

GURU TEGH BAHADUR INSTITUTE OF TECHNOLOGY



ACADEMIC SESSION: 2023-2024

BRANCH: ARTIFICIAL INTELLIGENCE & MACHINE LEARNING

SUBJECT: CN & IP
SUBJECT CODE: AIML-256

Name: YASH SHARMA

Enr. No.: 02313211622

List of Experiments

Subject: CN&IP

Paper Code: AIML-256

1. Introduction and Study of various Networking Devices.
2. Study of types of transmission medium used in networks.
3. Introduction to basic networking tools: Wireshark, Network Miner.
4. Hands-on of various services/Commands like Ping, Trace Route, etc.
5. Create various network topologies using Cisco Packet Tracer.
 - a) Ring Topology
 - b) Bus Topology
 - c) Star Topology
 - d) Mesh Topology
6. Study Various router configuration commands.
7. Implement a scenario to connect two devices (Hosts) on different networks and define a static route between two routers so that all the devices can ping any other device.
8. Take a scenario of two devices connected with different routers and define a default route between two routers so that all the devices can ping any other devices.
9. To configure a dynamic route (using RIP version 1) between two routers so that all the devices can ping any other device.
10. To configure a dynamic route (using EIGRP (autonomous system 100) between two routers so that all the devices can ping my other device.

Practical 1: Introduction and Study of various Networking Devices.

Overview:

Network devices are physical devices that enable communication and interaction between hardware on a computer network. Each networking device operates in a distinct computer network segment and performs distinct functions.

A network may require hundreds or thousands of different network devices to maintain and build out various LAN and WAN. Network devices like the hub, bridge, repeater, modem, router, gateways, etc..., are the basic building blocks of an extensive network.

Definition:

Network devices are physical devices that enable communication and interaction between hardware on a computer network. Network devices are building blocks that permit communication between services and the endpoint that consumes those services.

In other words, they're connectors that allow devices on a network to communicate with one another. Enabling communication on a network means anything that helps data get from the source destination.

When a network contains a large number of devices, too many data packets are transmitted over the same network path. This can cause congestion and performance reduction. The goal of networking devices is to provide for smooth communication between various hardware linked to a network. Adding a network device facilitates seamless sharing of network resources between different systems.

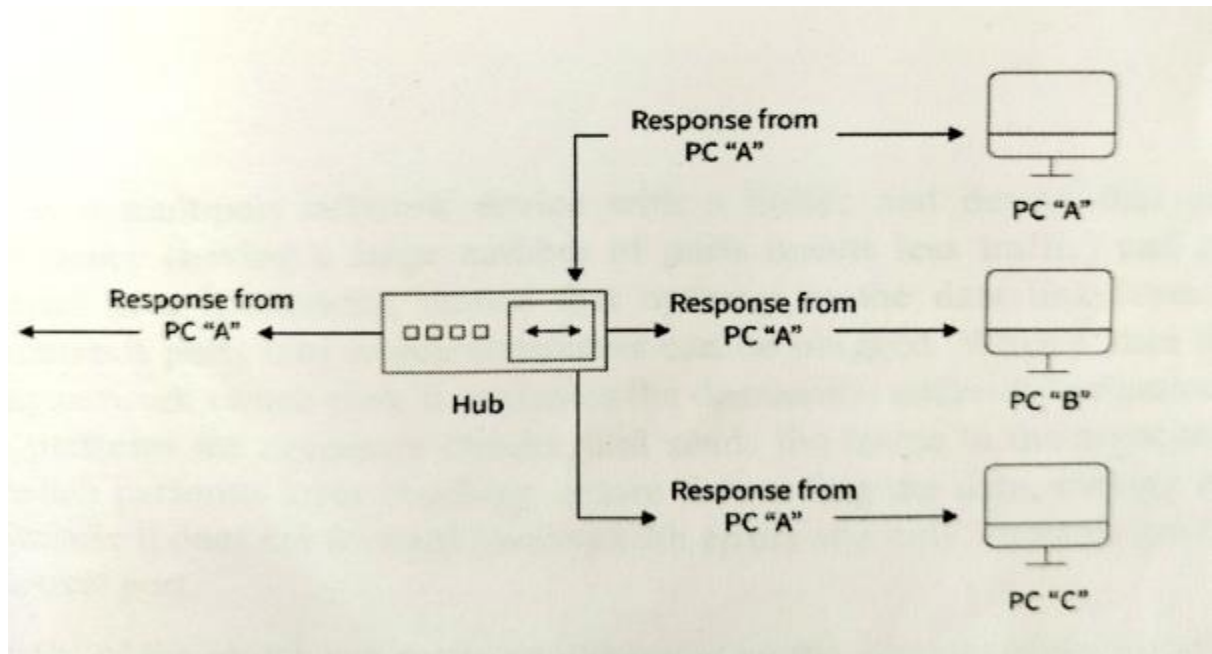
Types of Network Devices:

- Hub
- Switch
- Router
- Bridge
- Gateway
- Modem
- Repeaters
- Access point

HUB:

A hub is a physical-layer device that acts on individual bits rather than frames. When a bit, representing a zero or a one, arrives from one interface, the hub simply recreates the bit, boosts its energy strength, and transmits the bit into all the other interfaces. Whenever a hub receives a bit from one of its interfaces, it sends a copy to all other interfaces.

In particular, if a hub receives frames from two different interfaces at the same time, a collision occurs, and the nodes that created the frames must retransmit. A network hub does not have routing tables or intelligence that is utilized to transfer information and disseminate all network data across all connections.



Types of Hubs-

There are generally three types of hubs that are given below.

1. **Active Hub:** These hubs have their power source and can clean, enhance, and relay the network's signal. It functions as both a repeater and a wiring center. The active hub may repair damaged packets as they are being sent and can also hold the direction of the remaining packets and distribute them. If a port gets a weak but readable signal, the active hub reconstructs the weak signal into a more robust signal before distributing it to other ports. If any connecting device in the network is not operating, it can increase the signal.
2. **Passive Hub:** The passive hubs are the wire connection points that aid in the construction of the physical network. It can detect faults and manufacturing hardware. The passive hub accepts the packet through a port and distributes it to all ports. It comes with connectors that can be used in your network as a standard. All local area network (LAN) devices are linked to connector. These hubs do not clean or enhance signals before

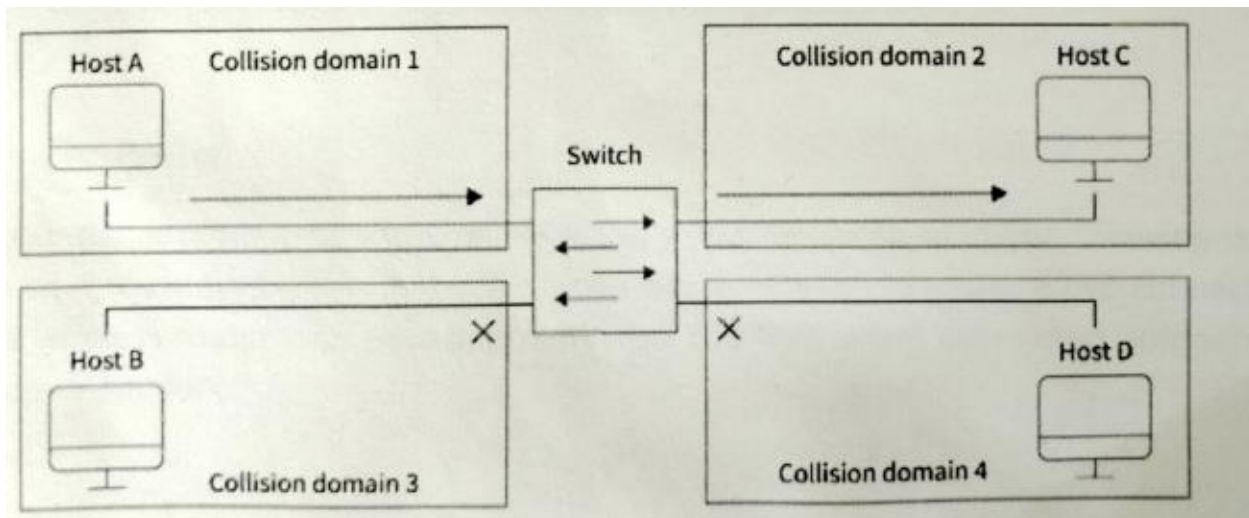
relaying them to the network as cannot be utilized to extend the distance between the nodes.

3. Intelligent Hub: It functions similarly to active hubs and offers remote management capabilities. They also supply network devices with variable data speeds. It allows an administrator to monitor traffic flowing through the hub and manage each port.

SWITCH:

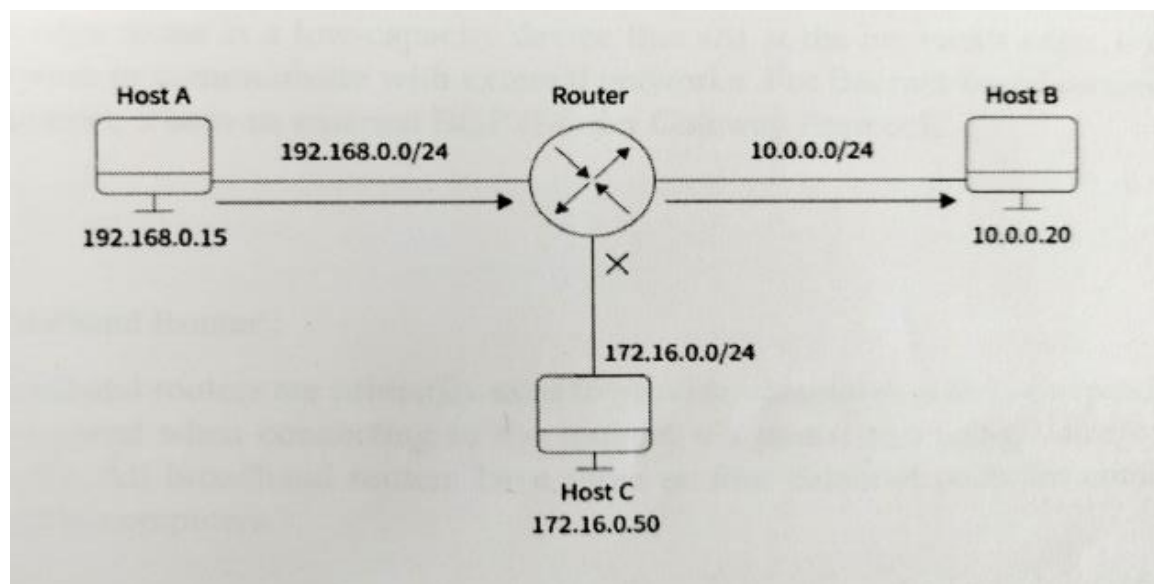
A switch is a multiport network device with a buffer and design that can improve its efficiency and performance. A switch is a networking device that operates at the data link layer. A switch has numerous ports into which computers can be plugged. When a data frame arrives at any switch port, it evaluates the destination address, performs necessary checks, and sends the frame to the associated device. The switch performs error checking before forwarding the data making it very efficient because it does not forward packets with errors and only forward good packets to the correct port.

The working of the switch can be easily illustrated by the diagram given below in which Host A sends some data to Host B.



ROUTER:

A router is a network device similar to a switch that routes data packets based on their IP addresses. The router is primarily a Network Layer device. A router is also known as an intelligent device because it can automatically calculate the best route to pass network packets from source to destination. A router examines a data packet's destination IP address and uses headers and forwarding tables to determine the best way to transfer the packets. It communicates between two or more networks using protocols such as ICMP.



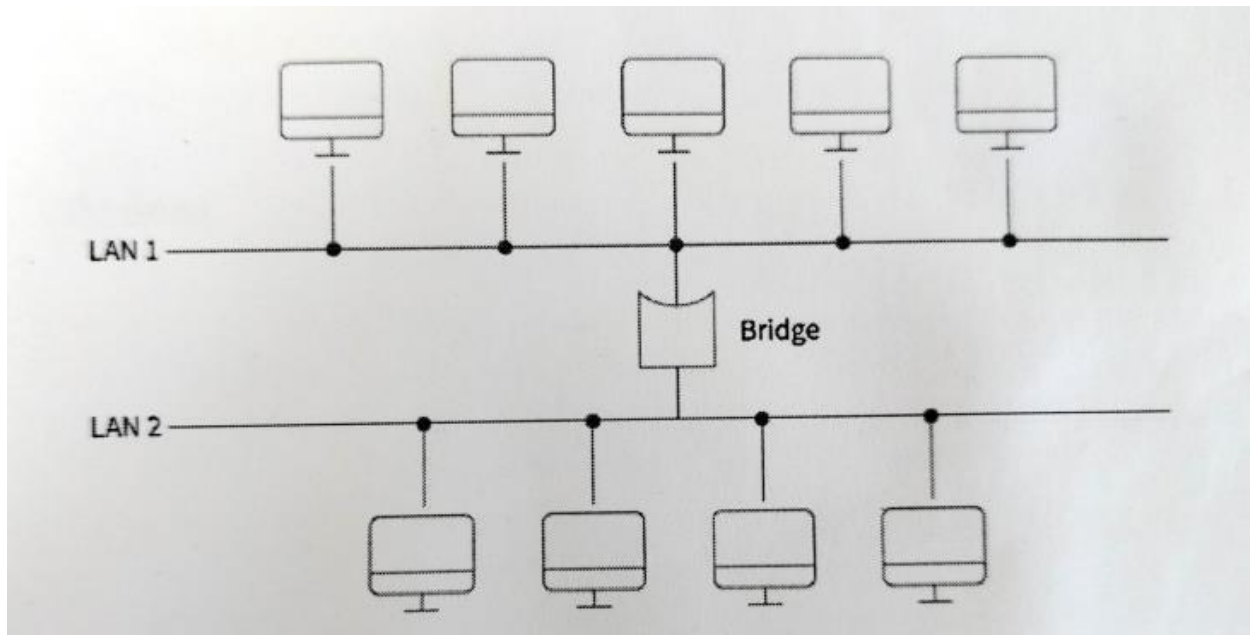
Types of Routers-

There are various types of routers used in networking as follows:

1. **Wireless Router:** These routers can generate a wireless signal in your home or office, allowing computers to connect to routers within a specific range and access the internet. When connected indoors, the wireless router's range is approximately 150 feet, when connected outdoors, the range is up to 300 feet.
2. **Brouter:** A brouter is a hybrid of a bridge and a router. It acts as a bridge, allowing data to be transferred between networks, and it can also route data within a network to individual systems, much like a router. As a result, it combines the functions of a bridge and a router by routing some incoming data to the appropriate systems while transferring the rest to another network.
3. **Core Router:** A core router is a kind of router that can route data within a network but cannot route data between networks. It is a computer communication system device that serves as the backbone of networks by connecting all network devices. It is used by internet service providers and offers a variety of fast and powerful data communication interfaces.
4. **Edge Router:** An edge router is a low-capacity device that sits at the network's edge. It enables an internal network to communicate with external networks. For internet-based connectivity with distant networks, it uses an external BGP (Border Gateway Protocol).
5. **Broadband Router:** Broadband routers are primarily used to provide computers with high-speed internet access. It is required when connecting to the internet via phone and using Voice over IP technology (VoIP). All broadband routers have three or four Ethernet ports for connecting laptop and desktop computers.

BRIDGE:

A bridge is a network device that operates at the data link layer device. A bridge is a repeater with the added functionality of filtering content by reading the MAC addresses of the source and destination. It is also used to connect two LANs that use the same protocol. It has a single input and output port, making it a two-port device.



Types of Bridges-

There are generally two types of bridges used in networking:

1. **Transparent Bridges:** A transparent bridge is a type of bridge that monitors incoming network traffic to determine media access control (MAC) addresses. These bridges operate in a manner that is transparent to all networked hosts. A transparent bridge stores MAC addresses in a table similar to a routing table and uses that information to route packets to their destination.
2. **Source Routing Bridges:** The source station performs the routing operation in these bridges, and the frame specifies which route to take. The host can find the frame by sending a special frame known as the discovery frame, which propagates throughout the network using all possible paths to the destination.

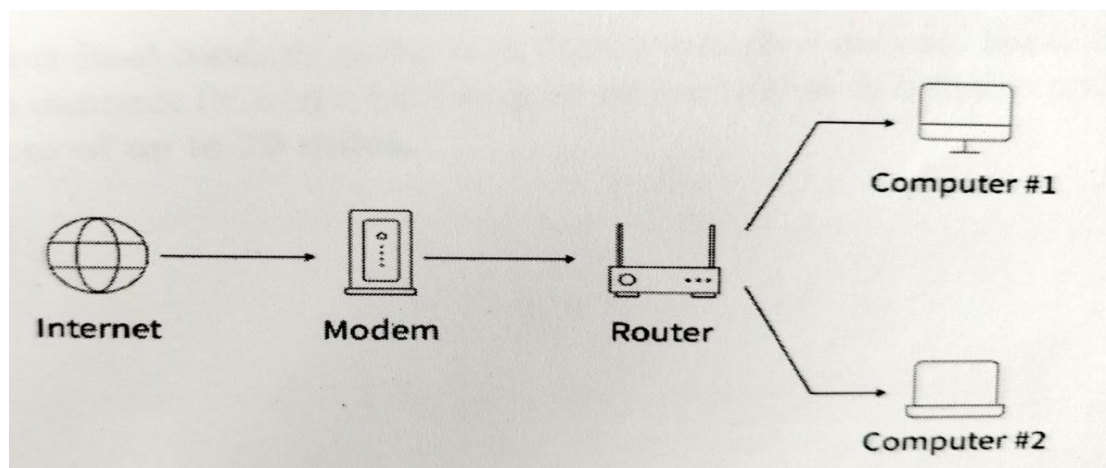
GATEWAY:

A gateway is a network node in telecommunications that connects two networks that use different transmission protocols. Gateways serve as network entry and exit points because all data must pass through or communicate with the gateway before being routed. Traffic that does not go through at least one gateway in most IP-based networks is traffic between the nodes on

the same local area network (LAN) segment. The primary benefit of using a gateway in personal or business scenarios is that it consolidates internet connectivity into a single device. A gateway node in the enterprise can also serve as a proxy server and a firewall

MODEM:

A modem is a network device that modulates and demodulates analog carrier signals (known as sine waves) to encode and decode digital data for processing. Because modems perform both of these tasks simultaneously, the term modem is a combination of "modulate" and "demodulate".



