



# Parul University

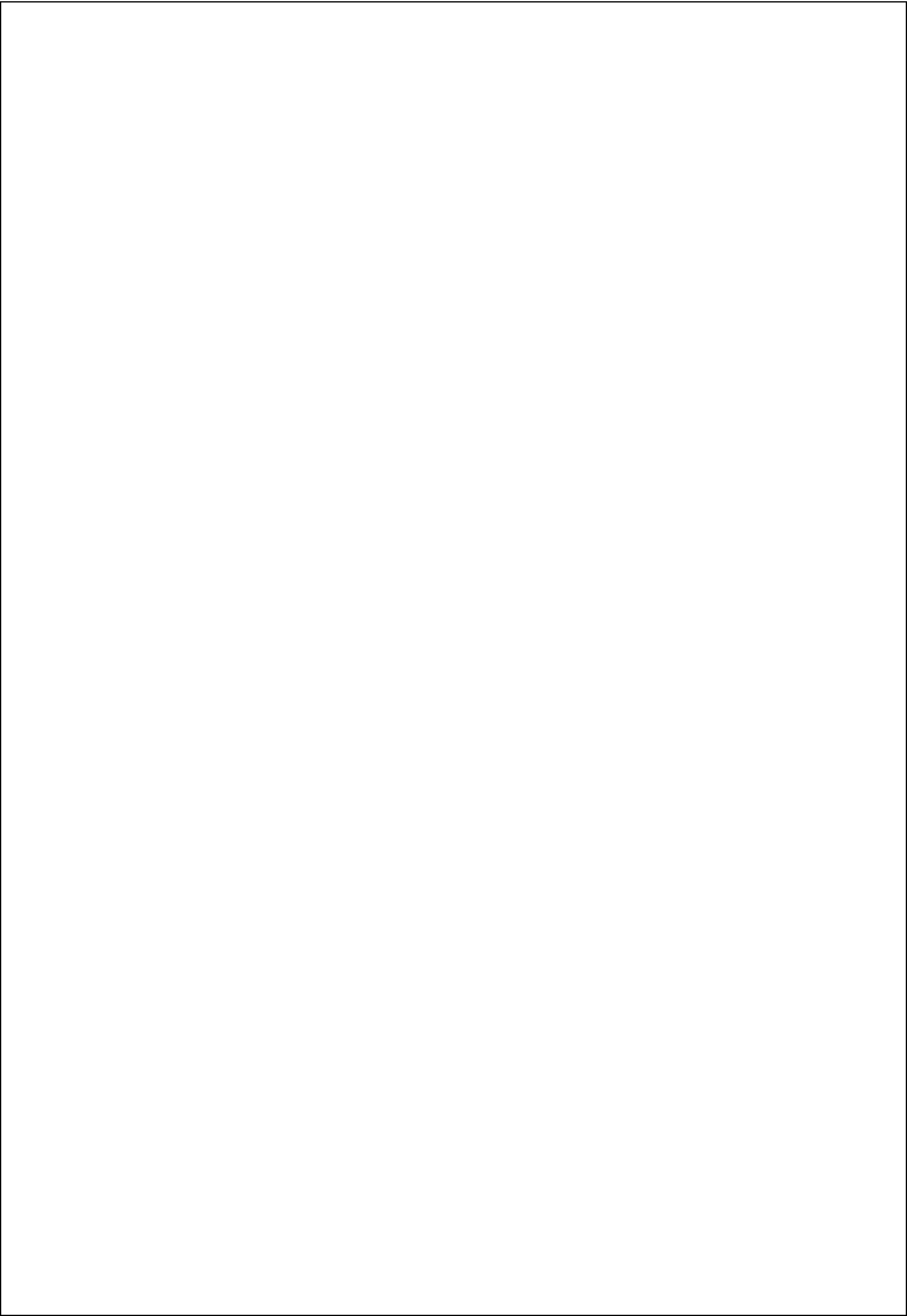
FACULTY OF ENGINEERING AND  
TECHNOLOGY  
BACHELOR OF TECHNOLOGY

Computer Network (303105256)

4<sup>TH</sup> SEMESTER (2<sup>ND</sup> YEAR)

Computer Science  
&  
Engineering

# Laboratory Manual





# Parul University

**FACULTY OF ENGINEERING AND TECHNOLOGY**

**BACHELOR OF TECHNOLOGY**

**CERTIFICATE**

**This is to certify that Mr./Ms \_\_\_\_\_**

**\_\_\_\_\_ with Enrollment no. \_\_\_\_\_**

**\_\_\_\_\_ has Successfully completed his/her**

**Laboratory Experiments in the Computer Network**

**(303105256) from the Department of Computer**

**Science & Engineering during the academic year\_**

**2024- 2025.**

**Date of Submission: .....**

**Staff In charge: .....**

**Head of Department: .....**

# INDEX

Sr. No	Experiment Title	Number of Hours	Page No.	Date of Performance	Date of Assessment	Marks (out of 10)	Sign
1	Experiments on Simulation Tools (CISCO PACKET TRACER).	2	1 - 7				
2	Experiment of Packet Capture Tool: Wireshark.	2	8 - 13				
3	To study behaviour of generic devices used for networking: (cisco packet tracer).	2	14 – 21				
4	To Perform the Data Link Layer (Error Detection).	2	22 - 24				
5	Virtual LAN.	2	25 - 29				
6	Wireless LAN.	2	30 - 33				
7	Internetworking with Routers.	2	34 – 38				
8	Implementation of Subnetting	2	39 - 43				
9	Routing at Networking Layer.	2	44 - 49				
10	Experiment on Transport Layer.	2	50 - 52				



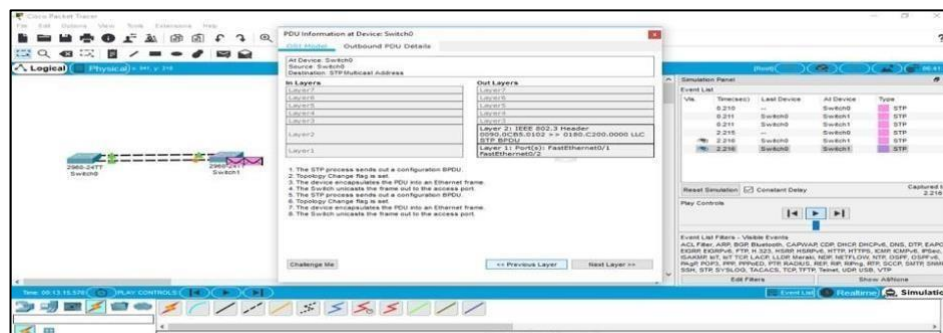
## Practical: 1

### **Aim: Experiments on Simulation Tools (CISCO PACKET TRACER).**

- Packet Tracer is Software or a protocol simulator developed by CISCO.
- Cisco Packet Tracer is a very powerful tool that displays various network and protocol simulation in real-time scenario and simulation mode.
- It gives the ability to design and analyze different types of real-time topologies and configure them as we do in the real world. In CISCO packet Tracer all the layer protocols are enabled or present, for example, Layer II Protocol such as Ethernet and PPP etc., Layer III Protocol such as IP (Internet Protocol), ICMP, (Internet Control Message Protocol), ARP (Address Resolution Protocol) etc., Layer IV Protocol such as TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).
- Packet Tracer support all the real-time routing Protocol such as Static Routing, Default Routing, RIPv1, RIPv2, EIGRP, OSPF, BGP etc. Cisco Packet Tracer provides the real-time network equipment with the packet tracer for working and provide the simulation window for virtual simulation.

### **Workspace of Cisco Packet Tracer:**

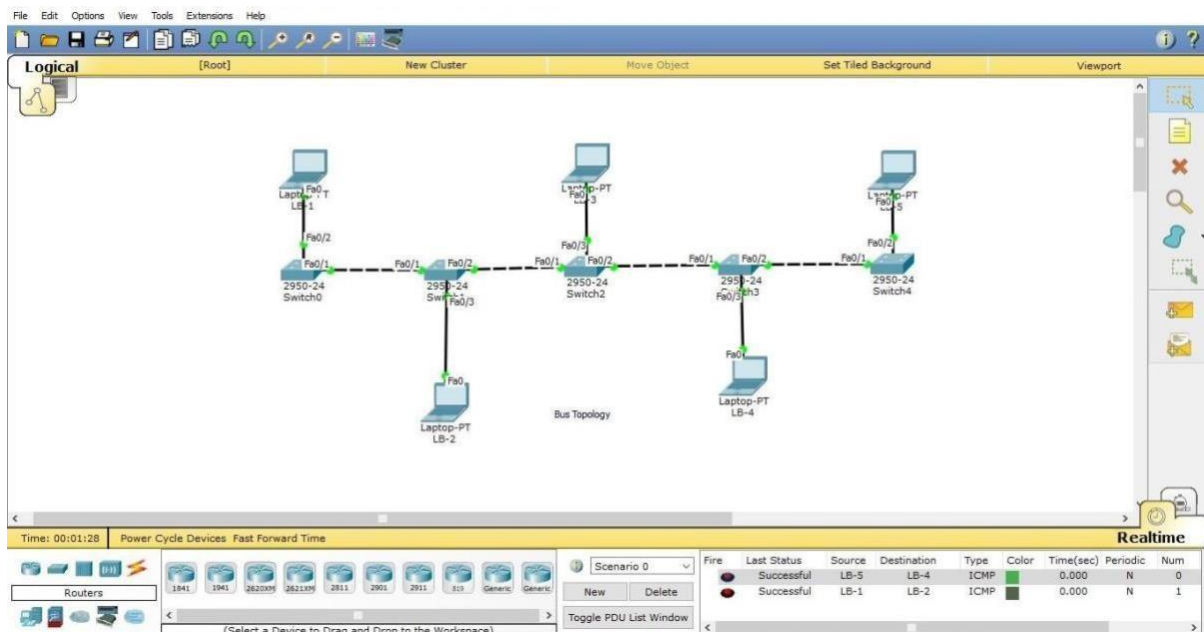
- The workspace is the place where all the components (routers, switches, end devices, firewall, servers and etc.) are placed and wired together to send and receive the packets.
- Workspace of Cisco Packet Tracer is very much flexible from the user point of view as it is a drag-and-drop workspace through which they can drag-and-drop the components and starts configuring it beforehand using the built-in bash command window which actually simulates the bash window of the real router.





**Topologies:** Network Topology is the schematic description of a network arrangement, connecting various nodes (sender and receiver) through lines of connection.

**Bus topology:** The bus topology is also called as line topology. All devices in this topology are connected through a single backbone connection. The application of bus topology can be seen in computer labs. When the backbone is damaged or destroyed, the whole system is destroyed.

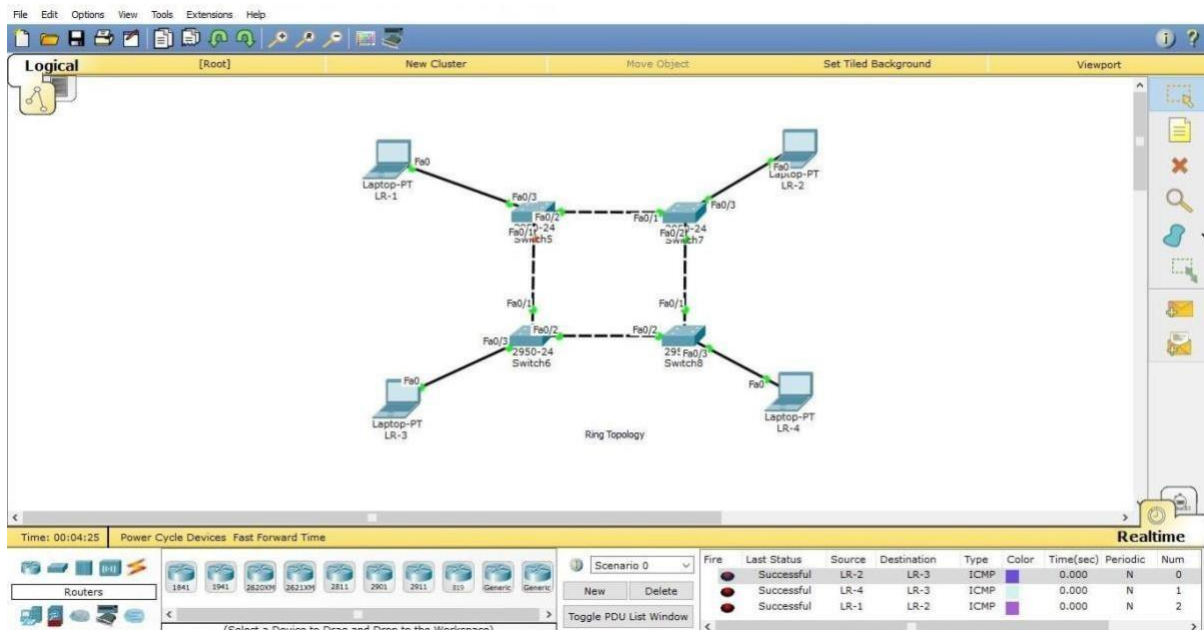


### Steps:

- 1) Open the CISCO PACKET TRACER software.
- 2) Drag N different PC's from end components and place it in the workspace.
- 3) Assign the different and unique IP address to each PC.
- 4) Select N switches and connect it to each PC through copper straight through wire to fast ethernet ports.
- 5) Connect each consecutive switch with each other with copper cross over wire to fast ethernet ports.



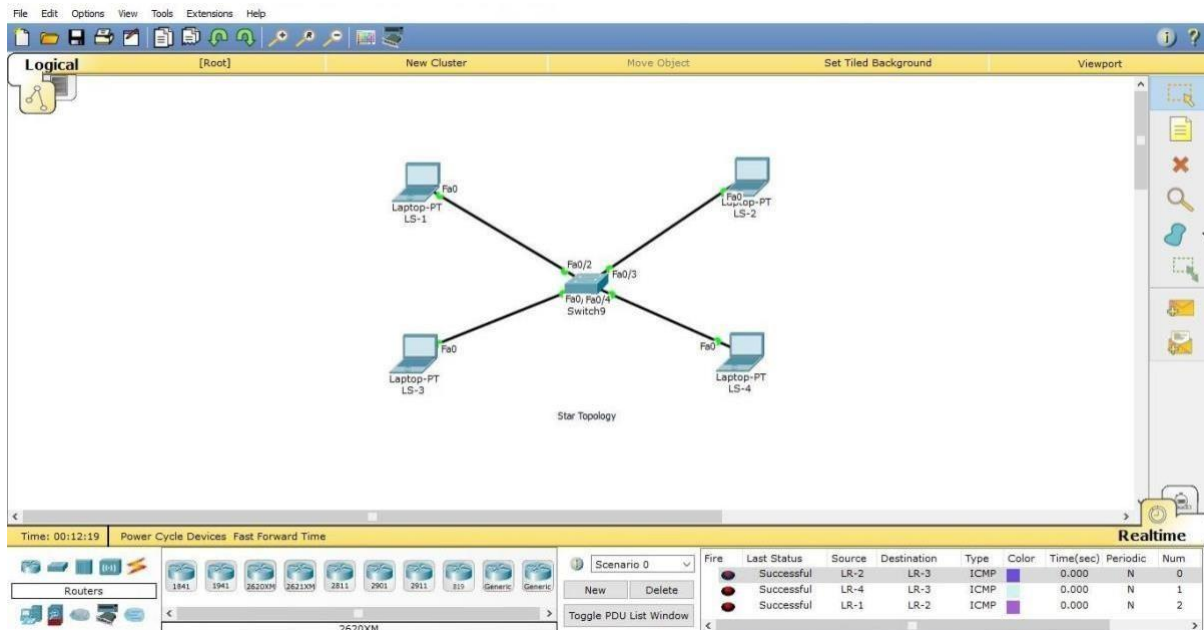
**Ring topology:** The ring topology creates a pattern like circle. All devices in a network are similar to a point on a circle where each point is connected to two other consecutive points. Similarly, in ring topology the devices are connected in circular path.



