


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

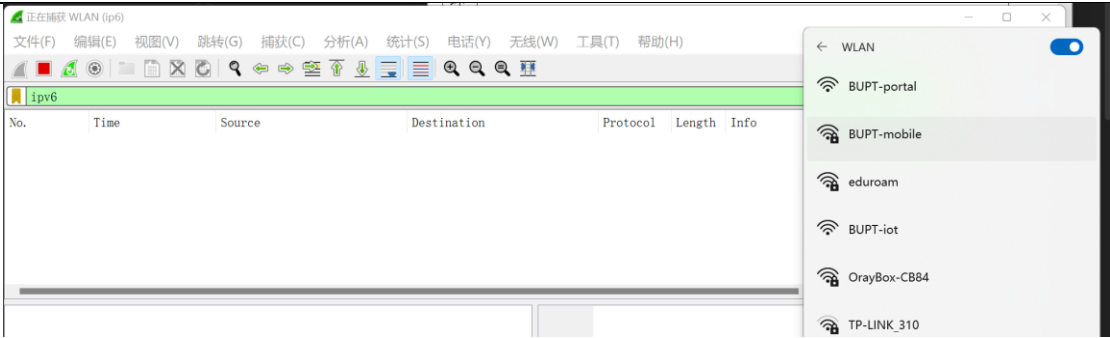
姓名： 陈朴炎
学号： 2021211138
班级： 2021211307

2024 年 6 月

实验报告

实验名称	IPv6 地址无状态自动配置实验		
实验目的	理解 IPv6 地址无状态自动配置的过程及原理		
实 验 完 成 人	陈朴炎	完成时间	2024.6.2
实验环境	<p>画出实验环境示意图，如下，一台本地 PC，以及路由器（忽略 ip 地址）</p>  <p>R1(config)# ipv6 unicast-routing</p> <p>2001:db8:cafe:1::/64 GUA ::1</p> <p>G0/0 LLA fe80::1</p> <p>WinPC LLA fe80::d0f8:9ff6:4201:7086</p>		

实验步骤与结果分析



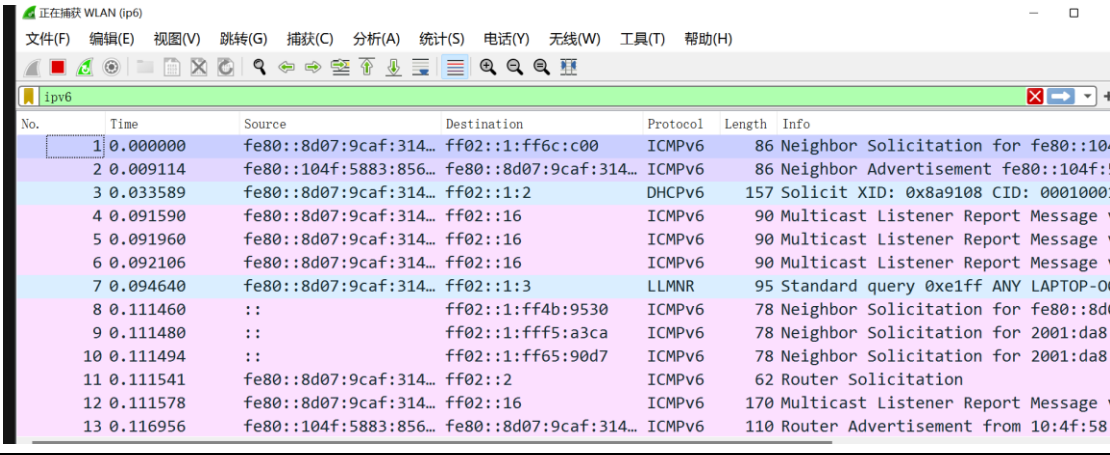
开启 wifi 且不连接到网络，ipconfig 如下：

无线网络适配器 WLAN：

媒体状态 : 媒体已断开连接

连接特定的 DNS 后缀 :

之后连接到校园网，可以看到一下子捕获了很多 ipv6 的报文：



使用 ipconfig 查看是否已经获取到了 ipv6 地址，如下，为
2001:da8:215:3c0a:e420:3f1b:48f5:a3ca:

