

SDN 实验报告——网络协议分析

(一) DHCP 协议

DHCP (Dynamic Host configuration protocol, 动态主机配置协议) 协议的主要功能是为客户端自动分配 IP 地址、子网掩码以及缺省网关、DNS 服务器 IP 地址等 TCP/IP 参数。

在 Windows 下通过 cmd 输入 ipconfig /release 及 ipconfig /renew 命令重新配置 IP 地址等参数。截获的 DHCP 报文如下:

71 8.912621	0.0.0.0	255.255.255.255	DHCP	344 DHCP Discover - Transaction ID 0x6e18b1a7
78 9.524847	192.168.1.1	255.255.255.255	DHCP	590 DHCP Offer - Transaction ID 0x6e18b1a7
79 9.528555	0.0.0.0	255.255.255.255	DHCP	370 DHCP Request - Transaction ID 0x6e18b1a7
81 9.730692	192.168.1.1	255.255.255.255	DHCP	590 DHCP ACK - Transaction ID 0x6e18b1a7

①DHCP Discover: DHCP 客户端在请求 IP 地址时并不知道 DHCP 服务器的位置,因此 DHCP 客户端会在本地网络内以广播方式(目的 IP 地址:255.255.255.255)发送 Discover 请求报文,以发现网络中的 DHCP 服务器。由于客户端此时还不知道自己属于哪一个网路,所以数据包的源 IP 地址为 0.0.0.0。

71 8.9126210.0.0.0255.255.255.255DHCP344 DHCP Discover - Transaction ID 0x6e18b1a7

Frame 71: 344 bytes on wire (2752 bits), 344 bytes captured (2752 bits) on interface \Device\NPF_{8B6AC3F0-68F4-4AC6-AA5A-71887A078039}, id 0
Ethernet II, Src: IntelCor_53:49:a9 (f8:e4:e3:53:49:a9), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
User Datagram Protocol, Src Port: 68, Dst Port: 67
Dynamic Host Configuration Protocol (Discover)
Message type: Boot Request (1) 客户端请求
Hardware type: Ethernet (0x01)
Hardware address length: 6
Hops: 0
Transaction ID: 0x6e18b1a7 客户端随机生成的 ID, 用以标志本次 DHCP 通信
Seconds elapsed: 0
Bootp flags: 0x8000, Broadcast flag (Broadcast)
1... .. = Broadcast flag: Broadcast
.000 0000 0000 0000 = Reserved flags: 0x0000
Client IP address: 0.0.0.0
Your (client) IP address: 0.0.0.0
Next server IP address: 0.0.0.0
Relay agent IP address: 0.0.0.0
Client MAC address: IntelCor_53:49:a9 (f8:e4:e3:53:49:a9)
Client hardware address padding: 00000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP

71 8.9126210.0.0.0255.255.255.255DHCP344 DHCP Discover - Transaction ID 0x6e18b1a7

> Option: (53) DHCP Message Type (Discover)
Length: 1
DHCP: Discover (1)
> Option: (61) Client identifier
Length: 7
Hardware type: Ethernet (0x01)
Client MAC address: IntelCor_53:49:a9 (f8:e4:e3:53:49:a9)
> Option: (50) Requested IP Address (192.168.1.110)
Length: 4
Requested IP Address: 192.168.1.110 请求分配的 IP 地址
> Option: (12) Host Name
Length: 15
Host Name: LAPTOP-ROMI2L28
> Option: (60) Vendor class identifier
Length: 8
Vendor class identifier: MSFT 5.0
> Option: (55) Parameter Request List
Length: 14
Parameter Request List Item: (1) Subnet Mask
Parameter Request List Item: (3) Router
Parameter Request List Item: (6) Domain Name Server
Parameter Request List Item: (15) Domain Name
Parameter Request List Item: (31) Perform Router Discover
Parameter Request List Item: (33) Static Route
Parameter Request List Item: (43) Vendor-Specific Information
Parameter Request List Item: (44) NetBIOS over TCP/IP Name Server
Parameter Request List Item: (46) NetBIOS over TCP/IP Node Type
Parameter Request List Item: (47) NetBIOS over TCP/IP Scope
Parameter Request List Item: (119) Domain Search
Parameter Request List Item: (121) Classless Static Route
Parameter Request List Item: (249) Private/Classless Static Route (Microsoft)
Parameter Request List Item: (252) Private/Proxy autodiscovery
> Option: (255) End

