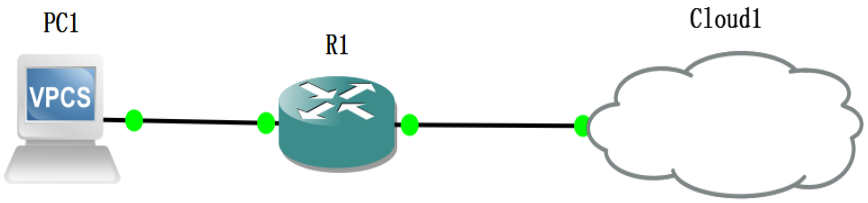
北 京 邮 电 大 学
计 算 机 科 学 与 技 术 学 院

《下一代 Internet 技术与协议》
实验报告

姓名：陈朴炎
学号：2021211138
班级：2021211307

2024 年 6 月

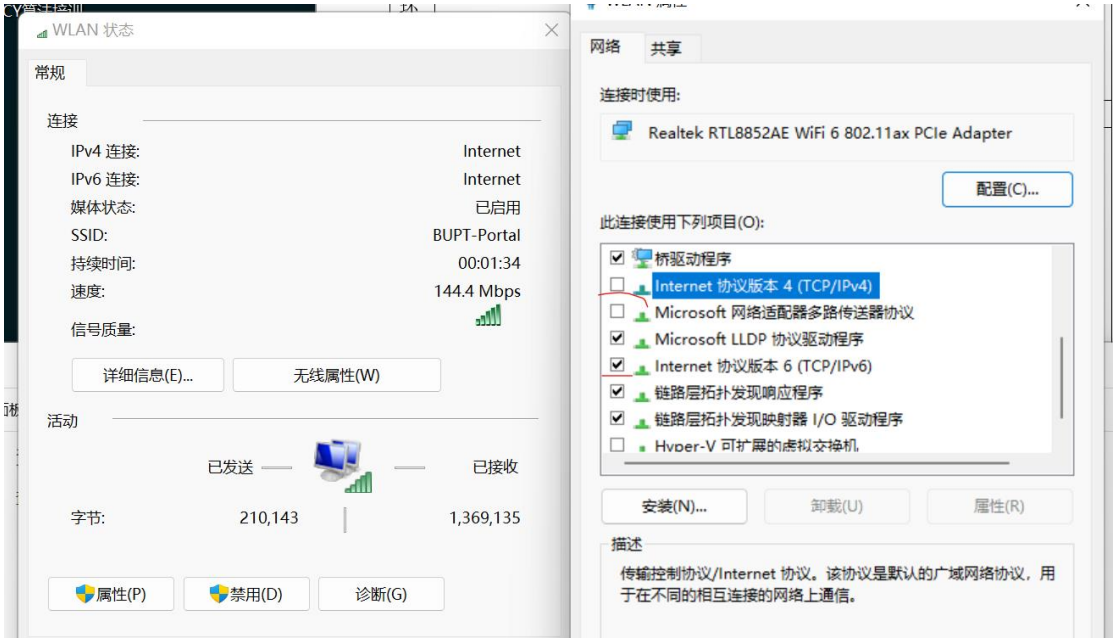
实验报告

实验名称	ICMPv6 实验		
实验目的	学会理解分析 ICMPv6 的报文		
实验完成人	陈朴炎	完成时间	2024.6.3
实验环境			

实验步骤与结果分析

1. 实验步骤以及 cmd 命令结果分析

连接手机热点，笔记本电脑的 IPv6 协议，关闭 IPv4 协议，如下：



在命令行上敲入：ipconfig -all，得到如下信息

```
无线局域网适配器 WLAN:

   连接特定的 DNS 后缀 . . . . . :
   描述. . . . . . . . . . . . . . : Realtek RTL8852AE WiFi 6 802.11ax PCIe Adapter
   物理地址. . . . . . . . . . . . : 74-4C-A1-B2-CD-3F
   DHCP 已启用 . . . . . . . . . . : 是
   自动配置已启用. . . . . . . . . : 是
   IPv6 地址 . . . . . . . . . . . : 2408:8409:1900:936b:c1ba:9a09:a4b9:2154(首选)
   临时 IPv6 地址. . . . . . . . . : 2408:8409:1900:936b:eca8:c4d6:c189:df(首选)
   本地链接 IPv6 地址. . . . . . . : fe80::8d07:9caf:314b:9530%3(首选)
   默认网关. . . . . . . . . . . . : fe80::5031:4ff:fe31:1047%3
   DHCPv6 IAID . . . . . . . . . . : 57953441
   DHCPv6 客户端 DUID  . . . . . . : 00-01-00-01-29-67-34-9C-74-4C-A1-B2-CD-3F
   DNS 服务器  . . . . . . . . . . : 2408:8409:1900:936b::51
   TCPIP 上的 NetBIOS  . . . . . . : 已禁用
```

我们一起分析一下这些地址。首先是 IPv6 地址：2408:8409:1900:936b:c1ba:9a09:a4b9:2154，根据地址首部 2408 可以得知，这是一个全球单播 IPv6 地址。这意味着它可以用于在全球范围内唯一标识一个设备，并进行网络通信。而临时 IPv6 地址为 2408:8409:1900:936b:eca8:c4d6:c189:df，它是隐私地址，会定期更换，主要用于外出通信时保护隐私，避免被跟踪。而链路本地地址为 fe80::8d07:9caf:314b:9530%3，这个地址主要用于路由器或者同网络内的其余用户通信。而默认网关 fe80::5031:4ff:fe31:1047%3，则为路由器的地址。

在 cmd 命令下，使用 nslookup 命令对 www.bupt.edu.cn 进行 DNS 解析，如下：

```
PS C:\Users\20531> nslookup www.bupt.edu.cn
服务器:  UnKnown
Address:  2408:8409:1900:936b::51

非权威应答:
名称:    vn46.bupt.edu.cn
Addresses:  2001:da8:215:4038::161
          211.68.69.240
Aliases:  www.bupt.edu.cn
```

可以看到，这个回应是从我们的本地 DNS 服务器传来的，它告诉我们这个网站的真实名称为 vn46.bupt.edu.cn，并且传来了这个网站的 IPv6 地址和 IPv4 地址。

