

IPv6 发展现状及技术介绍

(中证技术供稿)

一、背景分析

以 IPv4 为核心技术的 Internet 获得巨大成功,但随着网络技术的飞速发展,IPv4 地址资源的枯竭,以及其固有的局限性无法满足网络发展的需求,也带来了一些问题,比如现有的 IPv4 地址匮乏、服务保障问题等。而 IPv6 可以有效的改善这些问题,由 IPv4 向 IPv6 的升级过渡将成为互联网发展的趋势。

(一) IPv4 发展的瓶颈

在 Internet 快速发展的过程中,IPv4 协议在设计时存在的局限性凸显出来:

- IP 地址空间的局限性

IPv4 的地址位数为 32 位,可使用的 IP 地址数量约 43 亿个,全球公网 IPv4 地址已于 2011 年 2 月分配完毕,且各国家占比极度不均衡,部分国家占有相当规模的地址空间。

- 骨干路由器维护的路由表表项数量过大

由于 IPv4 发展初期的分配规划问题,许多 IPv4 地址块分配不连续,不能有效聚合路由。目前全球 IPv4 BGP 路由表仍不断增长,即使经过 CIDR 聚合(Classless Inter-Domain Routing,无类别域间路由),也有 70 万条左右,日益庞大的路由表耗用内存较多,对设备成本和转发效率都有一定的影响。

- IPv4 网络中主机终端配置复杂

在将主机节点接入网络时一般需要专业人员的指导和帮助，需要对网络节点设置 IP 地址、子网掩码、网关地址等，而用户更喜欢“即插即用”。

- 缺乏对安全的支持

TCP/IP 协议起初是面向军方网络的，认为使用者都是可靠的，没有考虑到网络安全问题。而用于保障 IP 数据传输安全的 IPSec (Internet Protocol Security, 因特网协议安全性) 仅作为 IPv4 协议的一个可选项，并不是它的组成部分。

- 缺乏对 QoS (Quality of Service, 服务质量) 的支持

IPv4 网络提供尽力交付的服务，不提供服务质量保证，如带宽、时延、误码率和抖动等。因此，IPv4 不能满足日益增长的业务类型对 QoS 的需求。

(二) IPv6 的发展

至 1992 年初，一些关于互联网地址系统的建议在 IETF (互联网工程任务组) 上提出，并于 1992 年底形成白皮书。在 1993 年 9 月，IETF 建立了一个临时的 ad-hoc 下一代 IP (IPng) 领域来专门解决下一代 IP 的问题。从 1996 年开始，一系列用于定义 IPv6 的 RFC 发表出来，最初的版本为 RFC1883。

2003 年 1 月 22 日，IETF 发布了 IPv6 测试性网络，即 6bone 网络。它是 IETF 用于测试 IPv6 网络而进行的一项 IPng 工程项目，该工程目的是测试如何将 IPv4 网络向 IPv6 网络迁移。作为 IPv6 问题测试的平台，6bone 网络包括协议的实现、IPv4 向 IPv6 迁移等功能。

截至 2009 年 6 月，6bone 网络技术已经支持了 39 个国家的

260 个组织机构。6bone 网络被设计成为一个类似于全球性层次化的 IPv6 网络，同实际的互联网类似，它包括伪顶级转接提供商、伪次级转接提供商和伪站点级组织机构。由伪顶级提供商负责连接全球范围的组织机构，伪顶级提供商之间通过 IPv6 的 1BGP-4 扩展来尽力通信，伪次级提供商也通过 BGP-4 连接到伪区域性顶级提供商，伪站点级组织机构连接到伪次级提供商。伪站点级组织机构可以通过默认路由或 BGP-4 连接到其伪提供商。6bone 最初开始于虚拟网络，它使用 IPv6-over-IPv4 隧道过渡技术。因此，它是一个基于 IPv4 互联网且支持 IPv6 传输的网络，后来逐渐建立了纯 IPv6 链接。

