

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   | IPv6 地址无状态自动配置实验   |      |            |
| 实验目的   | 通过 Wireshark 抓包，参照 ND 协议和无状态地址自动配置过程，对 IPv6 地址获取过程进行分析，学习 IPv6 地址无状态自动配置的原理。 |      |            |
| 实验完成人  | 鄭毓恒  | 完成时间 | 2023-05-22 |
| 实 验 环境   | Windows 11<br>WireShark 网络分析器  |      |            |
| 实验步骤与结果分析  |  |      |            |
| <p>断开校园网的连接,最好断开的时间长一些，关闭无线网络的自动连接校园网的选项，开启终端的 IPV6 协议，启动 wireshark 抓包软件，选择准备连接校园网的网卡，启动抓包。</p> <p>恢复校园网的连接，在 cmd 命令行模式，用 ipconfig 检查此网卡是否已经获取了 IPV6 地址。从下图可见，已经获取了 IPV6 地址<br/>2001:da8:215:3c0a:74b7:d176:afd9:6d09。</p> <div><pre>无线局域网适配器 WLAN:     连接特定的 DNS 后缀 . . . . . :     IPv6 地址 . . . . . : 2001:da8:215:3c0a:74b7:d176:afd9:6d09     临时 IPv6 地址. . . . . : 2001:da8:215:3c0a:b14d:4874:7a84:bc8     本地链接 IPv6 地址. . . . . : fe80::d307:6639:8dc8:2b4e%21     IPv4 地址 . . . . . : 10.128.241.232     子网掩码 . . . . . : 255.255.128.0     默认网关. . . . . : fe80::104f:5883:856c:c00%21                         10.128.128.1</pre></div> <p>关闭 wireshark 抓包，对抓包的内容进行分析，输入 ipv6 进行筛选，筛选出 ipv6 协议报文。</p> <div></div> |  |      |            |

在获取 IPv6 地址前，主机需要确定本地链接 IPv6 地址 fe80::d307:6639:8dcb:2b4e 是否已被占用，发送 135 Neighbor Solicitation 报文。从下图可见，主机发送的 NS 报文目的地址 Destination Address 是 ff02::1:ffcb:2b4e，是被请求节点的组播地址。目标地址 Target Address 就是要检测是否被占用的地址。后续没有收到相应的 136 Neighbor Advertisement 报文，本地链接 IPv6 地址可用。

```

  ▾ Ethernet II, Src: LiteonTe_6b:ee:8d (e0:0a:f6:6b:ee:8d), Dst: IPv6mcast_ff:cb:2b:4e (33:33:ff:cb:2b:4e)
    > Destination: IPv6mcast_ff:cb:2b:4e (33:33:ff:cb:2b:4e)
    > Source: LiteonTe_6b:ee:8d (e0:0a:f6:6b:ee:8d)
    Type: IPv6 (0x86dd)
  ▾ Internet Protocol Version 6, Src: ::, Dst: ff02::1:ffcb:2b4e
    0110 .... = Version: 6
    > .... 0000 0000 .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... 0000 0000 0000 0000 = Flow Label: 0x000000
    Payload Length: 24
    Next Header: ICMPv6 (58)
    Hop Limit: 255
    Source Address: ::
    Destination Address: ff02::1:ffcb:2b4e
  ▾ Internet Control Message Protocol v6
    Type: Neighbor Solicitation (135)
    Code: 0
    Checksum: 0x5db3 [correct]
    [Checksum Status: Good]
    Reserved: 00000000
    Target Address: fe80::d307:6639:8dcb:2b4e

```

为了获得 IPv6 地址的前缀，主机发送 133 Router Solicitation 报文给路由器，内容如下图。源地址是本地链接 IPv6 地址，而目的地址是 ff02::2，也就是组播节点地址。

```

  ▾ Ethernet II, Src: LiteonTe_6b:ee:8d (e0:0a:f6:6b:ee:8d), Dst: IPv6mcast_02 (33:33:00:00:00:02)
    > Destination: IPv6mcast_02 (33:33:00:00:00:02)
    > Source: LiteonTe_6b:ee:8d (e0:0a:f6:6b:ee:8d)
    Type: IPv6 (0x86dd)
  ▾ Internet Protocol Version 6, Src: fe80::d307:6639:8dcb:2b4e, Dst: ff02::2
    0110 .... = Version: 6
    > .... 0000 0000 .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... 0000 0000 0000 0000 = Flow Label: 0x000000
    Payload Length: 8
    Next Header: ICMPv6 (58)
    Hop Limit: 255
    Source Address: fe80::d307:6639:8dcb:2b4e
    Destination Address: ff02::2
  ▾ Internet Control Message Protocol v6
    Type: Router Solicitation (133)
    Code: 0
    Checksum: 0x8adc [correct]
    [Checksum Status: Good]
    Reserved: 00000000

```

主机收到了 134Router Advertisement 报文。该报文由 MAC 地址为 10:4f:58:6c:0c:00 的路由器发出，发给所有组播节点地址。Cur hop limit 字段表示跳数限制，为 64。Router Lifetime 字段为 1800s，表示默认路由器关联的生存期。Router Lifetime 仅适用于作为默认路由器的路由器应用；对包括在其他消息字段或选项中的信息不适用。需要对它们的信息规定时间限制的选项有它们自己的生存期字段。Reachable time，在收到可达性确认后节点假定该邻居是可到达的。它由 Neighbor Unreachability Detection 算法使用。此处为 0 意味着没有作出规定。Retrans Timer 表示重发的 Neighbor Solicitation 消息间隔时间，由地址解析和 Neighbor Unreachability Detection 算法使用。此处为 0 意味着没有作出规定。

```

  Ethernet II, Src: ArubaaHe_6c:0c:00 (10:4f:58:6c:0c:00), Dst: IPv6mcast_01 (33:33:00:00:00:01)
    > Destination: IPv6mcast_01 (33:33:00:00:00:01)
    > Source: ArubaaHe_6c:0c:00 (10:4f:58:6c:0c:00)
    Type: IPv6 (0x86dd)
  Internet Protocol Version 6, Src: fe80::104f:5883:856c:c00, Dst: ff02::1
    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: ff02::1
  Internet Control Message Protocol v6
    Type: Router Advertisement (134)
    Code: 0
    Checksum: 0x4dc7 [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)