通知服务器 Offer 以广播发出

设置请求选项列表, 客户端利用该选项指明需要从 DHCP 服务器获取哪些网络配置参数。如子网掩码、默认网关、DNS 服务器 IP 地址等。

②DHCP Offer: DHCP 服务器收到 Discover 报文后, 就会在所配置的地址池

中查找一个合适的 IP 地址，加上相应的租约期限和其他配置信息（如网关、DNS 服务器等），构造一个 Offer 报文，发送给 DHCP 客户端，告知用户本服务器可以为其提供 IP 地址。

[illegible]

③DHCP Request: DHCP 客户端可能会收到很多 Offer 报文, 通常是选择第一个 Offer 报文的服务器作为自己的目标服务器, 并向该服务器发送一个广播的 Request 请求报文, 通告选择的服务器, 希望获得所分配的 IP 地址。

```

79 9.528555      0.0.0.0      255.255.255.255      DHCP      370 DHCP Request - Transaction ID 0x6e18b1a7
  Frame 79: 370 bytes on wire (2960 bits), 370 bytes captured (2960 bits) on interface \Device\NPF_{8B6AC3F0-68F4-4AC6-AA5A-71887A078039}, id 0
  Ethernet II, Src: IntelCor_53:49:a9 (f8:e4:e3:53:49:a9), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
  User Datagram Protocol, Src Port: 68, Dst Port: 67
  Dynamic Host Configuration Protocol (Request)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x6e18b1a7 标志 ID, 仍然保持不变
    Seconds elapsed: 0
  > Bootp flags: 0x8000, Broadcast flag (Broadcast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 0.0.0.0 由于此时尚未分配到 IP 地址, 故源地址仍为 0.0.0.0
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: IntelCor_53:49:a9 (f8:e4:e3:53:49:a9)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Request)
    Length: 1
    DHCP: Request (3)
  > Option: (61) Client identifier
    Length: 7
    Hardware type: Ethernet (0x01)
    Client MAC address: IntelCor_53:49:a9 (f8:e4:e3:53:49:a9) 客户端 MAC 地址, 用以标志客户端
  > Option: (50) Requested IP Address (192.168.1.110)
    Length: 4
    Requested IP Address: 192.168.1.110
  > Option: (54) DHCP Server Identifier (192.168.1.1) 目标 DHCP 服务器的 IP 地址
    Length: 4
    DHCP Server Identifier: 192.168.1.1

```

```

79 9.528555      255.255.255.255    DHCP          370 DHCP Request - Transaction ID 0x6e18b1a7
  Option: (12) Host Name
    Length: 15
    Host Name: LAPTOP-ROMI2L28
  Option: (81) Client Fully Qualified Domain Name
    Length: 18
    Flags: 0x00
    A-RR result: 0
    PTR-RR result: 0
    Client name: LAPTOP-ROMI2L28
  Option: (60) Vendor class identifier
    Length: 8
    Vendor class identifier: MSFT 5.0
  Option: (55) Parameter Request List
    Length: 14
    Parameter Request List Item: (1) Subnet Mask
    Parameter Request List Item: (3) Router
    Parameter Request List Item: (6) Domain Name Server
    Parameter Request List Item: (15) Domain Name
    Parameter Request List Item: (31) Perform Router Discover
    Parameter Request List Item: (33) Static Route
    Parameter Request List Item: (43) Vendor-Specific Information
    Parameter Request List Item: (44) NetBIOS over TCP/IP Name Server
    Parameter Request List Item: (46) NetBIOS over TCP/IP Node Type
    Parameter Request List Item: (47) NetBIOS over TCP/IP Scope
    Parameter Request List Item: (119) Domain Search
    Parameter Request List Item: (121) Classless Static Route
    Parameter Request List Item: (249) Private/Classless Static Route (Microsoft)
    Parameter Request List Item: (252) Private/Proxy autodiscovery
  Option: (255) End
[Community ID: 1:t901j0qj7104wJM7gnaHTgmfv8=]

