



FACULTY OF ELECTRONICS

COMPUTER ENGINEERING AND TELECOMMUNICATIONS DEPARTMENT

LABORATORY WORK #4

Switches, MAC-IP Addressing, and ARP

Student: Mark Mikula

Teacher: Artūras Medeišis

Vilnius, 2025

Objective

This Cisco Packet Tracer lab built upon previous exercises to provide familiarisation with Cisco Catalyst switches, explore the interplay between Ethernet MAC and IP addressing, and demonstrate the Address Resolution Protocol (ARP) process

The lab involved setting up a simulated LAN topology using a router and multiple switches, configuring devices, and analyzing Layer 2 (MAC) and Layer 3 (IP) addressing using CLI commands and simulated packet capture.

Part 1: Familiarising with Cisco Catalyst Switches

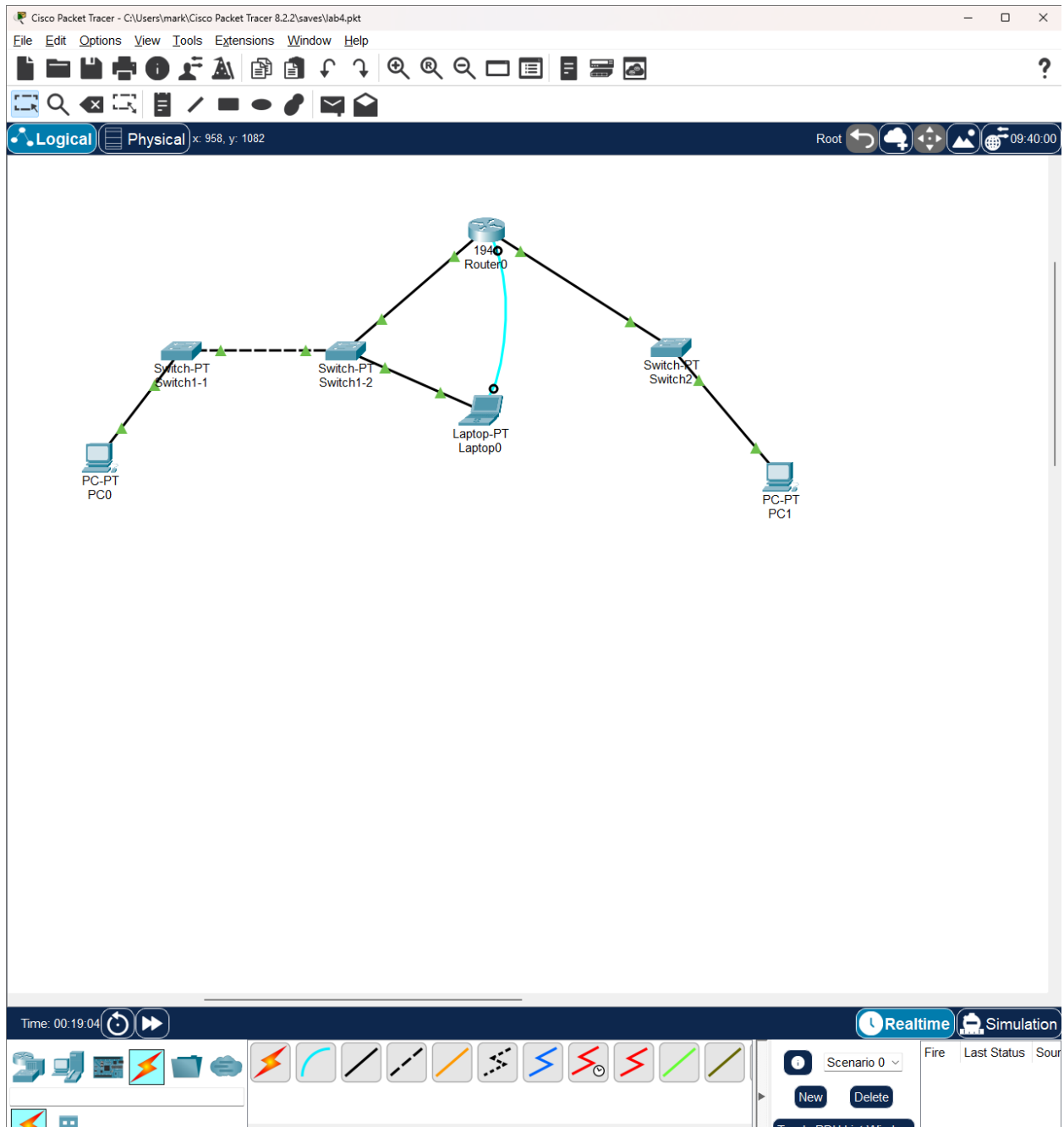
The lab introduced Cisco Catalyst switches, such as the Catalyst 3750 series, which are commonly used in enterprise access and distribution layers

