下一代Internet技术与协议

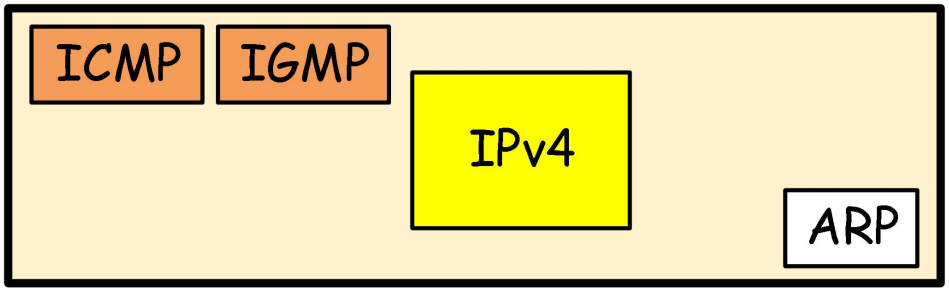
张冬梅
北京邮电大学 计算机学院
zhangdm@bupt.edu.cn

ICMP协议

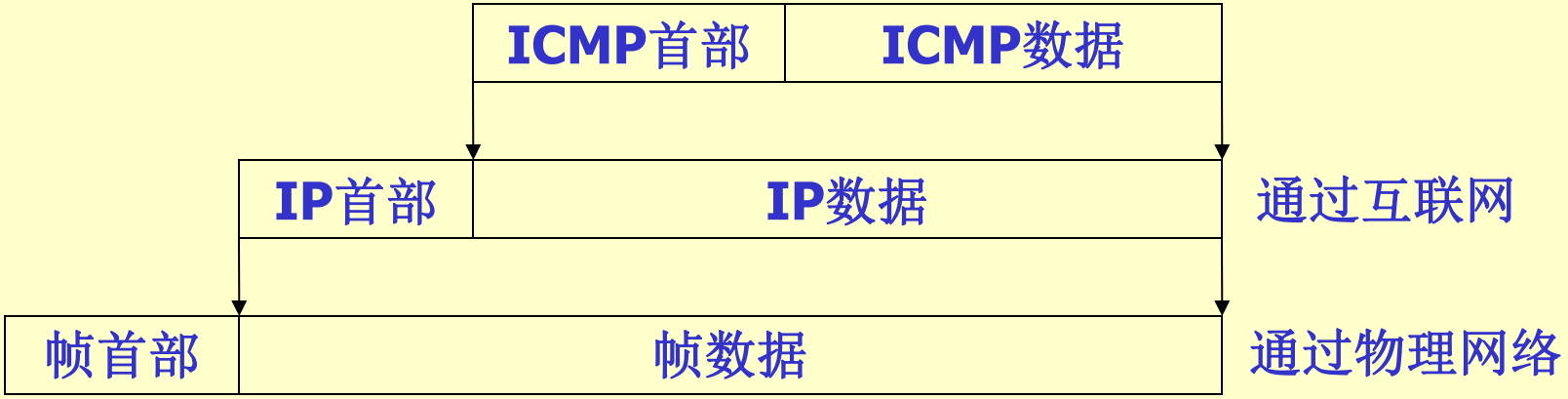
- 协议背景与功能
- ICMP格式与类型
- ICMP功能

协议背景与功能

- 协议背景
- 在协议栈位置
- IP与ICMP关系
  - IP与ICMP互相依赖
  - IP在发送一个差错报文时用到ICMP
  - ICMP用IP来封装传递报文
- ICMP功能
  - 使发送方了解为什么数据报无法投递(差错报告与诊断)
  - 管理查询（系统间调整）



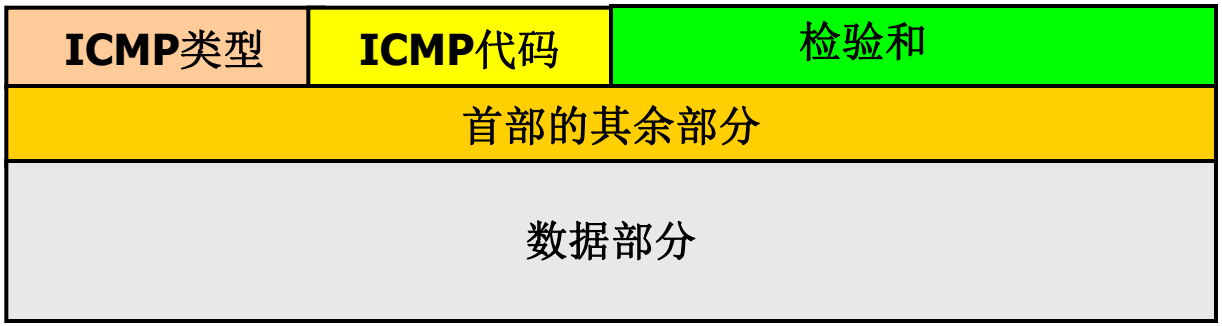
- ICMP报文的投递
  - 在一个IP数据报的数据部分通过互联网传送
  - 两级封装



  - 问题：为什么用IP进行封装？

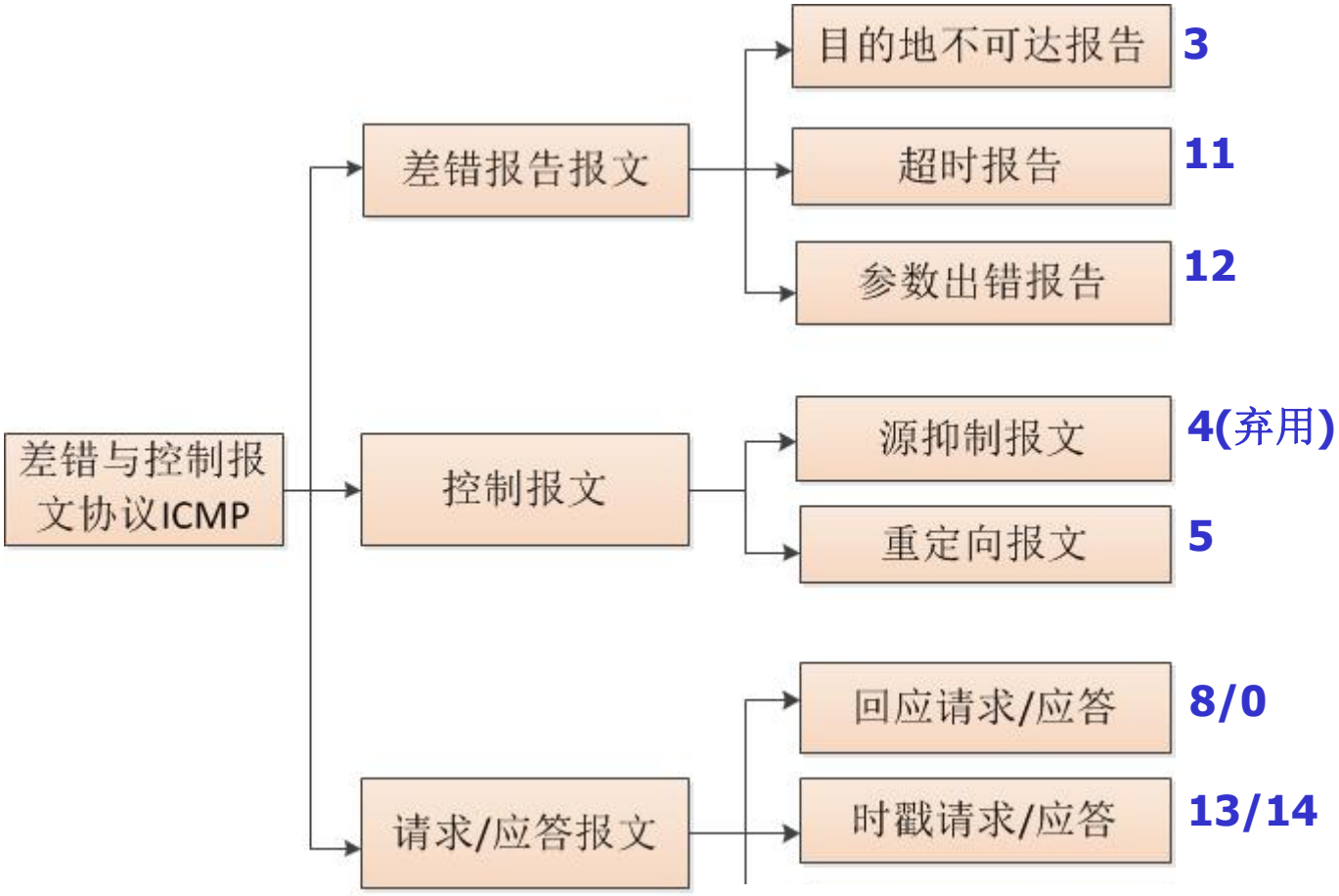
ICMP报文格式

- ICMP格式(8字节首部+可变长数据)



  - ICMP类型
  - ICMP代码：提供有关报文类型的进一步信息
  - 校验和: 包括整个报文，方法与IPv4相同(见附录1)。
  - 数据：差错报文中，携带用于找出引起差错的原始分组的信息；查询报文中，携带的是基于查询类型的额外信息

ICMPv4报文类型


差错与控制报文协议ICMP
差错报告报文
控制报文
请求/应答报文
目的地不可达报告
3
超时报告
11
参数出错报告
12
源抑制报文
4(弃用)
重定向报文
5
回应请求/应答
8/0
时戳请求/应答
13/14

ICMP报文地址

- 信源IP地址的选择
  - 如果系统只对应一个接口的一个IP地址，则用此地址即可
  - 如果系统只对应多个接口的多个IP地址，则按规则选取
    - case1：ICMP应答报文
      - 如果源报文的目的地址是单播地址，则信源地址为原报文的目的IP地址（问谁谁回答）；
      - 如果源报文的目的地址是组播或任播地址，则信源地址为收到原报文的接口的IP地址（谁收到谁回答）；

- case2：对于ICMP差错报文，则信源地址为报告出错信息的接口的IP地址；
- case3：对于其他ICMP报文，则信源地址为发送报文的链路的IP地址(主动发送的、以及不适用上述规则的)

- 信宿IP地址的选择
  - 提示：不同类型、不同用途的ICMP报文的信宿地址的选取规则不同

ICMPv4的几种使用

- 差错报告报文
- 控制报文
  - 拥塞控制与源抑制报文
  - 路由控制与重定向报文
- 请求/应答报文
  - 回应请求/应答
  - 时戳请求/应答

差错报告

- 功能

  ICMP对IP分组出现的差错进行报告，只报告错误，不纠错

- 把差错报文报告给最初的数据源
- 相关报文
  - 目的地不可达
  - 分组超时
  - 参数问题

差错报告

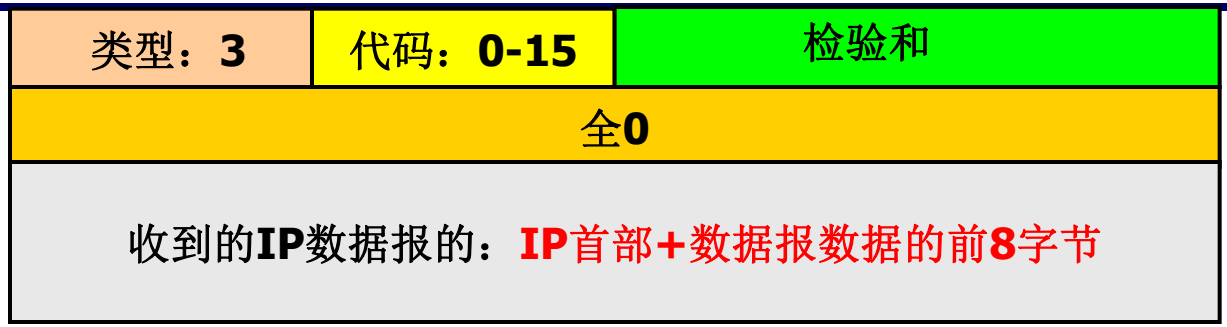
- 关于ICMP差错报文的要点
  - 对于携带ICMP差错报文的数据报，不再产生ICMP差错报文
  - 对于分片的数据报，如果不是第一个分片，则不产生ICMP差错报文
  - 对于具有多播地址的数据报，不产生ICMP差错报文
  - 对于具有特殊地址(127.0.0.0或0.0.0.0)的数据报，不产生ICMP差错报文