```

④DHCP ACK: DHCP 服务器收到 Request 请求报文后, 根据 Request 报文中携带的用户 MAC 地址来查找有没有相应的租约记录, 如果有则发送 ACK 应答报文, 通知用户可以使用分配的 IP 地址。

```
      81 9.730692    192.168.1.1        255.255.255.255    DHCP          590 DHCP ACK       - Transaction ID 0x6e18b1a7
✓ Option: (53) DHCP Message Type (ACK)
  Length: 1
  DHCP: ACK (5)
✓ Option: (54) DHCP Server Identifier (192.168.1.1)
  Length: 4
  DHCP Server Identifier: 192.168.1.1
✓ Option: (51) IP Address Lease Time
  Length: 4
  IP Address Lease Time: (7200s) 2 hours
✓ Option: (6) Domain Name Server
  Length: 8
  Domain Name Server: 61.134.1.4
  Domain Name Server: 218.30.19.40
✓ Option: (1) Subnet Mask (255.255.255.0)
  Length: 4
  Subnet Mask: 255.255.255.0
✓ Option: (3) Router
  Length: 4
  Router: 192.168.1.1
✓ Option: (255) End
  Option End: 255
Padding: 0000000000000000000000000000000000000000000000000000000000000000...
[Community ID: 1:RTU96ufLudxAgu4dGf2hzG8lF7w=]
```

ARP (Address Resolution Protocol, 地址转换协议) 是根据 IP 地址获取

当主机访问 `www.xjtu.edu.cn` 时，需要先访问 DNS 服务器进行域名解析，由于服务器 IP 地址与本机不在同一个网段中，故主机会先获取网关的 MAC 地址，再由网关代为转发数据包。截获报文如下：

①ARP 请求报文：由于此时主机不知道网关的 MAC 地址，故主机会将包含网关 IP 地址的 ARP 请求广播到局域网络上的所有主机，并接收返回消息，以此确定网关 MAC 地址。

②ARP 响应报文: 网关收到广播的 ARP 请求报文后, 发现报文中携带的 IP 地址与自己的相同, 便将自己的 MAC 地址填入 ARP 响应报文, 并传送给请求主机。

最终，主机在收到 ARP 响应报文后，将请求的 IP 地址与对应的 MAC 地址填入到 ARP 表（动态维护和更新）中。

DNS (Domain Name System, 域名系统) 是互联网的一项服务。它作为将域名和 IP 地址相互映射的一个分布式数据库, 允许终端设备将给定的人类可读 URL 转换为网络可以理解的机器可用 IP 地址, 能够使人更方便地访问互联网。

①DNS 查询报文:

```

* 104.17.150503 192.168.1.110 61.134.1.4 DNS 75 Standard query 0x331a A www.xjtu.edu.cn
* Frame 104: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\NPF_{8B6AC3F0-68F4-4AC6-AA5A-71887A078039}, id 0
* Ethernet II, Src: IntelCor_53:49:a9 (f8:e4:e3:53:49:a9), Dst: Tp-LinkT_ac:75:a0 (64:6e:97:ac:75:a0)
* Internet Protocol Version 4, Src: 192.168.1.110, Dst: 61.134.1.4 域名服务器地址，与 DHCP 服务器分配的地址相同
* User Datagram Protocol, Src Port: 49334, Dst Port: 53
* Domain Name System (query)
  Transaction ID: 0x331a
  > Flags: 0x0100 standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
* Queries
  > www.xjtu.edu.cn: type A, class IN 查询的域名，type A 表示记录 DNS 域名对应的 IP 地址，class IN 表示查询为互联网地址
  [Response In: 107]

[Community ID: 1:6i+v36Zodgy/ZY2zm1sP+2vdhga4=]
TRANSMISSION Data

```

②DNS 响应报文:

107	17.154860	61.134.1.4	192.168.1.110	DNS	91 Standard query response 0x331a A www.xjtu.edu.cn A 202.117.1.13
> Frame 107: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface \Device\NPF_{8B6AC3F0-68F4-4AC6-AA5A-71887A078039}, id 0					
> Ethernet II, Src: Tp-LinkT_ac:75:a0 (64:6e:97:ac:75:a0), Dst: IntelCor_53:49:a9 (f8:e4:e3:53:49:a9)					
> Internet Protocol Version 4, Src: 61.134.1.4, Dst: 192.168.1.110					
> User Datagram Protocol, Src Port: 53, Dst Port: 49334					
▼ Domain Name System (response)					
Transaction ID: 0x331a					
> Flags: 0x8180 Standard query response, No error					
Questions: 1					
Answer RRs: 1 应答标志					
Authority RRs: 0					
Additional RRs: 0					
▼ Queries					
> www.xjtu.edu.cn: type A, class IN					
▼ Answers					
> www.xjtu.edu.cn: type A, class IN, addr 202.117.1.13 返回域名所对应的 IP 地址					
[Request in: 104]					
[Time: 0.004357000 seconds]					
[Community ID: 1:Gi+v36ZodgV/Z22mlsP+2Vdhga4=]					

