厦門大學

信息学院软件工程系

计算机网络专题报告（期中考核）

题　　目　IPv6 技术发展—NDP 邻居发现协议

班　　级　软件工程 2021 级 2 班

姓　　名　黄勖

学　　号　22920212204392

2023 年 5 月 7 日

IPv6 技术发展—NDP 邻居发现协议

22920212204392 黄勖

目录

1 摘要 2
2 前言介绍 2
2.1 ICMPv6-Internet 控制报文协议 2
2.2 组播 MAC 地址格式 3
3 报文对比和内容简介 3
3.1 报文对比 3
3.2 报文内容与说明 4
4 具体功能和原理 4
4.1 路由发现 4
4.1.1 路由器通告 RA（Router Advertisement）报文 5
4.1.2 路由器请求 RS（Router Solicitation）报文 6
4.2 主机无状态地址自动配置 6
4.2.1 自动配置过程 7
4.3 IPv6 地址解析 9
4.3.1 邻居请求报文（Neighbor Solicition） 9
4.3.2 邻居通告报文（Neighbor Advertisement） 10
4.3.3 对比与优点 10
4.3.4 报文抓包解析 11
4.4 DAD 重复地址检测 13
4.4.1 简介 13
4.4.2 通信过程 13
4.4.3 冲突检测 14
4.4.4 抓包分析 14
4.5 邻居状态跟踪 15
4.5.1 五种邻居状态 16
4.5.2 邻居状态迁移 16
4.5.3 ARP 对比与特点 17
4.6 重定向过程 17
4.6.1 重定向报文的结构 18
4.6.2 重定向过程示例 18
5 NDP 攻防 18
6 结论 19
主要参考文献 20

1 摘要

IPv6 邻居发现协议（Neighbor Discovery Protocol, NDP）是 IPv6 网络中的一个重要协议，它用于发现 IPv6 网络中的邻居设备以及实现地址自动配置等功能。本文首先介绍了 IPv6 邻居发现协议的基本原理和功能，然后对 NDP 协议中的重要特性和问题进行了深入分析，包括路由发现、地址配置和状态跟踪等。最后，本文对 NDP 协议的安全性进行了讨论，并提出了一些解决方案和建议，以保障 IPv6 网络的安全性。[1][2]

2 前言介绍

IPv6 邻居发现协议依靠 ICMPv6 协议发现，它与 IPv4 网络中的 ARP（地址解析协议）和 RARP（反向地址解析协议）类似，但比它们更加灵活和功能强大。以下是一些关于了解 NDP 协议所需要的前置内容，供读者参考。

2.1 ICMPv6-Internet 控制报文协议

ICMPv6（Internet Control Message Protocol Version 6，互联网控制报文协议版本 6）是 IPv6 的基础协议之一。ICMPv6 的协议类型号（IPv6 报文中的 Next Header 字段的值）为 58。ICMPv6 的报文格式如图 1 所示：

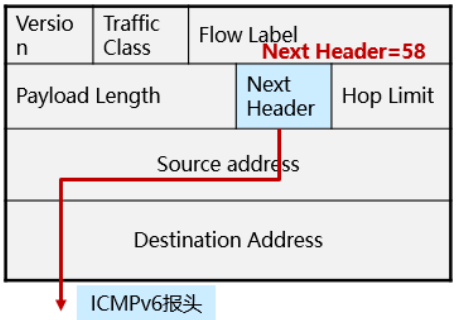

图 1 IPv6 报文

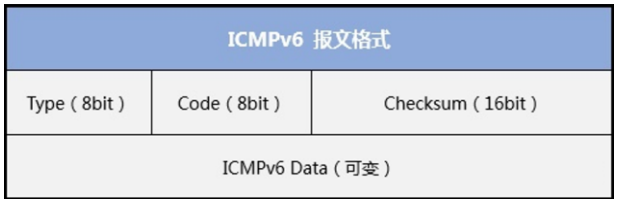

图 2 ICMPv6 的报文格式

报文中字段解释如下：[6]

- **Type**：表明消息的类型，0 至 127 表示差错报文类型，128 至 255 表示消息报文类型；
- **Code**：表示此消息类型细分的类型；
- **Checksum**：ICMPv6 报文的校验和；
- **Data**：ICMPv6 数据。

2.2 组播 MAC 地址格式

IPv6 组播 MAC 地址格式[2]如图 3；

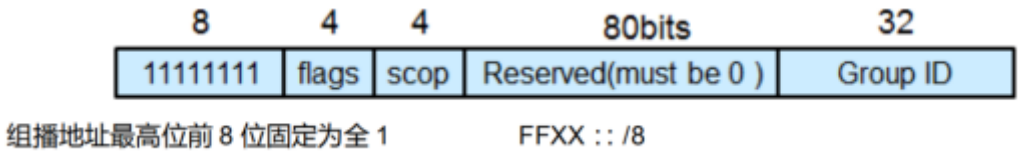

图 3 组播地址格式格式

（1）组播地址高 8bit 为固定值 FF。

（2）flags 位为 4bit：0000:永久分配或众所周知的; 0001:临时的。

（3）scop 用来限制组播数据流在网络中发送的范围。

（4）低 112 bit 为组播地址的可用组 ID。

3 报文对比和内容简介

3.1 报文对比

在 IPv4 中，ARP 报文是直接封装在以太网报文中，以太网协议类型为 0x0806，普遍观点认为 ARP 定位为第 2.5 层的协议。NDP 本身基于 ICMPv6 实现，以太

网协议类型为 0x86DD，即 IPv6 报文，IPv6 下一个报头字段值为 58，表示 ICMPv6 报文，由于 NDP 协议使用的所有报文均封装在 ICMPv6 报文中，一般来说，NDP 被看作第 3 层的协议。

