Shree Rahul Education Society's (Regd.)

SHREE L. R. TIWARI COLLEGE OF ENGINEERING

An Autonomous Institute Affiliated to University of Mumbai,

Approved by AICTE & DTE, Maharashtra State | NAAC Accredited, NBA Accredited Program | ISO 9001:2015 Certified | DTE Code No: 3423 | Recognized under Section 2(f) of the UGC Act 1956 | Minority Status (Hindi Linguistic)

DEPARTMENT OF COMPUTER ENGINEERING `

Computer Network Lab. (CML507)

Subject Code: CML507

Academic Year: 2025-26

Semester: V

Branch: Computer Engineering

Shree Rahul Education Society's (Regd.)

SHREE L. R. TIWARI COLLEGE OF ENGINEERING

An Autonomous Institute Affiliated to University of Mumbai,

Approved by AICTE & DTE, Maharashtra State | NAAC Accredited, NBA Accredited Program | ISO 9001:2015 Certified | DTE Code No: 3423 | Recognized under Section 2(f) of the UGC Act 1956 | Minority Status (Hindi Linguistic)

DEPARTMENT OF COMPUTER ENGINEERING

A Laboratory Journal for Computer Network Lab. (CML507)

ACADEMIC YEAR: 2025-2026

Course Name: Computer Network Lab. **Course Code:** CML507

Name: _____

Semester: V (Fifth) **Roll No. :** _____

DEPARTMENT OF COMPUTER ENGINEERING

VISION AND MISSION

Institution's

Vision	To be a world class institute and a front runner in educational and socioeconomic development of the nation by providing high quality technical education to students from all sections of society.
Mission	To provide superior learning experiences in a caring and conducive environment so as to empower students to be successful in life & contribute positively to society.
Quality Policy	We, at SHREE L. R. TIWARI COLLEGE OF ENGINEERING, shall dedicate and strive hard to continuously achieve academic excellence in the field of Engineering and to produce the most competent Engineers through objective & innovative teaching methods, consistent updating of facilities, welfare & quality improvement of the faculty & a system of continual process improvement.

Computer Engineering Department's

Vision	To be a department of high repute focused on quality education, training and skill development in the field of computer engineering to prepare professionals and entrepreneurs of high caliber with human values to serve our nation and globe.
Mission	**M1:** To provide fertile academic environment for the development of skilled professionals and empowered with knowledge, skills, values, and confidence to take the leadership role and to bridge the gap between industry institute and society in the field of Computer engineering. **M2:** To promote caring and interactive teaching practices in a rejoicing learning ambience with richly supported modern educational tools and techniques. **M3:** To enhance and revitalize research culture to provide practical exposure and to establish synergy between teaching and research and make it an enabler for speedy progress. **M4:** To pursue intensification of soft skills and personality development through interplay of achievers of all segments of our society. **M5:** To provide human values to students by promoting lifelong learning ability.
Program Educational Objectives	PEO1. To equip graduates with a strong foundation in mathematics, science, and core engineering principles, enabling them to analyze, design, and implement innovative computing solutions. PEO2. To develop professionals capable of excelling in multidisciplinary teams by applying their computer engineering expertise to overcome complex technical challenges in global, societal, and environmental contexts. PEO3. To empower graduates with ethics, leadership, and an innovative mindset to grow with technology and support the progress of industry and the community. PEO4. To foster a commitment to continuous learning and professional excellence through research, self-learning, and the effective use of modern computing tools in their careers.

Student's Signature

Shree Rahul Education Society's (Regd.)

SHREE L. R. TIWARI COLLEGE OF ENGINEERING

An Autonomous Institute Affiliated to University of Mumbai,

Approved by AICTE & DTE, Maharashtra State | NAAC Accredited, NBA Accredited Program | ISO 9001:2015 Certified | DTE Code No: 3423 | Recognized under Section 2(f) of the UGC Act 1956 | Minority Status (Hindi Linguistic)

DEPARTMENT OF COMPUTER ENGINEERING

Certificate

This is to certify that Mr. /Ms._____

Class_____ Roll No. _____ Exam Seat No. _____ of ***Fifth Semester of Degree in Computer Engineering*** *has completed the required number of Practical's / Term Work / Session in the subject* ***Computer Network Lab*** *from the* ***Department of Computer Engineering*** *during the academic year of* ***2025 -2026*** *as prescribed in the curriculum.*

Course in-Charge

Head of the Department

Date:

Seal of Institution

INSTRUCTION FOR STUDENTS

Students shall read the points given below for understanding the theoretical concepts and practical applications.

1) Listen carefully to the lecture given by teacher about importance of subject, curriculum philosophy learning structure, skills to be developed, information about equipment, instruments, procedure, method of continuous assessment, tentative plan of work in laboratory and total amount of work to be done in a semester.
2) Student shall undergo study visit of the laboratory for types of equipment, instruments, software to be used, before performing experiments.
3) Read the write up of each experiment to be performed, a day in advance.
4) Organize the work in the group and make a record of all observations.
5) Understand the purpose of experiment and its practical implications.
6) Write the answers of the questions allotted by the teacher during practical hours if possible or afterwards, but immediately.
7) Student should not hesitate to ask any difficulty faced during conduct of practical/exercise.
8) The student shall study all the questions given in the laboratory manual and practice to write the answers to these questions.
9) Student shall develop maintenance skills as expected by the industries.
10) Student should develop the habit of pocket discussion/group discussion related to the experiments/exercises so that exchanges of knowledge/skills could take place.
11) Student shall attempt to develop related hands-on-skills and gain confidence.
12) Student shall focus on development of skills rather than theoretical or codified knowledge.
13) Student shall visit the nearby workshops, workstation, industries, laboratories, technical exhibitions, trade fair etc. even not included in the Lab manual. In short, students should have exposure to the area of work right in the student hood.
14) Student shall insist for the completion of recommended laboratory work, industrial visits, answers to the given questions, etc.
15) Student shall develop the habit of evolving more ideas, innovations, skills etc. those included in the scope of the manual.
16) Student shall refer technical magazines, proceedings of the seminars, refer websites related to the scope of the subjects and update his knowledge and skills.
17) Student should develop the habit of not to depend totally on teachers but to develop self-learning techniques.
18) Student should develop the habit to react with the teacher without hesitation with respect to the academics involved.
19) Student should develop habit to submit the practical's, exercise continuously and progressively on the scheduled dates and should get the assessment done.
20) Student should be well prepared while submitting the write up of the exercise. This will develop the continuity of the studies and he/she will not be over loaded at the end of the term.

Student Signature

GUIDELINES FOR TEACHERS

Teachers shall discuss the following points with students before start of practical's of the subject.

1) Learning Overview: To develop better understanding of importance of the subject. To know related skills to be developed such as Intellectual skills and Motor skills.
2) Learning Structure: In this, topic and sub topics are organized in systematic way so that ultimate purpose of learning the subject is achieved. This is arranged in the form of fact, concept, principle, procedure, application and problem.
3) Know you're Laboratory Work: To understand the layout of laboratory, specifications of equipment/Instruments/Materials, procedure, working in groups, planning time etc. Also to know total amount of work to be done in the laboratory.
4) Teaching shall ensure that required equipment's are in working condition before start of experiment, also keep operating instruction manual available.
5) Explain prior concepts to the students before starting of each experiment.
6) Involve students' activity at the time of conduct of each experiment.
7) While taking reading/observation each student shall be given a chance to perform or observe the experiment.
8) If the experimental set up has variations in the specifications of the equipment, the teachers are advised to make the necessary changes, wherever needed.
9) Teacher shall assess the performance of students continuously as per norms prescribed by university of Mumbai and guidelines provided by IQAC.
10) Teacher should ensure that the respective skills and competencies are developed in the students after the completion of the practical exercise.
11) Teacher is expected to share the skills and competencies are developed in the students.
12) Teacher may provide additional knowledge and skills to the students even though not covered in the manual but are expected from the students by the industries.
13) Teachers shall ensure that industrial visits if recommended in the manual are covered.
14) Teacher may suggest the students to refer additional related literature of the Technical papers/Reference books/Seminar proceedings, etc.
15) During assessment teacher is expected to ask questions to the students to tap their achievements regarding related knowledge and skills so that students can prepare while submitting record of the practical's. Focus should be given on development of enlisted skills rather than theoretical /codified knowledge.
16) Teacher should enlist the skills to be developed in the students that are expected by the industry.
17) Teacher should organize Group discussions /brain storming sessions / Seminars to facilitate the exchange of knowledge amongst the students.
18) Teacher should ensure that revised assessment norms are followed simultaneously and progressively.
19) Teacher should give more focus on hands on skills and should actually share the same.
20) Teacher shall also refer to the circulars related to practical's supervise and assessment for additional guidelines.

Subject In-charge Signature

DEPARTMENT OF COMPUTER ENGINEERING

RECORD OF PROGRESSIVE ASSESSMENTS

Student Name: _____ **Roll No.: _____(TE CS SEM.-V)**
Course Name : Computer Network Lab. **Course Code: CML507**

Assessment of Experiments (A)

Sr. no.	Name of Experiments	Page No.	Date of Performance	Date of Submission	Assessment (out of 15)	Teacher's Signature and Remark	CO Covered
1	Study of RJ45 and CAT6 Cabling and connection using crimping tool.						CO1
2	Use basic networking commands in Linux (ping, tracert, nslookup, netstat, ARP, RARP, ip, ifconfig, dig, route						CO1
3	Use Wire shark to understand the operation of TCP/IP layers						CO2
4	Perform network discovery using discovery tools (eg. Nmap, mrtg)						CO2
5	Build a simple network topology and configure it for static routing protocol using packet tracer. Setup a network and configure IP addressing, sub netting, masking						CO2
6	Study and Installation of Network Simulator (NS3)						CO2
7	Socket programming using TCP or UDP						
8	Design VPN and Configure RIP/OSPF using Packet tracer						CO2
9	Perform File Transfer and Access using FTP						CO2
10	Perform Remote login using Telnet server						CO3
Average Marks (Out of 15)							

Assessment of Assignment (B)

Assignment No.	Page No.	Date of Performance	Date of Submission	Assessment (out of 18)	Teacher's Signature and Remark	CO Covered
Assignment No.1						CO1,CO2,CO3 CO4,CO5,CO6
Assignment No.2						
Converted Marks (Out of 5) (B)						

Assessments of Attendance (C)

CN Theory Attendance			CNL Practical Attendance			AVG. Attendance % (TH+PR)	Attendance Marks (D) (Out of 5)
TH (out of)	TH attend.	TH %	PR (out of)	PR Attend.	PR %		

Total Term Work Marks: A+B+C = _____ (Out of 25)

Student Signature

Subject In-charge

DEPARTMENT OF COMPUTER ENGINEERING

Program Outcome (POs & PSOs)

Program Outcomes are the skills and knowledge which the students have at the time of graduation. This will indicate what student can do from subject-wise knowledge acquired during the program .

PO	Graduate Attributes	Description of the Program outcome as defined by the NBA
PO-1	Engineering knowledge	Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.
PO-2	Problem analysis	Identify, formulate, review research literature, and analyses complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.
PO-3	Design/development of solutions	Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.
PO-4	Conduct investigations of complex problems	Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.
PO-5	Modern tool usage	Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modelling to complex engineering activities with an understanding of the limitations.
PO-6	The engineer and society	Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice.
PO-7	Environment and sustainability	Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.
PO-8	Ethics	Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.
PO-9	Individual and team work	Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.
PO-10	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.
PO-11	Project management and finance	Demonstrate knowledge and understanding of the 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.
PO-12	Life-long learning	Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.
Program Specific Outcomes (PSOs) defined by the programme. Baseline-Rational Unified Process(RUP)		
PSO-1	Computing solution to solve real life problem	The graduate must be able to develop, deploy, test and maintain the software or computing hardware solutions to solve real life problems using state of the art technologies, standards, tools and programming paradigms.
PSO-2	Computer Engineering knowledge and skills	The graduate should be able to adapt Computer Engineering knowledge and skills to create career paths in industries or business organizations or institutes of repute.

Student's Signature

DEPARTMENT OF COMPUTER ENGINEERING

Course Objectives and Outcomes

Academic Year: 2025-2026 **Class:** TE **Course Code:** CML507
Program: Computer Engineering **Div:** - **Course Name:** Computer Network.
Department: Computer Engineering **Sem.:** V

Course Objectives:

Sr. No.	Statement
1	To introduce concepts and fundamentals of data communication and computer networks.
2	To explore the inter-working of various layers of OSI.
3	To explore the issues and challenges of protocols design while delving into TCP/IP protocol suite.
4	To assess the strengths and weaknesses of various routing algorithms.
5	To understand various transport layer and application layer protocols.

Course Outcomes:

CO's No.	Abbre.	Statement
CML507.1	CO1	Demonstrate the concepts of data communication at physical layer and compare ISO - OSI model with TCP/IP model
CML507.2	CO2	Explore different design issues at data link layer.
CML507.3	CO3	Design the network using IP addressing and sub netting / super netting schemes.
CML507.4	CO4	Analyze transport layer protocols and congestion control algorithms
CML507.5	CO5	Explore protocols at application layer

Course Prerequisite:

Sr. No.	Pre-requisite
1	Knowledge of Algorithm
2	Knowledge of basic Numbering structure.

Teaching and Examination Scheme:

Teaching Scheme (Hrs)			Credits Assigned				Examination Scheme								
Theory	Pract	Tut	Theory	TW/ Pract	Tut	Total	Theory					TW	Oral	Oral & Pract	Total
							Internal Assessment			End Sem. Exam	Exam Duration (in Hrs)				
							Test 1	Test 2	Avg.						
3	2	-	-	1	-	-	20	20	20	80	3	25	25	25	175

Term Work (Total 25 Marks) = (Experiments: 15 mark + Assignment 5 Marks + Attendance: 05 marks (TH+PR)).

Shree Rahul Education Society's (Regd.)

SHREE L. R. TIWARI COLLEGE OF ENGINEERING

An Autonomous Institute Affiliated to University of Mumbai,

Approved by AICTE & DTE, Maharashtra State | NAAC Accredited, NBA Accredited Program | ISO 9001:2015 Certified | DTE Code No: 3423 | Recognized under Section 2(f) of the UGC Act 1956 | Minority Status (Hindi Linguistic)

DEPARTMENT OF COMPUTER ENGINEERING

Course Exit Form

Student Name: _____ **Roll No.:** _____

Class/Semester: TE CS SEM.-V **Academic Year: 2025-2026**

Course Name: Computer Network **Course Code: CML507**

Judge your ability with regard to the following points by putting a **(√),** on the scale of **1 (lowest) to 5 (highest),** based on the knowledge and skills you attained from this course.

Sr. No.	Your ability to	1 Lowest	2	3	4	5 Highest
1	**CSC503.1:** Demonstrate the concepts of data communication at physical layer and compare ISO - OSI model with TCP/IP model					
2	**CSC503.2:** Explore different design issues at data link layer.					
3	**CSC503.3:** Design the network using IP addressing and sub netting / super netting schemes					
4	**CSC503.4:**. Analyse transport layer protocols and congestion control algorithms					
5	**CSC503.5:** Explore protocols at application layer					

_____ _____

Student's Signature **Date**

Experiment No 1

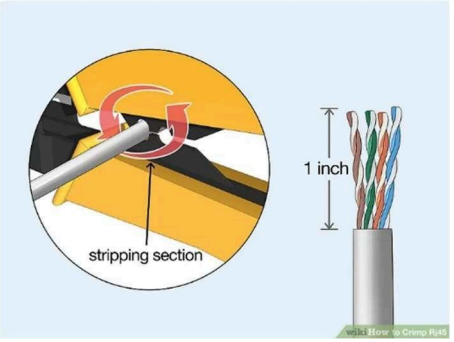
Title: Study of RJ45 and CAT6 Cabling and connection using crimping tools.

Aim: To crimp CAT6 cable and fix RJ45 connector.

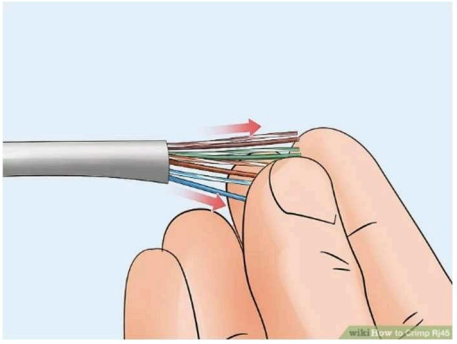
Theory:

Steps of Crimping:

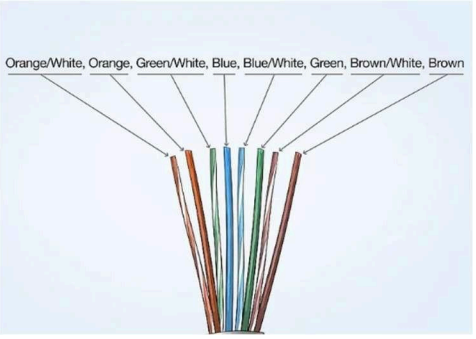
1. Strip the cable back 1 inch (25 mm) from the end. Insert the cable into the stripper section of the tool and squeeze it tight. Then, rotate the crimping tool around the cable in a smooth and even motion to create a clean cut. Keep the tool clamped and pull away towards the end of the wire to remove the sheathing. The stripping section is a round hole near the handle of the tool. The sheathing should come off cleanly, leaving the wires exposed.



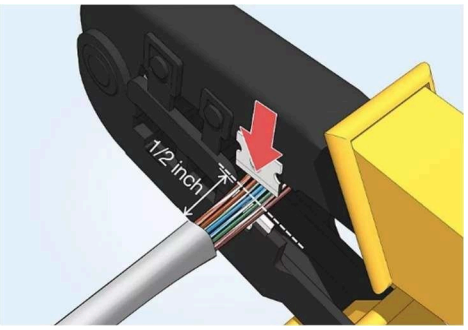
2. Untwist and straighten the wires inside of the cable. Inside of the cable you'll see a bunch of smaller wires twisted together. Separate the twisted wires and straighten them out so they're easier to sort into the right order. Cut off the small plastic wire separator or core so it's out of the way. Don't cut off or remove any of the wires or you won't be able to crimp them into the connector.



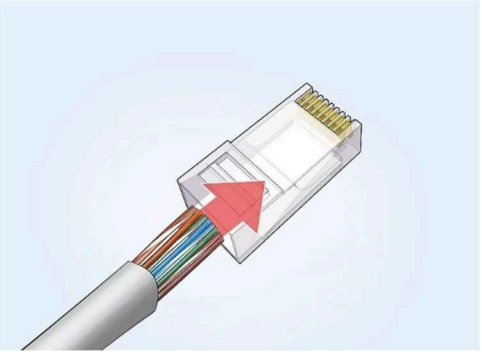
3. Arrange the wires into the right order. Use your fingers to put the wires in the correct order so they can be properly crimped. The proper sequence is as follows from left to right: Orange/White, Orange, Green/White, Blue, Blue/White, Green, Brown/White, Brown. There are 8 wires in total that need to be arranged in the right sequence. Note that the wires labeled Orange/White or Brown/White indicate the small wires that have 2 colors.



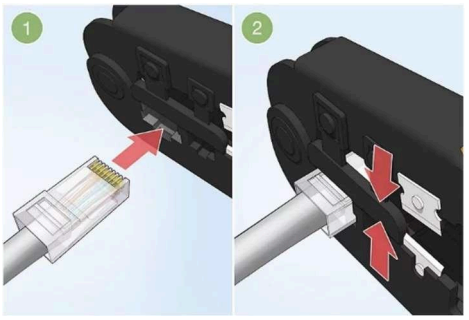
4. Cut the wires into an even line 1Ú2 inch (13 mm) from sheathing. Hold the wires with your thumb and index finger to keep them in order. Then, use the cutting section of the crimping tool to cut them into an even line. The cutting section of the tool will resemble wire cutters. The wires must be in an even line to be crimped into the RJ-45 connector properly. If you cut them in an uneven line, move further down the wires and cut them again.



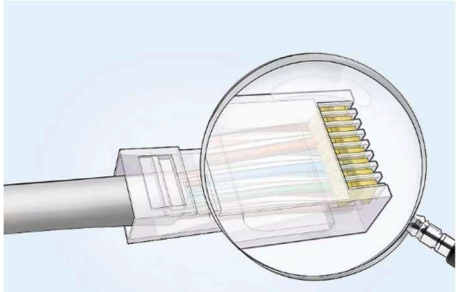
5. Insert the wires into the RJ-45 connector. Hold the RJ-45 connector so the clip is on the underside and the small metal pins are facing up. Insert the cable into the connector so that each of the small wires fits into the small grooves in the connector. The sheathing of the cable should fit just inside of the connector so it's past the base. If any of the small wires bend or don't fit into a groove correctly, take the cable out and straighten the wires with your fingers before trying again. The wires must be inserted in the correct order and each wire must fit into a groove before you crimp the connector.



6. Stick the connector into the crimping part of the tool and squeeze twice. Insert the connector in the crimping section of the tool until it can't fit any further. Squeeze the handles to crimp the connector and secure the wires. Release the handles, then squeeze the tool again to make sure all of the pins are pushed down. The crimping tool pushes small pins in the grooves down onto the wires to hold and connect them to the RJ-45 connector.



7. Remove the cable from the tool and check that all of the pins are down. Take the connector out of the tool and look at the pins to see that they're all pushed down in an even line. Lightly tug at the connector to make sure it's



attached to the cable. If any of the pins aren't pushed down, put the wire back into the crimping tool and crimp it again.

Crimping Tools:

1. Crimper:

2. Cable Stripper:

3. RJ45 Connector:

4. Cable Tester:

5..UTP Cable:

CAT specification:

Category	Standard Bandwidth	Max Data Rate	Shielding
Cat5e	100MHz (up to 350)	1000Mbps	UTP or STP
Cat6	250MHz (up to 550)	1000Mbps	UTP or STP
Cat6A	500MHz (up to 550)	10Gbps	UTP or STP
Cat7	600MHz	10Gbps	Shielded only
Cat8	2000MHz	25Gbps or 40Gbps	Shielded only

RJ connector specification:

Connector/Cable	Pinning
RJ-11 straight (4-wire)	Y (1-1), G (2-2), R (3-3), BL (4-4)
RJ-11 crossed (4-wire)	Y (1-4), G (2-3), R (3-2), BL (4-1)
RJ-11 straight (6-wire)	BL (1-1), Y (2-2), G (3-3), R (4-4), BK (5-5), W (6-6)
RJ-11 crossed (6-wire)	BL (1-6), Y (2-5), G (3-4), R (4-3), BK (5-2), W (6-1)
RJ-45 straight (8-wire)	BL (1-1), OR (2-2), BK (3-3), R (4-4), G (5-5), Y (6-6), BN (7-7), S (8-8)
RJ-45 USOC crossed (8-wire)	BL (1-8), OR (2-7), BK (3-6), R (4-5), G (5-4), Y (6-3), BN (7-2), S (8-1)
RJ-45 568A/B crossed (8-wire)	BL (1-3), OR (2-6), BK (3-1), R (4-5), G (5-4), Y (6-2), BN (7-8), S (8-7)
RJ-48C straight (8-wire)	OR/W (1-1), W/OR (2-2), (3-3) unused, BL/W (4-4), W/BL (5-5), (6-6) unused, BL drain (7-7), OR drain (8-8)
RJ-48C crossed (8-wire)	OR/W (1-4), W/OR (2-5), (3-3) unused, BL/W (4-1), W/BL (5-2), (6-6) unused, BL drain (7-7), OR drain (8-8)

Crossover cable combination:

WOrange	Orange	WGreen	Blue	WBlue	Green	WBrown	Brown
1	2	3	4	5	6	7	8
WGreen	Green	WOrange	Blue	WBlue	Orange	WBrown	Brown
3	6	1	4	5	2	7	8

Conclusion: Hence We have done Crimping of Ethernet wire Successfully.

Experiment No 2

Title: Use basic networking commands in Linux/windows.

Aim: To Learn and use basic networking commands (ping, tracert, nslookup, netstat, ARP, RARP, ip, ifconfig, dig, route)

Theory:

1. **Ping**

- The ping command is used to test connectivity between two hosts.
- It sends ICMP echo request messages to the destination.
- The destination host replies with ICMP reply messages.
- If the ping command gets a reply from the destination host, it
- displays the reply along with

round-trip times. The ping command uses the

following syntax.

ping destination host IP or name

The following command tests connectivity between the host computer and Google's server.

ping google.com

The following image shows the output of this command.

```
C:\Users\Admin>ping google.com

Pinging google.com [142.250.67.238] with 32 bytes of data:
Reply from 142.250.67.238: bytes=32 time=2ms TTL=119
Reply from 142.250.67.238: bytes=32 time=2ms TTL=119
Reply from 142.250.67.238: bytes=32 time=2ms TTL=119
Reply from 142.250.67.238: bytes=32 time=2ms TTL=119

Ping statistics for 142.250.67.238:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 2ms, Average = 2ms
```

2. Ipconfig

- This command displays all current TCP/IP network configuration values and refreshes Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) settings.

- This command is mainly used to view the IP addresses on the computers that are configured to obtain their IP address automatically

The following table lists some important options of the **ipconfig** command

Used without parameters	Displays the IP address, subnet mask, and default gateway for all adapters
/all	Displays the full TCP/IP configuration for all adapters.
/renew [Adapter]	Renews DHCP configuration for all adapters (if an adapter is not specified) or for a specific adapter if the Adapter parameter is included
/release [Adapter]	Sends a DHCPRELEASE message to the DHCP server to release the current DHCP configuration and discard the IP address configuration for either all adapters (if an adapter is not specified) or for a specific adapter if the Adapter parameter is included
/flushdns	Flushes and resets the contents of the DNS client resolver cache.

