Networking Academy

Name: Carosus, Cean A. Section: CS 203

Packet Tracer - Identify MAC and IP Addresses

Objectives

Part 1: Gather PDU Information for Local Network Communication

Part 2: Gather PDU Information for Remote Network Communication

Background

This activity is optimized for viewing PDUs. The devices are already configured. You will gather PDU information in simulation mode and answer a series of questions about the data you collect.

Instructions

Part 1: Gather PDU Information for Local Network Communication

Note: Review the Reflection Questions in Part 3 before proceeding with Part 1. It will give you an idea of the type of information you will need to gather. Gather PDU information as a packet travels from 172.16.31.5 to 172.16.31.2.

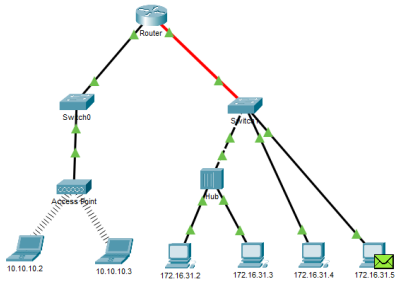
a. Click **172.16.31.5** and open the **Command Prompt**.

b. Enter the **ping 172.16.31.2** command.

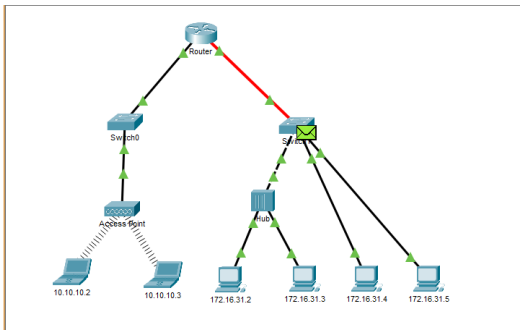
c. Switch to simulation mode and repeat the **ping 172.16.31.2** command. A PDU appears next to **172.16.31.5**.

d. Click the PDU and note the following information from the **OSI Model** and **Outbound PDU Layer** tabs:

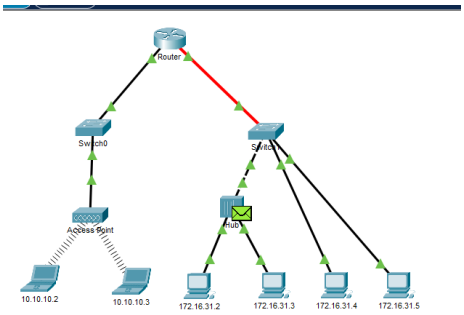
- Destination MAC Address: **000C:85CC:1DA7**



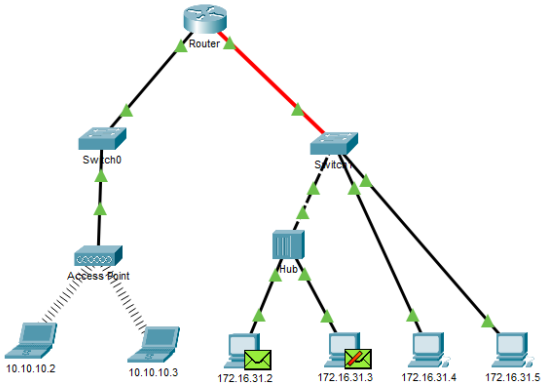
172.16.31.5 PDU



Switch PDU



Hub PDU



172.161.31.2 & 172.16.31.3 PDU

- Source MAC Address: **00D0:D311:C788**
- Source IP Address: **172.16.31.5**
- Destination IP Address: **172.16.31.2**
- At Device: **172.16.31.5**

e. Click **Capture / Forward (the right arrow followed by a vertical bar)** to move the PDU to the next device. Gather the same information from Step 1d. Repeat this process until the PDU reaches its destination. Record the PDU information you gathered into a spreadsheet using a format like the table shown below:

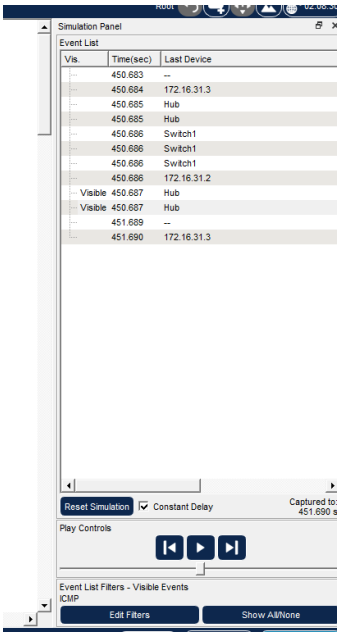
Example Spreadsheet Format

At Device	Dest. MAC	Src MAC	Src IPv4	Dest IPv4
172.16.31.5	000C:85CC:1DA7	00D0:D311:C788	172.16.31.5	172.16.31.2
Switch1	000C:85CC:1DA7	00D0:D311:C788	N/A	N/A
Hub	N/A	N/A	N/A	N/A
172.16.31.2	00D0:D311:C788	000C:85CC:1DA7	172.16.31.2	172.16.31.5

Step 2: Gather additional PDU information from other pings.

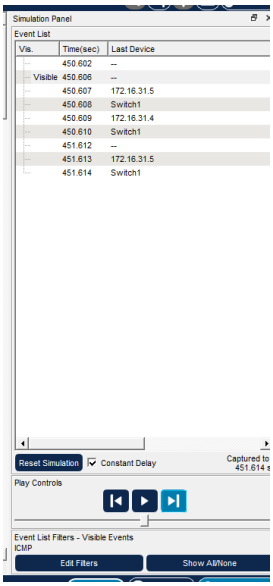
Repeat the process in Step 1 and gather the information for the following tests:

- Ping 172.16.31.2 from 172.16.31.3.



At Device	Dest. MAC	Src MAC	Src IPv4	Dest IPv4
172.16.31.3	000C.85CC.1DA7	0060.7036.2849	172.16.31.3	172.16.31.2
Switch1	000C:85CC:1DA7	0060.7036.2849	N/A	N/A
Hub	N/A	N/A	N/A	N/A
172.16.31.2	000C.85CC.1DA7	0060.7036.2849	172.16.31.2	172.16.31.5

- Ping 172.16.31.4 from 172.16.31.5.



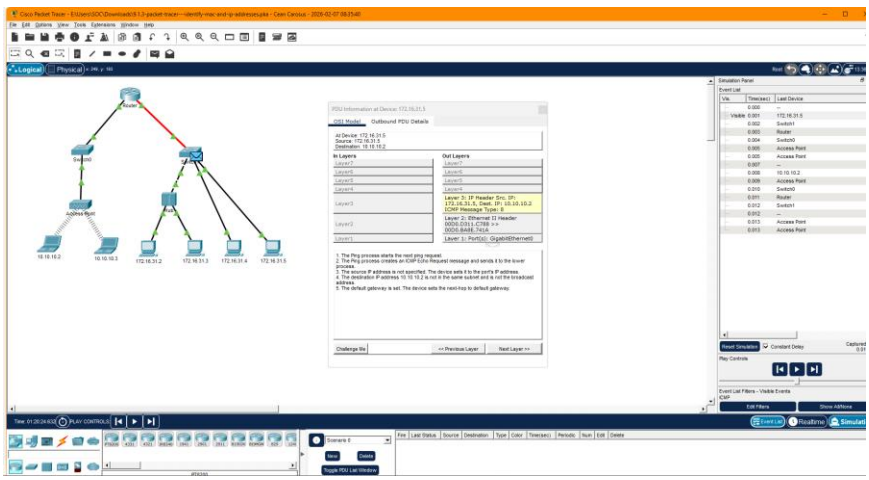
At Device	Dest. MAC	Src MAC	Src IPv4	Dest IPv4
172.16.31.3	000C.CF0B.BC80	00D0.D311.C788	172.16.31.5	172.16.31.4
Switch1	000C.CF0B.BC80	00D0.D311.C788	N/A	N/A
Hub	N/A	N/A	N/A	N/A
172.16.31.2	00D0.D311.C788	000C.CF0B.BC80	172.16.31.4	172.16.31.5

Return to Realtime mode.

Part 2: Gather PDU Information for Remote Network Communication

In order to communicate with remote networks, a gateway device is necessary. Study the process that takes place to communicate with devices on the remote network. Pay close attention to the MAC addresses used.

