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：_____鄭毓恒_____
学号：___2020211262___
班级：___2020211302___
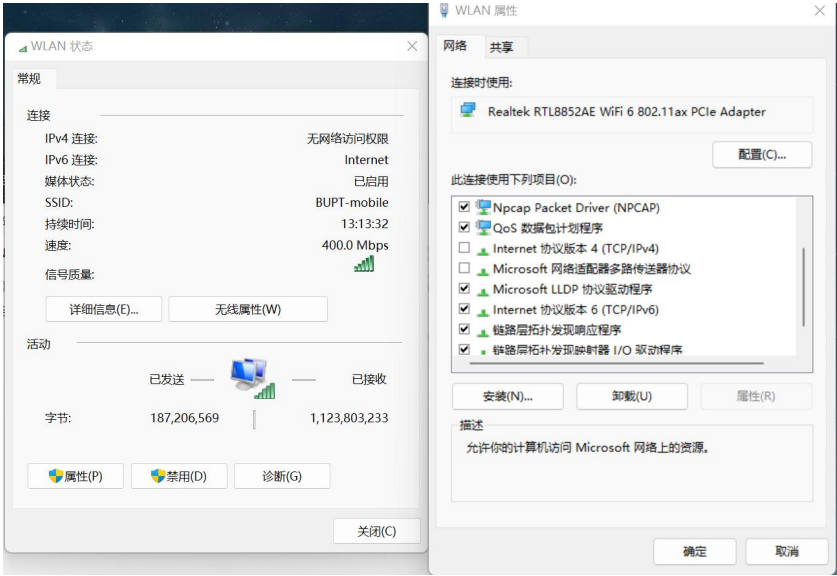
2023 年 5 月

实验报告

实验名称	ICMPv6 实验		
实验目的	通过 Wireshark 抓包，分析 ICMPv6 协议报文。		
实验完成人	郑毓恒	完成时间	2023-05-29
实 验 环 境	Windows 11 WireShark 网络分析器		

实验步骤与结果分析

连接网络，打开 IPv6 协议，关闭 IPv4 协议。

在 CMD 命令行模式下输入 ipconfig /all 命令，得到以下本机 IPv6 信息。本机的 IPv6
地址为 2001:da8:215:3c02:3049:73f2:dc55:ea00。

在 CMD 命令行模式下，使用 nslookup 命令对选定的网站域名 www.bupt.edu.cn 进行 DNS 解析，指定的 IPv6 服务器为 2400:3200::1。可以看到获取到该网站的 IPv6 地址 2001:da8:215:4038::161。

```
C:\Users\heng>nslookup www.bupt.edu.cn 2400:3200::1
服务器:  public1.alidns.com
Address:  2400:3200::1

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
```

Wireshark 抓到以下几个包。

No.	Time	Source	Destination	Protocol	Length	Info
17	3.493090	2001:da8:215:3c02:7…	2400:3200::1	DNS	152	Standard query 0x0001 PTR 1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0…
18	3.525722	2400:3200::1	2001:da8:215:3c02:7…	DNS	184	Standard query response 0x0001 PTR 1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0…
19	3.528447	2001:da8:215:3c02:7…	2400:3200::1	DNS	95	Standard query 0x0002 A www.bupt.edu.cn
20	3.560197	2400:3200::1	2001:da8:215:3c02:7…	DNS	130	Standard query response 0x0002 A www.bupt.edu.cn CNAME vn46.bupt.edu.cn A 2…
21	3.562970	2001:da8:215:3c02:7…	2400:3200::1	DNS	95	Standard query 0x0003 AAAA www.bupt.edu.cn
22	3.595763	2400:3200::1	2001:da8:215:3c02:7…	DNS	142	Standard query response 0x0003 AAAA www.bupt.edu.cn CNAME vn46.bupt.edu.cn …

