园区网中的 IPv6 实现及应用

Implementation and Application in Campus Network Based on IPv6

江 魁　张 凡　(深圳市深圳大学网络中心 518060)

摘要:该文结合一个大型园区网中 IPv6 网络建设项目的探索与实践,探讨了 IPv6 在园区网中实现及应用的关键技术和难点。首先给出 IPv6 地址规划原则,随后介绍 IPv6 接入的实现方法,最后说明 IPv6 应用的实现。

关键词: 下一代互联网 IPv6 园区网

1 引言

随着 Internet 规模不断扩展, IPv4 已无法满足网络对 IP 地址的庞大需求。IETF 制订了 IPv6 作为下一代互联网的协议,IPv6 以近乎无限的地址空间、层次化的地址结构、高速的路由、更强的安全性、对移动性和服务质量的友好支持等特性,成为替代 IPv4 的最佳协议。

2003 年国家发改委等八部委启动了 CNGI(中国下一代互联网)项目,其目标是在 2005 年底建成一个覆盖全国的 IPv6 网络。CERNET(中国教育和科研计算机网)在 2004 年开通的 IPv6 主干网 CERNET2 是 CNGI 核心网的重要组成部分[1]。我校是 CERNET 38 个主节点之一,进行 IPv6 网络建设,提供一个研究和应用 IPv6 的平台既是配合 CERNET 进行下一代互联网建设的重要任务,也是我校数字化校园项目中的重要子项目。

本文结合我校的项目实践,对 IPv6 在园区网中的实现及应用进行探讨。首先给出 IPv6 地址规划原则,随后阐述 IPv6 的接入,最后说明现有 IPv4 应用向 IPv6 应用的迁移,为各单位及高校建设基于 IPv6 的园区网络提供参考。

2 IPv6 地址规划

IPv6 地址结构不同于 IPv4,如何对地址进行有效规划是 IPv6 网络建设面临的首要问题。园区网具有承载业务多样性与用户数量递增性的特点,需要对其不断进行扩容升级。因此,保证地址分配的层次性与可扩展性是 IPv6 地址规划的重要原则。

层次性是指在划分 IPv6 地址时确保一个区域的地址块能在路由表中聚合为一条路由,从而有效控制路由表规模,提高网络运行效率。这要求在规划 IPv6 地址时结合网络物理拓扑,避免连续可聚合的前缀分配给物理拓扑分离的网络。可扩展性是指在划分 IPv6 地址时要充分考虑当前以及将来的网络需求,留有一定扩展余地。这要求在规划 IPv6 地址时充分考虑用户地址与网络地址两类用途。

IPv6 地址有 128 位,左边 64 位开始的前 3 位是格式前缀,其值是 001 代表地址为可聚集全局单播地址。随后是 13 位顶级集聚标识符(TLA ID),8 位 RES 保留位,24 位下一级集聚标识符(NLA ID)以及 16 位子网标识符(SLA ID)。最右边的 64 位是接口标识(Interface ID)。如图 1 所示。

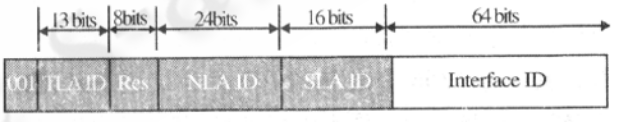

图 1　IPv6 地址结构图

虽然最新制订的 RFC 3513 中没有明确规定 64 位可分配网络前缀中全球可路由前缀和子网标识符各自位数,但分配给园区网的站点地址通常都采用/48 前缀[2]。因此在园区网中规划 IPv6 地址时,只有剩余的子网标识符(SLA ID)部分可以规划。例如,我校从 CERNIC(中国教育科研网网络信息中心)申请的 IPv6 地址范围是 2001:250:3C00::/48。根据地址规划的层次性与扩展性原则,我们实现的地址规划方案如表 1 所示。

