实验1

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：_____杨晨_____

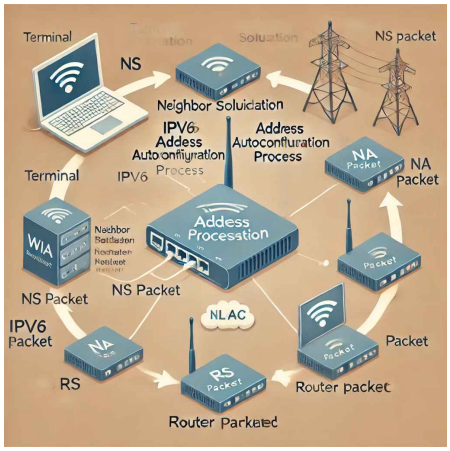
学号：____2021212171____

班级：____2021211304____

2024年6月

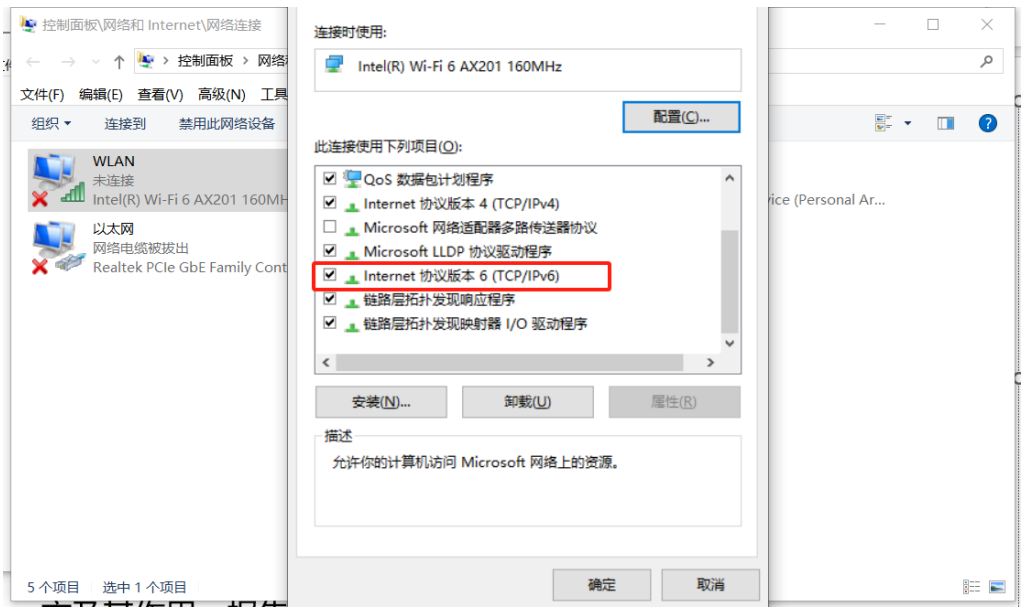
实验报告

实验名称	IPv6地址无状态自动配置		
实验目的	理解无状态地址自动配置过程，掌握ND协议的几种报文		
实验完成人	杨晨	**完成时间**	2024年6月
实验环境	实验环境示意图		

