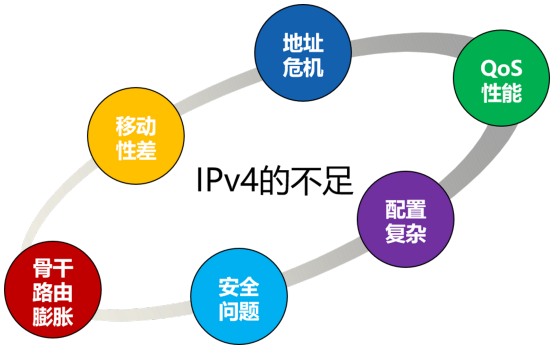
# IPv6

一、IPv6的研究与开发原因




1、IPv4存在地址不够用的问题
2、IPv4中的QoS为可选项，IPv6中的QoS为必选项
3、IPv4存在VLSM【可变长子网掩码】与CIDR【无类域间路由汇总】的问题，IPv6不存在子网的问题
4、IPv4存在安全性隐患
5、IPv4的ISP骨干路由器路由表膨胀
6、IPv4的移动性差

二、从IPv4过渡至IPv6时的临时解决方案
1、通过使用CIDR令骨干路由器的路由表尽量缩短
2、NAT
3、DHCP

三、IPv6的特点
1、拥有更大的地址空间结构【$2^{128}$】
2、拥有更高效的路由基础【取消了子网的概念】
3、更好的安全性
4、更好的移动性
5、更优的QoS性能

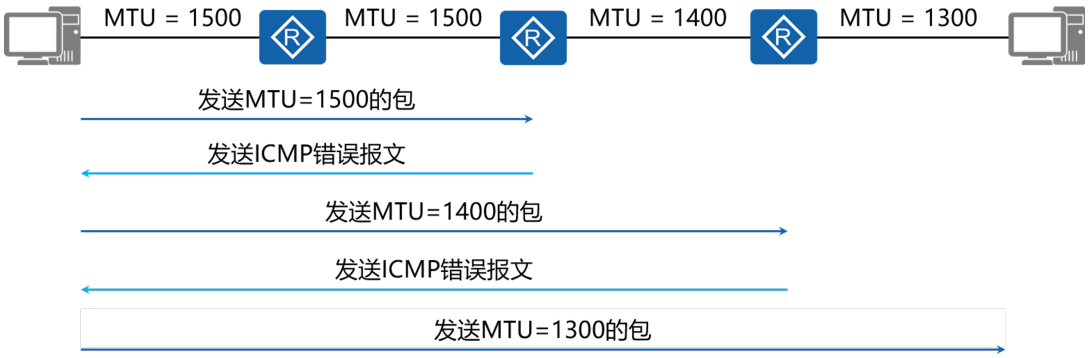
四、IPv6的包头格式


1、流量类型（流类别）字段：相当于IPv4中的QOS字段，规定使用的服务类型
2、流标签字段：长度为20位，用于标识同一业务流的数据。中间转发路由器对于同一源和目的的一个业务流数据采用相同的转发行为，来提高转发效率
3、下一报文首部字段：指出扩展头的位置
4、跳数限制：类似于IPv4中的TTL，但是跳数的上限由上层协议来规定
5、V6的IP地址变成128位

6、IPv6首部中没有首部长度字段，因为IPv6的首部是固定长度
7、IPv6首部中没有用于分段和重组的字段。IPv6的分段与重组只发生在源端和目的端，中间结点不再进行分段和重组。IPv6的分段和重组用的字段位于扩展报头
8、IPv6首部中没有校验和，校验依靠上层完成
9、在扩展首部中标识上层协议
10、在扩展首部中还包含加密和身份验证的字段

五、IPv6的地址结构
1、IPv6包含$2^{128}$个IP地址：340,282,366,920,938,463,463,374,607,431,768,211,456个地址
2、IPv6使用【:分十六进行】的形式进行表示

六、更高效的路由基础
1、IPv4存在众多不连续子网的问题，因而骨干路由器的路由表过于庞大；IPv6接入骨干网的ISP的地址空间是连续的
2、IPv6的中间转发路由器不再作分片和重组的工作，整条链路采用路径MTU发现机制，整个链路使用最小MTU发送数据

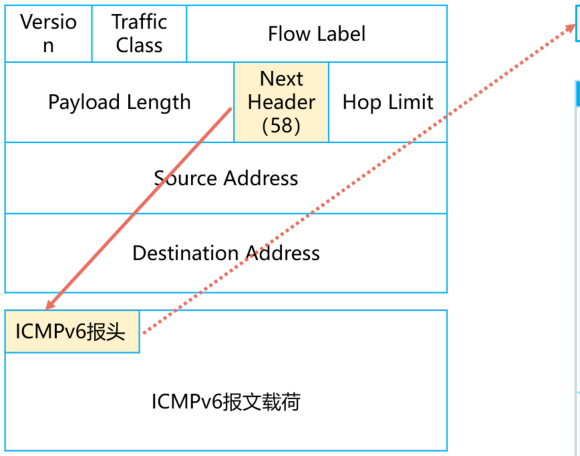



七、ICMPv4
1、Internet控制消息协议 — ICMP【Internet Control Message Protocol】是IP协议的辅助协议
2、ICMP协议用来在网络设备间传递各种差错和控制信息，对于收集各种网络信息、诊断和排除各种网络故障等方面起着至关重要的作用


| Type | Code | Checksum |
|---|---|---|
| ICMP的报文内容 | | |

| Type | Code | 描述 |
|---|---|---|
| 0 | 0 | Echo Reply |
| 3 | 0 | 网络不可达 |
| 3 | 1 | 主机不可达 |
| 3 | 2 | 协议不可达 |
| 3 | 3 | 端口不可达 |
| 5 | 0 | 重定向 |
| 8 | 0 | Echo Request |

