Computer Networks (CS303)

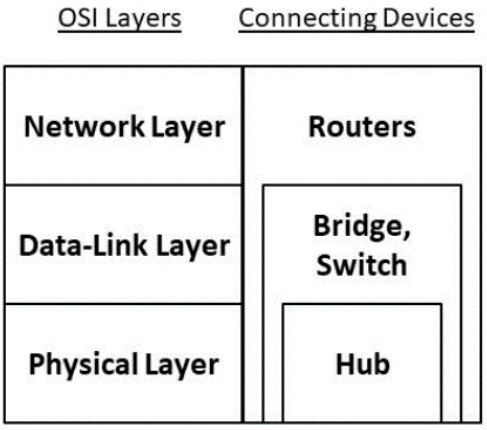
Assignment - 5

U19CS012

1. Create Manual for create different network topologies using Hub, Repeater, Switch and Router.

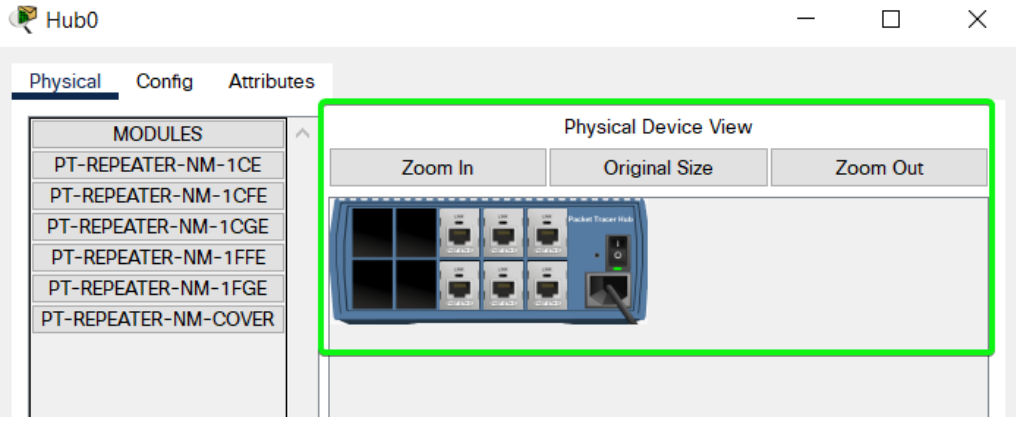
Routers, Hubs, Switches, and Bridges are all network connecting devices. **A network connecting device is a device that connects two or more devices together that are present in the same or different networks.**

All these connecting devices operate in some specific layers of the O.S.I. (Open System Interconnection) Model. These specifications are provided in the diagram below.



Connecting devices

1. Hub

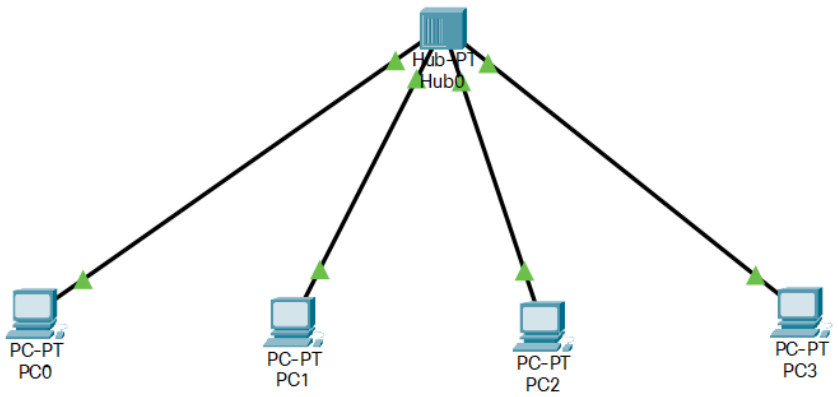


Hub is a very simple network connecting device.

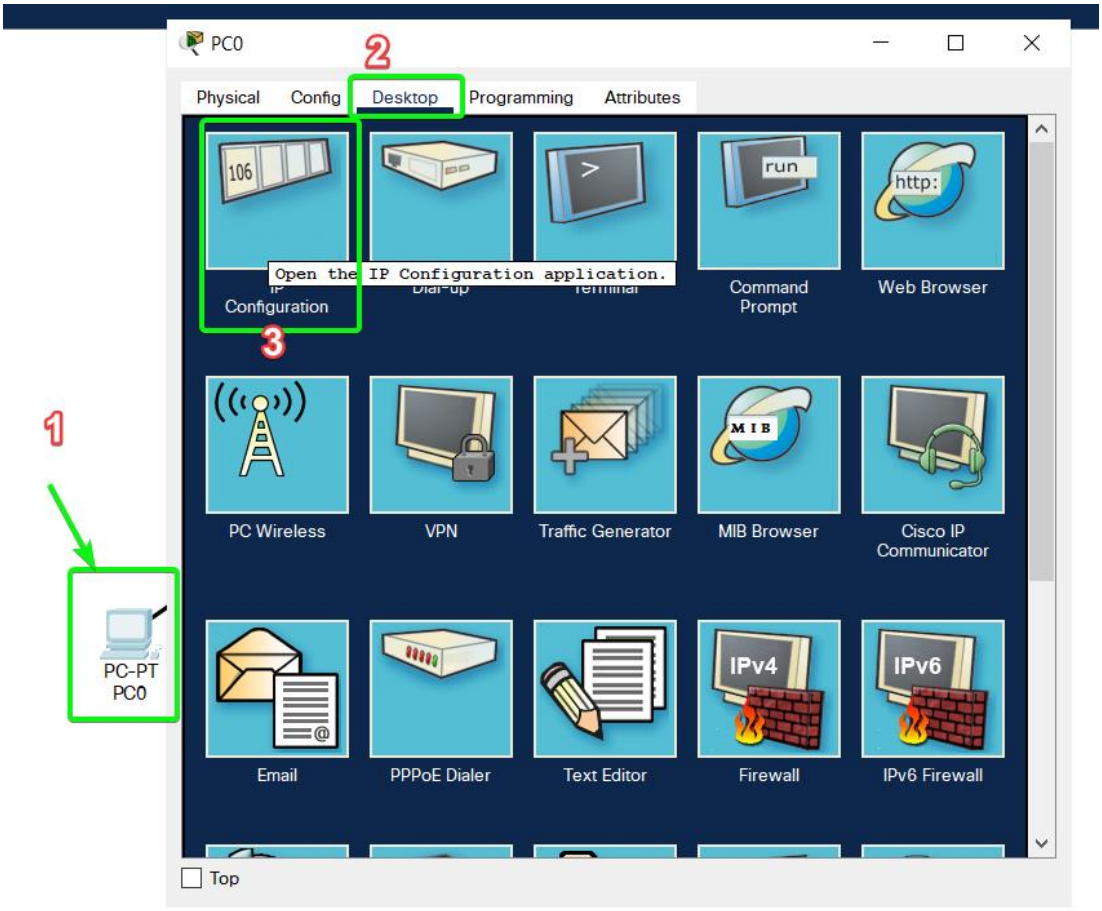
In Star/hierarchical topology, a Repeater is called Hub. It is also known as a **Multiport Repeater Device**.

A Hub is a **layer-1** device and operates **only in the physical network** of the OSI Model. Since it works in the **physical layer**, it mainly deals with the data in the form of bits or electrical signals. A Hub is mainly used to create a network and connect devices on the same network only.

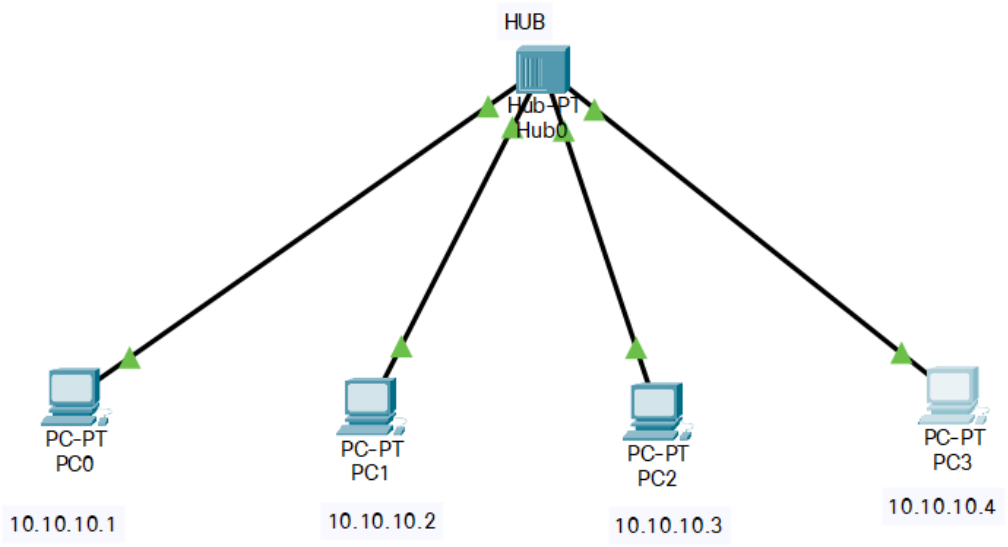
STEP 1: Create Simple Network as Shown Below using Hub, PC and Wires.



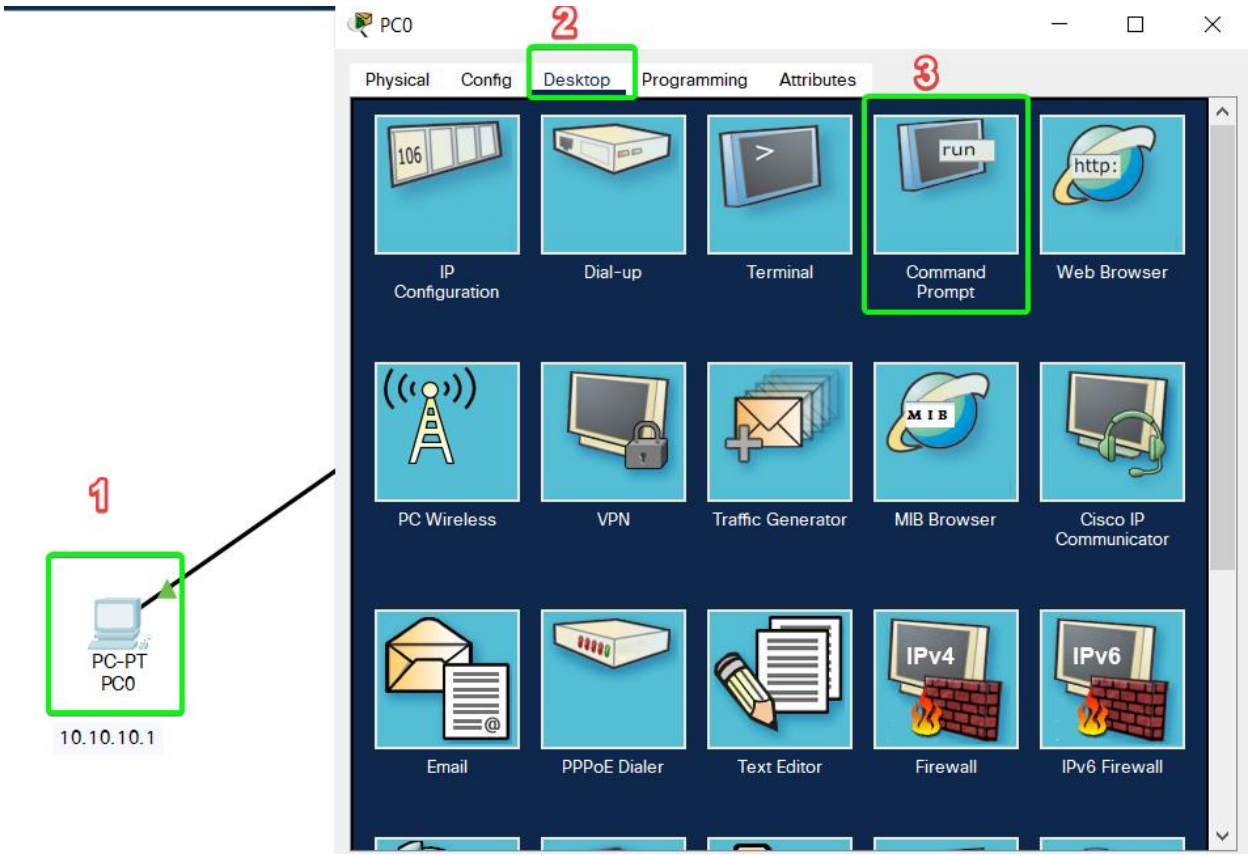
STEP 2: Assigning the IP Addresses to Each PC

