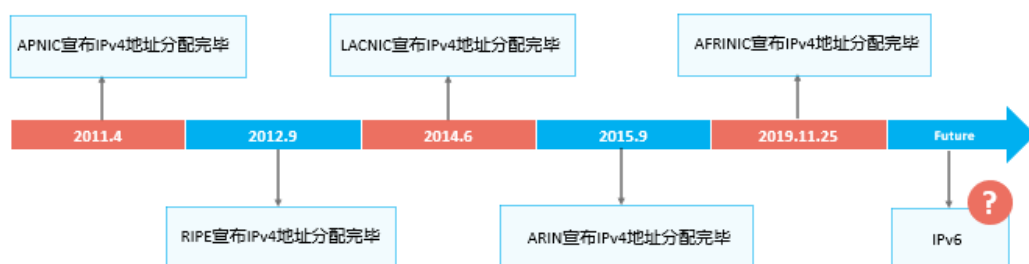


IPv6 概述

- IPv4 协议是目前广泛部署的因特网协议。在因特网发展初期，IPv4 以其协议简单、易于实现、互操作性好的优势而得到快速发展。但随着因特网的迅猛发展，IPv4 设计的不足也日益明显，IPv6 的出现，解决了 IPv4 的一些弊端。
- IPv6 (Internet Protocol Version 6) 也被称为 IPng (IP Next Generation)。它是 Internet 工程任务组 IETF (Internet Engineering Task Force) 设计的一套规范，是 IPv4 (Internet Protocol Version 4) 的升级版本。
- 本课程将介绍 IPv6 的基本概念、IPv6 地址分类、IPv6 报文格式等。

IPv4现状

2011年2月3日，IANA (Internet Assigned Numbers Authority, 因特网地址分配组织) 宣布将其最后的 468万个IPv4地址平均分配到全球5个RIR (Regional Internet Registry, 区域互联网注册管理机构)，此后IANA再没有可分配的IPv4地址。



- IANA，是负责全球互联网 IP 地址编号分配的机构。IANA 将部分 IPv4 地址分配给大洲级的 RIR，再由各 RIR 进行所辖区域内地址分配，五大 RIR 包括：
 - RIPE：Reseaux IP Europeans，欧洲 IP 地址注册中心，服务于欧洲、中东地区和中亚地区；
 - LACNIC：Latin American and Caribbean Internet Address Registry，拉丁美洲和加勒比海 Internet 地址注册中心，

服务于中美、南美以及加勒比海地区；

- ARIN : American Registry for Internet Numbers , 美国 Internet 编号注册中心 , 服务于北美地区和部分加勒比海地区 ;
- AFRINIC : Africa Network Information Centre , 非洲网络信息中心 , 服务于非洲地区 ;
- APNIC : Asia Pacific Network Information Centre , 亚太互连网络信息中心 , 服务于亚洲和太平洋地区。
- 实践证明 IPv4 是一个非常成功的协议 , 它本身也经受住了 Internet 从少量计算机组网发展到目前上亿台计算机互联的考验。但该协议是几十年前基于当时的网络规模而设计的。在今天看来 , IPv4 的设计者们对于 Internet 的估计和预想显得很不够充分。随着 Internet 的扩张和新应用的不断推出 , IPv4 越来越显示出它的局限性。
- Internet 规模的快速扩张是当时完全没有预料到的 , 特别是近十年来 , 更是爆炸式增长 , 已经走进了千家万户 , 人们的日常生活已经离不开它。但正因为发展太快 , IP 地址空间耗尽的问题迫在眉睫。
- 20 世纪 90 年代 , IETF 推出 NAT (Network Address Translation , 网络地址转换) 与 CIDR (Classless Inter Domain Routing , 无类别域间路由) 等技术来推迟 IPv4 地址耗尽发生的时间点。但是这些过渡方案只能减缓地址枯竭的速度 , 并不能从根本上解决问题。



全球IPv6发展现状

全球IPv6部署率显著增长

截止到2019年10月，综合IPv6部署率
在30%以上的国家或地区占了全球地图面积
一半以上

全球IPv6用户数量猛增

根据Google网站监测，至2019年9月，
使用IPv6访问Google网站的用户占总用户最高
已超过30%
相比2018年涨幅**35.3%**

主流软件、服务IPv6支持度提高

- 截止到2019年10月10日，全球所有网站中有14.6%的网站支持IPv6访问，排名前100万的网站中有19.2%，排名前1000的网站IPv6支持率接近30%。
- 全球主要的云服务商和CDN运营商Cloudflare、阿卡迈、微软云服务、亚马逊云服务等均已支持IPv6。
- 面向大众用户的操作系统Windows、MacOS已支持IPv6。

全球网络及域名系统IPv6部署情况

截至2019年10月，在全球1527个顶级域中，有1505个支持IPv6，
占总量的**98.6%**

- 数据来源：《2019 IPv6 支持度报告》——下一代互联网国家工程中心
- 综合 IPv6 部署率是根据各个国家地区的网络（IPv6 Prefix/Transit IPv6 AS），IPv6 网站及 IPv6 用户等数据按照一定权值并计算得出的 IPv6 部署综合情况。



Why IPv6 ?

IPv4



公网地址枯竭
包头设计不合理
路由表过大，查表效率低
对ARP的依赖，导致广播泛滥
.....

VS

IPv6



“无限”地址
地址层次化分配
即插即用
简化的报文头部
IPv6安全特性
保证端到端通信完整性
对移动性的支持
增强的QoS特性
.....



IPv6优势

“无限”地址空间

地址长度为128bit，海量的地址空间，满足物联网等新兴业务、有利于业务演进及扩展。

层次化的地址结构

相较于IPv4地址，IPv6地址的分配更加规范，利于路由聚合（缩减IPv6路由表规模）、路由快速查询。

即插即用

IPv6支持无状态地址自动配置（SLAAC），终端接入更简单。

简化的报文头部

简化报文头，提高效率；通过扩展包头支持新应用，利于路由器等网络设备的转发处理，降低投资成本。

安全特性

IPsec、真实源地址认证等保证端到端安全；避免NAT破坏端到端通信的完整性。

移动性

对移动网络实时通信有较大改进，整个移动网络性能有比较大的提升。

增强的QoS特性

额外定义了流标签字段，可为应用程序或者终端所用，针对特殊的服务和数据流，分配特定的资源。

- 近乎无限的地址空间：与 IPv4 相比，这是最明显的好处。IPv6 地址是由 128 bit 构成，单从数量级来说，IPv6 所拥有的地址容量是 IPv4 的约 8×10^{28} 倍，号称可以为全世界的每一粒沙分配一个网络地址。这使得海量终端同时在线，统一编址管理，变为可能，为万物互连提供了强有力的支撑。
- 层次化的地址结构：正因为有了近乎无限的地址空间，IPv6 在地址规划时就根据使用场景划分了各种地址段。同时严格要求单播 IPv6 地址段的连续性，便于 IPv6 路由聚合，缩小 IPv6 地址表规模。
- 即插即用：任何主机或者终端要获取网络资源，传输数据，都必须有明确的 IP 地址。传统的分配 IP 地址方式是手工或者 DHCP 自动获取，除了上述两个方式外，IPv6 还支持 SLAAC（Stateless Address Autoconfiguration，无状态地址自动配置）。
- 端到端网络的完整性：大面积使用 NAT 技术的 IPv4 网络，从根本上破坏了端到端连接的完整性。使用 IPv6 之后，将不再需要 NAT 网络设备，上网行为管理、网络监管等将变得简单，与此同时，应用程序也不需要开发复杂的 NAT 适配代码。

