Introduction to Computer Network Proj3 Report

0416324 胡安鳳

Exp1 UDP packets

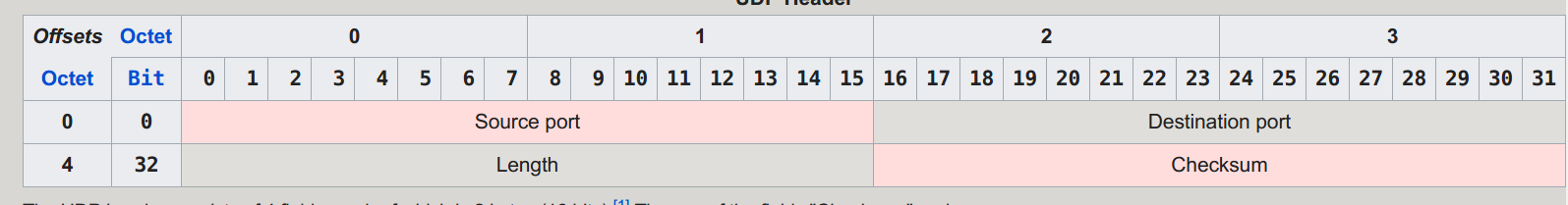
1.

Select the UDP packet. How many fields are there in UDP header? Name these fields.

Ans:

This picture is captured from wireshark, as we can see, there are total of four fields in header, including Source Port, Destination Port, Length of the total UDP data(including the header, unit in byte) and the checksum for error detection(but UDP does not implement error recovery, it has to be done by the application in upper level).

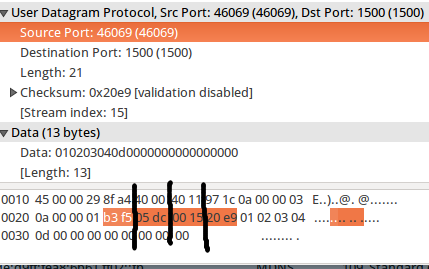
Validating from wikipedia, it is also 4 fields.



2.

Following the first operation, click on the header and observe the display at the bottom of Wireshark window. Determine the length(in bytes) of each field

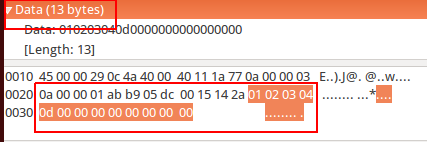
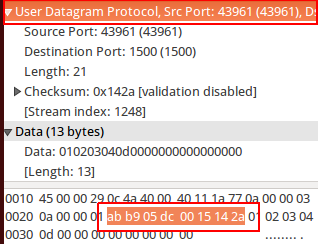
Ans:



As the picture taken form wireshark, each field is equally divided into 16bits, namely 2 bytes.

3.

Focus on Length field. According to the format:total Length = header + payload, fill in the numbers and explain how you calculate. Ans as follows:

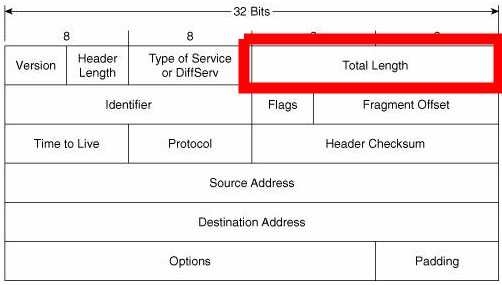


The UDP header is fixed into 8 bytes(see pic1) and in this experiment, I found that the data part, namely the payload part is 13 bytes(see pic2).

4.

What is the maximum number of bytes that can be included in a UDP payload? (Referred to class notes)

Ans:



In IPv4, the maximum length of packet size is 65535. So, for UDP datagram we have maximum data length as:

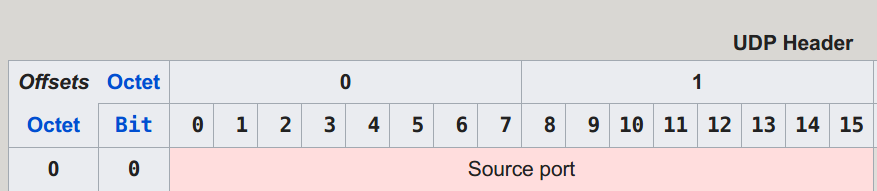
65535 bytes - 20 bytes(Size of IPv4 header) = 65515 bytes (including 8 bytes UDP header)

**And finally the payload should be 65515 – 8 = 65507 bytes**

5.

What is the largest possible source port number? (Referred to class notes)

Ans:

**2^16-1=65535**

Exp2 TCP packets

1.



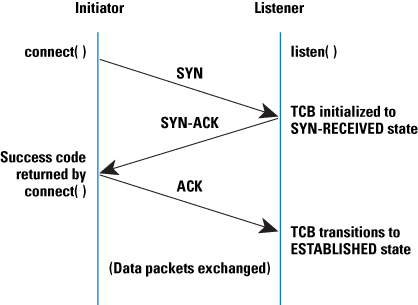
IP Addr Port

Client 10.0.0.3 8700

Server 10.0.0.1 38226

2.

Observing the experimental result, find the segments of “Three Way Handshake,” and answer the following questions.



(a)What are the Sequence

and ACK numbers in each of

the segments?

