Vidya Vikas Education Trust's

Universal College of Engineering

(Permanently unaided | Approved by AICTE, DTE & Affiliated to University of Mumbai)

Department of Computer Science & Engineering

COMPUTER NETWORK LAB

(CSL 502)

Lab Manual

Name:	**VIVEK.SHIVAKUMAR. HOTTI**
Roll No.:	**31**
Class:	**T. E-Computer Engineering**
Division:	**A**
Semester:	**5**
Professor:	**Professor Chinmay Raut**

2020 – 2021

Sem 5

Vision:

To be recognized globally as a department provides quality technical education that eventually caters to helping and serving the community.

Mission:

To develop human resources with sound knowledge in theory and practice of computer science and engineering. To motivate the students to solve real-world problems to help the society grow. To provide a learning ambience to enhance innovations, team spirit and leadership qualities for students.

Lab Code	Lab Name	Credits
CSL502	**Computer Network Lab**	**1**

Description:

Design and implementation of any case study/ applications /experiments / mini project based on departmental level courses using modern tools.

Term work:

The distribution of marks for term work shall be as follows:
Lab/ Experimental Work: 15
Report/ Documentation: 05
Attendance (Theory &amp; Practical): 05

Practical & Oral:

Examination is to be conducted based on respective departmental level courses by pair of internal and external examiners appointed by the University of Mumbai.

Vidya Vikas Education Trust's

Universal College of Engineering

(Permanently unaided | Approved by AICTE, DTE & Affiliated to University of Mumbai)

INDEX

Name: Vivek. Hotti **Roll:** 31

Class: TE- Computers **Division:** A

Semester: 5

EXPERIMENT – 01

AIM: To Study Different Types of Network Topologies of Computer Networks.

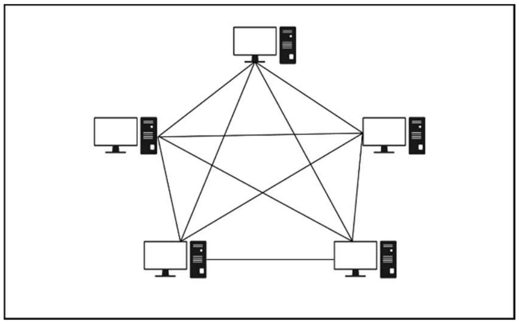
THEORY:

Introduction (Domain):

- Topology: The arrangement of a network that comprises nodes and connecting lines via sender and receiver is referred to as network topology. Topology defines the structure of the network of how all the components are interconnected to each other.

- There are 5 different types of Topologies namely:
  a. Mesh
  b. Star
  c. Bus
  d. Ring
  e. Tree

- Let us see each type of topology in detail:
  a) **MESH TOPOLOGY**:



In a mesh network, all of the computers are connected to each other. Not only does each computer send its own signals, but it also relays data from other computers. If there are N nodes, the nodes are connected to each other by a dedicated connection, during which information travels from node to node, and there are N(N-1)/2 links in the mesh. Every node has a point-to-point connection with the node on the other side. The mesh's connections are wired or wireless.

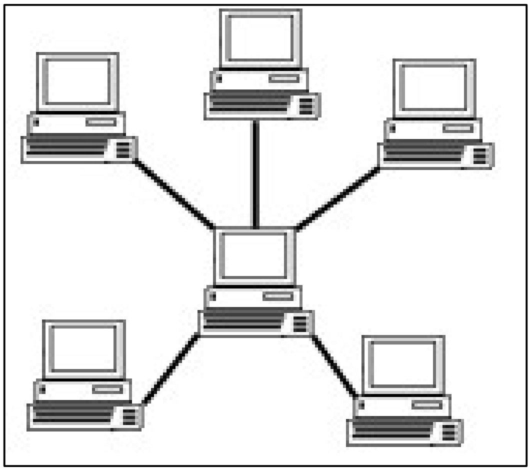
Advantages of Mesh Topology:

- It is robust.
- The fault is diagnosed easily. Data is reliable because data is transferred among the devices through dedicated channels or links.
- Provides security and privacy.

Disadvantages of Mesh Topology:

- Installation and configuration are difficult.
- The cost of cables is high as bulk wiring is required, hence suitable for a smaller number of devices.
- The cost of maintenance is high.

b) **STAR TOPOLOGY**:



Star topology is a network topology where each individual piece of a network is attached to a central node (often called a hub or switch). The attachment of these network pieces to the central component is visually represented in a form similar to a star. Star topology is also known as a star network.

In star topology, all the devices are connected to a single hub through a cable. This hub is the central node and all other nodes are connected to the central node. The hub can be passive in nature i.e., not intelligent hub such as broadcasting devices, at the same time the hub can be intelligent known as active hubs. Active hubs have repeaters in them.

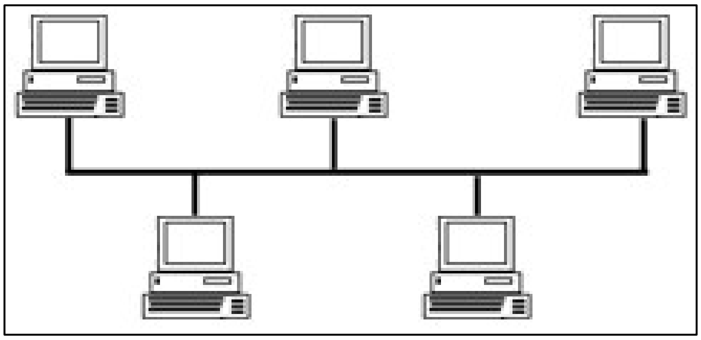
Advantages of Star Topology:

- If N devices are connected to each other in a star topology, then the number of cables required to connect them is N. So, it is easy to set up.
- Each device requires only 1 port i.e., to connect to the hub, therefore total number of ports required is N.

Disadvantages of Star Topology:

- If the concentrator (hub) on which the whole topology relies fails, the whole system will crash down.
- The cost of installation is high.
- Performance is based on the single concentrator i.e., hub.

c) **BUS TOPOLOGY**:



A bus topology is a topology for a Local Area Network (LAN) in which all the nodes are connected to a single cable. The cable to which the nodes connect is called a "backbone". If the backbone is broken, the entire segment fails. Bus topologies are relatively easy to install and don't require much cabling compared to the alternatives.
Bus topology is a network type in which every computer and network device is connected to a single cable. It transmits the data from one end to another in a single direction. No bi-directional feature is in bus topology. It is a multi-point connection and a non-robust topology because if the backbone fails the topology crashes.

Advantages of BUS Topology:

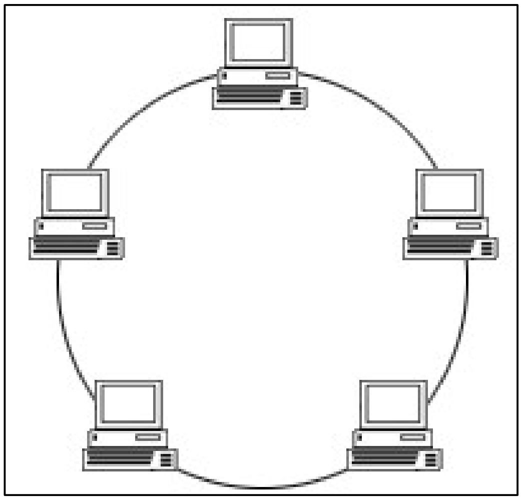
- If N devices are connected to each other in a bus topology, then the number of cables required to connect them is 1, which is known as backbone cable, and N drop lines are required.
- The cost of the cable is less as compared to other topologies, but it is used to build small networks.

Disadvantages of BUS Topology:

- If the common cable fails, then the whole system will crash down.

- If the network traffic is heavy, it increases collisions in the network. To avoid this, various protocols are used in the MAC layer known as Pure Aloha, Slotted Aloha, CSMA/CD, etc.
- Security is very low.

d) **RING TOPOLOGY**:



A ring topology is a network configuration where device connections create a circular data path. Each networked device is connected to two others, like points on a circle. Together, devices in a ring topology are referred to as a ring network.

In a ring network, packets of data travel from one device to the next until they reach their destination. Most ring topologies allow packets to travel only in one direction, called a unidirectional ring network. Others permit data to move in either direction, called bidirectional.

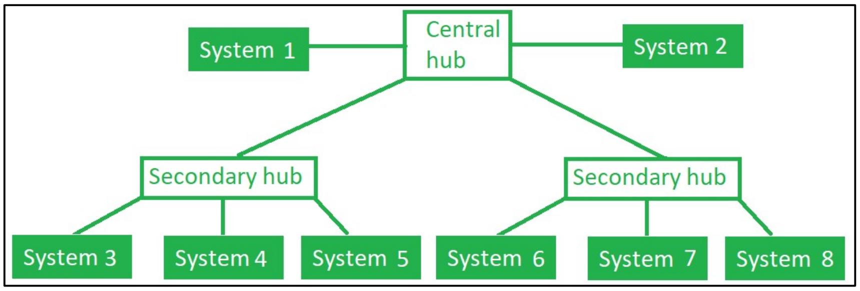
Advantages of RING Topology:

- The possibility of collision is minimum in this type of topology.
- Cheap to install and expand.

Disadvantages of RING Topology:

- Troubleshooting is difficult in this topology.
- The addition of stations in between or removal of stations can disturb the whole topology.
- Less secure.

e) **TREE TOPOLOGY**:



A tree topology is a special type of structure where many connected elements are arranged like the branches of a tree. For example, tree topologies are frequently used to organize the computers in a corporate network, or the information in a database.

This topology is the variation of Star topology. This topology has a hierarchical flow of data.

Advantages of TREE Topology:

- It allows more devices to be attached to a single central hub thus it increases the distance that is travel by the signal to come to the devices.
- It allows the network to get isolate and also prioritize from different computers.

Disadvantages of TREE Topology:

- If the central hub gets fails the entire system fails.
- The cost is high because of cabling.

CONCLUSION:

Hence, we have studied all the Different Types of Network Topologies of Computer Networks.

x-x-x

Experiment 01 Over

EXPERIMENT – 02

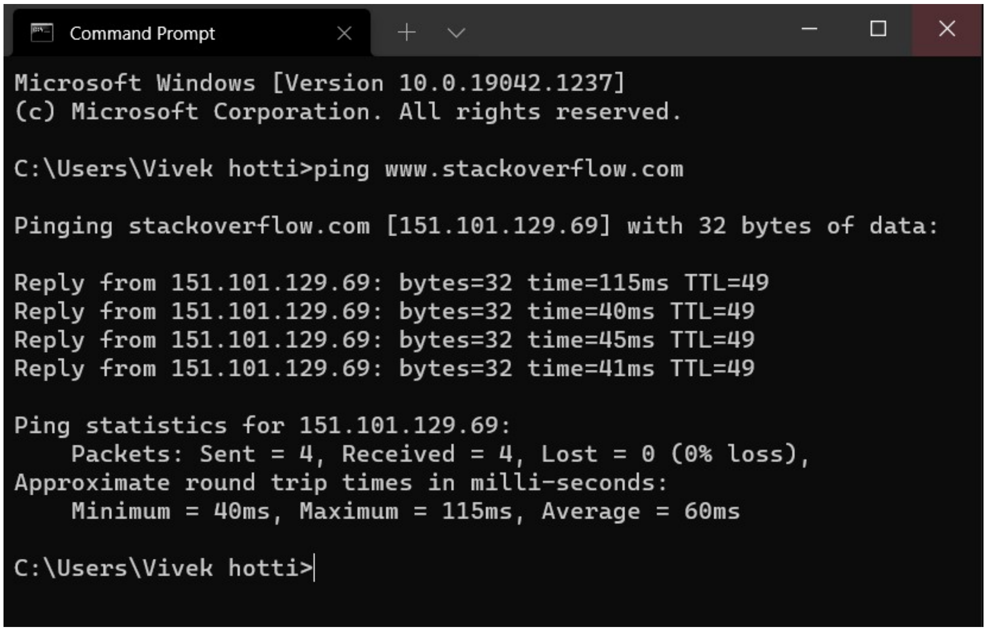
AIM: To Study Different Networking Commands.

THEORY:

The operating system consists of various built-in, command-line networking utilities that are used for network troubleshooting. We will see various networking commands which are most essentials for every network administrator.

Let's see some commands and understand how to execute them:

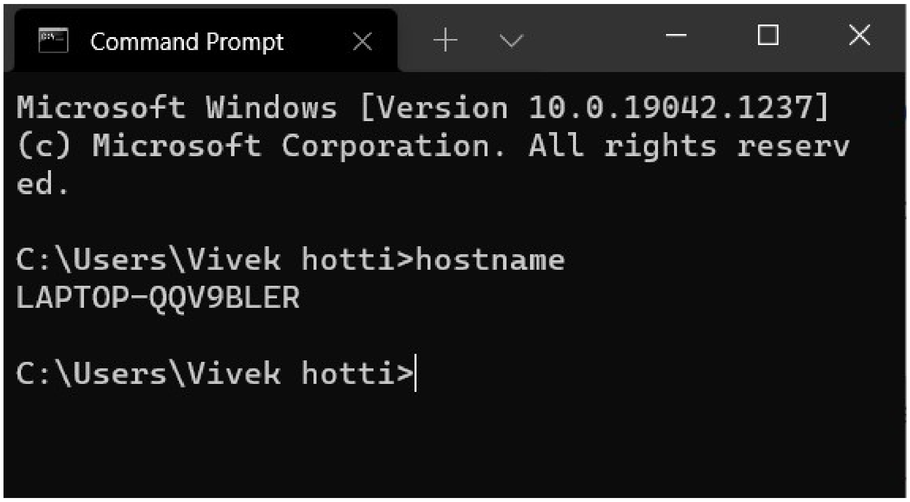
1) Ping command:



```
Microsoft Windows [Version 10.0.19042.1237]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Vivek hotti>ping www.stackoverflow.com

Pinging stackoverflow.com [151.101.129.69] with 32 bytes of data:

Reply from 151.101.129.69: bytes=32 time=115ms TTL=49
Reply from 151.101.129.69: bytes=32 time=40ms TTL=49
Reply from 151.101.129.69: bytes=32 time=45ms TTL=49
Reply from 151.101.129.69: bytes=32 time=41ms TTL=49

Ping statistics for 151.101.129.69:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 40ms, Maximum = 115ms, Average = 60ms

C:\Users\Vivek hotti>
```

Ping is used to testing a network host capacity to interact with another host. Just enter the command Ping, followed by the target host's name or IP address. The ping utilities seem to be the most common network tool. This is performed by using the Internet Control Message Protocol, which allows the echo packet to be sent to the destination host and a listening mechanism. If the destination host reply to the requesting host, that means the host is reachable. This utility usually gives a basic image of where there may be a specific networking issue.

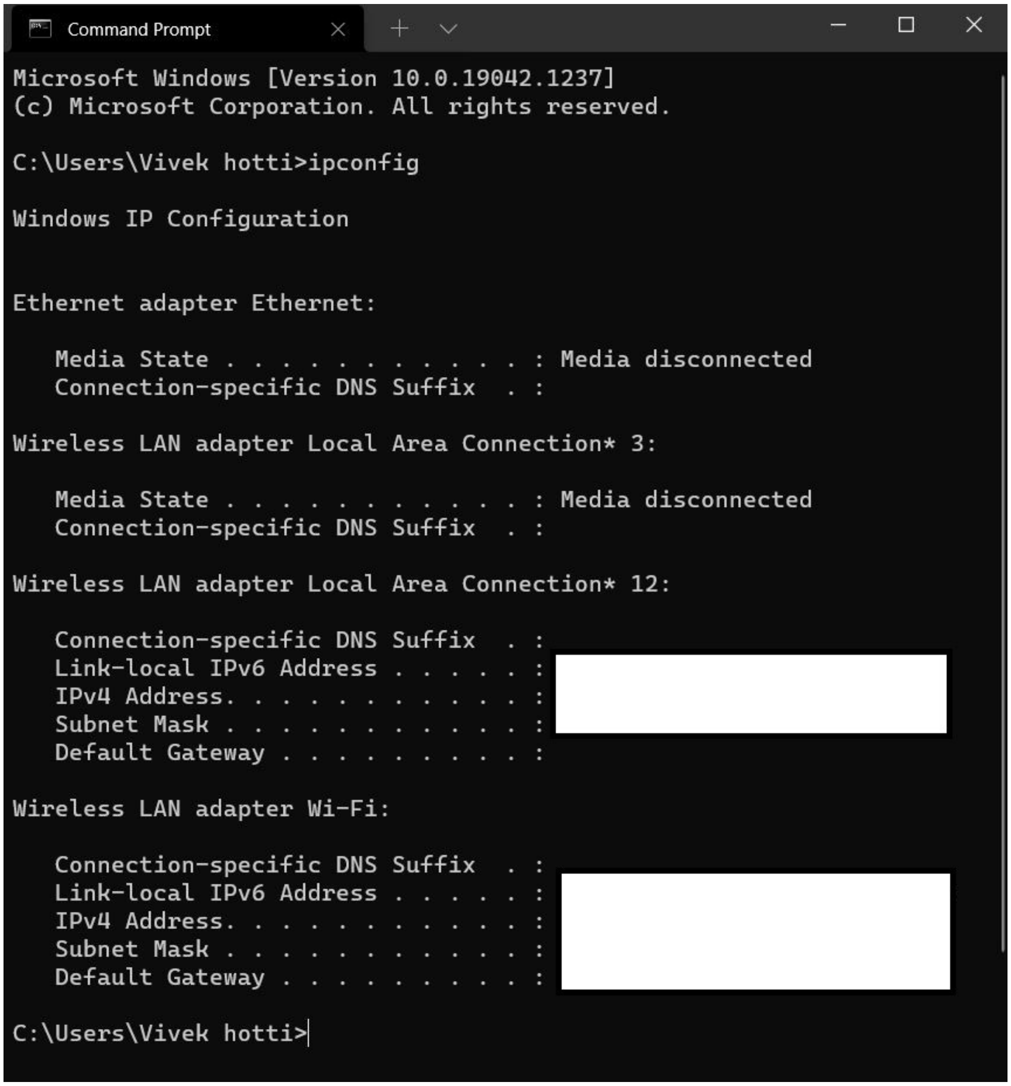
2) Hostname command:



```
Microsoft Windows [Version 10.0.19042.1237]
(c) Microsoft Corporation. All rights reserv
ed.

C:\Users\Vivek hotti>hostname
LAPTOP-QQV9BLER

C:\Users\Vivek hotti>
```

To communicate with each and other, the computer needs a unique address. A hostname can be alphabetic or alphanumeric and contain specific symbols used specifically to define a specific node or device in the network. For example, a hostname should have a domain name (TLD) of the top-level and a distance between one and 63 characters when used in a domain name system (DNS) or on the Internet.