3.2 报文内容与说明

表 1 NDP 使用的 ICMPv6 的相关报文

NDP 使用的 ICMPv6 的相关报文	Type 字段	说明
RS 路由器请求	133	主机刚刚接入网络、获取地址后，主机需要自动获得前缀、前缀长度、默认网关等信息时，就会发送 RS 消息。
RA 路由器通告报文	134	RA 消息由路由器周期性地发送，或者在收到主机发送的 RS 消息后立刻发送，为主机提供编址信息以及其他信息。
NS 邻居请求报文	135	当节点不知道目标地址的链路层地址时，将发送 NS 消息。
NA 邻居通告报文	136	当节点接收到 NS 消息后，会快速响应 NA 消息，或者当节点需要快速传播新的信息时，也会发送 NA 消息。
重定向报文	137	通过重定向消息，路由器可以通告更优的下一跳路由。

4 具体功能和原理[6]

4.1 路由发现

路由器发现功能用来发现与本地链路相连的设备，并获取与地址自动配置相关的前缀和其他配置参数。主要通过以下两种报文实现。

4.1.1 路由器通告 RA（Router Advertisement）报文

每台设备为了让二层网络上的主机和设备知道自己的存在，定时都会组播发送 RA 报文，RA 报文中会带有网络前缀信息及标志位信息。RA 报文的 Type 字段值为 134。

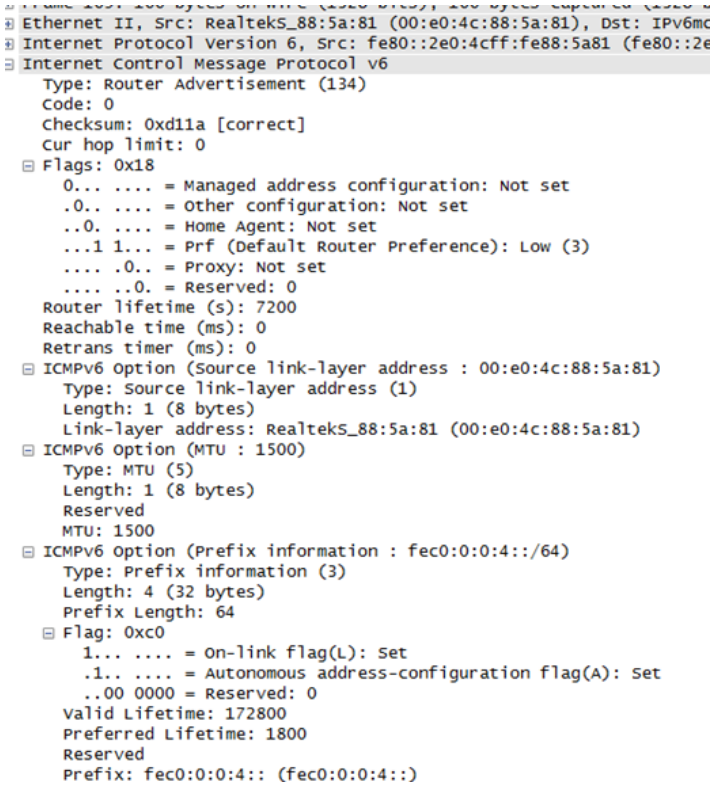

图 4 RA 邻居通告报文抓包示例

RA 报文中关键字段解释：

[1] M：表示无状态/有状态（DHCPv6）方式配置生成 IPv6 地址。

[2] O：表示除了 IPv6 地址以外的其他参数需要通过无状态/有状态（DHCPv6）配置获取。

[3] Router Lifetime：与默认路由器关联的生存期，以秒为单位。取 0 值的 Lifetime 指出路由器不是默认路由器并且不应当出现在默认路由器列表中。

[4] Reachable time：此时间以毫秒计，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。此值为 0 意味着没有规定。

［5］Retrans Timer：重发的 Neighbor Solicitation 消息间隔时间，以毫秒计。由地址解析和 Neighbor Unreachability Detection 算法使用。此值为 0 意味着没有规定。

4.1.2 路由器请求 RS（Router Solicitation）报文

很多情况下主机接入网络后希望尽快获取网络前缀进行通信，此时主机可以立刻发送 RS 报文，RS 报文的 Type 字段值为 133。

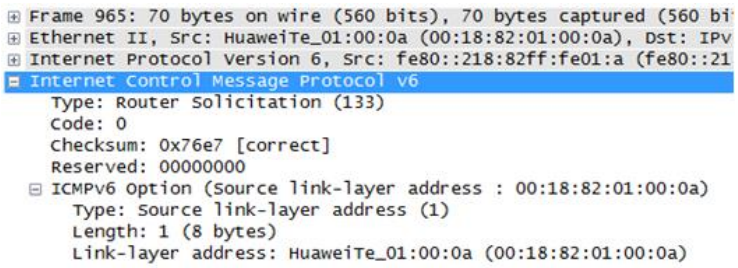

图 5 RS 报文抓包示例

在 IPv6 中，IPv6 地址可以支持无状态的自动配置，路由器发现功能是 IPv6 地址自动配置功能的基础。

4.2 主机无状态地址自动配置

IPv6 地址增长为 128 位，且终端节点多，对于自动配置的要求更为迫切，除保留了 DHCP 作为有状态自动配置外，还增加了无状态自动配置。无状态自动配置即自动生成链路本地地址，主机根据 RA 报文的前缀信息，自动配置全球单播地址等，并获得其他相关信息。

