计算机网络第四次实验实验报告

舒文炫

2021 年 10 月 10 日

目录

Chapter 1

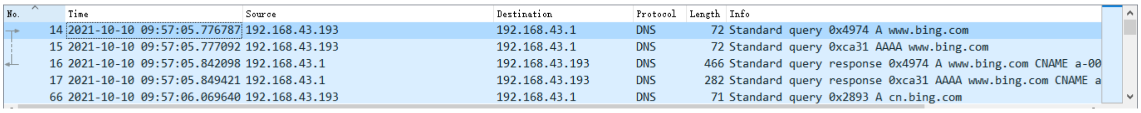
实验内容

本次实验主要学习 UDP 有关内容，主要了解 UDP 报文段格式等。

Chapter 2

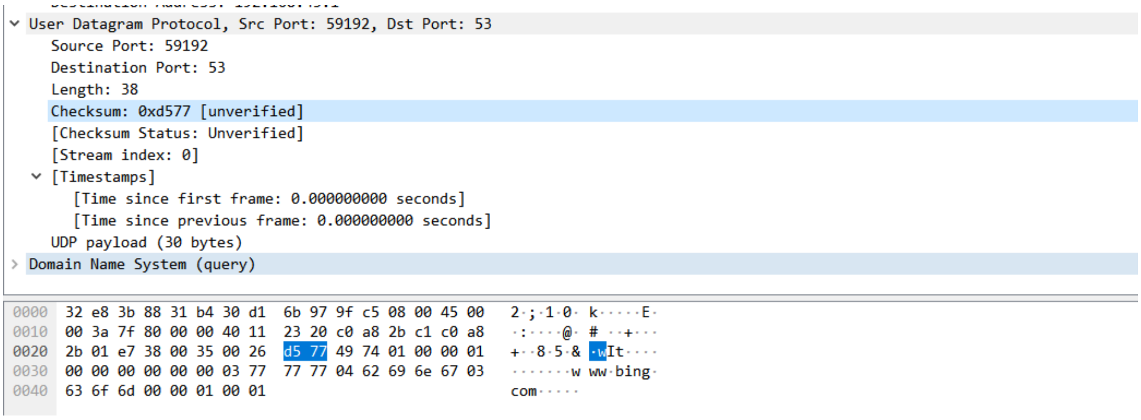
实验过程

首先打开浏览器，然后 wireshark 开始捕获，稍微过一段时间，在过滤器上输入 udp，过滤出 udp 包，截图如下



```
No.   Time                       Source          Destination     Protocol Length Info
   14 2021-10-10 09:57:05.776787 192.168.43.193  192.168.43.1    DNS          72 Standard query 0x4974 A www.bing.com
   15 2021-10-10 09:57:05.777092 192.168.43.193  192.168.43.1    DNS          72 Standard query 0xca31 AAAA www.bing.com
   16 2021-10-10 09:57:05.842098 192.168.43.1    192.168.43.193  DNS         466 Standard query response 0x4974 A www.bing.com CNAME a-00
   17 2021-10-10 09:57:05.849421 192.168.43.1    192.168.43.193  DNS         282 Standard query response 0xca31 AAAA www.bing.com CNAME a
   66 2021-10-10 09:57:06.069640 192.168.43.193  192.168.43.1    DNS          71 Standard query 0x2893 A cn.bing.com
```

