下一代互联网技术

第二章　IPV6协议

IPV6协议——下一代互联网的基础

- “IPv4地址协议转向IPv6地址协议是下一代互联网的起点，将对移动互联网和新媒体的发展起到重要的支持作用。”

-----邬贺铨

中国工程院院士

光纤传送网和宽带信息网著名专家

本章内容

- 2.1 IPV4局限性与IPV6特点
- 2.2 IPV6地址表达与分类
- 2.3 IPV6数据报及报头
- 2.4 ICMPV6协议
- 2.5 IPv4向IPv6过渡

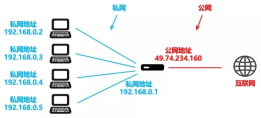
2.1.1 IPV4局限性

- IPv4面临的最紧迫问题是地址不足(约42.9亿个)
- 官方宣布IPv4地址全部耗尽的区域只有北美ARIN和欧洲RIPE NCC，实际上五区都有自己的IPv4地址调配流程，包括：分阶段消耗、预留策略和限量策略，以便延缓衰减时间顺利迁移至IPv6

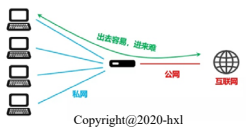
分配机构	地址耗尽日期	分配机构	地址耗尽日期
IANA	2011年1月31日	LACNIC(拉美)	2014年6月10日
APNIC(亚太)	2011年4月15日	ARIN(北美)	2015年9月24日
RIPE(欧洲)	2019年11月25日	AFRINIC(非洲)	2017年4月21日

2.1.1 IPV4局限性

- IPv4解决地址紧缺的主要研究方向在于如何减少地址空间的浪费并提高地址的使用效率：
  - 例如NAT(Network Address Translation，网络地址转换）

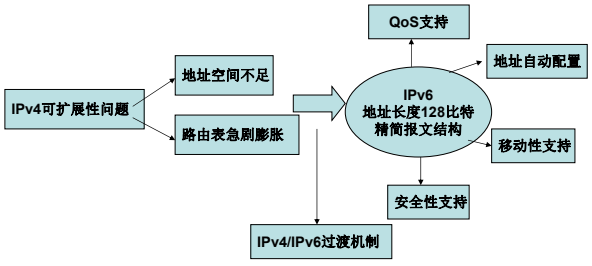


  - 缺点：虽然私网地址访问互联网地址方便，但互联网地址访问私网地址要解决穿透问题，使得很多应用都会受到限制，只能通过复杂的设置才能解决，严重影响网络的处理效率。



2.1.1 IPV4局限性

- 内容共享、游戏、VoIP、分布式协同工作等新的实时性因特网应用，对网络层实时数据传送服务质量Qos提出了更高的要求
- IPV4不支持移动性和网络管理能力，需要更简便的IP地址配置方案
- IP级安全性的需求



2.1.2 IPV6 特点

- 巨大的地址空间
- 简化的协议首部
- 身份认证和加密
- 更好的Qos保证
- 地址自动配置
- 使用新协议处理邻接点交互
- 支持层次化网络结构
- 可扩展性
- .....

2.1.2 IPV6 特点

- 巨大的地址空间
  - 128位地址长度可以提供3.402823669 $\times 10^{38}$个IP地址
  - 有效的分级寻址和路由结构
    - 允许使用多级的子网划分和地址分配，更好的适应ISP层次结构和网络层次结构
- 简化的协议首部格式
  - IPv6使用了固定格式的首部，并减少了需要检查和处理的字段数量，这将使得路由器选路效率更高。
    - 首部长度固定为40个字节8个字段
    - IPv6中的分片只能由源节点进行：该数据报经过的中间路由器不能再进行任何分片
    - 首部校验和将由更高层协议(UDP和TCP)负责。

2.1.2 IPV6 特点

- 身份认证和加密
  - Ø 支持IPSec协议，可以对网络层数据加密，并对IPV6报文进行校验，使用了两种安全性扩展：
    - IP身份验证头(AH)
    - IP封装安全性净荷(ESP)
- 更好的QoS保证
  - Ø 协议头中的通信流类型字段可以区分通信流的优先级
  - Ø 流标记字段使得路由器可以对属于一个流的数据报进行识别和特殊处理。
  - Ø 在IPv4中，每个包都是由中间路由器按照自己的方式来处理

2.1.2 IPV6 特点

- 地址自动配置
  - IPv6提供了有状态和无状态地址自动配置两种方案，实现即插即用
- 用新协议处理邻接点的交互
  - IPV6的邻接点发现协议使用了网络控制报文协议ICMPV6，以更加有效的组播和单播的邻接点发现报文,来解析邻接点的数据链路层地址,并监测邻接点是否可达,用来管理同一链路上的相邻结点之间的交互过程

2.1.2 IPV6 特点

- 支持层次化网络结构
  - IPv6采用的多层次地址结构提供了更多的路由信息
  - 几乎所有的路由算法都做了相应的改进
  - 还使用了一个单独的扩展首部来提供源站路由
- 可扩展性
  - 通过添加新的扩展报头，IPV6允许协议进行扩充，实现功能的扩展

随堂思考

- IPv6的唯一驱动力是地址空间不足？
- 不需要全新的IPv6，只要对IPv4进行扩充就足够？
- IPV4的NAT技术已较好的解决了地址空间不足的问题，例如P2P应用的问题已经可以通过UDP穿越等方法得到解决，BT等这些P2P应用已经可以在NAT后面连接，因此无需升级到IPV6.

随堂思考

- IPv6的唯一驱动力是地址空间不足？
  - 答：地址空间不足仅仅是其中的一个原因。若为解决地址空间不足，使用64位的地址就够了。采用128位地址，是因为它能提供更好的层次结构，这对高效的路由算法、地址自动配置来说是必不可少的。
- 不需要全新的IPv6，只要对IPv4进行扩充就足够？
  - 答：原始的TCP/IP框架已经发展到极限，已不可能再通过打补丁的方式来应付了IPV4暴露出来的缺陷，尤其无法保证多媒体业务的服务质量，以及提供网络安全性，移动性方面的支持。

随堂思考

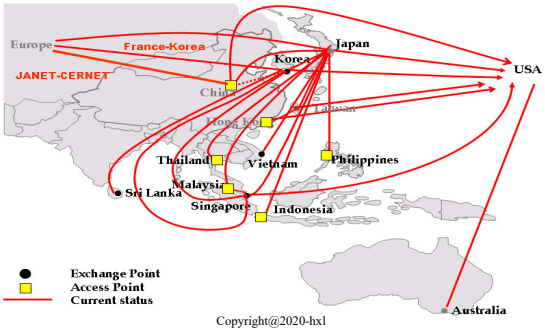
- IPV4的NAT技术已较好的解决了地址空间不足的问题，例如P2P应用的问题已经可以通过UDP穿越等方法得到解决，BT等这些P2P应用已经可以在NAT后面连接，因此无需升级到IPV6。
  - 答：NAT技术破坏了端到端的高性能通信模式，尽管很多P2P应用确实可以很好的克服NAT的穿越问题，但这些克服不是从TCP/IP协议的角度来解决，而是应用程序自定义私有协议来解决，这不符合网络分层设计原则，不但增加了程序设计人员重复劳动，降低效率，也提供给黑客更多发现应用程序漏洞的机会

2.1.3 IPV6 发展历程

- 1992年， 互联网工程任务组（IETF）成立下一代协议（IPng）工作组
- 1994年，IPng工作组提出下一代IP网络协议（IPv6）的推荐版本
- 1995年，NSF支持的下一代互联网NGI计划，建立了NGI的主干网vBNS，IPng工作组完成IPv6的协议文本
- 1998年，UCAID成立，提出Internet2计划，建立了Internet2的主干网Abilene，亚太地区先进网络计划APAN
- 1998年，IPV6被IETF正式推出，即互联网标准规范RFC2460
- 1999年，成立IPv6论坛，开始分配IPv6地址，确立IPv6标准草案
- 2001年，欧共体建立了下一代互联网的主干网GEANT，多数主机操作系统如WindowsXP，linux，Solaris开始支持IPv6
- 2003年，IETF发布了IPV6测试性网络6Bone

Asia-Pacific Advanced Network

- 日本、韩国和新加坡三国在1998年发起建立“亚太地区先进网络APAN”，加入下一代互联网的国际性研究。日本目前在国际IPv6的科学研究乃至产业化方面占据国际领先地位。



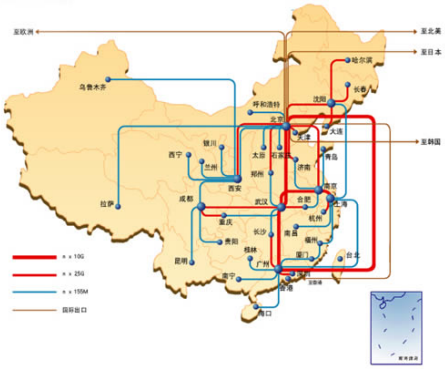
Initial GEANT2 topology

- 欧共体于2001年建立了横跨31个国家的主干网GéANT，并以此为基础全面进行下一代互联网各项核心技术的研究和开发。

2.1.4 IPV6在中国

- 2002年， 中国启动下一代互联网示范工程CNGI
- 2004年，中国建成CERNET2（第二代中国教育和科研计算机网）是中国下一代互联网示范工程CNGI最大的核心网，也是目前世界上规模最大的采用纯IPv6技术的下一代互联网主干网。2005年7月，美国政府决定2008年6月过渡到IPV6
- 2009年， 中国电信在湖南、江苏启动下一代互联网试点
- 2011年12月23日， 国务院出台下一代互联网规划
- 2012年6月6日，国际互联网协会专门举行了“世界IPv6启动纪念日”。这一天，多家知名网站(如Google、Facebook和Yahoo等)正式开始永久性支持IPv6访问

CERNET2 Backbone

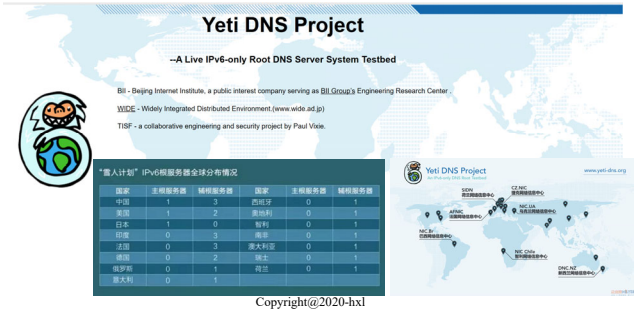


2.1.4 IPV6 在中国

- 2017年11月26日，中共中央办公厅、国务院办公厅印发《推进互联网协议第六版（IPv6）规模部署行动计划》。国内首个IPv6公共DNS 240c::6666正式发布。
- 2018年6月，三大运营商联合阿里云宣布，将全面对外提供IPv6服务，并计划在2025年前助推中国互联网真正实现“IPv6 Only”。
- 2018年7月，百度云推出IPv6落地方案，在第17届中国互联网大会上，腾讯披露了腾讯云IPv6“三步走”推进计划。
- 2018年11月，国家下一代互联网产业技术创新战略联盟在北京发布了中国首份IPv6业务用户体验监测报告显示，移动宽带IPv6普及率为6.16%，IPv6覆盖用户数为7017万户，IPv6活跃用户数仅有718万户，与国家规划部署的目标还有较大距离。
- 2018年12月6日，阿里云宣布为企业提供全栈IPv6解决方案，加速推进中国下一代互联网应用。
- 2019年4月16日，工业和信息化部发布《关于开展2019年IPv6网络就绪专项行动的通知》。
- 2019年5月，中国工信部称计划于2019年末，完成13个互联网骨干直联点IPv6的改造。

2.1.4 IPV6在中国

- 2017年11月28日，由下一代互联网国家工程中心牵头发起的“雪人计划”（www.yeti-dns.org），已在全球完成25台IPv6 DNS根服务器架设，中国部署了其中的4台，由1台主根服务器和3台辅根服务器组成。



扩展阅读

- 中国教育和科研计算机网
  https://www.edu.cn/xxh/ji_shu_ju_le_bu/cernet2_lpv6/
- 阿里巴巴宣布全面应用IPv6技术 布局下一代互联网
  http://www.xinhuanet.com/tech/2018-12/06/c_1123816703.htm
- 工信部宣布开展2019年IPv6网络就绪专项行动
  https://baijiahao.baidu.com/s?id=1630951817068802857&wfr=spider&for=pc
- 国内外 IPv6 网络发展现状——群文件及课程中心“课后阅读”

2.1.5 IPv6协议标准化及研究组织

- IETF ： http://www.ietf.org
  - IP Version 6 Working Group
    - 制订IPv6规范和标准
  - IPv6 Operations
    - 为运营IPv4/IPv6共存的Internet和在已有的IPv4网络或者新的网络安装中部署IPv6提供指导
  - 其它IPv6相关工作组
    - 6lowpan, mip6, mipshop, monami6, multi6, shim6…
- 3GPP ： http://www.3gpp.org
  - IP多媒体子系统 (IMS)使用IPv6
- ITU-T ： http://www.itu.int/ITU-T/index.html
  - 在电信网络中采用IPv6技术

2.1.5 IPv6协议标准化及研究组织

- The IPv6 Forum：http://www.ipv6forum.com
  - 倡导IPv6，提升IPv6的市场和用户意识
  - IPv6 Ready Logo Program (Phase 2)
- WIDE：http://www.wide.ad.jp
  - KAME，USAGE，TAHI：实现和验证IPv6
  - Nautilus6：移动通信中的IPv6应用
  - .....
- IPv6 Cluster：http://www.ist-ipv6.org
  - 欧洲IPv6研究和开发项目
  - IPv6 Cluster Member：Euro6IX ，6NET…

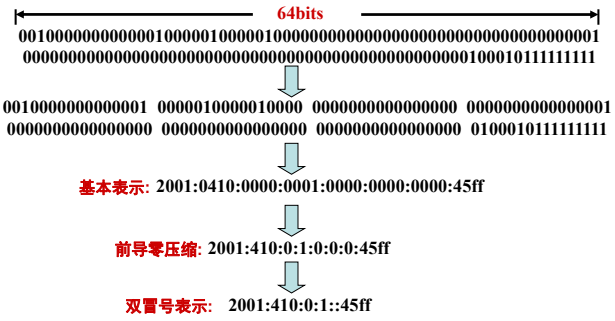
本章内容

- 2.1 IPV4局限性与IPV6特点
- 2.2 IPV6地址表达与分类
- 2.3 IPV6数据报及报头
- 2.4 ICMPV6协议
- 2.5 IPv4向IPv6过渡

2.2.1 IPV6地址表示

- IPV6地址表达方式
  - 基本表示方法：十六进制冒号分割法
    - 128位地址按每16位划分为一个位段,每个位段被转换为一个4位的十六进制数,并用冒号隔开
    - 如 21DA:0000:0000:0000:02AA:000F:FE08:9C5A
  - 前导零压缩法：压缩某些位段的前导零
    - 以上地址还可表示为21DA:0:0:0:2AA:F:FE08:9C5A
    - 不能把一个位段内部有效的0也压缩掉,如 FE08不能被压缩成FE8
  - 双冒号表示法（压缩零位）：
    - 以上地址还可表示为21DA::2AA:F:FE08:9C5A
    - ::在一个地址中只能出现一次

2.2.1 IPv6地址表示



2.2.1 IPv6地址表示

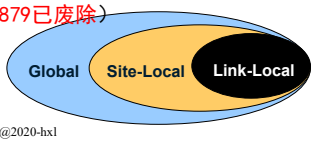
- IPV6不支持子网掩码，它以地址前缀表示法，来标识子网或IPV6路由。
- 地址前缀表示法：
  - 格式：IPv6地址/前缀长度
  - 64位前缀用来表示结点所在的子网
  - 任何少于64的前缀，要么是一个路由前缀（即汇总的路由条目），要么是一个包含了部分IPV6地址空间的地址范围
  - 在已经定义的IPV6单播地址中，默认用于标识子网的位数与用来标识子网内主机的位数都是64
  - 例子：P77

2.2.2 IPV6地址类型

- 单播地址(Unicast Address)
- 组播地址(Multicast Address)
- 任播地址(Anycast Address)
- 特殊地址
- 更详细内容请参考RFC4291

IPV6单播地址

- 标识IPV6网络的一个区域中单个网络接口地址，寻址到单播地址的分组将被发送到该接口
- 主要类型有：
  - 全球单播地址
    - 可以支持有效的多级寻址和路由的能力
    - 可以在全球范围的IPV6网络内有效的路由
  - 本地单播地址
    - 链路本地地址
    - 唯一本地地址
    - 站点本地地址（RFC3879已废除）



IPV6全球单播地址

- 全球单播地址（IPV6的公网地址，全球可达）

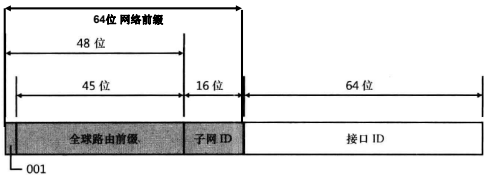


图 3-1　RFC 3587 定义的全球单播地址结构

- 全球路由前缀48位：由IANA来管理，分配给那些大的永久的ISP，标识路由层次结构的最高层，最高3位固定为001
- 子网ID：ISP在自己网络中建立的多级寻址机构，标识组织内的子网
- 接口ID：标识特定一个节点与子网的接口，包含IEEE EUI-64接口标识符的64位值

IPv6的接口标识符

- IPv6接口标识符的生成方式
  - 使用状态化地址自动配置技术来分配（DHCPV6）或手动配置地址来分配
  - 基于EUI-64接口标识符
    - EUI-48地址转换成EUI-64
    - 对U/L标志位值取反，获得IPV6接口标识符
    - 不论用户每次连接时分配的IPV6前缀是多少，都能唯一的标明这个用户的分组，并很容易追踪到一个特定用户。
    - 详细步骤
  - 随机接口标识符
    - 随机接口标识符的生成步骤
    - 采用随机接口标识符产生的IPV6地址都是临时地址，具有生存期的限制，有效生存期过后，将产生一个新的随机接口标识符和新的临时IPV6地址。