(四) TCP 协议

TCP (Transmission Control Protocol, 传输控制协议) 是为了在不可靠的互联网络上提供可靠的端到端字节流而专门设计的一个传输层协议。

①建立连接:

112	17.160862	192.168.1.110	202.117.1.13	TCP	66 62659 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
116	17.166530	202.117.1.13	192.168.1.110	TCP	66 80 → 62659 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1440 SACK_PERM WS=128
119	17.166680	192.168.1.110	202.117.1.13	TCP	54 62659 → 80 [ACK] Seq=1 Ack=1 Win=132352 Len=0

首先, 主机向服务器发送一个 SYN 位置 1 的连接请求报文, 当服务器收到该报文后, 发送 SYN 和 ACK 位均置 1 的报文来对第一个 SYN 报文段进行确认。最后, 主机再发送一个 ACK 位置 1 的确认报文, 来通知服务器双方已完成连接的建立。

三次握手除了完成可靠连接的建立外, 还使双方确认了各自的初始序号。从上图可以看出, 主机在发送连接建立请求报文时, 同时携带了序号 0 (Seq=0)。在服务器对连接请求进行响应时, 一方面对主机的起始序号进行了确认 (ACK=1), 另一方面也发送了自己的起始序号 0 (Seq=0)。最后, 主机在确认中携带了对服务器的起始序号 0 的确认 (ACK=1)。

此外, 为了达到最佳传输性能, TCP 在建立连接时还需要协商双方可接受的最大报文长度 (MSS) 及窗口缩放因子 (WS) 等。

②传输过程:

a) 正常情况下:

245	17.436075	192.168.1.110	202.117.1.13	HTTP	475 GET /img/logo_pic99.png HTTP/1.1
251	17.442133	202.117.1.13	192.168.1.110	TCP	1494 80 → 62659 [ACK] Seq=22899 Ack=2069 Win=19968 Len=1440 [TCP segment of a reassembled PDU]
252	17.442133	202.117.1.13	192.168.1.110	TCP	1494 80 → 62659 [ACK] Seq=24339 Ack=2069 Win=19968 Len=1440 [TCP segment of a reassembled PDU]
253	17.442133	202.117.1.13	192.168.1.110	TCP	1494 80 → 62659 [ACK] Seq=25779 Ack=2069 Win=19968 Len=1440 [TCP segment of a reassembled PDU]
254	17.442133	202.117.1.13	192.168.1.110	TCP	1494 80 → 62659 [ACK] Seq=27219 Ack=2069 Win=19968 Len=1440 [TCP segment of a reassembled PDU]
255	17.442133	202.117.1.13	192.168.1.110	TCP	1494 80 → 62659 [ACK] Seq=28659 Ack=2069 Win=19968 Len=1440 [TCP segment of a reassembled PDU]
256	17.442133	202.117.1.13	192.168.1.110	TCP	1494 80 → 62659 [ACK] Seq=30099 Ack=2069 Win=19968 Len=1440 [TCP segment of a reassembled PDU]
257	17.442133	202.117.1.13	192.168.1.110	TCP	1494 80 → 62659 [ACK] Seq=31539 Ack=2069 Win=19968 Len=1440 [TCP segment of a reassembled PDU]
258	17.442133	202.117.1.13	192.168.1.110	TCP	1494 80 → 62659 [ACK] Seq=32979 Ack=2069 Win=19968 Len=1440 [TCP segment of a reassembled PDU]
259	17.442133	202.117.1.13	192.168.1.110	TCP	1494 80 → 62659 [ACK] Seq=34419 Ack=2069 Win=19968 Len=1440 [TCP segment of a reassembled PDU]
260	17.442133	202.117.1.13	192.168.1.110	TCP	1494 80 → 62659 [ACK] Seq=35859 Ack=2069 Win=19968 Len=1440 [TCP segment of a reassembled PDU]
261	17.442133	202.117.1.13	192.168.1.110	HTTP	323 HTTP/1.1 200 OK (PNG)
272	17.442474	192.168.1.110	202.117.1.13	TCP	54 62659 → 80 [ACK] Seq=2069 Ack=37568 Win=132352 Len=0