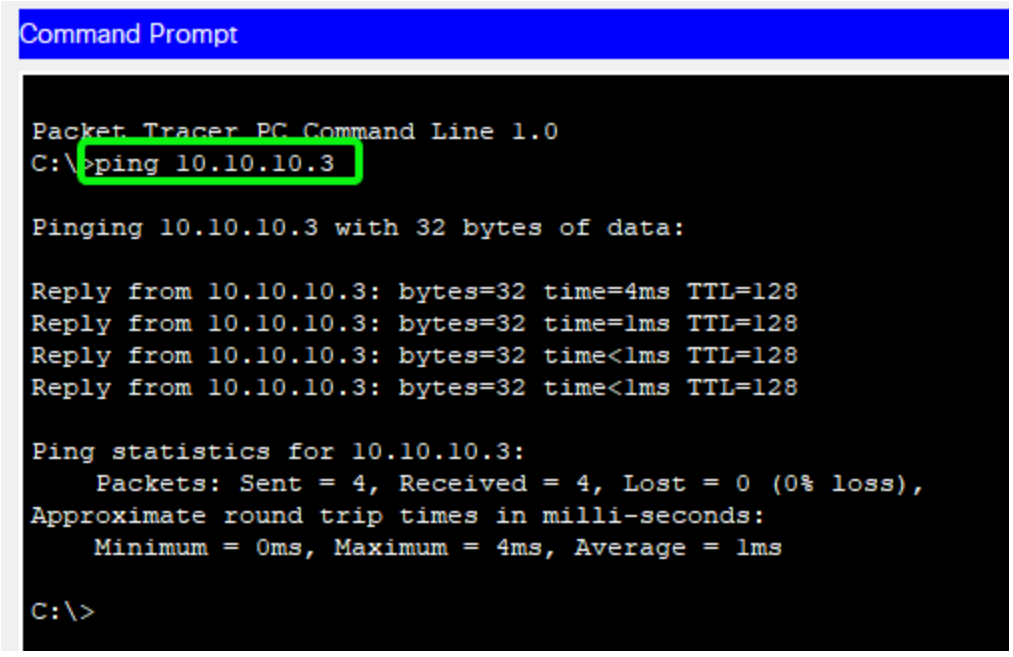


STEP 3: Label Each PC with its IP Address



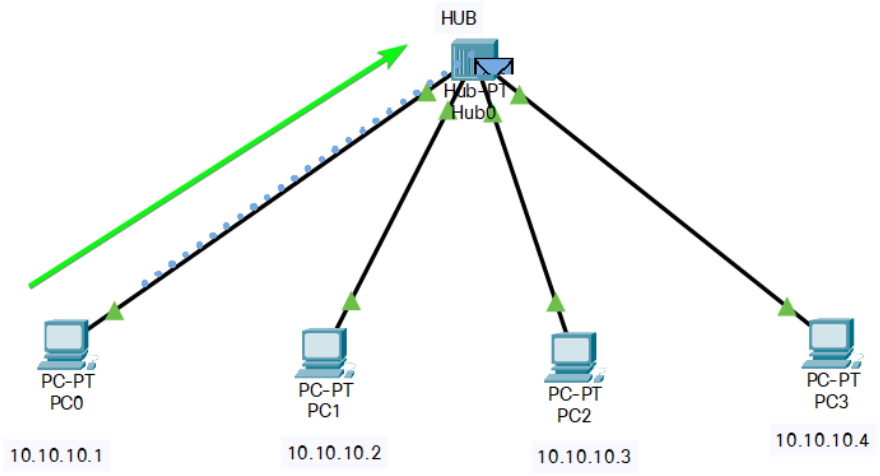
STEP 4: Write Ping Command from PC0 to PC2



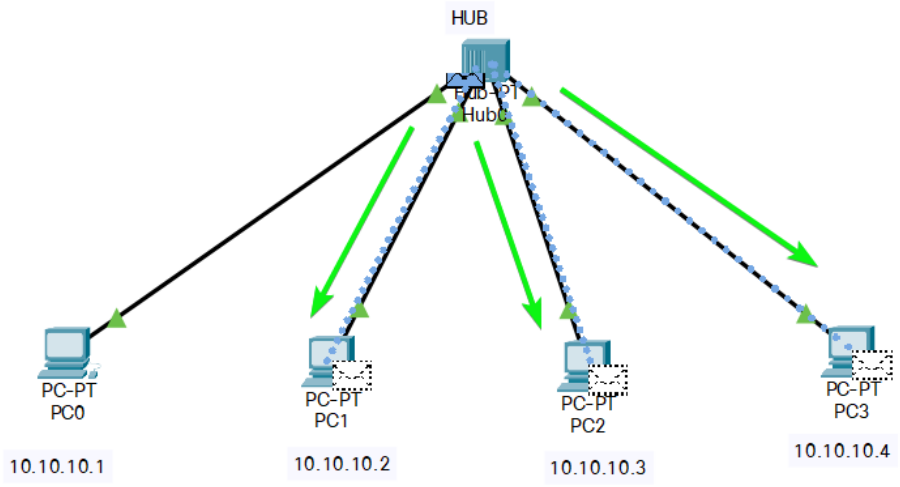


STEP 5: Simulation

1.) Packet is First Transmitted to HUB.

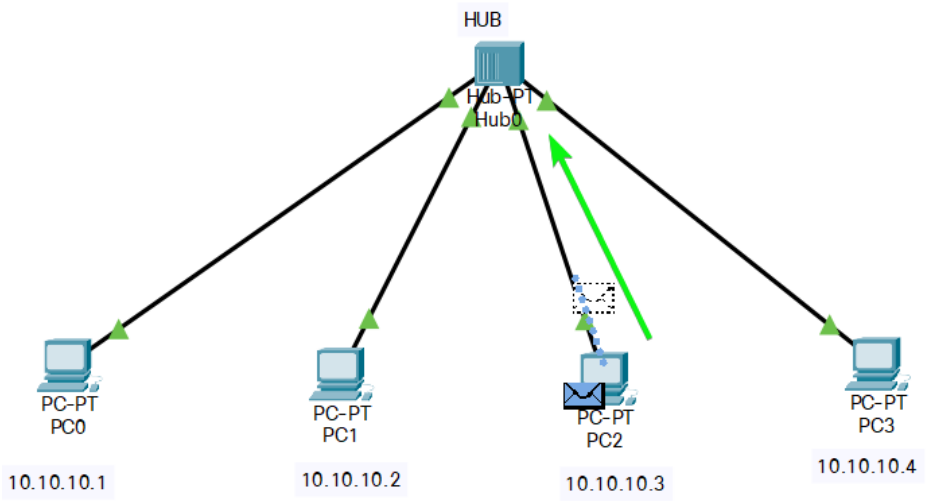


2.) Then Packet is broadcasted to all the Three Devices.

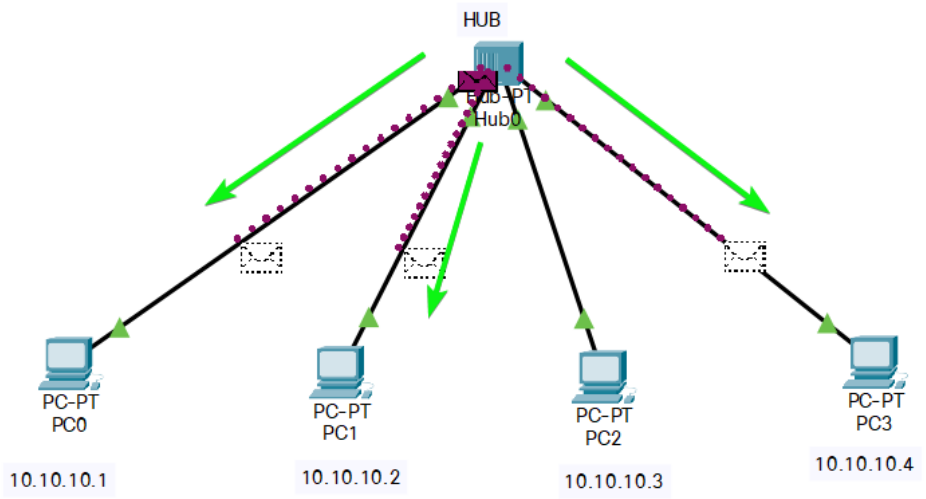


Packet at PC1 & PC3 Rejected. [Since they are Not Destination Address]

3.) Packet then went back from Destination Device [Reply].



4.) The Reply is broadcasted to all the Connected Devices.



The Reply Packet is rejected at PC1 and PC3.

A Hub is *not an intelligent device*, it forwards the incoming messages to other devices without checking for any errors or processing it. It does not maintain any address table for connected devices. It only knows that a device is connected to one of its ports. Hub **works Only in Same Network.**

When a data packet arrives at one of the ports of a Hub, it simply copies the data to every port. In other words, a hub **broadcasts** the incoming data packets in the network. Due to this, there are various security issues in the hub. Broadcasting also leads to **unnecessary data traffic** on the channel.

A Hub uses a **half-duplex** mode of communication. It shares the bandwidth of its channel with the connecting devices. It has only one collision domain, so there are more chances of collision and traffic on the channel. A hub is connected in limited network size. If the network size is increased, the speed of the network will slow down.

There are mainly two types of Hub, they are:

1. **Active Hub:** An Active hub is also known as **Concentrator**. It requires a power supply and can work as a repeater. Thus, it can analyze the data packets and can amplify the transmission signals, if needed.
2. **Passive Hub:** A passive hub does not need any power supply to operate. It only provides communication between the networking devices and does not amplify the transmission signals. In other words, it just forwards the data as it is.

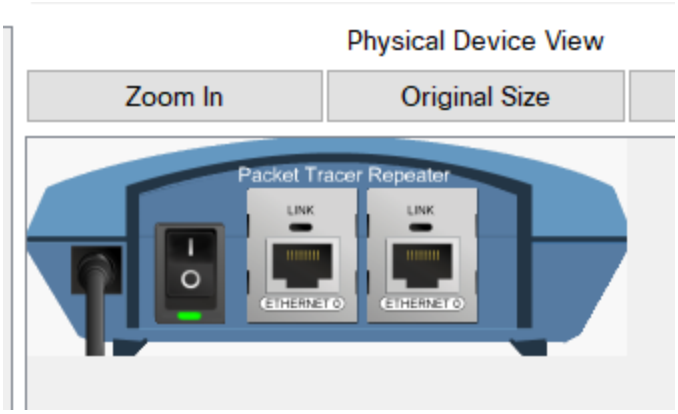
Advantages of a Hub:

1. It is **simple** to implement.
2. The implementation **cost** is **low**.
3. It does not require any special system administration configuration. We can just plug and play it.

Disadvantages of a Hub:

1. It can connect devices of the **same network** only.
2. It uses a **half-duplex** mode of communication.
3. It is **less secure**, as it broadcasts the data packets.
4. It can be used in a **limited network size** only.
5. Broadcasting induces **unnecessary traffic** on the channel.

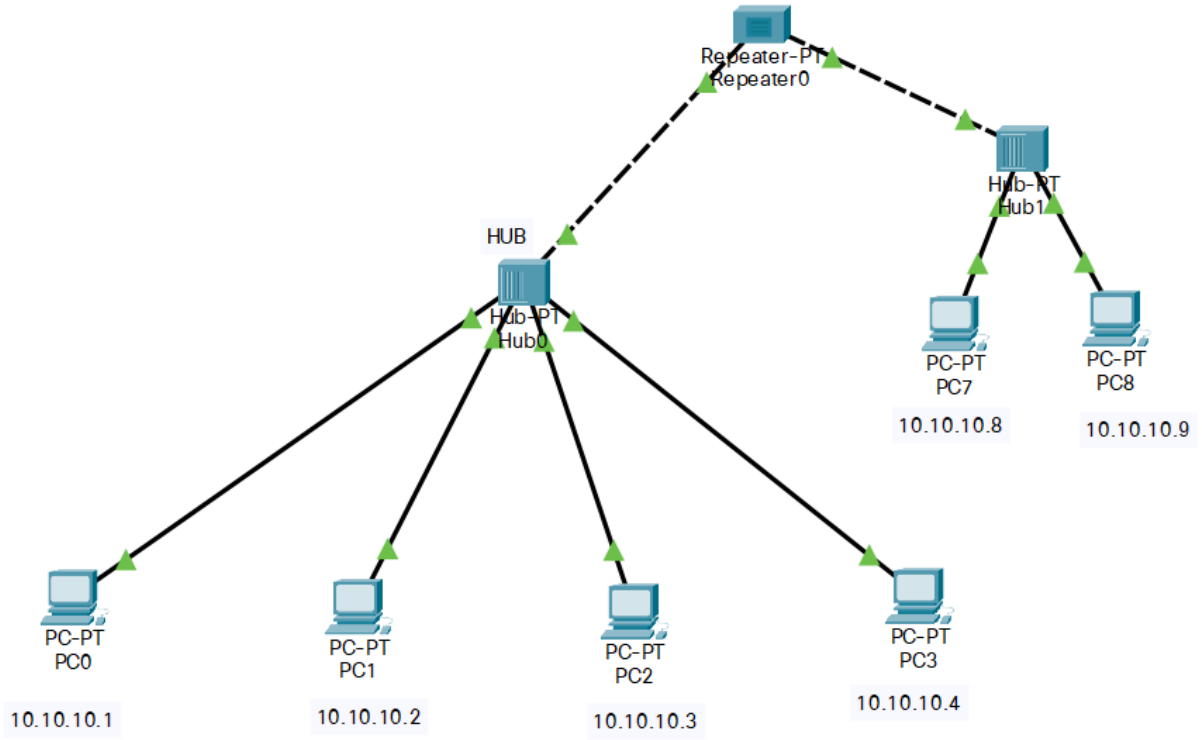
2. **Repeater** – A repeater operates at the physical layer.



Its job is to <u>regenerate the signal</u> over the same network before the signal becomes **too weak or corrupted** so as to **extend the length** to which the signal can be transmitted over the same network.

An important point to be noted about repeaters is that they **do not amplify the signal**. When the signal becomes weak, they copy the signal bit by bit and regenerate it at the original strength. It is a 2 port device.

