Practical 1

Aim: To study about CISCO PACKET TRACER and design various network topologies using the tool.

Cisco Packet Tracer as the name suggests, is a tool built by Cisco. This tool provides a network simulation to practice simple and complex networks.

The main purpose of Cisco Packet Tracer is to help students learn the principles of networking with hands-on experience as well as develop Cisco technology specific skills. Since the protocols are implemented in software only method, this tool cannot replace the hardware Routers or Switches. Interestingly, this tool does not only include Cisco products but also many more networking devices.

Using this tool is widely encouraged as it is part of the curriculum like CCNA, CCENT where Faculties use Packet Trace to demonstrate technical concepts and networking systems. Student complete assignments using this tool, working on their own or in teams.

Workspace:

1. **Logical:**

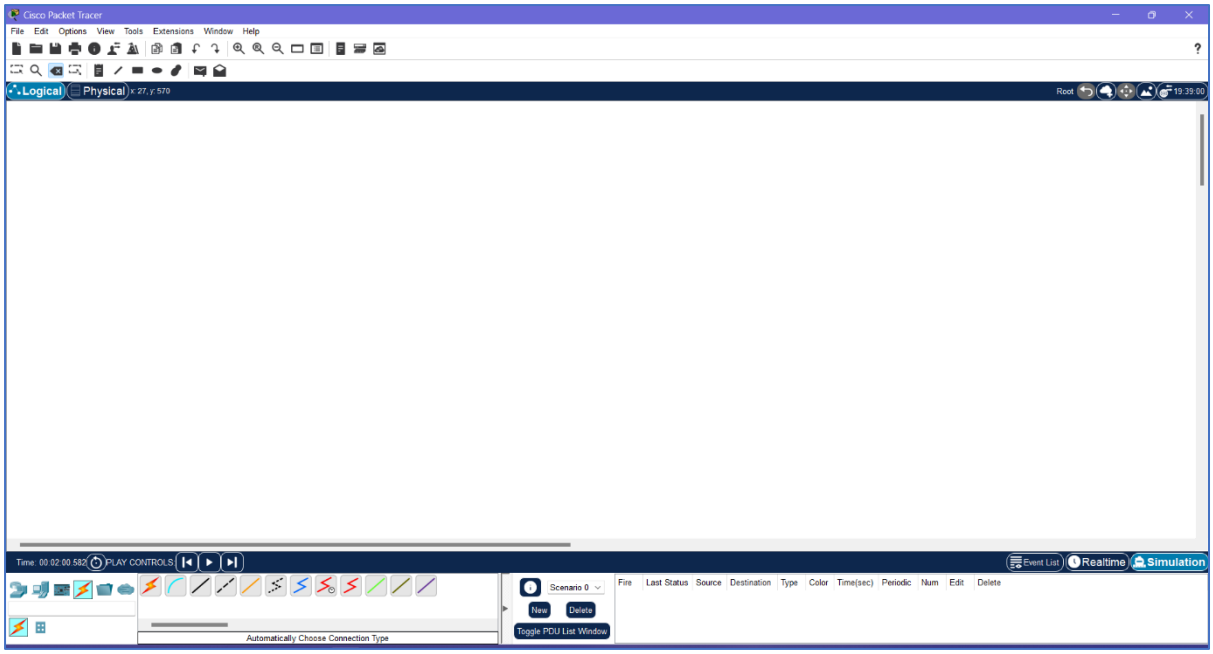
Logical workspace shows the logical network topology of the network the user has built. It represents the placing, connecting and clustering virtual network devices.

2. **Physical:**

Physical workspace shows the graphical physical dimension of the logical network. It depicts the scale and placement in how network devices such as routers, switches and hosts would look in a real environment. It also provides geographical representation of networks, including multiple buildings, cities and wiring closets.

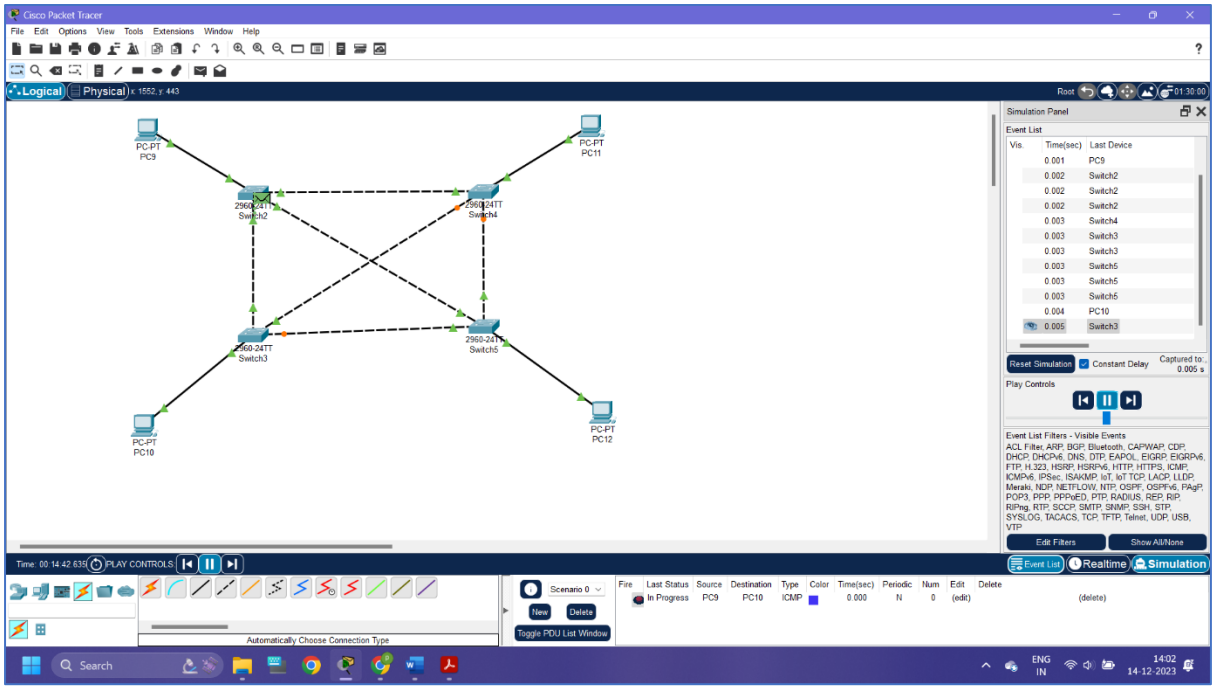
Key Features:

- Unlimited devices
- E-learning
- Customize single/multi user activities
- Interactive Environment
- Visualizing Networks
- Real-time mode and Simulation mode
- Self-paced
- Supports majority of networking protocols
- International language support
- Cross platform compatibility

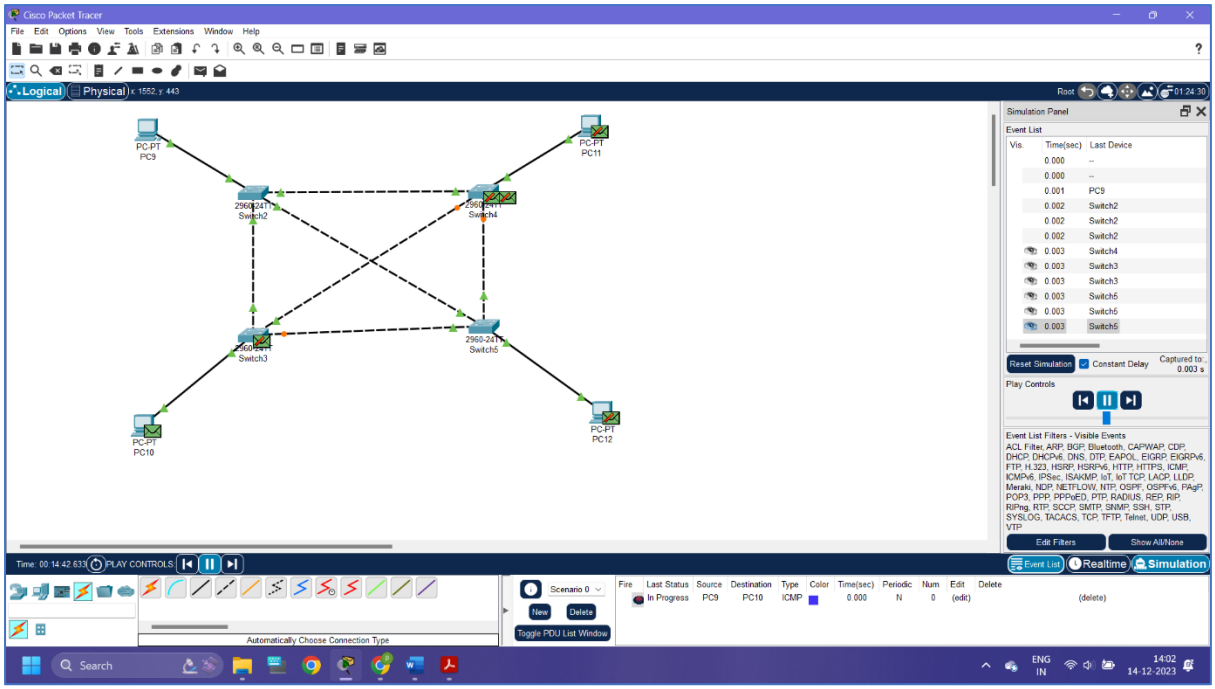


Initial Screen of CISCO PACKET TRACER

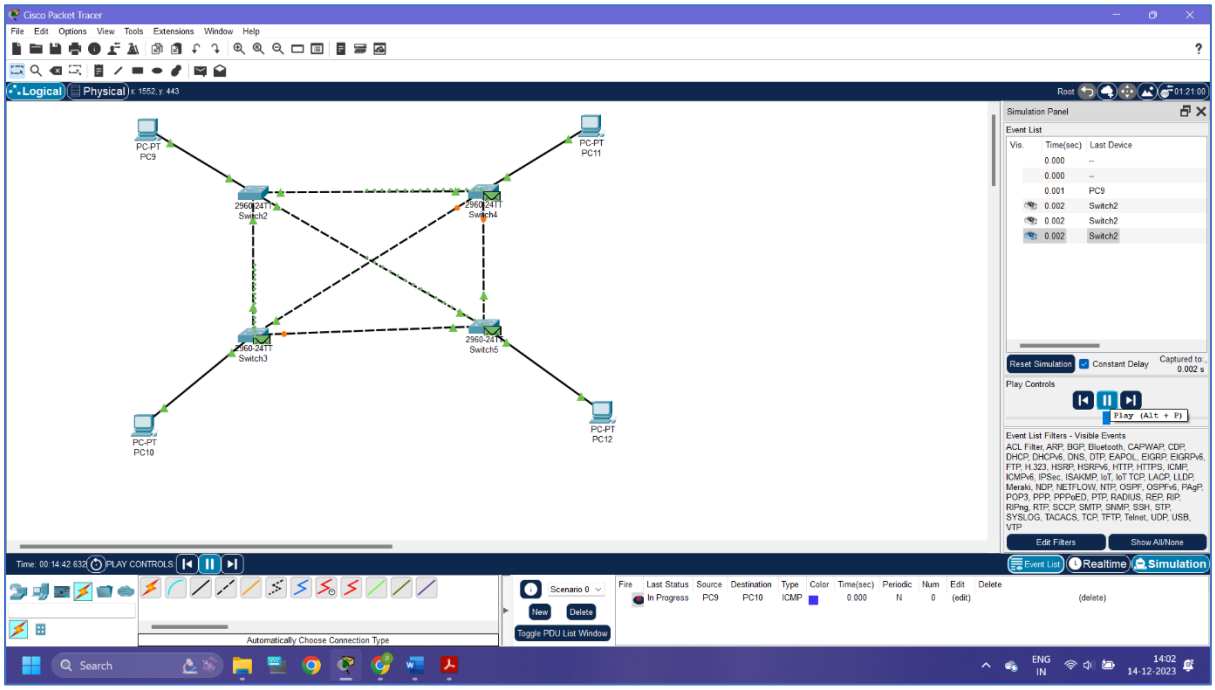
Designing the network topologies using the tool:



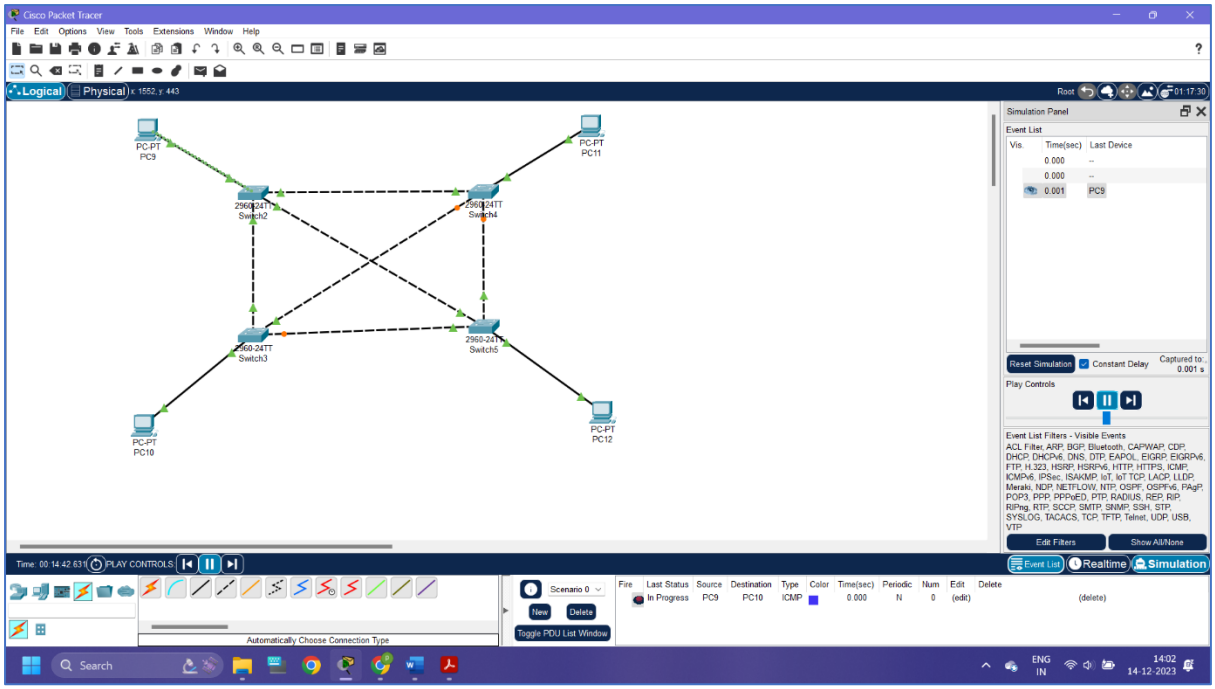
Mesh Topology



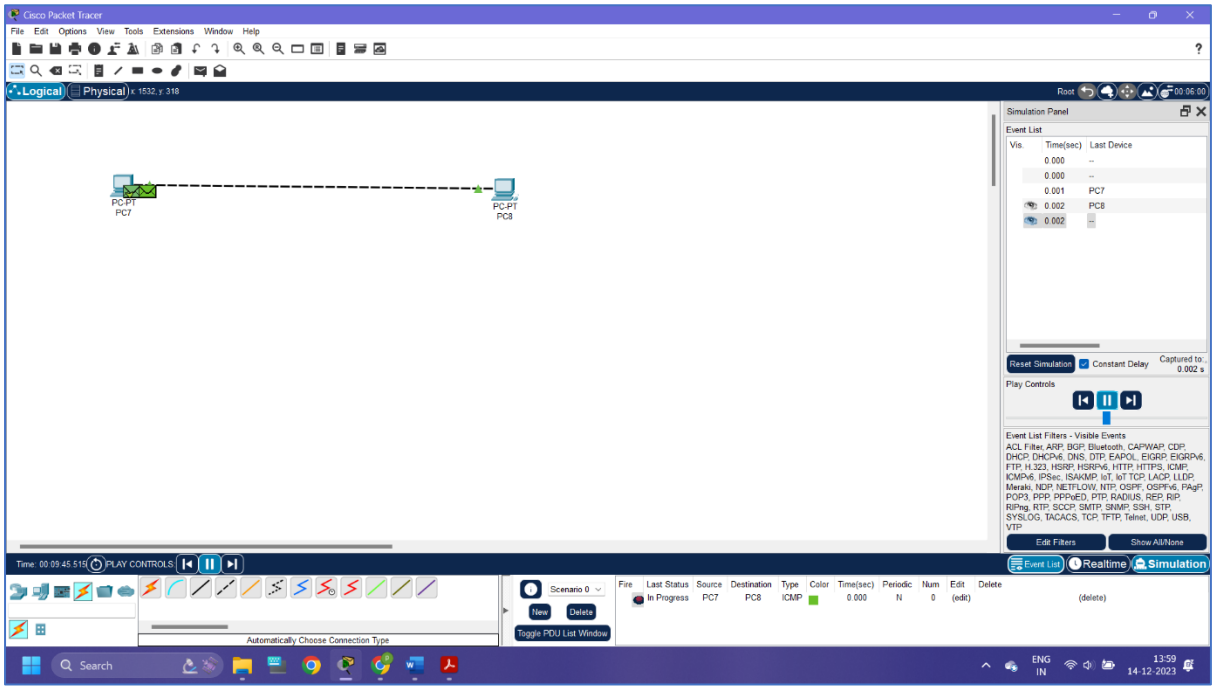
Mesh Topology



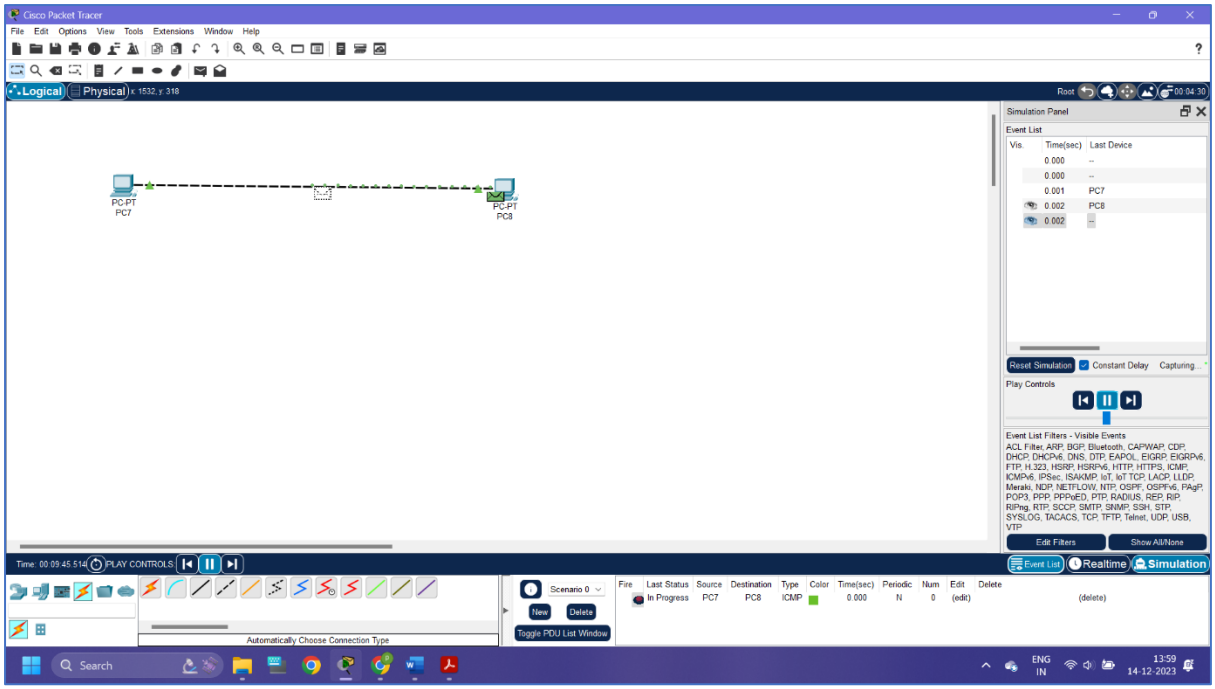
Mesh Topology



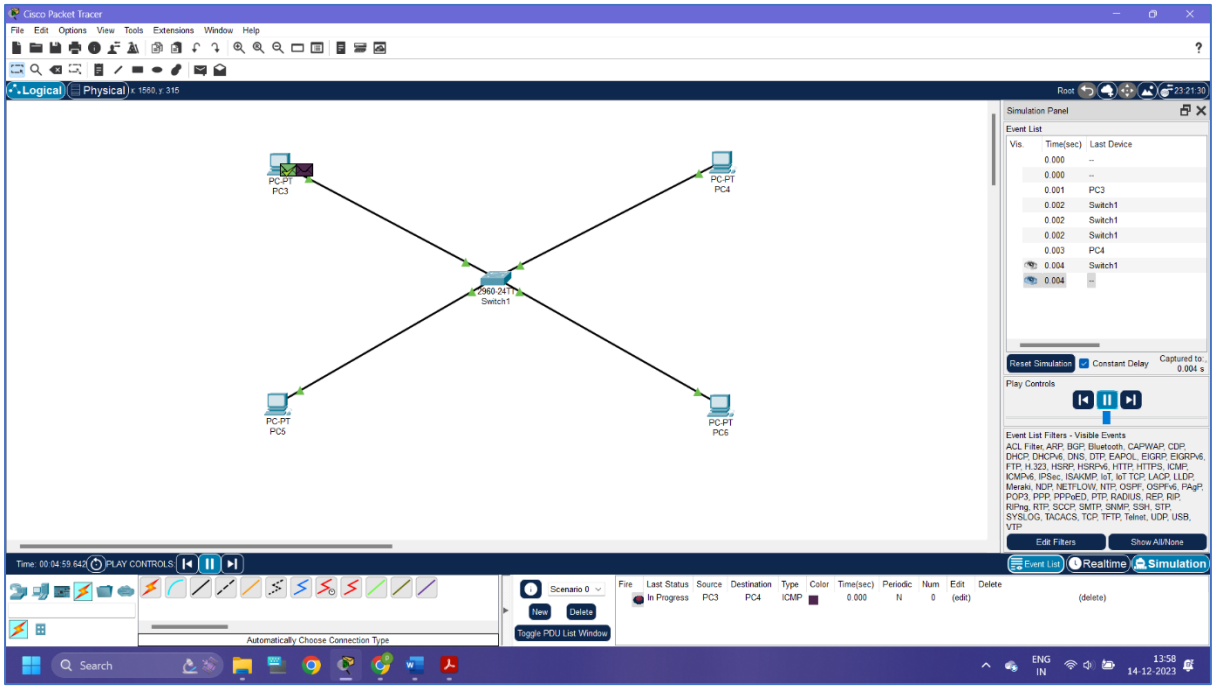
Mesh Topology



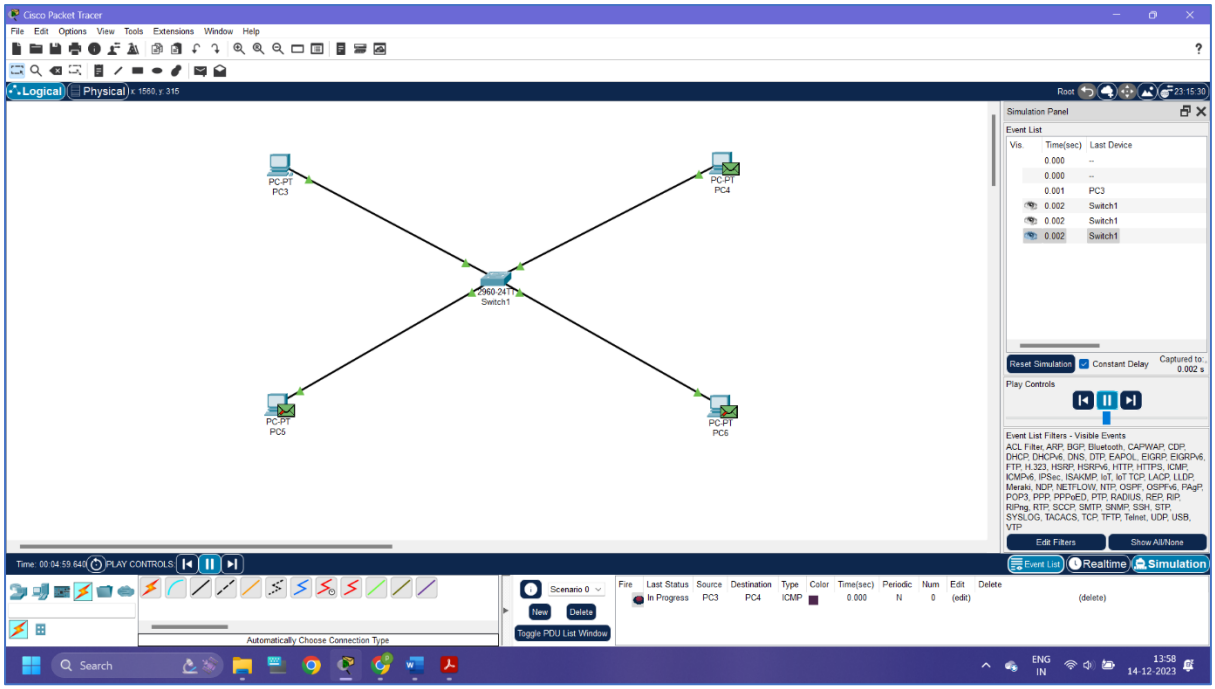
Communication between two computers



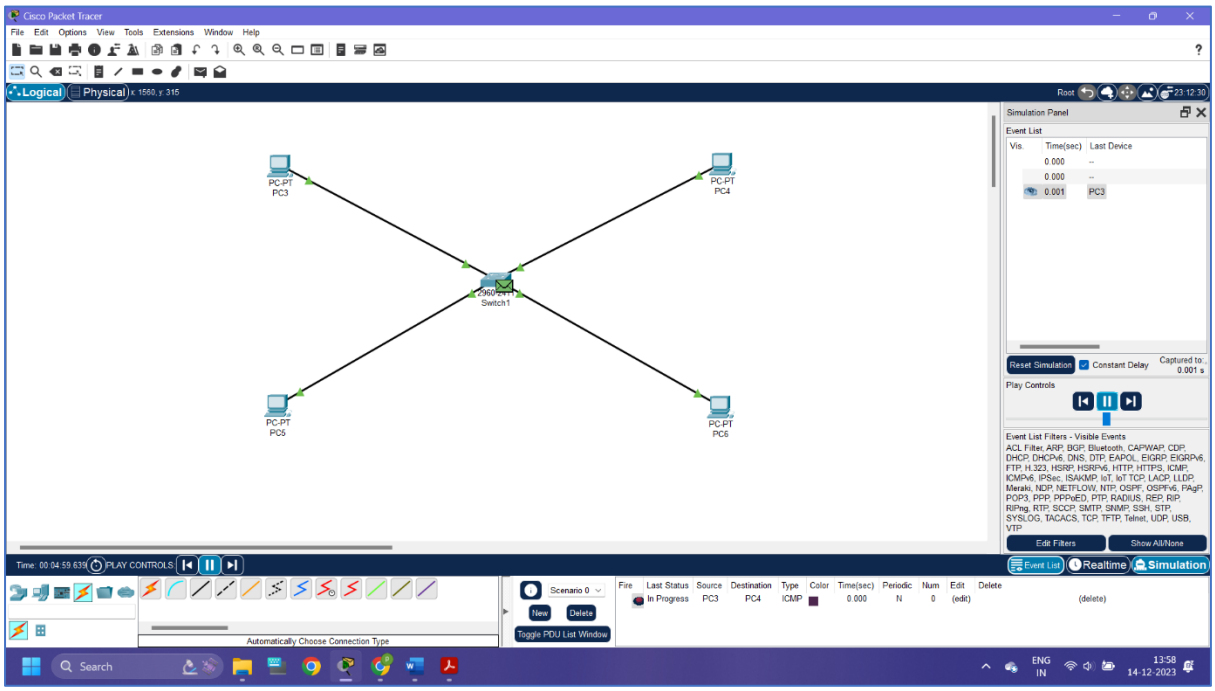
Communication between two computers



Star Topology



Star Topology



Star Topology

Practical 2

Aim: To study about WIRESHARK tool and demonstrate working of network packet analyzer using the tool.

Wireshark is a software tool used to monitor the network traffic through a network interface. It is the most widely used network monitoring tool today. Wireshark is loved equally by system administrators, network engineers, network enthusiasts, network security professionals and black hat hackers.

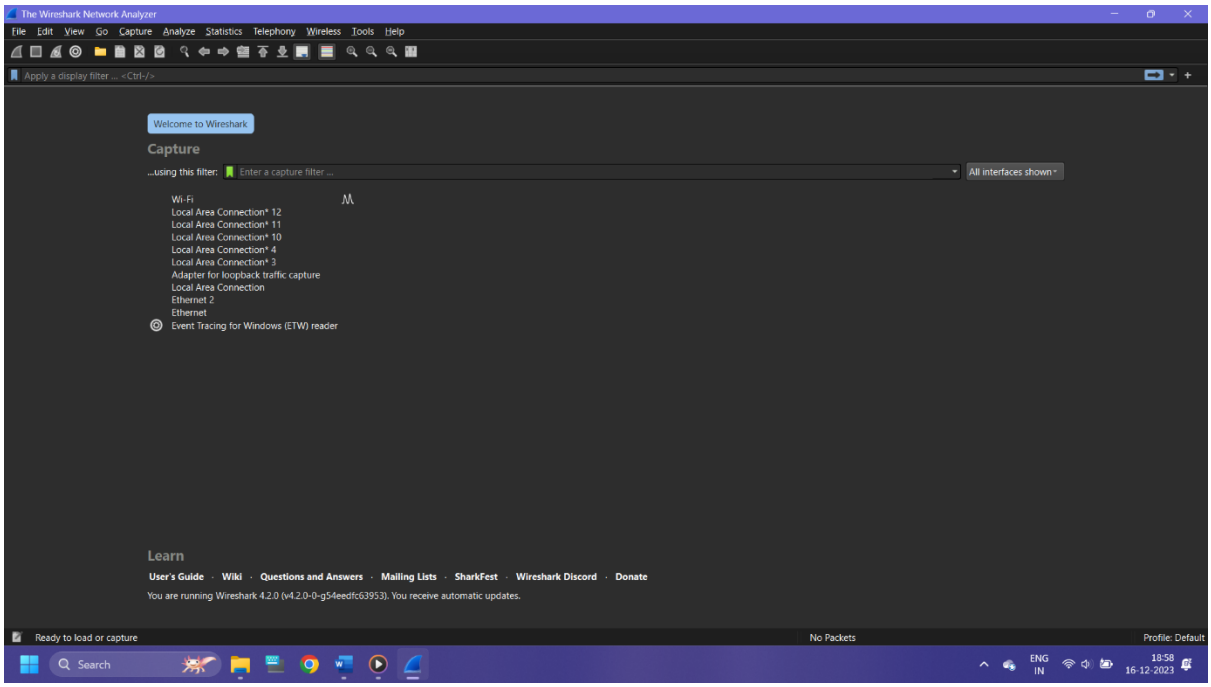
The extent of its popularity is such, that experience with Wireshark is considered as a valuable/essential trait in a computer networking-related professional.

There are many reasons why Wireshark is so popular:

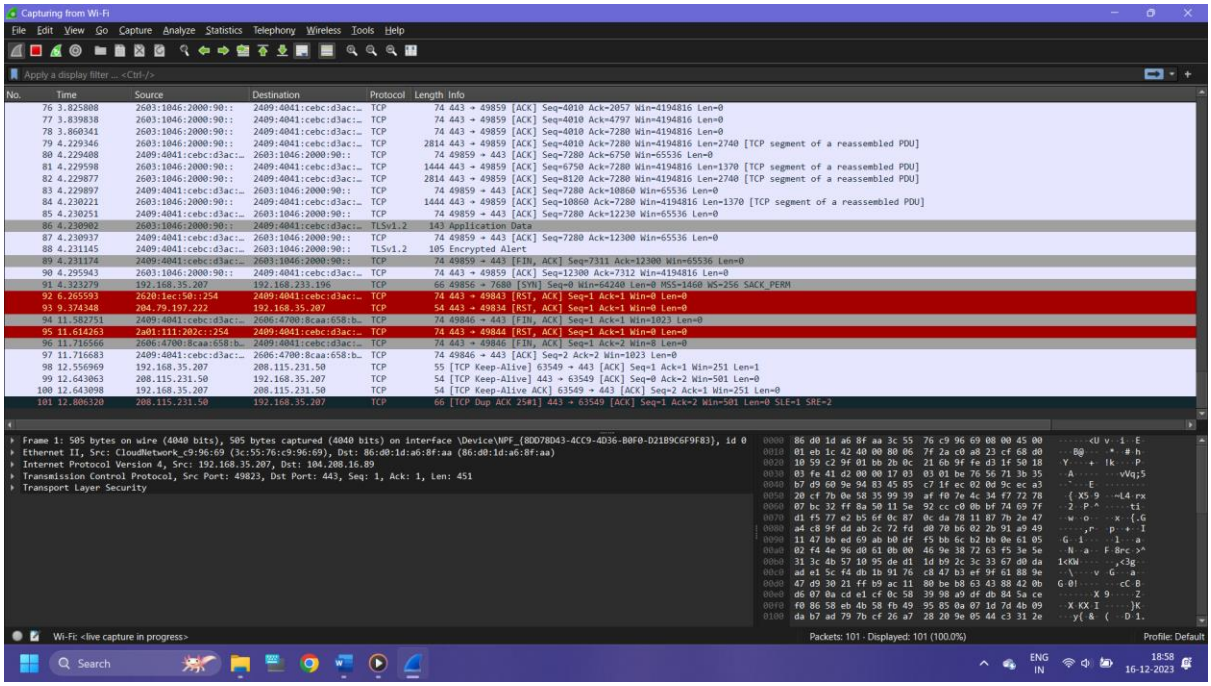
1. It has a great GUI as well as a conventional CLI (T Shark).
2. It offers network monitoring on almost all types of network standards (Ethernet, Wireless LAN, Bluetooth etc)
3. It is open-source with a large community of backers and developers.
4. All the necessary components for monitoring, analyzing and documenting the network traffic are present. It is free to use.

History of Wireshark:

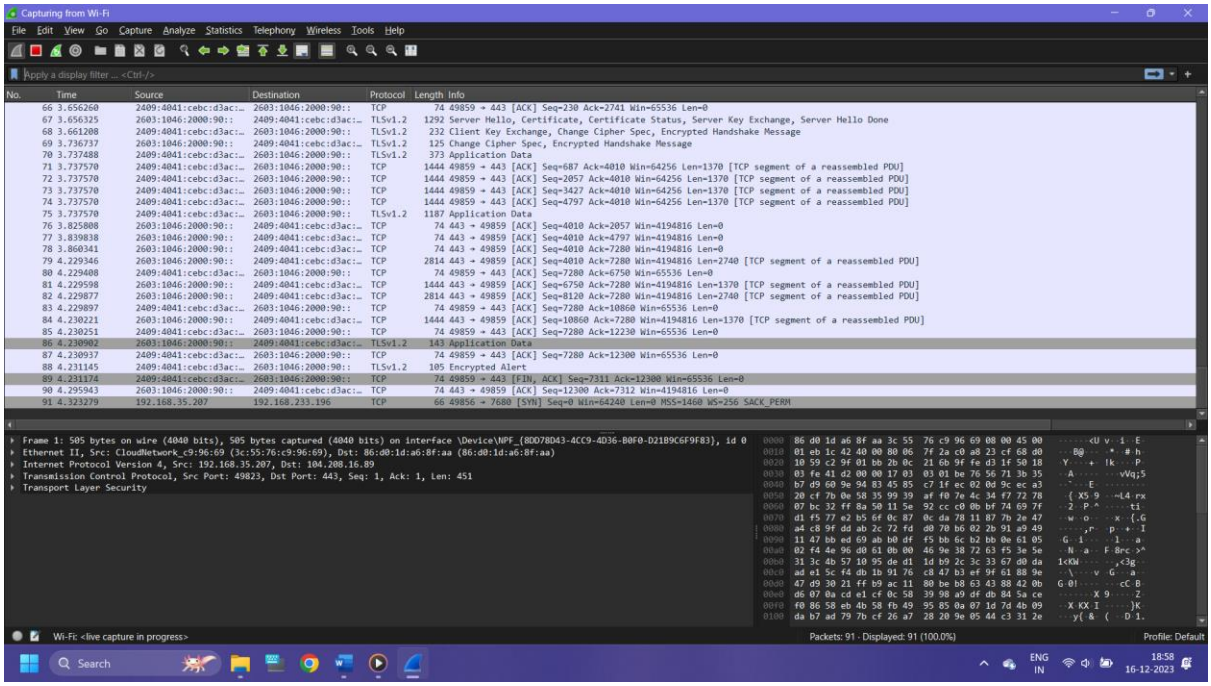
Wireshark was started with the intention of developing a tool for closely analyzing network packets. It was started by Gerald Combez in 1997. Its initial name was Ethereal. It was initially released in July 1998 as version 0.2.0. Due to the support, it got from the developer community, it grew rapidly and was released as version 1.0 in 2008, almost two years after it was renamed to Wireshark.



Starting Screen of Wireshark Tool



Network Analysis for Wi-Fi – 1



Network Analysis for Wi-Fi - 2

Practical 3

Aim: To study behavior of generic devices used for networking in CISCO PACKET TRACER.

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

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 to extend the length to which the signal can be transmitted over the same network. An important point to be noted about repeaters is that they not only amplify the signal but also regenerate it. When the signal becomes weak, they copy it bit by bit and regenerate it at its star topology connectors connecting following the original strength. It is a 2-port device.

Repeater

Hub:

A hub is a basically multi-port repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Hubs cannot filter data, so data packets are sent to all connected devices. In other words, the collision domain of all hosts connected through Hub remains one. Also, they do not have the intelligence to find out the best path for data packets which leads to inefficiencies and wastage.

Types of Hubs:

1. Active Hub: These are the hubs that have their power supply and can clean, boost, and relay the signal along with the network. It serves both as a repeater as well as a wiring centre. These are used to extend the maximum distance between nodes.
2. Passive Hub: These are the hubs that collect wiring from nodes and power supply from the active hub. These hubs relay signals onto the network without cleaning and boosting them and can't be used to extend the distance between nodes.

3. Intelligent Hub: It works like an active hub and includes remote management capabilities. They also provide flexible data rates to network devices. It also enables an administrator to monitor the traffic passing through the hub and to configure each port in the hub.

USB Hub

Bridge:

A bridge operates at the data link layer. A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of the source and destination. It is also used for interconnecting two LANs working on the same protocol. It has a single input and single output port, thus making it a 2-port device.

Types of Bridges

1. Transparent Bridges: These are the bridge in which the stations are completely unaware of the bridge's existence i.e. whether or not a bridge is added or deleted from the network, reconfiguration of the stations is unnecessary. These bridges make use of two processes i.e. bridge forwarding and bridge learning.
2. Source Routing Bridges: In these bridges, routing operation is performed by the source station and the frame specifies which route to follow. The host can discover the frame by sending a special frame called the discovery frame, which spreads through the entire network using all possible paths to the destination.

Bridge

Switch:

A switch is a multiport bridge with a buffer and a design that can boost its efficiency (a large number of ports imply less traffic) and performance. A switch is a data link layer device. The switch can perform error checking before forwarding data, which makes it very efficient as it does not forward packets that have errors and forward good packets selectively to the correct

port only. In other words, the switch divides the collision domain of hosts, but the broadcast domain remains the same.

Types of Switches

1. Unmanaged switches: These switches have a simple plug-and-play design and do not offer advanced configuration options. They are suitable for small networks or for use as an expansion to a larger network.
2. Managed switches: These switches offer advanced configuration options such as VLANs, QoS, and link aggregation. They are suitable for larger, more complex networks and allow for centralized management.
3. Smart switches: These switches have features similar to managed switches but are typically easier to set up and manage. They are suitable for small- to medium-sized networks.
4. Layer 2 switches: These switches operate at the Data Link layer of the OSI model and are responsible for forwarding data between devices on the same network segment.
5. Layer 3 switches: These switches operate at the Network layer of the OSI model and can route data between different network segments. They are more advanced than Layer 2 switches and are often used in larger, more complex networks.
6. PoE switches: These switches have Power over Ethernet capabilities, which allows them to supply power to network devices over the same cable that carries data.
7. Gigabit switches: These switches support Gigabit Ethernet speeds, which are faster than traditional Ethernet speeds.
8. Rack-mounted switches: These switches are designed to be mounted in a server rack and are suitable for use in data centres or other large networks.
9. Desktop switches: These switches are designed for use on a desktop or in a small office environment and are typically smaller in size than rack-mounted switches.
10. Modular switches: These switches have modular design, which allows for easy expansion or customization. They are suitable for large networks and data centres.

