Sardar Patel College of Engineering, Bakrol

Name:-	Vishwas R. Acharya
Enrollment No:-	181240116001
Subject:-	Computer Networks
Subject Code:-	3150710

Sr no.	Practical List	Page No.	Practical Date	Submission Date	Grade	Signature
1	Detail study regarding NS-2, Wireshark and Netsim.	2 - 7	01/07/2020	15/07/2020		
2	Study regarding Cripping tools and the IP with practical.	8 - 14	15/07/2020	22/07/2020		
3	Study about Cisco IP packet Tracer and according to that creating 2 different scenario.	15 - 23	22/07/2020	05/08/2020		
4	Creating a star, bus and mesh topology using Cisco IP packet tracer.	24 - 30	05/08/2020	19/08/2020		
5	Create Computer network using CISCO IP PACKET TRACER.	31 - 37	19/08/2020	02/09/2020		
6	Configuring RIP (Routing Information Protocol) with CISCO IP PACKET TRACER.	38 - 42	02/09/2020	16/09/2020		
7	Email communication using CISCO IP PACKET TRACER.	43 - 48	16/09/2020	30/09/2020		
8	Configure OSPF (Open Shortest Path First)	49 - 52	30/09/2020	07/10/2020		
9	Commands for Advance Networking.	53 - 57	07/10/2020	14/10/2020		

PRACTICAL NO: 1

Aim :- Study about different Network Analyser. 1) Wireshark 2) NetSim) NS-2 4) Cisco IP Packet Tracer.

WIRESHARK :

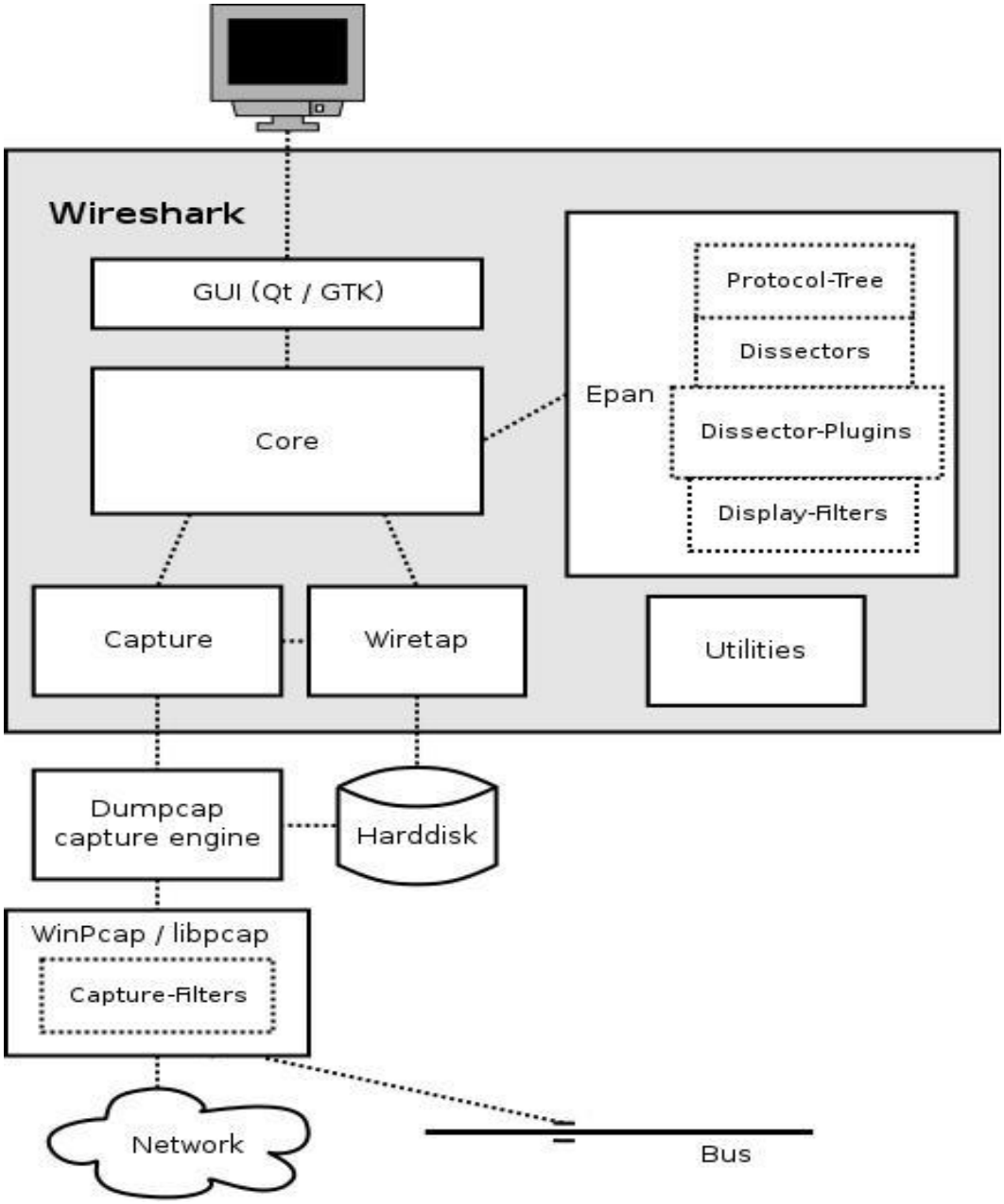
Introduction :

Wireshark was initially developed by Gerald Combs. Wireshark is a free and open source packet analyser. It is used for network troubleshooting, analysis, software and communication protocol development,and education. This analyser was also known as ethereal. On-going development and maintenance of wireshark is handled by the wireshark team, a loose group of individuals who fix bugs and provide new functionality.

Features :

- Wiresharks a data capturing program that understands the stricter of different networking protocol.
- It can describe roles and display the fields, along with their meanings as different networking protocols.
- Wireshark uses pcap (an API used for capturing network traffic) to capture packets, so it can only capture packet on the types of networks that pcap supports.
- Display packets with very detailed protocol information.
- Captured files can be programmtically edited or converted via command-line switches to the
  “editcap” program.
- Capture live packet data from a network interface.
- Wireshark shares many characteristics with tcpdump (prints out a description of the contents of packets on a network interface that match the Boollean expression). The difference is that it supports a graphical user interface (GUI) and has information filtering features.

Working:



For Capturing Of Packet

It takes packets from a network adapter and saves them to a file on your hard disk. Since raw network access requires elevated privileges these function are instead into the dumpcap program . it's only this program that needs these privilege, allowing the main part of the code (dissectors, user interface, etc.) to run with normal user privilege . To hide all the low-level machine dependent details from Wireshark, the libpcap and winpcap libraries are used. These libraries provide a general purpose interface to capture packets and are used by a wide variety of applications.

NETSIM :

Introduction :

Netsim is a discrete event simulator developed by Tetcos, in association with Indian institute of science. Netsim is a network simulation and network emulation tool used for network design & planning defence applications and network R & D. Also, various technologies such as cognitive Radio, Wireless Sensor Networks, Wireless LAN, Wi-Max, TCP,IP,etc. are covered in NetSim. The network emulator Add On Allows users to link netsim to live applicaton running on real devices. This allows for real traffic to flow via the emulator and experience network effects.

Features :

- Network area displaying the network devices with unique device name, ip address, port number and protocols supported.
- Supports SNMP version, TLI, TFTP client and server, FTP client, Telnet, Cisco ISO Software, Simulation, SSH, IPv4 and IPv6 address for all the above protocols.
- Option to configure unique OID values While creating a Network.
- Modification of IP address, ports of all selected devices in the network can be done.
- Also, View the properties of individual devices in the network from the network tree of from the network area.

Working :

By drag and drop of devices from device tree, adding bulk devices same type using network design wizard, adding bulk devices of devices of different devices types, adding new devices individually or in bulk, to existing network.

Ns-2:

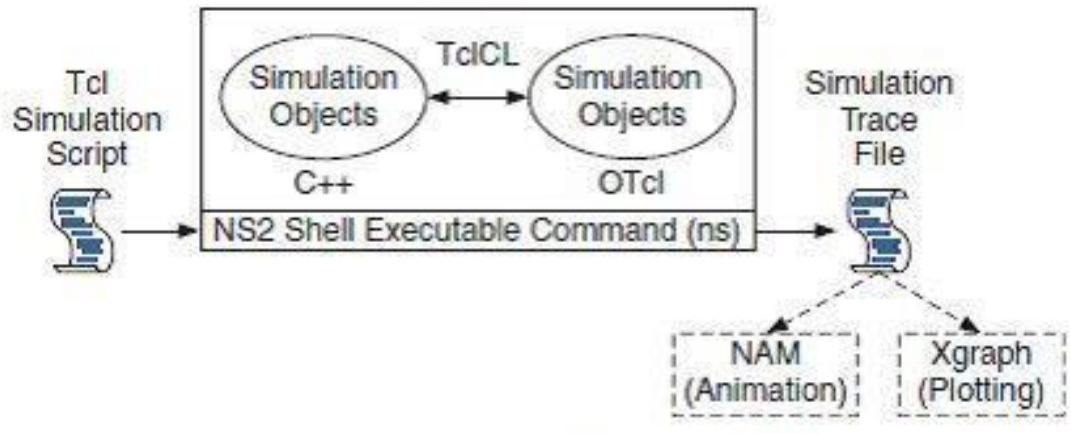
Introduction :

NS2 stand for network Simulator Version 2. It is an open-source event-driven simulator designed specifically for research in computer communication networks. NS2 consists of two key language C++ and object-oriented Tool Command Language (O Tel).While the C++ defines the internal mechanism (i.e a backend) of the simulation object, the OTel set up simulation by assuming and configuring the object as well as scheduling discrete events. The C++ and OTel are linked together using TelCL.

Features :

- It is a discrete event simulator for networking research.
- It provides substantial support to simulate bunch of protocols like TCP, UDP, FTP, HTTP and DSR.
- It simulates wired and wireless network.
- It is primarily Unix based.
- Uses TCL as its scripting language.
- Otcl : Object oriented support.
- Tclcl : C++ and otcl linkage.
- Discrete event scheduler.

Working :



Basic architecture of NS.

Advantages :

1. Cheap- Does not require costly equipment.
2. Complex scenarios can be easily tested.
3. Results can be quickly obtained- more ideas can be tested in a smaller time frame.
4. Supported protocols
5. Supported platforms
6. Modularity
7. Popular

Disadvantages :

1. Real system too complex to model. i.e complicated structure.
2. Bugs are unreliable.

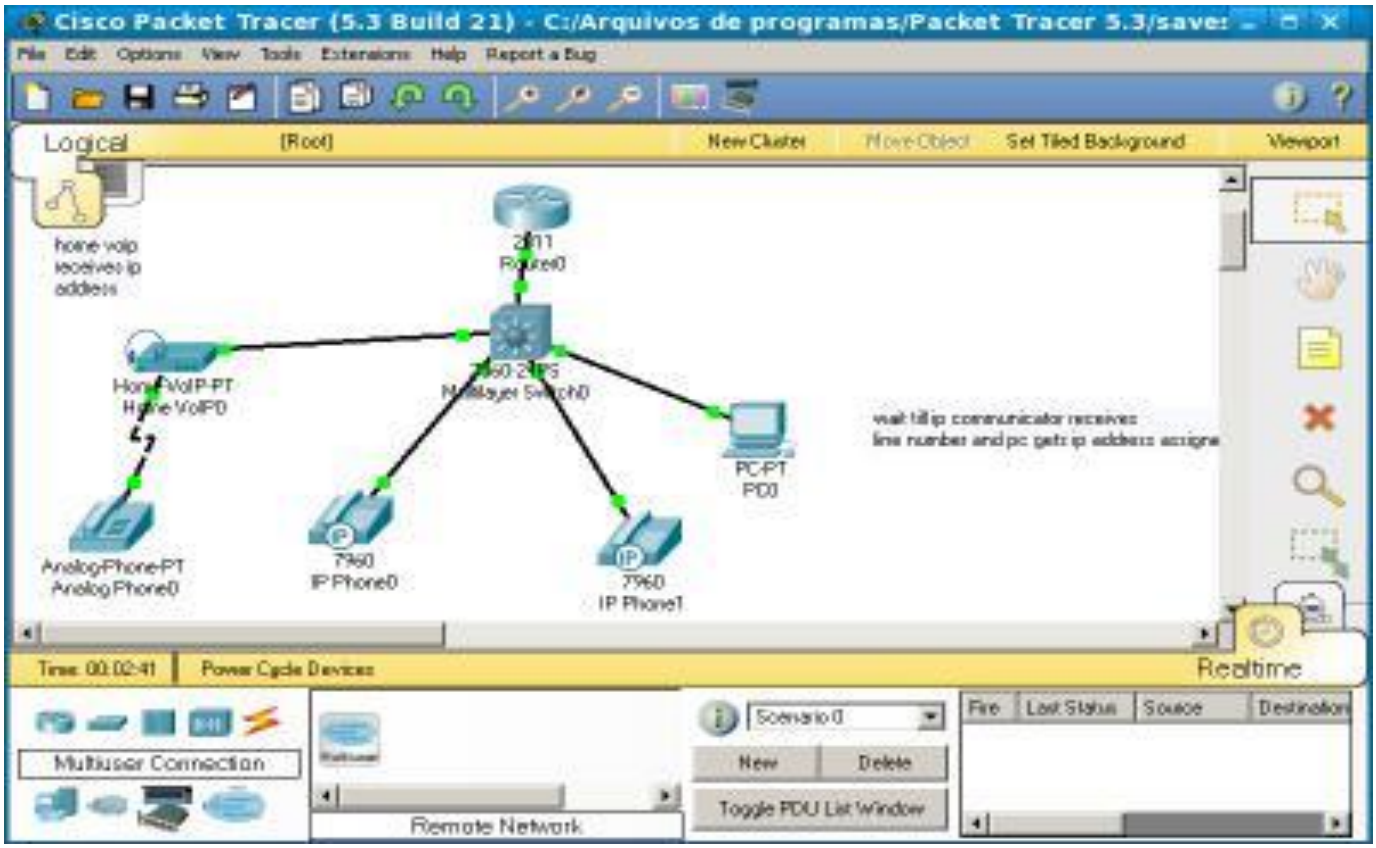
CISCO IP PACKET TRACER :

Cisco packet tracer is a network-capable application, with a multiuser peer-to-peer mode that allows collaborative construction of virtual network over a real network. Packet tracer is a cross-platform visual simulation tool designed by Cisco system that allows users to create network topologies and imitate modern computer network. The software allows users to simulate the configuration of cisco router and switch using a simulated command line interface. Packet tracer makes use of a drag and drop user interface, allowing users to add and remove simulated network devices as they see fit.

Features :

- Graphical representations visually simulate hardware.
- Offer the ability to insert interface cards into modular routers and switch, which then becomes part of the simulation.
- Multi-user functionality enables exciting collaborative and competitive interactions, providing the option to progress from individual to social learning and features social networking, and gamming.
- Providing a visual demonstration of complex technologies and configurations.

Working :



In order to create a topology, we will have to select some of the devices and put them in our main windows i.e the white portion of packet tracer. And here how it looks after we add the devices(in above fig).Now,we will have to connect these devices and for that we use cables. And after you successfully create the topology, you can check either the traffic is flowing or not selecting the packet from right panel and putting it on the both PCs.

Conclusion : Various information about different network analyser has been acquires through this practical.

PRACTICAL NO: 2

Aim :- Study about Crimping and IP Address.

CRIMPINGTOOL:

Introduction :

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 cable are created using a crimping tool (show below) to join the RJ-45 and RJ-11 connectors to the both ends of either phone or CAT5 cable.

How to Use Crimping Tool:

To use this crimping tool, each wire is first placed into the connector. Once all the wires are in the jack, the connectors 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 connector.

Diagram:

Application :

1. Crimping is most extensively used in metalworking.
2. Crimping is commonly used to fix bullets in their cartridge cases, for rapid but lasting electrical connections, securing lids on metal food cans, and many other applications. Because it can be a cold-working technique.
3. Crimping can also be used to form a strong bond between the work piece and a non-metallic component.

Types of Wires :

There are mainly 5 types of wire:

1. **Triplex Wires :**Triplex wires are usually used in single-phase service drop conductors, between the power pole and weather heads. They are composed of two insulated aluminum wires wrapped with a third bare wire which is used as a common neutral. The neutral is usually of a smaller gauge and grounded at both the electric meter and the transformer.

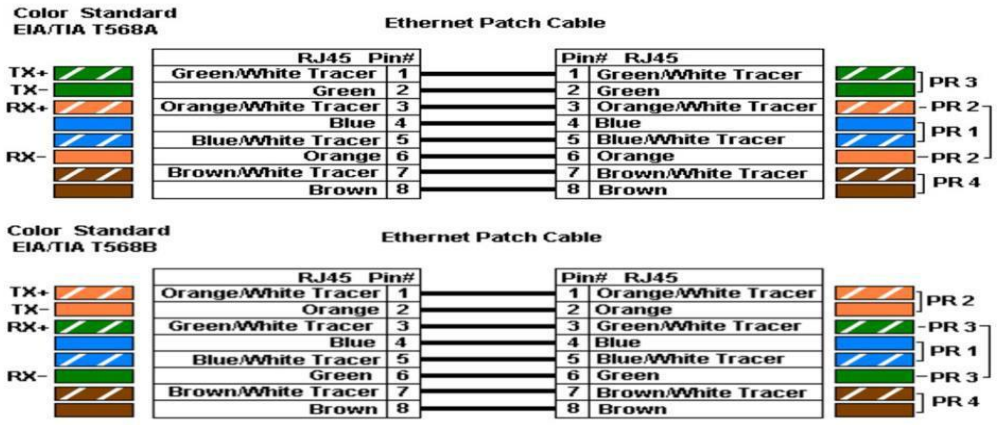
2. **Main Feeder Wires :** Main power feeder wires are the wires that connect the service weather head to the house. They're made with stranded or solid THHN wire and the cable installed is 25% more than the load required.

3. **Panel Feed Wires :** Panel feed cables are generally black insulated THHN wire. These are used to power the main junction box and the circuit breaker panels. Just like main power feeder wires, the cables should be rated for 25% more than the actual load.

4. **Non-Metallic Sheathed Wires :**Non-metallic sheath wire, or Romex, is used in most homes and has 2-3 conductors, each with plastic insulation, and a bare ground wire. The individual wires are covered with another layer of non-metallic sheathing. Since it's relatively cheaper and available in ratings for 15, 20 and 20 amps, this type is preferred for in-house wiring.

5. **Single Strand Wires :** Single strand wire also uses THHN wire, though there are other variants. Each wire is separate and multiple wires can be drawn together through a pipe easily. Single strand wires are the most popular choice for layouts that use pipes to contain wires.

Combination of Wire:



RJ-45 – The Connector:

A registered jack (RJ) is a standardized physical network interface for connecting telecommunications or data equipment. The physical connectors that registered jacks use are mainly of the modular connector and 50-pin miniature ribbon connector types. The most common twisted-pair connector is an 8-position, 8-contact (8P8C) modular plug and jack commonly referred to as an RJ45 connector.

An 8-pin/8-position plug or jack is commonly used to connect computers onto Ethernet-based local area networks (LAN).Two wiring schemes–T568A and T568B–are used to terminate the twisted-pair cable onto the connector interface.

Ethernet cables and 8P8C connectors are crimped into the wiring pattern to function. 8P8C can be used with other types of connections besides Ethernet; it is also used with RS-232 serial cables, for example. Because RJ45 is by far the predominant usage of 8P8C. Industry professionals use those two terms interchangeably.

Traditional dial-up moderns used a variation of RJ45 called RJ45s which features only 2 contacts (8P2C configuration) instead of eight. The close physical similarity of RJ45 and RJ45s made it difficult for an untrained eye to tell the two apart.

What is IP?

An IP address is a fascinating product of modern computer technology designed to allow one computer (or other digital device) to communicate with another via the Internet. IP addresses allow the location of literally billions of digital devices that are connected to the Internet to be pinpointed and differentiated from other devices. In the same sense that someone needs your mailing address to send you a letter, a remote computer needs your IP address to communicate with your computer.

