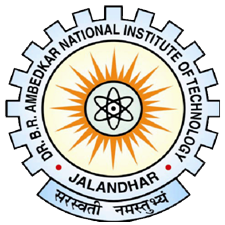
**COMPUTER NETWORK LAB**

**CSX-321**

LAB PRACTICALS RECORD

COMPUTER SCIENCE AND ENGINEERING



Department of Computer Science and Engineering

Dr B.R. Ambedkar National Institute of Technology

Jalandhar, Punjab, India

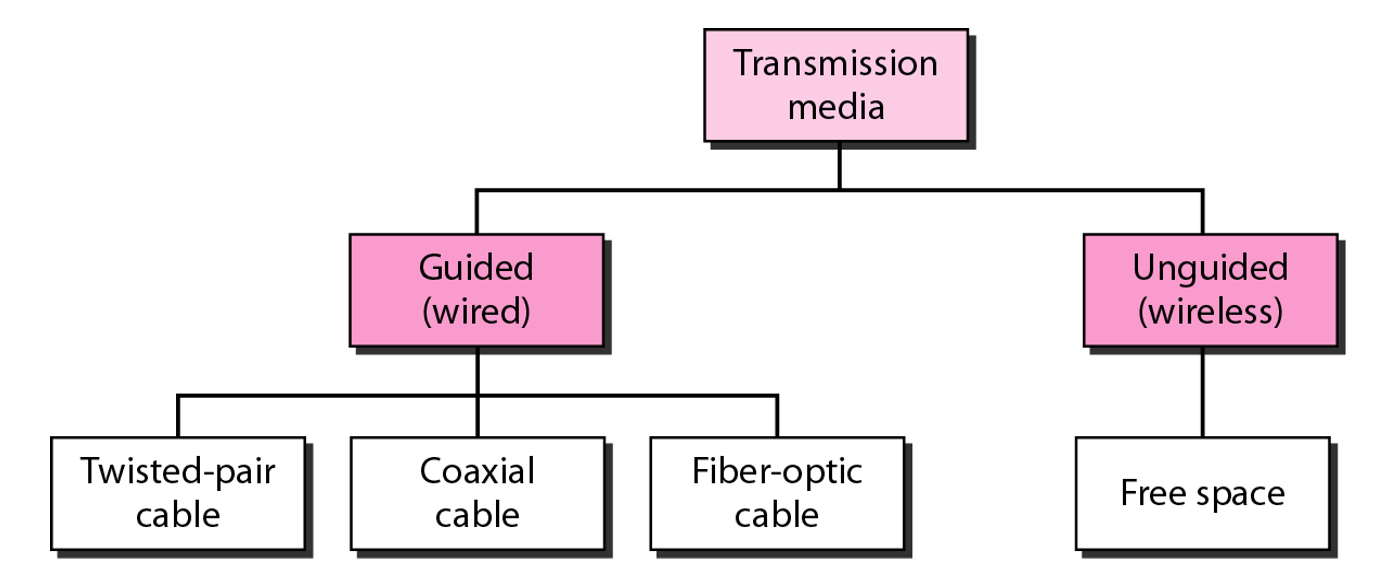
# List of Experiments

|  |  |  |
| --- | --- | --- |
| S. No. | Objectives | Page No. |
| 1 | Physical introduction to different Cables, Connectors, and tools. | 1-5 |
| 2 | Design a LAN cable and set up a LAN connection between two computers then share information between them (Hands on). | 6-10 |
| 3 | Connect and transferring data between two computers using cisco packet tracer simulation environment similar as hands on. Apply pinging command Also. | 11-12 |
| 4 | Implement various network topologies like Star, Bus, Ring, Mesh and Hybrid and share data between different network devices Using Cisco Packet Tracer. | 13-15 |
| 5 | Connect two different networks through a Router. | 16-17 |
| 6 | Implement Default Routing to connect multiple different networks and share data between different network devices Using Cisco Packet Tracer. | 18-19 |
| 7 | Implement Static Routing to connect multiple different networks and share data between different network devices Using Cisco Packet Tracer. | 20-21 |
| 8 | Implement Dynamic Routing to connect multiple different networks and share data between different network devices Using Cisco Packet Tracer. | 22-23 |
| 9 | Troubleshooting in Default, Static, and Dynamic Routing by connecting multiple networks. | 24-26 |
| 10 | Implementation of VLAN | 27-29 |
| 11 | Configure Static Network Address Translation (NAT) in Cisco Packet Tracer. | 30-32 |
| 12 | Configure Dynamic Network Address Translation (NAT) in Cisco Packet Tracer. | 33-34 |
| 13 | Configure Port Address Translation (PAT) in Cisco Packet Tracer. | 35-36 |

EXPERIMENT 1

# AIM : Physical introduction to different Cables, Connectors, and tools.

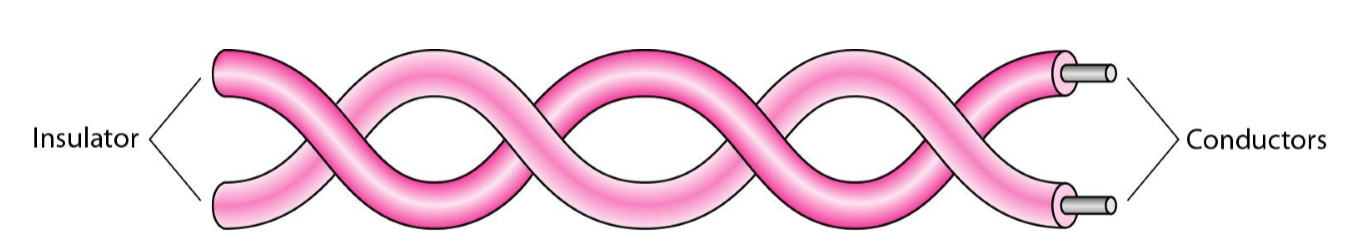
**CABLES**



### Fig 1.1 Different types of transmission media

Cable is the medium through which information usually moves from one network device to another.

# TWISTED PAIR CABLE



### Fig 1.2 Twisted pair cable

* A twisted pair consist of two conductors (normally copper), each with its own plastic insulation and twisted together.
* One of the wires is used to carry signals to the receiver, and the other is used only as a ground reference. The receiver uses the difference between the two.
* Twisted pair cabling comes in two varieties: shielded and unshielded.
* Compared to a [single conductor](https://en.wikipedia.org/wiki/Single-ended_signaling) or an untwisted [balanced pair](https://en.wikipedia.org/wiki/Balanced_pair), a twisted pair reduces [electromagnetic radiation](https://en.wikipedia.org/wiki/Electromagnetic_radiation) from the pair and [crosstalk](https://en.wikipedia.org/wiki/Crosstalk) between neighbouring pairs and improves rejection of external [electromagnetic interference](https://en.wikipedia.org/wiki/Electromagnetic_interference). It was invented by [Alexander Graham Bell](https://en.wikipedia.org/wiki/Alexander_Graham_Bell).

# UTP (UNSHIELDED TWISTED PAIR) CABLE

* The quality of UTP may vary from telephone-grade wire to extremely high-speed cable.
* Each pair is twisted with a different number of twists per inch to help eliminate interference from adjacent pairs and other electrical devices. The tighter the twisting, the higher the supported transmission rate and the greater the cost per foot.
* Although UTP cable is the least expensive cable, it may be susceptible to radio and electrical frequency interference (it should not be too close to electric motors, fluorescent lights, etc.).
* Unshielded twisted pair (UTP) cables are found in many [Ethernet](https://en.wikipedia.org/wiki/Ethernet) networks and telephone systems.

# Types of UTP cables

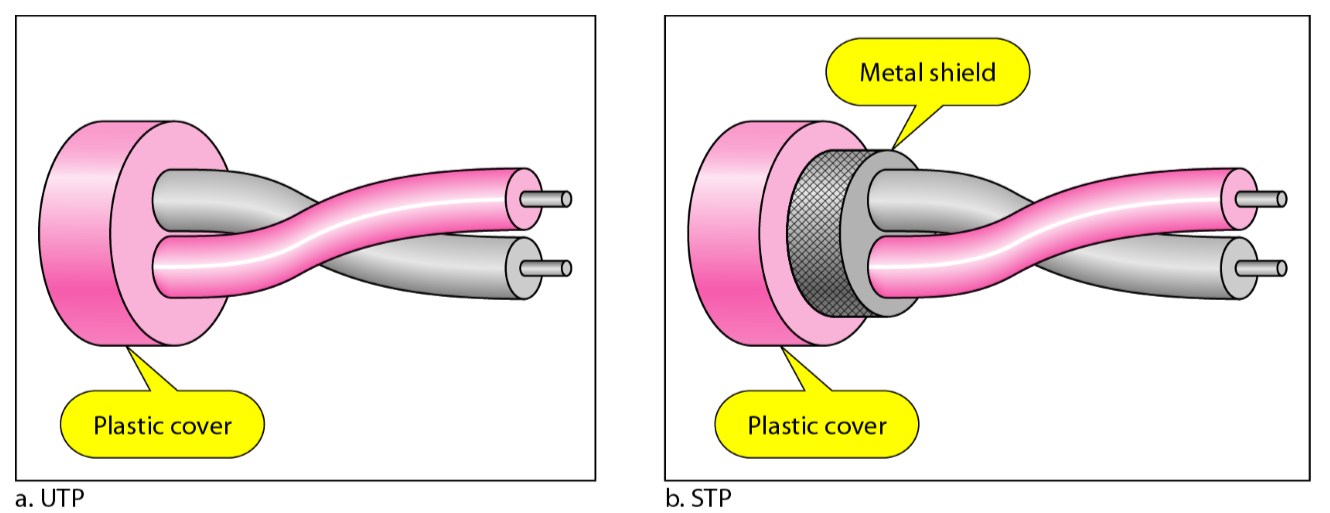
The [five categories of UTP](https://searchdatacenter.techtarget.com/definition/Categories-of-twisted-pair-cabling-systems) cable are :

* CAT3: Rarely used today, CAT3 is usually deployed in phone lines. It supports 10 [Mbps](https://searchnetworking.techtarget.com/definition/Mbps) for up to 100 meters.
* CAT4: Typically used in token ring networks, CAT4 supports 16 Mbps for up to 100 meters.
* CAT5: Used in Ethernet-based LANs, CAT5 contains two twisted pairs. It supports 100 Mbps for up to 100 meters.
* CAT5e: Used in Ethernet-based LANs, CAT5e contains four twisted pairs. It supports 1 [Gbps](https://whatis.techtarget.com/definition/Gbps-billions-of-bits-per-second) for 100 meters.
* CAT6: Used in Ethernet-based LANs and data center networks, CAT6 contains four tightly wound twisted pairs. It supports 1 Gbps for up to 100 meters and 10 Gbps for up to 50 meters.

The most common connector used with UTP cable is an [RJ-45](https://searchnetworking.techtarget.com/definition/telephone-jacks).

# STP (SHIELDED TWISTED PAIR) CABLE

* Shielded cables can help to extend the maximum distance of the cables.
* STP cabling includes metal shielding over each individual pair of copper wires. This type of shielding protects cable from external EMI (electromagnetic interferences).
* STP cable is more expensive and difficult to install, compared with UTP.



### Fig 1.3 Types of STP

# COAXIAL CABLES

* Coaxial cable is an electrical cable consisting of a round conducting wire, surrounded by an insulating spacer, surrounded by a cylindrical conducting sheath, and usually surrounded by a final insulating layer.
* Most common use of coax (the short form of coaxial cable) today is in standard cable TV.
* A PVC plastic jacket encases the covering The cable is designed to carry a high-frequency or broadband signal, as a high-frequency transmission line. Because the electromagnetic field carrying the signal exists (ideally) only in the space between the inner and outer conductors, it cannot interfere with or suffer interference from external electromagnetic fields.

# THICKNET, OR RG-8

is older and one of the first types of coaxial cable used in networks. RG-8 is strung in a physical bus topology. Its thick shielding makes it fairly immune to noise but also very rigid and difficult to work with.

# THINNET OR RG-58

cable is far more flexible than ThickNet and much easier to work with. RG-58 cabling is also strung as a physical bus. It is capable of connecting a maximum of 30 devices on up to a 185-meter length of cable.

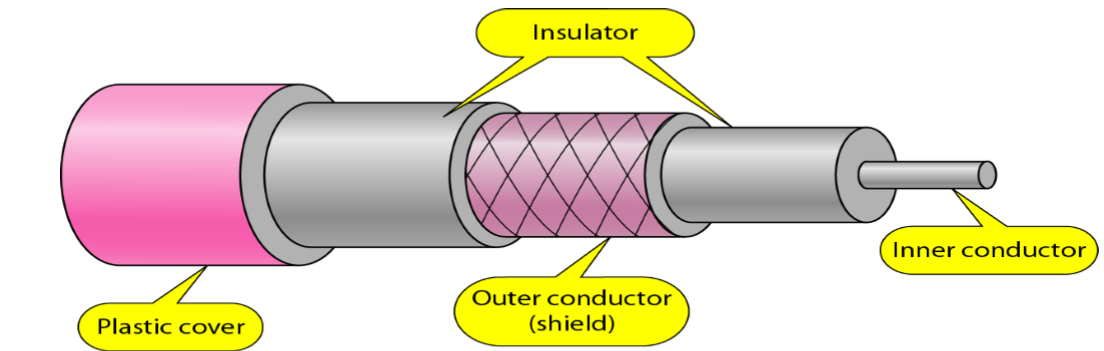
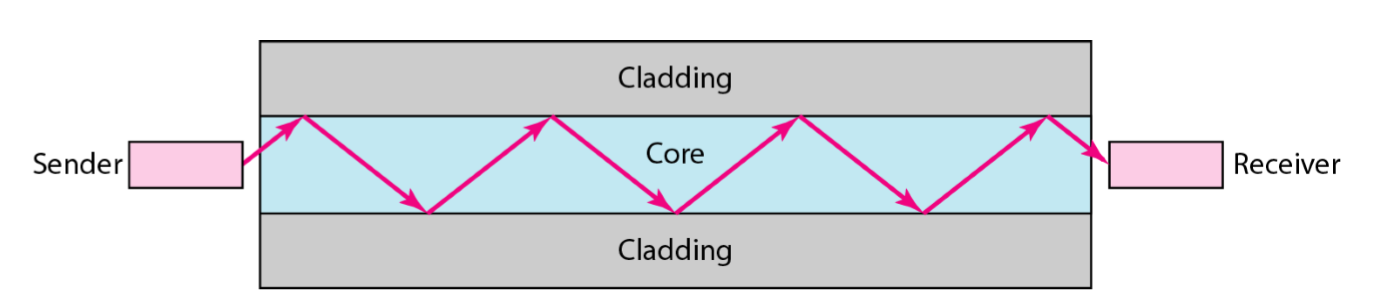


