LABORATORY RECORD

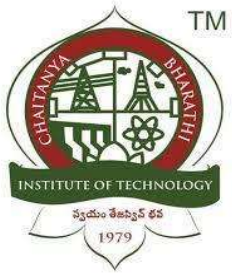
NAME: …….

ROLL NO: …… BRANCH & SECTION: ……

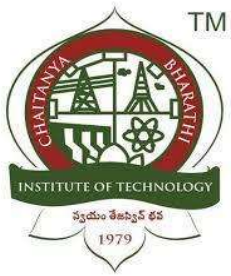
ACADEMIC YEAR: …… CLASS & SEMESTER: ……

COURSE WITH CODE……

DEPARTMENT: ……



CHAITANYA BHARATHI INSTITUTE OF TECHNOLOGY
(An Autonomous Institution, Affiliated to Osmania University, Approved by AICTE,
Accredited by NAAC with A++ Grade and Programs Accredited by NBA)
Chaitanya Bharathi Post, Gandipet, Kokapet (Vill.), Hyderabad, Ranga Reddy - 500 075, Telangana
www.cbit.ac.in



CHAITANYA BHARATHI INSTITUTE OF TECHNOLOGY

(An Autonomous Institution, Affiliated to Osmania University, Approved by AICTE,
Accredited by NAAC with A++ Grade and Programs Accredited by NBA)
Chaitanya Bharathi Post, Gandipet, Kokapet (Vill.), Hyderabad, Ranga Reddy - 500 075, Telangana
www.cbit.ac.in

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING (CSE)

Certificate

Certified that this is the bonafide record of the practical work done by the

candidate Mr/Ms. …….

Roll No:……..……of Program.....

Section……..……., Semester ……..in the Laboratory course with

Code……..……

during the academic year……

Total Number of Experiments prescribed: ……

Total Number of Experiments done: ……

Signature of the Faculty **HoD**

Semester End Examination held on……

Internal Examiner **External Examiner**

CHAITANYA BHARATHI INSTITUTE OF TECHNOLOGY

(An Autonomous Institution, Affiliated to Osmania University, Approved by AICTE,
Accredited by NAAC with A++ Grade and Programs Accredited by NBA)
Chaitanya Bharathi Post, Gandipet, Kokapet (Vill.), Hyderabad, Ranga Reddy - 500 075, Telangana
www.cbit.ac.in

Vision of Institute

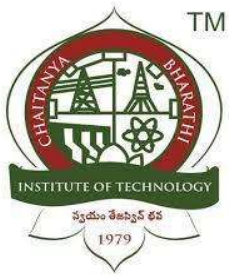
To be the Centre of Excellence in Technical Education and Research.

Mission of Institute

To address the Emerging needs through Quality Technical Education and Advanced Research.

Quality Policy

CBIT imparts value based Technical Education and Training to meet the requirements of students, Industry, Trade/ Profession, Research and Development Organizations for Self-sustained growth of Society.



CHAITANYA BHARATHI INSTITUTE OF TECHNOLOGY

(An Autonomous Institution, Affiliated to Osmania University, Approved by AICTE, Accredited by NAAC with A++ Grade and Programs Accredited by NBA)
Chaitanya Bharathi Post, Gandipet, Kokapet (Vill.), Hyderabad, Ranga Reddy - 500 075, Telangana
www.cbit.ac.in

DEPARTMENT OF CSE

Vision of the Department

To be in the frontiers of Computer Science and Engineering with academic excellence and Research.

Mission of the Department

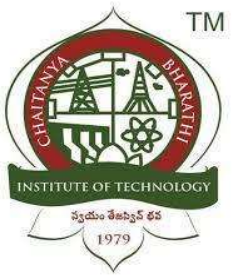
The mission of the Computer Science and Engineering Department is to:

1. Educate students with the best practices of Computer Science by integrating the latest research into the curriculum
2. Develop professionals with sound knowledge in theory and practice of Computer Science and Engineering
3. Facilitate the development of academia-industry collaboration and societal outreach programs
4. Prepare students for full and ethical participation in a diverse society and encourage lifelong learning

Program Educational Objectives (PEOs)

After the completion of the program, our:

1. Graduates will apply their knowledge and skills to succeed in theircareers and/or obtain advanced degrees, provide solutions as entrepreneurs
2. Graduates will creatively solve problems, communicate effectively, and successfully function in multi-disciplinary teams with superior work ethics and values
3. Graduates will apply principles and practices of Computer Science, mathematics, and science to successfully complete hardware and/or software-related engineering projects to meet customer business objectives
4. Graduates will have the ability to adapt, contribute, innovates modern technologies and systems in the domain of Cyber Security, IoT or productively engage in research



CHAITANYA BHARATHI INSTITUTE OF TECHNOLOGY

(An Autonomous Institution, Affiliated to Osmania University, Approved by AICTE,
Accredited by NAAC with A++ Grade and Programs Accredited by NBA)
Chaitanya Bharathi Post, Gandipet, Kokapet (Vill.), Hyderabad, Ranga Reddy - 500 075, Telangana
www.cbit.ac.in

DEPARTMENT OF CSE

Program Outcomes (POs)

PO1. Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems

PO2. Identify, formulate, review of research literature, and analyses complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering scien sciences

PO3.Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for public health and safety, and cultural, societal, and environmental considerations

PO4.Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions

PO5. Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools, including prediction and modelling to complex
engineering activities, with an understanding of the limitations

PO6. Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice

PO7. Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development

PO8.Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings

PO9. Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice

PO10.Communicate effectively on complex engineering activities with the engineering community and with the society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions

PO11.Demonstrate knowledge and understanding of the engineering and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments

PO12. Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change

Program Specific Outcomes (PSOs)

PSO1. Able to acquire the practical competency through emerging technologies and open-source platforms related to the areas of Cyber Security, IoT, and Blockchain

PSO2. Able to assess the hardware and software aspects necessary for the development of solutions to secure critical IT infrastructure and prepare collaborative plans for any incidence response

PSO3. Able to provide diversified solutions in product development by adhering to ethical values for the benefit of society

CHAITANYA BHARATHI INSTITUTE OF TECHNOLOGY

(An Autonomous Institution, Affiliated to Osmania University, Approved by AICTE, Accredited by NAAC with A++ Grade and Programs Accredited by NBA)
Chaitanya Bharathi Post, Gandipet, Kokapet (Vill.), Hyderabad, Ranga Reddy - 500 075, Telangana
www.cbit.ac.in

DEPARTMENT OF CSE

Name of the Laboratory Course with Code:

DATA COMMUNICATION AND COMPUTER NETWORKS LAB 20CSC24

Course Outcomes (COs):

CO1. Identify the different types of wiring equipment‟s used in the networks lab.

CO2. Understand the various network devices like repeater, hub, switch, and routers

CO3. Practice the basic network configuration commands like ifconfig, ping, traceroute, nslookup, dig, arp, netstat, nmap.

CO4. Design and demonstrate network topologies using GNS3.

CO5. Examine the packet transfer using tcpdump.

CO6. Analyze the network performance using Wireshark or any tool.

CO-PO/PSO Articulation Matrix:

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1															
CO2															
CO3															
CO4															
CO5															

CHAITANYA BHARATHI INSTITUTE OF TECHNOLOGY

(An Autonomous Institution, Affiliated to Osmania University, Approved by AICTE,
Accredited by NAAC with A++ Grade and Programs Accredited by NBA)

Chaitanya Bharathi Post, Gandipet, Kokapet (Vill.), Hyderabad, Ranga Reddy - 500 075, Telangana

www.cbit.ac.in

DEPARTMENT OF CSE

INDEX

Exp. No	Name of the Experiment	Date of Experiment	Date of Submission	Page No.	Record Marks/Grade	Signature of Faculty

EXPERIMENT – 1

AIM: Study of network media, cables, networking devices and cable construction.

DESCRIPTION:

Transmission Media:

A transmission medium is a physical path between the transmitter and the receiver i.e. it is the channel through which data is sent from one place to another. Transmission Media is broadly classified into the following types:

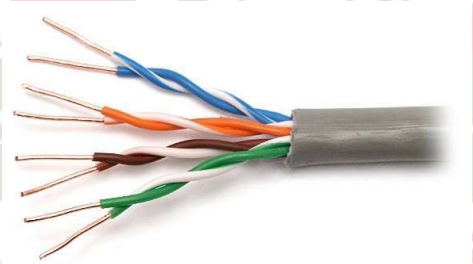
- **Guided Media**: It is also referred to as Wired or Bounded transmission media. Signals being transmitted are directed and confined in a narrow pathway by using physical links. There are three major types of guided media:

1. **Twisted pair cable**:

   It consists of 2 separately insulated conductor wires wound about each other. Generally, several such pairs are bundled together in a protective sheath. They are the most widely used Transmission Media. Twisted Pair is of two types:

   a) **Unshielded Twisted Pair (UTP):**

   UTP consists of two insulated copper wires twisted around one another. This type of cable has the ability to block interference and does not depend on a physical shield for this purpose.



Advantages:

- Least expensive
- Easy to install
- High-speed capacity.

Disadvantages:

- Susceptible to external interference
- Lower capacity and performance in comparison to STP
- Short distance transmission due to attenuation.

Specifications:

- Speed and throughput – 10 to 1000Mbps
- Average cost per node – least expensive
- Media and connector size – small
- Maximum cable length – 100m
- Signal type – electrical

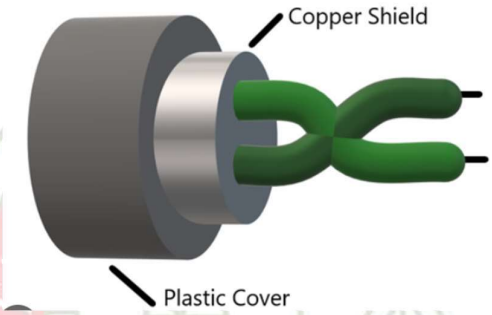
- EMI effect – maximum

Applications:

- Used in telephone connections and LAN network.

b) Shielded Twisted Pair (STP):

This type of cable consists of a special jacket (a copper braid covering or a foil shield) to block external interference. It is used in fast-data-rate Ethernet and in voice and data channels of telephone lines.



Advantages:

- Better performance at a higher data rate in comparison to UTP
- Eliminates crosstalk
- Comparatively faster

Disadvantages:

- Comparatively difficult to install and manufacture
- More expensive
- Bulky.

Specifications:

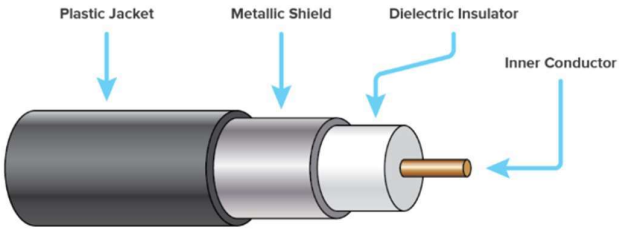
- Speed and throughput – 10 to 100Mbps
- Media and connector size – medium
- Maximum cable length – 100m
- Signal type – electrical
- EMI effect – maximum

Applications:

The shielded twisted pair type of cable is most frequently used in extremely cold climates, where the additional layer of outer covering makes it perfect for withstanding such temperatures or for shielding the interior components.

2. **Coaxial cable**:

It has an outer plastic covering containing an insulation layer made of PVC or Teflon and 2 parallel conductors each having a separate insulated protection cover. The coaxial cable transmits information in two modes: Baseband mode(dedicated cable bandwidth) and Broadband mode(cable bandwidth is split into separate ranges). Cable TVs and analog television networks widely use Coaxial cables.



Advantages:

- High Bandwidth
- Better noise Immunity
- Easy to install and expand
- Inexpensive.

Disadvantages:

- Single cable failure can disrupt the entire network

Specifications:

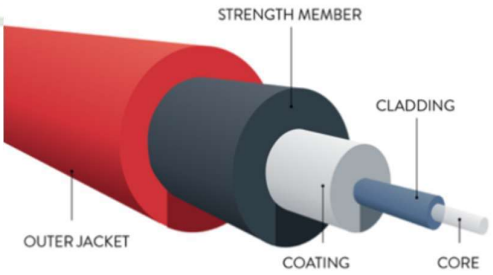
- Average cost per node – inexpensive
- Media and connector size – medium
- Maximum cable length – 500m(medium)
- EMI effect – maximum
- Attenuation – more
- Signal type – electrical

Applications:

Radio frequency signals are sent over coaxial wire. It can be used for cable television signal distribution, digital audio (S/PDIF), computer network connections (like Ethernet), and feedlines that connect radio transmitters and receivers to their antennas.

3. **Fibre optic cable**:

It uses the concept of refraction of light through a core made up of glass or plastic. The core is surrounded by a less dense glass or plastic covering called the cladding. It is used for the transmission of large volumes of data. The cable can be unidirectional or bidirectional. The WDM (Wavelength Division Multiplexer) supports two modes, namely unidirectional and bidirectional mode.



Advantages:

- Increased capacity and bandwidth
- Lightweight
- Less signal attenuation
- Immunity to electromagnetic interference
- Resistance to corrosive materials.

Disadvantages:

- Difficult to install and maintain
- High cost
- Fragile.

Specifications:

- Cost – inexpensive
- Attenuation – very less
- No EMI effect
- Bandwidth – Giga bps/km

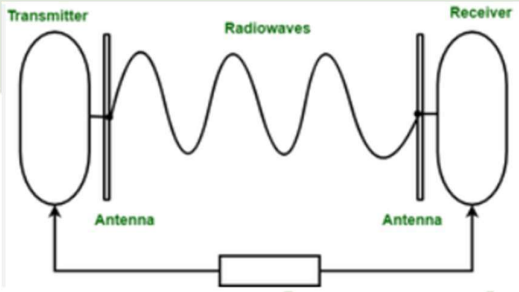
Applications:

Used in several types of medical instruments, used in transmission of data in aerospace, this is largely used in formation of internet cables, used for lighting purposes and safety measures in designing the interior and exterior of automobiles.

- **Unguided Media**: Unguided media transport electromagnetic waves without using a physical conductor. It is also known as unbounded or wireless media, and does not rely on physical pathways to transmit signals. Instead, they use wireless communication methods to propagate signals through the air or free space.

1. **Radio waves**:

These are easy to generate and can penetrate through buildings. The sending and receiving antennas need not be aligned. Frequency Range:3KHz – 1GHz.



Advantages:

- Ideal for broadcasting over vast distances.
- Can partially pass through walls and buildings.

Disadvantages:

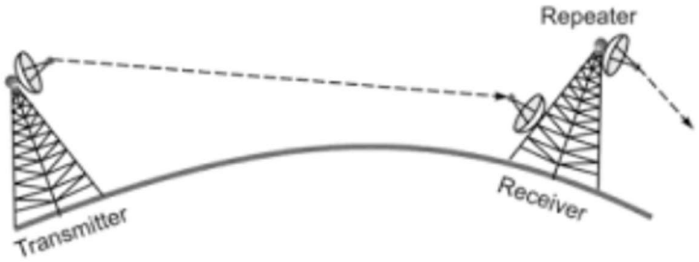
- May lead to congestion and limited user capacity
- Affected by other electronic devices and atmospheric conditions.

Applications:

- AM and FM radios and cordless phones use Radio waves for transmission.

2. **Microwaves**:

It is a line-of-sight transmission i.e., the sending and receiving antennas need to be properly aligned with each other. The distance covered by the signal is directly proportional to the height of the antenna. Frequency Range:1GHz – 300GHz.



Advantages:

- Suitable for high-speed data transmission
- Less prone to interference from other devices and weather conditions.

Disadvantages:

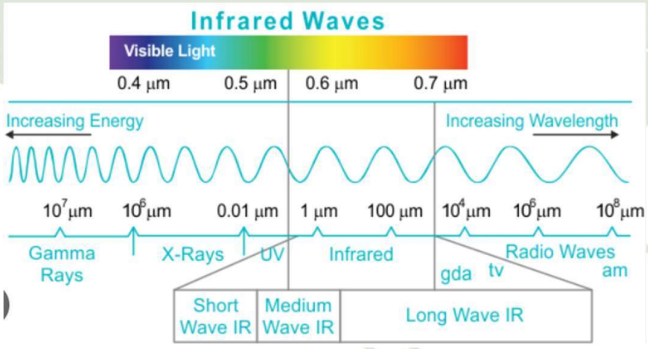
- Limited distance coverage compared to radio waves, less effective in areas with high humidity.

Applications:

- These are majorly used for mobile phone communication and television distribution.

3. **Infrared waves**:

Infrared waves are used for very short distance communication. They cannot penetrate through obstacles. This prevents interference between systems. Frequency Range:300GHz – 400THz.



Advantages:

- Offers a degree of security due to limited range and line-of-sight requirements
- Energy-efficient
- Making it suitable for remote controls.

Disadvantages:

- Short transmission distance with a direct line of sight
- Affected by sunlight and other light sources.

Applications:

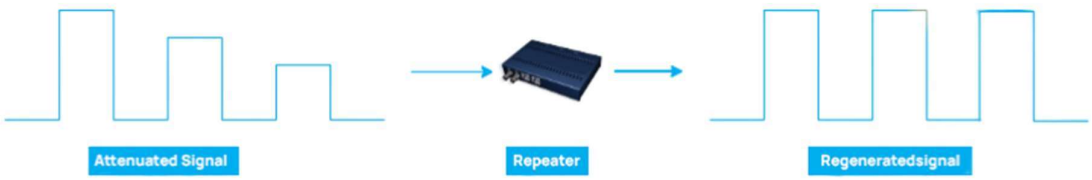
- It is used in TV remotes, wireless mouse, keyboard, printer, etc.

Network devices:

Network devices, also known as networking hardware, are physical devices that allow hardware on a computer network to communicate and interact with one another. For example Repeater, Hub, Bridge, Switch, Routers, Gateway, router, and NIC, etc.
There are various types of network devices such as:

1. **Repeater**:

A repeater is a device that amplifies and regenerates signals as they pass through the network. The primary purpose of a repeater is to extend the distance of a network by increasing the strength and quality of signals over long distances or through dense blocks.



There are various types of repeaters such as:

- Analog repeater: These repeaters work by amplifying the incoming signal and regenerating it at the output. It is used in older network technologies that operate on analog signals.
- Digital repeater: These repeaters work by regenerating the digital signal without amplifying it. It is used in modern network technologies which operate on digital signals.
- Local repeaters: Local repeaters are typically used in small networks where the distance between devices is limited.
- Remote repeaters: Remote repeaters are typically used in larger networks where the distance between devices is greater.

Advantages:

- Repeaters amplify signals, maintaining their strength throughout the line.
- It enables faster data transfer, critical for high-speed applications like video streaming.
- They reduce noise and distortions, leading to more stable and reliable signals.
- These allow signals to travel longer distances without losing strength or quality.

Disadvantages:

- The cost to build and maintain these is very high.
- These require a power source to operate, which can be a constraint in some situations.
- They introduce a delay in signal transmission, which can be difficult in real-time applications.
- Adding repeaters can increase its complexity, making troubleshooting and maintenance more difficult.

Applications:

- In both wired and wireless networks, repeaters enhance coverage by eliminating dead zones and improving connectivity.
- Repeaters are utilized in satellite communication systems to amplify and relay signals between ground stations and satellites.
- In radio communication, especially in amateur radio and broadcasting, repeaters enhance the coverage area by receiving and retransmitting radio signals, allowing them to reach a broader audience.
- Repeaters are employed in cable television distribution networks to amplify signals as they travel over long distances through coaxial cables.

2. **Hub:**

In networking, a hub is a device that links multiple computers and devices together. Hubs can also be referred to as repeaters or concentrators, and they serve as the center of a local area network (LAN). In a hub, each connected device is on the same subnet and receives all data sent to the hub. The hub then forwards that data out to all other connected devices, creating an efficient system for sharing data between users.

There are 3 different types of hubs

- Active hub: They have a power supply for regenerating, and amplifying the signals. When a port sends weak signalled data, the hub regenerates the signal and strengthens it, then send it further to all other ports. Active hubs are expensive in costs as compared to passive hubs.
- Passive hub: Passive hubs are simply used to connect signals from different network cables as they do not have any computerized element. They simply connect the wires of different devices in the star topology. Passive hubs do not do any processing or signal regeneration and that's why do not require electricity the most they can do is they can copy or repeat the signal. It can't clean the message, and it can't amplify or strengthen the signal.
- Intelligent hub: Intelligent hubs as the name suggests are smarter than active and passive hubs. The intelligent hub comprises a special monitoring unit named a Management Information Base (MIB). This is software that helps in analysing and troubleshooting network problems. Intelligent hubs work similarly to active hubs but with some management features. Like it can monitor the traffic of the network and the configuration of a port.

Advantages:

- Less expensive
- Does not impact network performance.
- Support different network media.
- Easily connects with different media.

Disadvantages:

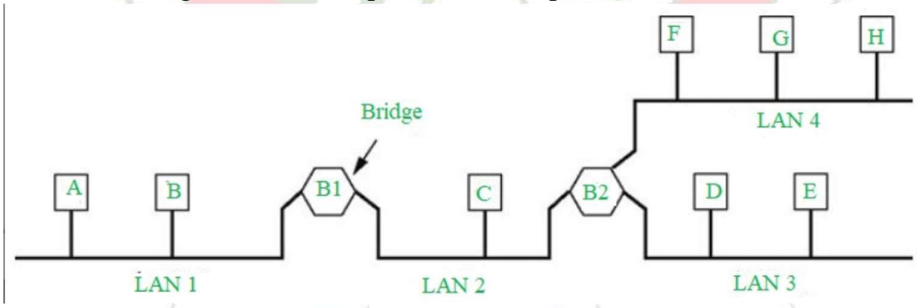
- It cannot find the best/ shortest path of the network.
- No mechanism for traffic detection.
- No mechanism for data filtration.
- Not capable of connecting to different network topologies like token, ring, ethernet, etc.

Applications:

- Hub is used to create small home networks.
- It is used for network monitoring.
- They are also used in organizations to provide connectivity.
- It can be used to create a device that is available thought out of the network.

3. **Bridge**:

A bridge in a computer network is a device used to connect multiple LANs together with a larger Local Area Network (LAN). The mechanism of network aggregation is known as bridging. The bridge is a physical or hardware device but operates at the OSI model's data link layer and is also known as a layer of two switches. They are used to divide network connections into sections, now each section has separate bandwidth and a separate collision domain. Here bridge is used to improve network performance.



There are 3 different types of bridges:

- Transparent bridge: Transparent bridges are invisible to other devices on the network. This bridge doesn't reconfigure the network on the addition or deletion of any station. The prime function of the transparent bridge is to block or forward the data according to the MAC address.
- Source routing bridge: Source routing bridges were developed and designed by IBM specifically for token ring networks. The frame's entire route is embedded with the data frames by the source station to perform the routing operation so that once the frame is forwarded it must follow a specific defined path/route.
- Translational bridge: Translational bridges convert the received data from one networking system to another. Or it is used to communicate or transmit data between two different types of networking systems. Like if we are sending data

from a token ring to an Ethernet cable, the translational cable will be used to connect both the networking system and transmit data.

Advantages:

- Bridges can be used as a network extension like they can connect two network topologies together.
- Highly reliable and maintainable. The network can be divided into multiple LAN segments.
- Simple installation, no requirement of any extra hardware or software except the bridge itself.
- Protocol transparency is higher as compared to other protocols.

Disadvantages:

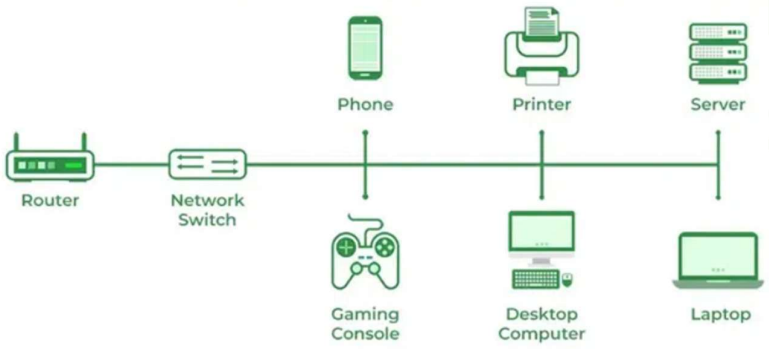
- Expensive as compared to hubs and repeaters.
- Slow in speed.
- Poor performance as additional processing is required to view the MAC address of the device on the network.
- As the traffic received is in bulk or is broadcasted traffic, individual filtering of data is not possible.