### Steps:

- 1) Open the CISCO PACKET TRACER software.
- 2) Drag N different PC's from end components and place it in the workspace.
- 3) Assign the different and unique IP address to each PC.
- 4) Drag N switches and connect it with each PC using copper straight through wire to the fast ethernet ports.
- 5) Connect each switch with its adjacent two switches using copper cross over wire through fast ethernet ports.

**Star topology:** Star topology is the best example of the LAN network. Where each and every node is connected to only central switch or hub. There is no direct communication within two devices without using central node as medium.

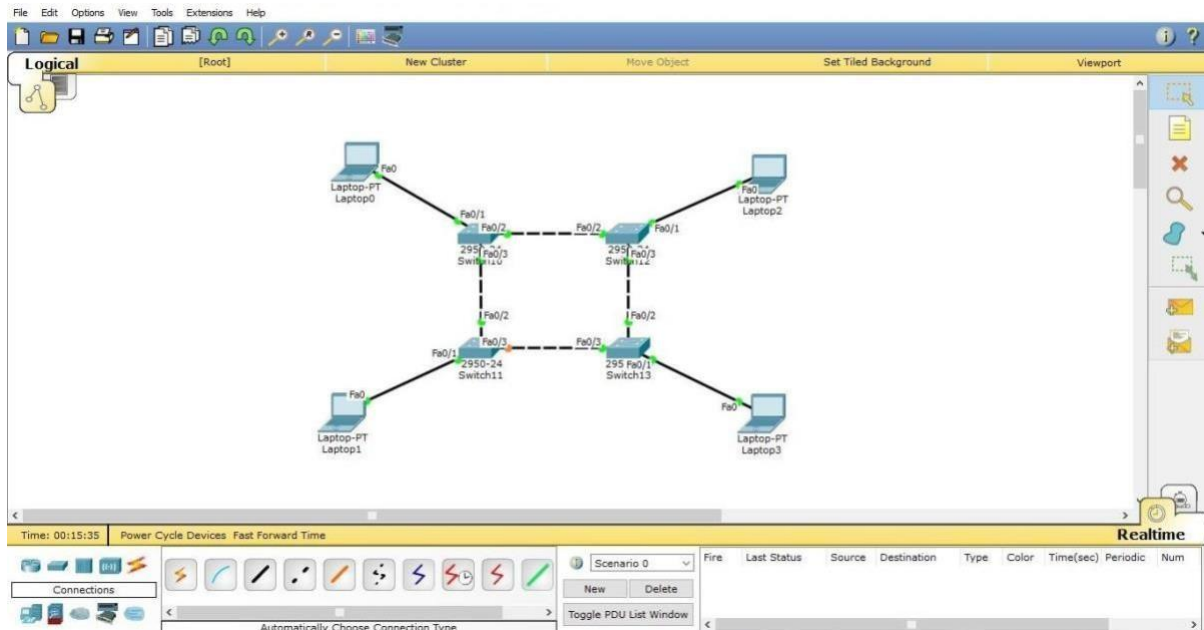


### Steps:

- 1) Open the CISCO PACKET TRACER software.
- 2) Drag N different PC's from end components and place it in the workspace.
- 3) Assign the different and unique IP address to each PC.
- 4) Drag a switch and place it in the middle of all devices and connect all devices to the switch using copper straight through wire by the fast ethernet ports.

**Mesh topology:** A mesh network doesn't follow any linear or hierarchical manner because one node is connected to all other nodes in that network. In mesh network all PC's communicate with each other through the unique communication path.

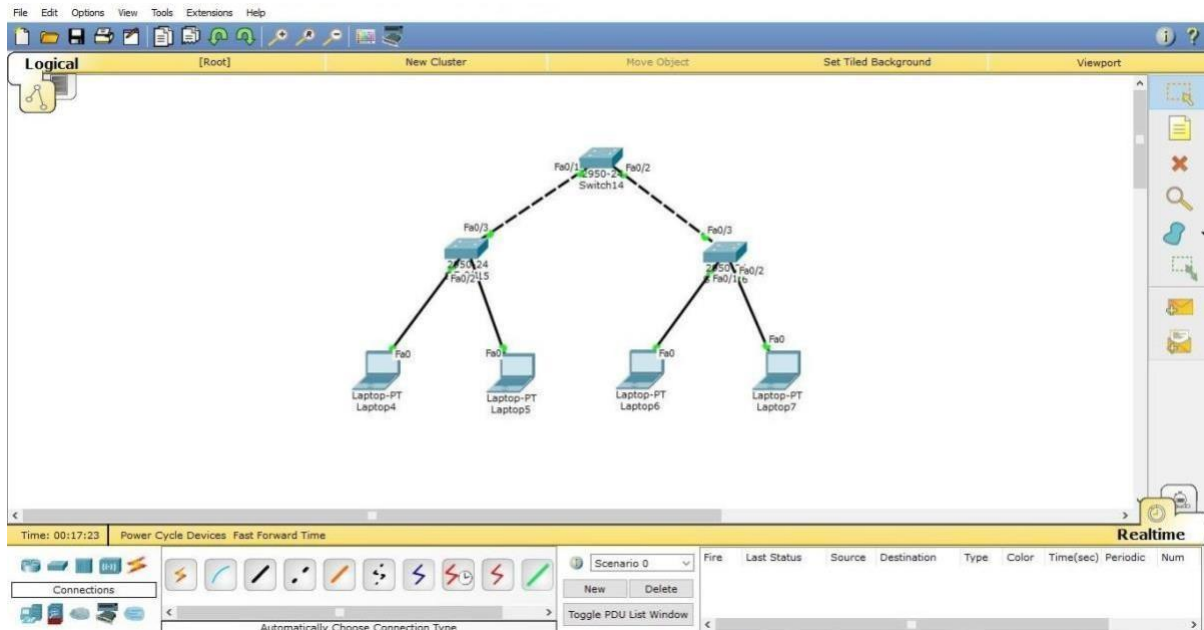




### Steps:

- 1) Open the CISCO PACKET TRACER software.
- 2) Drag N different PC's from end components and place it in the workspace.
- 3) Assign the different and unique IP address to each PC.
- 4) Drag N switches and connect it to each PC using copper straight through wire by fast ethernet ports.
- 5) Connect each switch with every other switch of the network using copper cross over wire by the fast ethernet ports.

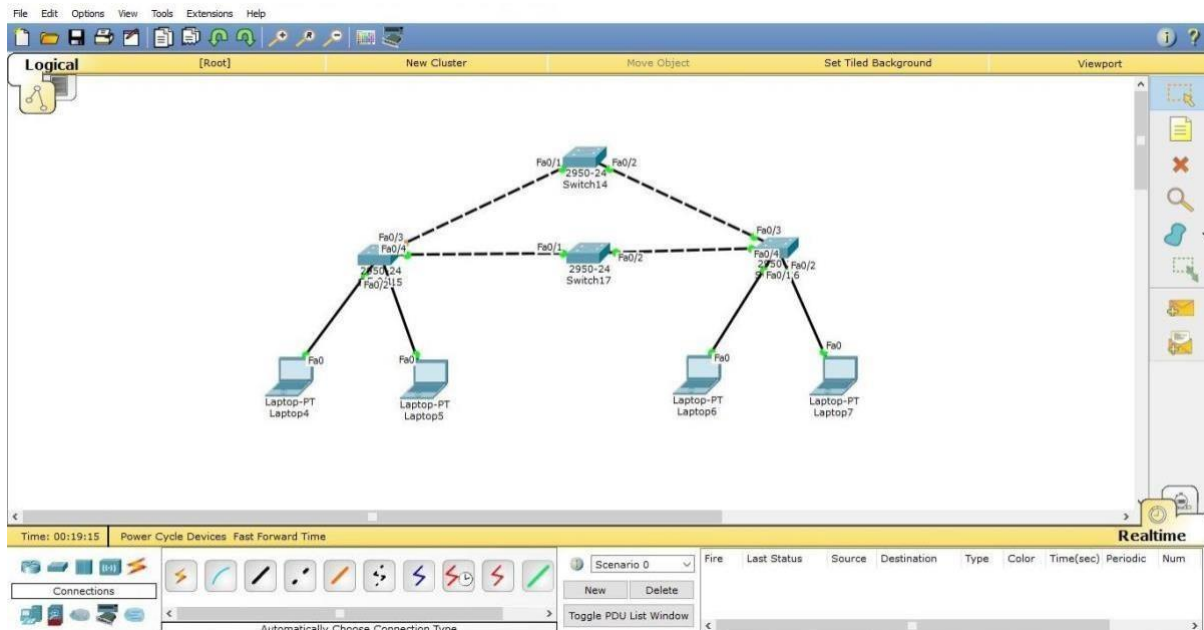
**Tree topology:** Tree topology is a different concept from other topologies like bus, tree, star, etc. It works with the hierarchical manner instead of linear manner. The tree topology network seems to be a tree and its different branches.



### Steps:

- 1) Open the CISCO PACKET TRACER software.
- 2) Drag N different PC's from end components and place it in the workspace.
- 3) Assign the different and unique IP address to each PC.
- 4) Drag N switches connect each switch with pc and connect it to two or more switches in hierarchical manner.

**Hybrid topology:** A hybrid topology refers to the network which uses two or more than two topologies together in a single network



### Steps:

- 1) Open the CISCO PACKET TRACER software.
- 2) Drag N different PC's from end components and place it in the workspace.
- 3) Assign the different and unique IP address to each PC.
- 4) Make two or more topology and then connect them together into a single network by connecting switches of different topology using copper cross over wire.



## **Practical: 2**

### **Aim: Experiment of Packet Capture Tool: Wireshark.**

#### **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 a sniffer, network protocol analyzer, and network analyzer. It is also used by network security engineers to examine security problems.

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

#### **USES OF WIRESHARK:**

**Wireshark can be used in the following ways:**

1. It is used by network security engineers to examine security problems.
2. It allows the users to watch all the 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 laptop, mobile phones, desktop, switch, routers, etc., communicate in a local network or the rest of the world.

#### **HISTORY OF WIRESHARK:**

In the late 1990's Gerald Combs, a computer science graduate of the University of Missouri-Kansas City was working for the small ISP (Internet Service Provider). The protocol at that time did not complete the primary requirements. So, he started writing the Ethernet trademark.



## **FUNCTIONALITY OF WIRESHARK:**

Wireshark is similar to TCP dump in networking. Tcpdump is a common packet analyzer which allows the user to display other packets and TCP/IP packets, being transmitted and received over a network attached to the computer. It has a graphic end and some sorting and filtering functions. Wireshark users can see all the traffic passing through the network.

Wireshark can also monitor the unicast traffic which is not sent to the network's MAC address interface. But the switch does not pass all the traffic to the port. Hence, the promiscuous mode is not sufficient to see all the traffic. The various network taps or port mirroring is used to extend capture at any point. Port mirroring is a method to monitor network traffic. When it is enabled, the switch sends the copies of all the network packets present at one port to another port.

## **WHAT IS COLOR CODING IN WIRESHARK?**

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

The temporary rules are there until the program is in active mode or until we quit the program. 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.

## **FEATURES OF WIRESHARK:**

- It is multi-platform software, i.e., it can run on Linux, Windows, OS X, FreeBSD, NetBSD, etc.
- It is a standard three-pane packet browser.
- It performs deep inspection of the hundreds of protocols.
- It often involves live analysis, i.e., from the different types of the network like the Ethernet, loopback, etc., we can read live data.
- It has sort and filter options which makes ease to the user to view the data. It is also useful in VoIP analysis.
- It can also capture raw USB traffic.



Various settings, like timers and filters, can be used to filter the output.

- It can only capture packet on the PCAP (an application programming interface used to capture the network) supported networks.
- Wireshark supports a variety of well-documented capture file formats such as the PcapNg and Libpcap. These formats are used for storing the captured data.
- It is the no.1 piece of software for its purpose. It has countless applications ranging from the tracing down, unauthorized traffic, firewall settings, etc.

### **INSTALLATION OF WIRESHARK SOFTWARE:**

Below are the steps to install the Wireshark software on the computer: Open the web browser. Search for 'Download Wireshark.'

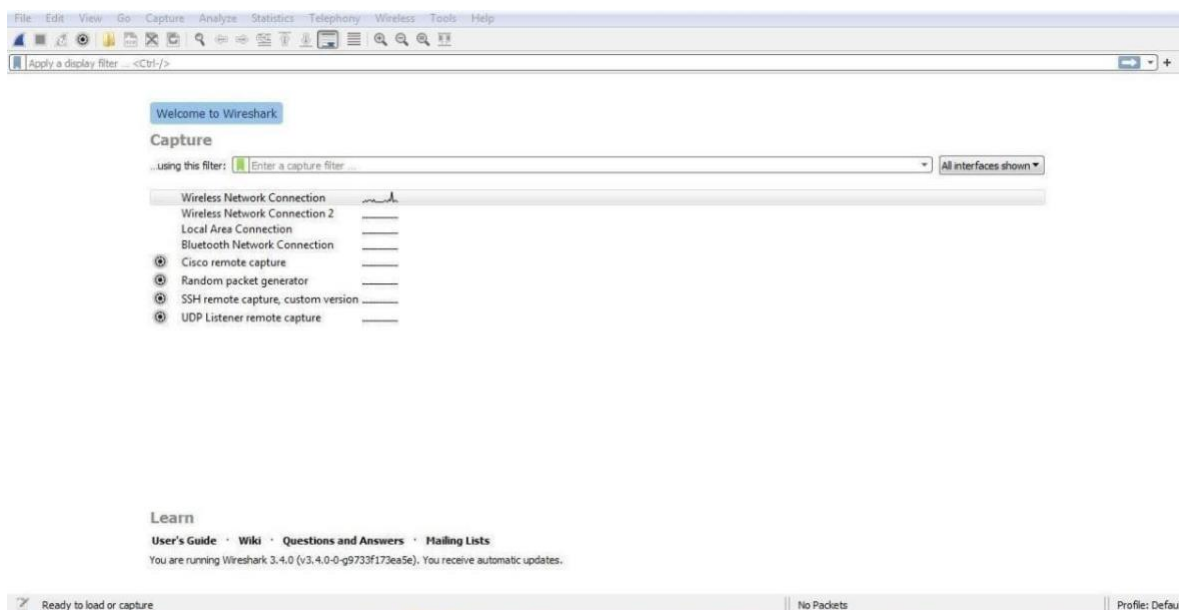
Select the Windows installer according to your system configuration, either 32-bit or 64-bit. Save the program and close the browser.

