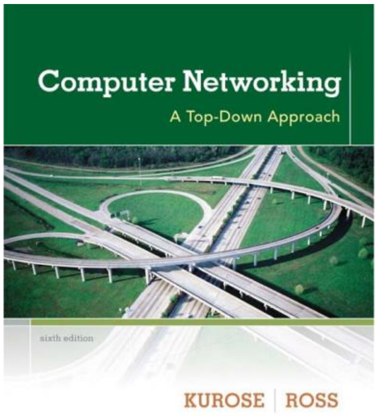
Wireshark Lab: ICMP v6.0

Supplement to *Computer Networking: A Top-Down Approach, 6th ed.*, J.F. Kurose and K.W. Ross

"Tell me and I forget. Show me and I remember. Involve me and I understand." Chinese proverb



Introduction

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

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

1. 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. Both of these Ping packets are ICMP packets.

Do the following:

- Let's begin by opening the Windows Command Prompt application *(Capture->Start)* and then press *OK* on the Wireshark Packet Capture Options screen (we'll not need to select any options here).
- Start up the Wireshark packet sniffer, and begin Wireshark packet capture.
- The ping command is in c:\windows\system32, so type either "ping –n 10 hostname" or "c:\windows\system32\ping –n 10 hostname" in the MS-DOS command line (without quotation marks), where hostname is a host on another continent. You can use the www.inria.fr 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.

What to hand in

You should hand in a screen shot of the Command Prompt window showing Ping packets sent and received including the RTT calculated. 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.

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? How is identification done?**
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? Explain each field in a line.**
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? Are there any additional fields in the reply packet? If yes, explain those fields as well.**

2. ICMP and Traceroute

Let's now continue ICMP by capturing the packets generated by the Traceroute program. You may recall that the Traceroute program can be used to figure out the path a packet takes from source to destination. Traceroute is implemented in different ways in Unix/Linux/MacOS 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. In the following, we'll use the native Windows *tracert* program.

Do the following:

- 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 either "tracert hostname" or "c:\windows\system32\tracert hostname" in the MS-DOS command line (without quotation marks), where hostname is a host on another continent. You use www.inria.fr for the Web server at INRIA, a computer science research institute in France. Then run the Traceroute program by typing return.
- When the Traceroute program terminates, stop packet capture in Wireshark.

What to hand in

For this part of the lab, you should hand in a screen shot of the Command Prompt window. 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.

Answer the following questions:

5. **What is the IP address of your host? What is the IP address of the target destination host?**
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?**
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?**
8. **Examine the ICMP error packet in your screenshot. It has more fields than the ICMP echo packet. What is included in those fields?**

9. **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?**
10. **Within the tracert measurements, is there a link whose delay is significantly longer than its previous links? On the basis of the router names, can you guess the location of the two routers on the end of this link (if any)?**

Modified by: Ifrah Saeed