- 安全性得到增强：IPsec (Internet Protocol Security , 因特网协议安全协议) 最初是为 IPv6 设计的，所以基于 IPv6 的各种协议报文 (路由协议、邻居发现等) ，都可以端到端地加密，当然该功能目前应用并不多。而 IPv6 的数据面报文安全性，跟 IPv4+IPsec 的能力，基本相同。
- 可扩展性强：IPv6 的扩展属性报文头部，并不是主数据包的一部分，但是在必要的时候，这些扩展头部会插在 IPv6 基本头部和有效载荷之间，能够协助 IPv6 完成加密功能、移动功能、最优路径选路、QoS 等，并可提高报文转发效率。
- 移动性改善：当一个用户从一个网段移动到另外一个网段，传统的网络会产生经典式“三角式路由”，IPv6 网络中，这种移动设备的通信，可不再经过原“三角式路由”，而做直接路由转发，降低了流量转发的成本，提升了网络性能和可靠性。
- QoS 可得到进一步增强：IPv6 保留了 IPv4 所有的 QoS 属性，额外定义了 20Byte 的流标签字段，可为应用程序或者终端所用，针对特殊的服务和数据流，分配特定的资源，目前该机制并没有得到充分的开发和应用。
-

IPv6 过渡技术简介 (1)

- 由于 NAT 技术的应用，缓解了 IPv4 地址不足产生的问题，但是部署 IPv6 是解决 IPv4 地址不足的最终方案。当前世界上不同地区对部署 IPv6 的需求强烈程度不一，且当前 IPv4 网络仍然占主流地位，因此短时间内 IPv6 和 IPv4 将会共存。
- IPv4 网络演变为 IPv6 网络主要有以下三种技术：
- 双栈技术：在一台设备上同时启用 IPv4 协议栈和 IPv6 协议栈的技术。
- 隧道技术：将一种协议的数据封装在另一种协议中的技术。
- 转换技术：将 IPv6 地址和 IPv4 地址进行转换的一种技

术。

- 没有最好的过渡技术方案，没有任何一种技术方案能够解决所有问题，通常是多种技术组合成不同的过渡方案，满足不同的网络访问场景。

IPv6现状

IPv6优势

IPv6过渡技术

IPv6路由

IPv6过渡技术简介 (2)

IPv4/IPv6双栈

隧道技术

转换技术

- 设备支持IPv4/IPv6，IPv4及IPv6在网络中独立部署，在一段时间内并存，对现有IPv4业务影响较小。
- 演进方案相对简单、易理解，网络规划设计工作量相对更少。
- 现有软硬件（网络设备、终端、操作系统等）已经有很大一部分支持双栈，甚至默认使能IPv6，可直接使用。
- 对设备的硬件/软件有要求，设备需支持双栈。

- 将IPv4流量封装在IPv6隧道中，或者将IPv6流量封装在IPv4隧道中。
- 适用于在IPv4传输网络中实现IPv6孤岛之间的互通，或者在IPv6传输网络中实现IPv4孤岛之间的互通。
- 部署隧道技术的设备（一般是隧道端点）需支持双栈及相应的隧道技术。
- 仅适用于实现孤岛互通的临时状态，并不适用于长期、稳定的业务形态。

- 将IPv4流量转换成IPv6（主要是IP头部的改写），反之亦然。
- 适用于纯IPv4网络与纯IPv6网络之间的通信，反之亦然。
- 破坏了端到端连接的完整性，需针对特殊应用提供ALG功能。
- 网络管理/审计变得复杂。
- 需在网络中部署网络层协议转换（NAT）设备、DNS设备。

IPv6 Host

双栈设备

双栈设备

IPv6

IPv4

IPv4 Host

IPv6 data

IPv4 data

IPv6

IPv4

IPv6 Over IPv4 Tunnel

IPv6

IPv6

NAT64

IPv4

DNS64

IPv6 data

IPv4 data

IPv6现状

IPv6优势

IPv6过渡技术

IPv6路由

IPv6路由协议简介

OSPFv3

IS-IS for IPv6

BGP4+

PIM

1. 基于链路运行，单链路支持多实例。
2. 取消LSA头部IP地址信息，实现与网络层协议解耦。
3. LSA内新定义泛洪范围字段，支持未知LSA的处理。
4. 新增LSA支持IPv6路由发布。

1. 不是新协议或新版本，仅是原有协议上做了简单扩展，IS-IS路由器和IS-IS路由器可以实现互通。
2. 新增1种NLPIID（网络层协议标识）宣告自身支持IPv6。
3. 新增2种TLV，支持宣告IPv6网络可达性和接口IPv6地址信息。

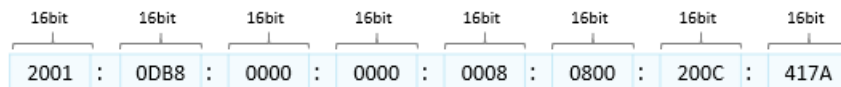
1. 不是新协议或新版本，只需在MP-BGP（BGP多协议）架构上支持IPv6地址族，BGP4+路由器和BGP4路由器可以实现互通。
2. 新增2种NLRI（网络层可达信息），支持发布IPv6可达路由及下一跳信息，支持撤销不可达路由。

1. PIM协议本义即为协议无关组播，PIM真正版本号仍为PIMv2。
2. 唯一区别在于协议报文地址及组播数据报文地址均使用IPv6地址。

版本未变，简单扩展

IPv6地址

- IPv6地址的长度为128bit。一般用冒号分割为8段，每一段16bit，每一段内用十六进制表示。



IPv6地址中的字母大小写不敏感，例如A等同于a。

- 与IPv4地址类似，IPv6也用“IPv6地址/掩码长度”的方式来表示IPv6地址。

IPv6地址： 2001:0DB8:2345:CD30:1230:4567:89AB:CDEF/64

地址空间

- 为什么IPv6协议的地址长度是128bit？
 - CPU处理字长发展至今分别经历了4bit、8bit、16bit、32bit、64bit等，当数据能用2的指数幂字长的二进制数表示时，CPU对数值的处理效率最高。
 - IPv4地址长度为32bit，原因之一就是当时互联网上的主机CPU字长为32bit。从处理效率和未来网络扩展性上考虑，将IPv6的地址长度定为128bit是十分合适的。
- IPv6的128bit地址是一个什么概念？
 - IPv4有 $(2^{32}) = 4,294,967,296$ 个地址。
 - IPv6有 $(2^{128} = 2^{96} \times 2^{32}) = 340,282,366,920,938,463,463,374,607,431,768,211,456$ 个地址(340万亿万亿万亿个地址)，相当于地球表面每平方米可以分配到67万亿个地址。
 - 夸张的说，地球上每一粒沙子都可以分配到一个IPv6地址。

