

《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

实验二 IPv6 地址获取过程抓包分析

一、实验内容和目的

本次实验内容：

1. 搭建环境，只允许局域网内运行 ipv6 协议。
2. 当局域网内通上网络，开启抓包软件。
3. 学会如何在 Wireshark 过滤数据包。

在本次实验过程中，了解 IPv6 地址有状态自动配置过程，分析所抓取的包的类型，并判断每一种数据包和 DHCPv6 服务器所起到的作用。

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，一部可以连接手机热点的路由器。

三、实验步骤

1. 报文抓取

将处在连接状态的校园网断开，通过 ipconfig 命令确保再次连接互联网时将执行有状态地址自动配置的过程。

关闭校园网后，打开 Wireshark 软件，监听 WLAN 端口

重新连接校园网，等待抓包，几秒后，再次使用 ipconfig 命令确认网卡已分配 IPv6 地址，停止抓包并分析报文。

无线局域网适配器 WLAN:

媒体状态 : 媒体已断开连接
连接特定的 DNS 后缀 :

```

无线局域网适配器 WLAN:

    连接特定的 DNS 后缀 . . . . . :
    本地链接 IPv6 地址. . . . . : fe80::8c7e:895f:ac96:105f%18
    IPv4 地址 . . . . . : 10.128.192.77
    子网掩码 . . . . . : 255.255.192.0
    默认网关. . . . . : 10.128.192.1
  
```

2.报文分析

根据收发报文过程和内容，可以将有状态地址自动配置分为

- DHCPv6 有状态自动分配。DHCPv6 服务器自动分配 IPv6 地址/PD 前缀及其他网络配置参数（DNS、NIS、SNTP 服务器地址等参数）
- DHCPv6 无状态自动分配。主机 IPv6 地址仍然通过路由通告方式自动生成，DHCPv6 服务器只分配除 IPv6 地址以外的配置参数，包括 DNS、NIS、SNTP 服务器等参数。

2.1 DHCPv6 有状态自动分配

有状态地址自动配置的方式下，主要采用动态主机配置协议（DHCP），需要配备专门的 DHCP 服务器，网络接口通过客户机/服务器模式从 DHCP 服务器处得到地址配置信息。在本次抓包中可以看到有几个 DHCPv6 包：

fe80::8c7e:895f:ac96:105f	ff02::1:2	DHCPv6	147 Solicit XID: 0xbcc319 CID: 000100012326f80754bf645049ba
fe80::7685:c4ff:fe11:2001	fe80::8c7e:895f:ac96:105f	DHCPv6	151 Advertise XID: 0xbcc319 IAA: 2001:da8:215:3c01::4:5ac1 CID: 000100012326f80754bf645049ba
fe80::8c7e:895f:ac96:105f	ff02::1:2	DHCPv6	147 Solicit XID: 0x86563f CID: 000100012326f80754bf645049ba
fe80::7685:c4ff:fe11:2001	fe80::8c7e:895f:ac96:105f	DHCPv6	151 Advertise XID: 0x86563f IAA: 2001:da8:215:3c01::4:5ac1 CID: 000100012326f80754bf645049ba
fe80::8c7e:895f:ac96:105f	ff02::1:2	DHCPv6	193 Request XID: 0x86563f CID: 000100012326f80754bf645049ba IAA: 2001:da8:215:3c01::4:5ac1
fe80::7685:c4ff:fe11:2001	fe80::8c7e:895f:ac96:105f	DHCPv6	151 Reply XID: 0x86563f IAA: 2001:da8:215:3c01::4:5ac1 CID: 000100012326f80754bf645049ba

首先 DHCPv6 客户端使用 Solicit 报文来确定 DHCPv6 服务器的位置，之后 DHCPv6 服务器发送 Advertise 报文来对 Solicit 报文进行回应，宣告自己能够提供 DHCPv6 服务。DHCPv6 客户端发送 Request 报文向 DHCPv6 服务器请求 IPv6 地址和其他配置信息

- DHCPv6 Request

```

> Internet Protocol Version 6, Src: fe80::8c7e:895f:ac96:105f, Dst: ff02::1:2
> User Datagram Protocol, Src Port: 546, Dst Port: 547
v DHCPv6
  Message type: Request (3)
  Transaction ID: 0x86563f
  > Elapsed time
  > Client Identifier
  > Server Identifier
  > Identity Association for Non-temporary Address
  > Client Fully Qualified Domain Name
  > Vendor Class
  > Option Request

