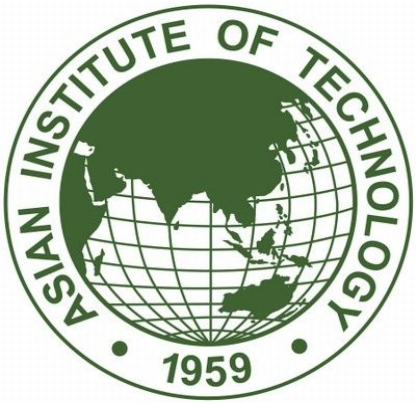
AT70.05
Computer Networks



Lab Assignment No:5

Submitted by :

Rajasekhar Ponakala - st119220

Problem 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.

Answer:

Usually UDP header contains four fields.

1.Source port

2.Destination port

3.length

4.Checksum

Wireshark packet capture -

```
     69 15.898321787   203.159.50.115       203.159.0.1          DNS      76     Standard query 0x4375
A www.facebook.com
Frame 69: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface 0
Ethernet II, Src: ChiconyE_87:a9:0a (64:5a:04:87:a9:0a), Dst: Cisco_43:f8:c1 (64:a0:e7:43:f8:c1)
Internet Protocol Version 4, Src: 203.159.50.115, Dst: 203.159.0.1
User Datagram Protocol, Src Port: 39436, Dst Port: 53
    Source Port: 39436
    Destination Port: 53
    Length: 42
    Checksum: 0x6230 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
Domain Name System (query)
```

Problem 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 UDP header of this packet has a fixed length of 8 bytes and the length of each of the UDP header fields is 2 bytes long.

Wireshark packet capture -

```
     69 15.898321787   203.159.50.115       203.159.0.1          DNS      76     Standard query 0x4375 A
www.facebook.com
Frame 69: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface 0
Ethernet II, Src: ChiconyE_87:a9:0a (64:5a:04:87:a9:0a), Dst: Cisco_43:f8:c1 (64:a0:e7:43:f8:c1)
Internet Protocol Version 4, Src: 203.159.50.115, Dst: 203.159.0.1
User Datagram Protocol, Src Port: 39436, Dst Port: 53
    Source Port: 39436
    Destination Port: 53
    Length: 42
    Checksum: 0x6230 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
Domain Name System (query)
0000  64 a0 e7 43 f8 c1 64 5a 04 87 a9 0a 08 00 45 00   d..C..dZ......E.
0010  00 3e bb ac 40 00 40 11 b5 4f cb 9f 32 73 cb 9f   .>..@.@..O..2s..
0020  00 01 9a 0c 00 35 00 2a 62 30 43 75 01 00 00 01   .....5.*b0Cu....
0030  00 00 00 00 00 00 03 77 77 77 08 66 61 63 65 62   .......www.faceb
0040  6f 6f 6b 03 63 6f 6d 00 00 01 00 01               ook.com.....
```

Problem 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.

Answers :

The length field gives the number of bytes in the UDP segment. As it is required because the size of the data field may differ from one UDP segment to next segment.

Wireshark packet capture -

```
     69 15.898321787   203.159.50.115       203.159.0.1          DNS      76     Standard query 0x4375
A www.facebook.com
Frame 69: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface 0
Ethernet II, Src: ChiconyE_87:a9:0a (64:5a:04:87:a9:0a), Dst: Cisco_43:f8:c1 (64:a0:e7:43:f8:c1)
Internet Protocol Version 4, Src: 203.159.50.115, Dst: 203.159.0.1
User Datagram Protocol, Src Port: 39436, Dst Port: 53
    Source Port: 39436
    Destination Port: 53
    Length: 42
    Checksum: 0x6230 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
Domain Name System (query)
```

Problem 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)

Answer :

The maximum number of bytes that can be included in a UDP payload is **2^16 -** bytes that are already being used by the header file. Hence maximum payload is 65535 - 8 = 65527.

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

Answer :
The largest port number is 2^16. i.e, 65535.

Problem 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).

Answer :