The following image shows the sample output of this command.

```
C:\Users\Admin>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::26d5:e37e:f865:4ab7%7
   IPv4 Address. . . . . . . . . . . : 192.168.3.108
   Subnet Mask . . . . . . . . . . . : 255.255.248.0
   Default Gateway . . . . . . . . . : fe80::928d:78ff:fef2:9c67%7
                                       192.168.0.1

Ethernet adapter vEthernet (Default Switch):

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::a310:6c34:559c:1315%26
   IPv4 Address. . . . . . . . . . . : 172.30.128.1
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . :

C:\Users\Admin>ipconfig/all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : 307-PC6
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
```

```
C:\Users\Admin>ipconfig/all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : 307-PC6
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek PCIe GbE Family Controller
   Physical Address. . . . . . . . . : 44-8A-5B-DF-6B-E3
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::26d5:e37e:f865:4ab7%7(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.3.108(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.248.0
   Default Gateway . . . . . . . . . : fe80::928d:78ff:fef2:9c67%7
                                       192.168.0.1
   DHCPv6 IAID . . . . . . . . . . . : 390367835
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-27-84-86-65-00-E0-4C-E1-22-0A
   DNS Servers . . . . . . . . . . . : 192.168.0.1
                                       8.8.8.8
   NetBIOS over Tcpip. . . . . . . . : Enabled

Ethernet adapter vEthernet (Default Switch):

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Hyper-V Virtual Ethernet Adapter
   Physical Address. . . . . . . . . : 00-15-5D-3D-CE-6E
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::a310:6c34:559c:1315%26(Preferred)
   IPv4 Address. . . . . . . . . . . : 172.30.128.1(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . :
   DHCPv6 IAID . . . . . . . . . . . : 436213085
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-27-84-86-65-00-E0-4C-E1-22-0A
   DNS Servers . . . . . . . . . . . : fec0:0:0:ffff::1%1
```

3.Tracert

- This command is used to diagnose path-related problems.
- On an IP network, routers exchange IP packets between the source and the destination.
- They take IP packets from the source host and forward them in a sequence until they reach the destination host.
- The sequence of routers between the source and destination is known as the path.
- A path consists of all routers in a sequence that IP packets sent from the source host traverse to reach the destination host.
- The tracert command prints the path.
- If all routers on the path are functional, this command prints the full path.
- If a router is down on the path, this command prints the path up to the last operational router.

The tracert command uses the following syntax.

tracert Destination Name or IP address

The following command traces the path to the host named www.google.co.in.

tracert www.google.co.in

The following table lists some important options of the **tracert** command.

Option	Description
-d	Do not resolve the IP addresses of intermediate routers to their names.
-h	Specifies the maximum number of hops (routers) to search on the path. The default is 30 hops.
-w	Specifies the amount of time in milliseconds to wait for a reply message from the router. If not received within the time-out, an asterisk (*) is displayed. The default time-out is 4000 (4 seconds).

The following image shows the output of this command.

```
C:\Users\Admin>tracert www.google.co.in

Tracing route to www.google.co.in [142.251.42.3]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  192.168.0.1
  2    19 ms    11 ms     1 ms  103.172.87.177
  3     *        *        *     Request timed out.
  4     2 ms     2 ms     1 ms  142.250.167.25
  5    14 ms     4 ms     3 ms  72.14.239.103
  6     1 ms     2 ms     2 ms  209.85.250.139
  7     2 ms     1 ms     2 ms  bom12s19-in-f3.1e100.net [142.251.42.3]

Trace complete.
```

2. **NetStat**

- NetStat is a networking utility that can be used to display all active network connections and their status. It can be used to identify which applications are using which ports and can be helpful in troubleshooting networking issues.
- Most Windows, Linux, UNIX, and other operating systems include Netstat as a Common TCP – IP networking command-line method.
- To use the NetStat command, open the Command Prompt and type "netstat" followed by any desired options.

netstat –f

Option	Description
-a	Displays all connection and ports
-b	Displays the executable involved in each connection or hearing port
-e	This will combine with the -sand display the ethernet statistics
-n	Displays the address and the port number in the form of numerical
-o	Displays the ID of each connection for the ownership process.
-r	Displays the routing table
-v	When used in combination with -b, the link or hearing port sequence for every executable is shown.

```
C:\Users\Admin>netstat -f

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    192.168.3.108:7680     192.168.5.97:2007      TIME_WAIT
  TCP    192.168.3.108:7680     192.168.5.97:2028      TIME_WAIT
  TCP    192.168.3.108:7680     madhurig-pc:50671      TIME_WAIT
  TCP    192.168.3.108:52070    bom12s20-in-f14.1e100.net:https  ESTABLISHED
  TCP    192.168.3.108:52072    bom07s24-in-f3.1e100.net:https  ESTABLISHED
  TCP    192.168.3.108:52075    bom12s19-in-f10.1e100.net:https  ESTABLISHED
  TCP    192.168.3.108:52076    bom12s19-in-f10.1e100.net:https  ESTABLISHED
  TCP    192.168.3.108:56050    20.198.119.143:https   ESTABLISHED
  TCP    192.168.3.108:56197    bom07s32-in-f14.1e100.net:https  ESTABLISHED
  TCP    192.168.3.108:56206    sb-in-f188.1e100.net:5228  ESTABLISHED
  TCP    192.168.3.108:56221    bom05s15-in-f3.1e100.net:https  ESTABLISHED
  TCP    192.168.3.108:56712    a23-212-161-101.deploy.static.akamaitechnologies.com:https  CLOSE_WAIT
  TCP    192.168.3.108:57004    bom07s16-in-f14.1e100.net:https  ESTABLISHED
  TCP    192.168.3.108:57148    dns.google:https       ESTABLISHED
  TCP    192.168.3.108:59363    bom07s31-in-f3.1e100.net:https  TIME_WAIT
  TCP    192.168.3.108:59428    a23-212-252-25.deploy.static.akamaitechnologies.com:https  CLOSE_WAIT
  TCP    192.168.3.108:59429    a23-212-254-41.deploy.static.akamaitechnologies.com:https  CLOSE_WAIT
  TCP    192.168.3.108:59430    103.157.178.209:https  CLOSE_WAIT
  TCP    192.168.3.108:59432    dns.google:https       TIME_WAIT
  TCP    192.168.3.108:59450    bom12s13-in-f5.1e100.net:https  ESTABLISHED
  TCP    192.168.3.108:59454    bom12s04-in-f10.1e100.net:https  TIME_WAIT
  TCP    192.168.3.108:59455    bom07s16-in-f3.1e100.net:https  TIME_WAIT
  TCP    192.168.3.108:59457    bom07s37-in-f10.1e100.net:https  TIME_WAIT
  TCP    192.168.3.108:59462    e2a.google.com:https   TIME_WAIT
  TCP    192.168.3.108:59466    sd-in-f100.1e100.net:https  TIME_WAIT
  TCP    192.168.3.108:59471    bom07s35-in-f10.1e100.net:https  ESTABLISHED
  TCP    192.168.3.108:59472    bom07s18-in-f13.1e100.net:https  ESTABLISHED
  TCP    192.168.3.108:59488    25.224.186.35.bc.googleusercontent.com:https  TIME_WAIT
  TCP    [fe80::26d5:e37e:f865:4ab7%7]:56092  DESKTOP-AI28PPD:8391   ESTABLISHED
```

1. Nslookup
   - Nslookup is a command-line networking tool used for querying Domain Name System (DNS) to obtain domain name or IP address mapping, or other DNS records.
   - Nslookup has two modes: interactive and non-interactive.
   - The Windows version of Nslookup is available as part of the Microsoft networking tools.
   - To use Nslookup on Windows, open the Command Prompt and type "nslookup" followed by the domain name or IP address you want to query.

     Nslookup……

     For example, to find the IP address of www.example.com, you would type:
     nslookup www.example.com

     Nslookup can also be used to find the name of a machine with a given IP address. For example, to find the name of the machine with the IP address 10.0.0.1, you would type:

     nslookup 10.0.0.1

```
C:\Users\Admin>nslookup
DNS request timed out.
    timeout was 2 seconds.
Default Server:  UnKnown
Address:  192.168.0.1
```

2. Route
   - The Route networking command is one of the most essential networking commands for Windows administrators. This command can be used to view and modify the network routing table. The route command can also be used to add or remove static routes from the routing table.
   - Routing tables are used to direct packets from one subnet to another. By using the route command, administrators can change the way network traffic is routed. This can be useful for troubleshooting networking issues or for implementing security measures.
   - The Route networking command can be executed from the Command Prompt or from PowerShell.

To view the current routing table, use the following syntax:

route print

To add a static route to the network routing table, use the following syntax:

route add <destination> mask <subnet mask> <gateway>

To remove a static route from the networking routing table, use the following syntax:

route delete <destination>

```
C:\Users\Admin>route print
===========================================================================
Interface List
  7...44 8a 5b df 6b e3 ......Realtek PCIe GbE Family Controller
  1...........................Software Loopback Interface 1
 26...00 15 5d 3d ce 6e ......Hyper-V Virtual Ethernet Adapter
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.0.1    192.168.3.108    291
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
      172.30.128.0    255.255.240.0         On-link      172.30.128.1   5256
      172.30.128.1  255.255.255.255         On-link      172.30.128.1   5256
    172.30.143.255  255.255.255.255         On-link      172.30.128.1   5256
       192.168.0.0    255.255.248.0         On-link     192.168.3.108    291
     192.168.3.108  255.255.255.255         On-link     192.168.3.108    291
     192.168.7.255  255.255.255.255         On-link     192.168.3.108    291
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link      172.30.128.1   5256
        224.0.0.0        240.0.0.0         On-link     192.168.3.108    291
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link      172.30.128.1   5256
  255.255.255.255  255.255.255.255         On-link     192.168.3.108    291
===========================================================================
Persistent Routes:
  Network Address          Netmask  Gateway Address  Metric
          0.0.0.0          0.0.0.0      192.168.0.1  Default
===========================================================================

IPv6 Route Table
===========================================================================
Active Routes:
 If Metric Network Destination      Gateway
  7    291 ::/0                     fe80::928d:78ff:fef2:9c67
  1    331 ::1/128                  On-link
 26   5256 fe80::/64                On-link
  7    291 fe80::/64                On-link
  7    291 fe80::26d5:e37e:f865:4ab7/128
                                    On-link
 26   5256 fe80::a310:6c34:559c:1315/128
                                    On-link
  1    331 ff00::/8                 On-link
 26   5256 ff00::/8                 On-link
  7    291 ff00::/8                 On-link
===========================================================================
Persistent Routes:
  None
```

