

Principles of Computer Networks

Homework 5*

Chenghua Liu[†]

liuch18@mails.tsinghua.edu.cn

Department of Computer Science

Tsinghua University

目录

1	problems in chapter 5	2
1.1	problem 2	2
1.2	problem 3	2
1.3	problem 9	2
1.4	problem 10	2
1.5	problem 22	2
1.6	problem 28	2
1.7	problem 34	3
1.8	problem 40	3
1.9	problem 42	3
2	IP、ICMP 及 ND 观察实验	3
2.1	IP 协议	3
2.1.1	观察普通 IP 分组	3
2.1.2	观察 IP 分片与重组	4
2.1.3	思考题	5
2.2	ICMP 协议	6
2.2.1	观察 ICMP 回显请求及回显应答	6
2.2.2	观察 ICMP 目标不可达消息	7
2.2.3	观察 ICMP 超时消息	7

*problems from Computer Networks, 5th Edition

[†]2018011687

2.2.4 思考题	8
2.3 ND 协议	8
2.3.1 观察地址解析 (Address Resolution) 过程及 ND 报文格式	8
2.3.2 观察 Router Advertisement 以及 DAD	10
2.3.3 思考题	10

1 problems in chapter 5

1.1 problem 2

虚电路网络也需要在两个主机之间寻找路径的能力，这是为了在开始传送前建立虚电路。

1.2 problem 3

- 滑动窗口大小
- 最大包长
- 数据传输速率

1.3 problem 9

设簇数为 x , 区域数为 y , 每个区域路由器数 z , $xyz \geq 4800$, 枚举求 $x + y + z$ 的最小值。
得 $x = 15, y = 16, z = 20$ 时路由表尺寸最小, 其中 x, y, z 可交换。路由表最小尺寸

$$(x + y + z - 2)_{min} = 49$$

因不必存储本 cluster 和本 region 的地址, 故结果减去 2。

1.4 problem 10

当路由器收到以移动设备为目的地的包时, 它会用 ARP 包询问其 MAC 地址。如果移动设备不在该路由器的网络中, Agent 可以用 Agent 的 MAC 地址响应, 使路由器将这个包发往 Agent。

1.5 problem 22

不能保证加急包比普通包更快。假设大部分包都要求加急, 那么用于发送加急包的路径会发生或接近拥塞, 使效率反而低于发送普通包的路径。

1.6 problem 28

主机位为 12 位, 共能容纳 $2^{12} - 2 = 4094$ 台主机。

1.7 problem 34

只要每个路由器都有单独的 ip 地址，且与同一个连接相关的数据包都通过同一路由器进出，就可以正常工作。

1.8 problem 40

$$\frac{2^{128}}{10^6 ps^{-1}} = 3.4 \times 10^{20} s \approx 1 \times 10^{13} year$$

1.9 problem 42

ARP 协议需要做相应调整。调整仅为技术性的，即需要将相应的地址字段从 32 位加长到 128 位以适应 IPv6 地址。

2 IP、ICMP 及 ND 观察实验

2.1 IP 协议

2.1.1 观察普通 IP 分组

1. 分组头部 Version 字段的值是不是 6?

分组头部的 version 是 6，如图。

1203 92.843103	2402:f000:1:404:166:1...	2402:f000:2:c001:9ca5...	ICMPv6	126 Echo (ping) reply id=0x0001, se
1204 92.846419	2402:f000:2:c001:9ca5...	2402:f000:1:404:166:1...	ICMPv6	126 Echo (ping) request id=0x0001, s
1205 92.856324	2402:f000:1:404:166:1...	2402:f000:2:c001:9ca5...	ICMPv6	126 Echo (ping) reply id=0x0001, se
1206 92.858986	2402:f000:2:c001:9ca5...	2402:f000:1:404:166:1...	ICMPv6	126 Echo (ping) request id=0x0001, s
1207 92.861264	2402:f000:1:404:166:1...	2402:f000:2:c001:9ca5...	ICMPv6	126 Echo (ping) reply id=0x0001, se