IPv6地址格式

IPv6地址格式

首选格式

- 冒号分割为8段，每一段16bit，每一段内用十六进制表示。
- 用“IPv6地址/掩码长度”的方式来表示。
- 例如：2001:0DB8:0000:0001:0000:0000:0000:45ff/64。

压缩格式

- 每段前导0可以省略，但是如果该段为全0，则至少保留一个“0”字符；拖尾的0不能被省略。
- 一个或多个连续的段为全0时，可用“::”表示，整个IPv6地址缩写中只允许有一个“::”。
- 例如：2001:DB8:0:1::45ff/64。

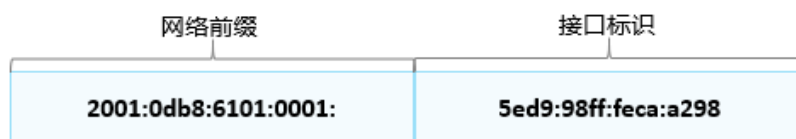
内嵌IPv4地址的格式

- 地址的前96bit为IPv6地址格式，后32bit为IPv4地址格式。
- IPv6部分可采用首选或压缩格式，IPv4部分采用点分十进制格式。
- 例如：0:0:0:0:0:0:166.168.1.2/64。

- IPv4 地址使用点隔开的 4 段十进制数加上掩码来表示，例如 192.168.1.1/24。IPv6 的地址有 128 位，沿用 IPv4 的十进制表示方法就显得太笨拙了，所以在 RFC2373 中定义了不同于 IPv4 的格式。

IPv6地址结构

- 一个IPv6地址可以分为如下两部分：
 - 网络前缀：nbit，相当于IPv4地址中的网络ID。
 - 接口标识：(128-n) bit，相当于IPv4地址中的主机ID。
- IPv6单播地址示例：2001:0db8:6101:0001:5ed9:98ff:fece:a298/64。



IPv6地址前缀

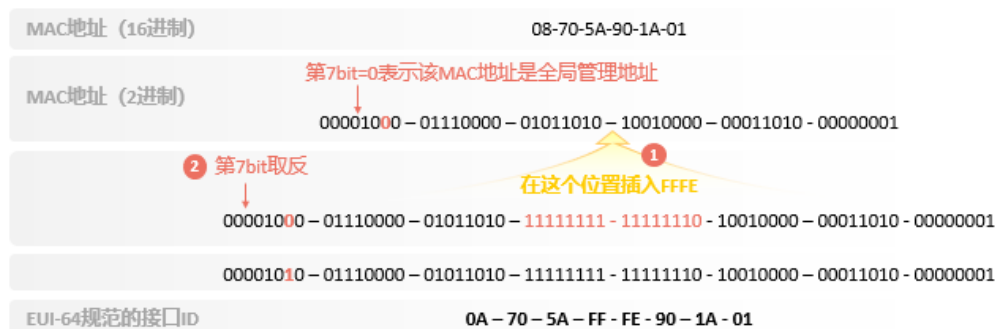
- 鉴于IPv4地址在规划和分配上的局限性，IETF对IPv6地址类型进行了精细划分，不同类型的IPv6地址被赋予了不同的前缀，且受地址分配机构的严格管理。
- 现阶段，常用的IPv6地址或前缀有：

IPv6地址或前缀	含义
2001::/16	用于IPv6 Internet，类似于IPv4公网地址
2002::/16	用于6to4隧道
FE80::/10	链路本地地址前缀，用于本地链路范围内的通信
FF00::/8	组播地址前缀，用于IPv6组播
::/128	未指定地址，类似于IPv4中的0.0.0.0
::1/128	环回地址，类似于IPv4中的127.0.0.1
...	...

- IPv6 前缀 IANA 最新定义

IPv6地址接口标识

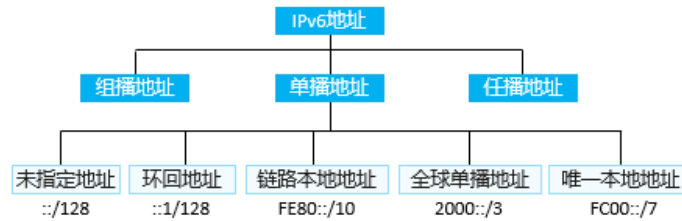
- 接口ID可通过三种方式生成：手工配置、系统自动生成，或基于IEEE EUI-64规范生成。
- 其中，基于IEEE EUI-64规范自动生成接口ID的方式最为常用，该方式将接口的MAC地址转换为IPv6接口标识。



- 目前有三种方式可以产生 IPv6 接口 ID：
- IEEE EUI-64 规范
- 接口 ID 的典型长度是 64 位，IEEE EUI-64 规范给出了一个由 48 位 MAC 地址自动生成 64 位 Interface ID 的方法。
- 具体的转换算法为：将上述的第 7bit0 转换为 1，在 MAC 地址的中间（24bit 处）插入两个字节：FFFE。
- 这种由 MAC 地址产生 IPv6 地址接口 ID 的方法可以减少配置的工作量，只需要获取一个 IPv6 前缀就可以与接口 ID 形成 IPv6 地址。
- 使用这种方式最大的缺点就是某些恶意者可以通过二层 MAC 推算出三层 IPv6 地址。
- 设备随机生成
- 设备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。
- 手动配置
- 顾名思义，手动配置就是人为指定接口 ID 来实现。



IPv6地址类型



- **单播地址 (Unicast Address)**：标识一个接口，目的地址为单播地址的报文会被送到被标识的接口。在IPv6中，一个接口拥有多个IPv6地址是非常常见的现象。
- **组播地址 (Multicast Address)**：标识多个接口，目的地址为组播地址的报文会被送到被标识的所有接口。只有加入相应组播组的设备接口才会侦听发往该组播地址的报文。
- **任播地址 (Anycast Address)**：任播地址标识一组网络接口（通常属于不同的节点）。目标地址是任播地址的数据包将发送给其中路由意义上最近的一个网络接口。
- IPv6没有定义广播地址 (Broadcast Address)



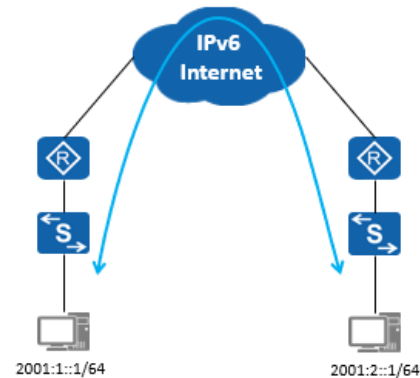
IPv6常见单播地址 - GUA

IPv6单播地址 IPv6组播地址 IPv6任播地址

GUA (Global Unicast Address, 全球单播地址)，也被称为可聚合全球单播地址。该类地址全球唯一，用于需要有互联网访问需求的主机，相当于IPv4的公网地址。



