

## Practical No. 1

### AIM: Physical Introduction To Cables , Connectors And Tools

#### CABLES:-

The following are the types of cables used in networking.

1. Unshielded Twisted Pair (UTP & STP) Cable
2. Fibre Optic Cable
3. Coaxial Cable

#### Twisted-Pair Cable

A twisted pair cable consists of two copper conductors, each one with its own plastic insulation and twisted together. One wire carries the signal and other is used as ground reference. The advantage of twisting is that both wires are equally affected by external influences. So the unwanted signals are canceled out as the receiver calculates the difference between signals in two wires.

This cable is of two types such as.

1. UTP (unshielded twisted pair)
2. STP (shielded twisted pair)

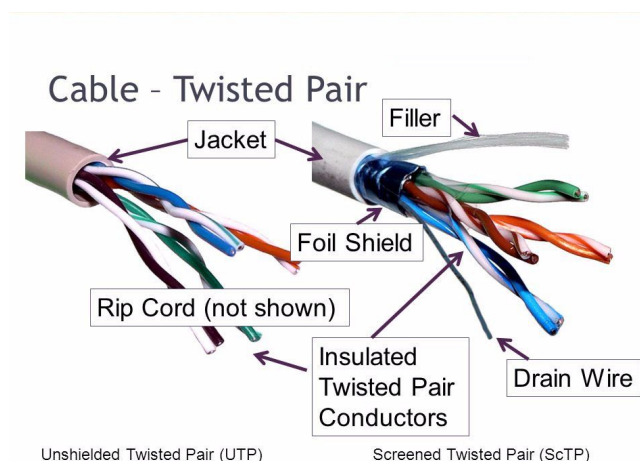
STP cable has one extra metal shield covering the insulated twisted pair conductors. But this is absent in UTP cables. The most common UTP connector is RJ45.

The unshielded twisted pair cable is classified into seven categories based on cable quality. Category 1 of cables is used in telephone lines with data rate around 0.1 Mbps. Whereas Category 5 used in LANs having 100 Mbps data rate.

Performance of twisted-pair cable is measured by comparing attenuation versus frequency. Attenuation increases with frequency above 100 kHz.

These cables are used in telephone lines to provide voice and data channels. DSL lines and

Local area networks also use twisted pair cables.

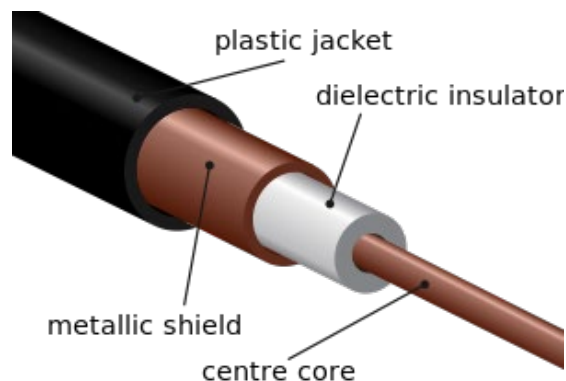


#### Coaxial Cable

Coaxial cable (coax) carries high frequency signals than twisted-pair cables. Coax has a central core conductor of solid wire enclosed in an insulator, which is covered by an outer conductor of metal foil. This outer conductor completes the circuit. Outer conductor is also enclosed in an insulator, and the whole cable is protected by a plastic cover.

These cables are categorized by RG (radio government) ratings. RG-59 used for Cable TV, RG-58 for thin Ethernet and RG-11 for thick Ethernet. The connector used in these cables is called BNC connector; it is used to connect the end of the cable to a device.

Though the coaxial cable has higher bandwidth, but its attenuation is much higher compare to twisted-pair cables. It is widely used in digital telephone networks where a single cable can carry data up to 600 Mbps. Cable TV networks use RG-59 coaxial cable. Traditional Ethernet LANs also use this cable.



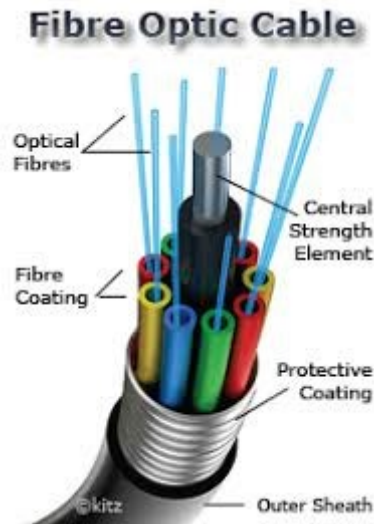
### **Fiber-Optic Cable**

A fiber optic cable transmits signals in the form of light. Optical fiber use reflection to guide light through a channel. It consists of two main parts: core and cladding. Core is denser compare to cladding and is made up of plastic or glass. Cladding acts as a protective cover to core. The difference in density of core and cladding is such that a beam of light moving through the core is reflected off the cladding, instead of being refracted into it.

Two modes of propagation of light are possible in optical fiber such as: multimode and single mode. Multimode fiber allows multiple beams from a light source move through the core. In multimode step-index fiber, the core density remains constant from the center to the edges. But in multimode graded-index fiber, core density gradually decreases from the center of the core to its edge. Graded-index fiber creates less distortion in the signal compare to step-index.

There are two types of connectors for fiber optic cables. The SC connector is used for cable TV, and ST connector used for connecting cable to networking devices. Attenuation in fiber optic cable is very low compare to other two types of cable. It provides very high bandwidth and immunity to electromagnetic interference. Light weight and greater immunity to tapping makes it more preferable cable.

Fiber optic cable is often used in backbone networks because of its wide bandwidth and cost effectiveness. Local areanetworks such as 100Base-FX network and 100Base-X use this cable. Also it is used by cable TV companies.

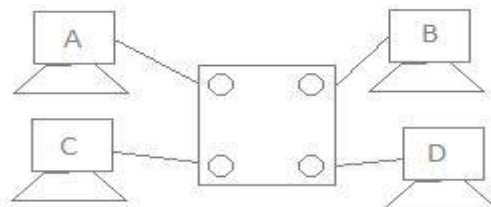


### CONNECTORS:-

To understand what connecting devices are, it is important to know about Backbone Networks. Backbone Network is a means of connecting 2 LAN's. It provides a transmission channel for packets from being transmitted from one LAN to the other. The individual LAN's are connected to the Backbone Network by using some types of devices such as Hubs, Repeaters, Switches, Bridges, Routers and Gateways.

#### Hub:

A hub works in the physical layer of the OSI model. It is basically a non-intelligent device, and has no decision-making capability.



Let's consider a 4-port network. There are 4 computers connected to the 4 ports. Suppose, if Computer A wants to send some data to Computer B using a Hub, then, Computer A broadcasts the data on the network, and Computer B, being connected to the network, has access to the data. But, in this case all the other ports connected to the network has access to the data that is being transmitted by Computer A. This happens because, the Hub works in the Physical Layer and hence it does not know about the MAC addresses of the ports connected to the network. So, there is a lack of security in the hub.

#### Repeater:

A repeater is a device similar to the Hub, but has additional features. It also works in the Physical layer. The repeaters are used in places where amplification of input signal is necessary. But, the kind of amplification done by the repeater is different from the regular amplification by amplifiers.

The repeaters are necessary since, during the transmission of the signals over long distances, the signal has attenuation, delay distortions and noise, which lead in loss of data. Hence, in order to prevent this, the regenerative repeaters are used. Hence, the repeater regenerates the faded signal. In addition, it has all the features of a Hub.

**Switch:**

A switch is a device that works in the 2<sup>nd</sup> layer of OSI model, the data link layer. Switch refers to the decision-making capacity. It has knowledge of the MAC addresses of the ports in the network.



If data has to be sent from Computer A to Computer B, then, the data is transferred to the Computer B only, and not to any other computers connected on the network. Hence, it establishes a link between the sender and the receiver based on the MAC addresses. This also means that when data is being sent from A to B, Computer C can establish a link with Computer D and communication can take place between them. So, simultaneous data transfer is possible in a switch. Also, Hub divides bandwidth, but a Switch does not.

It is also to be noted that a switch is a secure device, because it sends information only to the desired destinations, and also certain security features such as firewalls can be implemented in the Switches.

**Router:**

When there is more than one computer at home or in an organization, and we have a single internet connection, we need a Router. Router is a device which is used when multiple devices need to connect to the Internet using the same IP.

Any Internet Service Provider provides a single IP, and especially for personal use, the IP address is assigned dynamically. Suppose, an ISP has 1000 IP addresses, it does not mean that it has 1000 customers. An ISP assumes that not all devices will be connected to the internet at the same time. Hence, when a user wants to access the internet, any IP address from the pool of IP addresses from the ISP will be assigned to connect the user to the internet.



Hence, the router does the job of connecting multiple devices in a LAN to the internet using the same IP address. Since the router works in the Network Layer, it does on the basis of IP addresses.

**Gateway:**

The Gateway devices work in the Transport layer and above, where the different network technologies are implemented. A gateway is necessary when there are different technologies implemented by the different LAN's which are to be connected together.

Consider 2 networks, say in Mumbai, and a network in Bangalore. If data has to be sent from one place to another, we need to ensure that the network technology that is being used by both the networks are the same. If not, we need to use a Gateway.

### **TOOLS:-**

#### **Crimping tool**

A crimping tool is a device used to conjoin two pieces of metal by deforming one or both of them in a way that causes them to hold each other. The result of the tool's work is called a crimp. A good example of crimping is the process of affixing a connector to the end of a cable. For instance, network cables and phone cables are created using a crimping tool to join the RJ-45 and RJ-11 connectors to the both ends of either phone or CAT5 cable.



To use this crimping tool, each wire is first placed into the connector. Once all the wires are in the jack, the connector with wires are placed into the crimping tool, and the handles are squeezed together. Crimping punctures the plastic connector and holds each of the wires, allowing for data to be transmitted through the connect.

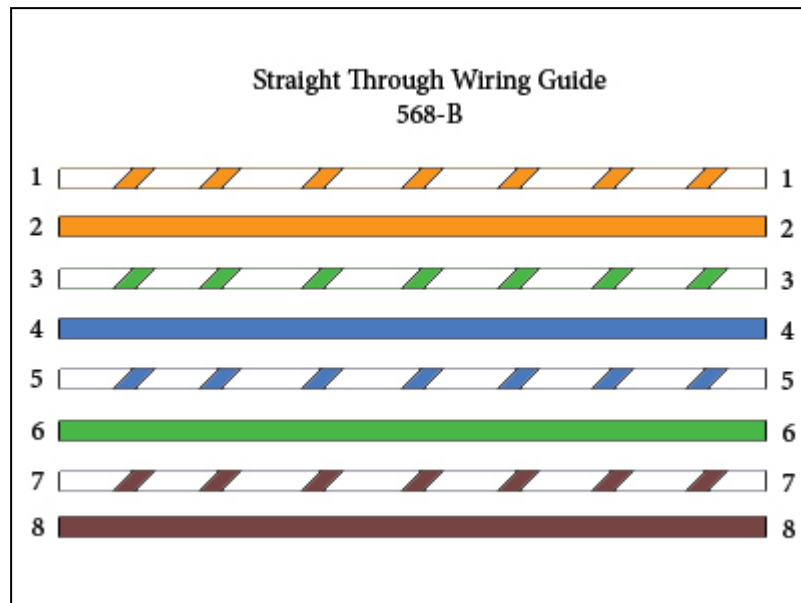
## Experiment No. 02

**AIM:** Design a LAN cable and set up a LAN connection between two computers and then share information between them (Hands on).

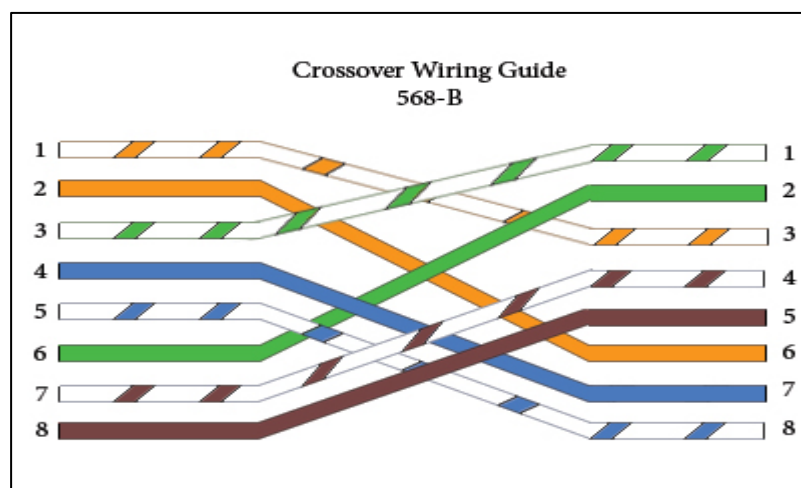
### THEORY:

Colour coding schemes:

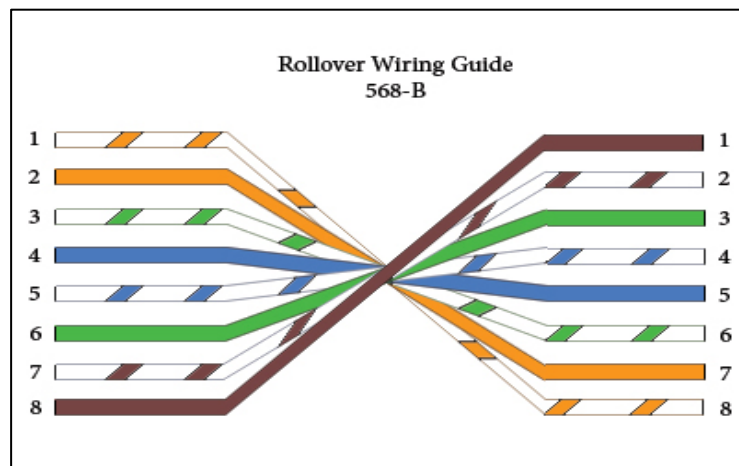
- 1) Straight Through: A straight through cable has identical ends.



- 2) Cross Over: A cross over cable has different ends.



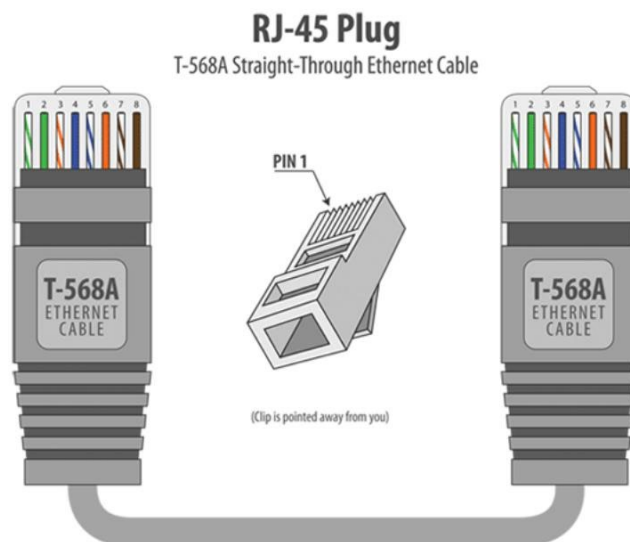
3) Roll Over: A roll over cable has opposite ends to the A jack.