无线局域网适配器 WLAN:

```
连接特定的 DNS 后缀 . . . . . :  
IPv6 地址 . . . . . : 2001:da8:215:3c0a:e420:3f1b:48f5:a3ca  
临时 IPv6 地址 . . . . . : 2001:da8:215:3c0a:713f:6b1b:2465:90d7  
本地链接 IPv6 地址 . . . . . : fe80::8d07:9caf:314b:9530%3  
IPv4 地址 . . . . . : 10.129.25.134  
子网掩码 . . . . . : 255.255.0.0  
默认网关 . . . . . : fe80::104f:5883:856c:c00%3  
10.129.0.1
```

关闭 wireshark 抓包，下面进行无状态 IPv6 地址分配过程解析和报文解析

IPv6 地址= 前缀+ 接口标识

前缀：相当于 v4 地址中的网络 ID

接口标识：相当于 v4 地址中的主机 ID

1. RS 请求报文

为配置接口，主机需要前缀信息，因此，它会发送一条路由请求 RS 消息。该消息以组播的方式发送给所有路由器。所有的路由器组播地址为 ff02::2，所以，我们需要在一开始找到目的地址为 ff02::2 的报文进行解析（或者在过滤器中输入 icmpv6.type == 133）。如下所示

No.	Time	Source	Destination	Protocol	Length	Info
7	0.094640	fe80::8d07:9caf:314...	ff02::1:3	LLMNR	95	Standard qu
8	0.111460	::	ff02::1:ff4b:9530	ICMPv6	78	Neighbor So
9	0.111480	::	ff02::1:fff5:a3ca	ICMPv6	78	Neighbor So
10	0.111494	::	ff02::1:ff65:90d7	ICMPv6	78	Neighbor So
11	0.111541	fe80::8d07:9caf:314...	ff02::2	ICMPv6	62	Router Soli
12	0.111578	fe80::8d07:9caf:314...	ff02::16	ICMPv6	170	Multicast L
13	0.116956	fe80::104f:5883:856...	fe80::8d07:9caf:314...	ICMPv6	110	Router Adver
14	0.310521	fe80::8d07:9caf:314...	ff02::1:ff6c:c00	ICMPv6	86	Neighbor So

```
> Frame 11: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on  
> Ethernet II, Src: LiteonTe_b2:cd:3f (74:4c:a1:b2:cd:3f), Dst: IPv6mcast  
v Internet Protocol Version 6, Src: fe80::8d07:9caf:314b:9530, Dst: ff02::  
  0110 .... = Version: 6  
  > .... 0000 0000 .... = Traffic Class: 0x00 (DSCP:  
    .... 0000 0000 0000 0000 0000 = Flow Label: 0x000000  
    Payload Length: 8  
    Next Header: ICMPv6 (58)  
    Hop Limit: 255  
    Source Address: fe80::8d07:9caf:314b:9530  
    Destination Address: ff02::2
```

从这个 IPv6 的报文里来看，它的源地址为 fe80::8d07:9caf:314b:9530，目的地址为 ff02::2，源地址刚好就是我们在命令行中 ipconfig 里的本地链接 IPv6 地址。因为 RS 报文是从终端设备发送给路由器的请求消息，所以这个报文的源地址就是链路本地地址，而目的地址则是所有路由器的组播地址。下面再看这个报文的

其他信息:

```
> Frame 11: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on
> Ethernet II, Src: LiteonTe_b2:cd:3f (74:4c:a1:b2:cd:3f), Dst: IPv6mcast
> Internet Protocol Version 6, Src: fe80::8d07:9caf:314b:9530, Dst: ff02::c
> Internet Control Message Protocol v6
  Type: Router Solicitation (133)
  Code: 0
  Checksum: 0x8d04 [correct]
  [Checksum Status: Good]
  Reserved: 00000000
```

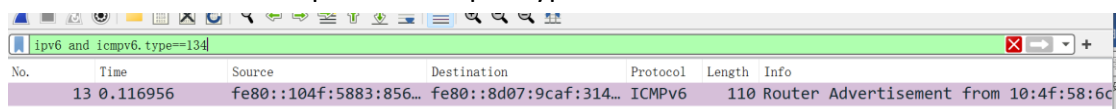
从这个 ICMP 报文中, 可以看出, 这个报文的类型是 Router Solicitation, 因为 RS 报文的类型就是 133。

