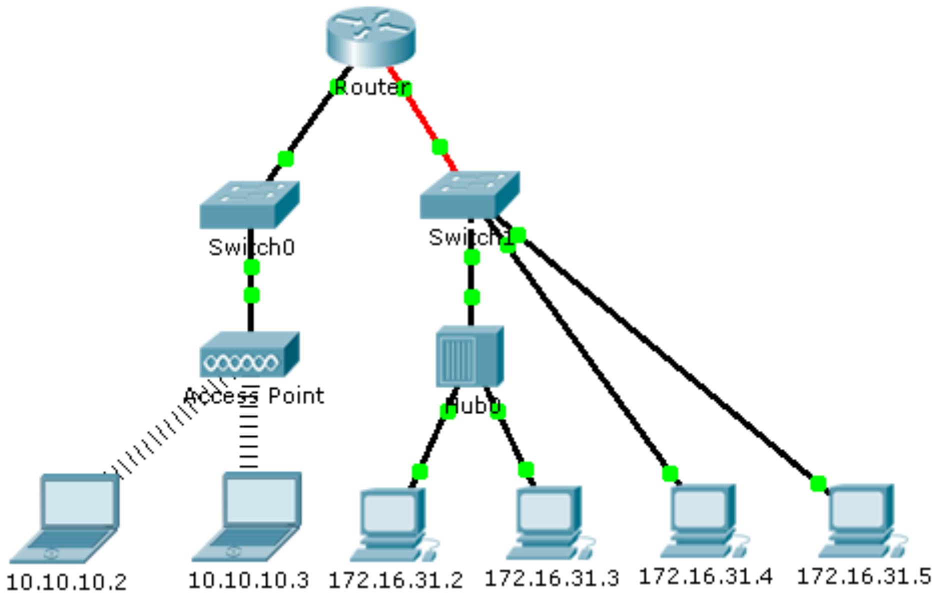
Packet Tracer - Identify MAC and IP Addresses

Topology



Objectives

Part 1: Gather PDU Information

Part 2: Reflection Questions

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.

1. Gather PDU Information

Note: Review the Reflection Questions in Part 2 before proceeding with Part 1. It will give you an idea of the types of information you will need to gather.

1. Gather PDU information as a packet travels from 172.16.31.2 to 10.10.10.3.

a. Click **172.16.31.2** and open the **Command Prompt**.

b. Enter the **ping 10.10.10.3** command.

c. Switch to simulation mode and repeat the **ping 10.10.10.3** command. A PDU appears next to **172.16.31.2**.

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

- Destination MAC Address: 00D0:BA8E:741A
- Source MAC Address: 000C:85CC:1DA7
- Source IP Address: 172.16.31.2
- Destination IP Address: 10.10.10.3
- At Device: Computer

e. Click **Capture / Forward** 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

Test	At Device	Dest. MAC	Src MAC	Src IPv4	Dest IPv4
Ping from 172.16.31.2 to 10.10.10.3	172.16.31.2	00D0:BA8E:741A	000C:85CC:1DA7	172.16.31.2	10.10.10.3
	Hub	--	--	--	--
	Switch1	00D0:BA8E:741A	000C:85CC:1DA7	--	--
	Router	0060:4706:572B	00D0:588C:2401	172.16.31.2	10.10.10.3
	Switch0	0060:4706:572B	00D0:588C:2401	--	--
	Access Point	--	--	--	--
	10.10.10.3	0060:4706:572B	00D0:588C:2401	172.16.31.2	10.10.10.3

- Ping 10.10.10.3 from 172.16.31.2.

Test	At Device	Dest. MAC	Src MAC	Src IPv4	Dest IPv4
Ping 10.10.10.3 from 172.16.31.2	172.16.31.2	00D0.BA8E.741A	000C.85CC.1DA7	172.16.31.2	10.10.10.3
	Hub	00D0.BA8E.741A	000C.85CC.1DA7	172.16.31.2	10.10.10.3
	Switch1	00D0.BA8E.741A	000C.85CC.1DA7	172.16.31.2	10.10.10.3
	172.16.31.3	00D0.BA8E.741A	000C.85CC.1DA7	172.16.31.2	10.10.10.3
	Router	0060.4706.572B	00D0.588C.2401	172.16.31.2	10.10.10.3
	172.16.31.5	00D0.BA8E.741A	000C.85CC.1DA7	172.16.31.2	10.10.10.3
	172.16.31.4	00D0.BA8E.741A	000C.85CC.1DA7	172.16.31.2	10.10.10.3
	Switch0	0060.4706.572B	00D0.588C.2401	172.16.31.2	10.10.10.3
	Access Point	0050.0FAB.6C82	00D0.588C.2401	172.16.31.2	10.10.10.3
	10.10.10.3	0060.4706.572B	00D0.588C.2401	10.10.10.3	172.16.31.2

