Week 9

Activity 1

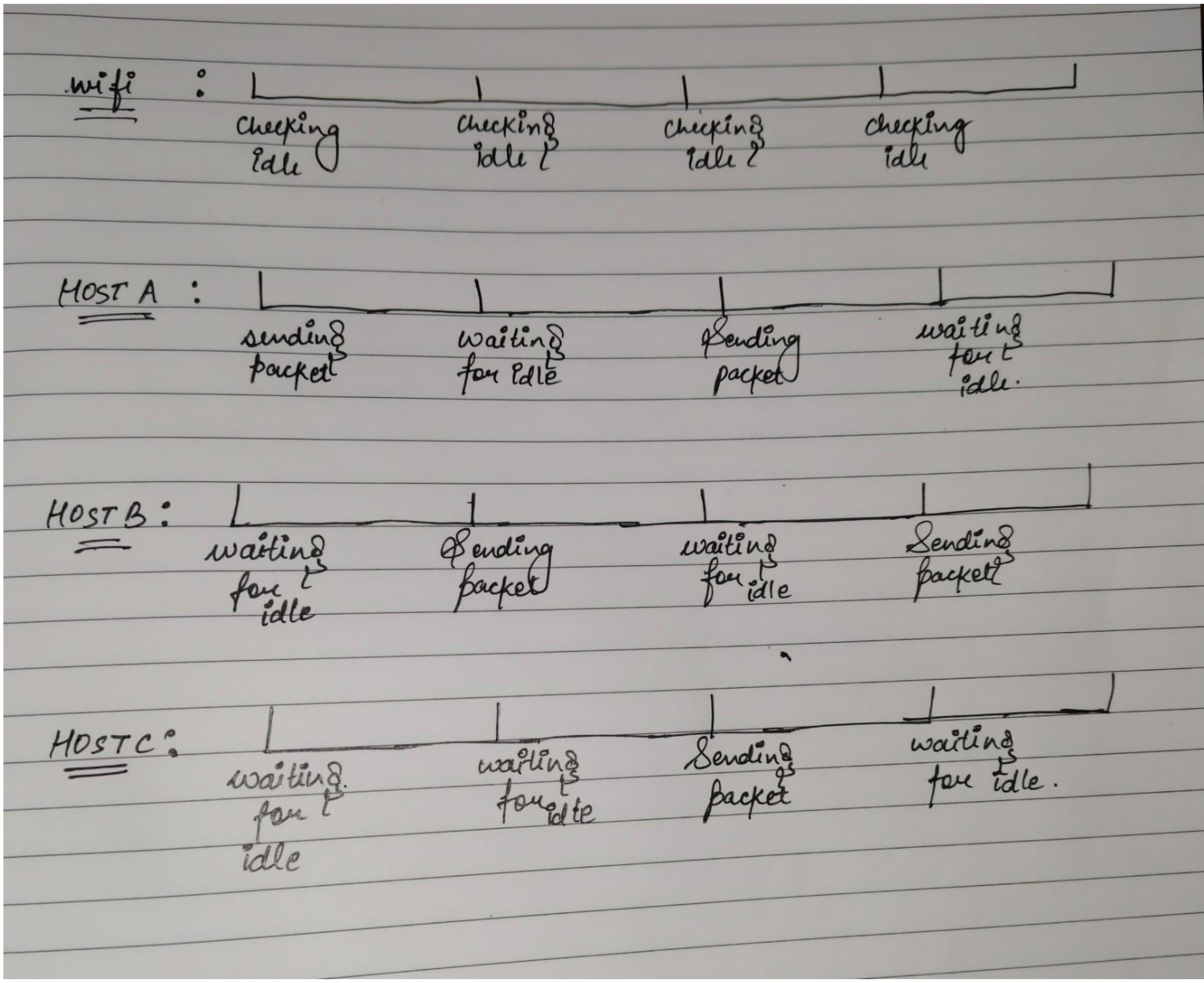
Group Members:

- **Archit**
- **Pranika**
- **Nadia**
- **Jasveena**
- **Gitanshi**

Role-Play Activity: Investigating MAC Protocol

1. **Scenario**:
    - **Archit**: Acts as the **Wi-Fi AP**.
    - **Pranika, Nadia, Jasveena, Gitanshi**: Each acts as **Host A, B, C** respectively.
2. **Protocol Design**:
    - **Archit (Wi-Fi AP)** checks whether the link is idle before any host can send a packet.
    - **Hosts A, B, C** will announce their intention to send a packet by saying, “I’m sending a packet!”
    - If more than one host attempts to send a packet simultaneously, a collision occurs. Both must back off and retry after a random delay.
3. **Collision Handling**:
    - If **Pranika (Host A)** and **Nadia (Host B)** attempt to send simultaneously, both will back off, wait for a random time, and retry.
4. **Timing Diagram**:
    - **Archit (Wi-Fi AP)** continually checks the idle state.
    - **Host A** attempts to send; if no collision, the packet is sent successfully.
    - **Host B** waits for the idle state, then attempts to send.

