Module 3 and 4 Assignment solutions

Sri Gnana Saravan.N

VIT Chennai

1.Simulate a small network with switches and multiple devices. Use ping to generate traffic and observe the MAC address table of the switch. Capture packets using Wireshark to anal Ethernet frames and MAC addressing.

Solution:

Pinging to generate traffic:

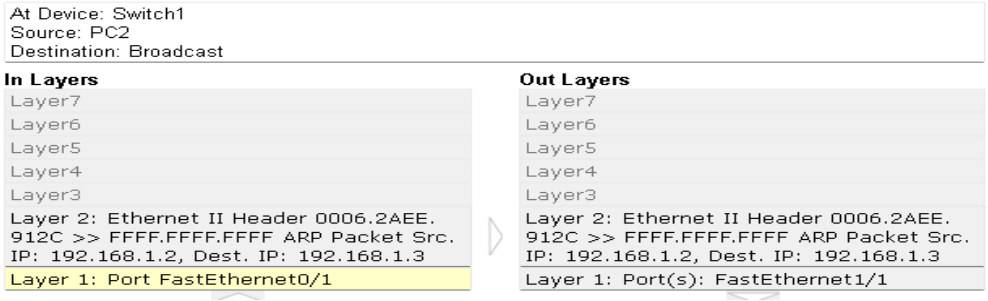
```
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=22ms TTL=128
Reply from 192.168.1.3: bytes=32 time=13ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 22ms, Average = 8ms
```

MAC Address Table:

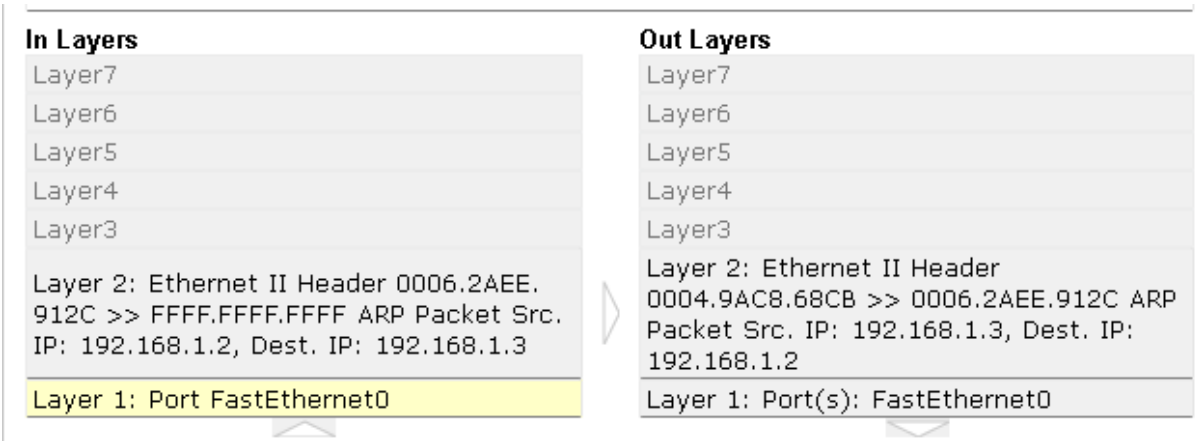
Example scenario where Switch only know about PC2 Address:

```
Switch#show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0004.9ac8.68cb    DYNAMIC     Fa1/1
```

Ethernet Frames:

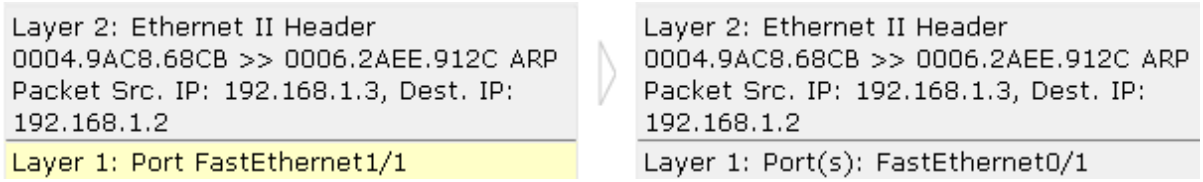


Here you can see that the Destination MAC Address is FFFF.FFFF.FFFF because it does'nt know about the other connected devices.When we try to ping to that particular system It learns the other devices MAC Address through ARP Protocol.Here the Switch will forward frames based on its mac address table.




