CS 315: Computer Networks Lab
Spring 2024-25, IIT Dharwad
Assignment-10
Wireshark Lab: ICMP
March 24, 2025

Lab Instructions

- Mark your attendance in the attendance sheet before leaving the lab.
- Handle the lab resources with utmost care.
- Please go through the following exercises in today's lab.
- It is recommended that you complete all the following exercises during the lab slot itself.
- If you face any difficulties, please feel free to seek help online or from your peers or TAs.
- After finishing all exercises, please carry your solutions with you (via email/pen drive) for future reference, and delete the files from the desktop.

Introduction

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

- ICMP messages generated by the Ping program;
- ICMP messages generated by the Traceroute program;

Part 0: Paste a screenshot of your system IP address, using ipconfig (on Windows) or ifconfig (on Mac and Linux), and fill out this Google form to submit the details of your system. The same system must be used to attempt all exercises of this lab.

Part-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 a 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:

```
For ubuntu: ping -c 5 wireshark.com
```

```
For Windows: ping -n 5 wireshark.com
```

1. How many ping requests and replies do you observe for the ping command?

2. What is the destination IP address in the ping request packets, specify the domain name associated with this IP address.
3. Examine the sequence number field in the ICMP Echo Request packets. How does it change for each packet?
4. How many different types of echo ping do you observe in the trace?
5. Provide the field name(s) and the value that remains unchanged in the ICMP ping request and replies.

Part-2: Traceroute on `ambergroupindia.com`

```
Ubuntu: traceroute -m 15 ambergroupindia.com
```

```
Windows: tracert -h 15 ambergroundindia.com
```

1. List all the unique IP addresses you observe for the traceroute on ambergroupindia.com.
2. For the command traceroute -m 15 ambergroupindia.com, what does the -m 15 flag do, and how does it affect the captured packets?
3. Which transport layer protocol is used in the ICMP packets?
4. What happens when a router does not respond to a traceroute probe? How is this represented in the captured packets?

Part-3: Traceroute on `drive.google.com`

```
For ubuntu: traceroute -I -q 1 drive.google.com
```

1. How does the '-q 1' option in the traceroute command to drive.google.com affect the captured packets?
2. What is the significance of the -I option in the traceroute command? How does it affect the type of packets sent compared to the default traceroute behaviour?
3. Compare the TTL values in ICMP Time Exceeded messages from different routers in the traceroute output. What pattern do you observe?
4. For the traceroute to drive.google.com, how many different unique IP addresses do you observe in the captured packets?
5. In the captured Wireshark packets, what type of ICMP messages do you observe for intermediate hops, and what type of response do you receive from the final destination?
6. What is the source IP address of the ICMP Time Exceeded messages, and what does it indicate about the network path?
7. If you compare the results of traceroute -I -q 1 drive.google.com and traceroute drive.google.com, what key differences would you expect in the captured packets?

Part-4: Controlling Packet Size `using ping`

```
For ubuntu: ping -s 1570 -c 5 www.godaddy.com
```

```
For Windows: ping -l 1570 -n 5 www.godaddy.com
```

1. What is the significance of the '-s 1570' option in the ping command? Calculate the total size of each ping request packet sent to the specified domain, including all protocol headers.
2. State the number of fields in the ICMP header along with its size.
3. What is the maximum ICMP packet size that can be transmitted without fragmentation, considering standard MTU constraints?
4. Does the captured packet trace indicate fragmentation for the ICMP echo request sent to the specified domain? If so, determine the total number of fragmented packets and analyze their fragment offset in the IP header.
5. What is the default ICMP payload size observed in the standard ping request to the specified domain using this command `ping -c 5 www.godaddy.com`? Additionally, analyze the difference in payload size between the default ping request and the custom-sized `ping -s 1570 -c 5 www.godaddy.com`.

Submission Details

- Write your ICMP answers in a single doc/tex file, and submit its PDF named after your IIT Dharwad roll number, which contains all answers (with screenshots, if necessary).