下一代Internet技术与协议

张冬梅
北京邮电大学 计算机学院
zhangdm@bupt.edu.cn

4.2 IPv6邻居发现（NDP）

- 4.2.1 概述
  - 4.2.1.1 NDP简介
  - 4.2.1.2 NDP基本功能
- 4.2.2 协议报文格式
  - 4.2.2.1 报文选项
  - 4.2.2.2 路由器请求与路由器公告报文
  - 4.2.2.3 邻居请求与邻居公告报文
  - 4.2.2.4 重定向报文
- 4.2.3 IPv6地址解析
- 4.2.4 无状态地址自动配置
- 4.2.5 重定向

4.2.1.1 NDP简介(1)

- 邻居发现协议NDP(Neighbor Discovery Protocol)是IPv6的一个关键协议
  - 综合了IPv4的一些协议并做了改进,还提供一些非常重要的功能
- 作用：确定邻居节点之间的关系，是单播通信的关键服务
- NDP在第三层上实现

IPv4 ARP协议报文

IPv6 ND协议报文

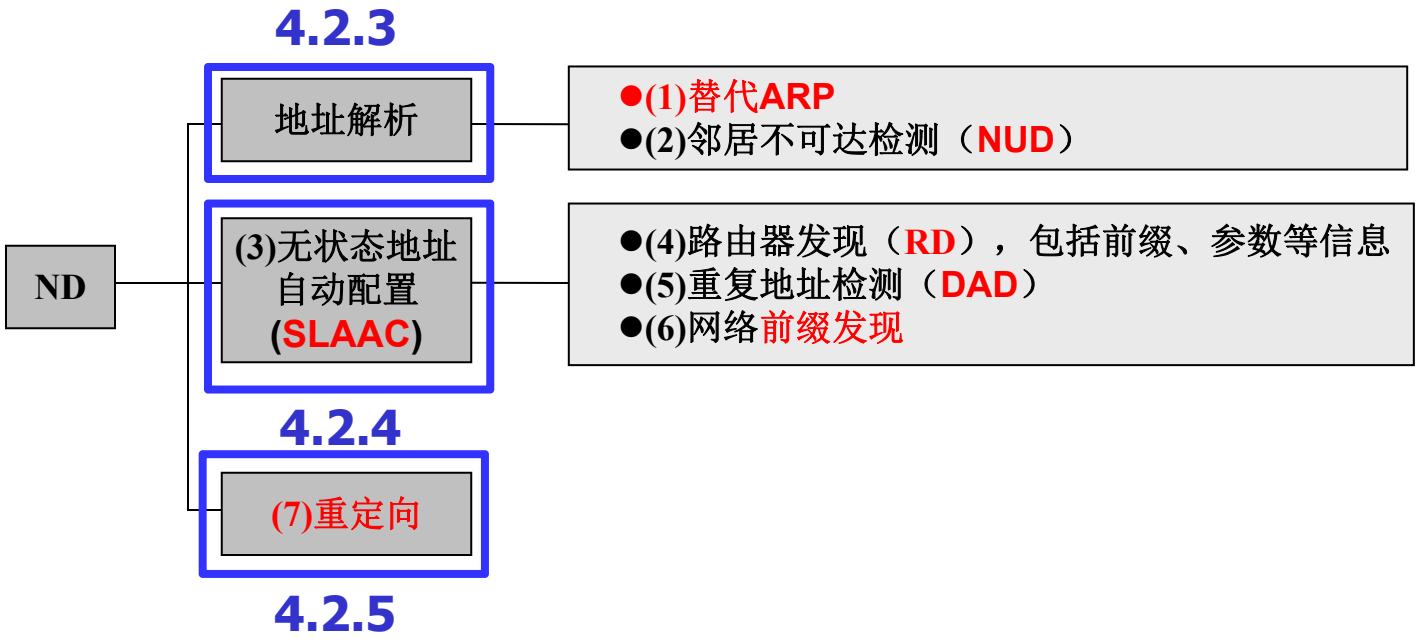
- SEND(SEcure Neighbor Discovery,RFC3971)是安全邻居发现协议，增加了认证等安全功能

NDP简介(2)

- 节点使用NDP
  - 解析下一跳邻居节点的链路层地址（**地址解析**）
  - 确定邻居节点是否可达（**邻居检测**）
  - 优化主机路由表（**路由优化**）
- 主机使用NDP
  - 发现邻居路由器（**网络发现**）
  - 自动配置地址、网络前缀、路由及其他网络参数（**地址配置**）
- 路由器使用NDP
  - 通告自己的存在、网络配置参数、路由以及链路前缀（**网络发现**）

4.2.1.2 NDP功能

- 基本功能



NDP概述

- IPv6主机维护的缓存信息(soft state)
  - 邻居节点缓存：维护最近通信的邻居的信息

邻居状态

邻居节点缓存		
下一跳地址	链路层地址	可达性状态

  - 目的地缓存：维护最近通信的目的地节点的下一跳IP地址

路由状态

目的缓存		
目的地址	下一跳地址	PMTU

NDP概述

- IPv6主机维护的缓存信息(soft state)
  - 前缀列表：包含链路上（on-link）前缀，是根据路由器使用RA通告的前缀而生成出来的
  - 默认路由器列表：包含RA中（on-link）路由器对应的IP地址，以及可以成为默认路由器的链路中（on-link）路由器的对应IP地址。

网络状态

网络前缀列表	默认路由器列表

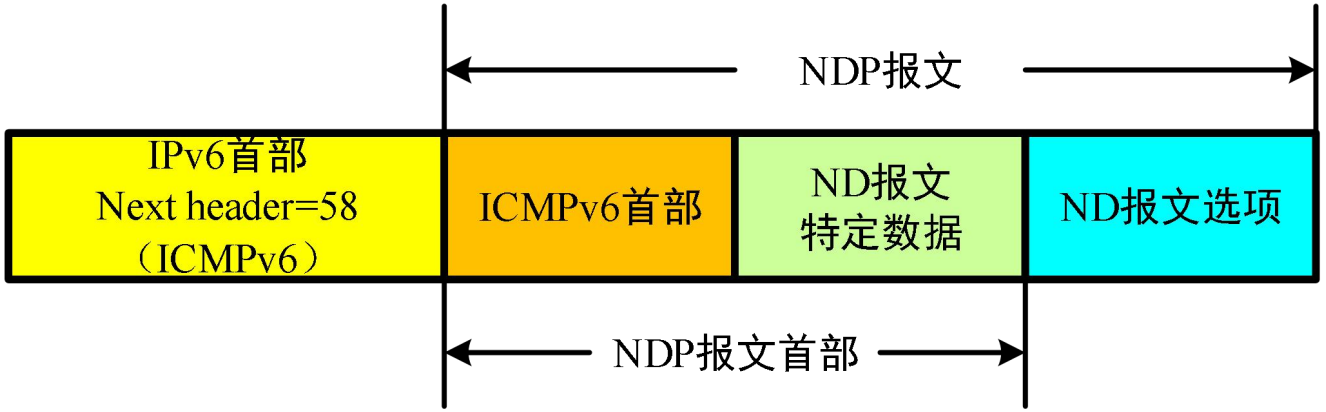
4.2.2 NDP协议报文

- ND协议使用ICMPv6报文类型

ICMPv6类型	消息名称
Type ＝ 133	RS －（Router Solicitation，路由器请求）
Type ＝ 134	RA －（Router Advertisement，路由器公告）
Type ＝ 135	NS －（ Neighbor Solicitation，邻居请求）
Type ＝ 136	NA －（ Neighbor Advertisement，邻居公告）
Type ＝ 137	Redirect －（重定向消息）

邻居发现协议报文

- IPv6首部+邻居发现报文首部+报文选项



- ND报文的IPv6首部的“跳数限制”设置为255

问题：为什么设为255而不是设为0？

4.2.2.1 邻居发现协议报文选项

- 邻居发现选项
  - 格式：采用类型-长度-值(TLV)格式

类型(8bit)	长度(8bit)	值(长度可变)

类型	选项名称
1	源链路层地址
2	目标链路层地址
3	前缀信息
4	被重定向首部
5	MTU
7	通告间隔
8	家乡代理信息
24	路由信息(MIPv6相关)

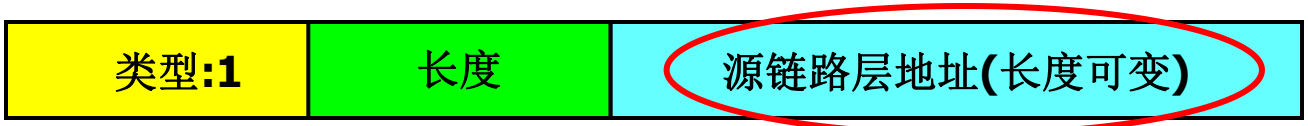
邻居发现协议报文选项

- 邻居发现选项与邻居发现报文的对应关系

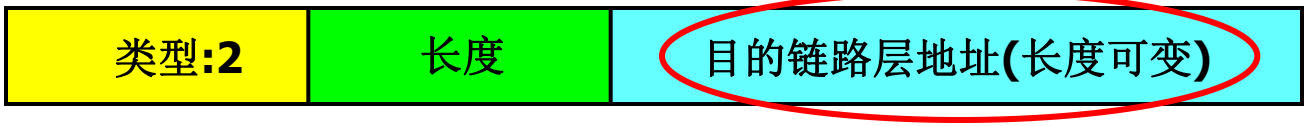
邻居发现报文	邻居发现报文选项
路由器请求RS	源链路层地址
路由器公告RA	源链路层地址、MTU、前缀信息 通告间隔、家乡代理信息、路由信息(MIPv6相关)
邻居请求NS	源链路层地址
邻居通告NA	目标链路层地址
重定向	目标链路层地址、被重定向首部

