

NETWORKING TRAINING - MODULE 1 & 2

Akash S, embedUR Systems

Task 1:

Consider a case, a folder has multiple files and how would copy it to destination machine path (Try using SCP, cp options in Linux)

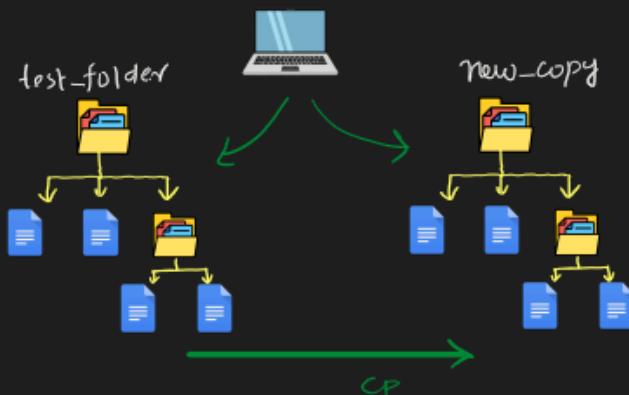
Explanation:

① Copy Files:

- cp - copy - locally
- SCP - Secure copy - remote machine

② CP Command:

- internally copies files & directories using cp



• Options:

→ -r → recursive copy

③ SCP Command:

- scp command copies to a remote machine
- Uses SSH to connect to a machine

(I) SSH Connection:

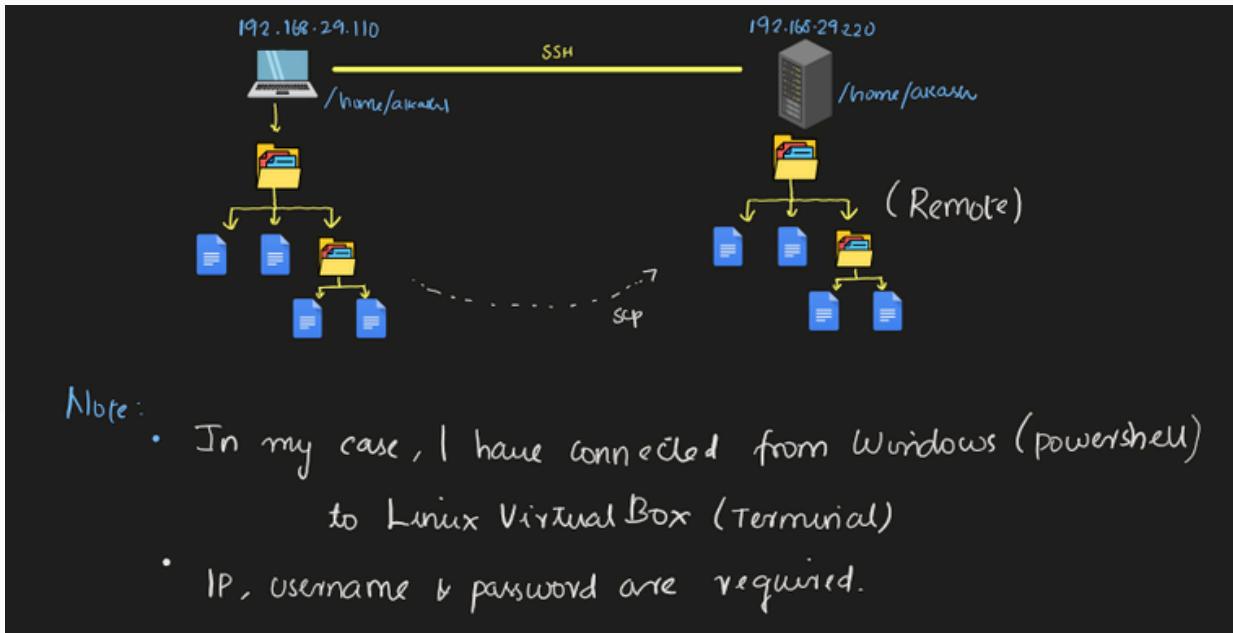
\$ ifconfig | grep inet → "192.168.29.220"

\$ ssh akash@192.168.29.220 → it encrypts data
 username



(II) Using scp:

```
$ scp -r newfolder akash@192.168.29.220 :/home/akash
```



Outputs:

```
akash@akash:~$ ls -R test_folder
test_folder:
file1.txt  file2.txt  subdir

test_folder/subdir:
file3.txt  new.log
akash@akash:~$ cp -r test_folder new_copy
akash@akash:~$ ls -R new_copy
new_copy:
file1.txt  file2.txt  subdir

new_copy/subdir:
file3.txt  new.log
akash@akash:~$
```

cp command

```
akash@akash:~$ mkdir newfolder
akash@akash:~$ cd newfolder
akash@akash:~/newfolder$ echo "new" > hello.txt
akash@akash:~/newfolder$ echo "new" > akash.txt
akash@akash:~/newfolder$ echo "new" > embedur.txt
akash@akash:~/newfolder$ ls
akash.txt  embedur.txt  hello.txt
akash@akash:~/newfolder$ cd ..
akash@akash:~$ scp -r newfolder akash@192.168.29.220:/home/akash
The authenticity of host '192.168.29.220 (192.168.29.220)' can't be established.
ED25519 key fingerprint is SHA256:TNxxyqoUqW2736kDierbkvwc4s/u9Z611B+igD
H/bwU8.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:1: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.29.220' (ED25519) to the list of known hosts.
akash@192.168.29.220's password:
akash.txt          100%    4     8.7KB/s  00:00
embedur.txt        100%    4     9.1KB/s  00:00
hello.txt          100%    4    10.6KB/s  00:00
akash@akash:~$
```

```
akash@akash:~$ pwd
/home/akash
akash@akash:~$ ls newfolder
akash.txt  embedur.txt  hello.txt
akash@akash:~$
```

scp command

Task 2:

Host a FTP and SFTP server and try PUT and GET operations.

Explanation:

① Protocols:

- FTP: File Transfer Protocol
- SFTP: Secure File Transfer Protocol 

② FTP:

(I) Add user:
\$ sudo adduser ftp-akash

(II) Connect SSH:

\$ ssh akash@192.168.29.220

(III) Protocol implementation:

localhost : \$ ftp localhost

Remote machine : \$ ftp 192.168.29.220

(IV) Operations:

- PUT: To send the file
- GET: To receive the file / download



③ SFTP:

(I) Add user:
\$ sudo adduser sftp-akash

(II) Connect SSH:

\$ ssh sftp-akash@192.168.29.220

(III) Protocol Implementation:

- localhost : \$ sftp sftp@localhost
- Remote machine : \$ sftp sftp@192.168.29.220

(IV) Operations:

- PUT: To send securely
- GET: To receive / download securely



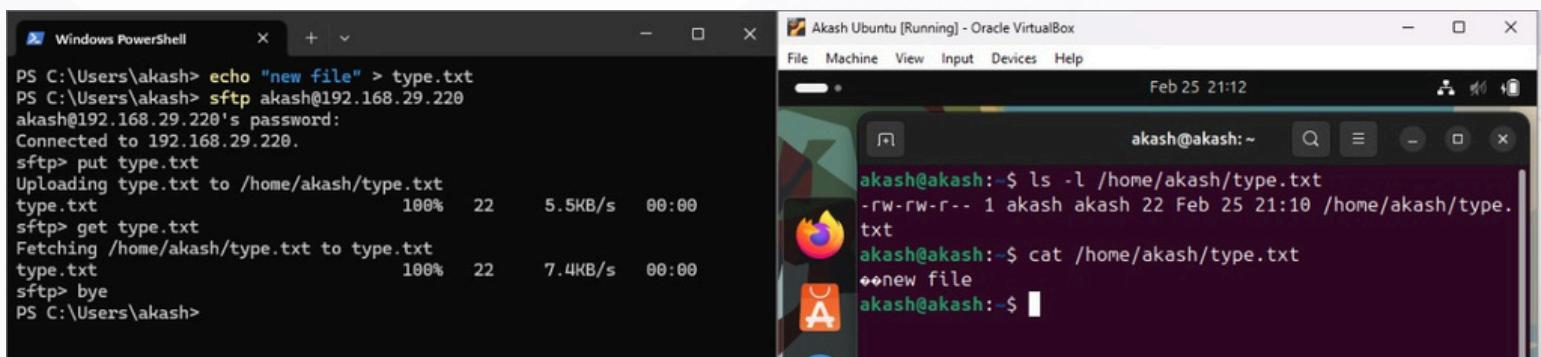
ftp:

```
akash@akash:~$ echo "Akash is an intern at embedUR" > new.txt
akash@akash:~$ ftp localhost
Connected to localhost.
220 (vsFTPd 3.0.5)
Name (localhost:akash): ftp_akash
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> put new.txt
local: new.txt remote: new.txt
229 Entering Extended Passive Mode (|||49119|)
150 Ok to send data.
100% |*****| 30 80.26 KiB/s 00:00 ETA
226 Transfer complete.
30 bytes sent in 00:00 (39.75 KiB/s)
ftp> ls
229 Entering Extended Passive Mode (|||34395|)
150 Here comes the directory listing.
-rw----- 1 1001 1001 30 Feb 25 19:14 new.txt
226 Directory send OK.
ftp> get new.txt
local: new.txt remote: new.txt
229 Entering Extended Passive Mode (|||47186|)
150 Opening BINARY mode data connection for new.txt (30 bytes).
```