Cisco Catalyst 3750 switches are typically used for aggregation of access layer switches or providing connectivity to end devices in a large network. They are considered Layer 3 devices, meaning they can perform both Layer 2 switching (forwarding frames based on MAC addresses) and Layer 3 routing (forwarding packets based on IP addresses), which offers enhanced usage possibilities like inter-VLAN routing and static routing

The physical setup involved connecting a Cisco 1941 router to switches (SW1-2 and SW2) and connecting two switches directly (SW1-1 and SW1-2)

Connecting two switches directly often requires a crossover UTP (Unshielded Twisted Pair) cable. A crossover cable is special because it swaps the transmit (TX) and receive (RX) wire pairs within the cable, allowing two devices configured to transmit on the same pins (like switch ports without auto-MDIX) to communicate directly

Basic router configuration was performed, similar to Lab 3, including setting IP addresses on interfaces



```
Laptop0
Physical Config Desktop Programming Attributes
Terminal
Press RETURN to get started!

Router>enable
Router#show ip interface brief
Interface          IP-Address      OK? Method Status          Protocol
GigabitEthernet0/0 unassigned      YES unset  administratively down down
GigabitEthernet0/1 unassigned      YES unset  administratively down down
Vlan1               unassigned      YES unset  administratively down down
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface GigabitEthernet0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
exit
Router(config)#interface GigabitEthernet0/1