2. 路由器 RA 回应报文

网络中的路由器接收到 RS 消息后, 或定期发送路由器通告 (Router Advertisement, RA) 消息, 向网络中的所有设备通告网络前缀信息。RA 消息包含多个信息选项, 包括前缀信息选项, 其中包含网络前缀和有效期。还可能包括默认网关信息、MTU 信息等。

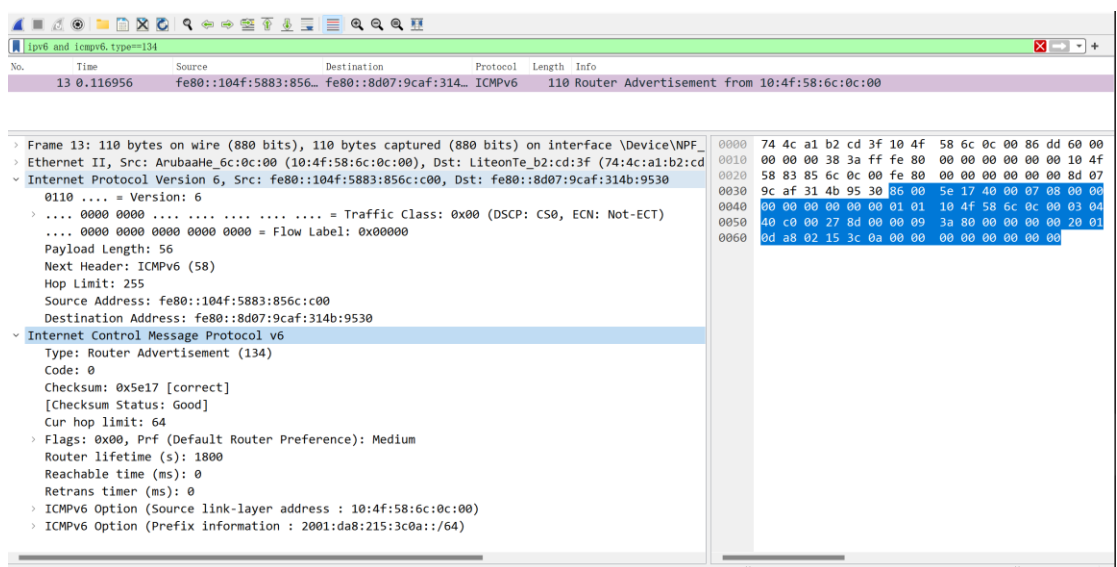
现在我们来一起看看 RA 报文:

在过滤器中输入 `ipv6 and icmpv6.type==134`, 得到如下报文



No.	Time	Source	Destination	Protocol	Length	Info
13	0.116956	fe80::104f:5883:856c:c00	fe80::8d07:9caf:314b:9530	ICMPv6	110	Router Advertisement from 10:4f:58:6c:0c:00

可以看到, 该报文的地址就是我们本机的本地连接地址。



Packet 13 details:

- Frame 13: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface \Device\NPF_{...}
- Ethernet II, Src: ArubaaHe_6c:0c:00 (10:4f:58:6c:0c:00), Dst: LiteonTe_b2:cd:3f (74:4c:a1:b2:cd:3f)
- Internet Protocol Version 6, Src: fe80::104f:5883:856c:c00, Dst: fe80::8d07:9caf:314b:9530
- 0110 = Version: 6
- 0000 0000 = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
- 0000 0000 0000 0000 = Flow Label: 0x000000
- Payload Length: 56
- Next Header: ICMPv6 (58)
- Hop Limit: 255
- Source Address: fe80::104f:5883:856c:c00
- Destination Address: fe80::8d07:9caf:314b:9530
- Internet Control Message Protocol v6
 - Type: Router Advertisement (134)
 - Code: 0
 - Checksum: 0x5e17 [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 : 10:4f:58:6c:0c:00)
 - ICMPv6 Option (Prefix information : 2001:da8:215:3c0a::/64)