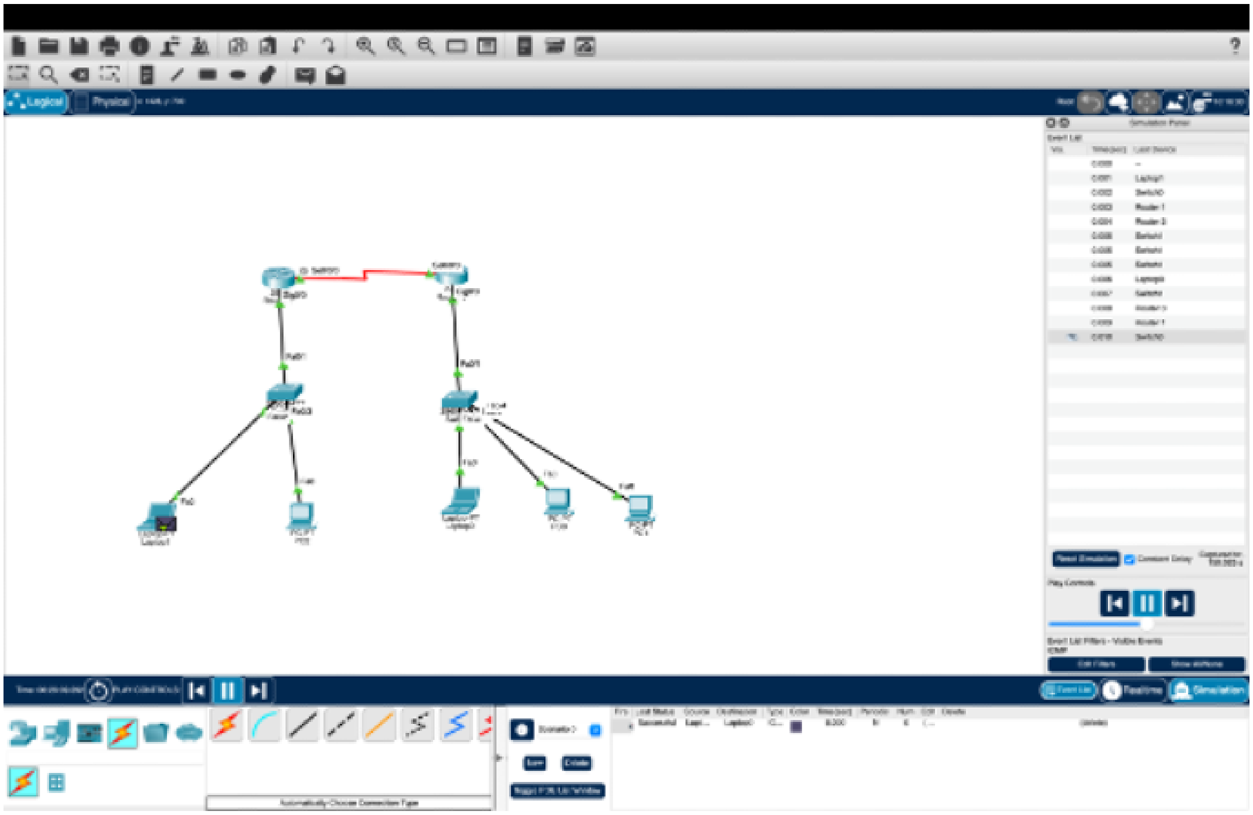
- ○ **Host C** checks and waits if the link is busy.



5. **Discussion**:

- ○ The **Medium Access Control (MAC) protocol** commonly used in Wi-Fi is **CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)**.
- ○ This protocol minimizes collisions by checking the channel's state and avoiding simultaneous transmissions.

