EXPERIMENT-2

Aim: To construct Peer to Peer Topology in CISCO Packet Tracer

Apparatus (Software): Packet tracer Software

Procedure: The word physical network topology is used to explain the manner in which a network is physically connected. Peer to peer is the relationship where the devices share the link equally.

Features of Peer to Peer: -

1. In peer to peer architecture every node is connected to other node directly.
2. Every computer node is referred as peer.
3. There is no need for full-time System Administrator. Every user is the administrator of his machine.

Disadvantages of Peer to peer: -

1. In this network, the whole system is decentralized thus it is difficult to administer. That is one person cannot determine the whole accessibility setting of whole network.
2. Data recovery or backup is very difficult. Each computer should have its own back-up system

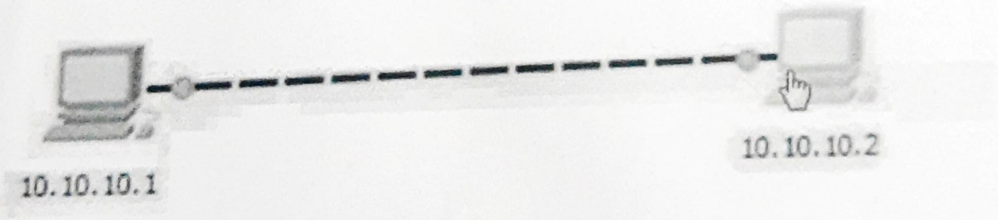
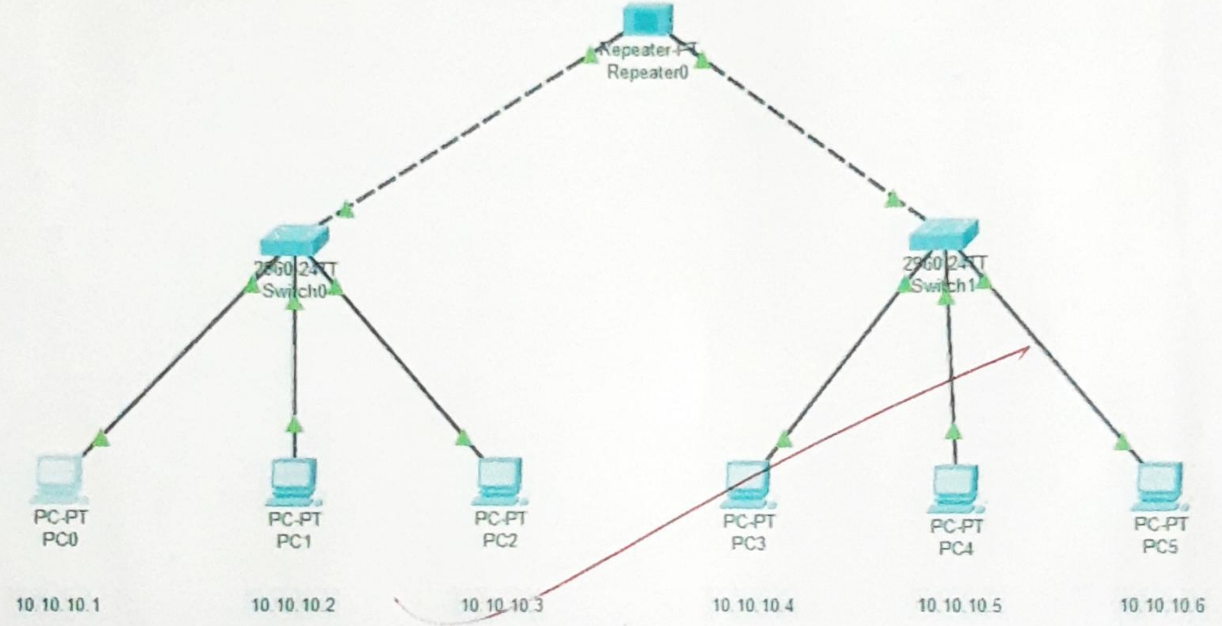


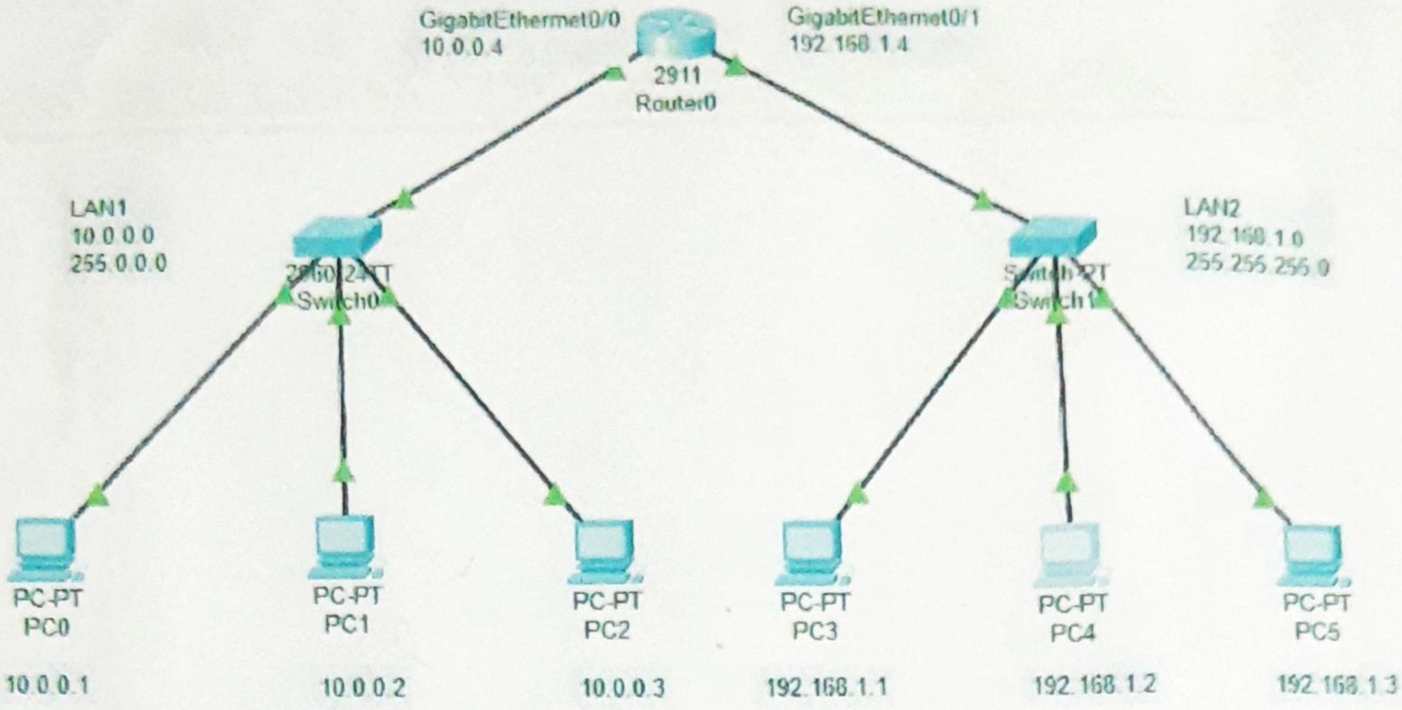
Figure: The picture show Peer to Peer Configuration

OBSERVATION: -

```
C:\>ping 10.0.0.3

Pinging 10.0.0.3 with 32 bytes of data:

Reply from 10.0.0.3: bytes=32 time<1ms TTL=127
Reply from 10.0.0.3: bytes=32 time<1ms TTL=127
Reply from 10.0.0.3: bytes=32 time<1ms TTL=127
Reply from 10.0.0.3: bytes=32 time<1ms TTL=127

Ping statistics for 10.0.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```




```
C:\>ping 10.10.10.2

Pinging 10.10.10.2 with 32 bytes of data:

Reply from 10.10.10.2: bytes=32 time<1ms TTL=128
Reply from 10.10.10.2: bytes=32 time<1ms TTL=128
Reply from 10.10.10.2: bytes=32 time<1ms TTL=128
Reply from 10.10.10.2: bytes=32 time<1ms TTL=128

Ping statistics for 10.10.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 10.10.10.3

Pinging 10.10.10.3 with 32 bytes of data:

Reply from 10.10.10.3: bytes=32 time<1ms TTL=128
Reply from 10.10.10.3: bytes=32 time<1ms TTL=128
Reply from 10.10.10.3: bytes=32 time<1ms TTL=128
Reply from 10.10.10.3: bytes=32 time<1ms TTL=128

Ping statistics for 10.10.10.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```



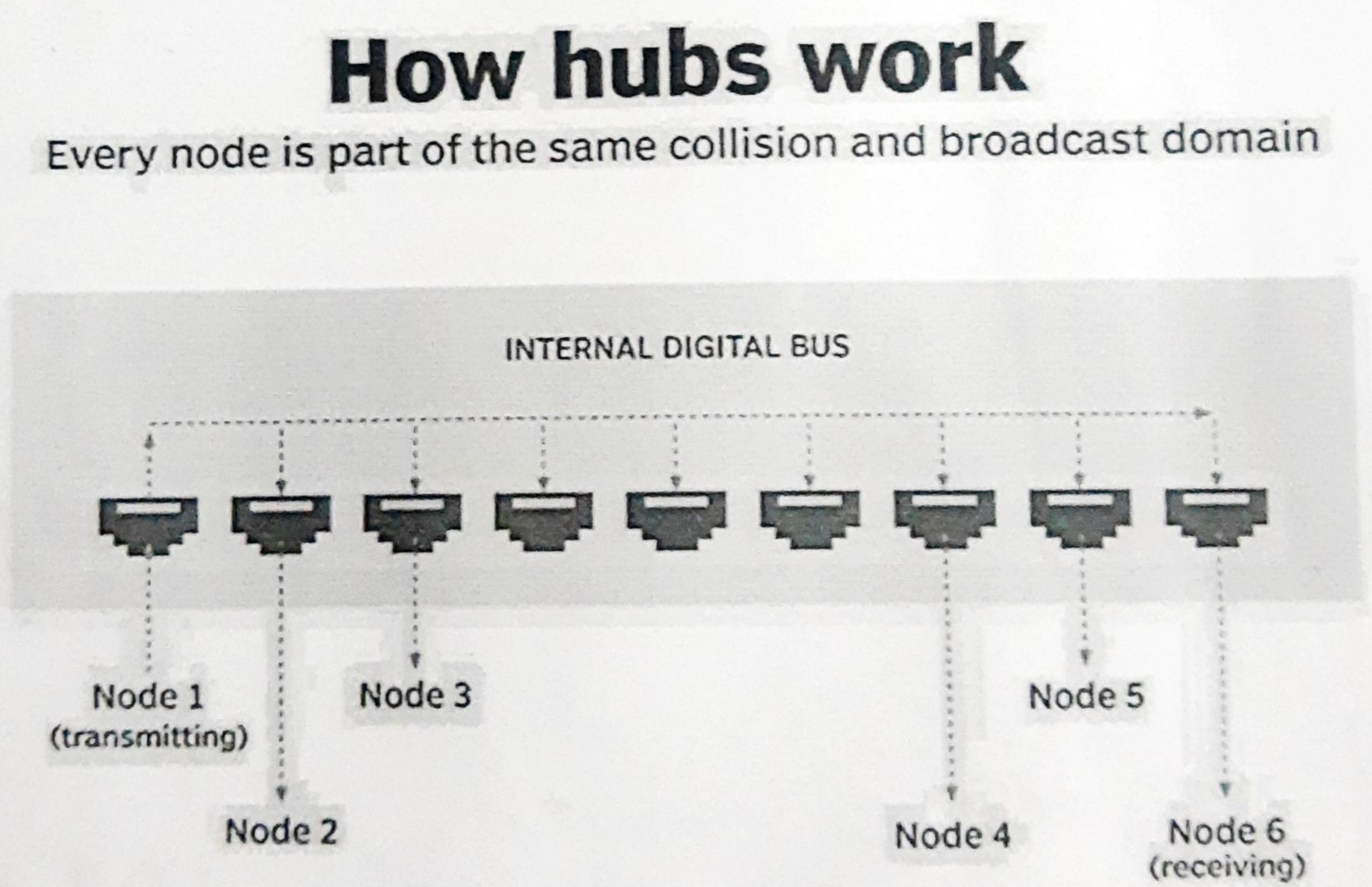

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:

Request timed out.
Reply from 10.0.0.2: bytes=32 time<1ms TTL=127
Reply from 10.0.0.2: bytes=32 time<1ms TTL=127
Reply from 10.0.0.2: bytes=32 time<1ms TTL=127

Ping statistics for 10.0.0.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:

Reply from 10.0.0.2: bytes=32 time=12ms TTL=127
Reply from 10.0.0.2: bytes=32 time<1ms TTL=127
Reply from 10.0.0.2: bytes=32 time<1ms TTL=127
Reply from 10.0.0.2: bytes=32 time=1ms TTL=127

Ping statistics for 10.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 12ms, Average = 3ms

C:\>ping 10.0.0.1

Pinging 10.0.0.1 with 32 bytes of data:

Reply from 10.0.0.1: bytes=32 time<1ms TTL=127
Reply from 10.0.0.1: bytes=32 time<1ms TTL=127
Reply from 10.0.0.1: bytes=32 time<1ms TTL=127
Reply from 10.0.0.1: bytes=32 time<1ms TTL=127

Ping statistics for 10.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

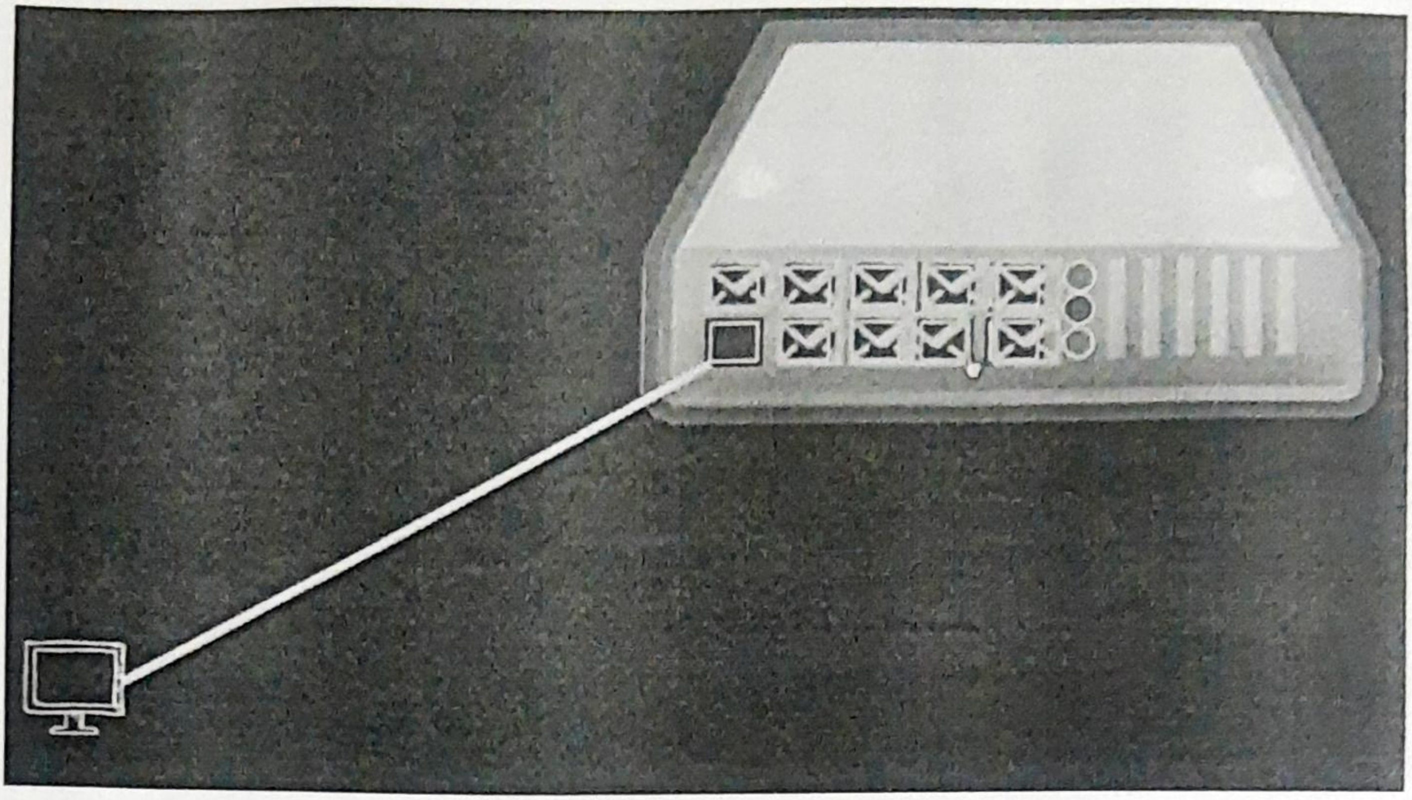
EXPERIMENT-3

Aim: To construct LAN using HUB in CISCO Packet Tracer

Apparatus (Software): Packet tracer Software

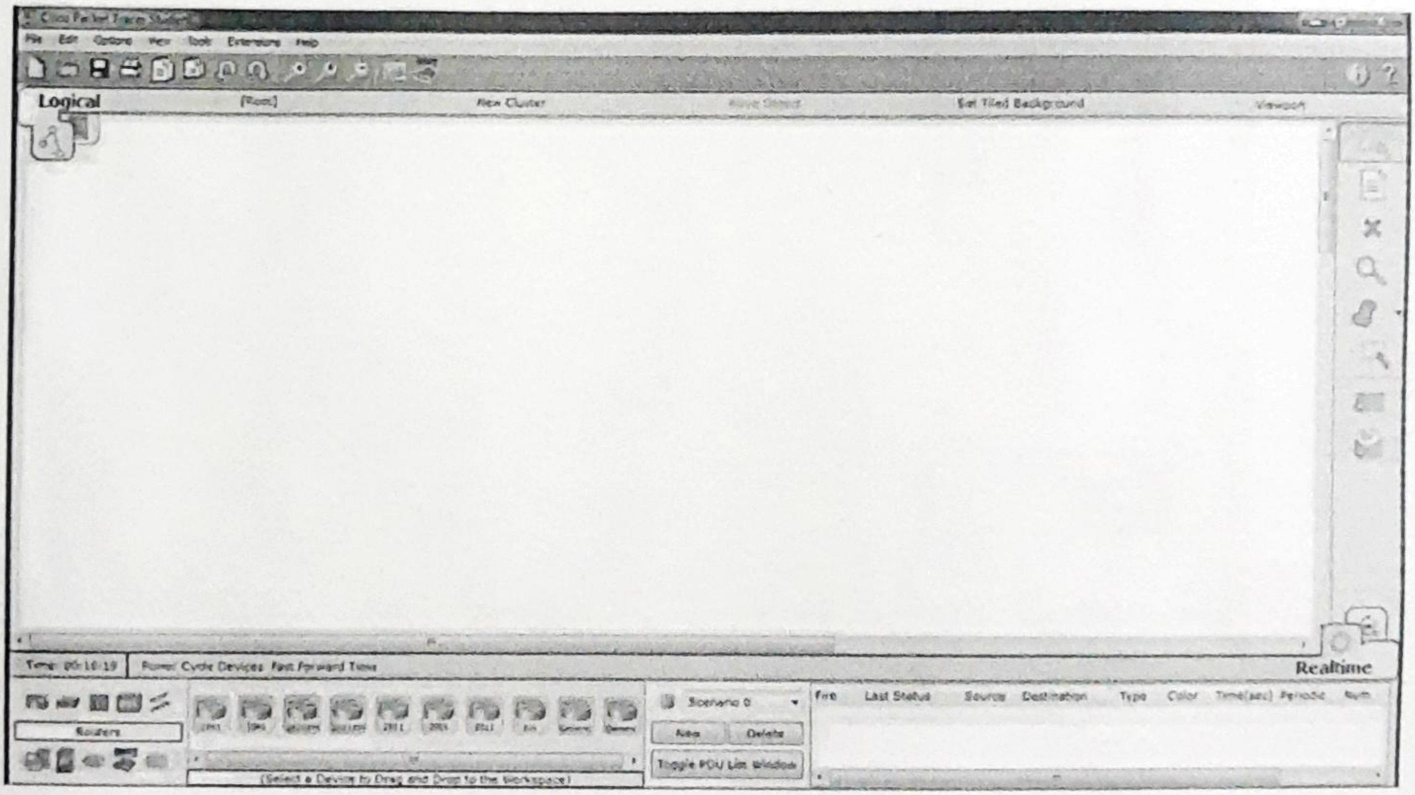
Theory: A network hub is a node that broadcasts data to every computer or Ethernet-based device connected to it. A hub is less sophisticated than a switch, the latter of which can isolate data transmissions to specific devices. Network hubs are best suited for small, simple local area network (LAN) environments. Hubs cannot provide routing capabilities or other advanced network services. Because they operate by forwarding packets across all ports indiscriminately, network hubs are sometimes referred to as "dumb switches."

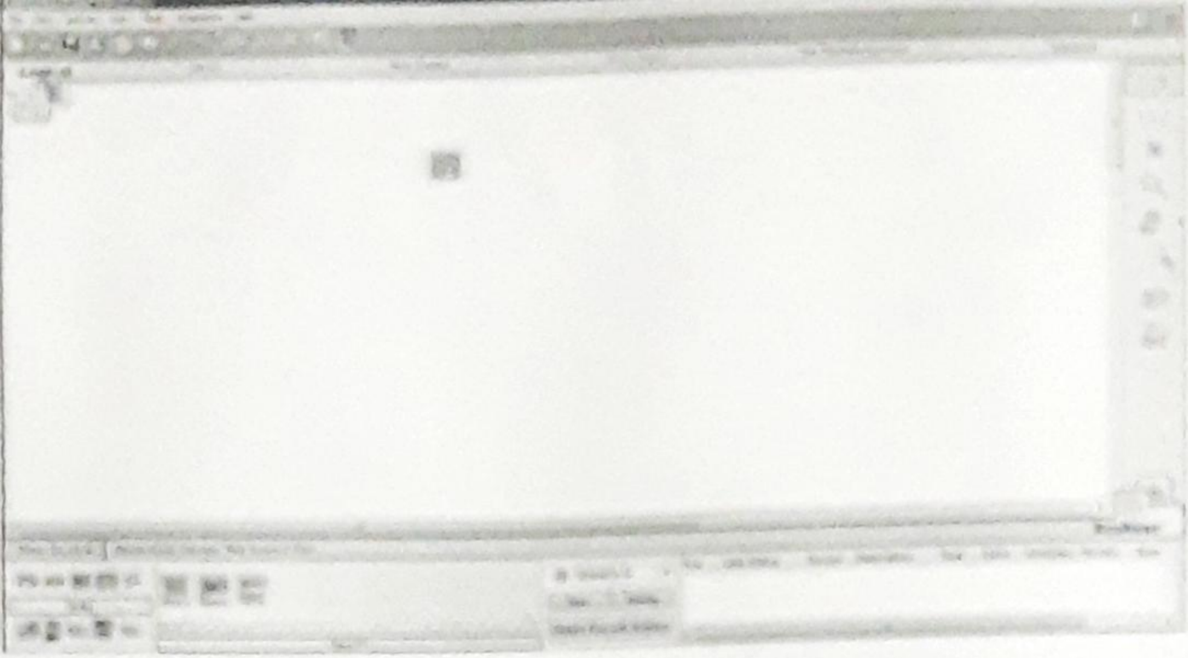




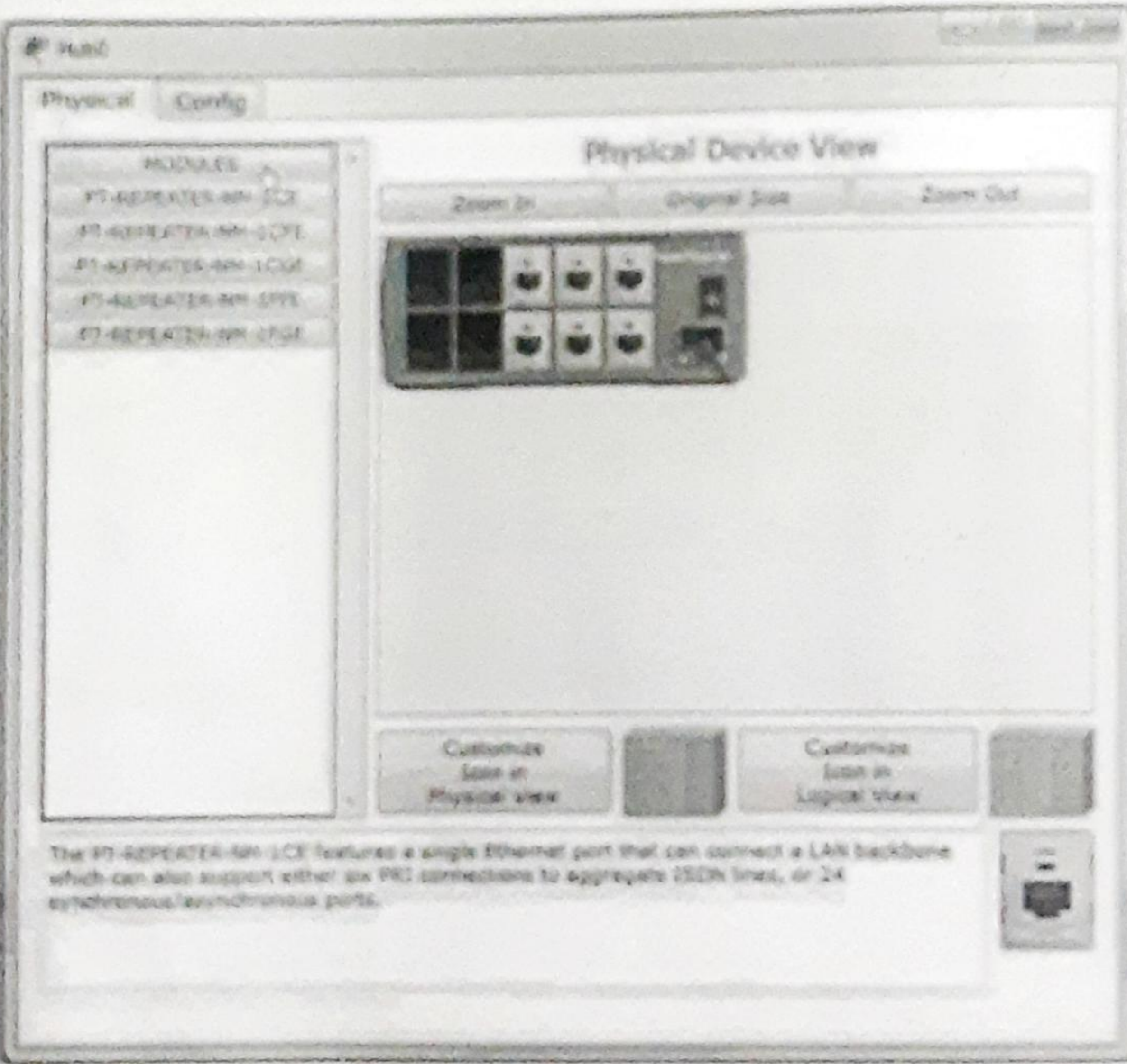
Procedure:

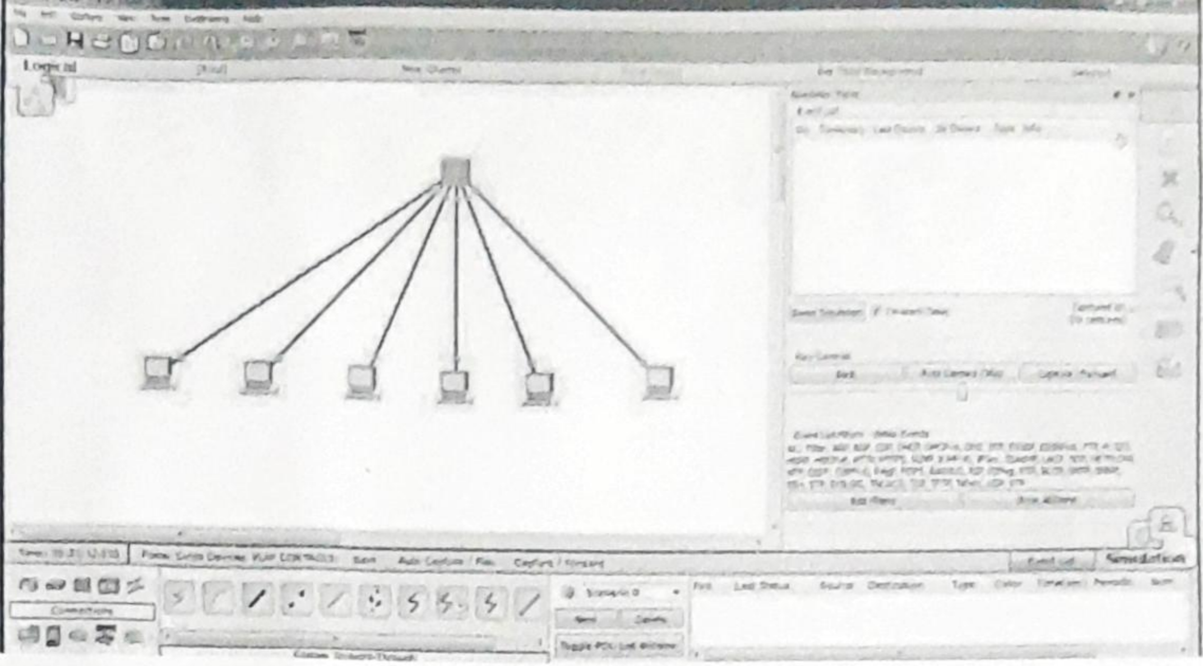
Step 1



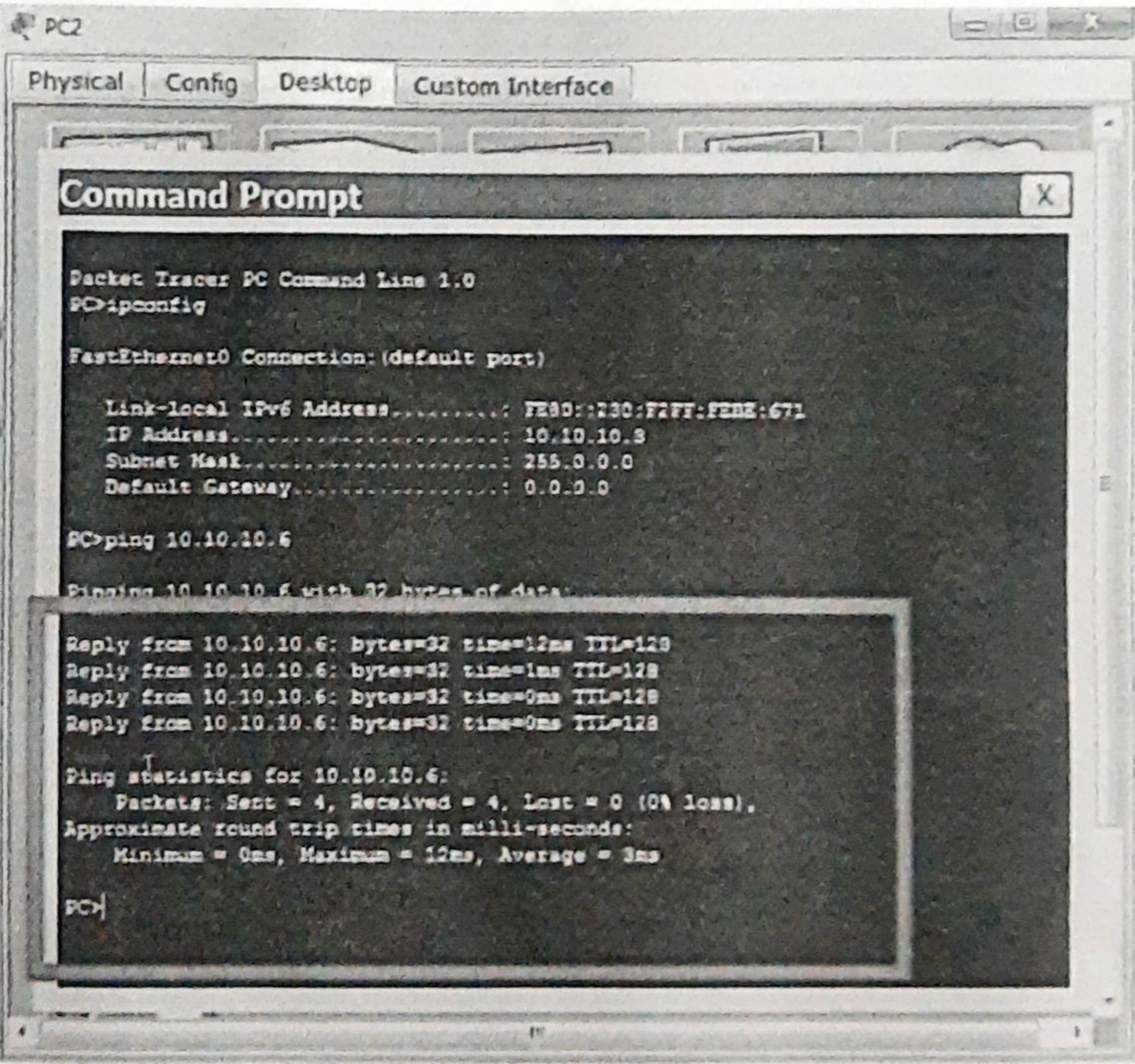


Step 3

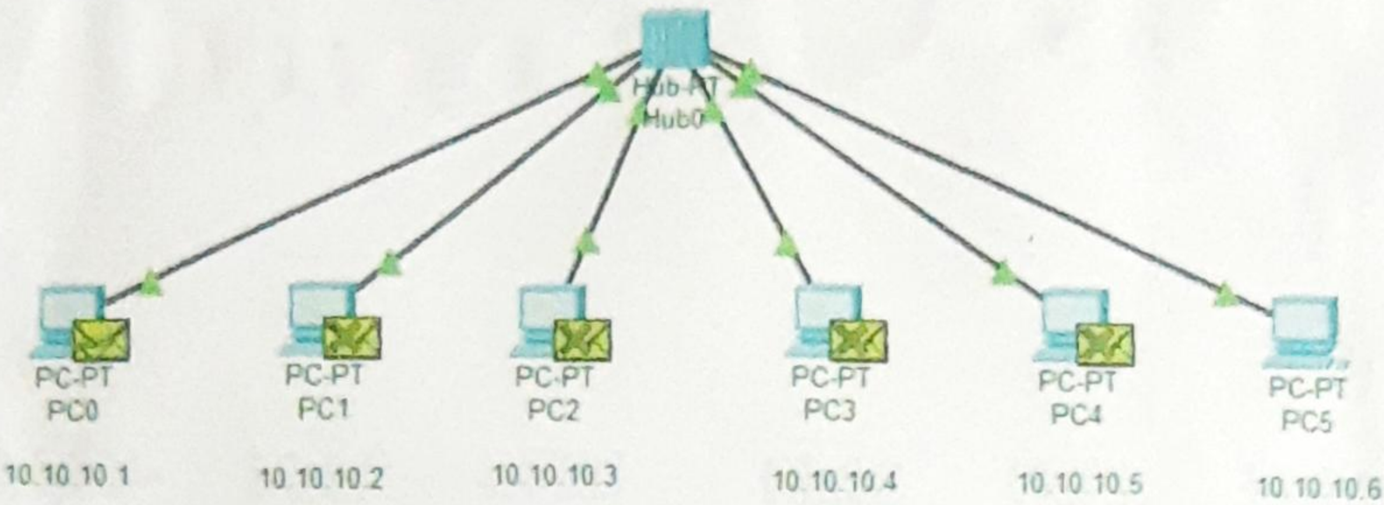

Physical
Config
MODULES
Physical Device View
Zoom In
Original Size
Zoom Out



Step 5

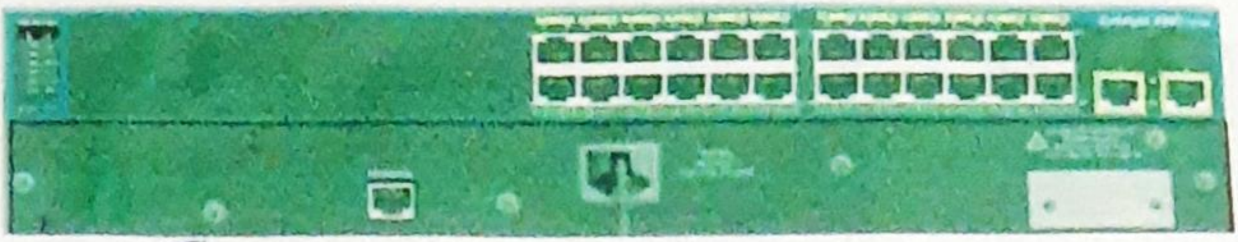


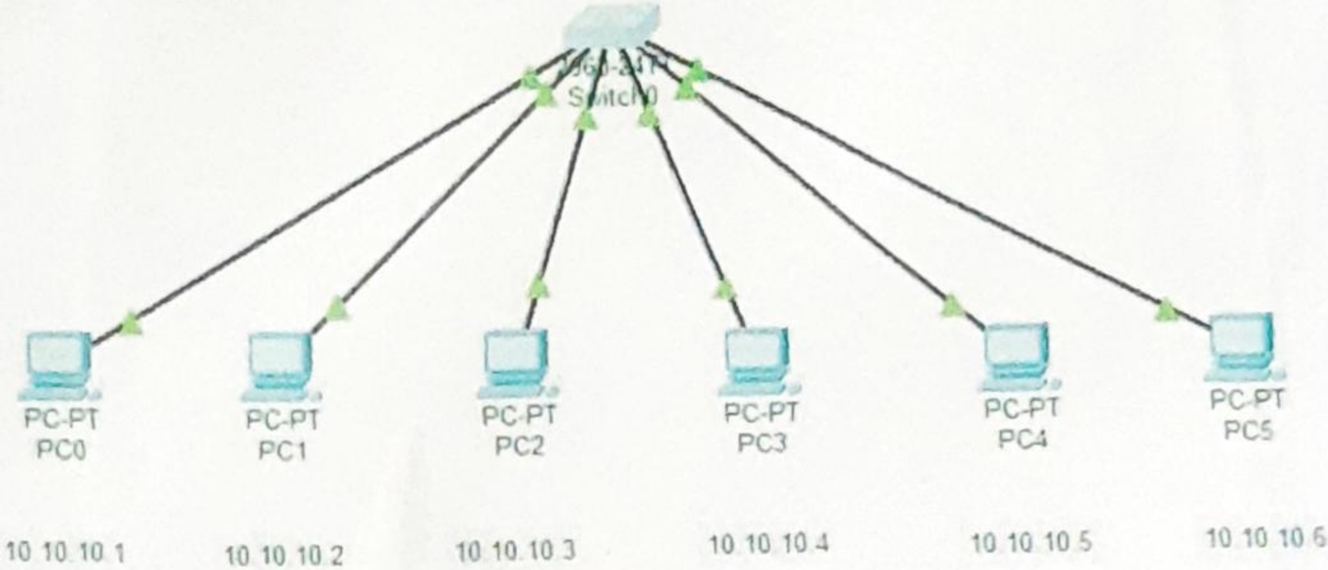
PC2
Physical
Config
Desktop
Custom Interface
Command Prompt
Packet Tracer PC Command Line 1.0
PC>ipconfig
FastEthernet0 Connection:(default port)
Link-local IPv6 Address.........: FE80::230:F2FF:FE8E:671
IP Address......................: 10.10.10.3
Subnet Mask.....................: 255.0.0.0
Default Gateway.................: 0.0.0.0
PC>ping 10.10.10.6
Pinging 10.10.10.6 with 32 bytes of data:
Reply from 10.10.10.6: bytes=32 time=12ms TTL=128
Reply from 10.10.10.6: bytes=32 time=1ms TTL=128
Reply from 10.10.10.6: bytes=32 time=0ms TTL=128
Reply from 10.10.10.6: bytes=32 time=0ms TTL=128
Ping statistics for 10.10.10.6:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 12ms, Average = 3ms
PC>




```
C:\>ping 10.10.10.6

Pinging 10.10.10.6 with 32 bytes of data:

Reply from 10.10.10.6: bytes=32 time<1ms TTL=128
Reply from 10.10.10.6: bytes=32 time<1ms TTL=128
Reply from 10.10.10.6: bytes=32 time<1ms TTL=128
Reply from 10.10.10.6: bytes=32 time<1ms TTL=128

Ping statistics for 10.10.10.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

```
C:\>ping 10.10.10.6

Pinging 10.10.10.6 with 32 bytes of data:

Reply from 10.10.10.6: bytes=32 time<1ms TTL=128
Reply from 10.10.10.6: bytes=32 time<1ms TTL=128
Reply from 10.10.10.6: bytes=32 time<1ms TTL=128
Reply from 10.10.10.6: bytes=32 time<1ms TTL=128

Ping statistics for 10.10.10.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```






```
Switch>EN
Switch#show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    000c.852b.c878    DYNAMIC     Fa0/1
   1    0090.0ca5.b774    DYNAMIC     Fa0/5
   1    0090.2b6a.427d    DYNAMIC     Fa0/3
   1    00d0.ba65.d1ae    DYNAMIC     Fa0/2
   1    00d0.d3dc.71ed    DYNAMIC     Fa0/6
   1    00e0.8f50.b1a9    DYNAMIC     Fa0/4
Switch#
```

EXPERIMENT-4

Aim: To construct LAN using switch in CISCO Packet Tracer

Apparatus (Software): Packet tracer Software

Theory: A network switch connects devices in a network to each other, enabling them to talk by exchanging data packets. Switches can be hardware devices that manage physical networks or software-based virtual devices.

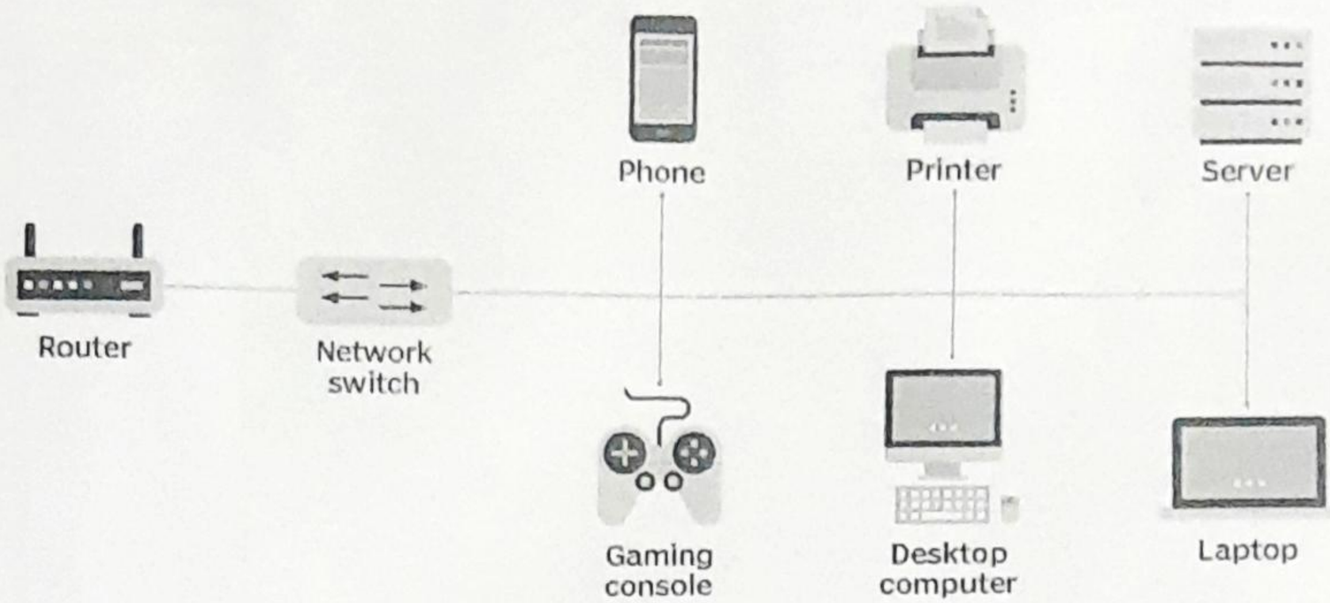
Switches form the vast majority of network devices in modern data networks. They provide the wired connections to desktop computers, wireless access points (APs), printers, industrial machinery and some internet of things devices, such as card entry systems. They connect the computers that host virtual machines (VMs) in data centers, as well as physical servers and much of the storage infrastructure. Switches carry vast amounts of traffic in telecommunications provider networks.

A network switch operates on Layer 2 of the Open Systems Interconnection (OSI) model -- the data-link layer. In a local area network (LAN) using Ethernet, a network switch determines where to send each incoming message frame by looking at the media access control (MAC) address. Switches maintain tables that match each MAC address to the port receiving the MAC address.

A network switch can be deployed in the following ways:

- Edge, or access, switches. These switches manage traffic either coming into or exiting the network. Devices like computers and APs connect to edge switches.
- Aggregation, or distribution, switches. These switches are placed within an optional middle layer in a network topology. Edge switches connect into these and send traffic from switch to switch or send it up to core switches.
- Core switches. These network switches form the backbone of the network. Core switches connect aggregation or edge switches, users or device edge networks to data center networks and enterprise LANs to routers.

How a network switch works

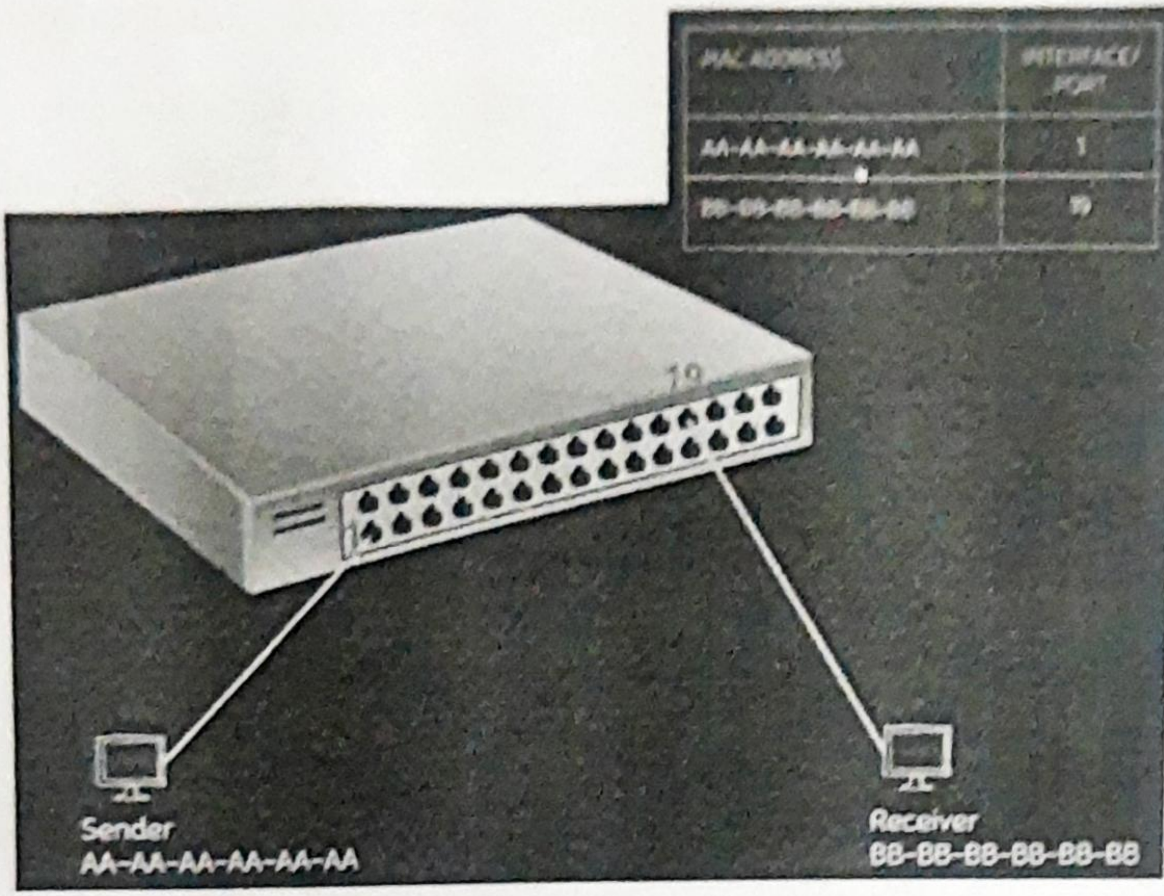


There are several types of switches in networking:

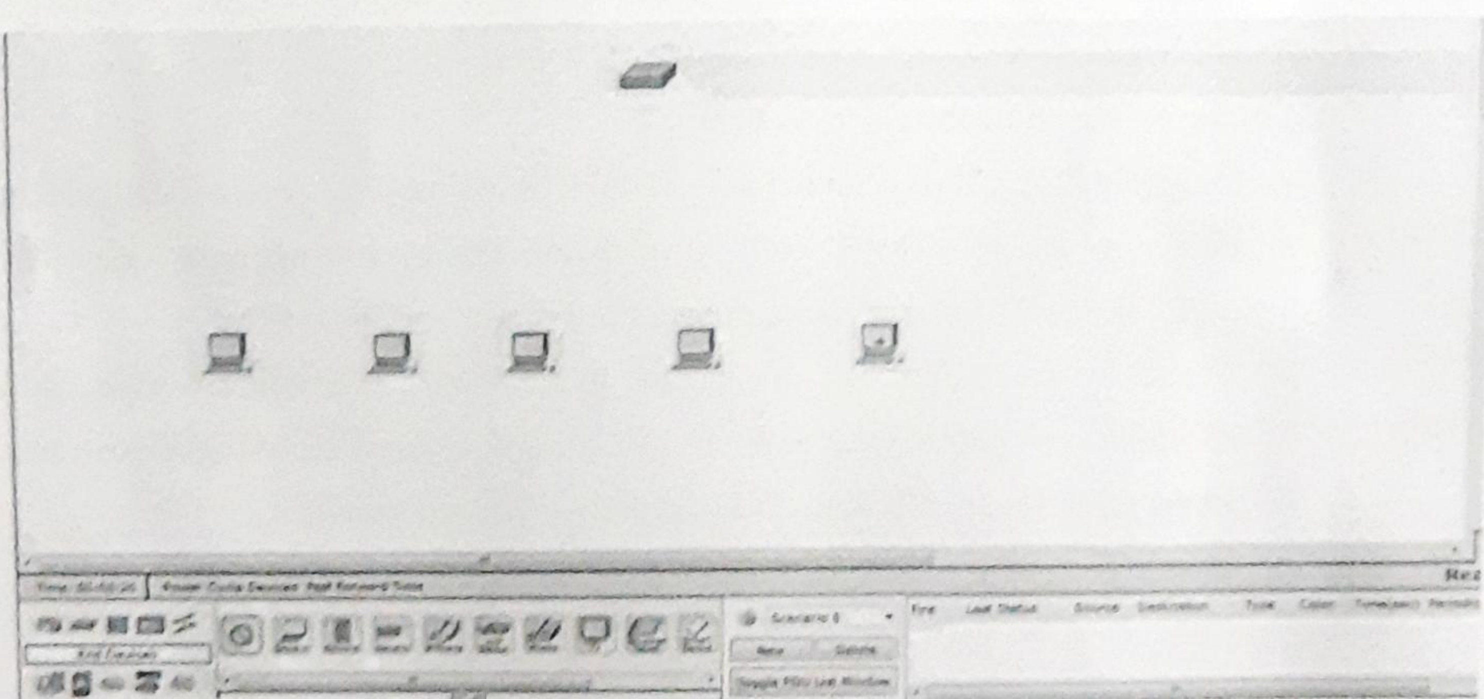
- Virtual switches are software-only switches instantiated inside VM hosting environments.
- Routing switches connect LANs. In addition to doing MAC-based Layer 2 switching, they perform routing functions at OSI Layer 3 (the network layer), directing traffic based on the Internet Protocol (IP) address in each packet.
- Managed switches let a user adjust each port on the switch. This enables monitoring and configuration changes.
- Unmanaged switches enable Ethernet devices to pass data automatically using auto negotiation, which determines parameters such as data rate. The configuration is fixed and cannot be edited.
- Smart switches can be configured to enable more control over data transmissions, but they have more limitations compared to managed switches. Smart switches are also known as partially managed switches.

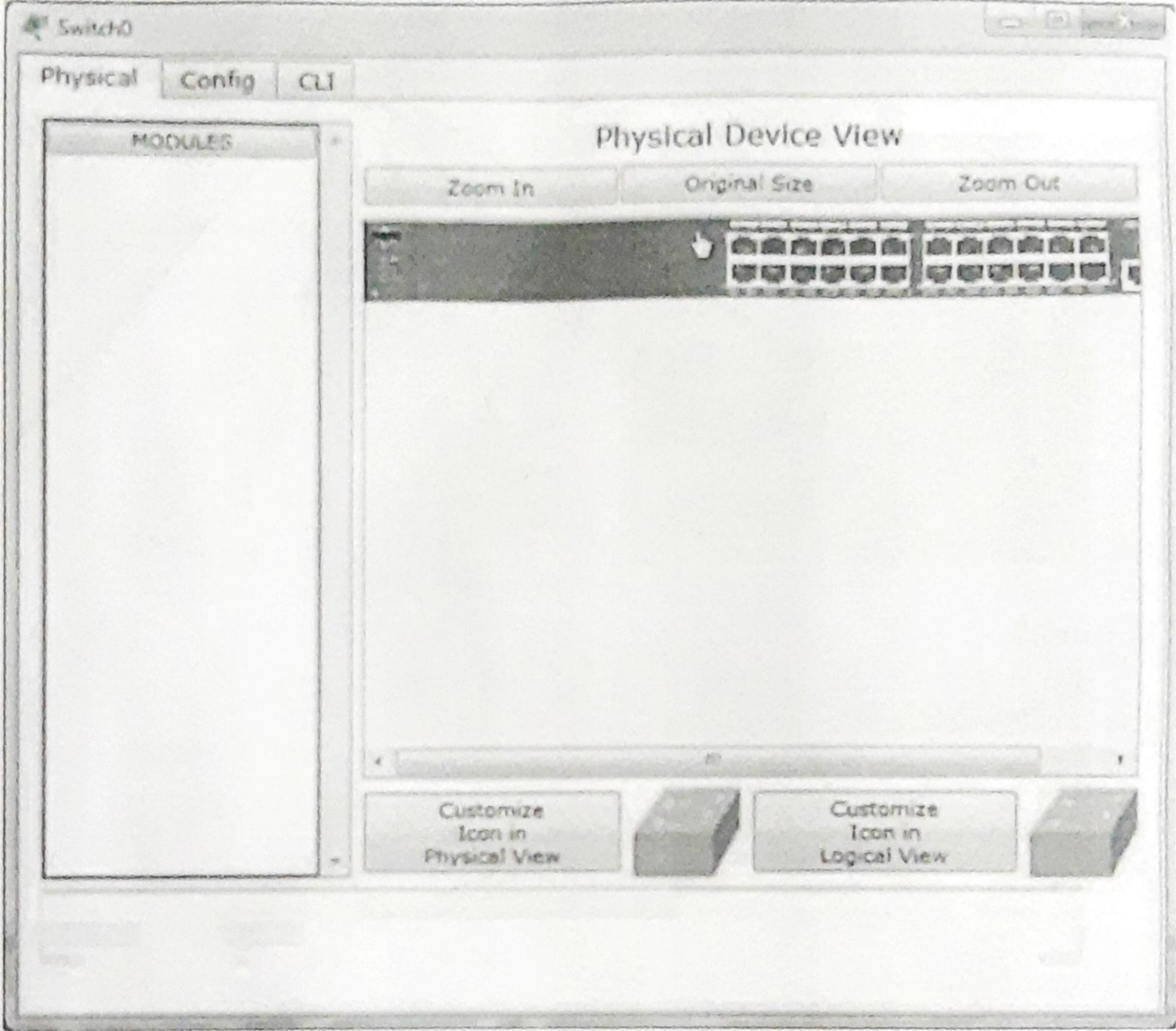
Procedure:

Step 1



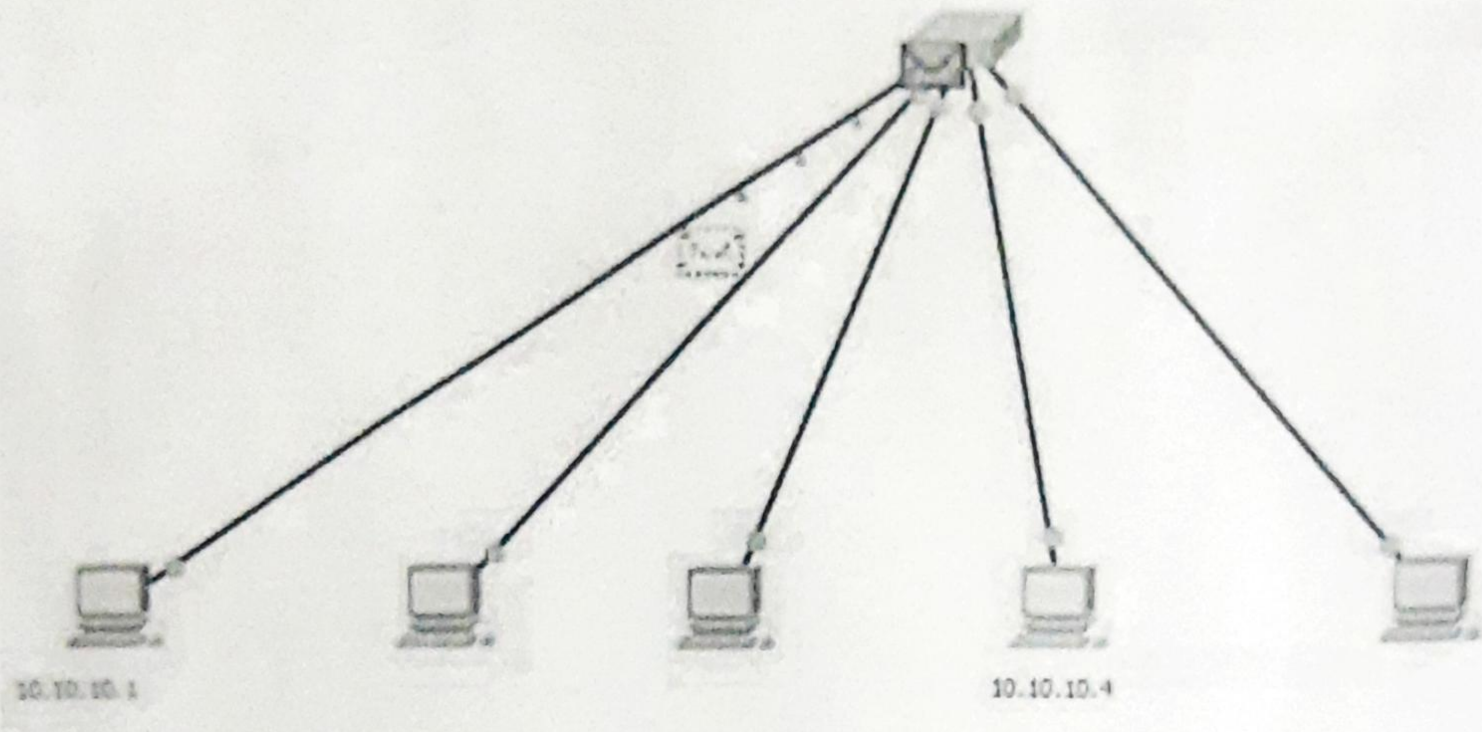
Step 2





Switch0
Physical
Config
CLI
MODULES
Physical Device View
Zoom In
Original Size
Zoom Out
Customize
Icon in
Physical View
Customize
Icon in
Logical View

Step 4



Step 5

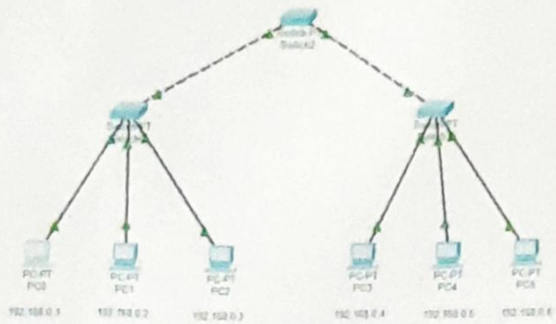
```
Switch>
Switch>EN
Switch#show mac-addres
Switch#show mac-address-table
```

```
Switch>
Switch>EN
Switch#show mac-addres
Switch#show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0001.63b6.6da8    DYNAMIC     Fa0/2
   1    0001.6476.e726    DYNAMIC     Fa0/1
   1    0001.c9e5.b3b2    DYNAMIC     Fa0/3
   1    0060.0f39.66c8    DYNAMIC     Fa0/5
   1    0090.2b81.6726    DYNAMIC     Fa0/4
Swit
```

OBSERVATION: -

Tree Topology

OBSERVATION:

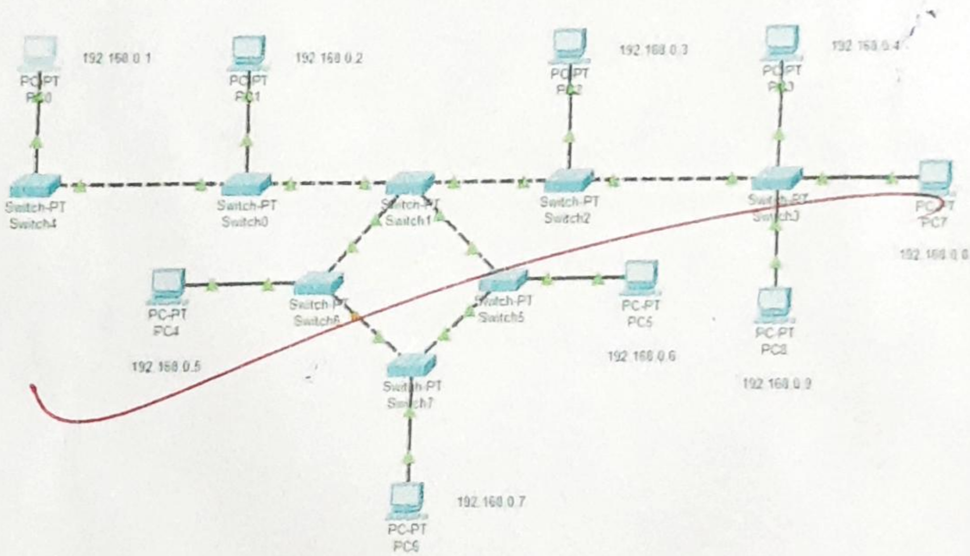


RESULT:

```
C:\>ping 192.168.0.6

Pinging 192.168.0.6 with 32 bytes of data:

Reply from 192.168.0.6: bytes=32 time=1ms TTL=128
Reply from 192.168.0.6: bytes=32 time<1ms TTL=128
Reply from 192.168.0.6: bytes=32 time<1ms TTL=128
Reply from 192.168.0.6: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.0.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Hybrid Topology

OBSERVATION:

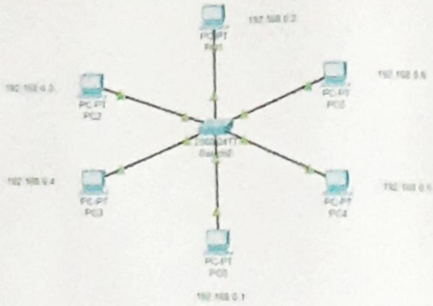


RESULT:

```
C:\>ping 192.168.0.9

Pinging 192.168.0.9 with 32 bytes of data:

Reply from 192.168.0.9: bytes=32 time=10ms TTL=128
Reply from 192.168.0.9: bytes=32 time<1ms TTL=128
Reply from 192.168.0.9: bytes=32 time<1ms TTL=128
Reply from 192.168.0.9: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.0.9:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 10ms, Average = 2ms
```

Star Topology

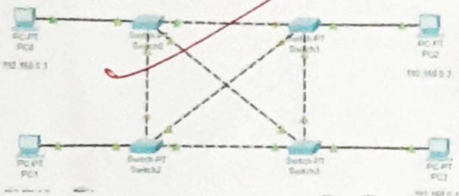
OBSERVATION:



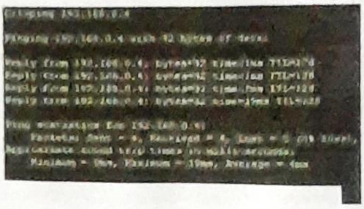
RESULT:

Mesh Topology

OBSERVATION:



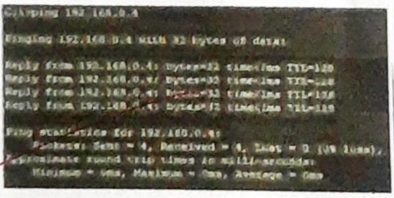
RESULT:



Bus Topology

OBSERVATION:

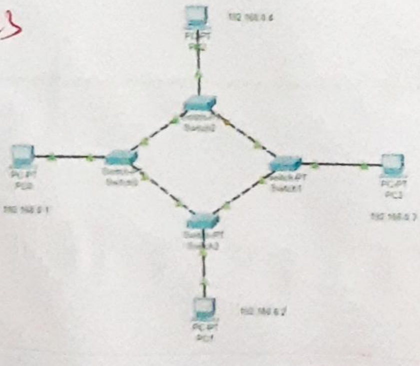
RESULT:



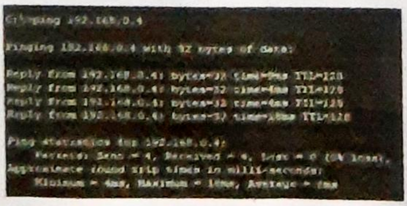
Ring Topology

OBSERVATION:

23



RESULT:



Experiment 5

Aim:- Study of various LAN topologies and their creation using network devices, cables and Computer.

Topology is derived from two Greek words topo and logy, where topo means 'place' and logy means 'study'. In computer networks, a topology is used to explain how a network is physically connected and the logical flow of information in the network. A topology mainly describes how devices are connected and interact with each other using communication links.

In computer networks, there are mainly two types of topologies, they are:

1. **Physical Topology:** A physical topology describes the way in which the computers or nodes are connected with each other in a computer network. It is the arrangement of various elements(link, nodes, etc.), including the device location and code installation of a computer network. In other words, we can say that it is the physical layout of nodes, workstations, and cables in the network.
2. **Logical Topology**: A logical topology describes the way, data flow from one computer to another. It is bound to a network protocol and defines how data is moved throughout the network and which path it takes. In other words, it is the way in which the devices communicate internally.

Network topology defines the layout, virtual shape, or structure of the network, not only physically but also logically. A network can have one physical topology and multiple logical topologies at the same time.

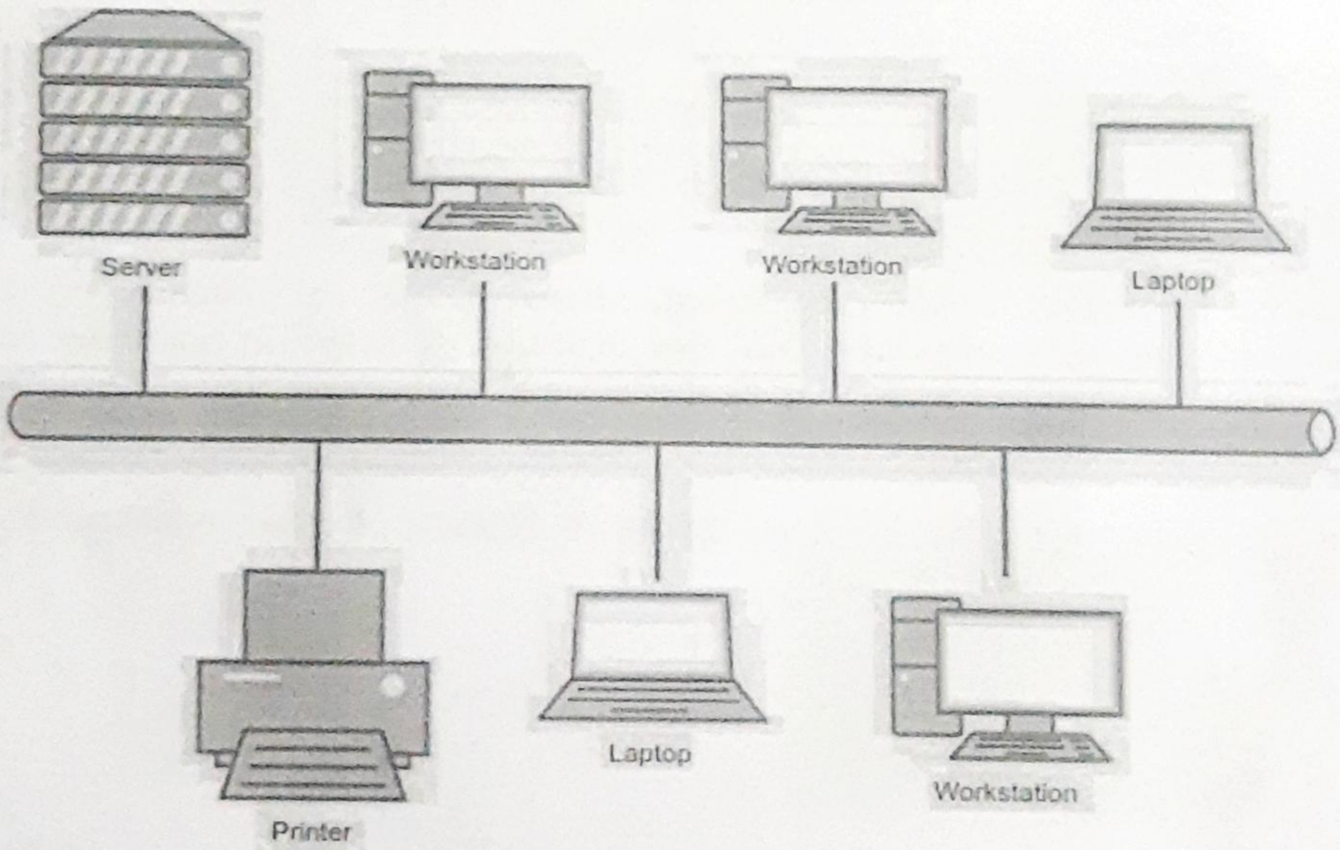
In a computer network, there are mainly six types of physical topology, they are:

1. **Bus Topology**
2. **Ring Topology**
3. **Star Topology**
4. **Mesh Topology**
5. **Tree Topology**
6. **Hybrid Topology**

1. **Bus Topology:**

Bus topology is the simplest kind of topology in which a common bus or channel is used for communication in the network. The bus is connected to various taps and droplines. Taps are the connectors, while droplines are the cables connecting the bus with the computer. In other words, there is only a single transmission line for all nodes.

In this topology, the bus acts as the backbone of the network, which joins every computer and peripherals in the network. Both ends of the shared channel have line terminators. The data is sent only in one direction and as soon as it reaches the end, the terminator removes the data from the communication line(to prevent signal bounce and data flow disruption).
In a bus topology, each computer communicates to another computer on the network independently. Every computer can share the network's total bus capabilities. The devices share the responsibility for the flow of data from one point to the other in the network.



Bus Topology

Following are the advantages of Bus topology:

1. Simple to use and install.
2. If a node fails, it will not affect other nodes.
3. Less cabling is required.
4. Cost-efficient to implement.

Following are the disadvantages of Bus topology:

1. Efficiency is less when nodes are more(strength of signal decreases).
2. If the bus fails, the network will fail.
3. A limited number of nodes can connect to the bus due to limited bus length.
4. Security issues and risks are more as messages are broadcasted to all nodes.
5. Congestion and traffic on the bus as it is the only source of communication.

2. Ring Topology :

Ring topology is a topology in which each computer is connected to exactly two other computers to form the ring. The message passing is unidirectional and circular in nature. This network topology is deterministic in nature, i.e., each computer is given access for transmission at a fixed time interval. All the nodes are connected in a closed-loop. This topology mainly works on a token-based system and the token travels in a loop in one specific direction.

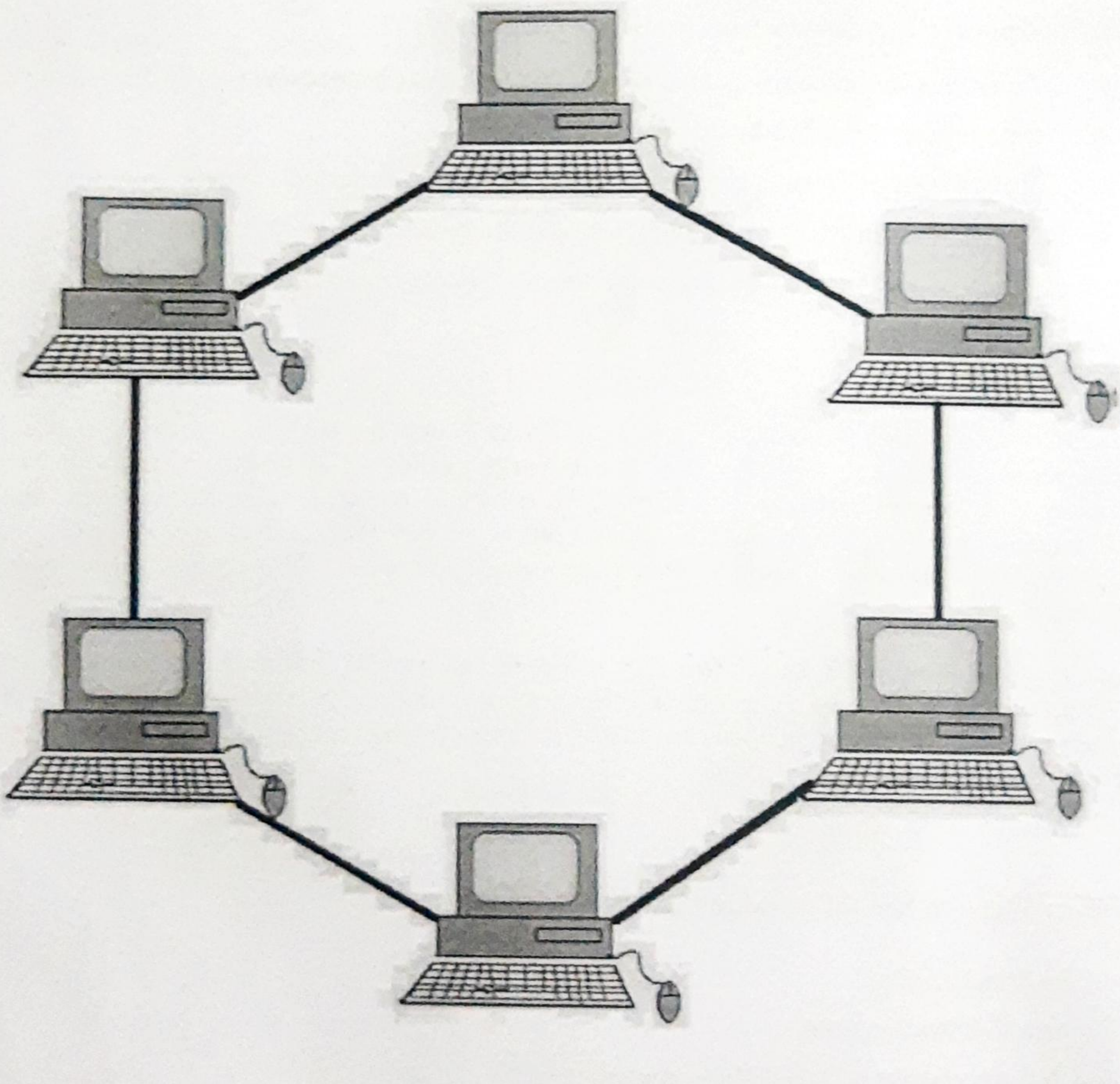
In a ring topology, if a token is free then the node can capture the token and attach the data and destination address to the token, and then leaves the token for communication. When this token reaches the destination node, the data is removed by the receiver and the token is made free to carry the next data.

Following are the advantages of Ring topology:

1. Easy Installation.
2. Less Cabling Required.
3. Reduces chances of data collision(unidirectional).
4. Easy to troubleshoot(the faulty node does not pass the token).
5. Each node gets the same access time.

Following are the disadvantages of Ring topology:

1. If a node fails, the whole network will fail.
2. Slow data transmission speed(each message has to go through the ring path).
3. Difficult to reconfigure(we have to break the ring).

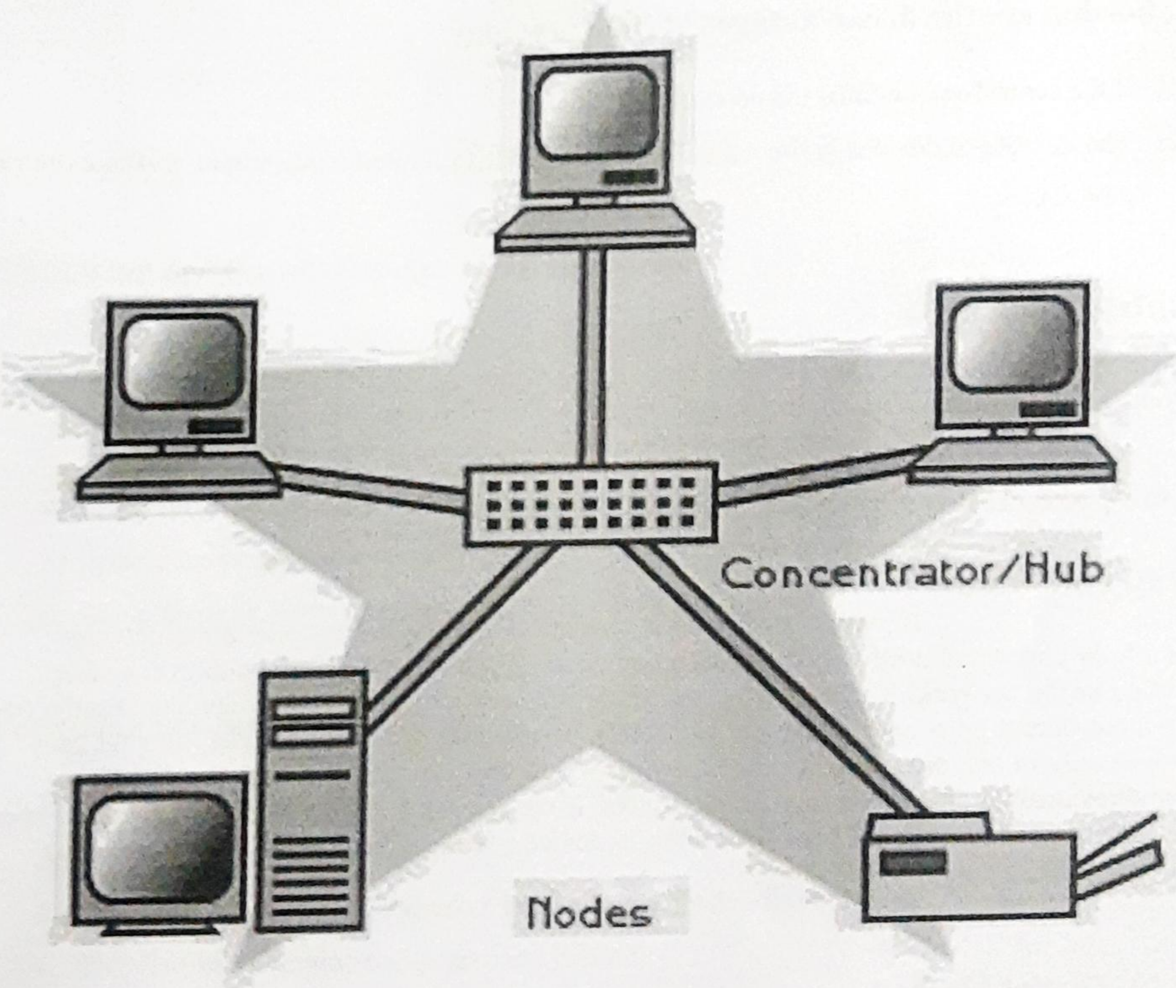


Ring Topology

3.Star Topology :

