Wireshark ICMP lab quiz

Due 10 May at 17:00 **Points** 9 **Questions** 9 **Available** until 17 May at 17:00
Time limit None **Allowed attempts** 5

Take the quiz again

Attempt history

	Attempt	Time	Score
LATEST	Attempt 1	1,198 minutes	9 out of 9

(!) Correct answers will be available 10 May at 17:05 - 20 Jun at 17:00.

Score for this attempt: 9 out of 9
Submitted 5 May at 11:09
This attempt took 1,198 minutes.

Last attempt details:

Time:	1,198 minutes
Current score:	9 out of 9
Kept score:	9 out of 9

4 More Attempts available

Take the quiz again

(Will keep the average of all your scores)

Question 1

1 / 1 pts

Wireshark Lab: ICMP v7.0

Adapted from Supplement to *Computer Networking: A Top-Down Approach, 7th 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

© 2005-2016, J.F Kurose and K.W. Ross, All Rights Reserved

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.

Before attacking this lab, you're encouraged to review the ICMP material in section 5.6 of the text[1]. ICMP is the Internet Control Message Protocol which allows network devices (like routers) to send information about errors or current state.

1. ICMP and Ping

Let's begin our ICMP adventure by capturing the packets generated by the Ping program. 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.

Do the following[2]:

- Let's begin this adventure by opening a terminal (Linux/MacOS or 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 /usr/sbin/ (usr/sbin32, so type either "ping -n 10 hostname" or "/usr/sbin/ping -n 10 hostname" in the Windows MS-DOS command line (without quotation marks) or for Mac/Linux type "ping -c 10 hostname" on the command line (again without quotation marks), where hostname is a host on another continent. If you're outside of Asia, you may want to enter www.uct.ch for the Web server at Hong Kong University of Science and Technology. The argument "-n 10" (windows) or "-c 10" (unix/mac) 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.

At the end of the experiment, your Command Prompt Window should look something like Figure 1. In this example, the source ping program is in Adelaide and the destination Ping program is in Massachusetts, USA. 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 375 msec.

Figure 1 Command Prompt window after entering Ping command.

Figure 2 provides a screenshot of the Wireshark output, after "Ping" 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 a private address (behind a NAT) of the form 192.168.0.12; the destination's IP address is that of the Web server at University of Massachusetts. 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.

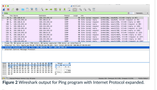

Figure 2 Wireshark output for Ping program with Internet Protocol expanded.

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 5.19 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.

Answer the following questions:

When using echo request/reply ICMP does not use port numbers (as TCP and UDP do). Why?

[1] References to figures and sections are for the 7th edition of our text, Computer Networks, A Top-down Approach, 7th ed., J.F. Kurose and K.W. Ross, Addison-Wesley/Pearson, 2016.

[2] If you are unable to run Wireshark live on a computer, you can download the zip file http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip (7z and extract the file ICMP-ethereal-trace-1. The traces in this zip file were collected by Wireshark running on one of the author's computers, while performing the steps indicated in the Wireshark lab. Once you have downloaded the trace, you can load it into Wireshark and view the trace using the File pull down menu, choosing Open, and then selecting the ICMP-ethereal-trace-1 trace file. You can then use this trace file to answer the questions below.

- Any process that has an ICMP socket is interested in "all" ICMP messages
- The ICMP messages are passed up to TCP/UDP for demultiplexing
- only one ICMP socket is allowed at a time, so it is delivered to that socket.
- Messages not associated with a particular TCP/UDP port use the identifier field to (demultiplex.

correct

Question 2

1 / 1 pts

ICMP echo request is ICMP type 0 code 0

- True
- False

Question 3

1 / 1 pts

Look at the ICMP types-least at the Internet Addresses and Name Authority (5). What ICMP type is used for multiple different errors (with different codes) related to being unable to reach the destination?

Enter the number.

3

Question 4

1 / 1 pts

Which of the following **ICMP** fields are the same between matching echo request and echo replies?

(choose ALL that apply)

- data
- type
- code
- identifier
- sequence number
- checksum

Question 5

1 / 1 pts

2. ICMP and Traceroute

Let's now continue our ICMP adventure by capturing the packets generated by the Traceroute program. The Traceroute program can be used to figure out the path a packet takes from source to destination. Traceroute is discussed in Section 1.4 and in Section 5.6 of the text.

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. For the first set of packets, the source sets the TTL field in the first packet to send 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. 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.

Do the following[1]:

- Let's begin by opening the Windows Command Prompt application (which can be found in your Accessories folder) or a Mac/Unix terminal.
- Start up the Wireshark packet sniffer, and begin Wireshark packet capture.
- The tracert command is in /usr/sbin/ (usr/sbin32, 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. (Note that on a Windows machine, the command is "tracert" and not "traceroute") For Mac/Unix the command is "traceroute hostname". If you are working in the labs, most student labs are not allowed to execute traceroute. If you are not able to run traceroute on the lab computer you can use the traceroute web page (5) provided by Telstra . If you're outside of Europe, you may want to enter www.ist.ch for the Web server at ENSIA, 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.

At the end of the experiment, your window should look something like Figure 4. In this figure, the client Traceroute program is in Adelaide and the target destination is in France. From this figure we see that for each TTL value, the source program sends three probe packets. Traceroute 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.

Note the lines with " * ". These are cases where the echo request (ping) did not get a reply. The can be due to timeout, but if all 3 are missing it is generally an indication that the router does not respond to ping requests. If you get several in a row, you are unlikely to be able to determine any router information beyond the last shown router. The web based trace route will stop as soon as it receives 3 failed pings.

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

Figure 5 Wireshark window of ICMP fields expanded for one ICMP error packet.

Answer the questions below:

"In traceroute, if ualy packets are sent, what is the protocol number (enter decimal number) in the probe packets?"

[1] If you are unable to run Wireshark live on a computer, you can download the zip file http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip (7z and extract the file ICMP-ethereal-trace-2. The traces in this zip file were collected by Wireshark running on one of the author's computers, while performing the steps indicated in the Wireshark lab. Once you have downloaded the trace, you can load it into Wireshark and view the trace using the File pull down menu, choosing Open, and then selecting the ICMP-ethereal-trace-2 trace file. You can then use this trace file to answer the questions.

17

Question 6

1 / 1 pts

"For traceroutes that use ICMP instead of UDP, the type of ICMP messages generated by the requests are the same as for ping."

- True
- False

Question 7

1 / 1 pts

"What additional information is returned with the TTL exceeded error messages, that is not returned in an echo reply?"

- checksum
- number of routers traversed
- original ICMP/UDP message
- (part of) original IP packet

Question 8

1 / 1 pts

"If the IP time to live (TTL) field is greater than the number of hops to the destination, traceroute's packets (ICMP or UDP) will not result in ICMP time to live exceeded messages."

- True
- False

Question 9

1 / 1 pts

Use traceroute (ideally after using **ssh** to log into ssc.cs.adelaide.edu.au machine at university) to trace between a computer in Australia and server at Carnegie Mellon University (www.net.cmu.edu). Approximately how many routers (hops) are traversed?

- 10
- 5
- 25
- 50

correct

Quiz score: 9 out of 9