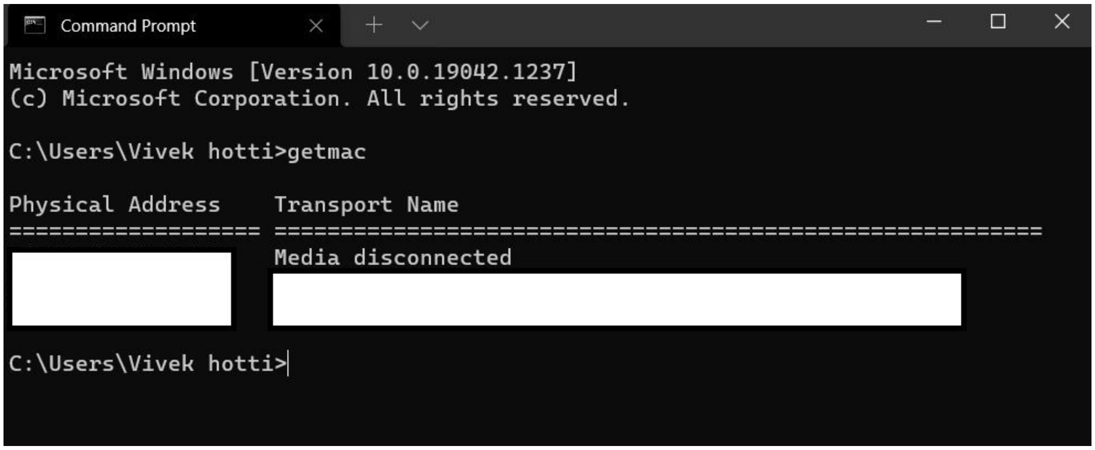
3)Ipconfig command:



```
Microsoft Windows [Version 10.0.19042.1237]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Vivek hotti>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 3:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 12:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : [redacted]
   IPv4 Address. . . . . . . . . . . :
   Subnet Mask . . . . . . . . . . . :
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : [redacted]
   IPv4 Address. . . . . . . . . . . :
   Subnet Mask . . . . . . . . . . . :
   Default Gateway . . . . . . . . . :

C:\Users\Vivek hotti>
```

The command IP config will display basic details about the device's IP address configuration. Just type IP config in the Windows prompt and the IP, subnet mask and default gateway that the current device will be presented. If you have to see full information, then type on command prompt config-all and then you will see full information. There are also choices to assist you in resolving DNS and DHCP issues.

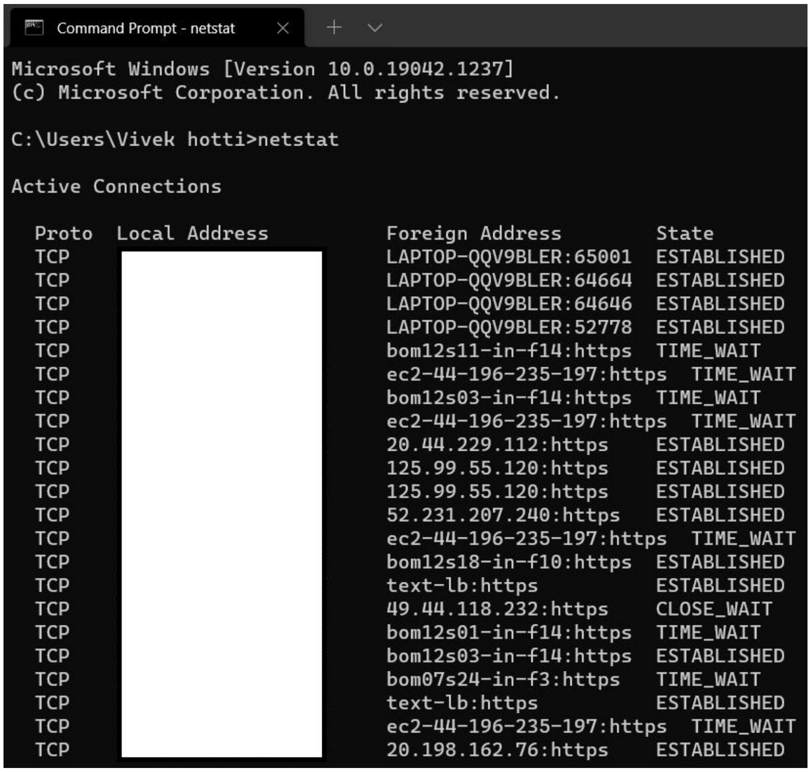
4) getmac command:



```
Microsoft Windows [Version 10.0.19042.1237]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Vivek hotti>getmac

Physical Address    Transport Name
=================== ==========================================================
                    Media disconnected
[redacted]          [redacted]

C:\Users\Vivek hotti>
```

Getmac is a Windows command used to display the Media Access Control (MAC) addresses for each network adapter in the computer. These activities will show you how to use the getmac command to display MAC addresses.

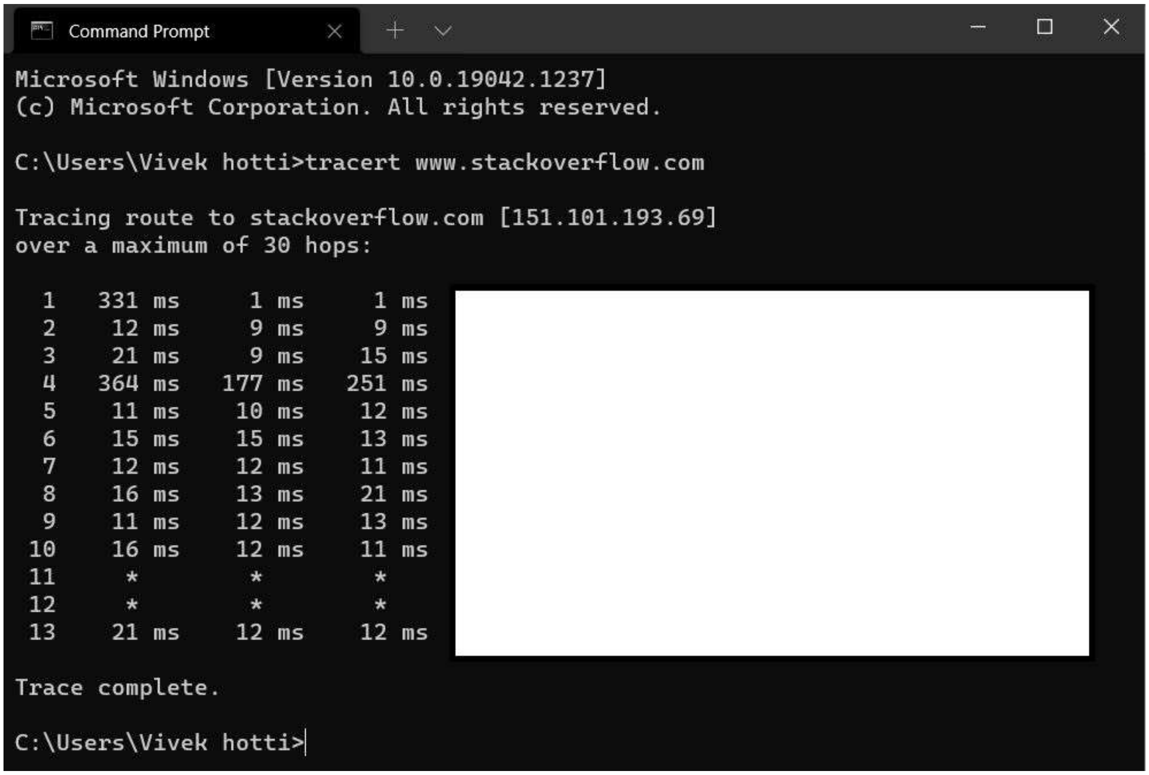
5) netstat command:



```
Microsoft Windows [Version 10.0.19042.1237]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Vivek hotti>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    [redacted]             LAPTOP-QQV9BLER:65001  ESTABLISHED
  TCP                           LAPTOP-QQV9BLER:64664  ESTABLISHED
  TCP                           LAPTOP-QQV9BLER:64646  ESTABLISHED
  TCP                           LAPTOP-QQV9BLER:52778  ESTABLISHED
  TCP                           bom12s11-in-f14:https  TIME_WAIT
  TCP                           ec2-44-196-235-197:https  TIME_WAIT
  TCP                           bom12s03-in-f14:https  TIME_WAIT
  TCP                           ec2-44-196-235-197:https  TIME_WAIT
  TCP                           20.44.229.112:https    ESTABLISHED
  TCP                           125.99.55.120:https    ESTABLISHED
  TCP                           125.99.55.120:https    ESTABLISHED
  TCP                           52.231.207.240:https   ESTABLISHED
  TCP                           ec2-44-196-235-197:https  TIME_WAIT
  TCP                           bom12s18-in-f10:https  ESTABLISHED
  TCP                           text-lb:https          ESTABLISHED
  TCP                           49.44.118.232:https    CLOSE_WAIT
  TCP                           bom12s01-in-f14:https  TIME_WAIT
  TCP                           bom12s03-in-f14:https  ESTABLISHED
  TCP                           bom07s24-in-f3:https   TIME_WAIT
  TCP                           text-lb:https          ESTABLISHED
  TCP                           ec2-44-196-235-197:https  TIME_WAIT
  TCP                           20.198.162.76:https    ESTABLISHED
```

Netstat is a Common TCP – IP networking command-line method present in most Windows, Linux, UNIX, and other operating systems. The netstat provides the statistics and information in the use of the current TCP-IP Connection network about the protocol.

6) tracert command:



```
Microsoft Windows [Version 10.0.19042.1237]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Vivek hotti>tracert www.stackoverflow.com

Tracing route to stackoverflow.com [151.101.193.69]
over a maximum of 30 hops:

  1   331 ms     1 ms     1 ms  [redacted]
  2    12 ms     9 ms     9 ms
  3    21 ms     9 ms    15 ms
  4   364 ms   177 ms   251 ms
  5    11 ms    10 ms    12 ms
  6    15 ms    15 ms    13 ms
  7    12 ms    12 ms    11 ms
  8    16 ms    13 ms    21 ms
  9    11 ms    12 ms    13 ms
 10    16 ms    12 ms    11 ms
 11     *        *        *
 12     *        *        *
 13    21 ms    12 ms    12 ms

Trace complete.

C:\Users\Vivek hotti>
```

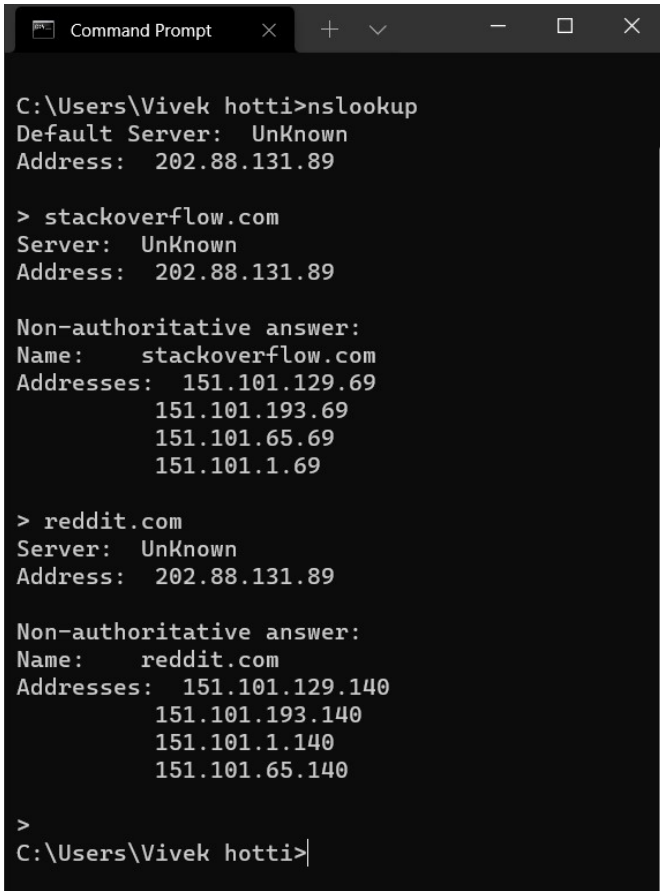
The tracert command is a Command Prompt command which is used to get the network packet being sent and received and the number of hops required for that packet to reach to target. This command can also be referred to as a traceroute. It provides several details about the path that a packet takes from the source to the specified destination.

Options for tracert Command are as follows-

- target: This is the destination, either an IP address or hostname.

- –d: This option prevents Tracert from resolving IP addresses to hostnames to get faster results.
- -h MaxHops: This Tracert option specifies the maximum number of hops in the search for the target. If the MaxHops option is not specified the target has not been found by 30 hops, then the tracert command will stop looking.
- -w timeout: A timeout value must be specified while executing this ping command. It adjusts the amount of time in milliseconds.

7) nslookup command:



```
C:\Users\Vivek hotti>nslookup
Default Server:  UnKnown
Address:  202.88.131.89

> stackoverflow.com
Server:  UnKnown
Address:  202.88.131.89

Non-authoritative answer:
Name:    stackoverflow.com
Addresses:  151.101.129.69
          151.101.193.69
          151.101.65.69
          151.101.1.69

> reddit.com
Server:  UnKnown
Address:  202.88.131.89

Non-authoritative answer:
Name:    reddit.com
Addresses:  151.101.129.140
          151.101.193.140
          151.101.1.140
          151.101.65.140

>
C:\Users\Vivek hotti>
```

The Nslookup, which stands for name server lookup command, is a network utility command used to obtain information about internet servers. It provides name server information for the DNS (Domain Name System), i.e., the default DNS server's name and IP Address.

CONCLUSION:

Hence, we have studied and also implemented different kinds of Networking commands on our terminal.

x-x-x

Experiment 02 Over

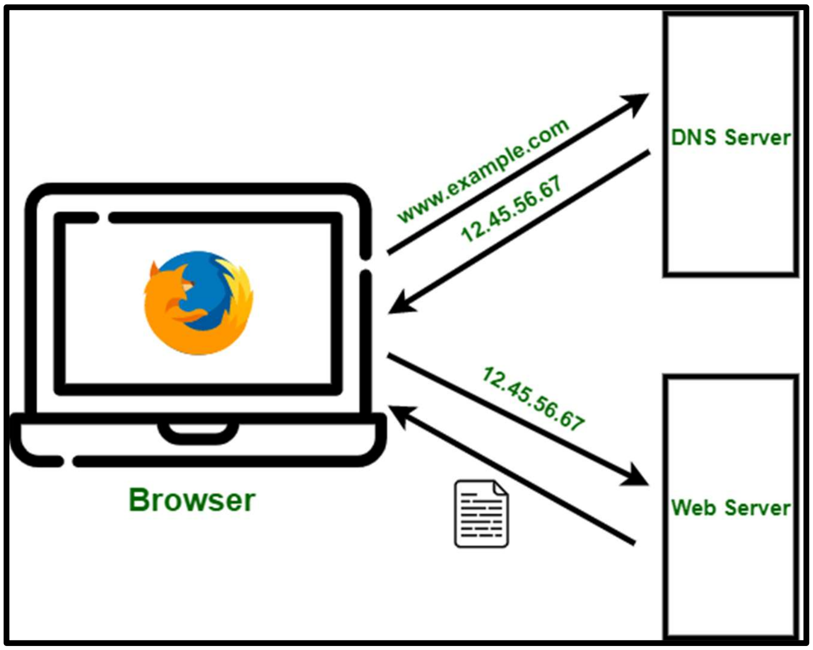
EXPERIMENT – 03

AIM: To Execute a JAVA Program on DNS.

THEORY:

DNS (Domain Name System)

All computers on the Internet, from your smart phone or laptop to the servers that serve content for massive retail websites, find and communicate with one another by using numbers. These numbers are known as IP addresses. When you open a web browser and go to a website, you don't have to remember and enter a long number. Instead, you can enter a domain name like example.com and still end up in the right place.



INPUT:

```
//Inet.java file
import java.net.InetAddress;
import java.net.*;

public class Inet
{
public static void main(String[] args)
{
try
{
        if(args.length>0)
{
String host = args[0];
InetAddress[] addresses = InetAddress.getAllByName(host);
for(InetAddress a : addresses)
        System.out.println(a);
}
else
{
        InetAddress localHost = InetAddress.getLocalHost();
        NetworkInterface networkInterface = NetworkInterface.getByInetAddress(localHost);
        String ipAddress = localHost.getHostAddress();
        String subnetMask =
        “/"+networkInterface.getInterfaceAddresses().get(0).getNetworkPrefixLength();
        System.out.println(ipAddress + subnetMask);
}
}
catch (Exception e)
        {
                e.printStackTrace();
        }
}
}
```

Step1: Create a file called “Inet.java” in your choice directory.

Step2: Copy the above code and paste it in your java file.

