Experiment – 1

Objective: To Create Cross-Over and straight through cable.
Apparatus required (Software): Cisco packet Tracer

Flow Chart:

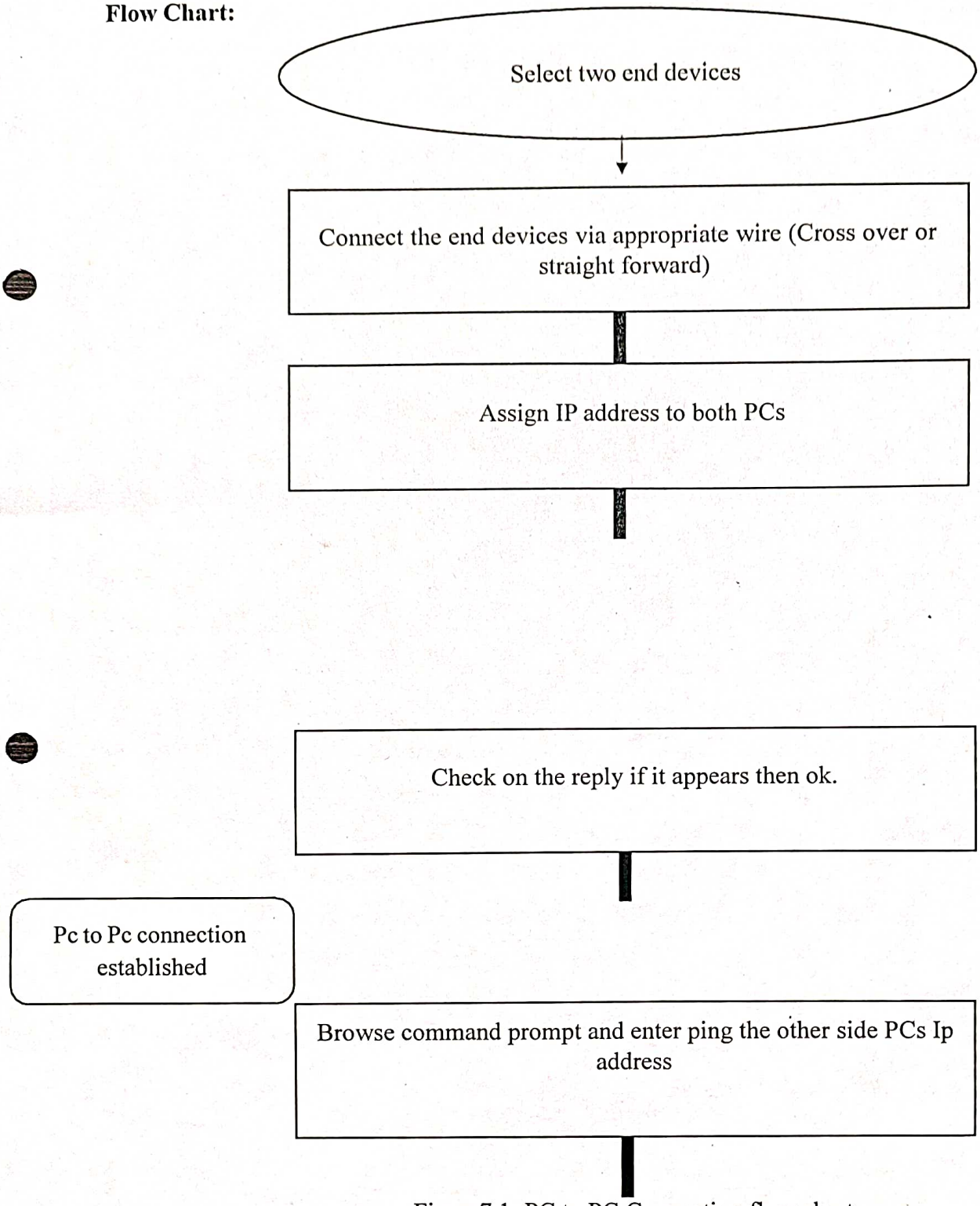


Figure7.1: PC to PC Connection flow chart

Procedure:

Step1: Select two end devices (PC, laptop, etc)

Move the cursor to the left corner of environment window and select the option after click on end device PC0 and PC1.

Step2: Connect the end devices via appropriate wire (Cross over or straight forward)

Take straight forward wire and connect switch with PCs through switch. Take cross over wire to directly connect with other PC.

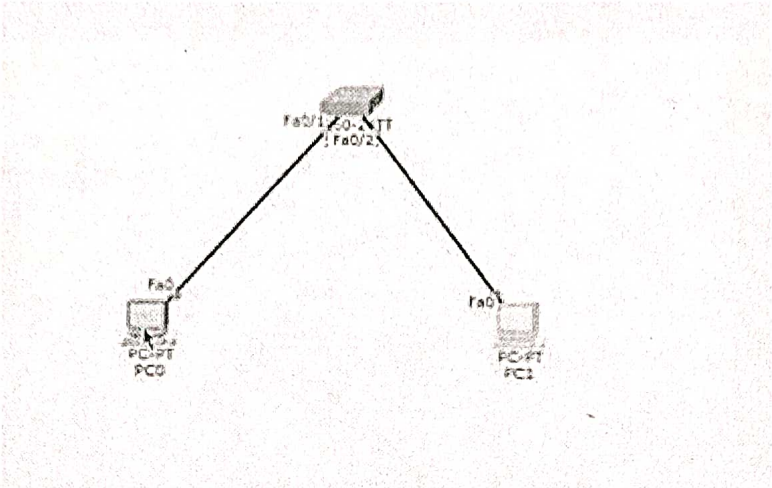


Figure 7.2 Straight Forward connection for 2 PCs

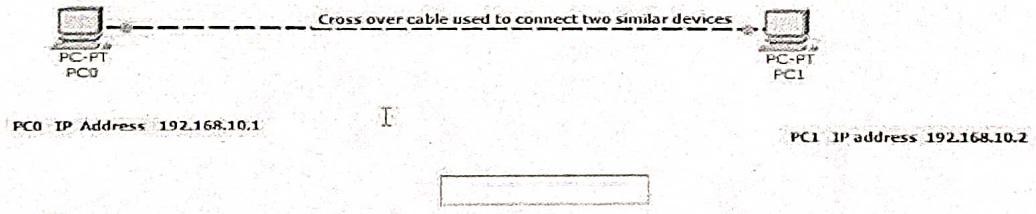


Figure 7.3 Cross over connection for 2 PCs

Step3: Assign IP address to both PCs

Give Ip address to both PCs after going on desktop on each.