Applications:

- Bridges divide a network into segments, reducing collision domains for improved performance.
- Bridges connect different network types, enabling seamless communication between heterogeneous networks.
- Bridges isolate collision domains, preventing network-wide collisions and enhancing overall network efficiency.

4. **Switch:**

A switch is a network device that operates at the Data Link Layer (Layer 2) of the OSI model. It connects devices within a local area network (LAN) and uses MAC addresses to forward data to the specific device in the network.



There are various types of switches:

- Unmanaged Switches: Unmanaged Switches are the devices that are used to enable Ethernet devices that help in automatic data passing. These are generally used for home networks and small businesses.
- Managed Switches: Managed Switches are switches having more complex networks. SNMP (Simple Network Management Protocol) can be used for

configuring managed switches. These types of switches are mostly used in large networks having complex architecture. They provide better security levels.

- LAN Switches: Also called ethernet switches or data switches. LAN switches always try to avoid overlapping of data packets in the network just by allocating bandwidth in such a manner.
- PoE Switches: Power over Ethernet (PoE) are the switches used in Gigabit Ethernets. PoE help in combining data and power transmission over the same cable so that it helps in receiving data and electricity over the same line.
- Virtual Switches: Virtual Switches are the switches that are inside Virtual Machine hosting environments.
- Routing Switches: These are the switches that are used to connect LANs.They also have the work of performing functions in the Network Layer of the OSI Model.

Advantages:

- Prevents traffic overloading in a network by segmenting the network into smaller subnets.
- Increases the bandwidth of the network.
- Less frame collision as the switch creates the collision domain for each connection.

Disadvantages:

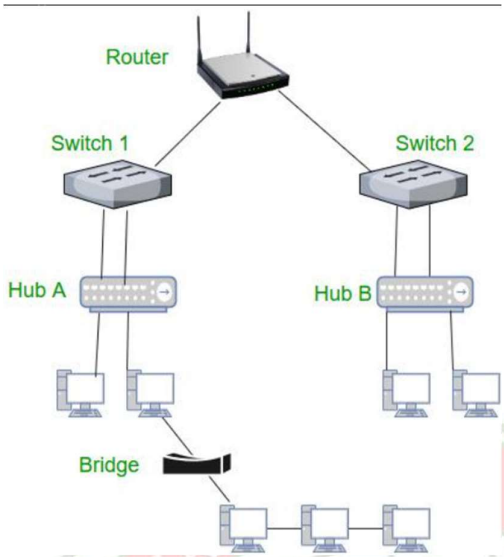
- It cannot stop traffic destined for a different LAN segment from traveling to all other LAN segments.
- Switches are more expensive.

Applications:

- Commonly used in large enterprise networks for connecting computers, printers, and servers.
- Essential in datacentres to manage and distribute network traffic efficiently.
- Found in home networks for connecting various devices like computers, smart TVs, and gaming consoles.
- Deployed in industrial environments to connect and control machinery and devices.

5. **Router:**

A Router is a networking device that forwards data packets between computer networks. One or more packet-switched networks or subnetworks can be connected using a router. By sending data packets to their intended IP addresses, it manages traffic between different networks and permits several devices to share an Internet connection.



There are various types of routers such as:

- Broadband Routers: it is used to connect computers or it is also used to connect to the internet.
- Wireless routers: These routers are used to create a wireless signal in your office or home. Wireless routers receive data packets over wired broadband, convert the packets written in binary code into radio signals that are picked up by electronic devices, and then convert them back into previous packets.
- Edge Routers: As the name indicates, these are located at the edges usually connected to an Internet Service Provider, and distribute packets across multiple packets.
- Core Routers: Core routers distribute packets within the same network. The main task is to carry heavy data transfers.

Advantages:

- Manages and allocates bandwidth efficiently, optimizing network performance.
- Makes intelligent routing decisions based on destination IP addresses, optimizing data transmission.
- Enables the creation of distinct subnets, enhancing network security and performance.
- Routers forward data packets between different networks, allowing communication between devices on separate networks.

Disadvantages:

- Routers can be more expensive than simpler network devices like switches.
- Configuration and management may require technical expertise, making them less user-friendly.
- In some cases, routers can become network bottlenecks if not properly configured.

Applications:

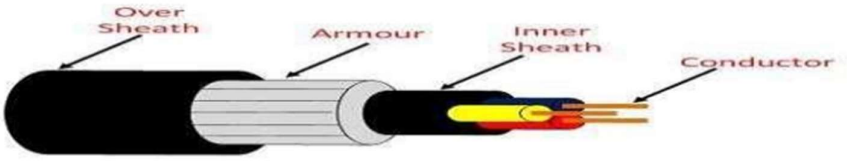
- Used in homes for connecting various devices to the internet and managing network traffic.
- Essential in large enterprise networks for managing complex network structures and ensuring secure communication.

- Connects geographically dispersed networks, forming a WAN and allowing seamless data exchange

CABLE CONSTRUCTION:

A cable used for the transmission and distribution of electrical energy is called electrical power cable. Power cable consists of two or more electrical conductors joined 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 drawbacks 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 details.



Electrical Power Cable

CONDUCTOR:

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

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

INSULATION:

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

- The insulator must have high insulation resistance.
- It should have high dielectric strength so that it does not allow the leakage current to pass through it.
- The material must have good mechanical strength.
- The dielectric material should be capable of operating at high temperatures.
- 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 aluminium sheath is also used in a power cable because it is cheaper, smaller in weight and high mechanical strength than the lead sheath. In oil-filled cables and telephone, cables corrugated seamless aluminium sheath is used because it has better-bending properties, reduced thickness, and lesser weight

PROTECTIVE COVERING:

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

ARMOURING:

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

CONCLUSION:

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

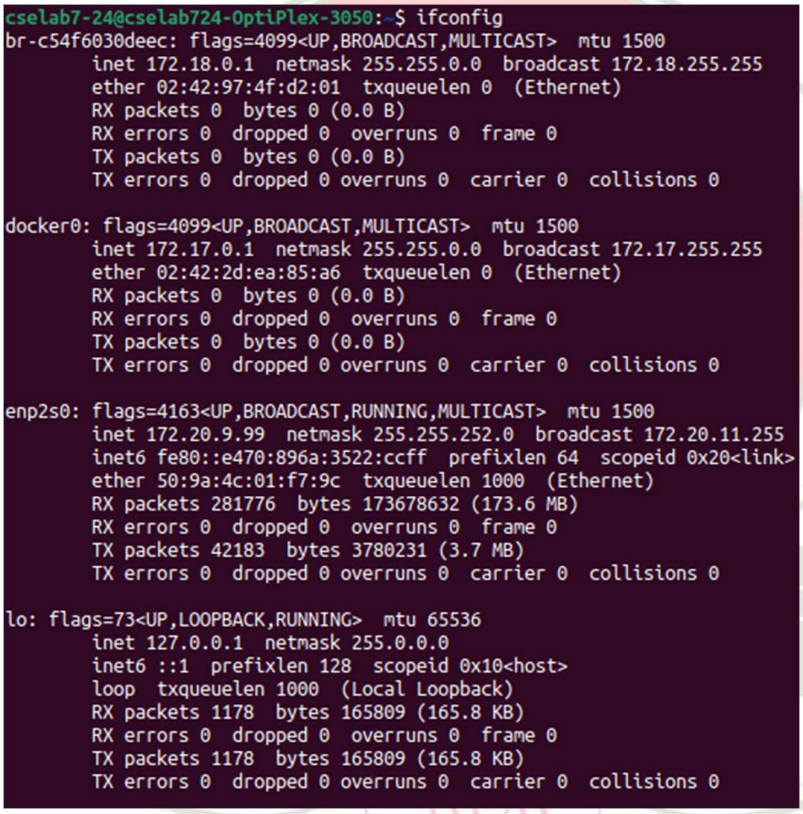
EXPERIMENT – 2

AIM: Demonstration of basic network commands / utilities in Linux

DESCRIPTION:

Linux networking commands are used extensively to inspect, analyse, maintain, and troubleshoot the networks connected to the system.

- **ifconfig (interface configurator)**: It is used to configure the kernel-resident network interfaces. It is used at the boot time to set up the interfaces as necessary.
  Syntax: ifconfig [options…] interface



```
cselab7-24@cselab724-OptiPlex-3050:~$ ifconfig
br-c54f6030deec: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.18.0.1  netmask 255.255.0.0  broadcast 172.18.255.255
        ether 02:42:97:4f:d2:01  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:2d:ea:85:a6  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

enp2s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.20.9.99  netmask 255.255.252.0  broadcast 172.20.11.255
        inet6 fe80::e470:896a:3522:ccff  prefixlen 64  scopeid 0x20<link>
        ether 50:9a:4c:01:f7:9c  txqueuelen 1000  (Ethernet)
        RX packets 281776  bytes 173678632 (173.6 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 42183  bytes 3780231 (3.7 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 1178  bytes 165809 (165.8 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1178  bytes 165809 (165.8 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Options:

-a: It is used to display all the interfaces available.

```
cselab6-14@cselab614-HP-Pro-3330-MT:~/160121733073$ ifconfig -a
enp5s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.20.10.122  netmask 255.255.252.0  broadcast 172.20.11.255
        inet6 fe80::5f54:f098:6569:2883  prefixlen 64  scopeid 0x20<link>
        ether d4:c9:ef:f2:a7:d1  txqueuelen 1000  (Ethernet)
        RX packets 809572  bytes 486667259 (486.6 MB)
        RX errors 0  dropped 12226  overruns 0  frame 0
        TX packets 182147  bytes 43635580 (43.6 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 12429  bytes 1571267 (1.5 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 12429  bytes 1571267 (1.5 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

-s: it is used to display a short list instead of details.

```
cselab6-14@cselab614-HP-Pro-3330-MT:~/160121733073$ ifconfig -s
Iface      MTU    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
enp5s0    1500   818866      0  12284 0        184175      0      0      0 BMRU
lo       65536    12563      0      0 0         12563      0      0      0 LRU
```

-v: version of the ifconfig

```
cselab6-14@cselab614-HP-Pro-3330-MT:~/160121733073$ ifconfig -v
enp5s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.20.10.122  netmask 255.255.252.0  broadcast 172.20.11.255
        inet6 fe80::5f54:f098:6569:2883  prefixlen 64  scopeid 0x20<link>
        ether d4:c9:ef:f2:a7:d1  txqueuelen 1000  (Ethernet)
        RX packets 822515  bytes 489689415 (489.6 MB)
        RX errors 0  dropped 12301  overruns 0  frame 0
        TX packets 184893  bytes 45008119 (45.0 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 12597  bytes 1588477 (1.5 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 12597  bytes 1588477 (1.5 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

- **ping**: PING (Packet Internet Groper) command is used to check the network connectivity between host and server/host. This command takes as input the IP address or the URL and sends a data packet to the specified address with the message “PING” and get a response from the server/host this time is recorded which is called latency.

```
cselab7-24@cselab724-OptiPlex-3050:~$ ping www.google.com
PING www.google.com (142.250.182.4) 56(84) bytes of data.
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=1 ttl=116 time=19.0 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=2 ttl=116 time=19.0 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=3 ttl=116 time=19.0 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=4 ttl=116 time=19.0 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=5 ttl=116 time=19.0 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=6 ttl=116 time=19.2 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=7 ttl=116 time=19.0 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=8 ttl=116 time=19.0 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=9 ttl=116 time=18.9 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=10 ttl=116 time=18.9 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=11 ttl=116 time=19.0 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=12 ttl=116 time=18.9 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=13 ttl=116 time=18.8 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=14 ttl=116 time=19.0 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=15 ttl=116 time=19.0 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=16 ttl=116 time=18.8 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=17 ttl=116 time=19.0 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=18 ttl=116 time=19.0 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=19 ttl=116 time=19.0 ms
64 bytes from maa05s18-in-f4.1e100.net (142.250.182.4): icmp_seq=20 ttl=116 time=19.0 ms
^C
--- www.google.com ping statistics ---
20 packets transmitted, 20 received, 0% packet loss, time 19035ms
rtt min/avg/max/mdev = 18.810/18.969/19.150/0.072 ms
```

Options:

ping -4: used IPV4 addresses respectively.

```
cselab7-24@cselab724-OptiPlex-3050:~$ ping -4 www.google.com
PING www.google.com (142.250.183.228) 56(84) bytes of data.
64 bytes from maa05s23-in-f4.1e100.net (142.250.183.228): icmp_seq=1 ttl=116 time=18.0 ms
64 bytes from maa05s23-in-f4.1e100.net (142.250.183.228): icmp_seq=2 ttl=116 time=18.1 ms
64 bytes from maa05s23-in-f4.1e100.net (142.250.183.228): icmp_seq=3 ttl=116 time=17.9 ms
64 bytes from maa05s23-in-f4.1e100.net (142.250.183.228): icmp_seq=4 ttl=116 time=18.1 ms
64 bytes from maa05s23-in-f4.1e100.net (142.250.183.228): icmp_seq=5 ttl=116 time=18.0 ms
^C
--- www.google.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4008ms
rtt min/avg/max/mdev = 17.915/18.010/18.073/0.057 ms
```

ping -a: The ping -a command in Linux is used to resolve the IP address of a host and display its hostname, if available.

```
cselab7-24@cselab724-OptiPlex-3050:~$ ping -a www.google.com
PING www.google.com (142.250.183.228) 56(84) bytes of data.
64 bytes from maa05s23-in-f4.1e100.net (142.250.183.228): icmp_seq=1 ttl=116 time=18.2 ms
64 bytes from maa05s23-in-f4.1e100.net (142.250.183.228): icmp_seq=2 ttl=116 time=18.0 ms
64 bytes from maa05s23-in-f4.1e100.net (142.250.183.228): icmp_seq=3 ttl=116 time=18.1 ms
64 bytes from maa05s23-in-f4.1e100.net (142.250.183.228): icmp_seq=4 ttl=116 time=17.9 ms
64 bytes from maa05s23-in-f4.1e100.net (142.250.183.228): icmp_seq=5 ttl=116 time=17.8 ms
64 bytes from maa05s23-in-f4.1e100.net (142.250.183.228): icmp_seq=6 ttl=116 time=18.0 ms
64 bytes from maa05s23-in-f4.1e100.net (142.250.183.228): icmp_seq=7 ttl=116 time=18.0 ms
64 bytes from maa05s23-in-f4.1e100.net (142.250.183.228): icmp_seq=8 ttl=116 time=18.0 ms
64 bytes from maa05s23-in-f4.1e100.net (142.250.183.228): icmp_seq=9 ttl=116 time=18.0 ms
64 bytes from maa05s23-in-f4.1e100.net (142.250.183.228): icmp_seq=10 ttl=116 time=18.1 ms
^C
--- www.google.com ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9017ms
rtt min/avg/max/mdev = 17.820/18.005/18.222/0.098 ms
```

ping -D: The ping -D option is used to set the "Don't Fragment" flag in the ICMP echo request packets sent by the ping command. When you set the "Don't Fragment" flag, it indicates that the packet should not be fragmented along its path to the target host. If the packet's size exceeds the Maximum Transmission Unit (MTU) of any network along the path, it will be discarded, and you'll receive an ICMP "Packet Too Big" error message.

```
cselab7-24@cselab724-OptiPlex-3050:~$ ping -D www.google.com
PING www.google.com (142.250.183.228) 56(84) bytes of data.
[1694755681.895557] 64 bytes from maa05s23-in-f4.1e100.net (142.250.183.228): icmp_seq=1 ttl=116 time=18.0 ms
[1694755682.897465] 64 bytes from maa05s23-in-f4.1e100.net (142.250.183.228): icmp_seq=2 ttl=116 time=17.9 ms
[1694755683.899629] 64 bytes from maa05s23-in-f4.1e100.net (142.250.183.228): icmp_seq=3 ttl=116 time=18.0 ms
[1694755684.900593] 64 bytes from maa05s23-in-f4.1e100.net (142.250.183.228): icmp_seq=4 ttl=116 time=17.8 ms
[1694755685.902574] 64 bytes from maa05s23-in-f4.1e100.net (142.250.183.228): icmp_seq=5 ttl=116 time=18.0 ms
[1694755686.904687] 64 bytes from maa05s23-in-f4.1e100.net (142.250.183.228): icmp_seq=6 ttl=116 time=18.0 ms
^C
--- www.google.com ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5009ms
rtt min/avg/max/mdev = 17.791/17.960/18.045/0.084 ms
```

- **traceroute**: It prints the route that packet takes to the host.
  Syntax: traceroute [options] host address

```
cselab6-14@cselab614-HP-Pro-3330-MT:~/160121733073$ traceroute cbit.ac.in
traceroute to cbit.ac.in (3.111.165.12), 30 hops max, 60 byte packets
 1  _gateway (172.20.8.1)  0.492 ms  0.477 ms  4.844 ms
 2  * * *
 3  10.22.22.1 (10.22.22.1)  2.150 ms  2.132 ms  2.178 ms
 4  * * *
 5  10.22.21.249 (10.22.21.249)  2.901 ms  2.915 ms  2.909 ms
 6  99.83.65.168 (99.83.65.168)  2.829 ms  2.805 ms  2.779 ms
 7  150.222.84.51 (150.222.84.51)  2.659 ms  2.636 ms  2.943 ms
 8  52.93.140.29 (52.93.140.29)  2.569 ms 52.93.140.51 (52.93.140.51)  2.881 ms 52.93.140.109 (52.93.140.109)  2.508 ms
 9  * * *
10  52.95.66.186 (52.95.66.186)  28.011 ms 52.95.66.120 (52.95.66.120)  20.371 ms 52.95.66.164 (52.95.66.164)  19.984 ms
11  52.95.64.134 (52.95.64.134)  19.918 ms 52.95.64.214 (52.95.64.214)  12.934 ms 52.95.64.250 (52.95.64.250)  19.905 ms
12  52.95.64.209 (52.95.64.209)  17.031 ms 52.95.64.143 (52.95.64.143)  20.996 ms 52.95.64.213 (52.95.64.213)  12.662 ms
13  99.83.76.247 (99.83.76.247)  12.563 ms 99.83.77.17 (99.83.77.17)  12.652 ms 99.83.77.9 (99.83.77.9)  12.572 ms
14  99.83.77.4 (99.83.77.4)  20.422 ms 99.83.76.140 (99.83.76.140)  20.861 ms 99.83.76.116 (99.83.76.116)  16.877 ms
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```

Options:

-4: Use IP version 4 only IPv4.

```
cselab6-14@cselab614-HP-Pro-3330-MT:~/160121733073$ traceroute -4 cbit.ac.in
traceroute to cbit.ac.in (3.111.165.12), 30 hops max, 60 byte packets
 1  _gateway (172.20.8.1)  0.366 ms  0.417 ms  0.401 ms
 2  103.52.36.129 (103.52.36.129)  16.266 ms  16.890 ms  17.514 ms
 3  10.22.22.1 (10.22.22.1)  2.584 ms  2.663 ms  2.712 ms
 4  10.22.22.253 (10.22.22.253)  2.182 ms  2.206 ms  2.319 ms
 5  10.22.21.249 (10.22.21.249)  1.689 ms  1.674 ms  1.683 ms
 6  99.83.65.168 (99.83.65.168)  2.436 ms  3.139 ms  3.118 ms
 7  * 150.222.84.43 (150.222.84.43)  2.962 ms 150.222.84.37 (150.222.84.37)  2.947 ms
 8  52.93.140.129 (52.93.140.129)  2.906 ms 52.93.140.83 (52.93.140.83)  2.892 ms 52.93.140.79 (52.93.140.79)  2.842 ms
 9  * * *
10  52.95.67.144 (52.95.67.144)  17.551 ms  17.535 ms 52.95.66.118 (52.95.66.118)  22.387 ms
11  52.95.64.186 (52.95.64.186)  20.493 ms 52.95.64.212 (52.95.64.212)  12.377 ms 52.95.64.238 (52.95.64.238)  13.131 ms
12  52.95.64.187 (52.95.64.187)  21.192 ms 52.95.64.181 (52.95.64.181)  20.364 ms 52.95.64.219 (52.95.64.219)  20.488 ms
13  99.83.77.9 (99.83.77.9)  12.418 ms 99.83.77.11 (99.83.77.11)  24.181 ms 99.83.77.23 (99.83.77.23)  24.147 ms
14  52.95.65.147 (52.95.65.147)  20.178 ms 99.83.76.116 (99.83.76.116)  23.442 ms 99.83.76.138 (99.83.76.138)  19.292 ms
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```

-n: Stop the resolving of the IP addresses.