差错报告

- 差错报文的数据部分包含
  - 原始数据报的IP首部
  - 数据报数据的前8个字节

终点不可达

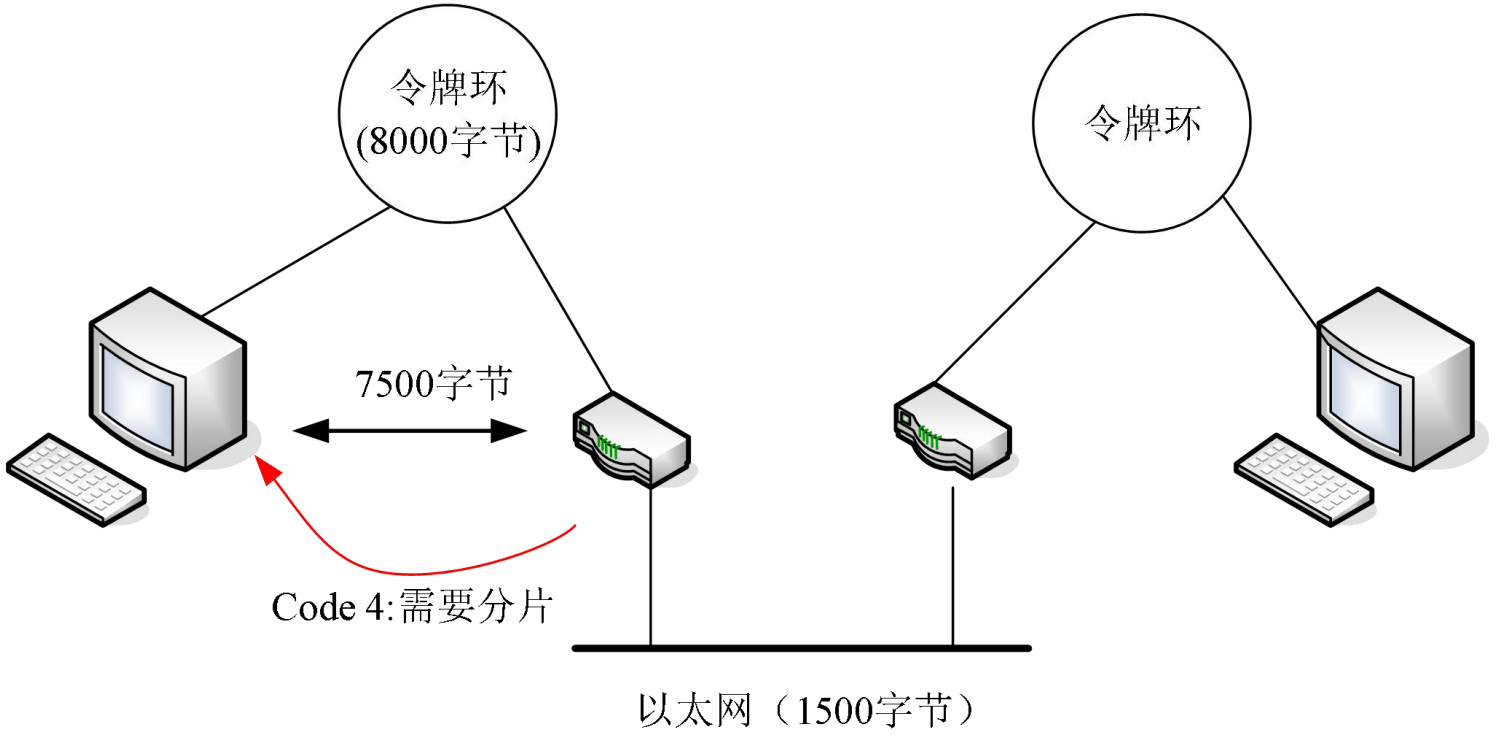
- 格式



代码	含义	代码	含义
0	网络不可达	8	源主机被隔离
1	主机不可达	9	管理上禁止与目的网络通信
2	协议不可达	10	管理上禁止与目的主机通信
3	端口不可达	11	对指明的服务类型，网络不可达
4	需要进行分片	12	对指明的服务类型，主机不可达
5	源路由不能完成	13	主机不可达，设置了过滤器
6	目的网络未知	14	主机不可达，违反了优先级策略
7	目的主机未知	15	主机不可达，优先级被截止

终点不可达

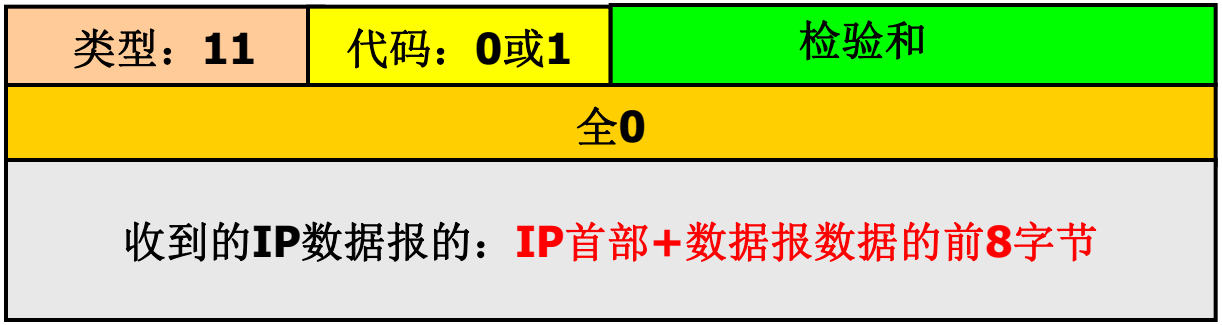
- 工作过程举例



- 说明：未收到终点不可达报文，不表示数据已经被交付。Why?

超时报文

- 两种情况
  - 报文超时(0)：TTL字段递减后为0，丢弃数据报，并发送超时报文
  - 重组超时(1)：终点在规定的时间内未收全全部报文分片，则丢弃已经收到的分片，并发送超时报文
- 格式



参数问题

- 格式

  - Code=0: 首部的某个字段有差错或二义性，指针字段值指向有问题的字节
  - Code=1：缺少所需要的选项部分。不使用指针。

差错报文

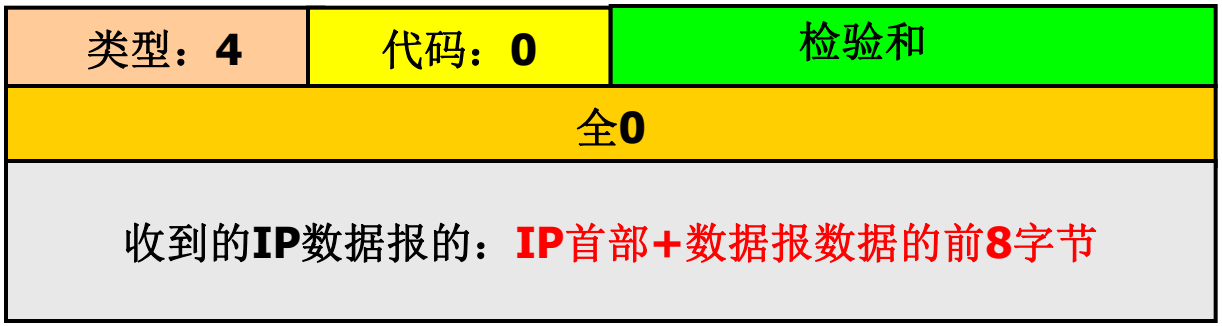
- 应用
  - 路径MTU发现
  - 路由跟踪

ICMP控制报文—源抑制

- 功能：拥塞控制
- 条件：当路由器接收IP数据报的速度比其处理IP数据报的速度快，或者路由器传入IP数据报的速度大于其传出IP数据报的速度时，会产生拥塞现象
- 措施：路由器通过发送源站抑制报文(Source Quench)来抑制源主机发送IP数据报的速率，进而避免可能产生的拥塞和差错

源抑制报文

- 格式



- 作用
  - 通知源点，数据报已经被丢弃
  - 警告源点，在路径中的某处出现了拥塞，源点需要放慢(抑制)发送过程。
- 说明
  - 对每一个因拥塞而被丢弃的数据报，发送一个源抑制报文
  - 没有机制告诉源点拥塞得到缓解
  - 多对一通信不一定有效果

源抑制报文

- 利用源抑制报文进行拥塞控制的过程
  - 路由器发生拥塞时发出ICMP源抑制报文
    - 拥塞判别方法

    (1) 检查路由器缓存是否已满

    (2) 缓存区输出队列设置一个阀值，判断队列中数据报个数是否超过阀值

    (3) 检测某输入线路的传输率是否过高
  - 源主机收到抑制报文后按一定的速率降低发往目标主机的数据报传输率
  - 如果在一定的时间间隔内源主机没有再收到抑制报文，便认为拥塞已经解除，源主机可逐渐恢复到原来的发送速率

源抑制报文

- 相关说明
  - 对网络的拥塞控制效率低且不公平
  - 1995年，RFC1812正式禁止路由器产生和转发源抑制消息
  - 2012年，RFC6633正式宣布传输层协议不再对ICMP源抑制消息做出响应

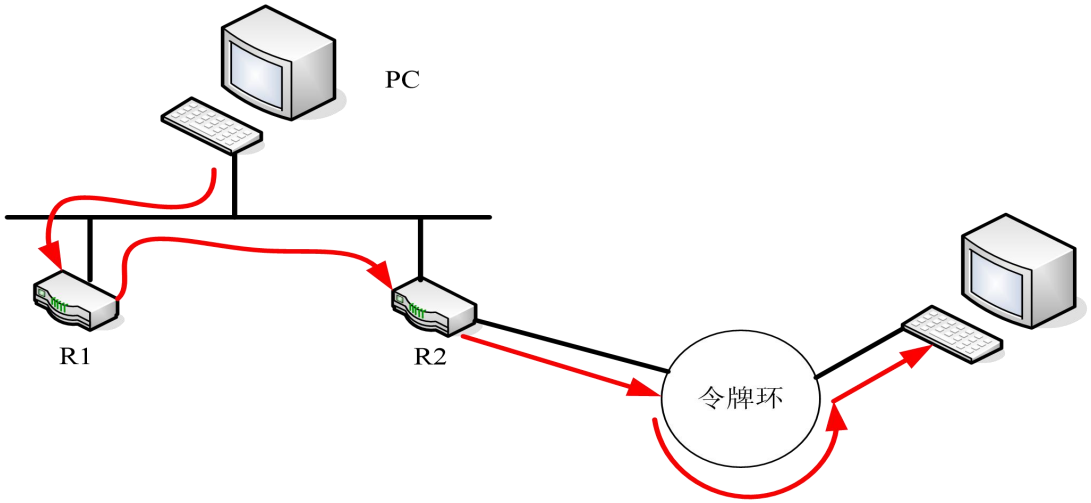
ICMP控制报文—重定向

- 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
  - 默认路由器
- 重定向报文可以增大和更新主机的路由表

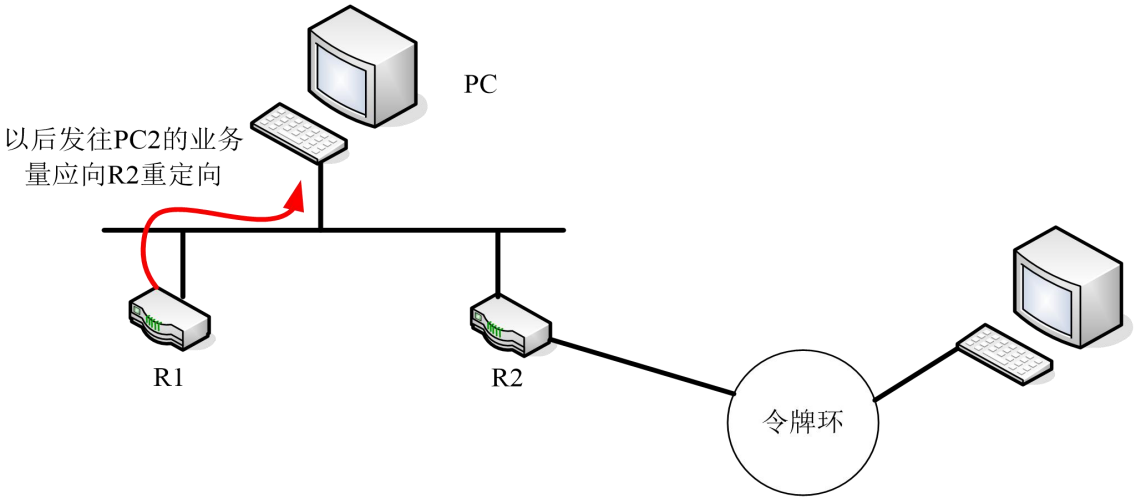
ICMP控制报文—重定向

- 功能：调整和优化主机的路由表配置
- 基本工作过程
  - PC向Router1发送IP数据报
  - Router1发现应该发给Router2，于是将信息转发给Router2
  - Router2继续转发IP包
  - Router1向PC发送重定向报文

