Tu Lam

CS 372 Lab

February 11th, 2021

Lab #2

(*IP Protocol & IP Datagram*)

1. *What is the IP address of your computer?*

Answer: The IP address of my computer is **192.168.1.9**

2. *Within the IP packet header, what is the value in the upper layer protocol field?*

Answer: Within the IP packet header, the value for the layer protocol field is **ICMP (1).**

3. *How many bytes are in the IP header? How many bytes are in the payload of the IP datagram? Explain how you determined the number of payload bytes.*

Answer: There are **20 bytes in the IP header** while there are **36 bytes in the payload of the IP datagram.** To determine the number of payload bytes, the WireShark tell us that there is a total length of 56 bytes and 20 bytes already went to the IP header, so from there we could do the remaining subtraction to get our payload:

$$56\, bytes - 20\, bytes = 36\, bytes\ of\ payload$$

4. *Has this IP datagram been fragmented? Explain how you determined whether or not the datagram has been fragmented.*

Answer: The IP datagram in this WireShark **has not been fragmented.** To determine this, we can see inside the Internet Protocol tab, there is a section called "**Fragment Offset**" which is set to 0, meaning that the IP datagram has not been fragmented.

5. *Which fields in the IP datagram always change from one datagram to the next within this series of ICMP messages sent by your computer?*

Answer: The fields that always change from one datagram to the next within the series of ICMP messages is: **Identification, Time to Live, Header Checksum** field.

6. *Which fields stay constant? Which of the fields must stay constant? Which fields must change? Why?*

Answer: For the fields that stay constant and the fields must stay constant will have the same contents:

- **Header Length, Source & Destination Address, Total Length, Version, and Differentiated Services Field**

While the field that must change is:

- **Identification, Time to Live, and Header Checksum**

The reason these must change is that the identification and header checksum is like a way to identify the ICMP uniqueness, if all of them are the same, it is hard to identify them. In the other fields, like the source & destination address is constant because the content is going in and out from the same sources and nothing is changing for this source.

7. *Describe the pattern you see in the values in the Identification field of the IP datagram.*

Answer: The pattern that I see in the Identification field of the IP datagram is that the field **increment by 1 every time** that there is an Echo (ping) request.

8. *What is the value in the Identification field and the TTL field?*

Answer: The value in the field at the first hop exceed is:

Identification: 62144

TTL: 54

9. *Do these values remain unchanged for all of the ICMP TTL-exceeded replies sent to your computer by the nearest (first hop) router? Why?*

Answer: The value remain unchanged is the TTL field while the Identification field does change as this act as a unique identifier for each ICMP. If there are two Identification with the same number mean that there is fragment that is divided into more ICMP.

10. *Find the first ICMP Echo Request message that was sent by your computer after you changed the Packet Size in pingplotter to be 2000. Has that message been fragmented across more than one IP datagram?*

Answer: For this I will be using the ip-ethereal-trace-1 packet trace to answer the question from here on out as I cannot find any fragmented in my trace.

Yes, there is more than one IP datagram that has been fragmented.

11. *Print out the first fragment of the fragmented IP datagram. What information in the IP header indicates that the datagram been fragmented? What information in the IP header indicates whether this is the first fragment versus a latter fragment? How long is this IP datagram?*

Answer: The information in the IP header indicates that the datagram been fragmented is the header field of Flags where it is given a hexadecimal number and a message that said there are "more fragments". The information that determines if the fragment is the first or not is the fragment offset = 0 meaning that it is the first fragment rather than the latter fragment. The length of the IP datagram in this is 1500.

12. *Print out the second fragment of the fragmented IP datagram. What information in the IP header indicates that this is not the first datagram fragment? Are there more fragments? How can you tell?*

Answer: The information in the IP header that indicate that this is not the first datagram fragment is that the fragment offset section is set to 1480. There are no more fragments after this, and we can tell by looking at the flag that it is not set by setting it to 0x00 and the message saying that "more fragments" is not display.

13. *What fields change in the IP header between the first and second fragment?*

Answer: The fields change in the IP header between the first and second fragment are: The **Total Length**, **Fragment Offset**, **Flag**, and the **Header Checksum.**

14. *How many fragments were created from the original datagram?*

Answer: There are a total of **3 original datagram** when switch to 3500 packet size.

15. *What fields change in the IP header among the fragments?*

Answer: The fields that change in the IP header among the fragment includes: The **Header Checksum**, the **Total Length**, **Flag**, and the **Fragment Offset.**

Everything else change in field except for the total length where 2 fragments hold the length of 1500 while the last fragment changes this length to a different number.