Step4: Browse command prompt and enter ping the other side PCs Ip address

Go to command prompt of any one of PCs and then enter command Ping IP address of other PCS.

Step5: Check on the reply if it appears then ok.

After entering ping if reply shows then connection successfully established.

Result- Both PCs are connected successfully.

Experiment No - 2

Objective: Study & Implementation of Network IP and Sub netting
Apparatus (Software): NA
Procedure: Following is required to be study under this practical.
Classification of IP address
As show in figure we teach how the ip addresses are classified and when they are used.

Class Address Range Supports Class A
1.0.0.1 to 126.255.255.254 Supports 16 million hosts on each of 127 networks.
Class B
Class C 128.1.0.1 to 191.255.255.254 Supports 65,000 hosts on each of 16,000 networks.
Class D
Class E 192.0.1.1 to 223.255.254.254 Supports 254 hosts on each of 2 million networks.
to 239.255.255.255 Reserved for multicast groups.

240.0.0.0 to 254.255.255.254 Reserved.

SUB NETTING

Subnetting is a process of dividing large network into the smaller networks based on layer 3 IP address. Every computer on network has an IP address that represent its location on network. Two version of IP addresses are available IPv4 and IPv6. In this article we will perform subnetting on IPv4.
IPv4
IP addresses are displayed in dotted decimal notation, and appear as four numbers separated by dots. Each number of an IP address is made from eight individual bits known as octet. Each octet can create number value from 0 to 255. An IP address would be 32 bits long in binary divided into the two components, network component and host component. Network component is used to identify the network that the packet is intend for, and host component is used to identify the individual host on network. IP addresses are broken into the two components:

Network component: - Defines network segment of device.
Host component: - Defines the specific device on a particular network segment
IP Classes in decimal notation
Class A addresses range from 1-126
Class B addresses range from 128-191
Class C addresses range from 192-223
Class D addresses range from 224-
239 Class E addresses range from
240-254

- 0 [Zero] is reserved and represents all IP addresses.
- 127 is a reserved address and is used for testing, like a loop back on an interface.
- 255 is a reserved address and is used for broadcasting purposes.

This tutorial is the second part of our article "Network Addressing Explained with Subnetting and VLSM". You can read other parts of this article here.

Basic of Network Addressing

This tutorial is the first part of this article. In this introductory part I explained how computers find each other in network with basic terminology of network addressing.

VLSM Tutorial with Examples

This tutorial is the last part of this article. In this part I will explain VLSM in detail with examples. Later I will provide a unique six steps method of VLSM that will help you in learning VLSM rapidly.

Subnet mask

Subnet mask is a 32 bits long address used to distinguish between network address and host address in IP address. Subnet mask is always used with IP address. Subnet mask has only one purpose, to identify which part of an IP address is network address and which part is host address.

For example how will we figure out network partition and host partition from IP address 192.168.1.10 ? Here we need subnet mask to get details about network address and host address.

- In decimal notation subnet mask value 1 to 255 represent network address and value 0 [Zero] represent host address.
- In binary notation subnet mask ON bit [1] represent network address while OFF bit[0] represent host address.

In decimal notation

IP address 192.168.1.10

Subnet mask 255.255.255.0

Network address is 192.168.1 and host address is 10.

In binary notation

IP address 11000000.10101000.00000001.00001010

Subnet mask 11111111.11111111.11111111.00000000

Network address is 11000000.10101000.00000001 and host address is 00001010

IP Class	Default Subnet	Network bits	Host bits	Total hosts	Valid hosts
A	255.0.0.0	First 8 bits	Last 24 bits	16, 777, 216	16, 777, 214
B	255.255.0.0	First 16 bits	Last 16 bits	65,536	65,534
C	255.255.255.0	First 24 bits	Last 8 bits	256	254

Network ID

First address of subnet is called network ID. This address is used to identify one segment or broadcast domain from all the other segments in the network.

Block Size

Block size is the size of subnet including network address, hosts addresses and broadcast address.

Broadcast ID

There are two types of broadcast, direct broadcast and full broadcast.
Direct broadcast or local broadcast is the last address of subnet and can be hear by all hosts in subnet.
Full broadcast is the last address of IP classes and can be hear by all IP hosts in network. Full broadcast address is 255.255.255.255
The main difference between direct broadcast and full broadcast is that routers will not propagate local broadcasts between segments, but they will propagate directed broadcasts.

Host Addresses

All address between the network address and the directed broadcast address is called host address for the subnet. You can assign host addresses to any IP devices such as PCs, servers, routers, and switches.

Program:

```
void main()
{ inta,b,c,d; clrscr(); printf("enter
the first octet"); scanf("%d",&a);
printf("\n"); printf("enter the
second octet"); scanf("%d",&b);
printf("\n"); printf("enter the
third octet"); scanf("%d",&c);
printf("\n"); printf("enter the
fourth octet");
scanf("%d",&d);              printf("\n");
if((a<=127)) {
printf("enterdip address belong to class A\n");
printf("network address of given ip address is %d.0.0.0",a);
}
else if((a>127)&&(a<=191))
{
printf("entered ip address belong to class B\n");
printf("network address of given ip address is %d.%d.0.0",a,b);
}
else if((a>191)&&(a<=223))
{
printf("entered ipadress belong to class C\n");
printf("network address of given ip address is %d.%d.%d.0",a,b,c);
}
else if((a>223)&&(a<=241))
{ printf("entered ip address belong to class
D\n");

printf("network address of given ip address is useed for reserved");
}
```

```
else if((a>241)&&(a<=255))
{
printf("entered ipadress belong to E\n"); printf("network address of
given ip address is used for multicasting");

} else {
printf("please enter the valid ip address\n");
}

getch(); }
```

Output:

- enter the first octet 123 enter the second octet 233 enter the third octet 12 enter the fourth octet 34 entered ip address belong to class A network address of given ip address is 123.0.0.0

Experiment-3

Objective: Connection of Computer in LAN & Configuration of router, hub, switch etc using simulators.
Apparatus: Cisco Packet Tracer

Procedure:

Configuration of Hub using Star Topology

Step 1:- Open Cisco packet Tracer Software and choose Generic Hub on workspace.

