# Practical 0

**Aim:-** To get familiarise with Cisco Packet Tracer and WireShark.

**Part A:-** What is Cisco Packet Tracer and Wireshark?

**Cisco Packet Tracer** is a network simulation tool developed by Cisco Systems. It's widely used for teaching and learning networking concepts, Internet of Things (IoT), and cybersecurity skills in a virtual lab environment. Packet Tracer allows users to create network topologies by dragging and dropping virtual devices like routers, switches, and PCs. It's a valuable tool for students and instructors to practice and understand networking without needing physical hardware.

**Features:**

1. **Network Simulation:** Create and simulate networks with a wide range of Cisco devices, including routers, switches, and PCs.
2. **Interactive Learning:** Provides an interactive platform for learning and understanding network concepts, protocols, and configurations.
3. **Multi-User Functionality:** Allows multiple users to collaborate and interact with the same network topology, enhancing collaborative learning.
4. **Network Modeling:** Supports complex network models with both logical and physical views, enabling users to visualize the entire network setup.
5. **IoT and Cybersecurity:** Includes simulation capabilities for Internet of Things (IoT) devices and cybersecurity scenarios, expanding learning opportunities.

**Use Cases:**

- **Education:** Widely used in academic institutions to teach networking fundamentals and Cisco certification courses (CCNA, CCNP).
- **Self-Learning:** Enables students and professionals to practice and reinforce their networking skills.
- **Network Design:** Helps network administrators and engineers to prototype and test network designs before deployment.

**Wireshark** is a free and open-source network protocol analyzer. It's used for network traffic analysis and troubleshooting. Wireshark captures and inspects packets from network connections, allowing users to see the detailed data being transmitted over the network. It's a powerful tool for network administrators, security professionals, and anyone interested in understanding network behavior and diagnosing issues.

**Features:**

1. **Packet Capture:** Captures live data packets from network interfaces, providing a detailed view of network activity.
2. **Protocol Analysis:** Supports thousands of network protocols, enabling users to analyze specific protocol behaviors and interactions.
3. **Filtering and Search:** Advanced filtering options allow users to focus on specific types of traffic or network events, making it easier to diagnose issues.
4. **Reassembly:** Reassembles and displays the data streams of certain protocols, such as TCP or HTTP, for detailed inspection.
5. **Visualization:** Offers graphical representations of traffic patterns and network statistics, helping users to understand network performance and trends.

**Use Cases:**

- **Network Troubleshooting:** Helps network administrators to identify and resolve network issues, such as latency, packet loss, and configuration errors.
- **Security Analysis:** Used by cybersecurity professionals to detect and analyze security threats, intrusions, and vulnerabilities.
- **Protocol Development:** Assists protocol developers in testing and debugging new protocols or modifications to existing ones.

## **Part B:-** How to work in Cisco Packet Tracer and Wireshark.

**Cisco Packet Tracer** is an advanced network simulation tool that allows users to visualize and experiment with network configurations and operations in a virtual environment. Here's a brief guide on how to get started:

1. **Creating a Network:**
    - Open Cisco Packet Tracer.
    - Drag and drop devices (like routers, switches, PCs) from the device palette onto the workspace.
    - Use the connection tool to link devices together with cables (copper straight-through, copper crossover, etc.).
2. **Configuring Devices:**
    - Click on a device to open its configuration window.
    - Configure basic settings like IP addresses, subnet masks, and routing protocols.
    - For routers and switches, use the CLI (Command Line Interface) tab to input commands.

3. **Simulating Network Activity:**
    - Use the simulation mode to visualize packet flows between devices.
    - Add applications (like web browsing or file transfer) to endpoints and observe how packets travel through the network.
4. **Collaborative Learning:**
    - Utilize multi-user functionality to collaborate with others on the same network topology, enhancing interactive learning experiences.
5. **Saving and Sharing:**
    - Save your network topology by going to File > Save.
    - Share the saved .pkt file with others who can open it in their Cisco Packet Tracer.

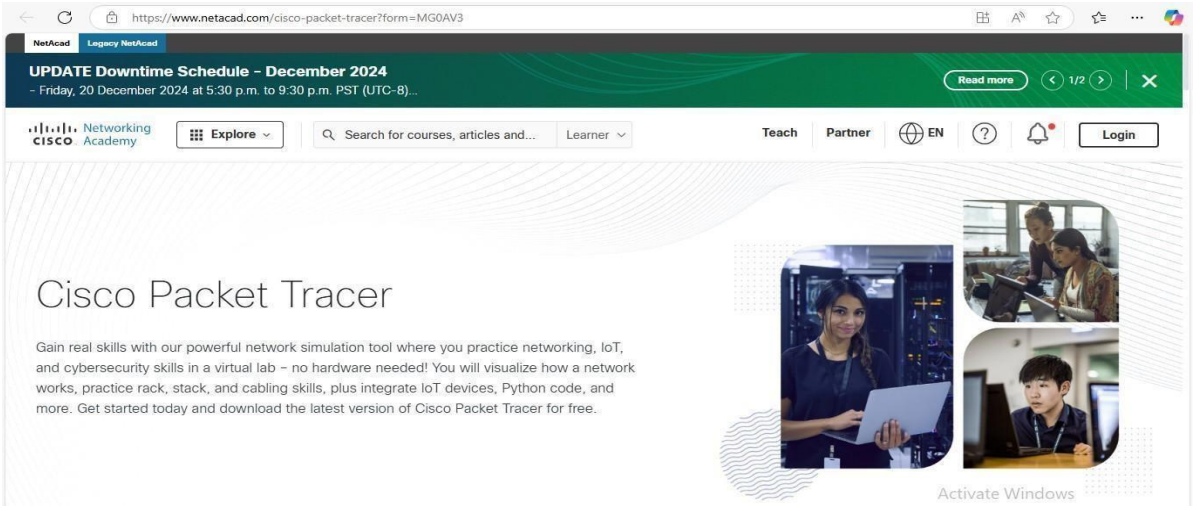
**Wireshark** is a powerful network protocol analyzer that captures and displays data packets traveling through a network. Here's how you can start using it:

1. **Capturing Packets:**
    - Open Wireshark.
    - Select the network interface you want to capture traffic from (e.g., Ethernet, Wi-Fi).
    - Click on the "Start Capturing Packets" button.
2. **Analyzing Packets:**
    - As packets are captured, they will appear in the main window.
    - Click on a packet to view its details. The window will split into three sections: a summary of the capture, detailed packet information, and a hexadecimal representation.
3. **Filtering Traffic:**
    - Use display filters to isolate specific types of traffic. For example, to view only HTTP traffic, type `http` in the filter bar.
    - Apply various filters to focus on specific protocols, IP addresses, or port numbers.
4. **Packet Reassembly:**
    - Use reassembly features to analyze complete data streams, such as reassembling TCP streams to view entire communications.
5. **Saving and Exporting:**
    - Save your capture data by going to File > Save As.
    - Export specific packets or entire capture sessions for further analysis.

**Part C:-** How to download the Cisco Packet Tracer and Wireshark.

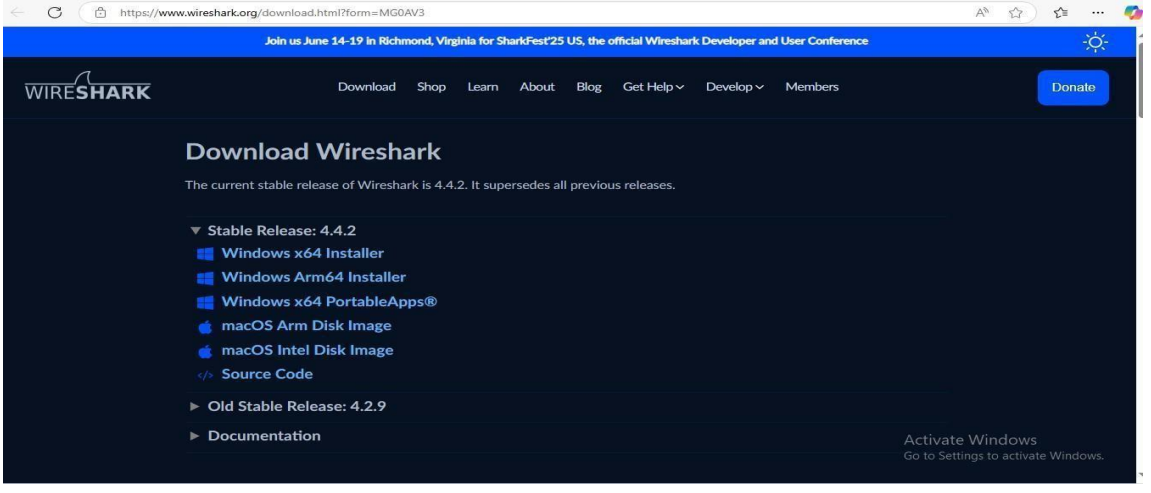
### Downloading Cisco Packet Tracer:-

1. **Visit the Cisco Networking Academy website:** Go to the Cisco Packet Tracer download page.
2. **Create an Account:** If you don't have a Cisco Networking Academy account, you'll need to create one.
3. **Download the Software:** Once logged in, you can download Cisco Packet Tracer for your operating system (Windows, macOS, or Linux).




### Downloading Wireshark:-

1. **Visit the Wireshark website:** Go to the Wireshark download page.
2. **Choose Your Version:** Select the appropriate installer for your operating system (Windows, macOS, or Linux).
3. **Download and Install:** Click the download link and follow the installation instructions.



# Practical 1

**Aim:-** Experiments on Simulation Tools (Cisco Packet Tracer).

## Topologies:-

1. **Ring :-**

A ring topology is a network configuration where device connections create a circular data path. Each networked device is connected to two others, like points on a circle. Together, devices in a ring topology are referred to as a ring network.