4.2.1 自动配置过程

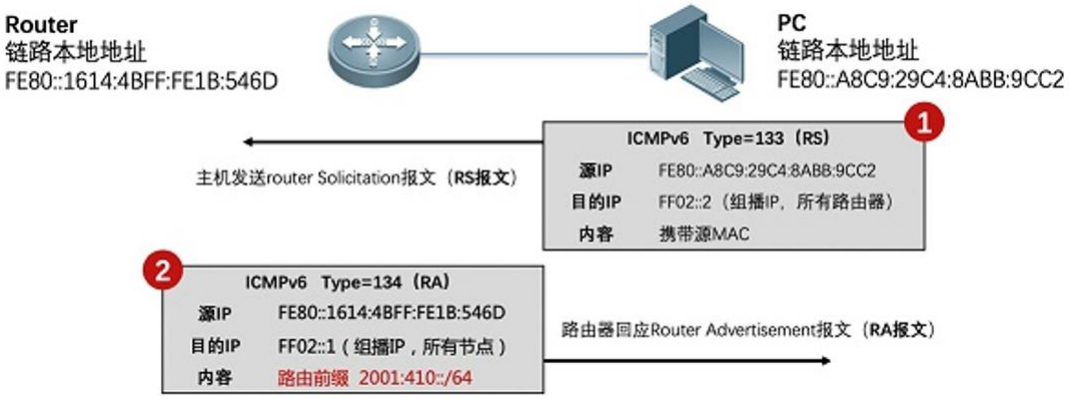

图 6 自动配置过程图示

1. 根据接口标识产生链路本地地址。
2. 发出邻居请求，进行重复地址检测。
3. 如地址冲突，则停止自动配置，需要手工配置。如不冲突，链路本地地址生效，节点具备本地链路通信能力。
4. 主机会发送 RS 报文（或接收到设备定期发送的 RA 报文）。
5. 根据 RA 报文中的前缀信息和接口标识得到 IPv6 地址。

图 7 详细解释了具体每一步的操作情景。

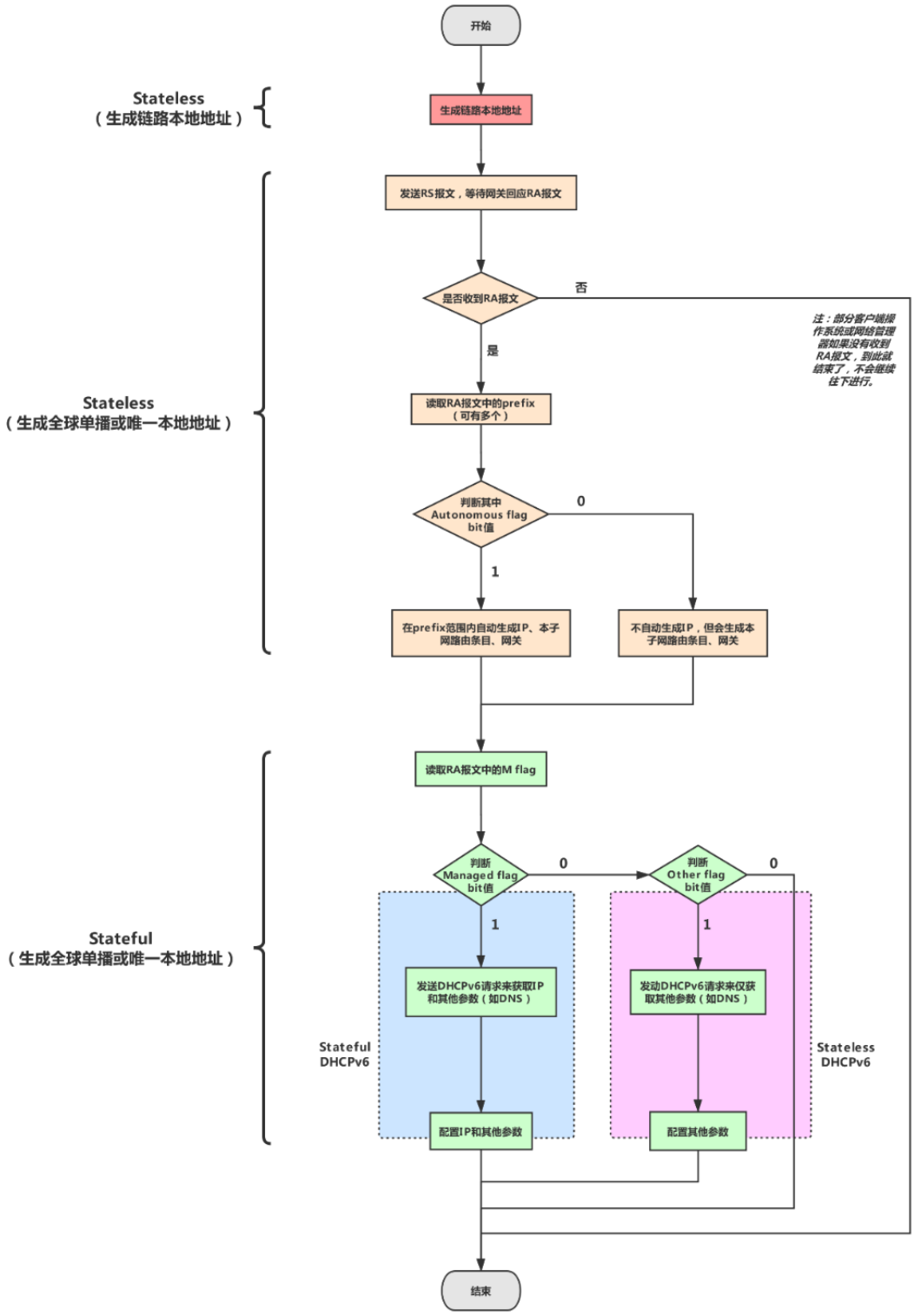

图 7 自动配置过程详解[3]

4.3 IPv6 地址解析

在 IPv4 中，当主机需要和目标主机通信时，需要先通过 ARP 协议获得目的主机的 MAC 地址。IPv6 采用邻居发现协议实现了这个功能，通过邻居请求报文 NS 和邻居通告报文 NA 来解析三层地址对应的链路层地址。

