Maxwell Sullivan: Computer Science
This blog was created to submit assignments for CSC251

Wireshark Lab 5: Exploring UDP

March 12, 2013
Lab Video:

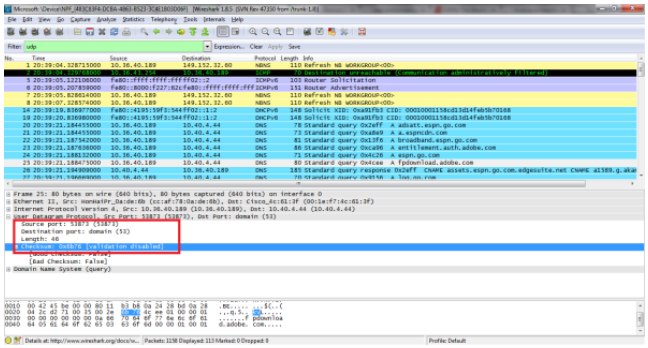
STEPS:

Start capturing packets in Wireshark and then do something that will cause your host to send and receive several UDP packets. It's also likely that just by doing nothing (except capturing packets via Wireshark) that some UDP packets sent by others will appear in your trace. In particular, the Simple Network Management Protocol (SNMP – chapter 9 in the text) sends SNMP messages inside of UDP, so it's likely that you'll find some SNMP messages (and therefore UDP packets) in your trace.

QUESTIONS:

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.

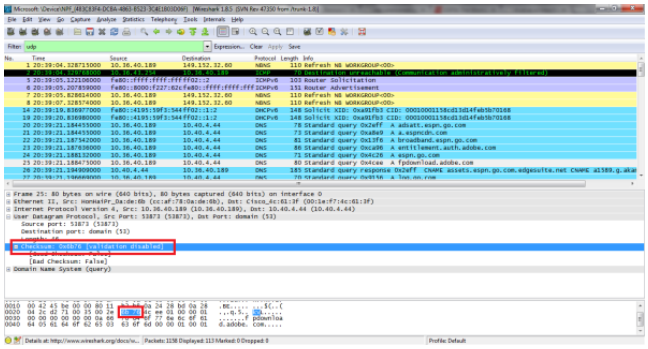
The header only contains 4 fields: the source port, destination port, length, and checksum.



(https://maxwellsullivan.files.wordpress.com/2013/03/wireshark5-1.png)

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.

Each of the UDP header fields is 2 bytes long



(https://maxwellsullivan.files.wordpress.com/2013/03/5-2.png)

3. The value in the Length field is the length of what? (You can consult the text for this answer). Verify your claim with your captured UDP packet.

The value in the length field, in the example below it is 46, is the sum of the 8 header bytes and the remaining data bytes encapsulated in the packet.

4. 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)

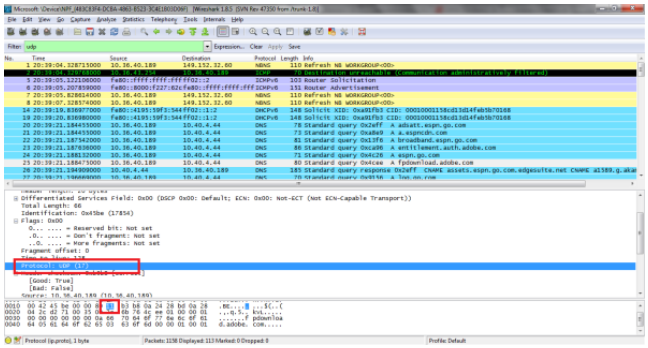
The maximum number of bytes that can be in the payload is 2^16- the bytes already being used by the header field (8). Therefore the maximum payload is 65535-8= 65527 bytes.

5. What is the largest possible source port number? (Hint: see the hint in 4.)

The largest possible source port number is 2^16 or 65535.

6. What is the protocol number for UDP? Give your answer in both hexadecimal and decimal notation. To answer this question, you'll need to look into the Protocol field of the IP datagram containing this UDP segment (see Figure 4.13 in the text, and the discussion of IP header fields).

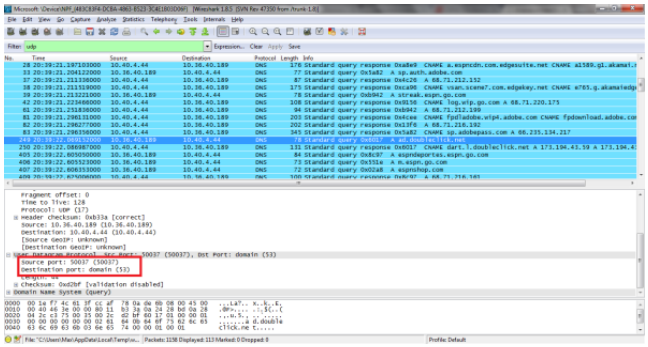
The protocol number for UDP is 17 in decimal notation which in hexadecimal notation is 0x11.



(https://maxwellsullivan.files.wordpress.com/2013/03/5-4.png)

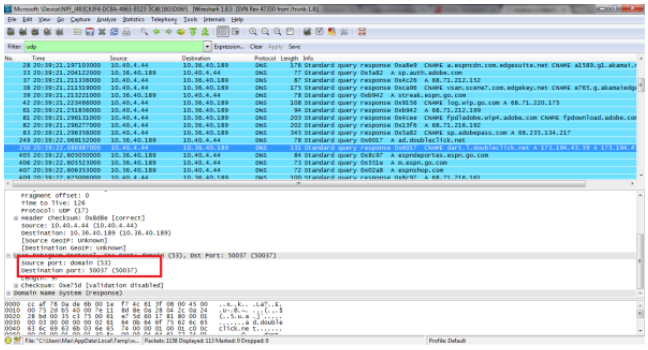
7. Examine a pair of UDP packets in which your host sends the first UDP packet and the second UDP packet is a reply to this first UDP packet. (Hint: for a second packet to be sent in response to a first packet, the sender of the first packet should be the destination of the second packet). Describe the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

UDP Sent by my host



(https://maxwellsullivan.files.wordpress.com/2013/03/5-5-2.png)

UDP Reply to Host



(https://maxwellsullivan.files.wordpress.com/2013/03/5-5-3.png)

> The relationship between port numbers is that the source port on the send message is the destination port of the receive message. The destination port for the send message is also the source port for the receive message.

From → Wireshark Labs

Leave a Comment