邻居发现协议的选项

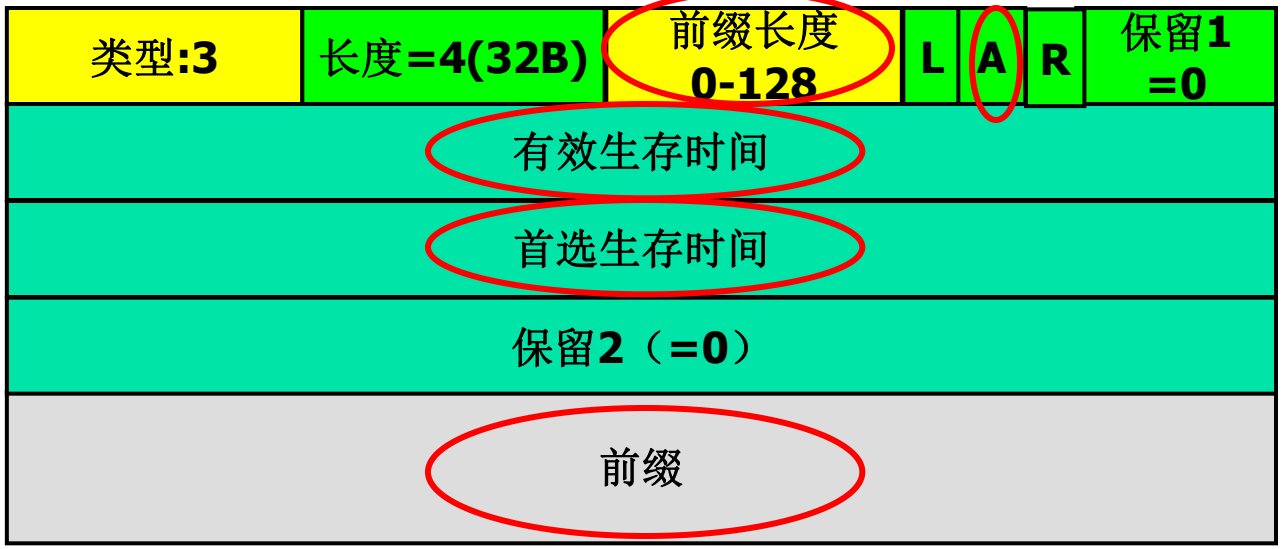
- 源链路层地址选项: 发送者的链路层地址



- 目的链路层地址选项： 目标链路层地址

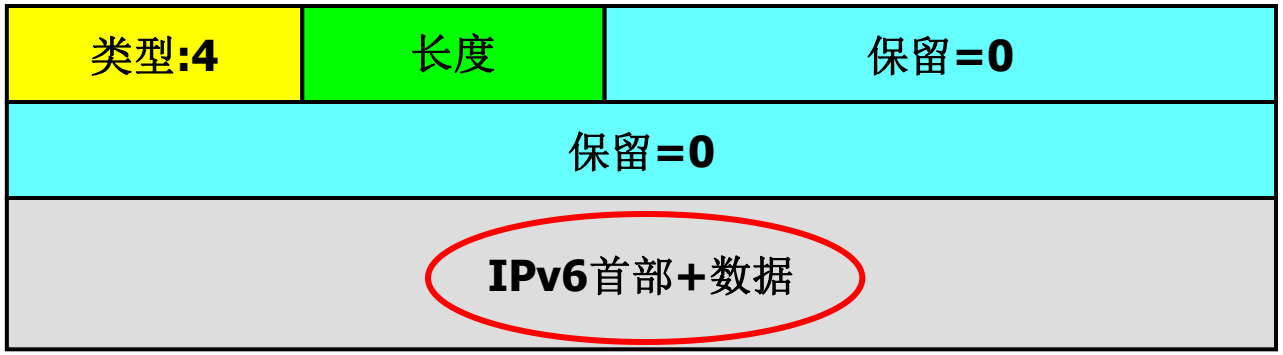


- 前缀信息选项： 一个IPv6前缀或者地址

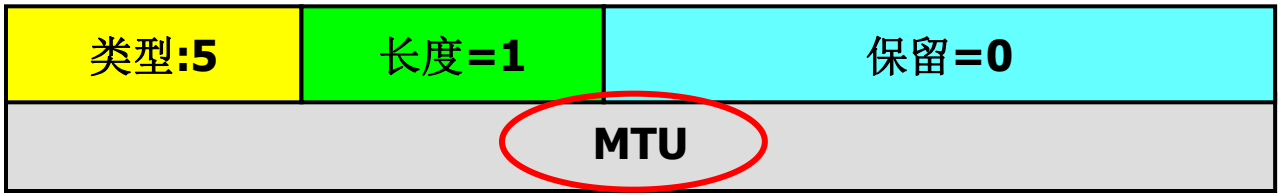


邻居发现协议的选项

- 被重定向首部：原始IPv6报文的部分

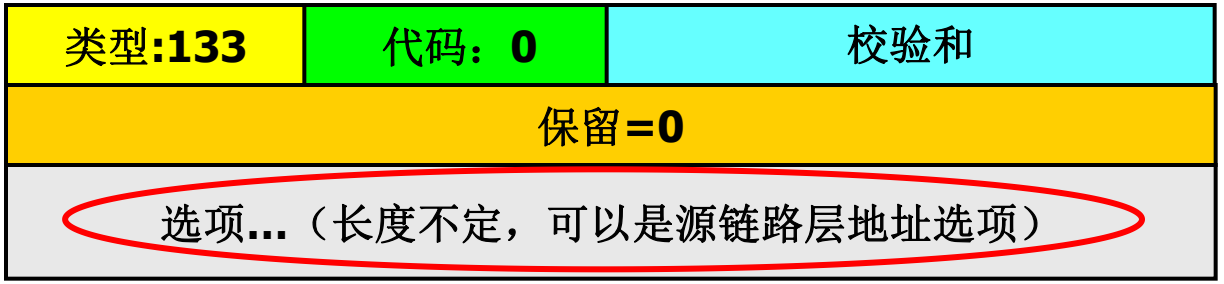


- MTU选项：推荐的MTU，确保链路上所有节点使用相同的MTU



4.2.2.2 路由器请求与公告报文

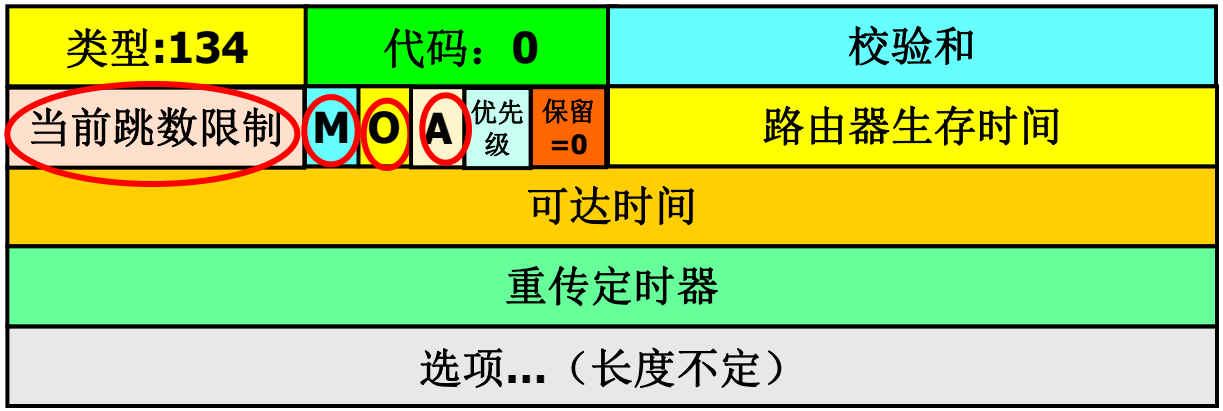
- 路由器请求RS/路由器通告RA
- 功能：主机用来查找与本网连接的路由器，表明路由器的存在及其功能
- RS



  - 源IP地址： 链路本地IPv6地址/::
  - 目的IP地址： FF02::2
  - Hop limited：255; Next header: 58(ICMPv6)
  - 选项：发送方物理地址(源链路层地址选项)

路由器请求与公告

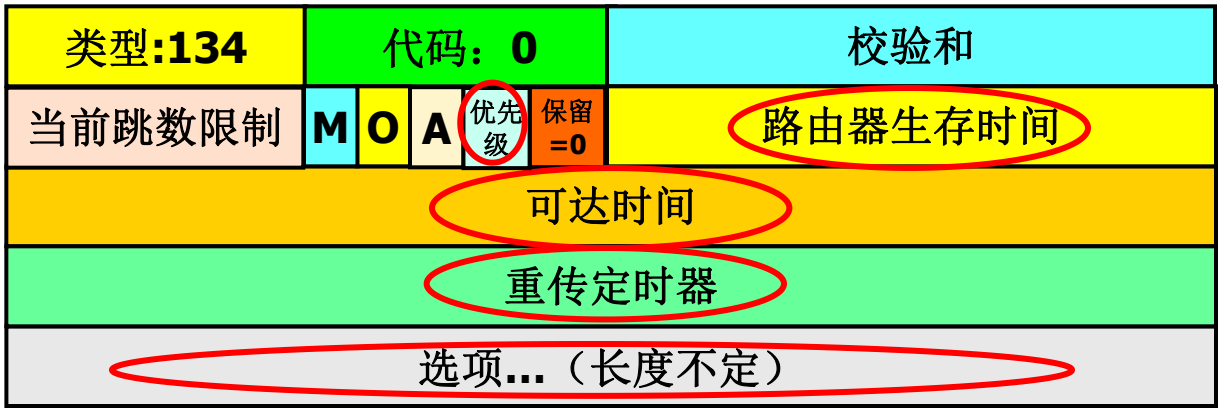
- RA
  - 源IP地址： 链路本地IPv6地址
  - 目的IP地址：FF02::1/发出请求报文的接口地址



  - 当前跳数限制
  - M=1，IPv6地址使用有状态的配置方式
  - O=1，除IPv6地址之外的网络信息也使用有状态配置
  - A=1，可以作为家乡本地代理(MIPv6使用)

路由器请求与公告

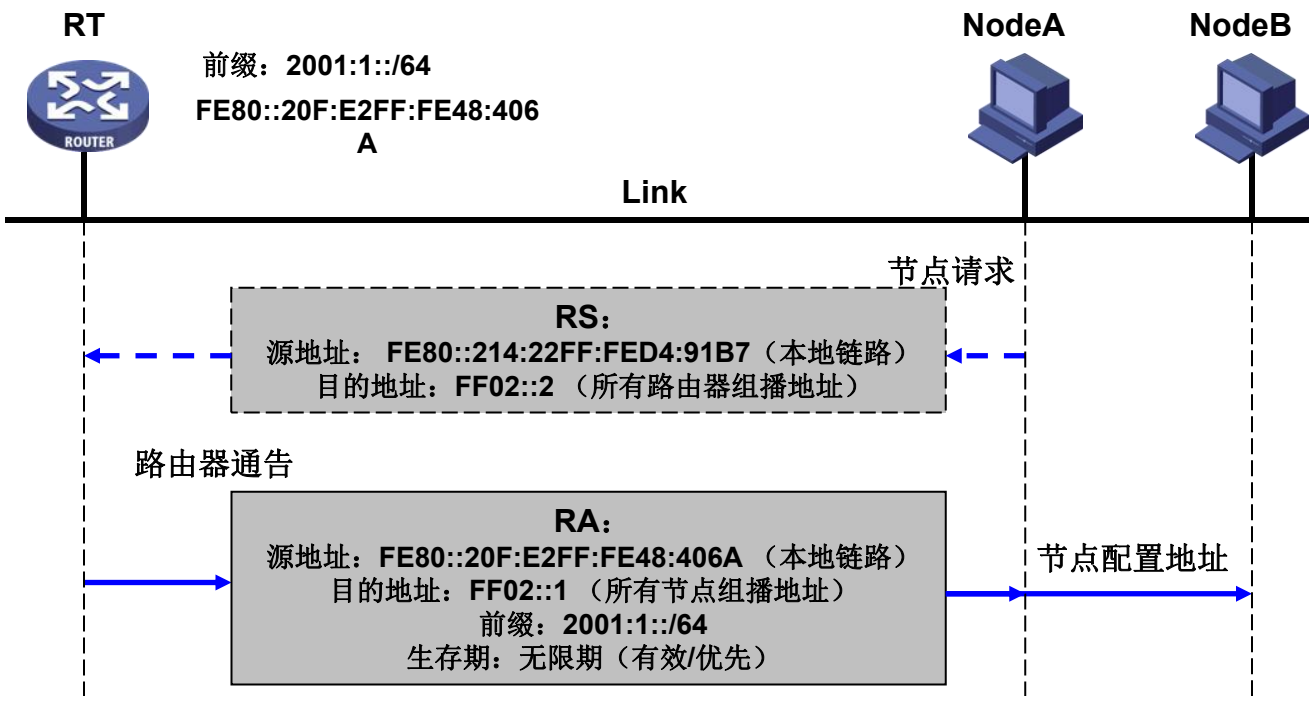
- RA



- 优先级(2bit)：01(高), 00(中), 11(低), 10(默认生存时间字段=0)
- 路由器生存时间
- 可达时间(ms)：邻居节点看作可达节点的时间
- 重传定时器(ms)
- 选项：源链路层地址、MTU、前缀信息、通告间隔、家乡代理信息、路由信息