需要注意的是，地址解析使用的是 NS 与 NA，路由发现使用 RA 与 RS。

IPv6 主机地址解析的过程如图 8 所示：

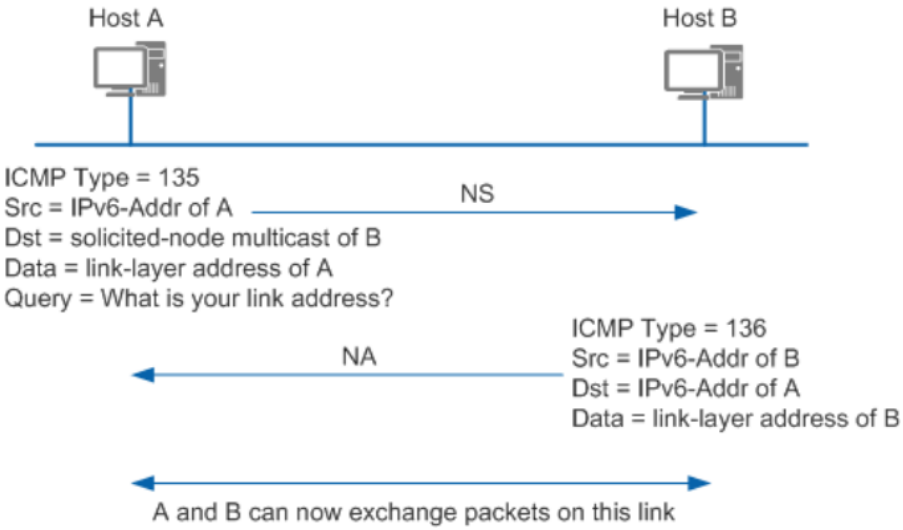

图 8 IPv6 地址解析过程

4.3.1 邻居请求报文（Neighbor Solicition）

Type	Code	checksum
Reserved		
Target Address		
Options...		

图 9 NS 报文格式

Type=135,code=0

Target Address 是需要解析的 IPv6 地址，因此该处不准出现组播地址。

Option 中携带了一个自己源的 MAC 地址

4.3.2 邻居通告报文（Neighbor Advertisement）

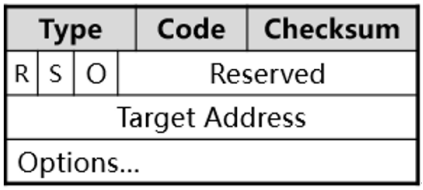

图 10 NA 报文格式

Type=136，Code=0

R 路由器标记（Router flag）。表示发送者是否为路由器

S 请求标记（Solicited flag）。表示发送邻居通告是否是响应某个邻居请求

O 替代标记（Overide flag）。表示邻居通告中的消息是否覆盖已有条目信息

Target Address 表示所携带的链路层地址对应的 IPv6 地址

Options 携带了自己作为源的 MAC 地址

4.3.3 对比与优点

IPv6 的地址解析过程 NS 报文在地址解析中的作用类似于 IPv4 中的 ARP 请求报文，NA 报文在地址解析中的作用类似于 IPv4 中的 ARP 应答报文。

相对 IPv4，IPv6 的地址解析有了以下变化：

[1] 不再使用 ARP，也不在使用广播方式，而是使用组播进行发送

[2] 地址解析在三层完成，针对不同的链路层协议可以采用相同的地址解析协议

由此，IPv6 的地址解析具有如下优点：

[1] 采用组播的方式发送 NS 消息更加高效，也减少了二层网络的性能压力

[2] 可以使用三层的安全机制（例如 IPSec）避免地址解析攻击

4.3.4 报文抓包解析

拓扑如图 11：

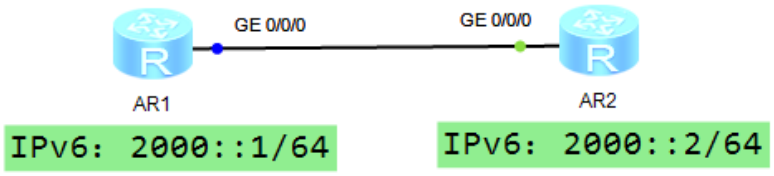

图 11 地址解析拓扑示例

首先在两端各配上 IPv6 地址，然后在 AR1 上 ping ipv6 -a 2000::1 2000::2。抓包如图 12：

No.	Time	Source	Destination	Protocol	Length	Info
1	1970/01…	2000::1	ff02::1:ff00:2	ICMPv6	86	Neighbor Solicitation for 2000::2 fr…
2	1970/01…	2000::2	2000::1	ICMPv6	86	Neighbor Advertisement 2000::2 (rtr,…
3	1970/01…	2000::1	2000::2	ICMPv6	118	Echo (ping) request id=0xd2ab, seq=2…
4	1970/01…	2000::2	2000::1	ICMPv6	118	Echo (ping) reply id=0xd2ab, seq=256…
5	1970/01…	2000::1	2000::2	ICMPv6	118	Echo (ping) request id=0xd2ab, seq=5…
6	1970/01…	2000::2	2000::1	ICMPv6	118	Echo (ping) reply id=0xd2ab, seq=512…
7	1970/01…	2000::1	2000::2	ICMPv6	118	Echo (ping) request id=0xd2ab, seq=7…
8	1970/01…	2000::2	2000::1	ICMPv6	118	Echo (ping) reply id=0xd2ab, seq=768…
9	1970/01…	2000::1	2000::2	ICMPv6	118	Echo (ping) request id=0xd2ab, seq=1…
…	1970/01…	2000::2	2000::1	ICMPv6	118	Echo (ping) reply id=0xd2ab, seq=102…
…	1970/01…	2000::1	2000::2	ICMPv6	118	Echo (ping) request id=0xd2ab, seq=1…
…	1970/01…	2000::2	2000::1	ICMPv6	118	Echo (ping) reply id=0xd2ab, seq=128…
…	1970/01…	fe80::2e0:fc…	2000::1	ICMPv6	86	Neighbor Solicitation for 2000::1 fr…
…	1970/01…	2000::1	fe80::2e0:fcff:fedc:…	ICMPv6	86	Neighbor Advertisement 2000::1 (rtr,…