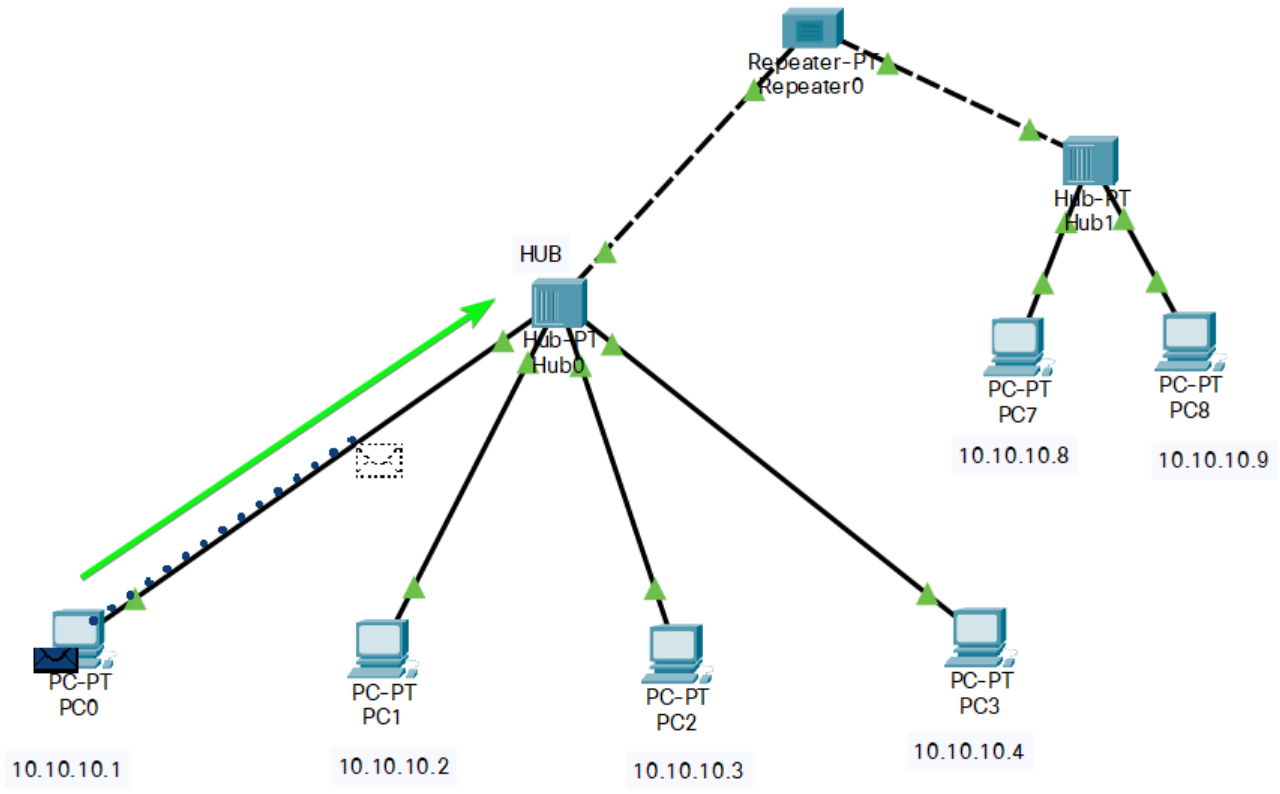
<u>STEP 1</u>: Create the Below Show Network

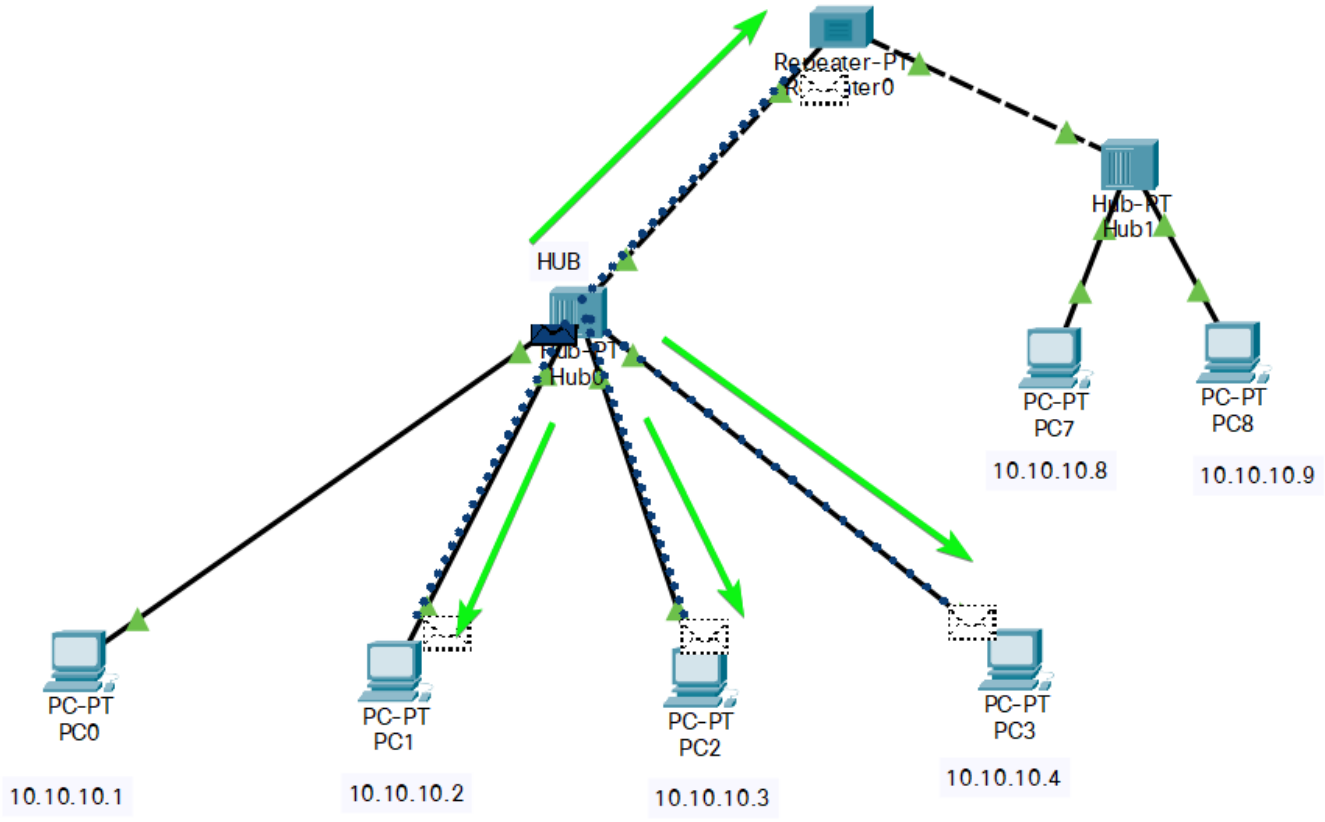


STEP 2: Ping from PC0 to PC8

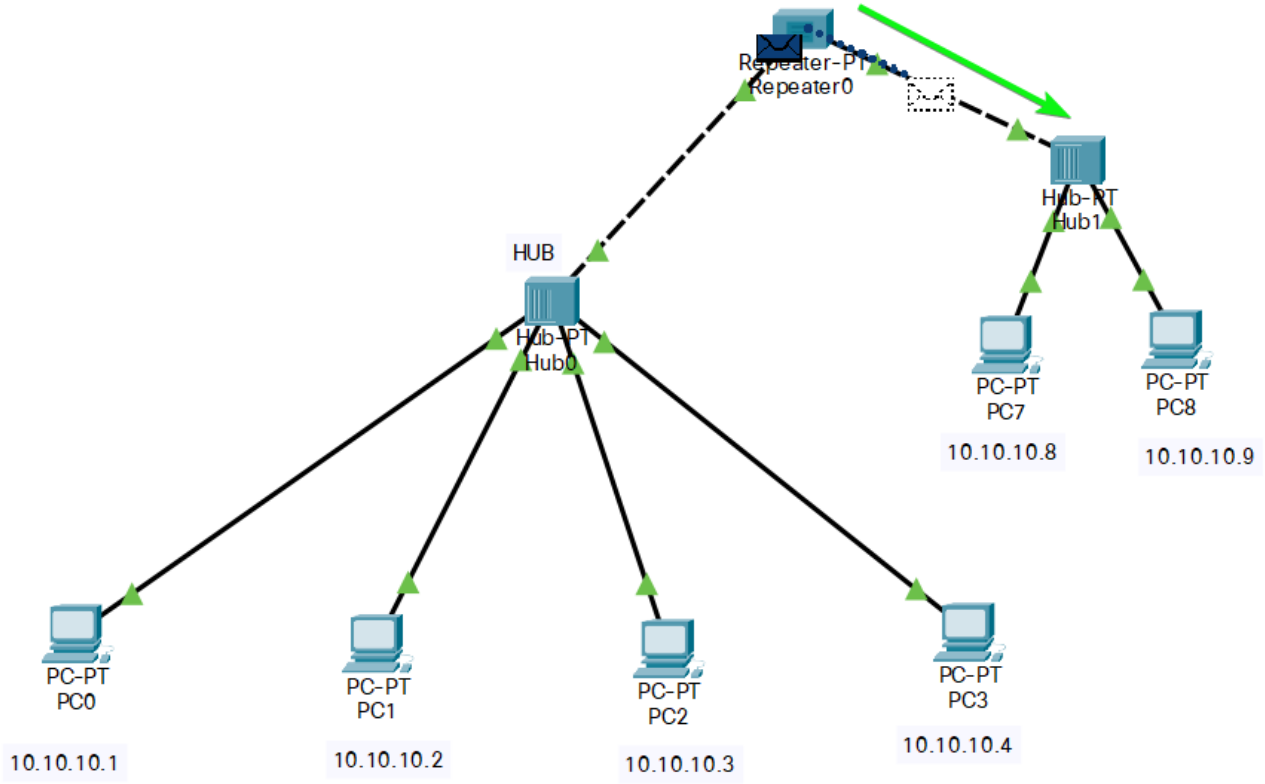
```
C:\>ping 10.10.10.9

Pinging 10.10.10.9 with 32 bytes of data:

Reply from 10.10.10.9: bytes=32 time=23ms TTL=128
Reply from 10.10.10.9: bytes=32 time=14ms TTL=128
Reply from 10.10.10.9: bytes=32 time=11ms TTL=128
Reply from 10.10.10.9: bytes=32 time=10ms TTL=128

Ping statistics for 10.10.10.9:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 23ms, Average = 14ms
```