表 1 IPv6 地址规划方案

地址	2001:250:3C00	xyrrpppp	oooooooo	EUI-64
说明	地址前缀	子网标识1	子网标识2	接口标识
位数	32	8	8	64

其中：

x：0 代表准备分配的地址，1 代表保留的地址；

y：0 代表使用的地址，1 代表保留的地址；

rr：00 代表分配给校园主干，01 代表分配给办公区，10 代表分配给宿舍区，11 分配给校外各单位；pppp：子网地址 1；

oooooooo：子网地址 2。

其中，2001:250:3C00::/49 拿出来分配使用，2001:250:3C00:8000::/49 保留。再将 2001:250:3C00::/49 中的 2001:250:3C00::/50 拿出来使用，2001:250:3C00:4000::/50 保留。在 2001:250:3C00::/50 中，2001:250:3C00::/52 用于校园主干网，2001:250:3C00:1000::/52 用于校内各院系等教学科研单位，2001:250:3C00:2000::/52 用于学生区与教工区宿舍楼，2001:250:3C00:3000::/52 用于与我校相连的各单位。对于 2001:250:3C00::/52 我们再分成 16 个/56，其中第一个/56，即 2001:250:3C00::/56 分成 256 个/64 地址用来提供各服务器、用户隧道接入以及路由两端的地址，其余 15 个/56 作为一级汇聚子网（等同于支持 IPV6 的汇聚层路由器个数），其中每个/56 分成 16 个/60 作为二级子网，第一个/60 分成 16 个/64 作为路由地址，第二个/60 保留，剩下的每个/60 可以继续分为 16 个/64，用来直接连接子网，也可以直接使用。对于其余三个/52 采用类似的分配机制。

从以上分配方案可知，对于已分配的/64 地址块的单位，我们预留了/56 的地址块以便网络扩展时无需另外分配地址，此外/56 的地址块也可直接分配给园区内中为其他机构提供接入的单位。最右边的 64 位采用 IEEE EUI-64 格式构造用于子网接口标识，便于将来进行 IPv6 地址的自动配置，因此没有对这部分地址进行划分[3]。

3 IPv6 接入

在完成 IPv6 地址规划后，需要考虑 IPv6 的接入。通过对各园区网实际需求分析，我们将 IPv6 接入分成两个层次考虑。第一个层次为网络边缘设备接入，该层次负责将园区网络接入 IPv6；第二个层次是园区网内用户接入，该层次负责将用户接入 IPv6。下面分别阐述这两个层次的接入解决方案。

3.1 边缘设备接入

对于边缘设备接入来说，其接入方式主要有纯 IPv6（Native IPv6）与隧道（Tunnel）两种方式。纯 IPv6 接入是指通过物理线路直接与 IPv6 网络连接，由于该方式能够保证 IPv6 应用的完全实现，因此在能够采用该方式接入时，优先选择此接入方式。如果无法以纯 IPv6 接入，就考虑各种隧道接入。

隧道的实现原理是将 IPv6 的分组封装到 IPv4 的分组中传送，封装后的 IPv4 分组源地址和目的地址分别是隧道入口和出口的 IPv4 地址，在分组到达隧道出口处时，再将 IPv6 分组取出转发给目的站点。目前有手工隧道、自动隧道、BGP 隧道等多种形式的隧道接入方式[4]。在园区网中，手工隧道与 BGP 隧道是可用于边缘设备隧道接入的两种方式。BGP 隧道除了以 BGP4+路由协议学习与发布 IPv6 地址信息，其建立隧道机制与手工隧道类似，下面以我校 BGP 隧道接入为例说明。

我们已正式加入 CERNET IPv6 主干网的 BGP 研究项目，通过 CERNET IPv6 试验床国家网络中心提供的 BGP 隧道接入 CERNET2。边缘设备采用 Cisco 7206，该设备能够支持 IPv6/IPv4 双协议栈以及各种隧道接入方式。BGP 对等体两端接口为全局 IPv4 地址，由接入服务提供商分配隧道两端 IPv6 地址与自治系统号，以下是 Cisco 7206 上 BGP 隧道的关键配置：

```
interface Tunnel0
 no ip address
 ipv6 address 3FFE:3240::FFFF:0:15:2/112
 tunnel source 210.39.x.x
 tunnel destination 202.38.x.x
 tunnel mode ipv6ip
router bgp 65023
```

```
no synchronization
bgp router – id 210.39.x.x
no bgp default ipv4 – unicast
bgp log – neighbor – changes
neighbor 3FFE:3240::FFFF:0:15:1 remote – as
65001
no auto – summary
!
address – family ipv6
neighbor 3FFE:3240::FFFF:0:15:1 activate
network 2001:250:3C00::/48
exit – address – family
!
```

