MGM's COLLEGE OF ENGINEERING AND TECHNOLOGY

Navi Mumbai-410209

DEPARTMENT OF COMPUTER ENGINEERING

Regulations: 2021 **Batch: 2024-25**

Year: TE **Semester: V**

CSL502 – COMPUTER NETWORKS

Prepared by
Prof.Dhanashri kane

LAB INCHARGE **HOD**

Prof. Dhanashri Kane **Dr. Rajesh Kadu**

INSTITUTE VISION & MISSION

VISION:

To become one of the outstanding Engineering Institute in India by providing a conductive and vibrant environment to achieve excellence in the field of Technology

MISSION:

To empower the aspiring professional students to be prudent enough to explore the world of technology and mound them to be proficient to reach the pinnacle of success in the competitive global economy.

COMPUTER ENGINEERING DEPARTMENT

VISION:

- To motivate and empower the students of computer engineering to become globally competent citizens with ethics to serve and lead the society
- To provide a stimulating educational environment for computer engineering graduates to face tomorrow's challenges and to inculcate social responsibility in them.

MISSION:

- To provide excellent academic environment by adopting an innovative teaching techniques
  through well-developed curriculum
- To foster a self-learning atmosphere for students to provide ethical solutions for societal
  Challenges
- To establish Center of Excellence in various domains of Computer Engineering and promote active research and development.
- To enhance the competency of the faculty in the latest technology through continuous development programs.
- To foster networking with alumni and industries.

PROGRAM EDUCATIONAL OBJECTIVES (PEO's)

PEO 1	To prepare the Learner with a sound foundation in the mathematical, scientific and engineering fundamentals.
PEO 2	To motivate the Learner in the art of self-learning and to use modern tools for solving real life problems.
PEO 3	To equip the Learner with broad education necessary to understand the impact of Computer Science and Engineering in a global and social context.
PEO 4	To encourage, motivate and prepare the Learner's for Lifelong learning.
PEO 5	To inculcate professional and ethical attitude, good leadership qualities and commitment to social responsibilities in the Learner's thought process.

PROGRAM OUTCOMES (POs)

Program Outcome Code	**Program Outcome Description**
PO1	**Basic Engineering knowledge:** An ability to apply the fundamental knowledge in mathematics, science and engineering to solve problems in Computer engineering.
PO2	**Problem Analysis:** Identify, formulate, research literature and analyze computer engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences and computer engineering and sciences
PO3	**Design/ Development of Solutions:** Design solutions for complex computer engineering problems and design system components or processes that meet specified needs with appropriate consideration for public health and safety, cultural, societal and environmental considerations.
PO4	**Conduct Investigations of Complex Engineering Problems**:- Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data and synthesis of information to provide valid conclusions.
PO5	**Modern Tool Usage:** Create, select and apply appropriate techniques, resources and modern computer engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations.

PO6	**The Engineer and Society:** Apply reasoning informed by contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to computer engineering practice.
PO7	**Environment and Sustainability**: Understand the impact of professional computer engineering solutions in societal and environmental contexts and demonstrate knowledge of and need for sustainable development.
PO8	**Ethics:** Apply ethical principles and commit to professional ethics and responsibilities and norms of computer engineering practice.
PO9	**Individual and Team Work:** Function effectively as an individual, and as a member or leader in diverse teams and in multidisciplinary settings.
PO10	**Communication:** Communicate effectively on complex engineering activities with the engineering community and with society at large, such as being able to comprehend and write effective reports and design documentation, make effective presentations and give and receive clear instructions.
PO11	**Project Management and Finance:** Demonstrate knowledge and understanding of computer engineering and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.
PO12	**Life-long Learning:** Recognize the need for and have the preparation and ability to engage in independent and lifelong learning in the broadest context of technological change.

PROGRAM SPECIFIC OUTCOMES (PSOs)

PSO1	Acquire skills to design, analyze and develop algorithms and implement them using high-level programming languages
PSO2	Contribute their engineering skills in computing and information engineering domains like network design and administration, database design and knowledge engineering.
PSO3	Develop strong skills in systematic planning, developing, testing implementing and providing IT solutions for different domains which helps in the betterment of life.

MGM's COLLEGE OF ENGINEERING AND TECHNOLOGY

NAVI MUMBAI – 410 209.

DEPARTMENT OF COMPUTER ENGINEERING

CSL502 – COMPUTER NETWORKS

LIST OF EXPERIMENTS

Suggested List of Experiments	
Sr. No.	**Title of Experiment**
1.	Study of RJ45 and CAT6 Cabling and connection using crimping tool.
2.	Use basic networking commands in Linux (ping, tracert, nslookup, netstat, ARP,RARP, ip, ifconfig, dig, route)
3.	Build a simple network topology and configure it for static routing protocol usingpacket tracer. Setup a network and configure IP addressing, subnetting, masking.
4.	Perform network discovery using discovery tools (eg. Nmap, mrtg)
5.	Use Wire shark to understand the operation of TCP/IP layers: ● Ethernet Layer: Frame header, Frame size etc. ● Data Link Layer: MAC address, ARP (IP and MAC address binding) ● Network Layer: IP Packet (header, fragmentation), ICMP (Query and Echo) ● Transport Layer: TCP Ports, TCP handshake segments etc. ● Application Layer: DHCP, FTP, HTTP header formats
6.	Use simulator (Eg. NS2) to understand functioning of ALOHA, CSMA/CD.
7.	Study and Installation of Network Simulator (NS3)
8.	A.Set up multiple IP addresses on a single LAN. B.Using nestat and route commands of Linux, do the following: ● View current routing table ● Add and delete routes ● Change default gateway C.Perform packet filtering by enabling IP forwarding using IPtables in Linux.
9.	Design VPN and Configure RIP/OSPF using Packet tracer.
10.	Socket programming using TCP or UDP
11.	Perform File Transfer and Access using FTP
12.	Perform Remote login using Telnet server

Lab Objectives:	
1	To practically explore OSI layers and understand the usage of simulation tools.
2	To analyze, specify and design the topological and routing strategies for an IPbased networking infrastructure.
3	To identify the various issues of a packet transfer from source to destination, and howthey are resolved by the various existing protocols
Lab Outcomes: On successful completion of lab, learner will be able to	
1	Design and setup networking environment in Linux.
2	Use Network tools and simulators such as NS2, Wireshark etc. to explore networking algorithms and protocols.
3	Implement programs using core programming APIs for understanding networking concepts.

Mapping of Course Outcomes (COs) to Program outcomes (POs)

PO / CO	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	M										M	
CO2	M	M										M
CO3			M						M			

Experiment No: 1

Aim: - Use of Crimping Tool for RJ45

Objective: -To understand how to attach a RJ45 to a cat5e network cable

Theory:- Crimping an RJ45 Connector Correctly Proper Wiring for Ethernet Cat5/Cat5e/Cat 6 Cables

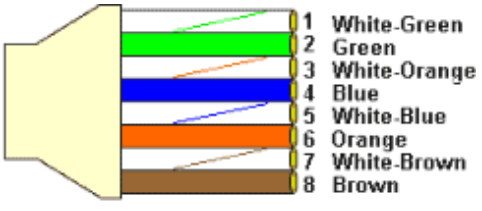
Cables can transmit information along their length. To actually get that information where it needs to go, you need to make the right connections to an RJ45 connector.

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

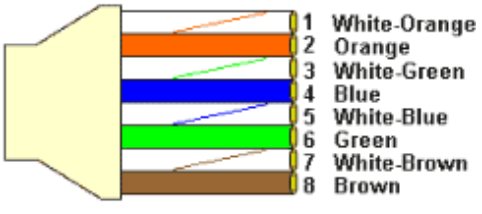
Registered Jack 45 (RJ45) is a standard type of physical connector for network cables. RJ45 connectors are commonly seen with Ethernet cables and networks.

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:



568A CABLE END



568B CABLE END

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 color codes is that the orange and green pairs are interchanged.

There is 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 endsof 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:

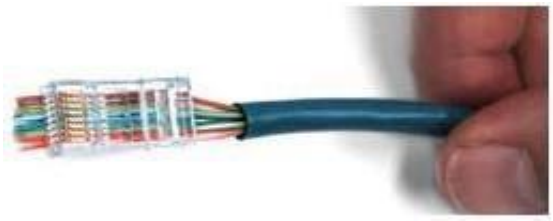
Holding the cable with the wire ends facing away from you. Moving from left to right, arrange the wires in a flat, side-by-side ribbon formation, placing them in the following order: white/orange, solid orange, white/green, solid blue, white/blue, solid green, white/brown, solid brown.

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

INDUSTRIAL APPLICATION:-

Network Connectivity can be done for any network (for office, company, organization)

REFERENCE:-

1)B.A. Forouzan, ―Data Communications and Networking .TMH (5e) 2)A.S.

2)Tanenbaum, ―Computer Networks‖, Pearson Education, (4e)

3) https://www.wikihow.com/Crimp-Rj45

VIVA QUESTIONS

1. Enlist colors used in LAN cables?

   ---

2. What is the difference between CAT5e and CAT6e?

   ---

3. State the uses of the network cable

   ---

4. Are the ends of the Rj45 cable waterproof.

5. Enlist different wired guided media.

6. Enlist types of Co-axial Cable.

7. Enlist types of Twisted Pair Cable.

8. Write application of Optical Fiber Cable.

9. Write on PPP networking?

---

10. Enlist types of Communication.

Experiment No:2

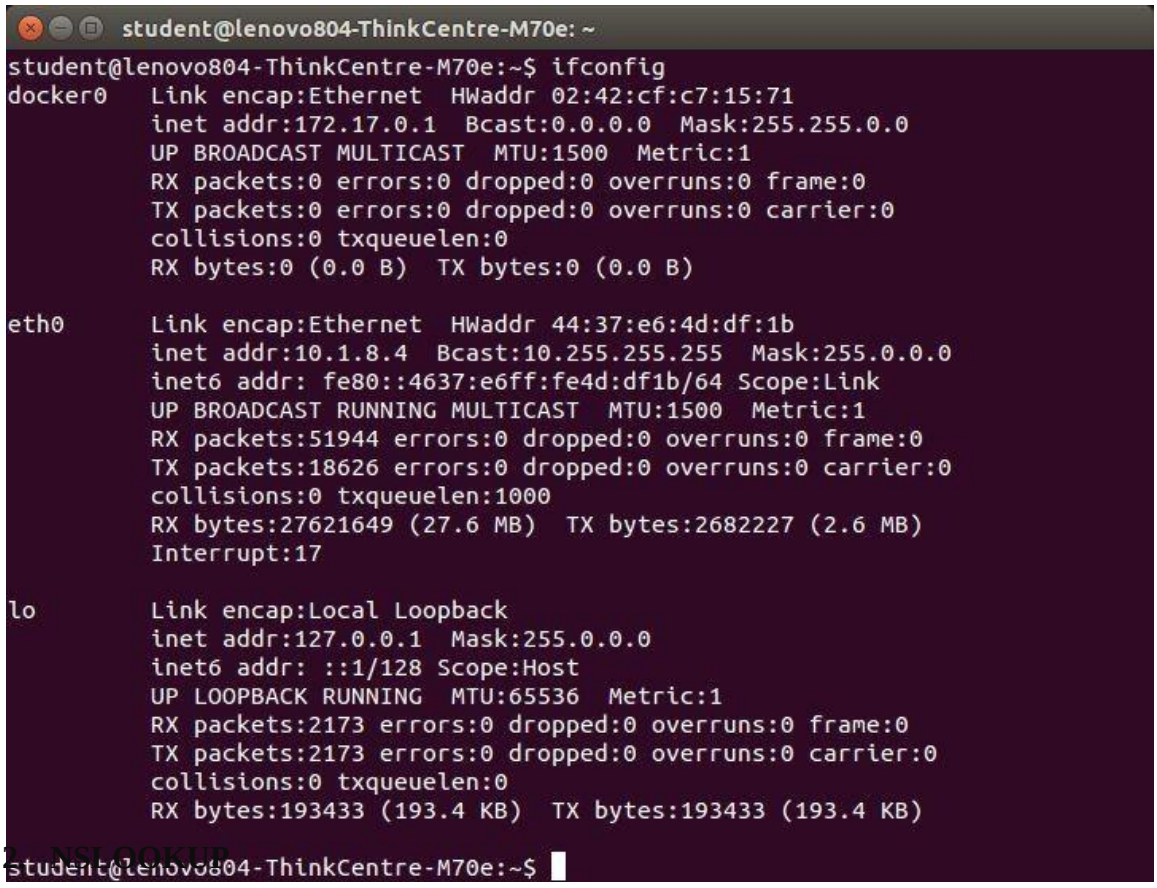
Aim: - Use basic networking commands in Linux (ping, tracert, nslookup, netstat, ARP, RARP, ip, ifconfig, dig, route)

Objective: - To learn the networking commands in Linux environment.

THEORY:

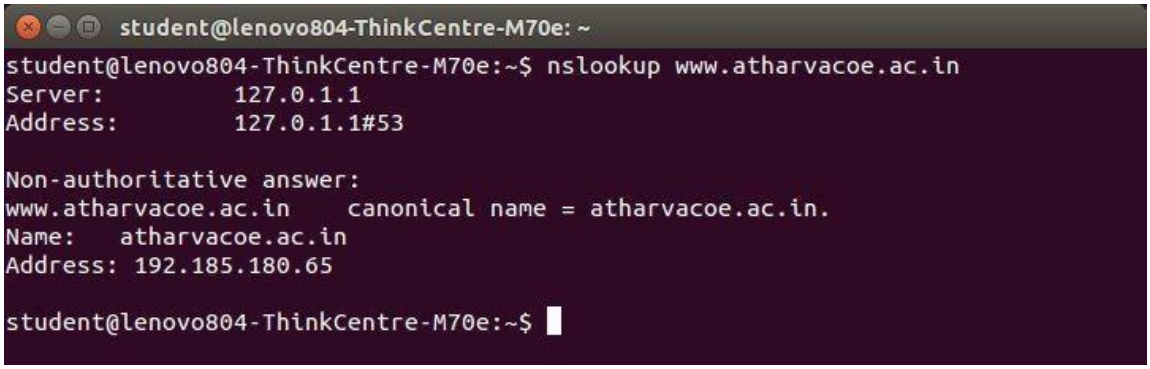
1. ifconfig

ifconfig(interface configuration) command is used to configure the kernel-resident network interfaces. It is used at the boot time to set up the interfaces as necessary. After that, it is usually used when needed during debugging or when you need system tuning. Also, this command is used to assign the IP address and netmask to an interface or to enable or disable a given interface.



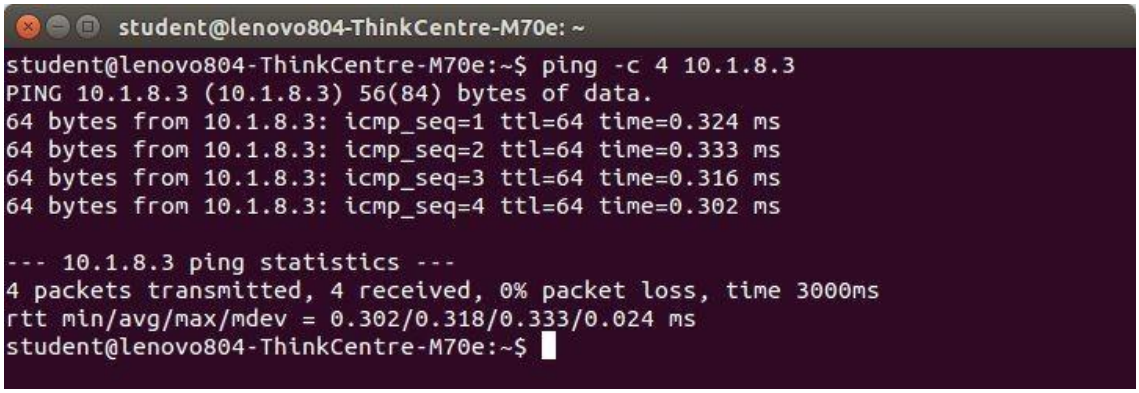
2. NSLOOKUP

Nslookup (stands for "Name Server Lookup") is a useful command for getting information from DNS server. It is a network administration tool for querying the Domain Name System (DNS) to obtain domain name or IP address mapping or any other specific DNS record. It is also used to troubleshoot DNS related problems.



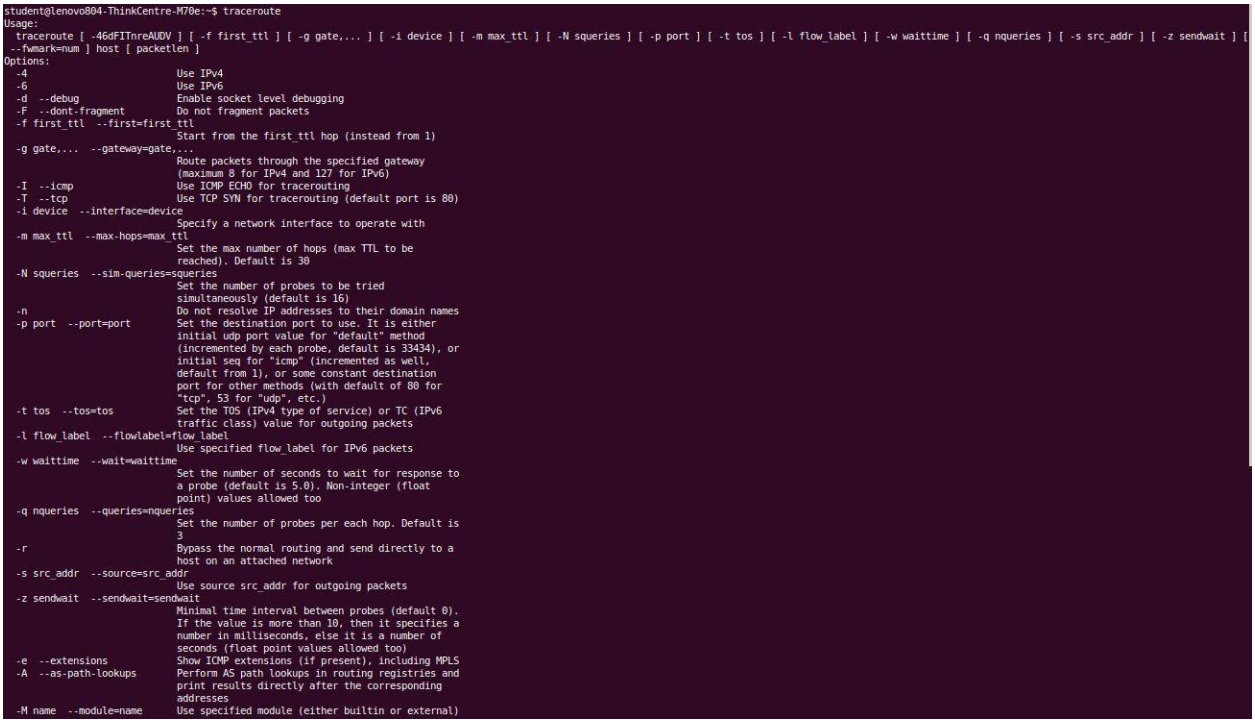
3. Ping

PING (Packet Internet Groper) command is used to check the network connectivity between host and server/host. This command takes as input the IP address or the URL and sends a data packet to the specified address with the message "PING" and get a response from the server/host this time is recorded which is called latency. Fast ping low latency means faster connection. Ping uses ICMP(Internet Control Message Protocol) to send an ICMP echo message to the specified host if that host is available then it sends ICMP reply message. Ping is generally measured in millisecond every modern operating system has this ping pre-installed.



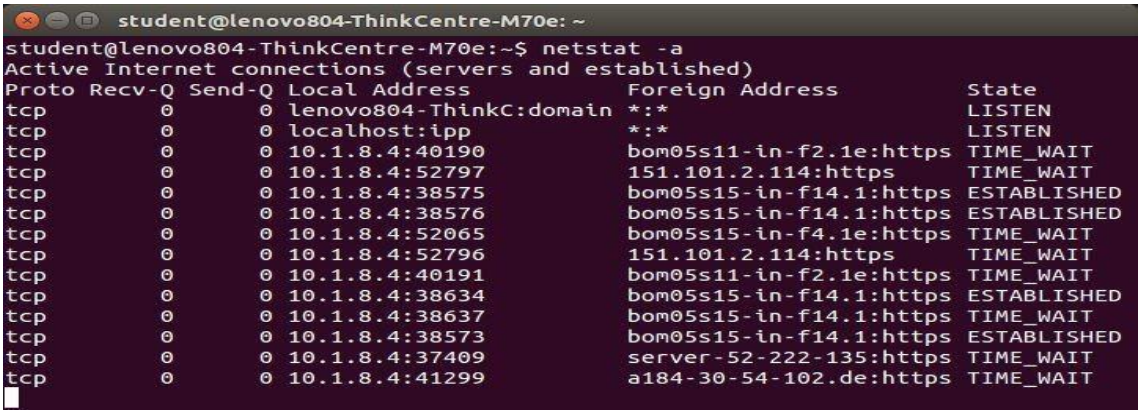
4. TRACEROUTE

traceroute command in Linux prints the route that a packet takes to reach the host. This command is useful when you want to know about the route and about all the hops that a packet takes. Below image depicts how traceroute command is used to reach the Google(172.217.26.206) host from the local machine and it also prints detail about all the hops that it visits in between.



5. Netstat

Netstat command displays various network related information such as network connections, routing tables, interface statistics, masquerade connections, multicast memberships etc.,



6. ARP

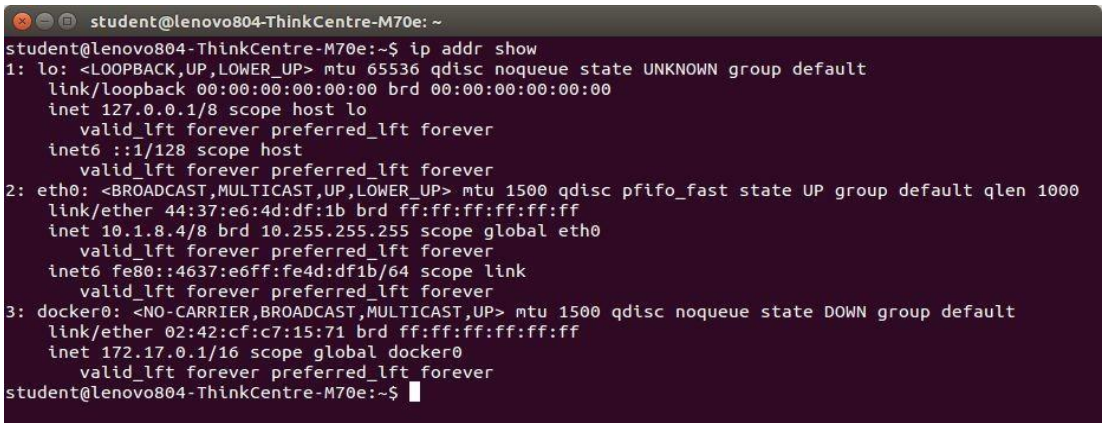
arp command manipulates the System's ARP cache. It also allows a complete dump of the ARP cache. ARP stands for Address Resolution Protocol. The primary function of this protocol is to resolve the IP address of a system to its mac address, and hence it works between level 2(Data link layer) and level 3(Network layer).

7. IP

ip command in Linux is present in the net-tools which is used for performing several network administration tasks. IP stands for Internet Protocol. This command is used to show or manipulate routing, devices, and tunnels. It is similar to *ifconfig* command but it is much more powerful with more functions and facilities attached to it. *ifconfig* is one of the deprecated commands in the net-tools of Linux that has not been maintained for many years. ip command is used to perform several tasks like assigning an address to a network interface or configuring network interface parameters.

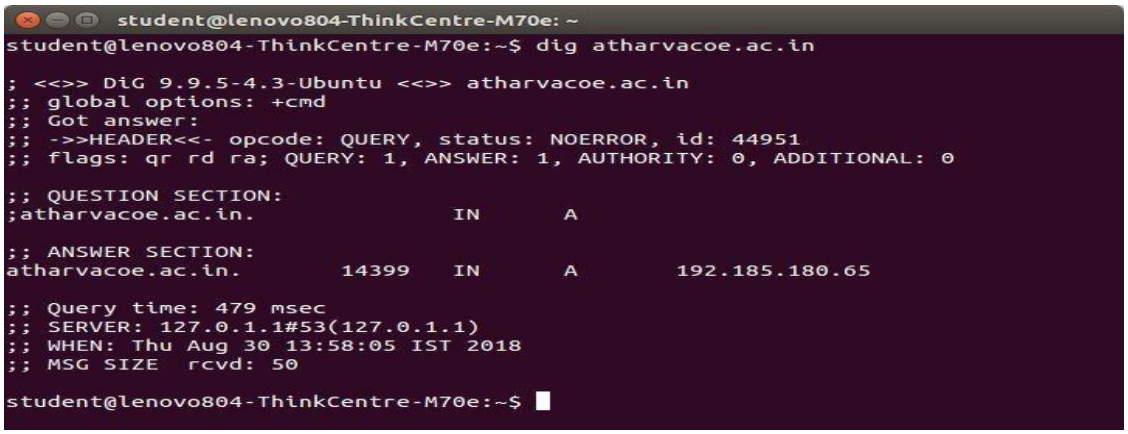
It can perform several other tasks like configuring and modifying the default and static routing, setting up tunnel over IP, listing IP addresses and property

information, modifying the status of the interface, assigning, deleting and setting up IP addresses and routes.



8. Dig

dig command stands for ***Domain Information Groper***. It is used for retrieving information about DNS name servers. It is basically used by network administrators. It is used for verifying and troubleshooting DNS problems and to perform DNS lookups. Dig command replaces older tools such as nslookup and the host.



CONCLUSION: Hence, in this experiment, we have successfully studied some important networking command and also implemented them in Linux

INDUSTRIAL APPLICATION:-

To use Linux networking in the industry

REFERENCE:-

1) B.A. Forouzan, ―Data Communications and Networking .TMH (5e)

2) A.S. Tanenbaum, ―Computer Networks‖, Pearson Education, (4e)

3) www.linuxandubuntu.com/home/10-essential-linux-network-commands

4) https://www.networkworld.com/.../unix-top-networking-commands

5) https://itsfoss.com › Linux › Basic Linux Networking Commands You Should Know

VIVA QUESTIONS

1. Explain hidden shares. How do they work?

---

2. State the seven layers in Open System Interconnection model.

---

3. What is the difference between ARP and RARP?

---

4. Illustrate Client/Server Model?

---

5. Explain MAC address?

---

6. Describe perquisites to configure server?

---

7. State how we will configure ADS?

---

8. How will you test LAN card?

Experiment No.3

AIM: Build a simple network topology and configure it for static routing protocol using packet tracer. Setup a network and configure IP addressing, subnetting, masking.