ICMP控制报文—重定向



IP分组非高效地传送



对主机的重定向

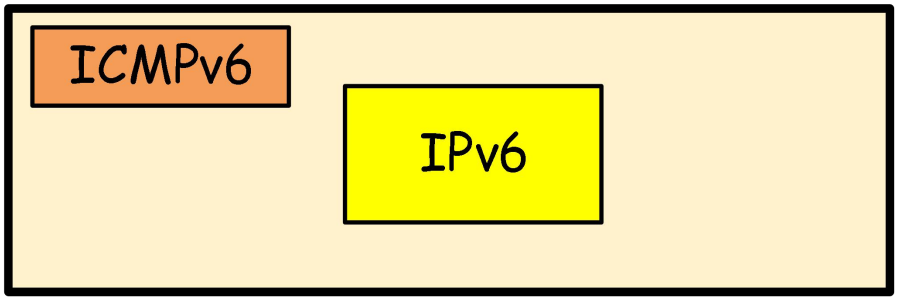
ICMP控制报文—重定向

- 格式

- 类型
  - 0—对特定网络的重定向报文
  - 1—对特定主机的重定向报文
  - 2—服务类型和特定网络的重定向报文
  - 3—服务类型和特定主机的重定向报文
- 特点
  - 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

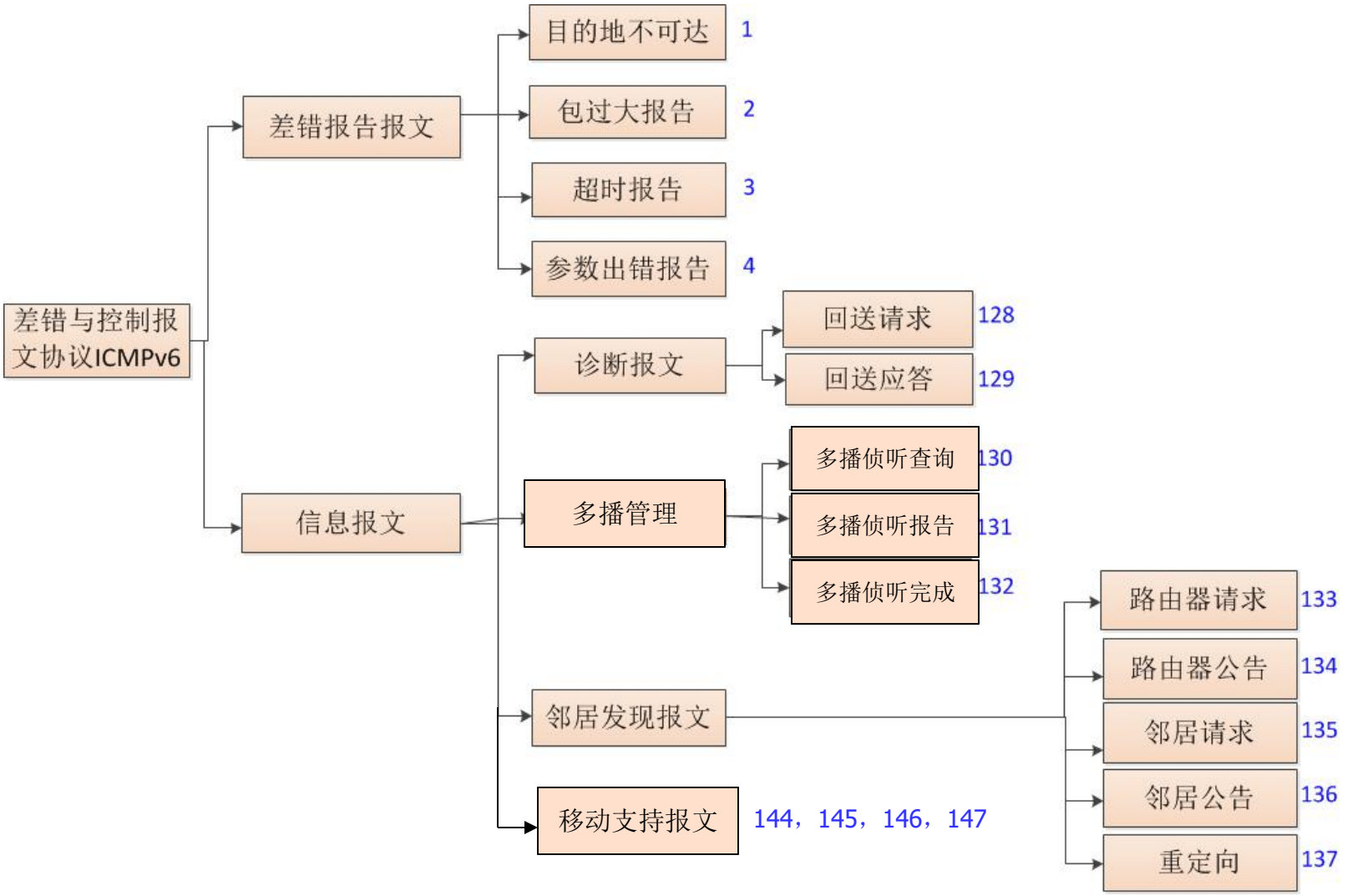
ICMPv6概述

- ICMPv6与IPv6一起工作， IPv6网络中每一个节点均要实现ICMPv6



- 功能
  - 当IPv6分组不能被正确处理时，ICMPv6向源节点报告IPv6分组在传输过程中的出错信息和通告信息，使网络节点知道网络状态。
  - 在IPv6网络中，用ICMPv6实现了IPv4网络中的ICMP、ARP、IGMP协议的功能，并增加了对移动IPv6的支持

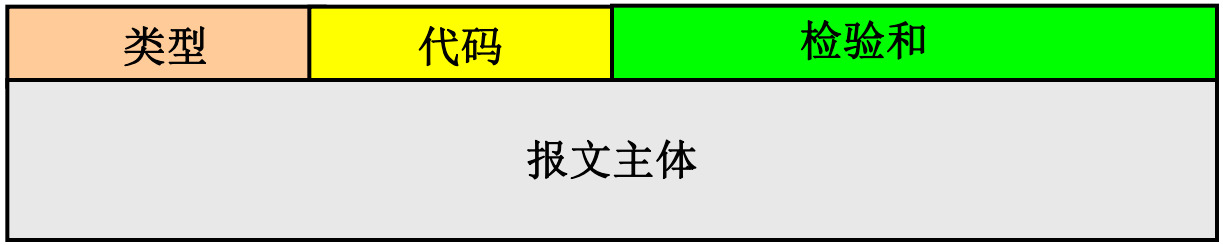
ICMPv6报文类型


差错与控制报文协议ICMPv6
差错报告报文
目的地不可达
1
包过大报告
2
超时报告
3
参数出错报告
4
信息报文
诊断报文
回送请求
128
回送应答
129
多播管理
多播侦听查询
130
多播侦听报告
131
多播侦听完成
132
邻居发现报文
路由器请求
133
路由器公告
134
邻居请求
135
邻居公告
136
重定向
137
移动支持报文
144，145，146，147

报文名称	ICMPv4类型	ICMPv6类型
目的地不可达	3	1
协议包过大	类型3代码4	2
源抑制	4	无
重定向	5	137
回声请求/应答	8/0	128/129
超时	11	3
参数错误	12	4
时间戳/时间戳回复	13/14	无
路由器请求RS/公告RA	10/9	133/134
邻居请求NS/公告	ARP	135/136
家乡代理地址发现请求/公告	无	144/145
移动前缀请求/公告	无	146/147
组成员管理	IGMP	130,131,132

ICMPv6协议格式

- ICMP分组格式
  - ICMPv6首部+ICMPv6报文主体
  - IPv6首部中：下一个首部=58



  - 类型
    - 最高位为0：差错报文
    - 最高位为1：查询报文
  - 校验和：伪头标校验

ICMPv6报文处理规则

- 当接收到ICMPv6差错报告报文时，如果无法识别具体的类型，必须将它交给上层协议模块进行处理；
- 当接收到ICMPv6信息报文时，如果无法识别具体的类型，将它丢弃；
- 所有的ICMPv6报文，都应该在IPv6所要求的最小MTU允许范围内，尽可能多地包括引发该ICMPv6差错报文的IPv6分组片段，以便给IPv6分组的源节点提供尽可能多的诊断信息

ICMPv6报文处理规则

- 不能产生ICMPv6差错报告报文的发送情况
  - 一个ICMPv6差错报告报文
  - 一个发往IPv6多播地址（或链路层多播地址）的分组
    - 例外情况：分组过大报文
  - IPv6分组的源地址无法唯一确定一个单独节点时，这种情况不能够引起ICMPv6差错报告报文的发送。

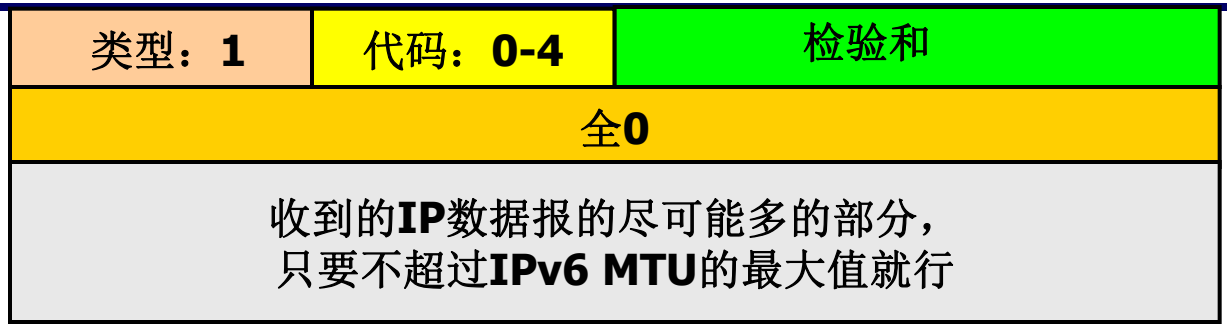
- IPv6节点必须限制其发送ICMPv6差错报文的速率。目前限制ICMPv6速率的方法：
  - 基于计时器的方法：T时间内只发送一个报文
  - 基于带宽的方法：ICMPv6差控报文占链路带宽的某个比例F