其中，有两个 DNS 协议报文。首先是由本机发给 DNS 服务器，询问 www.bupt.edu.cn 的 AAAA 地址。然后服务器回复本机，包含该网站的 AAAA 地址。

```
> Frame 21: 95 bytes on wire (760 bits), 95 bytes captured (760 bits) on interface \Device\NPF_{ED150
> Ethernet II, Src: LiteonTe_6b:ee:8d (e0:0a:f6:6b:ee:8d), Dst: ArubaaHe_6c:0c:00 (10:4f:58:6c:0c:00)
> Internet Protocol Version 6, Src: 2001:da8:215:3c02:7c71:592d:c73a:68ce, Dst: 2400:3200::1
> User Datagram Protocol, Src Port: 61987, Dst Port: 53
∨ Domain Name System (query)
     Transaction ID: 0x0003
   > Flags: 0x0100 Standard query
     Questions: 1
     Answer RRs: 0
     Authority RRs: 0
     Additional RRs: 0
   ∨ Queries
      > www.bupt.edu.cn: type AAAA, class IN
     [Response In: 22]
```

```
> Frame 22: 142 bytes on wire (1136 bits), 142 bytes captured (1136 bits) on interface \Device\NPF_{E
> Ethernet II, Src: ArubaaHe_6c:0c:00 (10:4f:58:6c:0c:00), Dst: LiteonTe_6b:ee:8d (e0:0a:f6:6b:ee:8d)
> Internet Protocol Version 6, Src: 2400:3200::1, Dst: 2001:da8:215:3c02:7c71:592d:c73a:68ce
> User Datagram Protocol, Src Port: 53, Dst Port: 61987
∨ Domain Name System (response)
     Transaction ID: 0x0003
   > Flags: 0x8180 Standard query response, No error
     Questions: 1
     Answer RRs: 2
     Authority RRs: 0
     Additional RRs: 0
   ∨ Queries
      > www.bupt.edu.cn: type AAAA, class IN
   ∨ Answers
      > www.bupt.edu.cn: type CNAME, class IN, cname vn46.bupt.edu.cn
      > vn46.bupt.edu.cn: type AAAA, class IN, addr 2001:da8:215:4038::161
     [Request In: 21]
     [Time: 0.032793000 seconds]
```

对刚才获取到的 IPv6 地址进行 ping 操作。

```
C:\Users\heng>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=2ms
来自 2001:da8:215:4038::161 的回复: 时间=2ms
来自 2001:da8:215:4038::161 的回复: 时间=2ms
来自 2001:da8:215:4038::161 的回复: 时间=2ms

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 = 2ms，最长 = 2ms，平均 = 2ms
```

Wireshark 捕获到以下报文。

No.	Time	Source	Destination	Protocol	Length	Info
11	4.048300	2001:da8:215:3c02:7...	2001:da8:215:4038::...	ICMPv6	94	Echo (ping) request id=0x0001, seq=91, hop limit=64 (reply in 12)
12	4.050756	2001:da8:215:4038::...	2001:da8:215:3c02:7...	ICMPv6	94	Echo (ping) reply id=0x0001, seq=91, hop limit=59 (request in 11)
13	5.052412	2001:da8:215:3c02:7...	2001:da8:215:4038::...	ICMPv6	94	Echo (ping) request id=0x0001, seq=92, hop limit=64 (reply in 14)
14	5.054366	2001:da8:215:4038::...	2001:da8:215:3c02:7...	ICMPv6	94	Echo (ping) reply id=0x0001, seq=92, hop limit=59 (request in 13)
16	6.063742	2001:da8:215:3c02:7...	2001:da8:215:4038::...	ICMPv6	94	Echo (ping) request id=0x0001, seq=93, hop limit=64 (reply in 17)
17	6.066419	2001:da8:215:4038::...	2001:da8:215:3c02:7...	ICMPv6	94	Echo (ping) reply id=0x0001, seq=93, hop limit=59 (request in 16)
18	7.068633	2001:da8:215:3c02:7...	2001:da8:215:4038::...	ICMPv6	94	Echo (ping) request id=0x0001, seq=94, hop limit=64 (reply in 19)
19	7.071154	2001:da8:215:4038::...	2001:da8:215:3c02:7...	ICMPv6	94	Echo (ping) reply id=0x0001, seq=94, hop limit=59 (request in 18)