Frame 1202: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits) on interface \Device\NPF_{2535945F-C11C-4EB5-80EA-278F297BDE07}, id 0
Ethernet II, Src: IntelCor_cc:dc:fb (3c:f0:11:cc:dc:fb), Dst: HuaweiTe_b9:7f:03 (90:03:25:b9:7f:03)
Internet Protocol Version 6, Src: 2402:f000:2:c001:9ca5:cf01:3ccb:5b92, Dst: 2402:f000:1:404:166:111:4:100
0110 = Version: 6
> 0000 0000 = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
.... 0000 0000 0000 0000 0000 = Flow Label: 0x000000

2. 选取一至两个分组验证一下 Payload Length、Source 以及 Destination 字段是否正确。

为 TCP 时：length=20，Source、Destination 字段正确。其中 source 为本机的 ipv6 临时地址，Destination 为清华官网的地址

374 13.288705	2402:f000:2:c001:9ca5...	2402:f000:1:400::2	TCP	74 50980 → 443 [ACK] Seq=1523 Ack=146287 Win=131072 Len=0
375 13.288730	2402:f000:2:c001:9ca5...	2402:f000:1:400::2	TCP	74 50980 → 443 [ACK] Seq=1523 Ack=148967 Win=131072 Len=0
376 13.288750	2402:f000:2:c001:9ca5...	2402:f000:1:400::2	TCP	74 50980 → 443 [ACK] Seq=1523 Ack=151647 Win=131072 Len=0
377 13.288778	2402:f000:2:c001:9ca5...	2402:f000:1:400::2	TCP	74 50980 → 443 [ACK] Seq=1523 Ack=154327 Win=131072 Len=0

> Frame 369: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{2535945F-C11C-4EB5-80EA-278F297BDE07}, id 0
Ethernet II, Src: IntelCor_cc:dc:fb (3c:f0:11:cc:dc:fb), Dst: HuaweiTe_b9:7f:03 (90:03:25:b9:7f:03)
Internet Protocol Version 6, Src: 2402:f000:2:c001:9ca5:cf01:3ccb:5b92, Dst: 2402:f000:1:400::2
0110 = Version: 6
> 0000 0000 = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
.... 1101 1100 1011 1101 0010 = Flow Label: 0xdcbd2
Payload Length: 20
Next Header: TCP (6)

为 ICMPv6 时, length=40, Source、Destination 字段正确。其中 source 为本机的 ipv6 临时地址, Destination 为清华官网的地址。

2534 331.589900	2402::f000:1:404:166:1..	2402::f000:1:404:166:1..	ICMPv6	94 Echo (ping) request id=0x0001, seq=115, hop limit=64 (request in 2533)
2546 332.602857	2402::f000:2:c001:9ca5..	2402::f000:1:404:166:1..	ICMPv6	94 Echo (ping) request id=0x0001, seq=116, hop limit=64 (reply in 2547)
2547 332.604778	2402::f000:1:404:166:1..	2402::f000:2:c001:9ca5..	ICMPv6	94 Echo (ping) reply id=0x0001, seq=116, hop limit=58 (request in 2546)
2553 333.619772	2402::f000:2:c001:9ca5..	2402::f000:1:404:166:1..	ICMPv6	94 Echo (ping) request id=0x0001, seq=117, hop limit=64 (reply in 2554)
2554 333.624181	2402::f000:1:404:166:1..	2402::f000:2:c001:9ca5..	ICMPv6	94 Echo (ping) reply id=0x0001, seq=117, hop limit=58 (request in 2553)
2866 395.132502	2402::f000:2:c001:9ca5..	2402::f000:1:404:166:1..	ICMPv6	94 Echo (ping) request id=0x0001, seq=118, hop limit=64 (reply in 2867)
2867 395.136348	2402::f000:1:404:166:1..	2402::f000:2:c001:9ca5..	ICMPv6	94 Echo (ping) reply id=0x0001, seq=118, hop limit=58 (request in 2866)
2868 396.143928	2402::f000:2:c001:9ca5..	2402::f000:1:404:166:1..	ICMPv6	94 Echo (ping) request id=0x0001, seq=119, hop limit=64 (reply in 2869)