ICMPv6的几种使用

- 差错报告
- 邻机发现：为了确定同一个链路上的邻居的链路层地址、发现路由器、随时跟踪哪些邻居可连接，以及检测更改的链路层地址。
- 组管理

目的地不可达

- 格式

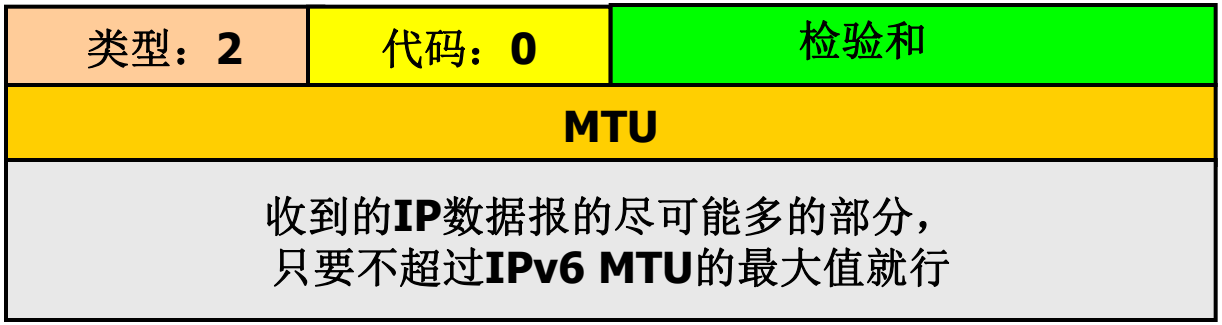


- 代码

代码	含义
0	没有路径到达目的地
1	与目的地的通信被禁止
2	超出源地址的范围
3	目的地址不可达
4	端口不可达

分组过大报文

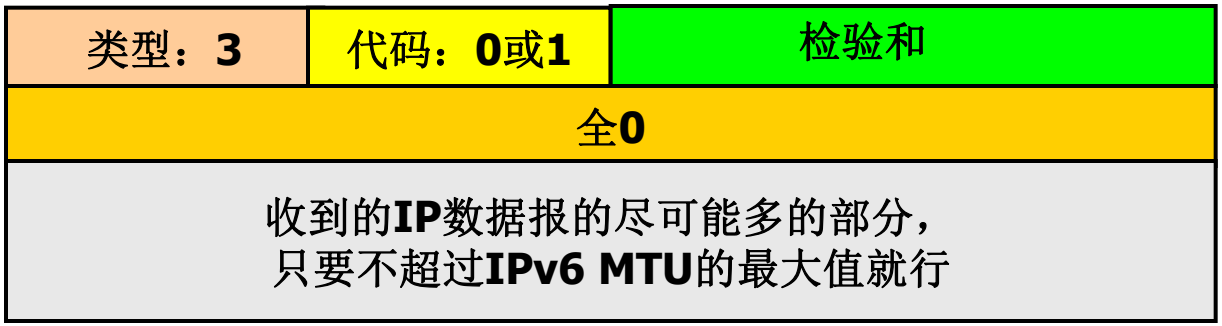
- 格式



- 主机收到该报文后必须通知上层进程

超时报文

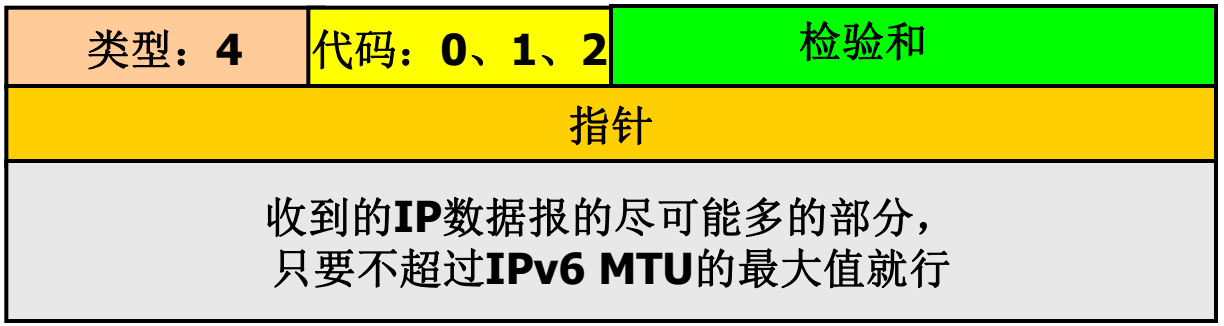
- 格式



  - Code=0：超出了跳数限制
  - Code=1：分组重组超时
- 应用：路由跟踪

参数问题报文

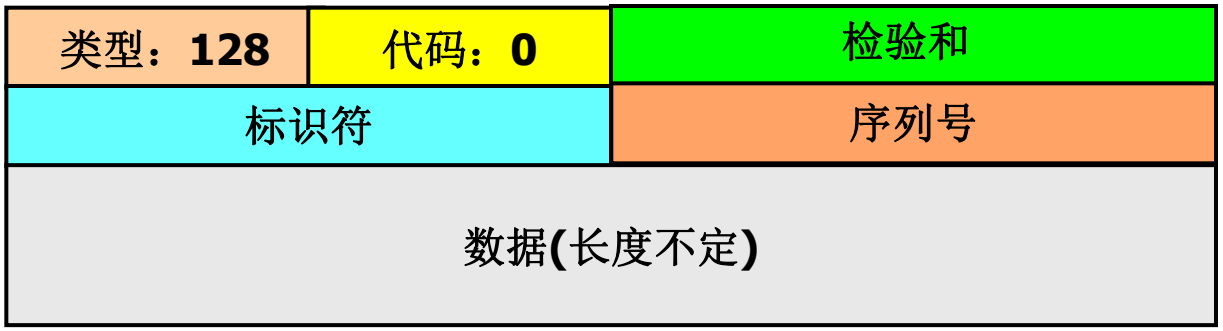
- IPv6基本首部或扩展首部出现问题，无法完成分组传输，目的节点或路由器会丢弃分组并发送ICMPv6参数问题报文
- 格式



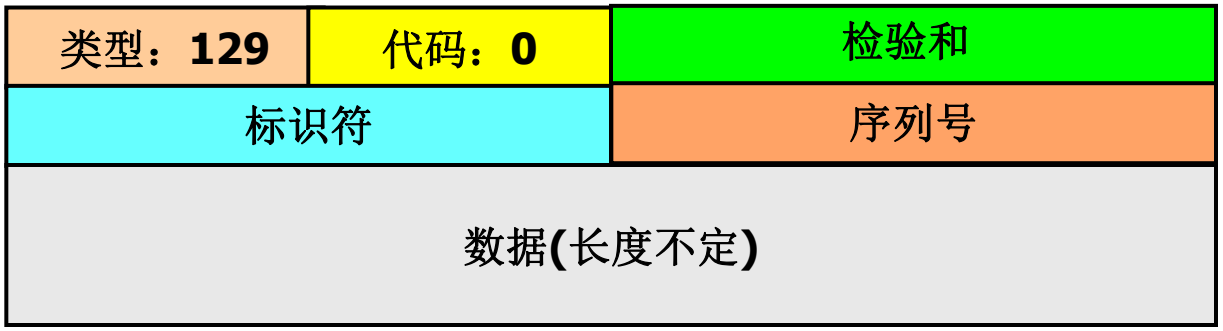
  - Code=0：错误的首部字段
  - Code=1：无法识别的下一首部类型
  - Code=2：无法识别的IPv6选项

查询报文

- 回声请求报文
  - 单播或多播
  - 格式



- 回声应答报文
  - 标识符
  - 序列号
  - 数据



与回声请求报文相匹配，请求报文数据完整复制到应答报文。

IPv6邻居发现

- 概述
- 主要用途
- 协议报文格式及选项
- 协议报文
  - 路由器请求与路由器公告
  - 邻居请求与邻居公告
- IPv6重定向
- IPv6地址解析

IPv6邻居发现

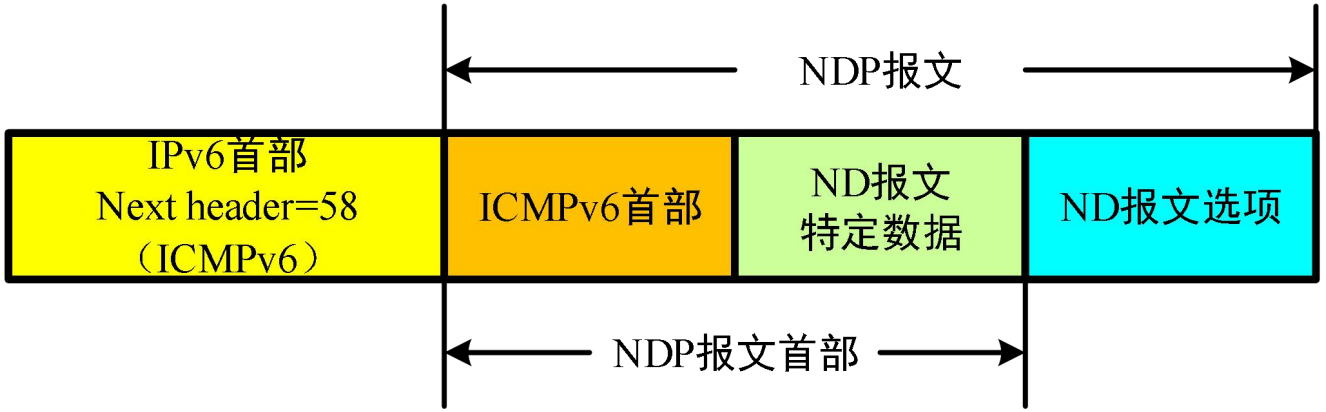
- 邻居发现协议NDP(Neighbor Discovery Protocol)
- 作用：确定邻居节点之间的关系，是单播通信的关键服务
  - 主机使用ND协议发现能为其转发分组的邻居路由器
  - 节点使用ND协议发现邻居的链路层地址
  - 节点使用ND协议发现邻居的IPv6地址
- 功能
  - 路由器发现RD
  - 邻居发现ND
  - 地址解析
  - 地址自动配置
  - 邻居可达性检测NUD
  - 重复地址检测DAD
  - 重定向

IPv6邻居发现

- SEND(SEcure Neighbor Discovery,RFC3971)是安全邻居发现协议，增加了认证等安全功能
- 相关的报文
  - 路由器请求/公告报文(RS/RA)
  - 邻居请求/公告报文(NS/NA): 地址解析
  - 重定向报文
- IPv6主机维护的缓存信息(soft state)
  - 邻居缓存：维护最近通信的邻居的信息
    - 邻居：可达性状态、链路层地址、单播IP地址等信息
  - 目的地缓存：维护最近通信的目的地节点的信息