八、ICMPv6概述
1、ICMPv6是IPv6的基础协议之一
2、在IPv6报文头部中，Next Header字段值为58则对应为ICMPv6报文
3、ICMPv6报文用于通告相关信息或错误
4、ICMPv6报文被广泛应用于其它协议中，包括NDP、Path MTU发现机制等
5、ICMPv6控制着IPv6中的地址自动配置、地址解析、地址冲突检测、路由选择、以及差错控制等关键环节
6、ICMPv6的报文格式如下：




| Type | Code | Checksum |
|---|---|---|

| 消息类型 | Type | 名称 | Code |
|---|---|---|---|
| 差错消息 | 1 | 目的不可达 | 0 无路由 |
| | | | 1 因管理原因禁止访问 |
| | | | 2 未指定 |
| | | | 3 地址不可达 |
| | | | 4 端口不可达 |
| | 2 | 数据包过长 | 0 |
| | 3 | 超时 | 0 跳数到0 |
| | | | 1 分片重组超时 |
| | 4 | 参数错误 | 0 错误的包头字段 |
| | | | 1 无法识别的下一包头类型 |
| | | | 2 无法识别的IPv6选项 |
| 信息消息 | 128 | Echo Request | 0 |
| | 129 | Echo Reply | 0 |

7、ICMPv6报文分为两类：

7.1、差错报文

7.1.1、差错报文【Error Messages】，也称为差错消息，Type字段最高bit为0，也就是ICMPv6 Type=[0，127]

7.1.2、差错消息用于报告在转发IPv6数据包过程中出现的错误，如常见的目的不可达、超时等等

7.2、信息报文

7.2.1、信息报文【Information Messages】，也称为信息消息，Type字段最高bit为1，也就是ICMPv6 Type=[128，255]

7.2.2、信息报文可以用来实现同一链路上节点间的通信和子网内的组播成员管理等

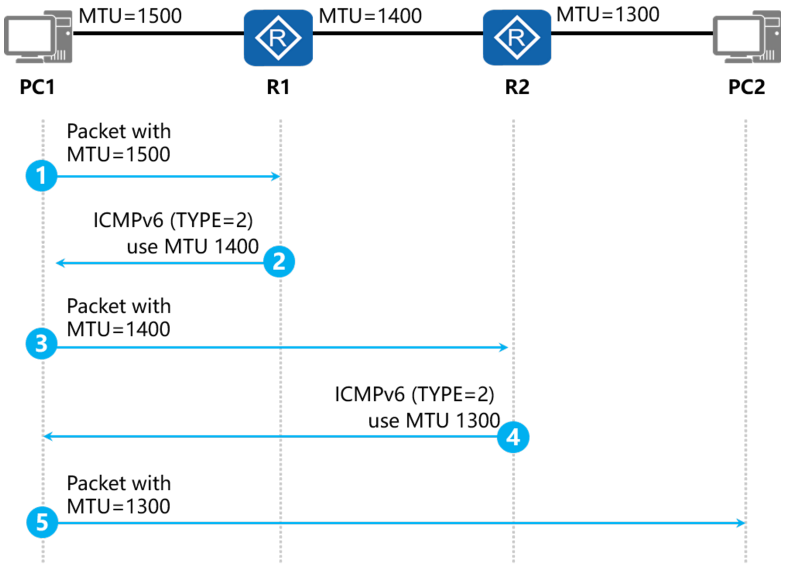
8、ICMPv6差错报文应用 — Path MTU发现

8.1、在IPv6中，中间转发设备不对IPv6报文进行分片，报文的分片将在源节点进行

8.2、PMTU【Path MTU】就是路径上的最小接口MTU

8.3、PMTUD【Path MTU发现机制】的主要目的是发现路径上的MTU，当数据包被从源转发到目的地的过程中避免分段

8.4、依赖PMTUD，数据的发送方可以使用所发现到的最优PMTU与目的地节点进行通信，这样可以避免数据包在从源传输到目的的过程之中，被中途的路由器分片而导致性能的下降




