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 analyze Ethernet frames and MAC addressing.

Generating traffic in networking means creating data packets that travel across a network to test, monitor, or analyze network behavior. Traffic can be generated manually using commands like `ping` or automatically using specialized tools.

Purpose of Generating Traffic

- **Testing Connectivity:** Using `ping` to check if devices can communicate.
- **Measuring Performance:** Using `iperf` to test bandwidth and latency.
- **Analyzing Security:** Using `hping3` for penetration testing.
- **Troubleshooting Issues:** Identifying packet loss and network congestion.

How does the mac address table change before and after receiving ping?

1) Before Receiving a Ping (Initial State)

- If the switch is **newly powered on** or **cleared**, its MAC table may be **empty**.
- If the MAC table already has some **previously learned addresses**, it might contain **some device entries** but not all.

2) During Ping (Learning Phase)

Step 1: ARP Request (Address Resolution Protocol)

- If the source device **does not know** the MAC address of the destination, it sends an **ARP request**.
- The switch receives the ARP request and **records the source MAC address** in its MAC table.

Step 2: ARP Reply

- The destination device responds with its **MAC address**.
- The switch **learns** the destination MAC and updates the MAC table.

Step 3: ICMP Echo Request (Ping)

- Now, the source sends an **ICMP Echo Request (Ping)** using the learned MAC address.
- The switch forwards it based on its MAC table.

Step 4: ICMP Echo Reply (Ping Response)

- The destination sends an **ICMP Echo Reply**, confirming connectivity.

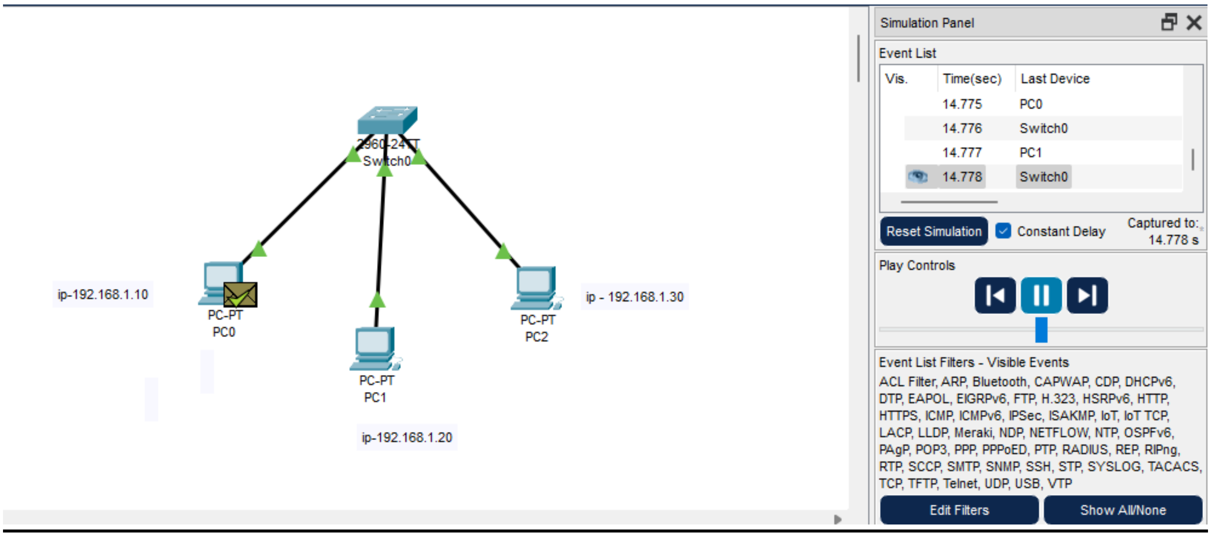
- The switch updates its MAC table if needed.

4. After Receiving a Ping (Updated MAC Table)

- The switch now has **both source and destination MAC addresses** recorded.
- Future communication between these devices **does not require broadcasting** (ARP requests), making traffic more efficient.