Star topology is a computer network topology in which all the nodes are connected to a centralized hub. The hub or switch acts as a middleware between the nodes. Any node requesting for service or providing service, first contact the hub for communication. The central device(hub or switch) has point to point communication link(the dedicated link between the devices which can not be accessed by some other computer) with the devices. The central device then broadcast or unicast the message based on the central device used. The hub broadcasts the message, while the switch unicasts the messages by maintaining a switch table. Broadcasting increases unnecessary data traffic in the network.

In a star topology, hub and switch act as a server, and the other connected devices act as clients. Only one input-output port and one cable are required to connect a node to the central device. This topology is better in terms of security because the data does not pass through every node.



Star Topology

Following are the advantages of Star topology:

1. Centralized control.
2. Less Expensive.
3. Easy to troubleshoot(the faulty node does not give response).
4. Good fault tolerance due to centralized control on nodes.
5. Easy to scale(nodes can be added or removed to the network easily).
6. If a node fails, it will not affect other nodes.
7. Easy to reconfigure and upgrade(configured using a central device).

Following are the disadvantages of Star topology:

1. If the central device fails, the network will fail.
2. The number of devices in the network is limited(due to limited input-output port in a central device).

4.Mesh Topology :

Mesh topology is a computer network topology in which nodes are interconnected with each other. In other words, direct communication takes place between the nodes in the network.

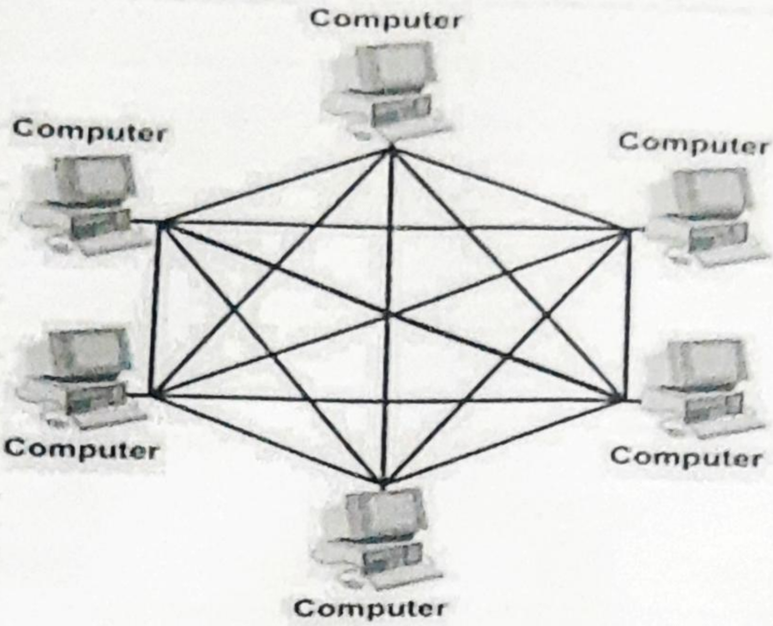
There are mainly two types of Mesh:

4 a). Full Mesh:

In which each node is connected to every other node in the network. In a fully connected mesh topology, each device has a point to point link with every other device in the network. If there are 'n' devices in the network, then each device has exactly '(n-1)' input-output ports and communication links. These links are simplex links, i.e., the data moves only in one direction. A duplex link(in which data can travel in both the directions simultaneously) can replace two simplex links. If we are using simplex links, then the number of communication links will be 'n(n-1)' for 'n' devices, while it is 'n(n-1)/2' if we are using duplex links in the mesh topology.

4 b). Partial Mesh:

In which, some nodes are not connected to every node in the network.



Mesh Topology

Following are the advantages of Mesh topology:

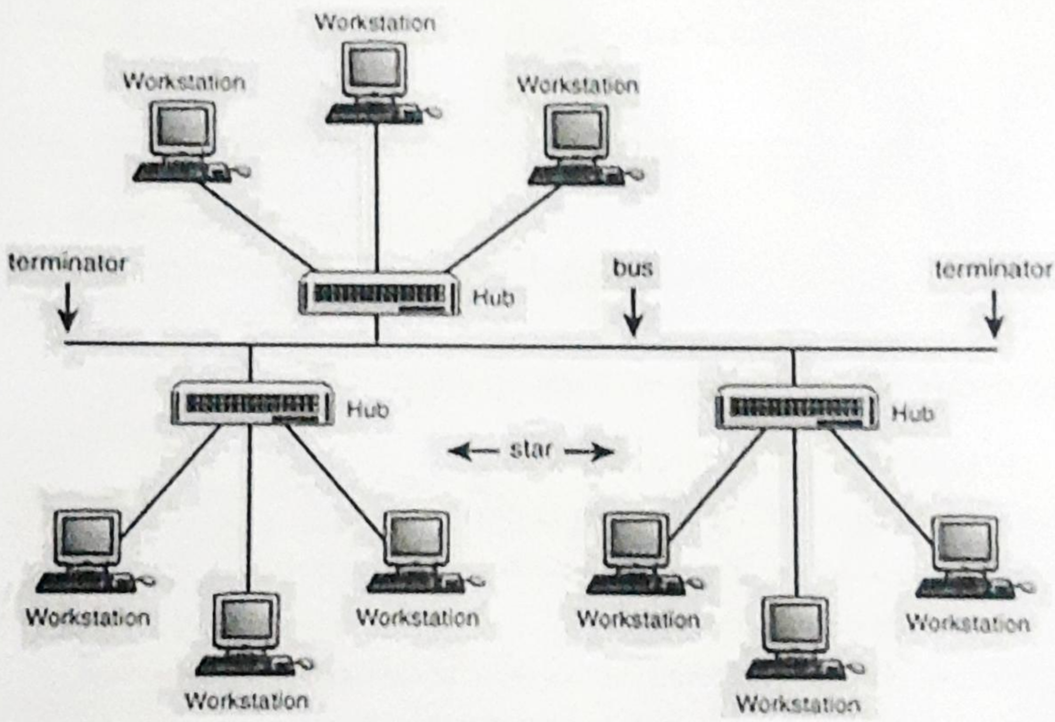
1. Dedicated links facilitate direct communication.
2. No congestion or traffic problems on the channels.
3. Good Fault tolerance due to the dedicated path for each node.
4. Very fast communication.
5. Maintains privacy and security due to a separate channel for communication.
6. If a node fails, other alternatives are present in the network.

Following are the disadvantages of Mesh topology:

1. Very high cabling required.
2. Cost inefficient to implement.
3. Complex to implement and takes large space to install the network.
4. Installation and maintenance are very difficult.

5. Tree Topology:

Tree topology is a computer network topology in which all the nodes are directly or indirectly connected to the main bus cable. Tree topology is a combination of Bus and Star topology. In a tree topology, the whole network is divided into segments, which can be easily managed and maintained. There is a main hub and all the other sub-hubs are connected to each other in this topology.



Tree Topology

Following are the advantages of Tree topology:

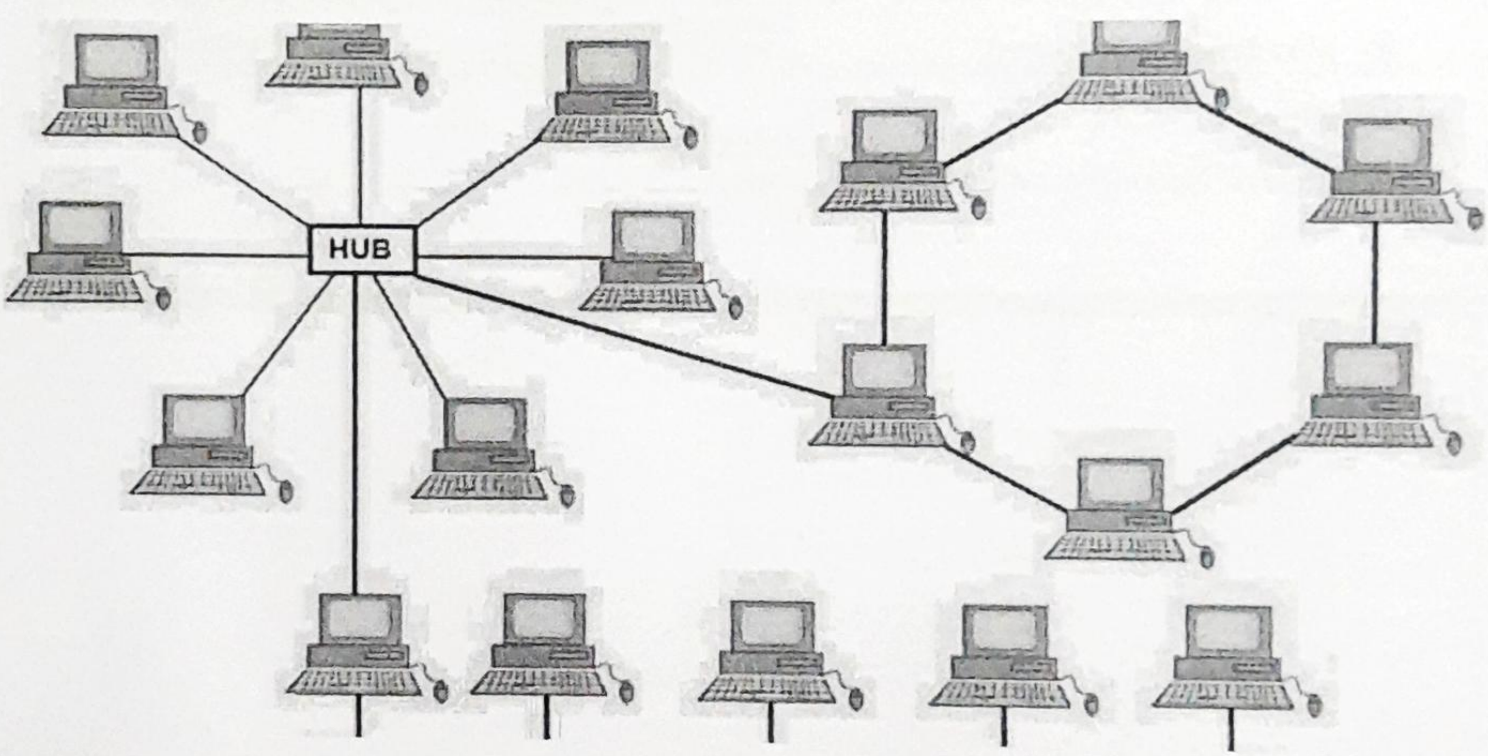
1. Large distance network coverage.
2. Fault finding is easy by checking each hierarchy.
3. Least or no data loss.
4. A Large number of nodes can be connected directly or indirectly.
5. Other hierarchical networks are not affected if one of them fails.

Following are the disadvantages of Tree topology:

1. Cabling and hardware cost is high.
2. Complex to implement.
3. Hub cabling is also required.
4. A large network using tree topology is hard to manage.
5. It requires very high maintenance.
6. If the main bus fails, the network will fail.

6. Hybrid Topology:

A Hybrid topology is a computer topology which is a combination of two or more topologies. In practical use, they are the most widely used.
In this topology, all topologies are interconnected according to the needs to form a hybrid. All the good features of each topology can be used to make an efficient hybrid topology.



Hybrid Topology

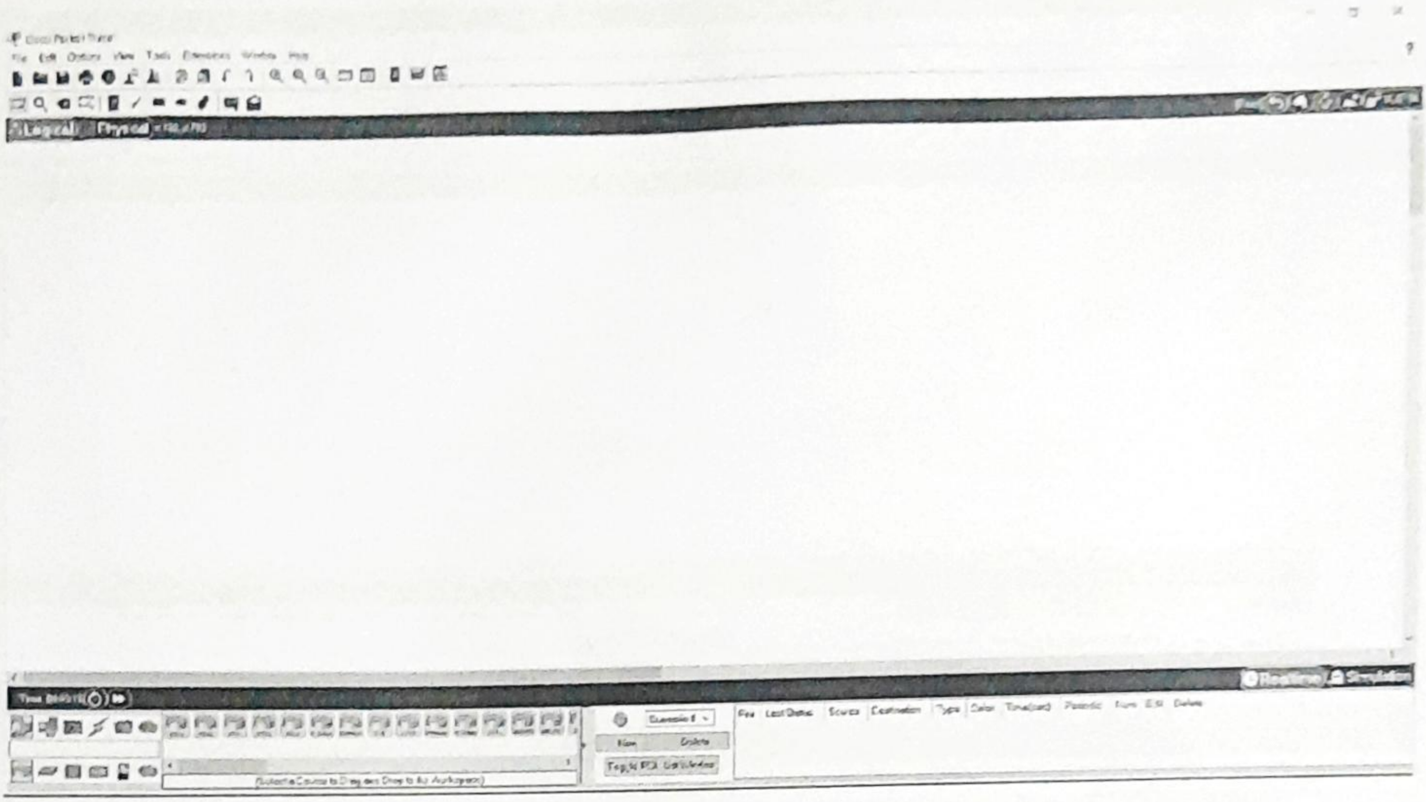
1. It can handle a large volume of nodes.
2. It provides flexibility to modify the network according to our needs.
3. Very Reliable(if one node fails it will not affect the whole network).

Following are the disadvantages of Hybrid topology:

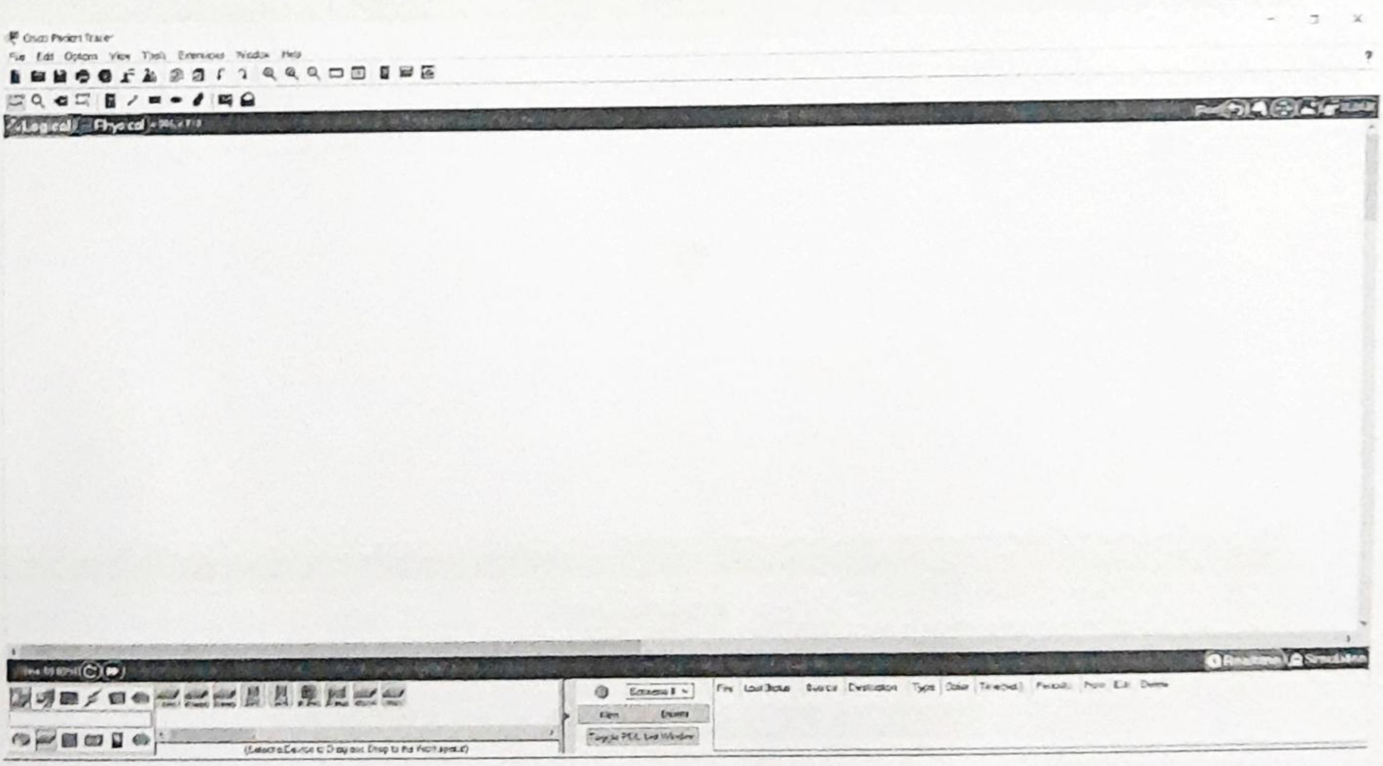
1. Complex design.
2. Expensive to implement.
3. Multi-Station Access Unit(MSAL) required.
4. Hence, after learning the various computer network topologies, we can conclude that some points need to be considered when selecting a physical topology:
5. Ease of Installation.
6. Fault Tolerance.
7. Implementation Cost.
8. Cabling Required.
9. Maintenance Required.
10. Reliable Nature.
11. Ease of Reconfiguration and upgradation.

→ Demonstration of a star topology by using cisco packet tracer

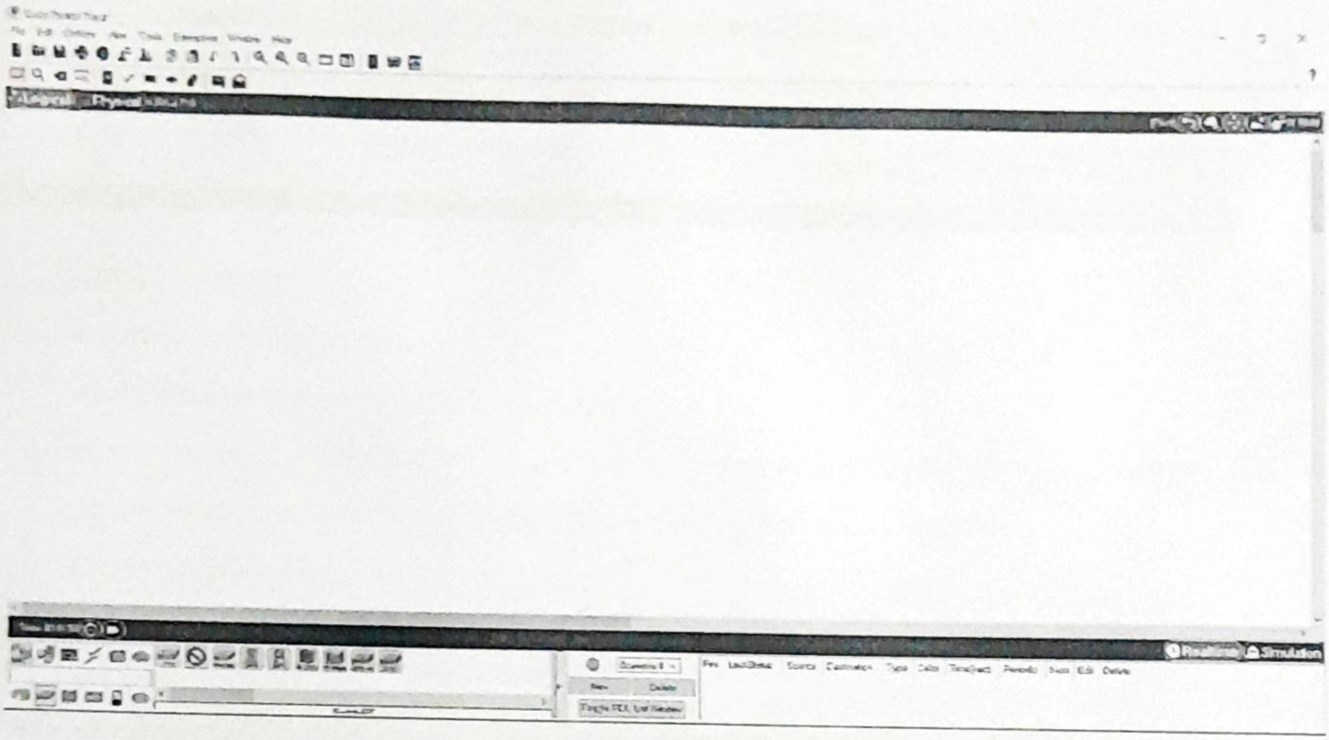
STEP 1: Open cisco packet tracer and choose <u>SWITCH PT</u> with name <u>SWITCH0</u>.



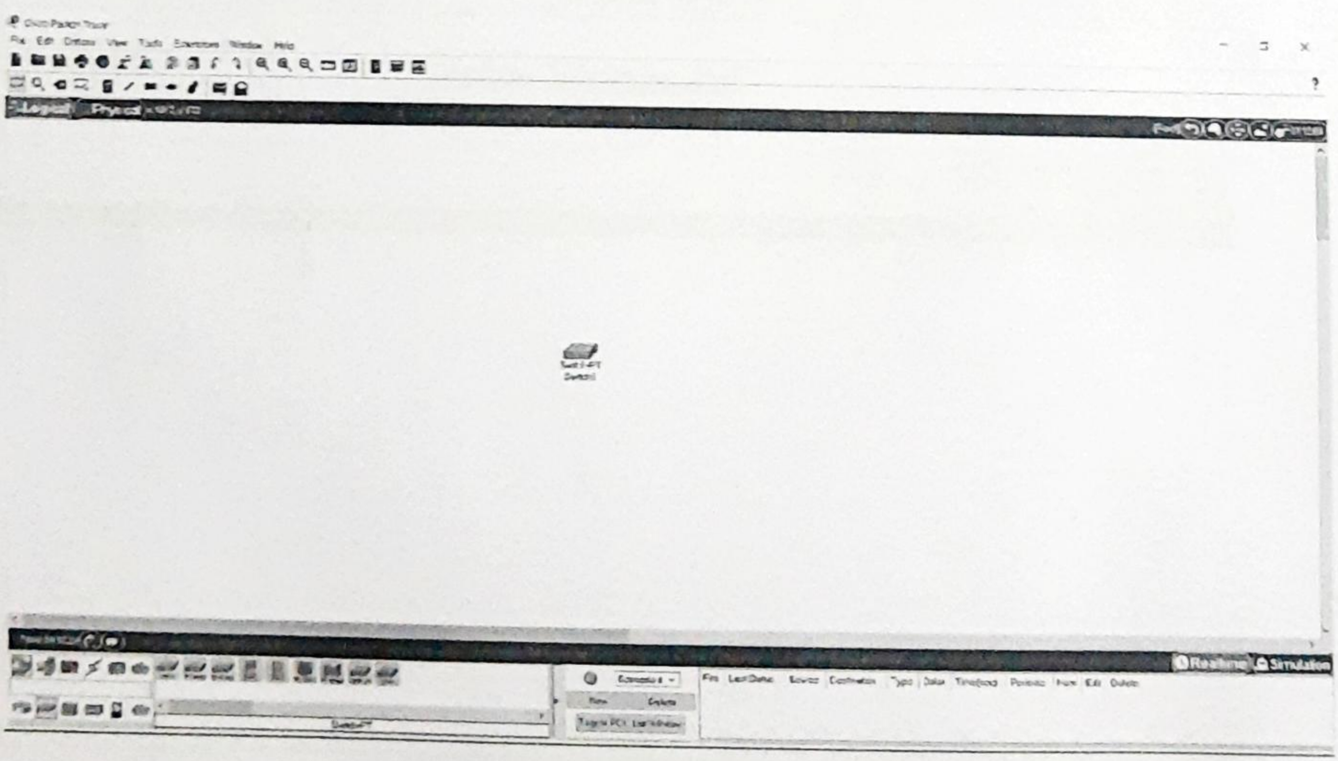
Click on switch option.



Choose SWITCH PT.