- 全局路由前缀：由提供商指定给一个组织机构，一般至少为48bit。
- 子网ID：组织机构根据自身网络需求划分子网。
- 接口标识：用来标识一个设备的接口。



- 可以向运营商申请 GUA 或者直接向所在地区的 IPv6 地址管理机构申请。

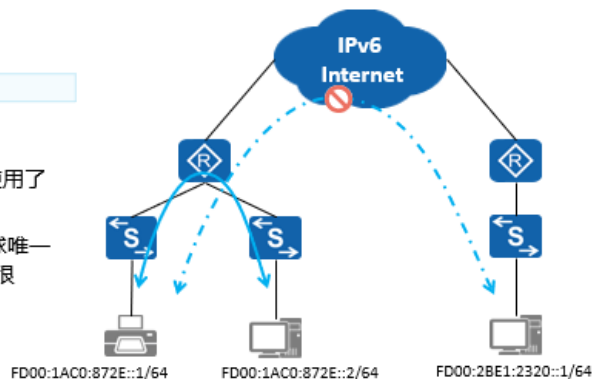


IPv6常见单播地址 - ULA

ULA (Unique Local Address, 唯一本地地址) 是IPv6私网地址, 只能够在内网中使用。该地址空间在IPv6公网中不可被路由, 因此不能直接访问公网。

8bit	40bit	16bit	64bit
1111 1101	Global ID	子网ID	接口标识
随机产生			

- 唯一本地地址使用FC00::/7地址块, 目前仅使用了FD00::/8地址段。FC00::/8预留为以后拓展用。
- ULA虽然只在有限范围内有效, 但也具有全球唯一的前缀 (虽然随机方式产生, 但是冲突概率很低)。

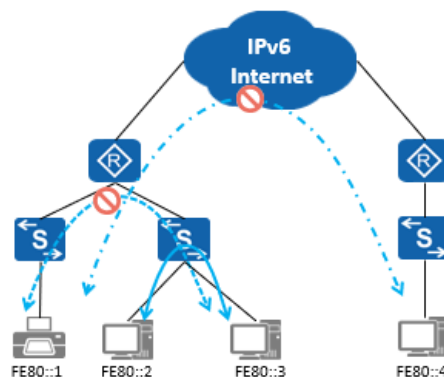


IPv6常见单播地址 - LLA

LLA (Link-Local Address, 链路本地地址) 是IPv6中另一种应用范围受限制的地址类型。LLA的有效范围是本地链路, 前缀为FE80::/10。

10bit	54bit	64bit
1111 1101 0	0	接口标识
固定为0		

- LLA用于一条单一链路层面的通信, 例如IPv6地址无状态自动配置、IPv6邻居发现等。
- 源或目的IPv6地址为链路本地地址的数据包将不会被转发到始发的链路之外, 换句话说, 链路本地地址的有效范围为本地链路。
- 每一个IPv6接口都必须具备一个链路本地地址。华为设备支持自动生成和手工指定两种配置方式。





IPv6组播地址

IPv6组播地址标识某个组，目的为组播地址的报文会被送到该组播组内的成员。组播地址由前缀（FF::/8），标志（Flag）字段、范围（Scope）字段以及组播组ID（Group ID）4个部分组成。

8bit	4bit	4bit	80bit	32bit
11111111	Flags	Scope	Reserved (必须为0)	Group ID

- Flags

- 用来表示永久或临时组播地址
 - 0000表示永久组播地址
 - 0001表示临时组播地址

- Scope

- 表示组播组的范围

- Group ID

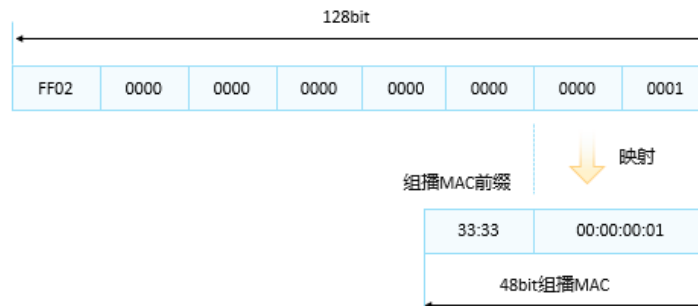
- 组播组ID

0: 预留;
 1: 节点本地范围; 单个接口有效, 仅用于Loopback通讯;
 2: 链路本地范围; 例如FF02::1
 5: 站点本地范围;
 8: 组织本地范围;
 E: 全球范围;
 F: 预留。



IPv6组播MAC

- 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。
- 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。



- 以太网传输单播IP报文的时候，目的MAC地址是下一跳的MAC地址。但是在传输组播数据包时，其目的地不再是一个具体的接收者，而是一个成员不确定的组，所以要使用组播MAC地址。

- IPv4组播MAC地址

- IANA规定，IPv4组播MAC地址的高24bit为0x01005E，第25bit为0，低23bit为IPv4组播地址的低23bit映射。

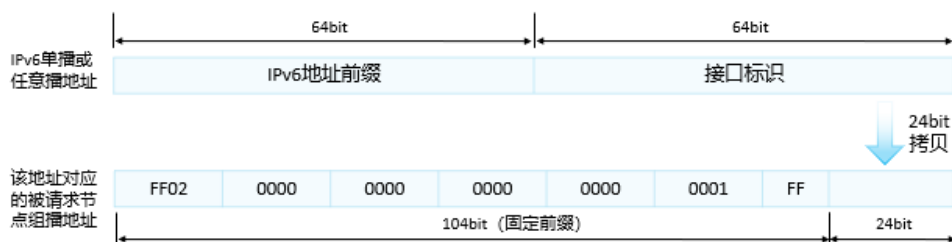
- 由于IPv4组播地址的高4bit是1110，代表组播标识，而低28bit中只有23bit被映射到IPv4组播MAC地址，这样I

Pv4 组播地址中就有 5bit 信息丢失。于是，就有 32 个 IPv4 组播地址映射到了同一个 IPv4 组播 MAC 地址上，因此在二层处理过程中，设备可能要接收一些本 IPv4 组播组以外的组播数据，而这些多余的组播数据就需要上层进行过滤了。

- IPv6 组播 MAC 地址
- 在以太网链路上发送 IPv6 组播数据包时，对应的 MAC 地址是 0x3333-A-A-A-A，其中 A-A-A-A 是组播 IP 地址的后 32bit 的直接映射。

被请求节点组播地址

当一个节点具有了单播或任播地址，就会对应生成一个被请求节点组播地址，并且加入这个组播组。该地址主要用于邻居发现机制和地址重复检测功能。被请求节点组播地址的有效范围为本地链路范围。

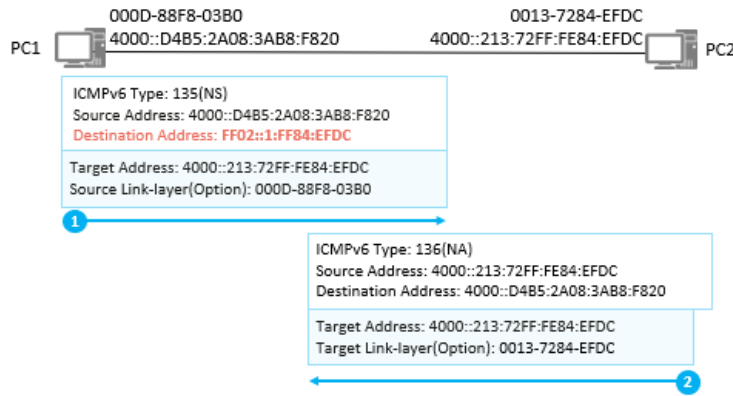


- 被请求节点组播地址的应用场景举例：在 IPv6 中，ARP 及广播都被取消，当设备需要请求某个 IPv6 地址对应的 MAC 地址时，设备依然需要发送请求报文，但是该报文是一个组播报文，其目的 IPv6 地址是目标 IPv6 单播地址对应的被请求节点组播地址，由于只有目标节点才会侦听这个被请求节点组播地址，所以该组播报文可以被目标节点所接收，同时不会占用其他非目标节点的网络性能。



