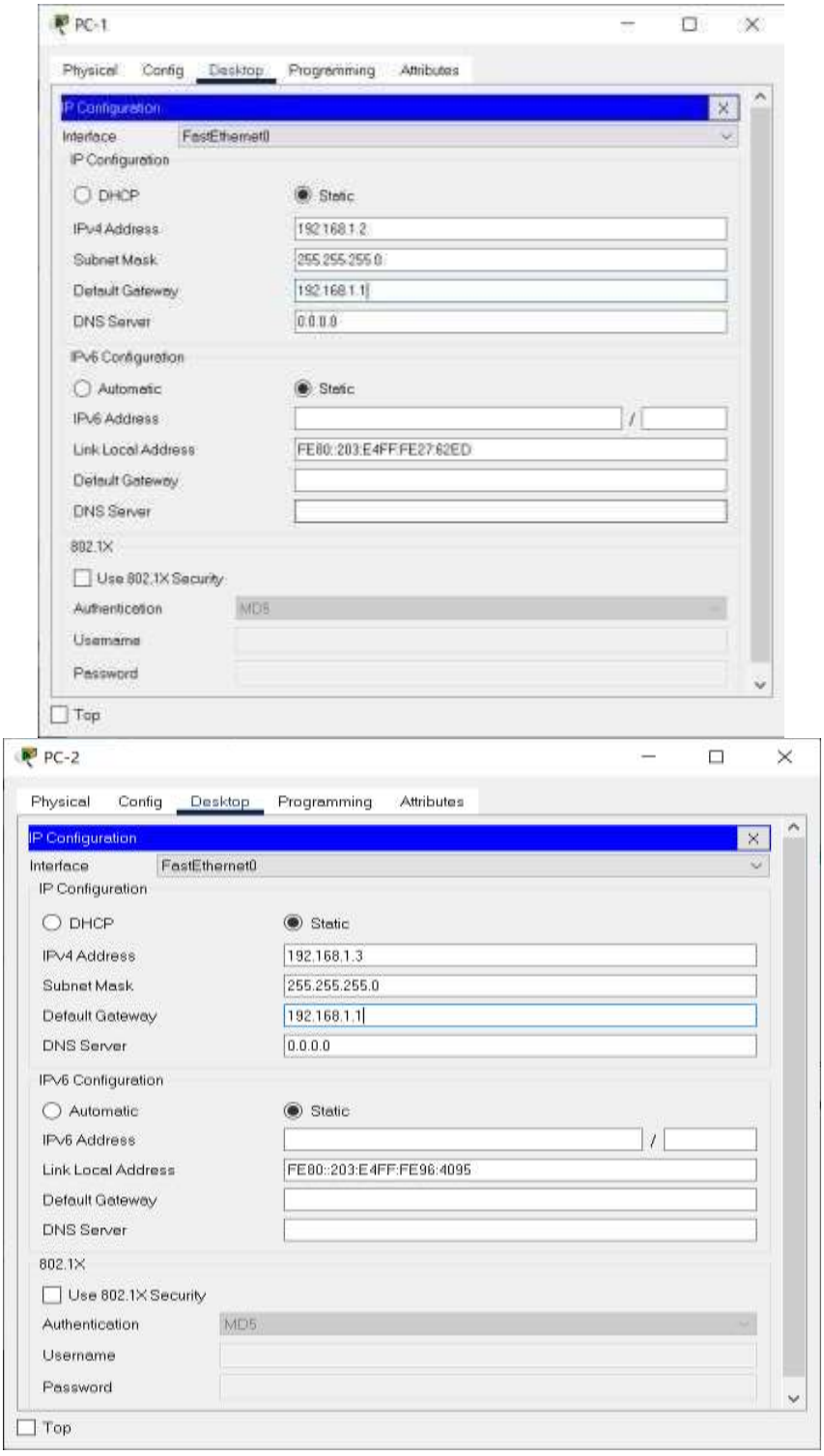

R3
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Serial0/0/0
Serial0/0/0
Port Status
On
Duplex
Full Duplex
Clock Rate
72000
IP Configuration
IPv4 Address
20.0.0.1
Subnet Mask
255.0.0.0
Tx Ring Limit
10
Equivalent IOS Commands
Router(config-if)#exit
Router(config)#
Router(config)#interface FastEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial0/0/0
Router(config-if)#clock rate 72000
Router(config-if)#
Top

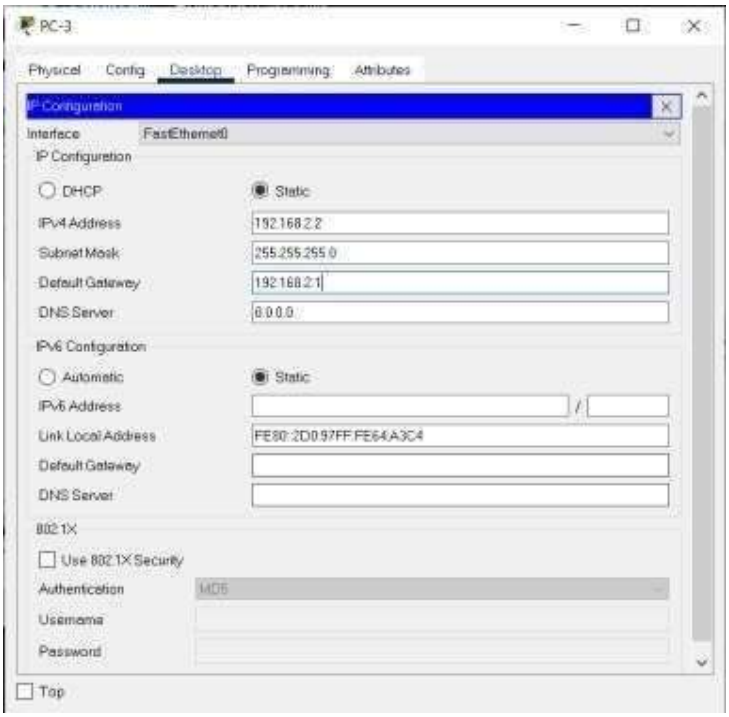

R1
Physical
Config
CLI
Attributes
IOS Command Line Interface
Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
Router(config-if)#interface serial 0/0/0
Router(config-if)#ip address 10.0.0.1 255.0.0.0
Router(config-if)#clock rate 72000
Router(config-if)#no shutdown
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
Router(config-if)#exit
Router(config)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
Router(config)#interface FastEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial0/0/0
Router(config-if)#exit
Router(config)#router eigrp 1
Router(config-router)#network 10.0.0.0
Router(config-router)#network 192.168.1.0
Router(config-router)#exit
Router(config)#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top

