**Pre-Lab Week 5 – ARP with Wireshark (Windows)**

**Learning Objectives:**

* Capture ARP packets in Wireshark on a Windows PC.
* Identify ARP Requests and ARP Replies.
* Understand how ARP enables IP communication at the Data Link Layer.

**Part 1 – Setup (Windows)**

1. Open Wireshark.
2. Select your active network interface (likely Wi-Fi or Ethernet).
3. Open Command Prompt (Run as administrator) and clear the ARP cache, using command:

**arp -d**

**Note!!** \* If you forget to run Command Prompt as Administrator and see this **erro**r:

*“The ARP entry deletion failed: The requested operation requires elevation”*

**Fix:** Close the window, then re-open Command Prompt by Right-click → Run as Administrator and try again.

1. Still in Command Prompt ping an external host to generate traffic;

**ping cisco.com**

**Part 2: Capture ARP in Wireshark**

1. While pinging, Wireshark will capture ARP traffic
2. Stop the capture once a few packets are collected.
3. In the Display Filter bar, type: arp
4. Take a screenshot of the filtered output showing ARP packets, and paste it below:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Part 3: Analyze ARP Packets**

1. Filter for ARP Request only. (Hint: use the command/filter from your Week 5 command reference.
2. In your ARP Request packet, look under the Ethernet II header.

What is the Destination MAC Address shown? \_\_\_\_\_\_\_\_\_\_

Why is the destination listed as Broadcast (ff:ff:ff:ff:ff:ff) ?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. What does the value ff:ff:ff:ff:ff:ff represent? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
2. In the same ARP Request packet you capture, record:

What is the Target MAC Address? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

What is the Target IP Address? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Please attach your screen shot of the ARP request, below:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Filter just ARP Reply. (Hint: use the command from your week 5 command reference)
2. In the ARP Reply packet you capture, record:

What is the Sender MAC Address? \_\_\_\_\_\_\_\_\_\_\_\_\_\_

What is the Sender IP Address? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Please attach your screen shot of the ARP reply, below:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_