Implementation:

Network:



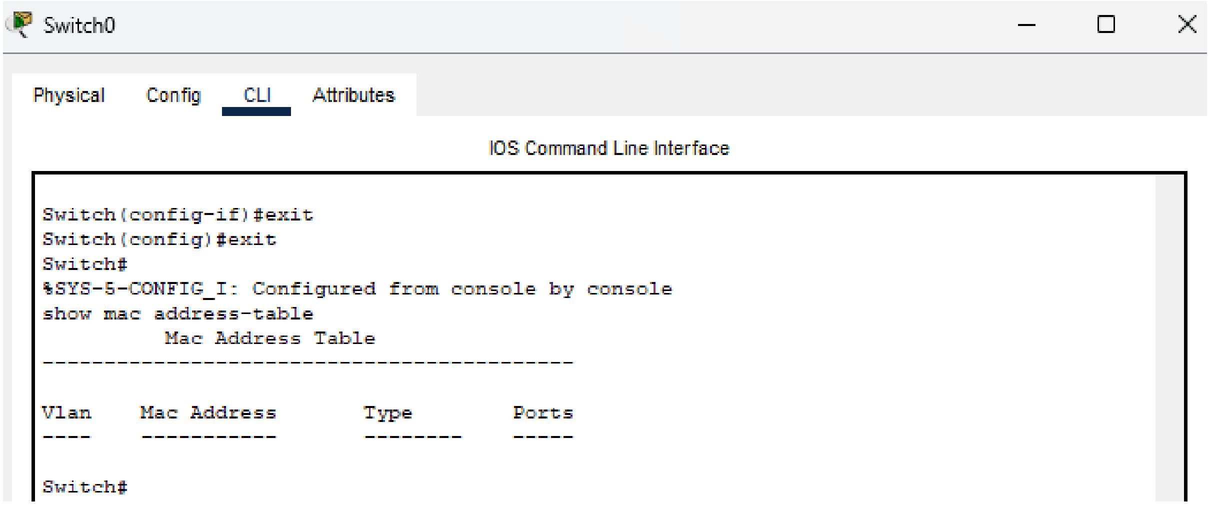
Vis.	Time(sec)	Last Device
	14.775	PC0
	14.776	Switch0
	14.777	PC1
	14.778	Switch0

Captured to:
14.778 s

Event List Filters - Visible Events
ACL Filter, ARP, Bluetooth, CAPWAP, CDP, DHCPv6, DTP, EAPOL, EIGRPv6, FTP, H.323, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, IoT, IoT TCP, LACP, LLDP, Meraki, NDP, NETFLOW, NTP, OSPFv6, PAgP, POP3, PPP, PPPoED, PTP, RADIUS, REP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, USB, VTP

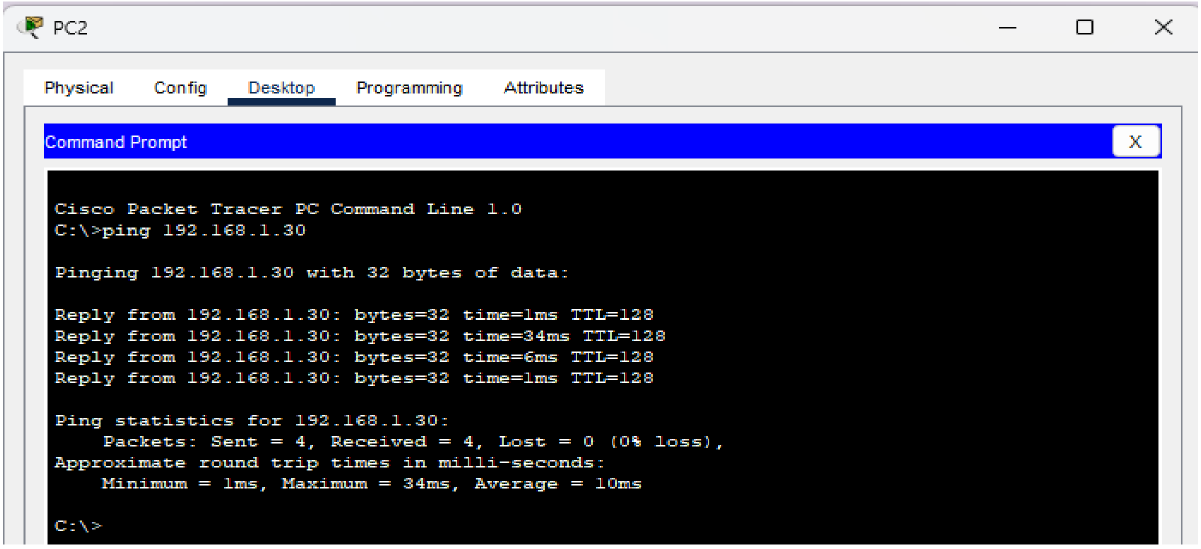
1.Before Pinging:

MAC address table of the switch:



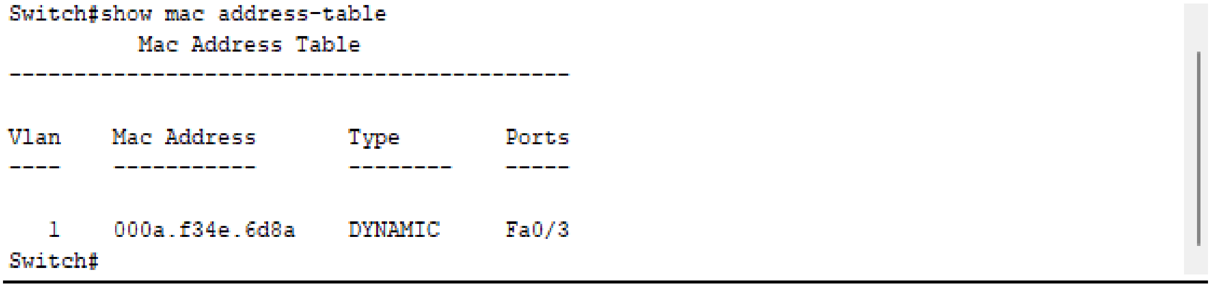
```
Switch(config-if)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console
show mac address-table
          Mac Address Table
-------------------------------------------

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

Switch#
```

2.After Pinging:



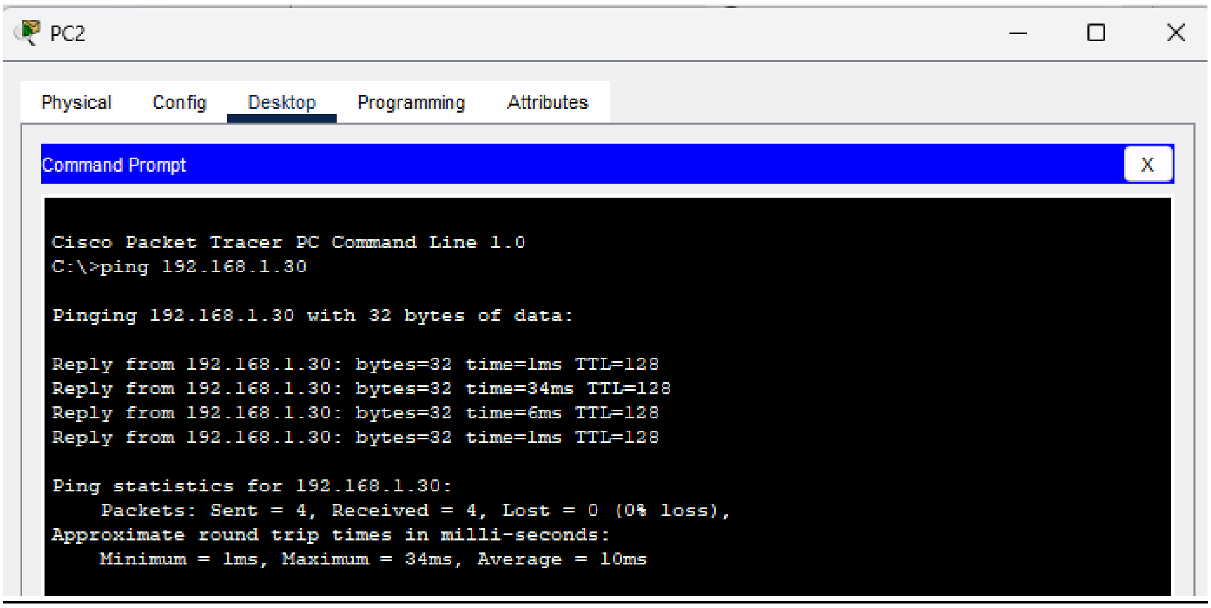
```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.30

Pinging 192.168.1.30 with 32 bytes of data:

Reply from 192.168.1.30: bytes=32 time=1ms TTL=128
Reply from 192.168.1.30: bytes=32 time=34ms TTL=128
Reply from 192.168.1.30: bytes=32 time=6ms TTL=128
Reply from 192.168.1.30: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.30:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 34ms, Average = 10ms

C:\>
```

After Pinging:MAC Address-table

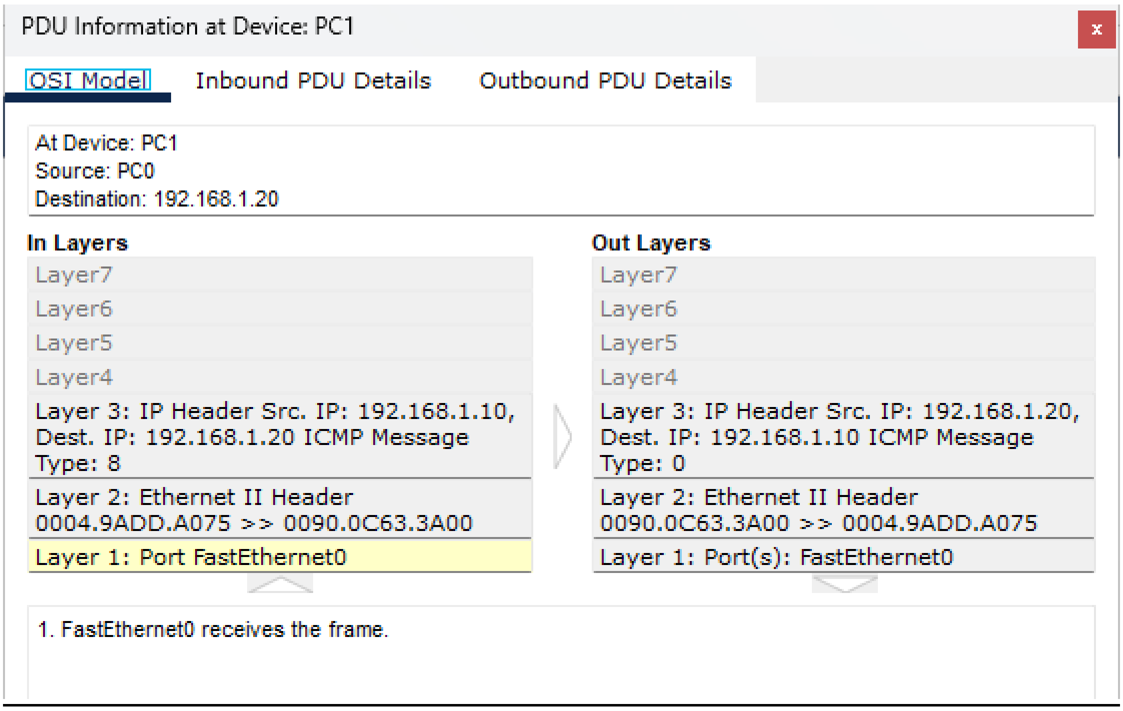


```
Switch#show mac address-table
          Mac Address Table
-------------------------------------------

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

   1    000a.f34e.6d8a    DYNAMIC     Fa0/3
Switch#
```

