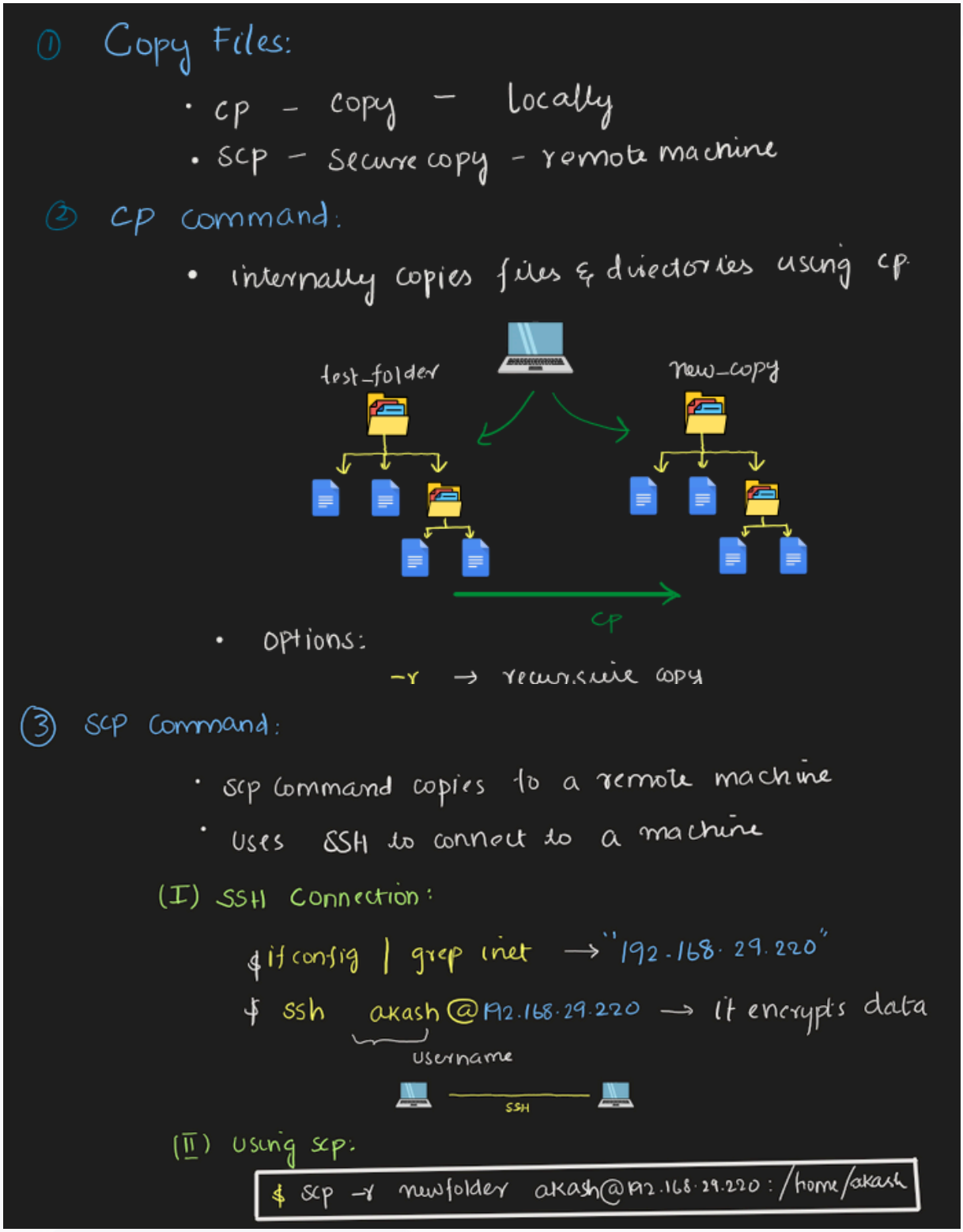
NETWORKING TRAINING - MODULE 1 & 2

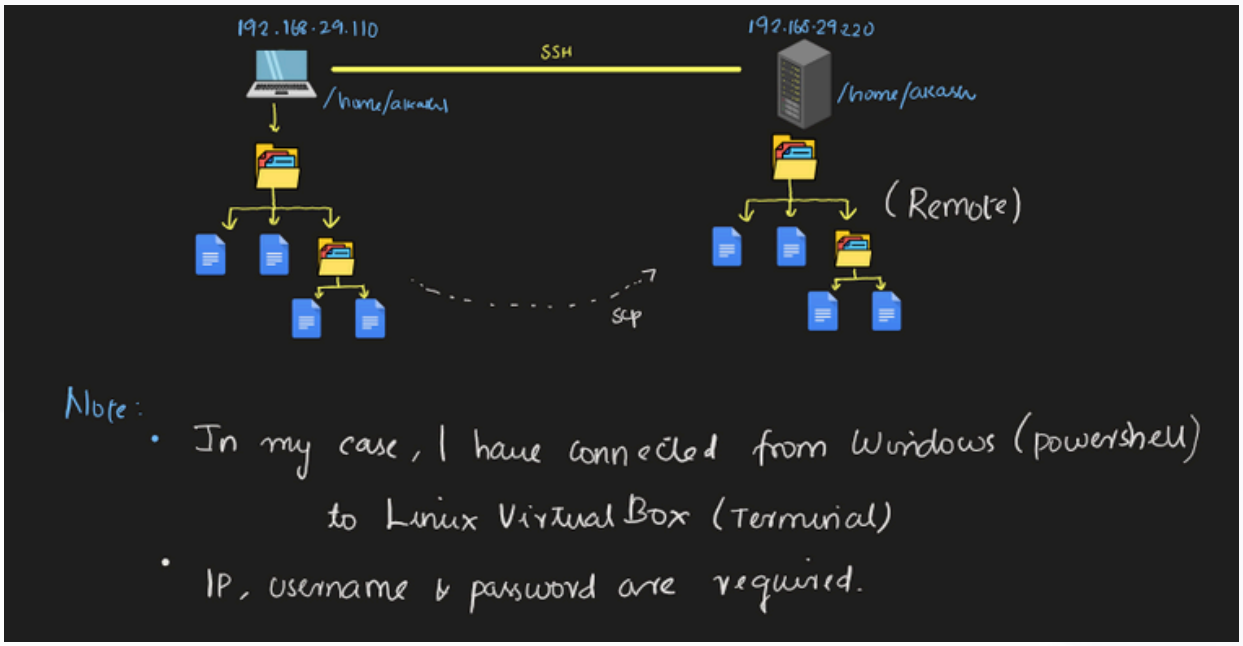
Akash S, embedUR Systems

Task 1:

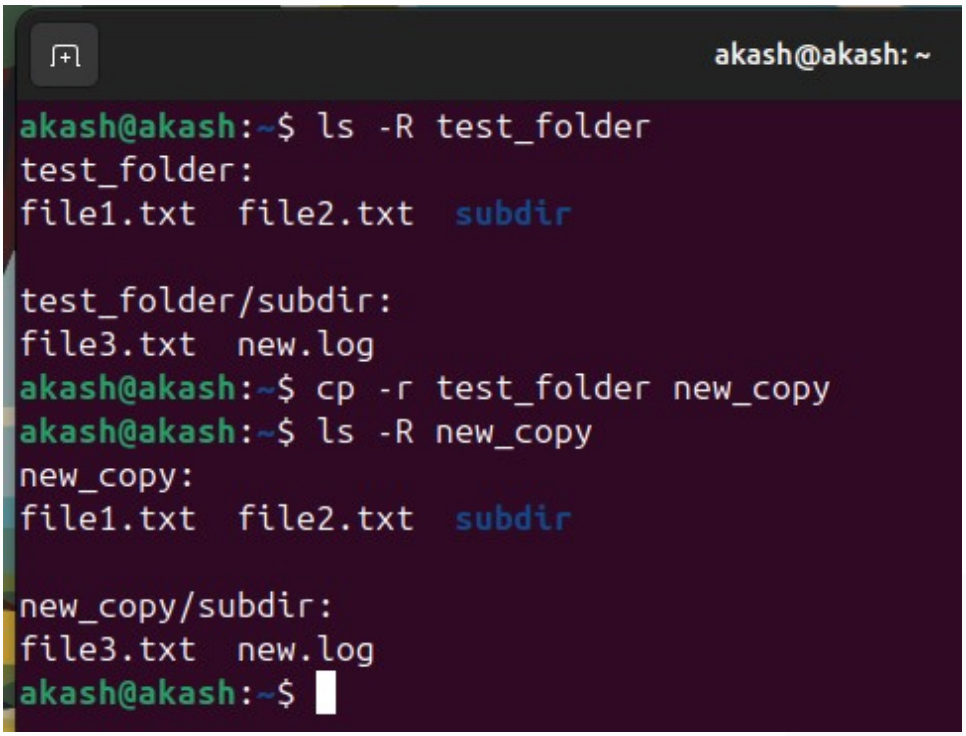
Consider a case, a folder has multiple files and how would copy it to destination machine path (Try using SCP, cp options in Linux)

Explanation:

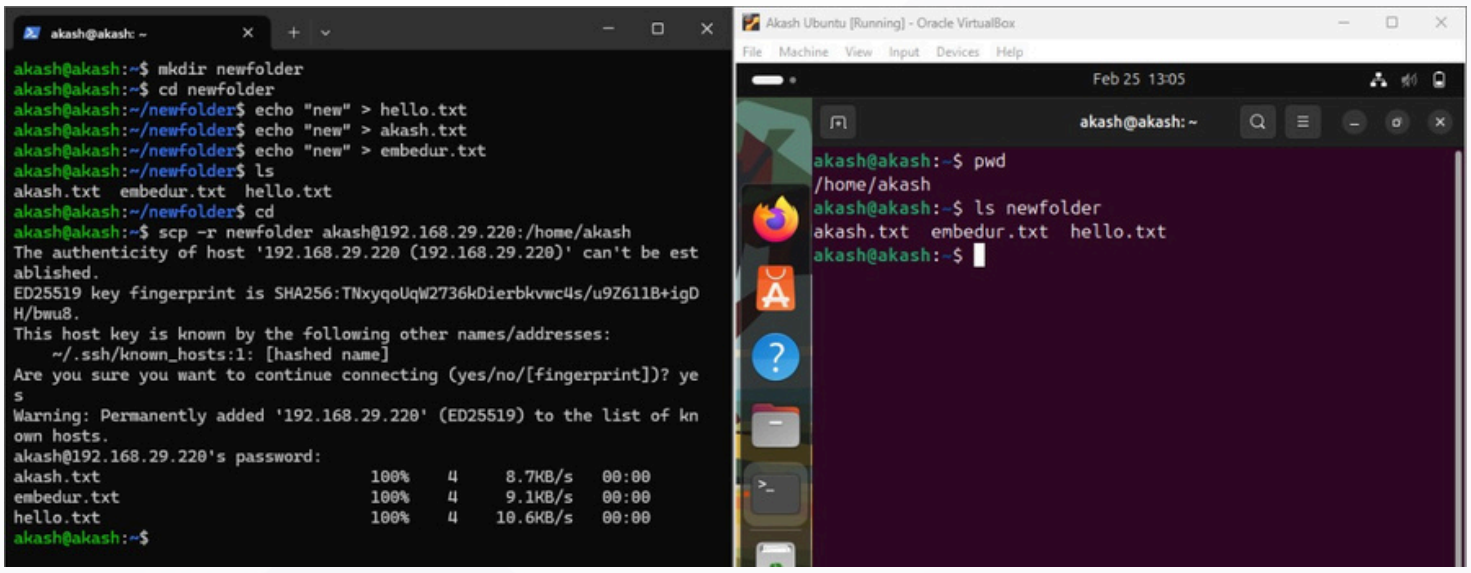




Outputs:



cp command

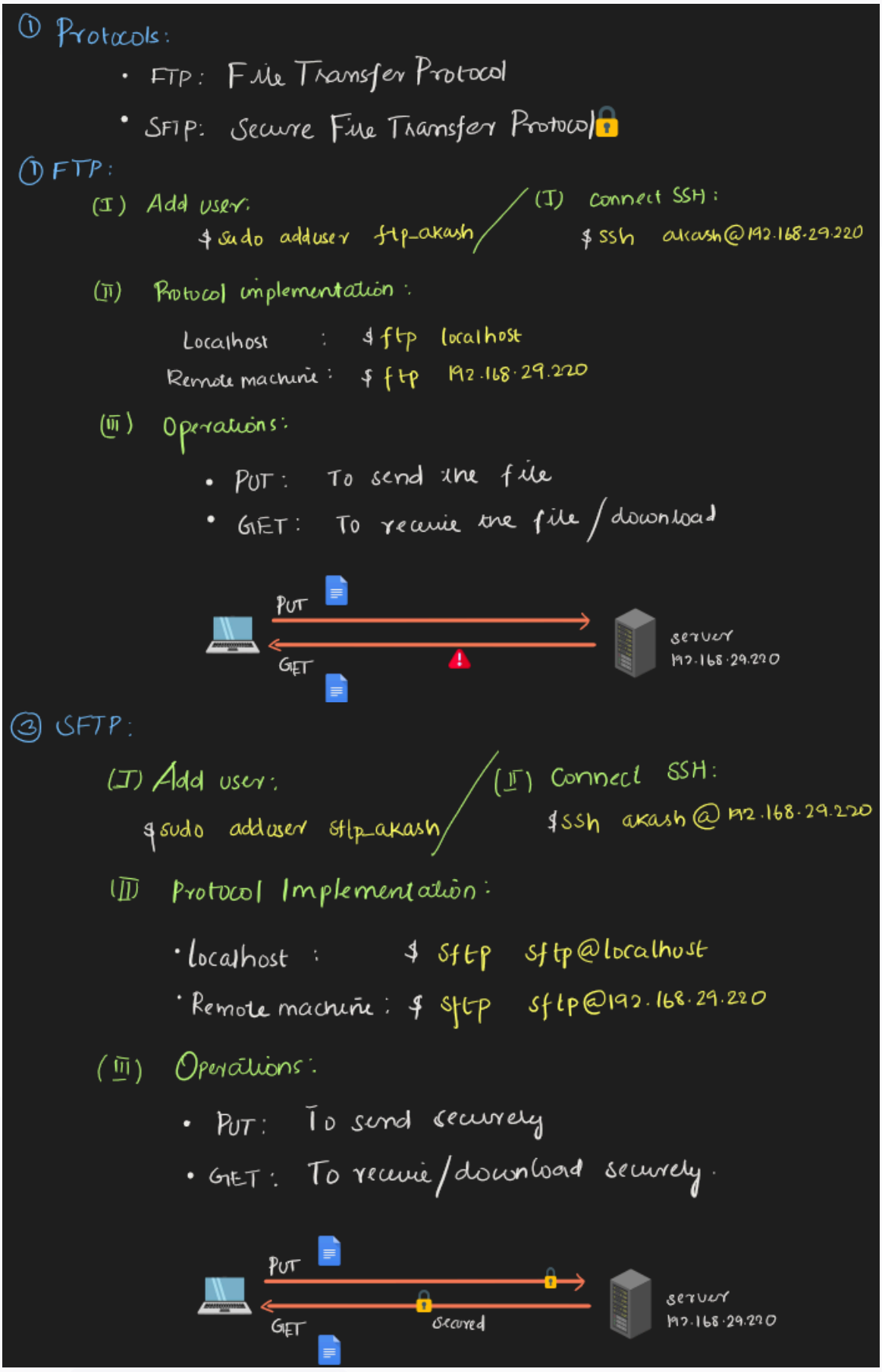


scp command

Task 2:

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

Explanation:



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

```
Windows PowerShell
PS C:\Users\akash> echo "new file" > type.txt
PS C:\Users\akash> sftp akash@192.168.29.220
akash@192.168.29.220's password:
Connected to 192.168.29.220.
sftp> put type.txt
Uploading type.txt to /home/akash/type.txt
type.txt                                      100%   22     5.5KB/s   00:00
sftp> get type.txt
Fetching /home/akash/type.txt to type.txt
type.txt                                      100%   22     7.4KB/s   00:00
sftp> bye
PS C:\Users\akash>
```

```
Akash Ubuntu [Running] - Oracle VirtualBox
File  Machine  View  Input  Devices  Help
Feb 25 21:12
akash@akash: ~
akash@akash:~$ ls -l /home/akash/type.txt
-rw-rw-r-- 1 akash akash 22 Feb 25 21:10 /home/akash/type.
txt
akash@akash:~$ cat /home/akash/type.txt
◆◆new file
akash@akash:~$
```

sftp with remote machine

Task 3:

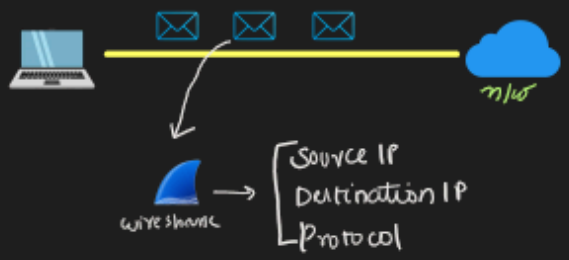
Explore with Wireshark/TCP-dump/cisco packet tracer tools and learn about packets filters.

Explanation:

① Wireshark:

→ Why?

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



→ Initialization:

→ Start wireshark

→ Select an interface

- enp0s3
- wi-fi
- eth0

→ Start capture

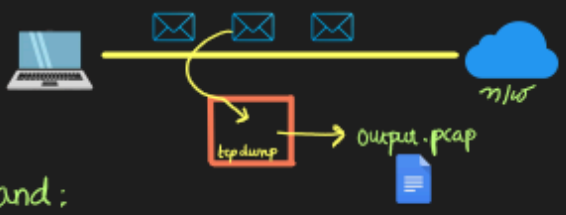
→ Examples:

- 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
- I/le can save them to a `.pcap' file.



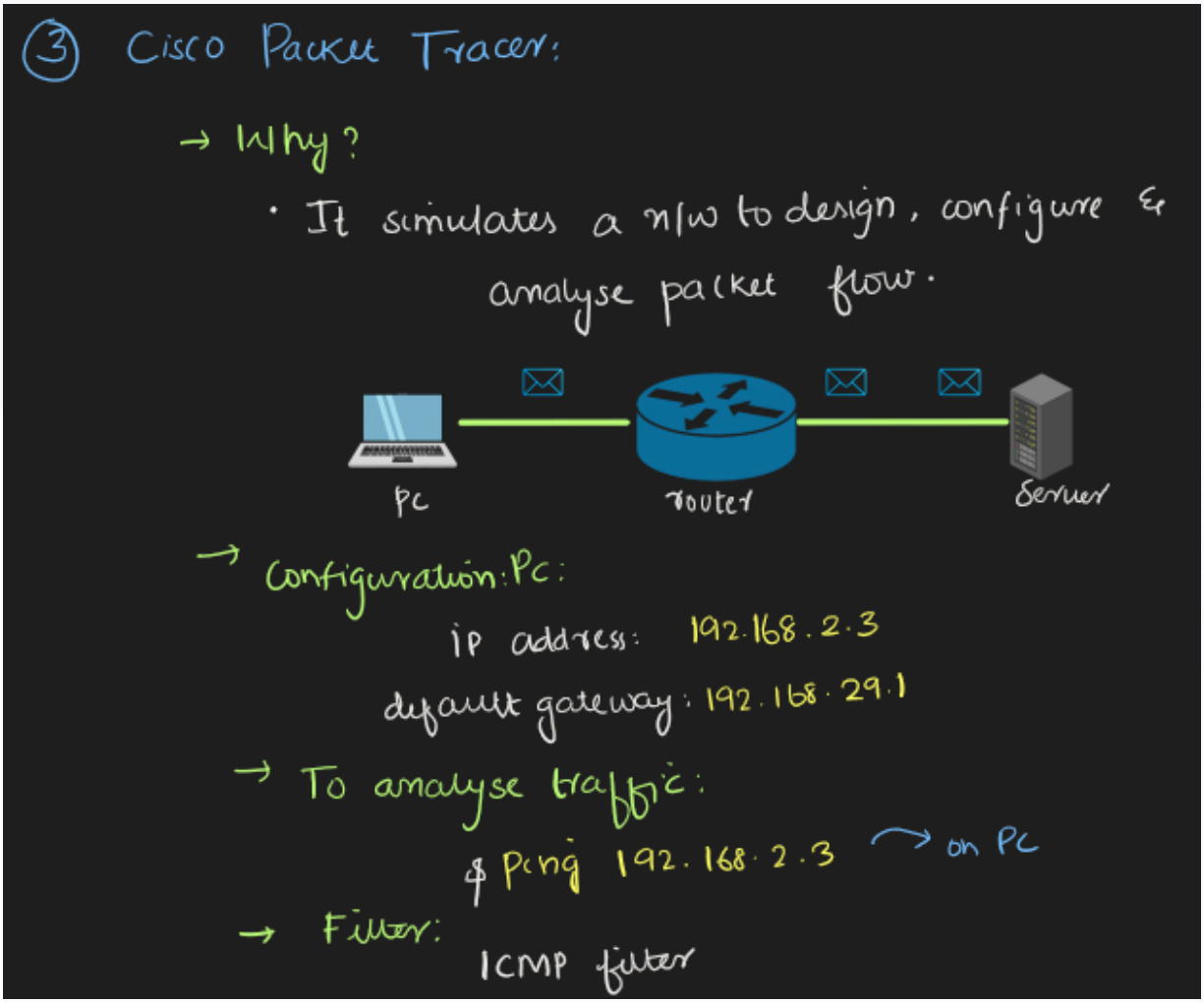
→ Command:

$ 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.