九、IPv6的安全性

IPv4中，IPSec为可选项，而在IPv6中，IPSec为必选项，其通过扩展包头来实现IPsec

十、IPv6的移动性与QoS

1、IPv4在设计之初并未考虑移动性问题，而IPv6设计时就考虑到对移动特性的支持，其可令每台设备拥有唯一且固定的全局单播地址

2、IPv6引入【流 | flow】的概念，提供对QoS的内置支持

十一、流 | flow

1、从同一个源发向同一个目的地【单播或组播】的包序列，信源希望中间路由器对这些包进行特殊处理

2、IPv6利用流类别、流标签实现了强大的QoS

十二、IPv6的地址表示结构

1、将每段转换为十六进制数，并用冒号隔开

eg：2001:0410:0000:0001:0000:0000:0000:45ff

2、压缩表示，可去掉不必要的【0】

eg：2001:410:0:1:0:0:0:45ff

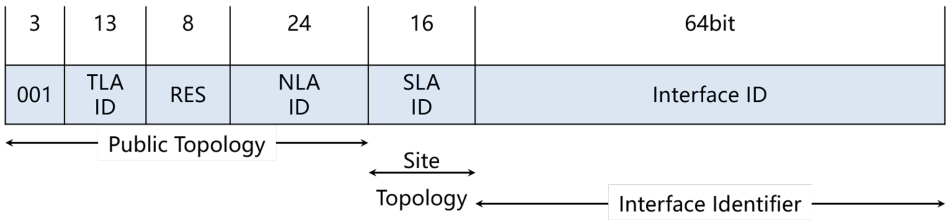
3、【::】表示多个连续的0

eg：2001:410:0:1::45ff

注：【::】在整个地址中只能出现一次

十三、IPv6的单播地址

1、全局单播地址 —— 相当于IPv4中的公有地址，其首部3位为001




其前45位可反映全球ISP的层次结构

1.1、TLA ID：顶级汇聚标识符

1.2、NLA ID：下一级汇聚标识符

1.3、SLA ID：站点汇聚标识符

2、链路本地地址 —— 用于IPv6中的邻居发现

2.1、IPv6中不存在广播，因此IPv4中的ARP在IPv6中无法工作，【邻居发现】是IPv6中和IPv4的ARP对应的寻址机制

2.2、链路本地地址以【FE80】开头

2.3、路由器不会转发链路本地地址


2.4、ICMPv6其它常用报文

邻居发现【RFC2461和RFC4861】

Type=133　路由器请求【Router Solicitation】

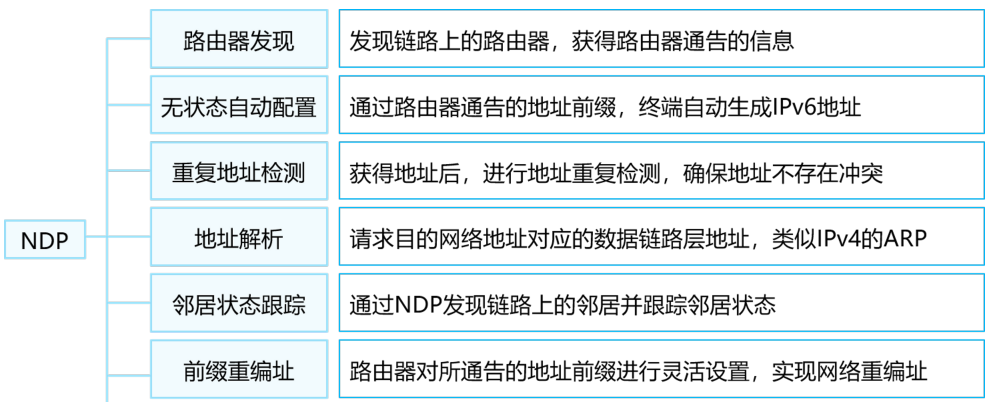
Type=134　路由器通告【Router Advertisement】

Type=135　邻居请求【Neighbor Solicitation】

Type=136　邻居通告【Neighbor Advertisement】

Type=137　重定向【Redirect】

2.5、RFC2461定义了IPv6邻居发现协议 — NDP，NDP是IPv6中非常核心的组件，其主要功能如下：




2.6、NDP使用以下几种ICMPv6报文：
2.6.1、RS【Router Solicitation】：路由器请求报文
2.6.2、RA【Router Advertisement】：路由器通告报文
2.6.3、NS【Neighbor Solicitation】：邻居请求报文
2.6.4、NA【Neighbor Advertisement】：邻居通告报文

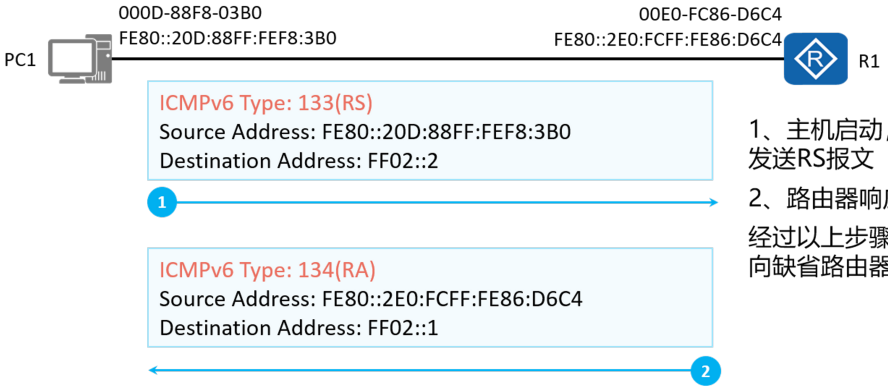
| 功能 \ ICMPv6报文 | RS 133 | RA 134 | NS 135 | NA 136 | 重定向 137 |
|---|---|---|---|---|---|
| 地址解析 | | | • | • | |
| 路由器发现 | • | • | | | |
| 前缀重编址 | • | • | | | |
| 重复地址检测 | | | • | • | |
| 重定向 | | | | | • |