sftp:

```
akash@akash:~$ touch sample.txt
akash@akash:~$ sftp sftp_akash@localhost
sftp_akash@localhost's password:
Connected to localhost.
sftp> ls
myfolder
sftp> cd myfolder
sftp> put sample.txt
Uploading sample.txt to /myfolder/sample.txt
sample.txt 100% 0 0.0KB/s 00:00
sftp> ls -l
-rw-rw-r-- ? 1002 1002 0 Feb 25 19:38 sample.txt
sftp> get sample.txt
Fetching /myfolder/sample.txt to sample.txt
sftp> exit
akash@akash:~$ ls -l sample.txt
-rw-rw-r-- 1 akash akash 0 Feb 25 19:39 sample.txt
akash@akash:~$
```

sftp with localhost



sftp with remote machine

Task 3:

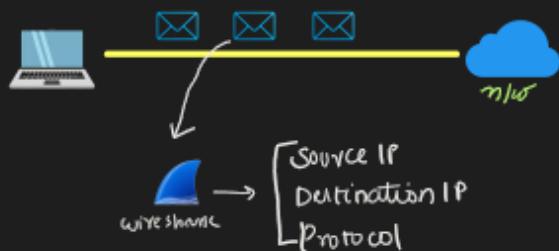
Explore with Wireshark/TCP-dump/cisco packet tracer tools and learn about packets filters.

Explanation:

① Wireshark:

→ Why?

- To capture packets.
- To Filter and analyse traffic.



→ Initialization:

- Start Wireshark
- Select an interface
 - enp0s3
 - wi-fi
 - eth0
- Start capture

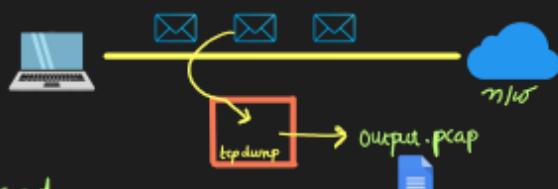
→ Examples:

- Filter options: ip.addr == 192.168.1.1
- ping 8.8.8.8 → icmp (filter).

② Tcpdump:

→ Uses:

- Captures network packets from a specific interface
- We can save them to a 'pcap' file.



Command:

→ \$ sudo tcpdump -i enp0s3

↳ Listen to all packets in enp0s3 interface & captures

\$ sudo tcpdump -i enp0s3 -w output.pkt.pcap

↳ Stores captured packets in a .pcap file.

③ Cisco Packet Tracer:

→ Why?

- It simulates a network to design, configure & analyse packet flow.



→ Configuration: PC:

IP address: 192.168.2.3

default gateway: 192.168.29.1

→ To analyse traffic:

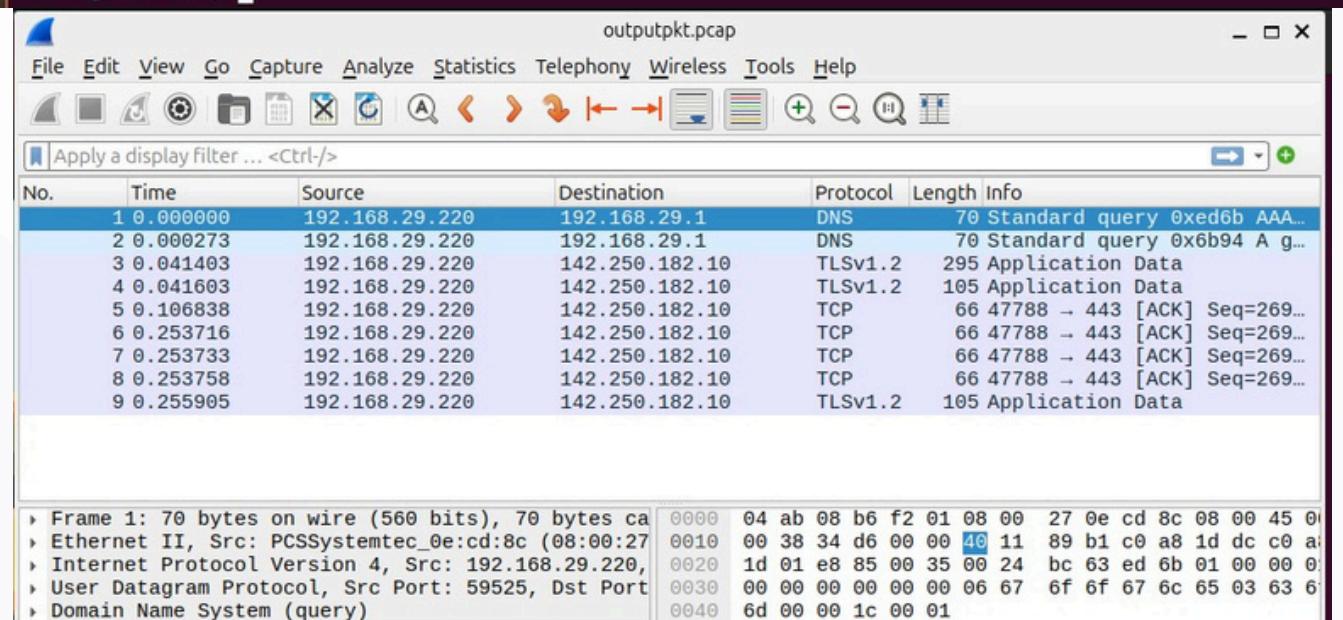
Ping 192.168.2.3 → on PC

→ Filter:

ICMP filter

Outputs:

```
akash@akash:~$ ip a | grep "inet"
    inet 127.0.0.1/8 scope host lo
        inet 192.168.29.220/24 brd 192.168.29.255 scope global dynamic noprefixroute enp0s3
akash@akash:~$ sudo tcpdump -i enp0s3 src host 192.168.29.220 -w outputpkt.pcap
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
^C9 packets captured
9 packets received by filter
0 packets dropped by kernel
akash@akash:~$ wireshark outputpkt.pcap &
[1] 11135
akash@akash:~$
```