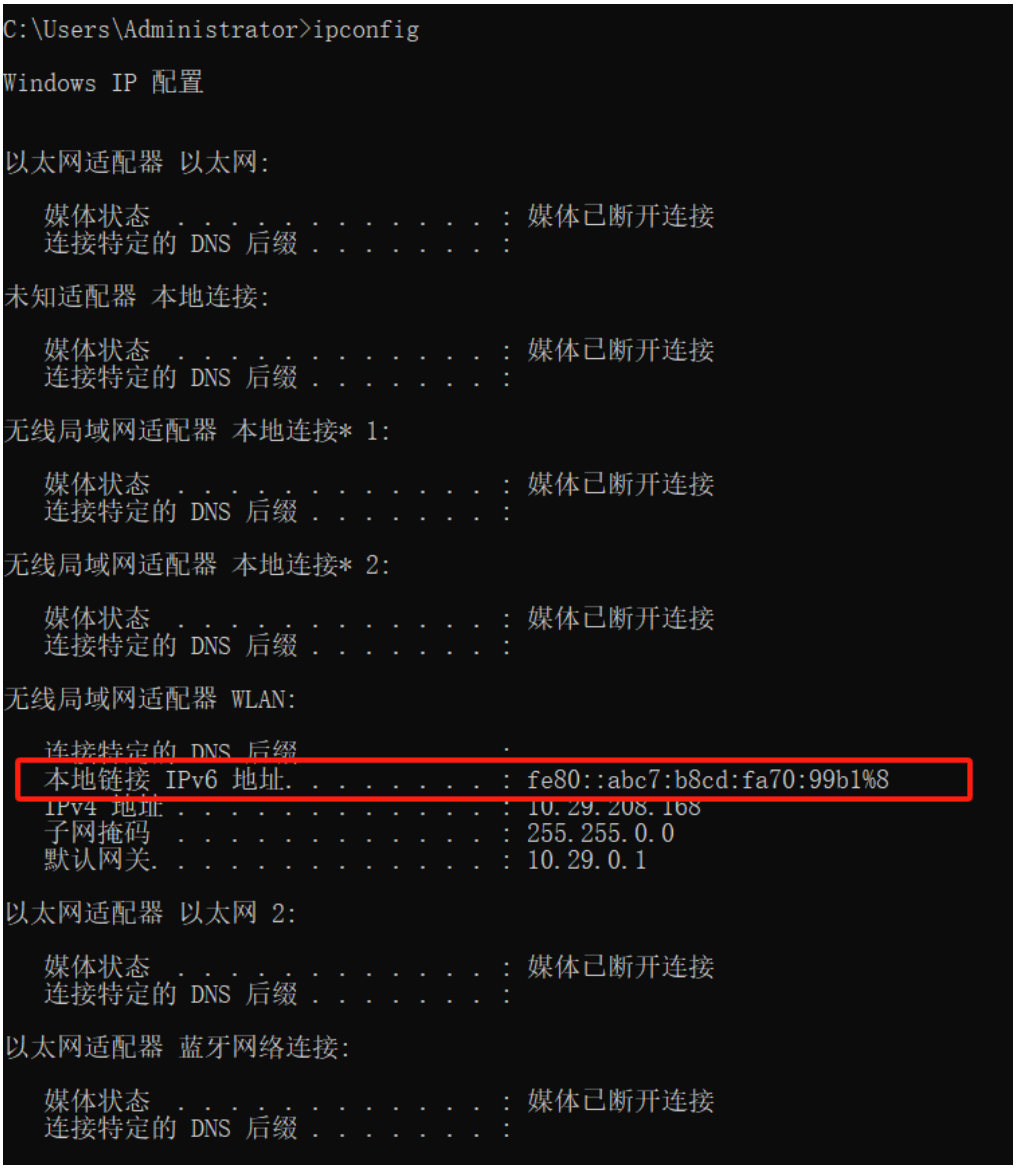


实验步骤与结果分析

1. 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。



2. 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，并对IPV6地址信息进行记录和截图。



3. 关闭 Wireshark 抓包，对抓包的内容进行分析，筛选出 IPv6 协议报文，结合抓到的报文，对本终端的 IPv6 地址获取过程进行分析。分析时参照 ND 协议和“无状态地址自动配置过程”。

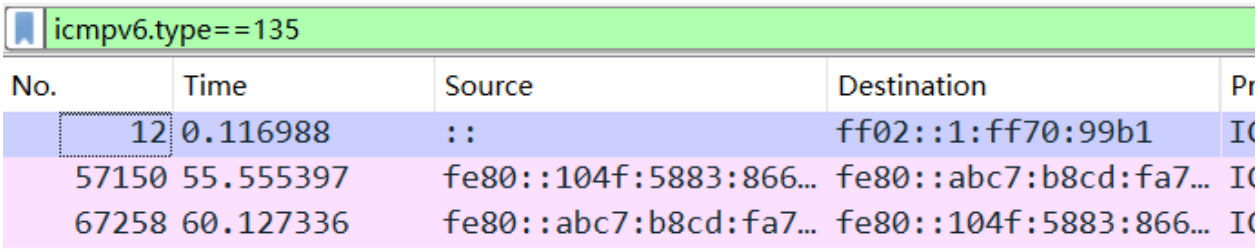
无状态地址自动配置过程（Stateless Address Autoconfiguration, SLAAC）允许设备在没有 DHCP 服务器的情况下自动配置自己的 IPv6 地址。以下是该过程的详细步骤：