从 2011 年开始，主要用在个人计算机和服务器系统上的操作系统基本上都支持高质量 IPv6 配置产品。例如，Microsoft Windows 从 Windows 2000 起就开始支持 IPv6，到 Windows XP 时已经进入了产品完备阶段。而 Windows Vista 及以后的版本，如 Windows 7、Windows 8 等操作系统都已经完全支持 IPv6，并对其进行了改进以提高支持度。Mac OS X Panther (10.3)、Linux 2.6、FreeBSD 和 Solaris 同样支持 IPv6 的成熟产品。一些应用基于 IPv6 实现。如 BitTorrent 点到点文件传输协议等，避免了使用 NAT 的 IPv4 私有网络无法正常使用的普遍问题。

2012 年 6 月 6 日，国际互联网协会举行了世界 IPv6 启动纪念日，这一天，全球 IPv6 网络正式启动。多家知名网站，如 Google、Facebook 和 Yahoo 等，于当天全球标准时间 0 点（北京时间 8 点整）开始永久性支持 IPv6 访问。

（三）国内背景

我们国家在 IPv6 部署及应用方面高度重视，由国家层面引导落地，2017 年 11 月，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》，明确了推进 IPv6 规模部署的路线图和时间表。我国的“十四五”规划纲要明确指出，要加快建设新型基础设施，全面推进互联网协议第六版（IPv6）商用部署。2021 年 7 月，工业和信息化部、中央网信办、发改委联合发布《关于加快推进互联网协议第六版（IPv6）规模部署和应用工作的通知》，通知明确了“十四五”我国 IPv6 规模部署和应用完成的主要指标和工作任务。

当前，IPv6 规模部署及应用仍在提速落地，尽管互联网应用 IPv6 热情、设备 IPv6 支持能力等问题和挑战依然存在，但是在国家政策的有力指引下，在互联网产业界各方的协同推进下，IPv6 改造将更加深入，产业生态将加速完善，基于 IPv6 的各类融合应用将快速涌现。

二、IPv6 地址结构

（一）IPv6 地址分类及编址：

IPv6 地址可分为三种，分别为单播地址、任播地址和组播地址。

- 单播地址：和 IPv4 中单播一样，每个地址只代表一个接口，目的是该地址的数据包只能够转发到该接口。全球单播地址的前三位 bit 固定为 001，前缀为 2000::/3，/3 表示子网掩码。
- 组播地址：和 IPv4 中组播一样，一个地址可以标识多个不同的接口或者节点，目的是该地址的数据报文会转

发到多个节点。

- 任播地址：一个地址可以标识多个不同接口或者节点，目的是该地址的数据报文会转发到最近的一个节点上（最近取决于单播路由计算的结果）。

IPv6 地址总共有 128bit，使用十六进制进行表示，具有如下特点：

- IPv6 地址以 16bit 为一分组、每个 16bit 分组通过 4 个 16 进制 (HEX) 字符来表达，共 8 组，中间通过冒号“:”隔开，如：2001:0DB8:0000:0000:FFFF:0000:0000:0D0C
- 每组的前导 0 可以省略，如 2001:DB8:0:0:FFFF:0:0:D0C;
- 连续的多组 0 可以表示为::，但是最多出现一次，如 2001:DB8::FFFF:0:0:D0C 或 2001:DB8:0:0:FFFF::D0C
- 前 64bit 标识网络部分，后 64bit 标识接口/主机部分
- 层次化地址结构，IP 管理更加便捷