No.	Time	Source	Destination	Protocol	Length	In
1	0.000000	2408:8409:1900:936b…	2404:6800:4008:c1b:…	TCP	75	1
2	0.431042	2404:6800:4008:c1b:…	2408:8409:1900:936b…	TCP	86	4
3	10.595892	2408:8409:1900:936b…	2408:8409:1900:936b…	DNS	152	S
4	10.815073	2408:8409:1900:936b…	2408:8409:1900:936b…	DNS	206	S
5	10.817422	2408:8409:1900:936b…	2408:8409:1900:936b…	DNS	95	S
6	10.835862	2408:8409:1900:936b…	2408:8409:1900:936b…	DNS	130	S
7	10.838242	2408:8409:1900:936b…	2408:8409:1900:936b…	DNS	95	S
8	10.864166	2408:8409:1900:936b…	2408:8409:1900:936b…	DNS	142	S
9	15.531200	2408:8409:1900:936b…	2408:8409:1900:936b…	ICMPv6	86	N

对北邮官网的 ipv6 地址进行 ping 操作，并截图记录：

```
PS C:\Users\20531> ping 2001:da8:215:4038::161

正在 Ping 2001:da8:215:4038::161 具有 32 字节的数据:
来自 2001:da8:215:4038::161 的回复: 时间=296ms
来自 2001:da8:215:4038::161 的回复: 时间=65ms
来自 2001:da8:215:4038::161 的回复: 时间=259ms
来自 2001:da8:215:4038::161 的回复: 时间=106ms

2001:da8:215:4038::161 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 65ms, 最长 = 296ms, 平均 = 181ms
```

128	151.811566	2408:8409:1900:936b…	2001:da8:215:4038::…	ICMPv6	94 Echo (pin
129	152.107611	2001:da8:215:4038::…	2408:8409:1900:936b…	ICMPv6	94 Echo (pin
130	152.824912	2408:8409:1900:936b…	2001:da8:215:4038::…	ICMPv6	94 Echo (pin
131	152.890547	2001:da8:215:4038::…	2408:8409:1900:936b…	ICMPv6	94 Echo (pin
132	153.827795	2408:8409:1900:936b…	2001:da8:215:4038::…	ICMPv6	94 Echo (pin
133	154.087297	2001:da8:215:4038::…	2408:8409:1900:936b…	ICMPv6	94 Echo (pin
134	154.841433	2408:8409:1900:936b…	2001:da8:215:4038::…	ICMPv6	94 Echo (pin
135	154.948314	2001:da8:215:4038::…	2408:8409:1900:936b…	ICMPv6	94 Echo (pin
136	156.564561	2408:8409:1900:936b…	2603:1040:5:8::2	TCP	75 [TCP Keep
137	156.771665	2603:1040:5:8::2	2408:8409:1900:936b…	TCP	86 [TCP Keep

然后对北邮官网的 IPv6 地址进行 tracert 操作，加上参数-d，截图记录；

```
    最短 = 65ms，最长 = 296ms，平均 = 181ms
PS C:\Users\20531> tracert -d 2001:da8:215:4038::161

通过最多 30 个跃点跟踪到 2001:da8:215:4038::161 的路由

  1     3 ms     3 ms     3 ms  2408:8409:1900:936b::51
  2     *        *        *     请求超时。
  3     *        *        *     请求超时。
  4    91 ms     *       70 ms  2408:8140:3fff:f803:103:f006:0:1009
  5    43 ms    17 ms    19 ms  2408:8140:3fff:f803:103:f006:0:1018
  6     *        *        *     请求超时。
  7     *        *        *     请求超时。
  8    62 ms    55 ms    19 ms  2408:8000:3::3ef
  9    13 ms    16 ms    14 ms  2001:da8:257:751::1
 10    78 ms    20 ms    11 ms  2001:da8:257:0:6100:64:1:62
 11    77 ms    18 ms    13 ms  2001:da8:2:5::2
 12    72 ms    28 ms    20 ms  2001:da8:2:123::2
 13    37 ms    20 ms    15 ms  2001:da8:215::2
 14    41 ms    21 ms    24 ms  2001:da8:215:0:10:0:3:2
 15    67 ms    14 ms    14 ms  2001:da8:215:0:10:0:4:3a
 16    56 ms    20 ms    17 ms  2001:da8:215:5030:3::2
 17    97 ms    23 ms    21 ms  2001:da8:215:4038::161

跟踪完成。
```

ipv6

No.
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375

tracert 命令用于追踪从源设备到目标地址之间的路由路径，显示每个跃点（即通过的路由器或其他网络设备）的延迟。从上图可以看出，一共经过了 17 个跃点，我们成功到达了目标地址。

第一个跃点，这是从源设备到第一个路由器的跃点，这个响应是最快的。第 2、3 这两个跃点没有响应，表示请求超时，这可能是路由器配置禁止 ICMP 回应或者网络防火墙阻止。第 3 到第 4 跃点，延迟时间是 91ms 和 70ms，延迟较高，可能是因为网络较为阻塞。在第 8 个跃点之后，设备逐渐接近目标地址。每个跃点的延迟相对较低，表明网络路径在这些节点之间是相对稳定和快速的。

我们从这 17 个跃点信息里，可以得到从源设备到目标 IPv6 地址 2001:da8:215:4038::161 的路径 tracert 过程。

224	280.603235	2408:8409:1900:936b…	fe80::5031:4ff:fe31…	ICMPv6	86
225	286.132278	2408:8409:1900:936b…	2001:da8:215:4038::…	ICMPv6	126
226	286.136108	2408:8409:1900:936b…	2408:8409:1900:936b…	ICMPv6	174
227	286.136466	2408:8409:1900:936b…	2001:da8:215:4038::…	ICMPv6	126
228	286.139732	2408:8409:1900:936b…	2408:8409:1900:936b…	ICMPv6	174
229	286.140027	2408:8409:1900:936b…	2001:da8:215:4038::…	ICMPv6	126
230	286.143034	2408:8409:1900:936b…	2408:8409:1900:936b…	ICMPv6	174
231	287.141963	2408:8409:1900:936b…	2001:da8:215:4038::…	ICMPv6	126
232	287.582168	2408:8409:1900:936b…	2408:8409:1900:936b…	DNS	112
233	287.582283	2408:8409:1900:936b…	2408:8409:1900:936b…	DNS	112
234	287.690742	2408:8409:1900:936b…	2408:8409:1900:936b…	DNS	112
235	287.690742	2408:8409:1900:936b…	2408:8409:1900:936b…	DNS	112
236	287.722585	2408:8409:1900:936b…	2408:8409:1900:936b…	DNS	222
237	287.722585	2408:8409:1900:936b…	2408:8409:1900:936b…	DNS	235
238	287.723354	2408:8409:1900:936b…	2408:8409:1900:936b…	DNS	125
239	287.723422	2408:8409:1900:936b…	2408:8409:1900:936b…	DNS	125