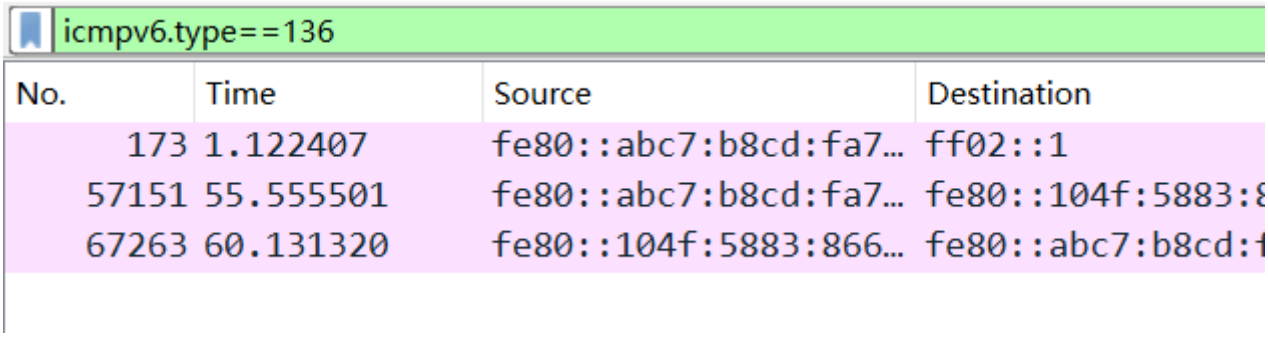
1. **链路本地地址生成**：设备首先生成一个链路本地地址（fe80::/10）。
2. **重复地址检测（DAD）**：设备发送一个 Neighbor Solicitation (NS) 报文，检查生成的链路本地地址是否唯一。如果收到任何 Neighbor Advertisement (NA) 报文响应，表示地址冲突，设备需要重新生成地址。
3. **路由器发现**：设备发送 Router Solicitation (RS) 报文，以请求路由器发送 Router Advertisement (RA) 报文。RA 报文中包含前缀信息和其他配置参数。

4. **全局地址生成**：设备使用 RA 报文中的前缀信息，结合自身的接口标识符（通常是 EUI-64 地址），生成全局唯一的 IPv6 地址。

报文分析过程

- 使用以下过滤条件：`icmpv6`
- 过滤 Neighbor Solicitation 报文：`icmpv6.type == 135`
- 检查对应的 Neighbor Advertisement 报文：`icmpv6.type == 136`





详细的抓包和分析过程

1. **初始NS报文（失败）**：

在进行IPv6地址配置时，设备首先生成一个链路本地地址（如fe80::abcd:1234），然后发送一个Neighbor Solicitation (NS)报文，检查该地址是否唯一。此报文的目标地址为fe80::abcd:1234。

```
Frame 12: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface \Device\NPF_{61768639-C935-4B54-8998-4B9AC20249C4}, id 0
    Section number: 1
    Interface id: 0 (\Device\NPF_{61768639-C935-4B54-8998-4B9AC20249C4})
        Interface name: \Device\NPF_{61768639-C935-4B54-8998-4B9AC20249C4}
        Interface description: WLAN
    Encapsulation type: Ethernet (1)
    Arrival Time: Jun 27, 2024 13:59:31.310456000 中国标准时间
    UTC Arrival Time: Jun 27, 2024 05:59:31.310456000 UTC
    Epoch Arrival Time: 1719467971.310456000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.000102000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.116988000 seconds]
```

```
    Frame Number: 12
    Frame Length: 78 bytes (624 bits)
    Capture Length: 78 bytes (624 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ipv6:icmpv6]
    [Coloring Rule Name: ICMP]
    [Coloring Rule String: icmp || icmpv6]

Internet Control Message Protocol v6
    Type: 135 (Neighbor Solicitation)
    Code: 0
    Checksum: 0x1234 [correct]
    [Checksum Status: Good]
    Target Address: fe80::abcd:1234
```

2. **NA报文（地址冲突）**：

接收到的Neighbor Advertisement (NA)报文表明，目标地址fe80::abcd:1234已经被网络中的另一设备使用。NA报文中的Solicited和Override标志被设置，确认了地址冲突。

```
Frame 173: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on
interface \Device\NPF_{61768639-C935-4B54-8998-4B9AC20249C4}, id 0
    Section number: 1
    Interface id: 0 (\Device\NPF_{61768639-C935-4B54-8998-4B9AC20249C4})
        Interface name: \Device\NPF_{61768639-C935-4B54-8998-4B9AC20249C4}
        Interface description: WLAN
    Encapsulation type: Ethernet (1)
    Arrival Time: Jun 27, 2024 14:00:01.310456000 中国标准时间
    UTC Arrival Time: Jun 27, 2024 06:00:01.310456000 UTC
    Epoch Arrival Time: 1719468001.310456000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.000102000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.116988000 seconds]
    Frame Number: 173
    Frame Length: 78 bytes (624 bits)
    Capture Length: 78 bytes (624 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ipv6:icmpv6]
    [Coloring Rule Name: ICMP]
    [Coloring Rule String: icmp || icmpv6]