**Procedure:**

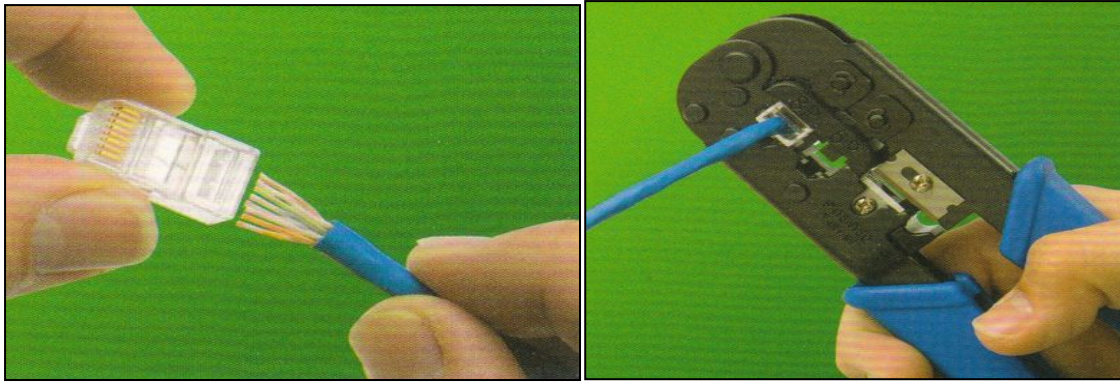
i) Prepare the cable

Start on one end and strip the cable jacket off (about 1") using a stripper or a knife. Be careful not to nick the wires, otherwise you will need to start over. Spread, untwist the pairs, and arrange the wires in the order of the desired cable end. Flatten the end between your thumb and forefinger. Trim the ends of the wires so they are even with one another, leaving only 1/2" in wire length. If it is longer than 1/2" it will be out-of-space and susceptible to crosstalk. Flatten and insure there are no spaces between wires.



Hold the RJ-45 plug with the clip facing down or away from you. Push the wires firmly into the plug. Inspect each wire is flat even at the front of the plug. Check the order of the wires. Double check again. Check that the jacket is fitted right against the stop of the plug. Carefully hold the wire and firmly crimp the RJ-45 with the crimper.





Check the colour orientation, check that the crimped connection is not about to come apart, and check to see if the wires are flat against the front of the plug. If even one of these are incorrect, you will have to start over. Test the Ethernet cable.

- ii) Configuration for transfer of data between two computers

### **Step 1: Connect both PCs with LAN cable**

Connect both computers to a LAN cable. You can use any LAN cable (crossover or ethernet cable). It doesn't matter on a modern computer because both of them use the same port and have very few functional differences.

### **Step 2: Enable Network Sharing on Both PCs**

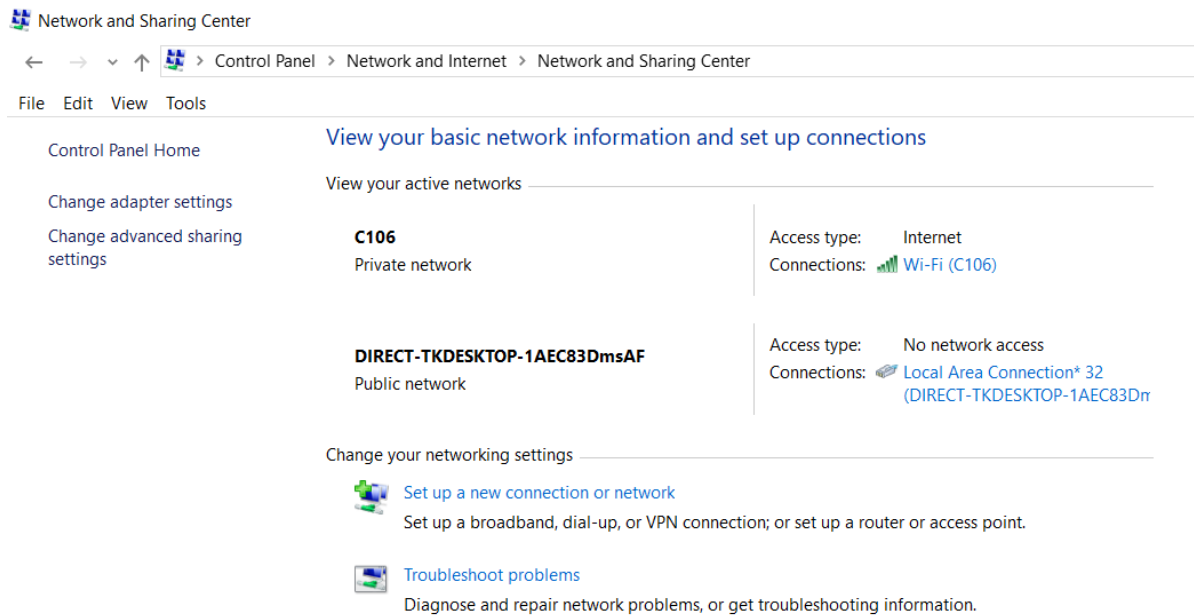
Now that you have physically connected both PCs with a LAN cable, we have to turn on Network Sharing on both computers to exchange files between them. It is a simple process step-by-step process. Make sure you do this on both PCs.

To enable sharing, go to the Start menu and search "Control Panel". Once you see it, click on it, to open it. Once the Control Panel window opens, click on Network and Internet. In the next dialogue box, open Network and Sharing Center. Alternatively, you can also type "Control Panel\Network and Internet\Network and Sharing Center" in the search box of Control Panel and hit Enter key. This will redirect you from Control Panel to Network and Sharing Center.

*Start → Control Panel → Network and Internet → Network and Sharing center*

On the left-hand side of 'Network and Sharing Center' window, click on "Change advanced sharing settings".





Here, you'll find three networks – Public, Private and All Network. Public Network is for places like airports and coffee shops, Private network is for an organization or your home network and All Network comprises of both. To make sure, the setup is flawless, we'll recommend you choose "All Networks".

Next, expand All Networks by clicking on the drop-down icon. Here, we need to enable Public Sharing so that the PCs can access files from each other over the LAN cable.

Once done, click Save Changes. Just as I said in the beginning, repeat the same steps for the other PC.

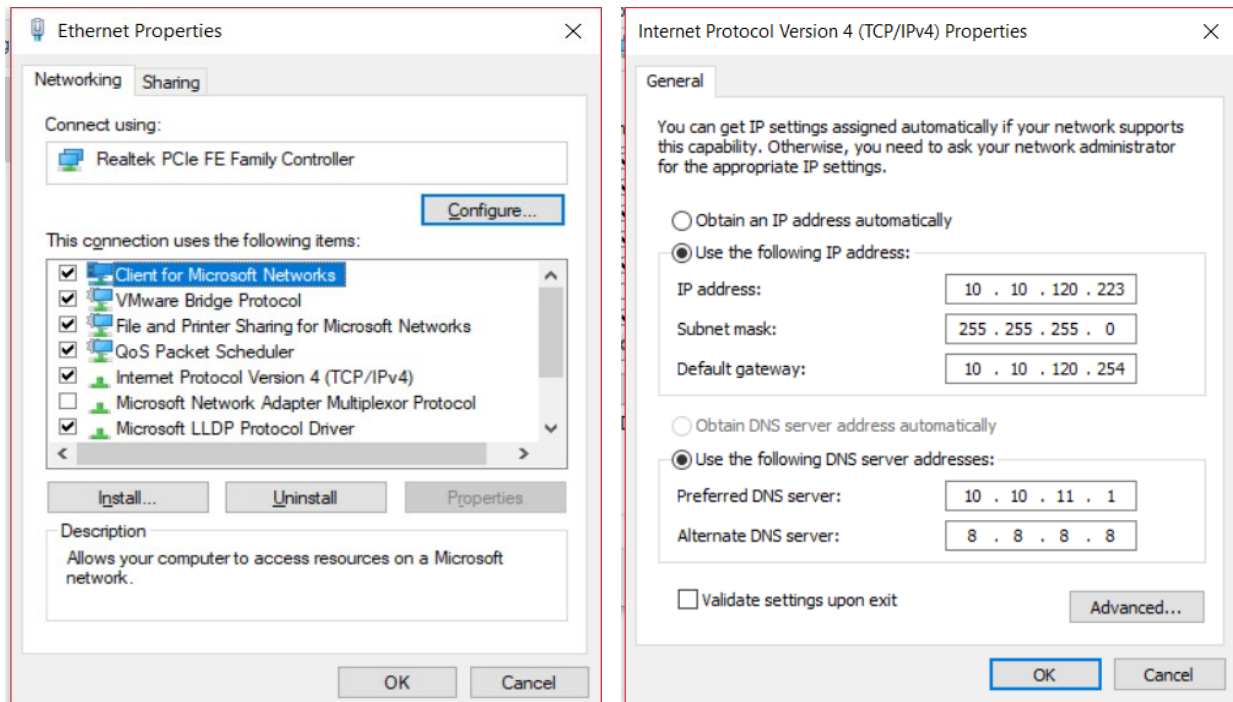
### Step 3: Setup IP

1. To set up IP address,

Control Panel → Network and Internet → Network and Sharing Center → Change Adapter Settings.

And choose Ethernet option.

2. In the next pop-up, select "Internet Protocol Version 4 (TCP/IPv4)". Now, click on Properties. This will open another dialogue box.
3. Here, you need to configure the two PCs with different IP settings.



On computer 1, select the option “Use the following IP address.” and, put the following values

- IP Address: 192.168.1.1
- Subnet mask: 225.225.225.0

On the second computer, do similar steps, but change the IP address as:

- IP address: 192.168.1.2
- Subnet mask: 225.225.225.0

What we are doing is keeping the subnet mask the same and changing the IP address.

To check whether the devices are connected or not, Open the RUN command and ping the IP address of the other device and if it does safely, you are connected.

To transfer files, open your Window’s File Explorer and click on Network tab at the left side of the window.

Here, you will find the device with you are connected. Just grab the file and paste it in the public folder in the computer icon.

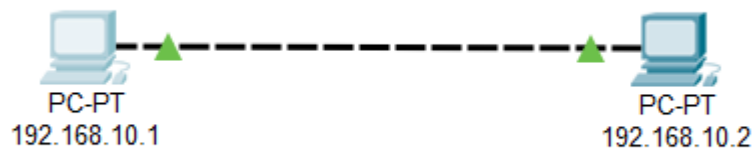
**RESULT:** Both the computers are successfully connected by LAN (ethernet) wire.

## Experiment No. 03

**Aim: - Connect and transferring data between two computers using cisco packet tracer simulation environment similar as hands on. Apply pinging command Also.**

**Procedure:-**

**Step 1:** Start with selecting two general computers (end devices) from the list down to the working space.



**Step 2:** Configure the IP address and subnet mask for both the computers either by using command prompt or by using desktop property given.

192.168.10.1

Physical Config **Desktop** Programming Attributes

IP Configuration X

Interface FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IP Address 192.168.10.1

