

# 《下一代 Internet 技术与协议》

## 课程实验报告



学院： 计算机学院（国家示范性软件学院）

班级： 2018211314

姓名： 李志毅

学号： 2018211582

# 实验一 IPv6 的使用和测试实验

## 一、实验内容和目的

本次实验内容：

1. 如何打开 Windows 系统的 ipv6 协议，关闭 ipv4 协议
2. 如何使用 ipconfig/all 命令和 ping 命令测试 ipv6 协议的成功使用

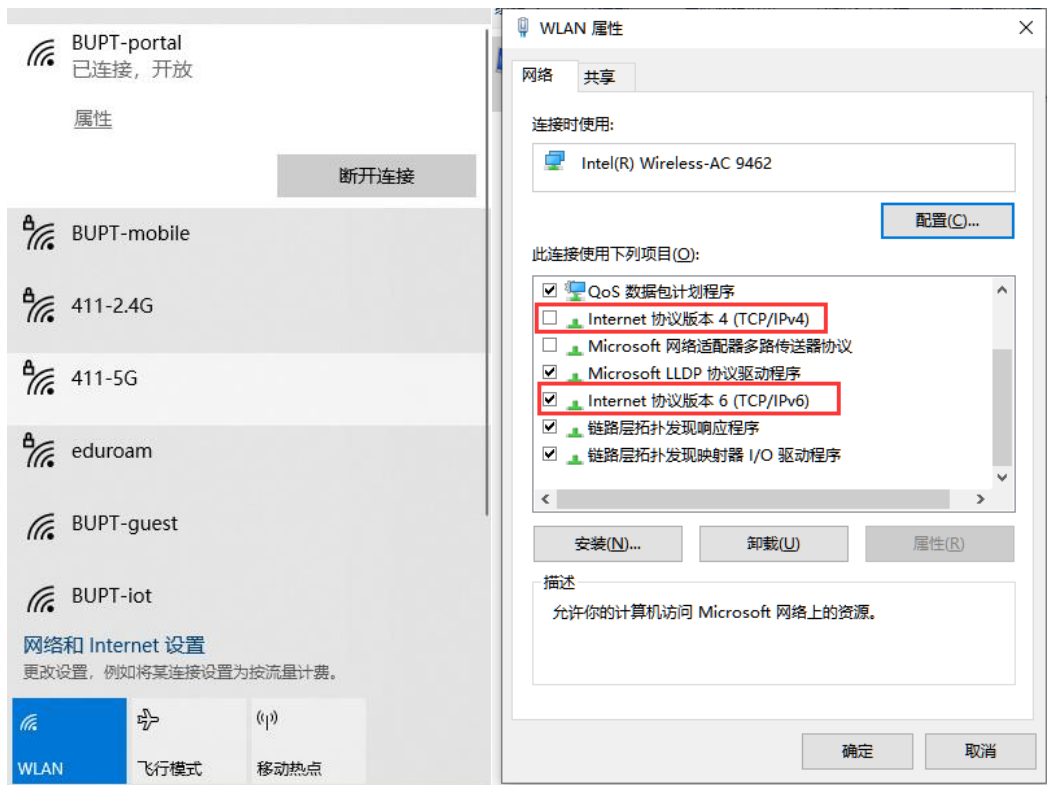
通过本次实验，可以了解 ipv6 协议在 Windows 如何使用，并熟悉常见的地址结合和 ping 命令数据包分析，以及判断该地址类型。

