ENGR 3321 - Lab 4: Wireshark UDP

14 October 2022

Nathan Cauwet

873271826

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.*

There are 4 fields: source, destination, length, and checksum

```
User Datagram Protocol, Src Port: 51116, Dst Port: 53
    Source Port: 51116
    Destination Port: 53
    Length: 37
  > Checksum: 0x31d5 [correct]
    [Checksum Status: Good]
    [Stream index: 0]
  > [Timestamps]
    UDP payload (29 bytes)
```

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.*

payload = 29 bytes, Length = 37, total length of IPv4 = 57, IPv4 header = 20

ipv4 length – ipv4 header length = 57-20 = 37 = Length

Length - payload = 8 bytes = UDP header size

If you click on User Datagram Protocol, it says the header is 8 bytes (verifying total UDP header size that I calculated above).

Since there are 4 header fields and the total header size is 8 bytes, **each header is 2 bytes**.

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.

Value in length field = 37 = the IPv4 packet (total size minus the header)

ipv4 packet = ipv4 length – ipv4 header length = 57-20 = 37 = Length

It is the length of the IPv4 packet

UDP payload + UDP header = 29 + 8 = 37 bytes = UDP packet length

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 length of a UDP packet is (2^{16} - 1) bytes (including the 8 header bytes), therefore maximum number of bytes allowed in a UDP payload is (2^{16} - 1)bytes – 8bytes = **65527 bytes**

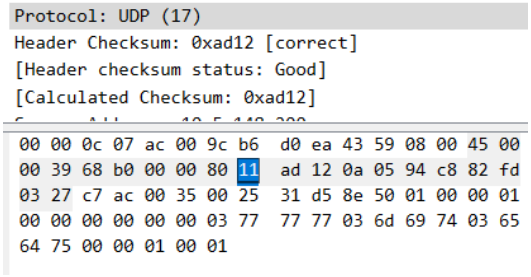
Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
Packet Lengths	4	115.50	71	160	0.0413	100%	0.0400	1.781

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

The largest possible source port number is = (2^{16} - 1) = 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).*

UDP protocol number is 17 in decimal and 0x11 in hexadecimal



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.*

The port numbers in the two packets are the same with the source and destination switched (src1 = dest2 and src2 = dest1).

Destination Port	Source Port	Info
53	51116	Standard query 0x8e50 A
53	51116	Standard query 0x8e50 A
51116	53	Standard query response

