Mihai Dan

11/18/2015

CS 372

Lab 4

**1.** Select the first ICMP Echo Request message sent by your computer, and expand the Internet Protocol part of the packet in the packet details window. What is the IP address of your computer?

The IP address of my computer is 172.16.0.17

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

The value in the upper 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.

a. IP header: 20 bytes

b. Payload of IP datagram: 36 bytes

The previous was calculated by taking the packet header size, which is 20 bytes, and subtracting it from the the full length of the package, which is 56 bytes.

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

The IP datagram has not been fragmented. This was determined by checking the more fragments field in the datagram. In this case, the bit was set to zero.

**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?

The fields that always change are Identification, TTL and header checksum.

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

**Fields that stay constant:**

a. Version – same IPv4 version

b. header length – all have the same header, meaning same length

c. source IP – sending from same source

d. destination IP – sending to same destination

e. Differentiated Services – all user same Type of Service class

f. Upper Layer Protocol – since they are all ICMP packets

**Fields that must stay constant**

a. Version – same IPv4 version

b. header length – all have the same header, meaning same length

c. source IP – sending from same source

d. destination IP – sending to same destination

e. Differentiated Services – all user same Type of Service class

f. Upper Layer Protocol – since they are all ICMP packets

**Fields that must change:**

a. Identification Number

b. TTL (Time To Live)

c. Header checksum

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

The ID field of the IP datagram is incremented with each ICMP Echo request.

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

ID field value: 55559

TTL field value: 64

**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?

The ID field changes for all of the ICMP TTL-exceeded replies sent to my computer. This is because the ID field is unique. If there are more than one packets with the same ID number, it means that they have been fragmented from one larger IP datagram. The TTL does not change, because the first hop router TTL is always the same.

**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?

*[Note: if you find your packet has not been fragmented, you should download the zip file*

*http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip and extract the ipethereal-trace-1packet trace. If your computer has an Ethernet interface, a packet size of 2000 should cause fragmentation.3]*

Yes, this packet has been fragmented into more than one IP datagram.

**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?

The part of the IP header that indicates that the datagram has been fragmented is the more fragments flag, which is set to true. The fragment offset flag is set to zero, meaning this is the first fragment in the sequence. This datagram is 1500 bytes long, including the header.

**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 the more fragments? How can you tell?

The fragment offset is set to 185, meaning this is the second packet after the first, which was 1480 bytes long. The more fragments flag is not set, meaning there are no more fragments coming.

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

a. total length

b. flags

c. fragment offset

d. checksum

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

There are three packets created from the original datagram.

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

a. The IP header fields that change between all packets are fragment offset and checksum.

b. First two packets have a length of 1500, while the last packet only has a length of 540.

c. First two packets have the more fragments bit set to 1, while the last packet is set to 0.