U10814
—
LAB 7: ICMP

Author	**Danny Werb**
Contributors	**George Harvey, Alexios Louridas & Seb Blair**
Last Update	**2023-04-20**
Number of pages	**3**

1 Introduction

This very short lab document is intended to help kick-start your understanding of the *ICMP* protocol for your upcoming assignment. Seeing *ICMP* in action helps, so it is advised that you run *Wireshark*. In VH1.01 / VH1.02 you can either run *Wireshark* on Windows, or you can run it in the *CCCU Lab Ubuntu* virtual machine via *VirtualBox*.

2 Setup

Whatever method you choose, make sure that all of the following points are true.

- *Wireshark* is running.
- *Wireshark* is able to capture from the correct network interface.
- A terminal is open and ready for your input.

3 ICMP Echo Request/Reply (Ping)

Ask your neighbours which IP addresses they have and note them down.

One application making use of the *ICMP* protocol is `ping`. Ensure *Wireshark* is capturing and then in the terminal type the following command substituting `ipAddress` for an actual IP address of course.

```
> ping ipAddress
```

4 Traceroute

Another useful tool using ICMP is `tracert`. On Linux and UNIX systems you can use `traceroute` and/or `mtr`. In this example use `traceroute` as follows. Obviously you need to substitute the appropriate IP address and if you are on a less restricted network with access to the Internet you can also give a domain name instead.

```
> traceroute ipAddress or domainName
```

Make sure that you save the packet capture from this session into a file that you can easily analyse at a later point and use to answer the below questions.

5 Questions

1. **PING Protocols Captured**

   (a) 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 when you execute `ping` on a domain name.

   (b) Identify the IP address returned in the DNS response message.

2. **ICMP Echo Request**

   (a) 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?

   (b) Next examine the ICMP message. What is the ICMP message type? What is the message identifier and sequence number?

   (c) 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**

   (a) 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?

   (b) 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.

   (c) 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.

   (a) How do the identifier and sequence numbers change with time?

   (b) Does the data sequence in the request and reply messages change?

   (c) 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.**

   (a) 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 when you execute `ping` on a domain name.

   (b) Identify the IP address returned in the DNS response message.

6. **ICMP Echo Request**

(a) 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 (if applicable). What are the protocol type and the Time-to-Live in the IP packet?

(b) Record the header of the IP packet for future reference.

(c) Examine the ICMP message. What is the ICMP message type? What are the message identifier and sequence number?

(d) 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**

(a) What are the source and destination addresses in the IP packet that carries the ICMP Time Exceeded message?

(b) Now examine the ICMP message. What is the ICMP message type?

(c) The ICMP Type, Code, and Checksum are followed by the IP header of the ICMP Echo Request Message. Compare the returned IP header to the IP header noted in step 6.

(d) Does the ICMP message carry any additional data?

(e) 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.

(a) 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?

(b) List the sequence of the source IP addresses in the packets that carry the ICMP Time Exceeded messages. Compare to the list provided by your traceroute.

(c) What is the received ICMP message when the ICMP Echo reply finally reaches the desired host?

(d) 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.