Ans:



1st part SEQ1=0 ACK1= No (No one has transmitted data to client yet, the 3-way handshaking is just about to begin)

2nd part SEQ2=0 (I send my SEQ data to the client host)

ACK2=1(I got client’s SEQ0 data and I expected to get the client’s next sequence which is 1)

3rd part SEQ3=1 (I send my SEQ data to the server host)

ACK3=1(I got the server’s SEQ0 data and I expected to get the client’s next sequence which is 1)

(b)Do these three segments

contain any data?

Ans:

No the real data transfer **happens when PSH flag is set**

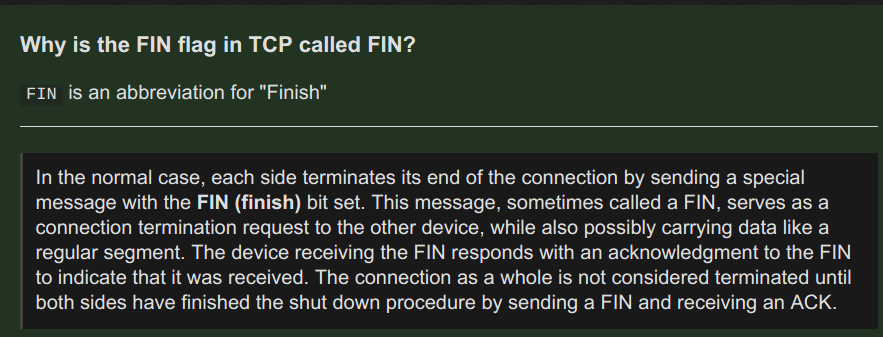
Reference to:

[https://read01.com/zh-tw/dE6deN.html#.Wi0lqHaGOIY](https://read01.com/zh-tw/dE6deN.html" \l ".Wi0lqHaGOIY)

3.Find segments in which the FIN Flag field is set. Explain the purpose of these segments.

Ans:

The packet with FIN flag indicates the TCP connection should be terminated.

Source: stackoverflow

4.Choose a packet from your experiment as an example.



(a) What is the value of window size?

Window size is 29200 as the picture shown above.

(b) What is it used for?

It is used for flow controlling in TCP

reference: <https://wizardforcel.gitbooks.io/network-basic/content/7.html>

(c) Find the sequence numbers of the segments that can be sent by the TCP sender

ExpBonus

1.

Find and mark the interface names of switch on the topology you created in previous experiments. (Mark the names on the green labels of the following picture.)

Ans:

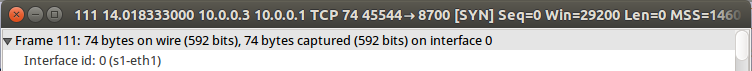
Consider the time sequence of wireshark from top to down of sending the data b/w h1,h3 with the following picture.

The data is transmitted in the blue line, either from h1 to h3 or from h3 to h1

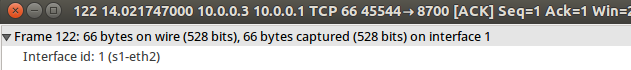
Take an example of data from h1 to h3, the only road the data does not pass is s2h2, hence path of data transmission is h1s1→s1s2→s2s3→s3h3 using this sequence, I can identify the label of each interface if the switch.

The following picture shows the result, and timing from start to end.

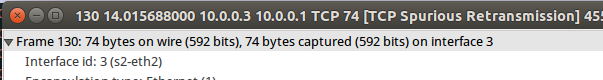
(Note, the time sequence does not listed in ascending order since there are many switch interfaces to be detected by the wireshark at the same time, however, we can still find the connectivity of the topology where each of the interface of the switch should be.)



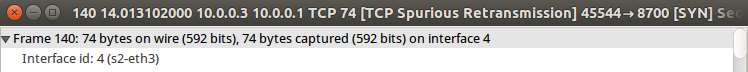
First, h1s1 and the label is s1-eth1



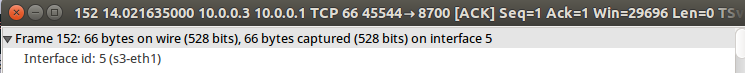
Then s1s2, first through s1-eth2



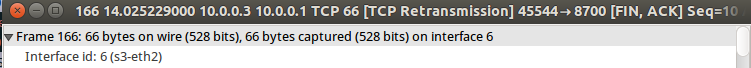
Then the s2-end part of s1s2, s2-eth2



Then s2s3, first through s2-eth3

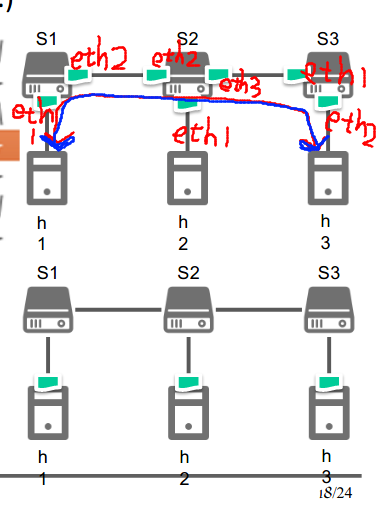


Then the s3-end part of s1s2, s3-eth1



And finally reach end

This is what the answer should be



2.How do you observe the packets passed through the interface of h1?

Ans:

Use the filter with dst addr or src addr==10.0.0.1 (h1 is the server) in wireshark