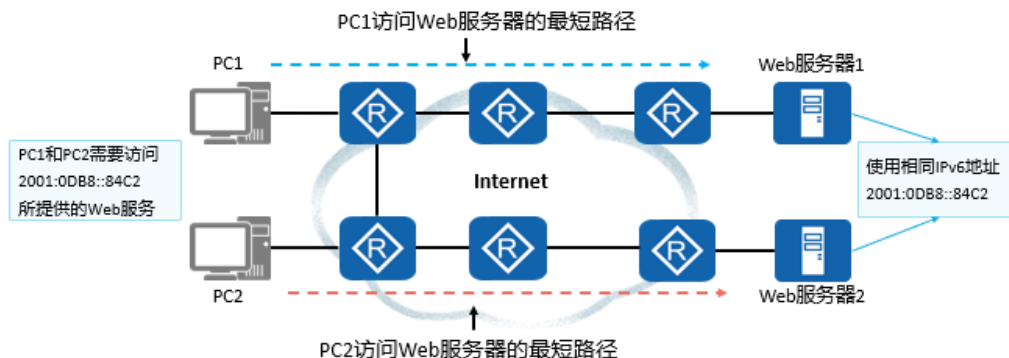
被请求节点组播地址 - 示例

PC1发送数据至PC2前，首先需要获取其MAC地址。PC1将发起类似IPv4中ARP的解析流程，IPv6使用ICMPv6的NS及NA报文来实现地址解析过程，NS报文的目IPv6地址为目标IPv6单播地址对应的被请求节点组播地址。



IPv6任播地址

任播地址标识一组网络接口（通常属于不同的节点）。任播地址可以作为IPv6报文的源地址，也可以作为目的地址。



- 任播过程涉及一个任播报文发起方和一个或多个响应方。
- 任播报文的发起方通常为请求某一服务（例如，Web 服务）的主机。
- 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。
- 网络中运用任播地址有很多优势：
- 业务冗余。比如，用户可以通过多台使用相同地址的服务器获取同一个服务（例如，Web 服务）。这些服务器都是任播报文的响应方。如果不是采用任播地址通信，当其中一台

服务器发生故障时，用户需要获取另一台服务器的地址才能重新建立通信。如果采用的是任播地址，当一台服务器发生故障时，任播报文的发起方能够自动与使用相同地址的另一台服务器通信，从而实现业务冗余。

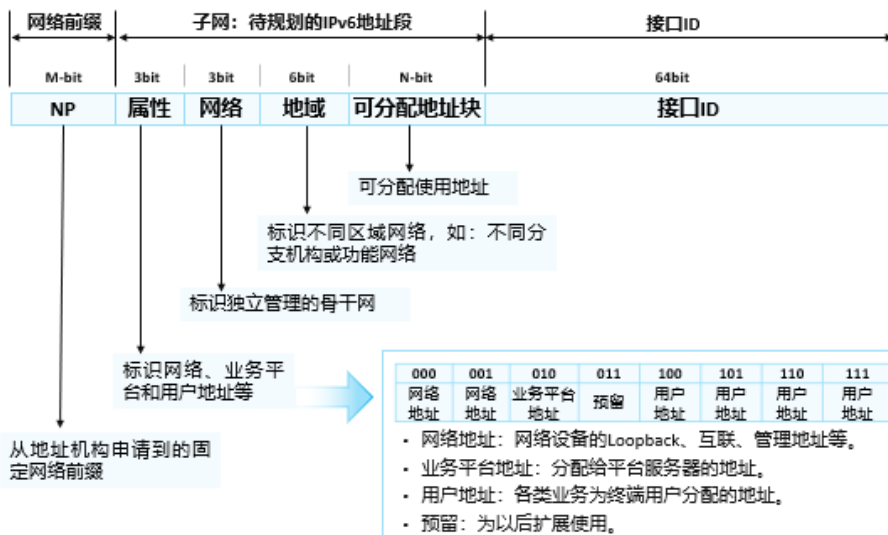
- 提供更优质的服务。比如，某公司在 A 省和 B 省各部署了一台提供相同 Web 服务的服务器。基于路由优选规则，A 省的用户在访问该公司提供的 Web 服务时，会优先访问部署在 A 省的服务器，提高访问速度，降低访问时延，大大提升了用户体验。



IPv6地址和IPv4地址比较

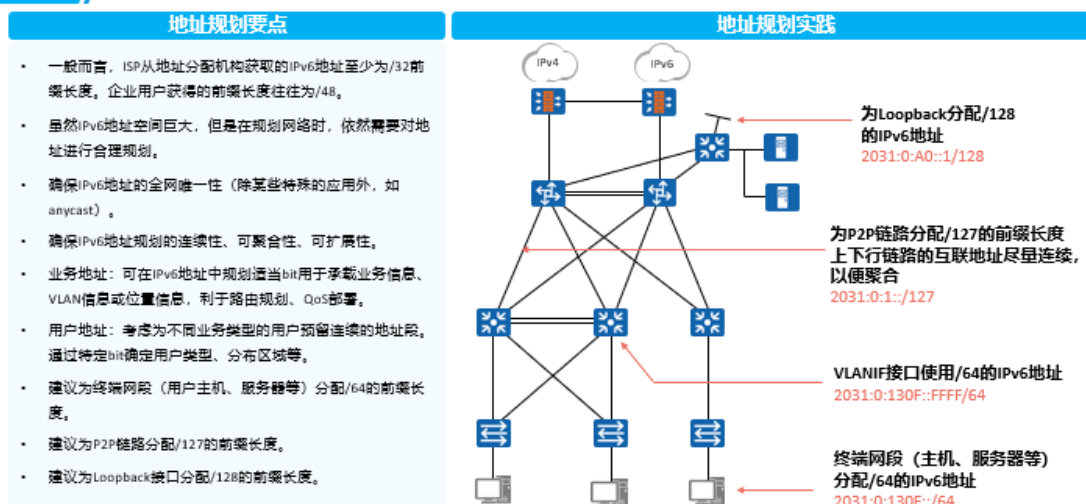
	IPv4	IPv6
地址空间	2 ³²	2 ¹²⁸
表示方式	点分十进制	冒号隔开的十六进制
地址类型	单播、组播、广播	单播、组播、任播
其它	A、B、C等主类地址	IPv6中无此概念
	组播地址 (224.0.0.0/4)	IPv6组播地址 (FF00::/8)
	广播地址	IPv6中无此概念
	未指定的地址0.0.0.0/32	未指定的地址::/128
	环回地址127.0.0.0/8	环回地址是::1/128
	公网IP地址	全球单播地址
	私网IP地址 (10.0.0.0/8, 172.16.0.0/12以及192.168.0.0/16)	唯一本地地址 (FD00::/8)
	APIPA地址 (169.254.0.0/16)	链路本地地址 (FE80::/10)