Activity 2

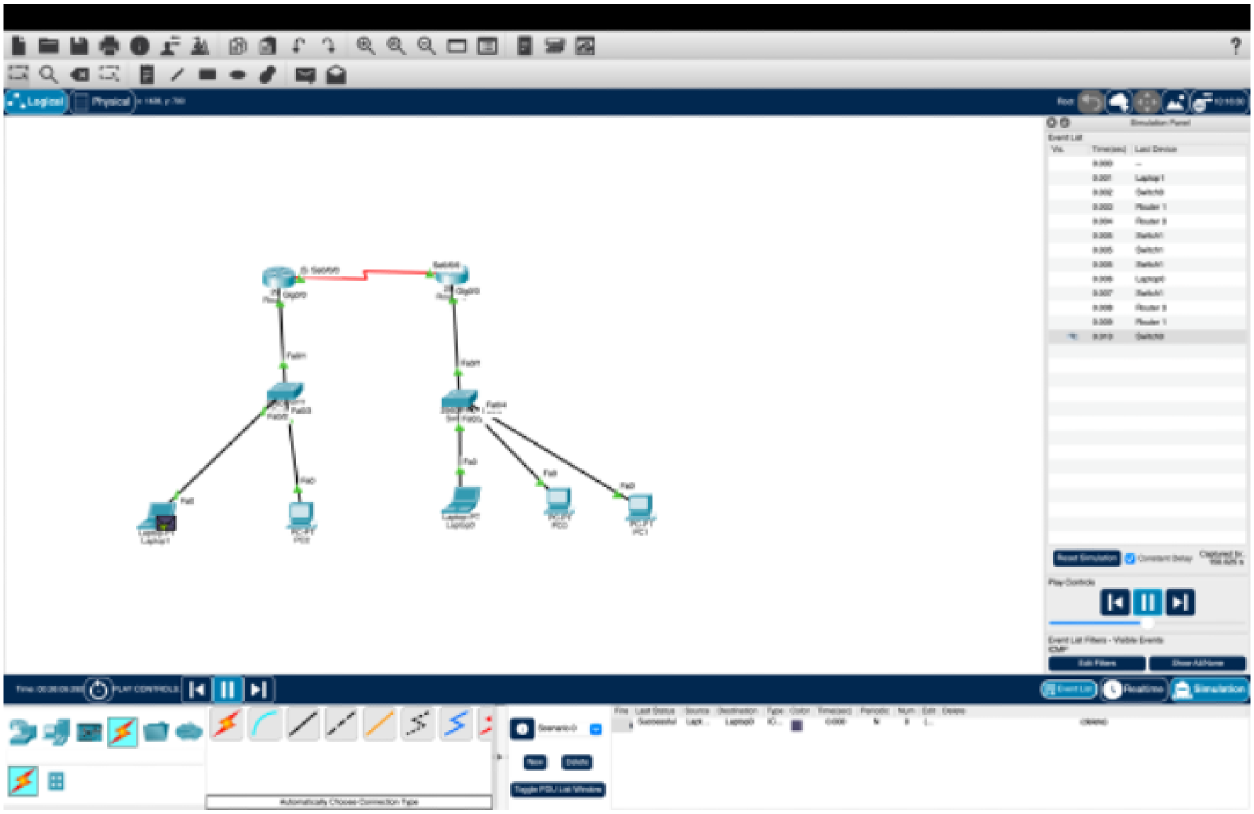


Simulation Panel

Event List

Vis.	Time(sec)	Last Device
	0.000	--
	0.001	Laptop1
	0.002	Switch0
	0.003	Router 1
	0.004	Router 0
	0.005	Switch1
	0.005	Switch1
	0.006	Switch1
	0.006	Laptop0
	0.007	Switch1
	0.008	Router 0
	0.009	Router 1
	0.010	Switch0

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
●	Successful	Lap...	Laptop0	IC...	■	0.000	N	0	(...	(delete)