- 观察 ping 应答分组中的 Hop Limit 值, 推断应答分组到达实验者主机之前经过了多少个路由器。

应答分组中, hop limit 为 59, 经过了 $64-59=5$ 个路由器。

1734 3.911969	2402::f000:1:404:166:1..	2402::f000:3:1001:4dc6..	ICMPv6	94 Echo (ping) reply id=0x0001, seq=5, hop limit=59
2100 4.935413	2402::f000:1:404:166:1..	2402::f000:3:1001:4dc6..	ICMPv6	94 Echo (ping) reply id=0x0001, seq=6, hop limit=59
2497 5.949784	2402::f000:1:404:166:1..	2402::f000:3:1001:4dc6..	ICMPv6	94 Echo (ping) reply id=0x0001, seq=7, hop limit=59
2960 6.965230	2402::f000:1:404:166:1..	2402::f000:3:1001:4dc6..	ICMPv6	94 Echo (ping) reply id=0x0001, seq=8, hop limit=59
4063 9.233106	2402::f000:1:404:166:1..	2402::f000:3:1001:4dc6..	ICMPv6	94 Echo (ping) reply id=0x0001, seq=9, hop limit=59
8120 10.240154	2402::f000:1:404:166:1..	2402::f000:3:1001:4dc6..	ICMPv6	94 Echo (ping) reply id=0x0001, seq=10, hop limit=59

2.1.2 观察 IP 分片与重组

- 确认 ping 每次 (每秒) 发出的若干 IP 分组是否带有分片扩展头, 其中的 Identification 值分别是多少, 是否一致。

0x641d03aa, 0x641d03ac, 0x641d03ae, 0x641d03b0, 不一致。

- 观察 ping 每次发出的若干 IP 分组的分片扩展头中的标志位, 它们的 MF (More Fragments) 分别是多少? 0 和 1 分别代表什么含义?

前两个的 MF 为 1, 最后一个是 0。

1 表示后面还有分段;

```

Internet Protocol Version 6, Src: 2402:f000:3:1001:4dc6:58a6:d7d6:71fa, Dst: 2402:f000:1:404:166:111:4:100
  0110 .... = Version: 6
  > .... 0000 0000 .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
  .... 0000 0000 0000 0000 = Flow Label: 0x000000
  Payload Length: 120
  Next Header: Fragment Header for IPv6 (44)
  Hop Limit: 64
  Source Address: 2402:f000:3:1001:4dc6:58a6:d7d6:71fa
  Destination Address: 2402:f000:1:404:166:111:4:100
  ▾ Fragment Header for IPv6
    Next header: ICMPv6 (58)
    Reserved octet: 0x00
    0000 1011 0101 0... = Offset: 362 (2896 bytes)
    .... = Reserved bits: 0
    .... = More Fragments: No
    Identification: 0x641d03aa

```

0 表示后面没有分段。

```

Internet Protocol Version 6, Src: 2402:f000:3:1001:4dc6:58a6:d7d6:71fa, Dst: 2402:f000:1:404:166:111:4:100
  0110 .... = Version: 6
  > .... 0000 0000 .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
  .... 0000 0000 0000 0000 = Flow Label: 0x000000
  Payload Length: 1456
  Next Header: Fragment Header for IPv6 (44)
  Hop Limit: 64
  Source Address: 2402:f000:3:1001:4dc6:58a6:d7d6:71fa
  Destination Address: 2402:f000:1:404:166:111:4:100
  ▾ Fragment Header for IPv6
    Next header: ICMPv6 (58)
    Reserved octet: 0x00
    0000 0000 0000 0... = Offset: 0 (0 bytes)
    .... = Reserved bits: 0
    .... = More Fragments: Yes
    Identification: 0x641d03aa

```

3. 观察 ping 每次发出的若干 IP 分组的分片扩展头中的偏移量 (Offset)，它们从小到大依次为多少？确认这样能够确保在分片乱序到达时，相应网络节点也能正确地重组出原来的分组。