图 12 ping ipv6 -a 2000::1 2000::2 抓包

①AR1 会以 2000::1（R1 的 IPv6 地址）作为源地址，目标地址为 2000::2（R2 的被请求节点组播地址）发送 NS 邻居请求报文，请求节点组播地址 ff02::1:ff00:2。然后将 AR1 的 MAC 地址携带在 ICMPv6 的 Option 中。

NS 报文内容如图 13：

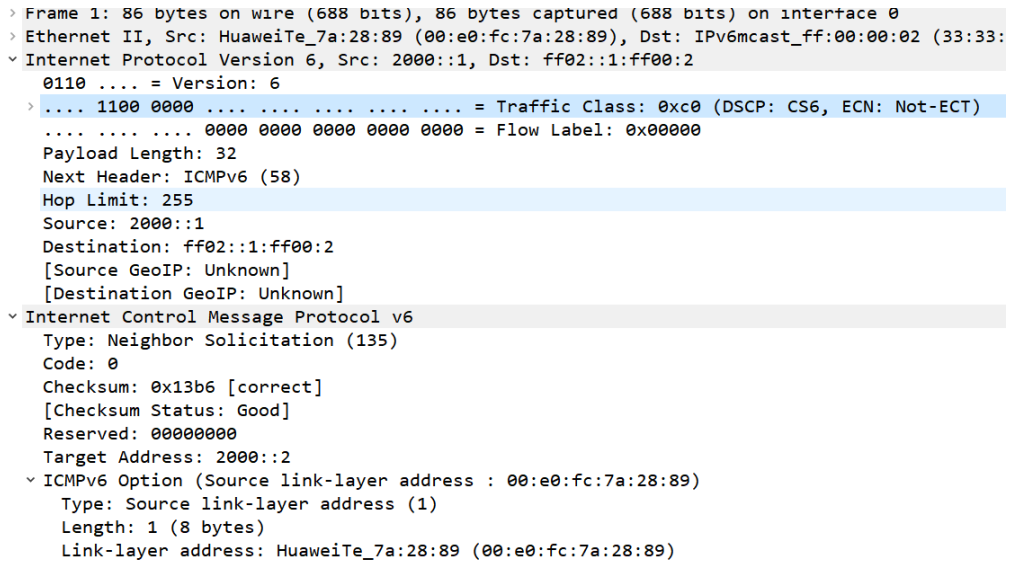

图 13 第一个 NS 报文

②当 AR2 收到 AR1 发送的 NA 报文后，检查 Target Address 字段并接收，并将对端的 IP 地址和 MAC 地址绑定到自己的邻居表中。然后以自己 IPv6 地址 2000::2 为源地址，2000::1 为目的地址回应 NA 报文。并将自己的 MAC 地址封装在 ICMPv6 的 Option 中，发送给对方，这样就完成了一个地址解析的过程[4]

NA 报文内容如图 14：

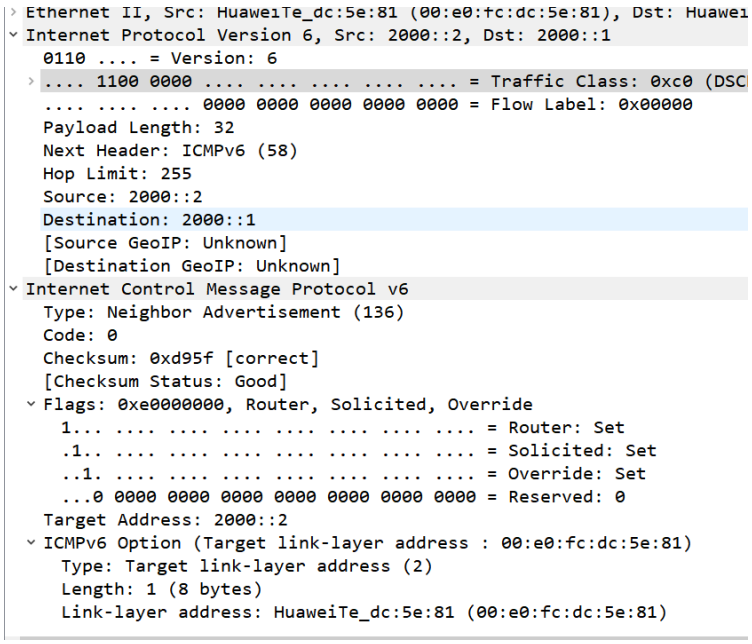

图 14 NA 报文抓包

4.4 DAD 重复地址检测

4.4.1 简介

重复地址检测 DAD（Duplicate Address Detect）是在接口使用某个 IPv6 单播地址之前进行的，为了探测是否有其它的节点使用了该地址。

一个 IPv6 单播地址在分配给一个接口之后且通过重复地址检测之前称为试验地址（Tentative Address）。此时该接口会加入两个组播组：ALL-NODES 组播组和试验地址所对应的 Solicited-Node 组播组。