Wireshark packet capture

```

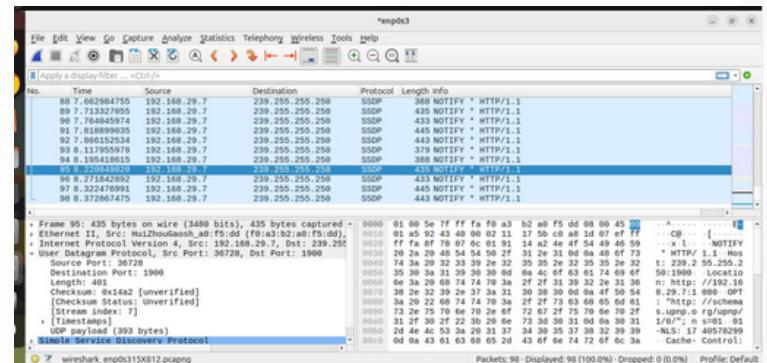
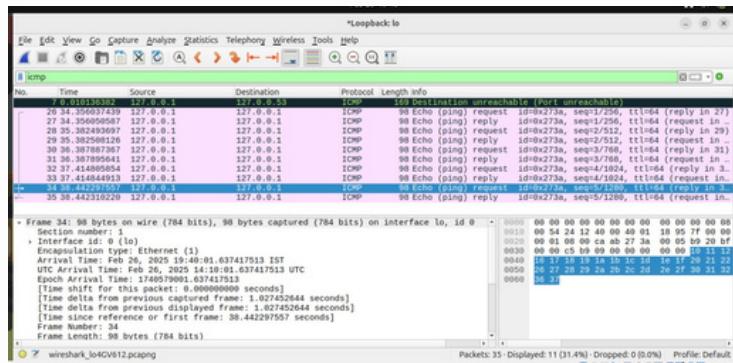
akash@akash:~$ sudo tcpdump -i enp0s3
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
19:46:46.894167 IP6 dell11s13-in-x0e.1e100.net.https > akash.49380: UDP, length 26
19:46:46.927473 IP 192.168.29.7.6537 > 255.255.255.6537: UDP, length 205
19:46:46.979286 IP akash.34353 > reliance.reliance.domain: 56724+ PTR? 1.5.8.9.9.1.1.f.3.9.c.f.4.b.b.d.a.1.8.a.f.4.0.e.1.0.2.0.5.0.4.2.ip6.arpa. (90)
19:46:46.981370 IP reliance.reliance.domain > akash.34353: 56724 NXDomain 0/0/0 (90)
19:46:46.983032 IP akash.45808 > reliance.reliance.domain: 59488+ PTR? 7.29.168.192.in-addr.arpa. (43)
19:46:46.984799 IP reliance.reliance.domain > akash.45808: 59488 NXDomain 0/0/0 (43)
19:46:47.094698 IP akash.50821 > reliance.reliance.domain: 6789+ PTR? 1.29.168.192.in-addr.arpa. (43)
19:46:47.095959 IP6 akash.49380 > dell11s13-in-x0e.1e100.net.https: UDP, length 29
19:46:47.103963 IP reliance.reliance.domain > akash.50821: 6789* 1/0/0 PTR reliance.reliance. (74)
19:46:47.104813 IP akash.45766 > reliance.reliance.domain: 6722+ PTR? 220.29.168.192.in-addr.arpa. (45)
19:46:47.110287 IP reliance.reliance.domain > akash.45766: 6722 NXDomain 0/0/0 (45)
19:46:47.167251 IP6 dell11s13-in-x0e.1e100.net.https > akash.49380: UDP, length 26
^C
12 packets captured
12 packets received by filter
0 packets dropped by kernel
akash@akash:~$ 

```

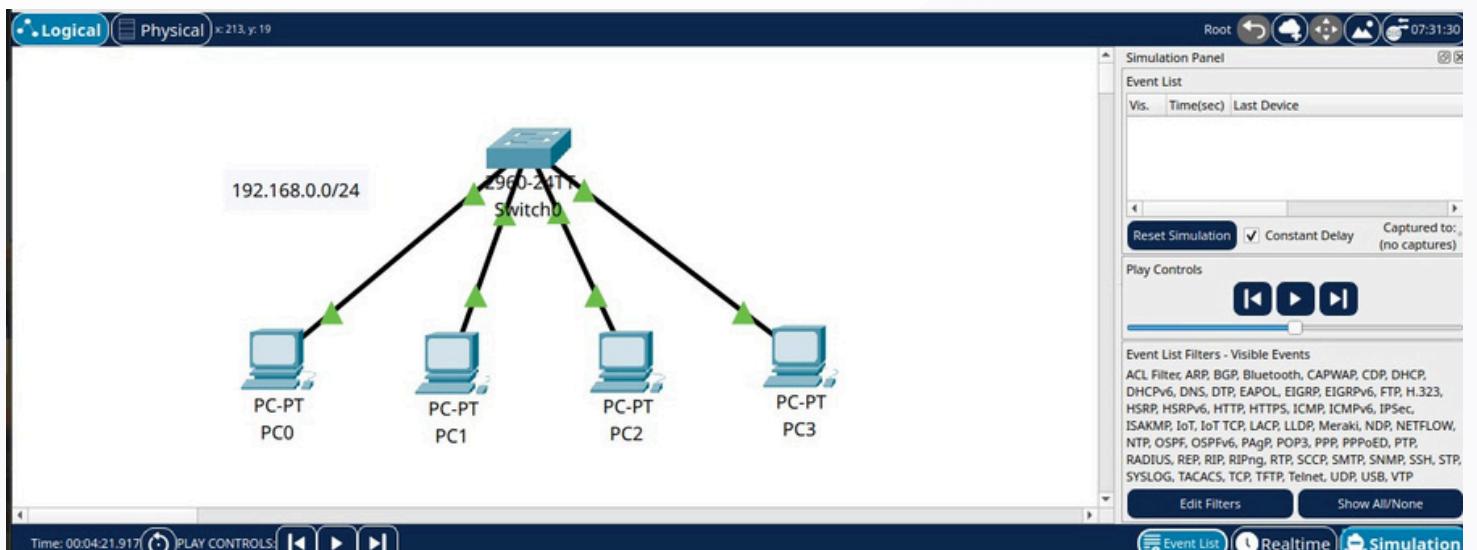
```

akash@akash:~$ sudo tcpdump -i enp0s3 -w outputpkt.pcap
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
^C406 packets captured
407 packets received by filter
0 packets dropped by kernel
akash@akash:~$ 

```



tcpdump



cisco packet tracer

Task 4:

Understand linux utility commands like - ping, arp (Understand each params from ifconfig output).

Explanation:

① ping :

- To test network connectivity
- It sends ICMP packets to check if a device is reachable



→ Commands:

- \$ ping 8.8.8.8
- \$ ping -c 5 192.168.29.1
- \$ ping google.com

② arp:

- Manage IP to MAC address Mapping
- Shows/modifies arp table

→ Commands:

```
$ arp -n
```

IP Address	HW Type	HW Address (MAC)
192.168.29.1	ether	04:ab:08:b6:f2:01
192.168.29.112	ether	C8:94:02:34:f1:69

To add a Static ARP

```
$ sudo arp -s 192.168.29.100 00:11:22:33:44:55
```

IP MAC
mapping → arp

③ To understand from ifconfig output:

```
akash@akash:~$ ifconfig
enp0s3: flags=4163<IP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.29.220 brd 192.168.29.255 broadcast 192.168.29.255
          netmask 255.255.255.0
          ether 00:0c:ab:08:b6:f2
          brd 192.168.29.255
          scopeid 0x0<global>
          link-layer
          txqueuelen 1000
          RX packets 12307 bytes 85880203 (8.5 MB)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 7276 bytes 2749794 (2.7 MB)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 brd 127.0.0.1
          netmask 255.0.0.0
          ether 00:00:00:00:00:00
          brd 00:00:00:00:00:00
          scopeid 0x10<host>
          link-layer
          txqueuelen 1000
          RX packets 674 bytes 64388 (64.3 KB)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 674 bytes 64388 (64.3 KB)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
akash@akash:~$
```

Outputs:

```
akash@akash:~$ ip route | grep default
default via 192.168.29.1 dev enp0s3 proto dhcp src 192.168.29.220 metric 100
akash@akash:~$ ping -c 5 -D 192.168.29.1
PING 192.168.29.1 (192.168.29.1) 56(84) bytes of data.
[1740674927.673095] 64 bytes from 192.168.29.1: icmp_seq=1 ttl=64 time=2.02 ms
[1740674928.675138] 64 bytes from 192.168.29.1: icmp_seq=2 ttl=64 time=2.25 ms
[1740674929.677886] 64 bytes from 192.168.29.1: icmp_seq=3 ttl=64 time=2.54 ms
[1740674930.681414] 64 bytes from 192.168.29.1: icmp_seq=4 ttl=64 time=4.18 ms
[1740674931.688920] 64 bytes from 192.168.29.1: icmp_seq=5 ttl=64 time=2.07 ms

--- 192.168.29.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4016ms
rtt min/avg/max/mdev = 2.016/2.611/4.184/0.807 ms
akash@akash:~$
```

ping command

```
akash@akash:~$ ip route | grep default
default via 192.168.29.1 dev enp0s3 proto dhcp src 192.168.29.220 metric 100
akash@akash:~$ arp -n | grep "192.168.29.1"
192.168.29.1          ether 04:ab:08:b6:f2:01      C           enp0s3
192.168.29.112         ether c8:94:02:34:f1:69      C           enp0s3
akash@akash:~$ arp -a
reliance.reliance (192.168.29.1) at 04:ab:08:b6:f2:01 [ether] on enp0s3
? (192.168.29.112) at c8:94:02:34:f1:69 [ether] on enp0s3
akash@akash:~$ arp -n
Address          HWtype  HWaddress          Flags Mask          Iface
192.168.29.1    ether    04:ab:08:b6:f2:01  C           enp0s3
192.168.29.112  ether    c8:94:02:34:f1:69  C           enp0s3
akash@akash:~$ sudo arp -s 192.168.29.100 00:11:22:33:44:55
[sudo] password for akash:
akash@akash:~$ arp -n
Address          HWtype  HWaddress          Flags Mask          Iface
192.168.29.1    ether    04:ab:08:b6:f2:01  C           enp0s3
192.168.29.112  ether    c8:94:02:34:f1:69  C           enp0s3
192.168.29.100  ether    00:11:22:33:44:55  CM          enp0s3
akash@akash:~$
```

arp command

Task 5:

Understand what happens when duplicate IPs configured in a network.