最后对此网站的 IPv6 进行 ping 操作，加上-l 3000，记录：

```
跟踪完成。
PS C:\Users\20531> ping -l 3000 2001:da8:215:4038::161

正在 Ping 2001:da8:215:4038::161 具有 3000 字节的数据:
来自 2001:da8:215:4038::161 的回复: 时间=174ms
来自 2001:da8:215:4038::161 的回复: 时间=239ms
来自 2001:da8:215:4038::161 的回复: 时间=221ms
来自 2001:da8:215:4038::161 的回复: 时间=138ms

2001:da8:215:4038::161 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 138ms, 最长 = 239ms, 平均 = 193ms
```

加上-l 3000 表示每个 ping 请求的数据包大小为 3000 字节，可以用来检测网络在处理大数据包时的性能。每个请求的响应时间分别为 174ms、239ms、221ms 和 138ms。数据包发送了 4 个，全部接收，没有丢失，说明网络连接稳定，没有丢包现象。

538	427.331396	2001:da8:215:4038::…	2408:8409:1900:936b…	ICMPv6	174
539	427.406759	2408:8409:1900:936b…	2603:1040:5:8::1	TCP	75
540	427.527542	2603:1040:5:8::1	2408:8409:1900:936b…	TCP	86
541	427.737038	2408:8409:1900:936b…	2603:1040:5:8::2	TCP	75
542	427.901155	2603:1040:5:8::2	2408:8409:1900:936b…	TCP	86
543	428.124469	2408:8409:1900:936b…	2001:da8:215:4038::…	IPv6	1414
544	428.124469	2408:8409:1900:936b…	2001:da8:215:4038::…	IPv6	1414
545	428.124469	2408:8409:1900:936b…	2001:da8:215:4038::…	ICMPv6	366
546	428.262752	2001:da8:215:4038::…	2408:8409:1900:936b…	IPv6	1510
547	428.262752	2001:da8:215:4038::…	2408:8409:1900:936b…	IPv6	1510
548	428.262752	2001:da8:215:4038::…	2408:8409:1900:936b…	ICMPv6	174
549	432.153862	fe80::5031:4ff:fe31…	fe80::8d07:9caf:314…	ICMPv6	86

查看本机各个接口的链路 MTU:netsh interface ipv6 show subinterfaces

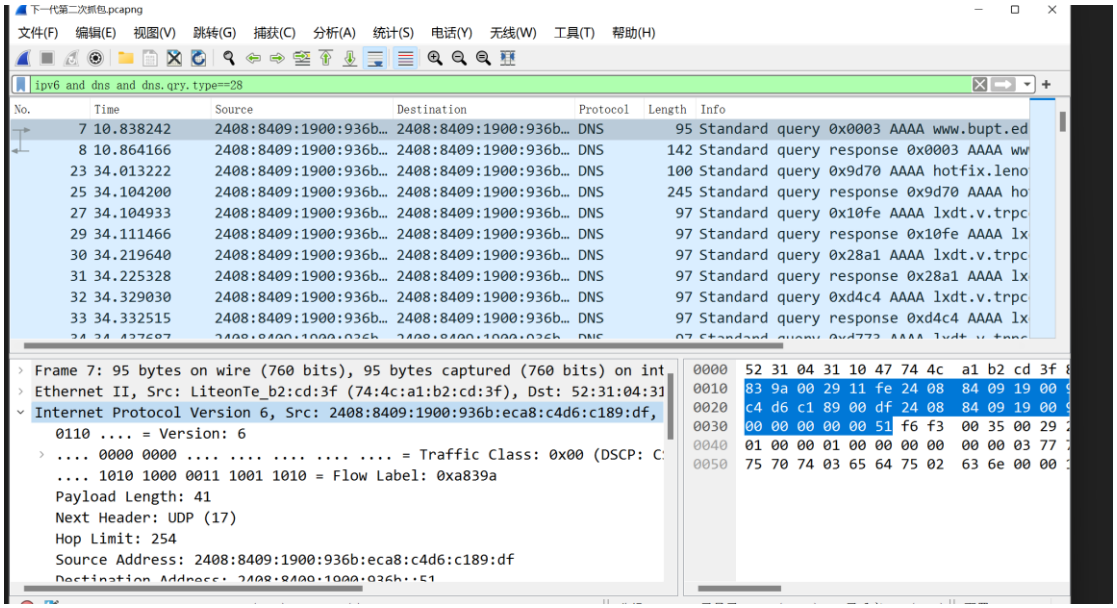
```
PS C:\Users\20531> netsh interface ipv6 show subinterfaces

       MTU  MediaSenseState      输入字节      输出字节  接口
----------  ---------------  ------------  ------------  -------------
4294967295                1             0         26519  Loopback Pseudo-Interface 1
      1500                5             0           152  本地连接
      1400                1      17588007       1001719  WLAN
      1500                5             0           152  蓝牙网络连接
      1500                5             0           152  本地连接* 8
      1500                5             0           152  本地连接* 12
      1500                1             0         38700  VMware Network Adapter VMnet1
      1500                1             0         38252  VMware Network Adapter VMnet8
```