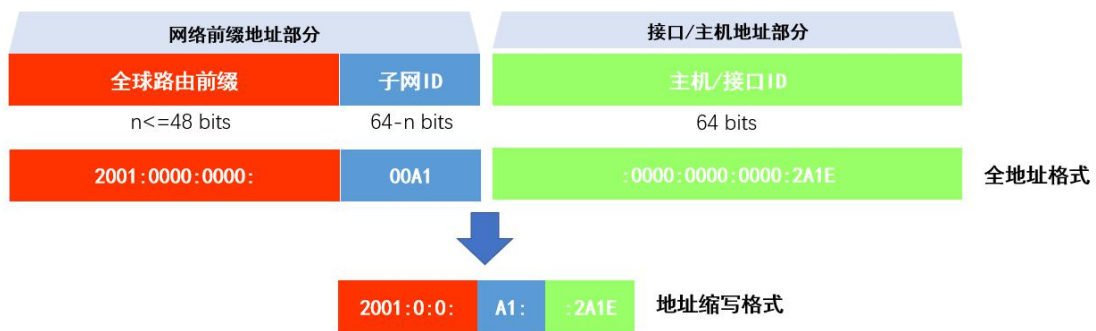


图 1：IPV6 地址格式

表 1：IPv6 和 IPv4 地址对比：

地址类型	IPv6	IPv4	作用
单播地址	本地环回地址 (::1/128)	本地环回地址 (127.0.0.1/32)	虚拟接口 (Loopback)
	全球单播地址 (2000::/3)	公网地址	全球唯一，Internet 可路由
	本地链路地址 (FE80::/10)	无	仅限于本地链路范围内使用，该

			地址作为源 IP 或目的 IP 均不可 Internet 路由。节点可自动生成，用于相邻节点之间使用，如邻居发现、无状态地址配置使用，实现即插即用功能。
	唯一本地地址 (FC00::/7)	私网地址 (10、172 等地址段)	全球唯一前缀，随机方式产生，可以进行网络之间私有连接。
组播地址	FF00::/8	224-239 地址段	组播应用
任播地址	任播地址	广播地址	任播地址无特殊地址段，应用于 MSDP 的 Anycast RP、CDN 等应用

(二) IPv6 的优点:

- IPv6 有 128 位地址结构，能够提供充足的地址空间。号称能够为地球上的每一粒沙子分配一个 IP 地址。
- 分层聚合，提高了路由效率。IPv6 可提供远大于 IPv4 的网络前缀，同一组织机构在其网络中可以只使用一个前缀。对于 ISP，则可获得更大的地址空间。这样 ISP 可以把所有客户聚合形成一个前缀并发布出去。分层聚合使全局路由表项数量很少，转发效率更高；
- 无需 NAT，Ip 地址足够，可分配给全球所有的物联网设备使用，无需 nat，解决 nat 地址溯源难的问题。
- 无广播，网络的稳定性更强
- QoS 更有保障，IPv6 新增的流标签，可以允许网络用户对通信质量提出要求。

表 2 IPv6 和 IPv4 地址优缺点对比:

描述	IPv4	IPv6
地址	长度为 32 位 (4 个字节)。地址由网络 and 主机部分组成，这取决于地址类。	长度为 128 位 (16 个字节)。基本体系结构的网络数字为 64 位，主机数字为 64 位。通常，IPv6 地址 (或其部分) 的主机部分将派生自 MAC 地址或其他接口标识。IPv6 地址的文本格式为

		XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX, 其中每个 x 都是十六进制数, 表示 4 位。可省略前导零。可在地址的文本格式中使用一次双冒号 (::), 用于指定任意数目的 0 位
地址分配	使用“无类域间路由”(CIDR)进行更小的分配。没有在机构和地区之间平均分配地址。	“因特网工程任务组织”(IETF)和“因特网体系结构委员会”(IAB)建议基本上为每个组织或实体分配一个/48子网前缀长度。它将保留 16 位供组织进行子网划分。
地址解析协议 (ARP)	IPv4 使用 ARP 来查找与 IPv4 地址相关联的物理地址 (如 MAC 或链路地址)。	IPv6 使用因特网控制报文协议版本 6 (ICMPv6)将这些功能嵌入到 IP 自身作为无状态自动配置和邻节点发现算法的一部分。因此, 不存在类似于 ARP6 之类的东西。
分片	如果一个信息包对于要传送它的下一链路来说太大, 那么可由发送方 (主机或路由器) 对其分段。	对于 IPv6, 只能在源节点进行分段, 且只能在目标节点完成重新装配。使用分段扩展报头。
IP 报头	根据提供的 IP 选项, 有 20-60 个字节的可变长度。	40 个字节的固定长度。没有 IP 报头选项。通常, IPv6 报头比 IPv4 报头简单。
IP 报头选项	IP 报头 (在任何传输报头之前) 可能附带各种选项。	IPv6 报头没有选项。而 IPv6 添加了附加 (可选) 的扩展报头。扩展报头包括 AH 和 ESP (和 IPv4 的一样)、逐跳扩展、路由、分段和目标。目前, IPv6 支持一些扩展报头。
回送地址	回送地址是地址为 127.*.* (通常是 127.0.0.1) 的接口, 只能由节点用来向自身发送信息包。该物理接口 (线路描述) 被命名为 *LOOPBACK。	与 IPv4 的概念相同。单个回送地址为 0000:0000:0000:0000:0000:0000:0000:0001 或 ::1 (简短版本)。虚拟物理接口被命名为 *LOOPBACK。

