Shane Ferrell, Jenna Sheldon, Sergio Bustamente

EEL4598 Fall 2023

Lab 1 Report

The Lab 1 demo recordings can be found here:

Part 1 <https://youtu.be/EyCEkO0lNiU>

Part 2 <https://uflorida-my.sharepoint.com/personal/sbustamante_ufl_edu/_layouts/15/onedrive.aspx?id=%2Fpersonal%2Fsbustamante%5Fufl%5Fedu%2FDocuments%2FEEL4598%20Demos&view=0>

Part 3 <https://drive.google.com/file/d/18z5nsO65N9W__cdJyzBbAAxO_WBxl0x9/view?usp=drive_link>

or in the Lab repository: <https://github.com/shaneferrellwv/computer-communications-labs/tree/main/lab01>

**Summary**

This lab included the exploration or ping, ICMP, and traceroute by observing them in action with the Wireshark tool.

**Part 1: ICMP and Ping**

Wireshark was used to observe packets on the network resulting from the ping command “ping -n 10 www.ust.hk”. This command sends 10 ping messages to a web server at Hong Kong University of Science and Technology. The resulting output is shown in Figure 1.

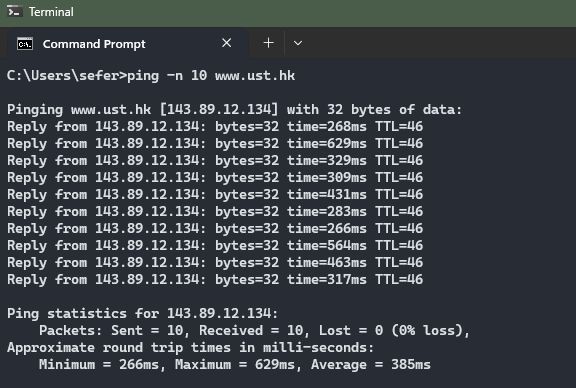


Figure 1: Output resulting from ping command.

The list of ICMP packets captured by Wireshark following the ping command are shown in Figure 2.

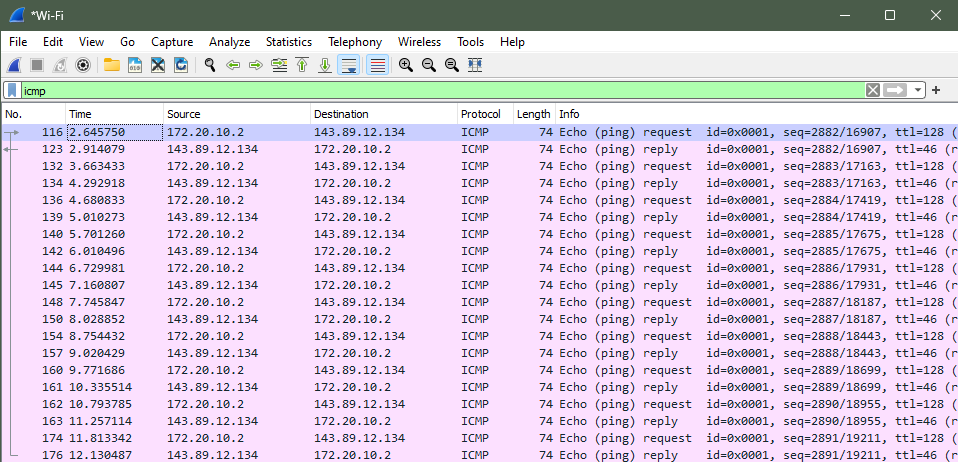


Figure 2: Captured ICMP packets resulting from ping command.

Details of the first packet are shown in Figure 3. The IP address of the host, listed in the Source Address field, is 172.20.10.2. The IP address of the destination host, listed in the Destination Address field, is 143.89.12.134.

