7) Test the Connectivity to a website using ping (use google).

The ping command is used to check whether a host is reachable across an ip network. It sends ICMP echo requests to the destination and waits for a response.

This helps in identifying network reachability and latency.

we use the following command for this

```
"ping google.com"
```

use ctrl+c to stop the ping test.

8) How can you integrate Mininet with Open Daylight as the SDN controller

pdf

9) Command to edit the network interface assigning the ip of Gateway

1) find your network interface name.

```
" ip a "
```

look for eth0, enp0s3, ens33.

2) Open the Netplan Configuration file

```
Sudo nano/etc/netplan/01-netcfg.yaml
```

changes for every machine
file name might be 50-cloud-init.yaml.

3) Edit the file to assign static ip and gateway.

Sample yaml file opens there we have to change the address and gateway.

4) Save and exit.

```
Ctrl +o enter ctrl +x.
```

5) Apply the Configuration.

```
Sudo netplan apply.
```

6) Verify new ip & gate way.

```
ip a
```

=> new ip

```
ip route
```

=> gateway

10) Command to list all active TCP Connections along with their process ids.

identify any connections in the LISTEN or ESTABLISHED state.

1) Open terminal

ctrl + Alt + T.

2) Run command to show TCP Connections :

=> using ss.

```
" sudo ss -tunlp "
```

=> using netstat (older mtd)

```
" Sudo netstat -antp "
```

-t -> TCP connections only

-u -> UDP " too.

-n -> numeric addresses, not hostnames.

-l -> show only listening ports.

-p -> show the process ID and program name.

o/p

3)

state	Recv-Q	Send-Q	Loc Add : Port	Pee Add : Port	process.
Lis					
Esta					

LISTEN - A program is waiting for incoming connections
(like web or SSH servers)

ESTABLISHED - A live, active connection between

4) filter specific states

only listening TCP

```
Sudo ss -tuln | grep LISTEN.
```

only established connections.

```
Sudo ss -tuna | grep ESTABLISHED.
```

11) Check Linux distribution with particular version, Command to check.

Objective => identify -> linux distribution name
version
other details.

1) Open terminal

2) run the below Command.

```
" lsb_release -a "
```

↳ o/p. Distributor id (ubuntu)
Description (ubuntu 22.04.8 LTS)
Release (22.04)
Code name . . . .

3) if lsb_release is Not Installed.

```
sudo apt update
sudo apt install lsb_release.
```

Now try the command

4) (optional) full os info file.

cat / etc /os - release.

Not compulsory

5) Kernel version.

uname -r

12) Open wireshark, capture -s strat, browse any web.
stop capture. after few sec.

1) open terminal

2) install wire shark (if not installed)

```
sudo apt update
sudo apt install wireshark.
```

It is installed as a desktop application.

2) Open wire shark.

Search for wireshark in your menu -> app menu. then open.

3) Choose a Network interface to Capture.

When wireshark opens,

↳ you'll see a list of network interfaces.

look for eth0 or enp0s3 (ethernet)

or

wlan0 (wireless / wifi)

Select the one currently active.

4) Start the Capture

click on the interface name

↓

wire shark starts Capturing packets live.

5) Open a web Browser and visit a website.

Open any browser (firefox or chrome).

goto a website

wikipedia.org or anything

stay on the site for 5-10 sec.

to allow packets to exchange.

6) Stop the Capture.

return to wireshark and click.

red square button (stop capture) at the top left.

7) filter & Review captured packets.

http -> only HTTP traffic

dns -> shows dns queries.

tcp -> shows TCP traffic.

You can click on any packet to expand the details (TCP heads, HTTP requests)