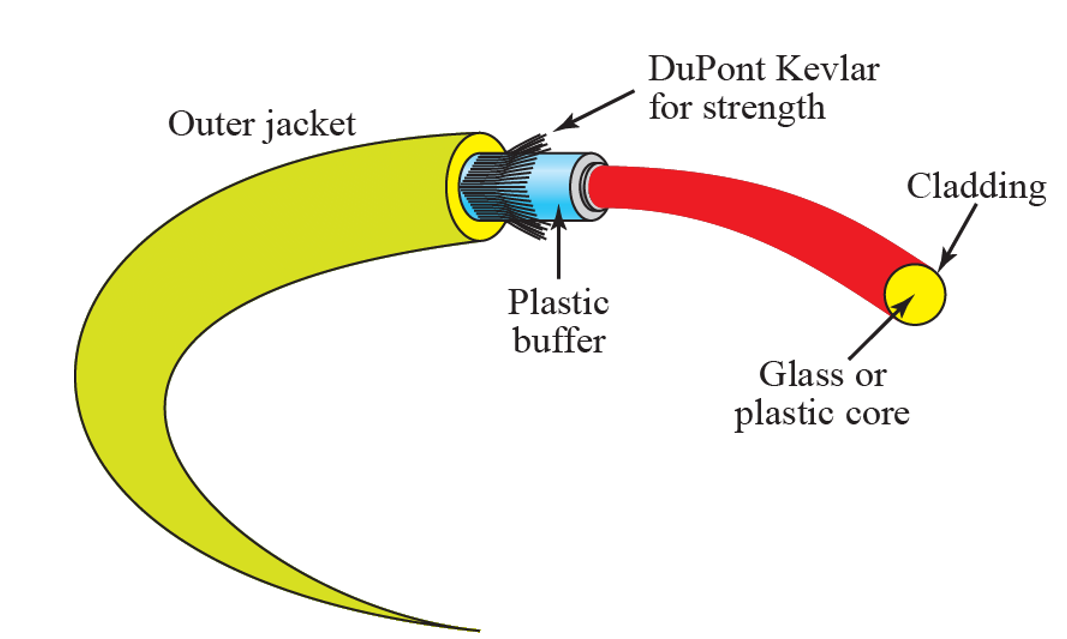
Fig: coaxial cable

### Fig 1.4

# FIBER OPTIC CABLE

* Fiber optic cabling consists of a center glass core surrounded by several layers of protective materials.
* It transmits light rather than electronic signals eliminating the problem of electrical interference. This makes it ideal for certain environments that contain a large amount of electrical interference. It has also made it the standard for connecting networks between buildings, due to its immunity to the effects of moisture and lighting.
* Fiber optic cable has the ability to transmit signals over much longer distances than coaxial and twisted pair. It also has the capability to carry information at vastly greater speeds. This capacity broadens communication possibilities to include services such as video conferencing and interactive services.
* The center core of fiber cables is made from glass or plastic fibers . A plastic coating then cushions the fiber center, and kevlar fibers help to strengthen the cables and prevent breakage. The outer insulating jacket made of teflon or PVC.
* There are two common types of fiber cables -- single mode and multimode. Multimode cable has a larger diameter; however, both cables provide high bandwidth at high speeds. Single mode can provide more distance, but it is more expensive.
* Optical fiber based communication is based on the phenomenon of total internal reflection

 *Fig 1.5 Transmission in Fibre Optic Cable*

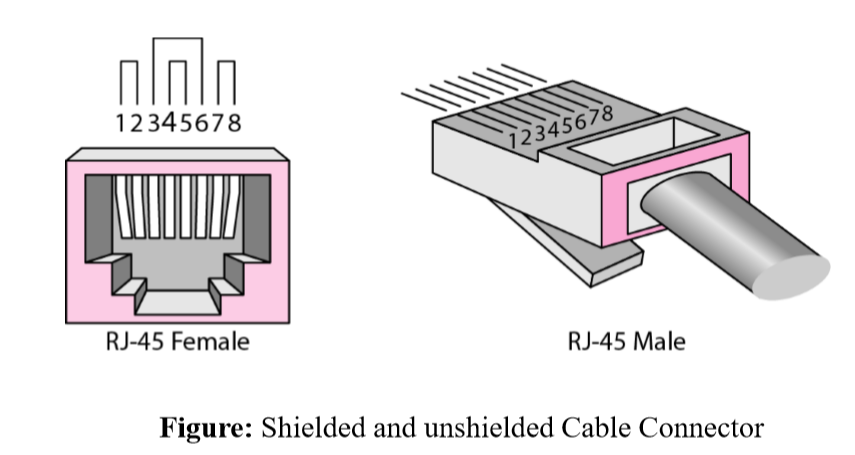


### Fig 1.6 Fibre Optic Cable

# CONNECTORS

# Unshielded Twisted Pair Connector

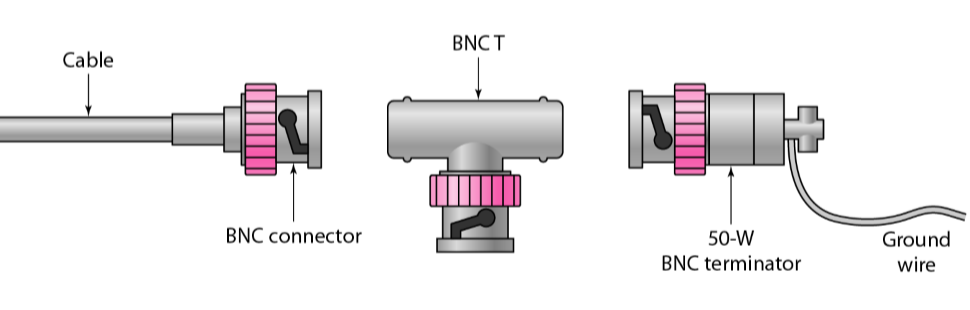
* The most common type of connector for Ethernet installations is referred to as an**"RJ-45" connector.** It is officially known as an 8P8C connector
* This is a plastic connector that looks like a large telephone-style connector.
* RJ stands for Registered Jack, implying that the connector follows a standard borrowed from the telephone industry. This standard designates which wire goes with each pin inside the connector.
* Categories 3 through 6 all use the RJ-45 connector, but Cat 7 utilizes a specialized version of the RJ-45 called the GigaGate45 (GG45), which grounds the cable and allows for higher data transmission rates.



### Fig 1.7

# Coaxial Cable Connectors

The most common type of connector used with coaxial cables is the Bayone-Neill-Concelman (BNC) connector . Different types of adapters are available for BNC connectors, including a T-connector, barrel connector, and terminator.



### *Fig 1.8 Coaxial Cable Connectors(BNC*)

# 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](https://www.computerhope.com/jargon/r/rj45.htm) and [RJ-11](https://www.computerhope.com/jargon/r/rj11.htm) connectors to the both ends of either phone or [Cat 5](https://www.computerhope.com/jargon/c/cat5.htm) cable.

# SWITCH

A switch, however, keeps a record of the MAC addresses of all the devices connected to it. With this information, a switch can identify which system is sitting on which port. So when a frame is received, it knows exactly which port to send it to, without significantly increasing network response times. And, unlike a hub, a 10/100Mbps switch will allocate a  full 10/100Mbps to each of its ports. So regardless of the number of PCs transmitting, users will always have access to the maximum amount of bandwidth.

# HUB

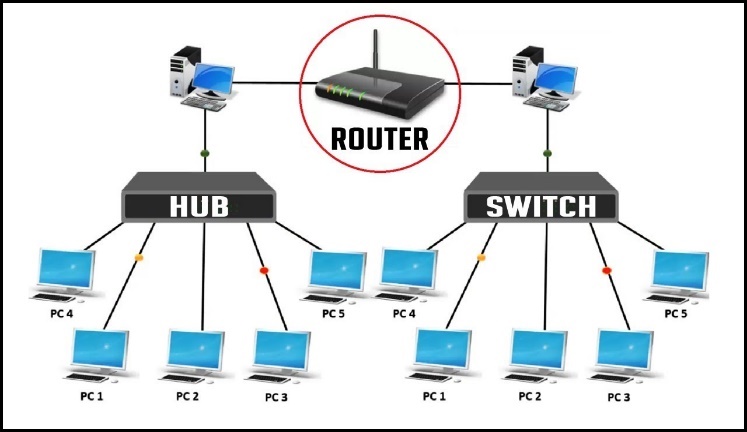
In a hub, a frame is passed along or "broadcast" to every one of its ports. It doesn't matter that the frame is only destined for one port. The hub has no way of distinguishing which port a frame should be sent to. Passing it along to every port ensures that it will reach its intended destination. This places a lot of traffic on the network and can lead to poor network response times. Additionally, a 10/100Mbps hub must share its bandwidth with each and every one of its ports. So when only one PC is broadcasting, it will have access to the maximum available bandwidth. If, however, multiple PCs are broadcasting, then that bandwidth will need to be divided among all of those systems, which will degrade performance.

# ROUTER

Routers are completely different devices. Where a hub or switch is concerned with transmitting frames, a router's job, as its name implies, is to route packets to other networks until that packet ultimately reaches its destination. One of the key features of a packet is that it not only contains data, but the destination address of where it's going. A router is typically connected to at least two networks, commonly two Local Area Networks (LANs) or Wide Area Networks (WAN) or a LAN and its ISP's network . for example, your PC or workgroup and EarthLink. Routers are located at gateways, the places where two or more networks connect. Using headers and forwarding tables, routers determine the best path for forwarding the packets. Router use protocols such as ICMP to communicate with each other and configure the best route between any two hosts.

Routers are also the only one of these devices that will allow you to share a single IP address among multiple network clients.

So, in short, a hub glues together an Ethernet network segment, a switch can connect multiple Ethernet segments more efficiently and a router can do those functions plus route TCP/IP packets between multiple LANs and/or WANs; and much more of course.



### *Fig1.9 Crimping Tool* *Fig 1.10 Hub vs Switch*

EXPERIMENT 2

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

# APPARATUS REQUIRED

* Ethernet Cable CAT5
* 2 RJ-45 connector
* Crimping Tool (This your all-in-one networking tool – specially shaped for pushing down the pins in the plug and able to strip the shielding off cables, as well as cut).

# ETHERNET CABLING

Ethernet cabling has been standard in networking installation for years. It’s the fastest way of connecting PCs together — to your router, or a central switch.

* The most common form of network cable is called **“unshielded twisted pair” (UTP).**
* The distinction between a straight through, crossover, and rollover cable comes down to the way that the connectors on each end are wired.
* A UTP cable contains eight wires.

In the twisted pair configuration, the eight wires within the cable are split up into four pairs. The two wires in a pair are twisted around each other. This treatment protects both wires from interference. The pairing is easy to spot because one of the two is encased in a coating of solid color while the other is white with a spiral stripe in the pair’s color. This pair’s colors are: Green, Orange, Blue, Brown.

# Cable connectors

The conventional name for the connectors on the ends of Ethernet cables is **RJ-45**. It is also known as “**8P8”**, which stands for “**eight positions, eight connectors**.”

 The UTP cable that is always used for Ethernet networks doesn’t need to contain eight wires. However, this is the convention. The blue pair and the brown pair don’t do anything.

The wires within the colored jackets are all identical. If you strip the casing of the blue-striped wire, it looks exactly the same as the orange solid wire when that is stripped.

The socket that the **RJ-45**fits into is soldered onto a network card. Every piece of equipment that can connect to a cabled network has to have a network card, which is also known as a **network interface controller, or NIC**.

Connector pin purposes

The important factor to remember when wiring **RJ-45**plugs is the function of each pin. The following list shows the purpose of each connector within the **8P8C**plug:

Pin 1: Transmit positive signal

Pin 2: Transmit negative signal

Pin 3: Receive positive signal

Pin 4: Nothing

Pin 5: Nothing

Pin 6: Receive negative signal

Pin 7: Nothing

Pin 8: Nothing

# Straight-Through Wired Cables

Straight-Through refers to cables that have the pin assignments on each end of the cable. In other words Pin 1 connector A goes to Pin 1 on connector B, Pin 2 to Pin 2 etc. Straight-Through wired cables are most commonly used to connect a host to client. When we talk about cat5e patch cables, the Straight-Through wired cat5e patch cable is used to connect computers, printers and other network client devices to the router switch or hub (the host device in this instance).

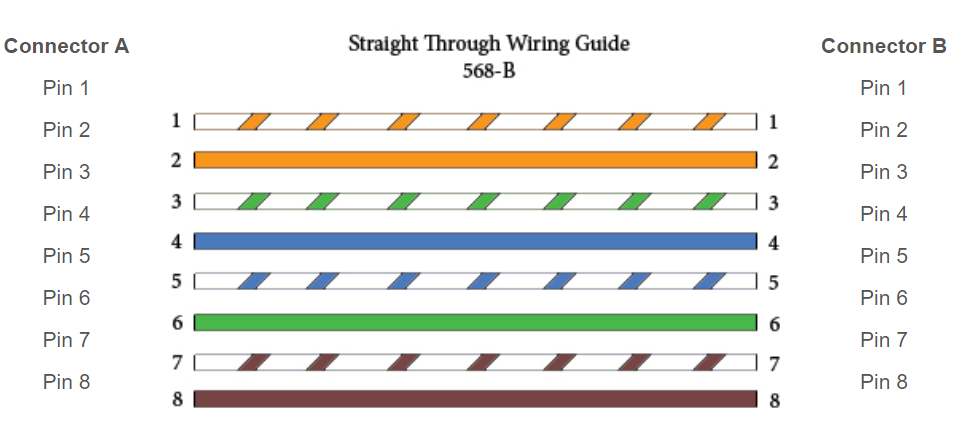


Fig 2.1 Straight through wire guide

# Crossover Wired Cables

Crossover wired cables (commonly called crossover cables) are very much like Straight-Through cables with the exception that TX and RX lines are crossed (they are at opposite positions on either end of the cable. Using the 568-B standard as an example below you will see that Pin 1 on connector A goes to Pin 3 on connector B. Pin 2 on connector A goes to Pin 6 on connector B etc. Crossover cables are most commonly used to connect two hosts directly. Examples would be connecting a computer directly to another computer, connecting a switch directly to another switch, or connecting a router to a router.

While in the past when connecting two host devices directly a crossover cable was required. Now days most devices have auto sensing technology that detects the cable and device and crosses pairs when needed.

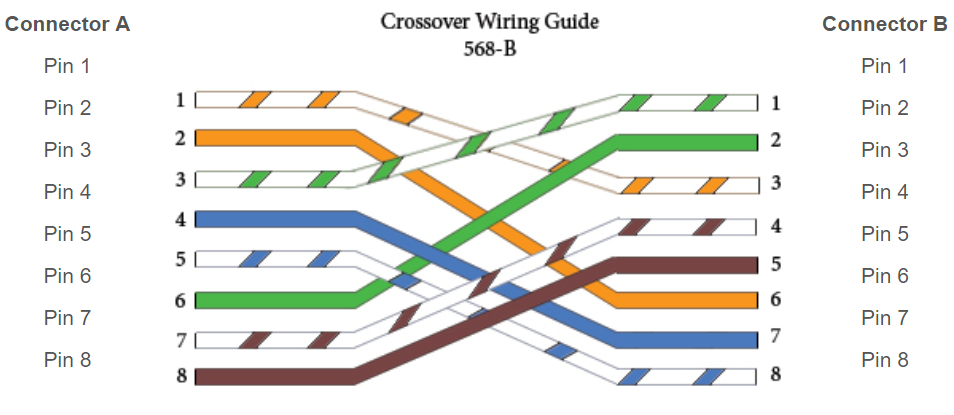


Fig 2.2 Cross wire guide

# Rollover Wired Cables

Rollover wired cables most commonly called rollover cables, have opposite Pin assignments on each end of the cable or in other words it is "rolled over". Pin 1 of connector A would be connected to Pin 8 of connector B. Pin 2 of connector A would be connected to Pin 7 of connector B and so on. Rollover cables, sometimes referred to as Host cables are most commonly used to connect to a devices console port to make programming changes to the device. Unlike crossover and straight-wired cables, rollover cables are not intended to carry data but instead create an interface with the device.