2. Gather additional PDU information from other pings.

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

- Ping 10.10.10.2 from 10.10.10.3.

Test	At Device	Dest. MAC	Src MAC	Src IPv4	Dest IPv4
Ping 10.10.10.2 from 10.10.10.3	10.10.10.3	0060.4706.572B	0060.2F84.4AB6	10.10.10.3	10.10.10.2
	Access Point	0060.2F84.4AB6	0060.4706.572B	10.10.10.3	10.10.10.2
	Switch0	0060.2F84.4AB6	0060.4706.572B	10.10.10.3	10.10.10.2
	Access Point	0050.0FAB.6C82	0060.4706.572B	10.10.10.3	10.10.10.2
	10.10.10.3	0050.0FAB.6C82	0060.4706.572B	10.10.10.3	10.10.10.2
	10.10.10.2	0060.2F84.4AB6	0060.4706.572B	10.10.10.2	10.10.10.3

- Ping 172.16.31.2 from 172.16.31.3.

Test	At Device	Dest. MAC	Src MAC	Src IPv4	Dest IPv4
Ping 172.16.31.2 from 172.16.31.3	172.16.31.3	000C.85CC.1DA7	0060.7036.2849	172.16.31.3	172.16.31.2
	Hub	000C.85CC.1DA7	0060.7036.2849	172.16.31.3	172.16.31.2
	Switch1	000C.85CC.1DA7	0060.7036.2849	172.16.31.3	172.16.31.2
	172.16.31.2	0060.7036.2849	000C.85CC.1DA7	172.16.31.2	172.16.31.3

- Ping 172.16.31.4 from 172.16.31.5.

Test	At Device	Dest. MAC	Src MAC	Src IPv4	Dest IPv4
Ping 172.16.31.4 from 172.16.31.5	172.16.31.5	FFFF.FFFF.FFFF	00D0.D311.C788	172.16.31.5	172.16.31.4
	Switch1	FFFF.FFFF.FFFF	00D0.D311.C788	172.16.31.5	172.16.31.4
	Router	FFFF.FFFF.FFFF	00D0.D311.C788	172.16.31.5	172.16.31.4
	172.16.31.4	00D0.D311.C788	000C.CF08.BC80	172.16.31.4	172.16.31.5

- Ping 172.16.31.4 from 10.10.10.2.

Test	At Device	Dest. MAC	Src MAC	Src IPv4	Dest IPv4
Ping 172.16.31.4 from 10.10.10.2	10.10.10.2	0060.2F84.4AB6	00D0.588C.2401	10.10.10.2	172.16.31.4
	Access Point	00D0.588C.2401	0060.2F84.4AB6	10.10.10.2	172.16.31.4
	Switch0	00D0.588C.2401	0060.2F84.4AB6	10.10.10.2	172.16.31.4
	Router	000C.CF08.BC80	00D0.BA8E.741A	10.10.10.2	172.16.31.4
	Switch1	000C.CF08.BC80	00D0.BA8E.741A	10.10.10.2	172.16.31.4
	Access Point	0050.0FAB.6C82	0060.2F84.4AB6	10.10.10.2	172.16.31.4
	10.10.10.3	0050.0FAB.6C82	0060.2F84.4AB6	10.10.10.2	172.16.31.4
	10.10.10.2	0050.0FAB.6C82	0060.2F84.4AB6	10.10.10.2	172.16.31.4
	172.16.31.4	00D0.BA8E.741A	000C.CF08.BC80	172.16.31.4	10.10.10.2

- Ping 172.16.31.3 from 10.10.10.2.