<u>The expanded details from the selected packet are included below:</u>

C:\Users\ncauw\OneDrive - University of Denver\Documents\wireshark-caps\lab4-cap-bothValidationsEnabled.pcapng 22 total packets, 2 shown

```
No.     Time               Source                Destination           Protocol Length Flags      Destination Port Source Port Info
      4 10:45:20.336335    10.5.148.200          130.253.3.39          DNS      71                53               51116       Standard
query 0x8e50 A www.mit.edu
Frame 4: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF_{3F3DB8EB-1AC0-401B-8543-3316F86ED445}, id 0
    Section number: 1
    Interface id: 0 (\Device\NPF_{3F3DB8EB-1AC0-401B-8543-3316F86ED445})
        Interface name: \Device\NPF_{3F3DB8EB-1AC0-401B-8543-3316F86ED445}
        Interface description: Wi-Fi
    Encapsulation type: Ethernet (1)
    Arrival Time: Oct  7, 2022 10:45:20.336335000 Mountain Daylight Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1665161120.336335000 seconds
    [Time delta from previous captured frame: 1.701068000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 1.781161000 seconds]
    Frame Number: 4
    Frame Length: 71 bytes (568 bits)
    Capture Length: 71 bytes (568 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:udp:dns]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
Ethernet II, Src: RivetNet_ea:43:59 (9c:b6:d0:ea:43:59), Dst: All-HSRP-routers_00 (00:00:0c:07:ac:00)
    Destination: All-HSRP-routers_00 (00:00:0c:07:ac:00)
        Address: All-HSRP-routers_00 (00:00:0c:07:ac:00)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: RivetNet_ea:43:59 (9c:b6:d0:ea:43:59)
        Address: RivetNet_ea:43:59 (9c:b6:d0:ea:43:59)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 10.5.148.200, Dst: 130.253.3.39
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        0000 00.. = Differentiated Services Codepoint: Default (0)
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 57
    Identification: 0x68b0 (26800)
    000. .... = Flags: 0x0
        0... .... = Reserved bit: Not set
        .0.. .... = Don't fragment: Not set
        ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0xad12 [correct]
    [Header checksum status: Good]
    [Calculated Checksum: 0xad12]
    Source Address: 10.5.148.200
    Destination Address: 130.253.3.39
User Datagram Protocol, Src Port: 51116, Dst Port: 53
    Source Port: 51116
    Destination Port: 53
    Length: 37
    Checksum: 0x31d5 [correct]
        [Calculated Checksum: 0x31d5]
    [Checksum Status: Good]
    [Stream index: 0]
    [Timestamps]
        [Time since first frame: 0.000000000 seconds]
        [Time since previous frame: 0.000000000 seconds]
    UDP payload (29 bytes)
Domain Name System (query)
    Transaction ID: 0x8e50
    Flags: 0x0100 Standard query
        0... .... .... .... = Response: Message is a query
        .000 0... .... .... = Opcode: Standard query (0)
        .... ..0. .... .... = Truncated: Message is not truncated
        .... ...1 .... .... = Recursion desired: Do query recursively
        .... .... .0.. .... = Z: reserved (0)
        .... .... ...0 .... = Non-authenticated data: Unacceptable
    Questions: 1
    Answer RRs: 0
```

```
    Authority RRs: 0
    Additional RRs: 0
    Queries
        www.mit.edu: type A, class IN
            Name: www.mit.edu
            [Name Length: 11]
            [Label Count: 3]
            Type: A (Host Address) (1)
            Class: IN (0x0001)
    [Response In: 6]
0000  00 00 0c 07 ac 00 9c b6 d0 ea 43 59 08 00 45 00   ..........CY..E.
0010  00 39 68 b0 00 00 80 11 ad 12 0a 05 94 c8 82 fd   .9h.............
0020  03 27 c7 ac 00 35 00 25 31 d5 8e 50 01 00 00 01   .'...5.%1..P....
0030  00 00 00 00 00 00 03 77 77 77 03 6d 69 74 03 65   .......www.mit.e
0040  64 75 00 00 01 00 01                              du.....
```