```

再来详细分析一下 Flags 标志位字段。第一位表示管理地址配置标识，为 0 表示无状态自动配置生成 IPv6 地址。第二位表示其他有状态配置标识，为 0 表示除了 IPv6 地址以外的其他参数需要通过无状态自动配置获取。接下来的三位分别为家乡代理标识、默认路由器优先级和代理标识，此处都为 0，没有设置。其他位为保留位，暂时没有含义。

```

  > Flags: 0x00, Prf (Default Router Preference): Medium
    0... .... = Managed address configuration: Not set
    .0... .... = Other configuration: Not set
    ..0. .... = Home Agent: Not set
    ...0 0... = Prf (Default Router Preference): Medium (0)
    .... .0.. = Proxy: Not set
    .... ..0. = Reserved: 0

```

捕获到的 RA 报文还有两个选项字段，首先看第一个，包含了路由器的链路层地址。

```
√ 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)
```

第二个选项字段为前缀信息。标志位 **Flag** 中，第一位为直连标记，为 **1** 表示该前缀可以作为直连判断。第二位为自动配置标记，为 **1** 表示该前缀用于无状态地址配置。第三位为路由器地址标记，此处为 **0**，没有设置。其他标志位为保留位。**Valid Lifetime** 字段为有效时间，表示该前缀产生的地址处于有效状态的时间，单位为秒。**Preferred Lifetime** 字段为优先时间，表示由该前缀通过无状态地址自动配置产生的地址处于优先状态的时间。**Prefix** 字段为前缀地址，也就是主机所需要的 IPv6 地址前缀，将其与接口 ID 进行合并，得到 IPv6 地址。

```
√ 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)
    1... .... = On-link flag(L): Set
    .1.. .... = Autonomous address-configuration flag(A): Set
    ..0. .... = Router address flag(R): Not set
    ...0 0000 = Reserved: 0
  Valid Lifetime: 2592000
  Preferred Lifetime: 604800
  Reserved
  Prefix: 2001:da8:215:3c0a::
```



与验证本地链接 IPv6 地址是否已被占用时一样，主机对得到的 IPv6 地址 2001:da8:215:3c0a:74b7:d176:afd9:6d09 和临时 IPv6 地址 2001:da8:215:3c0a:b14d:4874:7a84:bc8 进行验证，发送 NS 报文。随后并没有收到两个地址的 NA 报文，两个地址都可用，IPv6 地址无状态自动配置结束。

```

  ~ Ethernet II, Src: LiteonTe_6b:ee:8d (e0:0a:f6:6b:ee:8d), Dst: IPv6mcast_ff:d9:6d:09 (33:33:ff:d9:6d:09)
    > Destination: IPv6mcast_ff:d9:6d:09 (33:33:ff:d9:6d:09)
    > Source: LiteonTe_6b:ee:8d (e0:0a:f6:6b:ee:8d)
    Type: IPv6 (0x86dd)
  ~ Internet Protocol Version 6, Src: ::, Dst: ff02::1:ff d9:6d09
    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:ff d9:6d09
  ~ Internet Control Message Protocol v6
    Type: Neighbor Solicitation (135)
    Code: 0
    Checksum: 0x3dec [correct]
    [Checksum Status: Good]
    Reserved: 00000000
    Target Address: 2001:da8:215:3c0a:74b7:d176:afd9:6d09

  ~ Ethernet II, Src: LiteonTe_6b:ee:8d (e0:0a:f6:6b:ee:8d), Dst: IPv6mcast_ff:84:0b:c8 (33:33:ff:84:0b:c8)
    > Destination: IPv6mcast_ff:84:0b:c8 (33:33:ff:84:0b:c8)
    > Source: LiteonTe_6b:ee:8d (e0:0a:f6:6b:ee:8d)
    Type: IPv6 (0x86dd)
  ~ Internet Protocol Version 6, Src: ::, Dst: ff02::1:ff 84:bc8
    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:ff 84:bc8
  ~ Internet Control Message Protocol v6
    Type: Neighbor Solicitation (135)
    Code: 0
    Checksum: 0x8285 [correct]
    [Checksum Status: Good]
    Reserved: 00000000
    Target Address: 2001:da8:215:3c0a:b14d:4874:7a84:bc8

```

### 分析与思考

通过本次实验，抓取了 IPv6 地址获取过程的报文，并经过分析，学习到了 RS、RA、NS 等 IPv6 协议报文的内容、作用和各个字段的含义，对 IPv6 地址无状态自动配置的过程有了更深入的了解，对 ND 协议的知识更加掌握。

在实验过程中，起初获取的 IPv6 报文并没有完整的地址获取的过程。后来，发现是断网时间不够长，上次获取的 IPv6 地址仍可使用。尝试了通过 `ipconfig /release` 等 CMD 指令清除 IP 地址缓存也没用，只能通过延长断网时间解决，但也会使实验耗时更长。本次实验给的路由器给的 IPv6 地址前缀有效时间长达数天，因此没有选择延长断网时间来解决问题。只要有断网，主机还是会发送和接收到需要分析的 RS、RA、NS 和 NA 报文，只是顺序不同，同样可以从中了解无状态自动配置的原理。