Now after the frame passes to the switch,If the switch already learned the device MAC Address it will send to the respective device otherwise it will broadcast it.The Device which matches the Destination IP will respond with its MAC Address,so that switch will learn and update its MAC Table.

PC2 responds to the PC1 with its MAC Address:




Updated MAC Table of Switch:

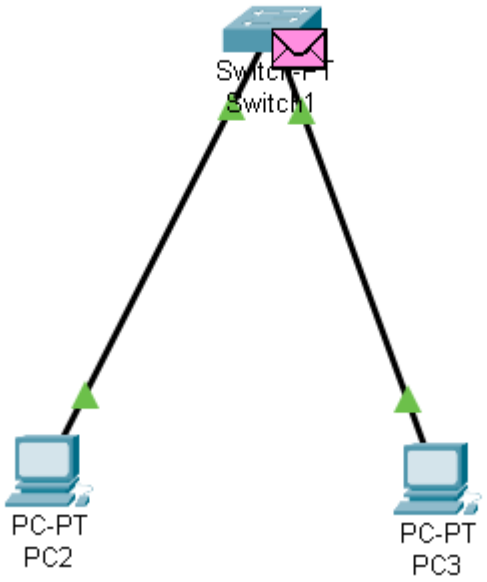
```
Switch#show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0004.9ac8.68cb    DYNAMIC     Fa1/1
   1    0006.2aee.912c    DYNAMIC     Fa0/1
```

2. Capture and analyze Ethernet frames using Wireshark, Inspect the structure Of the frame, including destination and source MAC addresses, Ethertype, payload, and FCS.

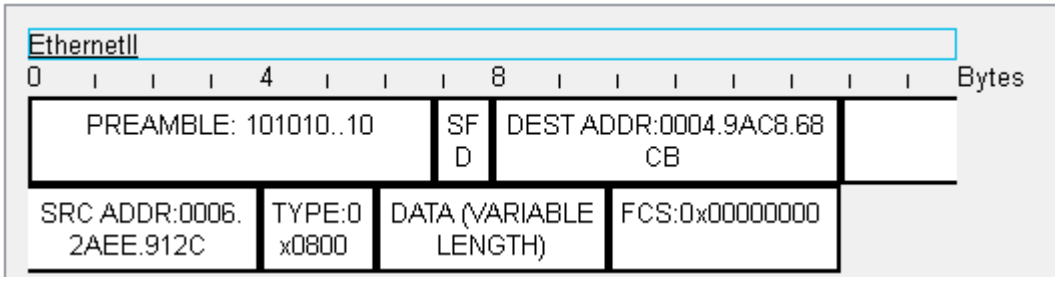
Use GNS3 or Packet Tracer to simulate network traffic.

Solution:

Simulating Network Traffic:




Ethernet Frame:




Here the Network is Simulated using Cisco Packet Tracer and the Frame is analyzed using Packet Tracer itself.

Here Preamble is totally 7 bytes,It is basically used for Synchronization of receiving devices.

SFD(Start Frame Delimiter) – It is 1byte to make the Start of the Ethernet Frame.

Destination MAC Address: It consists of 6 bytes to identify Receiving device's MAC Address.If it is FFFF.FFFF.FFFF then the message is broadcast.

Source MAC Address: It also consists of 6 bytes to identify sender MAC Address.

Type: Basically it protocol identifier .If it's 0x0800 Means its IPv4 Protocol.It says the payload contains IPv4 Packet So it should passes to IP stack.If its 0x0806 then its ARP request.

Data- It is variable length (46-1500 bytes).It contains IP Packets,TCP/UDP Segments,ARP Requests etc.

FCS – Frame Check Sequence.It consists of 4 bytes and it uses CRC for error detection.

3. Research the Linux kernel's handling of Ethernet devices and network interfaces. Write a short report on how the Linux kernel supports Ethernet communication (referencing kernel.org documentation).