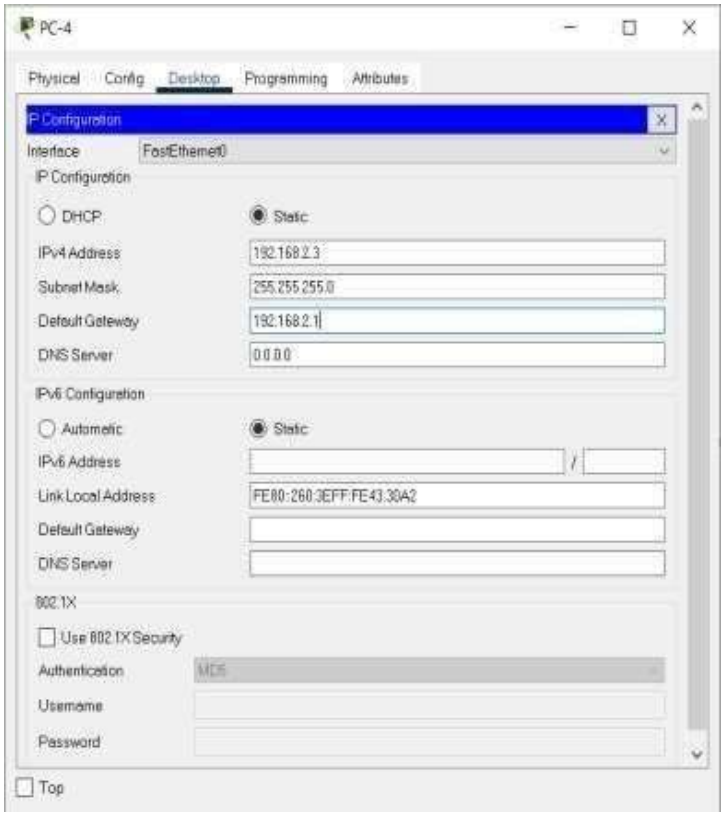

R2
Physical
Config
CLI
Attributes
IOS Command Line Interface
%LINK-5-CHANGED: Interface Serial0/1/0, changed state to down
Router(config-if)#exit
Router(config)#
%LINK-5-CHANGED: Interface Serial0/1/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to up
Router(config)#interface FastEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial0/0/0
Router(config-if)#clock rate 72000
This command applies only to DCE interfaces
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial0/1/0
Router(config-if)#clock rate 72000
This command applies only to DCE interfaces
Router(config-if)#exit
Router(config)#router eigrp 1
Router(config-router)#network 10.0.0.0
Router(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 10.0.0.1 (Serial0/0/0) is up: new adjacency
Router(config-router)#network 192.168.2.0
Router(config-router)#network 20.0.0.0
Router(config-router)#exit
Router(config)#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top

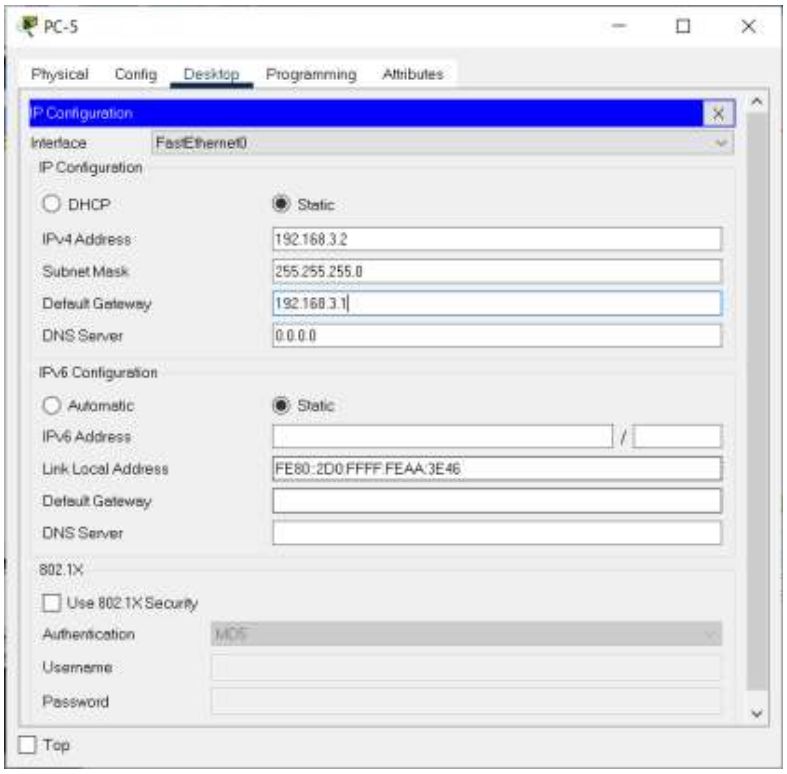

R3
Physical
Config
CLI
Attributes
IOS Command Line Interface
Router(config-if)#exit
Router(config)#interface serial 0/0/0
Router(config-if)#ip address 20.0.0.1 255.0.0.0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
Router(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
Router(config-if)#exit
Router(config)#
Router(config)#interface FastEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial0/0/0
Router(config-if)#clock rate 72000
Router(config-if)#exit
Router(config)#router eigrp 1
Router(config-router)#network 20.0.0.0
Router(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 20.0.0.2 (Serial0/0/0) is up: new adjacency
Router(config-router)#network 192.168.3.0
Router(config-router)#exit
Router(config)#
Ctrl+F6 to exit CLI focus
Copy
Paste
Top

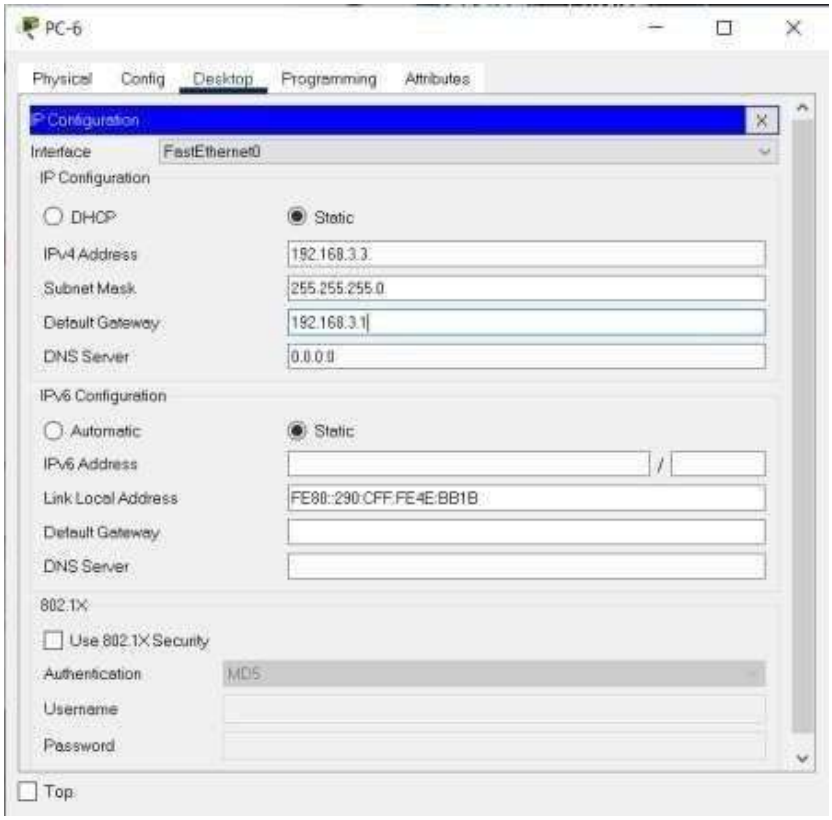
PC configuration:



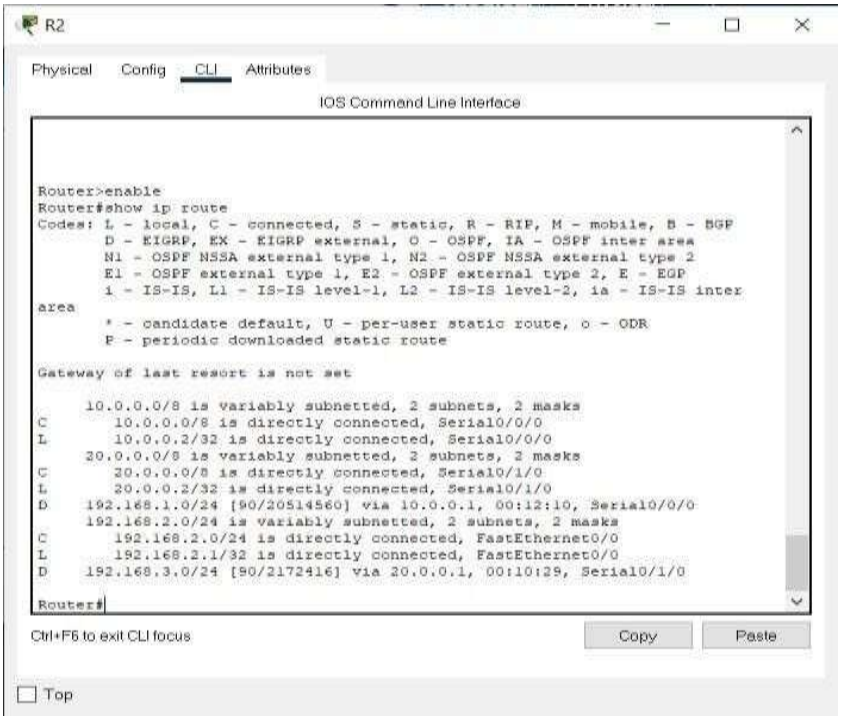

PC-3
Physical
Config
Desktop
Programming
Attributes
IP Configuration
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.2.2
Subnet Mask
255.255.255.0
Default Gateway
192.168.2.1
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address
FE80::2D0:97FF:FE64:A3C4
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top