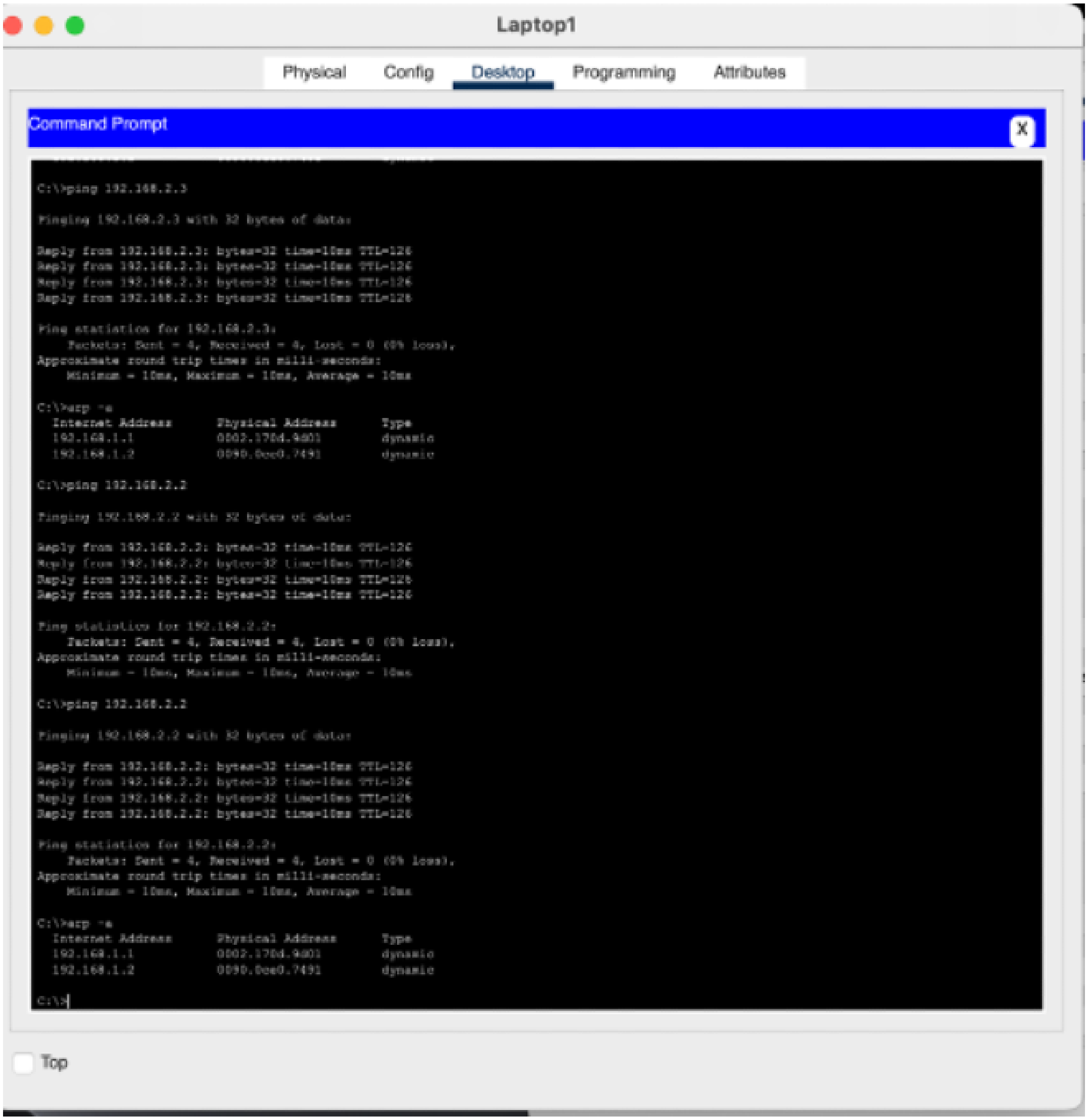


Simulation Panel

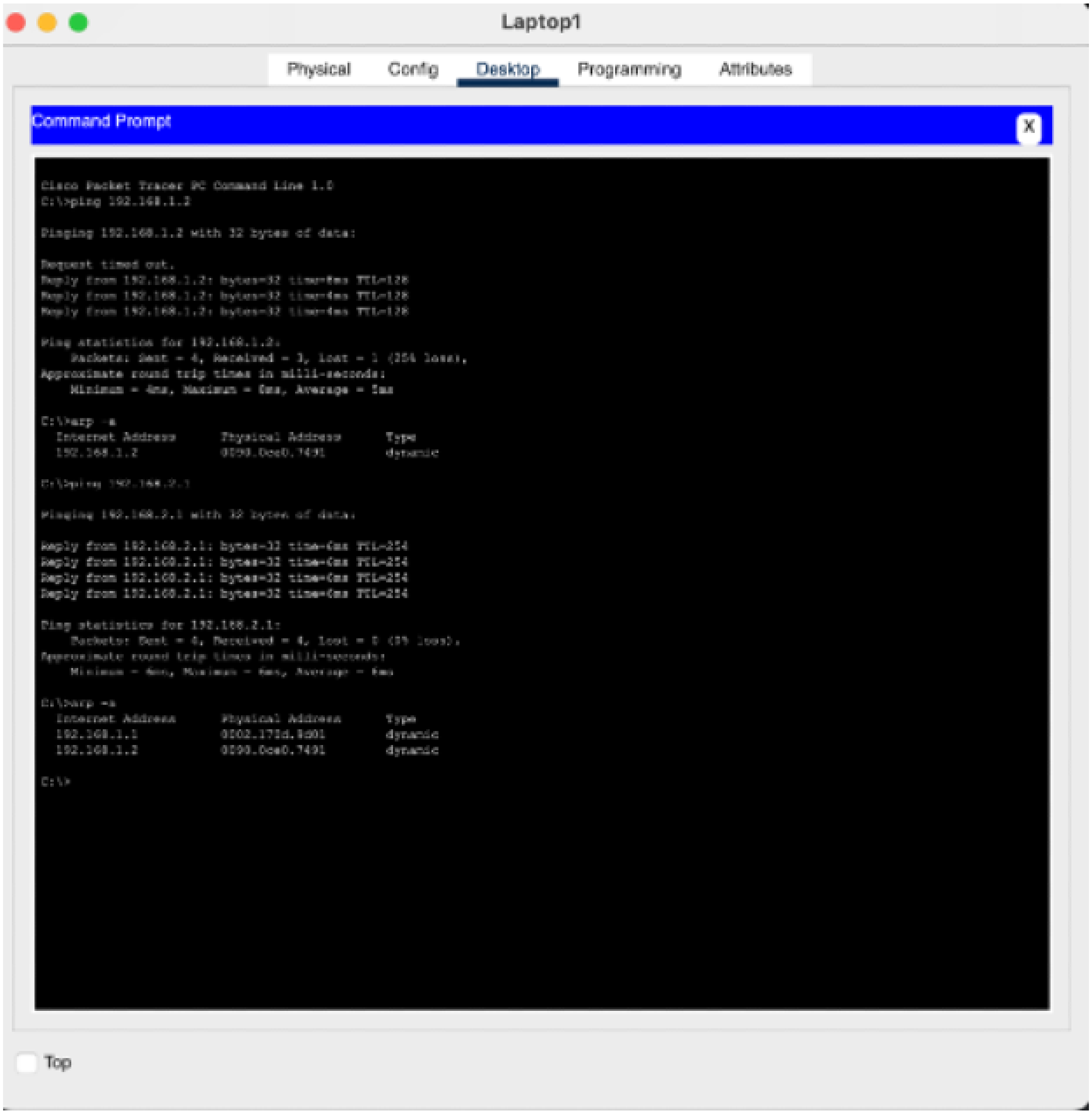
Event List

Vis.	Time(sec)	Last Device
	0.000	--
	0.001	Laptop1
	0.002	Switch0
	0.003	Router 1
	0.004	Router 0
	0.005	Switch1
	0.005	Switch1
	0.006	Switch1
	0.006	Laptop0
	0.007	Switch1
	0.008	Router 0
	0.009	Router 1
	0.010	Switch0