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:~$
```

outputpkt.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

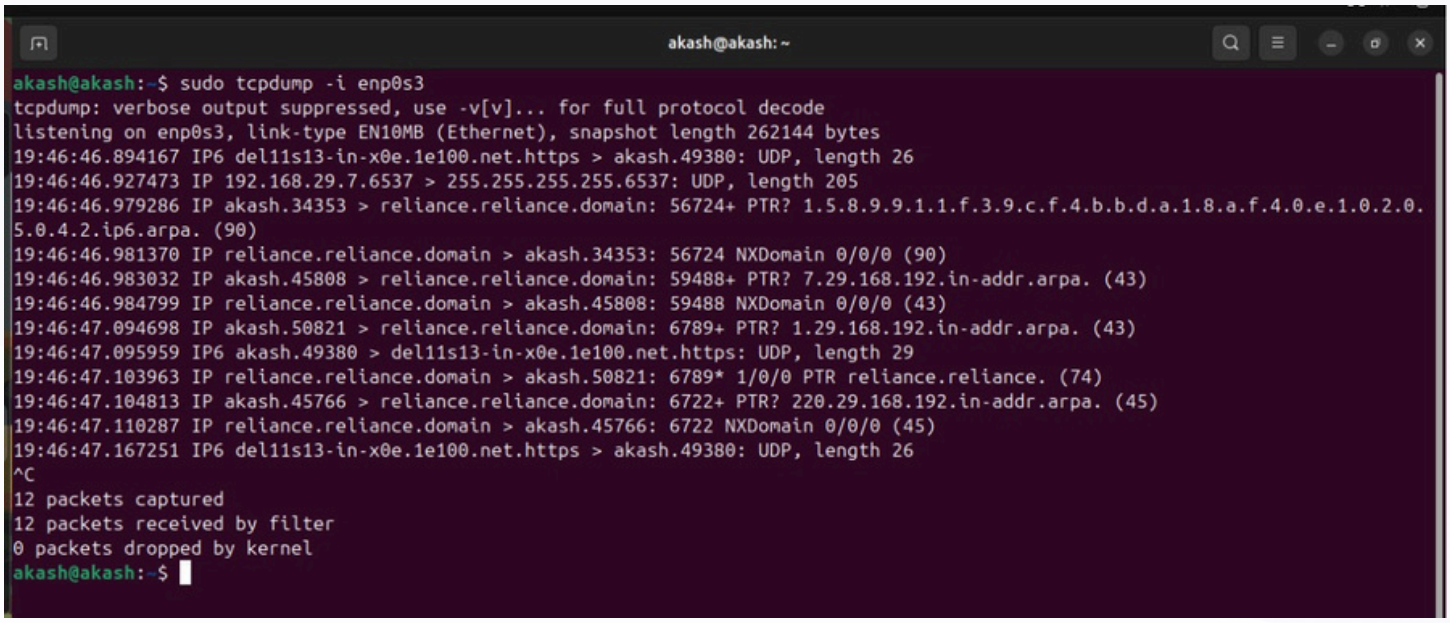
Apply a display filter ... <Ctrl-/>

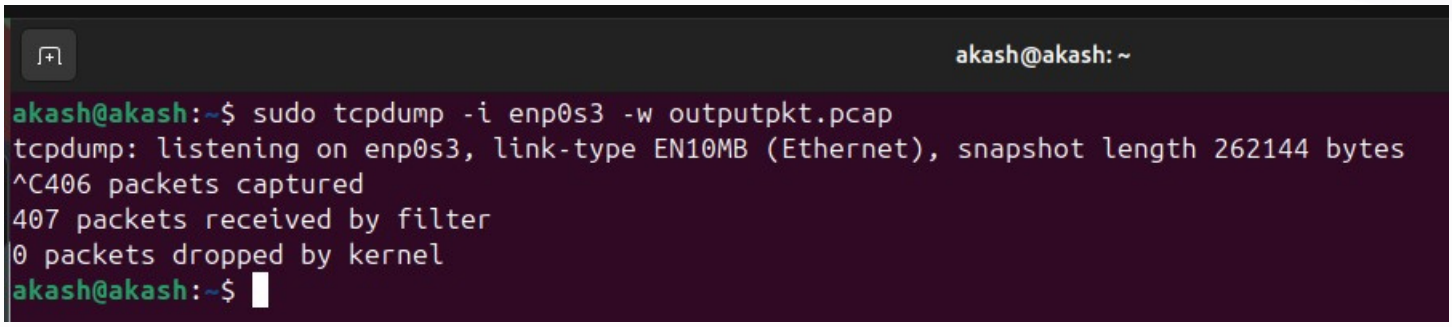
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.29.220	192.168.29.1	DNS	70	Standard query 0xed6b AAA…
2	0.000273	192.168.29.220	192.168.29.1	DNS	70	Standard query 0x6b94 A g…
3	0.041403	192.168.29.220	142.250.182.10	TLSv1.2	295	Application Data
4	0.041603	192.168.29.220	142.250.182.10	TLSv1.2	105	Application Data
5	0.106838	192.168.29.220	142.250.182.10	TCP	66	47788 → 443 [ACK] Seq=269…
6	0.253716	192.168.29.220	142.250.182.10	TCP	66	47788 → 443 [ACK] Seq=269…
7	0.253733	192.168.29.220	142.250.182.10	TCP	66	47788 → 443 [ACK] Seq=269…
8	0.253758	192.168.29.220	142.250.182.10	TCP	66	47788 → 443 [ACK] Seq=269…
9	0.255905	192.168.29.220	142.250.182.10	TLSv1.2	105	Application Data

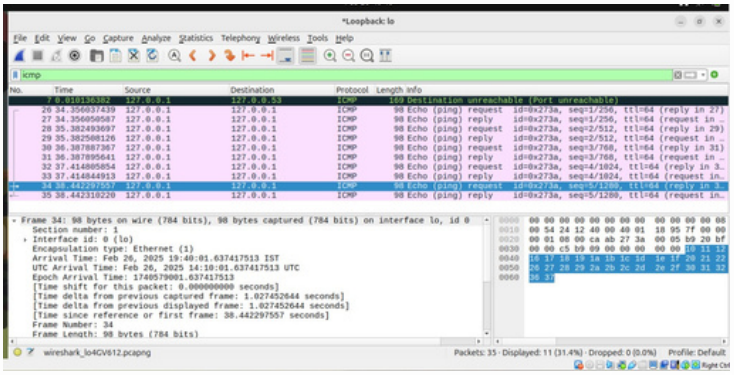
```
▸ Frame 1: 70 bytes on wire (560 bits), 70 bytes ca
▸ Ethernet II, Src: PCSSystemtec_0e:cd:8c (08:00:27
▸ Internet Protocol Version 4, Src: 192.168.29.220,
▸ User Datagram Protocol, Src Port: 59525, Dst Port
▸ Domain Name System (query)
```

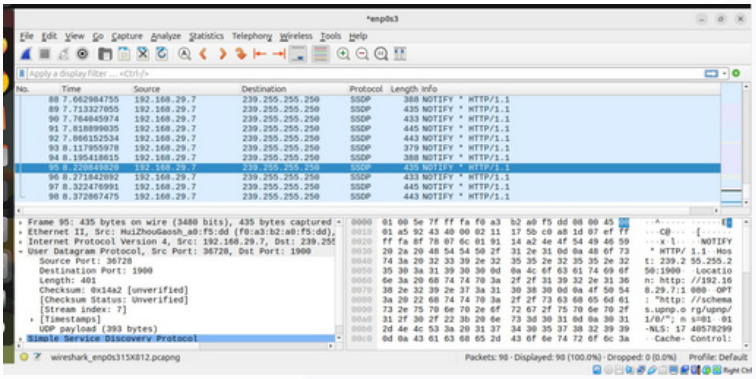
```
0000  04 ab 08 b6 f2 01 08 00  27 0e cd 8c 08 00 45 0
0010  00 38 34 d6 00 00 40 11  89 b1 c0 a8 1d dc c0 a
0020  1d 01 e8 85 00 35 00 24  bc 63 ed 6b 01 00 00 0
0030  00 00 00 00 00 00 06 67  6f 6f 67 6c 65 03 63 6
0040  6d 00 00 1c 00 01
```

Wireshark packet capture

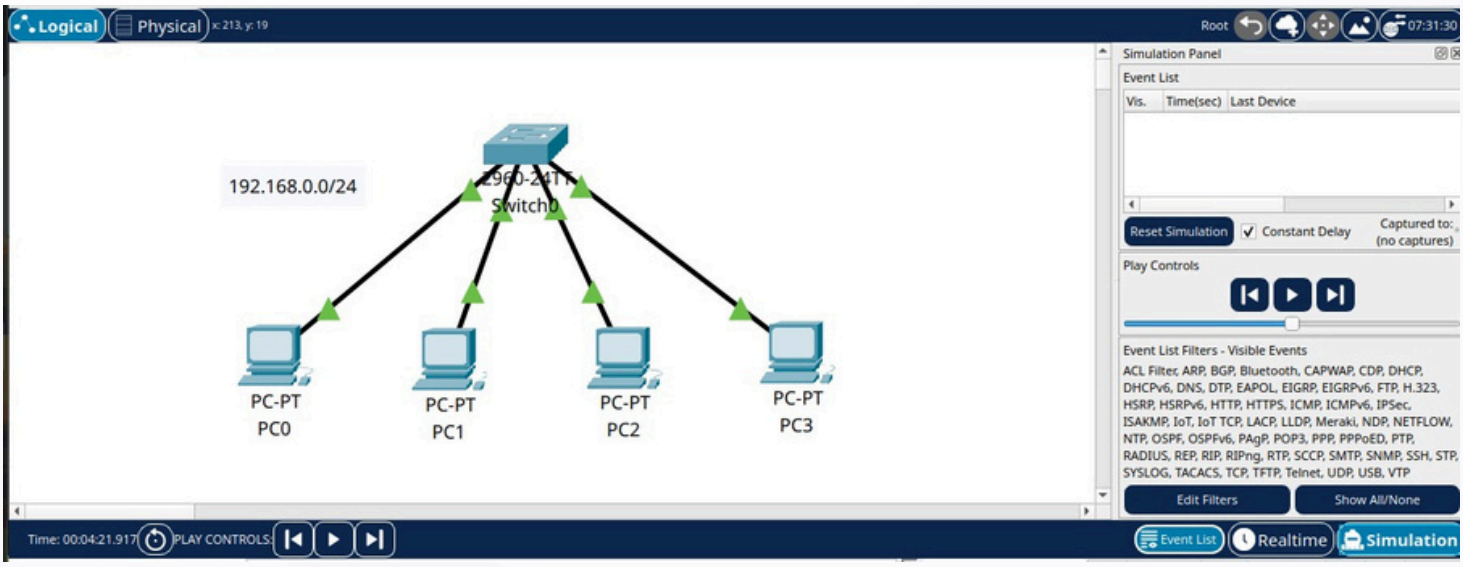








tcpdump

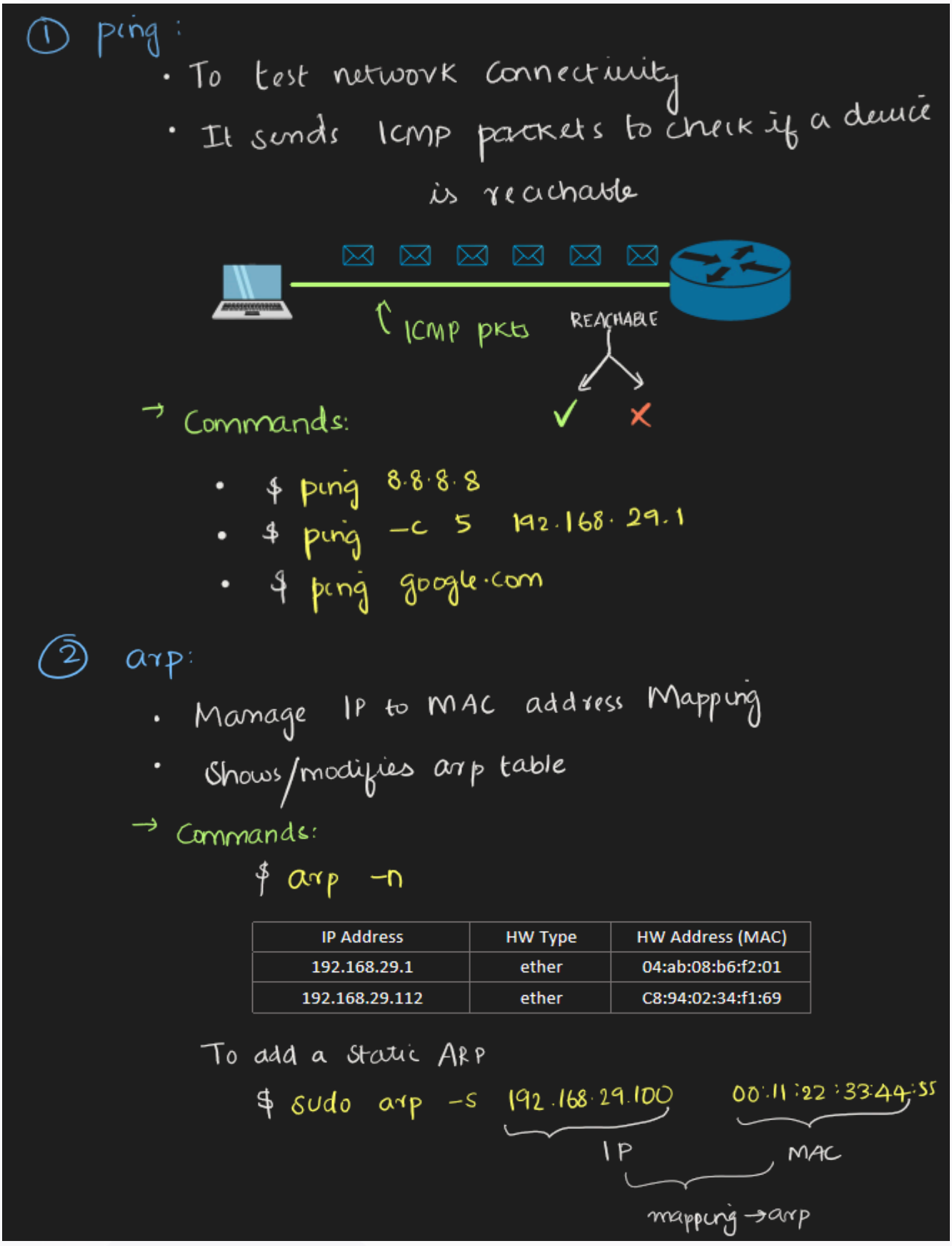


cisco packet tracer

Task 4:

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

Explanation:



Outputs:

```
akash@akash: ~
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

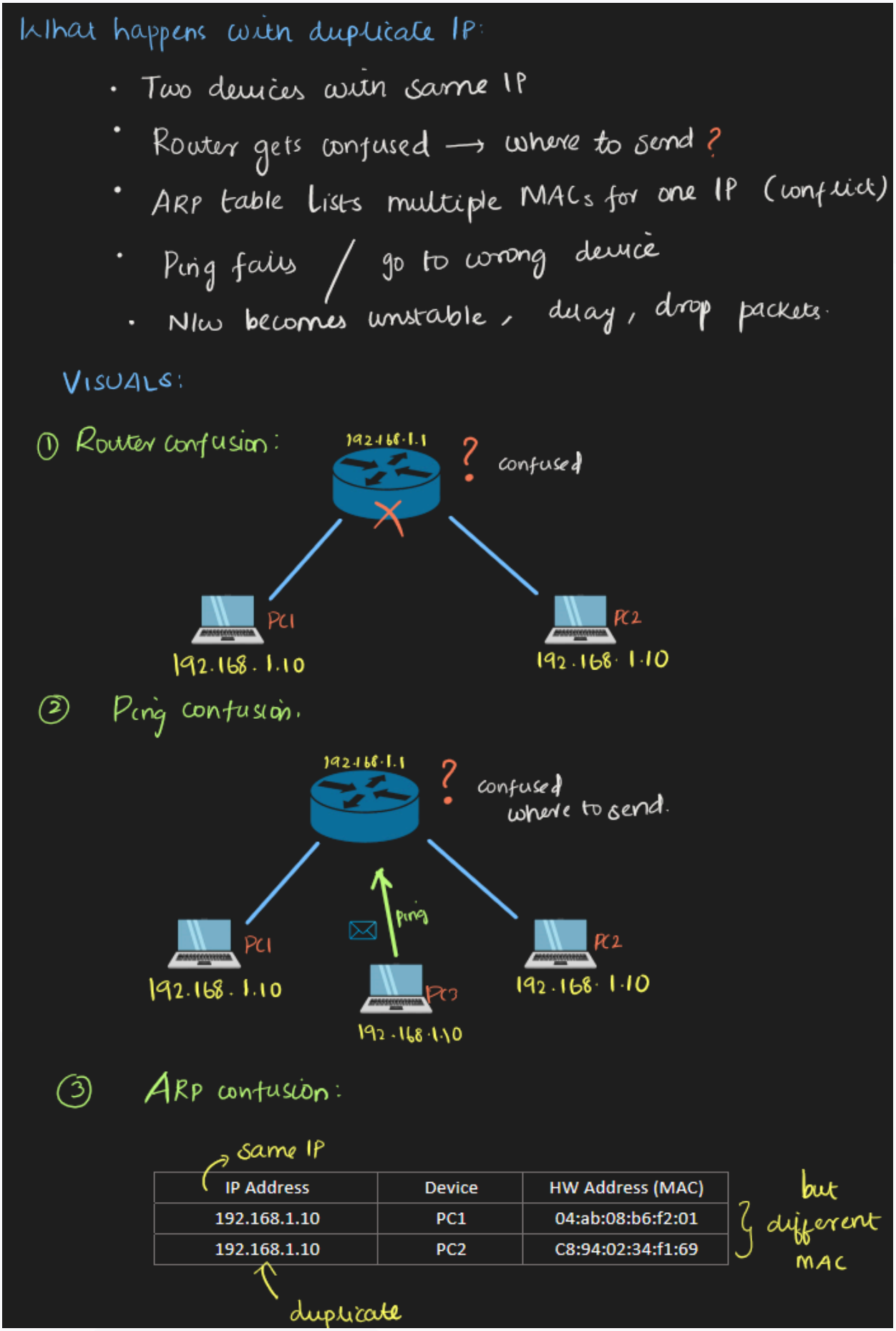
```
akash@akash: ~
akash@akash:~$ ip route | grep default
default via 192.168.29.1 dev enp0s3 proto dhcp src 192.168.29.220 metric 100
akash@akash:~$ arp -n | grep "192.168.29.1"
192.168.29.1             ether   04:ab:08:b6:f2:01   C                     enp0s3
192.168.29.112           ether   c8:94:02:34:f1:69   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

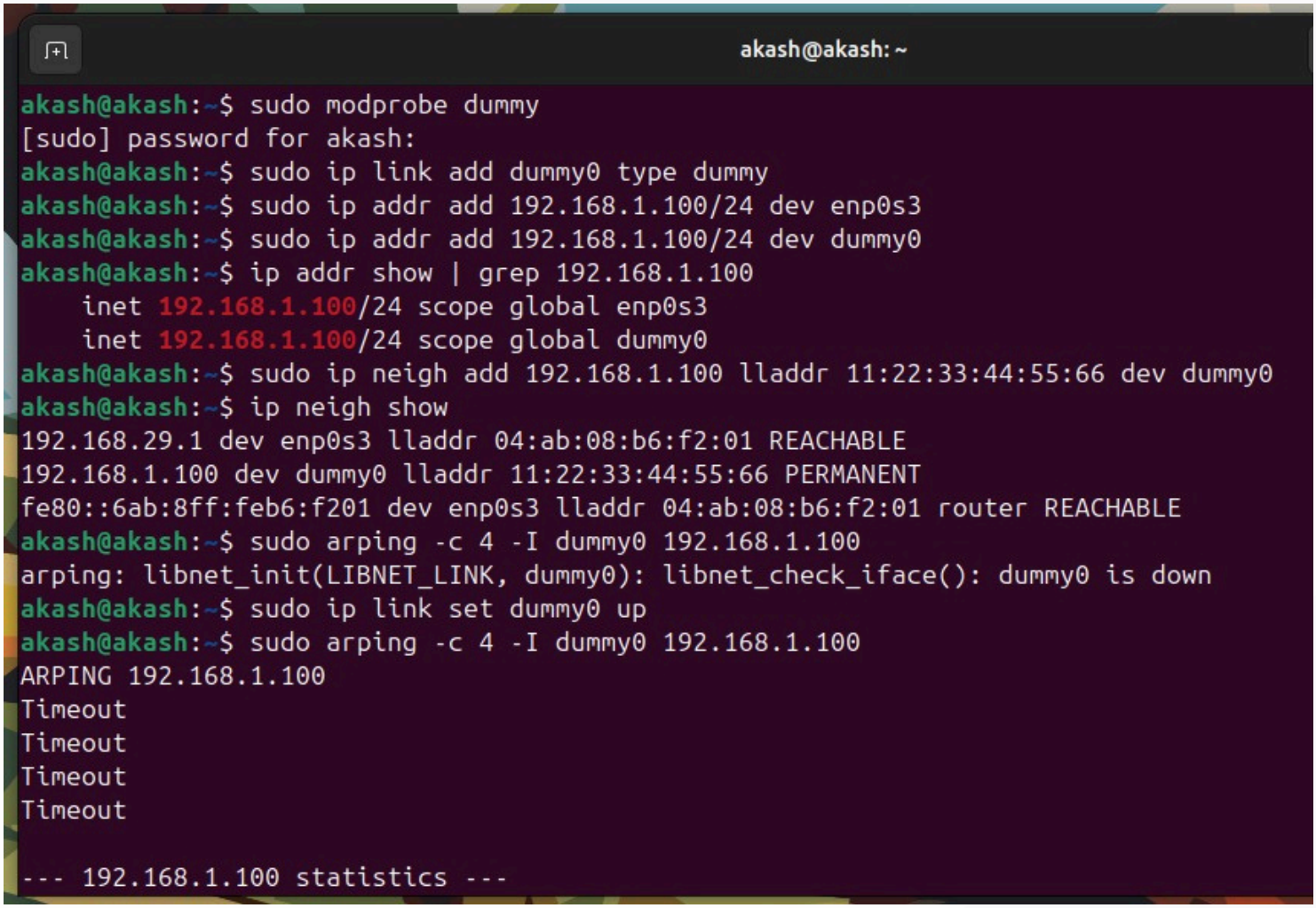
Task 5:

Understand what happens when duplicate IPs configured in a network.

Explanation:



Output:

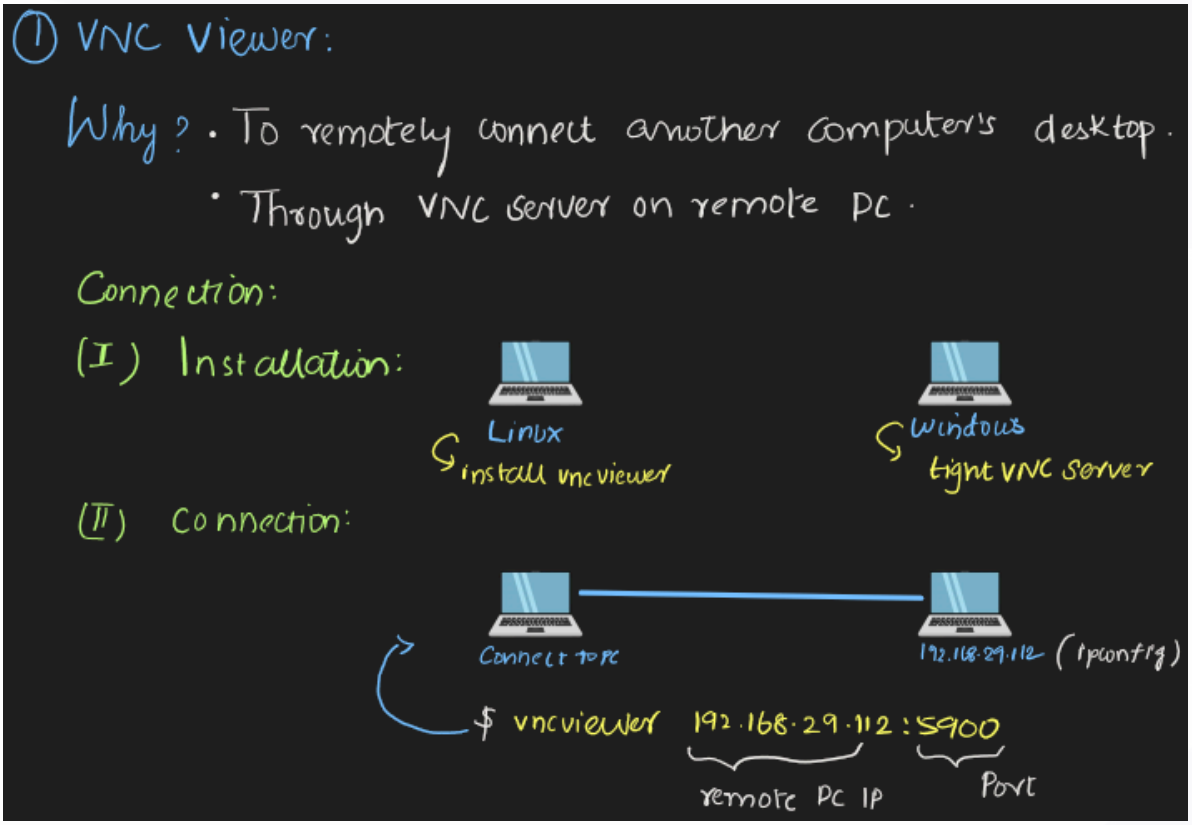


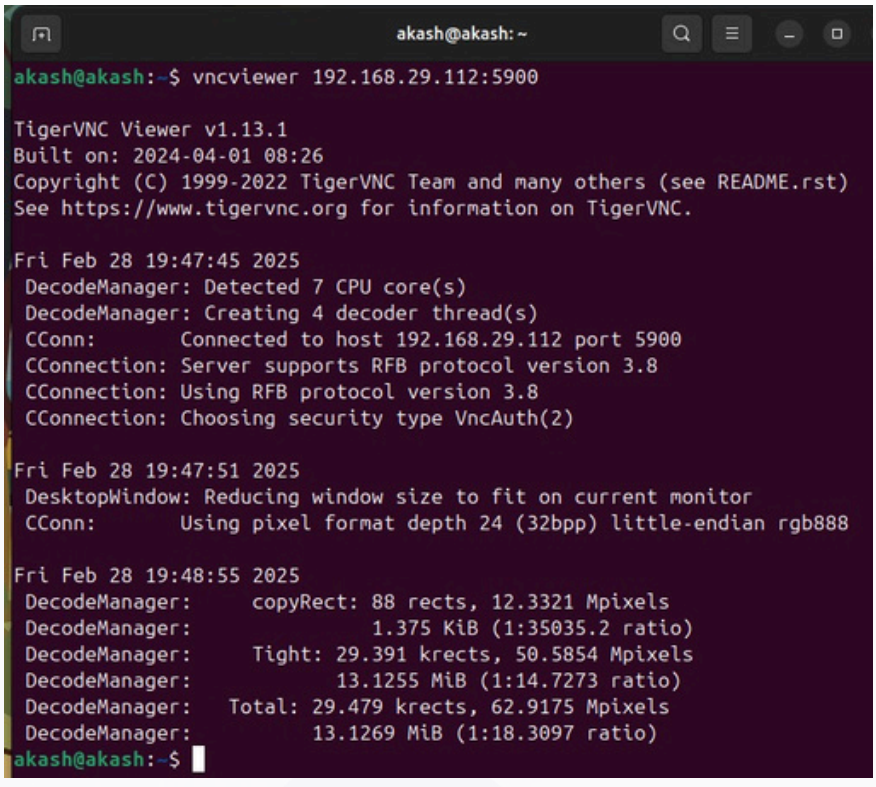
issues with duplicate IPs

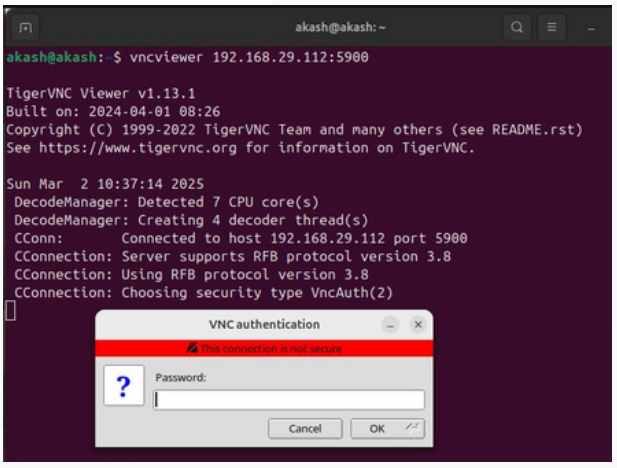
Task 6:

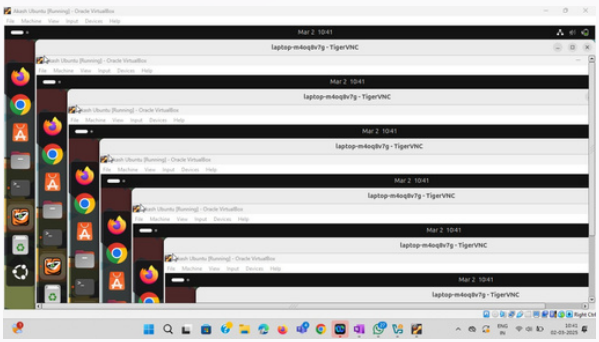
Understand how to access remote system using (VNC viewer, Anydesk, teamviewer and remote desktop connections)

Explanation:



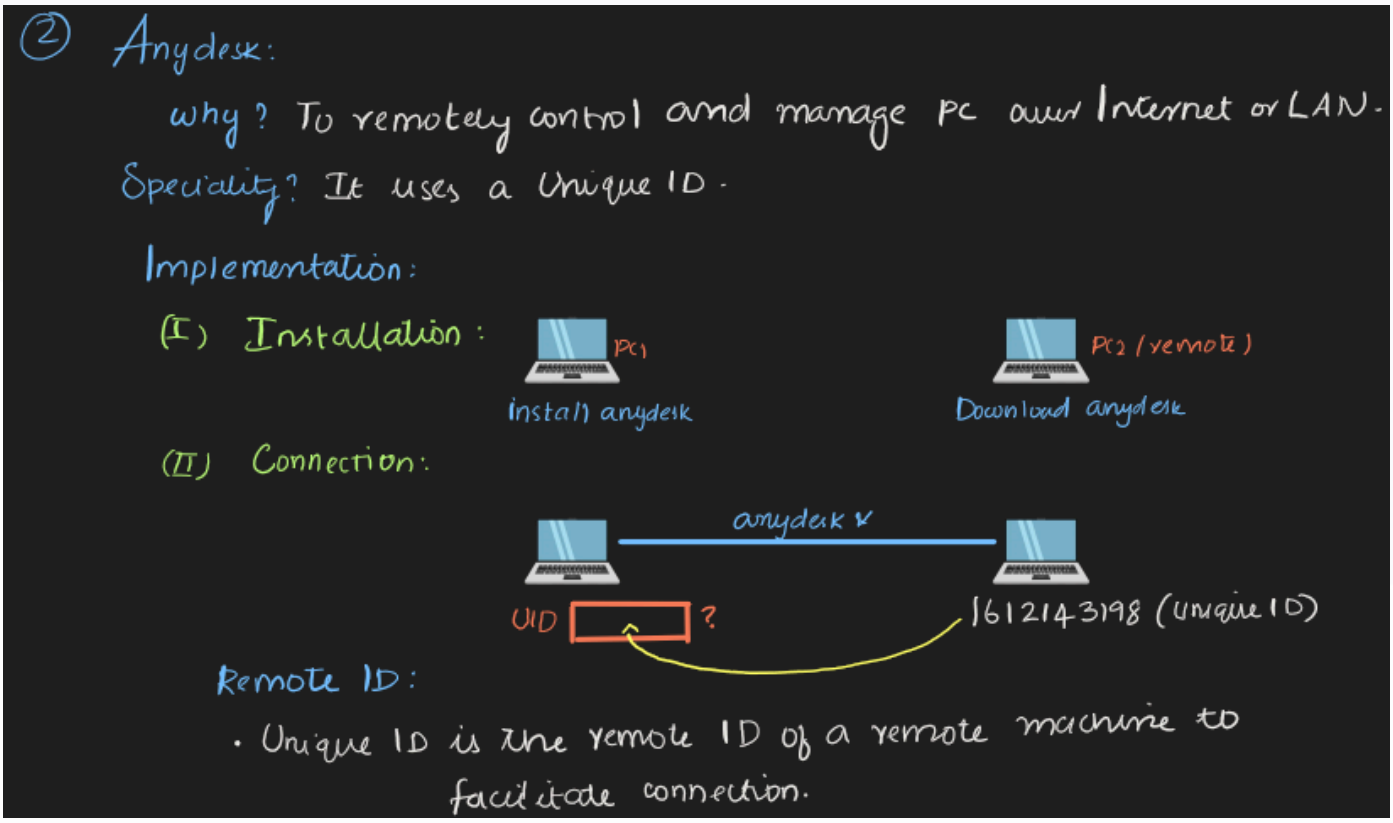


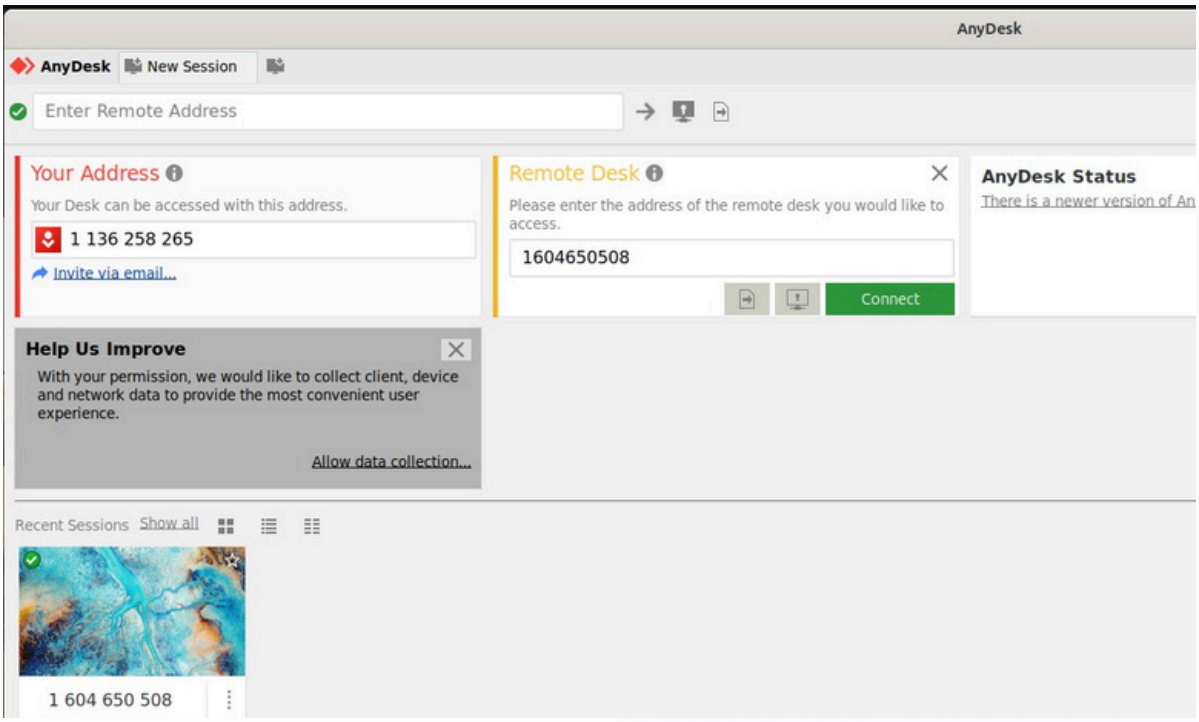


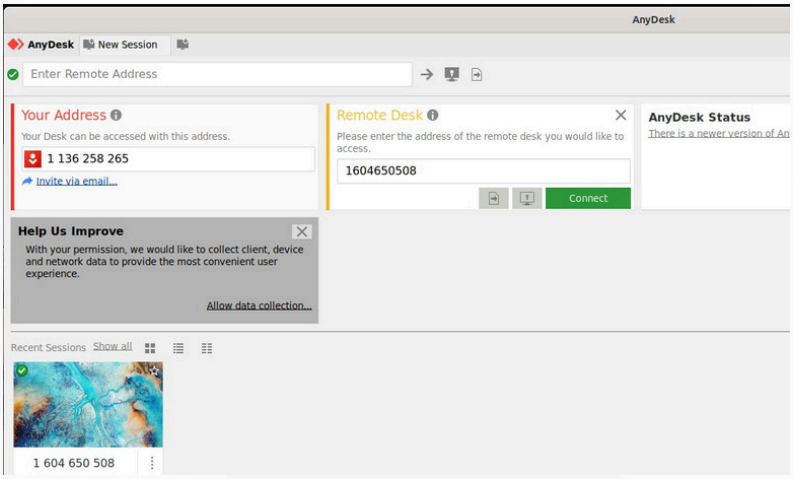


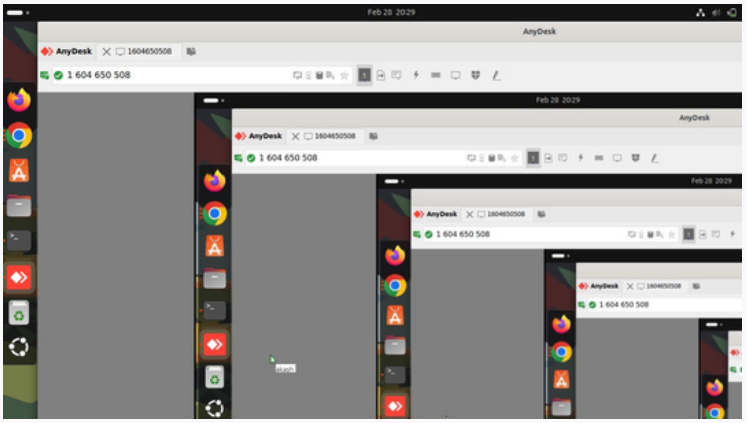
vncviewer

Anydesk:


② Anydesk:
why? To remotely control and manage PC over Internet or LAN.
Speciality? It uses a Unique ID.