Capturing packets using Wireshark to analyze Ethernet frames and MAC addressing:



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.30

Pinging 192.168.1.30 with 32 bytes of data:

Reply from 192.168.1.30: bytes=32 time=1ms TTL=128
Reply from 192.168.1.30: bytes=32 time=34ms TTL=128
Reply from 192.168.1.30: bytes=32 time=6ms TTL=128
Reply from 192.168.1.30: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.30:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 34ms, Average = 10ms
```



PDU Information at Device: PC1

OSI Model | Inbound PDU Details | Outbound PDU Details

At Device: PC1
Source: PC0
Destination: 192.168.1.20

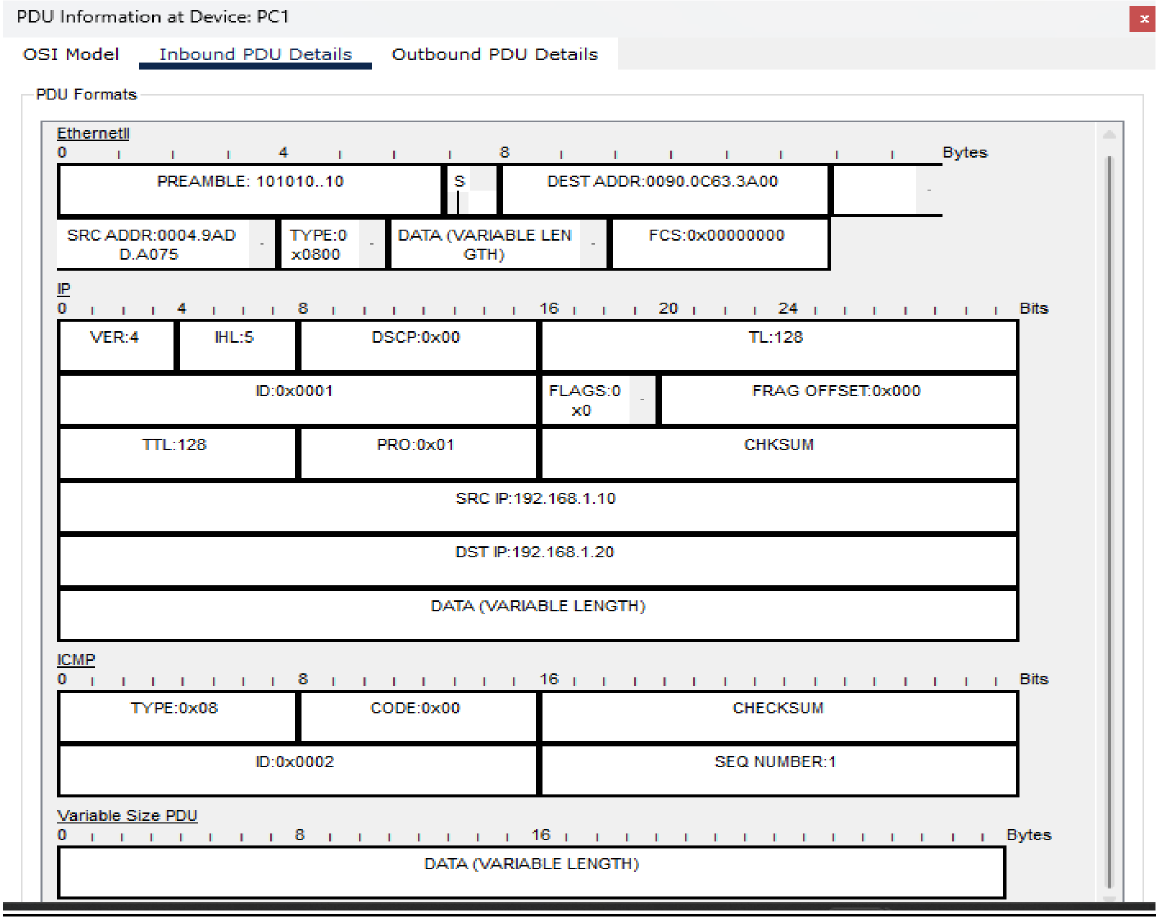
In Layers

Layer7
Layer6
Layer5
Layer4
Layer 3: IP Header Src. IP: 192.168.1.10, Dest. IP: 192.168.1.20 ICMP Message Type: 8
Layer 2: Ethernet II Header 0004.9ADD.A075 >> 0090.0C63.3A00
Layer 1: Port FastEthernet0

Out Layers

Layer7
Layer6
Layer5
Layer4
Layer 3: IP Header Src. IP: 192.168.1.20, Dest. IP: 192.168.1.10 ICMP Message Type: 0
Layer 2: Ethernet II Header 0090.0C63.3A00 >> 0004.9ADD.A075
Layer 1: Port(s): FastEthernet0

1. FastEthernet0 receives the frame.



PDU Information at Device: PC1

OSI Model | Inbound PDU Details | Outbound PDU Details

PDU Formats

EthernetII
0 4 8 Bytes
PREAMBLE: 101010..10 | S | DEST ADDR:0090.0C63.3A00
SRC ADDR:0004.9ADD.A075 | TYPE:0x0800 | DATA (VARIABLE LENGTH) | FCS:0x00000000

IP
0 4 8 16 20 24 Bits