Range and Classes of IP :

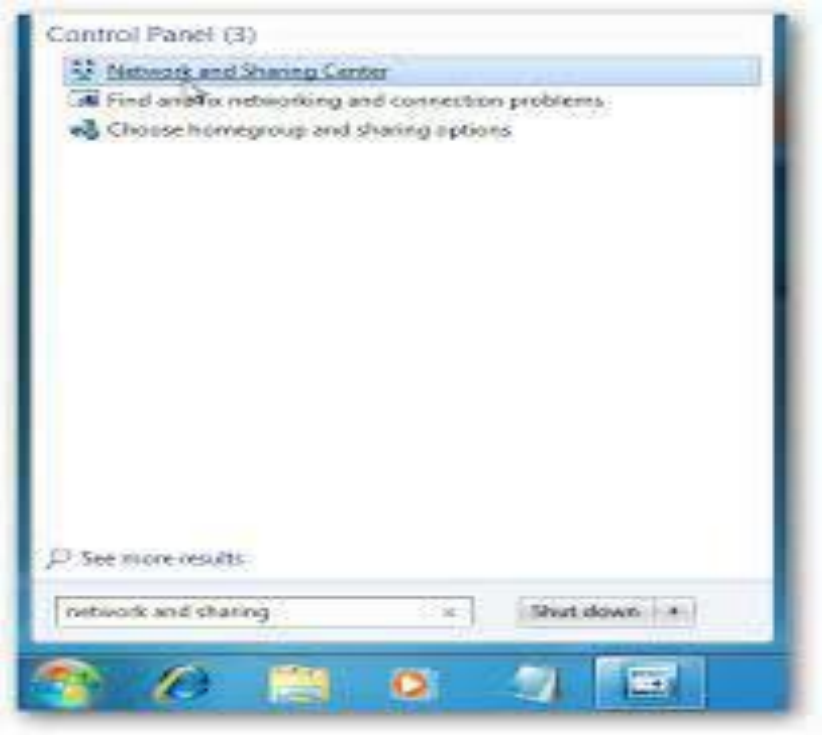
Class	1st Octal Decimal Range	Network/Host Id(N=Network, H=Host)
A	1-126	N.H.H.H
B	128-191	N.N.H.H
C	192-223	N.N.N.H
D	224-239	Reserved for Multicasting
E	240-254	Experimental;used for research

How to Give an IP Address?

For Windows 7,8.x or 10

Step 1:

To change the computer's IP address in Windows , type network and sharing into the Search in the Start Menu and select Network and Sharing Center when it comes up. If you are in Windows 8, it will be on the Start Screen itself, like the screenshot at the top of this articles. If you are in Windows 7 or 10 it'll be in the start menu.

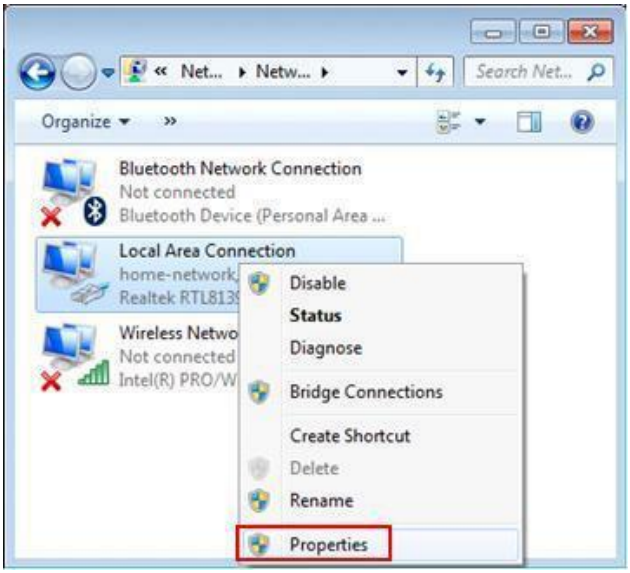


Step 2:

Then when the Network and Sharing Center opens, click on Change adapter settings. This will be the same on Windows 7,8.x or 10.

Step 3 :

Select the Local area connections, right click it and select **Properties**



Step 4:

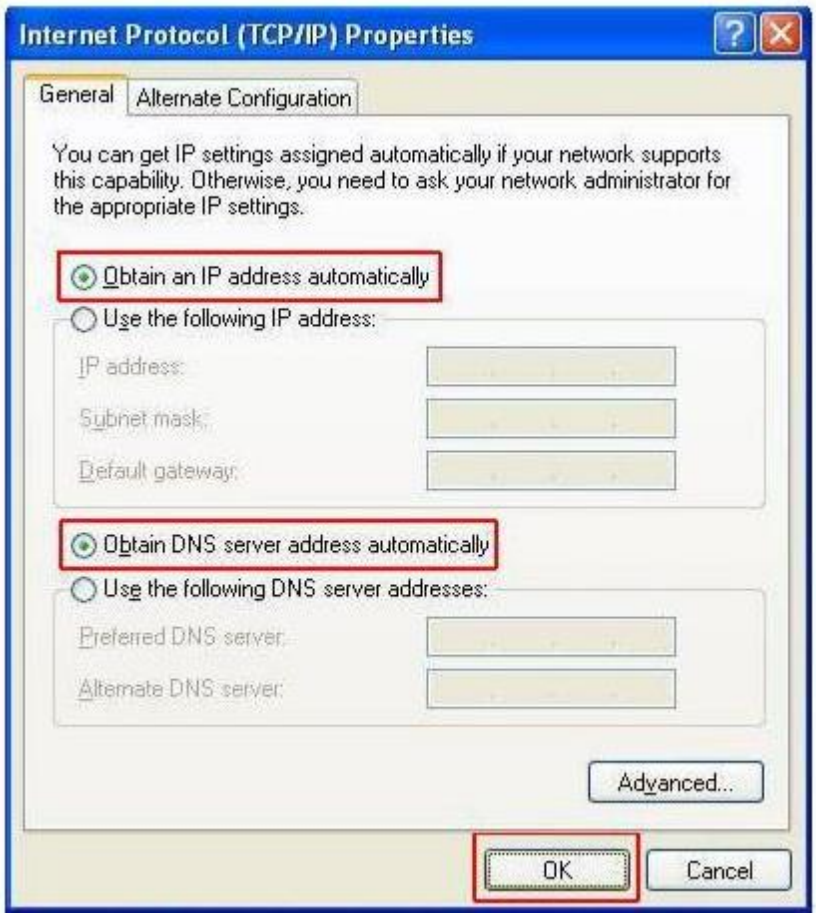
Select **Internet Protocol Version 4(TCP/IPv4),** double click it or click **Properties.**

Step 5:

There are two ways to configure the TCP/IP protocol below:

1. Assigned by DHCP Sever :

Select Obtain an IP address automatically and Obtain DNS Server address automatically, as shown in the figure below. These may be selected by default. Then click OK to save setting.



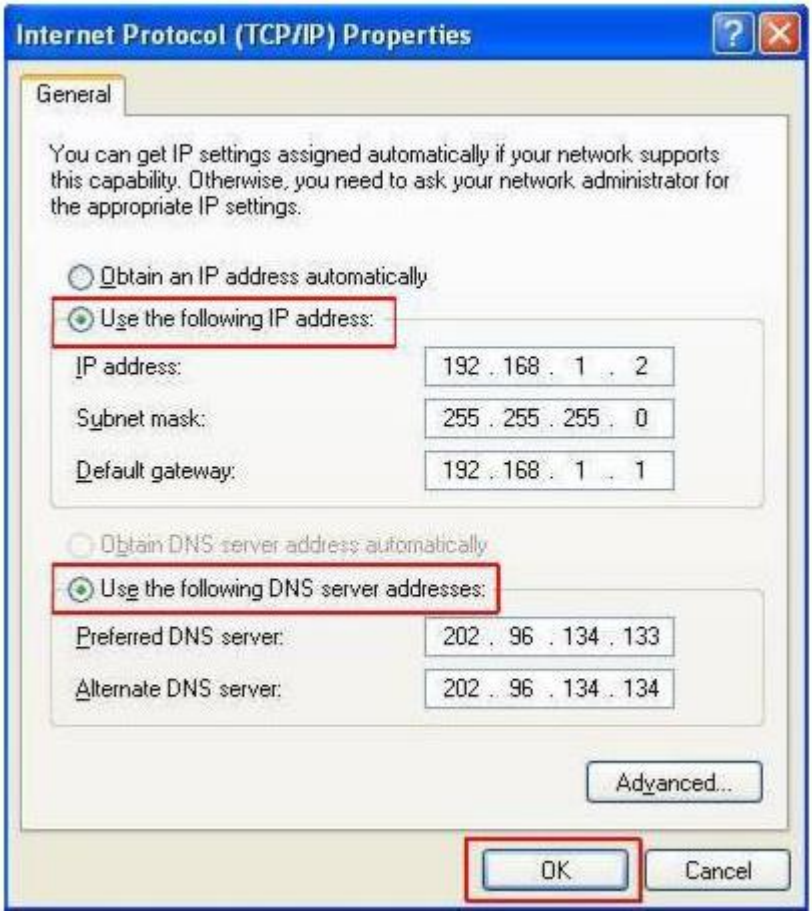
2.Assigned manually :

1) Select Use the following IP address, as shown in the following figure.

If the router's LAN IP address is 192.168.1.1, please type in IP address 192.168.1.x （x is from 2 to 253）, subnet mask 255.255.255.0, and default gateway 192.168.1.1.

2) Select Use the following DNS server addresses, as shown in the following figure. And then type the DNS server IP address, which should be provided by your ISP. Finally remember to click OK to save settings.

3) Note: In most cases, type your local area DNS server IP addresses into it. The Preferred DNS server is same to default gateway. For Secondary DNS server, you could leave it blank or type in 8.8.8.8.



Step 6:

Click OK to save and apply your settings.

Conclusion : From this practical, we can get the information about crimping tool, types of wire, range and combination of wire and also one can give IP address to device.

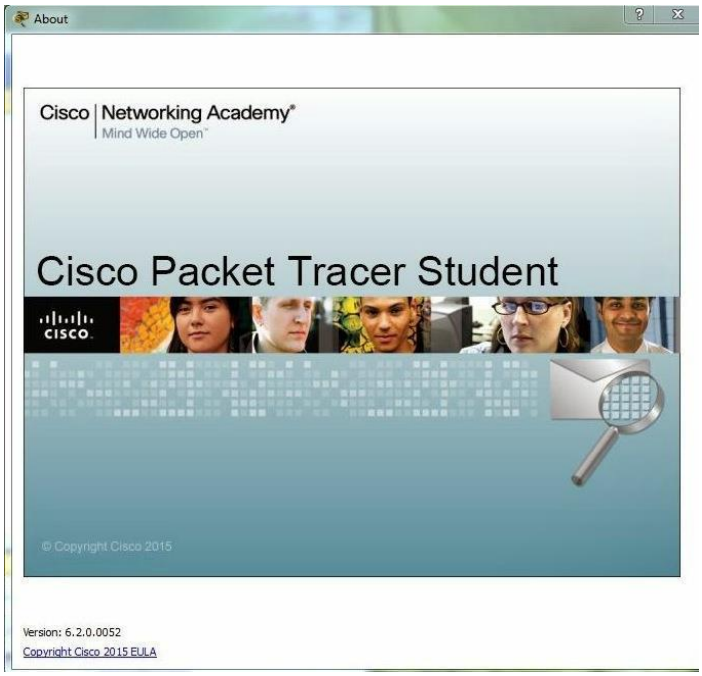
Practical No: 3

Aim: Study about CISCO IP Packet Tracer and different scenario.

❖ About IP Packet Tracer:

Packet Tracer is a cross-platform visual simulation program designed by Cisco Systems that allows users to create network topologies and imitate modern 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 user interface, allowing users to add and remove simulated network devices as they see fit.

Packet Tracer allows students to design complex and large networks, which is often not feasible with physical hardware, due to costs.



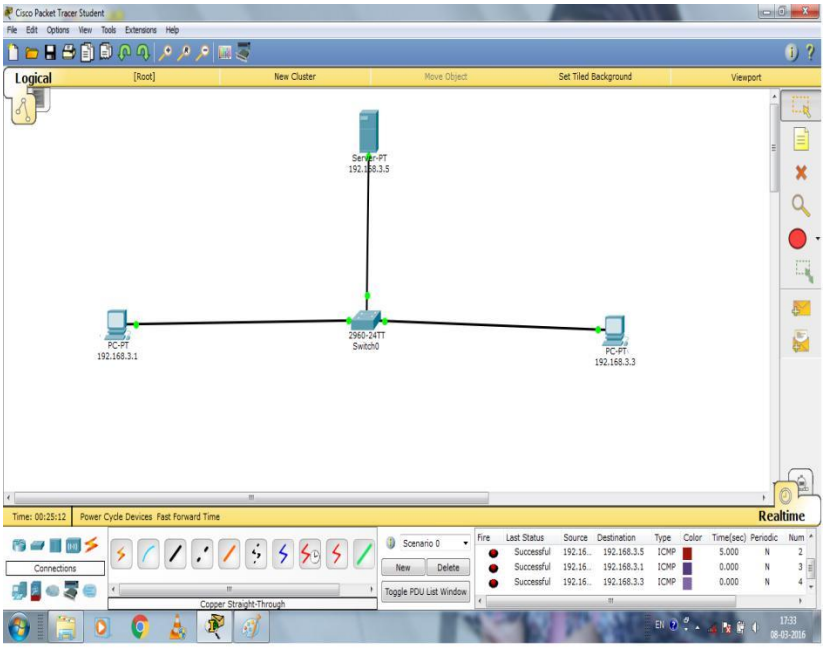
❖ Scenario-I

The diagram shows the simple network in which we have used two personal computers they are also called nodes, and a switch and a server. For communication between two nodes we have to establish connection between them. To establish the connection we have used cables. Here PC1 and and PC2 are connected with the switch and switch is directly connected to the server. Switch is used as an intermediate device between the nodes and the server.

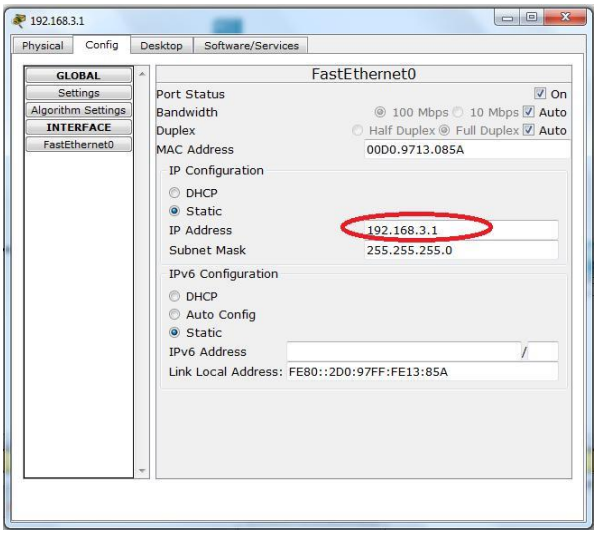
Implementation of scenario-I

Now we have to configure the system and the steps are given below:

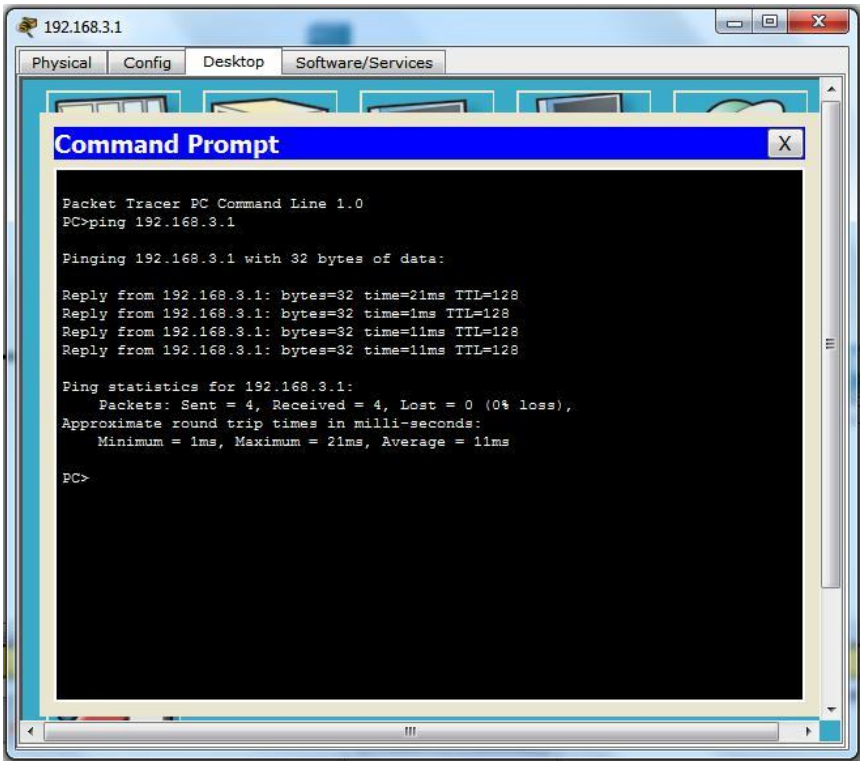
- Make simple network through drag and drop which shown in below screenshot .
- After that, right click below the device and give IP address to all devices.



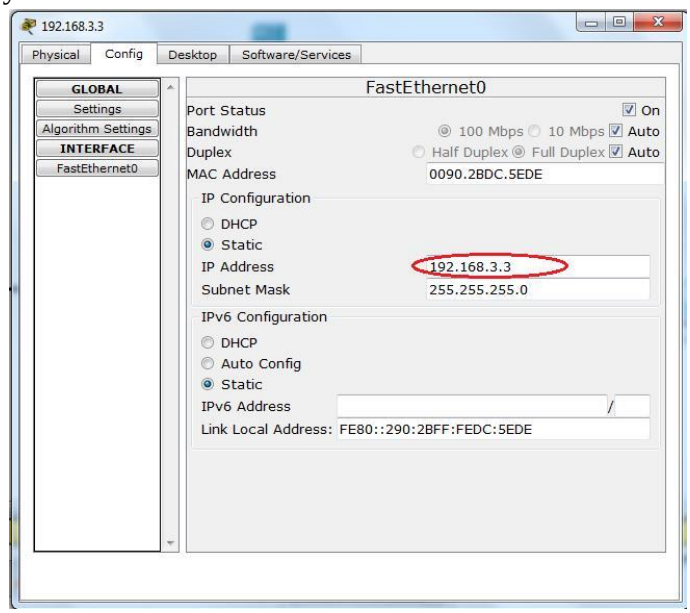
- Now IP configuration of PC1 double click on that device
- Then in “Config” option you can see “IP address” with blank box, write PC1’s ip address, which you can see below



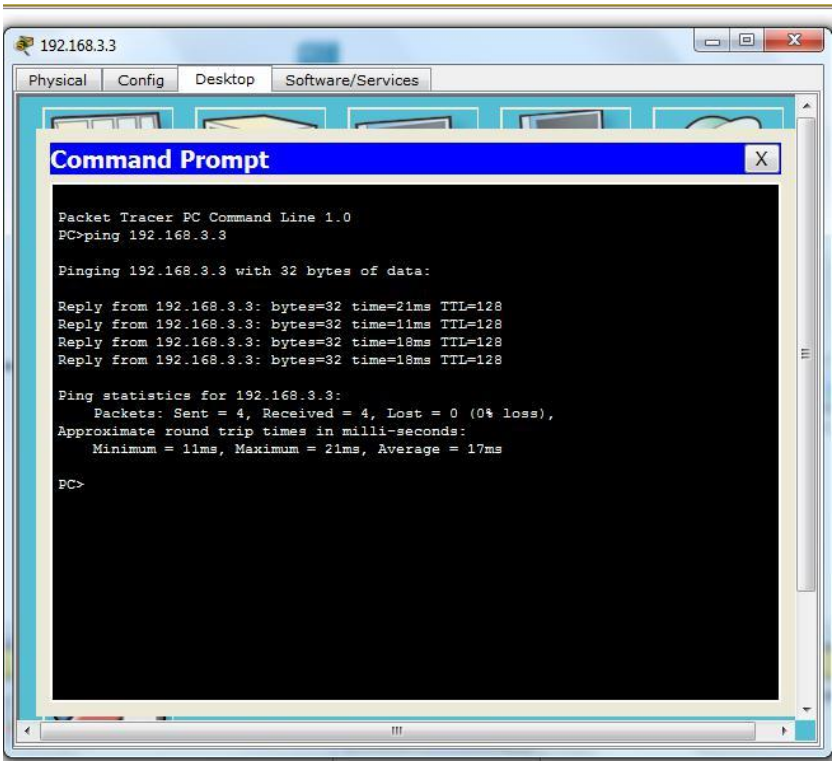
- Double click on PC1 then from the “Desktop” choose ”Command Propt” option click on that you can see below terminal
- Write into terminal “ping 192.168.3.1” IP of PC1 then prees “Enter”
- Then you can get output which shown below