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

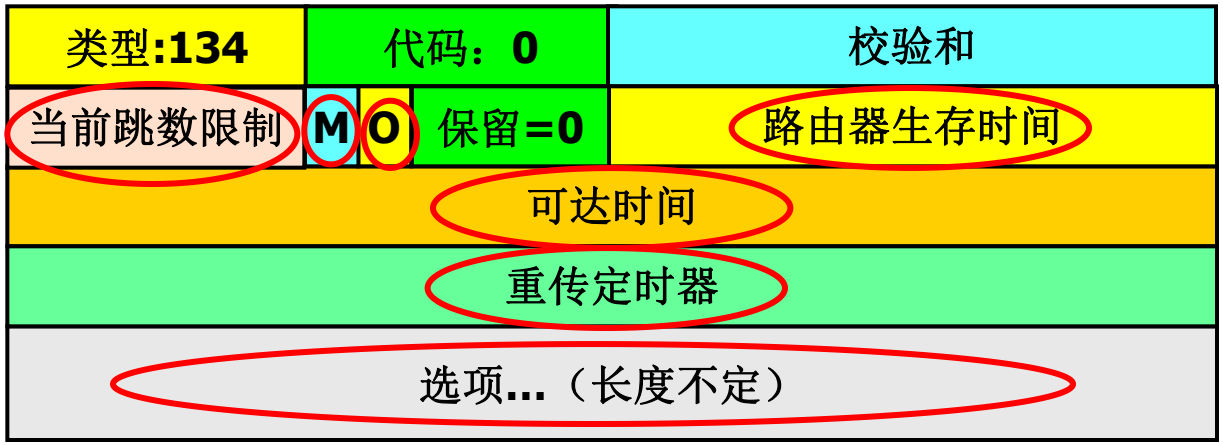
路由器请求与公告

- 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
- 路由器请求RS

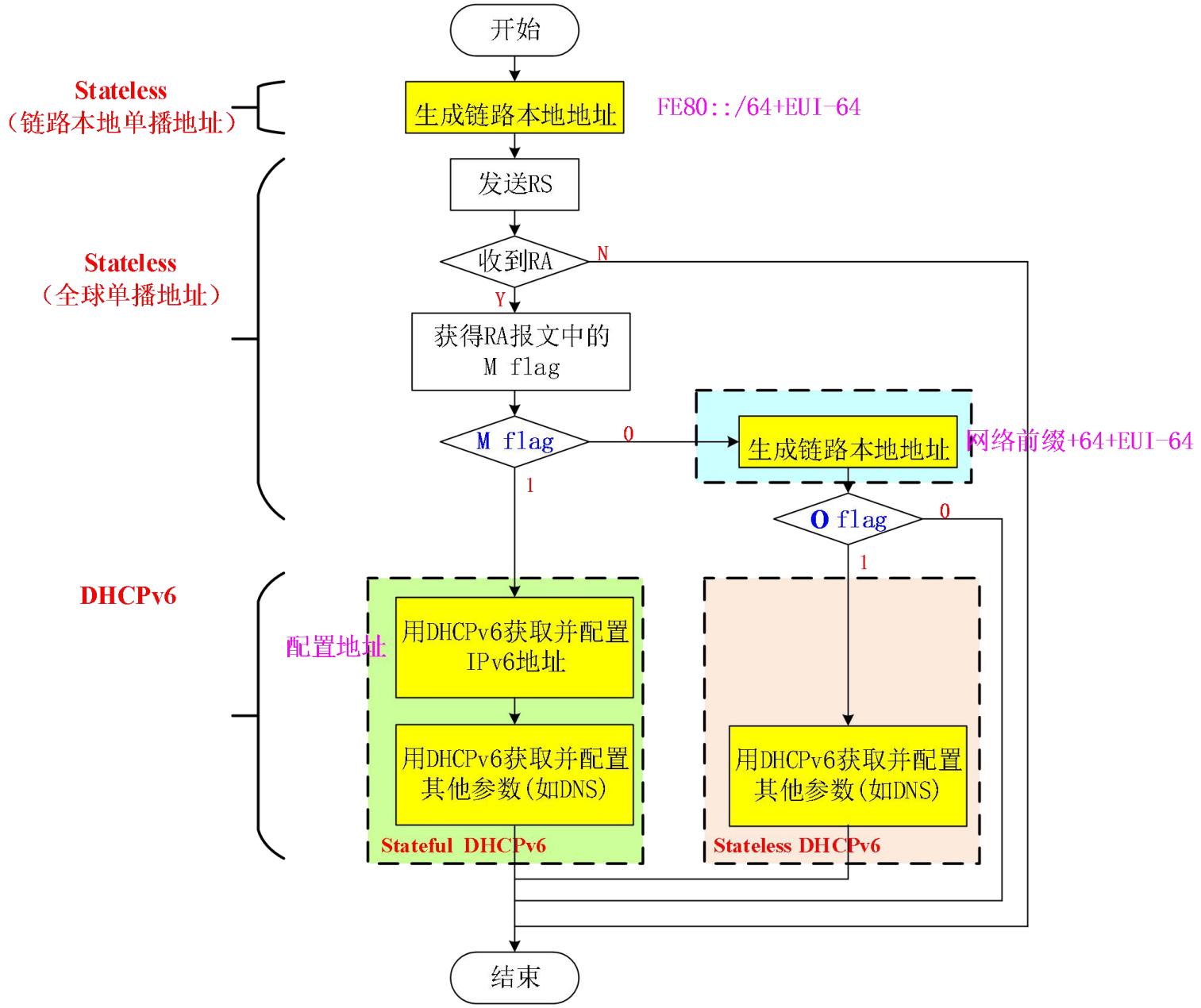
  - 源IP地址：链路本地地址/::
  - 目的IP地址：FF02::2
  - Next header：58(ICMPv6)
  - 选项：发送方物理地址(源链路层地址)

路由器请求与公告

- 路由器通告RA
  - 源IP地址： 链路本地地址
  - 目的IP地址：FF02::1/发出请求报文的接口地址

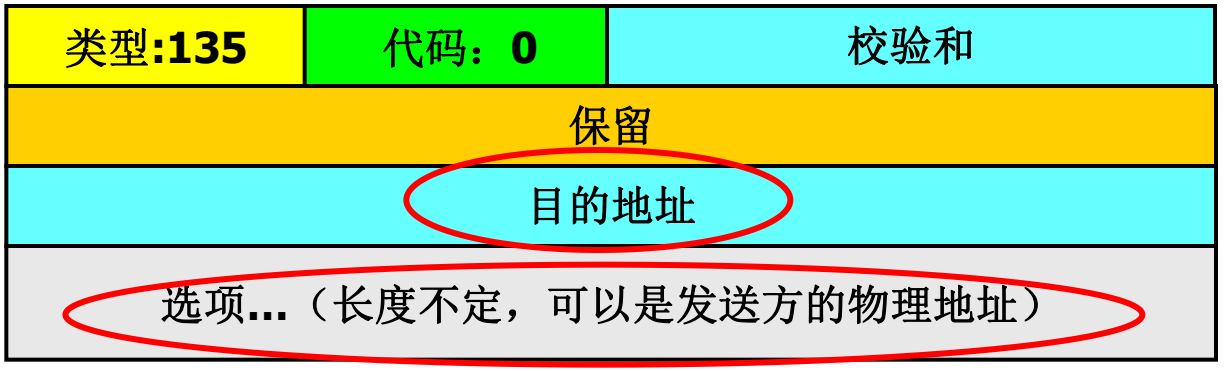


  - M标志： IPv6地址使用有状态的配置方式
  - O标志：除IPv6地址之外的网络信息也使用有状态配置
  - 选项：源链路层地址、MTU、前缀信息


开始
Stateless
（链路本地单播地址）
生成链路本地地址
FE80::/64+EUI-64
发送RS
Stateless
（全球单播地址）
收到RA
N
Y
获得RA报文中的
M flag
M flag
0
生成链路本地地址
网络前缀+64+EUI-64
1
O flag
0
1
DHCPv6
配置地址
用DHCPv6获取并配置
IPv6地址
用DHCPv6获取并配置
其他参数(如DNS)
Stateful DHCPv6
用DHCPv6获取并配置
其他参数(如DNS)
Stateless DHCPv6
结束

邻居请求和邻居通告

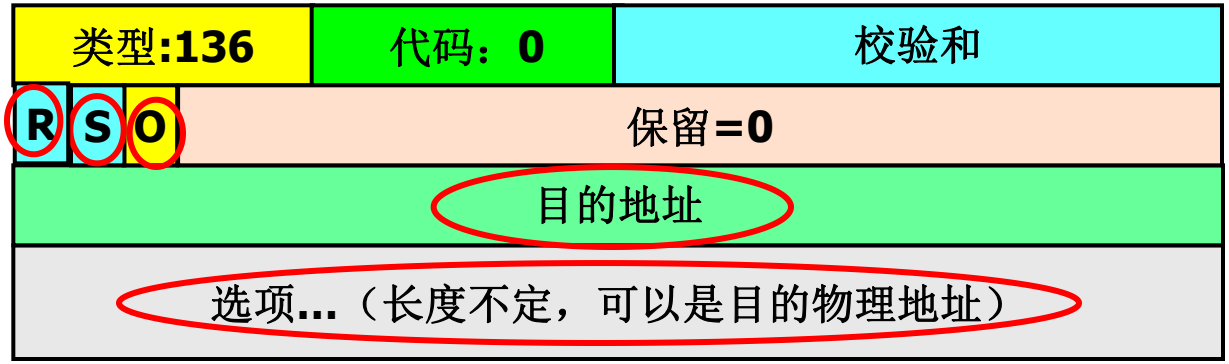
- 邻居请求NS/邻居通告NA
- 功能：实现地址解析、邻居不可达性检测和重复地址检测
- NS报文



- 源IP地址：接口单播地址/::
- 目的IP地址：多播地址/单播地址
- 目的地址：被请求的IPv6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

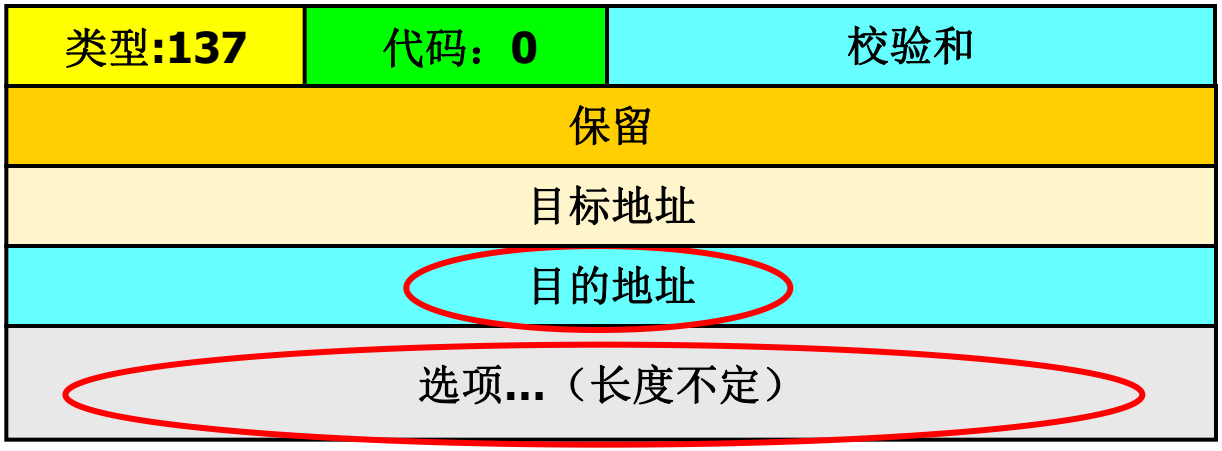
- NA报文



  - 源IP地址： 接口单播地址/::
  - 目的IP地址：FF02::1/单播地址
  - 目的地址：被请求的IPv6地址
  - 选项：目的结点物理地址(目的链路层地址)

重定向

- 功能:优化主机路由表
- 报文格式



  - 源IP地址： 接口链路本地地址
  - 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

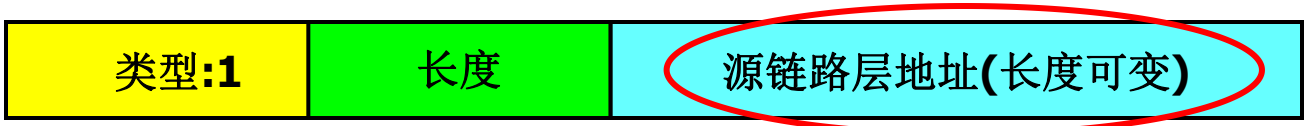
邻居发现协议报文选项

- IPv6首部+邻居发现报文首部+报文选项
- 邻居发现选项

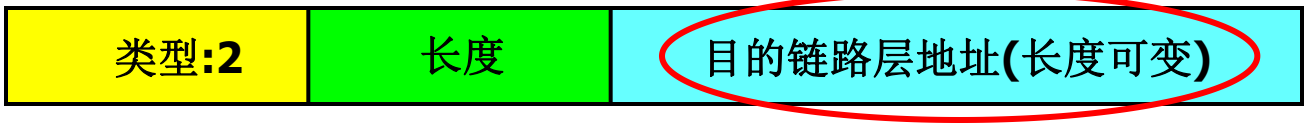
邻居发现报文	邻居发现选项
路由器请求RS	源链路层地址
路由器公告RA	源链路层地址、MTU、前缀信息 通告间隔、家乡代理信息、路由信息
邻居请求NS	源链路层地址
邻居通告NA	目的链路层地址
重定向	目的链路层地址、被重定向首部