Subnet Mask 255.255.255.0

Default Gateway 0.0.0.0

DNS Server 0.0.0.0

IPv6 Configuration

☐ DHCP ☐ Auto Config ☒ Static

IPv6 Address /

Link Local Address FE80::2E0:8FFF:FE75:858B

IPv6 Gateway

IPv6 DNS Server

802.1X

☐ Use 802.1X Security

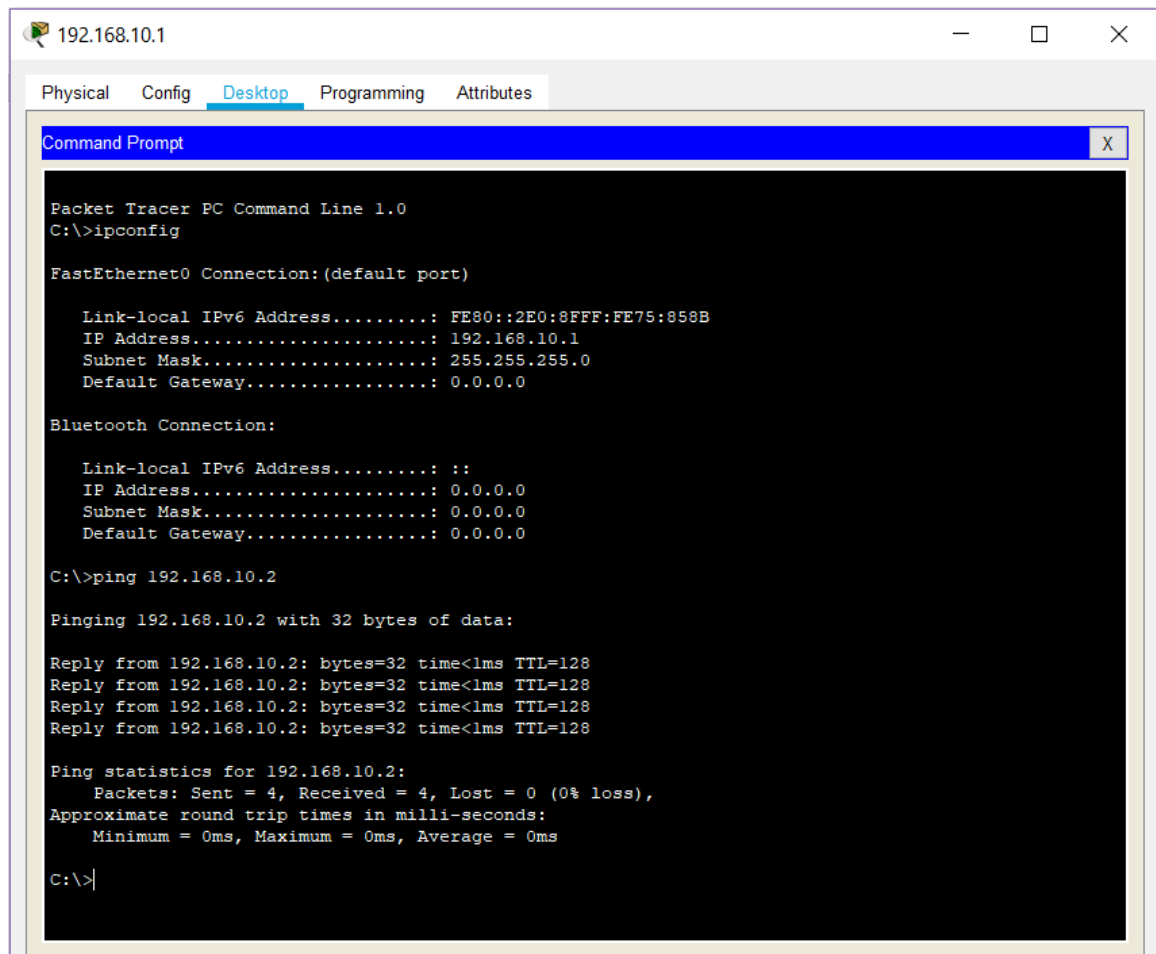
Authentication MD5

Username

Password

☐ Top

**Step 3:** - Ping the other computer in command prompt. If it is pinging, then the two computers are connected, otherwise not.



```
192.168.10.1
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection:(default port)

    Link-local IPv6 Address.....: FE80::2E0:8FFF:FE75:858B
    IP Address.....: 192.168.10.1
    Subnet Mask.....: 255.255.255.0
    Default Gateway.....: 0.0.0.0

Bluetooth Connection:

    Link-local IPv6 Address.....: ::
    IP Address.....: 0.0.0.0
    Subnet Mask.....: 0.0.0.0
    Default Gateway.....: 0.0.0.0

C:\>ping 192.168.10.2

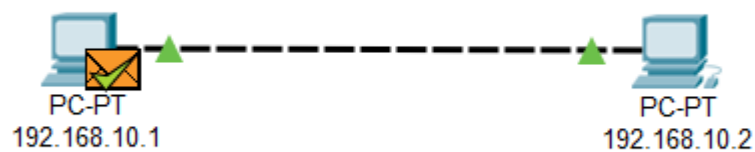
Pinging 192.168.10.2 with 32 bytes of data:

Reply from 192.168.10.2: bytes=32 time<1ms TTL=128
Reply from 192.168.10.2: bytes=32 time<1ms TTL=128
Reply from 192.168.10.2: bytes=32 time<1ms TTL=128
Reply from 192.168.10.2: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

**Step 4:** - Check the network status by sending an ICMP packet.



**Result:** - The message was successfully sent from one device to another.

## Experiment No. 04

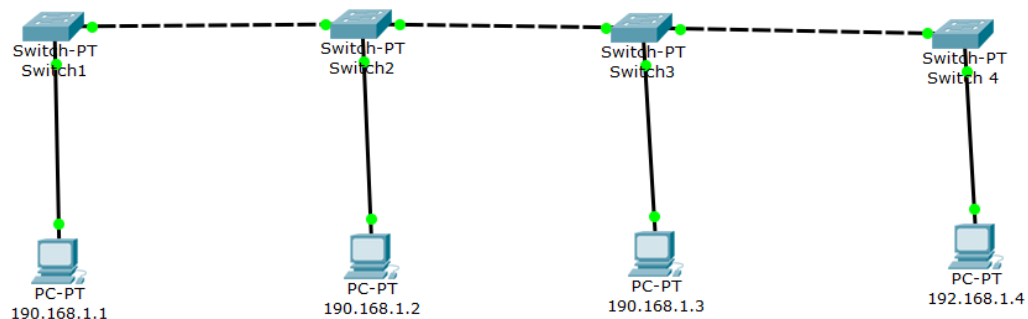
**Aim: To learn about different topologies and create LANs using them in cisco packet tracer.**

### Different types of Topologies:

#### Bus:

Bus topology uses one main cable to which all nodes are directly connected. The main cable acts as a backbone for the network. The first advantage of bus topology is that it is easy to connect a computer or peripheral device. The second advantage is that the cable requirements are relatively small, resulting in lower cost.

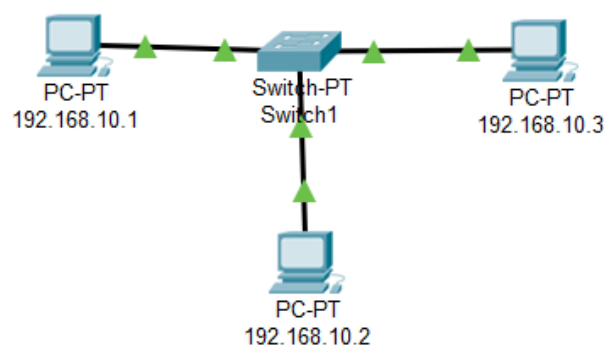
One of the major disadvantages is that if the main cable breaks, the entire network goes down. This type of network is also difficult to troubleshoot. For these reasons, this type of topology is not used for large networks, such as those covering an entire building.



#### Star:

In star topology, each computer is connected to a central hub using a point-to-point connection. The central hub can be a computer server that manages the network, or it can be a much simpler device that only makes the connections between computers over the network possible.

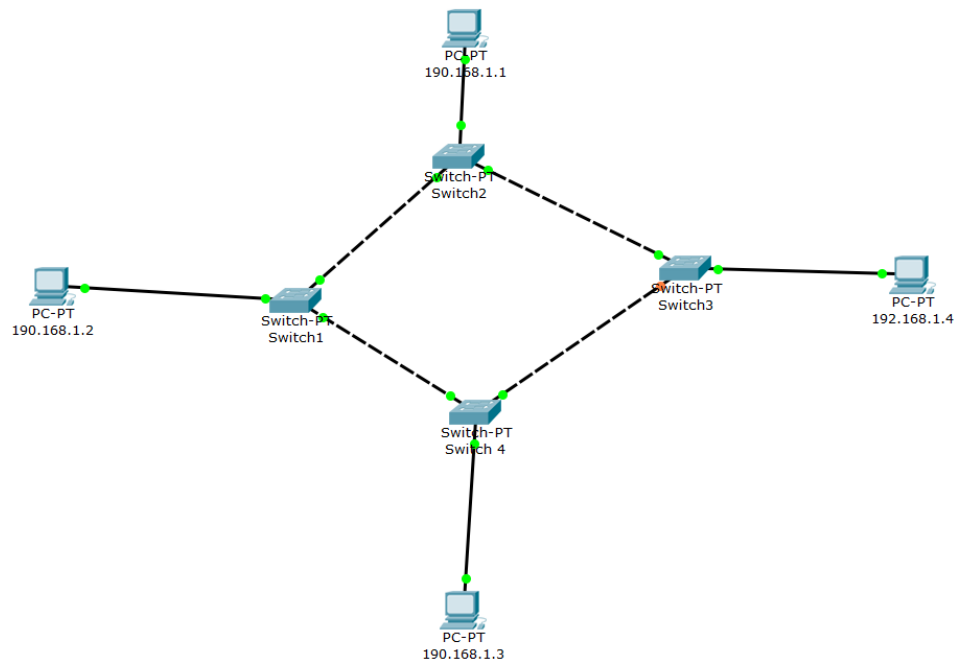
Star topology is very popular because the start-up costs are low. It is also easy to add new nodes to the network. The network is robust in the sense that if one connection between a computer and the hub fails, the other connections remain intact. If the central hub fails, however, the entire network goes down. It also requires more cable than bus topology and is, therefore, more expensive.



### Ring:

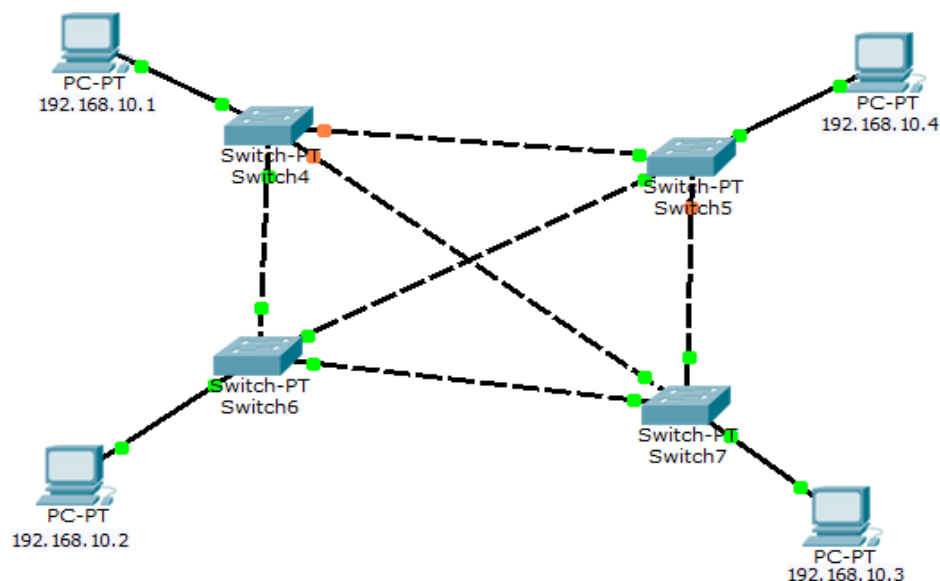
In ring topology, the computers in the network are connected in a circular fashion, and the data travels in one direction. Each computer is directly connected to the next computer, forming a single pathway for signals through the network. This type of network is easy to install and manage.

If there's a problem in the network, it is easy to pinpoint which connection is defective. It is also good for handling high-volume traffic over long distances since every computer can act as a booster of the signal. On the downside, adding computers to this type of network is more cumbersome, and if one single computer fails, the entire network goes down.



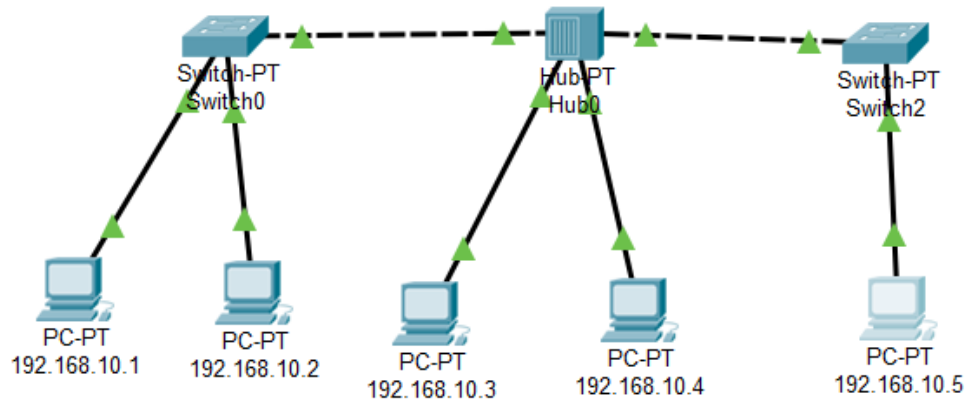
### Mesh:

In mesh topology, every node has a direct point-to-point connection to every other node. Because all connections are direct, the network can handle very high-volume traffic. It is also robust because if one connection fails, the others remain intact. Security is also high since data travels along a dedicated connection.



### Hybrid:

It is two different types of topologies which is a mixture of two or more topologies. For example, if in an office in one department ring topology is used and in another star topology is used, connecting these topologies will result in Hybrid Topology (bus topology and star topology).



#### Procedure:

- Open cisco packet tracer.
- Create the desired topology, using the given device in the device panel at the bottom left.
- Configure each device with a valid IP and other required entries for the connection to work.
- Wait till all the links become green. Or check by pinging command in command prompt.
- Now send a packet from one node to another.

```

Command Prompt
Packet Tracer PC Command Line 1.0
PC>ipconfig 192.168.1.4 255.255.255.0
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=12ms TTL=128
Reply from 192.168.1.1: bytes=32 time=3ms TTL=128
Reply from 192.168.1.1: bytes=32 time=0ms TTL=128
Reply from 192.168.1.1: bytes=32 time=0ms TTL=128

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 = 12ms, Average = 3ms
PC>

```

**Result:** The LAN was successfully created using various topologies.



## Experiment No. 05

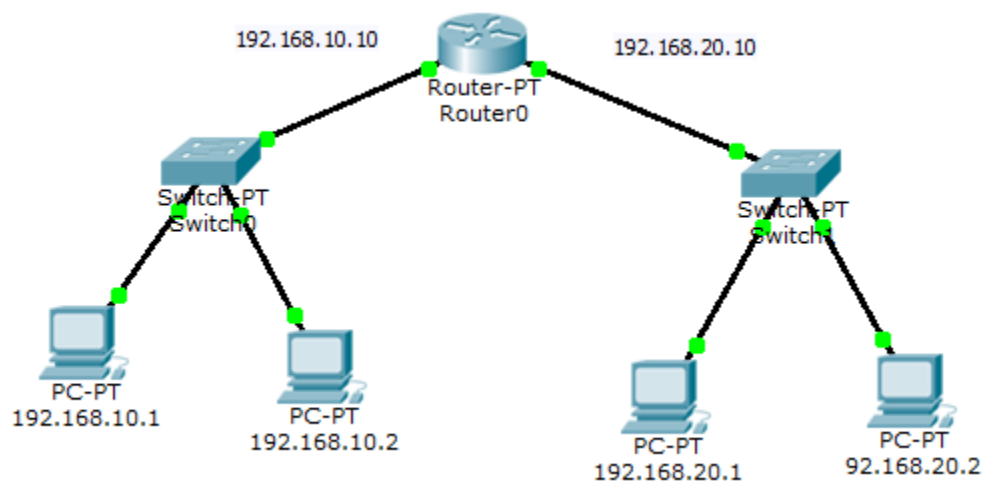
**AIM: - Connect two different networks through a Router.**

### Theory:

Any Internet Service Provider (ISP) provides a single IP, and especially for personal use, the IP address is assigned dynamically. This is done because, suppose, an ISP has 1000 IP addresses, it does not mean that it has 1000 customers. An ISP assumes that not all devices will be connected to the internet at the same time. Hence, when a user wants to access the internet, any IP address from the pool of IP addresses from the ISP will be assigned to connect the user to the internet.

### Procedure:-

**Step 1: - Set up the basic connection between the two PCs using router.**



**Step 2: - Configure the computers with valid IPs, Gateways, and the default subnet mask.**

192.168.10.1

### IP Configuration

IP Configuration

☐ DHCP ☒ Static

IP Address

192.168.10.1

Subnet Mask

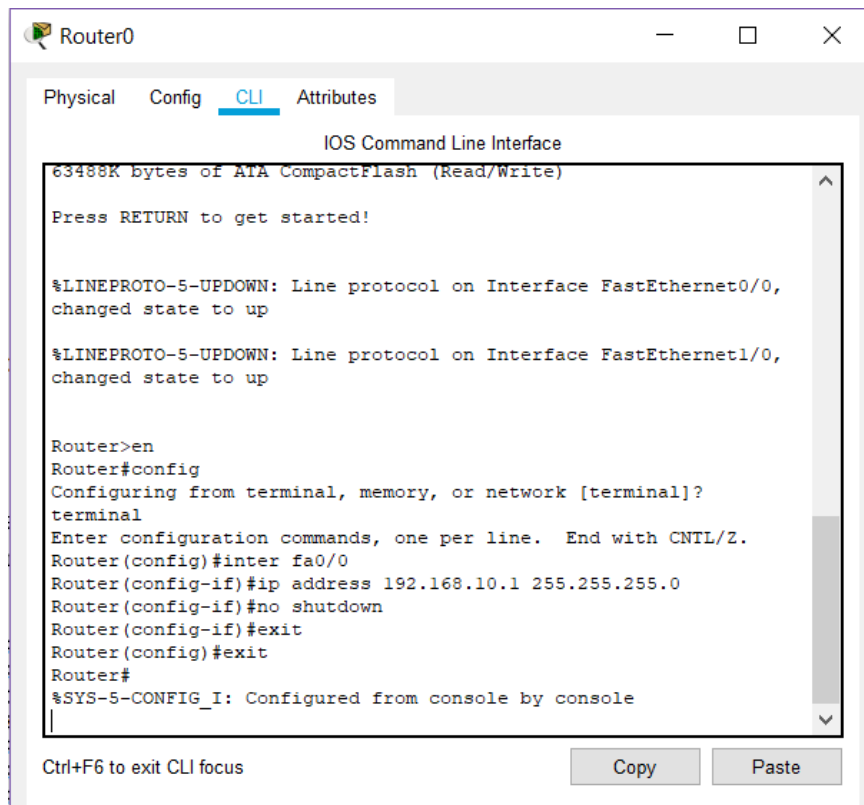
255.255.255.0

Default Gateway

192.168.10.10

DNS Server

**Step 3:** - Open the command line interface of the router and enter the following commands.



The screenshot shows the Router0 CLI interface with the following text:

```
Router0
Physical Config CLI Attributes
IOS Command Line Interface
63488K bytes of ATA CompactFlash (Read/Write)
Press RETURN to get started!