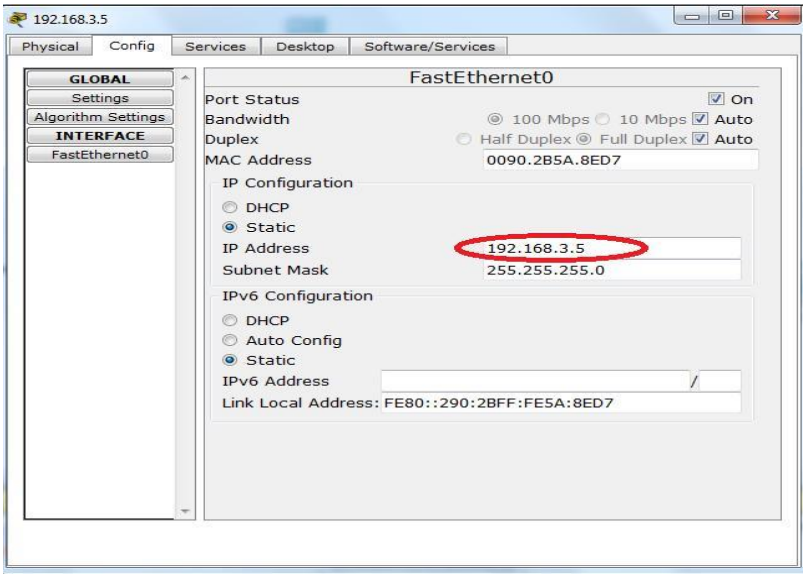
- Now IP configuration of PC2 double click on that device
- Then in “Config” option you can see “IP address” with blank box, write PC2’s IP address, which you can see below



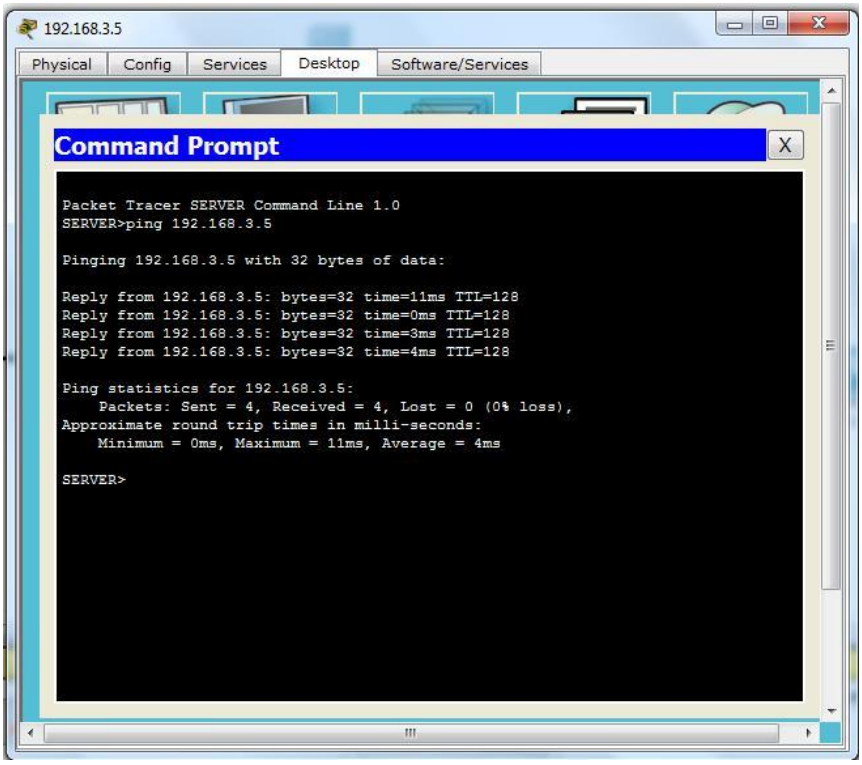
- Double click on PC2 then from the “Desktop” choose ”Command Propt” option click on that you can see below terminal
- Write into terminal “ping 192.168.3.3” IP of PC2 then press “Enter”
- Then you can get output which shown below



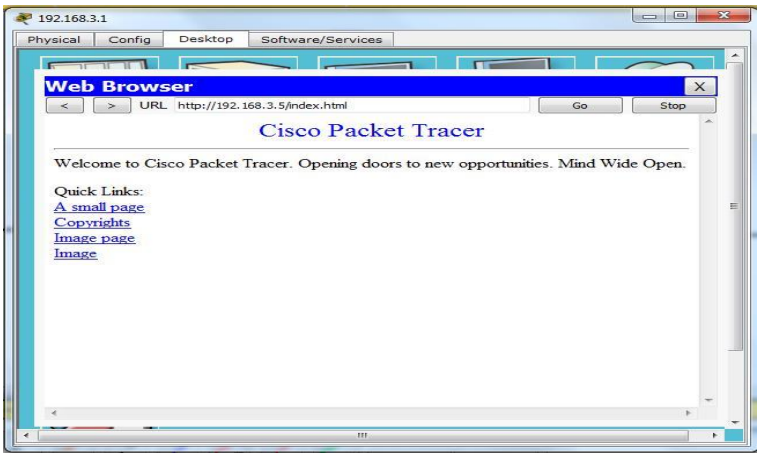
- Now IP configuration of server double click on that device
- Then in “Config” option you can see “IP address” with blank box, write server IP address then press “Enter”



- Now go to “Desktop” option you can see the dialog box.
- From above dialog box click on “Command Propt ” and open, after that write in terminal ”ping 192.168.3.5” which is IP of your sever then press “Enter”
- Then you can get output which shown below



- Now for ensuring that your network is working or not for that double click on pC1,yopu can see the be dialog box then from “Desktop” click on “Web Browser”
- After click on “Web Browser” you can see the dialog box like web page
- In the URL write “192.168.3.1” and press “Enter”
- After pressing Enter you can get the particular service
- If you get the service like shown below screenshot then your network is successfully working !!!



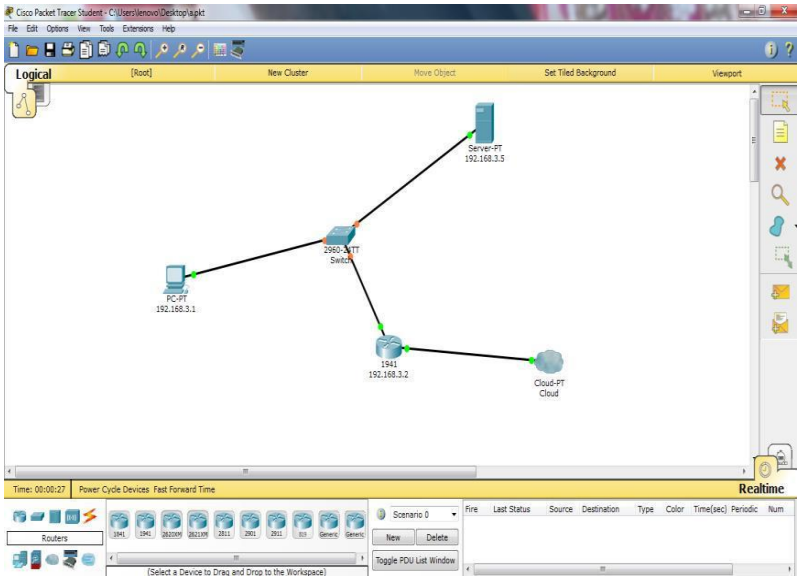
❖ Scenario-II

In the second scenario, here we have made a network. In which we take PC, Router, switch, sever and cloud. Using this components we made the below network. In additional here we used cloud and router .All this components are connected to each other.

❖ Implementation of scenario-II

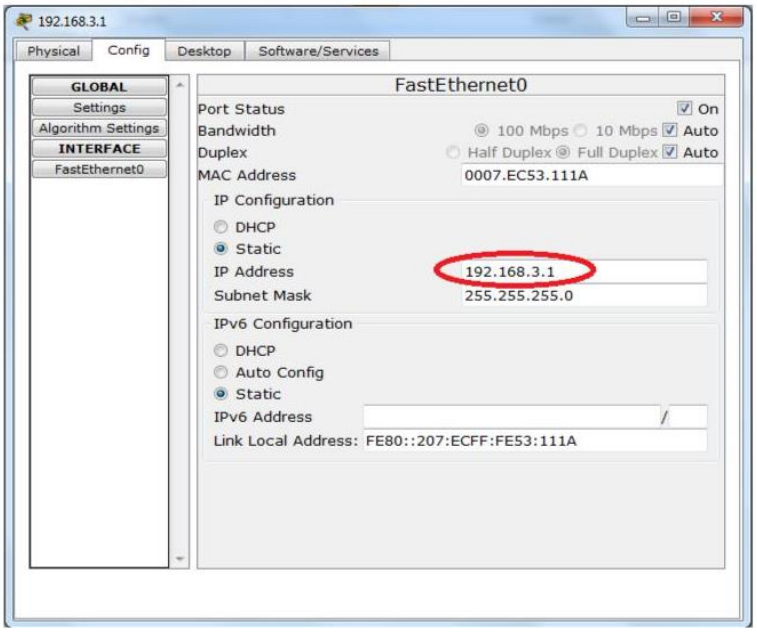
Now we have to configure the system and the steps are given below:

- Make simple network through drag and drop which shown in below screenshot.
- After that, right click below the device and give IP address to all devices.

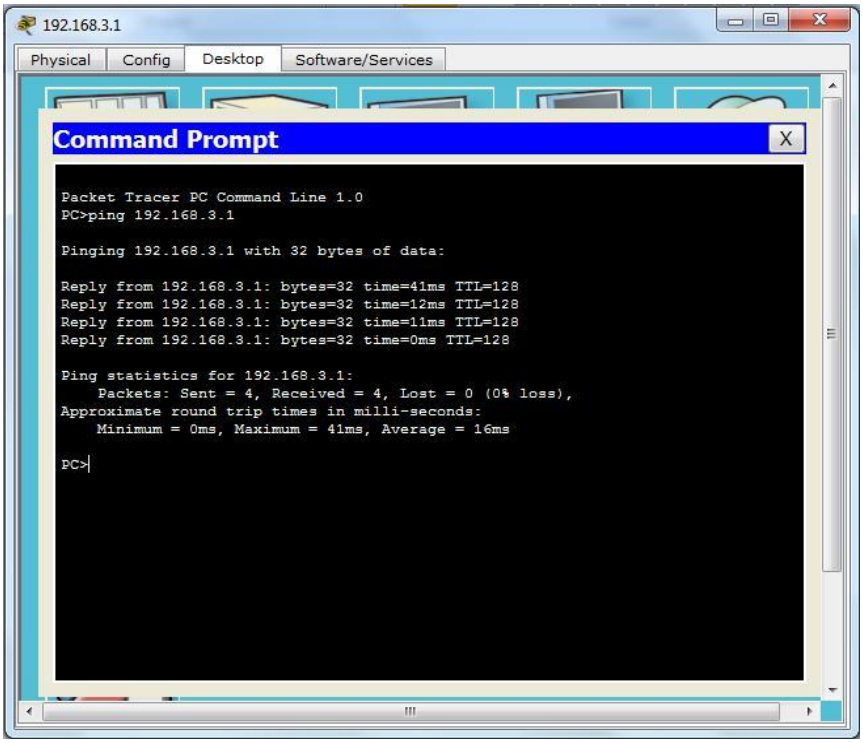


- Now double click on the PC, so one dialog box you can see like below. after that write the IP of that

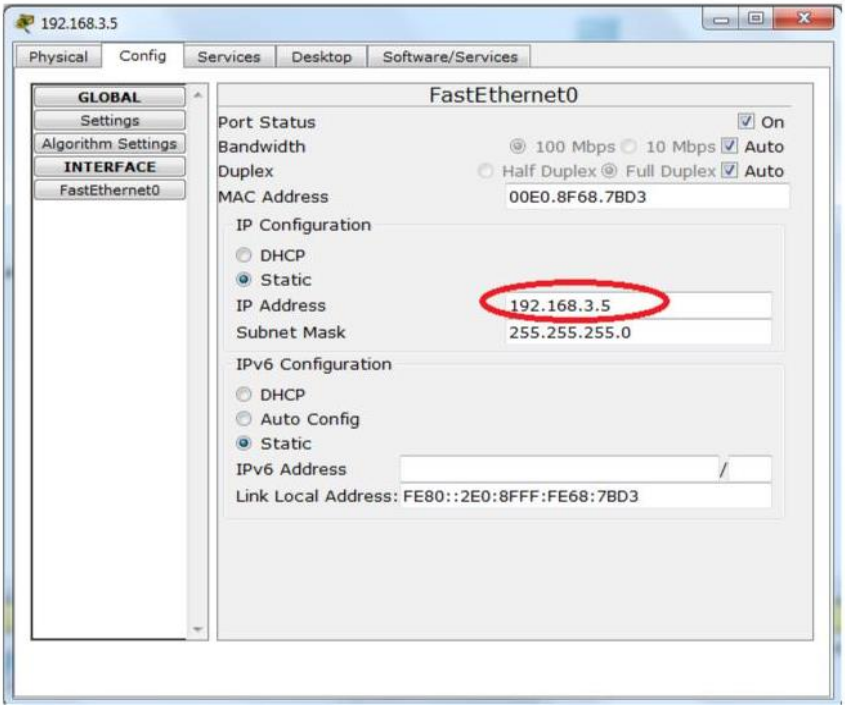
  PC into “IP Address”. The press “Enter’.



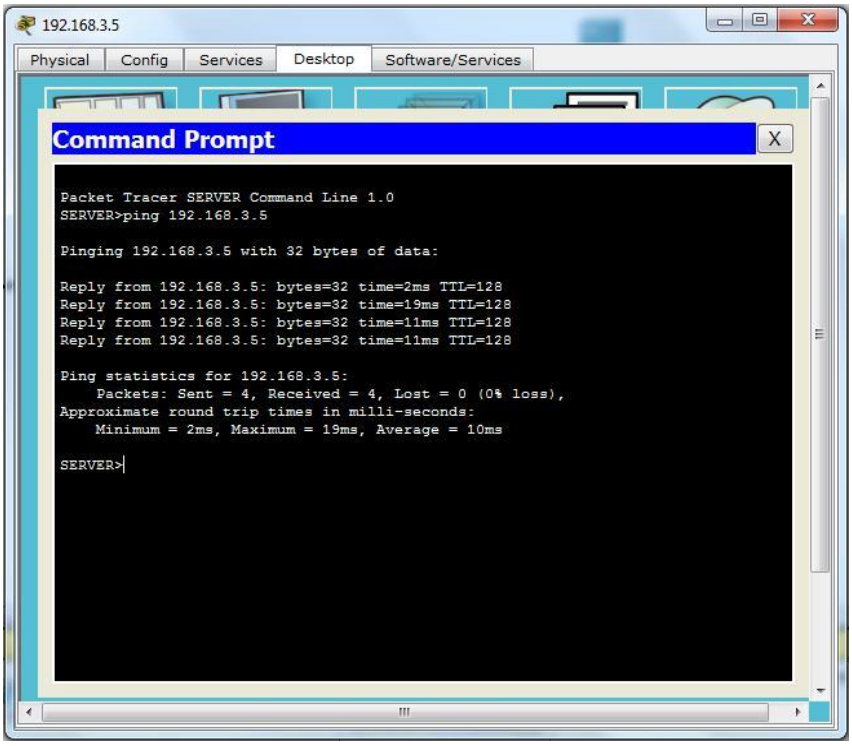
- After that from the “Desktop” choose “Command prompt” write “ping 192.168.3.1” and press “Enter”.



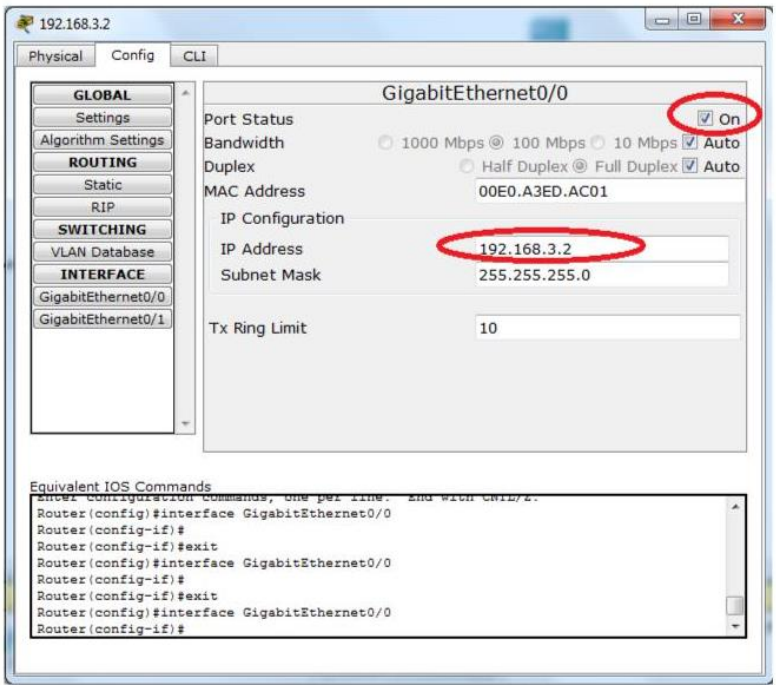
- Now same as above do to the server and write Server IP address.



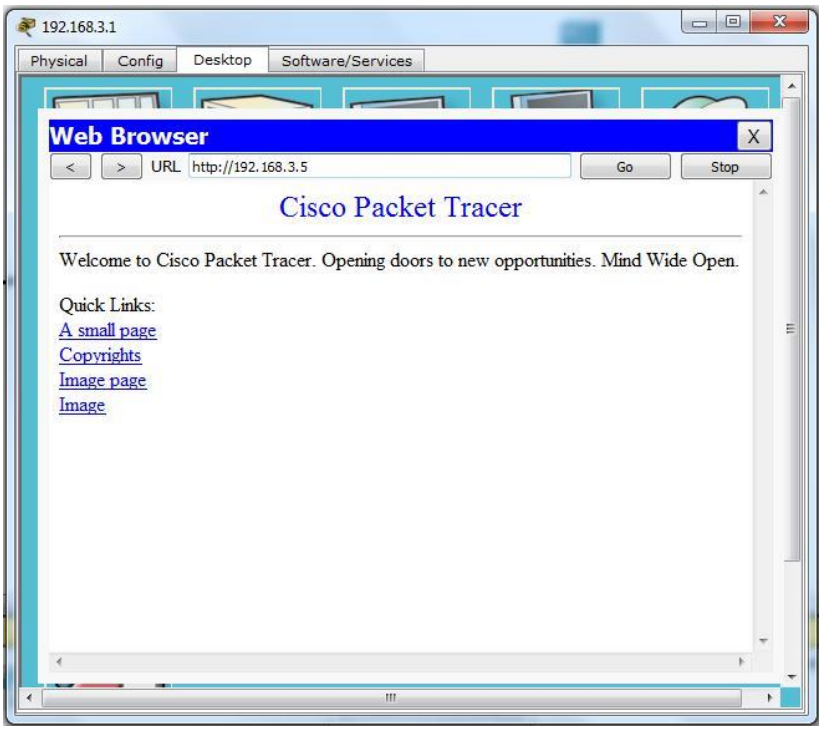
- After that write “ping 192.168.3.5” and press “Enter”.



Now, double click on Router and write IP into “IP Address” then click “ON”.



➢ After the configuration of all device at the end write the URL of server and you got the webpage like below:



- **Conclusion:**

By performing the above scenario, we are able to create virtual networks on IP Packet Tracer to distinguish the real network scenario.

PRACTICAL:04

AIM: - Creating Bus, Mesh and star Topology using Cisco IP packet Tracer

Theory:-

Bus Topology :It is a specific kind of network **topology** in which all of the various devices in the network are connected to a single cable or line. In general, the term refers to how various devices are set up in a network.

