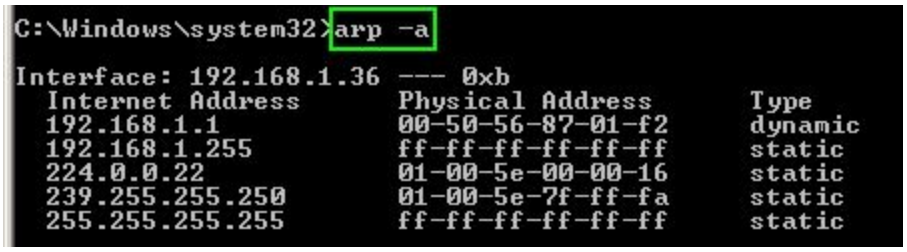
ARP Tables (GW)

ARP stands for Address Resolution Protocol. An IP address is the logical address of a computer, while the MAC address is the physical address of the computer. By using ARP, a computer can figure out another computer's MAC address by looking up the IP address in the table. ARP utilizes a table for IP to MAC translation.

A. Viewing the ARP Table

1. Open the **Command Prompt** by clicking on the Start button and typing **`cmd`** into the search box, then press Enter.
2. Type **`arp`** into the command line and press Enter. This will list information about ARP, as well as basic ARP commands. Read over the information.
3. Type **`arp -a`** and press Enter. The "arp -a" command is used to list the current ARP table.



In the above example, 192.168.1.36 is the IP address of the computer. 192.168.1.1 is the IP address of the **Default Gateway / DHCP Server**. Because the computer has **interacted** with the default gateway, the default gateway's IP address is listed in the ARP table as a dynamic entry.

4. Document your IP address, as well as your partner's IP address, below.

Your IP Address	Your Partner's IP Address

5. Ping your partner's computer by typing **`ping`** followed by his/her IP address. Below is an example:

```
C:\Windows\system32>ping 192.168.1.31

Pinging 192.168.1.31 with 32 bytes of data:
Reply from 192.168.1.31: bytes=32 time=1ms TTL=128
Reply from 192.168.1.31: bytes=32 time<1ms TTL=128
Reply from 192.168.1.31: bytes=32 time<1ms TTL=128
Reply from 192.168.1.31: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.31:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

6. Now that your computer has communicated with your partner's computer, check the ARP table again. Type **`arp -a`** into the command line.
7. Do you see any changes to the ARP table from the previous time you looked at it? You should see the addition of your **partner's IP address** as a **dynamic** entry, with the inclusion of your partner's **physical address**.
8. To confirm that the physical address is correct, type **`getmac -v`** into the command line. Locate the MAC address (the physical address of the Local Area Connection adapter) and share this information with your partner. Does your MAC address match the entry that your partner has in their ARP table?

```
C:\Users\Student1>getmac -v

Connection Name Network Adapter  Physical Address    Transport Name

============== ===============  ================== ============================
==============================
Local Area Conn Intel(R) PRO/10  00-50-56-87-00-5B   \Device\Tcpip_{E0B62666-8FF9
-4E9C-AFBC-B0FF0336C40D}
```

B. Modifying the ARP Table

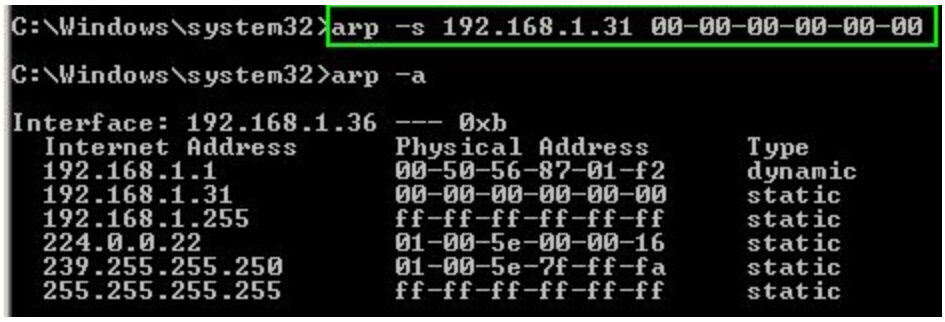
1. To remove an entry in the ARP table, the command is "**arp -d**" followed by the IP address of the entry you wish to delete. Try to delete your partner's computer from your ARP table, then view the table again. Below is an example:

```
C:\Windows\system32>arp -d 192.168.1.31

C:\Windows\system32>arp -a

Interface: 192.168.1.36 --- 0xb
  Internet Address      Physical Address      Type
  192.168.1.1           00-50-56-87-01-f2     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

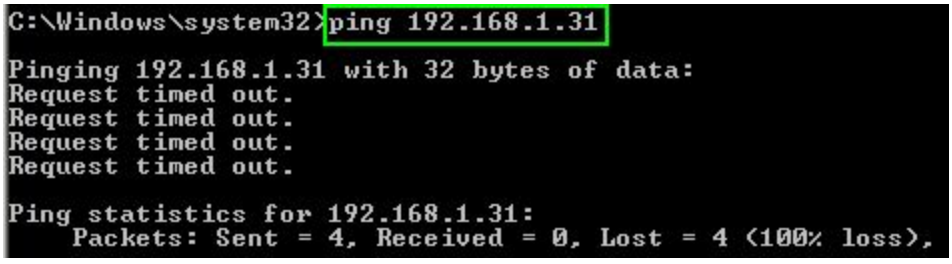
2. Now, your computer no longer has any record of your partner's MAC address. If you

were to interact with his/her computer again, the entry would be re-added. However, it is also possible to **manually enter the addresses as a static entry**.

3. If an attacker gains entry to someone's ARP table, the attacker can launch an **ARP spoofing attack** by manually adding an IP address, but assigning it the wrong MAC address on purpose. Because the two addresses do not match up, the data will not go where it is meant to, and other people **may not even be aware** that the ARP table was modified. In the next step, you will add your partner's computer to the ARP table once more, but this time, it will be done statically.
4. The correct format to add a static entry would be "**arp -s IPaddress MACaddress**". However, to demonstrate ARP spoofing, you will enter the correct IP address, but will **make up a fake MAC address** for your partner. An example is below:



5. Now that you have an incorrect static addition of your partner's computer in your ARP table, try to ping your partner's computer (type **`ping`** followed by their IP address). Is the ping successful?



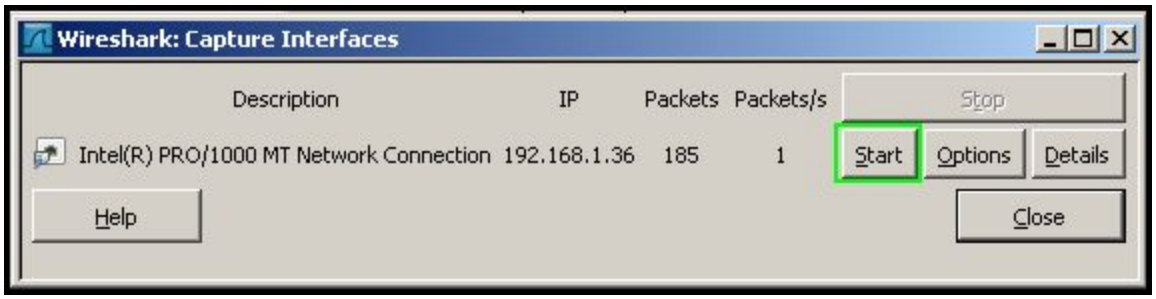
6. Because the IP address is not associated with its matching MAC address, the **connection cannot be made**. This could greatly impact the reliability of the network. In some cases, attacker's are able to edit an ARP table so that **confidential data is routed to the attacker's computer** instead of the computer the sender is intending it to go to.

Discuss with your partner the severity of the effects that could result from an attacker modifying an ARP table.

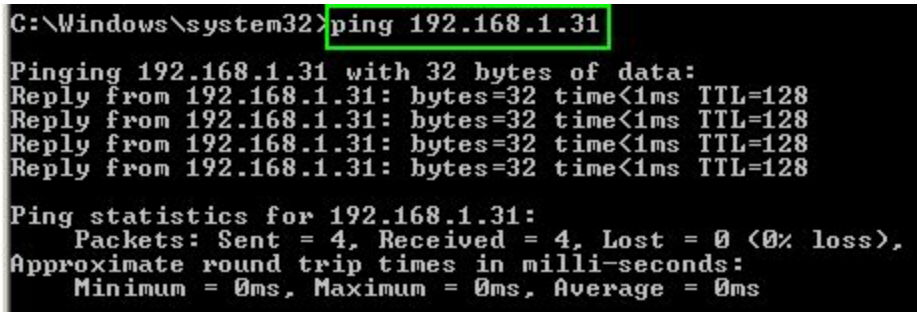
C. Capturing ARP Packets with Wireshark

Before starting this part of the activity, check your ARP table and remove any entries for your partner's IP address with the "**`arp -d`**" command. For this portion of the activity, you will use Wireshark to capture ARP packets.