1、2、3 偏移量分别为:0, 181,362。分别表示当前分片相对于用户数据起点的位置。

```

Internet Protocol Version 6, Src: 2402:f000:3:1001:4dc6:58a6:d7d6:71fa, Dst: 2402:f000:1:404:166:111:4:100
  0110 .... = Version: 6
  > .... 0000 0000 .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
  .... 0000 0000 0000 0000 = Flow Label: 0x000000
  Payload Length: 1456
  Next Header: Fragment Header for IPv6 (44)
  Hop Limit: 64
  Source Address: 2402:f000:3:1001:4dc6:58a6:d7d6:71fa
  Destination Address: 2402:f000:1:404:166:111:4:100
  ▾ Fragment Header for IPv6
    Next header: ICMPv6 (58)
    Reserved octet: 0x00
    0000 0101 1010 1... = Offset: 181 (1448 bytes)
    .... = Reserved bits: 0
    .... = More Fragments: Yes
    Identification: 0x641d03ac

```

4. 观察 ping 应答分组，其情况应当与 ping 请求分组类似。
确实。

2.1.3 思考题

1. 观察 traceroute 程序发送的一系列分组中的 Hop Limit 字段，它们有何特点？
特点为从 1 开始，每次发 3 个，而且如果没有回复，则 +1。

964 57.978478	2402:FFFF:2::001:9cA5, 2402:FFFF:1:404:168:1::ICMPv6	126 Echo (ping) request id=0x0001, seq=72, hop limit=1 (no response found)
965 57.980833	2402:FFFF:2::001:1592, 2402:FFFF:7:602:167C::ICMPv6	126 Time Exceeded (hop limit exceeded in transit)
966 58.003815	2402:FFFF:2::001:9cA5, 2402:FFFF:1:404:168:1::ICMPv6	126 Echo (ping) request id=0x0001, seq=73, hop limit=1 (no response found)
967 58.044400	2402:FFFF:2::001:1592, 2402:FFFF:2:000:9cA5::ICMPv6	126 Time Exceeded (hop limit exceeded in transit)
968 58.046915	2402:FFFF:2::001:9cA5, 2402:FFFF:1:404:168:1::ICMPv6	126 Echo (ping) request id=0x0001, seq=74, hop limit=1 (no response found)
969 58.056015	2402:FFFF:2::001:1592, 2402:FFFF:2:000:9cA5::ICMPv6	126 Time Exceeded (hop limit exceeded in transit)
970 59.059708	2402:FFFF:2::001:9cA5, 2402:FFFF:1:404:168:1::ICMPv6	126 Echo (ping) request id=0x0001, seq=75, hop limit=2 (no response found)
992 62.784188	2402:FFFF:2::001:9cA5, 2402:FFFF:1:404:168:1::ICMPv6	126 Echo (ping) request id=0x0001, seq=76, hop limit=2 (no response found)
1034 66.787037	2402:FFFF:2::001:9cA5, 2402:FFFF:1:404:168:1::ICMPv6	126 Echo (ping) request id=0x0001, seq=77, hop limit=2 (no response found)
1063 70.784349	2402:FFFF:2::001:9cA5, 2402:FFFF:1:404:168:1::ICMPv6	126 Echo (ping) request id=0x0001, seq=78, hop limit=2 (no response found)
1064 70.795846	2402:FFFF:0:24C::78, 2402:FFFF:2:001:9cA5::ICMPv6	126 Time Exceeded (hop limit exceeded in transit)
1065 70.797927	2402:FFFF:2::001:9cA5, 2402:FFFF:1:404:168:1::ICMPv6	126 Echo (ping) request id=0x0001, seq=79, hop limit=3 (no response found)
1066 70.800806	2402:FFFF:0:24C::78, 2402:FFFF:7:602:167C::ICMPv6	126 Time Exceeded (hop limit exceeded in transit)
1067 70.802709	2402:FFFF:2::001:9cA5, 2402:FFFF:1:404:168:1::ICMPv6	126 Echo (ping) request id=0x0001, seq=80, hop limit=3 (no response found)
1068 70.805193	2402:FFFF:0:24C::78, 2402:FFFF:2:001:9cA5::ICMPv6	126 Time Exceeded (hop limit exceeded in transit)
1069 71.818898	2402:FFFF:2::001:9cA5, 2402:FFFF:1:404:168:1::ICMPv6	126 Echo (ping) request id=0x0001, seq=81, hop limit=4 (no response found)