Implementation:
(I) Installation:
PC1
Install anydesk
PC2 (remote)
Download anydesk
(II) Connection:
anydesk ✓
UID
?
1612143198 (Unique ID)
Remote ID:
• Unique ID is the remote ID of a remote machine to facilitate connection.


AnyDesk
AnyDesk
New Session
Enter Remote Address
Your Address
Your Desk can be accessed with this address.
1 136 258 265
Invite via email...
Remote Desk
Please enter the address of the remote desk you would like to access.
1604650508
Connect
AnyDesk Status
There is a newer version of An
Help Us Improve
With your permission, we would like to collect client, device and network data to provide the most convenient user experience.
Allow data collection...
Recent Sessions
Show all
1 604 650 508


AnyDesk
AnyDesk
New Session
Enter Remote Address
Your Address
Your Desk can be accessed with this address.
1 136 258 265
Invite via email...
Remote Desk
Please enter the address of the remote desk you would like to access.
1604650508
Connect
AnyDesk Status
There is a newer version of An
Help Us Improve
With your permission, we would like to collect client, device and network data to provide the most convenient user experience.
Allow data collection...
Recent Sessions
Show all
1 604 650 508



Teamviewer:

③ TeamViewer:

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

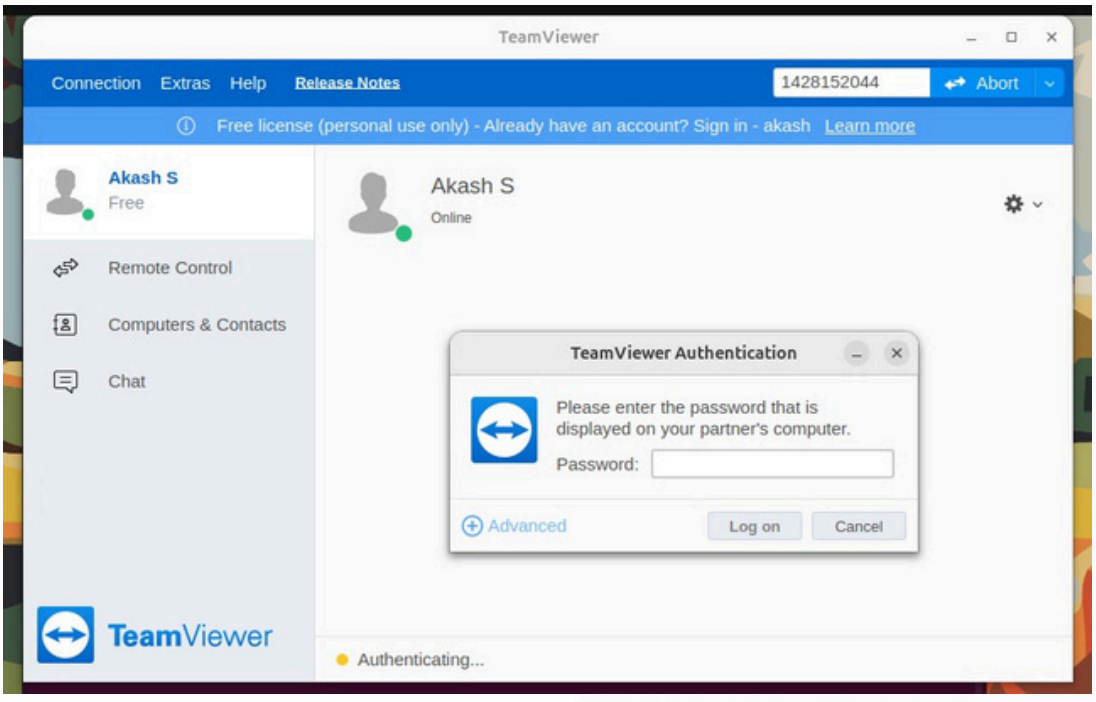
Implementation:

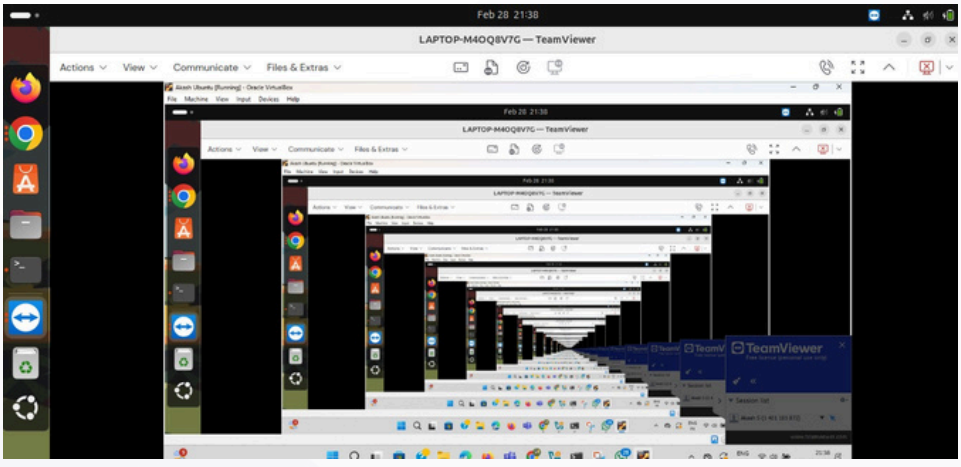
(I) Installation:

(II) Connection:

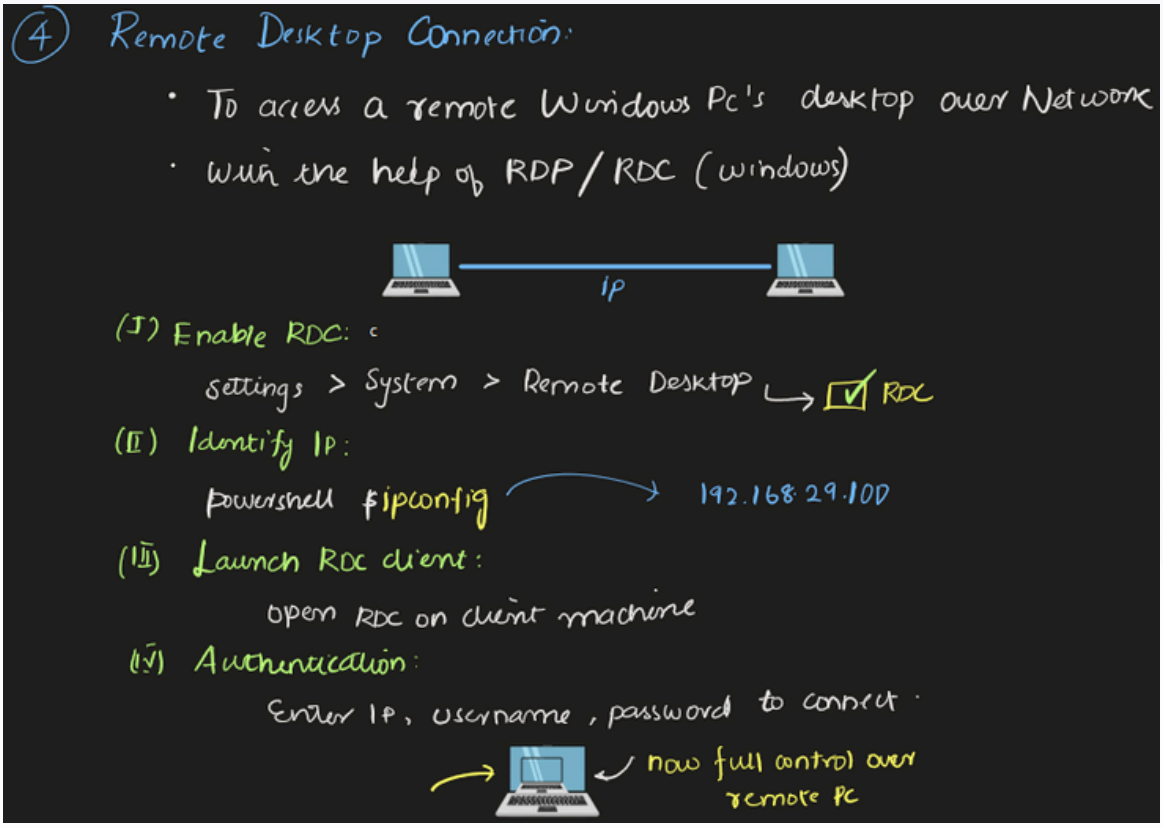
Speciality?

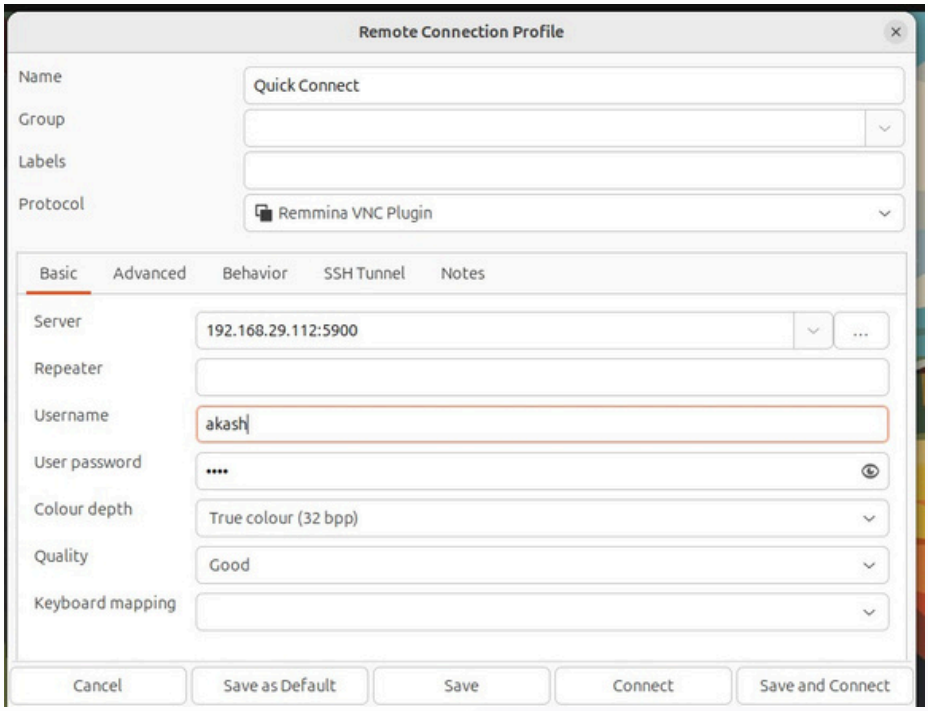
- Secure (because it utilises both ID & password)
- Easier team collaboration with a shared password.

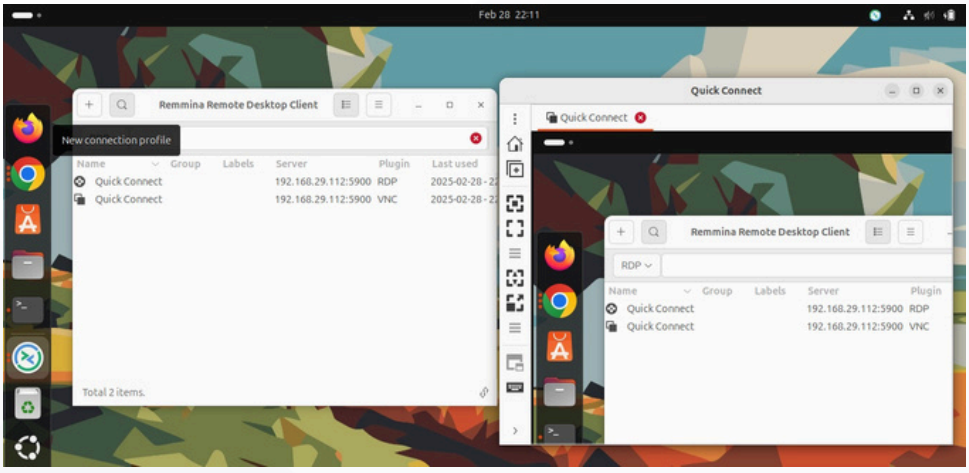




Remote Desktop Connection:



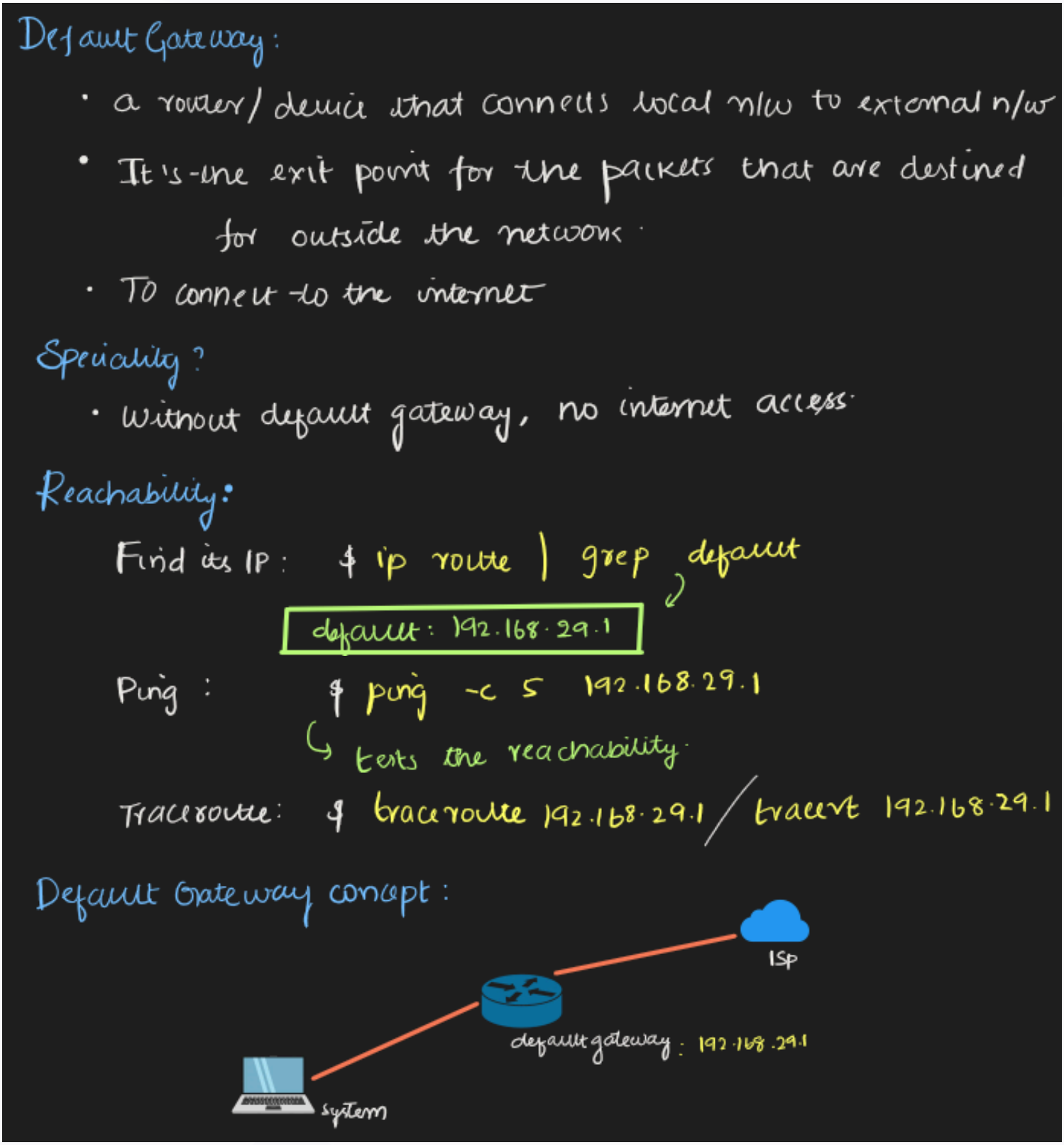




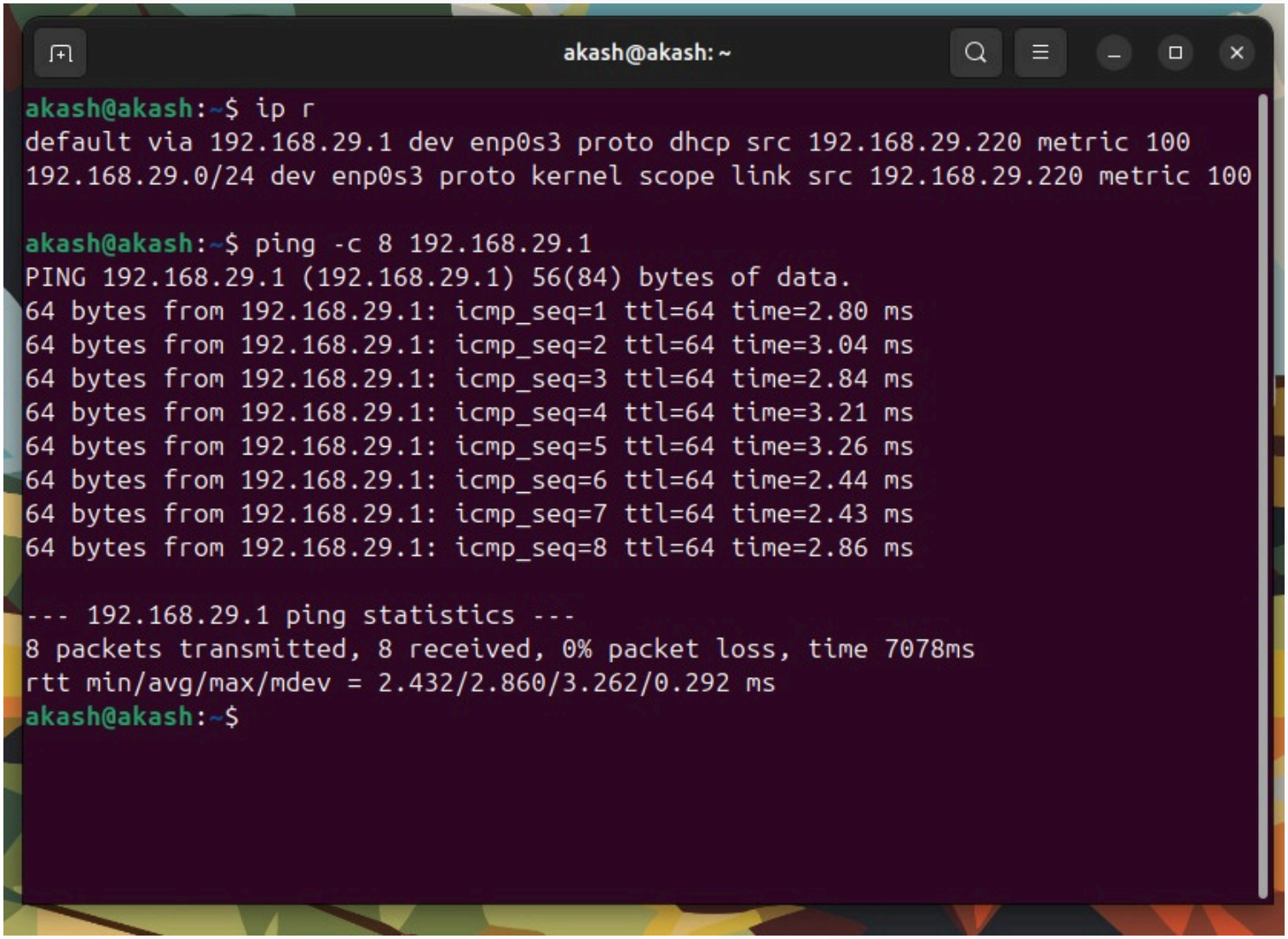
Task 7:

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

Explanation:



Output:

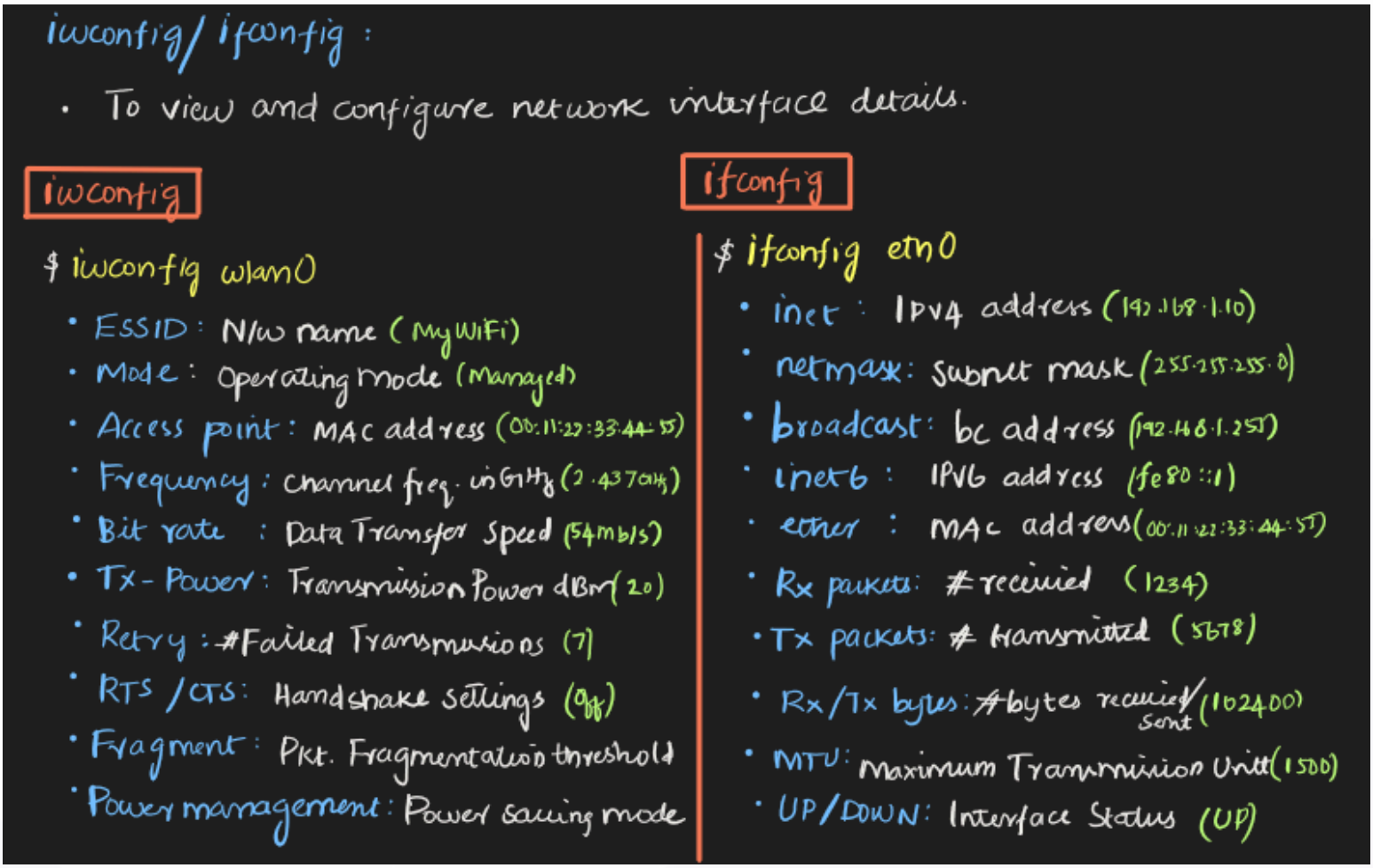


default gateway connectivity

Task 8:

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

Explanation:



Output:

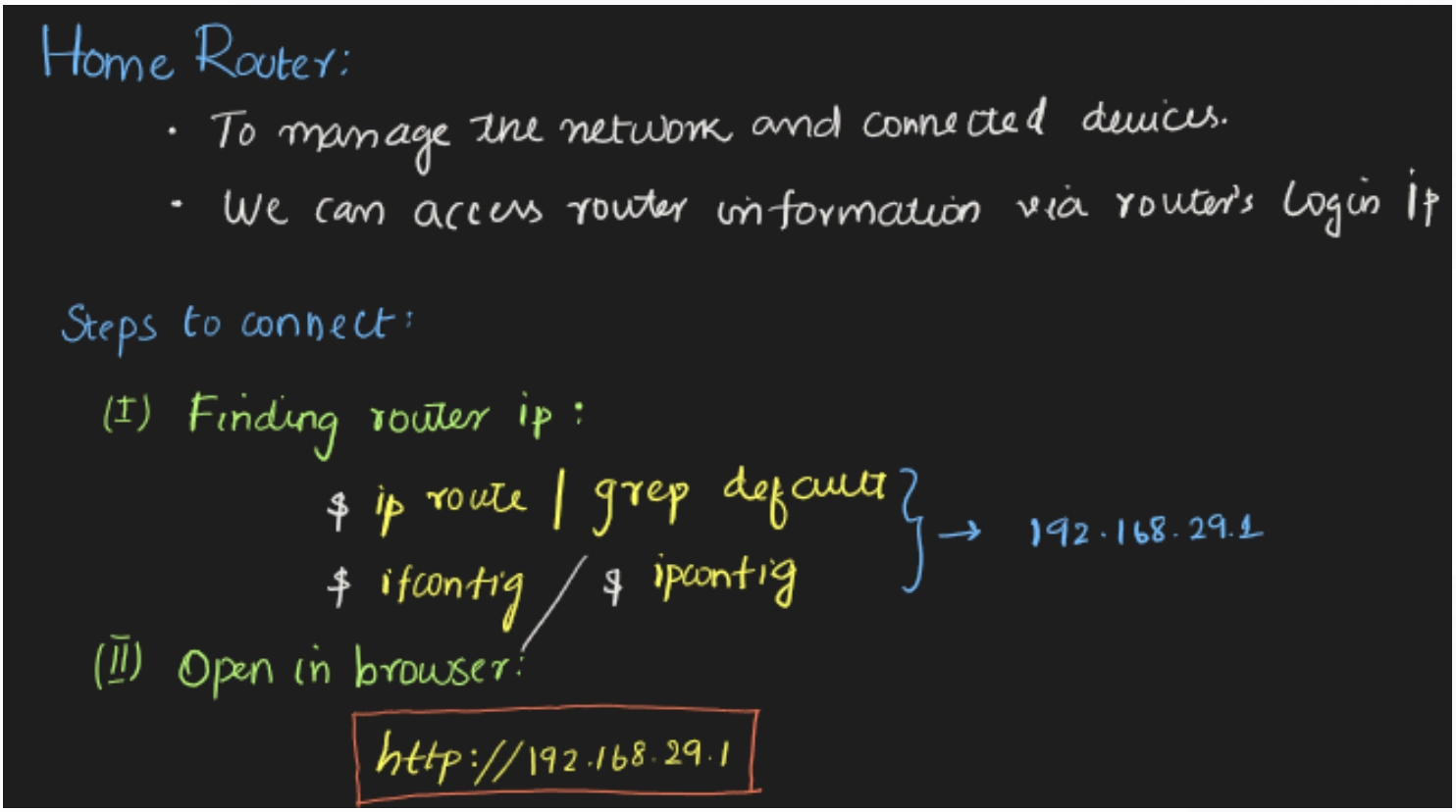
```
akash@akash: ~
akash@akash:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.29.220  netmask 255.255.255.0  broadcast 192.168.29.255
        inet6 fe80::a00:27ff:fe0e:cd8c  prefixlen 64  scopeid 0x20<link>
        inet6 2405:201:e04f:a81a:a00:27ff:fe0e:cd8c  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: ~
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:



(III) Login with username and password:

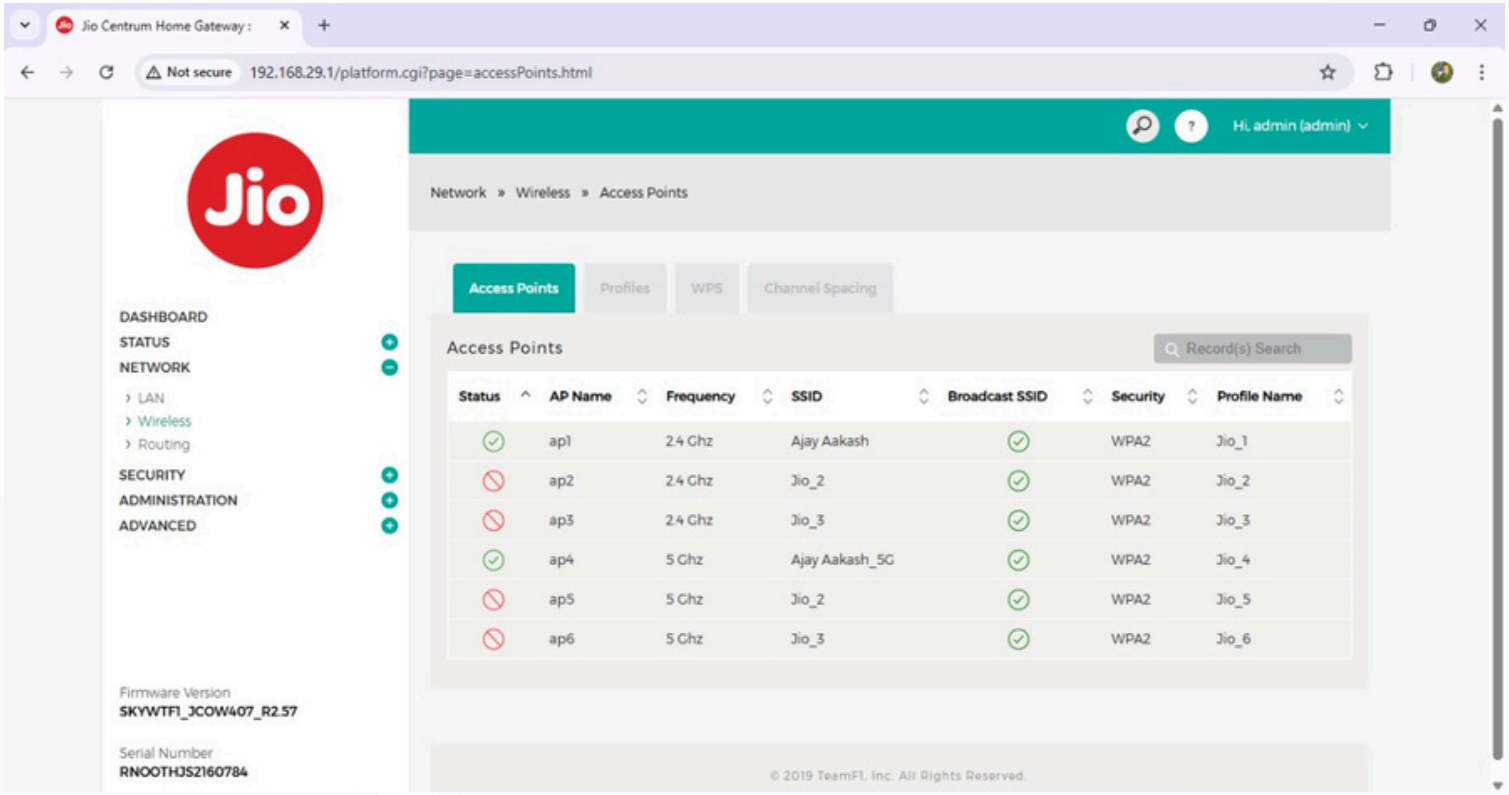
Username : akash

password : embedUR

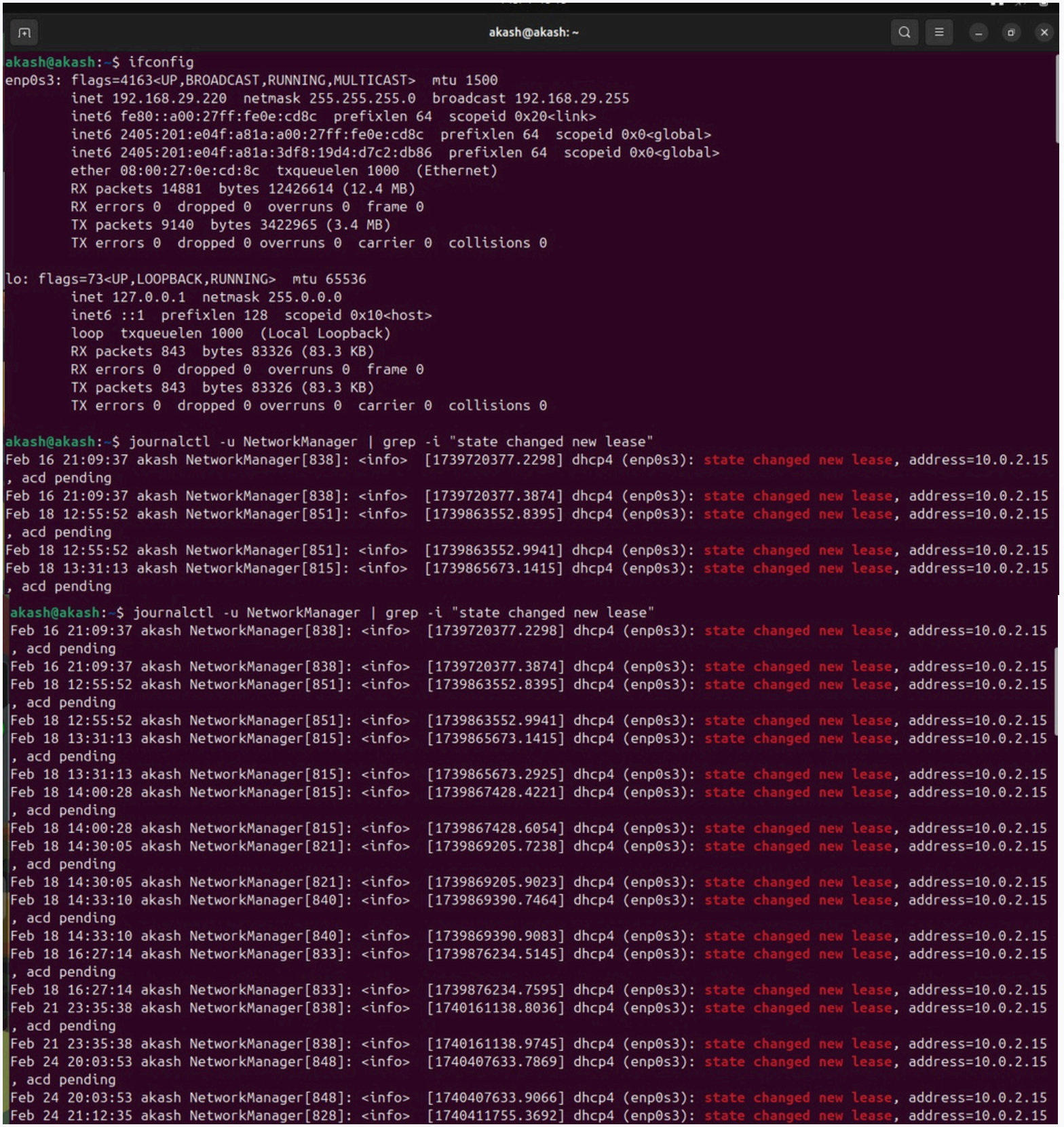
(IV) Checking connected devices:

Connected devices → LAN Status

WLAN Status



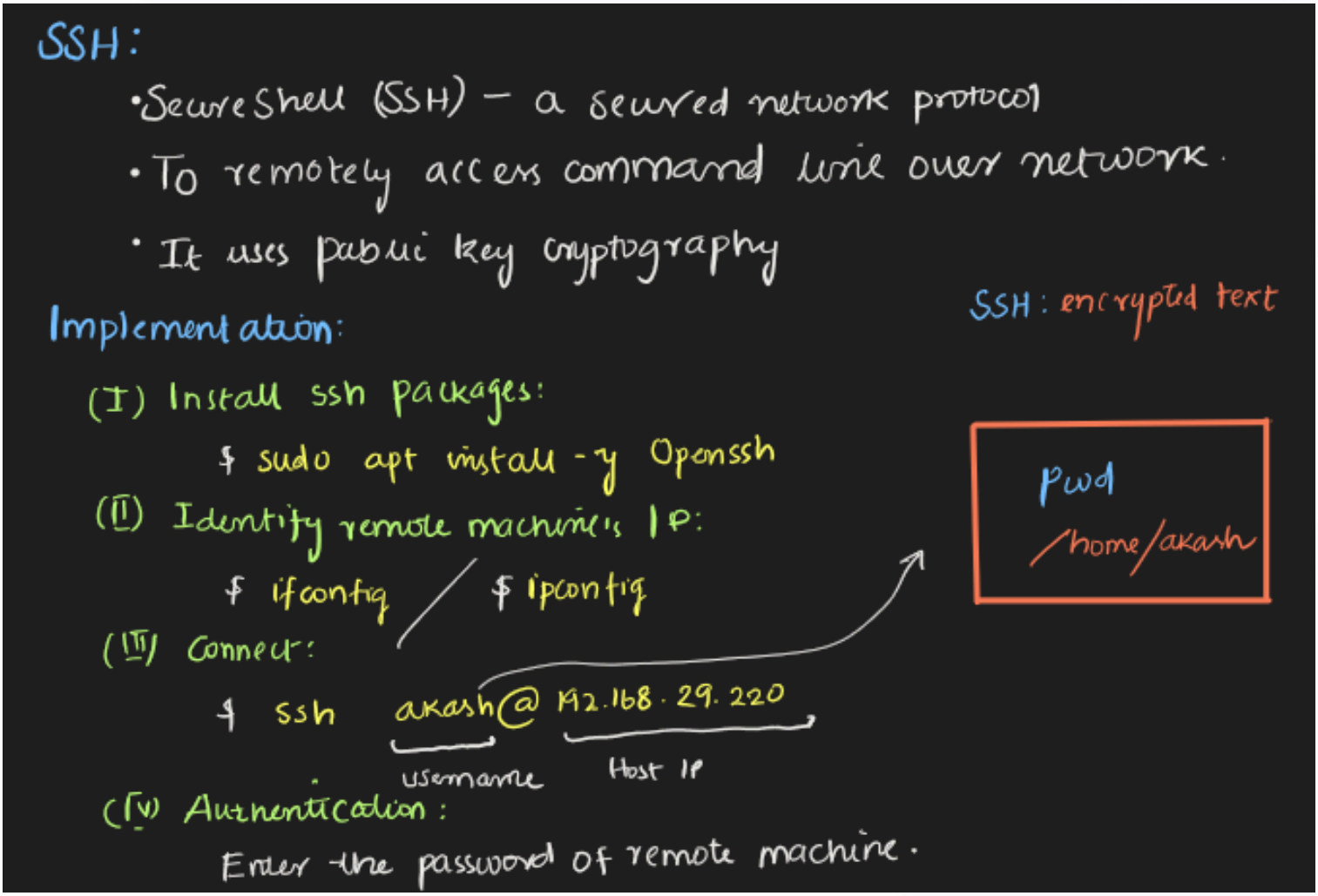
Output:

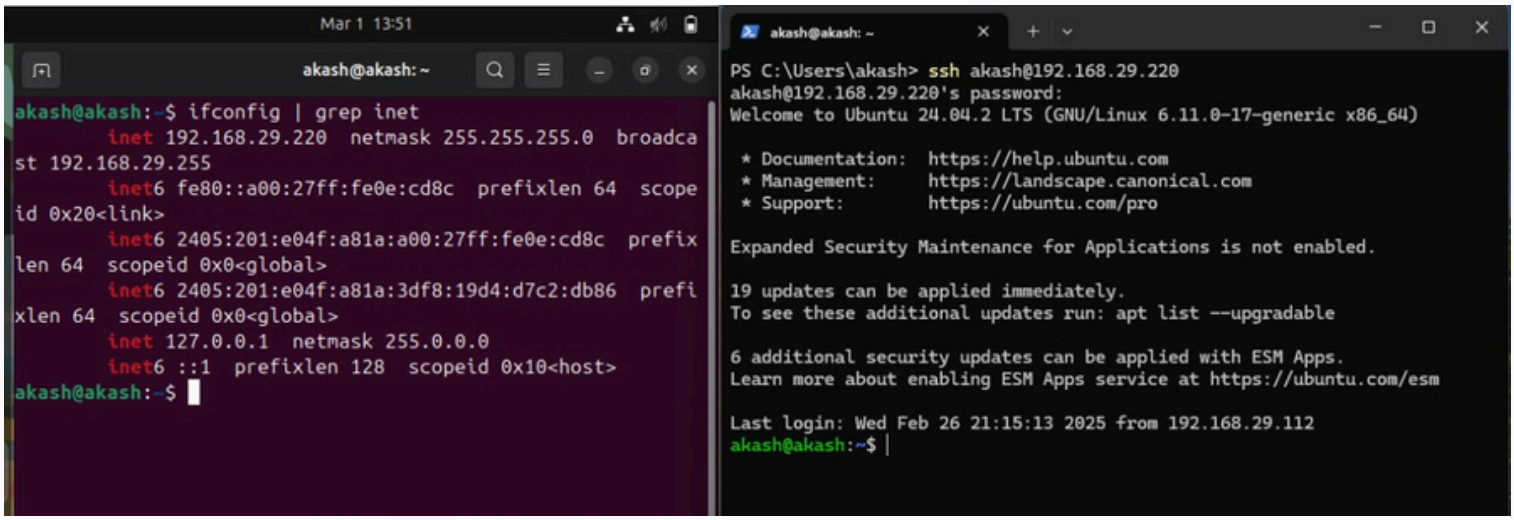

akash@akash: ~
akash@akash:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.29.220 netmask 255.255.255.0 broadcast 192.168.29.255
inet6 fe80::a00:27ff:fe0e:cd8c prefixlen 64 scopeid 0x20<link>
inet6 2405:201:e04f:a81a:a00:27ff:fe0e:cd8c prefixlen 64 scopeid 0x0<global>
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] dhcp4 (enp0s3): state changed new lease, address=10.0.2.15
, acd pending
Feb 16 21:09:37 akash NetworkManager[838]: <info> [1739720377.3874] dhcp4 (enp0s3): state changed new lease, address=10.0.2.15
Feb 18 12:55:52 akash NetworkManager[851]: <info> [1739863552.8395] dhcp4 (enp0s3): state changed new lease, address=10.0.2.15
, acd pending
Feb 18 12:55:52 akash NetworkManager[851]: <info> [1739863552.9941] dhcp4 (enp0s3): state changed new lease, address=10.0.2.15
Feb 18 13:31:13 akash NetworkManager[815]: <info> [1739865673.1415] dhcp4 (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] dhcp4 (enp0s3): state changed new lease, address=10.0.2.15
, acd pending
Feb 16 21:09:37 akash NetworkManager[838]: <info> [1739720377.3874] dhcp4 (enp0s3): state changed new lease, address=10.0.2.15
Feb 18 12:55:52 akash NetworkManager[851]: <info> [1739863552.8395] dhcp4 (enp0s3): state changed new lease, address=10.0.2.15
, acd pending
Feb 18 12:55:52 akash NetworkManager[851]: <info> [1739863552.9941] dhcp4 (enp0s3): state changed new lease, address=10.0.2.15
Feb 18 13:31:13 akash NetworkManager[815]: <info> [1739865673.1415] dhcp4 (enp0s3): state changed new lease, address=10.0.2.15
, acd pending
Feb 18 13:31:13 akash NetworkManager[815]: <info> [1739865673.2925] dhcp4 (enp0s3): state changed new lease, address=10.0.2.15
Feb 18 14:00:28 akash NetworkManager[815]: <info> [1739867428.4221] dhcp4 (enp0s3): state changed new lease, address=10.0.2.15
, acd pending
Feb 18 14:00:28 akash NetworkManager[815]: <info> [1739867428.6054] dhcp4 (enp0s3): state changed new lease, address=10.0.2.15
Feb 18 14:30:05 akash NetworkManager[821]: <info> [1739869205.7238] dhcp4 (enp0s3): state changed new lease, address=10.0.2.15
, acd pending
Feb 18 14:30:05 akash NetworkManager[821]: <info> [1739869205.9023] dhcp4 (enp0s3): state changed new lease, address=10.0.2.15
Feb 18 14:33:10 akash NetworkManager[840]: <info> [1739869390.7464] dhcp4 (enp0s3): state changed new lease, address=10.0.2.15
, acd pending
Feb 18 14:33:10 akash NetworkManager[840]: <info> [1739869390.9083] dhcp4 (enp0s3): state changed new lease, address=10.0.2.15
Feb 18 16:27:14 akash NetworkManager[833]: <info> [1739876234.5145] dhcp4 (enp0s3): state changed new lease, address=10.0.2.15
, acd pending
Feb 18 16:27:14 akash NetworkManager[833]: <info> [1739876234.7595] dhcp4 (enp0s3): state changed new lease, address=10.0.2.15
Feb 21 23:35:38 akash NetworkManager[838]: <info> [1740161138.8036] dhcp4 (enp0s3): state changed new lease, address=10.0.2.15
, acd pending
Feb 21 23:35:38 akash NetworkManager[838]: <info> [1740161138.9745] dhcp4 (enp0s3): state changed new lease, address=10.0.2.15
Feb 24 20:03:53 akash NetworkManager[848]: <info> [1740407633.7869] dhcp4 (enp0s3): state changed new lease, address=10.0.2.15
, acd pending
Feb 24 20:03:53 akash NetworkManager[848]: <info> [1740407633.9066] dhcp4 (enp0s3): state changed new lease, address=10.0.2.15
Feb 24 21:12:35 akash NetworkManager[828]: <info> [1740411755.3692] dhcp4 (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 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:

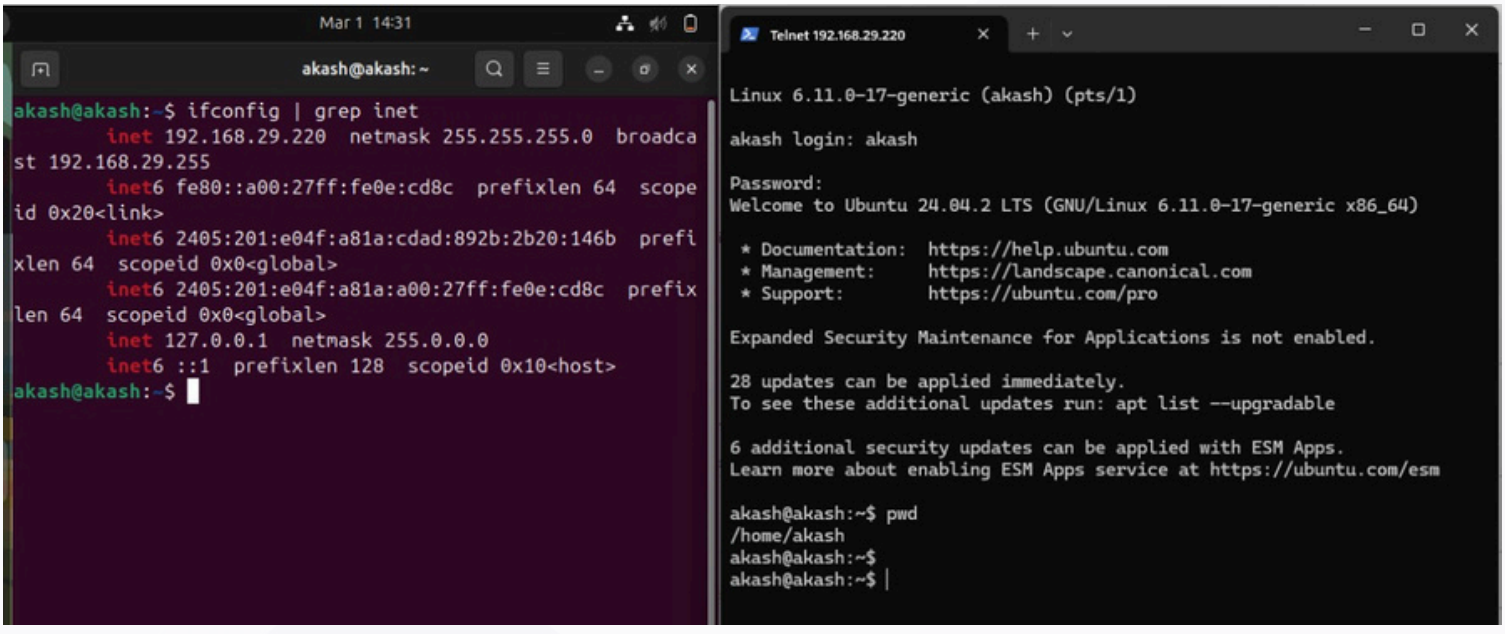
$ telnet 192.168.1.10 23

IP Port

(IV) Authentication

Enter username and password.

telnet: plaintext



THE END

AKASH S | embedUR Systems