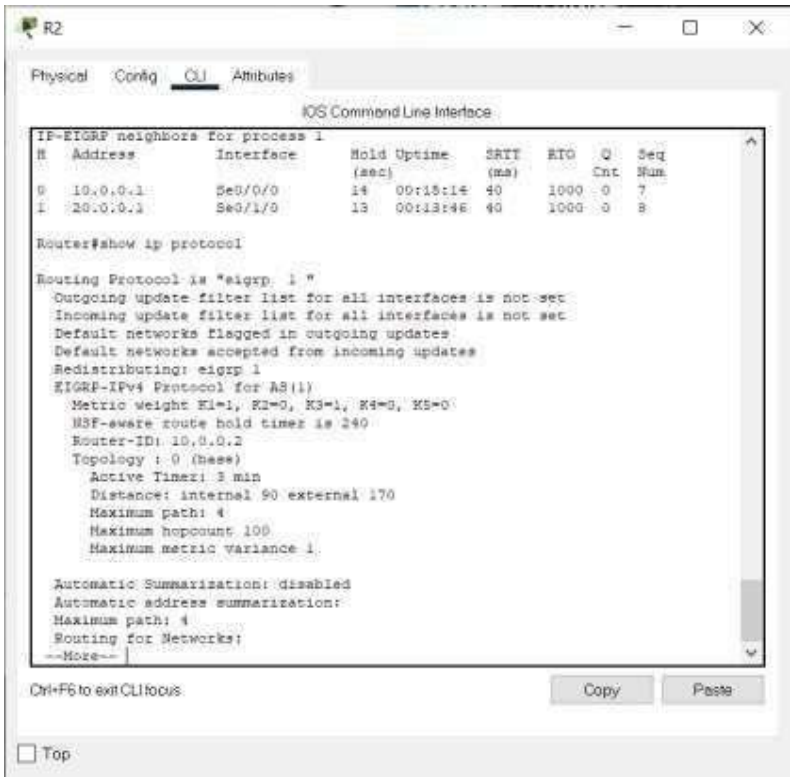

PC-4
Physical
Config
Desktop
Programming
Attributes
IP Configuration
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.2.3
Subnet Mask
255.255.255.0
Default Gateway
192.168.2.1
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address
FE80::260:3EFF:FE43:30A2
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top

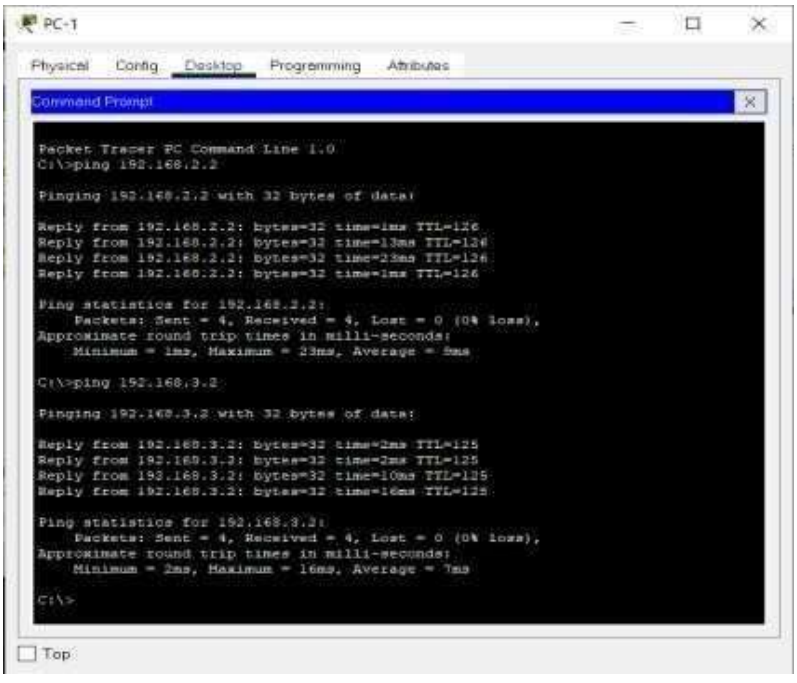

PC-5
Physical
Config
Desktop
Programming
Attributes
IP Configuration
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.3.2
Subnet Mask
255.255.255.0
Default Gateway
192.168.3.1
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address
FE80::2D0:FFFF:FEAA:3E46
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top


PC-6
Physical
Config
Desktop
Programming
Attributes
IP Configuration
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.3.3
Subnet Mask
255.255.255.0
Default Gateway
192.168.3.1
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address
FE80::290:CFF:FE4E:BB1B
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Username
Password
Top

Verification:







RESULTS: Basic EIGRP Configuration is demonstrated.

EXPERIMENT – 11

11. Analysis of network traces using Tcpdump

AIM: Analysis of network traces using Tcpdump

OBJECTIVE: To demonstrate Analysis of network traces using Tcpdump.

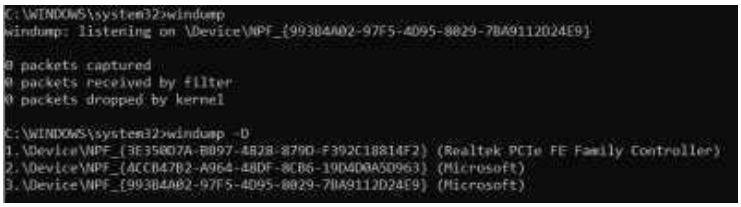
ALGORITHM:

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

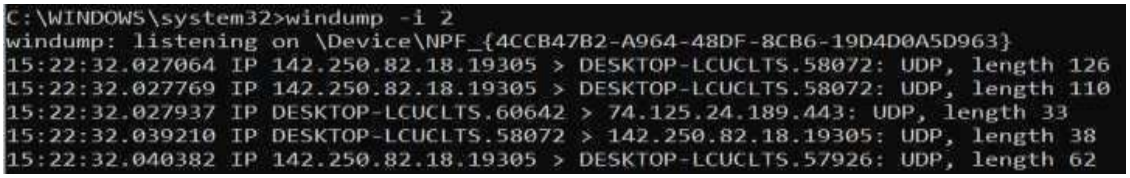
DESCRIPTION AND EXECUTION:

- 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 readfrom a saved packet file rather than to read packets from a network interface. In all cases, only packets that match expression will be processed by windump.