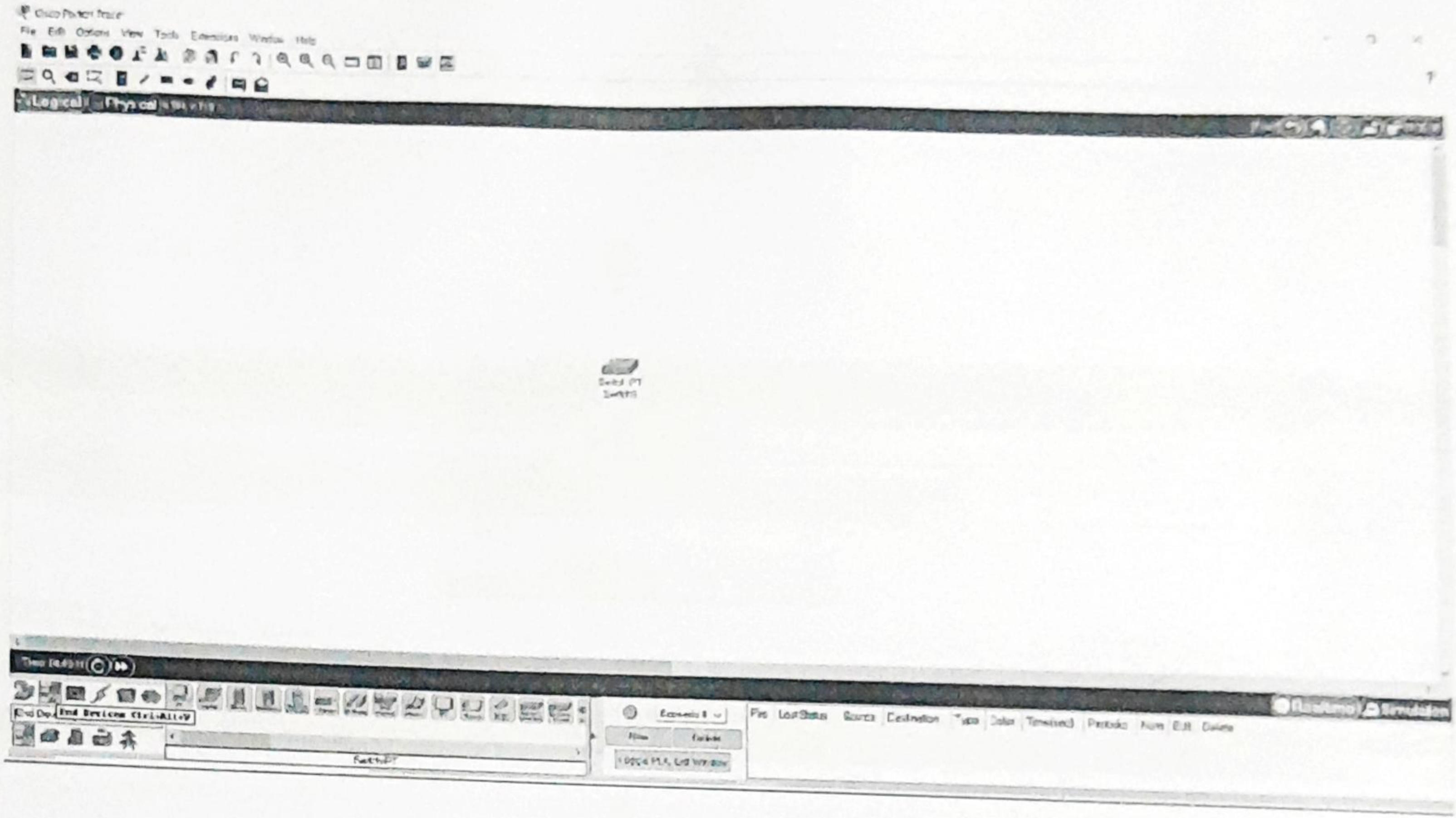


Click on SWITCH PT.

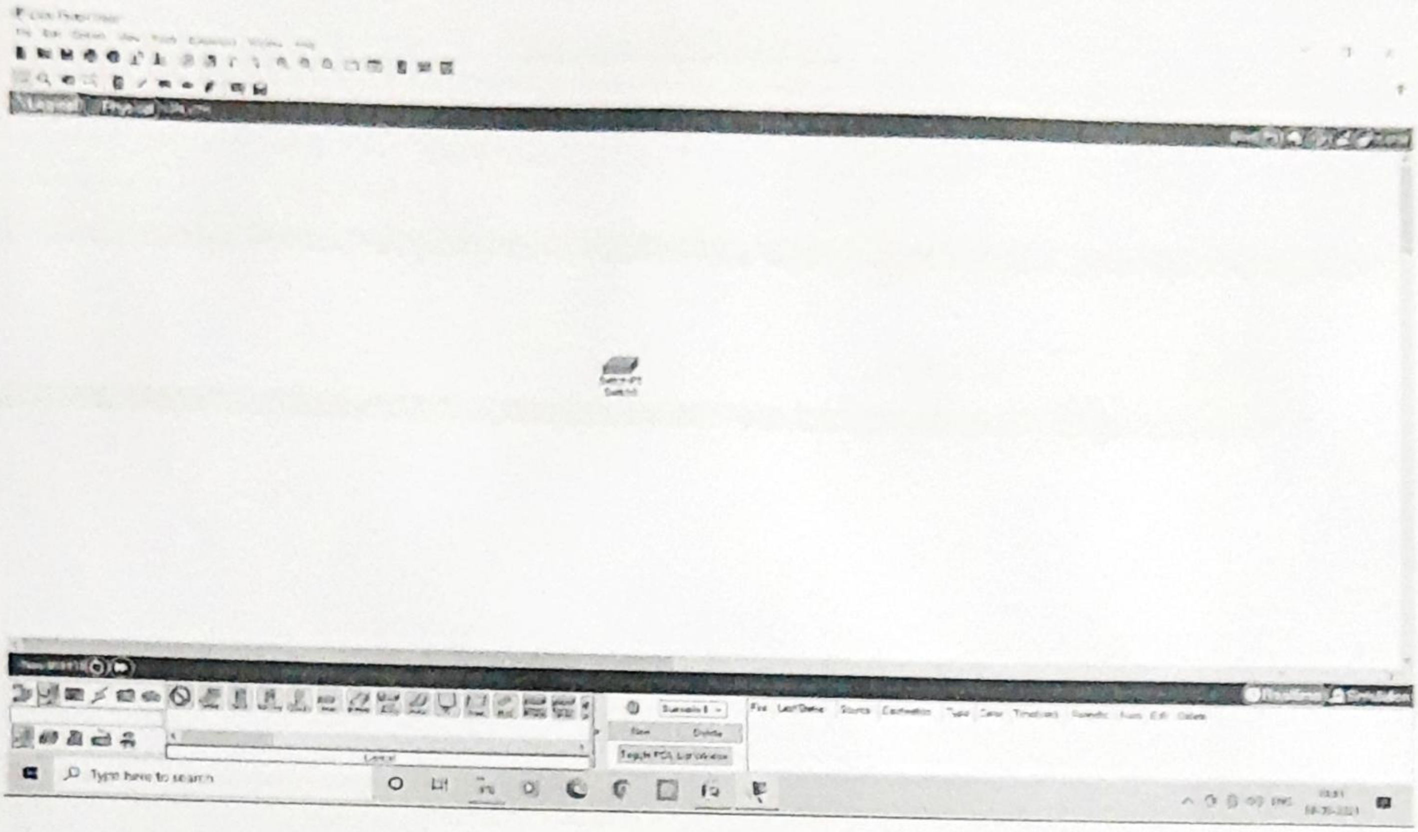


SWITCH PT is selected with name SWITCH 0.

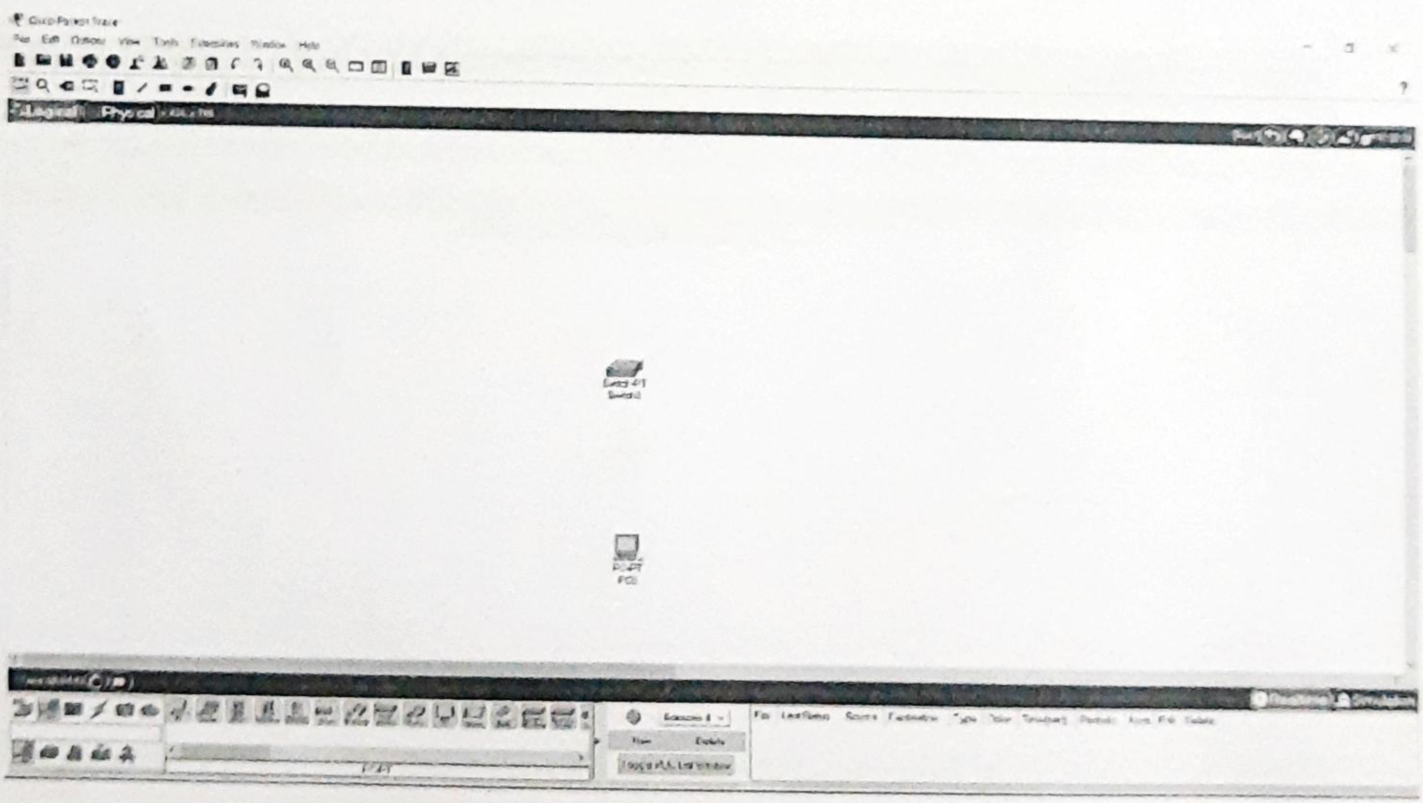
STEP 2 : Now click on end divcces and add PCs .



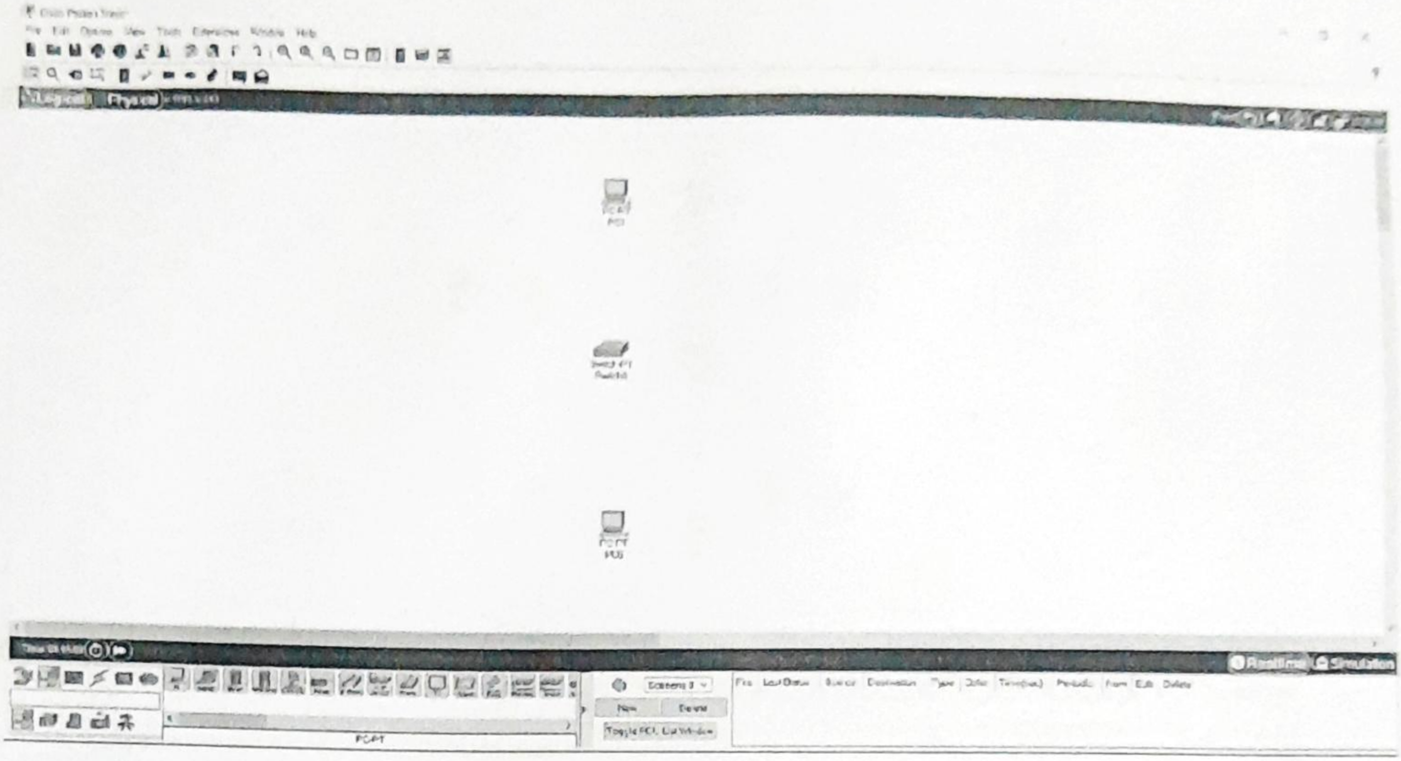
Clicking on end devices.



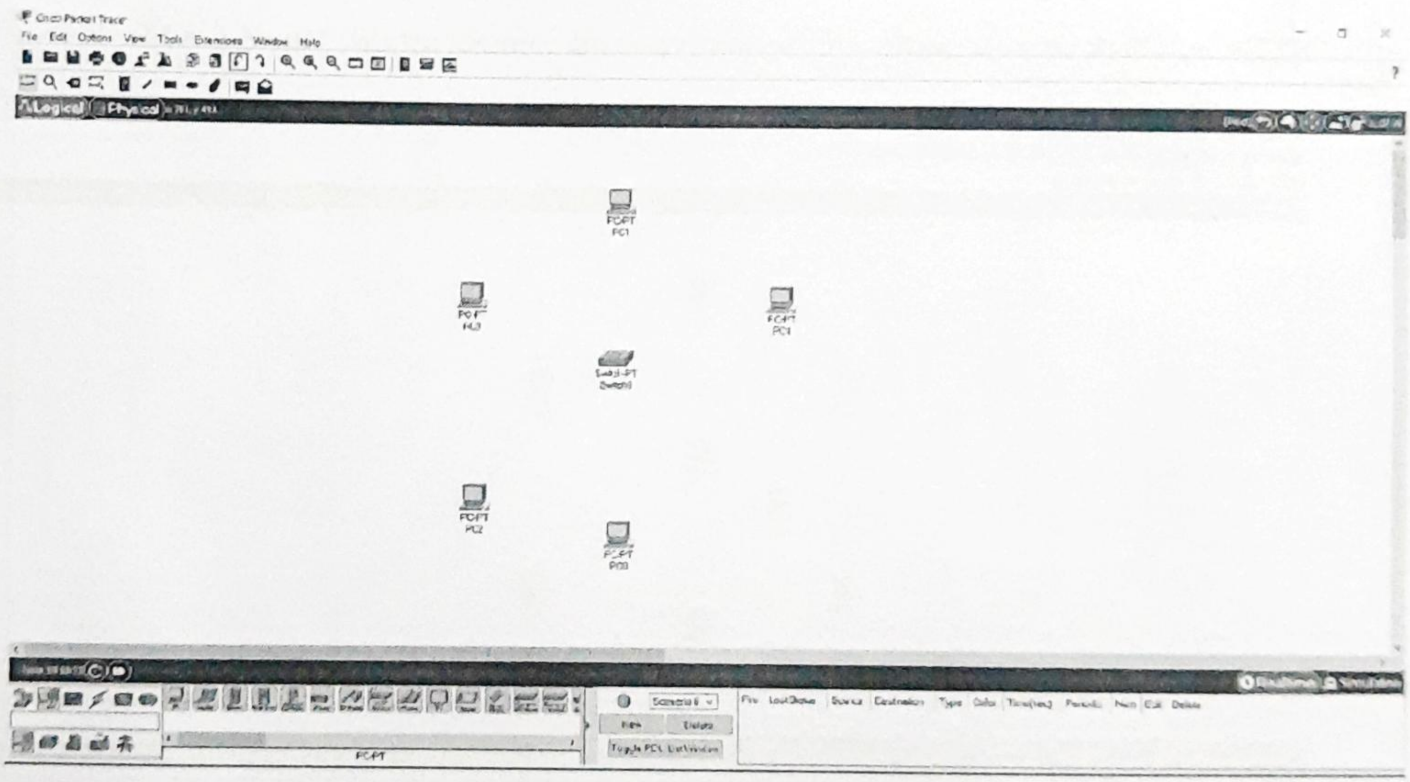
Choose PC as end devices.



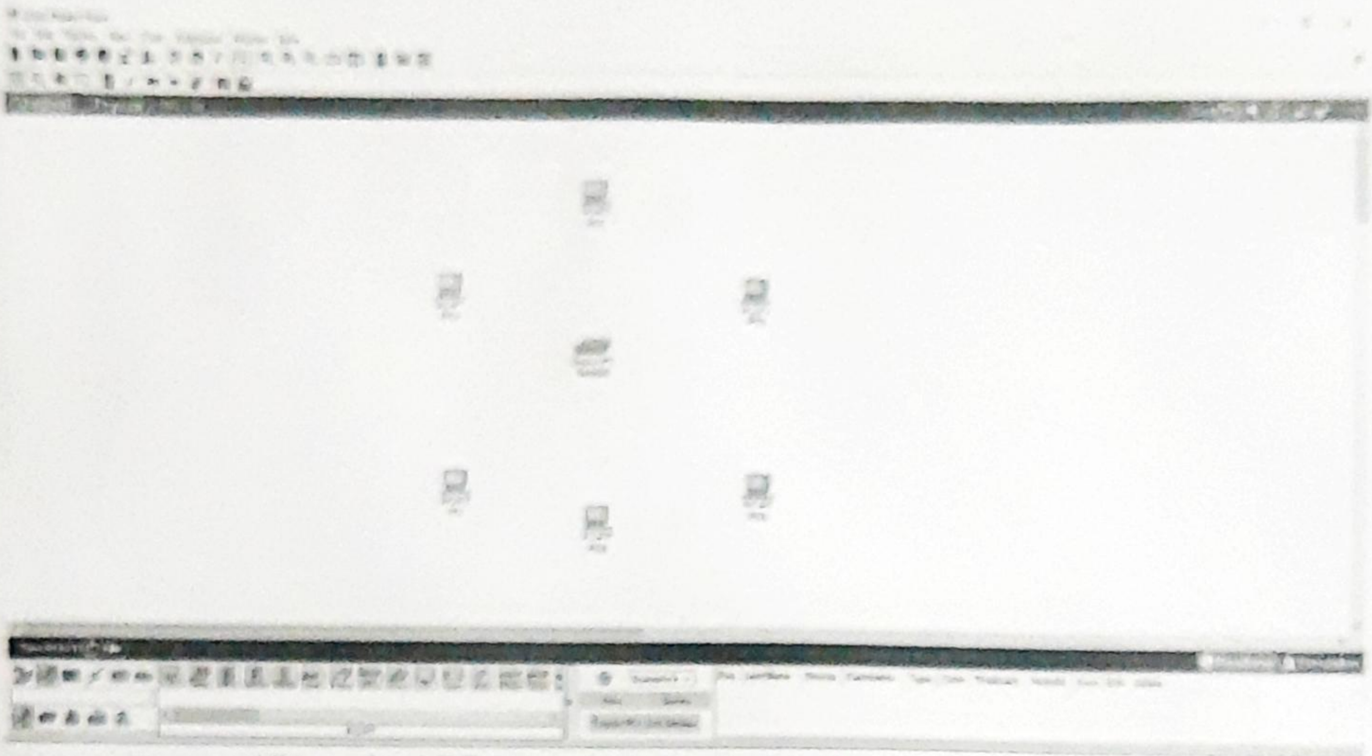
First PC selected.



Second PC selected.

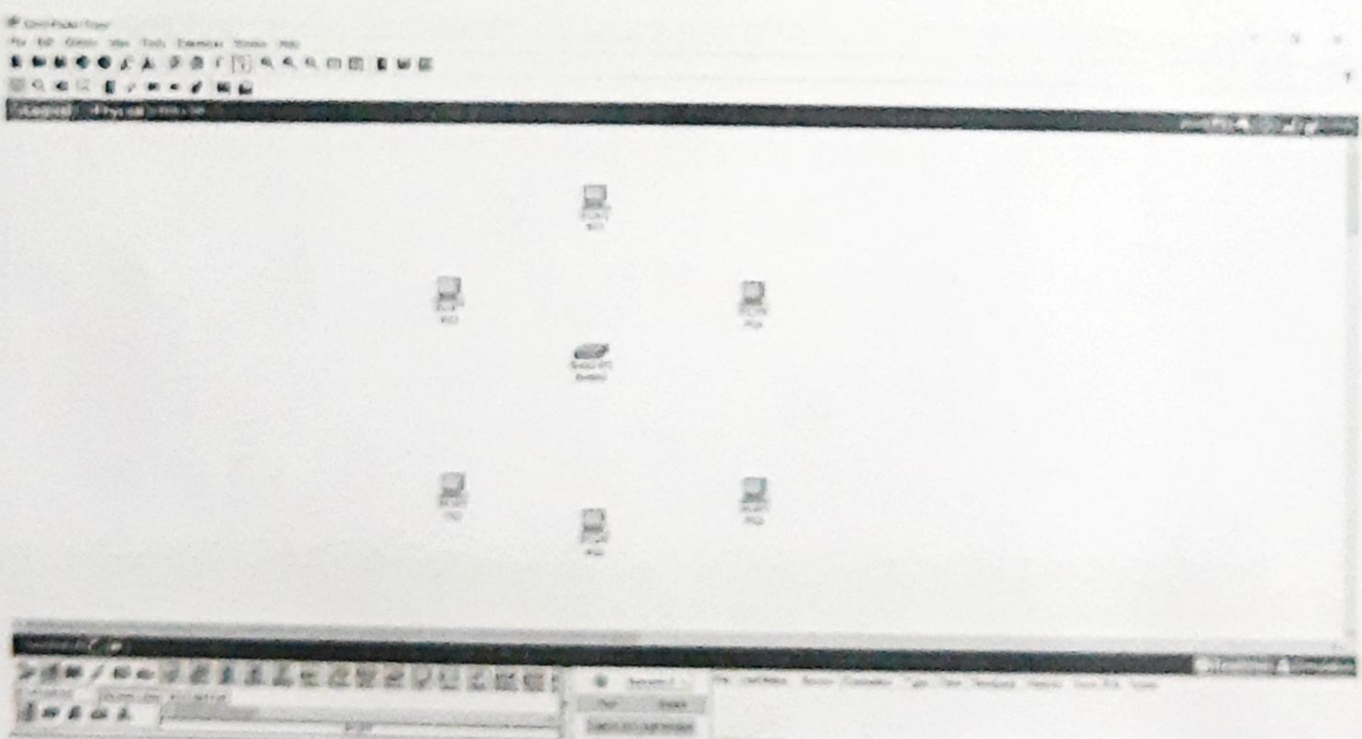


Four PCs are selected.

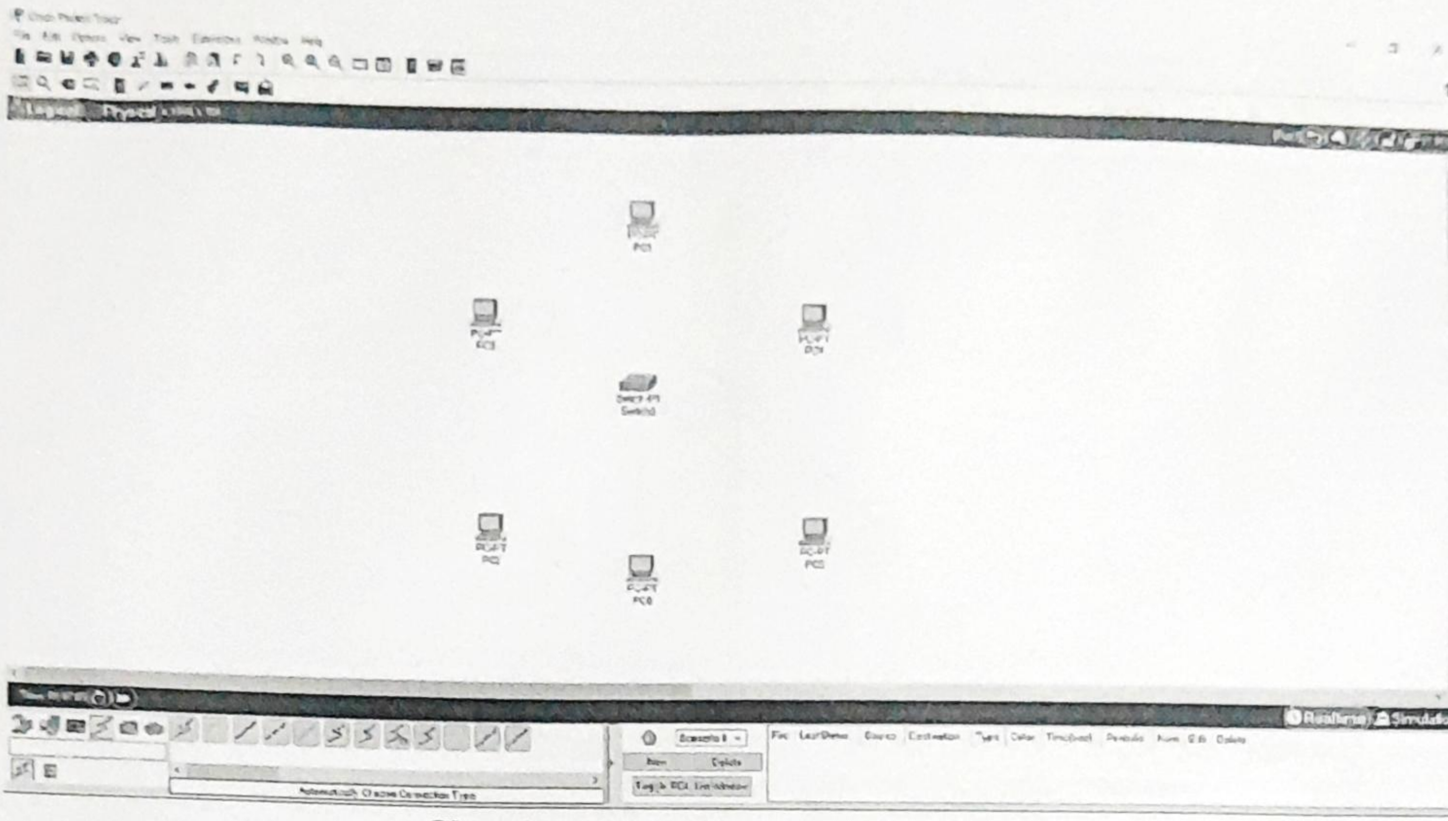


<u>All required PCs are selected and placed in STAR shape.</u>

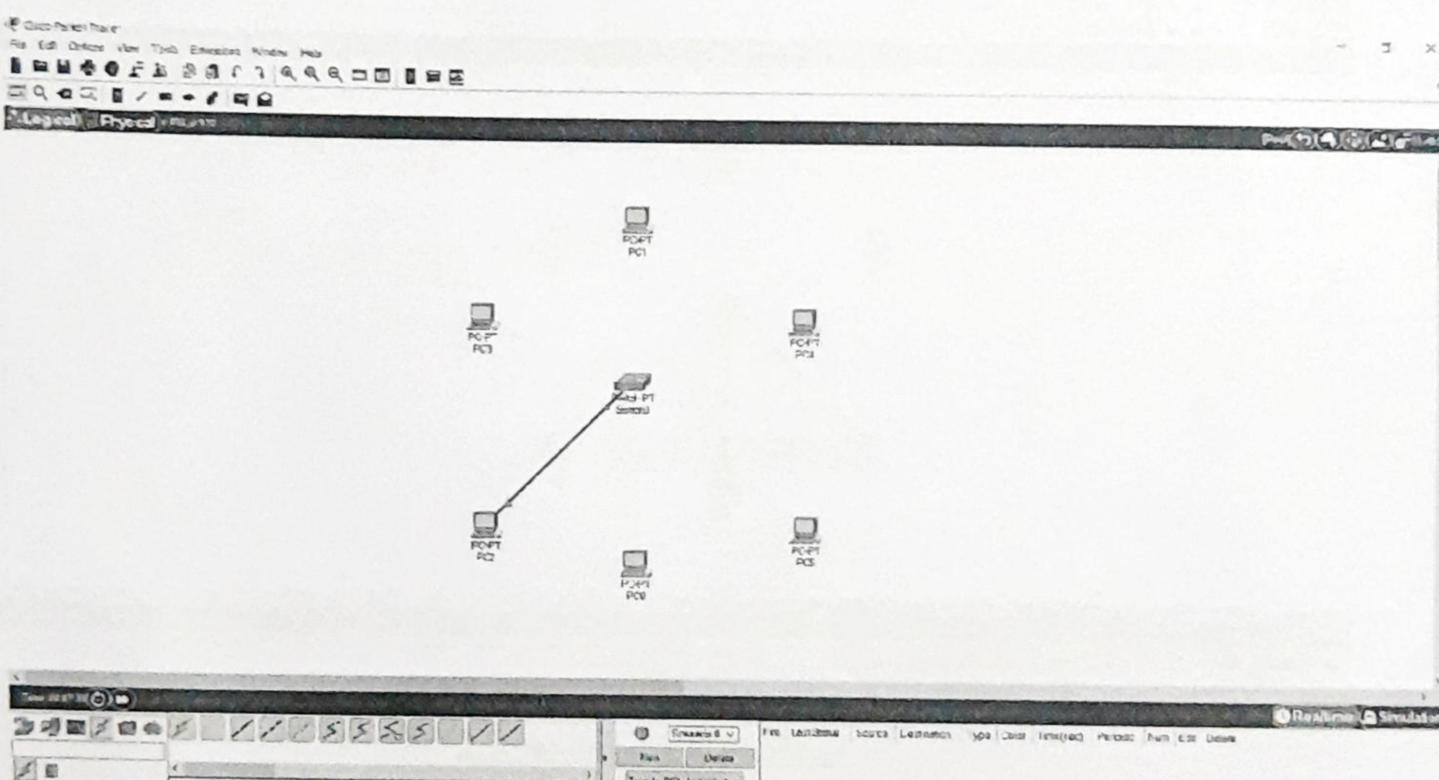
STEP 3 : Click on automatic connection type and connect all the PCs to SWITCH 0.



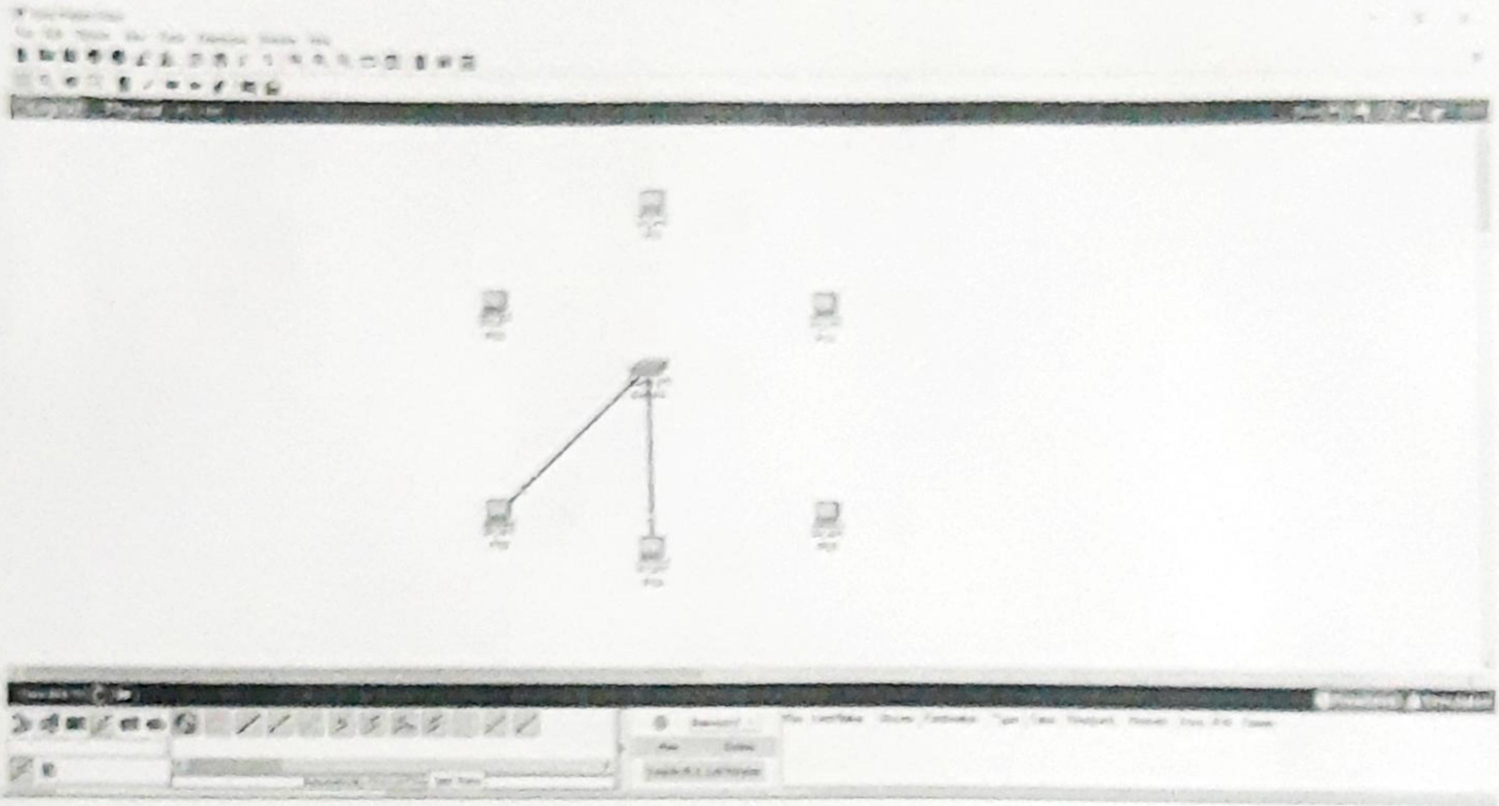
<u>Clicking on connection.</u>



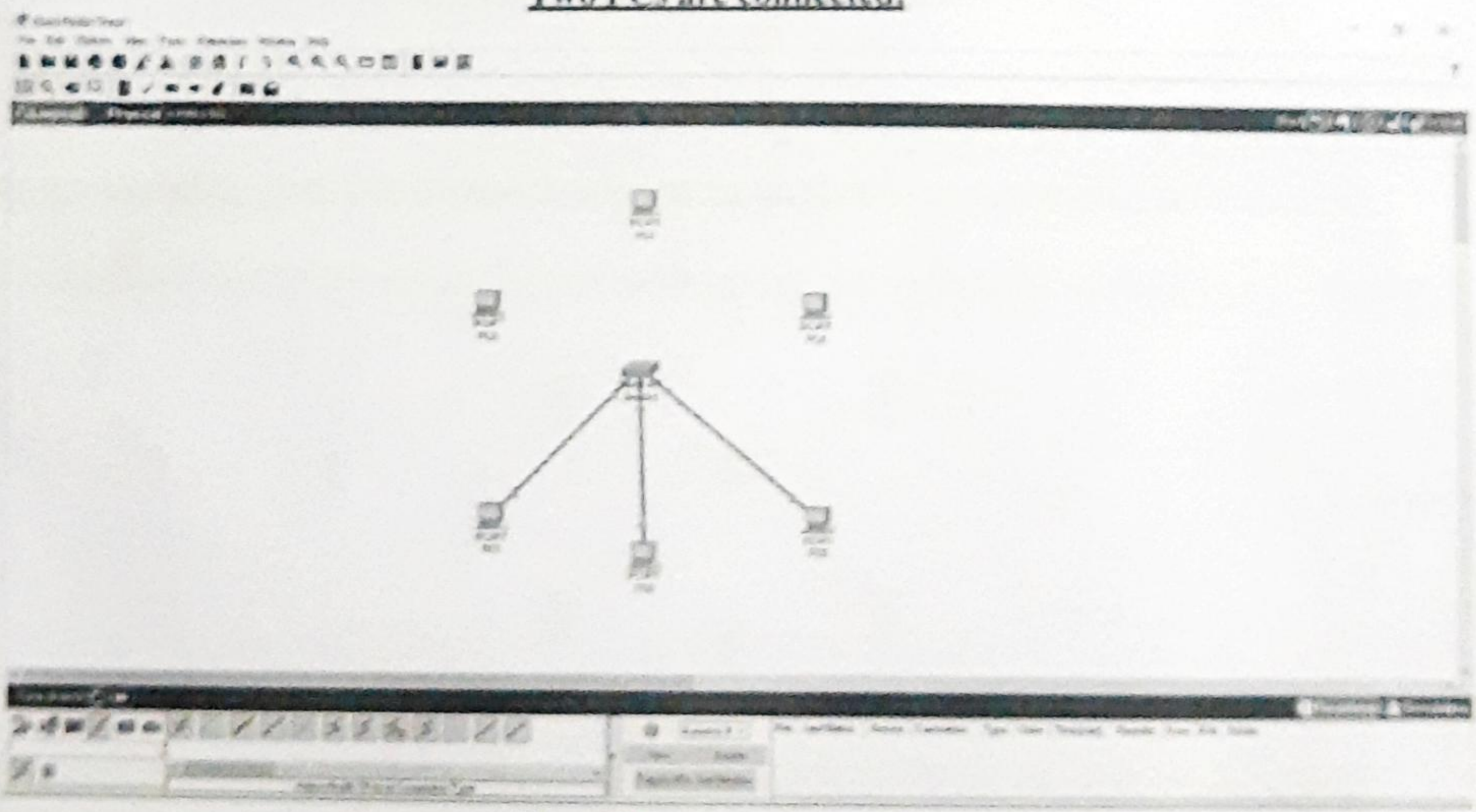
Choosing automatic connection type.



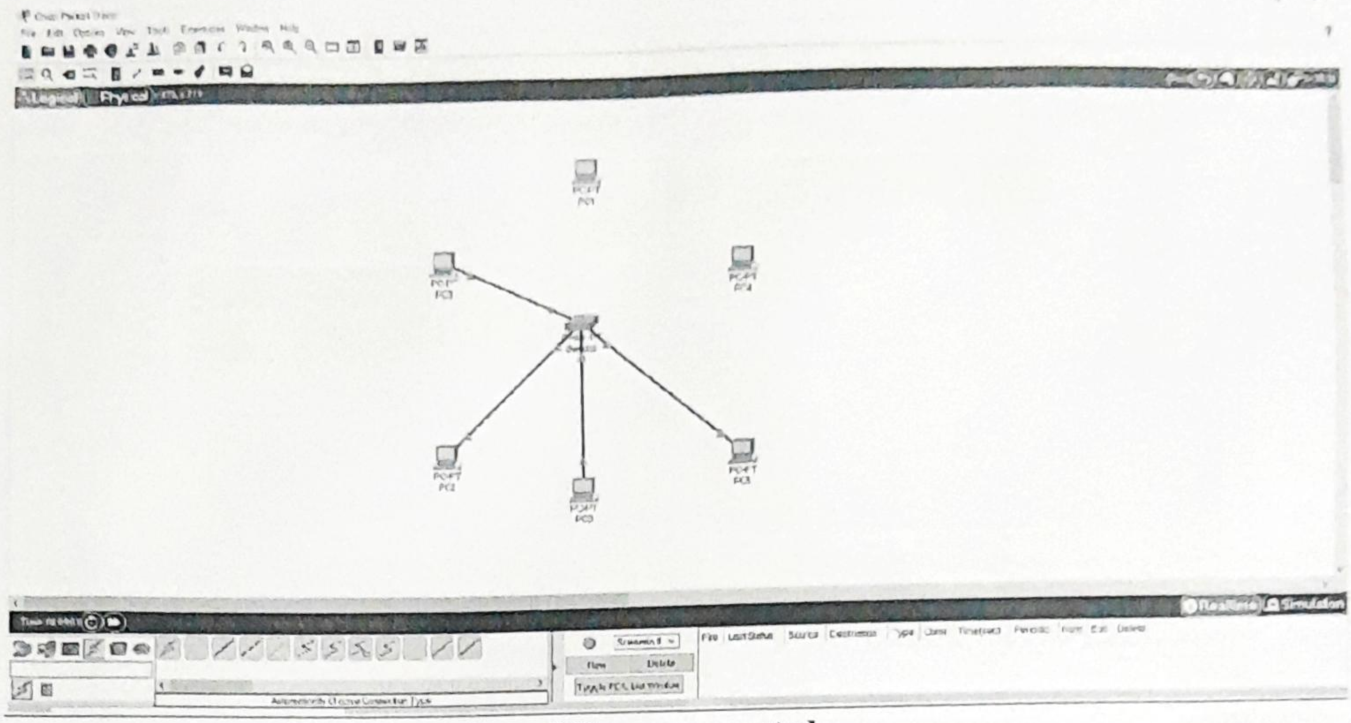
One PC is connected.



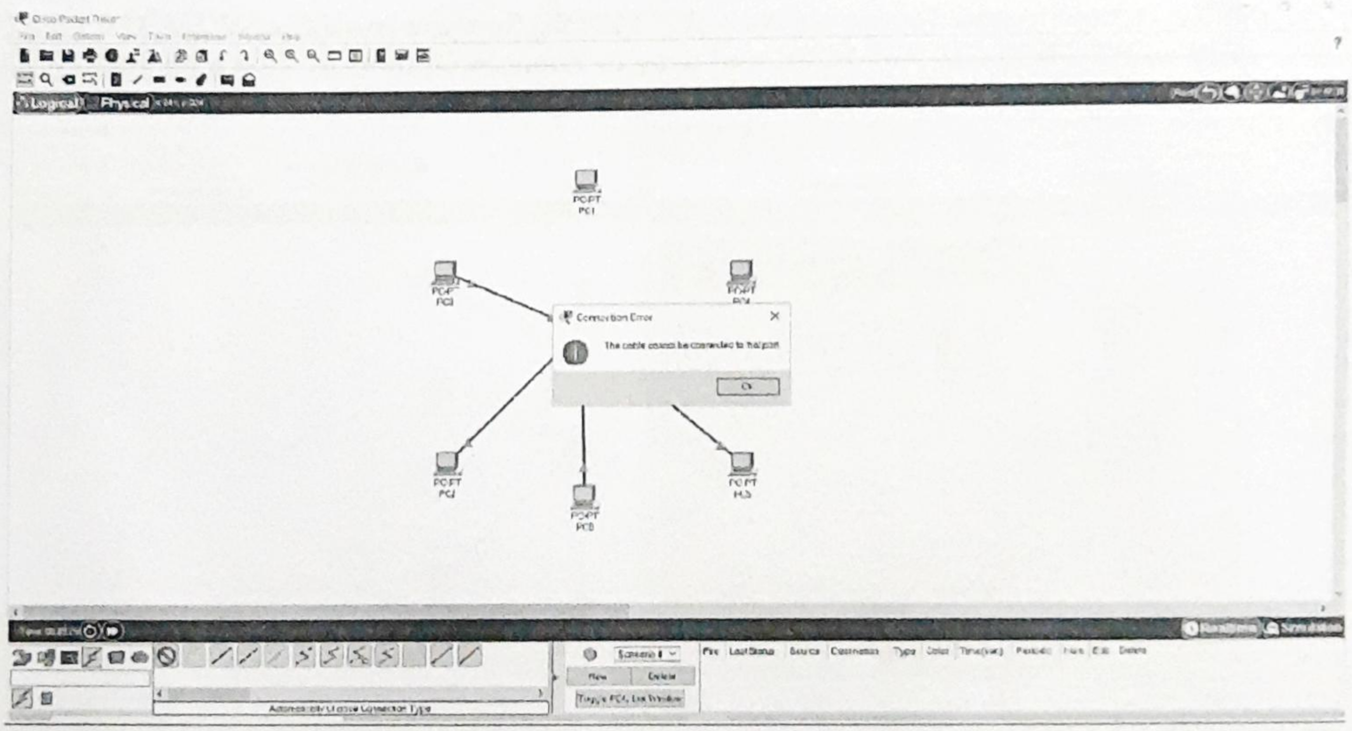
Two PCs are connected.



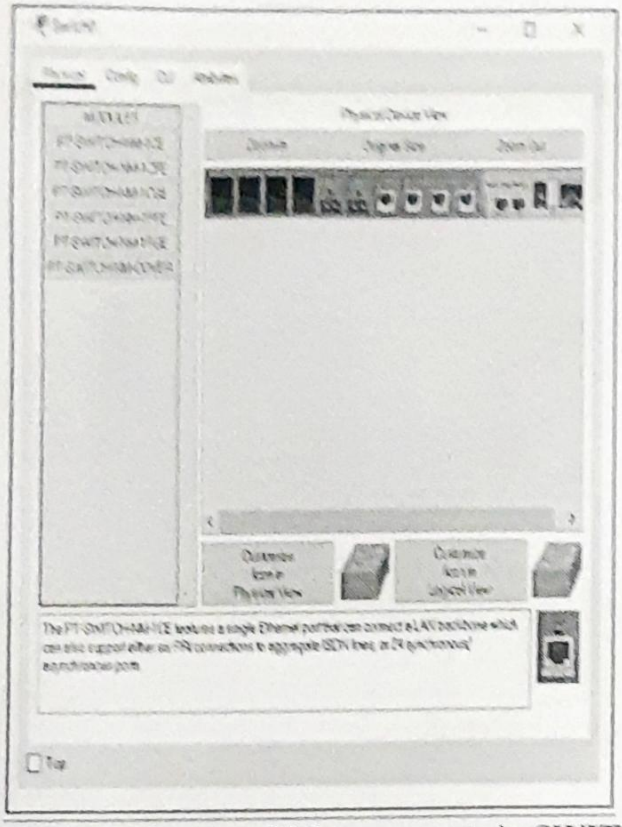
Three PCs are connected.



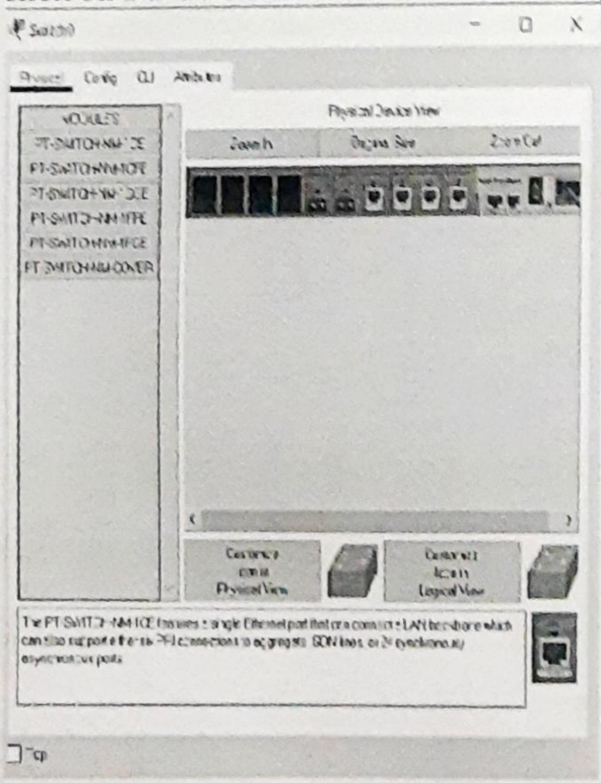
<u>Four PCs are connected.</u>



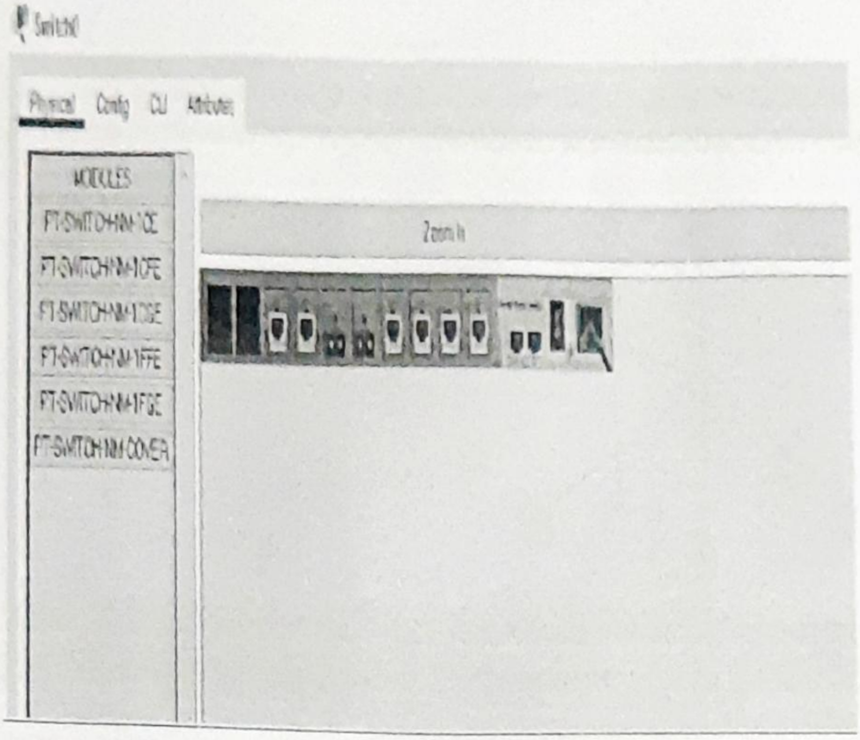
In 5th PC (PC4) connection there will show an error as shown in above picture. To resolve above error we click on switch PT (SWITCH 0) as shown below then it shows there are only 4 ports are available in SWITCH 0 . Now we need 2 more ports to make a star topology and connecting rest 2 PCs (PC4 & PC5).



STEP 4: Now to add 2 more ports in SWITCH 0 , first power off the SWITCH 0 then click on PT SWITCH-NM-1CFE and drag to Zoom in Options as shown below.

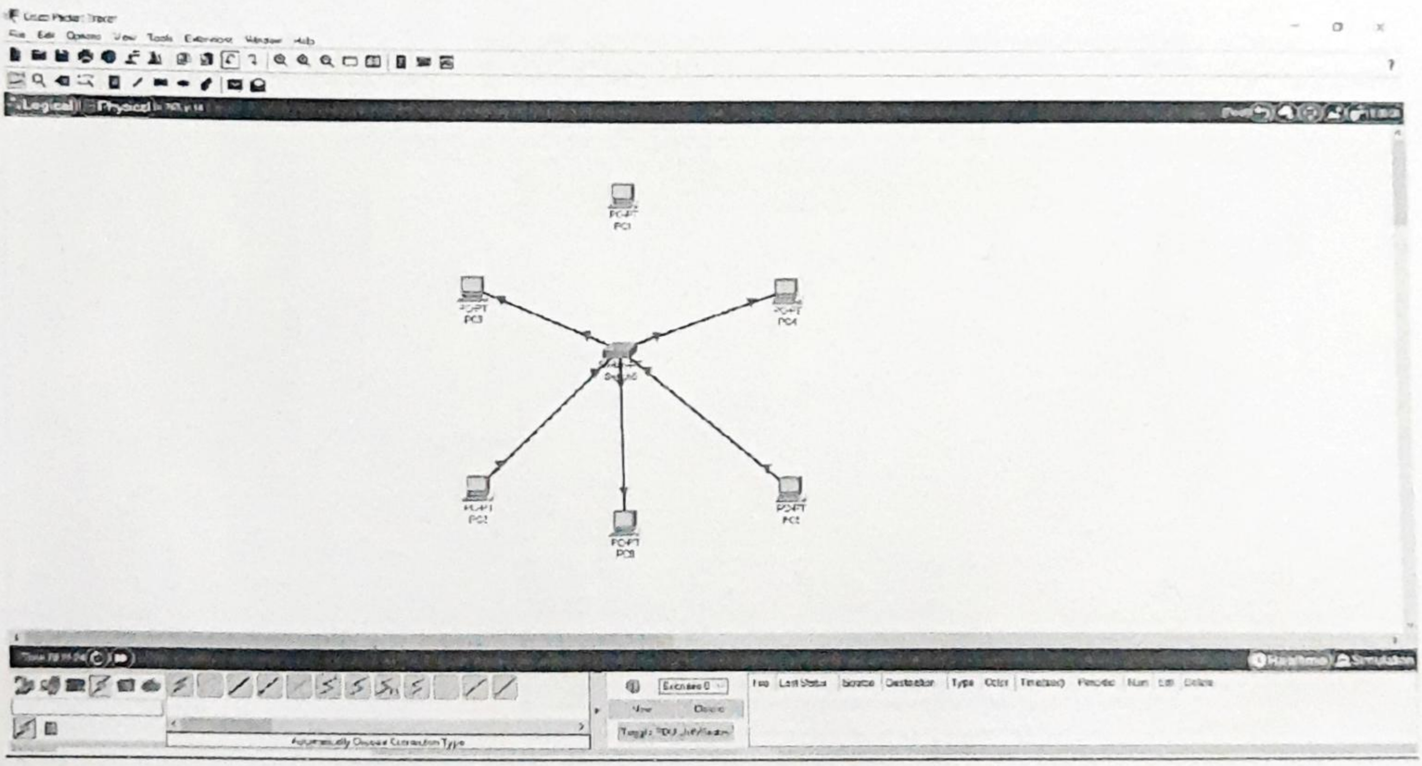


<u>POWER OFF SWITCH 0</u>

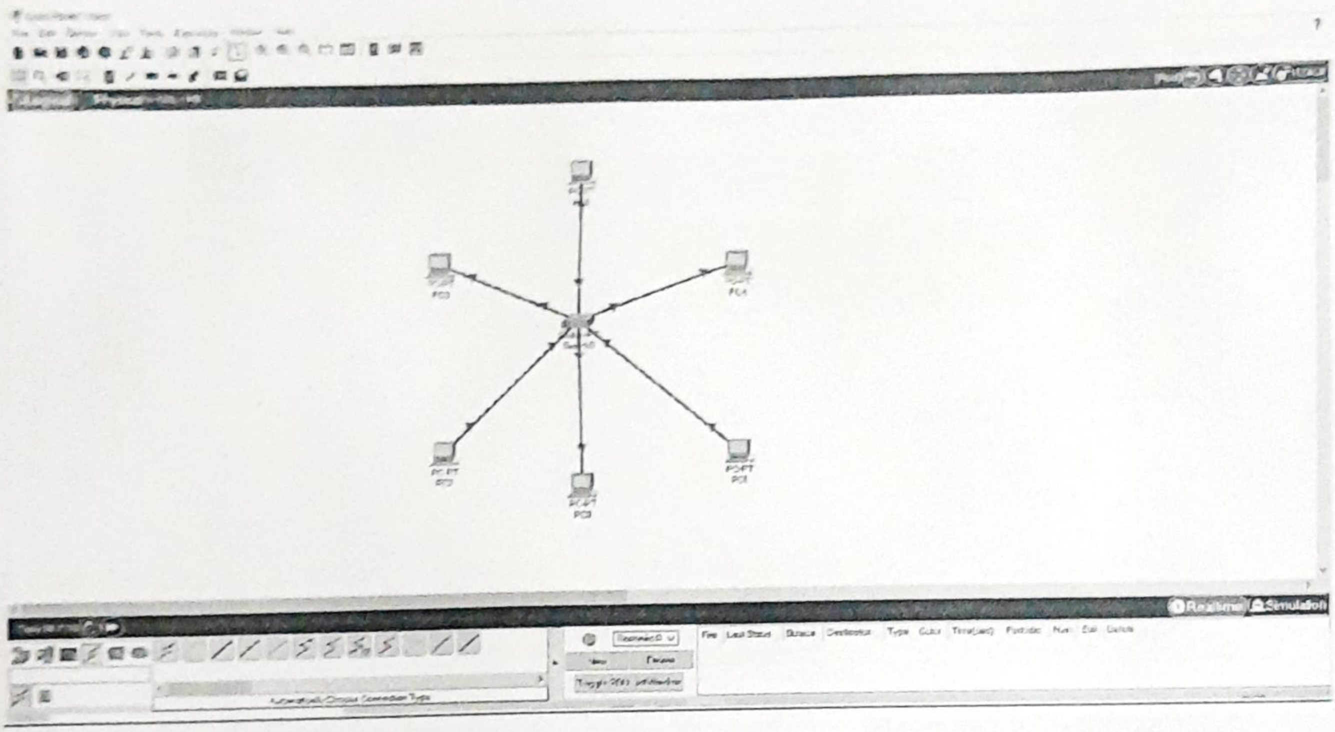


After adding 2 more ports

STEP 5: Now we connect the rest of two PCs (PC4 & PC5) as we connect previous PCs in STEP3 .

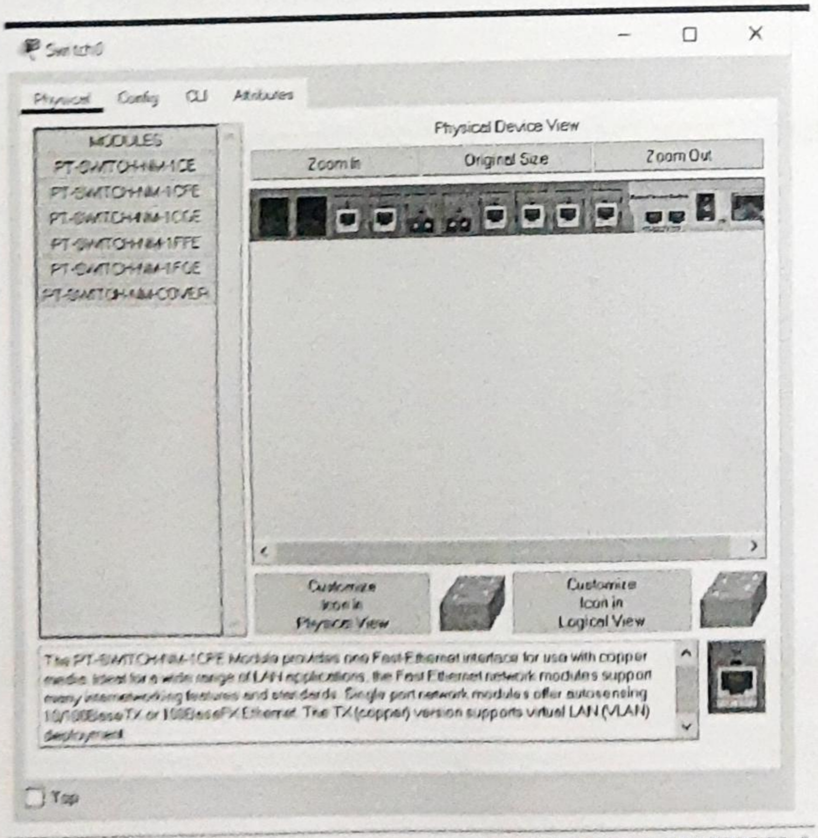


PC4 Connected.

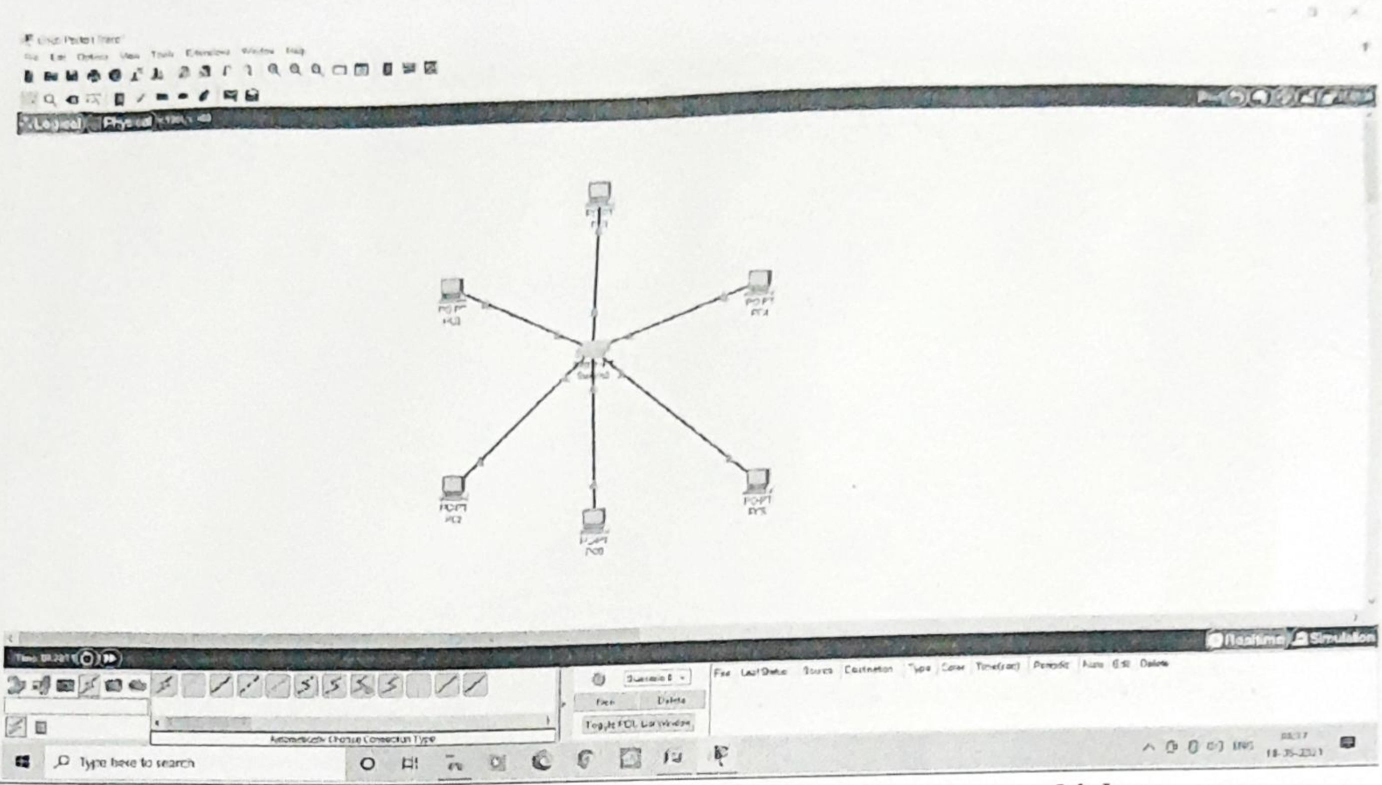


PC5 Connected.

STEP 6 : Now , power on the SWITCH 0 to check topology is working or not.

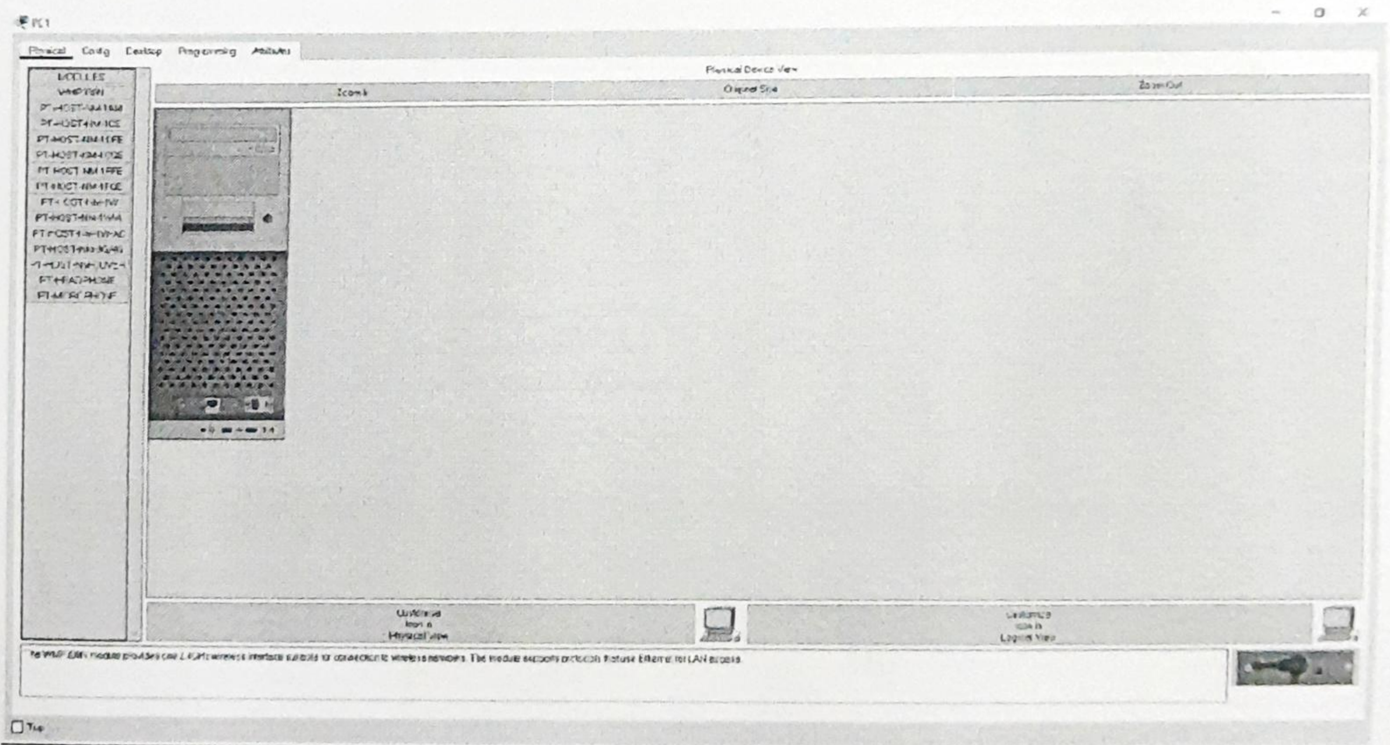


POWER ON SWITCH 0.

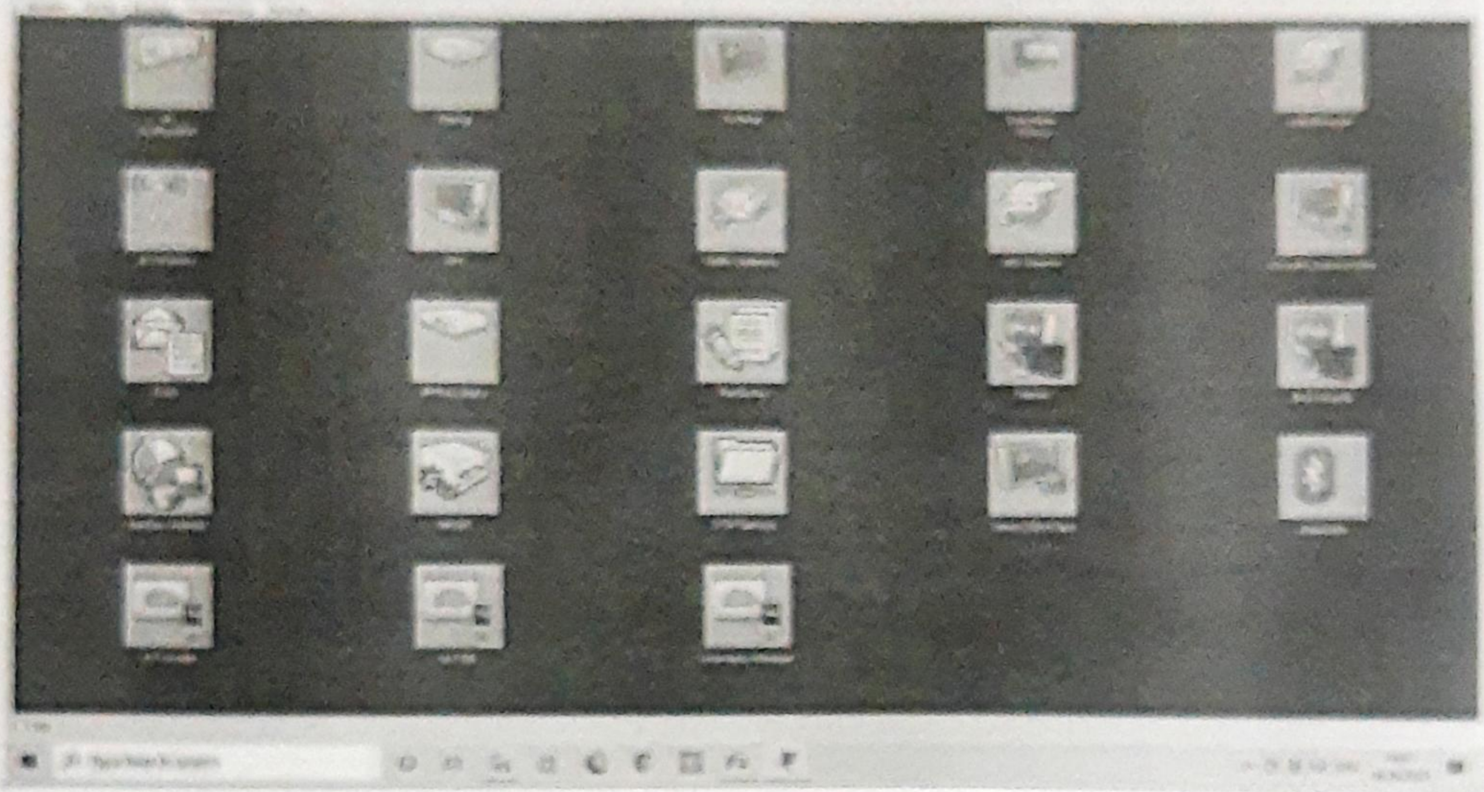


After power on of SWITCH 0 , all the red arrows have became green which means topology is working.

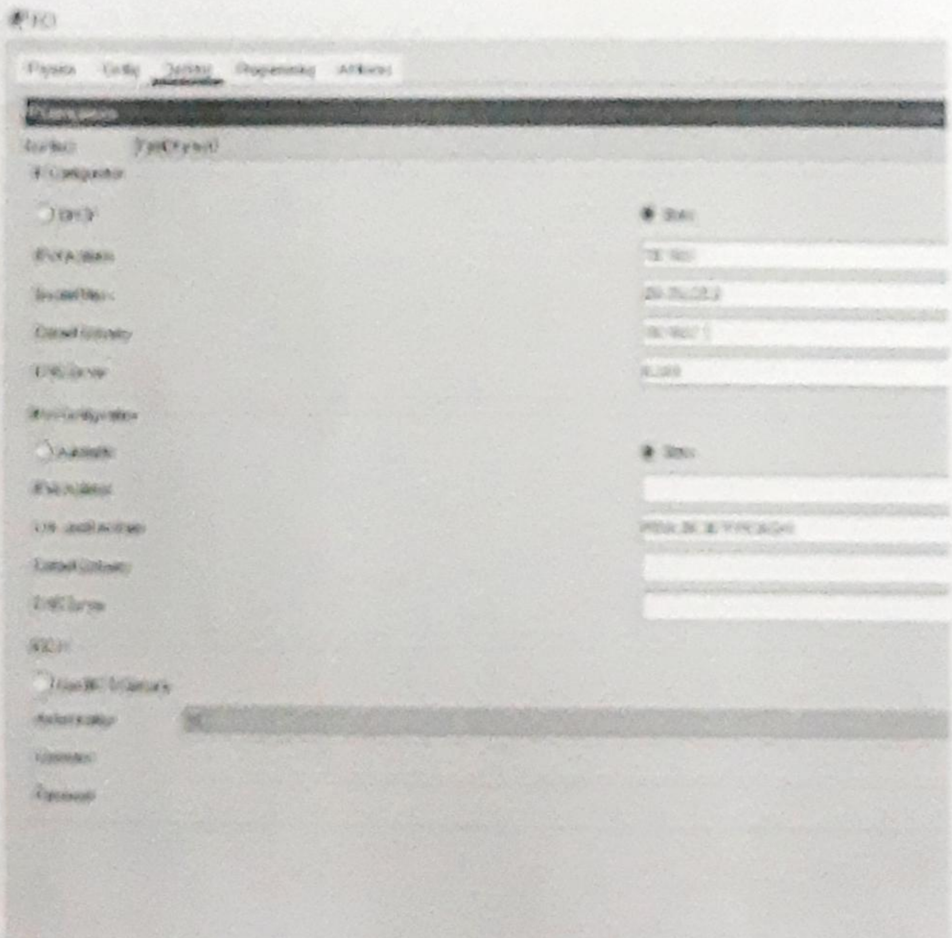
STEP 7 : Now by clicking each PC set their IP address,Subnet Make & Dfault Gateway from the following method.



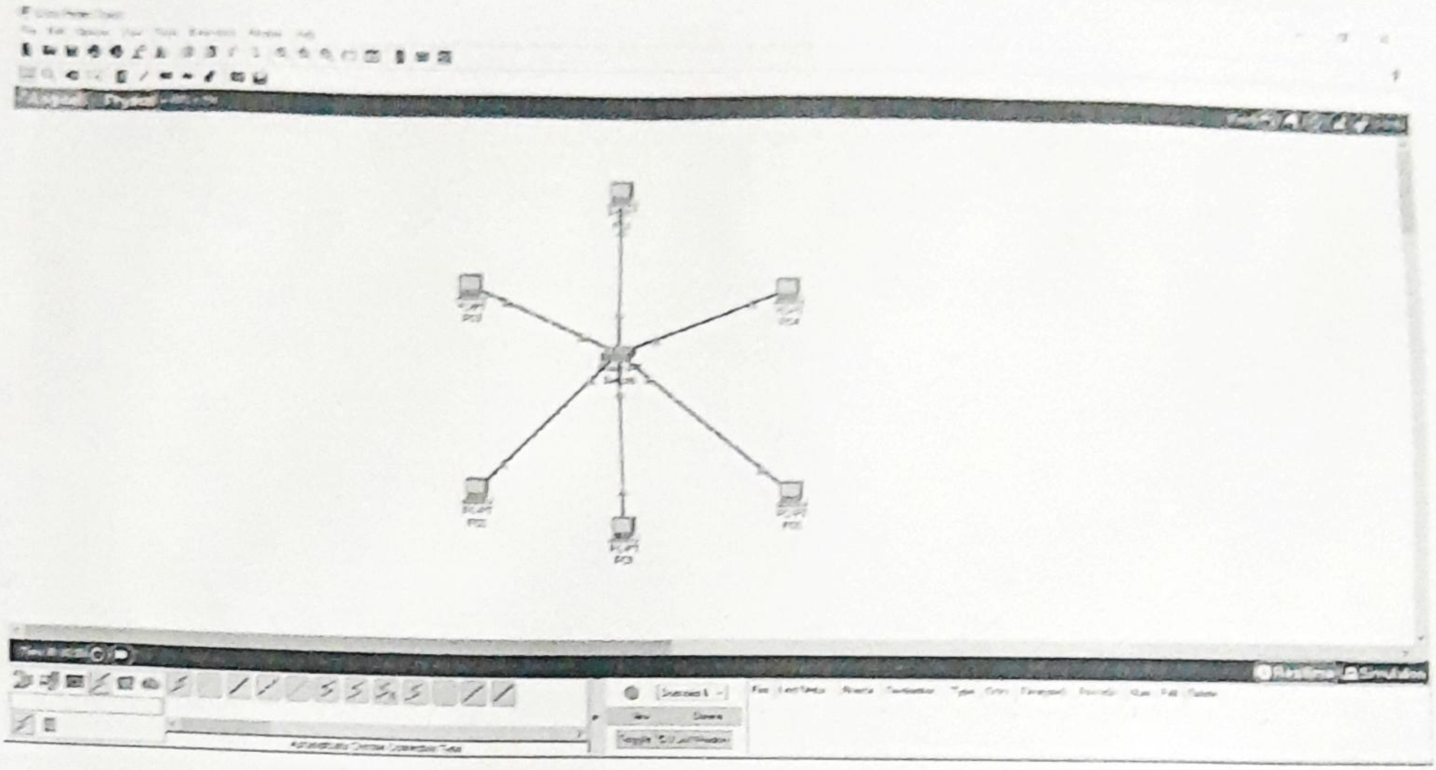
<u>After click on PC and now click on desktop.</u>



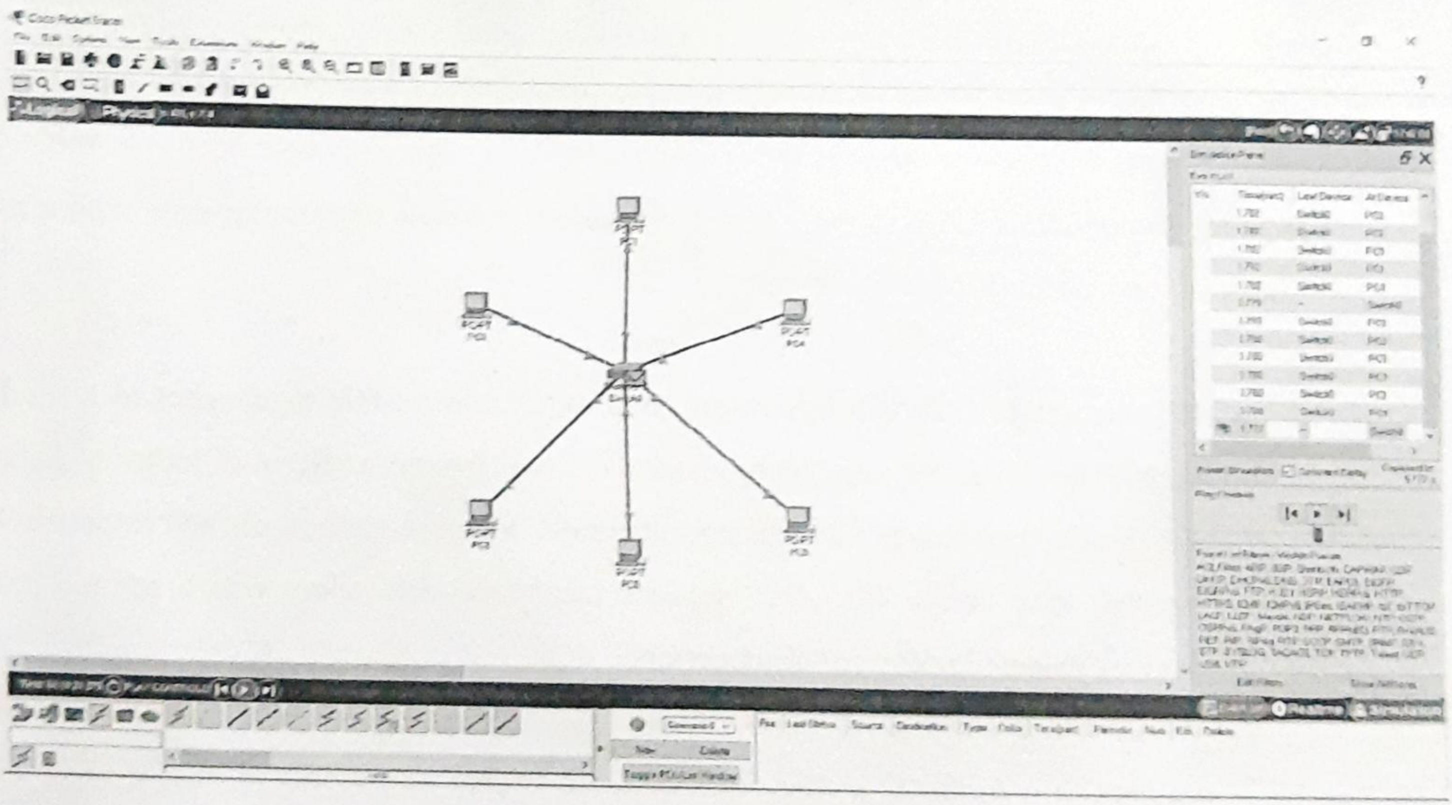
Now select IP configuration.



Now IP configuration is complete for PC1.



Now, star topology is completed.



After simulation of star topology.

EXPERIMENT-6

Aim: To Connect two different LAN using Router in CISCO Packet Tracer

Apparatus (Software): Packet tracer Software

Theory: A router is a device that connects two or more packet-switched networks or subnetworks. It serves two primary functions: managing traffic between these networks by forwarding data packets to their intended IP addresses, and allowing multiple devices to use the same Internet connection.

There are several types of routers, but most routers pass data between LANs (local area networks) and WANs (wide area networks). A LAN is a group of connected devices restricted to a specific geographic area. A LAN usually requires a single router.

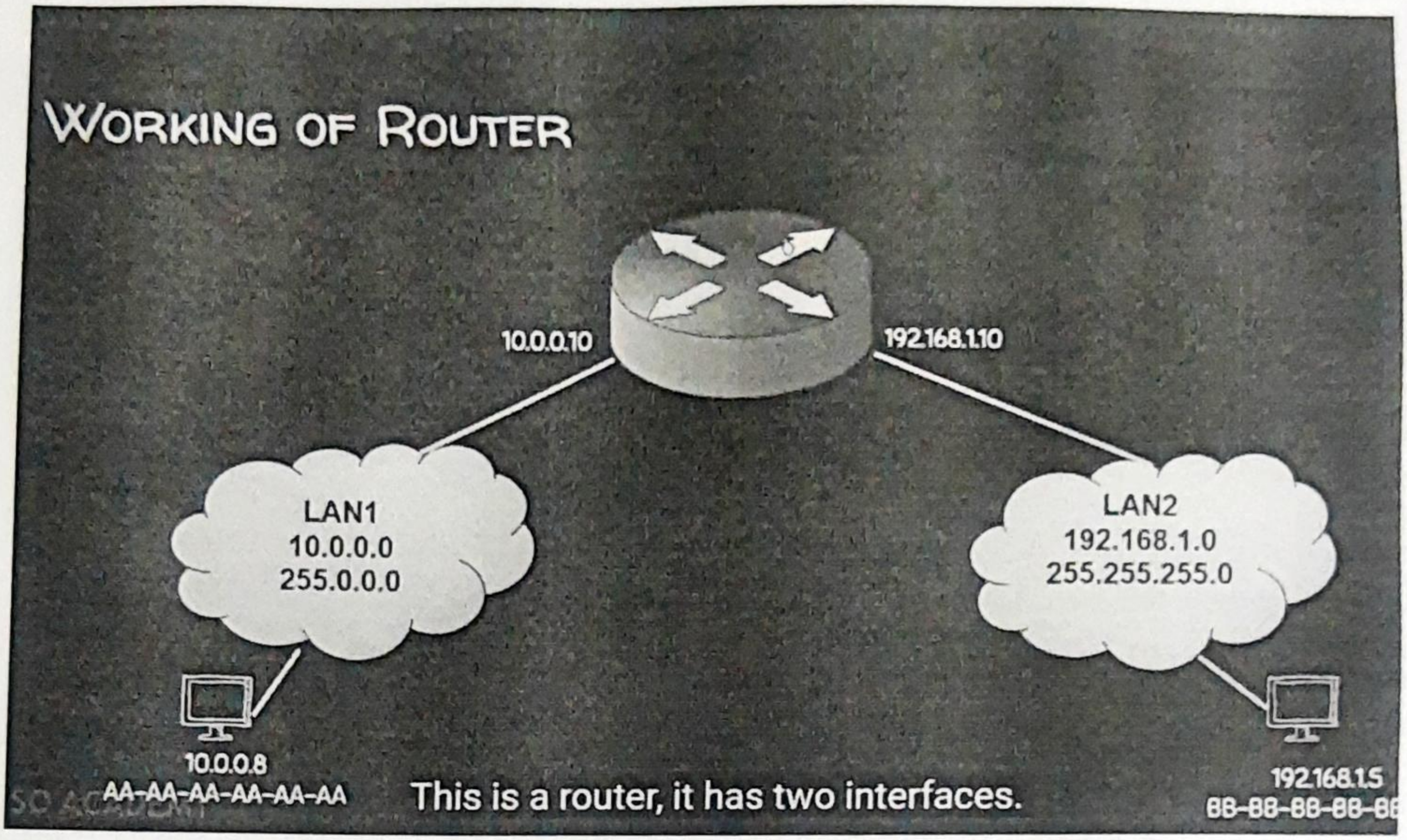
A WAN, by contrast, is a large network spread out over a vast geographic area. Large organizations and companies that operate in multiple locations across the country, for instance, will need separate LANs for each location, which then connect to the other LANs to form a WAN. Because a WAN is distributed over a large area, it often necessitates multiple routers and switches.

In order to connect a LAN to the Internet, a router first needs to communicate with a modem. There are two primary ways to do this:

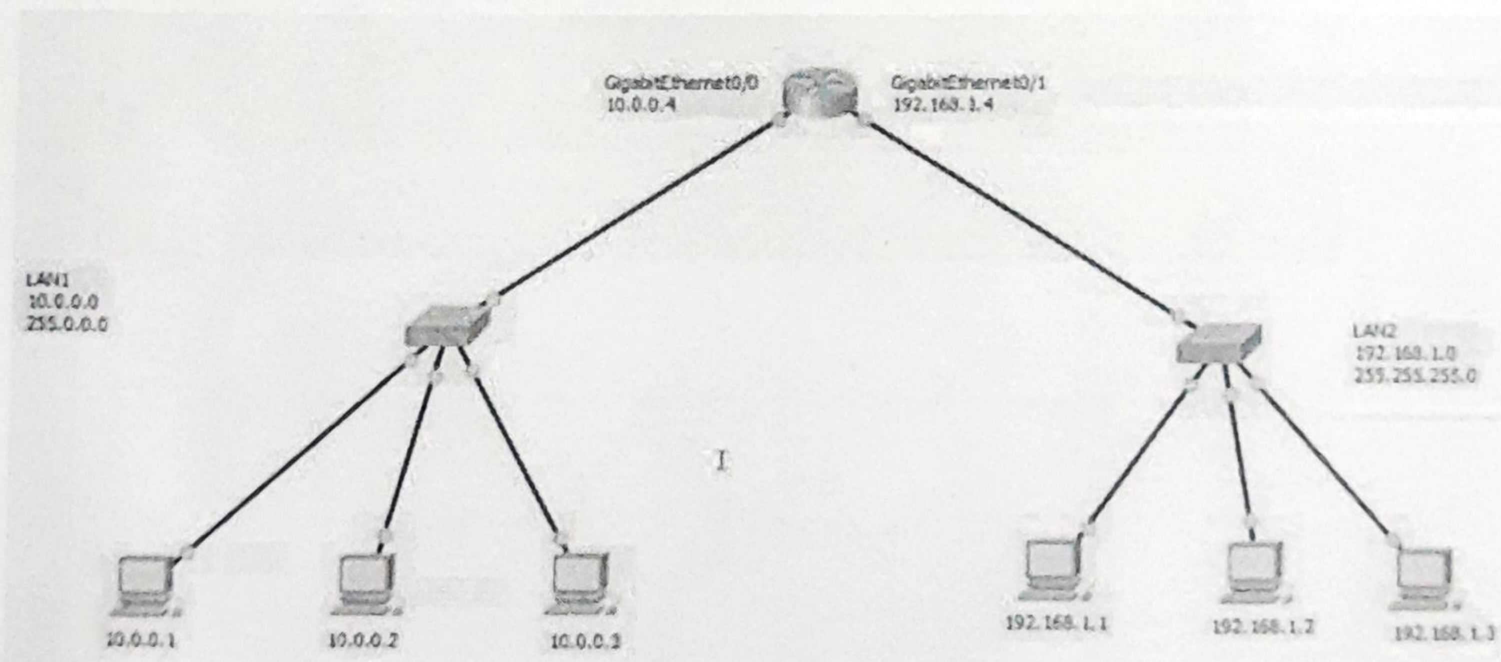
- Wireless router: A wireless router uses an Ethernet cable to connect to a modem. It distributes data by converting packets from binary code into radio signals, then wirelessly broadcasts them using antennae. Wireless routers do not establish LANs; instead, they create WLANs (wireless local area networks), which connect multiple devices using wireless communication.
- Wired router: Like a wireless router, a wired router also uses an Ethernet cable to connect to a modem. It then uses separate cables to connect to one or more devices within the network, create a LAN, and link the devices within that network to the Internet.

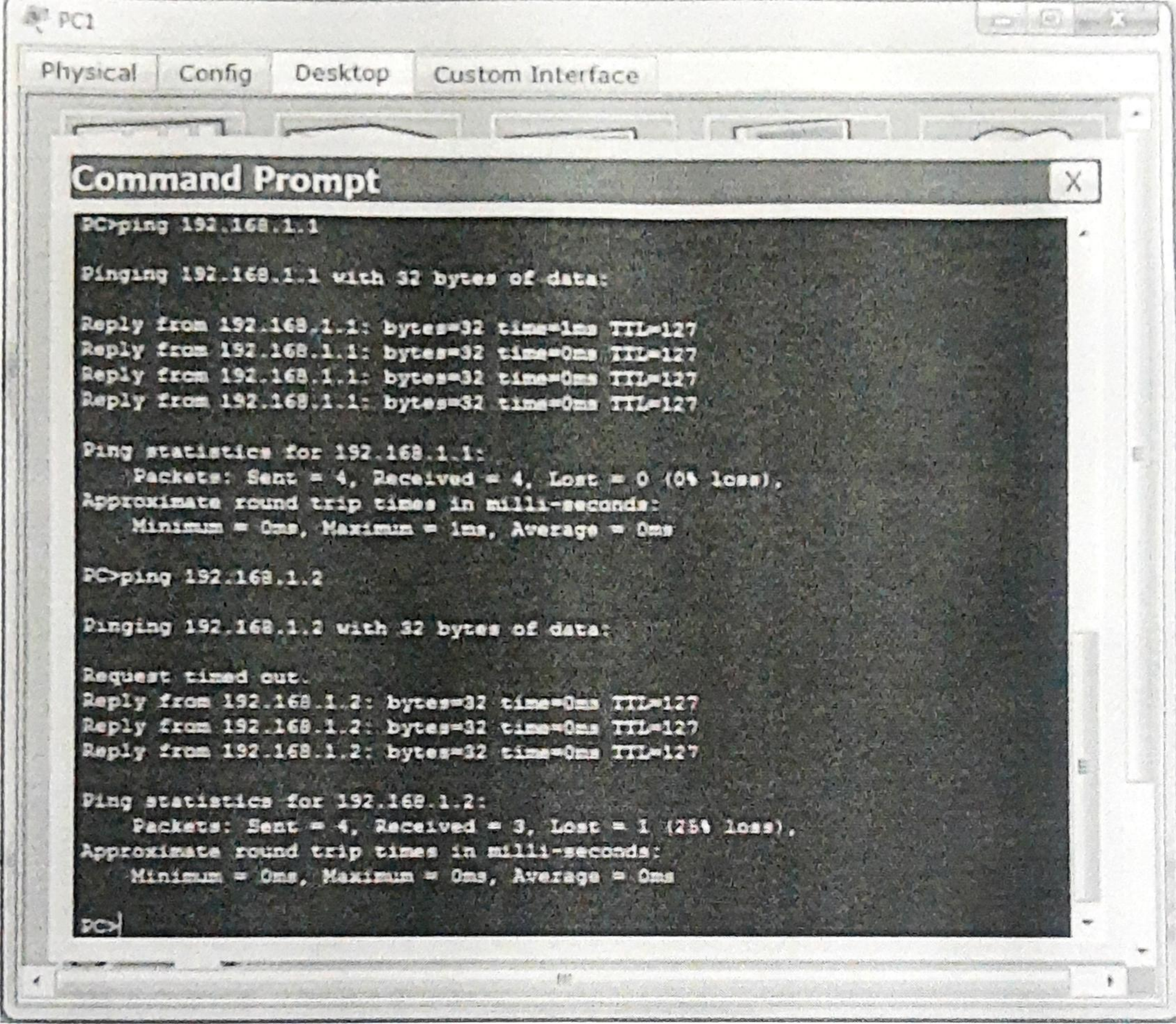
Procedure:

Step 1

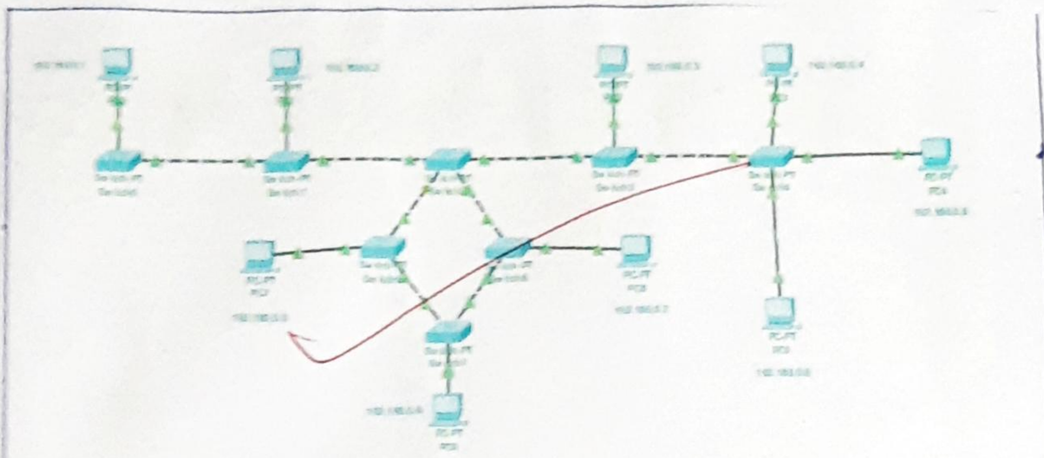


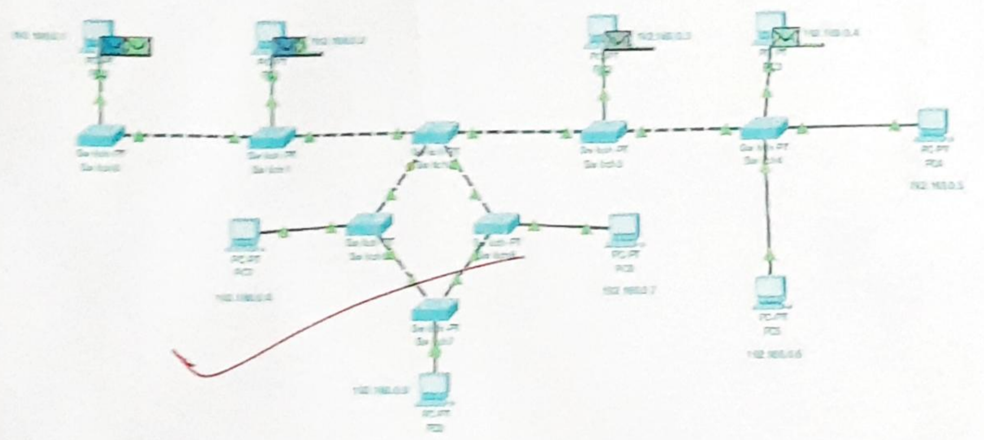
Step 2

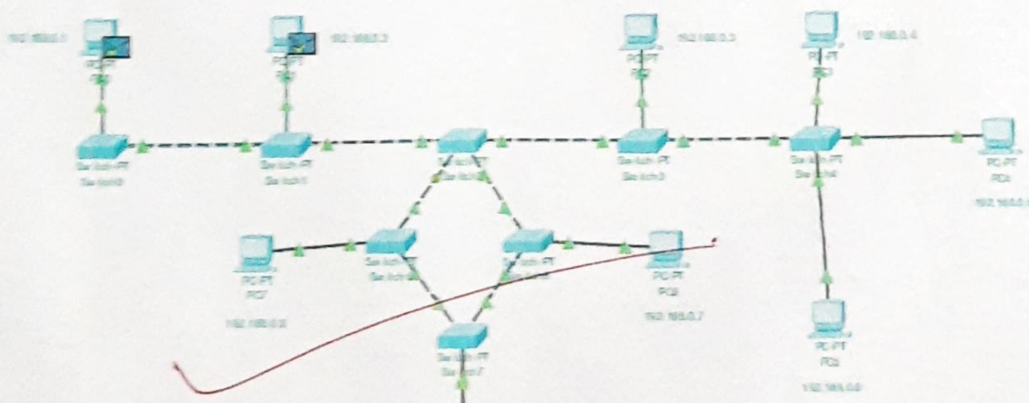



PC1
Physical
Config
Desktop
Custom Interface
Command Prompt
X
PC>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=1ms TTL=127
Reply from 192.168.1.1: bytes=32 time=0ms TTL=127
Reply from 192.168.1.1: bytes=32 time=0ms TTL=127
Reply from 192.168.1.1: bytes=32 time=0ms TTL=127
Ping statistics for 192.168.1.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
PC>ping 192.168.1.2
Pinging 192.168.1.2 with 32 bytes of data:
Request timed out.
Reply from 192.168.1.2: bytes=32 time=0ms TTL=127
Reply from 192.168.1.2: bytes=32 time=0ms TTL=127
Reply from 192.168.1.2: bytes=32 time=0ms TTL=127
Ping statistics for 192.168.1.2:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
PC>

ERVATION: -

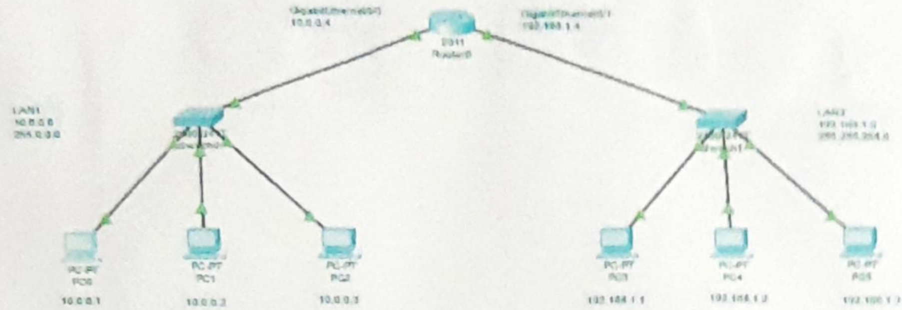


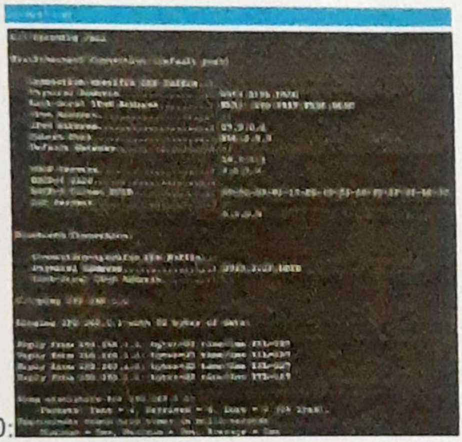