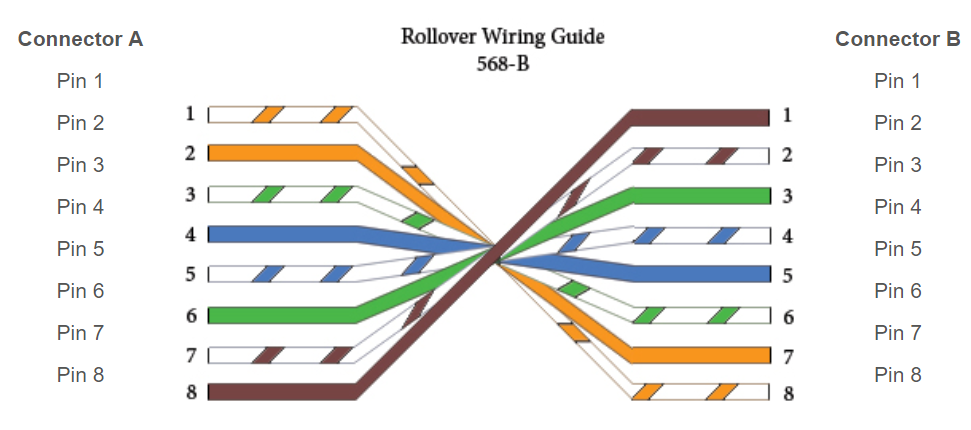
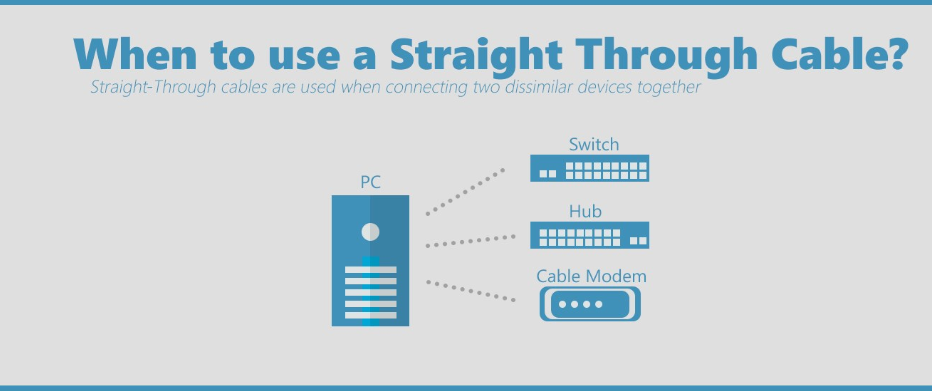


Fig 2.3 Rollover wire guide



### Fig 2.4 When to use Straight through wire

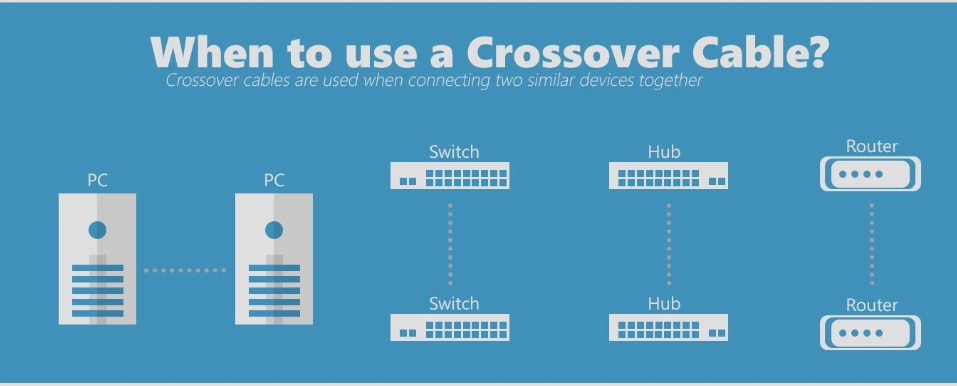


Fig 2.5 When to use Crossover cable

IMPORTANT POINTS:

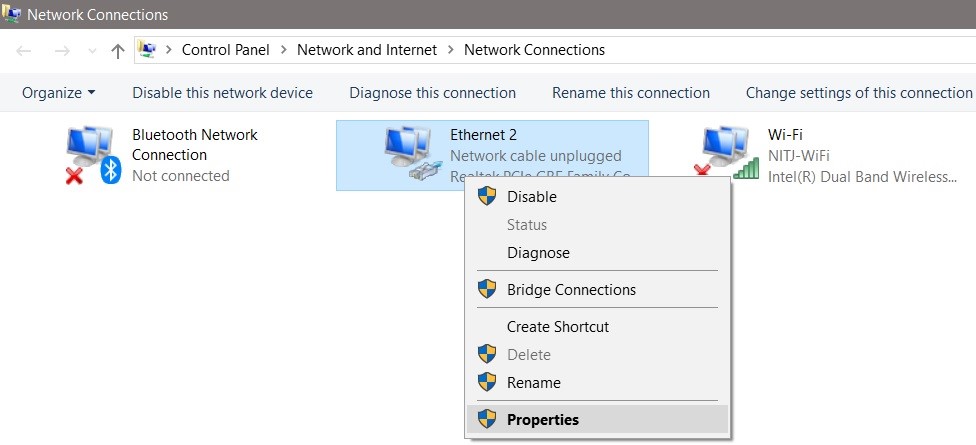
1. When the devices are same, then crossover cable is used.
2. When devices are different, Straight cable is used.So for router-to-router we need crossover cable.

# PROCEDURE

1. Strip about 1.5cm of cable shielding from both ends.
2. Untangle the wires (there should be 4 “twisted pairs”) and try to flatten the wires.
3. Arrange them in the order :white orange, orange, white green, blue, white blue, green, white brown, brown.
4. When you’ve got the order correct, bunch them together in a line. If you have some that stick up beyond the others, snip them back to a uniform level.
5. Hold the plug with the clip side facing **away** from you; the gold pins should be facing **towards** you. Push the cable right in — the notch at the end of the plug should just be over the cable shielding.
6. When the wires are sitting tightly in the plug, insert it into the crimping tool and push down. In theory the crimper is shaped to the exact right size.
7. Repeat for the other end.

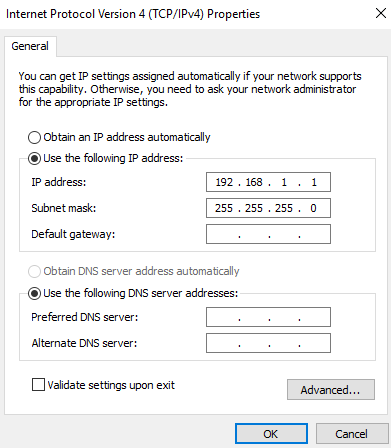
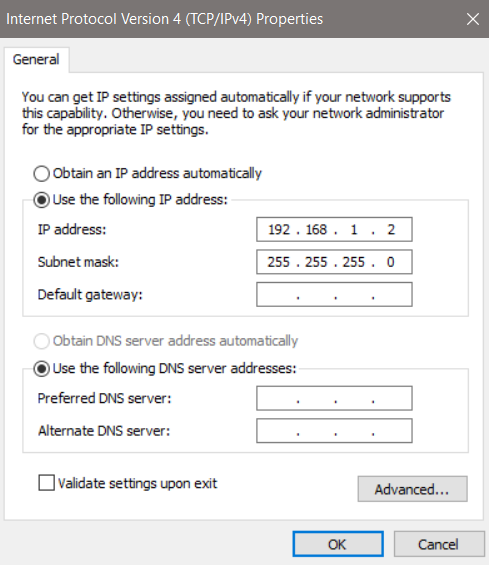
Setting Up LAN Connection

1. Connect the two ends of the cable to the LAN ports of the two computers to be connected.
2. Navigate to *Control Panel -> Network and Internet -> Network and Sharing Center-> Change Adaptor Settings*.
3. Select the appropriate connection for your LAN and right click on it and then select *Properties.* Local Area Connection Properties Window will appear.



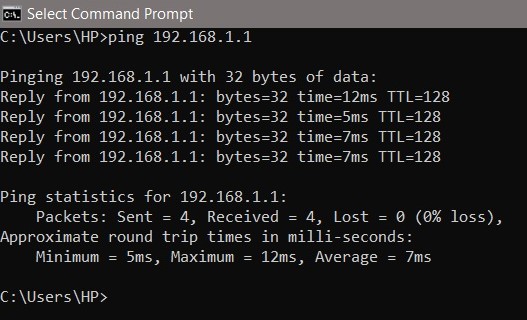
### Fig2.6 All Network Connections Available Shown

1. Select *Internet Protocol Version 4 (TCP/IPv4)* under the *Networking* tab and select *Properties*.
2. Set the IP addresses and Subnet Mask at the computers as shown in Fig.21 and Fig.21.

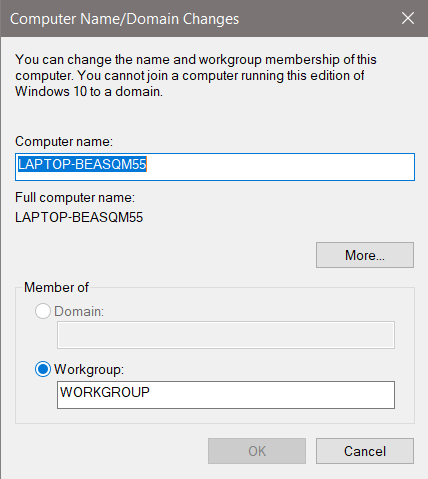
### Fig.2.7 Properties Window (Computer 1) Fig.2.8 Properties Window (Computer 2)

1. To check the connection, Restart both computers and use Ping Command on *Command Prompt* as shown in Fig.21.



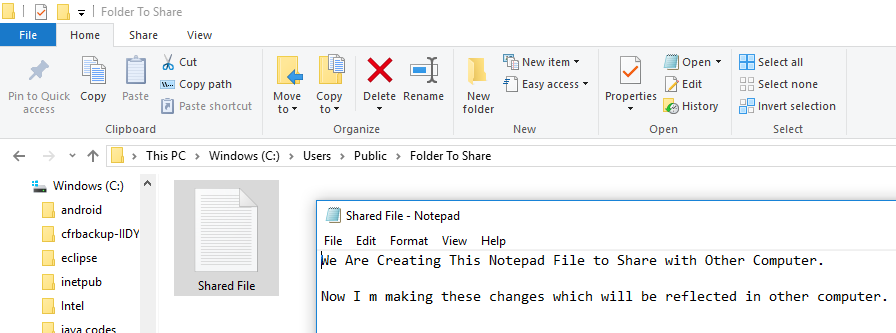
### Fig.2.9 Command Prompt (Computer 2) Fig.2.10 Command Prompt (Computer 2)

1. We need to check that the WORKGROUP on both the computers is same because otherwise the Ethernet Connection would not work. To check WORKGROUP, right click on *This PC* and select *Properties*. Click on *Change*.



### Fig2.11 Making Changes on Computer 2

1. Now we can share files between the computers. We can open other computer’s Users Folder in our computer. Just navigate to This PC >> Network.
2. We have created a folder named ‘Folder to Share’ in Public folder of Computer 1 from Computer 2.
3. Computer 1 can now see the same file in its system and make changes to it.



### Fig.2.12 Computer 1 making changes in the ‘Shared File’

1. The changes made by Computer 1 can be seen successfully received by Computer 2.
2. The Text File and Changes made in the Public Folder was shared Successfully and the changes were also reflected when made in one computer.

EXPERIMENT 3

# AIM: Connect and transferring data between two computers using cisco packet tracer simulation environment similar as hands on. Apply pinging command also.

# Cisco Packet Tracer

It is a [cross-platform](https://en.wikipedia.org/wiki/Cross-platform) visual [simulation](https://en.wikipedia.org/wiki/Simulation) tool designed by [Cisco Systems](https://en.wikipedia.org/wiki/Cisco_Systems) that allows users to create [network topologies](https://en.wikipedia.org/wiki/Network_topologies) and imitate modern [computer networks](https://en.wikipedia.org/wiki/Computer_networks). The software allows users to simulate the configuration of Cisco routers and switches using a simulated command line interface. Packet Tracer makes use of a [drag and drop](https://en.wikipedia.org/wiki/Drag_and_drop) user interface, allowing users to add and remove simulated network devices as they see fit. The software is mainly focused towards Certified Cisco Network Associate Academy students as an educational tool for helping them learn fundamental CCNA concepts.

# PROCEDURE

1. On CPT, drag 2 devices(PC’s).
2. Connect them by choosing the wire type. If we don’t know the type of wire needed, click on automatically choose connection type.
3. After connecting them establish a connection between them by configuring the IP of the devices
4. Click on device 1. And a dialog box will appear and click on Desktop and choose IP configuration box and fill the details as:

IP ADDRESS- 192.168.1.1

SUBNET MASK- 255.255.255.0

1. Click on device 2. And a dialog box will appear and click on Desktop and choose IP configuration box and fill the details as:

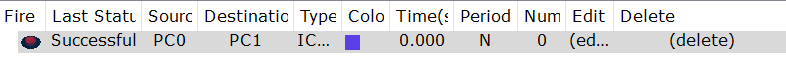
IP ADDRESS- 192.168.1.2

SUBNET MASK- 255.255.255.0

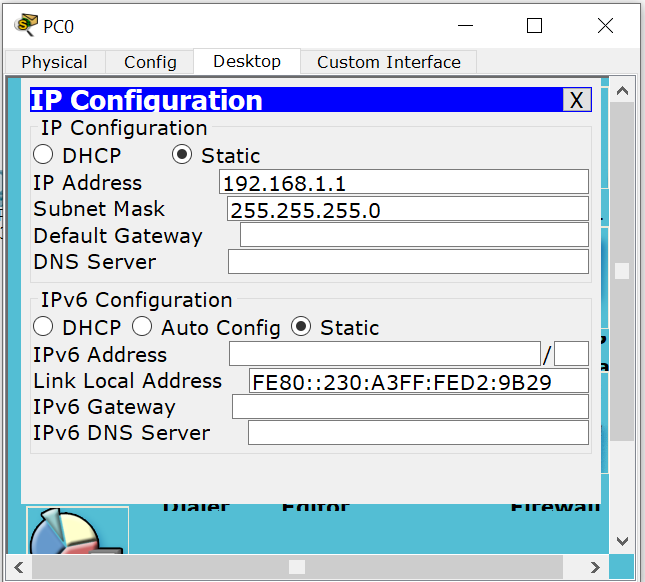
1. After establishing the connection, choose packet and drop it on device 1 and 2.
2. To verify whether connection has been established or not, click on device followed by Desktop and choose Command Prompt box and make use of ping command.
3. Click on Real Time Stimulation and then click on Auto Capture/Play.
4. View the packet transfer and acknowledgement.
5. Packet transfer is successful when Stimulation displays Successful.