2.7、路由器发现
2.7.1、路由器发现是指主机发现本地链路上路由器和确定其配置信息的过程
2.7.2、路由器发现可以同时实现以下三个功能：
a、路由器发现【Router Discovery】：主机定位邻居路由器以及选择哪一个路由器作为缺省网关的过程
b、前缀发现【Prefix Discovery】：主机发现本地链路上的一组IPv6前缀的过程，用于主机的地址自动配置
c、参数发现【Parameter Discovery】：主机发现相关操作参数的过程，如输出报文的缺省跳数限制、地址配置方式等信息

2.7.3、使用报文：
a、RS【路由器请求】
b、RA【路由器通告】

2.7.4、协议交互主要有两种情况：
a、主机发送RS触发路由器回应RA
b、路由器周期发送RA

2.8、路由器发现流程 — 主机请求触发
当主机启动时，主机会向本地链路范围内所有的路由器发送RS报文，触发路由器响应RA报文。主机发现本地链路上的路由器后，自动配置缺省路由器，建立缺省路由表、前缀列表和设置其它的配置参数




1、主机启动，向本地链路范围内所有的路由器发送RS报文

2、路由器响应RA报文

经过以上步骤，主机生成缺省路由，下一跳指向缺省路由器的链路本地地址

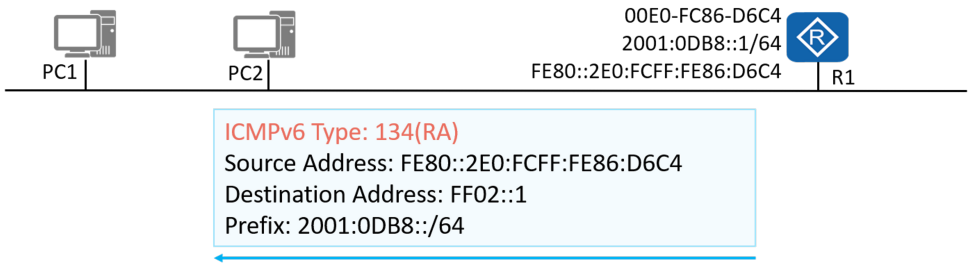
2.9、路由器发现流程 — 路由器周期性发送

2.9.1、路由器周期性的发送RA报文，RA发送间隔是一个有范围的随机值，缺省的最大时间间隔是600秒，最小时间间隔是200秒

2.9.2、对于定期发送的RA报文，其地址有如下要求：

a、Source Address：必须是发送接口的链路本地地址

b、Destination Address ： FF02::1




2.10、地址解析

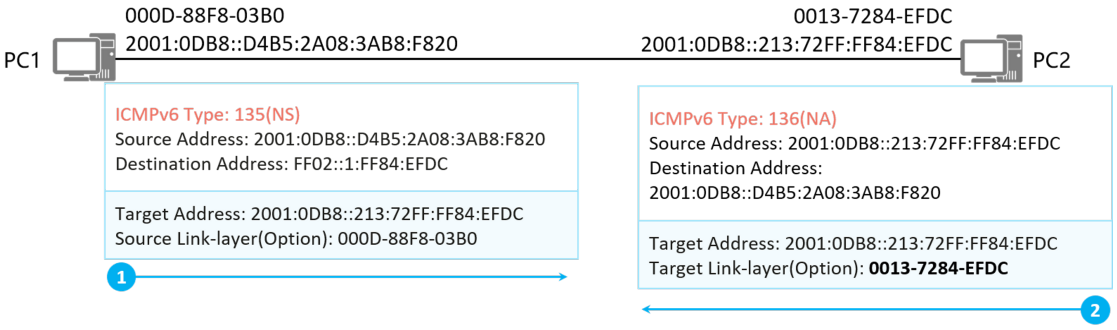
2.10.1、IPv6地址解析通过ICMPv6【NS和NA报文】来实现

2.10.2、在三层完成地址解析，主要带来以下几个好处：

a、地址解析在三层完成，不同的二层介质可以采用相同的地址解析协议

b、可以使用三层的安全机制避免地址解析攻击

c、使用组播方式发送请求报文，减少了二层网络的性能压力

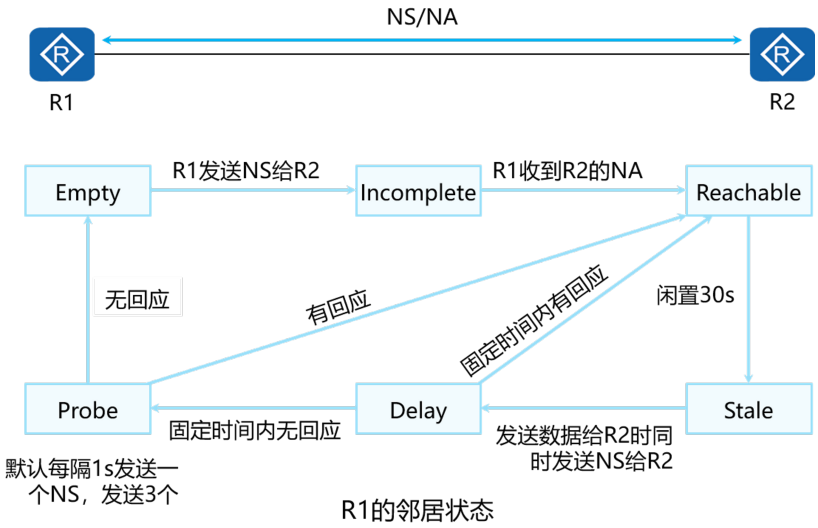



2.11、IPv6的邻居状态

2.11.1、IPv6节点需要维护一张邻居表，每个邻居都有相应的状态，状态之间可以迁移

2.11.2、5种邻居状态分别是：未完成【Incomplete】、可达【Reachable】、陈旧【Stale】、延迟【Delay】、探查【Probe】

| 状态 | 描述 |
| --- | --- |
| Incomplete | 邻居不可达。正在进行地址解析，邻居的链路层地址未探测到，如果解析成功，则进入Reachable状态 |
| Reachable | 邻居可达。表示在规定时间（邻居可达时间，缺省情况下是30秒）内邻居可达。如果超过规定时间，该表项没有被使用，则表项进入Stale状态 |
| Stale | 邻居是否可达未知。表明该表项在规定时间（邻居可达时间，缺省情况下是30秒）内没有被使用。此时除非有发送到邻居的报文，否则不对邻居是否可达进行探测 |
| Delay | 邻居是否可达未知。已向邻居发送报文，如果在指定时间内没有收到响应，则进入Probe状态 |
| Probe | 邻居是否可达未知。已向邻居发送NS报文，探测邻居是否可达。在规定时间内收到NA报文回复，则进入Reachable状态；否则进入Incomplete状态 |

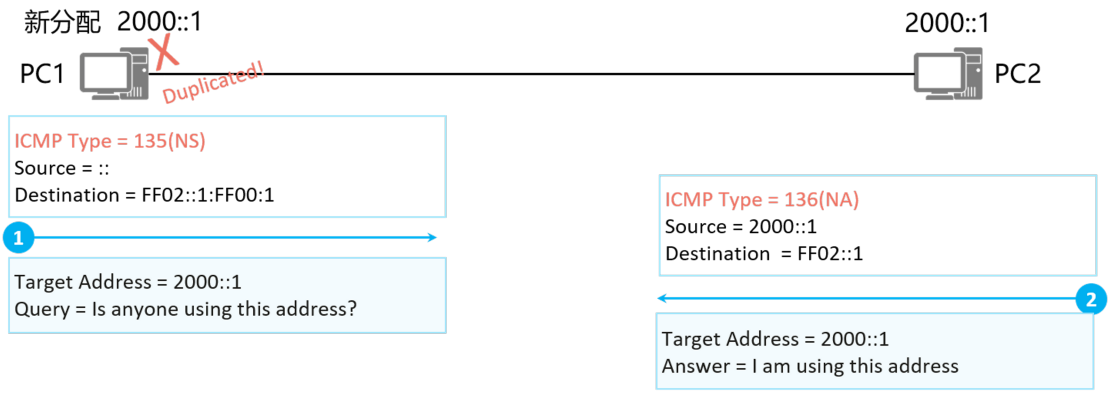


R1的邻居状态

2.12、重复地址检测

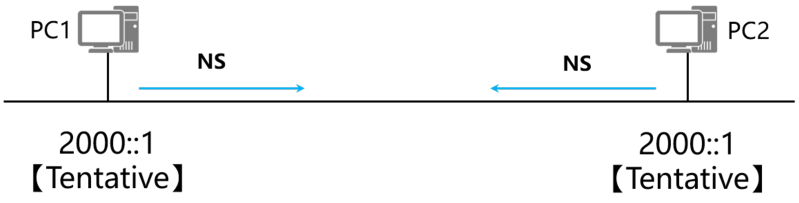
2.12.1、重复地址检测【Duplicate Address Detect | DAD】是指接口在使用某个IPv6地址之前，需要先探测是否有其它的节点使用了该地址，从而确保网络中没有两个相同的单播地址