IPv6地址规划举例

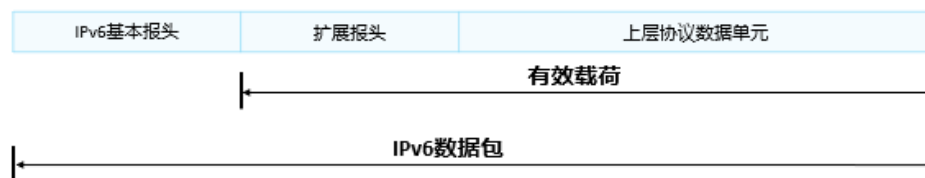


- 地址规划设计建议：
- 根据获取到的地址前缀，首先确定子网地址划分为几个功能块(如图中的 3+3+6+N)，明确各功能块的含义、占用多少 bit，避免地址浪费。

IPv6地址使用建议



IPv6报文构成

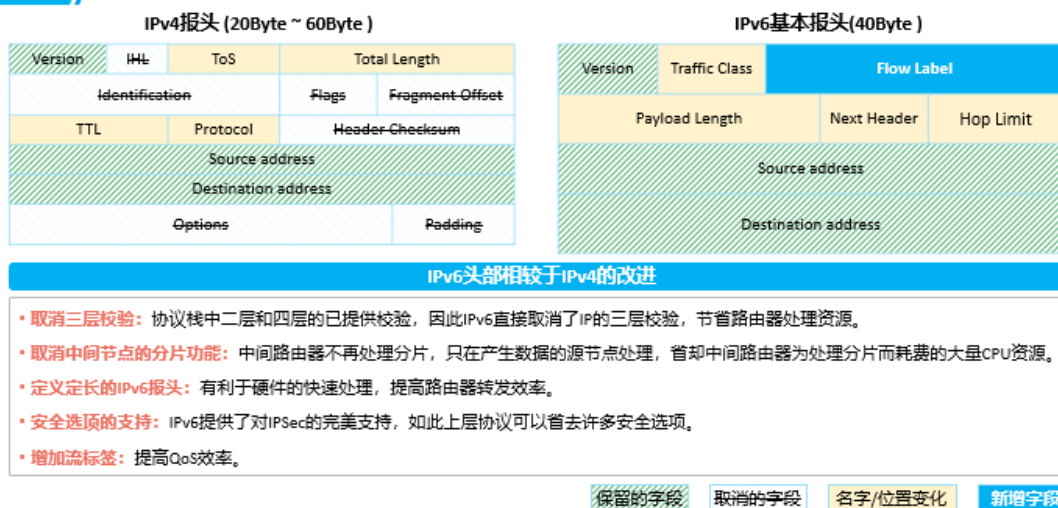


IPv6报文一般由三个部分组成：

- **基本报头**：提供报文转发的基本信息，路由器通过解析基本报头就能完成绝大多数的报文转发任务。
 - **扩展报头**：提供一些扩展的报文转发信息，如分段、加密等，该部分不是必需的，也不是每个路由器都需要处理，仅当需要路由器或目的节点做某些特殊处理时，才由发送方添加一个或多个扩展头。
 - **上层协议数据单元**：一般由上层协议报头和它的有效载荷构成，该部分与IPv4的上层协议数据单元相似。
- 从图中可以看出 IPv6 数据报文由以下几个部分组成：
 - **IPv6 基本报头 (IPv6 Header)**
 - 每一个 IPv6 数据报文都必须包含报头，其长度固定为 40 字节。
 - 基本报头提供报文转发的基本信息，会被转发路径上的所有路由器解析。
 - **扩展报头 (Extension Headers)**
 - IPv6 扩展报头是可能跟在基本 IPv6 报头后面的可选报头。IPv6 数据包中可以包含一个或多个扩展报头，当然也可以没有扩展头，这些扩展报头可以具有不同的长度。IPv6 报头和扩展报头代替了 IPv4 报头及其选项。新的扩展报头格式增强了 IPv6 的功能，使其具有极大的扩展性。与 IPv4 报头中的选项不同，IPv6 扩展报头没有最大长度的限制，因此可以容纳 IPv6 通信所需要的所有扩展数据。扩展报头提供报文转发的扩展信息，并不会被路径上所有的路由器解析，一般只会被目的路由器解析处理。
 - **上层协议数据单元 (Upper Layer Protocol Data Unit)**
 - 上层协议数据单元一般由上层协议报头和它的有效载荷构成，有效载荷可以是一个 ICMPv6 报文、一个 TCP 报文或

一个 UDP 报文。

IPv6基本报头



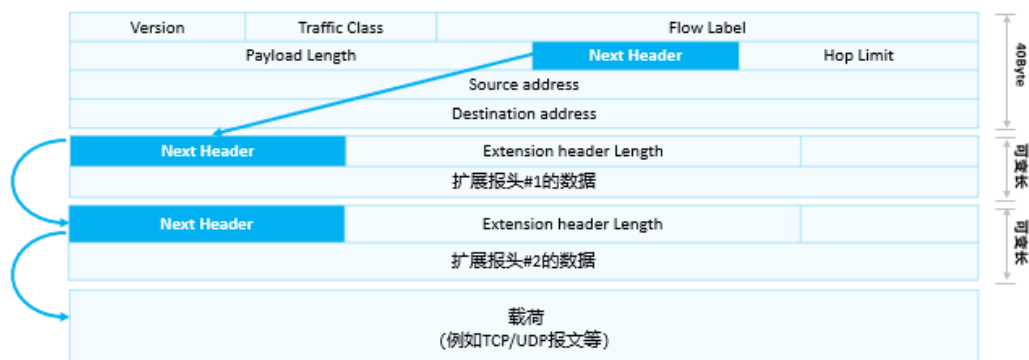
• IPv6 基本报头也称之为固定报头。固定报头包含 8 个字段，总长度为 40Byte。这 8 个字段分别为：版本 (Version)、流量类型 (Traffic Class)、流标签 (Flow Label)、净荷长度 (Payload Length)、下一个报头 (Next Header)、跳数限制 (Hop Limit)、源 IPv6 地址、目的 IPv6 地址。

- 版本 (Version)
- 该字段规定了 IP 协议的版本，其值为 6。长度为 4bit。
- 流类别 (Traffic Class)
- 该字段功能和 IPv4 中的服务类型功能类似，表示 IPv6 数据报文的类或优先级。长度为 8bit。
- 流标签 (Flow Label)
- 与 IPv4 相比，该字段是新增的。它用来标识这个数据报属于源节点和目标节点之间的一个特定数据报序列，它需要由中间 IPv6 路由器进行特殊处理。该字段长度为 20bit。一般来说一个流可以通过源/目的 IPv6 地址和流标签来确定。
- 有效载荷长度 (Payload Length)
- 该字段表示 IPv6 数据报有效载荷的长度。有效载荷是指