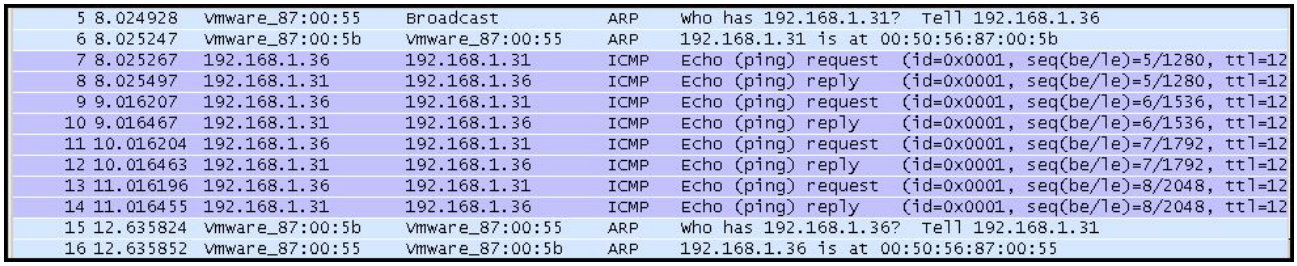
1. Open **Wireshark**. In the menu, select **Capture**, then click **Interfaces**. By clicking the **Start** button, Wireshark will begin to capture packets.



2. In the Command Prompt, type **`ping yourPartner'sIP`**, where "yourPartner'sIP" is your partner's IP address.



3. In Wireshark, stop capturing packets by clicking **Capture**, then clicking **Stop**. Notice that Wireshark has three main sections. The top section lists the captured packets, the middle section gives detailed information about the content of each packet, and the bottom section shows the raw data.
4. Look through the captured packets and search specifically for **ARP** and **ICMP** (Ping) packets. You should find that before the ping went to your partner's computer, an ARP broadcast first had to be sent to figure out your partner's MAC address. Then, the ping could go through. After the ping, there is another ARP request, this time coming from your partner's computer regarding the MAC address of your computer.



5	8.024928	vmware_87:00:55	Broadcast	ARP	Who has 192.168.1.31? Tell 192.168.1.36
6	8.025247	vmware_87:00:5b	vmware_87:00:55	ARP	192.168.1.31 is at 00:50:56:87:00:5b
7	8.025267	192.168.1.36	192.168.1.31	ICMP	Echo (ping) request (id=0x0001, seq(be/le)=5/1280, ttl=12
8	8.025497	192.168.1.31	192.168.1.36	ICMP	Echo (ping) reply (id=0x0001, seq(be/le)=5/1280, ttl=12
9	9.016207	192.168.1.36	192.168.1.31	ICMP	Echo (ping) request (id=0x0001, seq(be/le)=6/1536, ttl=12
10	9.016467	192.168.1.31	192.168.1.36	ICMP	Echo (ping) reply (id=0x0001, seq(be/le)=6/1536, ttl=12
11	10.016204	192.168.1.36	192.168.1.31	ICMP	Echo (ping) request (id=0x0001, seq(be/le)=7/1792, ttl=12
12	10.016463	192.168.1.31	192.168.1.36	ICMP	Echo (ping) reply (id=0x0001, seq(be/le)=7/1792, ttl=12
13	11.016196	192.168.1.36	192.168.1.31	ICMP	Echo (ping) request (id=0x0001, seq(be/le)=8/2048, ttl=12
14	11.016455	192.168.1.31	192.168.1.36	ICMP	Echo (ping) reply (id=0x0001, seq(be/le)=8/2048, ttl=12
15	12.635824	vmware_87:00:5b	Vmware_87:00:55	ARP	Who has 192.168.1.36? Tell 192.168.1.31
16	12.635852	vmware_87:00:55	Vmware_87:00:5b	ARP	192.168.1.36 is at 00:50:56:87:00:55

5. In the Command Prompt, enter **`arp -a`**. Notice that your partner's IP address and MAC address are recorded in the table.