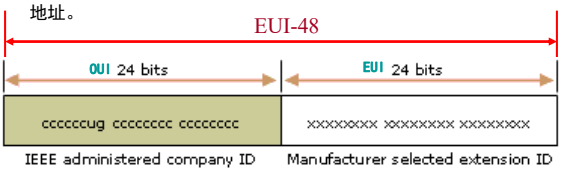
注意：为了保护隐私，Windows Vista和Windows Server Longhorn缺省使用随机接口标识生成非临时地址

随机接口标识符生成

- 若不能存储历史信息
  - 每次初始化IPv6协议栈的时候生成新随机接口标识
- 若支持存储历史信息，则基于链路层地址或序列号
  - 获取历史值，并且将其附到基于EUI-64地址的接口标识上
  - 对于第1步生成的值计算一个128比特的MD5摘要
  - 取第2步中最左边的64比特，并将第7比特设置为0，生成一个全局的随机接口标识符
  - 取第2步最右边的64比特并且将其保存，作为下一次计算的历史值

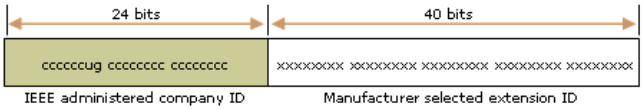
EUI-48地址

- IEEE802.3定义了48位介质访问控制(MAC)地址，如下所示：
- MAC地址具有全球唯一性，由厂商烧入网卡中，用来唯一标识网络链路层上的接口。
- 标志位：
  - U/L(全球/本地标志位)：在第一个字节的第7位，0-全局;1-本地管理
  - I/G(单个站/组)：在第一个字节的第8位，0-单播；1-组播
  - 对于一般的802网络接口，U/L和I/G比特都设置为0
  - 通常情况下，U/L和I/G位都会被设置为0，表示全球管理的单播MAC地址。



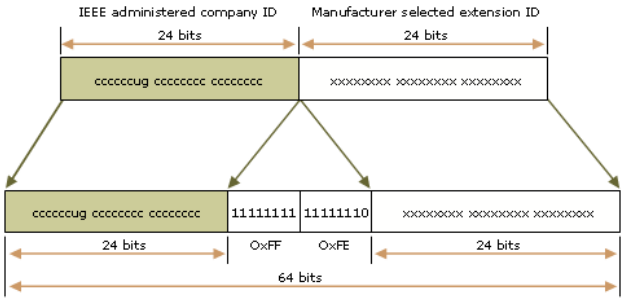
EUI-64地址

- 由EUI-48扩展而来，在RFC2373中定义
- 为网络接口卡制造商提供了更多的地址空间
- 标志位：
  - U/L：0-全局；1-本地管理
  - I/G：0-单播；1-组播



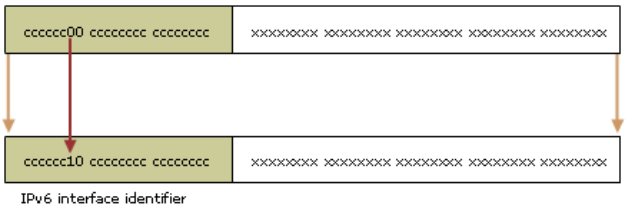
EUI-48到EUI-64的映射

- 在EUI-48的OUI和EUI之间插入16比特(0xFFFE)

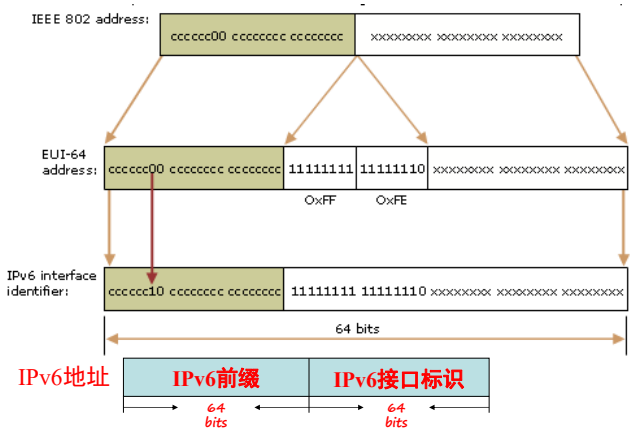


EUI-64地址到IPv6接口标识符的映射

- 对EUI-64地址的U/L比特取反，例如EUI-64地址中是1，则置为0，如EUI-64地址中是0，则置为1，I/G比特不变
- 原因（97）



EUI-48到IPv6接口标识符的映射



IPv6接口标识符映射的例子

- 主机A的以太网MAC地址为00-AA-00-3F-2A-1C

00	AA	00	FF	FE	3F	2A	1C

- 对首字节00000000的U/L位(第7位)取反为00000010

02	AA	00	FF	FE	3F	2A	1C

- 得到接口标识符：02AA:00FF:FE3F:2A1C
- 最后得到链路本地地址为：FE80::2AA:FF:FE3F:2A1C

IPV6本地单播地址

- 本地使用的单播地址
  - ➢唯一本地地址（前缀是FC00::/7）

8比特	40比特	16比特	64比特
1111 1100	0	子网ID	Interface ID

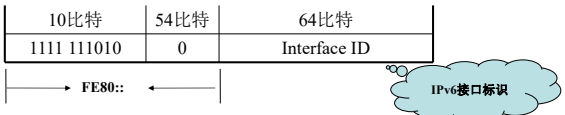
  - 相当于IPV4私网地址（10.0.0.0，172.16.0.0，192.168.0.0）
  - ➢ 链路本地(Link-local)地址(FE80::/64）

10比特	54比特	64比特
1111 111010	0	Interface ID

  - 前缀是FE80::0/64
  - 用于节点与同一链路上的邻居节点通信，所以每个接口必须至少有一个链路本地地址
  - 可自动配置，及用于邻接点发现

基于EUI-64生成链路本地地址实例

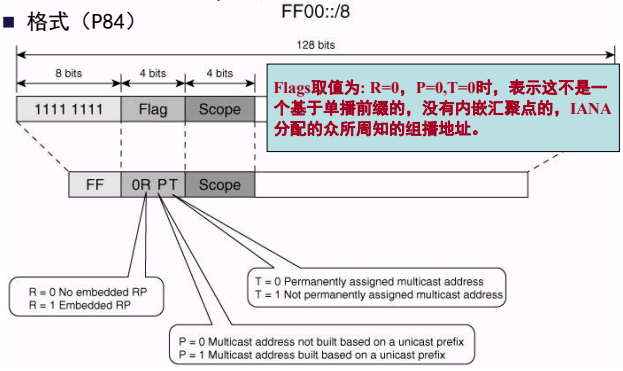
主机	IP地址	MAC地址
工作站	FE80::A00:20FF:FE01:C782	08:00:20:01:C7:82
PC	FE80::A07:1FF:FE33:D692	08:07:01:33:D6:92
Mac	FE80::A00:FF07:FE04:0388	08:00:07:04:03:88
小型机	FE80::A00:FF5A:FE00:B2C4	08:00:5A:00:B2:C4



对于同一链路或者网络内的节点之间的通信，包括邻接点发现机制，节点一般使用链路本地地址

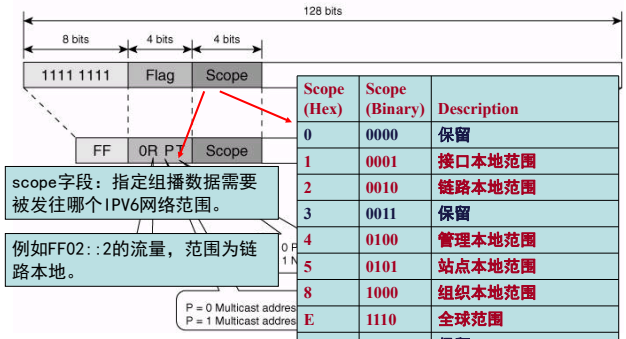
IPv6组播地址

- 组播地址标识的是相同或不同主机上的零到多个接口，去往某个组播地址的数据包，被发送到该地址标识的所有接口
- 格式（P84）



IPv6组播地址

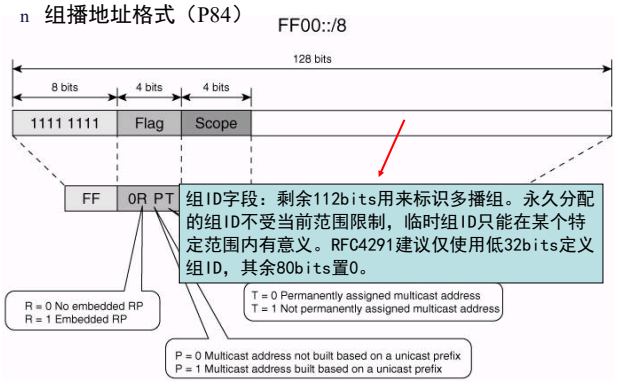
n 组播地址格式（P84） FF00::/8



Scope (Hex)	Scope (Binary)	Description
0	0000	保留
1	0001	接口本地范围
2	0010	链路本地范围
3	0011	保留
4	0100	管理本地范围
5	0101	站点本地范围
8	1000	组织本地范围
E	1110	全球范围
F	1111	保留

IPv6组播地址

n 组播地址格式（P84） FF00::/8



IPv6组播地址

- 已定义的常用的组播地址（P84）
  - 标识接口本地和链路本地范围内所有节点：
    - FF01::1(接口本地范围所有结点的组播地址）
    - FF02::1(链路本地范围所有结点的组播地址)
  - 标识本地接口、链路本地和站点本地范围内的所有路由:
    - FF01::2(接口本地范围所有路由器的组播地址)
    - FF02::2(链路本地范围所有路由器的组播地址)
    - FF05::2(站点本地范围所有路由器的组播地址)
- IPV6组播地址FF02:1替代了IPV4网络广播地址、子网广播地址、有限广播地址（255.255.255.255）。
- 了解最新的永久分配的IPV6组播地址：
  http://www.iana.org/assignments/ipv6-multicast-address

一种特殊的IPv6组播地址

- 请求节点组播地址（Solicited-node address）（P84）
  - 为了得知目的主机的链路层地址，IPV6协议采用邻接点请求/公告消息来共同完成链路层地址解析工作。
  - 为了不影响本地链路上所有节点，IPV6不能使用本地链路范围内所有节点的组播地址，而是使用请求节点组播地址。（IPV4采用ARP协议在链路层进行广播）
  - 每个节点都在自己的请求节点组播地址上监听来自本地链路其他节点的MAC地址解析请求（邻接点请求消息），并应答一个单播的邻接点公告消息告知自己的链路层地址。

一种特殊的IPv6组播地址

- 请求节点组播地址（Solicited-node address）（P84）
  - 每个节点必须为分配给它的每个单播和任播地址加入一个组播地址，用于重复地址检测和地址解析
  - 生成格式：FF02:0:0:0:0:1:FFXX:XXXX (X为单播或者泛播地址的低24比特部分)
    例如: 主机IPV6单播地址为FE80::02AA:B3FF:FE28:9C5A
    →FF02::1:FF28:9C5A

如图 3-6 所示为单播 IPv6 地址到相应的请求节点组播地址之间的映射关系。

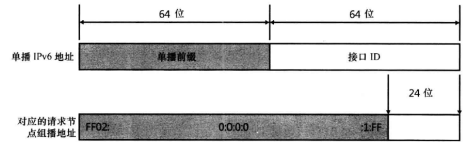
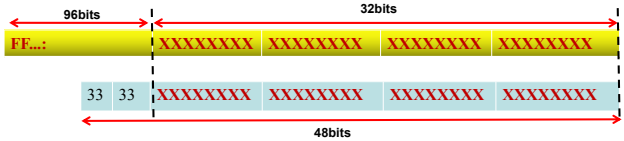


图 3-6 请求节点组播地址与单播地址的映射关系

IPv6组播MAC地址

- 映射组播IPV6地址到组播MAC地址（P85）
  - 在Ethernet网中发送IPV6组播数据包时，组播IPv6地址与组播MAC地址的映射关系如下所示：



  - 即：组播MAC地址的末32bits是由组播IPv6地址的末32bits直接映射得到
  - 例如 FF02::1:FF1A:22A1→33-33-FF-1A-22-A1

IPv6组播MAC地址

以太网的网络适配器维护着一张其感兴趣的目标 MAC 地址列表。若收到含有其感兴趣的目标 MAC 地址发来的以太网帧，网络适配器就会将其发送到上层进行进一步的处理。在默认情况下，这个表中包含了 MAC 层的广播地址（0xFF-FF-FF-FF-FF-FF）和分配给适配器的单播 MAC 地址。为了组播地址的高效性，表中可以加入或移除其他的组播目标地址。对于每一个主机所侦听的组播地址，在这台主机的感兴趣 MAC 地址列表中都有一个对应的条目。

例如，一个 MAC 地址为 00-AA-00-3F-2A-1C（链路本地地址为 FE80::2AA:FF:FE3F:2A1C）的 IPv6 主机可以将下列组播 MAC 地址添加到自己以太网适配器的感兴趣目标 MAC 地址列表中。

- 地址 33-33-00-00-00-01：该地址对应的是链路本地范围内所有节点的组播地址 FF02::1（完全展开后为 FF02:0000:0000:0000:0000:0000:0000:0001）。
- 地址 33-33-FF-3F-2A-1C：该地址对应的是请求节点地址 FF02::1:FF3F:2A1C。上文已提到过，请求节点地址为 FF02::1:FF00:0/104 的前缀和单播 IPv6 地址的末 24 位。

可以按照需要向表中添加主机侦听的额外的组播地址或将该地址从表中移除。

IPv6任播地址

- 目前IPv6关于任播没有明确定义，RFC 1546定义了任播的作用：“主机向一个任播地址（任意传送地址）发送分组，网络允许分组被路由到具有这个任播地址的所有节点中，距离最近的一个。
- “最近”的概念是由路由协议决定，它可以包括路由器跳数、服务器负载、到该服务器的往返时间（RTT，round－trip time）、链路的可用带宽和其它任何提供“最好”特征值（metric）的服务。
- 任播地址提供的服务：
  - 将一个任播地址分配给一组具有相同功能或内容的服务器集合，当客户需要服务的时候，可以访问个离客户“最近”的服务器，而无需为每个客户手工配置服务器列表。
  - 为网络中的一组能访问公共路由域的路由器分配一个任播地址。客户向该地址发送数据包时，会被依次转发给可用路由器。如RFC 3068中定义的6to4中继任播地址。移动IPv6也使用任播地址。

IPv6任播地址

- 任播地址类型
  - 子网-路由器任播地址（RFC 4291）
    - 格式：

n 比特	128-n 比特
子网前缀	0000000000000000000

    - 所有连接到某个子网的路由器接口，都有这个“子网-路由器任播地址”，用于与连接到特定子网的“最近”路由器进行通信，子网前缀标识了一条到达该子网的特定链路。

IPv6任播地址

- 任播地址类型
  - 保留的子网任播地址（RFC 2526）
    - 格式：对于需要64比特接口标识符（EUI-64格式）的任播地址

64比特	57比特	7比特
子网前缀	1111 1101 11.....1111	任播ID

    - 格式：对于其他类型的任播地址

64比特	121-n比特	7比特
子网前缀	1111 1111 11.....1111	任播ID

    - RFC2526中文版课后阅读：https://wenku.baidu.com/view/ed66780e52ea551810a6877d.html

特殊用途的IPv6地址

- 未指明地址：全0（::）
  - 在以下两种情况用于发送IPv6分组的网络节点的地址
    - 网络节点还没有配置地址
    - 网络接口配置的地址在本地链路上还不能确定是唯一的
- 回环地址（::1）
  - 指代网络节点本身

过渡地址

- 为了协助IPV4到IPV6的过渡，定义了如下地址：
  - IPV4-mapped IPV6 address:
    - 为IPV4主机映射到IPV6双栈网络时的临时IPV6地址
    - 可表示为：80个零+16个1+IPV4（32位）
    - IPV4 “192.31.20.46” ⟺ IPV6 “::FFFF:192.31.20.46”

本章内容

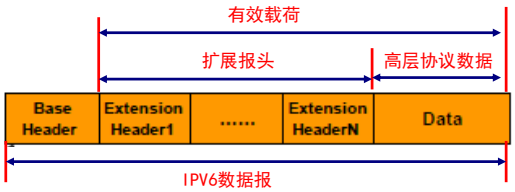
- 2.1 IPV4局限性与IPV6特点
- 2.2 IPV6地址表达与分类
- 2.3 IPV6数据报及报头
- 2.4 ICMPV6协议

本章内容

- 2.1 IPV4局限性与IPV6特点
- 2.2 IPV6地址表达与分类
- 2.3 IPV6数据报及报头
- 2.4 ICMPV6协议
- 2.5 IPv4向IPv6过渡

IPV6分组结构

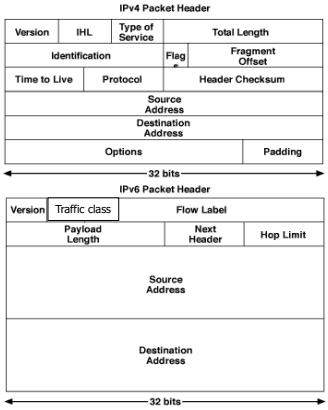
- IPV6分组的结构
  - IPV6分组是由一个40个字节IPV6基本报头、0个或多个不同长度的扩展报头、一个高层协议数据单元组成
  - IPV6分组的有效载荷包括扩展报头与高层协议数据



2.3.1 IPV6基本报头

- IPV6的基本报头与IPV4报头的比较：
  - IPV6: 6 个字段 + 2个地址
  - IPV4: 10个字段 + 2 个地址 + 选项
- IPV6删除：
  - 首部长度(Header length)
  - 服务类型(type of service)
  - 标识(identification)、标志(flags)、片偏移(fragment offset)
  - 首部校验和(Header Checksum)