我选出来的这个是对 bing.com 的 DNS 查询请求，与之对应后面有一个响应，DNS 是用 UDP 传输的。



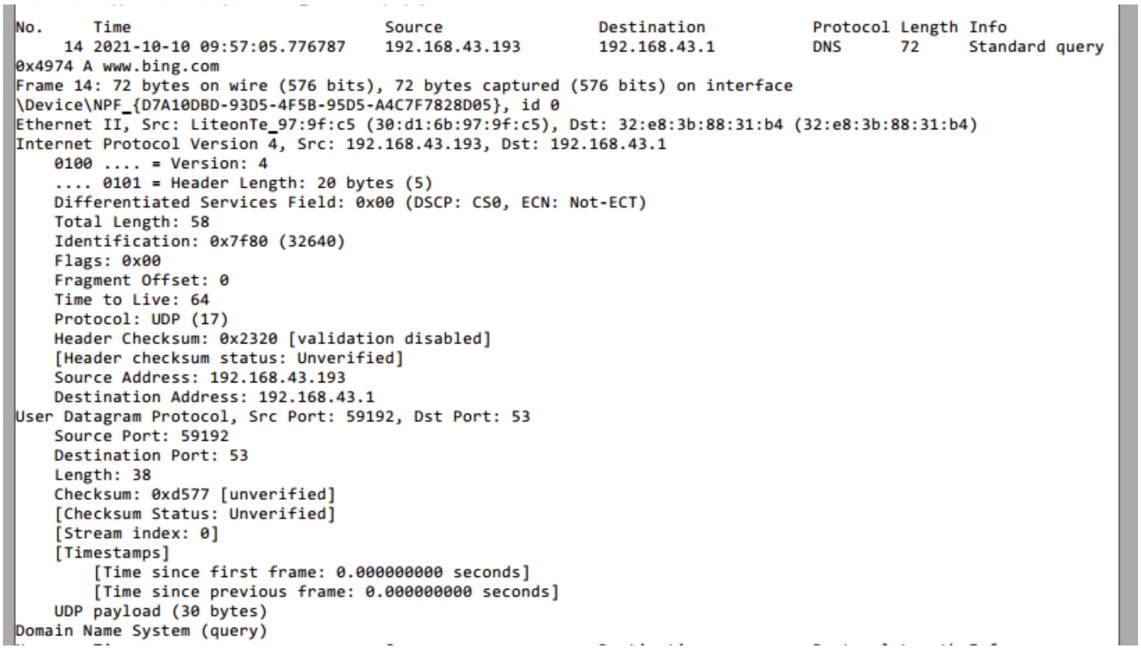
```
v User Datagram Protocol, Src Port: 59192, Dst Port: 53
    Source Port: 59192
    Destination Port: 53
    Length: 38
    Checksum: 0xd577 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  v [Timestamps]
      [Time since first frame: 0.000000000 seconds]
      [Time since previous frame: 0.000000000 seconds]
    UDP payload (30 bytes)
> Domain Name System (query)

0000  32 e8 3b 88 31 b4 30 d1  6b 97 9f c5 08 00 45 00   2·;·1·0· k·····E·
0010  00 3a 7f 80 00 00 40 11  23 20 c0 a8 2b c1 c0 a8   ·:····@· # ··+···
0020  2b 01 e7 38 00 35 00 26  d5 77 49 74 01 00 00 01   +··8·5·& ·wIt····
0030  00 00 00 00 00 00 03 77  77 77 04 62 69 6e 67 03   ·······w ww·bing·
0040  63 6f 6d 00 00 01 00 01                            com·····
```