Now, open the software, and follow the install instruction by accepting the license. The Wireshark is ready for use.

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

If you are Linux users, then you will find Wireshark in its package repositories.

By selecting the current interface, we can get the traffic traversing through that interface. The version used here is 3.0.3. This version will open as:





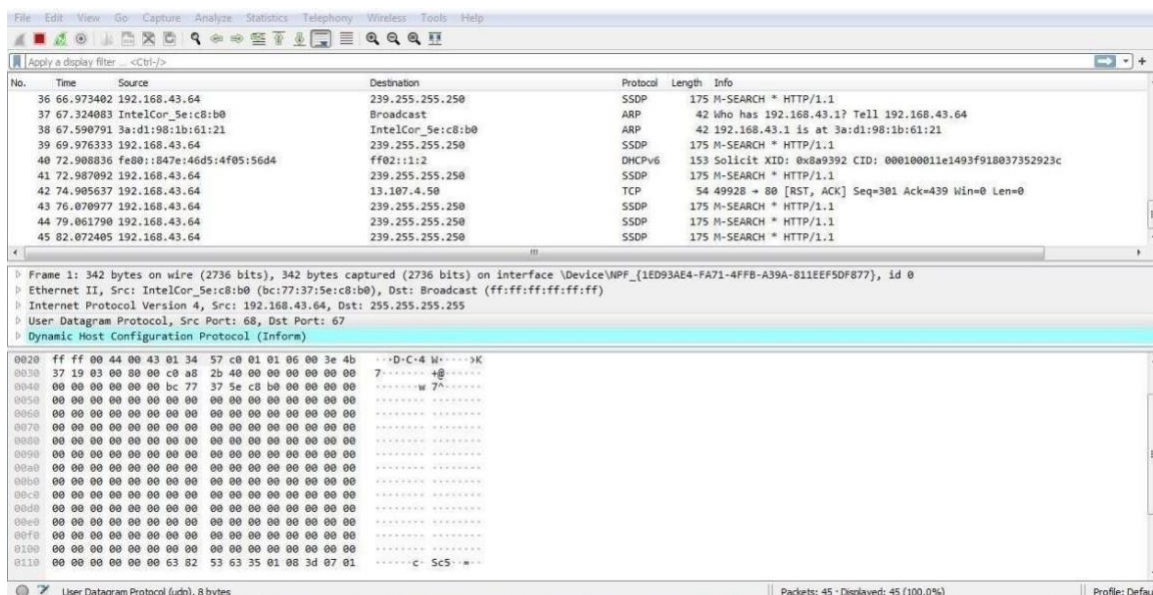
The screen/interface of the Wireshark is divided into five parts:

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 called the packet contents window, which displays the content in ASCII and hexadecimal format.

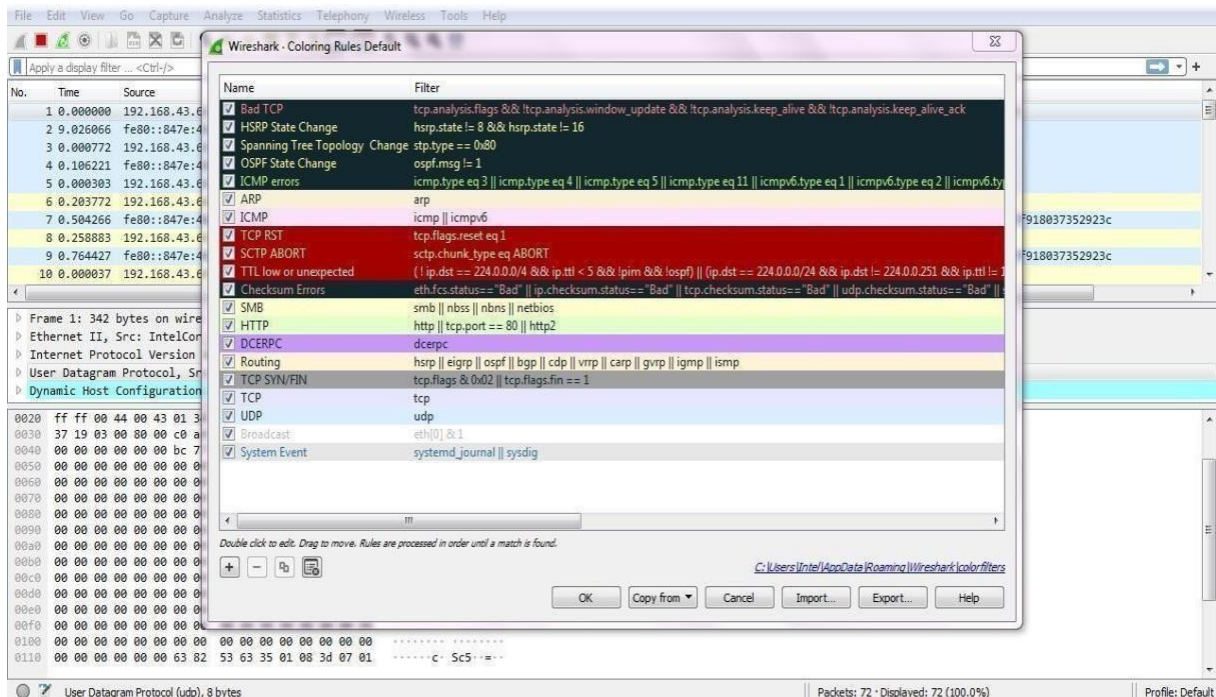
At last, is the filter field which is at the top of the display. The captured packets on the screen can be filtered based on any component according to your requirements. For example, if we want to see only the packets with the HTTP protocol, we can apply filters to that option. All the packets with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







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:

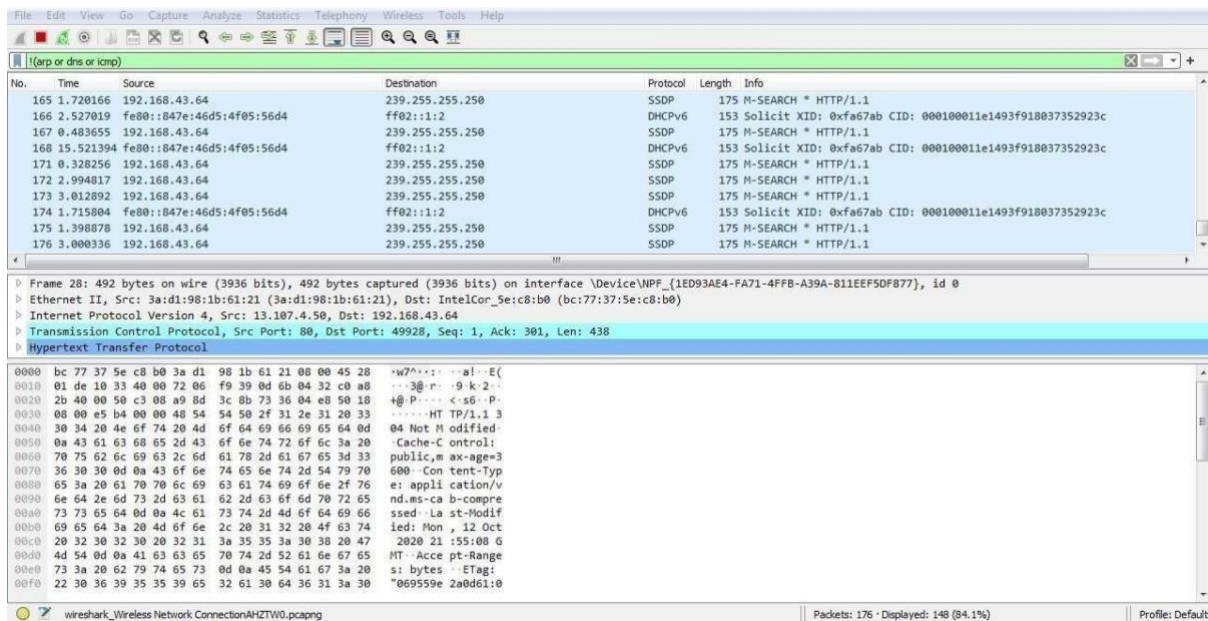


For the network administrator job, advanced knowledge of Wireshark is considered as the requirements. So, it is essential to understand the concepts of the software. It contains these 20 default coloring rules which can be added or removed according to the requirements. Select the option 'View' and then choose 'Colorize Packet List,' which is used to toggle the color on and off.

## **MOST USED FILTER 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.





File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Filter: (arp or dns or icmp)

No.	Time	Source	Destination	Protocol	Length	Info
165	1.720166	192.168.43.64	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
166	2.527019	fe80::847e:46d5:4f05:56d4	ff02::1:2	DHCPv6	153	Solicit XID: 0xfa67ab CID: 000100011e1493f918037352923c
167	0.483655	192.168.43.64	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
168	15.521394	fe80::847e:46d5:4f05:56d4	ff02::1:2	DHCPv6	153	Solicit XID: 0xfa67ab CID: 000100011e1493f918037352923c
171	0.328256	192.168.43.64	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
172	2.994817	192.168.43.64	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
173	3.012892	192.168.43.64	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
174	1.715804	fe80::847e:46d5:4f05:56d4	ff02::1:2	DHCPv6	153	Solicit XID: 0xfa67ab CID: 000100011e1493f918037352923c
175	1.398878	192.168.43.64	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
176	3.000336	192.168.43.64	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1

Frame 28: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface \Device\NPF\_{1ED93AE4-FA71-4FFB-A39A-811EEF5DF877}, id 0

Ethernet II, Src: 3a:d1:98:1b:61:21 (3a:d1:98:1b:61:21), Dst: IntelCor\_Se:c8:b0 (bc:77:37:5e:c8:b0)

Internet Protocol Version 4, Src: 13.107.4.50, Dst: 192.168.43.64

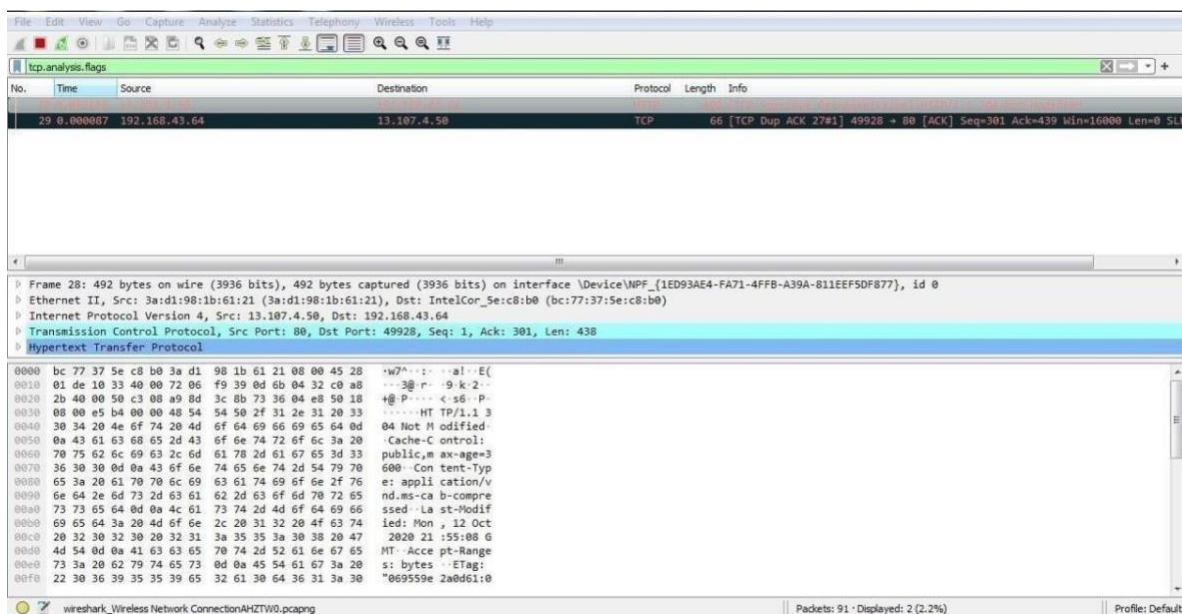
Transmission Control Protocol, Src Port: 80, Dst Port: 49928, Seq: 1, Ack: 301, Len: 438

Hypertext Transfer Protocol

```

0000 bc 77 37 5e c8 b0 3a d1 98 1b 61 21 08 00 45 28  w7^.....al..E(
0010 01 de 10 33 40 00 72 06 f9 39 0d 0b 04 32 c0 a8  --3@r-9k2-
0020 2b 40 00 50 c3 08 a9 8d 3c 0b 73 36 04 e8 50 18  +@P....<s6-P-
0030 08 00 e5 b4 00 00 48 54 54 50 2f 31 2e 31 20 33  ....HT TP/1.1 3
0040 30 34 20 4e 6f 74 20 4d 6f 64 69 66 69 65 64 0d 04 Not Modified
0050 0a 43 61 63 68 65 2d 43 6f 6e 74 72 6f 6c 3a 20  Cache-Control:
0060 70 75 62 6c 69 63 2c 6d 61 78 2d 61 67 65 3d 33 public,max-age=3
0070 36 30 30 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 600 Content-Type
0080 65 3a 20 61 70 70 6c 69 63 61 74 69 6f 6e 2f 76 e: application/v
0090 6e 64 2e 6d 73 2d 63 61 62 2d 63 6f 6d 70 72 65 nd.ms-cab-compre
00a0 73 73 65 64 0d 0a 4c 61 73 74 2d 4d 6f 64 69 66 ssed-La st-Modif
00b0 69 65 64 3a 20 4d 6f 6e 2c 20 31 32 20 4f 63 74 ied: Mon , 12 Oct
00c0 20 32 30 32 30 20 32 31 3a 35 35 3a 30 38 20 47 2020 21 :55:08 G
00d0 4d 54 0d 0a 41 63 63 65 70 74 2d 52 61 6e 67 65 MT-Accept-Range
00e0 73 3a 20 62 79 74 65 73 0d 0a 45 54 61 67 3a 20 s: bytes ETag:
00f0 22 30 36 39 35 39 65 32 61 30 64 36 31 3a 30 "069559e 2a0d61:0
  