### 

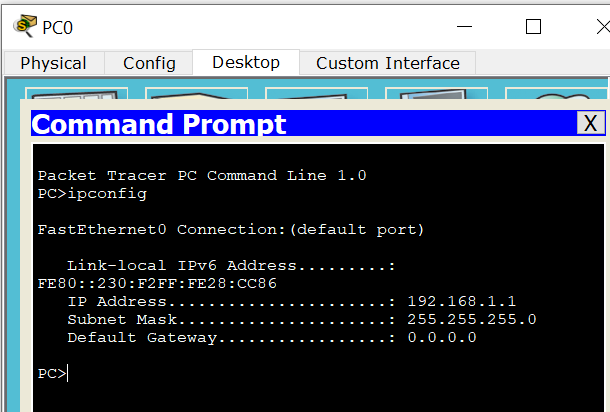
### Fig 3.1 Connection Set Up



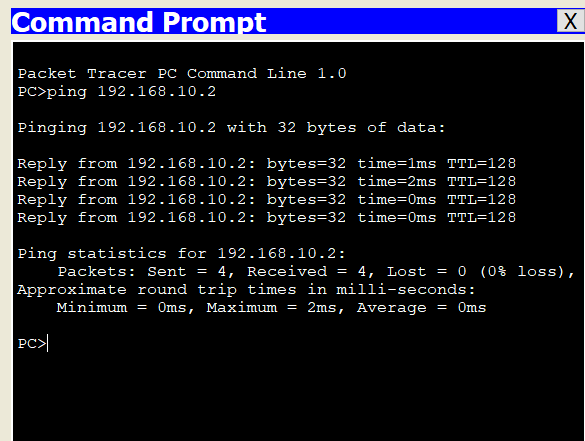
### Fig 3.2 Successful Transfer of packet depicting successful connection



### Fig 3.3 Configuration of each system



### Fig 3.4 Prompt showing IP Configurations of Computer



### Fig 3.5 Pinging the Computers

EXPERIMENT 4

# AIM : Implement various network topologies like Star, Bus, Ring, Mesh and Hybrid and share data between different network devices Using Cisco Packet Tracer.

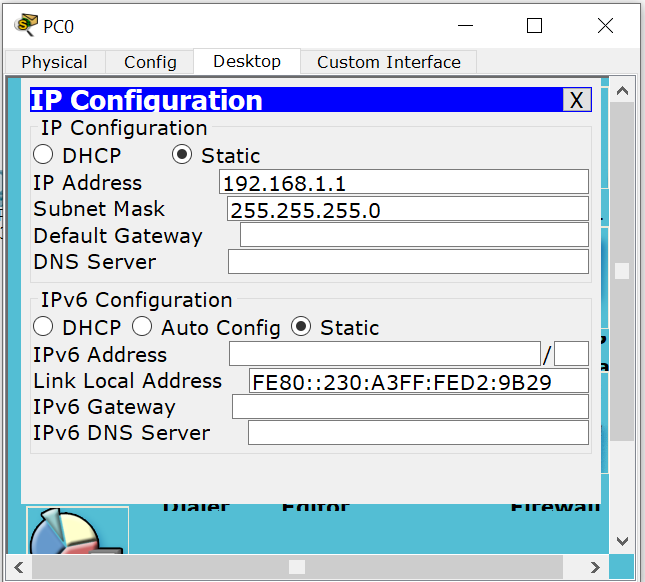
# TOPOLOGIES

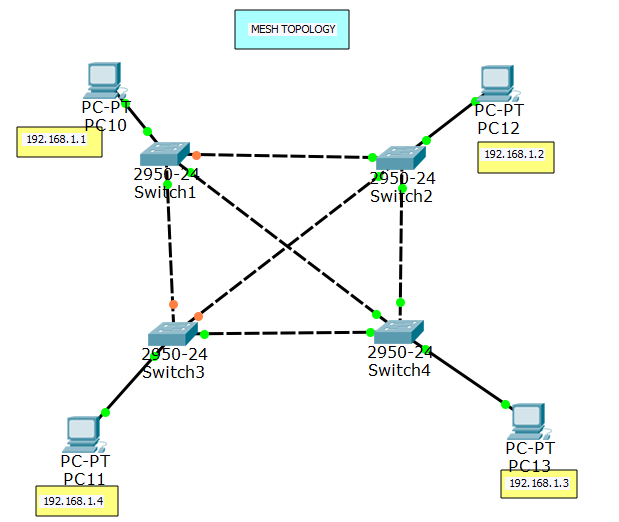
1. **Mesh Topology**- Every device has a dedicated point to point link to every other device.
2. **Star Topology**- Each device has a dedicated point-to-point link only to the central controller. The devices are not directly linked to one another.
3. **Bus Topology**- There is one long cable which acts as a backbone to link all the devices in the network, called Bus. The connection between the devices is multipoint.
4. **Ring Topology**- Each device has a dedicated point-to-point link only to the two devices on either side of it. A signal is passed along the ring in one direction, from device to device, until it reaches its destination.
5. **Hybrid Topology**- It is a combination of two or more topologies. Some of the examples of Hybrid Topology are given below.

# PROCEDURE

On CPT, put up any number of End Devices (like PCs, Laptops etc.) among which network is to be established.

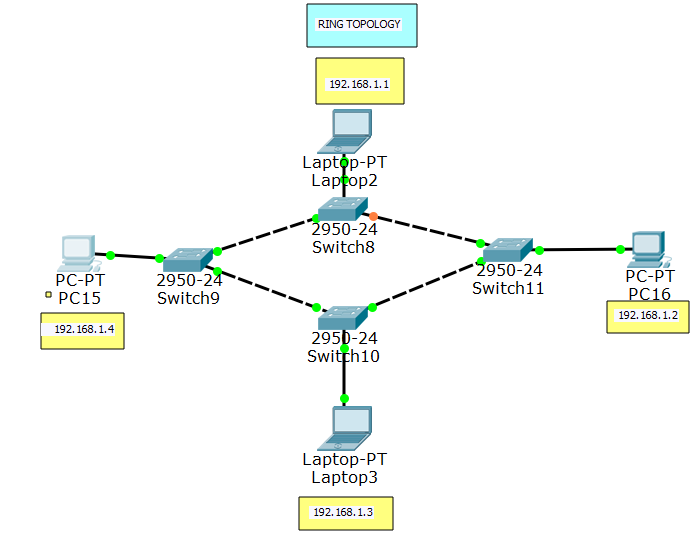
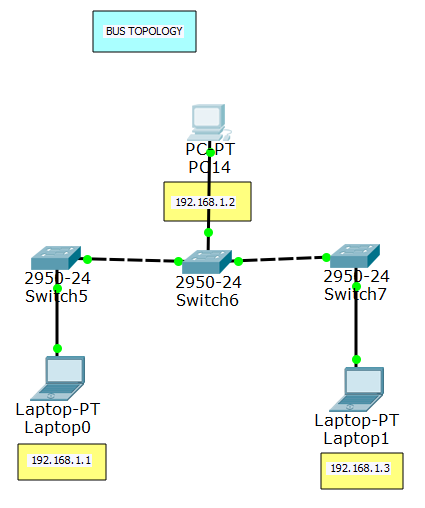
1. For Mesh Topology
2. Connect the end devices using cables which can be chosen by automatic cable connection.
3. For mesh topology each device should be connected to every other device.
4. Then establish a connection between all the devices by configuring them with suitable IP addresses.
5. Then do packet transfer and see the packet acknowledgement.
6. In this case, total number of wires/links needed are n(n-1)/2, where n is total number of devices.





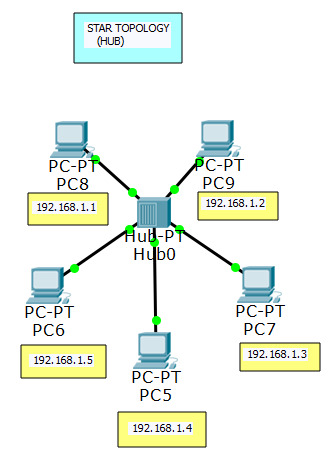
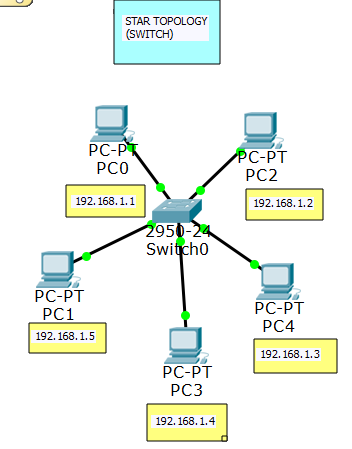
### Fig 4.1 Mesh topology Fig 4.2 Configuration of each system

1. For Ring Topology
2. Connect the end devices using cables which can be chosen by automatic cable connection.
3. For ring topology each device should be connected to 2 adjacent devices.
4. Then establish a connection between all the devices by configuring them with suitable IP addresses.
5. Then do packet transfer and see the packet acknowledgement.
6. In this case, total number of wires/links needed are n, where n is total number of devices.
7. For Bus Topology
8. All the devices are connected with a backbone cable to which cables from individual devices are attached using tappers and dropper.
9. Then establish a connection between all the devices by configuring them with suitable IP addresses.
10. Then do packet transfer and see the packet acknowledgement.
11. Here if backbone cable develops a default, network crashes.

### Fig 4.3 Ring Topology Fig 4.4 Bus Topology

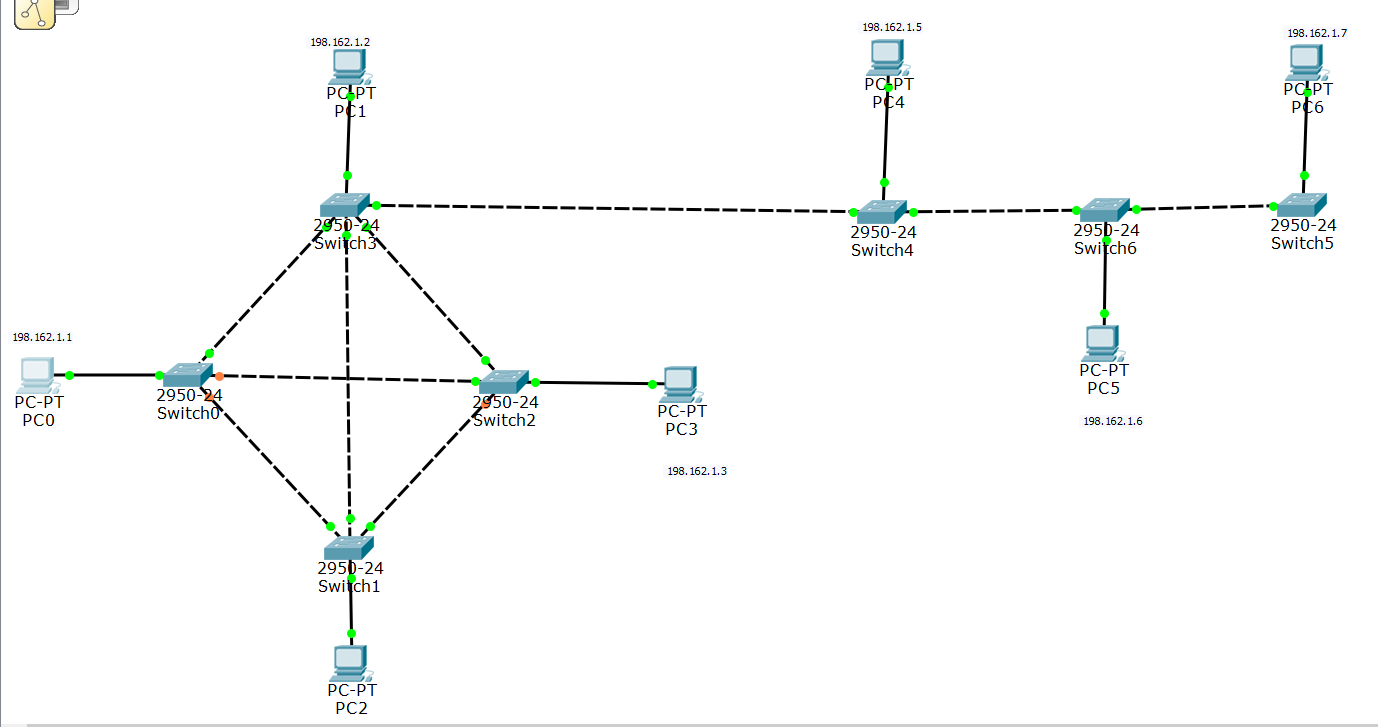
1. For Star Topology
2. All the end devices are connected to each other via a controller(hub/switch) .
3. Then establish a connection between all the devices by configuring them with suitable IP addresses.
4. Then do packet transfer and see the packet acknowledgement.
5. Here if controller develops a default, network crashes.

### Fig 4.5 Star Topology (hub) Fig 4.6 Ring Topology(Switch)

1. For Hybrid Topology

1. On CPT, put up any number of End Devices (like PCs, Laptops etc.) among which network is to be established.
2. Connect some devices with one topology and other devices with some other topology.
3. Then establish a connection between all the devices by configuring them with suitable IP addresses.
4. Then do packet transfer and see the packet acknowledgement.
5. Packet transfer is successful when Stimulation displays Successful.



### Fig 4.7 Hybrid Topology



### Fig 4.8 Successful Transfer of packet depicting successful connection

EXPERIMENT 5

# AIM : To connect networks using routers.

# ROUTER

A router is a device that analyses the contents of data packets transmitted within a network or to another network. Routers determine whether the source and destination are on the same network or whether data must be transferred from one network type to another, which requires encapsulating the data packet with routing protocol header information for the new network type.

A router examines a packet header's destination [IP address](https://searchwindevelopment.techtarget.com/definition/IP-address) and compares it against a [routing table](https://searchnetworking.techtarget.com/definition/routing-table) to determine the packet's best next [hop](https://whatis.techtarget.com/definition/hop). Routing tables list directions for forwarding data to particular network destinations, sometimes in the context of other variables, like cost. They amount to an algorithmic set of rules that calculate the best way to transmit traffic toward any given IP address.

A routing table often specifies a default route, which the router uses whenever it fails to find a better forwarding option for a given packet.

So, A router is a physical or [virtual appliance](https://searchservervirtualization.techtarget.com/definition/virtual-appliance) that passes information between two or more [packet-switched](https://searchnetworking.techtarget.com/definition/packet-switched) computer networks -- analysing a given data [packet](https://searchnetworking.techtarget.com/definition/packet)'s destination IP address, calculating the best way for it to reach that destination and then forwarding it accordingly.

A router is a common type of [gateway](https://internetofthingsagenda.techtarget.com/definition/gateway) -- positioned where two or more networks meet, including at each [point of presence](https://searchtelecom.techtarget.com/definition/point-of-presence-POP) on the internet. Hundreds of routers might forward a single packet as it moves from one network to the next on the way to its final destination.

# PROCEDURE

1. Make two or more different networks and configure them appropriately.
2. Connect the various networks using routers and configure them, as switches do not need to be configured but routers need configuration.
3. Connect one device of a particular network to router using wire and similarly with another device of another network.