2.12.2、接口在启用任何一个单播IPv6地址前都需要先进行DAD，包括Link-Local地址



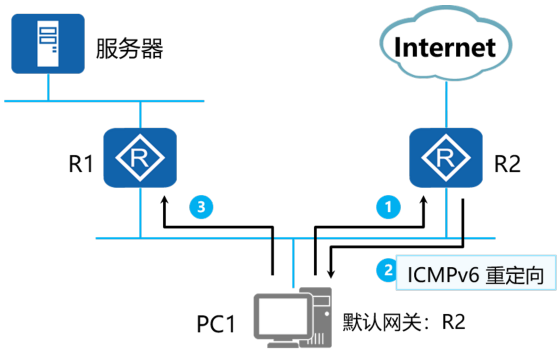

2.12.3、一个地址在通过重复地址检测之前称为【tentative地址 | 试验地址】，此时该接口不能使用这个试验地址进行单播通讯

2.12.4、若2个节点配置相同地址，同时作重复地址检测时，当一方收到对方发出的DAD NS报文，则接收方将不启用该地址



2.13、重定向

重定向是指网关设备发现报文从其它网关设备转发更优，它就会发送重定向报文告知报文的发送者，让报文发送者选择另一个网关设备




2.13.1、PC1希望发送报文到服务器，于是根据配置的默认网关地址向网关R2发送报文

2.13.2、网关R2收到报文后，检查报文信息，发现报文应该转发到与PC1在同一网段的另一个网关设备R1，此转发路径是更优的路径，于是R2会向PC1发送一个重定向消息，通知PC1去往服务器的报文应直接发给R1