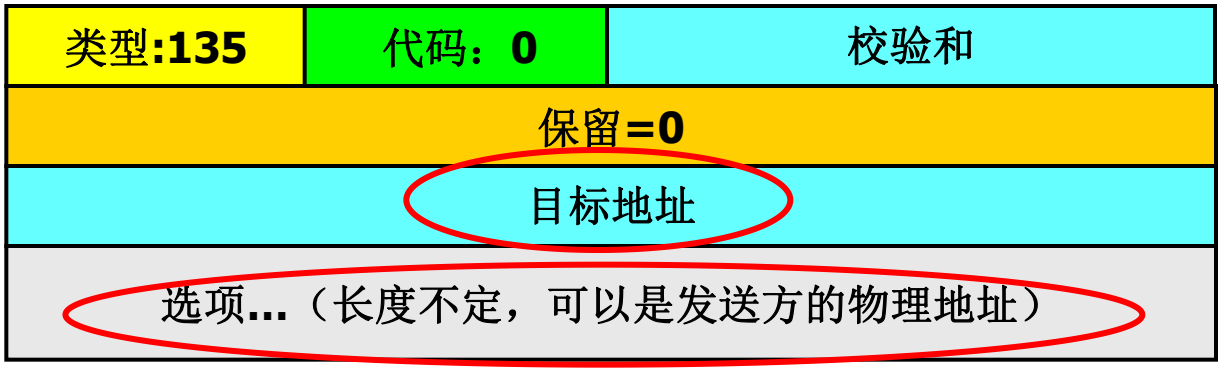
问题：主机收到RA消息后能够获得哪些配置参数？

主机请求触发路由器通告过程



4.2.2.3 邻居请求和邻居通告

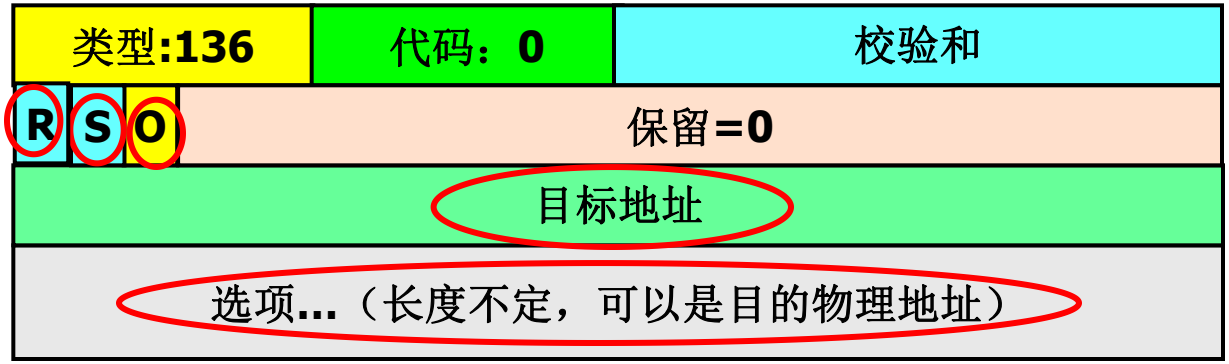
- 邻居请求NS/邻居通告NA
- 功能：实现地址解析、邻居不可达性检测和重复地址检测
- NS报文



- 源IP地址：接口单播IPv6地址/::(重复地址检测DAD)
- 目的IP地址：目标被请求节点组播地址/单播地址
- 目标(target)地址：被请求的IPv6单播地址
- 选项：发送方物理地址(源链路层地址)

邻居请求和邻居通告

- NA报文

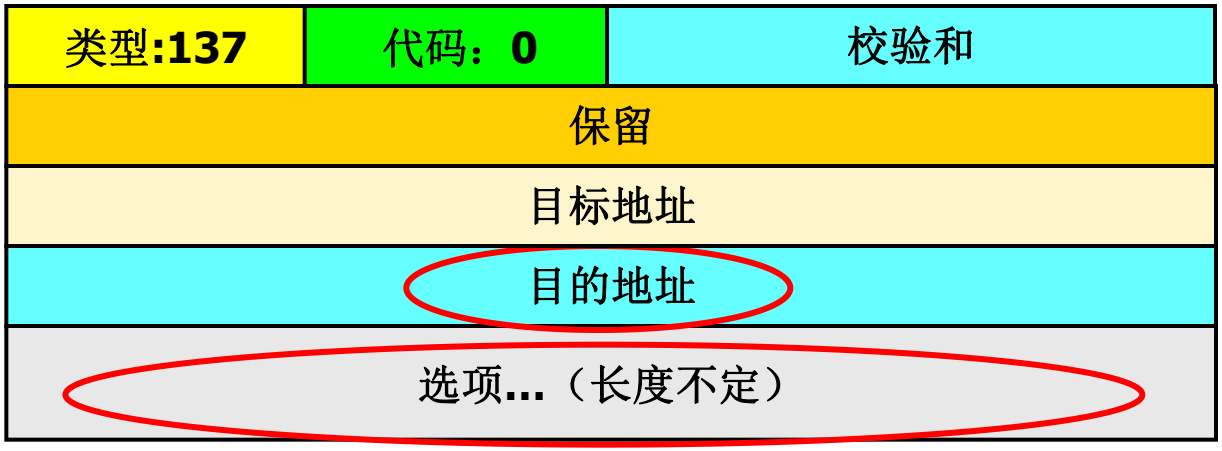


- 目的IP地址：　FF02::1/单播地址
- R：路由器标记，R=1，表示发送方为路由器；
- S：请求标记，S=1，表示NA是对NS消息进行的响应；
- O：覆盖标记，O=0，表示使用本消息的目标链路层地址覆盖邻居节点缓存条目中现存的链路层地址；
- 目标地址：被请求的IPv6地址
- 选项：目的结点物理地址(目的链路层地址)

什么时候节点会主动发送**NA**？

4.2.2.4 重定向

- 功能：优化主机路由表
- 报文格式

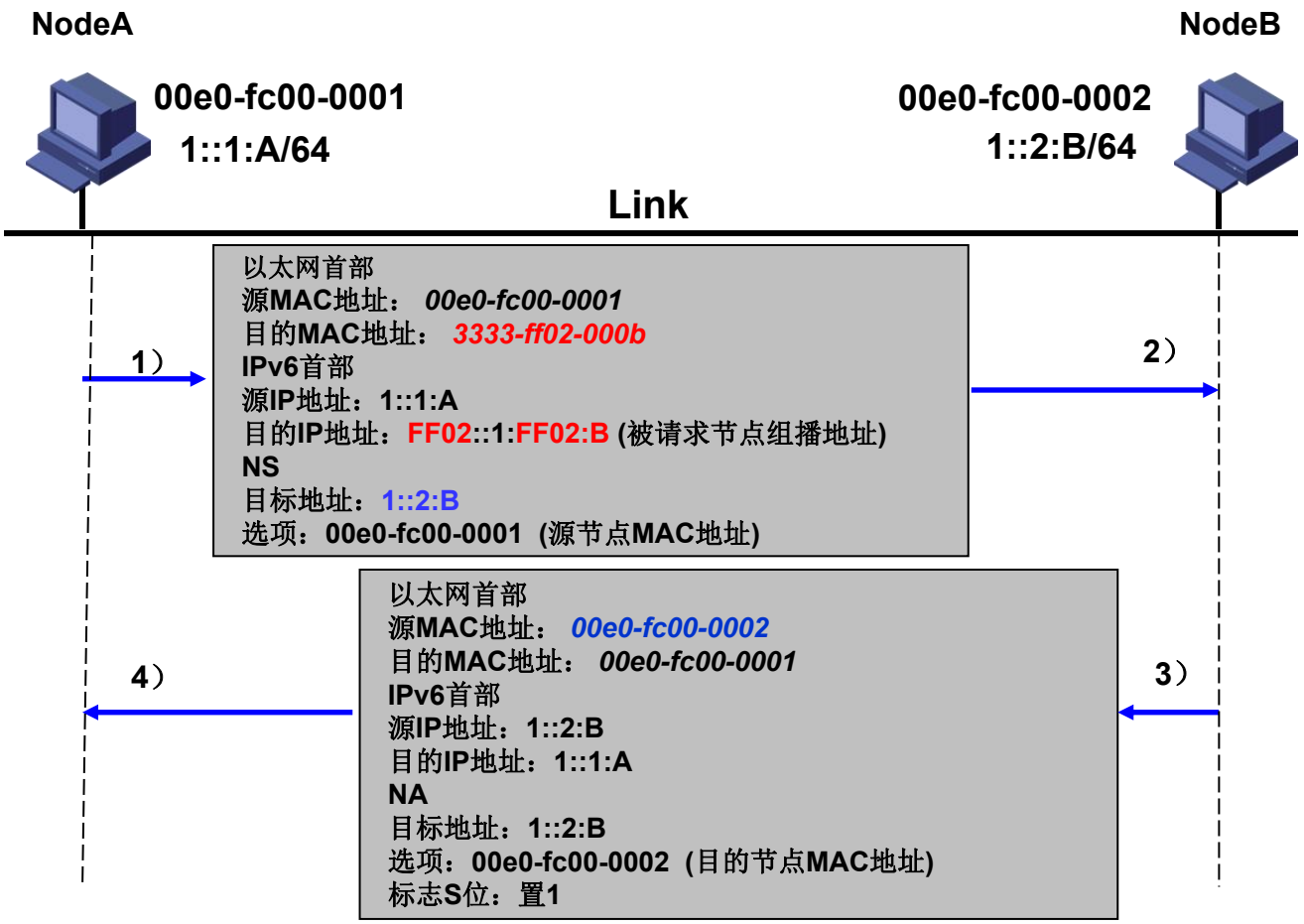


  - 源IP地址： 发送接口的链路本地IPv6地址
  - 目的IP地址： 触发重定向报文的IP数据报的源地址
  - 目标(Target)地址
    - 情况1：更好的第一跳路由器的链路本地地址
    - 情况2：与重定向消息的目的地址相同
  - 目的地址：触发重定向报文的IP数据报的目的地址
  - 选项：目标链路层地址、被重定向首部