Ping 命令将一个流程重复了 4 次。首先，本机向目的 IPv6 地址发 Echo request 报文，即向目标发送回复请求。ICMP 的 type 字段为 128，表示 echo request 类型。标识符为 1，序列号为 91。

```
> Frame 11: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface \Device\NPF_{ED15006
> Ethernet II, Src: LiteonTe_6b:ee:8d (e0:0a:f6:6b:ee:8d), Dst: ArubaaHe_6c:0c:00 (10:4f:58:6c:0c:00)
v Internet Protocol Version 6, Src: 2001:da8:215:3c02:7c71:592d:c73a:68ce, Dst: 2001:da8:215:4038::161
    0110 .... = Version: 6
    > .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... 0000 0000 0000 0000 0000 = Flow Label: 0x00000
    Payload Length: 40
    Next Header: ICMPv6 (58)
    Hop Limit: 64
    Source Address: 2001:da8:215:3c02:7c71:592d:c73a:68ce
    Destination Address: 2001:da8:215:4038::161
v Internet Control Message Protocol v6
    Type: Echo (ping) request (128)
    Code: 0
    Checksum: 0xf1dd [correct]
    [Checksum Status: Good]
    Identifier: 0x0001
    Sequence: 91
    [Response In: 12]
  > Data (32 bytes)
```

然后，目标主机回复本机。ICMP 的 type 字段为 129，表示 echo reply 报文。标识符为 1，序列号为 91，表示这个报文回复的是序列号同为 91 的 echo request 报文。

```
> Frame 12: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface \Device\NPF_{ED15006(
> Ethernet II, Src: ArubaaHe_6c:0c:00 (10:4f:58:6c:0c:00), Dst: LiteonTe_6b:ee:8d (e0:0a:f6:6b:ee:8d)
∨ Internet Protocol Version 6, Src: 2001:da8:215:4038::161, Dst: 2001:da8:215:3c02:7c71:592d:c73a:68ce
     0110 .... = Version: 6
  > .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
     .... 0000 0000 0000 0000 0000 = Flow Label: 0x00000
     Payload Length: 40
     Next Header: ICMPv6 (58)
     Hop Limit: 59
     Source Address: 2001:da8:215:4038::161
     Destination Address: 2001:da8:215:3c02:7c71:592d:c73a:68ce
∨ Internet Control Message Protocol v6
     Type: Echo (ping) reply (129)
     Code: 0
     Checksum: 0xf0dd [correct]
     [Checksum Status: Good]
     Identifier: 0x0001
     Sequence: 91
     [Response To: 11]
     [Response Time: 2.456 ms]
  > Data (32 bytes)
```

对该网站的 IPv6 地址进行 tracert 操作，得到以下结果。结果输出了从本机到目标地址总共需要 6 跳，以及每一跳的目标地址。

```
C:\Users\heng>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     *        *        *     请求超时。
  2     2 ms     1 ms     1 ms  2001:da8:215:0:10:0:28:1
  3     2 ms     1 ms     2 ms  2001:da8:215:0:10:0:4:21
  4     2 ms     1 ms     2 ms  2001:da8:215:0:10:0:4:3a
  5     3 ms     2 ms     2 ms  2001:da8:215:5030:3::2
  6     2 ms     1 ms     2 ms  2001:da8:215:4038::161

跟踪完成。
```