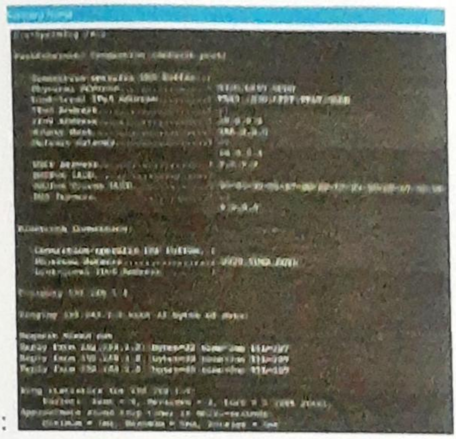
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num
	Successful	PC0	PC8	ICMP		0.000	N	0
	Successful	PC1	PC7	ICMP		0.000	N	1
	Successful	PC2	PC5	ICMP		0.000	N	2
	Successful	PC2	PC5	ICMP		0.000	N	2
	Successful	PC3	PC4	ICMP		0.000	N	3

RESULT:

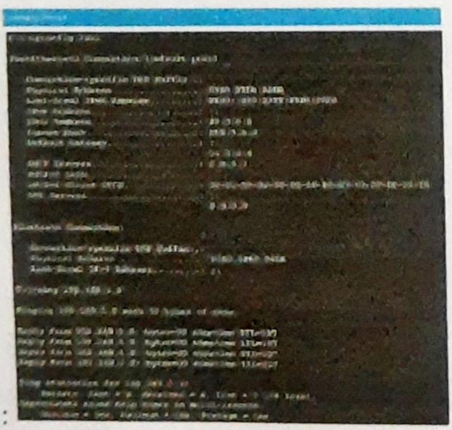




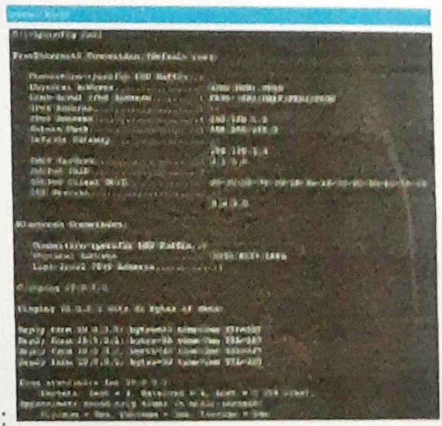
PC0:



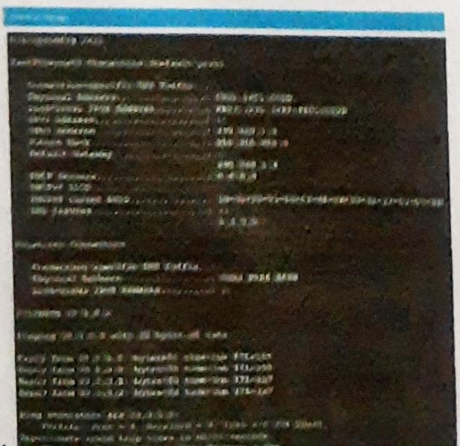
PC1:



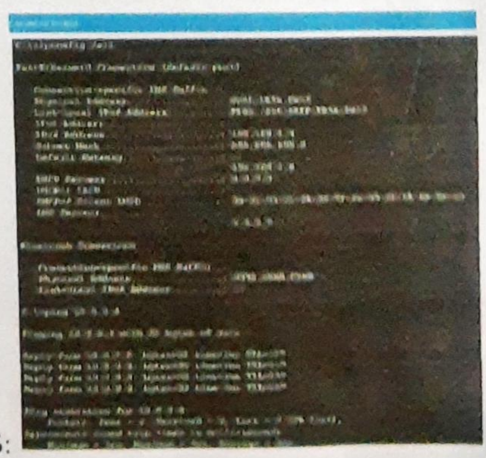
PC2:



PC3:



PC4:



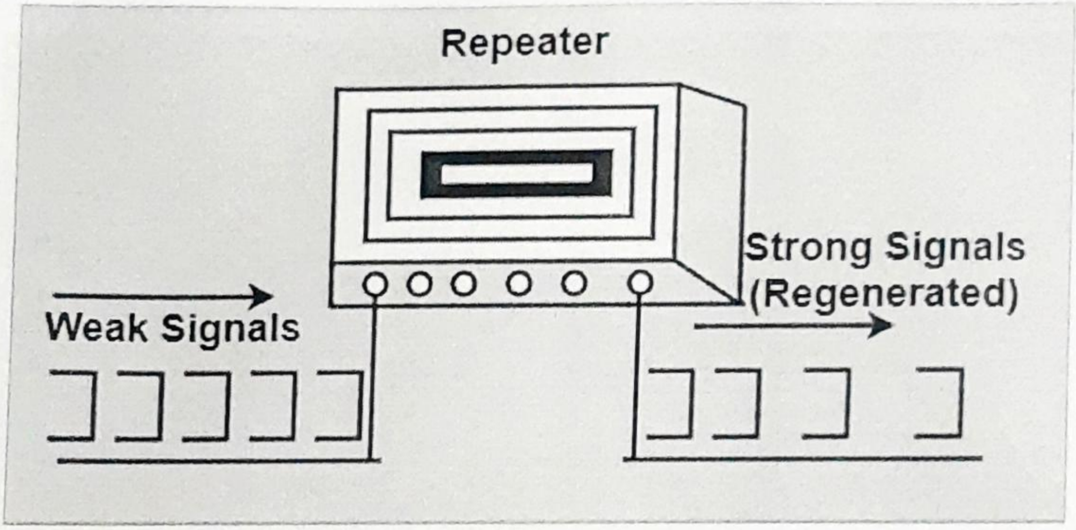
PC5:

EXPERIMENT-7

Aim: To Connect two different LAN using Repeater in CISCO Packet Tracer

Apparatus (Software): Packet tracer Software

Theory: A repeater is a dynamic network device used to reproduce the signals when they transmit over a greater distance so that the signal's strength remains equal. It can be used to create an Ethernet network. A repeater that occurs as the first layer of the OSI layer is the physical layer.



Features of Repeaters:

- **These repeaters are linked to each other at the physical layer. It sends the signals for the unsteady areas to enlarge the system signals. These receptors linked the various network signals to convert the data between the two devices. These repeaters can eliminate the distance between the two devices.**
- **The repeaters can frequently monitor the signals that are created between the two LANs. Repeaters can support dynamic networking. Multi-site connection solutions provide the 30 repeaters linked to it.**
- **The IP network links all the repeaters with an IP site relation network. This IP network can support a fast response to any issue in the repeater network. These receptors can support 100 % digital communication so that they do not require to wait for analog voice calls.**

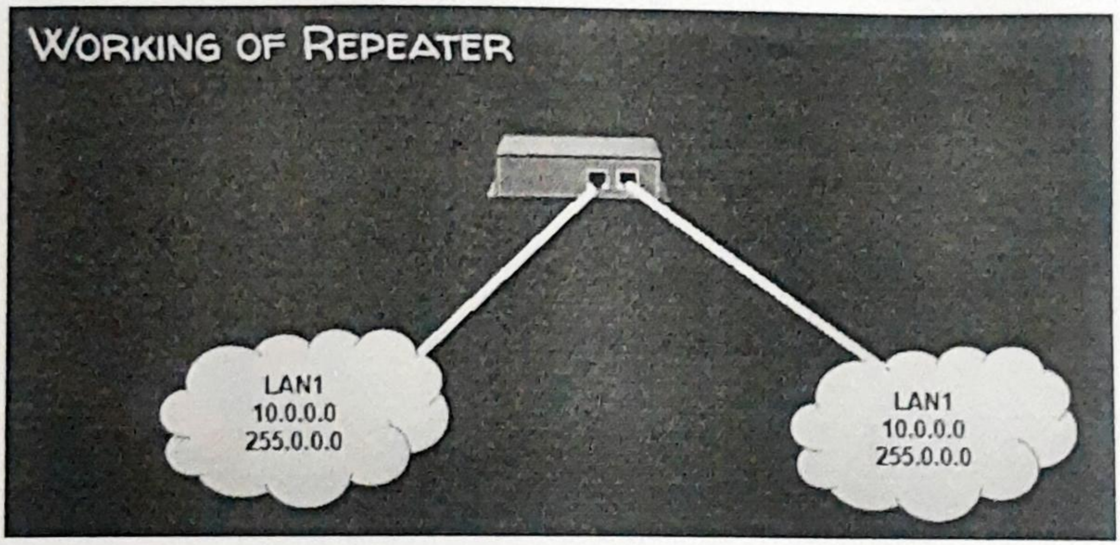
Advantages of Repeater

The main advantages of repeaters are –

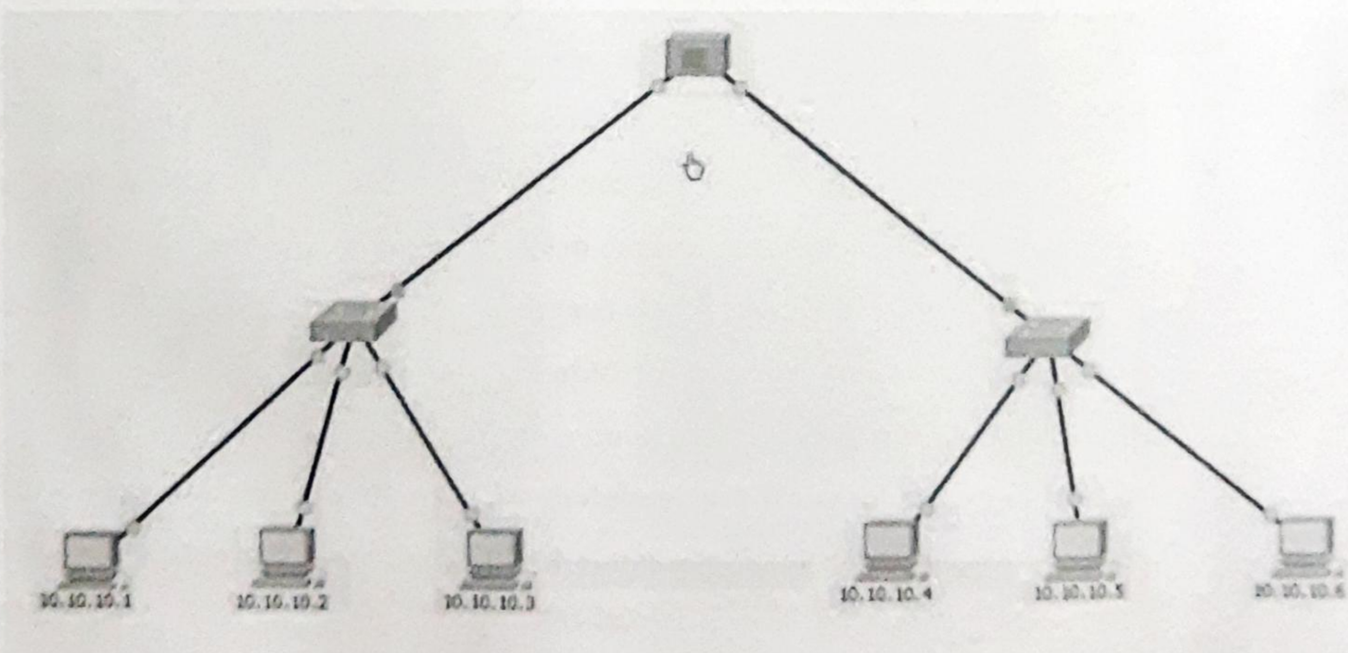
- The signals get weaker as they transit to greater distances. The repeater provides the stability of the signals. These repeaters are cost-effective and easy to use.
- The repeaters don't influence network performance. It is not all signals that can be linked using physical media.
- These repeaters can retransmit the information and powerful the weak signals.

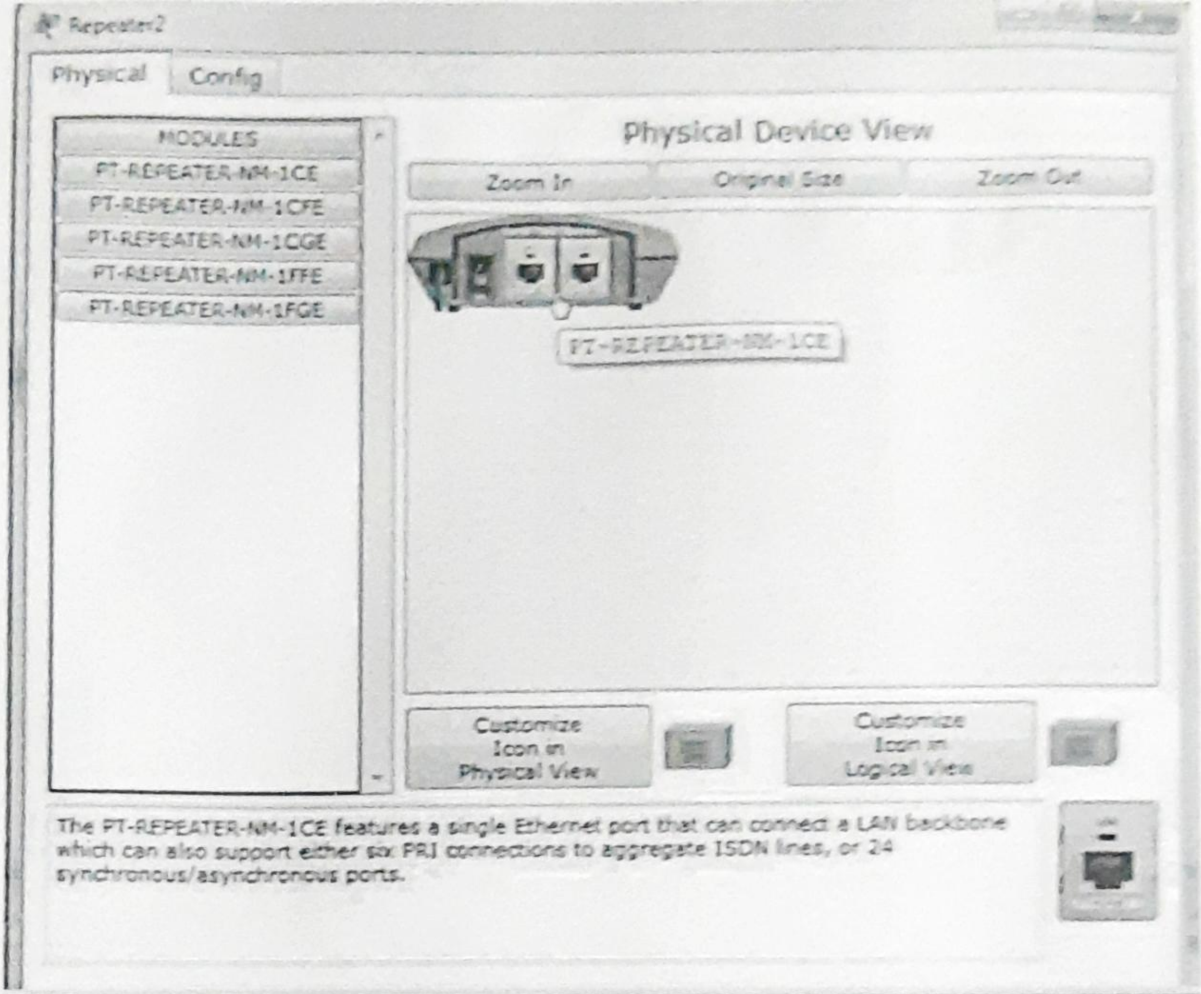
Procedure:

Step 1

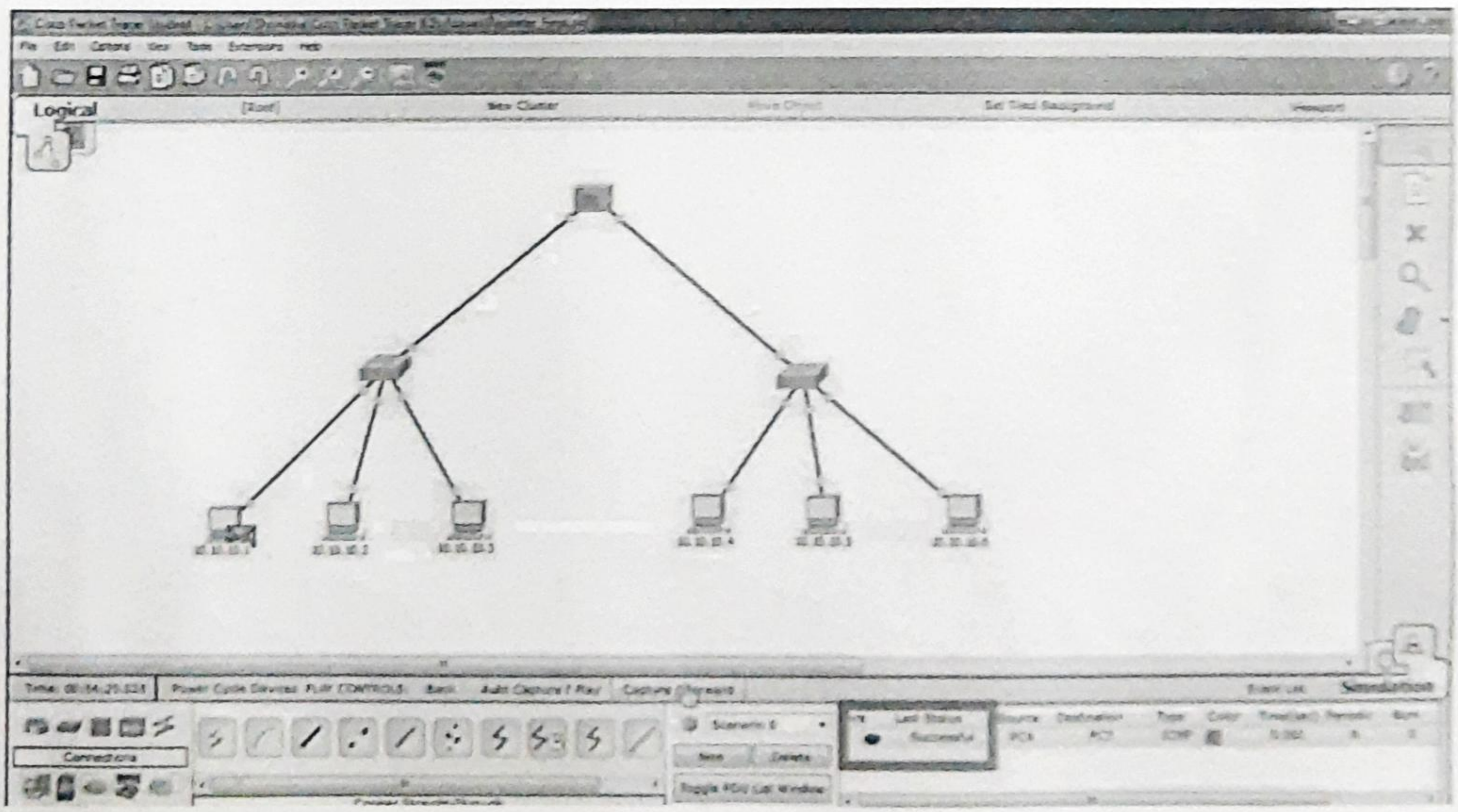


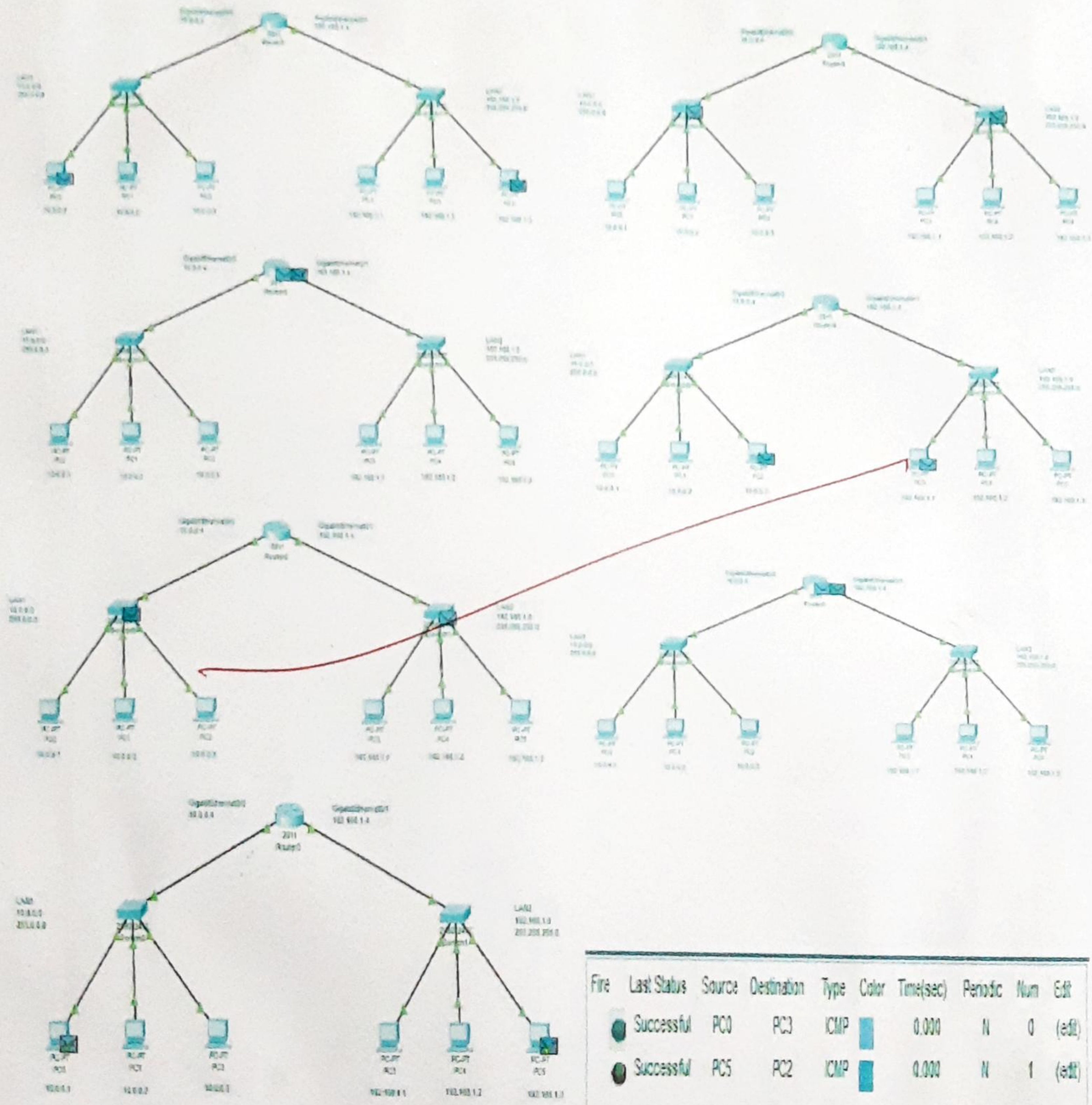
Step 2



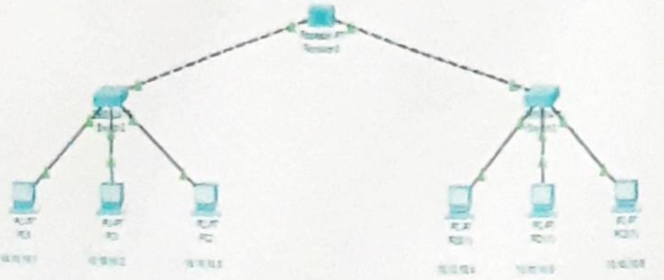

Repeater2
Physical
Config
MODULES
PT-REPEATER-NM-1CE
PT-REPEATER-NM-1CFE
PT-REPEATER-NM-1CGE
PT-REPEATER-NM-1FFE
PT-REPEATER-NM-1FGE
Physical Device View
Zoom In
Original Size
Zoom Out
PT-REPEATER-NM-1CE
Customize Icon in Physical View
Customize Icon in Logical View
The PT-REPEATER-NM-1CE features a single Ethernet port that can connect a LAN backbone which can also support either six PRI connections to aggregate ISDN lines, or 24 synchronous/asynchronous ports.

Step 4

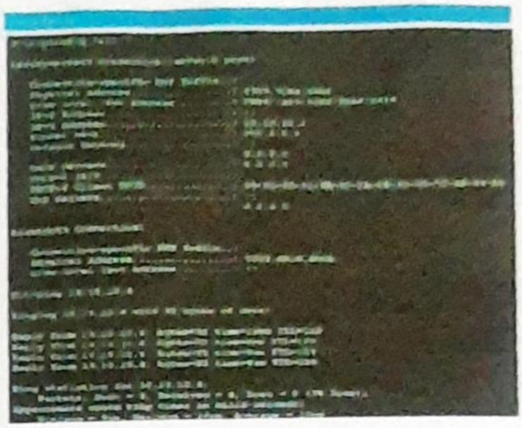

Logical



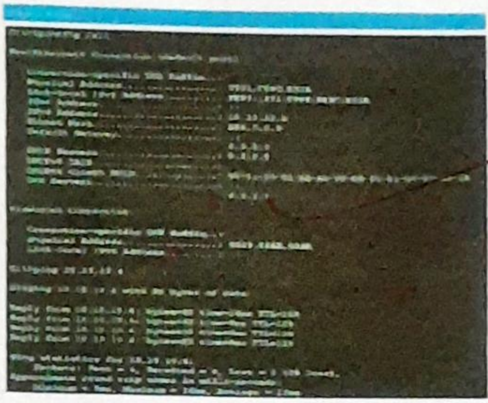
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Successful	PC0	PC3	ICMP		0.000	N	0	(edit)
	Successful	PC5	PC2	ICMP		0.000	N	1	(edit)



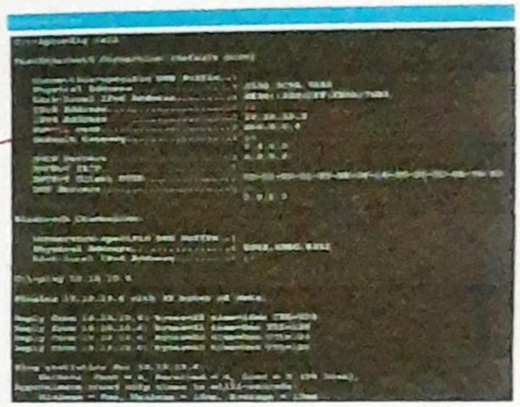
PCO:



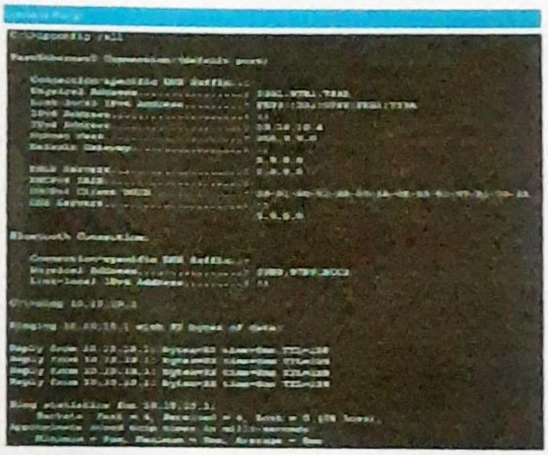
PC1:



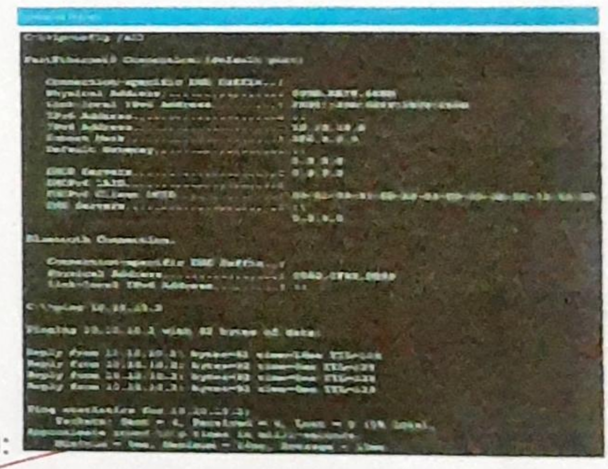
PC2:



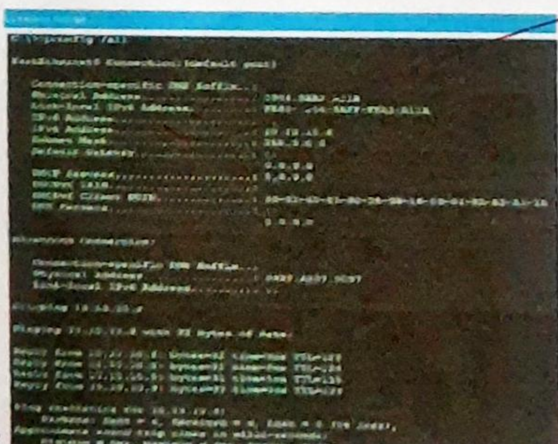
PC0(1):



PC1(1):



PC2(1):



EXPERIMENT-8

Aim: To Configure IP Static Routing in CISCO Packet Tracer

Apparatus (Software): Packet tracer Software

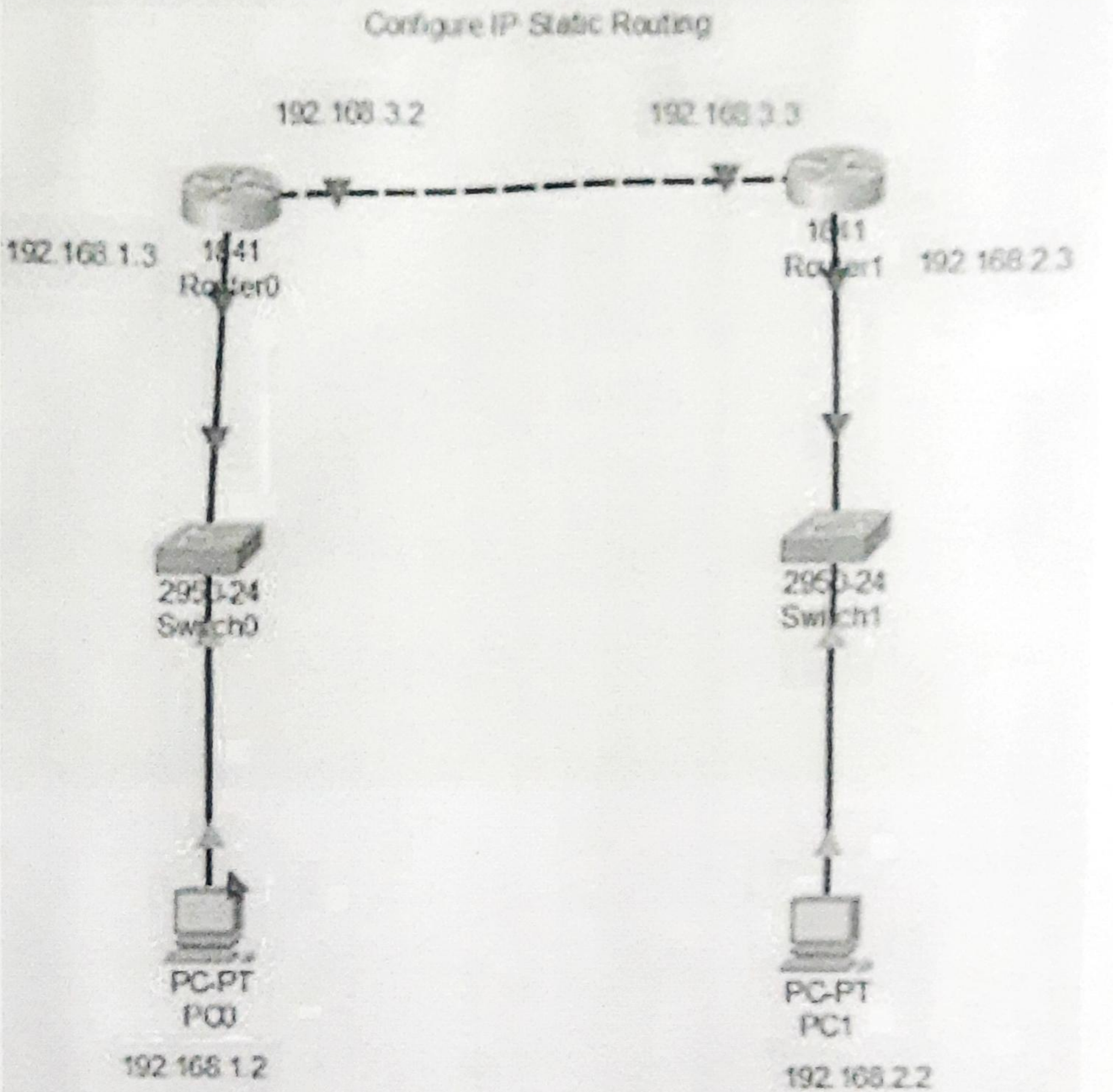
Theory: Static routing is a form of routing that occurs when a router uses a manually-configured routing entry, rather than information from dynamic routing traffic. In many cases, static routes are manually configured by a network administrator by adding in entries into a routing table, though this may not always be the case. Unlike dynamic routing, static routes are fixed and do not change if the network is changed or reconfigured. Static routing and dynamic routing are not mutually exclusive. Both dynamic routing and static routing are usually used on a router to maximise routing efficiency and to provide backups in case dynamic routing information fails to be exchanged. Static routing can also be used in stub networks, or to provide a gateway of last resort.

Static routing may have the following uses:

- Static routing can be used to define an exit point from a router when no other routes are available or necessary. This is called a default route.
- Static routing can be used for small networks that require only one or two routes. This is often more efficient since a link is not being wasted by exchanging dynamic routing information.
- Static routing is often used as a complement to dynamic routing to provide a failsafe backup if a dynamic route is unavailable.
- Static routing is often used to help transfer routing information from one routing protocol to another (routing redistribution).

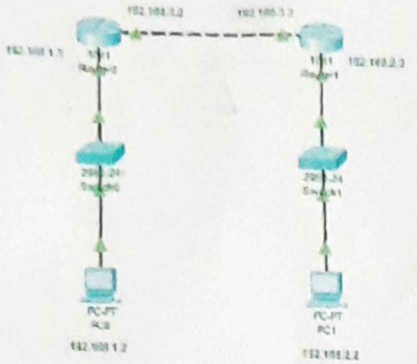
Static routing, if used without dynamic routing, has the following advantages:

- Static routing causes very little load on the CPU of the router, and produces no traffic to other routers.
- Static routing leaves the network administrator with full control over the routing behavior of the network.
- Static Routing is very easy to configure on small networks.


Configure IP Static Routing
192.168.3.2
192.168.3.3
192.168.1.3
1841
Router0
1841
Router1
192.168.2.3
2950-24
Switch0
2950-24
Switch1
PC-PT
PC0
PC-PT
PC1
192.168.1.2
192.168.2.2

Command Prompt