(三) 国际 IPv6 地址的分配

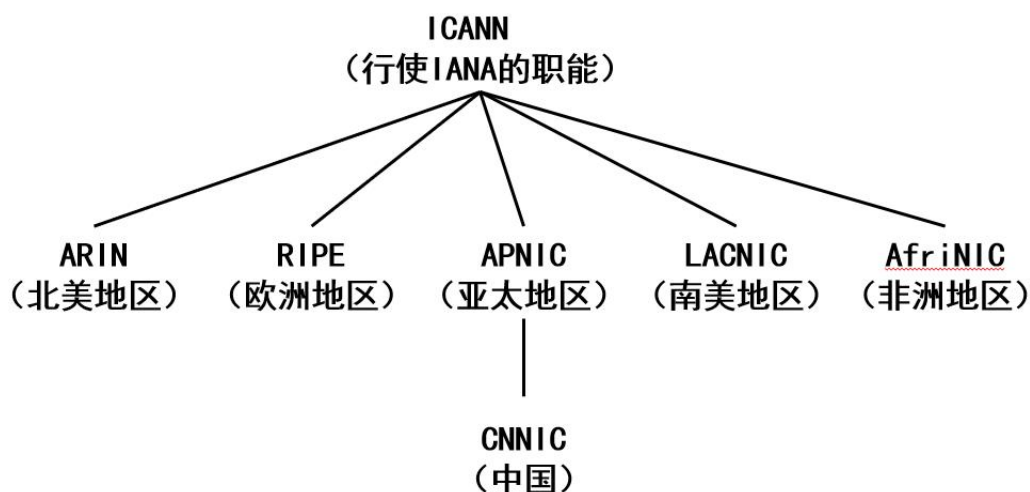


图 2 国际 IPv6 地址的分配

IPv6 全球单播地址为 $2000::/3$ ，即 $2000:: - 3fff:ffff$ 。由互联网数字分配机构（The Internet Assigned Numbers Authority, IANA）统一进行管理。目前，IPv6 已分配 $2000::/4$ ，其中各区域分配如下：

（1） $2000::/8$ 主要是 IPv6 互联网前期分配，在全球各地均有分配使用。

（2） $2400::/8$ 主要由 APNIC 管理（亚太互联网络信息中心）。

（3） $2600::/8$ 主要由 ARIN 管理（美洲互联网号码注册管理机构）。

（4） $2800::/8$ 主要由 LACNIC 管理（拉丁美洲和加勒比地区互联网地址注册管理机构）。

（5） $2a00::/8$ 主要由 RIPE 管理（欧洲互联网络信息中心）。

（6） $2c00::/8$ 主要由 AfriNIC 管理（非洲互联网络信息中心）。

三、IPv6 过渡技术

IPv6 经过 20 多年的发展研究实验，已经成为一项成熟技术，其具有大量 IP 地址数量、更小路由表、更安全等特点，为有效解决 IPv4 现存问题提供了途径。但是由于 IPv6 本身与 IPv4 不兼容，在 IPv6 成为主流协议之前，必须解决其过渡问题。

目前能够解决过渡问题的基本技术主要有三种：双栈技术，隧道技术及 NAT-PT 技术。

（一）双栈技术

双栈技术是指在网络节点上同时运行 IPv4 和 IPv6 两种协议，从而在 IP 网络中形成逻辑上相互独立的两张网络：IPv4 网

络和 IPv6 网络。连接双栈网络的设备同时也配置 IPv4 地址和 IPv6 地址，IPv4 协议栈和 IPv6 协议栈相互独立不存在 IPv4 和 IPv6 网络部署时的相互影响，可以按需部署。因此双栈技术目前被认为是部署 IPv6 网络最简单的方法，也被国内外运营商广泛采用。双栈技术可以实现 IPv4 和 IPv6 网络的共存，但是不能解决 IPv4 和 IPv6 网络之间的互通问题。而且双栈技术不会节省 IPv4 地址，不能解决 IPv4 地址用尽问题。双栈结构示例如下：