命令 tracert 的工作方式是通过向目标地址发送不同跳数限制(hop limit)值的 echo request 回复请求数据报文，确定到目标所采取的路由。每个跳数限制发送 3 个请求报文。每个中间路由器在转发报文前将数据包上的 hop limit 递减 1。当 hop limit 字段减为 0 时，路由器向源地址发送超时报文。

Wireshark 捕获的数据报文如下。跳数限制为 1 的请求报文没有收到路由器的超时报文，但也没有收到目标地址回复，本机判定为超时。跳数限制 2-5 的请求报文收到了路由器的超时报文，表示跳数已达上限。跳数限制为 6 的请求报文收到了目标地址的回复报文，表示从本机到目标地址最少需要 6 跳。

以下两个请求报文分别是跳数限制为 2 和 3 的请求报文，证明 tracert 通过更改 IPv6 协议的 Hop Limit 跳数限制字段，测试到目标地址的跳数。

这是跳数限制为 3 时，从路由器收到的超时报文，ICMP type 字段为 3。从报文源地址可知，是哪个路由器向本机发送的超时报文，也就是请求报文在前往目标地址路径上的那个路由器达到了跳数上限。

```
> Frame 62: 174 bytes on wire (1392 bits), 174 bytes captured (1392 bits) on interface \Device\NPF_{ED15006
> Ethernet II, Src: ArubaaHe_6c:0c:00 (10:4f:58:6c:0c:00), Dst: LiteonTe_6b:ee:8d (e0:0a:f6:6b:ee:8d)
∨ Internet Protocol Version 6, Src: 2001:da8:215:0:10:0:4:21, Dst: 2001:da8:215:3c02:7c71:592d:c73a:68ce
     0110 .... = Version: 6
   > .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
     .... 0000 0000 0000 0000 0000 = Flow Label: 0x00000
     Payload Length: 120
     Next Header: ICMPv6 (58)
     Hop Limit: 62
     Source Address: 2001:da8:215:0:10:0:4:21
     Destination Address: 2001:da8:215:3c02:7c71:592d:c73a:68ce
∨ Internet Control Message Protocol v6
     Type: Time Exceeded (3)
     Code: 0 (hop limit exceeded in transit)
     Checksum: 0xc12a [correct]
     [Checksum Status: Good]
     Reserved: 00000000
   > Internet Protocol Version 6, Src: 2001:da8:215:3c02:7c71:592d:c73a:68ce, Dst: 2001:da8:215:4038::161
   > Internet Control Message Protocol v6
```

下图是从目标地址收到的 echo reply 回复报文

```
> Frame 90: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits) on interface \Device\NPF_{ED1
> Ethernet II, Src: ArubaaHe_6c:0c:00 (10:4f:58:6c:0c:00), Dst: LiteonTe_6b:ee:8d (e0:0a:f6:6b:ee:8d)
∨ Internet Protocol Version 6, Src: 2001:da8:215:4038::161, Dst: 2001:da8:215:3c02:7c71:592d:c73a:68ce
     0110 .... = Version: 6
   > .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
     .... 0000 0000 0000 0000 0000 = Flow Label: 0x00000
     Payload Length: 72
     Next Header: ICMPv6 (58)
     Hop Limit: 59
     Source Address: 2001:da8:215:4038::161
     Destination Address: 2001:da8:215:3c02:7c71:592d:c73a:68ce
∨ Internet Control Message Protocol v6
     Type: Echo (ping) reply (129)
     Code: 0
     Checksum: 0x9b3c [correct]
     [Checksum Status: Good]
     Identifier: 0x0001
     Sequence: 128
     [Response To: 89]
     [Response Time: 2.051 ms]
   > Data (64 bytes)
```

对网站的 IPv6 地址进行 ping 操作，加上参数 -l 3000，即用含有 3000 字节长度数据字段的报文进行 ping 操作。

```
C:\Users\heng>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=19ms
来自 2001:da8:215:4038::161 的回复: 时间=14ms
来自 2001:da8:215:4038::161 的回复: 时间=15ms
来自 2001:da8:215:4038::161 的回复: 时间=15ms

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 = 14ms，最长 = 19ms，平均 = 15ms
```