```

之后 DHCPv6 服务器发送携带了地址和配置信息的 Reply 报文回应从 DHCPv6 客户端收到的 Solicit、Request 报文

- DHCPv6 Reply

```

> Internet Protocol Version 6, Src: fe80::7685:c4ff:fe11:2001, Dst: fe80::8c7e:895f:ac96:105f
> User Datagram Protocol, Src Port: 547, Dst Port: 546
v DHCPv6
  Message type: Reply (7)
  Transaction ID: 0x86563f
  v Identity Association for Non-temporary Address
    Option: Identity Association for Non-temporary Address (3)
    Length: 40
    IAID: 11b46921
    T1: 3600
    T2: 7200
  v IA Address
    Option: IA Address (5)
    Length: 24
    IPv6 address: 2001:da8:215:3c01::4:5ac1
    Preferred lifetime: 604802
    Valid lifetime: 2592000
  > Client Identifier
  > Server Identifier
  > Preference

```

可以看到 Reply 报文包含 DHCPv6 服务器回送的 IPv6 地址，为 2001:da8:215:3c01::4:5ac1，观察命令行中的地址可以看到一致

```

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:da8:215:3c01::4:5ac1(首选)
获得租约的时间 . . . . . : 2021年5月27日 23:06:24
租约过期的时间 . . . . . : 2021年6月26日 23:06:23

```

2.2 DHCPv6 无状态自动分配

第一步：本地主动发送询问报文

包括 NS 报文、RS 报文和两个 Multicast Listener report message 报文

::	ff02::1:ff96:105f	ICMPv6	78 Neighbor Solicitation for fe80::8c7e:895f:ac96:105f
::	ff02::1:ff96:105f	ICMPv6	78 Neighbor Solicitation for 2001:da8:215:3c01:8c7e:895f:ac96:105f
::	ff02::1:ff58:3772	ICMPv6	78 Neighbor Solicitation for 2001:da8:215:3c01:3130:93be:e258:3772
fe80::8c7e:895f:ac96:105f	ff02::2	ICMPv6	62 Router Solicitation
fe80::8c7e:895f:ac96:105f	ff02::16	ICMPv6	130 Multicast Listener Report Message v2
fe80::8c7e:895f:ac96:105f	ff02::1:ff11:2001	ICMPv6	86 Neighbor Solicitation for fe80::7685:c4ff:fe11:2001 from b4:69:21
fe80::7685:c4ff:fe11:2001	fe80::8c7e:895f:ac96:105f	ICMPv6	86 Neighbor Advertisement fe80::7685:c4ff:fe11:2001 (Pfr, sol, ovr)
fe80::8c7e:895f:ac96:105f	ff02::16	ICMPv6	110 Multicast Listener Report Message v2

两个 NS 报文的内容为：

● NS 报文 1

> Internet Protocol Version 6, Src: ::, Dst: ff02::1:ff96:105f
Internet Control Message Protocol v6
Type: Neighbor Solicitation (135)
Code: 0
Checksum: 0x985e [correct]
[Checksum Status: Good]
Reserved: 00000000
Target Address: fe80::8c7e:895f:ac96:105f

该报文属于地址冲突检测类邻节点请求报文，其 Target Address 为 **Solicited-Node** 组播组的 **fe80::8c7e:895f:ac96:105f**，用于进行重复地址检测。

无线局域网适配器 WLAN:	
连接特定的 DNS 后缀	:
本地链接 IPv6 地址.	: fe80::8c7e:895f:ac96:105f%18
IPv4 地址	: 10.128.192.77
子网掩码	: 255.255.192.0
默认网关.	: 10.128.192.1

这一地址在后续被用作本地链路 IPv6 地址。

● NS 报文 2

> Internet Protocol Version 6, Src: ::, Dst: ff02::1:ff96:105f
Internet Control Message Protocol v6
Type: Neighbor Solicitation (135)
Code: 0
Checksum: 0x2b20 [correct]
[Checksum Status: Good]
Reserved: 00000000
Target Address: 2001:da8:215:3c01:8c7e:895f:ac96:105f