2. ICMP、TCP、UDP 以及分片扩展头对应的 Next Header 值分别是多少? (请回答四个十进制整数)

UDP 如下图, ICMP、TCP 见 2.1.2 中的 2。

```
Internet Protocol Version 6, Src: fe80::5d0b:20d5:8175:753, Dst: ::02::fb
0110 .... = Version: 6
> .... 0000 0000 .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
.... 0001 1010 0110 1101 = Flow Label: 0x1a67d
Payload Length: 141
Next Header: UDP (17)
Hop Limit: 1
```

3. 分片扩展头 (若有) 在一个 IP 分组的什么位置, 即从第几个字节开始到第几个字节结束? 不带有和带有分片扩展头时, 上层协议的有效载荷 (payload) 分别从第几个字节开始? (请回答四个十进制整数, 从 0 开始数)

40 开始到 47 字节结束。

不带时, 从 40 开始。

带时, 从 48 开始。

4. 什么情况下 IP 分组需要分片? 在哪里分片? 口是在哪里重新组装起来的?

未分片数据包加 40 超过 MTU 时进行分片。在发送主机的网络层分片, 在目标主机的网络层组装。

5. 阅读 RFC8200: Internet Protocol, Version 6 (IPv6) Specification, 了解 IPv6 定义的扩展头 (Extension Header) 除了分片扩展头还有哪些, Next Header 值以及功能分别如何, 列举两个。

- Hop-by-Hop Options Header: Next Header=0; 功能是携带可能会在一个包转发路径上被每一个结点获得并处理的拓展信息。
- Routing Header: Next Header=43; 功能是由 IPv6 发送端指定一个或多个在转发到目标地址时需要经过了中间节点。

2.2 ICMP 协议

2.2.1 观察 ICMP 回显请求及回显应答

1. 观察 ICMP 回显请求及回显应答, 请确认 ICMP 消息的各个字段与标准是否一致。
一致。

- 一致。

```

Next Header: ICMPv6 (58)
Hop Limit: 64
Source Address: 2402:f000:2:c001:9ca5:cfdf:1:3ccb:5b92
Destination Address: 2402:f000:1:404:166:111:4:100
  Internet Control Message Protocol v6
    Type: Echo (ping) request (128)
    Code: 0
    Checksum: 0xe023 [correct]
    [Checksum Status: Good]
    Identifier: 0x0001
    Sequence: 118
    \[Response In: 2867\]
  Data (32 bytes)
    Data: 6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869

```

1. 观察捕捉到的 ICMP 目标不可达消息的各个字段。Type、Code 以及 Checksum 字段是否和标准一致？Unused 及其后面的内容是否正确？

一致，正确。

```

v Internet Protocol Version 6, Src: 2402:f000:1:400::2, Dst: 2402:f000:2:c001:9ca5:cfdd:3ccb:5b92
  0110 .... = Version: 6
  > .... 0000 0000 .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
  .... 0010 1110 0011 0101 0110 = Flow Label: 0x2e356
  Payload Length: 101
  Next Header: ICMPv6 (58)
  Hop Limit: 58
  Source Address: 2402:f000:1:400::2
  Destination Address: 2402:f000:2:c001:9ca5:cfdd:3ccb:5b92
v Internet Control Message Protocol v6
  Type: Destination Unreachable (1)
  Code: 4 (Port unreachable)
  Checksum: 0xc570 [correct]
  [Checksum Status: Good]

```

1. 发现命令行中显示的信息为“From ... icmp_seq=1 Time exceeded: Hop limit”（或“来自... 的回复: TTL 传输中过期。”）。这表示什么含义？这次 ping 操作是否成功获得对方主机的应答？

7

2. 捕捉的分组显示实验者主机收到了 ICMP 超时消息，请确认 ICMP 消息的各个字段与标准是否一致。

一致。

```
0110 .... = Version: 6
> .... 0000 0000 .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
.... 0000 0000 0000 0000 = Flow Label: 0x00000
Payload Length: 88
Next Header: ICMPv6 (58)
Hop Limit: 62
Source Address: 2402:f000:0:24c::78
Destination Address: 2402:f000:2:c001:9ca5:cf1:3ccb:5b92
v Internet Control Message Protocol v6
  Type: Time Exceeded (3)
  Code: 0 (hop limit exceeded in transit)
  Checksum: 0x7303 [correct]
  [Checksum Status: Good]
```