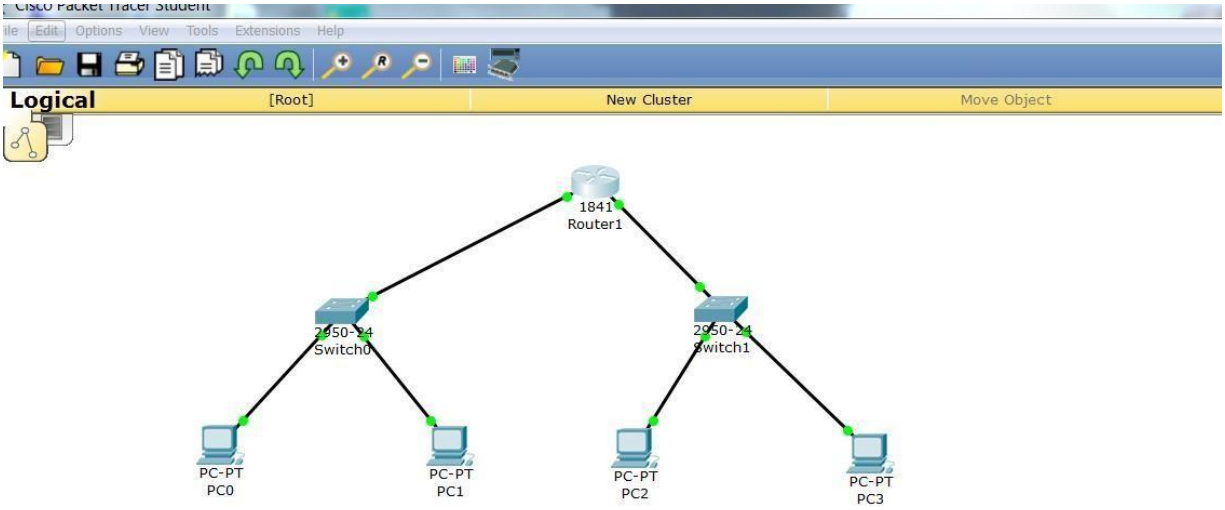
THEORY: Cisco Packet Tracer is a cross-platform visual simulation tool designed by Cisco Systems that allows users to create network topologies and imitate modern computer networks. The software allows users to simulate the configuration of Cisco routers and switches using a simulated command line interface. 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.

Steps:

1. Pick a total of 4 pcs in the packet tracer application. 2.We need 2 routers.

3.We need a single router.

Connect the devices as shown below:



4. Give the appropriate IP addresses to the pcs accordingly.
5. Test the network with the help of packets.

CONCLUSION: Hence we have successfully created simple network using CISCO PACKET TRACER.

INDUSTRIAL APPLICATION:-

To understand and implement the computer networking in the Industry.

REFERNCES:-

1. B.A Forouzan, ―Data Communications and Networking .TMH (5e) A.S. Tanenbaum, ―Computer Networks. ‖, Pearson Education, (4e) https://www.wikihow.com/Configure-a-Network-on-Cisco-Packet-Tracer
2. https://www.nsnam.org/docs/tutorial/html/building-topologies.html
3. www.conceptdraw.com/How-To-Guide/network-topology

VIVA QUESTIONS

1. Enlist some network tools to draw network topology diagram.

---

2. Illustrate LAN and WAN?

---

3. List features of Cisco's Packet Tracer.

---

4. State command is used to check connectivity between two machines in a network?

---

5. Explain adding of components in Cisco's Packet Tracer?

---

6. Define configuration IP address in Cisco's Packet Tracer?

7. Describe Subnet Mask?

8. Generate Hybrid Topology?

9. Write on PPP networking?

10. What is NIC?

Experiment No: 4

Aim: - Perform network discovery using discovery tools (eg. Nmap, mrtg)

Objective: - To learn the Connection Oriented and Connectionless Services of Data Communication

THEORY:

Nmap (Network Mapper) is a security scanner originally written by Gordon Lyon (also known by his pseudonym Fyodor Vaskovich) used to discover hosts and services on a computer network, thus creating a "map" of the network. To accomplish its goal, Nmap sends specially crafted packets to the target host and then analyzes the responses. Unlike many simple port scanners that just send packets at some predefined constant rate, Nmap accounts for the network conditions (latency fluctuations, network congestion, the target interference with the scan) during the run. Also, owing to the large and active user community providing feedback and contributing to its features, Nmap has been able to extend its discovery capabilities beyond simply figuring out whether a host is up or down and which ports are open and closed; it can determine the operating system of the target, names and versions of the listening services, estimated uptime, type of device, and presence of a firewall.

Nmap features include:

- Host Discovery – Identifying hosts on a network. For example, listing the hosts which respond to pings or have a particular port open.
- Port Scanning – Enumerating the open ports on one or more target hosts.
- Version Detection – Interrogating listening network services listening on remote devices to determine the application name and version number.

- OS Detection – Remotely determining the operating system and some hardware characteristics of network devices.

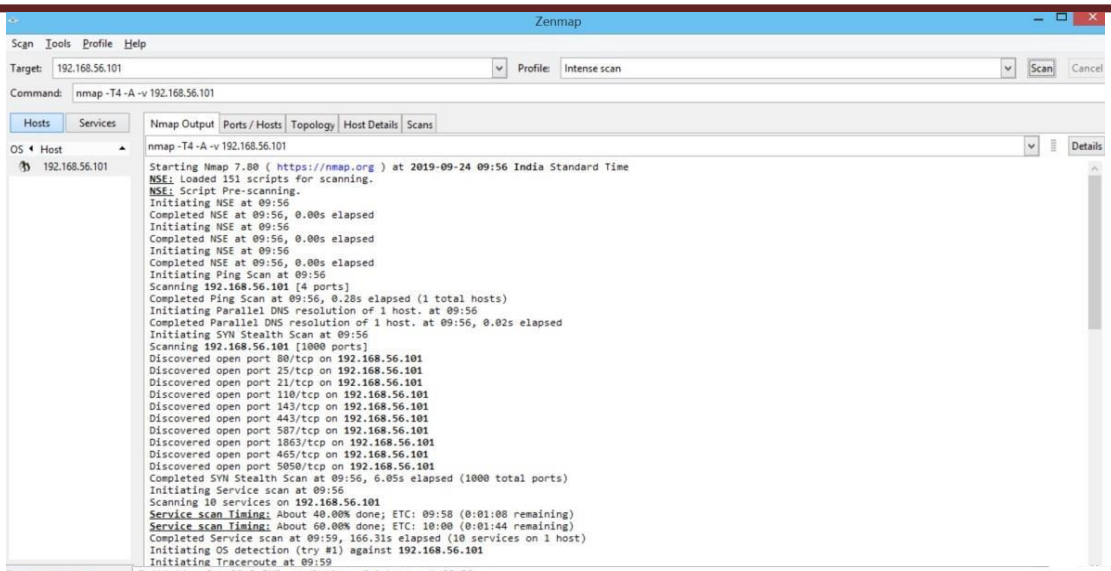
Basic commands working in Nmap:

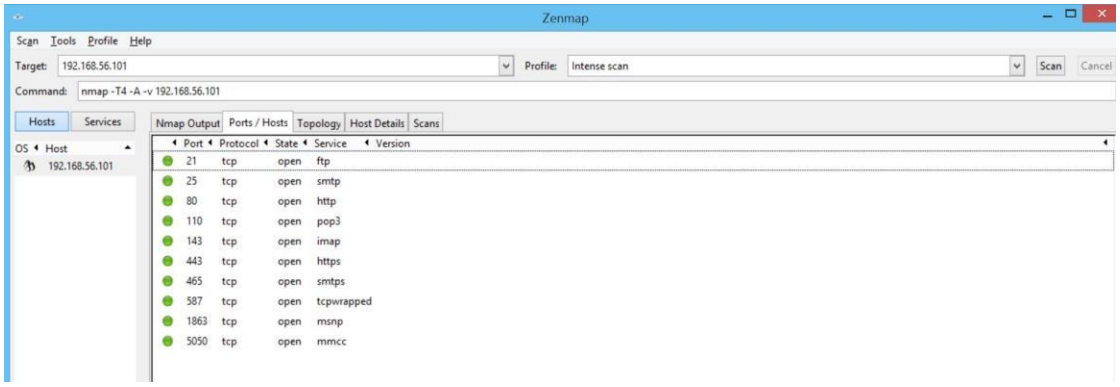
- For target specifications: nmap <target‘s URL or IP with spaces between them>
- For OS detection: nmap -O <target-host's URL or IP>
- For version detection: nmap -sV <target-host's URL or IP>

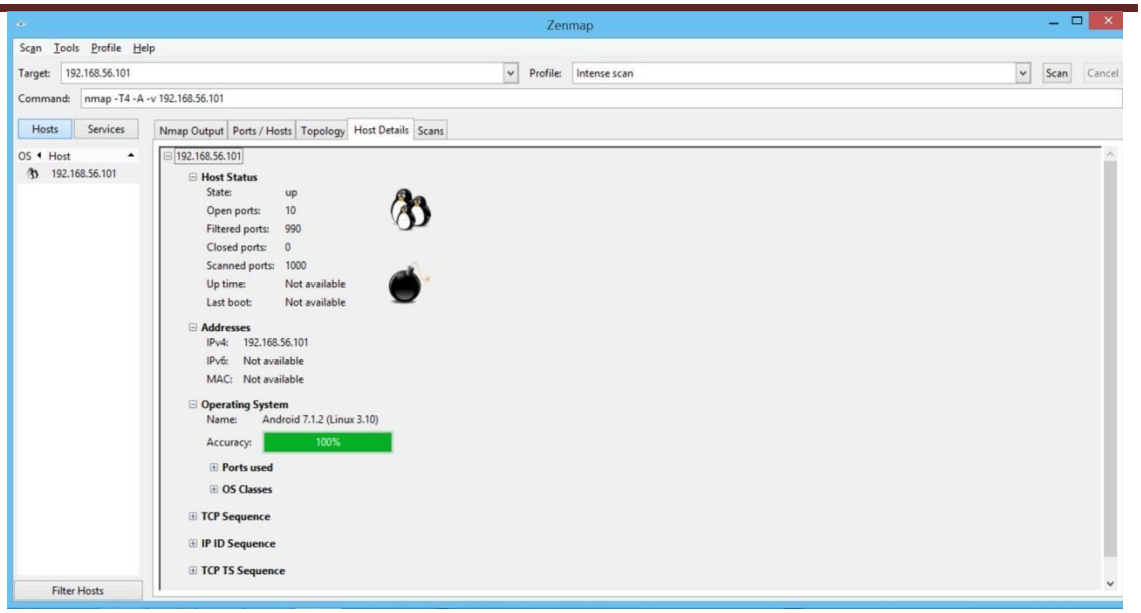
SYN scan is the default and most popular scan option for good reasons. It can be performed quickly, scanning thousands of ports per second on a fast network not hampered by restrictive firewalls. It is also relatively unobtrusive and stealthy since it never completes TCP connections

Algorithm\Implementation Steps\Installation Steps:

1. Download Nmap from www.nmap.org and install the Nmap Software with WinPcap Driver utility.
2. Execute the Nmap-Zenmap GUI tool from Program Menu or Desktop Icon
3. Type the Target Machine IP Address (ie.Guest OS or any website Address)
4. Perform the profiles shown in the utility.


Zenmap
Scan Tools Profile Help
Target: 192.168.56.101
Profile: Intense scan
Scan Cancel
Command: nmap -T4 -A -v 192.168.56.101
Hosts Services
OS Host
192.168.56.101
Nmap Output Ports / Hosts Topology Host Details Scans
nmap -T4 -A -v 192.168.56.101
Details
Starting Nmap 7.80 (https://nmap.org) at 2019-09-24 09:56 India Standard Time
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 09:56
Completed NSE at 09:56, 0.00s elapsed
Initiating NSE at 09:56
Completed NSE at 09:56, 0.00s elapsed
Initiating NSE at 09:56
Completed NSE at 09:56, 0.00s elapsed
Initiating Ping Scan at 09:56
Scanning 192.168.56.101 [4 ports]
Completed Ping Scan at 09:56, 0.28s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 09:56
Completed Parallel DNS resolution of 1 host. at 09:56, 0.02s elapsed
Initiating SYN Stealth Scan at 09:56
Scanning 192.168.56.101 [1000 ports]
Discovered open port 80/tcp on 192.168.56.101
Discovered open port 25/tcp on 192.168.56.101
Discovered open port 21/tcp on 192.168.56.101
Discovered open port 110/tcp on 192.168.56.101
Discovered open port 143/tcp on 192.168.56.101
Discovered open port 443/tcp on 192.168.56.101
Discovered open port 587/tcp on 192.168.56.101
Discovered open port 1863/tcp on 192.168.56.101
Discovered open port 465/tcp on 192.168.56.101
Discovered open port 5050/tcp on 192.168.56.101
Completed SYN Stealth Scan at 09:56, 6.05s elapsed (1000 total ports)
Initiating Service scan at 09:56
Scanning 10 services on 192.168.56.101
Service scan Timing: About 40.00% done; ETC: 09:58 (0:01:08 remaining)
Service scan Timing: About 60.00% done; ETC: 10:00 (0:01:44 remaining)
Completed Service scan at 09:59, 166.31s elapsed (10 services on 1 host)
Initiating OS detection (try #1) against 192.168.56.101
Initiating Traceroute at 09:59
192.168.56.101
Initiating Parallel DNS resolution of 1 host. at 09:59
Completed Parallel DNS resolution of 1 host. at 09:59, 0.00s elapsed
NSE: Script scanning 192.168.56.101.
Initiating NSE at 09:59
Completed NSE at 10:02, 169.07s elapsed
Initiating NSE at 10:02
Completed NSE at 10:04, 156.88s elapsed
Initiating NSE at 10:04
Completed NSE at 10:04, 0.00s elapsed
Nmap scan report for 192.168.56.101
Host is up (0.0016s latency).
Not shown: 990 filtered ports
PORT STATE SERVICE VERSION
21/tcp open ftp?
25/tcp open smtp?
|_smtp-commands: Couldn't establish connection on port 25
80/tcp open http?
110/tcp open pop3?
143/tcp open imap?
443/tcp open https?
465/tcp open smtps?
|_smtp-commands: Couldn't establish connection on port 465
587/tcp open tcpwrapped
|_smtp-commands: Couldn't establish connection on port 587
1863/tcp open msnp?
5050/tcp open mmcc?
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: phone|general purpose
Running: Google Android 7.X, Linux 3.X|2.6.X
OS CPE: cpe:/o:google:android:7.1.2 cpe:/o:linux:linux_kernel:3.10 cpe:/o:linux:linux_kernel:2.6
OS details: Android 7.1.2 (Linux 3.10), Linux 2.6.18 - 2.6.22
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=259 (Good luck!)
IP ID Sequence Generation: All zeros
Filter Hosts


Zenmap
Scan Tools Profile Help
Target: 192.168.56.101
Profile: Intense scan
Scan Cancel
Command: nmap -T4 -A -v 192.168.56.101
Hosts Services
OS Host
192.168.56.101
Nmap Output Ports / Hosts Topology Host Details Scans
Port Protocol State Service Version
21 tcp open ftp
25 tcp open smtp
80 tcp open http
110 tcp open pop3
143 tcp open imap
443 tcp open https
465 tcp open smtps
587 tcp open tcpwrapped
1863 tcp open msnp
5050 tcp open mmcc



CONCLUSION:- Thus, we have studied different options to scan ports in Nmap

INDUSTRIAL APPLICATION:-

For implementation of following services in networking,

1)Connection Oriented Data Communication

2)Connectionless Services of Data Communication

REFERNCES:-

1)https://www.it.uu.se/edu/course/homepage/distrinfo/ht09/presentations/Group2.ppt

2)www.csd.uoc.gr/~hy556/material/tutorials/cs556-3rd-tutorial.pdf

3)www2.ic.uff.br/~michael/kr1999/2-application/2_07-udpDev.html

4)B.A. Forouzan, ―Data Communications and Networking .TMH (5e)

5)A.S. Tanenbaum, ―Computer Networks‖, Pearson Education, (4e)

VIVA QUESTIONS

1. IllustratePeer to Peer network?

---

2. State how to find last address of a particular range.

---

3. How to find subnet mask if prefix is given?

---

4. Illustrate a socket?

5. Enlist stream classes related to socket.

6. The client in socket programming must know which two things?

7. Which of these class is used to create servers that listen for either local or remote client programs?

8. A port address in TCP/IP is.....bits long.

9. is a process-to-process protocol that adds only port addresses, checksum error control, and length information to the data from upper layer.

10. is responsible for converting the higher level protocol address (IP addresses) to physical network addresses.

Experiment No:5

Aim: - Use Wire shark to understand the operation of TCP/IP layers:

- Ethernet Layer: Frame header, Frame size etc.
- Data Link Layer: MAC address, ARP (IP and MAC address binding)
- Network Layer: IP Packet (header, fragmentation), ICMP (Query and Echo)
- Transport Layer: TCP Ports, TCP handshake segments etc.
- Application Layer: DHCP, FTP, HTTP header formats

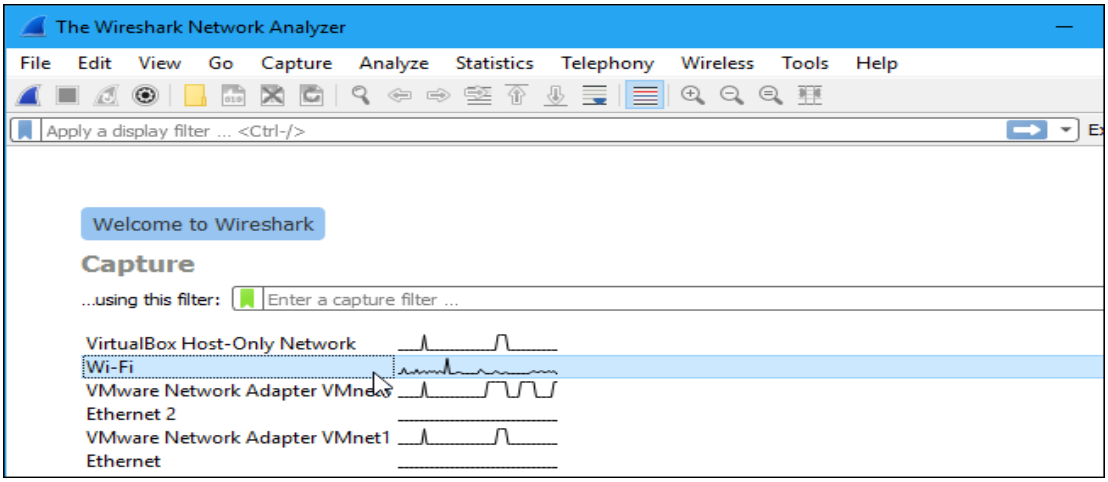
Objective: - To learn the communication between different host for transmission of data**.**

THEORY:

Wireshark, a network analysis tool formerly known as Ethereal, captures packets in real time and display them in human-readable format. Wireshark includes filters, color coding, and other features that let you dig deep into network traffic and inspect individual packets.

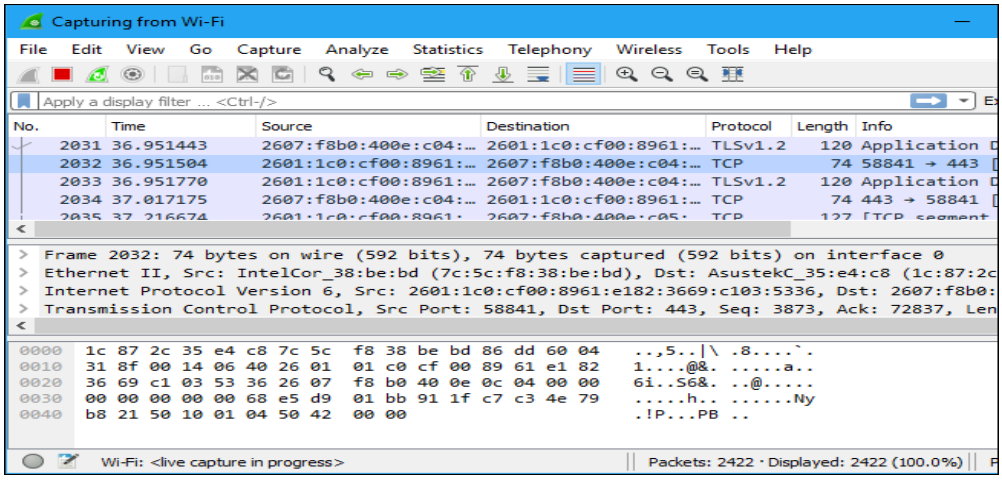
Capturing Packets

After downloading and installing Wireshark, you can launch it and double-click the name of a network interface under Capture to start capturing packets on that interface. For example, if you want to capture traffic on your wireless network, click your wireless interface. You can configure advanced features by clicking Capture > Options, but this isn't necessary for now.

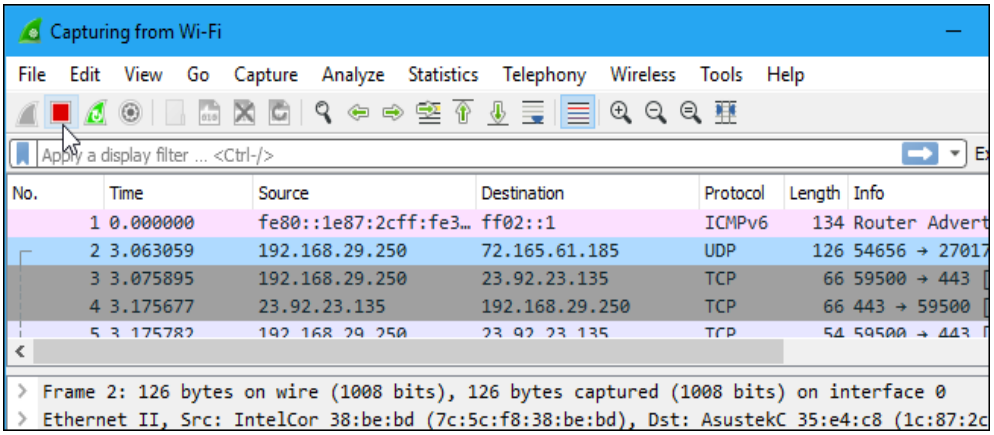


As soon as you click the interface's name, you'll see the packets start to appear in real time. Wireshark captures each packet sent to or from your system.

If you have promiscuous mode enabled—it's enabled by default—you'll also see all the other packets on the network instead of only packets addressed to your network adapter. To check if promiscuous mode is enabled, click Capture > Options and verify the "Enable promiscuous mode on all interfaces" checkbox is activated at the bottom of this window.



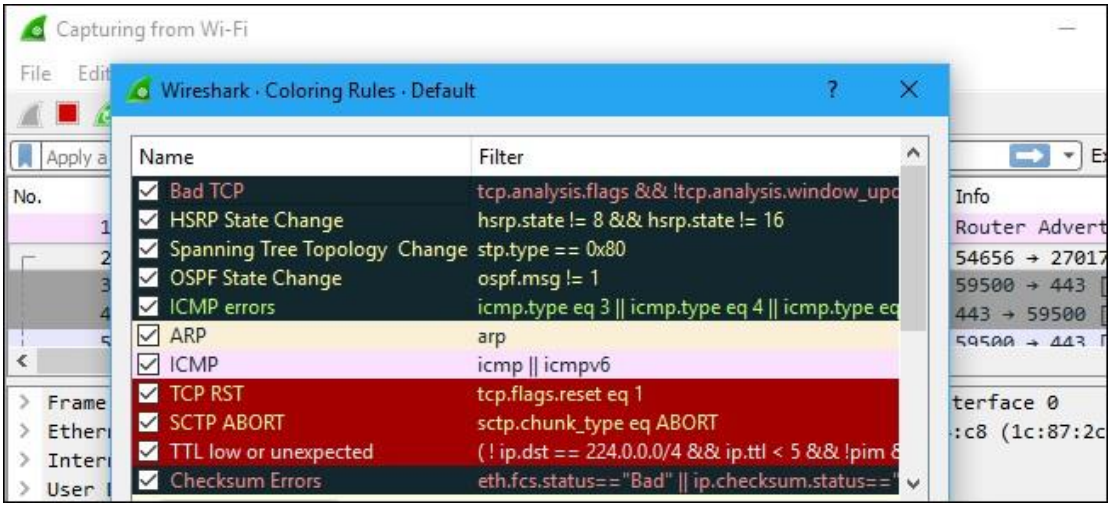
Click the red "Stop" button near the top left corner of the window when you want to stop capturing traffic.



Color Coding

You'll probably see packets highlighted in a variety of different colors. Wireshark uses colors to help you identify the types of traffic at a glance. By default, light purple is TCP traffic, light blue is UDP traffic, and black identifies packets with errors—for example, they could have been delivered out of order.

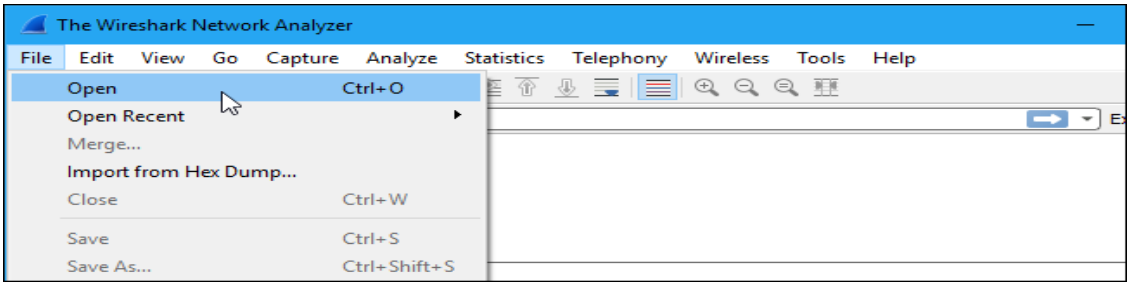
To view exactly what the color codes mean, click View > Coloring Rules. You can also customize and modify the coloring rules from here, if you like.



Sample Captures

If there's nothing interesting on your own network to inspect, Wireshark's wiki has you covered. The wiki contains a page of sample capture files that you can load and inspect. Click File > Open in Wireshark and browse for your downloaded file to open one.