3FFE:3240::FFFF:0:15:2 是 CERNET IPv6 试验床国家网络中心分配给隧道的本地 IPv6 地址，3FFE:3240::FFFF:0:15:1 是隧道对端的 IPv6 地址。自治系统号 65023 是分配给我们的自治系统号，该自治系统号为私有自治系统号，只能在 CERNET IPv6 试验床内部使用。自治系统号 65001 为 CERNET IPv6 试验床的自治系统号。我们申请的 IPv6 地址通过 network 命令发布到全球 IPv6 路由表中。

3.2 园区用户接入

与边缘设备接入 IPv6 类似，园区用户接入 IPv6 也优先采用纯 IPv6 接入，无法以该方式接入时采用隧道方式接入。园区用户采用纯 IPv6 接入需要网络设备能够同时支持 IPv6 和 IPv4，确保园区网同时支持两种业务流的承载与互通。但目前各园区网基本使用基于 ASIC 芯片的交换机，厂家不可能预先将 IPv6 集成到 ASCI 中，因此园区网采用纯 IPv6 接入往往要对现有网络设备更换，这不太可行。为此，我们提出以下策略：如果用户所连接的网络设备能够支持 IPv6 则采用纯 IPv6 接入，如果所连设备无法支持 IPv6 则采用隧道服务来向网络用户提供 IPv6 接入。园区网用户接入常用的隧道主要有 6to4、ISATAP 和 Tunnel Broker（隧道代理）[4]。我们的核心网络设备与汇聚网络设备均为 Nortel 的 Passport 8600，其上的软件暂无法支持 IPv6 协议。因此，我们采用了华为公司的 AR46 路由器向园区用户提供 IPv6 隧道接入，待将来网络设备升级支持 IPv6 后，我们再向用户提供纯 IPv6 接入。

3.2.1 6to4 隧道

6to4 隧道需要使用特殊的 6to4 地址，该地址以 2002:a.b.c.d 开头，其中 a.b.c.d 是 IPv4 地址，通过内嵌的 IPv4 地址查找 6to4 隧道的其他端点。对于 IPv6 网络之间的互联，需要提供 6to4 中继路由器，该设备负责在 6to4 网络和 IPv6 网络之间传输报文，同时要将 2002::/16 的路由信息通告到 IPv6 网络。6to4 的缺点是必须使用规定的 6to4 地址，另外使用 6to4 隧道的客户机 IP 必须是真实 IP。下面是 AR46 上 6to4 隧道的关键配置：

```
interface Tunnel1
 ipv6 address 2002:D227:xxxx::D227:xxxx/48
 tunnel – protocol ipv6 – ipv4 6to4
 source Ethernet1/0/0
#
ipv6 route – static 2002:: 16 Tunnel1
```

3.2.2 ISATAP

ISATAP 隧道的最大特点是可以在隧道两端设备之间运行邻居发现（Neighbor Discovery）协议，便于地址前缀的自动获取，此外客户机的 IP 地址即使是内部 IP（RFC 1918）也可以通过该隧道接入 IPv6 网络。下面是 AR46 上 ISATAP 隧道的关键配置：

```
interface Tunnel2
 ipv6 address 2001:250:3C00:1:0:5EFE:C0A8:
 4206/64
 undo ipv6 nd ra halt
 tunnel – protocol ipv6 – ipv4 isatap
 source LoopBack1
#
ipv6 route – static 2001:250:3C00:1:: 64 Tunnel2
```

3.2.3 Tunnel Broker

相比于其他隧道接入方式，Tunnel Broker 方式是一种有状态隧道技术，能够自动对隧道建立、修改、配置和删除，实现隧道的自动配置管理，特别适用园区网这类有大量分散的用户接入 IPv6 的环境。我们基于 RFC3053，在 FreeBSD 上实现了一个 Tunnel Broker 系统。该系统能够实现 IPv6 地址分配，提供动态生成脚本机制，并能自动进行已建隧道的修改与删除。用户通过该 Tunnel Broker 系统可在现有的 IPv4 网络上建