Hex view (offset 0000):

```
74 4c a1 b2 cd 3f 10 4f 58 6c 0c 00 86 dd 60 00
00 00 00 38 3a ff fe 80 00 00 00 00 00 10 4f
58 83 85 6c 0c 00 fe 80 00 00 00 00 00 8d 07
9c af 31 4b 95 30 86 00 5e 17 40 00 07 08 00 00
00 00 00 00 00 00 01 01 10 4f 58 6c 0c 00 03 04
40 c0 00 27 8d 00 00 09 3a 80 00 00 00 20 01
0d a8 02 15 3c 0a 00 00 00 00 00 00 00 00 00
```

点开看详细信息, 如上图所示。可以看到, 在 ICMPv6 报文中, 这个报文的 Type 值为 134, 表示这个是 Router Advertisement RA 报文。

```

Link-layer address: ArubaaHe_6c:0c:00 (10:4f:58:6c:0c:00)
  ▾ ICMPv6 Option (Prefix information : 2001:da8:215:3c0a::/64)
    Type: Prefix information (3)
    Length: 4 (32 bytes)
    Prefix Length: 64
    ▸ Flag: 0xc0, On-link flag(L), Autonomous address-configuration flag(A)
    Valid Lifetime: 2592000
    Preferred Lifetime: 604800
    Reserved
    Prefix: 2001:da8:215:3c0a::

```

在报文选项中，可以查看到这个网络的前缀信息：

2001:da8:215:3c0a::/64，表示前缀信息选项，包括：

Prefix: 2001:da8:215:3c0a::，表示网络前缀。

Prefix Length: 64，表示前缀长度为 64 位。

```

Retrans timer (ms): 0
  ▾ ICMPv6 Option (Source link-layer address : 10:4f:58:6c:0c:00)
    Type: Source link-layer address (1)
    Length: 1 (8 bytes)
    Link-layer address: ArubaaHe_6c:0c:00 (10:4f:58:6c:0c:00)

```

而这个 ICMPv6 报文选项则告诉了我们路由器的源链路地址 10:4f:58:6c:0c:00。

3. Neighbor Solicitation NS 消息

在设备生成链路本地地址后，会发送一个邻居请求(Neighbor Solicitation, NS)消息来执行重复地址检测(DAD)，以确保该地址在本地链路中是唯一的。

WLAN (pp)

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(V) 无线(W) 工具(T) 帮助(H)

ipv6 and icmpv6.type==135

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	fe80::8d07:9caf:314...	ff02::1:ff6c:c00	ICMPv6	86	Neighbor Solicitation for fe80::104f:5883:856c:c00 from 74:4c:a1:b2:cd:3f
8	0.111460	::	ff02::1:ff4b:9530	ICMPv6	78	Neighbor Solicitation for fe80::8d07:9caf:314b:9530
9	0.111480	::	ff02::1:fff5:a3ca	ICMPv6	78	Neighbor Solicitation for 2001:da8:215:3c0a:e420:3f1b:48f5:a3ca
10	0.111494	::	ff02::1:fff5:90d7	ICMPv6	78	Neighbor Solicitation for 2001:da8:215:3c0a:713f:6b1b:2465:90d7
14	0.310521	fe80::8d07:9caf:314...	ff02::1:ff6c:c00	ICMPv6	86	Neighbor Solicitation for fe80::104f:5883:856c:c00 from 74:4c:a1:b2:cd:3f

我们使用过滤条件：ipv6 and icmpv6.type==135

可以看到，在我们刚连上网时，第一条捕获到的报文就是 NS 报文，这条报文的源地址为我们的本地链路地址。这是因为当设备启动并连接到网络时，首先生成一个链路本地地址。这通常通过将设备的 MAC 地址转换为 EUI-64 格式，然后将其嵌入到前缀 FE80::/10 中生成。

```

> Frame 1: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface \Device\NPF_{00...
> Ethernet II, Src: LiteonTe_b2:cd:3f (74:4c:a1:b2:cd:3f), Dst: IPv6mcast_ff:6c:0c:00 (33:33:ff:6...
> Internet Protocol Version 6, Src: fe80::8d07:9caf:314b:9530, Dst: ff02::1:ff6c:c00
  ▾ Internet Control Message Protocol v6
    Type: Neighbor Solicitation (135)
    Code: 0
    Checksum: 0xa280 [correct]
    [Checksum Status: Good]
    Reserved: 00000000
    Target Address: fe80::104f:5883:856c:c00
    ▾ ICMPv6 Option (Source link-layer address : 74:4c:a1:b2:cd:3f)
      Type: Source link-layer address (1)
      Length: 1 (8 bytes)
      Link-layer address: LiteonTe_b2:cd:3f (74:4c:a1:b2:cd:3f)