```
cselab6-14@cselab614-HP-Pro-3330-MT:~/160121733073$ traceroute -n cbit.ac.in
traceroute to cbit.ac.in (3.111.165.12), 30 hops max, 60 byte packets
 1  172.20.8.1  0.499 ms  0.474 ms  0.458 ms
 2  103.52.36.129  4.510 ms  6.886 ms  6.871 ms
 3  10.22.22.1  1.961 ms  2.017 ms  2.074 ms
 4  * * *
 5  10.22.21.249  1.677 ms  1.662 ms  1.688 ms
 6  99.83.65.168  1.851 ms  1.490 ms  1.495 ms
 7  150.222.84.45  3.083 ms  2.156 ms *
 8  52.93.140.95  2.520 ms 52.93.140.145  4.755 ms 52.93.140.143  2.382 ms
 9  * * *
10  52.95.66.56  20.441 ms 52.95.67.100  12.267 ms 52.95.66.206  22.852 ms
11  52.95.64.184  20.441 ms 52.95.64.210  13.015 ms 52.95.64.236  12.468 ms
12  52.95.64.157  20.841 ms 52.95.64.253  12.676 ms 52.95.64.205  12.661 ms
13  99.83.76.133  31.777 ms 52.95.66.87  19.851 ms 99.83.76.105  20.694 ms
14  99.83.76.116  26.179 ms 52.95.65.145  26.158 ms 52.95.67.212  24.407 ms
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```

-m: to set the maximum number of hops for the packet to reach the destination.

```
cselab6-14@cselab614-HP-Pro-3330-MT:~/160121733073$ traceroute -m 5 cbit.ac.in
traceroute to cbit.ac.in (3.111.165.12), 5 hops max, 60 byte packets
 1  _gateway (172.20.8.1)  0.440 ms  0.397 ms  0.412 ms
 2  103.52.36.129 (103.52.36.129)  4.846 ms  5.628 ms  6.190 ms
 3  10.22.22.1 (10.22.22.1)  1.895 ms  1.962 ms  2.014 ms
 4  10.22.22.253 (10.22.22.253)  2.398 ms  2.442 ms  2.502 ms
 5  10.22.21.249 (10.22.21.249)  2.061 ms  2.041 ms  2.022 ms
```

- **nslookup (name server lookup)**: command for getting information from DNS server.
  Syntax: nslookup example.com/[IP address]

```
cselab6-14@cselab614-HP-Pro-3330-MT:~/160121733073$ nslookup cbit.ac.in
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   cbit.ac.in
Address: 3.111.165.12

cselab6-14@cselab614-HP-Pro-3330-MT:~/160121733073$
```

```
cselab6-14@cselab614-HP-Pro-3330-MT:~/160121733073$ nslookup 3.111.165.12
12.165.111.3.in-addr.arpa       name = ec2-3-111-165-12.ap-south-1.compute.amazonaws.com.

Authoritative answers can be found from:
165.111.3.in-addr.arpa  nameserver = ns2-24-ap-south-1.ec2-rdns.amazonaws.com.
165.111.3.in-addr.arpa  nameserver = ns4-24-ap-south-1.ec2-rdns.amazonaws.com.
165.111.3.in-addr.arpa  nameserver = ns3-24-ap-south-1.ec2-rdns.amazonaws.com.
165.111.3.in-addr.arpa  nameserver = ns1-24-ap-south-1.ec2-rdns.amazonaws.com.
```

Options:

-type=any: It shows us all the available DNS records.

```
cselab6-14@cselab614-HP-Pro-3330-MT:~/160121733073$ nslookup -type=any cbit.ac.in
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
cbit.ac.in      nameserver = ns-1525.awsdns-62.org.
cbit.ac.in      nameserver = ns-7.awsdns-00.com.
cbit.ac.in      nameserver = ns-1710.awsdns-21.co.uk.
cbit.ac.in      nameserver = ns-733.awsdns-27.net.
Name:   cbit.ac.in
Address: 3.111.165.12

Authoritative answers can be found from:
ns-7.awsdns-00.com      internet address = 205.251.192.7
ns-7.awsdns-00.com      has AAAA address 2600:9000:5300:700::1
ns-733.awsdns-27.net    internet address = 205.251.194.221
ns-733.awsdns-27.net    has AAAA address 2600:9000:5302:dd00::1
ns-1525.awsdns-62.org   internet address = 205.251.197.245
ns-1525.awsdns-62.org   has AAAA address 2600:9000:5305:f500::1
```

-type=a: To view all the available DNS records for the particular record.

```
cselab6-14@cselab614-HP-Pro-3330-MT:~/160121733073$ nslookup -type=a cbit.ac.in
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   cbit.ac.in
Address: 3.111.165.12
```

-type=ns: It will output the name server which are associated with the given domain.

```
cselab6-14@cselab614-HP-Pro-3330-MT:~/160121733073$ nslookup -type=ns cbit.ac.in
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
cbit.ac.in      nameserver = ns-1525.awsdns-62.org.
cbit.ac.in      nameserver = ns-1710.awsdns-21.co.uk.
cbit.ac.in      nameserver = ns-7.awsdns-00.com.
cbit.ac.in      nameserver = ns-733.awsdns-27.net.

Authoritative answers can be found from:
cbit.ac.in      internet address = 3.111.165.12
ns-7.awsdns-00.com      internet address = 205.251.192.7
ns-7.awsdns-00.com      has AAAA address 2600:9000:5300:700::1
ns-1525.awsdns-62.org   internet address = 205.251.197.245
ns-733.awsdns-27.net    has AAAA address 2600:9000:5302:dd00::1
ns-1525.awsdns-62.org   has AAAA address 2600:9000:5305:f500::1
ns-733.awsdns-27.net    internet address = 205.251.194.221
```

- **netstat:** To print network connections, routing tables, interface statistics
  Syntax – netstat

```
cselab7-04@cselab704-OptiPlex-3050:~$ netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:48444         localhost:12379         ESTABLISHED
tcp        0      0 localhost:52126         localhost:16443         ESTABLISHED
tcp        0      0 localhost:48378         localhost:12379         ESTABLISHED
tcp        0      0 localhost:48258         localhost:12379         ESTABLISHED
tcp        0      0 localhost:48294         localhost:12379         ESTABLISHED
tcp        0      0 localhost:48220         localhost:12379         ESTABLISHED
tcp        0      0 localhost:48712         localhost:12379         ESTABLISHED
tcp        0      0 localhost:48530         localhost:12379         ESTABLISHED
tcp        0      0 localhost:48574         localhost:12379         ESTABLISHED
tcp        0      0 localhost:48408         localhost:12379         ESTABLISHED
tcp        0      0 localhost:48482         localhost:12379         ESTABLISHED
tcp        0      0 localhost:48632         localhost:12379         ESTABLISHED
tcp        0      0 localhost:33242         localhost:8191          ESTABLISHED
tcp        0      0 localhost:48232         localhost:12379         ESTABLISHED
tcp        0      0 localhost:33148         localhost:8191          ESTABLISHED
tcp        0      0 localhost:8191          localhost:33162         ESTABLISHED
tcp        0      0 localhost:33172         localhost:8191          ESTABLISHED
tcp        0      0 localhost:48350         localhost:12379         ESTABLISHED
tcp        0      0 localhost:48322         localhost:12379         ESTABLISHED
tcp        0      0 localhost:48394         localhost:12379         ESTABLISHED
tcp        0      0 localhost:33164         localhost:8191          ESTABLISHED
tcp        0      0 localhost:48670         localhost:12379         ESTABLISHED
tcp        0      0 localhost:8191          localhost:33164         ESTABLISHED
tcp        0      0 localhost:48500         localhost:12379         ESTABLISHED
tcp        0      0 localhost:48678         localhost:12379         ESTABLISHED
tcp        0      0 localhost:48692         localhost:12379         ESTABLISHED
tcp        0      0 localhost:48570         localhost:12379         ESTABLISHED
tcp        0      0 localhost:8191          localhost:33242         ESTABLISHED
tcp        0      0 localhost:46632         localhost:16443         ESTABLISHED
tcp        0      0 localhost:48590         localhost:12379         ESTABLISHED
```

Options:
-a: used to display all the existing connections. Syntax : netstat -a

```
cselab7-04@cselab704-OptiPlex-3050:~$ netstat -a
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:33845         0.0.0.0:*               LISTEN
tcp        0      0 localhost:1338          0.0.0.0:*               LISTEN
tcp        0      0 localhost:34441         0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:sunrpc          0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:25000           0.0.0.0:*               LISTEN
tcp        0      0 localhost:ipp           0.0.0.0:*               LISTEN
tcp        0      0 localhost:10252         0.0.0.0:*               LISTEN
tcp        0      0 localhost:10251         0.0.0.0:*               LISTEN
tcp        0      0 localhost:10249         0.0.0.0:*               LISTEN
tcp        0      0 localhost:10256         0.0.0.0:*               LISTEN
tcp        0      0 localhost:2380          0.0.0.0:*               LISTEN
tcp        0      0 localhost:8065          0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:8089            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:8191            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:8000            0.0.0.0:*               LISTEN
tcp        0      0 localhost:domain        0.0.0.0:*               LISTEN
tcp        0      0 localhost:48444         localhost:12379         ESTABLISHED
tcp        0      0 localhost:52126         localhost:16443         ESTABLISHED
tcp        0      0 localhost:48378         localhost:12379         ESTABLISHED
tcp        0      0 localhost:48258         localhost:12379         ESTABLISHED
tcp        0      0 cselab704-OptiPle:55322 239.237.117.34.bc:https ESTABLISHED
tcp        0      0 localhost:48294         localhost:12379         ESTABLISHED
tcp        0      0 localhost:48220         localhost:12379         ESTABLISHED
tcp        0      0 cselab704-OptiPle:36524 maa03s40-in-f14.1:https TIME_WAIT
tcp        0      0 localhost:48712         localhost:12379         ESTABLISHED
tcp        0      0 cselab704-OptiPle:42782 maa05s10-in-f10.1:https ESTABLISHED
tcp        0      0 cselab704-OptiPle:53806 maa05s21-in-f14.1:https ESTABLISHED
tcp        0      0 localhost:48530         localhost:12379         ESTABLISHED
tcp        0      0 localhost:48574         localhost:12379         ESTABLISHED
tcp        0      0 localhost:48408         localhost:12379         ESTABLISHED
```

-at: to display only TCP connection. Syntax: netstat -at

```
cselab7-04@cselab704-OptiPlex-3050:~$ netstat -at
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:33845         0.0.0.0:*               LISTEN
tcp        0      0 localhost:1338          0.0.0.0:*               LISTEN
tcp        0      0 localhost:34441         0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:sunrpc          0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:25000           0.0.0.0:*               LISTEN
tcp        0      0 localhost:ipp           0.0.0.0:*               LISTEN
tcp        0      0 localhost:10252         0.0.0.0:*               LISTEN
tcp        0      0 localhost:10251         0.0.0.0:*               LISTEN
tcp        0      0 localhost:10249         0.0.0.0:*               LISTEN
tcp        0      0 localhost:10256         0.0.0.0:*               LISTEN
tcp        0      0 localhost:2380          0.0.0.0:*               LISTEN
tcp        0      0 localhost:8065          0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:8089            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:8191            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:8000            0.0.0.0:*               LISTEN
tcp        0      0 localhost:domain        0.0.0.0:*               LISTEN
tcp        0      0 localhost:48444         localhost:12379         ESTABLISHED
tcp        0      0 localhost:52126         localhost:16443         ESTABLISHED
tcp        0      0 localhost:48378         localhost:12379         ESTABLISHED
tcp        0      0 localhost:53066         localhost:16443         TIME_WAIT
tcp        0      0 localhost:48258         localhost:12379         ESTABLISHED
tcp        0      1 cselab704-OptiPle:35844 169.254.169.254:http    SYN_SENT
tcp        0      0 cselab704-OptiPle:55322 239.237.117.34.bc:https ESTABLISHED
tcp        0      0 localhost:48294         localhost:12379         ESTABLISHED
tcp        0      0 localhost:48220         localhost:12379         ESTABLISHED
tcp        0      0 localhost:48712         localhost:12379         ESTABLISHED
tcp        0      0 cselab704-OptiPle:42782 maa05s10-in-f10.1:https ESTABLISHED
tcp        0      0 cselab704-OptiPle:53806 maa05s21-in-f14.1:https ESTABLISHED
tcp        0      0 localhost:48530         localhost:12379         ESTABLISHED
tcp        0      0 localhost:48574         localhost:12379         ESTABLISHED
```

-au: to display only UDP connection. Syntax: netstat -au

```
cselab7-04@cselab704-OptiPlex-3050:~$ netstat -au
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp        0      0 0.0.0.0:59623           0.0.0.0:*
udp        0      0 0.0.0.0:43787           0.0.0.0:*
udp        0      0 0.0.0.0:60332           0.0.0.0:*
udp        0      0 0.0.0.0:mdns            0.0.0.0:*
udp        0      0 0.0.0.0:46502           0.0.0.0:*
udp        0      0 localhost:domain        0.0.0.0:*
udp        0      0 cselab704-OptiPl:bootpc _gateway:bootps         ESTABLISHED
udp        0      0 0.0.0.0:sunrpc          0.0.0.0:*
udp        0      0 0.0.0.0:8472            0.0.0.0:*
udp        0      0 0.0.0.0:631             0.0.0.0:*
udp        0      0 0.0.0.0:34239           0.0.0.0:*
udp6       0      0 [::]:mdns               [::]:*
udp6       0      0 [::]:40450              [::]:*
udp6       0      0 [::]:sunrpc             [::]:*
```

- **arp**: arp command manipulates the System's ARP cache. It also allows a complete dump of the ARP cache. ARP stands for Address Resolution Protocol. The primary function of this protocol is to resolve the IP address of a system to its mac address, and hence it works between level 2(Data link layer) and level 3(Network layer).

```
cselab7-04@cselab704-OptiPlex-3050:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
169.254.169.254                  (incomplete)                              enp2s0
172.20.8.17              ether   00:e0:4c:68:59:70   C                     enp2s0
_gateway                 ether   e4:8d:8c:17:b8:6a   C                     enp2s0
```

Options:

-a: addition of hosts.

```
cselab7-04@cselab704-OptiPlex-3050:~$ arp -a
? (169.254.169.254) at <incomplete> on enp2s0
? (172.20.8.17) at 00:e0:4c:68:59:70 [ether] on enp2s0
_gateway (172.20.8.1) at e4:8d:8c:17:b8:6a [ether] on enp2s0
```

-n, –numeric: This option shows numerical addresses instead of symbolic host, port or usernames.

```
cselab7-04@cselab704-OptiPlex-3050:~$ arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
169.254.169.254                  (incomplete)                              enp2s0
172.20.8.17              ether   00:e0:4c:68:59:70   C                     enp2s0
172.20.8.1               ether   e4:8d:8c:17:b8:6a   C                     enp2s0
cselab7-04@cselab704-OptiPlex-3050:~$
```

-v, –verbose: This option shows the verbose information.

```
cselab7-04@cselab704-OptiPlex-3050:~$ arp -v
Address                  HWtype  HWaddress           Flags Mask            Iface
169.254.169.254                  (incomplete)                              enp2s0
172.20.8.17              ether   00:e0:4c:68:59:70   C                     enp2s0
_gateway                 ether   e4:8d:8c:17:b8:6a   C                     enp2s0
Entries: 3      Skipped: 0      Found: 3
cselab7-04@cselab704-OptiPlex-3050:~$
```

- **hostname**: The hostname command in Linux and Unix-like operating systems is used to display or set the system's hostname.

```
cselab7-24@cselab724-OptiPlex-3050:~$ hostname
cselab724-OptiPlex-3050
```

Options:

hostname -f: The -f option with the hostname command is used to display the fully qualified domain name (FQDN) of the system.

```
cselab7-24@cselab724-OptiPlex-3050:~$ hostname -f
cselab724-OptiPlex-3050
```

- **tracepath:** tracepath command in Linux is used to traces path to destination discovering MTU along this path. It uses UDP port or some random port. It is similar to traceroute, but it does not require superuser privileges and has no fancy options.

```
cselab7-24@cselab724-OptiPlex-3050:~$ tracepath www.google.com
 1?: [LOCALHOST]                      pmtu 1500
 1:  _gateway                                              0.838ms
 1:  _gateway                                              0.738ms
 2:  103.52.36.129                                         3.511ms
 3:  10.22.22.1                                            1.918ms
 4:  10.22.22.253                                          2.253ms
 5:  10.22.21.249                                          1.851ms
 6:  72.14.203.80                                         19.011ms asymm 11
 7:  no reply
 8:  no reply
^C
```

Options:

tracepath -4: Uses the IPV4 address

```
cselab7-24@cselab724-OptiPlex-3050:~$ tracepath -4 www.google.com
 1?: [LOCALHOST]                      pmtu 1500
 1:  _gateway                                              0.751ms
 1:  _gateway                                              0.704ms
 2:  103.52.36.129                                         3.307ms
 3:  10.22.22.1                                            1.889ms
 4:  10.22.22.253                                         11.533ms
 5:  10.22.21.249                                          1.549ms
 6:  72.14.203.80                                         18.515ms asymm 11
 7:  no reply
^C
```

tracepath -n: This option prints primarily IP addresses numerically.

```
cselab7-24@cselab724-OptiPlex-3050:~$ tracepath -n www.google.com
 1?: [LOCALHOST]                      pmtu 1500
 1:  172.20.8.1                                            0.698ms
 1:  172.20.8.1                                            0.773ms
 2:  103.52.36.129                                         3.535ms
 3:  10.22.22.1                                           40.018ms
 4:  10.22.22.253                                          2.116ms
 5:  10.22.21.249                                          1.754ms
 6:  72.14.203.80                                         18.759ms asymm 11
 7:  no reply
^C
```

tracepath -b: This option print both of host names and IP addresses.

```
cselab7-24@cselab724-OptiPlex-3050:~$ tracepath -b www.google.com
 1?: [LOCALHOST]                      pmtu 1500
 1:  _gateway (172.20.8.1)                                 2.390ms
 1:  _gateway (172.20.8.1)                                 0.741ms
 2:  103.52.36.129 (103.52.36.129)                         3.464ms
 3:  10.22.22.1 (10.22.22.1)                              26.031ms
 4:  10.22.22.253 (10.22.22.253)                           3.116ms
 5:  10.22.21.249 (10.22.21.249)                           1.806ms
 6:  72.14.203.80 (72.14.203.80)                          22.560ms asymm 11
^C
```

CONCLUSION: The various network commands and their options, of linux operating system are studied.

EXPERIMENT – 3

AIM: PC network configuration for windows

DESCRIPTION:

Network configuration is the process of setting a network's controls, flow and operation to support the network communication of an organisation and/or network owner.

IP Address:

An IP (Internet Protocol) address is a numerical label assigned to each device participating in a computer network that uses the Internet Protocol for communication. IP addresses serve two main functions:

1. Network Addressing: IP addresses are used to uniquely identify a device on a network, allowing data packets to be routed to the correct destination.
2. Location Identification: IP addresses can provide information about the location of a device or the network it belongs to.

IPV4 –

IPv4, the fourth version of the Internet Protocol (IP), is the foundational protocol for internet communication within the TCP/IP suite. Its 32-bit addresses, exemplified as four octets like "192.168.0.1," allow for around 4.3 billion unique addresses. Commonly presented in dotted-decimal notation, each octet is expressed as a decimal number between 0 and 255. As the precursor to IPv6, IPv4 faces challenges due to its finite address space, prompting the development of its successor for sustained internet growth.

IPv4 classes:

- Class A (1.0.0.0 to 126.0.0.0): Class A addresses have a first octet in the range 1 to 126. They are used for large networks and can support up to 16 million hosts on each network. The first bit in the first octet is always 0.
- Class B: Class B addresses have a first octet in the range 128 to 191. They are used for medium-sized networks and can support up to 65,000 hosts on each network. The first two bits in the first octet are 10.
- Class C: Class C addresses have a first octet in the range 192 to 223. They are used for small networks and can support up to 254 hosts on each network. The first three bits in the first octet are 110.
- Class D: Class D addresses are used for multicast groups. They are not used for host addresses but for multicasting data to multiple hosts simultaneously.
- Class E: Class E addresses are reserved for experimental and research purposes and are not used in common networks.

IPV6 –

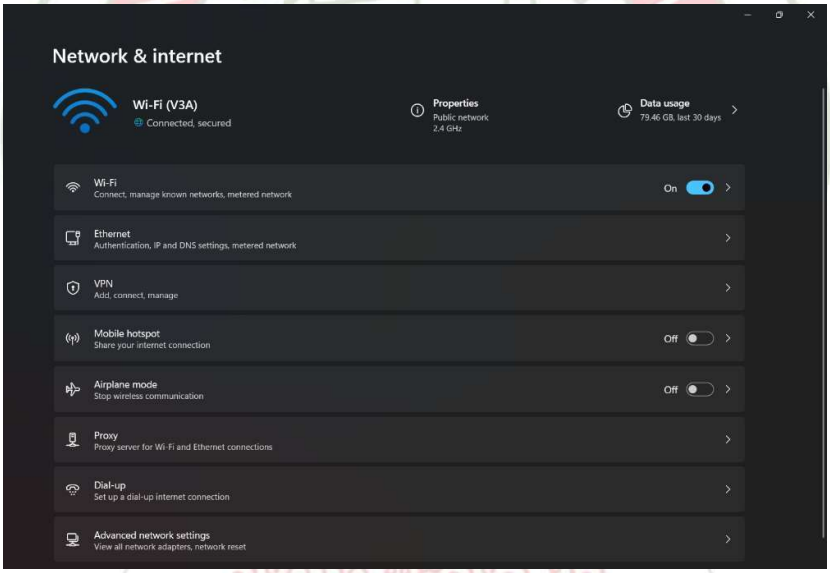
IPv6, the latest Internet Protocol version, succeeds IPv4 to overcome the limitations of address exhaustion in the face of the internet's rapid growth. With 128-bit addresses, IPv6 offers a vast address space, a significant upgrade from IPv4's 32-bit structure. This extended space accommodates an almost limitless number of unique IP addresses. Represented in hexadecimal notation, IPv6 addresses consist of eight groups of four digits separated by colons, exemplified by "2001:0db8:85a3:0000:0000:8a2e:0370:7334." This innovation ensures the continued expansion of the internet and efficiently caters to the escalating number of connected devices.

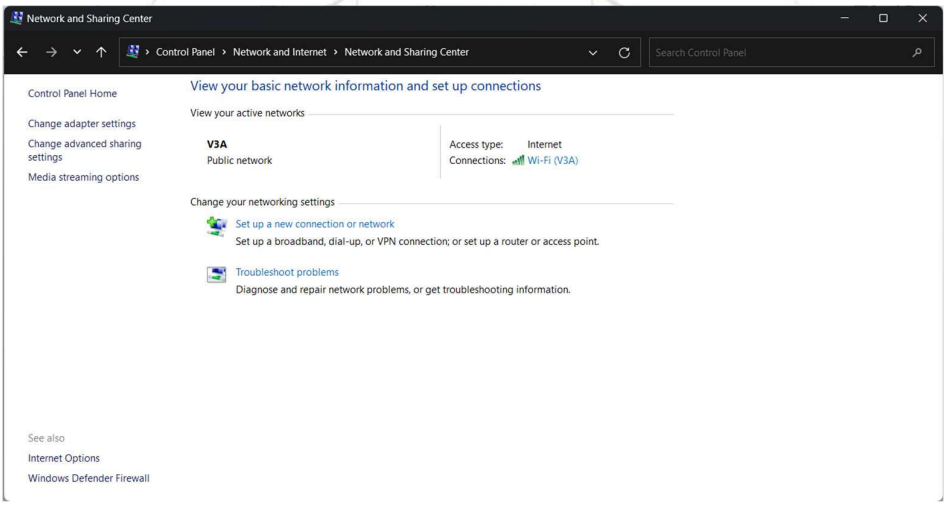
DNS (Domain Name System) Server –

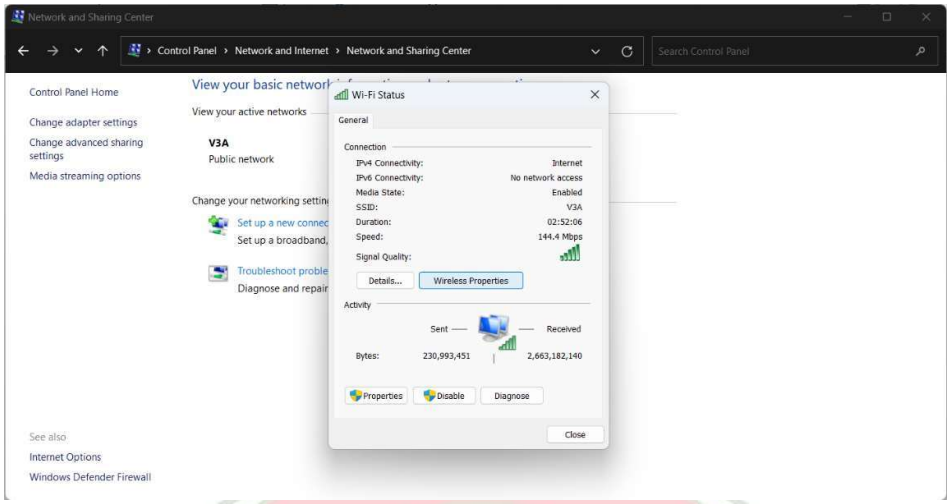
A Domain Name System (DNS) server is a crucial component of the internet infrastructure responsible for translating human-readable domain names into numerical IP addresses that computers use to identify each other on a network. Instead of users needing to remember and use IP addresses, such as "192.168.1.1," they can use domain names like www.example.com.

