**《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**

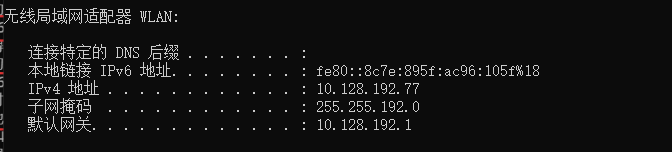
**1.报文抓取**

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。





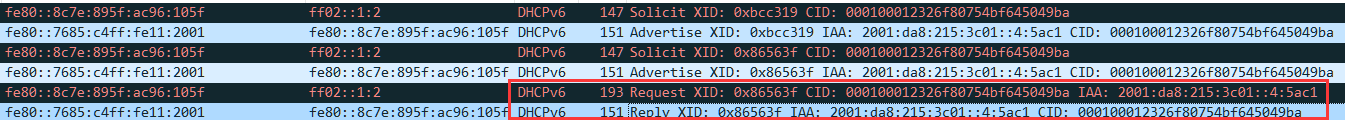
**2.报文分析**

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**

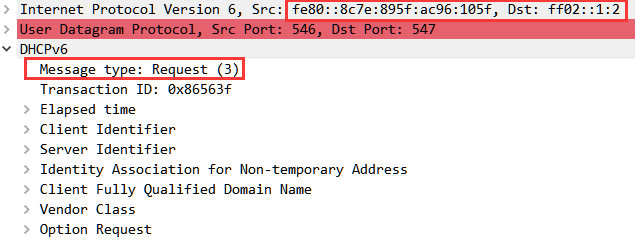
有状态地址自动配置的方式下，主要采用动态主机配置协议（DHCP），需要配备专门的DHCP服务器，网络接口通过客户机/服务器模式从DHCP服务器处得到地址配置信息。在本次抓包中可以看到有几个DHCPv6包：



首先DHCPv6客户端使用Solicit报文来确定DHCPv6服务器的位置，之

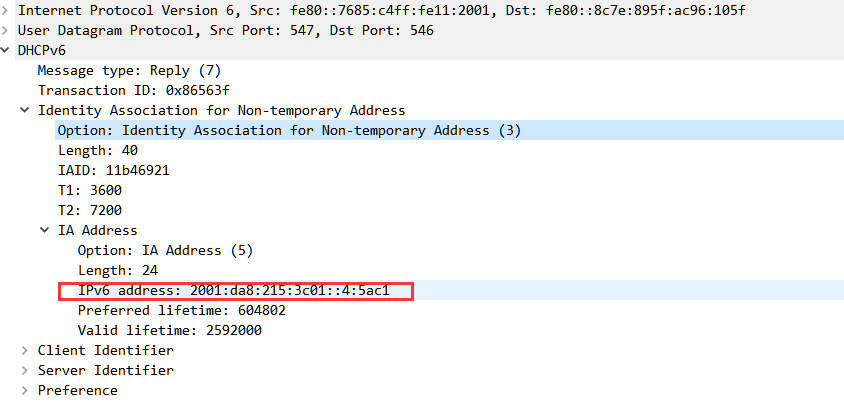
后DHCPv6服务器发送Advertise报文来对Solicit报文进行回应，宣告自己能够提供DHCPv6服务。DHCPv6客户端发送Request报文向DHCPv6服务器请求IPv6地址和其他配置信息

* DHCPv6 Request

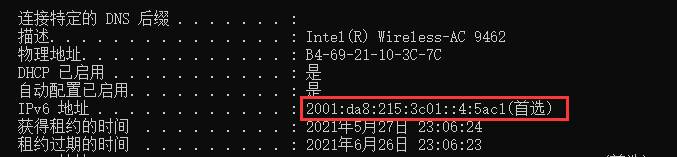


之后DHCPv6服务器发送携带了地址和配置信息的Reply报文回应从DHCPv6客户端收到的Solicit、Request报文

* DHCPv6 Reply



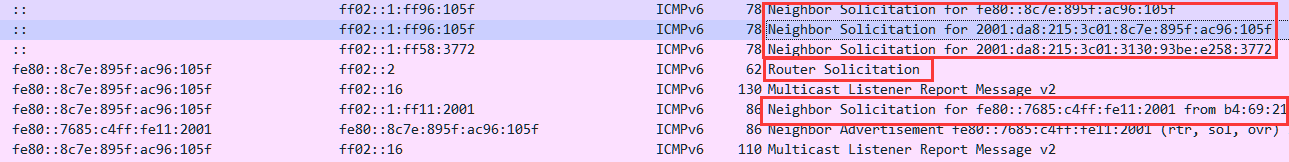
可以看到Reply报文包含DHCPv6服务器回送的IPv6地址，为**2001:da8:215:3c01::4:5ac1**，观察命令行中的地址可以看到一致