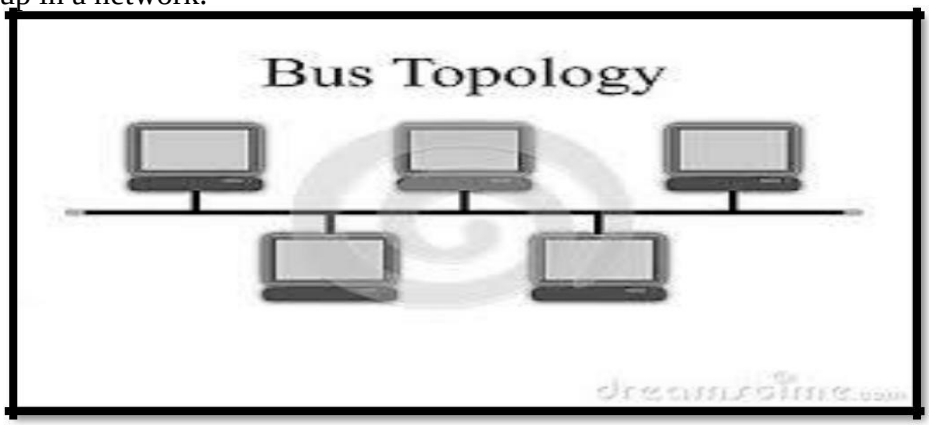
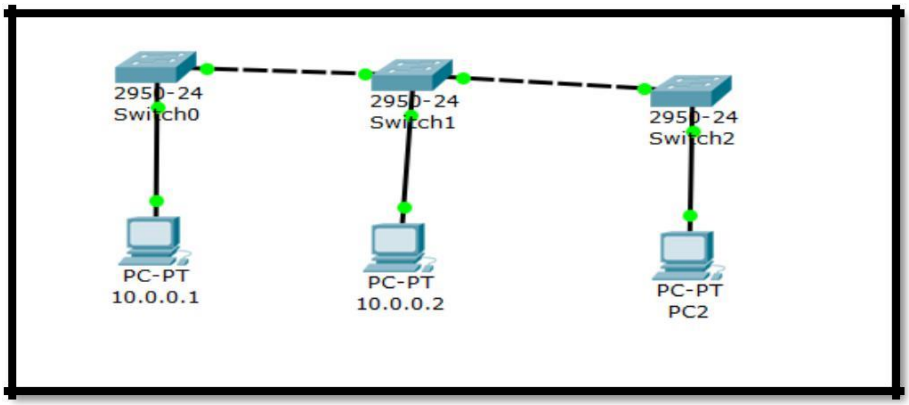


Figure: General Diagram

Practical Implementation:



Procedure:

1. First of all understand the environment of BUS topology and according to that design the system.
2. Take 3 generic system.
3. Take 3 Switches.
4. Connect those 3 systems with 3 switches using cables.

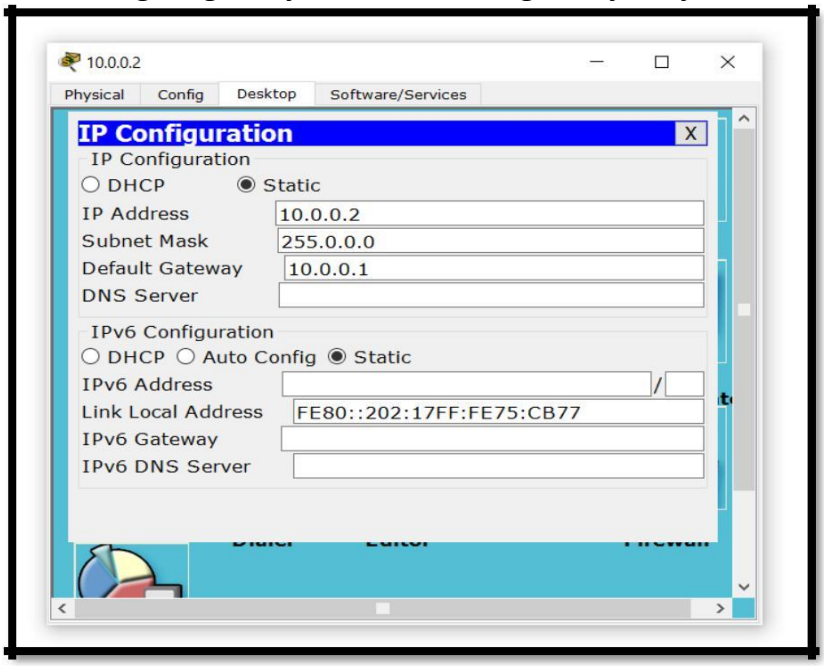
5. Configure each system by providing the IP address.

a. IP of system 1 :- 10.0.0.1

b. IP of system2 :- 10.0.0.2

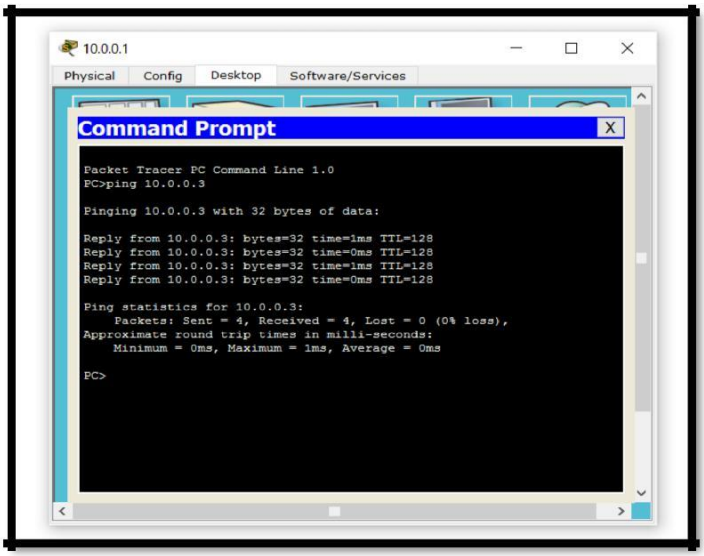
c. IP of system3 :- 10.0.0.3

6. After configuring the system, set default gateway of system 2 and system 3.

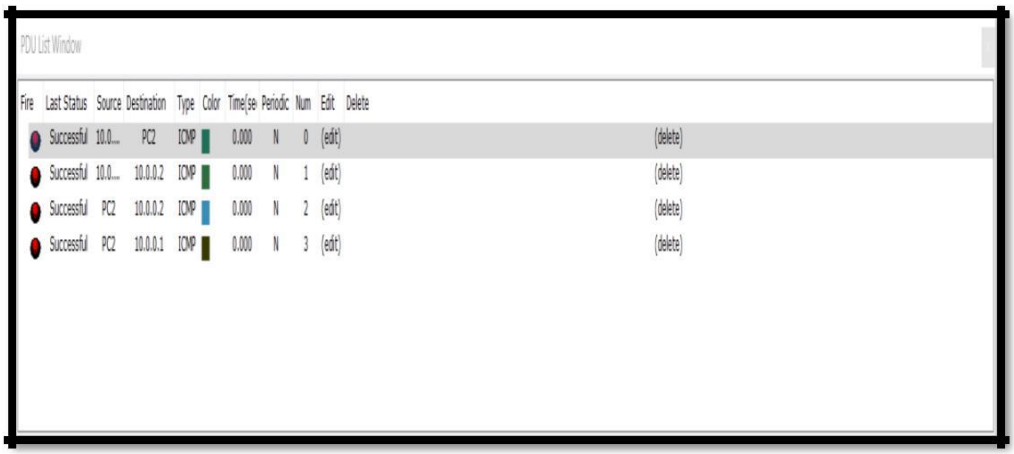


Default gateway is used to fetch or to get the service from the main system which is somewhere responsible for connecting the two different devices so that message or any other service request can be transmit from one device to other.

7. Once the gateway is set, to check whether it is successful connected or not we are going to use the ping command.



- After pinging to particular IP address if we get the response than it states that connection between the devices are successful, and now we are going to start sending the packet from one device to other.
- If the message sending from source to destination is successful, than we can able to take the readings as followed in figure: we can see the status packet delivery from different sources to different destination
- From above figure we can state that the connection is successful than the message can be delivered successful.



Mesh Topology: A **mesh** network is a network **topology** in which each node relays data for the network. All **mesh** nodes cooperate in the distribution of data in the network. **Mesh** networks can relay messages using either a flooding technique or a routing technique.

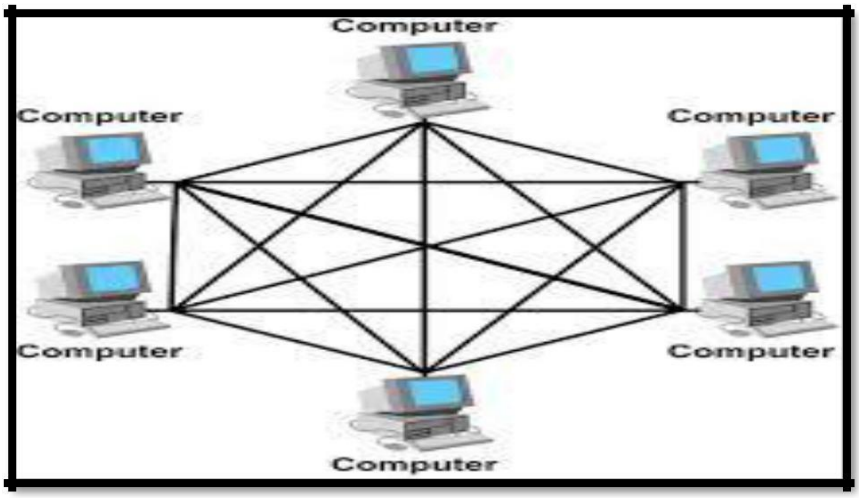


Figure : General Diagram

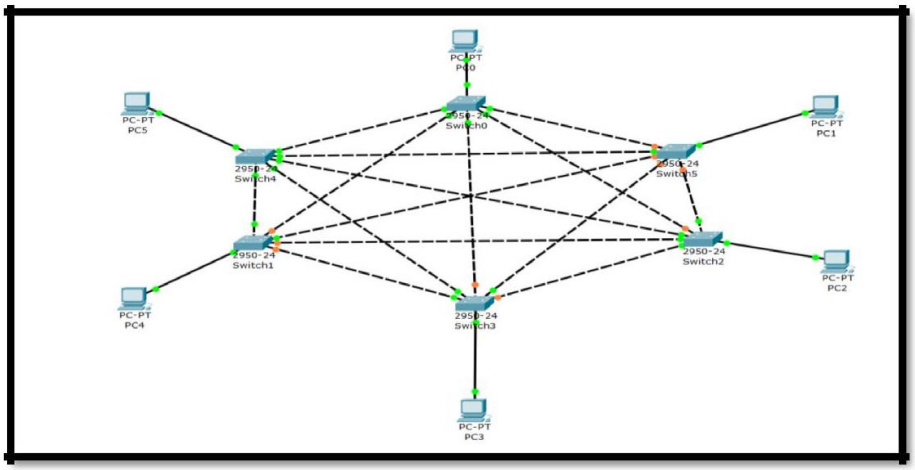


Figure : Network Diagram

Procedure:

1. Take 6 switches.
2. Arrange each of them in such a way that they form star.
3. After connection of all switches take 6 system each of them connected with one switch.
4. Now start configure the system by giving them IP and the address to Fast Ethernet for the communication purpose.

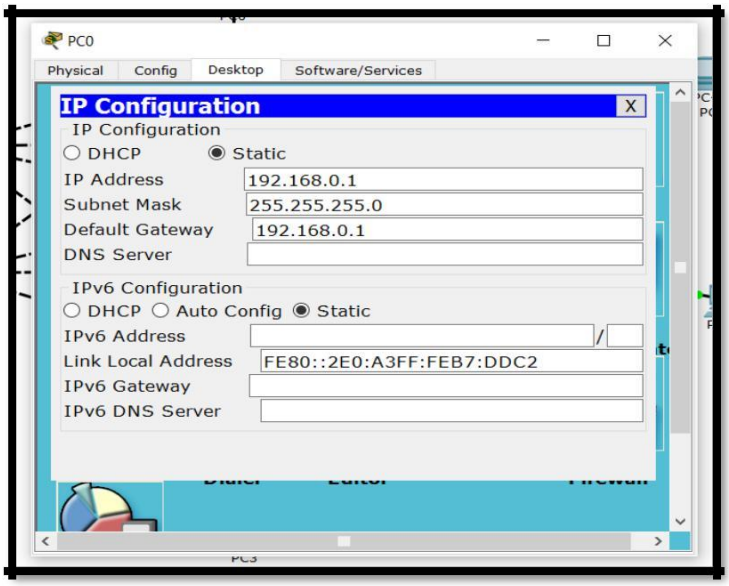


Figure : Configuration of PC

5. Configure all the system same way as shown in above figure.
6. After configuration start pinging to any system by using its IP.
7. If the pinging is successfully done than check the link by sending the packet, if the packet send successfully one can take the reading from the **simulation** option.

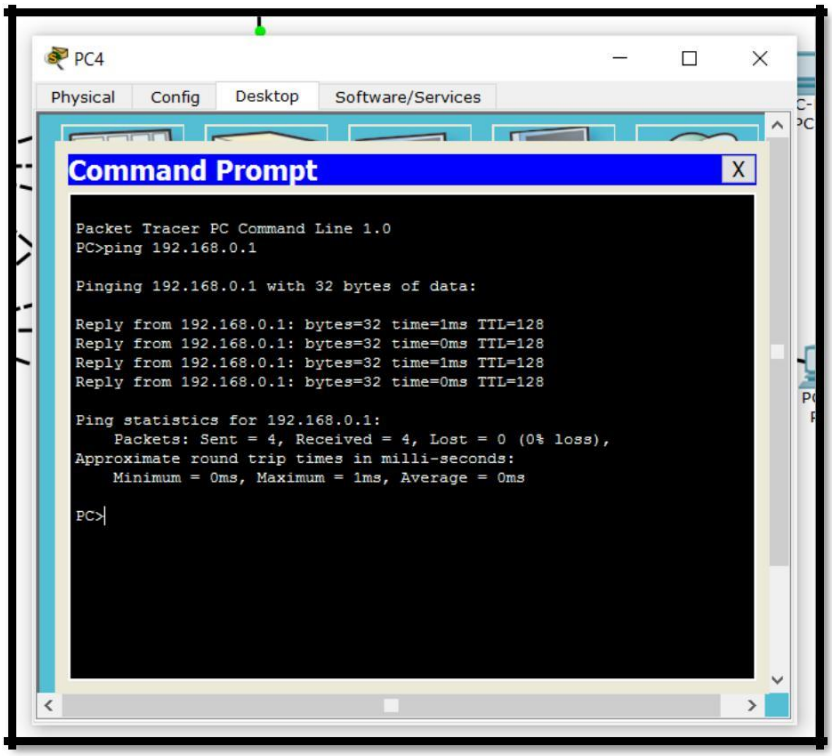


Figure: Shows the Pinging command to the Particular system.

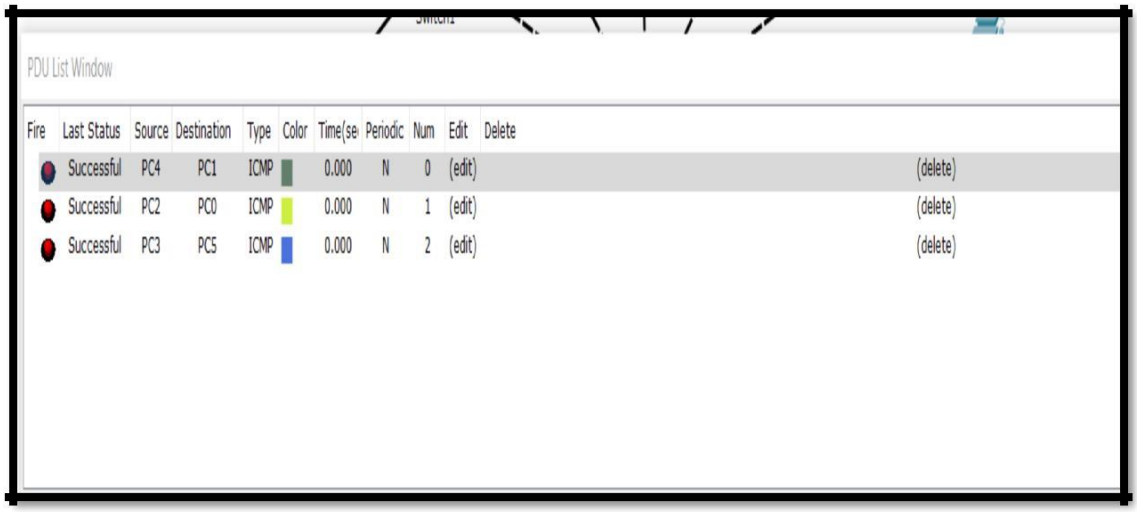


Figure: Shows the Successful status while sending the packet from different sender to different receiver

Star Topology: A **star topology** is a **topology** for a Local Area Network (LAN) in which all nodes are individually connected to a central connection point, like a hub or a switch. A **star** takes more cable than e.g. a bus, but the benefit is that if a cable fails, only one node will be brought down

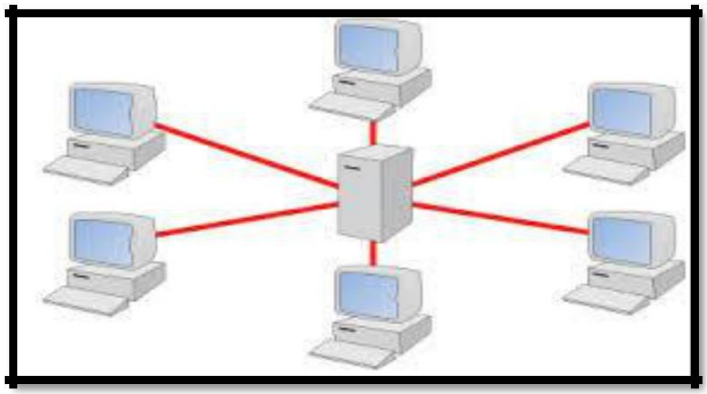


Figure: - General Diagram

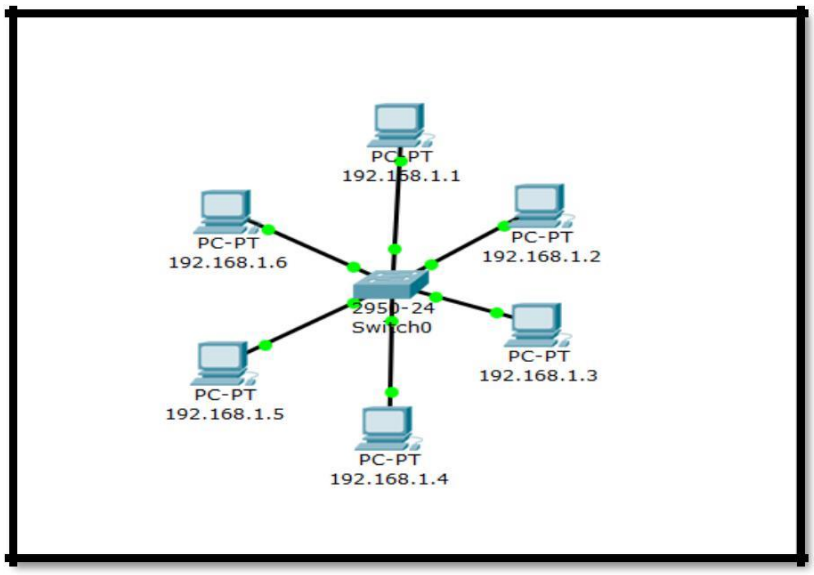
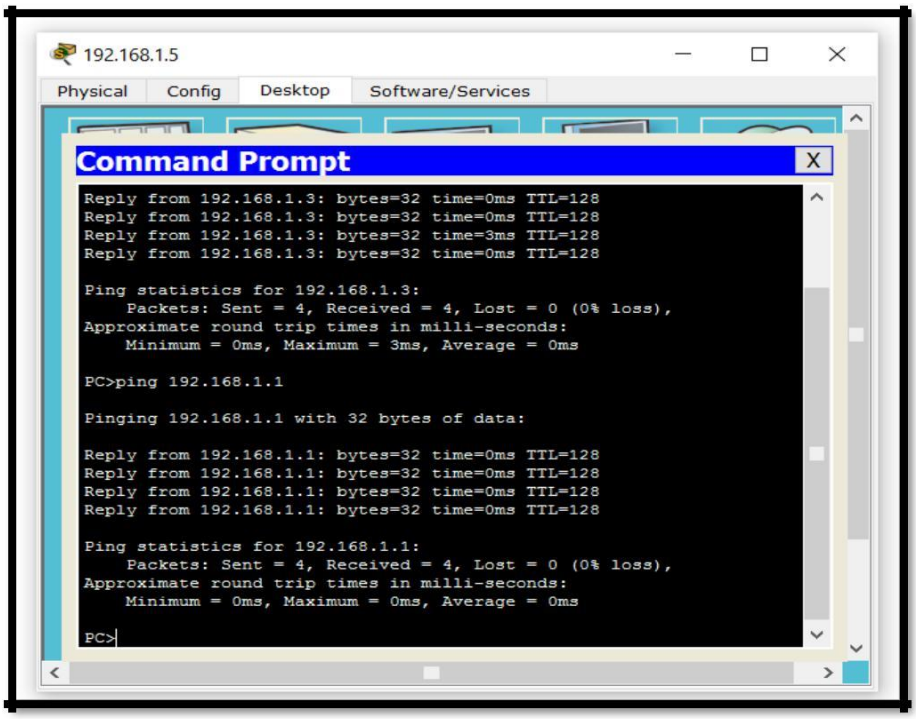