Solution:

Step 1:

- The Linux Networking Stack treats the Ethernet devices as separate interfaces like enp0s3,enp0s6 and these interfaces are exposed to user space application to access it via the network subsystem.In linux it will be in /dev/net/
- When the ethernet is plugged in,it will register the device using register API's

Step 2:

- Let's say if we are try to ping to another PC which is connected via Ethernet.
- Now the network subsystem adds the appropriate packet headers according to the protocol.Example it will add the IP header and all other headers.
- It uses Queue Data structure to systematically control the traffic.
- Now before it goes into the hardware layer,Ethernet driver file converts the packet into ethernet frame it will add its frame bits like Preamble,SFD,Source and Destination MAC Address etc..
- After that it sends the frame to NIC using DMA.
- NIC Hardware transfers the frame onto the network.

Step 3:

- In the receiving end,NIC Receives the Ethernet frame,the driver code will place the received frame in the sk_buff(Socket buffer).
- It checks the MAC Address from the frame to check whether the frame belongs to the system.
- After removing  the ethernet frame,it will route the packet to the Upper layer (IP Layer)
- After that User space application reads the data from that socket data structure.

4. Configure static IP addresses, modify MAC addresses, and verify network connectivity using ping and ifconfig commands.

Solution:

Static IP Configuration:

Instead of DHCP,We can statically add our System IP using the sudo ip addr add command,but after reboot it will be restored to the normal dhcp ip.

```
saravan@saravan-VirtualBox:~/Desktop$ sudo ip addr add 192.168.29.10/24 dev enp0
s8
saravan@saravan-VirtualBox:~/Desktop$ sudo ip link set enp0s8 up
saravan@saravan-VirtualBox:~/Desktop$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        ether 08:00:27:e1:52:52  txqueuelen 1000  (Ethernet)
        RX packets 1928  bytes 514102 (514.1 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 467  bytes 49028 (49.0 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.29.10  netmask 255.255.255.0  broadcast 0.0.0.0
        ether 08:00:27:0b:50:db  txqueuelen 1000  (Ethernet)
        RX packets 1619  bytes 126970 (126.9 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 127  bytes 11127 (11.1 KB)
        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)
```

After adding it manually we need to tell the default gateway,so that we can connect to the network.sudo ip route add default via [Our default gateway ip addr].

```
saravan@saravan-VirtualBox:~/Desktop$ sudo ip route add default via 192.168.29.1
saravan@saravan-VirtualBox:~/Desktop$
saravan@saravan-VirtualBox:~/Desktop$ ping www.google.com
PING www.google.com (142.250.192.164) 56(84) bytes of data.
64 bytes from del11s11-in-f4.1e100.net (142.250.192.164): icmp_seq=1 ttl=112 tim
e=53.7 ms
64 bytes from del11s11-in-f4.1e100.net (142.250.192.164): icmp_seq=2 ttl=112 tim
e=45.2 ms
64 bytes from del11s11-in-f4.1e100.net (142.250.192.164): icmp_seq=3 ttl=112 tim
e=47.8 ms
64 bytes from del11s11-in-f4.1e100.net (142.250.192.164): icmp_seq=4 ttl=112 tim
e=46.8 ms
64 bytes from del11s11-in-f4.1e100.net (142.250.192.164): icmp_seq=5 ttl=112 tim
e=46.7 ms
64 bytes from del11s11-in-f4.1e100.net (142.250.192.164): icmp_seq=6 ttl=112 tim
e=104 ms
^C
--- www.google.com ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5036ms
rtt min/avg/max/mdev = 45.234/57.431/104.240/21.103 ms
saravan@saravan-VirtualBox:~/Desktop$
```

MAC Address changing:

We can change the MAC Address of our system by installing macchanger package and type the command sudo macchanger -m [Your desired MAC address] [Interface name].You can revert it back using sudo macchanger -p [Interface name]