Network Switch

Router:

A router is a device like a switch that routes data packets based on their IP addresses. The router is mainly a Network Layer device. Routers normally connect LANs and WANs and have a

dynamically updating routing table based on which they make decisions on routing the data packets. The router divides the broadcast domains of hosts connected through it.

Router

Gateway:

A gateway, as the name suggests, is a passage to connect two networks that may work upon different networking models. They work as messenger agents that take data from one system, interpret it, and transfer it to another system. Gateways are also called protocol converters and can operate at any network layer. Gateways are generally more complex than switches or routers. A gateway is also called a protocol converter.

Gateway

Practical 4

Aim: To implement Error Detection Algorithm at Data Link Layer.

Hamming Code Implementation using C Language:

```
#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]);

   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("\nData sent : ");
       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(dataatrec[7-c]==0) {dataatrec[7-c]=1;}
else {dataatrec[7-c]=0;}
for (i=0;i<7;i++)
{
          printf("%d",dataatrec[i]);
}
}
}
```

Output:

```c
#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 ;
```

```
/tmp/WPYi7JExfH.o
Enter 4 bits of data one by one
0
1
0
1
0
1
Encoded data is
0000111

Enter received data bits one by one
1
1
0
1
0
1
0
0
0
0
Error on position 2
Data sent : 0000111
Data received : 1010000
Correct message is
1010010_
```

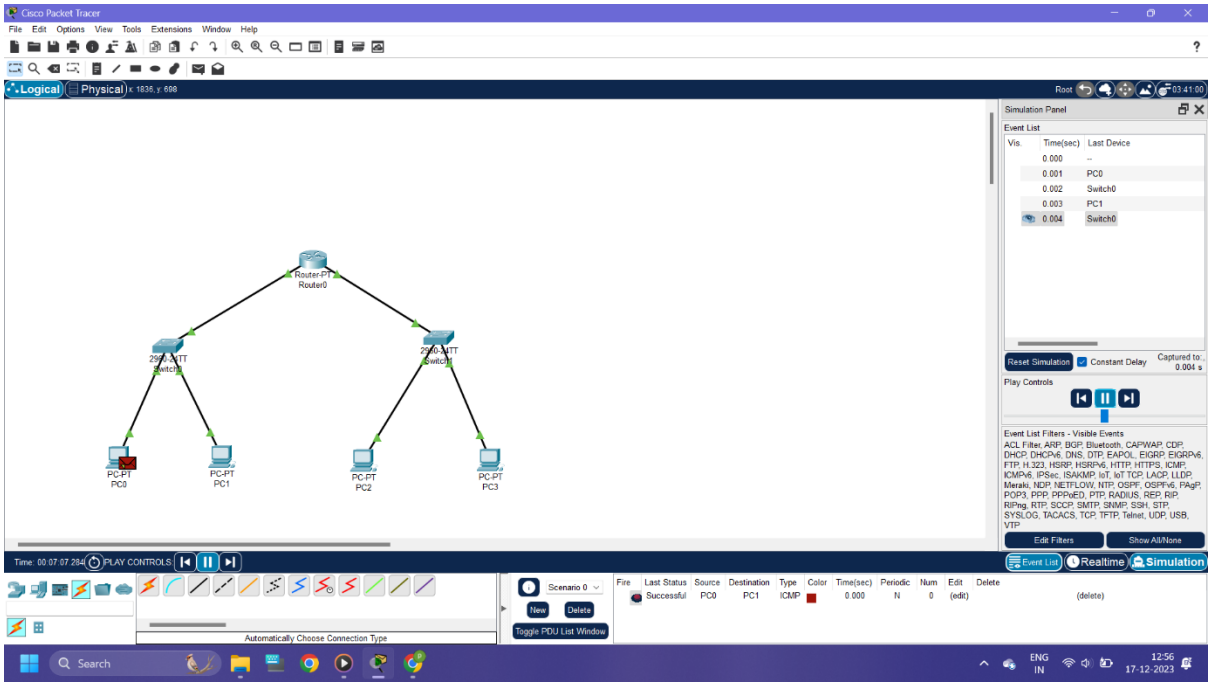
Practical 5

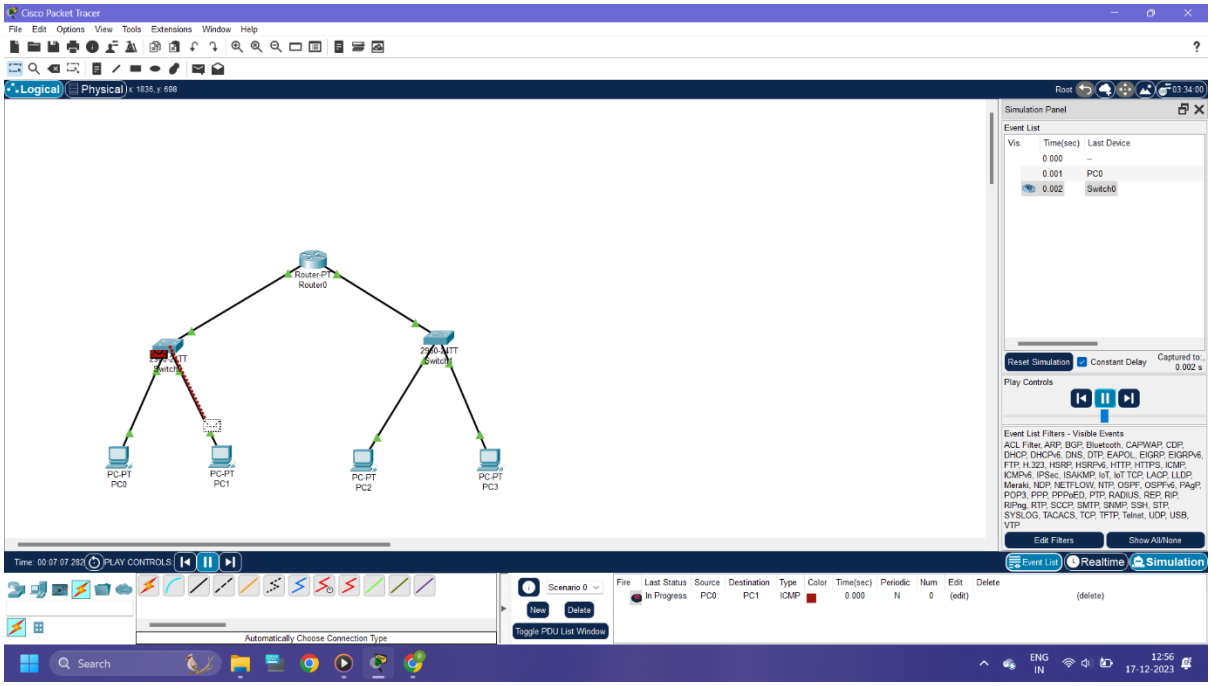
Aim: To implement VLAN.

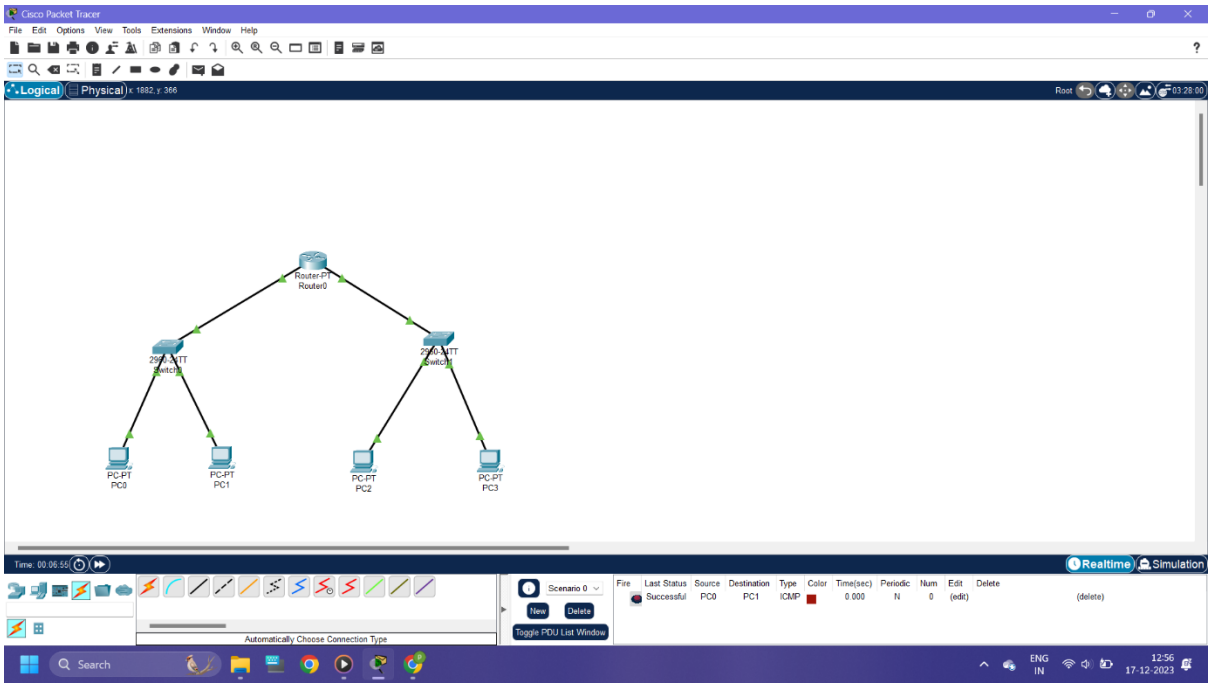
Virtual LAN (VLAN) is a concept in which we can divide the devices logically on layer 2 (data link layer). Generally, layer 3 devices divide the broadcast domain but the broadcast domain can be divided by switches using the concept of VLAN.

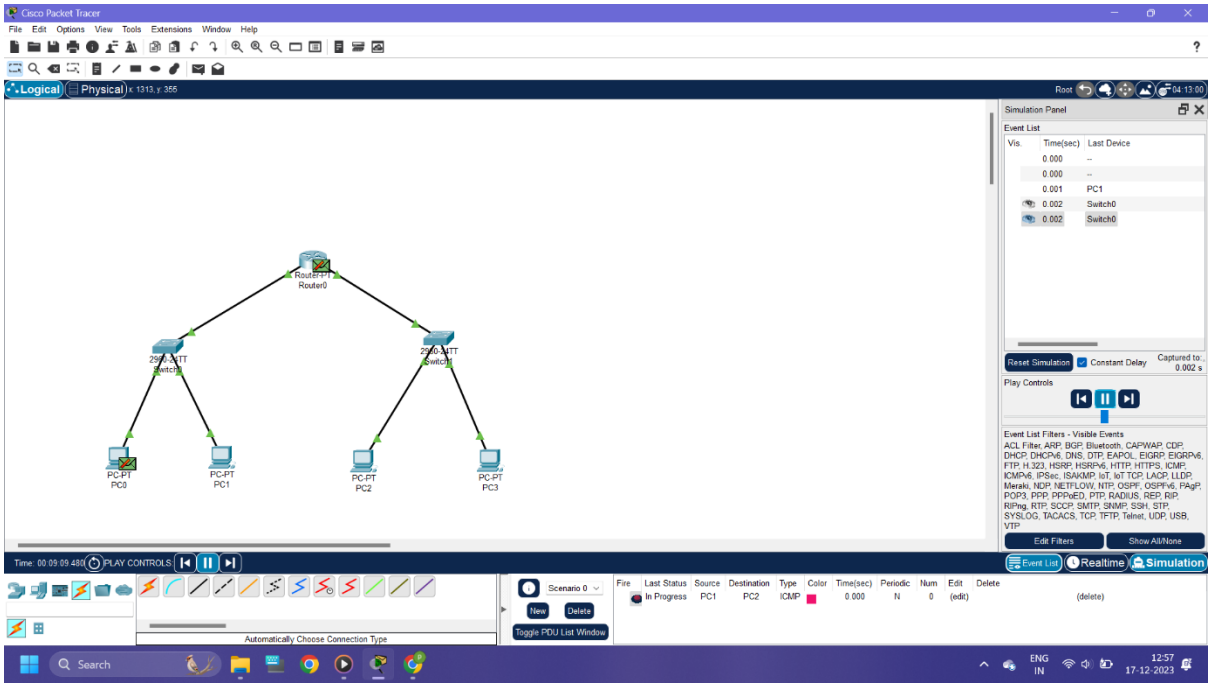
A broadcast domain is a network segment in which if a device broadcast a packet, then all the devices in the same broadcast domain will receive it. The devices in the same broadcast domain will receive all the broadcast packets but it is limited to switches only as routers don't forward out the broadcast packet. To forward out the packets to different VLAN (from one VLAN to another) or broadcast domains, inter VLAN routing is needed. Through VLAN, different small-size sub-networks are created which are comparatively easy to handle.

Implementation:




Cisco Packet Tracer
Router0
PC0
PC1
PC2
PC3
Simulation Panel
Event List
Reset Simulation
Constant Delay
Play Controls
Edit Filters
Show All/None
Realtime
Simulation
Automatically Choose Connection Type


Cisco Packet Tracer
Router0
PC0
PC1
PC2
PC3
Realtime
Simulation
Automatically Choose Connection Type



Advantages:

- Performance:

  The network traffic is full of broadcast and multicast. VLAN reduces the need to send such traffic to unnecessary destinations. e.g.-If the traffic is intended for 2 users but as 10 devices are present in the same broadcast domain, therefore, all will receive the traffic i.e. wastage of bandwidth but if we make VLANs, then the broadcast or multicast packet will go to the intended users only.

- Formation of virtual groups:

  As there are different departments in every organization namely sales, finance etc., VLANs can be very useful in order to group the devices logically according to their departments.

- Security:

  In the same network, sensitive data can be broadcast which can be accessed by the outsider but by creating VLAN, we can control broadcast domains, set up firewalls, restrict access. Also, VLANs can be used to inform the network manager of an intrusion. Hence, VLANs greatly enhance network security.

- Flexibility:
  VLAN provide flexibility to add, remove the number of hosts we want.
- Cost Reduction:
  VLANs can be used to create broadcast domains which eliminate the need for expensive routers. By using VLAN, the number of small size broadcast domain can be increased which are easy to handle as compared to a bigger broadcast domain.

Disadvantages:

1. Complexity: VLANs can be complex to configure and manage, particularly in large or dynamic cloud computing environments.
2. Limited scalability: VLANs are limited by the number of available VLAN IDs, which can be a constraint in larger cloud computing environments.
3. Limited security: VLANs do not provide complete security and can be compromised by malicious actors who are able to gain access to the network.
4. Limited interoperability: VLANs may not be fully compatible with all types of network devices and protocols, which can limit their usefulness in cloud computing environments.
5. Limited mobility: VLANs may not support the movement of devices or users between different network segments, which can limit their usefulness in mobile or remote cloud computing environments.
6. Cost: Implementing and maintaining VLANs can be costly, especially if specialized hardware or software is required.
7. Limited visibility: VLANs can make it more difficult to monitor and troubleshoot network issues, as traffic is isolated in different segments.

Real-Time Applications of VLAN:

Virtual LANs (VLANs) are widely used in cloud computing environments to improve network performance and security. Here are a few examples of real-time applications of VLANs:

1. Voice over IP (VoIP): VLANs can be used to isolate voice traffic from data traffic, which improves the quality of VoIP calls and reduces the risk of network congestion.

2. Video Conferencing: VLANs can be used to prioritize video traffic and ensure that it receives the bandwidth and resources it needs for high-quality video conferencing.
3. Remote Access: VLANs can be used to provide secure remote access to cloud-based applications and resources, by isolating remote users from the rest of the network.
4. Cloud Backup and Recovery: VLANs can be used to isolate backup and recovery traffic, which reduces the risk of network congestion and improves the performance of backup and recovery operations.
5. Gaming: VLANs can be used to prioritize gaming traffic, which ensures that gamers receive the bandwidth and resources they need for a smooth gaming experience.
6. IoT: VLANs can be used to isolate Internet of Things (IoT) devices from the rest of the network, which improves security and reduces the risk of network congestion.

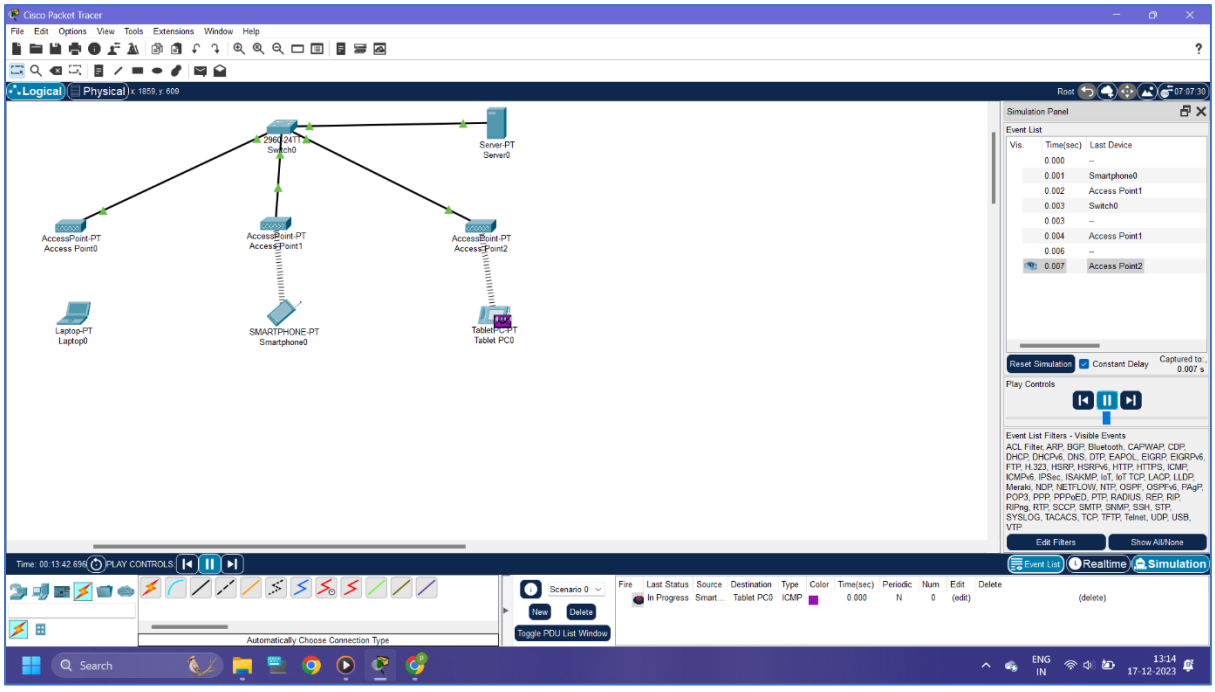
Practical 6

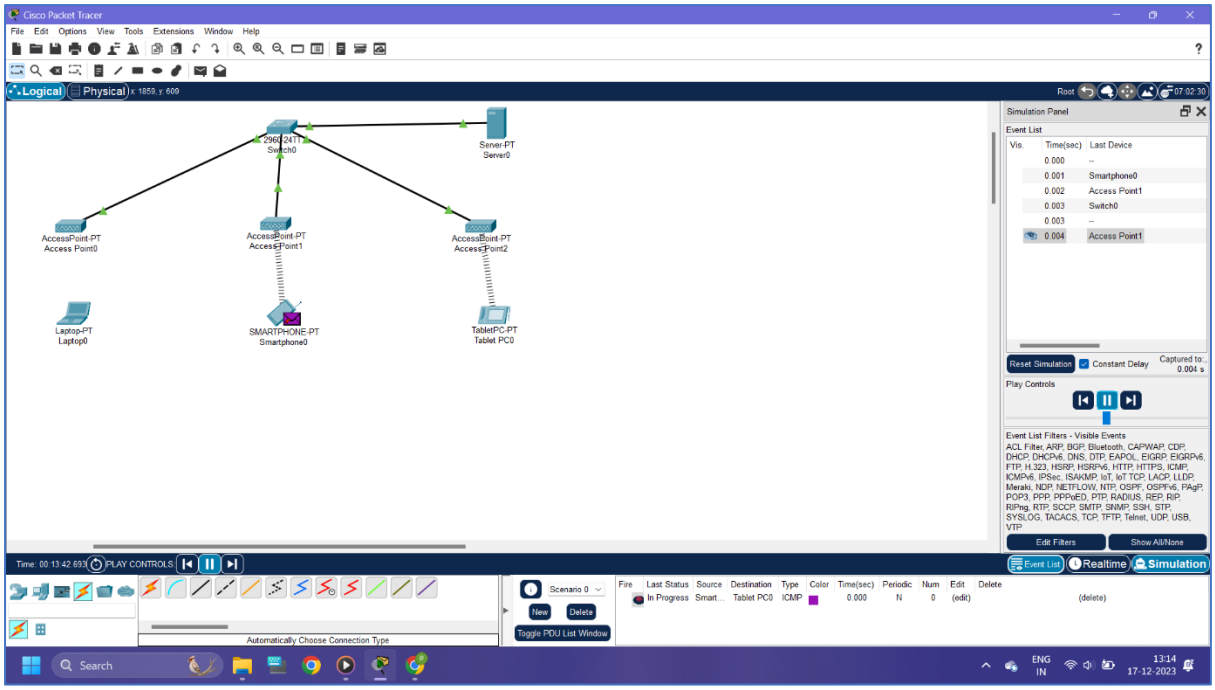
Aim: To implement WLAN.