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



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



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

```
C:\WINDOWS\system32>windump -i 2 -c5
windump: listening on \Device\NPF_{4CCB47B2-A964-48DF-8CB6-19D4D0A5D963}
22:29:46.139277 IP relay-e37a4922.net.anydesk.com.80 > DESKTOP-LCUCLTS.55623: . ack 3129932965 win 501
22:29:46.139364 IP DESKTOP-LCUCLTS.55623 > relay-e37a4922.net.anydesk.com.80: . ack 1 win 258
22:29:49.211407 IP ec2-15-206-34-128.ap-south-1.compute.amazonaws.com.443 > DESKTOP-LCUCLTS.55638: . ack 1627103327 win 10
22:29:49.211456 IP DESKTOP-LCUCLTS.55638 > ec2-15-206-34-128.ap-south-1.compute.amazonaws.com.443: . ack 1 win 255
22:29:49.388431 IP DESKTOP-LCUCLTS.55623 > relay-e37a4922.net.anydesk.com.80: . 0:1(1) ack 1 win 258
5 packets captured
6 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:\WINDOWS\system32>windump -i 2 -c5 -w cap.pcap
windump: listening on \Device\NPF_{4CCB47B2-A964-48DF-8CB6-19D4D0A5D963}
5 packets captured
34 packets received by filter
0 packets dropped by kernel

C:\WINDOWS\system32>
```

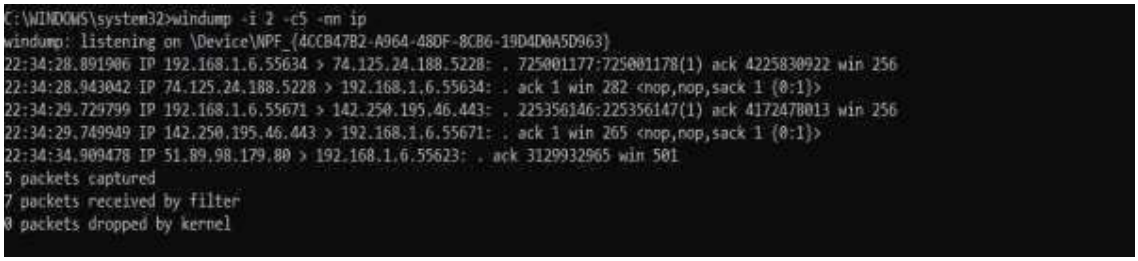
```
C:\WINDOWS\system32>windump -i 2 -nn ip
windump: listening on \Device\NPF_{4CCB47B2-A964-48DF-8CB6-19D4D0A5D963}
22:33:35.517654 IP 192.168.1.3.32925 > 239.255.255.250.1900: UDP, length 125
22:33:35.722293 IP 192.168.1.3.32925 > 239.255.255.250.1900: UDP, length 125
22:33:36.131920 IP 192.168.1.3.32925 > 239.255.255.250.1900: UDP, length 125
22:33:36.557573 IP 192.168.1.6.55663 > 172.217.163.142.443: . 21623370:21623371(1) ack 127570534 win 257
22:33:36.580508 IP 172.217.163.142.443 > 192.168.1.6.55663: . ack 1 win 261 <nop,nop,sack 1 {0:1}>
22:33:36.837495 IP 192.168.1.6.55664 > 172.217.163.142.443: . 1523443714:1523443715(1) ack 3395170178 win
22:33:36.854268 IP 172.217.163.142.443 > 192.168.1.6.55664: . ack 1 win 261 <nop,nop,sack 1 {0:1}>
22:33:38.181928 IP 192.168.1.3.5353 > 224.0.0.251.5353:  10 [3q][|domain]
22:33:39.820172 IP 52.109.8.21.443 > 192.168.1.6.55673: R 901927576:901927576(0) ack 3834849213 win 0
22:33:40.432270 IP 51.89.98.179.80 > 192.168.1.6.55623: . ack 3129932965 win 501
22:33:40.432324 IP 192.168.1.6.55623 > 51.89.98.179.80: . ack 1 win 258
```

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

```
C:\WINDOWS\system32>windump -r cap.pcap
reading from file cap.pcap, link-type EN10MB (Ethernet)
22:30:43.599298 IP DESKTOP-LCUCLTS.55634 > 74.125.24.188.5228: . 725001177:725001178(1) ack 4225830922 win 256
22:30:43.650743 IP 74.125.24.188.5228 > DESKTOP-LCUCLTS.55634: . ack 1 win 282 <nop,nop,sack 1 {0:1}>
22:30:43.706492 IP relay-e37a4922.net.anydesk.com.80 > DESKTOP-LCUCLTS.55623: . ack 3129932965 win 501
22:30:43.706565 IP DESKTOP-LCUCLTS.55623 > relay-e37a4922.net.anydesk.com.80: . ack 1 win 258
22:30:44.301838 IP DESKTOP-LCUCLTS.55688 > 192.168.1.1.53:  54056+ A? android.clients.google.com. (44)

C:\WINDOWS\system32>
```

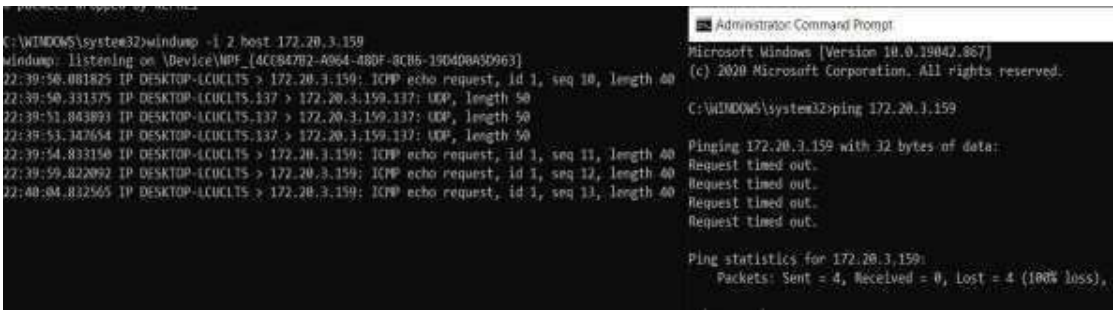
Windump -I -nnip: this filter captures the packets and DNS will be converts in to IP address.

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

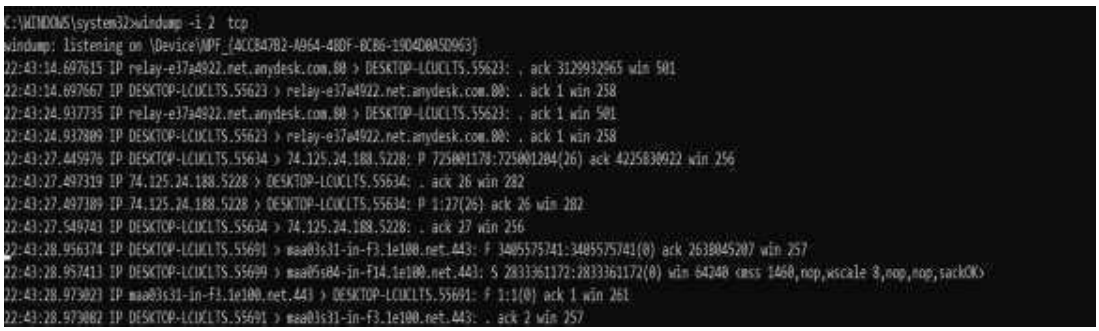


Windump -I port 80: this filter captures the packets whose port number is 80.

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



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



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

EXPERIMENT / PRACTICAL – 12

12. Analysis of network traces using Whireshark

AIM: Analysis of network traces using Whireshark

OBJECTIVE: To demonstrate Analysis of network traces using Whireshark.

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:

oSeveral filters such as ip.src, ip.dst are applied to packets on wireshark and the packets are analyzed.