Step1: Select PCs and switches(29050-24) then connect PCs to switches with straight-through(straight wire) and switches to switches with crossover(dashed wired)

Step2: Connect them as shown in the image above. Also give them a proper IP address.

Step3: Pass a message and check the simulation.

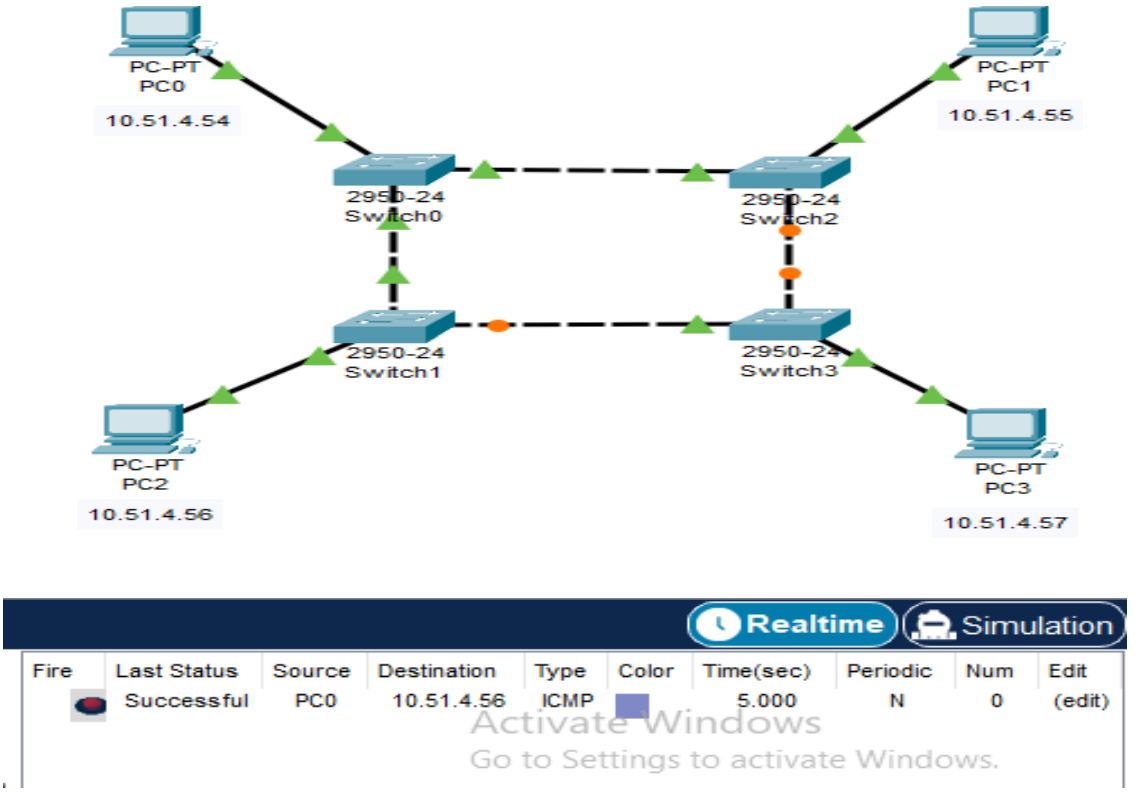



**Figure 1.1: Ring Topology**

## 2. MESH

A mesh topology is a network setup where each computer and network device is interconnected with one another. This topology setup allows for most transmissions to be distributed even if one of the connections goes down. It is a topology commonly used for wireless networks.

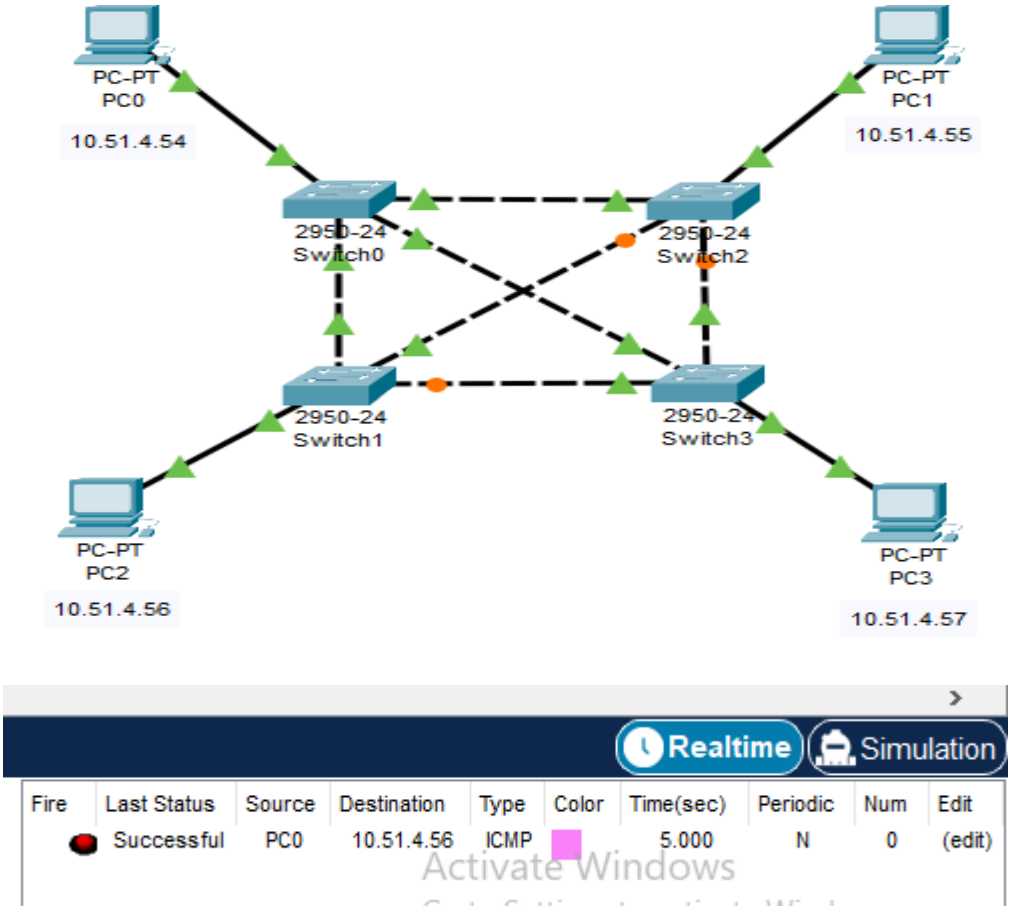



**Figure 1.2: Mesh Topology**

## 3. Star

A star topology is a topology for a Local Area Network (LAN) in which all nodes are individually connected to a central connection point, like a hub or a switch. A star takes more cable than e.g. a bus, but the benefit is that if a cable fails, only one node will be brought down.

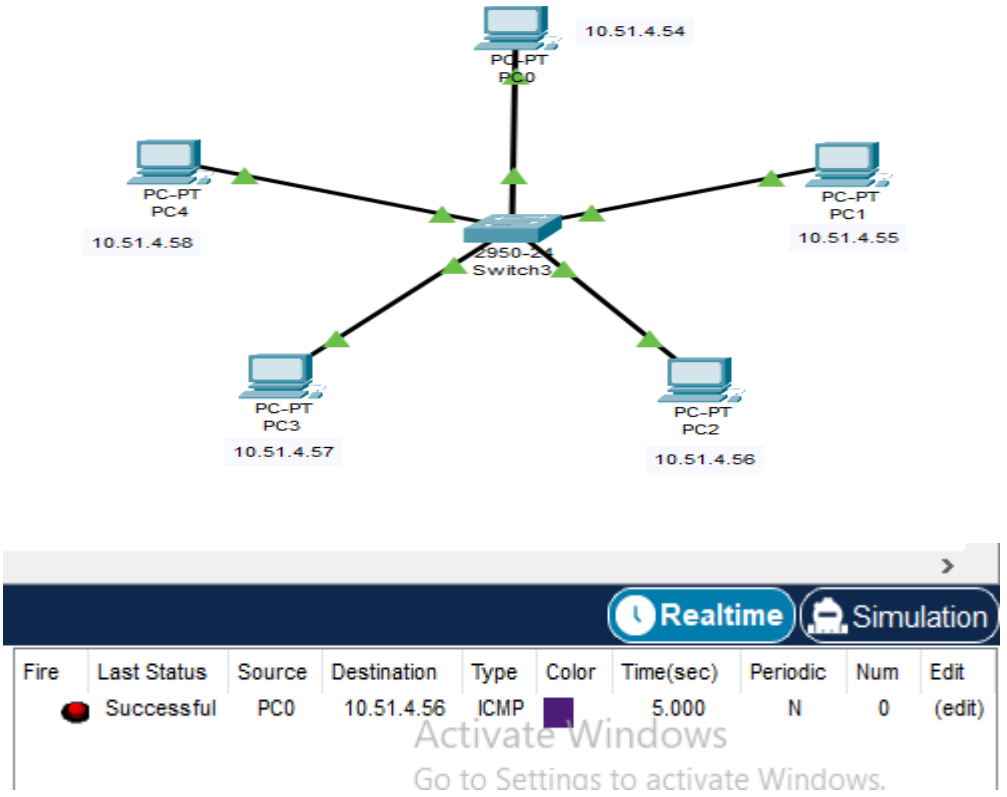
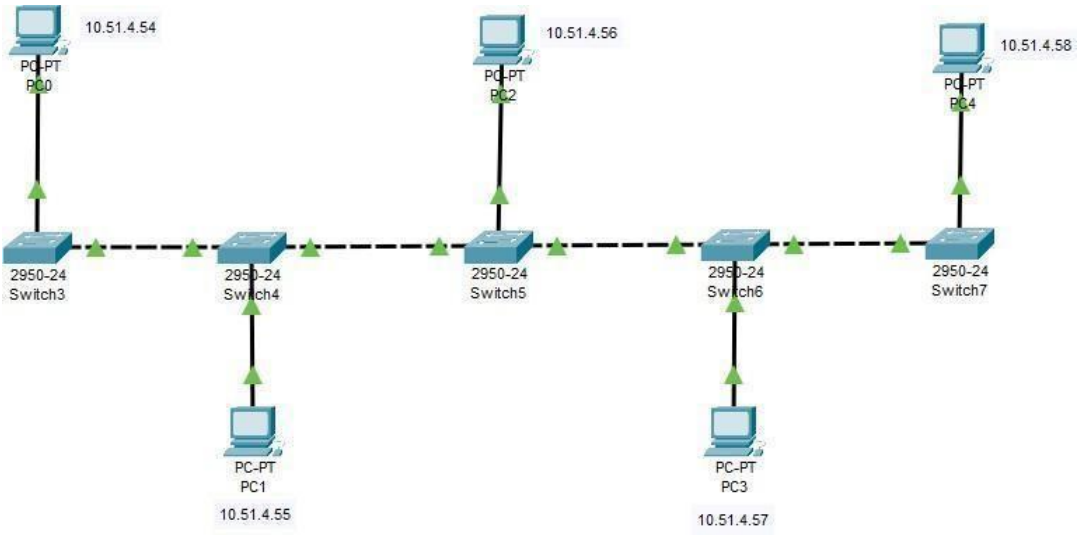