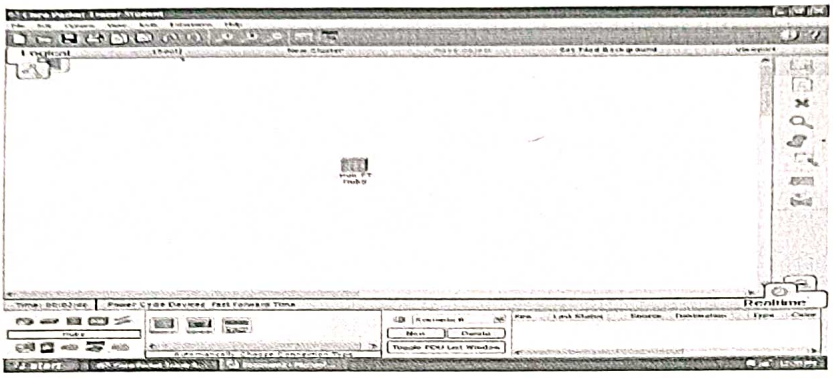


Figure 2.1: Generic Hub

Step 2:- Now choose end device as Generic. Connect end devices with Hub (Choose automatic connection type).

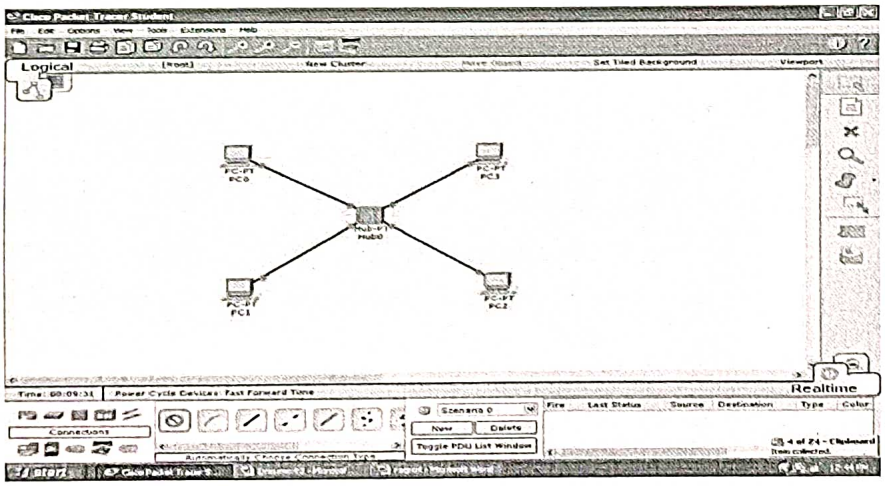


Figure 1: End devices connected with Hub

Step 3 :- Now click on each end device and enter IP address such as 10.0.0.1 and label the device with corresponding IP address using text tool available in cisco packet tracer.

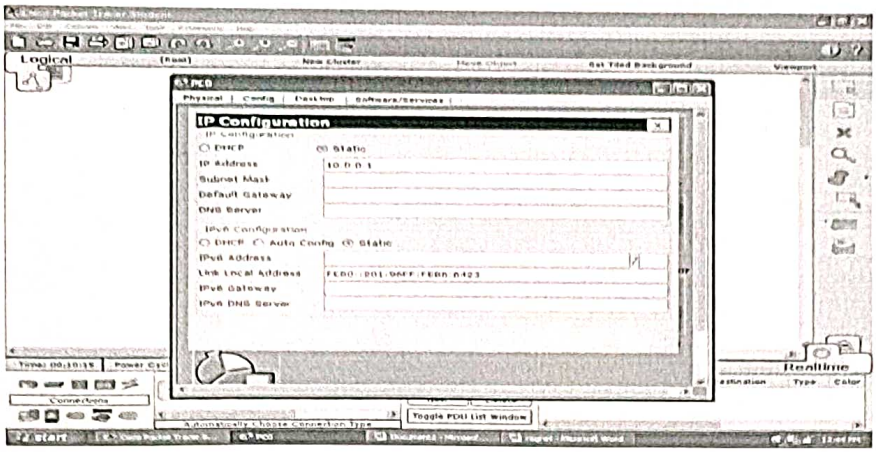


Figure 2.2: IP configuration of devices

Step 4:- Now select Simple Message(PDU) from right side of window and click over sender node and on receiver node.

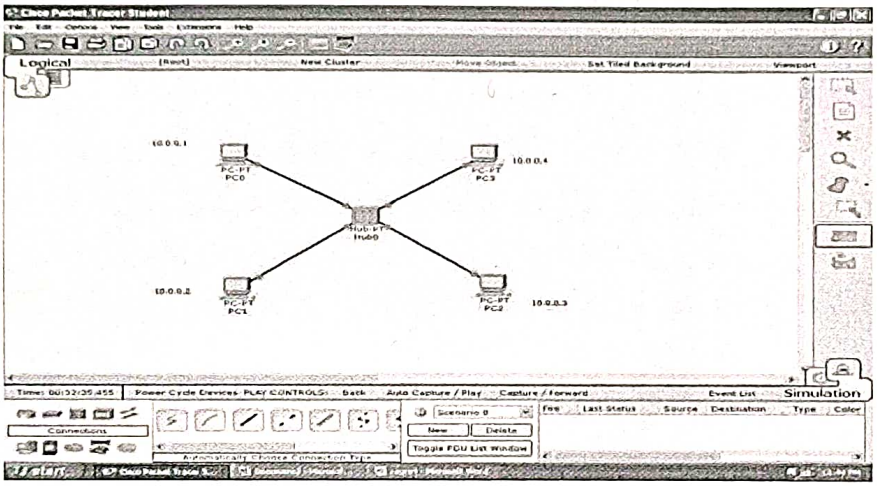


Figure 2.3: Selection of PDU

Step 5: Now click on simulation and click on AutoPlay to see effect.