## 二、实验环境

1 台装有 Windows 操作系统的 pc 机，要求能够连接到 Internet，并安装 Wireshark 等软件。1 部使用 SIM 卡连接网络的手机。

## 三、实验准备

### 1. 关闭 IPv4，打开 IPv6



## 2. 打开 PowerShell 窗口，输入 ipconfig -all 命令

```
无线局域网适配器 WLAN:

    连接特定的 DNS 后缀 . . . . . : 
    描述. . . . . : Intel(R) Wireless-AC 9462
    物理地址. . . . . : B4-69-21-10-3C-7C
    DHCP 已启用 . . . . . : 是
    自动配置已启用. . . . . : 是
    IPv6 地址 . . . . . : 2001:da8:215:3c02::4:dfde(首选)
    获得租约的时间 . . . . . : 2021年5月27日 15:10:13
    租约过期的时间 . . . . . : 2021年6月26日 14:29:07
    本地链接 IPv6 地址. . . . . : fe80::8c7e:895f:ac96:105f%18(首选)
    默认网关. . . . . : fe80::7685:c4ff:fe11:2001%18
    DHCPv6 IAID . . . . . : 297036065
    DHCPv6 客户端 DUID . . . . . : 00-01-00-01-23-26-F8-07-54-BF-64-50-49-BA
    DNS 服务器 . . . . . : fec0:0:0:ffff::1%1
                           fec0:0:0:ffff::2%1
                           fec0:0:0:ffff::3%1
    TCP/IP 上的 NetBIOS . . . . . : 已禁用
```

与 IPv6 相关的地址的相关信息整理为：

名称	地址	描述
IPv6 地址	2001:da8:215:3c02::4:dfde	属于 2000-3FFF 范围，为可汇聚全球单播地址
本地链接 IPv6 地址	fe80::8c7e:895f:ac96:105f%18	FE80-FEBF 范围，为链路本地单播地址
默认网关	fe80::7685:c4ff:fe11:2001%18	链路本地网关地址
DNS 服务器	fec0:0:0:ffff::1%1 fec0:0:0:ffff::2%1 fec0:0:0:ffff::3%1	IPv6 网络上的 DNS 服务器地址，FEC0 开头代表站点本地地址

## 3. 使用 nslookup 命令对选定的网站域名进行 DNS 解析，截图并记录其 IPv6 地址

```
C:\Users\hexing>nslookup paper.people.com.cn 240c::6666
服务器: UnKnown
Address: 240c::6666

非权威应答:
名称: paper.people.com.cn.wscdns.com
Addresses: 2408:8710:20:1040::16
          125.220.192.169
Aliases: paper.people.com.cn
```

#### 4. 对此网站的 IPv6 地址进行 ping 操作，截图记录

```
C:\Users\hexing>ping 2408:8710:20:1040::16

正在 Ping 2408:8710:20:1040::16 具有 32 字节的数据:
来自 2408:8710:20:1040::16 的回复: 时间=51ms
来自 2408:8710:20:1040::16 的回复: 时间=55ms
来自 2408:8710:20:1040::16 的回复: 时间=36ms
来自 2408:8710:20:1040::16 的回复: 时间=28ms

2408:8710:20:1040::16 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 = 28ms, 最长 = 55ms, 平均 = 42ms
```

#### 5. 对此网站的 IPv6 地址进行 tracert 操作，使用 tracert -d

#### XXXX:XXXX 的命令和参数-d，截图记录

```
C:\Users\hexing>tracert -d 2408:8710:20:1040::16

通过最多 30 个跃点跟踪到 2408:8710:20:1040::16 的路由

 1    4 ms    4 ms    4 ms    2001:da8:215:3c02::1
 2    9 ms    9 ms    5 ms    2001:da8:215:0:10:0:28:1
 3   49 ms    4 ms    3 ms    2001:da8:215:0:10:0:4:21
 4    8 ms    4 ms    4 ms    2001:da8:215:0:10:0:3:1
 5     *      *      *      请求超时。
 6    3 ms    6 ms    4 ms    2001:da8:2:123::1
 7    6 ms    6 ms    4 ms    2001:da8:2:5::1
 8    7 ms    6 ms    7 ms    2001:da8:2:2::2
 9   11 ms   12 ms   12 ms    2001:da8:2:27::2
10   30 ms   30 ms   32 ms    2001:da8:2:11::1
11   30 ms   30 ms   33 ms    2001:da8:2:753::2
12   33 ms   32 ms   34 ms    2001:da8:257:0:101:4:118:111
13   73 ms   27 ms   28 ms    2408:8000:3::340
14   29 ms   29 ms   29 ms    2408:8000:2:485::
15     *      *      *      请求超时。
16   32 ms   28 ms   30 ms    2408:8000:2002:8000::29
17   58 ms   33 ms   31 ms    2408:8710:10:1::35
18   28 ms   33 ms   29 ms    2408:8710:20:1040::16

跟踪完成。
```