Step3: To compile the program, go to your terminal and type:

```
javac Inet.java
```

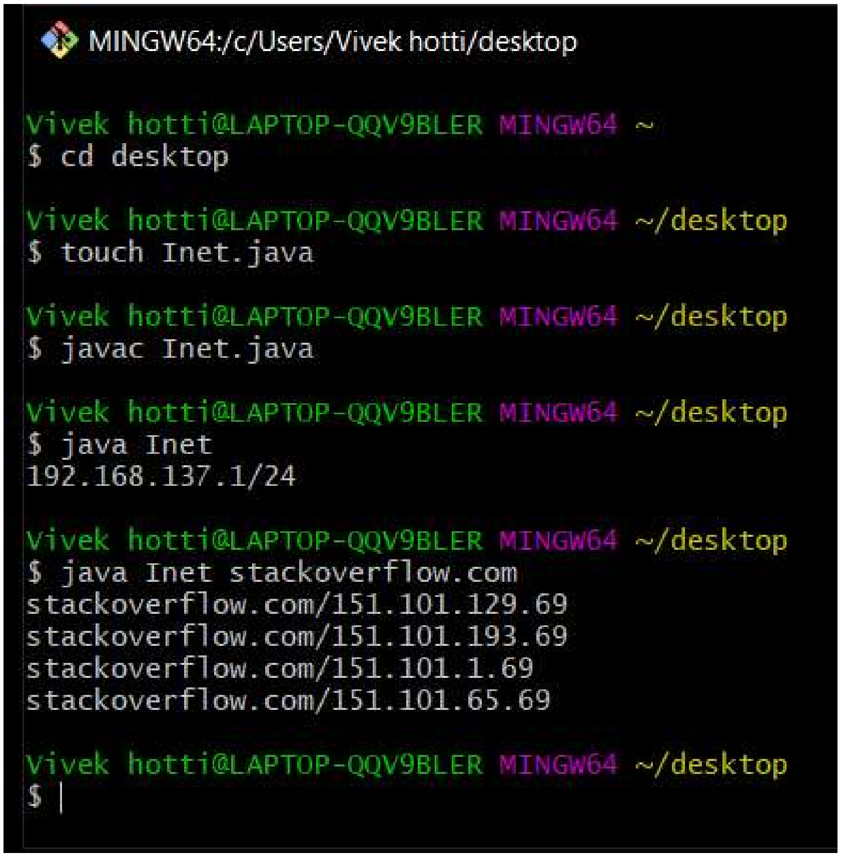
Step4: To run the program, inside the terminal type:

```
java Inet
```

Step4: To run the program, and know the DNS of a specific website, inside the terminal type:

```
java Inet website_name.com
```

OUTPUT:



MINGW64:/c/Users/Vivek hotti/desktop

```
Vivek hotti@LAPTOP-QQV9BLER MINGW64 ~
$ cd desktop

Vivek hotti@LAPTOP-QQV9BLER MINGW64 ~/desktop
$ touch Inet.java

Vivek hotti@LAPTOP-QQV9BLER MINGW64 ~/desktop
$ javac Inet.java

Vivek hotti@LAPTOP-QQV9BLER MINGW64 ~/desktop
$ java Inet
192.168.137.1/24

Vivek hotti@LAPTOP-QQV9BLER MINGW64 ~/desktop
$ java Inet stackoverflow.com
stackoverflow.com/151.101.129.69
stackoverflow.com/151.101.193.69
stackoverflow.com/151.101.1.69
stackoverflow.com/151.101.65.69

Vivek hotti@LAPTOP-QQV9BLER MINGW64 ~/desktop
$ |
```

CONCLUSION:

Hence, we have studied and also executed java program on DNS.

x-x-x

Experiment 03 Over

EXPERIMENT – 04

AIM: To Study JAVA Programs on Socket Programming.

THEORY:

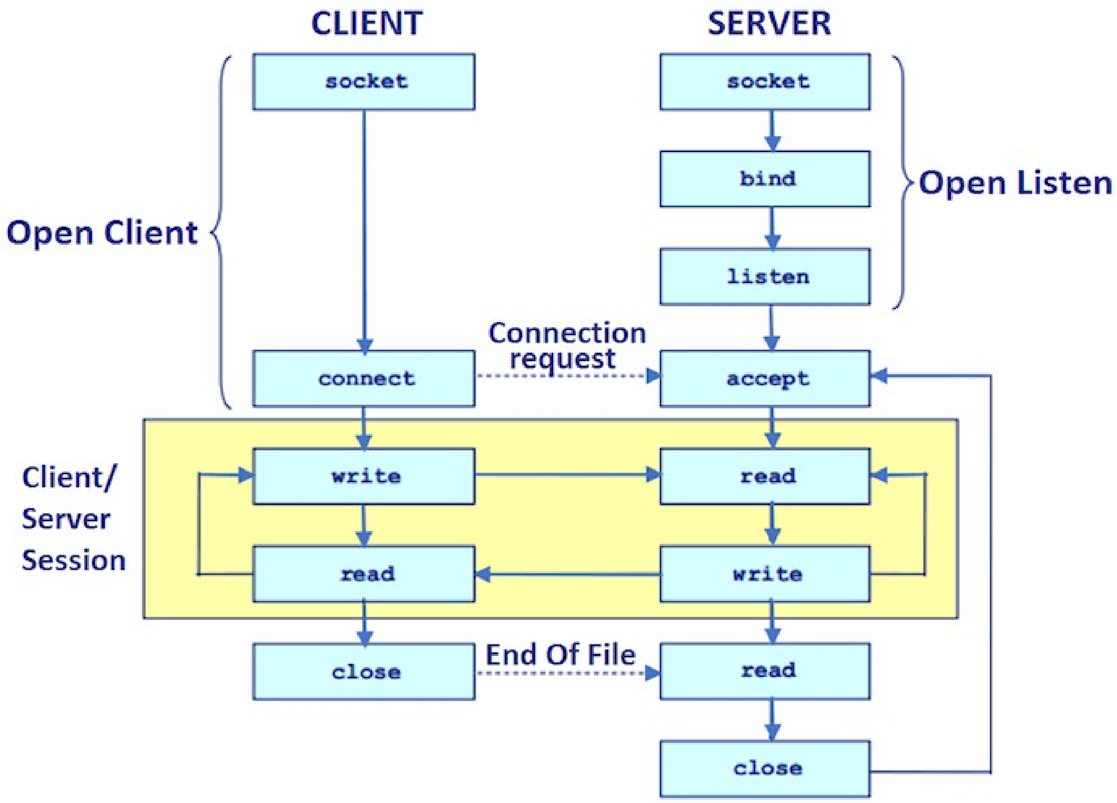
Java Socket programming is used for communication between the applications running on different JRE.

Java Socket programming can be connection-oriented or connection-less. Socket and ServerSocket classes are used for connection-oriented socket programming and DatagramSocket and DatagramPacket classes are used for connection-less socket programming.

The client in socket programming must know two information:

- IP Address of Server, and
- Port number.

Here, we are going to make one-way client and server communication. In this application, client sends a message to the server, server reads the message and prints it. Here, two classes are being used: Socket and ServerSocket. The Socket class is used to communicate client and server. Through this class, we can read and write message. The ServerSocket class is used at server-side. The accept () method of ServerSocket class blocks the console until the client is connected. After the successful connection of client, it returns the instance of Socket at server-side.



SOCKET API

INPUT:

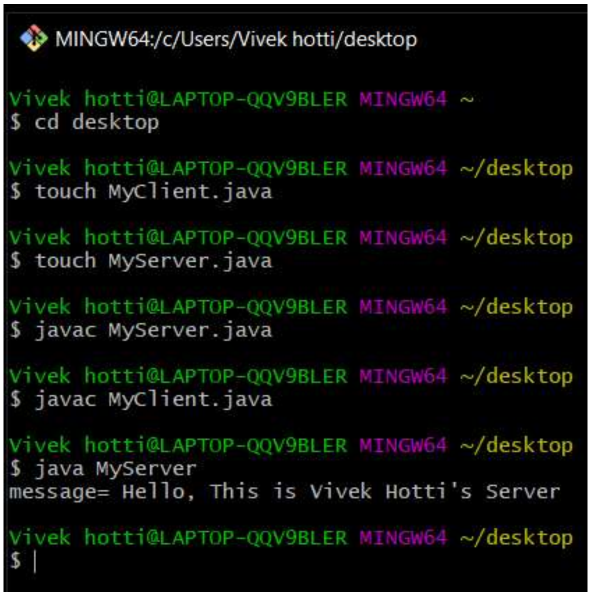
(MyClient.java)

```
import java.io.*;
import java.net.*;
public class MyClient
{
public static void main(String[] args)
            {
            try
            {
            Socket s=new Socket("localhost",6666);
            DataOutputStream dout=new DataOutputStream(s.getOutputStream());
            dout.writeUTF("Hello, This is Vivek Hotti's Server");
            dout.flush();
            dout.close();
            s.close();
            }
            catch(Exception e){System.out.println(e); }}}
```

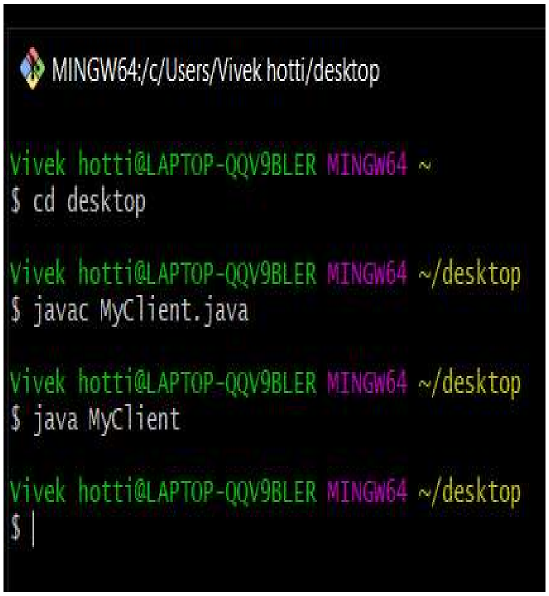
(MyServer.java)

```
import java.io.*;
import java.net.*;
public class MyServer
{
public static void main(String[] args)
        {
        try
        {
        ServerSocket ss=new ServerSocket(6666);
        Socket s=ss.accept();//establishes connection
        DataInputStream dis=new DataInputStream(s.getInputStream());
        String str=(String)dis.readUTF();
        System.out.println("message= "+str); ss.close();
        }
        catch(Exception e){System.out.println(e);}
        }
}
```

OUTPUT:



```
MINGW64:/c/Users/Vivek hotti/desktop

Vivek hotti@LAPTOP-QQV9BLER MINGW64 ~
$ cd desktop

Vivek hotti@LAPTOP-QQV9BLER MINGW64 ~/desktop
$ touch MyClient.java

Vivek hotti@LAPTOP-QQV9BLER MINGW64 ~/desktop
$ touch MyServer.java

Vivek hotti@LAPTOP-QQV9BLER MINGW64 ~/desktop
$ javac MyServer.java

Vivek hotti@LAPTOP-QQV9BLER MINGW64 ~/desktop
$ javac MyClient.java

Vivek hotti@LAPTOP-QQV9BLER MINGW64 ~/desktop
$ java MyServer
message= Hello, This is Vivek Hotti's Server

Vivek hotti@LAPTOP-QQV9BLER MINGW64 ~/desktop
$ |
```



```
MINGW64:/c/Users/Vivek hotti/desktop

Vivek hotti@LAPTOP-QQV9BLER MINGW64 ~
$ cd desktop

Vivek hotti@LAPTOP-QQV9BLER MINGW64 ~/desktop
$ javac MyClient.java

Vivek hotti@LAPTOP-QQV9BLER MINGW64 ~/desktop
$ java MyClient

Vivek hotti@LAPTOP-QQV9BLER MINGW64 ~/desktop
$ |
```

CONCLUSION:

Hence, we have studied and also executed java programs on Socket Programming.

x-x-x

Experiment 04 Over

EXPERIMENT – 05

AIM: Use of Crimping Tool for RJ45.

THEORY:

Crimping an RJ45 Connector Correctly Proper Wiring for Ethernet Cat5/Cat5e Cables:

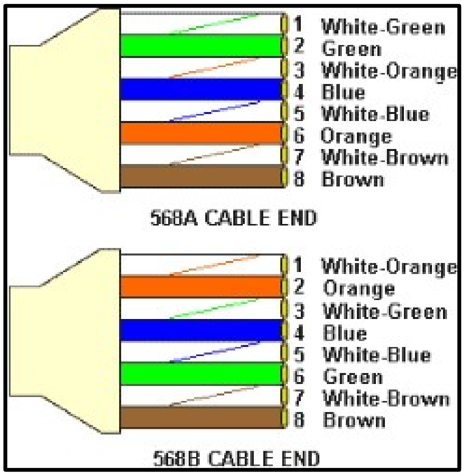
Cables can transmit information along their length. To actually get that information where it needs to go, you need to make the right connections to an RJ45 connector.

Your cable run needs to terminate into a connector, and that connector needs a jack to plug into.

Registered Jack 45 (RJ45) is a standard type of physical connector for network cables. RJ45 connectors are commonly seen with Ethernet cables and networks.

Modern Ethernet cables feature a small plastic plug on each end of the cable. That plug is inserted into RJ45 jacks of Ethernet devices. The term “plug” refers to the cable or “male” end of the connection while the term “jack” refers to the port or “female” end.

T568A or T568B Wiring Standard:



T568A and T568B are the two-colour codes used for wiring eight-position modular plugs. Both are allowed under the ANSI/TIA/EIA wiring standards. The only difference between the two colour codes is that the orange and green pairs are interchanged.

There are no transmission differences between T568A and T568B cabling schemes. North America's preference is for T568B. Both ends must use the same standard. It makes no difference to the transmission characteristics of data.

T568B wiring pattern is recognized as the preferred wiring pattern.

STEP 1:

Using a ***Crimping Tool***, trim the end of the cable you're terminating, to ensure that the ends of the conducting wires are even.

STEP 2:

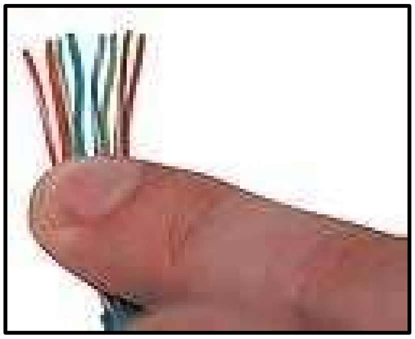
Being careful not to damage the inner conducting wires, strip off approximately 1 inch of the cable's jacket, using a ***modular crimping tool*** or a ***UTP cable stripper***.

STEP 3:

Separate the 4 twisted wire pairs from each other, and then unwind each pair, so that you end up with 8 individual wires. Flatten the wires out as much as possible, since they'll need to be very straight for proper insertion into the connector.

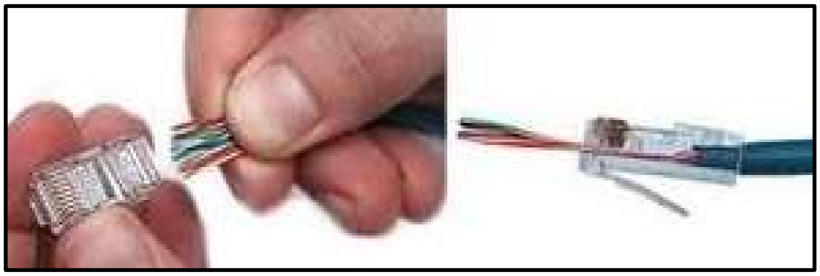
STEP 4:

Holding the cable with the wire ends facing away from you. Moving from left to right, arrange the wires in a flat, side-by-side ribbon formation, placing them in the following order: white/orange, solid orange, white/green, solid blue, white/blue, solid green, white/brown, solid brown.



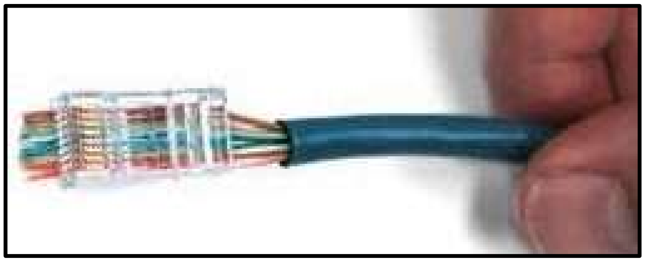
STEP 5:

Holding the RJ45 connector so that its pins are facing away from you and the plug-clip side is facing down, carefully insert the flattened, arranged wires into the connector, pushing through until the wire ends emerge from the pins. For strength of connection, also push as much of the cable jacket as possible into the connector.



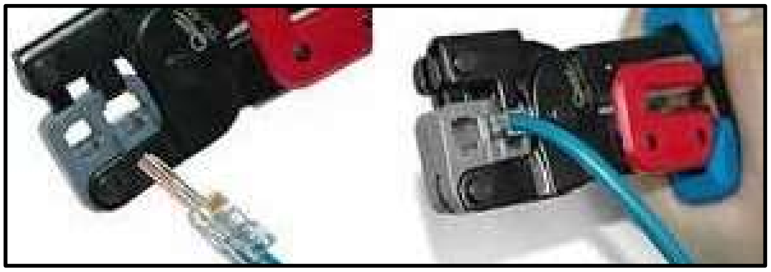
STEP 6:

Check to make sure that the wire ends coming out of the connector's pin side are in the correct order; if not, remove them from the connector, rearrange into proper formation, and re-insert. Remember, once the connector is crimped onto the cable, it's permanent. If you realize that a mistake has been made in wire order after termination, you'll have to cut the connector off and start all over again!



STEP 7:

Insert the prepared connector/cable assembly into the RJ45 slot in ***your crimping tool***. Firmly squeeze the crimper's handles together until you can't go any further. Release the handles and repeat this step to ensure a proper crimp.