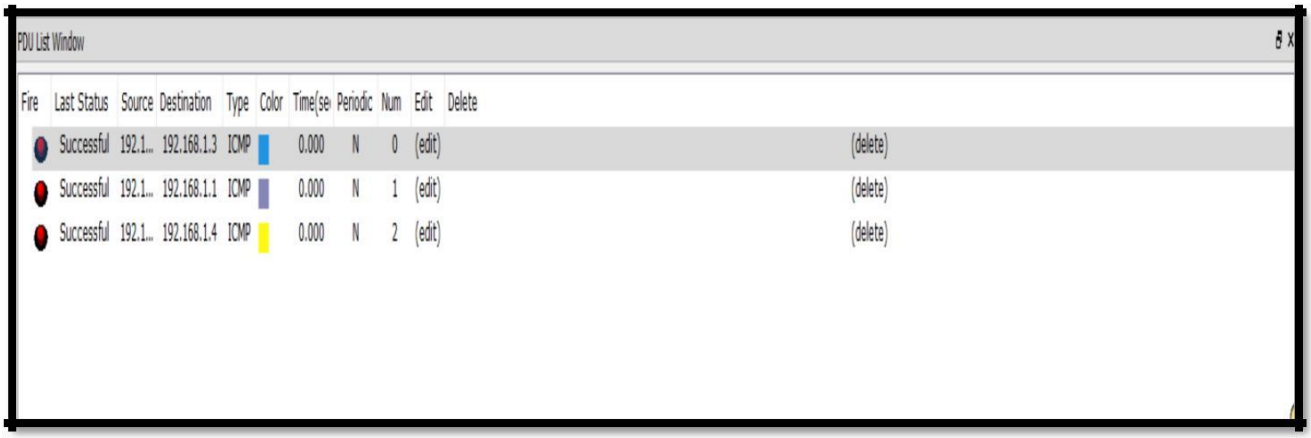
Figure: - Network Diagram

Procedure:

1. Take 6 system.
2. Configure each of system with their IP address.
3. Now check whether the system are completely connected with the other through ping command.



4. Once the system is successfully connected with other systems try to send the packets.



PRACTICAL:-05

AIM: Creating a Computer Networking Scenario Using Cisco IP Packet Tracer.

THEORY:

- ***Computer network***. A ***computer network*** or data ***network*** is a telecommunications ***network*** which allows ***computers*** to exchange data. In ***computer networks***, networked computing devices exchange data with each other using a data link. The connections between nodes are established using either cable media or wireless media.
- ***Devices used***:

1. End System: - *End systems* are the devices that provide information or services. The Internet's *end systems* include some computers with which the ***end*** user does not interact. These include e-mail servers and web servers.

2. Router: - A router is a device that forwards data packets along networks. A router is connected to at least two networks, commonly two LANs or WANs or a LAN and its ISP's network. Routers are located at gateways, the places where two or more networks connect.

3. Switch: - A switch is a device in a computer network that electrically and logically connects together other devices. Multiple data cables are plugged into a switch to enable communication between different networked devices. Switches manage the flow of data across a network by transmitting a received message only to the one or more devices for which the message was intended.

4. Wired media: - Wired communication refers to the transmission of data over a wire-based communication technology. Examples include telephone networks, cable television or internet access, and fiber-optic communication.

5. Wireless media: - Wireless is a term used to describe telecommunications in which electromagnetic waves (rather than some form of wire) carry the signal over part or all of the communication path. Some monitoring devices, such as intrusion alarms, employ acoustic waves at frequencies above the range of human hearing; these are also sometimes classified as wireless.

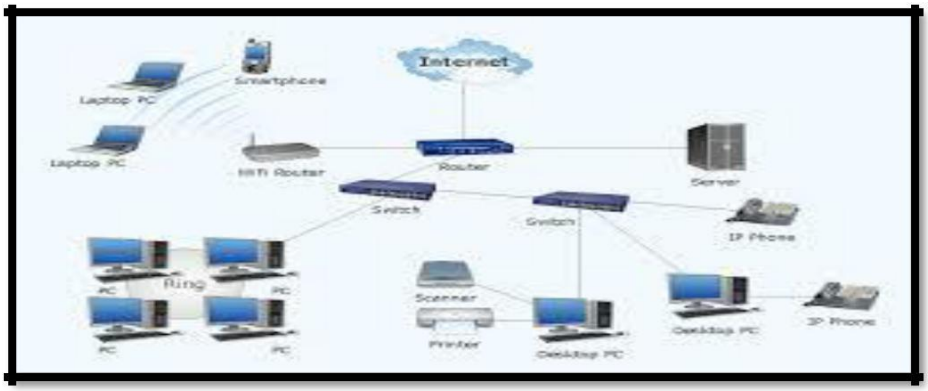
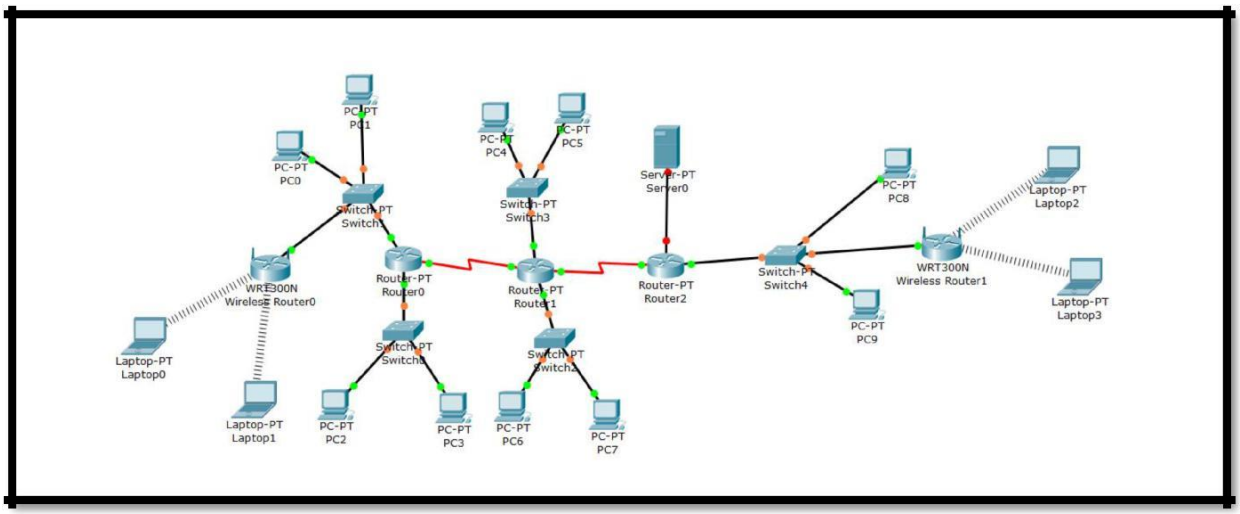


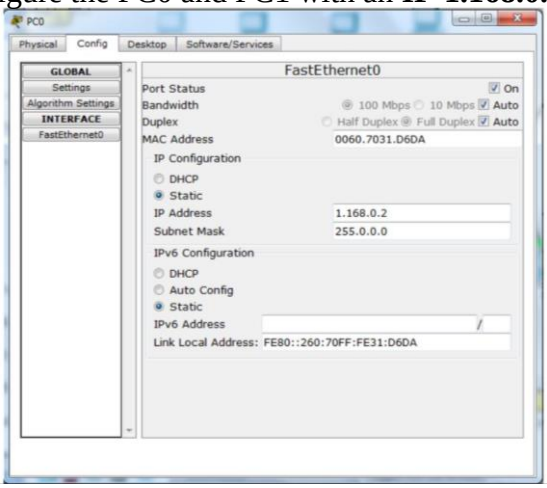
Figure: - General Diagram

Procedure:

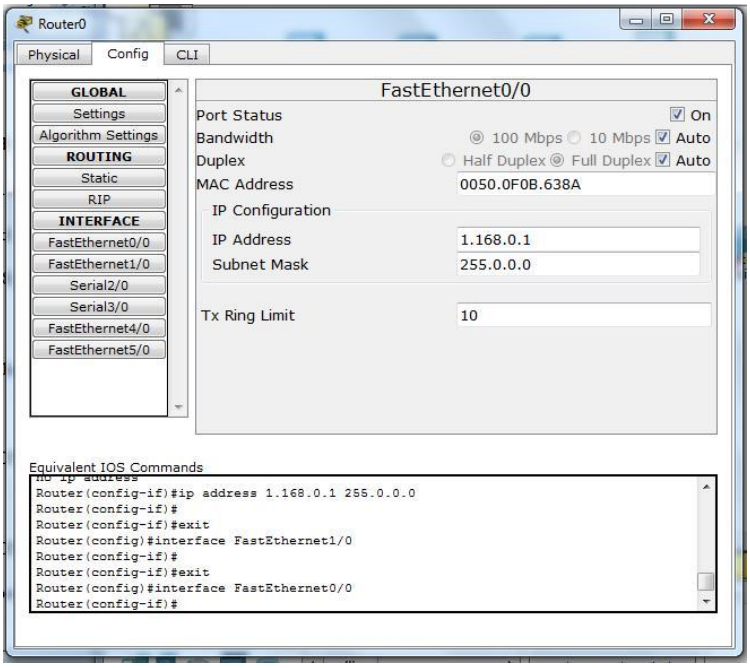
1. Take 10 systems name PC0-PC-9.
2. Take 3 switches.
3. Take 3 routers.
4. Connect PC0-PC1 with switch0.
5. Connect PC2-PC3 with switch1.
6. Connect switch0 with router0.
7. Connect PC4-PC5 with switch2.
8. Connect PC6-PC7 with Switch3.
9. Connect PC8-PC9 with switch4.
10. Connect Router 0 and Router 1.
11. Connect Router 2 with Switch4.
12. Connect switch 3 with Router 1 and Router1 to Router2.



13. Start Configure the PC0 and PC1 with an **IP-1.168.0.2, 1.168.0.3 and Gateway - 1.168.0.1**



14. Now configure the Router0 with fastethernet0/0 with an IP:-1.168.0.1 and also ON the port.



15. Now, same as above screenshot configure PC2 and PC3 with an IP-128.168.0.2, 128.168.0.3 and gateway-128.168.0.1

16. Again, configure the Router0 with fastethernet1/0 with an IP:-128.168.0.1 and also ON the port.

17. Configure PC4 and PC5 with an IP- 192.168.0.1 , 192.168.0.3 and gateway-192.168.0.1

18. Configure Router 1 with fastethernet0/0 with an IP 192.168.0.1 and also ON the port.

19. Configure PC6 and PC7 with an IP- 126.168.1.2 , 126.168.1.3 and gateway-126.168.1.1

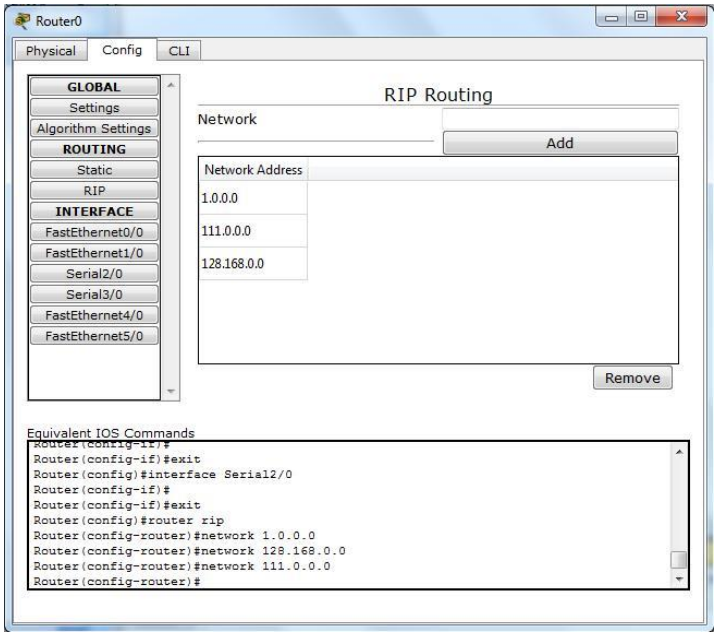
20. Configure Router 1 with fastethernet1/0 with an IP-126.168.1.1 and ON the port.

21. Configure PC8 and PC9 with an IP- 191.168.1.2, 191.168.1.3 and gateway-191.168.1.1.

22. Configure Router 2 with fastehternet0/0 with an IP-191.168.1.1 and ON the port.

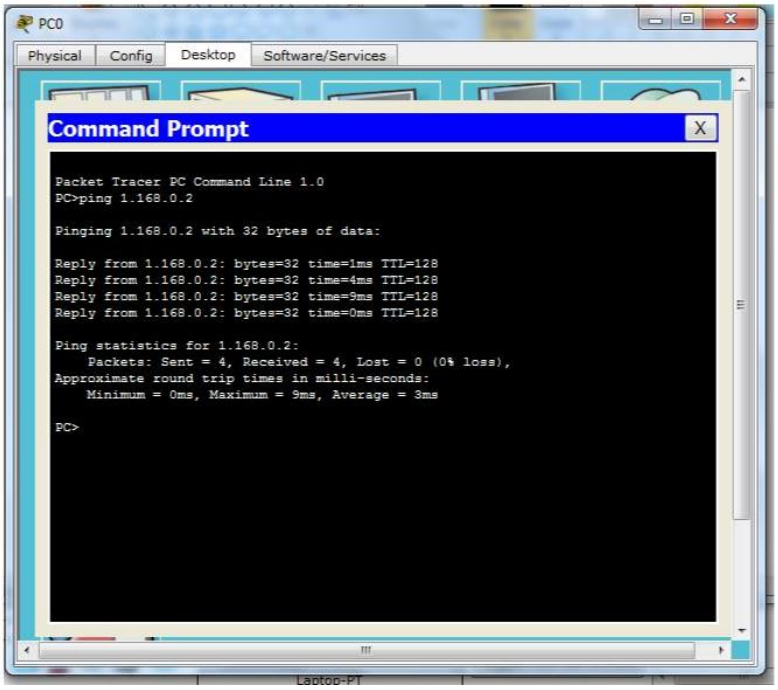
23. Now click on Router 0, go to serial2/0 give IP- 10.0.0.1 and ON the port.

24. Now go to RIP of router0 copy paste the address of fastethernet0/0, fastethernet1/0 and serial 2/0 of network 1 (i.e. PC0 and PC1).

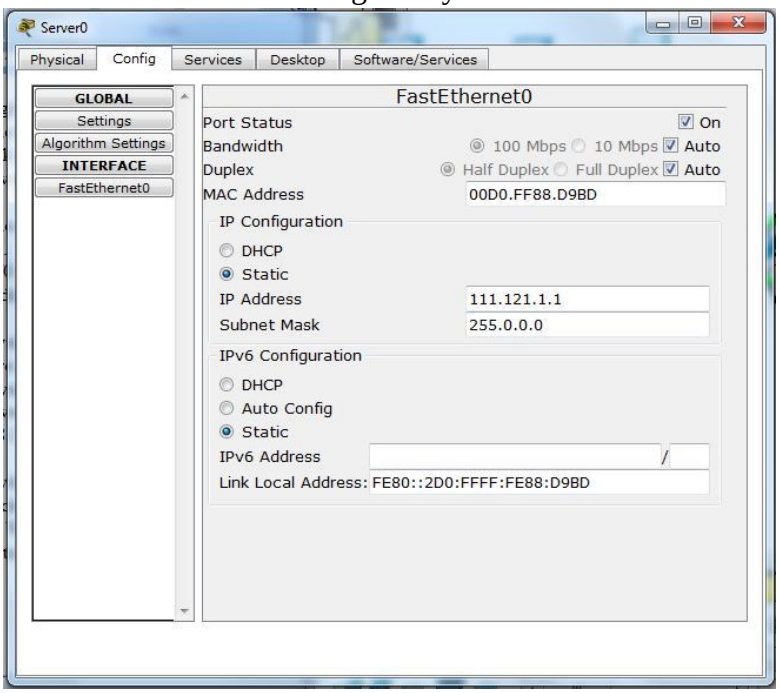


25. Click on Router1 go to serial2/0 and give IP 10.0.0.2 and in serial 3/0 give IP 128.0.0.1 and ON the port.
26. Go to RIP of router 1 and copy paste the address of fasthethernet0/0, fastethernet1/0, serial 2/0 and serial 3/0.
27. Click on Router2 and configure serial2/0 with an IP 128.0.03
28. Click on RIP of router 2 than add the address of Serial2/0 and fastethernet0/0.

Now start pinging from PC0 to other system, if the pinging command runs successfully than that means systems are connected correctly and then check it by sending packets from one system to others.



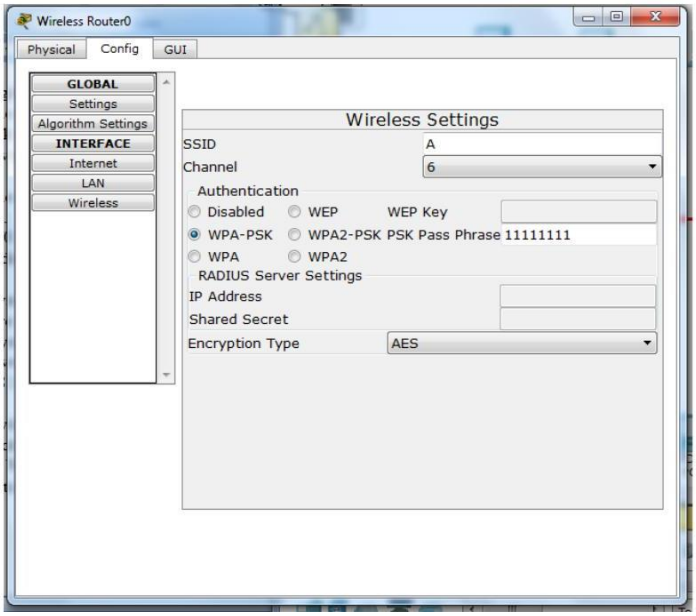
30. After checking this scenario, take 1 server connect it with switch 4 and configure the server with an IP 191.168.1.4 and gateway 191.168.1.1.



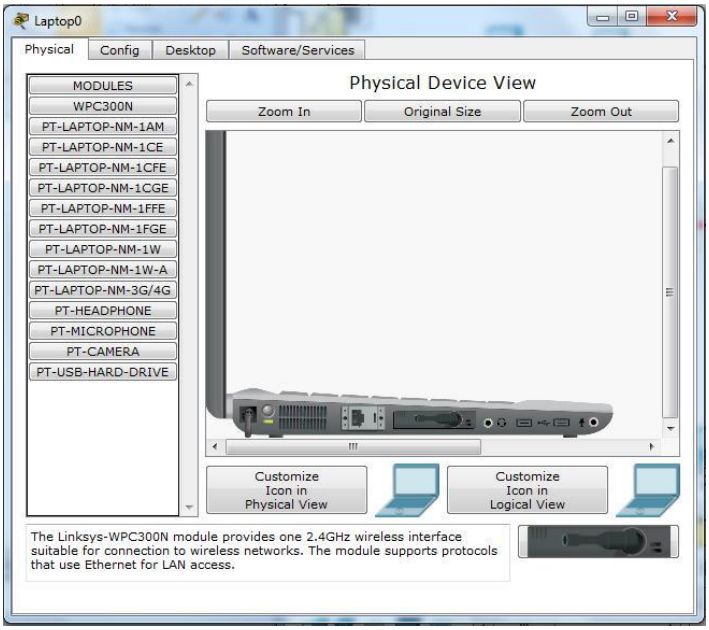
31. Take 2 laptops.