VER:4 | IHL:5 | DSCP:0x00 | TL:128
ID:0x0001 | FLAGS:0x0 | FRAG OFFSET:0x000
TTL:128 | PRO:0x01 | CHKSUM
SRC IP:192.168.1.10
DST IP:192.168.1.20
DATA (VARIABLE LENGTH)

ICMP
0 8 16 Bits
TYPE:0x08 | CODE:0x00 | CHECKSUM
ID:0x0002 | SEQ NUMBER:1

Variable Size PDU
0 8 16 Bytes
DATA (VARIABLE LENGTH)

Analysis of PDU Information from Cisco Packet Tracer:

In Layers (Left Side) → Outbound Packet from PC0

- **Layer 3 (Network Layer - IP Header)**
  - **Source IP:** `192.168.1.10` (PC0)
  - **Destination IP:** `192.168.1.20` (PC1)
  - **ICMP Type:** `8` (Echo Request - "ping" request)
- **Layer 2 (Data Link Layer - Ethernet Header)**
  - **Source MAC Address:** `0004.9ADD.A075` (PC0's MAC)
  - **Destination MAC Address:** `0090.0C63.3A00` (PC1's MAC)
- **Layer 1 (Physical Layer)**
  - **Port:** `FastEthernet0`

This means **PC0 is sending an ICMP Echo Request ("ping") to PC1.**

Out Layers (Right Side) → Response Packet from PC1

- **Layer 3 (Network Layer - IP Header)**
  - **Source IP:** `192.168.1.20` (PC1)
  - **Destination IP:** `192.168.1.10` (PC0)
  - **ICMP Type:** `0` (Echo Reply - response to the ping)
- **Layer 2 (Data Link Layer - Ethernet Header)**
  - **Source MAC Address:** `0090.0C63.3A00` (PC1's MAC)
  - **Destination MAC Address:** `0004.9ADD.A075` (PC0's MAC)
- **Layer 1 (Physical Layer)**
  - **Port:** `FastEthernet0`

This means **PC1 is replying to PC0’s ping request with an ICMP Echo Reply.**