紧跟 IPv6 报头的数据报的其它部分（即扩展报头和上层协议数据单元）。该字段长度为 16bit，能表示最大长度为 65535 Byte 的有效载荷。如果有效载荷的长度超过这个值，该字段会置 0，而有效载荷的长度用逐跳选项扩展报头中的超大有效载荷选项来表示。

- 下一个报头（Next Header）
- 该字段定义紧跟在 IPv6 报头后面的第一个扩展报头（如果存在）的类型，或者上层协议数据单元中的协议类型。该字段长度为 8bit。
- 跳数限制（Hop Limit）
- 该字段类似于 IPv4 中的 TTL（Time to Live）字段。它定义了 IP 数据报所能经过的最大跳数。每经过一个路由器，该数值减去 1，当该字段的值为 0 时，数据报将被丢弃。该字段长度为 8bit。
- 源地址（Source Address）
- 表示发送方的地址，长度为 128bit。
- 目的地址（Destination Address）
- 表示接收方的地址，长度为 128bit。

IPv6扩展报头 (1)

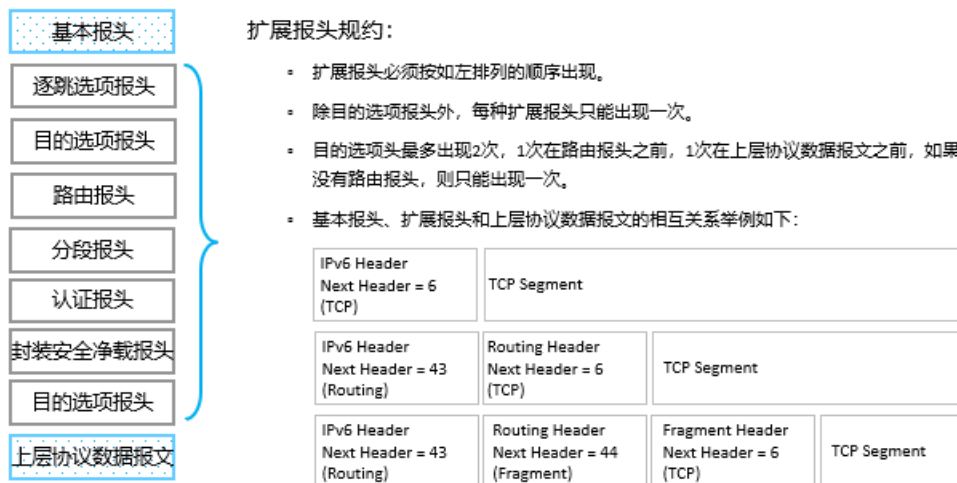


- **Next Header:** 下一报头，长度为8bit。与基本报头的Next Header的作用相同。指明下一个扩展报头（如果存在）或上层协议的类型。
- **Extension Header Length:** 报头扩展长度，长度为8bit。表示扩展报头的长度（不包含Next Header字段）。
- **Extension Header Data:** 扩展报头数据，长度可变。扩展报头的内容，为一系列选项字段和填充字段的组合。

• IPv6 报头设计中对原 IPv4 报头所做的一项重要改进就是将所有可选字段移出 IPv6 报头，置于扩展头中。IPv6 扩展报头是可能跟在基本 IPv6 报头后面的可选报头。为什么在 IPv6 中要设计扩展报头呢？因为在 IPv4 的报头中包含了所有的选项，每个中间路由器都必须检查这些选项是否存在，如果存在，就必须处理它们。这种设计方法会降低路由器转发 IPv4 数据包的效率。为了解决转发效率问题，在 IPv6 中，相关选项被移到了扩展报头中。中间路由器就不需要处理每一个可能出现的选项，这种处理方式提高了路由器处理数据包的速度，也提高了其转发性能。

• 通常，一个典型的 IPv6 包，没有扩展头。仅当需要路由器或目的节点做某些特殊处理时，才由发送方添加一个或多个扩展头。与 IPv4 不同，IPv6 扩展头长度任意，不受 40Byte 限制，以便于日后扩充新增选项，这一特征加上选项的处理方式使得 IPv6 选项能得以真正的利用。但是为了提高处理选项头和传输层协议的性能，扩展头总是 8Byte 长度的整数倍。

IPv6扩展报头 (2)



- 目前，RFC 2460 中定义了以下 6 个 IPv6 扩展头：
- 逐跳选项报头：该扩展头被每一跳处理，可包含多种选项，如路由器告警选项。
- 目的选项报头：目的地处理，可包含多种选项，如 Mobile IPv6 的家乡地址选项。
- 路由报头：指定源路由，类似 IPv4 源路由选项，IPv6 源节点用来指定信息报到达目的地的路径上所必须经过的中间节点。IPv6 基本报头的目的地址不是分组的最终目的地址，而是路由扩展头中所列的第一个地址。
- 分段报头：IP 报文分片信息，只由目的地处理。
- 认证报头：IPSec 用扩展头，只由目的地处理。
- 封装安全净载报头：IPSec 用扩展头，只由目的地处理。
- 逐跳选项扩展头和目的地选项扩展头内部提供选项功能，支持扩展性（如对移动性支持）。选项采用 TLV 方式。
- 如果数据报中没有扩展报头，也就是说数据包只包含基本报头和上层协议单元，基本报头的下一个报头（Next Header）字段值指明上层协议类型。在上例中，基本报头的下一个报头字段值为 6，说明上层协议为 TCP；如果报文有一个扩展报头，则基本报头的下一个报头（Next Header）字段值为扩

展报头类型（在上例中，指明紧跟在基本报头后面的扩展报头为 43，也就是路由报头），扩展报头的下一个报头字段指明上层协议类型；以此类推，如果数据报中报括多个扩展报头，则每一个扩展报头的下一个报头指明紧跟着自己的扩展报头的类型，最后一个扩展报头的下一个报头字段指明上层协议。



配置介绍 (1)

1. 使能设备的IPv6报文转发功能。

```
[<Huawei> system-view  
[Huawei] ipv6
```

2. 使能接口的IPv6功能。

```
[Huawei] interface interface-type interface-number  
[Huawei-GigabitEthernet1/0/0] ipv6 enable
```

3. 配置IPv6全球单播地址。

```
[Huawei-GigabitEthernet1/0/0] ipv6 address { ipv6-address prefix-length | ipv6-address/prefix-length }
```

每个接口下最多可配置10个全球单播地址。



配置介绍 (2)

1. 使能设备OSPFv3功能。

```
[<Huawei> system-view  
[Huawei] ospfv3 [ process-id ]
```

OSPFv3支持多进程，一台路由器上启动的多个OSPFv3进程之间由不同的进程号区分。OSPFv3进程号在启动OSPFv3时进行设置，它只在本地有效，不影响与其它路由器之间的报文交换。

2. 配置OSPFv3的Router ID。

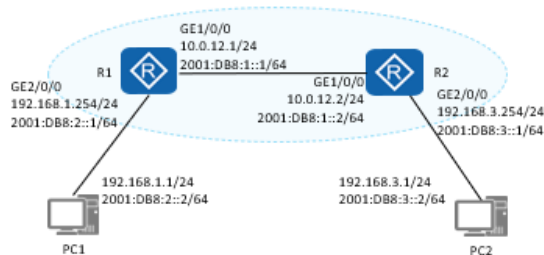
```
[Huawei-ospfv3-1] router-id router-id
```