## 四、抓包内容与分析

### 1. 使用 nslookup 命令对选定网站进行 DNS 解析

本次实验中，我选取的支持 IPv6 的网站为人民日报-人民网，域名为 <http://paper.people.com.cn/>，利用 nslookup 命令对该域名进行解析，指定 IPv6 服务器为 240c::6666，最终获取到的地址为 2408:8710:20:1040::16

使用 Wireshark 抓包可以看到：

40 19.814938	2001:da8:215:3c01:14d5:a3da:dc50:5249	240c::6666	DNS	99 Standard query 0x0002 A paper.people.com.cn
41 19.692632	2001:da8:215:3c01:14d5:a3da:dc50:5249	fec0:0:0:ffff::3	DNS	109 Standard query 0xcd2a AAAA v20.events.data.microsoft.com
42 20.604648	240c::6666	2001:da8:215:3c01:14d5:a3da:dc50:5249	DNS	159 Standard query response 0x0002 A paper.people.com.cn CNAME paper.people.com.cn.wscdns.com A 125.
43 20.616420	2001:da8:215:3c01:14d5:a3da:dc50:5249	240c::6666	DNS	99 Standard query 0x0003 AAAA paper.people.com.cn
44 20.728534	240c::6666	2001:da8:215:3c01:14d5:a3da:dc50:5249	DNS	171 Standard query response 0x0003 AAAA paper.people.com.cn CNAME paper.people.com.cn.wscdns.com AAA

本地向 DNS 服务器发送 DNS 请求报文，请求 paper.people.com.cn 的 AAAA 地址，而后 DNS 服务器向本地返回 DNS 响应报文，在报文中给 paper.people.com.cn 的 IPv6 地址信息，与 CMD 中显示一致

```
▼ Domain Name System (query)
  Transaction ID: 0x0003
  > Flags: 0x0100 Standard query
  Questions: 1
  Answer RRs: 0
  Authority RRs: 0
  Additional RRs: 0
  ▼ Queries
    ▼ paper.people.com.cn: type AAAA, class IN
      Name: paper.people.com.cn
      [Name Length: 19]
      [Label Count: 4]
      Type: AAAA (IPv6 Address) (28)
      Class: IN (0x0001)
      [Response In: 44]

▼ 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
    > paper.people.com.cn: type AAAA, class IN
  ▼ Answers
    > paper.people.com.cn: type CNAME, class IN, cname paper.people.com.cn.wscdns.com
    ▼ paper.people.com.cn.wscdns.com: type AAAA, class IN, addr 2408:8710:20:1040::16
      Name: paper.people.com.cn.wscdns.com
      Type: AAAA (IPv6 Address) (28)
      Class: IN (0x0001)
      Time to live: 120 (2 minutes)
      Data length: 16
      AAAA Address: 2408:8710:20:1040::16
      [Request In: 43]
  [Time: 0.112114000 seconds]
```