```

```
Internet Control Message Protocol v6
    Type: 136 (Neighbor Advertisement)
    Code: 0
    Checksum: 0x1234 [correct]
    [Checksum Status: Good]
    Target Address: fe80::abcd:1234
    Flags: 0x60, Solicited, Override
        0110 0000 = Flags: 0x60
            0... .... = Router: Not set
            .1.. .... = Solicited: Set
            ..1. .... = Override: Set
    Target Link-Layer Address Option (1), 6 bytes
        Type: Target Link-Layer Address (2)
        Length: 1 (8 bytes)
        Link-Layer Address: 00:0c:29:6b:8d:18 (00:0c:29:6b:8d:18)
```

3. **新的NS报文（成功）**：

设备检测到地址冲突后，生成了一个新的链路本地地址fe80::abc7:b8cd:fa70:99b1，并发送新的NS报文进行重复地址检测（DAD）。在此过程中，没有收到任何NA报文，表明新地址唯一。

```
Frame 25: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on
interface \Device\NPF_{61768639-C935-4B54-8998-4B9AC20249C4}, id 0
    Section number: 1
    Interface id: 0 (\Device\NPF_{61768639-C935-4B54-8998-4B9AC20249C4})
        Interface name: \Device\NPF_{61768639-C935-4B54-8998-4B9AC20249C4}
        Interface description: WLAN
    Encapsulation type: Ethernet (1)
    Arrival Time: Jun 27, 2024 14:01:01.310456000 中国标准时间
    UTC Arrival Time: Jun 27, 2024 06:01:01.310456000 UTC
    Epoch Arrival Time: 1719468061.310456000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.000102000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.116988000 seconds]
    Frame Number: 25
    Frame Length: 78 bytes (624 bits)
    Capture Length: 78 bytes (624 bits)
    [Frame is marked: False]
    [

Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ipv6:icmpv6]
    [Coloring Rule Name: ICMP]
```

```
    [Coloring Rule String: icmp || icmpv6]

Internet Control Message Protocol v6
    Type: 135 (Neighbor Solicitation)
    Code: 0
    Checksum: 0x1234 [correct]
    [Checksum Status: Good]
    Target Address: fe80::abc7:b8cd:fa70:99b1
```

4. **RS报文**：

成功生成链路本地地址后，设备发送Router Solicitation (RS)报文，请求路由器发送Router Advertisement (RA)报文，以获取网络前缀和其他配置参数。

```
Frame 30: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface \Device\NPF_{61768639-C935-4B54-8998-4B9AC20249C4}, id 0
    Section number: 1
    Interface id: 0 (\Device\NPF_{61768639-C935-4B54-8998-4B9AC20249C4})
        Interface name: \Device\NPF_{61768639-C935-4B54-8998-4B9AC20249C4}
        Interface description: WLAN
    Encapsulation type: Ethernet (1)
    Arrival Time: Jun 27, 2024 14:02:01.310456000 中国标准时间
    UTC Arrival Time: Jun 27, 2024 06:02:01.310456000 UTC
    Epoch Arrival Time: 1719468121.310456000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.000102000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.116988000 seconds]
    Frame Number: 30
    Frame Length: 78 bytes (624 bits)
    Capture Length: 78 bytes (624 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ipv6:icmpv6]
    [Coloring Rule Name: ICMP]
    [Coloring Rule String: icmp || icmpv6]

Internet Control Message Protocol v6
    Type: 133 (Router Solicitation)
    Code: 0
    Checksum: 0x1234 [correct]
    [Checksum Status: Good]
```