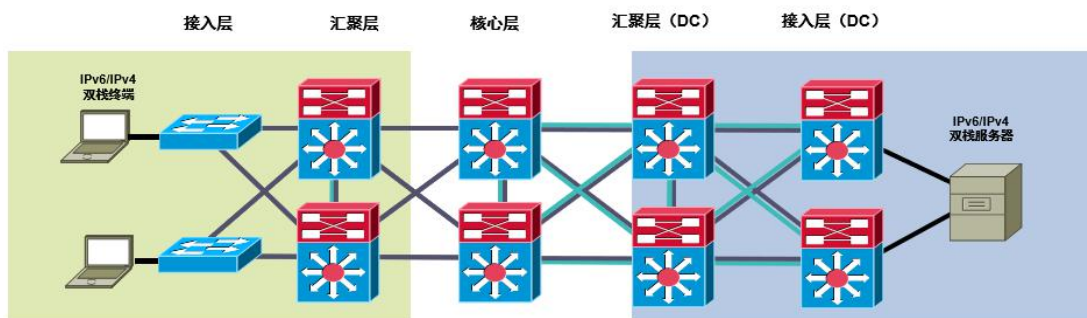


图 3 双栈结构示例

(二) 隧道技术

隧道技术是通过将一种 IP 协议数据包嵌套在另一种 IP 协议数据包中进行网络传递的技术，只要求隧道两端的设备支持两种协议。隧道类型有多种，按照隧道协议的不同分为 IPv4 over IPv6 隧道和 IPv6 over IPv4 隧道；根据隧道终点地址的获得方式，可将隧道分为配置型隧道（如手工隧道、GRE 隧道）和自动型隧道（如隧道代理、6to4、6over4、6RD、ISATAP、TEREDO、基于 MPLS 的隧道 6PE 等）。隧道技术本质上只是提供一个点到点的透明传送通道，无法实现 IPv4 节点和 IPv6 节点之间的通信。适用于同协议类型网络孤岛之间的互联。

这种技术的优点是，不用把所有的设备都升级为双栈，只要求 IPv4/IPv6 网络的边缘设备实现双栈和隧道功能。除边缘节点外，其它节点不需要支持双协议栈。隧道结构示例如下：

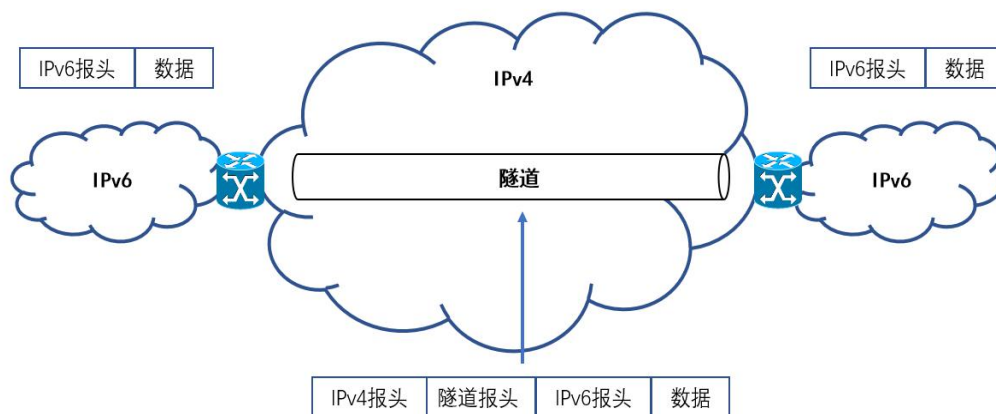


图 4 隧道结构示例

(三) NAT-PT 技术

1、NAT64

在过渡期间，IPv4 和 IPv6 共存的过程中，面临的一个主要问题是 IPv6 与 IPv4 之间如何互通。由于二者的不兼容性，因此无法实现二种不兼容网络之间的互访。为了解决这个难题，IETF 在早期设计了 NAT-PT 的解决方案：RFC2766，NAT-PT 通过 IPv6 与 IPv4 的网络地址与协议转换，实现了 IPv6 网络与 IPv4 网络的双向互访。但 NAT-PT 在实际网络应用中面临各种缺陷，IETF 推荐不再使用，因此已被 RFC4966 所废除。

