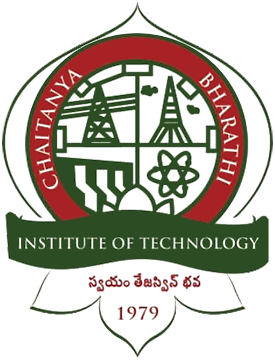
**CHAITANYA BHARATHI INSTITUTE OF**

**TECHNOLOGY**

**Gandipet, Hyderabad-506075**



**CERTIFICATE**

This is to certify that this is bonafide record of the word done by Mr. **Mohammed Faiz** bearing Roll no. **1601-18-733-095** of **3rd Year** B.Tech/B.E **Computer Science & Engineering** branch **6TH Semester Cse-2** Semester in the Laboratory **DATA COMMUNICATION AND NETWORKS LAB**  during The academic Year **2020-2021**

Number of experiments conducted: **9**

**Staff Member in Charge**

**External Examiner Internal Examiner**

## Experiment-1 Study of Network media, cables, and devices and Cable Construction

### NETWORK MEDIA ( TRANSMISSION MEDIA ) :

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 :

1. Guided media (wired)
2. 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 :

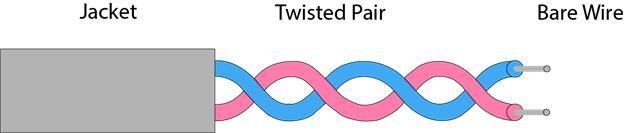
### Twisted pair cable :

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

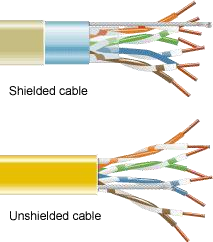
* + It is more expensive as compared to UTP and coaxial cable.
  + It has a higher attenuation rate.

### UnShielded 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



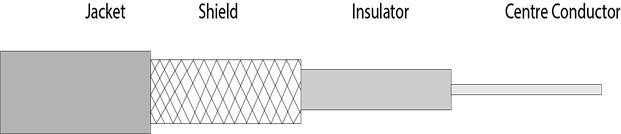
### Coaxial cable :

It has an outer plastic covering containing 2 parallel conductors each

having a separate insulated protection cover. The coaxial cable transmits information in 2 modes : **1)** Baseband Mode - dedicated cable bandwidth

**2)** Broadband mode - bandwidth is split into separate ranges

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



### Advantages :

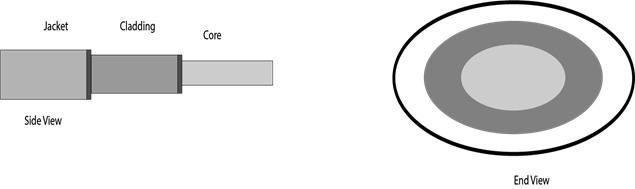
1. High Bandwidth
2. Better noise immunity
3. Easy to install and expand
4. Inexpensive

### Optical Fibre :

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. Fibre 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 Fibre optic cable:

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

1. **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.
2. **Jacket:** The protective coating consisting of plastic is known as a jacket. The main purpose of a jacket is to preserve the fibre strength, absorb shock and extra fibre protection.

### Advantages of Optical Fibre

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

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

### Disadvantages of Optical Fibre

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

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

### UNGUIDED MEDIA

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 :

### Radiowaves :

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.

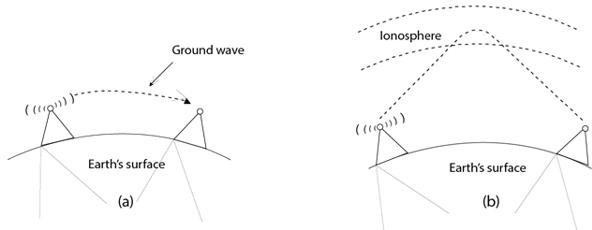
The frequency of radio waves about 30 hertz (Hz) to 300 gigahertz (GHz) and like all other electromagnetic waves radio waves travel at the speed of light in vacuum.

### 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.



### 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

### 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 neighbors. 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.

### NETWORK DEVICES

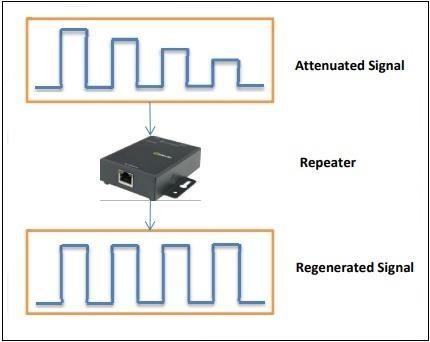
Hardware devices that are used to connect computers, printers, fax machines and other electronic devices to a network are called **network devices**. These devices transfer data in a fast, secure and correct way over same or different networks. Network devices may be inter-network or intra-network. Some 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.

### 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.



### 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.

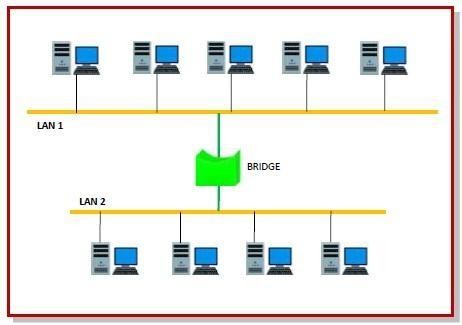


### Bridge

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.



### Two layer Switch

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). 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.

### Three layer Switch

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

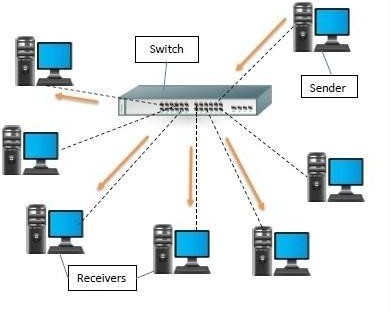
* + Comes with 24 Ethernet ports, but no WAN interface.
  + Acts as a switch to connect devices within the same subnet.
  + Switching algorithm is simple and is the same for most routed protocols.
  + Performs on tw[o OSI layers](http://techgenix.com/network-troubleshooting-osi/) — layer 2 and layer 3.

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

[Layer 2 switches](https://www.techopedia.com/definition/8011/layer-2-switch) 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.

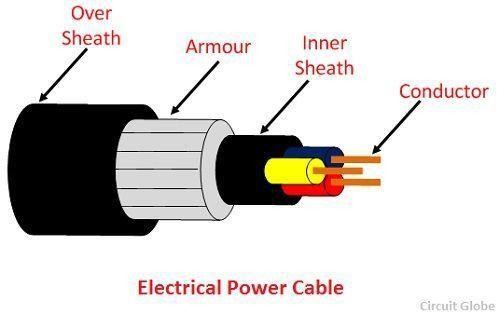
One option was to use a router instead of a switch, but then routers are slower than switches, so this could lead to slower performance.



### 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 more costly as compared to aerial cable for the same voltage which is one of the main draws back of electrical power cable.

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



### Conductor

Coppers and aluminum 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 aluminum are used to make a power cable.

For a conductor having more than three wires, the wire is arranged around a center 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 nonmigratory dielectric. Also, such type of dielectric material has good dielectric strength, low power loss, and low thermal resistance.

### Inner Sheath

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 aluminum 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 aluminum sheath is used because it has better-bending properties, reduced thickness, and lesser weight.