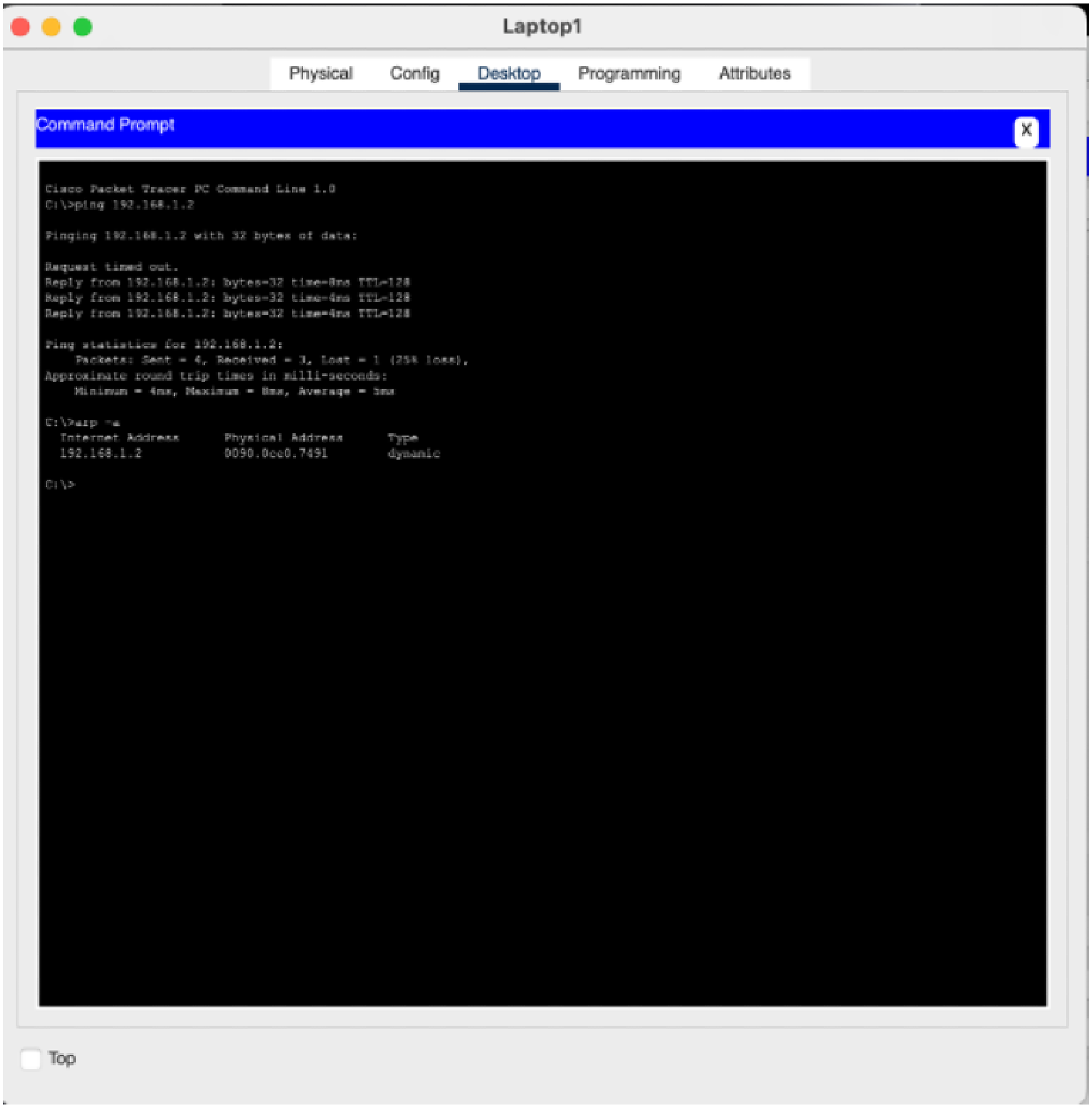
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
●	Successful	Lap...	Laptop0	IC...	■	0.000	N	0	(...	(delete)



```
C:\>ping 192.168.2.3

Pinging 192.168.2.3 with 32 bytes of data:

Reply from 192.168.2.3: bytes=32 time=10ms TTL=126
Reply from 192.168.2.3: bytes=32 time=10ms TTL=126
Reply from 192.168.2.3: bytes=32 time=10ms TTL=126
Reply from 192.168.2.3: bytes=32 time=10ms TTL=126

Ping statistics for 192.168.2.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 10ms, Average = 10ms

C:\>arp -a
  Internet Address      Physical Address      Type
  192.168.1.1           0002.170d.9d01        dynamic
  192.168.1.2           0090.0ce0.7491        dynamic

C:\>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.2.2: bytes=32 time=10ms TTL=126
Reply from 192.168.2.2: bytes=32 time=10ms TTL=126
Reply from 192.168.2.2: bytes=32 time=10ms TTL=126
Reply from 192.168.2.2: bytes=32 time=10ms TTL=126

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 10ms, Average = 10ms

C:\>ping 192.168.2.2

Pinging 192.168.2.2 with 32 bytes of data:

Reply from 192.168.2.2: bytes=32 time=10ms TTL=126
Reply from 192.168.2.2: bytes=32 time=10ms TTL=126
Reply from 192.168.2.2: bytes=32 time=10ms TTL=126
Reply from 192.168.2.2: bytes=32 time=10ms TTL=126

Ping statistics for 192.168.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 10ms, Average = 10ms

C:\>arp -a
  Internet Address      Physical Address      Type
  192.168.1.1           0002.170d.9d01        dynamic
  192.168.1.2           0090.0ce0.7491        dynamic

C:\>
```



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.2: bytes=32 time=8ms TTL=128
Reply from 192.168.1.2: bytes=32 time=4ms TTL=128
Reply from 192.168.1.2: bytes=32 time=4ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 8ms, Average = 5ms

C:\>arp -a
  Internet Address      Physical Address      Type
  192.168.1.2           0090.0ce0.7491        dynamic

C:\>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Reply from 192.168.2.1: bytes=32 time=0ms TTL=254
Reply from 192.168.2.1: bytes=32 time=0ms TTL=254
Reply from 192.168.2.1: bytes=32 time=0ms TTL=254
Reply from 192.168.2.1: bytes=32 time=0ms TTL=254

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>arp -a
  Internet Address      Physical Address      Type
  192.168.1.1           0002.173d.8d01        dynamic
  192.168.1.2           0090.0ce0.7491        dynamic

C:\>
```



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.2: bytes=32 time=8ms TTL=128
Reply from 192.168.1.2: bytes=32 time=4ms TTL=128
Reply from 192.168.1.2: bytes=32 time=4ms TTL=128

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 8ms, Average = 5ms

C:\>arp -a
  Internet Address      Physical Address      Type
  192.168.1.2           0090.0cc0.7491        dynamic

C:\>
```

Pinging from Laptop1 to PC2 (192.168.1.2):

ARP Request: Laptop1 broadcasts an ARP request for PC2's MAC address.

ARP Reply: PC2 replies with its MAC address.

Ping Success: ICMP echo requests/replies confirm successful communication.

Pinging from Laptop1 to Router1 (192.168.2.1):

ARP Resolution: Laptop1 sends an ARP request, and Router1 responds with its MAC address.