3. ARP
   - The Address Resolution Protocol, or ARP, is a networking utility used for mapping network addresses to physical addresses.
   - ARP is essential for networking communications, as it allows devices on a network to communicate with each other by translating IP addresses into physical addresses.
   - Although IP addresses are commonly used in network communications, packet delivery is ultimately determined by media access control (MAC). The mechanism for address resolution kicks in at this point.
   - If you’re having trouble communicating with a particular host, you can use the arp –a command to include the remote host IP address.
   - Address, Flags, Mask, IFace, Hardware Type, Hardware Address, and so on are all provided by the ARP command.

```
C:\Users\Admin>arp -a

Interface: 192.168.3.108 --- 0x7
  Internet Address      Physical Address      Type
  192.168.0.1           d4-76-a0-00-18-08     dynamic
  192.168.0.17          78-54-2e-5c-ce-7a     dynamic
  192.168.0.18          60-e3-27-f0-ee-54     dynamic
  192.168.0.103         d8-bb-c1-27-fa-b3     dynamic
  192.168.0.250         d8-bb-c1-27-fb-68     dynamic
  192.168.1.1           60-e3-27-f1-14-1c     dynamic
  192.168.1.55          00-e0-4d-3a-01-1d     dynamic
  192.168.3.5           60-e3-27-be-f9-c0     dynamic
  192.168.3.16          c0-c9-e3-b9-01-3c     dynamic
  192.168.3.20          90-8d-78-f2-9c-67     dynamic
  192.168.3.40          44-8a-5b-e4-5a-4c     dynamic
  192.168.3.46          44-8a-5b-df-6b-a3     dynamic
  192.168.3.72          44-8a-5b-df-6c-f8     dynamic
  192.168.3.196         d8-bb-c1-27-fa-73     dynamic
  192.168.4.4           b0-c5-54-de-22-ea     dynamic
  192.168.4.5           b0-c5-54-de-22-9c     dynamic
  192.168.4.17          98-da-c4-c7-af-5a     dynamic
  192.168.5.17          28-ee-52-b6-d4-d3     dynamic
  192.168.5.18          e4-c3-2a-84-c8-52     dynamic
  192.168.5.96          d8-bb-c1-27-f9-e5     dynamic
  192.168.5.97          d8-bb-c1-27-fa-64     dynamic
  192.168.5.102         d8-bb-c1-27-fa-7f     dynamic
  192.168.5.104         d8-bb-c1-27-fa-5e     dynamic
  192.168.5.105         d8-bb-c1-27-fa-89     dynamic
  192.168.5.107         d8-bb-c1-27-f9-c9     dynamic
  192.168.5.108         d8-bb-c1-27-fa-55     dynamic
  192.168.5.109         d8-bb-c1-27-f9-b9     dynamic
  192.168.5.111         d8-bb-c1-27-fa-72     dynamic
  192.168.5.118         d8-bb-c1-27-fa-58     dynamic
  192.168.5.177         0a-e0-af-c4-24-ce     dynamic
  192.168.7.7           d4-3d-7e-a9-aa-f8     dynamic
  192.168.7.21          00-e0-4c-36-00-4f     dynamic
  192.168.7.92          d4-3d-7e-c7-95-70     dynamic
  192.168.7.121         00-e0-4c-e1-22-0a     dynamic
  192.168.7.145         d8-bb-c1-27-fa-8b     dynamic
  192.168.7.186         d8-bb-c1-27-f9-cc     dynamic
  192.168.7.201         d8-cb-8a-67-bd-1e     dynamic
  192.168.7.219         d8-cb-8a-67-bd-d7     dynamic
  192.168.7.251         44-8a-5b-df-73-86     dynamic
  192.168.7.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

Interface: 172.30.128.1 --- 0x1a
  Internet Address      Physical Address      Type
  172.30.143.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

Conclusion:

We have learnt about how to Use basic networking commands in Linux /Windows.

Experiment No:3

TITLE: To study Wireshark.

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

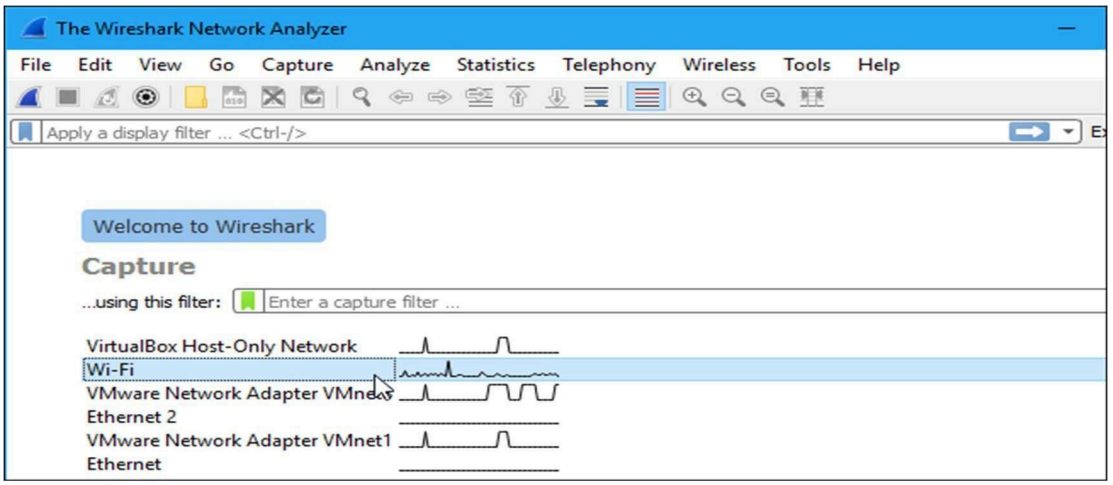
- Ethernet Layer: Frame header, Frame size etc.
- Data Link Layer: MAC address, ARP (IP and MAC address binding)
- Network Layer: IP Packet (header, fragmentation), ICMP (Query and Echo)
- Transport Layer: TCP Ports, TCP handshake segments etc.
- Application Layer: DHCP, FTP, HTTP header formats

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

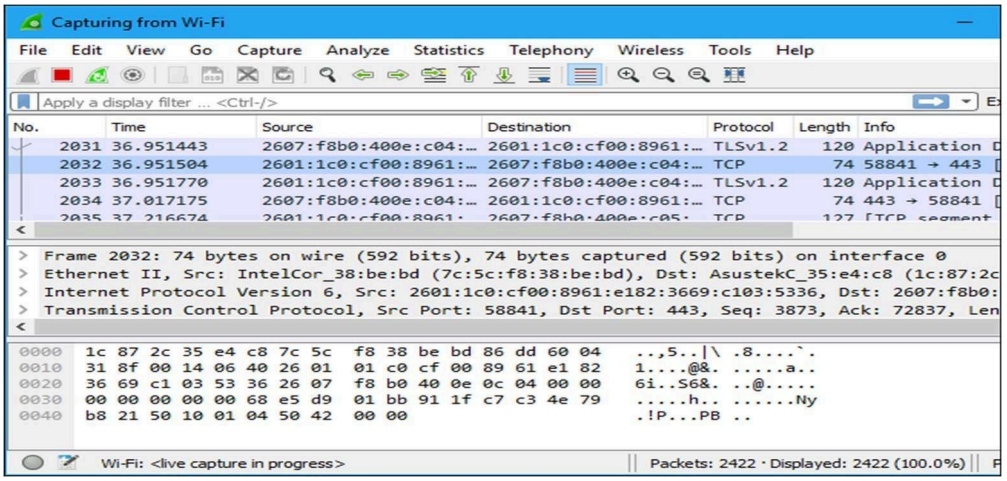
After downloading and installing Wireshark, you can launch it and double-click the name of a network interface under Capture to start capturing packets on that interface. For example, if you want to capture traffic on your wireless network, click your wireless interface. You can configure advanced features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



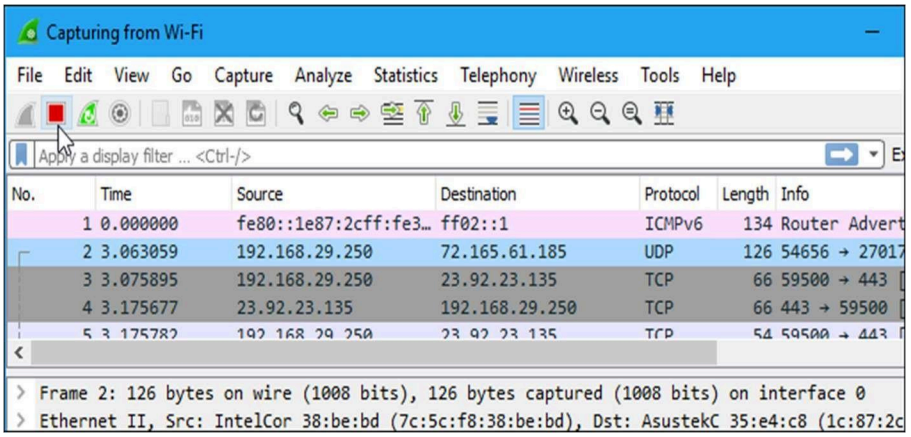
As soon as you click the interface's name, you'll see the packets start to appear in real time. Wireshark captures each packet sent to or from your system.

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.



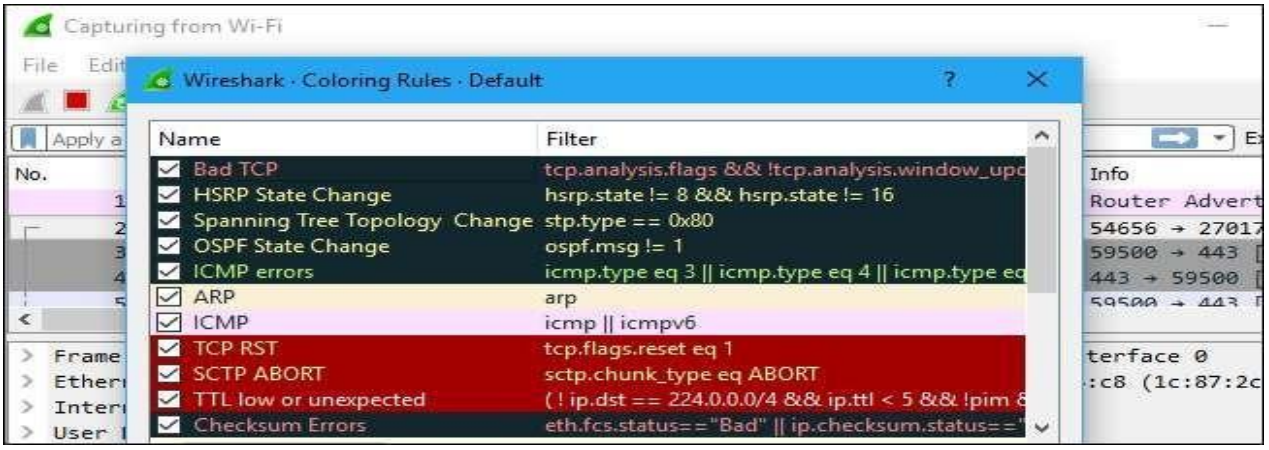
Click the red "Stop" button near the top left corner of the window when you want to stop capturing traffic.



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.

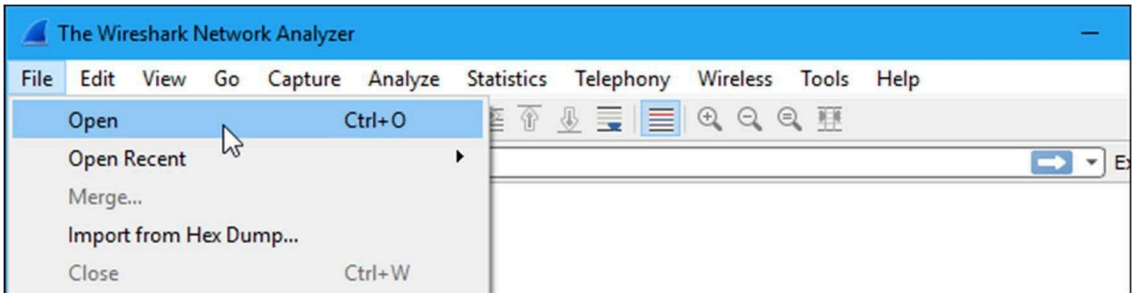
To view exactly what the color codes mean, click View > Coloring Rules. You can also customize and modify the coloring rules from here, if you like.



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.

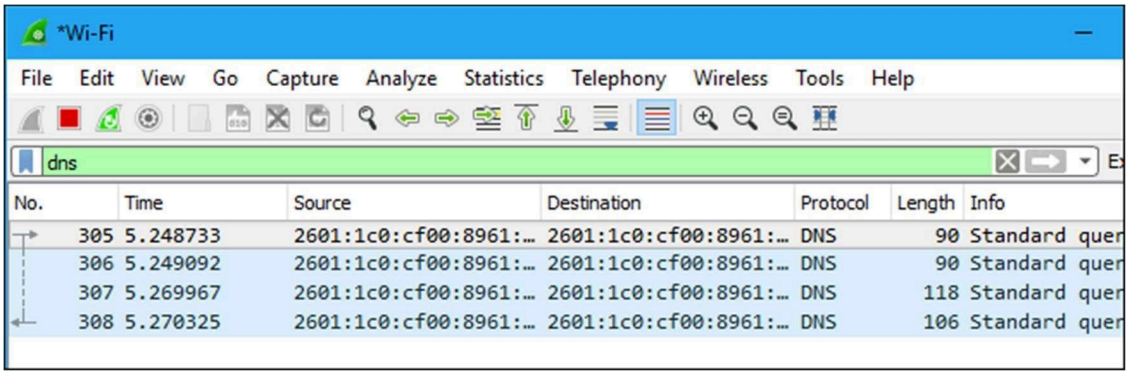
You can also save your own captures in Wireshark and open them later. Click File > Save to save your captured packets.



Filtering Packets

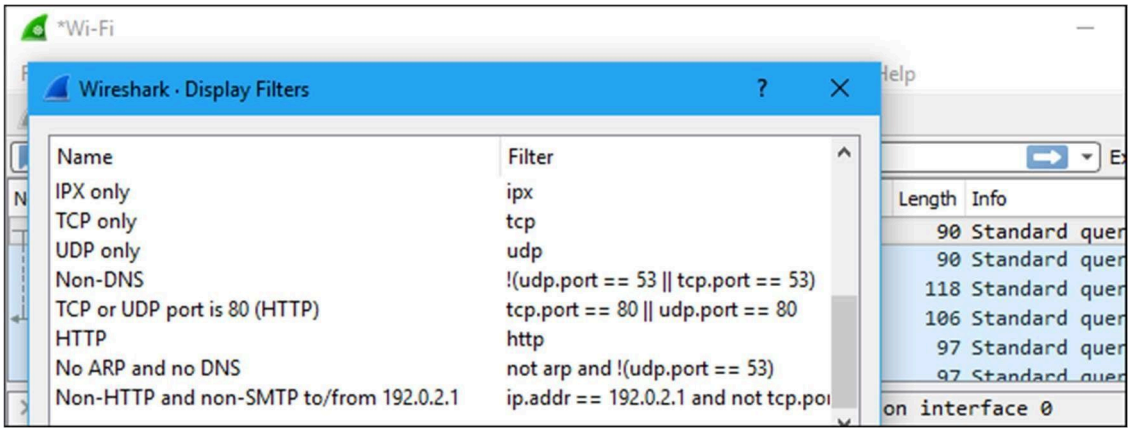
If you're trying to inspect something specific, such as the traffic a program sends when phoning home, it helps to close down all other applications using the network so you can narrow down the traffic. Still, you'll likely have a large amount of packets to sift through. That's where Wireshark's filters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



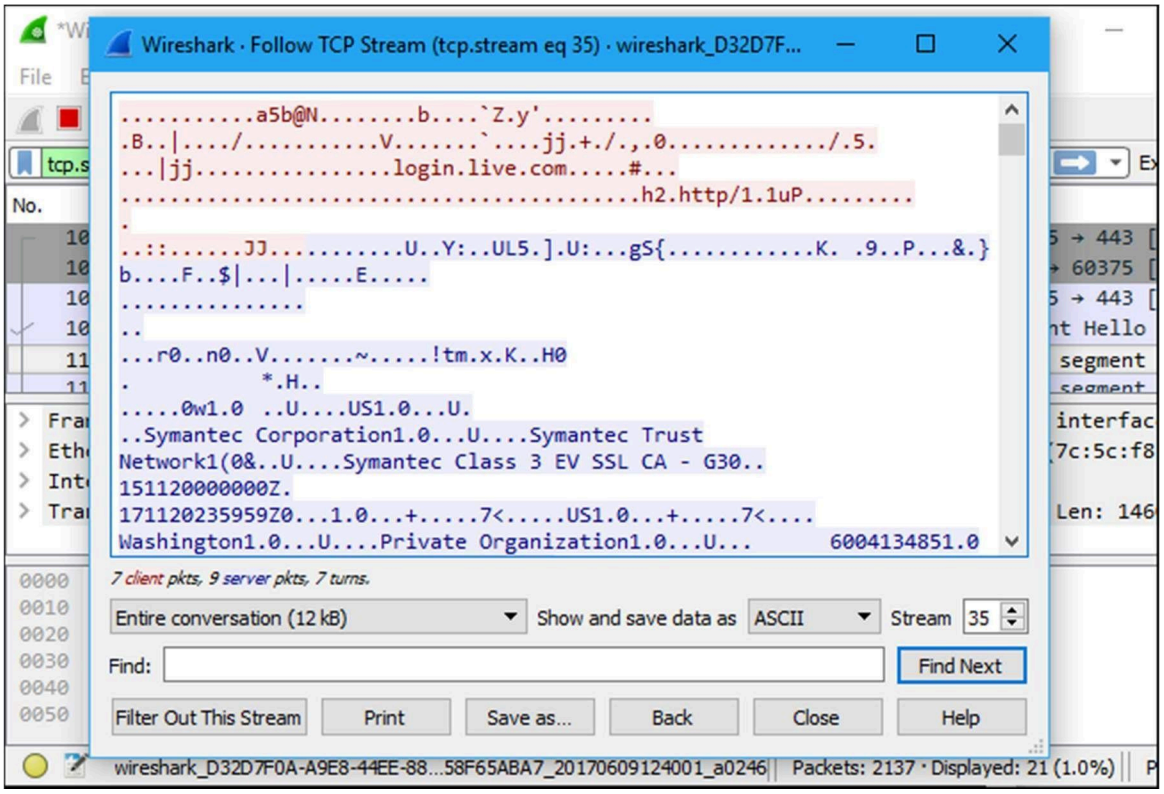
You can also click Analyze > Display Filters to choose a filter from among the default filters included in Wireshark. From here, you can add your own custom filters and save them to easily access them in the future.

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

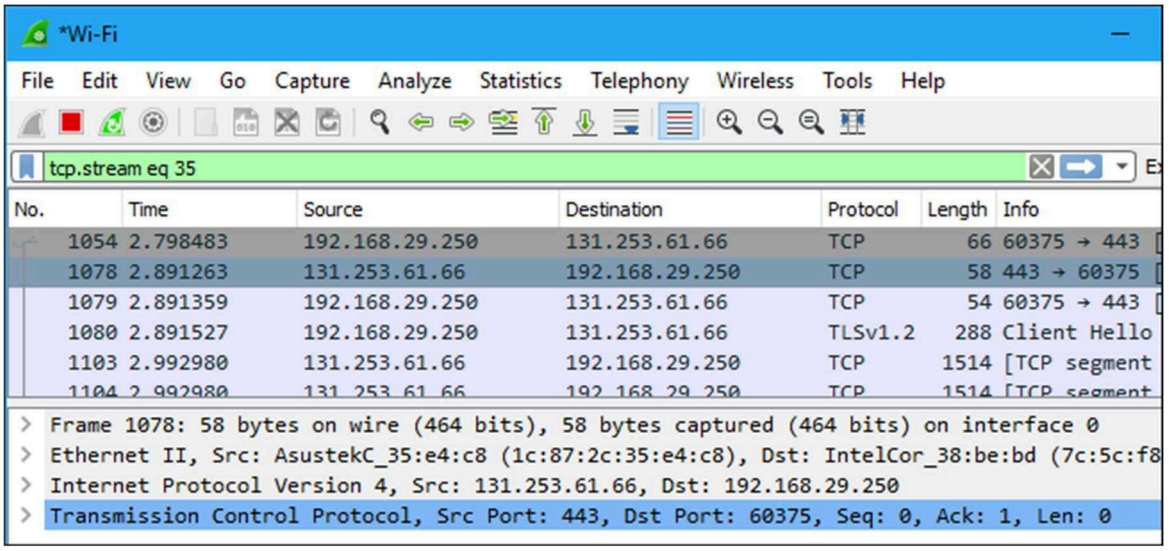


Another interesting thing you can do is right-click a packet and select Follow > TCP Stream.

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.

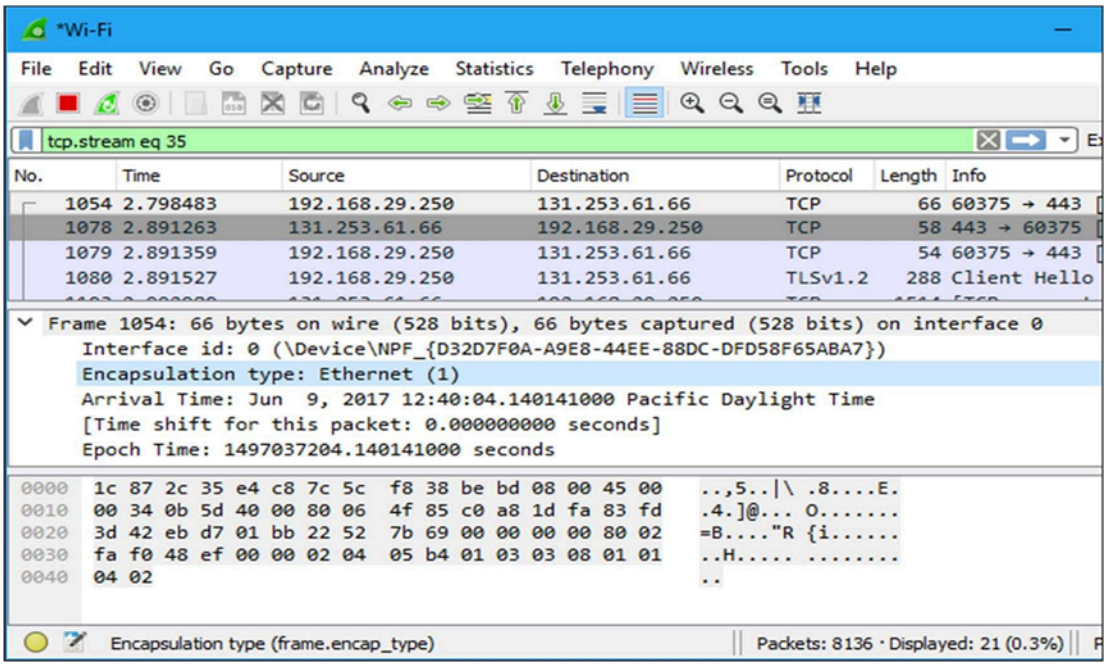


Close the window and you'll find a filter has been applied automatically. Wireshark is showing you the packets that make up the conversation.

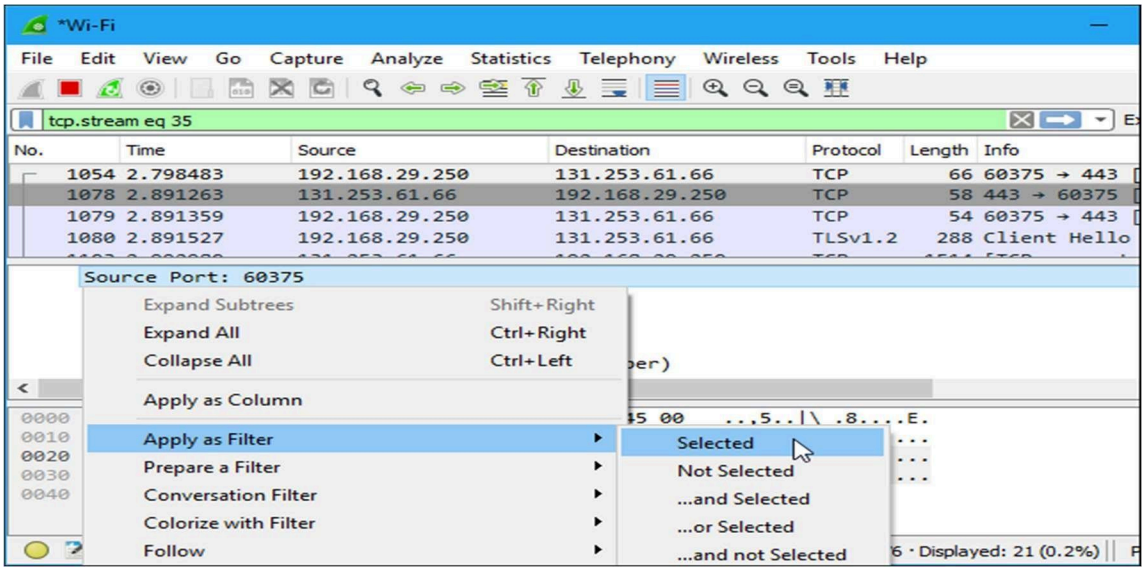


Inspecting Packets

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.

Wireshark Network Filtering:

Wireshark offers several filtering and search features that simplify locating and analyzing particular network events or problems.
There are several types of filters:

Capture filters: These filter incoming network traffic before captures it. Capture filters are based on the pcap filter syntax and can be specified in the capture options dialog box or at the command line when starting a capture.

Display filters: These are used to filter the captured network traffic that is displayed in main window. Display filters are based on Wireshark's display filter syntax and can be entered in the filter bar at the top of the main window.

Protocol filters: These filter network traffic based on the protocol being used. Protocol filters are available in the "Analyze" menu and can display only traffic that uses a specific protocol.

Conversation filters: These filter network traffic based on the conversation between two hosts. Conversation filters are available in the "Statistics" menu and display only traffic between hosts.

Features of Wireshark:

1. It is multi-platform software, i.e., it can run on Linux, Windows, OS X, FreeBSD, NetBSD, etc.
2. It is a standard three-pane packet browser.
3. It performs deep inspection of the hundreds of protocols.
4. It often involves live analysis, i.e., from the different types of the network like the Ethernet, loopback, etc., we can read live data.
5. It has sort and filter options which makes ease to the user to view the data.
6. It is also useful in VoIP analysis.
7. It can also capture raw USB traffic.
8. Various settings, like timers and filters, can be used to filter the output.
9. It can only capture packet on the PCAP (an application programming interface used to capture the network) supported networks.
10. Wireshark supports a variety of well-documented capture file formats such as the PcapNg and Libpcap. These formats are used for storing the captured data.
11. It is the no.1 piece of software for its purpose. It has countless applications ranging from the tracing down, unauthorized traffic, firewall settings, etc.

Uses of Wireshark:

Wireshark can be used in the following ways:

1. It is used by network security engineers to examine security problems.
2. It allows the users to watch all the traffic being passed over the network.
3. It is used by network engineers to troubleshoot network issues.
4. It also helps to troubleshoot latency issues and malicious activities on your network.
5. It can also analyze dropped packets.
6. It helps us to know how all the devices like laptop, mobile phones, desktop, switch, routers, etc., communicate in a local network or the rest of the world.

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

Experiment no: 4

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

AIM: Install Nmap and study it's working.

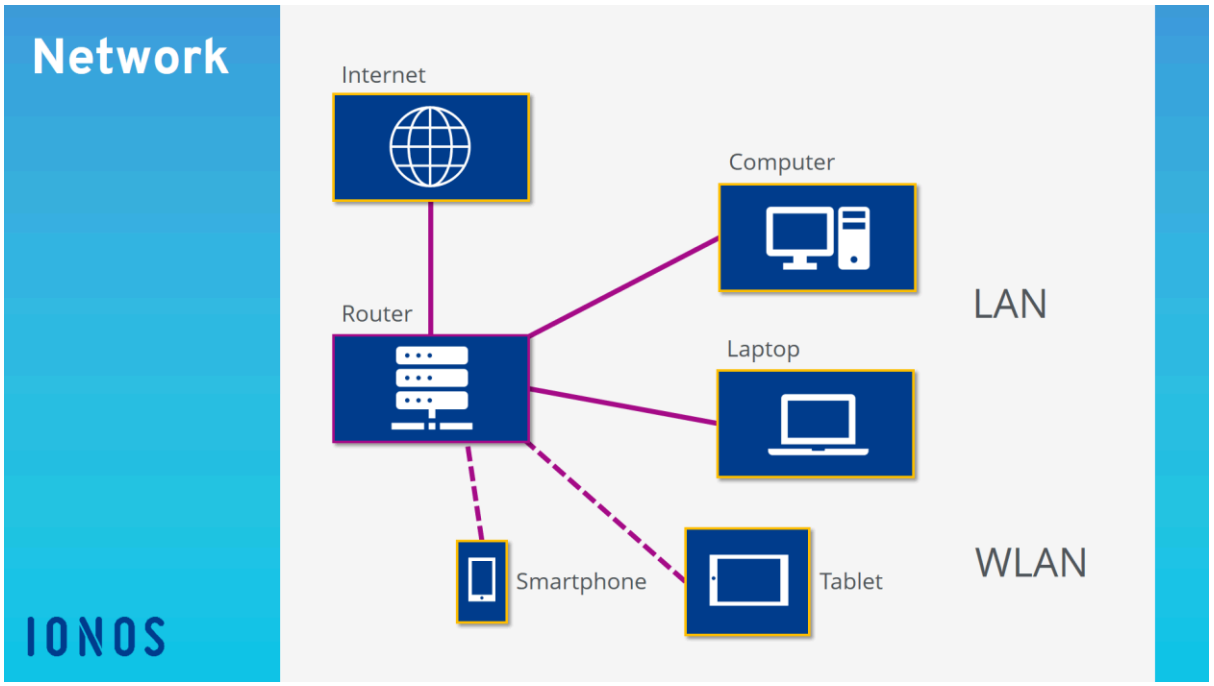
THEORY:

A network is defined as **the connection of at least two computer systems**, either by a cable or a wireless connection. The simplest network is a combination of two computers connected by a cable. This type of network is called a **peer-to-peer network**. There is no hierarchy in this network; both participants have equal privileges. Each computer has access to the data of the other device and can **share resources** such as disk space, applications or peripheral devices (printers, etc.).

Today's networks tend to be a bit more complex and don't just consist of two computers. Systems with more than ten participants usually use **client-server networks**. In these networks, a central computer (server) provides resources to the other participants in the network (clients).

In a typical client-server network there is a central node called the **server**. The server is connected to the other devices, which are called **clients**. This connection is either wireless (**Wireless LAN**) or wired (**LAN**).

In a typical home network, the router assumes the role of the server. It is connected to the Internet and provides the "Internet" resource for the other devices (computers, smartphones, etc.).



Different network discovery tools available

Atera: This cloud system is a remote monitoring and management package that has a network discovery feature to set up network asset management

NetBrain: Cloud-based paid service, this network monitor includes autodiscovery features and some great mapping options

Intermapper: Specialist network mapping tool for Windows, Linux, and Mac OS creates the layout of your current network after it searches via SNMP

Cacti: SNMP-driven network monitoring system that includes an autodiscovery phase; it installs on Unix, Linux, and Windows and is free to use

SolarWinds Network Performance Monitor: Offers automatic discovery and mapping of networks, including remote sites, cloud-based services, and WiFi

Faddom: A hybrid discovery and mapping service for applications and IT assets both on premise and in the cloud that includes a mapping function. Runs on site as a virtual appliance.

Nmap

Nmap is a network scanning tool—an open source Linux command-line tool—used for network exploration, host discovery, and security auditing. Gordon Lyon (pseudonym Fyodor Vaskovich) created it to help map an entire network easily and find its open ports and services.

In other words, you can use Nmap to scan IP addresses, search for security loopholes, and scan for open ports on your computer network by sending packets and analyzing the responses.

What does Nmap do?

At its core, Nmap uses IP packets to give you detailed, real-time information on all your networks, as well as the devices (servers, routers, switches, mobile devices) connected to them.

Here's a breakdown of the primary use of Nmap:

Scan every active IP address. You can get detailed information on every IP active on your network to determine whether an IP has been compromised. Nmap will tell you whether a legitimate service or an external hacker is using the IP.

Perform entire network scanning. You can get information on your network as a whole, including a list of live hosts and open ports and the OS of every connected device. Due to this, Nmap does a great job at monitoring your ongoing system and helping perform pen-testing.

Identify server vulnerabilities. You can use the tool to scan your web server for any security gaps to protect personal and business websites. Nmap helps simulate the process a malicious agent would typically use to attack your website.

Develop visual mappings. Nmap has a graphical user interface known as Zenmap. You can use it to create visual mappings of your network to facilitate better usability and reporting.

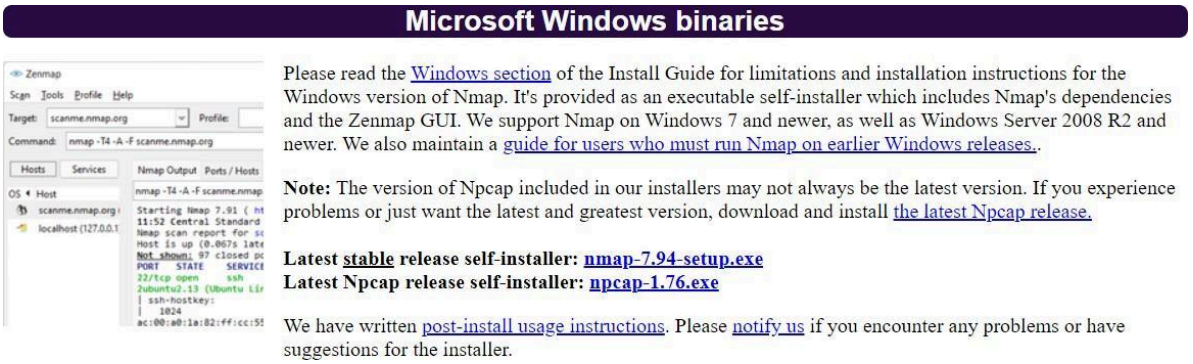
Automate system and vulnerability scans. Nmap has an incredible feature known as "Nmap Scripting Engine" (NSE). It's a scripting engine that lets you use a predefined set of scripts and automate networking features. Alternatively, you can write your own NSE scripts using the Lua programming language to make conclusions about the target host/service.

Although Nmap was developed for enterprise-scale networks, smaller companies are using the tool to scan connected devices. The exceptional rise of the IoT, in particular, has accelerated the increasing adoption of the tool to ensure top-notch data security.

Installation:

The installation process is easy, but it may vary based on your operating system. Below, we've covered how to install an app for Windows, MacBook, and Linux versions.

For Windows OS: Download and run the custom installer you get with Nmap (namp<version>setup.exe). This will automatically configure Nmap on your Microsoft system.



For Mac OS: Run the Nmap-<version>mpkg file to start the dedicated installer (you get this with Nmap).

Mac OS X Binaries

Nmap binaries for Apple macOS (x86-64) are distributed as a disk image file containing an installer. The installer allows installing Nmap, Zenmap, Ncat, and Ndiff. The programs have been tested on Mac OS X 10.9 and later. See the Mac OS X Nmap install page for more details. Users of PowerPC (PPC) Mac machines, which Apple ceased selling in 2006, should see this page instead for support information.

Latest stable release installer: nmap-7.94.dmg

For Linux OS: Run the following commands after opening the terminal to install Nmap

Linux RPM Source and Binaries

Many popular Linux distributions (Redhat, Mandrake, Suse, etc) use the RPM package management system for quick and easy binary package installation. We have written a detailed guide to installing our RPM packages, though these simple commands usually do the trick:

```
rpm -vhU https://nmap.org/dist/nmap-7.94-1.x86_64.rpm
rpm -vhU https://nmap.org/dist/zenmap-7.94-1.noarch.rpm
rpm -vhU https://nmap.org/dist/ncat-7.94-1.x86_64.rpm
rpm -vhU https://nmap.org/dist/nping-0.7.94-1.x86_64.rpm
```

You can also download and install the RPMs yourself:

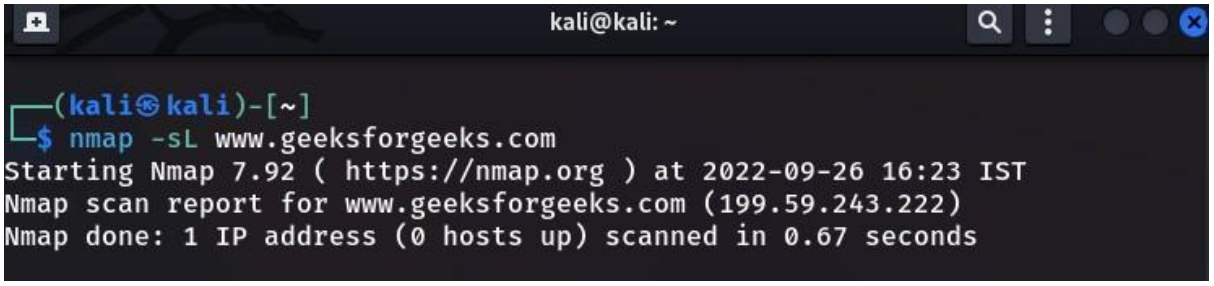
Latest stable release:
x86-64 (64-bit Linux) Nmap RPM: nmap-7.94-1.x86_64.rpm
x86-64 (64-bit Linux) Ncat RPM: ncat-7.94-1.x86_64.rpm
x86-64 (64-bit Linux) Nping RPM: nping-0.7.94-1.x86_64.rpm
Optional Zenmap GUI (all platforms): zenmap-7.94-1.noarch.rpm
Source RPM (includes Nmap, Zenmap, Ncat, and Nping): nmap-7.94-1.src.rpm

CentOS/Fedora: sudo dnf install nmap

Ubuntu/Debian: sudo apt-get install nmap

Working:

List Scan: A list scan generally lists the possible host without sending any packets to the targeted host.
nmap -sL www.geeksforgeeks.com



Ping Sweep: Ping sweep discovers on the basis the host is powered on.
nmap -sP www.geeksforgeeks.com

```
kali@kali: ~

┌──(kali㉿kali)-[~]
└─$ nmap -sP www.geeksforgeeks.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-26 16:32 IST
Nmap scan report for www.geeksforgeeks.com (199.59.243.222)
Host is up (0.0055s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
```

Disable ARP Ping: Nmap mostly uses ARP ping to discover the other host in the network. To disable ARP Ping, use option –disable-arp-ping.
nmap -sn www.geeksforgeeks.com –disable-arp-ping

```
kali@kali: ~

┌──(kali㉿kali)-[~]
└─$ nmap -sn www.geeksforgeeks.com --disable-arp-ping
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-26 16:40 IST
Nmap scan report for www.geeksforgeeks.com (199.59.243.222)
Host is up (0.0099s latency).
Nmap done: 1 IP address (1 host up) scanned in 5.95 seconds
```

TCP SYN Ping: Nmap checks whether a host is online.
nmap -PS www.geeksforgeeks.com

```
kali@kali: ~

┌──(kali㉿kali)-[~]
└─$ nmap -PS www.geeksforgeeks.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-26 16:45 IST
Nmap scan report for www.geeksforgeeks.com (199.59.243.222)
Host is up (0.0093s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 6.19 seconds
```

TCP ACK Ping: Nmap checks whether the host is responding.
nmap -sA www.geeksforgeeks.com

```
root@kali: /home/kali

┌──(root㉿kali)-[/home/kali]
└─# nmap -sA www.geeksforgeeks.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-26 16:51 IST
Nmap scan report for www.geeksforgeeks.com (199.59.243.222)
Host is up (0.011s latency).
All 1000 scanned ports on www.geeksforgeeks.com (199.59.243.222) are in ig
nored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 21.85 seconds
```

UDP Ping: Nmap sends the UDP packets to the targeted port.
nmap -sU www.geeksforgeeks.com

```
root@kali: /home/kali

┌──(root㉿kali)-[/home/kali]
└─# nmap -sU www.geeksforgeeks.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-27 12:38 IST
Nmap scan report for www.geeksforgeeks.com (199.59.243.222)
Host is up (0.0078s latency).
All 1000 scanned ports on www.geeksforgeeks.com (199.59.243.222) are in ig
nored states.
Not shown: 1000 open|filtered udp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 21.92 seconds
```

IP Protocol Ping: Nmap tries to send different packets using different protocols.
nmap -v -PO www.geeksforgeeks.com

```
root@kali: /home/kali

┌──(root㉿kali)-[/home/kali]
└─# nmap -v -PO www.geeksforgeeks.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-27 13:04 IST
Initiating Ping Scan at 13:04
Scanning www.geeksforgeeks.com (199.59.243.222) [3 ports]
Completed Ping Scan at 13:04, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:04
Completed Parallel DNS resolution of 1 host. at 13:04, 0.41s elapsed
Initiating SYN Stealth Scan at 13:04
Scanning www.geeksforgeeks.com (199.59.243.222) [1000 ports]
Discovered open port 443/tcp on 199.59.243.222
Discovered open port 80/tcp on 199.59.243.222
Completed SYN Stealth Scan at 13:04, 4.56s elapsed (1000 total ports)
Nmap scan report for www.geeksforgeeks.com (199.59.243.222)
Host is up (0.0073s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 10.21 seconds
           Raw packets sent: 2003 (88.076KB) | Rcvd: 5 (236B)
```

ARP Ping: ARP ping scan is used to discover the host devices in the same network. sometimes it will not visible due to firewall filtering.
nmap -PR www.geeksforgeeks.com

