In this lab, we’ll explore several aspects of the ICMP protocol:

- The Internet Control Message Protocol (ICMP) is one of the core protocols of the Internet Protocol Suite.
- ICMP messages generating by the Ping program;
- ICMP messages generated by the Traceroute program;
- the format and contents of an ICMP message.

I. ICMP and Ping

Let’s begin our ICMP adventure by capturing the packets generated by the Ping program. You may recall that the Ping program is simple tool that allows anyone (for example, a network administrator) to verify if a host is live or not. The Ping program in the source host sends a packet to the target IP address; if the target is live, the Ping program in the target host responds by sending a packet back to the source host. As you might have guessed (given that this lab is about ICMP), both of these Ping packets are ICMP packets.

Begin:

- Let’s begin this adventure by opening the Windows Command Prompt application (which can be found in your Accessories folder).
- Start up the Wireshark packet sniffer, and begin Wireshark packet capture.
- The ping command is in c:\windows\system32, so type “ping –n 10 hostname”. The argument “-n 10” indicates that 10 ping messages should be sent. Then run the Ping program by typing return.
- When the Ping program terminates, stop the packet capture in Wireshark.

Once the ping command is complete you should see ten replies from the destination address and at the bottom there should be ping statistics which include the percentage received and loss as well as the round trip time.

In the Wire Shark window there maybe many different connections taking place at once so in order to separate all other packet transmissions from the ICMP ping that we are focused on you will need to type “icmp” in the filter bar and then click apply, this should leave on the ICMP packets in the results for the capture. Observe that this ICMP packet is of Type 8 and Code 0 - a so-called ICMP “echo request” packet. Also note that this ICMP packet contains a checksum, an identifier, and a sequence number.
Questions

You should hand in a screen shot of the Command Prompt inserted in your word document. Whenever possible, when answering a question below, you should hand in a printout of the packet(s) within the trace that you used to answer the question asked. Annotate the printout to explain your answer. To print a packet, use File->Print, choose Selected packet only, choose Packet summary line, and select the minimum amount of packet detail that you need to answer the question. If you cannot print then use a screenshot and type the necessary information.

1. What is the IP address of your host? What is the IP address of the destination host? **Host: 10.0.0.11  Destination: 209.191.122.70 (www.yahoo.com)**

2. Why is it that an ICMP packet does not have source and destination port numbers? **ICMP does not use a port; it is an echo-reply protocol not a communication protocol.**

3. Examine one of the ping request packets sent by your host. What are the ICMP type and code numbers? **ICMP type: 8 code: 0**
   What other fields does this ICMP packet have? **The ICMP packet contains a checksum, an identifier, and a sequence number.**
   How many bytes are the checksum, sequence number and identifier fields?
   - **Checksum:** 0x4d0
   - **Identifier (Be):** 1
   - **Identifier (Le):** 256
   - **Sequence number (Be):** 77
   - **Sequence number (Le):** 197122

4. Examine the corresponding ping reply packet. What are the ICMP type and code numbers? **ICMP type: 0 code: 0**
   What other fields does this ICMP packet have? **The ICMP packet contains a checksum, an identifier, and a sequence number**
   How many bytes are the checksum, sequence number and identifier fields?
   - **Checksum:** 0x550e
   - **Identifier (Be):** 1
   - **Identifier (Le):** 256
   - **Sequence number (Be):** 77
   - **Sequence number (Le):** 197122
Windows Command Prompt: “ping -n 10 www.yahoo.com”

Packets Within Trace Used to Answer Questions
II. Using Tracert

Ping is a computer network administration utility used to test the reachability of a host on an Internet Protocol (IP) network and to measure the round-trip time for messages sent from the originating host to a destination computer. Ping operates by sending Internet Control Message Protocol (ICMP) echo request packets to the target host and waiting for an ICMP response. In the process it measures the time from transmission to reception (round-trip time)\[1\] and records any packet loss.

The next program that we will be using is called the trace route program. This is similar to the “Ping” program and can be ran by simply typing “tracert” followed by the host that you would like to trace. Example “tracert www.google.com”.

Traceroute is implemented in different ways in Unix/Linux and in Windows. In Unix/Linux, the source sends a series of UDP packets to the target destination using an unlikely destination port number; in Windows, the source sends a series of ICMP packets to the target destination. For both operating systems, the program sends the first packet with TTL=1, the second packet with TTL=2, and so on. Recall that a router will decrement a packet’s TTL value as the packet passes through the router. When a packet arrives at a router with TTL=1, the router sends an ICMP error packet back to the source.

Begin:
- Let’s begin by opening the Windows Command Prompt application (which can be found in your Accessories folder).
- Start up the Wireshark packet sniffer, and begin Wireshark packet capture.
- The tracert command is in c:\windows\system32, so type “tracert hostname”.
- Try to use locations outside of the US to get a longer Trace. I.E w\[www.inria.fr\]
- When the Traceroute program terminates, stop packet capture in Wireshark.

Notes:
Once the Tracert is complete you should be provided with information such as the amount of hops to complete route, and the time it took to get from each router in between the source and destination route.

Questions
You should hand in a screen shot of the Command Prompt inserted in your word document. Whenever possible, when answering a question below, you should hand in a printout of the packet(s) within the trace that you used to answer the question asked. Annotate the printout to explain your answer. To print a packet, use File->Print, choose Selected packet only, choose Packet summary line, and select the minimum amount of packet detail that you need to answer the question. If you cannot print then use a screenshot and type the necessary information.

5. What is the IP address of your host? What is the IP address of the target destination host? **Host: 168.223.219.243 Destination: 168.223.218.1**

6. If ICMP sent UDP packets instead (as in Unix/Linux), would the IP protocol
number still be 01 for the probe packets? If not, what would it be? No, it would be 08 instead of 01.

7. Examine the ICMP echo packet in your screenshot. Is this different from the ICMP ping query packets in the first half of this lab? If yes, how so? No

8. Examine the ICMP error packet in your screenshot. It has more fields than the ICMP echo packet.

   What is included in those fields? The length is larger and it The packet is ICMP type: 3 (destination unreachable) and code: 13 (communication administratively filtered) is included.

9. Examine the last three ICMP packets received by the source host.

   How are these packets different from the ICMP error packets? These packets differ in that they have ICMP type: 0 code: 0.

   Why are they different? They are different because they never reached the destination; they got dropped.
Windows Command Prompt: “tracert 168.223.218.1”

Packets Within Trace Used to Answer Questions (Tracert)