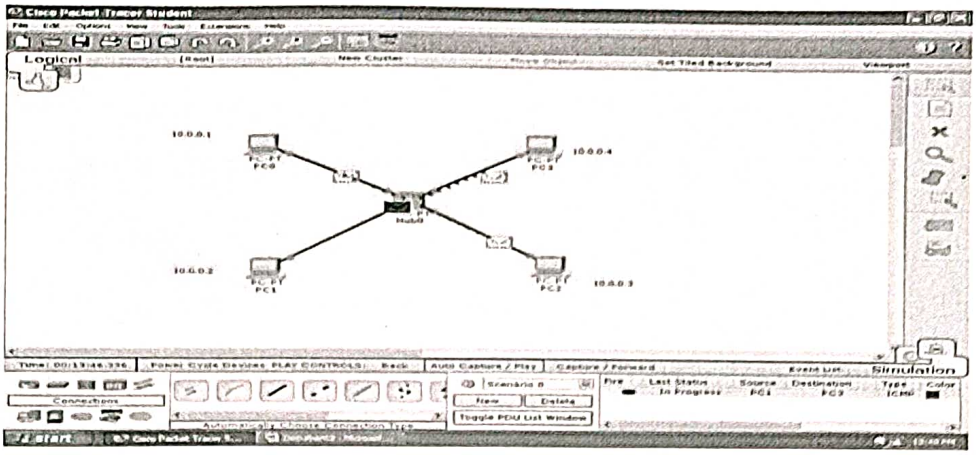


Figure 2.4: Simulation results

Configuration of Switch using Star Topology

Step 1:- Open Cisco packet Tracer Software and choose Generic Switch on workspace.

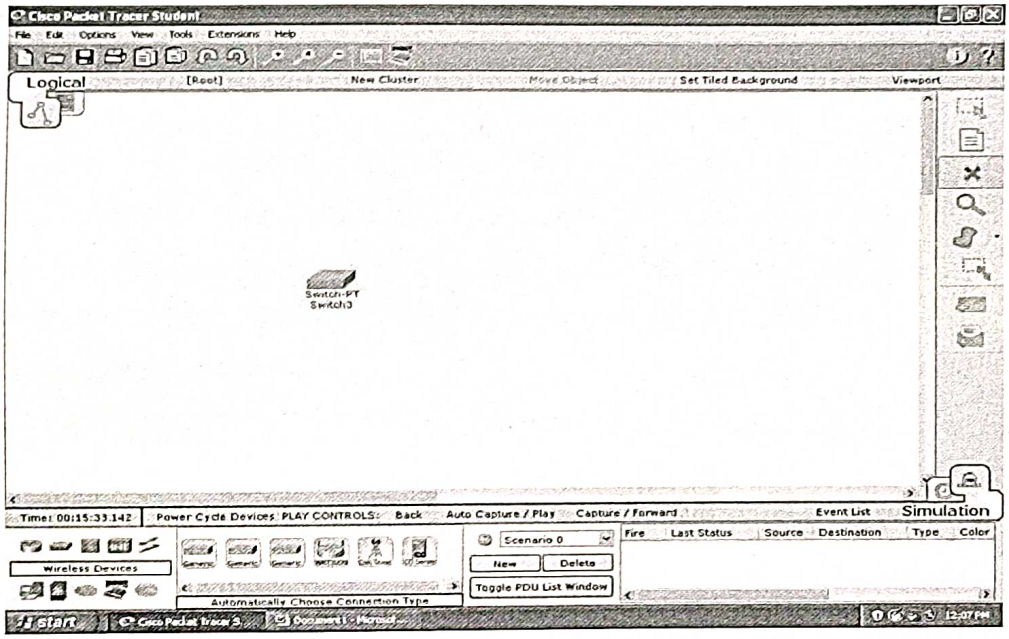


Figure 2.5:Generic Switch

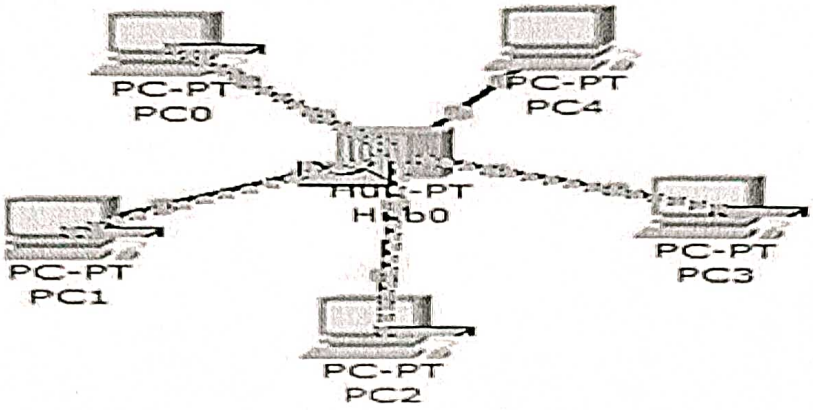


Fig16:Step16

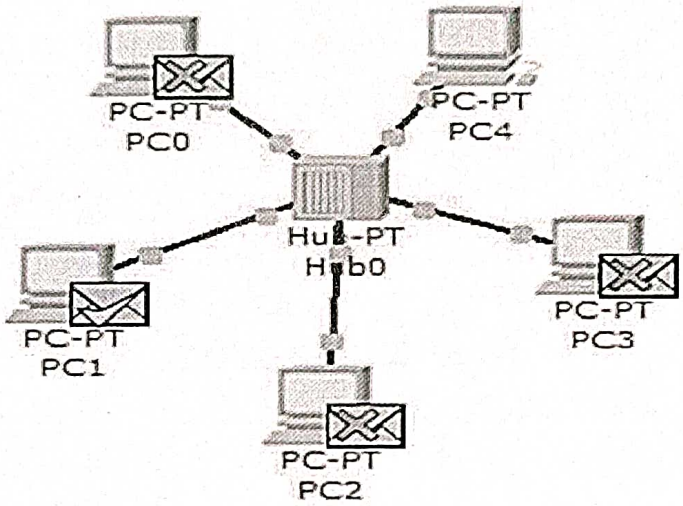


Fig17:Step17

Experiment-4

Objective: Running and using services/commands like ping, trace route, telnet, ftp etc.
Apparatus (Software): Command Prompt and Cisco Packet Tracer.

Procedure: In this experiment students must understand basic networking commands e.g. ping, tracert etc.