2.2.4 思考题

1. 前文观察的 ICMP 目标不可达消息的 Code 字段值为多少，代表什么含义？
4，端口不可达。
2. 前文观察的 ICMP 目标不可达消息以及超时消息的 Unused 字段之后的数据是什么内容？
最后一个接受到请求报文的路由器收到的 IPv6 Packet。
3. 前文观察的 ICMP 目标不可达消息以及超时消息分别由谁发送？
最后一个接受到请求报文的路由器。
4. 为什么有些类型的 ICMP 消息（例如目标不可达消息）中有一个 Unused 字段，而另一些（例如回显消息）则没有？注意它们的□度，分析这样设计可能是出于什么考虑。
可能是出于如下考虑：Unused 字段为了使得将 ICMP 报头补齐为 8 个字节，使按照 8 字节对齐、ICMP 报头格式一致。

2.3 ND 协议

2.3.1 观察地址解析（Address Resolution）过程及 ND 报文格式

1. Neighbor Solicitation 以及 Neighbor Advertisement 的 IP 分组头部、报文格式、内容以及携带的选项有何异同？所述选项包括源或目标链路层地址（Source/Target Link-Layer Address）等。
 - 相同：
Target Address、IPv6 报文头部格式、除源和目标地址外内容相同。
 - 不同：
NS 包括实验主机的 MAC 地址，ND 包括路由器的 MAC 地址，NS、ND 字段不同。


```

[Source SA MAC: HuaweiTe_b9:7f:03 (90:03:25:b9:7f:03)]
v Internet Control Message Protocol v6
  Type: Router Advertisement (134)
  Code: 0
  Checksum: 0x11fd [correct]
  [Checksum Status: Good]
  Cur hop limit: 64
  > Flags: 0x00, Prf (Default Router Preference): Medium
  Router lifetime (s): 1800
  Reachable time (ms): 0
  Retrans timer (ms): 0
  > ICMPv6 Option (Source link-layer address : 90:03:25:b9:7f:03)
  > ICMPv6 Option (MTU : 1500)
  > ICMPv6 Option (Prefix information : 2402:f000:2:c001::/64)

0110 .... = Version: 6
> .... 0000 0000 .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
.... 0000 0000 0000 0000 0000 = Flow Label: 0x000000
Payload Length: 24
Next Header: ICMPv6 (58)
Hop Limit: 255
Source Address: ::
Destination Address: ff02::1:ff75:753
v Internet Control Message Protocol v6
  Type: Neighbor Solicitation (135)
  Code: 0
  Checksum: 0x9830 [correct]
  [Checksum Status: Good]
  Reserved: 00000000
  Target Address: 2402:f000:2:c001:5d0b:20d5:8175:753

```

2. 这一次的 Neighbor Solicitation 以及 Neighbor Advertisement 的 IP 分组头部、报文格式、内容以及携带的选项与上文的有何异同？

NS 报文的 Destination Address 地址变成通过原来路由表中的路由的 IPv6 地址，源地址也从临时 IPv6 地址变为了 IPv6 地址。

ND 报文的目标地址也从临时 IPv6 地址成为了实验主机的 IPv6 地址，其它内容都是相同的。

```

v Internet Protocol Version 6, Src: 2402:f000:3:1001:4dc6:58a6:d7d6:71fa, Dst: ff02::1:ff37:8802
  0110 .... = Version: 6
  > .... 0000 0000 .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
  .... 0000 0000 0000 0000 0000 = Flow Label: 0x000000
  Payload Length: 32
  Next Header: ICMPv6 (58)
  Hop Limit: 255
  Source Address: 2402:f000:3:1001:4dc6:58a6:d7d6:71fa
  Destination Address: ff02::1:ff37:8802
v Internet Control Message Protocol v6
  Type: Neighbor Solicitation (135)
  Code: 0
  Checksum: 0x6684 [correct]
  [Checksum Status: Good]
  Reserved: 00000000
  Target Address: 2402:f000:2:c001:5d0b:20d5:8175:753

