**Layer 2 Lab**

The purpose of this lab is to understand ICMP, ARP, and the details of layer 2 headers used in network communication.

**Part 1**

First, let’s do a simple ping and examine the arp cache on your VM.

1. Start your CIT 247 Ubuntu VM and log in as student. The password is cit247.
2. Open a terminal window by right-clicking on your VM’s desktop and select Open Terminal. Find your IP address. (See the previous lab if you don’t remember how to do this.)

**Q1.1: What is the IP address that was assigned to your ens32 interface?**

**10.2.58.158**

**Q1.2: What is the MAC address of your ens32 interface?**

**00:50:56:b9:03:5a**

1. From your terminal window, ping 10.2.56.1. We will limit this to just one attempt by using the -c parameter. The command is **ping -c 1 10.2.56.1**. In the output, the ping statistics should show 0% packet loss. If not, try again. If you can’t get 0% packet loss, seek help on the discussion boards for this lab or from your instructor.
2. 10.2.56.1 is the IP address of your default gateway. Your default gateway is the router that provides you with connectivity to devices outside of the LAN that contains your VM. Examine the arp cache on your VM by issuing the **arp** command in your terminal window. Locate the entry with your default gateway’s IP address. (It’s probably the only entry, but there could be others.)

**Q1.3: What is the MAC address of your default gateway?**

**00:1d:71:f4:b0:00**

**Q1.4: Explain how the arp cache is used when you ping the default gateway.**

When you ping the default gateway, the arp cache is going to save the IP MAC address to the arp until the data is needed or times out.

Part 2

Next, let’s clear the arp cache and repeat the ping. This time, we’ll examine everything that is happening in detail with Wireshark.

1. Start Wireshark. Do this by issuing the command **sudo wireshark** in your terminal window.
2. Make sure there are no network applications (e.g. browsers) running on your VM.
3. Start a capture session on your Ethernet port by double-clicking on **ens32** in the Wireshark window.
4. Open another terminal window. Clear your arp cache by issuing the following command in your terminal window:

sudo ip -s neigh flush all

5. Once again, ping your default gateway using the command ping -c 1 10.2.56.1

1. Stop and save your Wireshark capture.
2. You should see an ICMP echo request packet and an ICMP echo reply packet in the packet list window of your Wireshark capture. (If you don’t see an echo request and echo reply, seek help from your instructor or the discussion board.) The echo request and echo reply were generated when you pinged 10.2.56.1. The echo request was sent from your VM to 10.2.56.1 and the echo reply was a response sent from 10.2.56.1 to your VM. The echo reply let your VM know that 10.2.56.1 is alive. It is important to understand that most communication between devices on a network involves traffic going both directions (aka request/reply).
3. Notice the frame numbers on the left of each packet in the packet list window. Wireshark generates these sequential numbers to help you identify each captured frame.

**Q2.1: What is the frame number of the echo request?**

**Frame 2978**

**Q2.2: What is the frame number of the echo reply?**

**Frame 2979**

1. Examine the Ethernet II data in the packet details window of the echo request and echo reply.

**Q2.3: List the following MAC addresses using xx:xx:xx:xx:xx:xx format:**

• **Source MAC address of the echo request:**

**00:50:56:b9:03:5a**• **Destination MAC address of the echo request:**

**00:1d:71:f4:b0:00**• **Source MAC address of the echo reply:**

**00:1d:71:f4:b0:00**

• **Destination MAC address of the echo reply:**

**00:50:56:b9:03:5a**

1. Prior to the ICMP packets in the packet list window, you should find two ARP packets related to your ping. There should be one that says, “**Who has 10.2.56.1? Tell *<your ip address>”***. This is the ARP request. You should also find an ARP reply saying that 10.2.56.1 is at xx:xx:xx:xx:xx:xx.

**Q2.4: What is the frame number of the ARP request?**

**Frame 2976  
Q2.5: What is the frame number of the reply to the above request?**

**Frame 2977**

**Q2.6: What is the source MAC address of the ARP request? What type of MAC address is this (unicast, multicast, broadcast)? What device was this frame sent from?**

**00:50:56:b9:03:5a**

**Unicast**

**The device was sent from frame 2976.**

**Q2.7: What is the destination MAC address of the ARP request? What type of MAC address is this? What devices does this destination address represent?**

**ff:ff:ff:ff:ff:ff**

**multicast/broadcast**

**The devices this destination address represent is all the frames or packets that are on being sent .**

**The device that this address represents is all the frames or packets that are being sent back to the host.**

***Submit your Wireshark capture file and responses to the questions on Canvas before the deadline.***