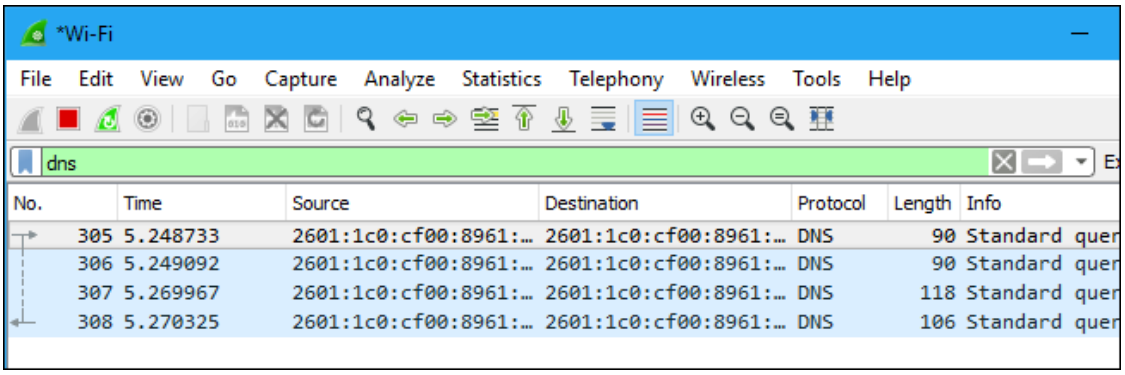
You can also save your own captures in Wireshark and open them later. Click File > Save to save your captured packets.



Filtering Packets

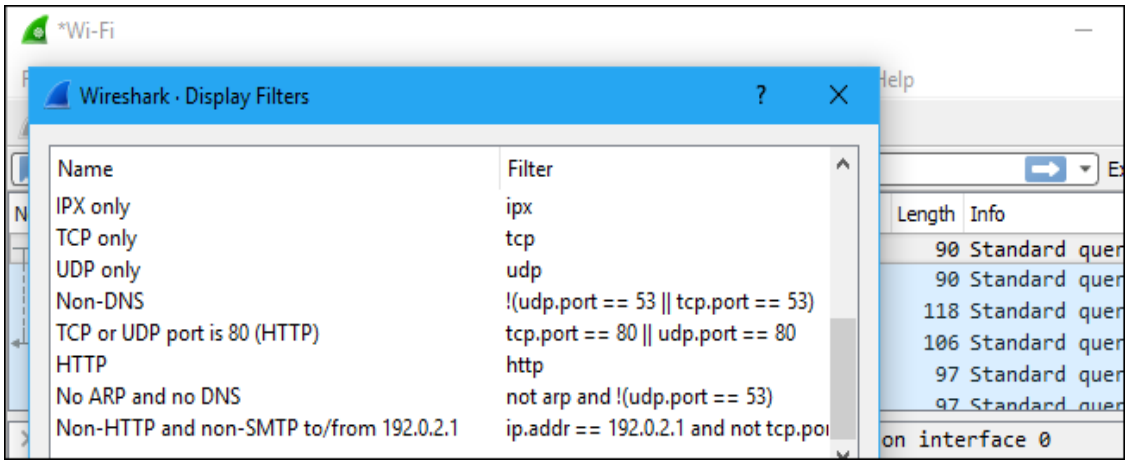
If you're trying to inspect something specific, such as the traffic a program sends when phoning home, it helps to close down all other applications using the network so you can narrow down the traffic. Still, you'll likely have a large amount of packets to sift through. That's where Wireshark's filters come in.

The most basic way to apply a filter is by typing it into the filter box at the top of the window and clicking Apply (or pressing Enter). For example, type "dns" and you'll see only DNS packets. When you start typing, Wireshark will help you autocomplete your filter.



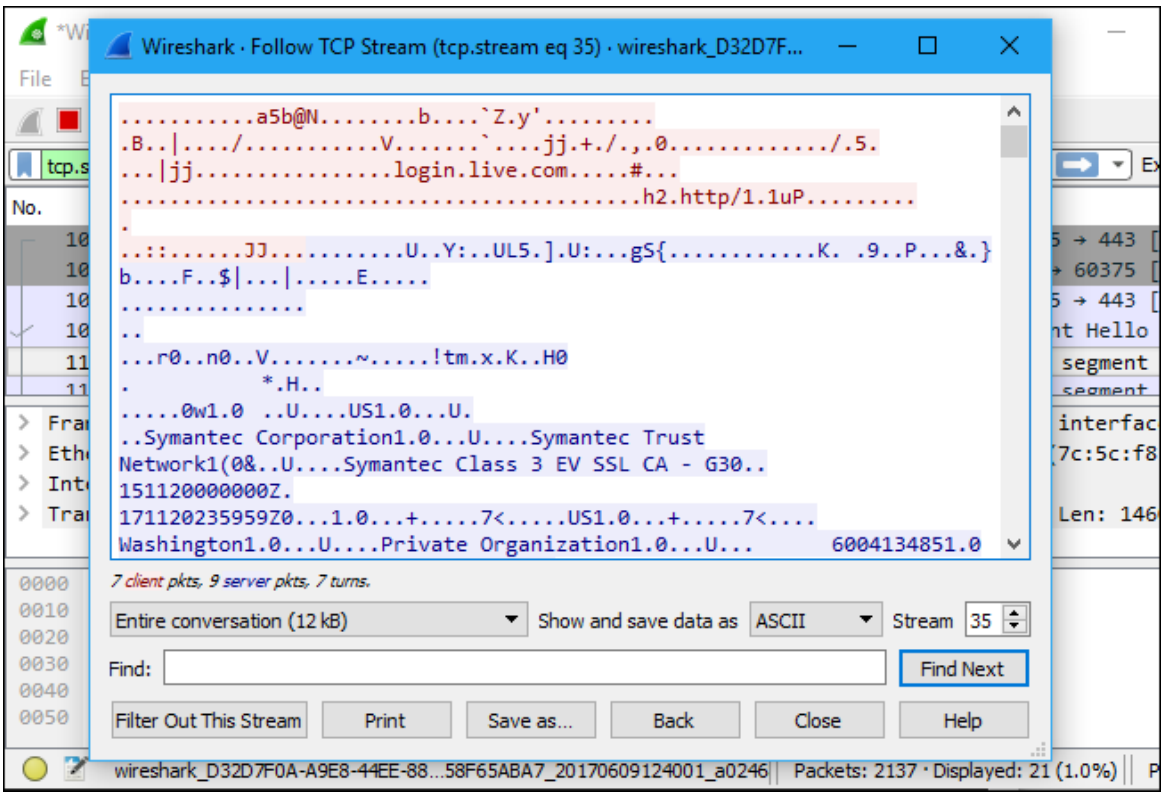
You can also click Analyze > Display Filters to choose a filter from among the default filters included in Wireshark. From here, you can add your own custom filters and save them to easily access them in the future.

For more information on Wireshark's display filtering language, read the Building display filter expressions page in the official Wireshark documentation.

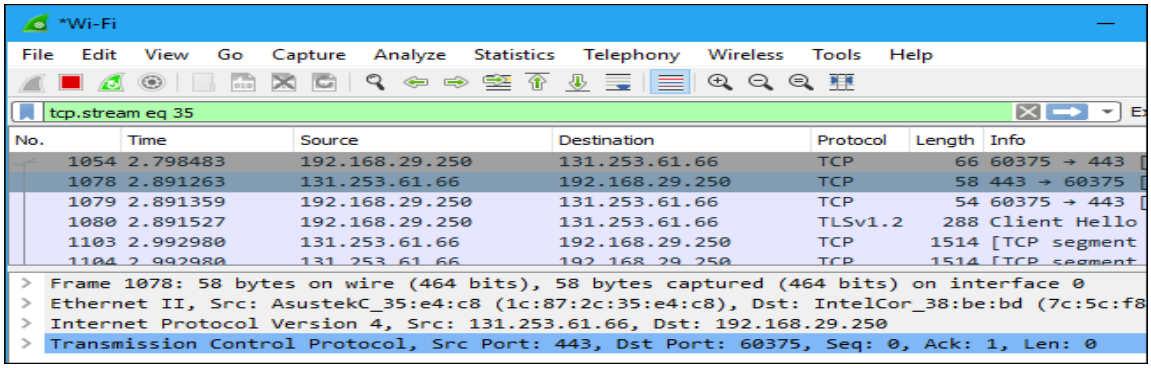


Another interesting thing you can do is right-click a packet and select Follow > TCP Stream.

You'll see the full TCP conversation between the client and the server. You can also click other protocols in the Follow menu to see the full conversations for other protocols, if applicable.

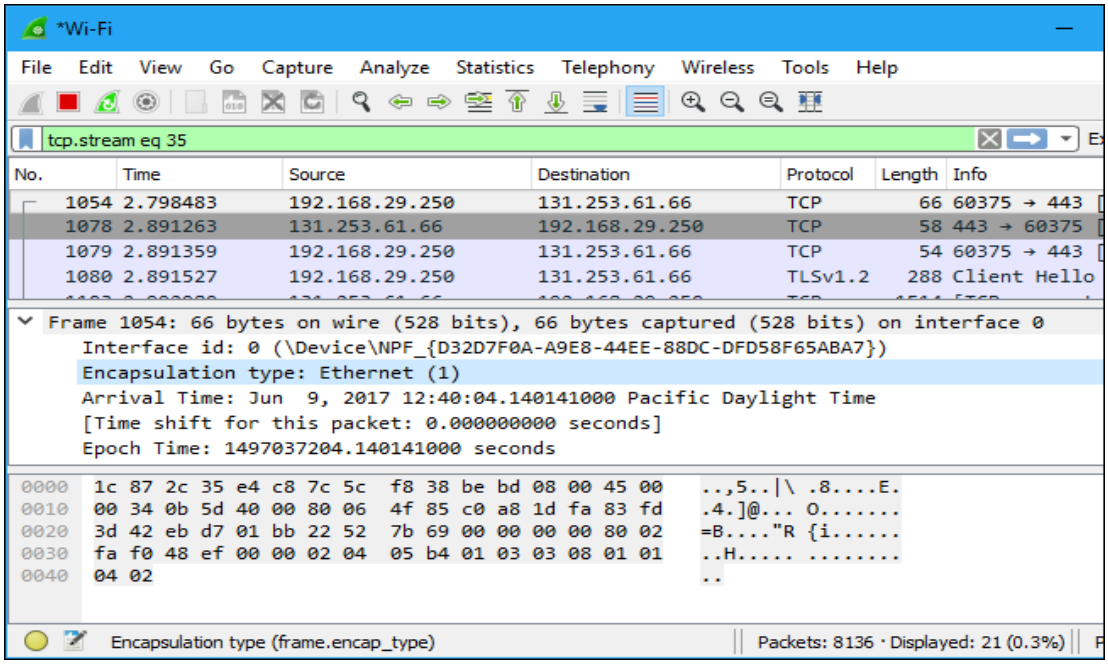


Close the window and you'll find a filter has been applied automatically. Wireshark is showing you the packets that make up the conversation.

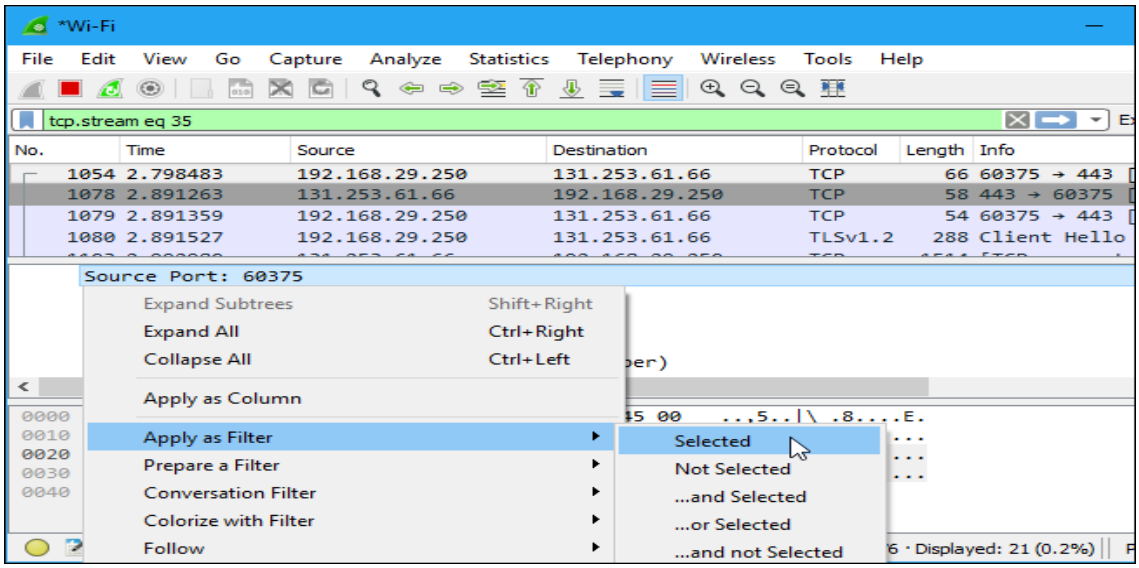


Inspecting Packets

Click a packet to select it and you can dig down to view its details.



You can also create filters from here — just right-click one of the details and use the Apply as Filter submenu to create a filter based on it.



Wireshark is an extremely powerful tool, and this tutorial is just scratching the surface of what you can do with it. Professionals use it to debug network protocol implementations, examine security problems and inspect network protocol internals.

RESULT:-

CONCLUSION:- Thus, we have studied the working of Wire Shark.

INDUSTRIAL APPLICATION:-Understand the Causes of congestion:

Insufficient memoryto hold these packets
Slow processors
Low bandwidth
Burstynature of traffic

REFERNCES:-

1)B.A. Forouzan, ―Data Communications and Networking .TMH (5e)

2)A.S. Tanenbaum, ―Computer Networks‖, Pearson Education, (4e)

3) nptel.ac.in/courses/106105080/pdf/M3L3.pdf

4) https://en.wikipedia.org/wiki/Sliding_window_protocol

5) www.ccs-labs.org/teaching/rn/animations/gbn_sr/

VIVA QUESTIONS

1. State the causes of congestion in network?

2. Enlist the effects of congestion on network?

3. List the types of ARQ protocols?

4. Explain the advantages of selective repeat ARQ?

5. Tell the location of sliding window protocols reside in OSI model?

6. Illustrate working of stop-n-wait protocol works?

7. State the disadvantages of stop-n-wait protocol?

8. How the Go-Back-N ARQ works?

9. List the advantages of selective repeat protocol?

10. State how to find subnet mask if prefix is given?

Experiment No:6

Aim: - Use simulator (Eg. NS2) to understand functioning of ALOHA, CSMA/CD.

Objective:- Use Network tools and simulators such as NS2, Wireshark etc. to explore networking algorithms and protocols.

THEORY:

I. Install Linux

II. Install NS2

III. Set Environmental variables

IV. Validation

V. Run the First nam

I. INSTALL LINUX (UBUNTU 8.10)

1. First of all, get the Linux OS image or CD. You can get it for free from Linux website

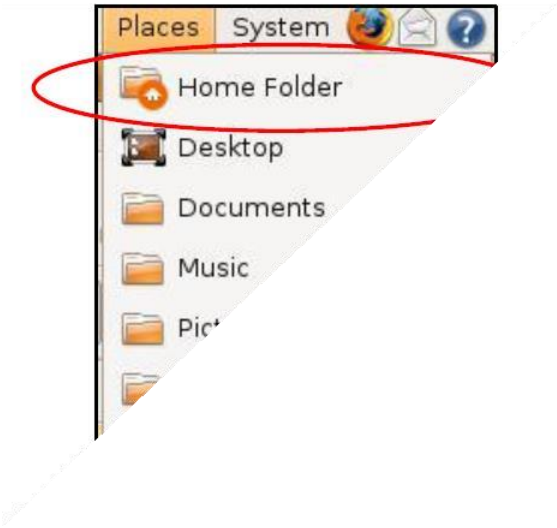
2. If you are a windows user, then you have to download Linux in a separate partition, or use a virtual machine. My advice to you is to use a virtual machine. One of the best virtual machine SW is Vmware. There are bunch of alternative Free SW to create Virtual machines, one of them is Virtual Box.

II. INSTALL NS2:-

1. Download the NS2 files from the Internet http://sourceforge.net/projects/nsnam/files/ns-2/2.34/

2. Extract the files

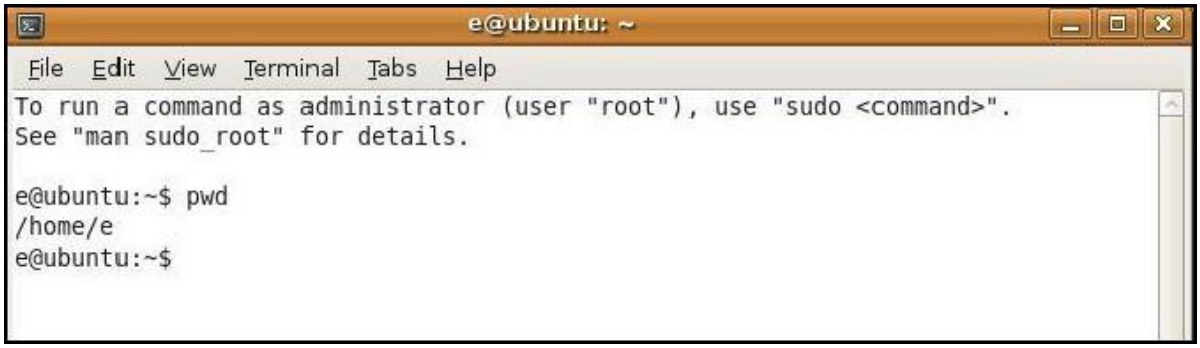
3. Put the files in the Home folder



4. Set the appropriate permissions for the ns-allinone-2.34 to allow executing the files inside it. To do that: Right click the folder -> Properties -> Permissions , and choose the appropriate group with the appropriate file access, then click "Allow executing file as program" and then click "Apply permissions to enclosed files"

5. From the Accessories -> Terminal

6. Type the following command to know in which directory you are: ~$ pwd

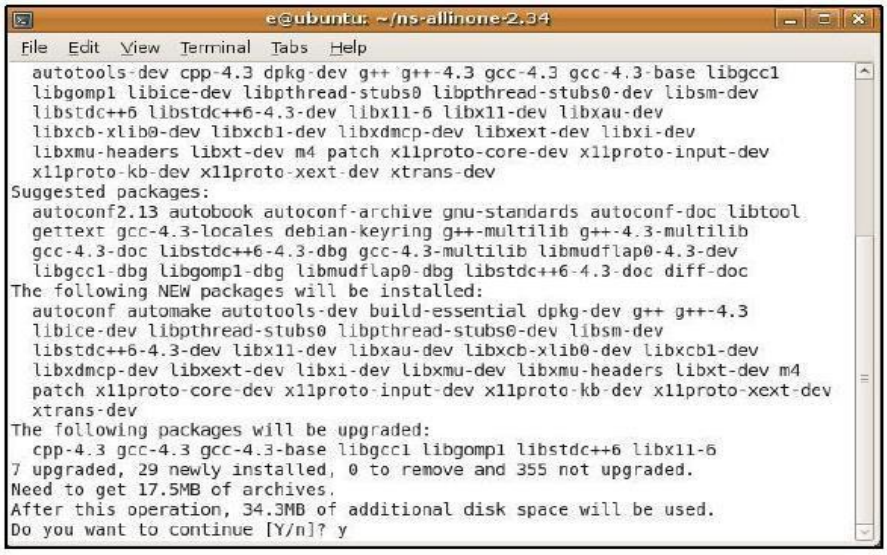


7. You need to be in the directory where you placed the ns-allinone-2.34 folder

8. If you are not in the /home/e , then move to it by using the command cd

9. Now, supposing you are in the directory /home/e (e can be any other user) type the following command to move inside the ns-allinone-2.34 using the command cd $ cd ns-allinone-2.34

10. Then, type the following command (you will be asked to enter the system password to process. Also, you will be asked if you want to continue, type: y to continue): $ sudo apt-get install build-essential autoconf automake libxmu-dev



11. Type the following command to install NS2 $ ./install

III. SET ENVIRONMENTAL VARIABLES

1. Write the following line: gedit ~/.bashrc

2. After the previous command, a file will open to you. Add the following lines to the end of the file. Replace "/your/path" by the folder where you placed the extracted ns-allinone-2.34 (For example, if your Linux user name is e, and you placed the ns-allinone-2.34 in the home directory, you have to change /your/path to /home/e)

#LD_LIBRARY_PATH

OTCL_LIB=/your/path/ns-allinone-2.34/otcl-1.13

NS2_LIB=/your/path/ns-allinone-2.34/lib

X11_LIB=/usr/X11R6/lib USR_LOCAL_LIB=/usr/local/lib export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:$OTCL_LIB:$NS2_LIB:$X11_LIB:$USR_LOCAL_LIB

TCL_LIBRARY TCL_LIB=/your/path/ns-allinone-2.34/tcl8.4.18/library USR_LIB=/usr/lib export TCL_LIBRARY=$TCL_LIB:$USR_LIB

#PATH

XGRAPH=/your/path/ns-allinone-2.34/bin:/your/path/ns-allinone2.34/tcl8.4.18/unix:/your/path/ns-allinone-2.34/tk8.4.18/unix NS=/your/path/ns-allinone-2.34/ns-2.34/

NAM=/your/path/ns-allinone-2.34/nam-1.14/ PATH=$PATH:$XGRAPH:$NS:$NAM

3. Save the file changes after your edit

4. Ensure that it immediately takes effect:

$ source ~/.bashrc

Note: the previous step is important; else you cannot successfully run ns-2.

5. Now, the installation has been completed. Try: $ ns 6. The "%" symbol appears on the screen. Type "exit" to quit.

IV.Validation

1. To run the ns validation suite: $ cd ns-2.34 $ ./validate

2. The validation will take long time, wait until it finish.

V.RUN YOUR FIRST NAM EXAMPLE

1. From the terminal type the following: $ cd ns-allinone-2.34 $ cd nam-1.14 $ cd edu $ exec nam A2-stop-n-wait-loss.nam

2. The following window appears, click the Play button to see the protocol animation

Input for Sample 1: Node 1 transmits data to Node

Node Properties	**NODE 1**
Transmission	Point-to-Point
Destination	Node-2
Traffic Type	Data
Application Data Size	
Distribution	Constant
Application Data Size (Bytes)	1472
Inter Arrival Time	
Distribution	Constant
Inter Arrival Time	20000

Simulation Time - 10 Seconds

(Note: The Simulation Time can be selected only after doing the following two tasks: Set the properties of Nodes and then click on the Simulate button).

Input for Sample 2: Node 1 transmits data to Node 2, Node 2 transmits data to Node 1.

Node Properties	NODE 1	NODE 2
Transmission	Point-to-Point	Point-to-Point
Destination	Node-2	Node-1
Traffic Type	Data	Data
Application Data Size		
Distribution	Constant	Constant
Application Data Size (Bytes)	1472	1472
Inter Arrival Time		
Distribution	Constant	Constant
Inter Arrival Time	20000	20000

Simulation Time - 10 Seconds

(Note: The Simulation Time can be selected only after doing the following two tasks: Set the properties of Nodes and Then click on the Simulate button).

Experiment 1: Node 1 transmits data to Node 2. Experiment 1: Node 1 transmits data to Node 2.

Experiment 2: Node 1 transmits data to Node 2, and Node 2 transmits data to Node 1.

Experiment 3: Node 1 transmits data to Node 2, and Node 2 transmits data to Node 3, and Node 3 transmits data to Node 1.

And so on do the experiment by increasing the number of nodes generating traffic as 4, 5, 7, 9, 10, 15, 20 22 and 24 nodes.

Simulation Time - 10 Seconds

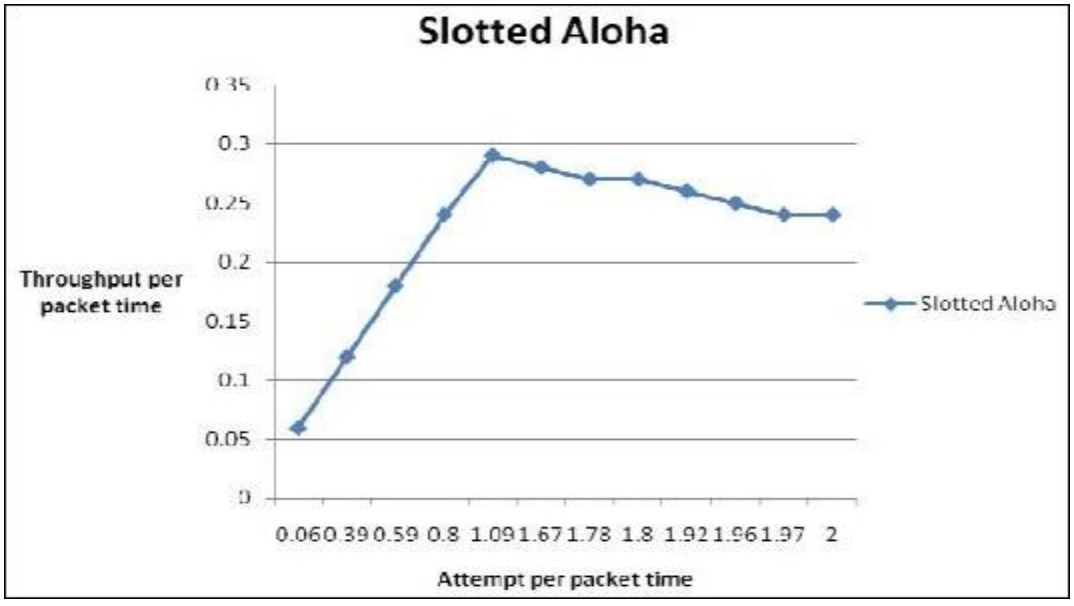
(Note: The Simulation Time can be selected only after doing the following two tasks: Set the properties of Nodes and then click on the Simulate button).

Comparison Table:

Number of nodes generating traffic	Throughput (mbps)	Total attempts	Throughput per packet time G	Attempts per packet time S
1	0.59	499	0.06	0.06
2	1.2	3308	0.12	0.39
3	1.8	4953	0.18	0.59
4	2.4	6691	0.24	0.80
5	2.9	9180	0.29	1.09
7	2.8	14012	0.28	1.67
9	2.7	14868	0.27	1.78
10	2.7	15078	0.27	1.80
15	2.6	16037	0.26	1.92
20	2.5	16437	0.25	1.96
22	2.4	16496	0.24	1.97
24	2.4	16755	0.24	2.00

RESULTS:-

We have obtained the following characteristic plot for the Slotted ALOHA, which matches the theoretical result.



