

HO CHI MINH UNIVERSITY OF TECHNOLOGY
Faculty of Computer Science and Engineering



Computer Networks

Report for lab 3a

Lecture: Nguyễn Mạnh Thìn
Student name: Đặng Trần Khánh-1852037



I. A first look at the captured trace

1. Select one UDP packet from your trace. From this packet, determine how many fields there are in the UDP header. Name these fields

Answer: There are 4 fields in the UDP header: Source port, Destination port, Length, Checksum.

No.	Time	Source	Destination	Protocol	Length	Info
5	22:00:03.869396	192.168.100.7	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
6	22:00:04.292545	192.168.100.7	172.217.163.238	UDP	1392	57474 → 443 Len=1350
7	22:00:04.292995	192.168.100.7	172.217.163.238	UDP	224	57474 → 443 Len=182
8	22:00:04.328386	172.217.163.238	192.168.100.7	UDP	68	443 → 57474 Len=26
9	22:00:04.672956	172.217.163.238	192.168.100.7	UDP	124	443 → 57474 Len=82
10	22:00:04.673231	172.217.163.238	192.168.100.7	UDP	435	443 → 57474 Len=393
11	22:00:04.680820	192.168.100.7	172.217.163.238	UDP	75	57474 → 443 Len=33
12	22:00:04.870278	172.217.163.238	192.168.100.7	UDP	75	443 → 57474 Len=33
13	22:00:04.870676	192.168.100.7	172.217.163.238	UDP	77	57474 → 443 Len=35
14	22:00:04.873133	192.168.100.7	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
15	22:00:04.974119	172.217.163.238	192.168.100.7	UDP	68	443 → 57474 Len=26
16	22:00:04.974507	192.168.100.7	172.217.163.238	UDP	77	57474 → 443 Len=35
17	22:00:05.875857	192.168.100.7	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
20	22:00:06.876686	192.168.100.7	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
25	22:00:09.785134	192.168.100.3	224.0.0.251	MDNS	130	Standard query 0x0000 PTR _companion-link._
26	22:00:09.785134	fe80::10:3460:41d6...	ff02::fb	MDNS	150	Standard query 0x0000 PTR _companion-link._
39	22:00:15.091274	192.168.100.7	172.217.25.4	UDP	1392	49788 → 443 Len=1350
40	22:00:15.092020	192.168.100.7	172.217.25.4	UDP	642	49788 → 443 Len=600
41	22:00:15.206265	192.168.100.7	172.217.25.4	UDP	1392	49788 → 443 Len=1350
42	22:00:15.211261	172.217.25.4	192.168.100.7	UDP	1392	443 → 49788 Len=1350
43	22:00:15.212001	192.168.100.7	172.217.25.4	UDP	75	49788 → 443 Len=33
44	22:00:15.212602	172.217.25.4	192.168.100.7	UDP	67	443 → 49788 Len=25

> Frame 6: 1392 bytes on wire (11136 bits), 1392 bytes captured (11136 bits) on interface \Device\NPF_{3219B7F4-C797-4F0F-9...}

> Ethernet II, Src: AzureWav_5b:72:7f (70:66:55:5b:72:7f), Dst: HuaweiTe_86:4d:dc (68:89:c1:86:4d:dc)

> Internet Protocol Version 4, Src: 192.168.100.7, Dst: 172.217.163.238

▼ User Datagram Protocol, Src Port: 57474, Dst Port: 443

Source Port: 57474
Destination Port: 443
Length: 1358
Checksum: 0x79f2 [unverified]
[Checksum Status: Unverified]
[Stream index: 1]
> [Timestamps]

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: The length of the UDP packet is 8 bytes (shown in the picture below). The length for each UDP header field is 2 bytes.

```

> Frame 6: 1392 bytes on wire (11136 bits), 1392 bytes captured (11136 bits) on interface \Device\NPF_{3219B7F4-...}
> Ethernet II, Src: AzureWav_5b:72:7f (70:66:55:5b:72:7f), Dst: HuaweiTe_86:4d:dc (68:89:c1:86:4d:dc)
> Internet Protocol Version 4, Src: 192.168.100.7, Dst: 172.217.163.238
< User Datagram Protocol, Src Port: 57474, Dst Port: 443
  Source Port: 57474
  Destination Port: 443
  Length: 1358
  Checksum: 0x79f2 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 1]
  > [Timestamps]
  > Data (1350 bytes)

```

0020	a3 ee e0 82 01 bb 05 4e 79 f2 65 e1 4c 2f 05 40	..N yU L/.@
0030	14 3f ce 15 b6 8e 45 96 5f e6 6c 1d 7b 7b 25 7e	?...E _l{ {~
0040	ac d7 a5 ec 8b 71 42 ce a2 25 64 26 2f 49 5d 79	...qB -%d&/Iy
0050	d4 6e ab 21 54 80 5a c2 da 77 f7 df 95 6a f4 a8	n!T.Z -w...j..