4.2.3 IPv6地址解析

- 相关的功能
  - 地址解析（ARP功能）
  - 邻居状态检测（邻居不可达检测NUD）
- 使用NS和NA报文实现
- 源节点向本链路上的其他系统组播邻机请求需要解决的问题
  - 如何保证请求消息只限制在本链路范围内？
  - 如何尽量减少处理NS消息的系统个数，最好只有所请求的系统处理该消息

(1)IPv6地址解析过程



邻居发现协议与ARP协议的比较

- IPv6不再执行ARP，主要原因如下：
  - 没有必要为每个不同类型网络都重新构造ARP
- 三层实现地址解析的好处
  - 1)加强了地址解析协议与底层链路的独立性
  - 2)增强了安全性
  - 3) 减少二层网络的性能压力
- 邻居发现可以用于实现的其他目标
  - 1）链路层地址变化、2）入境负载均衡
  - 3）任播地址、4）代理通告

(2) 邻机不可达检测

- NUD(Neighbor Unreachability Detection)
- 功能：实时监视邻机状态，了解新的拓扑结构，用于管理每个节点上的邻居缓存的状态
- 基本方法
  - 上层协议监视（首选）
  - ICMP监视
    - 定期发送**邻机请求**（单播）给邻机最新的链路地址
    - 邻居发送邻居通告（单播）进行响应
    - 使用S比特位判断通信链路的双向性
    - 使用R比特位判断节点性质（是否具备路由功能）

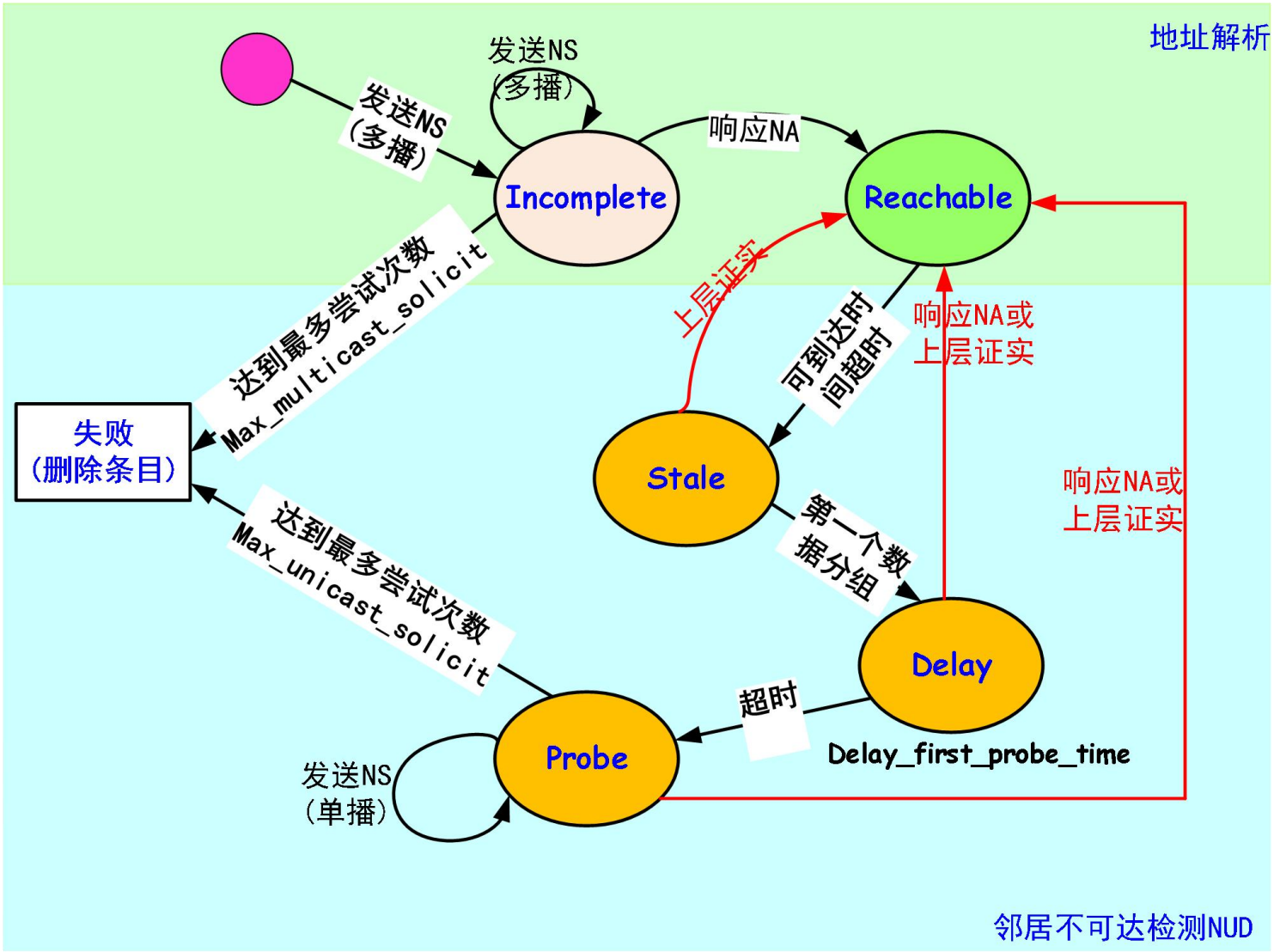
邻机不可达检测

- NUD是单向的
- 邻居缓存条目的状态

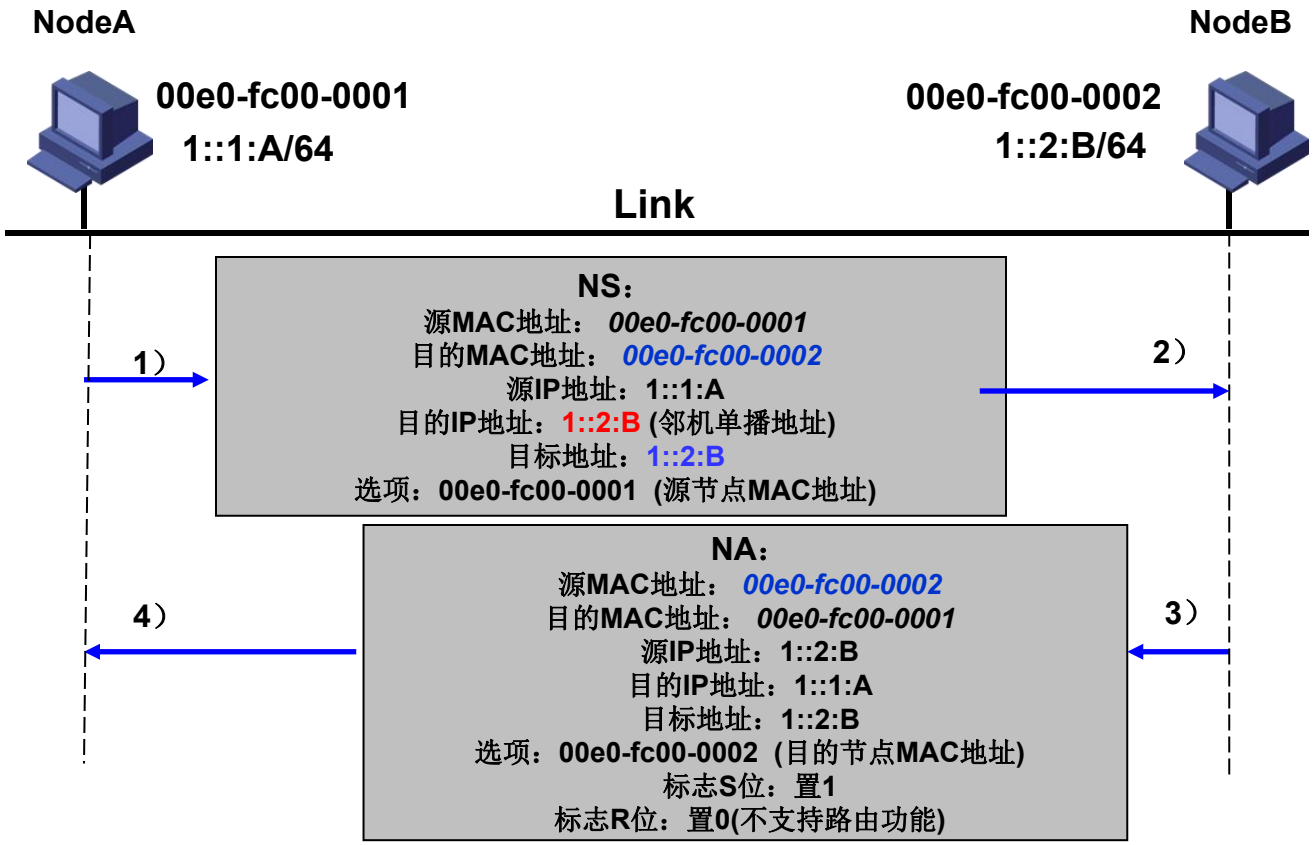
状态	说明
Incomplete（不完整的）	地址解析正在执行中
Reachable（可达到的）	邻居当前可达
Stale（过时的/失效的）	未确认的无效条目
Delay（延迟）	邻居的可达时间已经过期，等待上层协议的可达性确认
Probe（探测）	尝试发送NS（单播）获取可达性确认

  - Max-multicast-solicit(默认为3)
  - Max-unicast-solicit(默认为3)
  - Delay-first-probe-time(默认为5s)

邻机不可达检测


地址解析
发送NS
(多播)
发送NS
(多播)
响应NA
Incomplete
Reachable
达到最多尝试次数
Max_multicast_solicit
上层证实
可到达时
间超时
响应NA或
上层证实
失败
(删除条目)
Stale
响应NA或
上层证实
第一个数
据分组
达到最多尝试次数
Max_unicast_solicit
Delay
超时
Probe
Delay_first_probe_time
发送NS
(单播)
邻居不可达检测NUD

