Lab 9
ARP and ICMP

Prof. Kredo

Due: Start of lab Friday, April 10

Name:	
Name:	

Introduction

In this lab you will accomplish several goals:

- Explore ARP and the ARP cache of your host
- Examine how ICMP provides network diagnostics

Work in pairs for this lab using the equipment at your desk. Distribute the work evenly to make sure both group members know the material, as you will be required to know the material for evaluation.

1 Preliminary

Read and use the directions in this lab **carefully** as you can put your devices in an unusable state if you make errors. Reconfiguring your devices from scratch takes time and will delay your work on this lab.

Before working with any lab equipment, reset all devices to a known configuration. Follow the reset instructions posted on the bulletin board and on Learn. You will need one switch and one router for this lab.

Setup your network by connecting and configuring your devices according to the Lab 9 Diagram. Fill in the diagram with the addresses you select for the devices.

Entries in an ARP cache can be in one of several states. A valid entry is in the `REACHABLE` state. Entries in the `FAILED` or `STALE` state are considered incorrect or old and are not used by the operating system. If you see an entry in the `DELAY` state, then wait a couple seconds and display the ARP cache again to determine the final state.

2 ARP [30 Points]

You studied in class how ARP allows devices to find a data link layer (Ethernet) address for a known network layer (IP) address. In this section you will explore ARP and the cache stored by your host. You can view the ARP cache for your host by typing the command `ip neighbour` in a terminal of your host.

1. How many entries are in your ARP cache? Identify the machines corresponding to two of those entries.

2. If you pinged your router's lower interface right now, would your host generate an ARP request? Why or why not?

Lets clear out the ARP cache. Look at the man page for `ip` and delete all the entries in your ARP cache. Remember you will have to type `sudo ip` into the terminal to get the correct permissions.

3. What *single* command clears your ARP cache?

4. Ping your router's lower interface. Did the entry for your router's lower interface (re)appear in your ARP cache?

5. Attempt to ping an unused (not assigned to any device) IP address in your subnetwork. What does your ARP cache contain for that IP address?

Start a packet capture on eth0 and capture some ARP exchanges. You may need to modify your ARP cache and generate some traffic so your host sends ARP packets. Be sure to capture ARP requests and ARP replies.

6. Hardware size and Protocol size are two fields in ARP packets. What are they measuring the size of?

3 ICMP

ICMP provides diagnostics and error messages between devices for such things as connectivity tests (ping) and routing problems (destination unreachable).

3.1 ICMP ECHO [40 Points]

Let's first look at ECHO Request and ECHO Reply messages, more commonly known as ping packets. Start a new packet trace on the eth0 interface of your host and ping an interface on your router. Answer the following questions about the ECHO packets.

1. What's in the data portion of the ECHO Request? How does the relate to the ECHO Reply?

2. What is the Identifier value for the ICMP message sequence? What is the purpose of this field?

   Restart your packet capture on eth0 and ping an IP address (not a hostname) that lies outside all IP networks in the lab (outside 10.0.0.0/8 and 192.168.0.0/16).

3. What new ICMP message do you see?

4. Which device sent the message? What is the message telling your host?

Restart your packet capture on eth0 and ping an unused IP address within your host's network.

5. Are you able to ping the IP address? Do you see any ICMP messages in your packet trace?

Restart your packet capture on the **any** interface and ping the unused IP address again. When capturing on this interface you will not see any Ethernet headers. Look at the packets you captured and other pertinent information to answer the following questions.

6. What are the Destination and Source IP addresses for the ICMP messages?

7. What is odd about the ICMP IP addresses in the previous question? Why didn't you see them when capturing packets on the eth0 interface?

8. Looking at all the data you've collected and what you know about the network protocols you've studied, explain what happens when you ping an unused IP address in the same network as your host. Include all the packets listed in your capture and the reason they are sent in your explanation.

3.2 ICMP and `traceroute` [30 Points]

Reconnect and reconfigure your hosts to access the EXT network; you are done with the router and switch at this point and you may leave them disconnected. Ensure you have connectivity by `ping`ing an address outside the lab.

The `traceroute(8)` program introduced in an earlier lab relies on ICMP to discover the path packets take to a host. Before investigating how `traceroute` operates, try to find a host that you can reach with `traceroute` that (1) has mostly valid entries (few *** lines), (2) has a relatively small number of hops (12 or less is good), and (3) is off campus. Search for a host that satisfies these requirements before you continue.

Begin a new packet capture and perform a `traceroute` on the host you selected using the `-n` option, which shows you IP addresses instead of hostnames. When `traceroute` completes, stop your capture and save your file for later reference.

1. Take a look at your packet trace and try to deduce how `traceroute` finds the path taken by packets to reach a host. Using data from your packet trace, explain how `traceroute` operates.

If the host you selected has invalid entries (*** lines), then answer the next question. If your host did not have any invalid entries, then pick another host and perform a packet capture while you run `traceroute` to that host and answer the next question.

2. What do you think has happened when `traceroute` displays an invalid entry (*** line)?

Submit your completed lab handout by the next lab.

Lab 9 Diagram