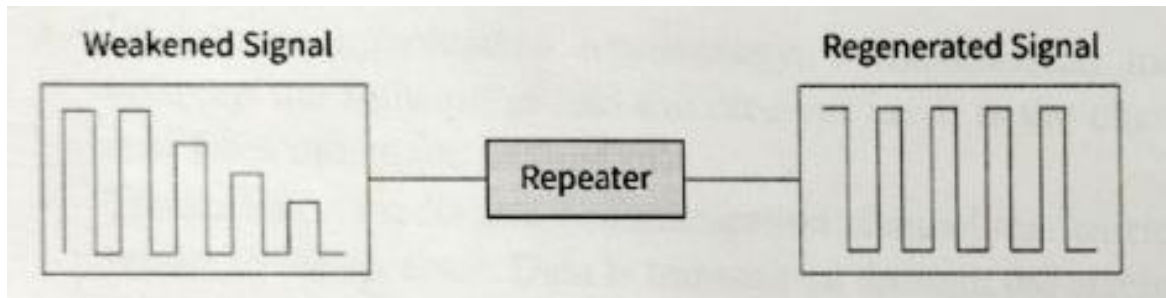
Types of Modems-

There are generally five types of modems.

1. **Optical Model:** Instead of other metallic media, optical cables are used in optical modems. It converts digital data signals into light pulses transmitted via the optical fiber it employs.
2. **Digital Modem:** Digital data is converted into digital signals by a digital model. The digital data is modulated on the digital carrier signals before being transmitted over the digital transmission lines.
3. **Acoustic Modem:** A specific modem called an "acoustic modem" can connect a phone handset to a gadget that traveling salespeople use to connect hotel phones. It has a microphone and speaker.
4. **Smart Modem:** The smart modem has capabilities for auto-dialing, auto-redialing, and auto-answering. It has a microprocessor onboard that performs auto-dial and auto-answering tasks using the Hayes AT command set.
5. **Short Haul Modem:** The short-haul modem is the one that is installed on your home computer. They are typically used to connect PCs in a building or office within this region and can transmit the data over distances of up to 20 miles.

REPEATER:

A repeater is a two-port device that operates at the physical layer. It is used to regenerate the signal over the same network before it becomes too weak or corrupted, allowing the signal to be transmitted for a longer distance over the same network. It is important to understand that repeaters do not amplify the signal. When the signal weakens, repeaters copy it bit by bit and regenerate it at its original strength.



Types of Repeaters-

On the basis of signals that repeaters generate.

1. **Analog Repeaters:** In an analog repeater, data is transmitted through analog signals to increase its amplitude. These repeaters are used in trunk lines to help broadcast multiple signals using frequency division multiplexing (FDM). It houses the linear amplifier as well as the filters.
2. **Digital Repeaters:** In a digital repeater, data is transmitted in the form of binary digits such as 0s and 1s. While transmitting data, 0 and 1 values are generated, and it is capable of transmitting data over long distances.

Access point:

A wireless device is typically meant by the term access point (AP), even though it technically refers to a wired or wireless connection. The Data Link layer of the OSI model is where an access point (AP) operates. An access point can function as a router or bridge, passing data transmissions from one access point to another. Wireless access points (WAPs) are devices that combine a transmitter and receiver (transceiver) to form a wireless LAN (WLAN). Access points are typically standalone network devices with an antenna, transmitter, and adapter built in. Access points use the wireless infrastructure network mode to connect WLANS to wired Ethernet LANS.

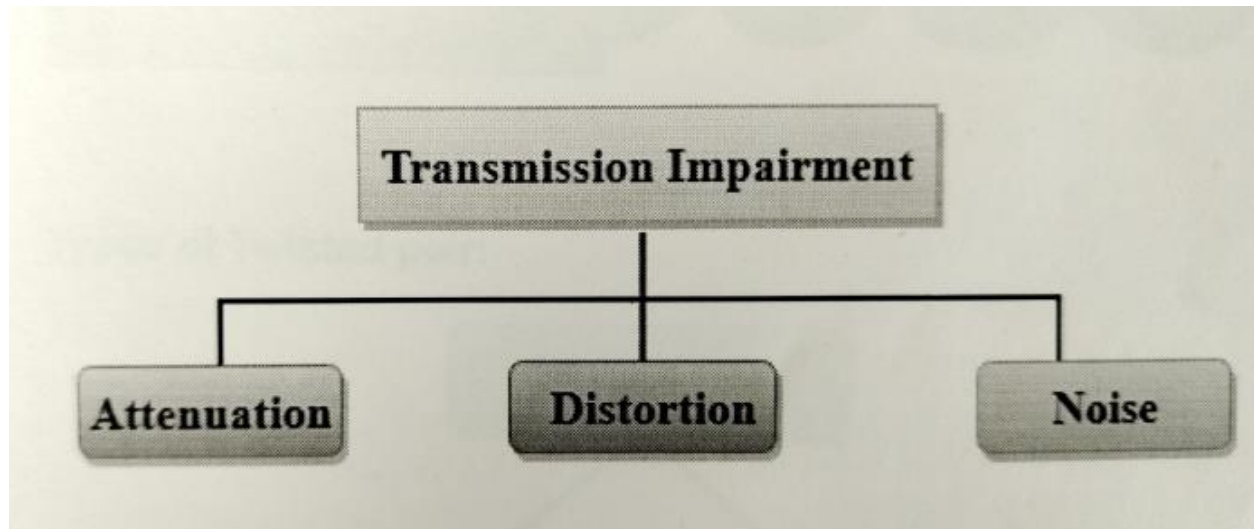
Practical 2: Study of types of transmission medium used in networks.

Transmission media:

- In data communication terminology, 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 a communication channel that carries the information from the sender to the receiver. Data is transmitted through the electromagnetic signals.
- The main functionality of the transmission media is to carry the information in the form of bits through LAN (Local Area Network).
- It is a physical path between transmitter and receiver in data communication.
- In a copper-based network, the bits are in the form of electrical signals. In a fiber-based network, the bits are in the form of light pulses.
- In the OSI (Open System Interconnection) phase, transmission media supports Layer 1. Therefore, it is considered to be a Layer I component.
- The electrical signals can be sent through the copper wire, fiber optics, atmosphere, water, and vacuum,
- The characteristics and quality of data transmission are determined by the characteristics of the medium and signal.
- Transmission media of two types are wired media and wireless media. In wired media, medium characteristics are more important whereas, in wireless media, signal characteristics are more important.
- Different transmission media have different properties such as bandwidth, delay, cost, and ease of installation and maintenance.
- The transmission media is available in the lowest layer of the OSI reference model, i.e. Physical layer.

Some factors need to be considered for designing the transmission media:

- Bandwidth: All the factors remain constant, the greater the bandwidth of a medium, the higher the data transmission rate of a signal.
- Transmission impairment: When the received signal is not identical to the transmitted one due to the transmission impairment. The quality of the signals will be destroyed due to transmission impairment.
- Interference: Interference is defined as the process of disrupting a signal when it travels over a communication medium with the addition of some unwanted signal.



- **Attenuation:** Attenuation means the loss of energy, i.e., the strength of the signal decreases with increasing distance which causes the loss of energy.
- **Distortion:** Distortion occurs when there is a change in the shape of the signal. This type of distortion is examined from different signals having different frequencies. Each frequency component has its propagation speed, so they reach at a different time which leads to the delay distortion.
- **Noise:** When data is traveled over a transmission medium, some unwanted signal is added to it which creates the noise.

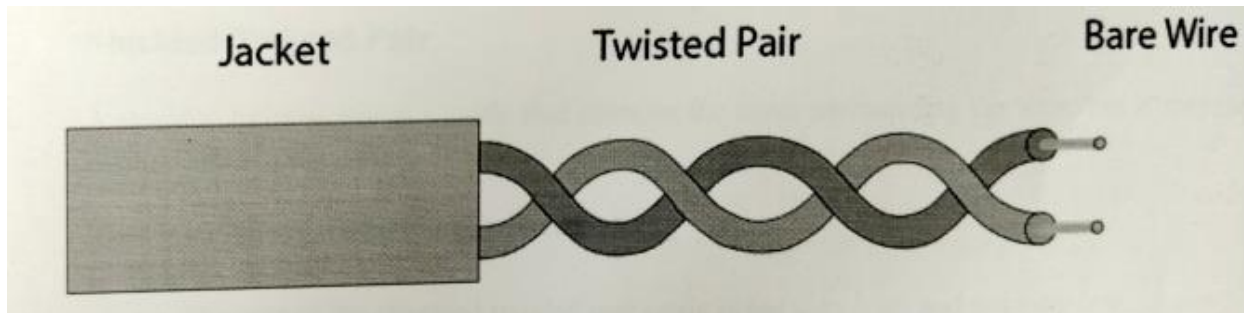
Guided Media:-

It is defined as the physical medium through which the signals are transmitted. It is also known as Bounded media.

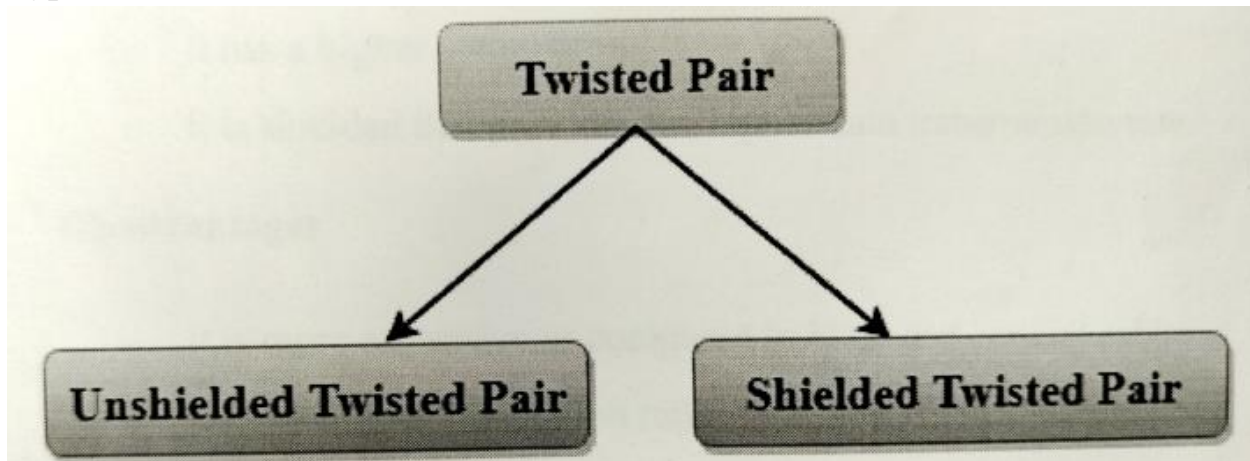
Types Of Guided Media-

Twisted pair:-

- Twisted pair is a physical media made up of a pair of cables twisted with each other. A twisted pair cable is cheap compared to other transmission media. Installation of the twisted pair cable is easy, and it is a lightweight cable. The frequency range for twisted pair cables is from 0 to 3.5KHz.
- A twisted pair consists of two insulated copper wires arranged in a regular spiral pattern.
- The degree of reduction in noise interference is determined by the number of turns per foot. Increasing the number of turns per foot decreases noise interference.



Types of Twisted Pair-



Unshielded Twisted Pair:- The unshielded twisted pair is widely used in telecommunication. Following are the categories of the unshielded twisted pair cable:

Category 1: Category 1 is used for telephone lines that have low-speed data.

Category 2: It can support up to 4 Mbps.

Category 3: It can support up to 16 Mbps.

Category 4: It can support up to 20 Mbps. Therefore, it can be used for long-distance communication.

Category 5: It can support up to 200Mbps.

Advantages of Unshielded Twisted Pair:

- It is cheap.
- Installation of the unshielded twisted pair is easy.
- It can be used for high-speed LAN.

Disadvantages:

- This cable can only be used for shorter distances because of attenuation.

Shielded Twisted Pair:- A shielded twisted pair is a cable that contains the mesh surrounding the wire that allows a higher transmission rate.

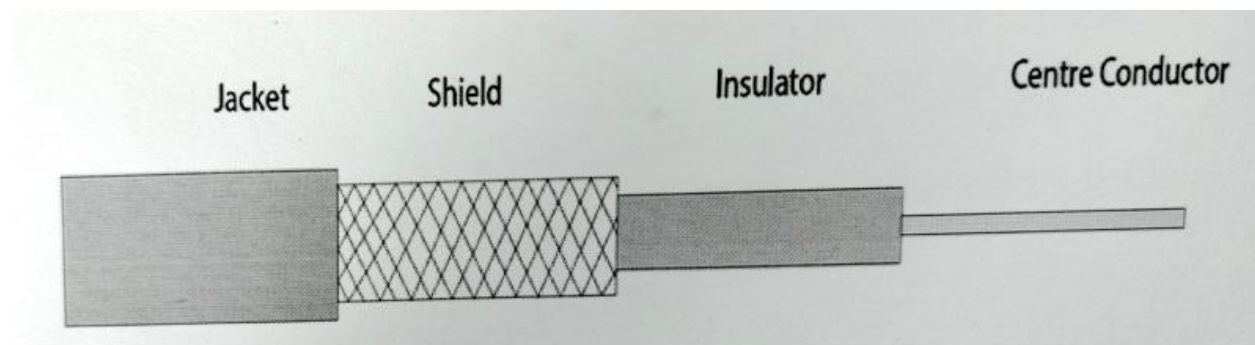
Characteristics of Shielded Twisted Pair-

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

Disadvantages-

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

Coaxial Cable:a



- Coaxial Cable is a very commonly used transmission media, for example, T.V. Wire is usually a coaxial cable.
- The name of the cable is the coaxial, as it contains two conductors parallel to each other.
- It has a higher frequency, as compared to Twisted pair cable.
- The inner conductor of the coaxial cable is made up of copper, and the outer conductor is made up of copper mesh. The middle core is made up of - conductive cover that separates the inner conductor from the outer conductor.
- The middle core is responsible for the data transferring, whereas, the copper mesh prevents from the E.M.I (Electromagnetic Interference)

Coaxial cable is of two types:

1. **Baseband transmission:** It is defined as the process of transmitting a single signal at high speed.
2. **Broadband transmission:** It is defined as the process of transmitting multiple signals simultaneously.

Advantages Of Coaxial cable:

- The data can be transmitted at high speed.
- It has better shielding as compared to twisted pair cable.

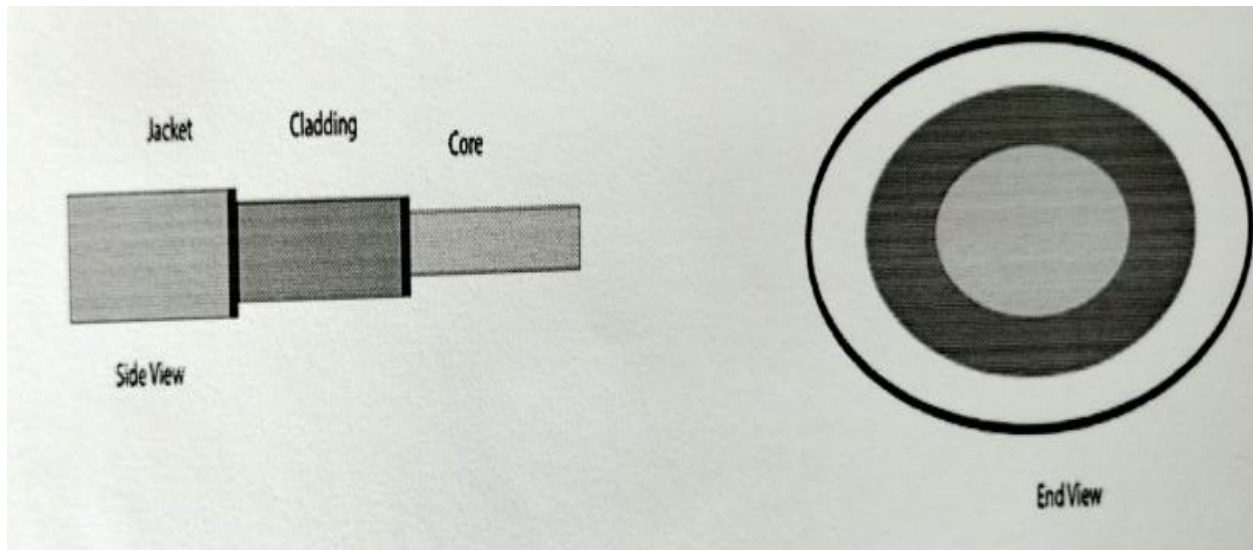
- It provides higher bandwidth.

Disadvantages Of Coaxial cable:

- It is more expensive as compared to twisted pair cable.
- If any fault occurs in the cable causes the failure in the entire network.

Fiber Optic:

- Fiber optic cable is a cable that uses electrical signals for communication.
- Fiber optic is a cable that holds the optical fibers coated in plastic that are used to send the data by pulses of light.
- The plastic coating protects the optical fibers from heat, cold, electromagnetic interference from other types of wiring.



Basic elements of fiber optic cable:

- Core: the optical fiber consists of a narrow strand of glass or plastic known as a core. A core is a light transmission area of the fiber. The more the area of the core, the more light will be transmitted into the fiber.
- Cladding: the concentric layer of glass is known as cladding. The main functionality of the cladding is to provide the lower refractive index at the core interface to cause the reflection within the core so that the light waves are transmitted through the fiber.
- Jacket: the protective coating consisting of plastic is known as a jacket. The main purpose of a jacket is to preserve the fiber strength, absorb shock, and extra fiber protection.

The following are the advantages of fiber optic cable over copper:

- Greater bandwidth: the fiber optic cable provides more bandwidth as compared to copper. Therefore, the fiber optic carries more data as compared to copper cable.
- Faster speed: fiber optical carries the data in the form of light. This allows the fiber optical cable to carry the signals at a higher speed.
- Longer distances: the fiber optic cable carries the data at a longer distance as compared to copper cable.
- Better reliability: the fiber optic cable is more reliable than the copper cable as it is immune to any temperature changes while it can obstruct the connectivity of copper cable.
- Thinner and sturdier: fiber optic cable is thinner and lighter in weight so it can withstand more pull pressure than copper cable.