### Protective Covering

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

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

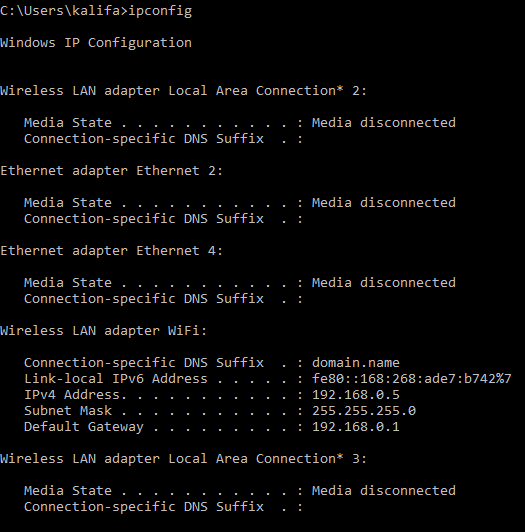
### Experiment 2 -Demonstration of basic network commands/utilities

**1)Ipconfig**

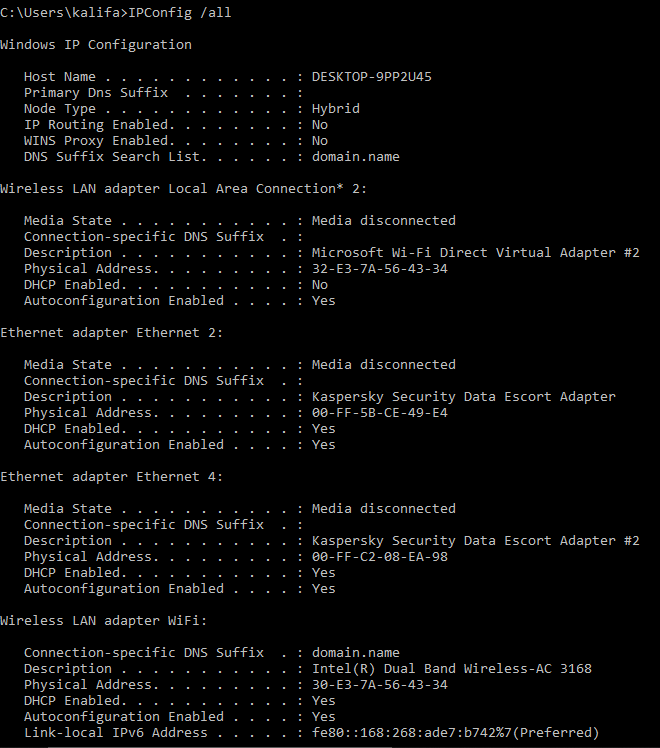
ipconfig (Internet Protocol configuration) is among the most common networking tool that allows you to query and show current TCP/IP (Transmission Control Protocol/Internet Protocol) network configuration.

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.



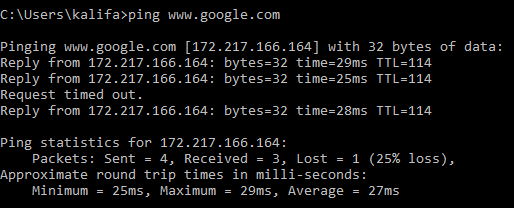
* IPConfig /all – Displays additional information for all network adapters



### Ping:

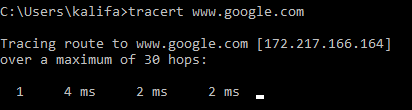
Verifies IP-level connectivity to another TCP/IP computer by sending Internet Control Message Protocol (ICMP) Echo Request messages. The receipt of corresponding Echo Reply messages are displayed, along with round-trip times. Ping is the primary TCP/IP command used to troubleshoot connectivity, reachability,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



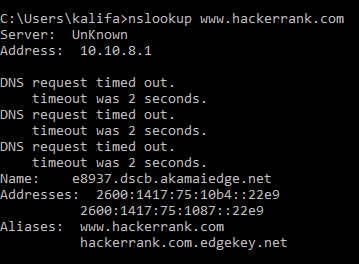
### Tracert

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



### nslookup :

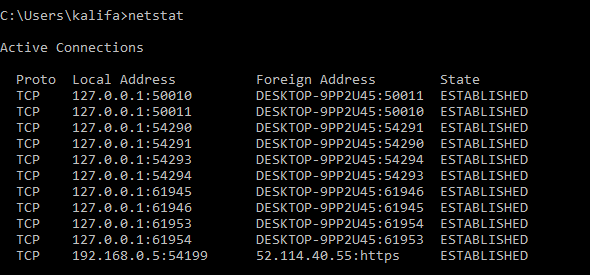
The nslookup (Name Server Lookup) tool can show valuable details to troubleshoot and resolve DNS-related issues. You can use this command to display the default DNS name and address of the local device, determine the domain name of an IP address or the name servers for a specific node.



### netstat:

The netstat (Network Statistics) tool displays statistics for all network connections. It allows you to understand open and connected ports to monitor and troubleshoot networking problems for Windows 10 and apps.

When using the netstat tool, you can list active network connections and listening ports. You can view network adapter and protocols statistics. You can even display the current routing table and much more.

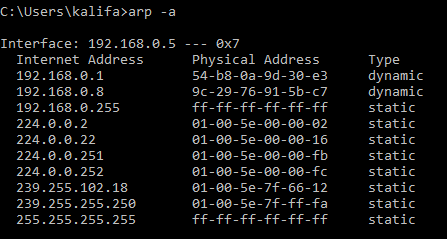


### arp:

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'



### 7)net

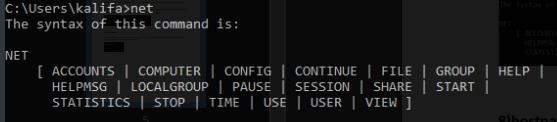
Used for: Displaying available Net switches Command to enter: net

The net command is definitely a versatile one, allowing you to manage many different aspects of a network and its settings such as network shares, users and print jobs, as just a few examples.

Running just net won’t do much, but it will present you with a list of all the switches that are available.

These include accounts to set password and logon requirements, file to show a list of open files

and sessions to list, or even disconnect, sessions on the network.



### hostname

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



**Aim:**

# DCCN LAB 3

## PC Network Configuration

To configure network on a computer

**Description:**

**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

**IP Address:**

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

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

**IPv4 Classes:**

There are 5 classes of IPv4 addresses:

1. 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 (27-2) and 16777214 hosts (224-2).

1. 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 (214) Network addresses and 65534 (216-2) Host addresses.

1. 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 is 255.255.255.x.

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

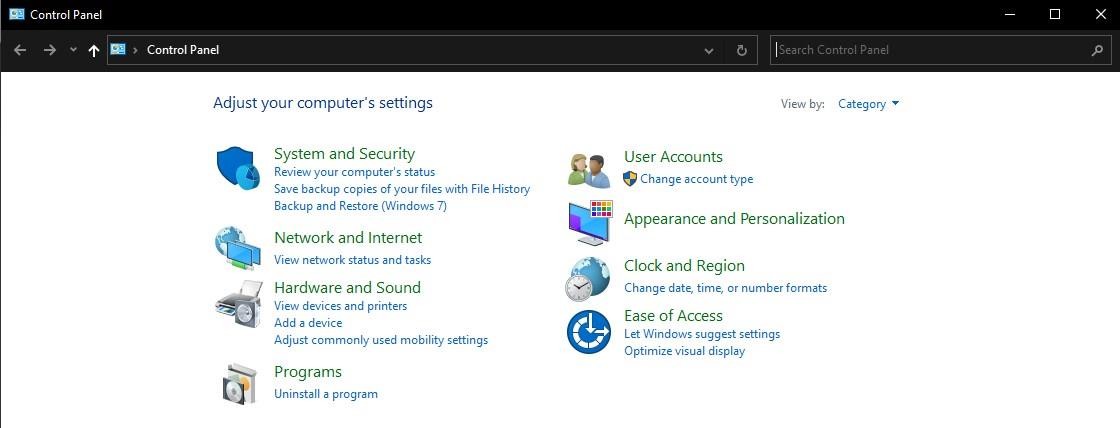
1. Class D:

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

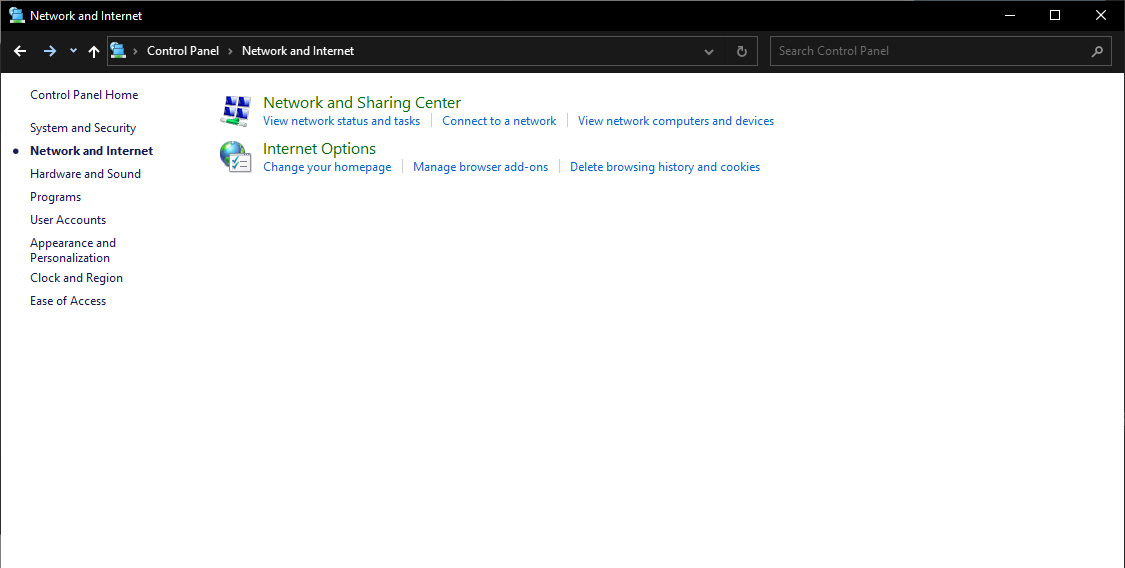
Class D has IP address range from 224.0.0.0 to 239.255.255.255. Class D is reserved for Multicasting. In multicasting data is not destined for a particular host, that is why there is no need to extract host address from the IP address, and Class D does not have any subnet mask.

1. Class E:

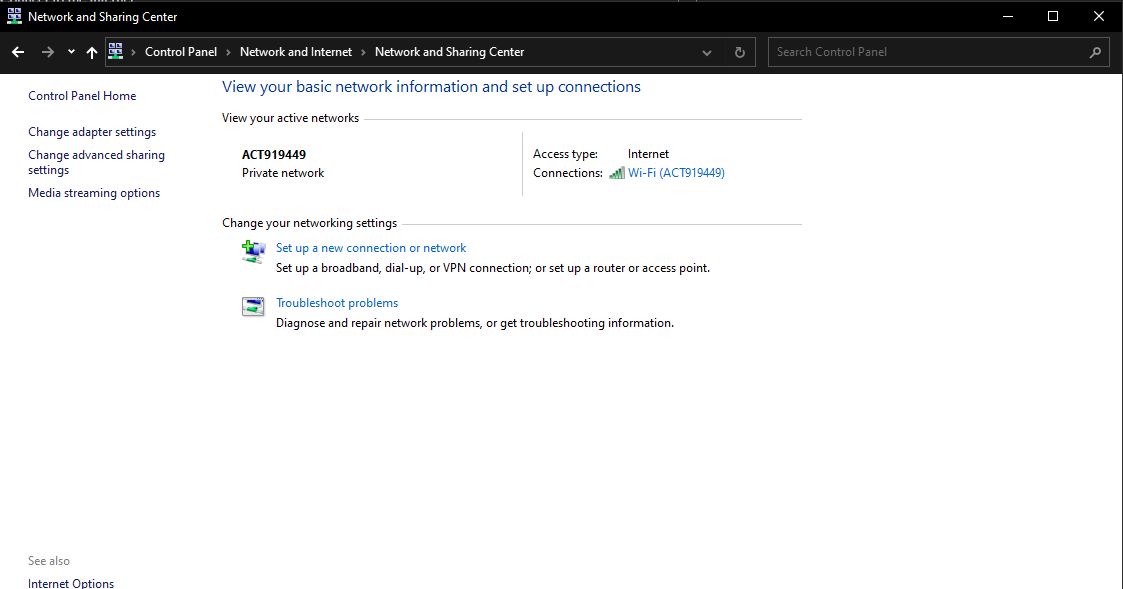
This IP Class is reserved for experimental purposes only for R&D or Study. IP addresses in this class ranges from 240.0.0.0 to 255.255.255.254. Like Class D, this class too is not equipped with any subnet mask.

Network Configuration: Open Control Panel

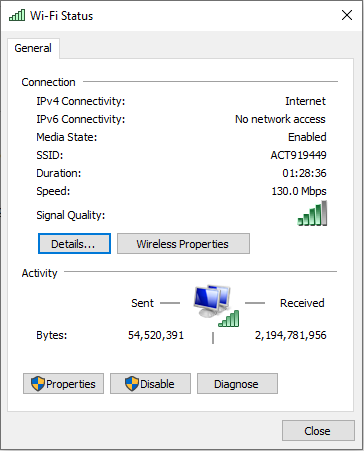
Open Network and Internet



Open Network and Sharing Center

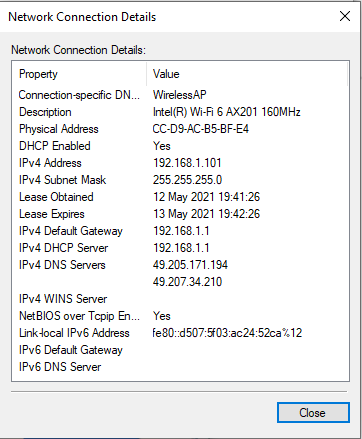


Go to Connection (Wi-Fi or LAN)

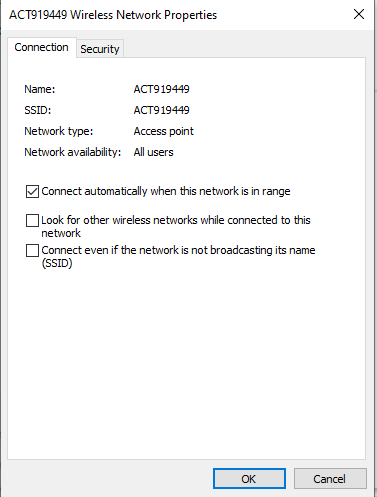


Details:

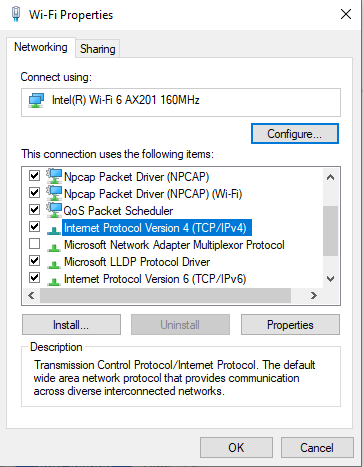
The IP address, Subnet mask and default gateways can be obtained here.



Wireless Properties:

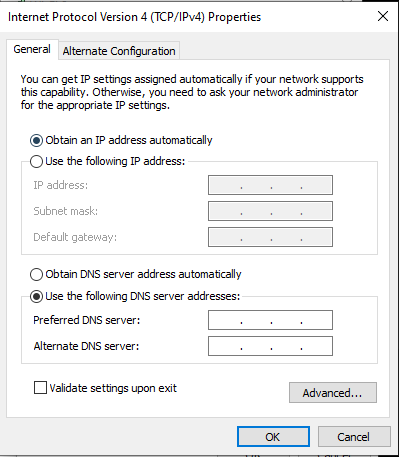


Wi-Fi Properties:



Internet Protocol Version 4 (TCP/IPv4):

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



**Result:**

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

# DCCN LAB 4

## Switch Based Network

**Aim:**

To build a switch based network using cisco packet tracer.

**Description:**

Resources: 1 Switch, 2 PCs, 1 Router.