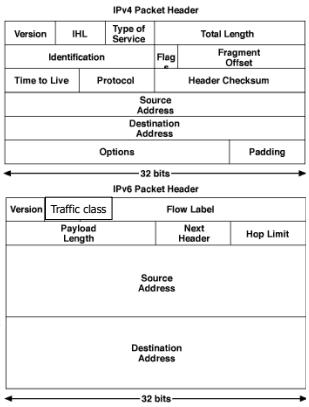
详见105-106



2.3.1 IPV6基本报头

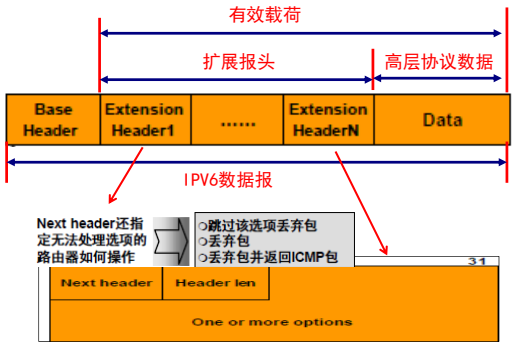
- IPV6增加：
  - 通信类型(Traffic class)
  - 流标记(Flow label)
- IPV6重命名：
  - 总长度(length) -> 有效载荷长度(Payload length)
  - 协议(Protocol) -> 下一个报头(Next header)
  - 生存时间(time to live) -> 跳数限制(Hop Limit)
  - 改善：用扩展报头取代了选项功能(Option mechanism)

详见105-106



2.3.2 IPV6扩展报头

- 每一个扩展报头都是由长度各不相同的若干字节组成，但必须是8字节的整数倍，格式如下所示。



IPV6报文实例

```
Internet Protocol Version 6, Src: fe80::3c7d:355f:e627:33c7 (fe80::3c7d:355f:e627:33c7), Dst: ff02::1:3 (ff02::1:3)
  0110 .... = Version: 6
    [0110 .... = This field makes the filter "ip.version == 6" possible: 6]
  .... 0000 0000 .... .... .... .... .... = Traffic class: 0x00000000
    .... 0000 00.. .... .... .... .... .... = Differentiated Services Field: Default (0x00000000)
    .... .... ..0. .... .... .... .... .... = ECN-Capable Transport (ECT): Not set
    .... .... ...0 .... .... .... .... .... = ECN-CE: Not set
  .... .... .... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
  Payload length: 32
  Next header: UDP (17)
  Hop limit: 1
  Source: fe80::3c7d:355f:e627:33c7 (fe80::3c7d:355f:e627:33c7)
  Destination: ff02::1:3 (ff02::1:3)
  [Source GeoIP: Unknown]
  [Destination GeoIP: Unknown]
User Datagram Protocol, Src Port: 59155 (59155), Dst Port: 5355 (5355)
  Source Port: 59155 (59155)
  Destination Port: 5355 (5355)
  Length: 32
  Checksum: 0xe1f0 [validation disabled]
    [Good Checksum: False]
    [Bad Checksum: False]
  [Stream index: 8]
Link-local Multicast Name Resolution (query)
```

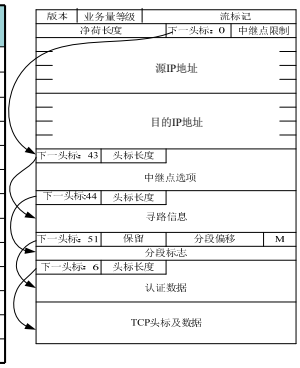

IPV6主要的几种扩展报头

- IPv6扩展报头实现了一些IP层的可选功能，不被中间路由器解析，一般只会被目的路由器解析，主要的扩展报头及推荐排列顺序为：
  - Hop-by-Hop Options header逐跳选项报头
    - 唯一一个链路上所有节点都要处理的扩展报头，必须排在第一位
  - Destination Options header目的选项报头
    - 最多出现两次，一次在路由报头前，一次在上层协议数据报文前，如果没有路由报头，只能出现一次
  - Routing header路由选项报头
  - Fragment header分片选项报头
  - Authentication header认证选项报头
  - Encapsulating Security Payload header封装安全有效载荷报头

IPV6扩展报头实例

- 由IPV6扩展报头的next head字段组成的指针链

Next header	含义	顺序
41	IPV6基本报头	1
0	逐跳选项报头（HOPOPT）	2
60	目的选项报头	3，8
43	路由选项报头	4
44	分片选项报头	5
51	认证选项报头（AH）	6
50	封装化安全载荷（ESP）	7
135	移动（MIPV6）	9
59	该报头是最后一个报头	最后
58	ICMPv6	最后
17	UDP	最后
6	TCP	最后
——	各种其他高层协议	最后



- 获得“Next header”字段意义的最新列表地址是：http://www.iana.org/assignments/protocol-numbers

逐跳选项扩展报头

- 作用：为发送到目的主机途中的每一跳路由器指定该数据包的转发参数
  - 头部扩展长度字段的值是整个逐跳选项报头中8字节块的块数（第一个8字节块不计），最小值是0

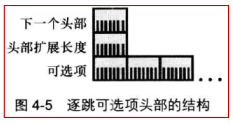


图 4-5 逐跳可选项头部的结构

  - 如果字节块数不足8字节的整数倍，需要在可选项字段中填充0
  - 因此逐跳可选扩展报头的总字节数 =(头部扩展长度字段值+1)*8
  - 可选项字段是一些字段的集合，这些字段既可用于描述数据包的某种特性，也可用于填充。结构如图4-6所示
    - 可选项类型字段
    - 可选项长度
    - 可选项数据

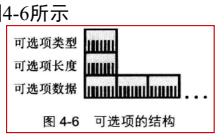


图 4-6 可选项的结构

逐跳选项扩展报头

- 可选项类型字段既要标识可选项，又要指定节点对它的处理方法，下表1列出了逐跳可选项和目的可选项报头的不同选项类型

可选项类型	选项/用途	起始位置要求
0	Pad1可选项 / 逐跳和目的选项报头	无
1	PadN可选项 / 逐跳和目的选项头报头	无
194(0xC2)	超大有效负荷可选项 / 逐跳选项报头	4n+2
5	路由器警告可选项 /逐跳选项报头	2n+0
201(0XC9)	本地地址可选项 / 目的选项报头	8n+6

相对逐跳选项报头或目的选项报头的头部的起始位置

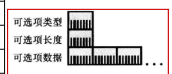


图 4-6 可选项的结构

- 表2 列出了节点未识别出可选项类型时采取的动作（由可选项类型字段头2位值决定）

值(二进制)	节点采取的动作
00	跳过此可选项
01	自行丢弃该数据包
10	丢弃该数据包，若IPV6头部中的对象地址字段是单播或者组播地址，则要向发送方发送ICMPV6参数问题（ICMP Parameter Problem）消息
11	丢弃该数据包，若IPV6头部中的对象地址字段不是组播地址，则要向发送方发送ICMPV6参数问题（ICMP Parameter Problem）消息

逐跳选项扩展报头——Pad1、PadN可选项

- Pad1可选项用于插入单个填充字节，没有可选项长度字段；PadN可选项用于插入N个填充字节，可选项长度字段值=N-2。
- 是为了满足整个逐跳选项报头为8字节块整数倍，以及其他可选项对起始位置的要求。

可选项类型	可选项长度	可选项数据	起始位置要求
0	无	无	无
1	设为填充字节数-2	无	无

图 4-7 Pad1 可选项的结构

- 如果节点无法识别这两个可选项，会跳过或将其丢弃。

值(二进制)	节点采取的动作
00	跳过此可选项
01	自行丢弃该数据包
10	丢弃该数据包，若IPV6头部中的对象地址字段是单播或者组播地址，则要向发送方发送ICMPV6参数问题（ICMP Parameter Problem）消息
11	丢弃该数据包，若IPV6头部中的对象地址字段不是组播地址，则要向发送方发送ICMPV6参数问题（ICMP Parameter Problem）消息

逐跳选项扩展报头——超大载荷可选项

- 超大载荷可选项定义于RFC 2765，可以表示最大为2^{32}-1字节的有效载荷。一般带着超过65535字节有效载荷的IPV6数据包就需要使用这个可选项。

可选项类型	可选项长度	超大载荷长度(字节)	起始位置要求
194(0xC2)	4	4294967295	4n+2

图 4-9 超大负载可选项的结构

- 如果节点无法识别这个可选项，会将其丢弃。

值(二进制)	节点采取的动作
00	跳过此可选项
01	自行丢弃该数据包
10	丢弃该数据包，若IPV6头部中的对象地址字段是单播或者组播地址，则要向发送方发送ICMPV6参数问题（ICMP Parameter Problem）消息
11	丢弃该数据包，若IPV6头部中的对象地址字段不是组播地址，则要向发送方发送ICMPV6参数问题（ICMP Parameter Problem）消息

逐跳选项扩展报头——路由器警告可选项

- 路由器警告可选项定义在RFC211，告知路由器这个数据包中的内容需要进行额外处理，通常用于组播侦听发现MLD和资源预留协议RSVP。

可选项类型	可选项长度	路由器警告值	起始位置要求
5	2	0	2n+0

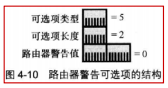


图 4-10 路由器警告可选项的结构

- 如果节点无法识别这个可选项，会将其丢弃。

值(二进制)	节点采取的动作
00	跳过此可选项
01	自行丢弃该数据包
10	丢弃该数据包，若IPV6头部中的对象地址字段是单播或者组播地址，则要向发送方发送ICMPV6参数问题（ICMP Parameter Problem）消息
11	丢弃该数据包，若IPV6头部中的对象地址字段不是组播地址，则要向发送方发送ICMPV6参数问题（ICMP Parameter Problem）消息

逐跳选项扩展报头——实例

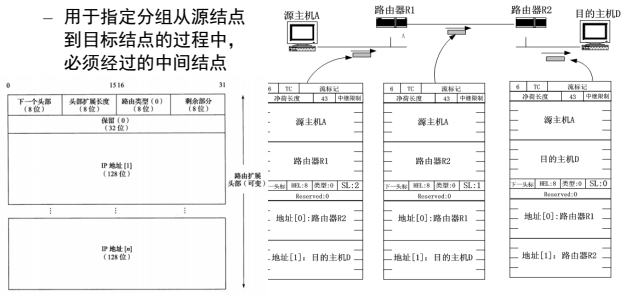
下面是 Network Monitor 3.4 显示出来的逐跳可选项头部。

```
  Frame:
+ Ethernet: Etype = IPv6
- Ipv6: Next Protocol = ICMPv6, Payload Length = 32
  + Versions: IPv6, Internet Protocol, DSCP 0
    PayloadLength: 32 (0x20)
    NextProtocol: HOPOPT, IPv6 Hop-by-Hop Option, 0(0)
    HopLimit: 1 (0x1)
    SourceAddress: FE80:0:0:0:2B0:D0FF:FEE9:4143
    DestinationAddress: FF02:0:0:0:0:0:1:FFE9:4143
  - HopbyHopHeader:
    NextHeader: ICMPv6
    ExtHdrLen: 0(8 bytes)
  - OptionRouterAlert:
   - OptionType: Router Alert
     Action: (00......) Skip over this option
     C:      (..0.....) Option Data does not change en-route
     OptionType: (...00101) Router Alert
    OptDataLen: 2 bytes
    Value: Datagram contains a Multicast Listener Discovery message, 0 (0x0)
  - OptionPadN:
   - OptionType: PadN
     Action: (00......) Skip over this option
     C:      (..0.....) Option Data does not change en-route
     OptionType: (...00001) PadN
    OptDataLen: 0 bytes
    OptionData: 0 bytes
+ Icmpv6: Multicast Listener Report
```

该实例中逐跳选项报头=1字节下一个头部字段+1字节的头部扩展长度字段+4字节路由警告可选字段，为了保证是8字节整数倍，再加上2字节的PadN字段填充

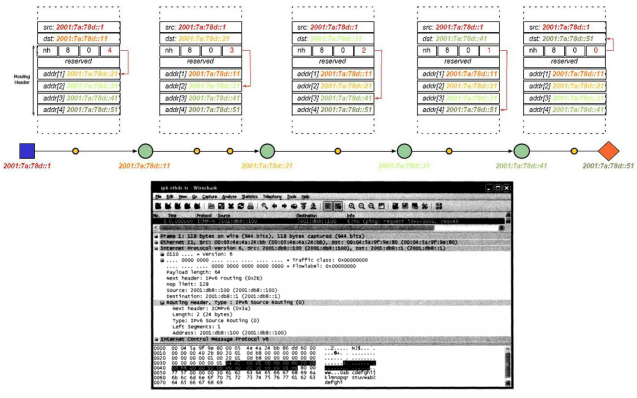
路由扩展报头

- 路由扩展报头
  - 用于指定分组从源结点到目标结点的过程中，必须经过的中间结点



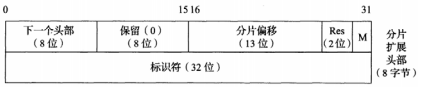
RH0由于允许在路由头部的多个位置指定相同地址。这可能导致流量在一条特定路径上的两台或多台路由器或主机之间重复转发。大量的流量负载可能在网络沿着特定路径创建，与相同路径上的其他流量竞争带宽而造成干扰。因此，RH0目前已被废弃，IPv6唯一支持的路由头部是RH2。RH2与RH0区别在于它只允许指定不同地址，而且在路由类型字段中定义为2。

路由扩展报头



分片扩展报头

- 分片扩展报头格式
  - 用于IPv6源节点向目的地发送一个大于路径MTU的数据报。仅数据报的发送者可以执行分片操作。1280字节是整个网络中针对IPv6定义的链路层最小MTU。



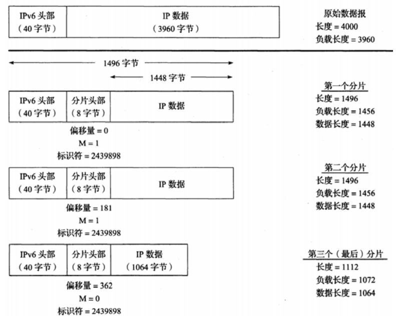
  - 保留字段和Res字段都为0，被接收方所忽略。
  - 分片偏移字段：有效载荷在原始数据报中以8字节为单位的偏移量。
  - M字段设置为1，表示在数据报中包含更多分片。否则表示该分片是原始数据报的最后一个分片。

分片扩展报头

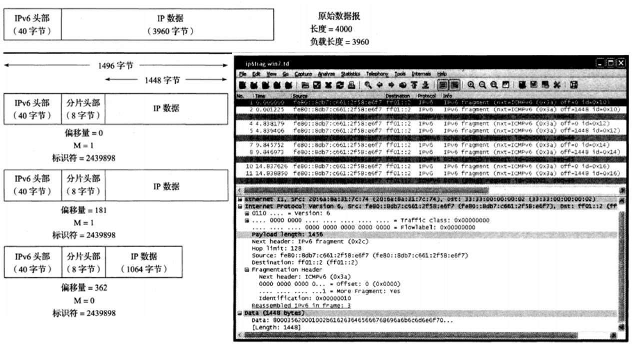
- 分片扩展报头格式
  - 在分片过程中，输入的数据报称为"原始数据报"，由两部分组成："不可分片部分"和"可分片部分"。
  - 不可分片部分包括：
    - IPv6固定报头
    - 任何到达目的地之前需要由中间节点处理的扩展报头(包括路由扩展报头及其之前的所有扩展报头)
    - 分片报头。
  - 可分片部分包括：
    - 数据报的其余部分(即目的选项扩展报头、AH报头、ESP报头、上层协议报头和有效载荷数据)。

分片扩展报头——实例

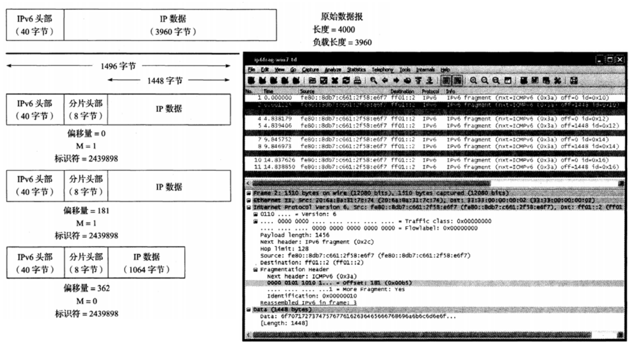
- 分片扩展报实例
  - 一个3960字节的有效载荷被分片，分片没有超过1500字节(以太网MTU)，分片数据部分必须为8字节的倍数。



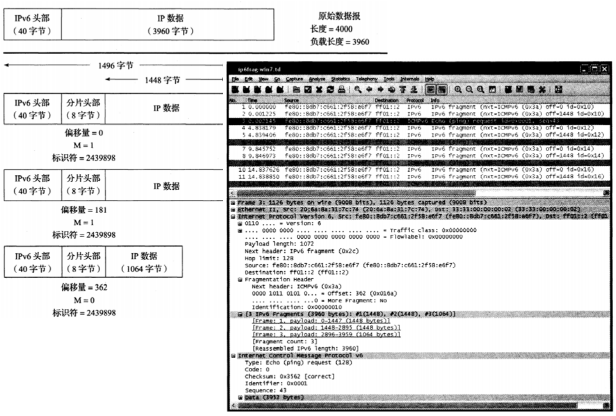
分片扩展报头——实例



分片扩展报头——实例



分片扩展报头——实例



分片扩展报头实例

- 分片报头实例

```
No.  Time        Source                   Destination               Protocol  Length  Info
  1 0.000000    fe80::20e:c6ff:fed6:5f89  fe80::ad67:ba9c:7082:d6c3  IPv6      1510 IPv6 fragment (off=0 m
  2 0.000358    fe80::20e:c6ff:fed6:5f89  fe80::ad67:ba9c:7082:d6c3  UDP        670 48815 → 3879 Len=2048

▷ Frame 2: 670 bytes on wire (5360 bits), 670 bytes captured (5360 bits)
▷ Ethernet II, Src: AsixElec_d6:5f:89 (00:0e:c6:d6:5f:89), Dst: HewlettP_53:d5:39 (f0:92:1c:53:d5:39)
◢ Internet Protocol Version 6, Src: fe80::20e:c6ff:fed6:5f89, Dst: fe80::ad67:ba9c:7082:d6c3
    0110 .... = Version: 6
  ▷ .... 0000 0000 .... .... .... .... .... = Traffic class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... .... .... 0000 0000 0000 0000 0000 = Flow label: 0x00000
    Payload length: 616
    Next header: Fragment Header for IPv6 (44)
    Hop limit: 64
    Source: fe80::20e:c6ff:fed6:5f89
    [Source SA MAC: AsixElec_d6:5f:89 (00:0e:c6:d6:5f:89)]
    Destination: fe80::ad67:ba9c:7082:d6c3
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
  ◢ Fragment Header for IPv6
      Next header: UDP (17)
      Reserved octet: 0x00
      0000 0101 1010 1... = Offset: 181 (1448 bytes)
      .... .... .... .00. = Reserved bits: 0
      .... .... .... ...0 = More Fragments: No
      Identification: 0x00000002
  ▷ [2 IPv6 Fragments (2056 bytes): #1(1448), #2(608)]
▷ User Datagram Protocol, Src Port: 48815, Dst Port: 3879
▷ Data (2048 bytes)
```