CONCLUSION:- Thus, we have studied and successfully understand functioning of ALOHA

INDUSTRIAL APPLICATION:-

Use of following Network Simulator for Industry

1. Network Simulator 2
2. Ubuntu OS

REFERNCES:-

1) www.srmuniv.ac.in/sites/default/files/downloads/EC0421_network_simulation.pdf
2) https://www.cse.iitb.ac.in/~sri/cs348/cs378-lab04.pdf
3) https://www.coursera.org/lecture/peer-to.../random-access-csma-and-csma-cd-Vkb7f
4) https://www.ijser.org/researchpaper/Detail-Comparison-of-Network-Simulators.pdf
5) B.A. Forouzan, ―Data Communications and Networking .TMH (5e)
6) A.S. Tanenbaum, ―Computer Networks‖, Pearson Education, (4e)

VIVA QUESTIONS

1. What is NS2?

---

2. Illustrate environment variables?

---

3. State how we know whether NS is running or not?

---

4. Illustrate trace files?

---

5. Write the essential packages for NS2 insatallation?

---

6. What is the use of sudo command?

---

7. State how we know whether NS has successfully implemented protocols?

---

8. What is gedit?

---

9. Tell use of is nam?

---

10. What is wireshark?

Experiment No: 7

Aim: - a. Set up multiple IP addresses on a single LAN.

b. Using nestat and route commands of Linux, do the following:

- View current routing table
- Add and delete routes
- Change default gateway

Perform packet filtering by enabling IP forwarding using IP tables in Linux.

Objective: - To learn how to Set up multiple IP addresses on a single LAN

THEORY:

First, let us find the IP address of the network card. In my Ubuntu 15.10 server, I use only one network card.

Run the following command to find out the IP address:

```
sudo ip addr
```

Sample output:

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default

 link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00

 inet 127.0.0.1/8 scope host lo

 valid_lft forever preferred_lft forever

 inet6 ::1/128 scope host

 valid_lft forever preferred_lft forever

2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000

 link/ether 08:00:27:2a:03:4b brd ff:ff:ff:ff:ff:ff
```

inet **192.168.1.103/24** brd 192.168.1.255 scope global enp0s3

valid_lft forever preferred_lft forever

inet6 fe80::a00:27ff:fe2a:34e/64 scope link

valid_lft forever preferred_lft forever

Or

```
sudo ifconfig
```

Sample output:

enp0s3 Link encap:Ethernet HWaddr 08:00:27:2a:03:4b

inet addr:**192.168.1.103** Bcast:192.168.1.255 Mask:255.255.255.0

inet6 addr: fe80::a00:27ff:fe2a:34e/64 Scope:Link

UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1

RX packets:186 errors:0 dropped:0 overruns:0 frame:0

TX packets:70 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:1000

RX bytes:21872 (21.8 KB) TX bytes:9666 (9.6 KB)

lo Link encap:Local Loopback

inet addr:127.0.0.1 Mask:255.0.0.0

inet6 addr: ::1/128 Scope:Host

UP LOOPBACK RUNNING MTU:65536 Metric:1

```
RX packets:217 errors:0 dropped:0 overruns:0 frame:0

TX packets:217 errors:0 dropped:0 overruns:0 carrier:0

collisions:0 txqueuelen:0

RX bytes:38793 (38.7 KB) TX bytes:38793 (38.7 KB)
```

As you see in the above output, my network card name is **enp0s3**, and its IP address is **192.168.1.103**.

Now let us add an additional IP address, for example **192.168.1.104**, to the Interface card.

Open your Terminal and run the following command to add additional IP.

```
sudo ip addr add 192.168.1.104/24 dev enp0s3
```

Now, let us check if the IP is added using command:

```
sudo ip address show enp0s3
```

Sample output:

```
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000

link/ether 08:00:27:2a:03:4e brd ff:ff:ff:ff:ff:ff

inet 192.168.1.103/24 brd 192.168.1.255 scope global enp0s3

valid_lft forever preferred_lft forever

inet 192.168.1.104/24 scope global secondary enp0s3

valid_lft forever preferred_lft forever
```

```
inet6 fe80::a00:27ff:fe2a:34e/64 scope link

valid_lft forever preferred_lft forever
```

Similarly, you can add as many IP addresses as you want.

Let us ping the IP address to verify it.

```
sudo ping 192.168.1.104
```

Sample output:

```
PING 192.168.1.104 (192.168.1.104) 56(84) bytes of data.

64 bytes from 192.168.1.104: icmp_seq=1 ttl=64 time=0.901 ms

64 bytes from 192.168.1.104: icmp_seq=2 ttl=64 time=0.571 ms

64 bytes from 192.168.1.104: icmp_seq=3 ttl=64 time=0.521 ms

64 bytes from 192.168.1.104: icmp_seq=4 ttl=64 time=0.524 ms
```

To check the routing table

Command*:* *nestat -rn*

Adding route

```
sudo route add -net 192.168.3.0 gw 192.168.1.1 netmask 255.255.255.0 dev eth0
```

Deleting route

```
sudo route del -net 192.168.3.0 gw 192.168.1.1 netmask 255.255.255.0 dev eth0
```

A quick way to add default route

