Mahavir Education Trust's

SHAH & ANCHOR KUTCHHI ENGINEERING COLLEGE

Chembur, Mumbai - 400 088

UG Program in Cyber Security

(POs) Engineering

Graduates will be able to:

1. **Engineering knowledge:** Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.
2. **Problem analysis:** Identify, formulate, review research literature, and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.
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.
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.
5. **Modern tool usage:** Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations.
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.
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.
8. **Ethics:** Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.
9. **Individual and team work:** Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.
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.
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.
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)

By the end of the educational experience our students will be able to:

1. The Cyber Security graduates are able to gain a thorough understanding of the Cyber Security landscape with its growing threats and vulnerabilities in the world of computing including software and hardware.
2. Attain skills to comprehend and anticipate future challenges and devise methods to meet them and also, be articulate and skilled to convince all the stakeholders.
3. The Cyber Security graduates are able to acquire and demonstrate the ability to use ethical standard tools, practices and technologies for the analysis, design, development, implementation and testing of innovative and optimal Cyber Security solutions without compromising the privacy needs of individual and entities and the security concerns of law enforcement agencies.

Mapping of PSOs to POs:

PSO Number	**PO Number**
PSO1	PO1, PO2, PO6,
PSO2	PO4, PO9, PO10,
POS3	PO3, PO5, PO7, PO8, PO11 PO12

Asha

**Dr. Asha
Durafe Program
Coordinator Cyber
Security Program**

Mahavir Education Trust's

SHAH & ANCHOR KUTCHHI ENGINEERING COLLEGE

Chembur, Mumbai - 400 088

UG Program in Cyber Security

Lab Code	CSL502	**Lab Name**	Computer Network Lab
Academic Year	2022-2023	**Semester**	V
Class	TE15	**Lab Coordinator**	Mrs.Rashmi Patel

Laboratory Outcomes (LO)

LO No.	**LO Statement** (At the end of the course, students will be able to …)	
CSL5021	Identify type of cables and understand connection using crimping tool,	3
CSL5022	Setup networking environment in Linux to understand Network commands and use of various tools such as wireshark, Nmap, iptables	3
CSL5023	Perform various server configurations in Linux	3
CSL5024	Design client server model using socket programming	3
CSL5025	Setup a Network using Cisco packet tracer and implement static routing.	4
CSL5026	Use of Cisco packet tracer to design VPN and explore networking algorithms.	3

List of Experiments

Sr. No.	Title	LO	PSO	PI
1	Study of RJ45 and CAT6 Cabling and connection using crimping tool.	1	1,2	1.3.1,2.2.1,2.2.2, 5.1.1,5.2.2
2	Use basic networking commands in Linux (ping, tracert, nslookup, netstat, ARP, RARP, ip, ifconfig, dig, route)	2	1,2	1.3.1,2.2.1,4.1.1, 4.1.2,3.1,4.3.2 .4.3.3,4.3.3,5.1.1, 5.2. 2,9.2.1
3	Build a simple network topology and configure it for static routing protocol using packet tracer. Setup a network and configure IP addressing, subnetting, masking.	5	1,2	1.3.1,2.2.1,4.1.1,4.1 .3,4.2.1,4. 3.1,4.3.2.4.3.3,4.3.3 ,5.1.1,5.2. 2,9.2.1

4	Perform network discovery using discovery tools (eg. Nmap, mrtg)	2	1,2	1.3.1,2.2.1, ,4.1.1,4.1.2,4.1.3,4.2.1,4.3.1,5.1.1,5.2.2,8.1.1, 10.1.1,10.1.2, 10.1.3
5	Use Wire shark to understand the operation of TCP/IP layers: ● Ethernet Layer: Frame header, Frame size etc. ● Data Link Layer: MAC address, ARP (IP and MAC address binding) ● Network Layer: IP Packet (header, fragmentation), ICMP (Query and Echo) ● Transport Layer: TCP Ports, TCP handshake segments etc. Application Layer: DHCP, FTP, HTTP header formats	2	1,2	1.3.1,2.2.1, ,4.1.1,4.1.2,4.1.3,4.2.1,4.3.1,5.1.1,5.2.2,10.1.1,10.1.2, 10.1.3
6	a. Set up multiple IP addresses on a single LAN. b. Using netstat and route commands of Linux, do the following: ● View current routing table ● Add and delete routes ● Change default gateway Perform packet filtering by enabling IP forwarding using IPtables in Linux.	3	1,2	1.3.1,2.2.1,4.1.1,4.1.2, 3.1,4.3.2.4.3.3,4.3.3,5.1.1,5.2.2,9.2.1
7	Design VPN and Configure RIP/OSPF using Packet tracer.	6	1,2	1.3.1,2.2.1, ,4.1.1,4.1.2,4.1.3,4.2.1,4.3.1,4.3.2.4.3.3
8	Socket programming using TCP or UDP	4	1,2	1.3.1,2.1.1,2.1.3,.2.4,2.2.5,4.3.3,5.1.1,5.2.1,8.

				1.1,10.1.1,10.1.2,10.1.3
9	Perform File Transfer and Access using FTP	3	1,2	1.3.1,2.2.1, ,4.1.1,4.1.2,4.1.3,4.2.1,4.3.1,5.1.1,5.2.2,8.1.1,10.1.1,10.1.2, 10.1.3
10	Perform Remote login using Telnet server	3	1,2	1.3.1,2.2.1, ,4.1.1,4.1.2,4.1.3,4.2.1,4.3.1,5.1.1,5.2.2,8.1.1, 10.1.1,10.1.2, 10.1.3
11	Study and implement SNMP format.	3	1,2	1.3.1,2.1.1,2.1.3,.2.4,2.2.5,4.3.3,5.1.1,5.2.1,8.1.1,10.1.1,10.1.2,10.1.3

PPatel

Name:Mrs. Rashmi Patel **Signature:**

Date:

Mahavir Education Trust's

SHAH & ANCHOR KUTCHHI ENGINEERING COLLEGE

Chembur, Mumbai - 400 088

UG Program in Cyber Security

Mahavir Education Trust's

SHAH & ANCHOR KUTCHHI ENGINEERING COLLEGE

Chembur, Mumbai - 400 088

UG Program in Cyber Security

Experiment Number:					
Date of Performance:	**03-08-2022**				
Date of Submission:	**10-08-2022**				
Program Execution/ formation/ correction/ ethical practices (07)	**Documentation (02)**	**Timely Submission (03)**	**Viva Answer to sample questions (03)**	**Experiment Total (15)**	**Sign**
07	02	03	03	15	PPatel

Experiment No. 1

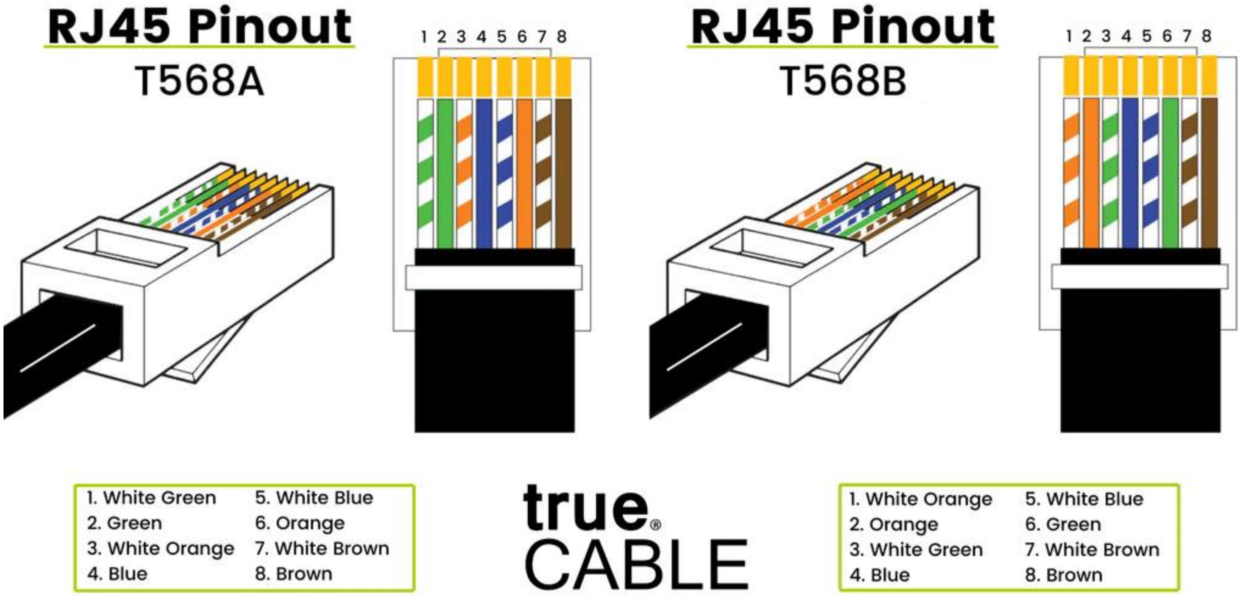
Aim: Study of RJ45 and CAT6 Cabling and connection using crimping tool.

Laboratory Outcome: CSL 5021

Problem Statement: Study of RJ45 and CAT6 Cabling and connection using crimping tool.

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

T568A and T568B are the termination standards used by Internet backbone infrastructure, Internet providers and all the way down to homeowners or businesses. The only real difference between these two pin-to-pair assignments are the green and orange pairs. These two sets are swapped in the cable. Even though these are switched, they are still both effectively direct or “straight through” connections.

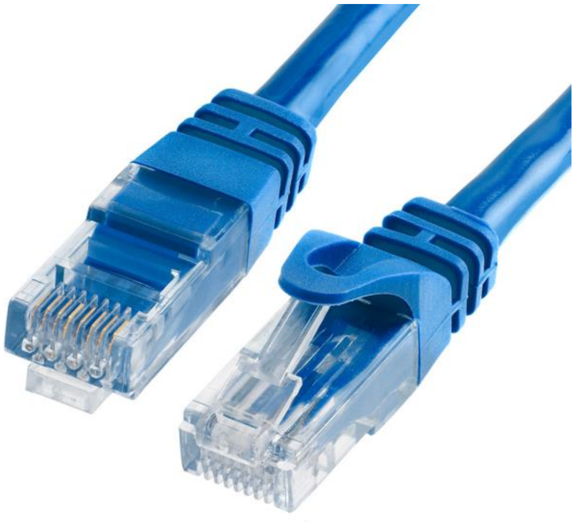


Cat5 cable : Category 5 **cable** (**Cat 5)** is a twisted pair **cable** for computer networks.Since 2001, the variant commonly in use is the Category 5e specification (Cat 5e).The **cable** standard provides performance of up to 100 MHz and is suitable for most varieties of Ethernet over twisted pair up to 2.5GBASE-T but more commonly runs at 1000BASE-T (Gigabit Ethernet) speeds.

Cat 5 cable

Cat 5e cable

Cat 6 cable : **Category 6 cable** (**Cat 6**) is a standardized twisted pair cable for Ethernet and other network physical layers that is backward compatible with the Category 5/5e and Category 3 cable standards. Cat 6 must meet more stringent specifications for crosstalk and system noise than Cat 5 and Cat 5e. The cable standard specifies performance of up to 250 MHz, compared to 100 MHz for Cat 5 and Cat 5e.

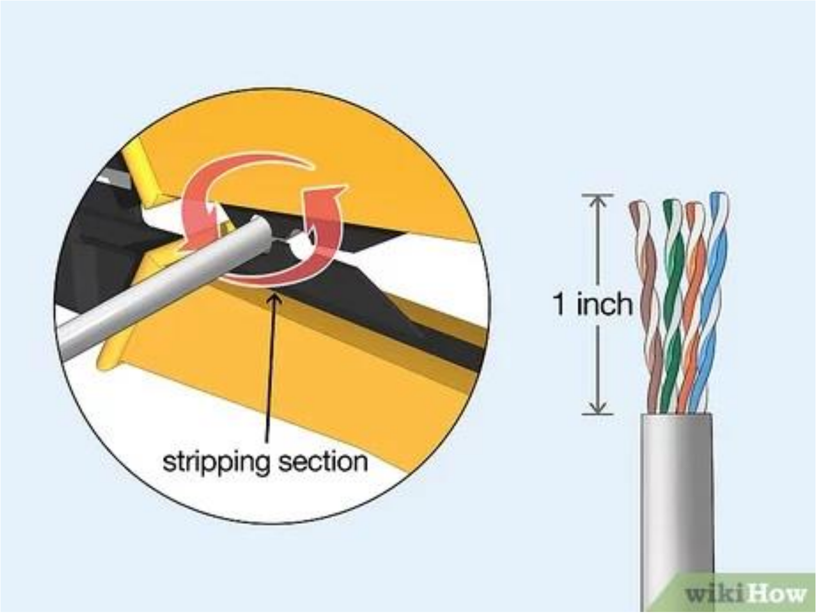


Crimping Tools : First, you’ll need the correct crimp tool. Check if your application requires using specific brands of crimp machines. If not, it’s enough to check if the device is working.

- Wire strippers. This handheld tool is essential to remove insulation from an electrical connection wire.
- Crimp terminals. You use this part for crimp terminations, which makes it vital for the process.
- Heat-shrink systems. Thanks to this part, you can place plastic insulation around the wires.

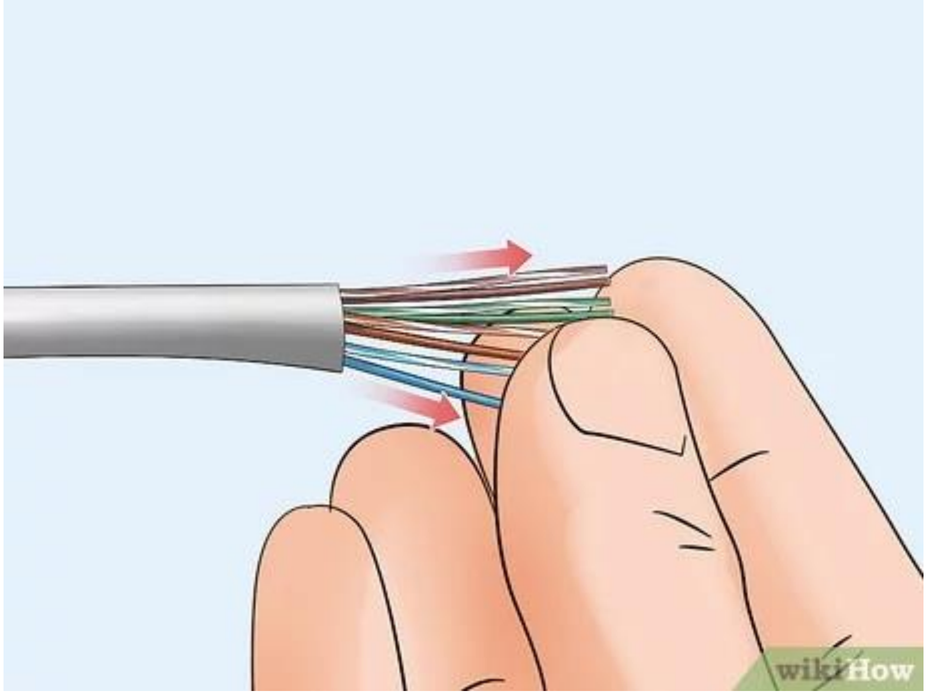
Step 1 : Strip the cable back 1 inch (25 mm) from the end. Insert the cable into the stripper section of the tool and squeeze it tight. Then, rotate the crimping tool around the cable in a smooth and even motion to create a clean cut. Keep the tool clamped and pull away towards the end of the wire to 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.



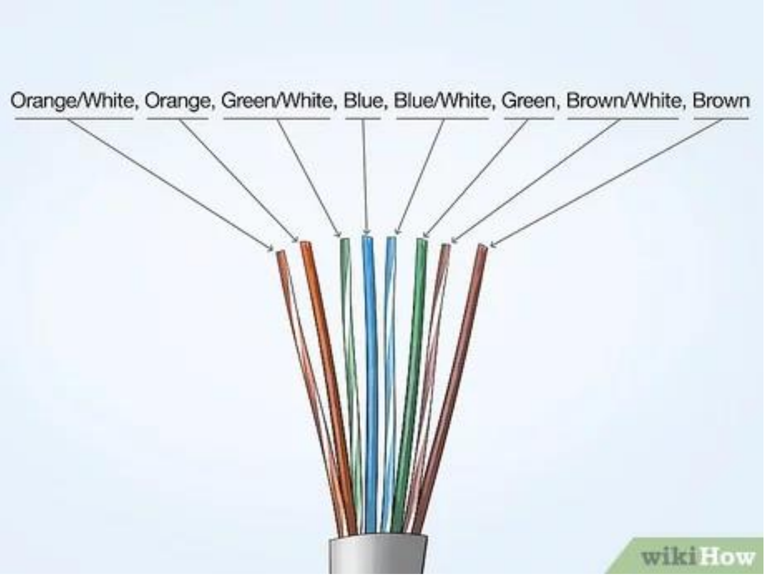
Step 2 : Untwist and straighten the wires inside of the cable. Inside of the cable you’ll see a bunch of smaller wires twisted together. Separate the twisted wires and straighten them out so they’re easier to sort into the right order.

- 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.



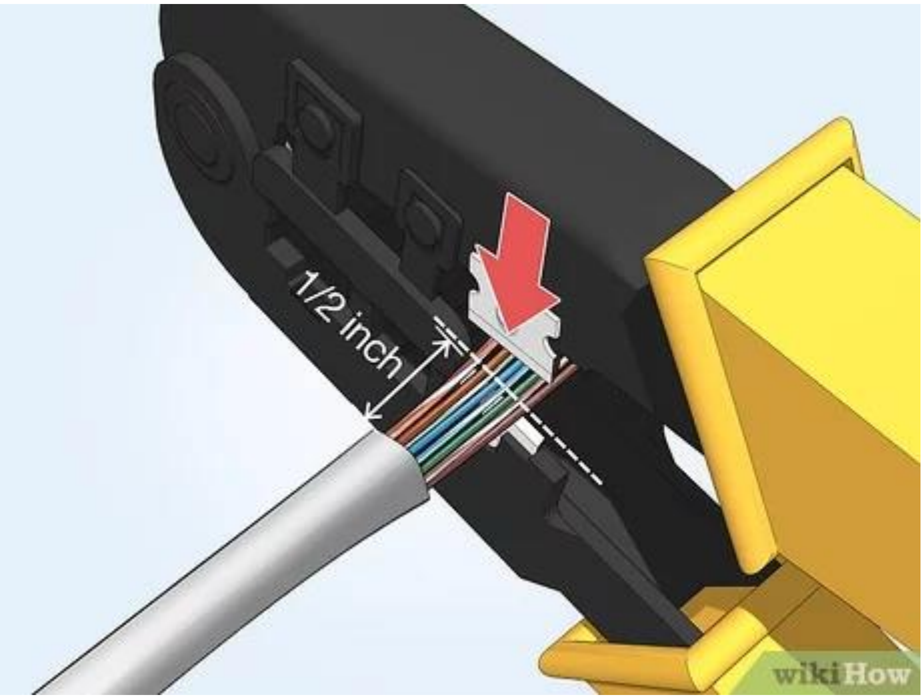
Step 3 : Arrange the wires into the right order. Use your fingers to put the wires in the correct order so they can be properly crimped. The proper sequence is as follows from left to right: Orange/White, Orange, Green/White, Blue, Blue/White, Green, Brown/White, Brown.

- 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.


Orange/White, Orange, Green/White, Blue, Blue/White, Green, Brown/White, Brown
wikiHow

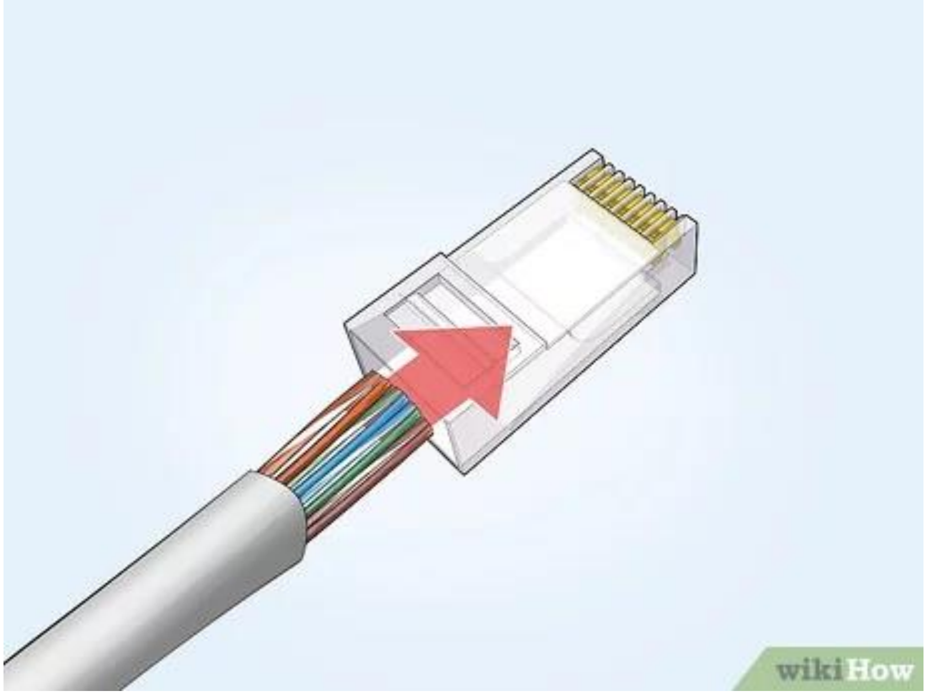
Step 4 : Cut the wires into an even line ½ inch (13 mm) from sheathing. Hold the wires with your thumb and index finger to keep them in order. Then, use the cutting section of the crimping tool to cut them into an even line.

- 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.



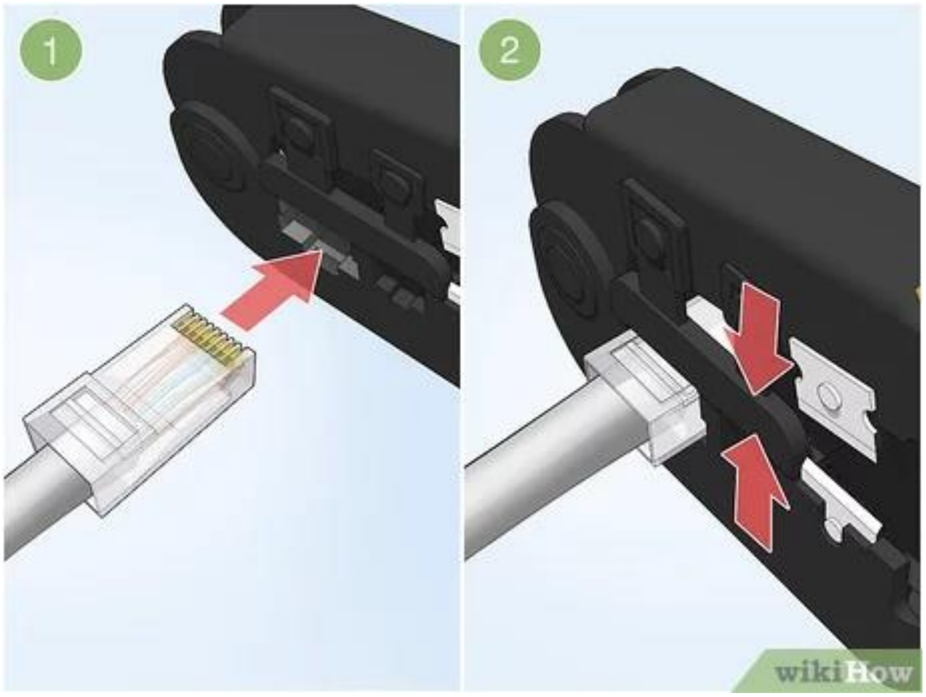
Step 5 : Insert the wires into the RJ-45 connector. Hold the RJ-45 connector so the clip is on the underside and the small metal pins are facing up. Insert the cable into the connector so that each of the small wires fits into the small grooves in the connector.

- 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.



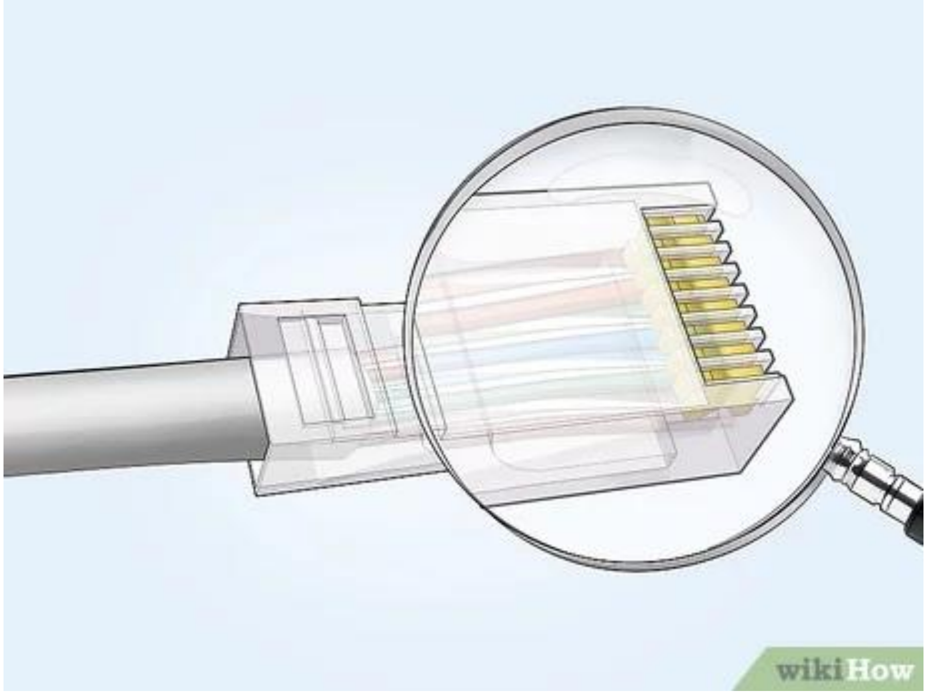
Step 6 : Stick the connector into the crimping part of the tool and squeeze twice. Insert the connector in the crimping section of the tool until it can’t fit any further. Squeeze the handles to crimp the connector and secure the wires. Release the handles, then squeeze the tool again to make sure all 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.



Step 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.



Conclusion: Able to connect RJ45 and CAT6 cable using crimping tool.

Mahavir Education Trust's

SHAH & ANCHOR KUTCHHI ENGINEERING COLLEGE

Chembur, Mumbai - 400 088

UG Program in Cyber Security

Experiment Number:					
Date of Performance:		10-08-2022			
Date of Submission:		17-08-2022			
Program Execution/ formation/ correction/ ethical practices (07)	**Documentation (02)**	**Timely Submission (03)**	**Viva Answer to sample questions (03)**	**Experiment Total (15)**	**Sign**
07	02	03	03	15	PPatel

Experiment No. 2

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

Laboratory Outcome: CSL5022

Related Theory: Every computer is connected to some other computer through a network whether internally or externally to exchange some information. This network can be small as some computers connected in your home or office, or can be large or complicated as in large University or the entire Internet.