**2.2 DHCPv6无状态自动分配**

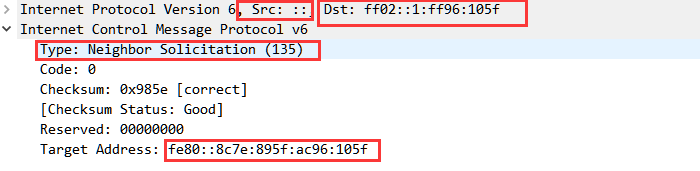
**第一步：本地主动发送询问报文**

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

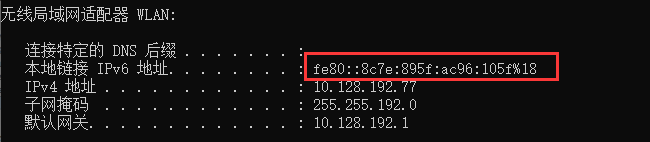


两个NS报文的内容为：

* **NS报文1**

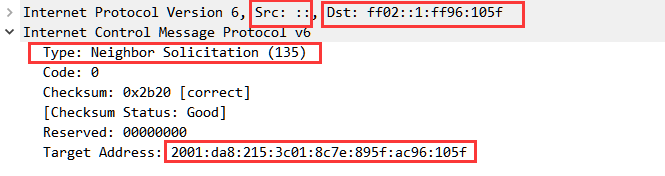


该报文属于地址冲突检测类邻节点请求报文，其Target Address为**Solicited-Node**组播组的**fe80::8c7e:895f:ac96:105f**，用于进行重复地址检测。

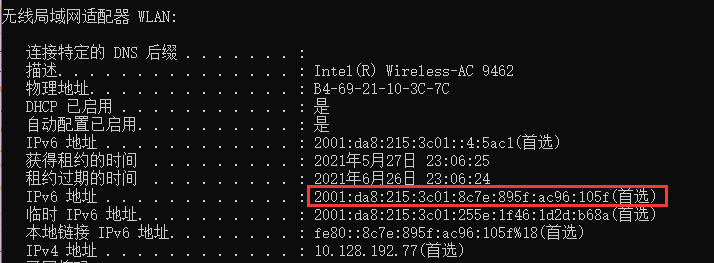


这一地址在后续被用作本地链路IPv6地址。

* **NS报文2**

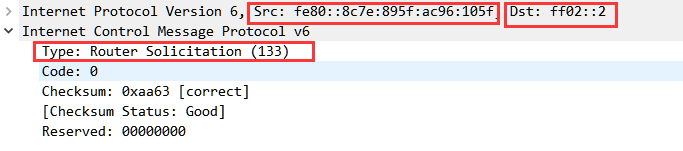


该报文也属于地址冲突检测类的邻节点请求报文，其Target Address为**2001:da8:215:3c01:8c7e:895f:ac96:105f**，用于重复地址检测。



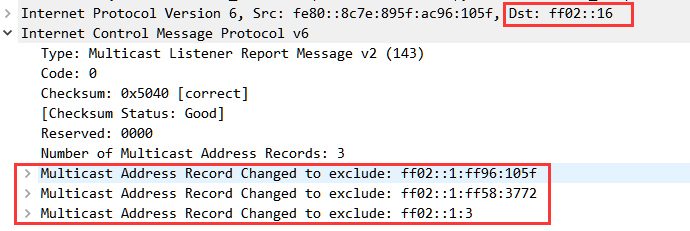
最终该地址被用作IPv6地址

* **RS报文**



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**



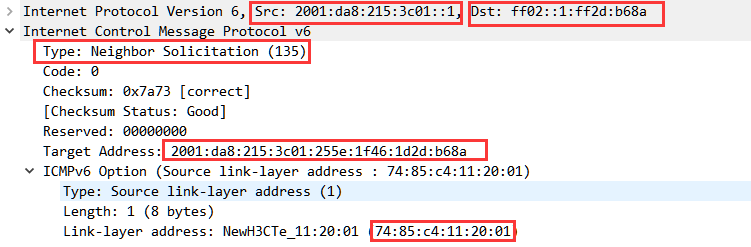
两个ICMPv6的Multicast Listener report message报文，用于向组播组报

