Wireshark Lab 1, part b: ICMP

In this portion of the lab, we will explore several aspects of the ICMP protocol:

- ICMP messages generated by the Ping program;
- ICMP messages generated by the Traceroute (tracert) program;
- the format and contents of an ICMP message.

Before attacking this lab, you are encouraged to review the ICMP material in the textbook (Section 4.4.3 in the 4th edition of the textbook.) We present this lab in the context of the Microsoft Windows operating system. However, it is straightforward to translate the lab to a Unix or Linux environment.

1. ICMP and Ping

You will begin 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 on-line 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.

To capture the packet stream generated by a ping do the following:

- Begin by opening the Windows Command Prompt window: Select “Run…” from the Windows Start menu and type “cmd” (without the quotes) in the text box and hit “OK”

- Start up the Wireshark packet sniffer, and begin Wireshark packet capture.

- At the Windows command prompt, type:
  
  ping –n 10 www.ust.hk

  to ping the web server at the Hong Kong University of Science and Technology. The argument “-n 10” indicates that 10 ping messages should be sent. If your path environment is not set up to find the ping command, you may need to use the complete path name:

  c:\windows\system32\ping –n 10 www.ust.hk

- When the Ping program terminates, stop the packet capture in Wireshark.

At the end of the experiment, your Command Prompt Window should look something like Figure 1. From this window we see that the source ping program sent 10 query packets and received 10 responses. Note also that for each response, the source calculates the round-trip time (RTT), which for the 10 packets is on average 224 msec.
Figure 1 Command Prompt window after entering Ping command.

Figure 2 provides a screenshot of the Wireshark output, after “icmp” has been entered into the filter display window. Note that the packet listing shows 20 packets: the 10 Ping queries sent by the source and the 10 Ping responses received by the source. Also note that the source’s IP address is 128.255.16.146 and the destination’s IP address is that of the Web server at HKUST. Now let’s zoom in on the first packet (sent by the client); in the figure below, the packet contents area provides information about this packet. We see that the IP datagram within this packet has protocol number 01, which is the protocol number for ICMP. This means that the payload of the IP datagram is an ICMP packet.
Figure 2 Wireshark output for Ping program with Internet Protocol expanded.

Figure 3 focuses on the same ICMP but has expanded the ICMP protocol information in the packet contents window. Observe that this ICMP packet is of Type 8 and Code 0 - a so-called ICMP “echo request” packet. (See Figure 4.23 of text.) Also note that this ICMP packet contains a checksum, an identifier, and a sequence number.
Figure 3 Wireshark capture of ping packet with ICMP packet expanded.

What to Hand In:

You should hand in a screen shot of the Command Prompt window similar to Figure 1 above. 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.

You should answer the following questions:

1. What is the IP address of your host? What is the IP address of the destination host?
2. Why is it that an ICMP packet does not have source and destination port numbers?
3. Examine one of the ping request packets sent by your host. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields?
4. Examine the corresponding ping reply packet. What are the ICMP type and code numbers? What other fields does this ICMP packet have? How many bytes are the checksum, sequence number and identifier fields?
2. ICMP and Traceroute

Now we will continue our investigation of ICMP by capturing the packets generated by the `tracert` program. You may recall that the `tracert` program can be used to figure out the path a packet takes from source to destination. `Tracert` is discussed in Section 1.6 and in Section 4.4 of the text.

Traceroute (`tracert`) 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. In the following, we will use the native Windows `tracert` program.

To capture the packet stream generated by a `tracert` command, do the following:

- Begin by opening the Windows Command Prompt window
- Start up the Wireshark packet sniffer, and begin Wireshark packet capture.
- At the Windows command prompt, enter:
  
  `tracert www.inria.fr`
  
  to trace the route to the web server at INRIA, a research institute in France. If your path environment is not set up, you may need to use the full path name:
  
  `c:\windows\system32\tracert www.inria.fr`
  
- When the Traceroute program terminates, stop packet capture in Wireshark.

At the end of the experiment, your Command Prompt Window should look something like Figure 4. From this figure we see that for each TTL value, the source program sends three probe packets. `Tracert` displays the RTTs for each of the probe packets, as well as the IP address (and possibly the name) of the router that returned the ICMP TTL-exceeded message.
Figure 4 Command Prompt window displays the results of the Traceroute program.

Figure 5 displays the Wireshark window for an ICMP packet returned by a router. Note that this ICMP error packet contains more fields than the Ping ICMP messages.
What to Hand In:

For this part of the lab, you should hand in a screenshot of the Command Prompt window. Whenever possible, when answering the questions 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.

Answer the following questions:

1. What is the IP address of your host? What is the IP address of the target destination host?
2. 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?
3. 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?
4. Examine the ICMP error packet in your screenshot. It has more fields than the ICMP echo packet. What is included in those fields?
5. Examine the last three ICMP packets received by the source host. How are these packets different from the ICMP error packets? Why are they different?
6. Within the tracert measurements, is there a link whose delay is significantly longer than others? Refer to the screenshot in Figure 4, is there a link whose delay is significantly longer than others? On the basis of the router names, can you guess the location of the two
routers on the end of this link?