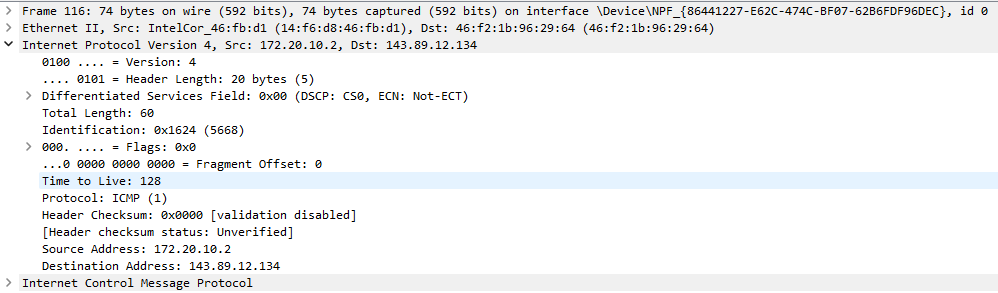


Figure 3: Details of first ICMP packet resulting from ping.

These ICMP packets lack source and destination port numbers because ICMP is a Network Layer protocol. ICMP is typically used for delivering error and control messages, while ports are typically associated with the transport layer.

Details of the ICMP for the first packet are shown in Figure 4. The ICMP type is 8 (Echo (ping) request) and the code number is 0. The packet also contains a checksum, two identifiers, and two sequence numbers which are represented by two bytes each.

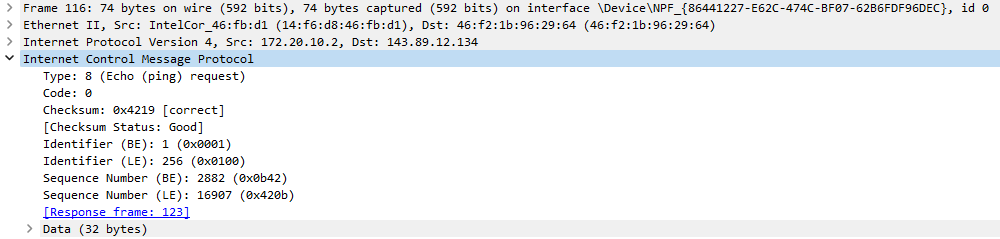


Figure 4: Details of the ICMP packet.

Details of the ICMP for the reply packet are shown in Figure 5. The ICMP type is 0 (Echo (ping) reply) and the code number is 0. The packet also contains a checksum, two identifiers, and two sequence numbers which are represented by two bytes each.

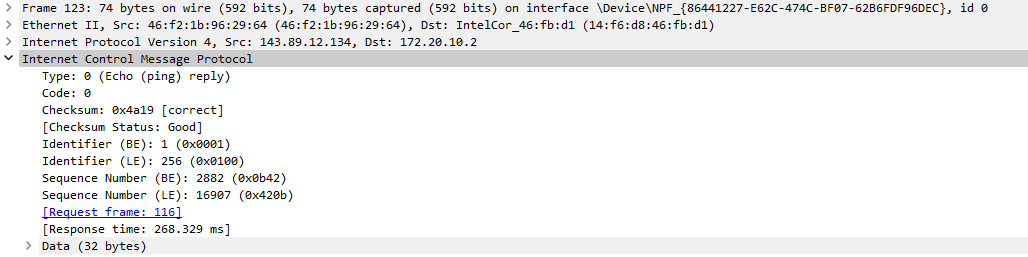


Figure 5: Details of the ICMP reply packet

**Part 2: ICMP and Traceroute**

Using the native Windows Command Prompt, we accessed the Tracert tool to analyze the path of a packet sent to a router located at a research institute in Paris, France. The tracert command sends three packets through a series of routers to their target destination and reports the roundtrip time between the source and each of these routers. We can use this information to identify possible sources of latency and packet loss. Figure 1 shows the result of running the tracert command with the target destination domain of www.inria.fr.

A computer screen with white text

Description automatically generated

Figure 6. Output of tracert command set to destination www.inria.fr

Here we observe that the IP address of the source host is 10.138.101.230, and the IP address of the destination host is 128.93.162.83.