```

wireshark\_Wireless Network ConnectionAHZTW0.pcapng | Packets: 176 · Displayed: 148 (84.1%) | Profile: Default



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Filter: tcp.analysis.flags

No.	Time	Source	Destination	Protocol	Length	Info
29	0.000007	192.168.43.64	13.107.4.50	TCP	66	[TCP Dup ACK 27#1] 49928 → 80 [ACK] Seq=301 Ack=439 Win=16000 Len=0 SL

Frame 28: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface \Device\NPF\_{1ED93AE4-FA71-4FFB-A39A-811EEF5DF877}, id 0

Ethernet II, Src: 3a:d1:98:1b:61:21 (3a:d1:98:1b:61:21), Dst: IntelCor\_Se:c8:b0 (bc:77:37:5e:c8:b0)

Internet Protocol Version 4, Src: 13.107.4.50, Dst: 192.168.43.64

Transmission Control Protocol, Src Port: 80, Dst Port: 49928, Seq: 1, Ack: 301, Len: 438

Hypertext Transfer Protocol

```

0000 bc 77 37 5e c8 b0 3a d1 98 1b 61 21 08 00 45 28  w7^.....al..E(
0010 01 de 10 33 40 00 72 06 f9 39 0d 0b 04 32 c0 a8  --3@r-9k2-
0020 2b 40 00 50 c3 08 a9 8d 3c 0b 73 36 04 e8 50 18  +@P....<s6-P-
0030 08 00 e5 b4 00 00 48 54 54 50 2f 31 2e 31 20 33  ....HT TP/1.1 3
0040 30 34 20 4e 6f 74 20 4d 6f 64 69 66 69 65 64 0d 04 Not Modified
0050 0a 43 61 63 68 65 2d 43 6f 6e 74 72 6f 6c 3a 20  Cache-Control:
0060 70 75 62 6c 69 63 2c 6d 61 78 2d 61 67 65 3d 33 public,max-age=3
0070 36 30 30 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70 600 Content-Type
0080 65 3a 20 61 70 70 6c 69 63 61 74 69 6f 6e 2f 76 e: application/v
0090 6e 64 2e 6d 73 2d 63 61 62 2d 63 6f 6d 70 72 65 nd.ms-cab-compre
00a0 73 73 65 64 0d 0a 4c 61 73 74 2d 4d 6f 64 69 66 ssed-La st-Modif
00b0 69 65 64 3a 20 4d 6f 6e 2c 20 31 32 20 4f 63 74 ied: Mon , 12 Oct
00c0 20 32 30 32 30 20 32 31 3a 35 35 3a 30 38 20 47 2020 21 :55:08 G
00d0 4d 54 0d 0a 41 63 63 65 70 74 2d 52 61 6e 67 65 MT-Accept-Range
00e0 73 3a 20 62 79 74 65 73 0d 0a 45 54 61 67 3a 20 s: bytes ETag:
00f0 22 30 36 39 35 39 65 32 61 30 64 36 31 3a 30 "069559e 2a0d61:0
  
```

wireshark\_Wireless Network ConnectionAHZTW0.pcapng | Packets: 91 · Displayed: 2 (2.2%) | Profile: Default



## Practical: 3

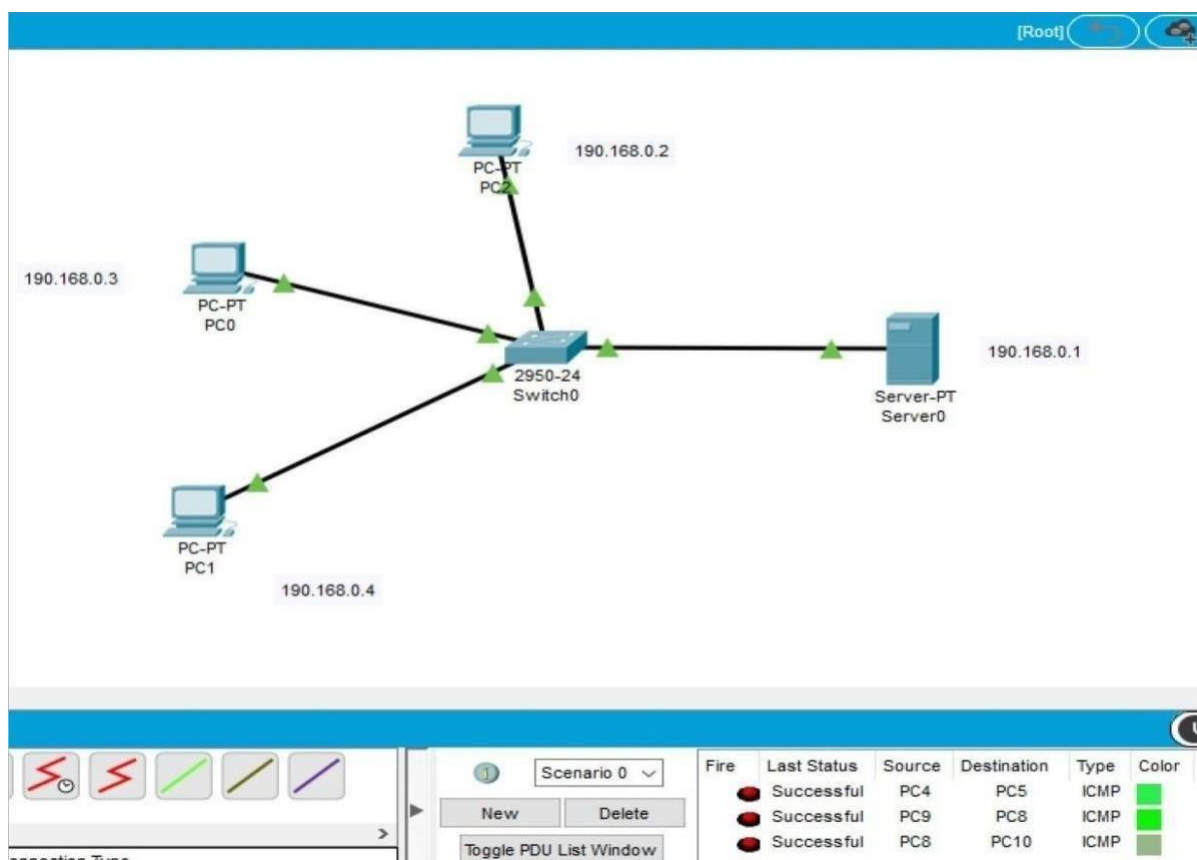
**Aim:** To study behaviour of generic devices used for networking: (cisco packet tracer).

### **THEORY:**

In this Practical we are going to learn the generic devices of Computer Networking.

### **1. WEB SERVER:**

A server is a computer connected to a network of other workstations called 'clients'. Client computers request information from the server over the network. Servers tend to have more storage, memory and processing power than a normal workstation.



### **USES:**

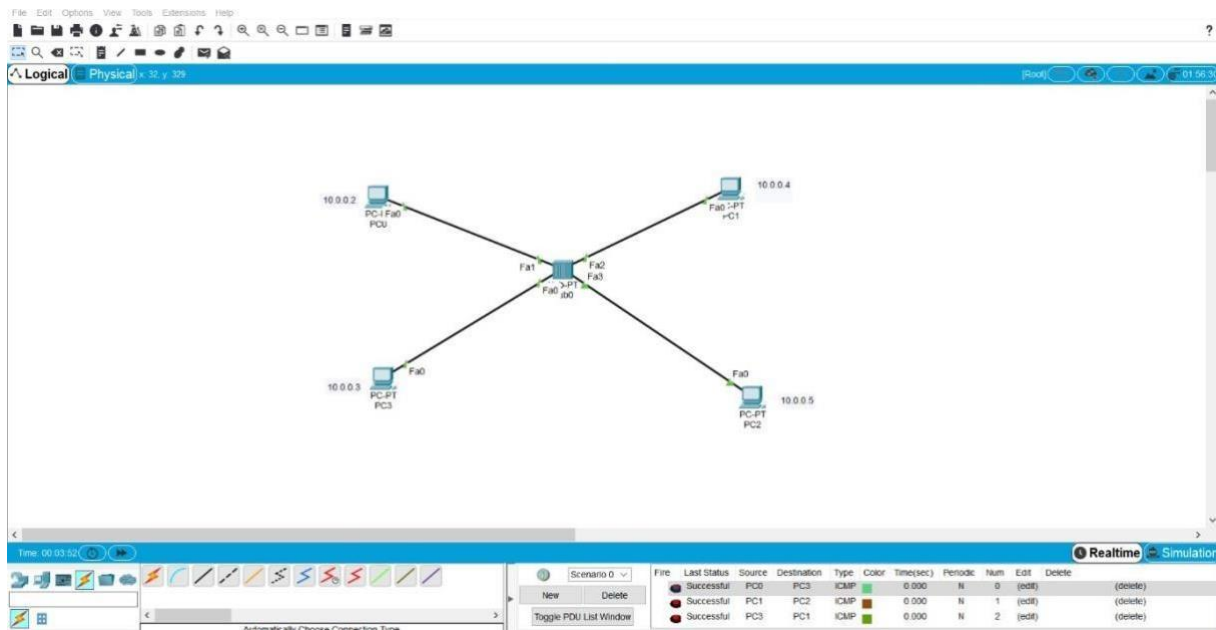
A server is a computer connected to a network of other workstations called 'clients'. Client computers request information from the server over the network. Servers tend to have more



storage, memory and processing power than a normal workstation.

## 2. HUB:

A hub is a physical layer networking device which is used to connect multiple devices in a network. They are generally used to connect computers in a LAN. A hub has many ports in it. A computer which intends to be connected to the network is plugged in to one of these ports.



### USES:

A hub is a physical layer networking device which is used to connect multiple devices in a network. They are generally used to connect computers in a LAN. A computer which intends to be connected to the network is plugged in to one of these ports.

## 3. ROUTERS:

A router receives and sends data on computer networks. Routers are sometimes confused with network hubs, modems, or network switches. However, routers can combine the functions of these components, and connect with these devices, to improve Internet access or help create business networks.

### USES:

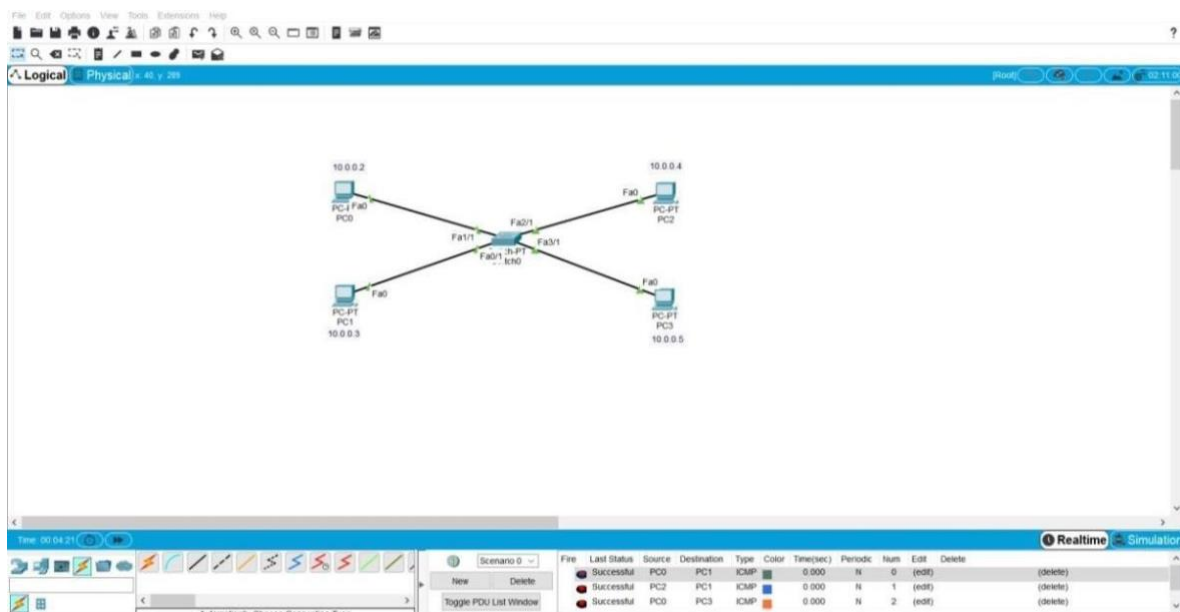
A router receives and sends data on computer networks. Routers are sometimes confused with network hubs, modems, or network switches. However, routers can combine the functions of these components, and connect with these devices, to improve Internet access or help create business networks.

## 4. SWITCHES:

A switch is a device in a computer network that connects other devices together. Multiple data cables are plugged into a switch to enable communication between different networked devices. Switches may also operate at higher layers of the OSI model, including the network layer and above.

**USES:**

Switches are key building blocks for any network. They connect multiple devices, such as computers, wireless access points, printers, and servers; on the same network within a building or campus. A switch enables connected devices to share information and talk to each other.





## **5. BRIDGE:**

A network bridge is a computer networking device that creates a single aggregate network from multiple communication networks or network segments. Routing allows multiple networks to communicate independently and yet remain separate, whereas bridging connects two separate networks as if they were a single network.

### **USES:**

A network bridge is a computer networking device that creates a single aggregate network from multiple communication networks or network segments. Routing allows multiple networks to communicate independently and yet remain separate, whereas bridging connects two separate networks as if they were a single network.

## **6. SERVER:**

A server is a computer or system that provides resources, data, services, or programs to other computers, known as clients, over a network. In theory, whenever computers share resources with client machines, they are considered servers.

## **7. WIRELESS DEVICES:**

Devices such as computers, tablets, and phones are common Clients on a network. Access Points (Master) most wireless networks are made using Access Points – devices that host and control the wireless connection for laptops, tablets, or smart phones.

## **8. LAPTOP:**

A laptop computer, sometimes called a notebook computer by manufacturers, is a battery- or AC powered personal computer generally smaller than a briefcase that can easily be transported and conveniently used in temporary spaces such as on airplanes, in libraries, temporary offices, and at meetings.

## **9. IP PHONE:**



IP telephony refers to any phone system that uses an internet connection to send and receive voice data. Unlike a regular telephone that uses landlines to transmit analog signals, IP phones connect to the internet via a router and modem.

#### **10. Modem:**



Modem is a device or program that enables a computer to transmit data over telephone or cable lines. Computer information is stored digitally, whereas information transmitted over telephone lines is transmitted in the form of analogy waves.

#### **11. Host:**



Host is a computer or other devices connected to a network. A host may work as a server offering information resources, services and application to users or other hosts.

#### **12. Repeater:**



A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network.