立隧道，获得 IPv6 地址，从而与其他 IPv6 主机通信。

4 IPv6 应用

接入 IPv6 网络后面临的重要问题是如何实现 IPv4 应用向 IPv6 应用的迁移，这对 IPv6 研究及实验有重要的促进作用，也是制约 IPv6 应用发展的关键。当前常用系统平台基本都提供对 IPv6 支持，如 Sun Solaris，Microsoft Windows 2000/XP/2003，Linux 与 FreeBSD 等。FreeBSD 是其中最早支持 IPv6 的系统，也是对 IPv6 支持最好的平台。在 FreeBSD 4.0 及更高版本中，不仅包括各种支持 IPv6 的应用工具，还包括各种 IPv6 网络应用程序。因此，FreeBSD 是园区网中实现 IPv6 应用服务的首选系统平台[5]。我们的经验表明，尽管 FreeBSD 提供支持 IPv6 的应用工具和程序，但要完全满足园区网实际需求，还要对某些程序进行修改，甚至重新设计。目前，我们已基于 FreeBSD 实现以下 IPv6 应用：

4.1 DNS

由于 IPv6 地址复杂性，人们必须通过域名方式访问各种 IPv6 应用，因此 DNS 是所有 IPv6 应用服务中最基本与关键的一项。从 IPv4 过渡到 IPv6 时，DNS 不仅要对 IPv4 地址和主机名进行解析，还要对 IPv6 地址和主机名进行解析。IETF 在 DNS 中为 IPv6 地址定义了新的资源记录类型，使其提供对 IPv6 的支持。在正向域名解析中，通过 AAAA 资源记录将主机名映射为 IPv6 地址；在反向域名解析中，通过 IP6. ARPA 中的 PTR 记录将 IPv6 地址映射为主机名。我们基于 FreeBSD 平台下的 BIND 9 实现了对 IPv4 与 IPv6 的双向解析。

4.2 WWW

我们采用 Apache 作为 IPv6 的 WWW 服务器。对于客户端部分，IE、Netscape 等常用浏览器都能支持 IPv6 访问。但目前 IE 不支持直接使用 IPv6 地址访问 WWW 站点，而 Netscape 可以支持。

4.3 FTP

我们采用 Porftpd 服务器软件作为 FTP 服务器。对于 FTP 客户端，Unix 平台可以使用 ncftp，Windows 平台在安装 IPv6 协议栈后可使用 ftp。此外还有一些支持 IPv6 的第三方工具，如 smartftp、FileZilla 等。

4.4 Proxy

我们采用 squid 作为 IPv6 下的代理服务器软件，客户端只要拥有支持 IPv6 的浏览器即可使用代理，要注意的是如在代理设置中直接输入 IPv6 地址，会由于浏览器无法识别产生错误。应当在建立代理服务器的域名记录后，在浏览器代理设置中指定域名来设置代理。

4.5 Mail

我们对 Postfix 进行了修改，解决了 IPv6 下多协议如 SMTP、POP3、IMAP 通信与 MX 记录解析的问题，构建了支持 IPv6 的邮件服务器。

5 结论

本文结合我校 IPv6 网络建设项目的探索与实践，阐述了 IPv6 在园区网中实现及应用的关键问题。目前国内很少有单位开始在园区网中进行 IPv6 网络建设，因此本文为各机构、企业在园区网内进行 IPv6 网络建设提供了一定的借鉴意义和参考价值。当然，IPv6 网络建设还包括相关的管理、安全等，如需要支持 IPv6 的网络管理系统与网络安全系统等，这是我们下一步的研究重点。

参考文献

1 吴建平，CNGI 和 CERNET2. CERNET 十届年会“迎接下一代互联网的挑战”主题演讲，http://www.edu.cn，2003。

2 R. Hinden，S. Deering. Internet Protocol Version 6 (IPv6) Addressing Architecture. RFC3513，2003。

3 马严，IPv6 及其在下一代校园网中的部署，CERNET 十届年会“迎接下一代互联网的挑战”主题演讲，http://www.edu.cn，2003。

4 华为 3COM 技术有限公司，IPV6 网络技术教育汇报，第三届全球 IPv6 高峰论坛，2004。

5 刘鸿彬、王忍成等，台湾地区 IPv6 网络现况，世界电信网络，2003(1)。