Test	At Device	Dest. MAC	Src MAC	Src IPv4	Dest IPv4
Ping 172.16.31.3 from 10.10.10.2	10.10.10.2	0060.2F84.4AB6	00D0.588C.2401	10.10.10.2	172.16.31.3
	Access Point	00D0.588C.2401	0060.2F84.4AB6	10.10.10.2	172.16.31.3
	Switch0	00D0.588C.2401	0060.2F84.4AB6	10.10.10.2	172.16.31.3
	Router	0060.7036.2849	00D0.BA8E.741A	10.10.10.2	172.16.31.3
	Switch1	0060.7036.2849	00D0.BA8E.741A	10.10.10.2	172.16.31.3
	Hub	0060.7036.2849	00D0.BA8E.741A	10.10.10.2	172.16.31.3
	172.16.31.2	0060.7036.2849	00D0.BA8E.741A	10.10.10.2	172.16.31.3
	172.16.31.3	00D0.BA8E.741A	0060.7036.2849	172.16.31.3	10.10.10.2

2. Reflection Questions

Answer the following questions regarding the captured data:

1. We’re their different types of wires used to connect devices? Yes, the wires in the topology include ‘Copper Straight-Through’ and ‘Fiber’;
2. Did the wires change the handling of the PDU in any way? It does not appear to change the handling;

- IP packets can be communicated as electronic signals over copper cable, as optical signals over fiber, or wirelessly as radio signals;
- In some cases, an intermediate device, usually a router, must split up a packet when forwarding it from one medium to another medium with a smaller MTU; This process is called fragmenting the packet or fragmentation;
- …one major characteristic of the media that the network layer considers: the maximum size of the PDU that each medium can transport. This characteristic is referred to as the maximum transmission unit (MTU).
- IP operates independently of the media that carry the data at lower layers of the protocol stack.
- Media Independent - Operation is independent of the medium (i.e., copper, fiber optic, or wireless) carrying the data.
- Introduction to v6 Networks

3. Did the **Hub** lose any of the information given to it? No;

- Full-Duplex Communication: Both devices can transmit and receive on the media at the same time. The data link layer assumes that the media is available for transmission for both nodes at any time. Ethernet switches operate in full-duplex mode by default but can operate in half-duplex if connecting to a device such as an Ethernet hub.
- Duplex communications refer to the direction of data transmission between two devices. Half-duplex communications restrict the exchange of data to one direction at a time while full-duplex allows the sending and receiving of data to happen simultaneously.
- Half-Duplex Communication: Both devices can transmit and receive on the media but cannot do so simultaneously. The half-duplex mode is used in legacy bus topologies and with Ethernet hubs. WLANs also operate in half-duplex. Half-duplex allows only one device to send or receive at a time on the shared medium and is used with contention-based access methods.
- Contention-based access – All nodes operating in half-duplex compete for the use of the medium, but only one device can send at a time. However, there is a process if more than one device transmits at the same time. Ethernet LANs using hubs and WLANs are examples of this type of access control.
- Introduction to v6 Networks

4. What does the **Hub** do with MAC addresses and IP addresses? It does not appear to do anything with the information;

- When a device is forwarding a message to an Ethernet network, it attaches header information to the frame. The header information contains the source and destination MAC address;

- Only the device that originally sent the ARP request will receive the unicast ARP reply. Once the ARP reply is received, the device will add the IPv4 address and the corresponding MAC address to its ARP table. Packets destined for that IPv4 address can now be encapsulated in frames using its corresponding MAC address.
- Only the device with an IPv4 address associated with the target IPv4 address in the ARP request will respond with an ARP reply. The ARP reply message includes:
    - Sender’s IPv4 address – This is the IPv4 address of the sender, the device whose MAC address was requested.
    - Sender’s MAC address – This is the MAC address of the sender, the MAC address needed by the sender of the ARP request.
- The ARP reply is encapsulated in an Ethernet frame using the following header information:
    - Destination MAC address – This is the MAC address of the sender of the ARP request.
    - Source MAC address – This is the sender of the ARP reply’s MAC address.
- If no device responds to the ARP request, the packet is dropped because a frame cannot be created.
- Introduction to v6 Networks

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

- Wireless Access Point (AP) – Concentrates the wireless signals from users and connects to the existing copper-based network infrastructure, such as Ethernet. Home and small business wireless routers integrate the functions of a router, switch, and access point into one device;

6. Was any MAC or IP address lost during the wireless transfer? The IP addresses do not appear be lost during the transfers; The MAC addresses appear to change when introduced to an access point and then possibly return;
7. What was the highest OSI layer that the **Hub** and **Access Point** used? The Access Point used Layer 1 for its highest layer and so did the Hub;
8. Did the **Hub** or **Access Point** ever replicate a PDU that was rejected with a red “X”? The Access Point replicates and the Hub appears to replicate as well.
9. When examining the **PDU Details** tab, which MAC address appeared first, the source or the destination?