Router(config-if)#ip address 10.1.1.1 255.255.255.0
Router(config-if)#no shutdown

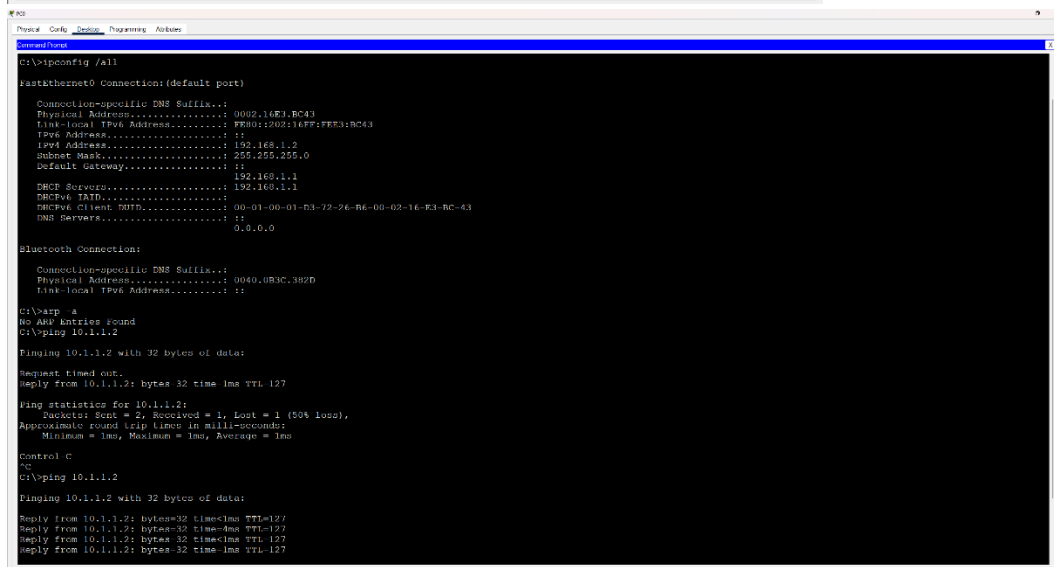
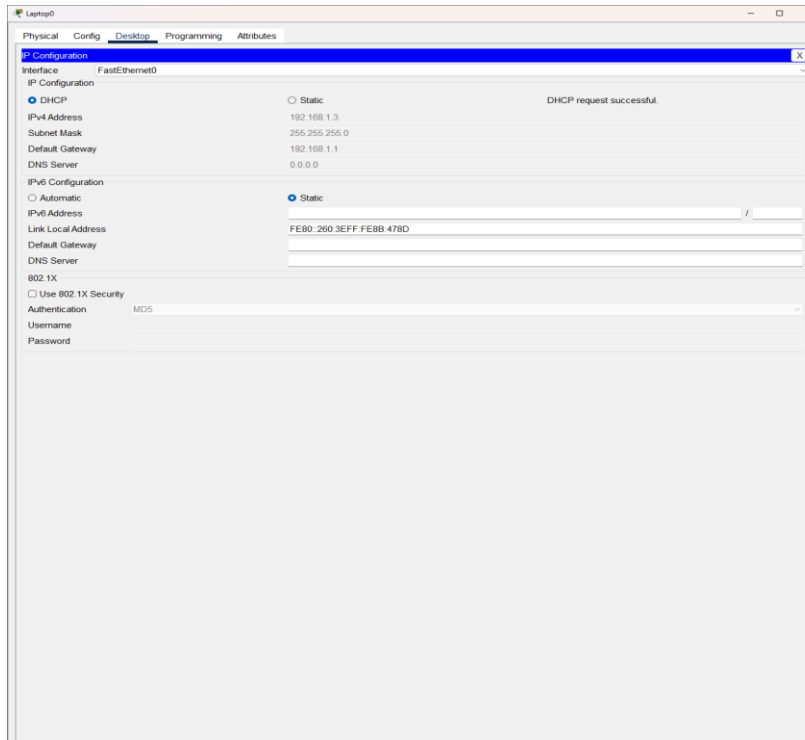
Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
exit
Router(config)#ip dhcp pool LW4_1
Router(dhcp-config)#network 192.168.1.0 255.255.255.0
Router(dhcp-config)#default-router 192.168.1.1
Router(dhcp-config)#exit
Router(config)#ip dhcp pool LW4_2
Router(dhcp-config)#network 10.1.1.0 255.255.255.0
Router(dhcp-config)#default-router 10.1.1.1
Router(dhcp-config)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
show ip interface brief
Interface          IP-Address      OK? Method Status          Protocol
GigabitEthernet0/0 192.168.1.1     YES manual up             up
GigabitEthernet0/1 10.1.1.1        YES manual up             up
Vlan1              unassigned      YES unset  administratively down down
Router#
```

Basic switch configuration involved connecting via console and setting the hostname, e.g., to SW1-1. While switches can forward frames without configuration, basic control commands are used for management. The initial state of the switch's MAC address table was checked using show mac address-table

Part 2: Connecting Subnets and investigating MAC-IP Addressing

The lab topology included a router (R1), two connected switches (SW1-1, SW1-2), and another switch (SW2), with PCs and a Laptop connected to the switches, forming two subnets (192.168.1.0/24 and 10.1.1.0/24) interconnected by the router



PCs were configured to obtain IP addresses via DHCP, and the `ipconfig /all` and `arp -a` commands were used to verify their network configurations and initial ARP tables