**Figure 1.3: Star Topology**

## 4. BUS

A bus topology is a topology for a Local Area Network (LAN) in which all the nodes are connected to a single cable. The cable to which the nodes connect is called a "backbone". If the backbone is broken, the entire segment fails.


10.51.4.54
PC-PT
PC0
10.51.4.56
PC-PT
PC2
10.51.4.58
PC-PT
PC4
2950-24
Switch3
2950-24
Switch4
2950-24
Switch5
2950-24
Switch6
2950-24
Switch7
PC-PT
PC1
10.51.4.55
PC-PT
PC3
10.51.4.57

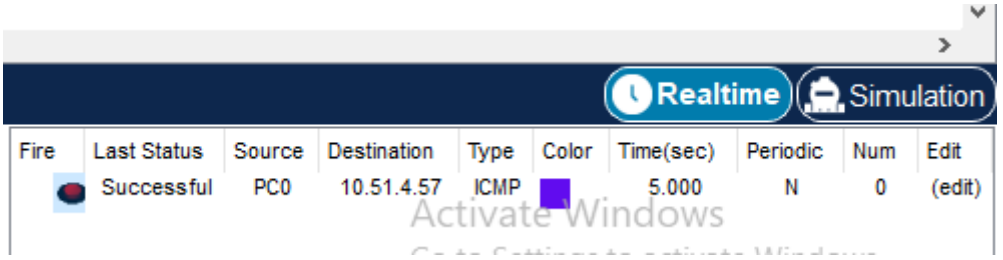
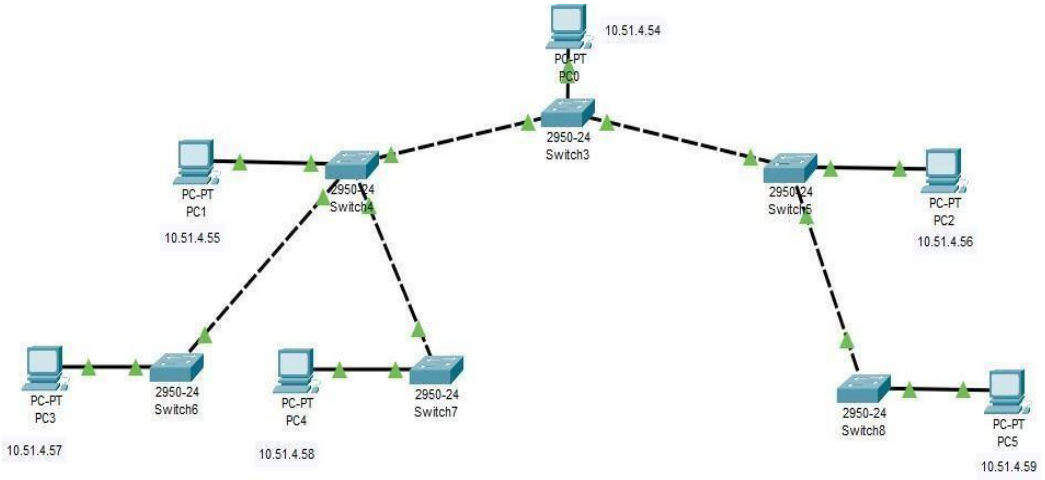



Figure 1.4: Bus Topology

## 5. TREE

A tree topology is a special type of structure where many connected elements are arranged like the branches of a tree. For example, tree topologies are frequently used to organize the computers in a corporate network, or the information in a database.



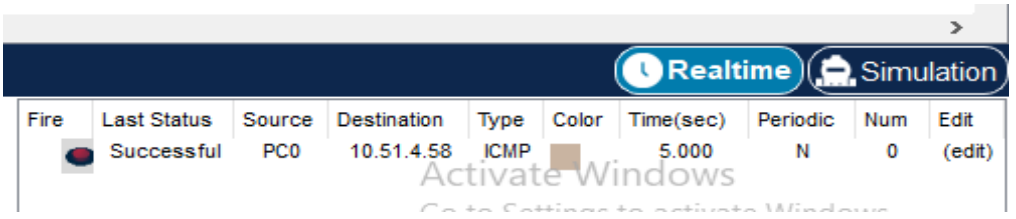




**Figure 1.5: Tree Topology**

## 6. HYBRID

A hybrid topology is a type of network topology that uses two or more different network topologies. These topologies can include a mix of bus topology, mesh topology, ring topology, star topology, and tree topology.

