**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.