为了解决 NAT-PT 中的各种缺陷，同时实现 IPv6 与 IPv4 之间的网络地址与协议转换技术，IETF 重新设计一项新的解决方案：NAT64 与 DNS64 技术。

NAT64 是一种有状态的网络地址与协议转换技术，一般只支

持通过 IPv6 网络侧用户发起连接访问 IPv4 侧网络资源。但 NAT64 也支持通过手工配置静态映射关系，实现 IPv4 网络主动发起连接访问 IPv6 网络。NAT64 可实现 TCP、UDP、ICMP 协议下的 IPv6 与 IPv4 网络地址和协议转换。DNS64 则主要是配合 NAT64 工作，主要是将 DNS 查询信息中的 A 记录 (IPv4 地址) 合成到 AAAA 记录 (IPv6 地址) 中，返回合成的 AAAA 记录给用户给 IPv6 侧用户。DNS64 也解决了 NAT-PT 中的 DNS-ALG 存在的缺陷。

NAT64 是 IPv6 网络发展初期的一种过渡解决方案，在 IPv6 发展前期会被广泛部署应用，而后期则会随着 IPv6 网络的发展壮大逐步退出历史舞台。

2、IVI

IVI 是一种基于运营商路由前缀的无状态 IPv4/IPv6 翻译技术。IVI 方案是由 CERNET2 的研究人员清华大学李星教授提出的，对应 RFC6052。

IVI 主要思路是从全球 IPv4 地址空间 (IPG4) 中，取出一部分地址映射到全球 IPv6 地址空间 (IPG6) 中。在 IPG4 中，每个运营商取出一部分 IPv4 地址，被用来在 IVI 过渡中使用，被取出的这部分地址称为 IVI4 (i) 地址，这部分地址不能分配给实际的真实主机使用了。

IVI 的地址映射规则是在 IPv6 地址中插入 IPv4 地址。地址的 0-31 位为 ISP 的 /32 位的 IPv6 前缀，32-39 位设置为 FF，表示这是一个 IVI 映射地址。40-71 位表示插入的全局 IPv4 空间 (IVIG4) 的地址格式，如 IPv4/24 映射为 IPv6/64 而 IPv4/32 映

射为 IPv6/72。

四、IPv6 展望

（一）IPv6 的部署建议

从目前的形势看,IPv4 的寿命还远远没有结束,IPv4 和 IPv6 会共存相当长一段时间, IPv6 将会渐进式的发展、扩张并逐步替代 IPv4。

所以,公司在部署 IPv6 时应着眼于长远发展,并渐进式增长,避免一蹴而就。一是做好培训,让技术人员对 IPv6 的知识和应用意义有明确的了解,并适当提供技术培训。二是提前规划,确定好公司的所选择的过渡技术,并在计划中着重考虑扩展性、可靠性和安全性。三是从边缘到核心,从辅助系统到核心系统,对公司内部网络、系统进行逐步改造,最后实现全面对于 IPv6 的支持。

（二）安全思考

虽然 IPSec 是 IPv6 的重要组成部分,可通过扩展首部提高安全性,但由于使用时间短,使用范围有限,地址空间大,IPv6 协议所面临的最大的安全风险是高度不确定性。原因如下:

- （1） IPv6 协议大规模推广使用时间不长,初期漏洞多,风险大。
- （2） 安全防护设备对于 IPv6 跟进尚需一段适应时间,现阶段主要模拟 IPv4 进行防护,难以防护 IPv6 特性产生的威胁。
- （3） 目前从 IPv6 方向发生的攻击数量不多,防守方的经验不足。

- (4) 由于 IPv4 和 IPv6 的共存,增加了安全的监控成本,对于人员、设备等资源的运用是一项挑战。