转发IPV6数据包的简化流程

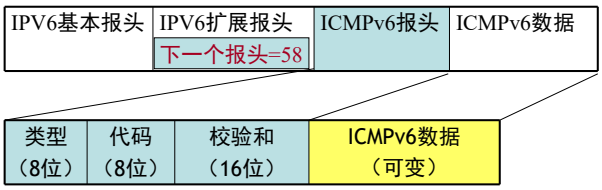
- 检验版本字段，确认分组按照IPV6协议要求封装
- 跳数限制字段(Hop Limit)的值减1
  - 如果新的Hop Limit的值=0，发送“超时-超过生存时间”ICMPv6报文给源结点，并丢弃该分组
- 检查下一个报头字段(Next header)的值
  - 如果值为0，处理逐跳选项报文
- 通过目的IP地址和本地路由表进行路由选择
  - 如果没找到合适路由，发送“目标不可达-没有到达目的路由”ICMPv6报文给源结点，并丢弃该分组
- 处理有效载荷长度字段(Payload length)的值
  - 如果转发接口的链路MTU<Payload length+40字节，则发送“数据包过大”ICMPv6报文给源结点，并丢弃该分组
- 根据路由选择结果选择合适的接口转发数据包

本章内容

- 2.1 IPV4局限性与IPV6特点
- 2.2 IPV6地址表达与分类
- 2.3 IPV6数据报及报头
- 2.4 ICMPV6协议
- 2.5 IPv4向IPv6过渡

2.4 ICMPv6协议

- ICMPv6报文与IPv6报文的关系：



类型：ICMPV6的报文类型

代码：从属于类型字段，可以在基本类型中再分出新的子类。

校验和：计算对象是ICMPV6类型字段+IPV6的伪报头，IPV6伪报头包括源地址字段、目的地址字段、ICMPV6数据包长度字段、下一个头部字段（即58）。

2.4 ICMPv6协议

- ICMPv6主要功能：进行错误报告和网络诊断等
- 与ICMPv4的不同之处：
  - 删除了一些不再使用的过时报文类型，定义了其他新的功能与报文
  - 合并了ICMP、IGMP与ARP等多个协议的功能。
- ICMPv6的控制信息类型主要划分为两种：
  - 错误类消息（0~127）
    - 用于报告IPV6分组在传输过程中出现的差错。
    - 常用类型：目的不可达、分组过大、超时与参数问题。
  - 信息类消息（128~255）
    - 用于提供网络诊断功能与附加的主机功能。
    - 常用类型：诊断报文、多播组管理、邻接点发现。

ICMPV6部分消息类型

类　型	正式名称	参　考	描　述
1 (+)	目的不可达	[RFC4443]	不可达的主机、端口、协议
2	数据包太大（PTB）	[RFC4443]	需要分片
3 (+)	超时	[RFC4443]	跳数用尽或者重组超时
4	参数问题	[RFC4443]	畸形数据包或者头部
100,101	为私人实验保留	[RFC4443]	为实验保留
127	为 ICMPv6 差错报文扩充保留	[RFC4443]	为更多的差错报文保留
128	回显请求	[RFC4443]	ping 请求，可能包含数据
129	回显应答	[RFC4443]	ping 应答，返回数据
130	组播侦听查询	[RFC2710]	查询组播订阅者（v1）
131	组播侦听报告	[RFC2710]	组播订阅者报告（v1）
132	组播侦听完成	[RFC2710]	组播取消订阅报文（v1）
133	路由器请求（RS）	[RFC4861]	IPv6 RS 和移动 IPv6 选项
134	路由器通告（RA）	[RFC4861]	IPv6 RA 和移动 IPv6 选项
135	邻居请求（NS）	[RFC4861]	IPv6 邻居发现（请求）
136	邻居通告（NA）	[RFC4861]	IPv6 邻居
137	重定向报文	[RFC4861]	使用另一
141	反向邻居发现请求报文	[RFC3122]	反向邻居 的 IPv6 地址

类　型	正式名称	参　考	描　述
142	反向邻居发现通告报文	[RFC3122]	反向邻居发现应答：报告给定的链路层地址的 IPv6 地址
143	组播侦听报告版本 2	[RFC3810]	组播侦听报告（v2）
144	本地代理地址发现请求报文	[RFC6275]	请求移动 IPv6 HA 地址，由移动节点发送
145	本地代理地址发现应答报文	[RFC6275]	包含 MIPv6 HA 地址，在本地网络中由合格的 HA 发送
146	移动前缀请求	[RFC6275]	当离开时请求本地前缀
147	移动前缀通告	[RFC6275]	提供从 HA 到移动节点的前缀
148	证书路径请求报文	[RFC3971]	一条证书路径的保护邻居发现（SEND）请求
149	证书路径通告报文	[RFC3971]	响应一个证书路径请求的 SEND
151	组播路由器通告	[RFC4286]	提供组播路由器的地址
152	组播路由器请求	[RFC4286]	请求组播路由器的地址
153	组播路由器终止	[RFC4286]	组播路由器使用结束
154	FMIPv6 报文	[RFC5568]	MIPv6 快速切换报文
200,201	为私人实验保留	[RFC4443]	为实验保留
255	为 ICMPv6 信息类报文扩充保留	[RFC4443]	为更多的信息类报文保留

2.4 ICMPv6协议

- **ICMPv6协议支持了下列技术的实现：**
  - **邻接点发现**
    - **取代了IPV4的ARP、路由器发现、重定向等**
  - **组播侦听发现**
  - **安全邻接点发现**

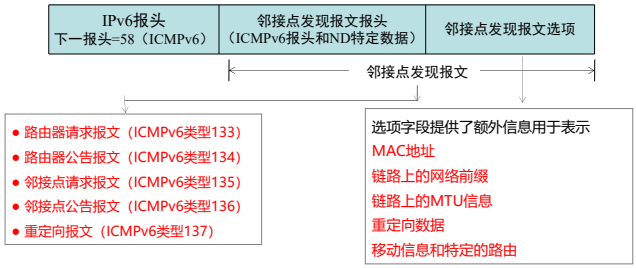
2.4.1 邻接点发现(ND)协议概述

- 邻接点发现协议(ND)用于确定邻接点之间的关系，它取代了IPv4的地址解析协议（ARP）、以及ICMPv4的路由器发现和重定向报文，还提供了额外的功能。
- IPv6的邻接点发现包括以下机制（P137-138）：
  - 路由器发现 ● 前缀发现 ● 参数发现 ● 地址自动配置 ● 地址解析
  - 次跳选择 ● 邻接点不可达检测 ● 重复地址检测 ● 重定向功能
- 不同主体使用ND的不同操作

节点使用ND	主机使用ND	路由器使用ND
解析某个IPv6数据包发往的邻接点的链路层地址	发现邻接点路由器	通告自己的存在、主机配置参数、路由以及链路上的前缀
确定邻接点的链路层地址发生改变的时间	自动配置地址、地址前缀、路由以及其他配置参数	提醒主机用于向特定目标转发数据报的更好次跳地址
确定邻接点是否可达		

2.4.1 邻接点发现协议概述

- 邻接点发现使用了5种ICMPv6报文。由报头（包含ICMPv6报头和ND报文特定数据）和零或多个选项组成。



2.4.1 邻接点发现协议概述

- 邻接点发现机制与上述五种ICMPV6报文的关系

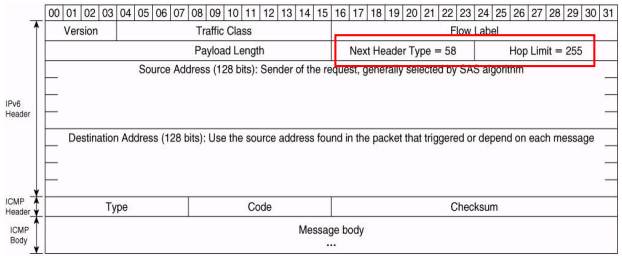
	类型133 路由器请求	类型134 路由器公告	类型135 邻接点请求	类型136 邻接点公告	类型137 重定向
地址解析			√	√	
重复地址检测			√	√	
邻接点不可达检测			√	√	
无状态地址自动配置		√	√	√	
路由器发现	√	√			
重定向					√

2.4.2 邻接点发现报文

- 下面先学习这五种ICMPV6报文的格式：
  - 路由器请求报文（类型133）
  - 路由器公告报文（类型134）
  - 邻接点请求报文（类型135）
  - 邻接点公告报文（类型136）
  - 重定向报文（类型137）

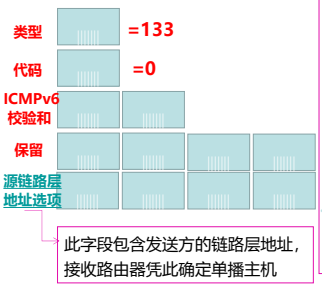
2.4.1 邻接点发现协议概述

- 注意：跳数限制字段被设置为255，以防止非本地链路的发送者假冒本地节点，发起ICMPV6网络攻击。



路由器请求（RS)报文

- 功能：用于发现链路上的IPv6路由器。IPV6主机主动发送一个多播的路由器请求报文以促使IPv6路由器立刻响应路由器公告（RA）报文。



1、例如对于以太网，路由器请求报文的以太网数据帧首部可如下设置：
源地址：发送方的MAC地址
对象地址：33-33-00-00-00-02
2、路由器请求报文的IPv6基本报头可如下设置：
源地址：或者是分配好的链路本地地址或者是未指定地址（::）
对象地址：链路本地范围的所有路由组播地址（FF02::2）
3、将跳限制设置为255

源和目标的链路层地址选项

- 源链路层地址选项表示发送方的链路层地址。邻接点请求、路由器请求和路由器公告报文中都有该选项。当报文的源地址是未指定地址（::）时，则不包含该选项。
- 目标链路层地址选项表示IPv6包应发送到的邻接点的链路层地址。邻接点公告和重定向报文中包含该选项。

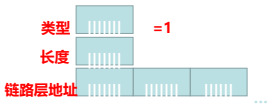


图1 源链路层地址选项

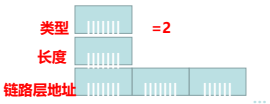


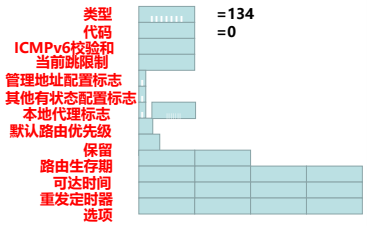
图2 目标链路层地址选项

路由器公告(RA)报文

- IPv6路由器：主动的“伪周期性“的发送路由器公告报文；或者在收到路由器请求报文后，应答以路由器公告报文；
  - 伪周期是指两次未经请求而主动发送路由器公告报文的时间间隔随机，以避免链路上多个路由器进行通告时同步。
- 路由器公告报文中包含的信息可供主机决定以下内容：链路前缀、链路MTU、特定路由、是否使用地址自动配置以及通过地址自动配置创建的地址的持续时间的有效性和优先性。

路由器公告（RA)报文

- 路由器公告报文中的格式如下



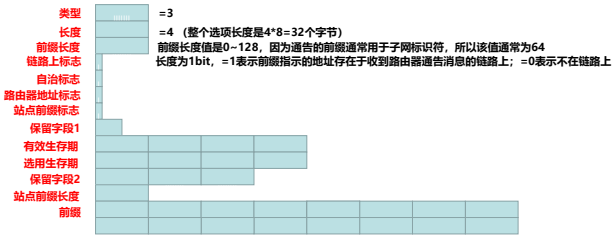
1、例如对于以太网，路由器公告报文的数据帧首部可如下设置：
源地址：发送方的MAC地址
对象地址：33-33-00-00-00-01
2、在路由器公告报文的IPv6基本报头中可如下设置：
源地址：发送接口的链路本地IPv6地址
对象地址：链路本地范围的所有节点的组播地址（FF02::1）或者发送路由器请求报文的主机的单播地址
3、跳限制设为255

路由器公告报文各字段解释

● 当前跳限制- 表示包的IPv6报头中跳限制字段的默认值，这些包由收到路由器公告信息的主机发送。
● 管理地址配置标志- 值为1时表示收到路由器公告报文的主机必须使用类似DHCPv6的地址配置协议。获取除使用无状态地址配置得到的地址之外的地址。字段长度为1位。
● 其他有状态配置标志- 值为1时表示收到路由器公告报文的主机必须使用地址配置协议（如DHCPv6），获取非地址配置的信息。字段长度为1位。
● 本地代理标志- 该标志是RFC3775为移动IPv6定义的。
● 默认路由器优先级- 如果多个路由器公告他们自己为默认路由器，则可以配置这些路由器，是他们有不同的优先级。有效值为01(高)、00(中)和11(低)，10(保留未使用)，字段长度为2位。
● 路由器生存期- 表示路由器作为默认路由器的生存期（以秒计算），字段长16位。最长的路由器生存期是65535秒（约18.2小时）。值为0表示此路由器不能充当默认路由器。
● 可达时间- 表示某个节点在收到邻接点的可达性确认后认为该节点保持可达的时间。
● 重发定时器- 表示邻接点请求报文之间重传的时间，用于邻接点不可达性检测。
● 可选项-源链路层地址选项、MTU选项、前缀信息选项、公告间隔选项、本地代理信息选项、路由信息选项

前缀信息选项

- 前缀信息选项在路由器公告报文中发送，用于表示地址前缀和地址自动配置的信息。一个路由器公告报文可以有多个前缀信息选项，以表示多个地址前缀。下图是前缀信息选项的结构：

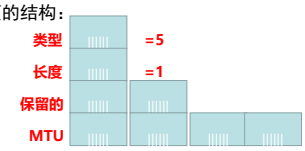


前缀信息选项各字段解释

● 前缀长度- 表示地址前缀中的前缀字段的先导位位数。8字节。可取0~128，为识别子网通常设为64。
● 链路上标志- 值为1时表示前缀所指示的地址存在于收到路由器公告报文的链路上，值为0表示不在
● 自治标志- 值为1时表示前缀用于创建一个自治(无状态)地址，值为0时表示前缀不作这个用途。
● 路由器标志- 该标志是RFC3775为移动IPv6定义的。
● 站点前缀标签- 值为1时表示由前缀字段定义的站点前缀和站点前缀长度字段用于更新站点前缀表。站点前缀表是由主机维护的，当全球地址匹配了站点前缀，就优先选用站点本地地址。
● 保留1、2- 保留1、2是为了将来使用所保留的字段，并且设置为0。
● 有效生存期- 表示地址保持有效的秒数，这个地址是基于包含的前缀并使用无状态地址配置。字段长度是32位。有效生存期也表示了所包含的前缀对于链路上确定过程的有效秒数。字段全1表示无限长。
● 选用生存期-表示地址保持选用状态的的秒数，这个地址基于包含的前缀并使用无状态地址配置。有效的无状态自动配置地址总是处于选用或弃用状态。选用生存期到期时地址从选用变为弃用。
● 站点前缀长度- 表示前缀字段中用于定义站点前缀的先导数位。只有当站点前缀标签为1时才有意义。
● 前缀- 表示了用无状态自动配置生成的IPv6地址的前缀。前缀长度字段和前缀字段的组合形成了唯一前缀，再加上接口标识就创建了IPv6地址。

MTU选项

- MTU选项是在路由器公告报文中发送的，用于表示链路的IPv6 MTU。当链路的IPv6 MTU未知或者由于转换的或混合介质桥接的配置而需要配置时，通常会使用该选项。MTU选项会覆盖接口硬件报告的IPv6 MTU。下图为MTU选项的结构：

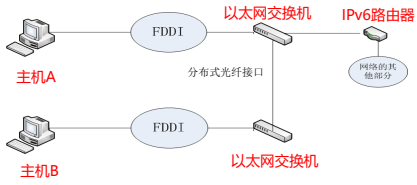


- MTU 该字段表示路由器向链路上所有主机在路由器公告报文中报告的IPv6 MTU。

→→ 在桥接或2层交换的环境中，同一个链路上可能存在不同的链路层技术，不同的技术会有不同的链路层MTU。该如何解决这个混合介质的问题呢？

MTU选项

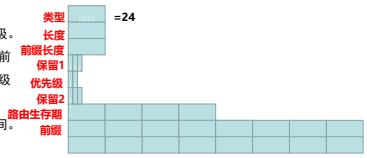
- 下图显示了转换配置，MTU选项在其中用于解决混合介质的问题。



主机A和B协商进行TCP连接，各自报告的TCP段的最大长度是4312（FDDI Ipv6的 MTU是4352，减去40字节的 IPv6报头）。但是，开始传输后，交换机会默默丢弃A、B之间传送的大于1500字节的数据包。有了MTU，子网IPV6路由器会向链路上的所有主机报告IPv6 MTU是1500。然后A和B调整MTU，传输的TCP不再被丢弃。

路由信息选项

路由信息选项在路由器公告报文中发送，用于表示接收主机添加到本地路由表的单个路由。下图显示了路由信息选项的结构。



●优先级 表示由公告路由发送时此路由的优先级。如果有多个路由器通过路由信息选项公告相同的前缀，则可以配置这些路由，让它们以不同的优先级公告路由。有效值为01(高)、00(中)和11(低)。