32. Take 1 wireless device and connect it with switch0.

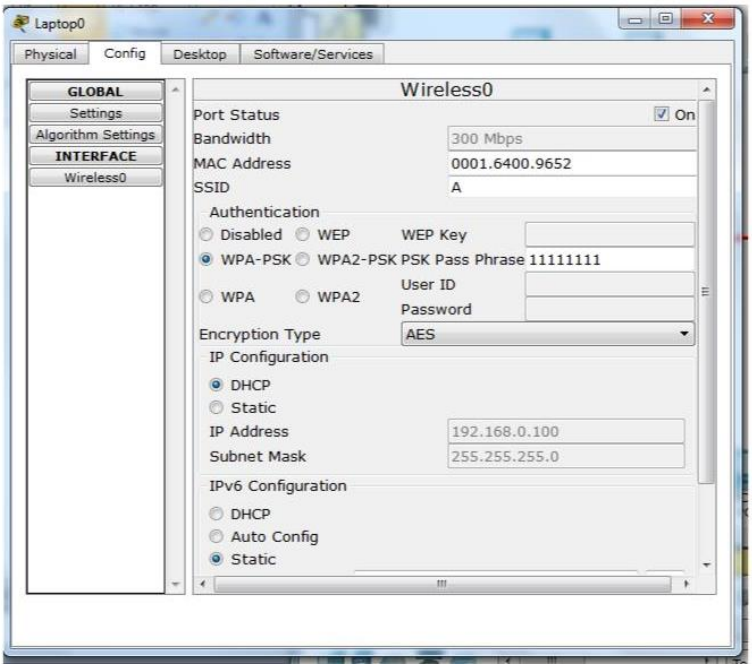
33. Now configure that wireless device, click on configure in that click on wireless and change the SSID to A and WPA-PSK to 11111111.



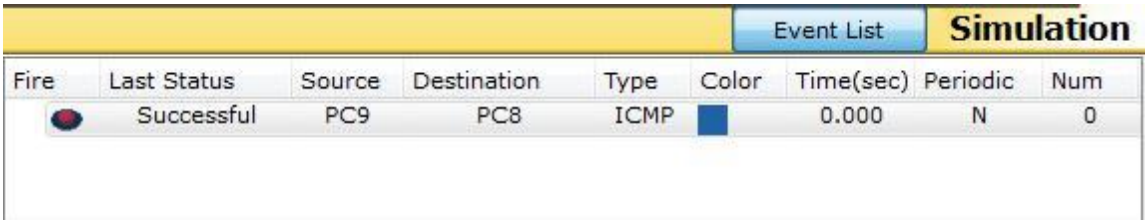
34. Now in Laptop change the ports by switch off the button and add change the ports.



Now in laptop1 and laptop2 click on configure in that click on wireless0 and change the SSID A. and WPA-PSK to 111111111.



36. Take other laptops and connect it with new wireless device2 with swtich4 (You have to take 1 more extension in switch4 if required).
37. Configure the wireless device2 with SSID-B and WPA-PSK to 11112222.
38. In both new laptops change the wireless setting to SSID B and WPA-PSK to 11112222.
39. After the configuration start send the packets and check the status of message passing.



PRACTICAL:-06

AIM: Configuring RIP (Routing Information Protocol) with CISCO IP PACKET TRACER

THEORY:

The Routing Information Protocol (RIP) defines a way for routers, which connect networks using the Internet Protocol (IP), to share information about how to route traffic among networks. RIP is classified by the Internet Engineering Task Force (IETF) as an Interior Gateway Protocol (IGP), one of several protocols for routers moving traffic around within a larger autonomous system network -- e.g., a single enterprise's network that may be comprised of many separate local area networks (LANs) linked through routers

Each RIP router maintains a routing table, which is a list of all the destinations (networks) it knows how to reach, along with the distance to that destination. RIP uses a distance vector algorithm to decide which path to put a packet on to get to its destination. It stores in its routing table the distance for each network it knows how to reach, along with the address of the "next hop" router -- another router that is on one of the same networks -- through which a packet has to travel to get to that destination. If it receives an update on a route, and the new path is

shorter, it will update its table entry with the length and next-hop address of the shorter path; if the new path is longer, it will wait through a "hold-down" period to see if later updates reflect the higher value as well, and only update the table entry if the new, longer path is stable

Using RIP, each router sends its entire routing table to its closest neighbours every 30 seconds. (The neighbours are the other routers to which this router is connected directly -- that is, the other routers on the same network segments this router is on.) The neighbours in turn will pass the information on to their nearest neighbours, and so on, until all RIP hosts within the network have the same knowledge of routing paths, a state known as convergence.

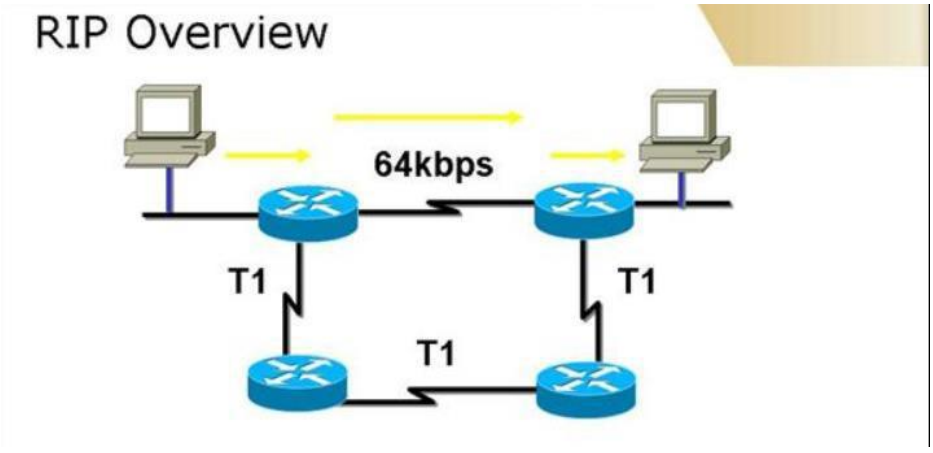
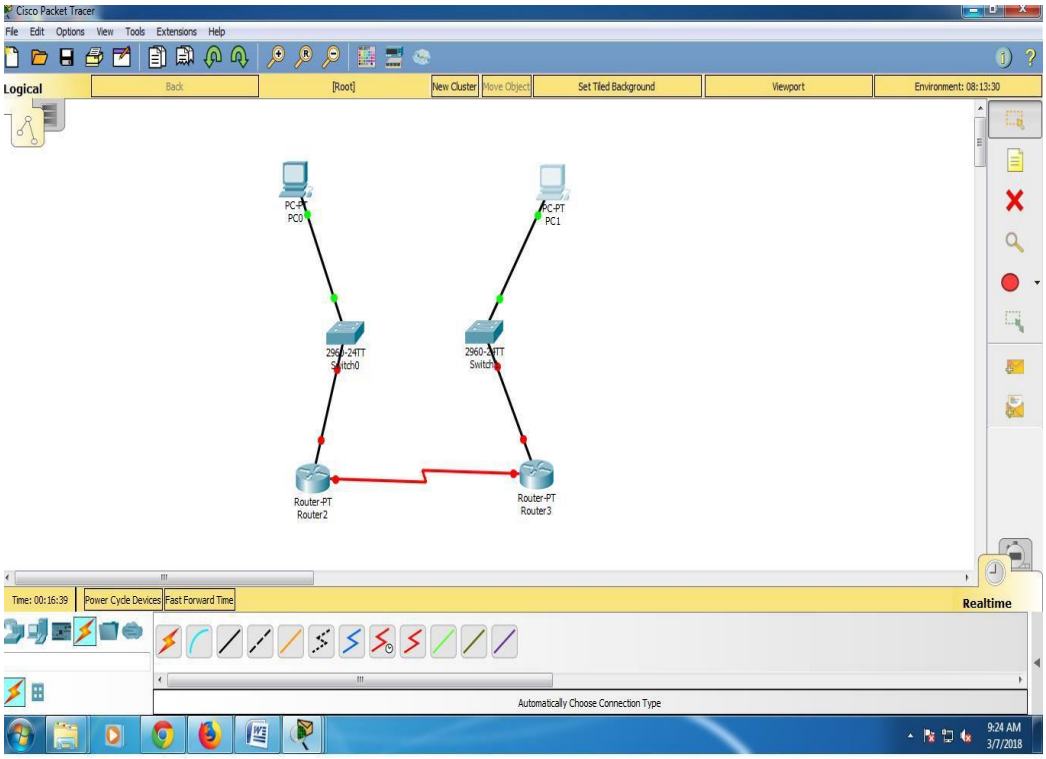


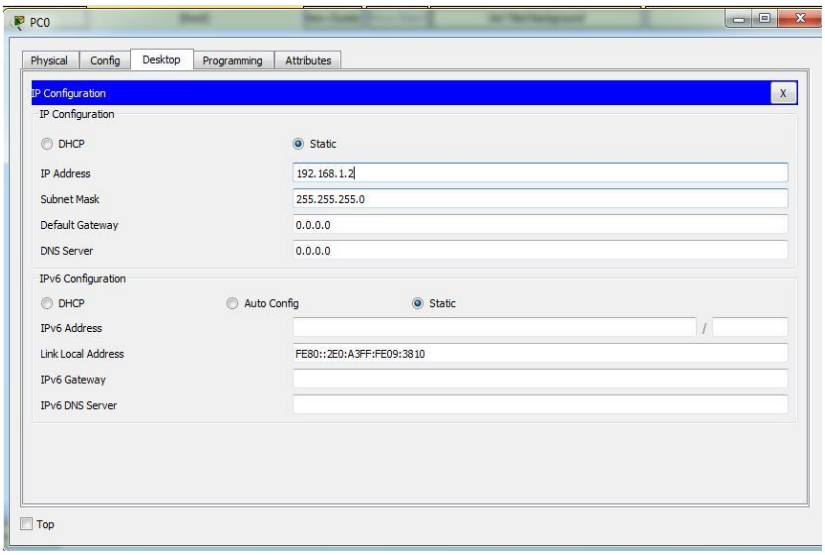
Figure: General Diagram

Procedure:

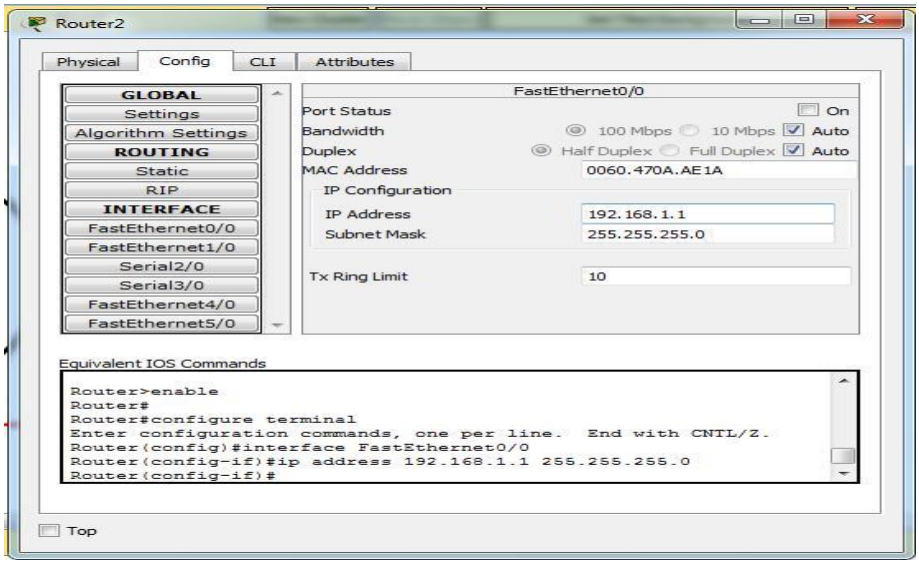
1. Take two system PC0 and PC1.
2. Highlight the network with 192.168.1.0 and 192.168.2.0 (both are of different network).
3. Take two switches.
4. Take two generic routers.
5. Connect PC0 with switch1 and connect that switch 1 with Router 0.
6. Connect PC1 with switch2 and connect that switch with Router 1.



7. Configure system 1 and 2 with IP 192.168.1.2 and 192.168.2.2 (because both system belongs to different network) and add gateway also with address 192.168.1.1 and 192.168.2.1

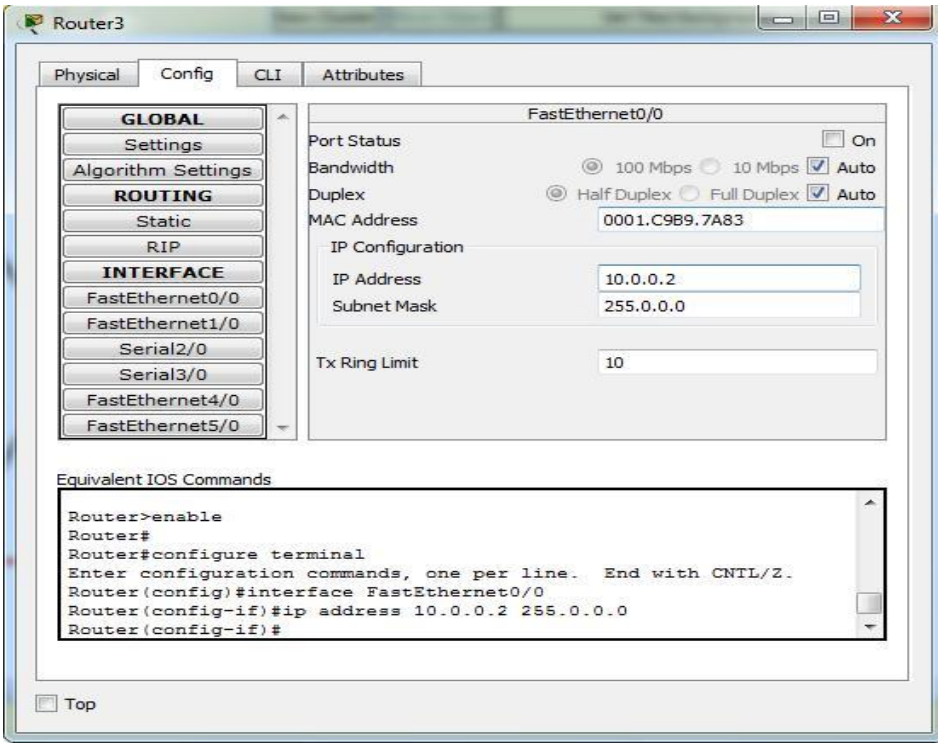


8. Configure Router 1 with fast Ethernet 0/0 with IP 192.168.1.1 and ON the port
9. Configure Router 2 with fast Ethernet0/1 with IP 192.168.2.1 and ON the port.



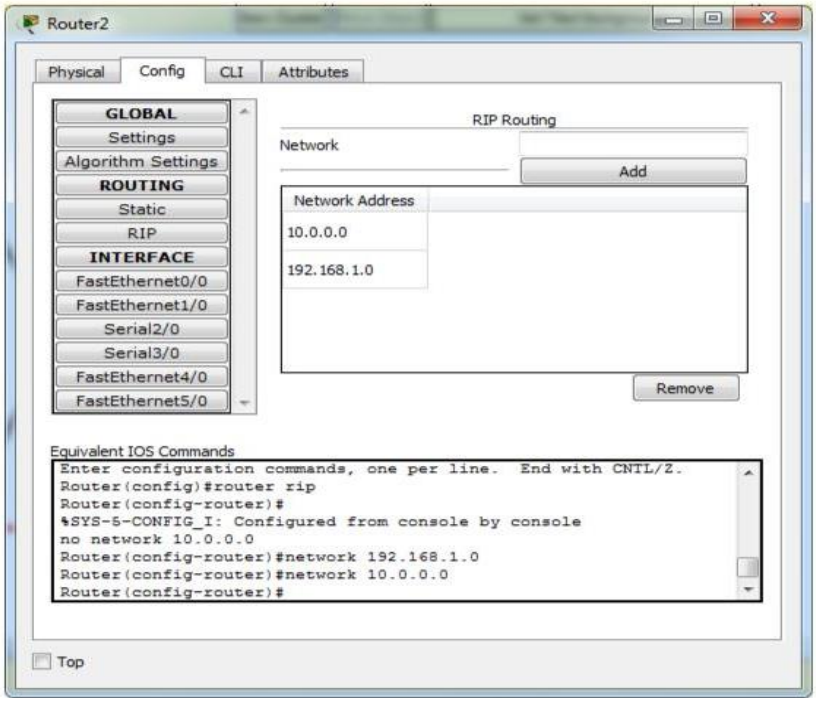
10. Go to Router1 in that configure serial 2/0 with IP 10.0.0.2 and ON the port and also set clock to 64000.

11. Go to Router2 in that configure serial2/0 with IP 10.0.0.3 and ON the port and clock is not set.

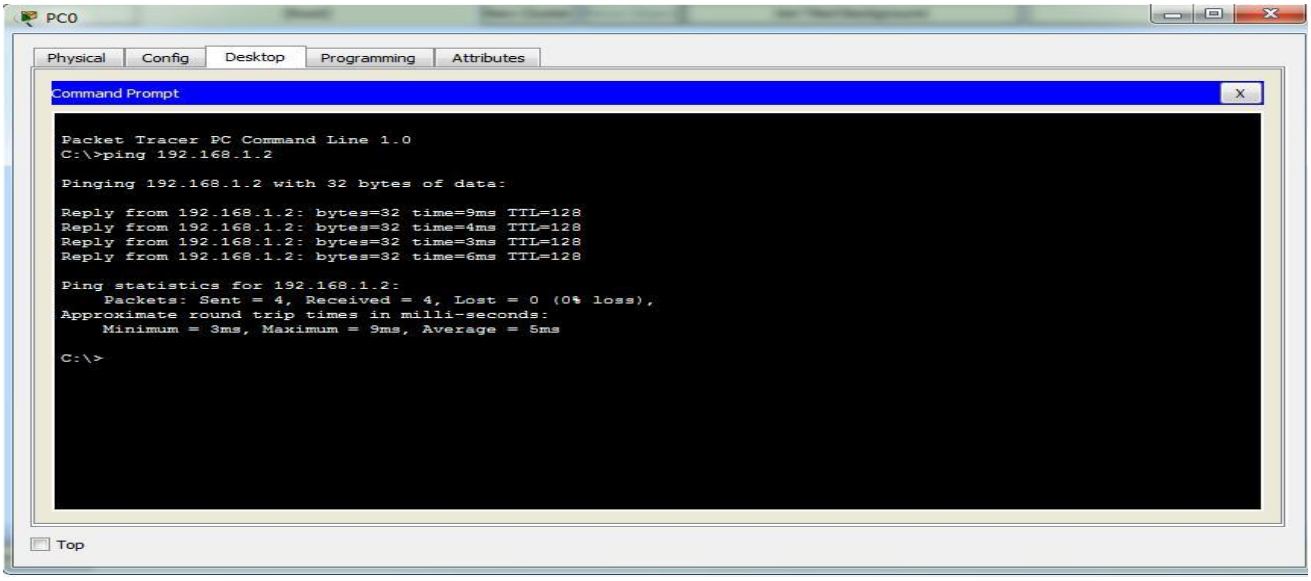


12. Now go to Router 2 in that configure RIP with the network address: 192.168.1.0 and 10.0.0.0 (because the router 0 knows about these 2 networks that why we add in RIP so that it can help further while sending packets) after adding go to setting and save the changes.

13. Now go to Router 2 in that configure RIP with the network address: 192.168.2.0 and 10.0.0.0 (because the router 0 knows about these 2 networks that why we add in RIP so that it can help further while sending packets) after adding go to setting and save the changes.



14. Start pinging from system1 to other, if it successful than start sending packet from system 1 to other.



15.Successfully working !!!

PRACTICAL:-07

AIM: Email communication using CISCO IP PACKET TRACER

THEORY:

Email, or electronic mail, is the most common method of exchanging digital messages and remains one of the most popular services currently available via the Internet, with over 90% of US Internet user's actively using email. Email systems consist of computer servers that process and store messages on behalf of users who connect to the email infrastructure via an email client or web interface. When someone sends an email, the message is transferred from his or her computer to the server associated with the recipient's address, usually via a number of other servers.