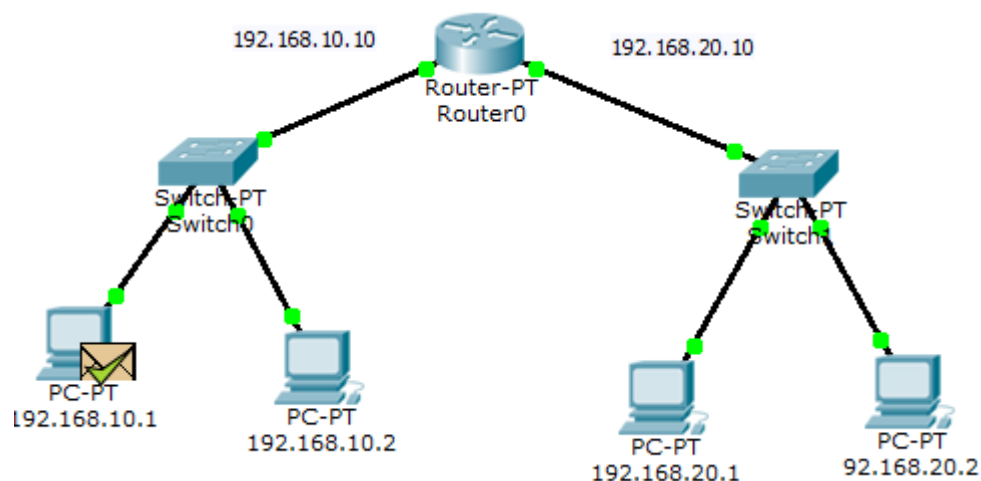
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0,
changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0,
changed state to up

Router>en
Router#config
Configuring from terminal, memory, or network [terminal]?
terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#inter fa0/0
Router(config-if)#ip address 192.168.10.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
```

At the bottom, there is a text prompt "Ctrl+F6 to exit CLI focus" and two buttons labeled "Copy" and "Paste".

**Step 4:** - Now in simulation mode send a simple PDU from 192.168.10.1 to 192.168.20.1.



**Result:** - The router was successfully configured.

## Experiment No. 06

**Aim: To implement default routing to connect multiple different networks and share data between network devices using cisco packet tracer.**

### Theory:

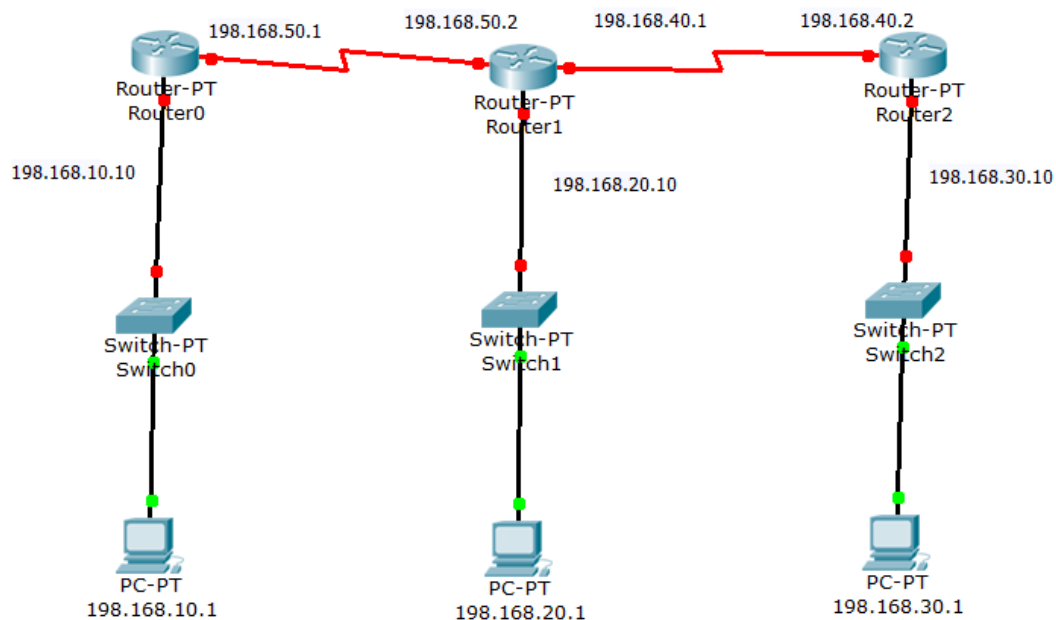
Routing is a process of selecting a path for traffic in a network or between or across multiple networks. Broadly, routing is performed in many types of network.

Default routing is one of the way routing can be done.

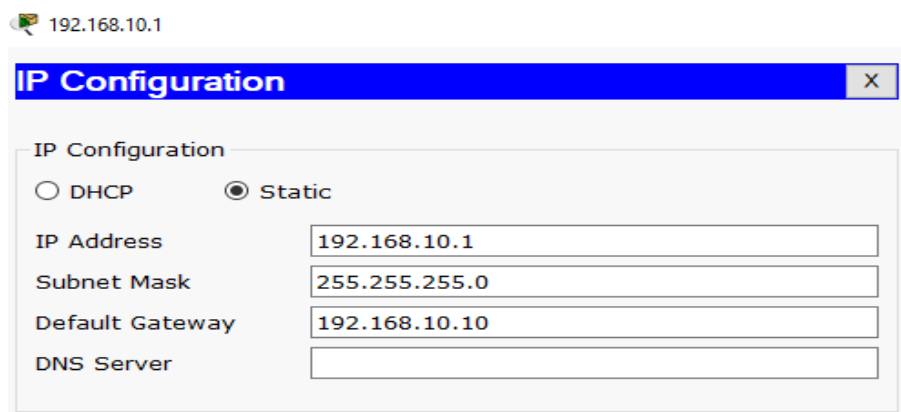
This is the method where the router is configured to send all packets towards a single router (next hop). It doesn't matter to which network the packet belongs, it is forwarded out to router which is configured for default routing. It is generally used with stub routers. A stub router is a router which has only one route to reach all other networks.

### Procedure :

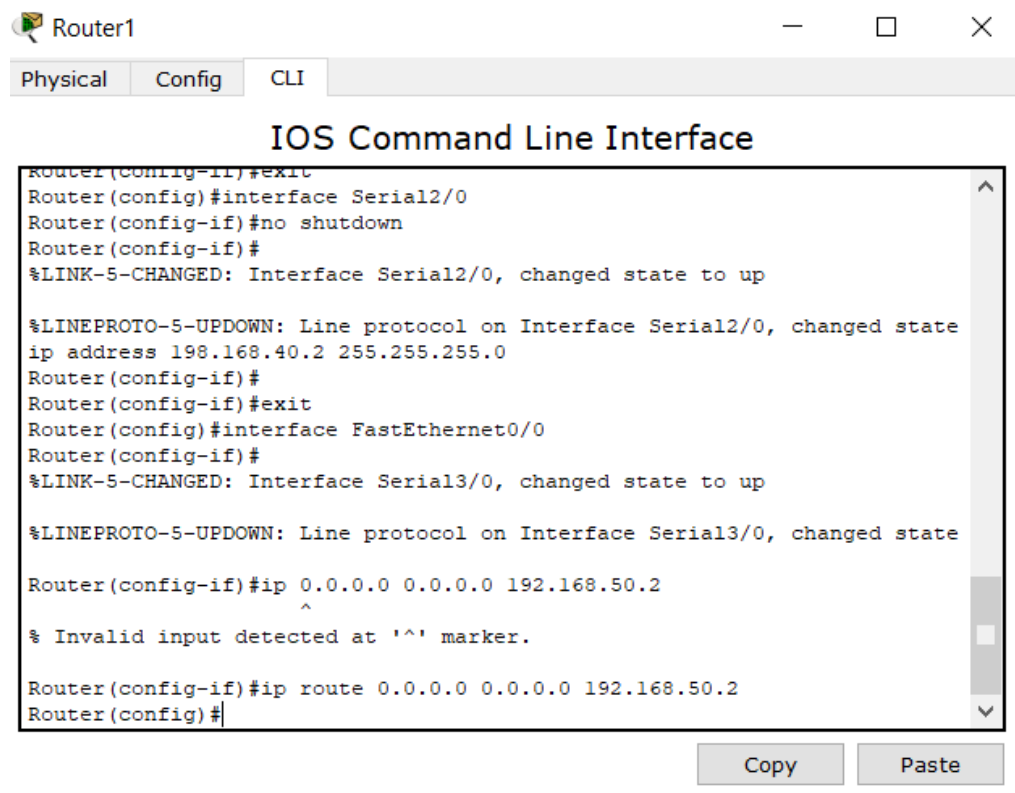
**Step 1:** Connect routers as shown in the figure, with the appropriate switch devices and end-devices.



**Step 2:** Assign IP address to each end-device and assign them a name as well. Configure the router with serial ports and switch them on.



**Step 3:** Route the path with proper CLI command.



```

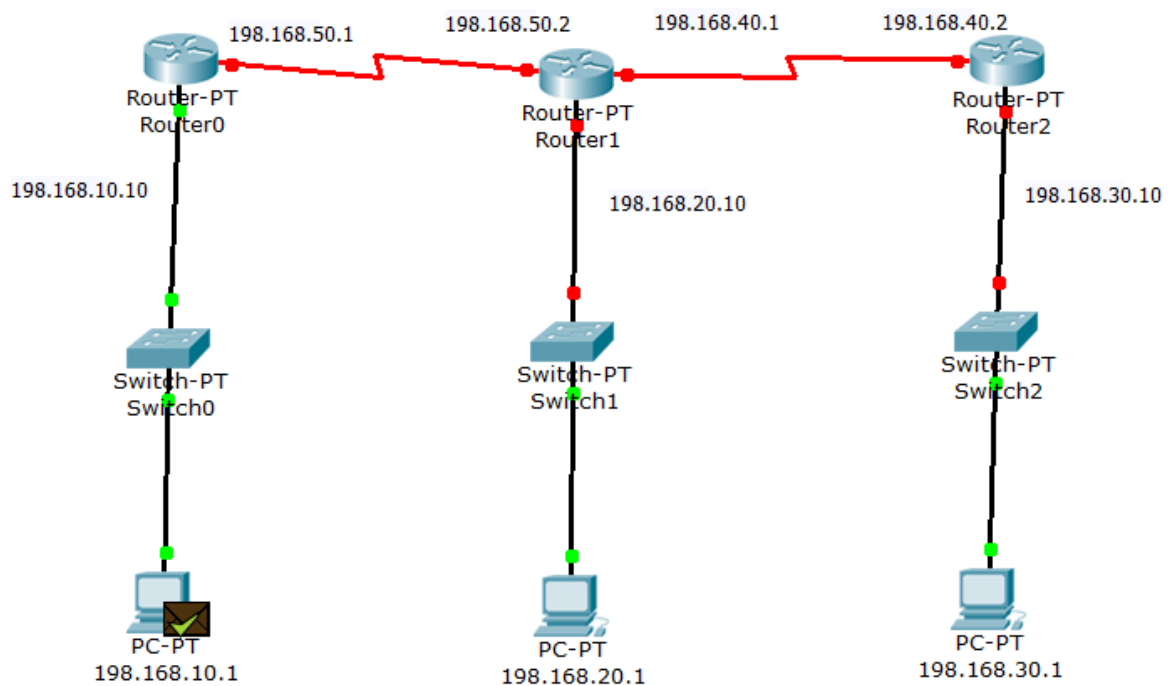
Router1
Physical Config CLI
IOS Command Line Interface
Router(config)#exit
Router(config)#interface Serial2/0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface Serial2/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state
ip address 198.168.40.2 255.255.255.0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/0
Router(config-if)#
%LINK-5-CHANGED: Interface Serial3/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial3/0, changed state
Router(config-if)#ip 0.0.0.0 0.0.0.0 192.168.50.2
^
% Invalid input detected at '^' marker.

Router(config-if)#ip route 0.0.0.0 0.0.0.0 192.168.50.2
Router(config)#
Copy Paste
  
```

**Step 4:** Transfer the ICMP packet to check the connection.



**RESULT:** Default routing has been implemented successfully.

## Experiment No. 07

**Aim: To implement static routing to connect multiple different networks and share data between different network devices using cisco packet tracer.**

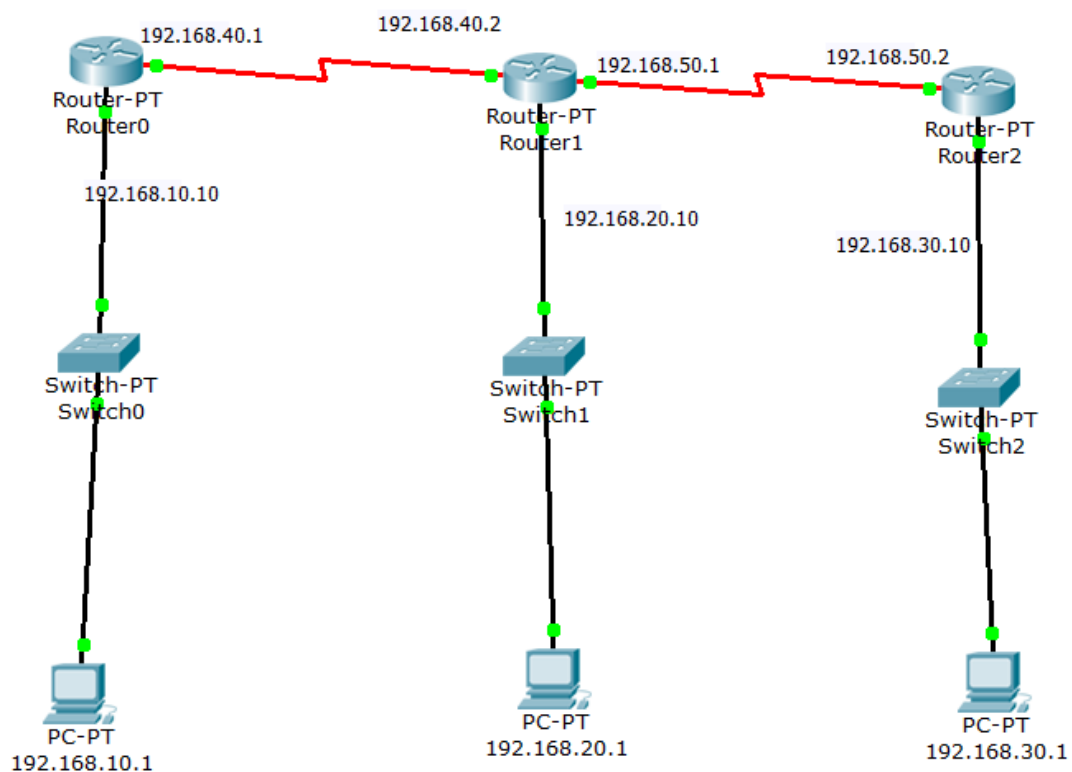
### Theory:

A routing table is a set of rules, often viewed in table format, that is used to determine where data packets traveling over an Internet Protocol (IP) network will be directed. All IP-enabled devices, including routers and switches, use routing tables.

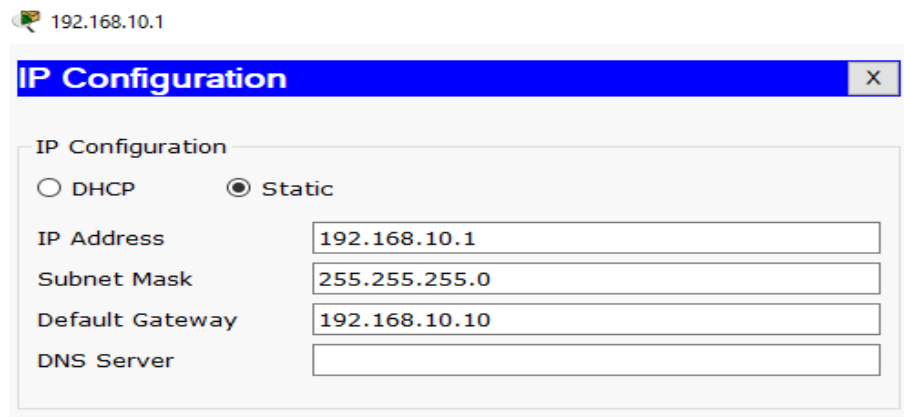
A routing table contains the information necessary to forward a packet along the best path toward its destination. Each packet contains information about its origin and destination. When a packet is received, a network device examines the packet and matches it to the routing table entry providing the best match for its destination. The table then provides the device with instructions for sending the packet to the next hop on its route across the network.

### Procedure:

**Step 1:** Connect routers as shown in the figure, with the appropriate switch devices and end-devices.



**Step 2:** Assign IP address to each end-device and assign them a name as well. Configure the router with serial ports and switch them on.



192.168.10.1

### IP Configuration

IP Configuration

☐ DHCP ☒ Static

IP Address: 192.168.10.1

Subnet Mask: 255.255.255.0

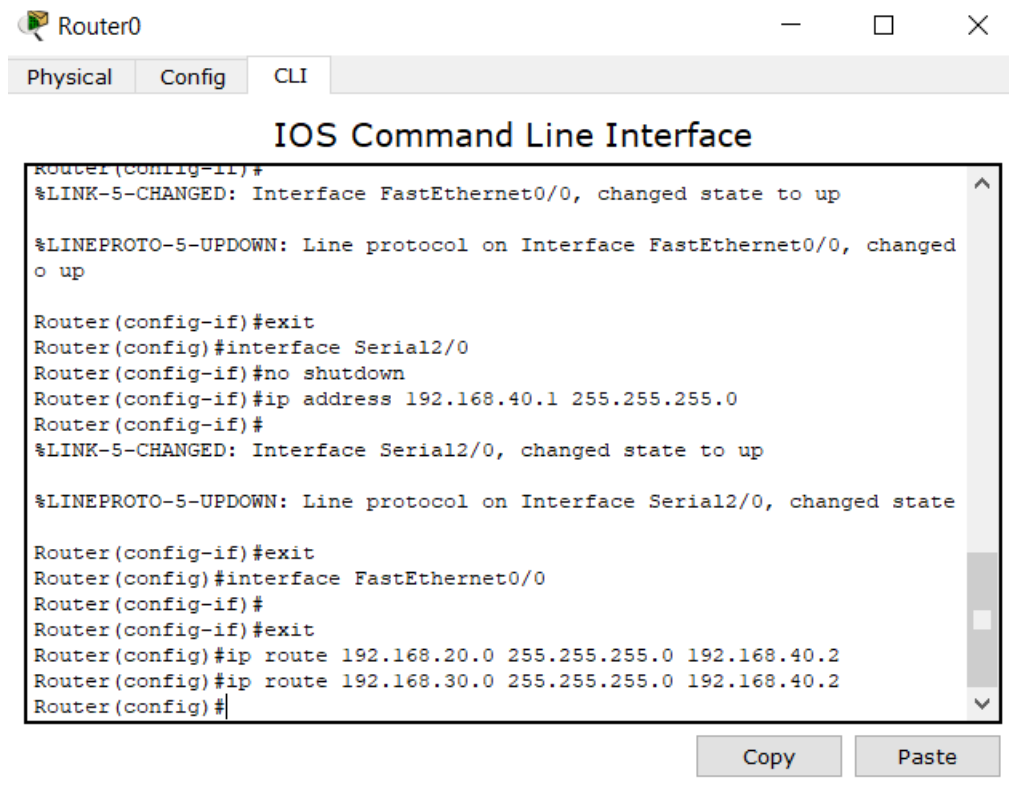
Default Gateway: 192.168.10.10

DNS Server:

**Step 3:** Configure Routers 1 and 2 in CLI so that they can send messages between each other.

To configure a static route:

R1(config)# ip route [destination\_network] [subnet\_mask] [next hope IP / exit interface ]



Router0

Physical Config CLI

### IOS Command Line Interface