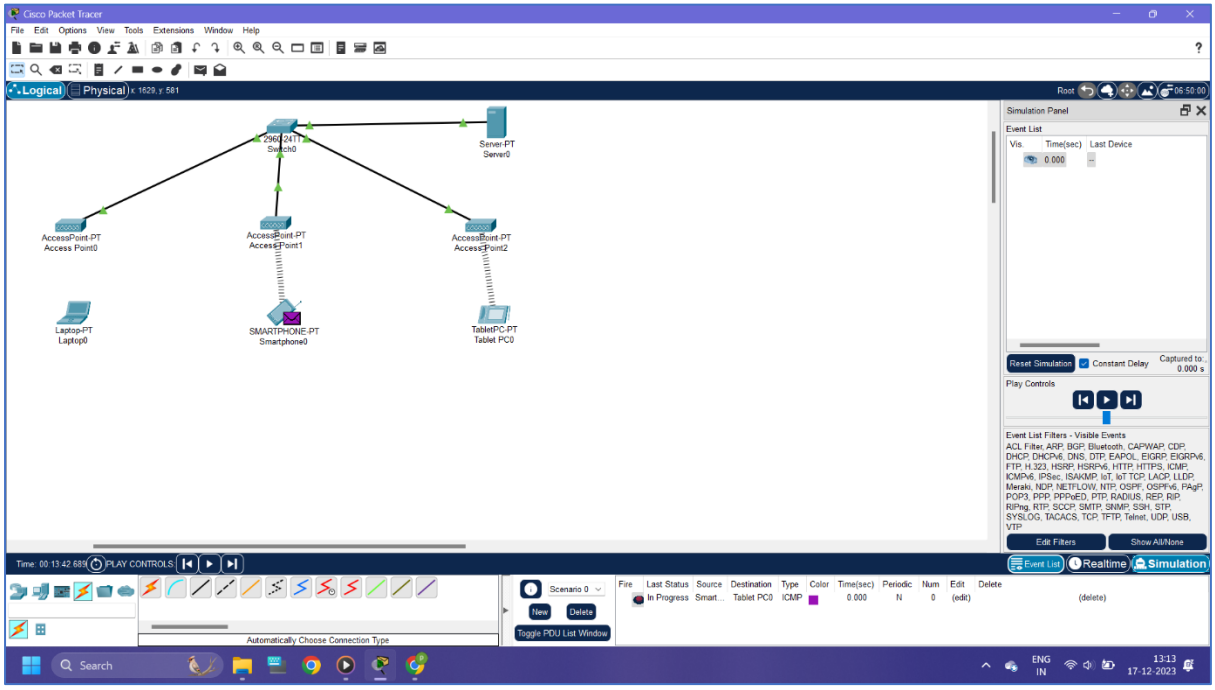
WLAN stands for Wireless Local Area Network. WLAN is a local area network that uses radio communication to provide mobility to the network users while maintaining the connectivity to the wired network. A WLAN basically, extends a wired local area network. WLANs are built by attaching a device called the access point (AP) to the edge of the wired network. Clients communicate with the AP using a wireless network adapter which is similar in function to an ethernet adapter. It is also called a LAWN is a Local area wireless network.

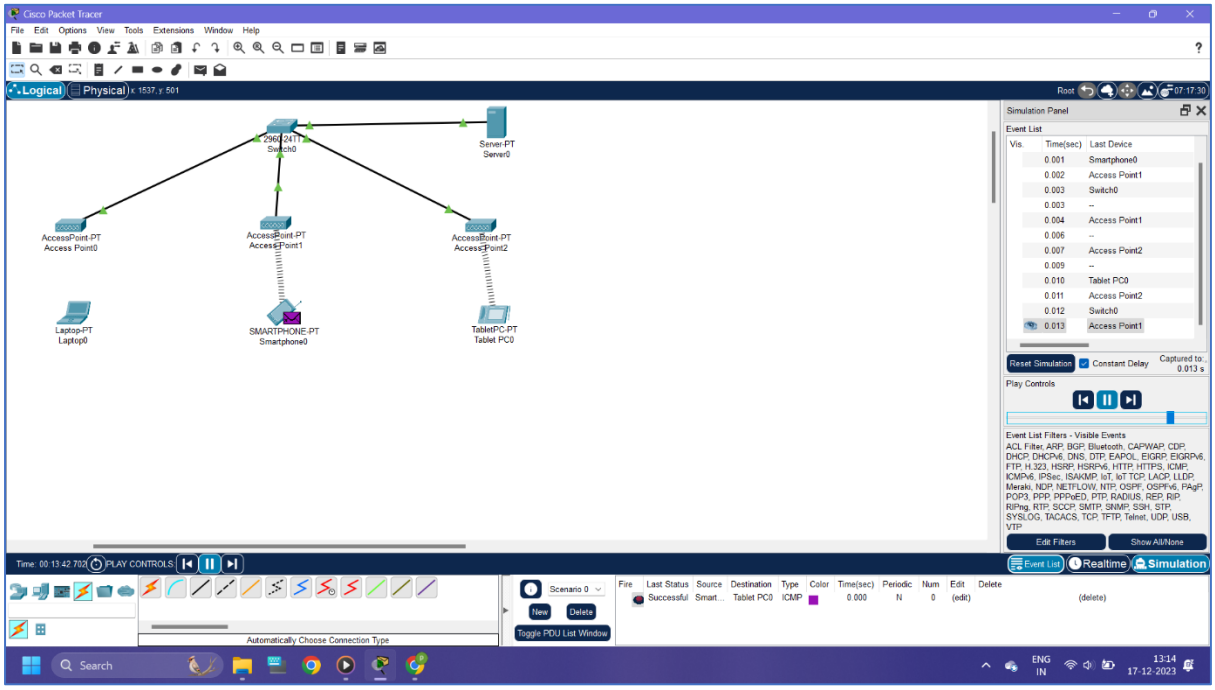
The performance of WLAN is high compared to other wireless networks. The coverage of WLAN is within a campus or building or that tech park. It is used in the mobile propagation of wired networks. The standards of WLAN are HiperLAN, Wi-Fi, and IEEE 802.11. It offers service to the desktop laptop, mobile application, and all the devices that work on the Internet. WLAN is an affordable method and can be set up in 24 hours. WLAN gives users the mobility to move around within a local coverage area and still be connected to the network. Latest brands are based on IEE 802.11 standards, which are the WI-FI brand name.

Implementation:




Cisco Packet Tracer
File Edit Options View Tools Extensions Window Help
Logical Physical
Root
Switch0
Server-PT Server0
AccessPoint-PT Access Point0
AccessPoint-PT Access Point1
AccessPoint-PT Access Point2
Laptop-PT Laptop0
SMARTPHONE-PT Smartphone0
TabletPC-PT Tablet PC0
Simulation Panel
Event List
Vis. Time(sec) Last Device
0.000 --
0.001 Smartphone0
0.002 Access Point1
0.003 Switch0
0.003 --
0.004 Access Point1
Reset Simulation
Constant Delay
Play Controls
Event List Filters - Visible Events
Edit Filters
Show All/None
Time: 00:13:42.693
PLAY CONTROLS
Realtime
Simulation
Scenario 0
New
Delete
Toggle PDU List Window
Automatically Choose Connection Type
Fire Last Status Source Destination Type Color Time(sec) Periodic Num Edit Delete
In Progress Smart... Tablet PC0 ICMP 0.000 N 0 (edit) (delete)
Search
ENG IN
13:14
17-12-2023


Cisco Packet Tracer
File Edit Options View Tools Extensions Window Help
Logical Physical
Root
Switch0
Server-PT Server0
AccessPoint-PT Access Point0
AccessPoint-PT Access Point1
AccessPoint-PT Access Point2
Laptop-PT Laptop0
SMARTPHONE-PT Smartphone0
TabletPC-PT Tablet PC0
Simulation Panel
Event List
Vis. Time(sec) Last Device
0.000 --
Reset Simulation
Constant Delay
Play Controls
Event List Filters - Visible Events
Edit Filters
Show All/None
Time: 00:13:42.689
PLAY CONTROLS
Realtime
Simulation
Scenario 0
New
Delete
Toggle PDU List Window
Automatically Choose Connection Type
Fire Last Status Source Destination Type Color Time(sec) Periodic Num Edit Delete
In Progress Smart... Tablet PC0 ICMP 0.000 N 0 (edit) (delete)
Search
ENG IN
13:13
17-12-2023


Cisco Packet Tracer
File Edit Options View Tools Extensions Window Help
Logical Physical
Switch0
Server-PT Server0
AccessPoint-PT Access Point0
AccessPoint-PT Access Point1
AccessPoint-PT Access Point2
Laptop-PT Laptop0
SMARTPHONE-PT Smartphone0
TabletPC-PT Tablet PC0
Simulation Panel
Event List
Vis. Time(sec) Last Device
0.001 Smartphone0
0.002 Access Point1
0.003 Switch0
0.004 Access Point1
0.006
0.007 Access Point2
0.009
0.010 Tablet PC0
0.011 Access Point2
0.012 Switch0
0.013 Access Point1
Reset Simulation
Constant Delay
Play Controls
Event List Filters - Visible Events
Edit Filters
Show All/None
Realtime
Simulation
Automatically Choose Connection Type
Scenario 0
New
Delete
Toggle PDU List Window
Fire Last Status Source Destination Type Color Time(sec) Periodic Num Edit Delete
Successful Smart... Tablet PC0 ICMP 0.000 N 0 (edit) (delete)
Search
ENG IN
13:14 17-12-2023

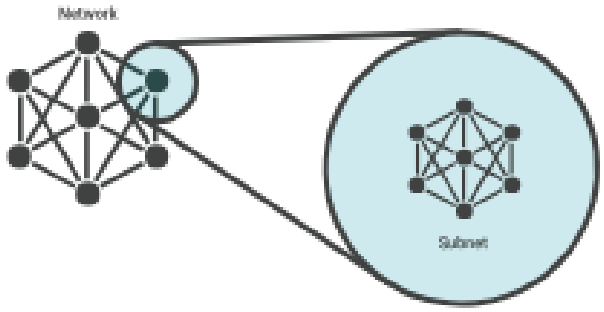
Practical 7

Aim: Internetworking with Routers.

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. Connections among routers can be implemented by using subnetting concept.

Subnet:

A subnet, or subnetwork, is a network inside a network. Subnets make networks more efficient. Through subnetting, network traffic can travel a shorter distance without passing through unnecessary routers to reach its destination.



Example:

Subnet the IP address 150.15.0.0 in 500 hosts in each subnet.

Step 1: Identify the class of the given IP address.

The given IP address belongs to class B.

Step 2: Identify the default mask.

255.255.0.0 => 1 1 1 1 1 1 1 1. 1 1 1 1 1 1 1 1. 0 0 0 0 0 0 0 0. 0 0 0 0 0 0 0 0

Step 3:

Number of hosts per subnet = 500

Convert the number of hosts per subnet into binary number i.e. 1 1 1 1 1 0 1 0 0 – 9 bits

So, we have to change in the default mask in the following manner.

1 1 1 1 1 1 1 1. 1 1 1 1 1 1 1 1. 1 1 1 1 1 1 1 0. 0 0 0 0 0 0 0 0

So, we can get a new subnet mask: 255.255.254.0

Step 4:

Network Ranges:

150.15.0.0 - 150.15.1.255

150.15.2.0 - 150.15.3.255

150.15.4.0 - 150.15.5.255

150.15.6.0 - 150.15.7.255

150.15.8.0 - 150.15.9.255

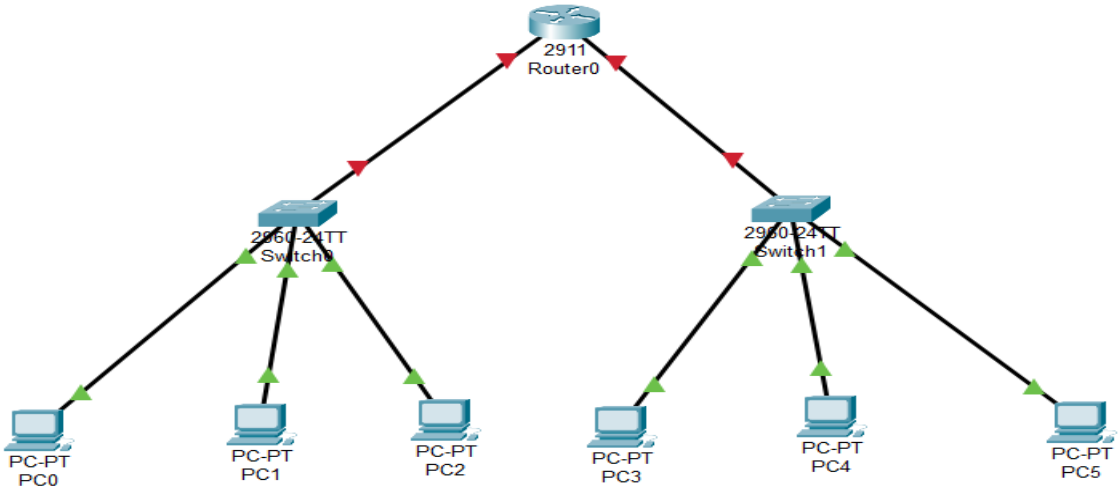
…

Practical Task:

We want to connect two different subnets 150.15.2.0 and 150.15.9.0. Let's see in the implementation part.

Implementation:

Step 1: Choose a router 2911, two switches 2960 and 6 different PCs and create a network as shown in figure.



Step 2:

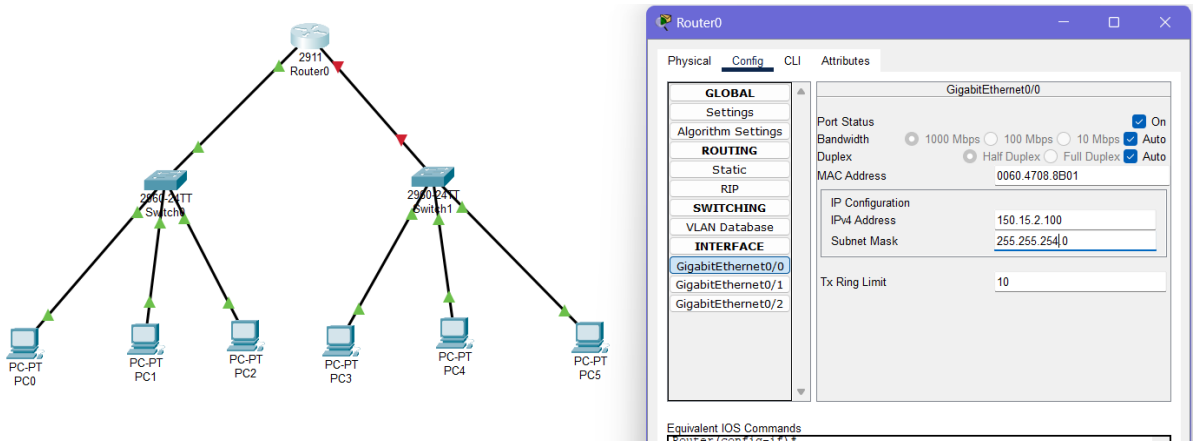
Configure the router by providing IP addresses to it on the following ports as shown below.

GigabitEthernet0/0: 150.15.2.100

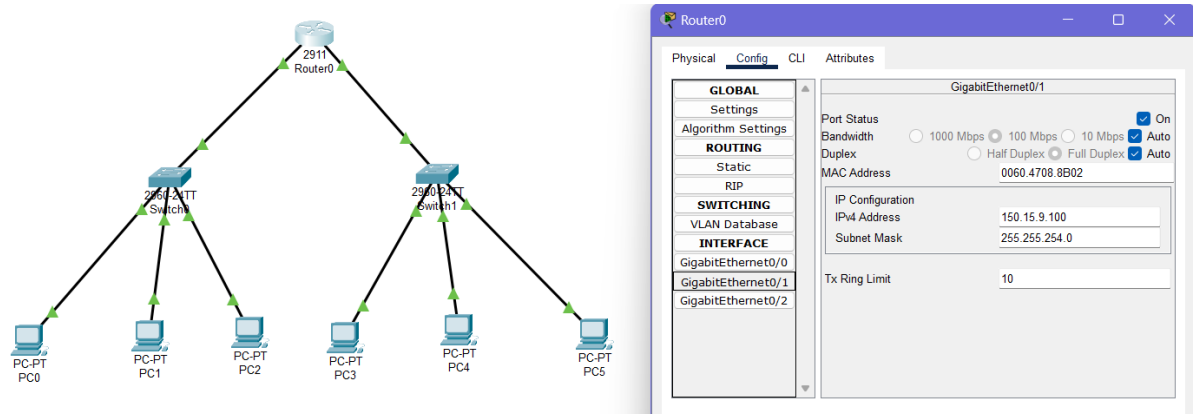
GigabitEthernet0/1: 150.15.9.100

Then ON the port status for both the ports.

Subnet mask should be set 255.255.254.0 as per our calculation.



Configuration on Port 0/0



Configuration on Port 0/1

Step 3:

Configuration of all 6 PCs.

Click on PC0.

Click on Desktop.

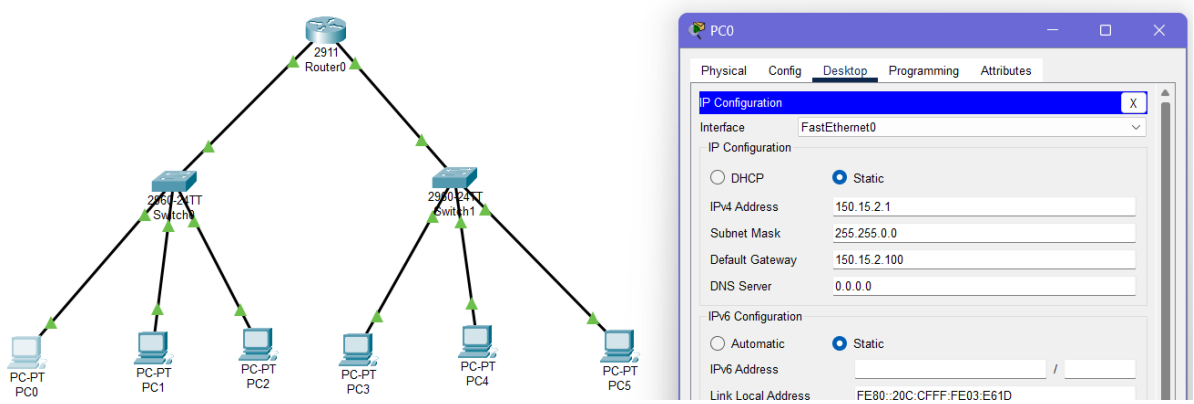
Click on IP Configuration.

IP Address should be set as 150.15.2.1 and the default mask will be set automatically 255.255.0.0 as PC's IP address belongs to class B.

Default Gateway must be the IP address of the router.