```
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.2.2: bytes=32 time<1ms TTL=126
Reply from 192.168.2.2: bytes=32 time<1ms TTL=126
Reply from 192.168.2.2: bytes=32 time=11ms TTL=126

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 11ms, Average = 3ms

C:\>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.2.2: bytes=32 time<1ms TTL=126
Reply from 192.168.2.2: bytes=32 time=12ms TTL=126
```

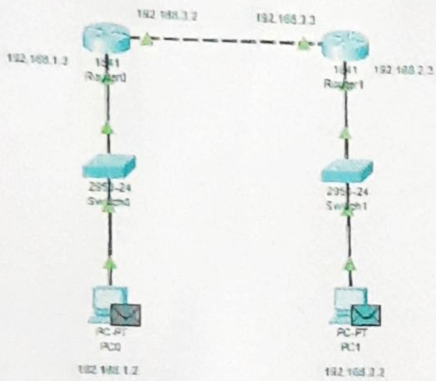


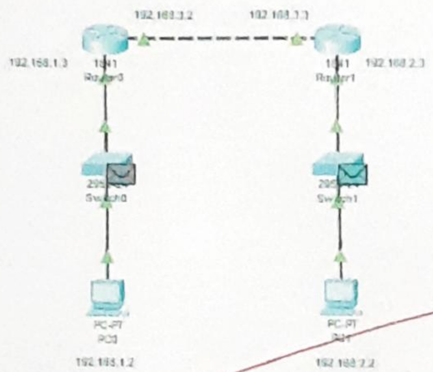
PC0:

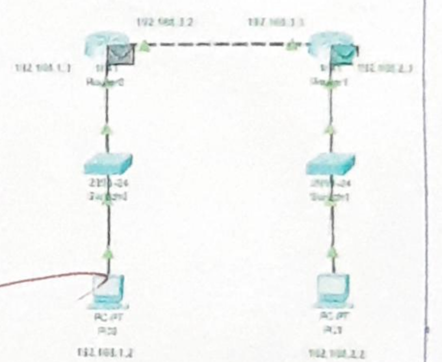
```
C:\>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.2.2: bytes=32 time=10ms TTL=126
Reply from 192.168.2.2: bytes=32 time=10ms TTL=126
Reply from 192.168.2.2: bytes=32 time=10ms TTL=126
Reply from 192.168.2.2: bytes=32 time=10ms TTL=126