```

```

  ▾ Internet Protocol Version 6, Src: fe80::9629:2fff:fe37:8802, Dst: 2402:f000:3:1001:4dc6:58a6:d7d6:71fa
    0110 .... = Version: 6
    > .... 1110 0000 .... = Traffic Class: 0xe0 (DSCP: CS7, ECN: Not-ECT)
      .... 0000 0000 0000 0000 = Flow Label: 0x00000
    Payload Length: 32
    Next Header: ICMPv6 (58)
    Hop Limit: 255
    Source Address: fe80::9629:2fff:fe37:8802
    Destination Address: 2402:f000:3:1001:4dc6:58a6:d7d6:71fa
    [Source SA MAC: NewH3CTe_37:88:02 (94:29:2f:37:88:02)]
  ▾ Internet Control Message Protocol v6
    Type: Neighbor Advertisement (136)
    Code: 0
    Checksum: 0xa032 [correct]
    [Checksum Status: Good]
    > Flags: 0xe0000000, Router, Solicited, Override

```

2.3.2 观察 Router Advertisement 以及 DAD

1. 观察 Router Advertisement 报文中含有的信息及选项，包括标志位、生存时间以及前缀信息等。应当可以确认实验者主机获得的 IP 地址（可以使用 ip addr 命令查看）是该前缀内的。在前缀内。
2. 观察并分析该 Neighbor Solicitation 的目标地址（Target Address）是什么含义。
Target Address 为关闭接口前实验主机的 IPv6 地址。

```

  ▾ Internet Protocol Version 6, Src: fe80::9629:2fff:fe37:8802, Dst: fe80::5d0b:20d5:8175:753
    0110 .... = Version: 6
    > .... 1110 0000 .... = Traffic Class: 0xe0 (DSCP: CS7, ECN: Not-ECT)
      .... 0000 0000 0000 0000 = Flow Label: 0x00000
    Payload Length: 32
    Next Header: ICMPv6 (58)
    Hop Limit: 255
    Source Address: fe80::9629:2fff:fe37:8802
    Destination Address: fe80::5d0b:20d5:8175:753
    [Source SA MAC: NewH3CTe_37:88:02 (94:29:2f:37:88:02)]
  ▾ Internet Control Message Protocol v6
    Type: Neighbor Advertisement (136)
    Code: 0
    Checksum: 0xaf4d [correct]

```

3. 观察该 Neighbor Solicitation 是否带有源或目标链路层地址（Source/Target Link-Layer Address）选项，思考其原因。

不带。原因可能是因为：即使发送源或目标链路层地址也不能使接受这条报文的人将 IP 地址和 MAC 地址进行映射。这时候发送是没有意义的。

2.3.3 思考题

1. 查阅相关文献，在实验者所使用的系统中，哪一个选项控制邻居缓存表项状态由 REACHABLE 变为 STALE 的超时时间（ReachableTime）？
windows 系统，BaseReachable Time 控制。
2. 前文观察的源地址不为未指定地址的组播 Neighbor Solicitation 会带有源链路层地址（Source Link-Layer Address）选项，对应的 Neighbor Advertisement 也会带有目标链路层地址（Tar-

get Link-Layer Address) 选项。然而, 前文观察的单播 Neighbor Solicitation 及其对应的 Neighbor Advertisement 有时可能不带这样的选项 (与实验环境有关), 这是为什么?

源链路层用于已编址的链路层, 如果 IPv6 头的源地址未指定, 则不能将其包括在哪。

NA 是同理的。

3. Router Advertisement 报文中的 M (Managed address configuration) 标志以及 O (Other configuration) 标志分别是什么含义?

- M: 管理地址标志位。
0: 无状态地址分配;1: 有状态地址分配。
- O: 其他状态标志位。
0: 客户端通过无状态获取除地址外的其他配置信息;1: 客户端通过有状态获取其他配置信息。

4. 前文观察的源地址为未指定地址的组播 Neighbor Solicitation 是否有对应的 Neighbor Advertisement? 这说明了什么问题?

没有。说明 IP 地址在链路上是唯一的, IP 地址未被其他主机占用, 配置生效。