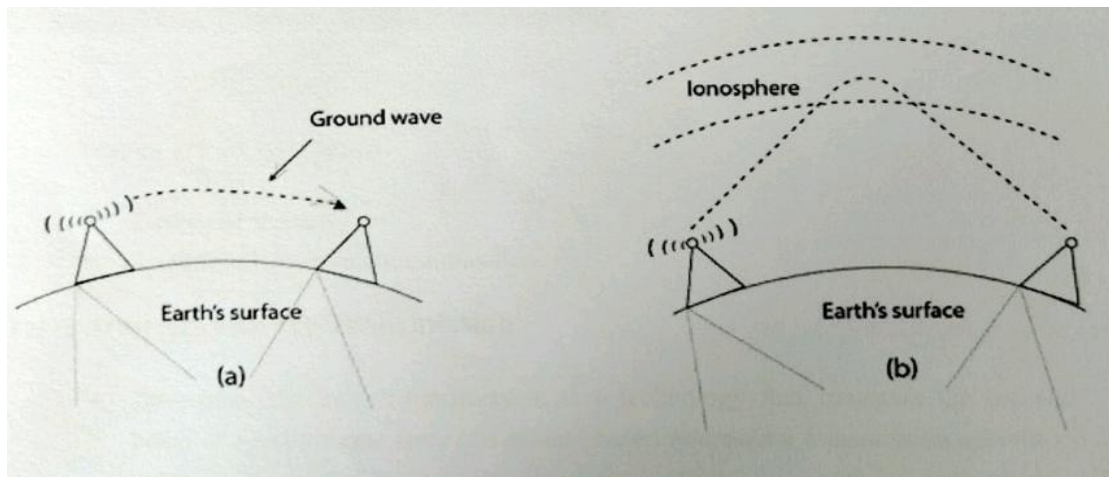
Unguided Transmission:-

- An unguided transmission transmits electromagnetic waves without using any physical medium. Therefore, it is also known as **wireless transmission**.
- In unguided media, air is the medium through which the electromagnetic energy can flow easily.

Unguided transmission is broadly classified into three categories:

Radio waves:

- Radio waves are electromagnetic waves that are transmitted in all the directions of free space.
- Radio waves are omnidirectional, i.e., the signals are propagated in all directions.
- The range in frequencies of radio waves is from 3 KHz to 1 KHz.
- In the case of radio waves, the sending and receiving antenna are not aligned, i.e., the wave sent by the sending antenna can be received by any receiving antenna.
- An example of a radio wave is **FM radio**.



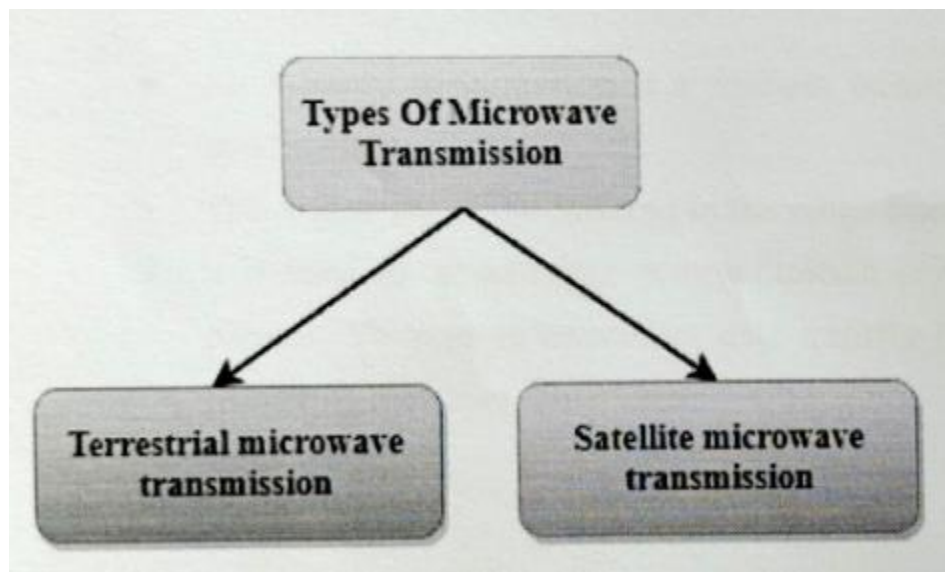
Applications Of Radio waves:

- A Radio wave is useful for multicasting when there is one sender and many receivers.
- An FM Radio, television, cordless phones are examples of a radio wave.

Disadvantages Of Radio transmission:

- Radio transmission is mainly used for wide area networks and mobile cellular phones.
- Radio waves cover a larger area, and they can penetrate the walls.
- Radio transmission provides a higher transmission rate.

Microwaves:



Microwaves are of two types:

1. **Terrestrial microwave**
2. **Satellite microwave communication**

Terrestrial Microwave Transmission-

- Terrestrial Microwave transmission is a technology that transmits the focused beam of a radio signal from one ground-based microwave transmission antenna to another.
- Microwaves are electromagnetic waves having the frequency in the range from 1GHz to 1000GHz.
- Microwaves are unidirectional as the sending and receiving antenna is to be aligned, i.e., the waves sent by the sending antenna are narrowly focussed.
- In this case, antennas are mounted on the towers to send a beam to another antenna which is km away.
- It works on the line-of-sight transmission, i.e., the antennas mounted on the towers are the direct sight of each other.

Satellite Microwave Communication-

- A satellite is a physical object that revolves around the Earth at a known height
- Satellite communication is more reliable nowadays as it offers more flexibility than cable and fiber optic systems.
- We can communicate with any point on the globe by using satellite communication.

Infrared Waves:

- An infrared transmission is a wireless technology used for communication over short ranges.
- The frequency of the infrared in the range from 300 GHz to 400 THz.
- It is used for short-range communication such as data transfer between two cell phones, TV remote operation, data transfer between a computer and cell phone resides in the same closed area.

Characteristics Of Infrared Waves:

- It supports high bandwidth, and hence the data rate will be very high.
- Infrared waves cannot penetrate the walls. Therefore, the infrared communication in one room cannot be interrupted by the nearby rooms.
- An infrared communication provides better security with minimum interference.
- Infrared communication is unreliable outside the building because the sun rays will interfere with the infrared waves.

Practical 3: Introduction to basic networking tools: Wireshark, Network miner.

What is Wireshark?

Wireshark is an open-source packet analyzer, which is used for education, analysis, software development, communication protocol development, and network troubleshooting.

It is used to track the packets so that each one is filtered to meet our specific needs. It is commonly called as sniffer, network analyzer, and protocol analyzer. It is also used by network security to examine security problems.

Wireshark is a free-to-use application that is used to apprehend the data back and forth. It is often called a free packet sniffer computer application. It puts the network card into an unselective mode that i.e., to accept all packets that it receives.

Uses of Wireshark:

1. It is used by network security engineers to examine security problems.
2. It allows users to watch all traffic being passed over the network.
3. It is used by network engineers to troubleshoot network issues.
4. It also helps to troubleshoot latency issues and malicious activities on your network.
5. It can also analyze dropped packets.
6. It helps us to know how all the devices like laptops, mobile phones, desktops, switches, routers, etc., communicate in a local network or the rest of the world.

What is a packet?

A packet is a unit of data that is transmitted over a network between the origin and the destination. Network packets are small, i.e., maximum of 1.5 Kilobytes for Ethernet packets and 64 Kilobytes for IP packets. The data packets in the Wireshark can be viewed online and can be analyzed offline.

Color coding in Wireshark:

The packets in the Wireshark are highlighted with blue, black, and green colors. These colors help users to identify the types of traffic. It is also called packet colorization. The kinds of coloring rules in the Wireshark are temporary rules and permanent rules.

- 1)The temporary rules are there until the program is in active mode or until we quit the program.
- 2)The permanent color rules are available until the Wireshark is in use or the next time you run the Wireshark. The steps to apply color filters will be discussed later in this topic.

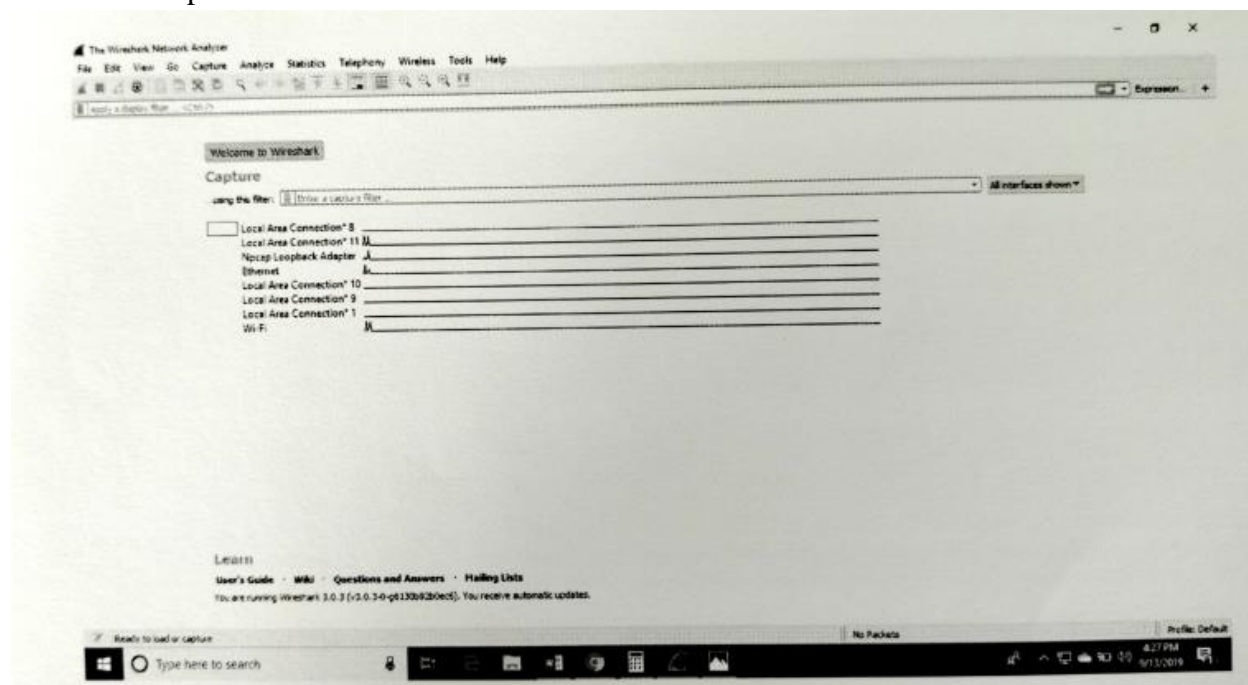
Installation of Wireshark Software:

Below are the steps to install the Wireshark software on the computer:

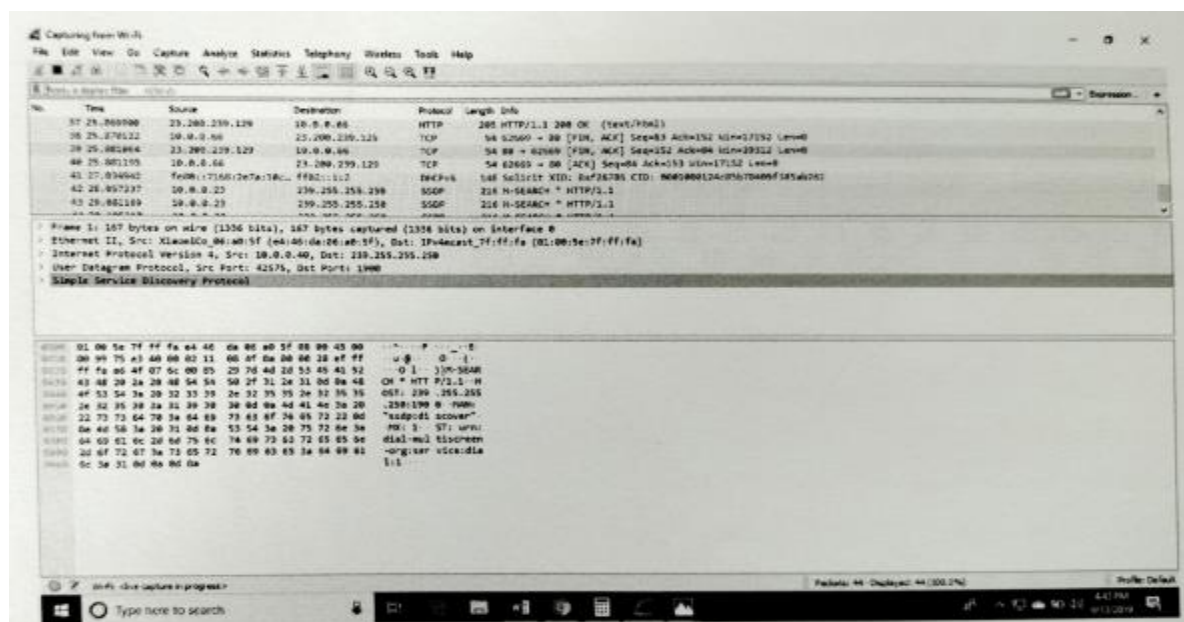
1. Open the web browser.
2. Search for 'Download Wireshark.'
3. Select the Windows installer according to your system configuration, either 32-bit or 64-bit. Save the program and close the browser.
4. Now, open the software, and follow the install instructions by accepting the license.
5. The Wireshark is ready for use.

On the network and Internet settings option, we can check the interface connected to our computer.

By selecting the current interface, we can get the traffic traversing through that interface. This version will open as:



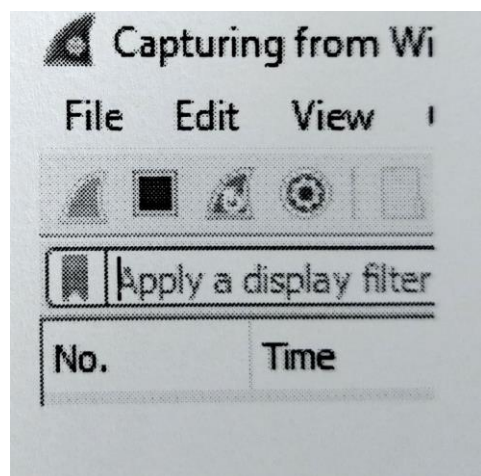
The options given on the list are the Interface list options. A number of interface options will be present. The selection of any option will determine all the traffic. For example, from the above fig. select the Wi-Fi option. After this, a new window opens up, which will show all the current traffic on the network. Below is the image that tells us about the live capture of packets and our Wireshark will look like:



The above arrow shows the packet content written in hexadecimal or the ASCII format. And the information above the packet content, are the details of the packet header.

It will continue listening to all the data packets, and you will get much data. If you want to see a particular data, then you can click on the red button. The traffic will be stationary, and you can note the parameters like time, source, destination, the protocol being used, length, and the Info. To view in-depth detail, you can click on that particular address; a lot of the information will be displayed below that.

There will be detailed information on HTTP packets, TCP packets, etc. The red button is shown below:

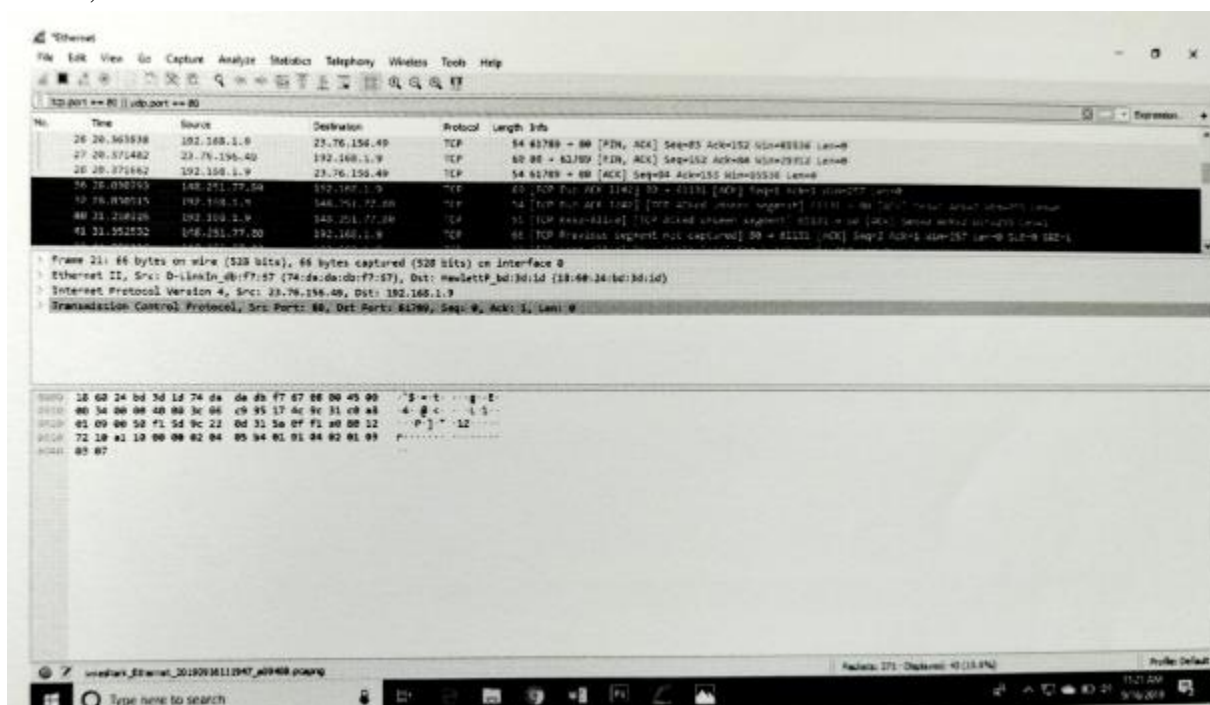


The screen/interface of the Wireshark is divided into five parts:

- First part contains a menu bar and the options displayed below it. This part is at the top of the window. File and the capture menus options are commonly used in Wireshark. The capture menu allows to start the capturing process. And the File menu is used to open and save a capture file.
- The second part is the packet listing window. It determines the packet flow or the captured packets in the traffic. It includes the packet number, time, source, destination, protocol, length, and info. We can sort the packet list by clicking on the column name.
- Next comes the packet header-detailed window. It contains detailed information about the components of the packets. The protocol info can also be expanded or minimized according to the information required.
- The bottom window is called the packet contents window, which displays the content in ASCII and hexadecimal format.