```
Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed
o up

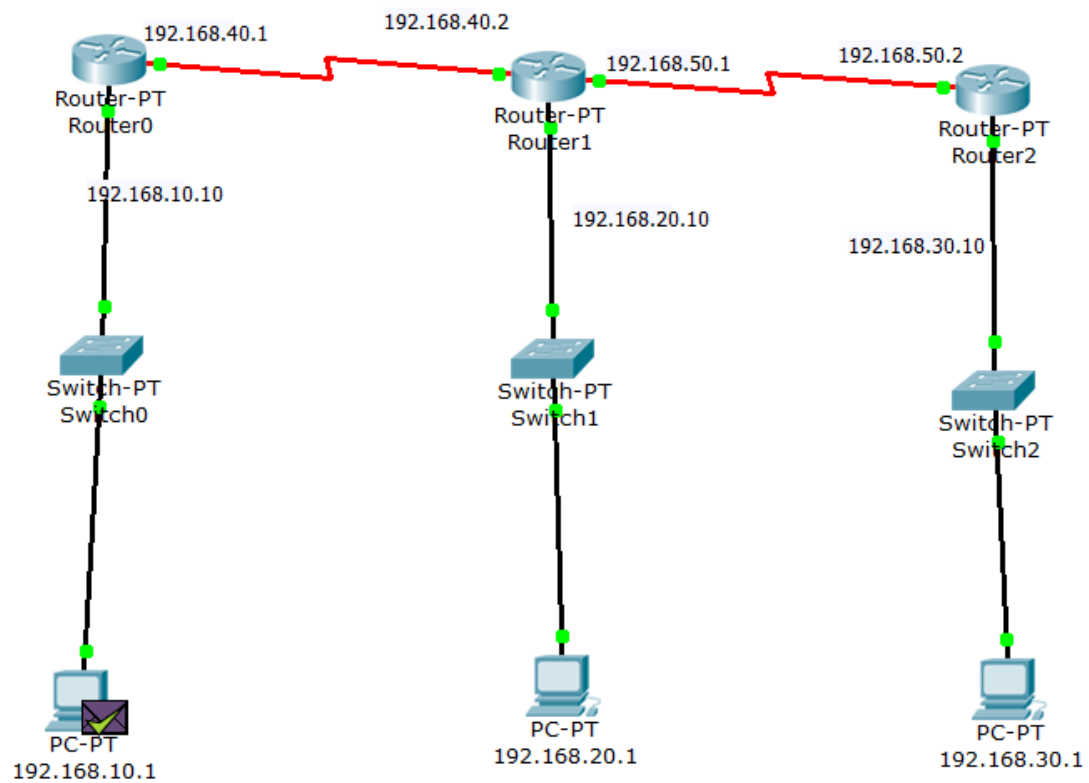
Router(config-if)#exit
Router(config)#interface Serial2/0
Router(config-if)#no shutdown
Router(config-if)#ip address 192.168.40.1 255.255.255.0
Router(config-if)#
%LINK-5-CHANGED: Interface Serial2/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state

Router(config-if)#exit
Router(config)#interface FastEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#ip route 192.168.20.0 255.255.255.0 192.168.40.2
Router(config)#ip route 192.168.30.0 255.255.255.0 192.168.40.2
Router(config)#
```

Copy Paste

**Step 4:** Check the network status by sending an ICMP packet.



**Result:** Successfully performed static routing in routers.



## Experiment No. 08

**AIM:- Implement Dynamic Routing to connect multiple different networks and share data between different network devices Using Cisco Packet Tracer.**

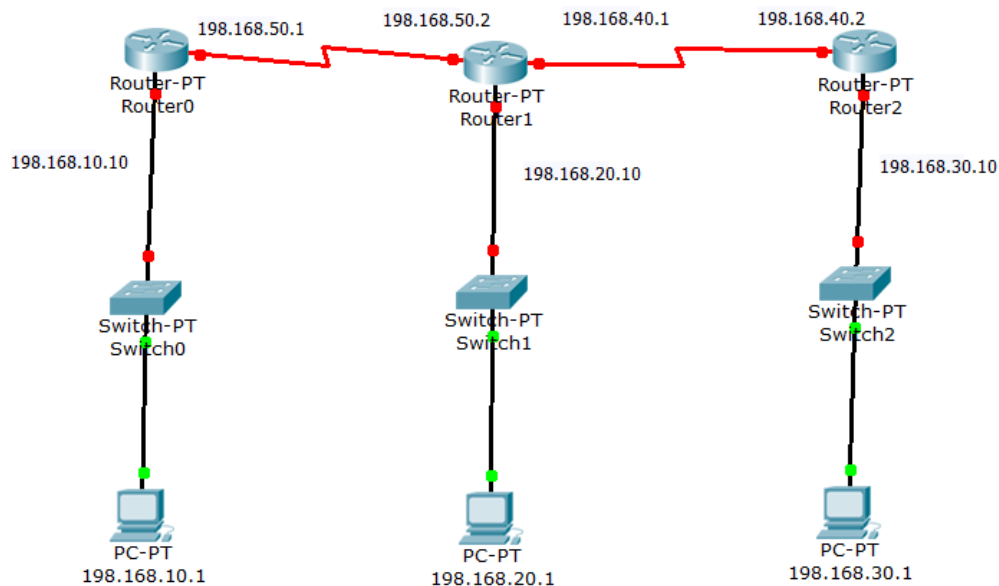
### Theory:

Dynamic routing is a networking technique that provides optimal data routing. Unlike static routing, dynamic routing enables routers to select paths according to real-time logical network layout changes. In dynamic routing, the routing protocol operating on the router is responsible for the creation, maintenance and updating of the dynamic routing table. In static routing, all these jobs are manually done by the system administrator.

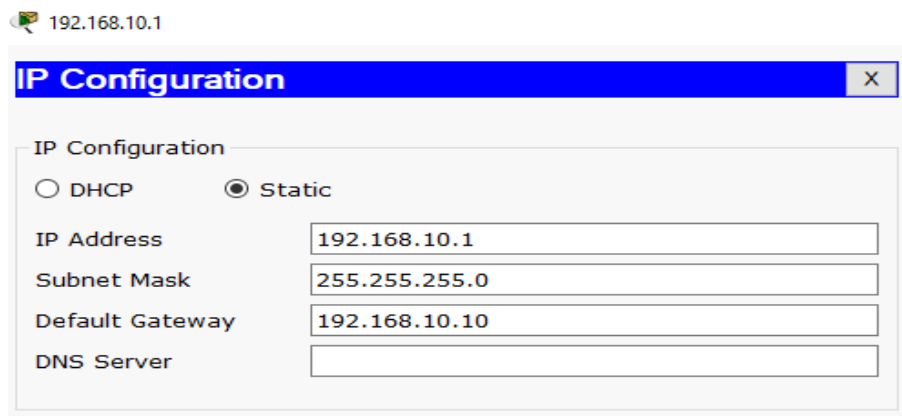
Dynamic routing uses multiple algorithms and protocols. The most popular are Routing Information Protocol (RIP) and Open Shortest Path First (OSPF).

### Procedure:

**Step 1:** Connect the networks as shown in the figure.



**Step 2:** Configure the networks of all end-devices and Configure the interfaces on R1, R2 and R3 routers with the IP addresses.



**Step 3:** Configure Routers 1 and 2 in CLI so that they can send messages between each other.

#### IOS Command Line Interface

```
Router(config-if)#exit
Router(config)#interface Serial2/0
Router(config-if)#ip address 192.168.60.2 255.255.255.0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface Serial2/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state to up

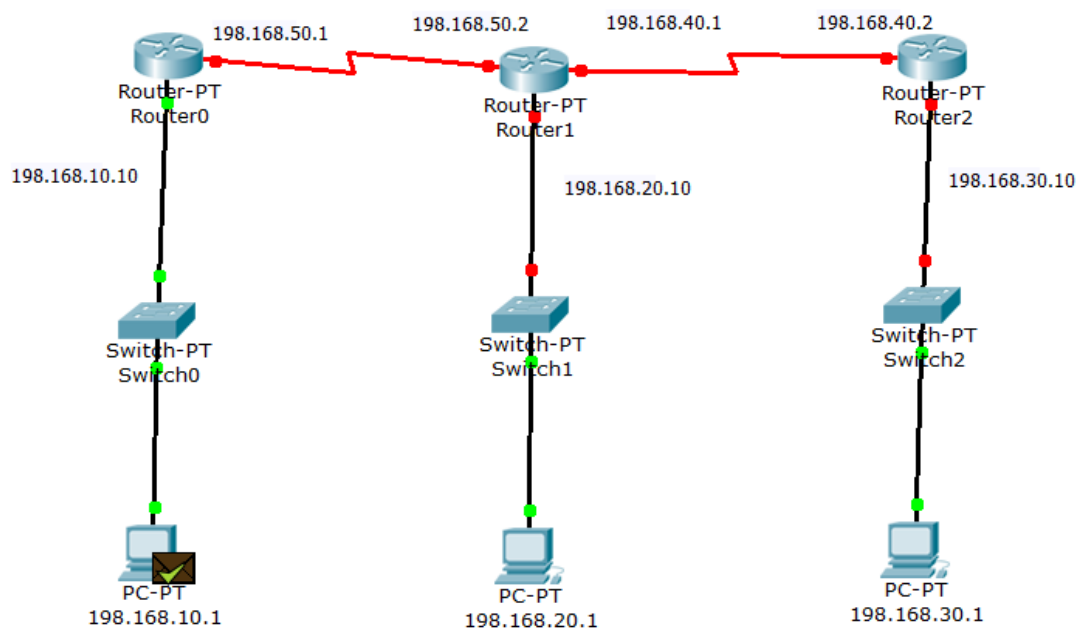
Router(config-if)#exit
Router(config)#interface Serial3/0
Router(config-if)#ip address 192.168.70.1 255.255.255.0
Router(config-if)#clock rate 2000000
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface Serial3/0, changed state to down
Router(config-if)#
%LINK-5-CHANGED: Interface Serial3/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial3/0, changed state to up