Maintaining a system's network is a task of System/Network administrator. Their task includes network configuration and troubleshooting.

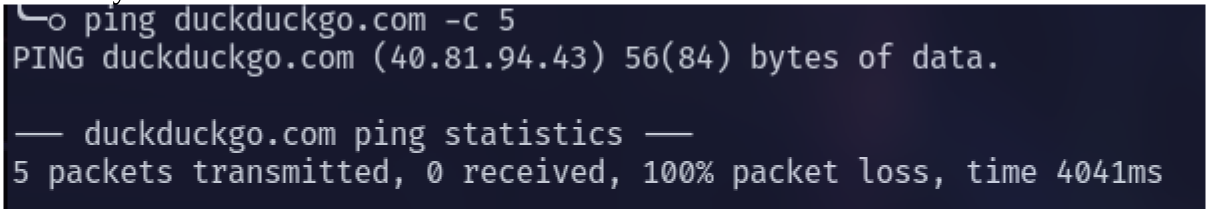
Program Listing And Output:

1. Ping :

PING (Packet Internet Groper) command is used to check the network connectivity between host and server/host.

OS:Linux.

syntax :

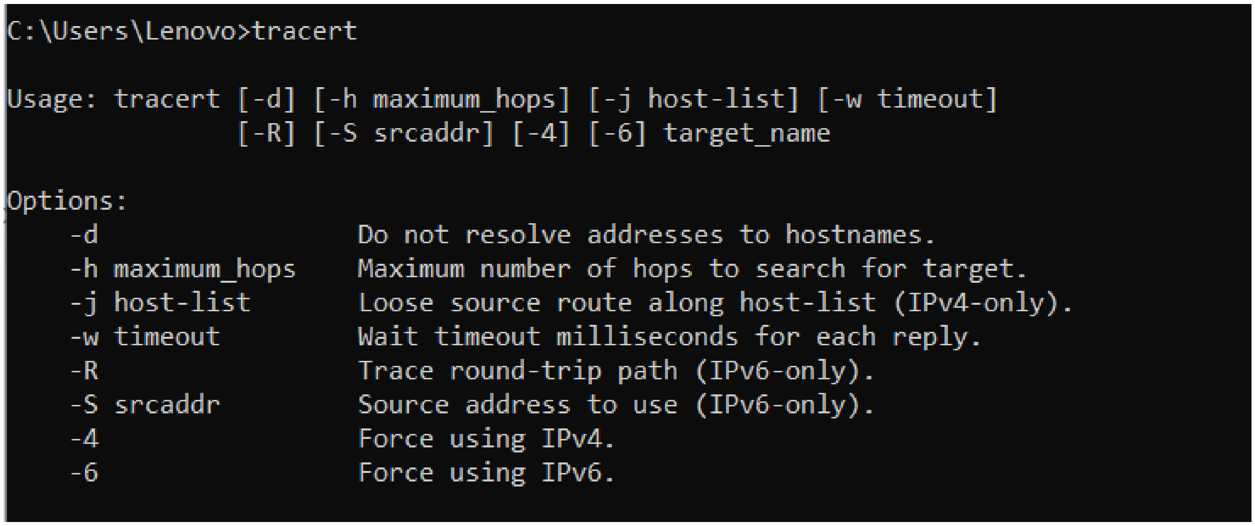


```
╰─o ping duckduckgo.com -c 5
PING duckduckgo.com (40.81.94.43) 56(84) bytes of data.

--- duckduckgo.com ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4041ms
```

2.Tracert :

tracert will only use ICMP echo requests.

OS: Windows.

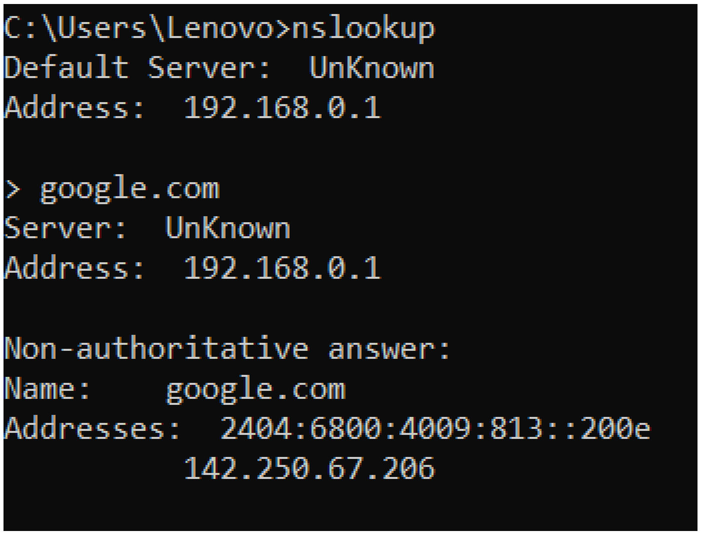


```
C:\Users\Lenovo>tracert

Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
               [-R] [-S srcaddr] [-4] [-6] target_name

Options:
    -d                 Do not resolve addresses to hostnames.
    -h maximum_hops    Maximum number of hops to search for target.
    -j host-list       Loose source route along host-list (IPv4-only).
    -w timeout         Wait timeout milliseconds for each reply.
    -R                 Trace round-trip path (IPv6-only).
    -S srcaddr         Source address to use (IPv6-only).
    -4                 Force using IPv4.
    -6                 Force using IPv6.
```

3. nslookup :

Nslookup (stands for “Name Server Lookup”) is a useful command for getting information from the DNS server.

OS:Linux and windows.



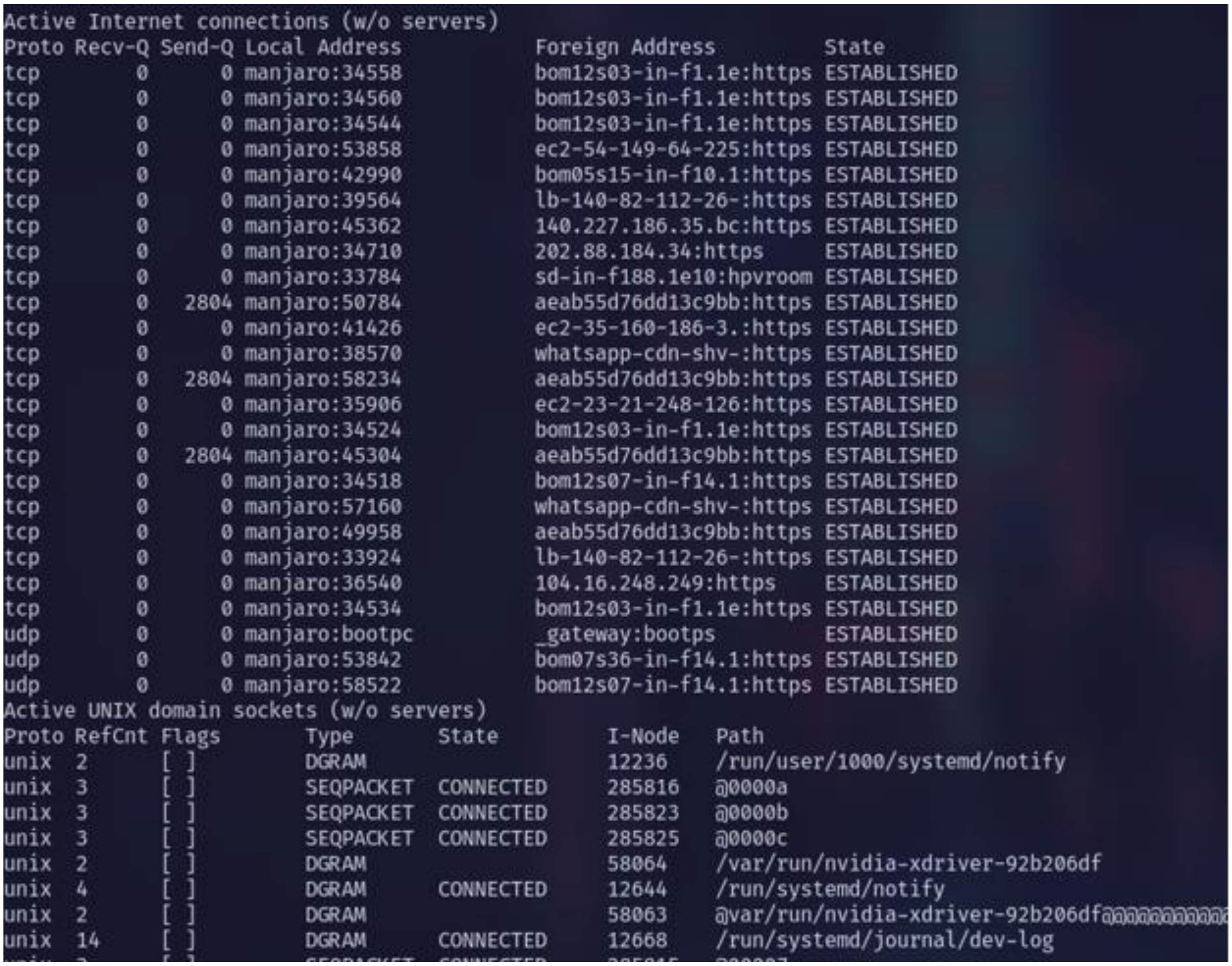
```
C:\Users\Lenovo>nslookup
Default Server:  UnKnown
Address:  192.168.0.1

> google.com
Server:  UnKnown
Address:  192.168.0.1

Non-authoritative answer:
Name:    google.com
Addresses:  2404:6800:4009:813::200e
          142.250.67.206
```

4. netstat :

The network statistics (netstat) command is a networking tool used for troubleshooting and configuration, that can also serve as a monitoring tool for connections over the network.

OS: Linux and windows.

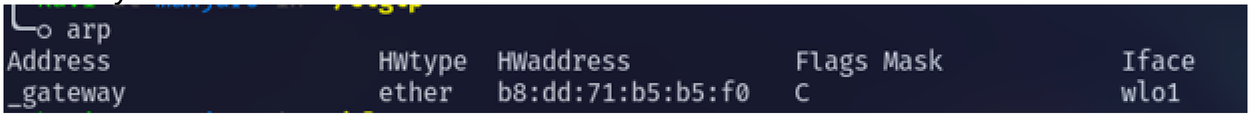
syntax :



```
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 manjaro:34558           bom12s03-in-f1.1e:https ESTABLISHED
tcp        0      0 manjaro:34560           bom12s03-in-f1.1e:https ESTABLISHED
tcp        0      0 manjaro:34544           bom12s03-in-f1.1e:https ESTABLISHED
tcp        0      0 manjaro:53858           ec2-54-149-64-225:https ESTABLISHED
tcp        0      0 manjaro:42990           bom05s15-in-f10.1:https ESTABLISHED
tcp        0      0 manjaro:39564           lb-140-82-112-26-:https ESTABLISHED
tcp        0      0 manjaro:45362           140.227.186.35.bc:https ESTABLISHED
tcp        0      0 manjaro:34710           202.88.184.34:https     ESTABLISHED
tcp        0      0 manjaro:33784           sd-in-f188.1e10:hpvroom ESTABLISHED
tcp        0   2804 manjaro:50784           aeab55d76dd13c9bb:https ESTABLISHED
tcp        0      0 manjaro:41426           ec2-35-160-186-3.:https ESTABLISHED
tcp        0      0 manjaro:38570           whatsapp-cdn-shv-:https ESTABLISHED
tcp        0   2804 manjaro:58234           aeab55d76dd13c9bb:https ESTABLISHED
tcp        0      0 manjaro:35906           ec2-23-21-248-126:https ESTABLISHED
tcp        0      0 manjaro:34524           bom12s03-in-f1.1e:https ESTABLISHED
tcp        0   2804 manjaro:45304           aeab55d76dd13c9bb:https ESTABLISHED
tcp        0      0 manjaro:34518           bom12s07-in-f14.1:https ESTABLISHED
tcp        0      0 manjaro:57160           whatsapp-cdn-shv-:https ESTABLISHED
tcp        0      0 manjaro:49958           aeab55d76dd13c9bb:https ESTABLISHED
tcp        0      0 manjaro:33924           lb-140-82-112-26-:https ESTABLISHED
tcp        0      0 manjaro:36540           104.16.248.249:https    ESTABLISHED
tcp        0      0 manjaro:34534           bom12s03-in-f1.1e:https ESTABLISHED
udp        0      0 manjaro:bootpc          _gateway:bootps         ESTABLISHED
udp        0      0 manjaro:53842           bom07s36-in-f14.1:https ESTABLISHED
udp        0      0 manjaro:58522           bom12s07-in-f14.1:https ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ]         DGRAM                    12236    /run/user/1000/systemd/notify
unix  3      [ ]         SEQPACKET  CONNECTED     285816   @0000a
unix  3      [ ]         SEQPACKET  CONNECTED     285823   @0000b
unix  3      [ ]         SEQPACKET  CONNECTED     285825   @0000c
unix  2      [ ]         DGRAM                    58064    /var/run/nvidia-xdriver-92b206df
unix  4      [ ]         DGRAM      CONNECTED     12644    /run/systemd/notify
unix  2      [ ]         DGRAM                    58063    @var/run/nvidia-xdriver-92b206df@@@@@@@@@@@
unix  14     [ ]         DGRAM      CONNECTED     12668    /run/systemd/journal/dev-log
```

5.ARP :

The arp command allows users to manipulate the neighbor cache or ARP table.
OS:Linux and windows.
syntax :



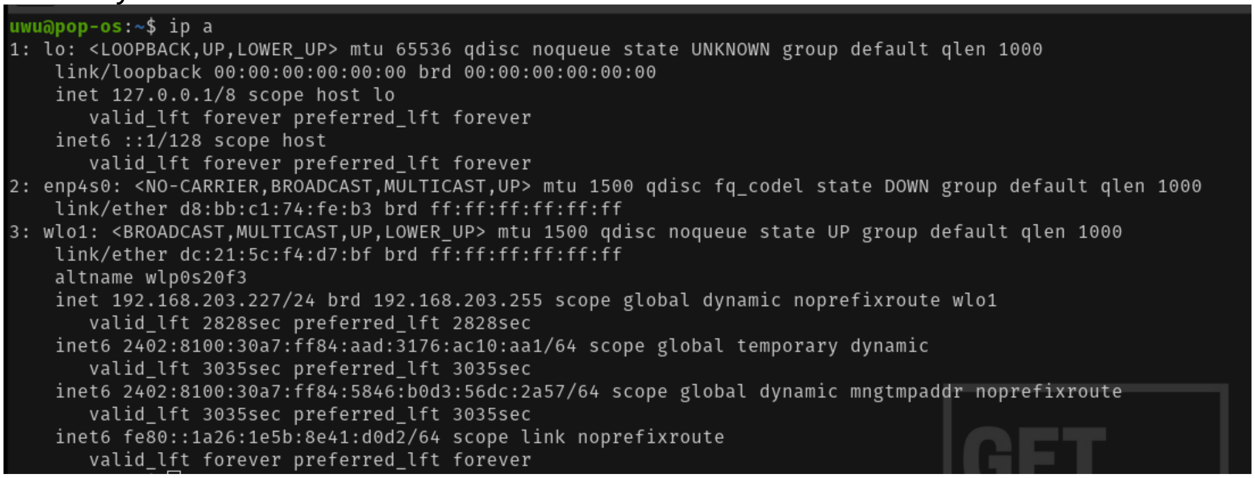
```
└─o arp
Address                  HWtype  HWaddress           Flags Mask            Iface
_gateway                 ether   b8:dd:71:b5:b5:f0   C                     wlo1
```

6.RARP :

7.ip :

OS: Linux.

syntax :



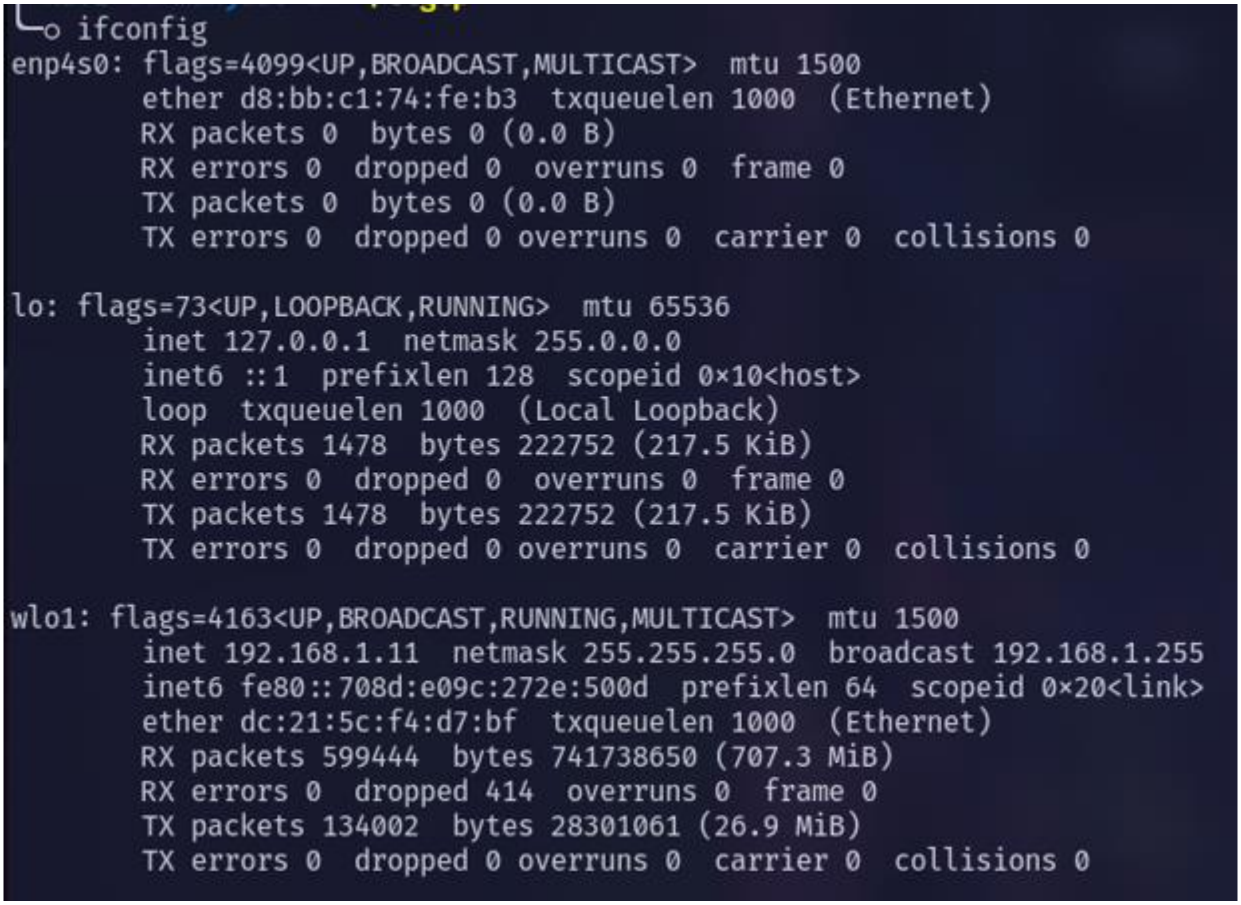
```
uwu@pop-os:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp4s0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq_codel state DOWN group default qlen 1000
    link/ether d8:bb:c1:74:fe:b3 brd ff:ff:ff:ff:ff:ff
3: wlo1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether dc:21:5c:f4:d7:bf brd ff:ff:ff:ff:ff:ff
    altname wlp0s20f3
    inet 192.168.203.227/24 brd 192.168.203.255 scope global dynamic noprefixroute wlo1
       valid_lft 2828sec preferred_lft 2828sec
    inet6 2402:8100:30a7:ff84:aad:3176:ac10:aa1/64 scope global temporary dynamic
       valid_lft 3035sec preferred_lft 3035sec
    inet6 2402:8100:30a7:ff84:5846:b0d3:56dc:2a57/64 scope global dynamic mngtmpaddr noprefixroute
       valid_lft 3035sec preferred_lft 3035sec
    inet6 fe80::1a26:1e5b:8e41:d0d2/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

8. ifconfig :

The “ifconfig” command is used for displaying current network configuration information, setting up an ip address, netmask, or broadcast address to a network interface, creating an alias for the network interface, setting up hardware address, and enable or disable network interfaces.

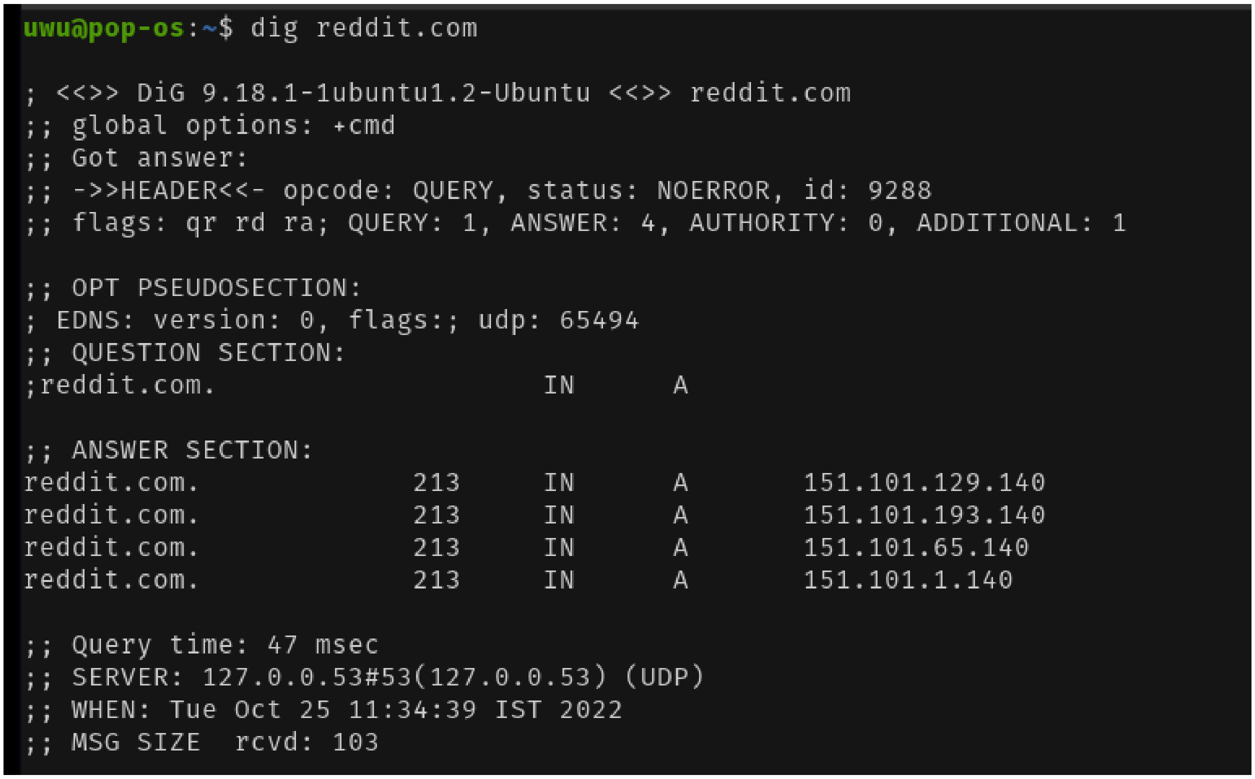
OS :Linux.

syntax :



```
└o ifconfig
enp4s0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether d8:bb:c1:74:fe:b3  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 1478  bytes 222752 (217.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1478  bytes 222752 (217.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlo1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.11  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::708d:e09c:272e:500d  prefixlen 64  scopeid 0×20<link>
        ether dc:21:5c:f4:d7:bf  txqueuelen 1000  (Ethernet)
        RX packets 599444  bytes 741738650 (707.3 MiB)
        RX errors 0  dropped 414  overruns 0  frame 0
        TX packets 134002  bytes 28301061 (26.9 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

9. dig :
dig command stands for ***Domain Information Groper***. It is used for retrieving information about DNS name servers. It is basically used by network administrators. It is used for verifying and troubleshooting DNS problems and to perform DNS lookups.
OS : Linux

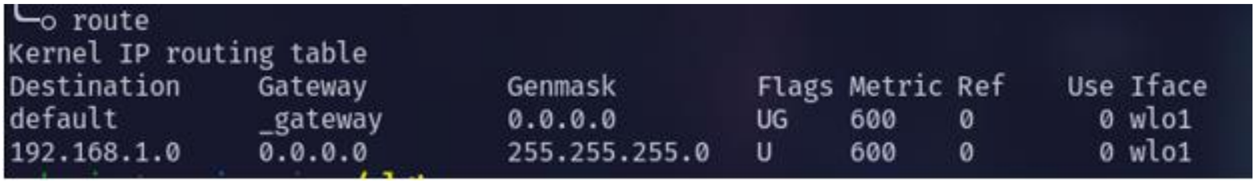


```
uwu@pop-os:~$ dig reddit.com

; <<>> DiG 9.18.1-1ubuntu1.2-Ubuntu <<>> reddit.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 9288
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;reddit.com.                    IN      A

;; ANSWER SECTION:
reddit.com.             213     IN      A       151.101.129.140
reddit.com.             213     IN      A       151.101.193.140
reddit.com.             213     IN      A       151.101.65.140
reddit.com.             213     IN      A       151.101.1.140

;; Query time: 47 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Tue Oct 25 11:34:39 IST 2022
;; MSG SIZE  rcvd: 103
```

10.route :

route command in Linux is used when you want to work with the IP/kernel routing table. It is mainly used to set up static routes to specific hosts or networks via an interface.

OS:Linux and windows.



```
└─o route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         _gateway        0.0.0.0         UG    600    0        0 wlo1
192.168.1.0     0.0.0.0         255.255.255.0   U     600    0        0 wlo1
```

Conclusion: Able to use basic networking commands in linux.

Mahavir Education Trust's

SHAH & ANCHOR KUTCHHI ENGINEERING COLLEGE

Chembur, Mumbai - 400 088

UG Program in Cyber Security

Experiment Number: 3					
Date of Performance:	**10-08-2022**				
Date of Submission:	**17-08-2022**				
Program Execution/ formation/ correction/ ethical practices (07)	**Documentation (02)**	**Timely Submission (03)**	**Viva Answer to sample questions (03)**	**Experiment Total (15)**	**Sign**
07	02	03	03	15	PPatel

Experiment No. 3

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

Laboratory Outcome: CSL5026

Related 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.

Using this tool is widely encouraged as it is part of the curriculum like CCNA, CCENT where Faculties use Packet Trace to demonstrate technical concepts and networking systems. Students complete assignments using this tool, working on their own or in teams.

Engineers prefer to test any protocols on Cisco Packet Tracer before implementing them. Also, Engineers who would like to deploy any change in the production network prefer to use Cisco Packet Tracer to first test the required changes and proceed to deploy if and only if everything is working as expected.