```

NS 报文中，ICMPv6 类型值为 135，code 通常为 0（表示未使用），reserved 字段通常为 0。target 地址为本地的链接地址，从上图可以看出这正是我们本地的链路地址。目标地址为 ff02::1:ffxx:xxxx，这表示链路本地范围内的多播地址。因为在生成本地链接地址之后，需要重复地址检测来确保这个地址能唯一标识这个网卡。

我们看到，第 8、9、10 这三个包的源地址都为::，这表示未指定地址，::在 IPv6 中表示未指定地址，它等价于全零地址（0:0:0:0:0:0:0:0 或缩写为::）。在重复地址检测（DAD）过程中，设备正在检查某个地址是否唯一，因此它不能使用该地址作为源地址。此时，设备会使用未指定地址作为 NS 包的源地址。在这个过程中，设备会发送一个 NS 消息，目标地址是新生成的地址，对应的多播地址是 ff02::1:ffxx:xxxx。

4. NA Neighbor Advertisement 消息

NA 消息用来响应邻居请求，当设备接收到 NS 消息后，如果目标地址匹配自身地址，它会发送 NA 消息进行响应。NA 消息用来重复地址检测（DAD），当设备检测到其他设备在使用相同的地址时，发送 NA 消息通知地址冲突。NA 消息还用来主动通告，设备主动发送 NA 消息来更新或通知其他设备关于地址、链路层地址或状态的变化。

在 Wireshark 中，我们输入过滤条件 `ipv6 and icmpv6.type==136` 来查看 NA 消息。

No.	Time	Source	Destination	Protocol	Length	Info
2	0.009114	fe80::104f:5883:856c:...	fe80::8d07:9caf:314...	ICMPv6	86	Neighbor Advertisement fe80::104f:5883:856c:c00 (rtr, sol, ovr) is at 10:4...
15	0.321275	fe80::104f:5883:856c:...	fe80::8d07:9caf:314...	ICMPv6	86	Neighbor Advertisement fe80::104f:5883:856c:c00 (rtr, sol, ovr) is at 10:4...
28	1.115893	fe80::8d07:9caf:314...	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::8d07:9caf:314b:9530 (ovr) is at 74:4c:a1:b2:c...
29	1.115910	2001:da8:215:3c0a:e...	ff02::1	ICMPv6	86	Neighbor Advertisement 2001:da8:215:3c0a:e420:3f1b:48f5:a3ca (ovr) is at 7...
30	1.115920	2001:da8:215:3c0a:7...	ff02::1	ICMPv6	86	Neighbor Advertisement 2001:da8:215:3c0a:713f:6b1b:2465:90d7 (ovr) is at 7...