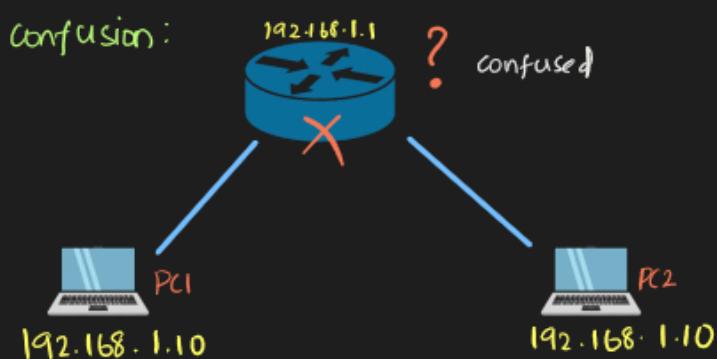
Explanation:

In what happens with duplicate IP:

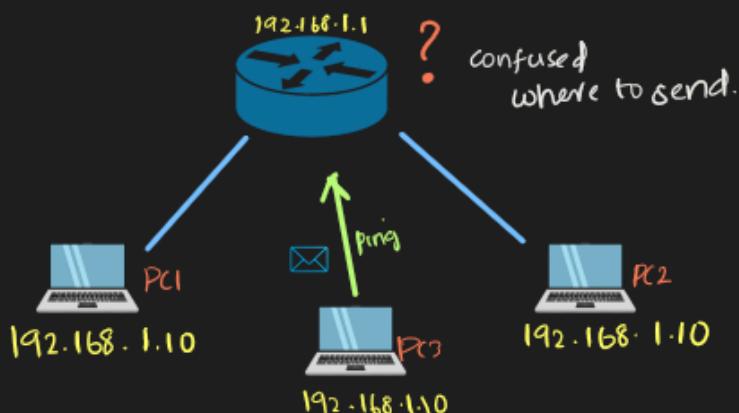
- Two devices with same IP
- Router gets confused → where to send?
- ARP table lists multiple MACs for one IP (conflict)
- Ping fails / go to wrong device
- Now becomes unstable, delay, drop packets.

VISUALS:

① Router confusion:



② Pinging confusion.



③ ARP confusion:

IP Address	Device	HW Address (MAC)
192.168.1.10	PC1	04:ab:08:b6:f2:01
192.168.1.10	PC2	C8:94:02:34:f1:69

Annotations: A curved arrow points from the first row to the IP column with the text "same IP". Another curved arrow points from the second and third rows to the IP column with the text "duplicate". A bracket on the right side groups the last two rows with the text "but different MAC".

Output:

```
akash@akash:~$ sudo modprobe dummy
[sudo] password for akash:
akash@akash:~$ sudo ip link add dummy0 type dummy
akash@akash:~$ sudo ip addr add 192.168.1.100/24 dev enp0s3
akash@akash:~$ sudo ip addr add 192.168.1.100/24 dev dummy0
akash@akash:~$ ip addr show | grep 192.168.1.100
    inet 192.168.1.100/24 scope global enp0s3
        inet 192.168.1.100/24 scope global dummy0
akash@akash:~$ sudo ip neigh add 192.168.1.100 lladdr 11:22:33:44:55:66 dev dummy0
akash@akash:~$ ip neigh show
192.168.29.1 dev enp0s3 lladdr 04:ab:08:b6:f2:01 REACHABLE
192.168.1.100 dev dummy0 lladdr 11:22:33:44:55:66 PERMANENT
fe80::6ab:8ff:feb6:f201 dev enp0s3 lladdr 04:ab:08:b6:f2:01 router REACHABLE
akash@akash:~$ sudo arping -c 4 -I dummy0 192.168.1.100
arping: libnet_init(LIBNET_LINK, dummy0): libnet_check_iface(): dummy0 is down
akash@akash:~$ sudo ip link set dummy0 up
akash@akash:~$ sudo arping -c 4 -I dummy0 192.168.1.100
ARPING 192.168.1.100
Timeout
Timeout
Timeout
Timeout
Timeout
--- 192.168.1.100 statistics ---
```

issues with duplicate IPs

Task 6:

Understand how to access remote system using (VNC viewer, Anydesk, teamviewer and remote desktop connections)

Explanation:

① VNC Viewer:

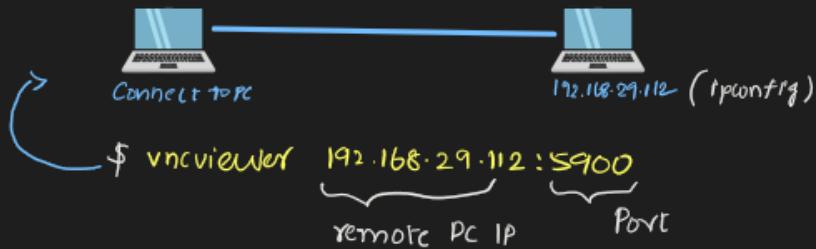
- Why? • To remotely connect another computer's desktop.
• Through VNC server on remote PC.

Connection:

(I) Installation:



(II) Connection:



```
akash@akash:~$ vncviewer 192.168.29.112:5900

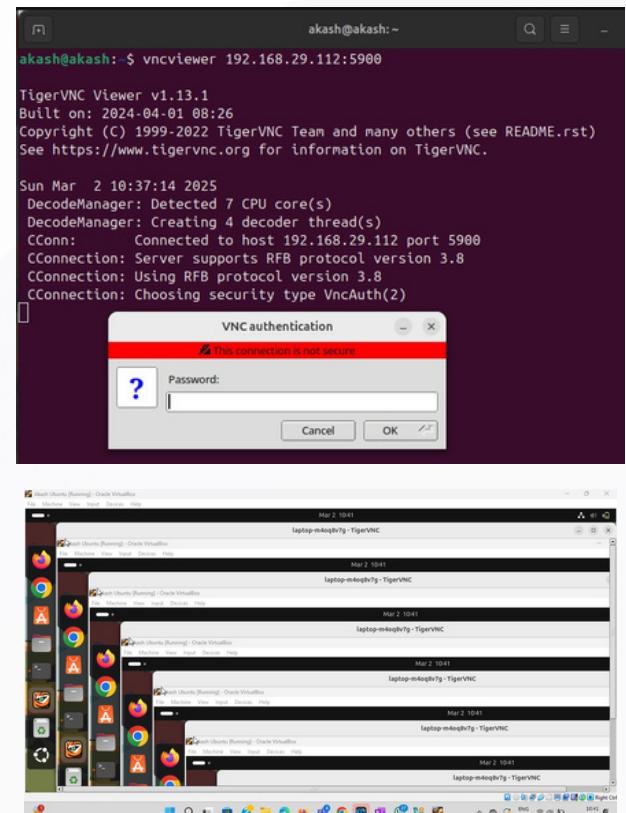
TigerVNC Viewer v1.13.1
Built on: 2024-04-01 08:26
Copyright (C) 1999-2022 TigerVNC Team and many others (see README.rst)
See https://www.tigervnc.org for information on TigerVNC.

Fri Feb 28 19:47:45 2025
DecodeManager: Detected 7 CPU core(s)
DecodeManager: Creating 4 decoder thread(s)
CConn: Connected to host 192.168.29.112 port 5900
CConnection: Server supports RFB protocol version 3.8
CConnection: Using RFB protocol version 3.8
CConnection: Choosing security type VncAuth(2)

Fri Feb 28 19:47:51 2025
DesktopWindow: Reducing window size to fit on current monitor
CConn: Using pixel format depth 24 (32bpp) little-endian rgb888

Fri Feb 28 19:48:55 2025
DecodeManager: copyRect: 88 rects, 12.3321 Mpixels
DecodeManager: 1.375 KiB (1:35035.2 ratio)
DecodeManager: Tight: 29.391 krects, 50.5854 Mpixels
DecodeManager: 13.1255 MiB (1:14.7273 ratio)
DecodeManager: Total: 29.479 krects, 62.9175 Mpixels
DecodeManager: 13.1269 MiB (1:18.3097 ratio)
akash@akash:~$
```

vncviewer



Anydesk:

② Anydesk:

why? To remotely control and manage PC over Internet or LAN.

Specificity? It uses a Unique ID.