可以看到，WLAN 接口的 MTU 为 1400。

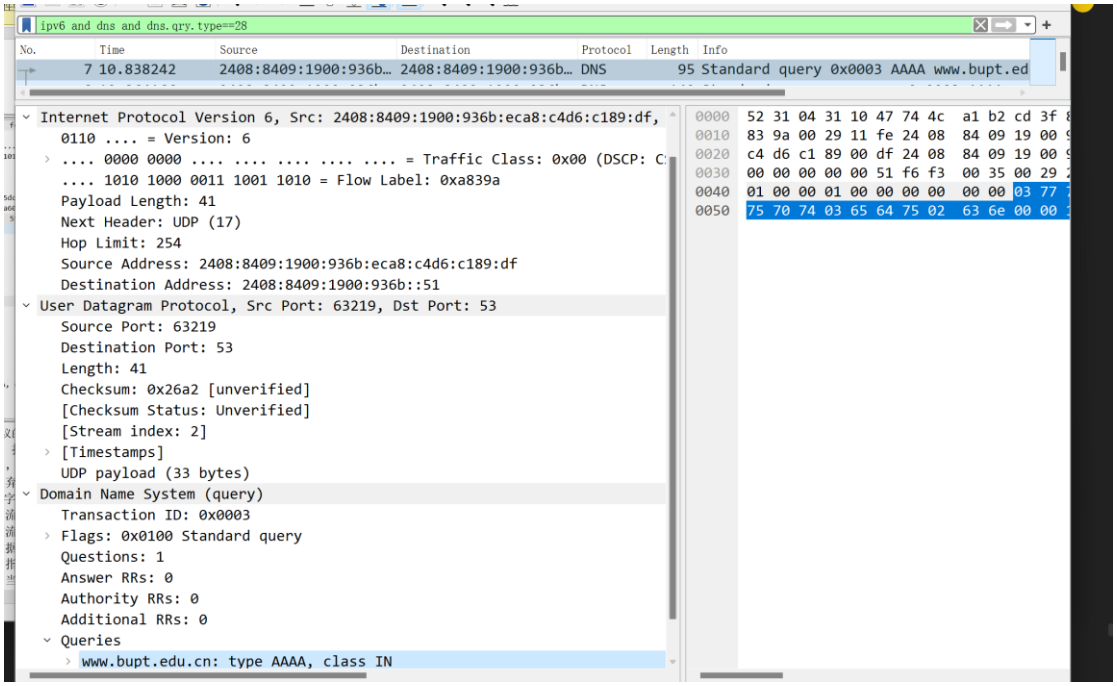
2. wireshark 抓包分析

2.1 nslookup 包

在过滤器中输入 ipv6 and dns and dns.qry.type==28，查看 nslookup 的包，如下。



具体信息如下所示：



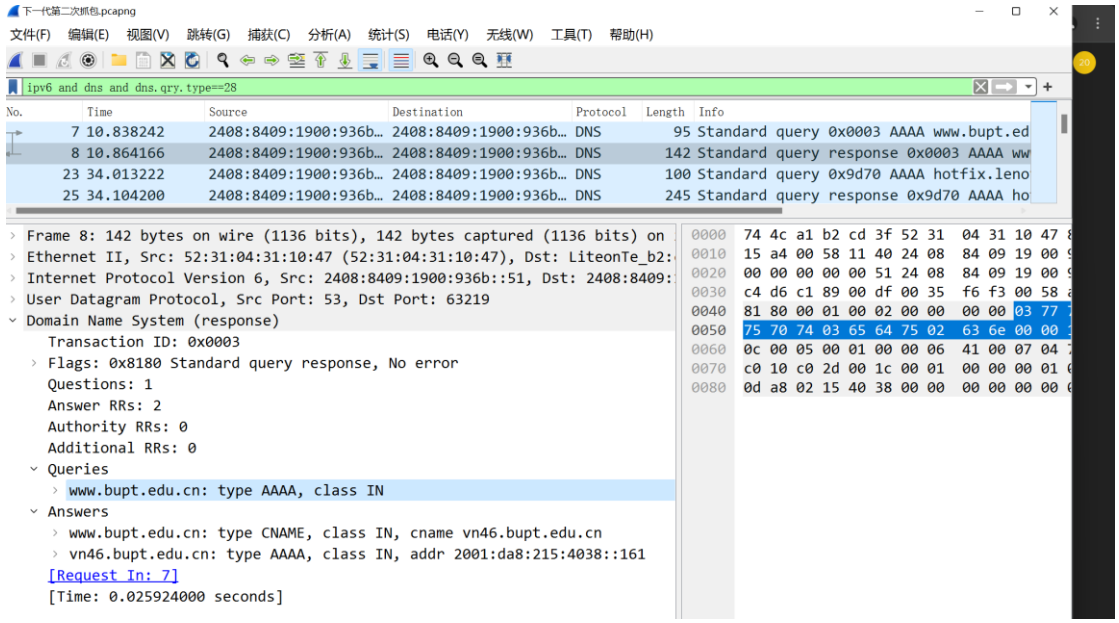
我们从 IPv6 层、UDP 层和 DNS 层分别分析：

IPv6 层：
版本：6（IPv6）
流量类别：0x00（默认服务类别）
流标签：0xa839a
有效载荷长度：41 字节
下一个头部：17（UDP）
跳限制：254
源地址：2408:8409:1900:936b:eca8:c4d6:c189:df
目的地址：2408:8409:1900:936b::51