## 2. 对此网站的 IPv6 地址进行 ping 操作

```
C:\Users\hexing>ping 2408:8710:20:1040::16

正在 Ping 2408:8710:20:1040::16 具有 32 字节的数据:
来自 2408:8710:20:1040::16 的回复: 时间=30ms
来自 2408:8710:20:1040::16 的回复: 时间=29ms
来自 2408:8710:20:1040::16 的回复: 时间=28ms
来自 2408:8710:20:1040::16 的回复: 时间=34ms

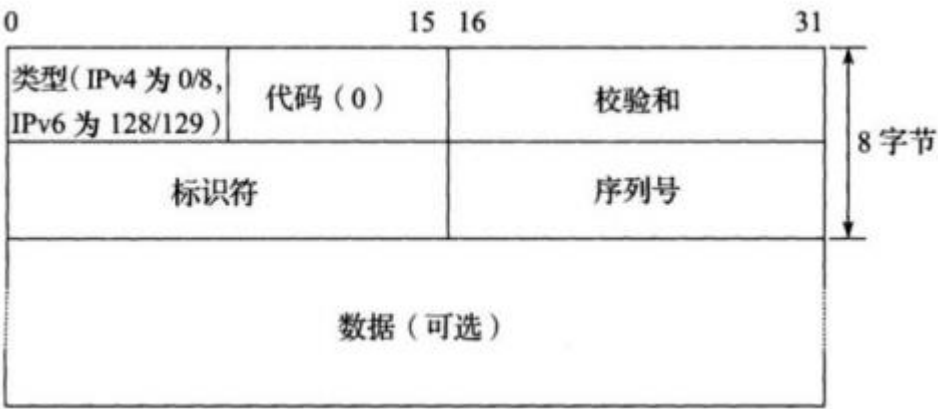
2408:8710:20:1040::16 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 28ms, 最长 = 34ms, 平均 = 30ms
```

```
16 2.356142      2001:da8:215:3c02::4:dfde      2408:8710:20:1040::16      ICMPv6      94 Echo (ping) request id=0x0001, seq=5, hop limit=128 (reply in 17)
17 2.386585      2408:8710:20:1040::16      2001:da8:215:3c02::4:dfde      2001:da8:215:3c02::4:dfde      ICMPv6      94 Echo (ping) reply id=0x0001, seq=5, hop limit=51 (request in 16)
26 3.370147      2001:da8:215:3c02::4:dfde      2408:8710:20:1040::16      2408:8710:20:1040::16      ICMPv6      94 Echo (ping) request id=0x0001, seq=6, hop limit=128 (reply in 27)
27 3.399243      2408:8710:20:1040::16      2001:da8:215:3c02::4:dfde      2001:da8:215:3c02::4:dfde      ICMPv6      94 Echo (ping) reply id=0x0001, seq=6, hop limit=51 (request in 26)
30 4.071543      fe80::7685:c4ff:fe11:2001      ff02::1      ICMPv6      118 Router Advertisement from 74:85:c4:11:20:01
35 4.381220      2001:da8:215:3c02::4:dfde      2408:8710:20:1040::16      2408:8710:20:1040::16      ICMPv6      94 Echo (ping) request id=0x0001, seq=7, hop limit=128 (reply in 36)
36 4.409632      2408:8710:20:1040::16      2001:da8:215:3c02::4:dfde      2001:da8:215:3c02::4:dfde      ICMPv6      94 Echo (ping) reply id=0x0001, seq=7, hop limit=51 (request in 35)
46 5.391801      2001:da8:215:3c02::4:dfde      2408:8710:20:1040::16      2408:8710:20:1040::16      ICMPv6      94 Echo (ping) request id=0x0001, seq=8, hop limit=128 (reply in 47)
47 5.425610      2408:8710:20:1040::16      2001:da8:215:3c02::4:dfde      2001:da8:215:3c02::4:dfde      ICMPv6      94 Echo (ping) reply id=0x0001, seq=8, hop limit=51 (request in 46)
```

ping 指令的作用是随机生成固定长度的数据包，通过 ICMP（Internet 控制消息协议）协议将数据包发送到指定主机，并侦听回显回复报文来探测与目标主机之间的连接。在本机的 CMD 当中显示出发送的数据、回复的时间等信息。

观察 CMD 中的输出可知：通过 ping 指令向 2408:8710:20:1040::16 发送了四段报文，并均得到了回复。再对比观察 wireshark 当中抓取到的报文，也同样捕获到了四组 ICMP 的 ping 报文，每组报文有两个包构成。