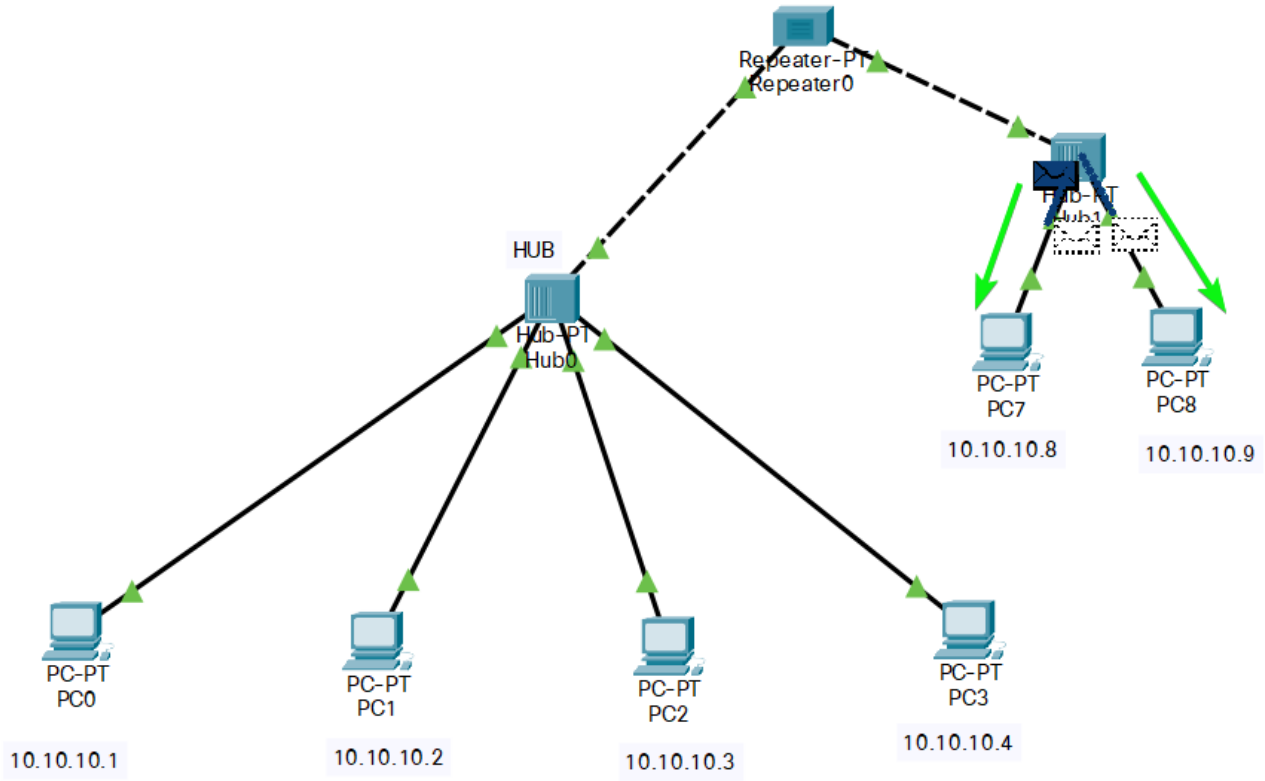
STEP 3: Simulation



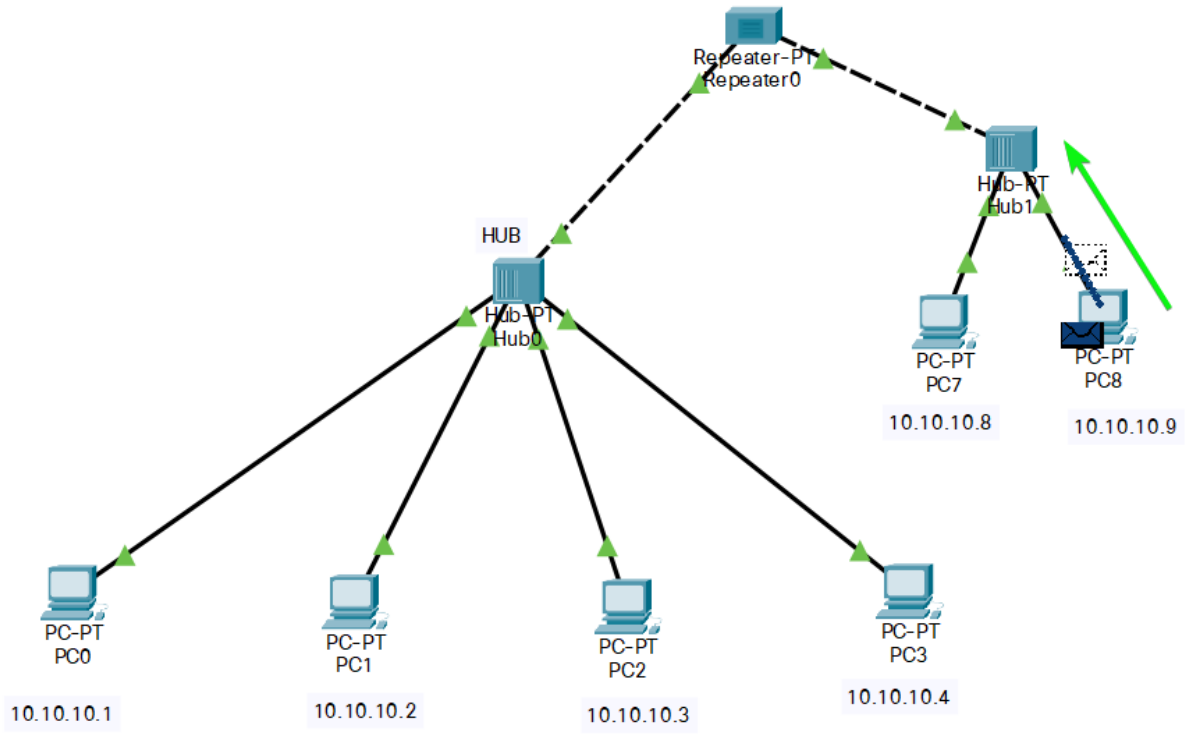


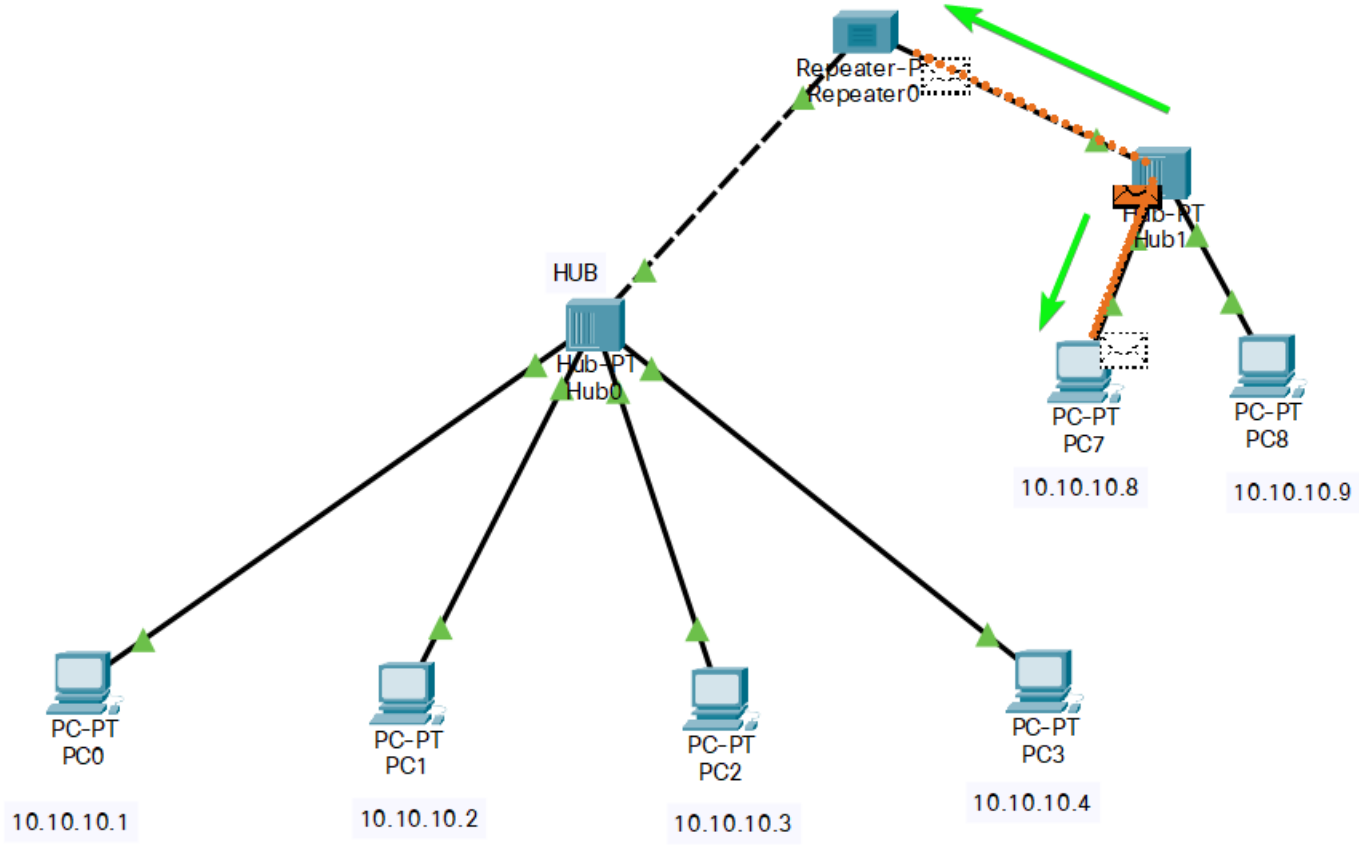
Packets at PC1, PC2 & PC3 are rejected.

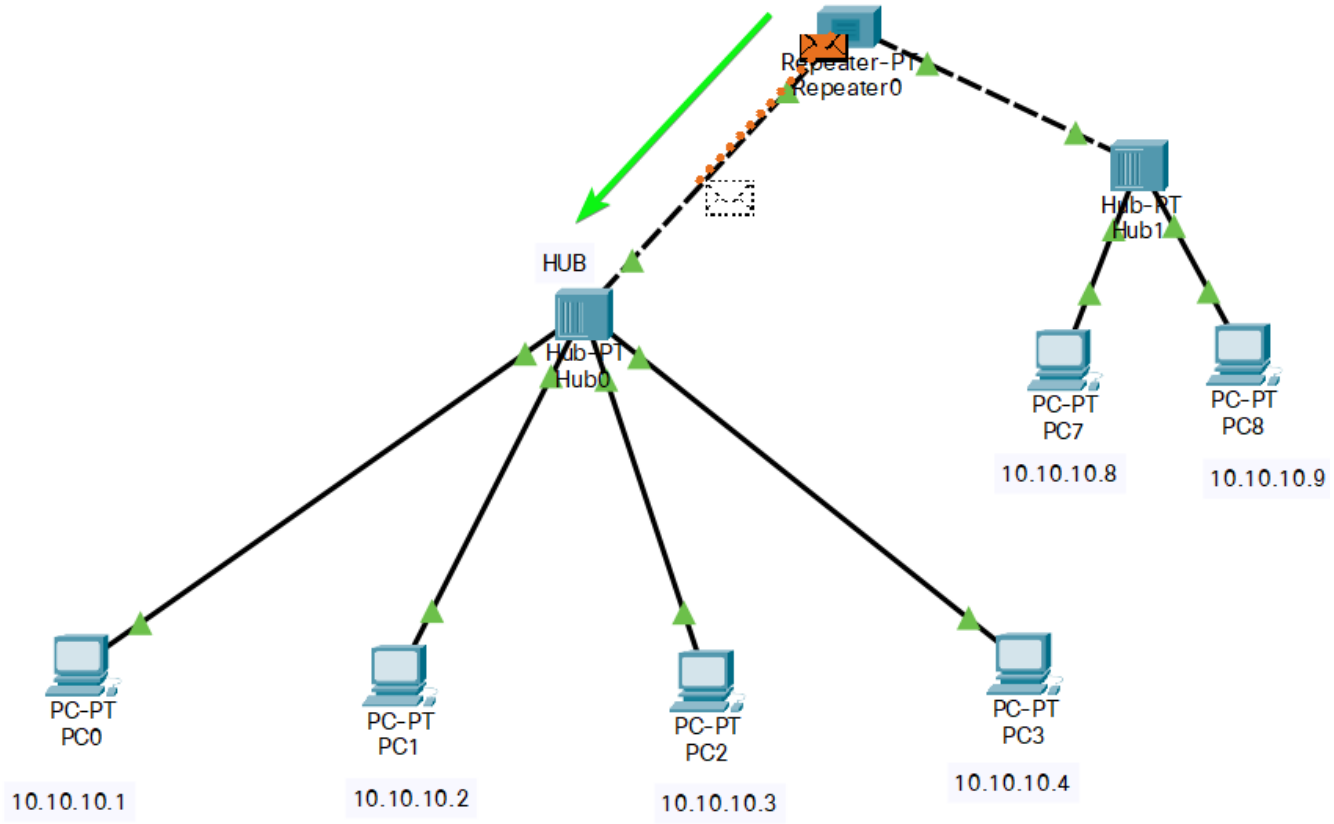


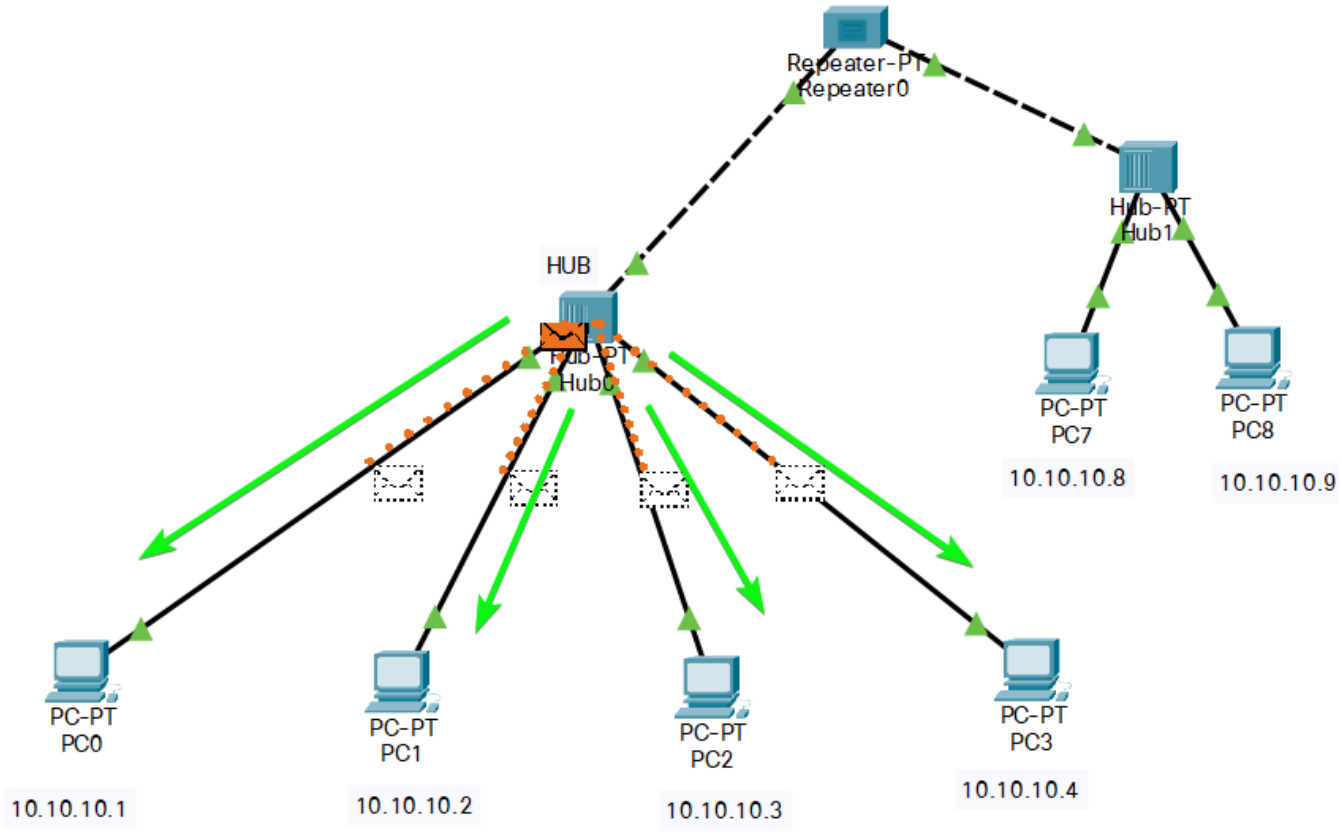


Packet at PC7 discarded.