3. The value in the Length field is the length of what? Verify your claim with your captured UDP packet.

Answer: The length field specifies the number of bytes in the UDP segment (header plus data). An explicit length value is needed since the size of the data field may differ from one UDP segment to the next. In the example below, the length field value is 34 which consists of 8 bytes of header and 26 bytes of data.

```

> Frame 8: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface \Device\NPF_...
> Ethernet II, Src: HuaweiTe_86:4d:dc (68:89:c1:86:4d:dc), Dst: AzureWav_5b:72:7f (70:66:55:5b:72:7f)
> Internet Protocol Version 4, Src: 172.217.163.238, Dst: 192.168.100.7
< User Datagram Protocol, Src Port: 443, Dst Port: 57474
  Source Port: 443
  Destination Port: 57474
  Length: 34
  Checksum: 0xd756 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 1]
  > [Timestamps]
  > Data (26 bytes)

```

0000	70 66 55 5b 72 7f 68 89 c1 86 4d dc 08 00 45 20	pfU[r.h -M...E
0010	00 36 00 00 40 00 3a 11 cb 1f ac d9 a3 ee c0 a8	-6-@.: -.....
0020	64 07 01 bb e0 82 00 22 d7 56 56 ee 22 39 6b 57	d-... "VW-"9kW
0030	e4 d0 3e 10 c4 af cb a3 14 03 32 03 fc 2c 9e 62	->-... -2-,-b
0040	ec 76 6b dd	-vk-

4. What is the maximum number of bytes that can be included in a UDP payload?

Answer: Since the length field is only capable of holding 16 bits (2 bytes). The total maximum bytes of the UDP packet can hold is $2^{16} - 1 = 65535$ bytes (minus 1 because bit starts at 0). After that, 8 bytes that counts for the header length are removed to achieve the maximum number of bytes that can be included in a UDP payload: $65535 - 8 = 65527$ bytes.

5. What is the largest possible source port number?

Answer: Similar to question 4, the Source port can hold up to 16 bits (2 bytes), the largest possible number is $2^{16} - 1 = 65535$

6. What is the protocol number for UDP?

Answer: The protocol number for UDP is 17, which 11 in hexadecimal (in packet content field)

```
> Frame 8: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface \Device\NPF_{3219B7F4-C797-4F0F-9E1A
> Ethernet II, Src: HuaweiTe_86:4d:dc (68:89:c1:86:4d:dc), Dst: AzureWav_5b:72:7f (70:66:55:5b:72:7f)
v Internet Protocol Version 4, Src: 172.217.163.238, Dst: 192.168.100.7
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0x20 (DSCP: CS1, ECN: Not-ECT)
    Total Length: 54
    Identification: 0x0000 (0)
    > Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 58
    Protocol: UDP (17)
    Header checksum: 0xcb1f [validation disabled]
    [Header checksum status: Unverified]
    Source: 172.217.163.238
    Destination: 192.168.100.7
v User Datagram Protocol, Src Port: 443, Dst Port: 57474
0000  70 66 55 5b 72 7f 68 89  c1 86 4d dc 08 00 45 20  pfU[r·h· ··M···E
0010  00 36 00 00 40 00 3a 11  cb 1f ac d9 a3 ee c0 a8  -6··@·:· ······
0020  64 07 01 bb e0 82 00 22  d7 56 56 ee 22 39 6b 57  d······" ·VW·"9kW
0030  e4 d0 3e 10 c4 af cb a3  14 03 32 03 fc 2c 9e 62  ··>····· ··2··,·b
0040  ec 76 6b dd                ·vk·
```

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. Describe the relationship between the port numbers in the two packets.

Answer:

The UDP packet sent by host (image below) shows the source port is 57474, the destination port is 443.