**A screenshot of a computer

Description automatically generated**

Figure 7. Wireshark capture incoming and outgoing ICMP packets

Expanding the ICMP dropdown menus confirms that the assigned protocol number of ICMP packets is 1, regardless of the type. If UDP packets were sent instead such as in a Unix/Linux system, the protocol number of the probe packets would be 0x11, or 17, because that is the assigned protocol number for UDP packets. Although the tracert program produces a different reply packet than the ping command used in part 1, the outgoing request packets are nearly identical. The only noticeable difference between the ICMP echo packet and the ICMP ping packets is the length of each packet. The echo packets are each 106 bytes, 32 bytes larger than the ping packets. Opening the details of the echo packets reveals that the data encapsulated by an echo packet is 64 bytes, whereas each ping packet only contains 32 bytes of data. Other than the size of the data, the fields are organized identically.

A screenshot of a computer

Description automatically generated

Figure 8. Echo (ping) request ICMP packets fields using tracert program

Compared to the ICMP echo packet, the ICMP error packet has an additional 28 bytes. These 28 bytes contain information about the echo packet that was sent out. The 20 bytes shown in figure 9 contain the IP header information, and the 8 bytes following the header information are the 8 bytes corresponding to the fields of the echo packet. This is the case for the error packet shown, but some of the other error packets have variations in length.

A screenshot of a computer

Description automatically generated

Figure 9. An additional 20 bytes corresponding to the header information of the echo request packet. The rest of the bytes contain the fields of the original echo request packet, including the data.

The last three ICMP packets are type 0, echo (ping) reply packets instead of type 11, time-to-live (TTL) exceeded packets. These echo reply packets signify that the echo request packets have made it all the way to their destination. These packets appear once the tracert program has found a data path through few enough connections to reach the destination before the TTL counter reaches 0.

A screenshot of a computer

Description automatically generated

Figure 10. Echo reply packet information

We refer to figure 6 to note that there is a significant latency increase between hops 19 and 20 for each of the three packets sent. The router names indicate that a router located in Washington, DC is trying to send the packet to a router in London. Transatlantic communication will inherently have a high latency due to long distances between routers. Based on the router names displayed by the tracert command, it can be inferred that the host router is located somewhere on UF’s campus, and the destination router is located at the INRIA research institute in France.

**Part 3: ICMP and Traceroute using Pingplotter**

A screenshot of a computer

Description automatically generated

*Figure 11: Screenshot of Pingplotter window, using ICMP to send and receive requests from* [*www.inria.fr*](http://www.inria.fr) *in the same way as in part 2 using another program*

The IP address of our host is 192.168.1.77. The IP address of our target destination host is 128.93.162.83.  
A screenshot of a video game

Description automatically generated

*Figure 12: IP Address shown from echo request packet*

No, the IP Protocol number would be 0x11 (17), the number for UDP

A black and white text

Description automatically generated

*Figure 13: UDP shown with ID number from Wireshark*

The Echo Packet is shown below. It is different than that of the first half of the lab in size of the packet sent, similar to described in section 2, as the tracert programs send the packets in a different way.

A screenshot of a computer

Description automatically generated

*Figure 14: Echo Packet Reply*

The ICMP error packet is shown below. In comparison to the echo reply, the error has a different type and Identification, although the same length and bytes on wire, containing IP and header information as described in Part 2.

A screenshot of a computer

Description automatically generated

*Figure 15: ICMP error packet*

The ICMP packets that are different than the error packets in that they are a different type, indicating that the message found its way within a short enough route as described in Part 2, not violating the TTL (time to live) as described in Part 2. An example of this is shown below.

A screenshot of a computer

Description automatically generated

*Figure 16: ICMP received replies*

Within the tracert measurements, the link whose delay is significantly longer are any who end in “.fr” rather than “.net”. This same idea is mimicked in my lab, where the links ending in “.fr” are longer than the “.net”, most likely because of the distance from here to routers in France, and propagation delay.

A screenshot of a computer

Description automatically generated

*Figure 17: significantly longer delays shown in tracert function*

Based on the router names, “attlocal” and “inria.fr”, we can assume that the protocol is being sent from a local device on an AT&T network to a router in France.