This makes the job easier for Engineers allowing them to add or remove simulated network devices, with a Command line interface and a drag and drop user interface.

Workspace :

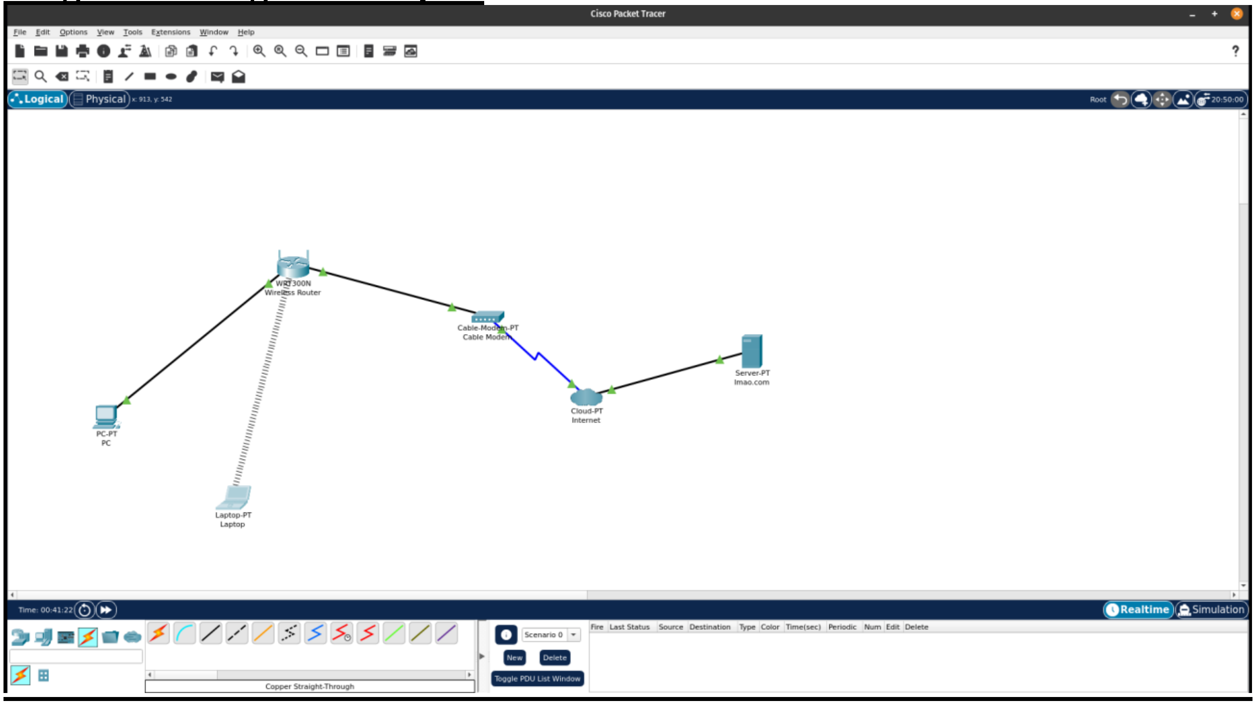
1. Logical –
   Logical workspace shows the logical network topology of the network the user has built. It represents the placing, connecting and clustering virtual network devices.
2. Physical –
   Physical workspace shows the graphical physical dimension of the logical network. It depicts the scale and placement in how network devices such as routers, switches and hosts would look in a real environment. It also provides geographical representation of networks, including multiple buildings, cities and wiring closets.

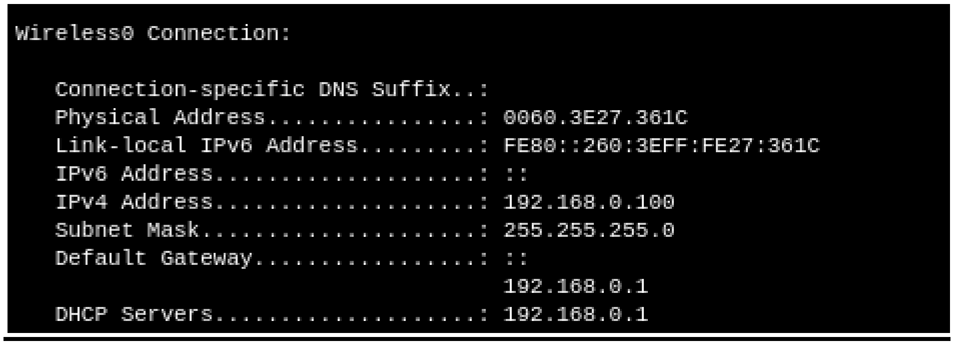
Key Features:

- Unlimited devices
- E-learning
- Customize single/multi user activities
- Interactive Environment
- Visualizing Networks
- Real-time mode and Simulation mode
- Self-paced

- Supports majority of networking protocols
- International language support
- Cross platform compatibility

Program Listing And Output:





```
Wireless0 Connection:

   Connection-specific DNS Suffix..:
   Physical Address................: 0060.3E27.361C
   Link-local IPv6 Address.........: FE80::260:3EFF:FE27:361C
   IPv6 Address....................: ::
   IPv4 Address....................: 192.168.0.100
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: ::
                                     192.168.0.1
   DHCP Servers....................: 192.168.0.1
```

Conclusion: Able to setup a network using cisco packet tracer and implement static routing.

Mahavir Education Trust's

SHAH & ANCHOR KUTCHHI ENGINEERING COLLEGE

Chembur, Mumbai - 400 088

UG Program in Cyber Security

Experiment Number: 4					
Date of Performance:		**17-08-2022**			
Date of Submission:		**24-08-2022**			
Program Execution/ formation/ correction/ ethical practices (07)	**Documentation (02)**	**Timely Submission (03)**	**Viva Answer to sample questions (03)**	**Experiment Total (15)**	**Sign**
07	02	03	03	15	PPatel

Experiment No. 4

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

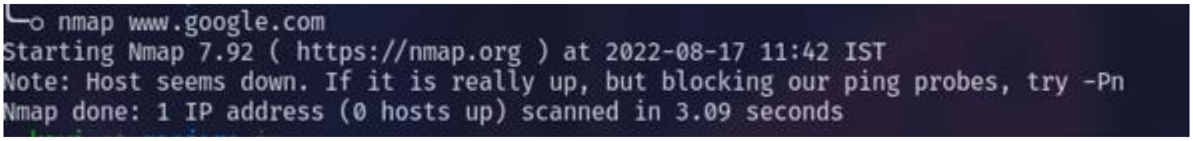
Laboratory Outcome: CSL5022

Problem Statement:

Related Theory: Networks can get very complicated. You might start with just a few devices connected to a modem and a printer, and at that point, your network is easy to map. However, once you maximize the use of your hardware by implementing **virtualization** and you start to add on specialized servers for storage and applications, you find it is easy to lose track of all of the paths you have created for your business network.

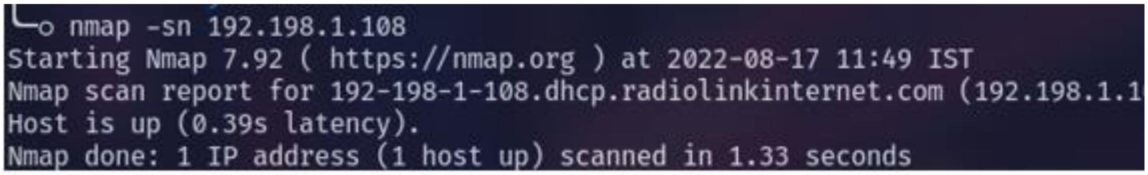
Program Listing And Output:

Nmap google.com



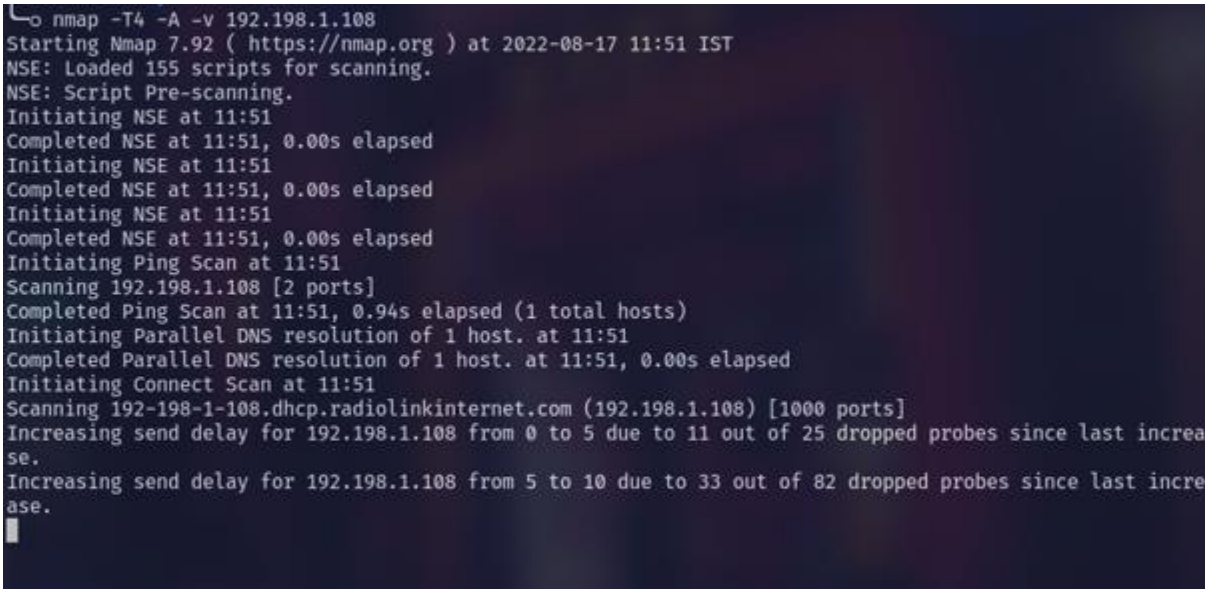
```
└─o nmap www.google.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-17 11:42 IST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.09 seconds
```

Nmap ping



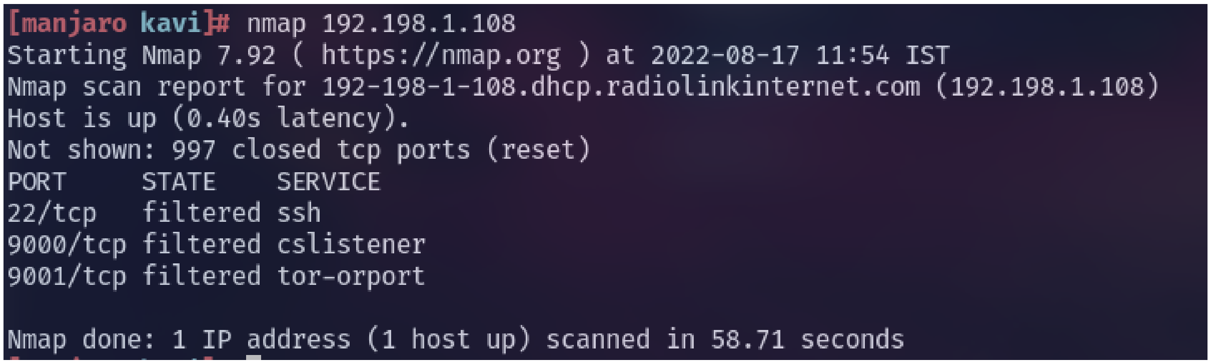
```
└o nmap -sn 192.198.1.108
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-17 11:49 IST
Nmap scan report for 192-198-1-108.dhcp.radiolinkinternet.com (192.198.1.1
Host is up (0.39s latency).
Nmap done: 1 IP address (1 host up) scanned in 1.33 seconds
```

Nmap intense



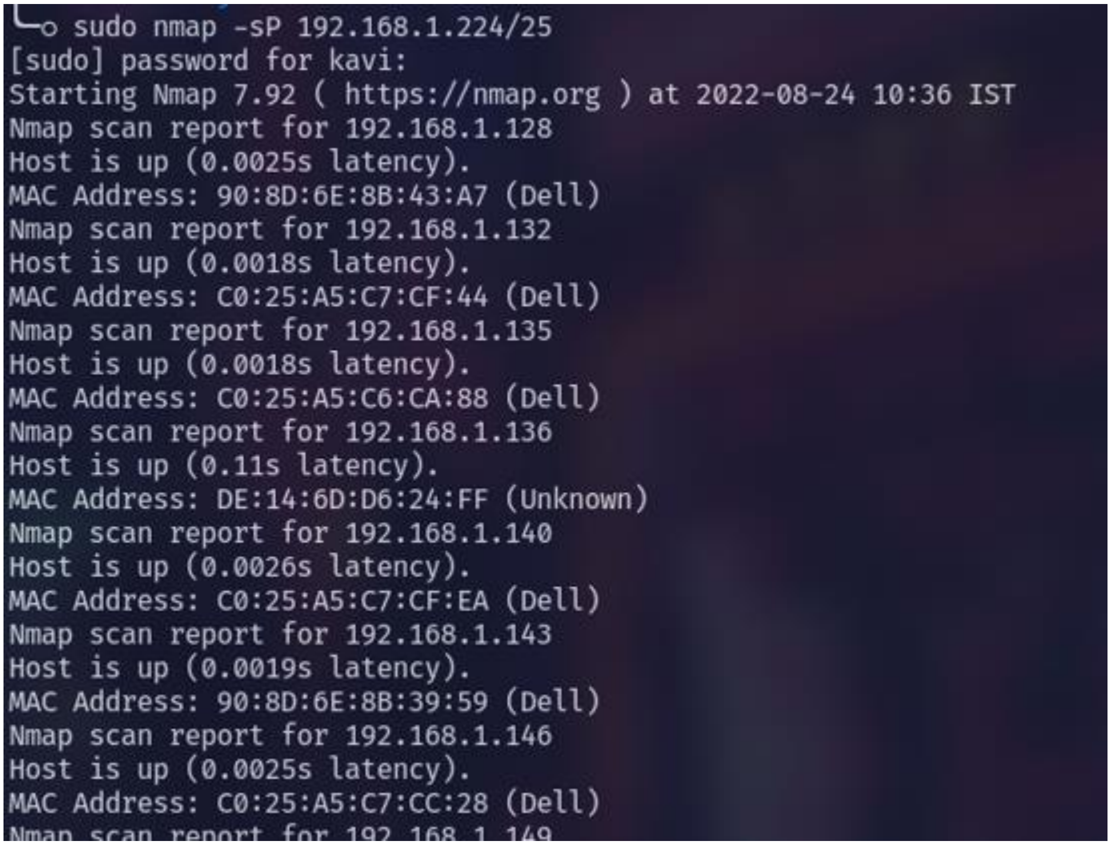
```
└o nmap -T4 -A -v 192.198.1.108
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-17 11:51 IST
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 11:51
Completed NSE at 11:51, 0.00s elapsed
Initiating NSE at 11:51
Completed NSE at 11:51, 0.00s elapsed
Initiating NSE at 11:51
Completed NSE at 11:51, 0.00s elapsed
Initiating Ping Scan at 11:51
Scanning 192.198.1.108 [2 ports]
Completed Ping Scan at 11:51, 0.94s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:51
Completed Parallel DNS resolution of 1 host. at 11:51, 0.00s elapsed
Initiating Connect Scan at 11:51
Scanning 192-198-1-108.dhcp.radiolinkinternet.com (192.198.1.108) [1000 ports]
Increasing send delay for 192.198.1.108 from 0 to 5 due to 11 out of 25 dropped probes since last increa
se.
Increasing send delay for 192.198.1.108 from 5 to 10 due to 33 out of 82 dropped probes since last incre
ase.
```

Nmap :



```
[manjaro kavi]# nmap 192.198.1.108
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-17 11:54 IST
Nmap scan report for 192-198-1-108.dhcp.radiolinkinternet.com (192.198.1.108)
Host is up (0.40s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE    SERVICE
22/tcp   filtered ssh
9000/tcp filtered cslistener
9001/tcp filtered tor-orport

Nmap done: 1 IP address (1 host up) scanned in 58.71 seconds
```

Nmap subnet :



```
└─o sudo nmap -sP 192.168.1.224/25
[sudo] password for kavi:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-24 10:36 IST
Nmap scan report for 192.168.1.128
Host is up (0.0025s latency).
MAC Address: 90:8D:6E:8B:43:A7 (Dell)
Nmap scan report for 192.168.1.132
Host is up (0.0018s latency).
MAC Address: C0:25:A5:C7:CF:44 (Dell)
Nmap scan report for 192.168.1.135
Host is up (0.0018s latency).
MAC Address: C0:25:A5:C6:CA:88 (Dell)
Nmap scan report for 192.168.1.136
Host is up (0.11s latency).
MAC Address: DE:14:6D:D6:24:FF (Unknown)
Nmap scan report for 192.168.1.140
Host is up (0.0026s latency).
MAC Address: C0:25:A5:C7:CF:EA (Dell)
Nmap scan report for 192.168.1.143
Host is up (0.0019s latency).
MAC Address: 90:8D:6E:8B:39:59 (Dell)
Nmap scan report for 192.168.1.146
Host is up (0.0025s latency).
MAC Address: C0:25:A5:C7:CC:28 (Dell)
Nmap scan report for 192.168.1.149
```

Conclusion: Able to understand Nmap commands for network discovery.

Mahavir Education Trust's

SHAH & ANCHOR KUTCHHI ENGINEERING COLLEGE

Chembur, Mumbai - 400 088

UG Program in Cyber Security

Experiment Number: 5					
Date of Performance:	**17-08-2022**				
Date of Submission:	**24-08-2022**				
Program Execution/ formation/ correction/ ethical practices (07)	**Documentation (02)**	**Timely Submission (03)**	**Viva Answer to sample questions (03)**	**Experiment Total (15)**	**Sign**
07	02	03	03	15	PPatel

Experiment No. 5

Aim: Use Wire shark to understand the operation of TCP/IP layers: ● Ethernet Layer: Frame header, Frame size etc. ● Data Link Layer: MAC address, ARP (IP and MAC address binding) ● Network Layer: IP Packet (header, fragmentation), ICMP (Query and Echo) ● Transport Layer: TCP Ports, TCP handshake segments etc. Application Layer: DHCP, FTP, HTTP header formats

Laboratory Outcome: CSL5022

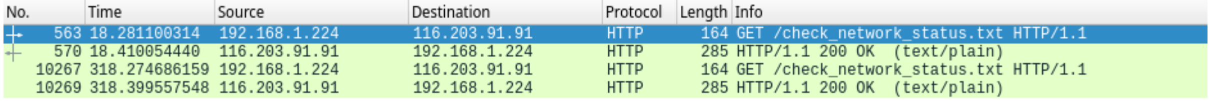
Related Theory:

Wireshark is the world's foremost and widely-used network protocol analyzer. It lets you see what's happening on your network at a microscopic level and is the de facto (and often de jure) standard across many commercial and non-profit enterprises, government agencies, and educational institutions. Wireshark development thrives thanks to the volunteer contributions of networking experts around the globe and is the continuation of a project started by Gerald Combs in 1998.

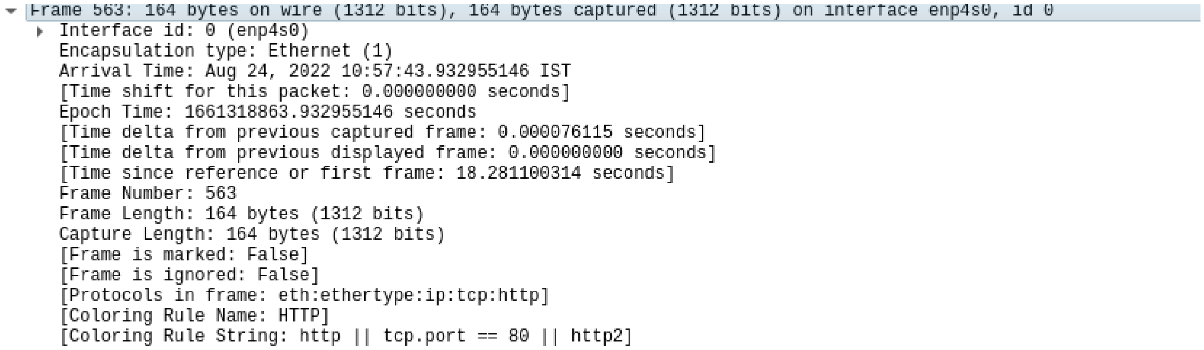
Wireshark has a rich feature set which includes the following:

- Deep inspection of hundreds of protocols, with more being added all the time
- Live capture and offline analysis
- Standard three-pane packet browser
- Multi-platform: Runs on Windows, Linux, macOS, Solaris, FreeBSD, NetBSD, and many others
- Captured network data can be browsed via a GUI, or via the TTY-mode TShark utility
- The most powerful display filters in the industry
- Rich VoIP analysis
- Read/write many different capture file formats: tcpdump (libpcap), Pcap NG, Catapult DCT2000, Cisco Secure IDS iplog, Microsoft Network Monitor, Network General Sniffer® (compressed and uncompressed), Sniffer® Pro, and NetXray®, Network Instruments Observer, NetScreen snoop, Novell LANalyzer, RADCOM WAN/LAN Analyzer, Shomiti/Finisar Surveyor, Tektronix K12xx, Visual Networks Visual UpTime, WildPackets EtherPeek/TokenPeek/AiroPeek, and many others
- Capture files compressed with gzip can be decompressed on the fly
- Live data can be read from Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, FDDI, and others (depending on your platform)
- Decryption support for many protocols, including IPsec, ISAKMP, Kerberos, SNMPv3, SSL/TLS, WEP, and WPA/WPA2
- Coloring rules can be applied to the packet list for quick, intuitive analysis
- Output can be exported to XML, PostScript®, CSV, or plain text

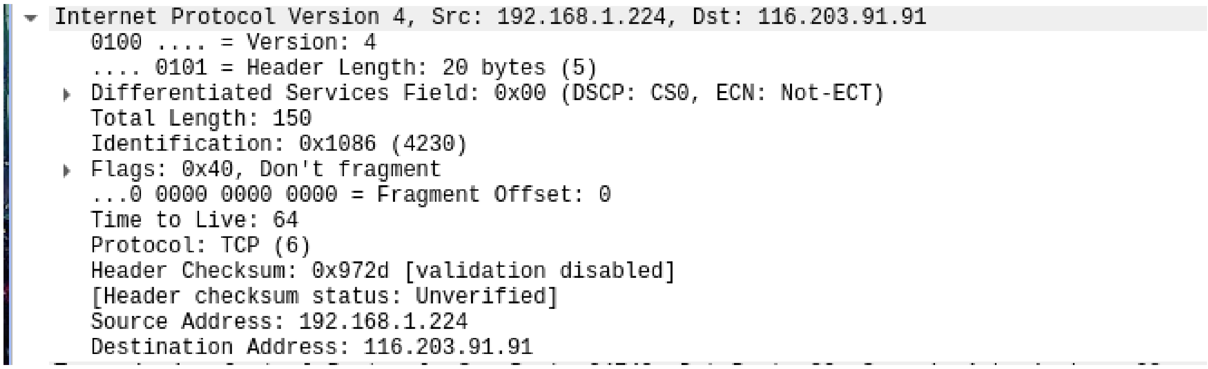
Program Listing And Output: HTTP :



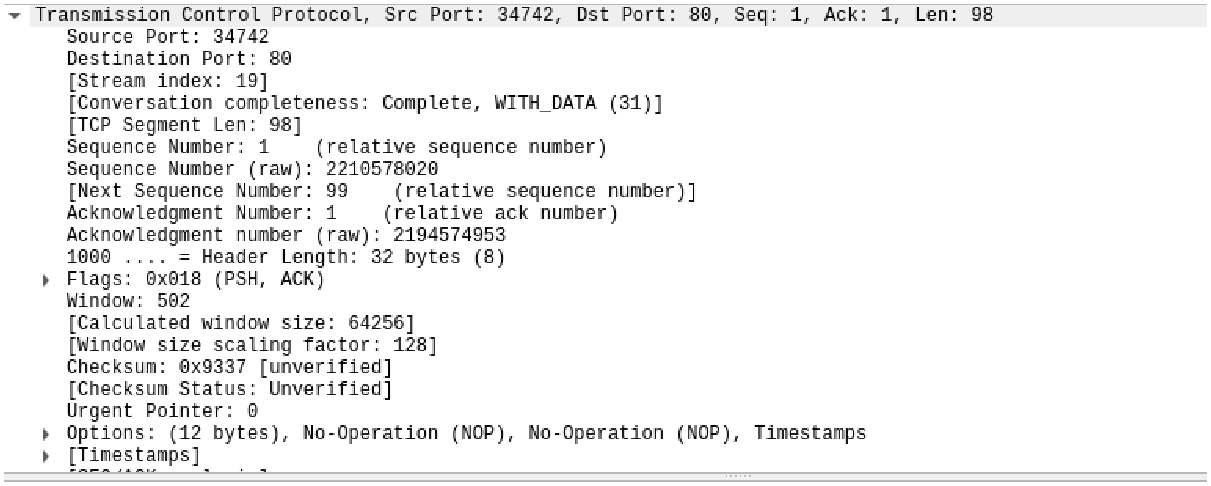
```
No.    Time          Source          Destination     Protocol  Length Info
   563 18.281100314  192.168.1.224   116.203.91.91   HTTP         164 GET /check_network_status.txt HTTP/1.1
   570 18.410054440  116.203.91.91   192.168.1.224   HTTP         285 HTTP/1.1 200 OK  (text/plain)
 10267 318.274686159 192.168.1.224   116.203.91.91   HTTP         164 GET /check_network_status.txt HTTP/1.1
 10269 318.399557548 116.203.91.91   192.168.1.224   HTTP         285 HTTP/1.1 200 OK  (text/plain)
```