Repeater-PT
Repeater0
Hub-PT
Hub1
HUB
Hub-PT
Hub0
PC-PT
PC7
PC-PT
PC8
10.10.10.8
10.10.10.9
PC-PT
PC0
PC-PT
PC1
PC-PT
PC2
PC-PT
PC3
10.10.10.1
10.10.10.2
10.10.10.3
10.10.10.4


Repeater-PT
Repeater0
Hub-PT
Hub1
HUB
Hub-PT
Hub0
PC-PT
PC7
PC-PT
PC8
10.10.10.8
10.10.10.9
PC-PT
PC0
PC-PT
PC1
PC-PT
PC2
PC-PT
PC3
10.10.10.1
10.10.10.2
10.10.10.3
10.10.10.4

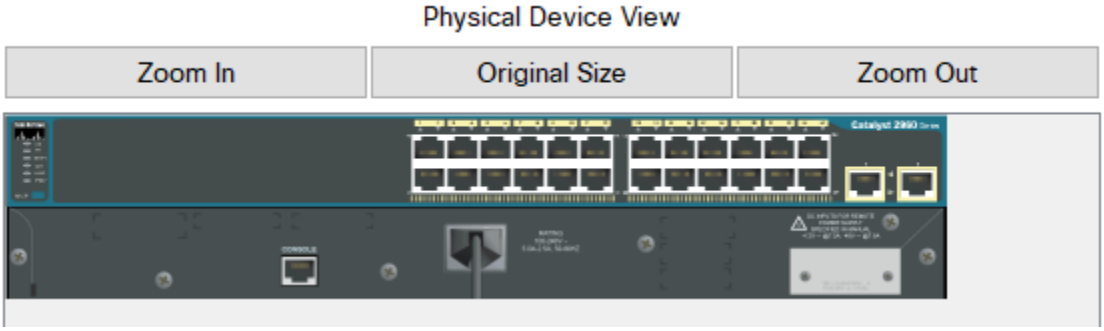


Reply Packet Received by PC0 Successfully and Discarded by PC1, PC2 & PC3.

3. Switch

A switch is a **layer-2 [Layer 3 Switch also]** network connecting device, i.e., it works on the physical and data-link layer of the OSI model.

It interprets data in the form of **data frames**. A switch acts as a multiport bridge in the network. It provides the bridging functionality with greater efficiency. [Note : Bridge is a Repeater with filtering capability.]

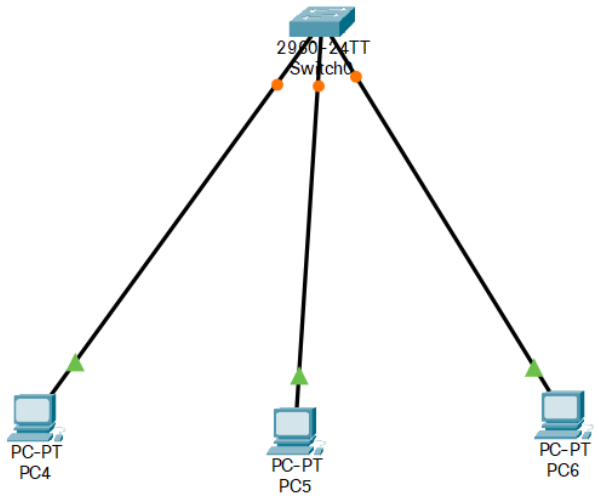


A switch maintains a Switch table which has the MAC addresses of all the devices connected to it. It is preferred more over the hub, as it reduces any kind of unnecessary traffic in the transmission channel.

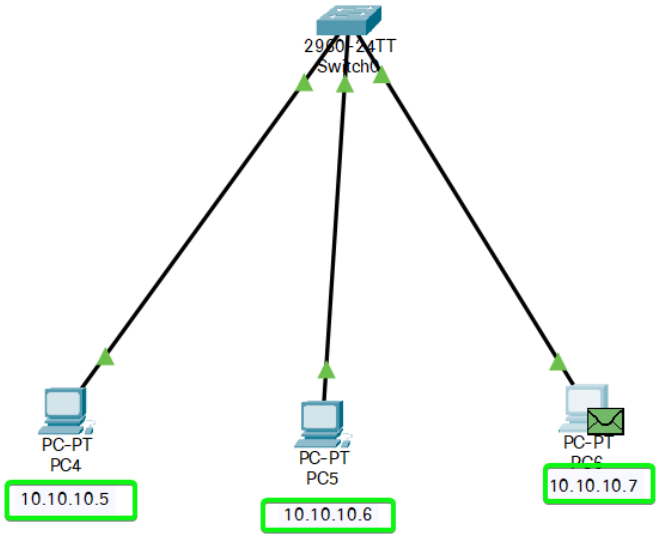
A switch can connect the devices only in the same network. It uses the **full-duplex** mode of communication and saves bandwidth. The switch table **keeps on updating every few seconds** for better processing.

A Switch is an **intelligent device with filtering capabilities**. It can discard the faulty data frames and will allow only the errorless data frames in the network. Also, it will forward the data frames to the specific node based on the MAC address (taken from the Switch table).

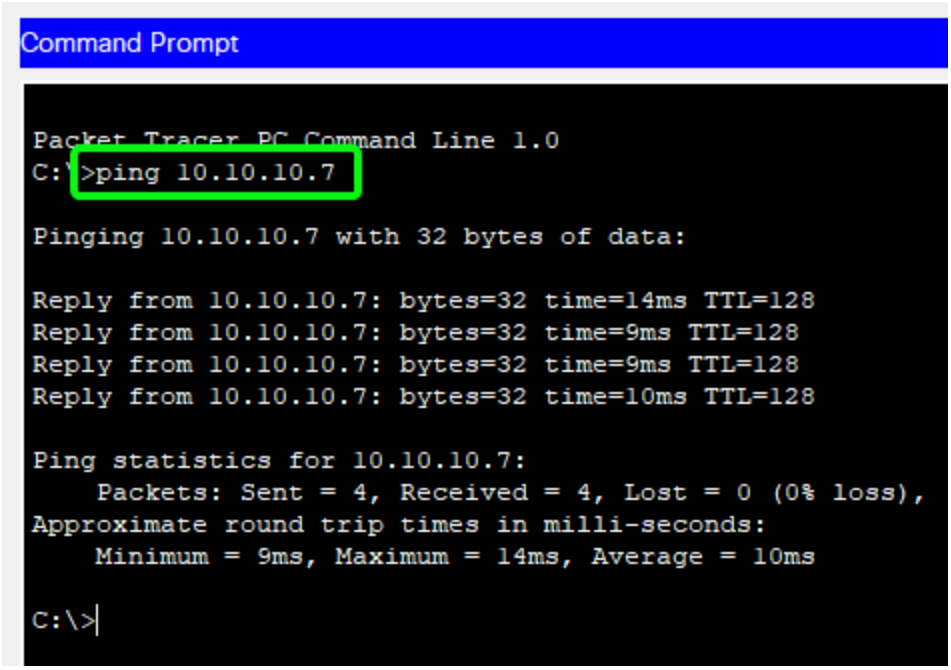
STEP 1: Create Simple Network as Shown Below using Switch {2960} , PC and Wires.



STEP 2: Assigning the IP Addresses to Each PC & Label them

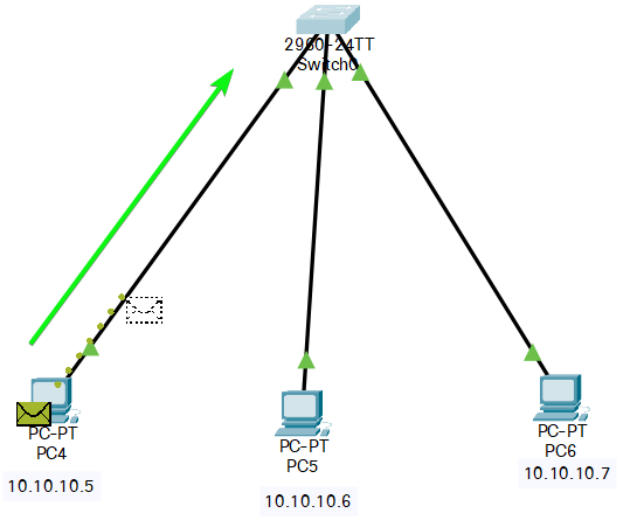


STEP 3: Write Ping Command from PC4 to PC6



STEP 4: Simulation

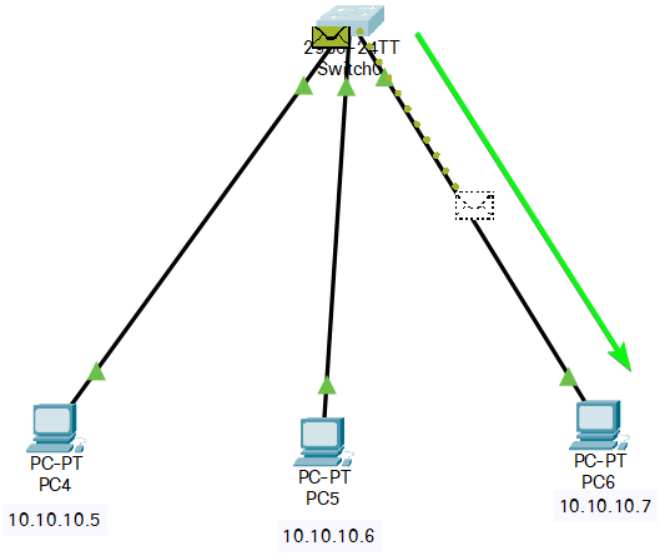
1.) Data Frame is sent to Switch.



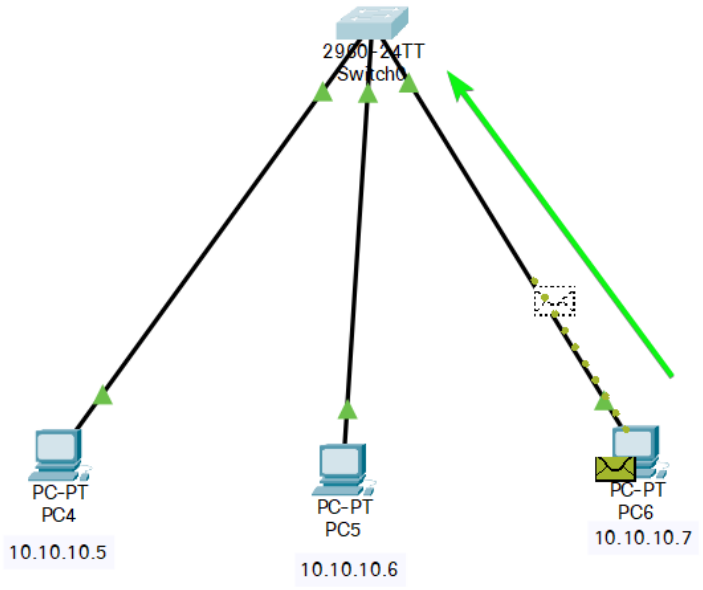
2.) When a data frame arrives at the Switch, it first **checks** for any kind of error in the data frame. If the frame is **error-free**, it will **search the MAC address** of the destination in the Switch table.

If the address is available in the switch table, it will forward the data frame to that specific node, else switch will register the MAC address in the switch table.

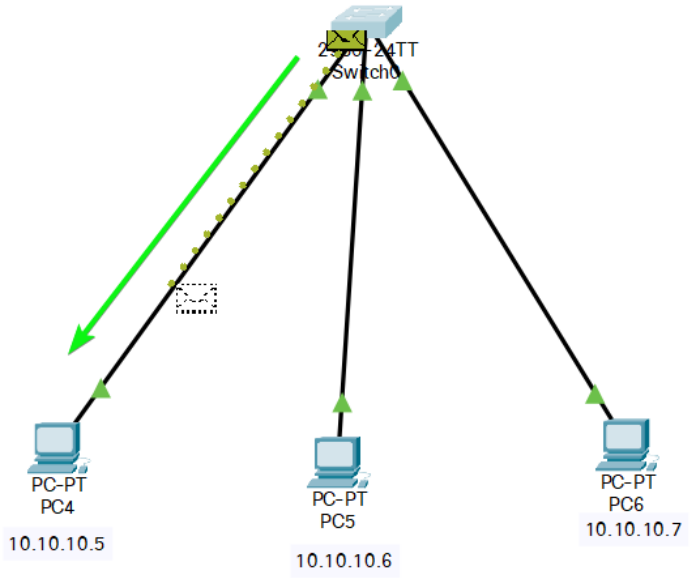
If the destination address is not specified, it will broadcast the data frame to each node in the network.



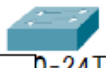
3.) Reply Sent from Destination PC to Switch



4.) Reply from Switch Reaches the Original Sender



A Switch can have 8/6/**24**/48 ports. The data transmission speed is slow in a switch (around 10-100 Mbps). Also, it has only one broadcasting domain.