该报文也属于地址冲突检测类的邻节点请求报文，其 Target Address 为

2001:da8:215:3c01:8c7e:895f:ac96:105f, 用于重复地址检测。

```
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:da8:215:3c01::4:5ac1(首选)
    获得租约的时间 . . . . . : 2021年5月27日 23:06:25
    租约过期的时间 . . . . . : 2021年6月26日 23:06:24
    IPv6 地址 . . . . . : 2001:da8:215:3c01:8c7e:895f:ac96:105f(首选)
    临时 IPv6 地址. . . . . : 2001:da8:215:3c01:255e:1f46:1d2d:b68a(首选)
    本地链接 IPv6 地址. . . . . : fe80::8c7e:895f:ac96:105f%18(首选)
    IPv4 地址 . . . . . : 10.128.192.77(首选)
```

最终该地址被用作 IPv6 地址

● RS 报文

```
> Internet Protocol Version 6, Src: fe80::8c7e:895f:ac96:105f, Dst: ff02::2
v Internet Control Message Protocol v6
  Type: Router Solicitation (133)
  Code: 0
  Checksum: 0xaa63 [correct]
  [Checksum Status: Good]
  Reserved: 00000000
```

RS 报文用于寻找本地链路内的所有路由器，其目的地址为组播地址

FF02::2，即站点路由器组播地址。

● 2 个 Multicast Listener report message

```
> Internet Protocol Version 6, Src: fe80::8c7e:895f:ac96:105f, Dst: ff02::16
v Internet Control Message Protocol v6
  Type: Multicast Listener Report Message v2 (143)
  Code: 0
  Checksum: 0x5040 [correct]
  [Checksum Status: Good]
  Reserved: 0000
  Number of Multicast Address Records: 3
    > Multicast Address Record Changed to exclude: ff02::1:ff96:105f
    > Multicast Address Record Changed to exclude: ff02::1:ff58:3772
    > Multicast Address Record Changed to exclude: ff02::1:3
```

两个 ICMPv6 的 Multicast Listener report message 报文，用于向组播组报告自己。

第二步：路由器或设备询问本地链路层地址

```
2001:da8:215:3c01::1 ff02::1:ff2d:b68a ICMPv6 86 Neighbor Solicitation for 2001:da8:215:3c01:255e:1f46:1d2d:b68a from 74:85:c4:11:20:01
2001:da8:215:3c01:255e:1f46:1d2d:b68a 2001:da8:215:3c01::1 ICMPv6 86 Neighbor Advertisement 2001:da8:215:3c01:255e:1f46:1d2d:b68a (sol, ovr) is at b4:69:21:10:3c:7c
```

● NS 报文

```
> Internet Protocol Version 6, Src: 2001:da8:215:3c01::1, Dst: ff02::1:ff2d:b68a
▼ Internet Control Message Protocol v6
  Type: Neighbor Solicitation (135)
  Code: 0
  Checksum: 0x7a73 [correct]
  [Checksum Status: Good]
  Reserved: 00000000
  Target Address: 2001:da8:215:3c01:255e:1f46:1d2d:b68a
  ▼ ICMPv6 Option (Source link-layer address : 74:85:c4:11:20:01)
    Type: Source link-layer address (1)
    Length: 1 (8 bytes)
    Link-layer address: NewH3CTe_11:20:01 74:85:c4:11:20:01
```

NS 报文的 Target Address 为 **2001:da8:215:3c01:255e:1f46:1d2d:b68a**，发送设备为 MAC 地址为 **74:85:c4:11:20:01** 的设备，即本链路中的路由器发送了一个 NS 报文，该报文为单播报文，目的地址为本地地址，向本机询问链路层地址，并说明自己的 MAC 地址。

● NA 报文

```
> Internet Protocol Version 6, Src: 2001:da8:215:3c01:255e:1f46:1d2d:b68a, Dst: 2001:da8:215:3c01::1
▼ Internet Control Message Protocol v6
  Type: Neighbor Advertisement (136)
  Code: 0
  Checksum: 0x8fb6 [correct]
  [Checksum Status: Good]
  Flags: 0x60000000, Solicited, Override
  Target Address: 2001:da8:215:3c01:255e:1f46:1d2d:b68a
  ▼ ICMPv6 Option (Target link-layer address : b4:69:21:10:3c:7c)
    Type: Target link-layer address (2)
    Length: 1 (8 bytes)
    Link-layer address: IntelCor_10:3c:7c (b4:69:21:10:3c:7c)
```

