

HACETTEPE UNIVERSITY DEPARTMENT OF
COMPUTER ENGINEERING
BBM 453 LAB EXPERIMENT



Mehmet Taha USTA – 21527472

Çağlar USLU – 21808388

Mehmet Taha USTA Source = 192.168.1.34

Çağlar USLU Source = 192.168.0.10

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

1 0.000000	192.168.1.41	224.0.0.251	MDNS	70 Standard query 0x0000 A wpad.local, "QM" question
2 0.000000	fe80::e868:176a:a0d...	ff02::fb	MDNS	90 Standard query 0x0000 A wpad.local, "QM" question
3 0.307162	192.168.1.41	192.168.1.255	NBNS	92 Name query NB DESKTOP-KK9C2GC<1c>
5 0.512038	192.168.1.41	192.168.1.255	NBNS	92 Name query NB WPAD<00>
6 1.024241	192.168.1.41	192.168.1.255	NBNS	92 Name query NB DESKTOP-KK9C2GC<1c>
10 1.288603	192.168.1.34	195.175.39.50	DNS	72 Standard query 0xdab6 A www.espn.com
11 1.289907	192.168.1.34	195.175.39.50	DNS	75 Standard query 0x6fb5 A secure.espn.com
16 1.293203	192.168.1.34	195.175.39.50	DNS	72 Standard query 0xe874 A dcf.espn.com
18 1.331329	192.168.1.41	192.168.1.255	NBNS	92 Name query NB WPAD<00>
24 1.370576	195.175.39.50	192.168.1.34	DNS	146 Standard query response 0xe874 A dcf.espn.com CNAME
26 1.372473	195.175.39.50	192.168.1.34	DNS	136 Standard query response 0xdab6 A www.espn.com A 54.1
27 1.373043	192.168.1.34	195.175.39.50	DNS	73 Standard query 0xe3df A a.espncdn.com
33 1.382843	192.168.1.34	195.175.39.49	DNS	75 Standard query 0x6fb5 A secure.espn.com
34 1.385572	195.175.39.50	192.168.1.34	DNS	183 Standard query response 0x6fb5 A secure.espn.com CNA
46 1.462736	195.175.39.50	192.168.1.34	DNS	181 Standard query response 0xe3df A a.espncdn.com CNAME
60 1.554196	195.175.39.49	192.168.1.34	DNS	183 Standard query response 0x6fb5 A secure.espn.com CNA
65 1.740845	fe80::e868:176a:a0d...	ff02::1:3	LLMNR	84 Standard query 0x7881 A wpad
66 1.740845	192.168.1.41	224.0.0.252	LLMNR	64 Standard query 0x7881 A wpad
127 2.047559	192.168.1.41	192.168.1.255	NBNS	92 Name query NB WPAD<00>

▶ Frame 10: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{D1B4F362-C83D-4147-9DE3-E73F2017E4}
▶ Ethernet II, Src: IntelCor_3c:ec:18 (d0:7e:35:3c:ec:18), Dst: ZyxelCom_87:a0:5c (b8:ec:a3:87:a0:5c)
▶ Internet Protocol Version 4, Src: 192.168.1.34, Dst: 195.175.39.50
▲ User Datagram Protocol, Src Port: 51565, Dst Port: 53
Source Port: 51565
Destination Port: 53
Length: 38
Checksum: 0x7c62 [unverified]
[Checksum Status: Unverified]
[Stream index: 3]
▶ [Timestamps]
UDP payload (30 bytes)
▶ Domain Name System (query)