当服务器收到主机发送的 HTTP 请求报文 (如上图中请求 png 图片) 后, 便将完整的图片数据分为几个 TCP 报文传送给主机, 并在最后发送一个 HTTP 响应报文表示一个对象的传输完成。主机在收到服务器发来的报文后, 向服务器发送一个确认报文表示成功收到数据。

b) 发生丢包、乱序等情况时:

818	17.514840	192.168.1.110	202.117.1.13	TCP	66 [TCP Dup ACK 73987] 62659 → 80 [ACK] Seq=2888 Ack=113745 Win=132352 Len=0 SLE=120945 SRE=131025
819	17.514862	192.168.1.110	202.117.1.13	TCP	66 [TCP Dup ACK 73988] 62659 → 80 [ACK] Seq=2888 Ack=113745 Win=132352 Len=0 SLE=120945 SRE=132465
820	17.515779	202.117.1.13	192.168.1.110	TCP	1494 80 → 62659 [ACK] Seq=132465 Ack=2888 Win=22144 Len=1440 [TCP segment of a reassembled PDU]
832	17.515858	192.168.1.110	202.117.1.13	TCP	66 [TCP Dup ACK 73989] 62659 → 80 [ACK] Seq=2888 Ack=113745 Win=132352 Len=0 SLE=120945 SRE=133905
916	17.524311	202.117.1.13	192.168.1.110	TCP	1494 [TCP Fast Retransmission] 80 → 62659 [ACK] Seq=113745 Ack=2888 Win=22144 Len=1440 [TCP segment of a reassembled PDU]
917	17.524311	202.117.1.13	192.168.1.110	TCP	1494 [TCP Retransmission] 80 → 62659 [ACK] Seq=115185 Ack=2888 Win=22144 Len=1440
918	17.524311	202.117.1.13	192.168.1.110	TCP	1494 [TCP Retransmission] 80 → 62659 [ACK] Seq=116625 Ack=2888 Win=22144 Len=1440
919	17.524311	202.117.1.13	192.168.1.110	TCP	1494 [TCP Retransmission] 80 → 62659 [ACK] Seq=118065 Ack=2888 Win=22144 Len=1440
920	17.524311	202.117.1.13	192.168.1.110	TCP	1494 [TCP Retransmission] 80 → 62659 [ACK] Seq=119505 Ack=2888 Win=22144 Len=1440


```
Hypertext Transfer Protocol
v HTTP/1.1 200 OK\r\n
  > [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
    Response Version: HTTP/1.1
    Status Code: 200
    [Status Code Description: OK]
    Response Phrase: OK
  Date: Tue, 07 Mar 2023 15:08:40 GMT\r\n
  Server: *****\r\n
  X-Frame-Options: SAMEORIGIN\r\n
  X-XSS-Protection: 1; mode=block\r\n
  X-Content-Type-Options: nosniff\r\n
  Referer-Policy: no-referer-when-downgrade\r\n
  X-Download-Options: noopen\r\n
  X-Permitted-Cross-Domain-Policies: master-only\r\n
  [truncated]Content-Security-Policy: default-src 'self' data: blob: *.conac.cn *.gov.cn *.jiathis.com *.baidu.com *.bshare.cn *.eol.cn *.qq.com *.kz
  Last-Modified: Tue, 07 Mar 2023 07:48:15 GMT\r\n
  Accept-Ranges: bytes\r\n
  Cache-Control: max-age=600\r\n
  Expires: Tue, 07 Mar 2023 15:18:40 GMT\r\n
  Vary: Accept-Encoding\r\n
  Content-Encoding: gzip\r\n
  ETag: "e54e-5f64aa2544dc0-gzip"\r\n

  > Content-Length: 13088\r\n
  Keep-Alive: timeout=5, max=100\r\n
  Connection: Keep-Alive\r\n
  Content-Type: text/html\r\n
  Content-Language: zh-CN\r\n
  \r\n
  [HTTP response 1/10]
  [Time since request: 0.006076000 seconds]
  [Request in frame: 121]
  [Next request in frame: 144]
  [Next response in frame: 168]
  [Request URI: http://www.xjtu.edu.cn/]
  Content-encoded entity body (gzip): 13088 bytes -> 58702 bytes
  File Data: 58702 bytes
  > Line-based text data: text/html (1005 lines)
  [community ID: 1:w0TndXpnklwzK0q7AxQlcPIg3SE=]
```