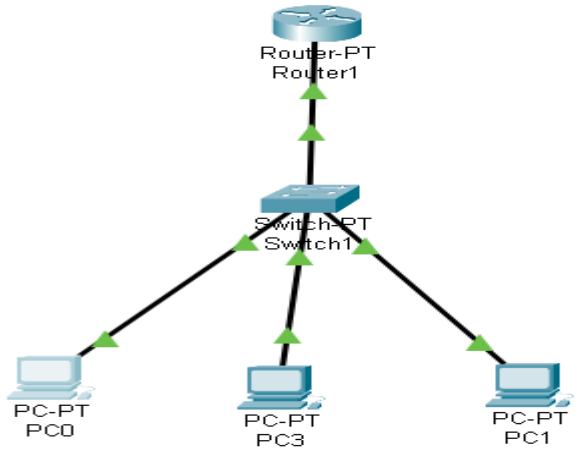
```
saravan@saravan-VirtualBox:~/Desktop$ sudo macchanger -p enp0s8
Current MAC:   78:e3:7d:f8:a3:e5 (unknown)
Permanent MAC: 08:00:27:0b:50:db (CADMUS COMPUTER SYSTEMS)
New MAC:       08:00:27:0b:50:db (CADMUS COMPUTER SYSTEMS)
```

But, Since MAC addresses are unique and hard-coded on network interface controller (NIC) cards, when the client wants to connect a new device or change an existing one, the ISP will detect different MAC addresses and might not grant Internet access to those new devices.

5. Troubleshoot Ethernet Communication with ping and traceroute -> Using cisco packet

Tracer.

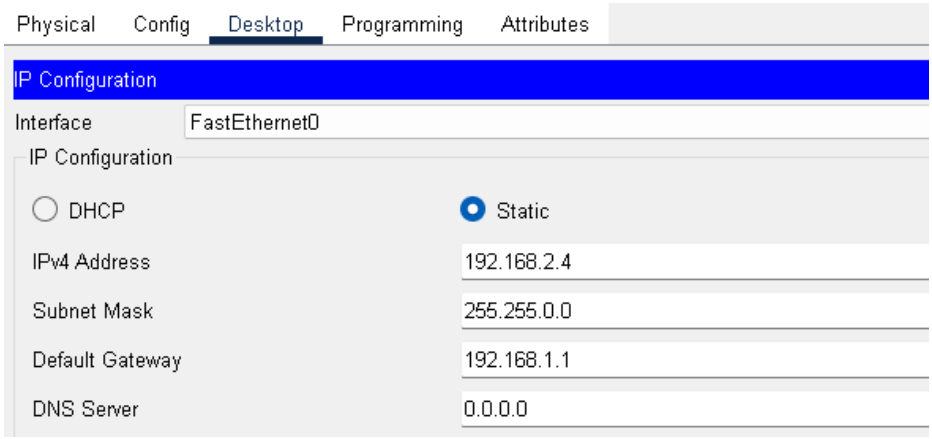
Solution:




Successful Ping:

```
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time=44ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 44ms, Average = 11ms
```

If IPs of PC are misconfigured or Subnet is misconfigured then the ping will fail.Here you can see that there is misconfiguration of IP Addresses and Subnet Mask.So that ping will fail.




```
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

tracert command:

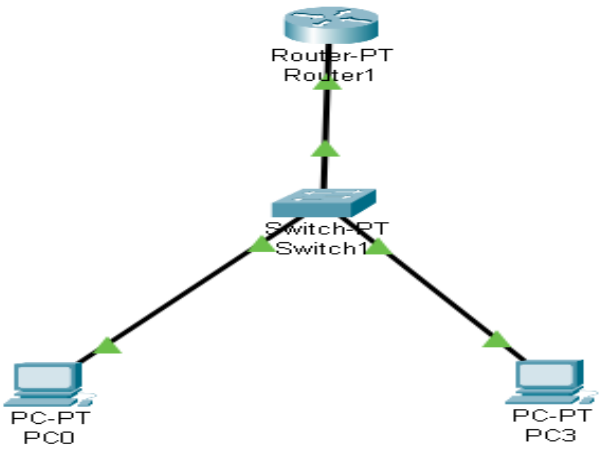
```
C:\>tracert 192.168.1.3

Tracing route to 192.168.1.3 over a maximum of 30 hops:

  1    0 ms       1 ms       0 ms       192.168.1.3

Trace complete.
```

It will tell how many hops that the packet is experiencing while transmitting the message and the hop count is equal to the no of devices that is in between the sender and receiver.Here it is one because only switch is in between the PC ‘s.

6. Create a simple LAN setup with two Linux machines connected via a switch.

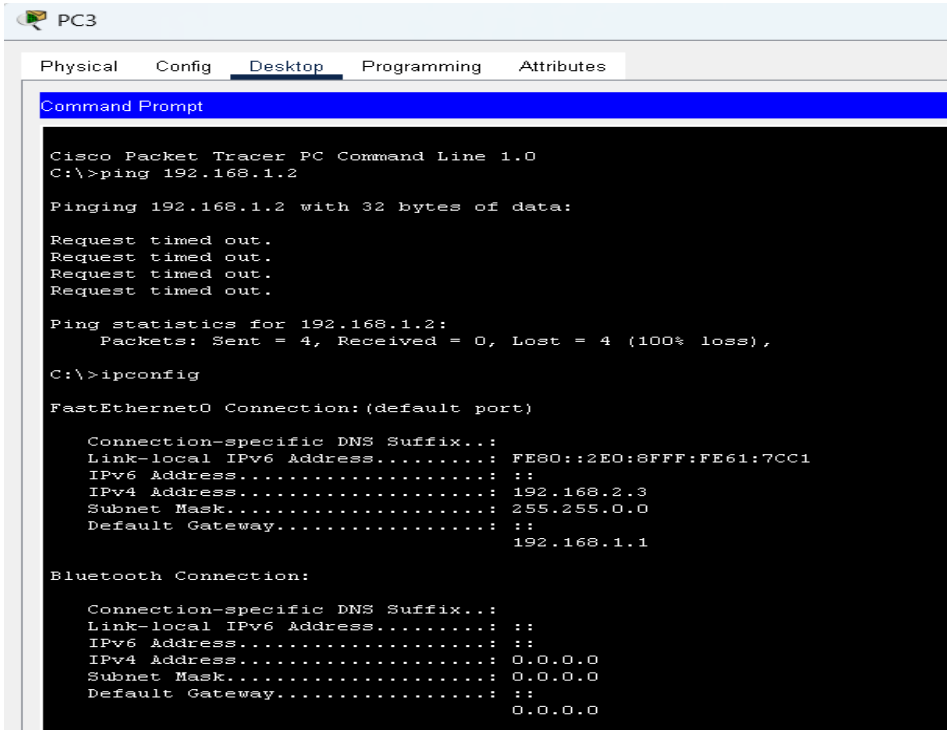
Solution:

Here the Two PC’s are viewed as two Linux Machines.

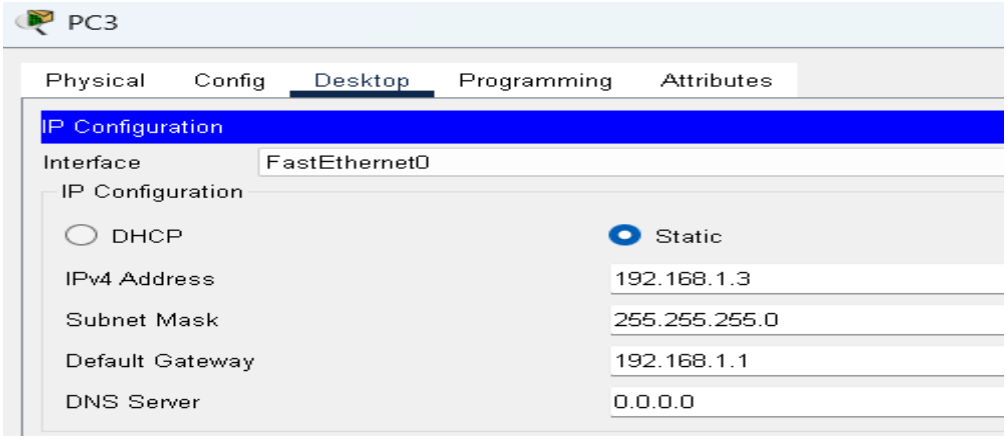



7. Ping from one machine to the other. If it fails, use ifconfig to ensure the IP addresses are configured correctly.

Solution:




Here Pinging from PC3 to PC1 fails,So I checked the IP addresses of the PC and it can be seen that IP address are misconfigured.So go to IP settings and change the IP address and check it again.Trouvleshooting via ping and tracert commands.

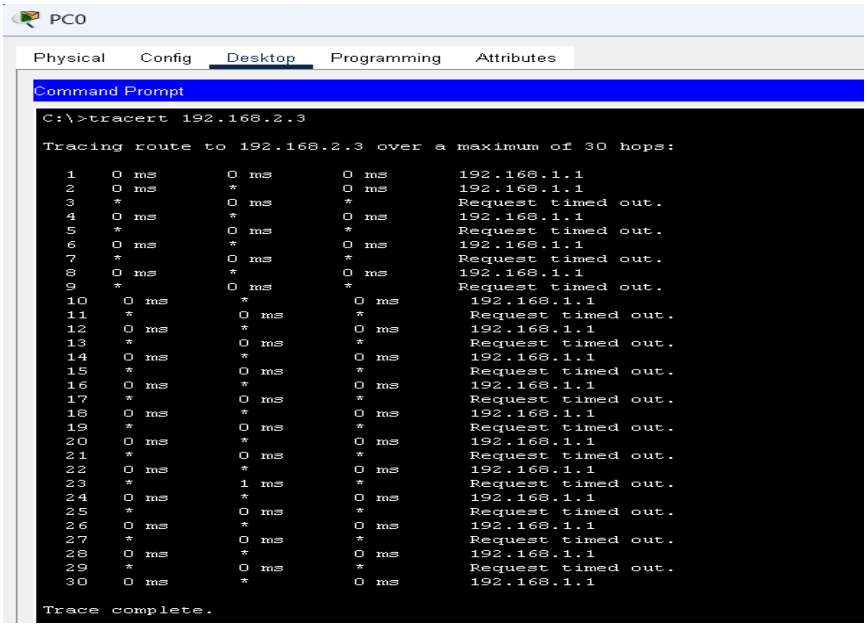