Ping Success: Communication between Laptop1 and Router1 is established.

Pinging from Laptop1 to Router2 (192.168.2.3):

ARP Resolution: Laptop1 resolves Router2's MAC address.

Ping Success: Communication between Laptop1 and Router2 is established.

ARP Table Analysis:

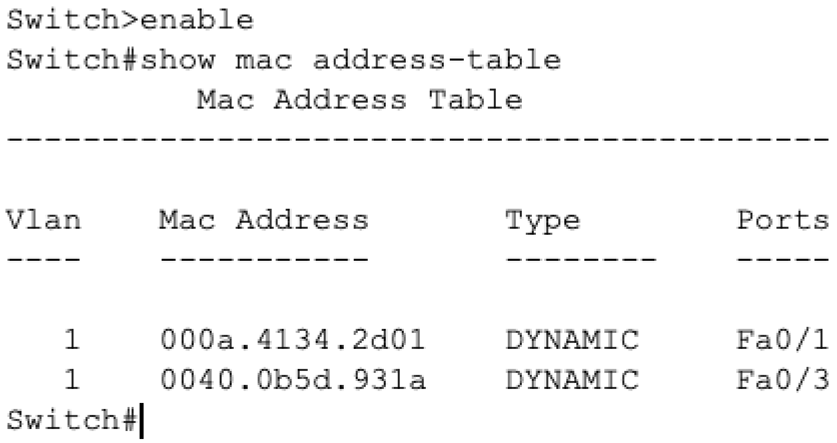
Laptop1 ARP Table: Shows IP-to-MAC mappings for PC2, Router1, and Router2.

PC2 and Router ARP Tables: Contain entries for communicating devices.

Observations:

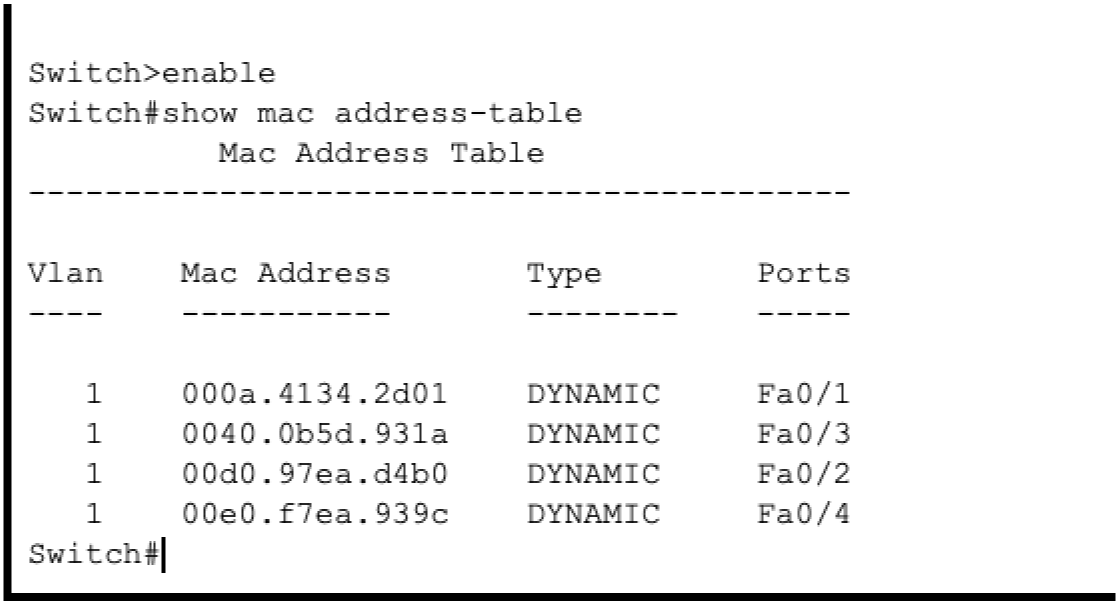
ARP resolves IP-to-MAC mappings efficiently, enabling communication across subnets.

Devices update their ARP tables upon receiving ARP replies, facilitating future communication.

