20170058 Keonwoo Kim · October 29, 2020
CS341 Introduction to Computer Networks

Wireshark #2

1. (UDP) [Refer `/tmp/wireshark_any_20201029172154_pP9xGd.pcapng` below.]

(1) Select one UDP packet from your trace. From this packet, determine how many fields there are in the UDP header. (You shouldn't look in the textbook! Answer these questions directly from what you observe in the packet trace.) Name these fields.

[Answer] There are 4 fields in the UDP header: `Source Port`, `Destination Port`, `Length`, and `Checksum`.

(2) By consulting the displayed information in Wireshark's packet content field for this packet, determine the length (in bytes) of each of the UDP header fields.

[Answer] Each field has a length of 2 bytes.

(3) What is the maximum number of bytes that can be included in a UDP payload? (Hint: the answer to this question can be determined by your answer to 2. above)

[Answer] Since the `Length` field is of length 2 bytes, which is 16 bits, the maximum length of a packet is $2^{16} - 1 = 65535$ [bytes]. Since the UDP header takes 8 bytes (from 1. and 22.), the maximum number of bytes that can be included in a UDP packet is $65535 - 8 = 65527$ [bytes].

(4) Examine a pair of UDP packets in which your host sends the first UDP packet and the second UDP packet is a reply to this first UDP packet. (Hint: for a second packet to be sent in response to a first packet, the sender of the first packet should be the destination of the second packet). Describe the relationship between the port numbers in the two packets.

[Answer] The source port of the reply packet is the same with the destination port of the first packet, and the destination port of the reply packet is the same with the source port of the first packet.

2. (TCP) [Refer `/tmp/wireshark_wlp1s0_20201029190844_2WuBOQ.pcapng` below.]

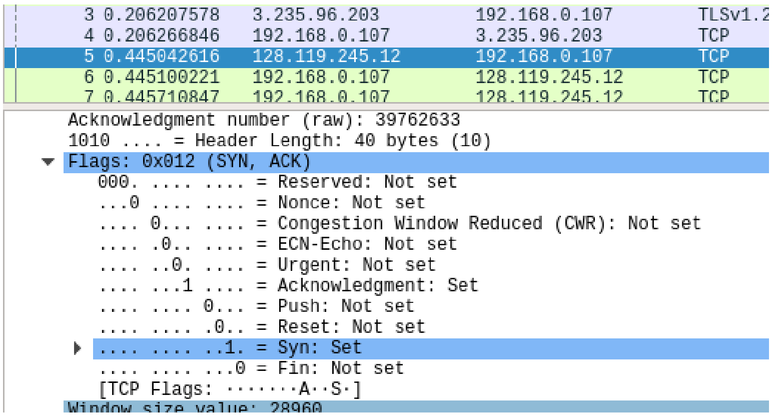
(1) What is the IP address and TCP port number used by your client computer (source) to transfer the file to gaia.cs.umass.edu?

[Answer] The IP address is `192.168.0.107`, and the TCP port number is `60286`.

(2) What is the sequence number of the SYNACK segment sent by gaia.cs.umass.edu to the client computer in reply to the SYN? What is the value of the Acknowledgement field in the SYNACK segment? How did gaia.cs.umass.edu determine that value? What is it in the segment that identifies the segment as a SYNACK segment?

[Answer] The sequence number of the SYNACK segment is `2050667101` (`0x7a3ab25d`,) and the value of the acknowledgement field in the SYNACK segment is `39762633` (`0x025ebac9`.) This value is determined by adding 1 to the sequence number of the SYN segment sent by the client.

The SYNACK segment is realized by the flags set, where the flags `0x12` mean that the acknowledgement flag and Syn flag are set as shown below.



```
   3 0.206207578   3.235.96.203       192.168.0.107      TLSv1.2
   4 0.206266846   192.168.0.107      3.235.96.203       TCP
   5 0.445042616   128.119.245.12     192.168.0.107      TCP
   6 0.445100221   192.168.0.107      128.119.245.12     TCP
   7 0.445710847   192.168.0.107      128.119.245.12     TCP

      Acknowledgment number (raw): 39762633
      1010 .... = Header Length: 40 bytes (10)
    ▾ Flags: 0x012 (SYN, ACK)
         000. .... .... = Reserved: Not set
         ...0 .... .... = Nonce: Not set
         .... 0... .... = Congestion Window Reduced (CWR): Not set
         .... .0.. .... = ECN-Echo: Not set
         .... ..0. .... = Urgent: Not set
         .... ...1 .... = Acknowledgment: Set
         .... .... 0... = Push: Not set
         .... .... .0.. = Reset: Not set
       ▸ .... .... ..1. = Syn: Set
         .... .... ...0 = Fin: Not set
         [TCP Flags: ·······A··S·]
      Window size value: 28960
```

(3) What is the sequence number of the TCP segment containing the HTTP POST command? Note that in order to find the POST command, you'll need to dig into the packet content field at the bottom of the Wireshark window, looking for a segment with a "POST" within its DATA field.

[Answer] The sequence number of the TCP segment containing the HTTP POST command is `39762633` (`0x025ebac9`.)

(4) What is the throughput (bytes transferred per unit time) for the TCP connection? Explain how you calculated this value.

[Answer] The last ACK number of the TCP connection is `39913225`. Therefore, since the TCP segment containing the HTTP POST command is sent, the client have sent $39913225 - 39762633 = 150592$ [bytes]. Note that the time difference between two segments is $3.006507397 - 0.241993047 = 2.76451435$ [seconds]. Therefore, the average throughput of the TCP connection is

$$\begin{aligned} 150592\,[\text{bytes}]/2.76451435\,[\text{seconds}] &= 54473.2205857\,[\text{bytes/second}] \\ &= \underline{435.785764686\,[\text{kbps}].} \end{aligned}$$