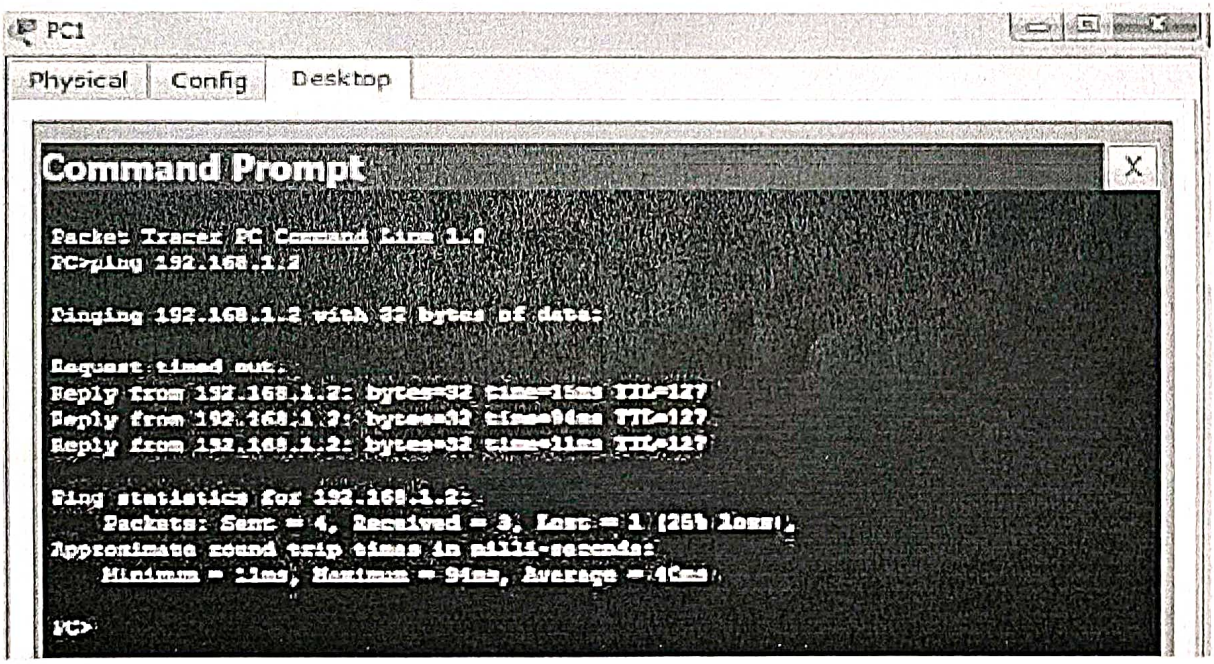
All commands related to Network configuration which includes how to switch to privilege mode and normal mode and how to configure router interface and how to save this configuration to flash memory or permanent memory. This commands includes

• Configuring the Router commands • General Commands to configure network • Privileged Mode commands of a router • Router Processes & Statistics • IP Commands • Other IP Command e.g. show ip route etc.

ping:

Verifies IP-level connectivity to another TCP/IP computer by sending Internet Control Message Protocol (ICMP) Echo Request messages. The receipt of corresponding Echo Reply messages is displayed, along with round-trip times. Ping is the primary TCP/IP command used to troubleshoot connectivity, reachability, and name resolution.

You can use ping to test both the computer name and the IP address of the computer. If pinging the IP address is successful, but pinging the computer name is not, you might have a name resolution problem. In this case, ensure that the computer name you are specifying can be resolved through the local Hosts file, by using Domain Name System (DNS) queries, or through NetBIOS name resolution techniques.



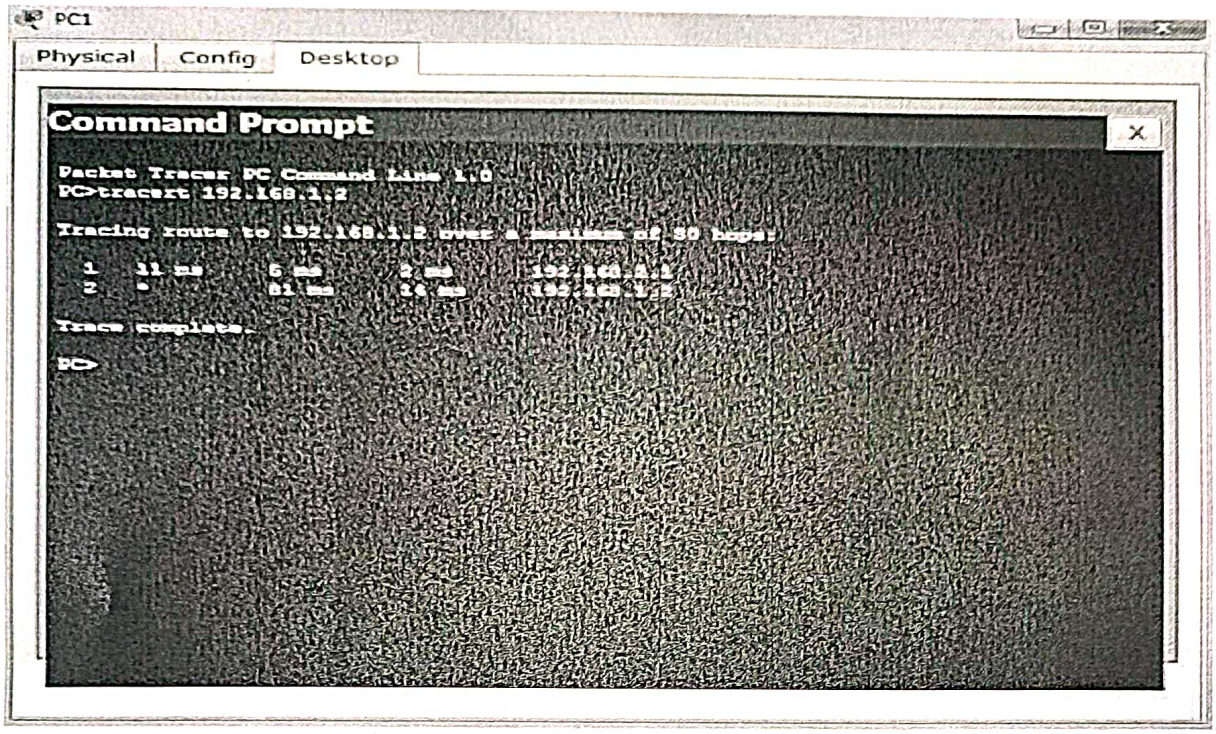
Traceroute:

Determines the path taken to a destination by sending Internet Control Message Protocol (ICMP) Echo Request messages to the destination with incrementally increasing Time to Live