For PC0, PC1 and PC2 which connected in the same network: 150.15.2.100

For PC3, PC4 and PC5 which connected in another same network: 150.15.9.100



For PC1: IP Address: 150.15.2.2

For PC2: IP Address: 150.15.2.3

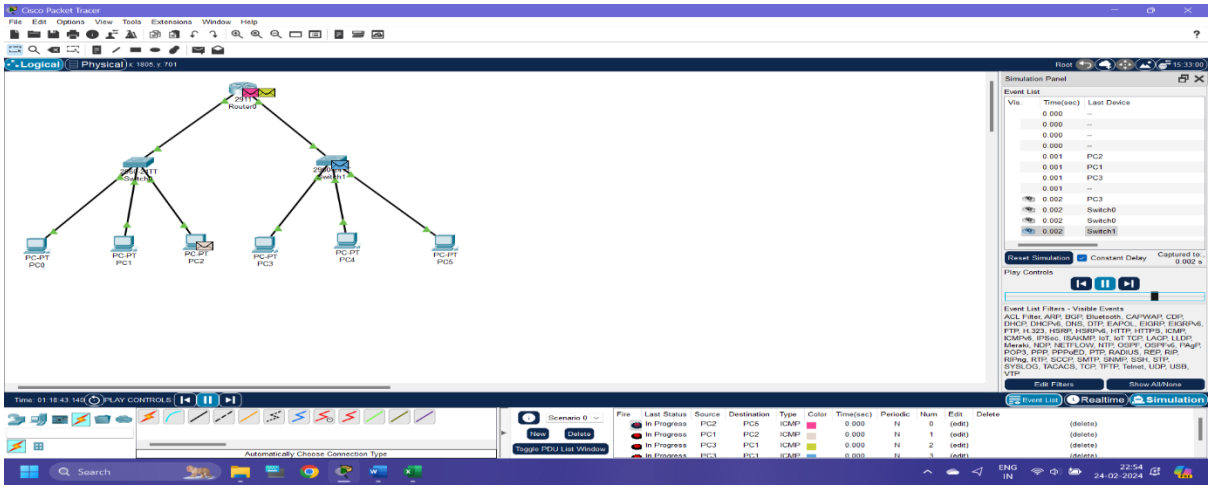
For PC3: IP Address: 150.15.9.1

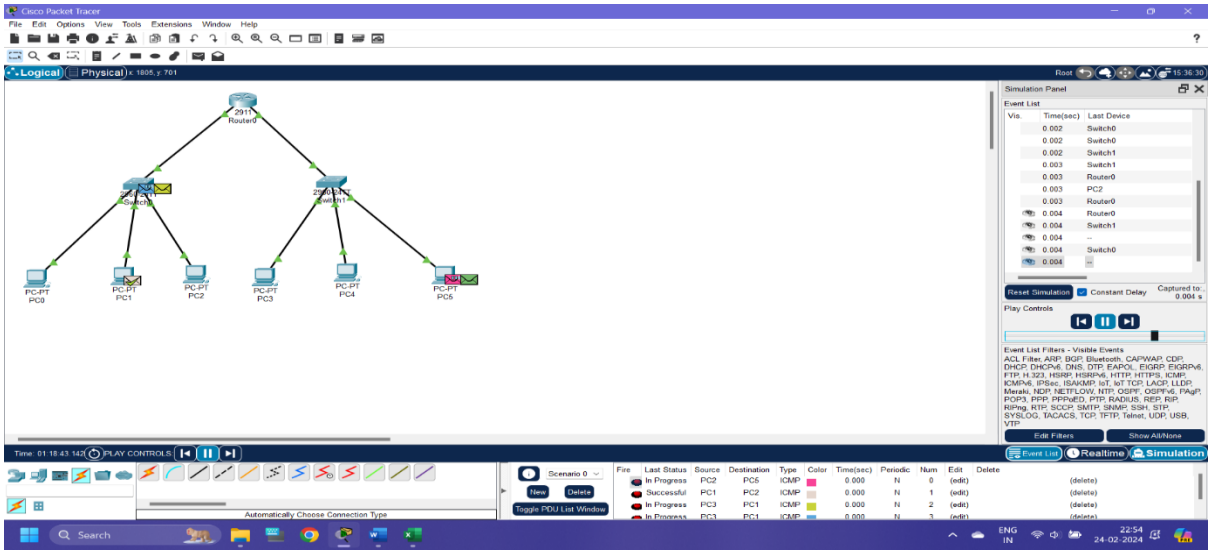
For PC4: IP Address: 150.15.9.2

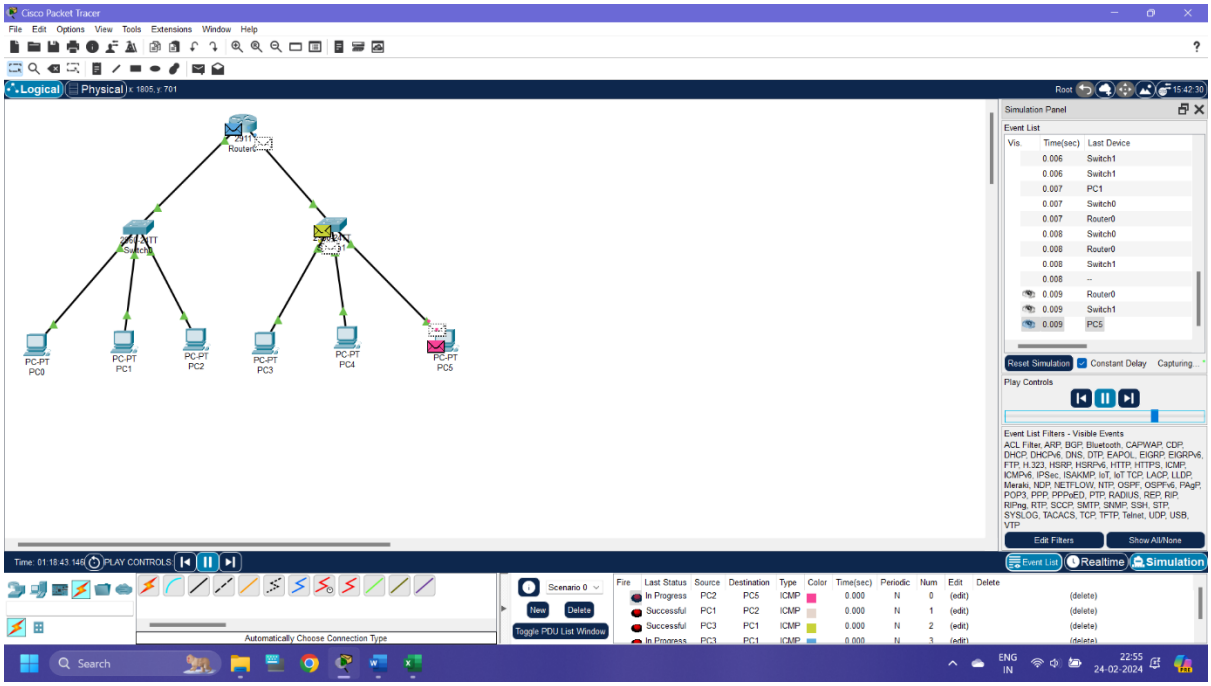
For PC5: IP Address: 150.15.9.3

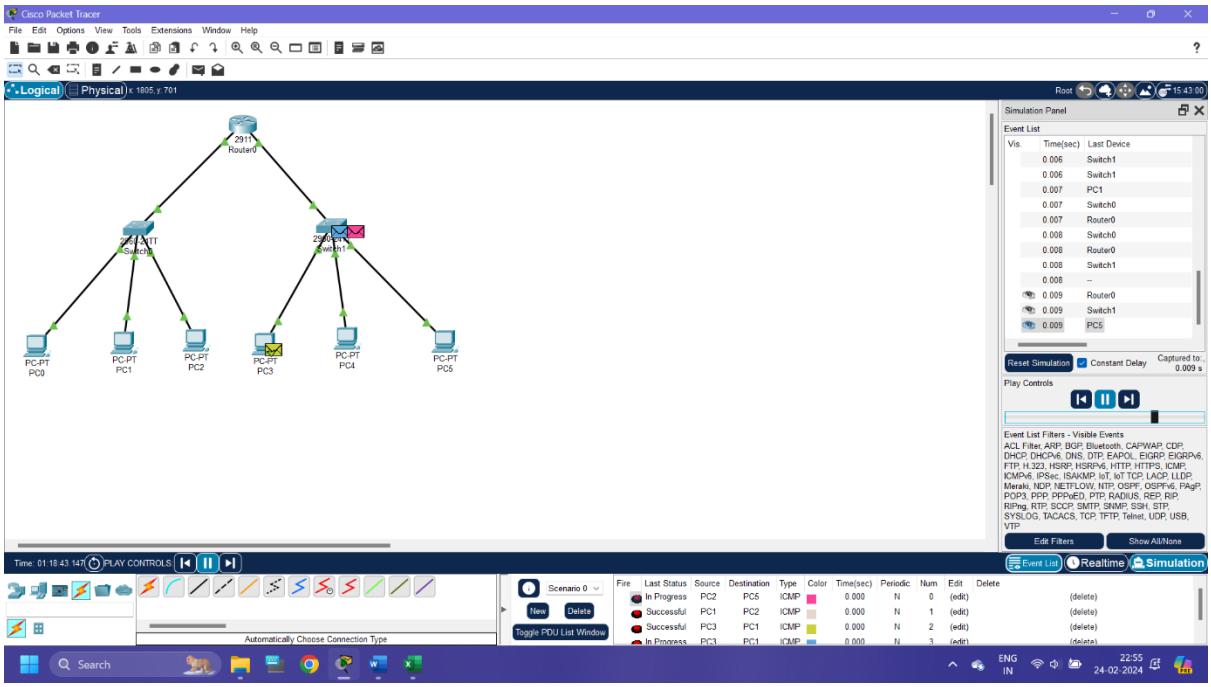
Step 4:

Now the configuration is completed. We have to check if the message will pass successfully or not. The screenshots are given below for the output.






Cisco Packet Tracer
Router0
Switch0
Switch1
PC-PT PC0
PC-PT PC1
PC-PT PC2
PC-PT PC3
PC-PT PC4
PC-PT PC5


Cisco Packet Tracer
Router0
Switch0
Switch1
PC-PT PC0
PC-PT PC1
PC-PT PC2
PC-PT PC3
PC-PT PC4
PC-PT PC5

Practical 8

Aim: To implement subnetting.

A subnet, or subnetwork, is a network inside a network. Subnets make networks more efficient. Through subnetting, network traffic can travel a shorter distance without passing through unnecessary routers to reach its destination.

Example:

Subnet the IP address 150.15.0.0 in 500 hosts in each subnet.

Step 1: Identify the class of the given IP address.

The given IP address belongs to class B.

Step 2: Identify the default mask.

255.255.0.0 => 1 1 1 1 1 1 1 1. 1 1 1 1 1 1 1 1. 0 0 0 0 0 0 0 0. 0 0 0 0 0 0 0 0

Step 3:

Number of hosts per subnet = 500

Convert the number of hosts per subnet into binary number i.e. 1 1 1 1 1 0 1 0 0 – 9 bits

So, we have to change in the default mask in the following manner.

1 1 1 1 1 1 1 1. 1 1 1 1 1 1 1 1. 1 1 1 1 1 1 1 0. 0 0 0 0 0 0 0 0

So, we can get a new subnet mask: 255.255.254.0

Step 4:

Network Ranges:

150.15.0.0 - 150.15.1.255

150.15.2.0 - 150.15.3.255

150.15.4.0 - 150.15.5.255

150.15.6.0 - 150.15.7.255

150.15.8.0 - 150.15.9.255

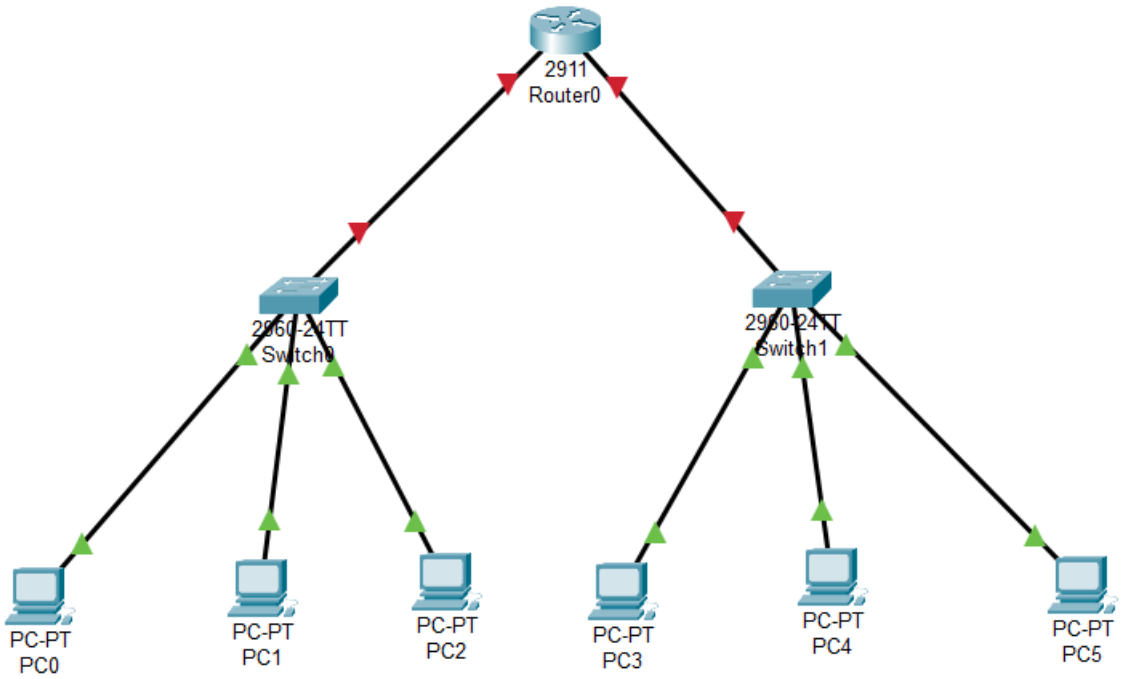
…

Practical Task:

We want to connect two different subnets 150.15.2.0 and 150.15.9.0. Let's see in the implementation part.

Implementation:

Step 1: Choose a router 2911, two switches 2960 and 6 different PCs and create a network as shown in figure.



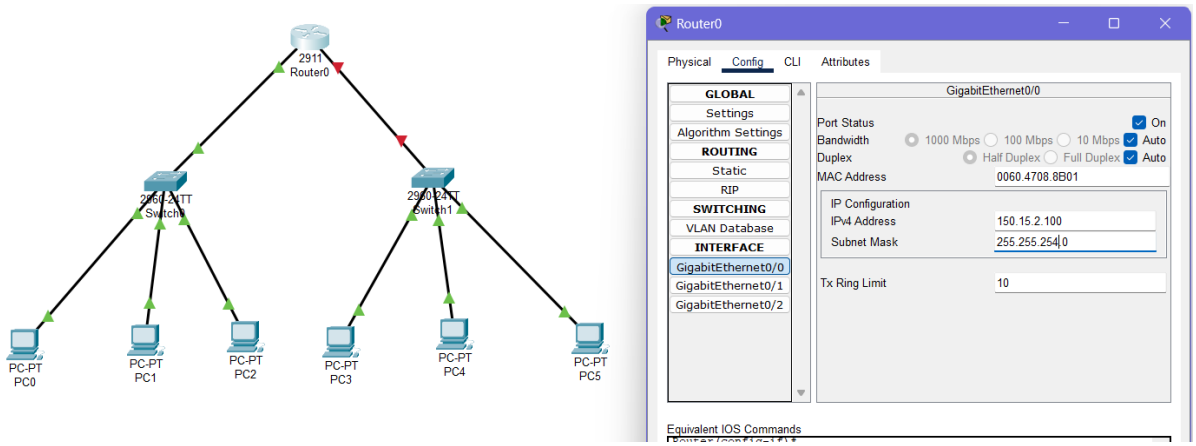
Step 2: Configure the router by providing IP addresses to it on the following ports as shown below.

GigabitEthernet0/0: 150.15.2.100

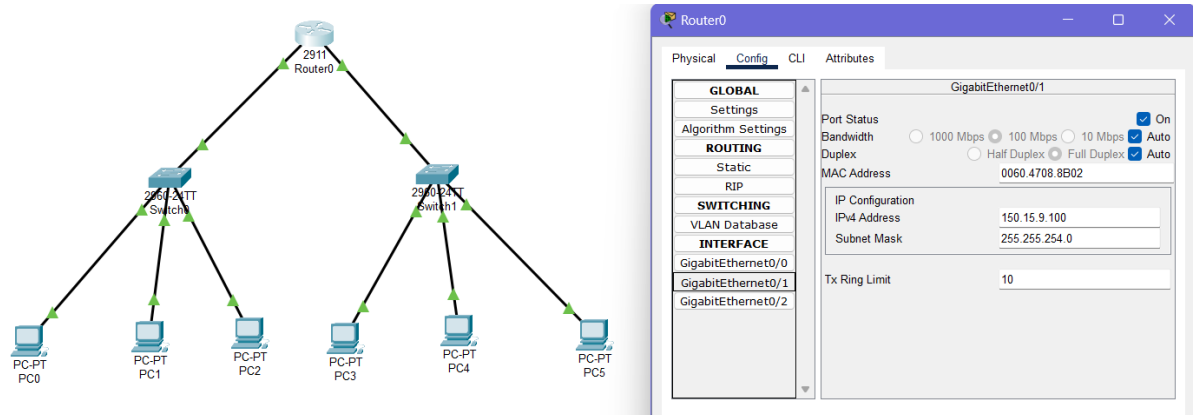
GigabitEthernet0/1: 150.15.9.100

Then ON the port status for both the ports.

Subnet mask should be set 255.255.254.0 as per our calculation.



Configuration on Port 0/0



Configuration on Port 0/1

Step 3:

Configuration of all 6 PCs.

Click on PC0.

Click on Desktop.

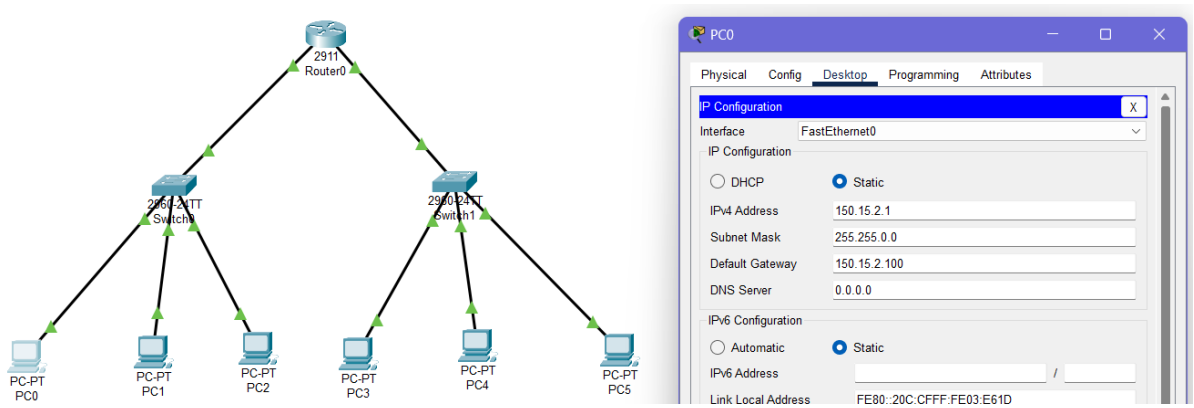
Click on IP Configuration.

IP Address should be set as 150.15.2.1 and the default mask will be set automatically 255.255.0.0 as PC's IP address belongs to class B.

Default Gateway must be the IP address of the router.