邻居发现协议的选项

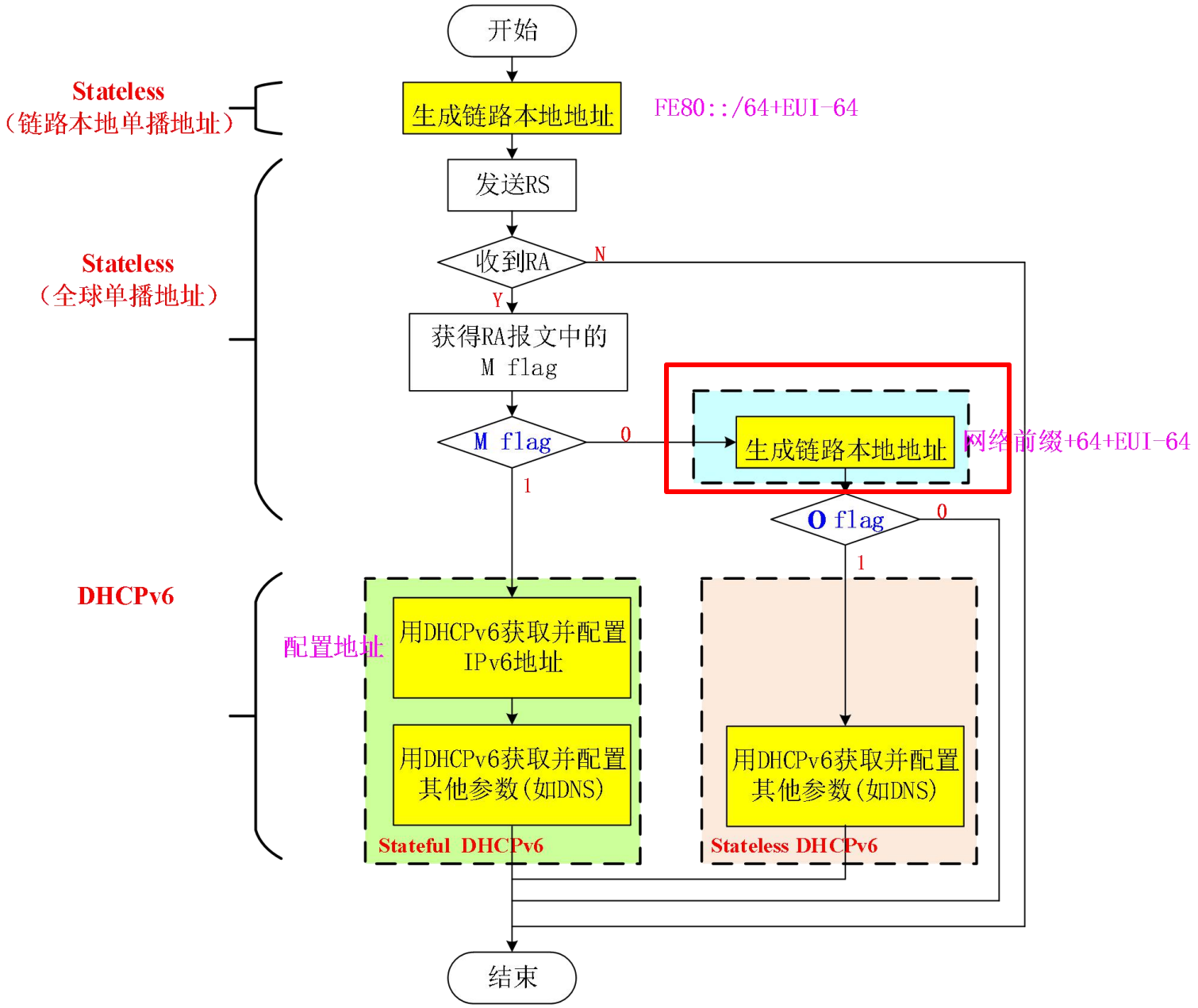
- 源链路层地址选项: 发送者的链路层地址



- 目的链路层地址选项： 目标链路层地址

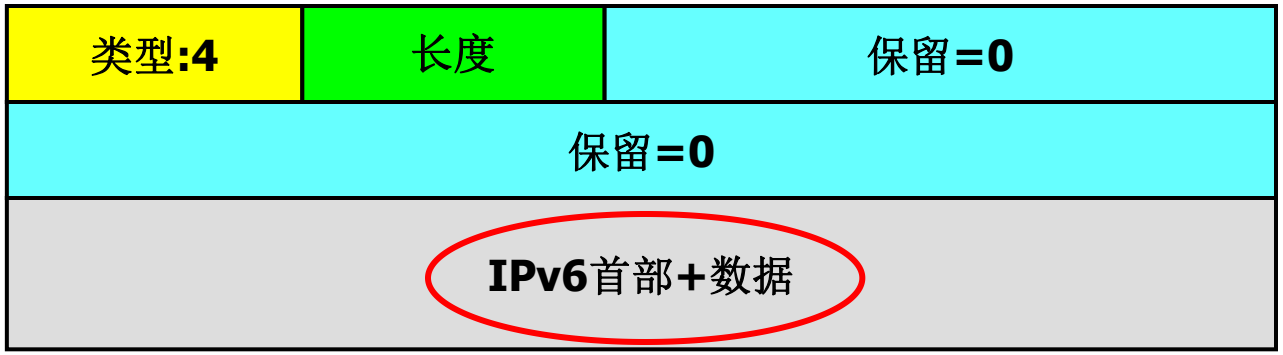


- 前缀信息选项： 一个IPv6前缀或者地址

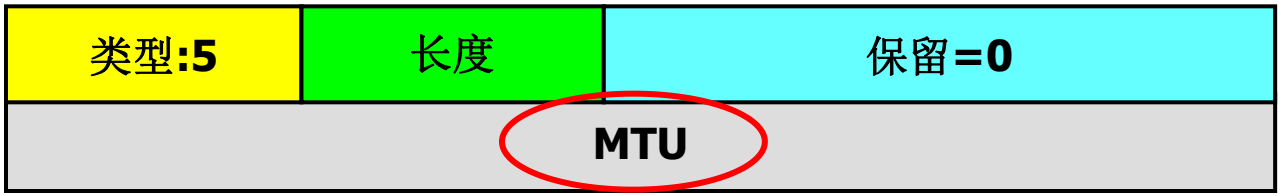

开始
Stateless
（链路本地单播地址）
生成链路本地地址
FE80::/64+EUI-64
发送RS
Stateless
（全球单播地址）
收到RA
N
Y
获得RA报文中的
M flag
M flag
0
1
生成链路本地地址
网络前缀+64+EUI-64
O flag
0
1
DHCPv6
配置地址
用DHCPv6获取并配置
IPv6地址
用DHCPv6获取并配置
其他参数(如DNS)
Stateful DHCPv6
用DHCPv6获取并配置
其他参数(如DNS)
Stateless DHCPv6
结束

邻居发现协议的选项

- 被重定向首部：原始IPv6报文的部分

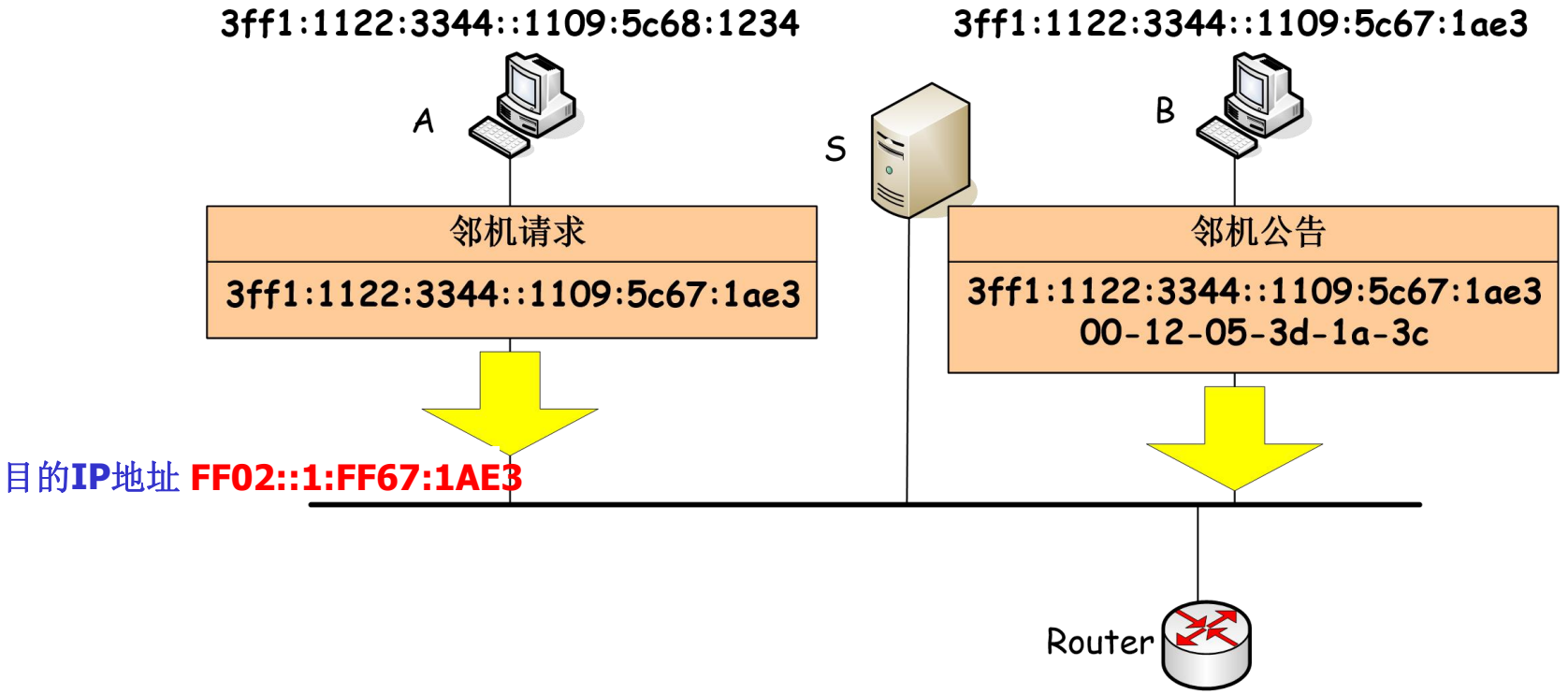


- MTU选项：推荐的MTU，确保链路上所有节点使用相同的MTU



IPv6地址解析

- 源向本链路上的其他系统组播邻机请求
  - 如何保证请求消息只限制在本链路范围内？
  - 如何既确保所查找的主机在组播组内又能尽量减少处理该请求消息的系统个数，最好只有所请求的系统处理该消息



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）

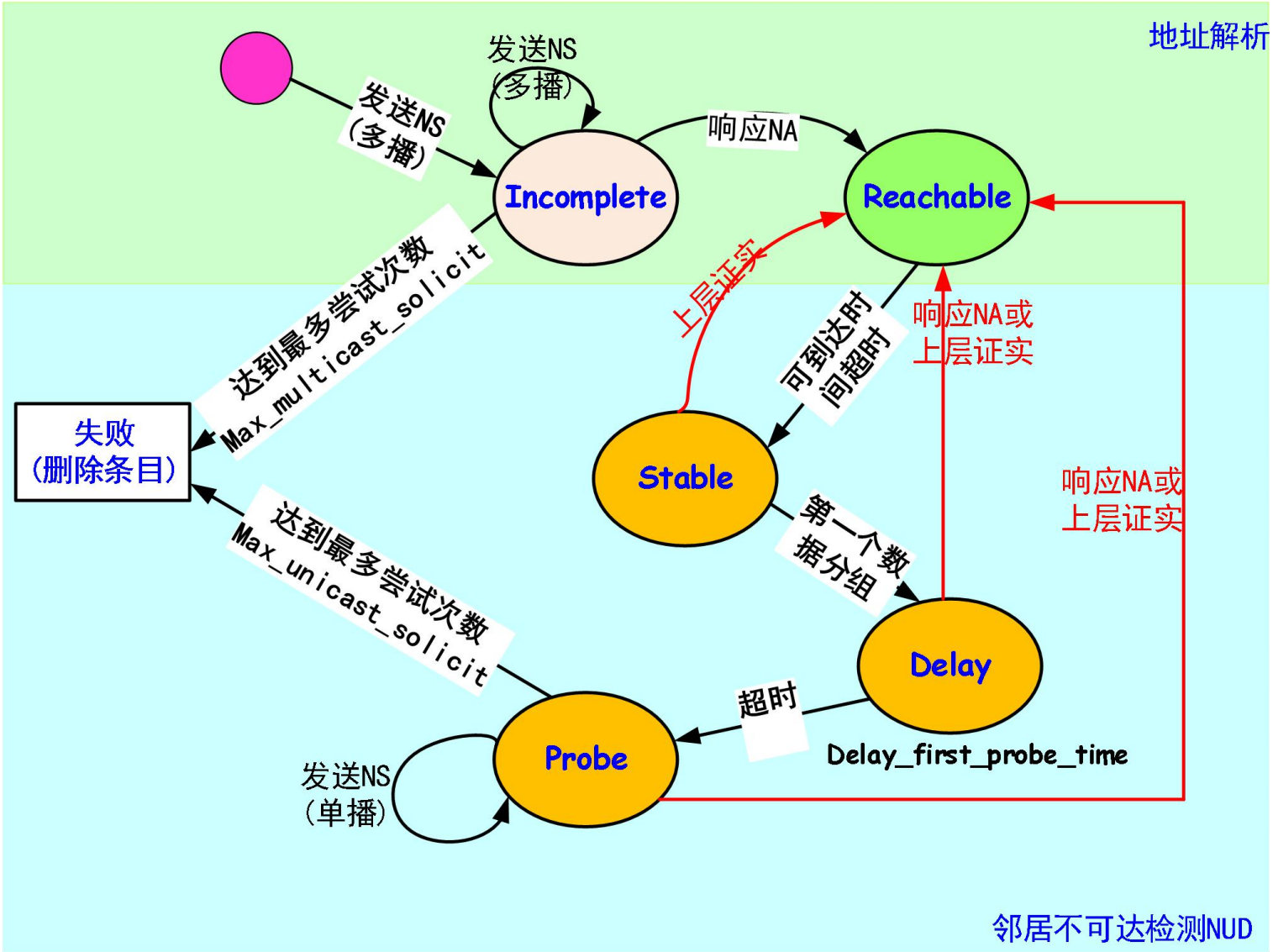
邻机不可达检测

- 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（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