2.13.3、PC1收到重定向消息后，会向R1发送报文，R1再将该报文转发至服务器

3、站点本地地址 —— 相当于IPv4中的私有地址

3.1、该地址不会被路由至公网

3.2、前缀为FEC0::/10

3.3、用于打印机，交换机等的管理地址

3.4、在IPv6大规模实现时，站点本地地址将不复使用


4、特殊IPv6地址

4.1、【::】相当于IPv4中的0.0.0.0

4.2、【::1】标识一个环回接口，相当于IPv4的127.0.0.1

5、兼容地址

5.1、与IPv4兼容的地址，【0:0:0:0:0:0:w.x.y.z】或【::w.x.y.z】

5.2、IPv4映射地址，【0:0:0:0:0:FFFF:w.x.y.z】或【::FFFF:w.x.y.z】

以上【6to4】地址用于IPv4的网络上传送IPv6的包

十四、IPv6的组播地址

1、组播的特点

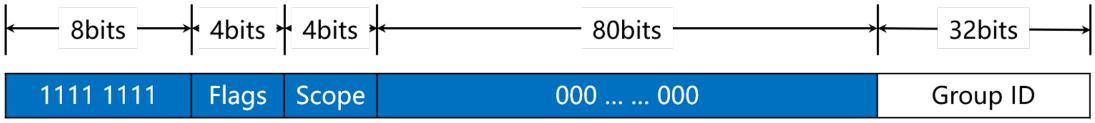
1.1、任意节点均可成为一个组播组的成员

1.2、一个源节点可以发送数据包到组播组

1.3、组播组的所有成员收到发往该组的数据包

1.4、组播地址在IPv6包中不能用作源地址或出现在任何选路头中

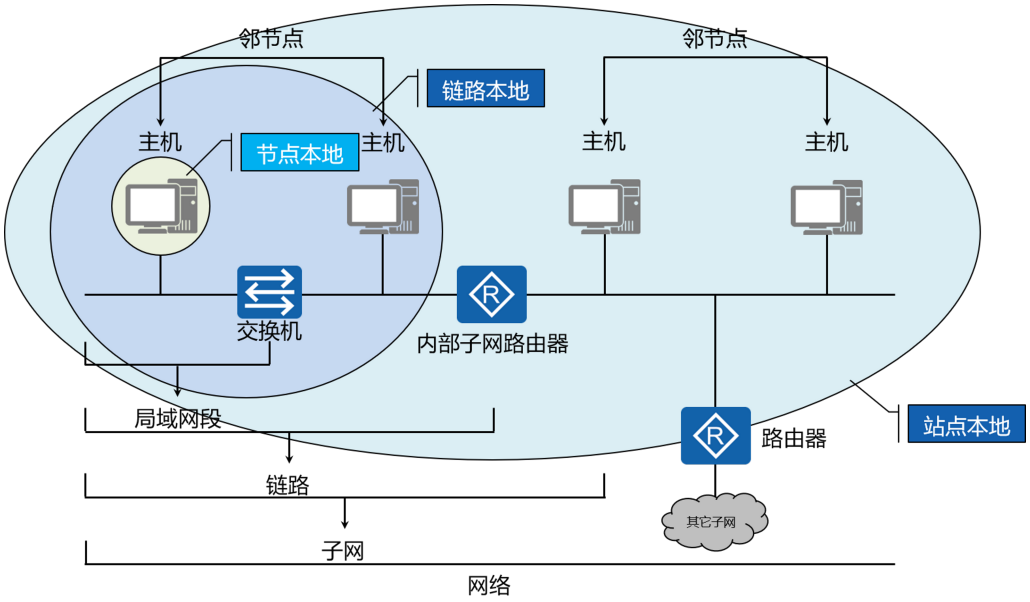
2、组播地址结构




2.1、IPv6组播地址其最高位前8位为1

2.2、标记【Flags】字段为四位，目前只用了最后一位；此位为0，则表示是一个永久组播地址，若为1，则表示是一个临时组播地址

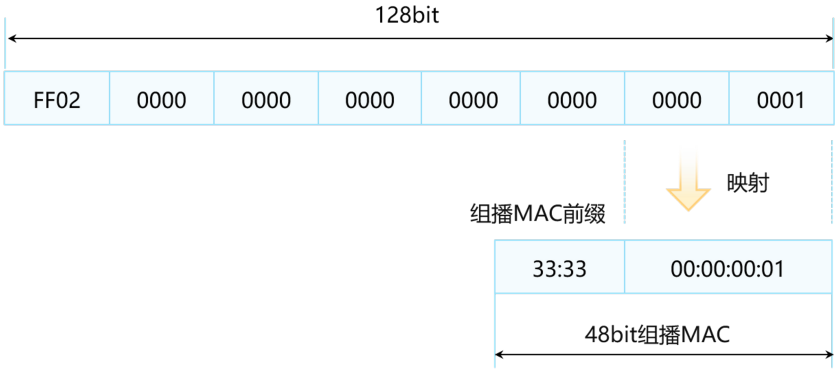
2.3、范围【Scope】字段为四位，其设置为0则表示【预留】；设置为1则表示【节点本地范围】；设置为2则表示【本地链路范围】；设置为5则表示【本地站点范围】；设置为8则表示【组织本地范围】；设置为E则表示【全球范围】；设置为F则表示【预留】