The devices are connected in a star topology:



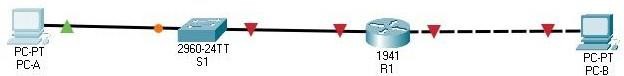
**Algorithm:**

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

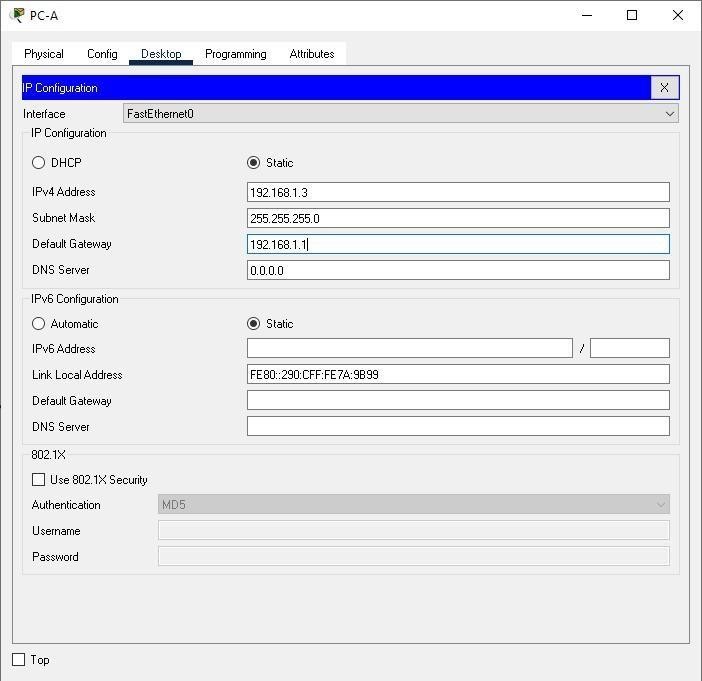
Laying out required devices:

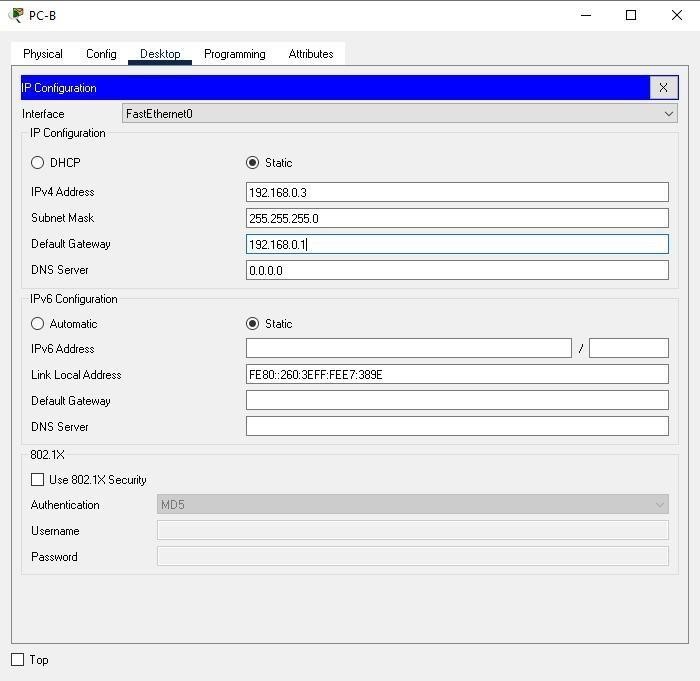


Connecting the devices using cables:

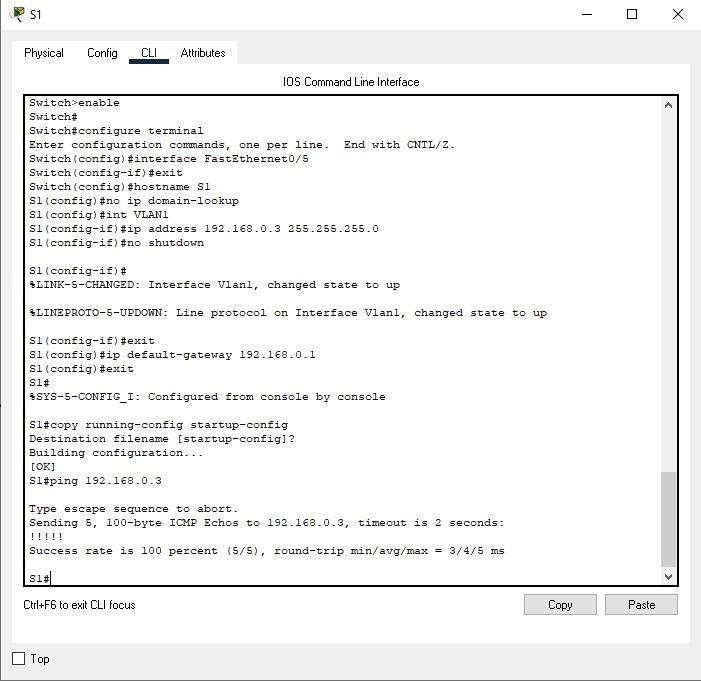


Configuring PC-A and PC-B:

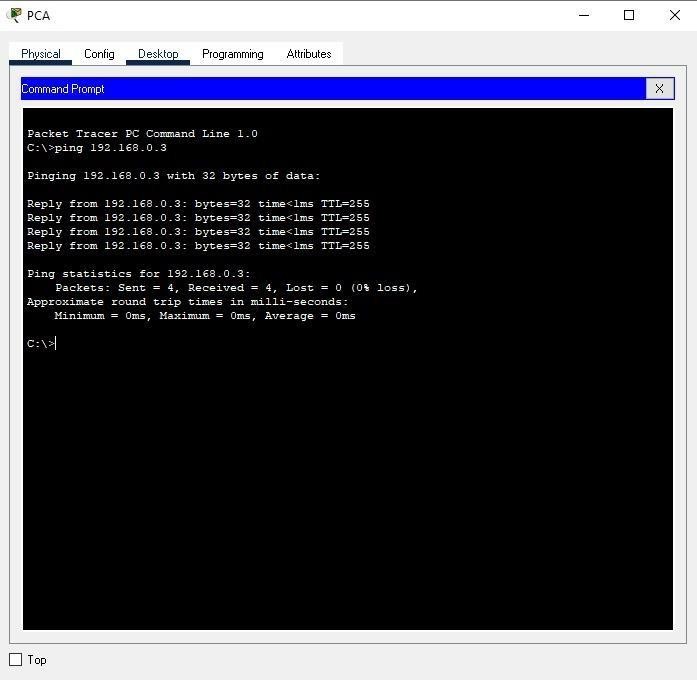




Configuring Switch S1:



Checking ping from PCA to PCB:



**Result:**

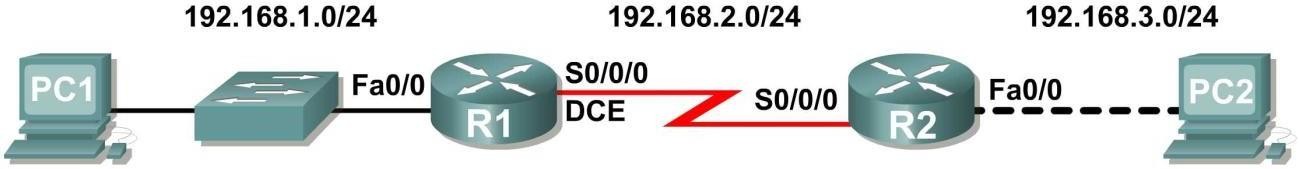
After the configuration and connection of all devices, the ping is successful from PC-A to PC-B.

**EXPERIMENT-5**

**Aim:**

To build a Basic Router Configuration based network using cisco packet tracer.

**Description:**

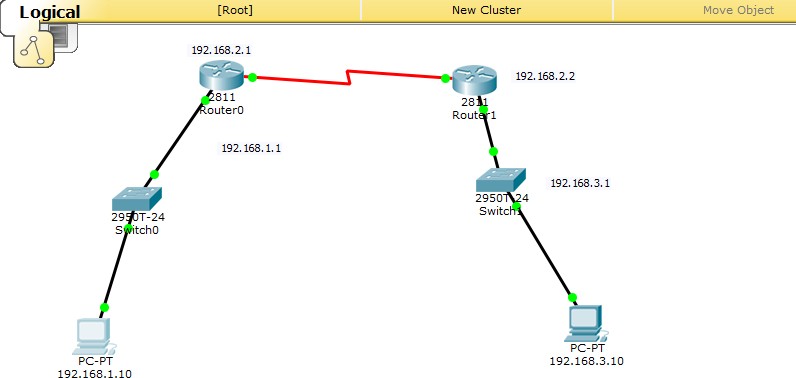
Resources: 2 Switch, 2 PCs, 2 Router.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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 |