告自己。

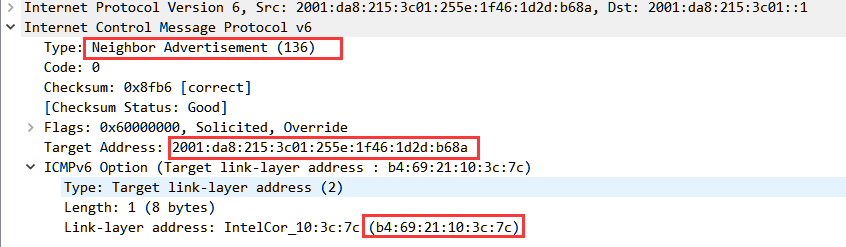
**第二步：路由器或设备询问本地链路层地址**



* **NS报文**

 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。

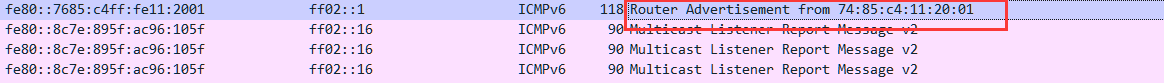
* **NA报文**



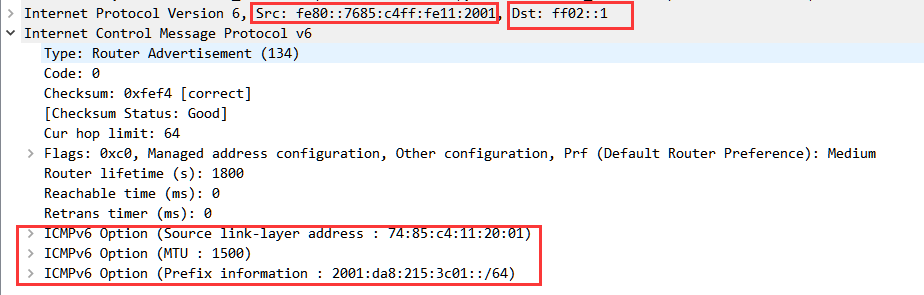
本机回送NA报文回复收到的NA询问报文，在报文中指明自己的MAC地址为**b4:69:21:10:3c:7c**



**第三步：网关响应本机的RS报文**



* **RA报文**



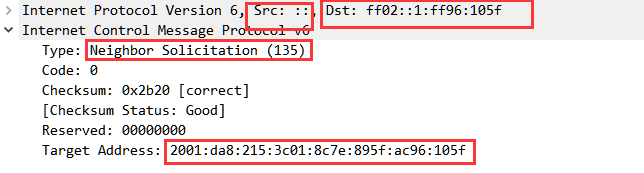
网关即出口路由器**74:85:c4:11:20:01**使用RA报文回送本地发送的RS报文，该报文携带了网关的相关信息，包括网关的链路层地址**74:85:c4:11:20:01**，本地链路的MTU：**1500**，本地链路的网络前缀**2001:da8:215:3c01::/64。**

**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。



* **NS报文**



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。



* **NS报文**

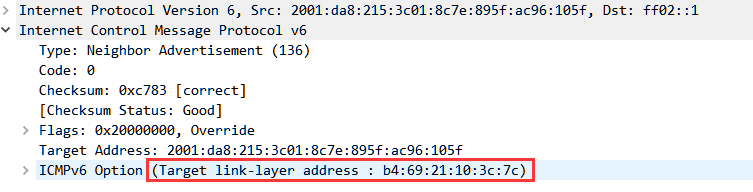
第二个NS报文同理，发送目的地址为**2001:da8:215:3c01:255e:1f46:1d2d:b68a**，为收到回复，说明未检测到冲突，将地址作为临时IPv6地址。