2.4、IPv6组播MAC地址

2.4.1、组播IPv6报文的目的IP为组播IPv6地址，同样，目的MAC为组播MAC地址

2.4.2、组播MAC的前16bit为“33:33”，是专门为IPv6组播预留的MAC地址前缀。后32bit从组播IPv6地址的后32bit直接映射而来




十五、IPv6的任播地址

1、任播地址是IPv6特有的地址类型，它用来标识一组网络接口

2、任播地址标识一组网络接口【通常属于不同的节点】

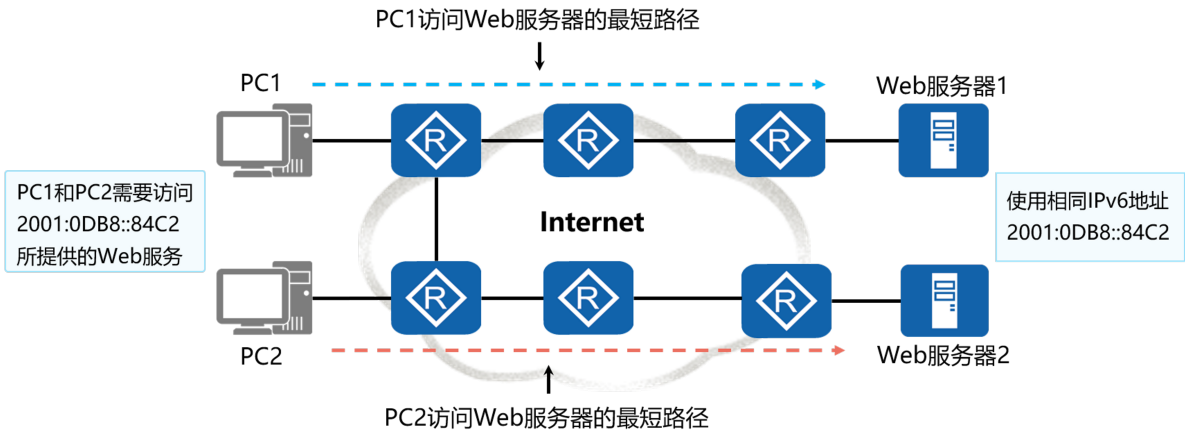
3、任播地址可以作为IPv6报文的源地址，也可以作为目的地址

4、任播过程涉及一个任播报文发起方和一个或多个响应方

5、任播报文的发起方通常为请求某一服务【Web服务】的主机

6、任播地址与单播地址在格式上无任何差异，唯一的区别是一台设备可以给多台具有相同地址的设备发送报文

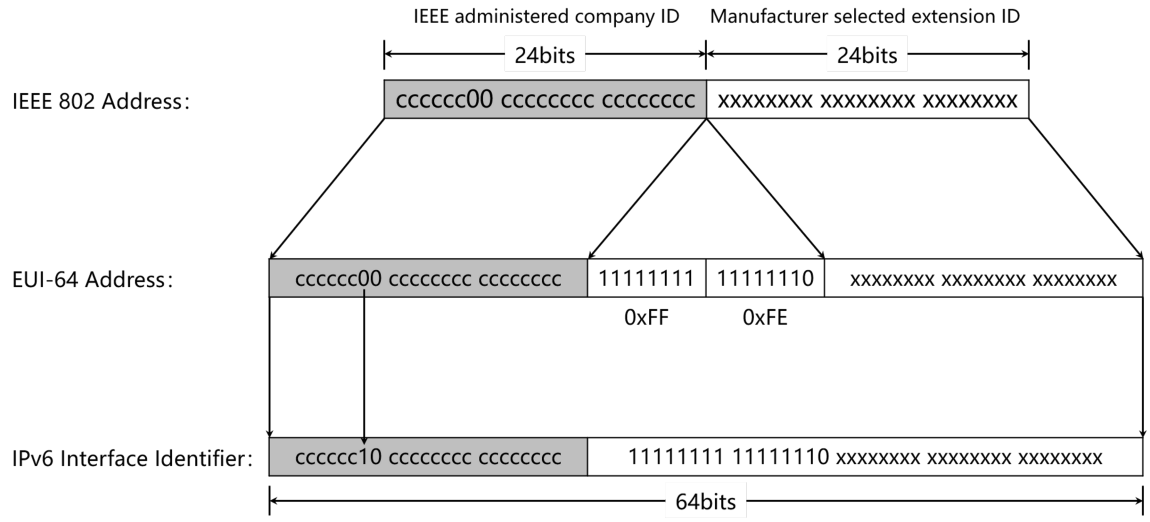
7、任播的优势：提高业务冗余性、提升客户服务体验



十六、IPv6的接口标识

三种方式可以生成IPv6的接口标识：

1、由扩展唯一标识符EUI-64派生出来的64位接口标识符