Implementation:

(I) Installation :



Install anydesk



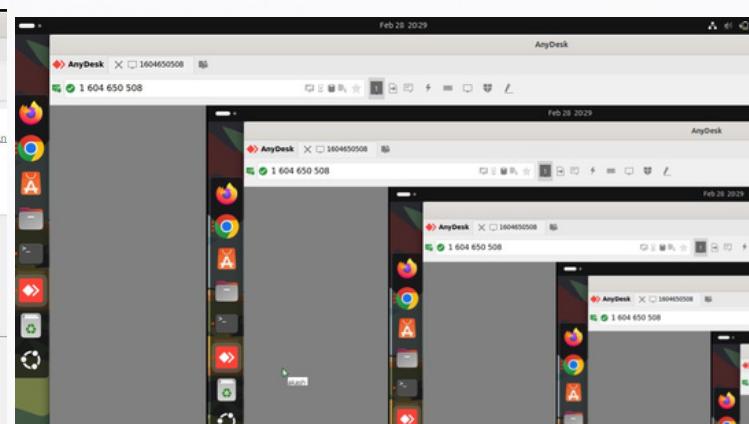
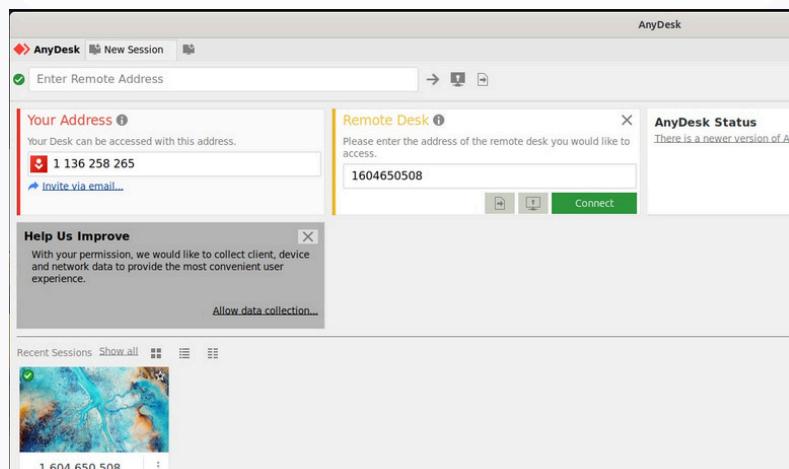
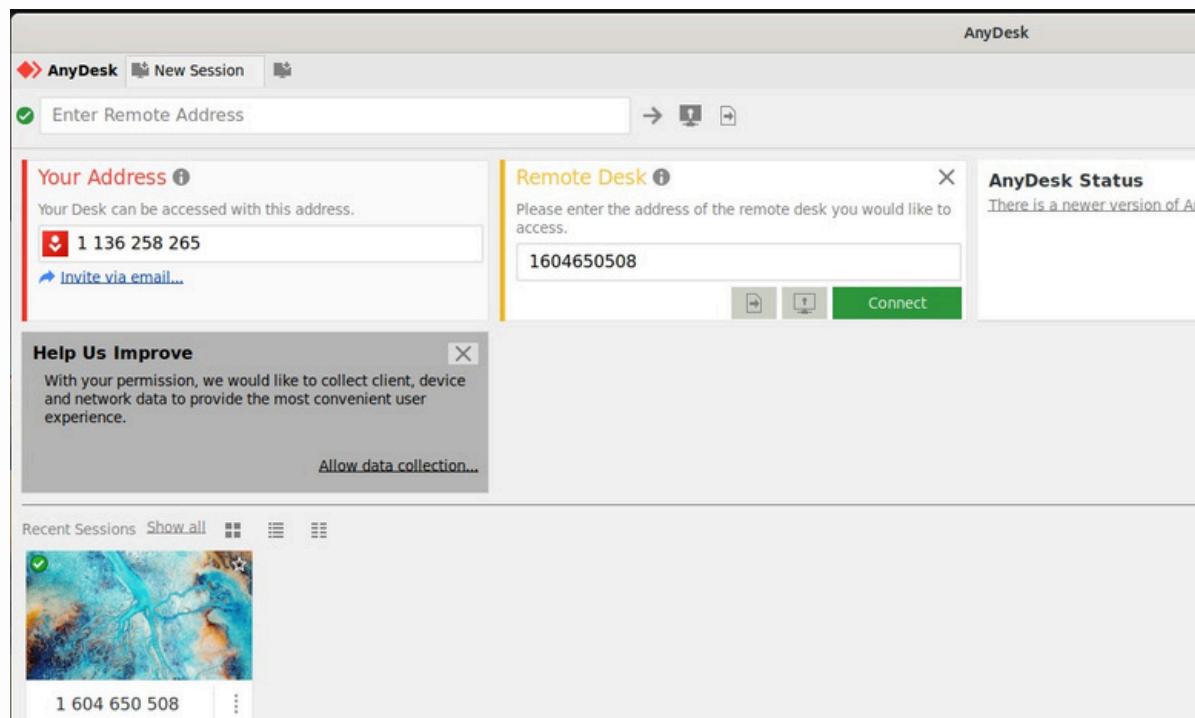
Download anydesk

(II) Connection:



Remote ID:

- Unique ID is the remote ID of a remote machine to facilitate connection.



Teamviewer:

③ TeamViewer:

- To remotely connect, access and manage PC over Internet or LAN.
- It uses and ID + password.

Implementation:

(I) Installation:



Install teamviewer



Download teamviewer

(II) Connection:



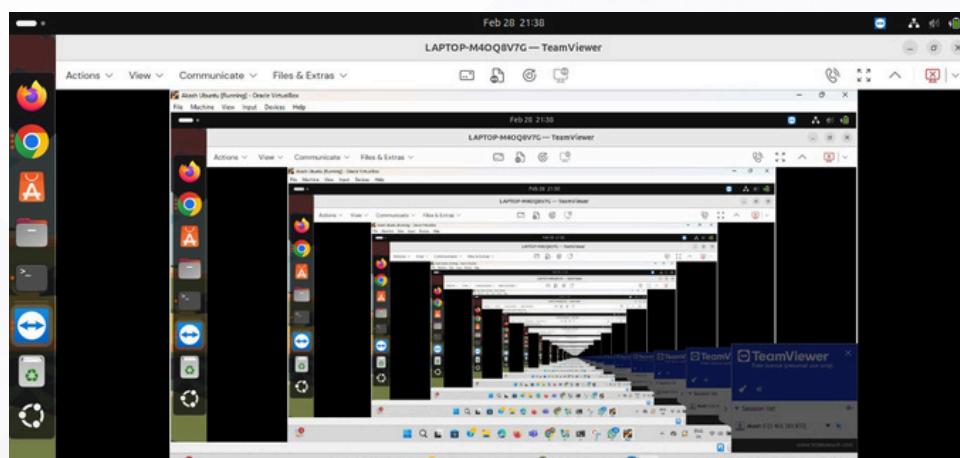
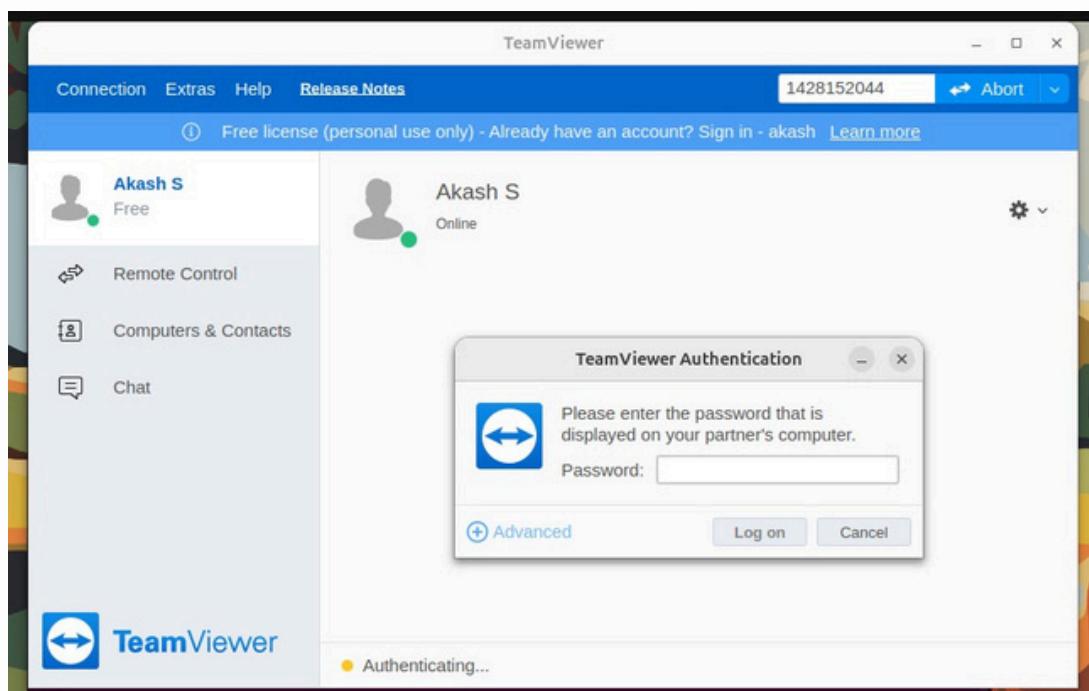
ID [] ?
Pwd []



1612143198 (ID)
***** (Pwd)

Specularity?