本机回送 NA 报文回复收到的 NA 询问报文，在报文中指明自己的 MAC 地址为 **b4:69:21:10:3c:7c**

```
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
```

第三步：网关响应本机的 RS 报文

fe80::7685:c4ff:fe11:2001	ff02::1	ICMPv6	118 Router Advertisement from 74:85:c4:11:20:01
fe80::8c7e:895f:ac96:105f	ff02::16	ICMPv6	90 Multicast Listener Report Message v2
fe80::8c7e:895f:ac96:105f	ff02::16	ICMPv6	90 Multicast Listener Report Message v2
fe80::8c7e:895f:ac96:105f	ff02::16	ICMPv6	90 Multicast Listener Report Message v2

● RA 报文

> Internet Protocol Version 6, Src: fe80::7685:c4ff:fe11:2001, Dst: ff02::1	
v Internet Control Message Protocol v6	
Type: Router Advertisement (134)	
Code: 0	
Checksum: 0xfef4 [correct]	
[Checksum Status: Good]	
Cur hop limit: 64	
> Flags: 0xc0, Managed address configuration, Other configuration, Prf (Default Router Preference): Medium	
Router lifetime (s): 1800	
Reachable time (ms): 0	
Retrans timer (ms): 0	
> ICMPv6 Option (Source link-layer address : 74:85:c4:11:20:01)	
> ICMPv6 Option (MTU : 1500)	
> ICMPv6 Option (Prefix information : 2001:da8:215:3c01::/64)	

网关即出口路由器 **74:85:c4:11:20:01** 使用 RA 报文回送本地发送的 RS 报文，该报文携带了网关的相关信息，包括网关的链路层地址 **74:85:c4:11:20:01**，本地链路的 MTU：**1500**，本地链路的网络前缀 **2001:da8:215:3c01::/64**。

第四步：地址生成并执行 DAD 检测

根据 RA 报文的本地链路网络前缀，生成了两个 IPv6 地址，利用 NS 报文进行地址冲突检测。

::	ff02::1:ff96:105f	ICMPv6	78 Neighbor Solicitation for 2001:da8:215:3c01:8c7e:895f:ac96:105f
::	ff02::1:ff2d:b68a	ICMPv6	78 Neighbor Solicitation for 2001:da8:215:3c01:255e:1f46:1d2d:b68a
fe80::8c7e:895f:ac96:105f	ff02::16	ICMPv6	110 Multicast Listener Report Message v2

● NS 报文

> Internet Protocol Version 6, Src: ::, Dst: ff02::1:ff96:105f	
v Internet Control Message Protocol v6	
Type: Neighbor Solicitation (135)	
Code: 0	
Checksum: 0x2b20 [correct]	
[Checksum Status: Good]	
Reserved: 00000000	
Target Address: 2001:da8:215:3c01:8c7e:895f:ac96:105f	

该 NS 报文属于地址冲突检测请求报文，发送给 Solicited-Node 组播组的 **2001:da8:215:3c01:8c7e:895f:ac96:105f**，用于重复地址检测，若该 NS 报文未

收到回复，说明未检测到冲突，可将该地址作为本地 IPv6 地址。

```
IPv6 地址 . . . . . : 2001:da8:215:3c01:8c7e:895f:ac96:105f(首选)
临时 IPv6 地址. . . . . : 2001:da8:215:3c01:255e:1f46:1d2d:b68a(首选)
本地链接 IPv6 地址. . . . . : fe80::8c7e:895f:ac96:105f%18(首选)
```

● NS 报文

第二个 NS 报文同理，发送目的地址为 **2001:da8:215:3c01:255e:1f46:1d2d:b68a**，为收到回复，说明未检测到冲突，将地址作为临时 IPv6 地址。