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

udp						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.41	224.0.0.251	MDNS	70	Standard query 0x0000 A wpad.local, "QM" questi
2	0.000000	fe80::e868:176a:a0d...	ff02::fb	MDNS	90	Standard query 0x0000 A wpad.local, "QM" questi
3	0.307162	192.168.1.41	192.168.1.255	NBNS	92	Name query NB DESKTOP-KK9C2GC<1c>
5	0.512038	192.168.1.41	192.168.1.255	NBNS	92	Name query NB WPAD<00>
6	1.024241	192.168.1.41	192.168.1.255	NBNS	92	Name query NB DESKTOP-KK9C2GC<1c>
10	1.288603	192.168.1.34	195.175.39.50	DNS	72	Standard query 0xdab6 A www.espn.com
11	1.289907	192.168.1.34	195.175.39.50	DNS	75	Standard query 0x6fb5 A secure.espn.com
16	1.293203	192.168.1.34	195.175.39.50	DNS	72	Standard query 0xe874 A dcf.espn.com
18	1.331329	192.168.1.41	192.168.1.255	NBNS	92	Name query NB WPAD<00>
24	1.370576	195.175.39.50	192.168.1.34	DNS	146	Standard query response 0xe874 A dcf.espn.com C
26	1.372473	195.175.39.50	192.168.1.34	DNS	136	Standard query response 0xdab6 A www.espn.com A
27	1.373043	192.168.1.34	195.175.39.50	DNS	73	Standard query 0xe3df A a.espncdn.com
33	1.382843	192.168.1.34	195.175.39.49	DNS	75	Standard query 0x6fb5 A secure.espn.com
34	1.385572	195.175.39.50	192.168.1.34	DNS	183	Standard query response 0x6fb5 A secure.espn.co
46	1.462736	195.175.39.50	192.168.1.34	DNS	181	Standard query response 0xe3df A a.espncdn.com
60	1.554196	195.175.39.49	192.168.1.34	DNS	183	Standard query response 0x6fb5 A secure.espn.co
65	1.740845	fe80::e868:176a:a0d...	ff02::1:3	LLMNR	84	Standard query 0x7881 A wpad
66	1.740845	192.168.1.41	224.0.0.252	LLMNR	64	Standard query 0x7881 A wpad
127	2.047559	192.168.1.41	192.168.1.255	NBNS	92	Name query NB WPAD<00>

▶ Frame 10: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{D1B4F362-C83D-4147-9DE3-E73F2...
 ▶ Ethernet II, Src: IntelCor_3c:ec:18 (d0:7e:35:3c:ec:18), Dst: ZyxelCom_87:a0:5c (b8:ec:a3:87:a0:5c)
 ▶ Internet Protocol Version 4, Src: 192.168.1.34, Dst: 195.175.39.50
 ▶ User Datagram Protocol, Src Port: 51565, Dst Port: 53

Source Port: 51565
 Destination Port: 53
 Length: 38
 Checksum: 0x7c62 [unverified]
 [Checksum Status: Unverified]
 [Stream index: 3]
 [Timestamps]
 UDP payload (30 bytes)

▶ Domain Name System (query)

0000	b8 ec a3 87 a0 5c d0 7e 35 3c ec 18 08 00 45 00~ 5<...E-
0010	00 3a 3d db 00 00 80 11 50 2c c0 a8 01 22 c3 af	...:=... P..."-..
0020	27 32 c9 6d 00 35 00 26 7c 62 da b6 01 00 00 01	'2-m-5-& 10.....
0030	00 00 00 00 00 00 03 77 77 77 04 65 73 70 6e 03w ww.espn-
0040	63 6f 6d 00 00 01 00 01	com.....

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 is 38, is the sum of the 8 header bytes and the remaining data bytes encapsulated in the packet.

udp						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.41	224.0.0.251	MDNS	70	Standard query 0x0000 A wpad.local, "QM" question
2	0.000000	fe80::e868:176a:a0d...	ff02::fb	MDNS	90	Standard query 0x0000 A wpad.local, "QM" question
3	0.307162	192.168.1.41	192.168.1.255	NBNS	92	Name query NB DESKTOP-KK9C2GC<1c>
5	0.512038	192.168.1.41	192.168.1.255	NBNS	92	Name query NB WPAD<00>
6	1.024241	192.168.1.41	192.168.1.255	NBNS	92	Name query NB DESKTOP-KK9C2GC<1c>
10	1.288603	192.168.1.34	195.175.39.50	DNS	72	Standard query 0xdab6 A www.espn.com
11	1.289907	192.168.1.34	195.175.39.50	DNS	75	Standard query 0x6fb5 A secure.espn.com
16	1.293203	192.168.1.34	195.175.39.50	DNS	72	Standard query 0xe874 A dcf.espn.com
18	1.331329	192.168.1.41	192.168.1.255	NBNS	92	Name query NB WPAD<00>
24	1.370576	195.175.39.50	192.168.1.34	DNS	146	Standard query response 0xe874 A dcf.espn.com CNAME twdc-dtci.edg
26	1.372473	195.175.39.50	192.168.1.34	DNS	136	Standard query response 0xdab6 A www.espn.com A 54.192.233.35 A 5
27	1.373043	192.168.1.34	195.175.39.50	DNS	73	Standard query 0xe3df A a.espncdn.com
33	1.382843	192.168.1.34	195.175.39.49	DNS	75	Standard query 0x6fb5 A secure.espn.com
34	1.385572	195.175.39.50	192.168.1.34	DNS	183	Standard query response 0x6fb5 A secure.espn.com CNAME secure.esp
46	1.462736	195.175.39.50	192.168.1.34	DNS	181	Standard query response 0xe3df A a.espncdn.com CNAME a.espncdn.co
60	1.554196	195.175.39.49	192.168.1.34	DNS	183	Standard query response 0x6fb5 A secure.espn.com CNAME secure.esp
65	1.740845	fe80::e868:176a:a0d...	ff02::1:3	LLMNR	84	Standard query 0x7881 A wpad
66	1.740845	192.168.1.41	224.0.0.252	LLMNR	64	Standard query 0x7881 A wpad
127	2.047559	192.168.1.41	192.168.1.255	NBNS	92	Name query NB WPAD<00>