```
route add default gw 192.168.1.1
```

A quick way to delete defualt route

```
route del default gw 192.168.1.1
```

CONCLUSION: Thus, we have studied and successfully add the multiple IP address and also perform actions in Linux

INDUSTRIAL APPLICATION:-

Set up multiple IP addresses on a single LAN

REFERNCES:-

1. **https://ieeexplore.ieee.org/document/5445843/**
2. B.A. Forouzan, ―Data Communications and Networking .TMH (5e)
3. A.S. Tanenbaum, ―Computer Networks‖, Pearson Education, (4e)

VIVA QUESTIONS

1. When the host has to send a packet , packet is thrown in_____.

2. True of False i) Token Bucket has maximum capacity. -
3. State the type of traffic shaping algorithms.

---

4. Bursty traffic is converted into uniform traffic by
   1) Leaky Bucket. Or 2) Token Buket

5. FIFO concept is use in _____.

6. In practice bucket is a finite queue outputs at finite rate is concept of

Experiment No: 8

Aim: - Study and Installation of Network Simulator (NS3)

Objective: - To Learn the data communication using Network Simulator (NS3).

THEORY:

The *ns-3* simulator is a discrete-event network simulator targeted primarily for research and educational use. The **ns-3 project**, started in 2006, is an open-source project developing *ns-3*.

The purpose of this tutorial is to introduce new *ns-3* users to the system in a structured way. It is sometimes difficult for new users to glean essential information from detailed manuals and to convert this information into working simulations. In this tutorial, we will build several example simulations, introducing and explaining key concepts and features as we go.

As the tutorial unfolds, we will introduce the full *ns-3* documentation and provide pointers to source code for those interested in delving deeper into the workings of the system.

A few key points are worth noting at the onset:

- *ns-3* is open-source, and the project strives to maintain an open environment for researchers to contribute and share their software.
- *ns-3* is not a backwards-compatible extension of **ns-2**; it is a new simulator. The two simulators are both written in C++ but *ns-3* is a new simulator that does not support the *ns-2* APIs.

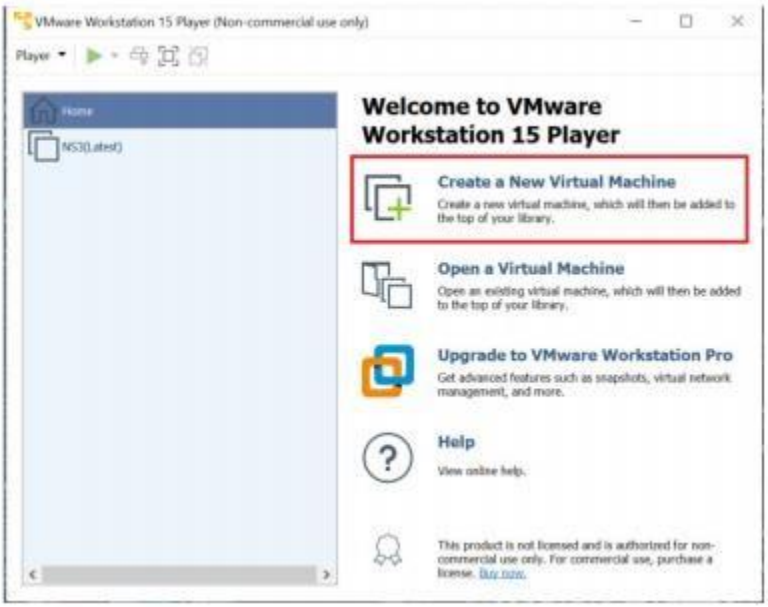
For the installation of NS3, VMware workstation is required to be installed, along with an Ubuntu system.

1. Download VMWare workstation from the website: https://my.vmware.com/en/web/vmware/downloads/info/slug/desktop_end_user_computing/vmware_workstation_player/15_0

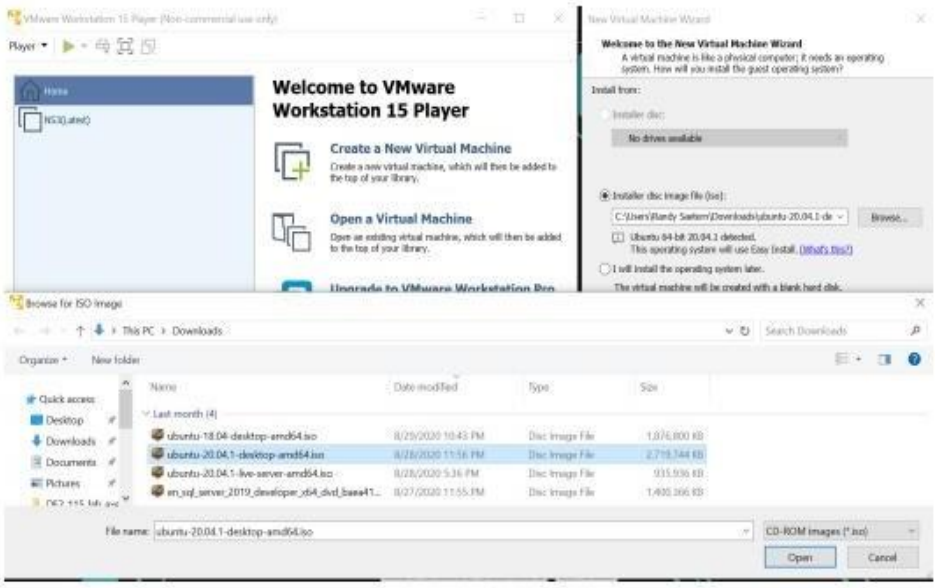
2. Download Ubuntu 20.04.01 Desktop AMD 64 from the website: https://ubuntu.com/download/desktop

3. Install VMWare workstation onto the computer system and open it

4. Set up the VMware workstation: a. Create a new virtual machine by selecting “Create New Virtual Machine.”



b. In the installer wizard, select installer disc image file(iso) and select the downloaded Ubuntu 20.04.01 AMD 64 iso file by browsing through the computer download files.



c. Name the machine and set the password.

d. Configure the Hardware:

i. For memory: set the value to 4600 MB or above.

ii. For faster VMware, set processors to 2.

5. Power on the virtual machine and let the machine update.

6. Within the Virtual machine, download NS3 on the VM by opening Mozilla firefox and downloading from the NS3 website.

7. Install prereq packages on Ubuntu using terminal:

a. Open the terminal by right clicking the desktop and select “open in terminal.”

b. Paste in this code and then press enter: sudo apt-get install g++ python3 python3-dev pkg-config sqlite3 python3- setuptools git qt5-default mercurial gir1.2-goocanvas-2.0 python-gi python-gi-cairo python3-gi python3-gi-cairo python3-pygraphviz gir1.2- gtk-3.0 ipython3 openmpi-bin openmpi-common openmpi-doc libopenmpi-dev autoconf cvs bzr unrar gdb valgrind uncrustify doxygen graphviz imagemagick texlive texlive-extra-utils texlive-latex-extra texlivefont-utils dvipng latexmk python3-sphinx dia gsl-bin libgsl-dev libgsl23 libgslcblas0 tcpdump sqlite sqlite3 libsqlite3-dev libxml2 libxml2-dev cmake libc6-dev libc6-dev-i386 libclang-6.0-dev llvm-6.0-dev automake python3-pip libgtk-3-dev synaptic vtun lxc uml-utilities

c. After the packages have finished downloading, paste in this code and press enter: sudo pip3 install cxxfilt

8. After installing the required packages, create a folder named workspace in the home directory and then put the NS3 tar package into the workspace. See example figure below.

9. Go to terminal and input these commands consecutively after each command finishes executing:

cd

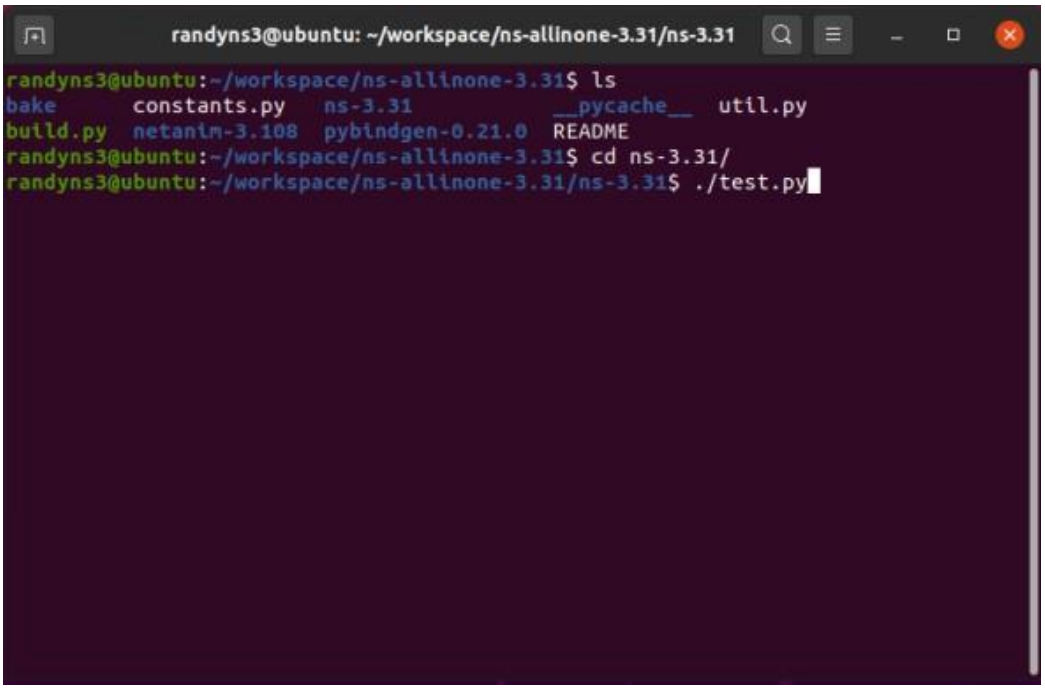
cd workspace

tar xjf <Name of Ns3 downloaded file name>

cd <Name of extracted Ns3>

./build.py --enable-examples --enable-tests

10. Test the NS3 build and installation success by running test.py in the ns directory using the following commands: cd ns- ./test.py



11. If all of the tests were passed, Congratulations! NS3 has now been installed successfully

CONCLUSION:- Thus, we have studied and successfully install NS3.

INDUSTRIAL APPLICATION:-

REFERNCES:-

1)B.A. Forouzan, ―Data Communications and Networking .TMH (5e)2)A.S.

VIVA QUESTIONS

1. What do u mean by FTP?

---

2. Define FTP Client?

---

3. What is FTP Server?

---

4. Explain the socket?

---

5. Enlist stream classes related to socket.

---

6. The client in socket programming must know which two things?

Experiment No: 9

Aim: - Design VPN and Configure RIP/OSPF using Packet tracer.

THEORY:

Routing Information Protocol (RIP) is a dynamic routing protocol which uses hop count as a routing metric to find the best path between the source and the destination network. It is a distance vector routing protocol which has AD value 120 and works on the application layer of OSI model. RIP uses port number 520.

Hop Count:

Hop count is the number of routers occurring in between the source and destination network. The path with the lowest hop count is considered as the best route to reach a network and therefore placed in the routing table. RIP prevents routing loops by limiting the number of hopes allowed in a path from source and destination. The maximum hop count allowed for RIP is 15 and hop count of 16 is considered as network unreachable.

Features of RIP:

1. Updates of the network are exchangedperiodically.
2. Updates (routing information) are always broadcast.
3. Full routing tables are sent in updates.
4. Routers always trust on routing information received from neighbour routers. This is also known as Routing on rumours.

Steps for implementing RIP:

Step1:

Select Router – select 1841 router and drag it to the screen (Router0).

Select another Router – select 1841 and drag it to right of the Router0 (Router1).

Select Switches – select 2950-24 and drag it below the Router0 (Switch0).

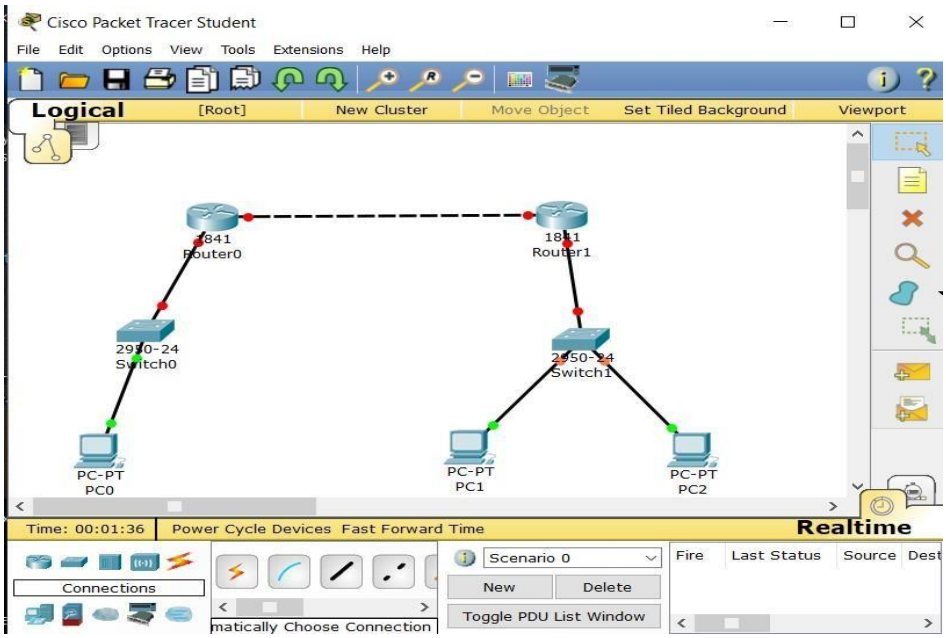
Select Switches – select 2950-24 and drag it below the Router1 (Switch1).

Select End Device – select Generic and drag it below Switch0 (PC-PT PC0).

Select End Device – select Generic and drag it below Switch1 (PC-PT PC1).

Select End Device – select Generic and drag it below Switch1 (PC-PT PC2).

Select Connections – Connect routers, switches and PCs to each other.

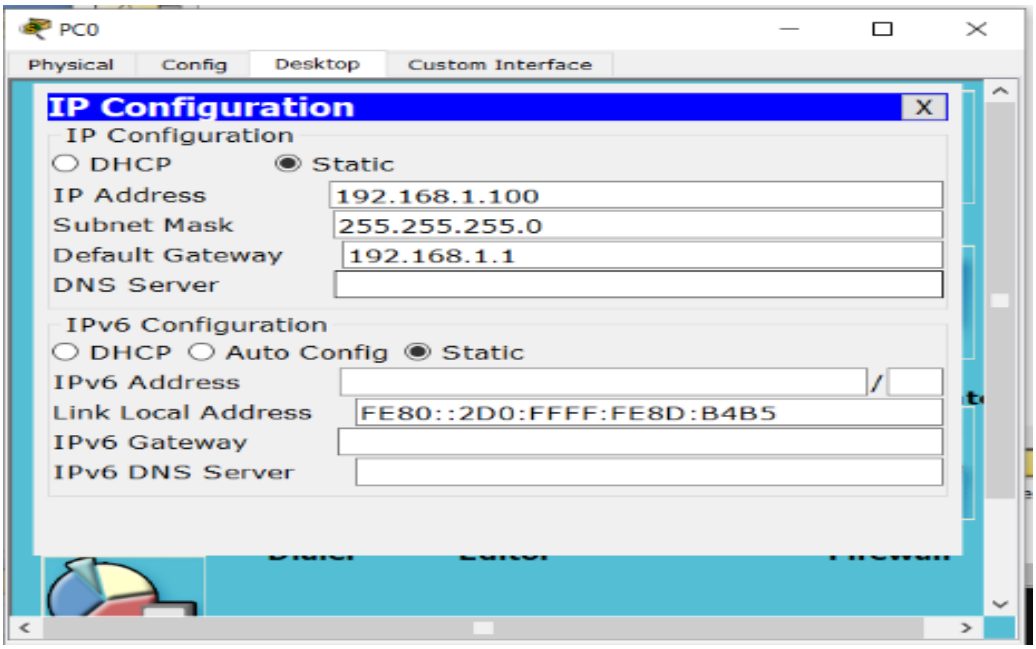


Step 2:

Click on PC0 and go to Desktop > IP Configuration

Add IP Address, as you will add the IP Address, Subnet Mask will be automatically added and displayed.

Add Default Gateway and close the window.

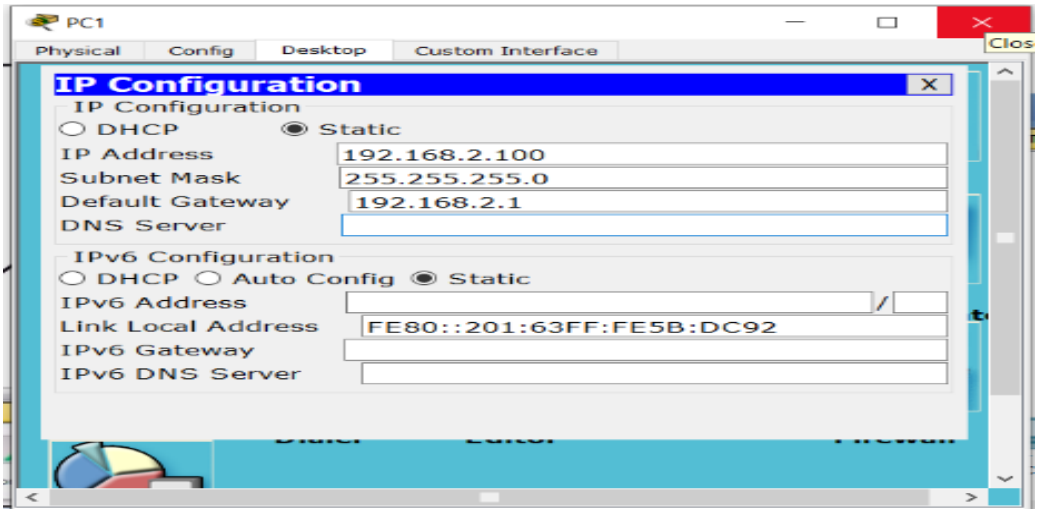


Step 3:

Click on PC1 and go to Desktop > IP Configuration

Add IP Address, as you will add the IP Address, Subnet Mask will be automatically added and displayed.

Add Default Gateway and close the window.

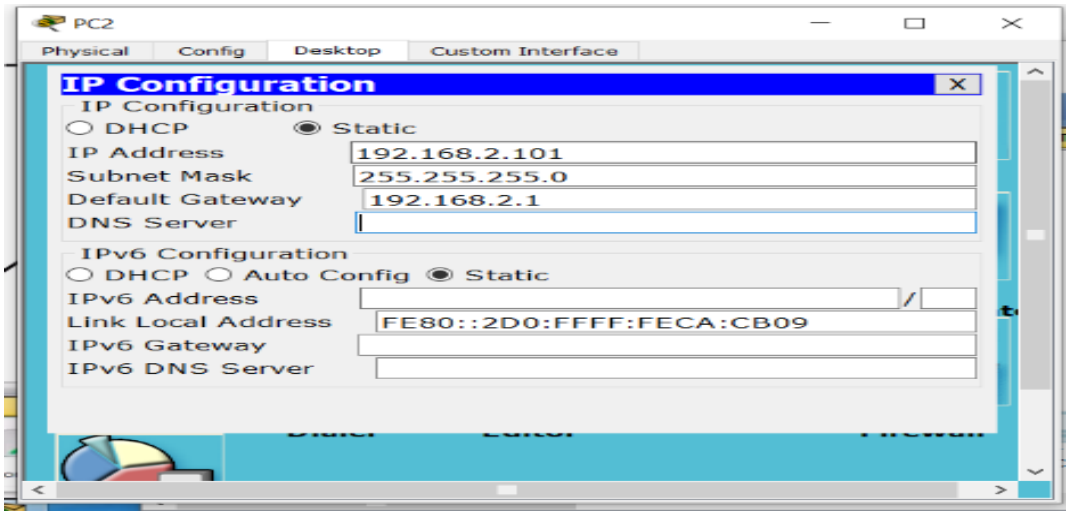


Step 4:

Click on PC2 and go to Desktop > IP Configuration

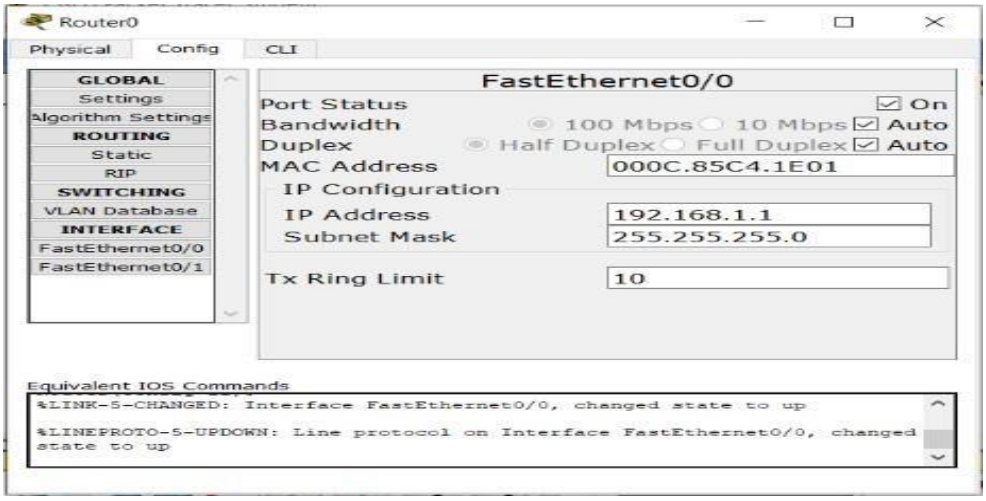
Add IP Address, as you will add the IP Address, Subnet Mask will be automatically added and displayed.