●路由生存期 表示前缀能够用于决定路由的时间。设置为0xFFFFFFFF时表示无限的路由生存期。

●前缀长度 表示对路由有用的前缀字段中的前导位位数，8位，有效值是0~128。

●长度 长度字段的值取决于路由的前缀长度和前缀字段的对应长度。如果前缀长度为是0（无前缀字段），则长度

字段的值为1；如果前缀长度>0且<65，则前缀字段的长度是64位，长度字段的值为2；如果前缀长度大于64，则前

缀字段的长度是128位，长度字段的值为3。

●前缀 前缀字段表示路由前缀。此字段的长度可以是0位、64位或者128位。

路由信息选项

路由信息可选项通常用于让主机在转发数据时能够做出更理想的转发决定。图 6-11 所示为一个可以利用路由信息可选项的简单网络配置的示例。

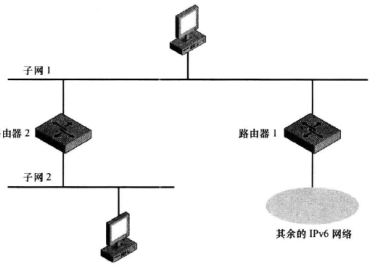


图 6-11 使用了路由信息可选项的配置示例

路由信息选项

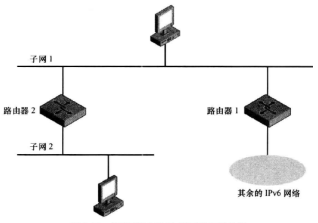


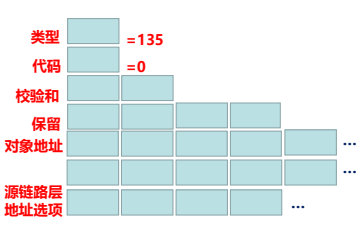
图 6-11 使用了路由信息可选项的配置示例

如果没有路由信息可选项，人们通常会通过配置，使这个网络中只有路由器 1 会将自己通告为子网 1 中的默认路由器。如果子网 1 的主机需要向子网 2 的主机发送流量，它就只能必须依靠路由器 1 发来的重定向消息，得知到达子网 2 主机的最佳下一跳地址应该是路由器 2。如需进一步了解相关内容，请参阅本章的“重定向功能”一节。

但是如果使用路由信息选项，就可以通过配置使路由器 2 通告子网 2 的前缀。根据从两个路由器收到的通告，子网 1 中的主机就可以自动地添加一条以路由器 1 为下一跳地址的默认路由，并为子网 2 前缀添加一条以路由器 2 为下一跳地址的精确路由。于是，子网 1 中的主机无需依靠路由器 1 的重定向，就可以到达子网 2 中的所有主机了。

邻接点请求(NS)报文

- 用于重复地址检测、邻接点可达性检测、地址解析、无状态地址自动配置。
- 下图为邻接点请求报文的结构：



● 对象地址- 表示进行地址检测、可达性检测和地址解析的目标节点的IPV6地址。

● 源链路层地址选项- 当该选项存在时，此字段包含发送方的链路层地址，接收路由器凭此确定单播主机

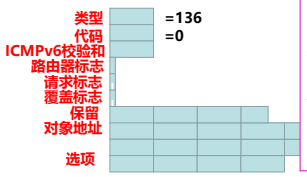
● 数据帧首部及IPV6 基本首部相应字段的内容，取决于邻接点请求报文的具体应用场景

邻接点公告(NA)报文

- 用于：或者对邻接点请求报文做出响应；或者周期发送以告知邻接点链路层地址或节点角色的变化。
- 报文包含的信息用于确定：邻接点公告报文的类型、发送方在网络中的角色以及发送方的链路层地址。

邻接点公告(NA)报文

- 邻接点公告报文格式如下：

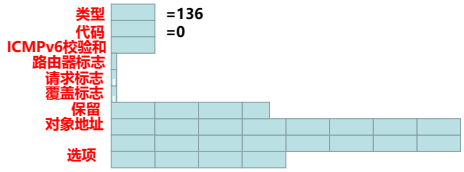


1、例如对于以太网，邻接点公告报文的数据帧首部可如下设置：
源地址：发送方的MAC地址
目的地址：对于非请求的邻接点公告，设为33-33-00-00-00-01；对于根据请求的邻接点公告，设为邻接点请求报文发送方的单播MAC地址

2、在邻接点公告报文的IPv6基本报头中可如下设置：
源地址：设置为发送方的IPV6单播地址；
目的地址：对于非请求的邻接点公告，设为链路本地范围的所有节点的组播IPV6地址（FF02::1）；对于根据请求的邻接点公告，设置为发送邻接点请求报文的主机的单播IPV6地址
3、将跳限制设为255

邻接点公告（NA)报文

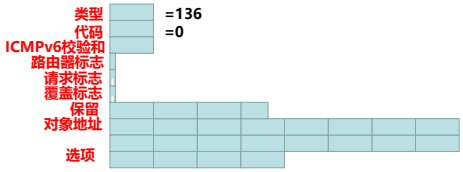
- 邻接点公告报文格式如下：



路由器标志- 表示该报文发送方的角色，若发送方是路由器，设置为1；否则为0。
请求标志- 值为1时表示邻接点公告报文是对邻接点请求报文的回应；值为0时表示是对组播邻接点公告和非请求单播邻接点公告的回应。
覆盖标志- 值为0时表示此报文包含的目标链路层地址选项中的链路层地址应该覆盖已存在的邻接点高速缓存条目内现存的链路层地址。

邻接点公告（NA)报文

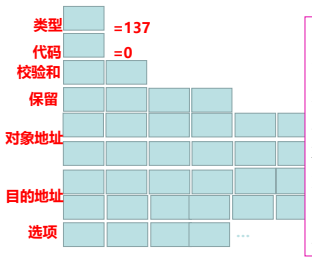
- 邻接点公告报文格式如下：



对象地址：表示要通告的地址。对于根据请求发送的邻接点公告，设置为相应的邻接点请求报文中的对象地址字段；对于非请求的邻接点公告，设置为其链路层地址或者角色已经变更的地址。
选项：如果存在目标链路层地址可选项，则会包含邻接点公告消息发送方的链路层地址

重定向报文

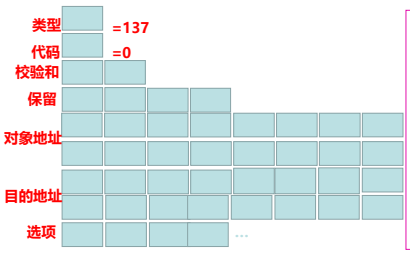
- 重定向报文由IPv6路由器发送，用于把到达指定目标的更佳首跳地址，单播告知始发主机。下图为重定向报文的结构：



1、例如对于以太网，重定向报文的数据帧首部可如下设置：
源地址：发送方的MAC地址
对象地址：始发主机的单播MAC地址
2、IPv6基本报头中可如下设置：
源地址：发送方的链路本地IPv6地址
目的地址：始发主机单播IPV6地址
3、将跳限制设为255

重定向报文

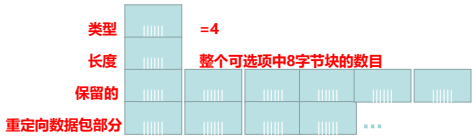
- 重定向报文由IPv6路由器发送，用于把到达指定目标的更佳首跳地址，单播告知始发主机。下图为重定向报文的结构：



对象地址- 表示指向目的地址字段的数据包的更佳的次跳地址。
目的地址- 包含引发路由器发送重定向报文的数据包的目的地址。
选项-包括目标链路层地址选项和重定向报头选项

重定向报头选项

- 重定向报头是在重定向报文中发送的，它用于表示造成路由器发送重定向报文的IPv6数据包。根据最初发送的IPv6数据包的长度，可以包括全部或部分重定向IPv6数据包。下图为重定向报头选项的结构：



保留 保留的字段是为将来使用所保留的48位字段，并设置为0
重定向数据包部分 初始的数据包（发送重定向数据包的原因）的先导部分，因此整个报文长度不会超过1280字节。

邻接点发现报文和选项小结

ND报文	可能包含的ND选项
路由器请求	源链路层地址选项：用于把单播路由器公告所响应的主机的链路层地址告知路由器
路由器公告	源链路层地址选项：用于把路由器的链路层地址告知接收主机
	前缀信息选项：用于把链路上前缀以及是否自动配置无状态地址告知接收主机
	MTU选项：用于把链路上的IPv6 MTU告知接收主机
	公告间隔选项：用于把路由器发送非请求多播路由器公告的频率告知接收主机
	本地代理信息选项：用于公告本地代理的优先级和生存期
	路由信息选项：用于告知特定路线上的接收主机添加本地路由表
邻接点请求	源链路层地址选项：用于把发送方的链路层地址告知接收节点
邻接点公告	目的链路层地址选项：用于把对应目的地址字段的链路层地址告知接收节点
重定向	重定向报头选项：用于包括全部重定向包，或其中一部分
	目的链路层地址选项：用于把对应目的地址字段的链路层地址告知接收节点

2.4.3 概念主机的数据结构

- 为了方便邻接点之间的交互，RFC4861定义了下列主机数据结构概念，作为存储ND过程中的信息：
  - 邻接点高速缓存
  - 目标高速缓存
  - 前缀列表
  - 默认路由器列表

2.4.3 概念主机的数据结构

- 邻接点高速缓存存储以下内容：每个邻接点的链路上IP地址、它对应的链路层地址、邻接点可达性标识。邻接点高速缓存相当于IPv4中的ARP高速缓存。

```
C:\Users\liang>netsh interface ipv6 show neighbors

Internet 地址                                 物理地址           类型
--------------------------------------------  -----------------  ----------
ff02::1                                       33-33-00-00-00-01  永久
ff02::2                                       33-33-00-00-00-02  永久
ff02::c                                       33-33-00-00-00-0c  永久
ff02::16                                      33-33-00-00-00-16  永久
ff02::fb                                      33-33-00-00-00-fb  永久
ff02::1:2                                     33-33-00-01-00-02  永久
ff02::1:3                                     33-33-00-01-00-03  永久
ff02::1:ff06:cca0                             33-33-ff-06-cc-a0  永久
```


2.4.3 概念主机的数据结构

- 目标高速缓存存储最近有传输流发往的目标的次跳地址。每个条目都包含目标IP地址、先前解析的次跳IPv6地址、到目标的路径MTU。

```
C:\Users\liang>netsh interface ipv6 show destinationcache

接口 47: 以太网

PMTU 目标地址                                  下一个跃点地址
---- ----------------------------------------  ----------------------------------------
1300 2001:478:65::53                           2001:478:65::53
65535 fe80::d05b:ff2e:1f3e:25cc                 fe80::d05b:ff2e:1f3e:25cc
```


2.4.3 概念主机的数据结构

- 前缀列表包含链路前缀。前缀列表中的每个条目为直接可达（相邻）目标定义一个IP地址的范围。此列表根据特定前缀生成，这些前缀是由路由器使用路由器公告报文公告生成的。
- 默认路由器列表包含：发送了路由器公告报文的链路上路由器相应的IP地址以及可以成为默认路由器的链路上路由器相应的IP地址。
- windows主机没有采用前缀列表和默认路由器列表，只使用路由表

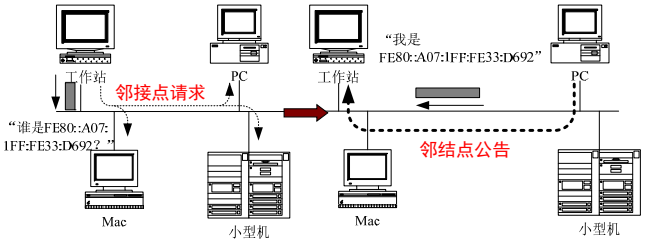
```
C:\Users\liang>netsh interface ipv6 show route

发布    类型      跃点数 前缀                    索引 网关/接口名称
------  --------  ------ ----------------------  ---  ------------------
否      手动         256 ::/0                     47  以太网
否      系统         256 ::1/128                   1  Loopback Pseudo-Interface 1
否      系统         256 2001:250:6803:109::/64   47  以太网
否      系统         256 2001:250:6803:109::387/128  47  以太网
否      系统         256 fe80::/64                47  以太网
否      系统         256 fe80::/64                 9  WLAN
否      系统         256 fe80::/64                11  本地连接* 1
否      系统         256 fe80::/64                 5  本地连接* 10
否      系统         256 fe80::444d:9085:c506:cca0/128  9  WLAN
否      系统         256 fe80::b4b9:2b50:176e:f1e7/128  5  本地连接* 10
否      系统         256 fe80::d05b:ff2e:1f3e:25cc/128  47  以太网
否      系统         256 fe80::f8e2:bea0:96bd:ad4/128  11  本地连接* 1
```

2.4.4 IPV6邻接点发现过程——地址解析

- IP地址到MAC地址映射（地址解析）
  - IPv4
    - 组播地址：直接映射
      - IP组播地址的低23位映射到MAC地址的低23位，前面加上01:00:5E | 01 00 5E | 0+IP组播地址低23位
    - 单播地址：地址解析协议ARP，链路层机制
  - IPv6
    - 组播地址：直接映射，IP组播地址的低32位映射到MAC地址的低32位，前面加上33 33 | 33 33 | IP组播地址低32位
    - 单播地址：邻接点发现机制，基于ICMPv6的地址解析，网络层

2.4.3 IPV6邻接点发现——地址解析

- 实例一：将IPv6地址解析成对应的MAC地址



主机	IP地址	以太网地址
工作站	FE80::A00:20FF:FE01:C782	08:00:20:01:C7:82
PC	FE80::A07:1FF:FE33:D692	02:07:01:33:D6:92
Mac	FE80::A00:07FF:FE04:0388	08:00:07:04:03:88
小型机	FE80::A00:5AFF:FE00:B2C4	08:00:5A:00:B2:C4

2.4.3 IPV6邻接点发现——地址解析

- IPV6 的地址解析过程是通过“邻接点请求”报文和“邻接点公告”报文的交互，来解析下一跳的链路层地址。
  - Step1：主机A希望得到主机B的MAC地址时，发出使用主机B的**被请求节点组播地址的**一个组播“邻接点请求”报文
  - Step2：当主机B收到“邻接点请求”报文后，就会根据请求报文中的源地址和链路层地址选项中的A主机的链路层地址，更新自己邻接点高速缓存。
  - Step3：主机B向A应答一个单播“邻接点公告”报文，报文中的“目的链路层地址选项”中填上自己的链路层地址。
  - Step4：主机A收到这个单播报文之后，创建一个关于主机B的地址映射表项，更新A的邻接点高速缓存。

被请求节点（Solicited-Node）组播地址

- IPv6中特有的组播地址
  - 用于重复地址检测
  - 地址解析等
- 被请求节点组播地址生成过程
  - 接口ID的后24位：XX:XXXX
  - 前缀FF02:0:0:0:0:1:FF
  - 最后组合成:FF02:0:0:0:0:1:FFXX:XXXX

邻接点请求消息(Neighbor Solicitation)

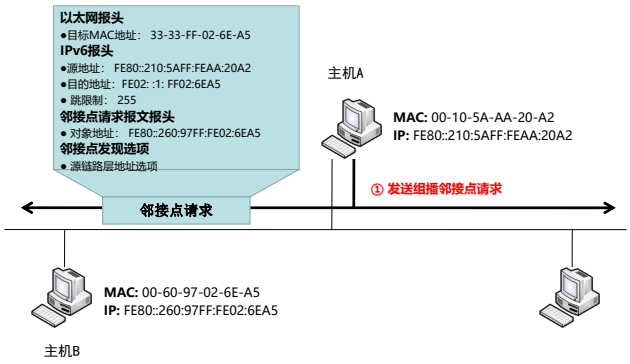
主机	IP地址	以太网地址
工作站	FE80::A00:20FF:FE01:C782	08:00:20:01:C7:82
PC	FE80::A07:1FF:FE33:D692	02:07:01:33:D6:92
Mac	FE80::A00:07FF:FE04:0388	08:00:07:04:03:88
小型机	FE80::A00:5AFF:FE00:B2C4	08:00:5A:00:B2:C4

邻接点公告消息(Neighbor Advertisement)

主机	IP地址	以太网地址
工作站	FE80::A00:20FF:FE01:C782	08:00:20:01:C7:82
PC	FE80::A07:1FF:FE33:D692	02:07:01:33:D6:92
Mac	FE80::A00:FF07:FE04:0388	08:00:07:04:03:88
小型机	FE80::A00:FF5A:FE00:B2C4	08:00:5A:00:B2:C4

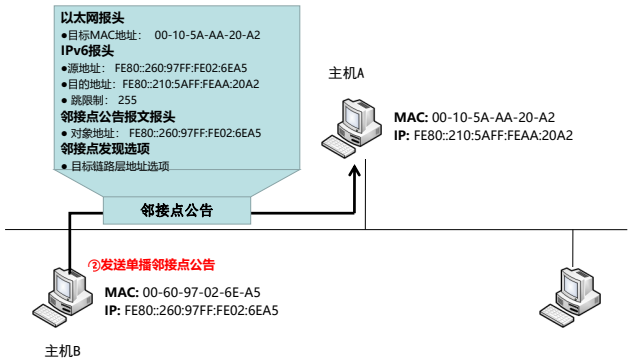
2.4.3 IPV6邻接点发现——地址解析

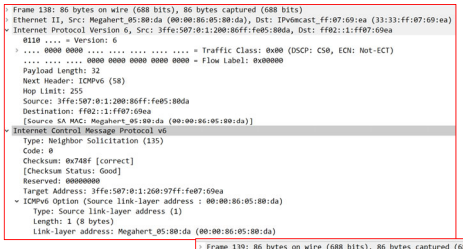
- 实例二：见教材P159



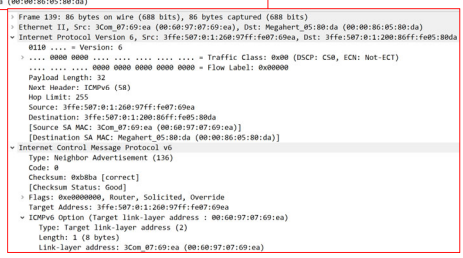
2.4.3 IPV6邻接点发现——地址解析

- 实例二：见教材P159

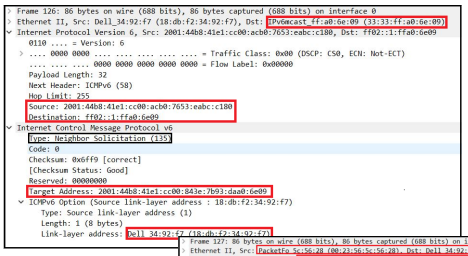




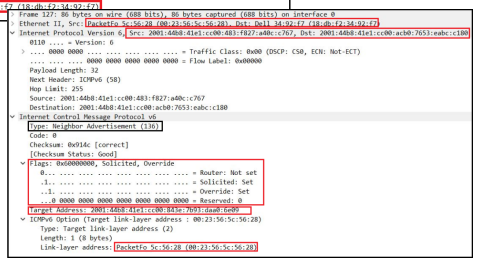
地址解析的报文实例



地址解析的报文实例



地址解析的报文实例



2.4.3 IPV6邻接点发现——重复地址检测

- IPV6使用“邻接点请求”报文和“邻接点公告”报文来检测主机的临时链路本地地址或临时全局地址，在本地链路上是否具有唯一性。
- 重复地址检测与地址解析的区别：
  - 源地址字段设置为：：
  - 邻接点公告报文的目的地址字段被设置为被请求节点组播地址
- 工作原理：
  - 主机发出组播的“邻接点请求”报文，查询自己的临时地址是否在本地链路具有唯一性。
  - 如果接收到响应该“邻接点请求”报文的“邻接点公告”报文，则表明已经有结点使用该临时地址，地址自动配置停止；否则表明临时地址是唯一的，可以使用。