▶ Frame 10: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{D1B4F362-C83D-4147-9DE3-E73F2017E46E}, id 0
 ▶ Ethernet II, Src: IntelCor_3c:ec:18 (d0:7e:35:3c:ec:18), Dst: ZyxelCom_87:a0:5c (b8:ec:a3:87:a0:5c)
 ▶ Internet Protocol Version 4, Src: 192.168.1.34, Dst: 195.175.39.50
 ▶ User Datagram Protocol, Src Port: 51565, Dst Port: 53
 Source Port: 51565
 Destination Port: 53
 Length: 38
 Checksum: 0x7c62 [unverified]
 [Checksum Status: Unverified]
 [Stream index: 3]
 ▶ [Timestamps]
 UDP payload (30 bytes)
 ▶ Domain Name System (query)

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.

udp						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.41	224.0.0.251	MDNS	70	Standard query 0x0000 A wpad.local, "QM" ques
2	0.000000	fe80::e868:176a:a0d...	ff02::fb	MDNS	90	Standard query 0x0000 A wpad.local, "QM" ques
3	0.307162	192.168.1.41	192.168.1.255	NBNS	92	Name query NB DESKTOP-KK9C2GC<1c>
5	0.512038	192.168.1.41	192.168.1.255	NBNS	92	Name query NB WPAD<00>
6	1.024241	192.168.1.41	192.168.1.255	NBNS	92	Name query NB DESKTOP-KK9C2GC<1c>
10	1.288603	192.168.1.34	195.175.39.50	DNS	72	Standard query 0xdab6 A www.espn.com
11	1.289907	192.168.1.34	195.175.39.50	DNS	75	Standard query 0x6fb5 A secure.espn.com
16	1.293203	192.168.1.34	195.175.39.50	DNS	72	Standard query 0xe874 A dcf.espn.com
18	1.331329	192.168.1.41	192.168.1.255	NBNS	92	Name query NB WPAD<00>
24	1.370576	195.175.39.50	192.168.1.34	DNS	146	Standard query response 0xe874 A dcf.espn.com
26	1.372473	195.175.39.50	192.168.1.34	DNS	136	Standard query response 0xdab6 A www.espn.com
27	1.373043	192.168.1.34	195.175.39.50	DNS	73	Standard query 0xe3df A a.espncdn.com
33	1.382843	192.168.1.34	195.175.39.49	DNS	75	Standard query 0x6fb5 A secure.espn.com
34	1.385572	195.175.39.50	192.168.1.34	DNS	183	Standard query response 0x6fb5 A secure.espn.
46	1.462736	195.175.39.50	192.168.1.34	DNS	181	Standard query response 0xe3df A a.espncdn.co
60	1.554196	195.175.39.49	192.168.1.34	DNS	183	Standard query response 0x6fb5 A secure.espn.
65	1.740845	fe80::e868:176a:a0d...	ff02::1:3	LLMNR	84	Standard query 0x7881 A wpad
66	1.740845	192.168.1.41	224.0.0.252	LLMNR	64	Standard query 0x7881 A wpad
127	2.047559	192.168.1.41	192.168.1.255	NBNS	92	Name query NB WPAD<00>