[Screenshot 2: PC IP Configs and Initial ARP Tables (ipconfig /all and arp -a output on PCs and Laptop)]

The assigned IP addresses corresponded to the addressing scheme in Figure 2

Hosts connected to SW1-1 and SW1-2 received IPs in the 192.168.1.0/24 network (e.g., 192.168.1.11, 192.168.1.12), while hosts on SW2 received IPs in the 10.1.1.0/24 network (e.g., 10.1.1.11). The sources mention DHCP leases but do not specify start/end times, which would be observable in a real-world scenario or Packet Tracer event list. At this stage, the ARP tables of PCs would primarily contain entries learned from previous communications or be empty, typically including the default gateway's IP/MAC if DHCP was used

```
PC1>ipconfig /all

Cisco Packet Tracer PC Command Line 1.0
C:\Windows [all]

FastEthernet0 Configuration (Default port)

Connection-specific DNS Suffix...:
Physical Address.....: 0009.1800.4700
Link-local IPv6 Address.....: FE80::1800:47FF:FE80:4700
IPv4 Address.....: 192.168.1.11
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.1.1

DHCP Server.....: 192.168.1.1
DHCPv6 Server.....:
DHCP Client ID.....: 00-01-80-01-18-10-00-00-00-00-00-00-00-00-00-00
DNS Servers.....:
0.0.0.0

Ethernet0 Configuration

Connection-specific DNS Suffix...:
Physical Address.....: 0004.5000.0000
Link-local IPv6 Address.....: FE80::5000:0000:0000:0000
IPv4 Address.....: 192.168.1.12

C:\Users\me
No ARP Entries Found
C:\Users\me\arp -a
Pinging 192.168.1.12 with 32 bytes of data:
Reply from 192.168.1.12: bytes=32 time=1ms TTL=128
Reply from 192.168.1.12: bytes=32 time=1ms TTL=128
Reply from 192.168.1.12: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.12:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
    Approximate round trip times in milliseconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
    Received 0
    C:\>
C:\>
```

```
PC2>ipconfig /all

Cisco Packet Tracer PC Command Line 1.0
C:\Windows [all]

FastEthernet0 Configuration (Default port)

Connection-specific DNS Suffix...:
Physical Address.....: 0009.1800.4700
Link-local IPv6 Address.....: FE80::1800:47FF:FE80:4700
IPv4 Address.....: 192.168.1.11
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.1.1

DHCP Server.....: 192.168.1.1
DHCPv6 Server.....:
DHCP Client ID.....: 00-01-80-01-18-10-00-00-00-00-00-00-00-00-00-00
DNS Servers.....:
0.0.0.0

Ethernet0 Configuration

Connection-specific DNS Suffix...:
Physical Address.....: 0004.5000.0000
Link-local IPv6 Address.....: FE80::5000:0000:0000:0000
IPv4 Address.....: 192.168.1.12

C:\Users\me
No ARP Entries Found
C:\Users\me\arp -a
Pinging 192.168.1.12 with 32 bytes of data:
Reply from 192.168.1.12: bytes=32 time=1ms TTL=128
Reply from 192.168.1.12: bytes=32 time=1ms TTL=128
Reply from 192.168.1.12: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.12:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
    Approximate round trip times in milliseconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
    Received 0
    C:\>
C:\>
```