5	22:00:03.869396	192.168.100.7	239.255.255.250	SSDP	215 M-SEARCH * HTTP/1.1
6	22:00:04.292545	192.168.100.7	172.217.163.238	UDP	1392 57474 → 443 Len=1350
7	22:00:04.292995	192.168.100.7	172.217.163.238	UDP	224 57474 → 443 Len=182
8	22:00:04.328386	172.217.163.238	192.168.100.7	UDP	68 443 → 57474 Len=26
9	22:00:04.672956	172.217.163.238	192.168.100.7	UDP	124 443 → 57474 Len=82
10	22:00:04.673231	172.217.163.238	192.168.100.7	UDP	435 443 → 57474 Len=393
11	22:00:04.680820	192.168.100.7	172.217.163.238	UDP	75 57474 → 443 Len=33
12	22:00:04.870278	172.217.163.238	192.168.100.7	UDP	75 443 → 57474 Len=33
13	22:00:04.870676	192.168.100.7	172.217.163.238	UDP	77 57474 → 443 Len=35
14	22:00:04.873133	192.168.100.7	239.255.255.250	SSDP	215 M-SEARCH * HTTP/1.1
15	22:00:04.974119	172.217.163.238	192.168.100.7	UDP	68 443 → 57474 Len=26
16	22:00:04.974507	192.168.100.7	172.217.163.238	UDP	77 57474 → 443 Len=35
17	22:00:05.875857	192.168.100.7	239.255.255.250	SSDP	215 M-SEARCH * HTTP/1.1
20	22:00:06.876686	192.168.100.7	239.255.255.250	SSDP	215 M-SEARCH * HTTP/1.1

Time to live: 128	
Protocol: UDP (17)	
Header checksum: 0xec2 [validation disabled]	
[Header checksum status: Unverified]	
Source: 192.168.100.7	
Destination: 172.217.163.238	
User Datagram Protocol, Src Port: 57474, Dst Port: 443	
Source Port: 57474	
Destination Port: 443	
Length: 190	
Checksum: 0xda7d [unverified]	
[Checksum Status: Unverified]	
[Stream index: 1]	
[Timestamps]	
Data (182 bytes)	
Data: 43e14c2f0540143fce41eb724797ee0844139f7f7d42b65e...	
[Length: 182]	

The UDP packet received by host (image below) shows the source port is 443, the destination port is 57474. It is clear that the source port of the UDP packet sent by the host is the same as the destination port of the reply packet. Similarly, the destination port of the UDP packet sent by host is the source port for the received packet.

No.	Time	Source	Destination	Protocol	Length	Info
5	22:00:03.869396	192.168.100.7	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
6	22:00:04.292545	192.168.100.7	172.217.163.238	UDP	1392	57474 → 443 Len=1350
7	22:00:04.292995	192.168.100.7	172.217.163.238	UDP	224	57474 → 443 Len=182
8	22:00:04.328386	172.217.163.238	192.168.100.7	UDP	68	443 → 57474 Len=26
9	22:00:04.672956	172.217.163.238	192.168.100.7	UDP	124	443 → 57474 Len=82
10	22:00:04.673231	172.217.163.238	192.168.100.7	UDP	435	443 → 57474 Len=393
11	22:00:04.680820	192.168.100.7	172.217.163.238	UDP	75	57474 → 443 Len=33
12	22:00:04.870278	172.217.163.238	192.168.100.7	UDP	75	443 → 57474 Len=33
13	22:00:04.870676	192.168.100.7	172.217.163.238	UDP	77	57474 → 443 Len=35
14	22:00:04.873133	192.168.100.7	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
15	22:00:04.974119	172.217.163.238	192.168.100.7	UDP	68	443 → 57474 Len=26
16	22:00:04.974507	192.168.100.7	172.217.163.238	UDP	77	57474 → 443 Len=35
17	22:00:05.875857	192.168.100.7	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
20	22:00:06.876686	192.168.100.7	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1

Time to live: 58	
Protocol: UDP (17)	
Header checksum: 0xcb1f [validation disabled]	
[Header checksum status: Unverified]	
Source: 172.217.163.238	
Destination: 192.168.100.7	
User Datagram Protocol, Src Port: 443, Dst Port: 57474	
Source Port: 443	
Destination Port: 57474	
Length: 34	
Checksum: 0xd756 [unverified]	
[Checksum Status: Unverified]	
[Stream index: 1]	
[Timestamps]	
Data (26 bytes)	
Data: 56ee22396b57e4d03e10c4afcba314033203fc2c9e62ec76...	
[Length: 26]	