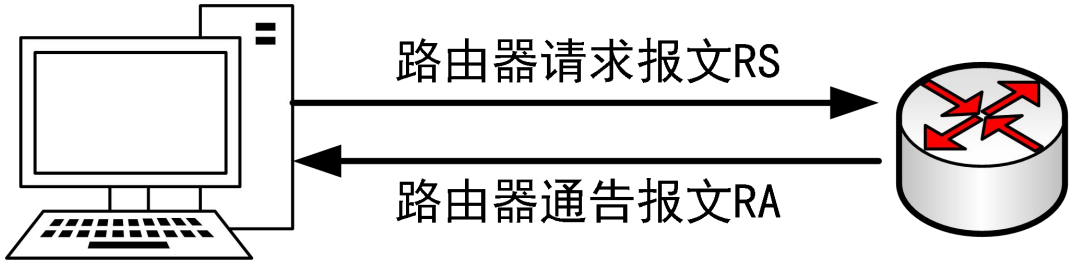
  - Max-multicast-solicit(默认为3)
  - Max-unicast-solicit(默认为3)
  - Delay-first-probe-time(默认为5s)

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)
Stable
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

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

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[illegible]址
  - 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

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）

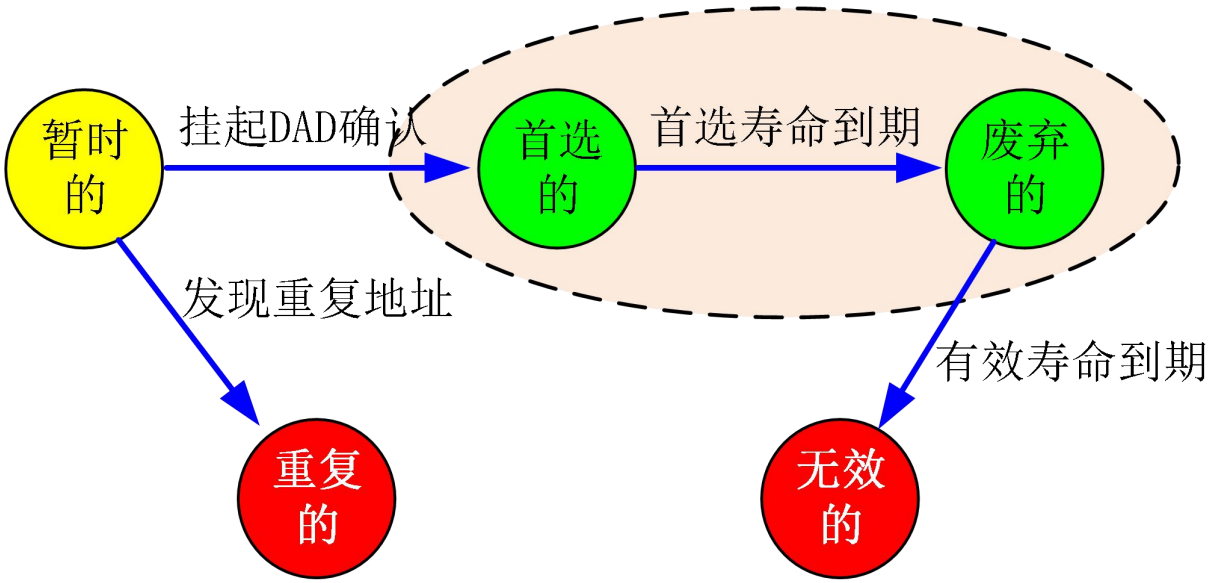
MAC

源：接口的MAC地址

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

地址自动配置

- IPv6单播地址状态
  - 首选状态和废弃状态是有效状态，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。



邻居发现协议小结

- 实现的功能
  - 路由器发现：前缀发现、参数发现(本地MTU之类信息)
  - 地址自动配置
  - 地址解析
  - 邻居不可达检测
  - 重复地址检测
  - 重定向

ICMP的应用

- 主机可达性测试：Ping
  - 方法：使用ICMP回送和应答消息来确定一台主机是否可达
  - 作用：Ping是因特网包探索器，Ping发送一个ICMP回声清求消息给目的地并报告是否收到所希望的ICMP回声应答使用ping命令，通过发送数据包，能够测试两台计算机之间的因特网连接是否正常、网卡配置是否正确、IP地址是否可使用等

ICMP的应用

- Traceroute命令
  - 作用：Traceroute命令依赖于ICMP协议，该测试工具能够跟踪数据包访问网络中某个节点时所走的路径，进行路由跟踪，以用来分析网络和排查网络故障。
  - 实现方法：通过发送小的数据包到目的设备直到其返回，来测量其需要多长时间。把一个TTL=1的数据报发送给目的主机，第1个路由器把TTL减小到0，丢弃该数据报并把ICMP超时消息返回给源主机，这样路径上第1个路由器就被标识了。随后不断增大TTL值重复该过程。

ICMP的应用

- 路径MTU发现
  - 方法：向目标节点发送“要求报告分片但又不被允许”的ICMP报文。
  - 步骤
    - 将IP数据报的标志域中的分片BIT位置1，不允许分片；
    - 路由器发现IP数据报长度大于MTU时，丢弃数据报，并发回一个要求分片的ICMP报文
    - 将IP数据报长度减小，分片BIT位置1重发，接收返回的ICMP报文分析
    - 发送一系列长度递减、不允许分片的数据报，通过接收返回的ICMP报的分析，可确定路径MTU.

ICMP相关的攻击

- 背景
  - 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
- 涉及ICMP的主要攻击类型
  - 信息泄露information disclosure
  - 泛洪攻击flood
  - 炸弹bomb

ICMP相关的攻击

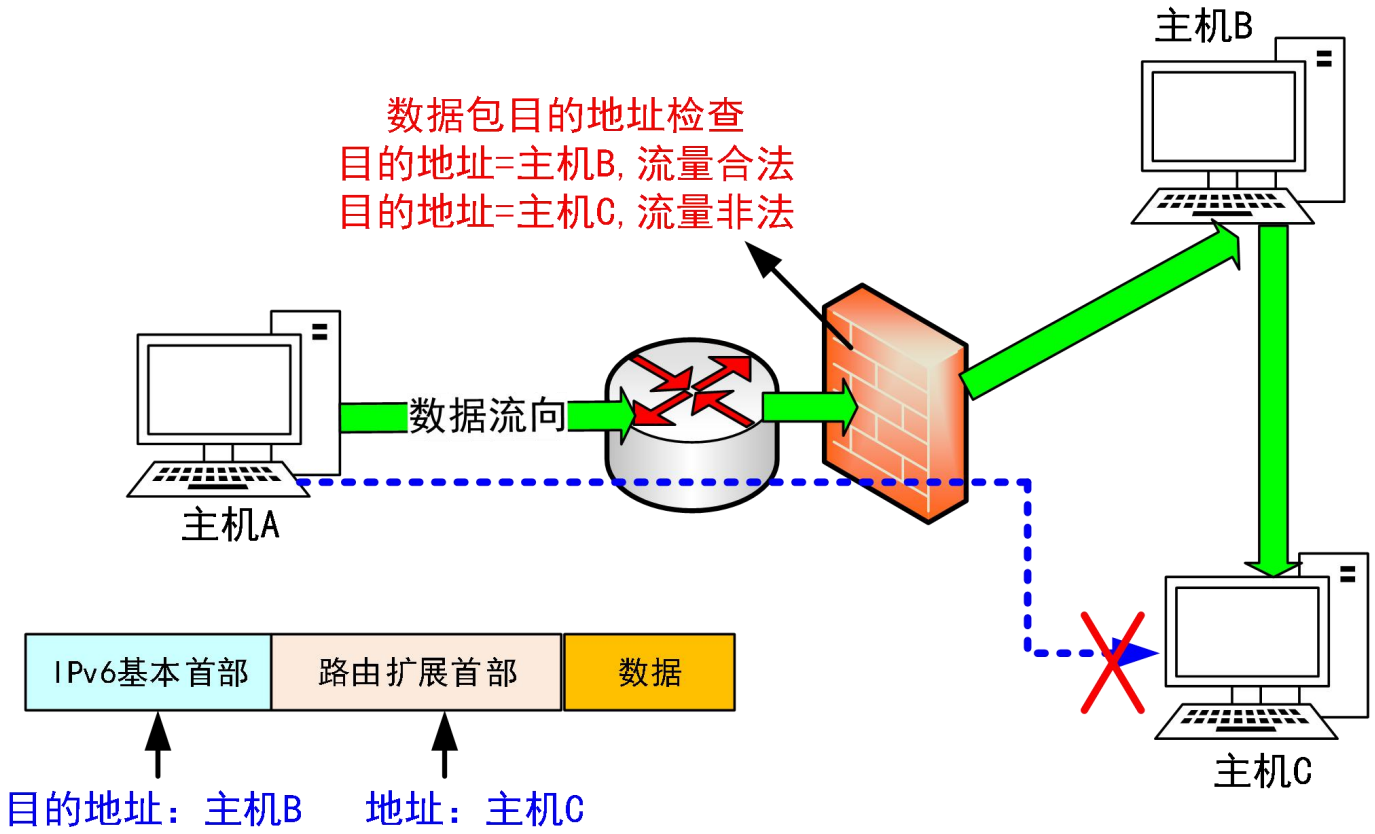
- ICMP差错报告存在的安全问题
  - ICMP的主要功能是在Internet体系结构中执行故障隔离功能，即主机和路由器采取的一组动作来确定是否存在网络故障
  - 主机或路由器报告的ICMP错误被传递给相应的传输协议(如TCP)来执行故障恢复功能
  - 攻击者可以向被攻击的系统发送一个精心设计的ICMP错误消息来执行各种攻击
  - 针对TCP协议的ICMP攻击被专门记录在 **RFC5927**

ICMP相关的攻击

- 侦查攻击：攻击者从被攻击网络中收集数据以便实施进一步的攻击。
  - 数据包括：网络中的设备地址、开放的端口等
  - Ping探测
- Flooding攻击：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
  - 滥用ICMPv6和多播地址
  - 滥用路由扩展首部

ICMP相关的攻击

- 协议欺骗攻击：利用协议漏洞进行攻击
  - 利用路由扩展首部的协议进行欺骗攻击

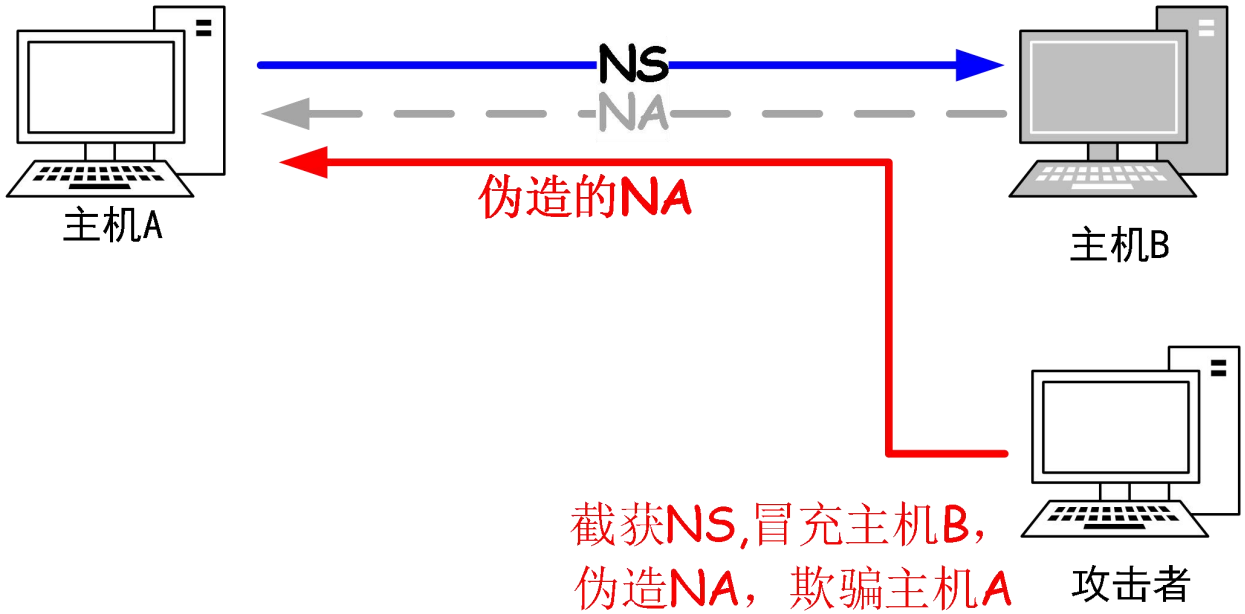


ICMP相关的攻击

- 冒充路由器发送虚假RA消息攻击
  - 虚假链路地址：DoS攻击、黑洞攻击
  - 发送错误网络前缀，使被攻击的节点按此参数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