OSPFv3的Router ID必须手工配置，如果没有配置ID号，OSPFv3无法正常运行。

3. 在接口上使能OSPFv3的进程，并指定所属区域。

```
[Huawei] interface interface-type interface-number  
[Huawei-GigabitEthernet1/0/0] ospfv3 process-id area area-id
```

案例：配置一个双栈网络 (1)



配置需求:

- 配置R1、R2的接口IP地址。
- R1和R2分别配置OSPFv2和OSPFv3，实现PC1和PC2的双栈互访。

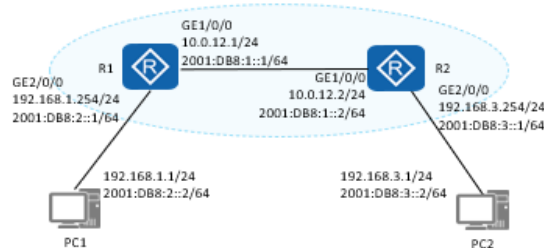
1. 在R1、R2全局和相关接口使能IPv6功能（以R1为例）。

```
[R1]ipv6
[R1]interface GigabitEthernet 1/0/0
[R1-GigabitEthernet1/0/0]ipv6 enable
[R1]interface GigabitEthernet 2/0/0
[R1-GigabitEthernet2/0/0]ipv6 enable
```

2. 在PC、R1、R2相应接口配置IPv4和IPv6全球单播地址（以R1为例）。

```
[R1]interface GigabitEthernet 1/0/0
[R1-GigabitEthernet1/0/0]ip address 10.0.12.1 24
[R1-GigabitEthernet1/0/0]ipv6 address 2001:DB8:1::1 64
[R1]interface GigabitEthernet 2/0/0
[R1-GigabitEthernet2/0/0]ip address 192.168.1.254 24
[R1-GigabitEthernet2/0/0]ipv6 address 2001:DB8:2::1 64
```

案例：配置一个双栈网络 (2)



配置需求:

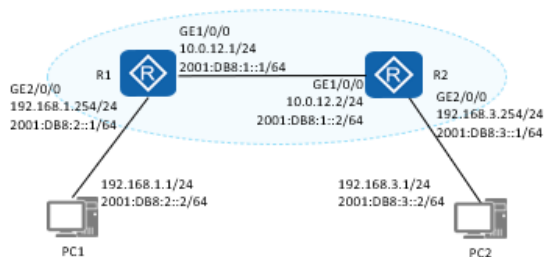
- 配置R1、R2的接口IP地址。
- R1和R2分别配置OSPFv2和OSPFv3，实现PC1和PC2的双栈互访。

在R1、R2配置OSPFv2使得PC1和PC2可以通过IPv4网络通信。

```
[R1]ospf 1 router-id 10.0.1.1
[R1-ospf-1]area 0
[R1-ospf-1-area-0.0.0.0]network 10.0.12.0 0.0.0.255
[R1-ospf-1-area-0.0.0.0]network 192.168.1.0 0.0.0.255
[R1-ospf-1-area-0.0.0.0]quit
[R1-ospf-1]
```

```
[R2]ospf 1 router-id 10.0.2.2
[R2-ospf-1]area 0
[R2-ospf-1-area-0.0.0.0]network 10.0.12.0 0.0.0.255
[R2-ospf-1-area-0.0.0.0]network 192.168.3.0 0.0.0.255
[R2-ospf-1-area-0.0.0.0]quit
[R2-ospf-1]
```


案例：配置一个双栈网络 (3)



配置需求：

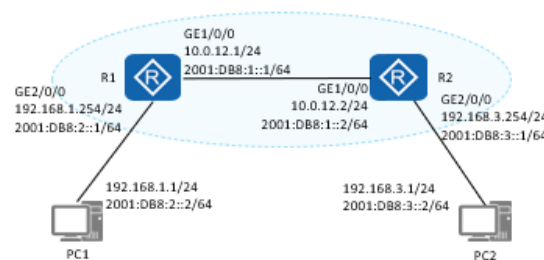
- 配置R1、R2的接口IP地址。
- R1和R2分别配置OSPFv2和OSPFv3，实现PC1和PC2的双栈互访。

在R1、R2配置OSPFv3使得PC1和PC2可以通过IPv6网络通信。

```
[R1]ospfv3
[R1-ospfv3-1]router-id 10.0.1.1
[R1-ospfv3-1]quit
[R1]interface gigabitethernet1/0/0
[R1-gigabitethernet1/0/0]ospfv3 1 area 0
[R1]interface gigabitethernet2/0/0
[R1-gigabitethernet2/0/0]ospfv3 1 area 0
```

```
[R2]ospfv3
[R2-ospfv3-1]router-id 10.0.2.2
[R2-ospfv3-1]quit
[R2]interface gigabitethernet1/0/0
[R2-gigabitethernet1/0/0]ospfv3 1 area 0
[R2]interface gigabitethernet2/0/0
[R2-gigabitethernet2/0/0]ospfv3 1 area 0
```

配置验证



在R1上Ping PC1的IPv6地址（IPv4略）。

```
<R1>ping ipv6 2001:db88:2::2
PING 2001:db88:2::2 : 56 data bytes, press CTRL_C to break
Reply from 2001:DB88:2::2:
bytes=56 Sequence=1 hop limit=255 time = 40 ms
Reply from 2001:DB88:2::2:
bytes=56 Sequence=2 hop limit=255 time = 10 ms
```

在PC1上Ping PC2的IPv6地址（IPv4略）。

```
PC1>ping 2001:db88:3::2
Ping 2001:db88:3::2: 32 data bytes, Press Ctrl_C to break
From 2001:db88:3::2: bytes=32 seq=1 hop limit=64 time<1 ms
From 2001:db88:3::2: bytes=32 seq=2 hop limit=64 time=16 ms
From 2001:db88:3::2: bytes=32 seq=3 hop limit=64 time=16 ms
From 2001:db88:3::2: bytes=32 seq=4 hop limit=64 time<1 ms
```

思考题：

- （简答题）简述 IPv6 相比于 IPv4 的优点。
- （简答题）简述 IPv6 报文头相比于 IPv4 的不同之处。

答案：

- “无限”地址空间，
- IPv6 与 IPv4 的不同之处：
- 采用了基本报头+扩展报头的报文形式。

- 取消了 IP 的校验：第二层和第四层的校验已经足够健壮了，因此 IPv6 直接取消了 IP 的三层校验，节省路由器处理资源。
- 取消中间节点的分片功能：中间路由器不再处理分片，只在产生数据的源节点处理，省却中间路由器为处理分片而耗费的大量 CPU 资源。
- 定义定长的 IPv6 报头：有利于硬件的快速处理，提高路由器转发效率。
- 安全选项的支持：IPv6 提供了对 IPSec 的完美支持，如此上层协议可以省去许多安全选项。
- 增加流标签：提高 QoS 效率。