1.1、首先将MAC一分为二

1.2、在中间填入0xFF 0xFE，得到EUI-64

1.3、将U/L位取反（由0变成1），最后得到IPv6接口标识符

注：全局/本地【Unit/Local】位是第一个字节的第7位，用于确定该地址是【全局管理】还是【本地管理】。若将U/L位置为0，则代表其通过分配唯一的公司ID，IEEE已对地址进行管理；若U/L位被置为1，则表示该地址为本地管理

2、采用随机生成的方法产生一个接口ID，目前Windows操作系统使用该方式

3、人为手工指定接口ID来实现

十七、IPv6的发展与实施部署

1、IPv6的发展

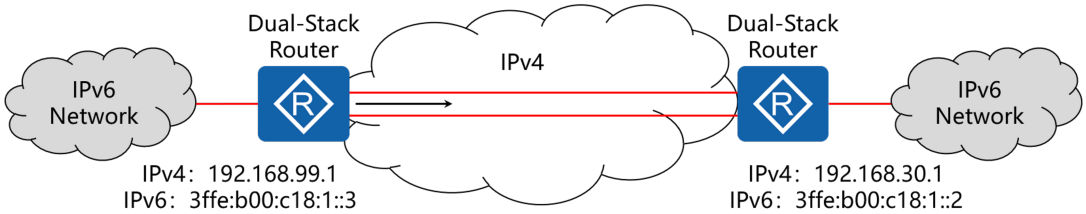
1.1、IPv4为主导协议，IPv6为孤岛协议

1.2、IPv4与IPv6并存

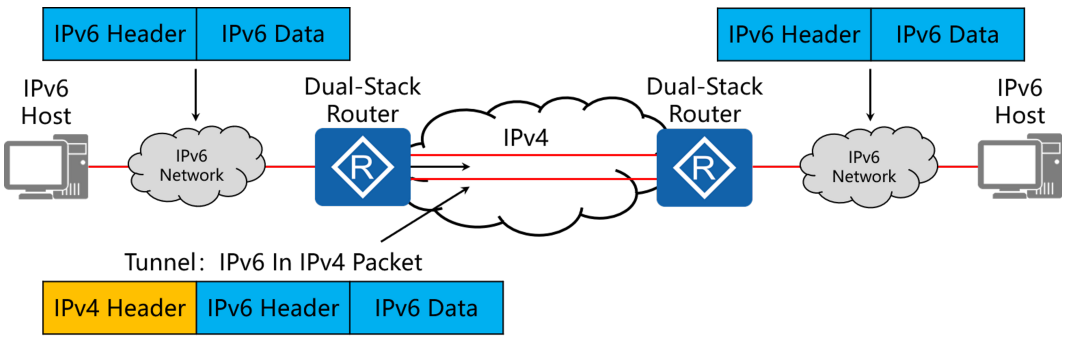
1.3、IPv6全面取代IPv4

十八、IPv4向IPv6过渡时期的过渡性技术

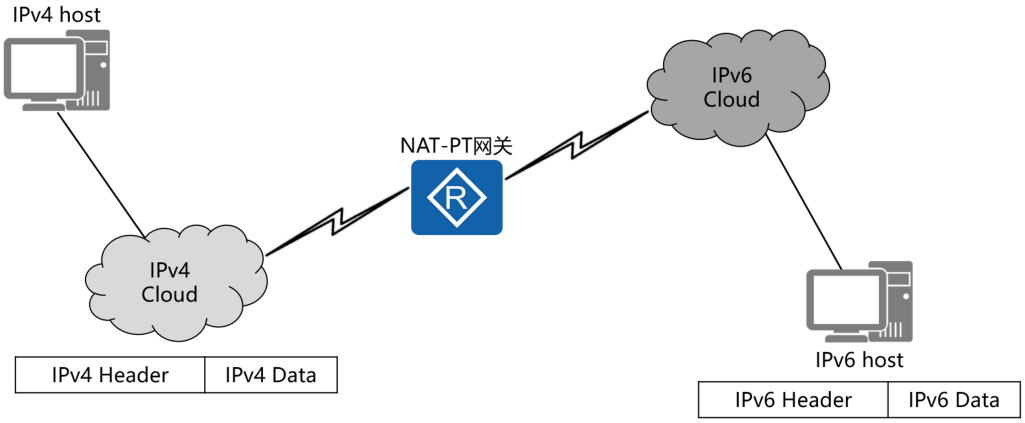
1、双协议栈




2、隧道【Tunnel】



3、网络地址转换【NAT】




十九、IPv6的配置

详细配置见实验手册