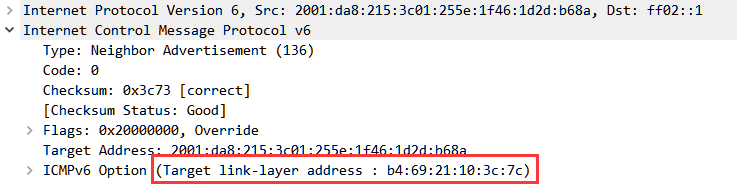
**第五步：检测完毕向链路节点通告**

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：



* **NA报文**



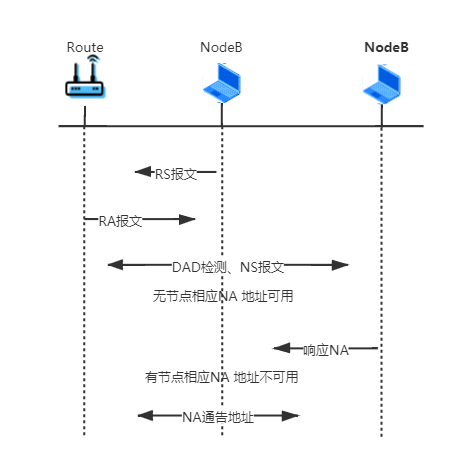


向链路中节点通告MAC地址为**b4:69:21:10:3c:7c**的设备的IPv6地址

**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。

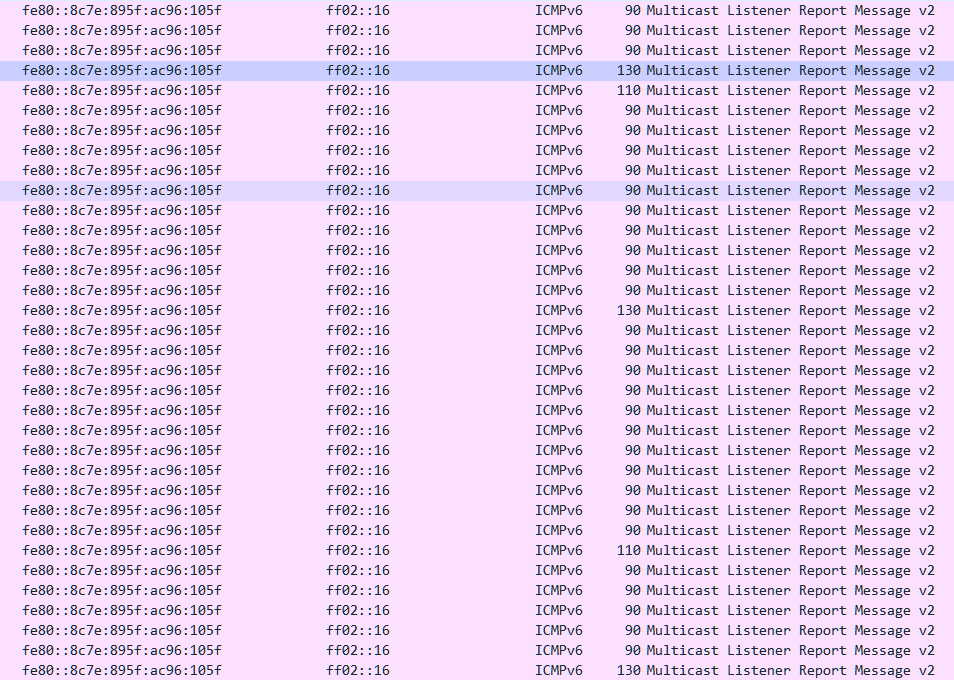


本次实验也遇到了一些问题，其中主要有以下几个问题：

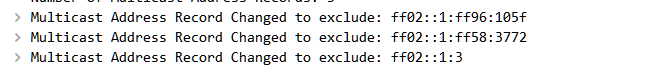
1.RA报文回复时间较长，由于Windows连接原因，连接wifi会经过正在连接到已连接的过程，这个过程会经历大概三秒，RA报文在“正在”连接过程中构建并收到，而“已连接”在完成地址配置后才会显示



2.Wireshark抓包的报文中含有大量的**ICMPv6 Multicast Listener Report Message v2**报文



该报文用于向组播组报告，仔细观察报文内容可以发现，该报文报告的内容为：



即本机在向组播组报告，在组播组地址中剔除某段地址，由于实验过程中组播组变化频率高，每台机器具有多个IPv6地址，产生了很多该报文。

**五、实验心得**

本次实验使用Wireshark抓包分析了本机连接到网络中时的有状态地址自动配置的过程，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、tarcert命令的工作原理，以及计算机网络路由的相关性知识。