**7.1.6 Lab – Use Wireshark to Examine Ethernet Frames**

## Part 1:  Examine the Header Fields in an Ethernet II Frame

### Step 4:  Examine the Ethernet II header contents of an ARP request.

1. What is significant about the contents of the destination address field?

Answer: All hosts on the LAN will receive this broadcast frame. The host with the IP address of 192.168.1.1 (default gateway) will send a unicast reply to the source (PC host). This reply contains the MAC address of the NIC of the default gateway.

1. Why does the PC send out a broadcast ARP prior to sending the first ping request?

Answer: The PC cannot send a ping request to a host until it determines the destination MAC address, so that it can build the frame header for that ping request. The ARP broadcast is used to request the MAC address of the host with the IP address contained in the ARP.

1. What is the MAC address of the source in the first frame?

Answer: in this case, it is f0:1f:af:50:fd:c8.

1. What is the Vendor ID (OUI) of the Source NIC in the ARP reply?

Answer: in this case, it is Netgear

1. What portion of the MAC address is the OUI?

Answer: The first 3 octets of the MAC address indicate the OUI.

1. What is the NIC serial number of the source?

Answer: 99:c5:72 in this case.

## Part 2:  Use Wireshark to Capture and Analyze Ethernet Frames

### Step 1:  Determine the IP address of the default gateway on your PC.

1.What is the IP address of the PC default gateway?

Answer: 172.16.176.1

### Step 6:  Examine the first Echo (ping) request in Wireshark.

1. What is the MAC address of the PC NIC?

Answer: (90:9c:4a:bd:32:fc)

2. What is the default gateway’s MAC address?

Answer: (74:83:c2:78:a8:8f)

3. What type of frame is displayed?

Answer: 0x0800 IPv4.

4.What is the source IP address?

Answer: 172.16.188.102

5. What is the destination IP address?

Answer: 172.16.176.1

6. What do the last two highlighted octets spell?

Answer: hi

7. What device and MAC address is displayed as the destination address?

Answer:

Apple\_bd:32:fc, (90:9c:4a:bd:32:fc).

### Step 7:  Capture packets for a remote host.

1. In the first echo (ping) request frame, what are the source and destination MAC addresses?

Answer: 

1. Why has the destination IP address changed, while the destination MAC address remained the same?

Answer: Layer 2 frames never leave the LAN. When a ping is issued to a remote host, the source will use the default gateway MAC address for the frame destination. The default gateway receives the packet, strips the Layer 2 frame information from the packet and then creates a new frame header with the MAC address of the next hop. This process continues from router to router until the packet reaches its destination IP address.

1. Wireshark does not display the preamble field of a frame header. What does the preamble contain?

Answer: The preamble field contains seven octets of alternating 1010 sequences, and one octet that signals the beginning of the frame, 10101011.

## 7.2.7 Lab – View Network Device MAC Addresses Answers

## Part 1:  Configure Devices and Verify Connectivity

### Step 2:  Configure the IPv4 address for the PC.

1. Were the pings successful? Explain.

Answer: No. The switch has not been configured yet.

### Step 4:  Verify network connectivity.

1. Were the pings successful?

Answer: The pings should be successful.

## Part 2:  Display, Describe, and Analyze Ethernet MAC Addresses

### Step 1:  Analyze the MAC address for the PC-A NIC.

1. What is the OUI portion of the MAC address for this device?

Answer: 5C-26-0A

1. What is the serial number portion of the MAC address for this device?

Answer: 24-2A-60

1. Using the example above, find the name of the vendor that manufactured this NIC.

Answer: Dell Inc.

1. From the command prompt on PC-A, issue the **ipconfig /all**command and identify the OUI portion of the MAC address for the NIC of PC-A.

Answer: 00-90-21

1. Identify the serial number portion of the MAC address for the NIC of PC-A.

Answer: b1-8b-39

1. Identify the name of the vendor that manufactured the NIC of PC-A.

Answer: Cisco systems

### Step 2:  Analyze the MAC address for the S1 F0/6 interface.

1. What is the MAC address for VLAN 1 on S1?

Answer: 0060.5ca7.38cc

1. What is the MAC serial number for VLAN 1?

Answer: a7-38-cc

1. What is the OUI for VLAN 1?

Answer: 00-60-5c

1. Based on this OUI, what is the name of the vendor?

Answer: Cisco Systems.

1. What does bia stand for?

Answer: Burned in address.

1. Why does the output show the same MAC address twice?

Answer: The MAC address can be changed via a software command. The actual address (bia) will still be there. It is shown in the parenthesis.

1. What Layer 2 addresses are displayed on S1?

Answer: S1 VLAN 1 and PC-A MAC addresses

1. What Layer 3 addresses are displayed on S1?
2. Answer: S1 and PC-A IP addresses

### Step 3:  View the MAC addresses on the switch.

1. Did the switch display the MAC address of PC-A? If you answered yes, what port was it on?

Answer: Yes. Port should be F0/6.

# Reflection Questions

1. Can you have broadcasts at the Layer 2 level? If so, what would the MAC address be?

Answer: You can have broadcasts at Layer 2. ARP will use broadcasts to find MAC address information. The broadcast address is FF.FF.FF.FF.FF.FF.

1. Why would you need to know the MAC address of a device?

Answer: There could be a variety of reasons. In a large network, it may be easier to pinpoint location and identity of a device by its MAC address instead of its IP address. The MAC OUI will list the manufacturer, which may help narrow down the search. Security measures can be applied at Layer 2, so knowledge of allowable MAC addresses is needed.

# **7.3.7 Lab – View the Switch MAC Address Table**

Part 2: Examine the Switch MAC Address Table

1. What are the Ethernet adapter physical addresses?

Answer: PC-A MAC Address: 00-50-56-B3-27-D6.

PC-B MAC Address: 00-50-56-B3-FF-54.

1. S1 Fast Ethernet 0/1 MAC Address: 00d0.58e8.3201

S2 Fast Ethernet 0/1 MAC Address: 0040.0b25.5701

Step 2: Display the switch MAC address table

1. Are there any MAC addresses recorded in the MAC address table?

Изображение выглядит как стол

Автоматически созданное описание

2. Does the MAC address table have any addresses in it for VLAN 1? Are there other MAC addresses listed?

Answer: No. The student will most likely discover that the MAC address for the other switch’s F0/1 switch port has been quickly reinserted in the MAC address table.

What might be some of the challenges on larger networks?

Answer: ARP broadcasts could cause broadcast storms. Because ARP and switch MAC tables do not authenticate or validate the IP addresses to MAC addresses it would be easy to spoof a device on the network.