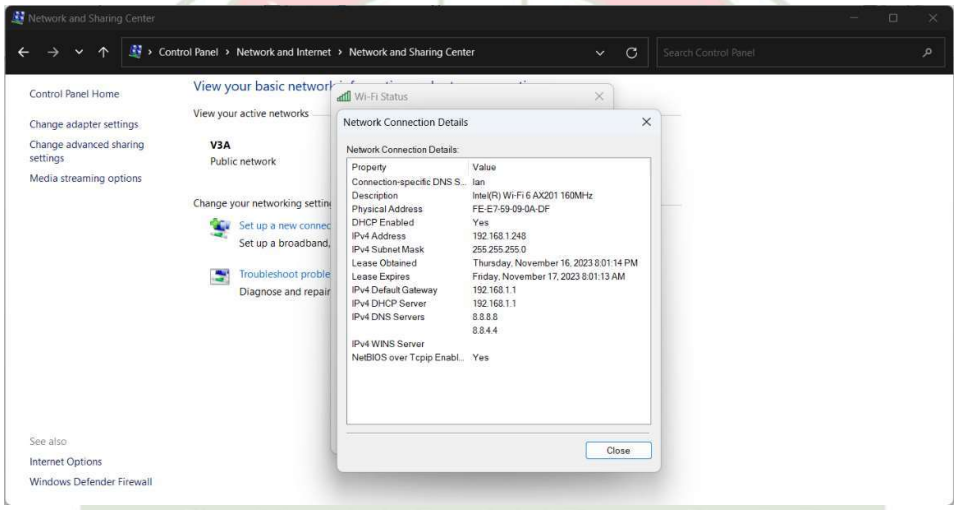
ALGORITHM:

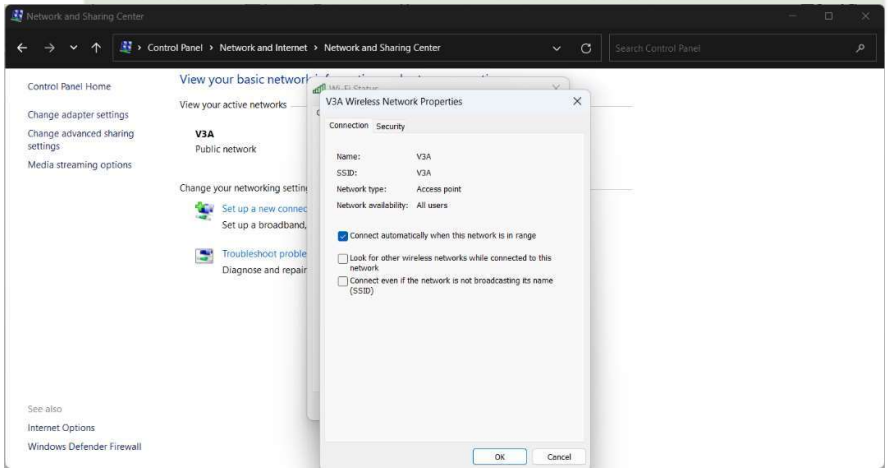
1. Start
2. Connect to the internet
3. Gather TCP/IP configuration information
4. Record IP address, Subnet Mask and Default gateway for the computer
5. Compare TCP/IP information with other computers
6. Check additional TCP/IP information
7. End

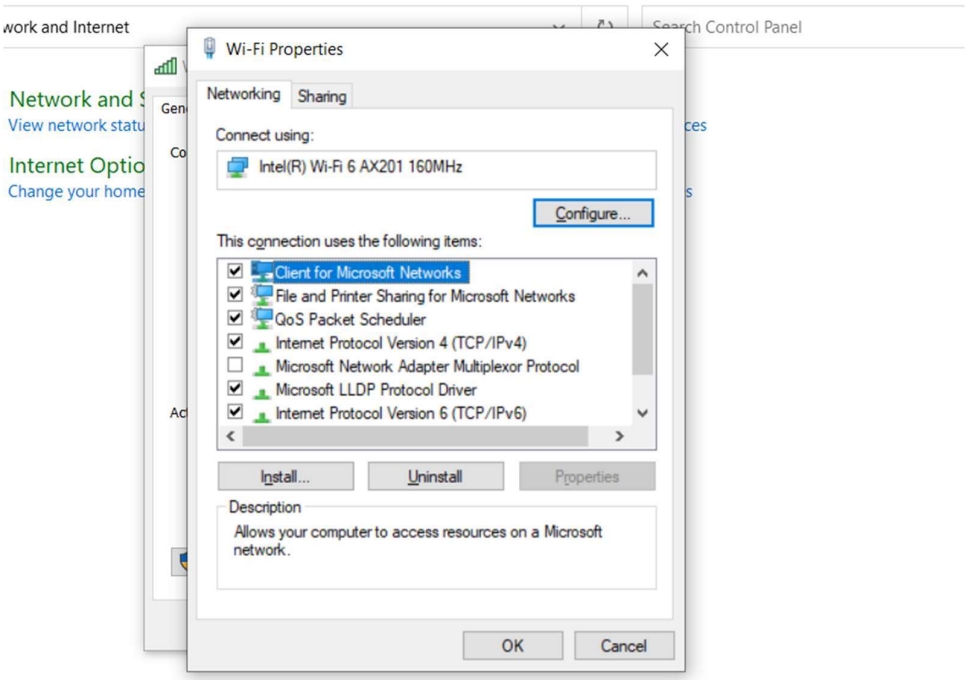


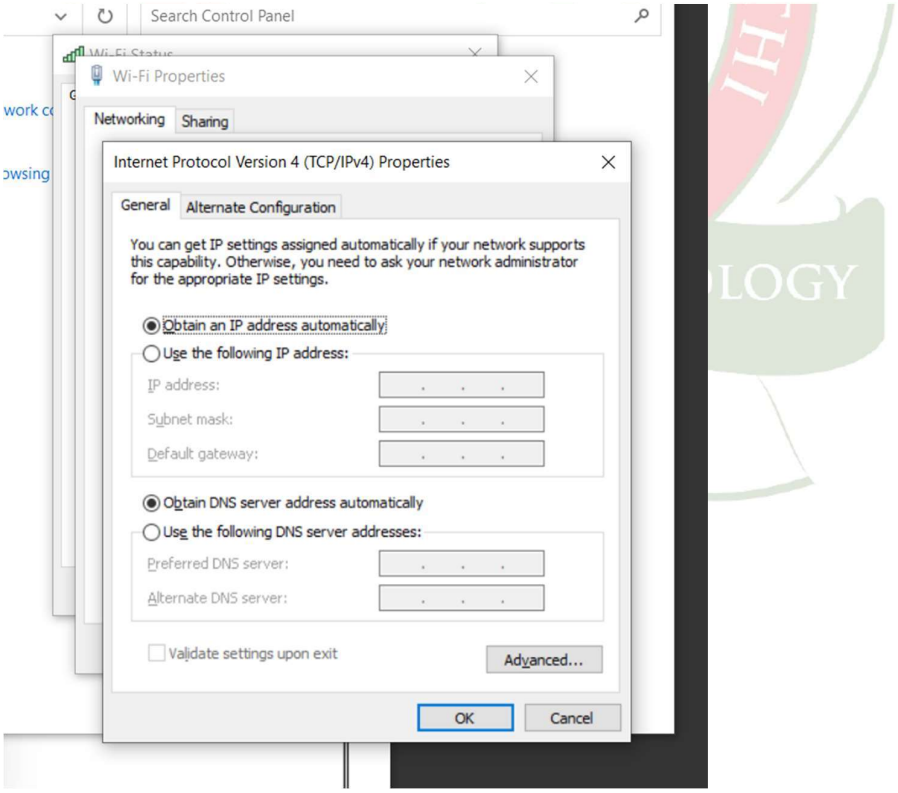












CONCLUSION: The network configuration of windows operating system is studied.

EXPERIMENT – 4

AIM: Analysis of network traces using Wireshark

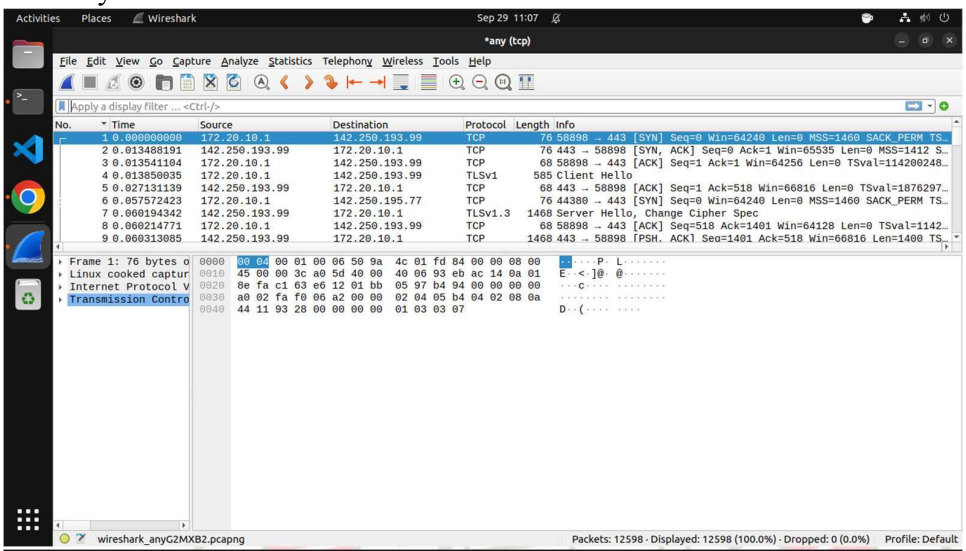
DESCRIPTION AND EXECUTION:

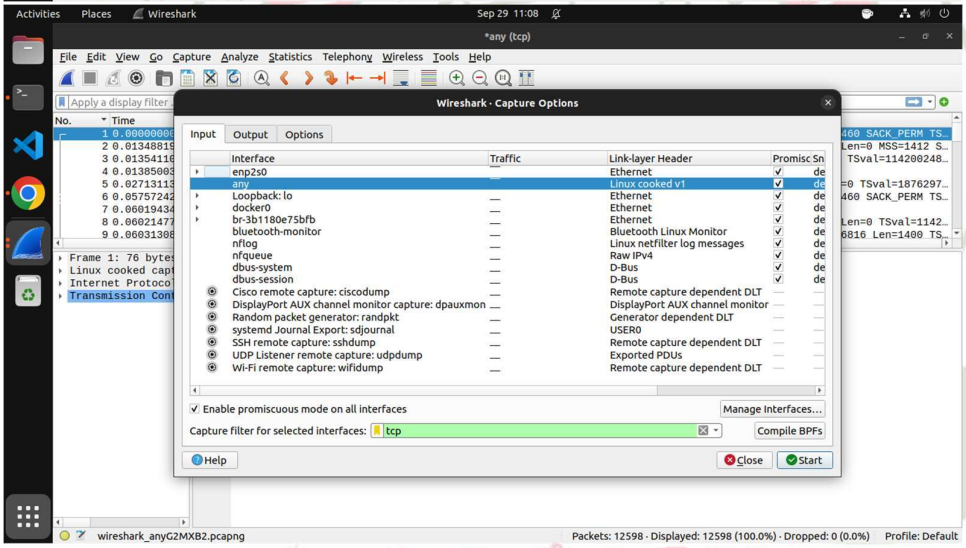
Wireshark is a widely used network protocol analyzer that allows you to capture and inspect the data traveling back and forth on a network in real-time. It is an open-source software and is available for various operating systems, including Windows, macOS, and Linux.

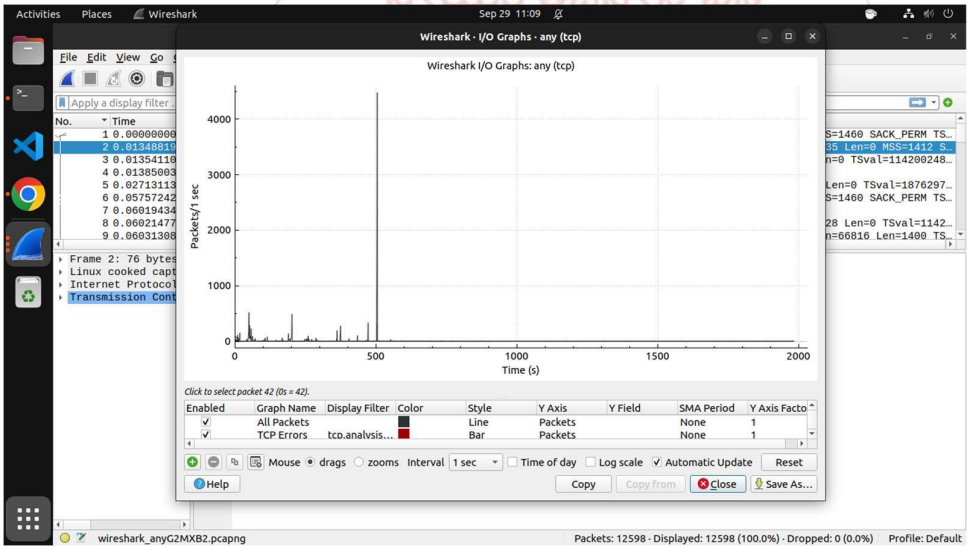
Key features of Wireshark include:

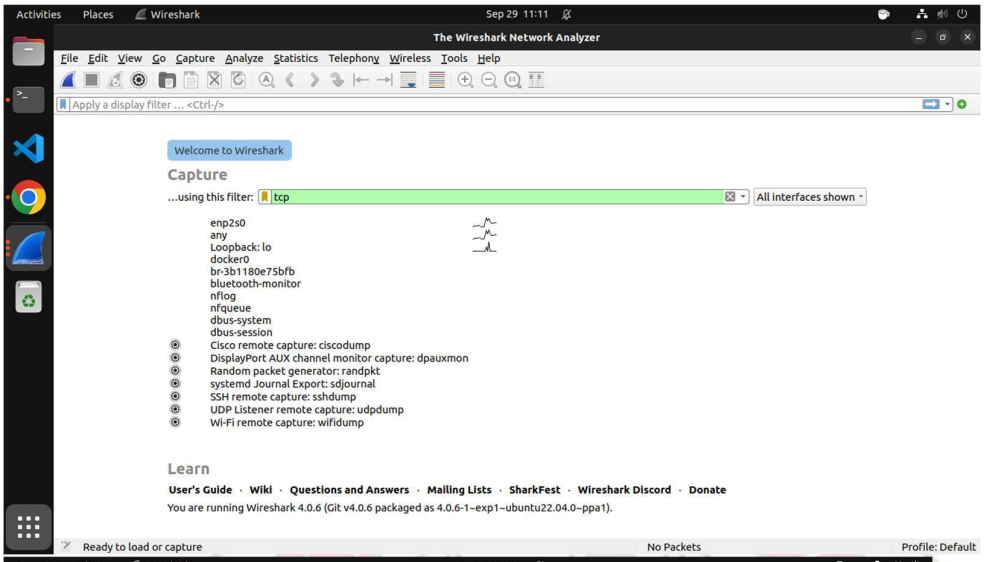
1. Packet Capture: Wireshark captures and displays the packets (units of data transmitted over a network) in real-time. It can capture data from a network interface or read from a previously captured file.
2. Protocol Analysis: It supports a wide range of network protocols, making it a versatile tool for analyzing and dissecting network traffic. Wireshark can interpret and display information about protocols at various layers of the OSI model.
3. Live Analysis and Offline Analysis: Wireshark can capture and analyze data in real-time as it is transmitted over a network. It can also analyze saved capture files, allowing for post-event analysis.
4. Filtering and Search: Wireshark provides powerful filtering options that allow users to focus on specific packets based on criteria such as source or destination address, protocol type, and more. This makes it easier to analyze specific aspects of network traffic.
5. Colorization and Graphs: The tool colorizes packets based on the protocol, making it visually intuitive to identify different types of traffic. Additionally, Wireshark can generate various graphs to visualize aspects of network performance.
6. Exporting Data: Users can export captured data to various file formats, including plain text, CSV, XML, or other formats suitable for use in other tools or for further analysis.
7. Security Analysis: Wireshark is often used for security analysis and troubleshooting. It can help identify security vulnerabilities, detect network attacks, and analyze the behavior of networked applications.

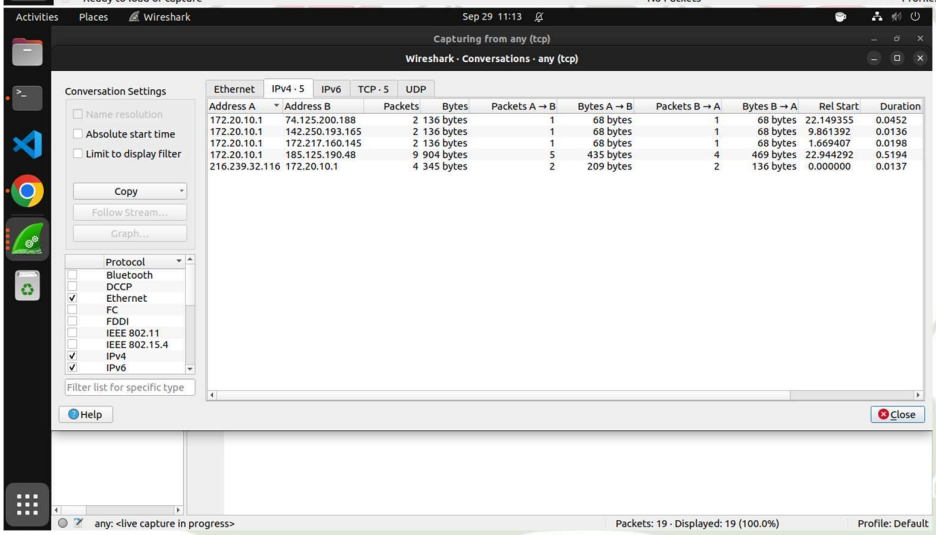
TCP-any


Activities Places Wireshark Sep 29 11:07
*any (tcp)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
No. Time Source Destination Protocol Length Info
1 0.000000000 172.20.10.1 142.250.193.99 TCP 76 58898 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TS...
2 0.013488191 142.250.193.99 172.20.10.1 TCP 76 443 → 58898 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1412 S...
3 0.013541104 172.20.10.1 142.250.193.99 TCP 68 58898 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=114200248...
4 0.013850035 172.20.10.1 142.250.193.99 TLSv1 585 Client Hello
5 0.027131139 142.250.193.99 172.20.10.1 TCP 68 443 → 58898 [ACK] Seq=1 Ack=518 Win=66816 Len=0 TSval=1876297...
6 0.057572423 172.20.10.1 142.250.195.77 TCP 76 44380 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TS...
7 0.060194342 142.250.193.99 172.20.10.1 TLSv1.3 1468 Server Hello, Change Cipher Spec
8 0.060214771 172.20.10.1 142.250.193.99 TCP 68 58898 → 443 [ACK] Seq=518 Ack=1401 Win=64128 Len=0 TSval=1142...
9 0.060313085 142.250.193.99 172.20.10.1 TCP 1468 443 → 58898 [PSH, ACK] Seq=1401 Ack=518 Win=66816 Len=1400 TS...
Frame 1: 76 bytes o
Linux cooked captur
Internet Protocol V
Transmission Contro
0000 00 04 00 01 00 06 50 9a 4c 01 fd 84 00 00 08 00
0010 45 00 00 3c a0 5d 40 00 40 06 93 eb ac 14 0a 01
0020 8e fa c1 63 e6 12 01 bb 05 97 b4 94 00 00 00 00
0030 a0 02 fa f0 06 a2 00 00 02 04 05 b4 04 02 08 0a
0040 44 11 93 28 00 00 00 00 01 03 03 07
wireshark_anyG2MXB2.pcapng
Packets: 12598 · Displayed: 12598 (100.0%) · Dropped: 0 (0.0%) Profile: Default

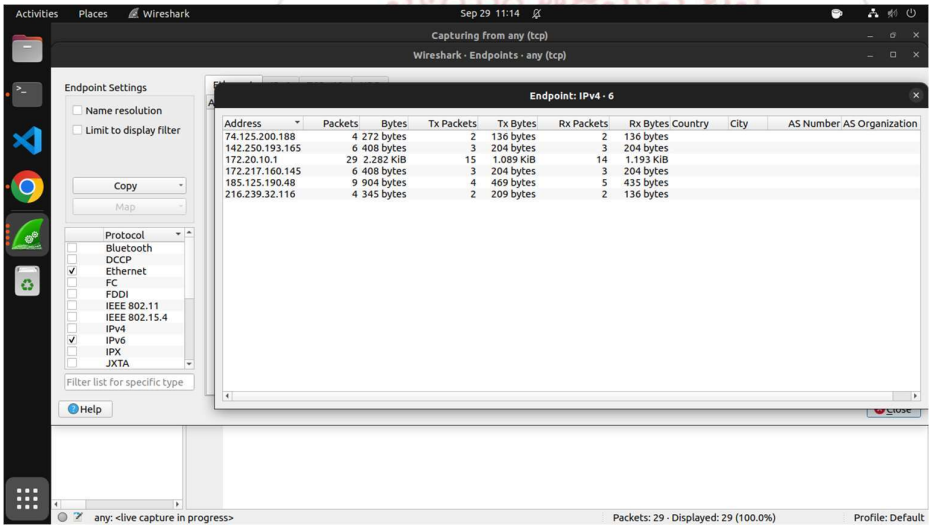

Activities Places Wireshark Sep 29 11:08
*any (tcp)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Capture Options
Input Output Options
Interface Traffic Link-layer Header Promisc Sn
enp2s0 Ethernet de
any Linux cooked v1 de
Loopback: lo Ethernet de
docker0 Ethernet de
br-3b1180e75bfb Ethernet de
bluetooth-monitor Bluetooth Linux Monitor de
nflog Linux netfilter log messages de
nfqueue Raw IPv4 de
dbus-system D-Bus de
dbus-session D-Bus de
Cisco remote capture: ciscodump Remote capture dependent DLT
DisplayPort AUX channel monitor capture: dpauxmon DisplayPort AUX channel monitor
Random packet generator: randpkt Generator dependent DLT
systemd Journal Export: sdjournal USER0
SSH remote capture: sshdump Remote capture dependent DLT
UDP Listener remote capture: udpdump Exported PDUs
Wi-Fi remote capture: wifidump Remote capture dependent DLT
Enable promiscuous mode on all interfaces
Manage Interfaces...
Capture filter for selected interfaces: tcp
Compile BPFs
Help Close Start
wireshark_anyG2MXB2.pcapng
Packets: 12598 · Displayed: 12598 (100.0%) · Dropped: 0 (0.0%) Profile: Default

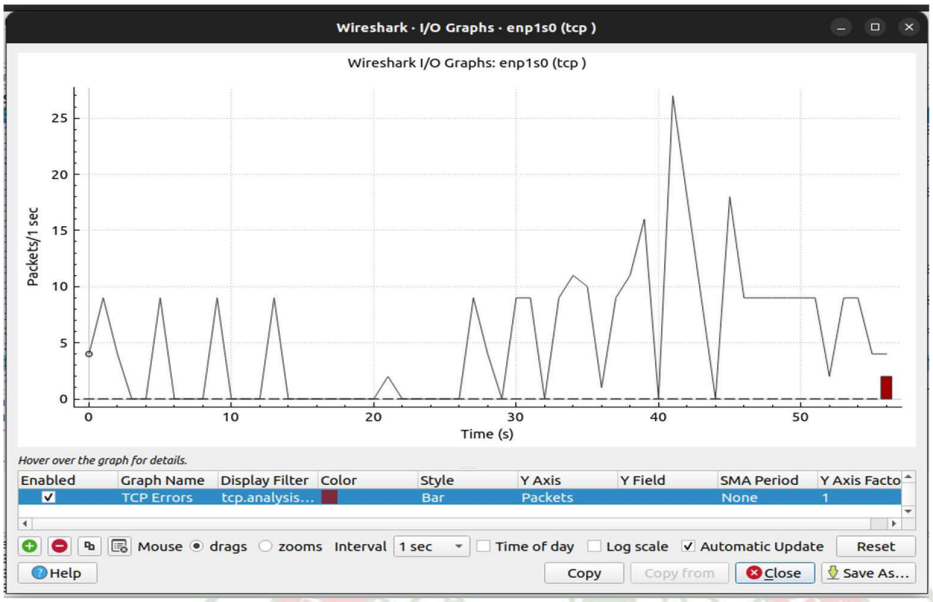

Activities Places Wireshark Sep 29 11:09
Wireshark · I/O Graphs · any (tcp)
Wireshark I/O Graphs: any (tcp)
Packets/1 sec
Time (s)
0
1000
2000
3000
4000
500
1500
Click to select packet 42 (0s = 42).
Enabled Graph Name Display Filter Color Style Y Axis Y Field SMA Period Y Axis Facto
All Packets Line Packets None 1
TCP Errors tcp.analysis... Bar Packets None 1
Mouse drags zooms Interval 1 sec Time of day Log scale Automatic Update Reset
Help Copy Copy from Close Save As...
wireshark_anyG2MXB2.pcapng
Packets: 12598 · Displayed: 12598 (100.0%) · Dropped: 0 (0.0%) Profile: Default