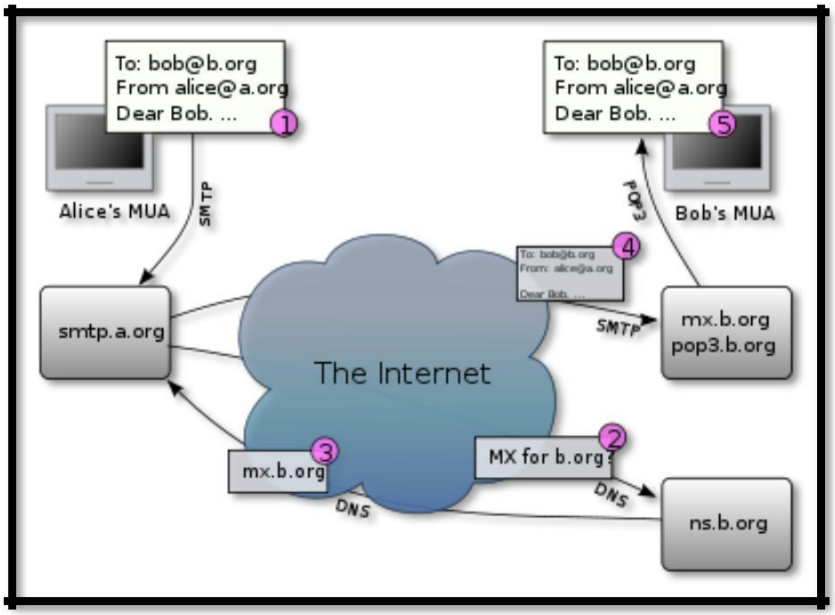
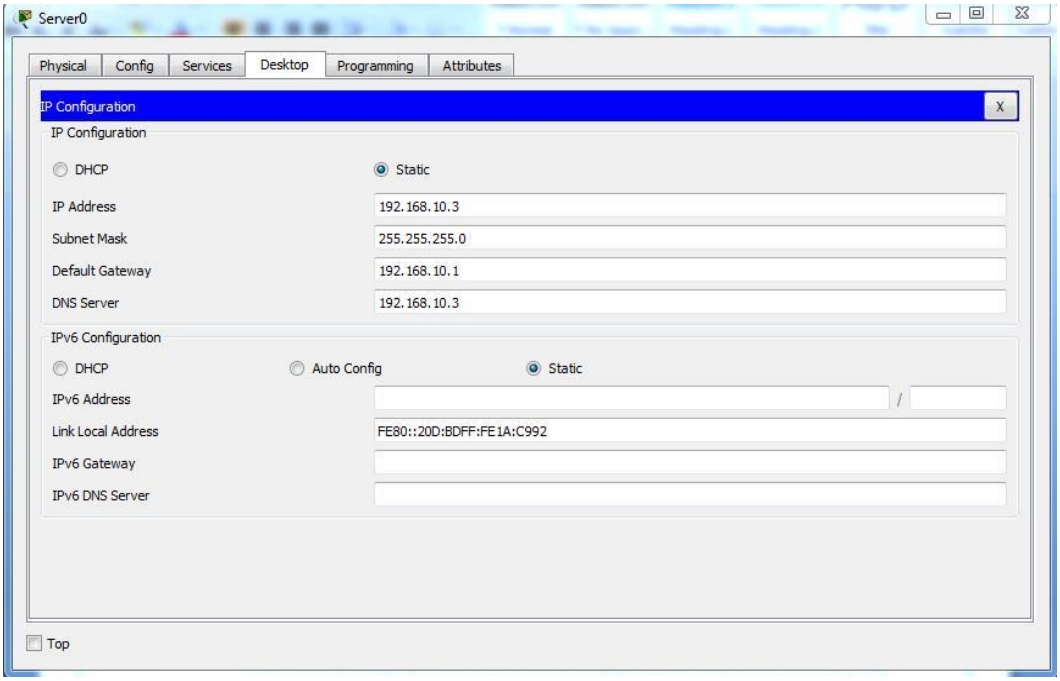


Figure: General Diagram

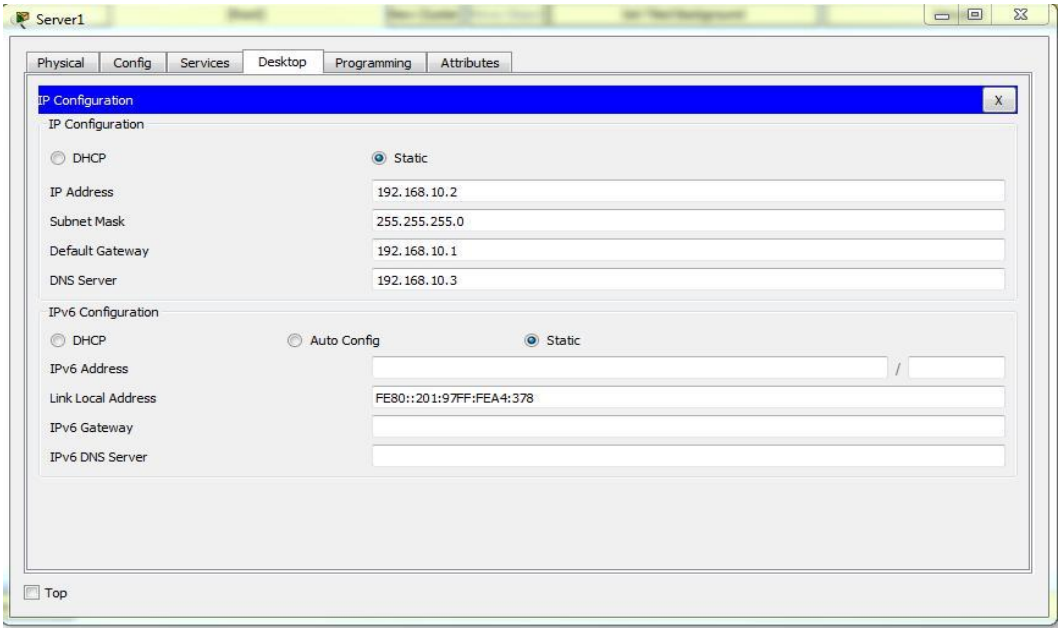
Procedure:

1. Take four servers name it as DNS, DHCP, HTTP and Email.
2. Label them as: DNS server: 192.168.10.3/24
   DHCP server: 192.168.10.2/24
   HTTP server: 192.168.10.3/24
   Email server: 192.168.10.4/24

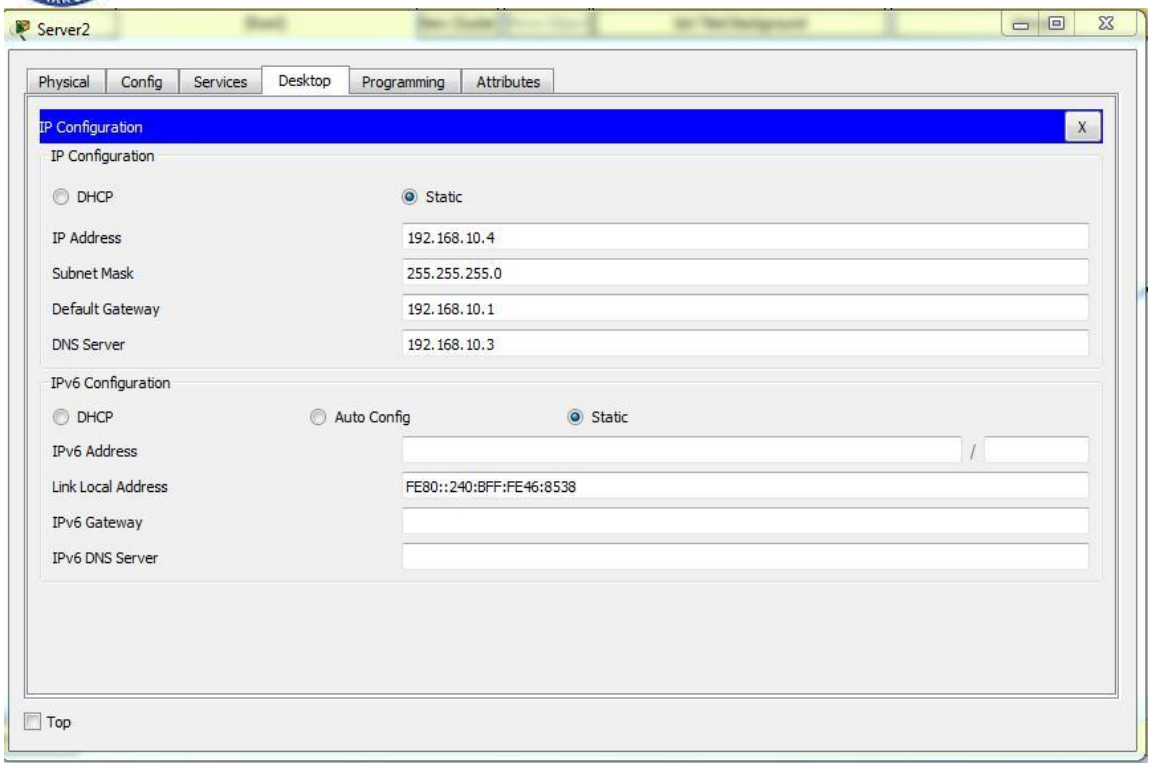
3. Click on DHCP server configure it with an IP 192.168.10.3 with gateway 192.168.10.1 and also DNS server 192.168.10.3



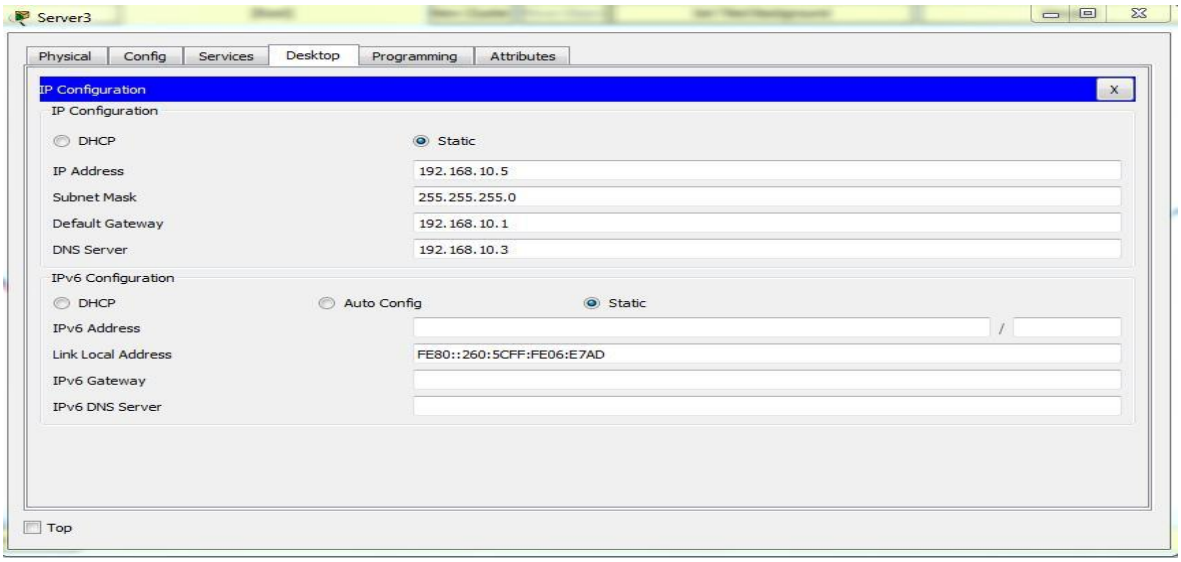
4. Click on DNS server configure it with an IP 192.168.10.2 with gateway 192.168.10.1 and also DNS server 192.168.10.3



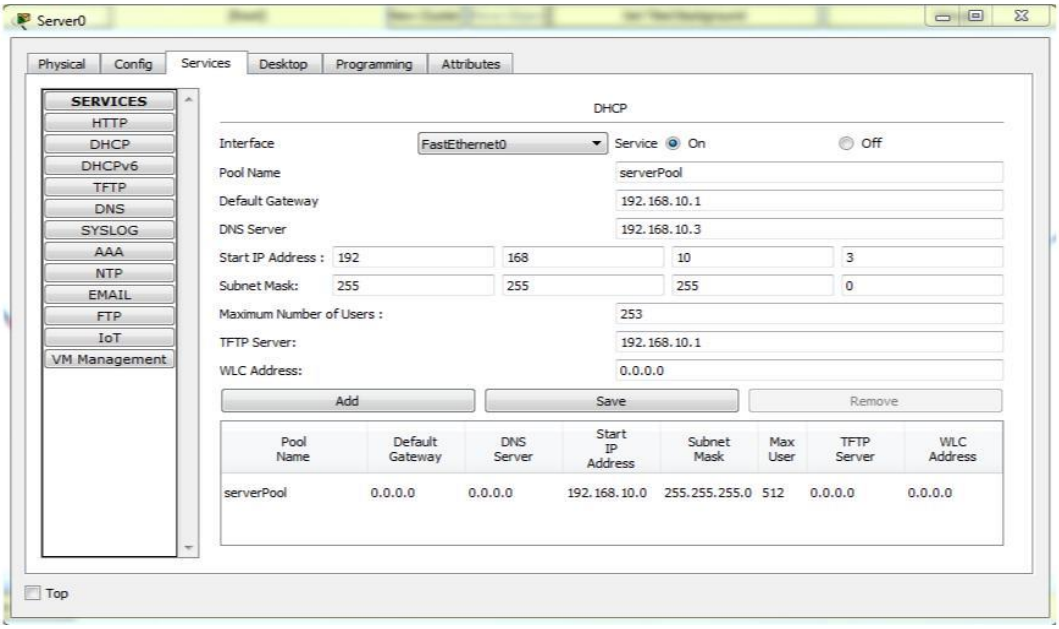
5. Click on EMAIL server configure it with an IP 192.168.10.4 with gateway 192.168.10.1 and also DNS server 192.168.10.3



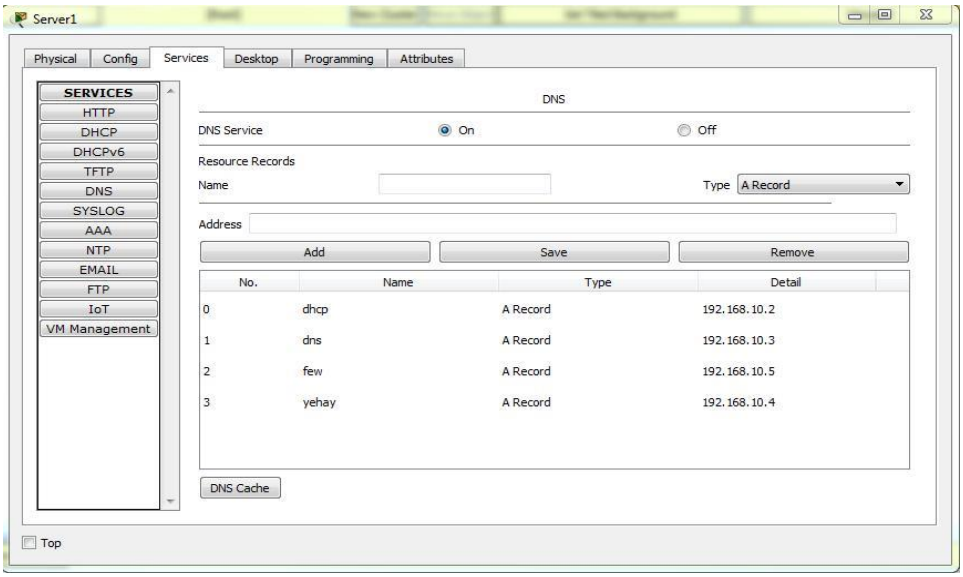
6. Click on HTTP server configure it with an IP 192.168.10.5 with gateway 192.168.10.1 and also DNS server 192.168.10.3



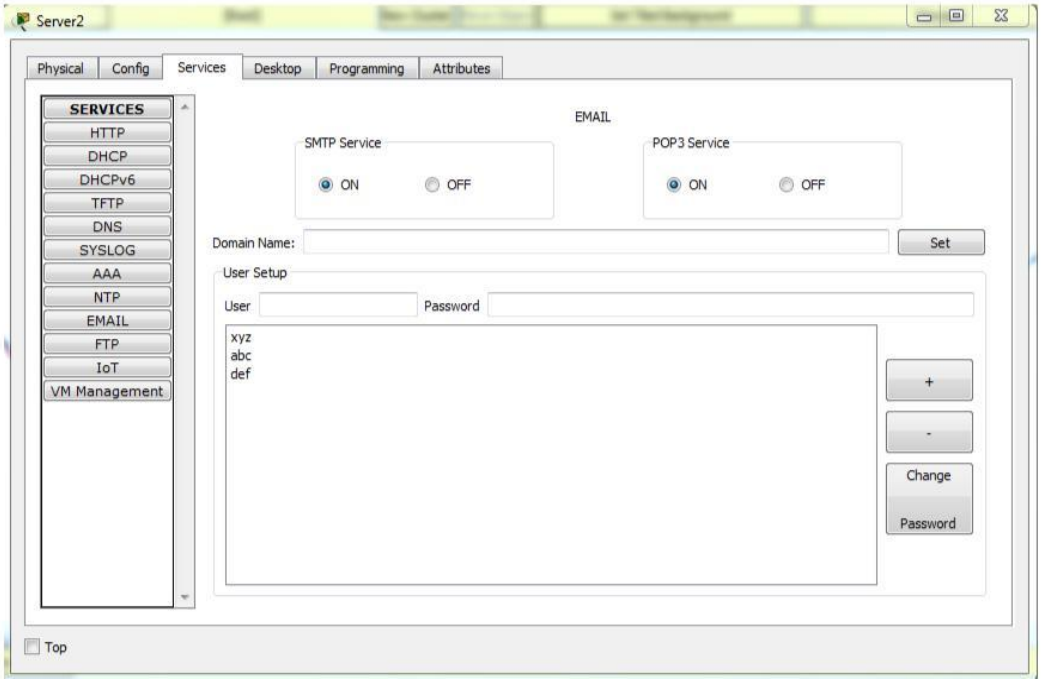
Configure the DHCP server by setting up the gateway IP and DNS now add address in START IP: 192.168.0.3 and TFTP sever address: 192.168.10.1



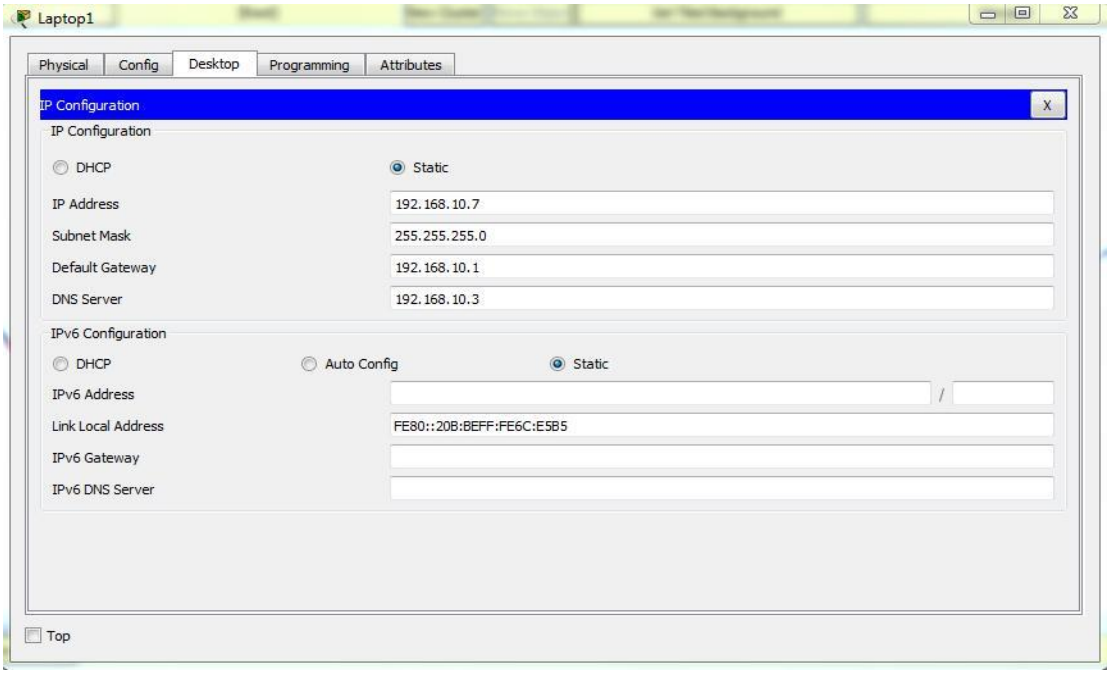
8. Configure DNS server in that write and Add them : DHCP in name give address 192.168.10.2, DNS 192.168.10.3,
FEW
192.168.10
.5,
YEHAY
192.168.10
.4