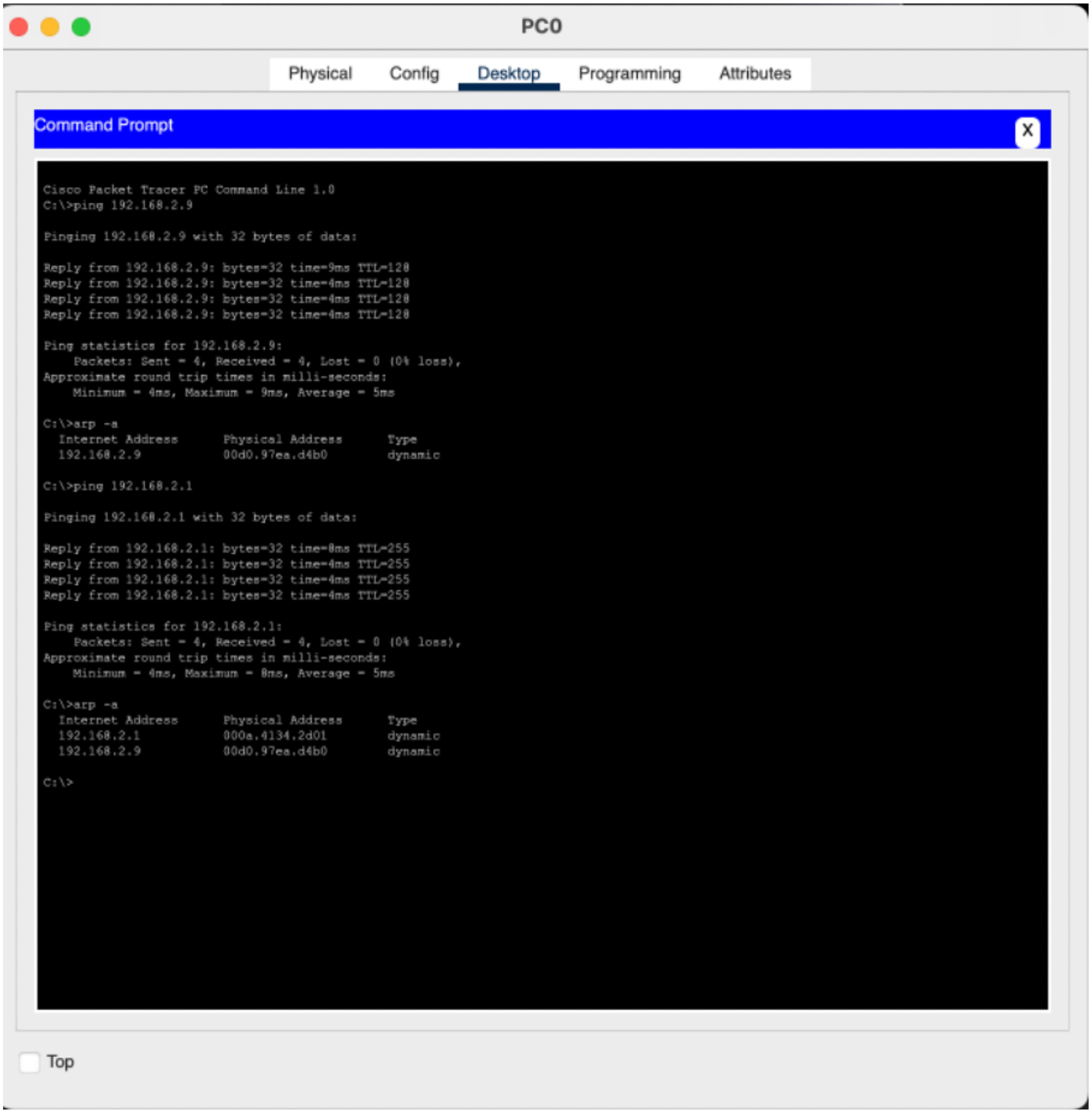


```
Switch>enable
Switch#show mac address-table
          Mac Address Table
-------------------------------------------

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

   1    000a.4134.2d01    DYNAMIC     Fa0/1
   1    0040.0b5d.931a    DYNAMIC     Fa0/3
Switch#
```