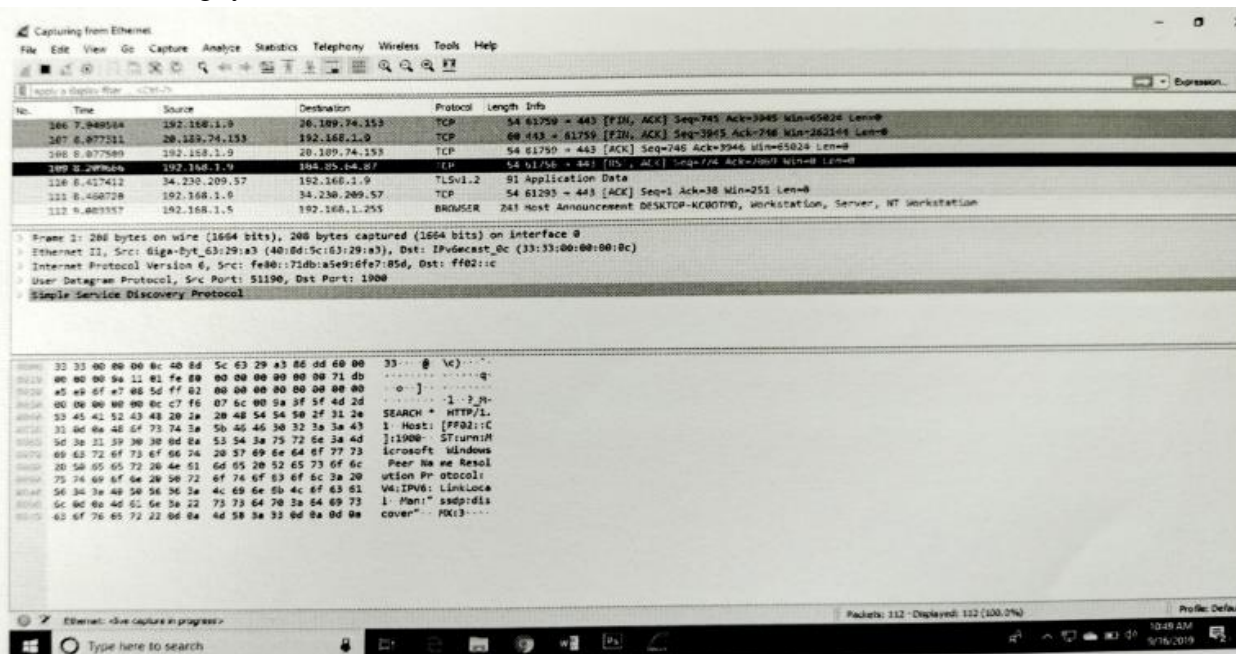
At last, is the filter field which is at the top of the display. The captured packets on the screen can be filtered based on any component according to your requirements. For example, if we want to see only the packets with the HTTP protocol, we can apply Filters to that option. All the packets with HTTP as the protocol will only be displayed on the screen, shown below:

Filters to that option. All the packets with HTTP as the protocol will only be displayed on the screen, shown below:

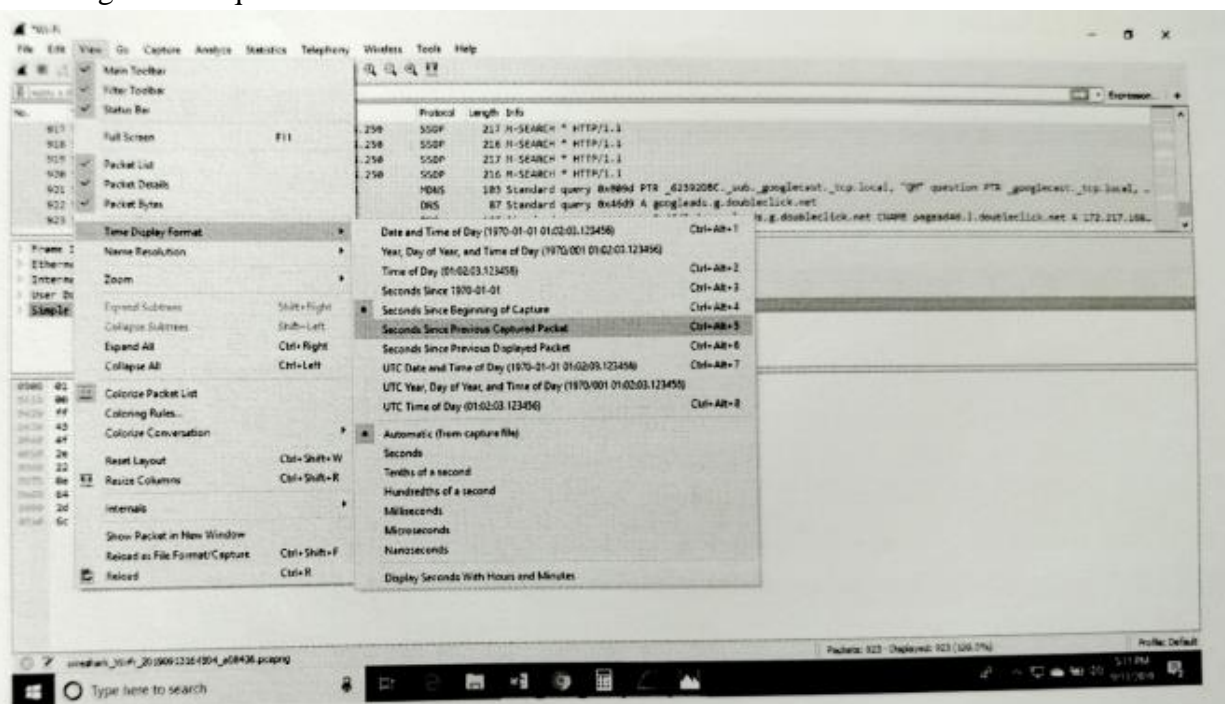


You can also select the connection to which your computer is connected. For example, in this PC, we have chosen the current network, i.e., the ETHERNET.

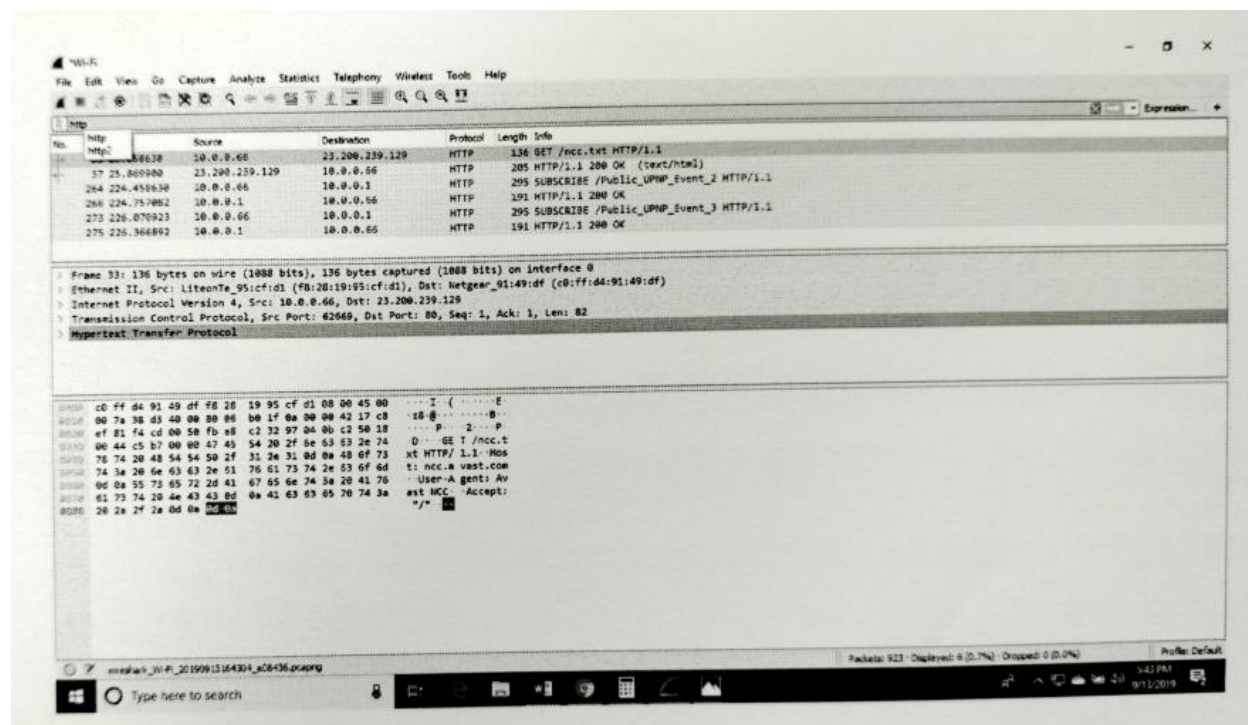
After connecting, you can watch the traffic below:



In the view option on the menu bar, we can also change the view of the interface. You can change the number of things in the view menu. You can also enable or disable any option according to the requirement.

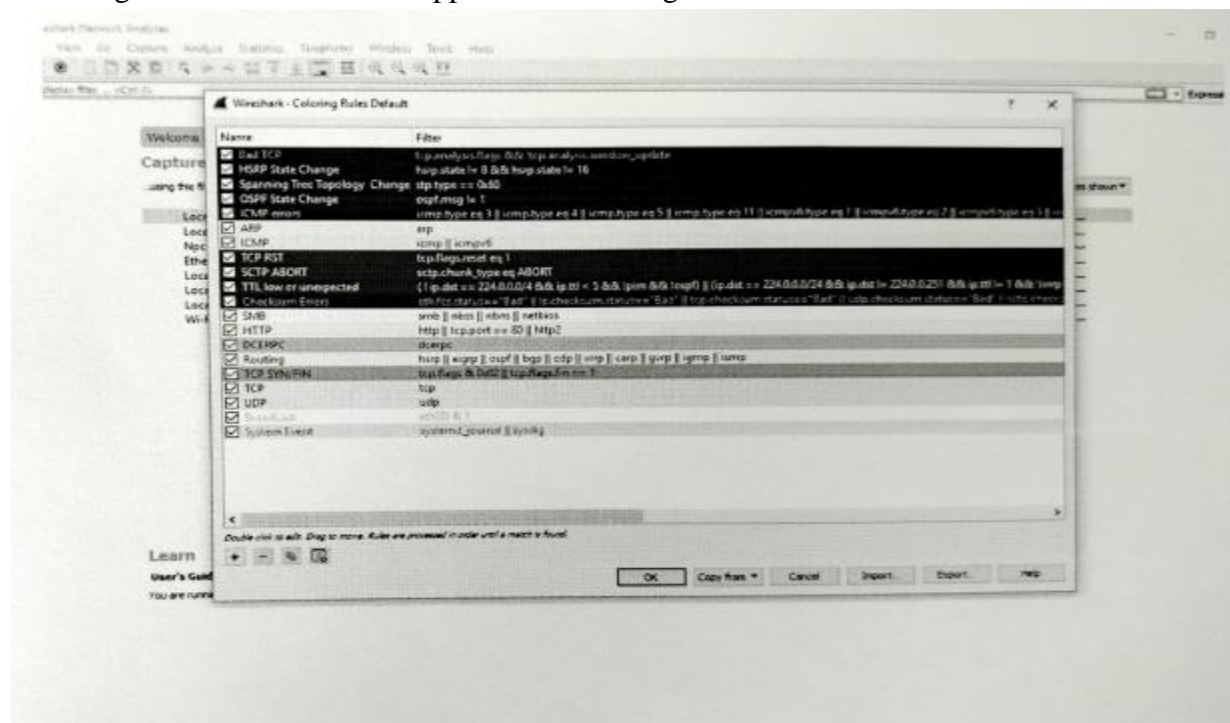


There is a filter block below the menu bar, from where a large amount of data can be filtered. For example, if we apply a filter for HTTP, only the interfaces with the HTTP will be listed.



If you want to filter according to the source, right-click on the source you want to filter and select 'Apply as Filter' and choose '...and filter.'

Steps for the permanent colorization are: click on the 'View' option on the menu bar and select 'Coloring Rules.' The table will appear like the image shown below:



Most used Filters in Wireshark:

Whenever we type any commands in the filter command box, it turns green if your command is correct. It turns red if it is incorrect or the Wireshark does not recognize your command.

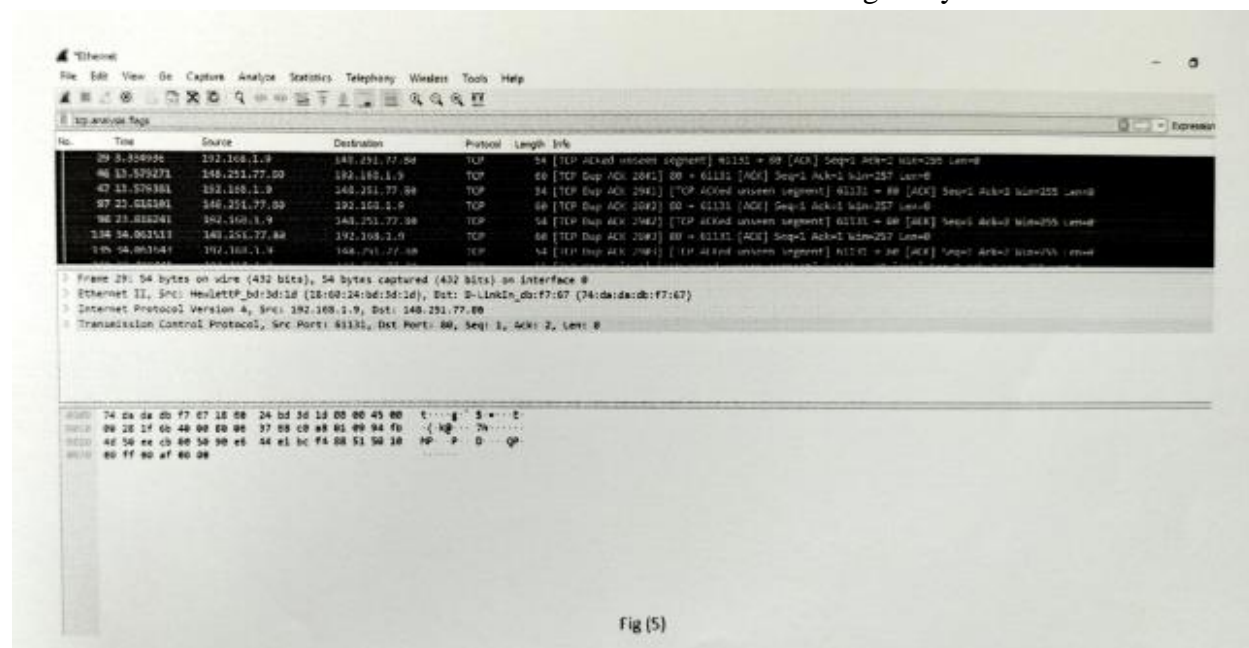


Fig (5)

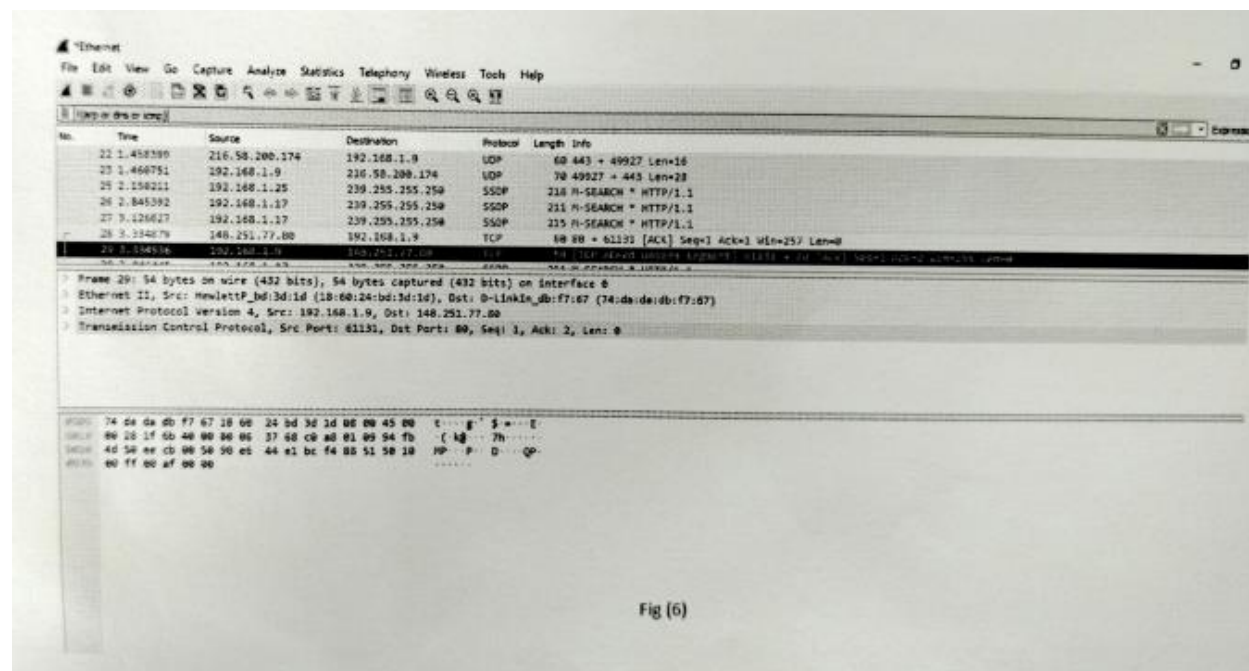


Fig (6)