Add Default Gateway and close the window.



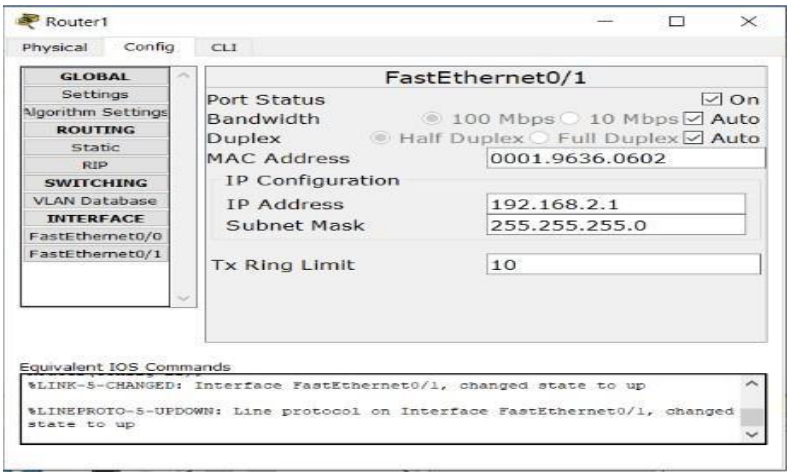
Step 5:

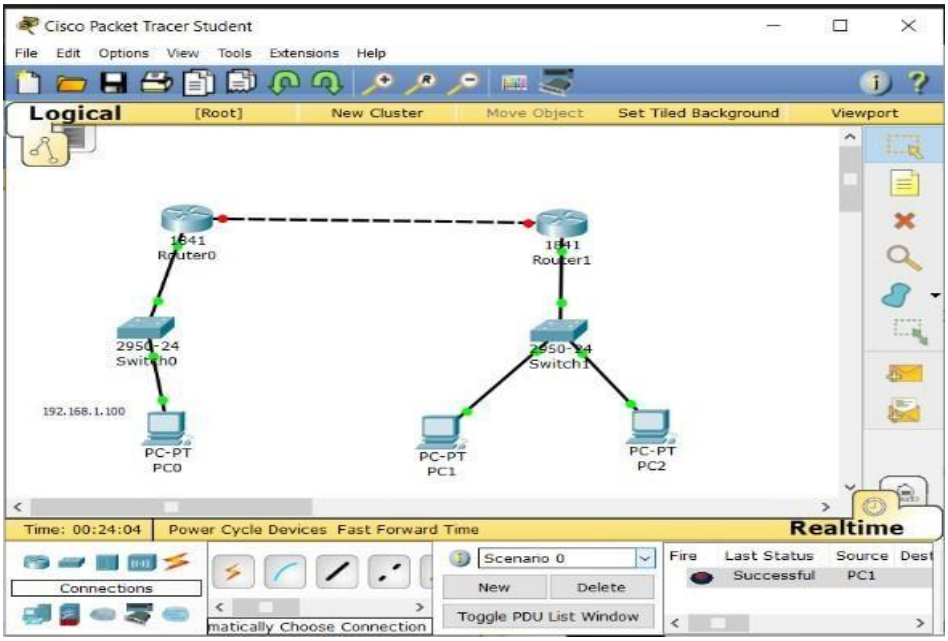
Click on Router0. Go to Config > FastEthernet0/0. Here, add IP Address and On the Port Status.



Step 6:

Click on Router1. Go to Config > FastEthernet0/1. Here, add IP Address and On the Port Status.

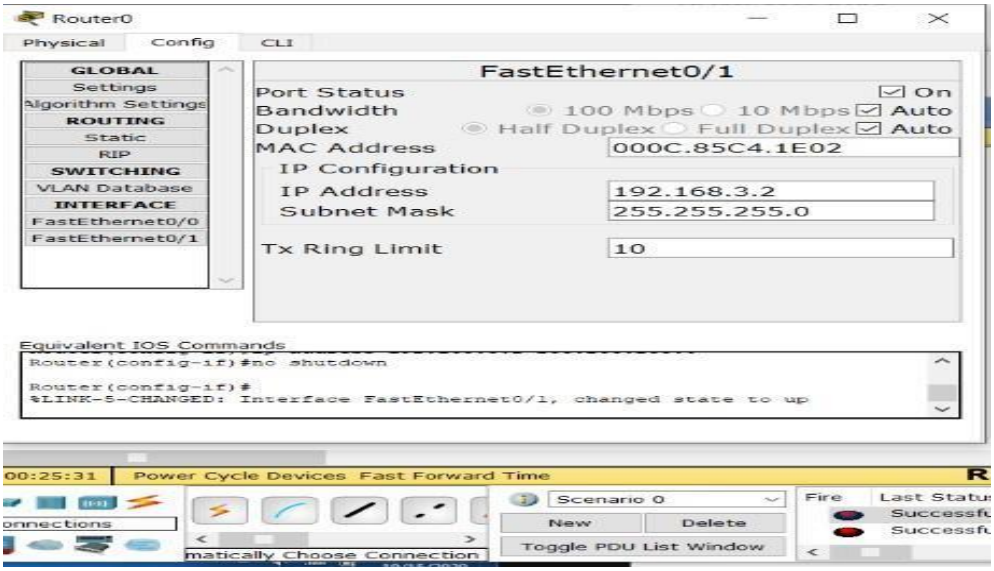




As you will see above, there is green dots which means connections are done successfully between Router, Switches and PCs.

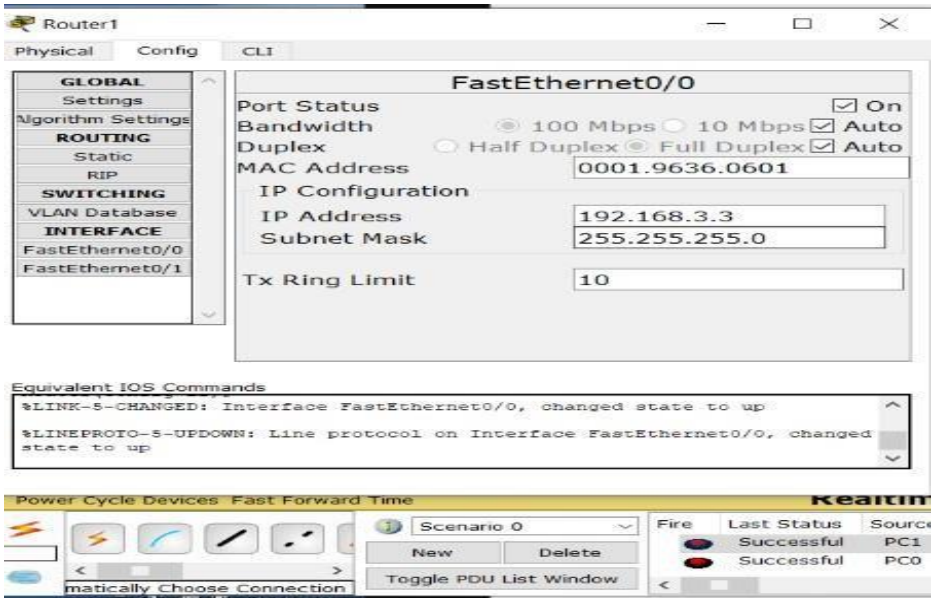
Step 7:

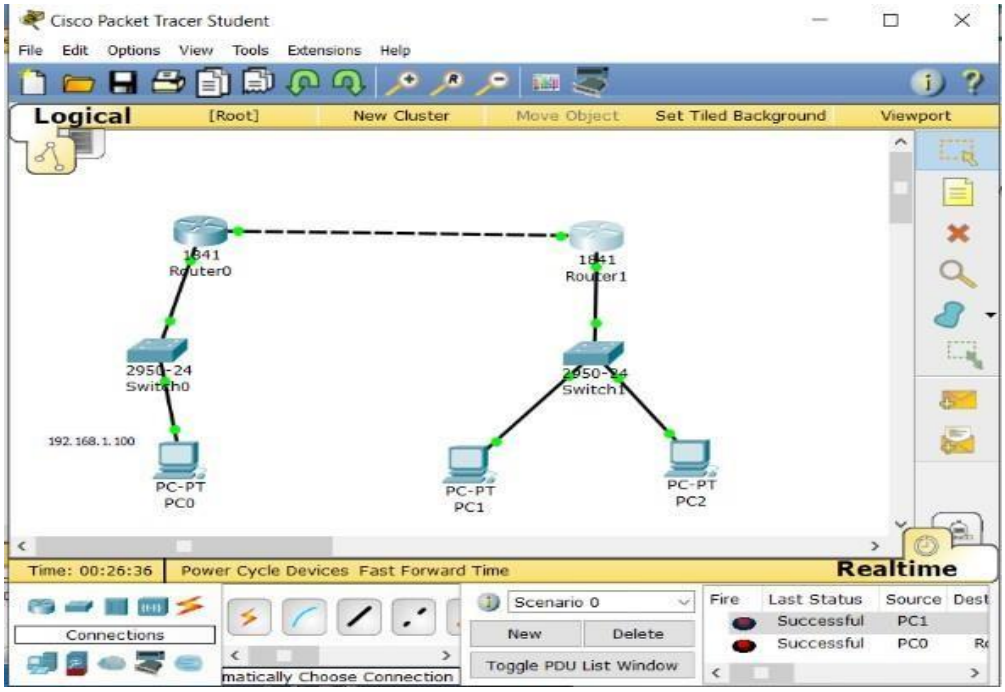
Click on Router0. Go to Config > FastEthernet0/1. Here, add IP Address and On the Port Status.



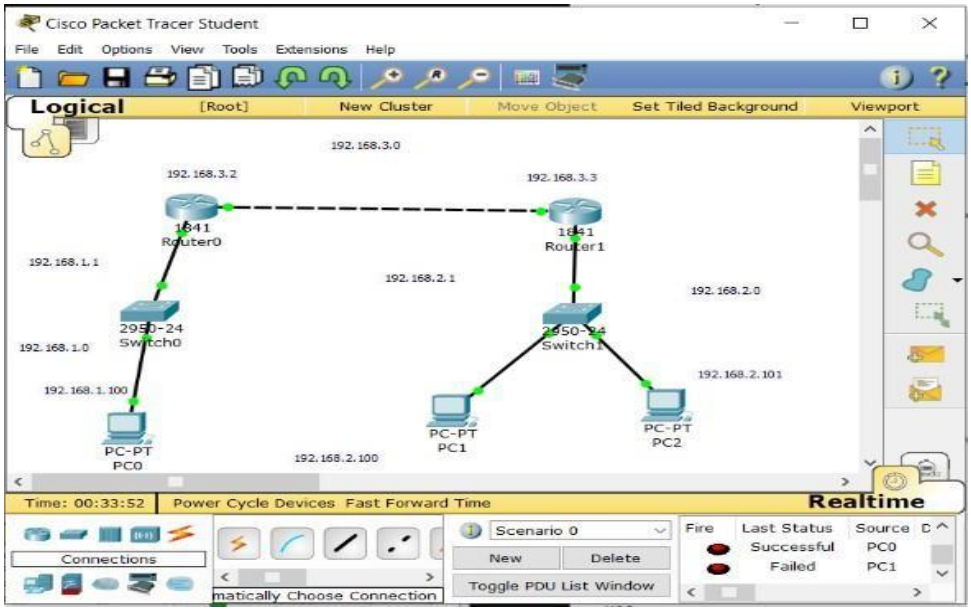
Step 8:

Click on Router1. Go to Config > FastEthernet0/0. Here, add IP Address and On the Port Status





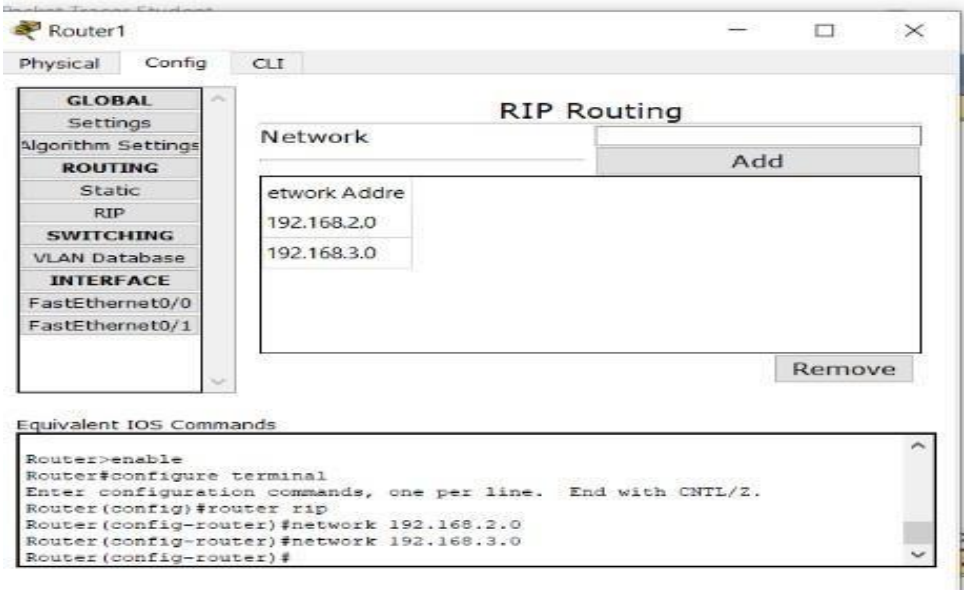
As you can see above, connection is done between both the Routers successfully



Step 9:

Click on Router1. Go to Config > RIP.

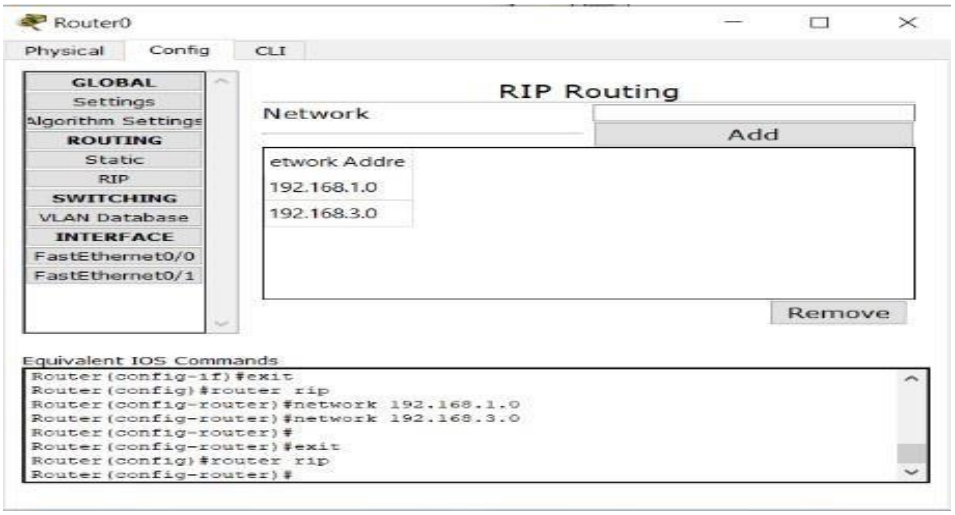
Here, add the network address to connect router1 with switch1, PC1, PC2 and router0.



Step 10:

Click on Router0. Go to Config > RIP.

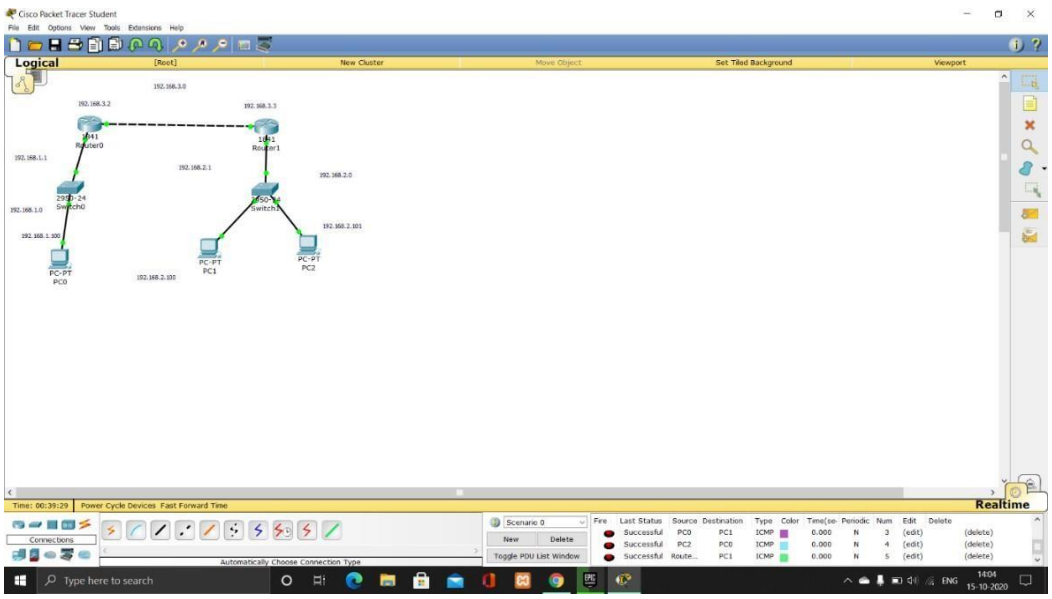
Here, add the network address to connect router0 with switch0, PC0 and router1.



Now, all the connections are done successfully, you can check it by clicking on this symbol

And then, click on any two PCs, you will get the status as successful.

RESULTS:-



So, Routing Information Protocol is done.

Steps for implementing VLAN:

Step1:

Select Router – select 1841 router and drag it to the screen (Router0).

Select another Router – select 1841 and drag it to right of the Router0 (Router1).

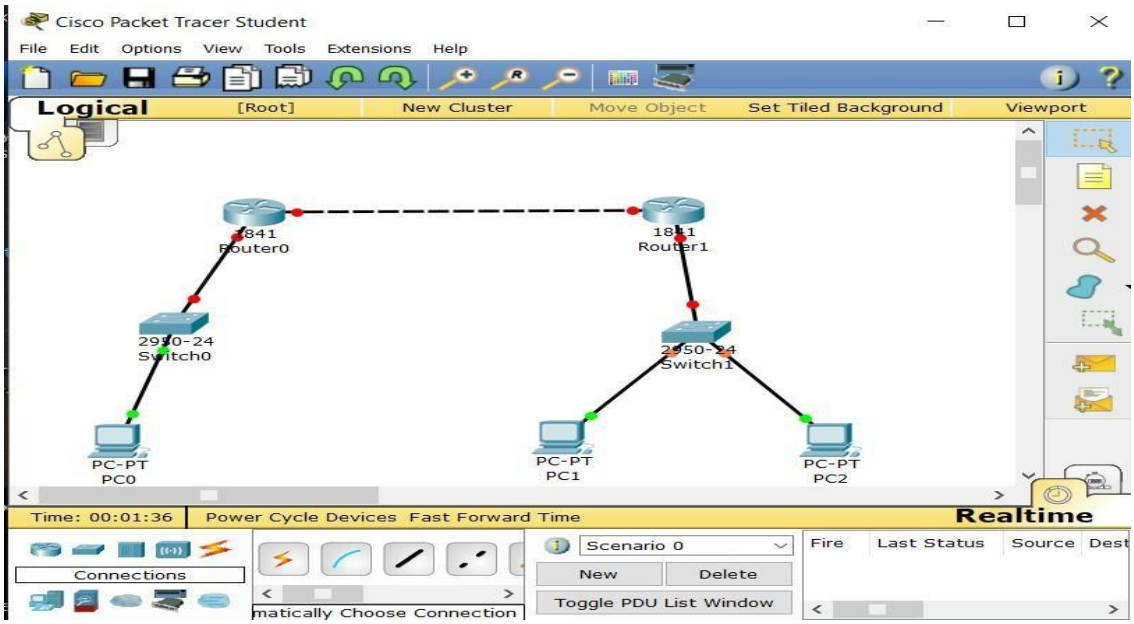
Select Switches – select 2950-24 and drag it below the Router0 (Switch0).

Select Switches – select 2950-24 and drag it below the Router1 (Switch1).

Select End Device – select Generic and drag it below Switch0 (PC-PT PC0).

Select End Device – select Generic and drag it below Switch1 (PC-PT PC1).

Select End Device – select Generic and drag it below Switch1 (PC-PT PC2).

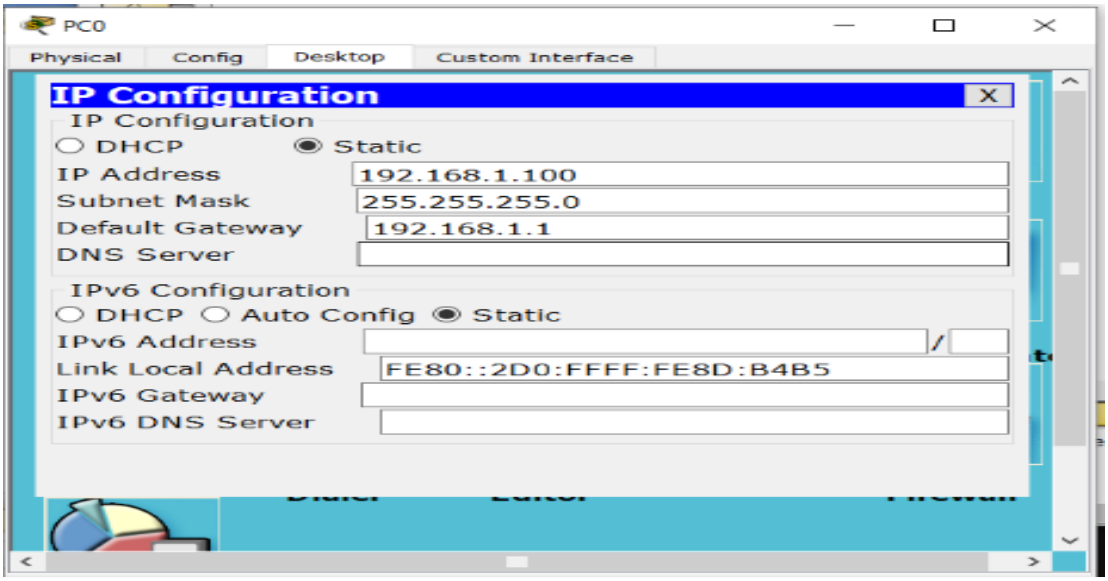


Step 2:

Click on PC0 and go to Desktop > IP Configuration

Add IP Address, as you will add the IP Address, Subnet Mask will be automatically added and displayed.

Add Default Gateway and close the window.

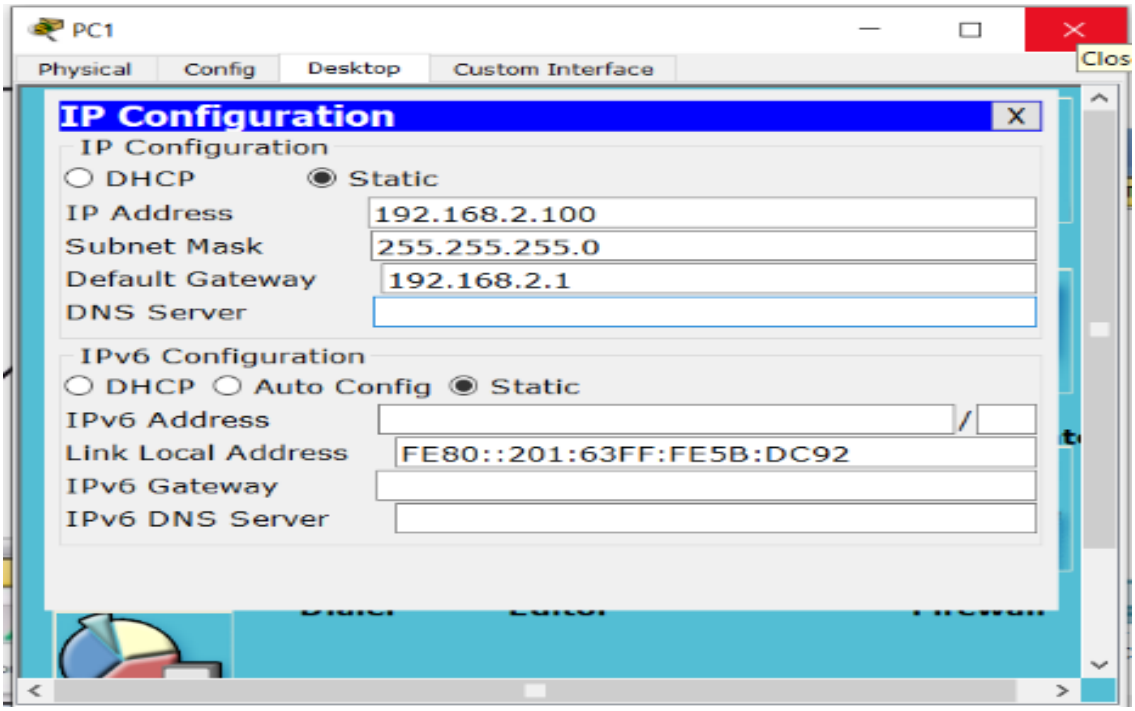


Step 3:

Click on PC1 and go to Desktop > IP Configuration

Add IP Address, as you will add the IP Address, Subnet Mask will be automatically added and displayed.

Add Default Gateway and close the window.

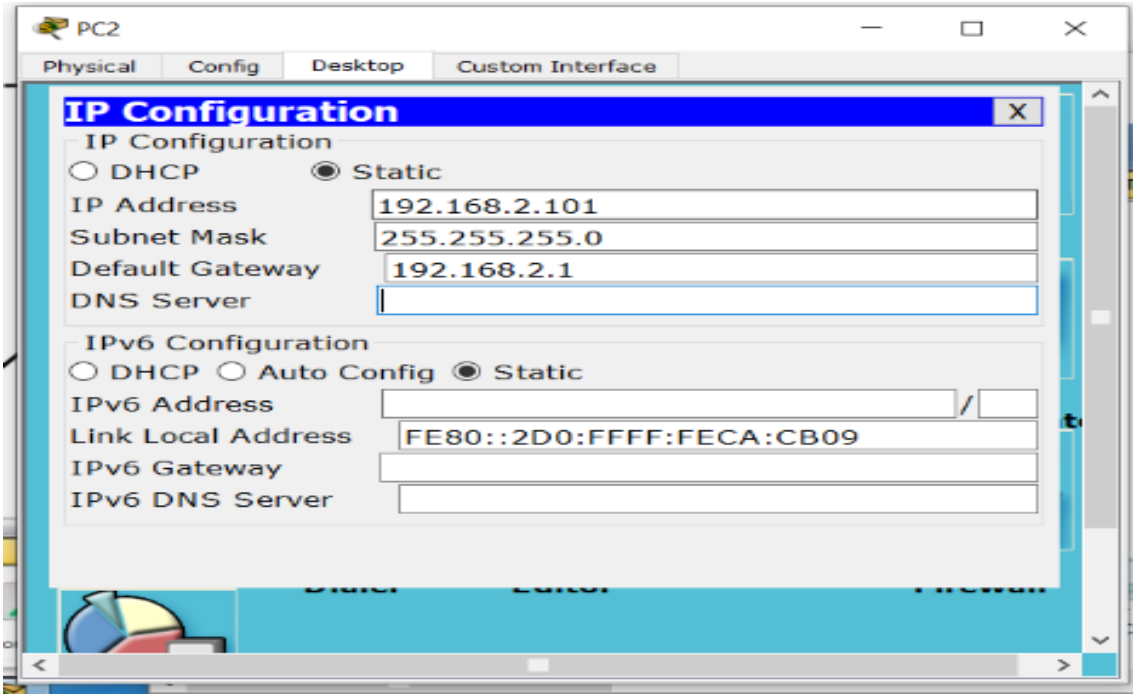


Step 4:

Click on PC2 and go to Desktop > IP Configuration

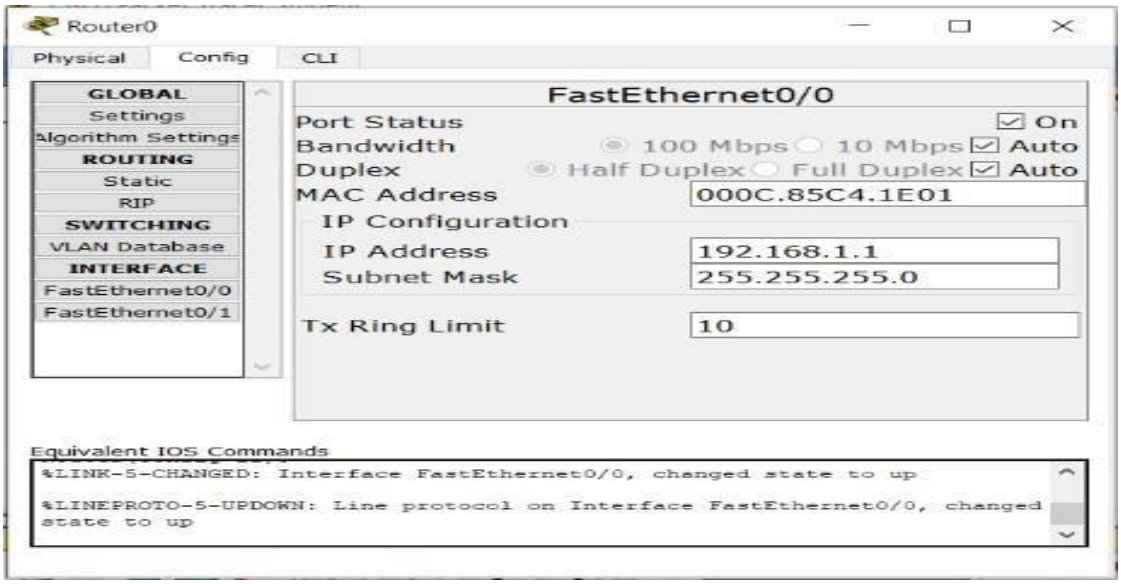
Add IP Address, as you will add the IP Address, Subnet Mask will be automatically added and displayed.

Add Default Gateway and close the window.



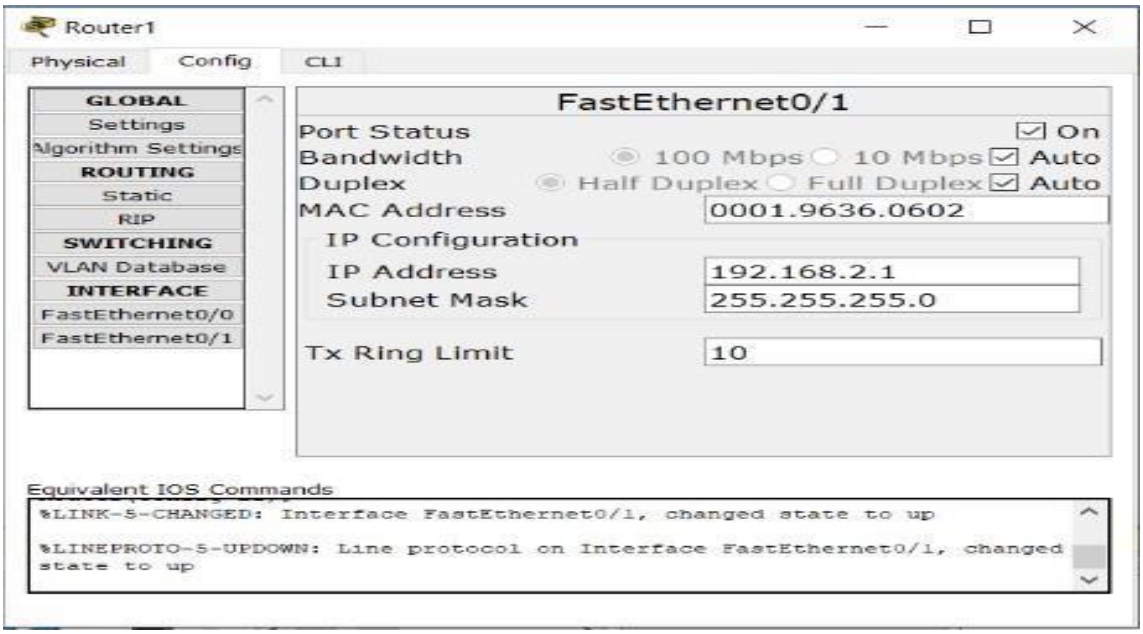
Step 5:

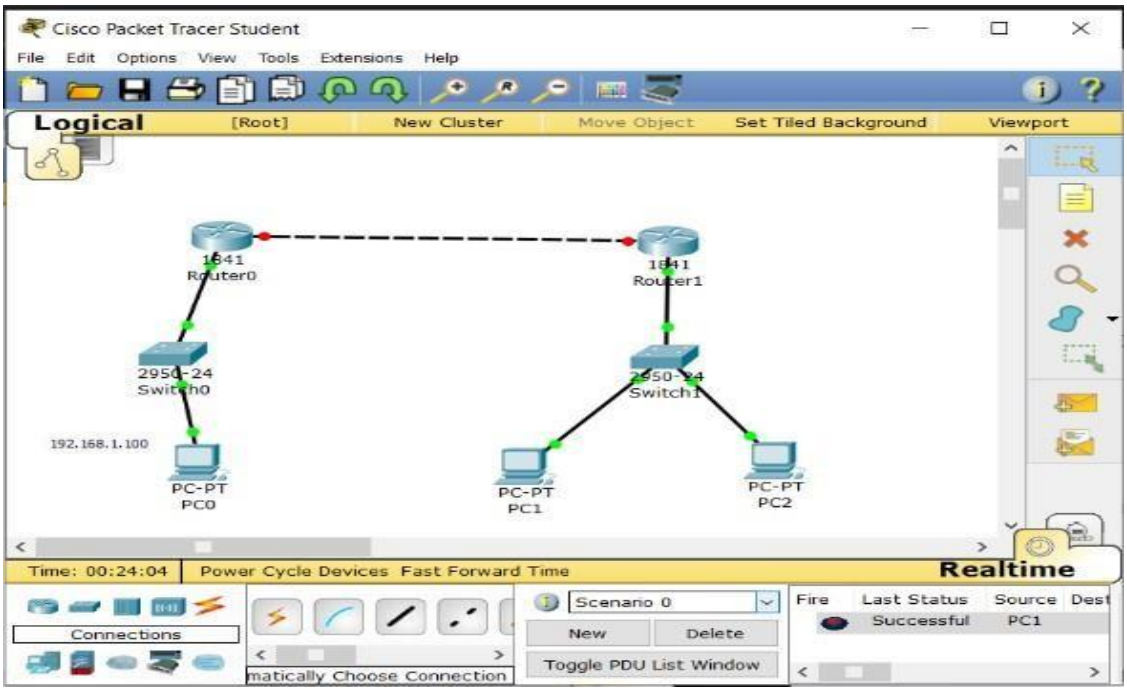
Click on Router0. Go to Config > FastEthernet0/0. Here, add IP Address and On the Port Status.



Step 6:

Click on Router1. Go to Config > FastEthernet0/1. Here, add IP Address and On the Port Status.

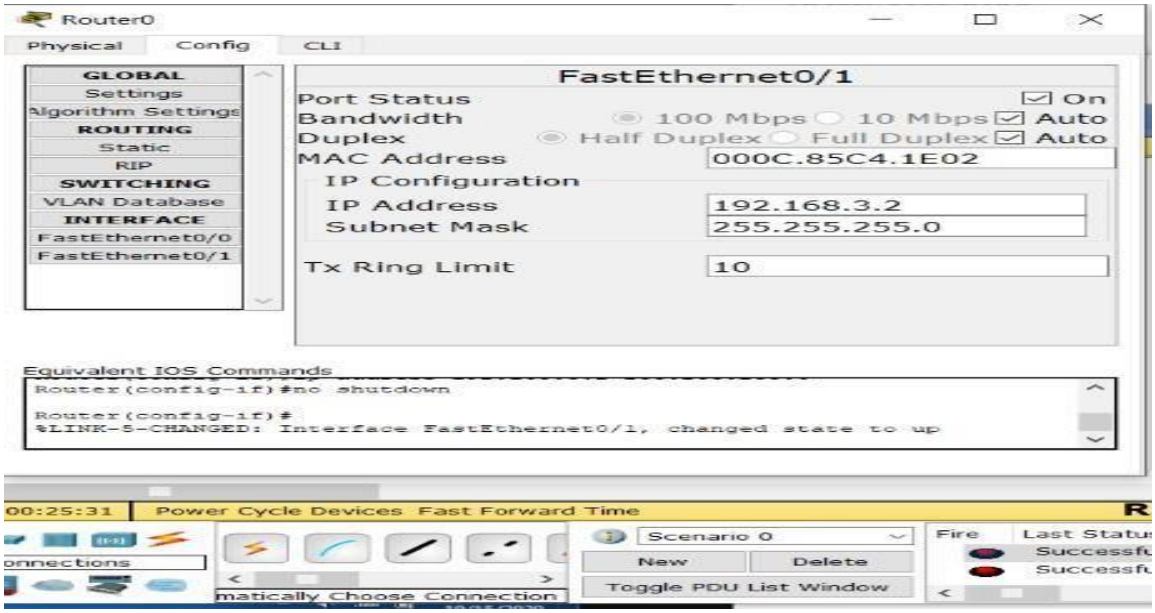




As you will see above, there is green dots which means connections are done successfully between Router, Switches and PCs.

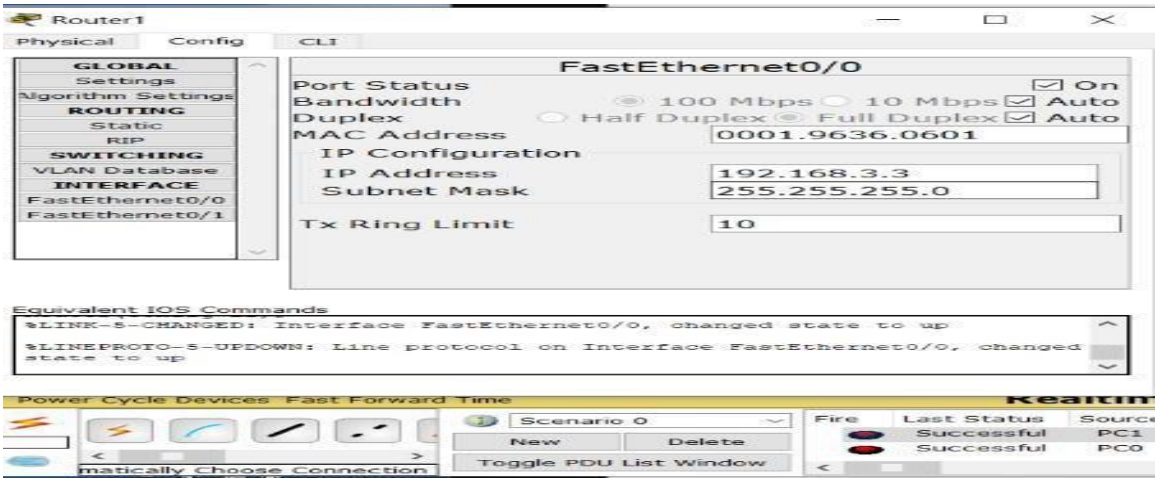
Step 7:

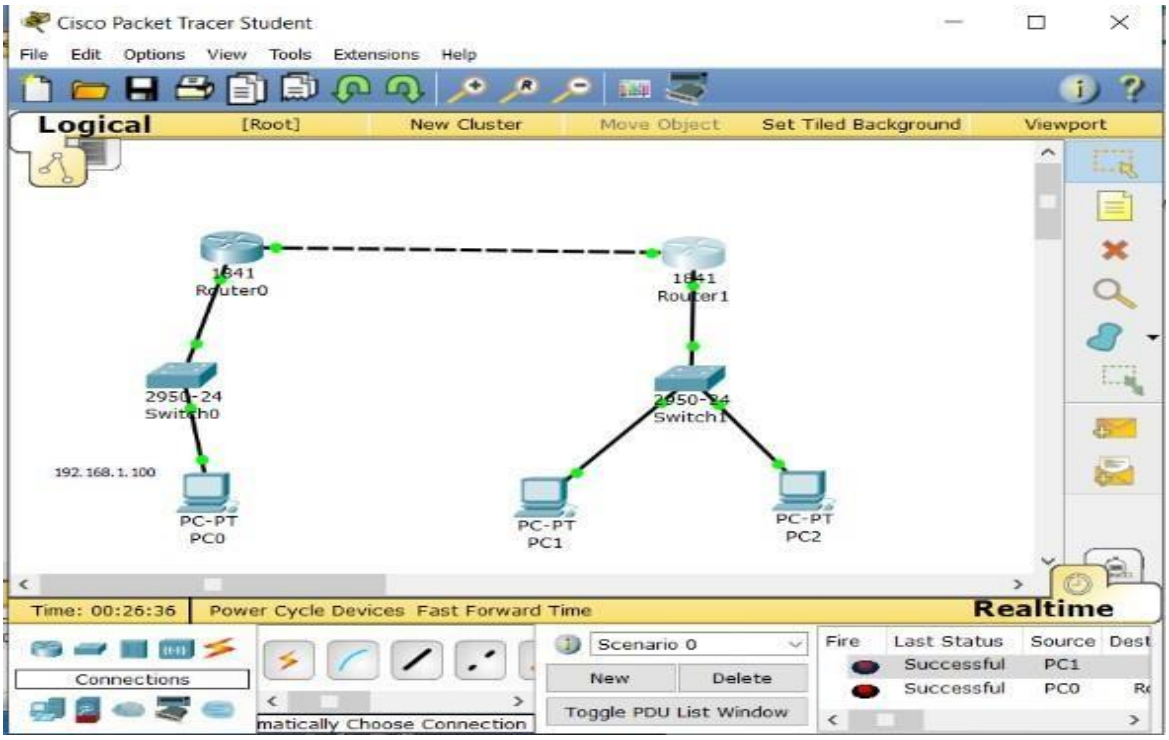
Click on Router0. Go to Config > FastEthernet0/1. Here, add IP Address and On the Port Status.



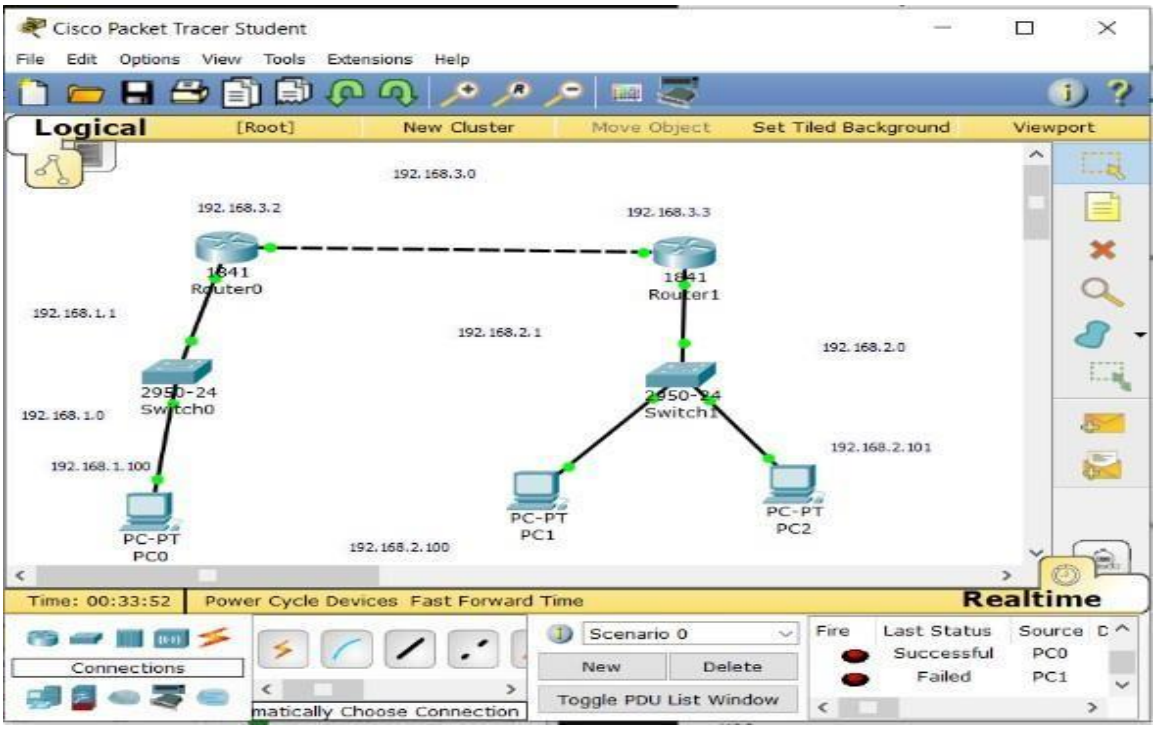
Step 8:

Click on Router1. Go to Config > FastEthernet0/0. Here, add IP Address and On the Port Status.





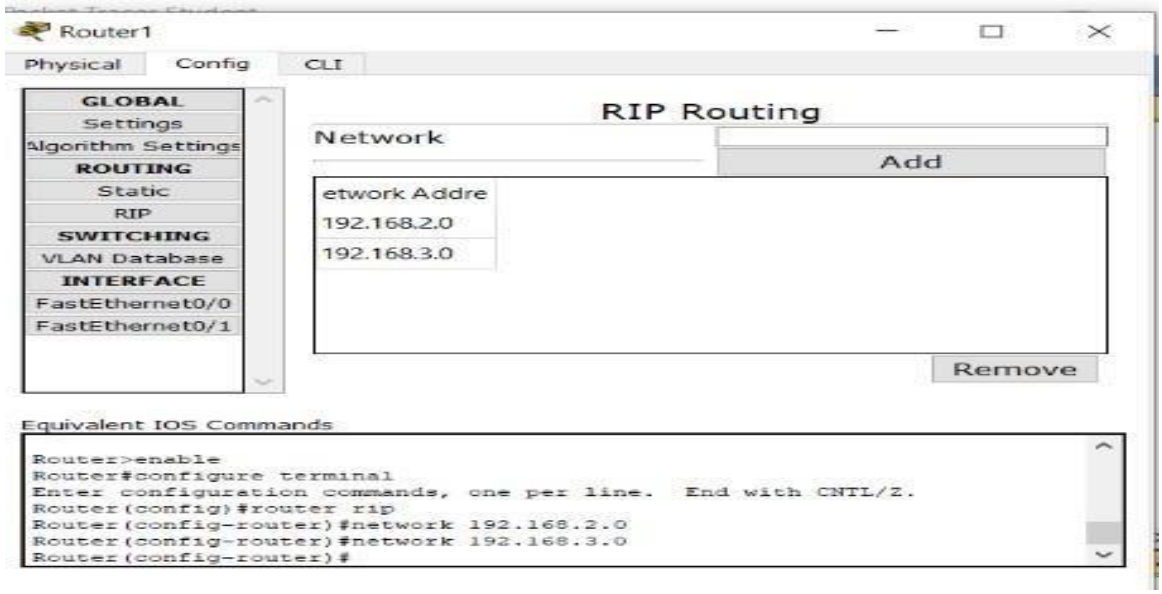
As you can see above, connection is done between both the Routers successfully.



Step 9:

Click on Router1. Go to Config > RIP.

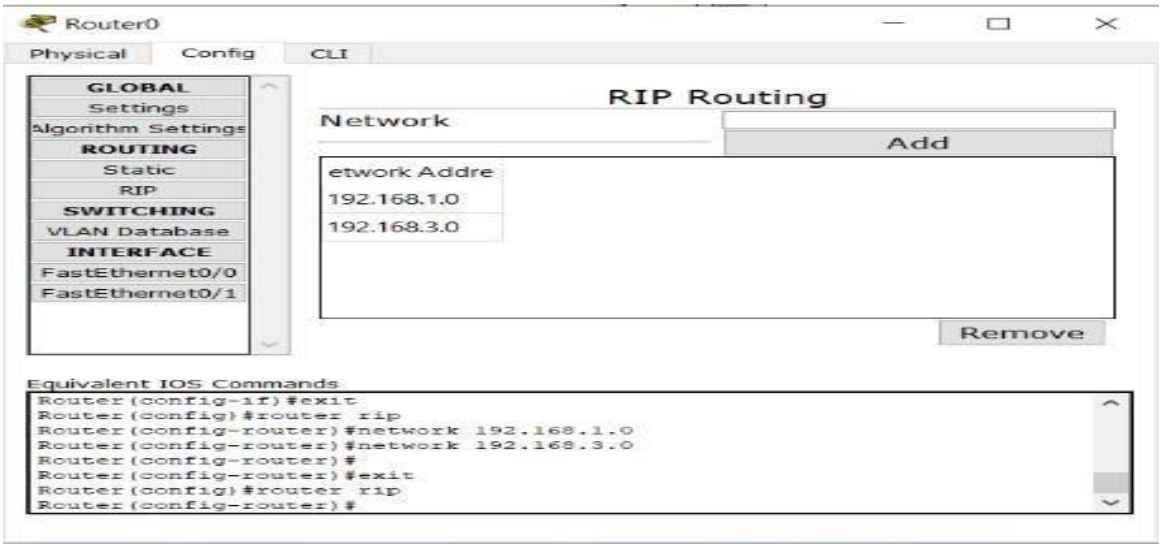
Here, add the network address to connect router1 with switch1, PC1, PC2 and router0.



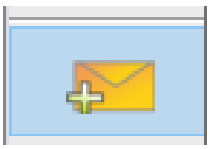
Step 10:

Click on Router0. Go to Config > RIP.

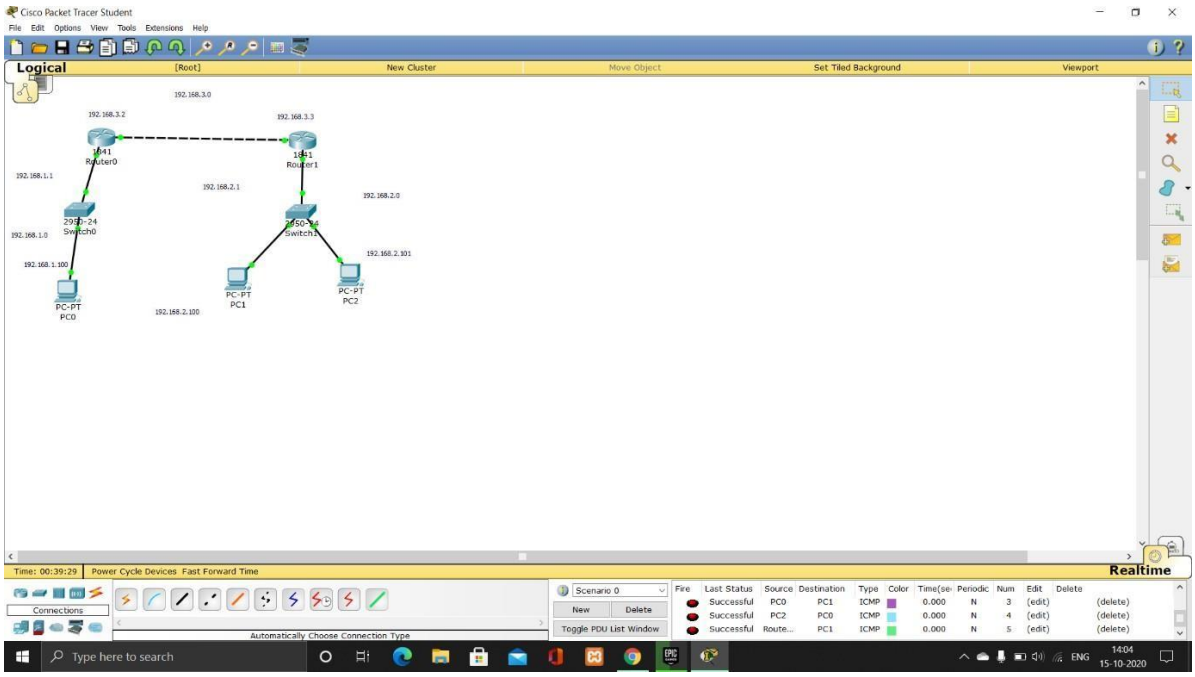
Here, add the network address to connect router0 with switch0, PC0 and router1.



Now, all the connections are done successfully, you can check it by clicking on this symbol



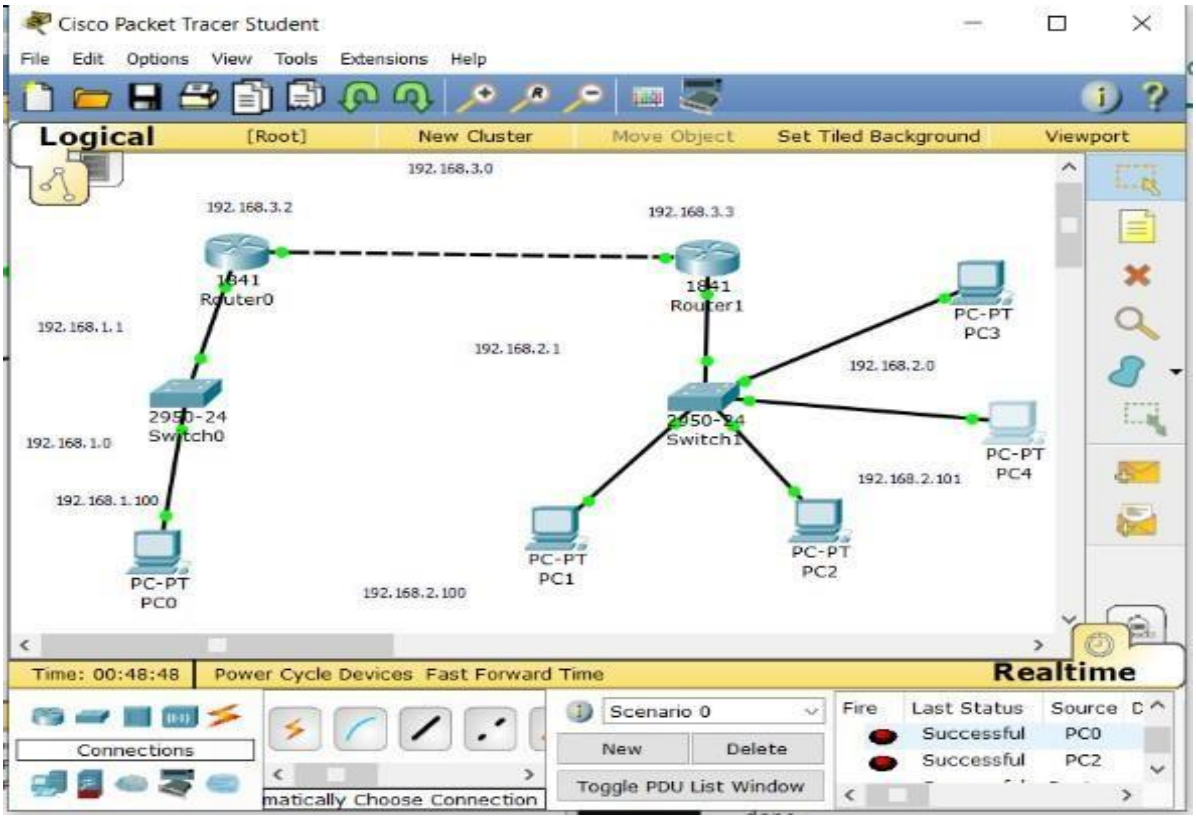
And then, click on any two PCs, you will get the status as successful.

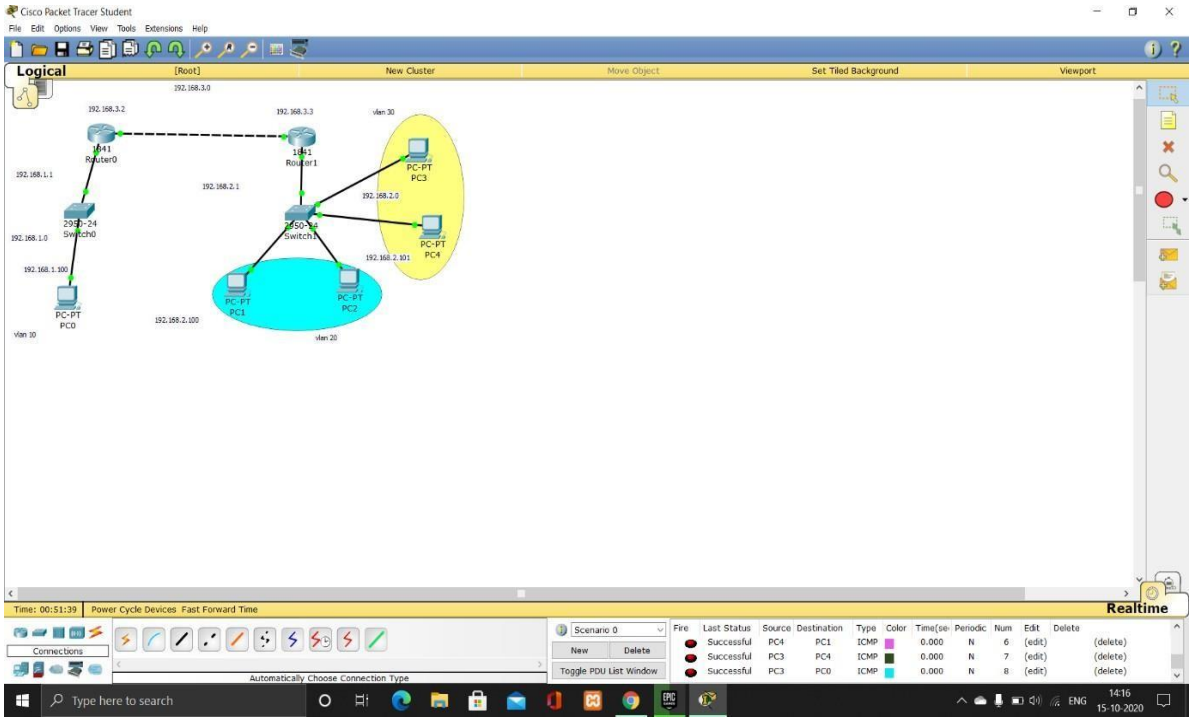


So till now, Routing Information Protocol is done. Now, we will start with implementing VLAN

Step 11:

Add two PC (PC 3 and PC4) and connect it with switch.


Cisco Packet Tracer Student
File Edit Options View Tools Extensions Help
Logical [Root] New Cluster Move Object Set Tiled Background Viewport
192.168.3.0
192.168.3.2
192.168.3.3
1841 Router0
1841 Router1
192.168.1.1
192.168.2.1
PC-PT PC3
192.168.2.0
2950-24 Switch0
2950-24 Switch1
192.168.1.0
PC-PT PC4
192.168.2.101
192.168.1.100
PC-PT PC1
PC-PT PC2
PC-PT PC0
192.168.2.100
Time: 00:48:48 Power Cycle Devices Fast Forward Time
Realtime
Connections
Scenario 0
New Delete
Toggle PDU List Window
Fire Last Status Source
Successful PC0
Successful PC2

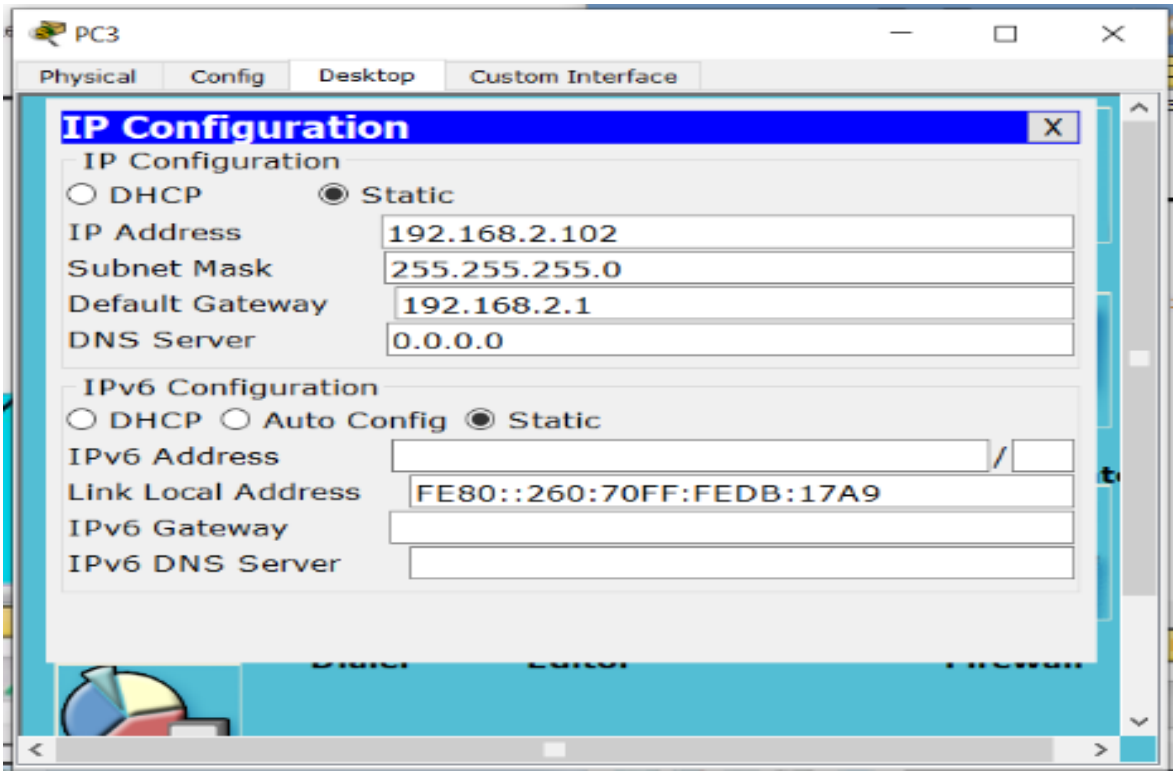

Cisco Packet Tracer Student
Logical [Root] New Cluster Move Object Set Tiled Background Viewport
Time: 00:51:39 Power Cycle Devices Fast Forward Time
Realtime
Connections
Automatically Choose Connection Type
Scenario 0
New Delete
Toggle PDU List Window
Type here to search
ENG
14:16
15-10-2020

Step 12:

Click on PC3 and go to Desktop > IP Configuration

Add IP Address, as you will add the IP Address, Subnet Mask will be automatically added and Displayed

Add Default Gateway and close the window.

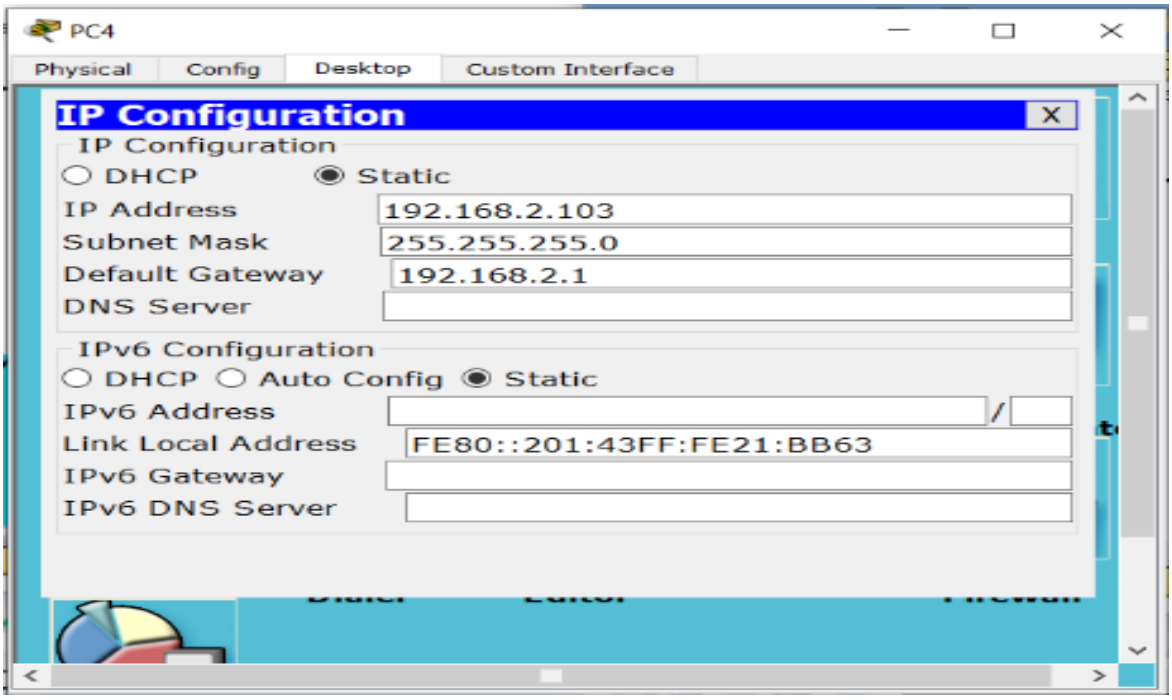


Step 13:

Click on PC3 and go to Desktop > IP Configuration

Add IP Address, as you will add the IP Address, Subnet Mask will be automatically added and displayed.

Add Default Gateway and close the window.



Step 14:

Click on Switch1 and go to CLI Add type the VLAN code – VLAN CODE:

VLAN

enable config t vlan 20

name purchase

exit

vlan 30 name sales

exit

int fa0/2

switchport access vlan 20

exit

int fa0/3

switchport access vlan 20

exit

int fa0/4

switchport access vlan 30

exit

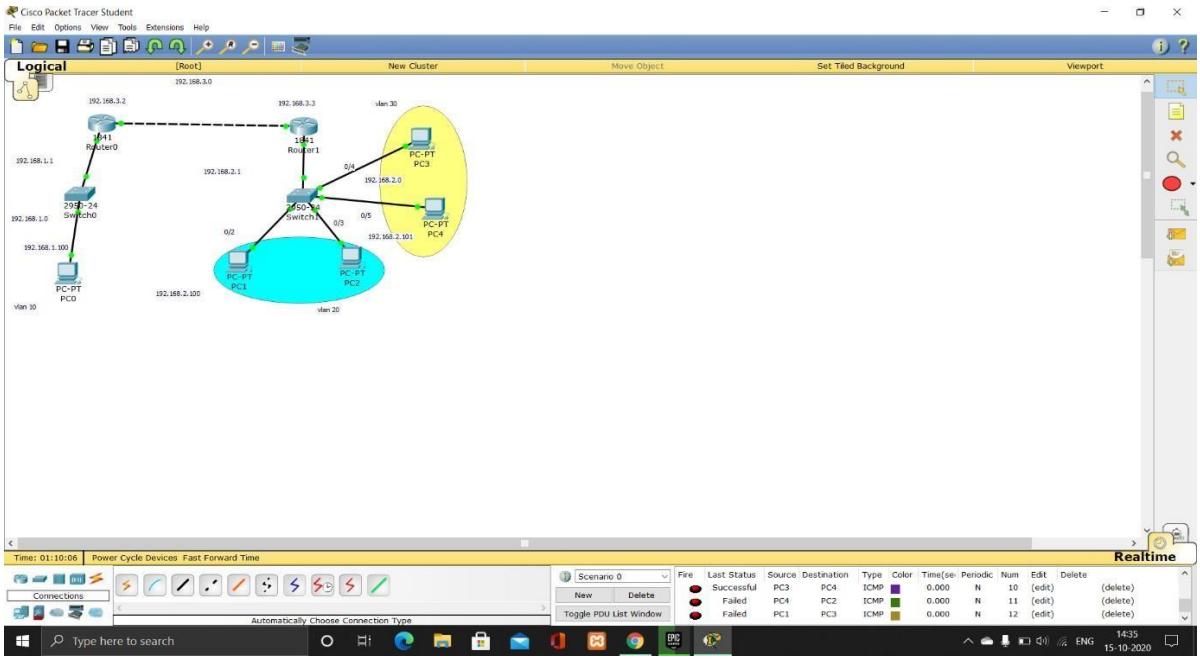
int fa0/5

switchport access vlan 30

exit

Final Output:

Now, PC1, PC2 are not connected to PC3 and PC4.



CONCLUSION: Thus, we have successfully implemented VLAN and RIP protocol.

INDUSTRIAL APPLICATION:-

Use for Data Communication or for Connecting one system with another

REFERNCES:-

1. B.A. Forouzan, ―Data Communications and Networking .TMH (5e)
2. www4.ncsu.edu/~kksivara/sfwr4c03/lectures/lecture7.pdf
3. www.instructables.com › technology › software
4. https://superuser.com/questions/.../how-to-telnet-to-an-ip-address-on-a-specific- port

VIVA QUESTIONS

1. What do u mean by TELNET?

---

2. Define the DEC?

---

3. Enlist the use of TELNET?

---

4. State domain name is used for Education?

---

5. Write domain name is used for India?

Experiment No.10

AIM: Java program for Socket Programming

THEORY:

Java Socket Programming

- 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:

a.IP Address of Server, and
b.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 printsit. 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 class

A socket is simply an endpoint for communications between the machines. The Socket class can be used to create a socket.

#ServerSocket class

The ServerSocket class can be used to create a server socket. This object is used to establish communication with the clients.

Creating Server:

To create the server application, we need to create the instance of ServerSocket class. Here, we are using 6666 port number for the communication between the client and server. You may also choose any other port number. The accept() method waits for the client. If clients connects with the given port number, it returns an instance of Socket.