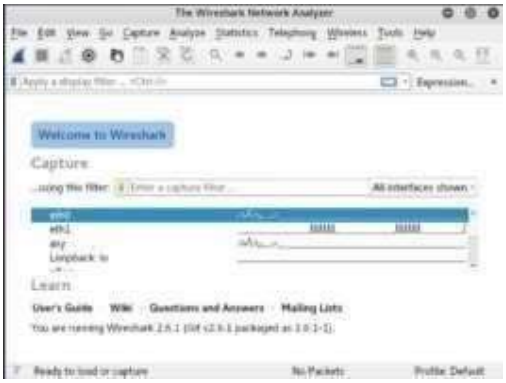
oWireshark is an open-source network protocol analysis software program started by GeraldCombs in1998.

oA global organization of network specialists and software developers support Wiresharkand 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 localnetwork and stores that data for offline analysis.

o Wireshark captures network traffic from Ethernet, Bluetooth, Wireless (IEEE.802.11),Token Ring, Frame Relay connections, and more.

o Wireshark allows you to filter the log either before the capture starts or during analysis, soyou 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 to do that. Clickthe first button on the tool bar, titled—StartCapturingPackets.‖

- **Analyzing Data Packets onWireshark**

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 indicatesthat 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.

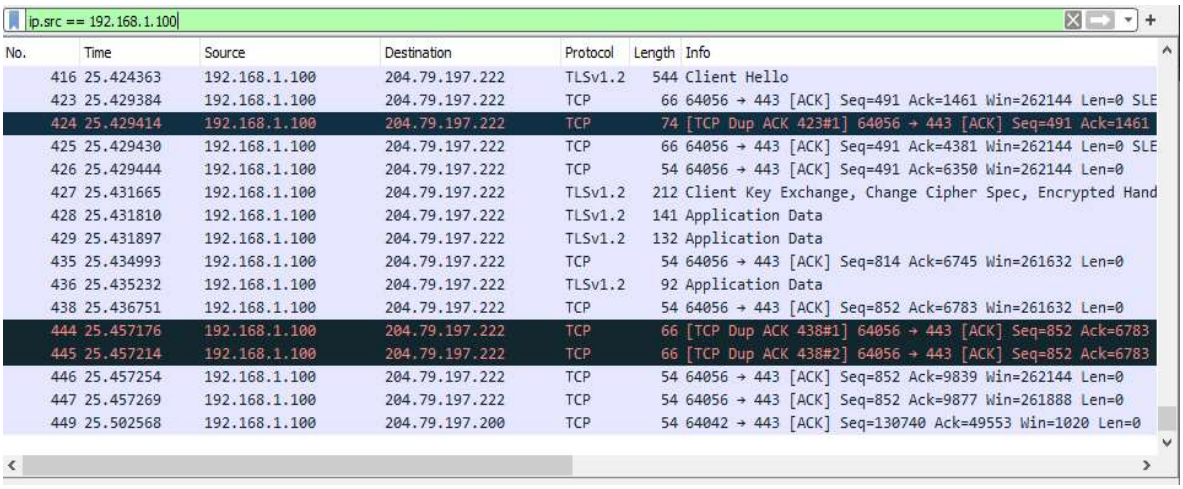
- **Destination**: This is the address of the destination of that packet.
- **Protocol**: This is the type of packet, for example, TCP, DNS, DHCPv6, or ARP.
- **Length**: This column shows you the length of the packet in bytes.
- **Info**: This column shows you more information about the packet contents, and will vary depending on what kind of packet itis.
- Wireshark Capture Filters Commands
- Capture filters limit the captured packets by the filter. Meaning if the packets don‘tmatch 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 net192.168.0.0/24: this filter captures all traffic on the subnet.

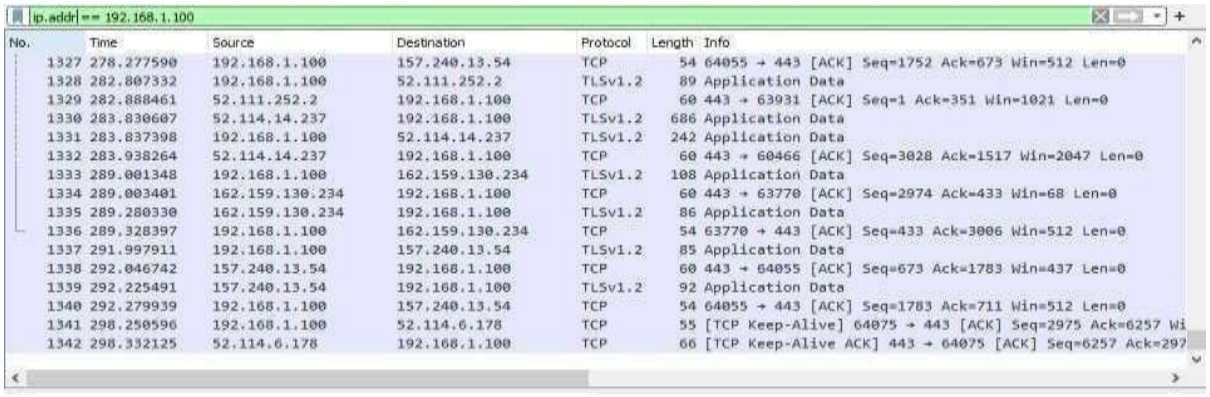
dst host IP-*address*: capture packets sent to the specified host. port 53: capture trafficon port 53only

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

Filters:

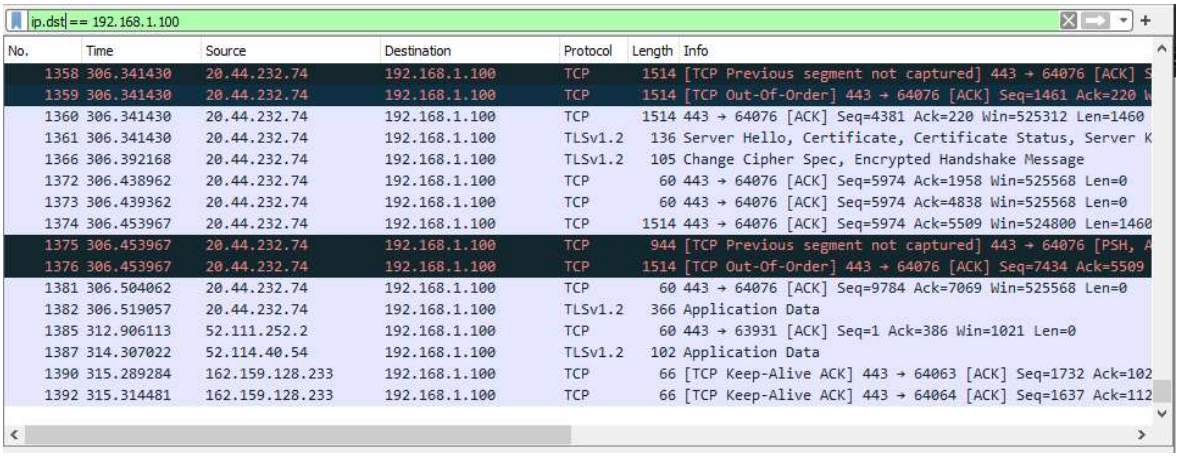
1. ip.src = =_address‘





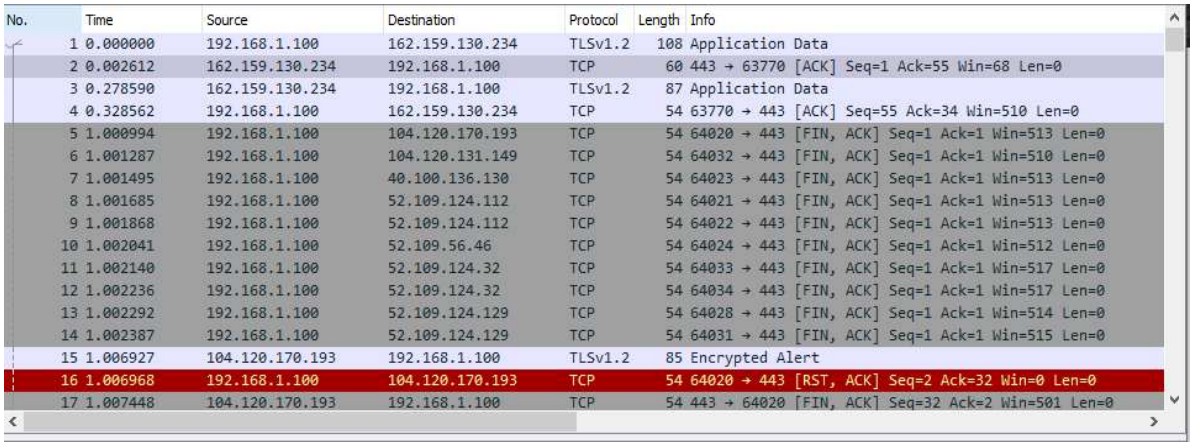
No.	Time	Source	Destination	Protocol	Length	Info
1327	278.277590	192.168.1.100	157.240.13.54	TCP	54	64055 → 443 [ACK] Seq=1752 Ack=673 Win=512 Len=0
1328	282.807332	192.168.1.100	52.111.252.2	TLSv1.2	89	Application Data
1329	282.888461	52.111.252.2	192.168.1.100	TCP	60	443 → 63931 [ACK] Seq=1 Ack=351 Win=1021 Len=0
1330	283.830607	52.114.14.237	192.168.1.100	TLSv1.2	686	Application Data
1331	283.837398	192.168.1.100	52.114.14.237	TLSv1.2	242	Application Data
1332	283.938264	52.114.14.237	192.168.1.100	TCP	60	443 → 60466 [ACK] Seq=3028 Ack=1517 Win=2047 Len=0
1333	289.001348	192.168.1.100	162.159.130.234	TLSv1.2	108	Application Data
1334	289.003401	162.159.130.234	192.168.1.100	TCP	60	443 → 63770 [ACK] Seq=2974 Ack=433 Win=68 Len=0
1335	289.280330	162.159.130.234	192.168.1.100	TLSv1.2	86	Application Data
1336	289.328397	192.168.1.100	162.159.130.234	TCP	54	63770 → 443 [ACK] Seq=433 Ack=3006 Win=512 Len=0
1337	291.997911	192.168.1.100	157.240.13.54	TLSv1.2	85	Application Data
1338	292.046742	157.240.13.54	192.168.1.100	TCP	60	443 → 64055 [ACK] Seq=673 Ack=1783 Win=437 Len=0
1339	292.225491	157.240.13.54	192.168.1.100	TLSv1.2	92	Application Data
1340	292.279939	192.168.1.100	157.240.13.54	TCP	54	64055 → 443 [ACK] Seq=1783 Ack=711 Win=512 Len=0
1341	298.250596	192.168.1.100	52.114.6.178	TCP	55	[TCP Keep-Alive] 64075 → 443 [ACK] Seq=2975 Ack=6257 Wi
1342	298.332125	52.114.6.178	192.168.1.100	TCP	66	[TCP Keep-Alive ACK] 443 → 64075 [ACK] Seq=6257 Ack=297

2. ip.addr = =_address‘
3. ip.dst == _address‘



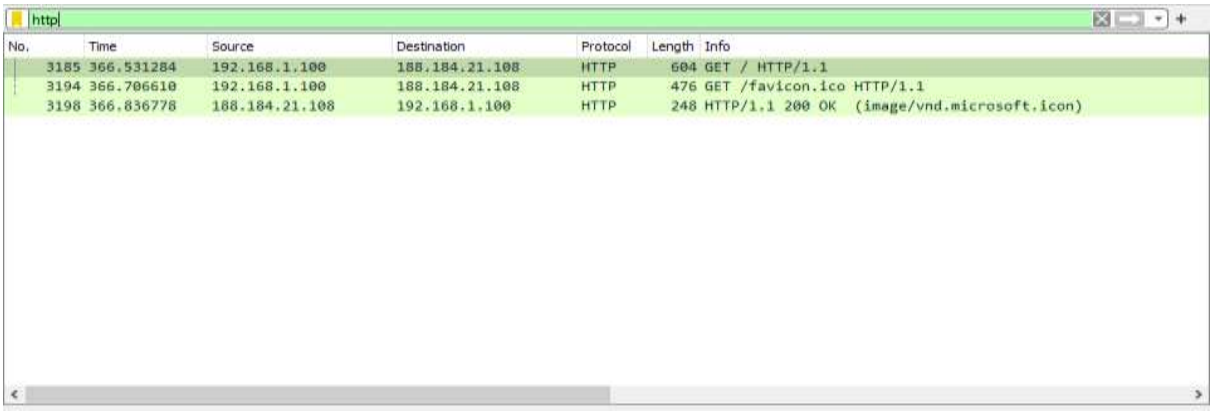
No.	Time	Source	Destination	Protocol	Length	Info
1358	306.341430	20.44.232.74	192.168.1.100	TCP	1514	[TCP Previous segment not captured] 443 → 64076 [ACK] S
1359	306.341430	20.44.232.74	192.168.1.100	TCP	1514	[TCP Out-Of-Order] 443 → 64076 [ACK] Seq=1461 Ack=220 W
1360	306.341430	20.44.232.74	192.168.1.100	TCP	1514	443 → 64076 [ACK] Seq=4381 Ack=220 Win=525312 Len=1460
1361	306.341430	20.44.232.74	192.168.1.100	TLSv1.2	136	Server Hello, Certificate, Certificate Status, Server K
1366	306.392168	20.44.232.74	192.168.1.100	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
1372	306.438962	20.44.232.74	192.168.1.100	TCP	60	443 → 64076 [ACK] Seq=5974 Ack=1958 Win=525568 Len=0
1373	306.439362	20.44.232.74	192.168.1.100	TCP	60	443 → 64076 [ACK] Seq=5974 Ack=4838 Win=525568 Len=0
1374	306.453967	20.44.232.74	192.168.1.100	TCP	1514	443 → 64076 [ACK] Seq=5974 Ack=5509 Win=524800 Len=1460
1375	306.453967	20.44.232.74	192.168.1.100	TCP	944	[TCP Previous segment not captured] 443 → 64076 [PSH, A
1376	306.453967	20.44.232.74	192.168.1.100	TCP	1514	[TCP Out-Of-Order] 443 → 64076 [ACK] Seq=7434 Ack=5509
1381	306.504062	20.44.232.74	192.168.1.100	TCP	60	443 → 64076 [ACK] Seq=9784 Ack=7069 Win=525568 Len=0
1382	306.519057	20.44.232.74	192.168.1.100	TLSv1.2	366	Application Data
1385	312.906113	52.111.252.2	192.168.1.100	TCP	60	443 → 63931 [ACK] Seq=1 Ack=386 Win=1021 Len=0
1387	314.307022	52.114.40.54	192.168.1.100	TLSv1.2	102	Application Data
1390	315.289284	162.159.128.233	192.168.1.100	TCP	66	[TCP Keep-Alive ACK] 443 → 64063 [ACK] Seq=1732 Ack=102
1392	315.314481	162.159.128.233	192.168.1.100	TCP	66	[TCP Keep-Alive ACK] 443 → 64064 [ACK] Seq=1637 Ack=112