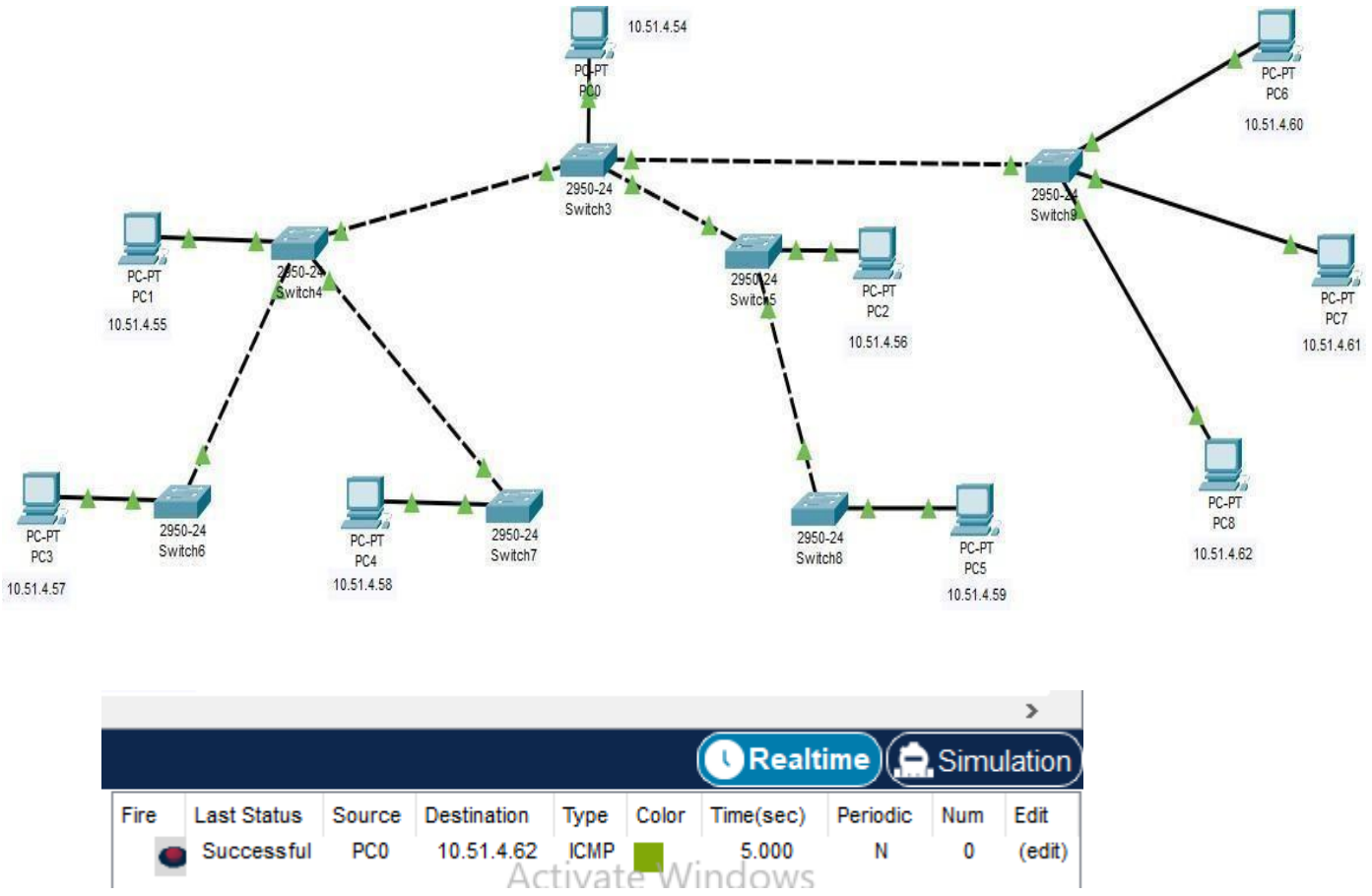


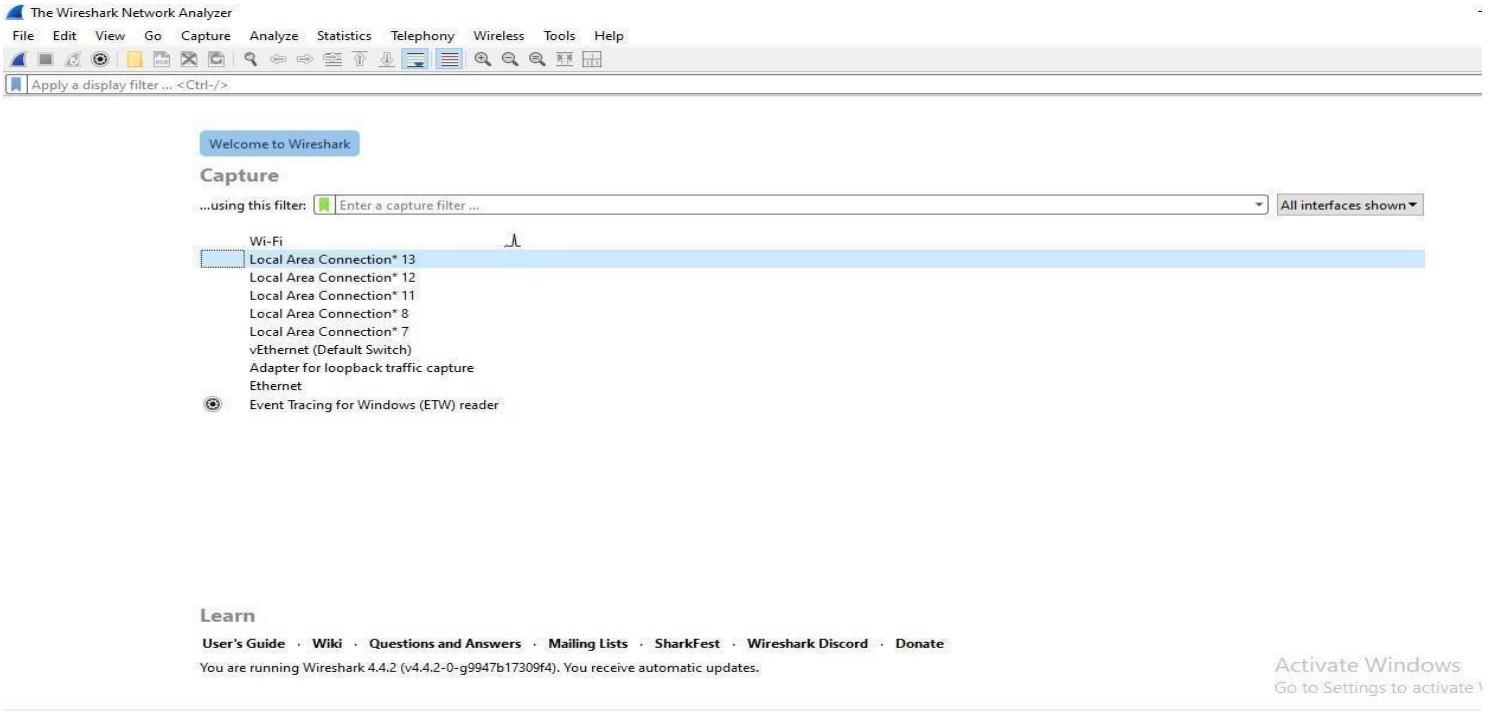

**Figure 1.6: Hybrid Topology**

# Practical 2

**Aim:-** To understand features of wireshark as a packet capture tool and understand encapsulation of information. Also study the effect of a few network commands.

**Purpose:**

The main objective of the proposed experiment is to give exposure of wire-shark tools to students so they can learn to monitor transmission packets being sent in Wi-Fi and LAN environments.

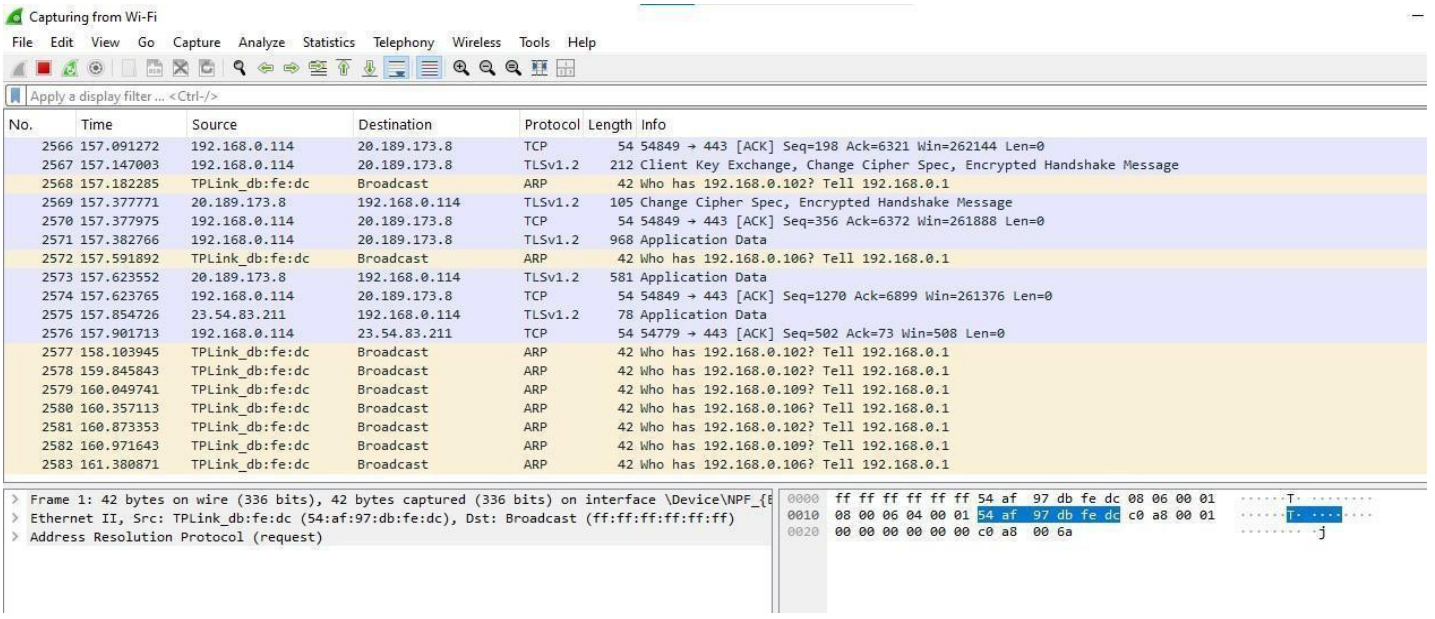



**Features:**

1. **Live Packet Capture:** Captures live data packets from network interfaces.
2. **File Import:** Can open files containing packet data captured with other programs like tcpdump.
3. **Protocol Dissectors:** Supports thousands of network protocols, providing detailed information about each packet.
4. **Detailed Display:** Displays packets with detailed protocol information, including headers and payloads.
5. **Filtering:** Allows users to filter packets based on various criteria, such as protocol type, IP address, or port number.

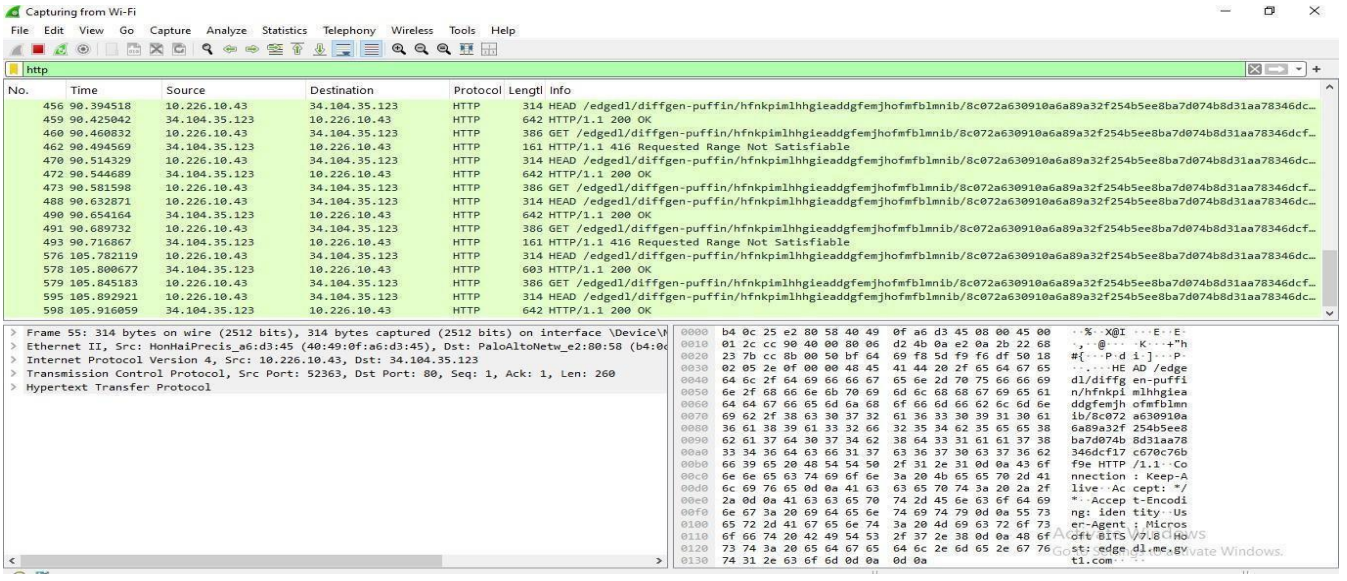
## Encapsulation of Information :-

Encapsulation is the process of wrapping data with protocol-specific headers and trailers as it moves down the OSI model layers. Each layer adds its own header (and sometimes trailer) to the data from the upper layer, creating a new data unit. For example, an HTTP message is encapsulated within a TCP segment, which is then encapsulated within an IP packet, and finally, the IP packet is encapsulated within an Ethernet frame.