请求报文和公告报文地址域的含义

- 邻接点请求报文地址字段含义：
  - IPV6基本报头的源地址（source address）:为未指定地址:: ；目的地址（destination address）:为对象地址的被请求节点IPV6组播地址（注：在发送邻接点请求报文前，结点的接口必须加入上述IPV6组播地址）
  - ICMPV6的对象地址（target address）：待检测唯一性的IPV6地址；
  - ICMPV6的源链路层地址选项(source link-level address)：发送该邻接点请求报文的主机的MAC地址。

被请求节点（Solicited-Node）组播地址

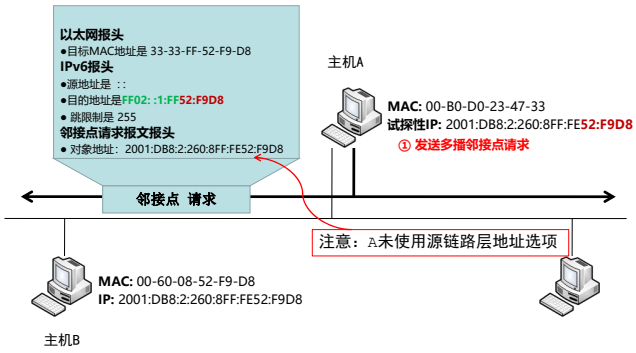
- IPv6中特有的组播地址
  - 用于重复地址检测
  - 获取本地链路上邻接点的链路层地址（地址解析）等
- 被请求节点(Solicited-Node)组播地址生成过程
  - 接口ID的后24位：XX:XXXX
  - 前缀FF02:0:0:0:0:1:FF
  - 最后组合成:FF02:0:0:0:0:1:FFXX:XXXX

请求报文和公告报文地址域的含义

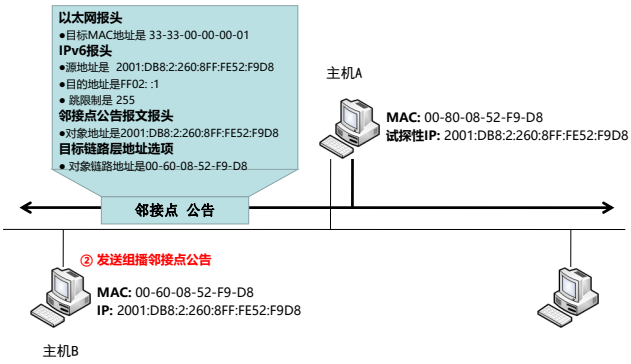
- 邻接点公告报文地址字段含义：：
  - IPV6基本报头的目的地址：链路本地范围所有结点多播地址FF02::1
    - 因为进行重复地址检测的发送方此时还不能使用被检测的IP地址，所以就不能接收单播的“邻接点公告”报文，所以只能是多播地址
  - ICMPV6的对象地址（target address)：
    - 对于主动发出的邻接点公告报文，表明发出报文的结点的链路层地址
    - 对于邻接点请求报文的响应，则是请求报文中的对象地址字段的值。
  - 对象链路层地址选项(Target link-level address)：发送该报文的主机的MAC地址。
  - 源链路层地址选项：无

2.4.3 IPV6邻接点发现——重复地址检测示例

重复地址检测实例见P165。



2.4.3 IPV6邻接点发现——重复地址检测示例



用于重复地址检测的邻接点请求报文

```
> Frame 5: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
> Ethernet II, Src: HsingTec_e3:e8:de (00:d0:09:e3:e8:de), Dst: IPv6mcast_ff:98:06:e1 (33:33:ff:98:06:e1)
v Internet Protocol Version 6, Src: ::, Dst: ff02::1:ff98:6e1
    0110 .... = Version: 6
  > .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... .... .... 0000 0000 0000 0000 0000 = Flow Label: 0x00000
    Payload Length: 24
    Next Header: ICMPv6 (58)
    Hop Limit: 255
    Source: ::
    Destination: ff02::1:ff98:6e1
v Internet Control Message Protocol v6
    Type: Neighbor Solicitation (135)
    Code: 0
    Checksum: 0x231f [correct]
    [Checksum Status: Good]
    Reserved: 00000000
    Target Address: 2001:6f8:102d:0:999:39d7:ce98:6e1
```

对重复地址的处理

- 主机收到一个邻接点请求报文，而此报文的对象地址也是该主机正在做DAD检测的地址。如果请求的源地址类型为IPV6_ADDR_ANY(全0地址::)，则主机从接口上删除这个地址，DAD检测失败；如果不是全0地址，主机不处理此请求

  说明有多台主机同时对同一IPv6地址开始DAD过程

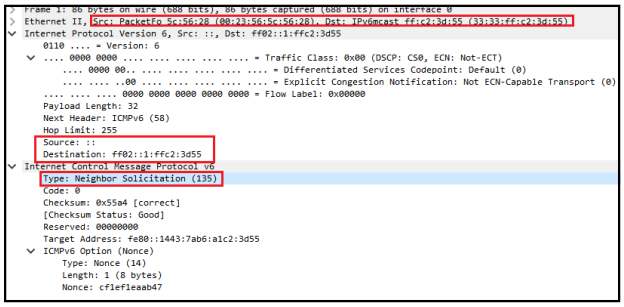
- 主机收到一个邻接点公告报文，而此报文的对象地址为其正在做DAD检测的地址，则主机从接口上删除这个地址（DAD检测失败）

  说明检测到地址重复

- 如果主机已完成为某个IPv6地址的DAD检测，随后收到来自其它主机发送的一个邻接点请求报文，而此报文源地址为全0地址::，对象地址是该主机已完成DAD检测的地址，则主机应该向全节点地址（FF02::1）发送邻接点公告

  告知其他主机地址重复

用于重复地址检测的邻接点请求报文



2.4.3 IPV6邻接点发现——路由器发现

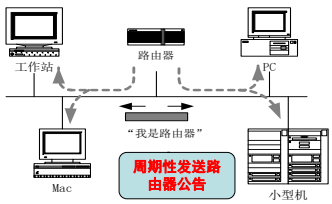
- 路由器发现:结点尝试发现本地链路上的路由器设置的过程
- 通过ICMPV6的“路由器请求和路由器公告”报文来实现。
- 实现的功能包括：
  - 帮助主机判断本地路由器是否存在，自动配置默认网关
  - 确定IPV6报头中的跳数限制字段的默认值
  - 确定结点是否应该为地址和其它配置参数，使用动态主机配置协议DHCPV6
  - 用于“邻接点请求”报文中的邻接点不可达检测和重发的定时器。
  - 需要添加到路由表的特定路由器
  - 为链路定义网络前缀列表，链路的MTU，以及自动配置地址的有效生存期和选用生存期。

2.4.3 IPV6邻接点发现——路由器发现

- IPV6路由器发现提供两种工作方式：
  - ①IPV6路由器在本地链路上主动发送伪周期的“路由器公告”报文，通告自己是本地链路上可用的一台路由器
    - 点击察看细节
  - ②正在启动的IPV6主机向链路本地范围内所有路由器组播地址，主动发送“路由器请求”报文,路由器应答“路由器公告”报文。
    - 点击察看细节

路由器主动发送“路由器公告”

- 路由器在本地链路上主动发送“路由器公告”报文，以宣告自己的存在，同时提供配置参数：如默认跳数限制、链路MTU、地址前缀和路由；
- 链路上的活动主机接收到报文后，使用上述参数来维护默认路由器列表、前缀列表及配置其它参数，进行自动配置地址和添加路由的操作。



路由器主动发送“路由器公告”

- 路由器公告消息（ Router Advertisement）

6	业务量类型	流标记：0	
净荷长度		下一头标:58	HOP限制:255
源IP地址:4C00::200:CFF:FE09:4B76			
链路本地范围所有结点组播地址			
目的IP地址:FF02::1			

类型:134	代码:0	校验和	
最大中继点	M O 保留	路由器生存时间	
可到达时间已过			
可到达的重发间隔			
选项代码:1	选项长度:1		
发送者链路地址:00000C094B76			
选项代码:5	选项长度:1	保留	
MTU尺寸			
选项代码:3	选项长度:4	前缀长度:64	L A
有效生存时间			
推荐生存时间			
保留			
前缀:4C00::200:CFF:FE09:4B76			

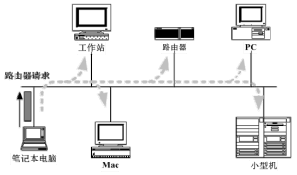
跳数限制为255，只在链路范围内有效
目的地址为链路范围内全节点地址

作用：由IPV6路由器周期性发送，包括主机配置需要的一些信息，如链路前缀、链路MTU、特定路由、是否使用地址自动配置以及由地址自动配置协议所创建地址的有效期与优先级等信息。

主机主动发送“路由器请求”

- 为了加快主机地址自动配置的速度，当主机接入网络时，它首先激活网络接口，向链路本地范围所有路由器多播地址FF02：2发送“路由器请求”报文
  - 如果主机已经配置了单播地址，则请求报文中的源地址为此单播地址；否则源地址为未指定地址“：：”。
- 收到“路由器请求”报文后，本地链路上的所有路由器都会向该主机单播地址(或链路本地范围内所有节点组播地址FF02::1)发送“路由器公告”报文。
- 主机收到“路由器公告”报文后，根据报文内容来建立默认路由器列表、前缀列表和其它配置参数。

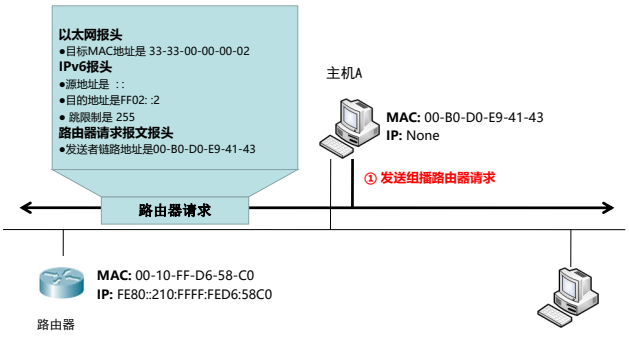
主机主动发送“路由器请求”



6	业务量类型	流标记:0
净荷长度:16	下一头标:58	Hop限制:255
源IP地址:FE80::260:8CFF:FE14:9252		
目的IP地址:FF02::2		
类型:133	代码:0	校验和
保留		
选项代码:1	选项长度:1	
发送者链路地址:00608C149252		

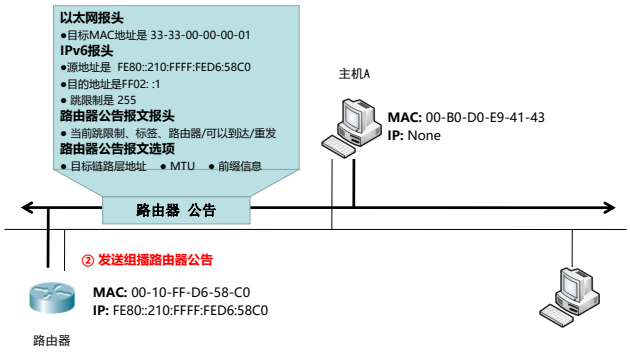
2.4.3 IPV6邻接点发现——路由器发现示例

- P169

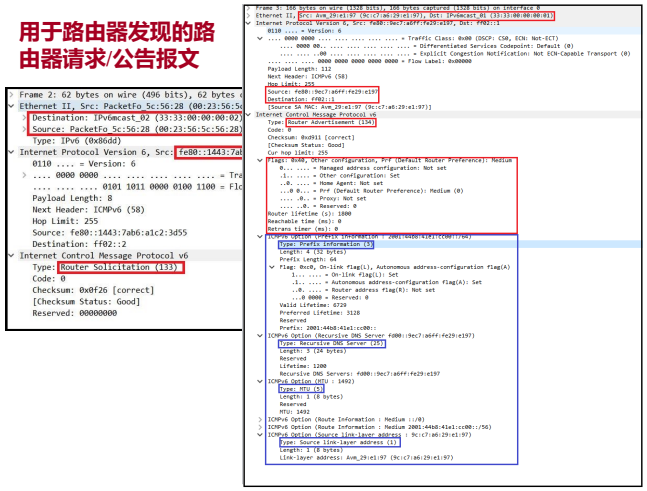


2.4.3 IPV6邻接点发现——路由器发现示例

- P170



用于路由器发现的路由器请求/公告报文



用于路由器发现的路由器请求报文

```
> Frame 131: 62 bytes on wire (496 bits), 62 bytes captured (496 bits)
> Ethernet II, Src: Megahert_05:80:da (00:00:86:05:80:da), Dst: IPv6mcast_02 (33:33:00:00:00:02)
v Internet Protocol Version 6, Src: fe80::200:86ff:fe05:80da, Dst: ff02::2
    0110 .... = Version: 6
  > .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... .... .... 0000 0000 0000 0000 0000 = Flow Label: 0x00000
    Payload Length: 8
    Next Header: ICMPv6 (58)
    Hop Limit: 255
    Source: fe80::200:86ff:fe05:80da
    Destination: ff02::2
    [Source SA MAC: Megahert_05:80:da (00:00:86:05:80:da)]
v Internet Control Message Protocol v6
    Type: Router Solicitation (133)
    Code: 0
    Checksum: 0x7557 [correct]
    [Checksum Status: Good]
    Reserved: 00000000
```

用于路由器发现的路由器公告报文

```
v Internet Protocol Version 6, Src: fe80::260:97ff:fe07:69ea, Dst: ff02::1
    0110 .... = Version: 6
  > .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... .... .... 0000 0000 0000 0000 0000 = Flow Label: 0x00000
    Payload Length: 64
    Next Header: ICMPv6 (58)
    Hop Limit: 255
    Source: fe80::260:97ff:fe07:69ea
    Destination: ff02::1
    [Source SA MAC: 3Com_07:69:ea (00:60:97:07:69:ea)]
v Internet Control Message Protocol v6
    Type: Router Advertisement (134)
    Code: 0
    Checksum: 0x4625 [correct]
    [Checksum Status: Good]
    Cur hop limit: 64
  > Flags: 0x00, Prf (Default Router Preference): Medium
    Router lifetime (s): 1800
    Reachable time (ms): 30000
    Retrans timer (ms): 1000
  v ICMPv6 Option (Source link-layer address : 00:60:97:07:69:ea)
      Type: Source link-layer address (1)
      Length: 1 (8 bytes)
      Link-layer address: 3Com_07:69:ea (00:60:97:07:69:ea)
  v ICMPv6 Option (MTU : 1500)
      Type: MTU (5)
      Length: 1 (8 bytes)
      Reserved
      MTU: 1500
  v ICMPv6 Option (Prefix information : 3ffe:507:0:1::/64)
      Type: Prefix information (3)
      Length: 4 (32 bytes)
      Prefix Length: 64
    > Flag: 0xc0, On-link flag(L), Autonomous address-configuration flag(A)
      Valid Lifetime: 3600000
      Preferred Lifetime: 3600000
      Reserved
      Prefix: 3ffe:507:0:1::
```

路由器发现过程总结

路由器伪周期性发送公告报文

↓

活动主机根据公告报文维护参数

正在启动的主机发送路由请求报文到所有路由器

↓

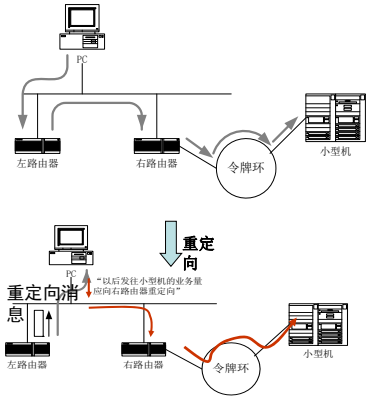
所有路由器向请求方（或多播的）发送公告报文

↓

主机根据公告报文创建默认路由表及前缀列表

2.4.3 IPV6邻接点发现——重定向功能的实现

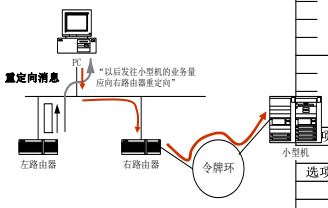
- 路由器使用重定向功能将更佳的首跳邻接点通知给初始主机，向指定目标发送的通信流应该首先转发到这个邻接点。如右图所示：



重定向功能的实现

重定向报文的结构

6	业务量类型	流标记:0
净荷长度	下一头标:58	Hop限制:255
源IP地址:左路由器		
目的IP地址:PC机		
类型:137	代码:0	校验和
保留:0		
对象地址:右路由器		
被重定向的目的IP地址:小型机		
选项代码:2	选项长度:1	
对象链路地址:右路由器		
选项代码:4	选项长度	保留:0
保留:0		
在重定向报文的总长度不超过1280字节的范围内把成为重定向的原数据报的一部分复制在此域内		