邻机不可达检测NUD

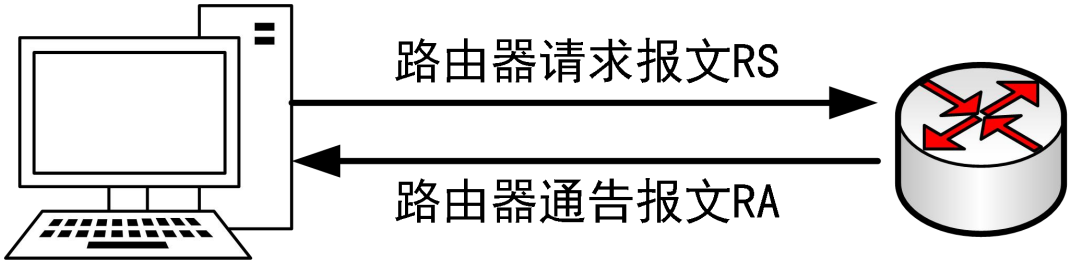

NodeA
NodeB
00e0-fc00-0001
1::1:A/64
00e0-fc00-0002
1::2:B/64
Link
NS：
源MAC地址： 00e0-fc00-0001
目的MAC地址： 00e0-fc00-0002
源IP地址：1::1:A
目的IP地址：1::2:B (邻机单播地址)
目标地址：1::2:B
选项：00e0-fc00-0001 (源节点MAC地址)
1）
2）
NA：
源MAC地址： 00e0-fc00-0002
目的MAC地址： 00e0-fc00-0001
源IP地址：1::2:B
目的IP地址：1::1:A
目标地址：1::2:B
选项：00e0-fc00-0002 (目的节点MAC地址)
标志S位：置1
标志R位：置0(不支持路由功能)
3）
4）

4.2.4 无状态地址自动配置

- 相关的功能
  - 路由器发现（RD）
  - 网络前缀发现、参数发现
  - 无状态地址自动配置(SLAAC)
  - 重复地址检测（DAD）
- 使用RS、RA、NS、NA报文实现

（1）路由器发现

- 主机发现路由器的两种方法
  - 等待路由器主动发送路由器公告
  - 主机进入网络后主动发送路由器请求报文



基本工作过程

- 笔记本电脑向Ethernet上的所有路由器组播路由器请求消息
  - 如何保证请求消息只限制在本链路范围内？
  - 如何确保只有路由器才响应该请求？
- 路由器接收该请求包
- 路由器向Ethernet上的所有主机通告自己的存在(或向请求节点告知自己的存在)
  - 如何确保向本链路上的所有主机广播？
- 主机收到路由器公告，在缓存中保存该路由器信息并调整自己的路由表配置

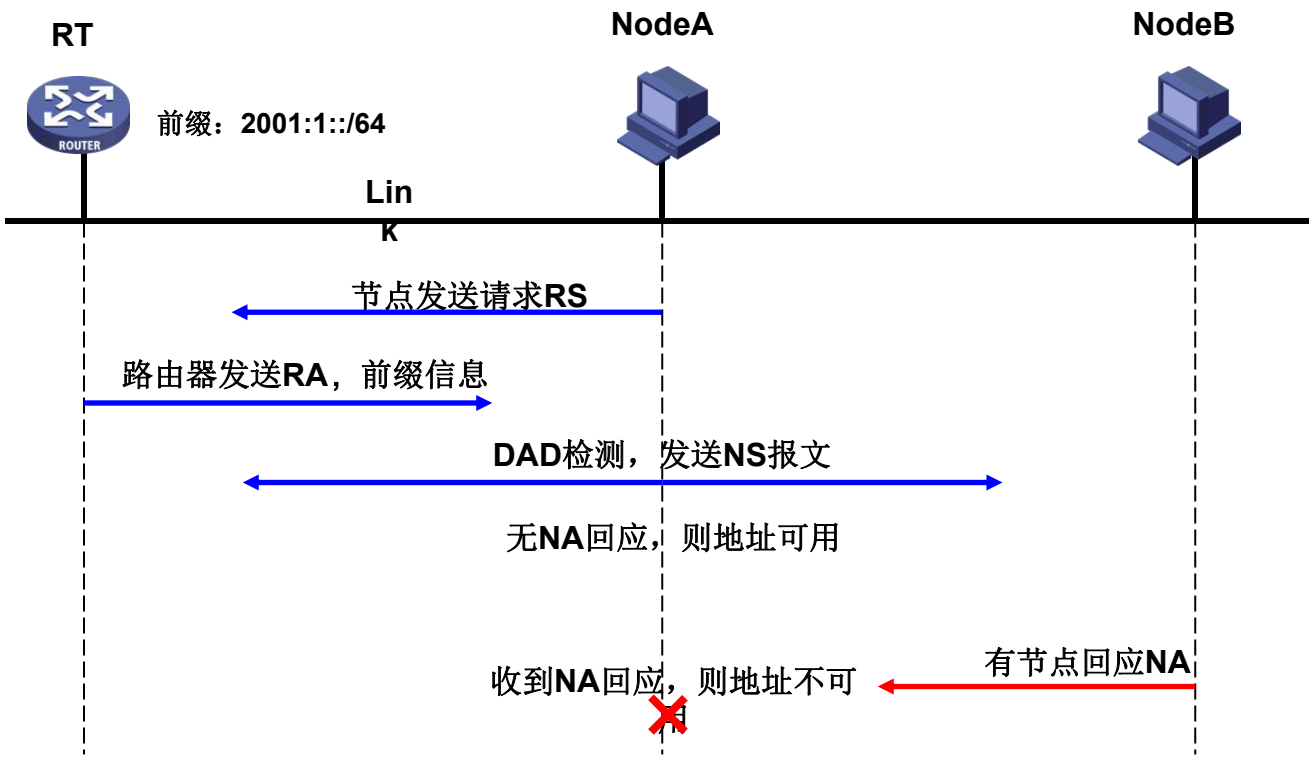
（2）无状态地址自动配置

- 无状态地址自动配置SLAAC(Stateless Address Auto-configuration)
- 功能：自动获得IP地址
- 条件：只有在支持多播的网络上才能实现，网络接口需要能够接收和发送多播分组
- 无状态地址自动配置主要适用于主机，路由器使用相同过程为其各接口产生并确认链路本地地址
- 过程
  - 主机为每个接口产生一个链路本
  - 主机探测现存的路由器

IPv6地址自动配置

- 原理：网络前缀+链路地址
  - 使用路由器公告报文RA中的地址前缀
  - 在没有路由器公告报文时使用链路局域地址
- 步骤
  - 创建链路本地单播：FE80::/10+EUI-64
  - 对链路本地单播地址执行DAD
  - 路由器公告消息提供地址配置信息，生成全局单播地址
  - 对全局单播地址执行DAD

无状态地址自动配置过程



（3）重复地址检测DAD

- 功能：检测无状态自动配置的IPv6地址是否与其他主机的IP地址冲突
- 相关的**ICMP邻居发现报文**
- 举例：检测2002::c003:1dff:fea0:0