#### **13. Automatically chose connection:**



lead to automatic connect and disconnect actions on Wi-Fi, in the Windows user interface but can be configured by using the at least one active Internet connection to a preferred type of network.

#### **14. Console:**



The console is a connection over serial port connection that allows a person access to a computer or network device console. Usually, a console is accessed over an SSH connection.

#### **15. Copper straight-through:**





Straight-through cable is a type of twisted pair copper wire cable for local area network (LAN) use for which the RJ-45 connectors at each end have the same pinout (i.e., arrangement of conductors).

### 16. Copper Crossover:



A crossover cable is a type of twisted pair copper wire cable for LANs (local area network) in which the wires on the cable are crossed over so that the receive signal pins on the RJ-45 connector on one end are connected to the transmit signal pins on the RJ-45 connector on the other end.

### 17. Fiber cable:



Fiber cables transmit pulses of light instead of electrical signals, so the terminations must be much more precise. Instead of merely allowing pins to make metal-to-metal contact, fiber optic connectors must align microscopic glass fiber perfectly in order to allow for communication.

### 18. Phone:



Phone a standard specifies both the physical connector and how it is wired, when modulator connectors are used, the latch release of the connector should be on the ridge side of flat phone wire in order to maintain polarity.

### 19. Coaxial cable:



Coaxial cable is **used as** a transmission line for radio frequency signals, taking a round cross section of the cable, one would find a signal centre solid wire symmetrically surrounded by a foil conductor.

### 20. Serial DCE data:



circuit training, data communications or data carrier equipment this is a modem or more generally adapter. It has to transmit the clock signal which controls the data rate.





## 21. DTE



DTE stands for data terminal equipment which is generally a terminal or a computer. It is a device that acts as an information source or an information sink for the binary digital data.

## 21. Octal:



Octal is a term that describes a base 8 number system. It consists of eight single digit numbers: 0, 1, 2, 3, 4, 5, 6 and 7. It can connect and access server to several different Cisco devices so that it can configure without plugging and unplugging.

## 22. USB:



USB is an industry standard that establishes specifications for cables and connectors and protocols for connection, communication and power supply between computers, peripheral devices and other computers.

### PC to PC Connection:

#### Steps:

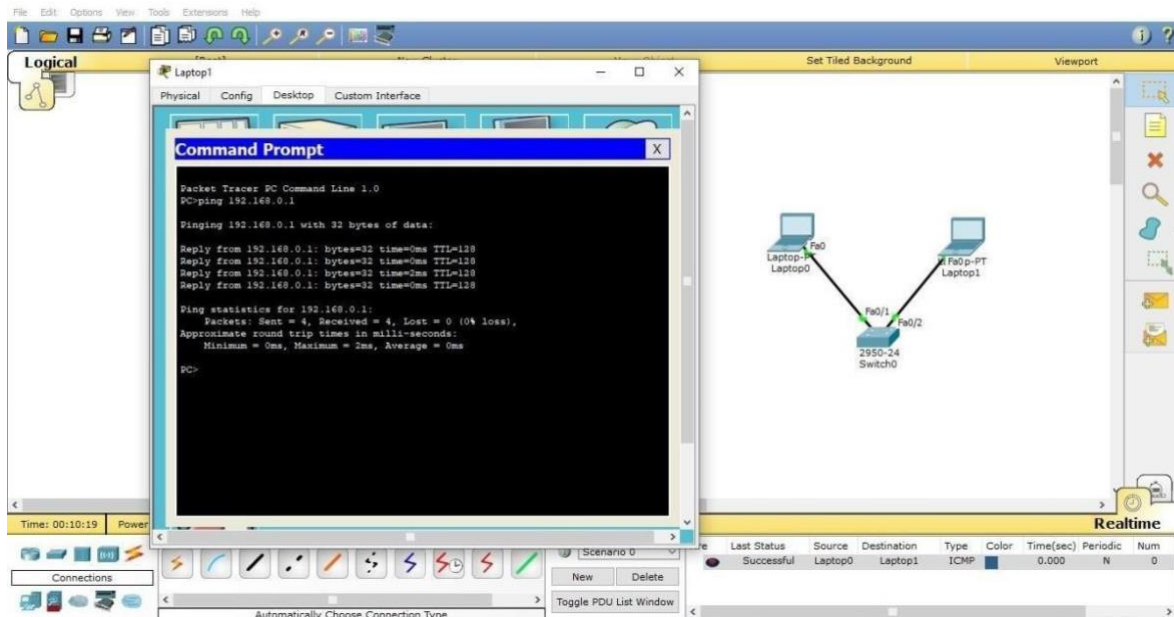
- ✓ Drag 2 PC's from end components.
- ✓ Assign a unique IP address to each PC.
- ✓ Drag a switch and connect 2 PC with a switch using copper straight through cable by fast ethernet ports.





**Parul<sup>TM</sup>**  
University

**Faculty of Engineering & Technology**  
**Subject Name : Computer Networks**  
**Subject Code : 303105256**  
**B.Tech Year 2<sup>nd</sup> Semester 4<sup>th</sup>**





## **Practical: 4**

### **Aim: To Perform the Data Link Layer (Error Detection) Hamming Code:**

Hamming code is a set of error-correction codes that can be used to detect and correct the errors that can occur when the data is moved or stored from the sender to the receiver. It is technique developed by R.W. Hamming for error correction.

#### **Redundant bits :**

Redundant bits are extra binary bits that are generated and added to the information-carrying bits of data transfer to ensure that no bits were lost during the data transfer. The number of redundant bits can be calculated using the following formula:

$$2^r \geq m + r + 1$$

where, r = redundant bit, m = data bit

Suppose the number of data bits is 7, then the number of redundant bits can be calculated using:

$$= 2^4 \geq 7 + 4 + 1$$

Thus, the number of redundant bits= 4

#### **Parity bits:**

A parity bit is a bit appended to a data of binary bits to ensure that the total number of 1's in the data is even or odd. Parity bits are used for error detection. There are two types of parity bits:

##### **1. Even parity bit:**

In the case of even parity, for a given set of bits, the number of 1's are counted. If that count is odd, the parity bit value is set to 1, making the total count of occurrences of 1's an even number. If the total number of 1's in a given set of bits is already even, the parity bit's value is 0.



## **2. Odd Parity bit :**

In the case of odd parity, for a given set of bits, the number of 1's are counted. If that count is even, the parity bit value is set to 1, making the total count of occurrences of 1's an odd number. If the total number of 1's in a given set of bits is already odd, the parity bit's value is 0.

### **General Algorithm of Hamming code :**

The Hamming Code is simply the use of extra parity bits to allow the identification of an error.

1. Write the bit positions starting from 1 in binary form (1, 10, 11, 100, etc).
2. All the bit positions that are a power of 2 are marked as parity bits (1, 2, 4, 8, etc).
3. All the other bit positions are marked as data bits.
4. Each data bit is included in a unique set of parity bits, as determined its bit position in binary form.
  - a. Parity bit 1 covers all the bits positions whose binary representation includes a 1 in the least significant position (1, 3, 5, 7, 9, 11, etc).
  - b. Parity bit 2 covers all the bits positions whose binary representation includes a 1 in the second position from the least significant bit (2, 3, 6, 7, 10, 11, etc).
  - c. Parity bit 4 covers all the bits positions whose binary representation includes a 1 in the third position from the least significant bit (4–7, 12–15, 20–23, etc).
  - d. Parity bit 8 covers all the bits positions whose binary representation includes a 1 in the fourth position from the least significant bit bits (8–15, 24–31, 40–47, etc).
  - e. In general, each parity bit covers all bits where the bitwise AND of the parity position and the bit position is non-zero.
5. Since we check for even parity set a parity bit to 1 if the total number of ones in the positions it checks is odd.
6. Set a parity bit to 0 if the total number of ones in the positions it checks is even.



## Program:-

```
Project Classes Debug [1] crc.cpp
1 #include <stdio.h>
2 #include <conio.h>
3 #include <string.h>
4 int main()
5 {
6     int i,j,keylen,msglen;
7     char input[100], key[30],temp[30],quot[100],rem[30],key1[30];
8
9     printf("Enter Data: ");
10    gets(input);
11    printf("Enter Key: ");
12    gets(key);
13    keylen=strlen(key);
14    msglen=strlen(input);
15    strcpy(key1,key);
16    for(i=0;i<keylen-1;i++)
17    {
18        input[msglen+i]='0';
19    }
20    for(i=0;i<keylen;i++)
21    {
22        temp[i]=input[i];
23        for(j=0;j<msglen;j++)
24        {
25            quot[i]=temp[j];
26            if(quot[i]!='0')
27            {
28                for(j=0;j<keylen;j++)
29                {
30                    key[j]='0';
31                }
32                for(j=0;j<keylen;j++)
33                {
34                    key[j]=key1[j];
35                }
36                for(j=keylen-1;j>0;j--)
37                {
38                    if(temp[j]==key[j])
39                    {
40                        rem[j-1]='0';
41                    }
42                    else
43                    {
44                        rem[j-1]='1';
45                    }
46                }
47                rem[keylen-1]=input[i+keylen];
48                strcpy(temp,rem);
49            }
50            printf("\nQuotient is ");
51            for(i=0;i<msglen;i++)
52            {
53                printf("%c",quot[i]);
54            }
55            printf("\nRemainder is ");
56            for(i=0;i<keylen-1;i++)
57            {
58                printf("%c",rem[i]);
59            }
60            printf("\nFinal data is: ");
61            for(i=0;i<msglen;i++)
62            {
63                printf("%c",input[i]);
64            }
65            getch();
66        }
67    }
68    int i;
69    a=[10]={1,2,3,4,5};
70 }
```

## Output: -

```
C:\Users\parul\Documents\crc.exe
Enter Data: 1011101
Enter Key: 111

Quotient is 1111100
Remainder is 00
Final data is: 101110100
```



## **Practical: 5**

### **Aim: Virtual LAN.**

#### **DESCRIPTION:**

- A virtual LAN (VLAN) is any broadcast domain that is partitioned and isolated in a computer network at the data link layer (OSI layer 2).
- LAN is the abbreviation for local area network and in this context virtual refers to a physical object recreated and altered by additional logic.
- VLANs work by applying tags to network frames and handling these tags in networking systems – creating the appearance and functionality of network traffic that is physically on a single network but acts as if it is split between separate networks.
- In this way, VLANs can keep network applications separate despite being connected to the same physical network, and without requiring multiple sets of cabling and networking devices to be deployed.
- VLANs allow network administrators to group hosts together even if the hosts are not directly connected to the same network switch. Because VLAN membership can be configured through software, this can greatly simplify network design and deployment. Without VLANs, grouping hosts according to their resource needs the labor of relocating nodes or rewiring data links
- VLANs allow networks and devices that must be kept separate to share the same physical cabling without interacting, improving simplicity, security, traffic management, or economy.
- For example, a VLAN could be used to separate traffic within a business due to users, and due to network administrators, or between types of traffic, so that users or low priority traffic cannot directly affect the rest of the network's functioning. Many Internet hosting services use VLANs to separate their customers' private zones from each other, allowing each customer's servers to be grouped together in a single network segment while being located anywhere in their data center. Some precautions are needed to prevent traffic "escaping" from a given VLAN, an exploit known as VLAN hopping.
- VLANs address issues such as scalability, security, and network management. Network architects set up VLANs to provide network segmentation. Routers between VLANs



filter broadcast traffic, enhance network security, perform address summarization, and mitigate network congestion.

- In a network utilizing broadcasts for service discovery, address assignment and resolution and other services, as the number of peers on a network grows, the frequency of broadcasts also increases. VLANs can help manage broadcast traffic by forming multiple broadcast domains. Breaking up a large network into smaller independent segments reduces the amount of broadcast traffic each network device and network segment has to bear. Switches may not bridge network traffic between VLANs, as doing so would violate the integrity of the VLAN broadcast domain.
- VLANs can also help create multiple layer 3 networks on a single physical infrastructure. VLANs are data link layer (OSI layer 2) constructs, analogous to Internet Protocol (IP) subnets, which are network layer (OSI layer 3) constructs. In an environment employing VLANs, a one-to-one relationship often exists between VLANs and IP subnets, although it is possible to have multiple subnets on one VLAN.
- Without VLAN capability, users are assigned to networks based on geography and are limited by physical topologies and distances. VLANs can logically group networks to decouple the users' network location from their physical location. By using VLANs, one can control traffic patterns and react quickly to employee or equipment relocations. VLANs provide the flexibility to adapt to changes in network requirements and allow for simplified administration.<sup>[2]</sup>
- VLANs can be used to partition a local network into several distinctive segments, for instance.

## **Cisco VLAN Trunking Protocol**

- VLAN Trunking Protocol (VTP) is a Cisco proprietary protocol that propagates the definition of VLANs on the whole local area network. VTP is available on most of the Cisco Catalyst Family products. The comparable IEEE standard in use by other manufacturers is GARP VLAN Registration Protocol (GVRP) or the more recent Multiple VLAN Registration Protocol (MVRP).



- The two common approaches to assigning VLAN membership are as follows:
- Static VLANs
- Dynamic VLANs
- Static VLANs are also referred to as port-based VLANs. Static VLAN assignments are created by assigning ports to a VLAN. As a device enters the network, the device automatically assumes the VLAN of the port. If the user changes ports and needs access to the same VLAN, the network administrator must manually make a port-to-VLAN assignment for the new connection.
- Dynamic VLANs are created using software or by protocol. With a VLAN Management Policy Server (VMPS), an administrator can assign switch ports to VLANs dynamically based on information such as the source MAC address of the device connected to the port or the username used to log onto that device. As a device enters the network, the switch queries a database for the VLAN membership of the port that device is connected to. Protocol methods include Multiple VLAN Registration Protocol (MVRP) and the somewhat obsolete GARP VLAN Registration Protocol (GVRP).
- In a switch that supports protocol-based VLANs, traffic is handled on the basis of its protocol. Essentially, this segregates or forwards traffic from a port depending on the particular protocol of that traffic; traffic of any other protocol is not forwarded on the port.
- For example, it is possible to connect the following to a given switch:
- A host generating Address Resolution Protocol (ARP) traffic to port 10
- A network with Internetwork Packet Exchange (IPX) traffic to port 20

### **1. Make a Network:**

We took router, switch, PC's.

We have 1 router, 1 switch, 3 PC's: PC0, PC1, PC2.