4.4.2 通信过程

IPv6 主机重复地址检测的过程如图 15 所示：

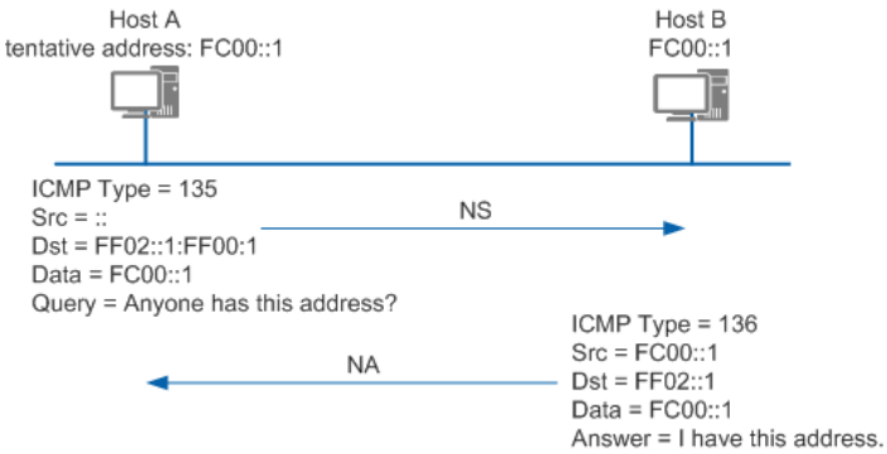

图 15 重复地址检测原理

Host A 的 IPv6 地址 FC00::1 为新配置地址，Host A 向 FC00::1 的 Solicited-Node 组播组发送一个以 FC00::1 为请求的目标地址的 NS 报文进行重复地址检测。当 Host B 收到该 NS 报文后，有两种处理方法：

1.如果 Host B 发现 FC00::1 是自身的一个试验地址，则 Host B 放弃使用这个地址作为接口地址，并且不会发送 NA 报文。

2.如果 Host B 发现 FC00::1 是一个已经正常使用的地址，Host B 会向 FF02::1 发送一个 NA 报文，该消息中会包含 FC00::1。这样，Host A 收到这个消息后就

会发现自身的试验地址是重复的。Host A 上该试验地址不生效，被标识为 duplicated 状态。

4.4.3 冲突检测

当两端同时检测时情况如图 16：

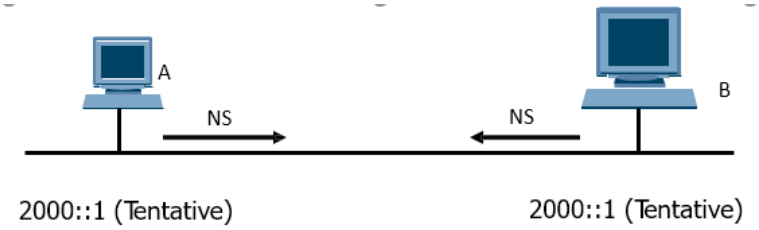

图 16 两端同时进行检测的情况

1.若 2 个节点配置相同地址，同时作重复地址检测时，一方收到对方发出的 DAD NS，则接收方将不启用该地址

2.一种极端的情况，如果同时收到 NS 报文，则两端都放弃改地址

4.4.4 抓包分析

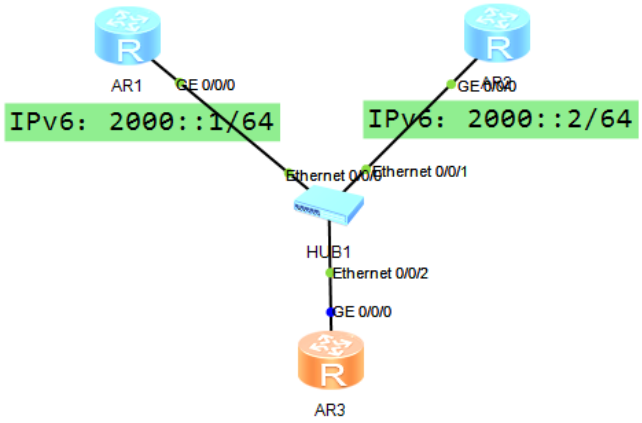

图 17 地址冲突检测拓扑

当在 AR3 上配置 2000::1/64 地址时，AR3 首先会以 :: 为源地址，以自己配置的 2000::1 为目的地址，发送 NS 报文。如果有来自 2000::1 的 NA 回复，则该地址不能用。如果没收到，则该地址可以使用。

