Kiernan Nikitow

Professor Melissourgos

CIS 337

10/24/2023

Lab 5: IP

In this lab, we are taking a deeper look at IP and UDP by tracking what happens when we use the traceroute command on the command line. The very first question we are asked (1) is what is the IP address of our computer by selecting one of the UDP segments; `Source Address: 192.168.86.61` In this picture, we can see that the source address (my computer in this case) is 192.168.86.61. We were then asked what the time-to-live (TTL) is in the IPv4 diagrams header (2), `Time to Live: 1` which we can see, is 1. Then for question 3, we were asked what the value was for the upper layer protocol field `Protocol: UDP (17)` which to the left, is UDP (17). The lab directed us next to look at what the length of the header (4) `Header Length: 20 bytes (5)` was which says 20 bytes. Similarly, we were asked what the total length of the payload was (5) which we can see `Total Length: 56` says 56. This means that since the header is 20 bytes, that means that the payload has to be 36 because 56 – 20 = 36 bytes. For question 6, we are asked to explain if the IP datagram has been fragmented, in the

```
.0.. .... = Don't fragment: Not set
..0. .... = More fragments: Not set
```

picture to the left, in the flags section, we can see that it says not set for any fragmenting, meaning that it is not fragmented. Question 7 was optional and since we did this as a class, we have skipped this question, however, question 8 asks us which of the fields in the IP datagram ALWAYS change from one datagram to the next within the series of UDP segments. We found that header checksum and identification change and this can be confirmed by the series of screenshots by 3 different packets which for me were packets 44, 48, and 50. `Header Checksum: 0x2faa` `Identification: 0xfda2 (64930)`

`Header Checksum: 0x2fa9` `Identification: 0xfda3 (64931)` `Header Checksum: 0x2fa8`

Identification: 0xfda1 (64929) . For question 9, we are asked what fields in the sequence of IP datagrams stay constant and why. We have found that flags, source/destination IP, header length, protocol, differentiated services, and version never change. Flags don't change because its not fragmented, source and destination don't change because we are tracing the route to the final destination. Header length doesn't change because it is IP. Differentiated services doesn't change because the packets are all the same, protocol doesn't because they are all UDP (17), and finally, Version doesn't change because the IP version is 4. Question 10 is asking us to describe the pattern we see in the values in the identification field of the IP datagrams being sent. In the above pictures, we can see that the very last number in the identification field is increasing by 1 each time we send them. Question 11 asked us what the upper layer protocol specified in the IP datagrams returned from the routers, which is Protocol: ICMP (1) ICMP (1) since I am on windows. Question 12 asked us if the values in the identification fields are similar in behavior to the answers to question 10. We found that they aren't the same because some packets are increased by one but some are by 2, others are unpredictable. It also asked if the values of TTL fields are similar across all if the ICMP packets from the different routers, and again, they aren't the same. 0x688a (26762) 0x688b (26763) 0x6889 (26761) There are some of the identification fields and we can see that they don't increase by a constant amount.

Time to Live: 61 Time to Live: 59 Time to Live: 253 Here we can see that the TTL of these packets are different. Question 13 asks us what the IPv6 address of the computer making the DNS AAAA request. Src: 2601:193:8302:4620:215c:f5ae:8b40:a27a, Here we can see the long string is the IPv6 address. The next question (14) asks us what is the IPv6 destination address for the datagram. To Dst: 2001:558:feed::1 the left we can see that the address is 2001:558:feed::1. Similar to before, question 15 asks how much payload data is carried which we can see is 37 bytes. Payload Length: 37 Question 16 asks us how many IPv6 addresses are returned in the response to the AAAA request. Here

we can see that it says the response is packet 27. Lastly, for question 17, it asks us what is the first of the IPv6 addresses returned by the DNS for youtube.com. here we can see that the source is

[Response In: 27] 2001:558:feed::1.