```
root@kali: /home/kali

┌──(root㉿kali)-[/home/kali]
└─# nmap -PR www.geeksforgeeks.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-27 13:20 IST
Nmap scan report for www.geeksforgeeks.com (199.59.243.222)
Host is up (0.0062s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 23.55 seconds
```

Function of TCP Window Scan:
Each packet that TCP Window Scan sends contains two headers. One header is called TCP Header (the one that gives the packet its TCP/IP look), and the other is called "TCP/UDP Data." This information is sent back to the person who initiated the scan, so that they may

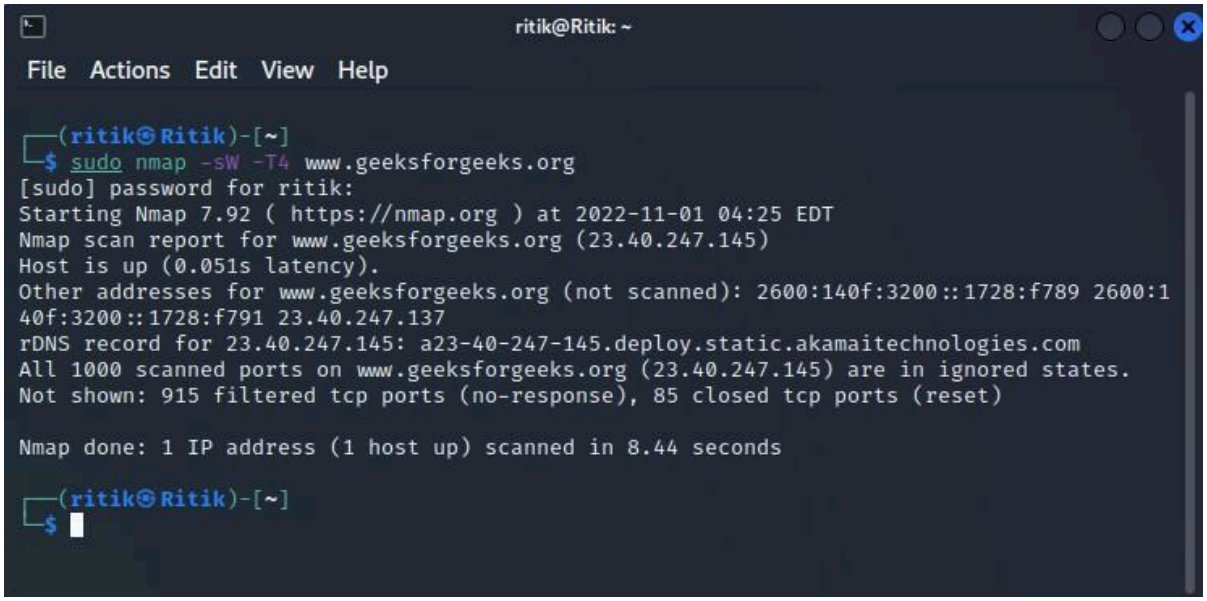
debug the problem if one does occur.
The IP addresses of all the computers on the network that were scanned and attacked.

- Ports in use on each computer, and
- The username/password combination for each valid username/password pair that was found.

TCP Window Scan on Nmap:

To view the TCP Window on the Nmap, open your terminal and then type in the following command:

nmap -sW -T4 (Any TCP Stream you want to search)



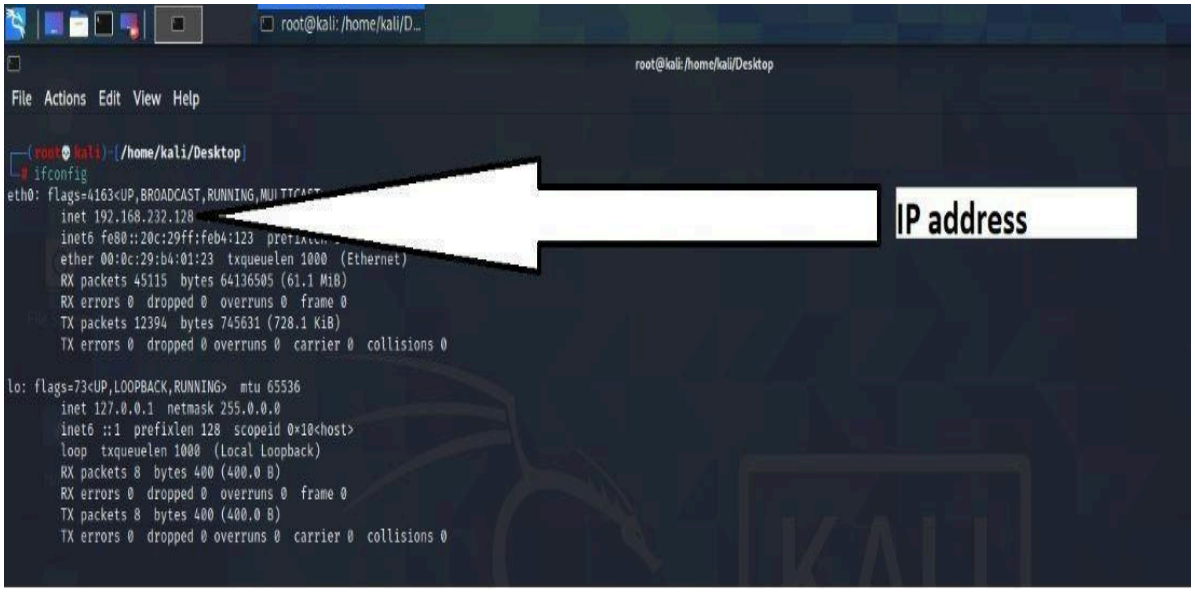
OS detection using NMAP

Now we need to run the actual commands to perform OS detection using NMAP, and at first, we will get the IP address of the host system, and then will perform a scan to get all active devices on the network.

Step 1: Getting the IP of the System
ifconfig

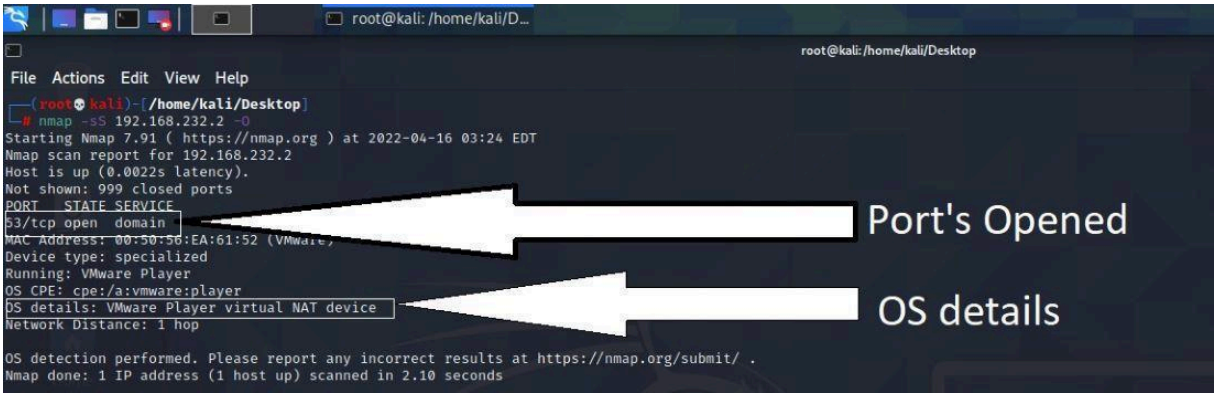
Step 2: List of active devices in the Network
nmap -sn 192.168.232.128/24

Step 2: List of active devices in the Network
nmap -sn 192.168.232.128/24



Step 2: List of active devices in the Network
nmap -sn 192.168.232.128/24

Let's do an SYN scan with OS detection in one of the active IPs
Let's select IP: 192.168.232.2
nmap -sS 192.168.232.2 -O



Running: VMware Player.
OS details: VMware Player virtual NAT device.

Let's now perform an Aggressive scan To guess the OS

- **-sV** stands for Service version.
- **-A** stands for Aggressive.

It will only display the chance of Operation System (OS) on the host computer with the help of Probability and Percentage.

nmap -sV 192.168.232.2 -A

Timing Options

The scan output accuracy is directly influenced by NMAP timing options set for a specific scan. For instance, when scanning a large number of targets on a fast network such as a Local Area Network [LAN], we can increase the number of parallel operations performed by NMAP to get faster results.

Nmap Timing Templates

Flag: *-T*

Syntax: *nmap -T[Template No.] [Target]*

Description: *Specify an NMAP timing template for a scan.*

Think of NMAP timing templates as shortcuts for different timing options.

NMAP provides six templates [0 to 5] we can use to slow down scanning [evade firewalls] or speed up [get faster results] – depending on the scanning scenario, as seen in below.

NMAP Timing Template	Name	Description
-T0	Paranoid scan	A very slow scan
-T1	Sneaky scan	Excellent for avoiding firewalls

-T2	Polite scan	Unlikely to interfere with the target system
-T3	Normal scan	The default NMAP timing template
-T4	Aggressive scan	Provides faster results on LANs
-T5	Insane scan	A fast aggressive scan

NMAP Timing Templates

Logging scans

Although seeing the results of scans on a case by case basis is very helpful in the short term; for longer assessment times (or for larger scans that would scroll off the screen), it's a good idea to log scans to file.

Nmap supports three different types of logging. Each type has a different flag to log that specific log type, and different purposes. Fortunately for us, the Nmap development team was smart enough to think ahead; using the -oA (output all) flag, it's possible to output all three log files. The second parameter to this flag is simply the base name of the logs. They will automatically have their own unique file extension.

```
dshaw@debian:~$ nmap scanme.nmap.org -oA logbase

Starting Nmap 6.47 ( http://nmap.org ) at 2014-12-11 17:04 PST
Nmap scan report for scanme.nmap.org (74.207.244.221)
Host is up (0.063s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
9929/tcp open  nping-echo

Nmap done: 1 IP address (1 host up) scanned in 12.58 seconds
dshaw@debian:~$ ls -ltr | grep logbase
-rw-r--r--  1 dshaw dshaw    5451 Dec 11 17:05 logbase.xml
-rw-r--r--  1 dshaw dshaw     384 Dec 11 17:05 logbase.nmap
-rw-r--r--  1 dshaw dshaw     380 Dec 11 17:05 logbase.gnmap
dshaw@debian:~$ _
```

Conclusion: Thus we have learn how to scan and uncover essential information concerning your host, ports, firewall, and OS, which can help network administrators do their job more effectively also Learning Nmap can significantly amp up your network security

EXPERIMENT NO. 5

TITLE: Simple network topology and configuration of static routing protocol using packet tracer.

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 as the name suggests, is a tool built by Cisco. This tool provides a network simulation to practice simple and complex networks. As Cisco believes, the best way to learn about networking is to do it.

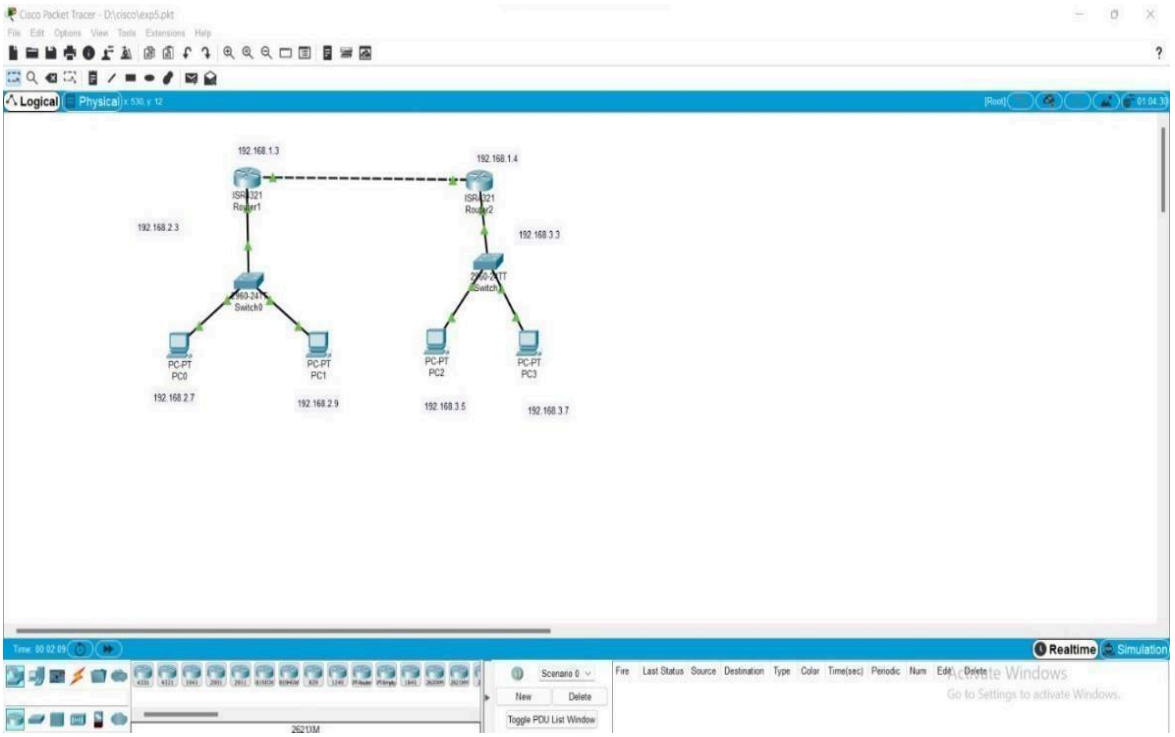
The main purpose of Cisco Packet Tracer is to help students learn the principles of networking with hands-on experience as well as develop Cisco technology specific skills. Since the protocols are implemented in software only method, this tool cannot replace the hardware Routers or Switches. Interestingly, this tool does not only include Cisco products but also many more networking devices.

STEPS ARE:

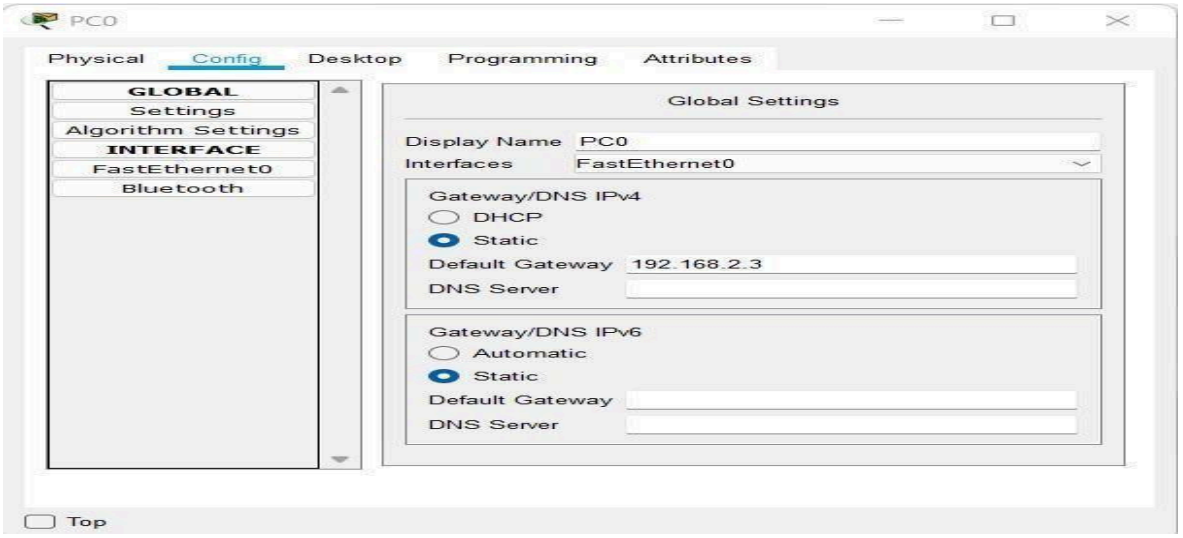
Step 1: Open Cisco Packet Tracer. Select Hub from Network Devices and place it on canvas.

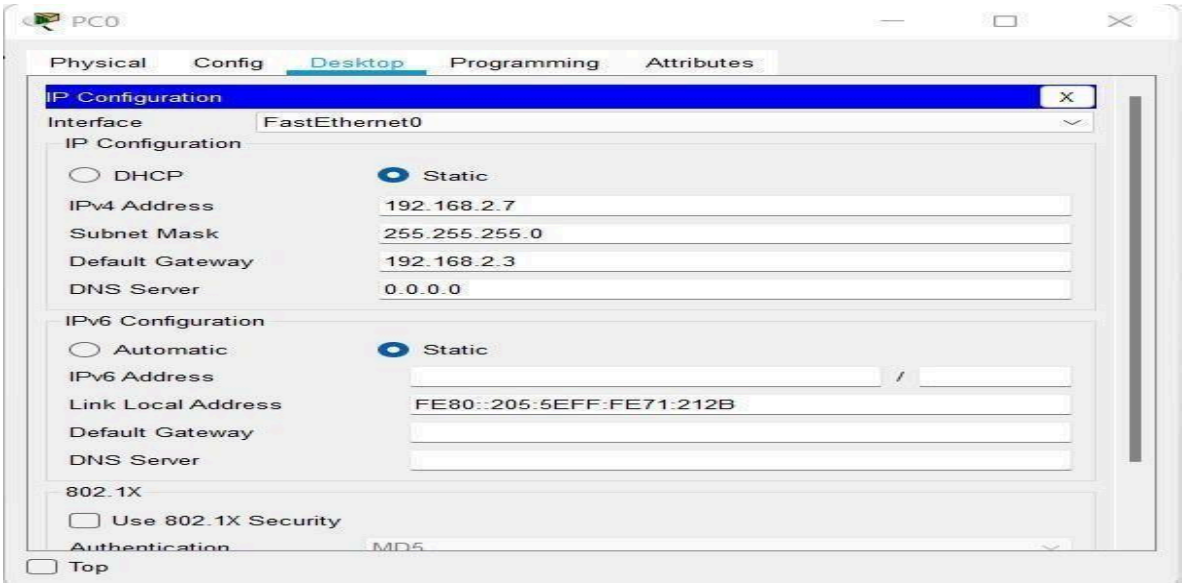
Step 2: Select few PCs or Laptops from End Devices and place them on canvas.

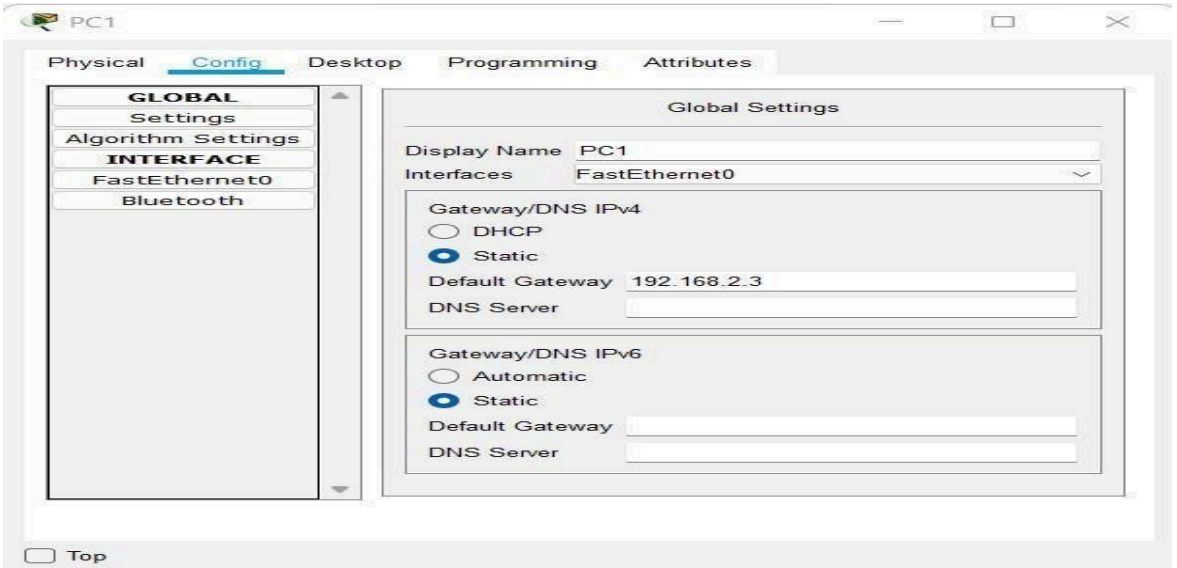
Step 3: Select Automatic Connections from Connections and connect them as shown below.

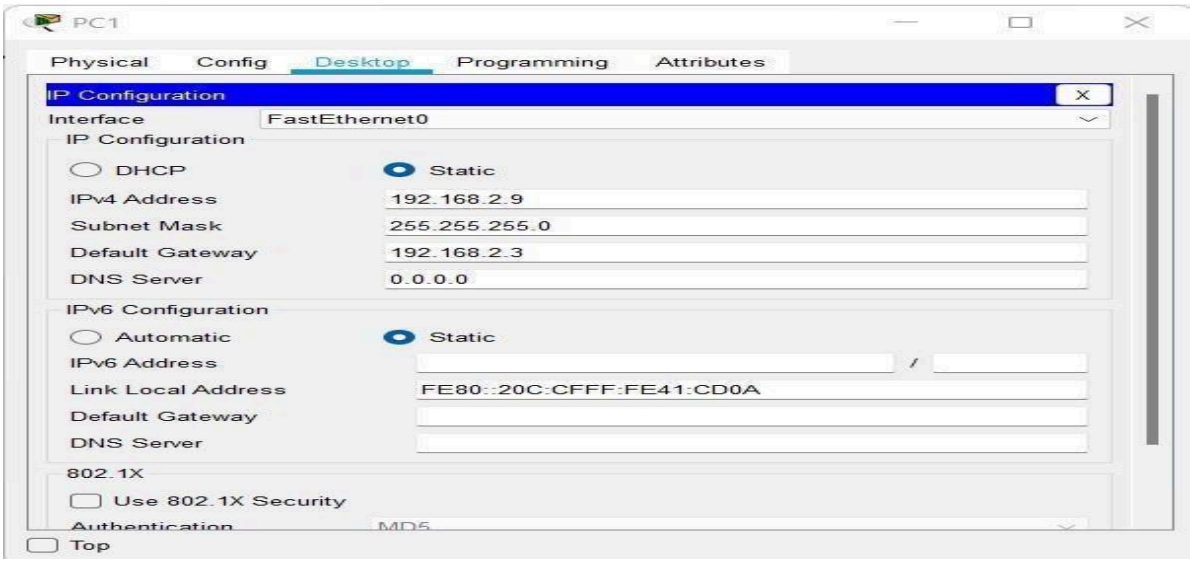


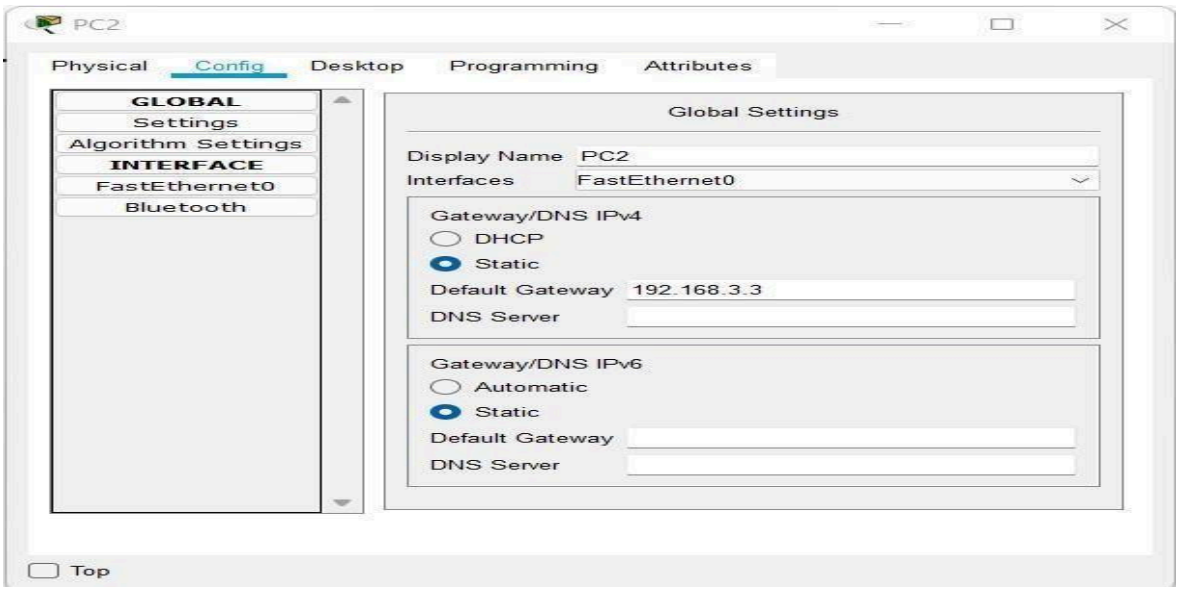
Step 4: Click on a PC. Go to Desktop IP Configuration and enter the IP as shown below.

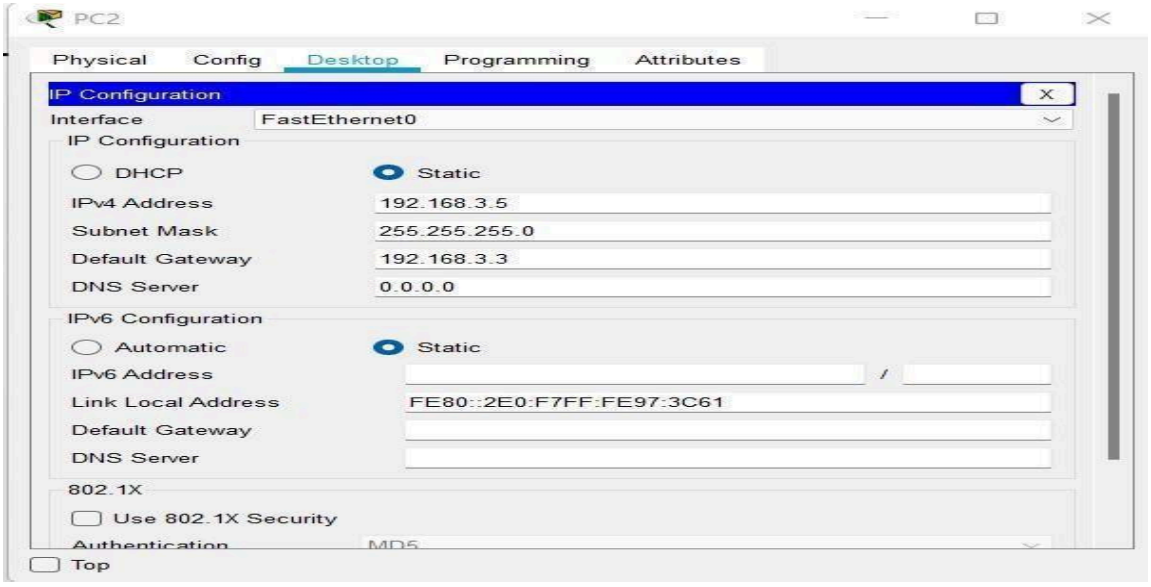


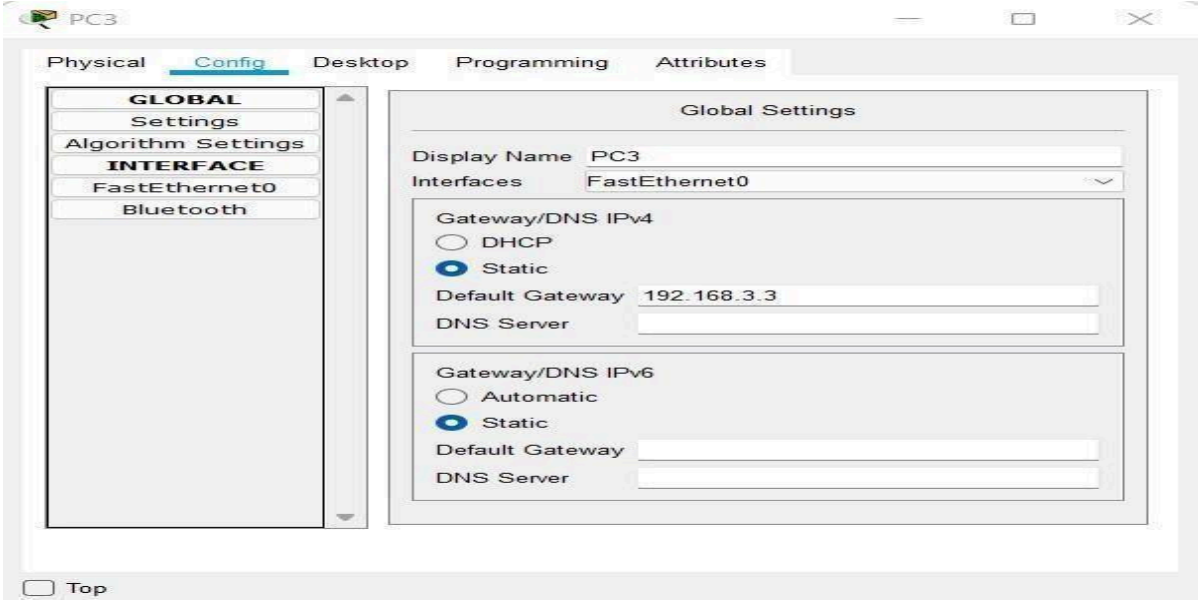


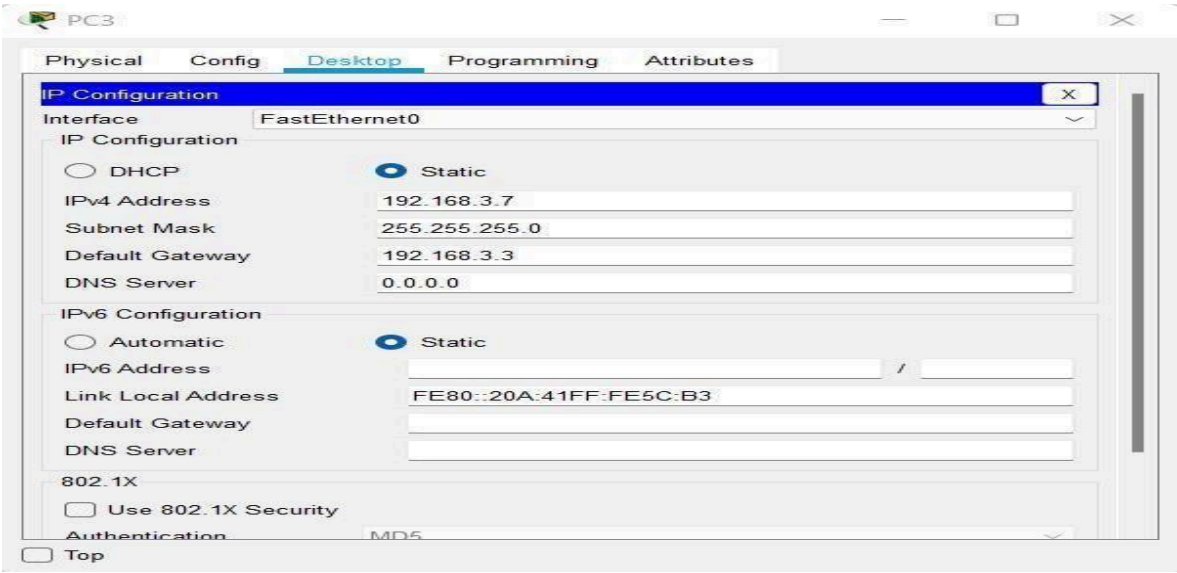


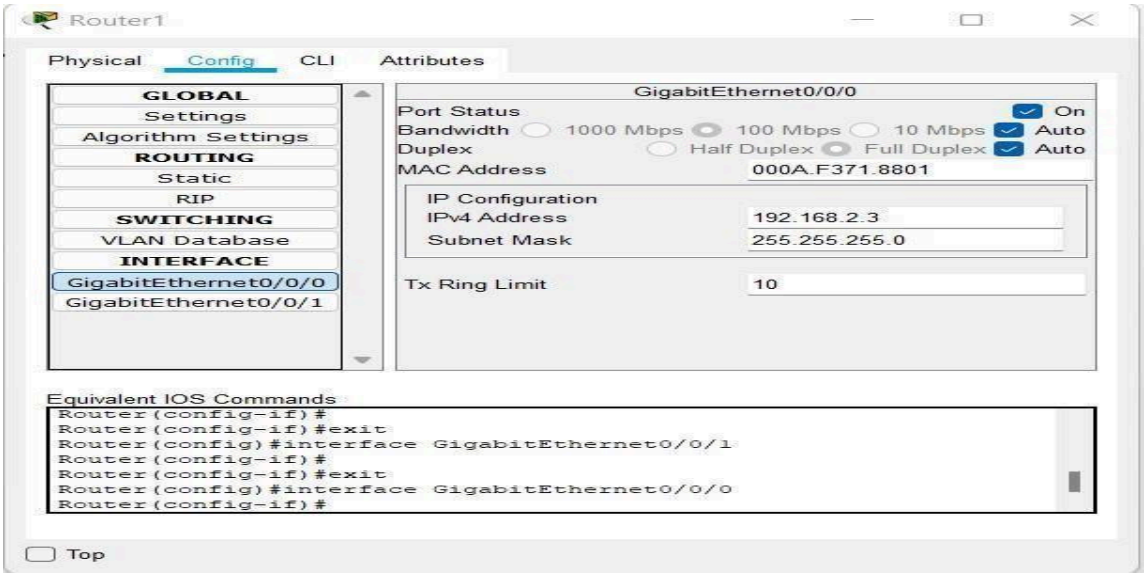

PC1
Physical
Config
Desktop
Programming
Attributes
IP Configuration
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.2.9
Subnet Mask
255.255.255.0
Default Gateway
192.168.2.3
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address
FE80::20C:CFFF:FE41:CD0A
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Top


PC2
Physical
Config
Desktop
Programming
Attributes
GLOBAL
Settings
Algorithm Settings
INTERFACE
FastEthernet0
Bluetooth
Global Settings
Display Name
PC2
Interfaces
FastEthernet0
Gateway/DNS IPv4
DHCP
Static
Default Gateway
192.168.3.3
DNS Server
Gateway/DNS IPv6
Automatic
Static
Default Gateway
DNS Server
Top


PC2
Physical
Config
Desktop
Programming
Attributes
IP Configuration
Interface
FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address
192.168.3.5
Subnet Mask
255.255.255.0
Default Gateway
192.168.3.3
DNS Server
0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address
FE80::2E0:F7FF:FE97:3C61
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication
MD5
Top


PC3
Physical
Config
Desktop
Programming
Attributes
GLOBAL
Settings
Algorithm Settings
INTERFACE
FastEthernet0
Bluetooth
Global Settings
Display Name PC3
Interfaces FastEthernet0
Gateway/DNS IPv4
DHCP
Static
Default Gateway 192.168.3.3
DNS Server
Gateway/DNS IPv6
Automatic
Static
Default Gateway
DNS Server
Top


PC3
Physical
Config
Desktop
Programming
Attributes
IP Configuration
Interface FastEthernet0
IP Configuration
DHCP
Static
IPv4 Address 192.168.3.7
Subnet Mask 255.255.255.0
Default Gateway 192.168.3.3
DNS Server 0.0.0.0
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address FE80::20A:41FF:FE5C:B3
Default Gateway
DNS Server
802.1X
Use 802.1X Security
Authentication MD5
Top


Router1
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0/0
GigabitEthernet0/0/1
GigabitEthernet0/0/0
Port Status On
Bandwidth 1000 Mbps 100 Mbps 10 Mbps Auto
Duplex Half Duplex Full Duplex Auto
MAC Address 000A.F371.8801
IP Configuration
IPv4 Address 192.168.2.3
Subnet Mask 255.255.255.0
Tx Ring Limit 10
Equivalent IOS Commands
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0/1
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0/0
Router(config-if)#
Top

Router1

Physical | Config | CLI | Attributes

GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0/0
GigabitEthernet0/0/1

GigabitEthernet0/0/1

Port Status: On
Bandwidth: 1000 Mbps, 100 Mbps, 10 Mbps, Auto
Duplex: Half Duplex, Full Duplex, Auto
MAC Address: 000A.F371.8802

IP Configuration
IPv4 Address: 192.168.1.2
Subnet Mask: 255.255.255.0

Tx Ring Limit: 10

Equivalent IOS Commands