4. tcp

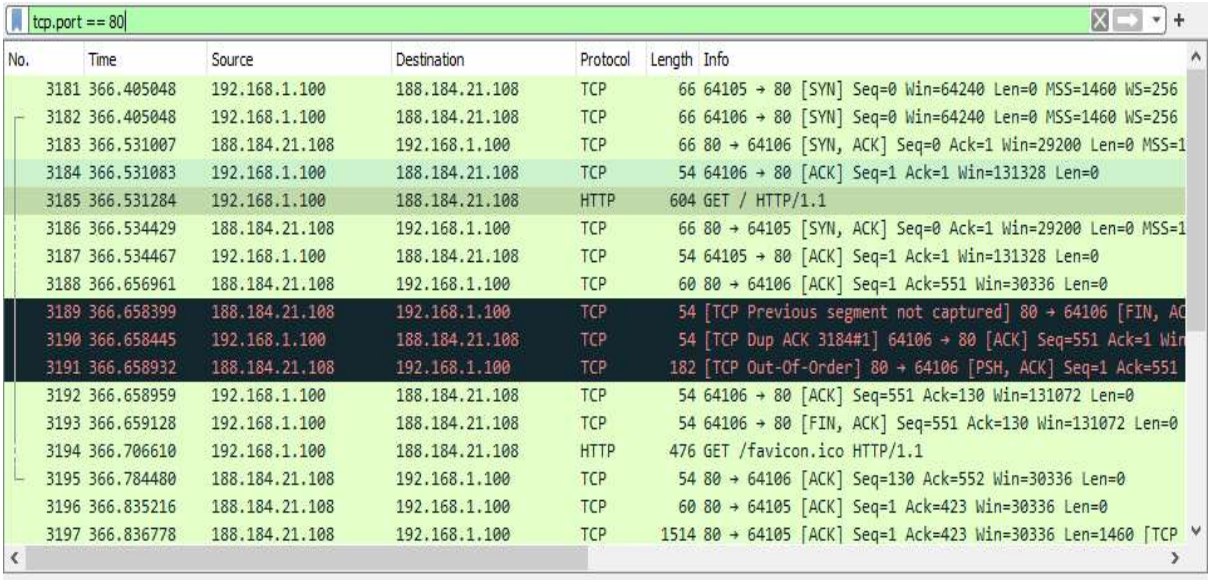


No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.100	162.159.130.234	TLSv1.2	108	Application Data
2	0.002612	162.159.130.234	192.168.1.100	TCP	60	443 → 63770 [ACK] Seq=1 Ack=55 Win=68 Len=0
3	0.278590	162.159.130.234	192.168.1.100	TLSv1.2	87	Application Data
4	0.328562	192.168.1.100	162.159.130.234	TCP	54	63770 → 443 [ACK] Seq=55 Ack=34 Win=510 Len=0
5	1.000994	192.168.1.100	104.120.170.193	TCP	54	64020 → 443 [FIN, ACK] Seq=1 Ack=1 Win=513 Len=0
6	1.001287	192.168.1.100	104.120.131.149	TCP	54	64032 → 443 [FIN, ACK] Seq=1 Ack=1 Win=510 Len=0
7	1.001495	192.168.1.100	40.100.136.130	TCP	54	64023 → 443 [FIN, ACK] Seq=1 Ack=1 Win=513 Len=0
8	1.001685	192.168.1.100	52.109.124.112	TCP	54	64021 → 443 [FIN, ACK] Seq=1 Ack=1 Win=513 Len=0
9	1.001868	192.168.1.100	52.109.124.112	TCP	54	64022 → 443 [FIN, ACK] Seq=1 Ack=1 Win=513 Len=0
10	1.002041	192.168.1.100	52.109.56.46	TCP	54	64024 → 443 [FIN, ACK] Seq=1 Ack=1 Win=512 Len=0
11	1.002140	192.168.1.100	52.109.124.32	TCP	54	64033 → 443 [FIN, ACK] Seq=1 Ack=1 Win=517 Len=0
12	1.002236	192.168.1.100	52.109.124.32	TCP	54	64034 → 443 [FIN, ACK] Seq=1 Ack=1 Win=517 Len=0
13	1.002292	192.168.1.100	52.109.124.129	TCP	54	64028 → 443 [FIN, ACK] Seq=1 Ack=1 Win=514 Len=0
14	1.002387	192.168.1.100	52.109.124.129	TCP	54	64031 → 443 [FIN, ACK] Seq=1 Ack=1 Win=515 Len=0
15	1.006927	104.120.170.193	192.168.1.100	TLSv1.2	85	Encrypted Alert
16	1.006968	192.168.1.100	104.120.170.193	TCP	54	64020 → 443 [RST, ACK] Seq=2 Ack=32 Win=0 Len=0
17	1.007448	104.120.170.193	192.168.1.100	TCP	54	443 → 64020 [FIN, ACK] Seq=32 Ack=2 Win=501 Len=0