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

Wireshark packet capture -

```
     69 15.898321787   203.159.50.115        203.159.0.1           DNS      76     Standard query 0x4375 A
www.facebook.com
Frame 69: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface 0
Ethernet II, Src: ChiconyE_87:a9:0a (64:5a:04:87:a9:0a), Dst: Cisco_43:f8:c1 (64:a0:e7:43:f8:c1)
Internet Protocol Version 4, Src: 203.159.50.115, Dst: 203.159.0.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 62
    Identification: 0xbbac (48044)
    Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 64
    Protocol: UDP (17)
    Header checksum: 0xb54f [validation disabled]
    [Header checksum status: Unverified]
    Source: 203.159.50.115
    Destination: 203.159.0.1
    [Source GeoIP: Thailand, AS4767 Computer Science, Bangkok, 40, Thailand, AS4767 Computer Science,
Bangkok, 40, 13.759400, 100.488899]
    [Destination GeoIP: Thailand, AS4767 Computer Science, Klong, 68, Thailand, AS4767 Computer Science,
Klong, 68, 6.802100, 100.621101]
User Datagram Protocol, Src Port: 39436, Dst Port: 53
Domain Name System (query)
0000  64 a0 e7 43 f8 c1 64 5a 04 87 a9 0a 08 00 45 00   d..C..dZ......E.
0010  00 3e bb ac 40 00 40 11 b5 4f cb 9f 32 73 cb 9f   .>..@.@..O..2s..
0020  00 01 9a 0c 00 35 00 2a 62 30 43 75 01 00 00 01   .....5.*b0Cu....
0030  00 00 00 00 00 00 03 77 77 77 08 66 61 63 65 62   .......www.faceb
0040  6f 6f 6b 03 63 6f 6d 00 00 01 00 01              ook.com.....
```

Problem 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.

Answer :

The source port of the UDP packet sent by the host is the same as the destination port of the reply packet, and also the destination port of the UDP packet sent by the host is the same as the source port of the reply packet.

UDP packets sent from my host -

```
    70 15.898338764   203.159.50.115       203.159.0.1          DNS      76     Standard query 0x6978
AAAA www.facebook.com
Frame 70: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface 0
Ethernet II, Src: ChiconyE_87:a9:0a (64:5a:04:87:a9:0a), Dst: Cisco_43:f8:c1 (64:a0:e7:43:f8:c1)
Internet Protocol Version 4, Src: 203.159.50.115, Dst: 203.159.0.1
User Datagram Protocol, Src Port: 39436, Dst Port: 53
    Source Port: 39436
    Destination Port: 53
    Length: 42
    Checksum: 0x3c12 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
Domain Name System (query)
0000  64 a0 e7 43 f8 c1 64 5a 04 87 a9 0a 08 00 45 00   d..C..dZ......E.
0010  00 3e bb ad 40 00 40 11 b5 4e cb 9f 32 73 cb 9f   .>..@.@..N..2s..
0020  00 01 9a 0c 00 35 00 2a 3c 12 69 78 01 00 00 01   .....5.*<.ix....
0030  00 00 00 00 00 00 03 77 77 77 08 66 61 63 65 62   .......www.faceb
0040  6f 6f 6b 03 63 6f 6d 00 00 1c 00 01              ook.com.....
```

UDP packets reply from host -

```
    72 15.899896597   203.159.0.1          203.159.50.115       DNS      168    Standard query response
0x6978 AAAA www.facebook.com CNAME star-mini.c10r.facebook.com AAAA 2a03:2880:f126:83:face:b00c:0:25de NS
a.ns.c10r.facebook.com NS b.ns.c10r.facebook.com
Frame 72: 168 bytes on wire (1344 bits), 168 bytes captured (1344 bits) on interface 0
Ethernet II, Src: Cisco_43:f8:c1 (64:a0:e7:43:f8:c1), Dst: ChiconyE_87:a9:0a (64:5a:04:87:a9:0a)
Internet Protocol Version 4, Src: 203.159.0.1, Dst: 203.159.50.115
User Datagram Protocol, Src Port: 53, Dst Port: 39436
    Source Port: 53
    Destination Port: 39436
    Length: 134
    Checksum: 0x7716 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
Domain Name System (response)
0000  64 5a 04 87 a9 0a 64 a0 e7 43 f8 c1 08 00 45 00   dZ....d..C....E.
0010  00 9a 68 ae 00 00 3e 11 49 f2 cb 9f 00 01 cb 9f   ..h...>.I.......
0020  32 73 00 35 9a 0c 00 86 77 16 69 78 81 80 00 01   2s.5....w.ix....
0030  00 02 00 02 00 00 03 77 77 77 08 66 61 63 65 62   .......www.faceb
0040  6f 6f 6b 03 63 6f 6d 00 00 1c 00 01 c0 0c 00 05   ook.com.........
0050  00 01 00 00 01 ea 00 11 09 73 74 61 72 2d 6d 69   .........star-mi
0060  6e 69 04 63 31 30 72 c0 10 c0 2e 00 1c 00 01 00   ni.c10r.........
0070  00 00 2e 00 10 2a 03 28 80 f1 26 00 83 fa ce b0   .....*.(..&.....
0080  0c 00 00 25 de c0 38 00 02 00 01 00 00 01 37 00   ...%..8.......7.
0090  07 01 61 02 6e 73 c0 38 c0 38 00 02 00 01 00 00   ..a.ns.8.8......
00a0  01 37 00 04 01 62 c0 69                           .7...b.i
```