Richard Aviles

10/31/2017

Wireshark Lab #5 - IP

1) The address of the computer is 192.168.1.159

2) The value in the upper protocol layer field is ICMP (1)

3) There are 20 bytes in the Header. There are 36 bytes in the payload. I got the header bytes from the header length field, and I got the payload bytes from subtracting the total length (56) from the header length.

56 bytes - 20 bytes = 36 bytes.

4) The IP datagram was not fragmented. I found out by checking the fragments flag and saw that it was not set.

5) I noticed three different fields changing: the identification field, the time to live field, and the header checksum field.

6) The source and destination fields stay constant because we aren’t changing where and from where we are sending the packets. The header length stays the same since they are all the same type of packets. Protocol field is always ICMP (1) so that stays constant. The version, differentiated services, total length, flags, and fragment offset fields all stay constant.

The fields that must stay constant are the version, header length, source, destination, and protocol fields. Source and destination never change because we are not changing the place we are sending packets to or who is sending them. The others all deal with ICMP packets so they have to be the same as well.

The fields that have to change are identification, time to live, and header checksum. Each packet has to have its own id number which is why it changes. The time to live changes because pingplotter is incrementing this so it always changes.

7) The pattern I see is that it goes down by one every time.

8) The value for the identification field is 29075. The value for the time to live field is 56.

9) The identification field changes because each packet has its own unique id number. The time to live field doesn’t change because if it is taking the same path it will always end in the same hops.

10) Yes it has been fragmented into two IP datagrams.

11) I know it has been fragmented because it has the more fragment field marked. I know this is the first one because the fragment offset is 0 which shows the start. I know they are the same because of their identification number. The total size of the first one is 1500.

12) I know this one is the second one because the fragment offset of this one is 1480. No more fragments after this one. I know this because the more fragment field is set back to 0. Also the next datagram has a different id number. At the bottom it also indicates there were 2 IPv4 Fragments (1980 bytes).

13) The total length changed between the two, as well as the more fragments field. The fragment offset and header checksum fields also changed between the two.

14) Three fragments were created.

15) In the first two the only things that changed was the fragment offset and header checksum fields. The last one had those two previously stated, as well as the more fragments field and total length changed.