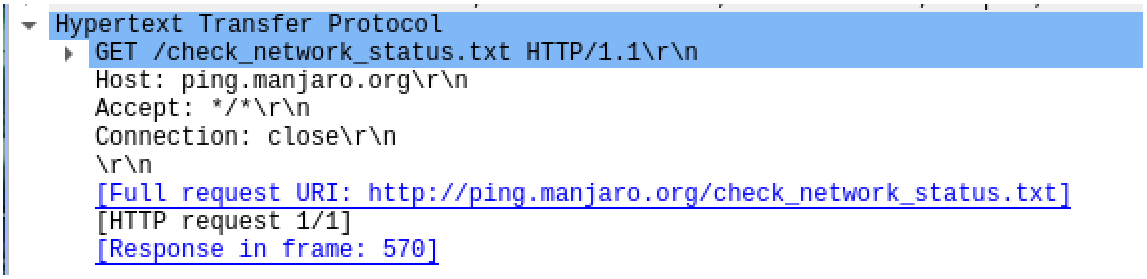
```
▾ Frame 563: 164 bytes on wire (1312 bits), 164 bytes captured (1312 bits) on interface enp4s0, id 0
   ▸ Interface id: 0 (enp4s0)
     Encapsulation type: Ethernet (1)
     Arrival Time: Aug 24, 2022 10:57:43.932955146 IST
     [Time shift for this packet: 0.000000000 seconds]
     Epoch Time: 1661318863.932955146 seconds
     [Time delta from previous captured frame: 0.000076115 seconds]
     [Time delta from previous displayed frame: 0.000000000 seconds]
     [Time since reference or first frame: 18.281100314 seconds]
     Frame Number: 563
     Frame Length: 164 bytes (1312 bits)
     Capture Length: 164 bytes (1312 bits)
     [Frame is marked: False]
     [Frame is ignored: False]
     [Protocols in frame: eth:ethertype:ip:tcp:http]
     [Coloring Rule Name: HTTP]
     [Coloring Rule String: http || tcp.port == 80 || http2]
```



```
▾ Internet Protocol Version 4, Src: 192.168.1.224, Dst: 116.203.91.91
     0100 .... = Version: 4
     .... 0101 = Header Length: 20 bytes (5)
   ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
     Total Length: 150
     Identification: 0x1086 (4230)
   ▸ Flags: 0x40, Don't fragment
     ...0 0000 0000 0000 = Fragment Offset: 0
     Time to Live: 64
     Protocol: TCP (6)
     Header Checksum: 0x972d [validation disabled]
     [Header checksum status: Unverified]
     Source Address: 192.168.1.224
     Destination Address: 116.203.91.91
```

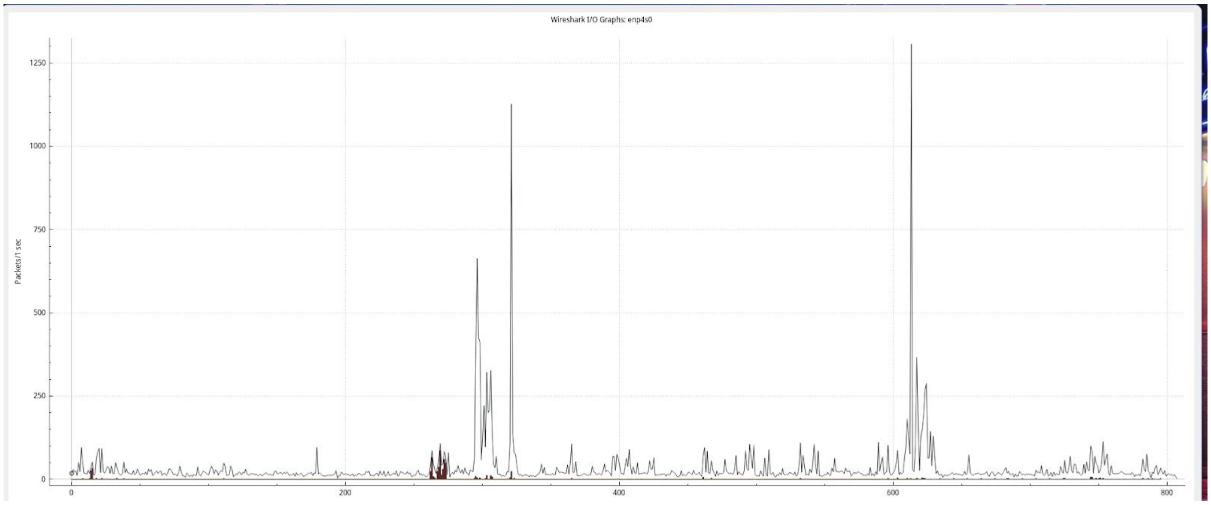


```
▾ Transmission Control Protocol, Src Port: 34742, Dst Port: 80, Seq: 1, Ack: 1, Len: 98
     Source Port: 34742
     Destination Port: 80
     [Stream index: 19]
     [Conversation completeness: Complete, WITH_DATA (31)]
     [TCP Segment Len: 98]
     Sequence Number: 1    (relative sequence number)
     Sequence Number (raw): 2210578020
     [Next Sequence Number: 99    (relative sequence number)]
     Acknowledgment Number: 1    (relative ack number)
     Acknowledgment number (raw): 2194574953
     1000 .... = Header Length: 32 bytes (8)
   ▸ Flags: 0x018 (PSH, ACK)
     Window: 502
     [Calculated window size: 64256]
     [Window size scaling factor: 128]
     Checksum: 0x9337 [unverified]
     [Checksum Status: Unverified]
     Urgent Pointer: 0
   ▸ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
   ▸ [Timestamps]
```

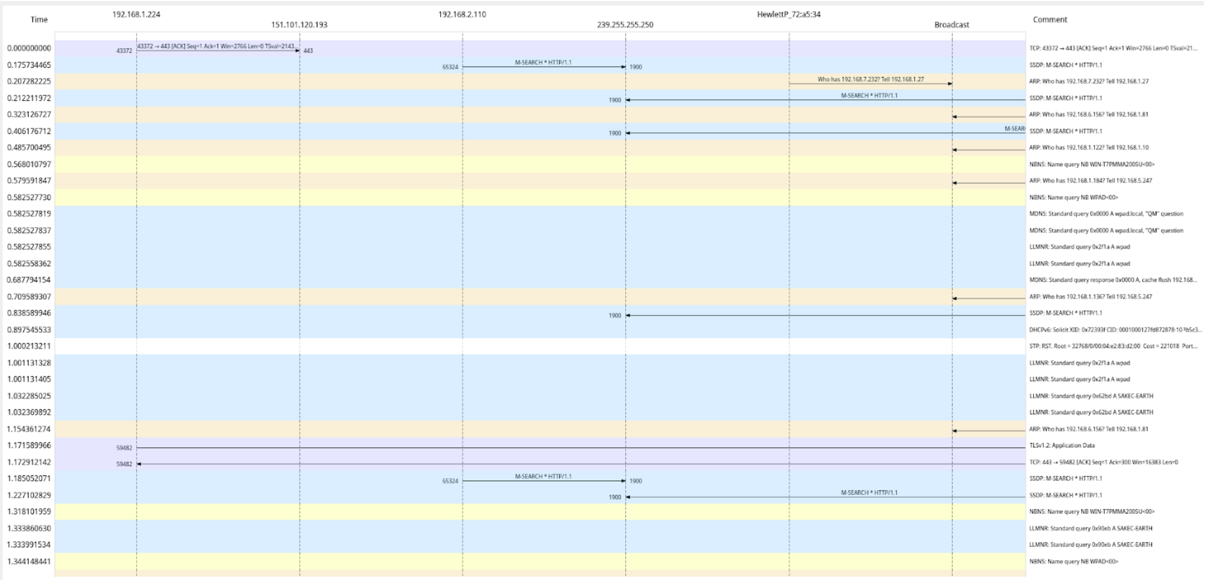


```
▾ Hypertext Transfer Protocol
  ▸ GET /check_network_status.txt HTTP/1.1\r\n
    Host: ping.manjaro.org\r\n
    Accept: */*\r\n
    Connection: close\r\n
    \r\n
    [Full request URI: http://ping.manjaro.org/check_network_status.txt]
    [HTTP request 1/1]
    [Response in frame: 570]
```

IO Graph

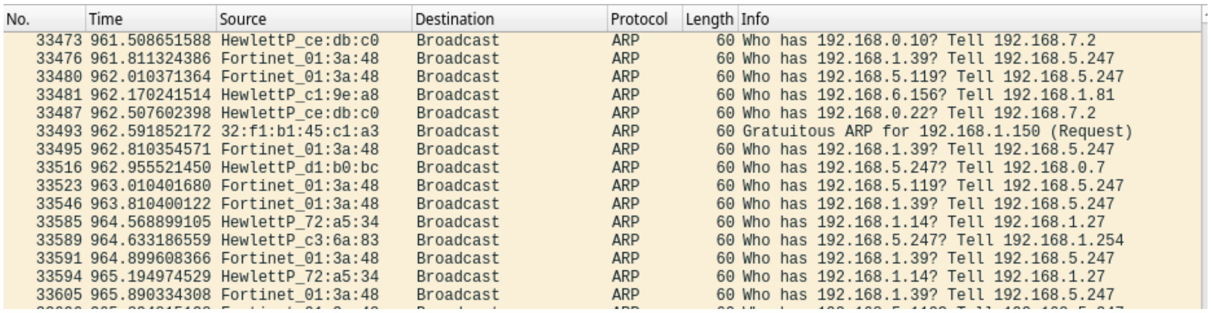


Flow Graph

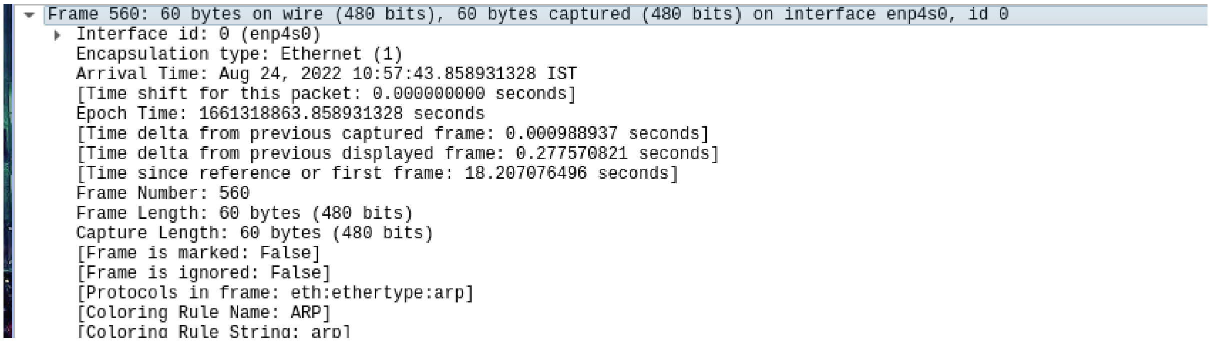


```
Time         Comment
0.000000000  TCP: 43372 → 443 [ACK] Seq=1 Ack=1 Win=2766 Len=0 TSval=21...
0.175734465  SSDP: M-SEARCH * HTTP/1.1
0.207282225  ARP: Who has 192.168.7.232? Tell 192.168.1.27
0.212211972  SSDP: M-SEARCH * HTTP/1.1
0.323126727  ARP: Who has 192.168.6.156? Tell 192.168.1.81
0.406176712  SSDP: M-SEARCH * HTTP/1.1
0.485700495  ARP: Who has 192.168.1.122? Tell 192.168.1.10
0.568010797  NBNS: Name query NB WIN-T7PMMA200SU<00>
0.579591847  ARP: Who has 192.168.1.184? Tell 192.168.5.247
0.582527730  NBNS: Name query NB WPAD<00>
0.582527819  MDNS: Standard query 0x0000 A wpad.local, "QM" question
0.582527837  MDNS: Standard query 0x0000 A wpad.local, "QM" question
0.582527855  LLMNR: Standard query 0x2f1a A wpad
0.582558362  LLMNR: Standard query 0x2f1a A wpad
0.687794154  MDNS: Standard query response 0x0000 A, cache flush 192.168...
0.709589307  ARP: Who has 192.168.1.136? Tell 192.168.5.247
0.838589946  SSDP: M-SEARCH * HTTP/1.1
0.897545533  DHCPv6: Solicit XID: 0x72393f CID: 0001000127fd872878-10³b5c3...
1.000213211  STP: RST. Root = 32768/0/00:04:e2:83:d2:00  Cost = 221018  Port...
1.001131328  LLMNR: Standard query 0x2f1a A wpad
1.001131405  LLMNR: Standard query 0x2f1a A wpad
1.032285025  LLMNR: Standard query 0x62bd A SAKEC-EARTH
1.032369892  LLMNR: Standard query 0x62bd A SAKEC-EARTH
1.154361274  ARP: Who has 192.168.6.156? Tell 192.168.1.81
1.171589966  TLSv1.2: Application Data
1.172912142  TCP: 443 → 59482 [ACK] Seq=1 Ack=300 Win=16383 Len=0
1.185052071  SSDP: M-SEARCH * HTTP/1.1
1.227102829  SSDP: M-SEARCH * HTTP/1.1
1.318101959  NBNS: Name query NB WIN-T7PMMA200SU<00>
1.333860630  LLMNR: Standard query 0x90eb A SAKEC-EARTH
1.333991534  LLMNR: Standard query 0x90eb A SAKEC-EARTH
1.344148441  NBNS: Name query NB WPAD<00>
```

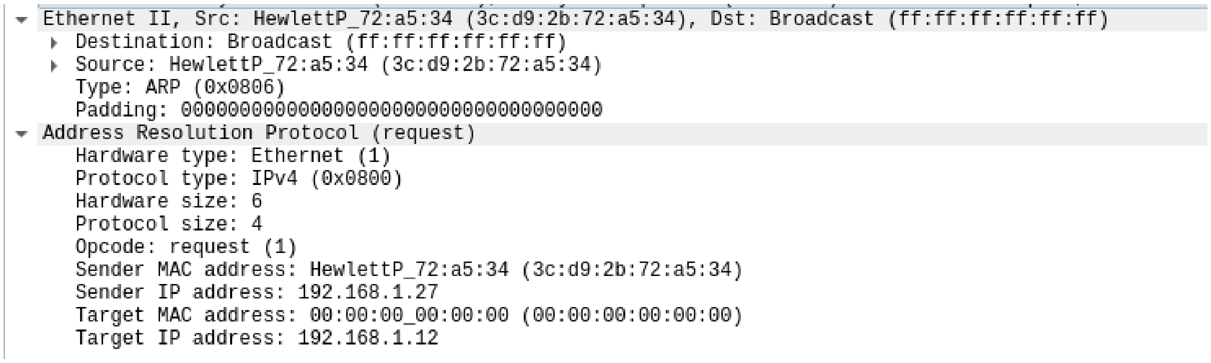
ARP:



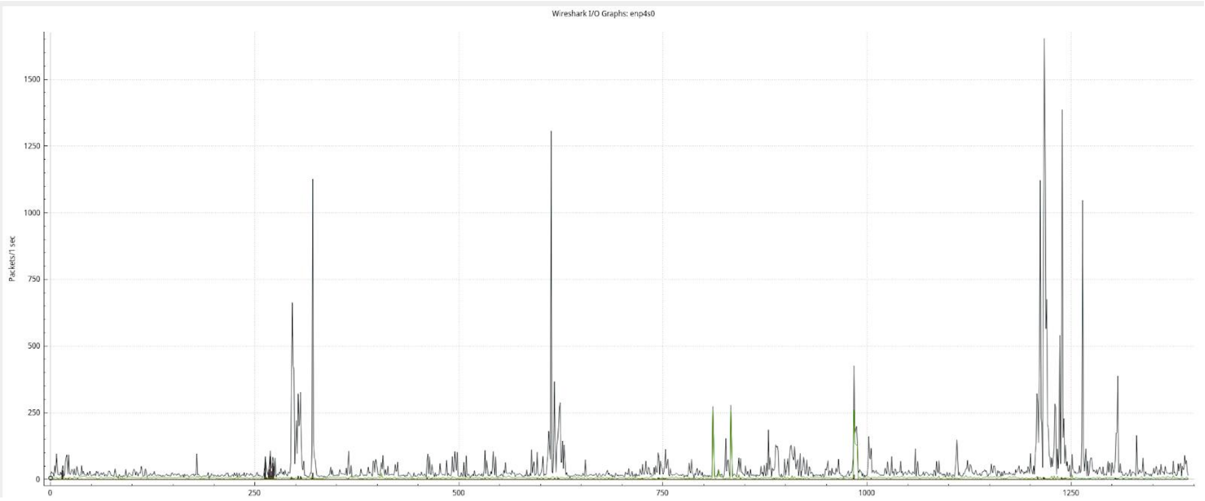
```
No.    Time           Source              Destination  Protocol  Length Info
 33473 961.508651588 HewlettP_ce:db:c0  Broadcast     ARP          60 Who has 192.168.0.10? Tell 192.168.7.2
 33476 961.811324386 Fortinet_01:3a:48  Broadcast     ARP          60 Who has 192.168.1.39? Tell 192.168.5.247
 33480 962.010371364 Fortinet_01:3a:48  Broadcast     ARP          60 Who has 192.168.5.119? Tell 192.168.5.247
 33481 962.170241514 HewlettP_c1:9e:a8  Broadcast     ARP          60 Who has 192.168.6.156? Tell 192.168.1.81
 33487 962.507602398 HewlettP_ce:db:c0  Broadcast     ARP          60 Who has 192.168.0.22? Tell 192.168.7.2
 33493 962.591852172 32:f1:b1:45:c1:a3  Broadcast     ARP          60 Gratuitous ARP for 192.168.1.150 (Request)
 33495 962.810354571 Fortinet_01:3a:48  Broadcast     ARP          60 Who has 192.168.1.39? Tell 192.168.5.247
 33516 962.955521450 HewlettP_d1:b0:bc  Broadcast     ARP          60 Who has 192.168.5.247? Tell 192.168.0.7
 33523 963.010401680 Fortinet_01:3a:48  Broadcast     ARP          60 Who has 192.168.5.119? Tell 192.168.5.247
 33546 963.810400122 Fortinet_01:3a:48  Broadcast     ARP          60 Who has 192.168.1.39? Tell 192.168.5.247
 33585 964.568899105 HewlettP_72:a5:34  Broadcast     ARP          60 Who has 192.168.1.14? Tell 192.168.1.27
 33589 964.633186559 HewlettP_c3:6a:83  Broadcast     ARP          60 Who has 192.168.5.247? Tell 192.168.1.254
 33591 964.899608366 Fortinet_01:3a:48  Broadcast     ARP          60 Who has 192.168.1.39? Tell 192.168.5.247
 33594 965.194974529 HewlettP_72:a5:34  Broadcast     ARP          60 Who has 192.168.1.14? Tell 192.168.1.27
 33605 965.890334308 Fortinet_01:3a:48  Broadcast     ARP          60 Who has 192.168.1.39? Tell 192.168.5.247
```

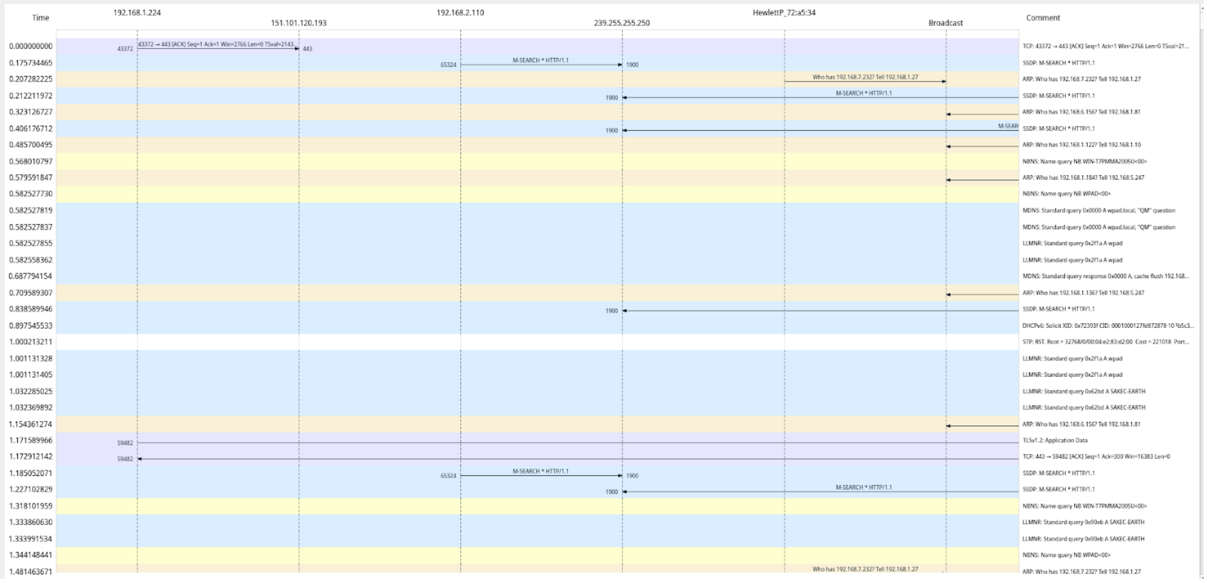


```
▾ Frame 560: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface enp4s0, id 0
  ▸ Interface id: 0 (enp4s0)
    Encapsulation type: Ethernet (1)
    Arrival Time: Aug 24, 2022 10:57:43.858931328 IST
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1661318863.858931328 seconds
    [Time delta from previous captured frame: 0.000988937 seconds]
    [Time delta from previous displayed frame: 0.277570821 seconds]
    [Time since reference or first frame: 18.207076496 seconds]
    Frame Number: 560
    Frame Length: 60 bytes (480 bits)
    Capture Length: 60 bytes (480 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:arp]
    [Coloring Rule Name: ARP]
    [Coloring Rule String: arp]
```



```
▾ Ethernet II, Src: HewlettP_72:a5:34 (3c:d9:2b:72:a5:34), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ▸ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  ▸ Source: HewlettP_72:a5:34 (3c:d9:2b:72:a5:34)
    Type: ARP (0x0806)
    Padding: 000000000000000000000000000000000000
▾ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: HewlettP_72:a5:34 (3c:d9:2b:72:a5:34)
    Sender IP address: 192.168.1.27
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.1.12
```





Time	Comment
0.000000000	TCP: 43372 → 443 [ACK] Seq=1 Ack=1 Win=2766 Len=0 TSval=21...
0.175734465	SSDP: M-SEARCH * HTTP/1.1
0.207282225	ARP: Who has 192.168.7.232? Tell 192.168.1.27
0.212211972	SSDP: M-SEARCH * HTTP/1.1
0.323126727	ARP: Who has 192.168.6.156? Tell 192.168.1.81
0.406176712	SSDP: M-SEARCH * HTTP/1.1
0.485700495	ARP: Who has 192.168.1.122? Tell 192.168.1.10
0.568010797	NBNS: Name query NB WIN-T7PMMA2005U<00>
0.579591847	ARP: Who has 192.168.1.184? Tell 192.168.5.247
0.582527730	NBNS: Name query NB WPAD<00>
0.582527819	MDNS: Standard query 0x0000 A wpad.local, "QM" question
0.582527837	MDNS: Standard query 0x0000 A wpad.local, "QM" question
0.582527855	LLMNR: Standard query 0x2f1a A wpad
0.582558362	LLMNR: Standard query 0x2f1a A wpad
0.687794154	MDNS: Standard query response 0x0000 A, cache flush 192.168...
0.709589307	ARP: Who has 192.168.1.136? Tell 192.168.5.247
0.838589946	SSDP: M-SEARCH * HTTP/1.1
0.897545533	DHCPv6: Solicit XID: 0x72393f CID: 0001000127fd872878·10 ³b5c3...
1.000213211	STP: RST. Root = 32768/0/00:04:e2:83:d2:00 Cost = 221018 Port...
1.001131328	LLMNR: Standard query 0x2f1a A wpad
1.001131405	LLMNR: Standard query 0x2f1a A wpad
1.032285025	LLMNR: Standard query 0x62bd A SAKEC-EARTH
1.032369892	LLMNR: Standard query 0x62bd A SAKEC-EARTH
1.154361274	ARP: Who has 192.168.6.156? Tell 192.168.1.81
1.171589966	TLSv1.2: Application Data
1.172912142	TCP: 443 → 59482 [ACK] Seq=1 Ack=300 Win=16383 Len=0
1.185052071	SSDP: M-SEARCH * HTTP/1.1
1.227102829	SSDP: M-SEARCH * HTTP/1.1
1.318101959	NBNS: Name query NB WIN-T7PMMA2005U<00>
1.333860630	LLMNR: Standard query 0x90eb A SAKEC-EARTH
1.333991534	LLMNR: Standard query 0x90eb A SAKEC-EARTH
1.344148441	NBNS: Name query NB WPAD<00>
1.481463671	ARP: Who has 192.168.7.232? Tell 192.168.1.27

<u>Conclusion:</u> Got a understanding of TCP/IP layers with help of wireshark.

Mahavir Education Trust's

SHAH & ANCHOR KUTCHHI ENGINEERING COLLEGE

Chembur, Mumbai - 400 088

UG Program in Cyber Security

Experiment Number: 6					
Date of Performance:					
Date of Submission:					
Program Execution/ formation/ correction/ ethical practices (07)	**Documentation (02)**	**Timely Submission (03)**	**Viva Answer to sample questions (03)**	**Experiment Total (15)**	**Sign**
07	02	03	03	15	PPatel

Aim:- a. Set up multiple IP addresses on a single LAN. b. Using netstat and route commands of Linux, do the following: ● View current routing table ● Add and delete routes ● Change default gateway Perform packet filtering by enabling IP forwarding using IPtables in Linux

Laboratory Outcome: CSL5022

Related Theory: **iptables** is a command line interface used to set up and maintain tables for the Netfilter firewall for IPv4, included in the Linux kernel. The firewall matches packets with rules defined in these tables and then takes the specified action on a possible match.

- *Tables* is the name for a set of chains.
- *Chain* is a collection of rules.
- *Rule* is condition used to match packet.
- *Target* is action taken when a possible rule matches. Examples of the target are ACCEPT, DROP, QUEUE.
- *Policy* is the default action taken in case of no match with the inbuilt chains and can be ACCEPT or DROP.