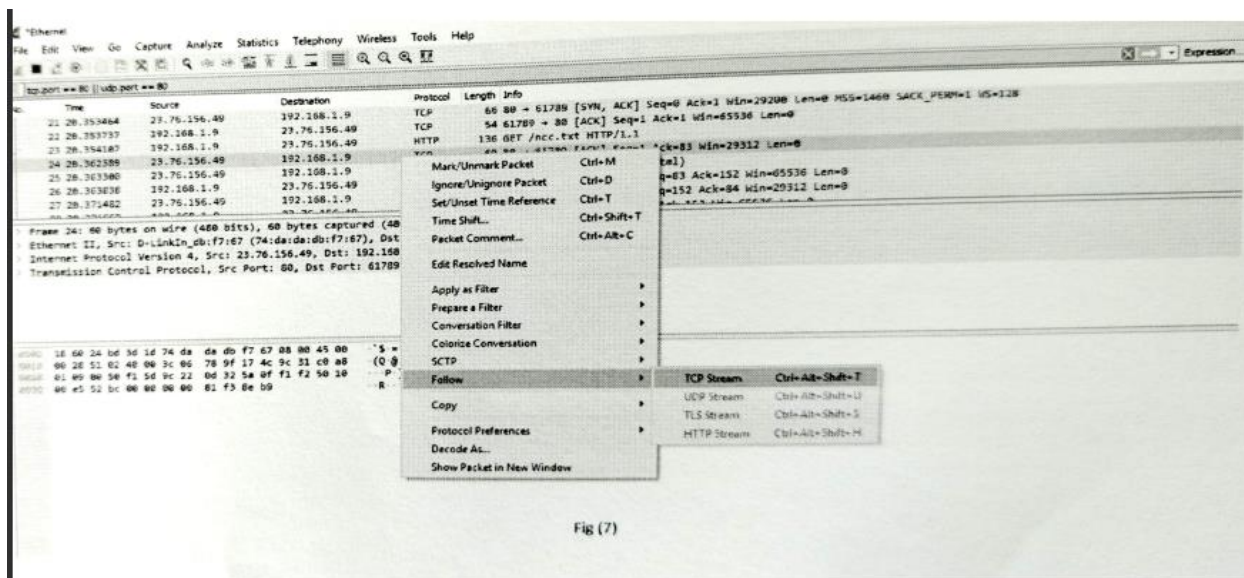


Fig (7)

Filters	Description
<p>ip.addr</p> <p>Example-ip.addr==10.0.10.142</p> <p>ip.src</p> <p>ip.dst</p>	<p>It is used to specify the IP address as the source or the destination.</p> <p>This example will filter based on this IP address as a source and a destination.</p> <p>If we want a particular source or destination then.</p> <p>It is used for the source filter.</p> <p>It is used for the destination.</p>
<p>Protocol</p> <p>Example- dns or http</p> <p>‘dns and http’ are never used.</p>	<p>This command filters based on the protocol.</p> <p>It requires the packet to be either dns protocol or http protocol and will display the traffic based on this.</p> <p>We would not use the command ‘dns and http’ because it requires the packet to be both, dns as well as http, which is impossible.</p>
<p>Tcp.port</p> <p>Example: tcp.port==443</p>	<p>It sets filters based on the specific port number. It will filter all the packets with this port number.</p>
<p>4. udp.port</p>	<p>It is the same as tcp.port. Instead, udp is used.</p>
<p>tcp.analysis.flags</p> <p>Example is shown in fig (5)</p>	<p>Wireshark can flag TCP problems. This command will only display the issues that Wireshark identifies.</p> <p>For example, packet loss, tcp segment not captured, etc. are some of the problems.</p> <p>It quickly identifies the problem and is widely used.</p>

6.! For example, !(arp or dns or icmp) This is shown in fig (6).	It is used to filter the list of protocols or applications, in which we are not interested. It will remove arp, dns, and icmp, and only the remaining will be left or it will clean the things that may not be helpful.
Select any packet. Right-click on it and select 'Follow' and then select 'stream.' Shown in fig. (7).	It is used if you want to work on a single connection in a TCP conversation. Anything related to the single TCP connection will be displayed on the screen
top contains the filter For example- tcp contains Facebook Or udp contains Facebook	It is used to display the packets which contain such words. In this, Facebook word in any packet in this trace file i.e., finding the devices, that are talking to Facebook. This command is useful if you are looking for a username, word, etc
http.request For the responses or the response code, file. you can type http.response.code==200	It will display all the http requests in the trace file You can see all the servers, the client is involved.
tcp.flags.syn==1 This is tcp.flags.reset	This will display all the packets with the sync built-in top header set to 1. This will show all the packets with top resets.

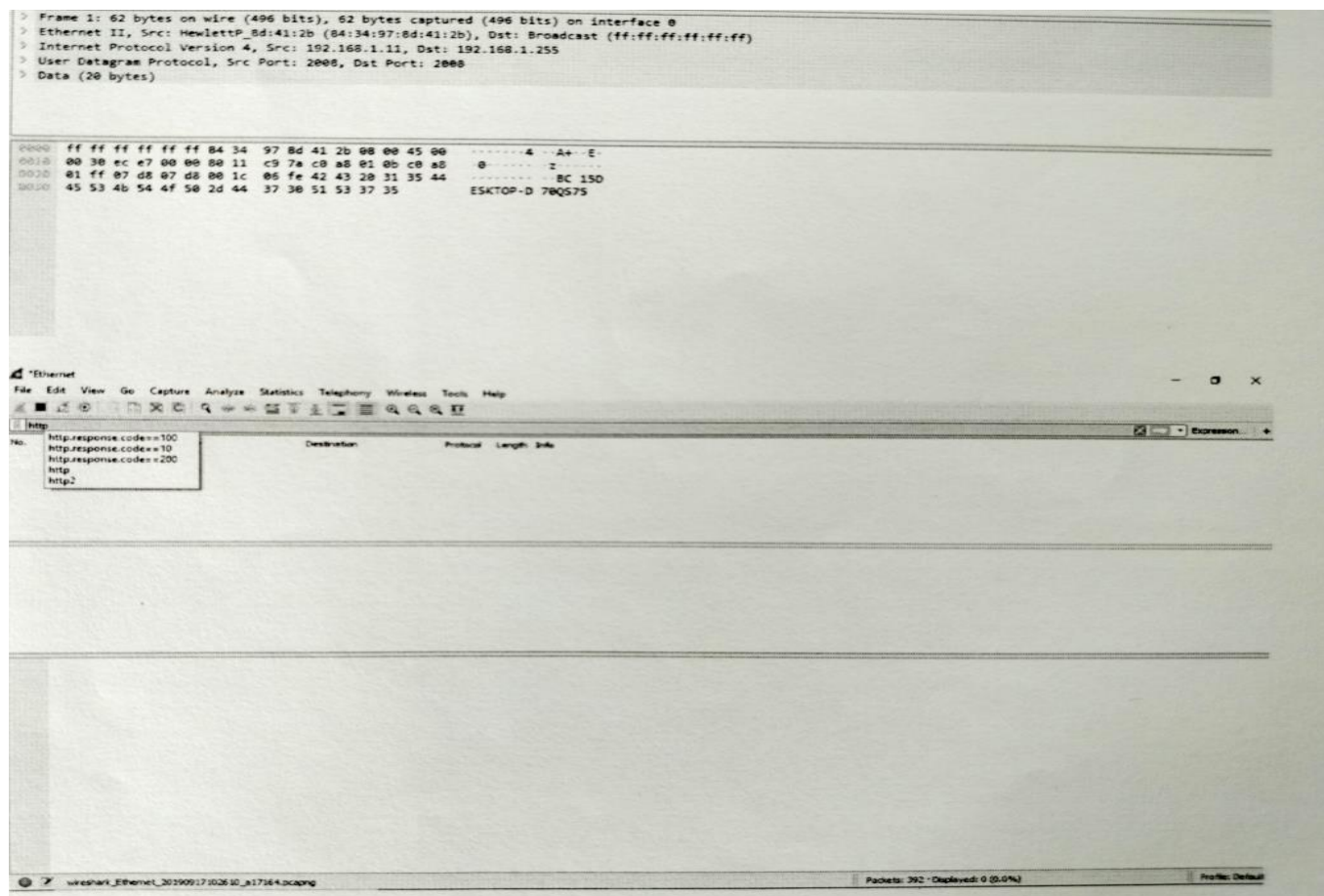
Wireshark packet sniffing

Wireshark is a packet sniffing program that administrators can use to isolate and troubleshoot problems on the network. It can also be used to capture sensitive data like usernames and passwords. It can also be used in the wrong way (hacking) to eavesdrop.

Packet sniffing is defined as the process of capturing the packets of data flowing across a computer network. The Packet sniffer is a device or software used for the process of sniffing.

Below are the steps for packet sniffing:

- Open the Wireshark Application.
- Select the current interface. Here in this example, the interface is External which we would be using.
- The network traffic will be shown below, which will be continuous. To stop or watch any particular packet, you can press the red button below the menu bar.



The above screen is blank, i.e.; there is no network traffic as of now.

Open the browser. In this example, we have opened the 'Internet Explorer.' You can choose any browser.

As soon as we open the browser, and type any address of the website, the traffic will start showing, and the exchange of the packets will also start. The image for this is shown below:



Practical 4: Hands on of various services/Commands like Ping, Trace Route etc.

Ping:

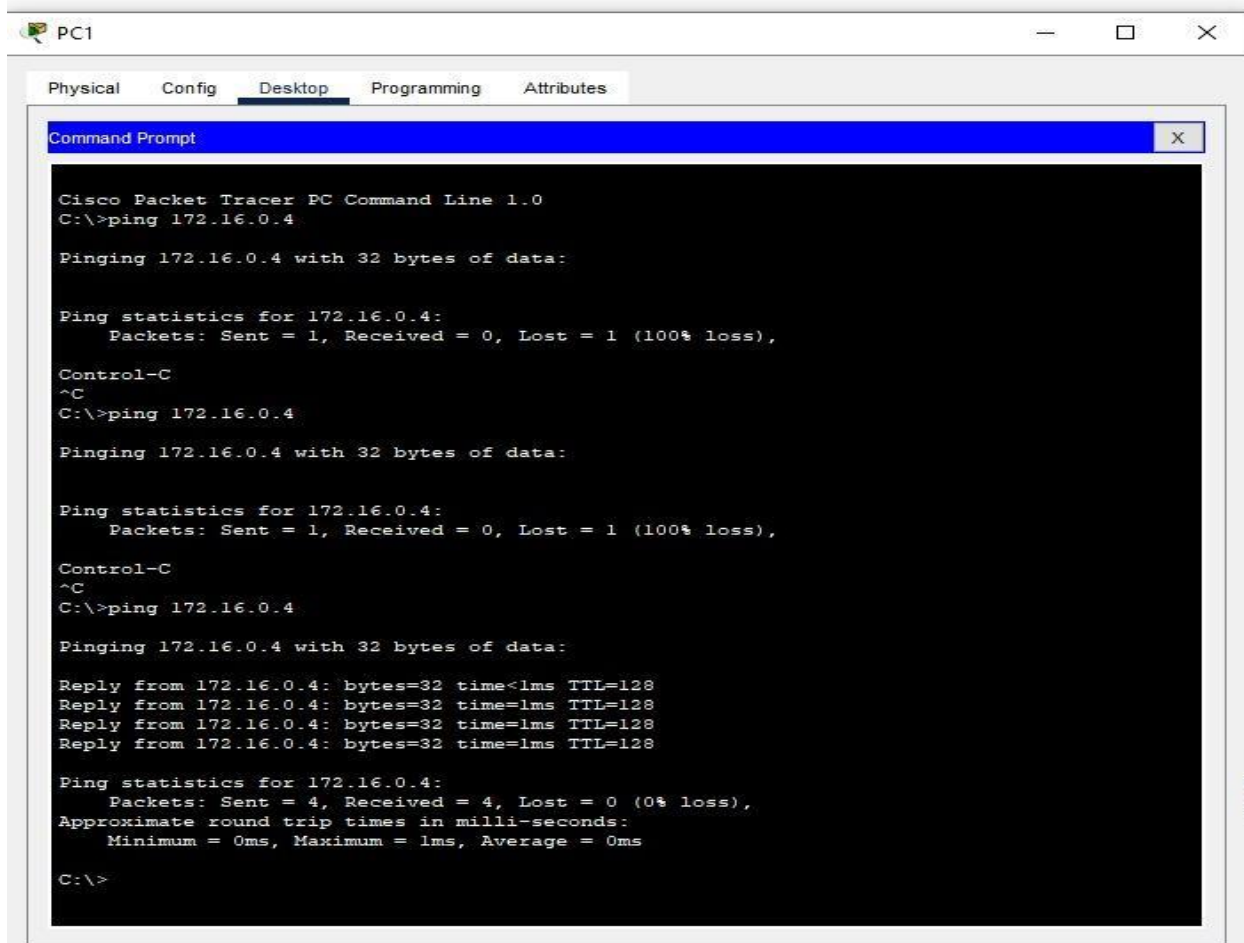
Ping is a network utility used to see if the end user can reach other devices connected to the internet. When using Ping, always test a few different sites to see if it is just one site or all sites. To ping a device, proceed as follows.

- Open a Windows Command Prompt window.
- At the command prompt, type, ping <IP address>, as shown below.

Note: You can interrupt Ping at any time by holding down the CTRL key, and pressing C on your keyboard.

Understanding Ping results-

Ping operates by sending ICMP Echo Request packets to the target device and waiting for an ICMP Echo Reply. The program reports errors, packet loss, and a statistical summary of the results.



```
PC1
Physical  Config  Desktop  Programming  Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 172.16.0.4

Pinging 172.16.0.4 with 32 bytes of data:

Ping statistics for 172.16.0.4:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),

Control-C
^C
C:\>ping 172.16.0.4

Pinging 172.16.0.4 with 32 bytes of data:

Ping statistics for 172.16.0.4:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),

Control-C
^C
C:\>ping 172.16.0.4

Pinging 172.16.0.4 with 32 bytes of data:

Reply from 172.16.0.4: bytes=32 time<lms TTL=128
Reply from 172.16.0.4: bytes=32 time=lms TTL=128
Reply from 172.16.0.4: bytes=32 time=lms TTL=128
Reply from 172.16.0.4: bytes=32 time=lms TTL=128

Ping statistics for 172.16.0.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>
```

PathPing:

This network utility is a more advanced version of the Ping tool, which performs a ping to each hop along the route to the destination (unlike Ping, which just pings from the originating device to the destination device). It is extremely useful in diagnosing packet loss, and can help with diagnosing slow speed faults. To PathPing a device, proceed as follows.

- Open a Windows Command Prompt window.
- At the command prompt, type, pathping <IP address>, as shown below.

Note: You can interrupt PathPing at any time by holding down the CTRL key, and pressing C on your keyboard.

Understanding PathPing results-

The advantages of PathPing over Ping and Traceroute are that each node is pinged as the result of a single command, and that the behavior of nodes is studied over an extended time period, rather than the default ping sample of four messages, or default traceroute single route trace. The disadvantage is that it takes a total of 25 seconds per hop to show the PathPing statistics.

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

Tracing route to www.google.com [142.250.194.100]
over a maximum of 30 hops:
 0  Dhananjay [192.168.1.2]
 1  192.168.1.1 [192.168.1.1]
 2  10.85.66.1 [10.85.66.1]
 3  103.151.230.1
 4  163.53.87.1
 5  72.14.209.116
 6  142.251.248.255
 7  142.251.52.223
 8  del12s04-in-f4.1e100.net [142.250.194.100]

Computing statistics for 200 seconds...
Hop  RTT      Source to Here  This Node/Link  Address
    0                                     Dhananjay [192.168.1.2]
    1   5ms      0/ 100 = 0%      0/ 100 = 0%      192.168.1.1 [192.168.1.1]
    2   6ms      2/ 100 = 2%      1/ 100 = 1%      10.85.66.1 [10.85.66.1]
    3   7ms      2/ 100 = 2%      1/ 100 = 1%      103.151.230.1
    4   9ms      2/ 100 = 2%      1/ 100 = 1%      163.53.87.1
    5  11ms      2/ 100 = 2%      1/ 100 = 1%      72.14.209.116
    6  10ms      2/ 100 = 2%      1/ 100 = 1%      142.251.248.255
    7  ---      100/ 100 =100%   99/ 100 = 99%    142.251.52.223
    8  11ms      1/ 100 = 1%      0/ 100 = 0%      del12s04-in-f4.1e100.net [142.250.194.100]

Trace complete.
```


Traceroute:

Traceroute is a computer network diagnostic tool for displaying the route (path), and measuring transit delays, of packets across an Internet Protocol (IP) network.

To run the Traceroute utility, proceed as follows.

- Open a Windows Command Prompt window.
- At the command prompt, type, `tracert <domain.ext>` (replace `<domain.ext>` with the domain name and extension that you would like to trace a route to).
- It may take a few seconds to respond, but this command will give a traceroute from your computer to the destination you selected.

Note: You can interrupt Traceroute at any time by holding down the CTRL key, and pressing C on your keyboard.

Understanding Traceroute results-

The Traceroute tool is used to map the hops between the end user and the destination server. This can help determine where any issues may lie on the network.

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

Tracing route to www.google.com [142.250.192.36]
over a maximum of 30 hops:

  1      1 ms      1 ms      1 ms    192.168.1.1 [192.168.1.1]
  2      4 ms      1 ms      2 ms    10.85.66.1 [10.85.66.1]
  3      5 ms      2 ms      2 ms    103.151.230.1
  4      6 ms      3 ms      3 ms    163.53.87.1
  5      7 ms      3 ms      3 ms    72.14.209.116
  6      5 ms      3 ms      3 ms    72.14.234.223
  7      6 ms      4 ms     23 ms    192.178.83.206
  8      6 ms      4 ms      6 ms    142.250.63.116
  9     27 ms     27 ms     27 ms    142.250.230.116
 10     24 ms     25 ms     25 ms    192.178.110.205
 11     26 ms     25 ms     26 ms    142.250.210.183
 12     25 ms     25 ms     26 ms    bom12s15-in-f4.1e100.net [142.250.192.36]

Trace complete.
```

Practical 5: Create various network topologies using Cisco Packet Tracer.

Topology:

In Computer Network, there are various ways through which different components are connected to one another. Network Topology is the way that defines the structure, and how these components are connected to each other.