```
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0/1
Router(config-if)#
```

Top

Router2

Physical | Config | CLI | Attributes

GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0/0
GigabitEthernet0/0/1

GigabitEthernet0/0/0

Port Status: On
Bandwidth: 1000 Mbps, 100 Mbps, 10 Mbps, Auto
Duplex: Half Duplex, Full Duplex, Auto
MAC Address: 00E0.F7B6.3701

IP Configuration
IPv4 Address: 192.168.3.3
Subnet Mask: 255.255.255.0

Tx Ring Limit: 10

Equivalent IOS Commands

```
Router>enable
Router#
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0/0
Router(config-if)#
```

Top

Router2

Physical | Config | CLI | Attributes

GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
GigabitEthernet0/0/0
GigabitEthernet0/0/1

GigabitEthernet0/0/1

Port Status: On
Bandwidth: 1000 Mbps, 100 Mbps, 10 Mbps, Auto
Duplex: Half Duplex, Full Duplex, Auto
MAC Address: 00E0.F7B6.3702

IP Configuration
IPv4 Address: 192.168.1.4
Subnet Mask: 255.255.255.0

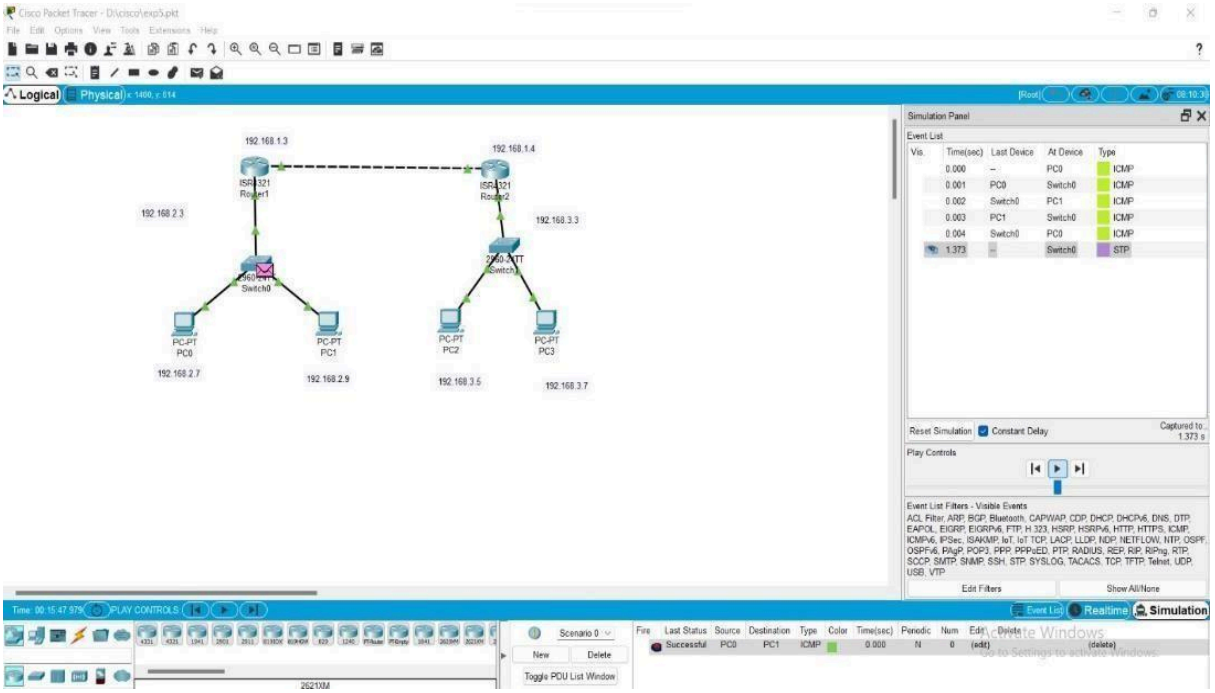
Tx Ring Limit: 10

Equivalent IOS Commands

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0/1
Router(config-if)#
```

Top

Step 5: After completing the setup, you now need to test your network. So click on Add simple PDU icon then select the any two PCs. After that Click on Simulation to see how your network works.



Conclusion: Hence we have learnt how to make a simple star network topology and implement the same.

EXPERIMENT 6

TITLE: Study and Installation of Network Simulator

(NS3) **AIM**: To study and learn to install 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 Set up the VMware workstation: a. Create a new virtual machine by selecting "Create New Virtual Machine."

4. 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.

5.Name the machine and set the password.

6.Configure the Hardware:

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

ii. For faster VMware, set processors to 2.

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

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

8.Install prereq packages on Ubuntu using terminal:

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

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

b. 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

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

cxxfilt

5. 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.

6. 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

7. Test the NS3 build and installation success by running test.py in the ns directory

using the following commands: cd ns- ./test.py

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

CONCLUSION: Thus, we have studied and successfully install NS3

EXPERIMENT
NO.07

Title: To understand Concept of socket

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 Server Socket classes are used for connection-oriented socket programming and Datagram Socket and Datagram Packet classes are used for connection-less socket programming.

The client in socket programming must know two information:

a. IP Address of Server, and

a. Port number.

Here, we are going to make one-way client and server communication. In this application, client sends a message to the server, server reads the message and prints it. Here, two classes are being used: Socket and Server Socket.

The Socket class is used to communicate client and server. Through this class, we can read and write message. The Server Socket class is used at server-side. The accept() method of Server Socket 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);}

```
}
}
```

