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：\_\_\_\_\_\_\_\_张晨阳\_\_\_\_\_\_\_

学号：\_\_\_\_\_\_2022211683\_\_\_\_\_\_

班级：\_\_\_\_\_\_2022211305\_\_\_\_\_\_

2025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 | | 学习分析 IPv6 地址获取过程，掌握ND协议的几种报文 | | |
| 实验完成人 | | 张晨阳 | 完成时间 | 2025.05 |
| 实验环境 | Windows 11  无线网卡：Realtek RTL8852BE WiFi 6 802.11ax PCle Adapter  Wireshark 4.2.5  BUPT-portal | | | |
| 实验步骤与结果分析 | | | | |
| 1. **断开校园网（手机热点）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（手机热点）的网卡，启动抓包。**     **2. 恢复校园网（手机热点）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。**    如图所示，无线局域网适配器 WLAN部分显示我们已经获取了IPV6地址：  IPv6 地址 . . . . . . . . . . . . : 2001:da8:215:3c0a:7eab:6a74:3a6d:a32e  临时 IPv6 地址. . . . . . . . . . : 2001:da8:215:3c0a:74e1:10a3:5376:a08d  本地链接 IPv6 地址. . . . . . . . : fe80::9783:ad5f:d9fa:5e6a%3**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”。3.1 Neighbor Discovery 协议**  IPv6 中的地址获取不再依赖传统的 ARP 和 DHCP 协议，而是通过一套新的协议机制完成，这就是 **邻居发现协议（Neighbor Discovery，简称 ND 协议）**。ND 协议基于 ICMPv6 协议实现，其核心功能包括：   * 路由器发现（Router Discovery） * 前缀发现（Prefix Discovery） * 参数自动配置（Autoconfiguration） * 地址重复检测（Duplicate Address Detection, DAD） * 邻居可达性检测（Neighbor Unreachability Detection）   ND 协议定义了以下几种关键的 ICMPv6 报文类型：   |  |  |  |  | | --- | --- | --- | --- | | **报文类型** | **名称** | **ICMPv6 类型码** | **作用** | | Router Solicitation (RS) | 路由器请求报文 | 133 | 终端发起请求，寻找本地链路上的路由器 | | Router Advertisement (RA) | 路由器通告报文 | 134 | 路由器广播网络前缀和其他配置信息 | | Neighbor Solicitation (NS) | 邻居请求报文 | 135 | 用于地址解析或重复地址检测 | | Neighbor Advertisement (NA) | 邻居通告报文 | 136 | 响应 NS 报文，确认地址可达性 |   **3.2无状态地址自动配置流程**  SLAAC 是一种无需 DHCP 服务器即可让终端自动获取 IPv6 地址的机制，依赖 ND 协议中的 RS 和 RA 报文。  整个过程如下：   1. **链路本地地址生成：**终端在启动网络接口后，首先基于接口 MAC 地址（或随机数）构建一个链路本地地址（Link-local Address，通常形如 fe80::/64），用于与本地链路上的设备通信。 2. **发送 Router Solicitation (RS)：**终端向局域网广播 RS 报文，请求网络中存在的 IPv6 路由器发送 Router Advertisement。 3. **接收 Router Advertisement (RA)：**本地链路中的 IPv6 路由器响应 RS 报文，发送 RA 报文，提供网络前缀、路由器地址、MTU 等信息。RA 报文中通常包含：  * Prefix Information：用于构造终端的全局地址 * Autonomous flag：指示是否允许使用该前缀进行 SLAAC 地址配置  1. **构造全局地址：**终端根据收到的前缀（如 2001:db8:abcd::/64）和自身的接口标识（Interface ID），自动拼接生成完整的全局单播地址。 2. **地址重复检测（Duplicate Address Detection, DAD）：**在使用新生成的地址前，终端发送一个 NS 报文，将目标地址设为该新地址，用于检测是否已有其他设备使用相同地址。  * 如果收到对应的 NA 报文，说明地址冲突，终端需重新生成地址； * 若未收到 NA，则说明该地址未被占用，可以使用。  1. **地址配置完成：**若 DAD 通过，终端正式启用该 IPv6 地址，可进行通信。   **3.3 报文分析**  我们使用过滤条件icmpv6。  **首先是RS报文：**    该报文为终端设备主动发出的 **Router Solicitation (RS)** ，ICMPv6 类型为 **133**。  **源地址**：fe80::9783:ad5f:d9fa:5e6a（终端的链路本地地址）  **目的地址**：ff02::2（所有本地链路上的路由器）  **链路层源MAC地址**：9c:2f:9d:91:d5:99  **作用说明**：终端在连接网络后，为尽快获取网络参数，主动请求局域网内的路由器发送 RA 报文。  **RA报文：**    该报文为局域网内的IPv6路由器对 RS 报文的响应，ICMPv6 类型为 **134**，即 **Router Advertisement (RA)** 报文。   * **源地址**：fe80::104f:5883:856c:c00（路由器的链路本地地址） * **目的地址**：ff02::1（所有IPv6主机） * **路由器源MAC地址**：10:4f:58:6c:0c:00 * **Prefix Information 前缀信息**：   **前缀地址**：2001:da8:215:3c0a::/64  **A位（Autonomous）**：为1，表示允许终端使用此前缀进行自动地址配置   * **作用说明**：RA报文中包含IPv6网络前缀和参数信息，终端将用该前缀与自身接口ID拼接生成全局IPv6地址。   **NS报文：**    此报文为终端向目标地址发送的 **Neighbor Solicitation (NS)** 报文，ICMPv6 类型为 **135**，用于进行 **DAD（重复地址检测）**。   * **源地址**：fe80::9783:ad5f:d9fa:5e6a * **目标地址（Target Address）**：fe80::104f:5883:856c:c00 * **目的地址**：ff02:1:ff6c:c00（为目标地址构造出的组播地址） * **作用说明**：终端通过发送 NS 报文检测其即将使用的地址是否被网络中其他设备占用。   **NA报文：**    该报文为目标设备回应 NS 的 **Neighbor Advertisement (NA)** 报文，ICMPv6 类型为 **136**。   * **源地址**：fe80::104f:5883:856c:c00 * **目的地址**：fe80::9783:ad5f:d9fa:5e6a（终端设备的链路本地地址） * **Flags**：Router=1，Solicited=1，Override=1 * **作用说明**：回应 NS 报文，确认该地址对应设备存在，可能说明该地址已被占用（如是对终端发送 DAD 的 NS 报文回应）。   **实际情况：**    发现该地址出现冲突后，使用新的地址再次进行了NS和NA报文，无冲突后采用新地址。  综上所述，终端设备通过以下步骤成功参与了IPv6地址的无状态配置过程：   1. 终端发送 RS 报文请求前缀信息 2. 路由器返回 RA 报文，提供 2001:da8:215:3c0a::/64 前缀 3. 终端生成完整 IPv6 地址，例如 2001:da8:215:3c0a:7eab:6a74:3a6d:a32e 4. 终端使用 NS 报文进行 DAD 检测 5. 若未收到 NA 报文（或 NA 报文不表示地址冲突），终端正式启用该地址 | | | | |
| 分析与思考 | | | | |
| 通过本次实验，我完整观察并分析了终端获取 IPv6 地址的过程，清晰识别出 ND 协议中 RS、RA、NS、NA 四类关键报文，验证了 **无状态地址自动配置（SLAAC）** 在校园网环境中的实际运行机制。这一过程无需 DHCPv6 支持，仅依赖路由器广播的前缀信息即可实现自动化地址生成与验证，体现了 IPv6 在地址配置方面的灵活性和先进性。  在实验过程中，我有以下几点思考：   1. **无状态配置过程的高效性：**相较于 IPv4 中依赖 DHCP 的方式，IPv6 的 SLAAC 无需中央服务器就能完成地址配置，极大降低了管理成本，适合大规模网络部署。这对如校园网、企业内部网等环境非常适用。 2. **ND 协议对安全的依赖性问题：**尽管 ND 协议简化了配置过程，但同时也存在一定的安全隐患。例如：RA 或 NA 报文可能被恶意设备伪造，从而导致地址冲突或网络重定向攻击。因此，在真实部署中，可能需要引入 RA-Guard 等安全机制进行保护。 3. **抓包验证提升理解效果：**相比理论学习，本次实验通过 Wireshark 实际抓取并分析了每一类报文，使我对 IPv6 网络配置机制有了更深入、直观的理解，特别是对地址生成、重复地址检测等过程的报文级细节掌握更加牢固。 4. **对实验环境与网络结构的依赖：**本次实验基于校园网的实际网络结构，路由器默认启用了 SLAAC 配置。如果网络环境中未启用 RA 广播或要求 DHCPv6 支持，则地址获取流程将有所不同。因此，在不同场景下应灵活选择合适的地址分配策略。 5. **对 IPv6 网络部署的进一步兴趣：**本实验激发了我对 IPv6 更深入研究的兴趣，例如探索 DHCPv6 的配置流程、了解临时地址（Temporary Address）与隐私扩展机制、以及如何在企业或数据中心环境中实现 IPv6 网络管理。   总体而言，本实验不仅加深了我对 IPv6 地址配置机制的理解，也让我认识到网络协议设计中效率与安全的平衡问题，为今后深入学习网络通信原理和协议栈打下了良好基础。 | | | | |