Step 1: Gather PDU information as a packet travels from 172.16.31.5 to 10.10.10.2.



a. Click **172.16.31.5** and open the **Command Prompt**.

b. Enter the **ping 10.10.10.2** command.

c. Switch to simulation mode and repeat the **ping 10.10.10.2** command. A PDU appears next to **172.16.31.5**.

d. Click the PDU and note the following information from the **Outbound PDU Layer** tab:

- Destination MAC Address: 00D0:BA8E:741A
- Source MAC Address: 00D0:D311:C788
- Source IP Address: 172.16.31.5
- Destination IP Address: 10.10.10.2
- At Device: 172.16.31.5

What device has the destination MAC that is shown?
172.16.31.5

e. Click **Capture / Forward (the right arrow followed by a vertical bar)** to move the PDU to the next device. Gather the same information from Step 1d. Repeat this process until the PDU reaches its destination. Record the PDU information you gathered from pinging 172.16.31.5 to 10.10.10.2 into a spreadsheet using a format like the sample table shown below:

At Device	Dest. MAC	Src MAC	Src IPv4	Dest IPv4
172.16.31.5	00D0:BA8E:741A	00D0:D311:C788	172.16.31.5	10.10.10.2
Switch1	00D0:BA8E:741A	00D0:D311:C788	N/A	N/A
Router	0060:2F84:4AB6	00D0:588C:2401	172.16.31.5	10.10.10.2
Switch0	0060:2F84:4AB6	00D0:588C:2401	N/A	N/A
Access Point	N/A	N/A	N/A	N/A
10.10.10.2	00D0:588C:2401	0060:2F84:4AB6	10.10.10.2	172.16.31.5

Part 3: Reflection Questions

Answer the following questions regarding the captured data:

1. Were there different types of cables/media used to connect devices? Specify each.

Yes. Ethernet cables were used between PCs, switches, hubs, and routers, and wireless media was used between the access point and the wireless PC.

2. Did the cables change the handling of the PDU in any way?

No. The cables only carried the data. The **devices**, not the cables, decided what to do with the PDU.e your answers here.

3. Did the **Hub** lose any of the information that it received?

No. The hub didn’t inspect or change the data at all.answers

4. What does the **Hub** do with MAC addresses and IP addresses?

   The hub doesn't look at them. It just floods the signal out all ports.

5. Did the wireless **Access Point** do anything with the information given to it?

   No. It simply forwarded the frame between wired and wireless networks.

6. Was any MAC or IP address lost during the wireless transfer?

   No. All addressing information stayed intact.

7. What was the highest OSI layer that the **Hub** and **Access Point** used?

   Layer 1 (Physical Layer)

8. Did the **Hub** or **Access Point** ever replicate a PDU that was rejected with a red "X"?

   Yes. They forwarded frames even if they were eventually rejected.

9. When examining the **PDU Details** tab, which MAC address appeared first, the source or the destination?

   The **destination MAC address**.

10. Why would the MAC addresses appear in this order?

    Because Ethernet frames are built with the destination address first so devices can quickly decide whether to process or ignore the frame.

11. Was there a pattern to the MAC addressing in the simulation?

    Yes. Each device had a consistent MAC address, and routers had different MACs on different interfaces.

12. Did the switches ever replicate a PDU that was rejected with a red "X"?

    No. Switches only forward frames out the correct port.

13. Every time that the PDU was sent between the 10 network and the 172 network, there was a point where the MAC addresses suddenly changed. Where did that occur?

    At the **router**.

14. Which device uses MAC addresses that start with 00D0:BA?

    the **router** interface connected to the local network.

15. What devices did the other MAC addresses belong to?

    They belonged to PCs, switches, and the router's other interface.

16. Did the sending and receiving IPv4 addresses change fields in any of the PDUs?

    No. The source and destination IP addresses stayed the same end-to-end.

17. When you follow the reply to a ping, sometimes called a *pong*, do you see the sending and receiving IPv4 addresses switch?

    Yes. The source and destination IPs swap during the pong.

18. What is the pattern to the IPv4 addressing used in this simulation?

    Each network uses a different subnet:

- 172.16.31.x for the local network
- 10.10.10.x for the remote network

19. Why do different IP networks need to be assigned to different ports of a router?

    Because a router separates networks, and each interface must belong to a different IP network.

20. If this simulation was configured with IPv6 instead of IPv4, what would be different?

    Addresses would be longer, written in hexadecimal, and there would be no ARP — IPv6 uses Neighbor Discovery instead.