上图中的 HTTP 响应报文回复的状态码为 200（状态语句 OK），属于处理成功响应类，表示动作被成功接收、理解和接受。响应报文除了给出头部字段的值外，在报文的主体部分还给出了请求的 Web 页面源码。

（六）UDP 协议

UDP（User Datagram Protocol，用户数据报协议）是一个简单的面向消息的传输层协议，尽管 UDP 提供标头和有效负载的完整性验证（通过校验和），但它不保证向上层协议提供消息传递，并且在发送后不会保留 UDP 消息的状态。因此，UDP 有时被称为不可靠的数据报协议。如果需要传输可靠性，则必须在用户应用程序中实现。

3152	18.641348	192.168.1.112	192.168.1.110	UDP	1270 3702 → 49690 Len=1228
3173	18.794383	192.168.1.112	192.168.1.110	UDP	1270 3702 → 49690 Len=1228
3192	19.032850	192.168.1.111	192.168.1.110	UDP	1274 3702 → 49690 Len=1232
3205	19.104902	192.168.1.112	192.168.1.110	UDP	1270 3702 → 49690 Len=1228
3208	19.258884	192.168.1.110	239.255.255.250	UDP	666 49690 → 3702 Len=624
3209	19.280212	192.168.1.102	192.168.1.110	UDP	1271 3702 → 49690 Len=1229

本次实验截获的 UDP 报文如上图所示。除此之外，还有一些报文（如：DNS、NBNS、MDNS、SSDP 等）也是通过 UDP 协议进行传输的。

（七）其它协议

①MDNS 协议：多播 DNS（Multicast DNS），MDNS 主要实现了在没有传统 DNS 服务器的情况下使局域网内的主机实现相互发现和通信，使用的端口为 5353，遵从 DNS 协议，使用现有的 DNS 信息结构、语法和资源记录类型，并且没有指定新的操作代码或响应代码。

3	0.932189	169.254.106.234	224.0.0.251	MDNS	82 Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
4	0.933642	169.254.106.234	224.0.0.251	MDNS	82 Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question

②IGMP 协议：互联网组管理协议（Internet Group Management Protocol），是 TCP/IP 协议族中负责 IPV4 组播成员管理的协议，其主要功能是在接收者主机

和直接相邻的组播路由器之间建立和维护组播组成员的关系。

6	1.506652	169.254.106.234	224.0.0.2	IGMPv2	46 Leave Group 239.255.255.250
7	1.508443	169.254.106.234	239.255.255.250	IGMPv2	46 Membership Report group 239.255.255.250
8	1.521647	169.254.106.234	224.0.0.252	IGMPv2	46 Membership Report group 224.0.0.252
9	1.521896	169.254.106.234	224.0.0.2	IGMPv2	46 Leave Group 224.0.0.252
10	1.522208	169.254.106.234	224.0.0.252	IGMPv2	46 Membership Report group 224.0.0.252

③SSDP 协议：简单服务发现协议（Simple Service Discovery Protocol）是一种应用层协议，提供了在局部网络里面发现设备的机制。

235	17.408018	192.168.1.110	239.255.255.250	SSDP	143 M-SEARCH * HTTP/1.1
236	17.412374	192.168.1.102	239.255.255.250	SSDP	217 M-SEARCH * HTTP/1.1

④TLS 协议：安全传输层协议（Transport Layer Security），用于在两个通信应用程序之间提供保密性和数据完整性。

3009	18.057021	192.168.1.110	20.44.10.123	TLSv1.2	92 Application Data
3010	18.059311	20.44.10.123	192.168.1.110	TLSv1.2	134 Application Data, Application Data
3011	18.071266	20.44.10.123	192.168.1.110	TLSv1.2	342 Application Data

⑤NBNS 协议：网络基本输入/输出系统（NetBIOS）名称服务器（NBNS）协议是 TCP/IP 上的 NetBIOS（NetBT）协议族的一部分，它在基于 NetBIOS 名称访问的网络上提供主机名和地址映射方法。

3145	18.567797	192.168.1.110	192.168.1.255	NBNS	110 Registration NB LAPTOP-ROMI2L28<20>
3146	18.583542	192.168.1.110	192.168.1.255	NBNS	110 Registration NB LAPTOP-ROMI2L28<00>

（八）总结

通过本次 Wireshark 抓包实验，我了解了主机从配置 IP 地址等网络参数到访问一个网站所经历的具体过程和涉及的相关网络协议，对计算机网络原理有了更进一步的理解。