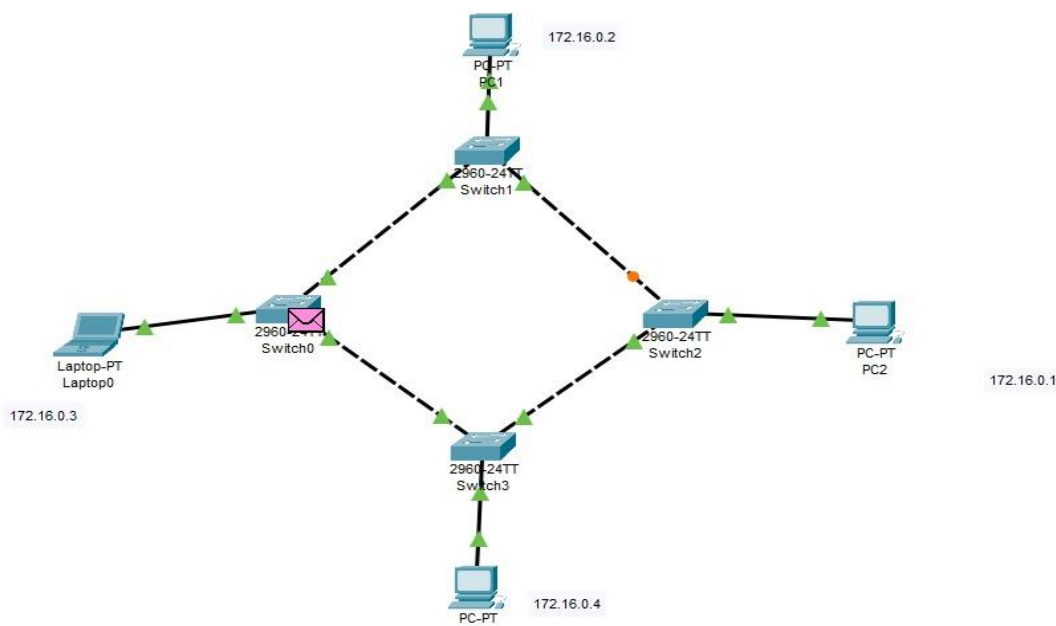
Types of Network Topology-

The arrangement of a network that comprises nodes and connecting lines via sender and receiver is referred to as Network Topology. The various network topologies are:

- Point to Point Topology
- Mesh Topology
- Star Topology
- Bus Topology
- Ring Topology
- Tree Topology
- Hybrid Topology

Ring Topology:

A ring topology is a type of network configuration in which each network device is connected to exactly two other devices, forming a single continuous pathway for signals through each device. Data travels in one direction around the ring until it reaches its destination.



Advantages:-

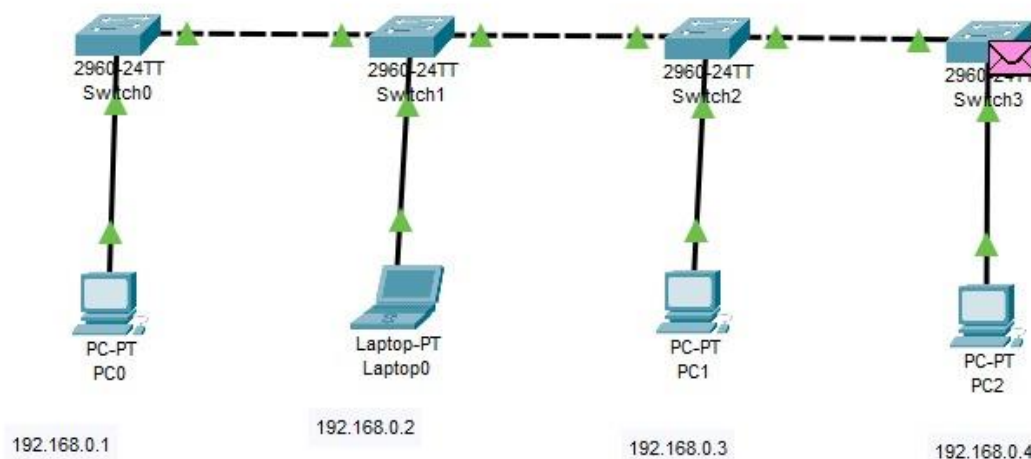
- 1) Simple and Easy to Install: Setting up a ring network is relatively straightforward as it involves connecting each device to its neighboring devices.
- 2) Efficient Data Transfer: Data travels directly between adjacent nodes, which can lead to faster and more efficient data transmission compared to some other topologies like bus networks.
- 3) No Centralized Device: Unlike star topologies where a central device manages communication, each device in a ring topology has equal status. This can enhance the overall robustness of the network.
- 4) No Collisions: In a ring topology, data collisions are minimized since only one device can transmit at a time. Each node receives data in a sequential manner.
- 5) Suitable for Limited Number of Nodes: Ring topologies are effective when the number of network nodes is relatively small and when the transmission distances between nodes are not too large.

Disadvantage:-

- 1) Single Point of Failure: The main drawback of a ring topology is its susceptibility to a single point of failure. If one node or connection in the ring fails, the entire network can be disrupted.
- 2) Difficult to Troubleshoot: Locating faults or failures in a ring network can be challenging. If a node fails or if there's a break in the cable, identifying the exact location of the problem can require significant effort and time.
- 3) Limited Scalability: Ring topologies may struggle to scale effectively as the number of nodes increases. Adding or removing nodes can disrupt the entire network and require reconfiguration.
- 4) Data Collision Risk with High Traffic: While collisions are less frequent compared to bus topologies, a high volume of traffic or frequent transmissions can still lead to data collisions and network congestion.
- 5) Higher Latency for Large Networks: As the number of nodes increases or if the physical size of the network grows, the latency (time delay) can increase due to the data having to traverse multiple nodes.

Bus Topology:

A bus topology is a type of network architecture where all devices are connected to a single communication line, often referred to as a "bus." In this setup, data travels along the bus, and each device on the network receives all transmissions but only processes those intended for it.



Advantages:-

1. **Simplicity:** Bus topology is straightforward to set up and understand. It requires minimal cabling compared to other topologies, making it cost-effective for small to medium-sized networks.
2. **Cost-Effective:** Because it requires less cabling and hardware, bus topology tends to be more economical, especially for smaller networks. This makes it a popular choice for small businesses and home networks.
3. **Ease of Expansion:** Adding new devices to a bus network is relatively easy. You can simply connect the new device to the main communication line without disrupting the existing network.
4. **Fault Isolation:** If a single device fails in a bus network, it typically does not affect the operation of other devices. The rest of the network can continue functioning normally.
5. **No Centralized Control:** Unlike some other topologies, such as star or ring, bus networks do not require a central controlling device, which can reduce complexity and points of failure.

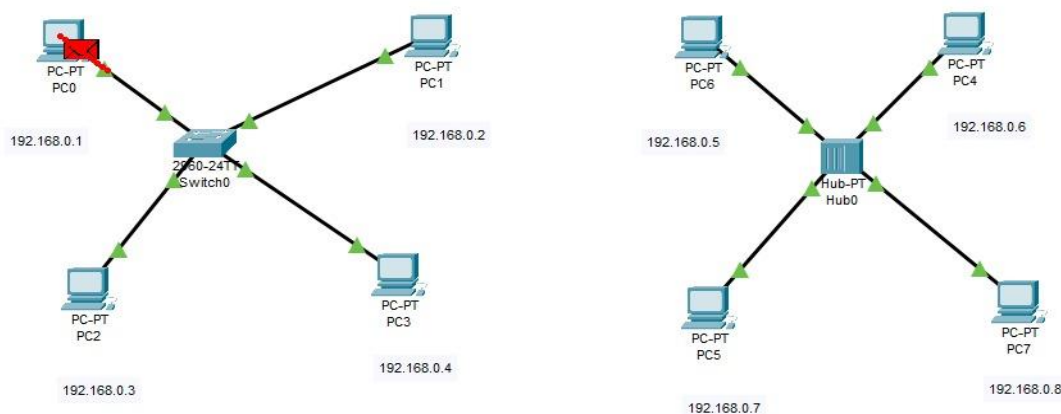
Disadvantages:-

1. **Limited Cable Length:** The length of the communication line (the bus) is limited due to factors such as signal attenuation and the need for proper termination. This limits the size of bus networks compared to other topologies.
2. **Potential for Collisions:** Because all devices share the same communication medium, there is a risk of collisions if multiple devices attempt to transmit data simultaneously. Collisions can lead to data corruption and network congestion.

3. **Performance Degradation:** As the number of devices connected to the bus increases, the performance of the network can degrade. This is because each device must contend for access to the communication line, leading to increased collisions and slower data transfer rates.
4. **Difficulty in Identifying Faults:** While a single device failure typically does not affect the rest of the network, identifying the location of a fault in the communication line can be challenging, especially in large networks.
5. **Security Concerns:** In a bus topology, all devices receive all transmissions. Without additional security measures, unauthorized users can eavesdrop on network traffic, posing security risks.

Star Topology:

A star topology, sometimes known as a star network, is a network topology in which each device is connected to a central hub. It is one of the most prevalent computer network configurations, and it's by far the most popular Network Topology. In this network arrangement, all devices linked to a central network device are displayed as a star.



Advantages:-

1. It is very reliable – if one cable or device fails then all the others will still work.
2. It is high-performing as no data collisions can occur.
3. Less expensive because each device only one I/O port and wishes to be connected with hub with one link.
4. Easier to put in
5. Robust in nature

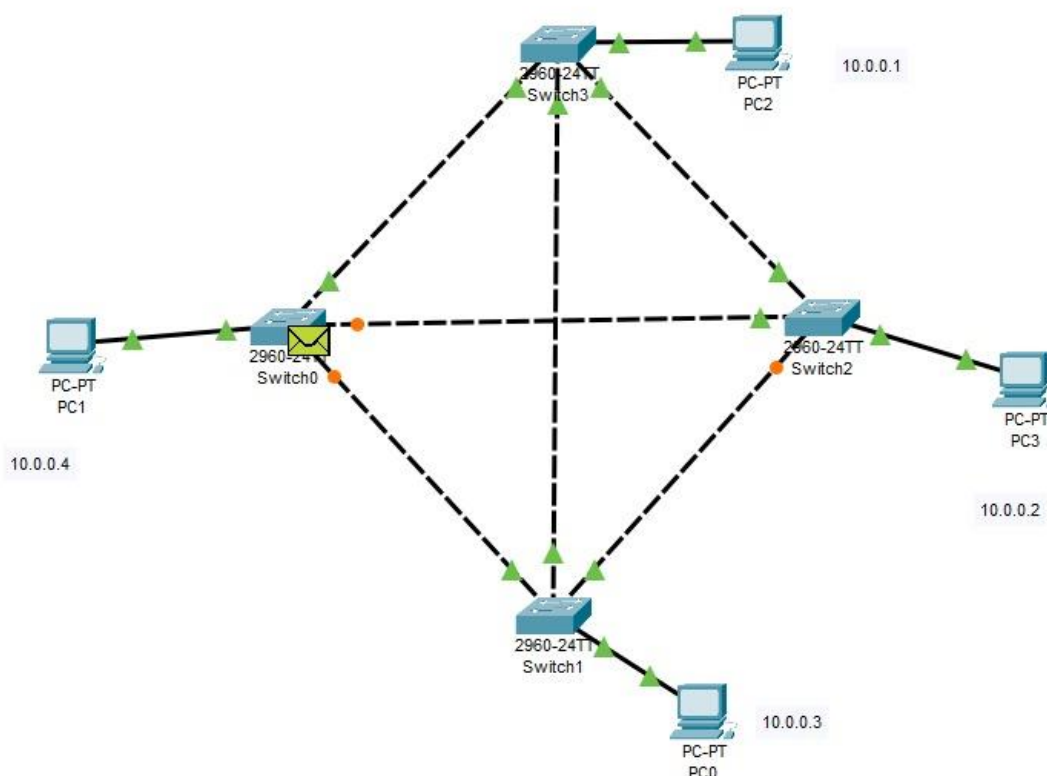
Disadvantages:-

1. Requires more cable than a linear bus.
2. If the connecting network device (network switch) fails, nodes attached are disabled and can't participate in network communication.

3. More expensive than linear bus topology due to the value of the connecting devices (network switches)
4. If hub goes down everything goes down, none of the devices can work without hub.
5. Hub requires more resources and regular maintenance because it's the central system of star.

Mesh Topology:

Mesh topology is a network topology where each device (or node) is connected to every other device, forming a web-like structure. This allows for multiple paths for data to travel between devices, providing redundancy and robustness to the network.



Advantages:-

1. Redundancy: Multiple paths for data to travel, making the network more reliable.
2. Robustness: Failure of one device won't affect the entire network.
3. Flexibility: Easy to add or remove devices without disrupting the network.
4. High availability: Network remains operational even if one or more devices fail.
5. Scalability: Can handle a large number of devices.

Disadvantages:-

1. Complexity: More connections and devices make the network harder to manage.
2. Cost: Requires more cables and devices, increasing costs.
3. Traffic congestion: Multiple devices sending data simultaneously can cause congestion.

4. Network maintenance: Difficult to identify and troubleshoot issues.
5. Security risks: More connections increase the risk of security breaches.

Practical 6: Study Various router configuration commands.

Configuring Global Parameters:

To configure the global parameters for your router, follow these steps.

SUMMARY STEPS-

1. **configure terminal**
2. **Hostname** *name*
3. **Enable secret** *password*
4. **No ip domain-lookup**

DETAILED STEPS-

	Command	Purpose
Step 1	configure terminal Example: Router> enable Router# configure terminal	Enters global configuration mode, when using the console port.
Step 2	Hostname <i>name</i> Example: Router(config)# hostname Router	Specifies the name for the router.
Step 3	Enable secret password Example: Router config # enable secret criny5ho	Specifies an encrypted password to prevent unauthorized access to the router.
Step 4	No ip domain lookup Example: Router config # no ip domain- lookup	Disables the router from translating unfamiliar words into IP addresses.

Configuring Gigabit Ethernet WAN interfaces:

SUMMARY STEPS-

1. **Configure terminal**
2. **interface gigabitethernet slot/port**
3. **ip address** ip-address mask
4. **No shutdown**
5. **Exit**

DETAILED STEPS:

	Command	Purpose
Step 1	Configure terminal Router # configure terminal	Enter global configuration mode
Step 2	Interface gigabitethernet slot/port Example: Router # interface gigabitethernet 0/8	Enter the configuration mode of the Gigabit Ethernet interface on the Router. Note: Gigabit Ethernet WAN interfaces are 0/8 and 0/9 for cisco C841M-8X ISR and 0/4 to 0/5 for cisco C841M-4X.
Step 3	ip address ip-address mask Example: Router(config-if) # ip address 192.168.12.2 255.255.255.0	Sets the ip address and subnet mask for the specified GE interface.
Step 4	No shutdown Example: Router(config-if) # no shutdown	Enables the GE interface, changing its state from administratively down to administratively up.
Step 5	Exit Example: Router(config-if) # exit	Exits configuration mode for the GE interface and returns to global configuration mode.

Configuring a Loopback Interface:**SUMMARY STEPS-**

1. Configure terminal
2. Interface *type number*
3. ip address ip-address mask
4. Exit

DETAILED STEPS-

	Command	Purpose
Step 1	Configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 2	Interface type number Example:	Enters configuration mode for the loopback interface.

	Router(config) # interface Loopback 0	
Step 3	IP address ip-address mask Example: Router(config-if) # ip address 10.108.1.1 255.255.255.0	Sets the IP address and subnet mask for the loopback interface.
Step 4	Exit Example: Router(config-if) # exit	Exits the configuration mode for the loopback interface and returns to global configuration mode.

Configuring Gigabit Ethernet LAN Interfaces:

To manually configure Gigabit Ethernet (GE) LAN Interfaces, follow these steps, beginning in global configuration mode.

SUMMARY STEPS-

1. **configure terminal**
2. **ip route** prefix mask {ip-address | interface-type interface-number [ip-address]}
3. **end**

DETAILED STEPS-

	COMMAND	PURPOSE
Step 1	Configure terminal Example: Router# configure terminal	Enter global configuration mode.
Step 2	ip route prefix mask {ip-address interface-type interface-number [ip-address]} Example: Router (config)# ip route 192.168.1.0 255.255.0.0 10.10.10.2	Specifies the static route for the IP packets.
Step 3	End Example: Router(config)# end	Exits router configuration mode, and enters privileged EXEC mode.

Configuring Dynamic Routes:

In dynamic routing, the network protocol adjusts the path automatically, based on network traffic or topology. Changes in dynamic routes are shared with other routes in the network. The Cisco routers can use IP routing protocols, such as Routing Information Protocol(RIP) or Enhanced

Interior Gateway Routing Protocol(EIGRP), to learn routes dynamically. You can configure either of these routing protocols on your router.

- “Configuring Routing Information Protocol”
- “Configuring Enhanced Interior Gateway Routing Protocol”

Configuring Routing Information Protocol

To configure the RIP routing protocol on the router, follow these steps, beginning in global configuration mode.

SUMMARY STEPS-

1. **Configure terminal**
2. **router rip**
3. **Version{1 | 2}**
4. **Network ip-address**
5. **No auto-summary**
6. **End**

DETAILED STEPS-

	Command	Task
Step 1	Configure terminal Example: Router > Configure terminal	Enters global configuration mode.
Step 2	router rip Example: Router(config) # router rip	Enters Router configuration mode and enables RIP on the router.
Step 3	Version { 1 2 } Example: Router (config-router) # version 2	Specifies use of RIP version 1 and 2.
Step 4	Network ip-address Example: Router (config-router) #network 192.168.1.1	Specifies a list of networks on which RIP is to be applied using the address of the network of each directly connected network.
Step 5	no auto-summary Example: Router (config-router) # no auto-summary	Disables automatic summarization of subnet routes into network level routes. This allows sub prefix routing information to pass across classful network boundaries.