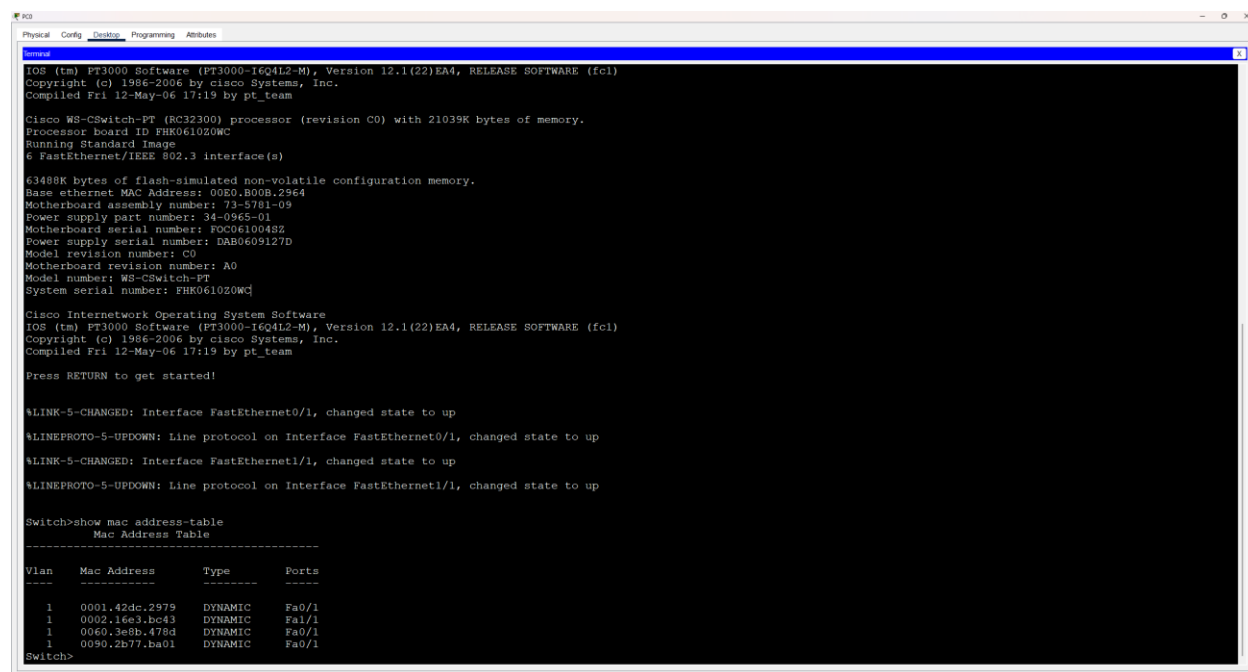
Ping tests were performed between devices on the same and different subnets to confirm communication

MAC and ARP Table Analysis:

```
C:\>arp -a

Internet Address      Physical Address      Type
192.168.1.1           0090.2b77.ba01       dynamic
192.168.1.3           0060.3e8b.478d       dynamic
```

The SW1-1 MAC table lists MAC addresses learned on its ports



```
Switch>show mac address-table
Mac Address Table
-----
Vlan    Mac Address      Type      Ports
----    -
1       0001.42dc.2979   DYNAMIC   Fa0/1
1       0002.16e3.bc43   DYNAMIC   Fa1/1
1       0060.3e8b.478d   DYNAMIC   Fa0/1
1       0090.2b77.ba01   DYNAMIC   Fa0/1
Switch>
```

After communication, this would include the MAC addresses of PC1, PC2 (directly connected), R1's Gi0/0 interface (connected via SW1-2), and potentially the Laptop's MAC (learned via SW1-2 and SW2)

Switch ports can have more than one MAC address assigned

This occurs on ports connected to other switches (like the link between SW1-1 and SW1-2) or hubs, where traffic from multiple devices passes through a single port. SW1-1's port connected to SW1-2 would learn the MACs of PC1, PC2, and R1 if they communicate through that link

There is a significant difference between the ARP table of a PC and the MAC table of a switch

A PC's ARP table is a Layer 3 to Layer 2 mapping (IP to MAC) used for communication within its local IP subnet or to find its default gateway's MAC for inter-subnet communication. A switch's MAC address table is a Layer 2 mapping (MAC to Port) used for forwarding Ethernet frames and is unaware of IP addresses