邻机请求消息NS

IP基本头标

源IP：未指定（：：）

目的IP： **FF02::1:ffa0:0**

对象IP地址（ICMP头标）

2002::c003:1dff:fea0:0

发信者链路地址（ICMP选项）

邻机公告消息NA

IP基本头标

源IP： **2002::c003:1dff:fea0:0**

目的IP：**FF02::1**

对象IP地址（ICMP头标）

2002::c003:1dff:fea0:0

R比特（系统是否为路由器）

S比特（报文是应答还是自发的）

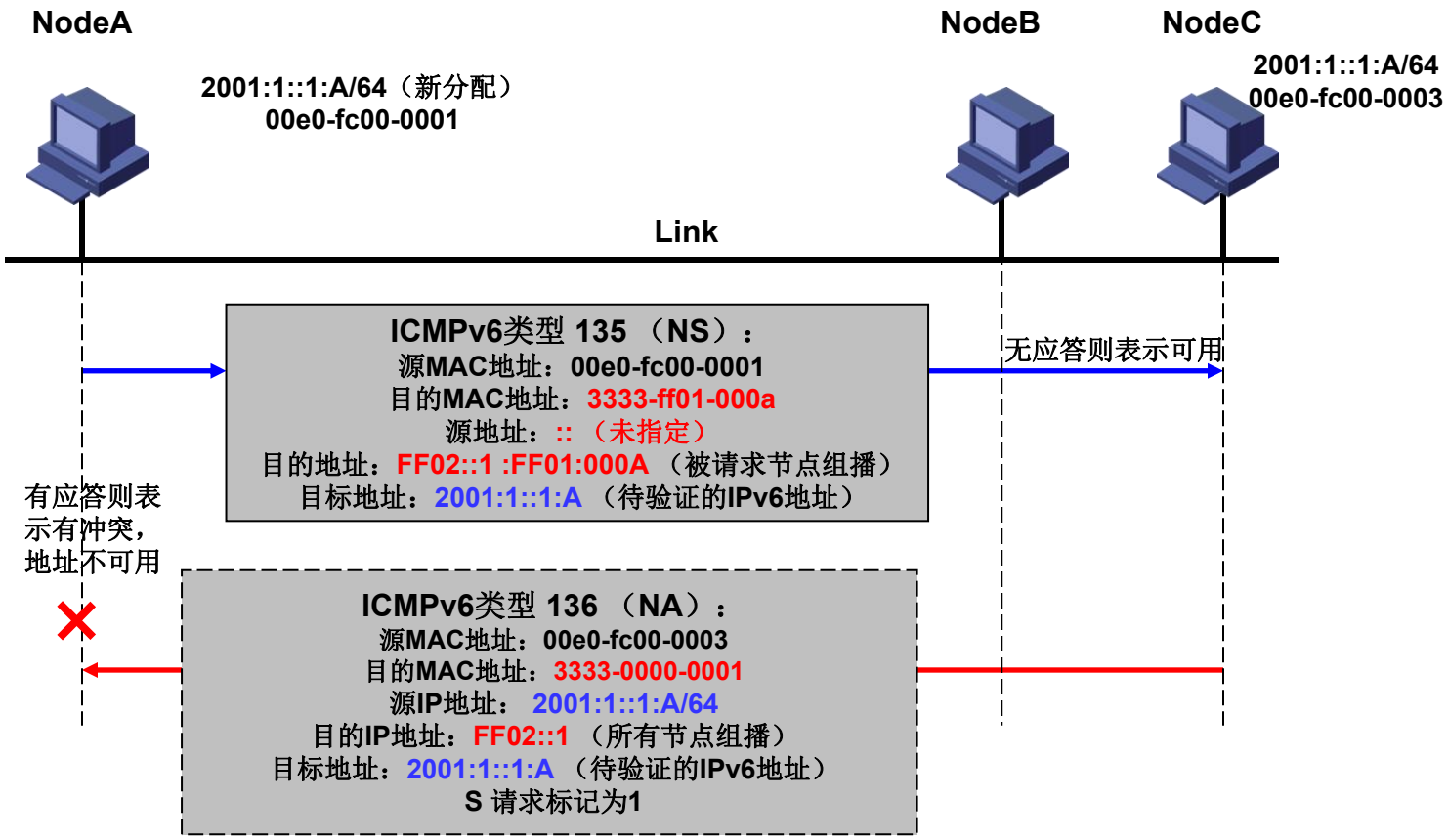
对象链路地址（ICMP选项）

MAC

源：接口的MAC地址

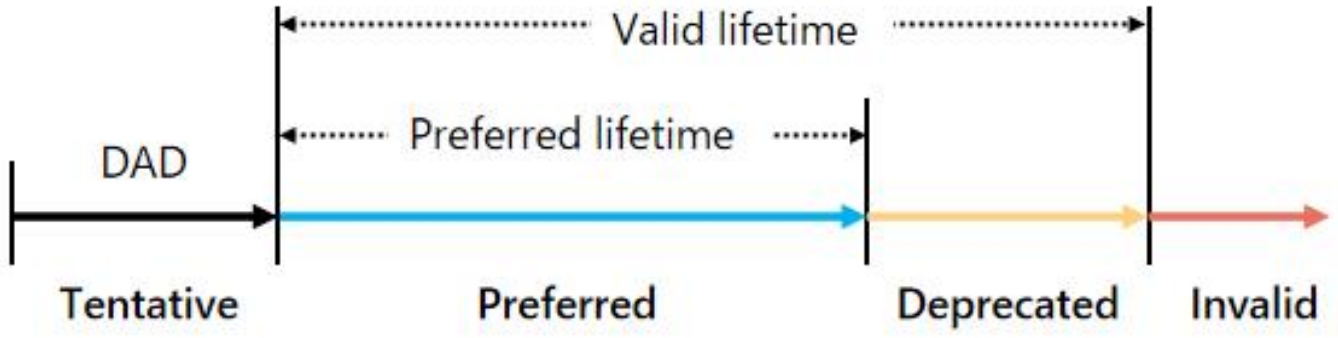
目的：33:33 + IP地址的后32位=33:33:FF:A0:00:00

重复地址检测DAD过程



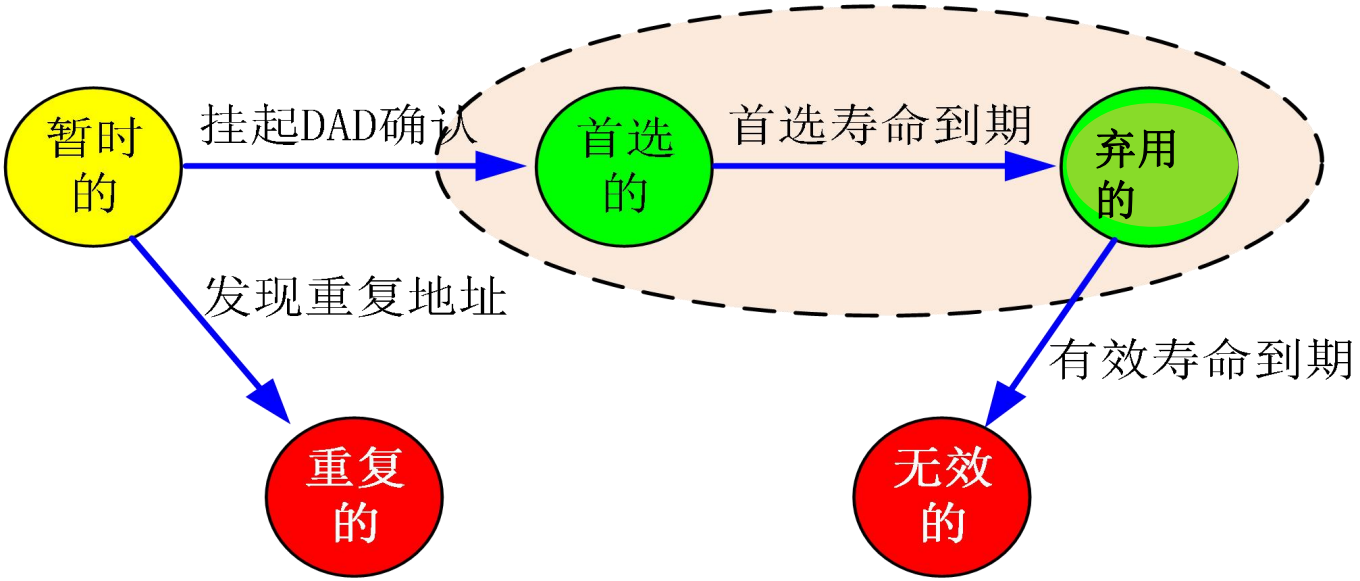
地址自动配置

- IPv6单播地址状态
  - 首选状态(Preferred)和弃用状态(Deprecated)是*有效状态*，每个有效状态都有两种类型的寿命：首选寿命和有效寿命，有效大于等于首选
  - 暂时状态(Tentative)的地址不会被分配给接口，不能在任何通信中使用，但是可以为了执行DAD算法可以发送和接收邻居发现消息，其他类型的分组都会被丢弃。



地址自动配置

- 状态转移图

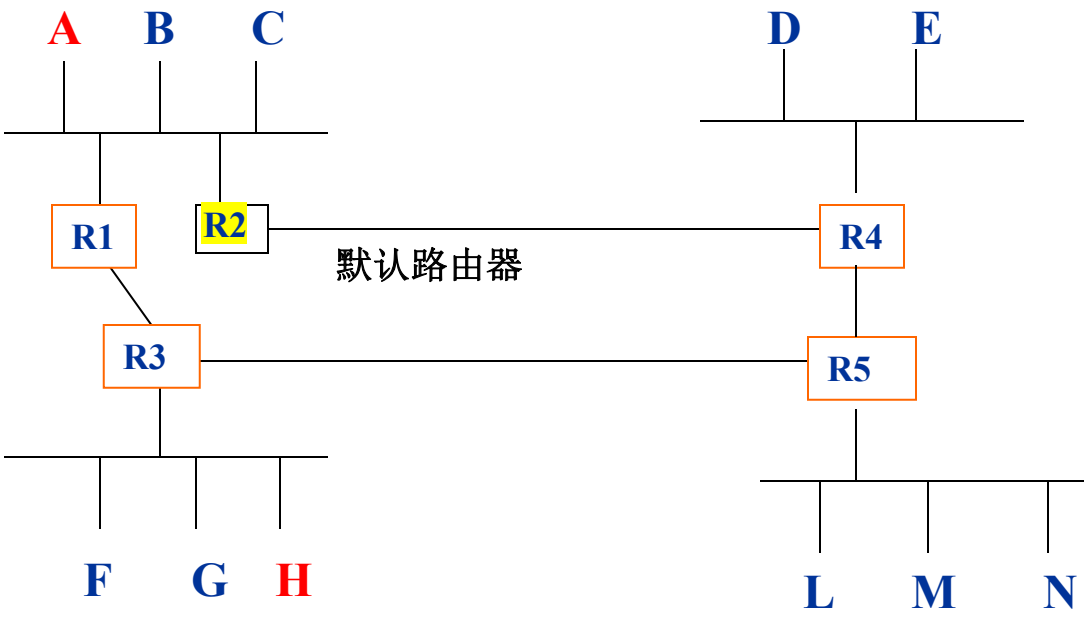


- 命令：netsh interface ipv6 show address

4.2.5 重定向

- 主机通常采用静态路由选择，不参与路由更新过程
- 主机路由表表项有限
  - 本地网络（**前缀列表缓存**）
  - 默认路由器（**默认路由器列表缓存**）
- 重定向报文功能：调整和优化主机的路由表配置（将更优的首跳邻居节点通知给发送主机）

