Eddie C. Fox

March 5, 2017

CS 372 Introduction to Networking

Lab 4

Part 2: A look at the captured trace

Note, I am using the ethereal trace because I couldn't capture live results. So my results will match those of the trace. Will include clickable links to my screenshots.

1. The address of my computer (in the trace) is 192.168.1.102. The source address field. http://puu.sh/uvsxB/b728a74930.png
2. The value of the upper layer protocol field is ICMP (1). Screenshot taken from the ICMP echo request packet from question 1. http://puu.sh/uvsLK/66856eeee5.png
3. Each packet is 56 bytes total and the header length is 20 bytes, giving us a payload size of 36 bytes. http://puu.sh/uvxy4/7c14dbf687.png
4. The fragment offset is 0 and the More fragments flag is not set, so the packet is not fragmented. http://puu.sh/uvygx/cd83c978df.png
5. The identification, time to live, and header checksum change. I'll give two screenshots of two ICMP echo request packets. Packet 1: http://puu.sh/uvyX8/643a127415.png

   Packet 2: http://puu.sh/uvz5G/b2d2c57e1d.png

6. Using same screenshots as in previous. Which fields stay constant: Version because we are using ipv4 protocol. Header length because we use ICMP packets. Source and destination IP, because we still have the same source and destination IP. Upper layer protocol, because they are all ICMP packets. The fields that must change are the same as the previous question. Identification, time to live, and header checksum.
7. The identifications increment by 1 each ICMP echo packet.
8. Identification: 13008. Time to live: 1. http://puu.sh/uvCtn/1684977281.png
9. The identification changes because every unique datagram has a unique identification. If it didn't, it is a fragment. The time to live stays the same because it is the first hop router doesn't change.

Fragmentation:

10. Yes it is fragmented. http://puu.sh/uvDuD/be50c54dcf.png
11. Use the following screenshot: http://puu.sh/uvEOr/c76241e206.png The flag for more fragments was set, meaning that it is fragmented, besides the fact that it says Fragmented IP protocol. The fact that the fragment offset is 0 means it is the first fragment. The length of the datagram is 1500 including the header.

12. http://puu.sh/uvFvP/4da96dd594.png We can tell it's a fragment because the fragment offset is 1480. And we can tell it is the last fragment because the more fragments flag isn't set.
13. The total length changes from 1500 (first) to 548 (second). More fragments changes from 1 SET (first) to 0 NOT SET (second). Checksum changes from 0x077b to 0x2a7a.

Ping Plotter set to 3500:

14. 3 fragments total. http://puu.sh/uvG8N/af45871d85.png
15. All packets have different fragment offsets and checksums. Fragment offsets: 0 (1st packet), 1480 (2nd packet), 2960 (3rd packet). Checksums: 0x0751 (1st packet), 0x0698 (2nd packet), 0x2983 (3rd packet). First two packets have a length of 1500, 3rd fragment has a total length of 568. First two packets have more fragments flag set (1) while the last segment has the more fragments flag not set (0). Packet 1: http://puu.sh/uvH3R/f8154f5171.png Packet 2: http://puu.sh/uvH6a/4feee9fe93.png Packet 3: http://puu.sh/uvH0y/3407f8b94b.png