左路由器向PC机发送重定向消息

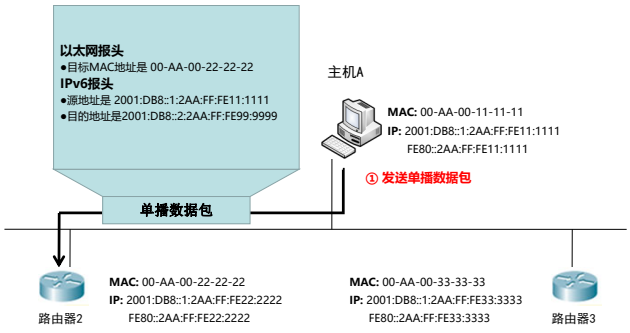
重定向功能实现步骤

- 1）初始主机转发单播数据包到默认路由器
- 2）路由器处理数据包时发现初始主机是邻接点，而且初始主机和次跳地址也都在同一链路上
- 3）路由器向初始主机发送重定向报文。在重定向报文的对象地址字段设置结点的下一跳地址，初始主机应该将寻址到目的地址的后续数据包都先发送到这个对象地址指定的结点。
- 4）路由器将数据包转发给合适的次跳地址。
- 5）初始主机在接收到重定向报文后用对象地址字段中的地址更新目标缓存中的条目。如果目标链路层地址选项在报文中，则使用报文内容来创建或更新邻接点缓存条目。

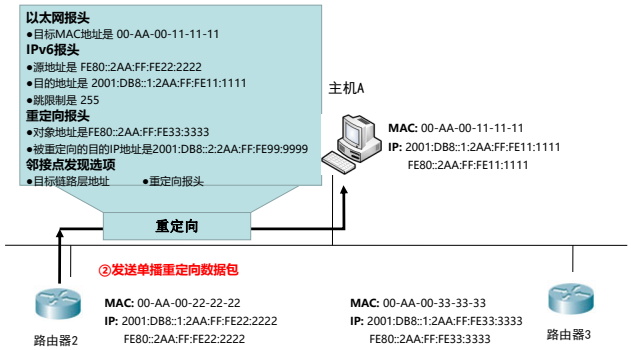
注意：重定向报文仅由初始主机和目标之间路径上的第一个路由器发送。主机从不发送，路由器也不会基于接收到的重定向报文以更新路由表。

重定向示例

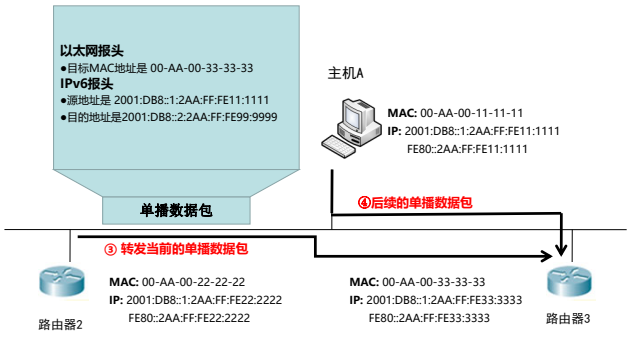
- P172



重定向示例

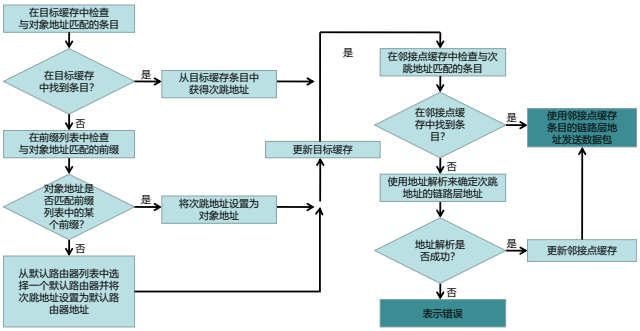


重定向示例



主机发现流程图

[IPv6主机发送单播 IPv6数据包的过程使用本地主机的概念数据结构和ND协议的组合方法]

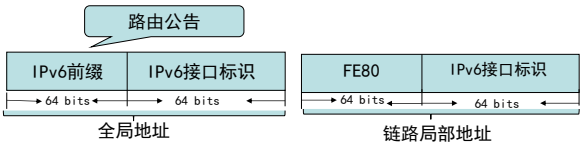


2.4.3 IPV6邻接点发现——IPv6地址自动配置

- 无状态(stateless)地址自动配置
  - RFC2462
  - 不需要对主机进行手动配置
  - 不需要额外的服务器，通过邻接点发现协议中的“路由器通告”、“邻接点请求”、“邻接点通告”报文来实现。
  - 不易管理
- 有状态(stateful)地址自动配置(DHCPv6)
  - RFC3315
  - DHCP v6服务器管理地址池，为主机分配IPv6前缀、IPv6地址和其他网络配置参数，如：DNS、WINS等配置信息
  - 易于管理，在结点对IPV6地址分配要求严格时使用。
  - 无状态和有状态地址自动配置可以同时使用，前者用于自动配置主机地址，后者用来获取其它的信息

IPv6无状态地址自动配置

- 无状态地址自动配置的基本思想：
  - 因为IPV6接口标识可以由EUI-48地址自动生成，所以无状态地址自动配置的关键在于如何获得IPV6前缀。
  - 一般情况下，主机需要的前缀是与主机连接的路由器接口的前缀。
  - 为了获得这个前缀，需要利用邻接点发现协议中的“路由器请求”、“路由器公告”报文来实现。
  - 实现过程见下页



IPv6无状态地址自动配置

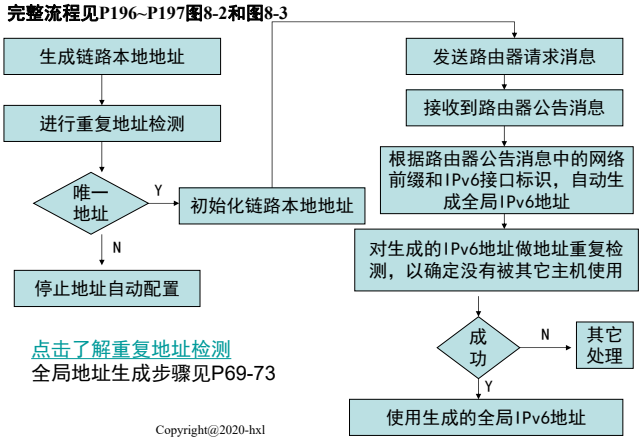
- 首先，主机为网络接口自动配置链路本地地址
  - ①生成64比特的IPv6接口标识
    - 48比特MAC地址→64比特EUI-64地址→IPv6接口标识
    - 随机接口标识
  - ②组合前缀FE80::/64和IPv6接口标识生成链路本地地址
  - ③对临时链路本地地址进行重复地址检测（DAD），若DAD失败，必须为主机进行手动配置；若DAD通过，继续下一步
  - ④在网卡上注册与链路本地地址对应的被请求节点组播地址的链路层组播地址
- 接下来，主机为网络接口自动配置全局地址.....

IPv6无状态地址自动配置

- 接下来，主机为网络接口自动配置全局地址
  - ①主机发送路由器请求报文，路由器响应路由器通告报文
  - ②生成64比特的IPv6接口标识（同上）
  - ③主机根据收到的路由器通告报文，设置跳数限制、可达时间、重发定时器及MTU等
    - 对于每个路由器通告报文包含的前缀信息可选项，执行如下操作：
      - 如果链路上标记设置为1，将该前缀添加到前缀列表
      - 如果自治标记设置为1，则将此网络前缀和IPv6接口标识生成全局IP地址
      - 对全局IP 地址进行重复地址检测DAD，检测通过启用该地址
    - 如果路由器通告报文的“管理地址配置”标记设置为1，则使用DHCPV6协议进行地址配置
    - 如果路由器通告报文的“其他状态配置”标记设置为1，则使用DHCPV6协议来获取其他配置参数。

IPv6无状态地址自动配置简化流程

完整流程见P196~P197图8-2和图8-3

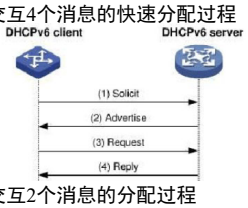


点击了解重复地址检测

全局地址生成步骤见P69-73

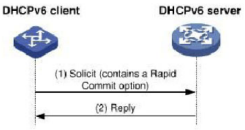
DHVPv6地址自动配置

- DHCPv6服务器为客户端分配地址/前缀的过程分为两类：
  - 交互4个消息的快速分配过程



①客户端发送Solicit消息请求服务器为其分配地址/前缀和网络配置参数
②客户端接收到多个服务器回复的Advertise消息，根据消息接收的先后顺序、服务器优先级等，选择其中一台服务器，并向该服务器发送Request消息，请求服务器确认为其分配地址/前缀和网络配置参数

  - 交互2个消息的分配过程

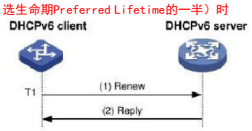


①Solicit消息中携带Rapid Commit选项，表示客户端希望服务器能够为其快速配置地址
②服务器如果支持地址快速分配，则返回Reply消息，为客户端分配IPV6地址

DHCPv6地址/前缀租约更新过程

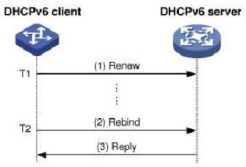
- DHCPv6服务器分配的IPv6地址/前缀具有一定的租借期限。租借期限由有效生命期(Valid Lifetime)决定。在有效生命期到达之前，如果DHCPv6客 户端希望继续使用该地址/前缀，则需要更新地址/前缀租约。

地址/前缀租借时间到达时间T1（推荐值为首选生命期Preferred Lifetime的一半）时



通过Renew更新地址/前缀租约

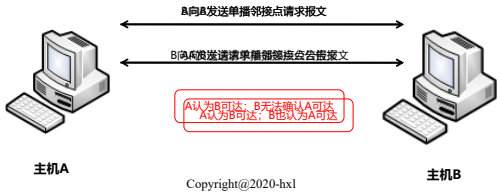
T1时发送的Renew请求更新租约，客户端没有收到DHCPv6服务器的回应报文



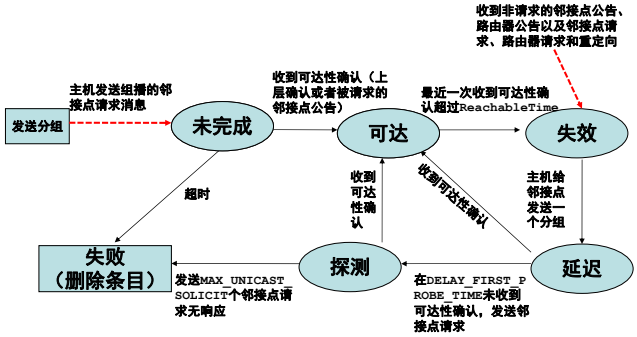
通过Rebind更新地址/前缀租约

2.4.3 IPV6邻接点发现——邻接点不可达检测NUD

- NUD（Neighbor Unreachability Detective）是节点确定它邻居可达性的过程
  - 确认可达性的方法之一：查看邻接点缓存中邻接点条目的状态，可以判断邻接点的可达性，而通过发送单播邻接点请求报文和接收邻接点公告报文，可以帮助维护邻接点缓存。
  - 确认可达性的另一个方法是：利用上层协议进行两方通信交互。



主机的邻接点缓存条目的状态



2.4.3 IPV6邻接点发现——邻接点不可达检测NUD

- 邻接点高速缓存表的邻接点条目有以下5种状态：
  - “未完成(Imcomplete)”：
    - 主机使用多播的"邻接点请求"，解析某个邻接点的链路层地址，此时主机创建了该邻接点的新的高速缓存表项，但表项中还未填入此邻接点的的链路层地址；
    - 如果超时且尝试Max_unicase_solicit(默认为3)次后未仍未收到邻接点的“可达性”信息（如：响应“邻接点请求”的单播“邻接点公告”），删除此邻接点对应的高速缓存条目。
  - “可达(Reachable)”：
    - 主机接收到某个邻接点的可达性确认信息，如果此邻接点的表项状态为“未完成(Imcomplete)”，将邻接点的链路层地址填入表项、“ReachableTime”定时器开始计时
    - 定时器超时前，或与此邻接点的上层协议通信仍然继续，表项始终保持“可达(Reachable)”状态。

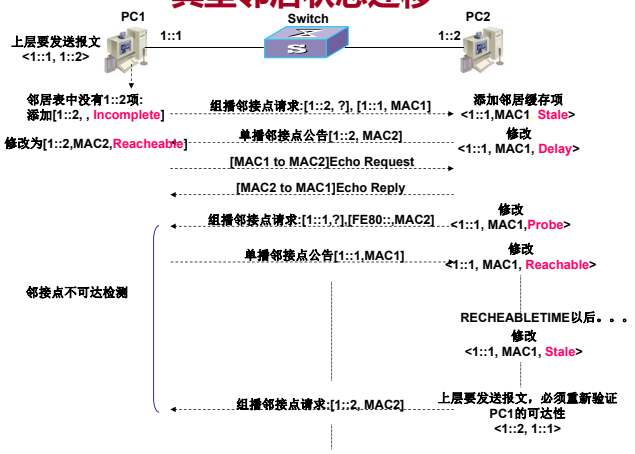
2.4.3 IPV6邻接点发现——邻接点不可达检测NUD

- 邻接点高速缓存表的邻接点条目有以下5种状态：
  - “失效(Stale)”：
    - 某邻接点表项在“可达(Reachable)”状态下“ReachableTime”定时器超时，则表项进入“失效(Stale)”状态，直到有数据包发送给这个邻接点
    - 或者主机收到某个邻接点发送的未经请求的“邻接点公告”、“路由器公告”以及“重定向”等报文时，此邻接点对应的表项也进入“失效(Stale)”状态

2.4.3 IPV6邻接点发现——邻接点不可达检测NUD

- 邻接点高速缓存表的邻接点条目有以下5种状态：
  - “延迟(Delay)”：
    - 主机往处于“失效(Stale)”状态的邻接点发送报文，则该邻接点对应表项进入“延迟(Delay)”状态，期待上层协议提供该邻接点的“可达性”信息。
    - 在Delay_first_probe_time时间之内收到该邻接点的“可达性”信息，表项进入“可达(Reachable)”状态；若未能收到，则向该邻节点发送“邻接点请求”报文，表项进入“探测(probe)”状态。
  - “探测(probe)”：
    - 主机持续向处于“探测(probe)”状态的邻接点发送“邻接点请求”，直到收到“可达到性”信息，两个请求间隔为retrans timer毫秒，最多尝试Max_unicase_solicit(默认为3)次后未收到邻接点的可达性确认信息，删除此邻接点对应的高速缓存条目。

典型邻居状态迁移



本章内容

- 2.1 IPV4局限性与IPV6特点
- 2.2 IPV6地址表达与分类
- 2.3 IPV6数据报及报头
- 2.4 ICMPV6协议
- 2.5 IPv4向IPv6过渡

2.5 IPv4向IPv6过渡

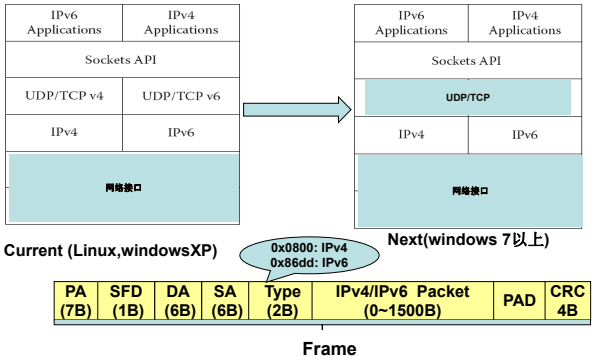
- IPv4/IPv6过渡的两大主流技术
  - IPv4/IPv6双协议栈或双协议层
    - 即主机和路由器在同一网络接口上运行IPv6栈和IPv4栈。这样，双栈节点既可以接受和发送IPv4包，也可以接受和发送IPv6包，因而两个协议可以在同一网络中共存。
  - 隧道技术
    - 通过报文封装的方式连接被其他类型网络分隔的同一类型节点或网络。隧道的端点可以是主机或者路由器，但必须是双协议栈的节点。
    - 过渡初期，IPv6 over IPv4隧道用来在IPv4网络上连接孤立的IPv6节点，将IPv6的分组封装在IPv4分组中，从而实现两个IPv6孤岛之间的连接。

2.5 IPv4向IPv6过渡

- 双栈技术
  - 优点是互通性好，易于理解；
  - 缺点是需要给每个新的IPv6协议的网络设备和终端分配IPv4地址，不能解决IPv4地址短缺问题；实现全网的双栈部署需巨额投资。
- 隧道技术
  - 优点在于透明性，IPv4 / IPv6主机之间的通信可以忽略隧道的存在，隧道只起物理通道的作用，它不需要大量的IPv6专用路由器设备和专用链路，可以明显减少投资，具有良好可扩展性；
  - 缺点在于配置隧道比较麻烦，而且隧道技术不能实现IPv4和IPv6主机之间的通信。

IPv4向IPv6过渡的双协议栈

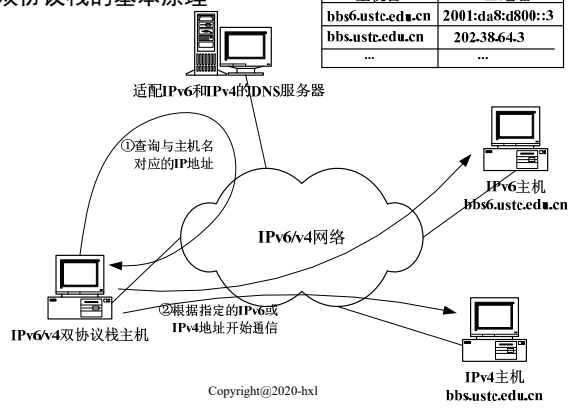
- 双协议栈（P259）
- 双IP层(P258)



IPv4向IPv6过渡的双协议栈

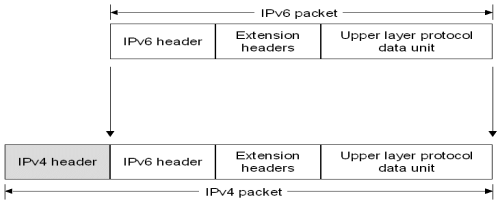
- 双协议栈的基本原理

主机名	IP地址
bbs6.ustc.edu.cn	2001:da8:d800::3
bbs.ustc.edu.cn	202.38.64.3
...	...



