Wireshark Exercise 2

Probing the Internet (ICMP, PING, Traceroute)

Objective

In this exercise we investigate two applications of the Internet Control Message Protocol (ICMP): 1. PING uses ICMP to determine whether a host is reachable: 2. Traceroute uses ICMP to allow users to determine the route that an IP packet takes from a local host to a remote host.

Protocols Examined

- ICMP: Echo, Echo Reply, Time Exceeded messages.
- IP Time-to-Live
- PING application
- Traceroute application

Background Material

Textbook pages: Chapter 4 (pages 163 - 166).
RFC: ICMP (RFC 792, http://www.freesoft.org/CIE/RFC/792/1.htm).
PING, Traceroute commands: Consult your system documentation for information on using these commands. For example, in Windows XP, start "Help and Support", then enter "ping" or "tracert" in the search window and press Enter.

Procedure

PING

1. Prepare Wireshark for a packet capture.
2. Open a Command Prompt window. (In Windows XP, from the "All Programs" Menu, select "Accessories" and then "Command Prompt").
3. Type "PING <website>"; Do NOT press ENTER.
4. Start Wireshark packet capture.
5. Press ENTER in Command Prompt window. You should obtain a series of replies as shown in Figure 2.26 in the textbook.
6. Stop packet capture when Command Prompt returns.
7. Save the contents in the Command Prompt window using a screen capture (Alt PrtSc).

Traceroute

1. Prepare Wireshark for a packet capture.
2. Open a Command Prompt window. (In Windows XP, from the "All Programs" Menu, select "Accessories" and then "Command Prompt").
3. Type "tracert <website>"; Do NOT press ENTER.
4. Start Wireshark packet capture.
5. Press ENTER in Command Prompt window. You should obtain a series of replies as shown in Figure 2.27 in the textbook.

6. Stop packet capture when Command Prompt returns.
7. Save the contents in the Command Prompt window using a screen capture (Alt PrtSc).
8. If the series of replies is very long, then you may wish to capture the replies in a text file by using the command: "tracert <website> > <filename>".

Protocol Analysis Questions

To answer the following questions, start Wireshark and open the packet capture file created above.

1. ***PING Protocols Captured***.
   - Examine the protocol column in the top pane of the Wireshark window. You will find a series of ICMP packets. It is likely that these ICMP packets are preceded by a DNS query/response message pair.
   - Identify the IP address returned in the DNS response message.
2. ***ICMP Echo Request***
   - Examine the IP packet that carries the first ICMP Echo Request. What is the destination IP address in the IP packet? What is the protocol type? What is the Time-to-Live?
   - Next examine the ICMP message. What is the ICMP message type? What is the message identifier and sequence number?
   - Highlight the data bytes carried in the request message. Note the corresponding character sequence in the third pane of the Wireshark window.
3. ***ICMP Echo Reply***
   - What are the source and destination addresses in the IP packet that carries the first ICMP Echo Reply? What are the protocol type and the Time-to-Live?
   - Now examine the ICMP reply message. What is the ICMP message type? Compare the message identifier and sequence number in the reply message with the corresponding numbers in the request message?
   - Highlight the data bytes in the reply message and compare the data sequence with that in the request message.
4. ***Repeat*** steps 2 and 3 for the remaining Echo request and Echo reply messages.
   - How do the identifier and sequence numbers change with time?
   - Does the data sequence in the request and reply messages change?
   - Calculate the time that elapses between the sending of each Echo request and the receipt of the corresponding Echo reply. Compare the maximum, average, and minimum of the delays with those provided by the PING command.
5. ***Traceroute Protocols Captured***.
   - Examine the protocol column in the top pane of the Wireshark window. You will find a series of ICMP packets. Once again, it is likely that these ICMP packets are preceded by a DNS query/response message pair.
   - Identify the IP address returned in the DNS response message.
6. ***ICMP Echo Request***

- Determine the destination address in the IP packet that carries the first ICMP Echo Request. Compare to the address returned by the DNS response message. What are the protocol type and the Time-to-Live in the IP packet?
- Record the header of the IP packet for future reference.
- Examine the ICMP message. What is the ICMP message type? What are the message identifier and sequence number?
- How many data bytes are carried in the request message? Note the character sequence corresponding to the data bytes in the third pane of the Wireshark window.

7. ICMP Time Exceeded

- What are the source and destination addresses in the IP packet that carries the ICMP Time Exceeded message?
- Now examine the ICMP message. What is the ICMP message type?
- The ICMP Type, Code, and Checksum are followed by 32 zeros and then by the IP header of the ICMP Echo Request Message. Compare the returned IP header to the IP header noted in step 6.
- Does the ICMP message carry any additional data?
- Next compare the message identifier and sequence number in the Time Exceeded message with the corresponding numbers in the request message?

8. ***Repeat*** steps 6 and 7 for the remaining Echo request and Time Exceeded messages.
   - Track the evolution of the TTL in the Echo request packets. Are there any repeated values of TTL? Is there a pattern to the repetitions?
   - List the sequence of the source IP addresses in the packets that carry the ICMP Time Exceeded messages. Compare to the list provided by Traceroute.
   - What is the received ICMP message when the ICMP Echo reply finally reaches the desired host?
   - Calculate the time that elapses between the sending of each Echo request and the receipt of the corresponding Time-Exceeded message. Compare the delay values obtained with the results provided by the Traceroute command.