For PC0, PC1 and PC2 which connected in the same network: 150.15.2.100

For PC3, PC4 and PC5 which connected in another same network: 150.15.9.100



For PC1: IP Address: 150.15.2.2

For PC2: IP Address: 150.15.2.3

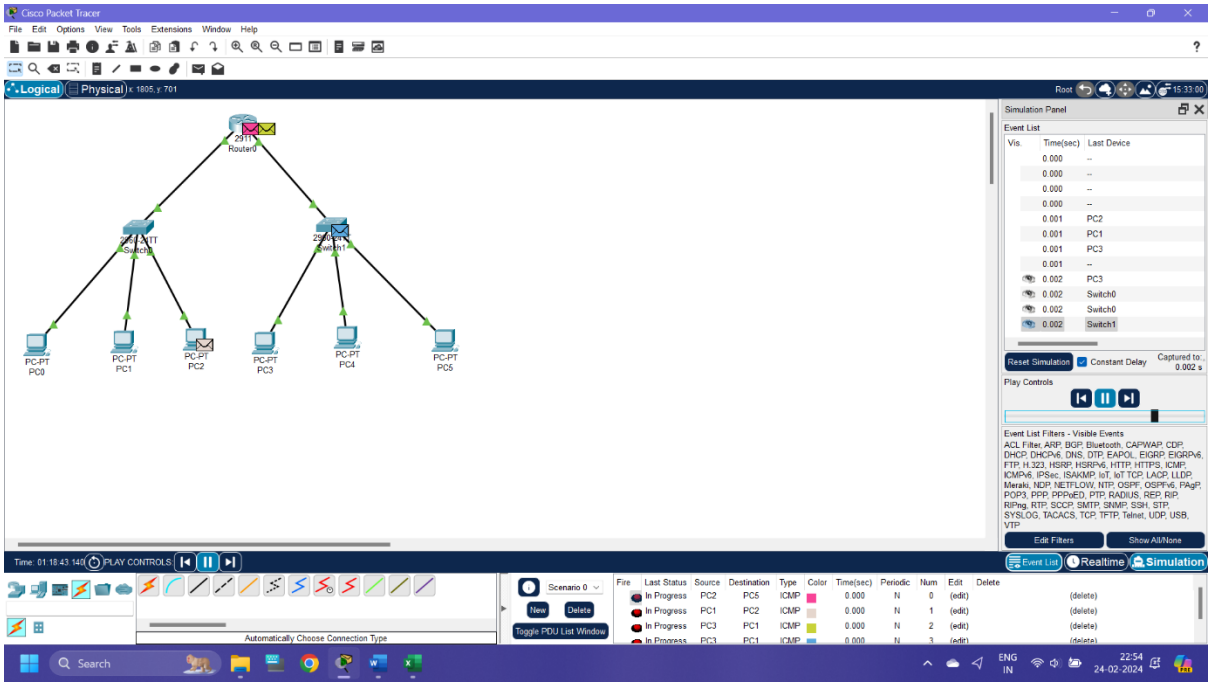
For PC3: IP Address: 150.15.9.1

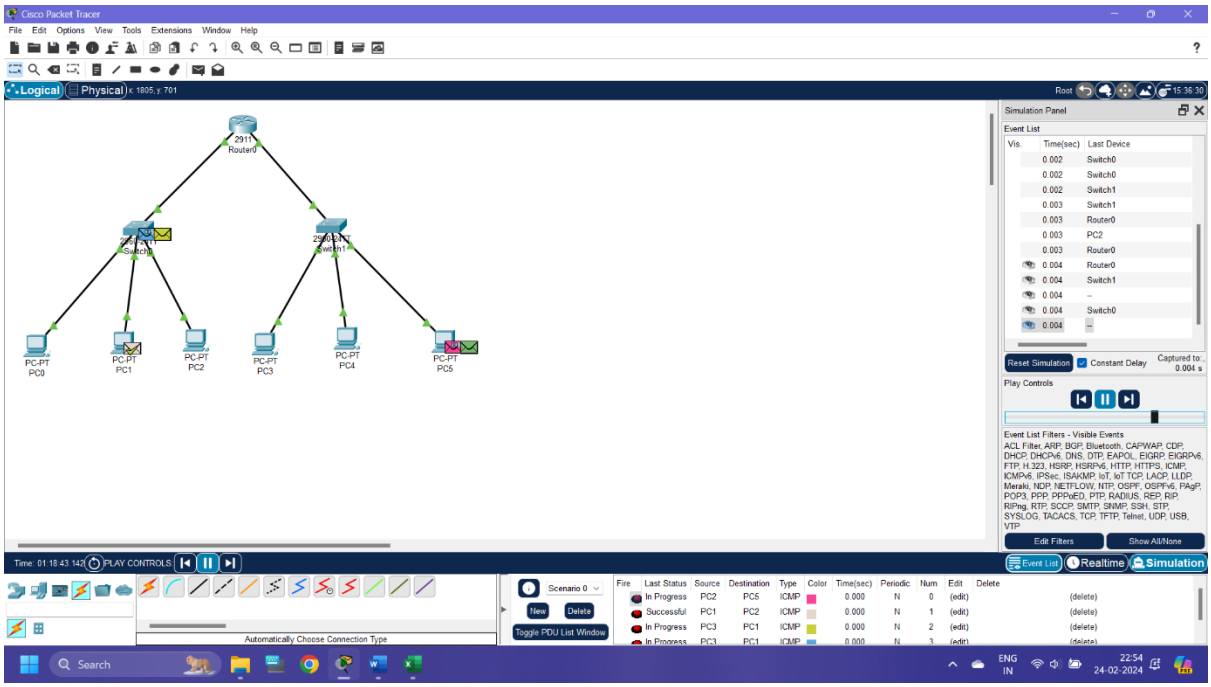
For PC4: IP Address: 150.15.9.2

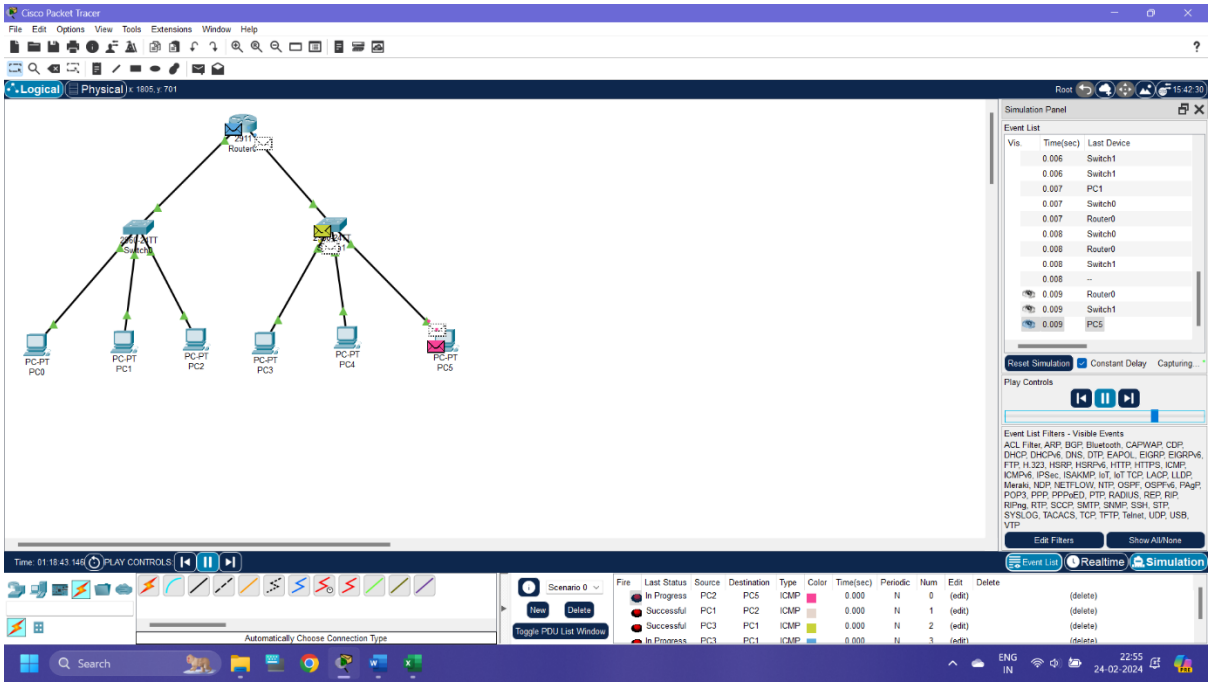
For PC5: IP Address: 150.15.9.3

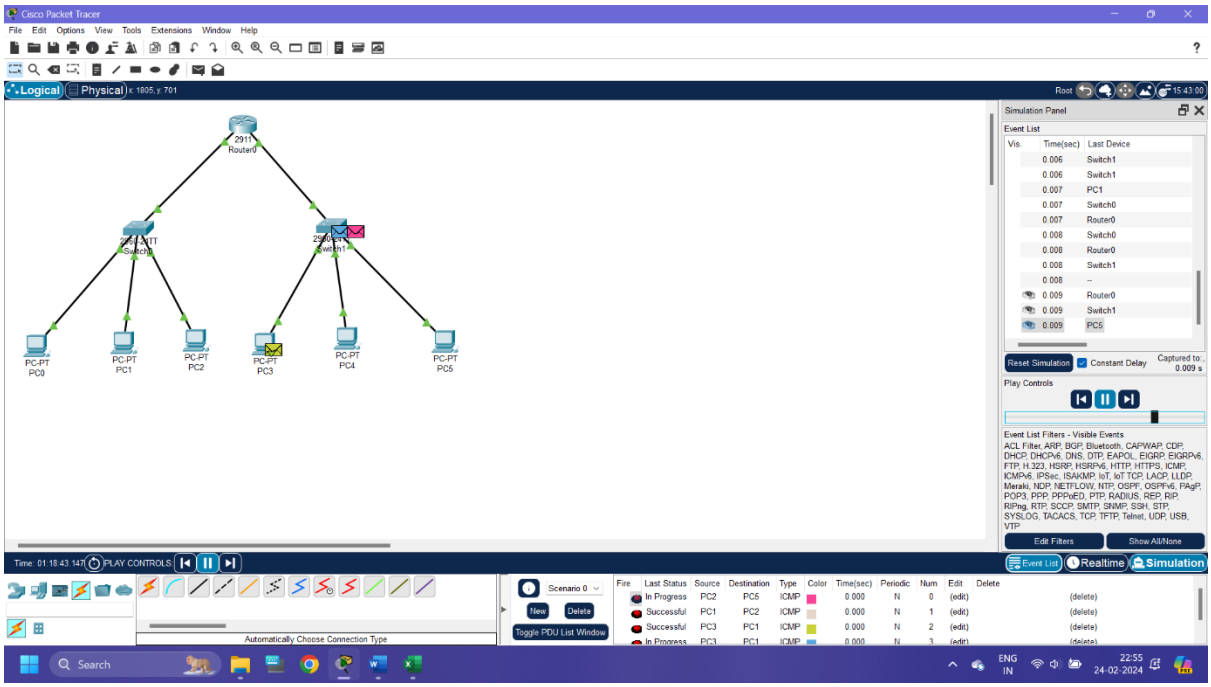
Step 4:

Now the configuration is completed. We have to check if the message will pass successfully or not. The images are given below for the output.


Cisco Packet Tracer
Logical
Physical
Router0
Switch0
Switch1
PC-PT PC0
PC-PT PC1
PC-PT PC2
PC-PT PC3
PC-PT PC4
PC-PT PC5
Simulation Panel
Event List
Reset Simulation
Constant Delay
Play Controls
Edit Filters
Show All/None
Realtime
Simulation
New
Delete
Toggle PDU List Window
Automatically Choose Connection Type


Cisco Packet Tracer
Logical
Physical
Router0
Switch0
Switch1
PC-PT PC0
PC-PT PC1
PC-PT PC2
PC-PT PC3
PC-PT PC4
PC-PT PC5
Simulation Panel
Event List
Reset Simulation
Constant Delay
Play Controls
Edit Filters
Show All/None
Realtime
Simulation
New
Delete
Toggle PDU List Window
Automatically Choose Connection Type


Cisco Packet Tracer
Logical
Physical
Router0
Switch0
Switch1
PC-PT PC0
PC-PT PC1
PC-PT PC2
PC-PT PC3
PC-PT PC4
PC-PT PC5
Simulation Panel
Event List
Reset Simulation
Constant Delay
Play Controls
Edit Filters
Show All/None
Realtime
Simulation
Automatically Choose Connection Type
Toggle PDU List Window


Cisco Packet Tracer
Logical
Physical
Router0
Switch0
Switch1
PC-PT PC0
PC-PT PC1
PC-PT PC2
PC-PT PC3
PC-PT PC4
PC-PT PC5
Simulation Panel
Event List
Reset Simulation
Constant Delay
Play Controls
Edit Filters
Show All/None
Realtime
Simulation
Automatically Choose Connection Type
Toggle PDU List Window

Practical 9

Aim: To implement and study routing at Network layer.

Routing is a procedure of making decisions in which the router (which is a hardware device used in networking to receive and send data in the form of packets on a network) selects the best path to make data transfer from source to destination. A router exists in the network layer in the OSI as well as TCP/IP model.

Some functions of a router are:

1. Building an optimal path on a network to reach its destination (in which static and dynamic routing take place).
2. Taking routing decisions.
3. Balancing load.

Types of Routing:

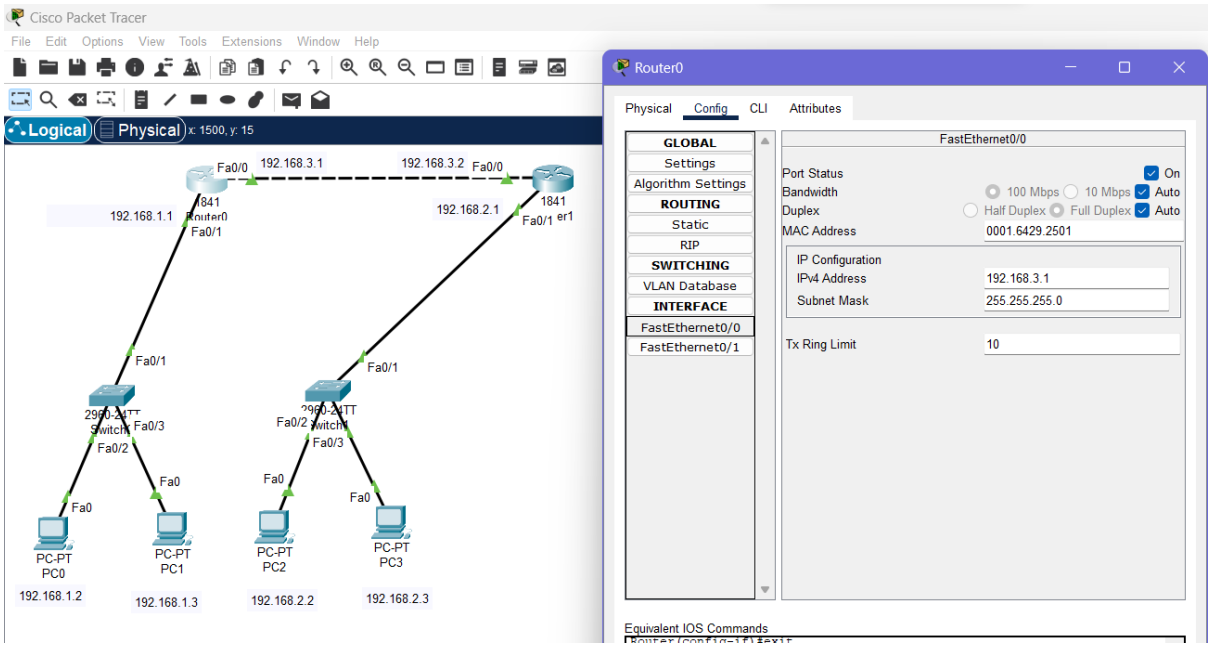
1. **Static routing:** Static routing is a process in which we have to manually add routes to the routing table. No routing overhead for the router CPU which means a cheaper router can be used to do routing. It adds security because only an only administrator can allow routing to particular networks only.

2. **Dynamic routing:** Dynamic routing is known as a technique of finding the best path for the data to travel over a network in this process a router can transmit data through various different routes and reach its destination on the basis of conditions at that time of communication circuits.

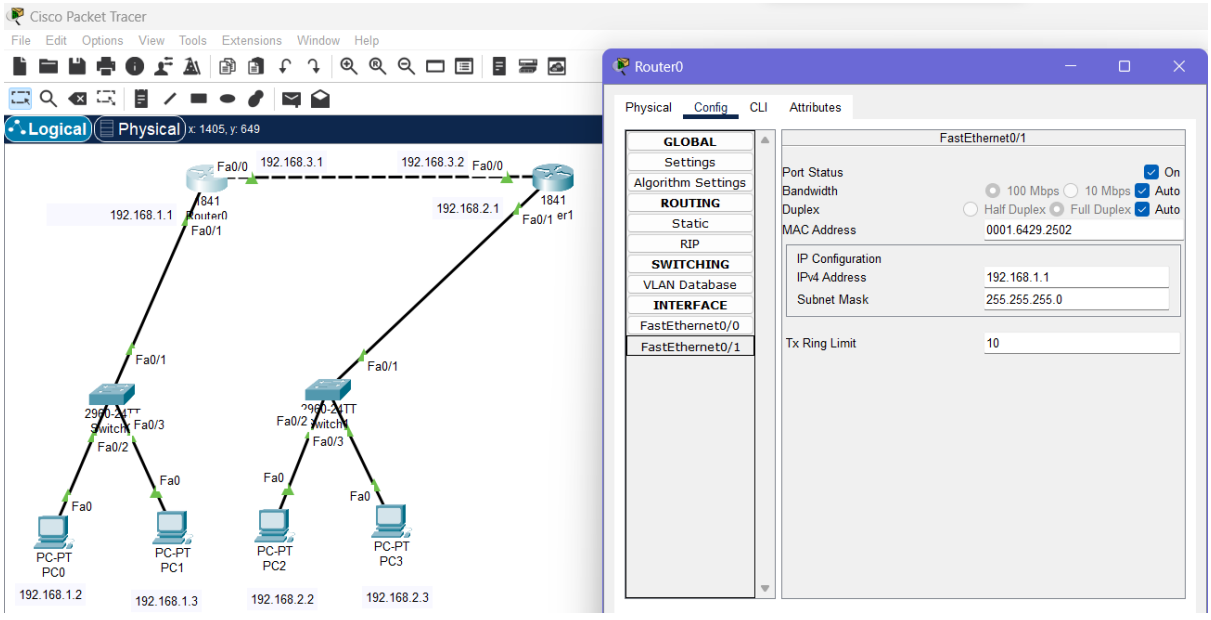
We will implement here about static routing and dynamic routing both.

Implementation of Static Routing:

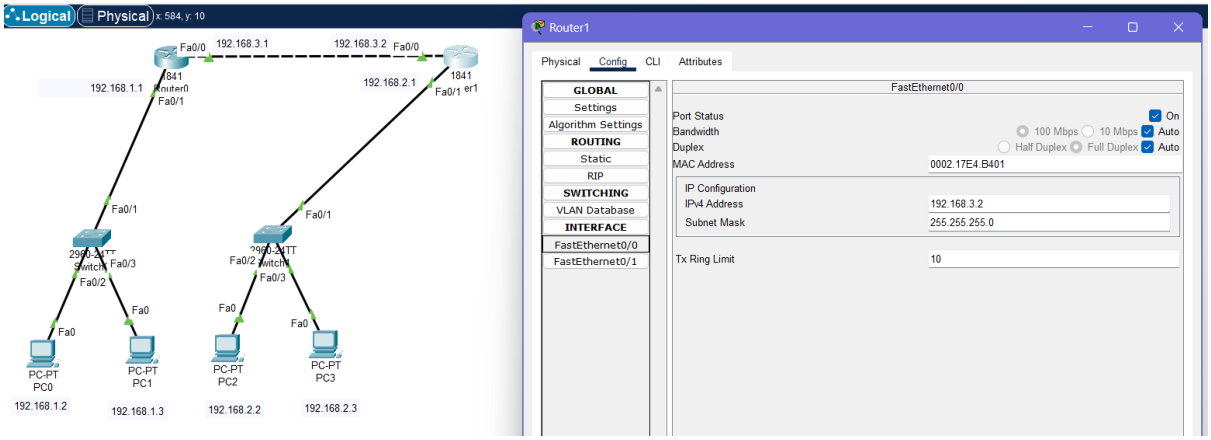
Step 1: Configure FastEthernet0/0 Port of Router0.