Syntax:

iptables --table *TABLE* -A/-C/-D... *CHAIN rule* --jump *Target*

TABLE

There are five possible tables:

- **filter:** Default used table for packet filtering. It includes chains like INPUT, OUTPUT and FORWARD.
- **nat :** Related to Network Address Translation. It includes PREROUTING and POSTROUTING chains.
- **mangle :** For specialised packet alteration. Inbuilt chains include PREROUTING and OUTPUT.
- **raw :** Configures exemptions from connection tracking. Built-in chains are PREROUTING and OUTPUT.
- **security :** Used for Mandatory Access Control

CHAINS

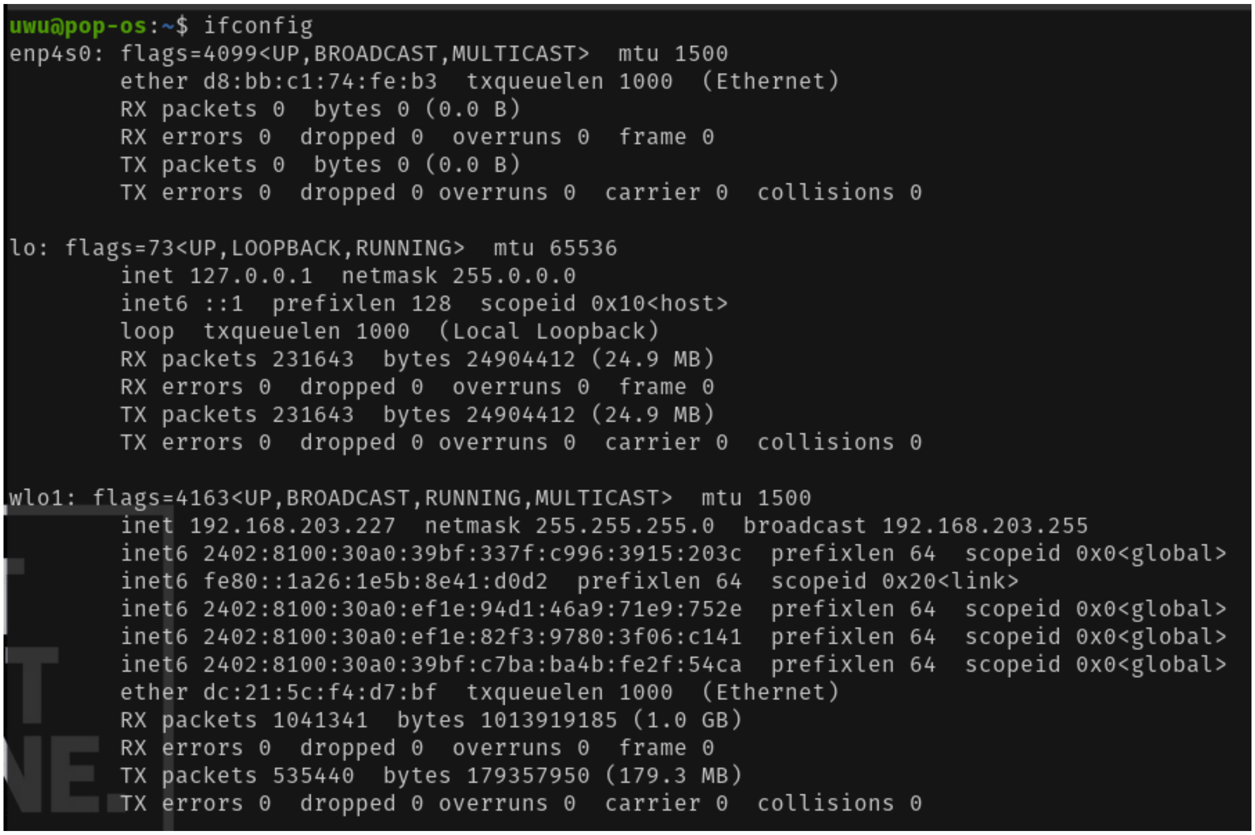
There are few built-in chains that are included in tables. They are:

- **INPUT :**set of rules for packets destined to localhost sockets.
- **FORWARD :**for packets routed through the device.
- **OUTPUT :**for locally generated packets, meant to be transmitted outside.
- **PREROUTING :**for modifying packets as they arrive.
- **POSTROUTING :**for modifying packets as they are leaving.

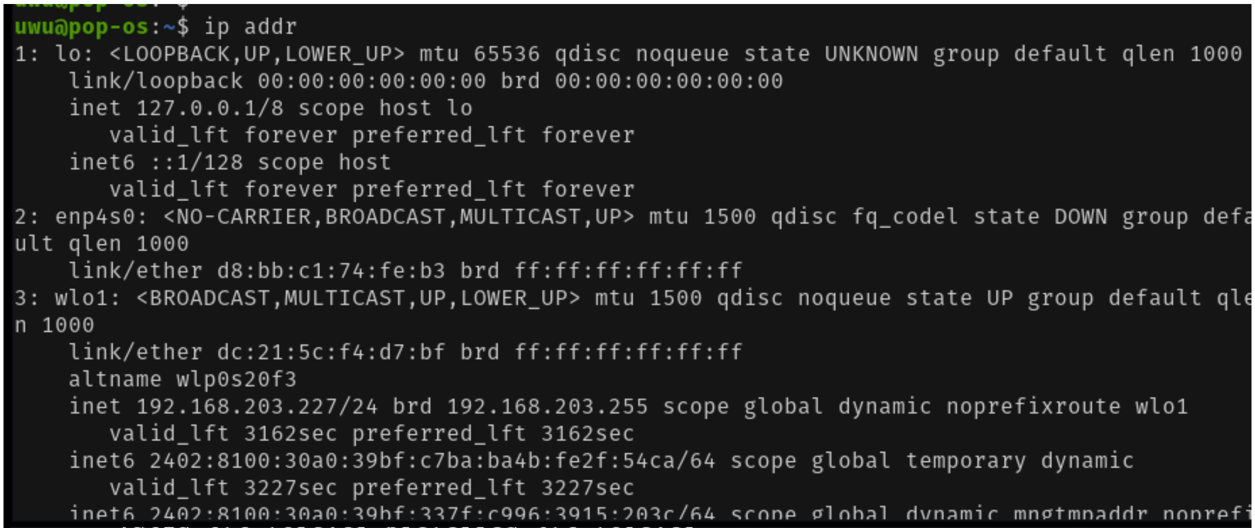
Netstat command displays various network related information such as network connections, routing tables, interface statistics, masquerade connections, multicast memberships etc.,

route command in Linux is used when you want to work with the IP/kernel routing table. It is mainly used to set up static routes to specific hosts or networks via an interface. It is used for showing or update the IP/kernel routing table.

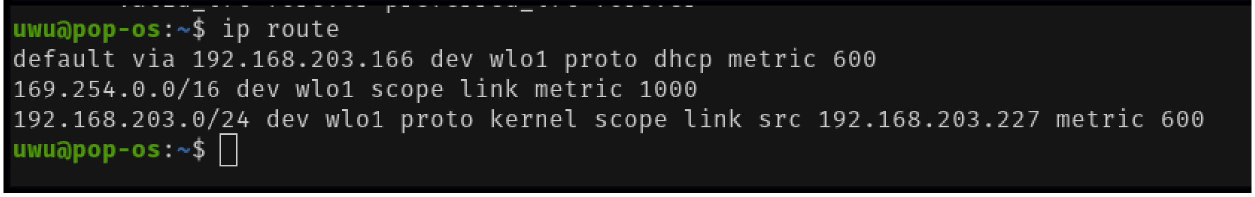
Program Listing And Output:



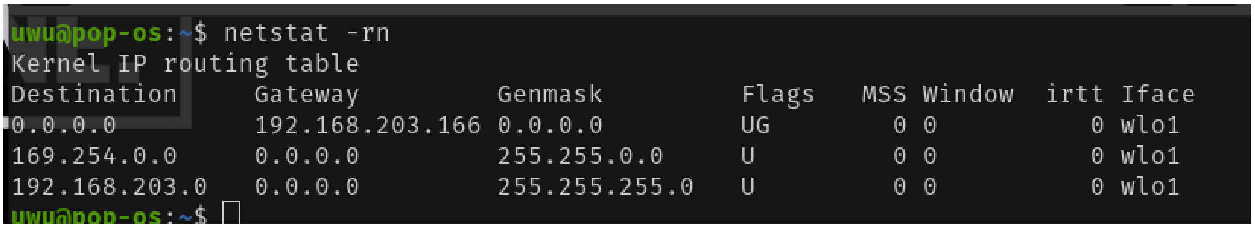
```
uwu@pop-os:~$ ifconfig
enp4s0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether d8:bb:c1:74:fe:b3  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 231643  bytes 24904412 (24.9 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 231643  bytes 24904412 (24.9 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlo1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.203.227  netmask 255.255.255.0  broadcast 192.168.203.255
        inet6 2402:8100:30a0:39bf:337f:c996:3915:203c  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::1a26:1e5b:8e41:d0d2  prefixlen 64  scopeid 0x20<link>
        inet6 2402:8100:30a0:ef1e:94d1:46a9:71e9:752e  prefixlen 64  scopeid 0x0<global>
        inet6 2402:8100:30a0:ef1e:82f3:9780:3f06:c141  prefixlen 64  scopeid 0x0<global>
        inet6 2402:8100:30a0:39bf:c7ba:ba4b:fe2f:54ca  prefixlen 64  scopeid 0x0<global>
        ether dc:21:5c:f4:d7:bf  txqueuelen 1000  (Ethernet)
        RX packets 1041341  bytes 1013919185 (1.0 GB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 535440  bytes 179357950 (179.3 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```



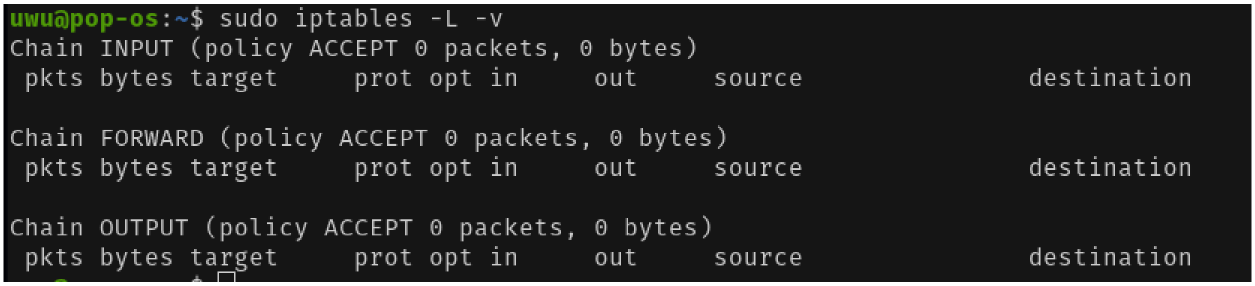
```
uwu@pop-os:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp4s0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq_codel state DOWN group defa
ult qlen 1000
    link/ether d8:bb:c1:74:fe:b3 brd ff:ff:ff:ff:ff:ff
3: wlo1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qle
n 1000
    link/ether dc:21:5c:f4:d7:bf brd ff:ff:ff:ff:ff:ff
    altname wlp0s20f3
    inet 192.168.203.227/24 brd 192.168.203.255 scope global dynamic noprefixroute wlo1
       valid_lft 3162sec preferred_lft 3162sec
    inet6 2402:8100:30a0:39bf:c7ba:ba4b:fe2f:54ca/64 scope global temporary dynamic
       valid_lft 3227sec preferred_lft 3227sec
    inet6 2402:8100:30a0:39bf:337f:c996:3915:203c/64 scope global dynamic mngtmpaddr noprefi
```



```
uwu@pop-os:~$ ip route
default via 192.168.203.166 dev wlo1 proto dhcp metric 600
169.254.0.0/16 dev wlo1 scope link metric 1000
192.168.203.0/24 dev wlo1 proto kernel scope link src 192.168.203.227 metric 600
uwu@pop-os:~$
```



```
uwu@pop-os:~$ netstat -rn
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
0.0.0.0         192.168.203.166 0.0.0.0         UG        0 0          0 wlo1
169.254.0.0     0.0.0.0         255.255.0.0     U         0 0          0 wlo1
192.168.203.0   0.0.0.0         255.255.255.0   U         0 0          0 wlo1
uwu@pop-os:~$
```



```
uwu@pop-os:~$ sudo iptables -L -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

Conclusion: Able to configure linux network with iptables, netstat and route

Mahavir Education Trust's

SHAH & ANCHOR KUTCHHI ENGINEERING COLLEGE

Chembur, Mumbai - 400 088

UG Program in Cyber Security

Experiment Number: 7					
Date of Performance:		24-08-2022			
Date of Submission:		07-09-2022			
Program Execution/ formation/ correction/ ethical practices (07)	**Documentation (02)**	**Timely Submission (03)**	**Viva Answer to sample questions (03)**	**Experiment Total (15)**	**Sign**
07	02	03	02	14	PPatel

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

Laboratory Outcome: CSL5026

Related Theory:

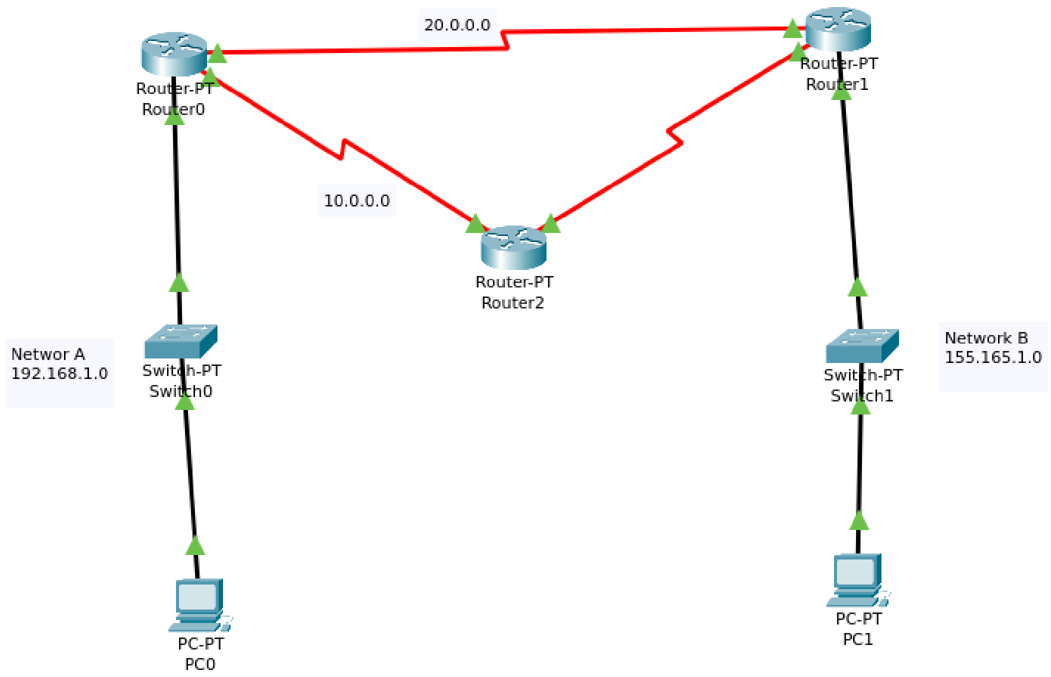
A virtual private network, better known as a VPN, gives you online privacy and anonymity by creating a private network from a public internet connection. VPNs mask your internet protocol (IP) address so your online actions are virtually untraceable. Most important, VPN services establish secure and encrypted connections to provide greater privacy than even a secured Wi-Fi hotspot.

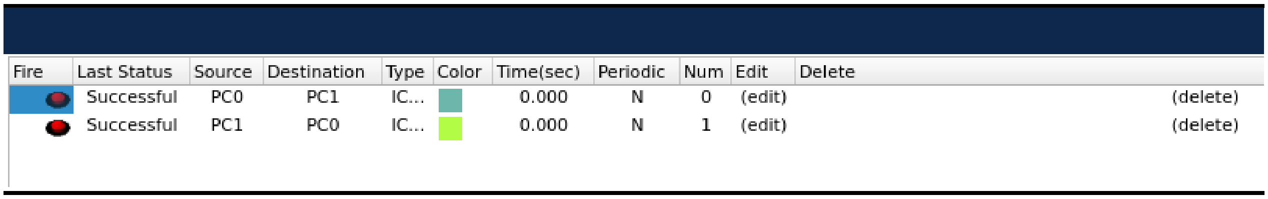
RIP (Routing Information Protocol), is an example of distance vector routing for local networks. RIP works to deliver the whole routing table to all active interfaces every 30 seconds. In RIP protocol, hop count is the only metrics to decide the best path to a remote network. Let's take an example to see how RIP protocol works: Assuming, we have two paths available from the Source to the Destination. It is clear that Path 2 will be selected by RIP protocol since it has fewer hop counts.

OSPF (Open Shortest Path First), a link-state routing protocol, is massively adopted in large enterprise networks. OSPF routing protocol collects link state information from routers in the network and determines the routing table information to forward packets. This occurs by creating a topology map for the network.Unlike RIP, OSPF only exchanges routing information when there’s a change in network topology. OSPF protocol best fits for complex networks that comprise multiple subnets working to ease network administration and optimize traffic. It effectively calculates the shortest path with minimum network traffic when the change occurs.

Program Listing And Output:

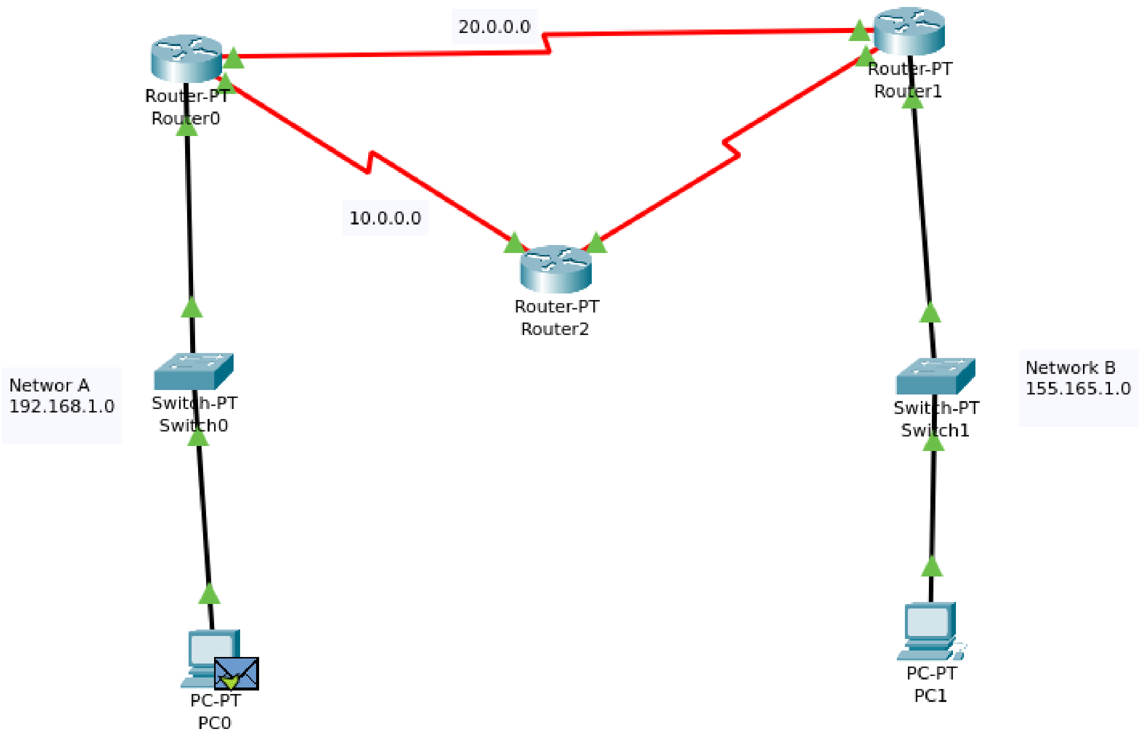
Realtime :

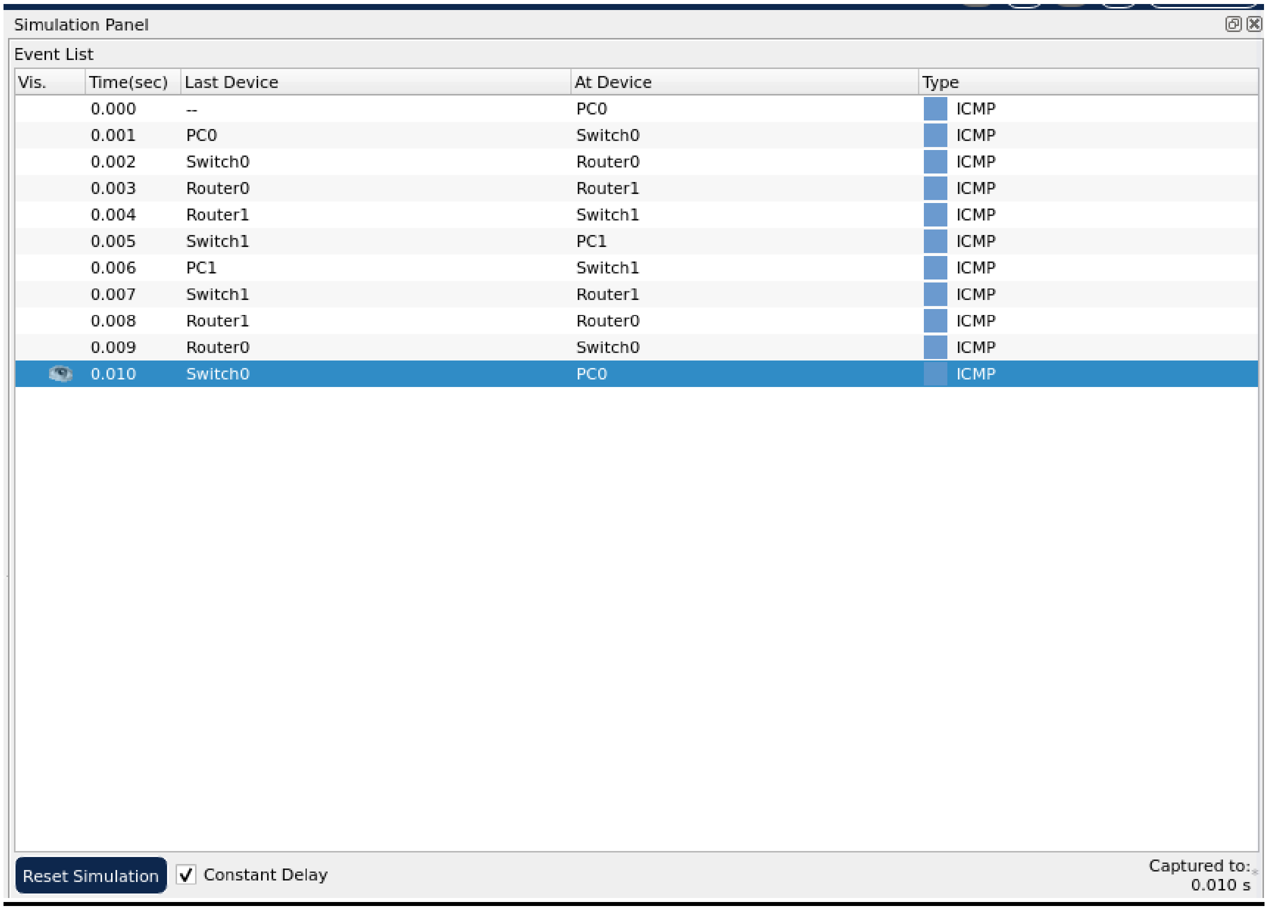




Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
●	Successful	PC0	PC1	IC...	🟩	0.000	N	0	(edit)	(delete)
●	Successful	PC1	PC0	IC...	🟩	0.000	N	1	(edit)	(delete)

<u>Simulation :</u>


20.0.0.0
Router-PT
Router0
Router-PT
Router1
10.0.0.0
Router-PT
Router2
Networ A
192.168.1.0
Switch-PT
Switch0
Switch-PT
Switch1
Network B
155.165.1.0
PC-PT
PC0
PC-PT
PC1



Simulation Panel

Event List

Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	PC0	🟦 ICMP
	0.001	PC0	Switch0	🟦 ICMP
	0.002	Switch0	Router0	🟦 ICMP
	0.003	Router0	Router1	🟦 ICMP
	0.004	Router1	Switch1	🟦 ICMP
	0.005	Switch1	PC1	🟦 ICMP
	0.006	PC1	Switch1	🟦 ICMP
	0.007	Switch1	Router1	🟦 ICMP
	0.008	Router1	Router0	🟦 ICMP
	0.009	Router0	Switch0	🟦 ICMP
👁	0.010	Switch0	PC0	🟦 ICMP

Captured to:
0.010 s

<u>Conclusion: </u>Able to use cisco packet racer for designing VPN and configure OSPF.

Mahavir Education Trust's

SHAH & ANCHOR KUTCHHI ENGINEERING COLLEGE

Chembur, Mumbai - 400 088

UG Program in Cyber Security

Experiment Number: 8					
Date of Performance:		**07-09-2022**			
Date of Submission:		**14-09-2022**			
Program Execution/ formation/ correction/ ethical practices (07)	**Documentation (02)**	**Timely Submission (03)**	**Viva Answer to sample questions (03)**	**Experiment Total (15)**	**Sign**
07	02	02	03	14	PPatel

Aim: Socket programming using TCP or UDP

Laboratory Outcome: CSL5024

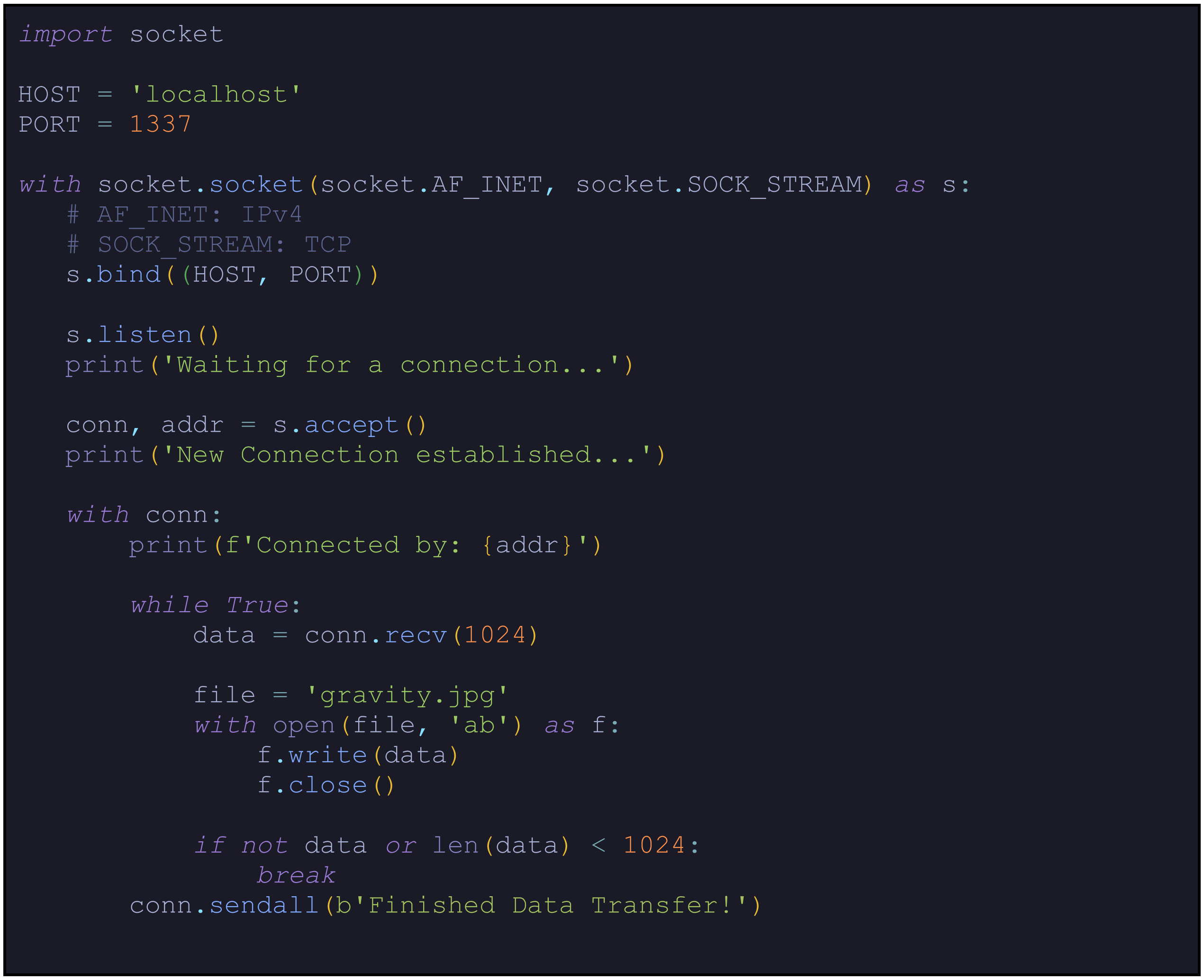
Related Theory:

The **Transmission Control Protocol** (**TCP**) is one of the main protocols of the Internet protocol suite. It originated in the initial network implementation in which it complemented the Internet Protocol (IP). Therefore, the entire suite is commonly referred to as TCP/IP. TCP provides reliable, ordered, and error-checked delivery of a stream of octets (bytes) between applications running on hosts communicating via an IP network. Major internet applications such as the World Wide Web, email, remote administration, and file transfer rely on TCP, which is part of the Transport Layer of the TCP/IP suite. SSL/TLS often runs on top of TCP.