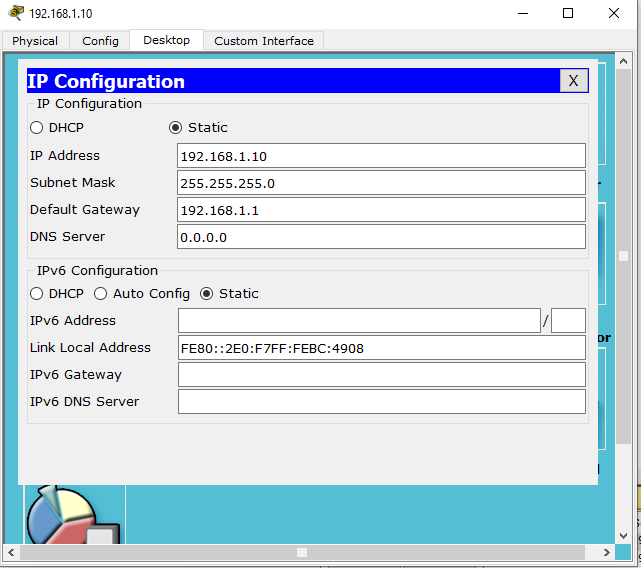
**Algorithm:**

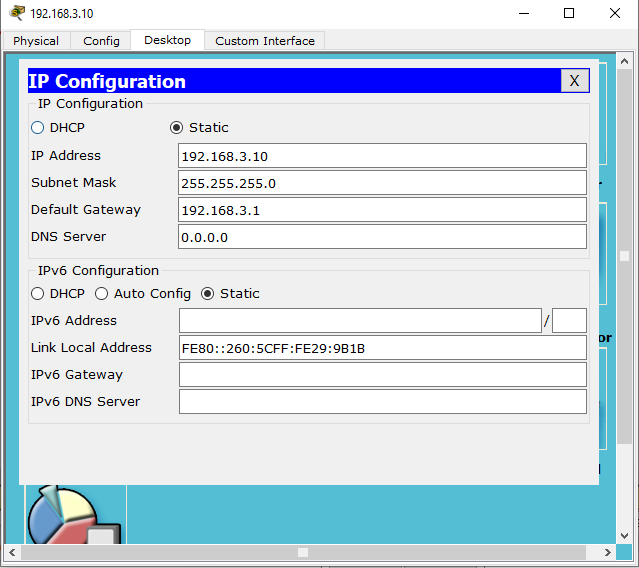
1. Start
2. Setup the Topology and initialize devices
3. Configure Devices and router and verify connectivity
4. Display Device information
5. End

**Connecting the devices using cables:**

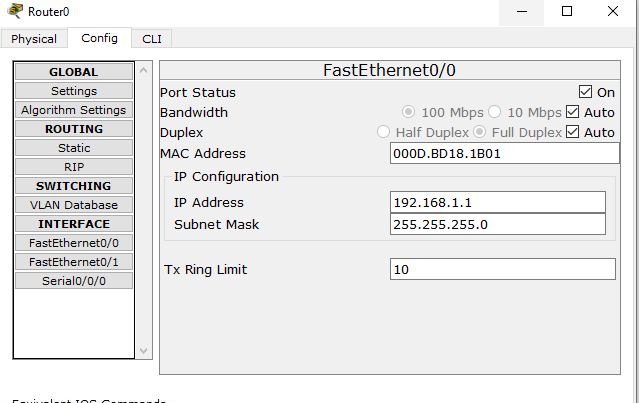
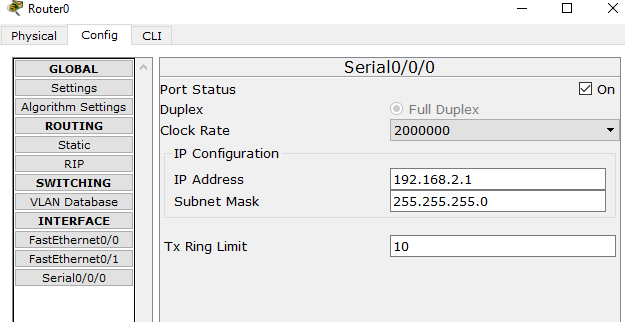


### Configuring PC-A and PC-B:



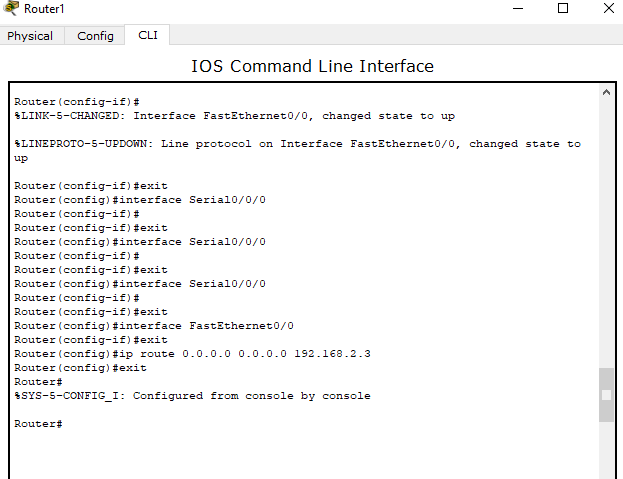
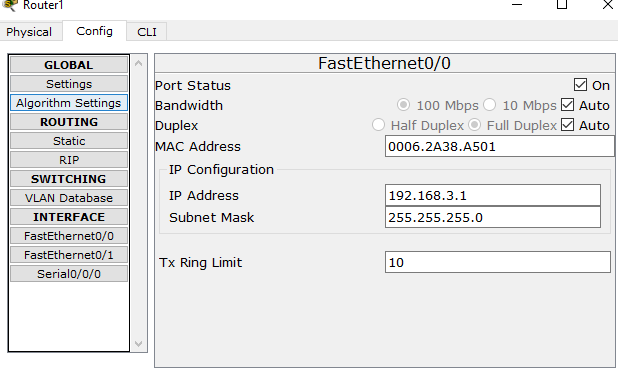
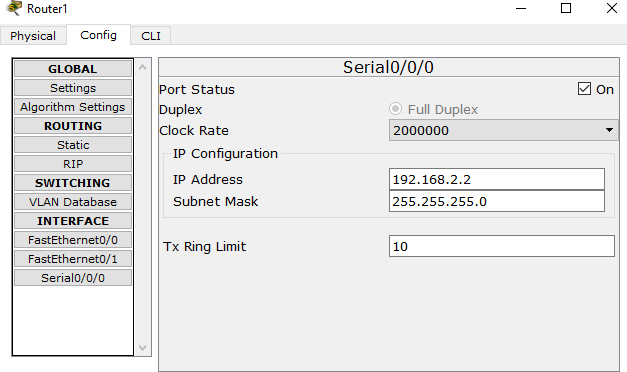


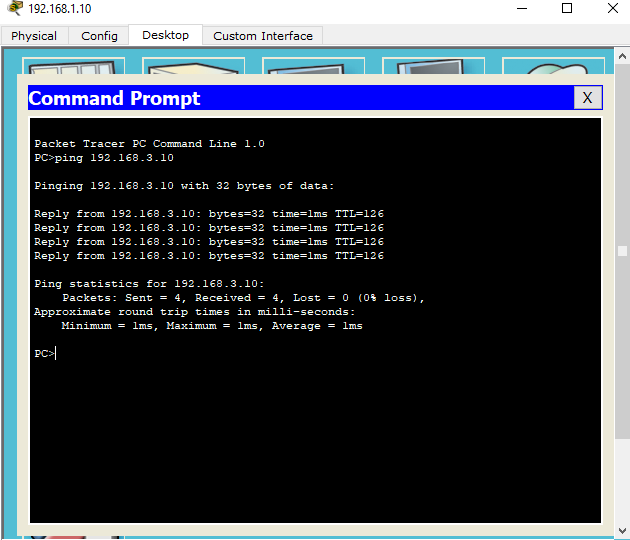
**Configuring router 1:**





**Configuring router 2:**



**Checking ping from PCA to PCB:**

**Result:**

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

### EXPERIMENT-6

**Aim:**

To ***Configure OSPF in a Single Area***

**Description:**

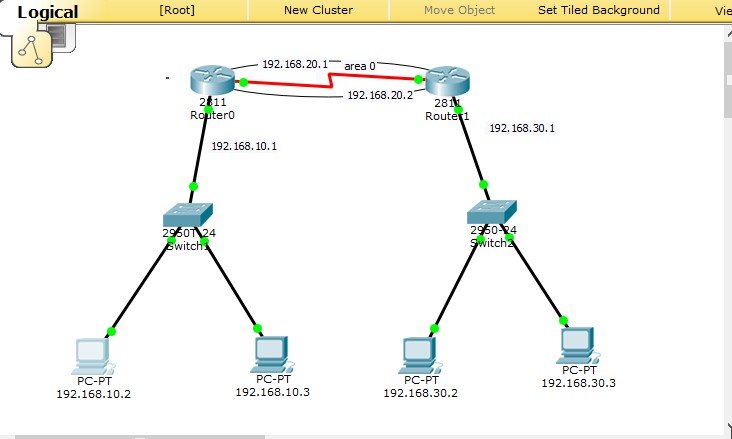
* + OSPF is a link-state routing protocol. Link-state protocols use the shortest path first (SPF) algorithm to populate the routing table. OSPF shares information with every router in the network.
  + OSPF is considered a difficult protocol to configure and requires a thorough understanding of terms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