STEP 8:

If your crimper doesn't automatically trim the wire ends upon termination, carefully cut wire ends to make them as flush with the connector's surface as possible. The closer the wire ends are trimmed, the better your final plug-in connection will be.

STEP 9:

After the first termination is complete, repeat process on the opposite end of your cable.

CONCLUSION:

Thus, we have studied the use of crimping tool for RJ-45.

x-x-x

Experiment 05 Over

EXPERIMENT – 06

AIM: To study the working of WireShark.

THEORY:

Wire shark is a network packet analyzer. A network packet analyzer presents captured packet data in as much detail as possible.

You could think of a network packet analyzer as a measuring device for examining what's happening inside a network cable, just like an electrician uses a voltmeter for examining what's happening inside an electric cable (but at a higher level, of course).

In the past, such tools were either very expensive, proprietary, or both. However, with the advent of Wireshark, that has changed. Wireshark is available for free, is open source, and is one of the best packets analysers available today.

Here are some reasons people use Wire shark:

- Network administrators use it to troubleshoot network problems
- Network security engineers use it to examine security problems
- QA engineers use it to verify network applications
- Developers use it to debug protocol implementations
- People use it to learn network protocol

Internals Features

The following are some of the many features Wire shark provides:

- Available for UNIX and Windows.
- Capture live packet data from a network interface.
- Open files containing packet data captured with tcpdump/WinDump, Wireshark, and many other packets capture programs.
- Import packets from text files containing hex dumps of packet data.

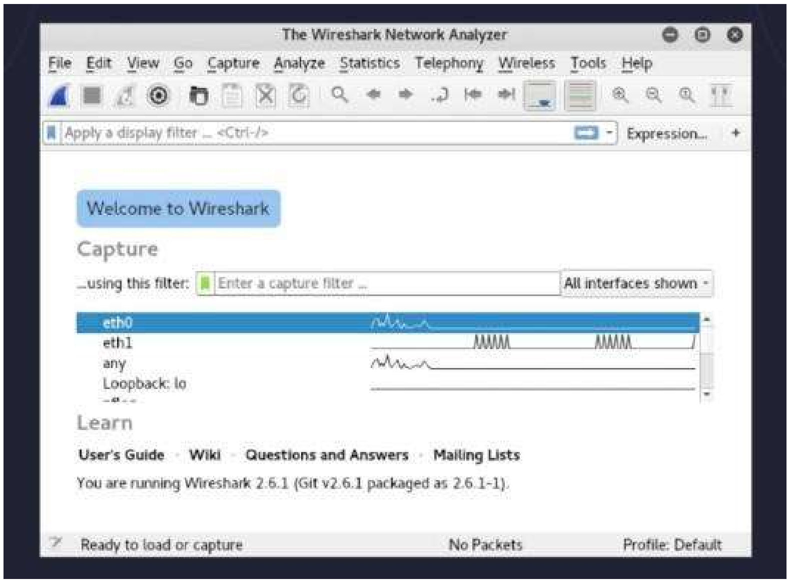
- Display packets with very detailed protocol information.
- Save packet data captured.
- Export some or all packets in a number of capture file formats.
- Filter packets on many criteria.
- Search for packets on many criteria.
- Colorize packet display based on filters.
- Create various statistics.

Data Packets on Wireshark

Now that we have Wireshark installed let's go over how to enable the Wireshark packet sniffer and then analyze the network traffic.

Capturing Data Packets on Wireshark

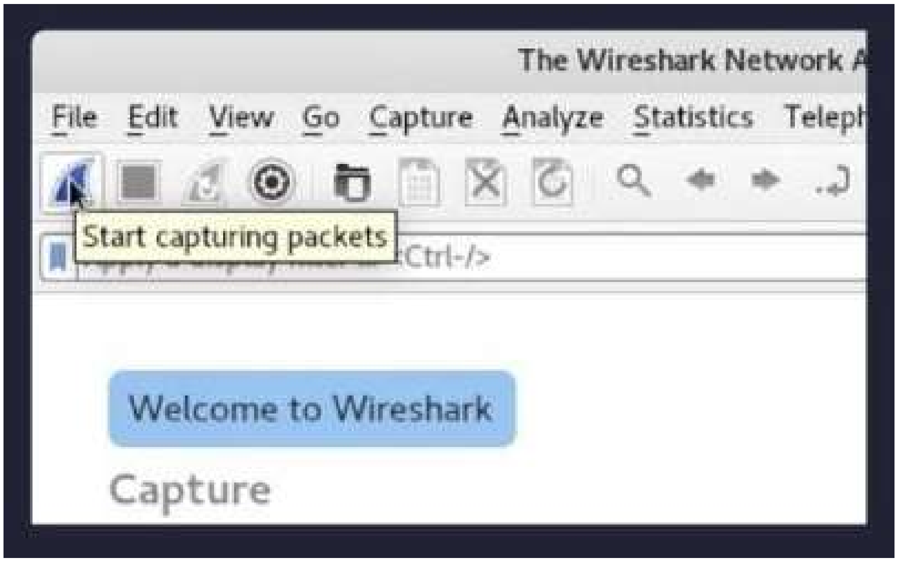
When you open Wireshark, you see a screen that shows you a list of all of the network connections you can monitor. You also have a capture filter field, so you only capture the network traffic you want to see.



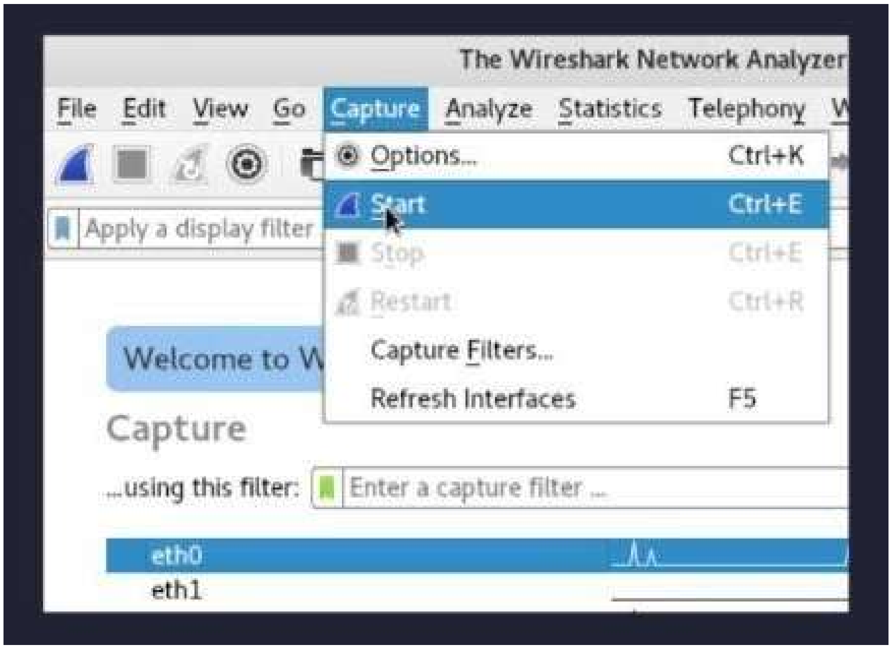
You are running Wireshark 2.6.1 (Git v2.6.1 packaged as 2.6.1-1).

You can select one or more of the network interfaces using "shift left-click." Once you have the network interface selected, you can start the capture, and there are several ways to do that.

Click the first button on the toolbar, titled "**Start Capturing Packets**".

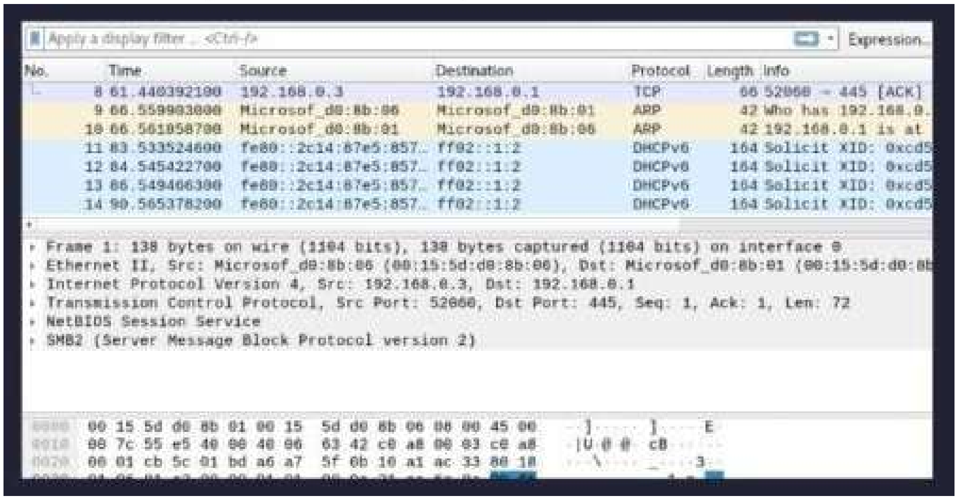


You can select the menu item **Capture -> Start**.



Or you could use the keystroke **Control – E**.

During the capture, Wire shark will show you the packets that it captures in real-time.



```
No.   Time           Source                   Destination          Protocol  Length Info
    8 61.440392100   192.168.0.3              192.168.0.1          TCP           66 52060 → 445 [ACK]
    9 66.559903000   Microsof_d0:8b:06        Microsof_d0:8b:01    ARP           42 Who has 192.168.0.
   10 66.561058700   Microsof_d0:8b:01        Microsof_d0:8b:06    ARP           42 192.168.0.1 is at
   11 83.533524600   fe80::2c14:87e5:857…     ff02::1:2            DHCPv6       164 Solicit XID: 0xcd5
   12 84.545422700   fe80::2c14:87e5:857…     ff02::1:2            DHCPv6       164 Solicit XID: 0xcd5
   13 86.549466300   fe80::2c14:87e5:857…     ff02::1:2            DHCPv6       164 Solicit XID: 0xcd5
   14 90.565378200   fe80::2c14:87e5:857…     ff02::1:2            DHCPv6       164 Solicit XID: 0xcd5

› Frame 1: 138 bytes on wire (1104 bits), 138 bytes captured (1104 bits) on interface 0
› Ethernet II, Src: Microsof_d0:8b:06 (00:15:5d:d0:8b:06), Dst: Microsof_d0:8b:01 (00:15:5d:d0:8b
› Internet Protocol Version 4, Src: 192.168.0.3, Dst: 192.168.0.1
› Transmission Control Protocol, Src Port: 52060, Dst Port: 445, Seq: 1, Ack: 1, Len: 72
› NetBIOS Session Service
› SMB2 (Server Message Block Protocol version 2)

0000  00 15 5d d0 8b 01 00 15  5d d0 8b 06 08 00 45 00   ..]......]....E.
0010  00 7c 55 e5 40 00 40 06  63 42 c0 a8 00 03 c0 a8   .|U.@.@.cB......
0020  00 01 cb 5c 01 bd a6 a7  5f 0b 10 a1 ac 33 80 18   ...\...._....3..
```

CONCLUSION:

Thus, we have studied the working of Wire Shark.

x-x-x

Experiment 06 Over

EXPERIMENT – 07

AIM: To create simple network using cisco packet tracer.

THEORY:

Packet Tracer is a cross-platform visual simulation tool 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. The software is mainly focused towards Certified Cisco Network Associate Academy students as an educational tool for helping them learn fundamental CCNA concepts.

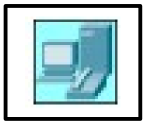
Previously students enrolled in a CCNA Academy program could freely download and use the tool free of charge for educational use.

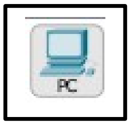
IMPLEMENTATION:

The following are the steps to create a simple network using a cisco packet tracer: -

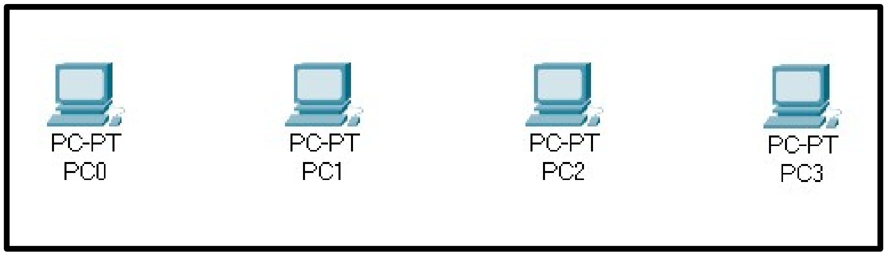
Step 1) Open the Cisco Packet Tracer Application that is installed from their website.

Step 2) On the bottom left toolbar, select End Devices Icon & then Generic PC icon.

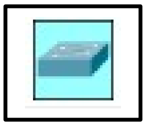




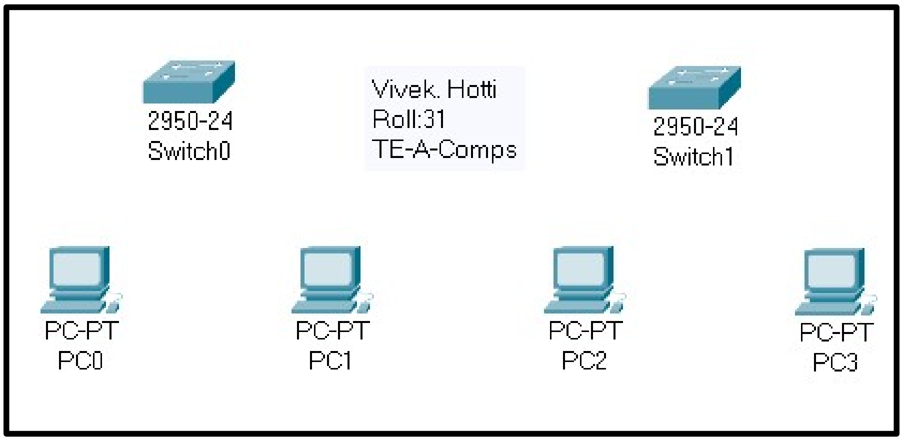
Step 3) Add 4 generic computers on the canvas:



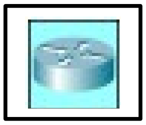
Step 4) Now we have to add switches. So, click on the switches icon, and then on 2950-24 Variant:



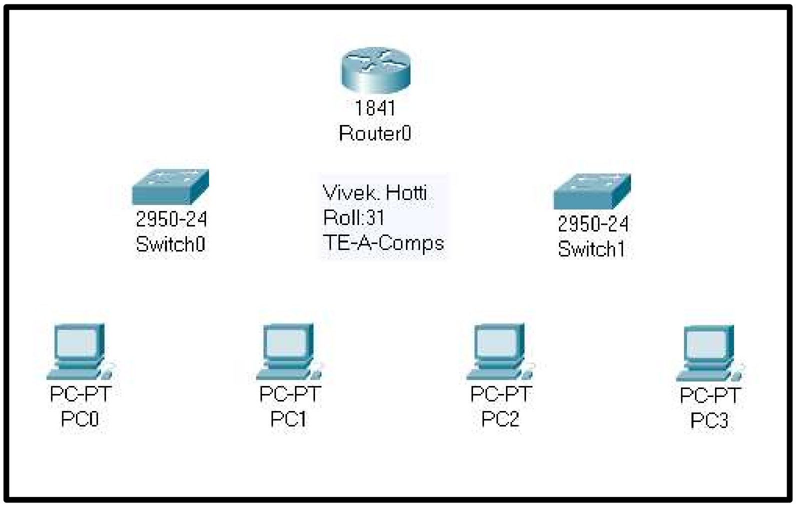
Step 5) And place it in such a manner as below:



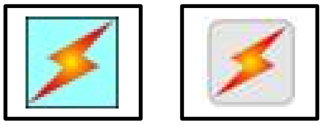
Step 6) Now we have to add Routers. So, click on the router's icon and then on 1841 variant:



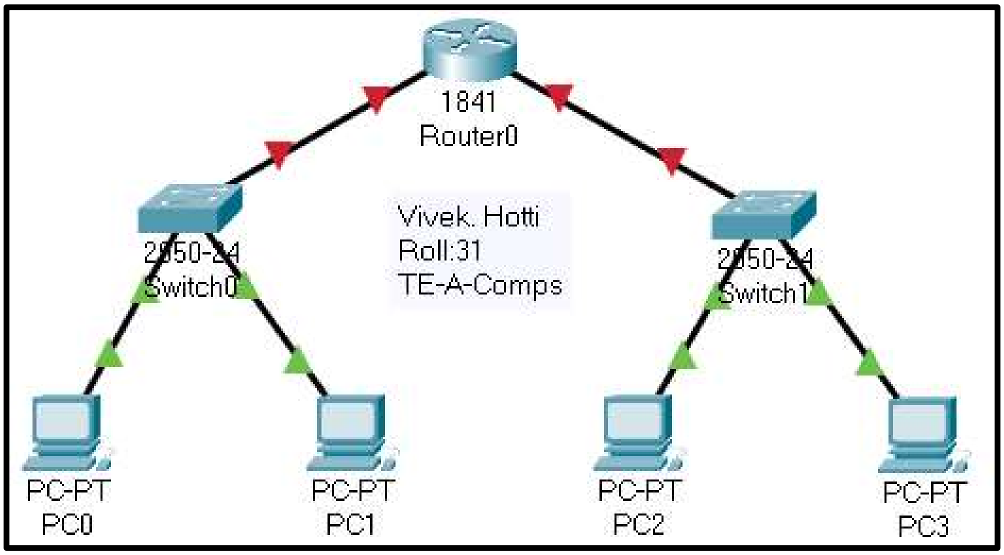
Step 7) And place it in such a manner as below:



Step 8) Now we have to make connections. So, we click on the Connections Icon and then on the Power Variant.