从这些报文来看，No.2 的报文是用来回应第一次发送的 NS 请求报文

No.15 是回应的最后一个从主机发出来的 NS 请求报文。

而 No.28 的，源地址为本地链接地址，No.29 的源地址为 PC 的 IPv6 地址，No.30 的源地址为 PC 的临时 IPv6 地址。

如何从报文来看我们的设备链路地址是否有重复呢？

我们检查 NS 消息对应的 NA 报文，并且 NS 消息的源地址是::，目标地址是设备生成的链路本地地址。

在发送 NS 消息后，设备等待一定时间，通常是 1 秒钟。

捕获并分析网络上的 NA 消息，如果在等待时间内收到针对目标地址的 NA 消息，表示该地址已经在网络中被使用，即地址重复。

如果未收到 NA 消息，则表示该地址在网络中是唯一的，可以使用。

很明显，从结果来看，我们中间的两个 NS 报文都没有收到对应的回复，所以可以肯定的是这个链接地址是唯一的。

现在我们一起看 No.2 的 NA 报文：

ipv6 and icmpv6.type==136						
No.	Time	Source	Destination	Protocol	Length	Info
2	0.009114	fe80::104f:5883:856c:c00	fe80::8d07:9caf:314b:9530	ICMPv6	86	Neighbor Advertisement fe80::104f:5883:856c:c00
15	0.321275	fe80::104f:5883:856c:c00	fe80::8d07:9caf:314b:9530	ICMPv6	86	Neighbor Advertisement fe80::104f:5883:856c:c00
28	1.115893	fe80::8d07:9caf:314b:9530	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::8d07:9caf:314b:9530
29	1.115910	2001:da8:215:3c0a:e420:3f1b:48f5:a3ca	ff02::1	ICMPv6	86	Neighbor Advertisement 2001:da8:215:3c0a:e420:3f1b:48f5:a3ca
30	1.115920	2001:da8:215:3c0a:713f:6b1b:2465:90d7	ff02::1	ICMPv6	86	Neighbor Advertisement 2001:da8:215:3c0a:713f:6b1b:2465:90d7

Internet Protocol Version 6, Src: fe80::104f:5883:856c:c00, Dst: fe80::8d07:9caf:314b:9530		0000	74 4c a1 b2 cd 3f
0110 = Version: 6		0010	00 00 00 20 3a ff
> 0000 0000 = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)		0020	58 83 85 6c 0c 00
.... 0000 0000 0000 0000 = Flow Label: 0x000000		0030	9c af 31 4b 95 30
Payload Length: 32		0040	00 00 00 00 00 00
Next Header: ICMPv6 (58)		0050	10 4f 58 6c 0c 00
Hop Limit: 255			
Source Address: fe80::104f:5883:856c:c00			
Destination Address: fe80::8d07:9caf:314b:9530			
Internet Control Message Protocol v6			
Type: Neighbor Advertisement (136)			
Code: 0			
Checksum: 0x40b4 [correct]			
[Checksum Status: Good]			
> Flags: 0xe0000000, Router, Solicited, Override			
Target Address: fe80::104f:5883:856c:c00			
ICMPv6 Option (Target link-layer address : 10:4f:58:6c:0c:00)			
Type: Target link-layer address (2)			
Length: 1 (8 bytes)			
Link-layer address: ArubaHe_6c:0c:00 (10:4f:58:6c:0c:00)			

这个邻居通告（NA）报文的关键信息如下：

源地址：fe80::104f:5883:856c:c00，这是发送 NA 消息的设备的链路本地地址。

目的地址：fe80::8d07:9caf:314b:9530，这是接收 NA 消息的设备的链路本地地址。

目标地址：fe80::104f:5883:856c:c00，这是发送 NA 消息的设备的链路本地地址。

Router flag (R): 1，表示发送设备是一个路由器。

Solicited flag (S): 1，表示这是对邻居请求（NS）消息的响应。

Override flag (O): 1，表示该消息应覆盖任何现有的缓存条目。

链路层地址：10:4f:58:6c:0c:00，这是发送设备的 MAC 地址。

这个 NA 消息是对邻居请求（NS）消息的响应，确认了源设备（路由器）的链路本地地址和 MAC 地址，同时通过设置标志位表示该信息应覆盖现有的缓存条目。

下面我们来看 No.28 的这个报文，它的目的地址为 ff02::1。

15	0.321275	fe80::104f:5883:856c:c00	fe80::8d07:9caf:314b:9530	ICMPv6	86	Neighbor Advertisement fe80::104f:5883:856c:c00 (rtr, sol, ovr) is at 10:4f:58:6c:0c:00
28	1.115893	fe80::8d07:9caf:314b:9530	ff02::1	ICMPv6	86	Neighbor Advertisement fe80::8d07:9caf:314b:9530 (ovr) is at 74:4c:a1:b2:cd:3f
29	1.115910	2001:da8:215:3c0a:e420:3f1b:48f5:a3ca	ff02::1	ICMPv6	86	Neighbor Advertisement 2001:da8:215:3c0a:e420:3f1b:48f5:a3ca (ovr) is at 74:4c:a1:b2:cd:3f
30	1.115920	2001:da8:215:3c0a:713f:6b1b:2465:90d7	ff02::1	ICMPv6	86	Neighbor Advertisement 2001:da8:215:3c0a:713f:6b1b:2465:90d7 (ovr) is at 74:4c:a1:b2:cd:3f