```
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time=9ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time=7ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 9ms, Average = 4ms
```

8.Use traceroute to identify where the packets are being dropped if the ping fails.

Solution:

After ping fails,try to trace the route where it getting failed and it is going to the router(Default Gateway successfully) but from router to the PC the packet is getting lost.It can be captured using the tracert command.



9. Describe how you would configure a basic LAN interface using the ip command in Linux (kernel.org).

Solution:

To configure a basic LAN interface in Linux we can use several commands.

Step 1:

ip link show ---->It will list out all the network interfaces and also it will show whether the state of the link is up or down.If it is down we can't able to connect to the network.

Step 2:

sudo ip addr add [your desired ip address] dev [your network interface name]

sudo ip addr add 192.168.1.5/24 dev enp0s3

It will add the IP address statically

Step 3:

Also we can use

sudo dhclient enp0s3 ----->To dynamically assign the IP address using DHCP Client.

Step 4:

If we assigned statically,then we need to tell the interface which route to follow to connect to the network.So we will configure default gateway ip address to connect to the internet.

sudo ip route add default via 192.168.1.1

Step 5:

We need to set the link up to get connect to internet

sudo ip link set enp0s3 up------>It will set the state of the link up.

sudo ip link set enp0s3 down------>It will set the state of the link down.

10. Use Linux to view the MAC address table of a switch (if using a Linux-based network switch). Use the bridge or ip link commands to inspect the MAC table and demonstrate a basic switch's operation.

Solution:

We can use sudo ip link show command to see the MAC addresses of all the interfaces and also the state of the interface.Using bridge fdb show command we can see the MAC address table(Switch forwarding table).Switch will receive the Sender packet,first it will see the

Source MAC if it’s not in the MAC table,it will add the Source MAC address.Next, it will see whether Destination MAC Address is in the forwarding table.If its in the Forwarding table,It will forward the packet to the respective port of the device,if it’s not the packet will be flooded to all the ports and It will get a reply from the matched MAC address device and it will add the respective MAC address of device’s port.