In this lab, I observed Address Resolution Protocol operations to learn how Layer 2 and Layer 3 interoperate using Wireshark.

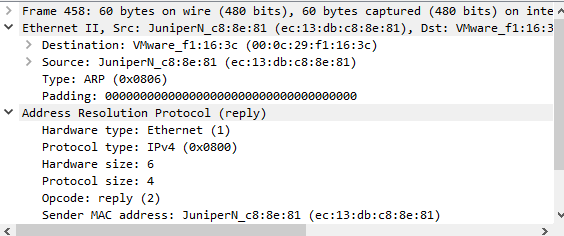
“arp -d” dumps the arp cache.

Link to tech journal: <https://github.com/seraphimgerber/NET-150>

default gateway = 192.168.3.250

**Deliverable 1: Find the ARP broadcast that your computer used to find the gateway's MAC address. Provide a screenshot that shows the source and destination MAC address of this broadcast.**

**Deliverable 2: Find the ARP reply from the gateway back to your computer. Provide a screenshot that shows the ARP reply packet indicating the MAC address for your gateway.**

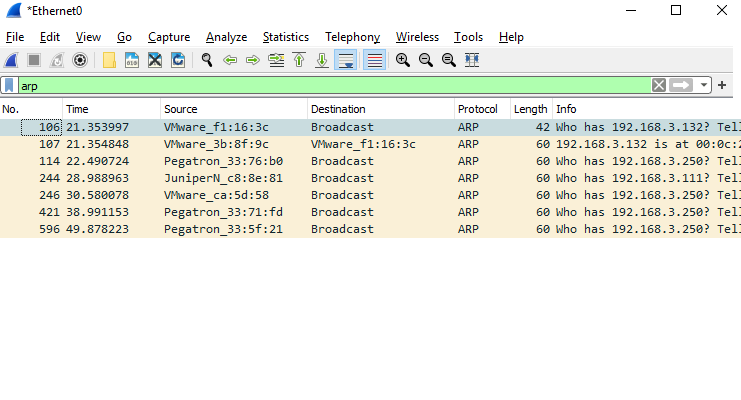


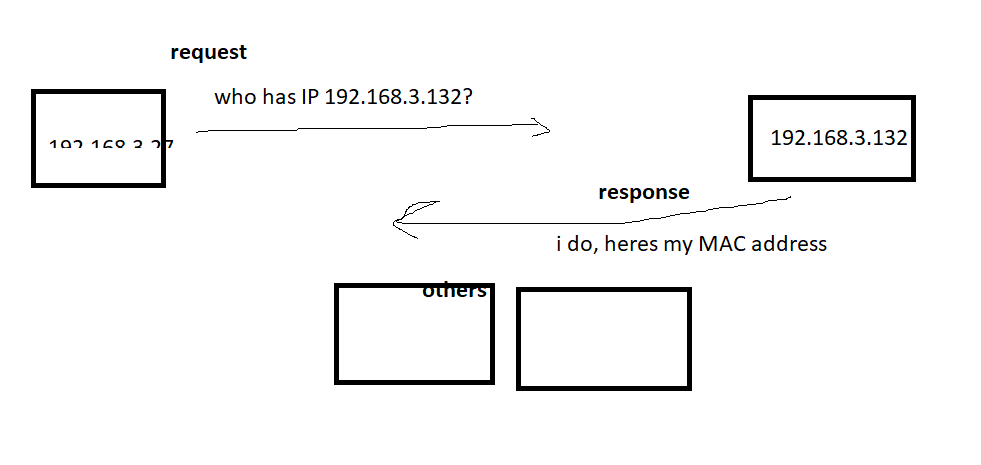
**Deliverable 3: What is the message sent in the ARP Request? What is the message sent in the ARP Reply?**

The message sent in the ARP Request is “Who has 192.168.3.250? Tell 192.168.3.27”

The message sent in the ARP Reply is “192.168.3.250 is at ec:13:db:c8:8e:81”

**Deliverable 4. Figure out how to create a display filter for ARP traffic only and provide a screenshot showing any ARP traffic related to your neighbor's system.**

**Deliverable 5. Using a piece of paper and a pencil/pen or even a whiteboard. Draw out the sequence of ARP request and Response to and from your neighbor. Take a picture of this with a mobile device and include it as part of your deliverable.**



**Deliverable 6. This is important. What do you see in the ARP request and reply? Can you discern the MAC address for the google DNS server or not? Can you explain what happened?**

It is the same as the request, but I cannot get an answer since it isn’t in the LAN. The ping command only searches for IP, and since I am not on the same LAN as google, I cannot get their MAC address.