Configure router from each side of network as follows:

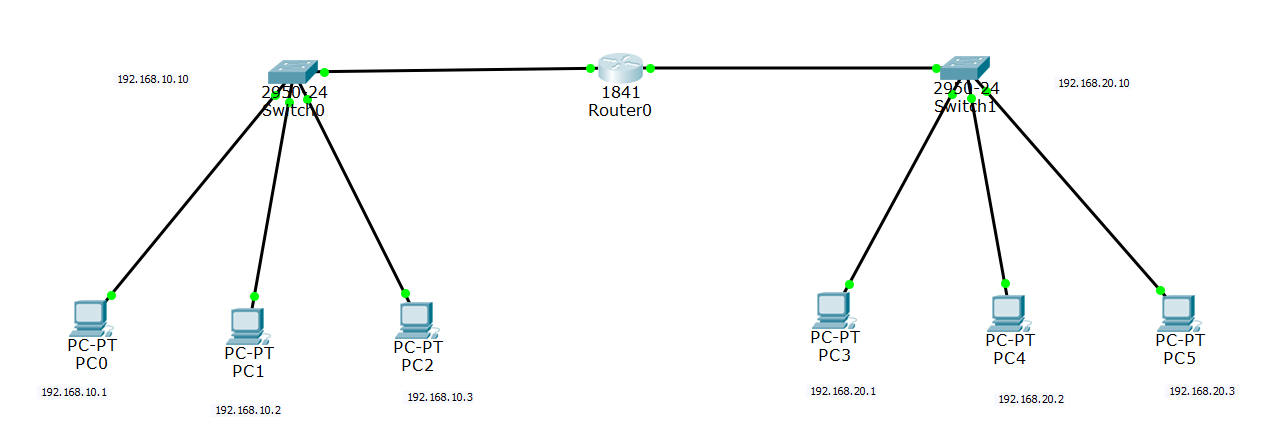
IP ADDRESS: 192.168.10.1

SUBNET MASK: 255.255.255.0

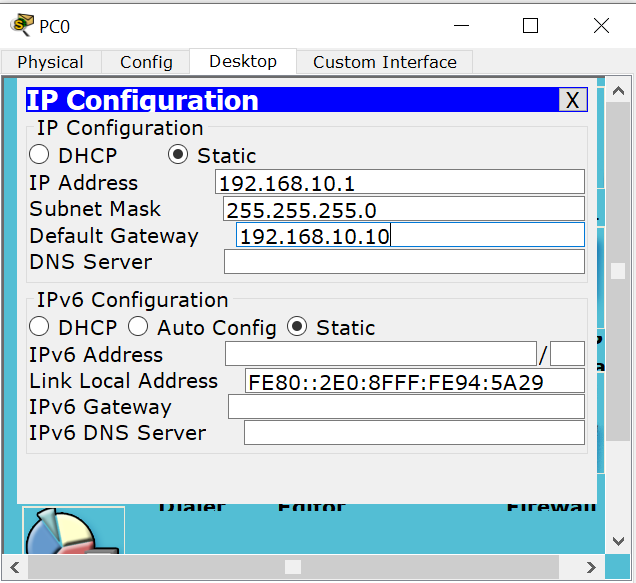
GATEWAY: 192.168.10.10

1. After proper configuration of devices and routers open command prompt of router ,i.e. Command Line Interface(CLI) for configuring routers.
2. On the Command Prompt window, select no when asked whether to continue with configuration dialog by typing no or n.
3. Then write enable or ena.
4. Write config and then press enter.
5. Write inter “Router Name”, router name can be known by hovering on red dot on link of router with switch.
6. Write ip address 192.168.10.10 255.255.255.0 (ip address format should match with that of the network).
7. Then write no shutdown, to activate router.
8. Exit.

Repeat the same procedure for all the networks connected to the router.

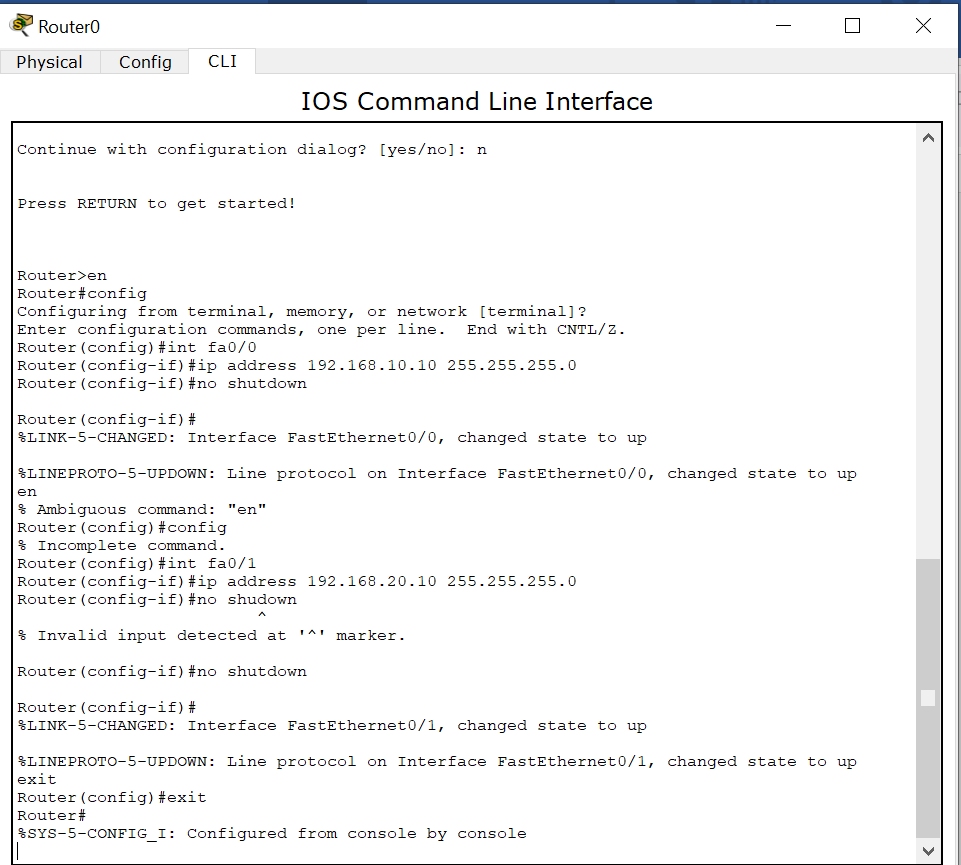


### Fig 5.1 Network topology showing IP Address of each Connected Computer with switch star topology





### Fig 5.2 Configuration of respective system of network 2 Fig 5.3 Configuration of respective system of network 1



### Fig 5.4 Commands to Configure Router

EXPERIMENT 6

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

# DEFAULT ROUTING

Default Routing defines the [packet](https://en.wikipedia.org/wiki/Packet_(information_technology)) forwarding rule to use when no specific route can be determined for a given [Internet Protocol](https://en.wikipedia.org/wiki/Internet_Protocol) (IP) destination address. All packets for which destinations are not established in the [routing table](https://en.wikipedia.org/wiki/Routing_table) are sent via the default route.

The default route generally points to another router, which treats the packet the same way: if a route matches, the packet is forwarded accordingly, otherwise the packet is forwarded to the default route of that router. The route evaluation process in each router uses the [longest prefix match](https://en.wikipedia.org/wiki/Longest_prefix_match) method to obtain the most specific route. The network with the longest subnet mask that matches the destination [IP address](https://en.wikipedia.org/wiki/IP_address) is the next-hop network gateway. The process repeats until a packet is delivered to the destination. Each router traversal counts as one hop in the distance calculation for the transmission path.

The default route is designated as the zero-address [0.0.0.0](https://en.wikipedia.org/wiki/0.0.0.0) and the subnet mask is given as /0, which effectively specifies all networks, and is the shortest match possible. The device to which the default route points is often called the [Default Gateway](https://en.wikipedia.org/wiki/Default_gateway).

In default routing there is no need of destination address. To reduce size of routing table and work of network engineer. But it is slow routing.

# PROCEDURE

1. First Create a topology like this.
2. Assign IP address for both PC's with appropriate IP and subnet mask and default gateway.

For network 1

IP ADDRESS: 192.168.10.1

SUBNET MASK: 255.255.255.0

GATEWAY: 192.168.10.1

1. Configure the IP addresses of the computers according to their default gateway.
2. Configure each Router and set Default Routes for each router using the command:

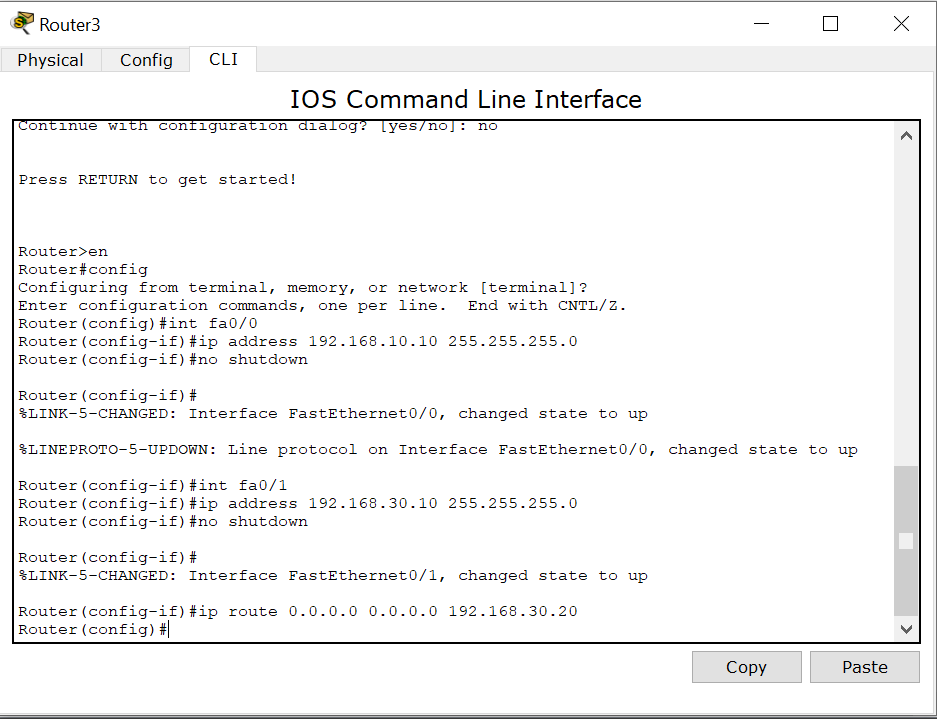
*ip route <ip\_address><subnet\_mask><next\_hop\_address>.*

Here both IP Address and Subnet Mask will be set zero for the default route.

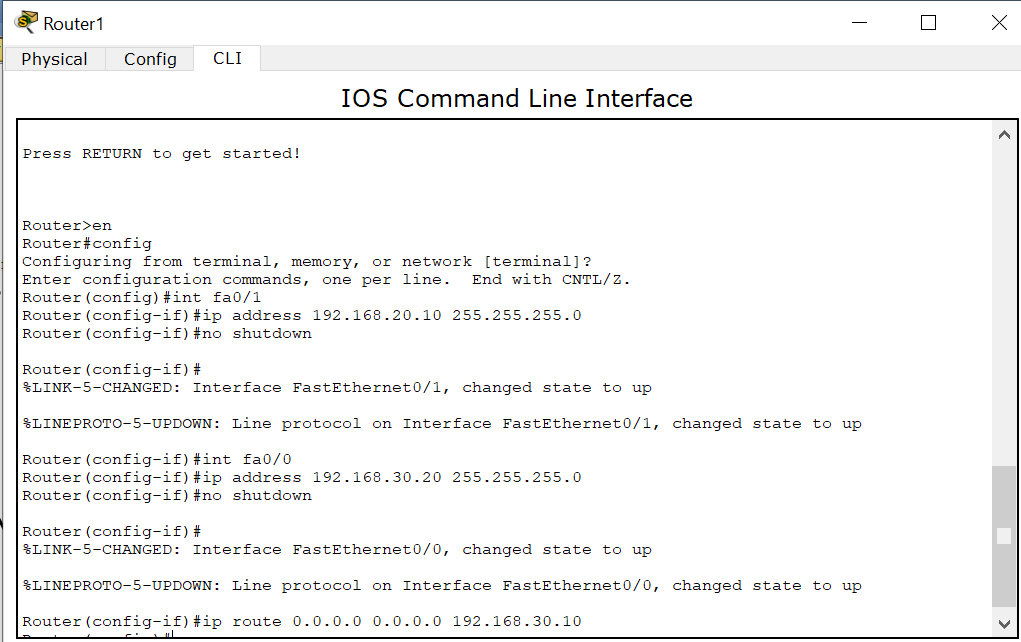
1. Now the networks are ready to transfer messages between them.

### 

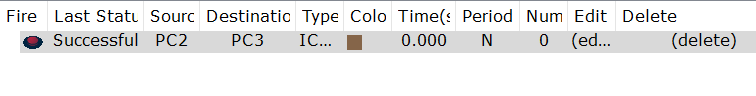
### Fig 6.1 Network topology showing IP Address of each Connected Computer with switch star topology



### Fig.6.2 Commands to configure interfaces of Router3



### Fig.6.3 Commands to configure interfaces of Router 1



### Fig 6.4 Successful Transfer of packet depicting successful connection

EXPERIMENT 7

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

# ROUTING

Routing is one of the most essential procedures in data communication. It ensures that data travels from one network to another with optimal speed and minimal delay, and that its integrity is maintained in the process.

# STATIC ROUTING

Static routing is considered the simplest form of routing.Static routing is a type of network routing technique that performs routing decisions with preconfigured routes in the routing table. Static routing is not a routing protocol; instead, it is the manual configuration and selection of a network route, usually managed by the network administrator. It is employed in scenarios where the network parameters and environment are expected to remain constant, where the choices in route selection are limited, or there is only a single default route available. Also, static routing can be used if you have only few devices for route configuration and there is no need for route change in the future.

Static routing is only optimal in a few situations. Network degradation, latency and congestion are inevitable consequences of the non-flexible nature of static routing because there is no adjustment when the primary route is unavailable.

**Advantage of static routing**

It is easy to implement.

It is most secure way of routing, since no information is shared with other routers.

It puts no overhead on resources such as CPU or memory.

**Disadvantage of static routing**

It is suitable only for small network.

If a link fails it cannot reroute the traffic.

# PROCEDURE

1. First Create a topology like this
2. Assign IP address for both PC's with appropriate IP and subnet mask and default gateway.

For network 1

IP ADDRESS: 192.168.10.1

SUBNET MASK: 255.255.255.0

GATEWAY: 192.168.10.1

1. Now configure both router with static route

First give appropriate IP addresses to all the interfaces of router and them make static routing table.