UDP 层：
源端口：63219
目的端口：53
长度：41 字节
校验和：0x26a2（未验证）
数据流索引：2
时间戳：有

DNS 层：
事务 ID：0x0003
标志：0x0100（标准查询）
问题数：1
回答数：0
授权资源记录数：0
附加资源记录数：0

这个包的回复包信息如下：



事务 ID：0x0003。这个事务 ID 用于匹配请求和响应。

标志：0x8180。0x8180 表示这是一个标准查询响应，没有错误。

问题数：1，表示在请求中有一个查询问题。

回答数：2，表示响应中有两个回答资源记录（RR）。

授权资源记录数：0，表示没有授权资源记录。

附加资源记录数：0，表示没有附加资源记录。

查询部分，查询域名：www.bupt.edu.cn

类型：AAAA，类：IN（Internet）

回答部分

第一个回答资源记录：

域名：www.bupt.edu.cn

类型：CNAME（Canonical Name）

类：IN（Internet）

别名：vn46.bupt.edu.cn

第二个回答资源记录：

域名：vn46.bupt.edu.cn

类型：AAAA（IPv6 地址）

类：IN（Internet）

地址：2001:da8:215:4038::161

其他信息

请求 ID：7

表示该响应对应请求包中的第 7 帧。

响应时间：0.025924000 秒

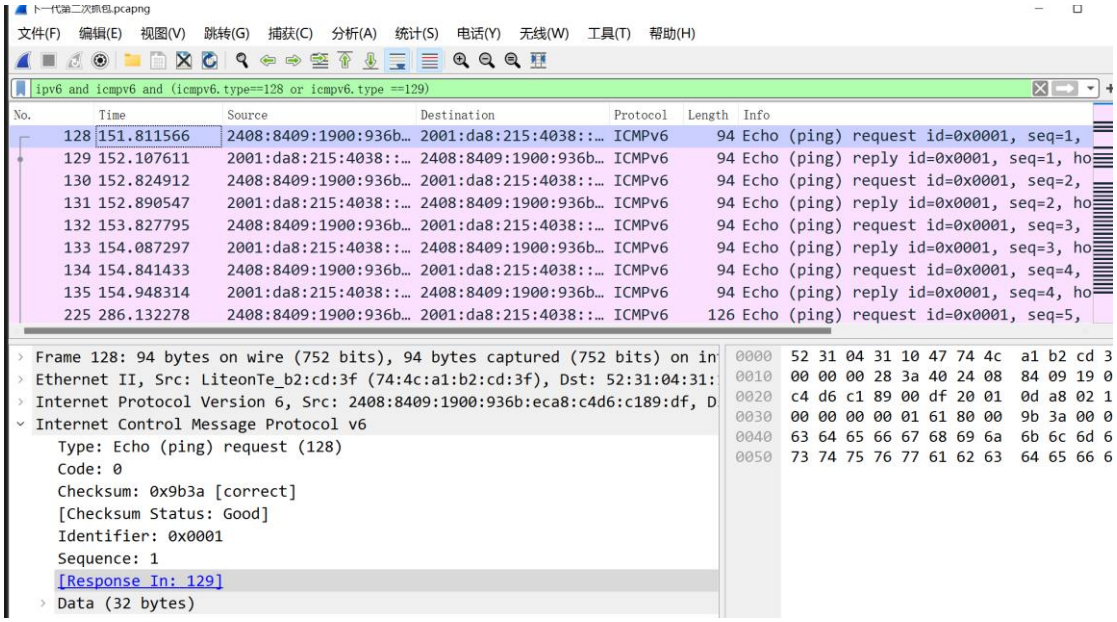
表示从发送请求到收到响应所用的时间。

2.2 ping

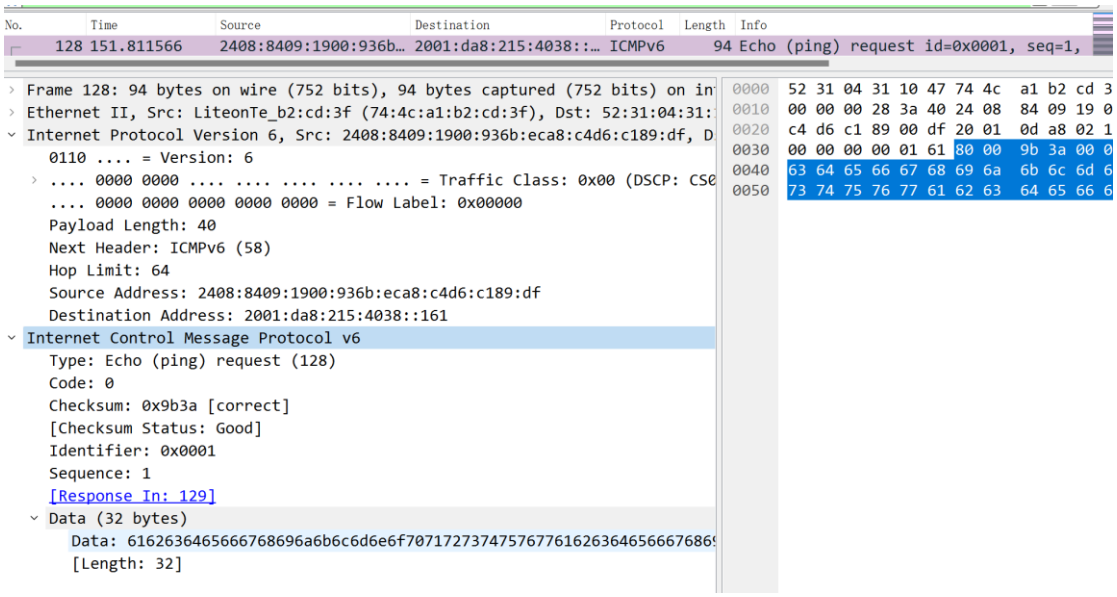
我们在过滤器中输入：

ipv6 and icmpv6 and (icmpv6.type==128 or icmpv6.type ==129)

就可以过滤出 ping 的请求包和 ping 的回应包。其中，ping 的请求包 icmpv6 的类型为 128，而回应包的 icmpv6 的类型为 129。如下：