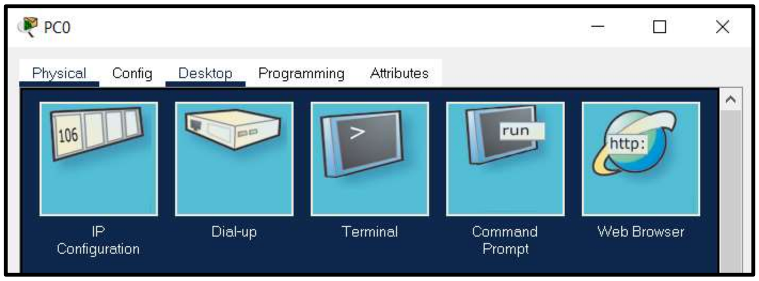


And then make connections like these:

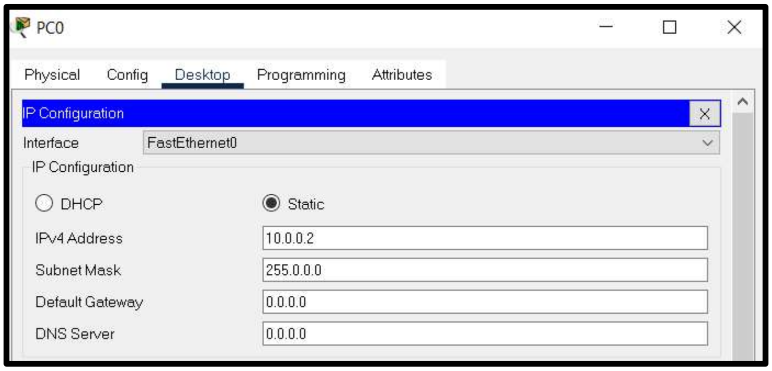


Hence now our structure is ready. Now we need to focus on creating a network.

Step 9) To create a network we have to provide, IP address. To do that, click on a PC on the canvas. A dialog box appears, then click on desktop.



Then click on the first option IP Configuration. And then give an IP address and it generates a subnet mask automatically. And then close the dialog box.



Interface: FastEthernet0

IP Configuration

○ DHCP ● Static

IPv4 Address: 10.0.0.2

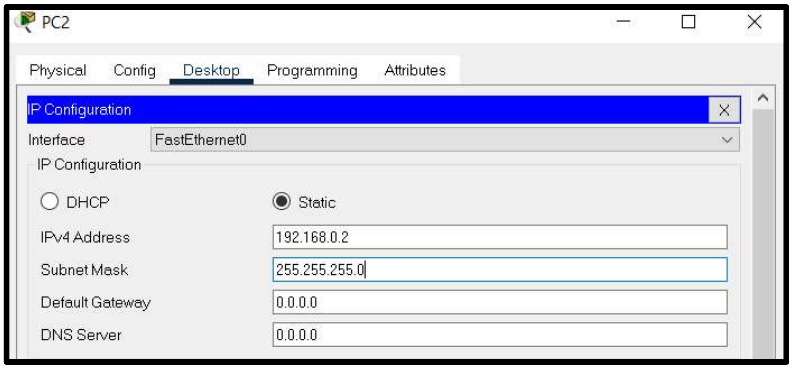
Subnet Mask: 255.0.0.0

Default Gateway: 0.0.0.0

DNS Server: 0.0.0.0

Repeat this for both the PC's, on the left by increasing the last digit by 1.

For the both PC's on right a new IP will be given:



Interface: FastEthernet0

IP Configuration

○ DHCP ● Static

IPv4 Address: 192.168.0.2

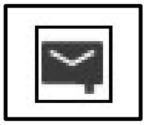
Subnet Mask: 255.255.255.0

Default Gateway: 0.0.0.0

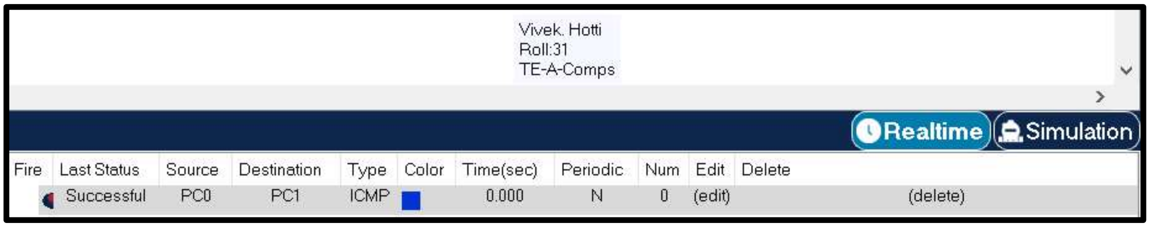
DNS Server: 0.0.0.0

Repeat this for both the PC's, on the right by increasing the last digit by 1.

Step 10) Then click the icon to add a simple PDU. And then on the left-hand cluster click on the first PC and then on the second PC.



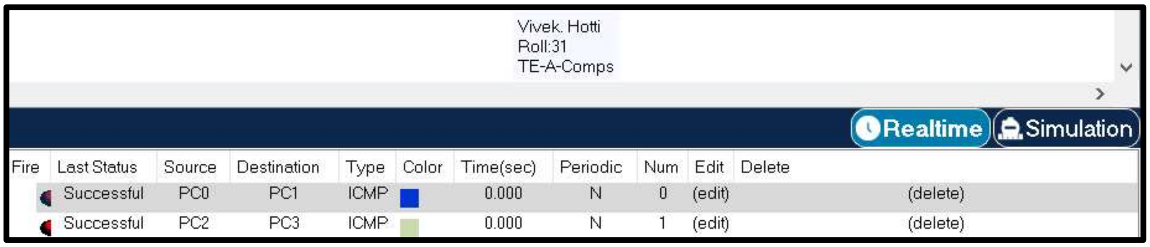
In the bottom right dialog box, you will be able to see the message successful. This means that we have successfully pinged from PC1 to PC2:



Vivek. Hotti
Roll:31
TE-A-Comps

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

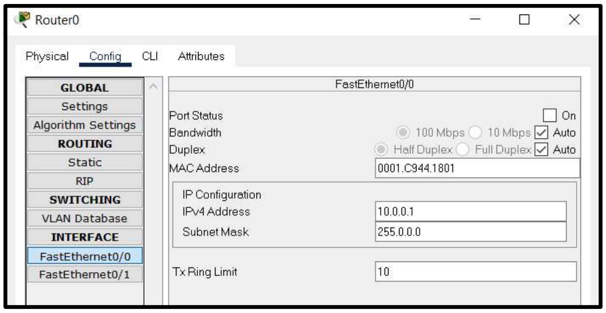
Repeat the same for the right-hand cluster. In the bottom right dialog box, you will be able to see the message successful. This means that we have successfully pinged from PC3 to PC4:



Vivek. Hotti
Roll:31
TE-A-Comps

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
◖	Successful	PC0	PC1	ICMP	🟦	0.000	N	0	(edit)	(delete)
◖	Successful	PC2	PC3	ICMP	🟩	0.000	N	1	(edit)	(delete)

Step 11) Now we need to configure the Router, in order to send messages / successfully ping between PCs of Left-hand and Right-hand clusters. To do that, click on the router on your canvas. A dialog box will appear. Next, click on Config. Then click on Fast Ethernet 0/0. Then provide the first ip address for the left-hand cluster: 10.0.0.1



FastEthernet0/0

Port Status □ On

Bandwidth ● 100 Mbps ○ 10 Mbps ☑ Auto

Duplex ○ Half Duplex ○ Full Duplex ☑ Auto

MAC Address 0001.C944.1801

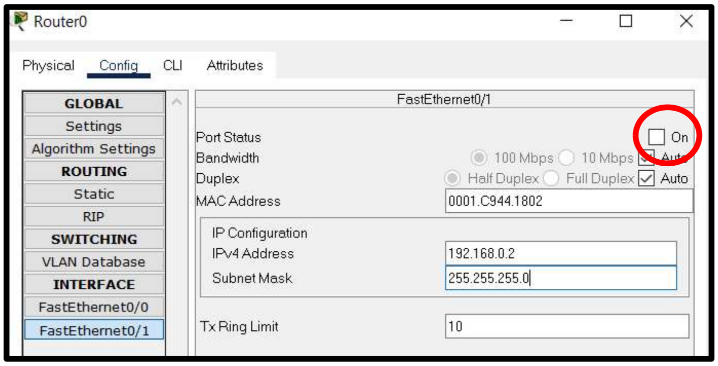
IP Configuration

IPv4 Address 10.0.0.1

Subnet Mask 255.0.0.0

Tx Ring Limit 10

Then click on Fast Ethernet 0/1. Then provide the first ip address for the right-hand cluster: 192.168.0.1



FastEthernet0/1

Port Status □ On

Bandwidth ● 100 Mbps ○ 10 Mbps ☑ Auto

Duplex ○ Half Duplex ○ Full Duplex ☑ Auto

MAC Address 0001.C944.1802

IP Configuration

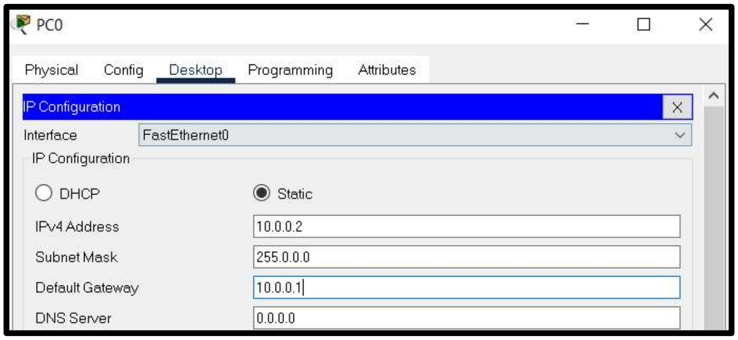
IPv4 Address 192.168.0.2

Subnet Mask 255.255.255.0

Tx Ring Limit 10

Click on the ON button before closing the dialog box in bothe the cases.

Step 12) Now that our router is attached to the switches, we have to provide default gateway to our PCs. For both the PCs in the Left-hand Cluster, it will be 10.0.0.1.



IP Configuration

Interface FastEthernet0

IP Configuration

○ DHCP ● Static

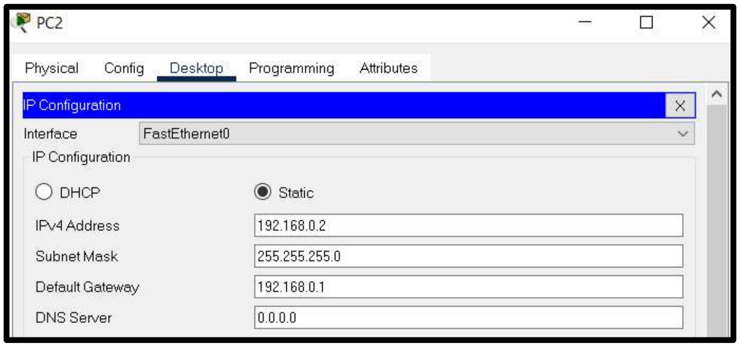
IPv4 Address 10.0.0.2

Subnet Mask 255.0.0.0

Default Gateway 10.0.0.1

DNS Server 0.0.0.0

For both the PCs in the Right-hand Cluster, it will be 192.168.0.1



Interface: FastEthernet0

IP Configuration

○ DHCP ● Static

IPv4 Address: 192.168.0.2

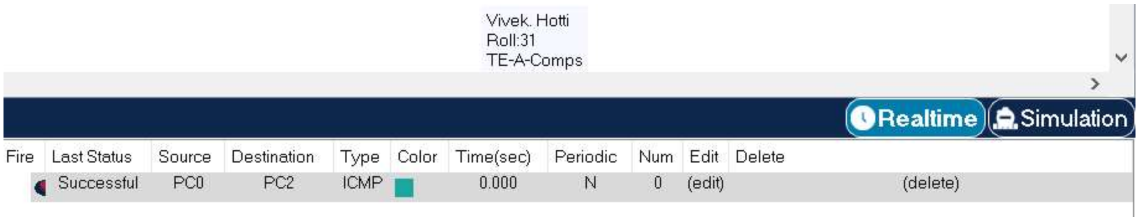
Subnet Mask: 255.255.255.0

Default Gateway: 192.168.0.1

DNS Server: 0.0.0.0

Now try pinging / sending a message from a PC on the left cluster to a PC on the right cluster. If it shows successful, then everything is working properly.

FINAL OUTPUT:



Vivek. Hotti
Roll:31
TE-A-Comps

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
●	Successful	PC0	PC2	ICMP	🟩	0.000	N	0	(edit)	(delete)

CONCLUSION:

Thus, we have studied & practically completed & created a simple network from Cisco Packet Tracer.

x-x-x

Experiment 07 Over

EXPERIMENT – 08

AIM: To create a simple network with Routing Information Protocol using Cisco packet tracer.

THEORY:

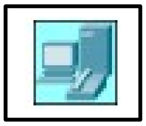
The Routing Information Protocol (RIP) is one of the oldest distance-vector routing protocols which employs the hop count as a routing metric. RIP prevents routing loops by implementing a limit on the number of hops allowed in a path from source to destination.

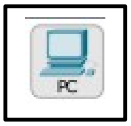
IMPLEMENTATION:

To create a simple network with Routing Information Protocol using Cisco packet tracer, we need to follow the following steps:

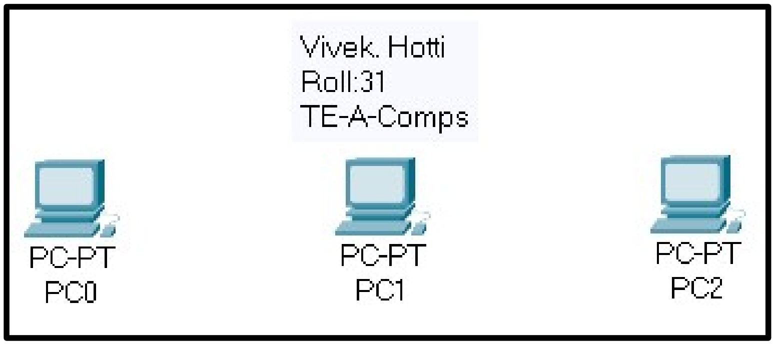
Step 1) Open the Cisco Packet Tracer Application that is installed from their website.

Step 2) On the bottom left toolbar, select End Devices Icon & then Generic PC icon.

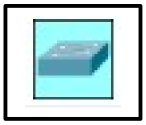


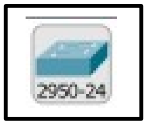


Step 3) Add 3 generic computers on the canvas:

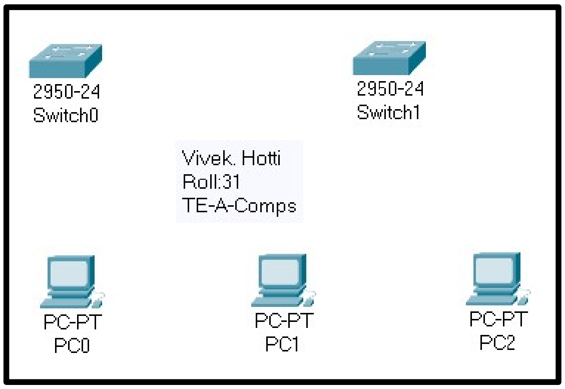


Step 4) Now we have to add switches. So, click on the switches icon, and then on 2950-24 Variant:

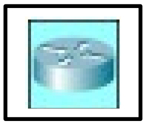


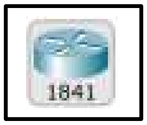


Step 5) And place it in such a manner as below:

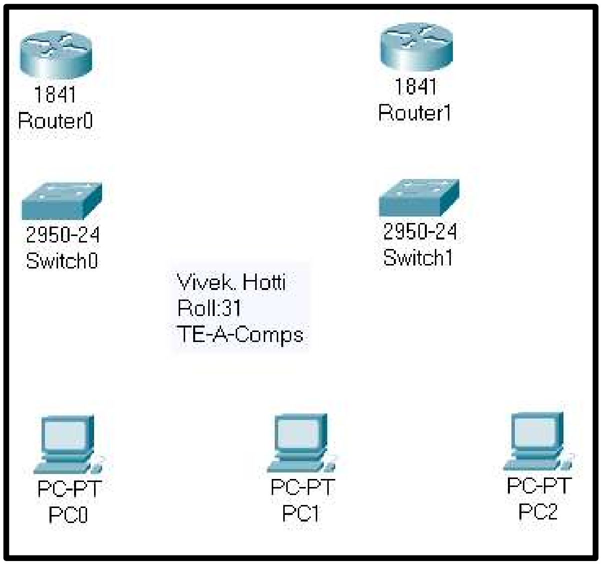


Step 6) Now we have to add Routers. So, click on the router's icon and then on 1841 variant:

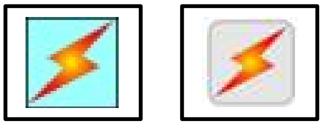




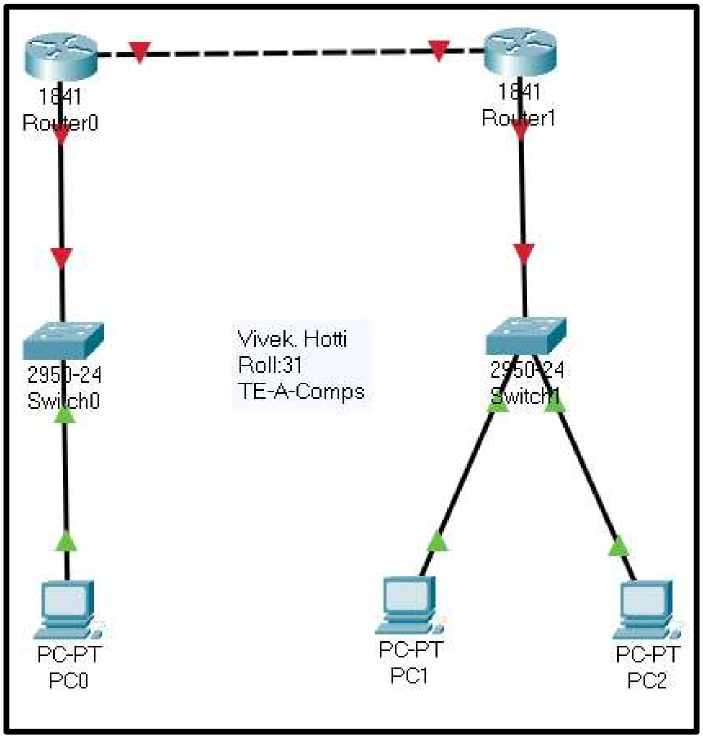
Step 7) And place it in such a manner as below:



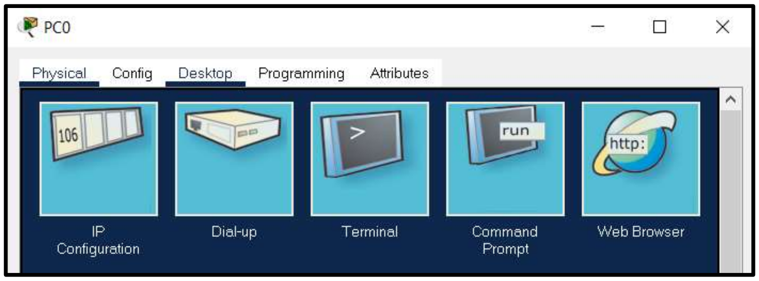
Step 8) Now we have to make connections. So, we click on the Connections Icon and then on the Power Variant.