Router(config-if)#exit
Router(config)#router rip
Router(config-router)#network 192.168.20.0
Router(config-router)#
```

**Step 4:** Check the network status by sending an ICMP packet.



**Result:** Successfully performed static routing in routers.

## Experiment No. 9

**AIM:-**Use and Observe various Troubleshooting commands in Routing.

**Theory:-** Some commands used in Troubleshooting routing.

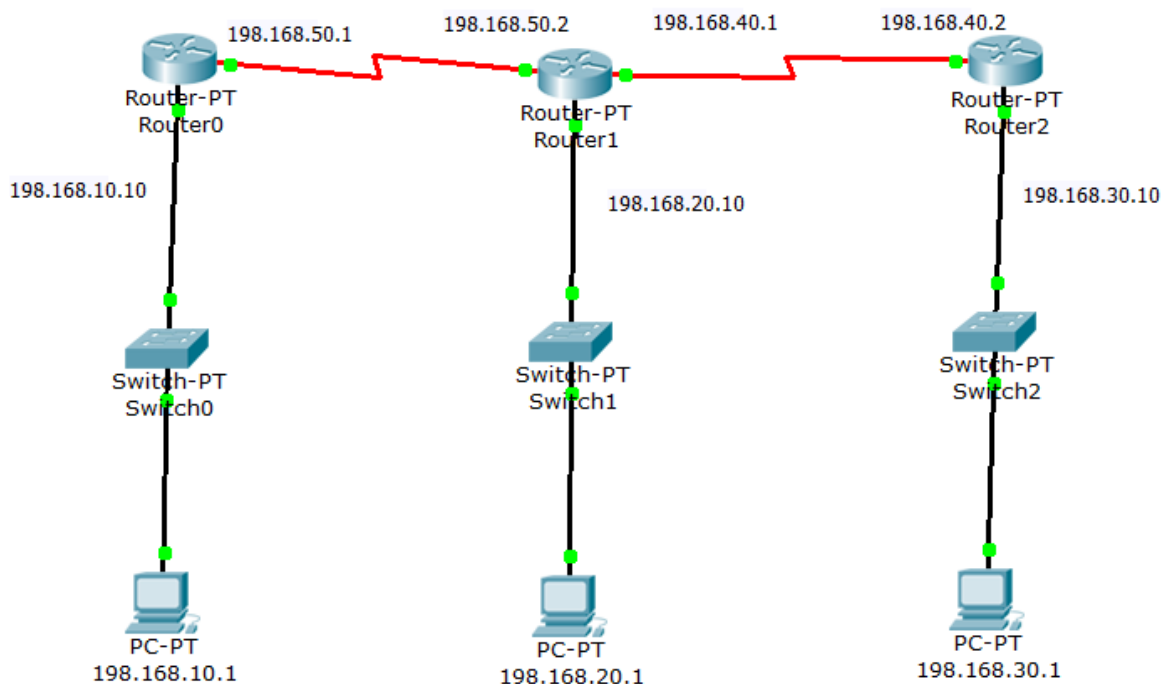
**Show IP route:-**Use the show ip route command to find detailed information regarding the routes configured on the router.

**Show IP interface:-**The show ip interface command will provide details regarding layer 3 configuration on the interfaces. Using this command you can see the IP address and mask configured on a given interface, whether an access list is applied on the interface as well as basic

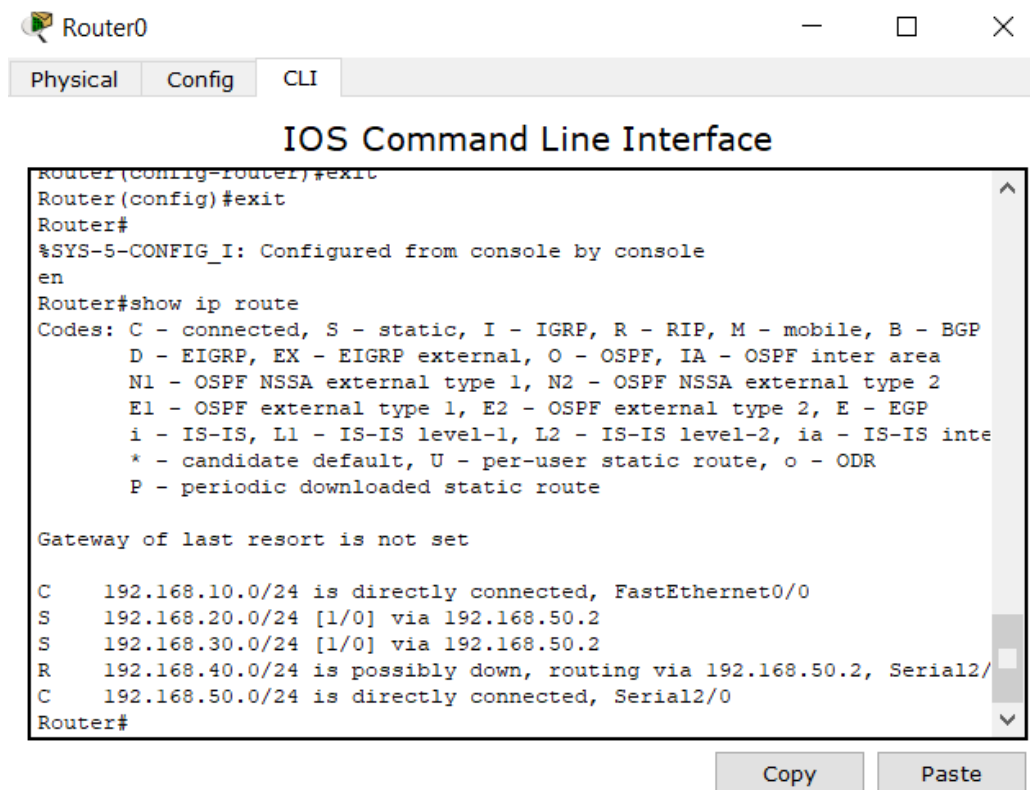
**Trace route:-** The trace route command traces the end-to-end path a packet takes though an internetwork. Similarly with PING, it uses the ICMP protocol with TTL timeouts to perform its operation.

### Procedure:

**Step 1:-**Set up a network as shown in Fig.



**Step 2:-**Type show ip route command in Router0.



The screenshot shows the Router0 CLI window with the 'CLI' tab selected. The title bar reads 'Router0'. Below the tabs, the text 'IOS Command Line Interface' is displayed. The command prompt is 'Router(config)#exit', followed by 'Router#'. The command '%SYS-5-CONFIG\_I: Configured from console by console' is shown, followed by 'en'. The command 'Router#show ip route' is entered, and the output is displayed. The output lists the routing table contents, including codes for various protocols and a list of routes. The routes are: C 192.168.10.0/24 is directly connected, FastEthernet0/0; S 192.168.20.0/24 [1/0] via 192.168.50.2; S 192.168.30.0/24 [1/0] via 192.168.50.2; R 192.168.40.0/24 is possibly down, routing via 192.168.50.2, Serial2/0; C 192.168.50.0/24 is directly connected, Serial2/0. The command prompt is 'Router#'. Below the output, there are 'Copy' and 'Paste' buttons.

```

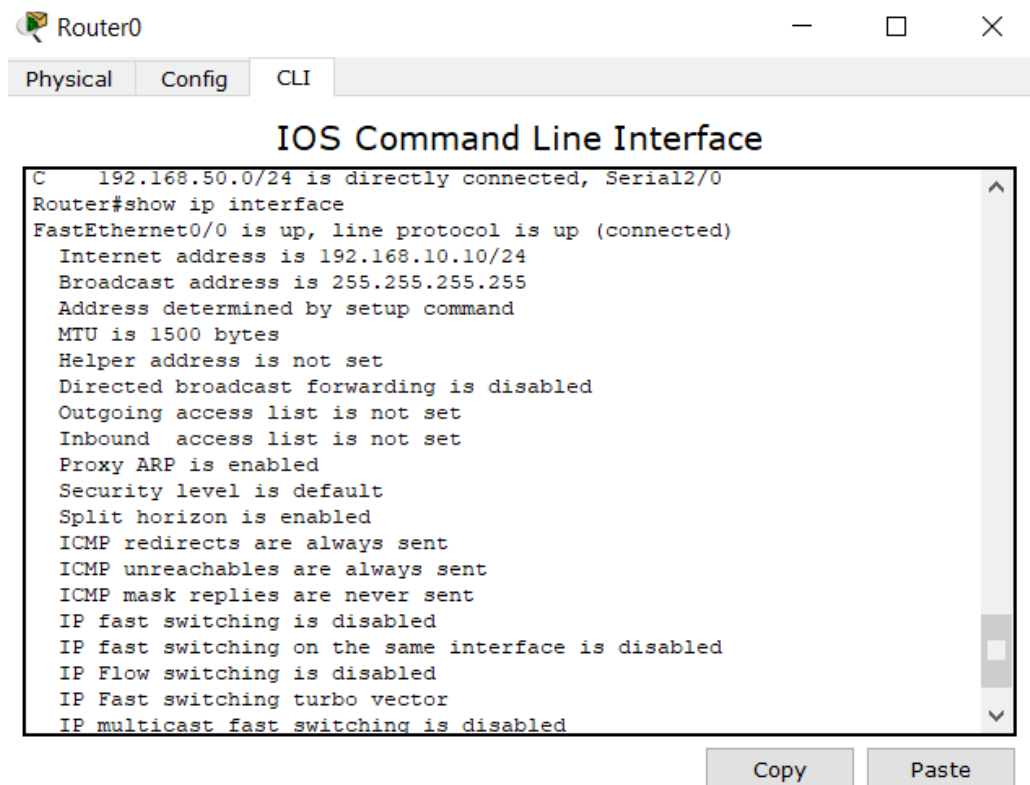
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
en
Router#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.10.0/24 is directly connected, FastEthernet0/0
S    192.168.20.0/24 [1/0] via 192.168.50.2
S    192.168.30.0/24 [1/0] via 192.168.50.2
R    192.168.40.0/24 is possibly down, routing via 192.168.50.2, Serial2/0
C    192.168.50.0/24 is directly connected, Serial2/0
Router#

```

**Step 3:-**Type show ip interface command in Router0.



The screenshot shows the Router0 CLI window with the 'CLI' tab selected. The title bar reads 'Router0'. Below the tabs, the text 'IOS Command Line Interface' is displayed. The command prompt is 'Router#show ip interface', and the output is displayed. The output shows the status of the FastEthernet0/0 interface, including its IP address, broadcast address, MTU, and various protocol settings. The command prompt is 'Router#'. Below the output, there are 'Copy' and 'Paste' buttons.

```

C    192.168.50.0/24 is directly connected, Serial2/0
Router#show ip interface
FastEthernet0/0 is up, line protocol is up (connected)
  Internet address is 192.168.10.10/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound access list is not set
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is disabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP Fast switching turbo vector
  IP multicast fast switching is disabled

```

**Result:-** Successfully performed troubleshooting.

## Experiment No. 10

**AIM: Setup a simple Virtual Lan Network.**

**Theory:-**

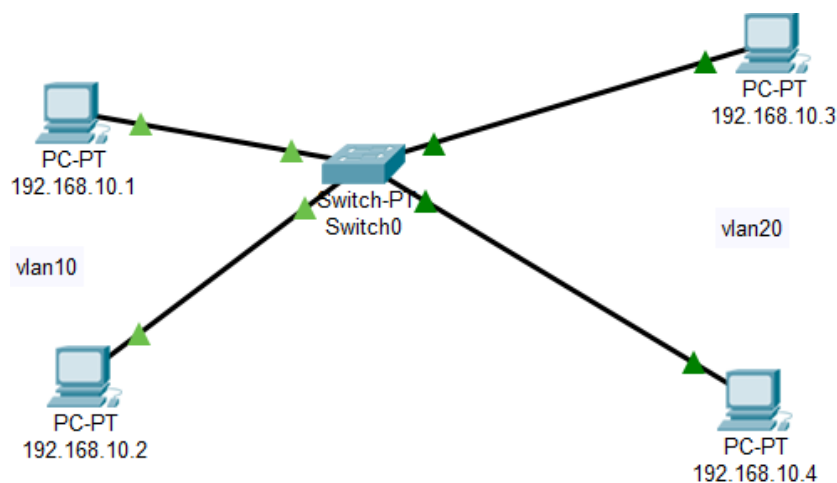
Virtual LANs(VLANs)are used to break up broadcast domains in a Layer 2 switched internetwork. As VLANs promote efficient use of network resources.

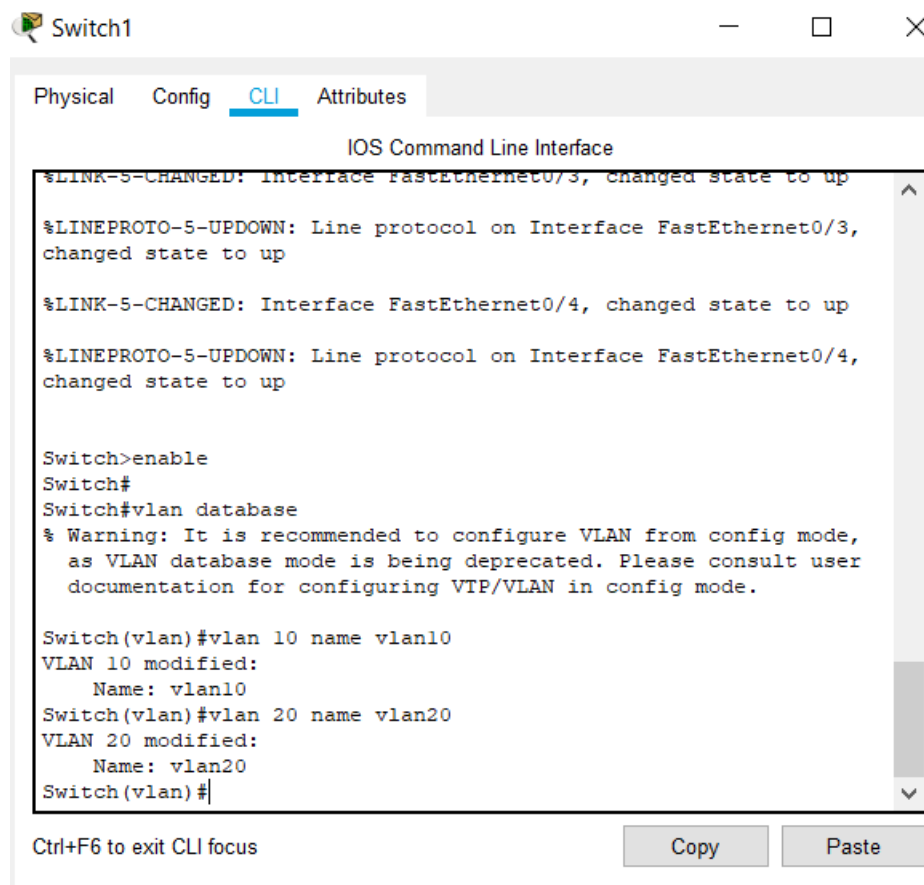
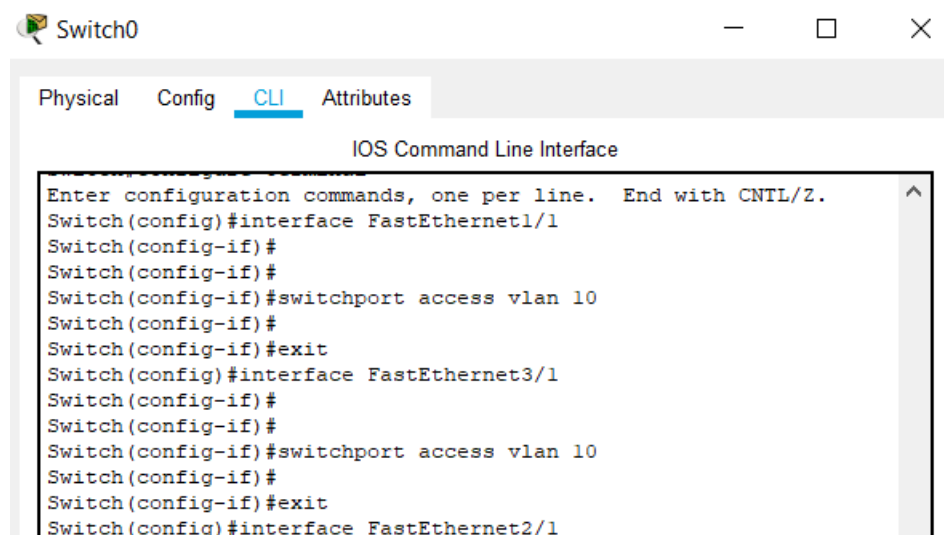
Virtual LAN (VLAN) is a concept in which we can divide the devices logically on layer 2 (data link layer). Generally, layer 3 devices divides broadcast domain but broadcast domain can be divided by switches using the concept of VLAN.

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

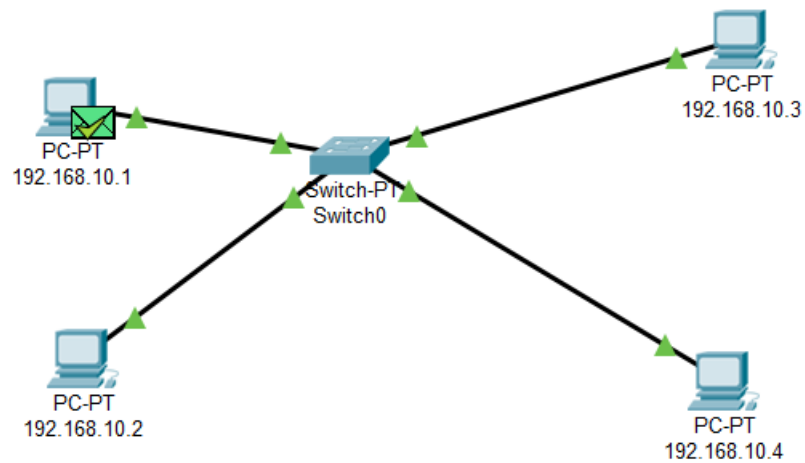
**Procedure:**

**Step 1:-** Connect the networks as shown in the figure.



**Step 2:-**Create two VLANs vlan10 and vlan20**Step 3:-**Add 192.168.10.1 , 192.168.10.2 to VLAN 10 and 192.168.10.3 , 192.168.10.4 to VLAN 20.

**Step4:-** Check the network status by sending an ICMP packet.



**Result:-**

The message was successfully sent from one device to another in same VLAN but not in another VLAN.



## Experiment No. 11

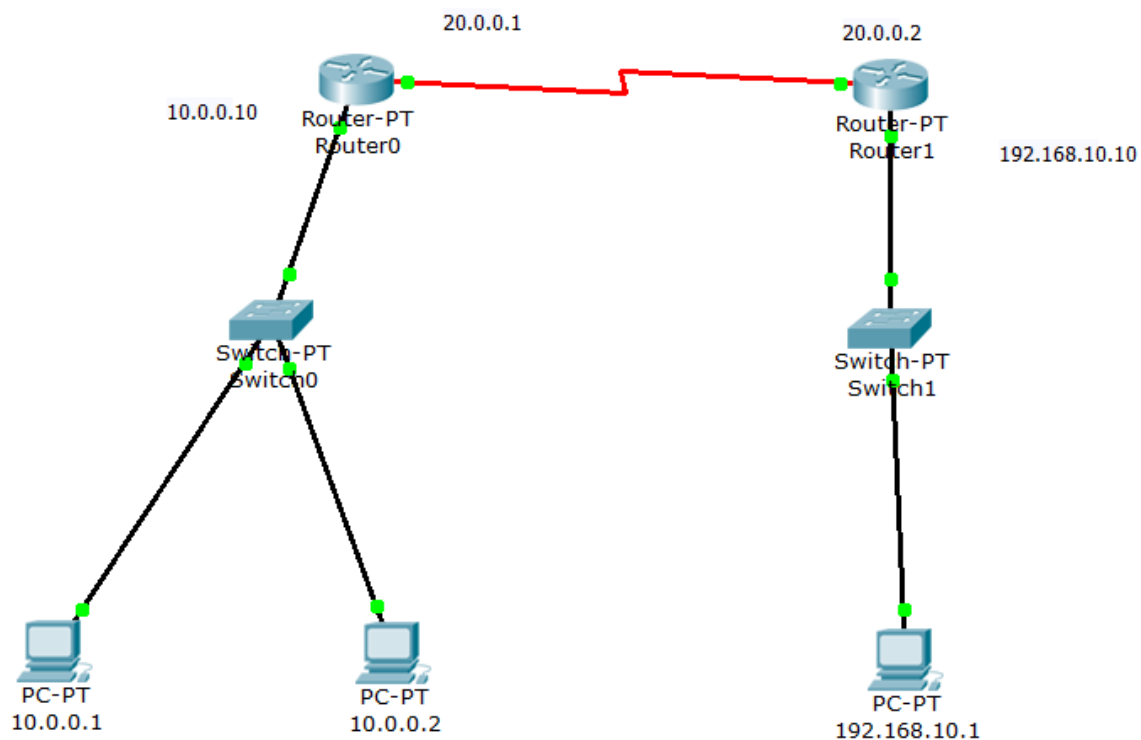
**Aim -Configure Static Network Address Translation (NAT) in Cisco Packet Tracer.**

**Theory: -**

Static NAT is used to do a one-to-one mapping between an inside address and an outside address. Static NAT also allows connections from an outside host to an inside host. Usually, static NAT is used for servers inside your network. For example, you may have a web server with the inside IP address 192.168.0.10 and you want it to be accessible when a remote host makes a request to 209.165.200.10. For this to work, you must do a static NAT mapping between those two IPs.

**Procedure: -**

**Step 1: -** Connect routers as shown in the figure, with the appropriate switch devices and end-devices.



**Step 2:** -Open the Command line Interface of both the routers and also run the following commands as shown below.

Router0

Physical Config CLI

### IOS Command Line Interface