一个包是由本机向目标主机（2408:8710:20:1040::16）发送的 Echo request 包；另一个包是由目标主机接受到本机发送的 Echo request 后回复的 Echo reply 包。由于四组报文的内容基本一致，因此在此只对第一组报文进行详细分析。



## ● ICMPv6-Echo request

```

v Internet Protocol Version 6, Src: 2001:da8:215:3c02::4:dfde, Dst: 2408:8710:20:1040::16
  0110 .... = Version: 6
  > .... 0000 0000 .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
  .... 0000 0000 0000 0000 = Flow Label: 0x00000
  Payload Length: 40
  Next Header: ICMPv6 (58)
  Hop Limit: 128
  Source Address: 2001:da8:215:3c02::4:dfde
  Destination Address: 2408:8710:20:1040::16
v Internet Control Message Protocol v6
  Type: Echo (ping) request (128)
  Code: 0
  Checksum: 0xcdc0 [correct]
  [Checksum Status: Good]
  Identifier: 0x0001
  Sequence: 6
  [Response In: 27]
v Data (32 bytes)
  Data: 6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869
  [Length: 32]
```

该报文是由本机发往目标主机（2408:8710:20:1040::16）的 echo request 报文，即向目标主机发送回显请求。其中 ICMP 报文 Type 字段为 128，代表该报文为 echo request 报文；code 字段内容为 0，checksum 校验和根据报文内容生成；标识符为 1；序列号为 6；数据内容由 ping 指令随机生成长度 32bytes。

## ● ICMPv6-Echo reply

```

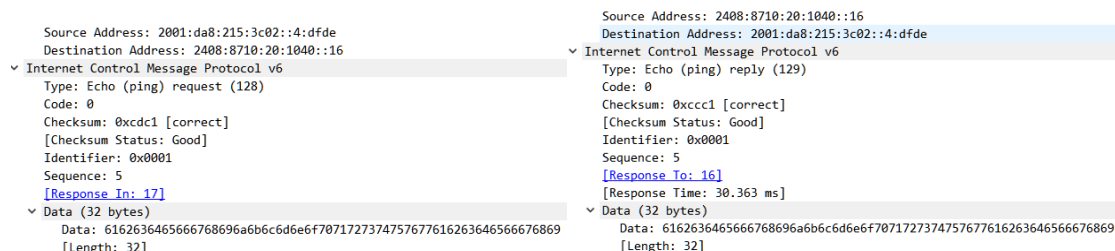
v Internet Protocol Version 6, Src: 2408:8710:20:1040::16, Dst: 2001:da8:215:3c02::4:dfde
  0110 .... = Version: 6
  > .... 0000 0000 .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
  .... 0000 0000 0000 0000 = Flow Label: 0x00000
  Payload Length: 40
  Next Header: ICMPv6 (58)
  Hop Limit: 51
  Source Address: 2408:8710:20:1040::16
  Destination Address: 2001:da8:215:3c02::4:dfde
v Internet Control Message Protocol v6
  Type: Echo (ping) reply (129)
  Code: 0
  Checksum: 0xcc0 [correct]
  [Checksum Status: Good]
  Identifier: 0x0001
  Sequence: 6
  [Response To: 26]
  [Response Time: 29.096 ms]
v Data (32 bytes)
  Data: 6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869
  [Length: 32]
```

该报文是由目标主机(2408:8710:20:1040::16)发往本机的 echo reply 报文，即向目标主机发送回复报文。其中 ICMP 报文 Type 字段为 129，代表该报文为 echo reply 报文；code 字段内容为 0；checksum 校验和根据报文内容生成；标识符为 1；序列号为 6；数据内容 data 与 echo request 报文中数据一致。

对比同组报文，传送方向分别为本机到目标主机、目标主机到本机；类

型分别为 128 (echo request)、129 (echo reply); 校验和不同, 根据报文生成; 序列号相同均为 6; 数据 data 由 ping 指令随机生成。

其余报文同理:



### 3. 对此网站的 IPv6 地址进行 tracert 操作

```
C:\Users\hexing>tracert -d 2408:8710:20:1040::16

通过最多 30 个跃点跟踪到 2408:8710:20:1040::16 的路由

 1      4 ms      4 ms      4 ms  2001:da8:215:3c02::1
 2      9 ms      9 ms      5 ms  2001:da8:215:0:10:0:28:1
 3     49 ms      4 ms      3 ms  2001:da8:215:0:10:0:4:21
 4      8 ms      4 ms      4 ms  2001:da8:215:0:10:0:3:1
 5      *         *         *    请求超时。
 6      3 ms      6 ms      4 ms  2001:da8:2:123::1
 7      6 ms      6 ms      4 ms  2001:da8:2:5::1
 8      7 ms      6 ms      7 ms  2001:da8:2:2::2
 9     11 ms     12 ms     12 ms  2001:da8:2:27::2
10     30 ms     30 ms     32 ms  2001:da8:2:11::1
11     30 ms     30 ms     33 ms  2001:da8:2:753::2
12     33 ms     32 ms     34 ms  2001:da8:257:0:101:4:118:111
13     73 ms     27 ms     28 ms  2408:8000:3::340
14     29 ms     29 ms     29 ms  2408:8000:2:485::
15      *         *         *    请求超时。
16     32 ms     28 ms     30 ms  2408:8000:2002:8000::29
17     58 ms     33 ms     31 ms  2408:8710:10:1::35
18     28 ms     33 ms     29 ms  2408:8710:20:1040::16
```

通过向目标地址发送不同跳数限制(hop limit)值的“Internet 控制消息协议 (ICMP)”回显请求数据包, tracert 诊断程序确定到目标所采取的路由。要求路径上的每个路由器在转发数据包之前至少将数据包上的 hop limit 递减 1。当数据包上的 hop limit 减为 0 时, 路由器应该将“已超时”的消息发回源地址。

tracert 先发送 hop limit 为 1 的回显请求数据包, 并在随后的每次发送过程将 hop limit 递增 1, 直到目标响应或 hop limit (最大为 30) 达到最



大值，从而确定路由。通过检查中间路由器发回的“已超时”的消息确定路由。某些路由器不经询问直接丢弃 hop limit 过期的数据包，这在捕获报文时不会存在回显 应答报文。

跟踪路由（Tracert）是路由跟踪实用程序，用于确定 IP 数据包访问目标所采取的路径，其工作原理是通过向目标发送不同跳转限制（hop limit）值的“Internet 控制消息协议（ICMP）”回应数据包，跟踪路由诊断程序确定到目标所采取的路由。实际应用中可以使用跟踪路由命令确定数据包在网络上的停止位置。

Wireshark 软件中捕获的报文情况如下:

84	20.367799	2001:da8:215:c002::4:dfde	2408:8710:20:1040::16	IOHPv6	126 Echo (ping) request ID=00001, seq=50, hop limit=10 (no response found)
85	20.368035	2001:da8:215:c002::4:dfde	2408:8710:20:1040::16	IOHPv6	174 Time Exceeded (hop limit exceeded in transit)
86	20.401654	2001:da8:215:c002::4:dfde	2408:8710:20:1040::16	IOHPv6	126 Echo (ping) request ID=00001, seq=51, hop limit=10 (no response found)
87	20.432373	2001:da8:215:c002::4:dfde	2408:8710:20:1040::16	IOHPv6	174 Time Exceeded (hop limit exceeded in transit)
88	20.435720	2001:da8:215:c002::4:dfde	2408:8710:20:1040::16	IOHPv6	126 Echo (ping) request ID=00001, seq=52, hop limit=10 (no response found)
89	20.466785	2001:da8:215:c002::4:dfde	2408:8710:20:1040::16	IOHPv6	174 Time Exceeded (hop limit exceeded in transit)
90	21.460650	2001:da8:215:c002::4:dfde	2408:8710:20:1040::16	IOHPv6	126 Echo (ping) request ID=00001, seq=53, hop limit=11 (no response found)
91	21.520662	2001:da8:215:c002::4:dfde	2408:8710:20:1040::16	IOHPv6	174 Time Exceeded (hop limit exceeded in transit)
92	21.568066	2001:da8:215:c002::4:dfde	2408:8710:20:1040::16	IOHPv6	126 Echo (ping) request ID=00001, seq=54, hop limit=11 (no response found)
93	21.532804	2001:da8:215:c002::4:dfde	2408:8710:20:1040::16	IOHPv6	174 Time Exceeded (hop limit exceeded in transit)
94	21.535313	2001:da8:215:c002::4:dfde	2408:8710:20:1040::16	IOHPv6	126 Echo (ping) request ID=00001, seq=55, hop limit=11 (no response found)
95	21.568441	2001:da8:215:c002::4:dfde	2408:8710:20:1040::16	IOHPv6	174 Time Exceeded (hop limit exceeded in transit)
96	21.514113	fe80::7685:c4f7:fe11:2001:1001	fe80::7685:c4f7:fe11:2001:1001	IOHPv6	118 Router Advertisement ID=00001, seq=45, rtr=11, hop limit=1
97	22.565554	2001:da8:215:c002::4:dfde	2408:8710:20:1040::16	IOHPv6	126 Echo (ping) request ID=00001, seq=56, hop limit=12 (no response found)
98	22.559489	2001:da8:257:0:101::4:118:111	2001:da8:257:0:101::4:118:111	IOHPv6	174 Time Exceeded (hop limit exceeded in transit)
99	22.601638	2001:da8:215:c002::4:dfde	2408:8710:20:1040::16	IOHPv6	126 Echo (ping) request ID=00001, seq=57, hop limit=12 (no response found)
100	22.613864	2001:da8:257:0:101::4:118:111	2001:da8:257:0:101::4:118:111	IOHPv6	174 Time Exceeded (hop limit exceeded in transit)
101	22.636092	2001:da8:215:c002::4:dfde	2408:8710:20:1040::16	IOHPv6	126 Echo (ping) request ID=00001, seq=58, hop limit=12 (no response found)
102	22.670877	2001:da8:257:8:101::4:118:111	2001:da8:257:8:101::4:118:111	IOHPv6	174 Time Exceeded (hop limit exceeded in transit)

结合命令行显示以及抓包分析结果可知，每次主机向目标地址发送递增的 hop 限制的 Echo request 报文，并且每次发送三个为一组。当 hop limit 减为 0 时，中间路由将会向主机回发超时报文，主机以此获得每一跳的路由信息。在实际实验过程中，总共进行了 hop limit 1~21 的 echo request，其中除了 5 以外，每个跳数限制下的请求报文均得到了回应。

总体而言，我们可以将整个过程分为三类：发送的 request 有收到超时 time exceeded 的(1-4 & 6-20)；发送的 request 没有收到超时 time exceeded 的(5)；发送的 echo request 收到了 echo reply 报文的回复(21)。

- ICMPv6-Echo Request

[illegible]

## ● ICMPv6-time Exceeded

```
> Internet Protocol Version 6, Src: 2001:da8:2:11::1, Dst: 2001:da8:215:3c02::4:dfde
v Internet Control Message Protocol v6
  Type: Time Exceeded (3)
  Code: 0 (hop limit exceeded in transit)
  Checksum: 0xe925 [correct]
  [Checksum Status: Good]
  Reserved: 00000000
v Internet Protocol Version 6, Src: 2001:da8:215:3c02::4:dfde, Dst: 2408:8710:20:1040::16
  0110 .... = Version: 6
  > .... 0000 0000 .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
  .... 0000 0000 0000 0000 = Flow Label: 0x00000
  Payload Length: 72
  Next Header: ICMPv6 (58)
  Hop Limit: 1
  Source Address: 2001:da8:215:3c02::4:dfde
  Destination Address: 2408:8710:20:1040::16
v Internet Control Message Protocol v6
  Type: Echo (ping) request (128)
  Code: 0
  Checksum: 0x7818 [unverified] [in ICMP error packet]
  [Checksum Status: Unverified]
  Identifier: 0x0001
  Sequence: 50
v Data (64 bytes)
  Data: 0000000000000000000000000000000000000000000000000000000000000000...
  [Length: 64]
```

```
8      7 ms      6 ms      7 ms      2001:da8:2:2::2
9      11 ms     12 ms     12 ms     2001:da8:2:27::2
10     30 ms     30 ms     32 ms     2001:da8:2:11::1
11     30 ms     30 ms     33 ms     2001:da8:2:753::2
12     33 ms     32 ms     34 ms     2001:da8:257:0:101:4:118:111
13     73 ms     27 ms     28 ms     2408:8000:3::340
14     29 ms     29 ms     29 ms     2408:8000:2:485::
15      *        *        *        请求超时。
16     32 ms     28 ms     30 ms     2408:8000:2002:8000::29
17     58 ms     33 ms     31 ms     2408:8710:10:1::35
18     28 ms     33 ms     29 ms     2408:8710:20:1040::16
```