The User Datagram Protocol, or UDP, is a communication protocol used across the Internet for especially time-sensitive transmissions such as video playback or DNS lookups. It speeds up communications by not formally establishing a connection before data is transferred. This allows data to be transferred very quickly, but it can also cause packets to become lost in transit — and create opportunities for exploitation in the form of DDoS attacks.

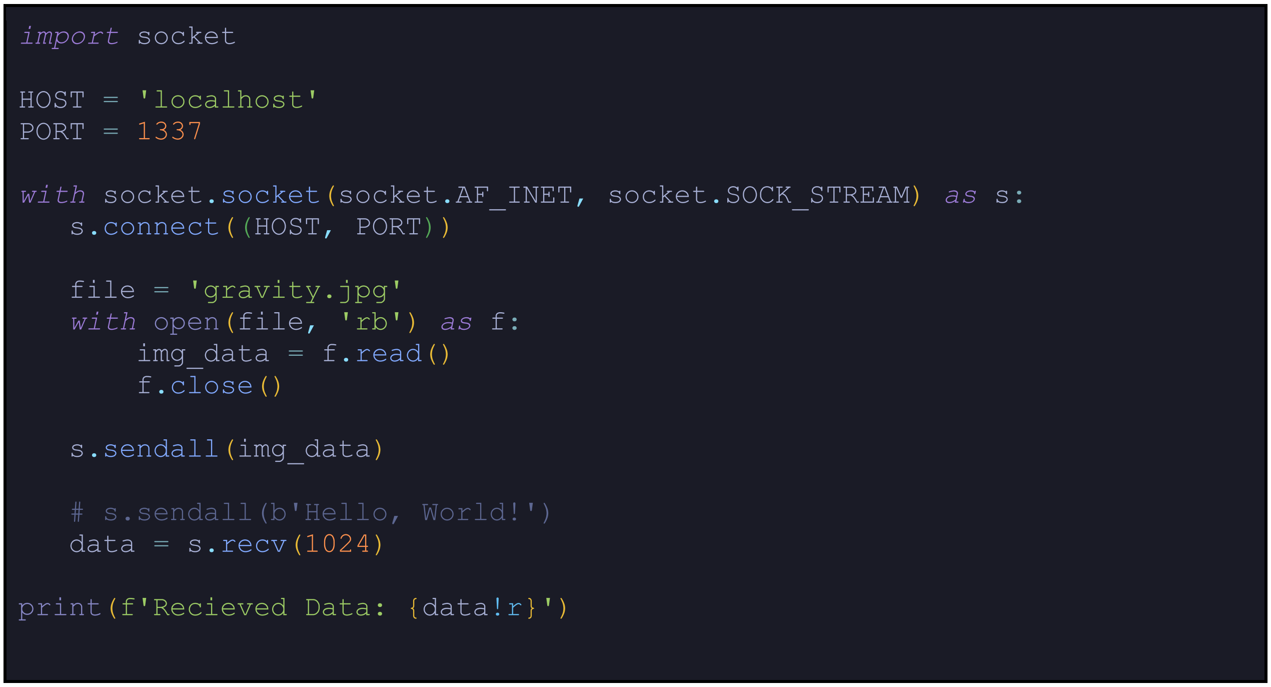
Program Listing And Output:

Server.py



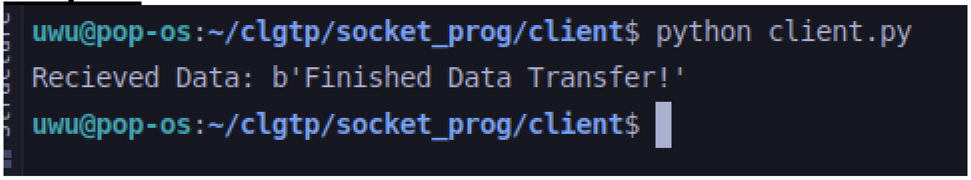
```python
import socket

HOST = 'localhost'
PORT = 1337

with socket.socket(socket.AF_INET, socket.SOCK_STREAM) as s:
   # AF_INET: IPv4
   # SOCK_STREAM: TCP
   s.bind((HOST, PORT))

   s.listen()
   print('Waiting for a connection...')

   conn, addr = s.accept()
   print('New Connection established...')

   with conn:
       print(f'Connected by: {addr}')

       while True:
           data = conn.recv(1024)

           file = 'gravity.jpg'
           with open(file, 'ab') as f:
               f.write(data)
               f.close()

           if not data or len(data) < 1024:
               break
       conn.sendall(b'Finished Data Transfer!')
```

Client.py

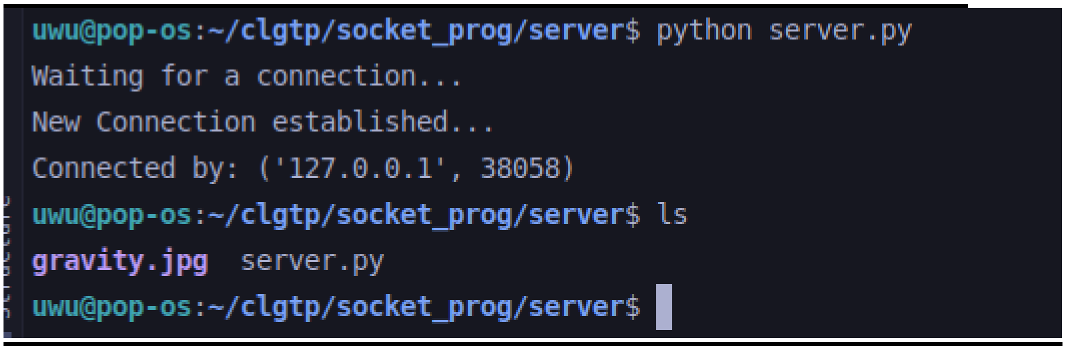


```
import socket

HOST = 'localhost'
PORT = 1337

with socket.socket(socket.AF_INET, socket.SOCK_STREAM) as s:
   s.connect((HOST, PORT))

   file = 'gravity.jpg'
   with open(file, 'rb') as f:
       img_data = f.read()
       f.close()

   s.sendall(img_data)

   # s.sendall(b'Hello, World!')
   data = s.recv(1024)

print(f'Recieved Data: {data!r}')
```

Output :



```
uwu@pop-os:~/clgtp/socket_prog/client$ python client.py
Recieved Data: b'Finished Data Transfer!'
uwu@pop-os:~/clgtp/socket_prog/client$
```



```
uwu@pop-os:~/clgtp/socket_prog/server$ python server.py
Waiting for a connection...
New Connection established...
Connected by: ('127.0.0.1', 38058)
uwu@pop-os:~/clgtp/socket_prog/server$ ls
gravity.jpg  server.py
uwu@pop-os:~/clgtp/socket_prog/server$
```

Conclusion: Able to create socket program for file transfer.

Mahavir Education Trust's

SHAH & ANCHOR KUTCHHI ENGINEERING COLLEGE

Chembur, Mumbai - 400 088

UG Program in Cyber Security

Experiment Number: 9					
Date of Performance:	**14-09-2022**				
Date of Submission:	**23-09-2022**				
Program Execution/ formation/ correction/ ethical practices (07)	**Documentation (02)**	**Timely Submission (03)**	**Viva Answer to sample questions (03)**	**Experiment Total (15)**	**Sign**
07	02	03	03	15	PPatel

Aim: Perform File Transfer and Access using FTP **.**

Laboratory Outcome: CSL5023

Related Theory:

File transfer protocol (FTP) is an Internet tool provided by TCP/IP. The first feature of FTP is developed by Abhay Bhushan in 1971. It helps to transfer files from one computer to another by providing access to directories or folders on remote computers and allows software, data, text file to be transferred between different kinds of computers. The end-user in the connection is known as localhost and the server which provides data is known as the remote host.

The goals of FTP are:

- It encourages the direct use of remote computers.
- It shields users from system variations (operating system, directory structures, file structures, etc.)
- It promotes sharing of files and other types of data.

Why FTP?

FTP is a standard communication protocol. There are various other protocols like HTTP which are used to transfer files between computers, but they lack clarity and focus as compared to FTP. Moreover, the systems involved in connection are heterogeneous systems, i.e. they differ in operating systems, directory, structures, character sets, etc the FTP shields the user from these differences and transfer data efficiently and reliably. FTP can transfer ASCII, EBCDIC, or image files. The ASCII is the default file share format, in this, each character is encoded by NVT ASCII. In ASCII or EBCDIC the destination must be ready to accept files in this mode. The image file format is the default format for transforming binary files.

FTP Clients

FTP works on a client-server model. The FTP client is a program that runs on the user’s computer to enable the user to talk to and get files from remote computers. It is a set of commands that establishes the connection between two hosts, helps to transfer the files, and then closes the connection. Some of the commands are: *get filename(retrieve the file from server), mget filename(retrieve multiple files from* the *server), ls(lists files available in the current directory of the server).* There are also built-in FTP programs, which makes it easier to transfer files and it does not require remembering the commands.

Type of FTP Connections

FTP connections are of two types:

Active FTP connection: In an Active FTP connection, the client establishes the command channel and the server establishes the data channel. When the client requests the data over the connection the server initiates the transfer of the data to the client. It is not the default connection because it may cause problems if there is a firewall in between the client and the server.

Passive FTP connection: In a Passive FTP connection, the client establishes both the data channel as well as the command channel. When the client requests the data over the connection, the server sends a random port number to the client, as soon as the client receives this port number it establishes the data channel. It is the default connection, as it works better even if the client is protected by the firewall.

Anonymous FTP

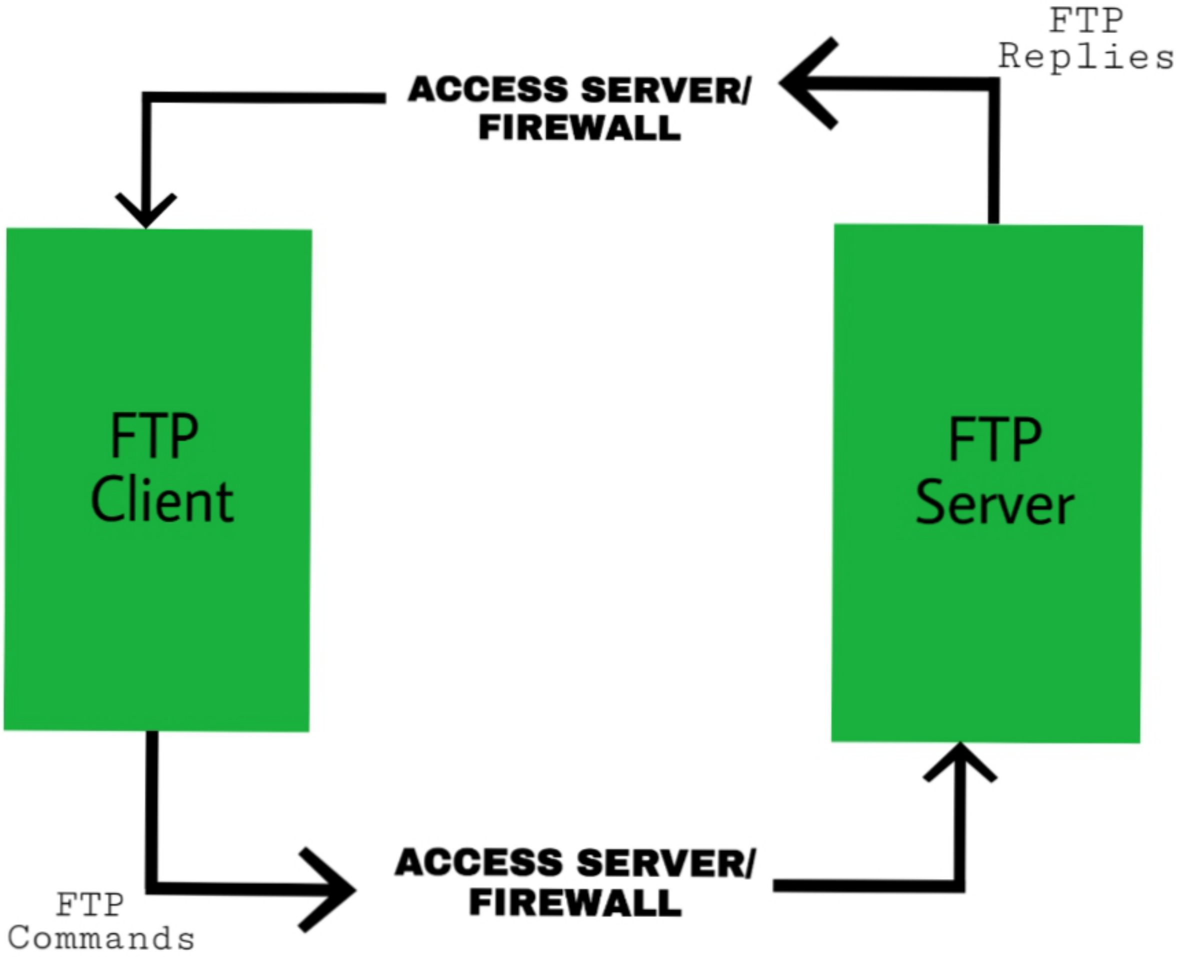
Some sites can enable anonymous FTP whose files are available for public access. So, the user can access those files without any username or password. Instead, the username is set to anonymous and the password to the guest by default. Here, the access of the user is very limited. For example, the user can copy the files but not allowed to navigate through directories.

How FTP works?

The FTP connection is established between two systems and they communicate with each other using a network. So, for the connection, the user can get permission by providing the credentials to the FTP server or can use anonymous FTP.

When an FTP connection is established, there are two types of communication channels are also established and they are known as command channel and data channel. The command channel is used to transfer the commands and responses from client to server and server to client. FTP uses the same approach as TELNET or SMTP to communicate across the control connection. It uses the NVT ASCII character set for communication. It uses port number 21. Whereas the data channel is used to actually transfer the data between client and server. It uses port number 20.

The FTP client using the URL gives the FTP command along with the FTP server address. As soon as the server and the client get connected to the network, the user logins using User ID and password. If the user is not registered with the server, then also he/she can access the files by using the anonymous login where the password is the client’s email address. The server verifies the user login and allows the client to access the files. The client transfers the desired files and exits the connection. The figure below shows the working of FTP.



Transmission mode

FTP transfer files using any of the following modes:

- **Stream Mode:** It is the default mode. In steam mode, the data is transferred from FTP to TCP in stream bytes. Here TCP is the cause for fragmenting data into small segments. The connection is automatically closed if the transforming data is in the stream bytes. Otherwise, the sender will close the connection.
- **Block Mode:** In block mode, the data is transferred from FTP to TCP in the form of blocks, and each block followed by a 3-byte header. The first byte of the block contains the information about the block so it is known as the description block and the other two bytes contain the size of the block.
- **Compressed Mode:** This mode is used to transfer big files. As we know that, due to the size limit we can not transfer big files on the internet, so the compressed mode is used to decrease the size of the file into small and send it on the internet.

Applications of FTP

The following are the applications of FTP:

- FTP connection is used by different big business organizations for transferring files in between them, like sharing files to other employees working at different locations or different branches of the organization.
- FTP connection is used by IT companies to provide backup files at disaster recovery sites.
- Financial services use FTP connections to securely transfer financial documents to the respective company, organization, or government.
- Employees use FTP connections to share any data with their co-workers.

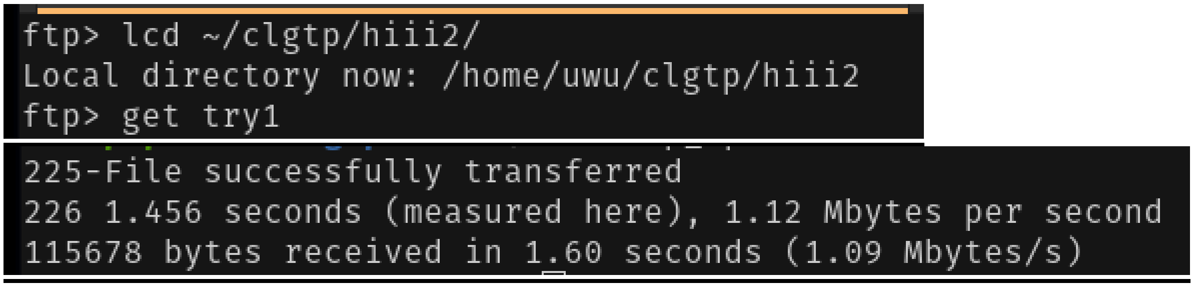
Advantages

- **Multiple transfers:** FTP helps to transfer multiple large files in between the systems.
- **Efficiency:** FTP helps to organize files in an efficient manner and transfer them efficiently over the network.
- **Security:** FTP provides access to any user only through user ID and password. Moreover, the server can create multiple levels of access.
- **Continuous transfer:** If the transfer of the file is interrupted by any means, then the user can resume the file transfer whenever the connection is established.
- **Simple:** FTP is very simple to implement and use, thus it is a widely used connection.
- **Speed:** It is the fastest way to transfer files from one computer to another.

Disadvantages

- **Less security:** FTP does not provide an encryption facility when transferring files. Moreover, the username and passwords are in plain text and not a combination of symbols, digits, and alphabets, which makes it easier to be attacked by hackers.
- **Old technology:** FTP is one of the oldest protocols and thus it uses multiple TCP/IP connections to transfer files. These connections are hindered by firewalls.
- **Virus:** The FTP connection is difficult to be scanned for viruses, which again increases the risk of vulnerability.
- **Limited:** The FTP provides very limited user permission and mobile device access.
- **Memory and programming:** FTP requires more memory and programming efforts, as it is very difficult to find errors without the commands.

Program Listing And Output:



```
ftp> lcd ~/clgtp/hiii2/
Local directory now: /home/uwu/clgtp/hiii2
ftp> get try1
```

```
225-File successfully transferred
226 1.456 seconds (measured here), 1.12 Mbytes per second
115678 bytes received in 1.60 seconds (1.09 Mbytes/s)
```

Conclusion: Able to transfer files and data on ftp protocol from linux.

Mahavir Education Trust's

SHAH & ANCHOR KUTCHHI ENGINEERING COLLEGE

Chembur, Mumbai - 400 088

UG Program in Cyber Security

Experiment Number: 10					
Date of Performance:	**23-09-2022**				
Date of Submission:	**30-09-2022**				
Program Execution/ formation/ correction/ ethical practices (07)	**Documentation (02)**	**Timely Submission (03)**	**Viva Answer to sample questions (03)**	**Experiment Total (15)**	**Sign**
07	02	02	03	14	PPatel

Aim: Perform Remote login using Telnet server.

Laboratory Outcome: CSL5023

Related Theory:

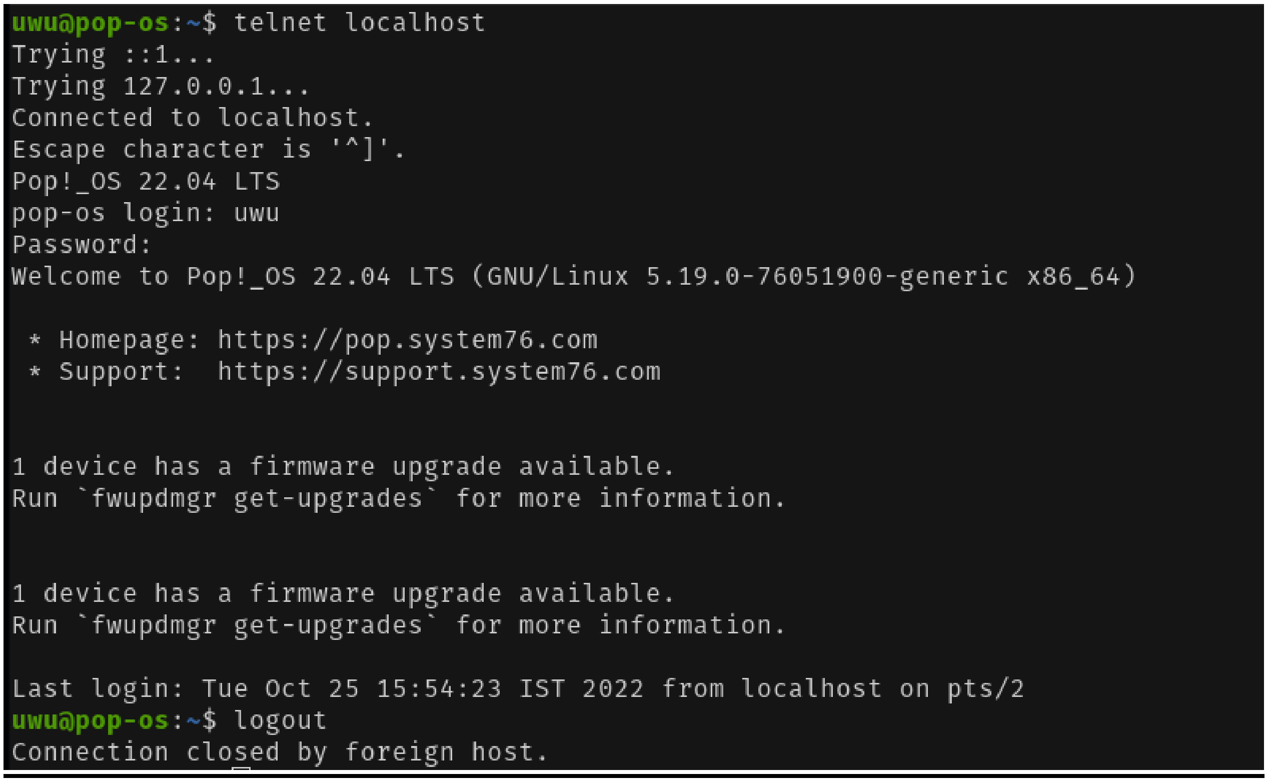
Telnet is an application protocol used on the Internet or local area network to provide a bidirectional interactive text-oriented communication facility using a virtual terminal connection.User data is interspersed in-band with Telnet control information in an 8-bit byte oriented data connection over the Transmission Control Protocol (TCP).

Telnet was developed in 1969 beginning with RFC 15, extended in RFC 855, and standardized as Internet Engineering Task Force (IETF) Internet Standard STD 8, one of the first Internet standards. The name stands for "**tel**etype **net**work".

Historically, Telnet provided access to a command-line interface on a remote host. However, because of serious security concerns when using Telnet over an open network such as the Internet, its use for this purpose has waned significantly in favor of SSH

The term *telnet* is also used to refer to the software that implements the client part of the protocol. Telnet client applications are available for virtually all computer platforms. *Telnet* is also used as a verb. *To telnet* means to establish a connection using the Telnet protocol, either with a command line client or with a graphical interface. For example, a common directive might be: "*To change your password, telnet into the server, log in and run the passwd command.*" In most cases, a user would be *telnetting* into a Unix-like server system or a network device (such as a router).

Program Listing And Output:



```
uwu@pop-os:~$ telnet localhost
Trying ::1...
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
Pop!_OS 22.04 LTS
pop-os login: uwu
Password:
Welcome to Pop!_OS 22.04 LTS (GNU/Linux 5.19.0-76051900-generic x86_64)

 * Homepage: https://pop.system76.com
 * Support:  https://support.system76.com


1 device has a firmware upgrade available.
Run `fwupdmgr get-upgrades` for more information.


1 device has a firmware upgrade available.
Run `fwupdmgr get-upgrades` for more information.

Last login: Tue Oct 25 15:54:23 IST 2022 from localhost on pts/2
uwu@pop-os:~$ logout
Connection closed by foreign host.
```

Conclusion: Able to use telnet to set up a remote connection.

Mahavir Education Trust's

SHAH & ANCHOR KUTCHHI ENGINEERING COLLEGE

Chembur, Mumbai - 400 088

UG Program in Cyber Security

Experiment Number: 11					
Date of Performance:		**30-09-2022**			
Date of Submission:		**07-10-2022**			
Program Execution/ formation/ correction/ ethical practices (07)	**Documentation (02)**	**Timely Submission (03)**	**Viva Answer to sample questions (03)**	**Experiment Total (15)**	**Sign**
07	02	03	03	15	PPatel

Aim:- Study and implement SNMP format.

Laboratory Outcome: CSL5026

Related Theory: If an organization has 1000 devices then to check all devices, one by one every day, are working properly or not is a hectic task. To ease these up, Simple Network Management Protocol (SNMP) is used.

Simple Network Management Protocol (SNMP) –

SNMP is an application layer protocol that uses UDP port number 161/162.SNMP is used to monitor the network, detect network faults, and sometimes even used to configure remote devices.

SNMP components –

There are 3 components of SNMP:

1. **SNMP Manager –**
   It is a centralized system used to monitor network. It is also known as Network Management Station (NMS)

2. **SNMP agent –**
   It is a software management software module installed on a managed device. Managed devices can be network devices like PC, routers, switches, servers, etc.

3. **Management Information Base –**
   MIB consists of information on resources that are to be managed. This information is organized hierarchically. It consists of objects instances which are essentially variables.

SNMP messages –

Different variables are:

1. **GetRequest –**
   SNMP manager sends this message to request data from the SNMP agent. It is simply used to retrieve data from SNMP agents. In response to this, the SNMP agent responds with the requested value through a response message.

2. **GetNextRequest –**
   This message can be sent to discover what data is available on an SNMP agent. The SNMP manager can request data continuously until no more data is left. In this way, the SNMP manager can take knowledge of all the available data on SNMP agents.

3. **GetBulkRequest –**
   This message is used to retrieve large data at once by the SNMP manager

from the SNMP agent. It is introduced in SNMPv2c.

4. **SetRequest –**
   It is used by the SNMP manager to set the value of an object instance on the SNMP agent.

5. **Response –**
   It is a message sent from the agent upon a request from the manager. When sent in response to Get messages, it will contain the data requested. When sent in response to the Set message, it will contain the newly set value as confirmation that the value has been set.

6. **Trap –**
   These are the message sent by the agent without being requested by the manager. It is sent when a fault has occurred.