该截图里面的十六进制码是这个报文的具体内容。

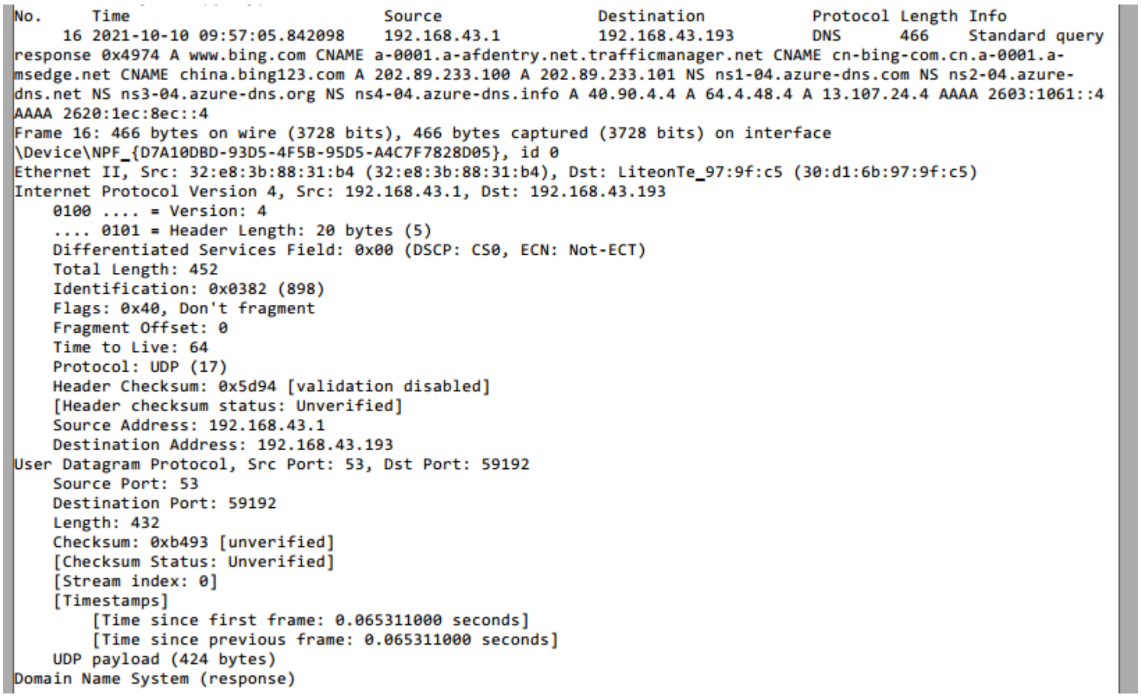
后面两张截图，是将具体内容打印出来的截图

这是 query 报文截图：



```
No.     Time                          Source                Destination           Protocol Length Info
     14 2021-10-10 09:57:05.776787    192.168.43.193        192.168.43.1          DNS      72     Standard query
0x4974 A www.bing.com
Frame 14: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface
\Device\NPF_{D7A10DBD-93D5-4F5B-95D5-A4C7F7828D05}, id 0
Ethernet II, Src: LiteonTe_97:9f:c5 (30:d1:6b:97:9f:c5), Dst: 32:e8:3b:88:31:b4 (32:e8:3b:88:31:b4)
Internet Protocol Version 4, Src: 192.168.43.193, Dst: 192.168.43.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 58
    Identification: 0x7f80 (32640)
    Flags: 0x00
    Fragment Offset: 0
    Time to Live: 64
    Protocol: UDP (17)
    Header Checksum: 0x2320 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.43.193
    Destination Address: 192.168.43.1
User Datagram Protocol, Src Port: 59192, Dst Port: 53
    Source Port: 59192
    Destination Port: 53
    Length: 38
    Checksum: 0xd577 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
    [Timestamps]
        [Time since first frame: 0.000000000 seconds]
        [Time since previous frame: 0.000000000 seconds]
    UDP payload (30 bytes)
Domain Name System (query)
```

这是对应 response 报文截图:



```
No.     Time                          Source                Destination           Protocol Length Info
     16 2021-10-10 09:57:05.842098    192.168.43.1          192.168.43.193        DNS      466    Standard query
response 0x4974 A www.bing.com CNAME a-0001.a-afdentry.net.trafficmanager.net CNAME cn-bing-com.cn.a-0001.a-
msedge.net CNAME china.bing123.com A 202.89.233.100 A 202.89.233.101 NS ns1-04.azure-dns.com NS ns2-04.azure-
dns.net NS ns3-04.azure-dns.org NS ns4-04.azure-dns.info A 40.90.4.4 A 64.4.48.4 A 13.107.24.4 AAAA 2603:1061::4
AAAA 2620:1ec:8ec::4
Frame 16: 466 bytes on wire (3728 bits), 466 bytes captured (3728 bits) on interface
\Device\NPF_{D7A10DBD-93D5-4F5B-95D5-A4C7F7828D05}, id 0
Ethernet II, Src: 32:e8:3b:88:31:b4 (32:e8:3b:88:31:b4), Dst: LiteonTe_97:9f:c5 (30:d1:6b:97:9f:c5)
Internet Protocol Version 4, Src: 192.168.43.1, Dst: 192.168.43.193
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 452
    Identification: 0x0382 (898)
    Flags: 0x40, Don't fragment
    Fragment Offset: 0
    Time to Live: 64
    Protocol: UDP (17)
    Header Checksum: 0x5d94 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.43.1
    Destination Address: 192.168.43.193
User Datagram Protocol, Src Port: 53, Dst Port: 59192
    Source Port: 53
    Destination Port: 59192
    Length: 432
    Checksum: 0xb493 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
    [Timestamps]
        [Time since first frame: 0.065311000 seconds]
        [Time since previous frame: 0.065311000 seconds]
    UDP payload (424 bytes)
Domain Name System (response)
```

Chapter 3

实验思考题

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.

我选择了第 14 个包，这是对 bing.com 的 DNS 查询请求，查看我打印出来的 query 详细信息，在首部有

Source Port: 59192
Destination Port: 53
Length: 38
Checksum: 0xd577 [unverified]
这四行，分别是源端口号，目标端口号，长度，检查和。

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.

这个需要对应我的第二张截图，将鼠标放在对应的行上，下面的十六进制码会有对应的地方被标出来，可以看到从第 23 个字节开始，每两个字节对应一个 field。source port 是 e7 38,destination port 是 00 35，length 是 00 26，checksum 是 d5 77

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.

观察打印出来的 query 信息，length 域的值为 38.

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)

由第二题，length 域的长度为两个字节，从而其值最大对应十六进制数 0xffff, 十进制就是 65535，但是考虑到首部要占 8 个字节，ip 的所以 payload 最大为 65527 个字节。这是理论上的最大长度. 不过实际上超过 512 个字节，会选择用 tcp 了。

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

由第 2 题，源端口号是两个字节，最大值为 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).

观察我的 query 报文截图，在 ip datagram 那里有一行，Protocol: UDP (17)，表示 UDP 的协议号是 17，这是十进制表示，若用 16 进制表示，UDP 的协议号是 0x11.

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.

对比一下我的 query 截图和 response 截图里面的端口，在 query 截图里面端口为 Src Port: 59192, Dst Port: 53，在 response 截图里面端口为 Src Port: 53, Dst Port: 59192，可以发现，前一个 UDP 包源端口是后一个 UDP 包的目标端口，前一个 UDP 包的目标端口是后一个 UDP 包的源端口。

Chapter 4

实验总结

本次实验让我更深刻的理解了 UDP 报文段的结构，其中比较印象深刻的是在 length 那里，理论上 UDP 最大的 payload 是 65527 个字节，但是涉及实际应用，局域网链路层的 MTU(最大传输单元) 是 1500 字节, 去掉 ip 首部和 udp 首部，这里的 udp 最大为 1472 字节。internet 下的时候，MTU 是各个路由器进行一个配置的。通常路由器默认的 MTU 为 576 字节。同理 UDP 最大为 548。所以，为了适应网络环境，DNS 协议在返回的数据报大于 512 的时候，会转化为 TCP 协议。