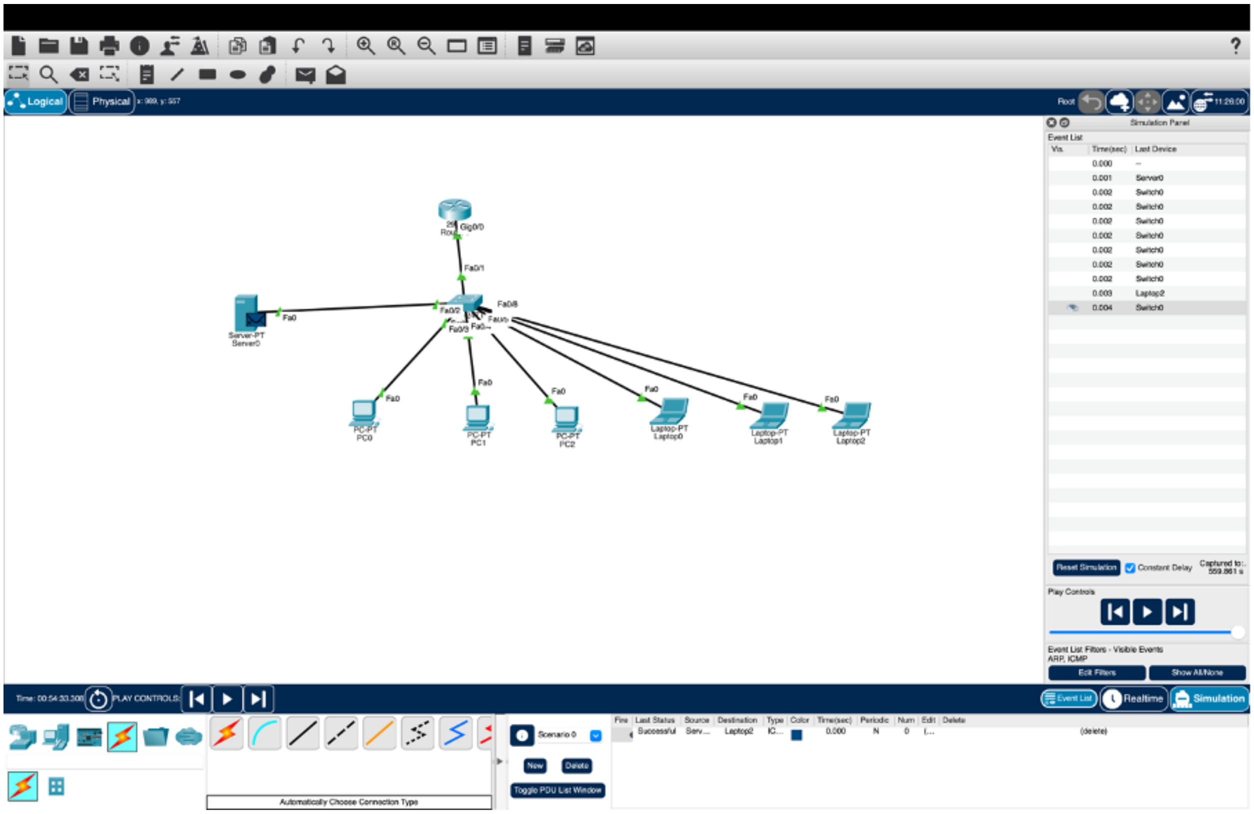
Activity 3



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

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

   1    000a.4134.2d01    DYNAMIC     Fa0/1
   1    0040.0b5d.931a    DYNAMIC     Fa0/3
   1    00d0.97ea.d4b0    DYNAMIC     Fa0/2
   1    00e0.f7ea.939c    DYNAMIC     Fa0/4
Switch#
```



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.2.9

Pinging 192.168.2.9 with 32 bytes of data:

Reply from 192.168.2.9: bytes=32 time=9ms TTL=128
Reply from 192.168.2.9: bytes=32 time=4ms TTL=128
Reply from 192.168.2.9: bytes=32 time=4ms TTL=128
Reply from 192.168.2.9: bytes=32 time=4ms TTL=128

Ping statistics for 192.168.2.9:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 9ms, Average = 5ms

C:\>arp -a
  Internet Address      Physical Address      Type
  192.168.2.9           00d0.97ea.d4b0        dynamic

C:\>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Reply from 192.168.2.1: bytes=32 time=8ms TTL=255
Reply from 192.168.2.1: bytes=32 time=4ms TTL=255
Reply from 192.168.2.1: bytes=32 time=4ms TTL=255
Reply from 192.168.2.1: bytes=32 time=4ms TTL=255

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 8ms, Average = 5ms

C:\>arp -a
  Internet Address      Physical Address      Type
  192.168.2.1           000a.4134.2d01        dynamic
  192.168.2.9           00d0.97ea.d4b0        dynamic

C:\>
```



Event List

Vis.	Time(sec)	Last Device
	0.000	--
	0.001	Server0
	0.002	Switch0
	0.002	Switch0
	0.002	Switch0
	0.002	Switch0
	0.002	Switch0
	0.002	Switch0
	0.002	Switch0
	0.003	Laptop2
	0.004	Switch0

Event List Filters - Visible Events
ARP, ICMP

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Successful	Serv...	Laptop2	IC...	■	0.000	N	0	(...	(delete)

1. Initial MAC Address Table:

- Ports Fa0/1, Fa0/2, Fa0/3, and Fa0/4 were associated with the MAC addresses 000a.4134.2d01, 00d0.97ea.d4b0, 0040.0b5d.931a, and 00e0.f7ea.939c respectively.

2. After Clearing and Pinging:

- The MAC addresses for Fa0/1 (000a.4134.2d01) and Fa0/3 (0040.0b5d.931a) were re-learned, indicating active communication from devices on these ports.

3. ARP Table on PC0:

- After pinging, PC0 resolved the IPs 192.168.2.9 and 192.168.2.1 to MAC addresses 00d0.97ea.d4b0 and 000a.4134.2d01 respectively, confirming successful network communication.

Conclusion:

- The switch's MAC address table dynamically updates based on active device communication, while the ARP table on PCs maps IP addresses to MAC addresses, ensuring correct packet routing within the network.

EXERCISES :

QUESTION : What are the differences between CRC and checksum techniques?

Differences Between CRC and Checksum Techniques

1. **Error Detection**:

   - **CRC**: More effective at detecting complex errors, including burst errors.

   - **Checksum**: Detects single-bit and some multiple-bit errors but is less reliable.

2. **Calculation Method**:

   - **CRC**: Uses polynomial division for a robust error-checking remainder.

   - **Checksum**: Involves summing data bytes and taking a modulo, making it simpler.

3. **Complexity**:

   - **CRC**: More computationally intensive but highly accurate.

   - **Checksum**: Easier and faster to compute but less powerful.

4. **Common Uses**:

   - **CRC**: Found in network communications and protocols needing high reliability.

   - **Checksum**: Used in basic file integrity checks and simpler network protocols.

In essence, CRC offers better error detection, while checksums are quicker and simpler but less effective.

QUESTION : What are the advantages and disadvantages of the three types of MAC protocols that we have discussed?

Advantages and Disadvantages of MAC Protocols

1. **TDMA (Time Division Multiple Access)**

- **Advantages**: Predictable performance with no collisions; each device gets a specific time slot.
- **Disadvantages**: Inefficient under light load; complex synchronization required.

2. **FDMA (Frequency Division Multiple Access)**

- **Advantages**: Allows simultaneous transmission; low latency as devices transmit concurrently.
- **Disadvantages**: Fixed bandwidth can lead to inefficiencies; potential for interference.

3. **CSMA (Carrier Sense Multiple Access)**

- **Advantages**: Efficient use of the medium; simpler to implement.
- **Disadvantages**: Susceptible to collisions; increased latency under heavy load.

QUESTION : How do ARP spoofing and ARP cache poisoning attacks impact the functionalities/operations of the networks?

Impact of ARP Spoofing and ARP Cache Poisoning

1. **Traffic Interception**: Attackers can redirect data meant for a legitimate device, allowing them to eavesdrop on communications.

2. **Data Manipulation**: Intercepted data can be altered before reaching the intended recipient, compromising data integrity.

3. **Denial of Service (DoS)**: Network devices may become unreachable, disrupting normal operations.

4. **Performance Issues**: Rerouted traffic can overload the network, slowing down performance.

5. **Identity Theft**: Attackers can impersonate legitimate devices, gaining unauthorized access to sensitive information.

6. **Security Breaches**: These attacks undermine overall network security, facilitating further malicious activities.