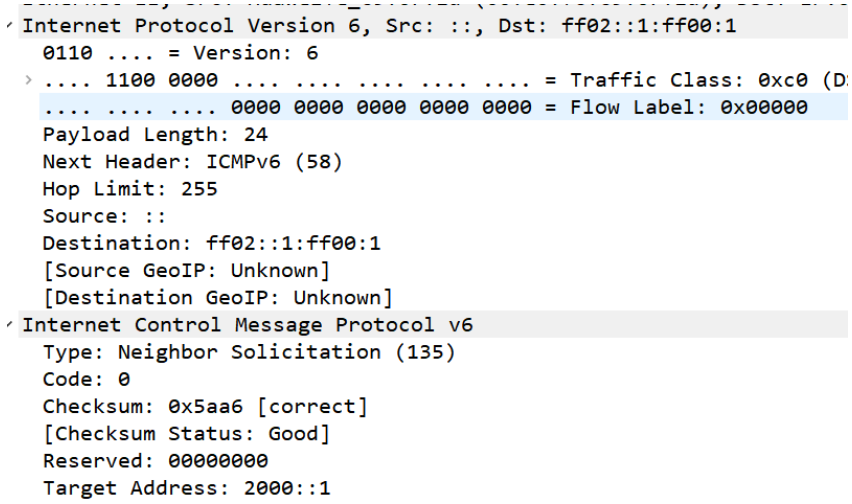

图 18 重复地址检测 NS 报文

在这个报文中因为 AR1 上已经使用了 2000::1/64 地址，所以会回复一个 NA。如图 19：

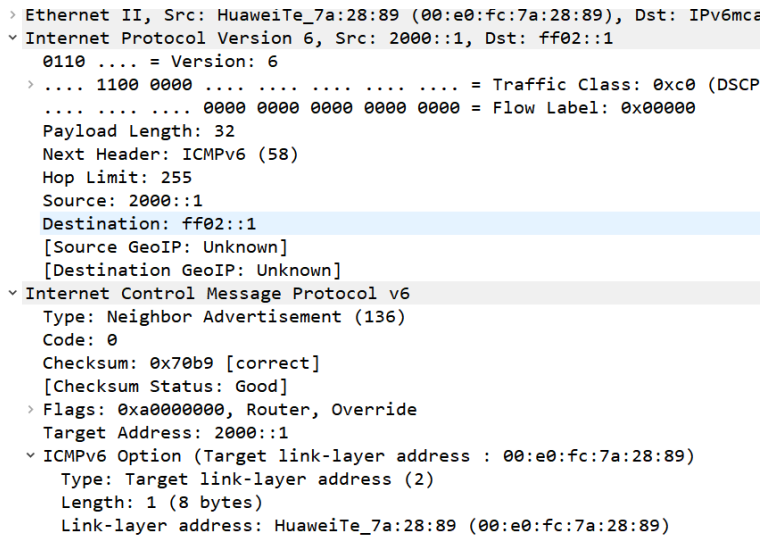

图 19 AR1 回复的 NA

4.5 邻居状态跟踪

NDP 的一个重要特征是检测同一链路上以前相连通的两个节点现在是否依然连通，这是通过 NUD（Neighbor Unreachability Detection，邻居不可达检测）完成的。NUD 帮助维护多个邻居条目组成的邻居缓存，每个邻居都有相应的状态，状态之间可以迁移。

4.5.1 五种邻居状态

- **未完成(Incomplete)**：表示正在解析地址，但邻居链路层地址尚未确定。
- **可达(Reachable)**：表示地址解析成功，该邻居可达。
- **陈旧(Stale)**：表示可达时间耗尽，未确定邻居是否可达。
- **延迟(Delay)**：邻居可达性未知。Delay 状态不是一个稳定的状态，而是一个延时等待状态。
- **探测(Probe)**：邻居可达性未知,正在发送邻居请求探针以确认可达性。

```
[AR1]dis ipv6 neighbors
--------------------------------------------------------------------------
IPv6 Address : 2000::2
Link-layer   : 00e0-fcdc-5e81                    State : STALE
Interface    : GE0/0/0                           Age   : 2
VLAN         : -                                 CEVLAN: -
VPN name     :                                   Is Router: TRUE
Secure FLAG  : UN-SECURE

IPv6 Address : FE80::2E0:FCFF:FEDC:5E81
Link-layer   : 00e0-fcdc-5e81                    State : STALE
Interface    : GE0/0/0                           Age   : 2
VLAN         : -                                 CEVLAN: -
VPN name     :                                   Is Router: TRUE
Secure FLAG  : UN-SECURE

--------------------------------------------------------------------------
Total: 2        Dynamic: 2        Static: 0
```

图 20 IPv6 邻居状态

4.5.2 邻居状态迁移

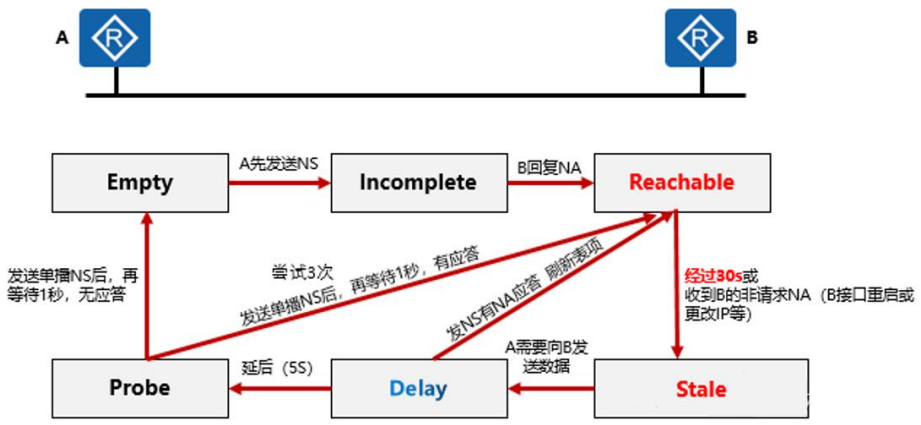

图 21 邻居状态迁移图示

下面以 A、B 两个邻居节点之间相互通信过程说明邻居状态迁移的过程。

1. A 先发送 NS 报文，并生成缓存条目

2. 若 B 回复 NA 报文，则邻居状态由 Incomplete 变为 Reachable。

3. 经过邻居可达时间（默认 30s），邻居状态由 Reachable 变为 Stale，即未知是否可达。如果 A 收到 B 的非请求 NA 报文（MAC 地址修改），且报文中携带的 B 的链路层地址和表项中不同，则邻居状态马上变为 Stale。

4. 若 A 要向 B 发送数据，则邻居状态由 Stale 变为 Delay，并发送 NS 请求。

5. 在经过一段固定时间后，邻居状态由 Delay 变为 Probe，其间若有 NA 应答，则邻居状态由 Delay 变为 Reachable。

6. 在 Probe 状态，A 每隔一秒发送单播 NS，有应答则邻居状态变为 Reachable，否则邻居状态变为 Empty，即删除表项。

从以上的机制可以看出 IPv6 的邻居关系优于 IPv4 的 ARP，IPv6 的邻居关系维护机制确保通讯发起之前邻居是可达的，而 ARP 本身是做不到的，仅仅通过老化机制来实现。