IPv4向IPv6过渡的隧道技术

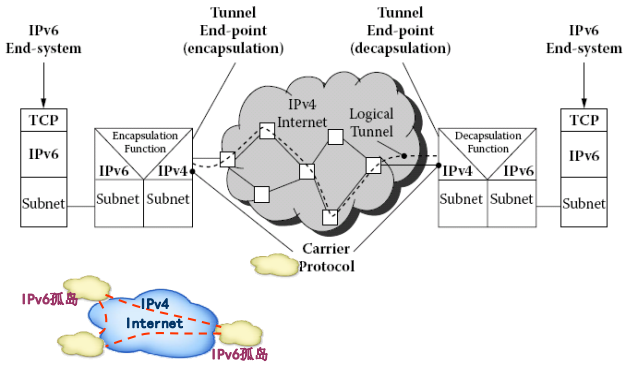
■ IPv6 over IPv4（IPv6-in-IPv4）隧道封装



通过将IPv6数据包作为负载封装在IPV4协议中，实现被封装的协议数据单元(IPv6)通过封装协议的网络(即IPv4网络)进行传输，IPV4头部协议字段值为41，表示这是一个经过封装的IPV6分组。源地址和目的地址分别为隧道端点的IPV4地址

IPv6 overIPv4 隧道

■ 隧道协议体系结构



IPv6 over IPv4（IPv6-in-IPv4）隧道封装

```
> Frame 1: 899 bytes on wire (7192 bits), 899 bytes captured (7192 bits)
> Ethernet II, Src: HonHaiPr_41:9c:20 (00:16:cf:41:9c:20), Dst: Unispher_41:65:41 (00:90:1a:41:65:41)
> PPP-over-Ethernet Session
> Point-to-Point Protocol
v Internet Protocol Version 4, Src: 70.55.213.211, Dst: 192.88.99.1
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 877
    Identification: 0x9359 (37721)
  > Flags: 0x0000
    ...0 0000 0000 0000 = Fragment offset: 0
    Time to live: 128
    Protocol: IPv6 (41)
    Header checksum: 0x64aa [validation disabled]
    [Header checksum status: Unverified]
    Source: 70.55.213.211
    Destination: 192.88.99.1
v Internet Protocol Version 6, Src: 2002:4637:d5d3::4637:d5d3, Dst: 2001:4860:0:2001::68
    0110 .... = Version: 6
  > .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
    .... .... .... 0000 0000 0000 0000 0000 = Flow Label: 0x00000
    Payload Length: 817
    Next Header: TCP (6)
    Hop Limit: 128
    Source: 2002:4637:d5d3::4637:d5d3
    Destination: 2001:4860:0:2001::68
```

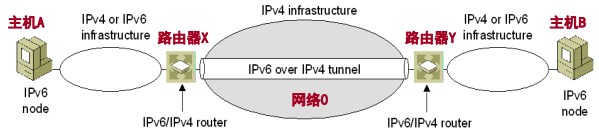
IPv6 overIPv4 隧道

- 隧道配置的三种情况
  - 路由器-路由器隧道
  - 主机-主机隧道
  - 路由器-主机\主机-路由器隧道
- 隧道配置的两种类型
  - 手工配置隧道
  - 自动配置隧道

路由器-路由器隧道

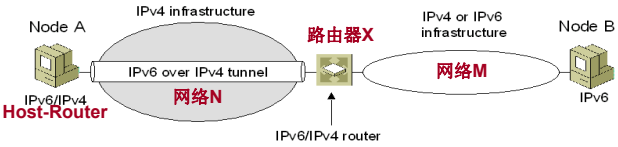
- 路由器-路由器隧道。
  - 路由器X和路由器Y使用隧道方式来传送经过网络0的包，网络0只支持IPv4，网络的其他部分可支持IPV6。主机A可以透明地将IPv6包发送给主机B，这两个主机都不必考虑中间插入的IPv4网络(即网络0)。这种情况下，主机A和主机B都是只支持IPv6的节点。

Router-Router



主机-路由器隧道

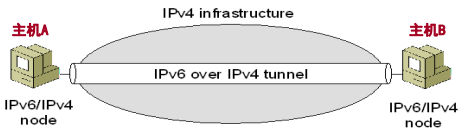
- 主机-路由器隧道。
  - 假设此时主机A和路由器X为双栈节点，网络N只支持IPv4，而网络的其他部分都只支持IPv6。这种情况下，主机A仅对发往路由器X的IPv6包采用隧道方式；一旦通过了只支持IPv4的网络N，路由器X就对这些通过隧道传送的包拆包，然后按正常方式通过IPv6网络转发。
- 路由器-主机隧道（与上述情况相反）。
  - 此时网络M只支持IPv4，主机B为双栈结点，网络的其他部分都只支持IPv6。这种情况下，隧道传送发生在路由器X和主机B之间。在网络的其他部分，IPv6包可以自由传送。



主机-主机隧道

- 主机-主机隧道
  - 假设此时只有主机A和主机B同时支持IPv4和IPv6，而网络的其他部分都只支持IPv4。这种情况下，隧道传送发生在主机A和主机B之间。对于发往主机B的IPv6包，主机A必须把它们封装在IPv4包中，以便由只支持IPv4的路由器来运载。

Host-Host



隧道的配置方式

- 手工配置隧道(Configured Tunneling)
  - 对每个IPv6分组，都事先手工配置它所对应的隧道端点，主要是用于隧道封装所需的IPv4地址
  - 手工配置隧道适合于比较固定的IPv6 连接，缺点是每两个IPv6 网络之间都要手工建立隧道配置比较麻烦。
- 自动配置隧道(Automatic Tunneling)
  - 分组中所包含的IPv6地址决定隧道的端点，主要是指用于隧道封装所需的IPv4地址

这里讨论的是IPv6分组如何通过IPv4网络传输的情况

自动配置的本质是建立一个IPv6地址到IPv4地址之间的映射关系

手工配置隧道

- IPv6报文被包含在IPv4报文中作为IPv4的载荷

- 手工配置隧道通常用于路由器-路由器的隧道，必须在隧道两端的路由器上都创建隧道接口，并添加使用隧道接口的路由
- 例如：在Windows中创建 IPv6-in-IPv4 隧道使用命令：
  - netsh interface ipv6 add v6v4tunnel [interface=]Name [localaddress=]IPv4Address [remoteaddress=]IPv4Address
    - [interface=]Name 是隧道接口名称
    - [localaddress=]IPv4Address 指定本地隧道端点的 IPv4 地址
    - [remoteaddress=]IPv4Address 指定远程隧道端点的 IPv4 地址

手工配置隧道

例如，有两个测试实验室子网分别位于内联网的不同部分。路由器 1 连接到 IPv6 子网 2001:db8:0:1::/64，并且 IPv4 地址是 131.107.47.121。路由器 2 连接到 IPv6 子网 2001:db8:0:2::/64，并且 IPv4 地址是 157.54.9.211。图 11-9 所示为这个配置。

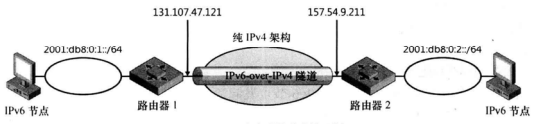


图 11-9 手动配置隧道的示例

为了在路由器 1 和路由器 2 之间配置一个隧道，要在路由器 1 上运行下列命令：

```
netsh interface ipv6 add v6v4tunnel Tunnel To2 131.107.47.121 157.54.9.211
netsh interface ipv6 add route 2001:db8:0:2::/64 TunnelTo2
```

同样，还要在路由器 2 上运行下列命令：

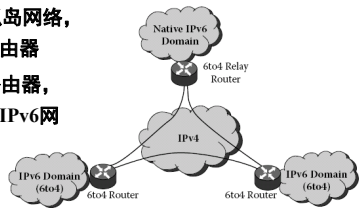
```
netsh interface ipv6 add v6v4tunnel TunnelTo1 157.54.9.211 131.107.47.121
netsh interface ipv6 add route 2001:db8:0:1::/64 TunnelTo1
```

自动配置隧道

- 自动配置隧道
  - **6over4协议(略)：6over4(IPv4 组播隧道)是一种应用在区域范围的自动隧道机制，也称为虚拟以太网。它的作用是使得一个具备组播能力的IPv4局域网内孤立的IPv4 / IPv6节点间能够实现IPv6的组播连接。需要IPv4组播支持。**
  - **6to4协议（P263）**
  - **ISATAP（站点内自动隧道寻址）协议(P244)**
  - **6PE协议(略)：利用BGP/MPLS VPN的技术原理，将IPv6网络视为一个VPN，通过IPv4 MPL主干网连接IPv6孤岛，控制层面采用多协议边界网关协议完成IPv6路由交互，数据层面采用MPLS协议对IPv6报文进行转发。**

6to4协议

- **通过IPv4网络连接IPv6孤岛网络，隧道的两个端点为6to4路由器**
- **可通过6to4中继(Relay)路由器，使6to4网点连接到大的纯IPv6网络**



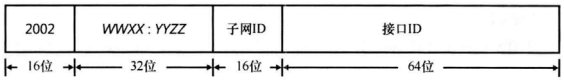
6to4主机：最少配置了一个6to4 IPv6地址，所配置的IPV6地址的前缀中嵌入了对应6to4路由器的IPV4地址

6to4路由器：IPv6/IPv4双栈路由器，执行隧道封装和解封装操作，在6to4主机和其它的6to4路由器之间、6to4中继路由器之间，通过隧道转发目的地址为6to4 IPv6地址的数据

6to4 中继路由器：IPv6/IPv4双栈路由器，位于IPV6网络和IPV4公网边界处，在IPv6主机和6to4路由器之间转发目的地址为6to4 IPv6地址的数据，使用任播地址192.88.99.1作为通用6to4中继路由器地址。

6to4协议

- **6to4地址**

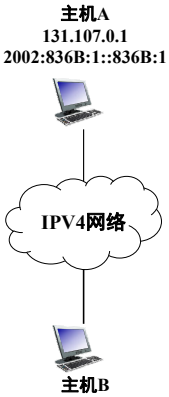


  - **2002::/16是为6to4保留的地址空间**
  - **WWXX:YYZZ是分配给支持6to4主机或6to4路由器的公有IPv4地址(w.x.y.z)的十六进制冒号表示**
- **优点**
  - **不需要为每条隧道预先配置，维护方便**
- **缺点**
  - **6to4网络需要使用公有IPV4地址和不含NAT的路由路径**

6to4隧道化示例

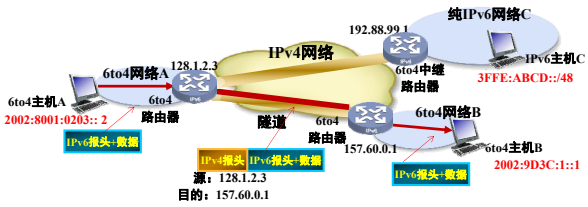
- **当主机A直接向主机B的6to4地址发送IPV6流量时，6to4隧道接口使用自身的公共IPV4地址做为源IPV4地址，然后根据目的主机B的IPV6地址生成要封装的IPV4首部的目的地址，具体地址示例如下：**

字段	值
IPV6源地址	2002:836B:1::836B:1
IPV6目的地址	2002:9D36:1::9D36:1
IPV4源地址	131.107.0.1
IPV4目的地址	157.54.0.1



IPV4和IPV6网络上的6to4组件

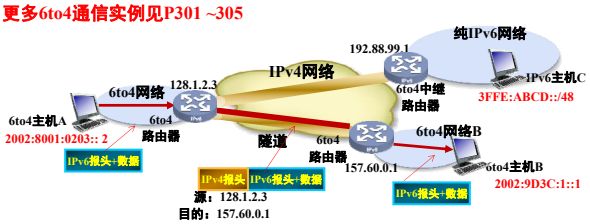
- **在通过6to4路由器连接到IPV4网络的6to4网络中，6to4路由器会公告前缀2002:WWXX:YYZZ:SubnetID::/64**
- **例如在6to4网络B：路由器在内网通告2002:9D3C:1:1::/64前缀(64位前缀的子网ID可以手动指定，也可以由路由器自动决定），6to4主机B使用无状态地址自动配置技术，自动配置地址2002:9D3C:1:1::1**



6to4主机与IPV6公网主机通信

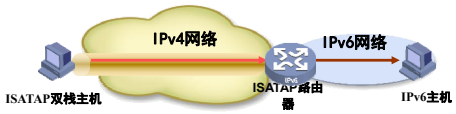
- **1、主机C主动向6to4主机A发送报文时，报文被转发至6to4中继路由器**
- **2、中继路由器对报文的目标IP地址检查后发现是一个6to4主机，因而提取*8001:0203*，得到*128.1.2.3*作为对端地址，进行IPv4隧道封装并发往IPV4公网**
- **3、6to4路由器收到隧道报文后解封装发回主机A**

更多6to4通信实例见P301 ~305



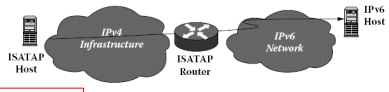
ISATAP协议

- ISATAP隧道技术
  - 连接IPv4网络内的双栈主机和IPv6网络，在IPv4报文中封装IPv6报文
  - ISATAP设计初衷是用于对生产网络的测试环境，或者测试一些通过IV6环境的应用程序。
- 优点
  - IPv4网络内的双栈主机可自动获得IPv6前缀
- 缺点
  - IPv4网络内的双栈主机ISATAP主机无法自动获取ISATAP路由器地址，需要预先静态配置或DHCP协议动态获取

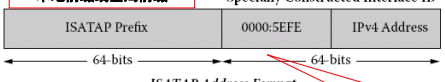


ISATAP隧道技术

- ISATAP地址



ISTAP路由器公告的链路本地前缀或全局前缀



ISATAP Address Format

ISATAP 主机IP地址前缀

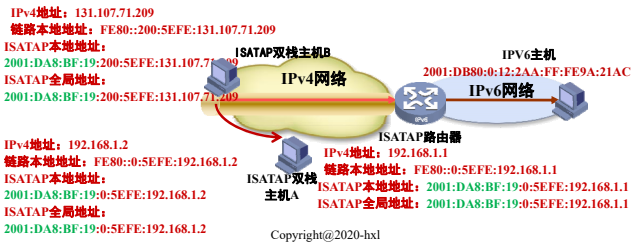
Example:
IPv4 Address is: 142.34.14.35
Routing Prefix is: 2001:4C03:0:1

ISATAP IPv6 Address is: 2001:4C03:0:1::5EFE:142.34.14.35
Link-local Variant is: FE80::5EFE:142.34.14.35

前缀0000:5EFE，其中0000为：000000ug00000000，当确定IPv4地址是公网地址时，u=1，否则u=0；g表示是否为群组，所以0200：5EFE用于表示一个公有的单播IPV4地址；0000:5EFE用于表示一个私有的单播IPV4地址

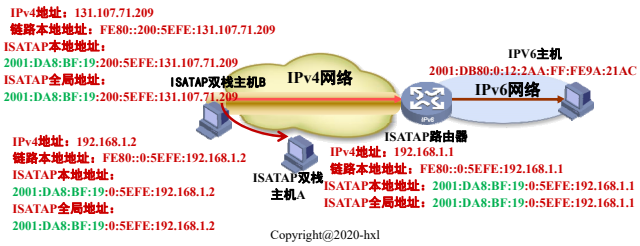
ISATAP地址配置实例

- 1、图中双栈主机A和B位于同一个ISATAP子网，该子网内ISATAP路由器拥有*2001:DA8:BF:19::/64*的全局子网前缀
- 2、ISATAP主机A根据自己IPv4地址生成 ISATAP链路本地地址
- 3、主机A向ISATAP路由器发送路由器请求（可通过DNS解析将主机名ISATAP解析为ISATAP路由器的IPv4地址~P276），该消息使用 ISATAP链路本地地址，通过隧道发送。
- 4、ISATAP路由器响应路由器公告报文，ISATAP主机A根据公告中的前缀生成全局的ISATAP地址



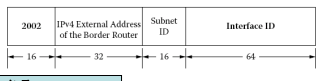
ISATAP通信示例——ISTAP主机到IPV6主机

- 1、ISATAP主机A将IPv6报文封装上IPv4首部，源地址为自身的IPv4地址，发送至预先配置好的ISATAP路由器的IPv4地址。
- 2、当ISATAP路由器收到IPv6-over-IPv4隧道报文时，对其解封装，将得到的IPv6报文发送至IPv6公网；当路由器收到IPv6回程报文时，取报文的IPv6目的地址后32bits作为目的IPv4地址，为回程报文封装上IPv4首部，通过隧道发回ISATAP主机A
- 3、当通信双方为同一个ISATAP域下的ISATAP主机时，可以直接通信(P282图12-6)

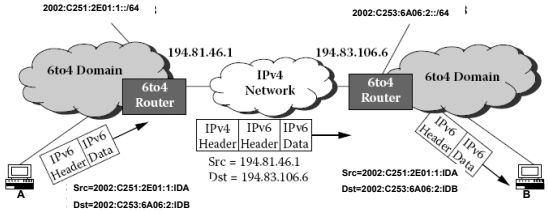


6to4协议实例

- 实例



6to4路由器上路由表项：
2002::/16 其它6to4站点
缺省(::) 6to4 relay router



IPv6 Host (e.g.
2002:C251:2E01:1:IDA

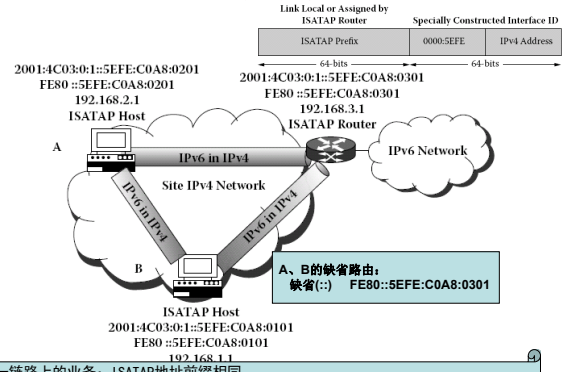
Note: C251:2E01 (hex) is equivalent to 194.81.46.1 (dotted decimal)
1100 0010 0101 0001 0010 1110 0000 0001

IPv6 Host (e.g.
2002:C253:6A06:2:IDB

Note: C253:6A06 is equivalent to 194.83.106.6
1100 0010 0101 0011 0110 1010 0000 0110

ISATAP协议实例

实例



对于同一链路上的业务：ISATAP地址前缀相同
A、B交换IPv6分组使用链路局部地址，通过之间的IPv6-in-IPv4隧道转发
对于不同链路上的业务：ISATAP地址前缀不同
根据缺省路由，A、B将IPv6分组通过IPv6-in-IPv4隧道发送到ISATAP路由器

本章结束