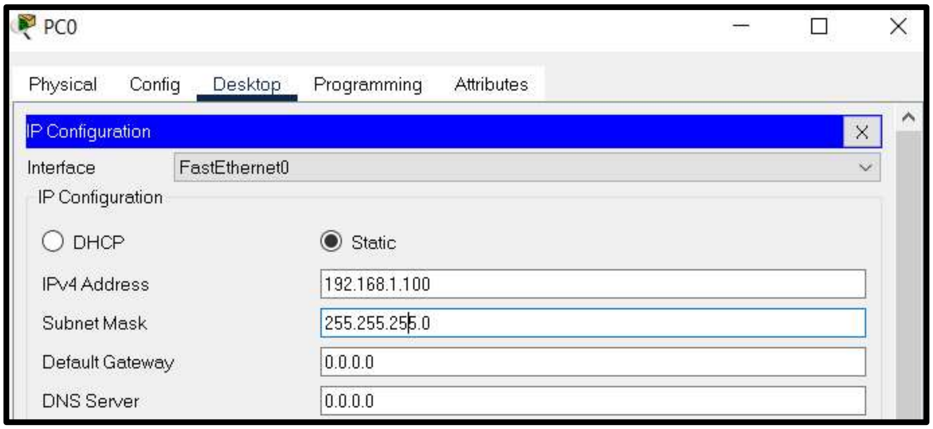
And then make connections like these:



Step 9) Now click on a PC0 on the canvas. A dialog box appears, then click on desktop.



Then click on the first option IP Configuration. And then give an IP address and it generates a subnet mask automatically. And then close the dialog box.



IP Configuration

Interface FastEthernet0

IP Configuration

○ DHCP ● Static

IPv4 Address 192.168.1.100

Subnet Mask 255.255.255.0

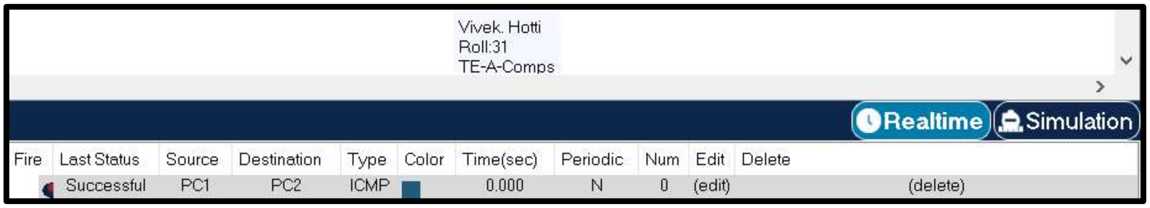
Default Gateway 0.0.0.0

DNS Server 0.0.0.0

Repeat this for PC1 and PC2 by giving them IP's of 192.168.2.100 and 192.168.2.101.

Step 10) Then click the icon to add a simple PDU. And then on the right-hand cluster click on PC1 and then on the PC2.

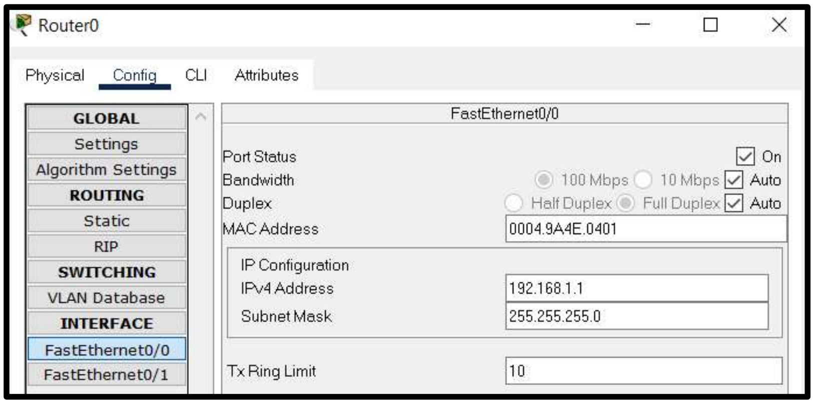
In the bottom right dialog box, you will be able to see the message successful. This means that we have successfully pinged from PC1 to PC2:



Vivek. Hotti
Roll:31
TE-A-Comps

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
●	Successful	PC1	PC2	ICMP	■	0.000	N	0	(edit)	(delete)

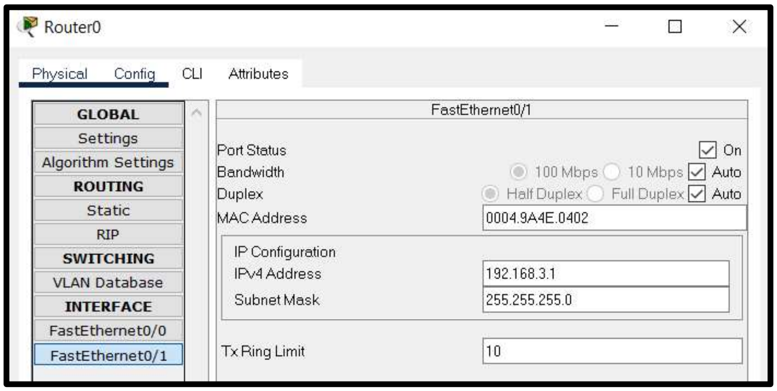
Step 11) Now we need to configure the Router0, in order to send messages / successfully ping between PCs of Left-hand and Right-hand clusters. To do that, click on Router0. A dialog box will appear. Next, click on Config. Then click on Fast Ethernet 0/0. Then provide the ip address: 192.168.1.1



FastEthernet0/0

Port Status ☑ On
Bandwidth ● 100 Mbps ○ 10 Mbps ☑ Auto
Duplex ○ Half Duplex ● Full Duplex ☑ Auto
MAC Address 0004.9A4E.0401
IP Configuration
IPv4 Address 192.168.1.1
Subnet Mask 255.255.255.0
Tx Ring Limit 10

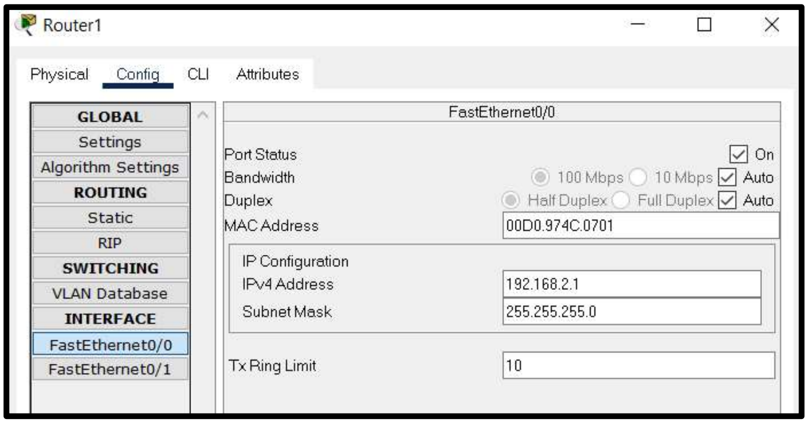
Once again, click on Router0. A dialog box will appear. Next, click on Config. Then click on Fast Ethernet 0/1. Then provide the ip address: 192.168.3.1



FastEthernet0/1

Port Status ☑ On
Bandwidth ● 100 Mbps ○ 10 Mbps ☑ Auto
Duplex ● Half Duplex ○ Full Duplex ☑ Auto
MAC Address 0004.9A4E.0402
IP Configuration
IPv4 Address 192.168.3.1
Subnet Mask 255.255.255.0
Tx Ring Limit 10

Step 12) Now we need to configure the Router1, in order to send messages / successfully ping between PCs of Left-hand and Right-hand clusters. To do that, click on Router1. A dialog box will appear. Next, click on Config. Then click on Fast Ethernet 0/0. Then provide the ip address: 192.168.2.1



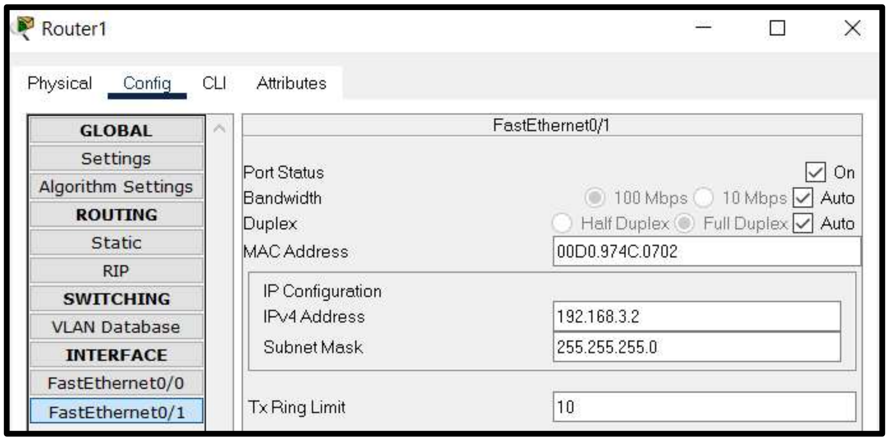
FastEthernet0/0

Port Status ☑ On
Bandwidth ● 100 Mbps ○ 10 Mbps ☑ Auto
Duplex ● Half Duplex ○ Full Duplex ☑ Auto
MAC Address 00D0.974C.0701

IP Configuration
IPv4 Address 192.168.2.1
Subnet Mask 255.255.255.0

Tx Ring Limit 10

Once again, click on Router1. A dialog box will appear. Next, click on Config. Then click on Fast Ethernet 0/1. Then provide the ip address: 192.168.3.2



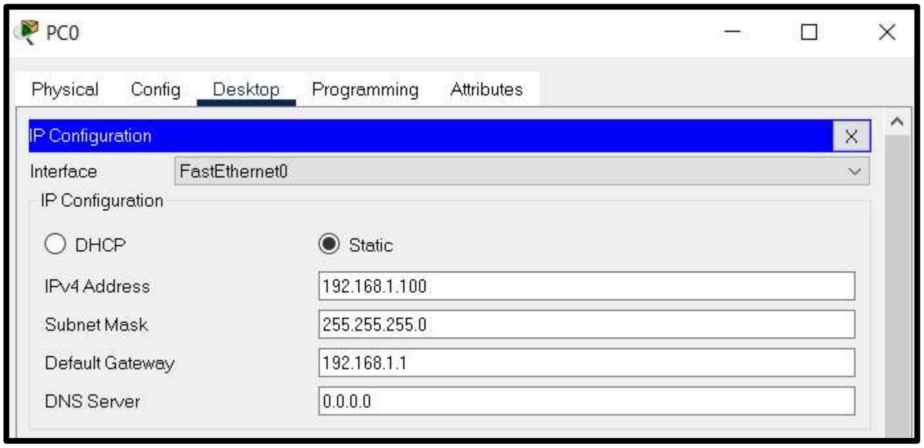
FastEthernet0/1

Port Status ☑ On
Bandwidth ● 100 Mbps ○ 10 Mbps ☑ Auto
Duplex ○ Half Duplex ● Full Duplex ☑ Auto
MAC Address 00D0.974C.0702

IP Configuration
IPv4 Address 192.168.3.2
Subnet Mask 255.255.255.0

Tx Ring Limit 10

Step 12) Now that our router is attached to the switches, we have to provide default gateway to our PCs. For PC0 it will be: 192.168.1.1



IP Configuration

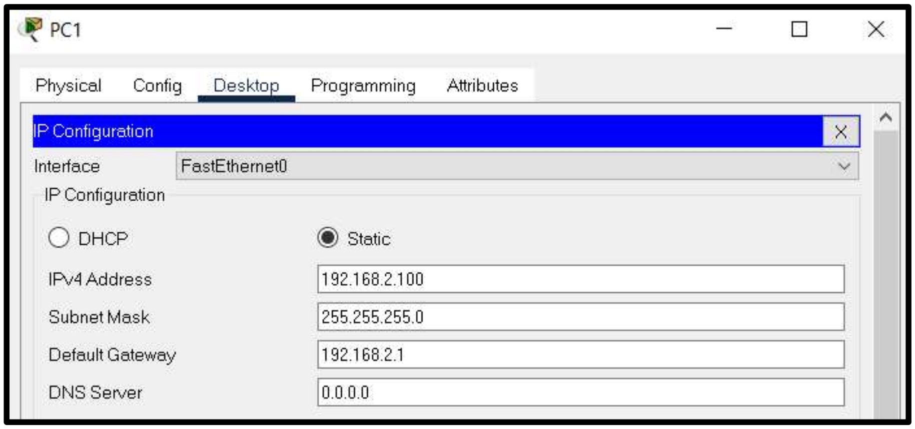
Interface	FastEthernet0

IP Configuration

○ DHCP ● Static

IPv4 Address	192.168.1.100
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1
DNS Server	0.0.0.0

For PC1 & PC2, it will be: 192.168.2.1



IP Configuration

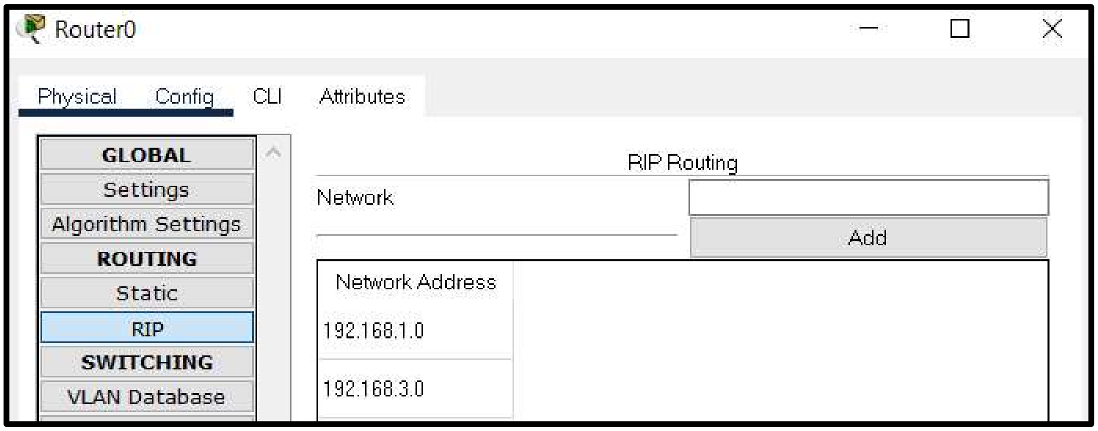
Interface	FastEthernet0

IP Configuration

○ DHCP ● Static

IPv4 Address	192.168.2.100
Subnet Mask	255.255.255.0
Default Gateway	192.168.2.1
DNS Server	0.0.0.0

Step 12) Now we have to provide identity to the routers so that they can communicate amongst themselves. We need to setup the Routing Information Protocol. Click on Router 0 & select RIP from the dialog box and enter the Ips: 192.169.1.0 & 192.168.3.0 one by one and click add.

