CS 315: Computer Networks Lab
Spring 2024-25, IIT Dharwad
Assignment-7
Wireshark Lab: IP
February 17, 2025

Lab Instructions

- Login to the Ubuntu OS on your machine. The login credentials are as follows:
  - Username: user
  - Password: 123456
- 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 investigate the celebrated IP protocol, focusing on the IPv4 and IPv6 datagram. This lab has three parts.

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: Basic IPv4

In this part, we'll analyze packets in a trace of IPv4 datagrams sent and received by the `Ping`. Use the following to capture and analyze an IPv4 trace in Wireshark, open a terminal and follow these steps:

On Linux/macOS:

```
ping google.com -c 5
```

On Windows:

```
ping -n 5 google.com
```

Answer the following questions.

1. What is the source and destination IP address for the above ping request you observe in your trace?
2. Mention the protocol used in the ping request.
3. State the number of fields in the IPv4 header along with its size.

Select the first UDP segment sent by your computer due to this `Ping` command.

4. List the type of queries used for the above request. Expand the Internet Protocol part of the packet in the packet details window. What is the version of the IP address used for the above request?
5. What is the value in the time-to-live (TTL) field in this IPv4 datagram's header?
6. What is the value in the upper layer protocol field in this IPv4 datagram's header?
7. How many bytes are in the payload of the IP datagram? Explain how you determined the number of payload bytes.
8. Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.

Next, let's look at the ICMP packets being sent from your computer and returned to your computer. The display filter that you can use to show just these packets is "icmp".

9. Mention the number of requests and replies you observe from your computer to the requested domain name.
10. State the types of ping requests and replies you observe in the trace for the requested domain name.
11. List in detail the fields that vary as well as remain constant from the ping request and replies in the IP datagrams.

Part 2: Fragmentation

Use the following command in the terminal and capture the trace in Wireshark to answer the following questions.

```
wget "https://files.testfile.org/PDF/50MB-TESTFILE.ORG.pdf"
```

Answer the following:

1. What are the IP addresses of the client and the above-requested domain?
2. Which transport layer protocol is being used to establish the connection between the client and the requested domain?
3. What is the IP version?
4. In the entire TCP stream for the above request, what is the value of the last Ack number and what does it signify?

Part 3: IPv6

In this final section, we'll take a quick look at the IPv6 datagram using Wireshark. The Internet is still primarily at IPv4 network, and your computer or your ISP may not be configured for IPv6, let's look at a trace of already captured packets that contain some IPv6 packets. To generate this trace, our web browser opened the `youtube.com` homepage. YouTube (and Google) provide fairly widespread support for IPv6.

Open the file provided `Assignment_7_Part3_IPv6.pcapng`.

This is a DNS request (contained in an IPv6 datagram) to an IPv6 DNS server for the IPv6 address of youtube.com. The DNS AAAA request type is used to resolve names to IPv6 IP addresses.

Answer the following questions:

1. What is the IPv6 source and destination address of the computer making the DNS AAAA request for the above-requested web browser?
2. What are the values of the flow label for these IPv6 datagrams?
3. How much payload data are carried for these IPv6 datagrams? What does this signify?
4. What is the upper layer protocol to which this datagram's payload will be delivered at the destination?

Lastly, find the IPv6 DNS response to the IPv6 DNS AAAA requests made in this trace. This DNS response contains IPv6 addresses for youtube.com.

5. How many IPv6 addresses are returned in response to the AAAA requests?

Submission Details

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