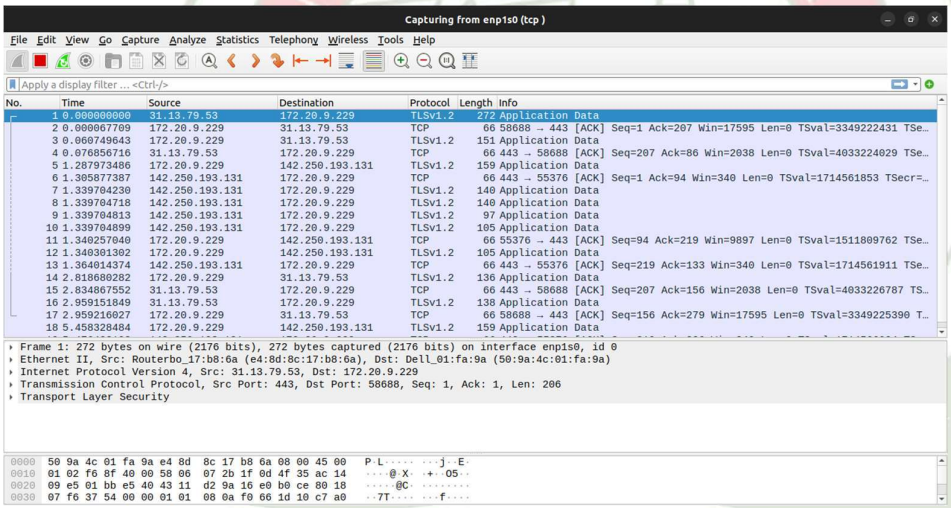

Activities
Places
Wireshark
Sep 29 11:11
The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter: tcp
All interfaces shown
enp2s0
any
Loopback: lo
docker0
br-3b1180e75bfb
bluetooth-monitor
nflog
nfqueue
dbus-system
dbus-session
Cisco remote capture: ciscodump
DisplayPort AUX channel monitor capture: dpauxmon
Random packet generator: randpkt
systemd Journal Export: sdjournal
SSH remote capture: sshdump
UDP Listener remote capture: udpdump
Wi-Fi remote capture: wifidump
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate
You are running Wireshark 4.0.6 (Git v4.0.6 packaged as 4.0.6-1~exp1~ubuntu22.04.0~ppa1).
Ready to load or capture
No Packets
Profile: Default


Activities
Places
Wireshark
Sep 29 11:13
Capturing from any (tcp)
Wireshark · Conversations · any (tcp)
Conversation Settings
Name resolution
Absolute start time
Limit to display filter
Copy
Follow Stream...
Graph...
Ethernet
IPv4 · 5
IPv6
TCP · 5
UDP
Address A Address B Packets Bytes Packets A → B Bytes A → B Packets B → A Bytes B → A Rel Start Duration
172.20.10.1 74.125.200.188 2 136 bytes 1 68 bytes 1 68 bytes 22.149355 0.0452
172.20.10.1 142.250.193.165 2 136 bytes 1 68 bytes 1 68 bytes 9.861392 0.0136
172.20.10.1 172.217.160.145 2 136 bytes 1 68 bytes 1 68 bytes 1.669407 0.0198
172.20.10.1 185.125.190.48 9 904 bytes 5 435 bytes 4 469 bytes 22.944292 0.5194
216.239.32.116 172.20.10.1 4 345 bytes 2 209 bytes 2 136 bytes 0.000000 0.0137
Protocol
Bluetooth
DCCP
Ethernet
FC
FDDI
IEEE 802.11
IEEE 802.15.4
IPv4
IPv6
Filter list for specific type
Help
Close
any: <live capture in progress>
Packets: 19 · Displayed: 19 (100.0%)
Profile: Default

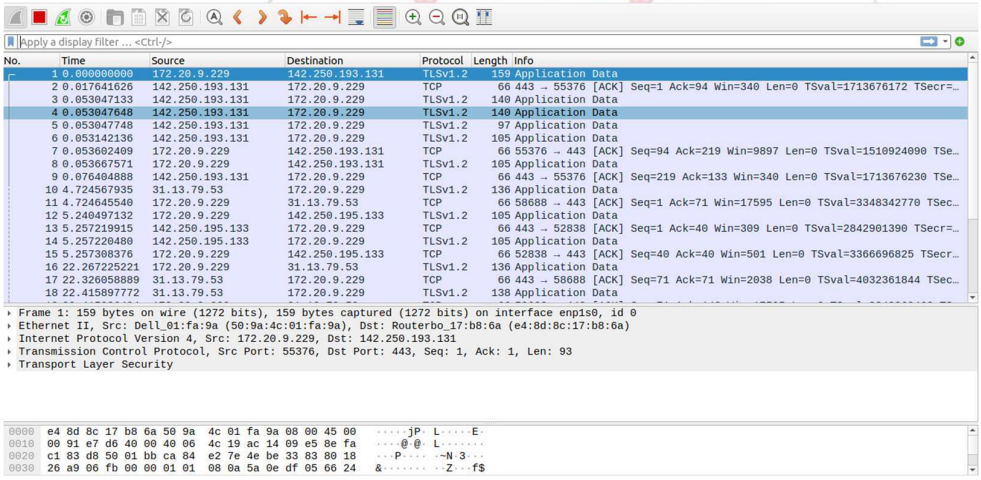
TCP- IPv6

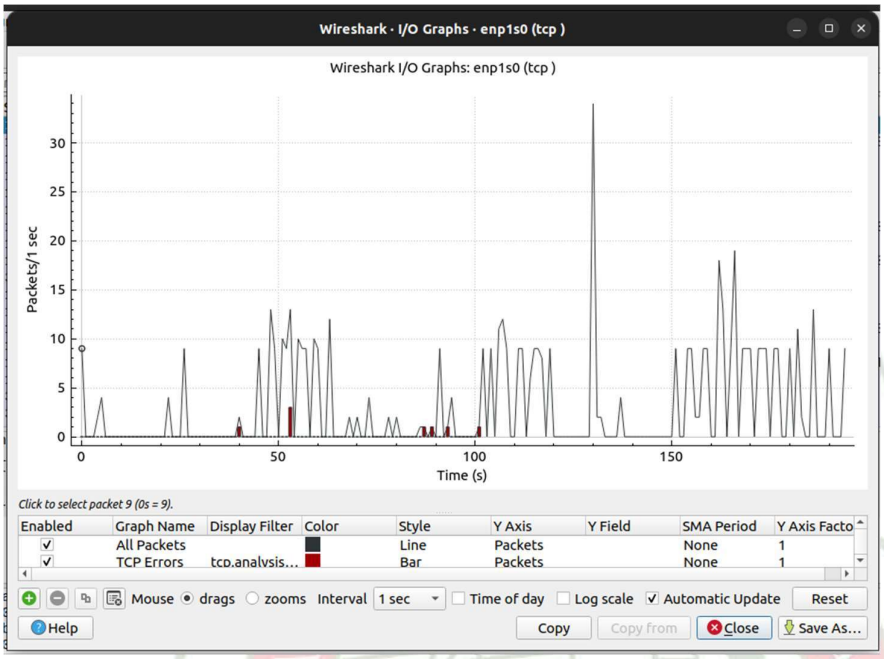

Activities
Places
Wireshark
Sep 29 11:14
Capturing from any (tcp)
Wireshark · Endpoints · any (tcp)
Endpoint Settings
Name resolution
Limit to display filter
Copy
Map
Endpoint: IPv4 · 6
Address Packets Bytes Tx Packets Tx Bytes Rx Packets Rx Bytes Country City AS Number AS Organization
74.125.200.188 4 272 bytes 2 136 bytes 2 136 bytes
142.250.193.165 6 408 bytes 3 204 bytes 3 204 bytes
172.20.10.1 29 2.282 KiB 15 1.089 KiB 14 1.193 KiB
172.217.160.145 6 408 bytes 3 204 bytes 3 204 bytes
185.125.190.48 9 904 bytes 4 469 bytes 5 435 bytes
216.239.32.116 4 345 bytes 2 209 bytes 2 136 bytes
Protocol
Bluetooth
DCCP
Ethernet
FC
FDDI
IEEE 802.11
IEEE 802.15.4
IPv4
IPv6
IPX
JXTA
Filter list for specific type
Help
any: <live capture in progress>
Packets: 29 · Displayed: 29 (100.0%)
Profile: Default



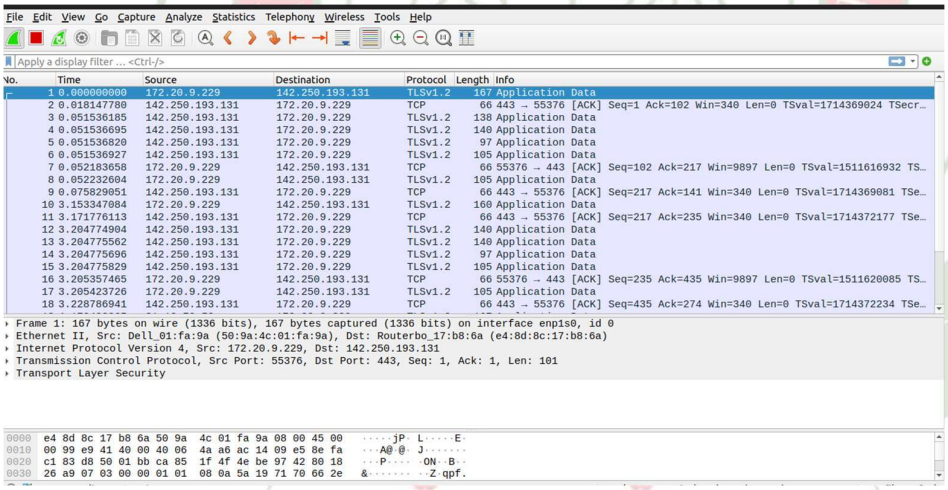


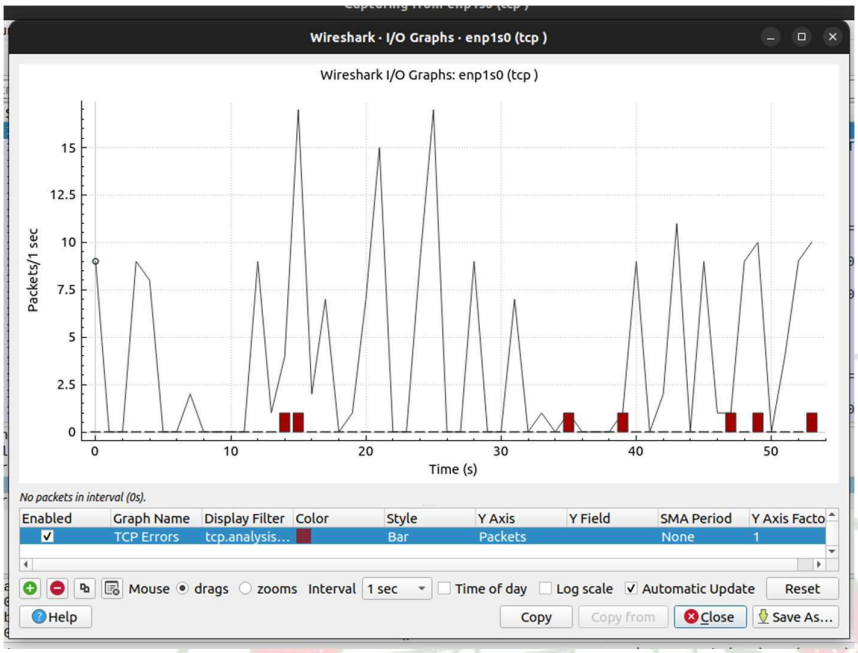
TCP-IPv4 address 192.0.2.1





TCP IPV4 only





RESULT: The packets received and sent are analysed using filters in Wireshark.

EXPERIMENT – 5

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

DESCRIPTION:

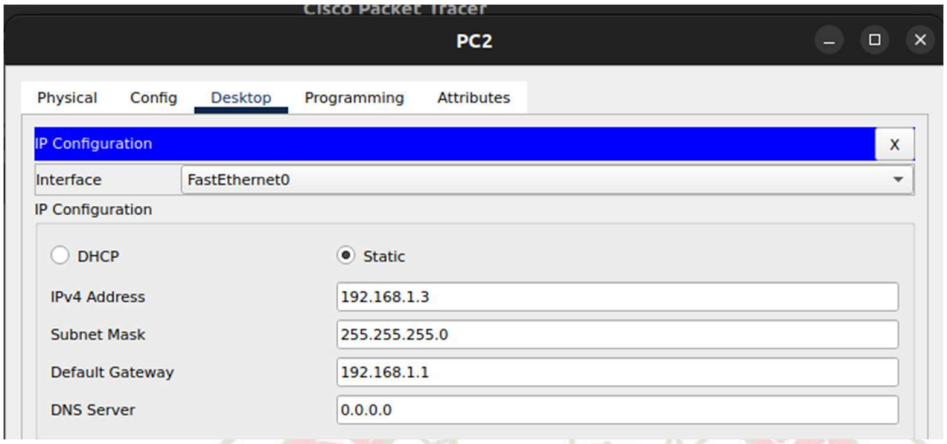
Packet Tracer is a cross-platform visual simulation tool designed by Cisco Systems that allows users to create network topologies and imitate modern computer networks. The software allows users to simulate the configuration of Cisco routers and switches using a simulated command line interface.

To build a switch based network:

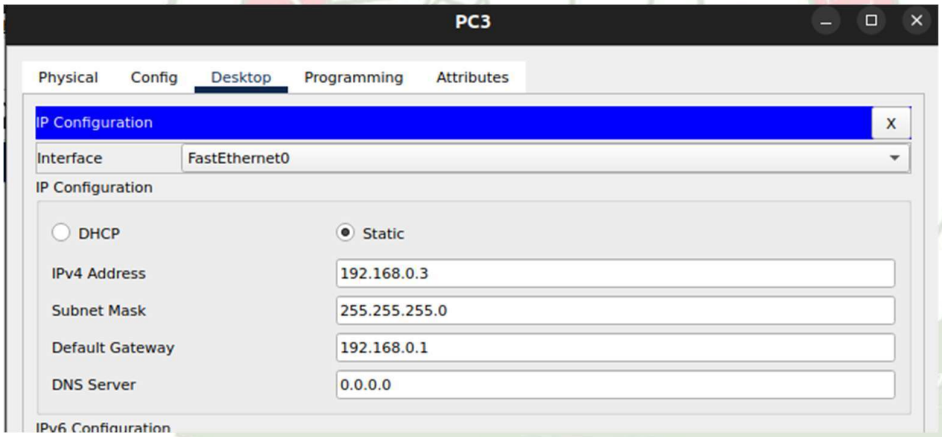
- Open packet tracker.
- At the bottom we can find many options such as network devices, end device, components, connections etc.
- Select end devices and then choose two PCs, switch-PT and router 1941.
- Connect all the devices as shown in the below figure, using copper straight-through wire.
- Change the configuration of the devices accordingly.
- For PC2, set the IPv4 address to 192.168.1.3, the subnet mask to 255.255.255.0 and the default gateway as 192.168.1.1.
- For PC3, set the IPv4 address to 192.168.1.1, the subnet mask to 255.255.255.0 and the default gateway as 192.168.1.3.
- To configure a router, for router gigabit ethernet 0/0 set the IPv4 address as 192.168.1.1(which is the default gateway address of PC2) and subnet mask as 255.255.255.0.
- Similarly for router gigabit ethernet 0/1 set the IPv4 address as 192.168.0.1(default gateway of PC3) and the subnet mask as 255.255.255.0.
- To configure the switch, go to command line interface (CLI) and type the below commands:
  - Interface VLAN1
  - Ip address 192.168.1.2 255.255.255.0
  - No shutdown

Switch based network:

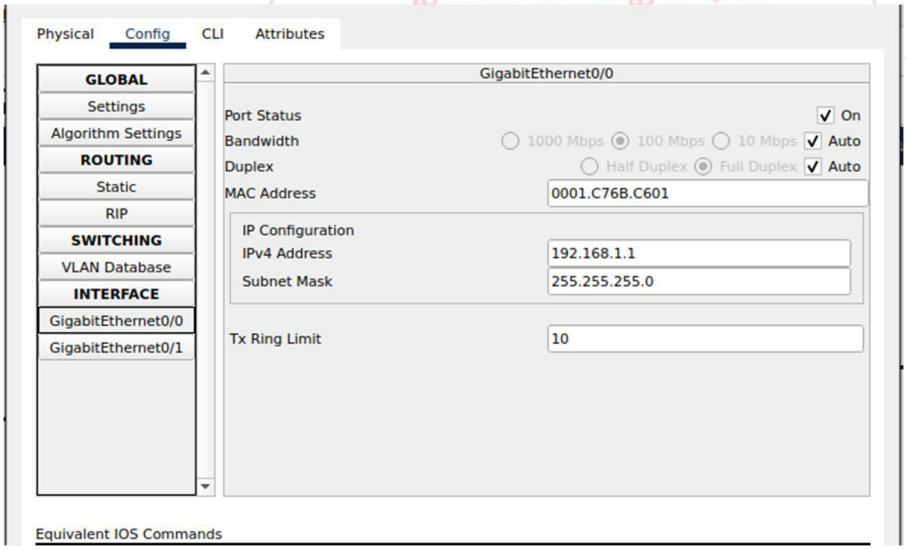
Configuration of First PC:



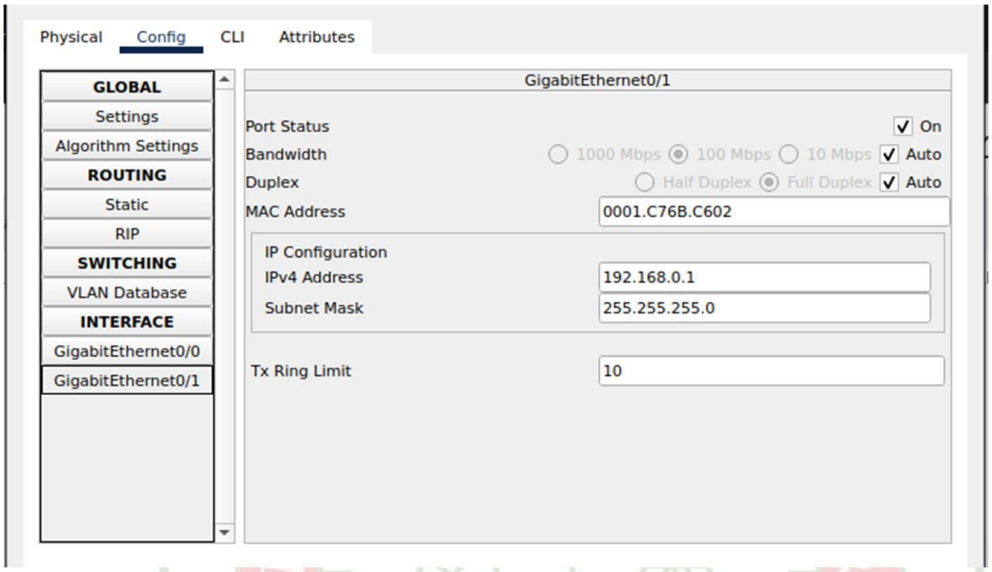
Configuration of second PC:



Configuration of router: GigabitEthernet0/0



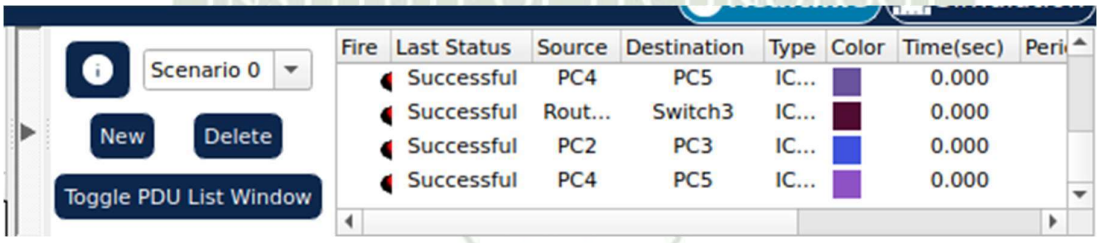
GigabitEthernet0/1



Configuration of switch:

```
Switch(config)#interface VLAN1
Switch(config-if)#ip address 192.168.1.2
% Incomplete command.
Switch(config-if)#ip address 192.168.1.2 255.255.255.0
Switch(config-if)#no shutdown
```

Result :



CONCLUSION:

We can see that the packet is successfully transmitted from PC4 to PC5. Thus the configurations and connections are correct.

EXPERIMENT – 6

AIM: Configuration Of Cisco Router 2900

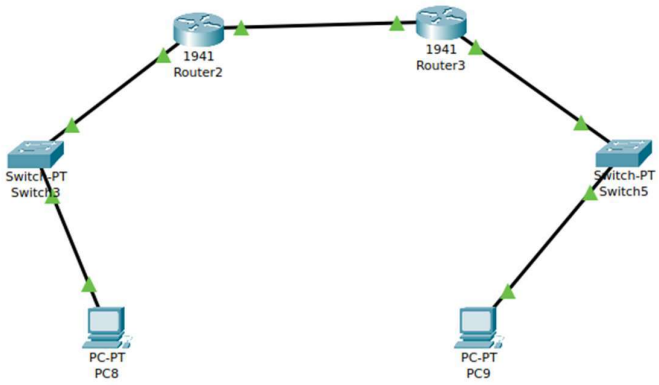
DESCRIPTION:

Configuring a Cisco router involves accessing the device through a command-line interface (CLI) and making configuration changes to various settings.