0-24TT
itch0

```
Device Name: Switch0
Custom Device Model: 2960 IOS15
Hostname: Switch
```

Port	Link	VLAN	IP Address	MAC Address
FastEthernet0/1	Down	1	--	000A.416A.C001
FastEthernet0/2	Down	1	--	000A.416A.C002
FastEthernet0/3	Down	1	--	000A.416A.C003
FastEthernet0/4	Down	1	--	000A.416A.C004
FastEthernet0/5	Down	1	--	000A.416A.C005
FastEthernet0/6	Down	1	--	000A.416A.C006
FastEthernet0/7	Down	1	--	000A.416A.C007
FastEthernet0/8	Down	1	--	000A.416A.C008
FastEthernet0/9	Down	1	--	000A.416A.C009
FastEthernet0/10	Down	1	--	000A.416A.C00A
FastEthernet0/11	Down	1	--	000A.416A.C00B
FastEthernet0/12	Down	1	--	000A.416A.C00C
FastEthernet0/13	Down	1	--	000A.416A.C00D
FastEthernet0/14	Down	1	--	000A.416A.C00E
FastEthernet0/15	Down	1	--	000A.416A.C00F
FastEthernet0/16	Down	1	--	000A.416A.C010
FastEthernet0/17	Down	1	--	000A.416A.C011
FastEthernet0/18	Down	1	--	000A.416A.C012
FastEthernet0/19	Down	1	--	000A.416A.C013
FastEthernet0/20	Down	1	--	000A.416A.C014
FastEthernet0/21	Down	1	--	000A.416A.C015
FastEthernet0/22	Down	1	--	000A.416A.C016
FastEthernet0/23	Down	1	--	000A.416A.C017
FastEthernet0/24	Down	1	--	000A.416A.C018
GigabitEthernet0/1	Down	1	--	000A.416A.C019
GigabitEthernet0/2	Down	1	--	000A.416A.C01A
Vlan1	Down	1	<not set>	0040.0B86.0098

```
Physical Location: Intercity > Home City > Corporate Office > Main Wiring Closet > Rack > Switch0
```

There are mainly four types of Switches, they are:

1. **Store and Forward Switch:** It is the most widely and commonly used switch. It does not forward the data frames unless the frames are errorless and completely received in the switch buffer. It is reliable in nature.
2. **Cut-through Switch:** Cut-through switches have no error checking. Also, it starts sending the data frame to the destination node when it starts receiving it. It is unreliable in nature.
3. **Fragment-Free Switch:** It is a combination of store and forward, and cut-through switch. It checks only the starting 64 bytes (header information) of the data frame before transmitting the frame.
4. **Adaptive Switch:** It is the most advanced kind of switch which automatically chooses any of the above three switches as per the need.

Advantages of using a Switch:

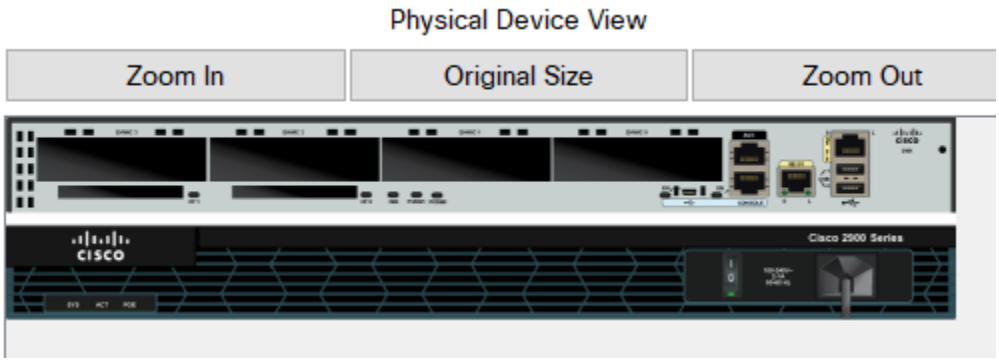
1. The implementation cost is **medium**.
2. It does not require any special system administration configuration. We can just **plug and play** it.
3. **Improves security** by limiting the scope of data frames.
4. It has the **filtering capability**.
5. It can be used in a **large** network.
6. It uses full-duplex mode of communication
7. It has multiple collision domains, so there are least or no collisions in the channel.

Disadvantages of using a Switch:

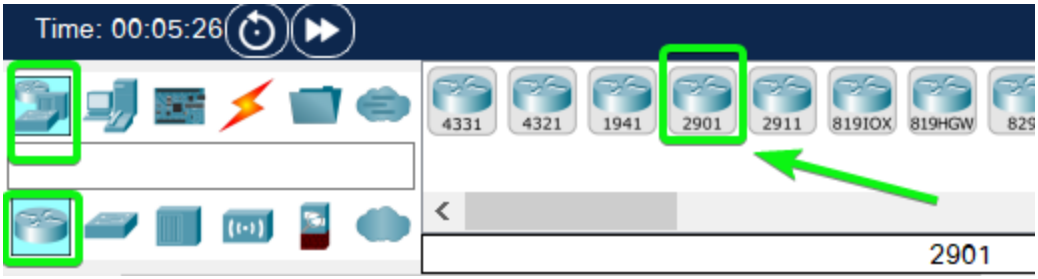
1. It can connect devices of the same network only.
2. There is a delay in forwarding the frames due to error checking.
3. There is a need to maintain a **Switch table**.

4. Router

A Router is a **layer-3** network connecting device, i.e., it works on the physical, data-link and network layer of the OSI model. It interprets data in the form of **data packets**. It can connect **two physically and logically different network** devices with each other. A Router is used to connect the networks or it routes traffic between the networks. **In other words, Router is the Gateway of a network**.

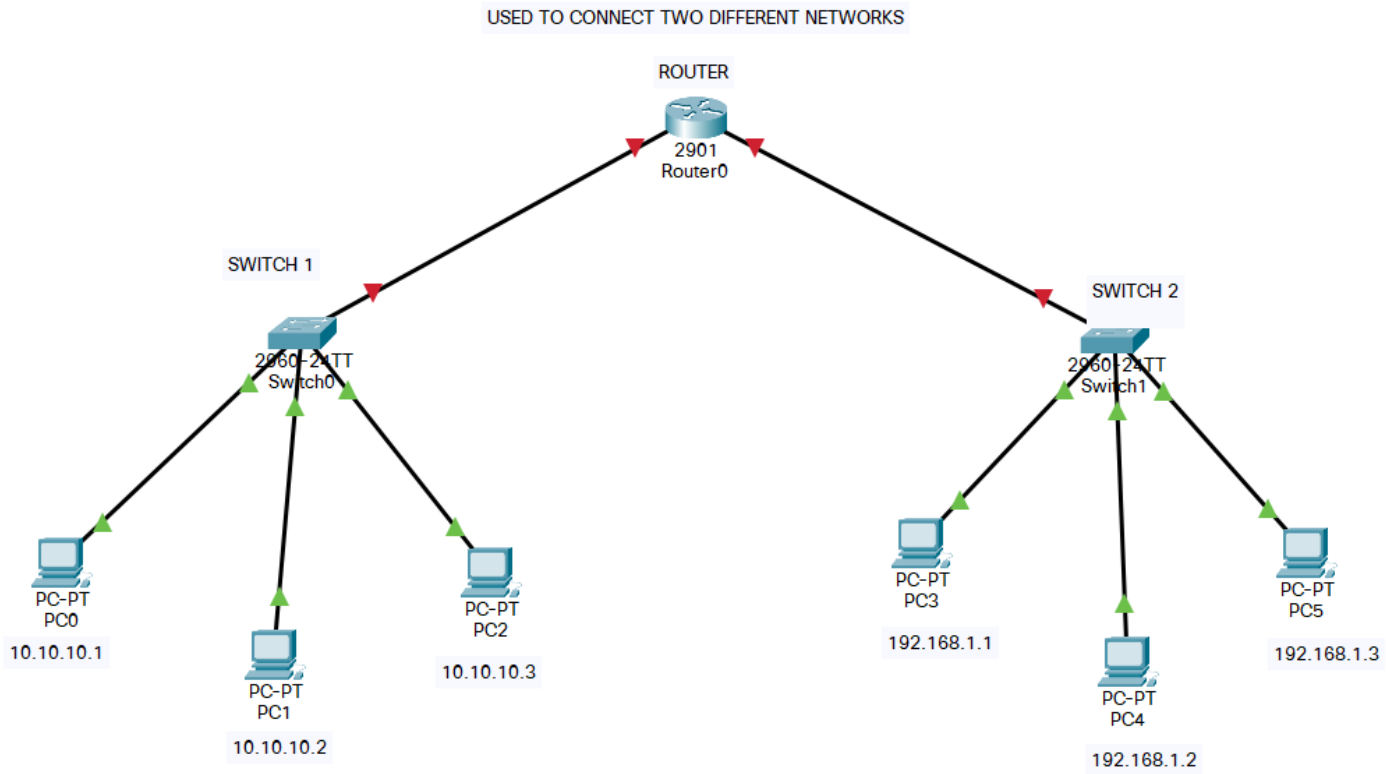


Since, connecting two devices of **different networks**, the connecting device should implement an Internet Protocol (IP) address. So, the Router has a physical and Logical (Internet Protocol) address for each of its interfaces.



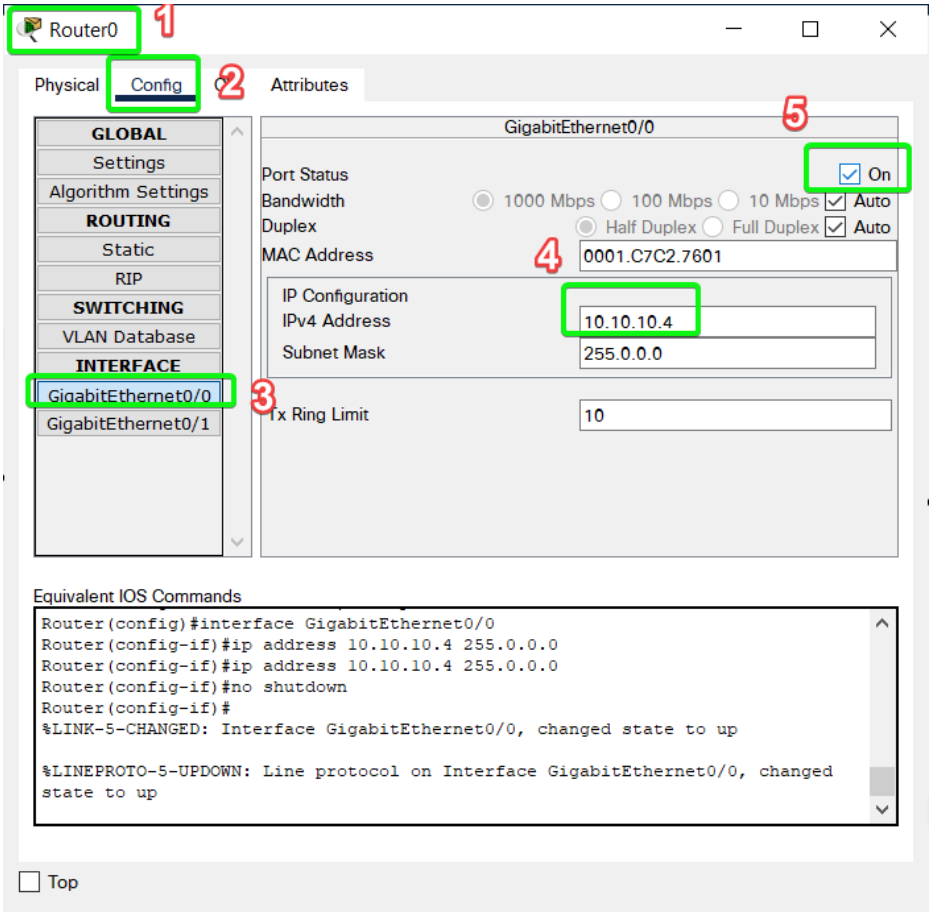
It routes or forwards the data packets from one network to another based on their **IP addresses**. It *changes the physical address* of the data packet (both source and destination) when it forwards the data packets.