我们抓出 No.128 和 No.129 这一对请求-回应报文进行分析。



ICMPv6 层

Type: 128，表示这是一个 Echo Request（ping 请求）报文。

Code: 0，表示没有子类型。

Checksum: 报文的校验和，用于错误检测，这里是 0x9b3a，校验正确。

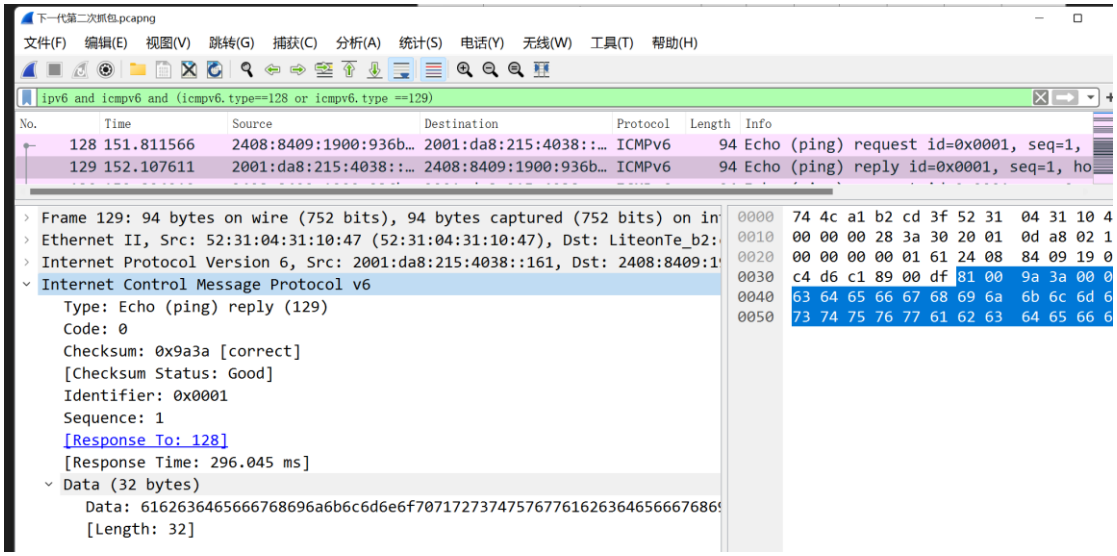
Identifier: 标识符，用于匹配请求和回复，这里是 0x0001。

Sequence: 序列号，用于匹配请求和回复，这里是 1。

Response In: 129，表示响应的帧号。

Data: 报文携带的数据部分，这里是 32 字节。

No.129 报文信息如下：



Type 是 129，表示这是一个 ICMPv6 Echo Reply（ping 回复）报文。

Code 是 0，表示没有子类型。

此处的校验和值为 0x9a3a，表示校验正确。

Identifier 是 0x0001，与对应的请求相匹配。

Sequence 是 1，也与对应的请求相匹配。

指示此回复是响应于哪个类型的请求，这里是 128，表示响应于 Echo (ping) request。

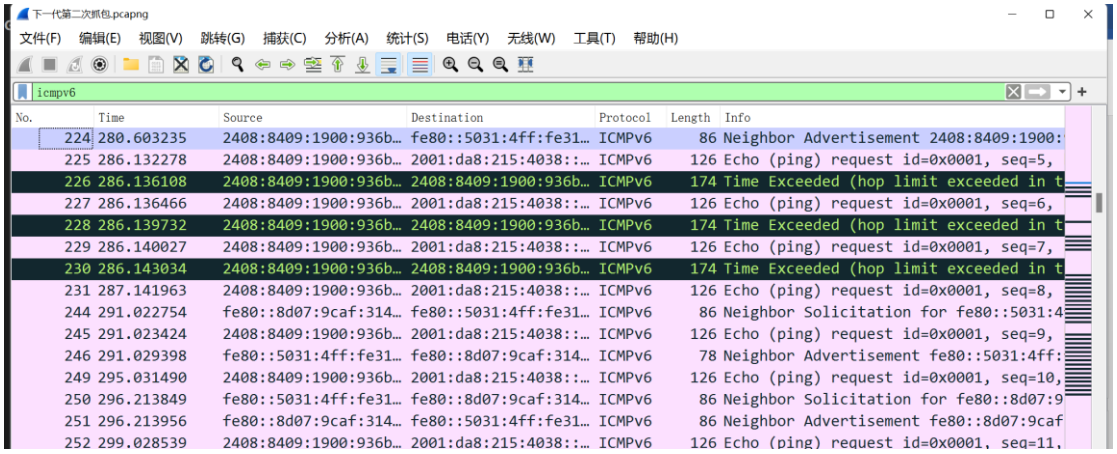
响应时间，表示从发送 Echo Request 到接收 Echo Reply 的时间，这里是 296.045 毫秒。

数据字段，携带了一串十六进制编码的数据，长度为 32 字节。

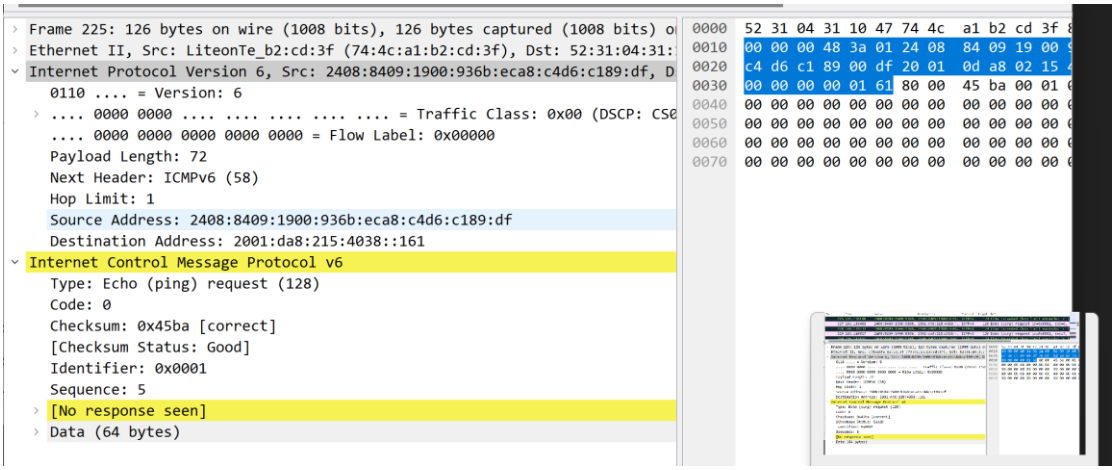
这个 ICMPv6 Echo Reply 报文是对之前发送的 ICMPv6 Echo Request 报文的响应。它表示目标主机已收到了请求并且成功地进行了响应。响应时间给出了往返时间的一个部分，指示了从发送请求到接收响应的时间。

2.3 tracert

下面这些报文是我在 tracert 命令时收到的报文



我们来看一下 No.225 这个包：



源地址：2408:8409:1900:936b:eca8:c4d6:c189

目的地址：2001:da8:215:4038::161

版本：6

流量类：0x00 (DSCP: CS0, ECN: Not-ECT)

流标签：0x00000

负载长度：72

下一头部：ICMPv6 (58)

跳限：1

ICMPv6

类型：Echo (ping) request (128)

代码：0

校验和：0x45ba (正确)