ICMP重定向应用举例

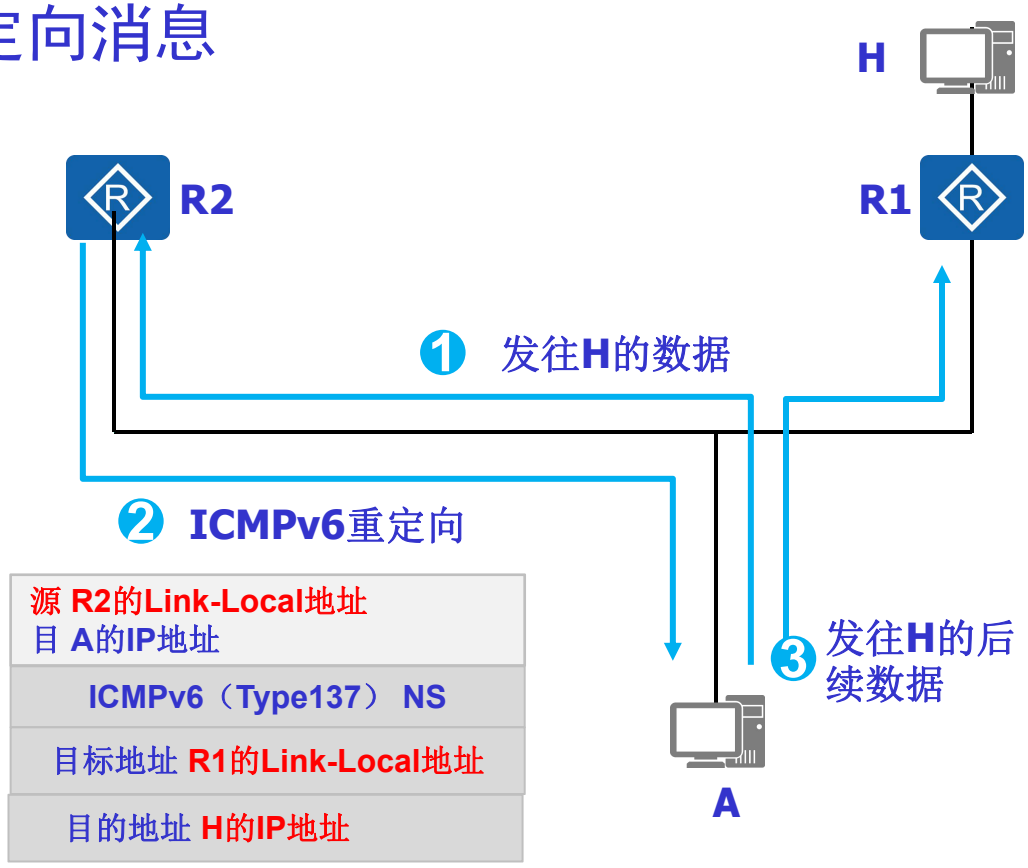


例 A--→H

A的默认路由器是R2，R2又把信息路由给R1、R3，同时产生重定向消息给A，A利用此消息优化本地路由表，将后续数据直接发往R1

ICMP重定向步骤

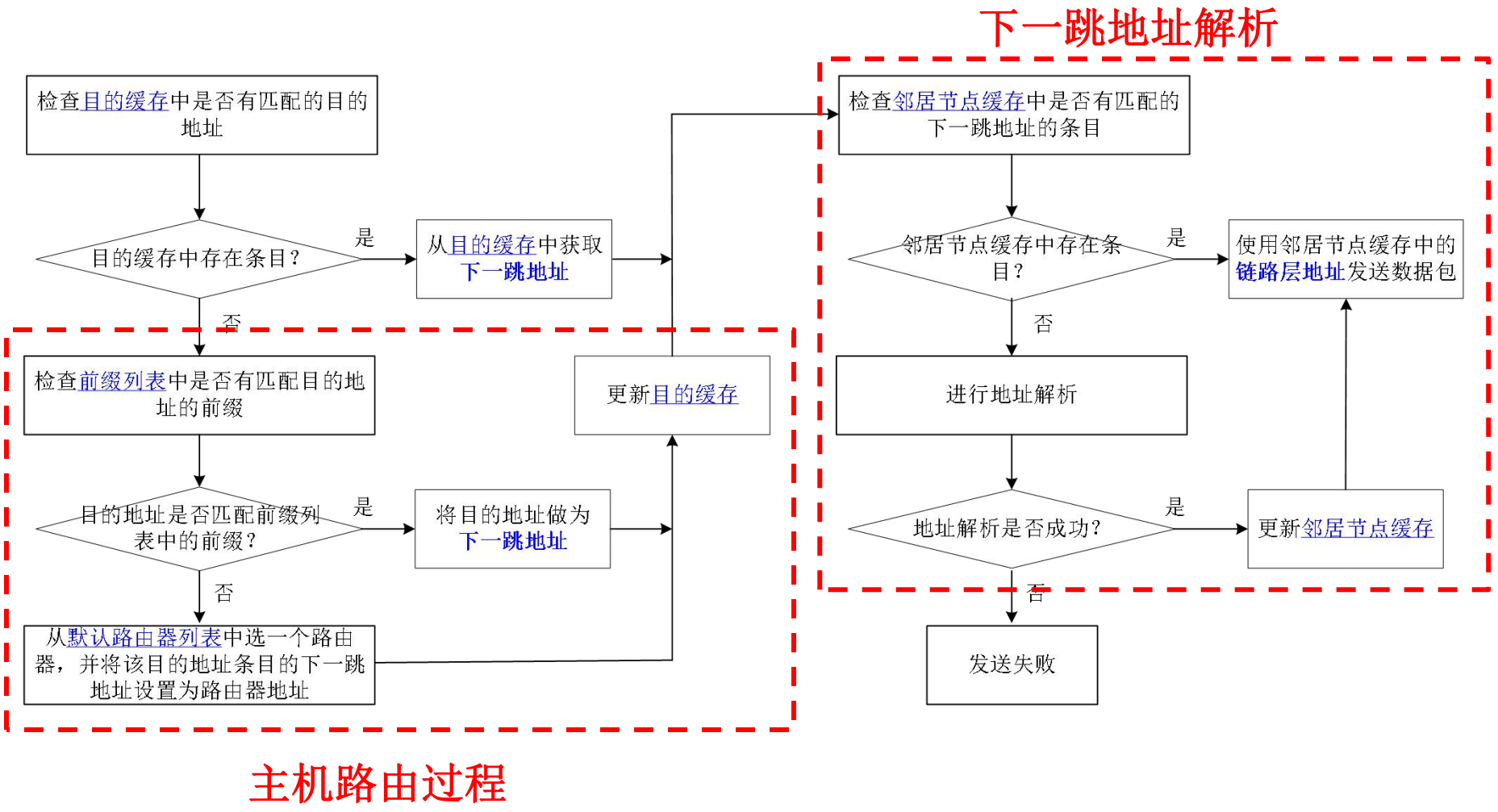
- 1、始发主机A向默认路由器R2发送IPv6数据包
- 2、R2处理数据包并发现下一跳地址R1与A在同一链路上
- 3、R2向A发送ICMPv6重定向消息
- 4、R2转发数据包给R1
- 5、A处理重定向消息并更新路由表（目的地址缓存中的目的地址条目）和邻居节点缓存条目
- 6、后续发往H的IPv6数据包直接发给R1



ICMP控制报文—重定向

- 使用重定向的两种情况
  - 推荐“更接近”目标的可用路由器的IPv6地址
  - 通知始发主机，目的地址是一个邻居节点（主机的前缀列表信息不全，没有包含目的地址的前缀）
- 重定向消息
  - 发送方：始发主机的默认路由器
  - 接收方：某个IP数据包的始发主机
- 优点：保证主机有一个动态、小而优的寻径表
- 缺点：只能用于同一网络内的网关与主机之间的路径信息交换

主机发送IP数据包过程



NDP小结（1）

- NDP实现的主要功能与所使用的ICMPv6报文的关系

功能	RS（133）	RA（134）	NS（135）	NA（136）	Redirect（137）
地址解析			✓	✓	
路由器发现RD	✓	✓			
无状态地址自动配置SLAAC	✓	✓			
邻居不可达性检测NUD			✓	✓	
前缀发现	✓	✓			
重复地址检测DAD			✓	✓	
重定向					✓

NDP小结（2）

- NS和NA在不同功能过程中的地址设置

功能	地址解析	邻居不可达性检测	重复地址检测
NS 源IP	源节点的单播IPv6地址	源节点的单播IPv6地址	未指定地址 **::**
NS 目的IP	目标节点的被请求节点组播地址 **FF02::1:FFXX:XXXX**	目标节点的单播IPv6地址	目标节点的被请求节点组播地址 **FF02::1:FFXX:XXXX**
NA 源IP	发送主机的单播IPv6地址	发送主机的单播IPv6地址	发送主机的单播IPv6地址（全局单播地址GUA）
NA 目的IP	NS消息的源地址（单播IPv6地址）	NS消息的源地址（单播IPv6地址）	本链路全节点组播地址 **FF02::1**

IPv6邻居发现协议的改进

- IPv6邻居发现协议体现了IPv6新的特征，其前缀发现和邻居不可达检测是全新的机制，地址解析和重定向在IPv4中也出现过，但是分别用不同的协议实现

表 4-11　IPv6 邻居发现协议特征及与 IPv4 对应功能的比较

IPv6 邻居发现特征	IPv4 对应的情况	描述
路由器发现	ICMP 路由器发现（RFC 1256）	使结点发现所连接链路上的路由器
前缀发现	无	使结点学习所连接链路上的网络前缀
参数发现	PMTU 发现（RFC 1191）	使结点学习链路上参数，如 MTU、跳数限制等
地址自动配置	无	结点的接口自动配置一个地址
地址解析	ARP	结点为链路上的目的结点确定其链路层地址
确定下一跳	ARP 缓存或默认路由器	为给定目的地确定下一跳地址
邻居不可达性检测	失效网关检查（RFC 1122、816）	使结点可以检测到不可达的邻居
重复地址检测	源地址=0 的 ARP	结点可以确定地址已被占用
重定向	ICMP 重定向	路由器通知主机结点到目的地存在更合适的下一跳
默认路由器和具体的路由选择	无	使路由器通知多点接入主机存在更合适的默认路由器和更好的路由
代理结点	代理-ARP	代表其他结点接收分组

SEND概述

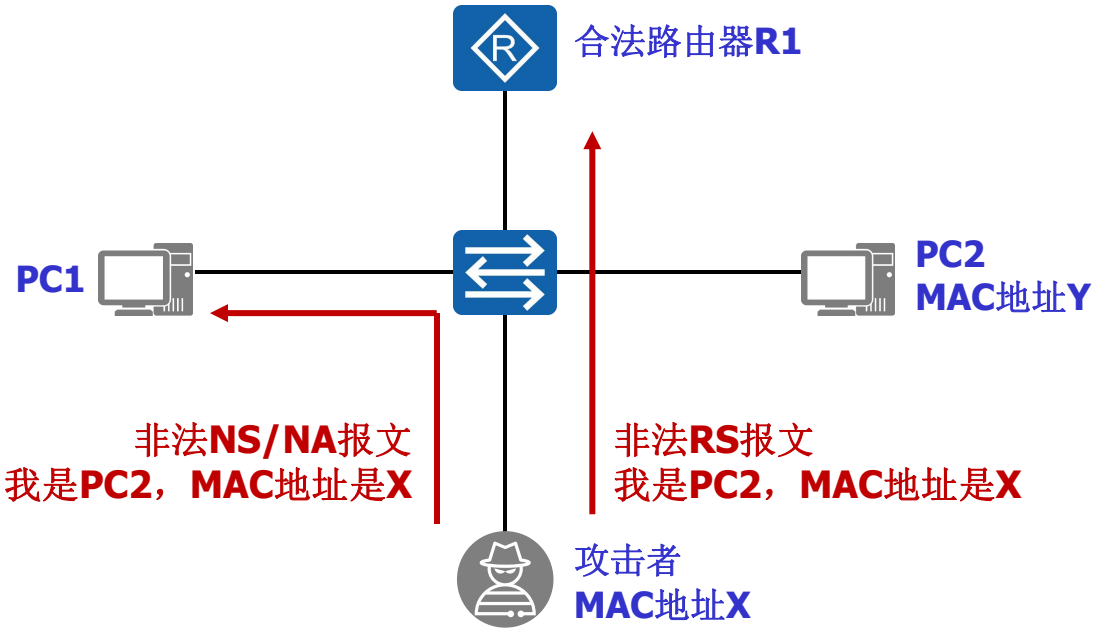
- NDP实现了IPv6节点“即插即用”的新特性
  - 无状态地址自动配置SLACC
- NDP假设前提：链路上全部节点均可信
  - ICMP协议不包含对消息内容的合法性检查，对消息来源的认证
  - 恶意节点可以伪造和篡改ICMP消息，实施各类攻击

NDP相关的攻击

- 涉及ICMP的主要攻击类型
  - 信息泄露information disclosure
  - 泛洪攻击flooding: 发送大量超过网络设备或主机处理能力的流量，造成这些设备拒绝服务DoS
  - 炸弹bomb：发送特殊构造的报文，导致目标IP或ICMP的处理崩溃或终止
  - 协议欺骗攻击：攻击者仿冒其他用户的地址发送NS/NA/RS，改写网关上或者其他用户的ND表项，导致被仿冒用户无法正常接收报文。