- Secure (because it utilises both ID & password)
- Easier team collaboration with a shared password.



Remote Desktop Connection:

④ Remote Desktop Connection:

- To access a remote Windows PC's desktop over Network
- With the help of RDP / RDC (Windows)



(I) Enable RDC:

settings > System > Remote Desktop RDC

(II) Identify IP:

powershell ipconfig → 192.168.29.10D

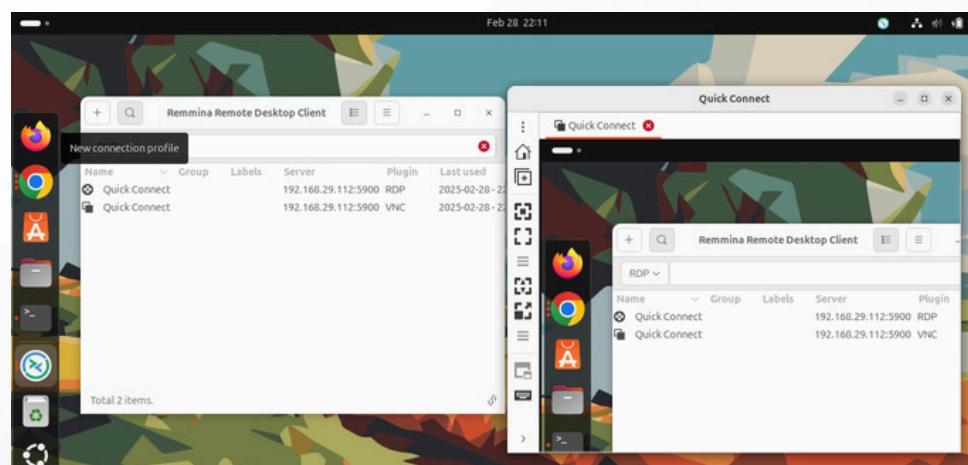
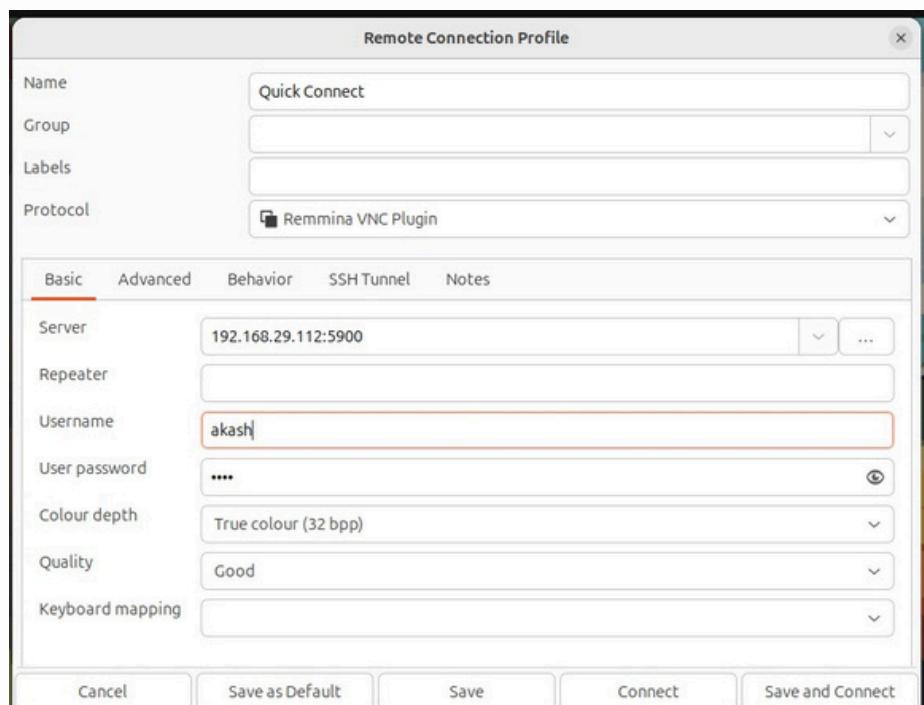
(III) Launch RDC client:

Open RDC on client machine

(IV) Authentication:

Enter IP, Username, password to connect

→ now full control over
remote PC



Task 7:

How to check your default gateway is reachable or not and understand about default gateway.

Explanation:

Default Gateway:

- a router/device that connects local n/w to external n/w
- It's the exit point for the packets that are destined for outside the network
- To connect to the internet

Speciality?

- Without default gateway, no internet access

Reachability:

Find its IP: `$ ip route | grep default`

`default: 192.168.29.1`

Ping :

`$ ping -c 5 192.168.29.1`

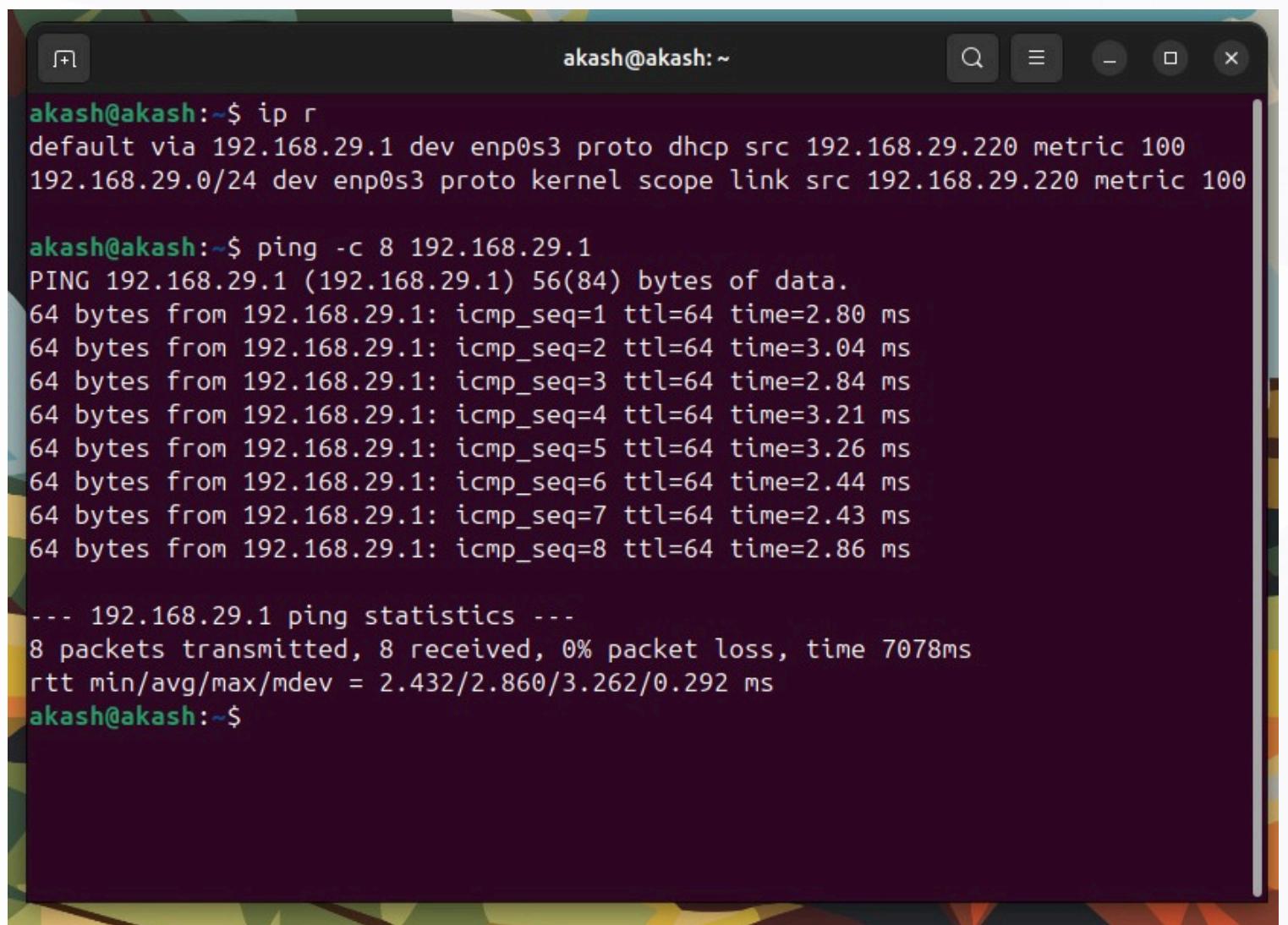
↳ Tests the reachability

Traceroute: `$ traceroute 192.168.29.1 / tracert 192.168.29.1`

Default Gateway concept:



Output:



A screenshot of a terminal window titled "akash@akash:~". The terminal displays the following command-line session:

```
akash@akash:~$ ip r
default via 192.168.29.1 dev enp0s3 proto dhcp src 192.168.29.220 metric 100
192.168.29.0/24 dev enp0s3 proto kernel scope link src 192.168.29.220 metric 100

akash@akash:~$ ping -c 8 192.168.29.1
PING 192.168.29.1 (192.168.29.1) 56(84) bytes of data.
64 bytes from 192.168.29.1: icmp_seq=1 ttl=64 time=2.80 ms
64 bytes from 192.168.29.1: icmp_seq=2 ttl=64 time=3.04 ms
64 bytes from 192.168.29.1: icmp_seq=3 ttl=64 time=2.84 ms
64 bytes from 192.168.29.1: icmp_seq=4 ttl=64 time=3.21 ms
64 bytes from 192.168.29.1: icmp_seq=5 ttl=64 time=3.26 ms
64 bytes from 192.168.29.1: icmp_seq=6 ttl=64 time=2.44 ms
64 bytes from 192.168.29.1: icmp_seq=7 ttl=64 time=2.43 ms
64 bytes from 192.168.29.1: icmp_seq=8 ttl=64 time=2.86 ms

--- 192.168.29.1 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7078ms
rtt min/avg/max/mdev = 2.432/2.860/3.262/0.292 ms
akash@akash:~$
```

default gateway connectivity

Task 8:

Check iwconfig/ifconfig to understand in detail about network interfaces (check about interface speed, MTU and other parameters)

Explanation:

iwconfig/ ifconfig :

- To view and configure network interface details.

iwconfig

```
$ iwconfig wlan0
```

- ESSID: N/w name (My WiFi)
- Mode: Operating mode (Managed)
- Access point: MAC address (00:11:22:33:44:55)
- Frequency: Channel freq. in GHz (2.4370GHz)
- Bit rate: Data Transfer Speed (54mb/s)
- Tx-Power: Transmission Power dBm(20)
- Retry: #Failed Transmissions (7)
- RTS /CTS: Handshake settings (off)
- Fragment: Pkt. Fragmentation threshold
- Power management: Power saving mode

ifconfig

```
$ ifconfig eth0
```

- inet : IPv4 address (192.168.1.10)
- netmask: subnet mask (255.255.255.0)
- broadcast: bc address (192.168.1.255)
- inet6 : IPv6 address (fe80::1)
- ether : MAC address (00:11:22:33:44:55)
- Rx packets: #received (1234)
- Tx packets: #transmitted (5678)
- Rx/Tx bytes: #bytes received/sent (102400)
- MTU: Maximum Transmission Unit (1500)
- UP/DOWN: Interface Status (UP)

Output:

```
akash@akash:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.29.220 netmask 255.255.255.0 broadcast 192.168.29.255
        inet6 fe80::a00:27ff:fe0e:cd8c prefixlen 64 scopeid 0x20<link>
        inet6 2405:201:e04f:a81a:a00:27ff:fe0e:cd8c prefixlen 64 scopeid 0x0<global>
        inet6 2405:201:e04f:a81a:f830:ff0d:dd34:b046 prefixlen 64 scopeid 0x0<global>
        ether 08:00:27:0e:cd:8c txqueuelen 1000 (Ethernet)
        RX packets 48998 bytes 51187757 (51.1 MB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 20591 bytes 6802616 (6.8 MB)
        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 1366 bytes 128761 (128.7 KB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 1366 bytes 128761 (128.7 KB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

akash@akash:~$ sudo ethtool enp0s3 | grep -i speed
    Speed: 1000Mb/s
akash@akash:~$
```

```
akash@akash:~$ sudo ethtool enp0s3 | grep "Link detected"
    Link detected: yes
akash@akash:~$ sudo ethtool enp0s3 | grep -A5 "Advertised"
    Advertised link modes:  10baseT/Half 10baseT/Full
                            100baseT/Half 100baseT/Full
                            1000baseT/Full
    Advertised pause frame use: No
    Advertised auto-negotiation: Yes
    Advertised FEC modes: Not reported
    Speed: 1000Mb/s
    Duplex: Full
    Auto-negotiation: on
    Port: Twisted Pair
    PHYAD: 0
akash@akash:~$ ifconfig enp0s3 | grep -E "RX errors|TX errors|collisions"
    RX errors 0 dropped 0 overruns 0 frame 0
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
akash@akash:~$
```

Task 9:

Log in to your home router's web interface (usually at 192.168.1.1 or 192.168.0.1) and check the connected devices list.

Explanation:

Home Router:

- To manage the network and connected devices.
- We can access router information via router's login IP

Steps to connect:

(I) Finding router ip :

\$ ip route | grep default }
\$ ifconfig / \$ ipconfig } → 192.168.29.1

(II) Open in browser:

<http://192.168.29.1>



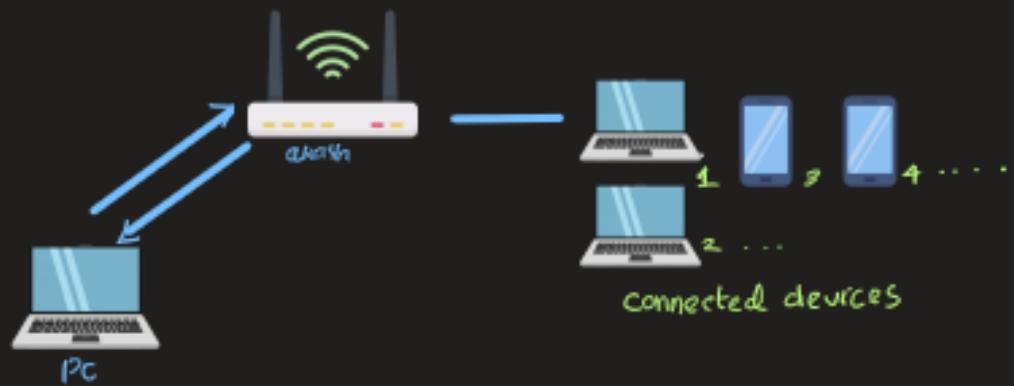
(III) Login with username and password:

Username: ajayakash
password : embederUR

(IV) Checking connected devices:

Connected devices → LAN Status

WLAN Status



Screenshot of the Jio Centrum Home Gateway web interface, showing the "Access Points" page. The interface includes a sidebar with navigation links like Dashboard, Status, Network, Security, Administration, and Advanced. The main content area shows a list of access points with columns for Status, AP Name, Frequency, SSID, Broadcast SSID, Security, and Profile Name. The list includes entries for ap1 through ap6, each with a different status (green checkmark or red X), frequency (2.4 Ghz or 5 Ghz), SSID (Ajay Aakash, Jio_2, Jio_3, Ajay Aakash_5G, Jio_2, Jio_3), broadcast SSID (Ajay Aakash, Jio_2, Jio_3, Ajay Aakash_5G, Jio_2, Jio_3), security (WPA2), and profile name (Jio_1, Jio_2, Jio_3, Jio_4, Jio_5, Jio_6).