```

Router(config-if)#
%LINK-5-CHANGED: Interface Serial2/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state

Router(config-if)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
en
Router#en
Router#config
Configuring from terminal, memory, or network [terminal]? terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip nat inside source static 10.0.0.1 40.0.0.1
Router(config)#inter fa0/0
Router(config-if)#ip nat inside
Router(config-if)#interface serial2/0
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#ip route 0.0.0.0 0.0.0.0 20.0.0.2
Router(config)#

```

Copy Paste

Router1

Physical Config CLI

### IOS Command Line Interface

```

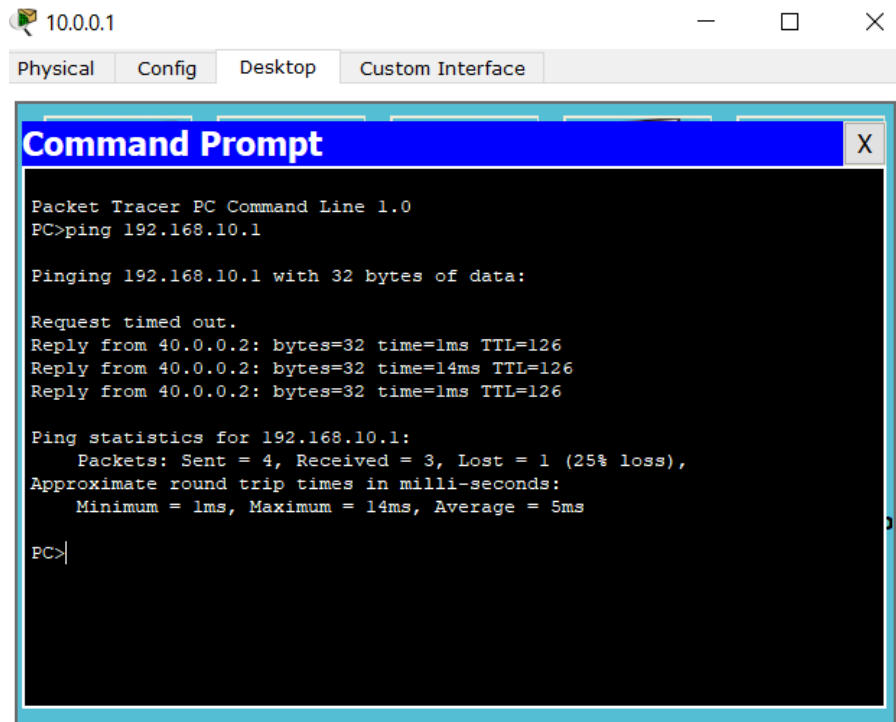
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed
o up
ip address 192.168.10.10 255.255.255.0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface Serial2/0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface Serial2/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0, changed state
ip address 20.0.0.2 255.0.0.0
Router(config-if)#exit
Router(config)#ip nat inside source static 192.168.10.1 40.0.0.2
Router(config)#inter fa0/0
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#inter serial2/0
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#ip route 0.0.0.0 0.0.0.0 20.0.0.1
Router(config)#