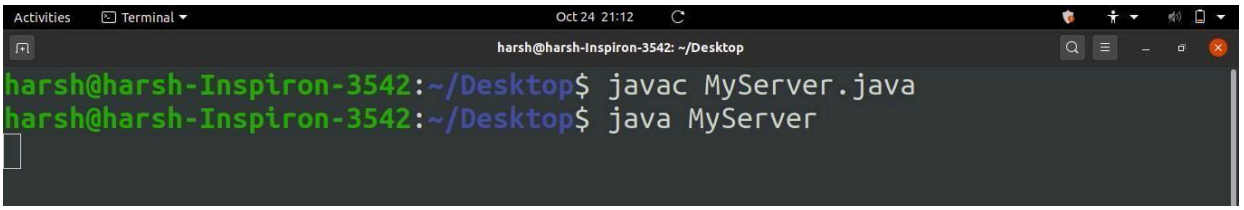
MyClient.java file

```
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:

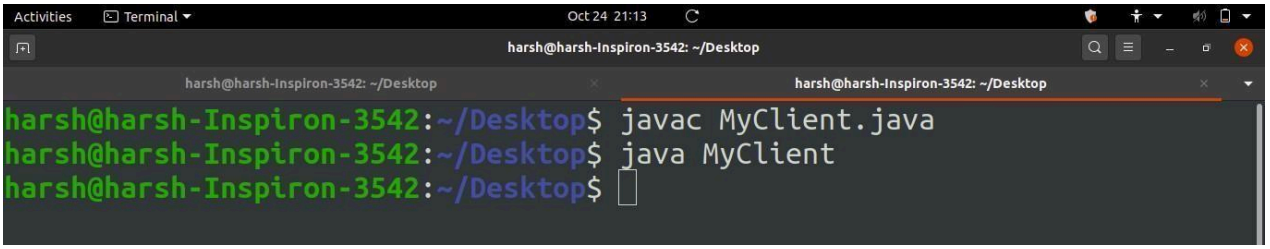
To execute this program open two command prompts and execute each program at each command prompt as displayed in the below figures.

First run Myserver.java file in terminal/cmd,



Running MyServer.java

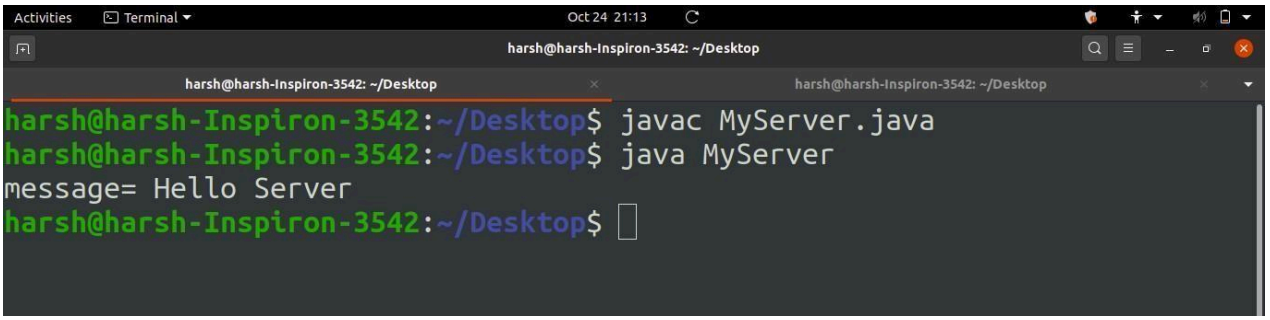
Then in new terminal/cmd run MyClient.java file,



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,

Fig.



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 8

TITLE: Design VPN and Configure RIP/OSPF using Packet tracer. **AIM:** To 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:

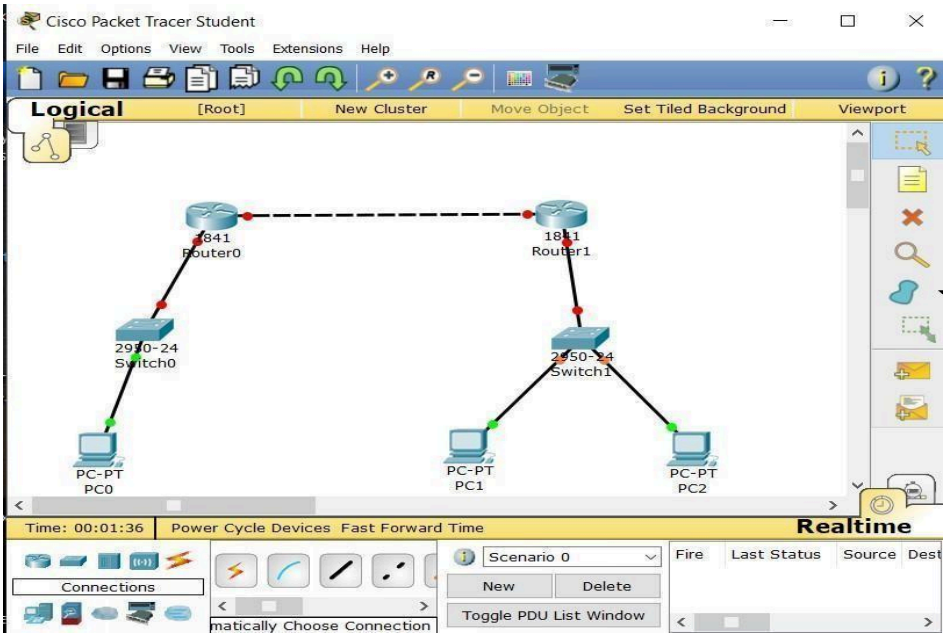
1. Updates of the network are exchanged periodically.
2. Updates (routing information) are always broadcast.
3. Full routing tables are sent in updates.
4. Routers always trust on routing information received from neighbour routers. This is also known as Routing on rumours.

<u>Steps for implementing RIP:</u>

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.

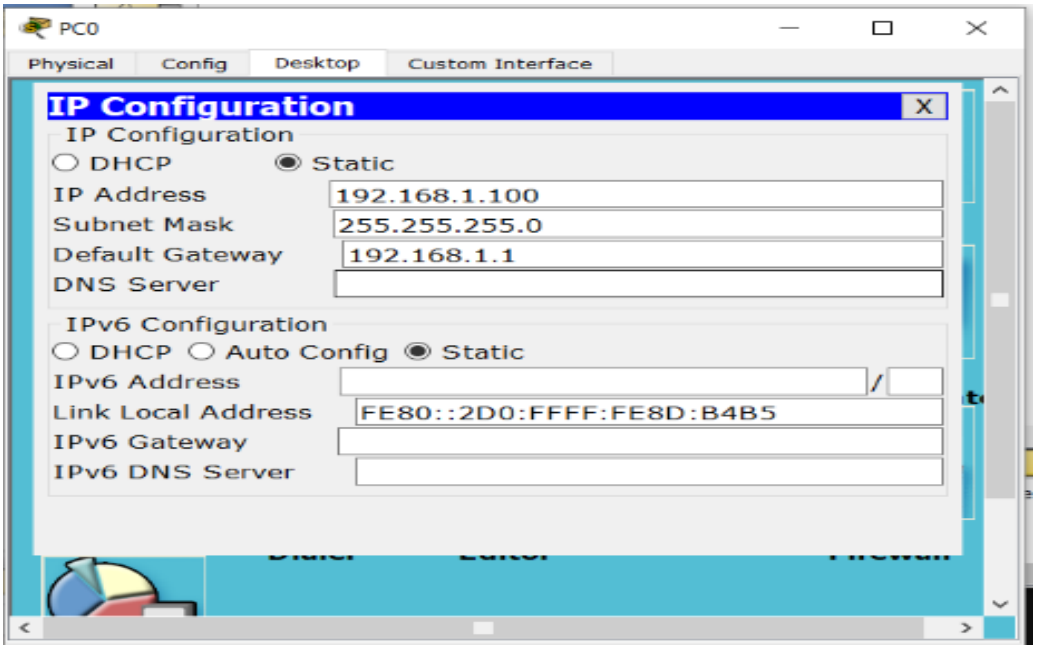


Step 2:

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.

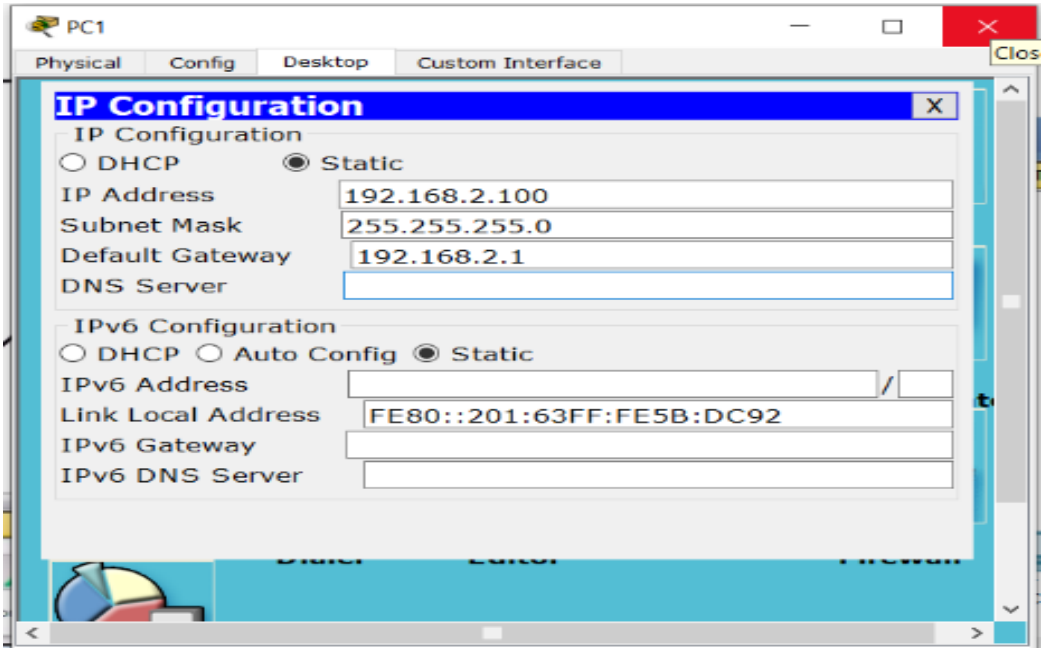
Add Default Gateway and close the window.



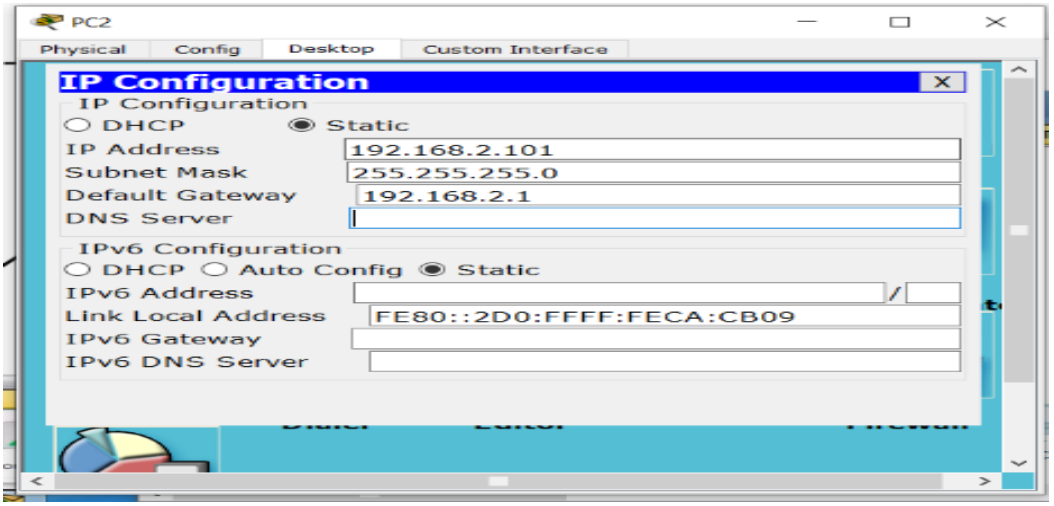
Step 3:

Click on PC1 and go to Desktop > IP Configuration

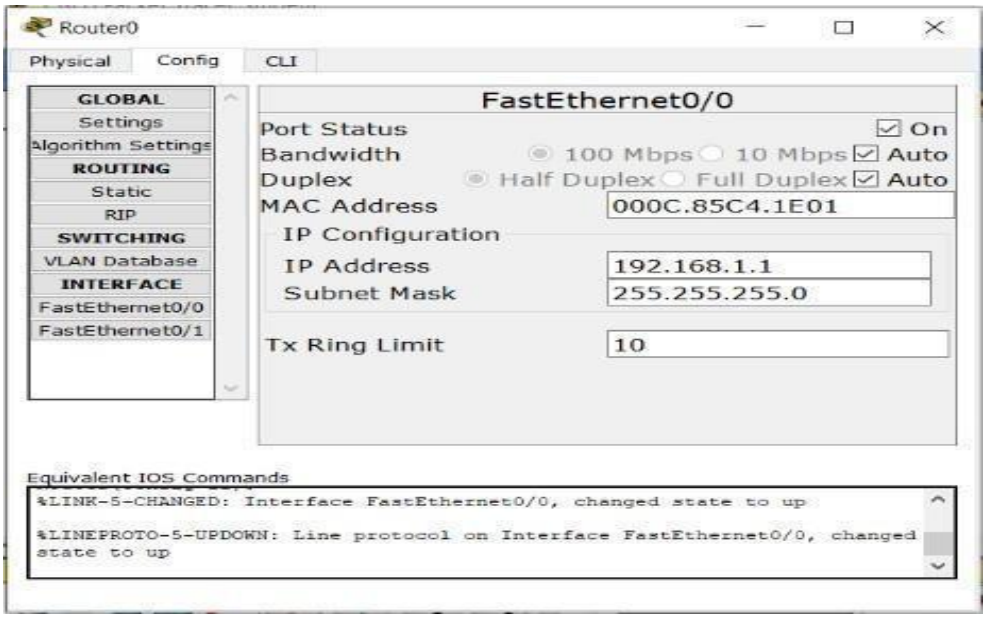
Add IP Address, as you will add the IP Address, Subnet Mask will be automatically added and displayed.
Add Default Gateway and close the window.



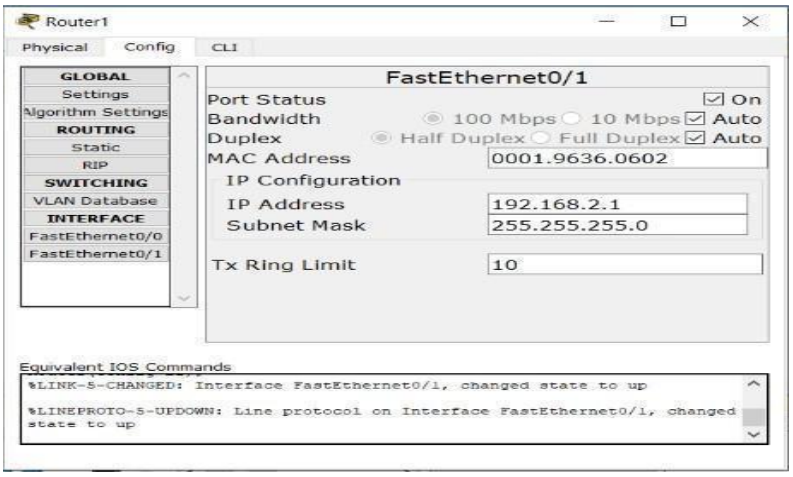
Step 4:
Click on PC2 and go to Desktop > IP Configuration
Add IP Address, as you will add the IP Address, Subnet Mask will be automatically added and displayed.
Add Default Gateway and close the window.

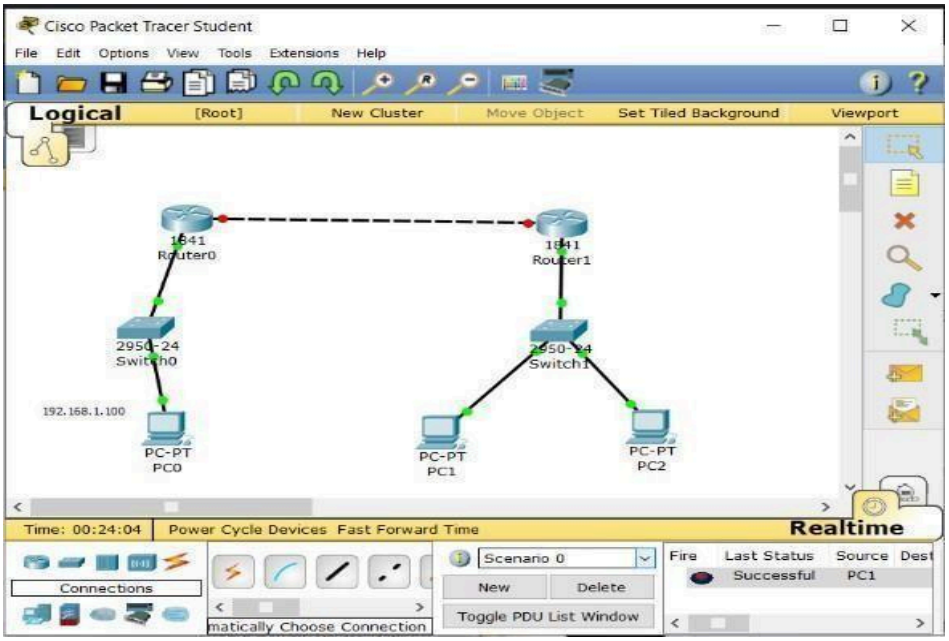


Step 5:
Click on Router0. Go to Config > FastEthernet0/0. Here, add IP Address and On the Port Status.



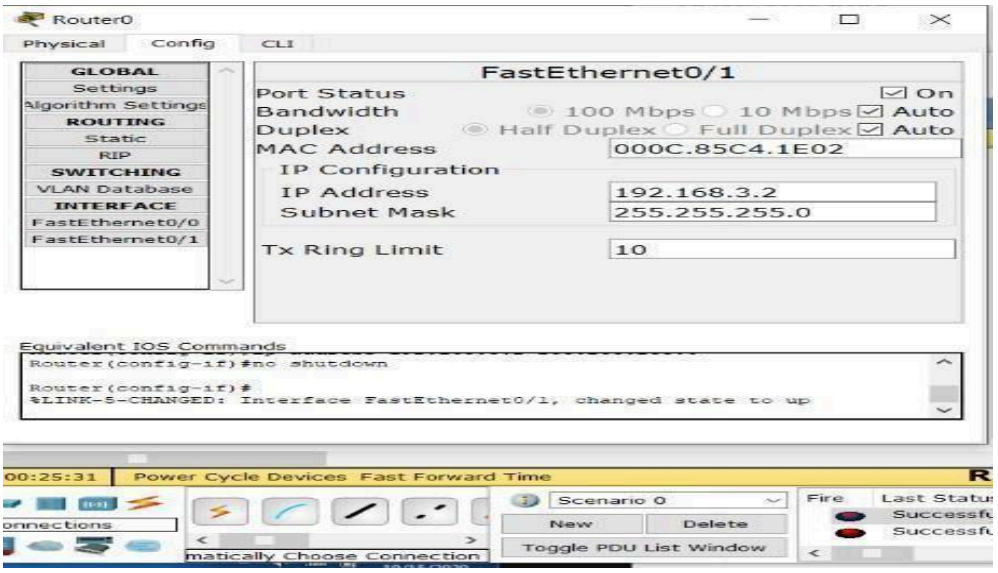
Step 6:
Click on Router1. Go to Config > FastEthernet0/1. Here, add IP Address and On the Port Status.



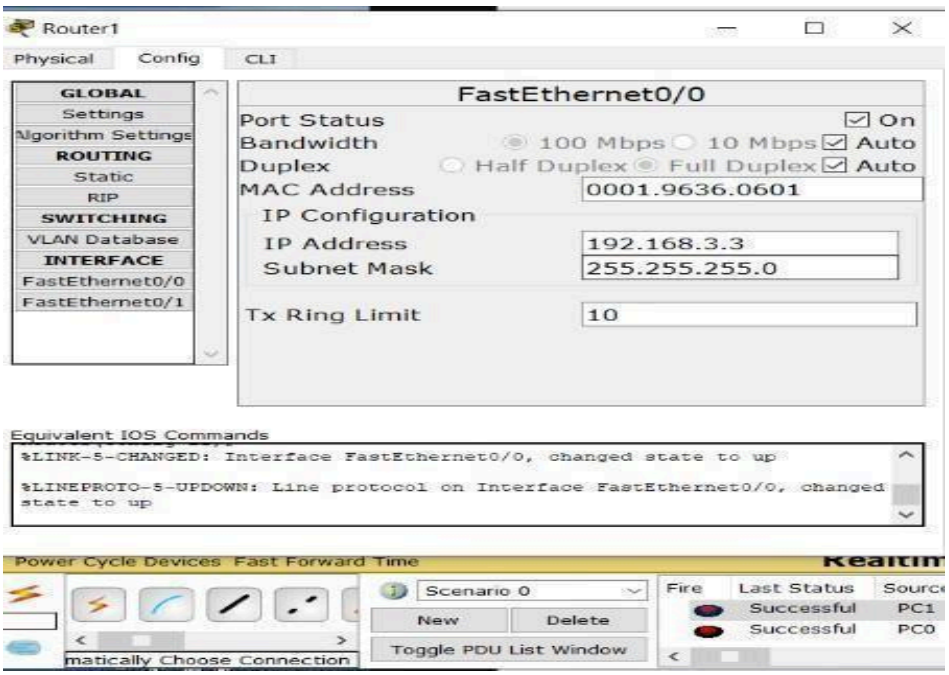


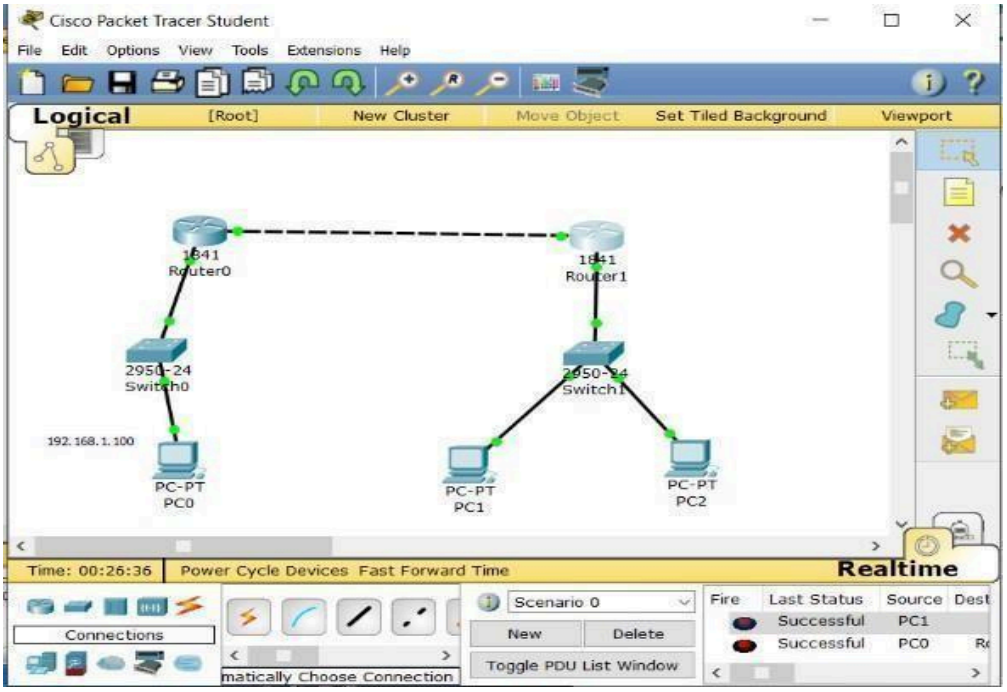
As you will see above, there is green dots which means connections are done successfully between Router, Switches and PCs.

Step 7:
Click on Router0. Go to Config > FastEthernet0/1. Here, add IP Address and On the Port Status.

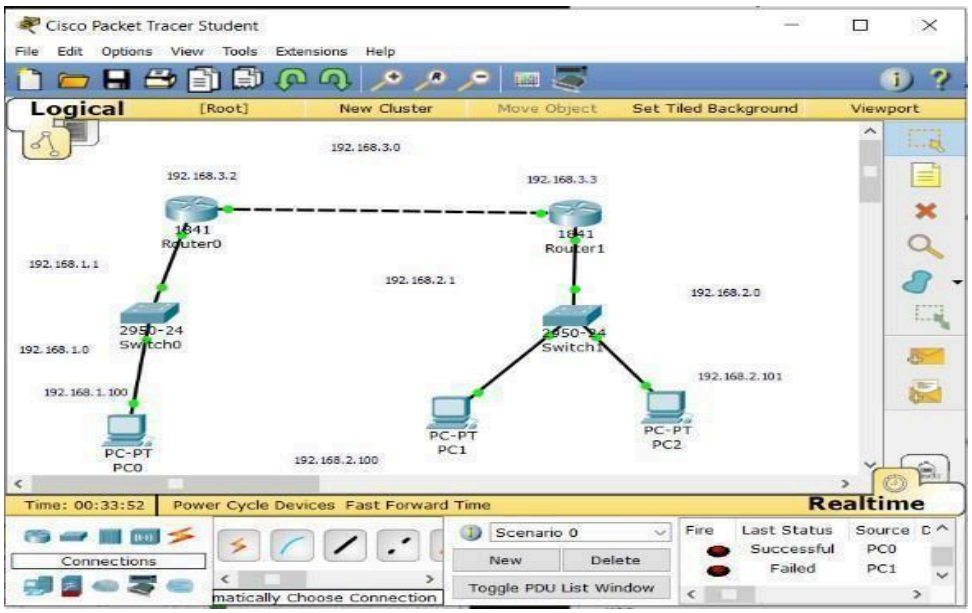


Step 8:
Click on Router1. Go to Config > FastEthernet0/0. Here, add IP Address and On the Port Status.





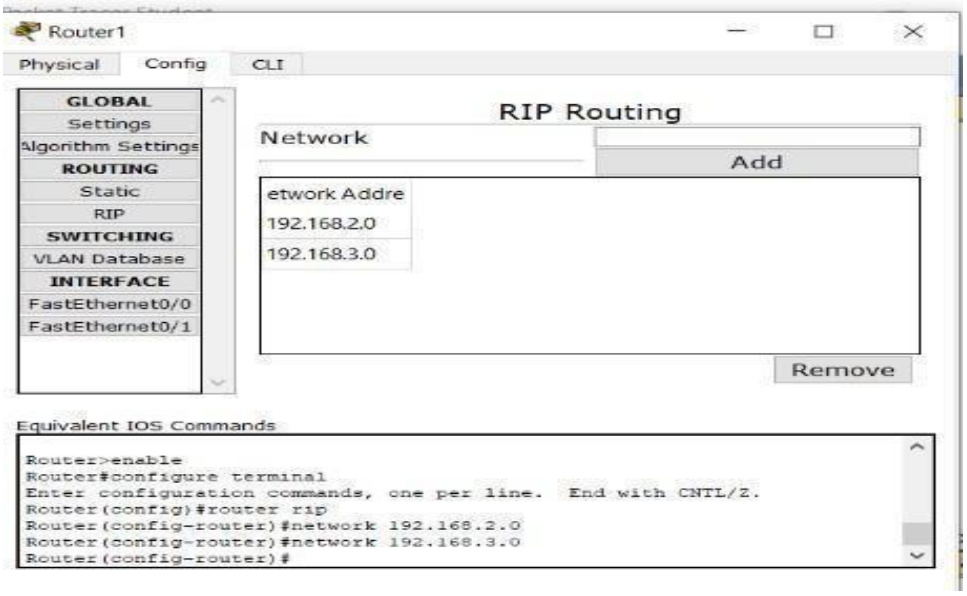
As you can see above, connection is done between both the Routers successfully



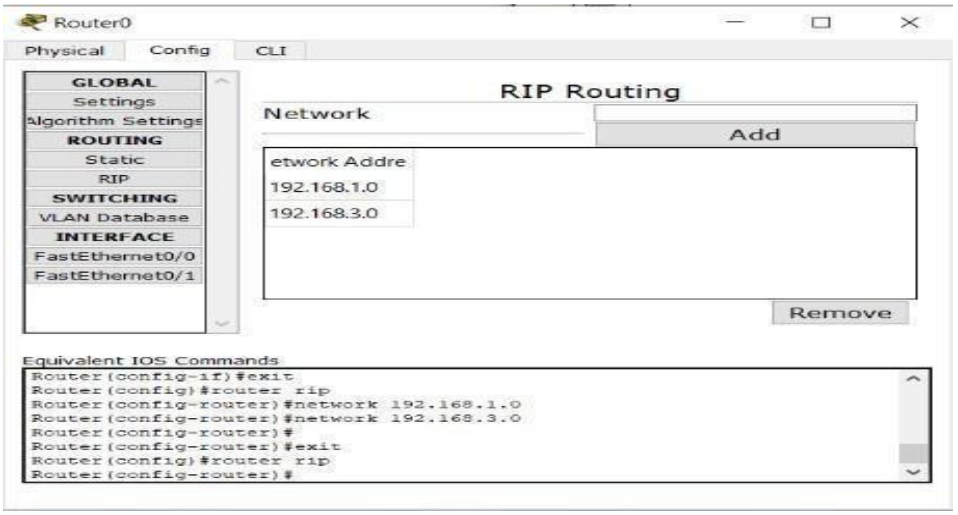
Step 9:

Click on Router1. Go to Config > RIP.

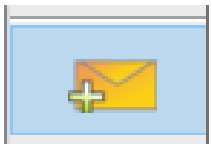
Here, add the network address to connect router1 with switch1, PC1, PC2 and router0.



Step 10:
Click on Router0. Go to Config > RIP.
Here, add the network address to connect router0 with switch0, PC0 and router1.

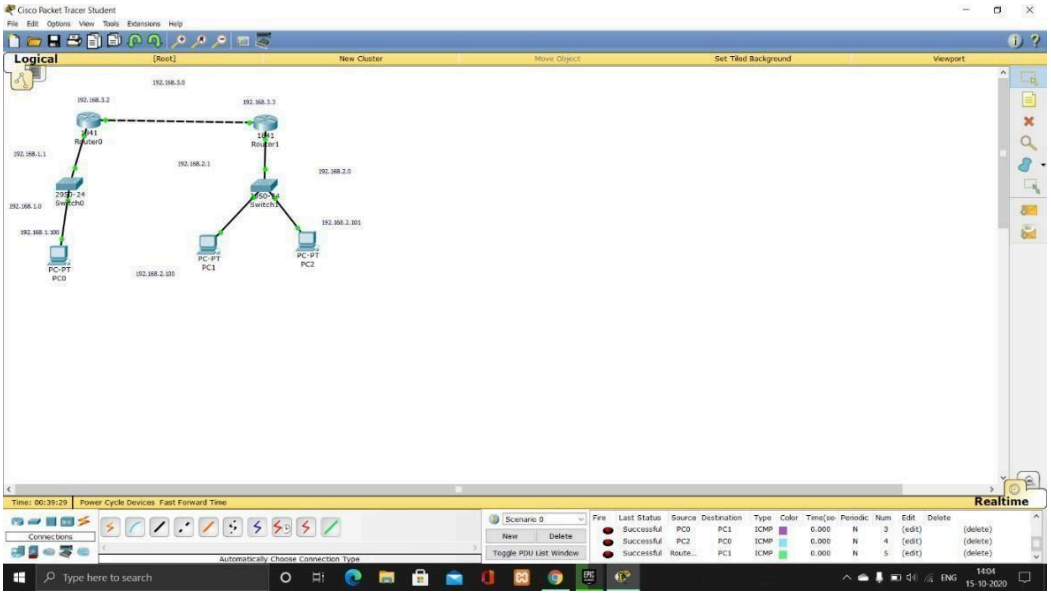


Now, all the connections are done successfully, you can check it by clicking on this symbol



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