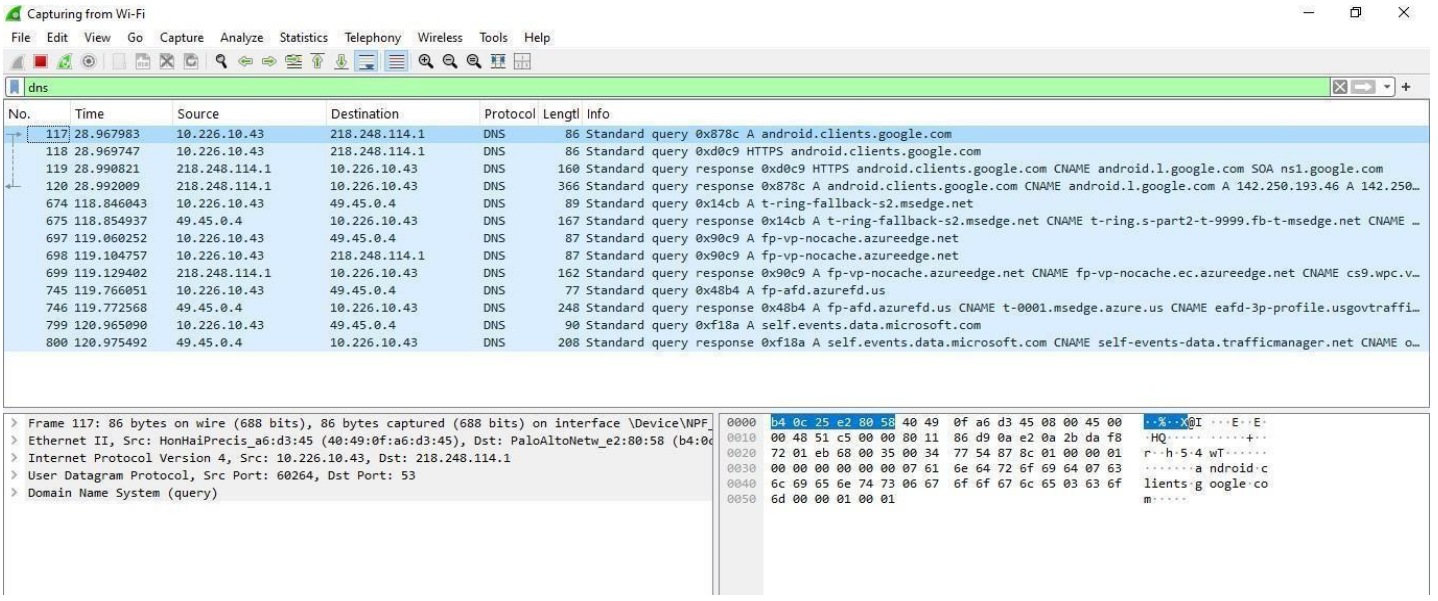

## HTTP (Hypertext Transfer Protocol) :-

HTTP is the foundation of data communication on the web. It's the protocol used to load web pages using hypertext links. It defines how messages are formatted and transmitted, and how web servers and browsers should respond to various commands. When you enter a URL in your web browser, an HTTP request is sent to the web server, which then returns the requested webpage.



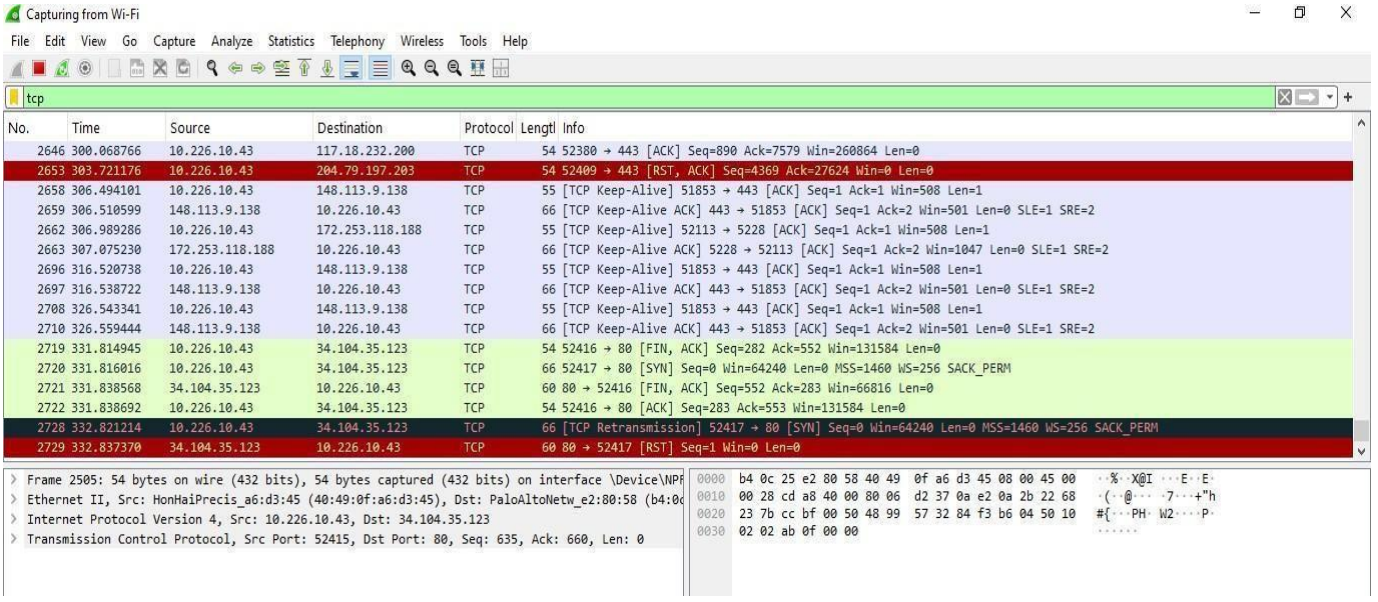
## DNS (Domain Name System) :-

DNS is like the phonebook of the internet. It translates domain names (like www.example.com) into IP addresses that computers use to identify each other on the network. When you type a domain name into your browser, a DNS server translates that name into the corresponding IP address, allowing your browser to locate the web server and access the website.




## TCP (Transmission Control Protocol) :-

TCP is one of the main protocols in the Internet Protocol (IP) suite. It provides reliable, ordered, and error-checked delivery of data between applications communicating over a network. TCP ensures that data sent from one end of a connection arrives correctly at the other end, by establishing a connection, managing data transfer, and handling errors or lost packets.



# Practical 3

**Aim :-** To study behavior of generic devices used for networking: (Cisco Packet Tracer)

**Summary of devices we use:**

**Switch 2950-54:**

The Cisco Catalyst 2950C 24 and Catalyst 2950T 24 Switches belong to the Cisco Catalyst 2950 series of high-performance, standalone, 10/100 auto sensing Fast Ethernet and Gigabit Ethernet switches. Both products bring intelligent services to the network edge to accommodate the needs of growing workgroups and server connectivity.

**Router 4321:**

The Cisco 4000 Series Integrated Services Routers (ISR) revolutionize WAN communications in the enterprise branch. With new levels of built-in intelligent network capabilities and convergence, the routers specifically address t\he growing need for application-aware networking in distributed enterprise sites.

**Hub-pt:**

Hub is a very simple network device that is used in LANs. It is basically a multiport repeater. Hubs do not decide anything and forwards any traffic to all of the ports. So, they are not smart devices.

**Server:**

Servers are an entirely different breed when compared to other end devices. They have various functionalities and also have space for two network interfaces. The modules available for servers are the same as PC modules, except that the servers do not have the PC-HOST-NM-1AM module.

**Meraki server:**

The Meraki cloud solution is a centralized management service that allows users to manage all of their Meraki network devices via a single simple and secure platform. Users are able to deploy, monitor and configure their Meraki devices via the Meraki dashboard web interface or via APIs.

**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.

**Voip device:**

A VoIP phone or IP phone uses voice over IP technologies for placing and transmitting telephone calls over an IP network, such as the Internet, instead of the traditional public switched telephone network (PSTN).

**Copper straight through wire:**

This is a standard Ethernet cable that is used to connect two devices that operate in different layers of the OSI model (such as hub to router and switch to PC). It can be used with Ethernet, Fast Ethernet and Gigabit Ethernet port types.

**Copper cross over wire:**

This Ethernet cable connects devices operating in the same OSI layer (such as hub to hub, PC to PC, PC to router, and PC to printer). This cable can also be used with Ethernet, Fast Ethernet and Gigabit Ethernet ports .

**Phone:-**

The mobile phone network enables wireless communication using mobile devices, such as mobile phones, smartphones or tablets. Mobile phone networks provide the necessary infrastructure and are operated by mobile phone providers.

**Automatically choose connection wire:**

Connections can be made automatically by choosing the connection type shown below. Router links will be red or not active until you correctly configure the interfaces.

**Coaxial wire:**

The coaxial cable used to connect the Cisco uBR7200 series universal broadband routers at the headend should be very high-quality cable because imperfections that do not visibly affect video transmissions can significantly affect digital data transmissions.

**Sniffer:**

I have assignment that i need to create full "Network", using all device like switch, hub, server ..etc.The problem that i force that i need to use "Sniffer" its first time to me using that device. I need help on how to configure or connect the Sniffer with my network.

**Smart device:**

A smart device is an electronic device, generally connected to other devices or networks via different wireless protocols such as Bluetooth, Zigbee, NFC, Wi-Fi, LiFi, 5G, etc., that can operate to some extent interactively and autonomously.

**Mcu-pt board:**

Components are physical objects that connect to microcontrollers (MCU-PT) or single boarded computers (SBC-PT). They typically do not have a network interface and rely on the MCU-PT or SBC-PT for network access. These are simple devices that only communicate through their analog or digital slots.