```
ServerSocket ss=new ServerSocket(6666);
Socket s=ss.accept();//establishes connection and waits for the client
```

Creating Client:

To create the client application, we need to create the instance of Socket class. Here, we need to pass the IP address or hostname of the Server and a port number. Here, we are using "localhost" because our server is running on same system.

```
Socket s=new Socket("localhost",6666);
```

Code:-

MyServer.java file

```
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);}
}
}
```

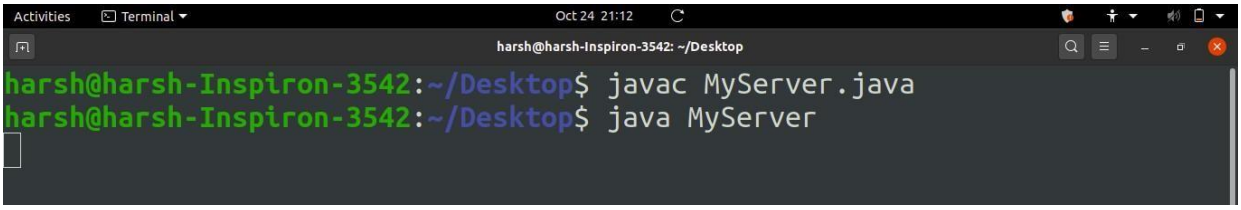
MyClient.java file

```
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 Server");
dout.flush();
dout.close();
s.close();
}catch(Exception e){System.out.println(e);}
}
}
```

Output:

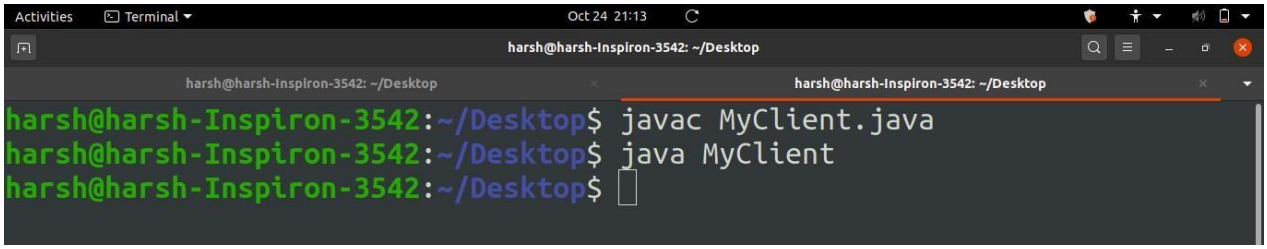
To execute this program open two command prompts and execute each program at each command prompt as displayed in the below figures.

First run Myserver.java file in terminal/cmd,



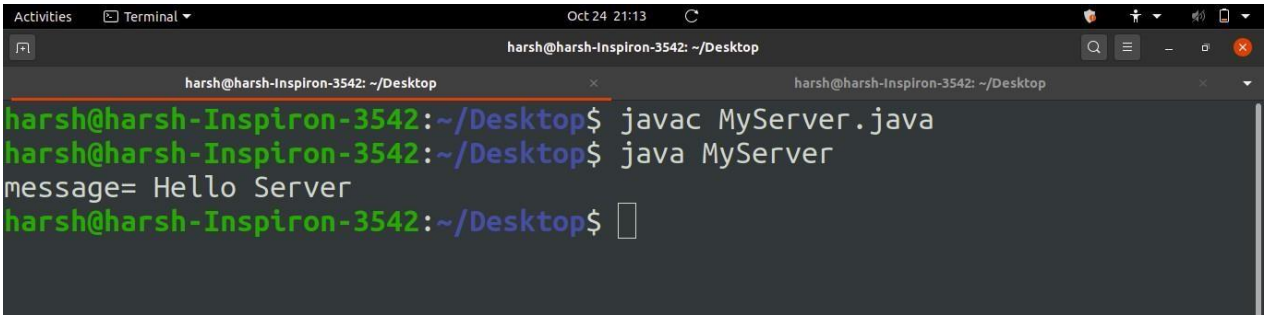
Running MyServer.java

Then in new terminal/cmd run MyClient.java file,



Running MyClient.java

As soon as you run MyClient program a message is sent to server and displayed in MyServer Terminal/CMD as shown below



Message displayed in MyServer after running MyClient

CONCLUSION:- So, in this experiment we have successfully understood the concept of Socket Programming and implemented it using Java Programming

Experiment No.11

AIM: Perform File Transfer and Access using FTP

THEORY:

Transferring files from a client computer to a server computer is called **"uploading"** and transferring from a server to a client is **"downloading".**

Requirements for using FTP

1. An FTP client like Auto FTP Manager installed on your computer

2. Certain information about the FTP server you want to connect to:

a. The **FTP server address.** This looks a lot like the addresses you type to browse web sites.

Example : Server address is "ftp.videodesk.net".

Sometimes the server address will be given as a numeric address, like "64.185.225.87".

b. A user name and password. Some FTP servers let you connect to them anonymously.

For anonymous connections, you do not need a user name and password. To transfer files, provide your client software (Auto FTP Manager) with the server address, user name, and password. After connecting to the FTP server, you can use Auto FTP Manager's **File Manager** to upload, download and delete files. Using the File Manager is a lot like working with Windows Explorer.

FTP and Internet Connections

FTP uses one connection for commands and the other for sending and receiving data. FTP has a standard port number on which the FTP server "listens" for connections. A port is a "logical connection point" for communicating using the Internet Protocol (IP). The standard port number used by FTP servers is 21 and is used only for sending commands. Since port 21 is used exclusively for sending commands, this port is referred to as a **command port.** For example, to get a list of folders and files present on the FTP server, the FTP Client issues a "LIST" command. The FTP

server then sends a list of all folders and files back to the FTP Client. So what about the internet connection used to send and receive data? The port that is used for transferring data is referred to as a **data port.** The number of the data port will vary depending onthe "mode" of the connection. (See below for Active and Passive modes.)

Active and Passive Connection Mode

The FTP server may support **Active** or **Passive** connections or both. In an Active FTP connection, the client opens a port and listens and the server actively connects to it. In a Passive FTP connection, the server opens a port and listens (passively) and the client connects to it. You must grant Auto FTP Manager access to the Internet and to choose the right type of FTP Connection Mode. Most FTP client programs select passive connection mode by default because server administrators prefer it as a safety measure. Firewalls generally block connections that are "initiated" from the outside. Using passive mode, the FTP client (like Auto FTP Manager) is "reaching out" to the server to make the connection. The firewall will allow these outgoing connections, meaning that no special adjustments to firewall settings are required.

If you are connecting to the FTP server using **Active mode** of connection you must set your firewall to accept connections to the port that your FTP client will open. However, many Internet service providers block incoming connections to all ports above 1024. Active FTP servers generally use port 20 as their data port.

IMPLEMENTATION:

Step 1: Installation of the Package

1. # rpm –ivh vsftpd-

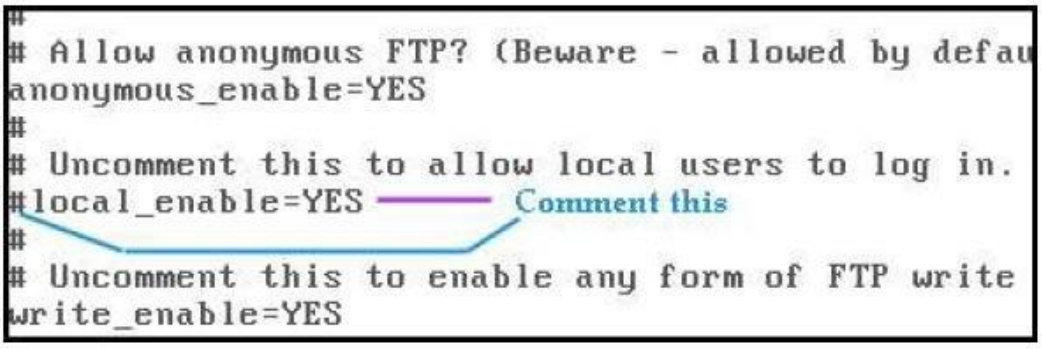
```
[root@server ~]# vi /etc/vsftpd/vsftpd.conf
```

Step 2: Editing Configuration files

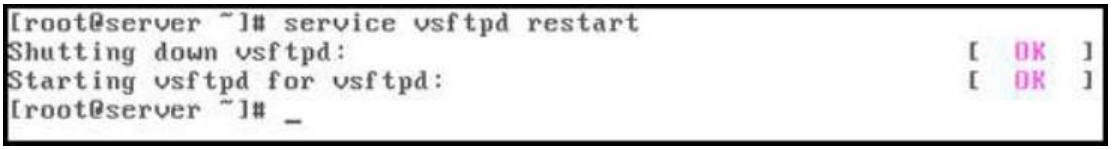
1. Open ftp configuration file **/etc/vsftpd/vsftpd.conf**

2. Set up anonymous access of FTP server.

vsftpd.conf is the main configuration file of FTP server and it contains lot of directives. Configuration of an anonymous-only download is relatively simple. Default configuration of vsftpd.conf already supports anonymous-only download. But it also supports access from local users. All you need to do is disable the directive which allows locally configured users to login with their accounts.



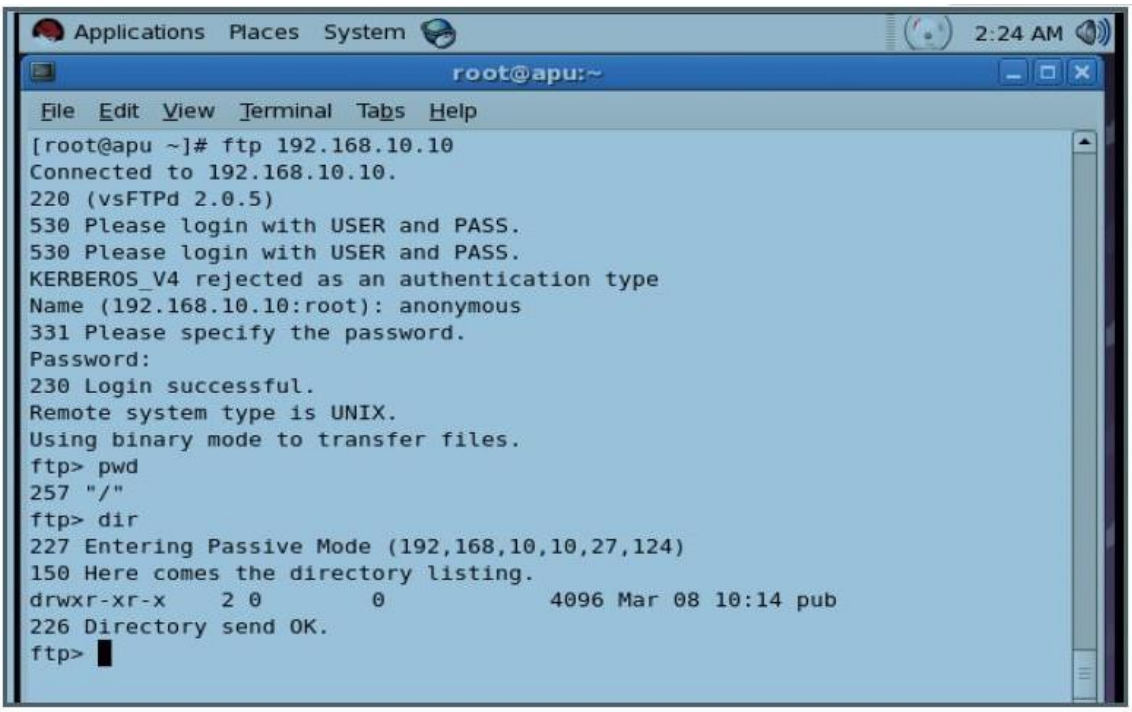
Step 3: Restart the vsftpd service



Step 4: Check connectivity with FTP Server.

 # Ping ip address of the ftp server (192.168.10.10)

Step 5: Test the FTP server and transfer files using command prompt.

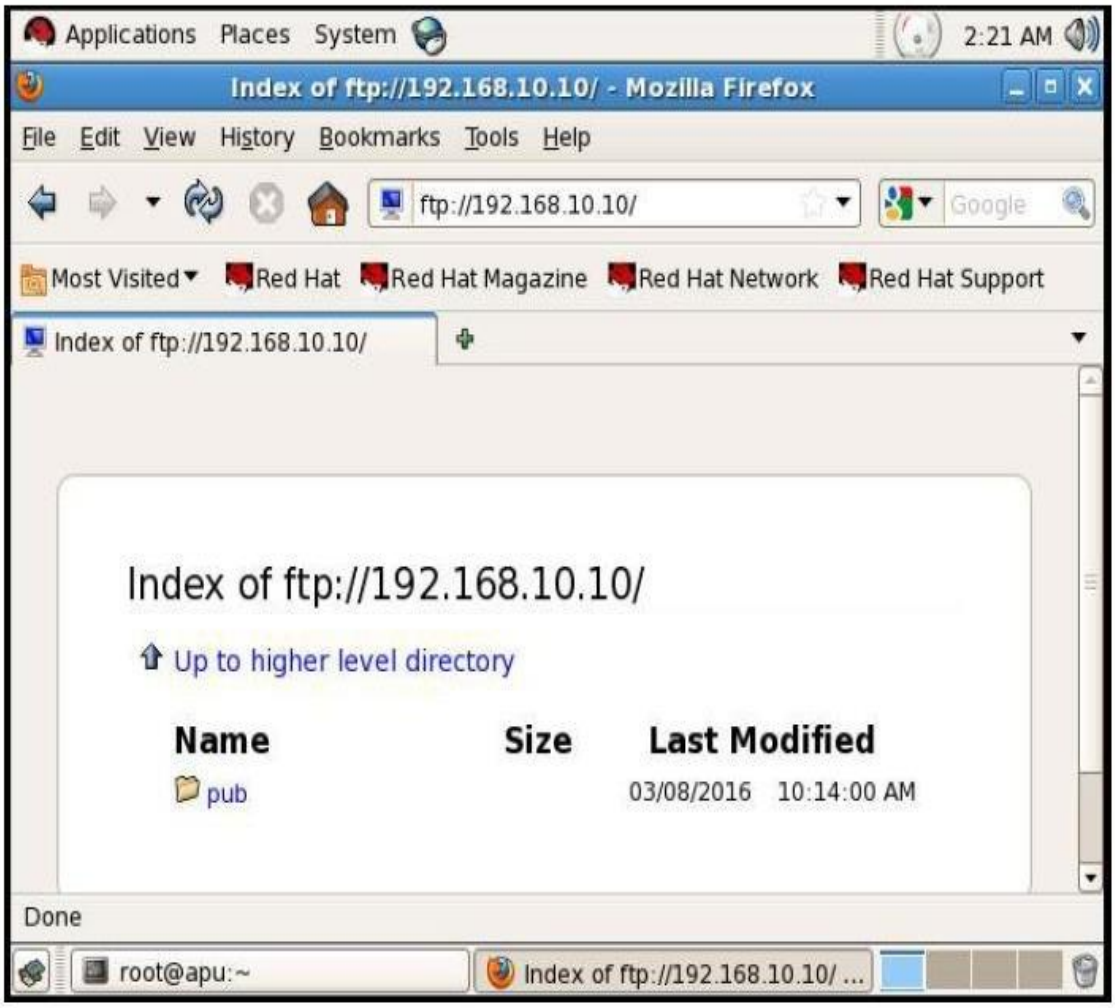