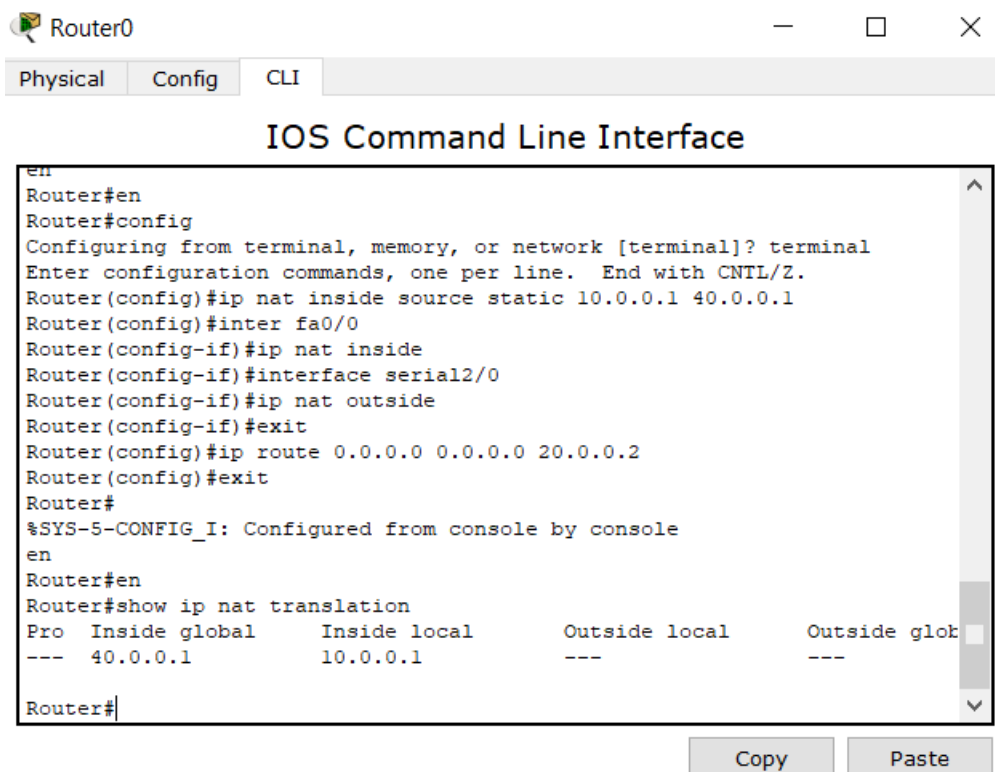
```

Copy Paste

**Step 3-** Check the connections via putting commands on the PC of inside area on command prompt As shown below.



**Step 4:** In router0 type the following command to view the NAT translation table.



**RESULT-** Static NAT configured successfully.

## Experiment No. 12

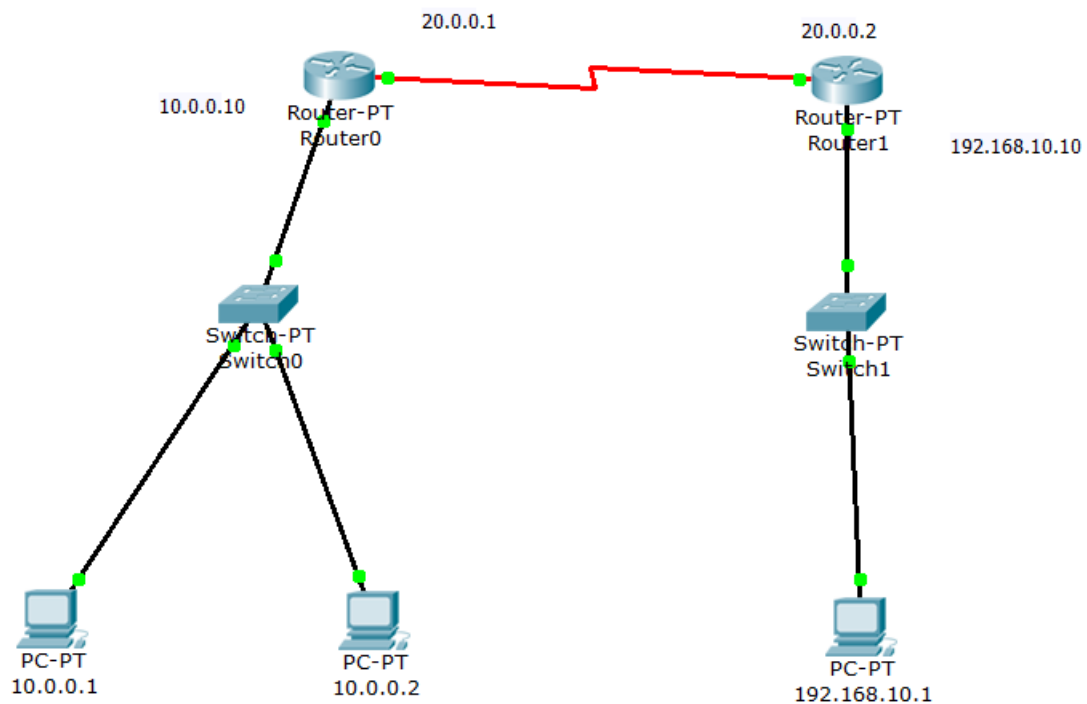
**Aim-** Configure Dynamic Network Address Translation (NAT) in cisco packet tracer.

### Theory:-

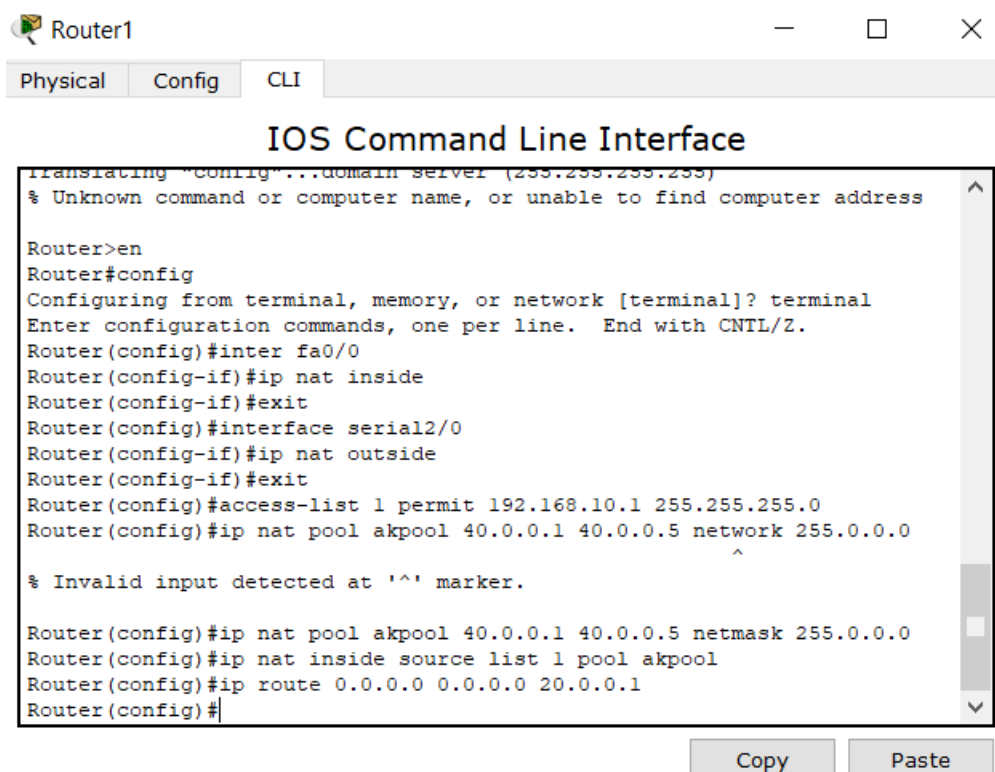
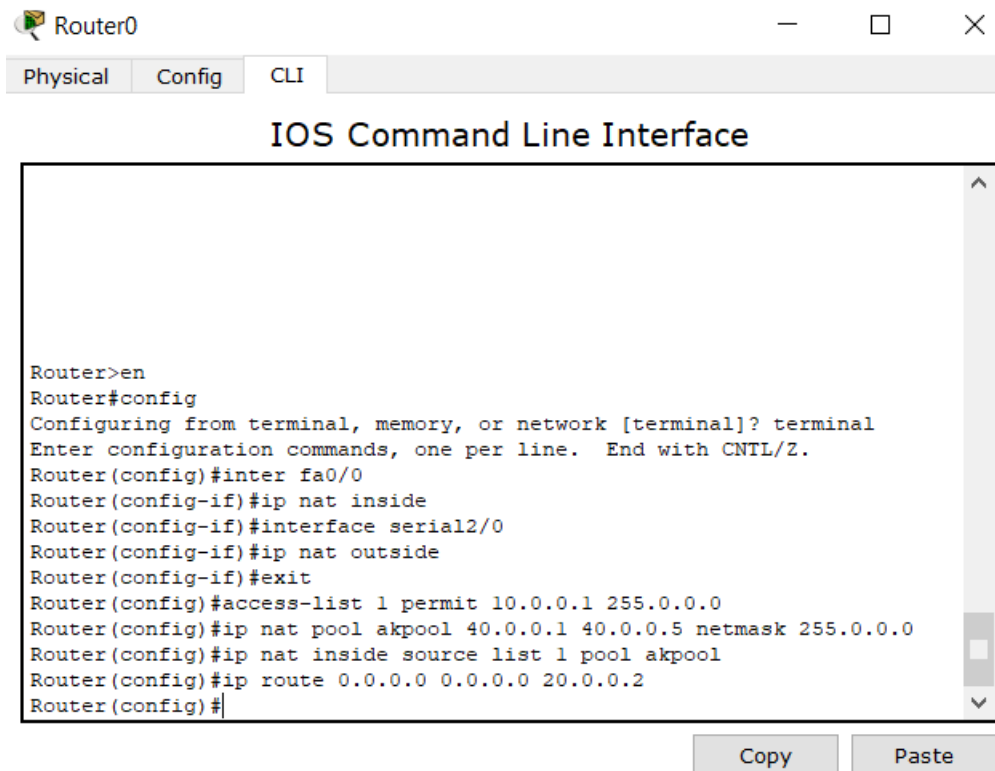
Dynamic network address translation (Dynamic NAT) is a technique in which multiple public Internet Protocol (IP) addresses are mapped and used with an internal or private IP address. It allows a user to connect a local computer, server or networking device to an external network or Internet group with an unregistered private IP address that has a group of available public IP addresses.

### Procedure: -

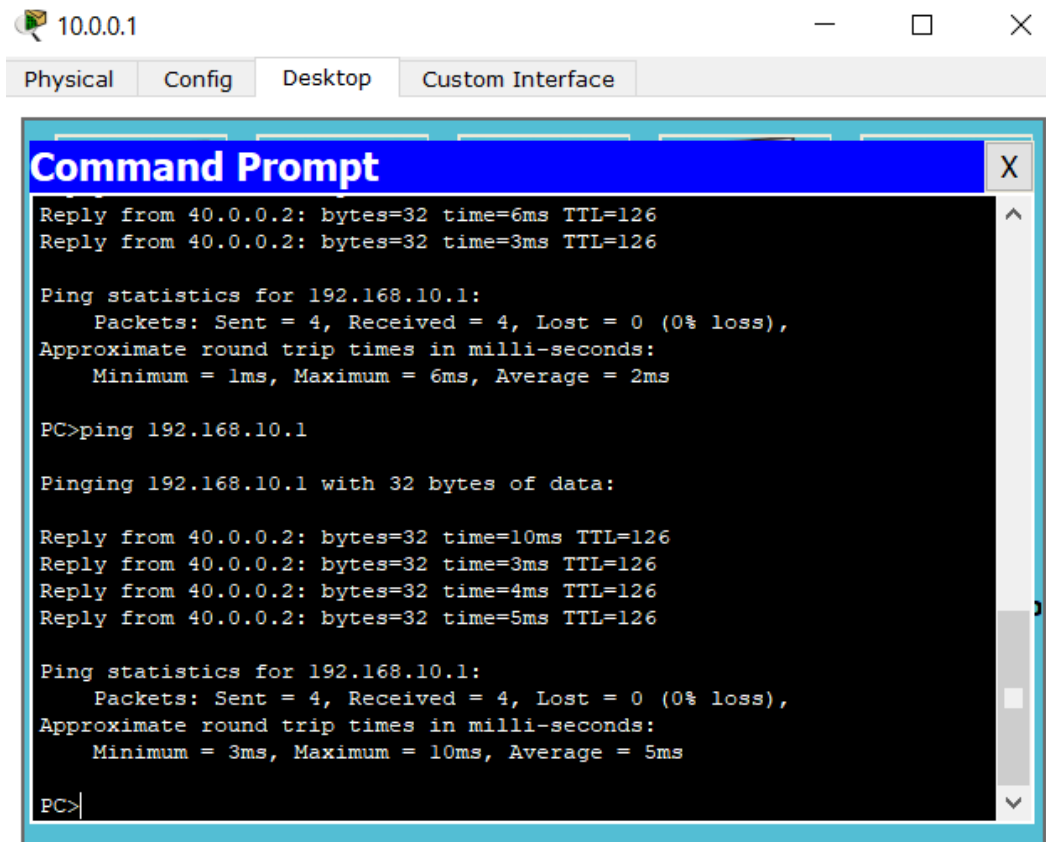
**Step 1:** Connect routers as shown in the figure, with the appropriate switch devices and end-devices.



**Step 2:** -Open the Command line Interface and run following commands on both routers.



**Step 3:** - Configure the Dynamic LAN via using these commands in inner PCs command prompt.



**RESULT:** -Dynamic NAT configured successfully.

## Experiment No. 13

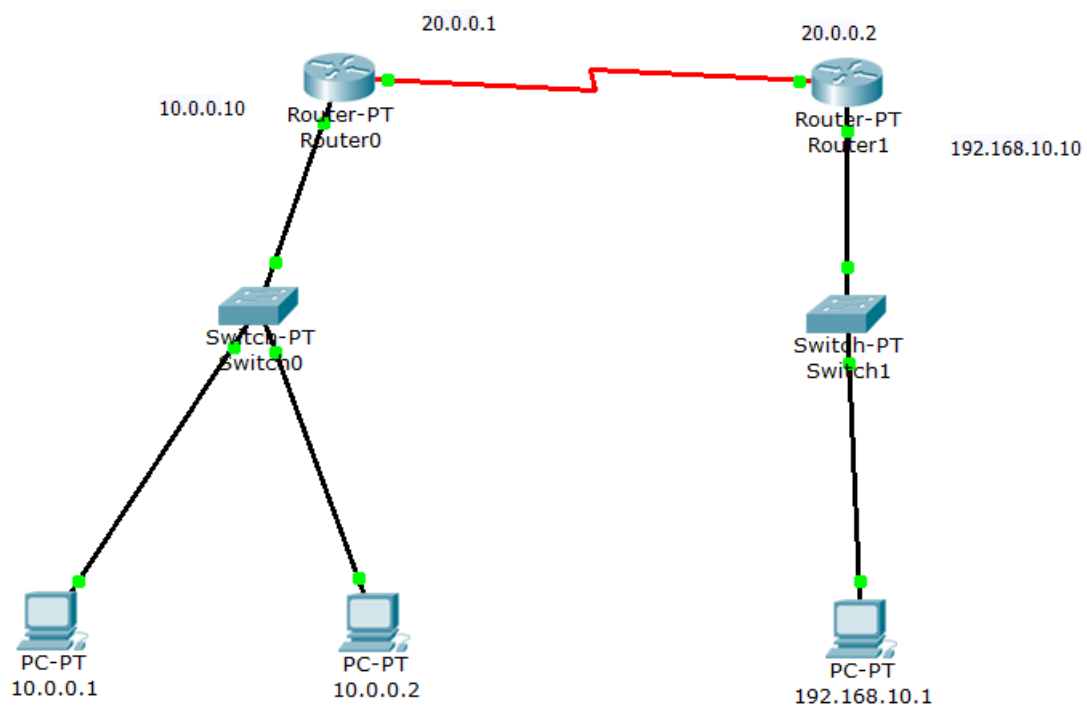
**Aim :** Configure Port Address Translation (PAT) in Cisco Packet Tracer.

### Theory :

Port Address Translation (PAT), is an extension to network address translation (NAT) that permits multiple devices on a local area network (LAN) to be mapped to a single public IP address. The goal of PAT is to conserve IP addresses.

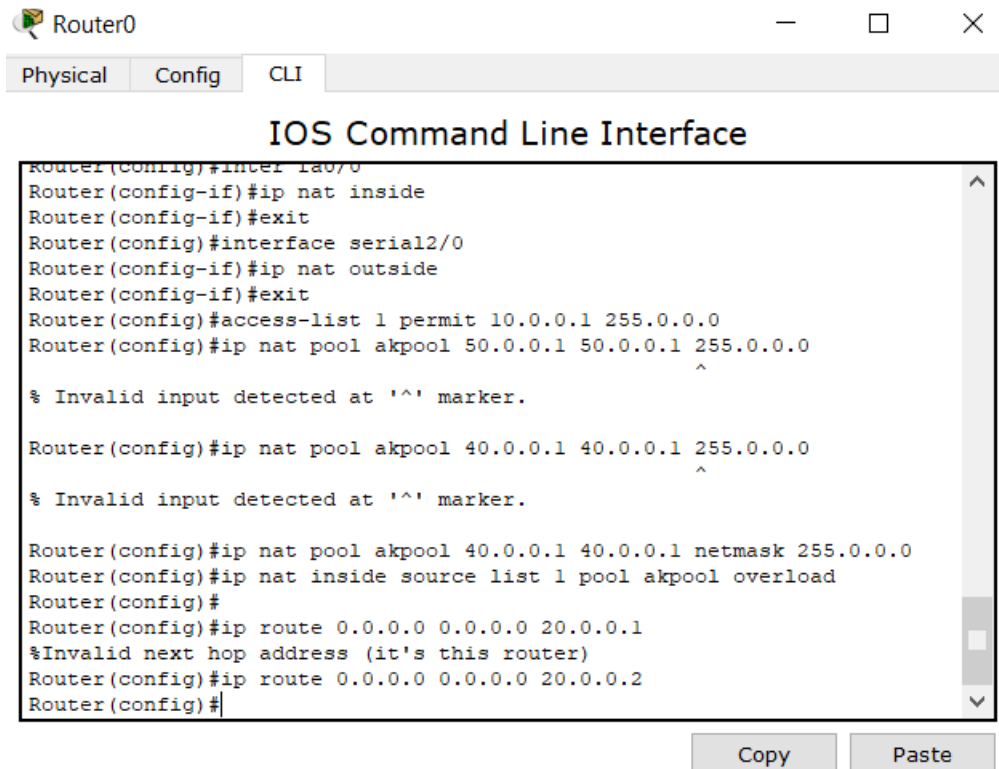
### Procedure: -

**Step 1: -** Connect routers as shown in the figure, with the appropriate switch devices and end-devices.



**Step 2: -**Open the Command line Interface and run following commands on both routers.





Router0

Physical Config CLI

### IOS Command Line Interface

```

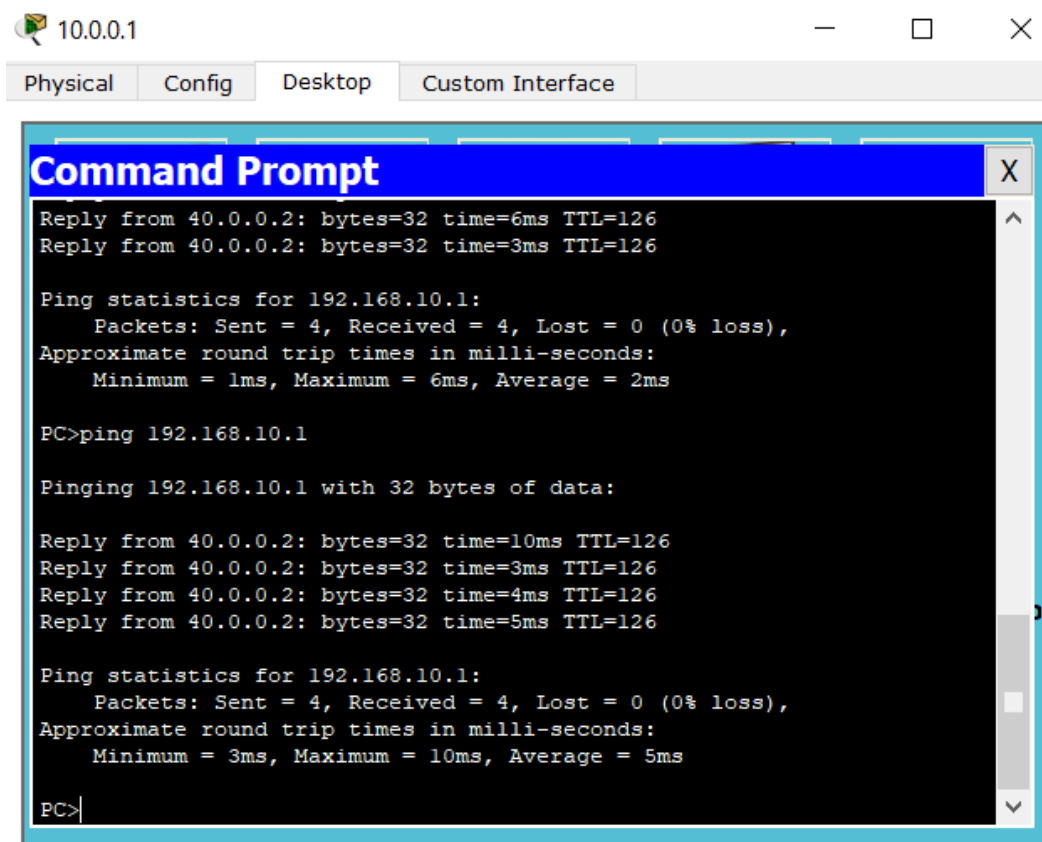
Router(config)#inter fa0/0
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#interface serial2/0
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#access-list 1 permit 10.0.0.1 255.0.0.0
Router(config)#ip nat pool akpool 50.0.0.1 50.0.0.1 255.0.0.0
                                     ^
% Invalid input detected at '^' marker.

Router(config)#ip nat pool akpool 40.0.0.1 40.0.0.1 255.0.0.0
                                     ^
% Invalid input detected at '^' marker.

Router(config)#ip nat pool akpool 40.0.0.1 40.0.0.1 netmask 255.0.0.0
Router(config)#ip nat inside source list 1 pool akpool overload
Router(config)#
Router(config)#ip route 0.0.0.0 0.0.0.0 20.0.0.1
%Invalid next hop address (it's this router)
Router(config)#ip route 0.0.0.0 0.0.0.0 20.0.0.2
Router(config)#
  
```

Copy Paste

**Step 3:** - Configure the Dynamic LAN via using these commands in inner PCs command prompt.



10.0.0.1

Physical Config Desktop Custom Interface

### Command Prompt

```

Reply from 40.0.0.2: bytes=32 time=6ms TTL=126
Reply from 40.0.0.2: bytes=32 time=3ms TTL=126

Ping statistics for 192.168.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 6ms, Average = 2ms

PC>ping 192.168.10.1

Pinging 192.168.10.1 with 32 bytes of data:

Reply from 40.0.0.2: bytes=32 time=10ms TTL=126
Reply from 40.0.0.2: bytes=32 time=3ms TTL=126
Reply from 40.0.0.2: bytes=32 time=4ms TTL=126
Reply from 40.0.0.2: bytes=32 time=5ms TTL=126

Ping statistics for 192.168.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 10ms, Average = 5ms

PC>
  
```

**Result:** Successfully performed Port Address Translation(PAT).