Total Length: 58	
Identification: 0x3ddb (15835)	
Flags: 0x00	
0... = Reserved bit: Not set	
.0.. = Don't fragment: Not set	
..0. = More fragments: Not set	
Fragment Offset: 0	
Time to Live: 128	
Protocol: UDP (17)	
Header Checksum: 0x502c [validation disabled]	
[Header checksum status: Unverified]	
Source Address: 192.168.1.34	
Destination Address: 195.175.39.50	

0000	b8 ec a3 87 a0 5c d0 7e	35 3c ec 18 08 00 45 00\~ 5<....E-
0010	00 3a 3d db 00 00 80 11	50 2c c0 a8 01 22 c3 af	:=... P,..."..
0020	27 32 c9 6d 00 35 00 26	7c 62 da b6 01 00 00 01	'2-m-5-& b.....
0030	00 00 00 00 00 00 03 77	77 77 04 65 73 70 6e 03w ww-espn-
0040	63 6f 6d 00 00 01 00 01		com.....

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

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.41	224.0.0.251	MDNS	70	Standard query 0x0000 A wpad.local, "QM" question
2	0.000000	fe80::e868:176a:a0d...	ff02::fb	MDNS	90	Standard query 0x0000 A wpad.local, "QM" question
3	0.307162	192.168.1.41	192.168.1.255	NBNS	92	Name query NB DESKTOP-KK9C2GC<1c>
5	0.512038	192.168.1.41	192.168.1.255	NBNS	92	Name query NB WPAD<00>
6	1.024241	192.168.1.41	192.168.1.255	NBNS	92	Name query NB DESKTOP-KK9C2GC<1c>
10	1.288603	192.168.1.34	195.175.39.50	DNS	72	Standard query 0xdab6 A www.espn.com
11	1.289907	192.168.1.34	195.175.39.50	DNS	75	Standard query 0x6fb5 A secure.espn.com
16	1.293203	192.168.1.34	195.175.39.50	DNS	72	Standard query 0xe874 A dcf.espn.com
18	1.331329	192.168.1.41	192.168.1.255	NBNS	92	Name query NB WPAD<00>
24	1.370576	195.175.39.50	192.168.1.34	DNS	146	Standard query response 0xe874 A dcf.espn.com CNAME twdc-dtci.edge.nc0.co
26	1.372473	195.175.39.50	192.168.1.34	DNS	136	Standard query response 0xdab6 A www.espn.com A 54.192.233.35 A 54.192.233.
27	1.373043	192.168.1.34	195.175.39.50	DNS	73	Standard query 0xe3df A a.espn.com
33	1.382843	192.168.1.34	195.175.39.49	DNS	75	Standard query 0x6fb5 A secure.espn.com
34	1.385572	195.175.39.50	192.168.1.34	DNS	183	Standard query response 0x6fb5 A secure.espn.com CNAME secure.espn.com
46	1.462736	195.175.39.50	192.168.1.34	DNS	181	Standard query response 0xe3df A a.espn.com CNAME a.espn.com
60	1.554196	195.175.39.49	192.168.1.34	DNS	183	Standard query response 0x6fb5 A secure.espn.com CNAME secure.espn.com
65	1.740845	fe80::e868:176a:a0d...	ff02::1:3	LLMNR	84	Standard query 0x7881 A wpad
66	1.740845	192.168.1.41	224.0.0.252	LLMNR	64	Standard query 0x7881 A wpad
127	2.047559	192.168.1.41	192.168.1.255	NBNS	92	Name query NB WPAD<00>

> Frame 10: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface \Device\NPF_{D1B4F362-C83D-4147-9DE3-E73F2017E46E}, id 0
 > Ethernet II, Src: IntelCor_3c:ec:18 (d0:7e:35:3c:ec:18), Dst: ZyxelCom_87:a0:5c (b8:ec:a3:87:a0:5c)
 > Internet Protocol Version 4, Src: 192.168.1.34, Dst: 195.175.39.50
 > User Datagram Protocol, Src Port: 51565, Dst Port: 53

Source Port: 51565
 Destination Port: 53
 Length: 38
 Checksum: 0x7c62 [unverified]
 [Checksum Status: Unverified]
 [Stream index: 3]
 [Timestamps]
 UDP payload (30 bytes)