Router address: gig 0/0.10 VLAN 10

Ip Address :192.168.10.1/24

gig 0/0.20 VLAN 20

Ip Address:192.168.20.1/24

gig 0/0.30 VLAN 30

Ip Address:192.168.30.1/24

PC0 Address: VLAN 10



192.168.10.2/24

192.168.10.1

PC1 Address: VLAN 20

192.168.10.2/24

192.168.10.1

PC2 Address: VLAN 30

192.168.30.2/24

192.168.30.1

## **2. configure VLAN to switch:**

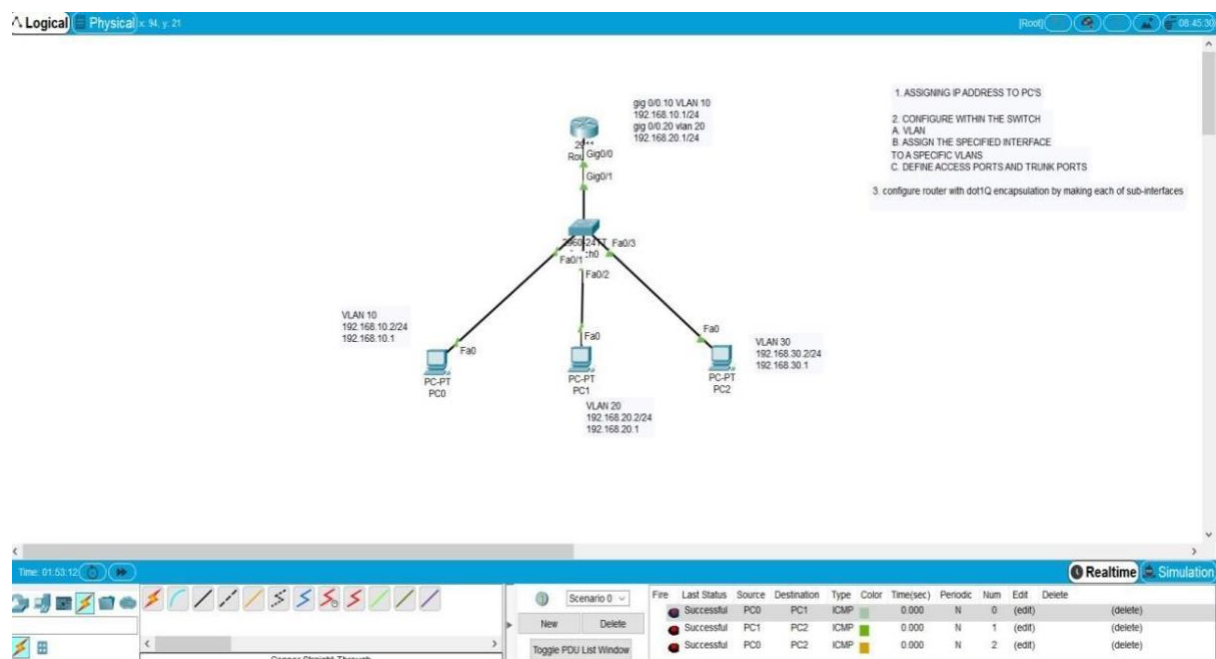
1. switch>enable
2. switch# configure terminal
3. switch(config)# interface gigabitethernet 0/1
4. switch(config-if)# switchport access vlan 10
5. switch(config-if)# switchport mode trunk
6. switch(config-if)# no shutdown
7. switch(config-if)# exit
8. switch(config)# Interface FastEthernet0/1
9. switch(config-if)# switchport access vlan 10
10. switch(config-if)# switchport mode access
11. switch(config-if)# no shutdown
12. switch(config-if)# exit
13. switch(config)# Interface FastEthernet0/2
14. switch(config-if)# switchport access vlan 20
15. switch(config-if)# switchport mode access
16. switch(config-if)# no shutdown
17. switch(config-if)# exit
18. switch(config)# Interface FastEthernet0/3
19. switch(config-if)# switchport access vlan 30
20. switch(config-if)# switchport mode access
21. switch(config-if)# no shutdown
22. switch(config-if)# exit





### 3. configure Switch to Router:

1. router>enable
2. router# configure terminal
3. router(config)# interface gigabitethernet 0/0.10
4. router(config-if)# encapsulation dot1Q 10
5. router(config-if)# ip address 192.168.10.1 255.255.255.0
6. router(config-if)# no shutdown
7. router(config-if)# exit
8. router(config)# interface gigabitethernet 0/0.20
9. router(config-if)# encapsulation dot1Q 20
10. router(config-if)# ip address 192.168.20.1 255.255.255.0
11. router(config-if)# no shutdown
12. router(config-if)# exit
13. router(config)# interface gigabitethernet 0/0.30
14. router(config-if)# encapsulation dot1Q 30
15. router(config-if)# ip address 192.168.30.1 255.255.255.0
16. router(config-if)# no shutdown
17. router(config-if)# exit





## **Practical: 6**

### **Aim: Wireless LAN.**

#### **WLAN:**

A Wireless LAN is a wireless computer network that links two or more devices using wireless communication to form a local area network (LAN) within a limited area such as a home, school, computer laboratory, campus, or office building. This gives users the ability to move around within the area and remain connected to the network. Through a gateway, a WLAN can also provide a connection to the wider Internet.

#### **SUMMARY:**

1. First create a wired topology between router, switch and pc to send message by wired communication. As Shown below. Provide IP address to pc and to router also.
2. Go to Router configuration and then to the fast Ethernet port on which switch is connected then provide their IP address to it and turn on the port status as shown below.
3. We need access point to connect the other devices wireless. So, connect access point to switch by copper straight through wire as shown below.
4. Now give WEP key and SSID to access point to secure the network.

#### **1. WLAN FOR TABLET:**

1. Take Tablet go to IP configuration and provide IP address and default gateway.
2. Now go to wireless configuration give WEP key and SSID then close it.



```
Physical  Config  Desktop  Custom Interface

Command Prompt

Packet Tracer PC Command Line 1.0
PC>ping 192.0.0.2

Pinging 192.0.0.2 with 32 bytes of data:

Reply from 192.0.0.2: bytes=32 time=0ms TTL=128
Reply from 192.0.0.2: bytes=32 time=0ms TTL=128
Reply from 192.0.0.2: bytes=32 time=0ms TTL=128
Reply from 192.0.0.2: bytes=32 time=0ms TTL=128

Ping statistics for 192.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

PC>
```

```
Physical  Config  Desktop  Custom Interface

Command Prompt

Packet Tracer PC Command Line 1.0
PC>ping 192.0.0.1

Pinging 192.0.0.1 with 32 bytes of data:

Reply from 192.0.0.1: bytes=32 time=0ms TTL=128
Reply from 192.0.0.1: bytes=32 time=0ms TTL=128
Reply from 192.0.0.1: bytes=32 time=0ms TTL=128
Reply from 192.0.0.1: bytes=32 time=0ms TTL=128

Ping statistics for 192.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

PC>
```



## 2.WLAN FOR SMARTPHONE:

1. Take smartphone to go IP configuration and provide IP address to it and set router's IP as the default gateway of smartphone
2. Then go to Wireless Configuration setting give WEP key and SSID of access point then close it.

Smartphone1

Physical Config **Desktop** Programming Attributes

Command Prompt

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=44ms TTL=128
Reply from 192.168.1.3: bytes=32 time=32ms TTL=128
Reply from 192.168.1.3: bytes=32 time=21ms TTL=128
Reply from 192.168.1.3: bytes=32 time=42ms TTL=128

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 21ms, Maximum = 44ms, Average = 34ms

C:\>
```

☐ Top

Smartphone0

Physical Config **Desktop** Programming Attributes

Command Prompt

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.4

Pinging 192.168.1.4 with 32 bytes of data:

Reply from 192.168.1.4: bytes=32 time=43ms TTL=128
Reply from 192.168.1.4: bytes=32 time=33ms TTL=128
Reply from 192.168.1.4: bytes=32 time=45ms TTL=128
Reply from 192.168.1.4: bytes=32 time=32ms TTL=128

Ping statistics for 192.168.1.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 32ms, Maximum = 45ms, Average = 38ms

C:\>
```

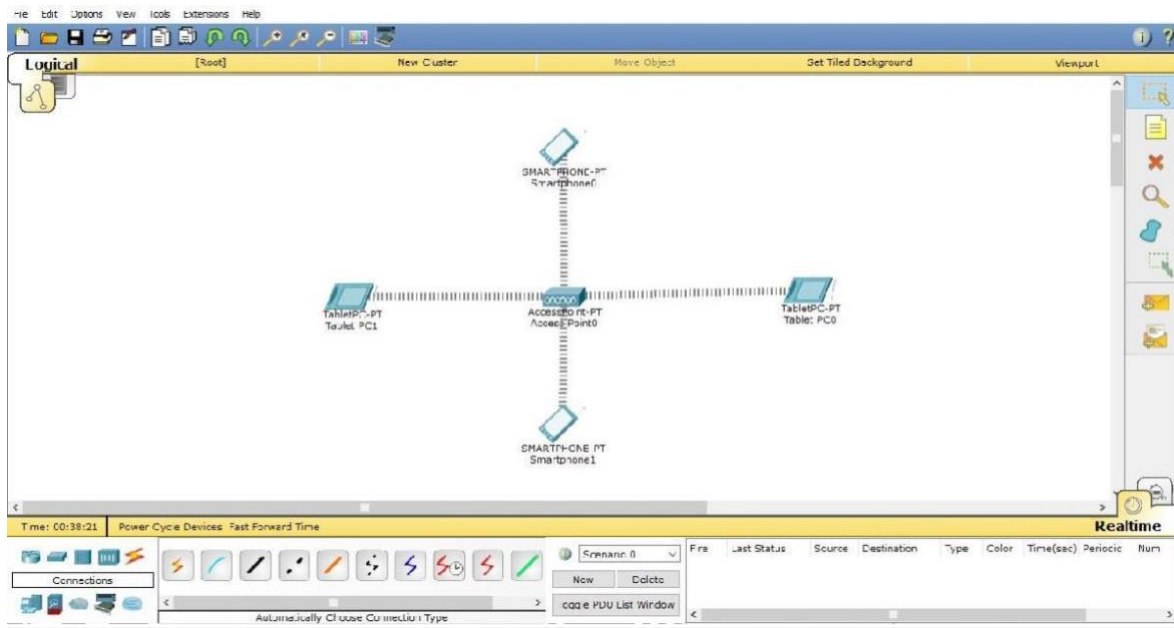
☐ Top



**Parul<sup>TM</sup>**  
University

**Faculty of Engineering & Technology**  
**Subject Name : Computer Networks**  
**Subject Code : 303105256**  
**B.Tech Year 2<sup>nd</sup> Semester 4<sup>th</sup>**

## WIRELESS LAN:





## **Practical: 7**

### **Aim: Internetworking with routers:**

#### **1: Experiment on same subnet**

#### **2: Perform Experiment across the subnet and observe functioning of Router via selecting suitable pair of Source and destination.**

In real world scenario, networks under same administration are generally scattered geographically. There may exist requirement of connecting two different networks of same kind as well as of different kinds. Routing between two networks is called internetworking.

Networks can be considered different based on various parameters such as, Protocol, topology, Layer-2 network and addressing scheme.

In internetworking, routers have knowledge of each other's address and addresses beyond them. They can be statically configured go on different network or they can learn by using internetworking routing protocol.

Routing protocols which are used within an organization or administration are called Interior Gateway Protocols or IGP. RIP, OSPF are examples of IGP. Routing between different organizations or administrations may have Exterior Gateway Protocol, and there is only one EGP i.e. Border Gateway Protocol.

### **Tunnelling:**

If they are two geographically separate networks, which want to communicate with each other, they may deploy a dedicated line between or they have to pass their data through intermediate networks.

Tunnelling is a mechanism by which two or more same networks communicate with each other, by passing intermediate networking complexities. Tunnelling is configured at both ends.



When the data enters from one end of Tunnel, it is tagged. This tagged data is then routed inside the intermediate or transit network to reach the other end of Tunnel. When data exists the Tunnel, its tag is removed and delivered to the other part of the network.

Both ends seem as if they are directly connected and tagging makes data travel through transit network without any modifications.

### **Packet fragmentation:**

Most Ethernet segments have their maximum transmission unit (MTU) fixed to 1500 bytes. A data packet can have more or less packet length depending upon the application. Devices in the transit path also have their hardware and software capabilities which tell what amount of data that device can handle and what size of packet it can process.

If the data packet size is less than or equal to the size of packet the transit network can handle, it is processed neutrally. If the packet is larger, it is broken into smaller pieces and then forwarded. This is called packet fragmentation. Each fragment contains the same destination and source address and routed through transit path easily. At the receiving end it is assembled again.

If a packet with DF (don't fragment) bit set to 1 comes to a router which cannot handle the packet because of its length, the packet is dropped.

When a packet is received by a router has its MF (more fragments) bit set to 1, the router then knows that it is a fragmented packet and parts of the original packet is on the way.

If packet is fragmented too small, the overhead is increases. If the packet is fragmented too large, intermediate router may not be able to process it and it might get dropped.

### **PROCEDURE STEPS FOR CISCO PACKET TRACER:**

#### **Step 1: Make an arrangement of the following experiment.**

We took 2 routers, 2 switch, 4 PC's and they are connected with each other.



2 Routers are connected with serial 2/0 wire as 2 of the same devices cannot be connected with straight or normal wire.

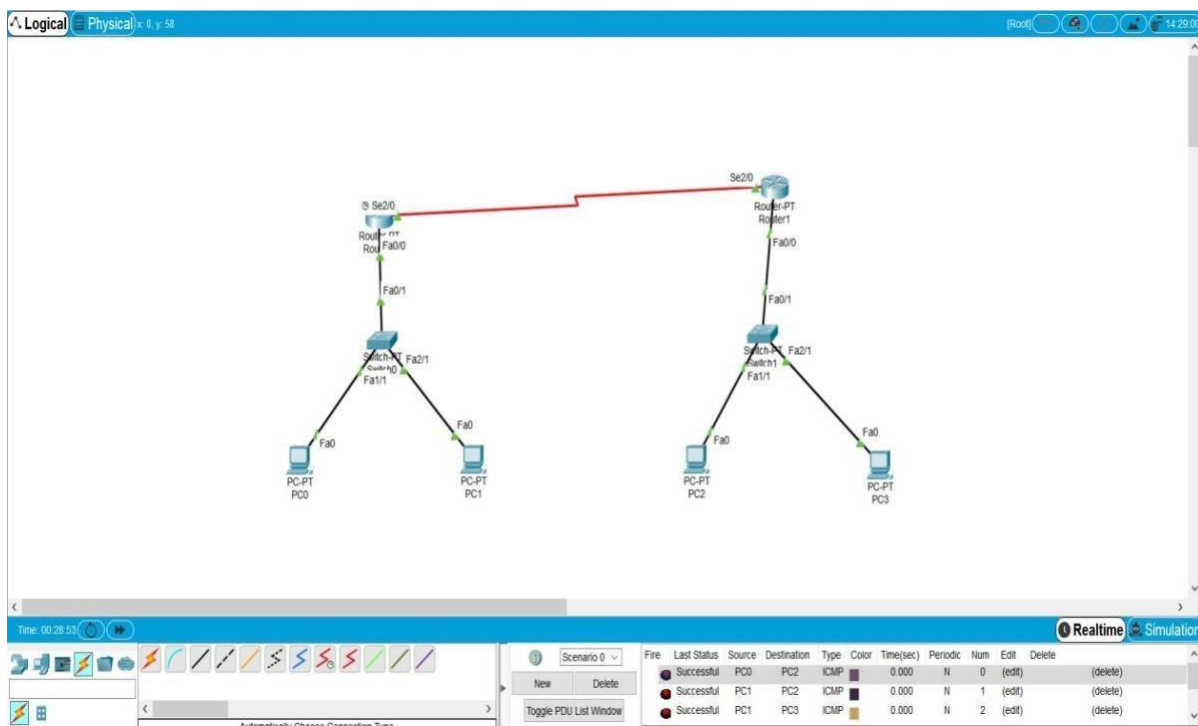
Switches are arranged in that manner that 1 switch connects only 1 Router and another switch connect another Router.