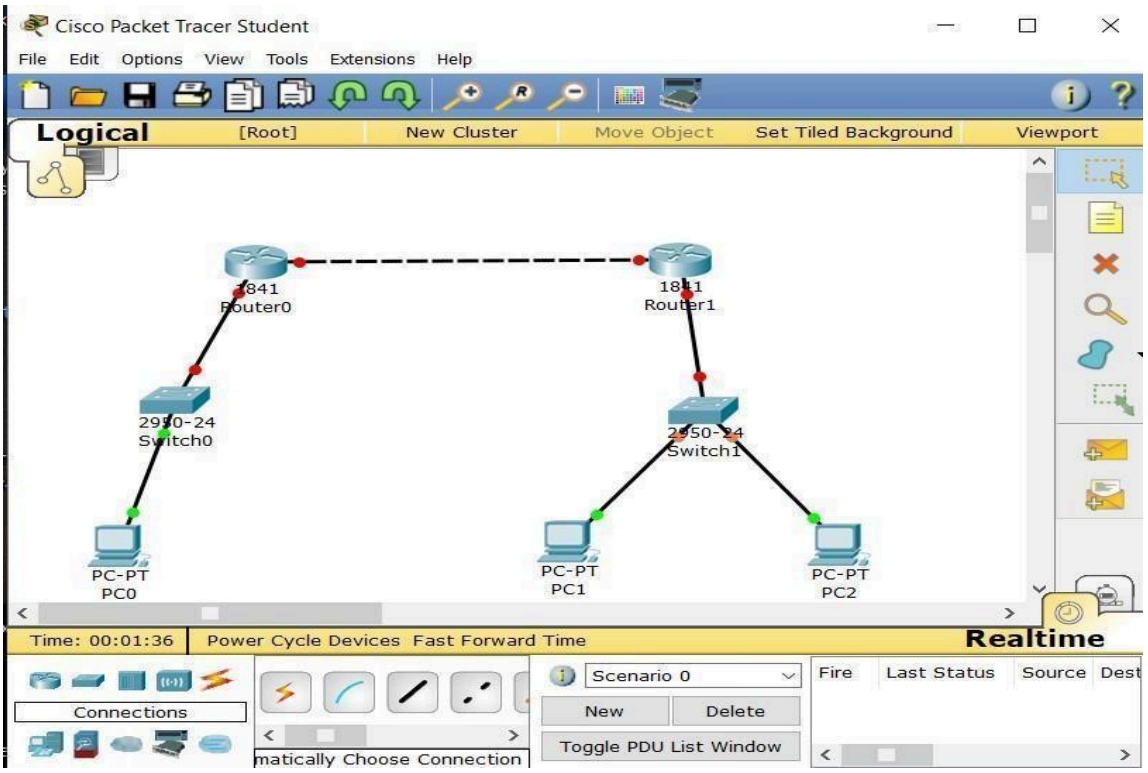
Final Output:



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

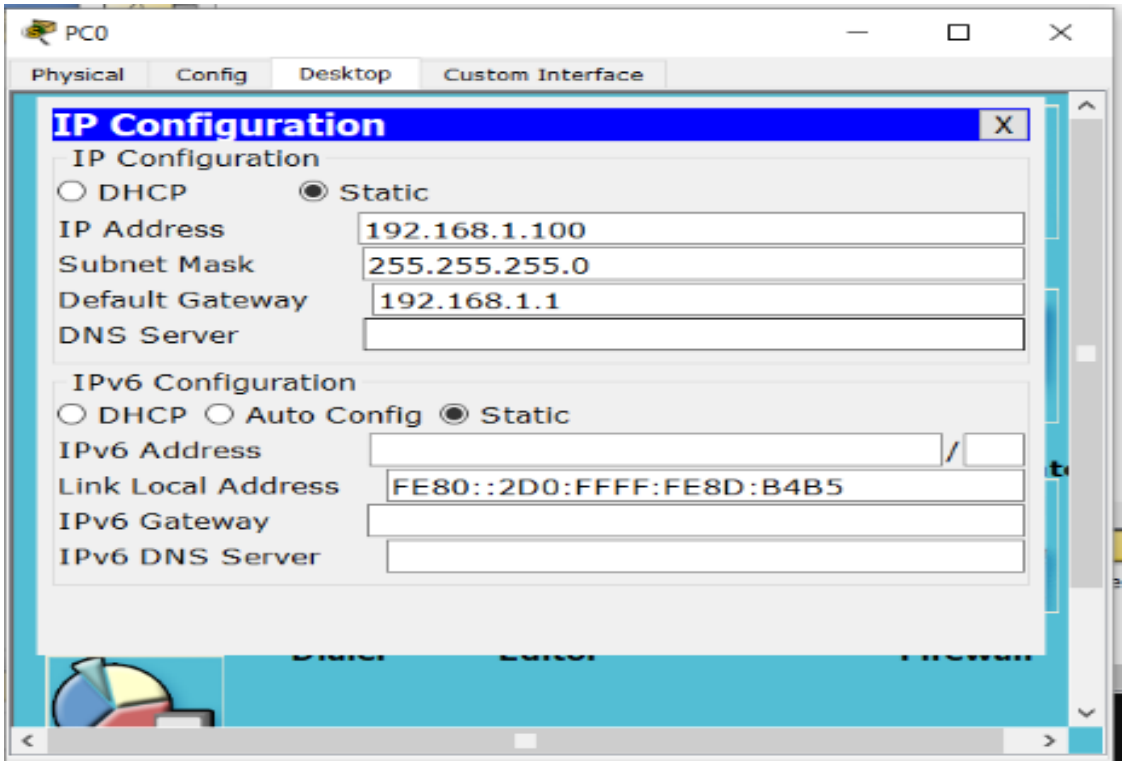


Step 2:

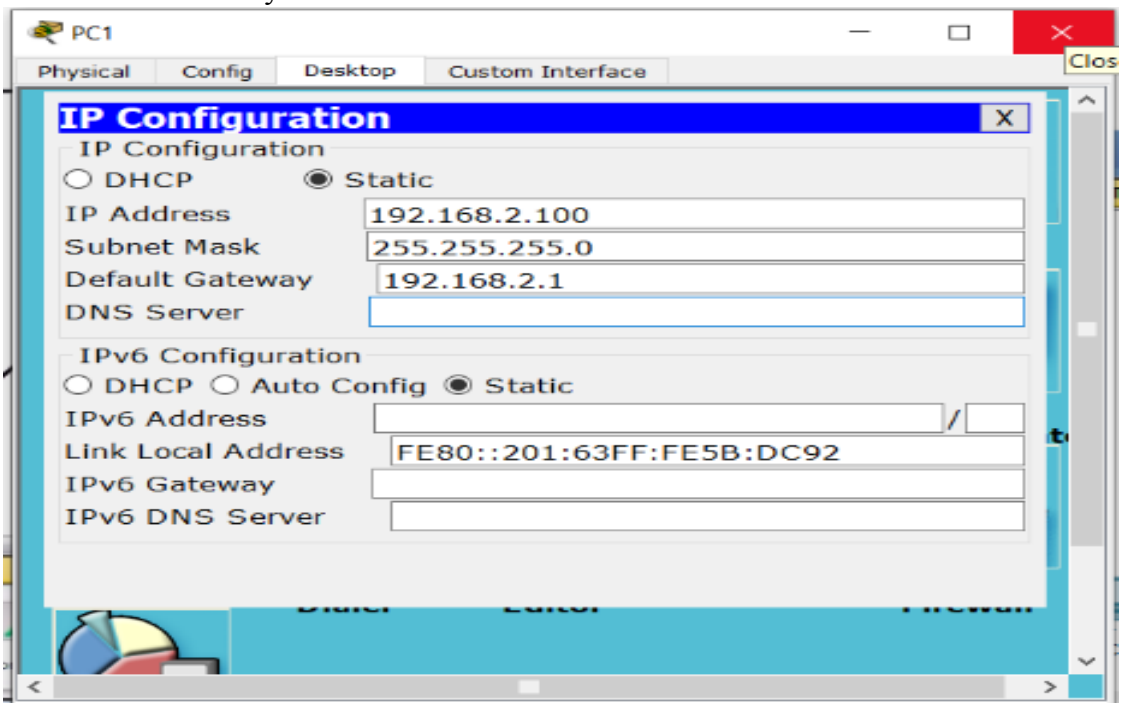
Click on PC0 and go to Desktop > IP Configuration

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

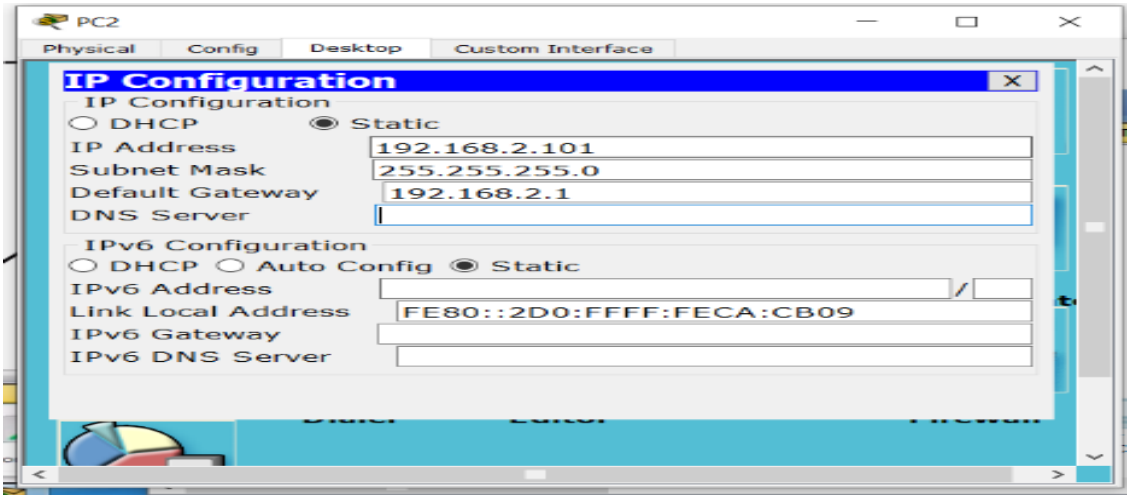
Add Default Gateway and close the window.



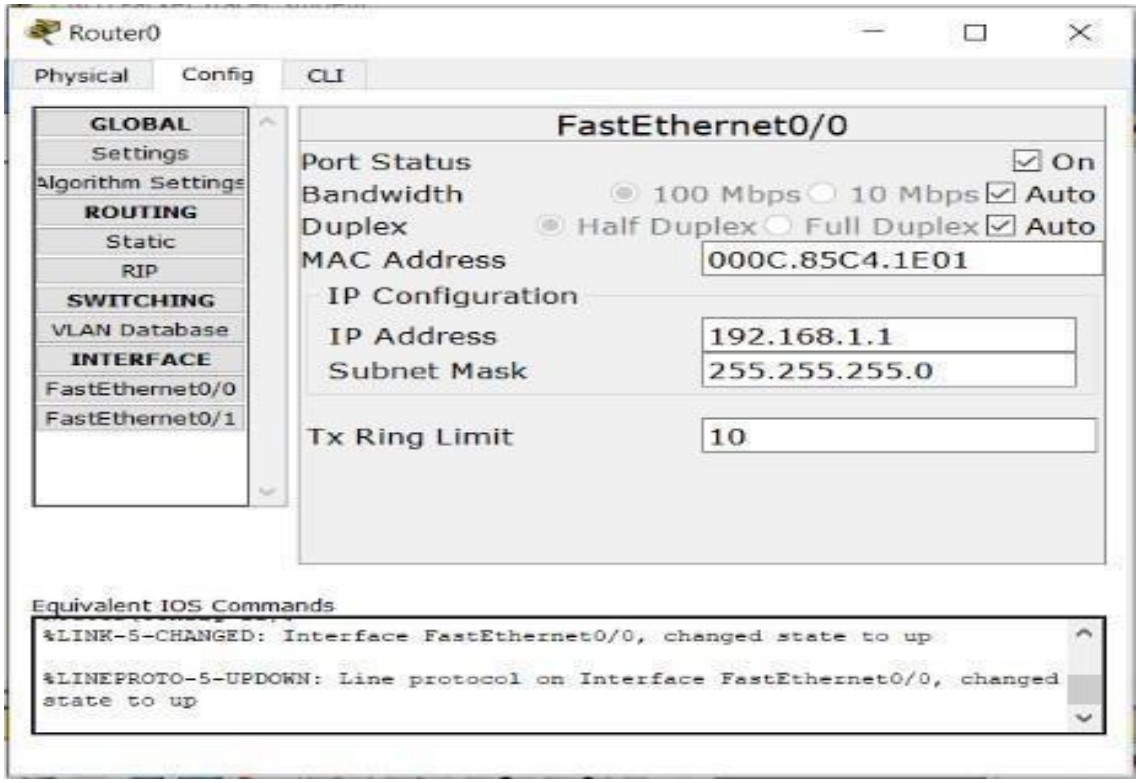
Step 3:
Click on PC1 and go to Desktop > IP Configuration
Add IP Address, as you will add the IP Address, Subnet Mask will be automatically added and displayed.
Add Default Gateway and close the window.



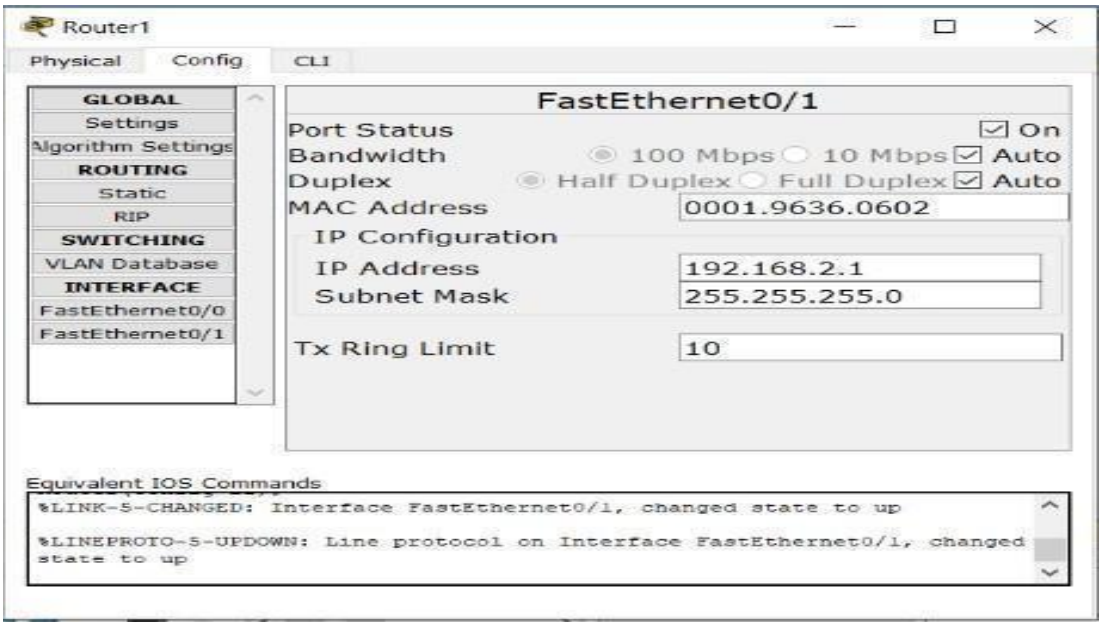
Step 4:
Click on PC2 and go to Desktop > IP Configuration
Add IP Address, as you will add the IP Address, Subnet Mask will be automatically added and displayed.
Add Default Gateway and close the window.

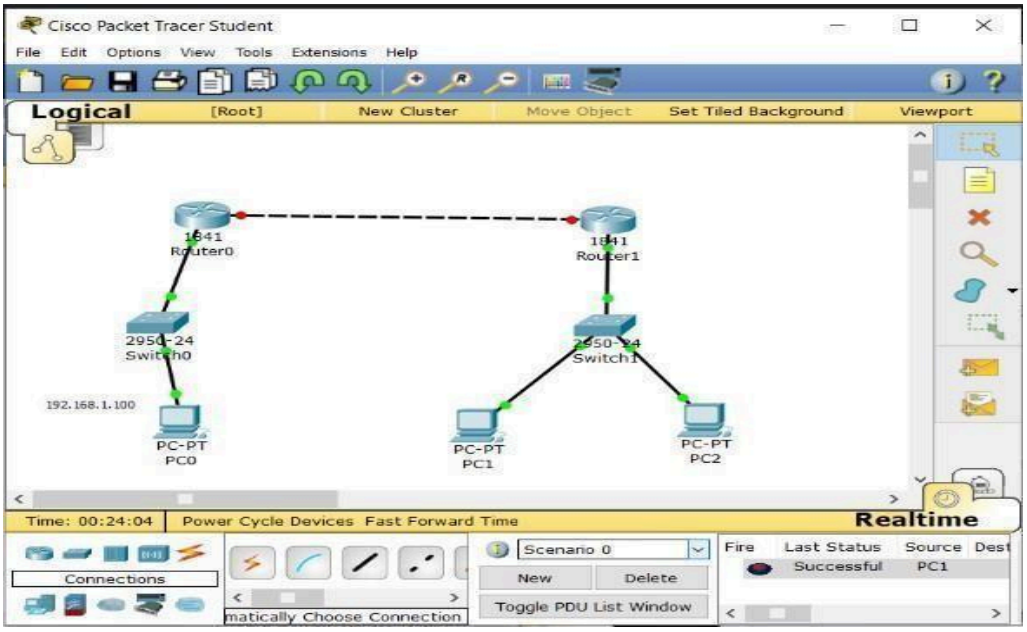


Step 5:
Click on Router0. Go to Config > FastEthernet0/0. Here, add IP Address and On the Port Status.



Step 6:
Click on Router1. Go to Config > FastEthernet0/1. Here, add IP Address and On the Port Status.

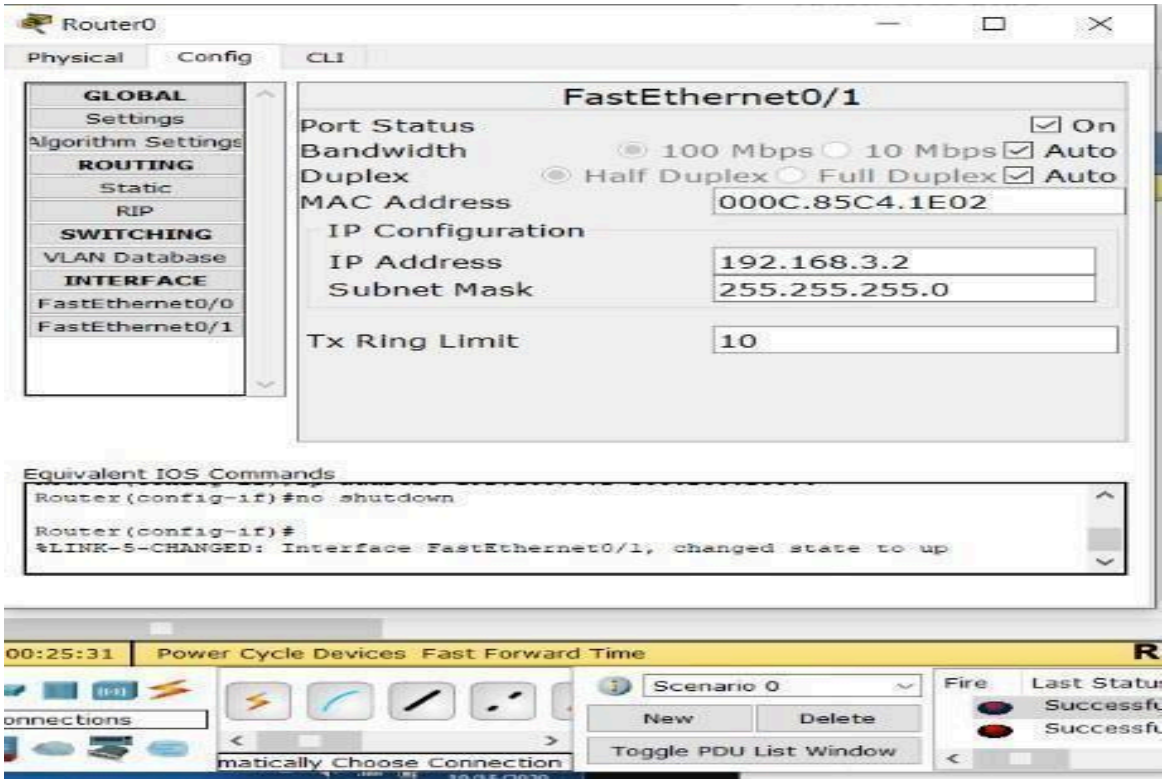




As you will see above, there is green dots which means connections are done successfully between Router, Switches and PCs.

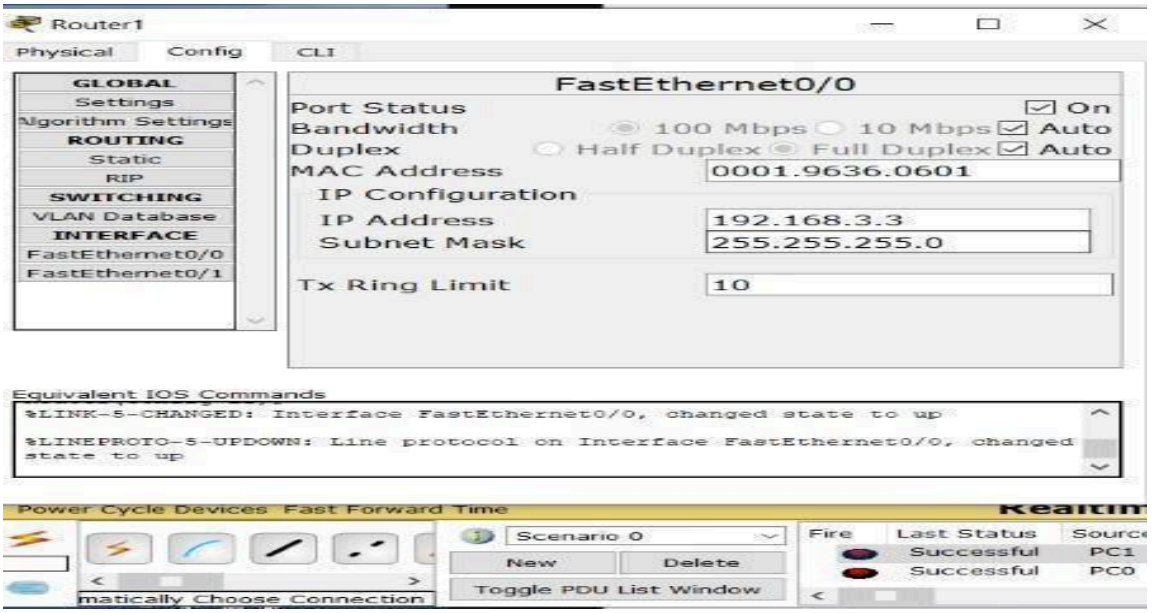
Step 7:

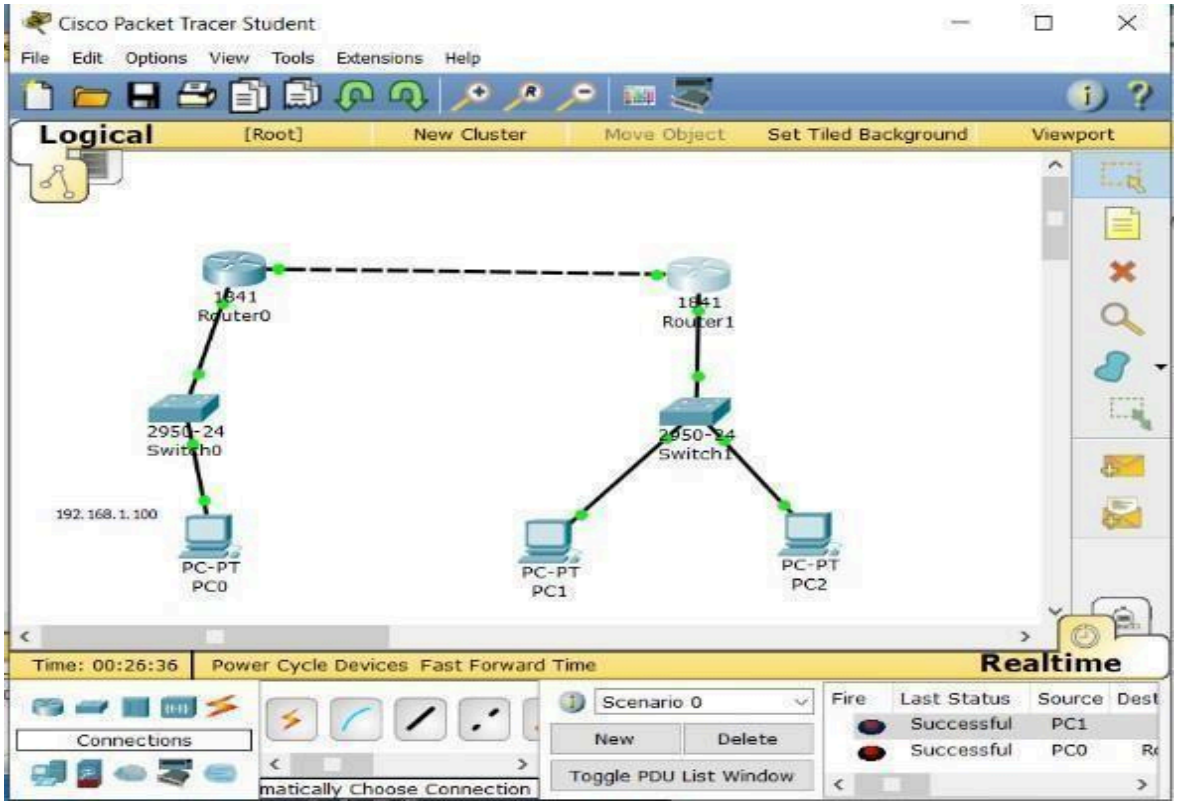
Click on Router0. Go to Config > FastEthernet0/1. Here, add IP Address and On the Port Status.



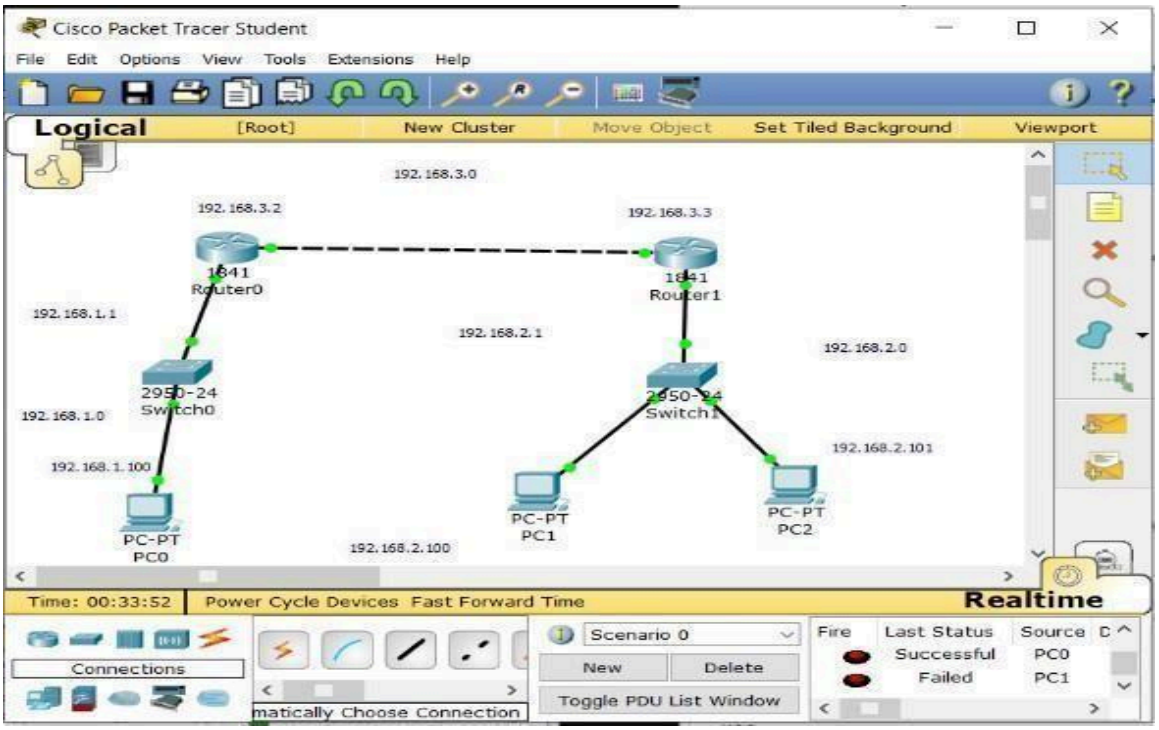
Step 8:

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

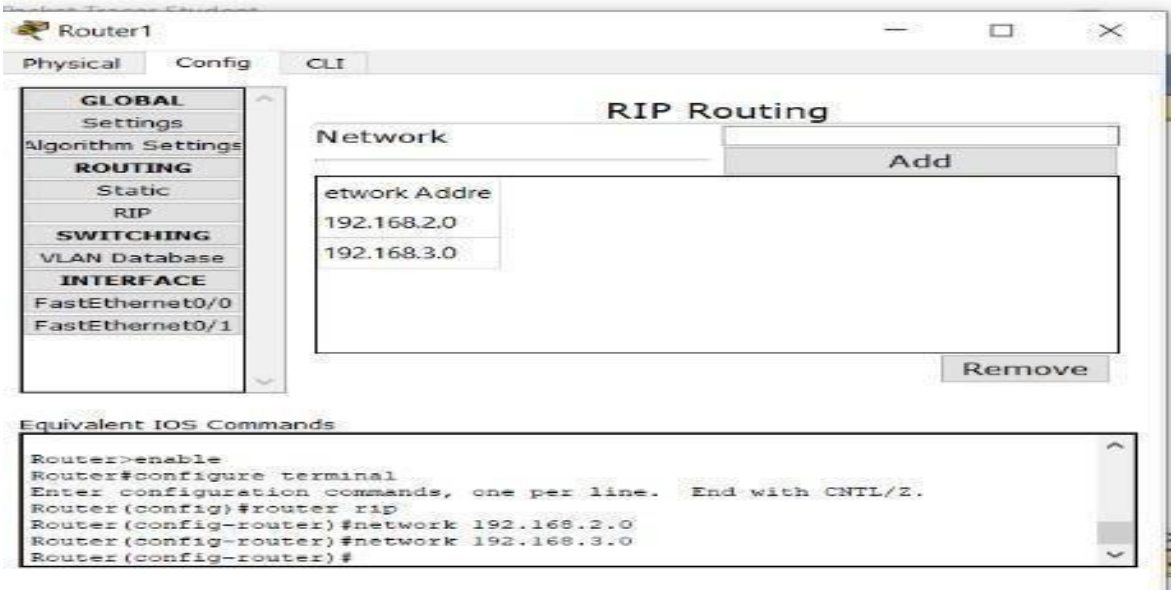




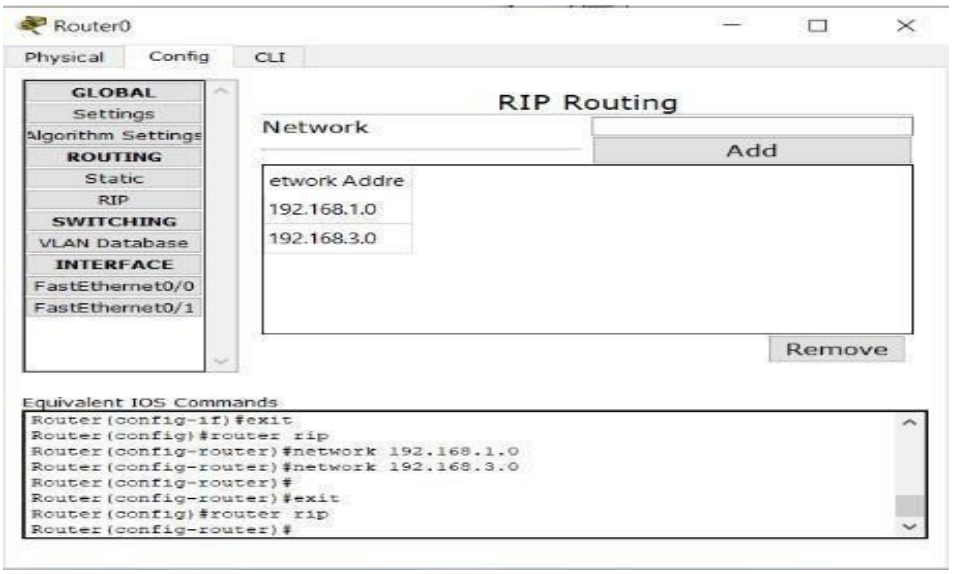
As you can see above, connection is done between both the Routers successfully.



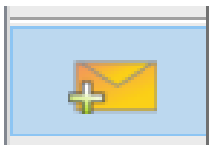
Step 9:
Click on Router1. Go to Config > RIP.
Here, add the network address to connect router1 with switch1, PC1, PC2 and router0.



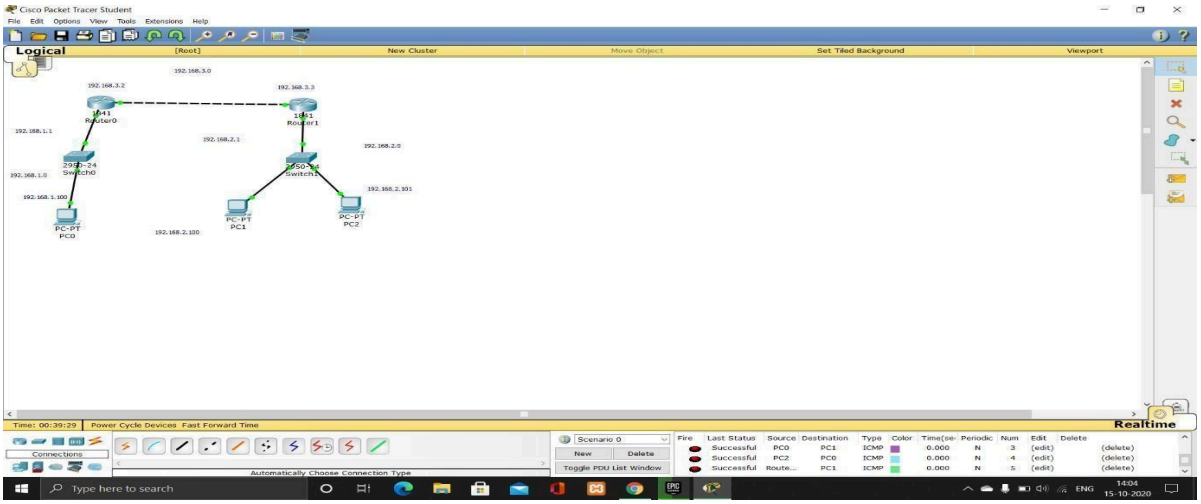
Step 10:
Click on Router0. Go to Config > RIP.
Here, add the network address to connect router0 with switch0, PC0 and router1.



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

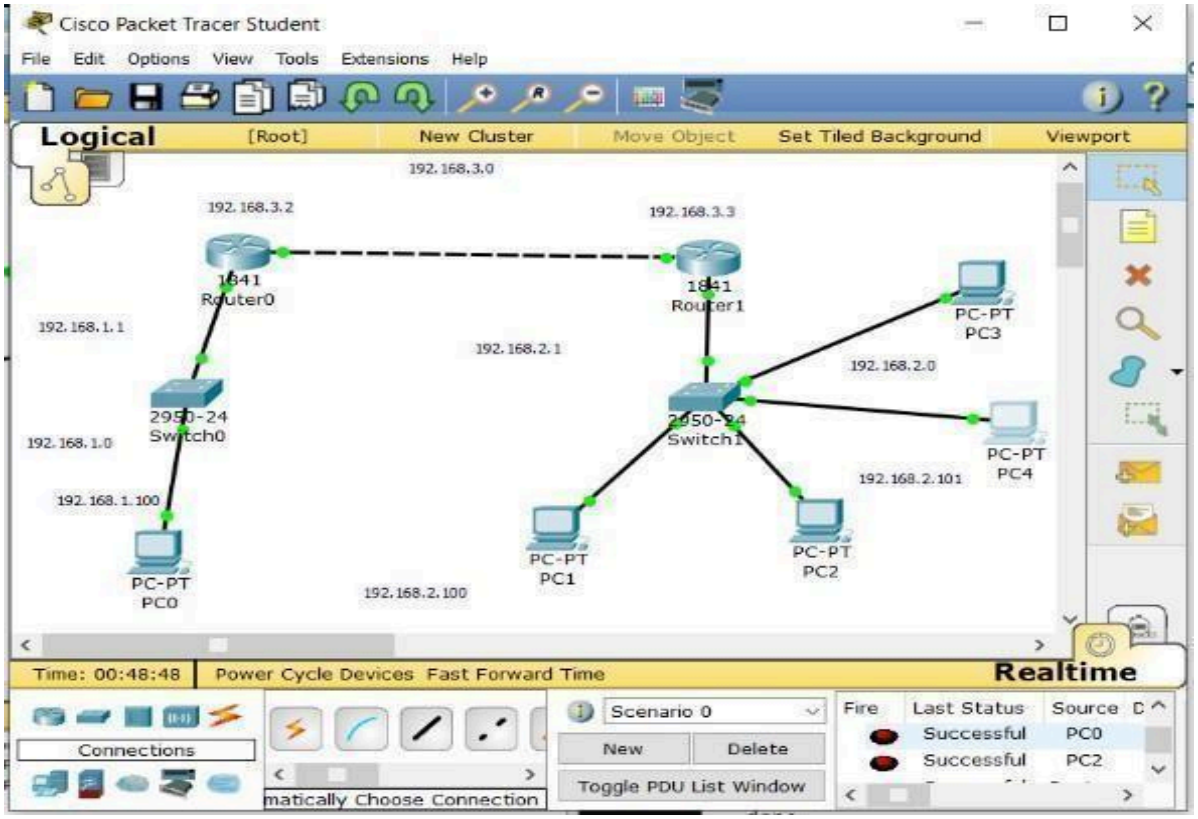


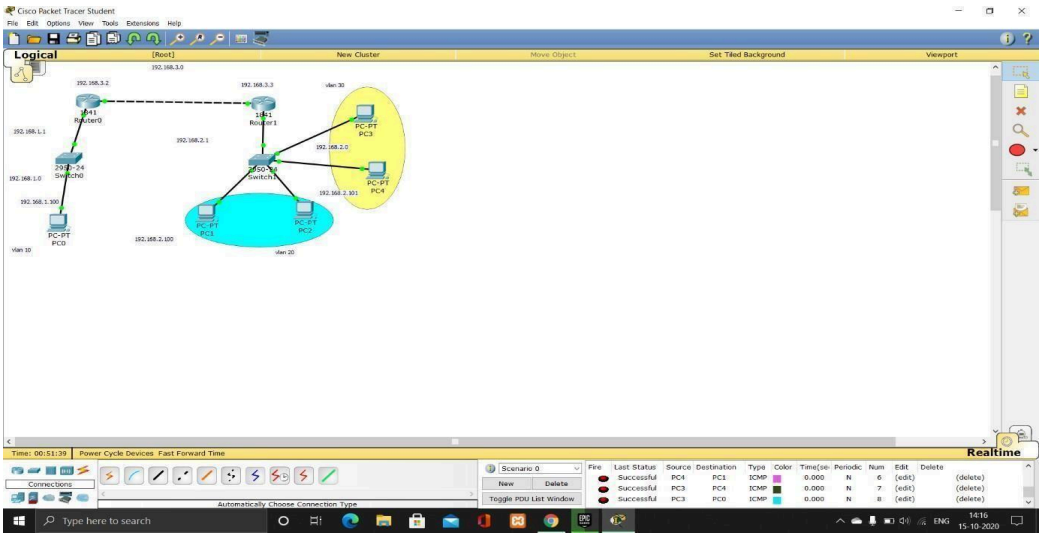
And then, click on any two PCs , you will get the status as successful.



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

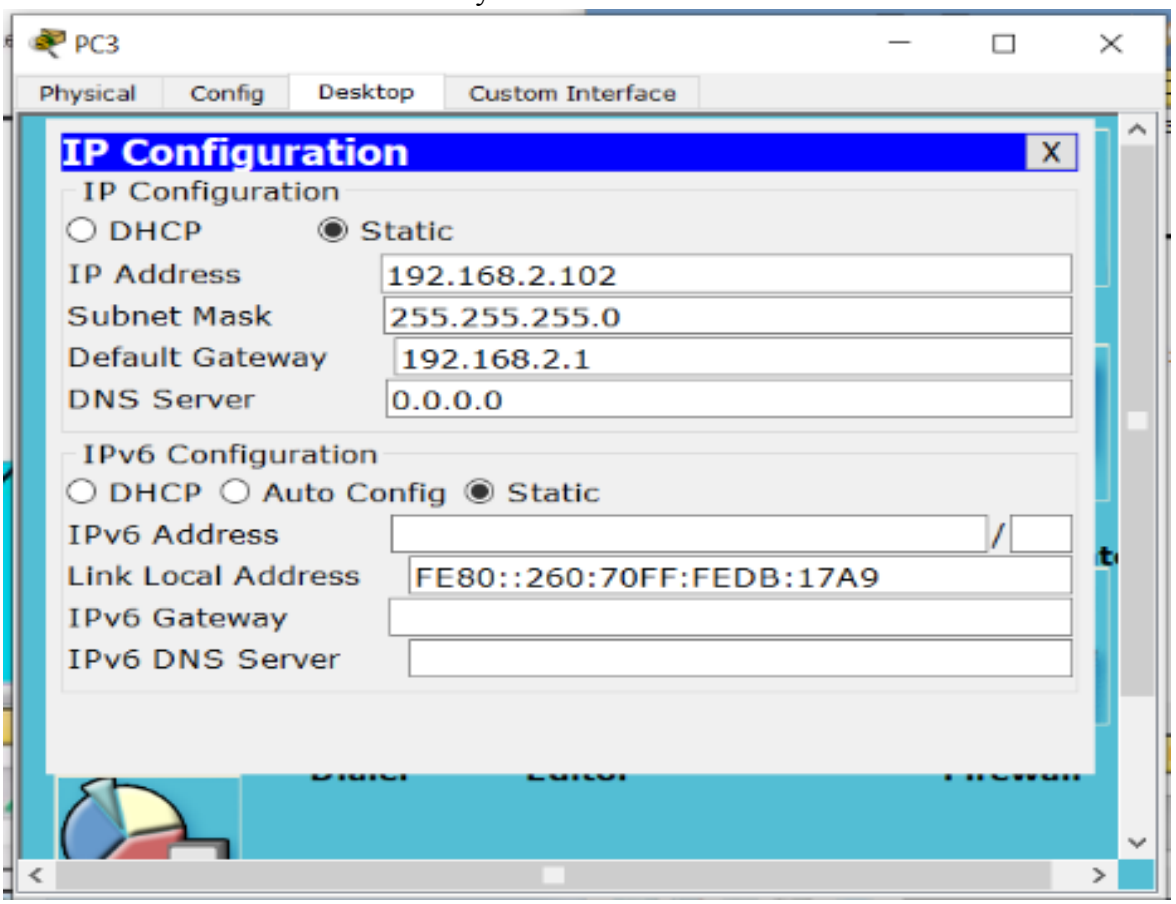
Step 11:
Add two PC (PC 3 and PC4) and connect it with switch.





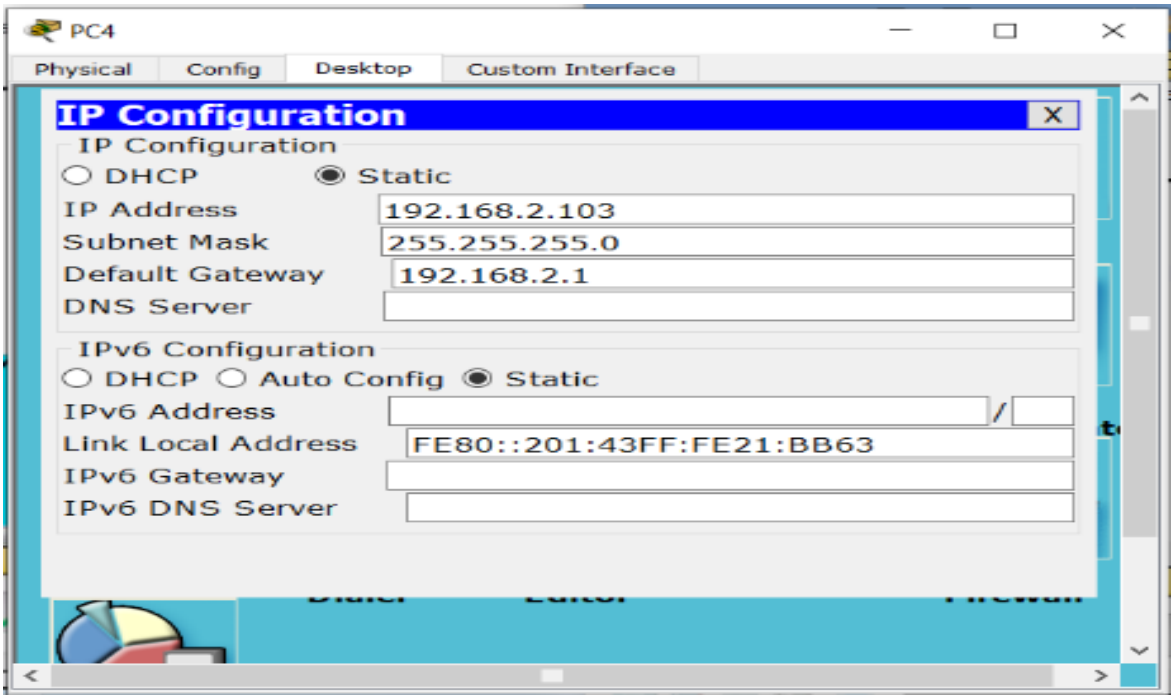
Step 12:
Click on PC3 and go to Desktop > IP Configuration
Add IP Address, as you will add the IP Address, Subnet Mask will be automatically added and displayed.

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

Switch1

Physical Config CLI

IOS Command Line Interface

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed
state to up

%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed
state to up

%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to up

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


Switch>enable
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 20
Switch(config-vlan)#name sales
Switch(config-vlan)#exit
Switch(config)#vlan 30
Switch(config-vlan)#name purchase
Switch(config-vlan)#exit
Switch(config)#
```