Internet Protocol Version 6, Src: fe80::8d07:9caf:314b:9530, Dst: ff02::1		0000	33 33 00 00 00 01 74 4c a1 b2 cd 3f 86 dd 60 00
0110 = Version: 6		0010	00 00 00 20 3a ff fe 80 00 00 00 00 00 8d 07
> 0000 0000 = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)		0020	9c af 31 4b 95 30 ff 02 00 00 00 00 00 00 00
.... 0000 0000 0000 0000 = Flow Label: 0x000000		0030	00 00 00 00 00 01 88 00 95 f9 20 00 00 00 fe 80
Payload Length: 32		0040	00 00 00 00 00 00 8d 07 9c af 31 4b 95 30 02 01
Next Header: ICMPv6 (58)		0050	74 4c a1 b2 cd 3f
Hop Limit: 255			
Source Address: fe80::8d07:9caf:314b:9530			
Destination Address: ff02::1			
Internet Control Message Protocol v6			
Type: Neighbor Advertisement (136)			
Code: 0			
Checksum: 0x95f9 [correct]			
[Checksum Status: Good]			
> Flags: 0x20000000, Override			
Target Address: fe80::8d07:9caf:314b:9530			
ICMPv6 Option (Target link-layer address : 74:4c:a1:b2:cd:3f)			
Type: Target link-layer address (2)			
Length: 1 (8 bytes)			
Link-layer address: LiteonTe_b2:cd:3f (74:4c:a1:b2:cd:3f)			

这个邻居通告（NA）报文的关键信息如下：

源地址：fe80::8d07:9caf:314b:9530，这是发送 NA 消息的设备的链路本地地址。

<p>目的地址：ff02::1，这是一个 IPv6 多播地址，表示所有节点。</p> <p>目标地址：fe80::8d07:9caf:314b:9530，这是发送 NA 消息的设备的链路本地地址。</p> <p>Override flag (O): 1，表示该消息应覆盖任何现有的缓存条目。</p> <p>链路层地址：74:4c:a1:b2:cd:3f，这是发送设备的 MAC 地址。</p> <p>这个 NA 消息的作用是向网络上的其他设备宣布发送设备的存在，并提供其链路本地地址和对应的链路层地址（MAC 地址）。由于目的地址是 ff02::1，表示该消息是发送给网络上的所有节点，因此它是一个通告，表示发送设备的链路本地地址为 fe80::8d07:9caf:314b:9530，对应的链路层地址为 74:4c:a1:b2:cd:3f。</p> <p>后面还有通告得到 IPv6 地址(No.29)和临时 IPv6 地址(No.30)，这里就不再赘述。</p>
<p>分析与思考</p> <p>通过本次实验，我们详细研究了 IPv6 无状态地址自动配置过程及邻居发现协议的工作机制，理解了 RA、NS 和 NA 消息在其中的关键作用。实验表明，SLAAC 和 ND 协议为设备提供了自动化和高效的 IP 地址配置与管理机制，显著提升了网络配置和管理的自动化程度和可靠性。</p> <p>在实验中，我理解了 IPv6 无状态地址自动配置的过程：当 IPv6 设备首次连接到网络时，它会自动生成一个链路本地地址。接着，设备发送一个邻居发现协议（NDP）的邻居请求 NS 报文，以确认该地址在网络中是唯一的。如果没有收到任何邻居应答 NA 报文，则表明该地址没有冲突，设备可以使用此链路本地地址。随后，设备监听路由器发送的路由通告 RA 报文，从中获取网络前缀和其他配置信息。设备利用这些信息，通过将网络前缀与一个自动生成的接口标识符结合，形成一个全局唯一的 IPv6 地址。同样，设备会发送 NS 报文以检测这个新生成的 IPv6 地址是否存在冲突。若在一定时间内未收到 NA 报文，设备即可确认此地址的唯一性并进行使用，完成无状态地址自动配置过程。</p> <p>同时，我也体会到了 IPv6 无状态地址配置的优势：简化了终端设备的网络配置过程，不需要手动配置 IP 地址，减少了配置错误的可能性。通过 RA 和 NS/NA 消息，设备可以自动化管理 IP 地址的分配和冲突检测，提高了网络管理的效率。</p> <p>而 NDP 协议也非常重要，NS/NA 消息确保了网络中每个 IPv6 地址的唯一性，避免了地址冲突。NA 消息主动通告设备的存在和地址信息，使得网络中的设备能够互相了解彼此的存在，确保通信的正常进行。</p>