ICMP相关的攻击

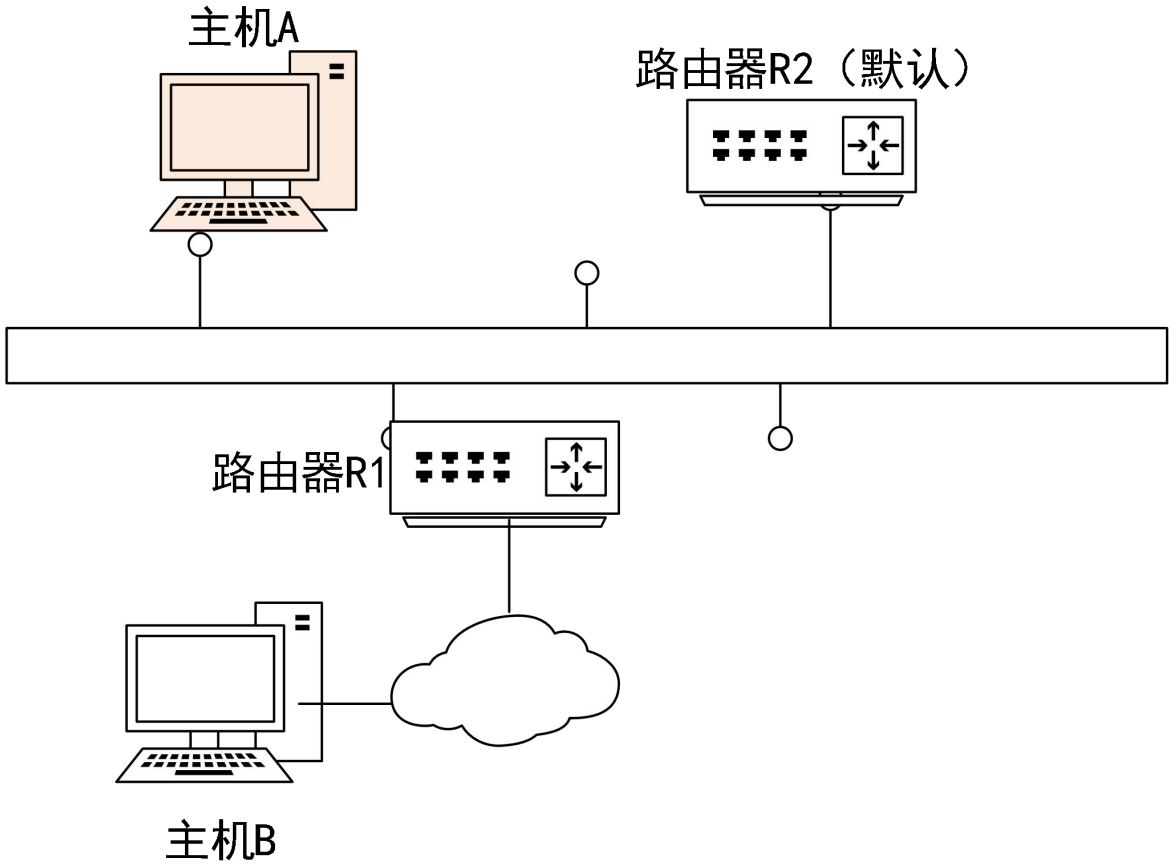
- 基于邻居发现的DoS攻击
  - 基于NUD进行DoS攻击



  - 基于DAD进行DoS攻击

ICMP相关的攻击

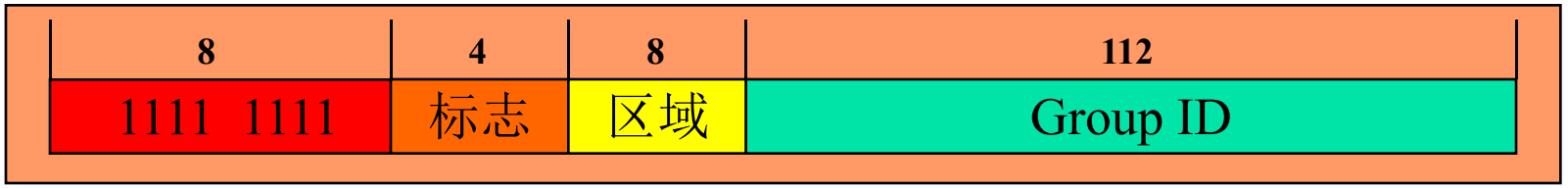
- 基于重定向的攻击



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**。

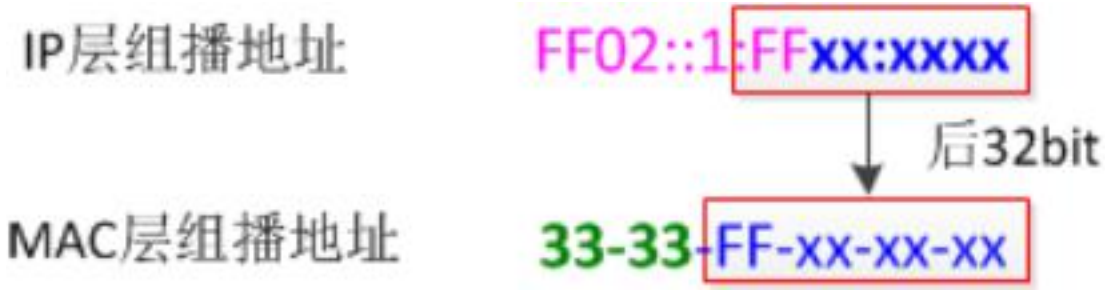
附录B：IPv6组播IP地址与组播MAC地址之间的换算方法

- 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

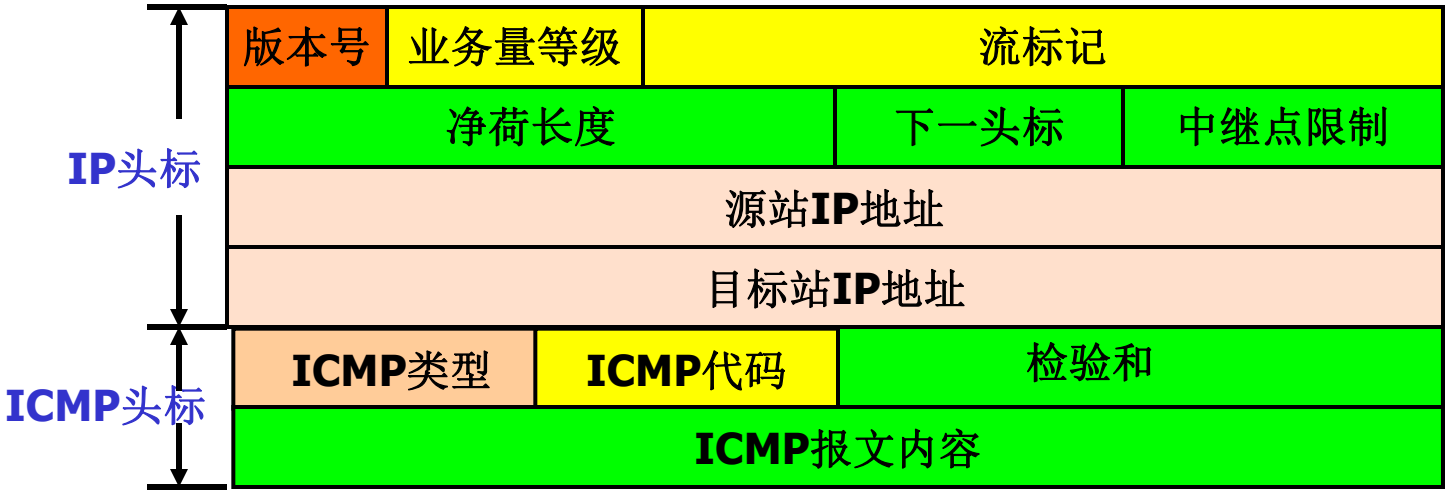
举例：00-AA-00-3F-2A-1C

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

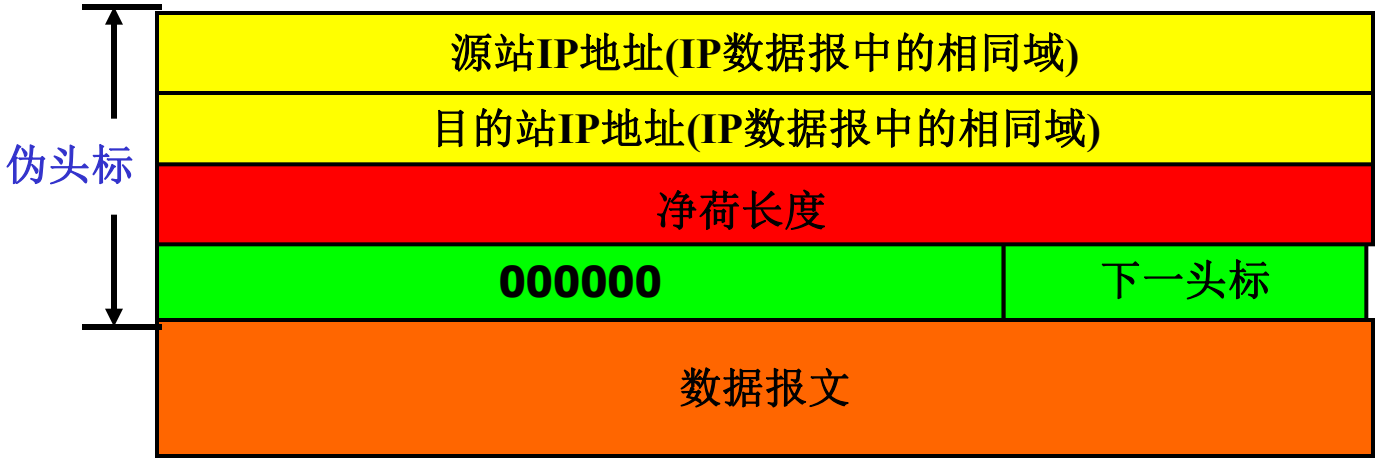
即：02-AA-00-FF-FE-3F-2A-1C

附录D：伪头标校验

- 关于数据的校验问题
  - IP基本头标无校验
  - IP包中的数据部分的报文格式中如果有校验和域，则该校验和的计算需要使用伪头标



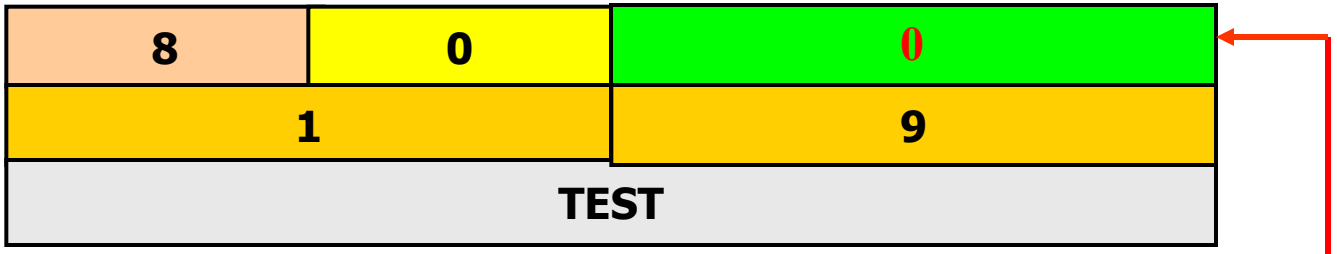
- IP基本头标中的关键数据
  - 信源地址
  - 信宿地址
  - 下一头标
  - 净荷长度



附录E: 16比特校验

- 校验和的计算
  - 校验和字段设置为0
  - 计算校验域内的所有16位字之和
  - 取反，得到校验和
- 校验和的检测
  - 计算校验域内的所有16位字之和
  - 把得到的和求反
  - 结果如果为16个0，则接受，否则拒绝。

附录1: 16特加法校验



8 和 0	00001000	00000000
0	00000000	00000000
1	00000000	00000001
9	00000000	00001001
T 和 E	01010100	01000101
S 和 T	01010011	01010100
和	10101111	10100011
校验和	01010000	01011100