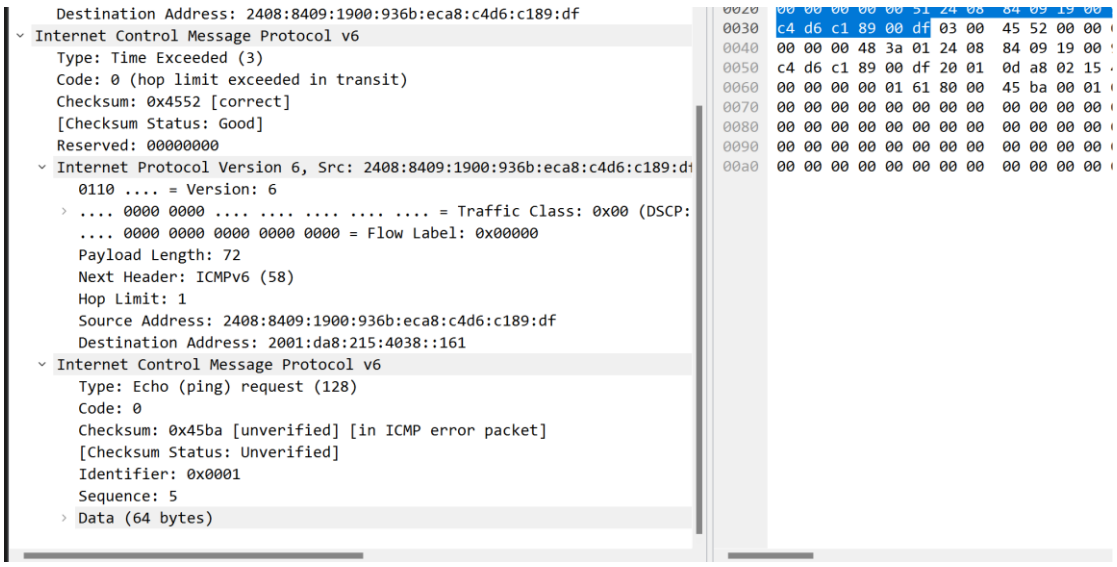
标识符：0x0001

序列号：5

数据（64 字节）

由于 Hop Limit 设置为 1，这通常意味着这是用于路由跟踪（traceroute）的 ICMP Echo 请求包。traceroute 工具通过发送一系列的 ICMP Echo 请求包，每个包的跳限（TTL 或 Hop Limit）值逐渐增加，从 1 开始，依次递增。每个中间路由器在转发包时都会减少跳限值，并在跳限值减为 0 时返回一个 ICMP "Time Exceeded" 消息。因此，这个报文符合用于 traceroute 操作的典型模式。

我们再看一下 No.226 这个出错的报文：



这个报文是一个 ICMPv6 "Time Exceeded" (时间超时) 消息，它通常出现在 traceroute 的过程中。当一个数据包的 Hop Limit (跳限制) 达到零时，路由器会丢弃该包并返回一个 "Time Exceeded" 消息给发送者。具体来说，报文信息如下：

ICMPv6 报头 (ICMPv6 Header)

类型 (Type): Time Exceeded (3) – 时间超时

代码 (Code): 0 (hop limit exceeded in transit) – 跳数限制在传输中超出

校验和 (Checksum): 0x4552 (正确)

保留字段 (Reserved): 00000000

嵌入的原始 IPv6 报头 (Embedded Original IPv6 Header)

源地址 (Source Address): 2408:8409:1900:936b:eca8:c4d6

目的地址 (Destination Address): 2001:da8:215:4038::161

版本 (Version): 6

流量类别 (Traffic Class): 0x00 (DSCP: CS0, ECN: Not-ECT)

流标签 (Flow Label): 0x00000

有效载荷长度 (Payload Length): 72 字节

下一个报头 (Next Header): ICMPv6 (58)

跳数限制 (Hop Limit): 1

嵌入的原始 ICMPv6 报头 (Embedded Original ICMPv6 Header)

类型 (Type): Echo (ping) request (128) - 回显请求 (ping)

代码 (Code): 0

校验和 (Checksum): 0x45ba (未验证) [在 ICMP 错误包中]

标识符 (Identifier): 0x0001

序列号 (Sequence): 5

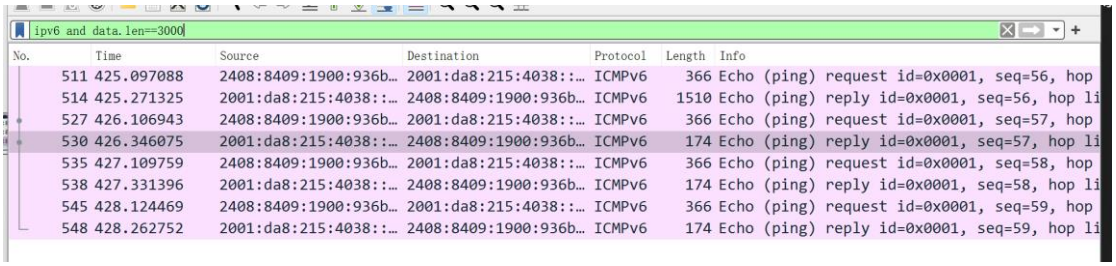
数据 (Data): 64 字节

解释：这个报文是一个 ICMPv6 "Time Exceeded" 消息，表明一个发往 2001:da8:215:4038::161 的 ICMPv6 Echo 请求 (ping) 包由于 Hop Limit 到达 0 而被

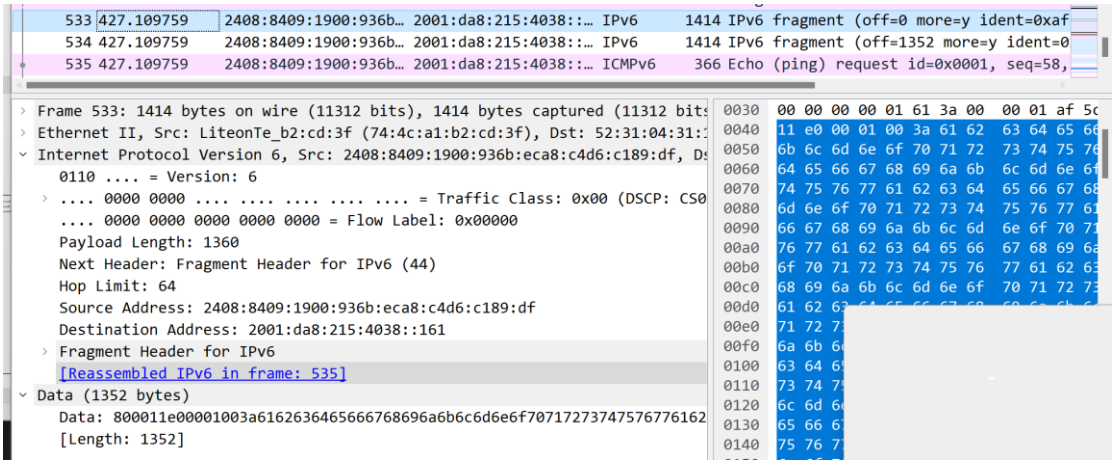
路由器丢弃。源地址 2408:8409:1900:936b:eca8:c4d6:c189:df 发送了一个 ICMPv6 Echo 请求 (ping) 包给目的地址 2001:da8:215:4038::161，Hop Limit 设置为 1。当这个包经过地址 2408:8409:1900:936b::51 的路由器时，Hop Limit 减为 0，该路由器丢弃了这个包并返回一个 ICMPv6 "Time Exceeded" 消息给发送者。这个 "Time Exceeded" 消息的源地址为 2408:8409:1900:936b::51，目的地址为 2408:8409:1900:936b:eca8:c4d6:c189:df。