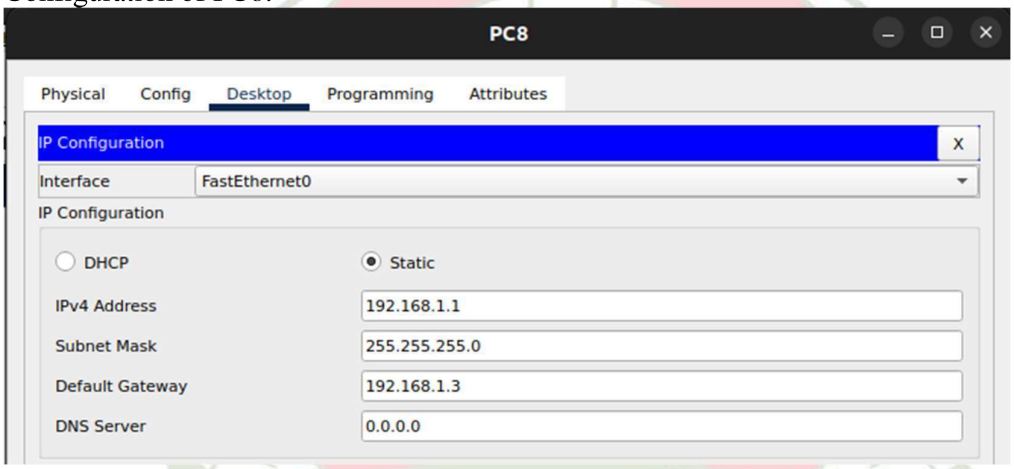
To configure a cisco router:

- Open packet tracker.
- At the bottom we can find many options such as network devices, end device, components, connections etc.
- Select end devices and then choose two PCs, 2 switch-PT and 2 routers- 1941.
- Connect all the devices as shown in the below figure, using copper straight-through wire.
- Change the configuration of the devices accordingly.
- For PC8, set the IPv4 address to 192.168.1.1, the subnet mask to 255.255.255.0 and the default gateway as 192.168.1.3.
- For PC9, set the IPv4 address to 192.168.2.1, the subnet mask to 255.255.255.0 and the default gateway as 192.168.2.3.
- To configure a router2, for router gigabit ethernet 0/0 set the IPv4 address as 192.168.1.3(which is the default gateway of PC8) and subnet mask as 255.255.255.0.
- Similarly, for router2 gigabit ethernet 0/1 set the IPv4 address as 192.168.3.1 and the subnet mask as 255.255.255.0.
- In the routing options, go to static and add the network 192.168.2.0 and the next hop as 192.168.3.2 for router2.
- To configure a router3, for router gigabit ethernet 0/0 set the IPv4 address as 192.168.2.3(which is the default gateway of PC9) and subnet mask as 255.255.255.0.
- Similarly, for router3 gigabit ethernet 0/1 set the IPv4 address as 192.168.3.2 and the subnet mask as 255.255.255.0.
- In the routing options, go to static and add the network 192.168.1.0 and the next hop as 192.168.3.1 for router3.
- Make sure the port status is on while configuring the routers.
- To configure the switch3, go to command line interface (CLI) and type the below commands:
    - Interface VLAN1
    - Ip address 192.168.1.2 255.255.255.0
    - No shutdown
- To configure the switch3, go to command line interface (CLI) and type the below commands:
    - Interface VLAN1
    - Ip address 192.168.2.2 255.255.255.0
    - No shutdown

Configuration of router:



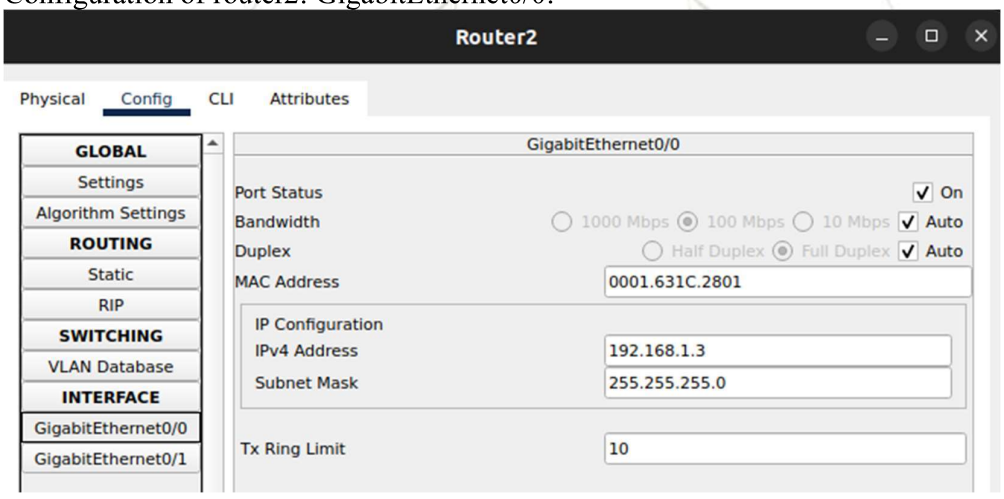
Configuration of PC8:



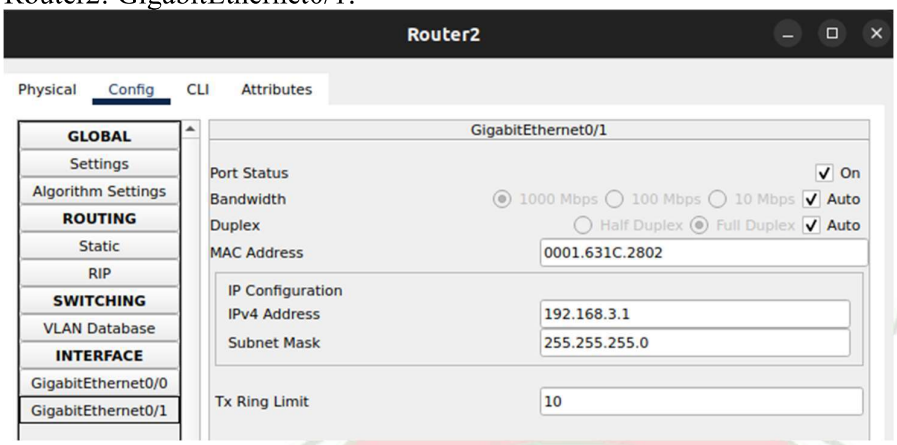
Configuration of Switch 3:

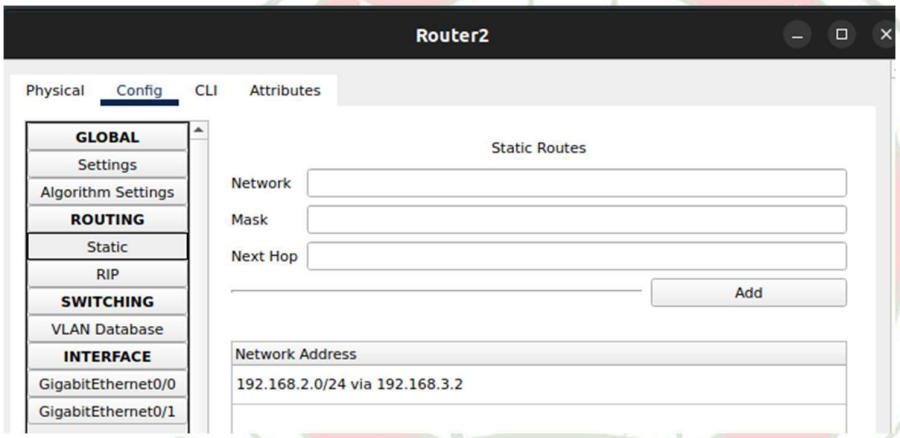
```
Switch(config-if)#interface VLAN1
Switch(config-if)#ip address 192.168.1.5 255.255.255.0
Switch(config-if)#no shutdown
```

Configuration of router2: GigabitEthernet0/0:

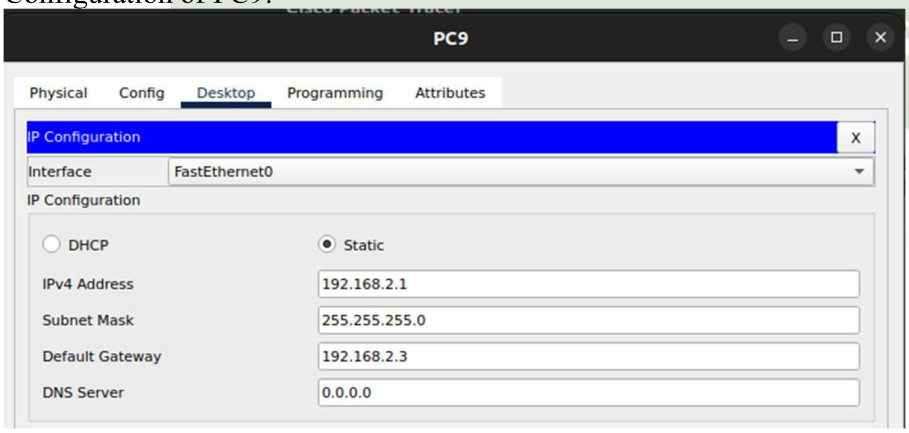


Router2: GigabitEthernet0/1:





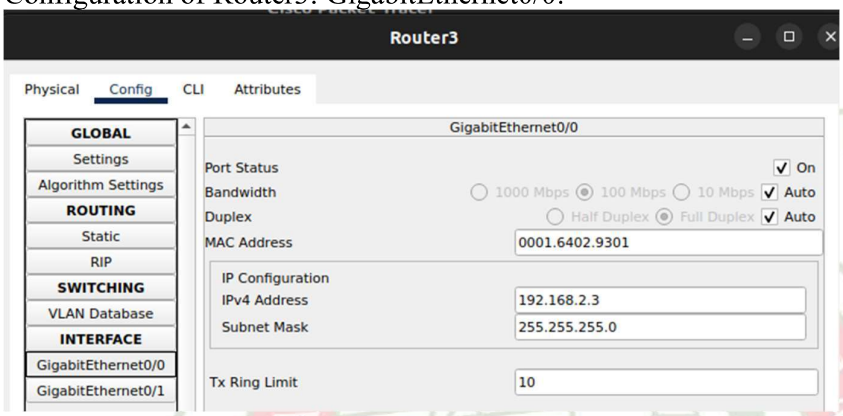
Configuration of PC9:



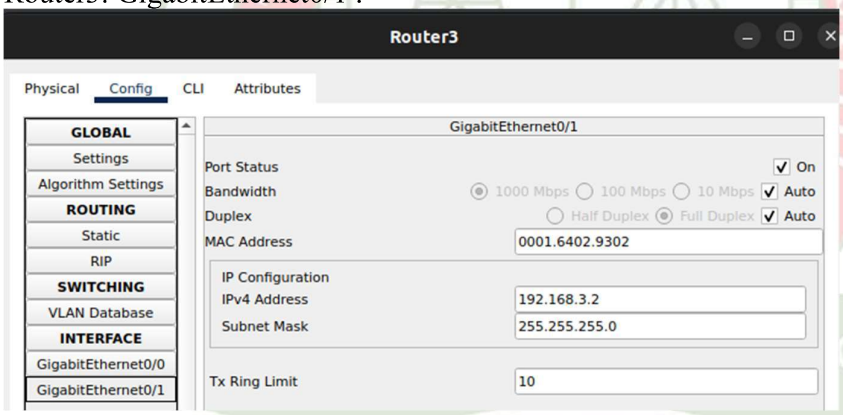
Configuration of switch 5:

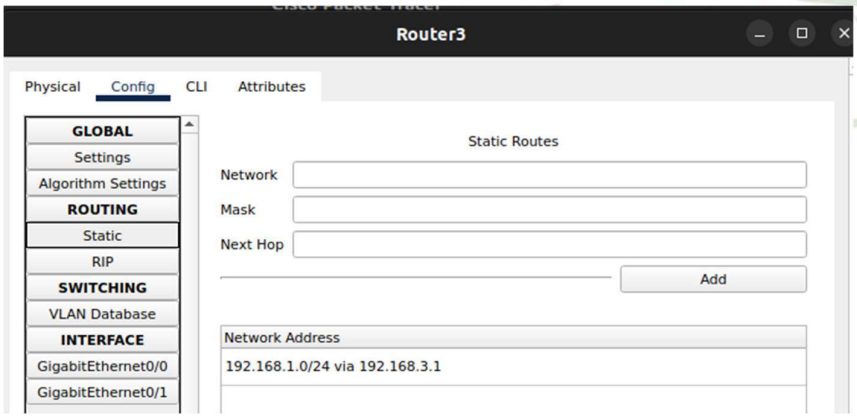
```
Switch(config)#interface FastEthernet0/1
Switch(config-if)#interface VLAN1
Switch(config-if)#ip address 192.168.2.2 255.255.255.0
Switch(config-if)#no shutdown

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

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

Configuration of Router3: GigabitEthernet0/0:

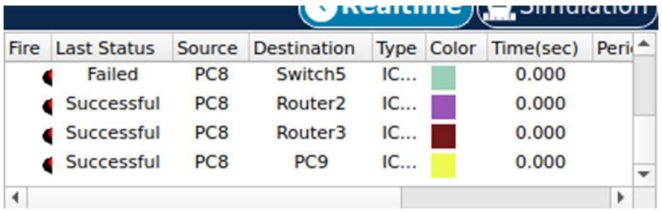


Router3: GigabitEthernet0/1 :





Result:



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Peri
	Failed	PC8	Switch5	IC...		0.000	
	Successful	PC8	Router2	IC...		0.000	
	Successful	PC8	Router3	IC...		0.000	
	Successful	PC8	PC9	IC...		0.000	

CONCLUSION: We can see that the packet is successfully transmitted from PC8 to PC9. Thus, the configurations and connections are correct.

EXPERIMENT - 7

AIM: Configuration of VLAN in Cisco switch

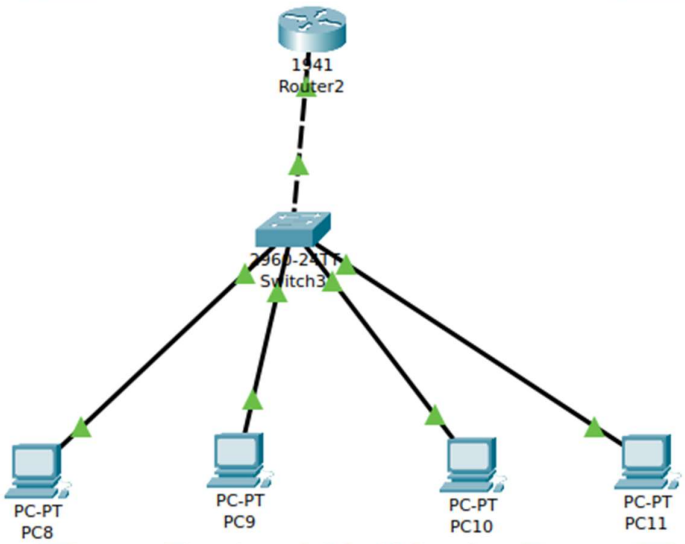
DESCRIPTION:

VLAN (Virtual Local Area Network) is a way to logically divide a physical network into separate, isolated segments. This segmentation helps improve network efficiency, security, and management by grouping devices based on criteria like function or department, even if they share the same physical infrastructure. VLANs allow for better control of broadcast traffic, enhanced security, and increased flexibility in network design.

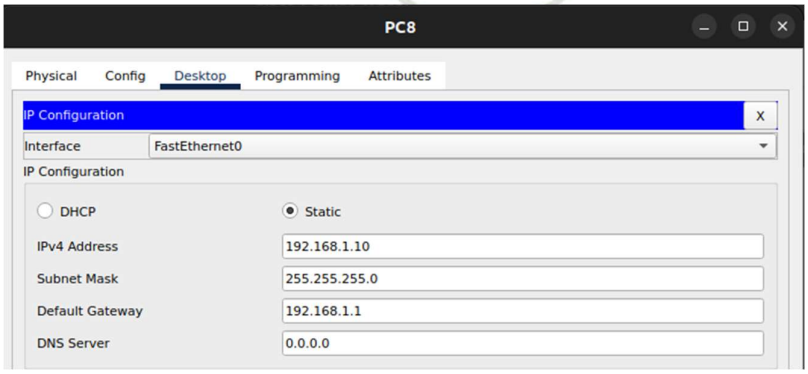
VLAN in Cisco switch:

- Open packet tracker.
- At the bottom we can find many options such as network devices, end device, components, connections etc.
- Select end devices and then choose 4 PCs, a switch-PT and a router- 1941.
- Connect all the devices as shown in the below figure, using connecting wires.
- Change the configuration of the devices accordingly.

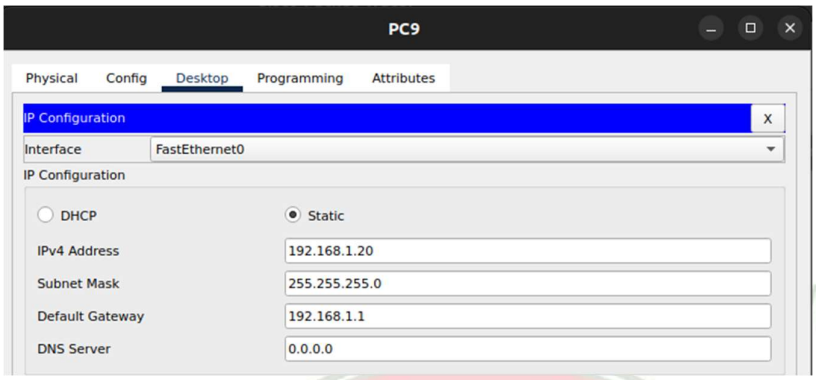
Configuration of VLAN:



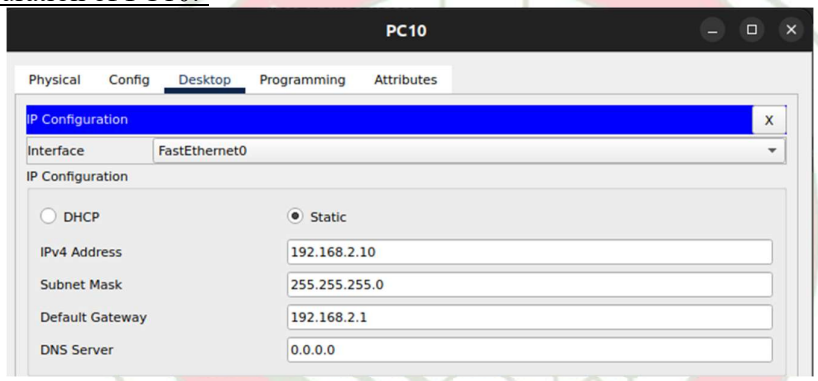
Configuration of PC8:



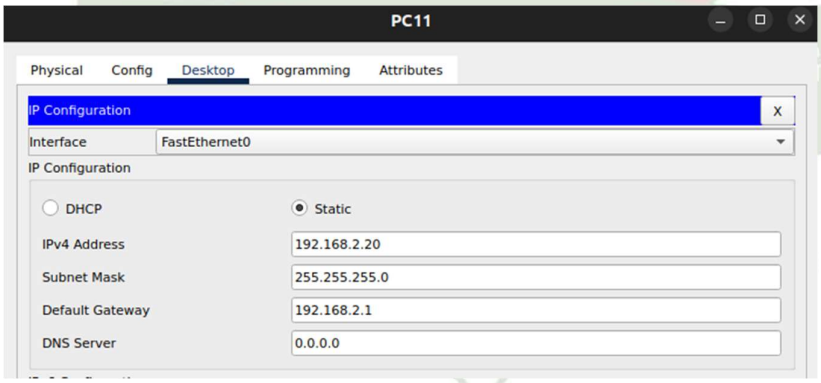
Configuration of PC9:



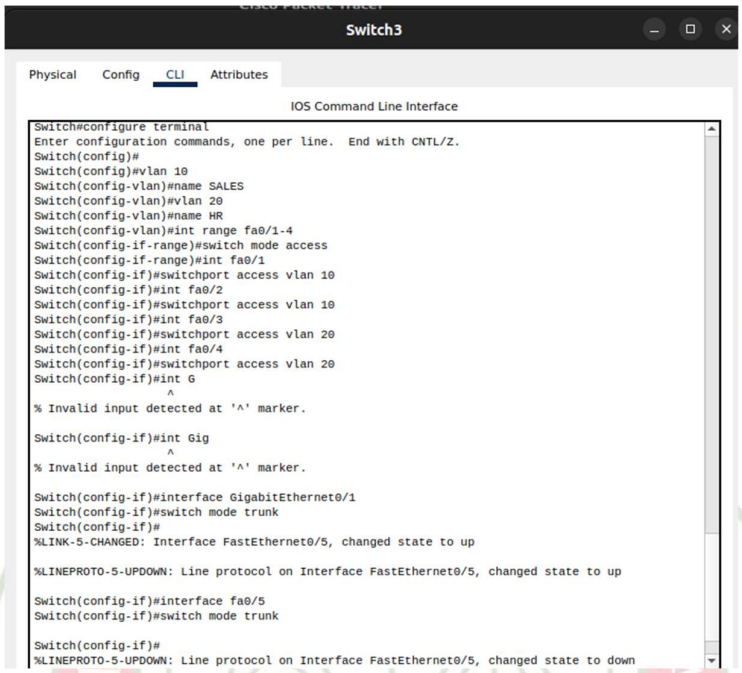
Configuration of PC10:



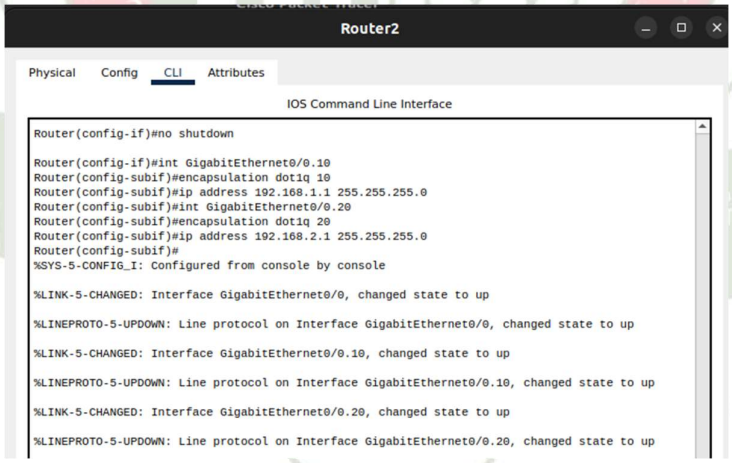
Configuration of PC11:



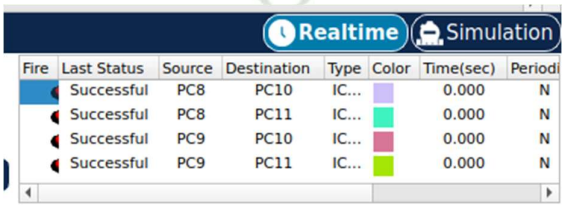
Configuration of switch:



Configuration of Router:



RESULT:



CONCLUSION:

We can see that the packet is successfully transmitted from PC8 to PC9. Thus the configurations and connections are correct.

EXPERIMENT -8

AIM: Develop different local area networks using GNS3. Connect two or more Local area networks. Explore various sub-netting options.

DESCRIPTION:

GNS3 stands for Graphical Network Simulator-3 which is an open source network software emulator that allows the combination of virtual and real networks, used to simulate complex network designs. It uses Dynamips emulation software to simulate Cisco IOS.

The resources utilized are 3 PCs, 1 switch.

Steps to create GNS3 topology with 3 PC's and 1 Switch:

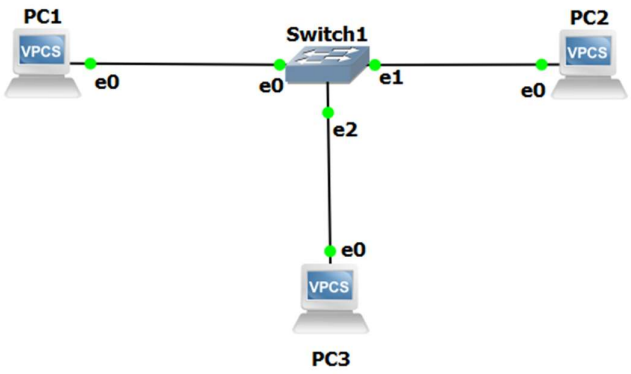
1) Click on **End devices** in the Devices Toolbar, drag and drop 3 instances of **VPCS** to the GNS3 Workspace

2) Click on **Switches** in the Devices Toolbar. Drag and drop the built-in ethernet switch

3) Click the **Add a Link** button, and add links from each PC to switch.

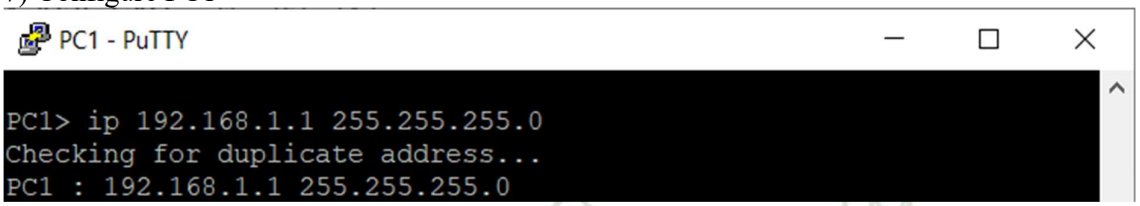
4) Click on the **Interface labels** button on the GNS3 Toolbar, which shows interfaces connected between devices.

5) Click the Green "Play" button on the GNS3 Toolbar to power on all devices in the topology.

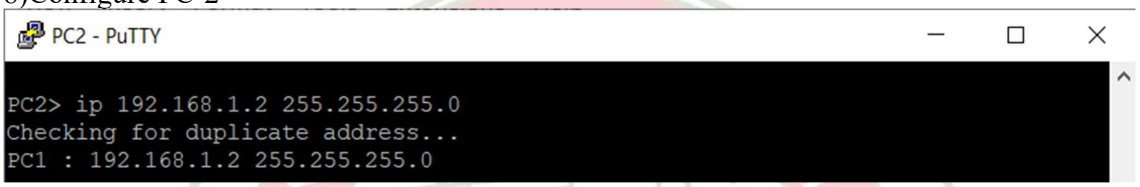


6) Click the **Console connect to all devices** button on the GNS3 Toolbar to open a connection to every device in the topology.

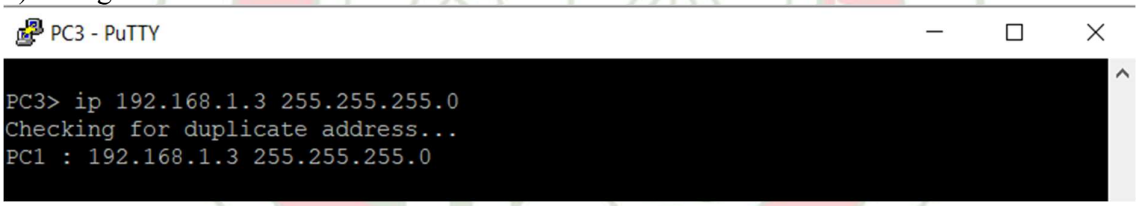
7) Configure PC1



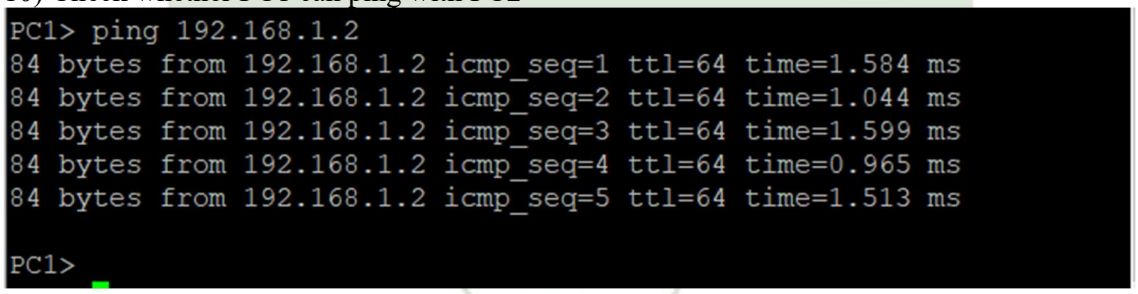
8)Configure PC-2



9)Configure PC3



10) Check whether PC1 can ping with PC2



11) Similarly, check with other PC's

RESULT: After the configuration and connection of all devices, the ping is successful between all the PC's

EXPERIMENT-9

AIM: Configure Static routing using GNS3 tool.

ALGORITHM:

1.Start

2.Setup the topology and initialise devices.

3.Configure devices and verify connectivity.

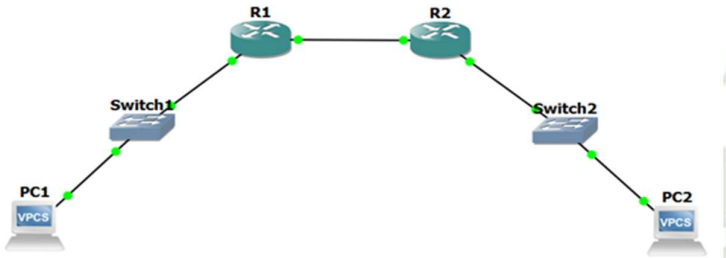
3.Display device information

4.End

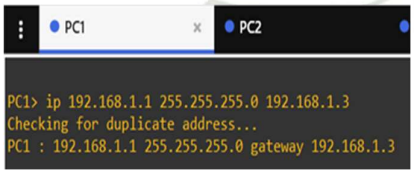
DESCRIPTION AND EXECUTION:

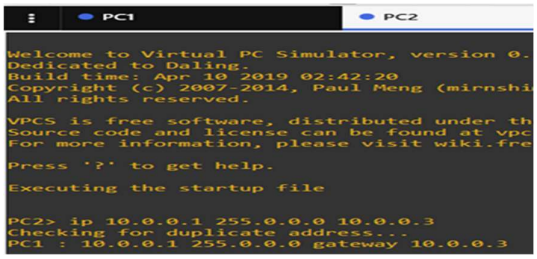
The resources utilized are 2 PCs, 2 switches and 2 routers.

Arrange the resources in the topology format given below and begin by configuring the PC's with IP addresses followed by configuration of the routers.

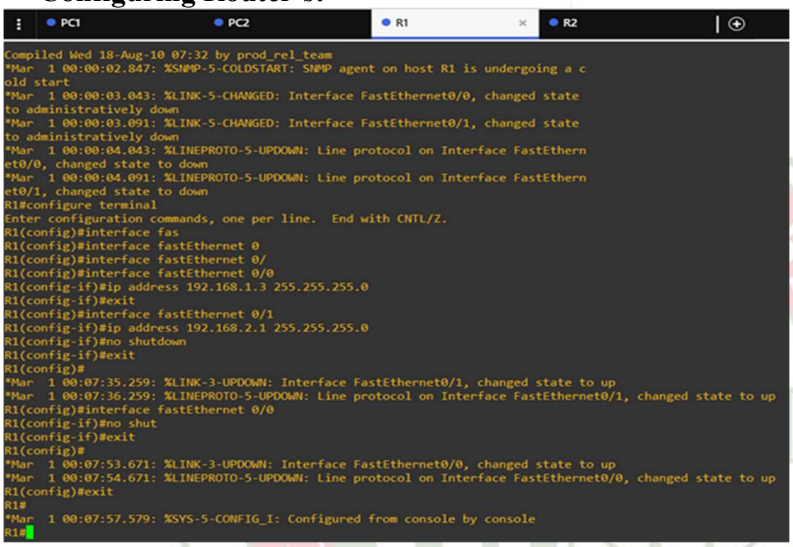


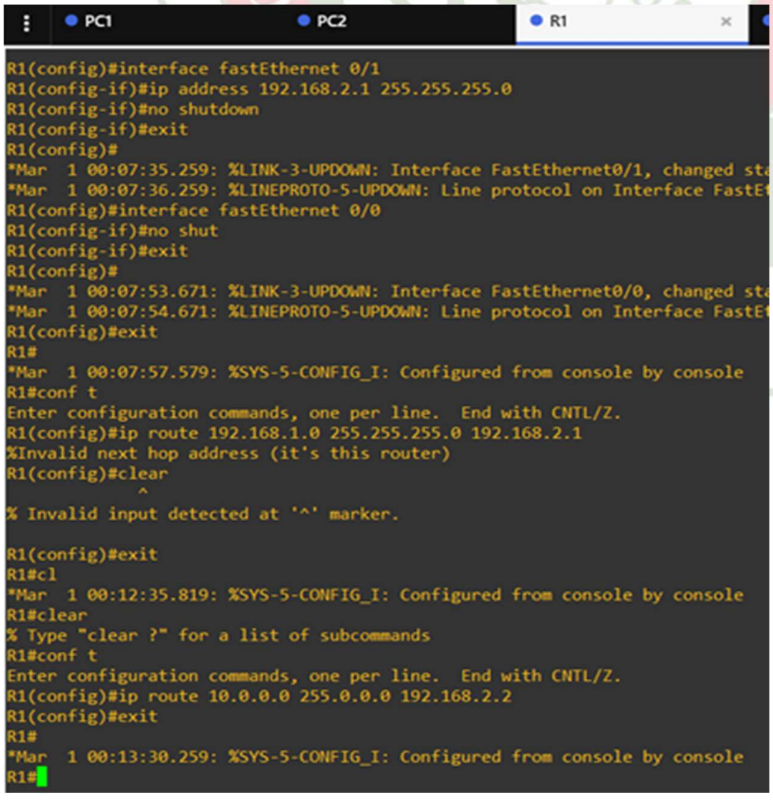
Configuring PC's:



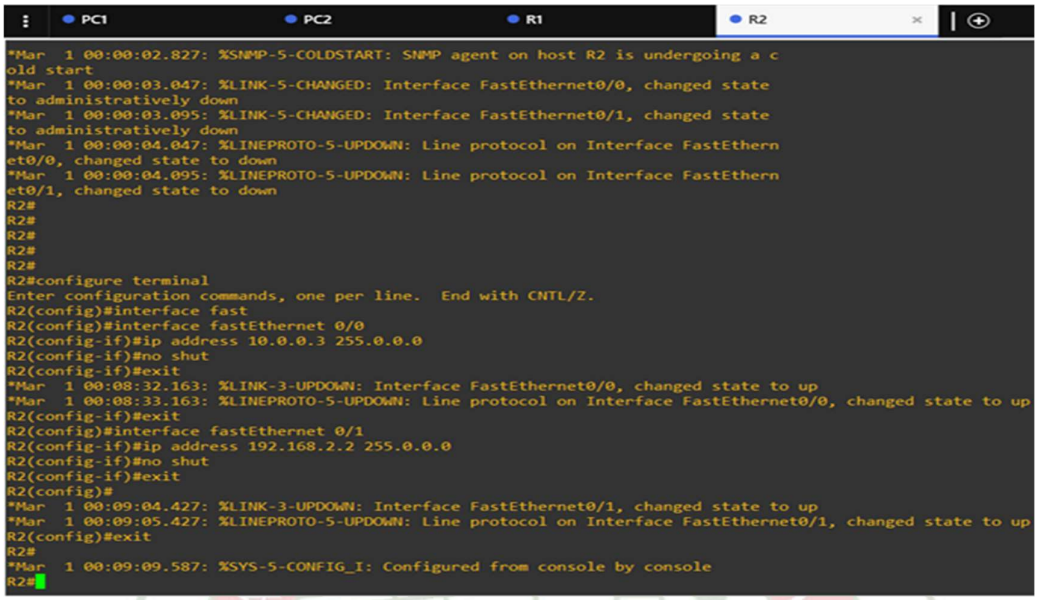


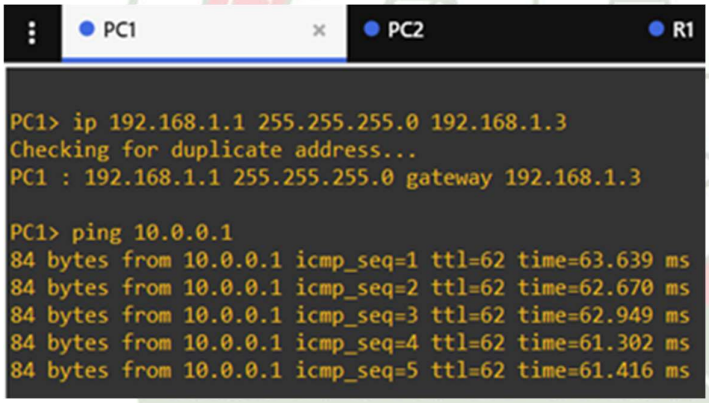
Configuring Router's:





Checking connection:





RESULT: After the configuration and connection of all devices, the ping is successful from PC1 to PC2

EXPERIMENT-10

AIM: Basic OSPF configuration using GNS3 tool.

ALGORITHM:

1.Start

2.Setup the topology and initialise devices.

3.Configure devices and verify connectivity.

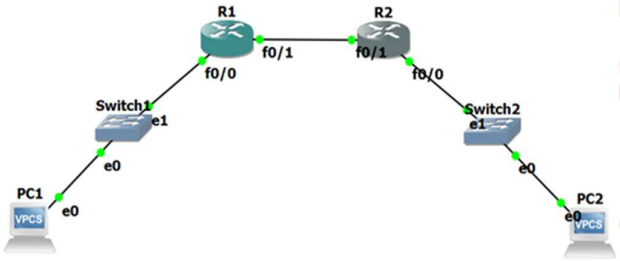
3.Display device information

4.End

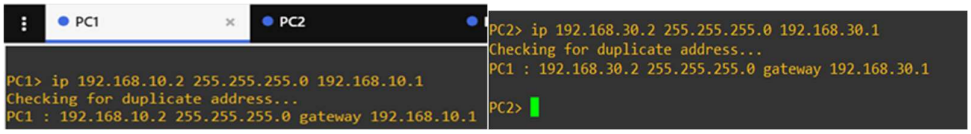
DESCRIPTION AND EXECUTION:

Open Shortest Path First (OSPF) is a link-state routing protocol that is used to find the best path between the source and the destination router using its own Shortest Path First). OSPF is developed by Internet Engineering Task Force (IETF) as one of the Interior Gateway Protocol (IGP), i.e, the protocol which aims at moving the packet within a large autonomous system or routing domain. It is a network layer protocol which works on protocol number 89 and uses AD value 110. OSPF uses multicast address 224.0.0.5 for normal communication and 224.0.0.6 for update to designated router(DR)/Backup Designated Router (BDR).

The resources utilized are 4 PCs, 1 switch and 1 router. Arrange the resources in the topology format given below and begin by configuring the PC's with IP addresses followed by configuration of the switch and router.



Configuring PC's:



Configuring Router's

PC1 PC2 R1 R2

