

VIETNAM NATIONAL UNIVERSITY HO CHI MINH CITY
HO CHI MINH CITY UNIVERSITY OF TECHNOLOGY
FACULTY OF COMPUTER SCIENCE AND ENGINEERING



COMPUTER NETWORKS (LAB)

Report lab 4b

Wireshark Lab: UDP v8.0

Advisor(s): Nguyễn Mạnh Thìn

Student(s): Vũ Nguyễn Lan Vi ID 2153094

HO CHI MINH CITY, APRIL 2024



Contents

1	Exercise	4
---	----------	---



1 Exercise

- **Question 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 in my the UDP header: Source port, destination port, length, checksum.

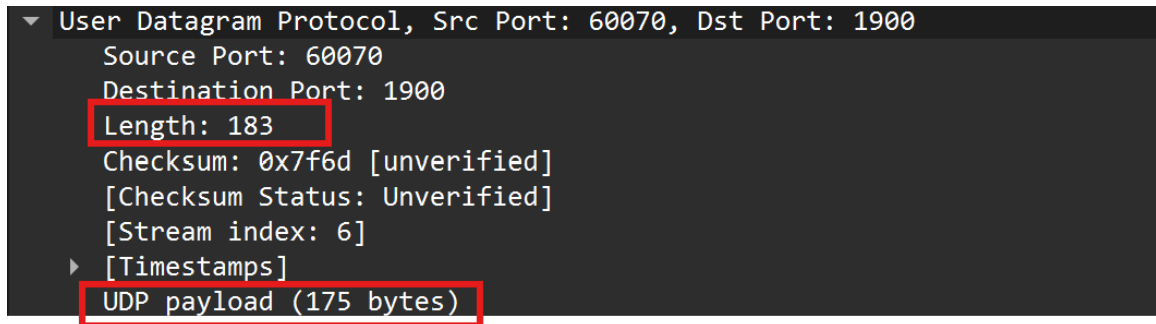
```
1838 24.679672 10.130.44.19 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
1839 24.706990 10.130.44.19 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
2057 25.686507 10.130.44.19 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
2058 25.717959 10.130.44.19 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
2079 26.687979 10.130.44.19 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
2080 26.719922 10.130.44.19 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
2110 27.703565 10.130.44.19 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
2112 27.734522 10.130.44.19 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
2676 39.004631 10.130.44.19 10.130.0.1 DNS 83 Standard query 0xd5bf A www.msftcc
2677 39.013012 10.130.0.1 10.130.44.19 DNS 227 Standard query response 0xd5bf A w
9363 69.073559 10.130.44.19 10.130.0.1 DNS 83 Standard query 0x8f39 A www.msftcc
9371 69.085674 10.130.0.1 10.130.44.19 DNS 211 Standard query response 0x8f39 A w
14324 99.210059 10.130.44.19 10.130.0.1 DNS 83 Standard query 0xa00a A www.msftcc

▶ Frame 1838: 217 bytes on wire (1736 bits), 217 bytes captured (1736 bits) on interface \Device\NPF_{72832CC4-6
▶ Ethernet II, Src: AzureWaveTec_d1:f0:99 (b4:8c:9d:d1:f0:99), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
▶ Internet Protocol Version 4, Src: 10.130.44.19, Dst: 239.255.255.250
▼ User Datagram Protocol, Src Port: 60069, Dst Port: 1900
  Source Port: 60069
  Destination Port: 1900
  Length: 183
  Checksum: 0x6942 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 5]
  ▶ [Timestamps]
  UDP payload (175 bytes)
▶ Simple Service Discovery Protocol
```

- **Question 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. The length of UDP headers are always 8 bytes. Hence, the length of each UDP header fields is 2 bytes.

```
Frame 2080: 217 bytes on wire (1736 bits), 217 bytes captured (1736 bits) on interface \Device\NPF_{72832CC4-6
Ethernet II, Src: AzureWaveTec_d1:f0:99 (b4:8c:9d:d1:f0:99), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
Internet Protocol Version 4, Src: 10.130.44.19, Dst: 239.255.255.250
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 203
    Identification: 0xde32 (56882)
  ▼ 0000 .... = 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: 1
    Protocol: UDP (17)
    Header Checksum: 0xb460 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.130.44.19
    Destination Address: 239.255.255.250
  User Datagram Protocol, Src Port: 60070, Dst Port: 1900
  Simple Service Discovery Protocol
```