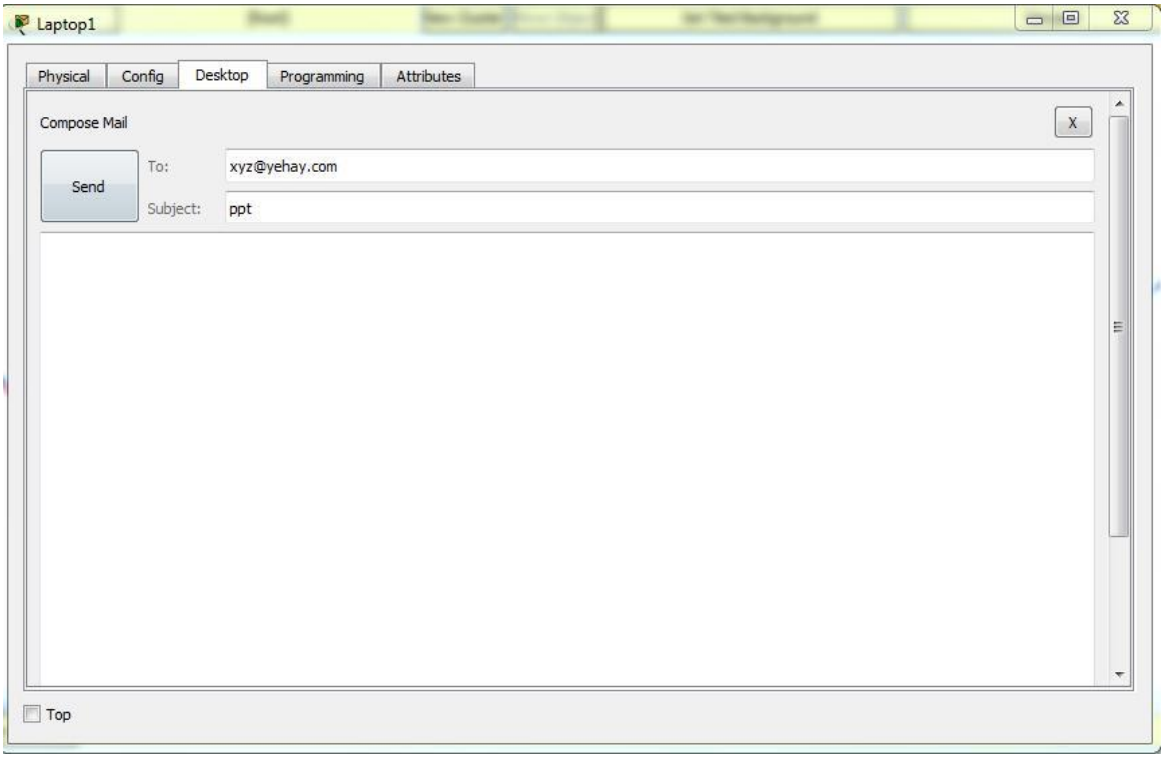
9. Now go to Email server configure the domain name yehay.com and set it and do enter any ID and Password. (ID and password you can enter as many as u want).



10. Click on all systems one by one and set IP dynamically.



11. Click on system 1 and click on EMAIL service and enter name and ID (name=xyz, ID xyz@yehay.com) and enter incoming and outgoing mail server: 192.168.10.4 and also enter username and password and save it and repeat the same for other systems but remember put different NAME and PASSWORDS.



12. Go to system 1 in that go to Email service and compose the message and the email address of the other system (which you have entered) and then send. Now one can see the receive mail from its own system by clicking on receive button from Email Service.

PRACTICAL:-08

AIM: Configure OSPF (Open Shortest Path First)

THEORY:

Open Shortest Path First (**OSPF**) is a routing protocol for Internet Protocol (IP) networks. It uses a link state routing algorithm and falls into the group of interior routing protocols, operating within a single autonomous system (AS). OSPF is an interior gateway protocol (IGP) for routing Internet Protocol (IP) packets solely within a single routing domain, such as an autonomous system. It gathers link state information from available routers and constructs a topology map of the network. The topology is presented as a routing table to the Internet Layer which routes datagrams based solely on the destination IP address found in IP packets. OSPF supports Internet Protocol Version 4 (IPv4) and Internet Protocol Version 6 (IPv6) networks and features variable (VLSM) and Classless Inter-Domain Routing (CIDR) addressing models.

OSPF detects changes in the topology, such as link failures, and converges on a new loop-free routing structure within seconds. It computes the shortest path tree for each route using a method based on Dijkstra's algorithm, a shortest path first algorithm.

The OSPF routing policies for constructing a route table are governed by link cost factors (external metrics) associated with each routing interface. Cost factors may be the distance of a router (round-trip time), data throughput of a link, or link availability and reliability, expressed as simple unit less numbers. This provides a dynamic process of traffic load balancing between routes of equal cost. OSPF uses multicast addressing for route flooding on a broadcast domain. For non-broadcast networks, special provisions for configuration facilitate neighbour discovery. OSPF multicast IP packets never traverse IP routers (never traverse Broadcast Domains), they never travel more than one hop. OSPF is therefore a Link Layer protocol in the Internet Protocol Suite.

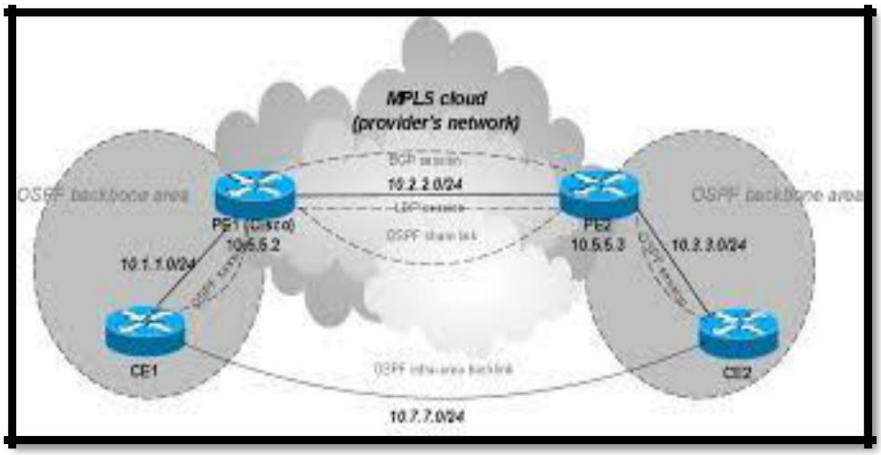
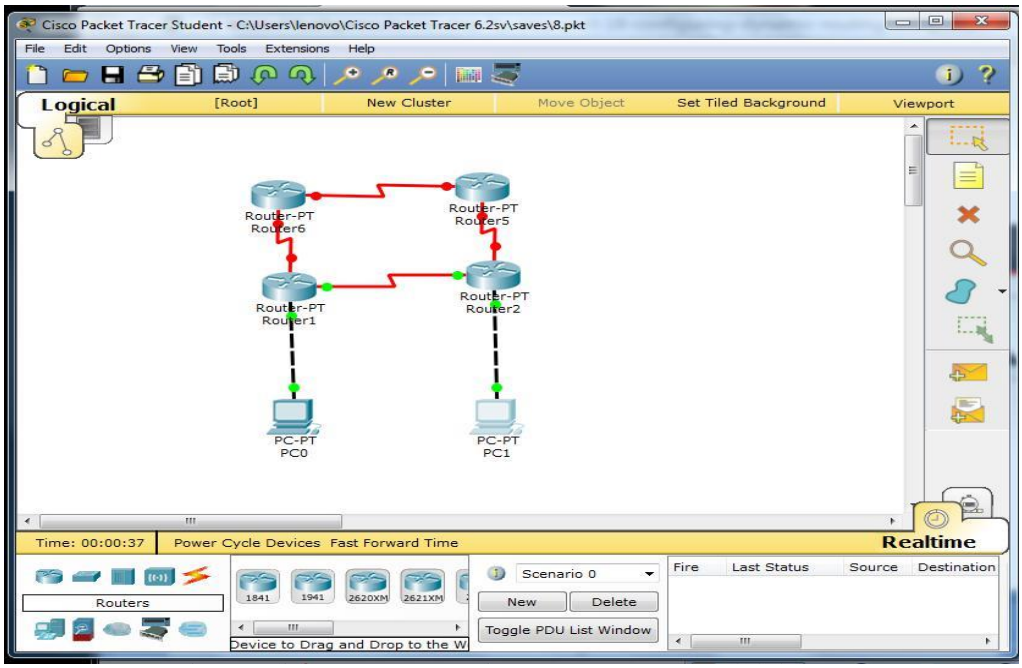
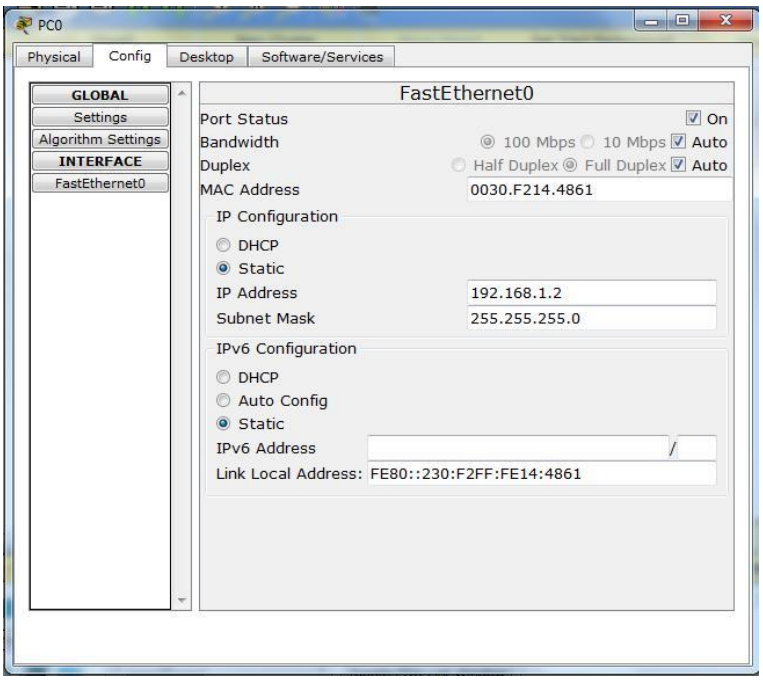


Figure: General Diagram



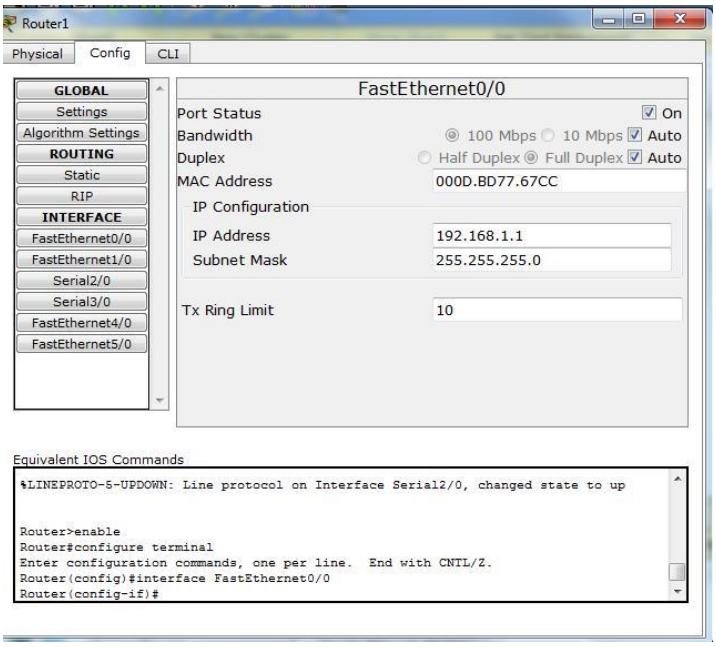
Procedure:

1. Take 1 system PC0 and give IP address 192.168.1.2 and insert gateway 192.168.1.1
2. Take 2nd system PC1 and give IP address 192.168.2.2 and insert gateway 192.168.2.1



3. Take router 1 and configure it with fasteth0/0 with an IP 192.168.1.1 , make port ON and give address to serial 2/0 10.10.0.2.

4. Take router 2 configure it with fasteth 0/0 with an IP 192.168.2.1 , make port ON and give address to serial 2/0 10.10.0.3.



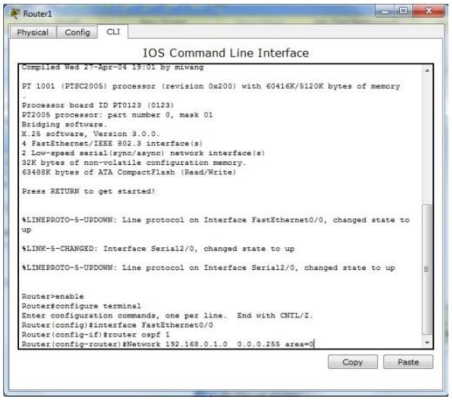
5. Go to router 2 in that got to CLI in that type ospf command.

6. After typing OSPF command, write down the further commands in that:

- Conf t
- Router ospf 1
- Network 192.168.2.0 0.0.0.255 area=0 0.255.255.255
- Network 10.0.0.0 area=0
- Exist

7. Same way configure router1

- Router ospf 1
- Network 192.168.1.0 0.0.0.255 area=0
- Network 10.0.0.0 0.255.255.255 area=0
- Exist



8. To check we send message from PC0 to PC1.
9. Take one more router.
10. Configure router 3: Serial 3/0 :

IP 11.10.0.2 Port : ON

11. Click on router 1 :Serial2/0:

IP 12.10.0.2 Port: ON

Clock: not set

12. Click on router2: Serial 3/0

IP 12.10.0.3 Clock:64000 Port:ON

13. Click on router3 go to CLI and configure the router

- Type command: router ospf 1
- Network 12.0.0.0 0.255.255.255 area=0
- Network 11.0.0.0 0.255.255.255 area=0
- Exit.

14. Click on router1 go to CLI and configure the router • Type command: router ospf 1

- Network 11.0.0.0 0.255.255.255 area=0 • Exit.

15. Click on router 2 go to CLI and configure the router • Type command: router ospf 1

- Network 11.0.0.0 0.255.255.255 area=0 • Exit

16. Start sending packet and note down the readings.

PRACTICAL: 9

AIM: - Commands for Advance Networking

Commands :-

Ping

PING: Test the network connection with a remote IP address

```
ping-t [IP or host]

ping-l 1024 [IP or host]
```

The -t option to ping continuously until Ctrl-C is pressed.
If you specify the -t option you can always get statistics without interrupting pings by pressing Ctrl + Break

This command is also useful to generate network load by specifying the size of the packet with the -l option and the packet size in bytes.

Tracert

TRACERT: Displays all intermediate IP addresses through which a packet passes through, between the local machine and the specified IP address.

```
tracert [@IP or host]

tracert -d [@IP or host]
```

This command is useful if the ping command does return any data, to determine at what level the connection failed.

IpConfig

IPCONFIG: Displays or refresh the TCP/IP configuration

ipconfig /all [/release [adapter]] [/renew [adapter]] /flushdns /displaydns /registerdns [-a] [-a] [-a]
This command, when executed with no options, displays the current IP address, the subnet mask and default gateway (network interfaces of the local machine)

- /all: Displays all network configuration, including DNS, WINS, DHCP servers, etc ...

- /renew [adapter]: Renews DHCP configuration for all adapters (if adapter is not specified) or a specific adapter indicated by the [adapter] parameter.
- /flushdns: Empty and reset the DNS client resolver cache. This option is useful to exclude negative entries and all other entries added dynamically to the cache.

NetStat

NETSTAT: Displays the status of the TCP/IP stack on the local machine

```
NETSTAT [-a] [-e] [-n] [-s] [-p proto] [-r] [interval]
```

- -a Displays all connections and listening ports (server-side connections are normally inhibited).
- -e Displays Ethernet statistics. Can be combined with the -s option.
- -n Displays addresses and port numbers in numerical form.
- -p proto Shows connections for the protocol specified by proto, proto may be TCP or UDP. Used with the -s option to display per-protocol statistics, proto may be TCP, UDP or IP.
- -r Displays the contents of the routing table.

Route

ROUTE: Displays or modifies the routing table

```
ROUTE [-f] [command [destination] [MASK network mask] [gateway]
```

- -f Clears the routing tables of all gateway entries. Used in conjunction with one of the below "commands", the tables are cleared before executing the command.
- -p Makes the entry into the table, residual (after reboot).

Specify one of four commands:

- DELETE: Deletes a route.
- PRINT: Displays a route.
- ADD: Adds a route.
- CHANGE: Modifies an existing route.
- destination: Specifies the host.
- MASK: If the MASK keyword is present, the next parameter is interpreted as the network mask parameter.

- netmask: Provided, it specifies the value of the subnet mask to be associated with this route entry. Unspecified, it takes the default value of 255.255.255.255.
- Gateway: Specifies the gateway.
- METRIC: Specifies the cost metric for the destination

Arp

ARP: Resolving IP addresses to MAC addresses. Displays and modifies the translation tables of IP addresses to physical addresses used by the ARP address resolution protocol.

```
ARP -s adr_inet adr_eth [adr_if]

ARP -d adr_inet [adr_if]

ARP -a [adr_inet] [-N adr_if]
```

- -a Displays active ARP entries by interrogating the current data protocol. If adr_inet is specified, only the physical and IP addresses of the specified computer are displayed. If more than one network interface uses ARP, entries for each ARP table are displayed.
- -g is the same as -a
- adr_inet Specifies an internet address.
- -N adr_if Displays ARP entries for the network interface specified by adr_if.
- -d Deletes the host specified by adr_inet.
- -s Adds the host and associates the adr_inet internet address with the adr_eth physical address. The physical address is given as 6 hexadecimal bytes separated by hyphens. The entry is permanent.
- adr_eth Specifies a physical address.

Nbtstat

NBTSTAT: Update cache of the LMHOSTS file. Displays protocol statistics and current TCP/IP connections using NBT (NetBIOS over TCP/IP).

```
NBTSTAT [-a Remote Name] [-A IP address] [-c] [-n] [-r] [-R] [-s] [S] [interval]
```

-a (adapter status) display the table (names) of the remote machine (known name).
-A (adapter status) display the table (names) of the remote machine (IP address).
-c (cache) display the remote name cache including the IP addresses.
-n (names) Lists local NetBIOS names.

-r (resolved) Lists names resolved by broadcast and via WINS.
-R (Reload) Clear and reload the table cache with the remote names.
-S (Sessions) Lists the sessions table with the destination IP addresses.
-s (sessions) Lists the sessions table with the destination IP addresses converted to host names via the hosts file.
Example :
nbtstat -A @IP
This command returns the NetBIOS name, system name, users connected ... to the remote machine.

Telnet

TELNET

```
telnet <IP or host>

telnet <IP or host> <port TCP>
```

The telnet command to access to a remote host in Terminal mode (passive screen) . It also allows you to check if any TCP service is running on a remote server by specifying the IP address after the TCP port number. Thus we can test whether the SMTP Service is running on a Microsoft Exchange server, using the IP address of the SMTP connector, and then 25 as the port number. The most common ports are:

- ftp (21),
- telnet (23),
- smtp (25),
- www (80),
- kerberos (88),
- pop3 (110),
- nntp (119)
- and nbt (137-139).

Hostname

HOSTNAME: Displays the name of the machine

Ftp

FTP: Client to upload files

```
ftp -s:<file>
```

- -s This option allows you to run FTP in batch mode: Specifies a text file containing FTP commands.

Nslookup

Nslookup sends DNS requests to a DNS server

```
nslookup [domain] [dns server]
```

The nslookup command to send DNS requests to a server. By default, if you do not specify the DNS server, the command will use the one that is configured for your network interface (the one you use to surf the internet, for example).