LAN Addressing Table

| Host Name | MAC address | IP address | Switching port | Switch Port |
|-----------|-------------|------------|----------------|-------------|
|-----------|-------------|------------|----------------|-------------|

| | | | | |
|----------|----------------|-------------|--|-------|
| R1 Gi0/0 | 0001.C916.A301 | 192.168.1.1 | | SW1-2 |
|----------|----------------|-------------|--|-------|

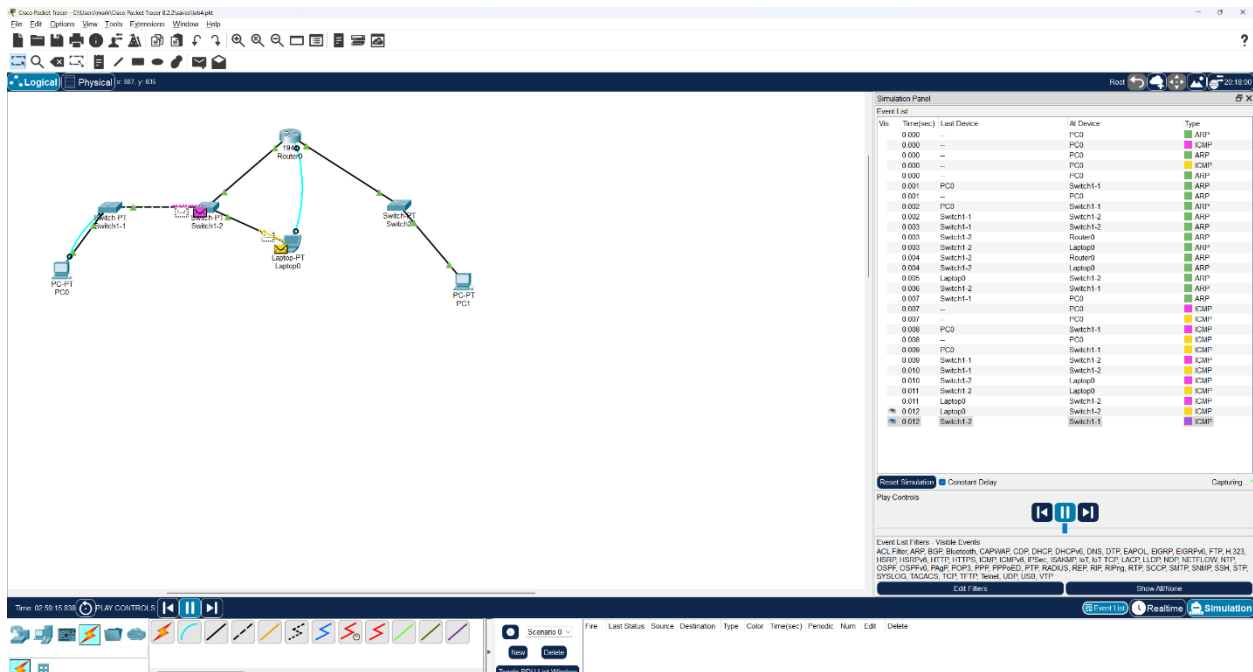
| | | | | |
|----------|----------------|----------|-----|--|
| R1 Gi0/1 | 0001.C916.A302 | 10.1.1.1 | SW2 | |
|----------|----------------|----------|-----|--|

| | | | | |
|--------------|----------------|--------------|-------|--|
| PC1 Ethernet | 00D0.BC0B.8CD1 | 192.168.1.11 | SW1-1 | |
|--------------|----------------|--------------|-------|--|

| | | | | |
|--------------|----------------|--------------|-------|--|
| PC2 Ethernet | 0060.2F44.92BB | 192.168.1.12 | SW1-1 | |
|--------------|----------------|--------------|-------|--|

| | | | | |
|-----------------|----------------|-----------|-----|--|
| Laptop Ethernet | 00E0.B098.C6AD | 10.1.1.11 | SW2 | |
|-----------------|----------------|-----------|-----|--|

