### Part 1: Capture and Analyze Local ICMP Data in Wireshark

#### Step 1: Retrieve your PC interface addresses.

1. Does the source MAC address match your PC interface ?

Answer: Yes

1. Does the destination MAC address in Wireshark match your team member MAC address?

Answer: Yes

1. How is the MAC address of the pinged PC obtained by your PC?

Answer: The MAC address is obtained through an ARP request.

### Step 2:  Examining and analyzing the data from the remote hosts.

1. What is significant about this information?

Answer: The MAC addresses for all three locations are the same.

1. How does this information differ from the local ping information you received in Part 1?

Answer: A ping to a local host returns the MAC address of the PC NIC. A ping to a remote host returns the MAC address of the default gateway LAN interface.

Reflection Question

Why does Wireshark show the actual MAC address of the local hosts, but not the actual MAC address for the remote hosts?

Answer: MAC addresses for remote hosts are not known on the local network, so the MAC address of the default-gateway is used. After the packet reaches the default-gateway router, the Layer 2 information is stripped from the packet and a new Layer 2 header is attached with the destination MAC address of the next hop router.