

UDP

Yogesh P
201EE138

1. Select the first UDP segment in your trace. What is the packet number of this segment in the trace file? What type of application-layer payload or protocol message is being carried in this UDP segment? Look at the details of this packet in Wireshark. How many fields there are in the UDP header?

A: Packet number is 8, Application layer protocol is HTTP/1.1, There are Four Fields.

The image shows a Wireshark packet capture analysis. The top pane displays a list of network packets. Packet 8, at time 2.766974, is selected. It is a UDP segment from source 10.0.0.254 to destination 239.255.255.250, with length 326 bytes. The protocol is identified as NOTIFY * HTTP/1.1.

The middle pane shows the details of the selected packet. It is a User Datagram Protocol (UDP) segment, Src Port: 47931, Dst Port: 1900. The length is 292 bytes. The checksum is 0xe99e (unverified). The stream index is 0. The UDP payload (284 bytes) is a Simple Service Discovery Protocol (SSDP) message.

The bottom pane shows the raw packet data in hexadecimal and ASCII. The ASCII column shows the SSDP NOTIFY message structure, including fields like 'NOTIFY', 'HTTP/1.1', and 'T: 239.2.55.255.2'.

No.	Time	Source	Destination	Protocol	Length	Info
5	2.764896	10.0.0.254	239.255.255.250	SSDP	317	NOTIFY * HTTP/1.1
6	2.765750	10.0.0.254	239.255.255.250	SSDP	317	NOTIFY * HTTP/1.1
7	2.766303	10.0.0.254	239.255.255.250	SSDP	326	NOTIFY * HTTP/1.1
8	2.766974	10.0.0.254	239.255.255.250	SSDP	326	NOTIFY * HTTP/1.1
9	2.767715	10.0.0.254	239.255.255.250	SSDP	381	NOTIFY * HTTP/1.1
10	2.768361	10.0.0.254	239.255.255.250	SSDP	381	NOTIFY * HTTP/1.1
11	2.769103	10.0.0.254	239.255.255.250	SSDP	391	NOTIFY * HTTP/1.1
12	2.769651	10.0.0.254	239.255.255.250	SSDP	391	NOTIFY * HTTP/1.1
15	3.325064	10.0.0.44	75.75.75.75	DNS	77	Standard query 0x3c29 A gaia.cs.umass.edu
17	3.348972	75.75.75.75	10.0.0.44	DNS	93	Standard query response 0x3c29 A gaia.cs.umass.edu A 128.119.245.12
30	3.427392	10.0.0.44	75.75.75.75	DNS	83	Standard query 0xeda4 A maxcdn.bootstrapcdn.com
31	3.428514	10.0.0.44	75.75.75.75	DNS	79	Standard query 0xa79 A ajax.googleapis.com
35	3.445049	75.75.75.75	10.0.0.44	DNS	135	Standard query response 0xeda4 A maxcdn.bootstrapcdn.com CNAME cds.j3z9t3p6.hwcdn.net A 209.197.3.15
36	3.448906	75.75.75.75	10.0.0.44	DNS	95	Standard query response 0xa79 A ajax.googleapis.com A 172.217.12.202
521	3.678228	10.0.0.44	75.75.75.75	DNS	75	Standard query 0xdcfa A www.pearson.com
522	3.678393	10.0.0.44	75.75.75.75	DNS	79	Standard query 0xb436 A www.vitalsource.com
523	3.678598	10.0.0.44	75.75.75.75	DNS	72	Standard query 0xd3a3 A redshelf.com
526	3.695928	75.75.75.75	10.0.0.44	DNS	169	Standard query response 0xdcfa A www.pearson.com CNAME wildcard.pearson.com.edgekey.net CNAME e290.x.akamaiedge.net A 23.34.92...
527	3.698647	10.0.0.44	75.75.75.75	DNS	74	Standard query 0xe1a9 A www.amazon.com
528	3.703716	75.75.75.75	10.0.0.44	DNS	159	Standard query response 0xb436 A www.vitalsource.com A 104.17.67.241 A 104.17.65.241 A 104.17.68.241 A 104.17.69.241 A 104.17.6...