For R0

Destination Subnet Mask Next Hop

192.168.20.0 255.255.255.0 192.168.50.2

192.168.30.0 255.255.255.0 192.168.50.2

For R1

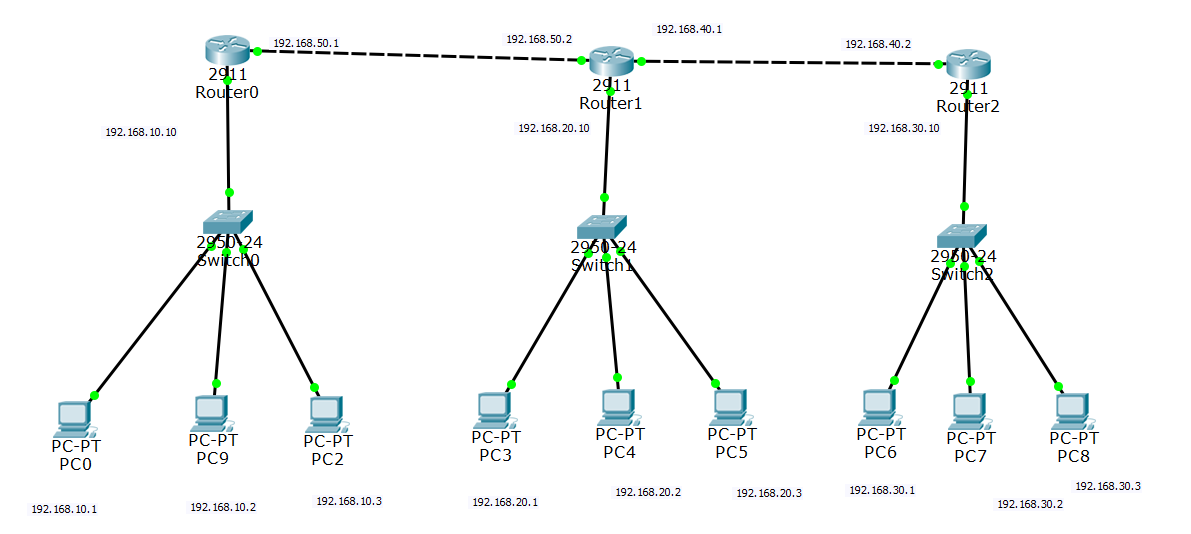
192.168.10.0 255.255.255.0 192.168.50.1

192.168.30.0 255.255.255.0 192.168.40.2

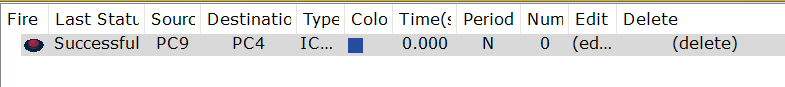
For R2

192.168.20.0 255.255.255.0 192.168.40.1

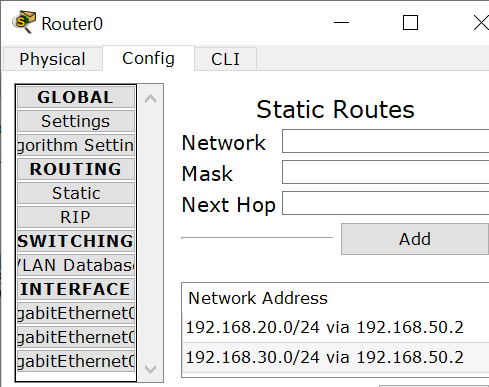
192.168.10.0 255.255.255.0 192.168.40.1



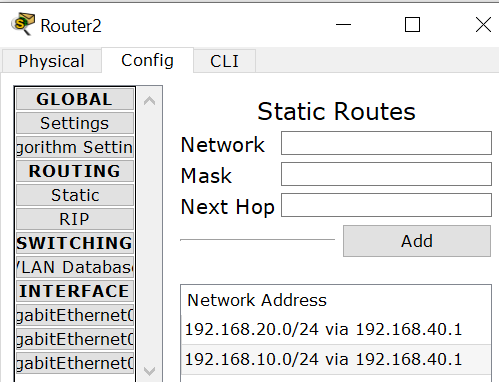
### Fig 7.1 Network topology showing IP Address of each Connected Computer with switch star topology



### Fig 7.2 Successful Transfer of packet depicting successful connection

### Fig 7.3 Configuring router 0 for static routing Fig 7.4 Configuring router1 for static routing



### Fig 7.5 Configuring router2 for static routing

EXPERIMENT 8

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

# DYNAMIC ROUTING

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, also called adaptive routing, is a process where a router can forward data via a different route or given destination based on the current conditions of the communication circuits within a system. The term is most commonly associated with [data networking](https://en.wikipedia.org/wiki/Data_networking) to describe the capability of a network to 'route around' damage, such as loss of a node or a connection between nodes, so long as other path choices are available. Dynamic routing allows as many routes as possible to remain valid in response to the change.  
  
Dynamic routing uses multiple algorithms and protocols. The most popular are Routing Information Protocol (RIP) and Open Shortest Path First (OSPF).

Dynamic routing is easy to configure on large networks and is more intuitive at selecting the best route, detecting route changes and discovering remote networks. However, because routers share updates, they consume more bandwidth than in static routing; the routers' CPUs and RAM may also face additional loads as a result of routing protocols. Finally, dynamic routing is less secure than static routing.

# PROCEDURE

1. First Create a topology like this
2. Assign IP address for both PC's with appropriate IP and subnet mask and default gateway.

For network 1

IP ADDRESS: 192.168.10.1

SUBNET MASK: 255.255.255.0

GATEWAY: 192.168.10.1

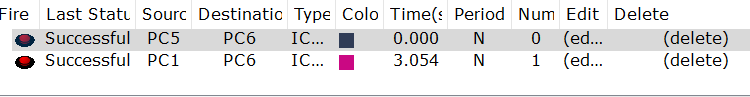
1. Now configure both router with dynamic route

First give appropriate IP addresses to all the interfaces of router and give the IP,addresses of all the networks involved.

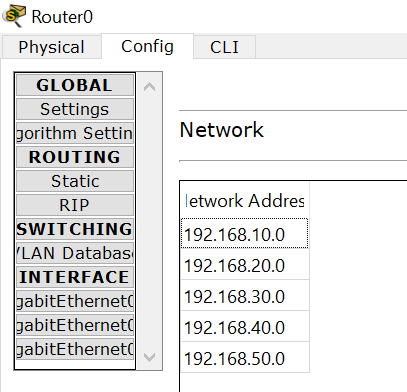
|  |  |  |
| --- | --- | --- |
| For R0  192.168.10.0  192.168.20.0  192.168.30.0  192.168.40.0  192.168.50.0 | For R1  192.168.10.0  192.168.20.0  192.168.30.0  192.168.40.0  192.168.50.0 | For R2  192.168.10.0  192.168.20.0  192.168.30.0  192.168.40.0  192.168.50.0 |



### Fig 8.1 Network topology showing IP Address of each Connected Computer with switch star topology



### Fig 8.2 Successful Transfer of packet depicting successful connection



### Fig 8.3 Configuring router 0 for dynamic routing

EXPERIMENT 9

# AIM: Troubleshooting in Default, Static, and Dynamic Routing by connecting multiple networks.

# NETWORK TROUBLESHOOTING

Network troubleshooting is the collective measures and processes used to identify, diagnose and resolve problems and issues within a computer network. It is a systematic process that aims to resolve problems and restore normal network operations within the network.

Some of the commands used for network troubleshooting are:

The *show ip route* command is used to show a router's routing table. This displays the list of all networks that the router can reach, and how to get there.

* *show ip route* : (with no arguments) Displays all IP routes.
* *show ip route <ip\_address>* : (with the address argument) Displays routes to a specific IP address.
* *show ip route <subnet\_mask>* : (with the mask argument) Displays routes with a specific network mask.

The show interface command displays the status of the router's interfaces. We can also specify a certain interface, otherwise status of all interfaces is shown.

* *show interface <interface\_name>*

# PROCEDURE

1. Set up the connections as shown below.



### Fig 9.1 Network topology showing IP Address of each Connected Computer with switch star topology

1. Assign IP address for PC's with appropriate IP and subnet mask and default gateway. Set router interface using IP configuration option for systems and CLI for router interfaces.

For network 1

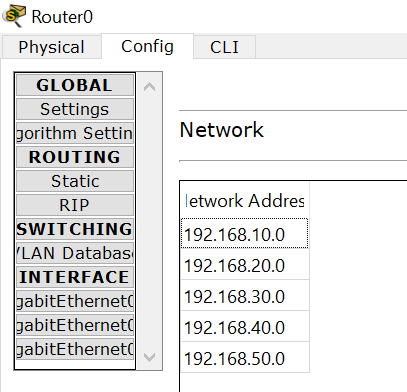
IP ADDRESS: 192.168.10.1

SUBNET MASK: 255.255.255.0

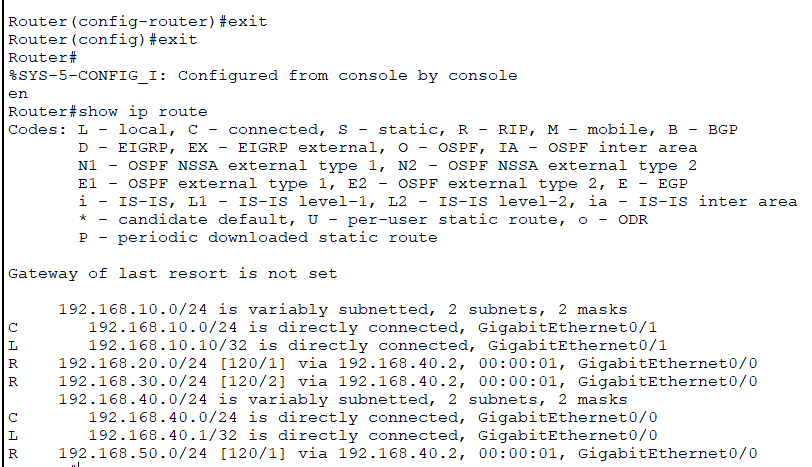
GATEWAY: 192.168.10.1

1. Add dynamic routing table for each router.
2. Check IP and interface information for routers using following commands shown in figure.

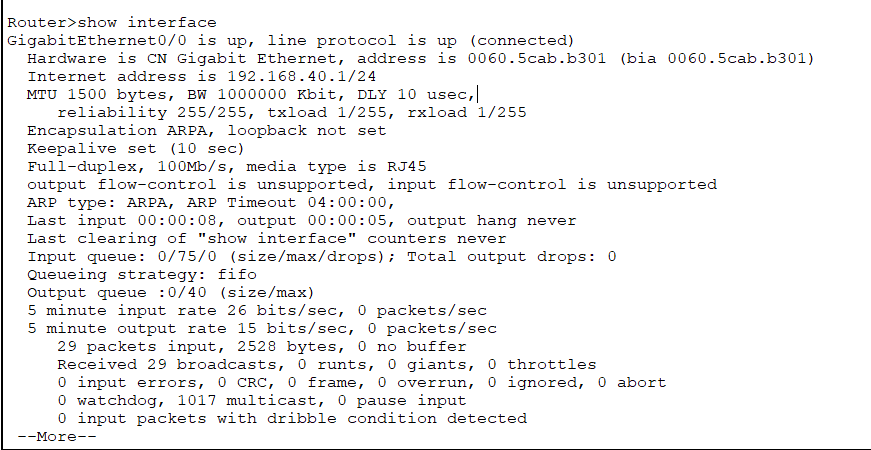
* Show ip route
* Show interface



### Fig 9.2 Configuring router 0 for dynamic routing



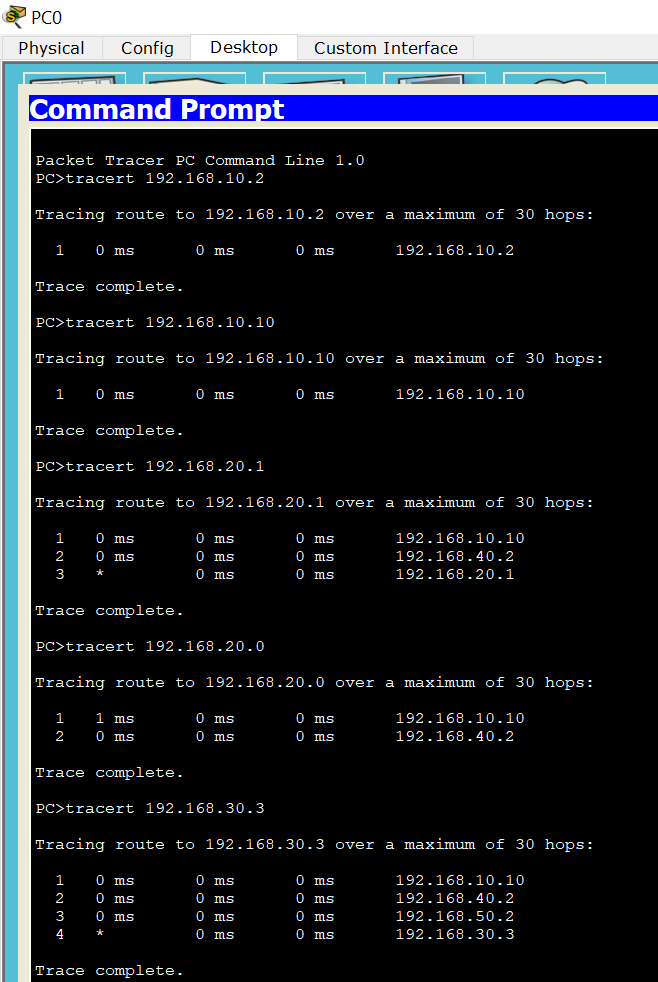
### Fig 9.3 Checking IP information



### Fig 9.4 checking interface information

1. For systems, trace route of message from one system to another using following command at sender side.

* Trace rt destination ip



### Fig 9.5 Trace route of message from one system to another

1. Troubleshooting was performed successfully.

EXPERIMENT 10

# AIM: To establish a virtual LAN network.

# VLAN

A VLAN is a group of devices on one or more LANs that are configured to communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, they are extremely flexible.

VLANs are often associated with IP subnetworks. For example, all of the end stations in a particular IP subnet belong to the same VLAN. Traffic between VLANs must be routed. You must assign LAN interface VLAN membership on an interface-by-interface basis (this is known as interface-based or static VLAN membership).

You can set the following parameters when you create a VLAN in the management domain:

•https://www.cisco.com/c/dam/en/us/td/i/templates/blank.gifVLAN number

•https://www.cisco.com/c/dam/en/us/td/i/templates/blank.gifVLAN name

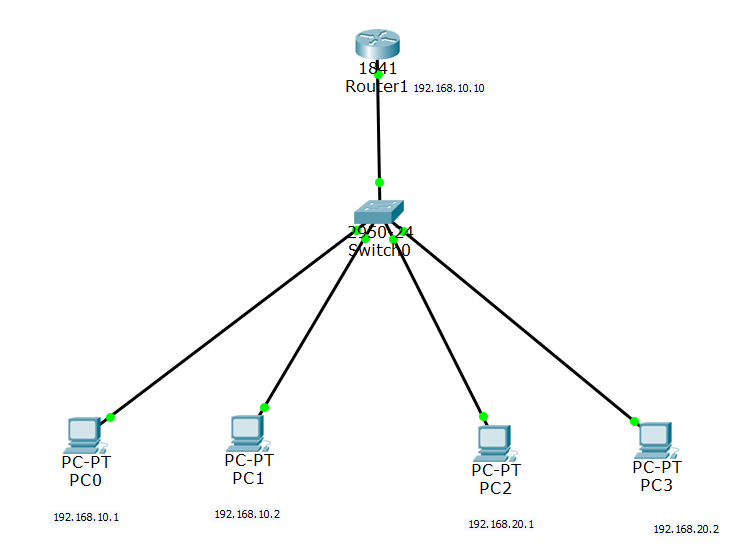
Virtual LAN (VLAN) is a concept in which we can divide the devices logically on layer 2 (data link layer). Generally, layer 3 devices divides broadcast domain but broadcast domain can be divided by switches using the concept of VLAN. A broadcast domain is a network segment in which if a device broadcast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

**ADVANTAGES:**

* performance –The network traffic is full of broadcast and multicast. VLAN reduces the need to send such traffic to unnecessary destination.e.g-If the traffic is intended for 2 users but as 10 devices are present in the same broadcast domain therefore all will receive the traffic i.e wastage of bandwidth but if we make VLANs, then the broadcast or mulicast packet will go to the intended users only.
* formation of virtual groups – As there are different departments in every organisation namely sales, finance etc., VLANs can be very useful in order to group the devices logically according to their departments.
* security – In the same network, sensitive data can be broadcast which can be accessed by the outsider but by creating VLAN, we can control broadcast domains, set up firewalls, restrict access. Also, VLANs can be used to inform the network manager of an intrusion. Hence, VLANs greatly enhance network security.
* Flexibility – VLAN provide flexibility to add, remove the number of host we want.
* Cost reduction – VLANs can be used to create broadcast domains which eliminate the need for expensive routers.
* By using Vlan, the number of small size broadcast domain can be increased which are easy to handle as compared to a bigger broadcast domain.