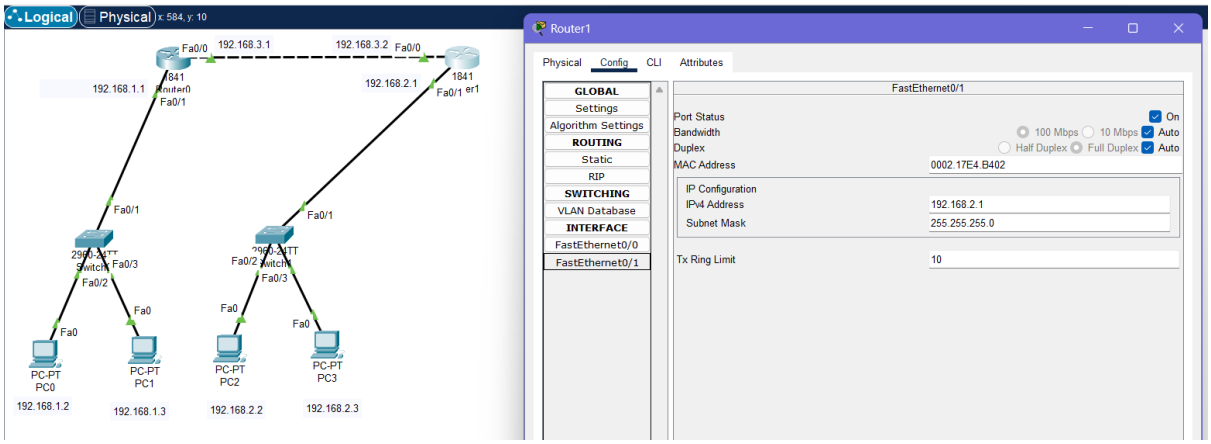
Step 2: Configure FastEthernet0/1 Port of Router0.



Step 3: Configure FastEthernet0/0 Port of Router1.



Step 4: Configure FastEthernet0/0 Port of Router1.



Step 5: Configure all the PCs as per the following table.

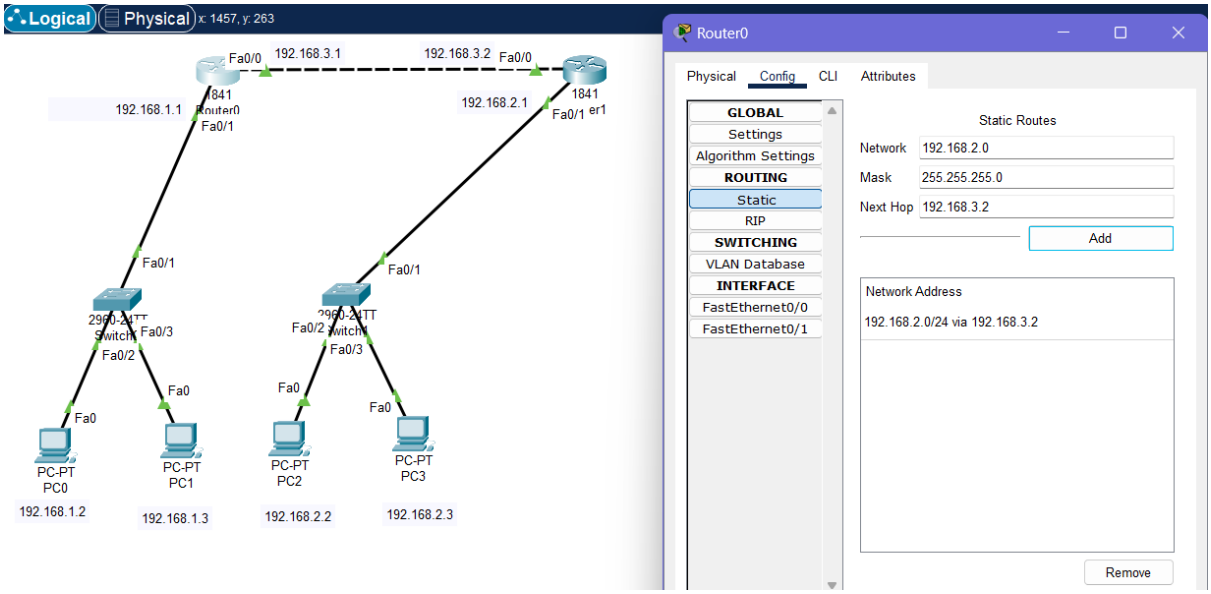
	IPv4 Address of PC	Gateway Router of PC
PC0	192.168.1.2	192.168.1.1
PC1	192.168.1.3	192.168.1.1
PC2	192.168.2.2	192.168.2.1
PC3	182.168.2.3	192.168.2.1

Step 6: Click on Router0. Then click on “static”. Fill all the following fields as per the given data. Finally click on “Add” button.

Network: 192.168.2.0

Mask: 255.255.255.0

Next Hop: 192.168.3.2

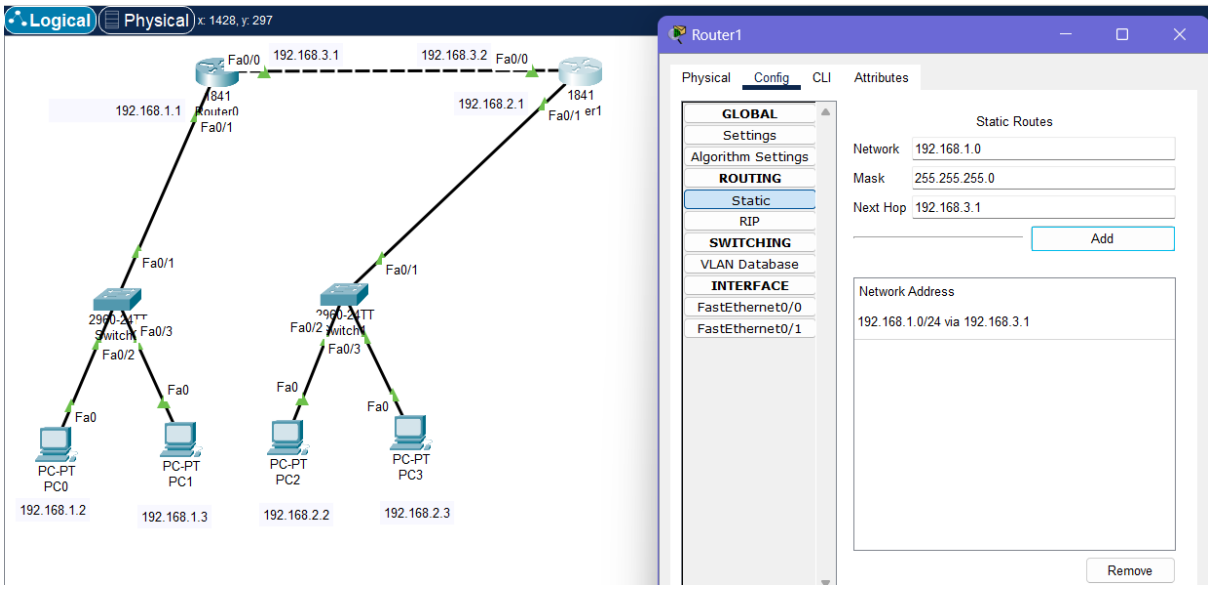


Step 7: Click on Router1. Then click on “static”. Fill all the following fields as per the given data. Finally click on “Add” button.

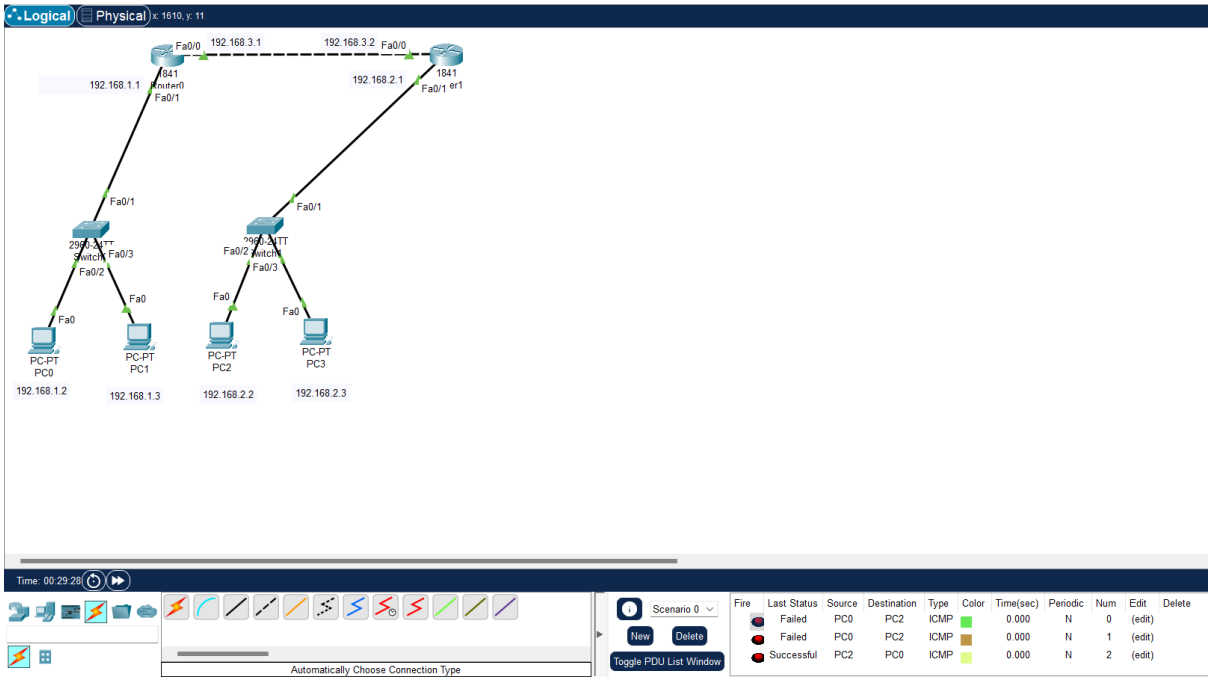
Network: 192.168.1.0

Mask: 255.255.255.0

Next Hop: 192.168.3.1

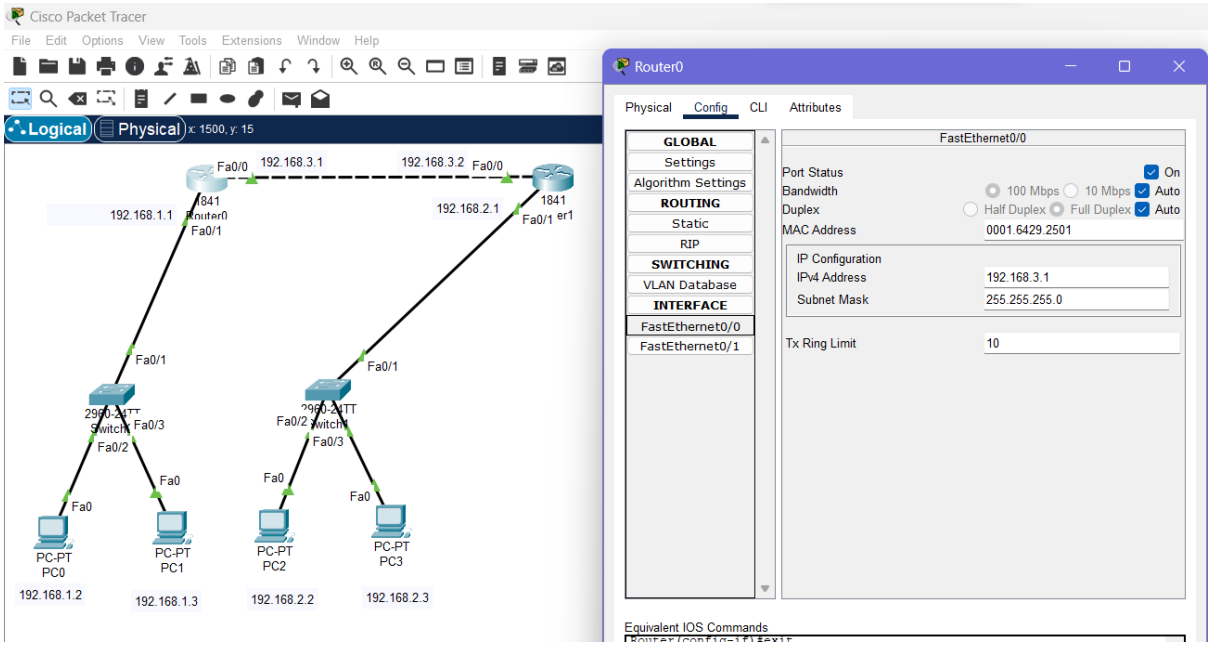


Step 8: Check if the connection is working or not by taking a message and pass it from one PC to another one and check the status if it is successful or not.

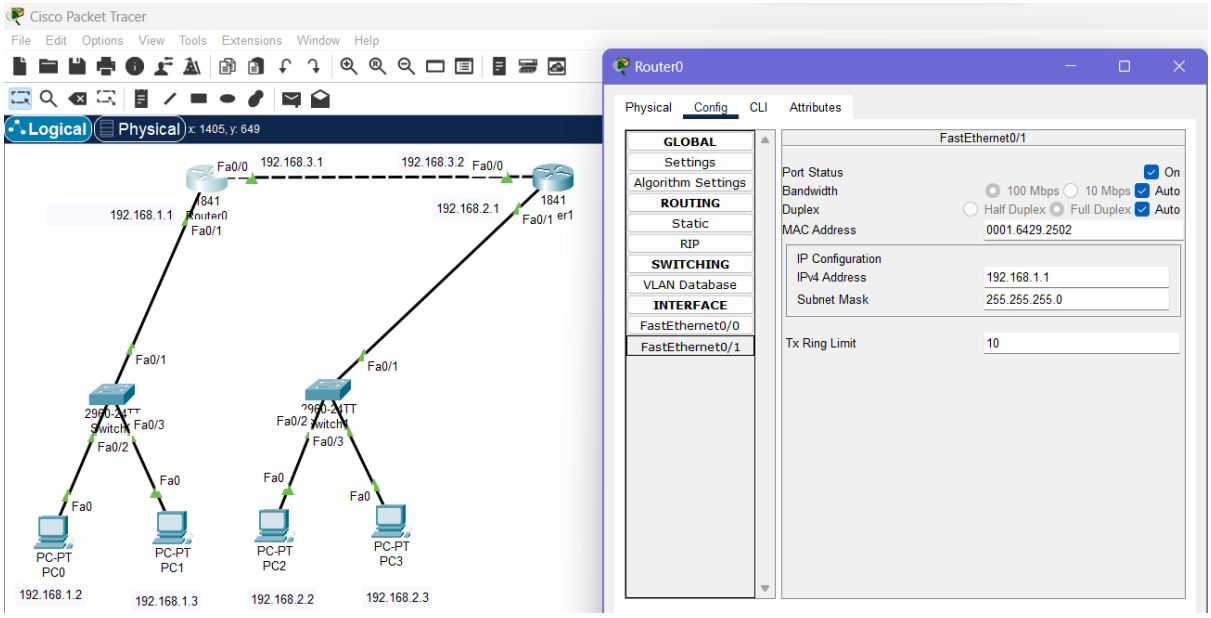


Implementation of Dynamic Routing:

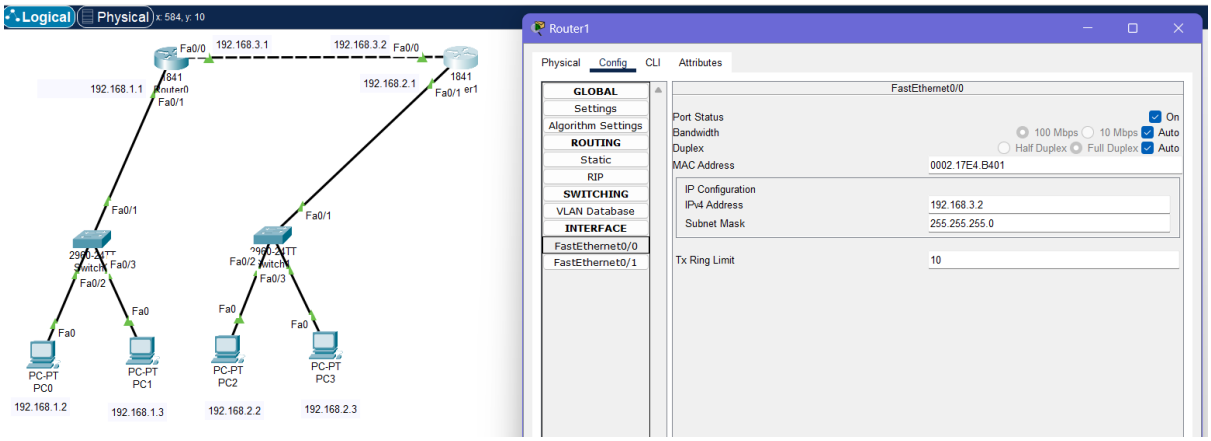
Step 1: Configure FastEthernet0/0 Port of Router0.



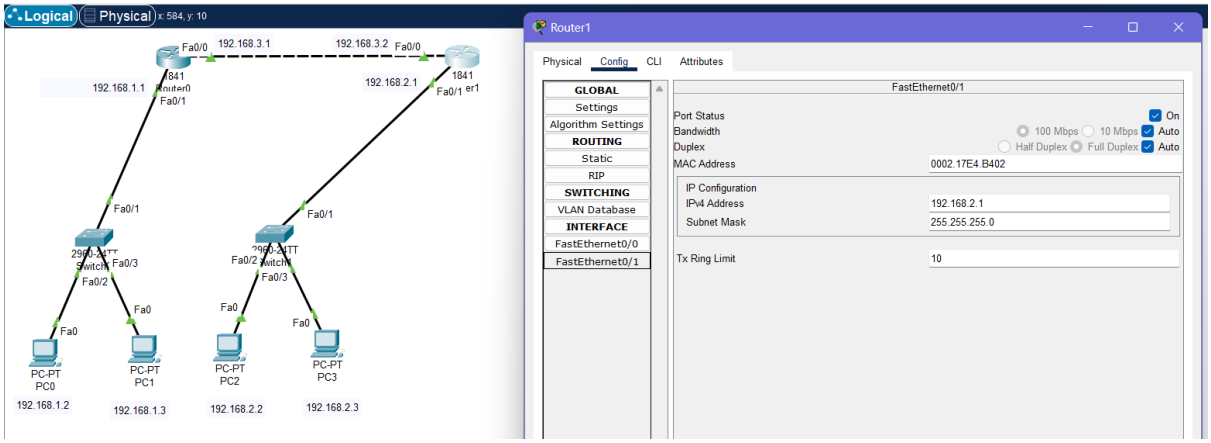
Step 2: Configure FastEthernet0/1 Port of Router0.



Step 3: Configure FastEthernet0/0 Port of Router1.



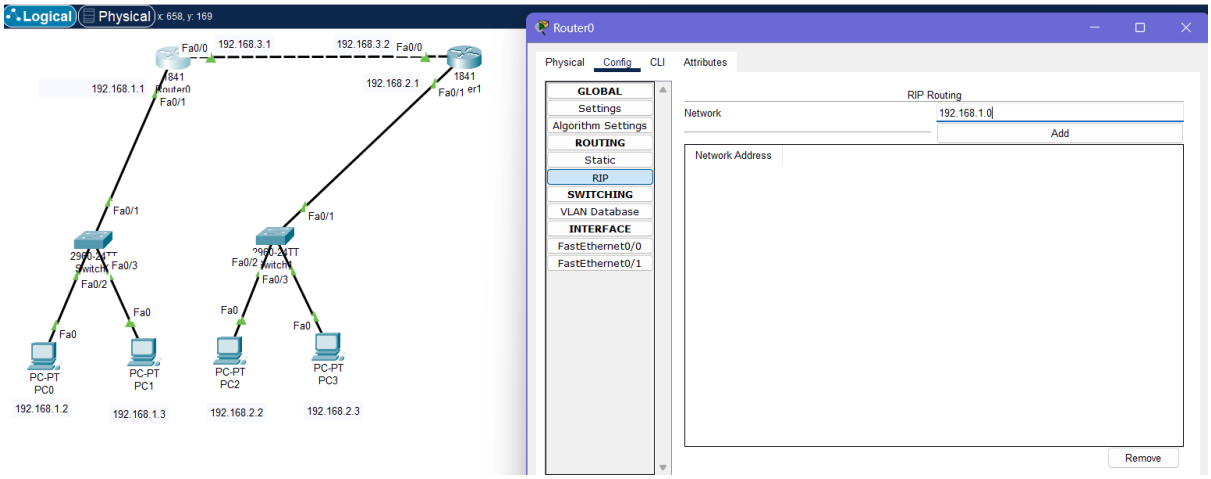
Step 4: Configure FastEthernet0/0 Port of Router1.