Frame 8: 326 bytes on wire (2608 bits), 326 bytes captured (2608 bits) on interface en0, id 0
Ethernet II, Src: NarayInforma_03:02:01 (00:05:04:03:02:01), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
Internet Protocol Version 4, Src: 10.0.0.254, Dst: 239.255.255.250
User Datagram Protocol, Src Port: 47931, Dst Port: 1900
Source Port: 47931
Destination Port: 1900
Length: 292
Checksum: 0xe99e [unverified]
[Checksum Status: Unverified]
[Stream index: 0]
[Timestamps]
UDP payload (284 bytes)
Simple Service Discovery Protocol

0000 01 00 5e 7f ff fa 00 05 04 03 02 01 08 00 45 00 ..^.....E-
0010 01 38 a1 c6 40 00 04 11 d8 f6 0a 00 00 fe ef ff -8-@.....
0020 ff fa bb 3b 07 6c 01 24 e9 9e 4e 4f 54 49 46 59 ...;1.\$NOTIFY
0030 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48 4f 53 * HTTP/1.1 -HOS
0040 54 3a 20 32 33 39 2e 32 35 35 2e 32 35 35 2e 32 T: 239.2 55.255.2
0050 35 30 3a 31 39 30 30 0d 0a 43 41 43 48 45 2d 43 50:1900 -CACHE-C
0060 4f 4e 54 52 4f 4c 3a 20 6d 61 78 2d 61 67 65 3d ONTROL: max-age=
0070 31 38 30 31 0d 0a 4e 54 53 3a 20 73 73 64 70 3a 1801-NT S: ssdp:
0080 61 6c 69 76 65 0d 0a 4c 4f 43 41 54 49 4f 4e 3a alive-L OCATION:
0090 20 68 74 74 70 3a 2f 2f 31 30 2e 30 2e 30 2e 32 http:// 10.0.0.2
00a0 35 34 3a 34 39 31 35 32 2f 77 70 73 5f 64 65 76 54:49152 /wps_dev
00b0 69 63 65 2e 78 6d 6c 0d 0a 53 45 52 56 45 52 3a ice.xml -SERVER:
00c0 20 55 6e 73 70 65 63 69 66 69 65 64 2c 20 55 50 Unspeci fied, UP
00d0 6e 50 2f 31 2e 30 2c 20 55 6e 73 70 65 63 69 66 nP/1.0, Unspecif
00e0 69 65 64 0d 0a 4e 54 3a 20 75 75 69 64 3a 31 32 ied-NT: uuid:12
00f0 36 30 63 61 39 37 2d 61 66 37 39 2d 35 36 39 32 60ca97-a f79-5692
0100 2d 38 66 31 35 2d 37 30 63 30 34 39 32 38 34 63 -8f15-70 c049284c
0110 62 61 0d 0a 55 53 4e 3a 20 75 75 69 64 3a 31 32 ba -USN: uuid:12
0120 36 30 63 61 39 37 2d 61 66 37 39 2d 35 36 39 32 60ca97-a f79-5692
0130 2d 38 66 31 35 2d 37 30 63 30 34 39 32 38 34 63 -8f15-70 c049284c
0140 62 61 0d 0a 5d 0a ba

Details at: https://www.wireshark.org/docs/wsug_html_chunked/ChAdvChecksums.html (udp.checksum), 2 bytes
Packets: 563 · Displayed: 24 (4.3%)
Profile: Default

2. By consulting the displayed information in Wireshark's packet content field for this packet (or by consulting the textbook), what is the length (in bytes) of each of the UDP header fields?

A: 2 bytes each, total is 8 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.

A: 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. The length of UDP payload for selected packet is 32 bytes. $292 \text{ bytes} - 8 \text{ bytes} = 286 \text{ bytes}$.

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

A: Here the largest source port number is $2^{16}-1=65535$, The UDP header is 8 bytes so maximum number of bytes which can be included in the UDP payload is $65535-8=65527$ bytes.

5. What is the largest possible source port number?

A: Maximum possible source port number is $2^{16}-1=65535$.

6.What is the protocol number for UDP? Give your answer in decimal notation. To answer this question, you'll need to look into the Protocol field of the IP datagram containing this UDP segment.

A:The IP protocol number for UDP is 0x11 hex, which is 17 in decimal value

The image shows a Wireshark capture of a network packet. The top pane displays a list of packets, with packet 17 selected. The middle pane shows the details of packet 17, which is a DNS response. The bottom pane shows the raw packet data in hexadecimal and ASCII.

Packets List:

No.	Time	Source	Destination	Protocol	Length	Info
5	2.764896	10.0.0.254	239.255.255.250	SSDP	317	NOTIFY * HTTP/1.1
6	2.765750	10.0.0.254	239.255.255.250	SSDP	317	NOTIFY * HTTP/1.1
7	2.766303	10.0.0.254	239.255.255.250	SSDP	326	NOTIFY * HTTP/1.1
8	2.766974	10.0.0.254	239.255.255.250	SSDP	326	NOTIFY * HTTP/1.1
9	2.767715	10.0.0.254	239.255.255.250	SSDP	381	NOTIFY * HTTP/1.1
10	2.768361	10.0.0.254	239.255.255.250	SSDP	381	NOTIFY * HTTP/1.1
11	2.769103	10.0.0.254	239.255.255.250	SSDP	391	NOTIFY * HTTP/1.1
12	2.769651	10.0.0.254	239.255.255.250	SSDP	391	NOTIFY * HTTP/1.1
15	3.325064	10.0.0.44	75.75.75.75	DNS	77	Standard query 0x3c29 A gaia.cs.umass.edu
17	3.348972	75.75.75.75	10.0.0.44	DNS	93	Standard query response 0x3c29 A gaia.cs.umass.edu A 128.119.245.12
30	3.427392	10.0.0.44	75.75.75.75	DNS	83	Standard query 0xeda4 maxcdn.bootstrapcdn.com
31	3.428514	10.0.0.44	75.75.75.75	DNS	79	Standard query 0xa79 A ajax.googleapis.com
35	3.445049	75.75.75.75	10.0.0.44	DNS	135	Standard query response 0xeda4 A maxcdn.bootstrapcdn.com CNAME cds-j3z9t3p6.hwcdn.net A 209.197.3.15
36	3.448906	75.75.75.75	10.0.0.44	DNS	95	Standard query response 0xa79 A ajax.googleapis.com A 172.217.12.202
521	3.678228	10.0.0.44	75.75.75.75	DNS	75	Standard query 0xdcfa A www.pearson.com
522	3.678393	10.0.0.44	75.75.75.75	DNS	79	Standard query 0xb436 A www.vitalsource.com
523	3.678598	10.0.0.44	75.75.75.75	DNS	72	Standard query 0xd3a3 A redshelf.com
526	3.695928	75.75.75.75	10.0.0.44	DNS	169	Standard query response 0xdcfa A www.pearson.com CNAME wildcard.pearson.com.edgekey.net CNAME e290.x.akamaiedge.net A 23.34.92...
527	3.698647	10.0.0.44	75.75.75.75	DNS	74	Standard query 0xe1a9 A www.amazon.com
528	3.703716	75.75.75.75	10.0.0.44	DNS	159	Standard query response 0xb436 A www.vitalsource.com A 104.17.67.241 A 104.17.65.241 A 104.17.68.241 A 104.17.69.241 A 104.17.6...

Packet 17 Details:

- Frame 17: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on interface en0, id 0
- Ethernet II, Src: Maxlinear_80:00:00 (00:50:f1:80:00:00), Dst: Apple_98:d9:27 (78:4f:43:98:d9:27)
- Internet Protocol Version 4, Src: 75.75.75.75, Dst: 10.0.0.44
 - 0100 = Version: 4
 - 0101 = Header Length: 20 bytes (5)
 - Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 - Total Length: 79
 - Identification: 0x0000 (0)
 - 010. = Flags: 0x2, Don't fragment
 - ...0 0000 0000 0000 = Fragment Offset: 0
 - Time to Live: 58
 - Protocol: UDP (17)
 - Header Checksum: 0x9fdc [validation disabled]
 - [Header checksum status: Unverified]
 - Source Address: 75.75.75.75
 - Destination Address: 10.0.0.44
- User Datagram Protocol, Src Port: 53, Dst Port: 58350
- Domain Name System (response)

Raw Data:

```
0000 78 4f 43 98 d9 27 00 50 f1 80 00 00 08 00 45 00 xOC...'P .....E-
0010 00 4f 00 00 40 00 3a 11 9f dc 4b 4b 4b 4b 0a 00 .O..@.: ..KKKK..
0020 00 2c 00 35 e3 ee 00 3b 4a f2 3c 29 81 80 00 01 .,5...; J<)....
0030 00 01 00 00 00 00 04 67 61 69 61 02 63 73 05 75 .....g aia:cs u
0040 6d 61 73 73 03 65 64 75 00 00 01 00 01 c0 0c 00 mass-edu .....
0050 01 00 01 00 00 54 60 00 04 80 77 f5 0c .....T' ..w...
```

7. Examine the 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). What is the packet number of the first of these two UDP segments in the trace file? What is the value in the source port field in this UDP segment? What is the value in the destination port field in this UDP segment? What is the packet number of the second of these two UDP segments in the trace file? What is the value in the source port field in this second UDP segment? What is the value in the destination port field in this second UDP segment? Describe the relationship between the port numbers in the two packets.

A:Packet number of the first UDP segment: 15 , Source port field: 10.0.0.44 ,

Destination port field: 75.75.75.75 , Packet number of the second UDP segment: 17,

Source port field: 75.75.75.75 ,Destination port field: 10.0.0.44,

The relationship between the port numbers in the two packets is that the source port of the first packet (10.0.0.44) corresponds to the destination port of the second packet, indicating a reply from the destination (75.75.75.75) back to the sender (10.0.0.44).