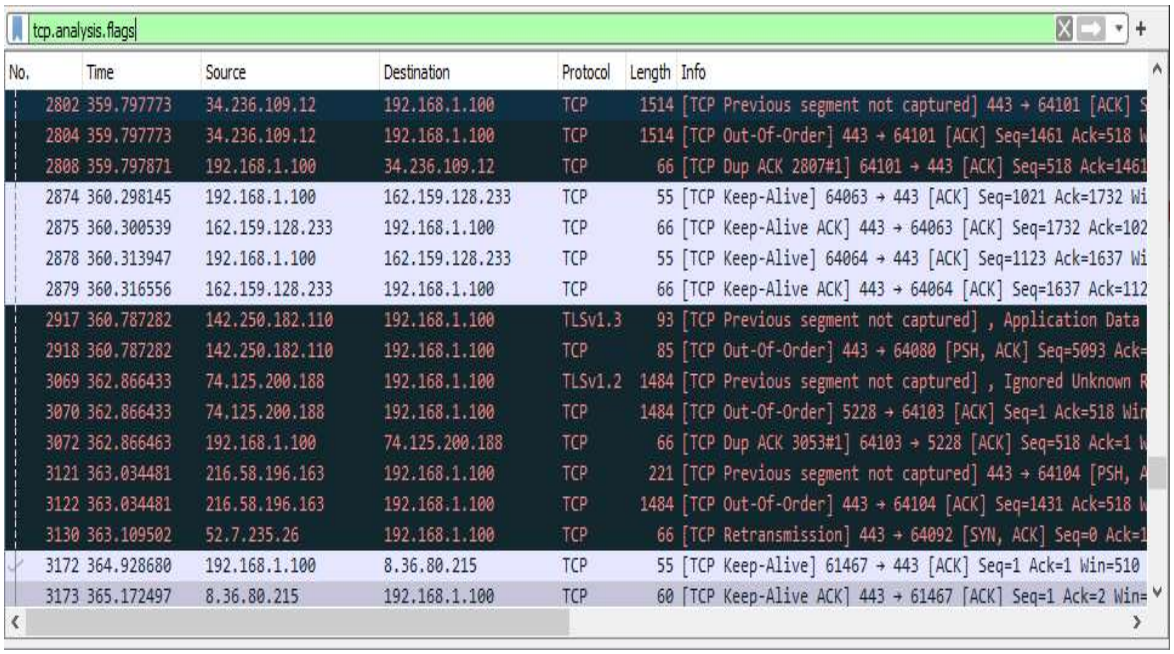
5. http



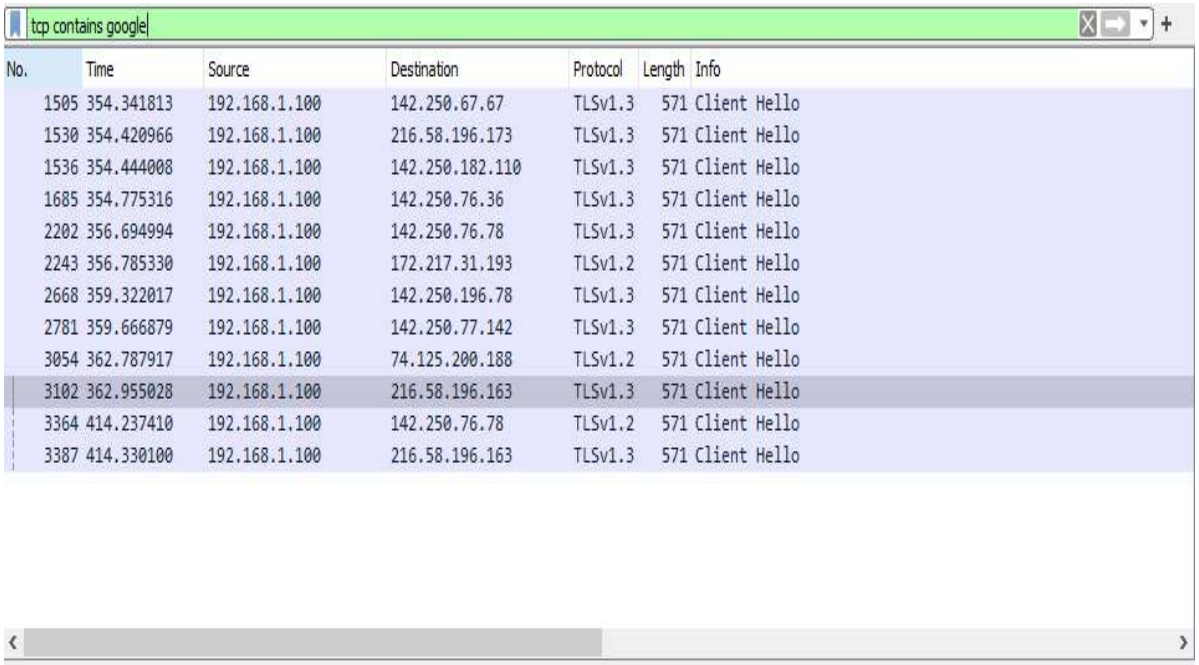
4. tcp.port



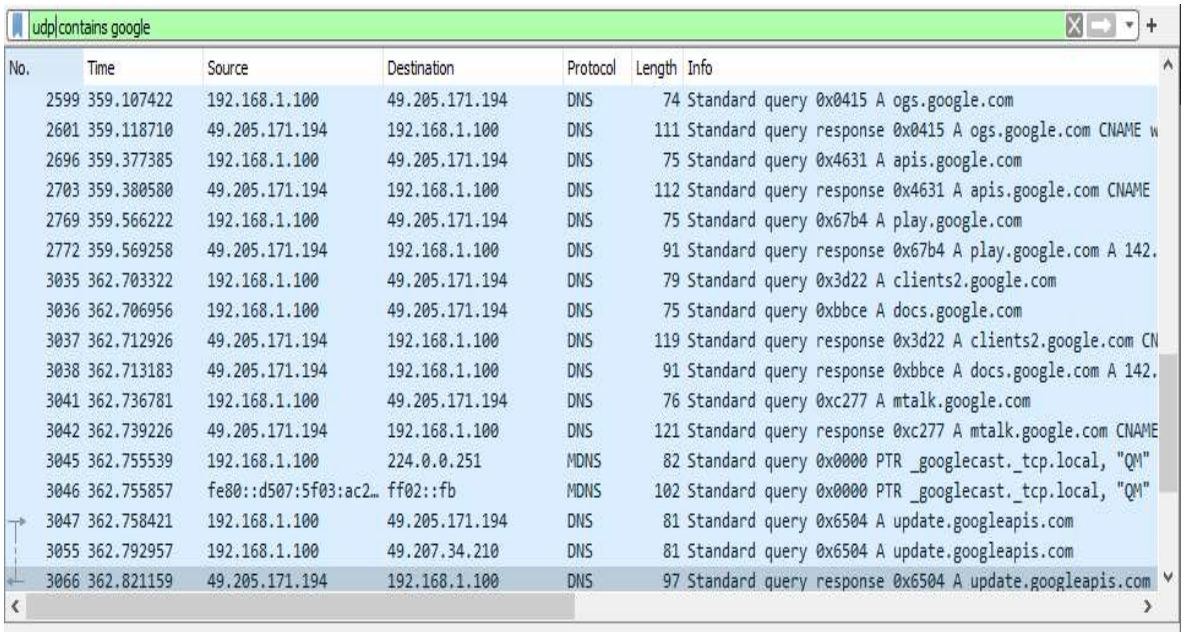
5. tcp.analysis.flags



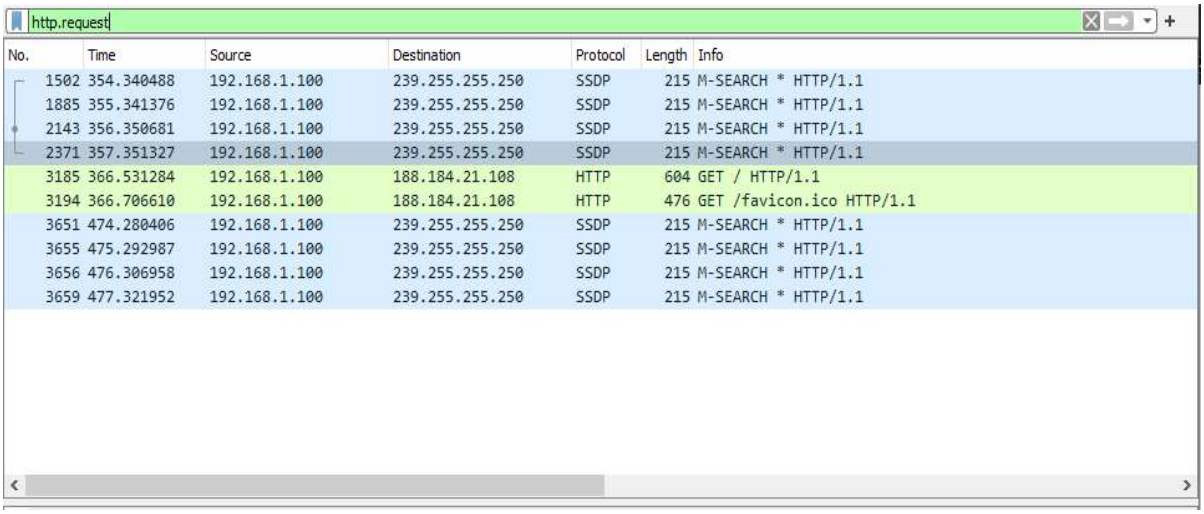
7. tcp contains



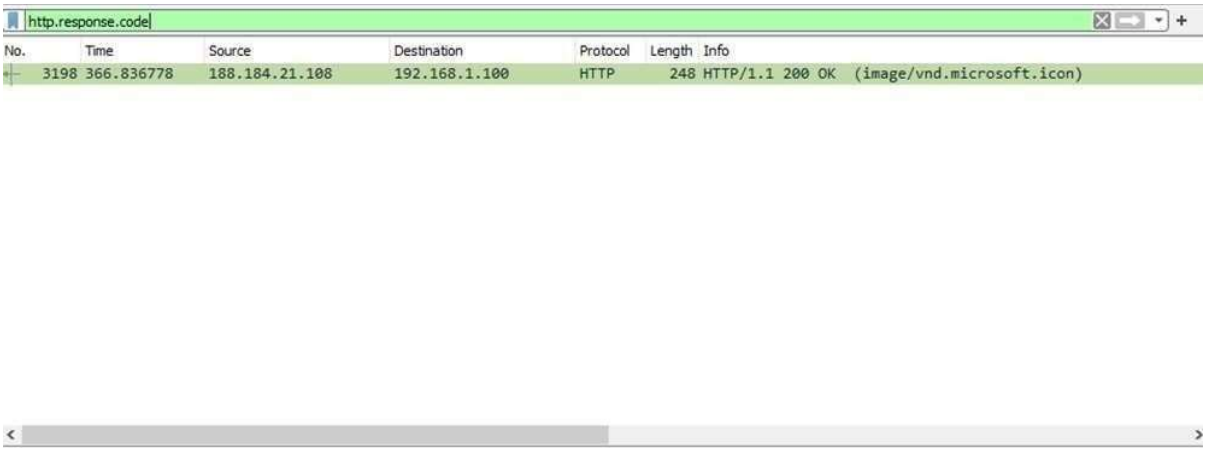
8. udp contains



9. http.request



10. http.response.code



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