由如上报文可以看出，本机向目标主机发送了 hop limit 为 1 的报文，在经过一跳到达一个路由节点后，由于 hop limit 被减为 0，对应路由返回 time exceeded 报文。在返回的 time exceeded 的报文中可以看到对应的源地址与最终得出的路由结果里对应节点的地址一致

同时发现，当 hop limit=5 时：

```
30 4.478893      2001:da8:215:3c02::4:dfde      2408:8710:20:1040::16      ICMPv6 126 Echo (ping) request id=0x0001, seq=35, [hop limit=5] (no response found!)
34 6.245719      fe80::7685:c4ff:fe11:2001      ff02::1      ICMPv6 118 Router Advertisement from 74:85:c4:11:20:01
35 8.199141      2001:da8:215:3c02::4:dfde      2408:8710:20:1040::16      ICMPv6 126 Echo (ping) request id=0x0001, seq=36, [hop limit=5] (no response found!)
36 9.317394      fe80::7685:c4ff:fe11:2001      ff02::1      ICMPv6 118 Router Advertisement from 74:85:c4:11:20:01
37 11.647237      fe80::7685:c4ff:fe11:2001      2001:da8:215:3c02::4:dfde      ICMPv6 86 Neighbor Solicitation for 2001:da8:215:3c02::4:dfde from 74:85:c4:11:20:01
38 11.647514      2001:da8:215:3c02::4:dfde      fe80::7685:c4ff:fe11:2001      ICMPv6 86 Neighbor Advertisement 2001:da8:215:3c02::4:dfde (sol, ovr) is at b4:69:21:10:3c
40 12.198016      2001:da8:215:3c02::4:dfde      2408:8710:20:1040::16      ICMPv6 126 Echo (ping) request id=0x0001, seq=37, [hop limit=5] (no response found!)
```

[illegible]

hop limit 为 5 并未收到类似的 time exceed 报文回复,说明没有报文回复,可能原因是: 那一跳禁止 ping、不对 TTL 超时响应处理等

当 hop limit 达到 18 时, echo request 抵达目标地址

(2408:8710:20:1040::16)

```
16    32 ms    28 ms    30 ms    2408:8000:2002:8000::29
17    58 ms    33 ms    31 ms    2408:8710:10:1::35
18    28 ms    33 ms    29 ms    2408:8710:20:1040::16
跟踪完成。
C:\Users\hexing>
```

## 五、实验问题与心得

本次实验使用 Wireshark 抓包分析了 ping 命令和 tracert 命令执行过程中的报文收发情况，主要分析了 ICMPv6 报文的各项字段和整个过程，通过本实验，让我对于 ICMPv6 协议的具体内容有了更深的理解，对 Wireshark 抓包软件的使用更加熟练，对 ICMPv6 协议下的各种类型包有了更好的掌握，锻炼了我的实践能力和分析能力，让我进一步理解了 ping、tracert 命令的工作原理，以及计算机网络路由的相关性知识。