第五步：检测完毕向链路节点通告

上一步执行完毕后，若没有地址冲突，则本地获得那两个 IPv6 地址，通过 NA 报文向链路上节点通告 MAC 地址和 IPv6 地址信息：

2001:da8:215:3c01:8c7e:895f:ac96:105f	ff02::1	ICMPv6	86 Neighbor Advertisement 2001:da8:215:3c01:8c7e:895f:ac96:105f (ovr) is at b4:69:21:10:3c:7c
2001:da8:215:3c01:255e:1f46:1d2d:b68a	ff02::1	ICMPv6	86 Neighbor Advertisement 2001:da8:215:3c01:255e:1f46:1d2d:b68a (ovr) is at b4:69:21:10:3c:7c
fe80::8c7e:895f:ac96:105f	ff02::16	ICMPv6	90 Multicast Listener Report Message v2

● NA 报文

```
> Internet Protocol Version 6, Src: 2001:da8:215:3c01:8c7e:895f:ac96:105f, Dst: ff02::1
v Internet Control Message Protocol v6
  Type: Neighbor Advertisement (136)
  Code: 0
  Checksum: 0xc783 [correct]
  [Checksum Status: Good]
  > Flags: 0x20000000, Override
  Target Address: 2001:da8:215:3c01:8c7e:895f:ac96:105f
  > ICMPv6 Option (Target link-layer address : b4:69:21:10:3c:7c)

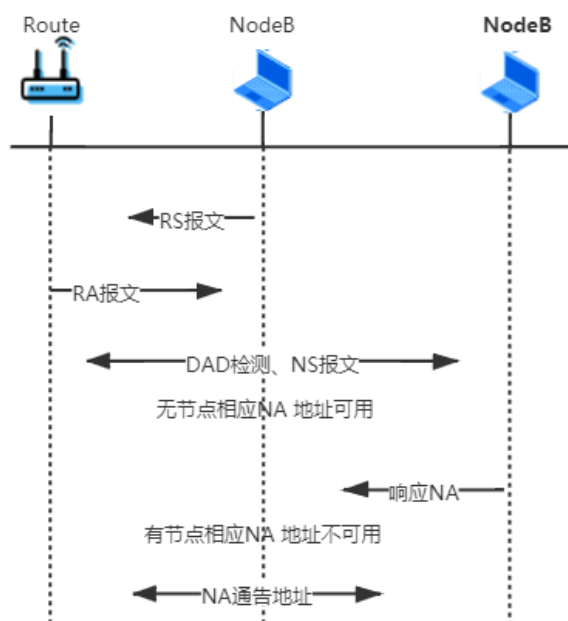
> Internet Protocol Version 6, Src: 2001:da8:215:3c01:255e:1f46:1d2d:b68a, Dst: ff02::1
v Internet Control Message Protocol v6
  Type: Neighbor Advertisement (136)
  Code: 0
  Checksum: 0x3c73 [correct]
  [Checksum Status: Good]
  > Flags: 0x20000000, Override
  Target Address: 2001:da8:215:3c01:255e:1f46:1d2d:b68a
  > ICMPv6 Option (Target link-layer address : b4:69:21:10:3c:7c)
```

向链路中节点通告 MAC 地址为 **b4:69:21:10:3c:7c** 的设备的 IPv6 地址

四、实验总结

本次实验通过抓包分析的方法，具体的分析了本地有状态地址自动配置的过程，其中又分为 DHCPv6 有状态自动分配和 DHCPv6 无状态自动分配，其中无状态自动分配的主要流程可抽象成如下所示：

节点首先发送 RS 请求找到路由器，路由器回送 RA 信息，包含网络前缀信息等，本机依照网络前缀信息生成 IPv6 地址，使用 NS 报文执行 DAD 检测，若无节点回送 NA 报文，说明地址可用，若有节点回送 NA 报文，说明地址有冲突，需要执行进一步操作，当地址确认后，本机发送 NA 通告报文，向网络中节点通告自身的 IPv6 地址和 MAC 地址。



本次实验也遇到了一些问题，其中主要有以下几个问题：

1. RA 报文回复时间较长，由于 Windows 连接原因，连接 wifi 会经过正在连接到已连接的过程，这个过程会经历大概三秒，RA 报文在“正在”连接过程中构建并收到，而“已连接”在完成地址配置后才会显示



2. Wireshark 抓包的报文中含有大量的 ICMPv6 Multicast Listener Report

Message v2 报文