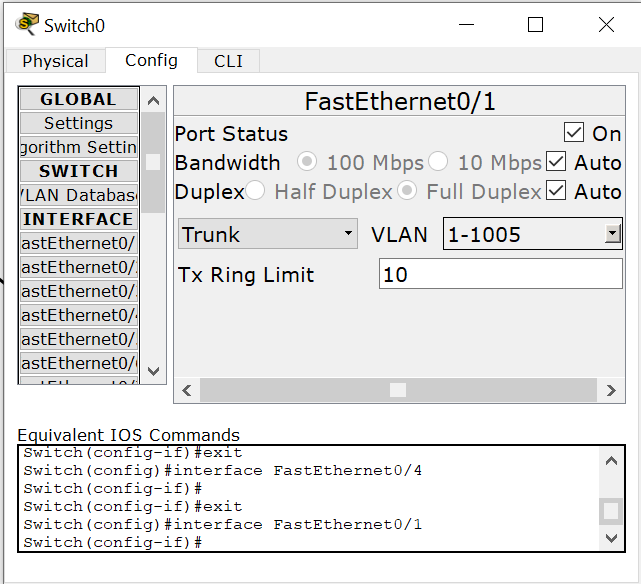
# PROCEDURE

1. Set up connections as shown.
2. Set IP addresses for routers and systems and default gateways
3. Set Switch configuration by going to switch -> VLAN database and set VLAN number as 10 and VLAN name as ‘’(can be any name) and press add.



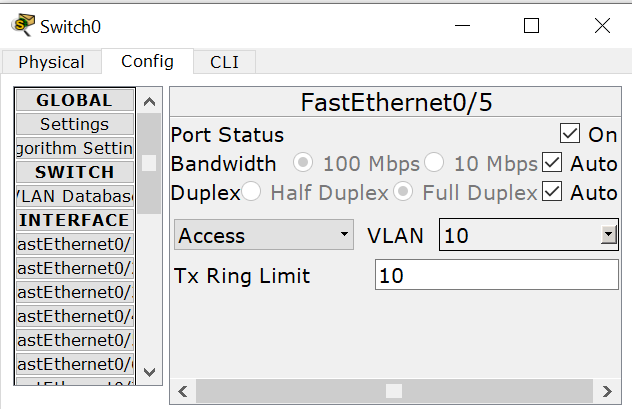
### Fig 10.1 Network topology showing IP Address of each Connected Computer with switch star topology

1. Go to Fast Ethernet0/1, i.e. router and switch in switch and select trunk mode.

### Fig 10.3 Adding a New VLAN Fig 10.3 Access Mode of Interface Fa0/1 is set to ‘Trunk’

1. For interfaces corresponding to both systems of virtual network setup, select VLAN as 10,lab1 in switch config.

### Fig.10.3 Setting VLAN of Interface Fa0/4 to 10 Fig.10.4 Setting VLAN of Interface Fa0/5 to 10

1. Go to router , then CLI and setup virtual network using following commands :

* config
* int fa 0/0.1
* encapsulation dot1q 20
* ip address 192.168.20.1 255.255.255.0

1. Transmit message from sender to receiver to check the virtual network set.



### Fig 10.5 Successful Transfer of packet depicting successful connection

EXPERIMENT 11

# AIM: Configure Static Network Address Translation (NAT) in Cisco Packet Tracer.

# NAT

NAT is a method of remapping one IP [address space](https://en.wikipedia.org/wiki/Address_space) into another by modifying [network address](https://en.wikipedia.org/wiki/Network_address) information in the [IP header](https://en.wikipedia.org/wiki/IP_header) of packets while they are in transit across a traffic [routing device](https://en.wikipedia.org/wiki/Router_(computing)). The technique was originally used as a shortcut to avoid the need to readdress every host when a network was moved. It has become a popular and essential tool in conserving global address space in the face of [IPv4 address exhaustion](https://en.wikipedia.org/wiki/IPv4_address_exhaustion). One Internet-routable [IP address](https://en.wikipedia.org/wiki/IP_address) of a NAT gateway can be used for an entire [private network](https://en.wikipedia.org/wiki/Private_network). Basically, NAT allows a single device, such as a router, to act as an agent between the Internet (or public network) and a local network (or private network), which means that only a single unique IP address is required to represent an entire group of computers to anything outside their network.

**Types of NAT**

* Static NAT
* Dynamic NAT
* Port Address Translation (PAT)

# Advantages of NAT

* NAT conserves legally registered IP addresses .
* It provides privacy as the device IP address, sending and receiving the traffic, will be hidden.

# Disadvantage of NAT

* Translation results in switching path delays.

NAT inside and outside addresses :

**Inside local address** – An IP address that is assigned to a host on the Inside (local) network. The address is probably not a IP address assigned by the service provider i.e., these are private IP address. This is the inside host as seen from the inside network.

**Inside global address** – IP address that represents one or more inside local IP addresses to the outside world. This is the inside host as seen from the outside network.

**Outside local address** – This is the actual IP address of the destination host in the local network after translation.

**Outside global address** – This is the outside host as seen from the outside network. It is the IP address of the outside destination host before translation.

**Static NAT**

It is an one-to-one mapping of a [private IP address](http://www.omnisecu.com/tcpip/what-are-private-ip-addresses.php) to a public IP address. Static NAT (Network Address Translation) is useful when a network device inside a private network needs to be accessible from internet (used for web hosting).

It is not used in organisations as there are many devices who will need Internet access and to provide Internet access, public IP address is needed. Suppose, if there are 3000 devices who needs access to Internet, the organisation have to buy 3000 public addresses that will be very costly.

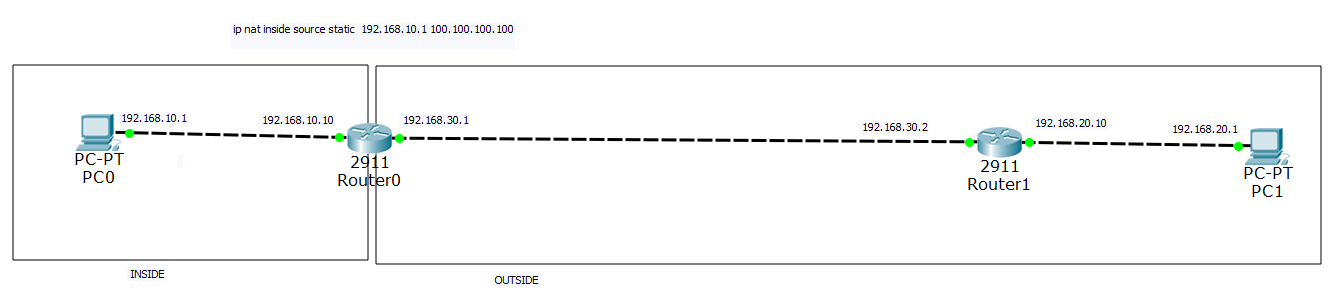
# PROCEDURE

1. Set up connections as shown.
2. Set IP addresses for routers and systems and default gateways
3. Configure the router interfaces (dynamic)using the following commands in the CLI of the router.

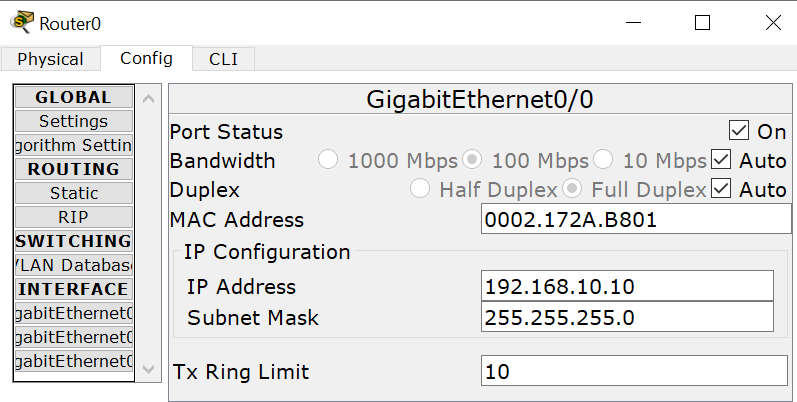
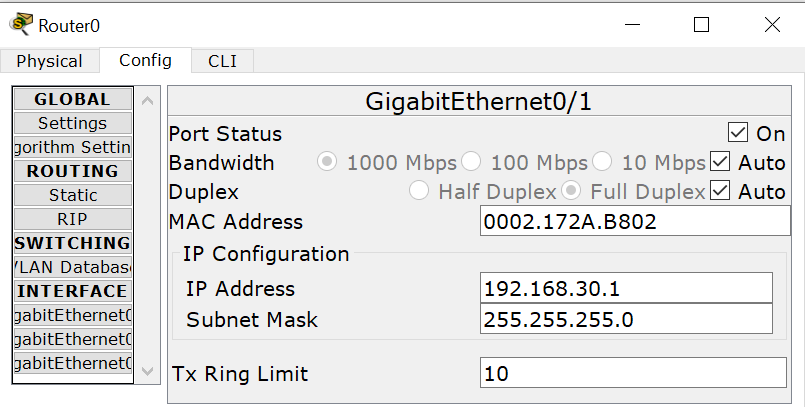
*router rip*

*network <network\_ip>* (for every network connected to router)

or just write corresponding ip addresses in router table.

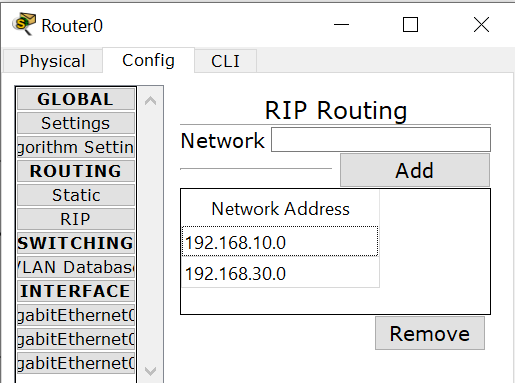
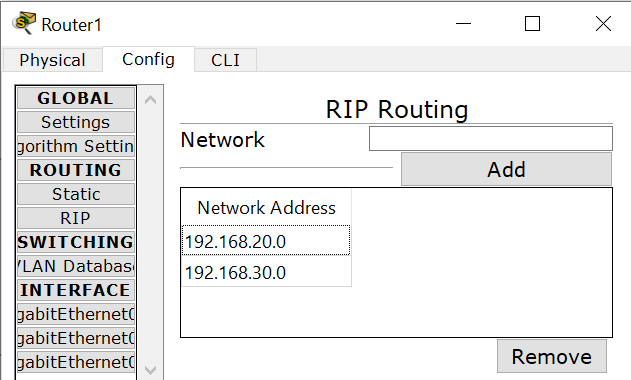


### Fig 11.1 Physical Connection Representation

### Fig 11.2 Doing Configuration of interface 0/0 Fig 11.3 Doing Configuration of interface 0/0

1. Do the RIP configuration of every router similarly as shown below for Router 1 (Dynamic Routing).

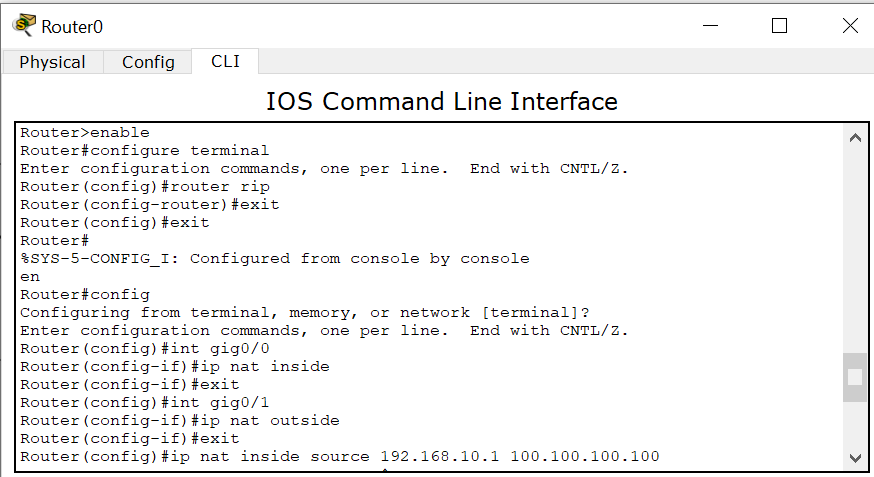
 

### Fig 11.4 RIP Configuration of router 0 Fig 11.5 RIP Configuration of router 0

### 

1. Let us make 192.168.10.1 private (inside network). Use the following commands to set up inside and outside networks for NAT.
2. Let the public address provided by the ISP is 100.100.100.100. Now we need to map this public IP address to the local IP address i.e., 192.168.10.1. The command to be used is

*ip nat inside source static <local\_ip\_address> <global\_ip\_address>*



### Fig 11.6 Mapping the Local IP Address to the Global IP Address

1. *debug ip nat* command can be used to check if the Network is working fine. It turns the debugging on. So after we execute a ping system on the network, the IP NAT debugging is shown
2. You can use the show ip nat translation command to verify that the translation does exist in the translation table.



### Fig.11.7 Translation Table

EXPERIMENT 12

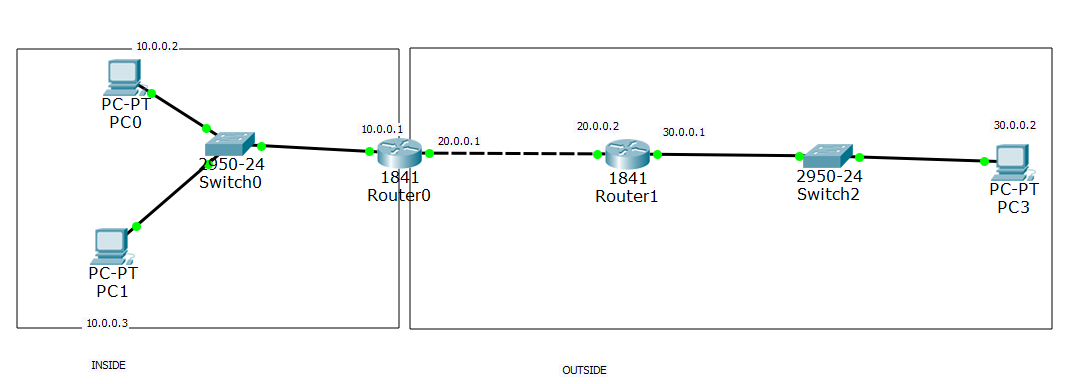
# AIM- Configure Dynamic Network Address Translation (NAT) in Cisco Packet Tracer.

# DYNAMIC NAT

Dynamic NAT can be defined as mapping of a [private IP address](http://www.omnisecu.com/tcpip/what-are-private-ip-addresses.php) to a public IP address from a group of public IP addresses called as NAT pool. Dynamic NAT establishes a one-to-one mapping between a [private IP address](http://www.omnisecu.com/tcpip/what-are-private-ip-addresses.php) to a public IP address. Here the public IP address is taken from the pool of IP addresses configured on the end NAT router. The public to private mapping may vary based on the available public IP address in NAT pool. If the IP address of pool are not free, then the packet will be dropped as only fixed number of private IP address can be translated to public addresses. NAT is used when the number of users who wants to access the Internet are fixed. This is also very costly as the organisation have to buy many global IP addresses to make a pool. The way dynamic NAT differs from static NAT is that where static NAT provides a one-to-one internal to public static IP address mapping, dynamic NAT usually uses a group of available public IP addresses.