Step 6	end Example: Router (config-router) # end	Exits router configuration mode and enters privileged EXEC mode.
---------------	--	--

Configuring Enhanced Interior Gateway Routing Protocol

To configure enhanced interior gateway routing protocol (EGRP) perform these steps -

SUMMARY STEPS -

1. **configure terminal**
2. **router eigrp as-number**
3. **network ip-address**
4. **end**

DETAILED STEPS

	Command	Purpose
Step 1	Configure terminal Example: Router > configure terminal	Enter global configuration mode.
Step 2	Router eigrp as-number Example: Router(config) # Router eigrp 109	Enter router configuration mode, and enable EIGRP on the router. The autonomous system number identifies the route to other EIGRP routers and is used to tag the EIGRP information.
Step 3	Network ip-address Example: Router (config)# Network 192.145.1.0	Specifies a lot of networks on which EIGRP is to be applied, using the IP address of a network of directly connected networks.
Step 4	End Example: Router(config router)#end Router#	Exits router configuration mode, and enters privileged EXEC mode

Configure Serial Interface:

This section contains the following tasks:

- Configuring a Synchronous Serial Interface

- Configuring an Asynchronous Serial Interface

Configuring a Synchronous Serial Interface:

To configure a synchronous serial interface, perform the task in the following sections. Each task in the list is identified as either required or optional.

- Specifying a Synchronous Serial Interface (Required)
- Specifying a Synchronous Serial Encapsulation (Optional)

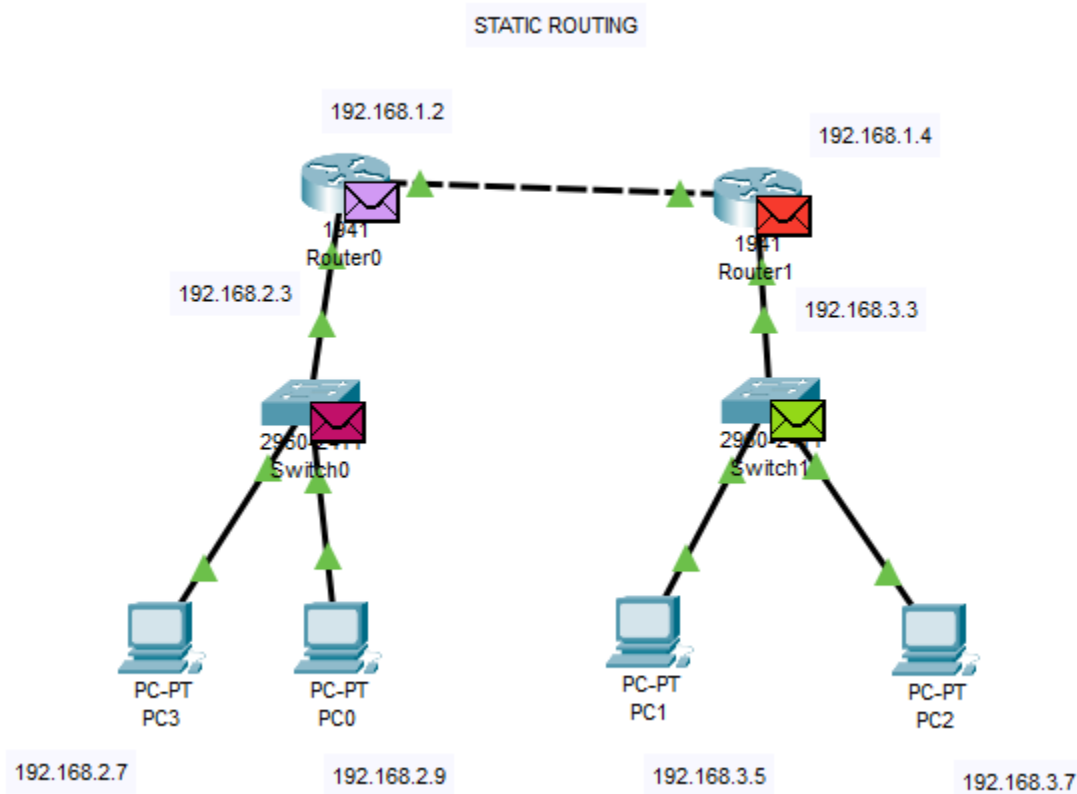
Specifying a Synchronous Serial Interface:

To specify a Synchronous serial interface and interface configuration mode, use the following commands in global configuration mode

Command	Purpose
Router (config)#interface serial wic/slot/port Router# interface serial 0/0/0	Specifies the serial interface and enters interface configuration mode.

Practical 7: Implement a scenario to connect two devices (Hosts) on different networks and define a static route between two routers so that all the devices can ping any other device.

Static Routing: Static routing is a process in which we have to manually add routes to the routing table.



Advantages:-

- i. Simplicity: Static routing is easy to configure and manage, making it suitable for small networks or where network topology changes infrequently. There's no need for routing protocols, reducing complexity.
- ii. Low Overhead: Since static routes are manually configured, they don't generate overhead traffic like dynamic routing protocols. This can be beneficial in terms of network performance and bandwidth conservation.
- iii. Predictability: With static routes, network administrators have precise control over the routing table. They can determine the exact path packets will take, which can be advantageous in certain scenarios where specific routing paths are desired.

- iv. Security: Static routes can enhance network security by providing a level of control over the flow of traffic. Administrators can define exactly which routes are allowed, which can help prevent unauthorized access to certain parts of the network.
- v. Stability: Static routes don't change unless manually modified, so there's less likelihood of unexpected routing changes that could disrupt network operations. This stability can be advantageous in environments where consistency and predictability are crucial.

Disadvantage:-

- i. Manual Configuration: Static routes require manual configuration on each router in the network. This can be cumbersome and error-prone, especially in large or complex networks. Any changes to the network topology or addressing scheme require manual updates to the static routes.
- ii. Limited Scalability: Static routing does not scale well in large or dynamic networks. As the network grows, managing and updating static routes becomes increasingly difficult and impractical. Dynamic routing protocols, on the other hand, can automatically adapt to changes in the network topology.
- iii. Lack of Redundancy: Static routes do not offer built-in redundancy or failover mechanisms. If a link or router fails along a static route, traffic may be unable to reach its destination until the route is manually reconfigured to use an alternate path.
- iv. Suboptimal Routing: Static routes do not consider metrics such as link bandwidth, latency, or load when making routing decisions. As a result, traffic may be routed inefficiently, leading to suboptimal performance or congestion on certain links.
- v. Difficulty in Troubleshooting: Troubleshooting network issues can be more challenging with static routing. Since routes are manually configured and maintained, identifying problems such as misconfigurations or routing loops may require a thorough manual inspection of router configurations.

```
Router(config)#
Router(config)#router rip
Router(config-router)#no network 192.168.1.0
Router(config-router)#no network 192.168.2.0
```

Steps to Configure and Verify Two Router Connections in Cisco Packet Tracer:

Step 1: First, open the Cisco packet tracer desktop and select the devices.

Step 2: Configure the PCs (hosts) with IPv4 address and Subnet Mask according to the IP addressing.

Step 3: Assigning IP address using the ipconfig command.

Step 4: Configure router with IP address and subnet mask.

Step 5: After configuring all of the devices we need to assign the routes to the routers.

Step 6: Verifying the network by pinging the IP address of any PC. Use the ping command to do so.

PC3

Physical Config **Desktop** Programming Attributes

IP Configuration X

Interface: FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IPv4 Address: 192.168.2.7

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.2.3

DNS Server: 0.0.0.0

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address: /

Link Local Address: FE80::2D0:BCFF:FE3D:8C8E

Default Gateway:

DNS Server:

802.1X

☐ Use 802.1X Security

Authentication: MD5

Username:

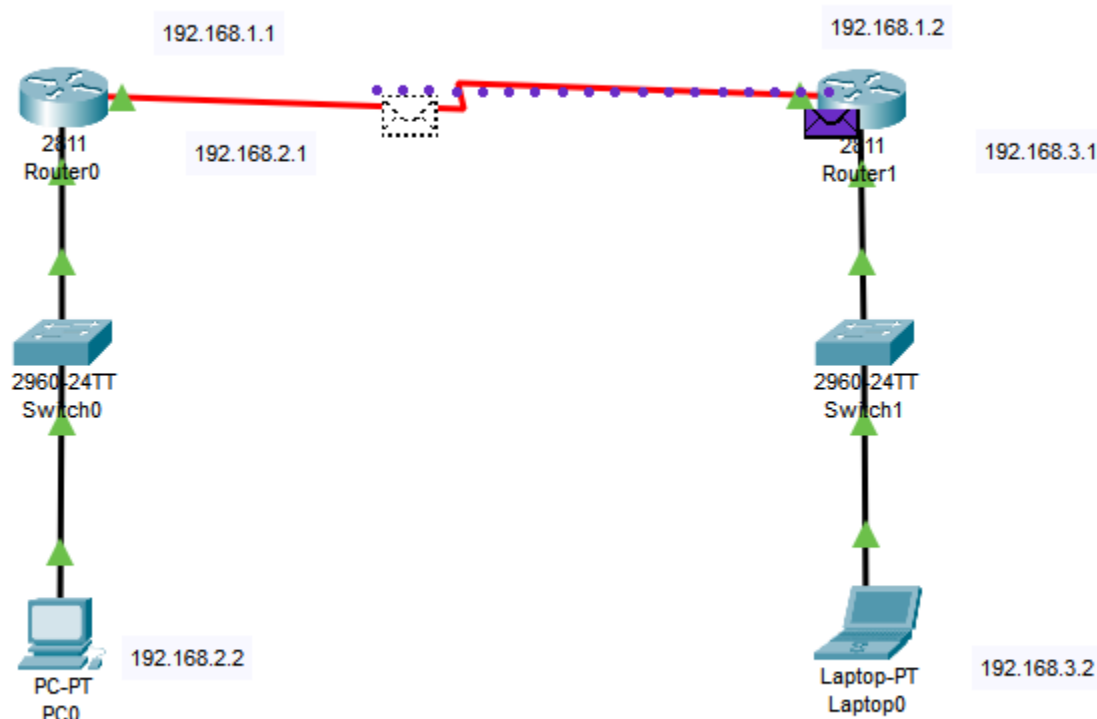
Password:

☐ Top

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	Router0	PC1	ICMP		0.000	N	0	(edit)	(delete)
	Successful	PC3	PC2	ICMP		0.000	N	1	(edit)	(delete)
	Successful	Router0	Router1	ICMP		0.000	N	2	(edit)	(delete)

Practical 8: Take a scenario of two devices connected with different routers and define a default route between two routers so that all the devices can ping any other devices.

Default Routing: This is the method where the router is configured to send all packets toward a single router (next hop). It doesn't matter to which network the packet belongs, it is forwarded out to the router which is configured for default routing. It is generally used with stub routers. A stub router is a router that has only one route to reach all other networks.



Advantages:-

- i. **Simplicity:** It simplifies network configurations by providing a default path for packets that don't match any specific route entries. This reduces the need for extensive routing tables.
- ii. **Scalability:** Default routing can improve the scalability of large networks by minimizing the size of routing tables. This is particularly beneficial in networks with a large number of subnets or routes.
- iii. **Traffic Control:** It allows for centralized traffic control and management. By directing all unspecified traffic towards a default gateway, network administrators can implement traffic shaping, access control, and security policies more effectively.

Disadvantages:-

- i. Suboptimal Routing: Since all packets are forwarded to the default gateway, they may be routed through suboptimal paths, leading to increased latency and potential network congestion.
- ii. Single Point of Failure: Relying on a single default gateway creates a single point of failure. If the default gateway becomes unreachable or malfunctions, communication with external networks may be disrupted.
- iii. Security Risks: Default routing can pose security risks if unauthorized access is gained to the default gateway. Attackers may intercept or manipulate traffic that is being forwarded through the default gateway.

Commands to Configure and Verify Two Router Connections in Cisco Packet Tracer:

```

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface serial 0/0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#clock rate 128000
Router(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
Router(config-if)#interface fastethernet 0/0
Router(config-if)#ip address 192.168.2.1 255.255.255.0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
exit
Router(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.2
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Router#

```

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface serial 0/0/0
Router(config-if)#ip address 192.168.1.2 255.255.255.0
Router(config-if)#clock rate 128000
This command applies only to DCE interfaces
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
interfac
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed stat
Router(config-if)#interface fastethernet 0/0
Router(config-if)#ip address 192.168.3.1 255.255.255.0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

Router(config-if)#exit

Router(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.1
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Router#|
```


Router1
— □ ×

Physical
Config
CLI
Attributes

MODULES

NM-1E

NM-1E2W

NM-1FE-FX

NM-1FE-TX

NM-1FE2W

NM-2E2W

NM-2FE2W

NM-2W

NM-4A/S

NM-4E

NM-8A/S

NM-8AM

NM-Cover

NM-ESW-161

HWIC-1GE-SFP

HWIC-2T

HWIC-4ESW

HWIC-8A

HWIC-AP-AG-B

WIC-1AM


WIC-1ENET

WIC-1T


WIC-2AM

Physical Device View


Zoom In
Original Size
Zoom Out




Customize
Icon in
Physical View









Customize
Icon in
Logical View



The NM-1E features a single Ethernet port that can connect a LAN backbone which can also support either six PRI connections to aggregate ISDN lines, or 24 synchronous/asynchronous ports.



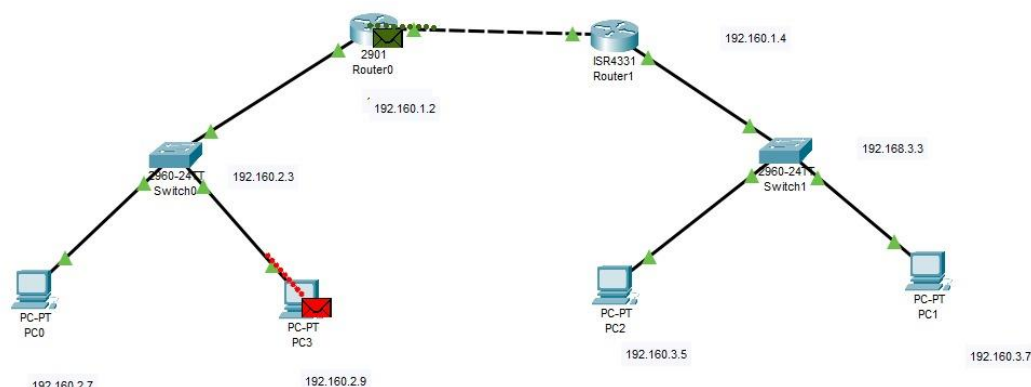
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC0	Laptop0	ICMP		0.000	N	0	(edit)	(delete)
	Successful	Router0	Laptop0	ICMP		0.000	N	1	(edit)	(delete)
	Successful	Router1	PC0	ICMP		0.000	N	2	(edit)	(delete)

Practical 9: To configure a dynamic route (using RIP version 1) between two routers so that all the devices can ping any other devices.

Dynamic routing makes automatic adjustments of the routes according to the current states of the route in the routing table. Dynamic routing uses protocols to discover network destinations and the routes to reach them. RIP and OSPF are the best examples of dynamic routing protocols. Automatic adjustments will be made to reach the network destination if one route goes down.

A dynamic protocol has the following features:

- The routers should have the same dynamic protocol running in order to exchange routes.
- When a router finds a change in the topology then the router advertises it to all the other routers.



Advantages:-

- Improved Route Efficiency: Dynamic routing platforms include updated communication and GPS tracking solutions that allow a dispatcher or user to review the on-road performance of a delivery route in real time.
- Increased Stops Per Hour: By using a dynamic routing platform, delivery companies can improve their services drastically and decrease overall stops per hour.
- Reduced Operational Costs: A dynamic routing platform perform various tasks including printing out reports or displaying them on an easy-to-access dashboard.

Disadvantages:-

- Complexity: Dynamic routing protocols require configuration and maintenance, which can be complex, especially in large networks. Administrators need to understand the intricacies of the protocol and its interactions with other network components.

- ii. **Resource Utilization:** Dynamic routing protocols consume CPU, memory, and bandwidth resources. In networks with limited resources or high traffic volume, this can lead to performance issues.
- iii. **Security Concerns:** Dynamic routing protocols may be vulnerable to various security threats, such as spoofing, hijacking, or denial-of-service attacks. Implementing appropriate security measures, such as authentication and encryption, adds complexity and overhead.

Steps to Configure and Verify Two Router Connections in Cisco Packet Tracer:

Step 1: First, create a network topology of these given devices.

Step 2: Configuring Hosts (PCs) with IP addresses and Default Gateway using IP Addressing.

Step 3: Configuring the Interfaces (routers) with IP Addresses and Default gateways and assigning the default routes.

Step 4: After configuring all the devices red indicator turns into green and the network is live so we can send and receive packets.

The screenshot displays the Cisco Packet Tracer configuration interface. At the top, there are tabs for 'Physical', 'Config', 'CLI', and 'Attributes'. The 'Config' tab is selected. On the left side, there is a vertical menu with categories: 'GLOBAL' (containing 'Settings' and 'Algorithm Settings'), 'ROUTING' (containing 'Static' and 'RIP'), 'SWITCHING' (containing 'VLAN Database'), and 'INTERFACE' (containing 'GigabitEthernet0/0' and 'GigabitEthernet0/1'). The 'RIP' option under 'ROUTING' is currently selected. The main area of the interface is titled 'RIP Routing'. It features a 'Network' label above a text input field. Below this input field is a table with the following structure:

Network Address
192.160.1.0
192.160.2.0

To the right of the table is an 'Add' button. Below the table is a 'Remove' button.

Physical Config **Desktop** Programming Attributes

IP Configuration [X]

Interface: FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IPv4 Address: 192.160.2.7

Subnet Mask: 255.255.255.0

Default Gateway: 192.160.1.2

DNS Server: 0.0.0.0

IPv6 Configuration

☒ Automatic ☐ Static

IPv6 Address: /

Link Local Address: FE80::202:16FF:FE68:BC94

Default Gateway:

DNS Server:

802.1X

☐ Use 802.1X Security

Authentication: MD5

Username:

Password:

Equivalent IOS Commands