STEP 1: Create Simple Network as Shown Below

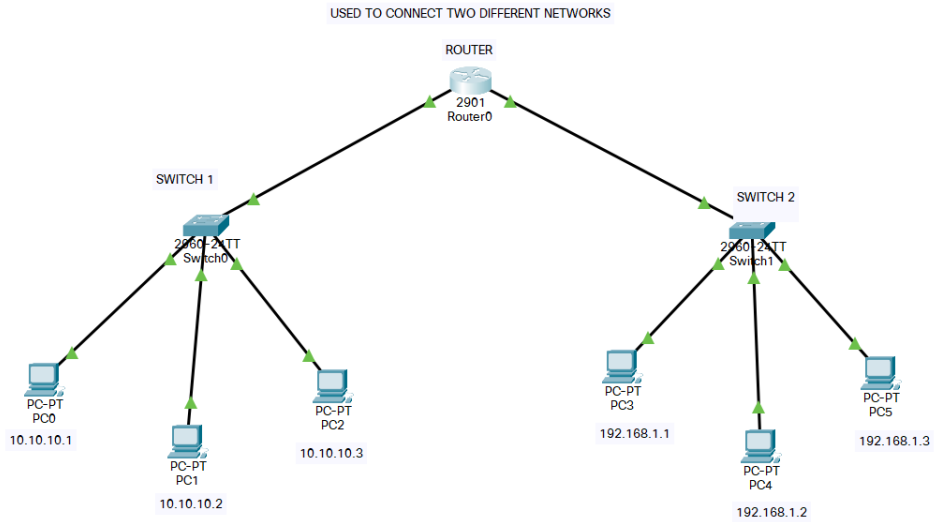


STEP 2: Configure all the PC and Label them as Shown Above

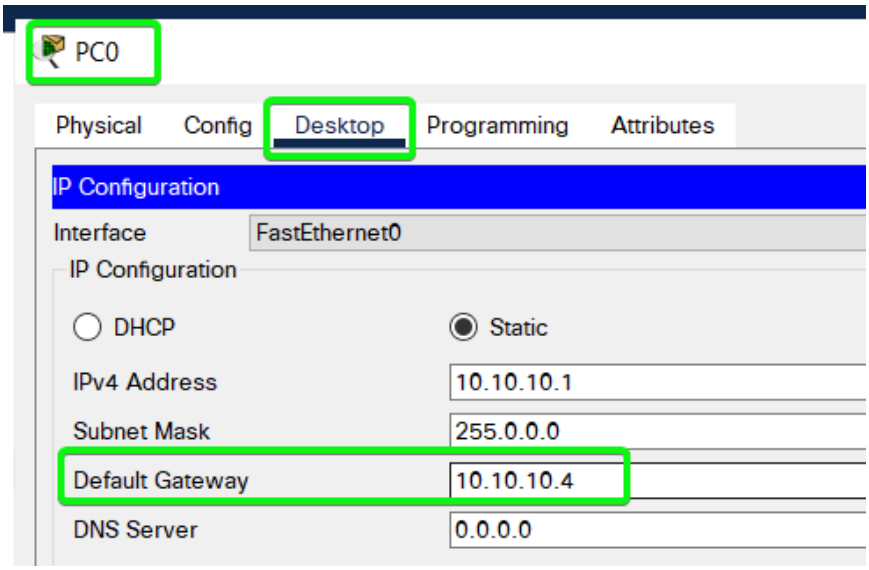
STEP 3: Activate the Router



Similarly, do it for 192.168.1.4 for Right Hand Side Network.[Router Connected]

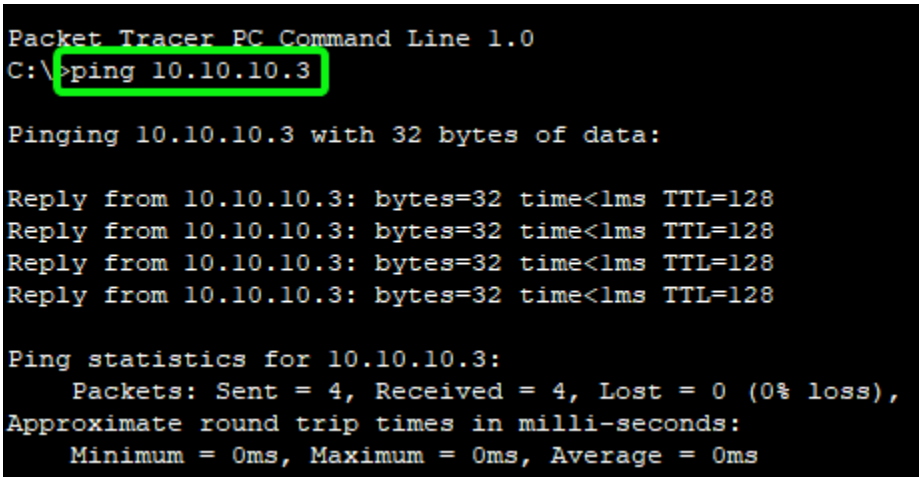


STEP 4: Configure all the PC to have Default Gateway of IP Address of Port of Router

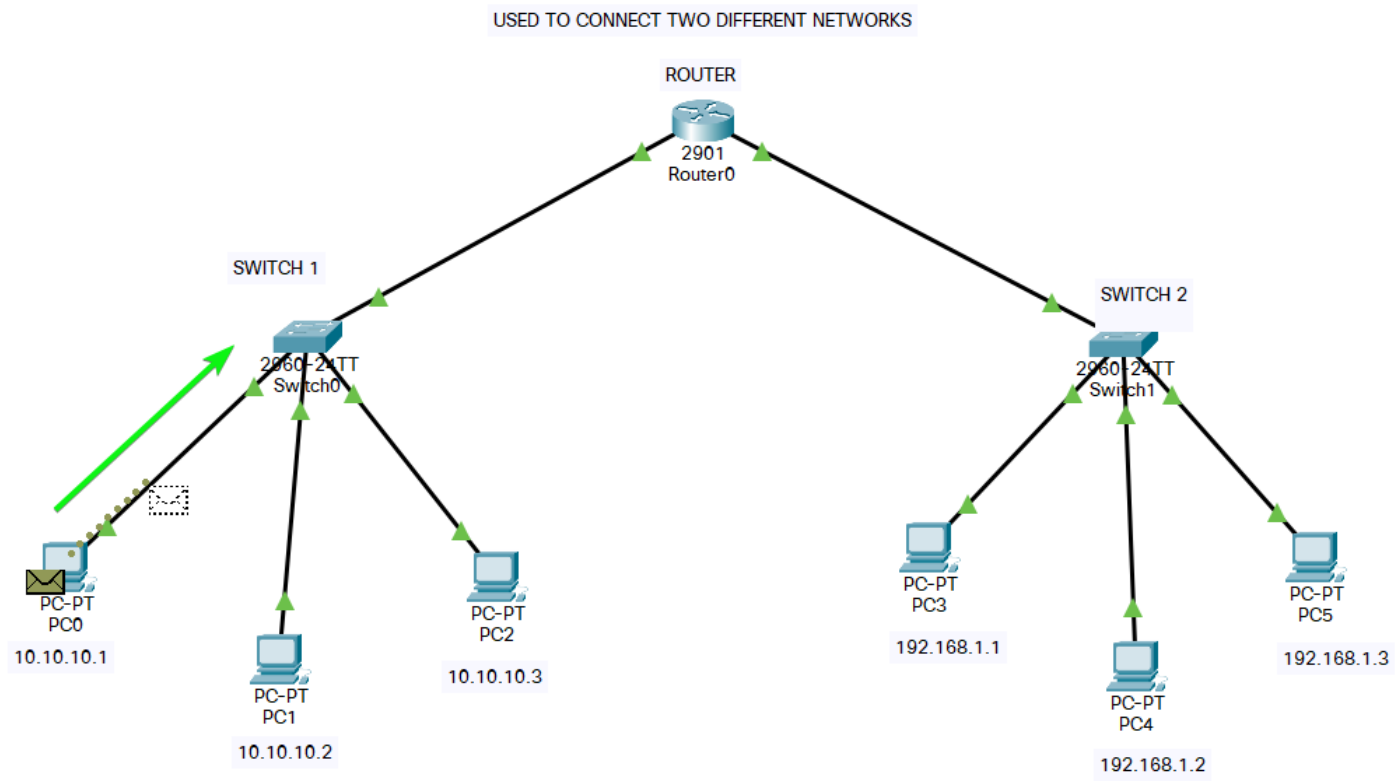


STEP 5: Simulation

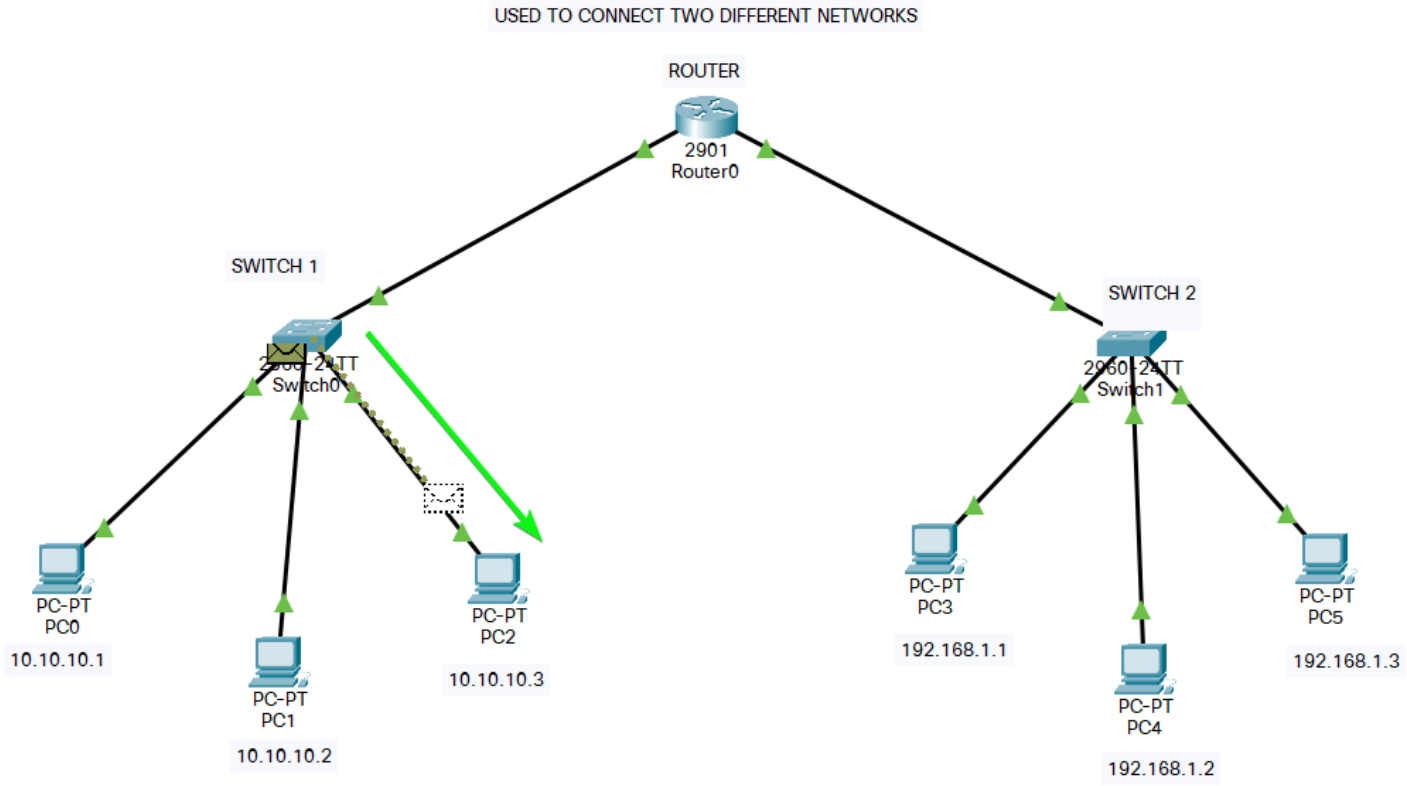
(A) INTRA NETWORK [Ping from PC0 to PC2]