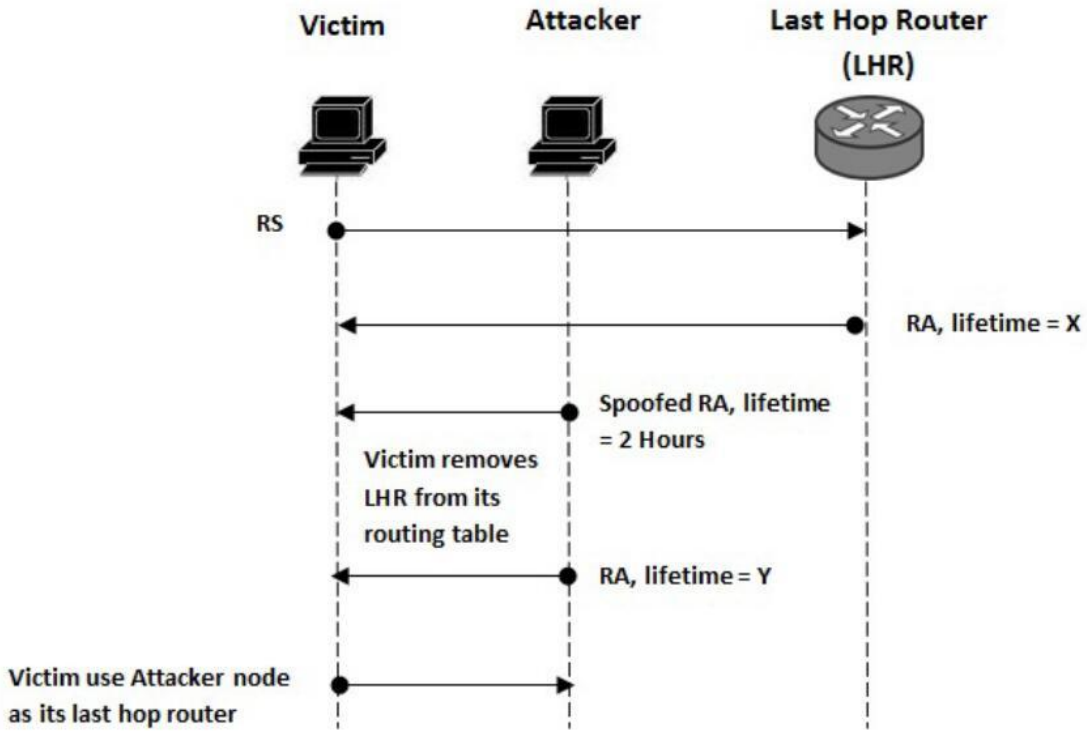
NDP攻击

- NS/NA欺骗攻击



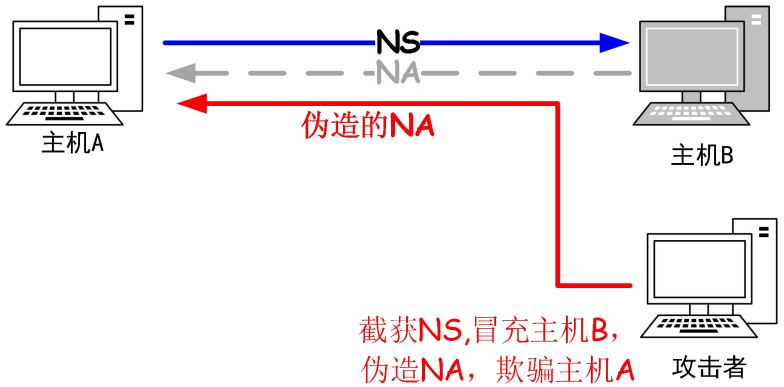
NDP相关的攻击

- 路由器欺骗：冒充路由器发送虚假RA消息攻击
  - 发送错误网络前缀，使目标节点配置后无法正常通信
  - 发送过小的MTU值、跳数限制和路由器生存时间，使被攻击的节点按此参数配置后，发出的IP分组无法到达目的节点

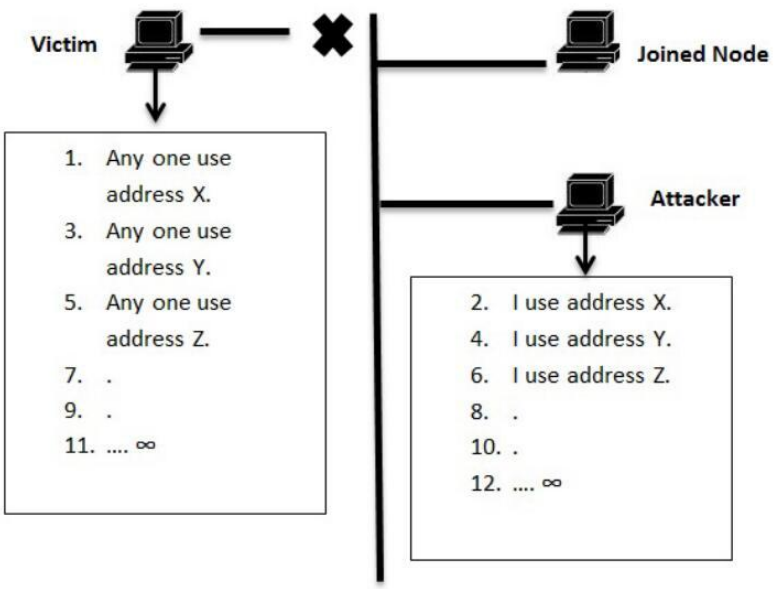


NDP相关的攻击

- NUD失败

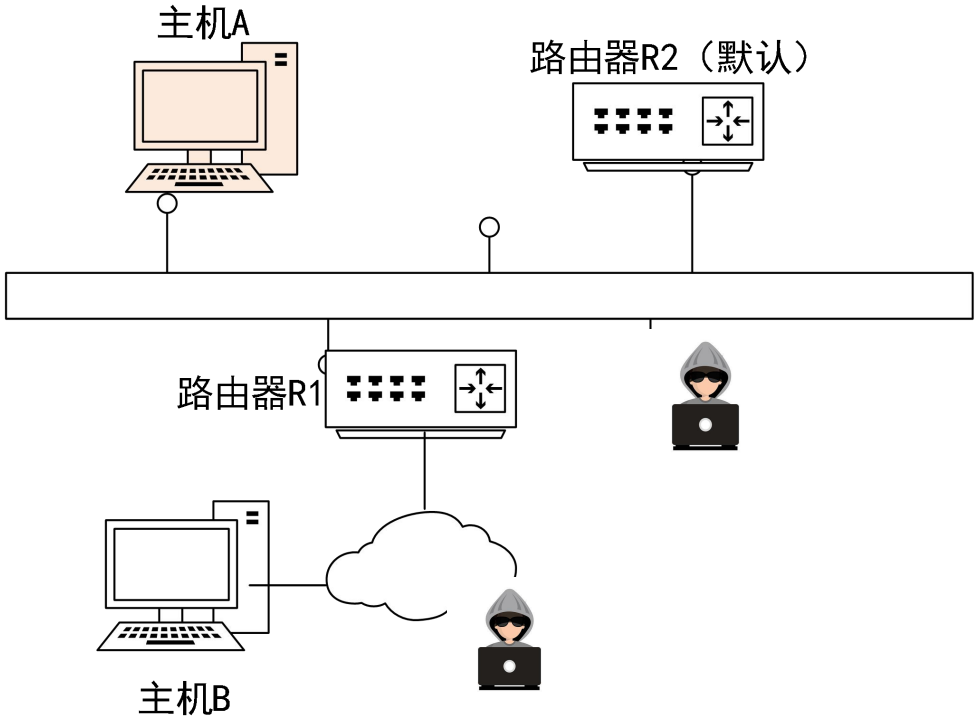


- 基于DAD进行DoS攻击



NDP相关的攻击

- 基于重定向的攻击
  - ICMP 欺骗，黑客主机伪装为路由器向目标主机发送重定向报文
  - ICMPv6重定向的保护机制：导致重定向的数据包的一个副本必须包括在ICMPv6重定向消息中



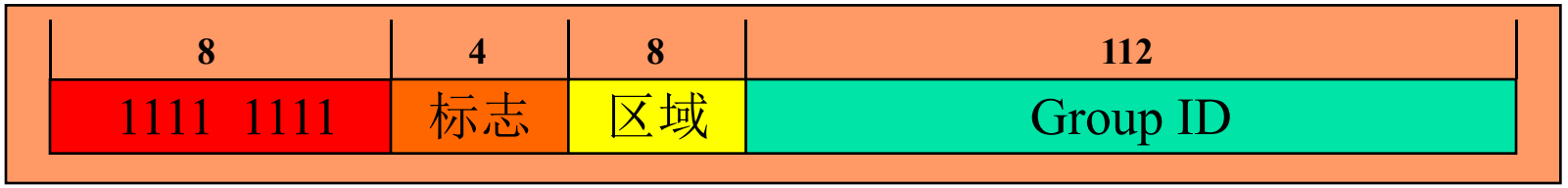
SEND

- NDP存在的主要安全问题
  - 不能抗重传攻击
  - 没有对消息源进行认证
  - 没有对路由器进行合法性认证
- SEcure Neighbor Discovery (RFC 3971)
  - 时间戳、nonce随机数(抗重放)
  - 地址加密生成CGAs、RSA数字签名(源认证)
  - X.509公钥证书(路由器身份认证)
- 未被广泛应用
  - 实现复杂、对节点计算资源和带宽资源要求高

谢　谢！

附录A：IPv6组播地址

- 组播地址格式



  - 标志(000T)
    - T=0 永久性地址，所有的主机和路由器都知道；
    - T=1 非永久地址，暂时使用
  - 区域: 标识组播地址的有效范围
    - 2: 链路局域范围（限制在单一链路范围内）
    - E: 全局范围
  - Group ID：标识组播组，在给定范围内，可以是永久的也可以是暂时的

被请求节点组播地址

- 被请求的节点地址

  Group ID = FF02:0:0:0:0:1:FFXX:XXXX

  此组播地址由一个节点的单播或任播地址生成

- 应用
  - RFC 4861中规定，在节点进行**地址解析**时，要将邻居请求消息发送到请求目标地址的**被请求-节点多播地址**。
  - RFC4862 无状态地址自动配置中规定，在节点执行**重复地址检测**时，要将邻居请求消息发送到请求目标地址的**被请求-节点多播地址**。

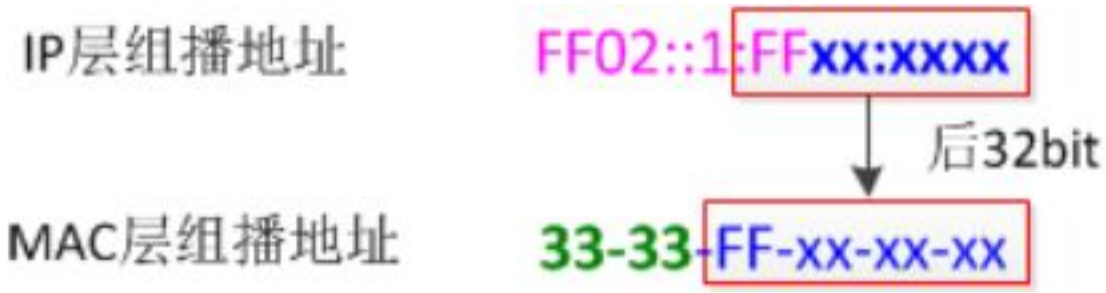
附录B：IPv6组播IP地址与组播MAC地址之间的换算方法

- 被请求节点组播地址：

  FF02::1:FFXX:XXXX

- 链路层组播地址：

  33-33-FF-XX-XX-XX



附录C：以太网地址转换

- EUI-48：

  XX-XX-XX-XX-XX-XX

- EUI-64：

  XX-XX-XX-FF-FE-XX-XX-XX

然后对第1个字节的第七位求反

举例：00-AA-00-3F-2A-1C

00000010-AA-00-FF-FE-3F-2A-1C

即：02-AA-00-FF-FE-3F-2A-1C