Wireshark 捕获到的数据报文。

与不带参数的 ping 操作对比，ping -l 3000 不止在报文的数据字段长度有不同。同时，由于 3000 字节的数据过长，超出了转发接口的最大传输单元值 MTU。因此，这次的数据报文都采用了 IP 分片技术，则在转发报文前，先将其分为更小的片，然后在到达目标地址时，由目标主机进行重组。

以下是本机发送的 echo request 请求报文。在 IPv6 协议头中，有 Fragment Header 分片头。其中，Offset 字段表示这个分片报文的数据在总体数据中的偏移量，More Fragments 字段表示这个报文之后还有同属一组的分片。从下图可见，这个报文的数据偏移量是 2896，并且是该组最后一个报文。Wireshark 软件不会显示所有的分片，但在 IPv6 字段的下方有提示消息，表示总共收到 3 个分片，组装后长度为 3008 字节。

以下是本机收到的 echo reply 回复报文。在 IPv6 协议头中，从下图可见，这个报文的数据偏移量是 0，并且之后还有分片。在 IPv6 字段的下方有提示消息，表示总共收到 3 个分片，组装后长度为 3008 字节。

```
> Frame 22: 1510 bytes on wire (12080 bits), 1510 bytes captured (12080 bits) on interface \Device\NPF_
> Ethernet II, Src: ArubaaHe_6c:0c:00 (10:4f:58:6c:0c:00), Dst: LiteonTe_6b:ee:8d (e0:0a:f6:6b:ee:8d)
∨ Internet Protocol Version 6, Src: 2001:da8:215:4038::161, Dst: 2001:da8:215:3c02:7c71:592d:c73a:68ce
    0110 .... = Version: 6
  > .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... 0000 0000 0000 0000 0000 = Flow Label: 0x00000
    Payload Length: 1456
    Next Header: Fragment Header for IPv6 (44)
    Hop Limit: 59
    Source Address: 2001:da8:215:4038::161
    Destination Address: 2001:da8:215:3c02:7c71:592d:c73a:68ce
  ∨ Fragment Header for IPv6
      Next header: ICMPv6 (58)
      Reserved octet: 0x00
      0000 0000 0000 0... = Offset: 0 (0 bytes)
      .... .... .... .00. = Reserved bits: 0
      .... .... .... ...1 = More Fragments: Yes
      Identification: 0xb8247a88
  > [3 IPv6 Fragments (3008 bytes): #22(1448), #20(1448), #21(112)]
∨ Internet Control Message Protocol v6
    Type: Echo (ping) reply (129)
    Code: 0
    Checksum: 0x677e [correct]
    [Checksum Status: Good]
    Identifier: 0x0001
    Sequence: 153
    [Response To: 19]
    [Response Time: 19.559 ms]
  > Data (3000 bytes)
```

分析与思考

通过本次实验，抓取了 DNS 解析的 DNS 报文、ping、tracert 和长报文 ping 过程的 ICMPv6 报文，并经过分析，学习到了 echo request 和 echo reply 等 ICMPv6 协议报文的内容、作用和各个字段的含义，更加掌握 ICMPv6 协议的原理和 wireshark 软件的使用方法。

在实验过程中，起初关闭本机的 IPv4 协议后，变成了离线状态，无法上网，也久无法进行 nslookup 和 ping 操作。后来通过 ipconfig 分析本机 IP 信息发现，当只使用 IPv6 协议时，本机使用的 DNS 服务器地址以 fec0 开头，代表站点本地地址，也就是暂时没有合适的 IPv6 DNS 服务器。后来发现，nslookup 命令可以加入参数，选择指定的 DNS 服务器进行解析。使用了阿里巴巴公司的 IPv6 DNS 服务器，成功完成 nslookup 操作。