(TTL) field values. The path displayed is the list of near-side router interfaces of the routers in the path between a source host and a destination. The near-side interface is the interface of the

router that is closest to the sending host in the path. Used without parameters, tracert displays help.
To trace the path to the host named www.google.co.in use following command tracert

www.google.co.in

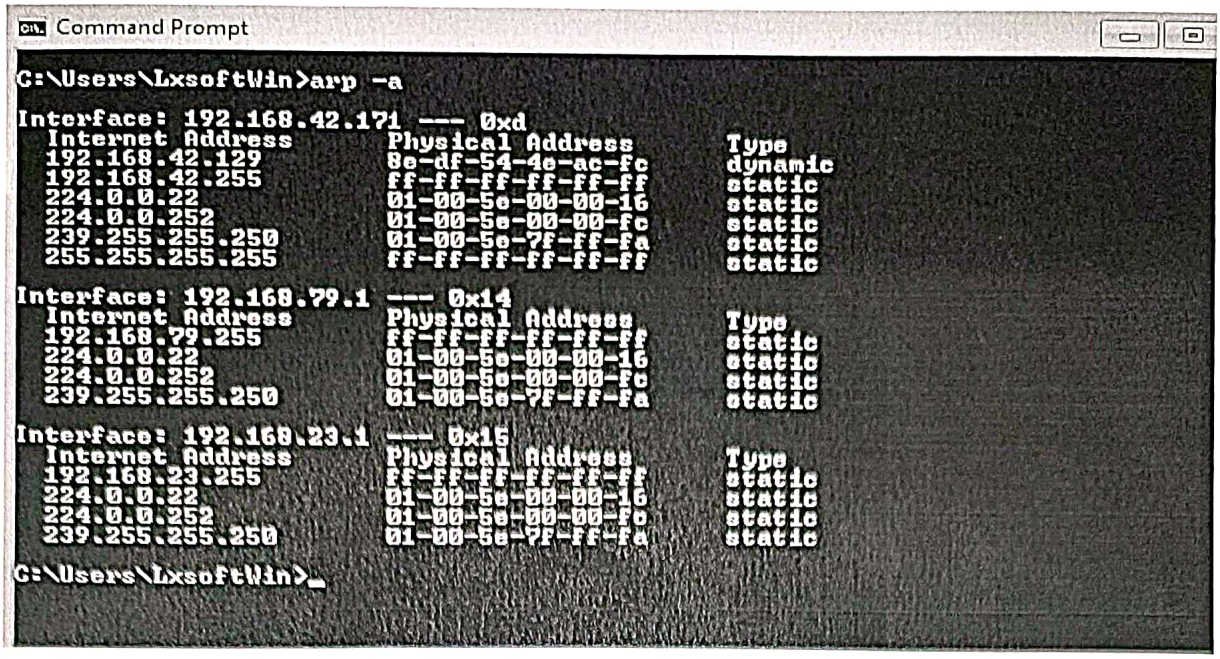


Arp

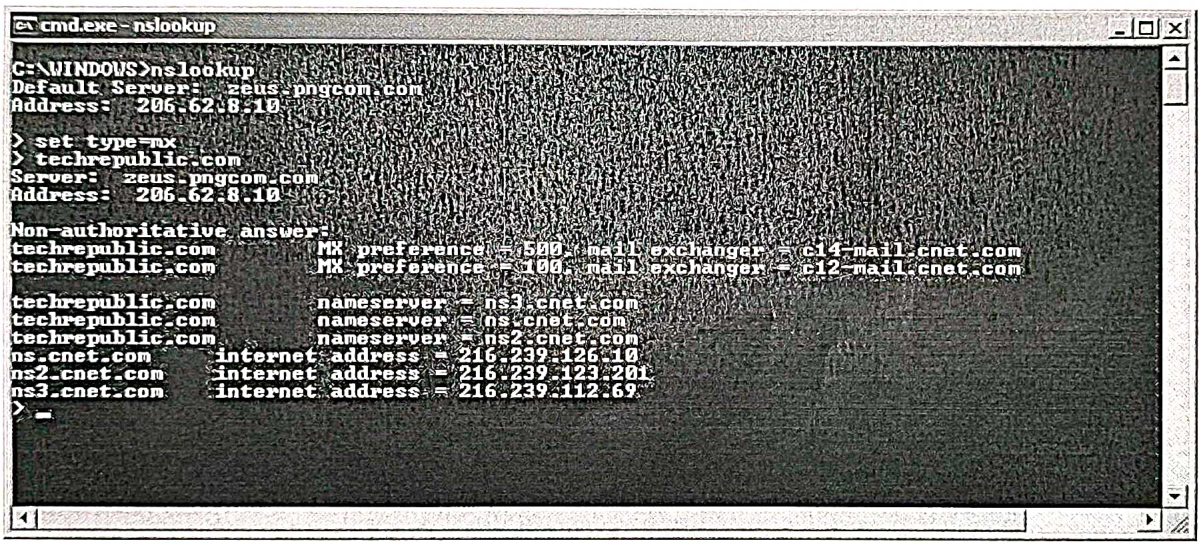
Displays and modifies entries in the Address Resolution Protocol (ARP) cache, which contains one or more tables that are used to store IP addresses and their resolved Ethernet or Token Ring physical addresses. There is a separate table for each Ethernet or Token Ring network adapter installed on your computer.

To display the ARP cache tables for all interfaces use following command arp

-a



Nslookup (stands for "Name Server Lookup") is a useful command for getting information from DNS server. It is a network administration tool for querying the Domain Name System (DNS) to obtain domain name or IP address mapping or any other specific DNS record. It is also used to troubleshoot DNS related problems.



EXPERIMENT 5

OBJECTIVE : Configure a network topology using Packet Tracer Software.

BRIEF DESCRIPTION : In this experiment, the objective is to design and configure a network topology using Packet Tracer software. The network will consist of multiple devices such as routers, switches, and PCs, connected in a specific arrangement. The experiment will focus on implementing static routing within the network. Static routing involves manually configuring the routing tables on the routers, specifying the next hop for each destination network. This allows for explicit control over the network traffic flow.