- **Question 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 length field is the length of header plus data. As showing in the picture below:
 $\text{Length} = \text{header length} + \text{payload length} = 8 + 175 = 182$ (bytes).



```
▼ User Datagram Protocol, Src Port: 60070, Dst Port: 1900
  Source Port: 60070
  Destination Port: 1900
  Length: 183
  Checksum: 0x7f6d [unverified]
  [Checksum Status: Unverified]
  [Stream index: 6]
  ▶ [Timestamps]
  UDP payload (175 bytes)
```

- **Question 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)
 $\text{Maximum length of UDP payload} = \text{Maximum datagram length} - \text{Header length} = 65535 - 8 = 65527$ (bytes).
- **Question 5:** What is the largest possible source port number? (Hint: see the hint in 4.)
Source port number is limited by 16 bits. Hence, the largest possible source port number is $2^{16} - 1 = 65535$.
- **Question 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: 17 (decimal) or 0x11 (hexadecimal).



```
Frame 45: 222 bytes on wire (1776 bits), 222 bytes captured (1776 bits) on interface \Device\NPF_{72832CC4-6...
Ethernet II, Src: HewlettPacka_4d:44:ac (00:26:55:4d:44:ac), Dst: AzureWaveTec_d1:f0:99 (b4:8c:9d:d1:f0:99)
Internet Protocol Version 4, Src: 10.130.0.1, Dst: 10.130.44.19
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 208
  Identification: 0xc7ff (51199)
  0000 .... = 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: 64
  Protocol: UDP (17)
  Header checksum: 0x7106 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 10.130.0.1
  Destination Address: 10.130.44.19
User Datagram Protocol, Src Port: 53, Dst Port: 64412
  Source Port: 53
```

- **Question 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 source port of the sender and the destination port of the receiver are the same (63666), the destination port of the sender and the source port of the receiver are the same (53).

```
420 3.827581 10.130.44.19 10.130.0.1 DNS 75 Standard query 0xd26a A windows.msn.com
423 3.843537 10.130.0.1 10.130.44.19 DNS 150 Standard query response 0xd26a A windows
478 5.188427 10.130.44.19 10.130.0.1 DNS 91 Standard query 0xc618 A settings-win.dat
479 5.219886 10.130.0.1 10.130.44.19 DNS 222 Standard query response 0xc618 A setting
936 8.922806 10.130.44.19 10.130.0.1 DNS 83 Standard query 0x7dab A www.msftconnectt

Frame 420: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\NPF_{72832CC4-654F-4...
Ethernet II, Src: AzureWaveTec_d1:f0:99 (b4:8c:9d:d1:f0:99), Dst: HewlettPacka_4d:44:ac (00:26:55:4d:44:ac)
Internet Protocol Version 4, Src: 10.130.44.19, Dst: 10.130.0.1
User Datagram Protocol, Src Port: 63666, Dst Port: 53
  Source Port: 63666
  Destination Port: 53
  Length: 41
  Checksum: 0xb9bc [unverified]
  [Checksum Status: Unverified]
  [Stream index: 2]
  [Timestamps]
  UDP payload (33 bytes)
Domain Name System (query)
```



No.	Time	Source	Destination	Protocol	Length	Info
420	3.827581	10.130.44.19	10.130.0.1	DNS	75	Standard query 0xd26a A windows.msn.com
423	3.843537	10.130.0.1	10.130.44.19	DNS	150	Standard query response 0xd26a A windows.
478	5.188427	10.130.44.19	10.130.0.1	DNS	91	Standard query 0xc618 A settings-win.data
479	5.219886	10.130.0.1	10.130.44.19	DNS	222	Standard query response 0xc618 A settings
936	8.922806	10.130.44.19	10.130.0.1	DNS	83	Standard query 0x7dab A www.msftconnectte

▶ Frame 423: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits) on interface \Device\NPF_{72832CC4-65	0000
▶ Ethernet II, Src: HewlettPacka 4d:44:ac (00:26:55:4d:44:ac), Dst: AzureWaveTec_d1:f0:99 (b4:8c:9d:d1:f0:99)	0010
▶ Internet Protocol Version 4, Src: 10.130.0.1, Dst: 10.130.44.19	0020
▶ User Datagram Protocol, Src Port: 53, Dst Port: 63666	0030
Source Port: 53	0040
Destination Port: 63666	0050
Length: 116	0060
Checksum: 0x3047 [unverified]	0070
[Checksum Status: Unverified]	0080
[Stream index: 2]	0090
▶ [Timestamps]	
UDP payload (108 bytes)	