Each switch is connected to 2 PC.

Router-switch is connected through copper-straight through wire.

Switch-PC's are also connected with copper-straight through wire.

We made an arrangement in the cisco packet tracer as followed by figure given below:



**Step 2: Then we gave the CLI commands to both the Routers.**

**CLI commands For Router0:**

1. Router> enable
2. Router# configure terminal
3. Router(config-if)#interface fastethernet 0/0





4. Router(config-if)# ip address 192.168.1.1 255.255.255.0
5. Router(config-if)# Description router0 1 range
6. Router(config-if)# no shutdown
7. Router(config-if)# exit
8. Router(config)#exit
9. Router# configure Terminal
10. Router(config)# interface Serial2/0
11. Router(config-if)# ip address 192.168.2.1 255.255.255.0
12. Router(config-if)# clock rate 64000
13. Router(config-if)# no shutdown
14. Router(config-if)# exit
15. Router(Config)# exit

#### **CLI Commands for Router1:**

1. Router>enable
2. Router# configure Terminal
3. Router(config)# interface fastethernet 0/0
4. Router(config-if)# ip address 192.168.2.1 255.255.255.0
5. Router(config-if)# no shutdown
6. Router(config-if)# exit
7. Router(config)# exit
8. Router# Configure terminal
9. Router(config)# interface serial 2/0
10. Router(config-if)# ip address 192.168.1.1 255.255.255.0
11. Router(config-if)#no shutdown
12. Router(config-if)#exit
13. Router(config)#exit

**Step 3: we assigned the IP address, subnet mask, default gateway to each and every PC's which are connected to the switches.**

**Step 4: We checked the PC are connected with each other correctly by using Command Prompt by giving the IP address to other PC's**



## Step 5: connected Successful

```
PCO
Physical Config Desktop Programming Attributes
Command Prompt

Packet Tracer PC Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection:(default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::240:BFF:FEC4:782C
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 192.168.1.2
    Subnet Mask . . . . .: 255.255.255.0
    Default Gateway . . . . .: ::
    192.168.1.1

Bluetooth Connection:

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: ::
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 0.0.0.0
    Subnet Mask . . . . .: 0.0.0.0
    Default Gateway . . . . .: ::
    0.0.0.0

C:\>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Reply from 192.168.2.1: bytes=32 time=1ms TTL=255
Reply from 192.168.2.1: bytes=32 time<1ms TTL=255
Reply from 192.168.2.1: bytes=32 time=1ms TTL=255
Reply from 192.168.2.1: bytes=32 time=1ms TTL=255

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.2.2: bytes=32 time=2ms TTL=126
Reply from 192.168.2.2: bytes=32 time=1ms TTL=126
Reply from 192.168.2.2: bytes=32 time=2ms TTL=126

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

```
PCO
Physical Config Desktop Programming Attributes
Command Prompt

    Link-local IPv6 Address . . . . .: ::
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 0.0.0.0
    Subnet Mask . . . . .: 0.0.0.0
    Default Gateway . . . . .: ::
    0.0.0.0

C:\>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Reply from 192.168.2.1: bytes=32 time=1ms TTL=255
Reply from 192.168.2.1: bytes=32 time<1ms TTL=255
Reply from 192.168.2.1: bytes=32 time=1ms TTL=255
Reply from 192.168.2.1: bytes=32 time=1ms TTL=255

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.2.2: bytes=32 time=2ms TTL=126
Reply from 192.168.2.2: bytes=32 time=1ms TTL=126
Reply from 192.168.2.2: bytes=32 time=2ms TTL=126

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\>
C:\>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.2.2: bytes=32 time=1ms TTL=126
Reply from 192.168.2.2: bytes=32 time=6ms TTL=126
Reply from 192.168.2.2: bytes=32 time=1ms TTL=126
Reply from 192.168.2.2: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 6ms, Average = 2ms