4.5.3 ARP 对比与特点

IPv6 的邻居关系维护机制确保通讯发起之前邻居是可达的，而 ARP 本身是做不到的，仅仅通过老化机制来实现。

4.6 重定向过程

当网关路由器知道更好的转发路径时，它就会发送重定向报文告知报文的发送者，让报文发送者选择另一个网关设备。重定向报文也承载在 ICMPv6 报文中，其 Type 字段值为 137，报文中会携带更好的路径下一跳地址和需要重定向转发的报文的目的地址等信息。（和 IPv4 机制相同）

4.6.1 重定向报文的结构

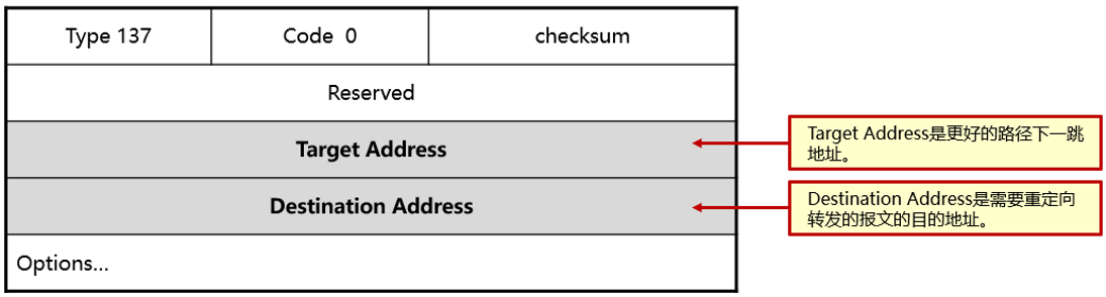

图 22 重定向报文结构

4.6.2 重定向过程示例

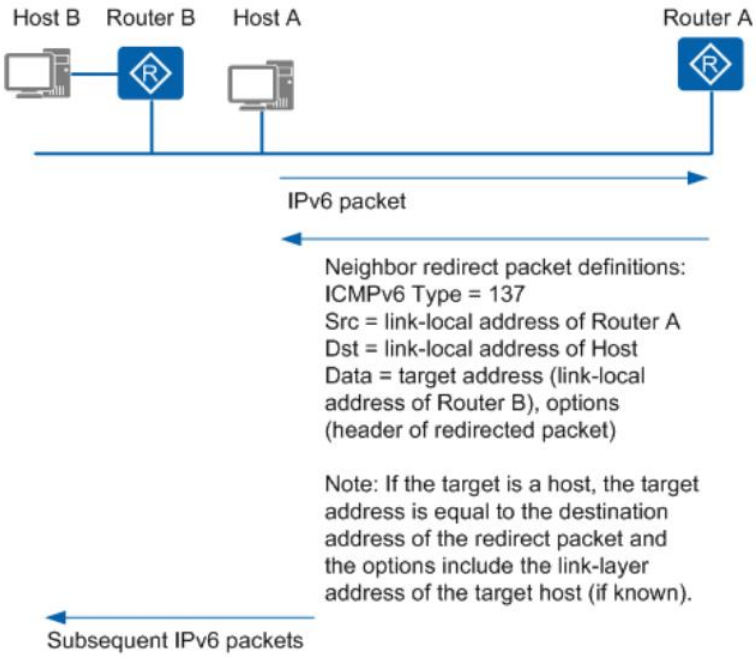

图 23 重定向过程示例

5 NDP 攻防

由于 NDP 协议在 IPv6 网络中具有重要作用，因此攻击者可能会利用 NDP 协议来进行攻击。常见的 NDP 攻击包括欺骗攻击、洪泛攻击和剥夺攻击等。[1]

欺骗攻击是指攻击者伪造一个 IPv6 地址和 MAC 地址，发送一个虚假的邻居通告数据包，将虚假的邻居信息存储到目标 IPv6 节点的邻居缓存中，从而实现对目标 IPv6 节点的欺骗和控制。

洪泛攻击是指攻击者向 IPv6 网络中广播大量的 NDP 数据包，从而占用网络带宽和资源，导致网络拥塞和瘫痪。

剥夺攻击是指攻击者通过不断发送虚假的路由通告数据包，将合法的路由信息从路由缓存中逐出，从而导致网络通信受阻和中断。

为了防止 NDP 攻击，IPv6 节点可以采取多种安全措施，包括开启安全防护功能、限制 NDP 数据包的发送和接收、使用加密通信和认证机制等。[5]

6 结论

NDP 协议是 IPv6 网络中的重要协议，它提供了邻居发现、邻居缓存和路由缓存等功能，为 IPv6 网络的通信提供了基础支撑。然而，NDP 协议也存在着安全风险和攻击威胁，因此需要采取有效的安全措施来保护 IPv6 网络的安全和稳定。未来，随着 IPv6 网络的普及和发展，NDP 协议将继续发挥重要作用，并不断演进和完善，以适应新的网络环境和应用场景。

主要参考文献

[1]杨志刚,张长河，祝跃飞.IPv6 邻居发现协议安全机制研究[J]. 计算机应用,2006,26(4): 938.

[2] IPv6 基础知识 https://blog.csdn.net/ttood/article/details/118528246

[3] 初识 IPv6 有状态、无状态地址相关协议

https://blog.csdn.net/u011029104/article/details/119427279

[4] GHAITHM H A,FIRAS Q K,AHMED K, et al. Denial of service attack on neighbor discovery protocol processes in the network of IPv6 link-local[J].International Journal of Electrical and Electronic Engineering and Telecommunications，2020，9(4):247.

[5] 崔北亮,岳阳.IPv6 中邻居发现协议剖析及攻防探索[J].南京工业大学学报 (自然科学版),2021,43(06):746-754.

[6] 一文解释 NDP 协议（IPv6 邻居发现协议）&ICMPv6

https://blog.csdn.net/qq_33162707/article/details/124625008