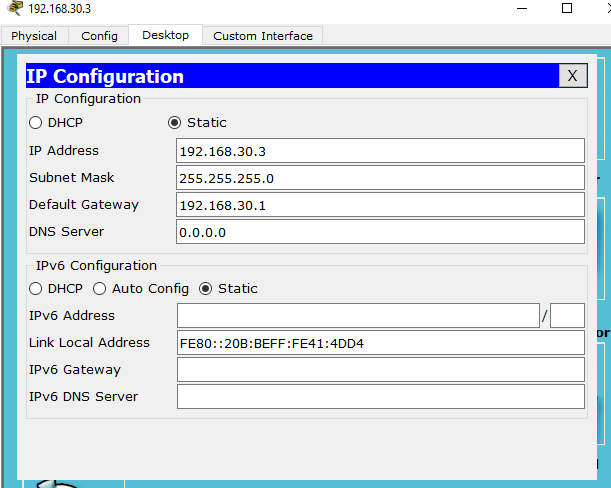
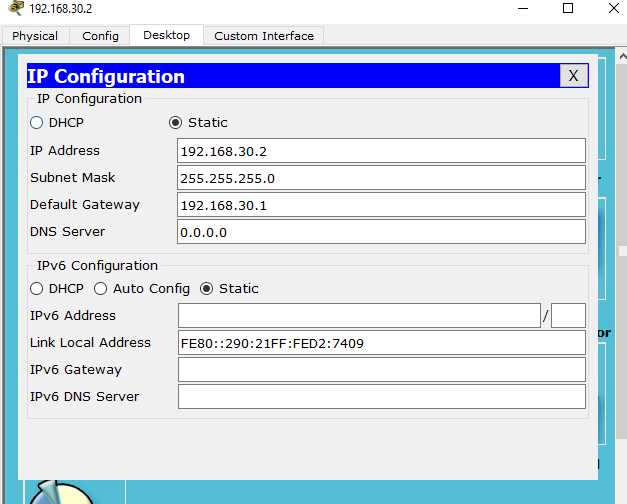
**Resources**: 2 Switch, 4 PCs, 2 Router

**Algorithm:**

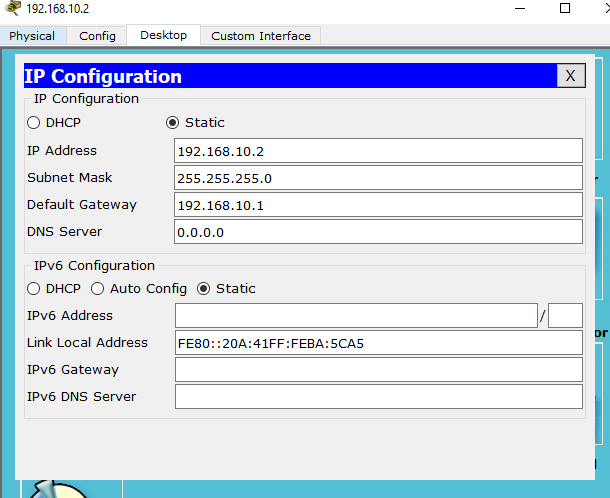
1. Start
2. Setup the Topology and initialize devices
3. Configure Devices and verify connectivity
4. Display Device information
5. End

### Connecting the devices using cables:



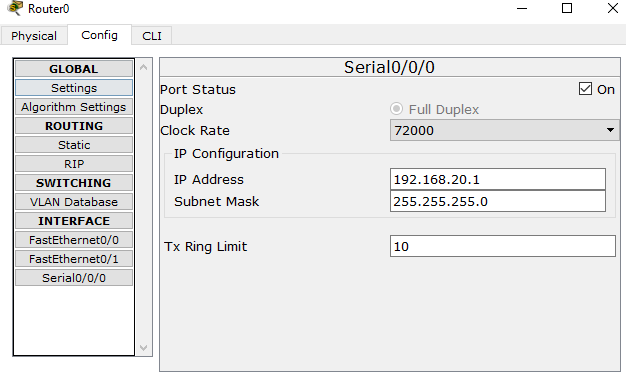


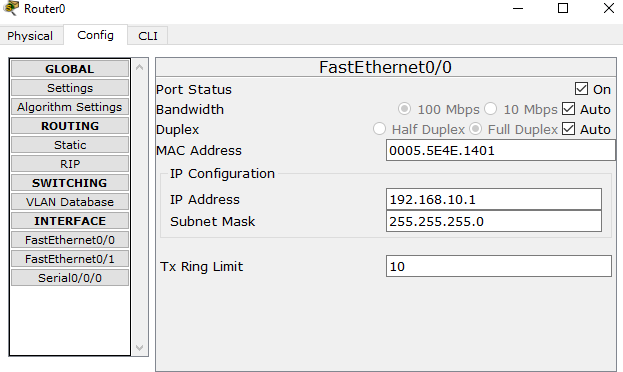
Configuring PC’s:



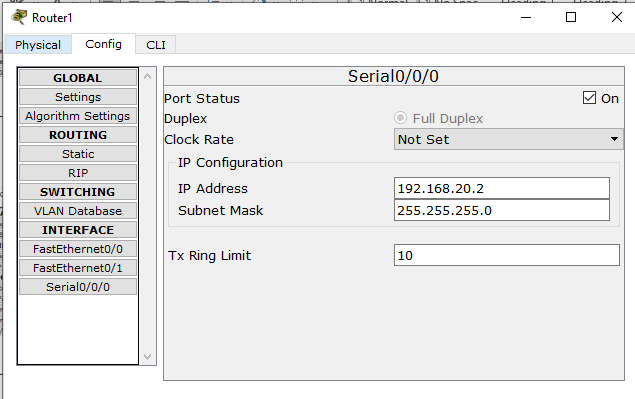
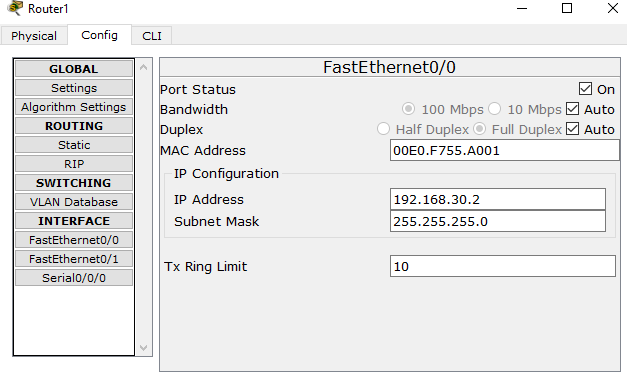
### Configuring Routers:

Router 0: Config

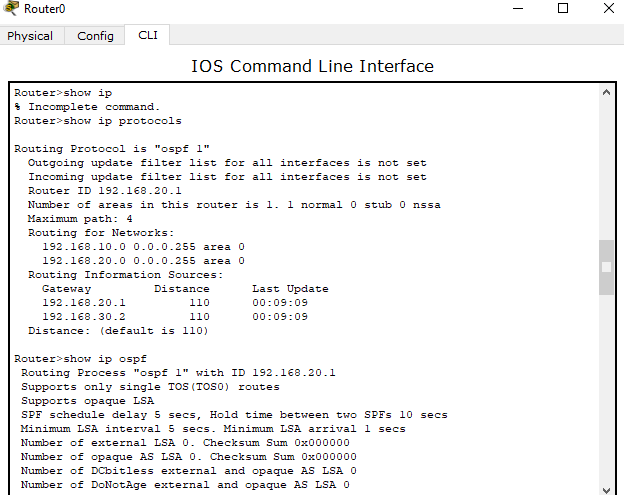
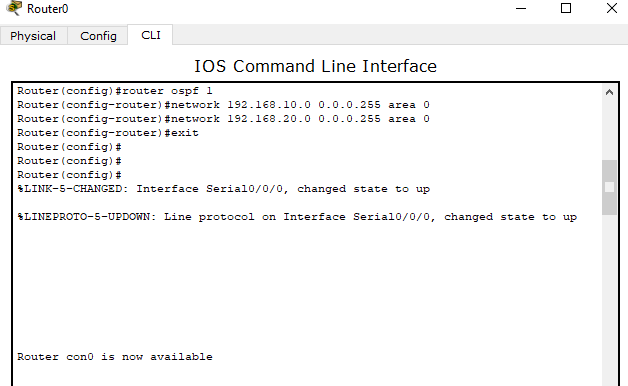




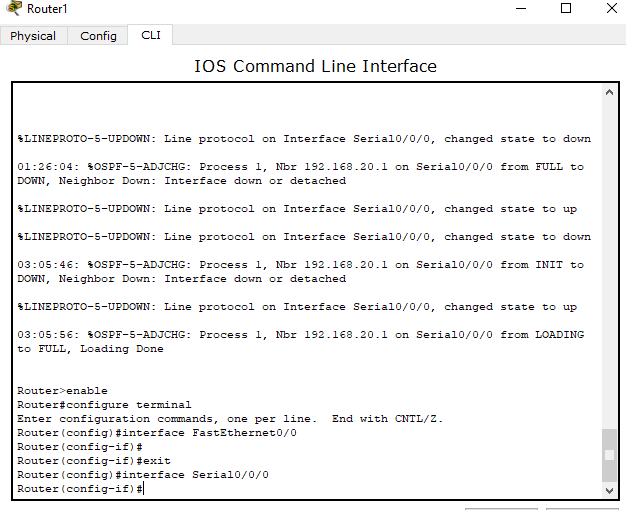
Router 1: config



Router 0: CLI



Router 1: CLI



### Checking ping

**Result:**

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

**EXPERIMENT-7 EIGRP CONFIG**

**AIM**: To configure EIGRP.

**OBJECTIVE**: To display EIGRP with a process ID of 1.

**DESCRIPTION**: Enhanced Interior Gateway Routing Protocol is an interior gateway protocol suited for many different topologies and media. In a well-designed network, EIGRP scales well and provides extremely quick convergence times with minimal network traffic. It has very low usage of network resources during normal operations; only hello packets are transmitted on a stable network.

When a change occurs, only routing table changes are propagated, not the entire routing table; this reduces the load on the routing protocol itself places on the network. It has rapid convergence times for changes in the network topology (in some situations convergence can be almost instantaneous). It is an enhanced distance vector protocol, relying on the Diffused Update Algorithm (DUAL) to calculate the shortest path to a destination within a network.

**ALGORITHM**:

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

**COMMANDS & OUTPUT:**

*Setup topological network:*

Graphical user interface, diagram, application

Description automatically generated

*Router configuration:*

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated Graphical user interface, text, application

Description automatically generated Graphical user interface, application

Description automatically generated Graphical user interface, application

Description automatically generated Graphical user interface, application

Description automatically generated Graphical user interface, text

Description automatically generated Graphical user interface, text, application

Description automatically generated Graphical user interface, text

Description automatically generated

*PC configuration:*

Graphical user interface, text, application, email

Description automatically generated Graphical user interface, application

Description automatically generated Graphical user interface, application, email

Description automatically generated Graphical user interface, text, application, email

Description automatically generated Graphical user interface, application

Description automatically generated Graphical user interface, text, application, email

Description automatically generated

*Verification:*

Graphical user interface, text

Description automatically generated

Text

Description automatically generatedGraphical user interface, text

Description automatically generated

Graphical user interface, text

Description automatically generated

## EXPERIMENT- 08

**AIM: Analysis of network traces using windump.**

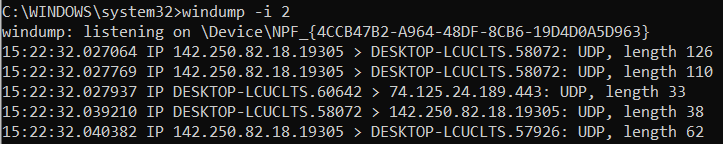
**DESCRIPTION:** windump prints out a description of the contents of packets on a network interface that match the Boolean expression. It can also be run with the **-w** flag, which causes it to save the packet data to a file for later analysis, and/or with the **-r** flag, which causes it to read from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

by windump.

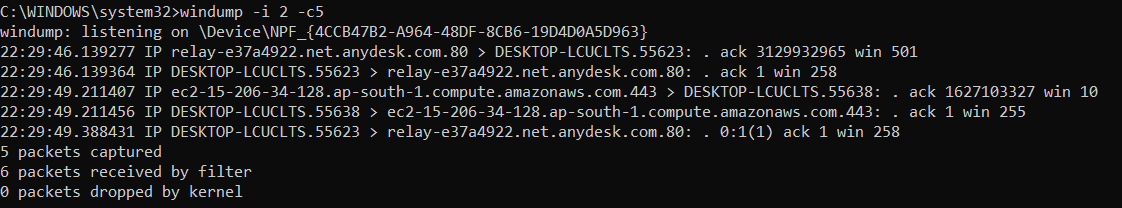
**Windump -D**: displays the list of interfaces which are connected to the system. We can use any of the interfaces by specifying its number.



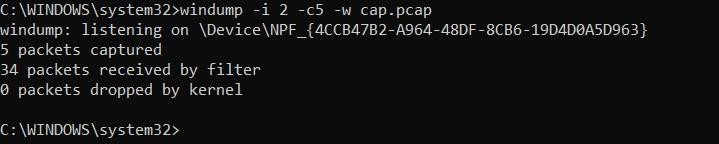
**Windump -i 2**: By giving this command we will get the list of packets captured from the interface 2.



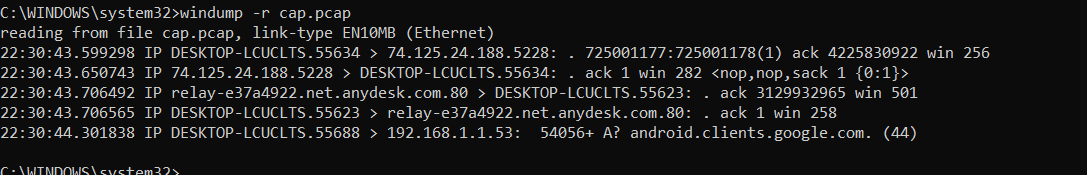
**Windump -i 2 -c5**: By giving this command we will get the list of filters captured from the interface 2 but only limited to 5 filters since, we mentioned count as 5 (-c5).



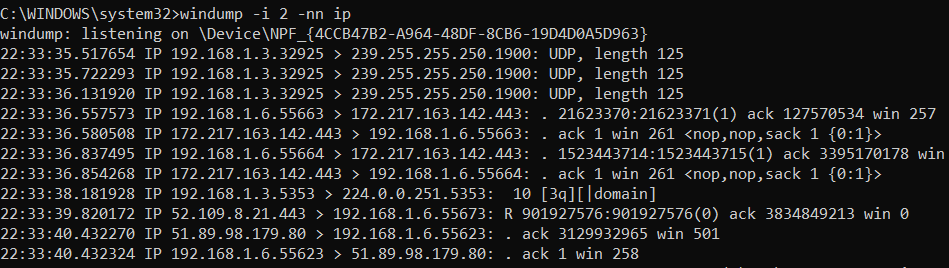
**Windump -I 2 -c5 -w cap.pcap**: this filter is used to write in to a file in which the file name is cap.pcap .but its limited to only 5 packets.