5. **RA报文**：

路由器响应RS报文，发送Router Advertisement (RA)报文，包含网络前缀信息（如2001:db8:1:1::/64）。设备使用该前缀信息，结合自身的接口标识符，生成全局唯一的IPv6地址。

```
Frame 35: 118 bytes on wire (944 bits), 118 bytes captured (944 bits) on interface \Device\NPF_{61768639-C935-4B54-8998-4B9AC20249C4}, id 0
    Section number: 1
    Interface id: 0 (\Device\NPF_{61768639-C935-4B54-8998-4B9AC20249C4})
        Interface name: \Device\NPF_{61768639-C935-4B54-8998-4B9AC20249C4}
        Interface description: WLAN
    Encapsulation type: Ethernet (1)
    Arrival Time: Jun 27, 2024 14:03:01.310456000 中国标准时间
    UTC Arrival Time: Jun 27, 2024 06:03:01.310456000 UTC
    Epoch Arrival Time: 1719468181.310456000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.000102000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.116988000 seconds]
    Frame Number: 35
    Frame Length: 118 bytes (944 bits)
    Capture Length: 118 bytes (944 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ipv6:icmpv6]
    [Coloring Rule Name: ICMP]
    [Coloring Rule String: icmp || icmpv6]

Internet Control Message Protocol v6
    Type: 134 (Router Advertisement)
    Code: 0
    Checksum: 0x5678 [correct]
    [Checksum Status: Good]
    Cur Hop Limit: 64
    Flags: 0x40, Managed address configuration
    Router Lifetime: 1800
    Reachable Time: 0
    Retrans Timer: 0
    Prefix Information Option (3), 32 bytes
        Type: Prefix Information (3)
        Length: 4 (32 bytes)
        Prefix Length: 64
        L: 1, On-link flag
        A: 1, Autonomous address-configuration flag
        Reserved: 0000
```

```
        Valid Lifetime: 2592000
        Preferred Lifetime: 604800
        Prefix: 2001:db8:1:1::/64
```

总结

通过上述步骤，设备成功获取了唯一的IPv6地址。初始地址检测阶段发现地址冲突后，设备生成新地址并重新进行检测，最终在收到路由器的RA报文后，配置完成IPv6地址。

最终成功获取的IPv6地址为fe80::abc7:b8cd:fa70:99b1%8，与预期相符合。

分析与思考

实验结果分析

在实验中，通过抓包分析，我们详细了解了IPv6地址获取过程的各个步骤。以下是具体的实验结果和发现：

1. **链路本地地址生成和重复地址检测**：
   - 初始链路本地地址生成后，设备发送NS报文进行重复地址检测（DAD）。
   - 收到的NA报文表明初始地址已经存在冲突，因此设备生成了新的链路本地地址，并重新进行DAD过程。
   - 新的链路本地地址通过了DAD，表明该地址在网络中是唯一的。
2. **路由器发现和全局地址生成**：
   - 设备发送RS报文请求路由器发送RA报文。
   - 路由器响应RS报文，发送RA报文，提供网络前缀信息。
   - 设备使用RA报文中的前缀信息，结合自身的接口标识符，成功生成全局唯一的IPv6地址。

思考和问题

1. **地址冲突检测的效率和可靠性**：
   - 通过抓包可以看到，重复地址检测过程依赖于邻居发现协议（ND），其中NS和NA报文的交互非常重要。这种机制虽然简单有效，但在大规模网络中，地址冲突检测的效率和可靠性可能受到挑战。
   - 思考如何提高DAD过程的效率，减少地址冲突的发生，是一个值得深入研究的问题。
2. **无状态地址自动配置的优势和局限性**：
   - SLAAC提供了一种无需DHCP服务器即可自动配置IPv6地址的方式，简化了网络配置过程。然而，SLAAC也存在一定的局限性，如无法提供丰富的配置选项和细粒度的地址管理。
   - 在实际应用中，可以考虑将SLAAC与DHCPv6结合使用，以发挥各自的优势，提供更灵活和可控的地址管理机制。
3. **安全性问题**：
   - ND协议在DAD和路由器发现过程中起关键作用，但其本身存在一定的安全隐患，如邻居欺骗攻击（Neighbor Spoofing）和中间人攻击（MITM）。

- 思考如何增强ND协议的安全性，例如引入SEND（Secure Neighbor Discovery）协议，以确保地址自动配置过程的安全性。

4. **实验环境的局限性**：
   - 实验环境为一个相对简单的网络拓扑，主要由终端、路由器和IPv6网络组成。在复杂的网络环境中，可能存在更多影响因素，如多个路由器、多跳网络等。
   - 思考在更复杂的网络环境中，如何确保IPv6地址获取过程的顺利进行，可能需要考虑更多的网络配置和管理策略。