2.4 ping -l

我们输入过滤条件：data.len ==3000 来查看数据字段带有 3000 个字节的 ping 包，如下所示：



将过滤条件改为 ipv6，我们查看 533 到 535 这个包



IPv6 报头 (Internet Protocol Version 6)

源 IP 地址 (Source IP Address): 2408:8409:1900:936b:eca8:c4d6:c189:df

目标 IP 地址 (Destination IP Address): 2001:da8:215:4038::161

版本 (Version): 6

流量类别 (Traffic Class): 0x00 (DSCP: CS0, ECN: Not-ECT)

流标签 (Flow Label): 0x00000

有效载荷长度 (Payload Length): 1360 字节

下一个报头 (Next Header): Fragment Header for IPv6 (44)

跳数限制 (Hop Limit): 64

IPv6 分片报头 (Fragment Header for IPv6)

下一个报头 (Next header): ICMPv6 (58)

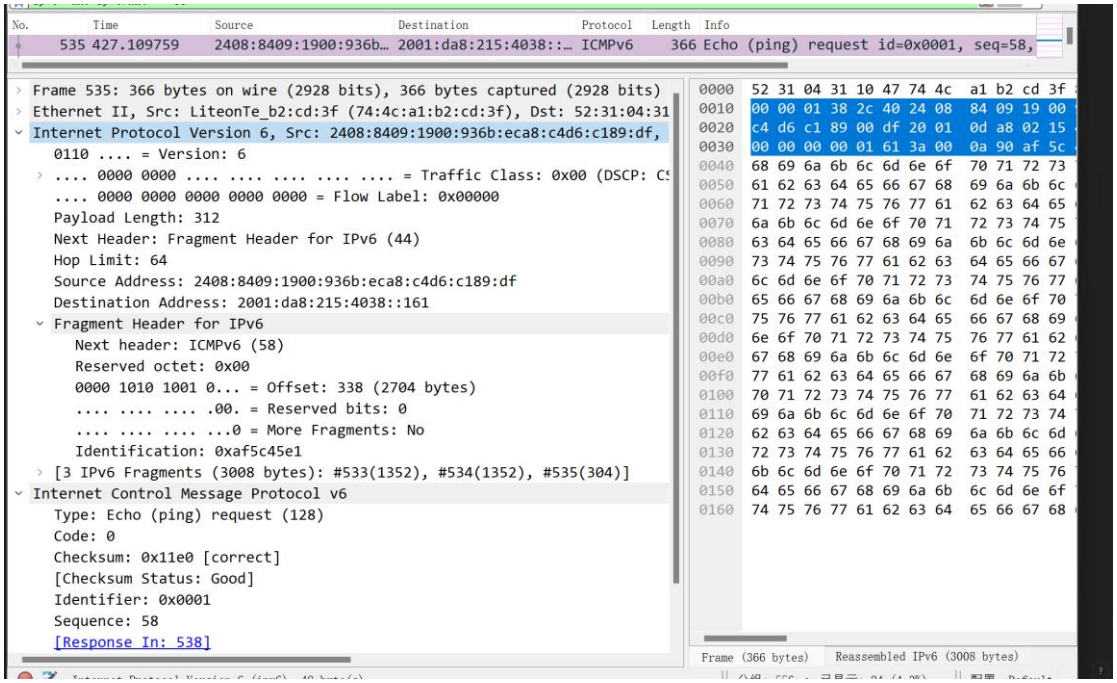
保留字节 (Reserved octet): 0x00

偏移量 (Offset): 0 (0 bytes)

更多分片 (More Fragments): 是 ，说明它后面还有其他的同一帧的报文。

标识符 (Identification): 0xaf5c45e1
数据部分 (Data)
长度 (Length): 1352 字节
该报文是一个 IPv6 分片报文，表示一个较大的 IPv6 报文被分片传输。这里的分片偏移量是 0，表示这是第一个分片。标识符 0xaf5c45e1 用于识别属于同一个原始报文的所有分片。因为“更多分片”位设置为 1，这表示还有后续的分片。

对于 535 这个报文，详细信息如下：



IPv6 分片报头 (Fragment Header for IPv6)
下一个报头 (Next header): ICMPv6 (58)
保留字节 (Reserved octet): 0x00
偏移量 (Offset): 338 (2704 字节)
更多分片 (More Fragments): 否 (No)
标识符 (Identification): 0xaf5c45e1

ICMPv6 报头 (Internet Control Message Protocol v6)
类型 (Type): Echo (ping) request (128)
代码 (Code): 0
校验和 (Checksum): 0x11e0 (正确)
标识符 (Identifier): 0x0001
序列号 (Sequence): 58

该报文是一个 IPv6 分片报文的最后一个分片，偏移量为 338，没有更多的分片。这是一个 ICMPv6 的 Echo 请求，用于进行 Ping 操作。标识符为 0x0001，序列号为 58。通过分析这个报文，可以确定它是一个 ICMPv6 Echo 请求报文，用于 Ping 操作，包含了 3000 字节的数据。

分析与思考
在本次实验中，我通过使用不同的网络命令（ping、nslookup、tracert -d、ping -l 3000）以及 Wireshark 工具进行了 ICMPv6 报文的抓包分析。通过观察和分析抓取到的报文，我对 ICMPv6 协议有了更深入的理解，并学会了如何分析和解释这些报文。通过观察和分析 ICMPv6 报文的各个字段，我了解了报文的结构和含义，包括类型、代码、校验和、标识符、序列号等重要字段的作用。 我理解了不同类型报文的作用，比如 Echo Request 、Echo Reply、Time Exceeded、Fragment Header for IPv6 等。 Echo Request 用于测试网络连接是否正常以及目标主机是否可达，发送者向目标主机发送 Echo 请求报文，目标主机收到后会返回 Echo Reply 报文，表示连接正常。；Echo Reply 用于回复 Echo 请求报文，确认目标主机的可达性目标主机收到 Echo 请求报文后，会发送 Echo Reply 报文作为回应，其中携带与请求中相同的标识符和序列号。Time Exceeded 用于指示数据包在转发过程中被丢弃，因为其生存时间超过了指定的最大跳数（TTL）。路由器在转发数据包时，如果生存时间（TTL）减至 0，则会将其丢弃并发送 Time Exceeded 报文给数据包的源主机。而 Fragment Header for IPv6 用于在 IPv6 报文中进行分片，将过大的报文分割成多个较小的报文传输。当 IPv6 报文超过链路最大传输单元（MTU）时，源主机会将报文分片，并在每个分片中添加 Fragment Header，以便目标主机重组原始报文。