7. **InformRequest –**
   It was introduced in SNMPv2c, used to identify if the trap message has been received by the manager or not. The agents can be configured to send trap message continuously until it receives an Inform message. It is the same as a trap but adds an acknowledgement that the trap doesn’t provide.

SNMP security levels –

It defines the type of security algorithm performed on SNMP packets. These are used in only SNMPv3. There are 3 security levels namely:

1. **noAuthNoPriv –**
   This (no authentication, no privacy) security level uses a community string for authentication and no encryption for privacy.

2. **authNopriv –** This security level (authentication, no privacy) uses HMAC with Md5 for authentication and no encryption is used for privacy.

3. **authPriv –** This security level (authentication, privacy) uses HMAC with Md5 or SHA for authentication and encryption uses the DES-56 algorithm.

SNMP versions –

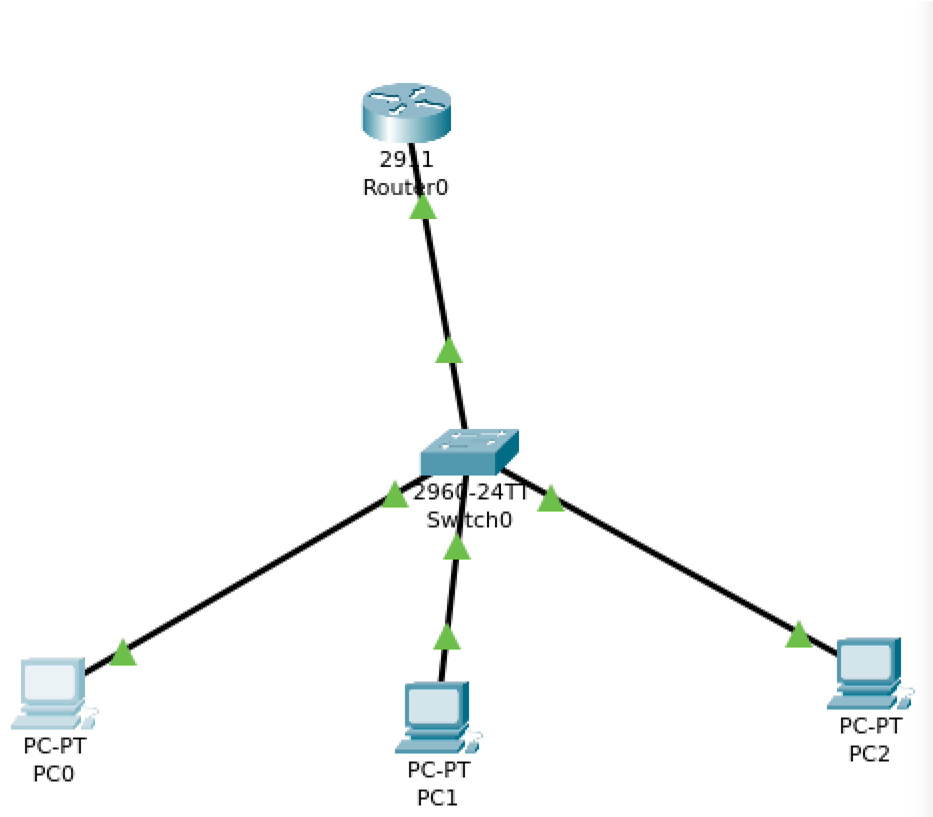
There are 3 versions of SNMP:

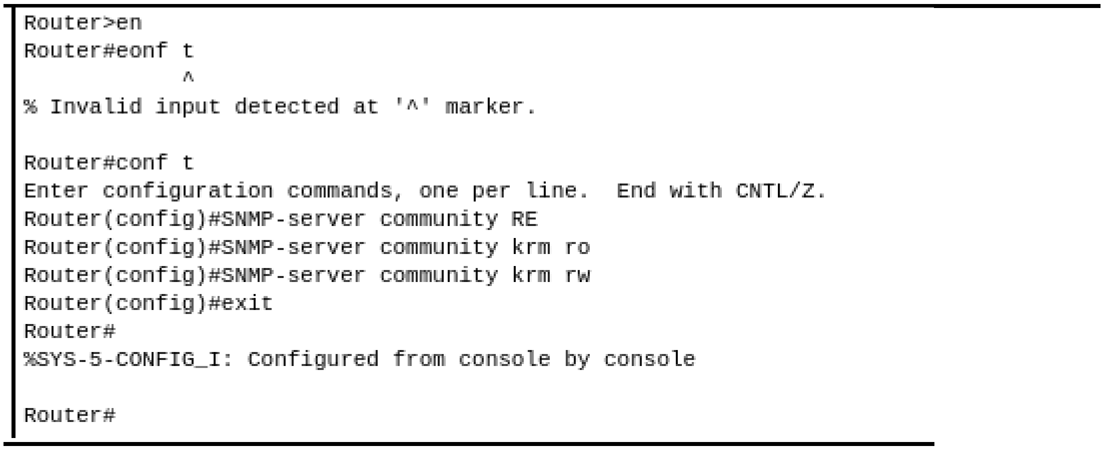
1. **SNMPv1 –**
   It uses community strings for authentication and uses UDP only.

2. **SNMPv2c –**
   It uses community strings for authentication. It uses UDP but can be configured to use TCP.

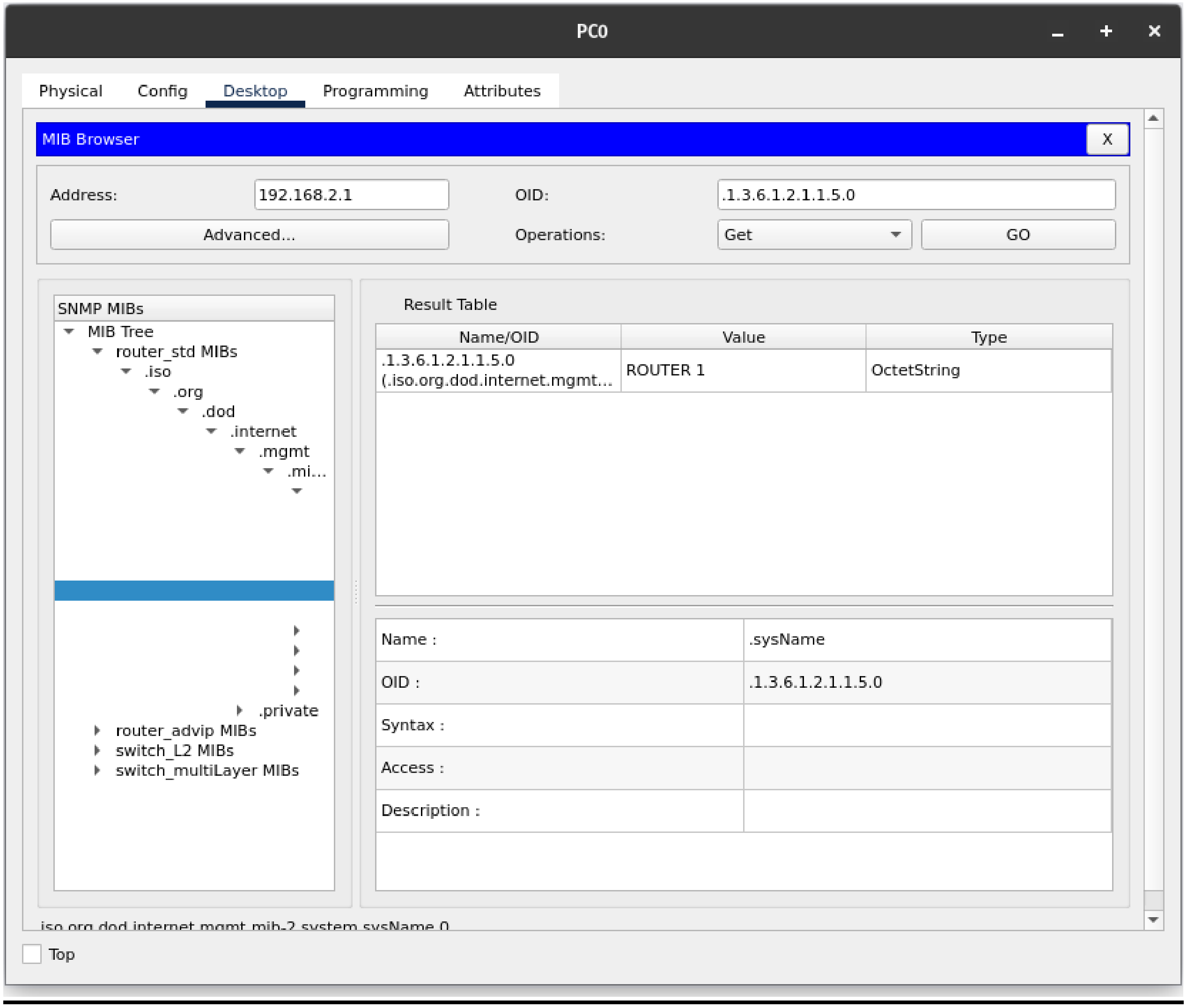
3. **SNMPv3 –**
   It uses Hash-based MAC with MD5 or SHA for authentication and DES-56 for privacy. This version uses TCP. Therefore, the conclusion is the higher the version of SNMP, the more secure it will be.

Program Listing And Output:





```
Router>en
Router#eonf t
        ^
% Invalid input detected at '^' marker.

Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#SNMP-server community RE
Router(config)#SNMP-server community krm ro
Router(config)#SNMP-server community krm rw
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#
```



Address: 192.168.2.1

OID: .1.3.6.1.2.1.1.5.0

Operations: Get

Result Table

Name/OID	Value	Type
.1.3.6.1.2.1.1.5.0 (.iso.org.dod.internet.mgmt...	ROUTER 1	OctetString

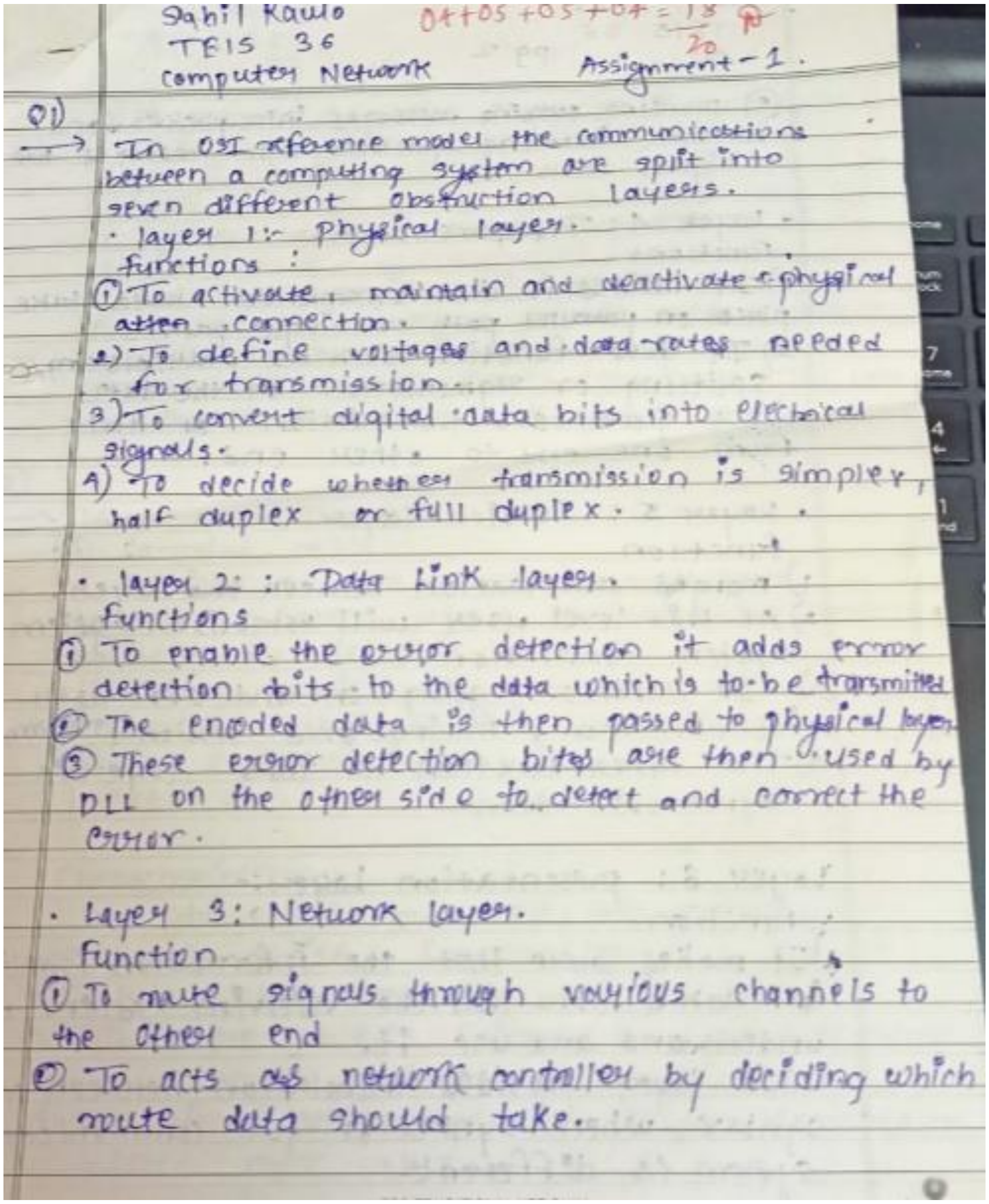
Name :	.sysName
OID :	.1.3.6.1.2.1.1.5.0
Syntax :	
Access :	
Description :	

.iso.org.dod.internet.mgmt.mib-2.system.sysName.0

Conclusion: Able to create and configure a SNMP connection in cisco packet tracer.

Assignment 1

Marks: 18/20



Sahil Kawo
TEIS 36
computer Network

04+05+05+04 = $\frac{18}{20}$

Assignment - 1.

Q1)

→ In OSI reference model the communications between a computing system are split into seven different obstruction layers.

· layer 1:- physical layer.

functions :

① To activate, maintain and deactivate physical ~~atten~~ connection.

2) To define voltages and data-rates needed for transmission.

3) To convert digital data bits into electrical signals.

4) To decide whether transmission is simplex, half duplex or full duplex.

· layer 2: : Data Link layer.

functions

① To enable the error detection it adds error detection bits to the data which is to-be transmitted

② The encoded data is then passed to physical layer

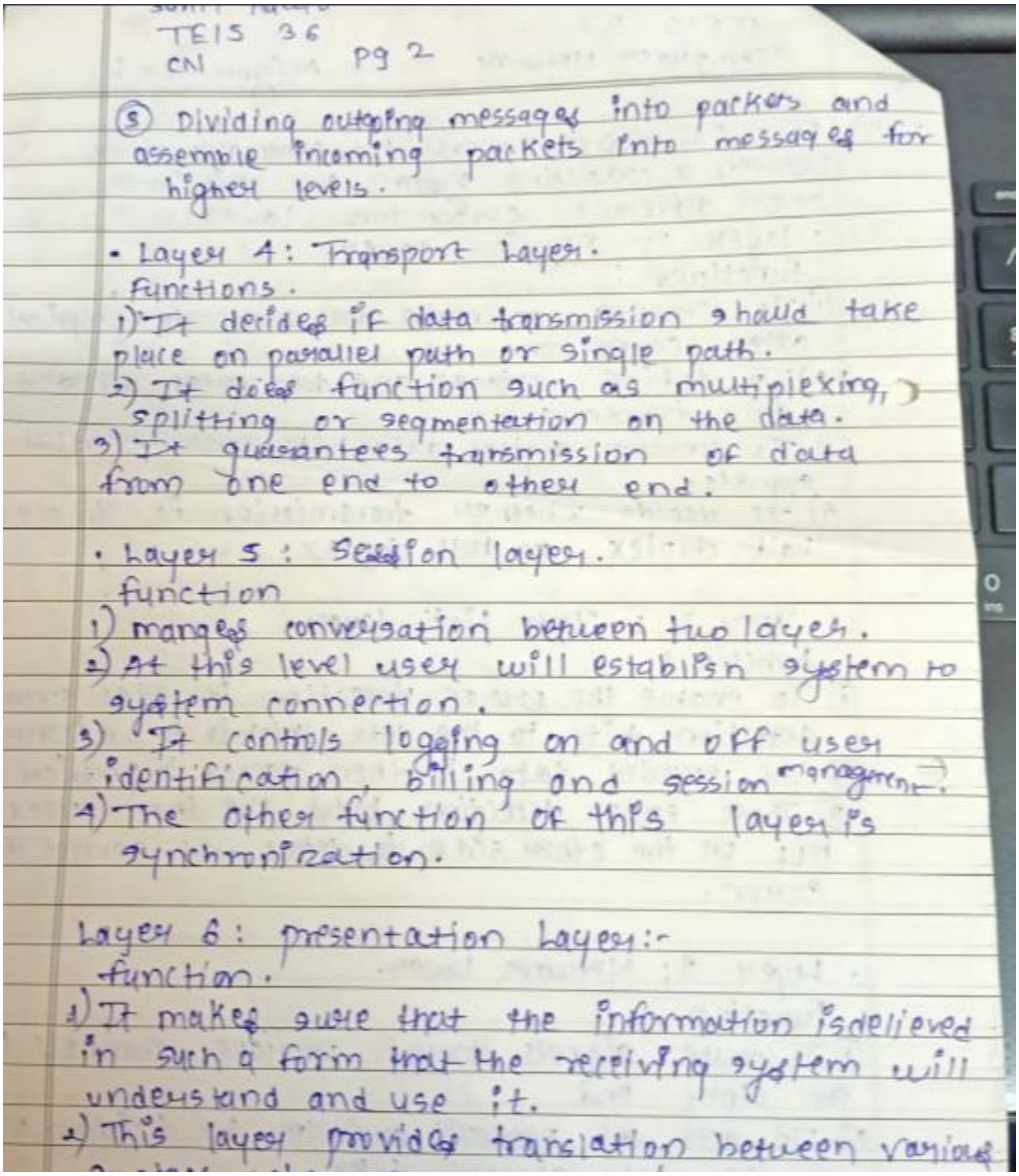
③ These error detection bites are then used by DLL on the other side to detect and correct the error.

· Layer 3: Network layer.

Function

① To route signals through various channels to the other end

② To acts as network controller by deciding which route data should take.



TEIS 36
CN pg 2

⑤ Dividing outgoing messages into packets and assemble incoming packets into messages for higher levels.

- Layer 4: Transport Layer.

Functions.

1) It decides if data transmission should take place on parallel path or single path.

2) It does function such as multiplexing, splitting or segmentation on the data.

3) It guarantees transmission of data from one end to other end.

- Layer 5: Session layer.

function

1) manages conversation between two layer.

2) At this level user will establish system to system connection.

3) It controls logging on and off user identification, billing and session management.

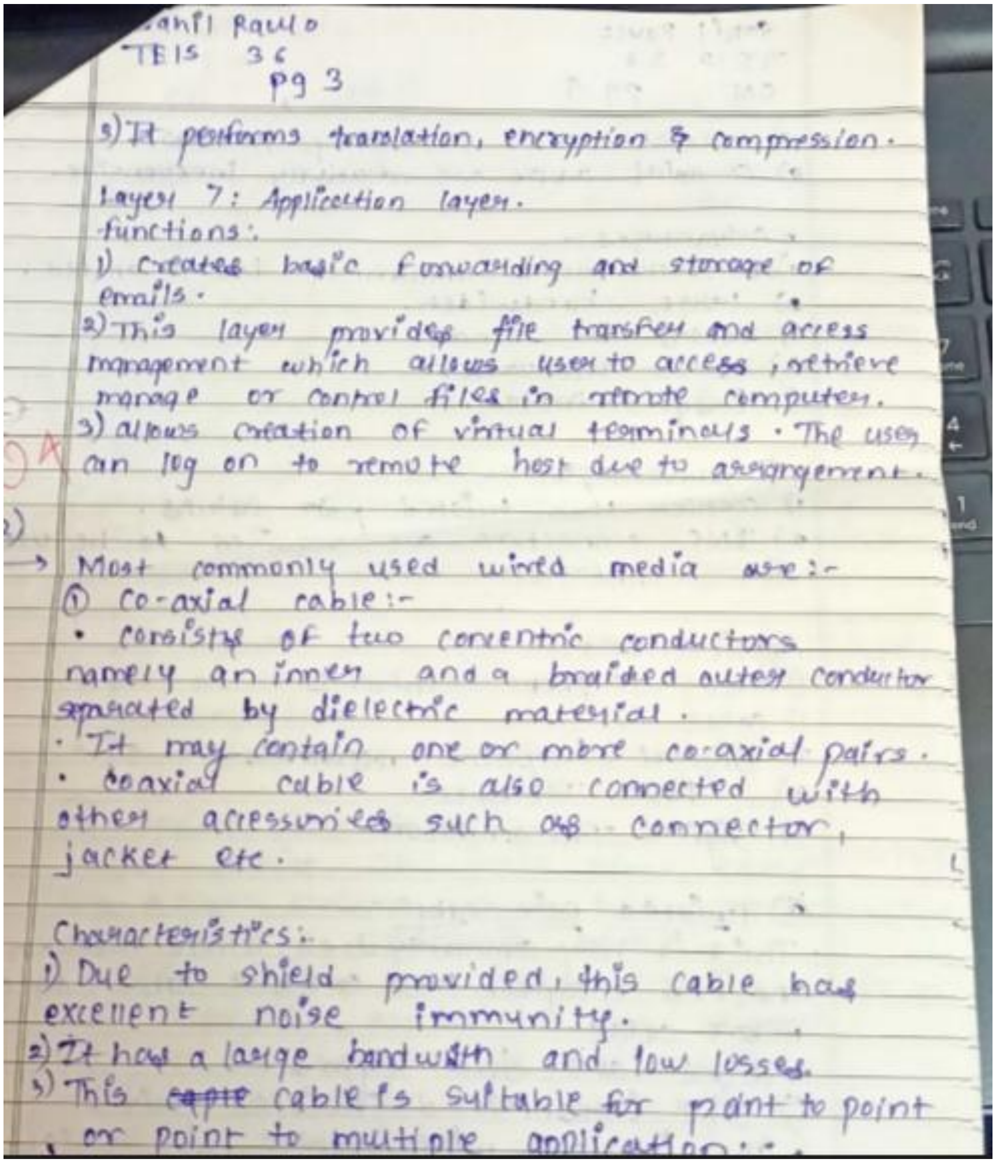
4) The other function of this layer is synchronization.

Layer 6: presentation Layer:-

function.

1) It makes sure that the information is delieved in such a form that the receiving system will understand and use it.

2) This layer provides translation between various



anil Raulo
TE IS 36
pg 3

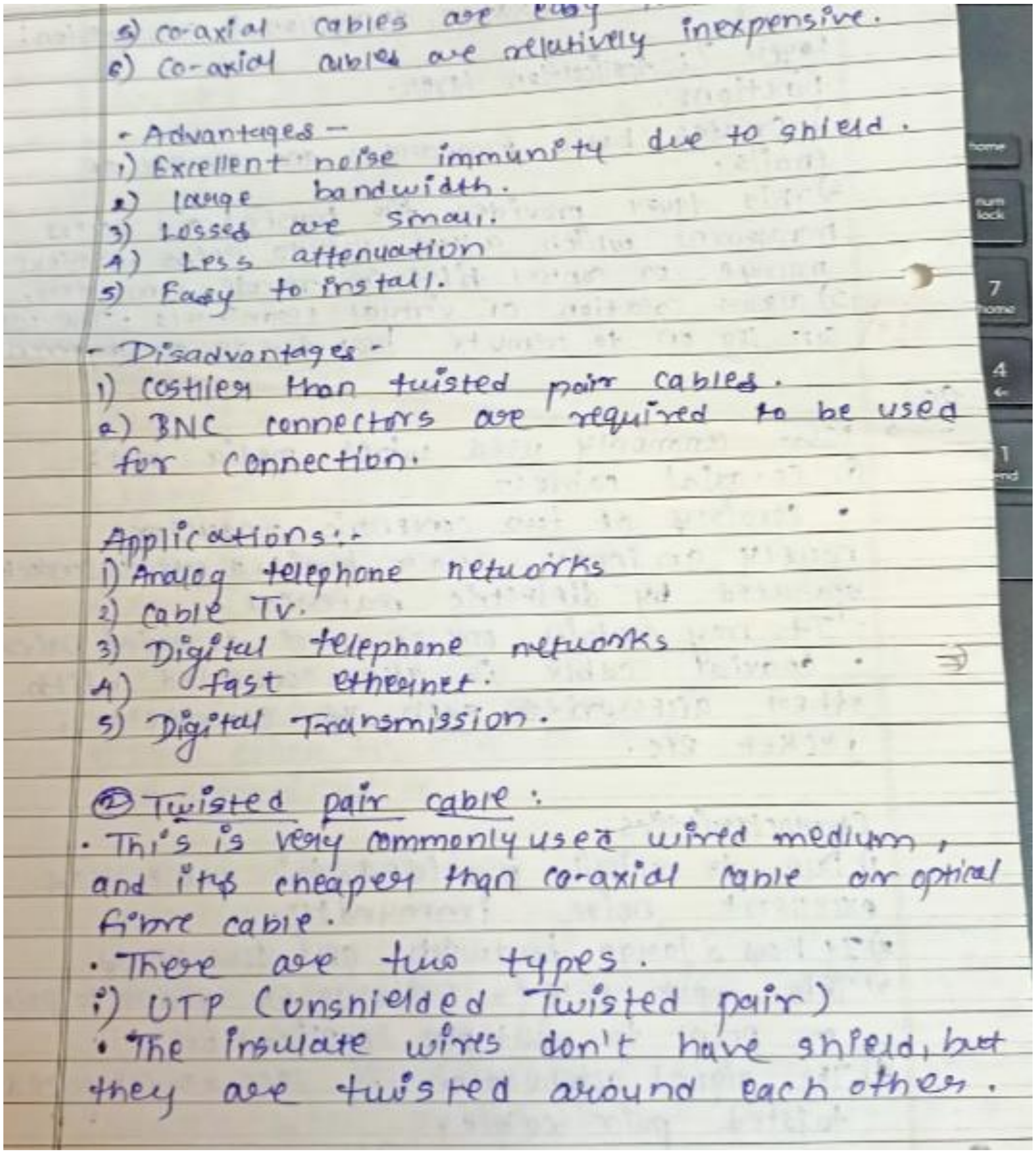
3) It performs translation, encryption & compression.

Layer 7: Application layer.
functions:
1) creates basic forwarding and storage of emails.
2) This layer provides file transfer and access management which allows user to access, retrieve manage or control files in remote computer.
3) allows creation of virtual terminals. The user can log on to remote host due to arrangement.

2)

→ Most commonly used wired media are:-
① Co-axial cable:-
• consists of two concentric conductors namely an inner and a braided outer conductor separated by dielectric material.
• It may contain one or more co-axial pairs.
• coaxial cable is also connected with other accessories such as connector, jacket etc.