**Web server in Cisco packet trace :-**

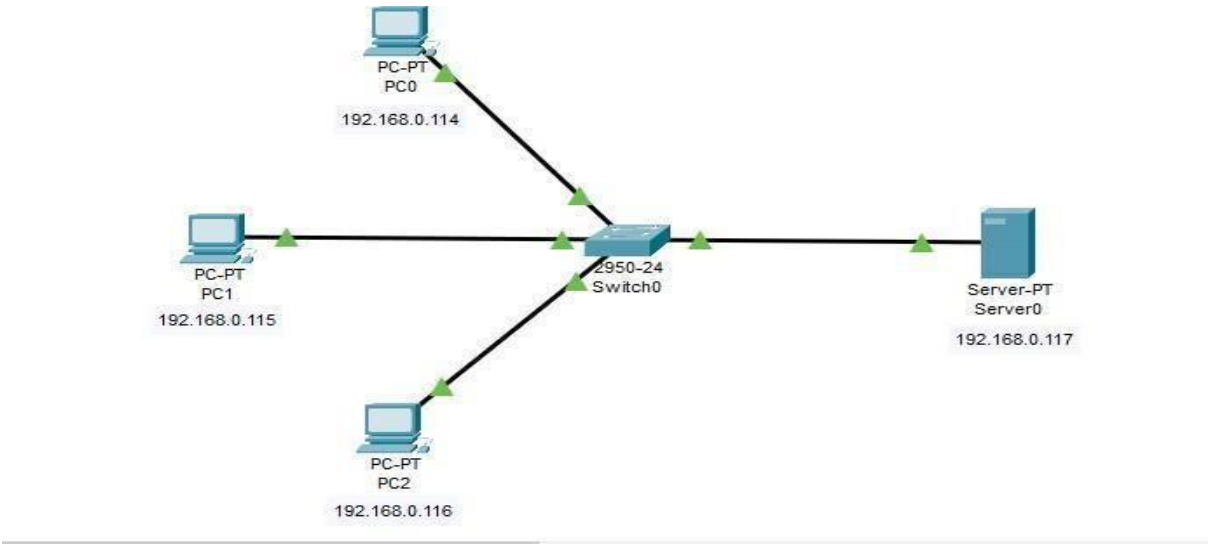



**Figure 3.1**

• In this lesson we will learn about how to create the first web server on cisco packet tracer that can be applied on a real time web server.

• So we are taking a few PCs and one web server and one switch for connecting all devices. Make sure all devices should be connected by straight through cable because for connecting different devices, straight through cable is required. Assign IPs to each end device (server and PCs) of a single network with subnet mask It can different as per your choice.

• Then go to server>services>http in that enable http and https modes.In that go to index.html and edit. In that write the message you want… At the end click on save.and close it .

• Then we go to PC1 and in that we select the desktop and we write the IP address of the server and click on enter. You can see the message which you wrote in the server message.

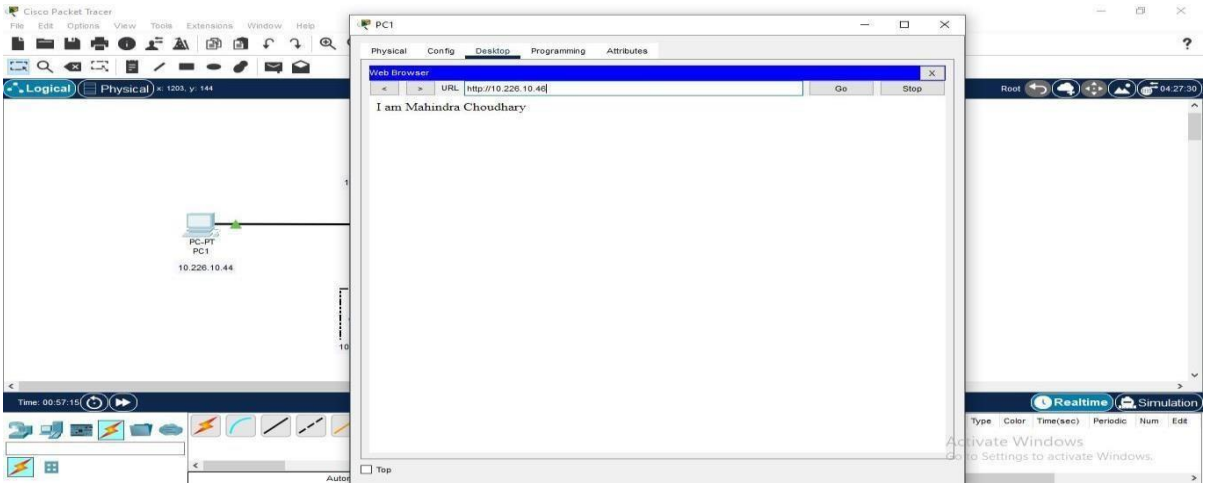



**Figure 3.2**

• If you want to see that your connection is proper or not then you want to click on your pc then desktop>command prompt and in that you need to write ping 190.0.0.1(IT_address). And enter.

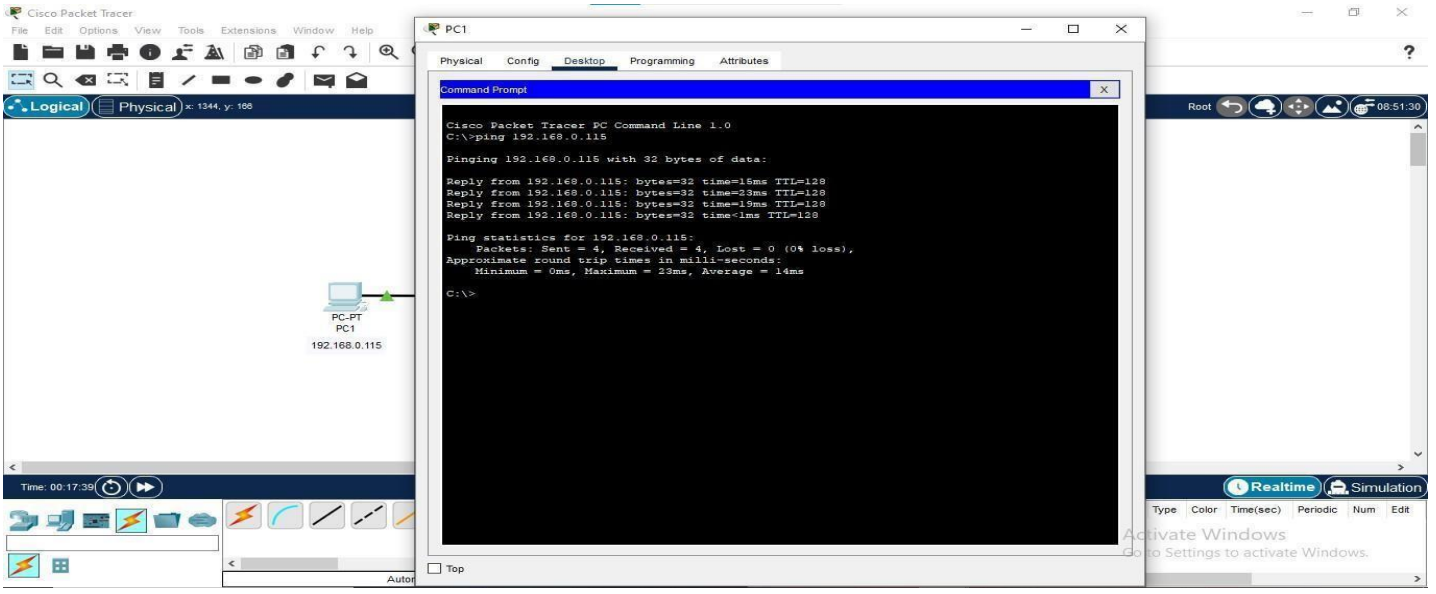



**Figure 3.3**

**Use of switch :-**

A switch is used in a wired network to connect to other devices using Ethernet cables. The switch allows each connected device to talk to the others. Wireless-only networks do not use switches because devices such as wireless routers and adapters communicate directly with one another.

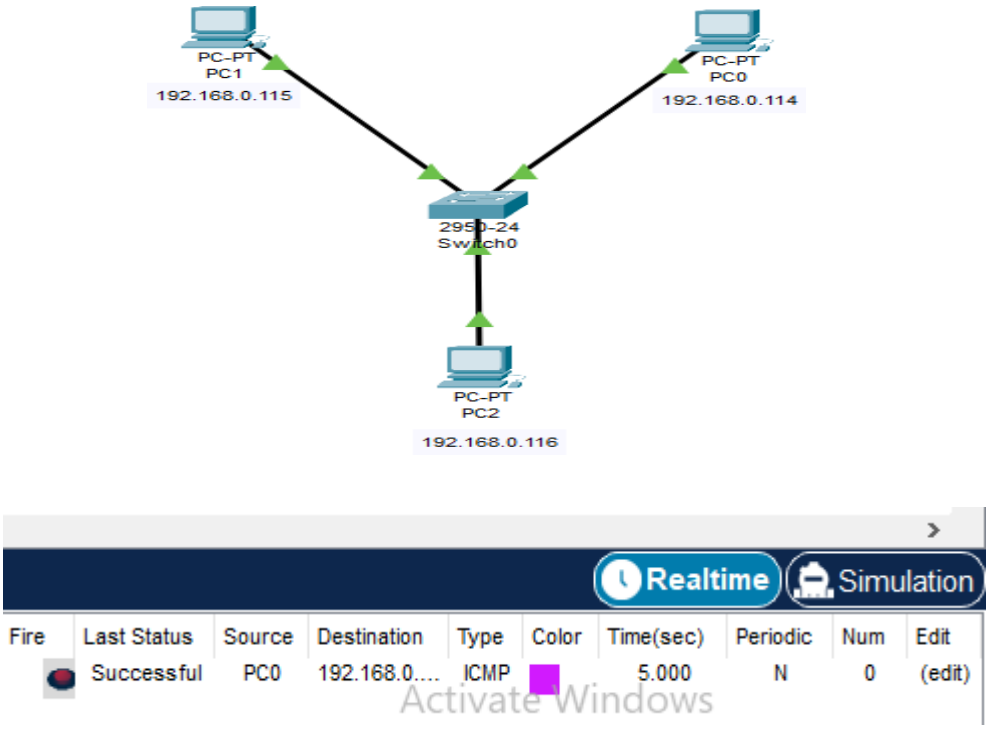



**Figure 3.4**

• Connect multiple hosts: Normally, a switch provides a large number of ports for cable connections, allowing for star topology routing. It is usually used to connect multiple PCs to the network.