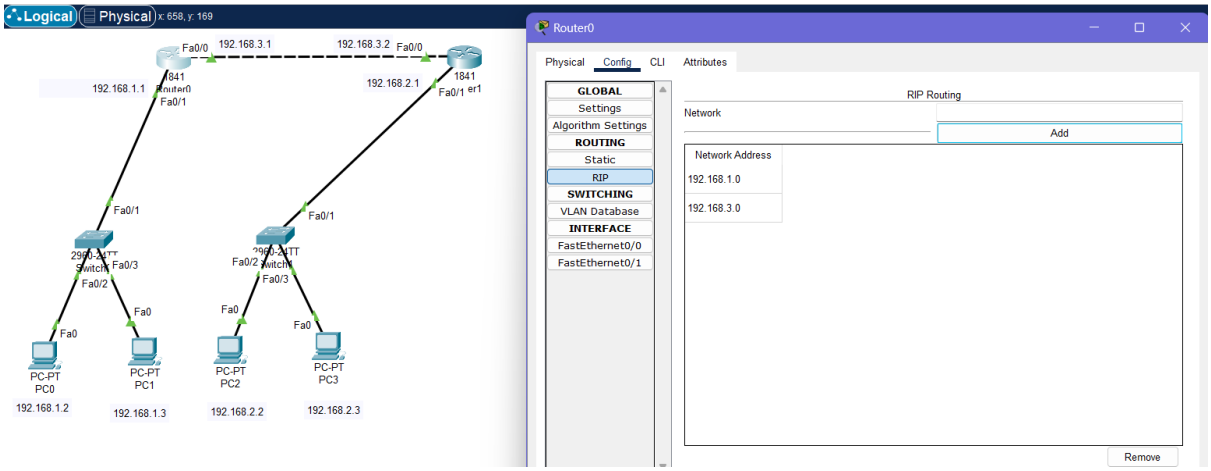
Step 5: Configure all the PCs as per the following table.

	IPv4 Address of PC	Gateway Router of PC
PC0	192.168.1.2	192.168.1.1
PC1	192.168.1.3	192.168.1.1
PC2	192.168.2.2	192.168.2.1
PC3	182.168.2.3	192.168.2.1

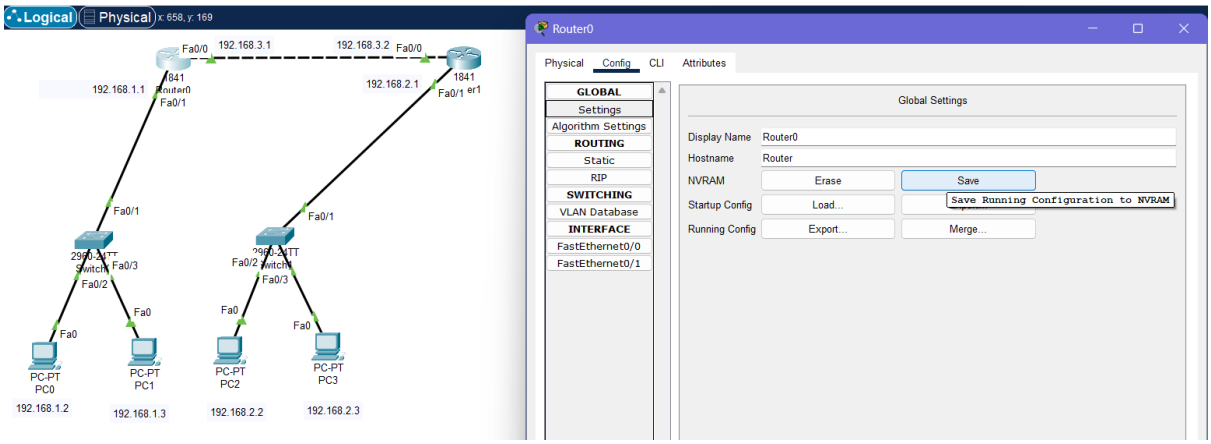
Step 5: Click on Router0. Click on RIP. In Network field, enter the following data as per the given image.



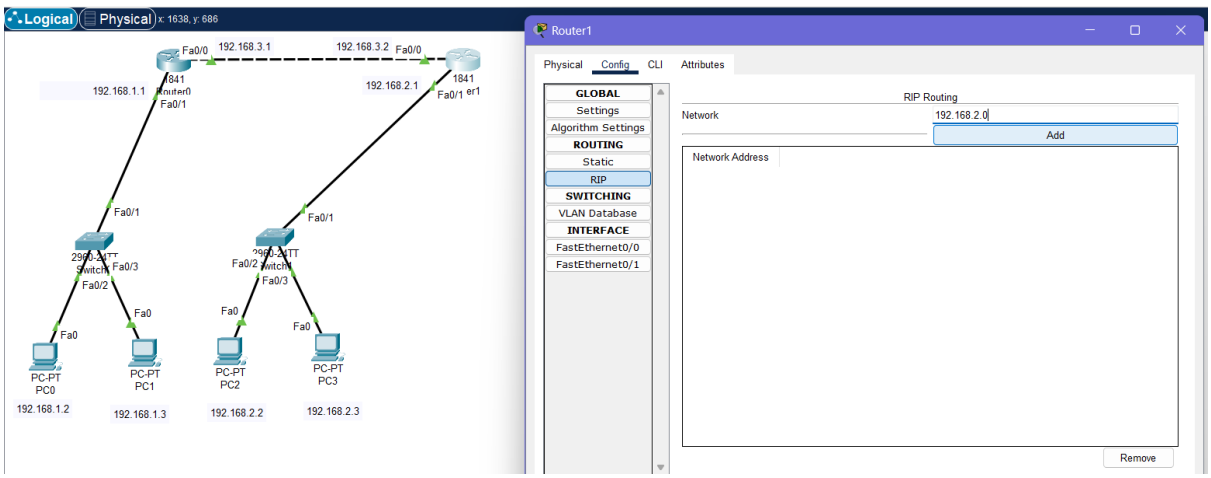
Click on “Add”.



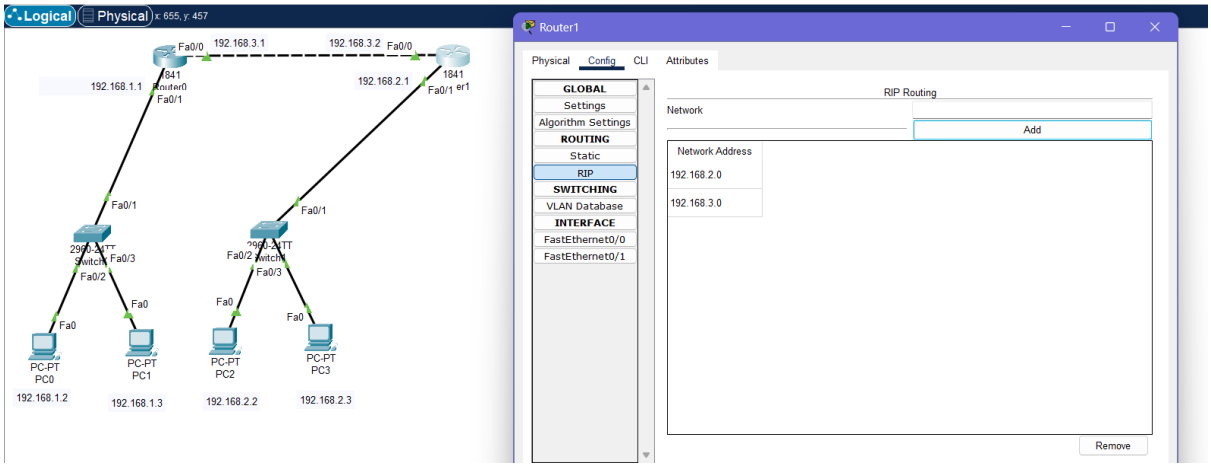
Click on “Settings” and then click on “Save”.



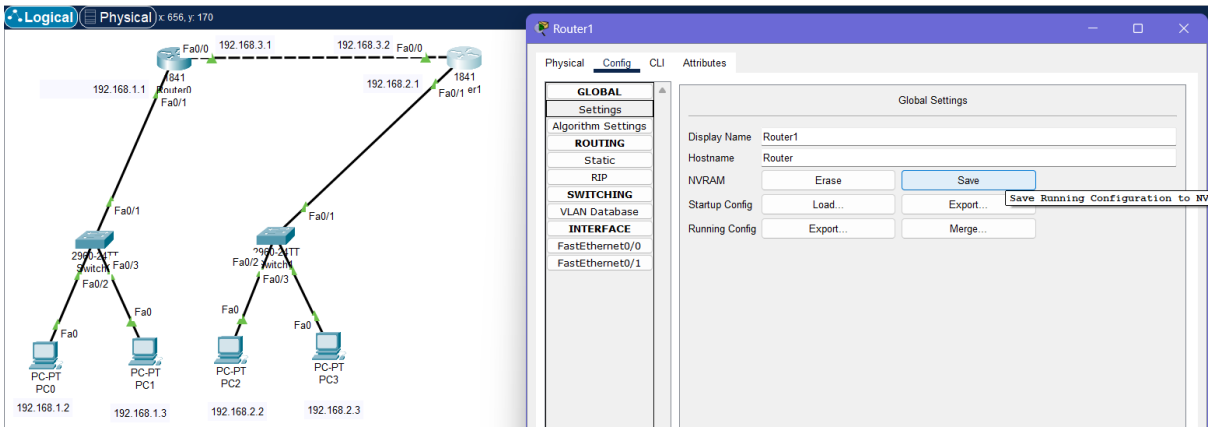
Step 6: Click on Router1. Click on RIP. In Network field, enter the following data as per the given image.



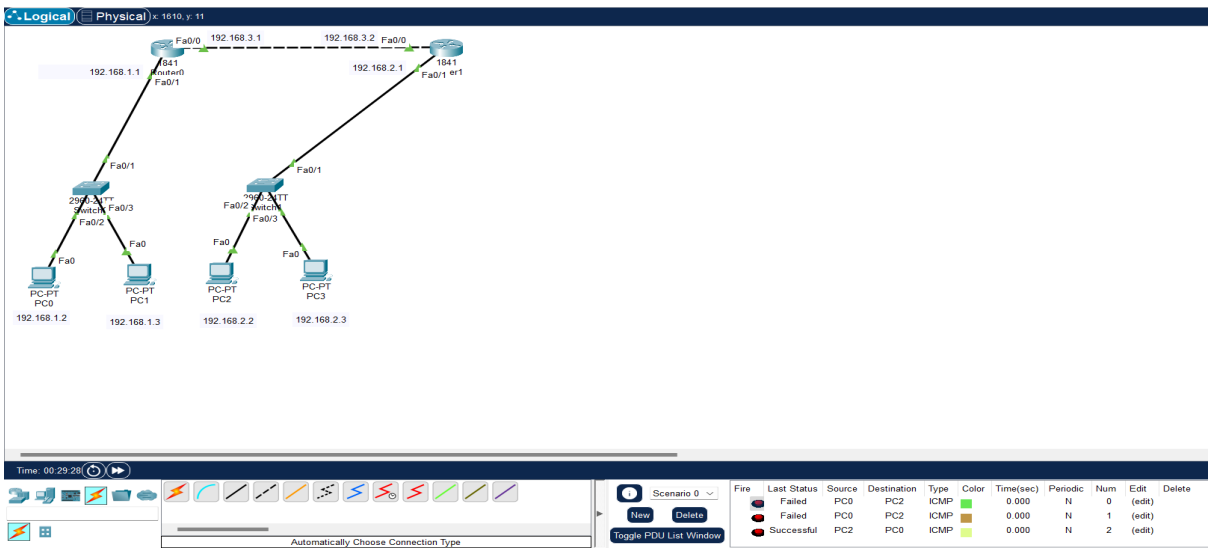
Click on “Add”.



Click on “Settings” and then click on “Save”.



Step 7: Check if the connection is working or not by taking a message and pass it from one PC to another one and check the status if it is successful or not.



Practical 10

Aim: Experiments on Transport Layer.

FTP (File Transfer Protocol) is a network protocol for transmitting files between computers over Transmission Control Protocol/Internet Protocol (TCP/IP) connections. Although many file transfers can be conducted using Hypertext Transfer Protocol (HTTP) -- another protocol in the TCP/IP suite -- FTP is still commonly used to transfer files behind the scenes for other applications, such as banking services.

FTP is a client-server protocol that relies on two communications channels between the client and server: a command channel for controlling the conversation and a data channel for transmitting file content.

Here is how a typical FTP transfer works:

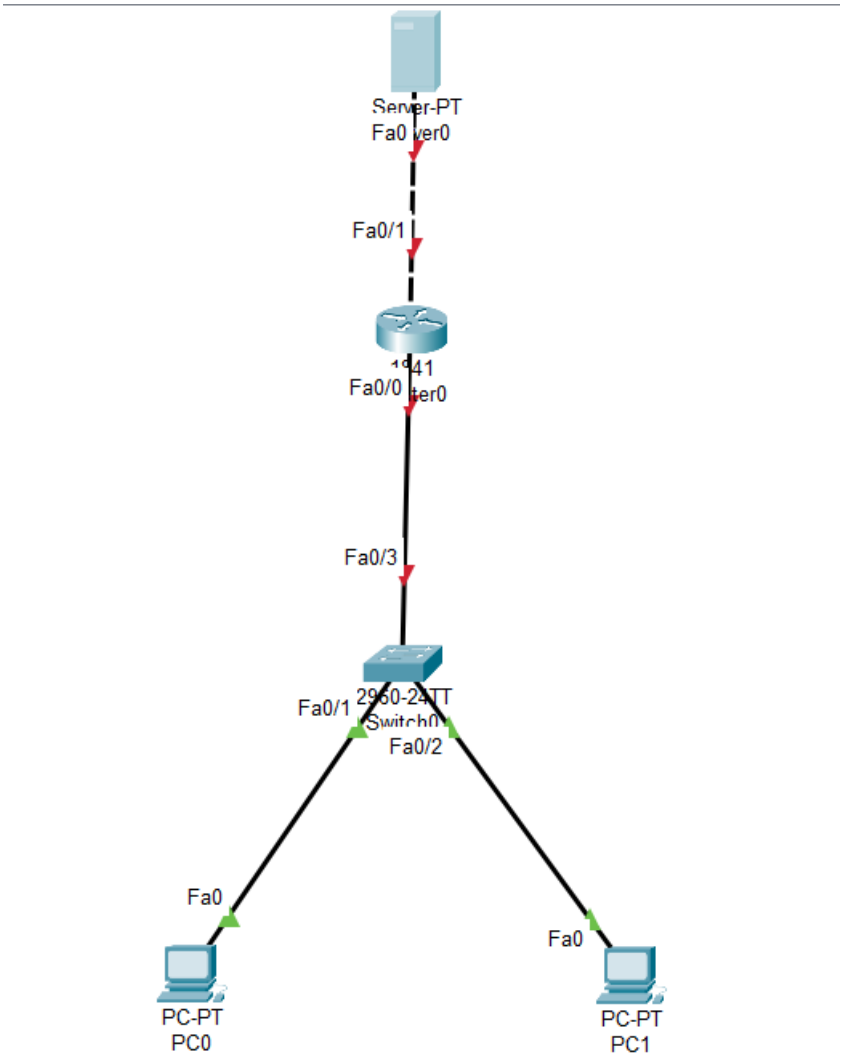
- A user typically needs to log on to the FTP server, although some servers make some or all of their content available without a login, a model known as anonymous FTP.
- The client initiates a conversation with the server when the user requests to download a file.
- Using FTP, a client can upload, download, delete, rename, move and copy files on a server.

FTP sessions work in active or passive modes:

1. Active mode. After a client initiates a session via a command channel request, the server creates a data connection back to the client and begins transferring data.
2. Passive mode. The server uses the command channel to send the client the information it needs to open a data channel. Because passive mode has the client initiating all connections, it works well across firewalls and network address translation gateways.

Implementation of FTP:

Step 1: Create a network by using a server, a router, a switch and 2 PCs.



Step 2: Configure the components as follows.

Router0 - FastEthernet 0/1 – 10.10.10.1

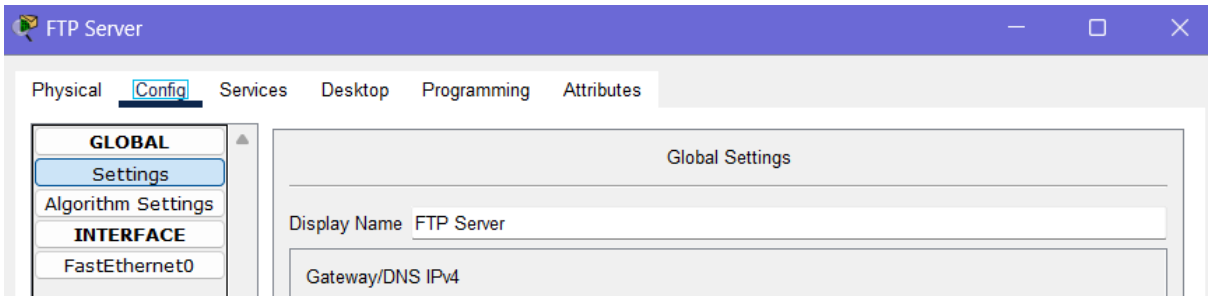
Router0 - FastEthernet 0/0 – 192.168.0.1

PC0 – IP Address – 192.168.0.2 and Default Gateway – 192.168.0.1

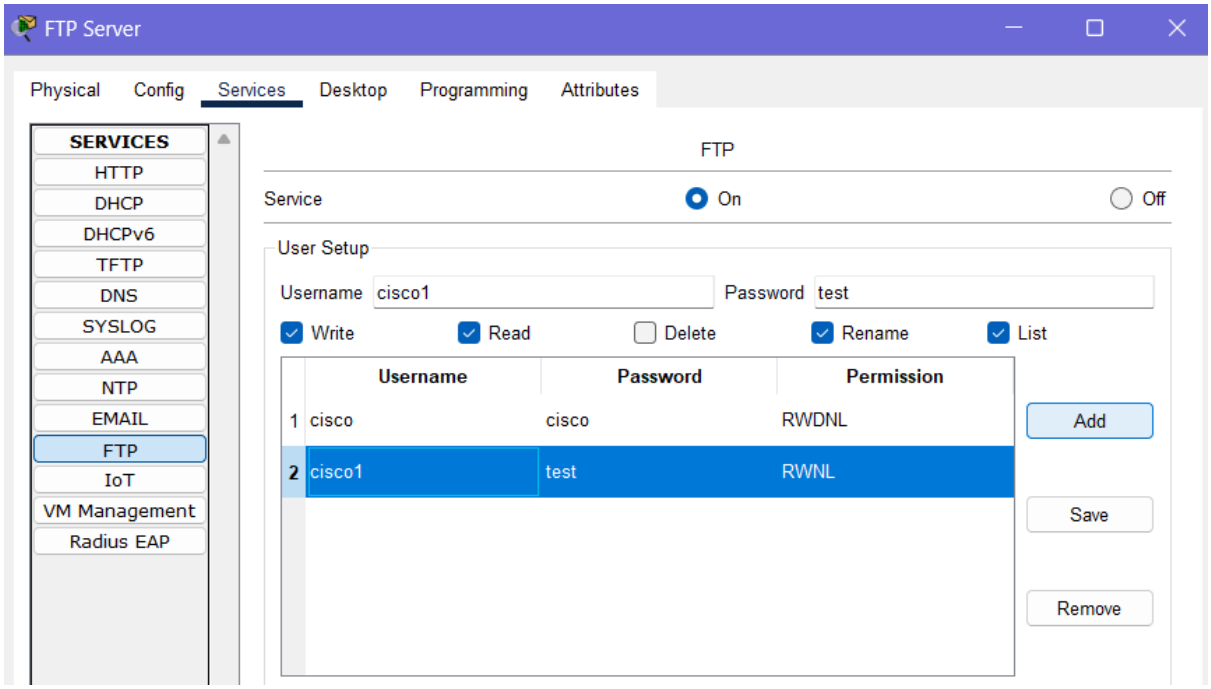
PC1 – IP Address – 192.168.0.3 and Default Gateway – 192.168.0.1

Server – IP Address - 10.10.10.2 and Default Gateway – 10.10.10.1

Step 3: Click on Server. Click on “Config”. Click on “Settings”. Click on “Display Name”. Change the name “FTP Server”.



Step 4: Click on “Services”. Click on “FTP”. In “Username”, write *cisco1*. In “Password”, write *test*. Tick on “Write”, “Read”, “Rename”, “List”. Click “Add”.



Step 5: Click on PC1 => Desktop => Text Editor. Write “Hi”. Save this with filename.txt.

Step 6:

Click on “Command Prompt” of PC1.

Type the command - **Ping 10.10.10.2** and Press “Enter”.

Now type username and password and Press “Enter”.

After login, Type the command – **ftp > put hello.txt** and Press “Enter”.

For checking, ftp>dir.