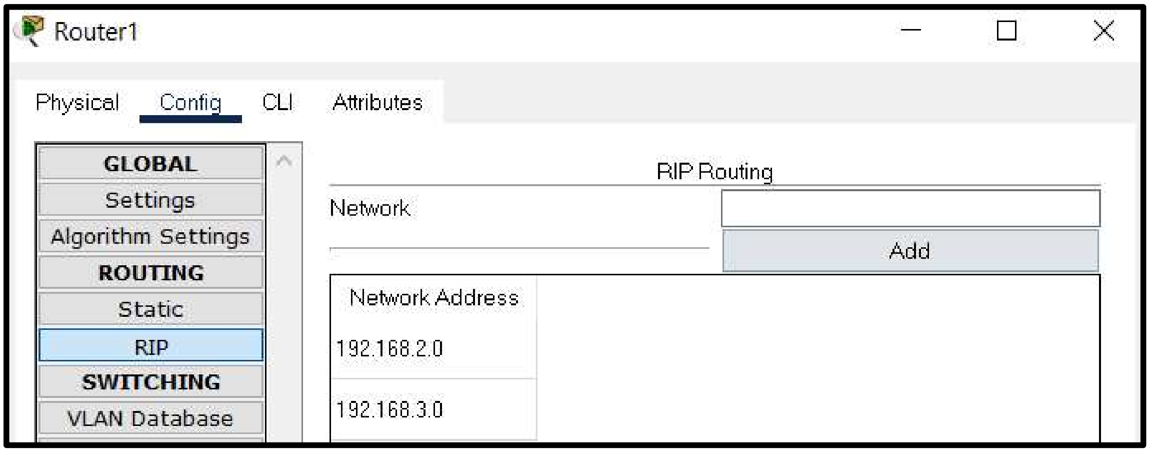


RIP Routing

Network

Network Address
192.168.1.0
192.168.3.0

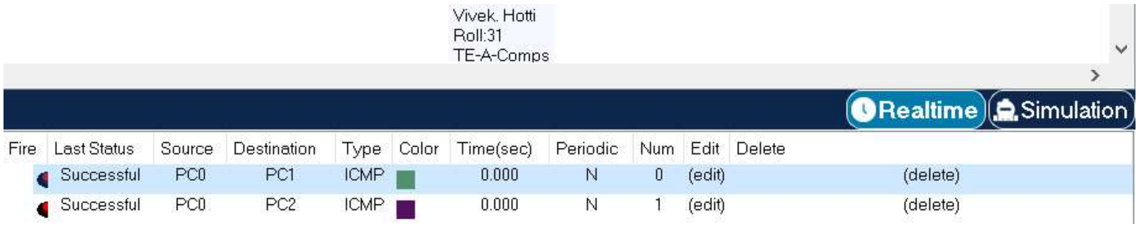
Same now we do with Router 1. We enter the Ips: 192.168.2.0 & 192.168.3.0 one by one and click add:



Network Address
192.168.2.0
192.168.3.0

Now try pinging / sending a message from a PC on the left cluster to a PC on the right cluster. If it shows successful, then everything is working properly as shown in the Final Output Below.

FINAL OUTPUT:



Vivek. Hotti
Roll:31
TE-A-Comps

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	PC0	PC1	ICMP	🟩	0.000	N	0	(edit)	(delete)
	Successful	PC0	PC2	ICMP	🟪	0.000	N	1	(edit)	(delete)

CONCLUSION:

Hence, we created a network with Routing Information Protocol using Cisco packet tracer.

x-x-x

Experiment 08 Over

EXPERIMENT – 09

AIM: To create network with VLAN using cisco packet tracer.

THEORY:

A VLAN (virtual LAN) is a subnetwork which can group together collections of devices on separate physical local area networks (LANs). A LAN is a group of computers and devices that share a communications line or wireless link to a server within the same geographical area.

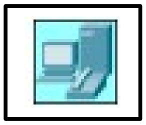
VLANs make it easy for network administrators to partition a single switched network to match the functional and security requirements of their systems without having to run new cables or make major changes in their current network infrastructure. VLANs are often set up by larger businesses to re-partition devices for better traffic management.

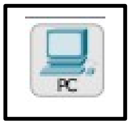
IMPLEMENTATION:

To create a network with VLAN using Cisco packet tracer, we need to follow the following steps:

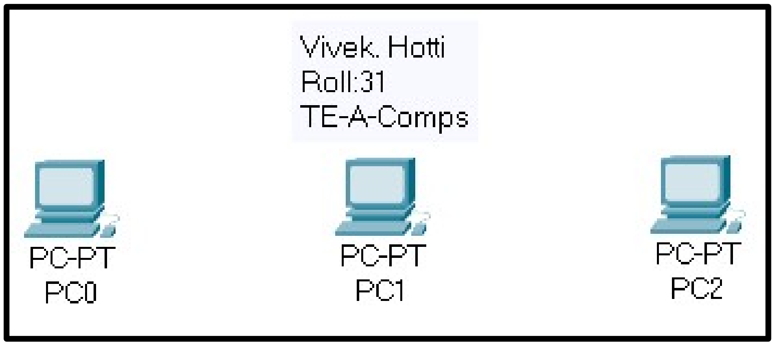
Step 1) Open the Cisco Packet Tracer Application that is installed from their website.

Step 2) On the bottom left toolbar, select End Devices Icon & then Generic PC icon.

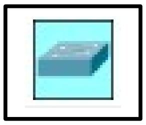


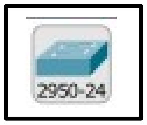


Step 3) Add 3 generic computers on the canvas:

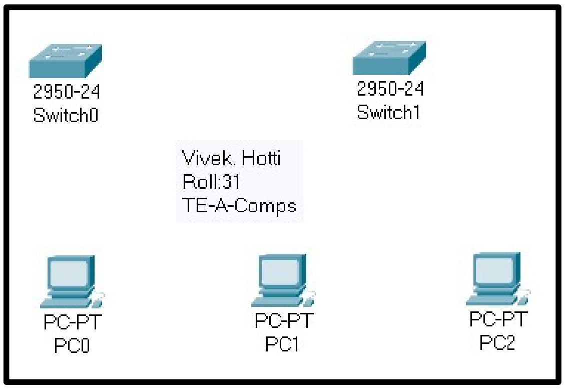

Vivek. Hotti
Roll:31
TE-A-Comps

Step 4) Now we have to add switches. So, click on the switches icon, and then on 2950-24 Variant:

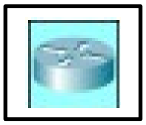


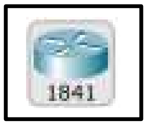


Step 5) And place it in such a manner as below:

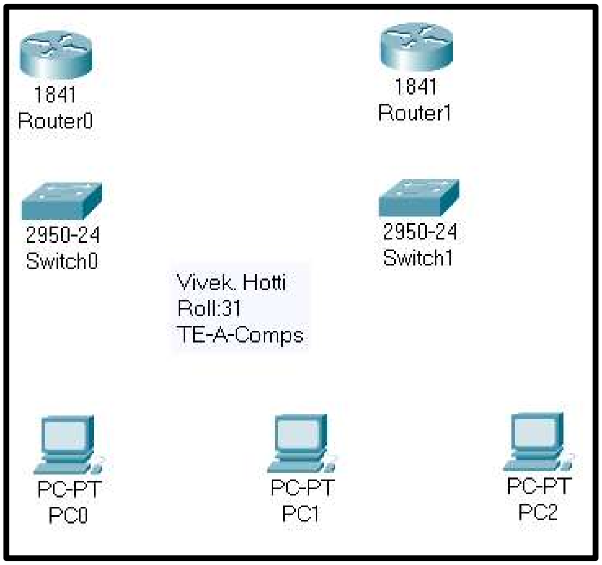

Vivek. Hotti
Roll:31
TE-A-Comps

Step 6) Now we have to add Routers. So, click on the router's icon and then on 1841 variant:

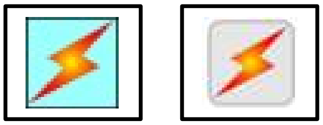




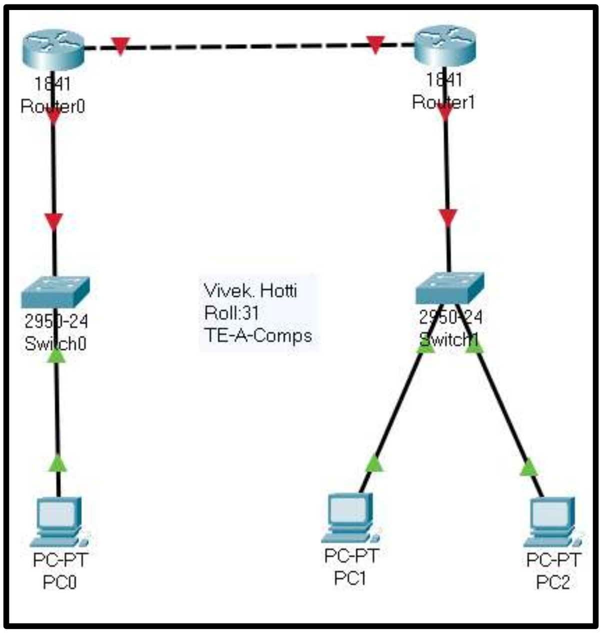
Step 7) And place it in such a manner as below:



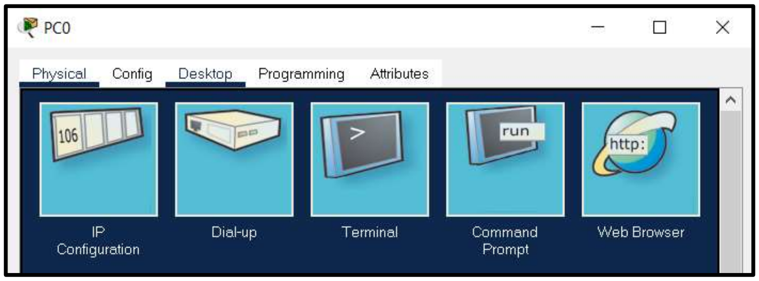
Step 8) Now we have to make connections. So, we click on the Connections Icon and then on the Power Variant.



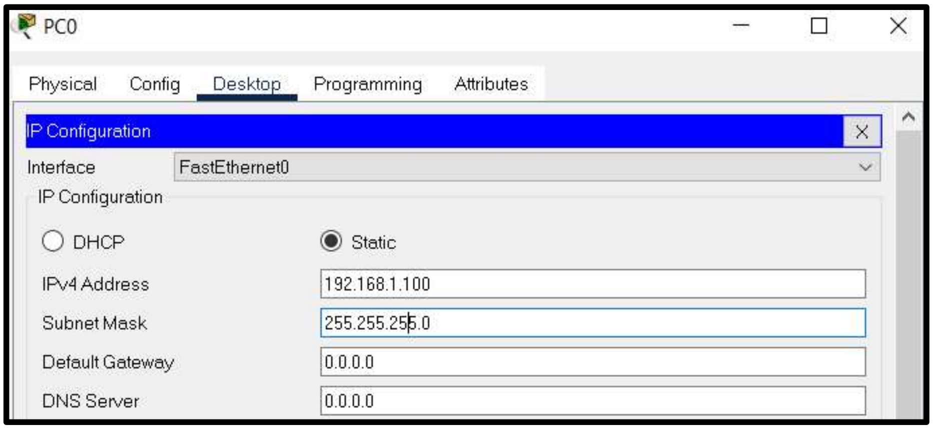
And then make connections like these:



Step 9) Now click on a PC0 on the canvas. A dialog box appears, then click on desktop.



Then click on the first option IP Configuration. And then give an IP address and it generates a subnet mask automatically. And then close the dialog box.



Interface FastEthernet0

IP Configuration

○ DHCP ● Static

IPv4 Address 192.168.1.100

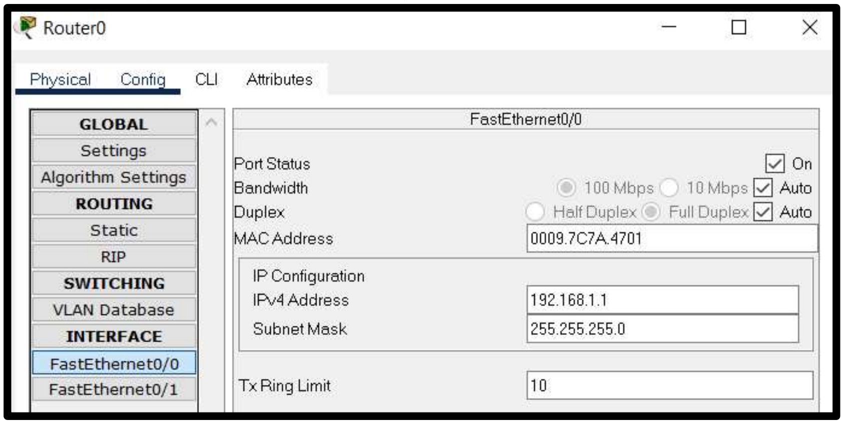
Subnet Mask 255.255.255.0

Default Gateway 0.0.0.0

DNS Server 0.0.0.0

Repeat this for PC1 and PC2 by giving them IP's of 192.168.2.100 and 192.168.2.101.

Step 10) Now we configure the router. To do that click on Router0. A dialog box will appear. Next, click on Config. Then click on Fast Ethernet 0/0. Then provide the ip address: 192.168.1.1



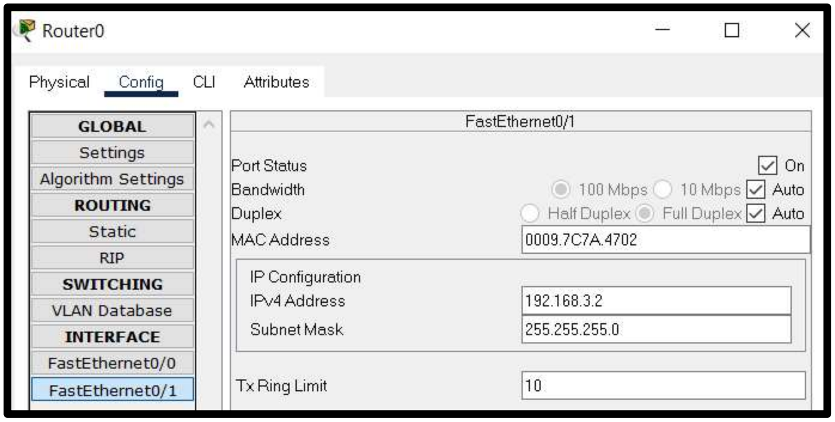
FastEthernet0/0

Port Status ☑ On
Bandwidth ● 100 Mbps ○ 10 Mbps ☑ Auto
Duplex ○ Half Duplex ● Full Duplex ☑ Auto
MAC Address 0009.7C7A.4701

IP Configuration
IPv4 Address 192.168.1.1
Subnet Mask 255.255.255.0

Tx Ring Limit 10

Then for the same Router 0 click on Fast Ethernet 0/1. Then provide the ip address: 192.168.3.2



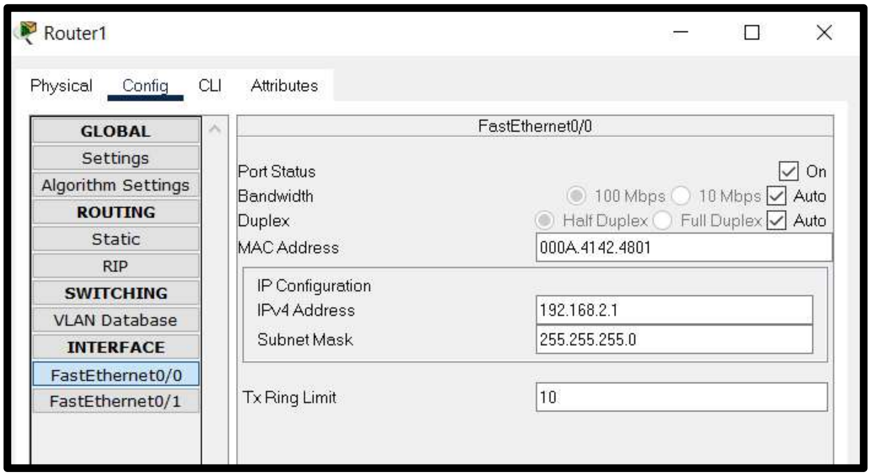
FastEthernet0/1

Port Status ☑ On
Bandwidth ● 100 Mbps ○ 10 Mbps ☑ Auto
Duplex ○ Half Duplex ● Full Duplex ☑ Auto
MAC Address 0009.7C7A.4702

IP Configuration
IPv4 Address 192.168.3.2
Subnet Mask 255.255.255.0

Tx Ring Limit 10

Do the same thing for Router 1. For Ethernet 0/0, provide the ip address: 192.168.2.1



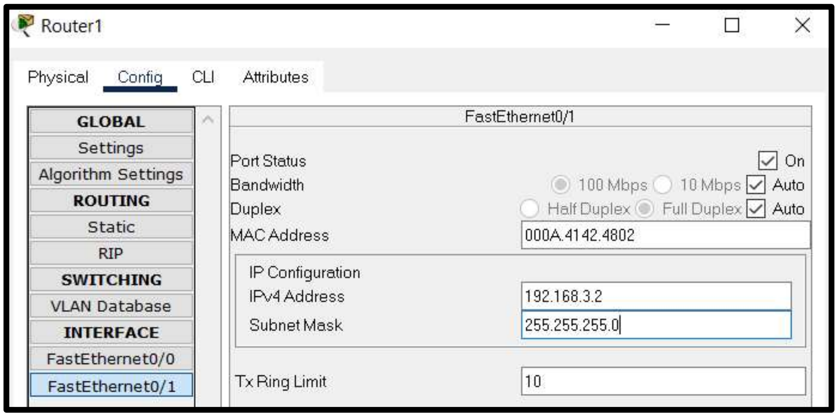
FastEthernet0/0

Port Status ☑ On
Bandwidth ● 100 Mbps ○ 10 Mbps ☑ Auto
Duplex ● Half Duplex ○ Full Duplex ☑ Auto
MAC Address 000A.4142.4801

IP Configuration
IPv4 Address 192.168.2.1
Subnet Mask 255.255.255.0

Tx Ring Limit 10

For Ethernet 0/1, provide the ip address: 192.168.3.2



Router1

FastEthernet0/1

Port Status ☑ On

Bandwidth ● 100 Mbps ○ 10 Mbps ☑ Auto

Duplex ○ Half Duplex ● Full Duplex ☑ Auto

MAC Address 000A.4142.4802

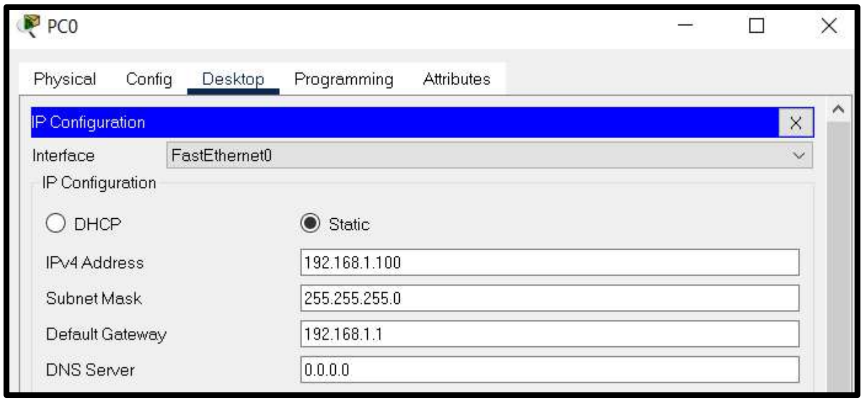
IP Configuration

IPv4 Address 192.168.3.2

Subnet Mask 255.255.255.0

Tx Ring Limit 10

Step 10) Now we have to setup default gateway of each PC. For PC0, it is: 192.168.1.1. For PC1 & PC2 it is 192.168.2.1