C:\Users\ncauw\OneDrive - University of Denver\Documents\wireshark-caps\lab4-cap-bothValidationsEnabled.pcapng 22 total packets, 2 shown

```
No.     Time               Source                Destination           Protocol Length Flags      Destination Port Source Port Info
      6 10:45:20.378774    130.253.3.39          10.5.148.200          DNS      160               51116            53          Standard
query response 0x8e50 A www.mit.edu CNAME www.mit.edu.edgekey.net CNAME e9566.dscb.akamaiedge.net A 23.222.166.107
Frame 6: 160 bytes on wire (1280 bits), 160 bytes captured (1280 bits) on interface \Device\NPF_{3F3DB8EB-1AC0-401B-8543-3316F86ED445}, id
0
    Section number: 1
    Interface id: 0 (\Device\NPF_{3F3DB8EB-1AC0-401B-8543-3316F86ED445})
        Interface name: \Device\NPF_{3F3DB8EB-1AC0-401B-8543-3316F86ED445}
        Interface description: Wi-Fi
    Encapsulation type: Ethernet (1)
    Arrival Time: Oct  7, 2022 10:45:20.378774000 Mountain Daylight Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1665161120.378774000 seconds
    [Time delta from previous captured frame: 0.007393000 seconds]
    [Time delta from previous displayed frame: 0.042439000 seconds]
    [Time since reference or first frame: 1.823600000 seconds]
    Frame Number: 6
    Frame Length: 160 bytes (1280 bits)
    Capture Length: 160 bytes (1280 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:udp:dns]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
Ethernet II, Src: Cisco_1c:dc:fb (00:6c:bc:1c:dc:fb), Dst: RivetNet_ea:43:59 (9c:b6:d0:ea:43:59)
    Destination: RivetNet_ea:43:59 (9c:b6:d0:ea:43:59)
        Address: RivetNet_ea:43:59 (9c:b6:d0:ea:43:59)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Source: Cisco_1c:dc:fb (00:6c:bc:1c:dc:fb)
        Address: Cisco_1c:dc:fb (00:6c:bc:1c:dc:fb)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 130.253.3.39, Dst: 10.5.148.200
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        0000 00.. = Differentiated Services Codepoint: Default (0)
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 146
    Identification: 0x4ab0 (19120)
    000. .... = Flags: 0x0
        0... .... = Reserved bit: Not set
        .0.. .... = Don't fragment: Not set
        ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 124
    Protocol: UDP (17)
    Header Checksum: 0xceb9 [correct]
    [Header checksum status: Good]
    [Calculated Checksum: 0xceb9]
    Source Address: 130.253.3.39
    Destination Address: 10.5.148.200
User Datagram Protocol, Src Port: 53, Dst Port: 51116
    Source Port: 53
    Destination Port: 51116
    Length: 126
    Checksum: 0x44c8 [correct]
        [Calculated Checksum: 0x44c8]
    [Checksum Status: Good]
    [Stream index: 0]
    [Timestamps]
        [Time since first frame: 0.042439000 seconds]
        [Time since previous frame: 0.042439000 seconds]
    UDP payload (118 bytes)
Domain Name System (response)
    Transaction ID: 0x8e50
    Flags: 0x8180 Standard query response, No error
        1... .... .... .... = Response: Message is a response
        .000 0... .... .... = Opcode: Standard query (0)
        .... .0.. .... .... = Authoritative: Server is not an authority for domain
        .... ..0. .... .... = Truncated: Message is not truncated
        .... ...1 .... .... = Recursion desired: Do query recursively
        .... .... 1... .... = Recursion available: Server can do recursive queries
        .... .... .0.. .... = Z: reserved (0)
```

```
        .... .... ..0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
        .... .... ...0 .... = Non-authenticated data: Unacceptable
        .... .... .... 0000 = Reply code: No error (0)
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 0
    Queries
        www.mit.edu: type A, class IN
            Name: www.mit.edu
            [Name Length: 11]
            [Label Count: 3]
            Type: A (Host Address) (1)
            Class: IN (0x0001)
    Answers
        www.mit.edu: type CNAME, class IN, cname www.mit.edu.edgekey.net
            Name: www.mit.edu
            Type: CNAME (Canonical NAME for an alias) (5)
            Class: IN (0x0001)
            Time to live: 1475 (24 minutes, 35 seconds)
            Data length: 25
            CNAME: www.mit.edu.edgekey.net
        www.mit.edu.edgekey.net: type CNAME, class IN, cname e9566.dscb.akamaiedge.net
            Name: www.mit.edu.edgekey.net
            Type: CNAME (Canonical NAME for an alias) (5)
            Class: IN (0x0001)
            Time to live: 60 (1 minute)
            Data length: 24
            CNAME: e9566.dscb.akamaiedge.net
        e9566.dscb.akamaiedge.net: type A, class IN, addr 23.222.166.107
            Name: e9566.dscb.akamaiedge.net
            Type: A (Host Address) (1)
            Class: IN (0x0001)
            Time to live: 20 (20 seconds)
            Data length: 4
            Address: 23.222.166.107
    [Request In: 4]
    [Time: 0.042439000 seconds]
0000  9c b6 d0 ea 43 59 00 6c bc 1c dc fb 08 00 45 00   ....CY.l......E.
0010  00 92 4a b0 00 00 7c 11 ce b9 82 fd 03 27 0a 05   ..J...|......'..
0020  94 c8 00 35 c7 ac 00 7e 44 c8 8e 50 81 80 00 01   ...5...~D..P....
0030  00 03 00 00 00 00 03 77 77 77 03 6d 69 74 03 65   .......www.mit.e
0040  64 75 00 00 01 00 01 c0 0c 00 05 00 01 00 00 05   du..............
0050  c3 00 19 03 77 77 77 03 6d 69 74 03 65 64 75 07   ....www.mit.edu.
0060  65 64 67 65 6b 65 79 03 6e 65 74 00 c0 29 00 05   edgekey.net..)..
0070  00 01 00 00 00 3c 00 18 05 65 39 35 36 36 04 64   .....<...e9566.d
0080  73 63 62 0a 61 6b 61 6d 61 69 65 64 67 65 c0 3d   scb.akamaiedge.=
0090  c0 4e 00 01 00 01 00 00 00 14 00 04 17 de a6 6b   .N.............k
```