```

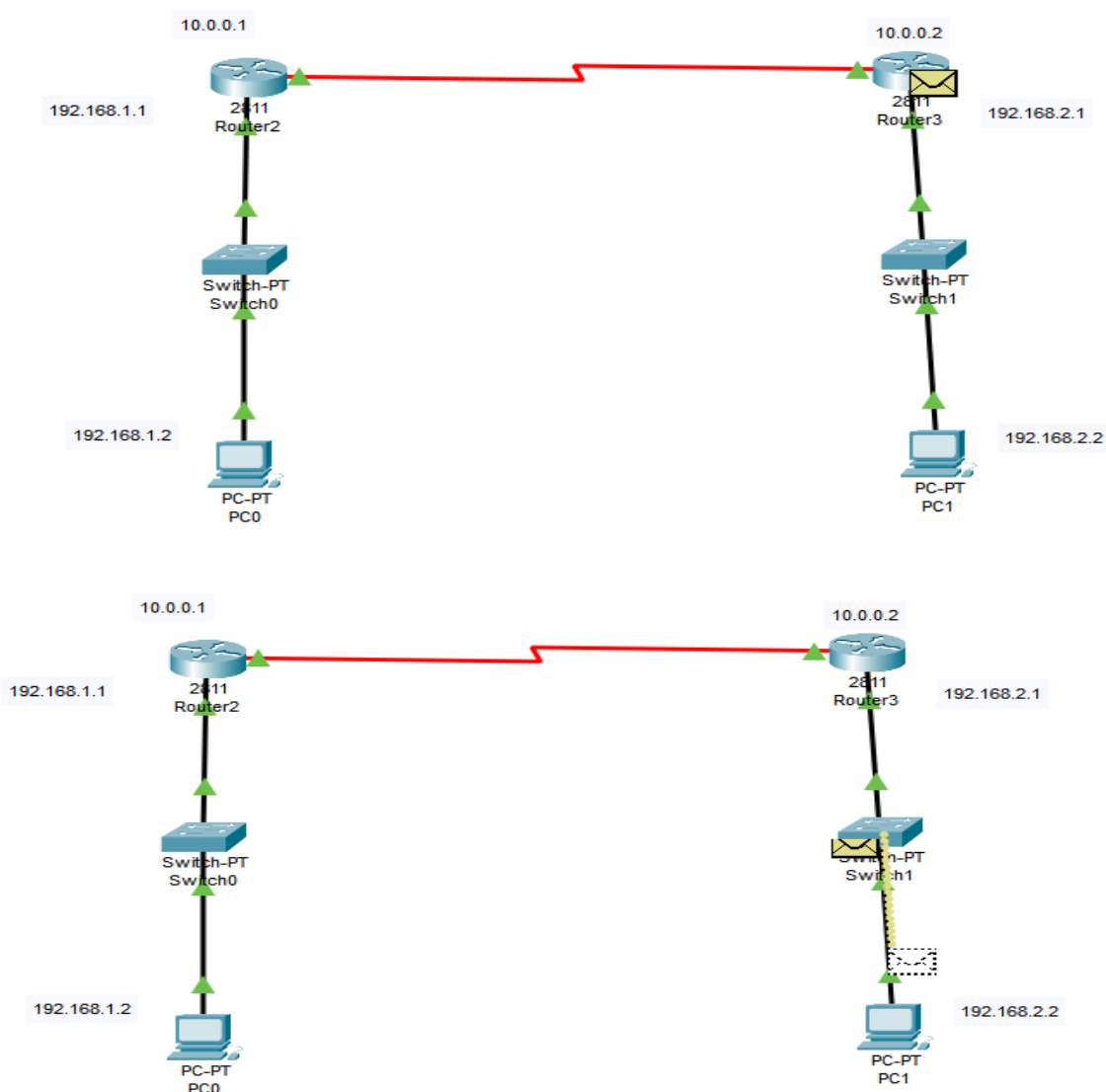
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0
Router(config-if)#
%SYS-5-CONFIG_I: Configured from console by console

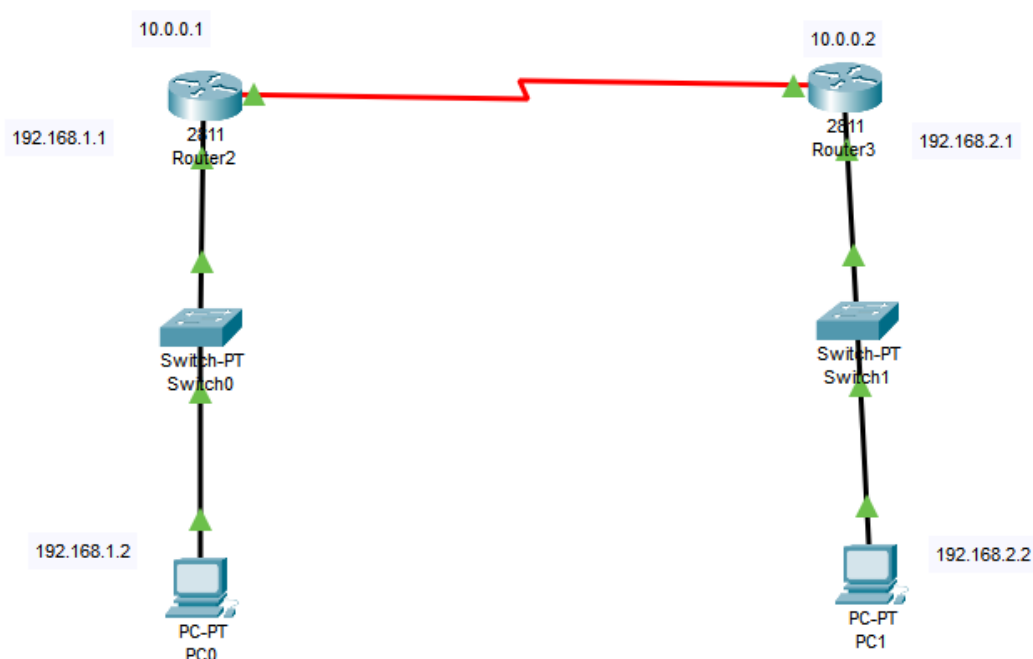
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0
Router(config-if)#
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0
Router(config-if)#

```

Practical 10: To configure a dynamic route (using EIGRP (autonomous system 100) between two routers so that all the devices can ping my other device.

EIGRP, or Enhanced Interior Gateway Routing Protocol, is a sophisticated routing protocol commonly used in large enterprise networks. Developed by Cisco Systems, EIGRP combines the advantages of both distance vector and link-state routing protocols, offering features like rapid convergence, efficient bandwidth utilization, and support for multiple network protocols.





Key features of EIGRP include:

- **Fast Convergence:** EIGRP converges quickly in response to network changes, thanks to its Diffusing Update Algorithm (DUAL), which allows routers to independently calculate routes and make fast routing decisions.
- **Support for VLSM and CIDR:** EIGRP supports Variable Length Subnet Masking (VLSM) and Classless Inter-Domain Routing (CIDR), allowing for efficient use of IP address space and route summarization.
- **Reduced Bandwidth Usage:** EIGRP minimizes bandwidth consumption by sending partial updates only when there are changes in the network topology, rather than periodic updates like traditional distance vector protocols.
- **Load Balancing:** EIGRP supports equal-cost load balancing, allowing routers to distribute traffic across multiple paths with the same metric cost, improving network performance and reliability.
- **Loop-Free Topology:** EIGRP uses the concept of a feasible successor to prevent routing loops. Feasible successors are backup routes that satisfy the loop-free condition and can be quickly used if the primary route fails.

Difference between EIGRP and IGRP:

EIGRP (Enhanced Interior Gateway Routing Protocol) and IGRP (Interior Gateway Routing Protocol) are both routing protocols developed by Cisco for use in computer networks. However, there are significant differences between the two:

I. Age and Evolution:

- IGRP was the earlier protocol, introduced by Cisco in the late 1980s.
- EIGRP was developed later by Cisco as an enhancement to IGRP to overcome some of its limitations and provide more features and efficiency.

II. Metric Calculation:

- IGRP uses a composite metric based solely on bandwidth and delay.
- EIGRP uses a more sophisticated composite metric, taking into account bandwidth, delay, load, reliability, and MTU (Maximum Transmission Unit) of the path.

III. Protocol Features:

- EIGRP offers features like unequal-cost load balancing and route summarization, which IGRP lacks.
- EIGRP supports VLSM (Variable Length Subnet Masking) and CIDR (Classless Inter-Domain Routing), while IGRP only supports classful routing.

IV. Convergence and Scalability:

- EIGRP generally converges faster than IGRP because it uses Diffusing Update Algorithm (DUAL), which allows for quicker convergence and loop-free routing.
- EIGRP is more scalable than IGRP due to its support for larger networks and more efficient use of bandwidth.

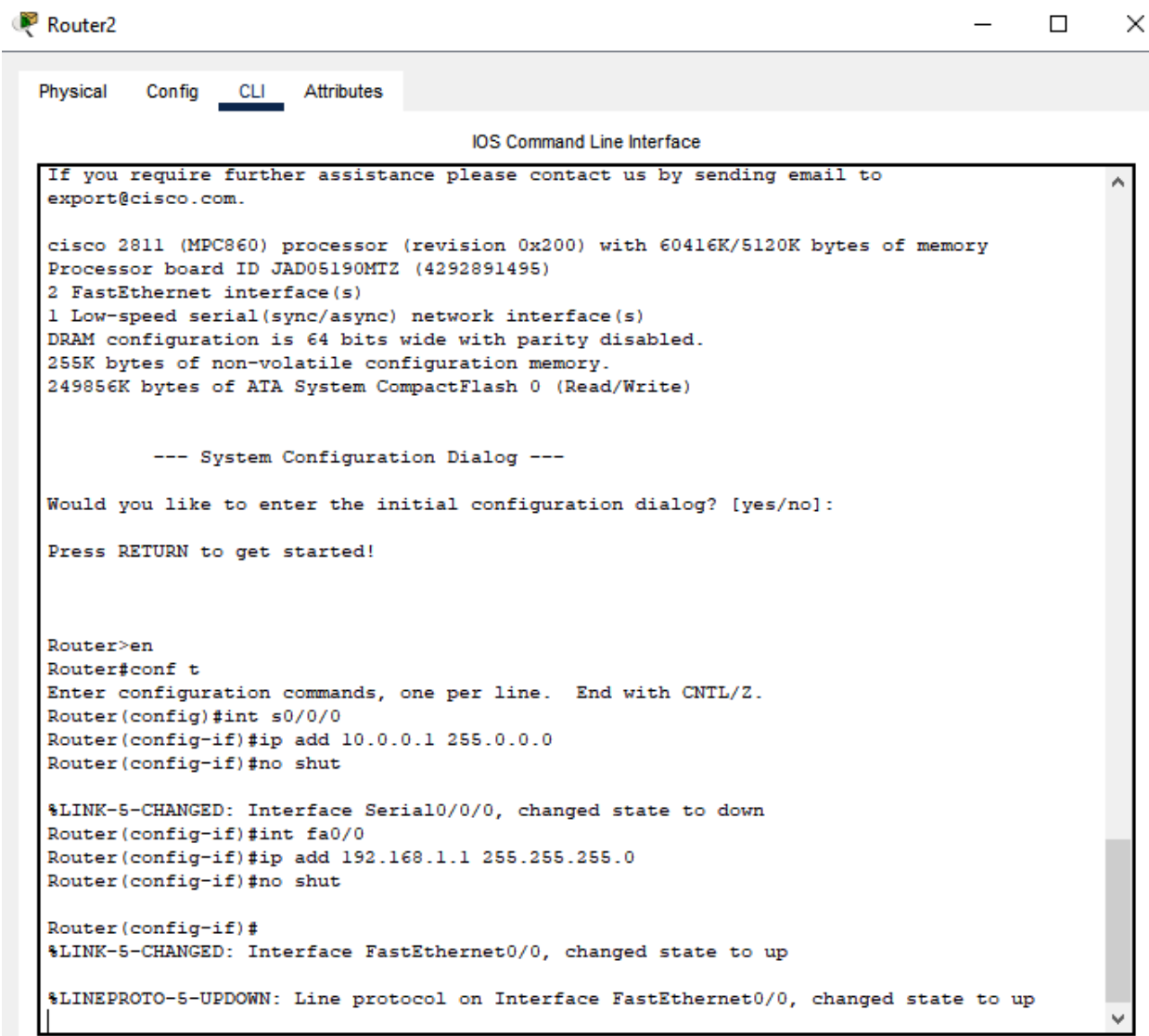
V. Compatibility:

- EIGRP is backward compatible with IGRP, meaning that EIGRP routers can communicate with IGRP routers, but with some limitations.
- IGRP routers cannot understand EIGRP advertisements, so they cannot be directly integrated into an EIGRP network without a migration plan.

Advantages of EIGRP:

- i. Advanced Protocol: EIGRP is an advanced distance-vector routing protocol that helps in automating routing decisions & configurations on a computer network.
- ii. Multi-Network Support: One striking feature of EIGRP is that it supports both IPv6 and IPv4 networks.
- iii. Rate of Convergence: EIGRP is preferred because it converges rapidly for any change encountered in the network topology. Usually, EIGRP will converge in 200 milliseconds. It uses ECMP (Equal-Cost Multi-Path) to make use of links more efficient.
- iv. Reduces Traffic: EIGRP helps in reducing network traffic by only enabling “need-based” updates.

- v. Provides Encryption: It provides encryption for security and can be used with iBGP for WAN routing.



The screenshot shows the Cisco Router2 CLI interface. The top bar has tabs for Physical, Config, CLI (selected), and Attributes. The main window displays the IOS Command Line Interface. It starts with a message about contacting Cisco support. Then, it shows system information: cisco 2811 (MPC860) processor (revision 0x200) with 60416K/5120K bytes of memory, Processor board ID JAD05190MTZ (4292891495), 2 FastEthernet interface(s), 1 Low-speed serial(sync/async) network interface(s), DRAM configuration is 64 bits wide with parity disabled, 255K bytes of non-volatile configuration memory, and 249856K bytes of ATA System CompactFlash 0 (Read/Write). A System Configuration Dialog follows, asking if the user wants to enter the initial configuration dialog (yes/no). The user presses RETURN to get started. The CLI then shows the user entering 'en' to enter enable mode, followed by 'conf t' to enter configuration mode. The user enters configuration commands: 'int s0/0/0', 'ip add 10.0.0.1 255.0.0.0', and 'no shut'. The system responds with '%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down'. The user then enters 'int fa0/0', 'ip add 192.168.1.1 255.255.255.0', and 'no shut'. The system responds with '%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up'. Finally, the user enters 'end' to exit configuration mode, and the system responds with '%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up'.

```

Router2
Physical Config CLI Attributes
IOS Command Line Interface
If you require further assistance please contact us by sending email to
export@cisco.com.

cisco 2811 (MPC860) processor (revision 0x200) with 60416K/5120K bytes of memory
Processor board ID JAD05190MTZ (4292891495)
2 FastEthernet interface(s)
1 Low-speed serial(sync/async) network interface(s)
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

--- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]:

Press RETURN to get started!

Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int s0/0/0
Router(config-if)#ip add 10.0.0.1 255.0.0.0
Router(config-if)#no shut

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down
Router(config-if)#int fa0/0
Router(config-if)#ip add 192.168.1.1 255.255.255.0
Router(config-if)#no shut

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

```

```

Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#router eigrp 100
Router(config-router)#network 10.0.0.0
Router(config-router)#network 192.168.1.0
Router(config-router)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

```

```

Router3
Physical  Config  CLI  Attributes

IOS Command Line Interface

255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

--- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]:

Press RETURN to get started!

Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int s0/0/0
Router(config-if)#ip add 10.0.0.2 255.0.0.0
Router(config-if)#no shut

Router(config-if)#
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
int f
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
a0/0
Router(config-if)#int fa0/0
Router(config-if)#ip add 192.168.2.1 255.255.255.0
Router(config-if)#no shut

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

Router(config-if)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#router eigrp 100
Router(config-router)#network 10.0.0.0
Router(config-router)#
%DUAL-5-NBRCHANGE: IP-EIGRP 100: Neighbor 10.0.0.1 (Serial0/0/0) is up: new adjacency

Router(config-router)#network 192.168.2.0
Router(config-router)#end
Router#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
[OK]

```

```
Router#sh ip route
```

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area

* - candidate default, U - per-user static route, o - ODR

P - periodic downloaded static route

Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks

C 10.0.0.0/8 is directly connected, Serial10/0/0

L 10.0.0.1/32 is directly connected, Serial10/0/0

192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks

C 192.168.1.0/24 is directly connected, FastEthernet0/0

L 192.168.1.1/32 is directly connected, FastEthernet0/0

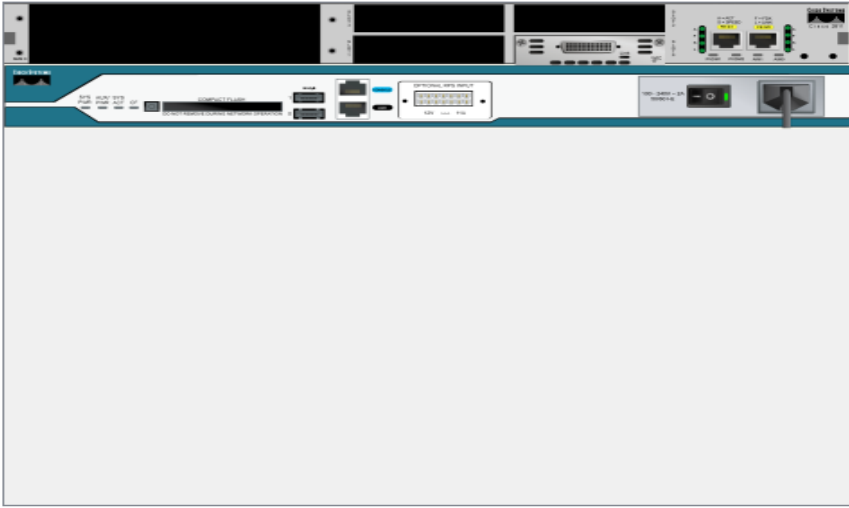
D 192.168.2.0/24 [90/20514560] via 10.0.0.2, 00:02:18, Serial10/0/0

Router3

Physical Config CLI Attributes

Physical Device View





Zoom In Original Size Zoom Out



Customize Icon in Physical View

Customize Icon in Logical View

The NM-1E features a single Ethernet port that can connect a LAN backbone which can also support either six PRI connections to aggregate ISDN lines, or 24 synchronous/asynchronous ports.

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC0	PC1	ICMP		0.000	N	0	(edit)	(delete)
	Successful	Router2	PC1	ICMP		0.000	N	1	(edit)	(delete)