```
o up
*Mar  1 00:00:03.591: %SYS-5-CONFIG_I: Configured from memory by console
*Mar  1 00:00:03.951: %SYS-5-RESTART: System restarted --
Cisco IOS Software, 3600 Software (C3660-A3JK9S-M), Version 12.4(25d), RELEASE S
OFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2010 by Cisco Systems, Inc.
Compiled Wed 18-Aug-10 07:32 by prod_rel_team
*Mar  1 00:00:03.963: %SNMP-5-COLDSTART: SNMP agent on host R1 is undergoing a c
old start
*Mar  1 00:00:04.455: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et0/0, changed state to down
*Mar  1 00:00:04.459: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et0/1, changed state to down
*Mar  1 00:00:05.595: %LINK-5-CHANGED: Interface FastEthernet0/0, changed state
to administratively down
*Mar  1 00:00:05.599: %LINK-5-CHANGED: Interface FastEthernet0/1, changed state
to administratively down
R1#
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface f0/0
R1(config-if)#ip address 192.168.10.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#
*Mar  1 00:07:06.711: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar  1 00:07:07.711: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R1(config)#interface f0/1
R1(config-if)#ip address 192.168.20.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#
*Mar  1 00:07:26.499: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
*Mar  1 00:07:27.499: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
R1(config)#
```

PC1 PC2 R1

```
R1(config)#router ospf 1
R1(config-router)#network 192.168.10.0 0.0.0.255 area 0
R1(config-router)#network 192.168.20.0 0.0.0.255 area 0
R1(config-router)#exit
```

PC1 PC2 R1 R2

```
*Mar  1 00:00:03.419: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state t
o up
*Mar  1 00:00:03.555: %SYS-5-CONFIG_I: Configured from memory by console
*Mar  1 00:00:03.915: %SYS-5-RESTART: System restarted --
Cisco IOS Software, 3600 Software (C3660-A3JK9S-M), Version 12.4(25d), RELEASE S
OFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2010 by Cisco Systems, Inc.
Compiled Wed 18-Aug-10 07:32 by prod_rel_team
*Mar  1 00:00:03.923: %SNMP-5-COLDSTART: SNMP agent on host R2 is undergoing a c
old start
*Mar  1 00:00:04.415: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et0/0, changed state to down
*Mar  1 00:00:04.419: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthern
et0/1, changed state to down
*Mar  1 00:00:05.559: %LINK-5-CHANGED: Interface FastEthernet0/0, changed state
to administratively down
*Mar  1 00:00:05.563: %LINK-5-CHANGED: Interface FastEthernet0/1, changed state
to administratively down
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#interface f0/0
R2(config-if)#ip address 192.168.30.1 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#
*Mar  1 00:07:30.127: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar  1 00:07:31.127: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state
R2(config)#interface f0/1
R2(config-if)#ip address 192.168.20.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#
*Mar  1 00:07:53.079: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
*Mar  1 00:07:54.079: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state
R2(config)#
```

```
PC1  PC2  R1  R2
R2(config-if)#exit
R2(config)#
*Mar  1 00:07:30.127: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar  1 00:07:31.127: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R2(config)#interface f0/1
R2(config-if)#ip address 192.168.20.2 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#
*Mar  1 00:07:53.079: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
*Mar  1 00:07:54.079: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
R2(config)#router ospf 1
R2(config-router)#network 192.168.20.0 0.0.0.255 area 0
R2(config-router)#network 192.168
*Mar  1 00:30:12.335: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.20.1 on FastEthernet0/1 from LOADING to FULL, Loading Done
R2(config-router)#network 192.168.30.0 0.0.0.255 area 0
R2(config-router)#end
R2#
*Mar  1 00:30:48.555: %SYS-5-CONFIG_I: Configured from console by console
R2#
```

Checking connection:

```
PC1  PC2  R1
Press '?' to get help.

Executing the startup file


PC2> ip 192.168.30.2 255.255.255.0 192.168.30.1
Checking for duplicate address...
PC1 : 192.168.30.2 255.255.255.0 gateway 192.168.30.1

PC2> pimg 192.168.10.2
Bad command: "pimg 192.168.10.2". Use ? for help.

PC2> ping 192.168.10.2
84 bytes from 192.168.10.2 icmp_seq=1 ttl=62 time=36.087 ms
84 bytes from 192.168.10.2 icmp_seq=2 ttl=62 time=44.473 ms
84 bytes from 192.168.10.2 icmp_seq=3 ttl=62 time=38.276 ms
84 bytes from 192.168.10.2 icmp_seq=4 ttl=62 time=36.353 ms
84 bytes from 192.168.10.2 icmp_seq=5 ttl=62 time=36.766 ms
```

RESULT: After the configuration and connection of all devices, the ping is successful from PC1 to PC2

EXPERIMENT-11

AIM: Basic EIGRP Configuration using GNS3 tool.

ALGORITHM:

1.Start

2.Setup the topology and initialise devices.

3.Configure devices and verify connectivity.

3.Display device information

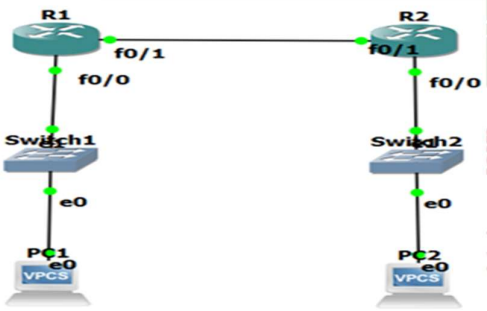
4.End

DESCRIPTION AND EXECUTION:

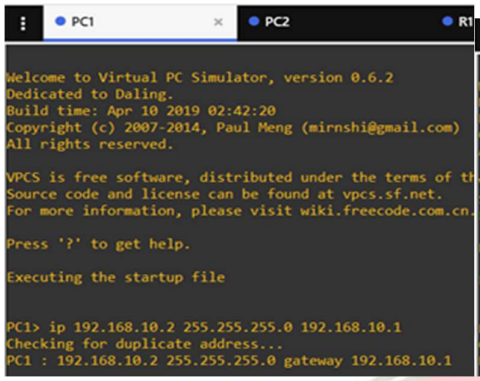
Enhanced Interior Gateway Routing Protocol (EIGRP) is a dynamic routing protocol that is used to find the best path between any two-layer 3 devices to deliver the packet. EIGRP works on network layer Protocol of OSI model and uses protocol number 88. It uses metrics to find out the best path between two layer 3 devices (router or layer 3 switches) operating EIGRP.

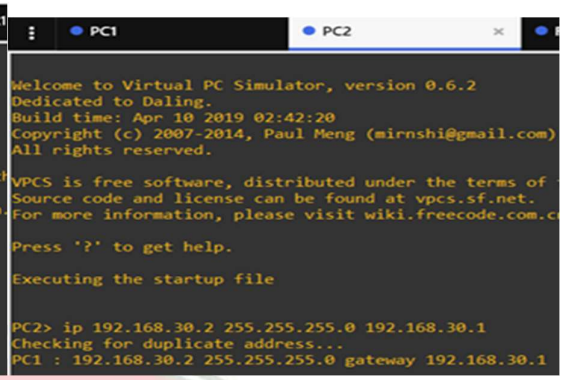
The resources utilized are 2 PCs, 2 switches and 2 routers.

Arrange the resources in the topology format given below and begin by configuring the PC's with IP addresses followed by configuration of the switch and router.

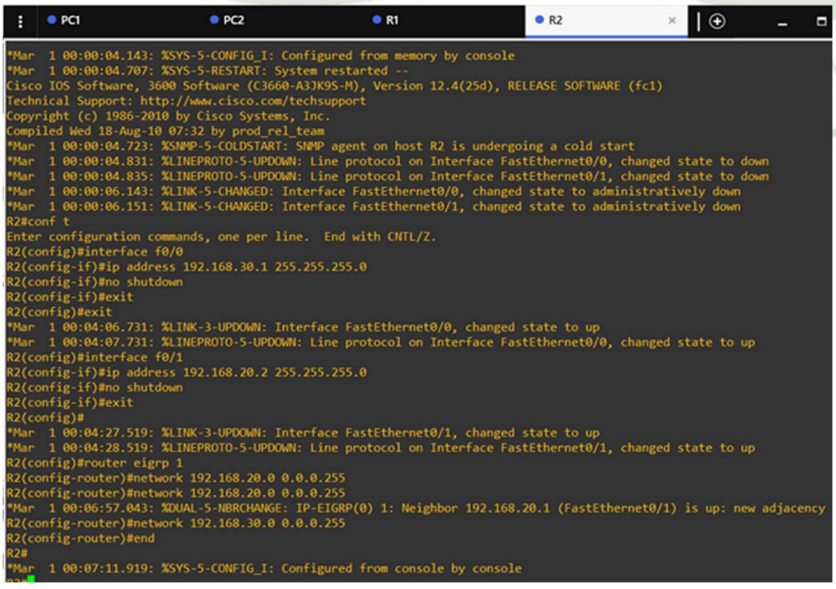


Configuring PC's:

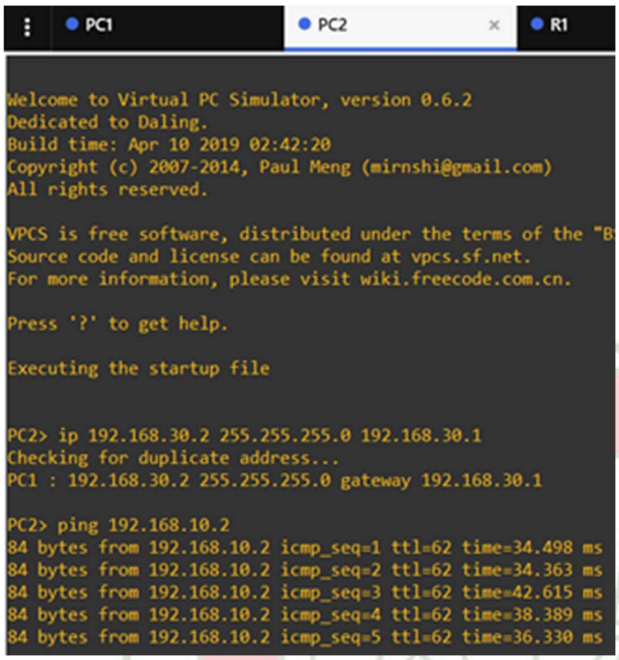


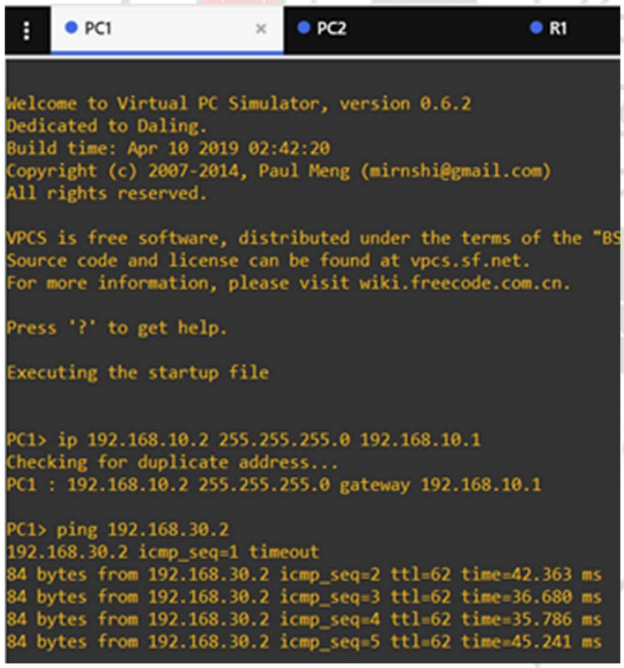


Configuring Routers:



Checking connection:





RESULT: After the configuration and connection of all devices, the ping is successful between PCs

EXPERIMENT-12

AIM: Illustrate TCPDUMP command

DESCRIPTION:

tcpdump is a packet sniffing and packet analyzing tool for a System Administrator to troubleshoot connectivity issues in Linux. It is used to capture, filter, and analyze network traffic such as TCP/IP packets going through your system. It is many times used as a security tool as well. It saves the captured information in a pcap file, these pcap files can then be opened through Wireshark or through the command tool itself.

COMMANDS:

Installing tcpdump tool in Linux

For RedHat based linux OS

yum install tcpdump

For Ubuntu/Debian OS

apt install tcpdump

Working with tcpdump command:

1. To capture the packets of current network interface
   sudo tcpdump
   This will capture the packets from the current interface of the network through which the system is connected to the internet.

OUTPUT:

```
onworks@onworks-Standard-PC-i440FX-PIIX-1996:~$ sudo tcpdump
[sudo] password for onworks:
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ens3, link-type EN10MB (Ethernet), capture size 262144 bytes
05:48:14.000181 IP6 onworks-Standard-PC-i440FX-PIIX-1996.39452 > 2001:67c:1560:8003::c7.ntp: NTPv4, Clie
nt, length 48
05:48:14.003418 IP onworks-Standard-PC-i440FX-PIIX-1996.40401 > 10.0.2.3.domain: 17769+ [1au] PTR? 7.c.0
.0.0.0.0.0.0.0.0.0.0.0.3.0.0.8.0.6.5.1.c.7.6.0.1.0.0.2.ip6.arpa. (101)
05:48:14.024113 IP 10.0.2.3.domain > onworks-Standard-PC-i440FX-PIIX-1996.40401: 17769 NXDomain 0/1/1 (1
65)
05:48:14.024254 IP onworks-Standard-PC-i440FX-PIIX-1996.40401 > 10.0.2.3.domain: 17769+ PTR? 7.c.0.0.0.0
.0.0.0.0.0.0.0.0.3.0.0.8.0.6.5.1.c.7.6.0.1.0.0.2.ip6.arpa. (90)
05:48:14.043893 IP 10.0.2.3.domain > onworks-Standard-PC-i440FX-PIIX-1996.40401: 17769 NXDomain 0/1/0 (1
54)
05:48:14.044492 IP onworks-Standard-PC-i440FX-PIIX-1996.38770 > 10.0.2.3.domain: 48851+ [1au] PTR? f.9.f
.e.7.b.8.3.0.e.5.9.c.b.0.f.0.0.0.0.0.0.0.0.0.0.0.0.c.e.f.ip6.arpa. (101)
05:48:14.050374 IP 10.0.2.3.domain > onworks-Standard-PC-i440FX-PIIX-1996.38770: 48851 NXDomain 0/1/1 (1
65)
05:48:14.050442 IP onworks-Standard-PC-i440FX-PIIX-1996.38770 > 10.0.2.3.domain: 48851+ PTR? f.9.f.e.7.b
.8.3.0.e.5.9.c.b.0.f.0.0.0.0.0.0.0.0.0.0.0.0.c.e.f.ip6.arpa. (90)
05:48:14.056105 IP 10.0.2.3.domain > onworks-Standard-PC-i440FX-PIIX-1996.38770: 48851 NXDomain 0/1/0 (1
54)
05:48:14.057724 IP onworks-Standard-PC-i440FX-PIIX-1996.51120 > 10.0.2.3.domain: 44979+ [1au] PTR? 3.2.0
.10.in-addr.arpa. (50)
05:48:14.062638 IP 10.0.2.3.domain > onworks-Standard-PC-i440FX-PIIX-1996.51120: 44979 NXDomain 0/0/1 (5
0)
05:48:14.062690 IP onworks-Standard-PC-i440FX-PIIX-1996.51120 > 10.0.2.3.domain: 44979+ PTR? 3.2.0.10.in
-addr.arpa. (39)
05:48:14.067810 IP 10.0.2.3.domain > onworks-Standard-PC-i440FX-PIIX-1996.51120: 44979 NXDomain 0/0/0 (3
9)
05:48:14.068863 IP onworks-Standard-PC-i440FX-PIIX-1996.44277 > 10.0.2.3.domain: 27335+ [1au] PTR? 15.2.
0.10.in-addr.arpa. (51)
05:48:14.074037 IP 10.0.2.3.domain > onworks-Standard-PC-i440FX-PIIX-1996.44277: 27335 NXDomain 0/0/1 (5
1)
05:48:14.074090 IP onworks-Standard-PC-i440FX-PIIX-1996.44277 > 10.0.2.3.domain: 27335+ PTR? 15.2.0.10.i
n-addr.arpa. (40)
05:48:14.079237 IP 10.0.2.3.domain > onworks-Standard-PC-i440FX-PIIX-1996.44277: 27335 NXDomain 0/0/0 (4
0)
05:48:19.255857 ARP, Request who-has 10.0.2.3 tell onworks-Standard-PC-i440FX-PIIX-1996, length 28
```

2. To capture packets from a specific network interface

sudo tcpdump -i wlo1

This command will now capture the packets from wlo1 network interface.

Output:

```
onworks@onworks-Standard-PC-i440FX-PIIX-1996:~$ sudo tcpdump -i ens3
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ens3, link-type EN10MB (Ethernet), capture size 262144 bytes
05:52:28.931050 IP api.snapcraft.io.https > onworks-Standard-PC-i440FX-PIIX-1996.50582: Flags [F.], seq
0, ack 546792116, win 8760, length 0
05:52:28.931051 IP api.snapcraft.io.https > onworks-Standard-PC-i440FX-PIIX-1996.60882: Flags [F.], seq
0, ack 108906055, win 8760, length 0
05:52:28.931848 IP onworks-Standard-PC-i440FX-PIIX-1996.52595 > 10.0.2.3.domain: 39045+ [1au] PTR? 15.2.
0.10.in-addr.arpa. (51)
05:52:28.937091 IP 10.0.2.3.domain > onworks-Standard-PC-i440FX-PIIX-1996.52595: 39045 NXDomain 0/0/1 (5
1)
05:52:28.937253 IP onworks-Standard-PC-i440FX-PIIX-1996.52595 > 10.0.2.3.domain: 39045+ PTR? 15.2.0.10.i
n-addr.arpa. (40)
05:52:28.942497 IP 10.0.2.3.domain > onworks-Standard-PC-i440FX-PIIX-1996.52595: 39045 NXDomain 0/0/0 (4
0)
05:52:28.943034 IP onworks-Standard-PC-i440FX-PIIX-1996.59248 > 10.0.2.3.domain: 13188+ [1au] PTR? 40.92
.189.91.in-addr.arpa. (54)
05:52:28.963868 IP 10.0.2.3.domain > onworks-Standard-PC-i440FX-PIIX-1996.59248: 13188 1/0/1 PTR api.sna
pcraft.io. (84)
05:52:28.964545 IP onworks-Standard-PC-i440FX-PIIX-1996.36643 > 10.0.2.3.domain: 32716+ [1au] PTR? 3.2.0
.10.in-addr.arpa. (50)
05:52:28.969811 IP 10.0.2.3.domain > onworks-Standard-PC-i440FX-PIIX-1996.36643: 32716 NXDomain 0/0/1 (5
0)
05:52:28.969931 IP onworks-Standard-PC-i440FX-PIIX-1996.36643 > 10.0.2.3.domain: 32716+ PTR? 3.2.0.10.in
-addr.arpa. (39)
05:52:28.975127 IP 10.0.2.3.domain > onworks-Standard-PC-i440FX-PIIX-1996.36643: 32716 NXDomain 0/0/0 (3
9)
05:52:29.338869 IP onworks-Standard-PC-i440FX-PIIX-1996.50588 > api.snapcraft.io.https: Flags [S], seq 6
32749650, win 64240, options [mss 1460,sackOK,TS val 527748808 ecr 0,nop,wscale 7], length 0
05:52:30.439288 IP api.snapcraft.io.https > onworks-Standard-PC-i440FX-PIIX-1996.60880: Flags [F.], seq
0, ack 1150855087, win 8760, length 0
```

3. To capture specific number of packets

sudo tcpdump -c 4 -i wlo1

This command will capture only 4 packets from the wlo1 interface.

OUTPUT

```
onworks@onworks-Standard-PC-i440FX-PIIX-1996:~$ sudo tcpdump -c 4 -i ens3
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ens3, link-type EN10MB (Ethernet), capture size 262144 bytes
05:53:58.218801 IP api.snapcraft.io.https > onworks-Standard-PC-i440FX-PIIX-1996.50590: Flags [F.], seq
0, ack 2605884239, win 8760, length 0
05:53:58.219421 IP onworks-Standard-PC-i440FX-PIIX-1996.59279 > 10.0.2.3.domain: 6954+ [1au] PTR? 15.2.0
.10.in-addr.arpa. (51)
05:53:58.224558 IP 10.0.2.3.domain > onworks-Standard-PC-i440FX-PIIX-1996.59279: 6954 NXDomain 0/0/1 (51
)
05:53:58.224629 IP onworks-Standard-PC-i440FX-PIIX-1996.59279 > 10.0.2.3.domain: 6954+ PTR? 15.2.0.10.in
-addr.arpa. (40)
4 packets captured
9 packets received by filter
0 packets dropped by kernel
onworks@onworks-Standard-PC-i440FX-PIIX-1996:~$
```

4. To print captured packets in ASCII format

sudo tcpdump -A -i wlo1

This command will now print the captured packets from wlo1 to ASCII value.

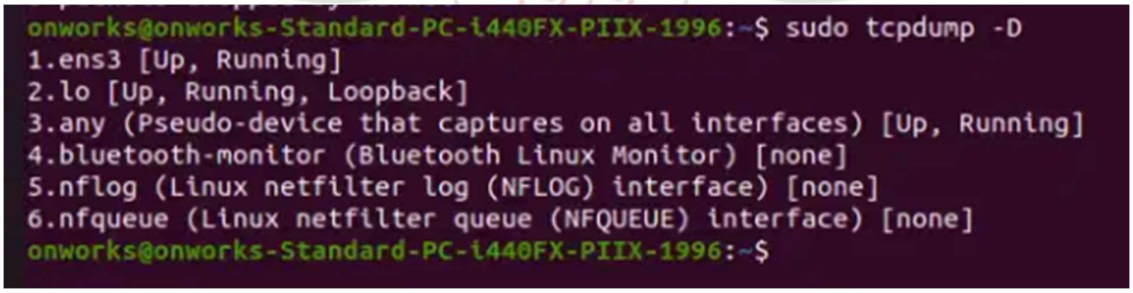
OUTPUT:

5. To display all available interfaces

sudo tcpdump -D

This command will display all the interfaces that are available in the system.

OUTPUT:



6. To display packets in HEX and ASCII values
sudo tcpdump -XX -i wlo1
This command will now print the packets captured from the wlo1 interface in the HEX and ASCII values.
OUTPUT:

```
onworks@onworks-Standard-PC-i440FX-PIIX-1996:~$ sudo tcpdump -XX -i ens3
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ens3, link-type EN10MB (Ethernet), capture size 262144 bytes
06:06:08.998046 IP onworks-Standard-PC-i440FX-PIIX-1996.60890 > api.snapcraft.io.https: Flags [S], seq 5
18894480, win 64240, options [mss 1460,sackOK,TS val 924234676 ecr 0,nop,wscale 7], length 0
        0x0000:  5255 0a00 0202 5254 0012 3456 0800 4500  RU....RT..4V..E.
        0x0010:  003c dba1 4000 4006 9b3b 0a00 020f 5bbd  .<..@.@..;....[.
        0x0020:  5c13 edda 01bb 1eed b390 0000 0000 a002  \...............
        0x0030:  faf0 c40d 0000 0204 05b4 0402 080a 3716  ..............7.
        0x0040:  b3b4 0000 0000 0103 0307                 ..........
06:06:08.998122 IP onworks-Standard-PC-i440FX-PIIX-1996.60888 > api.snapcraft.io.https: Flags [S], seq 2
244248178, win 64240, options [mss 1460,sackOK,TS val 924234676 ecr 0,nop,wscale 7], length 0
        0x0000:  5255 0a00 0202 5254 0012 3456 0800 4500  RU....RT..4V..E.
        0x0010:  003c 8f47 4000 4006 e795 0a00 020f 5bbd  .<.G@.@.......[.
        0x0020:  5c13 edd8 01bb 85c4 8272 0000 0000 a002  \........r......
        0x0030:  faf0 c40d 0000 0204 05b4 0402 080a 3716  ..............7.
        0x0040:  b3b4 0000 0000 0103 0307                 ..........
06:06:08.998784 IP onworks-Standard-PC-i440FX-PIIX-1996.56572 > 10.0.2.3.domain: 17108+ [1au] PTR? 19.92
.189.91.in-addr.arpa. (54)
        0x0000:  5255 0a00 0203 5254 0012 3456 0800 4500  RU....RT..4V..E.
        0x0010:  0052 827d 4000 4011 a00c 0a00 020f 0a00  .R.}@.@.........
        0x0020:  0203 dcfc 0035 003e 1861 42d4 0100 0001  .....5.>.aB.....
        0x0030:  0000 0000 0001 0231 3902 3932 0331 3839  .......19.92.189
        0x0040:  0239 3107 696e 2d61 6464 7204 6172 7061  .91.in-addr.arpa
        0x0050:  0000 0c00 0100 0029 0200 0000 0000 0000  .......).........
06:06:09.329377 IP 10.0.2.3.domain > onworks-Standard-PC-i440FX-PIIX-1996.56572: 17108 1/0/1 PTR api.sna
pcraft.io. (84)
        0x0000:  5254 0012 3456 5255 0a00 0202 0800 4500  RT..4VRU......E.
        0x0010:  0070 57e2 0000 4011 0a8a 0a00 0203 0a00  .pW...@.........
        0x0020:  020f 0035 dcfc 005c 96e1 42d4 8180 0001  ...5...\..B.....
        0x0030:  0001 0000 0001 0231 3902 3932 0331 3839  .......19.92.189
        0x0040:  0239 3107 696e 2d61 6464 7204 6172 7061  .91.in-addr.arpa
        0x0050:  0000 0c00 01c0 0c00 0c00 0100 000e 1000  ................
```

7. To save captured packets into a file
sudo tcpdump -w captured_packets.pcap -i wlo1

This command will now output all the captures packets in a file named as captured_packets.pcap.
OUTPUT

```
onworks@onworks-Standard-PC-i440FX-PIIX-1996:~$ sudo tcpdump -w captured_packets.pcap -i ens3
[sudo] password for onworks:
tcpdump: listening on ens3, link-type EN10MB (Ethernet), capture size 262144 bytes
^C6945 packets captured
6945 packets received by filter
0 packets dropped by kernel
onworks@onworks-Standard-PC-i440FX-PIIX-1996:~$
```

8. To read captured packets from a file
sudo tcpdump -r captured_packets.pcap

This command will now read the captured packets from the captured_packets.pcap file.

OUTPUT

```
06:09:49.639495 IP onworks-Standard-PC-i440FX-PIIX-1996.43466 > ubuntu-mirror-1.ps6.canonical.com.http:
Flags [.], ack 366723, win 65535, length 0
^C06:09:49.639491 IP ubuntu-mirror-1.ps6.canonical.com.http > onworks-Standard-PC-i440FX-PIIX-1996.43466
: Flags [P.], seq 366723:368183, ack 487, win 8760, length 1460: HTTP

onworks@onworks-Standard-PC-i440FX-PIIX-1996:~$ sudo tcpdump -r captured_packets.pcap
06:09:50.673298 IP ubuntu-mirror-1.ps6.canonical.com.http > onworks-Standard-PC-i440FX-PIIX-1996.43466:
Flags [P.], seq 8782587:8784047, ack 6995, win 8760, length 1460: HTTP: HTTP/1.1 200 OK
06:09:50.673314 IP onworks-Standard-PC-i440FX-PIIX-1996.43466 > ubuntu-mirror-1.ps6.canonical.com.http:
Flags [.], ack 8784047, win 65535, length 0
06:09:50.673298 IP ubuntu-mirror-1.ps6.canonical.com.http > onworks-Standard-PC-i440FX-PIIX-1996.43466:
Flags [P.], seq 8784047:8784659, ack 6995, win 8760, length 612: HTTP
06:09:50.677271 IP ubuntu-mirror-1.ps6.canonical.com.http > onworks-Standard-PC-i440FX-PIIX-1996.43466:
Flags [P.], seq 8784659:8786119, ack 6995, win 8760, length 1460: HTTP: HTTP/1.1 200 OK
06:09:50.677277 IP onworks-Standard-PC-i440FX-PIIX-1996.43466 > ubuntu-mirror-1.ps6.canonical.com.http:
Flags [.], ack 8786119, win 65535, length 0
06:09:50.677271 IP ubuntu-mirror-1.ps6.canonical.com.http > onworks-Standard-PC-i440FX-PIIX-1996.43466:
Flags [P.], seq 8786119:8787361, ack 6995, win 8760, length 1242: HTTP
06:09:50.689237 IP ubuntu-mirror-1.ps6.canonical.com.http > onworks-Standard-PC-i440FX-PIIX-1996.43466:
Flags [P.], seq 8787361:8787592, ack 6995, win 8760, length 231: HTTP: HTTP/1.1 200 OK
06:09:50.689246 IP onworks-Standard-PC-i440FX-PIIX-1996.43466 > ubuntu-mirror-1.ps6.canonical.com.http:
Flags [.], ack 8787592, win 65535, length 0
06:09:50.689360 IP ubuntu-mirror-1.ps6.canonical.com.http > onworks-Standard-PC-i440FX-PIIX-1996.43466:
Flags [P.], seq 8787592:8788344, ack 6995, win 8760, length 752: HTTP: HTTP/1.1 200 OK
06:09:50.733069 IP onworks-Standard-PC-i440FX-PIIX-1996.43466 > ubuntu-mirror-1.ps6.canonical.com.http:
Flags [.], ack 8788344, win 65535, length 0
06:09:51.971131 IP onworks-Standard-PC-i440FX-PIIX-1996.43466 > ubuntu-mirror-1.ps6.canonical.com.http:
Flags [F.], seq 6995, ack 8788344, win 65535, length 0
06:09:51.971237 IP ubuntu-mirror-1.ps6.canonical.com.http > onworks-Standard-PC-i440FX-PIIX-1996.43466:
Flags [.], ack 6996, win 8760, length 0
06:09:51.971622 IP onworks-Standard-PC-i440FX-PIIX-1996.55472 > 141.30.62.22.http: Flags [F.], seq 11122
, ack 11759863, win 65535, length 0
06:09:51.971678 IP 141.30.62.22.http > onworks-Standard-PC-i440FX-PIIX-1996.55472: Flags [.], ack 11123,
 win 8760, length 0
06:09:51.990490 IP 141.30.62.22.http > onworks-Standard-PC-i440FX-PIIX-1996.55472: Flags [R.], seq 11759
863, ack 11123, win 8760, length 0
06:09:52.120914 IP ubuntu-mirror-1.ps6.canonical.com.http > onworks-Standard-PC-i440FX-PIIX-1996.43466:
Flags [R.], seq 8788344, ack 6996, win 8760, length 0
06:09:52.769093 IP6 onworks-Standard-PC-i440FX-PIIX-1996 > fec0::2: ICMP6, neighbor solicitation, who ha
s fec0::2, length 32
06:09:52.769195 IP6 fec0::2 > onworks-Standard-PC-i440FX-PIIX-1996: ICMP6, neighbor advertisement, tgt i
s fec0::2, length 32
onworks@onworks-Standard-PC-i440FX-PIIX-1996:~$ ^C
onworks@onworks-Standard-PC-i440FX-PIIX-1996:~$
```

9. To capture packets with ip address
sudo tcpdump -n -i wlo1

This command will now capture the packets with IP addresses.
OUTPUT

```
onworks@onworks-Standard-PC-i440FX-PIIX-1996:~$ sudo tcpdump -n -i ens3
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ens3, link-type EN10MB (Ethernet), capture size 262144 bytes
06:13:49.830711 IP 10.0.2.15.50648 > 91.189.92.40.443: Flags [S], seq 2473722447, win 64240, options [ms
s 1460,sackOK,TS val 527781608 ecr 0,nop,wscale 7], length 0
06:13:49.830770 IP 10.0.2.15.50646 > 91.189.92.40.443: Flags [S], seq 4139998373, win 64240, options [ms
s 1460,sackOK,TS val 527781608 ecr 0,nop,wscale 7], length 0
06:13:50.730668 IP 91.189.92.40.443 > 10.0.2.15.50646: Flags [F.], seq 0, ack 4139998374, win 8192, leng
th 0
06:13:50.730668 IP 91.189.92.40.443 > 10.0.2.15.50638: Flags [F.], seq 0, ack 478652487, win 8760, lengt
h 0
06:13:50.730668 IP 91.189.92.40.443 > 10.0.2.15.50630: Flags [F.], seq 0, ack 3530249906, win 8760, leng
th 0
06:13:50.730668 IP 91.189.92.40.443 > 10.0.2.15.50628: Flags [F.], seq 0, ack 3627054957, win 8760, leng
th 0
06:13:51.944216 IP 91.189.92.40.443 > 10.0.2.15.50626: Flags [F.], seq 0, ack 816105158, win 8760, lengt
h 0
06:13:51.944216 IP 91.189.92.40.443 > 10.0.2.15.50624: Flags [F.], seq 0, ack 3202938958, win 8760, leng
th 0
^C
8 packets captured
8 packets received by filter
0 packets dropped by kernel
onworks@onworks-Standard-PC-i440FX-PIIX-1996:~$
```

10. To capture only TCP packets
sudo tcpdump -i wlo1 tcp

This command will now capture only TCP packets from wlo1.
OUTPUT:

```
onworks@onworks-Standard-PC-i440FX-PIIX-1996:~$ sudo tcpdump -i ens3 tcp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ens3, link-type EN10MB (Ethernet), capture size 262144 bytes
06:14:24.384720 IP onworks-Standard-PC-i440FX-PIIX-1996.50650 > api.snapcraft.io.https: Flags [S], seq 1
615645445, win 64240, options [mss 1460,sackOK,TS val 527816168 ecr 0,nop,wscale 7], length 0
06:14:24.500819 IP api.snapcraft.io.https > onworks-Standard-PC-i440FX-PIIX-1996.50636: Flags [F.], seq
0, ack 2567671397, win 8760, length 0
06:14:24.500820 IP api.snapcraft.io.https > onworks-Standard-PC-i440FX-PIIX-1996.50634: Flags [F.], seq
0, ack 3404788314, win 8760, length 0
06:14:24.871697 IP api.snapcraft.io.https > onworks-Standard-PC-i440FX-PIIX-1996.50640: Flags [F.], seq
0, ack 3663748440, win 8760, length 0
06:14:25.880965 IP api.snapcraft.io.https > onworks-Standard-PC-i440FX-PIIX-1996.50650: Flags [F.], seq
0, ack 1615645446, win 8760, length 0
06:14:26.379730 IP api.snapcraft.io.https > onworks-Standard-PC-i440FX-PIIX-1996.50638: Flags [F.], seq
0, ack 478652487, win 8760, length 0
06:14:26.379730 IP api.snapcraft.io.https > onworks-Standard-PC-i440FX-PIIX-1996.50630: Flags [F.], seq
0, ack 3530249906, win 8760, length 0
06:14:26.379730 IP api.snapcraft.io.https > onworks-Standard-PC-i440FX-PIIX-1996.50628: Flags [F.], seq
0, ack 3627054957, win 8760, length 0
^C
8 packets captured
8 packets received by filter
0 packets dropped by kernel
onworks@onworks-Standard-PC-i440FX-PIIX-1996:~$
```

CONCLUSION: The tcpdump command is studied and analysed