Status	AP Name	Frequency	SSID	Broadcast SSID	Security	Profile Name
✓	ap1	2.4 Ghz	Ajay Aakash	Ajay Aakash	WPA2	Jio_1
✗	ap2	2.4 Ghz	Jio_2	Jio_2	WPA2	Jio_2
✗	ap3	2.4 Ghz	Jio_3	Jio_3	WPA2	Jio_3
✓	ap4	5 Ghz	Ajay Aakash_5G	Ajay Aakash_5G	WPA2	Jio_4
✗	ap5	5 Ghz	Jio_2	Jio_2	WPA2	Jio_5
✗	ap6	5 Ghz	Jio_3	Jio_3	WPA2	Jio_6

Firmware Version: SKYWTI_3COW407_R2.57
Serial Number: RNOOTHJS2160784

Output:

```
akash@akash:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.29.220 netmask 255.255.255.0 broadcast 192.168.29.255
        inet6 fe80::a00:27ff:fe0e:cd8c prefixlen 64 scopeid 0x20<link>
        inet6 2405:201:e04f:a81a:a00:27ff:fe0e:cd8c prefixlen 64 scopeid 0x0<global>
        inet6 2405:201:e04f:a81a:3df8:19d4:d7c2:db86 prefixlen 64 scopeid 0x0<global>
    ether 08:00:27:0e:cd:8c txqueuelen 1000 (Ethernet)
    RX packets 14881 bytes 12426614 (12.4 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 9140 bytes 3422965 (3.4 MB)
    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 843 bytes 83326 (83.3 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 843 bytes 83326 (83.3 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

akash@akash:~$ journalctl -u NetworkManager | grep -i "state changed new lease"
Feb 16 21:09:37 akash NetworkManager[838]: <info> [1739720377.2298] dhcpc4 (enp0s3): state changed new lease, address=10.0.2.15
, acd pending
Feb 16 21:09:37 akash NetworkManager[838]: <info> [1739720377.3874] dhcpc4 (enp0s3): state changed new lease, address=10.0.2.15
Feb 18 12:55:52 akash NetworkManager[851]: <info> [1739863552.8395] dhcpc4 (enp0s3): state changed new lease, address=10.0.2.15
, acd pending
Feb 18 12:55:52 akash NetworkManager[851]: <info> [1739863552.9941] dhcpc4 (enp0s3): state changed new lease, address=10.0.2.15
Feb 18 13:31:13 akash NetworkManager[815]: <info> [1739865673.1415] dhcpc4 (enp0s3): state changed new lease, address=10.0.2.15
, acd pending
akash@akash:~$ journalctl -u NetworkManager | grep -i "state changed new lease"
Feb 16 21:09:37 akash NetworkManager[838]: <info> [1739720377.2298] dhcpc4 (enp0s3): state changed new lease, address=10.0.2.15
, acd pending
Feb 16 21:09:37 akash NetworkManager[838]: <info> [1739720377.3874] dhcpc4 (enp0s3): state changed new lease, address=10.0.2.15
Feb 18 12:55:52 akash NetworkManager[851]: <info> [1739863552.8395] dhcpc4 (enp0s3): state changed new lease, address=10.0.2.15
, acd pending
Feb 18 12:55:52 akash NetworkManager[851]: <info> [1739863552.9941] dhcpc4 (enp0s3): state changed new lease, address=10.0.2.15
Feb 18 13:31:13 akash NetworkManager[815]: <info> [1739865673.1415] dhcpc4 (enp0s3): state changed new lease, address=10.0.2.15
, acd pending
Feb 18 13:31:13 akash NetworkManager[815]: <info> [1739865673.2925] dhcpc4 (enp0s3): state changed new lease, address=10.0.2.15
Feb 18 14:00:28 akash NetworkManager[815]: <info> [1739867428.4221] dhcpc4 (enp0s3): state changed new lease, address=10.0.2.15
, acd pending
Feb 18 14:00:28 akash NetworkManager[815]: <info> [1739867428.6054] dhcpc4 (enp0s3): state changed new lease, address=10.0.2.15
Feb 18 14:30:05 akash NetworkManager[821]: <info> [1739869205.7238] dhcpc4 (enp0s3): state changed new lease, address=10.0.2.15
, acd pending
Feb 18 14:30:05 akash NetworkManager[821]: <info> [1739869205.9023] dhcpc4 (enp0s3): state changed new lease, address=10.0.2.15
Feb 18 14:33:10 akash NetworkManager[840]: <info> [1739869390.7464] dhcpc4 (enp0s3): state changed new lease, address=10.0.2.15
, acd pending
Feb 18 14:33:10 akash NetworkManager[840]: <info> [1739869390.9083] dhcpc4 (enp0s3): state changed new lease, address=10.0.2.15
Feb 18 16:27:14 akash NetworkManager[833]: <info> [1739876234.5145] dhcpc4 (enp0s3): state changed new lease, address=10.0.2.15
, acd pending
Feb 18 16:27:14 akash NetworkManager[833]: <info> [1739876234.7595] dhcpc4 (enp0s3): state changed new lease, address=10.0.2.15
Feb 21 23:35:38 akash NetworkManager[838]: <info> [1740161138.8036] dhcpc4 (enp0s3): state changed new lease, address=10.0.2.15
, acd pending
Feb 21 23:35:38 akash NetworkManager[838]: <info> [1740161138.9745] dhcpc4 (enp0s3): state changed new lease, address=10.0.2.15
Feb 24 20:03:53 akash NetworkManager[848]: <info> [1740407633.7869] dhcpc4 (enp0s3): state changed new lease, address=10.0.2.15
, acd pending
Feb 24 20:03:53 akash NetworkManager[848]: <info> [1740407633.9066] dhcpc4 (enp0s3): state changed new lease, address=10.0.2.15
Feb 24 21:12:35 akash NetworkManager[828]: <info> [1740411755.3692] dhcpc4 (enp0s3): state changed new lease, address=10.0.2.15
```

Task 11:

Using a terminal, connect to a remote machine via SSH and telnet.

Explanation:

SSH:

- Secure Shell (SSH) – a secured network protocol
- To remotely access command line over network
- It uses public key cryptography

Implementation:

SSH: encrypted text

(I) Install ssh packages:

```
$ sudo apt install -y openssh
```

(II) Identify remote machine's IP:

```
$ ifconfig / $ ipconfig
```

(III) Connect:

```
$ ssh akash@ 192.168.29.220  
username Host IP
```

(IV) Authentication:

Enter the password of remote machine.

```
pwd  
/home/akash
```

The screenshot shows two terminal windows. The left window is titled 'akash@akash:' and displays the output of the 'ifconfig' command, listing network interfaces with their IP addresses and broadcast ranges. The right window is titled 'akash@akash:' and shows an SSH session. It prompts for a password, displays a welcome message for Ubuntu 24.04.2 LTS, and provides documentation links. It also shows system updates and ESM information, ending with a login history entry.

```
Mar 1 13:51 akash@akash:~$ ifconfig | grep inet
    inet 192.168.29.220 netmask 255.255.255.0 broadcast 192.168.29.255
        inet6 fe80::a00:27ff:fe0e:cd8c prefixlen 64 scopeid 0x20<link>
            inet6 2405:201:e04f:a81a:a00:27ff:fe0e:cd8c prefixlen 64 scopeid 0x0<global>
            inet6 2405:201:e04f:a81a:3df8:19d4:d7c2:db86 prefixlen 64 scopeid 0x0<global>
            inet 127.0.0.1 netmask 255.0.0.0
                inet6 ::1 prefixlen 128 scopeid 0x10<host>
akash@akash:~$ PS C:\Users\akash> ssh akash@192.168.29.220
akash@192.168.29.220's password:
Welcome to Ubuntu 24.04.2 LTS (GNU/Linux 6.11.0-17-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

19 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

6 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm

Last login: Wed Feb 26 21:15:13 2025 from 192.168.29.112
akash@akash:~$ |
```

ssh connection

telnet:

Telnet :

- Teletype Network (Telnet) — protocol to access remote pc
- Actions : → remote login → Testing
→ file transfer → Remote maintenance
→ Network management
- Telnet is older and less secure. → sends data in plaintext
↳ So best alternative is SSH

Implementation :

(I) Install telnet:

\$ sudo apt install -y telnetd

(II) Identify remote machine's IP:

\$ ifconfig / \$ ipconfig

(III) Connect:

\$ telnet 192.168.1.10 23
IP Port

(IV) Authentication

Enter Username and password.

telnet: plaintext

```
Mar 1 14:31 akash@akash:~$ ifconfig | grep inet
    inet 192.168.29.220 netmask 255.255.255.0 broadcast 192.168.29.255
        inet6 fe80::a00:27ff:fe0e:cd8c prefixlen 64 scopeid 0x20<link>
            inet6 2405:201:e04f:a81a:cdad:892b:2b20:146b prefixlen 64 scopeid 0x0<global>
            inet6 2405:201:e04f:a81a:a00:27ff:fe0e:cd8c prefixlen 64 scopeid 0x0<global>
        inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
akash@akash:~$ |
```

```
Linux 6.11.0-17-generic (akash) (pts/1)
akash login: akash
Password:
Welcome to Ubuntu 24.04.2 LTS (GNU/Linux 6.11.0-17-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

28 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

6 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm

akash@akash:~$ pwd
/home/akash
akash@akash:~$ |
akash@akash:~$ |
```

THE END

AKASH S | embedUR Systems