• Forwards a message to a specific host: Like a bridge, a switch uses the same forwarding or filtering logic on each port. When any host on the network or a switch sends a message to another host on the same network or the

• ame switch, the switch receives and decodes the frames to read the physical (MAC) address portion of the message.

• Manage traffic: A switch in networking can manage traffic either coming into or exiting the network and can connect devices like computers and access points with ease.

• Keep electrical signal undistorted: When a switch forwards a frame, it regenerates an undistorted square electrical signal.

• Increase LAN bandwidth: A switch divides a LAN into multiple collision domains with independent broadband, thus greatly increasing the bandwidth of the LAN.

**Use of 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.

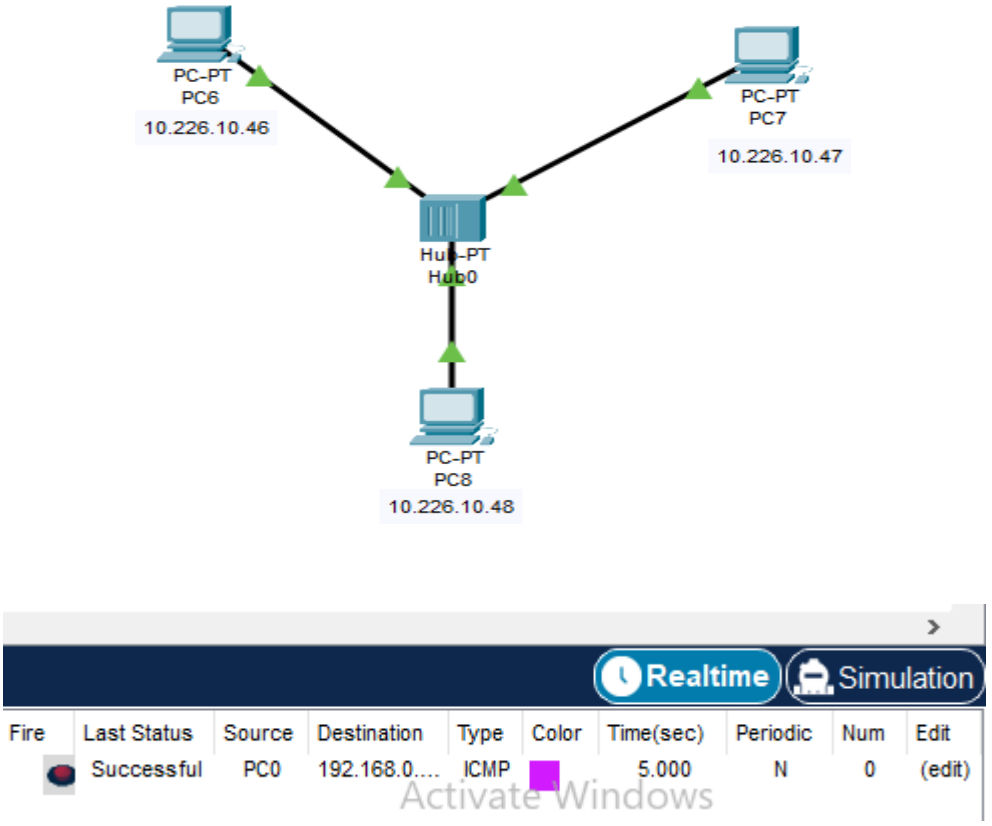



**Figure 3.5**

A hub has many ports in it. A computer which intends to be connected to the network is plugged into one of these ports. When a data frame arrives at a port, it is broadcast to every other port, without considering whether it is destined for a particular destination or not.

When a Hub receives data from one of the connected devices, it passes data to all the other ports without checking for the destination device except the port through which it receives the data. Below figure, shows the working of a HUB.


**Figure 3.6**

Consider, Device A wants to send data to device D. When device A sends data, the hub receives it through one port and transfers the data to all the other connected devices instead of passing it to only device D. This feature of the hub leads to congestion and extends the collision domain. So, it is considered as an inefficient device and needs more bandwidth for working.

**Difference between switch and hub :-**

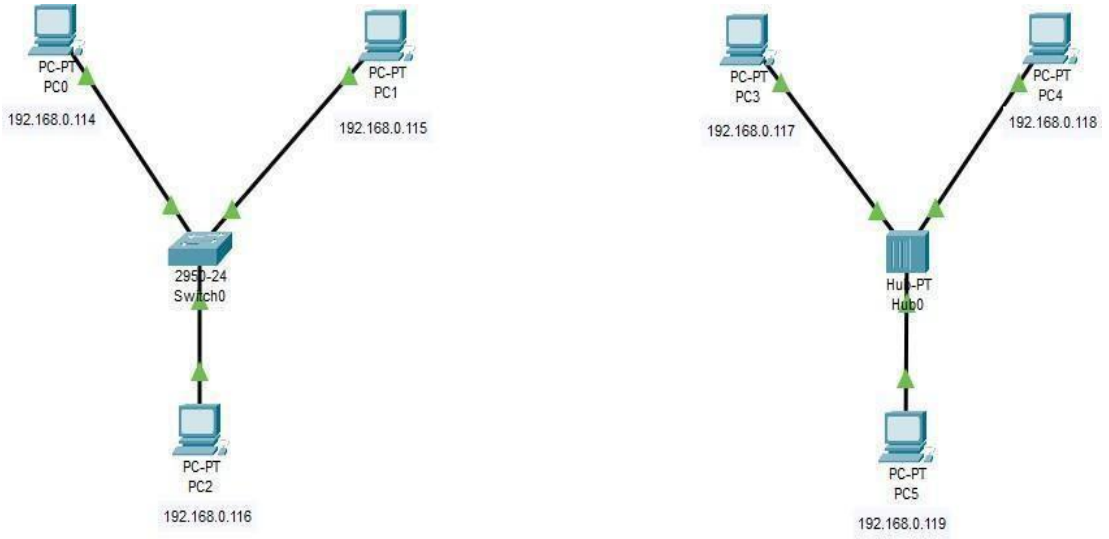



**Figure 3.7**

| HUB | SWITCH |
|---|---|
| • A hub operates on the physical layer. | • A switch operates on the data link layer. |
| • Hubs perform frame flooding that can be unicast, multicast, or broadcast. | • It performs broadcast, then the unicast and multicast as needed. |
| • Just a singular domain of collision is present in a hub. | • Varied ports have separate collision domains. |
| • Transmission mode is Half-duplex. | • Transmission mode is Full duplex. |
| • Hubs operates as a Layer 1 device per the OSI model. | • Network switches help you to operate at Layer 2 of the OSI model. |
| • To connect a network of personal computers should be joined through a central hub. | • Allow connecting multiple devices and ports. |
| • Uses electrical signal orbits. | • Uses frame & packet |
| • Does not offer Spanning-Tree. | • Multiple Spanning-Tree is possible |
| • Collisions occur mostly in setups using hubs. | • No collisions occur in a full-duplex switch. |
| • Hub is a passive device. | • A switch is an active device |
| • A network hub can't store MAC addresses. | • Switches use CAM (Content Accessible Memory) that can be accessed by ASIC (Application Specific Integrated Chips). |
| • Not an intelligent device. | • Intelligent device. |
| • Its speed is up to 10 Mbps. | • 10/100 Mbps, 1 Gbps, 10 Gbps |
| • Does not use software. | • Has software for administration. |

# Practical 4

**Aim :-** Data Link Layer (Error Detection).

The **Data Link Layer** is the second layer in the OSI (Open Systems Interconnection) model, positioned just above the Physical Layer. Its primary purpose is to provide reliable data transfer across a physical link by organizing data into frames, detecting and correcting errors, and controlling the flow of data.

## Key Functions of the Data Link Layer :-

1. **Framing :-**
   - Divides data from the Network Layer into manageable units called *frames* for transmission.
   - Adds a header and a trailer to the frame to provide necessary information for error detection and control.
2. **Error Detection and Correction :-**
   - Ensures that errors introduced during transmission (e.g., due to noise, interference) are identified and, if possible, corrected.
   - Common techniques include :-
     - **Parity Checking**: Adds a parity bit to detect single-bit errors.
     - **Cyclic Redundancy Check (CRC)**: Adds a checksum value derived from the data, which is verified at the receiver.
     - **Checksums**: A simpler error-checking method based on the summation of data segments.
3. **Flow Control :-**
   - Manages the rate of data transfer to ensure the receiver is not overwhelmed by data.
4. **Error Handling :-**
   - Retransmits corrupted frames when errors are detected, using techniques like Automatic Repeat Request (ARQ).
5. **Addressing :-**
   - Incorporates physical addresses (MAC addresses) to identify devices on the same local network.
6. **Medium Access Control (MAC) :-**
   - Coordinates access to the physical transmission medium to avoid collisions.

**Error Detection:**

Error detection is a crucial aspect of the Data Link Layer. It ensures the integrity of data during transmission. When data is sent over a network, it is susceptible to corruption caused by electrical noise, interference, or hardware issues. Error detection techniques help identify these corruptions.