## **PROCEDURE**

1. Set up connections as shown.



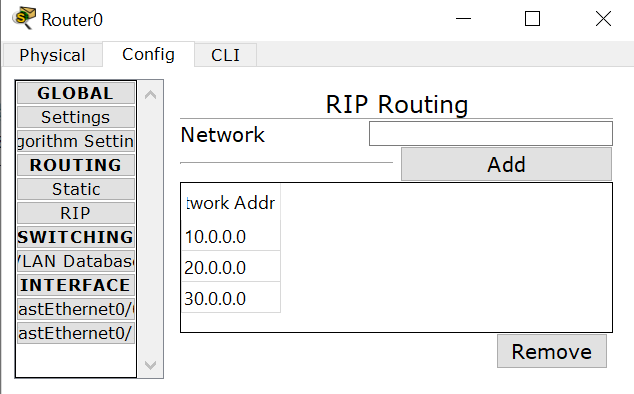
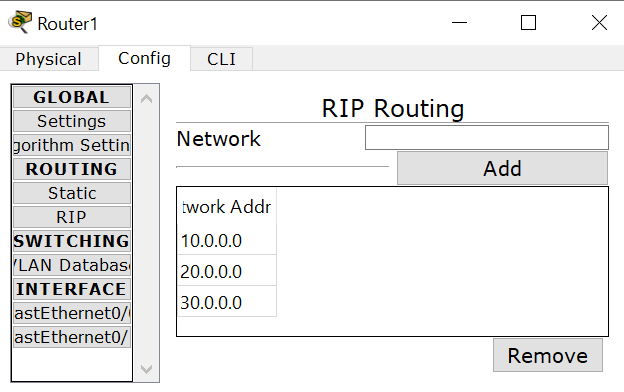
### Fig 12.1 Physical Connection Representation

1. Set IP addresses for routers and systems and default gateways
2. Configure the router interfaces according to dynamic routing using the following commands in the CLI of the router.

*router rip*

*network <network\_ip>* (for every network connected to router)

or just write corresponding ip addresses in router table.

### Fig 12.2 RIP Configuration of router 0 Fig 12.3 RIP Configuration of router 0

1. Suppose we want to make 10.0.0.0 private (inside network). Use the following commands to set up inside and outside networks for NAT.
2. First we need to configure the traffic that will be permitted for which following command will be used:

*access-list <access-list\_number> permit <inside\_network\_ip> <reverse\_subnet\_mask>*

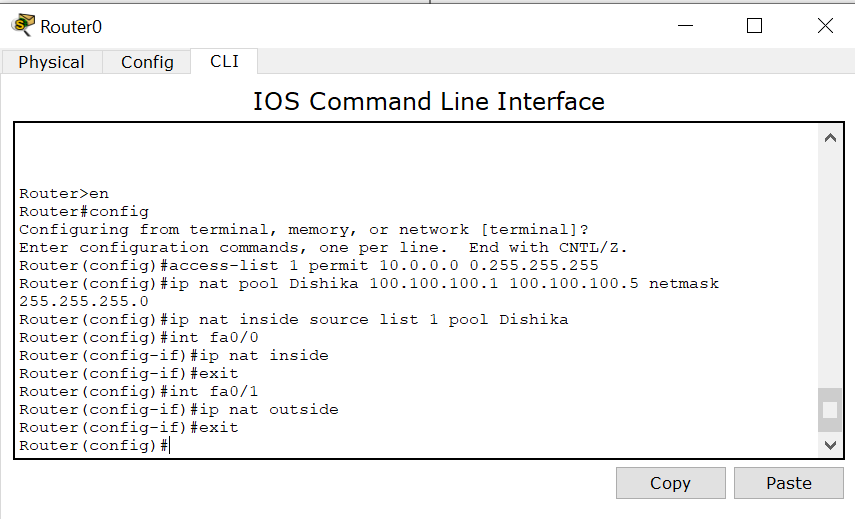
1. Let the public addresses provided by the ISP are from 100.100.100.1 to 100.100.100.5.

Now we will configure a pool of these addresses for the NAT using the following command:

*ip nat pool <pool\_name> <starting\_ip> < ending\_ip > netmask <subnet\_mask>*

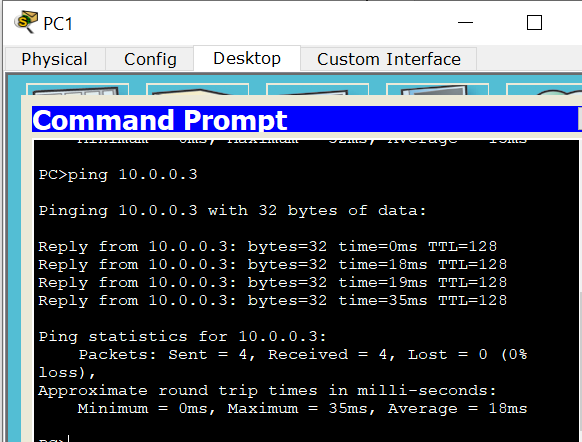
1. Now we will associate the access list with the pool of addresses using the following command:

*ip nat inside source list <access-list\_number> pool <pool\_name>*



### Fig 12.4 Mapping the Local IP Address to the Global IP Address

1. *debug ip nat* command can be used to check if the Network is working fine. It turns the debugging on. So after we execute a ping system on the network, the IP NAT debugging is shown.
2. You can use the show ip nat translation command to verify that the translation does exist in the translation table.

### Fig.12.5 Translation Table Fig 12.6 Pinging an External IP

1. The Network is ready to communicate messages.

EXPERIMENT 13

# AIM- Configure Port Address Translation (PAT) in Cisco Packet Tracer.

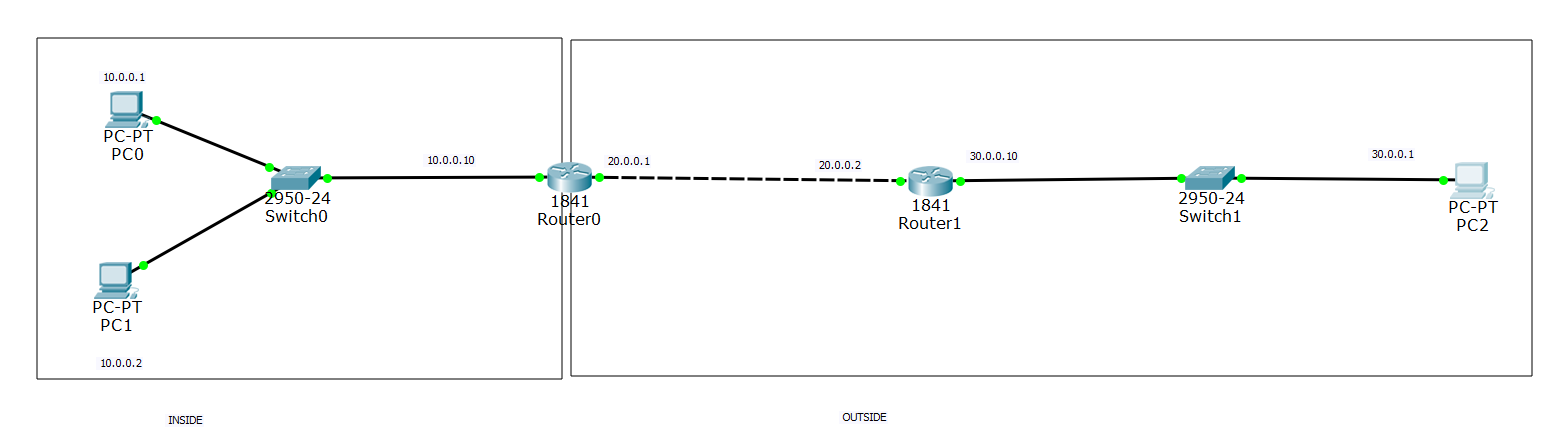
**PORT ADDRESS TRANSLATION (PAT)**

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](https://searchwindevelopment.techtarget.com/definition/IP-address). The goal of PAT is to conserve IP addresses.

In such a scenario, the Internet Service Provider ([ISP](https://searchwindevelopment.techtarget.com/definition/ISP)) assigns a single IP address to the home network's [router](https://searchnetworking.techtarget.com/definition/router). When Computer X logs on the Internet, the router assigns the client a [port number](https://searchnetworking.techtarget.com/definition/port-number), which is appended to the internal IP address. This, in effect, gives Computer X a unique address. If Computer Z logs on the Internet at the same time, the router assigns it the same local IP address with a different port number. Although both computers are sharing the same public IP address and accessing the Internet at the same time, the router knows exactly which computer to send specific [packet](https://searchnetworking.techtarget.com/definition/packet)s to because each computer has a unique internal address.

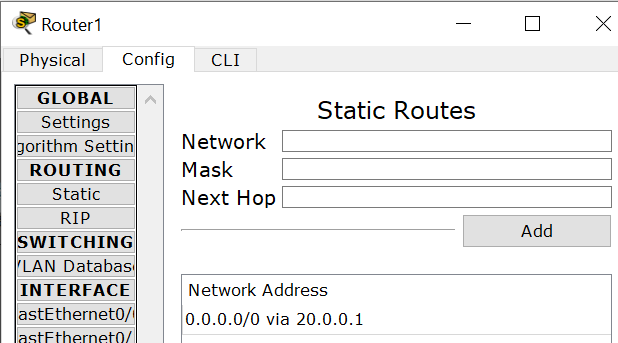
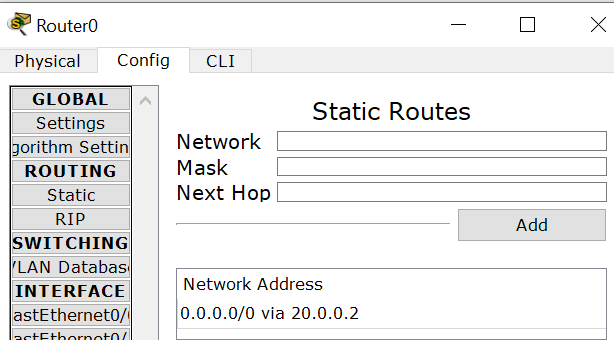
## **PROCEDURE**

1. Set up connections as shown.



### Fig 13.1 Physical Connection Representation

1. Set IP addresses for routers and systems and default gateways
2. Configure the router interfaces according to default routing by writing corresponding IP addresses in static router table.



### Fig 13.2 RIP Configuration of router 0 Fig 13.3 RIP Configuration of router 0

1. Suppose we want to make 10.0.0.0 private (inside network). Use the following commands to set up inside and outside networks for NAT.
2. First we need to configure the traffic that will be permitted for which following command will be used:

*access-list <access-list\_number> permit <inside\_network\_ip> <reverse\_subnet\_mask>*

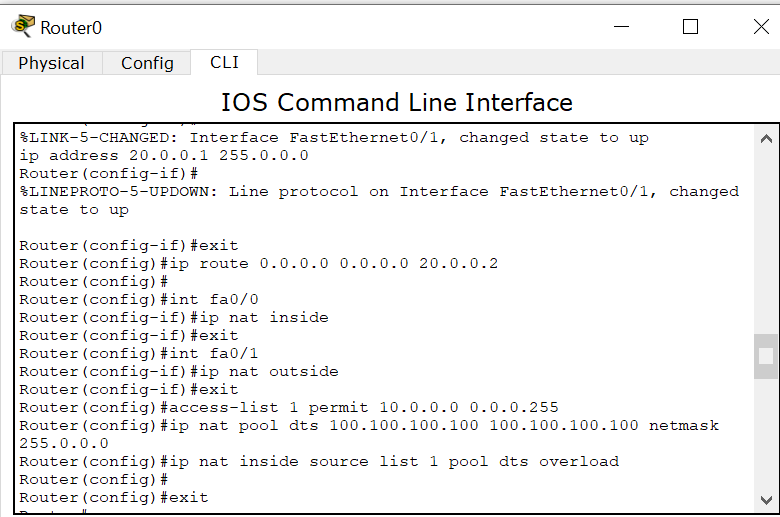
1. Let the public addresse provided by the ISP is 100.100.100.100.

Now we will configure a pool of these addresses for the NAT using the following command:

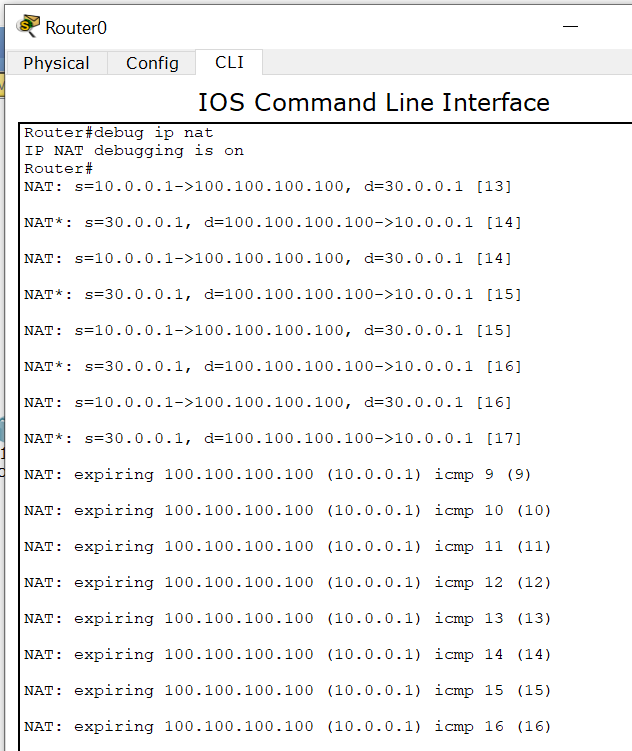
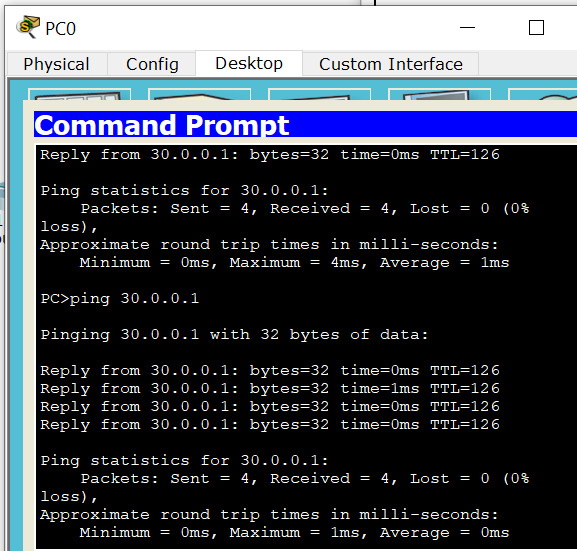
*ip nat pool <pool\_name> <public\_ip\_address> < public\_ip\_address > netmask <subnet\_mask>*

1. Now we will associate the access list with the pool of addresses using the following command:

*ip nat inside source list <access-list\_number> pool <pool\_name> overload*

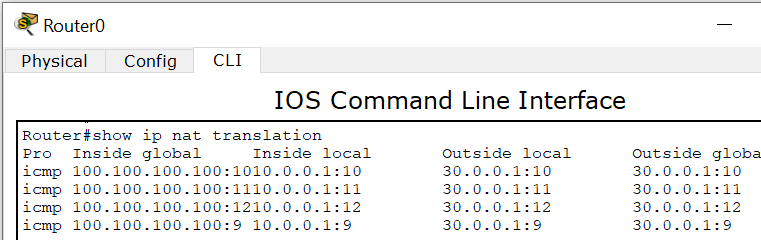


### Fig 13.4 Mapping the Local IP Address to the Global IP Address

1. *debug ip nat* command can be used to check if the Network is working fine. It turns the debugging on. So after we execute a ping system on the network, the IP NAT debugging is shown.

### Fig 13.5 Pinging an External IP Fig 13.6 Debugging

1. You can use the show ip nat translation command to verify that the translation does exist in the translation table.



### Fig.13.7 Translation Table

1. The Network is ready to communicate messages.