Copy Paste

Switch1

Physical Config CLI

IOS Command Line Interface

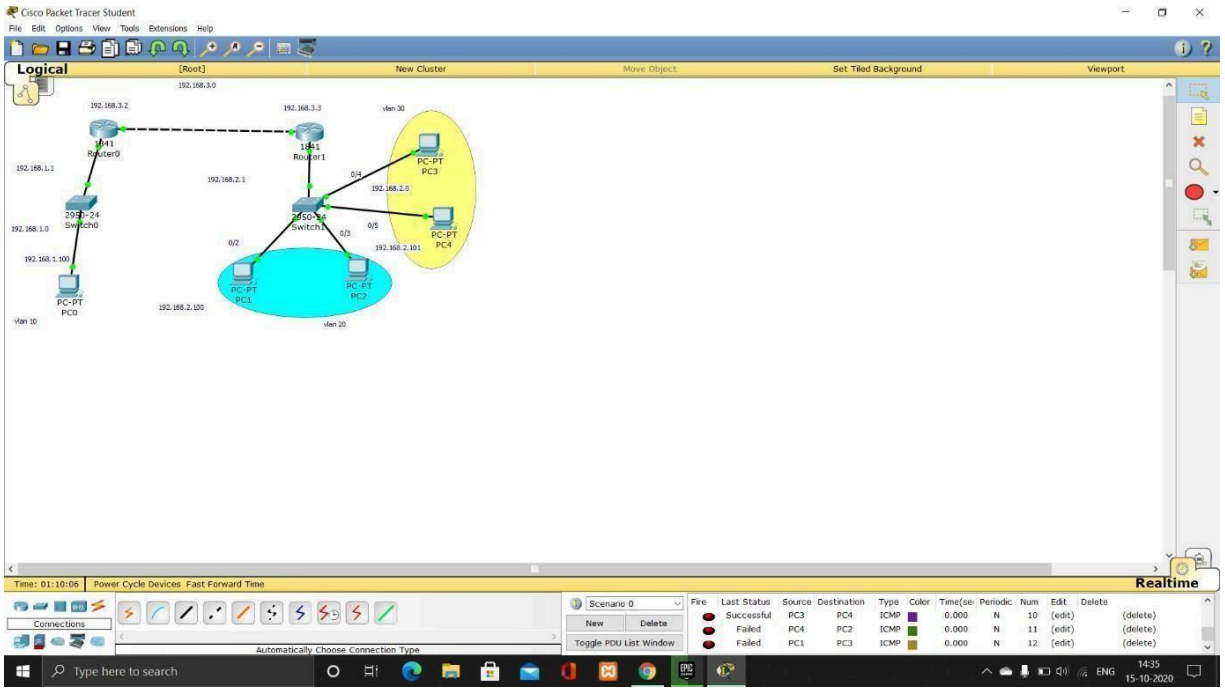
```
state to up


Switch>enable
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 20
Switch(config-vlan)#name sales
Switch(config-vlan)#exit
Switch(config)#vlan 30
Switch(config-vlan)#name purchase
Switch(config-vlan)#exit
Switch(config)#int fa0/2
Switch(config-if)#switchport access vlan 20
Switch(config-if)#exit
Switch(config)#int fa0/3
Switch(config-if)#switchport access vlan 20
Switch(config-if)#exit
Switch(config)#int fa0/4
Switch(config-if)#switchport access vlan 30
Switch(config-if)#exit
Switch(config)#int fa0/5
Switch(config-if)#switchport access vlan 30
Switch(config-if)#exit
Switch(config)#
```

Copy Paste

Final Output:

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



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

EXPERIMENT
NO.09

Title: To study FTP protocol
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 on the "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.

```
#
# Allow anonymous FTP? (Beware - allowed by defau
anonymous_enable=YES
#
# Uncomment this to allow local users to log in.
#local_enable=YES ——— Comment this
#
# Uncomment this to enable any form of FTP write
write_enable=YES
```

Step 3: Restart the vsftpd service

```
[root@server ~]# service vsftpd restart
Shutting down vsftpd:                                      [  OK  ]
Starting vsftpd for vsftpd:                                [  OK  ]
[root@server ~]# _
```

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

```
Applications  Places  System                                  2:24 AM
root@apu:~
File  Edit  View  Terminal  Tabs  Help
[root@apu ~]# ftp 192.168.10.10
Connected to 192.168.10.10.
220 (vsFTPd 2.0.5)
530 Please login with USER and PASS.
530 Please login with USER and PASS.
KERBEROS_V4 rejected as an authentication type
Name (192.168.10.10:root): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pwd
257 "/"
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>
```

```
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

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 ~]#
```

1.Edit VSFTPD configuration file.

```
Applications  Places  System                    2:58 AM
root@apu:~
File  Edit  View  Terminal  Tabs  Help
[root@apu ~]# vi etc/vsftpd/vsftpd.conf
```

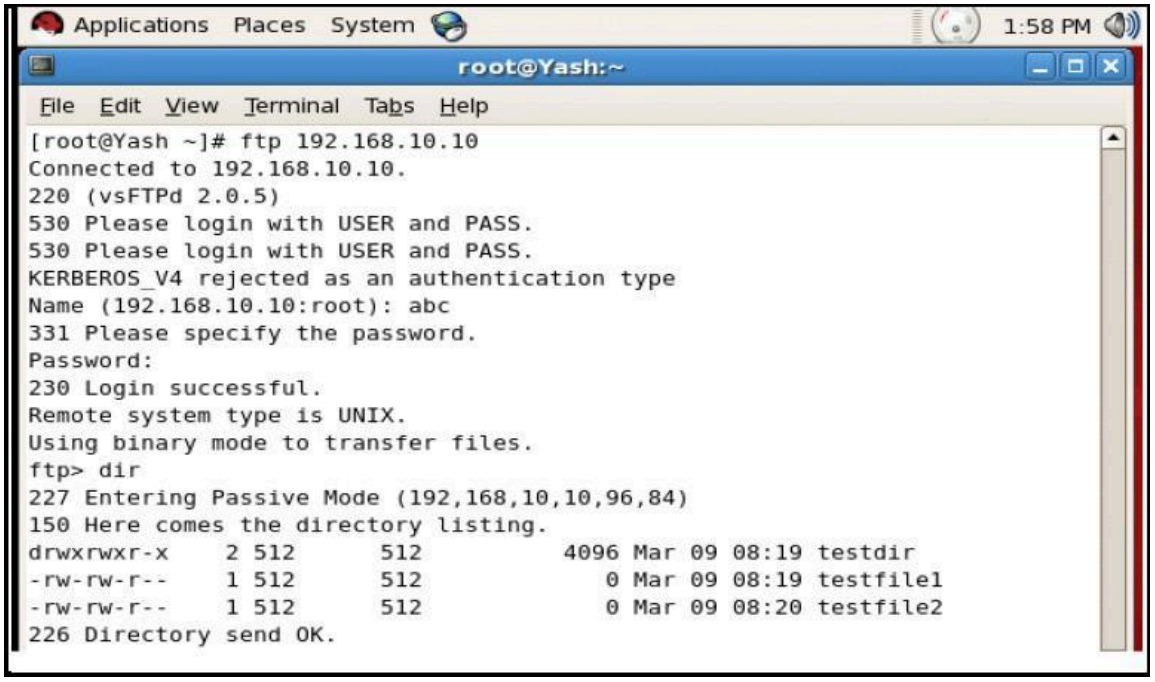
```
# Allow anonymous FTP? (Beware - allowed by default if you comment this out$
anonymous_enable=NO
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
```

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

2.Restart VSFTPD service.

Access FTP server through command prompt

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



upload/download file.

```
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
227 Entering Passive Mode (192,168,10,10,151,62)
150 Here comes the directory listing.
drwxrwxr-x    2 512      512          4096 Mar 09 08:19 testdir
-rw-rw-r--    1 512      512             0 Mar 09 08:19 testfile1
-rw-rw-r--    1 512      512             0 Mar 09 08:20 testfile2
226 Directory send OK.
ftp> get testfile1
local: testfile1 remote: testfile1
227 Entering Passive Mode (192,168,10,10,75,108)
150 Opening BINARY mode data connection for testfile1 (0 bytes).
226 File send OK.
ftp> put testfile1
local: testfile1 remote: testfile1
227 Entering Passive Mode (192,168,10,10,95,176)
150 Ok to send data.
226 File receive OK.
ftp>
```

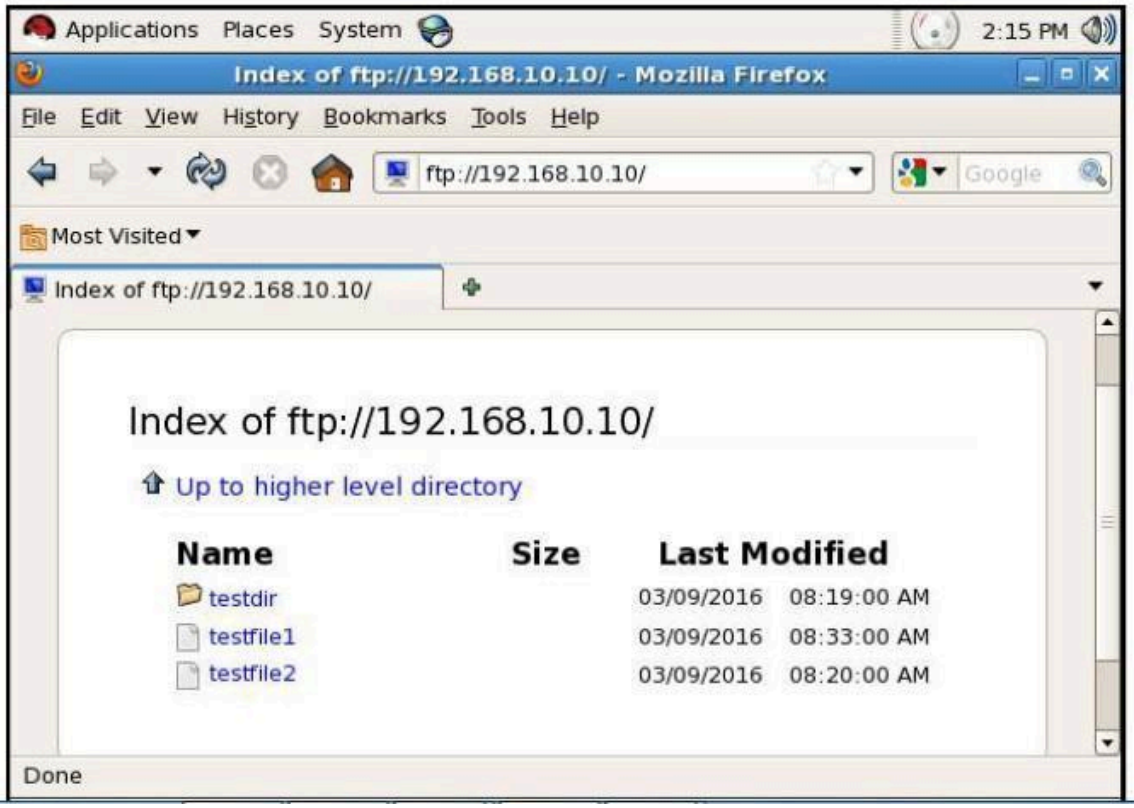
Default location :

```
[root@Yash ~]# ftp 192.168.10.10
Connected to 192.168.10.10.
220 (vsFTPd 2.0.5)
530 Please login with USER and PASS.
530 Please login with USER and PASS.
KERBEROS_V4 rejected as an authentication type
Name (192.168.10.10:root): abc
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pwd
257 "/home/abc"
ftp>
```

- **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.

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 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.10

Title:-To study Telnet protocol

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 a packet 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
0. 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-

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

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

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 ~]# _
```

```
[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.