Characteristics:
1) Due to shield provided, this cable has excellent noise immunity.
2) It has a large bandwidth and low losses.
3) This ~~cable~~ cable is suitable for point to point or point to multiple application:.



5) co-axial cables are easy

6) Co-axial cables are relatively inexpensive.

- Advantages –

1) Excellent noise immunity due to shield.
2) large bandwidth.
3) Losses are small.
4) Less attenuation
5) Easy to install.

- Disadvantages -

1) costlier than twisted pair cables.
2) BNC connectors are required to be used for connection.

Applications :-

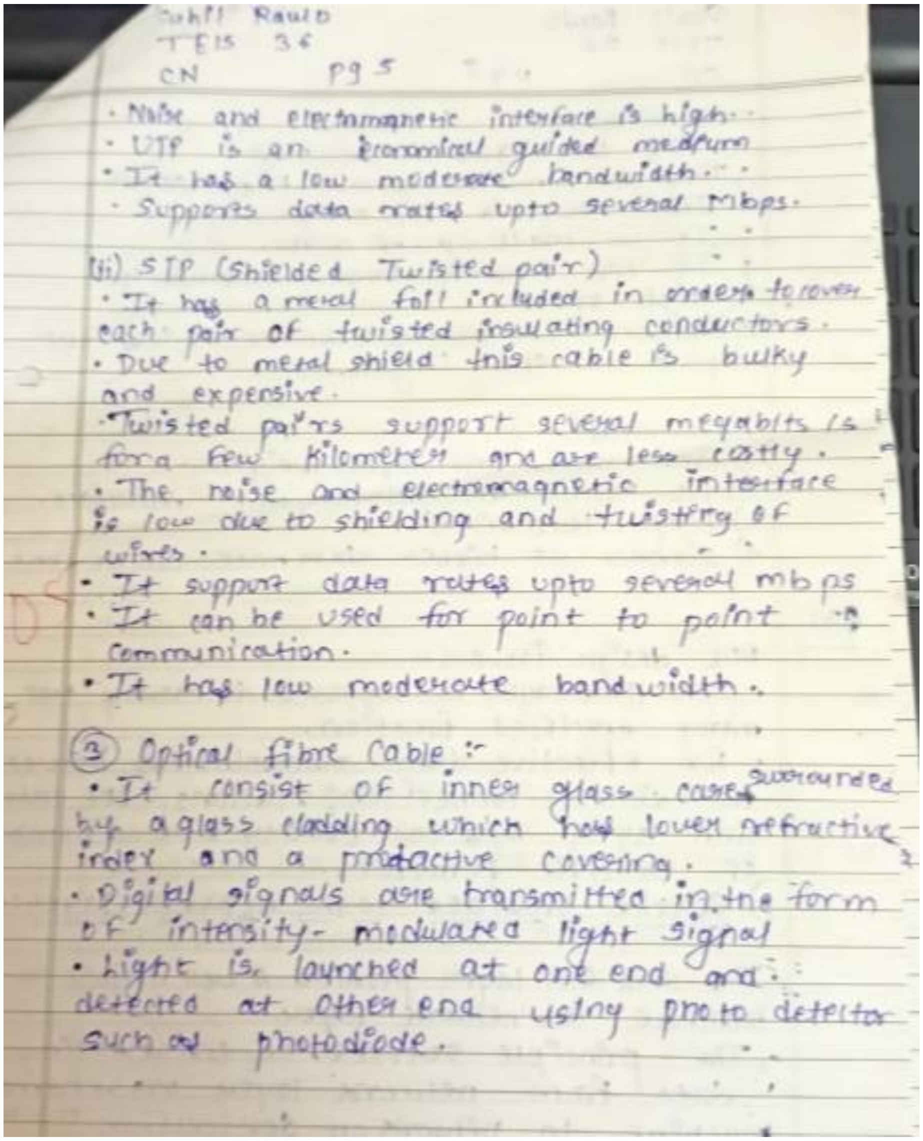
1) Analog telephone networks
2) cable TV.
3) Digital telephone networks
4) fast ethernet.
5) Digital Transmission.

② Twisted pair cable :

- This is very commonly used wired medium, and its cheaper than co-axial cable or optical fibre cable.
- There are two types.

i) UTP (unshielded Twisted pair)

- The insulate wires don't have shield, but they are twisted around each other.



Sahil Rawlo
TEIS 36
CN pg 5

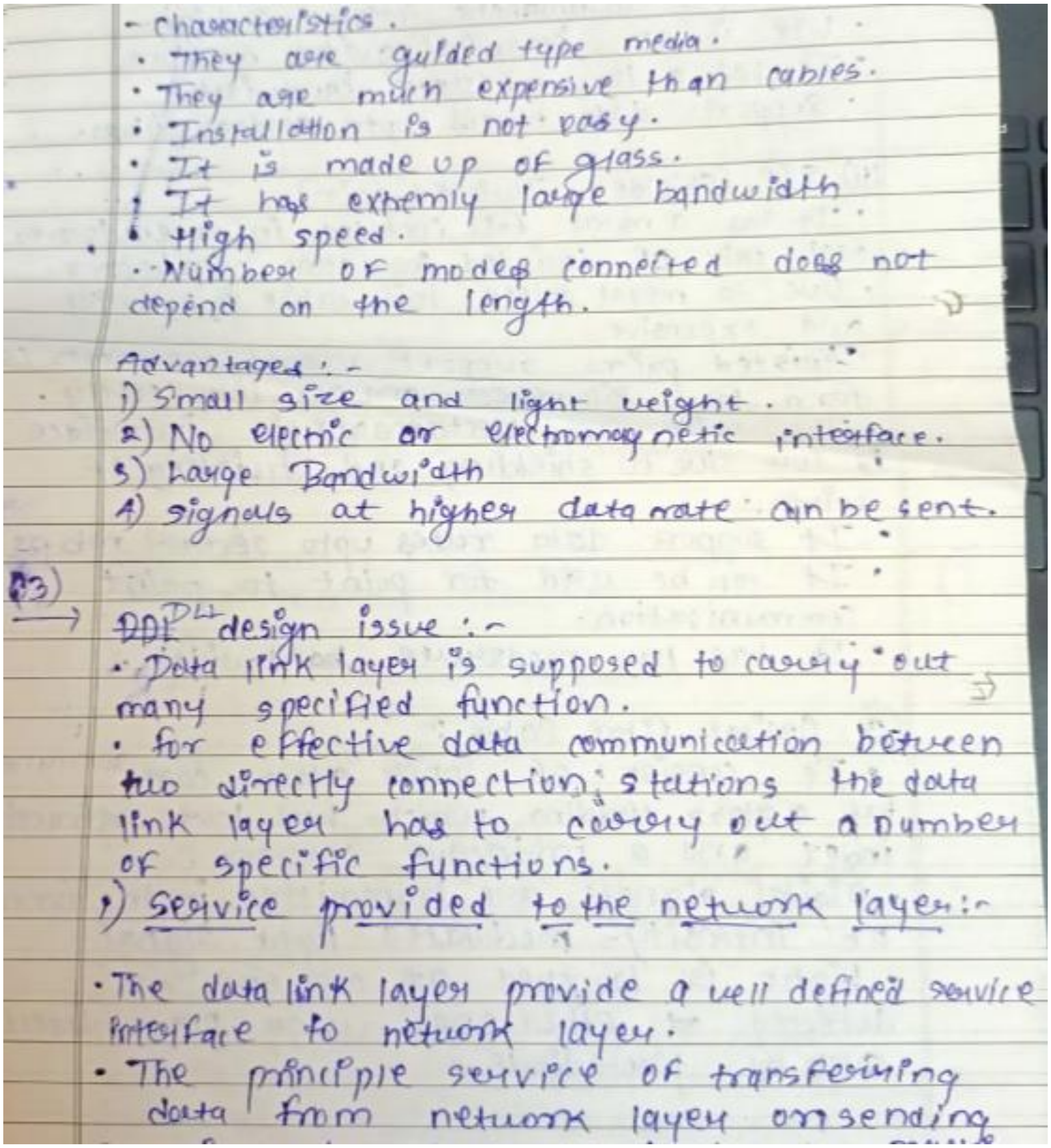
- Noise and electromagnetic interface is high.
- UTP is an economical guided medium
- It has a low moderate bandwidth.
- Supports data rates upto several mbps.

(ii) STP (Shielded Twisted pair)

- It has a metal foil included in orders to cover each pair of twisted insulating conductors.
- Due to metal shield this cable is bulky and expensive.
- Twisted pairs support several megabits/s for a few kilometers and are less costly.
- The noise and electromagnetic interface is low due to shielding and twisting of wires.
- It support data rates upto several mbps
- It can be used for point to point communication.
- It has low moderate bandwidth.

③ Optical fibre Cable :-

- It consist of inner glass cores surrounded by a glass cladding which has lower refractive index and a protective covering.
- Digital signals are transmitted in the form of intensity- modulated light signal
- Light is launched at one end and detected at other end using photo detector such as photodiode.



- Characteristics .
- They are guided type media.
- They are much expensive than cables.
- Installation is not easy.
- It is made up of glass.
- It has extremly large bandwidth
- High speed.
- Number of nodes connected does not depend on the length.

Advantages :-

1) Small size and light weight.
2) No electric or electromagnetic interface.
3) Large Bandwidth
4) signals at higher data rate can be sent.

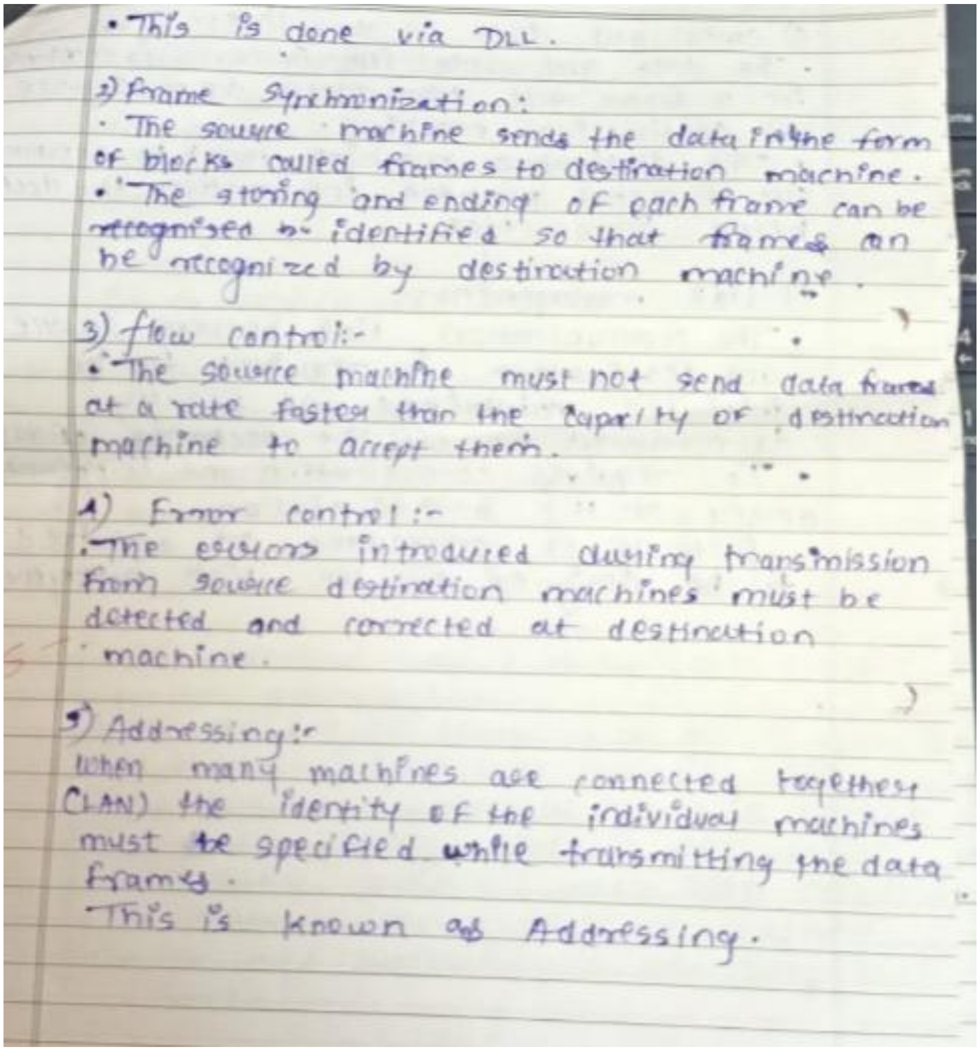
Q3)

→ ~~DDL~~ DL design issue :-

- Data link layer is supposed to carry out many specified function.
- for effective data communication between two directly connection; stations the data link layer has to carry out a number of specific functions.

1) Service provided to the network layer:-

- The data link layer provide a well defined service interface to network layer.
- The principle service of transferring data from network layer on sending



- This is done via DLL.

2) Frame Synchronization:

- The source machine sends the data in the form of blocks called frames to destination machine.
- The storing and ending of each frame can be ~~recognised~~ ~~or~~ identified so that frames can be recognized by destination machine.

3) flow control:-

- The source machine must not send data frames at a rate faster than the capacity of destination machine to accept them.

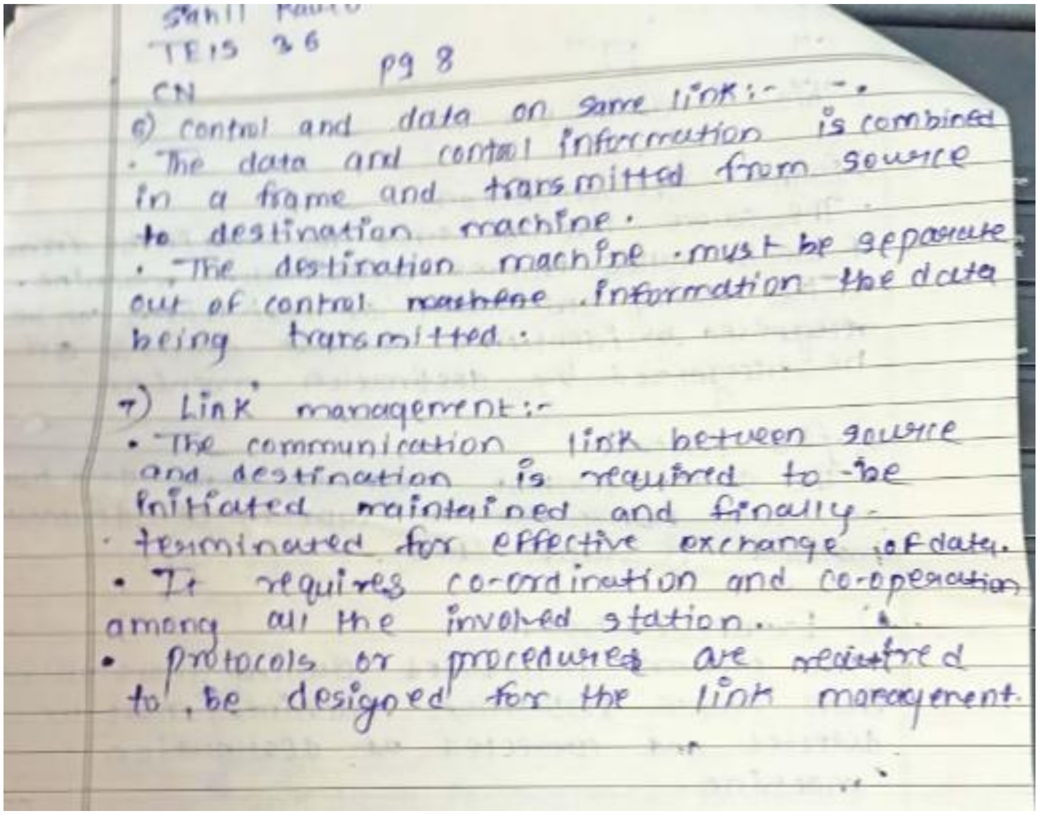
4) Error control:-

- The errors introduced during transmission from source destination machines must be detected and corrected at destination machine.

5) Addressing:-

When many machines are connected together (LAN) the identity of the individual machines must be specified while transmitting the data frames.

- This is known as Addressing.



Sahil Rau

TEIS 36

pg 8

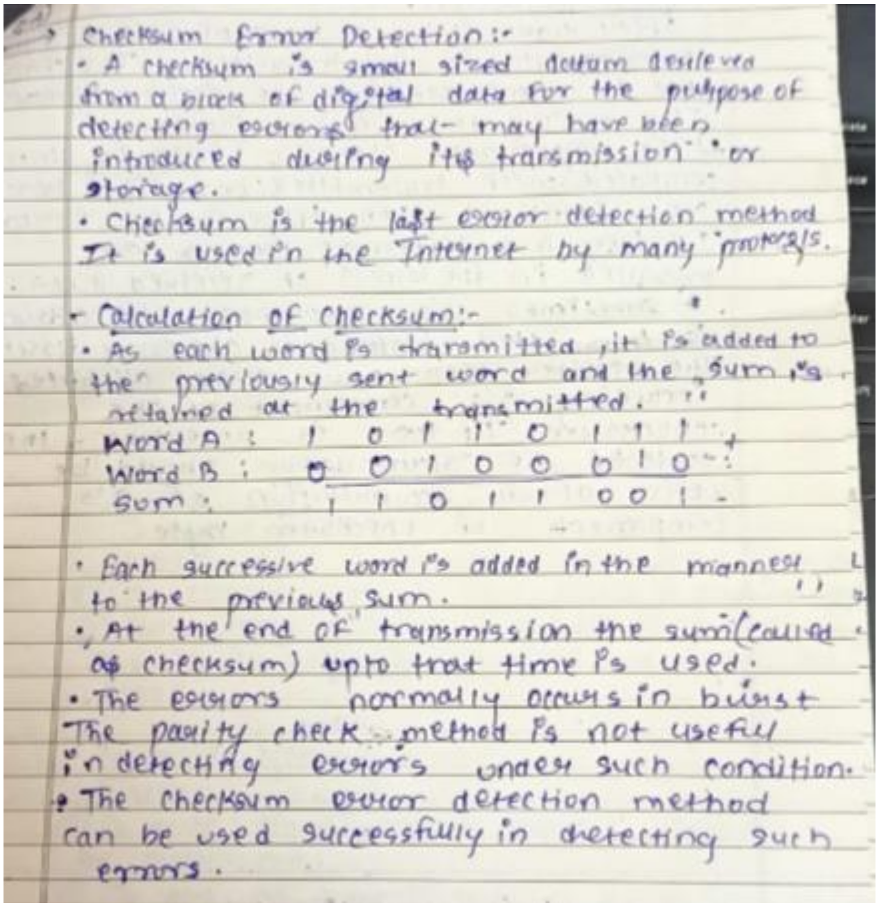
CN

6) control and data on same link:-

- The data and control information is combined in a frame and transmitted from source to destination machine.
- The destination machine must be separate out of control ~~machine~~ information the data being transmitted.

7) Link management:-

- The communication link between source and destination is required to be initiated maintained and finally terminated for effective exchange of data.
- It requires co-ordination and co-operation among all the involved station.
- protocols or procedures are required to be designed for the link management.



Checksum Error Detection:-

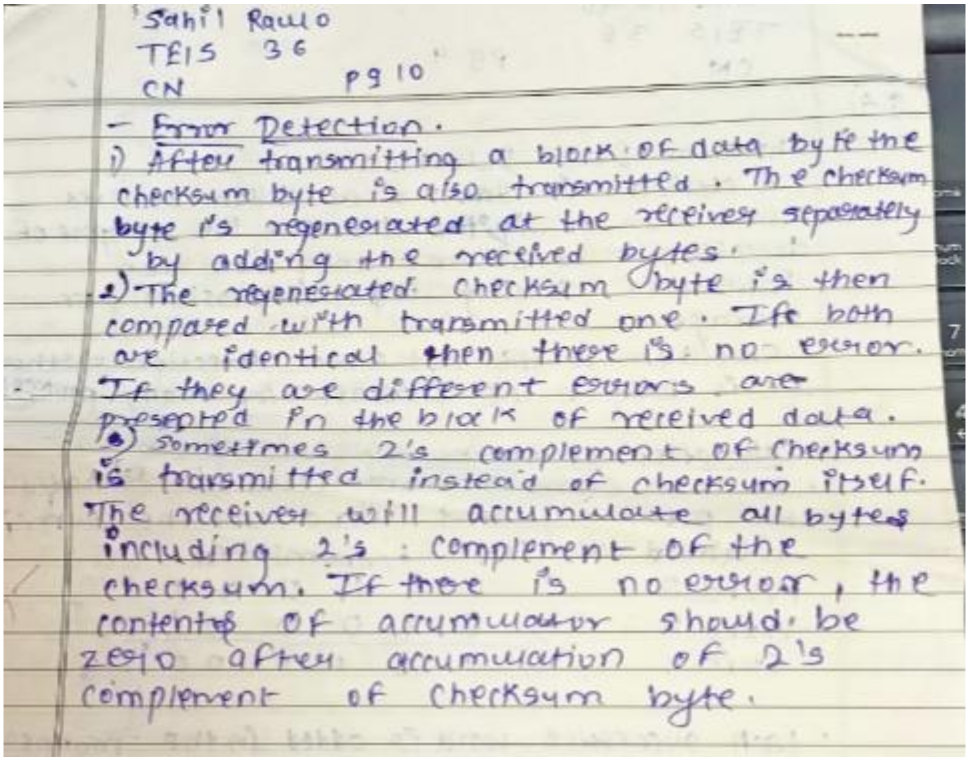
- A checksum is small sized datum desleved from a block of digital data for the purpose of detecting errors that may have been introduced during its transmission or storage.
- Checksum is the last error detection method It is used in the Internet by many protocols.

Calculation of checksum:-

- As each word is transmitted, it is added to the previously sent word and the sum is retained at the transmitted.

Word A : 1 0 1 1 0 1 1 1 +
Word B : 0 0 1 0 0 0 1 0
Sum : 1 1 0 1 1 0 0 1

- Each successive word is added in the manner to the previous sum.
- At the end of transmission the sum (called as checksum) upto that time is used.
- The errors normally occurs in burst The parity check method is not useful in detecting errors under such condition.
- The checksum error detection method can be used successfully in detecting such errors.



Sahil Raulo
TEIS 36
CN pg 10

- Error Detection.

1) After transmitting a block of data byte the checksum byte is also transmitted. The checksum byte is regeneorated at the receiver separately by adding the received bytes.

2) The regeneorated checksum byte is then compared with transmitted one. Ift both are identical then there is no error. If they are different errors are presepted in the block of received data.

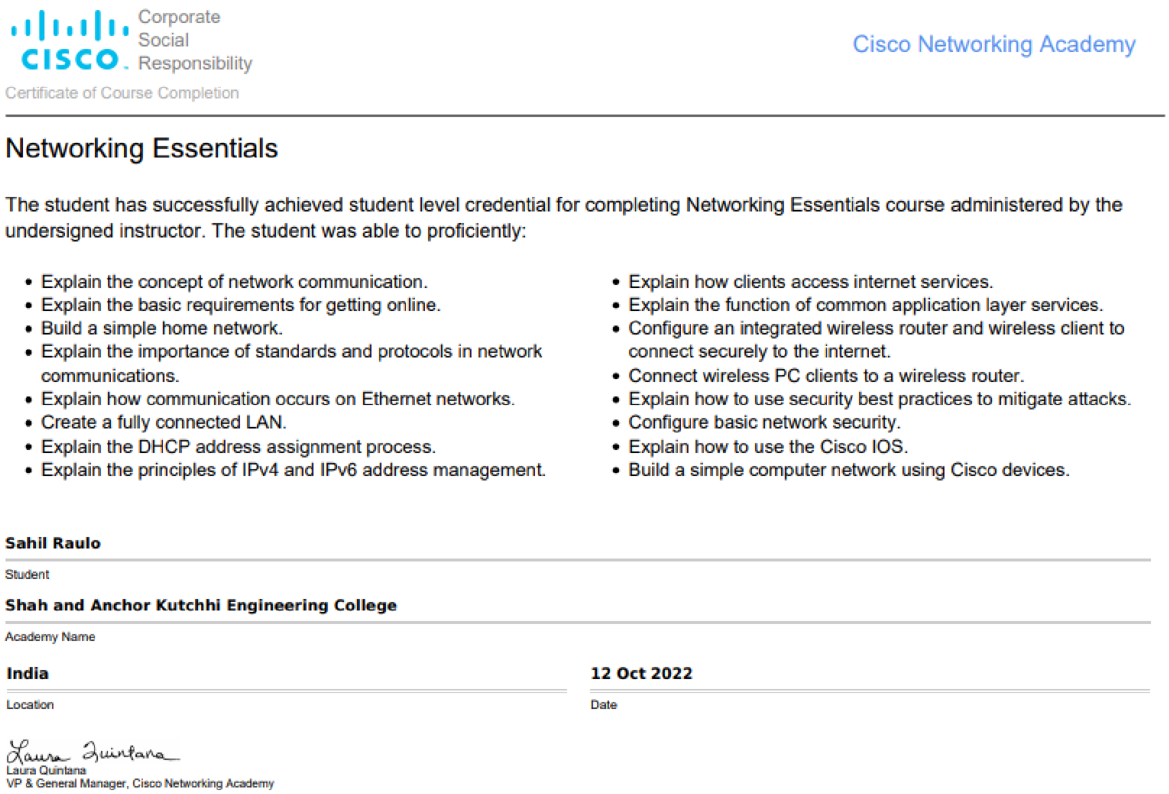
3) Sometimes 2's complement of checksum is transmitted instead of checksum itself. The receiver will accumulate all bytes including 2's complement of the checksum. If there is no error, the contentes of accumulator should be zero after accumulation of 2's complement of checksum byte.

Mahavir Education Trust's

SHAH & ANCHOR KUTCHHI ENGINEERING COLLEGE

Chembur, Mumbai - 400 088

UG Program in Cyber Security



CISCO Corporate Social Responsibility

Certificate of Course Completion

Cisco Networking Academy

Networking Essentials

The student has successfully achieved student level credential for completing Networking Essentials course administered by the undersigned instructor. The student was able to proficiently:

- Explain the concept of network communication.
- Explain the basic requirements for getting online.
- Build a simple home network.
- Explain the importance of standards and protocols in network communications.
- Explain how communication occurs on Ethernet networks.
- Create a fully connected LAN.
- Explain the DHCP address assignment process.
- Explain the principles of IPv4 and IPv6 address management.
- Explain how clients access internet services.
- Explain the function of common application layer services.
- Configure an integrated wireless router and wireless client to connect securely to the internet.
- Connect wireless PC clients to a wireless router.
- Explain how to use security best practices to mitigate attacks.
- Configure basic network security.
- Explain how to use the Cisco IOS.
- Build a simple computer network using Cisco devices.

Sahil Raulo

Student

Shah and Anchor Kutchhi Engineering College

Academy Name

India

Location

12 Oct 2022

Date

Laura Quintana

Laura Quintana
VP & General Manager, Cisco Networking Academy