Errors in data transmission can occur in various forms, depending on how bits are altered during transit. The main types are **single-bit error** and **burst-bit error**:

**1. Single-Bit Error :-**

- **Definition:** Only one bit in a data unit (e.g., a frame or packet) is altered during transmission.
- **Causes:** Typically occurs due to a brief noise spike or electrical interference.

**Detection and Correction :-**

- Simple error detection methods like **parity checks** are sufficient to detect single-bit errors. Correction may require retransmission.

**2. Burst-Bit Error:**

- **Definition:** Two or more consecutive bits in a data unit are altered during transmission.
- **Causes:** Commonly caused by interference lasting over multiple clock cycles, such as electrical surges or cross-talk.

**Detection and Correction:**

- Techniques like **CRC** or **interleaving** are effective in detecting burst errors.
- Correcting burst errors can be challenging without retransmission.

**Common Techniques for Error Detection:**

1. **Parity Bit:**

    - Adds an extra bit to the data to make the number of 1s either even (even parity) or odd (odd parity).
    - Simple and fast but can detect only single-bit errors.

2. **Checksum:**
    - Divides data into segments, sums them, and appends the sum (checksum) to the data.
    - The receiver recalculates the sum to detect mismatches.
3. **Cyclic Redundancy Check (CRC):**
    - Uses polynomial division to calculate a checksum based on the data.
    - Extremely robust and widely used in network protocols like Ethernet.
4. **Hamming Code:**
    - Adds redundancy bits to data, allowing the detection and correction of single-bit errors and detection of double-bit errors.
5. **Frame Check Sequence (FCS):**
    - A field in the frame's trailer containing a value calculated from the frame's contents (e.g., using CRC).

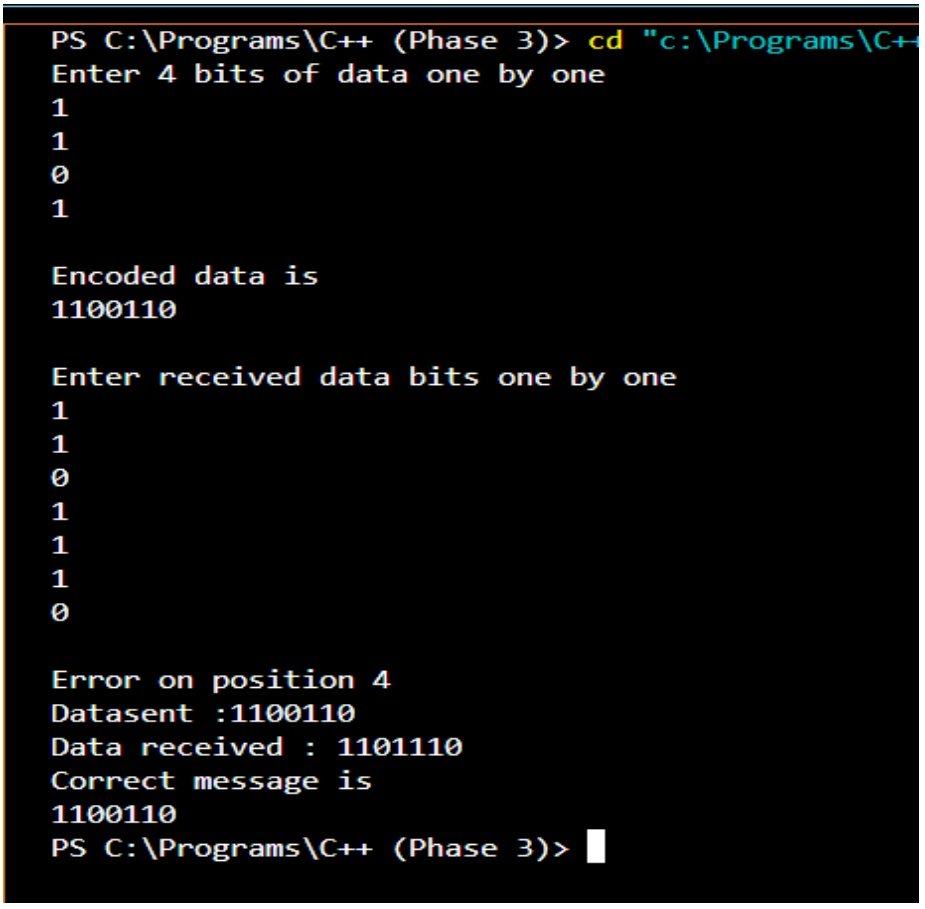
**Source Code :-**

```
#include<stdio.h>

void main(){

int data[10];

int dataatrec[10],c,c1,c2,c3,i;

printf("Enter 4 bits of data one by one\n");

scanf("%d",&data[0]);

scanf("%d",&data[1]);

scanf("%d",&data[2]);

scanf("%d",&data[4]);

//Calculation of even parity

data[6]=data[0]^data[2]^data[4];

data[5]=data[0]^data[1]^data[4];

data[3]=data[0]^data[1]^data[2];
```

```
printf("\nEncoded data is\n");
for(i=0;i<7;i++)
printf("%d",data[i]);
printf("\n\nEnter received data bits one by one\n");
for(i=0;i<7;i++)
scanf("%d",&dataatrec[i]);
c1=dataatrec[6]^dataatrec[4]^dataatrec[2]^dataatrec[0]
;
c2=dataatrec[5]^dataatrec[4]^dataatrec[1]^dataatrec[0]
;
c3=dataatrec[3]^dataatrec[2]^dataatrec[1]^dataatrec[0]
; c=c3*4+c2*2+c1 ;
if(c==0) {
printf("\nNo error while transmission of data\n");
}
else {
printf("\nError on position
%d",c); printf("\nDatasent :");
for(i=0;i<7;i++)
printf("%d",data[i]);
printf("\nData received : ");
for(i=0;i<7;i++)
printf("%d",dataatrec[i]);
printf("\nCorrect message is\n");
//if errorneous bit is 0 we complement it else vice versa
if(dataatrec[7-c]==0)
```

```
dataatrec[7-c]=1;

else

dataatrec[7-c]=0;

for (i=0;i<7;i++) {

printf("%d",dataatrec[i]);

}

}

}
```

**Output :-**



# Practical 5

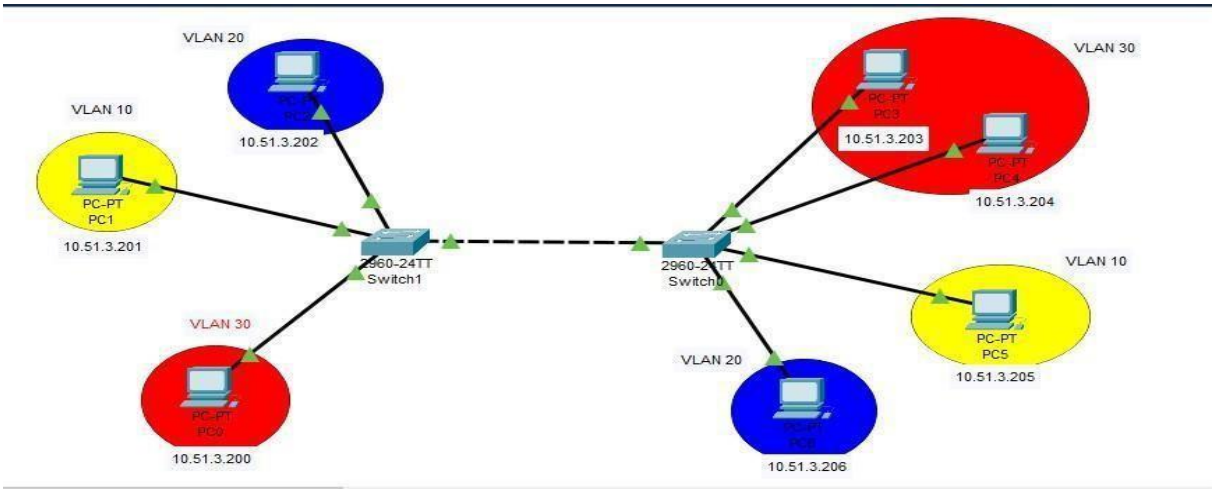
**Aim :- Virtual LAN :** Simulate Virtual LAN Configuration using cisco packet tracer Tracer Simulation

**DESCRIPTION -**

STEP 1: Make a network

• Connect the pcs and switches shown in the below figure.Give IP address.

• Connect pcs to switches with copper straight through and connect switches to one another with copper cross over.




STEP 2: Configure VLAN on all switches.

• Go to switch0 CLI, enter ENA command to enable switch.

Physical Config CLI Attributes

IOS

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state to up
Switch>en
Translating "Switch>en"...domain server (255.255.255.255)
% Unknown command or computer name, or unable to find computer address

Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#name blue
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name yellow
Switch(config-vlan)#exit
Switch(config)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#show vlan brief
```

Write the following. commands conf t>vlan 10> name yellow>exit as shown below.

• Do the same for second Vlan 20 and name it orange.

• Repeat the process for switch1.

To see the vlan the command used is >show vlan brief. The output of the command is below,

```
Switch#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
10   blue                             active
20   yellow                           active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
Switch#
Switch#
```

STEP 3: Configure TRUNK MODE.

• To enable trunk mode the first go to switch CLI

• The command ena>conf t>interface fa0/7>switchport mode trunk.

• This is to be done for every switches ports.

• The below figure shows the command.

```
Switch>ena
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface fa0/6
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
Switch(config)#interface fa0/5
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
Switch(config)#
```

STEP 4: Configure ACCESS MODE.

• ACCESS MODE is configured for all the pcs who are connect to the switch

• To configure access mode for pc command ena>conf t>interface fa0/1>switchport mode access>switchport access vlan10>exit.

```
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#ena
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface fa0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console
```

This is to be done with each pc connected to the switch.

Communication in same and different vlans with two switches.