Packet Encapsulation Analysis: Simulation was used to analyze packets during ping operations. Specifically, the ARP process and ICMP (ping) packets were observed



Deleting the ARP cache (arp -d) before pinging a destination on the same subnet triggers an ARP request for the destination's IP address to discover its MAC address

The first packet sent in this scenario is typically an ARP broadcast request. When pinging a destination on a different subnet, the PC ARPs for its default gateway's IP address to get the router's MAC. The sequence of packets would differ: an ARP request/reply for the gateway followed by the ICMP packet for inter-subnet ping, versus an ARP request/reply for the destination followed by the ICMP packet for same-subnet ping (if the MAC is not known)

The encapsulation of packets, particularly MAC addresses, changes as they traverse different network segments and pass through a router

Addresses: Host: PC1 (Source) Host: Laptop (Destination)

Destination MAC 0001.C916.A301 (R1's Gi0/0 MAC)

Source MAC 00D0.BC0B.8CD1 (PC1's MAC)

Source IP 192.168.1.11

Destination IP 10.1.1.11

Ping packet sent from PC1 (192.168.1.11) to PC2 (192.168.1.12) - Same Subnet

Addresses: Host: PC1 (Source) Host: PC2 (Destination)

Destination MAC 0060.2F44.92BB (PC2's MAC)

Source MAC 00D0.BC0B.8CD1 (PC1's MAC)

Source IP 192.168.1.11

Destination IP 192.168.1.12

Ping packet from PC1 (192.168.1.11) as received in PC2 (192.168.1.12) - Received Frame

Addresses: Host: PC1 (Source - IP Header) Host: PC2 (Destination - IP Header)

Destination MAC 0060.2F44.92BB (PC2's MAC)

Source MAC 00D0.BC0B.8CD1 (PC1's MAC)

Source IP 192.168.1.11

Destination IP 192.168.1.12

Addressing Differences and Encapsulation Change: The difference in MAC-IP addressing for the two initial ping packets (PC1 to Laptop vs. PC1 to PC2) lies in the destination MAC address

For the same-subnet ping (PC1 to PC2), the destination MAC is the target host's (PC2's) MAC address. For the different-subnet ping (PC1 to Laptop), the destination MAC is the MAC address of the default gateway (R1's interface Gi0/0), because the PC knows the destination IP is not local and must send it to the router. The source IP and destination IP addresses in the IP header remain the actual source and destination IPs (PC1 and Laptop/PC2, respectively) in both cases

The encapsulation of the PC1->Laptop packet changed at the router

The IP packet itself (containing the original source and destination IPs) remained intact. However, upon receiving the frame from PC1, the router (R1) decapsulated the Ethernet frame to read the destination IP address in the IP header. It then looked up the destination network (10.1.1.0/24) in its routing table and determined the packet needed to exit via interface Gi0/1. R1 then re-encapsulated the IP packet into a new Ethernet frame with the source MAC address being R1's Gi0/1 MAC (0001.C916.A302) and the destination MAC address being the Laptop's MAC (00E0.B098.C6AD), after performing an ARP request for the Laptop's IP if necessary. MAC addresses are local to each Layer 2 segment, hence they change at Layer 3 boundaries (routers)

Conclusion

This lab provided valuable practical experience in configuring Cisco switches and a router to create a layered LAN topology

It deepened understanding of Ethernet MAC and IP addressing principles and the ARP process, which is fundamental for Layer 2/Layer 3 interaction. By examining ARP tables and MAC address tables and analyzing simulated packet captures, the lab clearly demonstrated how devices resolve IP addresses to MAC addresses for communication and how MAC addresses are used and updated by switches and routers. Connectivity tests verified the network configuration and the functionality of ARP and routing. The analysis of packet encapsulation highlighted the crucial role routers play in changing Layer 2 information while preserving Layer 3 information when forwarding packets between different subnets. Overall, the lab successfully clarified the interplay between MAC and IP addressing at different layers of the network stack