   - The destination appears to be first and the source appears to be after;

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

- The destination address may be on a different network than the source address;
- If the destination IPv4 address is on a different network than the source IPv4 address, the device will search the ARP table for the IPv4 address of the default gateway.
- If the device locates the IPv4 address, its corresponding MAC address is used as the destination MAC address in the frame.
- In cut-through switching, the switch acts upon the data as soon as it is received, even if the transmission is not complete. The switch buffers just enough of the frame to read the destination MAC address so that it can determine to which port to forward the data. The destination MAC address is located in the first 6 bytes of the frame following the preamble. The switch looks up the destination MAC address in its switching table, determines the outgoing interface port, and forwards the frame onto its destination through the designated switch port.
- The destination IP address may be on the same IP network as the source or may be on a remote network.
- When a NIC receives an Ethernet frame, it examines the destination MAC address to see if it matches the device's physical MAC address stored in RAM. If there is no match, the device discards the frame.
- For a unicast packet to be sent and received, a destination IP address must be in the IP packet header. A corresponding destination MAC address must also be present in the Ethernet frame header; The process that a source host uses to determine the destination MAC address is known as Address Resolution Protocol (ARP).
- Although the destination MAC address can be a unicast, broadcast, or multicast address, the source MAC address must always be a unicast.
- Destination MAC Address – This 6-byte field is the identifier for the intended recipient. As you will recall, this address is used by Layer 2 to assist devices in determining if a frame is addressed to them. The address in the frame is compared to the MAC address in the device. If there is a match, the device accepts the frame. It can be a unicast, multicast, or broadcast address.
- Source MAC Address – This 6-byte field identifies the frame's originating NIC or interface. It must be a unicast address.
- Introduction to v6 Networks

11. Was there a pattern to the MAC addressing in the simulation? No;

12. Did the switches ever replicate a PDU that was rejected with a red "X"? No;

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?

    - It appears to change at the 'Router' and sometimes at the 'Access Point'.

14. Which device uses MAC addresses starting with 00D0? Router initially toward the Src Mac Address;

15. To what devices did the other MAC addresses belong?

- The devices sending the message to the device receiving the message;

16. Did the sending and receiving IPv4 addresses switch in any of the PDUs? It appears to not change until the ping reaches its destination (the ping address is reached; then the addresses switch if you continue to ping);

17. If you follow the reply to a ping, sometimes called a *pong*, do the sending and receiving IPv4 addresses switch? When the ping address is reached, the addresses appears to switch, especially if one continues to fast forward the simulation of the topology;

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

- The src and the dest of the IPv4 have a consistent pattern with each device that a message is sent from. There appears to be a source, where the message was sent, and a destination, where the ping is addressed.

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

-Routers examine the destination IP address to determine the best path to forward the IP packet. This is similar to how the postal service forwards mail based on the address of the recipient.
-The router receives the information and sends the information to the appropriate receiver; Similar to the way mail is sent, received by the postal service (like the router) and then sent to the appropriate receiver.
-There must be a way to track the receiver and the sender with some devices to technically communicate the message being delivered;
- Introduction to v6 Networks

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

- Pv6 uses a similar process to ARP for IPv4, known as ICMPv6 neighbor discovery. IPv6 uses neighbor solicitation and neighbor advertisement messages, similar to IPv4 ARP requests and ARP replies.

- For an IPv6 address, the multicast MAC address begins with 33-33.
- The range of IPv4 multicast addresses is 224.0.0.0 to 239.255.255.255. The range of IPv6 multicast addresses begins with
- EtherType Field – This 2-byte field identifies the upper layer protocol encapsulated in the Ethernet frame. Common values are, in hexadecimal, 0 × 800 for IPv4, 0 × 86DD for IPv6 and 0 × 806 for ARP.
- Introduction to v6 Networks

Suggested Scoring Rubric

There are 20 questions worth 5 points each for a possible score of 100.