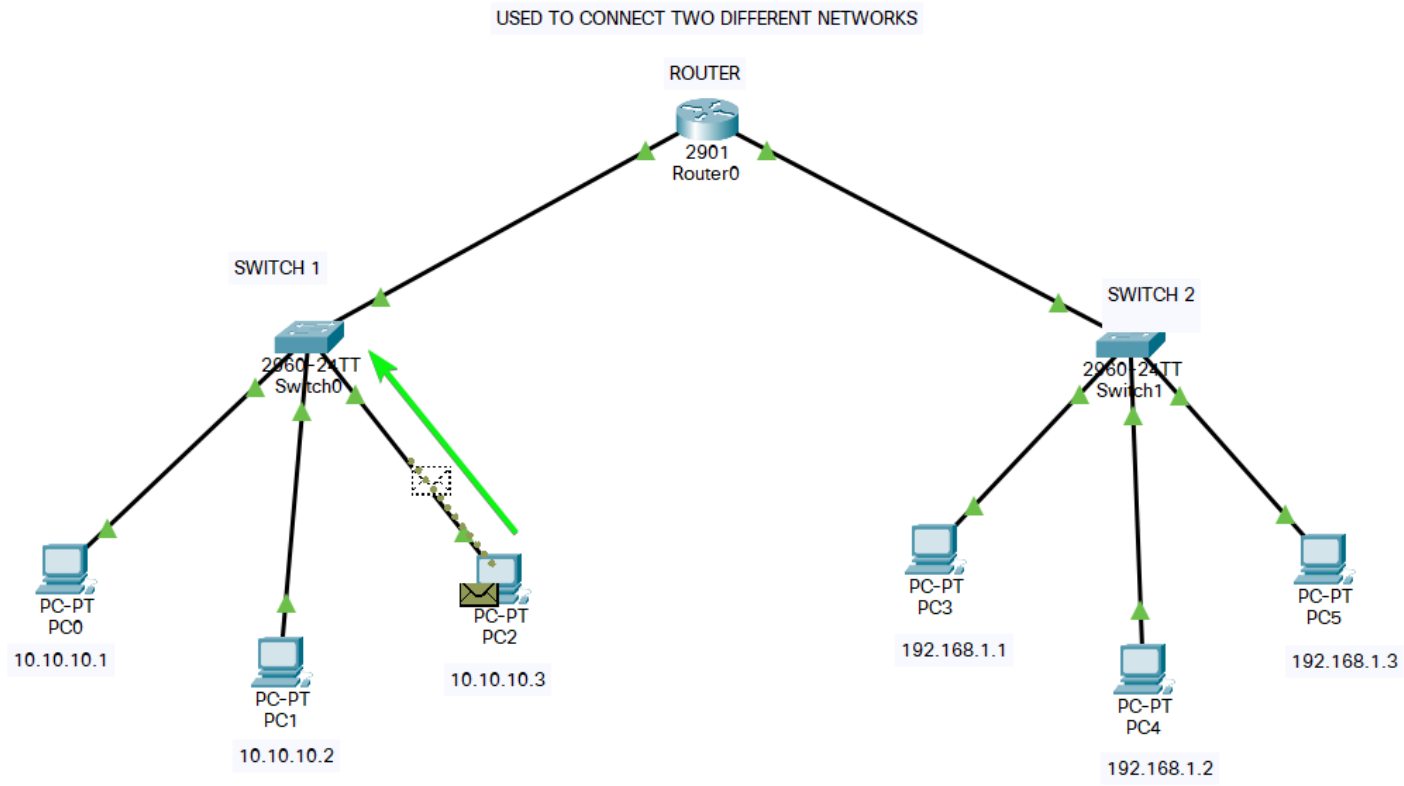
(1) Packet Send from PC0 to SWITCH 1



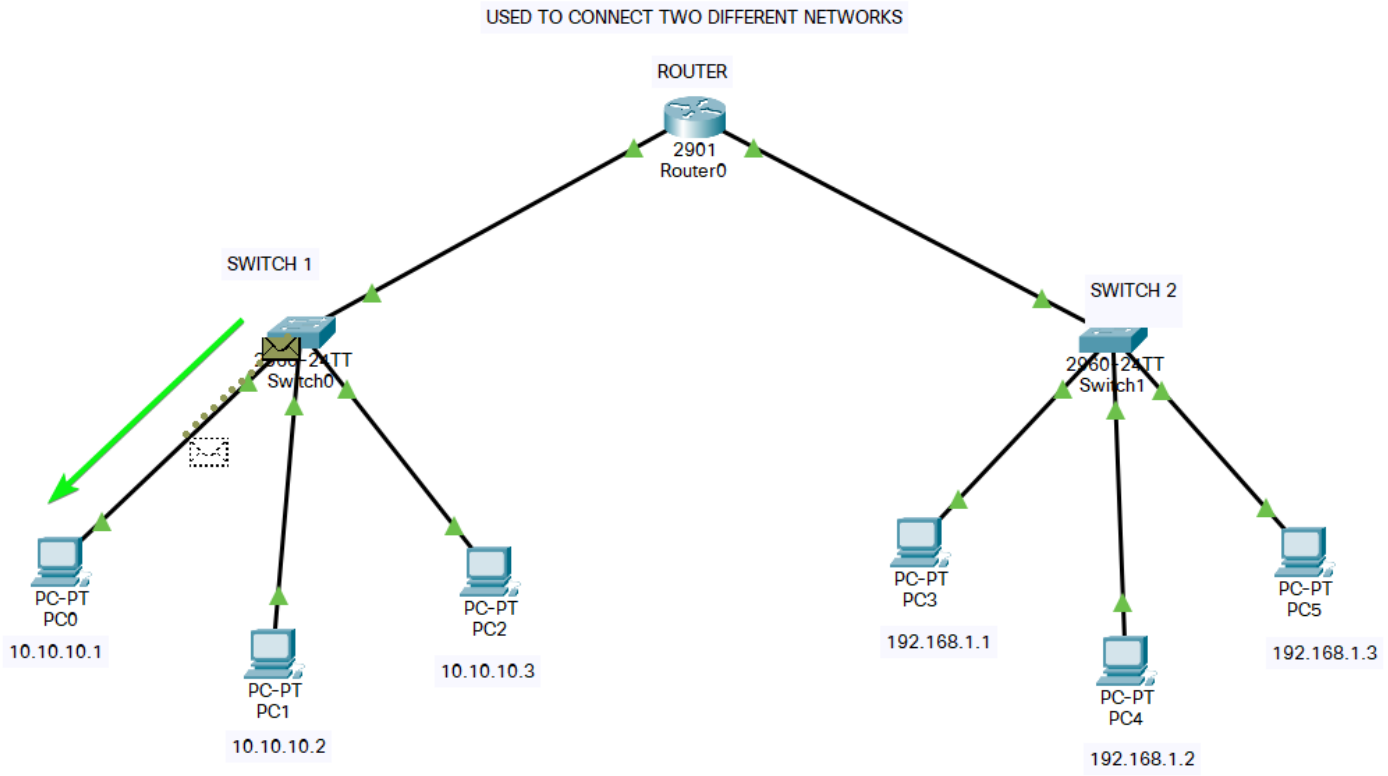
(2) Packet Sent from SWITCH 1 to PC3 {Since Same Network}



(3) Reply from PC2 sent to SWITCH1



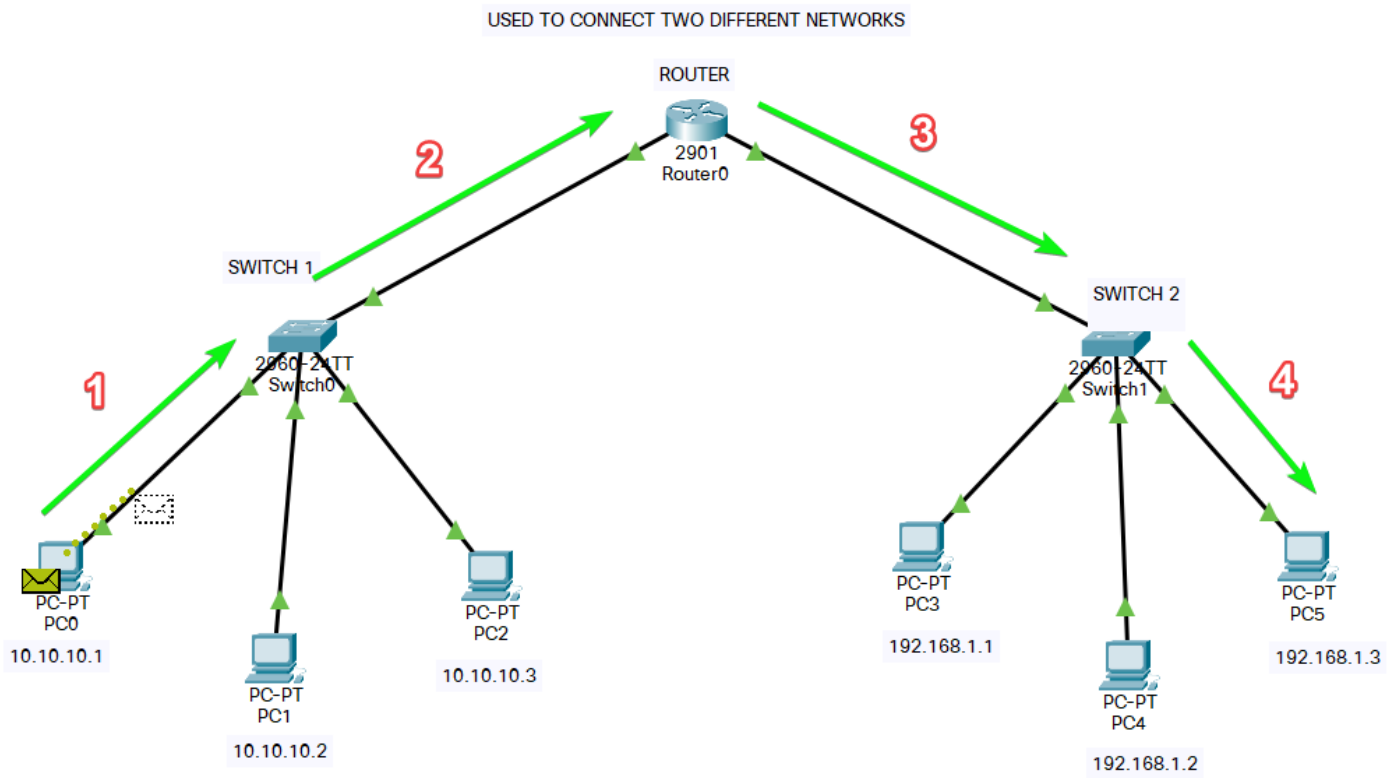
(4) Packet from SWITCH 1 to PC0



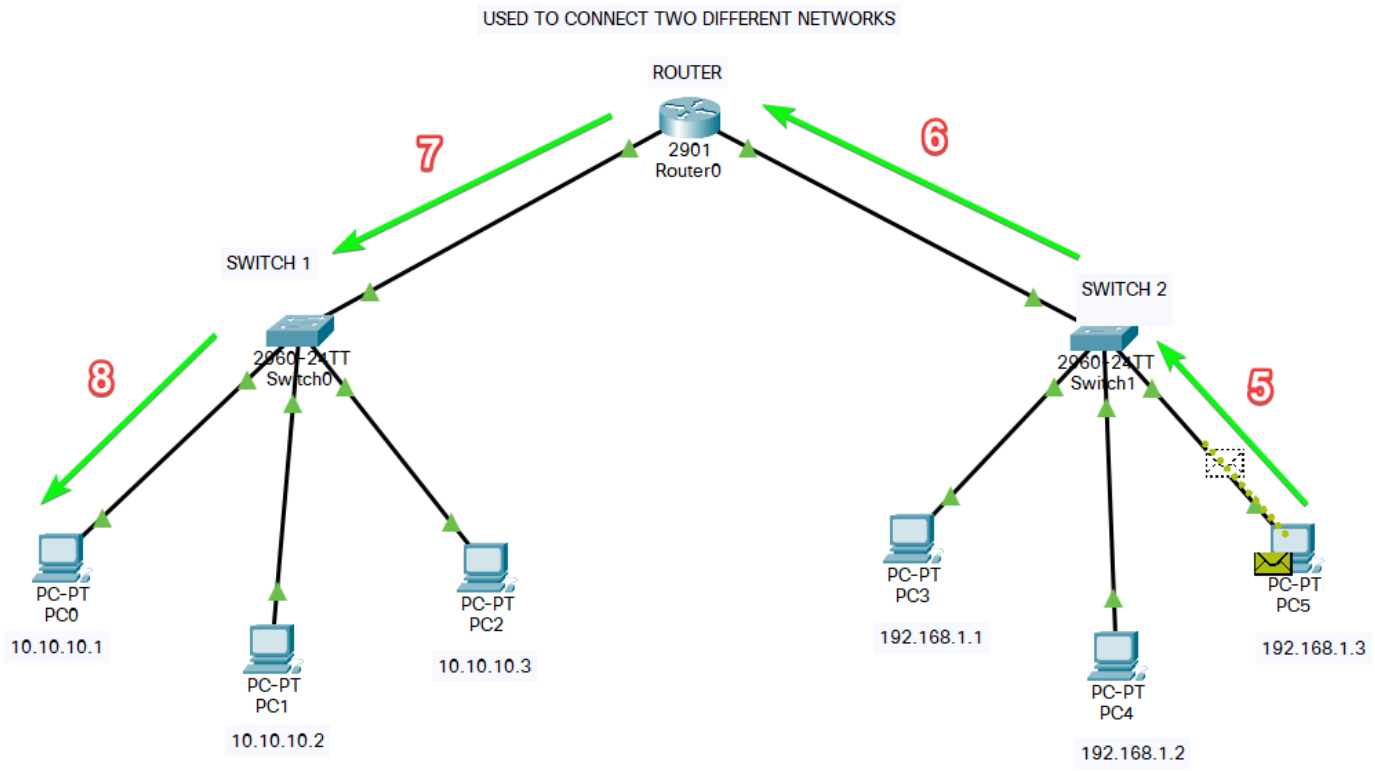
(B) INTER NETWORK [Ping PC0 to PC5]

```
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=16ms TTL=127
Reply from 192.168.1.3: bytes=32 time=17ms TTL=127
Reply from 192.168.1.3: bytes=32 time=16ms TTL=127
Reply from 192.168.1.3: bytes=32 time=16ms TTL=127

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 16ms, Maximum = 17ms, Average = 16ms
```

(1) Below Image Arrows Shows How Packet Travels from PC0 to PC5 via Router



(2) Below Image Arrows Shows How Packet Returns Back from PC5 to PC0 via Router



A router maintains a routing table using the routing algorithms. When a data packet is received at the router, it first checks the **IP address**.

If the IP address is the same as the network's IP address, it receives the data packet, else it forwards the data packet to the destination IP address using the routing table.

There are mainly two types of routing performed by Routers, they are:

1. **Static Routing:** In Static Routing, the path for the data packets is manually set. It is generally used for small networks.
2. **Dynamic Routing:** In Dynamic Routing, various routing algorithms are used to find the best and shortest path for the data packets.

Advantages of using a Router:

1. It can connect devices and provides routing facilities over different networks implementing the same protocol and structure.
2. Improves **security** by limiting the scope of data packets.
3. It has the filtering capability.
4. It can be used in a **large network.**
5. It uses full-duplex mode of communication
6. It has control over both the collision and broadcast domain.

Disadvantages of using a Router:

1. It is very complex to implement.
2. The implementation cost is quite **high**.
3. There is a need to maintain a **Routing table**.
4. There is a delay in forwarding the packets due to error checking.
5. It requires a special system administration configuration.

SUBMITTED BY:

U19CS012

BHAGYA VINOD RANA