PC0

IP Configuration

Interface FastEthernet0

IP Configuration

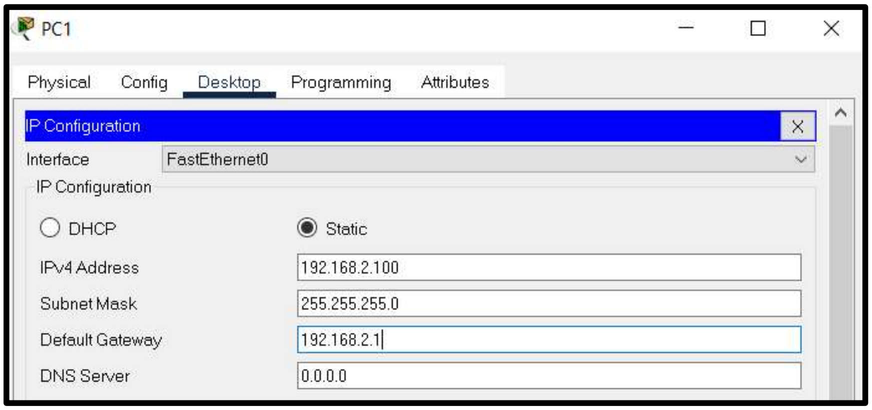
○ DHCP ● Static

IPv4 Address 192.168.1.100

Subnet Mask 255.255.255.0

Default Gateway 192.168.1.1

DNS Server 0.0.0.0



PC1

IP Configuration

Interface FastEthernet0

IP Configuration

○ DHCP ● Static

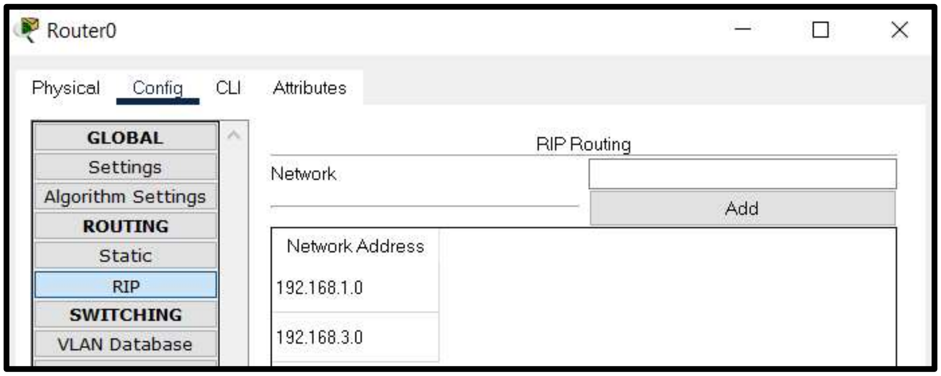
IPv4 Address 192.168.2.100

Subnet Mask 255.255.255.0

Default Gateway 192.168.2.1

DNS Server 0.0.0.0

Step 11) Now we have to provide identity to the routers so that they can communicate amongst themselves. We need to setup the Routing Information Protocol. Click on Router 0 & select RIP from the dialog box and enter the Ips: 192.169.1.0 & 192.168.3.0 one by one and click add.



RIP Routing

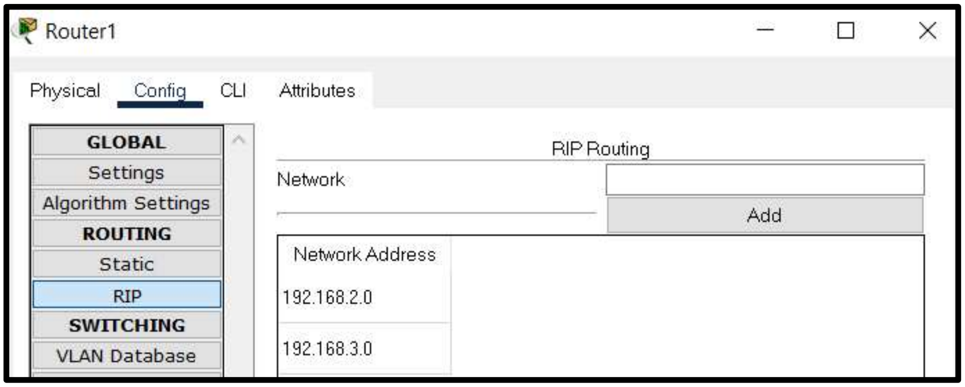
Network

Network Address

192.168.1.0

192.168.3.0

Same now we do with Router 1. We enter the Ips: 192.168.2.0 & 192.168.3.0 one by one and click add:



RIP Routing

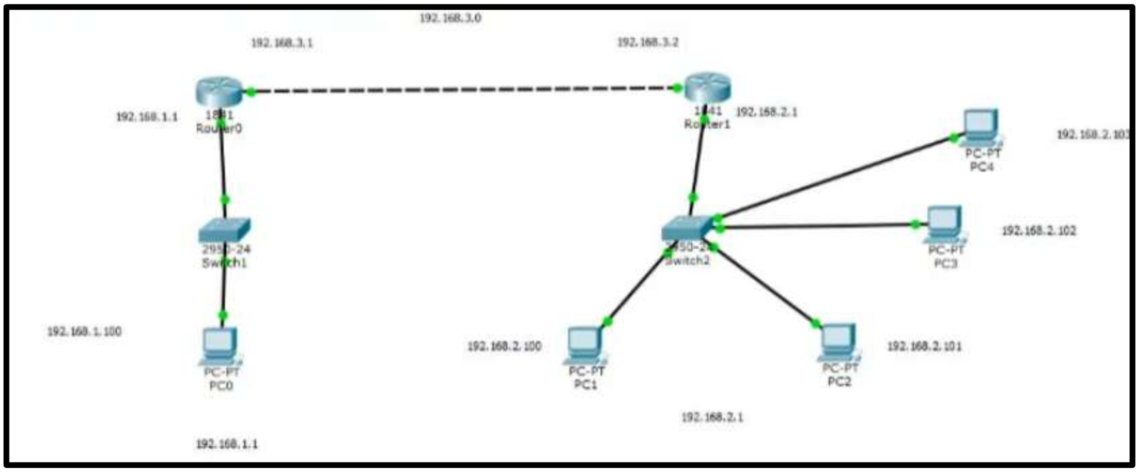
Network

Network Address

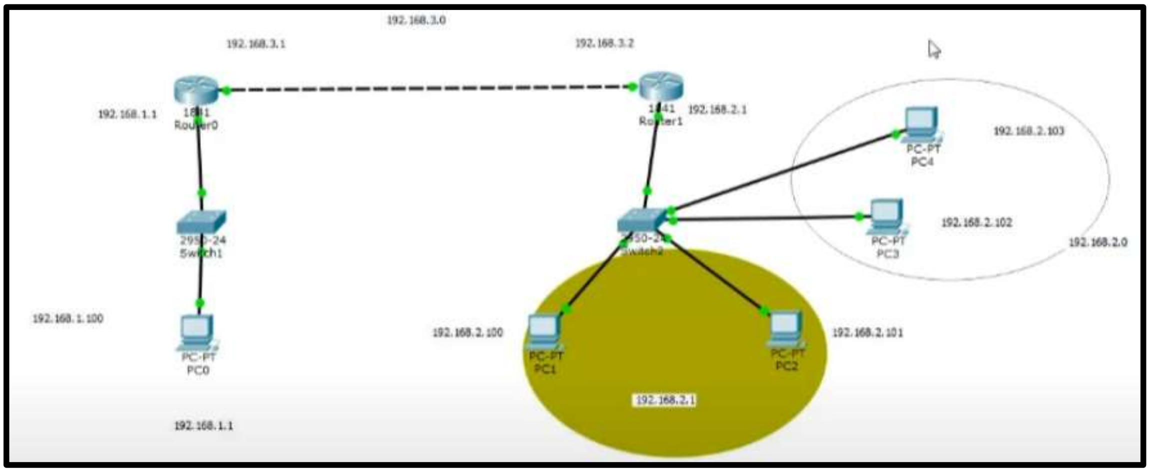
192.168.2.0

192.168.3.0

Step 12) Adding more PC's.



FINAL OUTPUT:



CONCLUSION:

Hence, we created a VLAN using Cisco packet tracer.

x-x-x

Experiment 09 Over

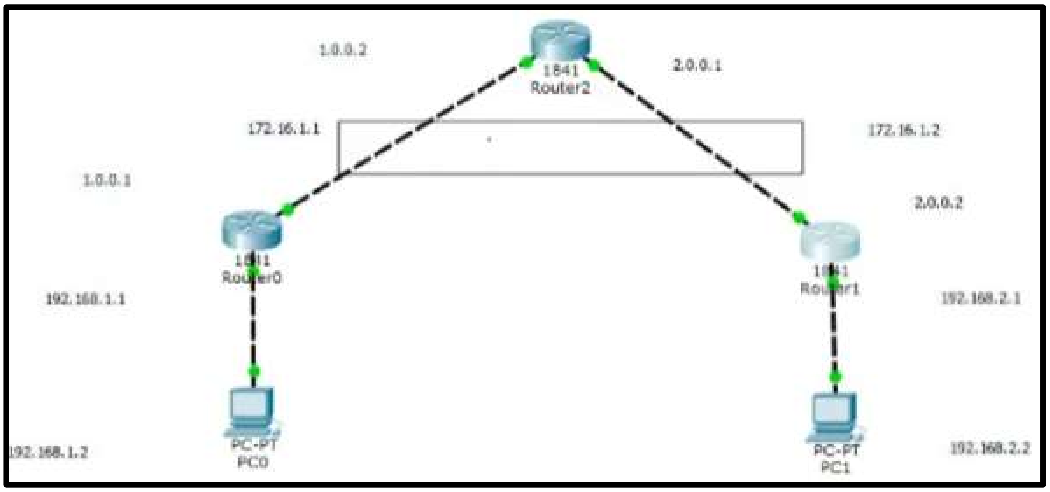
EXPERIMENT – 10

AIM: To create network with Virtual Private Network using cisco packet tracer.

THEORY:

A virtual private network, or VPN, is an encrypted connection over the Internet from a device to a network. The encrypted connection helps ensure that sensitive data is safely transmitted. It prevents unauthorized people from eavesdropping on the traffic and allows the user to conduct work remotely.

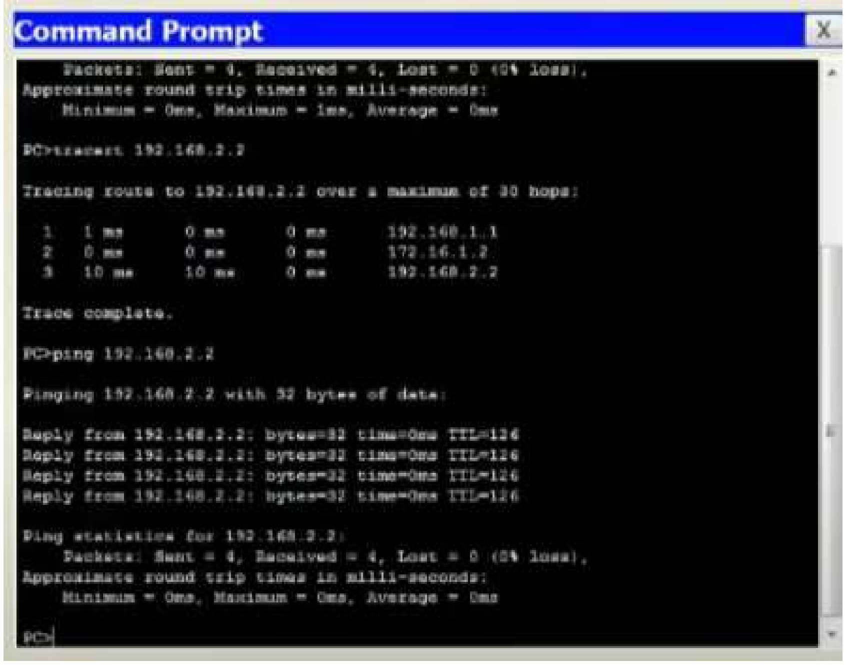
IMPLEMENTATION:



2 PC's, 3 Routers, 1 central and other 2 Local.

FINAL OUTPUT:

Hence the network is pinging successfully as shown in the below output.



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

PC>tracert 192.168.2.2

Tracing route to 192.168.2.2 over a maximum of 30 hops:

  1   1 ms      0 ms      0 ms      192.168.1.1
  2   0 ms      0 ms      0 ms      172.16.1.2
  3   10 ms     10 ms     0 ms      192.168.2.2

Trace complete.

PC>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.2.2: bytes=32 time=0ms TTL=126
Reply from 192.168.2.2: bytes=32 time=0ms TTL=126
Reply from 192.168.2.2: bytes=32 time=0ms TTL=126
Reply from 192.168.2.2: bytes=32 time=0ms TTL=126

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

PC>
```

CONCLUSION:

Hence, we created a Virtual Private Network using Cisco packet tracer.

x-x-x

Experiment 10 Over

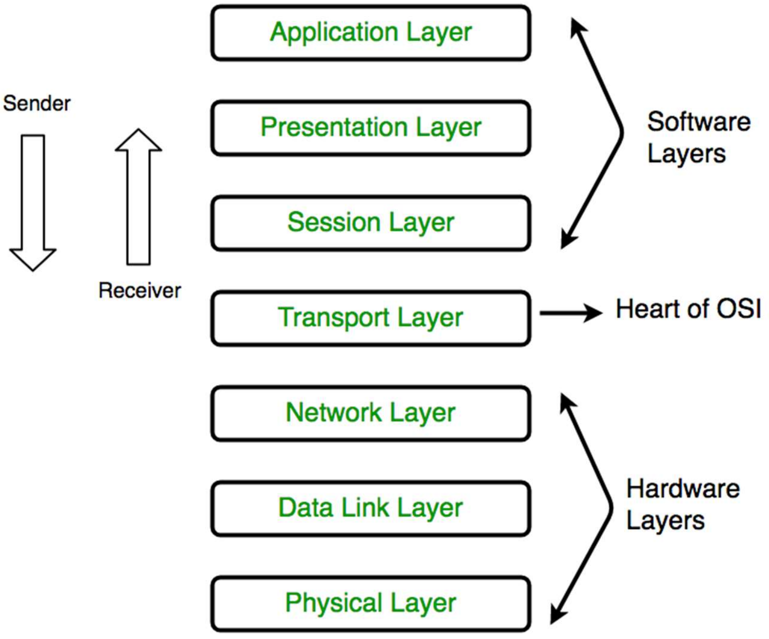
ASSIGNMENT – 01

Q.1) Explain OSI Models with all 7 layers?

The users of a computer are located over a wide physical range.i.e., all over the world. Therefore, to ensure that nationwide and worldwide data communication systems can be developed and are compatible to each other, an international group of standards has been developed. These standards fit into a framework which has been developed by the "International organization of standardization (ISO)".

The framework is called as "Model for open system interconnection (OSI)" and it is normally referred to as the "OSI Reference model".

It is a 7-layer architecture with each layer having specific functionality to perform. All these 7 layers work collaboratively to transmit the data from one person to another across the globe.



Level	Name of the Layer	Functions
1.	Physical Layer	• Make & Break Connections • Define voltages & Data rates • Convert data bits into electrical signal • Decide whether transmission is simplex, half duplex or full duplex
2.	Data Link Layer	• Synchronization • Error detection • Error Correction • To assemble outgoing messages into frames
3.	Network Layer	• Routing of the signals • Divide the outgoing message into packets • To act as network controller for routing data
4.	Transport Layer	• Decides whether transmission should be parallel or single path • Multiplexing • Splitting or segmenting the data • To break the data into smaller units for efficient handling
5.	Session Layer	• To manage and synchronize conversation between two systems • Controlling logging in and off • User identification

		• Billing and session management
6.	Presentation Layer	• Works as a translating layer
7.	Application layer	• Retransferring files of information • LOGIN • Password checking etc,

Q.2) Explain the duties of Data Link Layer?

Functions of the data link layer are synchronization and error control for the information which is to be transmitted over the physical link. The duties include to enable the error detection by adding error detection bits to the data which is transmitted. The encoded data is then passes to the physical layer. Also, at this level the outgoing messages are assembled into frames and the system for the acknowledgements to be received after every frame is transmitted. Correct operation of the data link layer ensures reliable transmission of each message. Examples of data link layer protocol are HDLC, SDLC and X.25 protocols.

The functions of the data Link layer are:

- **Framing**: Framing is a function of the data link layer. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver. This can be accomplished by attaching special bit patterns to the beginning and end of the frame.

0101 0101 0010 1011 01010101010

- **Physical Addressing**: After creating frames, Data link layer adds physical addresses (MAC address) of sender and/or receiver in the header of each frame.

- **Error control:** Data link layer provides the mechanism of error control in which it detects and retransmits damaged or lost frames.

- **Flow control:** The data rate must be constant on both sides else the data may get corrupted thus, flow control coordinates that amount of data that can be sent before receiving acknowledgement.

- **Access control:** When a single communication channel is shared by multiple devices, MAC sub-layer of data link layer helps to determine which device has control over the channel at a given time.

x-x-x

Assignment 01 Over

(((((( ))))))

(You have reached the end of the C.N Lab Manual)