```
ftp> dir
227 Entering Passive Mode (192,168,10,10,27,124)
150 Here comes the directory listing.
drwxr-xr-x    2 0        0            4096 Mar 08 10:14 pub
226 Directory send OK.
ftp> cd pub
250 Directory successfully changed.
ftp> ls
227 Entering Passive Mode (192,168,10,10,92,177)
150 Here comes the directory listing.
-rw-r--r--    1 0        0               0 Mar 08 10:17 file
226 Directory send OK.
ftp> get file
local: file remote: file
227 Entering Passive Mode (192,168,10,10,26,245)
150 Opening BINARY mode data connection for file (0 bytes).
226 File send OK.
ftp> put file
local: file remote: file
227 Entering Passive Mode (192,168,10,10,177,44)
550 Permission denied.
ftp>
```

We can download the file using anonymous user but cannot upload the file. Also the default data location (or pwd) of FTP server will be pub directory during anonymous access.

b. Access the FTP server and transfer files using command prompt

1) First go to browser then and type FTP://192.168.10.10. It will show default location of pub Directory



2) User Specific Authentication

1) Create local user and provide password to it.

```
[root@apu ~]# adduser abc
[root@apu ~]# passwd abc
Changing password for user abc.
New UNIX password:
BAD PASSWORD: it is too short
Retype new UNIX password:
passwd: all authentication tokens updated successfully.
[root@apu ~]#
```

root@apu:~

2) Edit VSFTPD configuration file:-

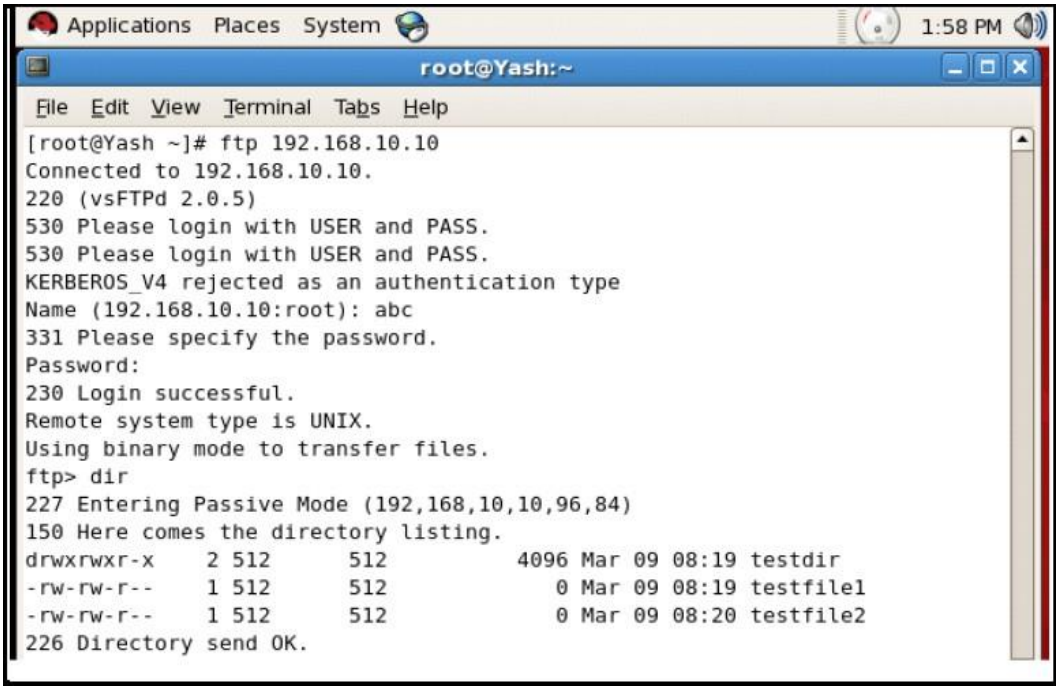

```
# Allow anonymous FTP? (Beware - allowed by default if you comment this out$
anonymous_enable=NO
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
```

```
# Uncomment this to enable any form of FTP write command.
write_enable=YES
#
```

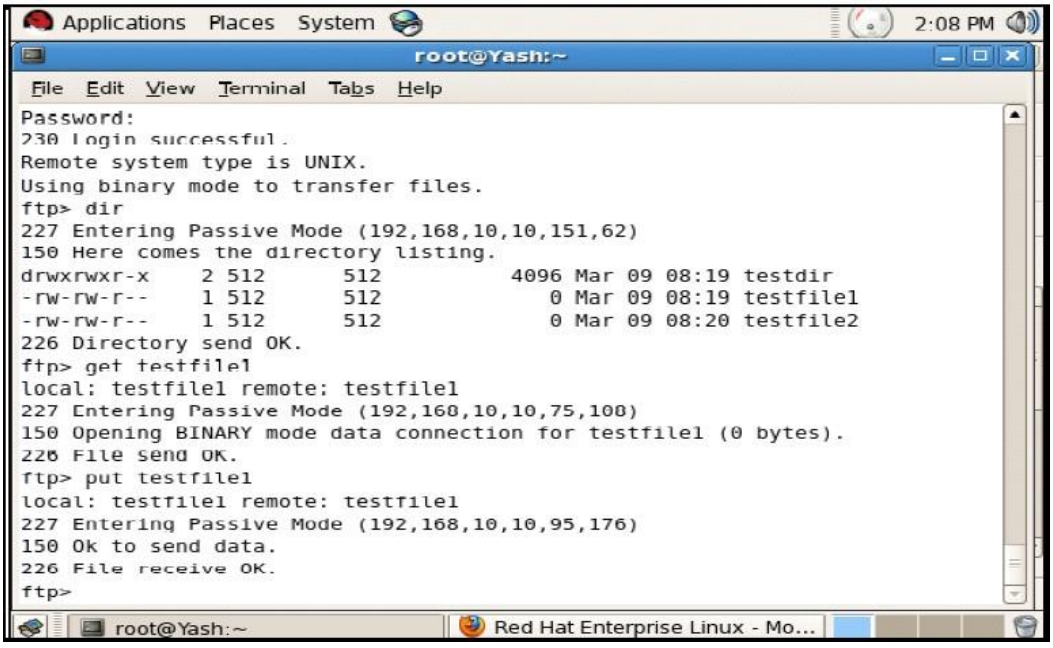
3) Restart VSFTPD service:-

Access FTP server through command prompt

Login from local user abc and create a testfiles and testdir.



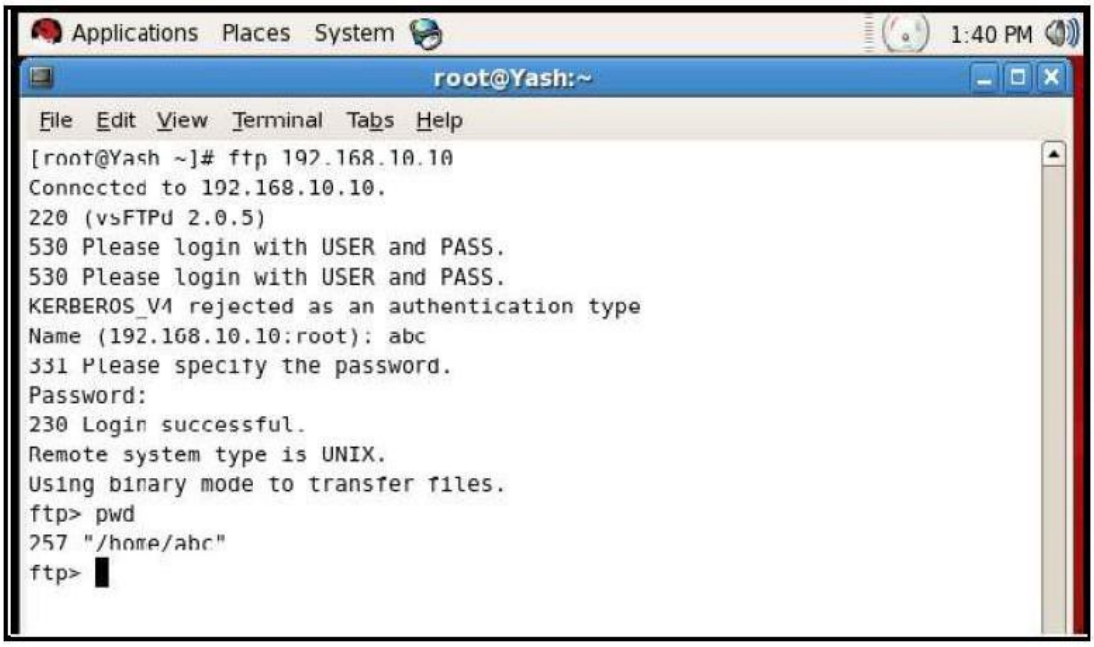
upload/download file.



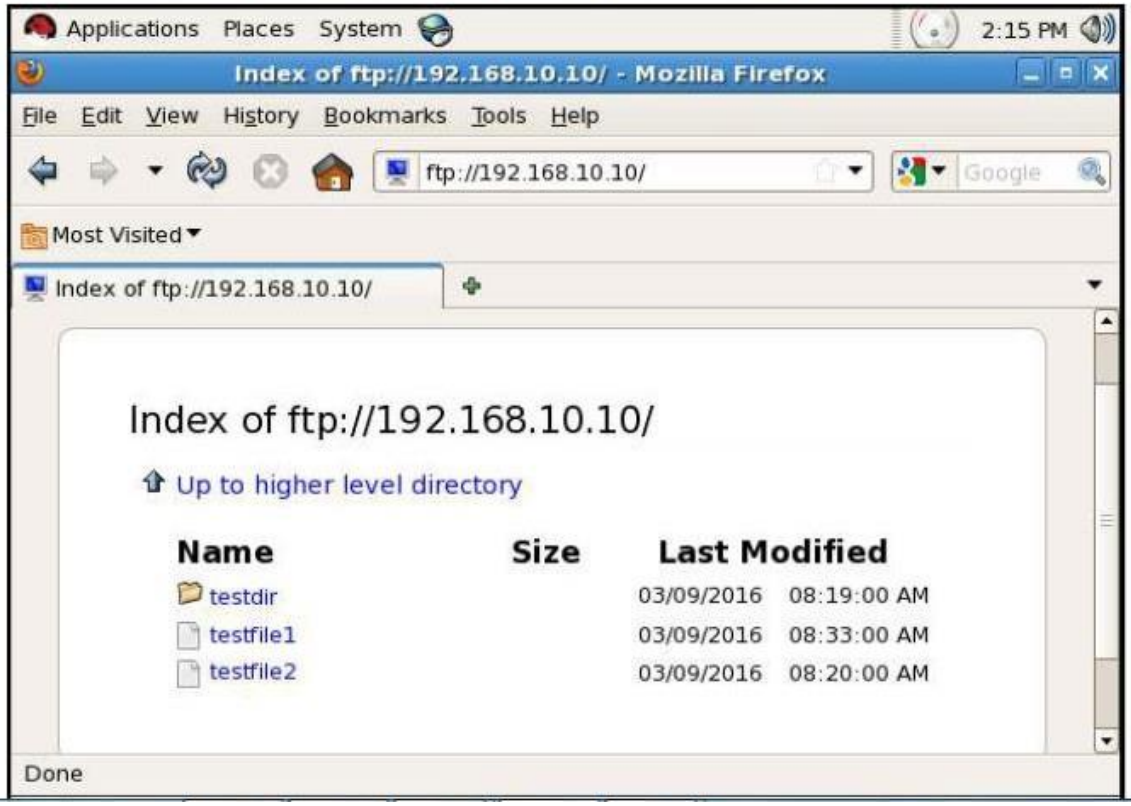
- **To access FTP server through browser:**

Now go to browser and type FTP://192.168.10.10. Add username and password of local user and press enter.

Default location :



List of directories and files created in local user will be shown .



CONCLUSION:

The File Transfer Protocol (FTP) is a standard network protocol used to transfer computer files from one host to another host over a TCP-based network, such as the Internet. FTP is built on a client-server architecture and uses separate control and data connections between the client and the server.

During the Anonymous access of FTP server default location of FTP data will be pub directory.

However during user specific access default location of ftp data will be user directory in /home on server.

Experiment No.12

AIM: Perform Remote login using Telnet server

THEORY:

Telnet protocol allows you to connect to remote hosts over TCP/IP network. Telnet was developed in 1969. Telnet was initially developed for private use where security was not primary concern. Telnet protocol has serious security issue. Security expert recommend that the use of Telnet for remote login should be discontinued under all normal circumstances.

-Telnet Server

-Telnet Client

-Telnet Sever

Telnet server software is installed on remote host. You need to configure it before client can connect with it.

-Telnet Client

Telnet client software allows you to connect telnet server. Once telnet client establishes a connection to the remote host, client becomes a virtual terminal, allowing you to communicate with the remote host from your computer.

Security issue with Telnet Telnet by default does not encrypt any data sent over the connection.

Anyone who has access to network device located on the network between the two hosts like router, switch, hub or gateway where Telnet is being used can intercept the packets passing by and obtain login, password and whatever else is typed with apacket sniffer software.

-Telnet protocol have no implementations that would ensure that communication is carried out between the two hosts is not intercepted in the middle.

-In RHEL Telnet is part of the xinetd daemon.

-Telnet use plain text to transmit password.

-root user is not allowed to connect using Telnet.

-Command-line telnet clients are built into all major operating systems.

IMPLEMENTATION:

Configure Telnet in RHEL 6

Three RPM are required to configure telnet server in linux.

•xinetd

•telnet-server

•telnet-client

Step 1: Installation of Packages:-

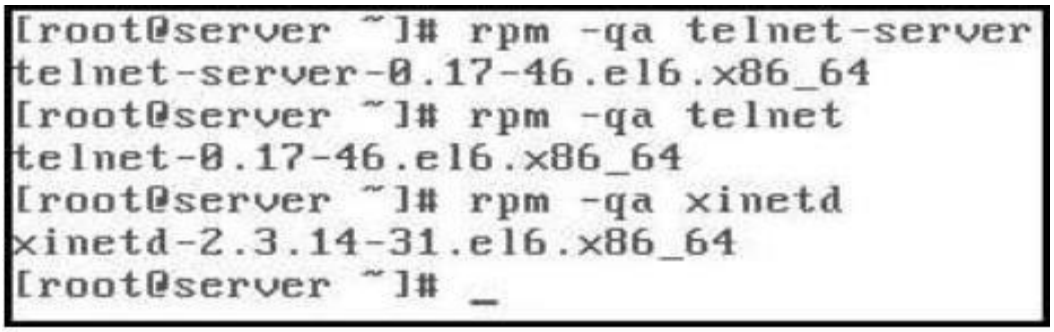
1. Login using root account. Necessary rpm for telnet server is xinetd, telnet-server and telnet .

rpm –ivh xinetd-2.3.14-31.e16.X86_64

rpm –ivh telnet-server-

rpm –ivh telnet-

2.To check whether the package is installed on the system.



The version numbers of the package should not matter, Red Hat Network (RHN) will always provide you with the latest version of the package.

Step 2: Check Configuration files

Once you have the packages installed, check the **/etc/xinetd.d/telnet** file.

```
[root@server ~]# vi /etc/xinetd.d/telnet _
```

ensure that **disable** = **yes** is changed to read **disable** = **no**.

```
# default: on
# description: The telnet server serves telnet sessions; it uses \
#       unencrypted username/password pairs for authentication.
service telnet
{
        disable = no
        flags           = REUSE
        socket_type     = stream
        wait            = no
        user            = root
        server          = /usr/sbin/in.telnetd
        log_on_failure  += USERID
}
```

Turn the Telnet server **on** using the **chkconfig** command.

```
[root@server ~]# chkconfig --list telnet
telnet          off
[root@server ~]# chkconfig telnet on
[root@server ~]# chkconfig --list telnet
telnet          on
[root@server ~]# _
```

Also check xinetd service

```
[root@server ~]# chkconfig --list xinetd
xinetd          0:off   1:off   2:on    3:on    4:on    5:on    6:off
[root@server ~]# _
```

Step 3: Restart the xinetd service.

```
[root@server ~]# service xinetd restart
Stopping xinetd:                                           [  OK  ]
Starting xinetd:                                           [  OK  ]
[root@server ~]# _
```

Step 4: Disable Firewall.

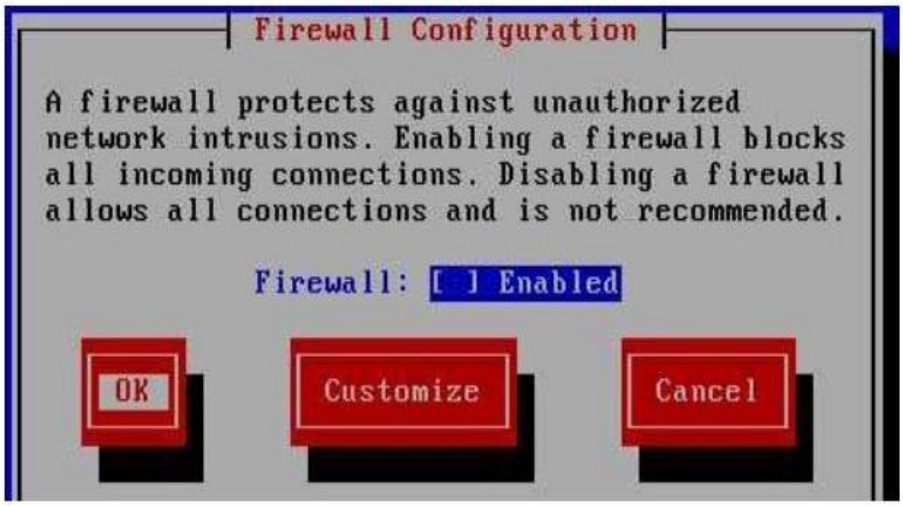
Run setup command

```
[root@server ~]# setup_
```

select Firewall configuration

Firewall is enabled by default

To disable the firewall unselect the enable.



Ignore the warning and select OK and press enter

Select Quit and press enter to save the configuration.

Configure telnet client in RHEL

Step 1: Installation of Packages

1. Login using root account. Necessary rpm for telnet server is xi

   # rpm –ivh xinetd-2.3.14-31.e16.X86_64

   # rpm –ivh telnet-

2. To check whether the package is installed on the system.

```
[root@linuxclient ~]# rpm -qa telnet
telnet-0.17-46.el6.x86_64
[root@linuxclient ~]# rpm -qa xinetd
xinetd-2.3.14-31.el6.x86_64
[root@linuxclient ~]# _
```

check telnet service status on it if it is set to off

```
[root@linuxclient ~]# chkconfig --list telnet
telnet          off
[root@linuxclient ~]# chkconfig telnet on
[root@linuxclient ~]# chkconfig --list telnet
telnet          on
[root@linuxclient ~]# _
```

Step 2: Edit configuration files:

open configuration file of telnet

```
[root@linuxclient ~]# vi /etc/xinetd.d/telnet
```

check telnet service is enabled make sure that **disable = yes** is changed to **disable = no**

```
# default: on
# description: The telnet server serves telnet
#       unencrypted username/password pairs for
service telnet
{
        disable = no
        flags           = REUSE
        socket_type     = stream
        wait            = no
        user            = root
        server          = /usr/sbin/in.telnetd
        log_on_failure  += USERID
}
```

Step 3: Restart the xinetd service

```
[root@linuxclient ~]# service xinetd restart
Stopping xinetd:                                           [  OK  ]
Starting xinetd:                                           [  OK  ]
[root@linuxclient ~]# _
```

Step 4: Check connectivity with server

```
[root@linuxclient ~]# ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=8.86 ms
^C
--- 192.168.1.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 761ms
rtt min/avg/max/mdev = 8.860/8.860/8.860/0.000 ms
[root@linuxclient ~]# _
```

We are getting reply of ping from server so we have connectivity with server .connect with telnet server. root user is not allowed to login from telnet. We need to create a normal user account.

```
[root@server ~]# ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:0C:29:6F:D9:13
          inet addr:192.168.1.1  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe6f:d913/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:25 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:4409 (4.3 KiB)

[root@server ~]# telnet 192.168.1.1
Trying 192.168.1.1...
Connected to 192.168.1.1.
Escape character is '^]'.
Red Hat Enterprise Linux Server release 6.1 (Santiago)
Kernel 2.6.32-131.0.15.el6.x86_64 on an x86_64
login: testuser
Password:
[testuser@server ~]$ _
```

We have successfully connected with Telnet server. To terminate telnet session logout from test user. We have successfully configured Telnet client on RHEL 6.

To terminate telnet session logout from logged in user.

```
[root@server ~]# telnet 192.168.1.1
Trying 192.168.1.1...
Connected to 192.168.1.1.
Escape character is '^]'.
Red Hat Enterprise Linux Server release 6.1 (Santiago)
Kernel 2.6.32-131.0.15.el6.x86_64 on an x86_64
login: testuser
Password:
[testuser@server ~]$ exit
logout
Connection closed by foreign host.
[root@server ~]# _
```

Conclusion –

Telnet is an application protocol used on the Internet or local area networks to provide a bidirectional interactive text-oriented communication facility using a virtual terminal connection. However, telnet by default does not encrypt any data sent over the connection (including passwords), and so it is often feasible to eavesdrop on the communications and use the password later for malicious purposes