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 10ms, Average = 10ms
```

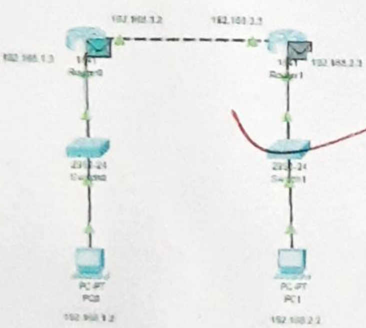
PC1:

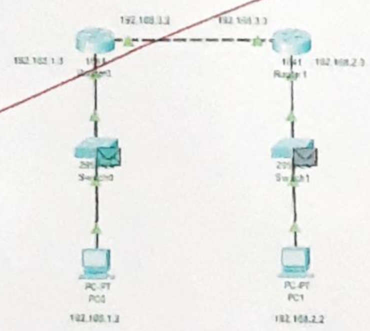
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time<1ms TTL=126
Reply from 192.168.1.2: bytes=32 time<1ms TTL=126
Reply from 192.168.1.2: bytes=32 time<1ms TTL=126
Reply from 192.168.1.2: bytes=32 time=12ms TTL=126

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 12ms, Average = 3ms
```

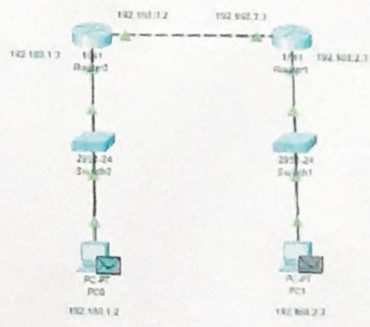


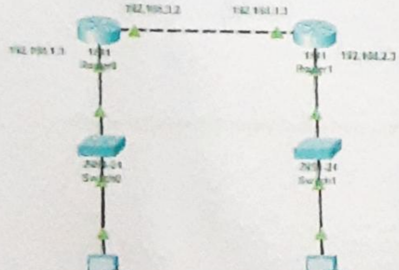




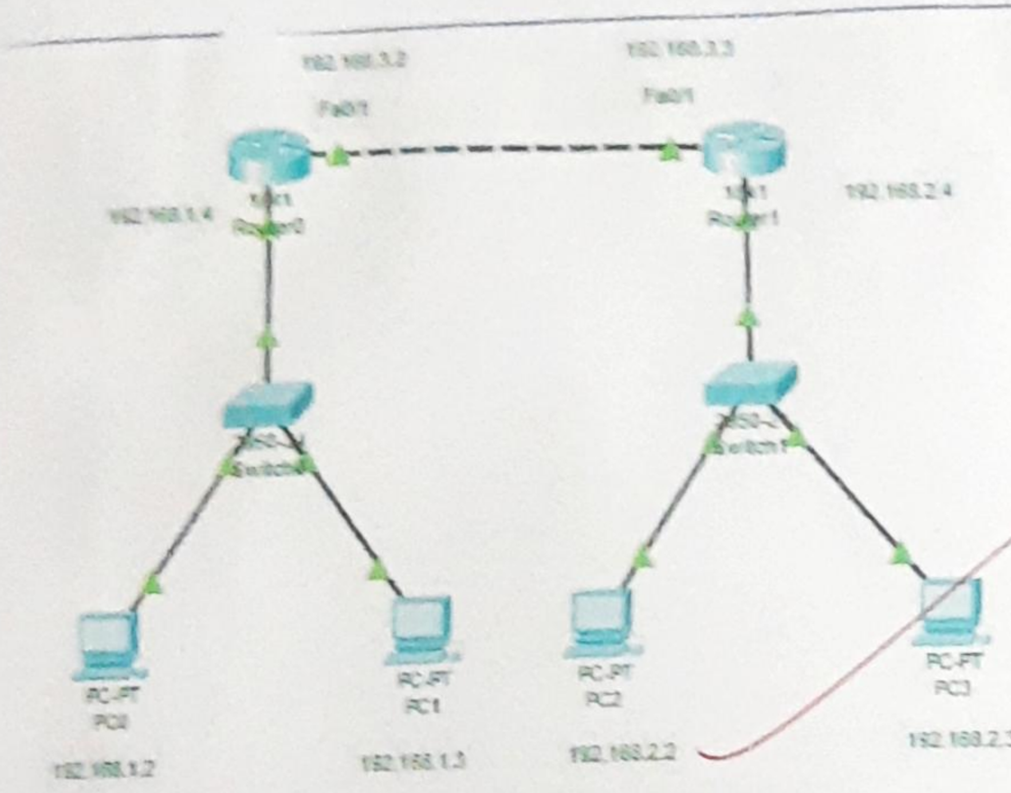








Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Successful	PC0	PC1	ICMP		0.000	N	0	(edit)
	Successful	PC1	PC0	ICMP		0.000	N	1	(edit)



PC0:

```
C:\>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

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

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

PC1:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

PC2:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:

Reply from 192.168.2.3: bytes=32 time<1ms TTL=128
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

PC3:

```
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time<1ms TTL=126
Reply from 192.168.1.3: bytes=32 time<1ms TTL=126
Reply from 192.168.1.3: bytes=32 time<1ms TTL=126
Reply from 192.168.1.3: bytes=32 time<1ms TTL=126

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

EXPERIMENT-9

Aim: To Configure IP Static Routing using two routers, two switches and 4 PC in CISCO Packet Tracer

Apparatus (Software): Packet tracer Software

Theory: Static routing is a form of routing that occurs when a router uses a manually-configured routing entry, rather than information from dynamic routing traffic. In many cases, static routes are manually configured by a network administrator by adding in entries into a routing table, though this may not always be the case. Unlike dynamic routing, static routes are fixed and do not change if the network is changed or reconfigured. Static routing and dynamic routing are not mutually exclusive. Both dynamic routing and static routing are usually used on a router to maximise routing efficiency and to provide backups in case dynamic routing information fails to be exchanged. Static routing can also be used in stub networks, or to provide a gateway of last resort.

Static routing may have the following uses:

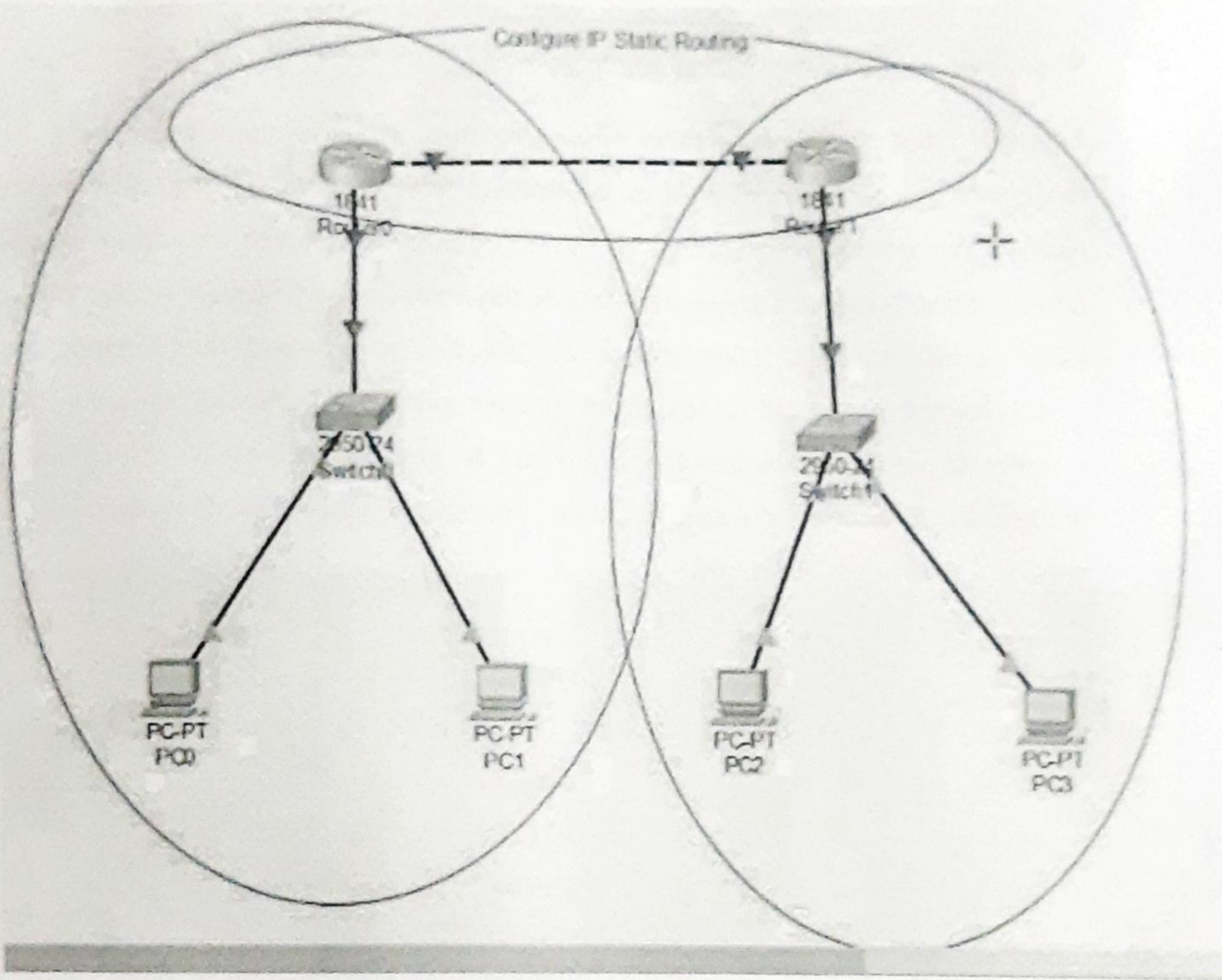
- Static routing can be used to define an exit point from a router when no other routes are available or necessary. This is called a default route.
- Static routing can be used for small networks that require only one or two routes. This is often more efficient since a link is not being wasted by exchanging dynamic routing information.
- Static routing is often used as a complement to dynamic routing to provide a failsafe backup if a dynamic route is unavailable.
- Static routing is often used to help transfer routing information from one routing protocol to another (routing redistribution).

Static routing, if used without dynamic routing, has the following advantages:

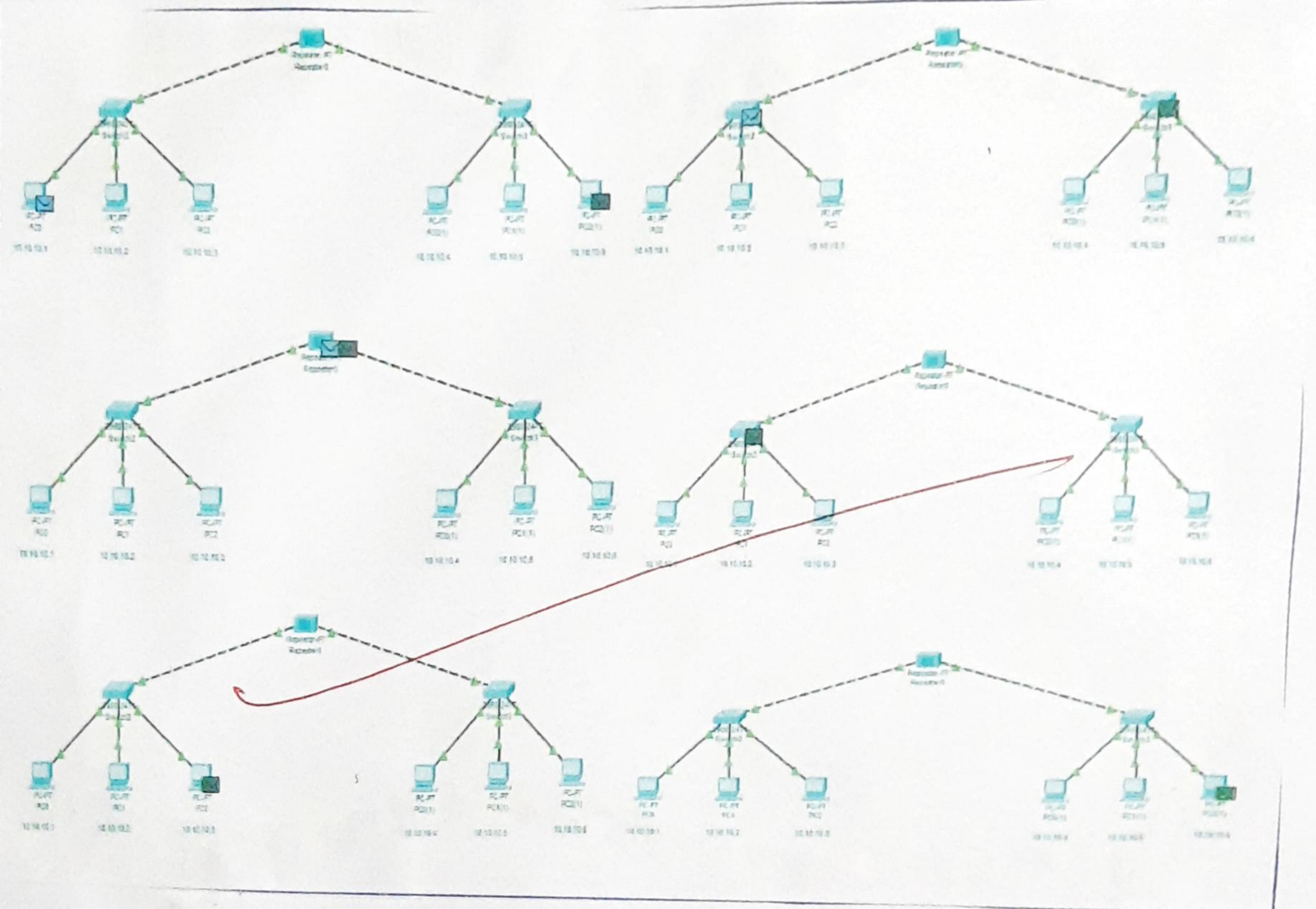
- Static routing causes very little load on the CPU of the router, and produces no traffic to other routers.
- Static routing leaves the network administrator with full control over the routing behavior of the network.
- Static Routing is very easy to configure on small networks.

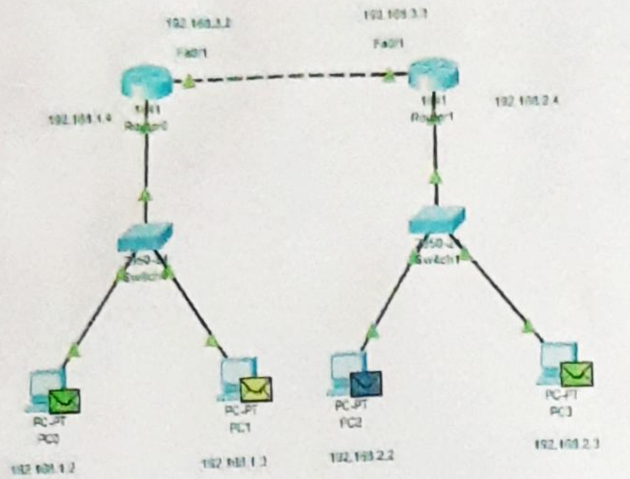
Procedure:

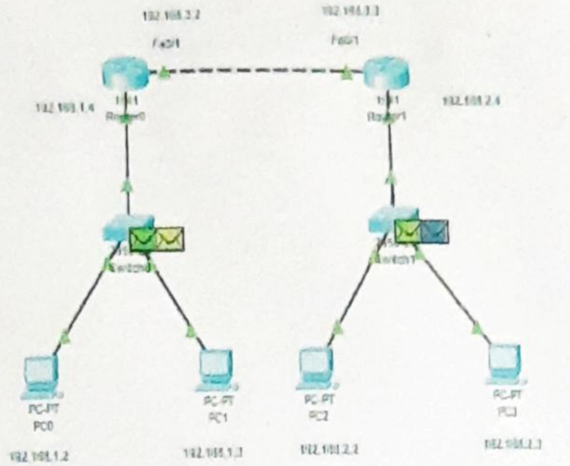
Step 1

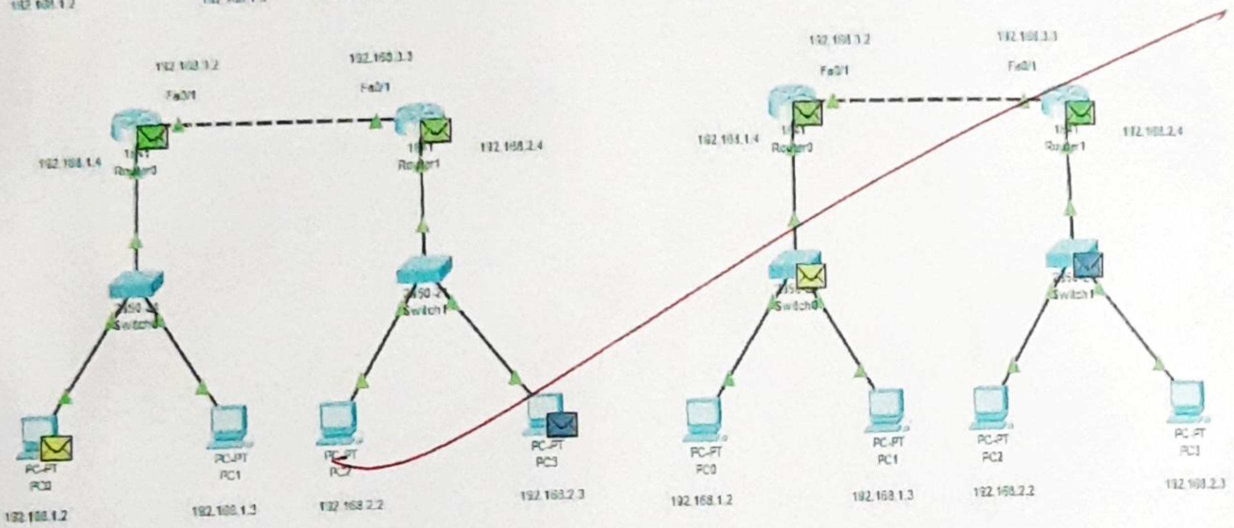


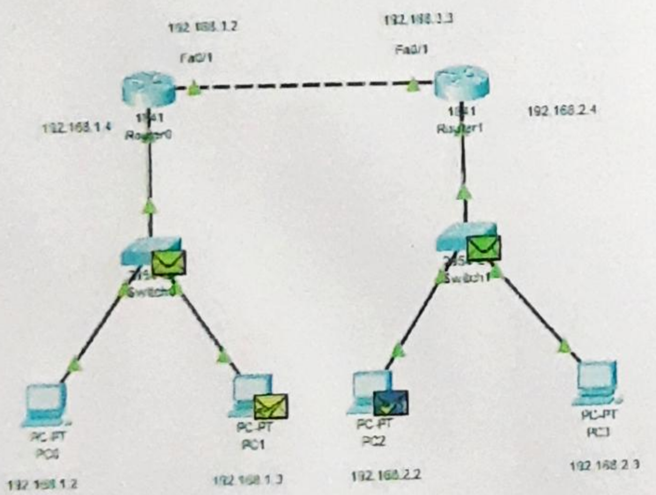
OBSERVATION: -

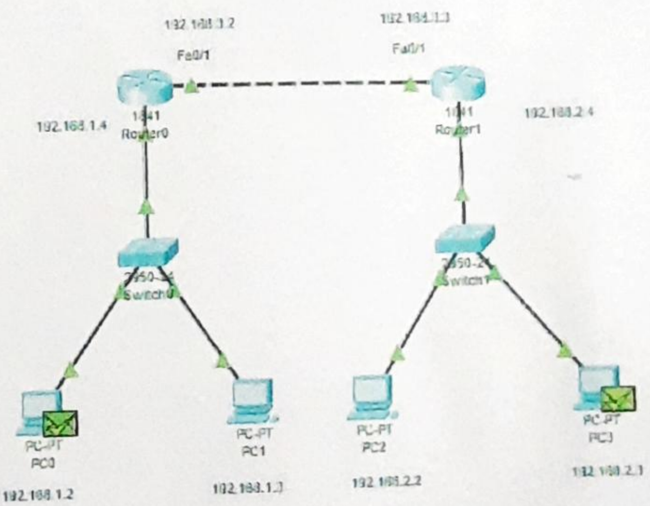












Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num
	Successful	PC0	PC2	ICMP		0.000	N	0
	Successful	PC3	PC1	ICMP		0.000	N	1
	Successful	PC1	PC0	ICMP		0.000	N	2
	Successful	PC2	PC3	ICMP		0.000	N	3

EXPERIMENT-10

Aim: To Configure IP Static Routing using three routers, three switches and 6 PC in CISCO Packet Tracer

Apparatus (Software): Packet tracer Software

Theory: Static routing is a form of routing that occurs when a router uses a manually-configured routing entry, rather than information from dynamic routing traffic. In many cases, static routes are manually configured by a network administrator by adding in entries into a routing table, though this may not always be the case. Unlike dynamic routing, static routes are fixed and do not change if the network is changed or reconfigured. Static routing and dynamic routing are not mutually exclusive. Both dynamic routing and static routing are usually used on a router to maximise routing efficiency and to provide backups in case dynamic routing information fails to be exchanged. Static routing can also be used in stub networks, or to provide a gateway of last resort.

Static routing may have the following uses:

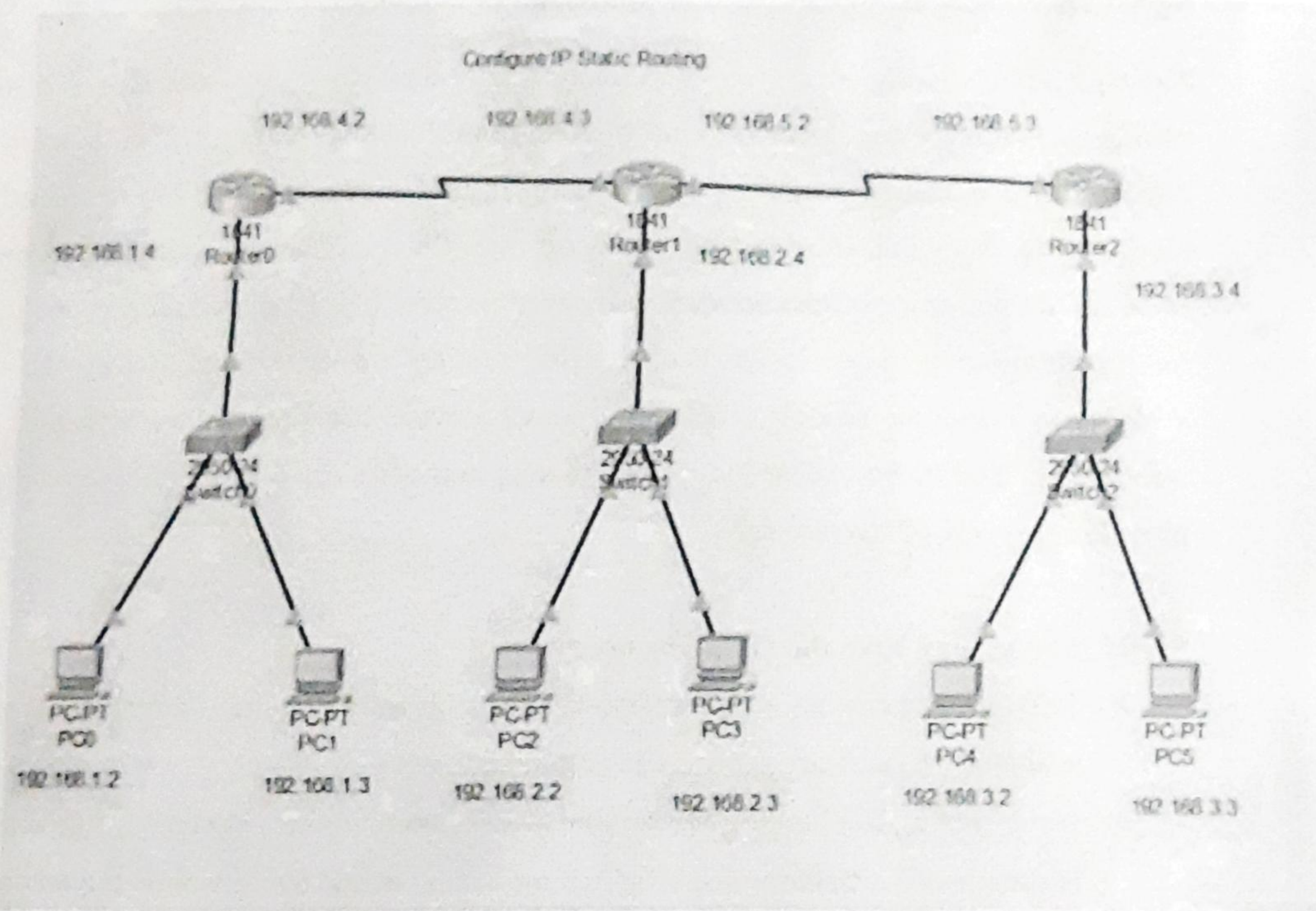
- Static routing can be used to define an exit point from a router when no other routes are available or necessary. This is called a default route.
- Static routing can be used for small networks that require only one or two routes. This is often more efficient since a link is not being wasted by exchanging dynamic routing information.
- Static routing is often used as a complement to dynamic routing to provide a failsafe backup if a dynamic route is unavailable.
- Static routing is often used to help transfer routing information from one routing protocol to another (routing redistribution).

Static routing, if used without dynamic routing, has the following advantages:

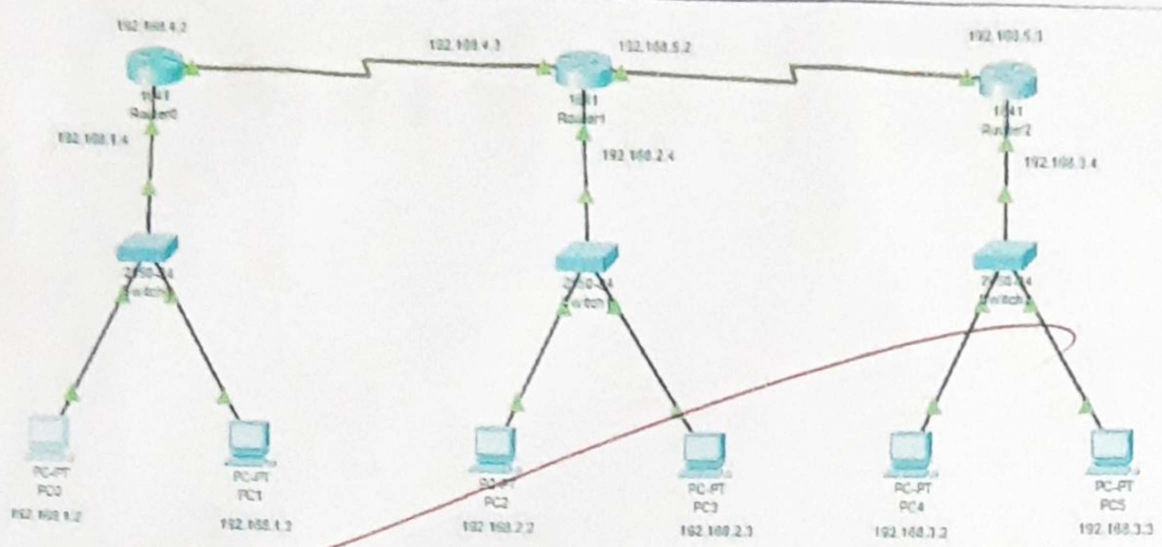
- Static routing causes very little load on the CPU of the router, and produces no traffic to other routers.
- Static routing leaves the network administrator with full control over the routing behavior of the network.
- Static Routing is very easy to configure on small networks.

Procedure:

Step 1



OBSERVATION: -



PC0:

```
C:\>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.2.2: bytes=32 time=7ms TTL=126
Reply from 192.168.2.2: bytes=32 time=1ms TTL=126
Reply from 192.168.2.2: bytes=32 time=8ms TTL=126
Reply from 192.168.2.2: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 8ms, Average = 4ms
```

PC1:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

PC2:

```
C:\>ping 192.168.3.2

Pinging 192.168.3.2 with 32 bytes of data:

Reply from 192.168.3.2: bytes=32 time=2ms TTL=126
Reply from 192.168.3.2: bytes=32 time=1ms TTL=126
Reply from 192.168.3.2: bytes=32 time=1ms TTL=126
Reply from 192.168.3.2: bytes=32 time=6ms TTL=126

Ping statistics for 192.168.3.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 6ms, Average = 2ms
```

PC3:

```
C:\>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.2.2: bytes=32 time<1ms TTL=128
Reply from 192.168.2.2: bytes=32 time<1ms TTL=128
Reply from 192.168.2.2: bytes=32 time<1ms TTL=128
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128

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

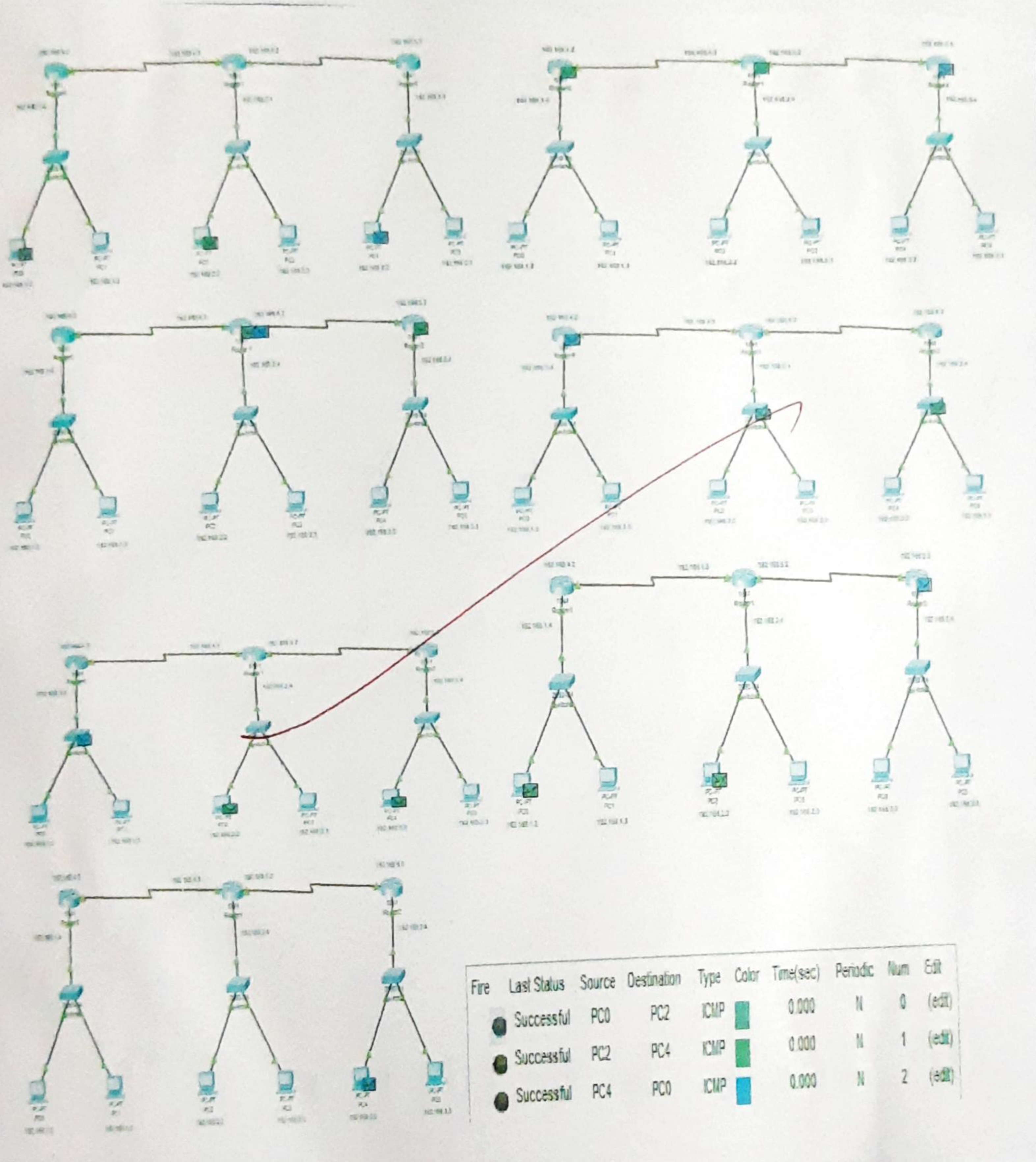
PC4:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=2ms TTL=125
Reply from 192.168.1.2: bytes=32 time=2ms TTL=125
Reply from 192.168.1.2: bytes=32 time=2ms TTL=125
Reply from 192.168.1.2: bytes=32 time=2ms TTL=125

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 2ms, Average = 2ms
```

PC5:

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.3.2

Pinging 192.168.3.2 with 32 bytes of data:

Reply from 192.168.3.2: bytes=32 time<1ms TTL=128
Reply from 192.168.3.2: bytes=32 time<1ms TTL=128
Reply from 192.168.3.2: bytes=32 time<1ms TTL=128
Reply from 192.168.3.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.3.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

RESULT:



Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Successful	PC0	PC2	ICMP		0.000	N	0	(edit)
	Successful	PC2	PC4	ICMP		0.000	N	1	(edit)
	Successful	PC4	PC0	ICMP		0.000	N	2	(edit)