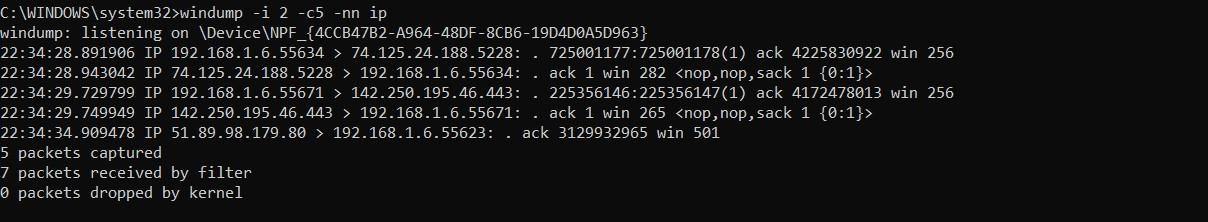
**Windump -I 2 -r cap.pcap**: this filter is used to read from a file in which the file name is cap.pcap .but its limited to only 5 packets.



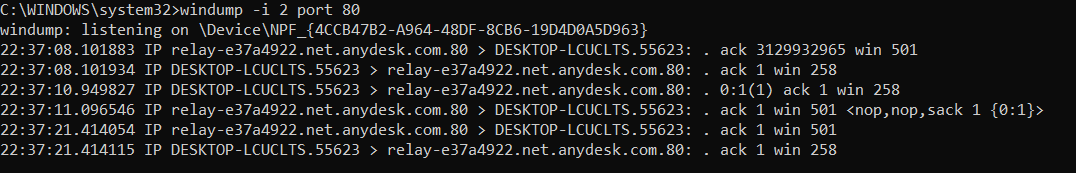
**Windump -I -nn ip**: this filter captures the packets and DNS will be converts in to IP address.



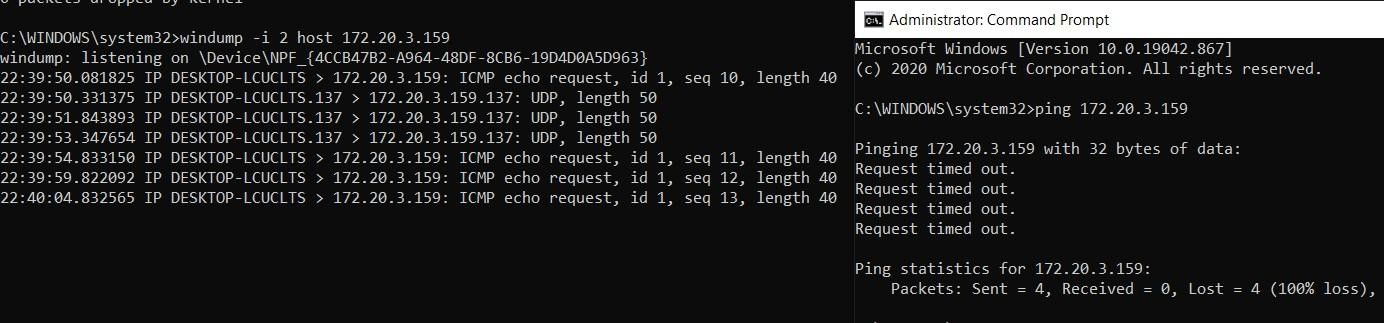
**Windump -I -c5 -nn ip** :this filter captures only 5 packets and DNS will be converts in to IP address



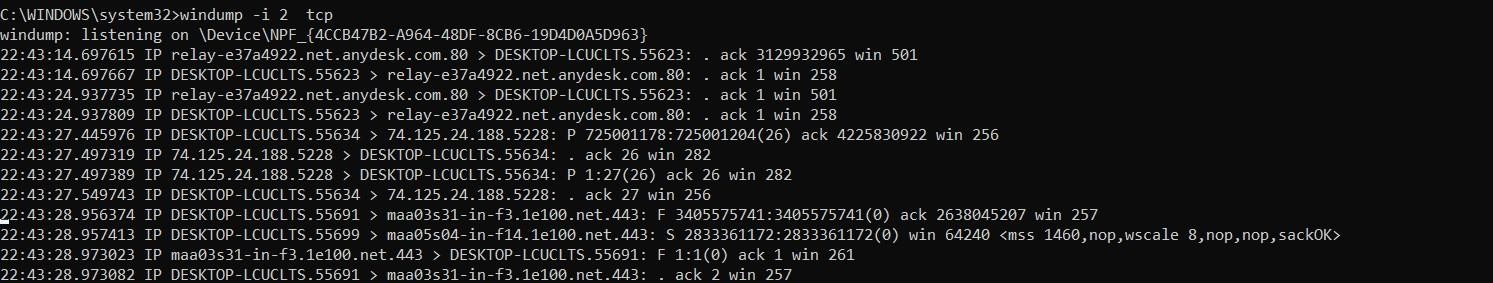
**Windump -I port 80**: this filter captures the packets whose port number is 80.



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



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



## Experiment-9

**AIM: Analysis of network traces using Whireshark**

**What is Wireshark?**

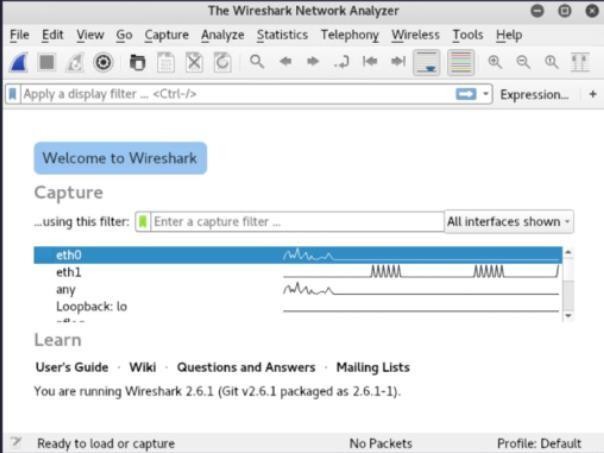
[Wireshark](https://www.wireshark.org/) is an open-source network protocol analysis software program started by [Gerald Combs i](https://blog.wireshark.org/author/admin/)n 1998. A global organization of network specialists and software developers support Wireshark and continue to make updates for new network technologies and encryption methods.

**How does Wireshark work?**

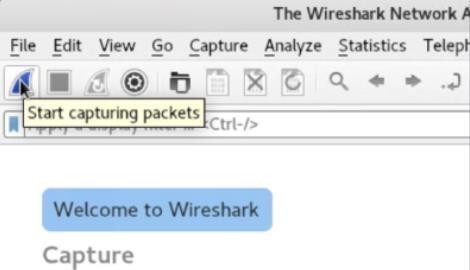
Wireshark is a packet sniffer and analysis tool. It captures network traffic on the local network and stores that data for offline analysis. Wireshark captures network traffic from Ethernet, Bluetooth, Wireless (IEEE.802.11), Token Ring, Frame Relay connections, and more.

Wireshark allows you to filter the log either before the capture starts or during analysis, so you can narrow down and zero into what you are looking for in the network trace. For example, you can set a filter to see TCP traffic between two IP addresses. You can set it only to show you the packets sent from one computer. The filters in Wireshark are one of the primary reasons it became the standard tool for packet analysis.

**Capturing Data Packets on Wireshark**

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.Click the first button on the toolbar, titled “Start Capturing Packets.”



**Analyzing Data Packets on Wireshark**

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

* + **No.**: This is the number order of the packet that got captured. The bracket indicates that this packet is part of a conversation.
  + **Time**: This column shows you how long after you started the capture that this packet got captured. You can change this value in the Settings menu if you need something different displayed.
  + **Source**: This is the address of the system that sent the packet.
  + **Destination**: This is the address of the destination of that packet.
  + **Protocol**: This is the type of packet, for example, TCP, DNS, DHCPv6, or ARP.
  + **Length**: This column shows you the length of the packet in bytes.
  + **Info**: This column shows you more information about the packet contents, and will vary depending on what kind of packet it is.

**Wireshark Capture Filters Commands**

[Capture filters](https://wiki.wireshark.org/CaptureFilters) limit the captured packets by the filter. Meaning if the packets don’t match the filter, Wireshark won’t save them. Here are some examples of capture filters:

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

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

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