STEPS FOR HANDLING NETWORK :

1. Design the Network Topology:
    - Identify the devices required for your network, such as routers, switches, and PCs.
    - Determine the logical layout of your network, including the IP addressing scheme for each subnet. Use Packet Tracer's device palette to drag and drop the necessary devices onto the workspace.
    - Connect the devices using appropriate cables and configure their interfaces with IP addresses.
2. Configure IP Addresses:
    - Access the CLI (Command Line Interface) of each device (e.g., router or PC) in Packet Tracer.
    - Configure the IP addresses for the interfaces of each device according to the logical layout you designed.
    - Use the "ip address" command followed by the desired IP address and subnet mask to assign IP addresses to the interfaces.
3. Enable Routing:
    - Determine the routing protocol or method you want to use (in this case, static routing).
    - Access the CLI of each router in Packet Tracer.
    - Configure static routes on each router to direct traffic to the appropriate destination networks.
    - Use the "ip route" command followed by the destination network address, subnet mask, and next-hop router's IP address to configure static routes.
4. Verify Connectivity:
    - Use Packet Tracer's simulation mode to test network connectivity.

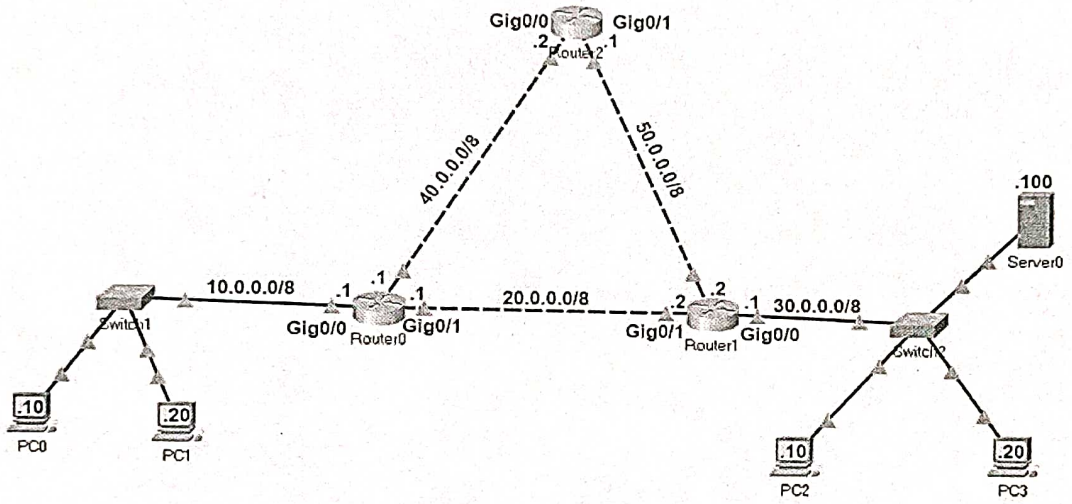
- Ping from one device to another to verify that the static routes are correctly configured.
- Ensure that the ICMP (Internet Control Message Protocol) traffic is allowed through any firewalls or security features on the devices.

5. Monitor and Troubleshoot:
   - Monitor the network for any issues or errors.
   - If any connectivity or routing problems arise, use Packet Tracer's logging and debugging features to troubleshoot.
   - Check the routing tables on each router to ensure that the correct static routes are present.
6. Document the Configuration:

Document the network topology, including the IP addresses assigned to each device and the configured static routes.

- Take screenshots or export the configuration files from Packet Tracer for reference purposes.

EXPRIMENT SETUP : Design network topology



In this lab, each network has two routes to reach. We will configure one route as the main route and another route as the backup route. If the link bandwidth of all routes is the same, we use the route that has the least number of routers as the main route. If the link bandwidth and the number of routers are the same, we can use any route as the main route and another route as the backup route. If we specify two routes for the same destination, the router automatically selects the best route for the destination and adds the route to the routing table. If you manually want to select a route that the router should add to the routing table, you have to set the AD value of the route lower than other

routes. For example, if you use the following commands to create two static routes for network 30.0.0/8, the route will place the first route to the routing table.

```
#ip route 30.0.0.0 255.0.0.0 20.0.0.2 10
#ip route 30.0.0.0 255.0.0.0 40.0.0.2 20
```

Creating, adding, verifying static routes :

Routers automatically learn their connected networks. We only need to add routes for the networks that are not available on the router's interfaces. For example, network 10.0.0.0/8, 20.0.0.0/8 and 40.0.0.0/8 are directly connected to Router0. Thus, we don't need to configure routes for these networks. Network 30.0.0.0/8 and network 50.0.0.0/8 are not available on Router0. We have to create and add routes only for these networks.

The following table lists the connected networks of each router.

Router	Available networks on local interfaces	Networks available on other routers' interfaces
Router0	10.0.0.0/8, 20.0.0.0/8, 40.0.0.0/8	30.0.0.0/8, 50.0.0.0/8
Router1	20.0.0.0/8, 30.0.0.0/8, 50.0.0.0/8	10.0.0.0/8, 40.0.0.0/8
Router2	40.0.0.0/8, 50.0.0.0/8	10.0.0.0/8, 20.0.0.0/8, 30.0.0.0/8

Router1 configuration

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip route 10.0.0.0 255.0.0.0 20.0.0.1 10
Router(config)#ip route 10.0.0.0 255.0.0.0 50.0.0.1 20
Router(config)#ip route 40.0.0.0 255.0.0.0 20.0.0.1 10
Router(config)#ip route 40.0.0.0 255.0.0.0 50.0.0.1 20
Router(config)#exit
Router#show ip route static
S 10.0.0.0/8 [10/0] via 20.0.0.1
S 40.0.0.0/8 [10/0] via 20.0.0.1
Router#
```

Router2 configuration

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip route 10.0.0.0 255.0.0.0 40.0.0.1
Router(config)#ip route 30.0.0.0 255.0.0.0 50.0.0.2
Router(config)#exit
```

Experiment-6

Objective : Configure a Network using Distance Vector and Link State Routing protocol.
Apparatus required (Software): Cisco packet Tracer
Flow Chart:

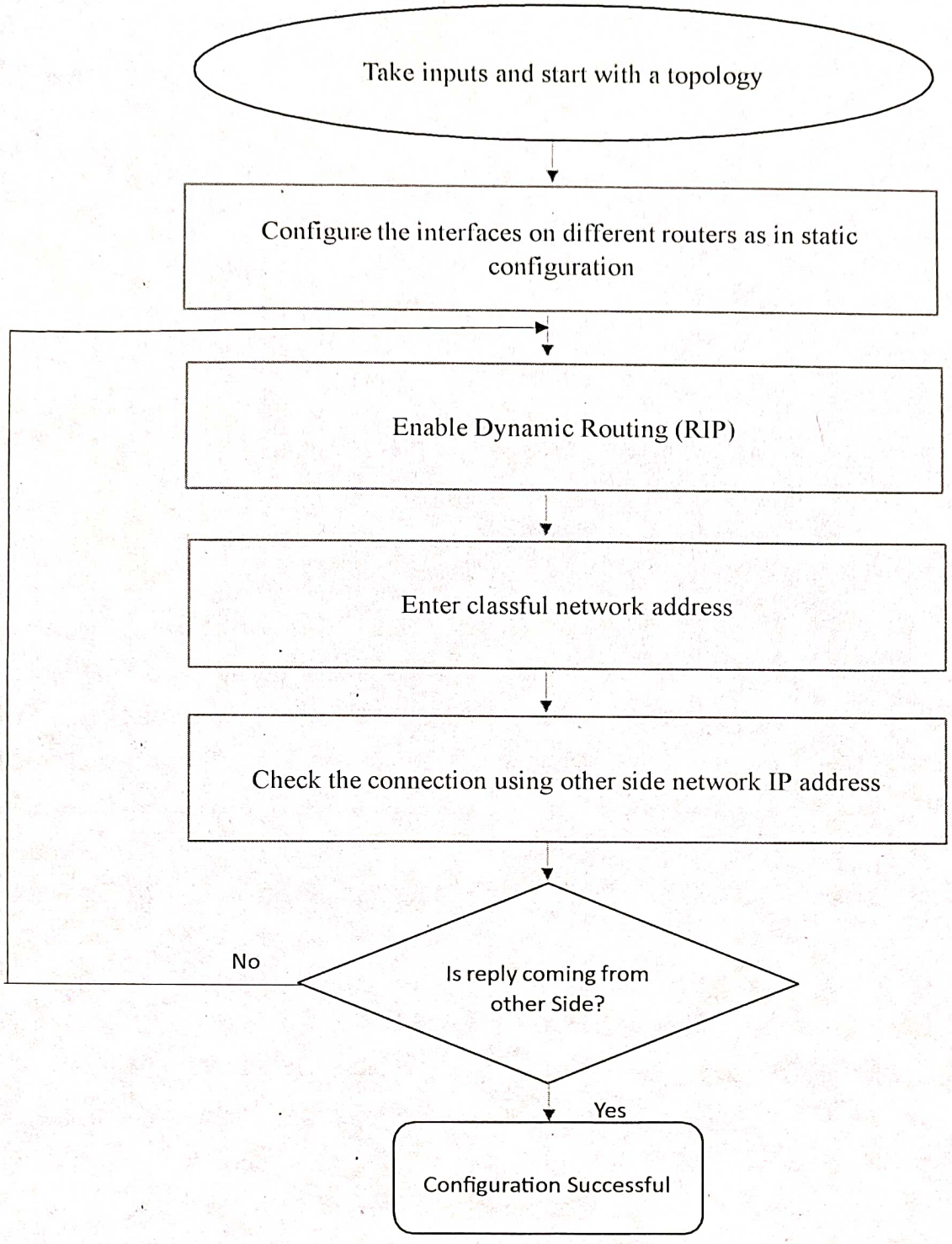


Figure. 9.1 Flow Chart for RIP configuration

Procedure: RIPv1 sends updates as broadcasts to address 255.255.255.255.

Step1: Configure the Router as per the network topology shown in figure

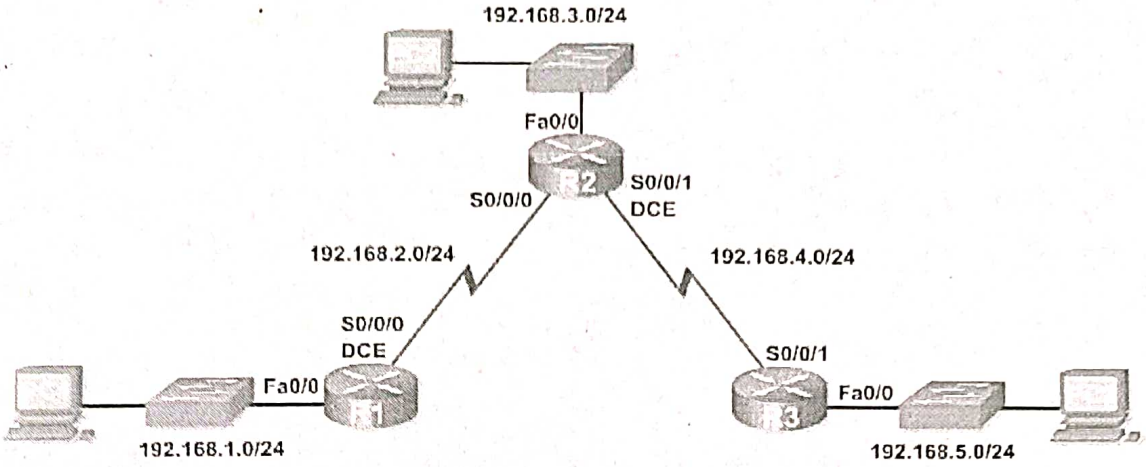


Figure. 9.2 Topology for RIP

Step 2: Configure the interfaces on R1, R2, and R3 as in static configuration.

Configure the interfaces on the R1, R2, and R3 routers with the IP addresses from the table under the Topology Diagram.

Step 3: Configure Ethernet interfaces of PC1, PC2, and PC3

Configure the Ethernet interfaces of PC1, PC2, and PC3 with the IP addresses and default gateways from under the Topology Diagram. **Step4: Enable dynamic routing**

To enable a dynamic routing protocol, enter global configuration mode and use the Router command. Enter router? at the global configuration prompt to a see a list of available routing protocols on your router.

To enable RIP, enter the command router rip in global configuration mode.

R1(config)#router rip

Step 5: Enter classful network addresses

Once We are in routing configuration mode, enter the classful network address for each directly connected network, using the network command with the following command:

R1(config-router)#network 192.168.4.0

R1(config-router)#network 192.168.5.0

Repeat the same step 4 & 5 for R2 & R3.

Step 6: Check the connection using other side network IP address

Once the network configured then go to any one PCs desktop and enters the other network address. See the output on command prompt. ping 192.168.5.0

Step 7: If the reply comes connection will be considered as successful otherwise repeat the same and troubleshoot from step 3 onward.

Input: Ip addressing, right connection and configuration commands as per procedures.