UDP Reply to Host

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.41	224.0.0.251	MDNS	70	Standard query 0x0000 A wpad.local, "QM" question
2	0.000000	fe80::e868:176a:a0d...	ff02::fb	MDNS	90	Standard query 0x0000 A wpad.local, "QM" question
3	0.307162	192.168.1.41	192.168.1.255	NBNS	92	Name query NB DESKTOP-KK9C2GC<1c>
5	0.512038	192.168.1.41	192.168.1.255	NBNS	92	Name query NB WPAD<00>
6	1.024241	192.168.1.41	192.168.1.255	NBNS	92	Name query NB DESKTOP-KK9C2GC<1c>
10	1.288603	192.168.1.34	195.175.39.50	DNS	72	Standard query 0xdab6 A www.espn.com
11	1.289907	192.168.1.34	195.175.39.50	DNS	75	Standard query 0x6fb5 A secure.espn.com
16	1.293203	192.168.1.34	195.175.39.50	DNS	72	Standard query 0xe874 A dcf.espn.com
18	1.331329	192.168.1.41	192.168.1.255	NBNS	92	Name query NB WPAD<00>
24	1.370576	195.175.39.50	192.168.1.34	DNS	146	Standard query response 0xe874 A dcf.espn.com CNAME twdc-dtci.edge.nc0.co CNAME edge-geo.nc0.co A 52.51.219.145
26	1.372473	195.175.39.50	192.168.1.34	DNS	136	Standard query response 0xdab6 A www.espn.com A 54.192.233.35 A 54.192.233.15 A 54.192.233.21 A 54.192.233.56
27	1.373043	192.168.1.34	195.175.39.50	DNS	73	Standard query 0xe3df A a.espn.com
33	1.382843	192.168.1.34	195.175.39.49	DNS	75	Standard query 0x6fb5 A secure.espn.com
34	1.385572	195.175.39.50	192.168.1.34	DNS	183	Standard query response 0x6fb5 A secure.espn.com CNAME secure.espn.com.edgesuite.net CNAME a1988.gl.akamai.net
46	1.462736	195.175.39.50	192.168.1.34	DNS	181	Standard query response 0xe3df A a.espn.com CNAME a.espn.com.stls.edgesuite.net CNAME a1793.gl.akamai.net
60	1.554196	195.175.39.49	192.168.1.34	DNS	183	Standard query response 0x6fb5 A secure.espn.com CNAME secure.espn.com.edgesuite.net CNAME a1988.gl.akamai.net
65	1.740845	fe80::e868:176a:a0d...	ff02::1:3	LLMNR	84	Standard query 0x7881 A wpad
66	1.740845	192.168.1.41	224.0.0.252	LLMNR	64	Standard query 0x7881 A wpad
127	2.047559	192.168.1.41	192.168.1.255	NBNS	92	Name query NB WPAD<00>

Frame 26: 136 bytes on wire (1088 bits), 136 bytes captured (1088 bits) on interface \Device\NPF_{D1B4F362-C83D-4147-9DE3-E73F2017E46E}, id 0

Ethernet II, Src: ZyxelCom_87:a0:5c (b8:ec:a3:87:a0:5c), Dst: IntelCor_3c:ec:18 (d0:7e:35:3c:ec:18)

Internet Protocol Version 4, Src: 195.175.39.50, Dst: 192.168.1.34

User Datagram Protocol, Src Port: 53, Dst Port: 51565

Source Port: 53

Destination Port: 51565

Length: 102

Checksum: 0x7a9f [unverified]

[Checksum Status: Unverified]

[Stream index: 3]

[Timestamps]

UDP payload (94 bytes)

Domain Name System (response)

0000 d0 7e 35 3c ec 18 b8 ec a3 87 a0 5c 08 00 45 00 --5<... ..E

0010 00 7a 3d ef 40 00 fa 11 95 d7 c3 af 27 32 c0 a8 ze@... '2...

0020 01 22 00 35 c9 6d 00 66 7a 9f da b6 81 80 00 01 ".5m-f Z.....

0030 00 04 00 00 00 00 03 77 77 77 04 65 73 70 6e 03w ww.espn...

0040 63 6f 6d 00 00 01 00 01 c0 0c 00 01 00 01 00 00 com.....

0050 00 3c 00 04 36 c0 e9 23 c0 0c 00 01 00 01 00 00 <.6..#

0060 00 3c 00 04 36 c0 e9 0f c0 0c 00 01 00 01 00 00 <.6..#

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.