C:\>
```



## **Practical: 8**

**Aim: Implementation of SUBNETTING: Design multiple subnet with suitable number of hosts. Make a plan to assign static IP addressing across all subnet to explain implementation of SUBNETTING.**

### **SUBNETTING:**

A subnetwork or subnet is a logical subdivision of an IP network.

The practice of dividing a network into two or more networks is called subnetting.

### **ADVANTAGES OF SUBNETTING:**

Subnetting was so helpful to solve the problem of lacking IP addresses on the Internet.

Allowing to use two or more LAN technologies together in the same network.

Subnets also helpful to minimize the size of the routing tables on the internet since additional network numbers will not be added to the table.

When a bigger network is divided into smaller networks, in order to maintain security, then that is known as Subnetting. so, maintenance is easier for smaller networks.

### **DESCRIPTION OF SUBNETTING IP ADDRESS THAT WE TOOK:**

IP ADDRESS: 194.4.3.0/25

CIDR NUMBER: 25

CLASS: CLASS C

SUBNET MASK: 255.255.255.224

BITS OF SUBNET: 3

NO OF HOST BITS: 5

TOTAL NUMBER OF SUBNETS: 8

VALID HOST:  $32-2=30$

BLOCK SIZE:  $256-224=32$



	SUBNET 0	SUBNET 1	SUBNET 2	SUBNET 3
SUBNET	194.4.3.0	194.4.3.32	194.4.3.64	194.4.3.96
FIRST ADDRESS	194.4.3.1	194.4.3.33	194.4.3.65	194.4.3.97
LAST ADDRESS	194.4.3.30	194.4.3.62	194.4.3.94	194.4.3.126
BROADCAST ADDRESS	194.4.3.31	194.4.3.63	194.4.3.95	194.4.3.127

	SUBNET 4	SUBNET 5	SUBNET 6	SUBNET 7
SUBNET	194.4.3.128	194.4.3.160	194.4.3.192	194.4.3.224
FIRST ADDRESS	194.4.3.129	194.4.3.161	194.4.3.193	194.4.3.225
LAST ADDRESS	194.4.3.158	194.4.3.190	194.4.3.222	194.4.3.254
BROADCAST ADDRESS	194.4.3.159	194.4.3.191	194.4.3.223	194.4.3.255

## **PROCEDURE STEPS FOR CISCO PACKET.**

### **STEP:1**

Here we need two generic routers (router0 and router1).

And need two generic switch (switch0 and switch1).

And we need four generic PC (PC0,PC1,PC2,PC3).

We use automatically choose connection type for connect router, switch and PC.

Connect Two Router with serial 2/0.



## **STEP 2: Then we gave the CLI commands to both the Routers.**

### **CLI COMMAND FOR ROUTER0:**

1. Router> enable
2. Router# configure terminal
3. Router(config)# interface fa0/0
4. Router(config-if)# ip address 194.4.3.10 255.255.255.224
5. Router(config-if)#no shutdown
6. Router(config-if)#exit
7. Router(config)# exit
8. Router# configure terminal
9. Router(config)#interface se 2/0
10. Router(config-if)# ip address 194.4.3.33 255.255.255.224
11. Router(config-if)# no shutdown
12. Router(config-if)#exit
13. Router(config)# exit
14. Router>enable
15. Router(config)#configure terminal
16. Router(config-if)#ip route 194.4.3.64 255.255.255.224 194.4.3.34
17. Router(config-if)#exit
18. Router(config)#exit

### **CLI COMMANDS FOR ROUTER1:**

1. Router> enable
2. Router# configure terminal
3. Router(config)# interface se 0/0
4. Router(config-if)# ip address 194.4.3.34 255.255.255.224
5. Router(config-if)#no shutdown
6. Router(config-if)#exit
7. Router(config)# exit
8. Router# configure terminal
9. Router(config)#interface fa 0/0



10. Router(config-if)# ip address 194.4.3.65 255.255.255.224
11. Router(config-if)# no shutdown
12. Router(config-if)#exit
13. Router(config)# exit
14. Router>enable
15. Router(config)#configure terminal
16. Router(config-if)#ip route 194.4.3.0 255.255.255.224 194.4.3.10
17. Router(config-if)#ip route 194.4.3.0 255.255.255.224 194.4.3.33
18. Router(config-if)#exit
19. Router(config)#exit

**STEP 3: we assigned the IP address, subnet mask, default gateway to each and every PC's which are connected to the switches.**

**PC0:**

Ip address:194.4.3.2

Subnet mask: 255.255.255.224

Default gateway: 194.4.3.10

**PC1:**

Ip address:194.4.3.3

Subnet mask: 255.255.255.224

Default gateway: 194.4.3.10

**PC2:**

Ip address:194.4.3.65

Subnet mask: 255.255.255.224

Default gateway: 194.4.3.65

**PC3:**

Ip address:194.4.3.66

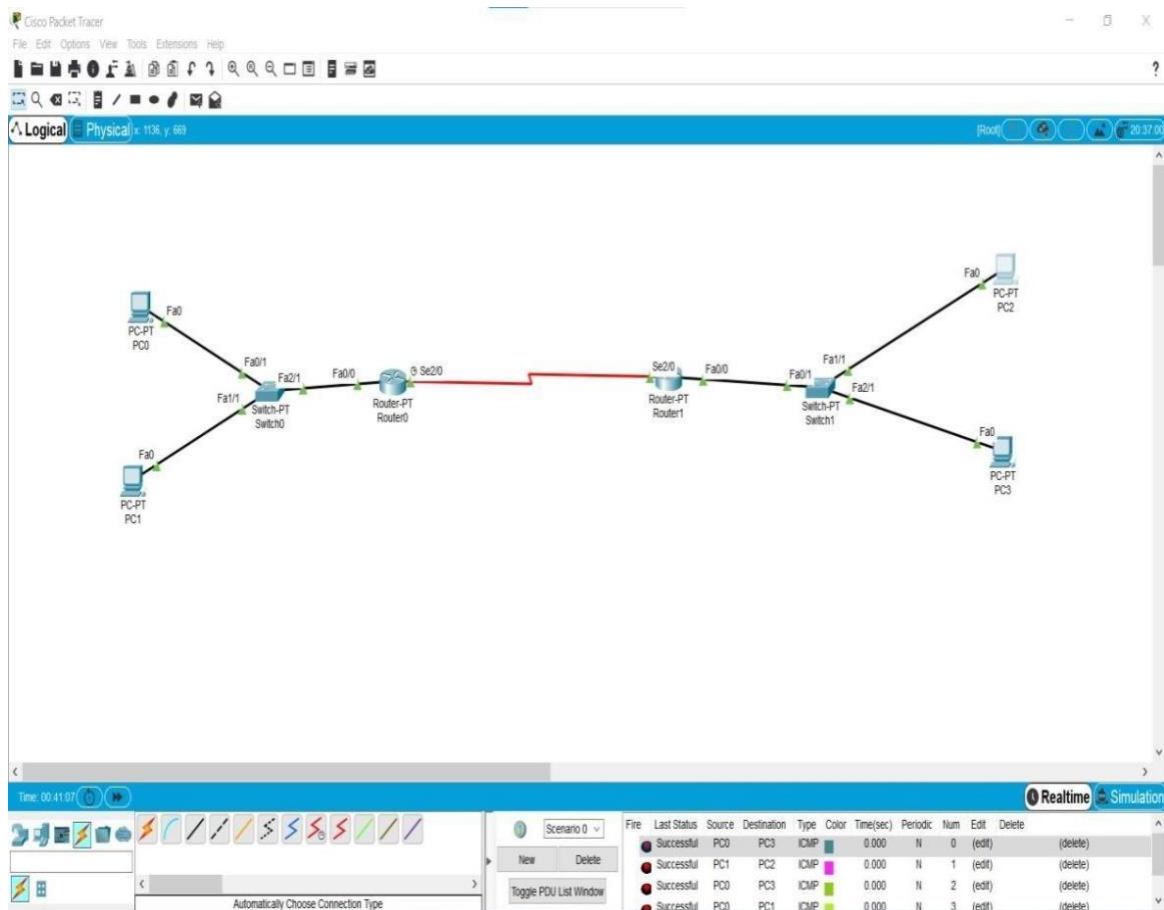


Subnet mask: 255.255.255.224

Default gateway: 194.4.3.65

**STEP 4: We checked the PC are connected with each other correctly by using Command Prompt by giving the IP address of other PC's**

**STEP 5: connected Successful**





## **Practical: 9**

### **Aim: Routing at Network Layer: Simulate Static and Dynamic Routing Protocol Configuration using CISCO Packet Tracer.**

#### **THEORY:**

Routing is a process which is performed by layer 3 (or network layer) devices in order to deliver the packet by choosing an optimal path from one network to another.

The network layer is responsible for routing, which is moving packets across the network using the most appropriate paths.

It also addresses messages and translates logical addresses (i.e., IP addresses) into physical addresses (i.e., MAC addresses).

#### **1. Static routing:**

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

##### **Advantages:**

- No routing overhead for router CPU which means a cheaper router can be used to do routing.
- It adds security because only administrator can allow routing to particular networks only.
- No bandwidth usage between routers.

##### **Disadvantage:**

- For a large network, it is a hectic task for administrator to manually add each route for the network in the routing table on each router.
- The administrator should have good knowledge of the topology. If a new administrator comes, then he has to manually add each route so he should have very good knowledge of the routes of the topology.

### **PROCEDURE STEPS FOR CISCO PACKET.**

#### **STEP:1**

Here we need three generic routers (router0, router1, router 2).

And need three generic switch (switch0, switch1, switch 3).

And we need six generic PC (PC0,PC1,PC2,PC3,PC4,PC5).





We use automatically choose connection type for connect router, switch and PC.

Connect three Router with serial 2/0.

**STEP 2: Then we gave the CLI commands to both the Routers.**

**CLI COMMAND FOR ROUTER0:**

1. Router> enable
2. Router# configure Terminal
3. Router(config)# interface serial 2/0
4. Router(config-if)#ip address 192.168.10.1 255.255.255.0
5. Router(config-if)# no shutdown
6. Router(config-if)# exit
7. Router(config)#exit
8. Router# configure Terminal
9. Router(config)# interface fa 0/0
10. Router(config-if)#ip address 192.168.30.1 255.255.255.0
11. Router(config-if)# no shutdown
12. Router(config-if)# exit
13. Router(config)#exit
14. Router(config)# ip dhcp pool a
15. Router(config-if)# network 192.168.30.0 255.255.255.0
16. Router(config-if)# default-router 192.168.30.1
17. Router(config-if)# exit
18. Router(config)# Router rip
19. Router(config-if)#network 192.168.10.0
20. Router(config-if)# network 192.168.30.0
21. Router(Config-if)#exit
22. Router(config)# interface Serial 2/0
23. Router(config-if)# clock Rate 4000000
24. Router(config-if)#exit
25. Router(config)# interface Serial 2/0



26. Router(config-if)# clock Rate 4000000

27. Router(config-if)#exit

### **CLI COMMAND FOR ROUTER 1:**

1. Router> enable
2. Router# configure Terminal
3. Router(config)# interface serial 2/0
4. Router(config-if)#ip address 192.168.10.2 255.255.255.0
5. Router(config-if)# no shutdown
6. Router(config-if)# exit
7. Router(config)#exit
8. Router# configure Terminal
9. Router(config)# interface serial 3/0
10. Router(config-if)#ip address 192.168.20.1 255.255.255.0
11. Router(config-if)# no shutdown
12. Router(config-if)# exit
13. Router(config)#exit
14. Router(config)# interface fa 0/0
15. Router(config-if)#ip address 192.168.40.1 255.255.255.0
16. Router(config-if)# no shutdown
17. Router(config-if)# exit
18. Router(config)#exit
19. Router(config)# ip dhcp pool b
20. Router(config-if)# network 192.168.40.0 255.255.255.0
21. Router(config-if)# default-router 192.168.40.1
22. Router(config-if)# exit
23. Router(config)# Router rip
24. Router(config-if)#network 192.168.10.0
25. Router(config-if)# network 192.168.20.0
26. Router(config-if)# network 192.168.40.0
27. Router(config-if)# network 192.168.20.0
28. Router(config-if)# network 192.168.10.0



29. Router(Config-if)#exit
30. Router(config)# interface Serial 2/0
31. Router(config-if)# clock Rate 4000000
32. Router(config-if)#exit
33. Router(config)# interface Serial 2/0
34. Router(config-if)# clock Rate 4000000
35. Router(config-if)#exit

### **CLI COMMANDS FOR ROUTER2:**

1. Router> enable
2. Router# configure Terminal
3. Router(config)# interface serial 2/0
4. Router(config-if)#ip address 192.168.20.1 255.255.255.0
5. Router(config-if)# no shutdown
6. Router(config-if)# exit
7. Router(config)#exit
8. Router# configure Terminal
9. Router(config)# interface fa 0/0
10. Router(config-if)#ip address 192.168.50.1 255.255.255.0
11. Router(config-if)# no shutdown
12. Router(config-if)# exit
13. Router(config)#exit
14. Router(config)# ip dhcp pool e
15. Router(config-if)# network 192.168.50.1 255.255.255.0
16. Router(config-if)# default-router 192.168.50.1
17. Router(config-if)# exit
18. Router(config)# Router rip
19. Router(config-if)#network 192.168.20.0
20. Router(config-if)# network 192.168.50.0
21. Router(Config-if)#exit
22. Router(config)# interface Serial 2/0
23. Router(config-if)# clock Rate 4000000



- 24. Router(config-if)#exit
- 25. Router(config)# interface Serial 2/0
- 26. Router(config-if)# clock Rate 4000000
- 27. Router(config-if)#exit

**STEP 3: we assigned the IP address, subnet mask, default gateway to each and every PC's which are connected to the switches.**

**PC0:**

Ip address:192.168.30.2

Subnet mask: 255.255.255.0

Default gateway: 192.168.30.1

**PC1:**

Ip address:192.168.30.3

Subnet mask: 255.255.255.0

Default gateway: 192.168.30.1

**PC2:**

Ip address:192.168.40.3

Subnet mask: 255.255.255.0

Default gateway: 192.168.40.1

**PC3:**

Ip address:192.168.40.2

Subnet mask: 255.255.255.0

Default gateway: 192.168.40.1

**PC4:**

Ip address:192.168.50.2



Subnet mask: 255.255.255.0

Default gateway: 192.168.50.1

#### PC5:

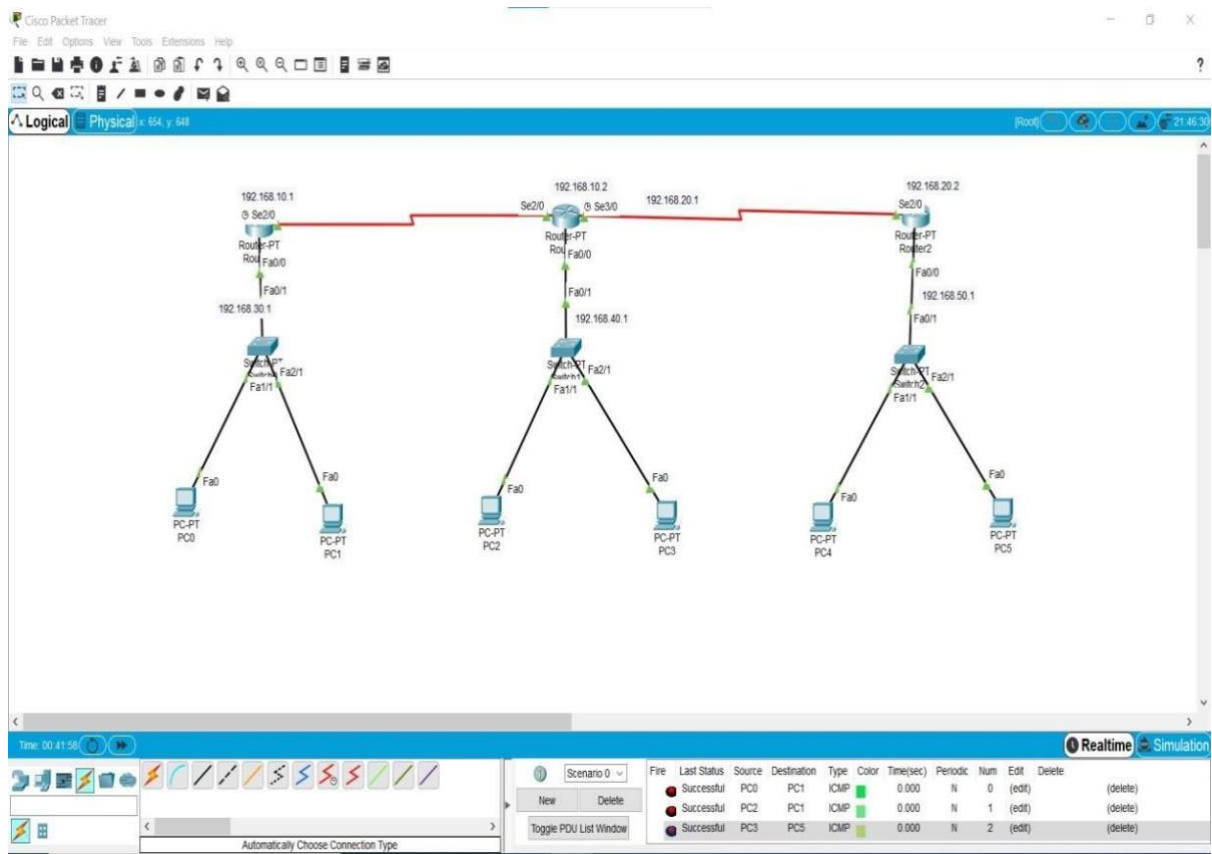
Ip address: 192.168.50.3

Subnet mask: 255.255.255.0

Default gateway: 192.168.50.1

**STEP 4: We checked the PC are connected with each other correctly by using Command Prompt by giving the IP address of other PC's**

**STEP 5: connected Successful**





## **Practical: 10**

### **Aim: Experiment on Transport Layer: Implement echo client server using TCP/UDP sockets.**

1: Experiment on same subnet.

2: Perform Experiment across the subnet and observe functioning of Router via selecting suitable pair of Source and destination.

Transport Layer:

The transport layer is the layer in the open system interconnection (OSI) model responsible for end-to-end communication over a network.

It provides logical communication between application processes running on different hosts within a layered architecture of protocols and other network components.

The transport layer is represented by two protocols: TCP and UDP.

The IP protocol in the network layer delivers a datagram from a source host to the destination host.

TCP:

TCP stands for Transmission Control Protocol.

It provides full transport layer services to applications.

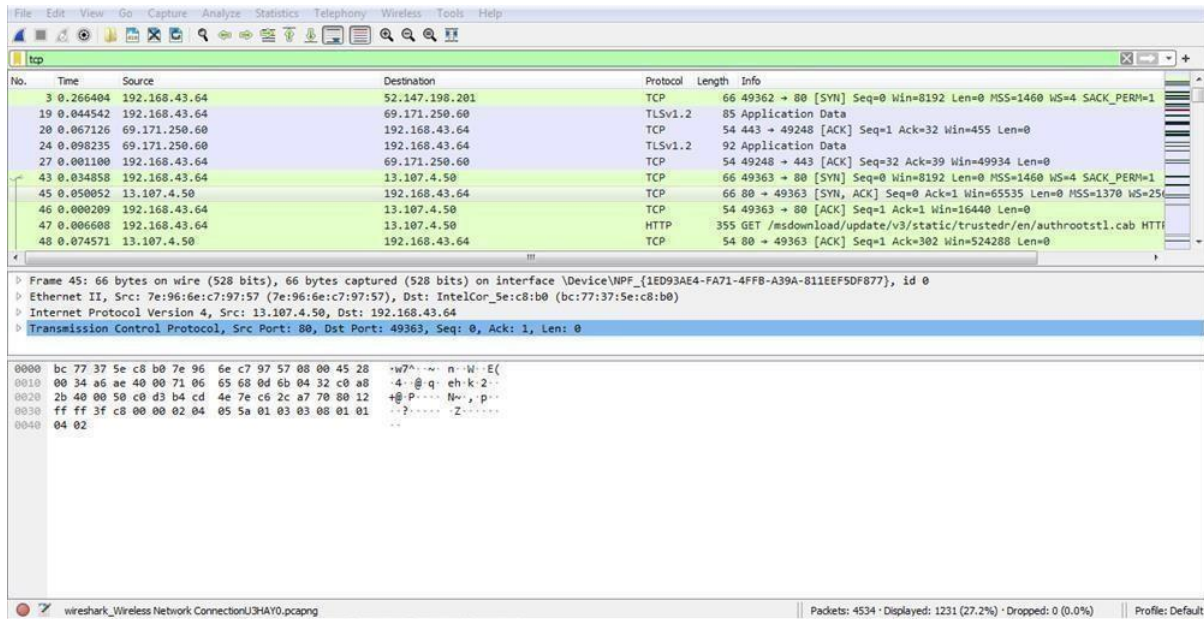
It is a connection-oriented protocol means the connection established between both the ends of the transmission. For creating the connection, TCP generates a virtual circuit between sender and receiver for the duration of a transmission.

#### **STEPS FOR DOING IN WIRELESS NETWORK CONNECTION:**

- STEP:1 OPEN SOFTWARE
- STEP:2 SELECT WI-FI OPTION
- STEP:3 CLICK ON THE SEARCH BAR AND SEARCH 'tcp'.



## OUTPUT:



UDP: UDP stands for User Datagram Protocol.

UDP is a simple protocol and it provides non sequenced transport functionality.

UDP is a connectionless protocol.

This type of protocol is used when reliability and security are less important than speed and size.

UDP is an end-to-end transport level protocol that adds transport level addresses, checksum error control, and length information to the data from the upper layer.

The packet produced by the UDP protocol is known as a user datagram.

### STEPS FOR DOING IN WIRELESS NETWORK CONNECTION:

- STEP:1 OPEN SOFTWARE
- STEP:2 SELECT WI-FI OPTION
- STEP:3 CLICK ON THE SERCH BAR AND SERCH 'UDP'



## OUTPUT:

The screenshot shows a Wireshark packet capture interface. The top pane displays a list of captured packets, primarily UDP traffic. The bottom pane provides a detailed view of the selected packet (Frame 2), showing the Ethernet II header, Internet Protocol Version 4 header, and the User Datagram Protocol (UDP) payload, which is a NetBIOS Name Service packet. The packet details include the source and destination IP addresses, port numbers, and the NetBIOS Name Service data.

No.	Time	Source	Destination	Protocol	Length	Info
14..	0.156940	172.217.194.189	192.168.43.64	UDP	69	443 → 55846 Len=27
14..	0.201138	192.168.43.64	172.217.194.189	UDP	75	55846 → 443 Len=33
14..	0.145005	172.217.194.189	192.168.43.64	UDP	69	443 → 55846 Len=27
14..	0.401051	192.168.43.64	172.217.194.189	UDP	75	55846 → 443 Len=33
14..	0.159729	172.217.194.189	192.168.43.64	UDP	69	443 → 55846 Len=27
14..	0.588196	192.168.43.64	255.255.255.255	DHCP	342	DHCP Inform - Transaction ID 0xf3de30f3
14..	0.213070	192.168.43.64	172.217.194.189	UDP	75	55846 → 443 Len=33
14..	0.191049	192.168.43.64	172.217.194.189	UDP	75	55846 → 443 Len=33
14..	0.067257	172.217.194.189	192.168.43.64	UDP	69	443 → 55846 Len=27
14..	0.060662	172.217.194.189	192.168.43.64	UDP	70	443 → 55846 Len=28

Frame 2: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface \Device\NPF\_{1ED93AE4-FA71-4FFB-A39A-811EEF50F877}, id 0  
Ethernet II, Src: IntelCor\_Sec8:b0 (bc:77:37:5e:c8:b0), Dst: Broadcast (ff:ff:ff:ff:ff:ff)  
Internet Protocol Version 4, Src: 192.168.43.64, Dst: 192.168.43.255  
User Datagram Protocol, Src Port: 137, Dst Port: 137  
NetBIOS Name Service

0000 ff ff ff ff ff ff bc 77 37 5e c8 b0 08 00 45 00 .....w7^...E-  
0010 00 4e 26 fb 00 00 08 11 3b 14 c0 a8 2b 40 c0 a8 ..N8....;...+@..  
0020 2b ff 00 09 00 09 00 3a 50 20 94 49 01 10 00 01 +.....!P.I.....  
0030 00 00 00 00 00 00 20 46 48 46 41 45 42 45 45 43 .....F HFAEBEEC  
0040 41 43 41 43 41 43 41 43 41 43 41 43 41 43 41 43 ACACACAC ACACACAC  
0050 41 43 41 43 41 41 41 00 00 20 00 01 ACACAAA:.....