IPv6 主干环境下的校园网接入

周渔，龚俭

(东南大学计算机系 江苏省计算机网络技术重点实验室 南京 210096)

摘　要：IPv6 主干网的开通预示着 IPv6 结束了试验阶段而开始全面部署，但在原有 IPv4 网络基础上进行 IPv6 的大规模接入是一个值得研究的新课题。该文以 CERNET 的双主干核心网、地区接入网以及校园网为背景，分析了在校园网接入 IPv6 时新的需求，针对这些需求给出了一个隧道接入平台，并将其与 6to4 方案进行了对比，结果表明其具有结构简单和通用性等优点。

关键词：IPv6 主干，校园网接入，隧道技术

中图分类号：TP393　　**文献标识码**：A

Campus Networks Access in IPv6 Backbone Environment

Zhou Yu　Gong Jian

(Department of Computer Science and Engineering, Southeast University, Nanjing 210096)

Abstract: The open up of IPv6 backbone indicates the end of IPv6 tryout and its all-around deployment, but deploying IPv6 on a large scale in the old IPv4 network is a new field that deserved research. Based on the CERNET dual backbone, regional access network and the campus networks, the paper analyzes the new demands of campus networks when they access IPv6, gives a tunnel access architecture according to these demands. The result of comparing this architecture with 6to4 shows its simple structure and generality.

Key words: IPv6 backbone, campus network access, tunnel techniques

1　引言

随着近年来用户数以及众多新型应用的急剧增加，基于 IPv4 的全球互联网已很难满足要求，具有众多良好特性的 IPv6 则由此应运而生，而全面采用 IPv6 的下一代互联网将提供更高效的服务。但由 IPv4 迁移到 IPv6 将是一个逐步且漫长的过程，两者必将共存相当长时间。IETF 对此进行了广泛研究，并已针对不同的情景和要求提出了相应的迁移技术，这些技术本身已比较全面和成熟，当前的研究点在于如何合理使用它们来部署 IPv6 网络。

IPv6 的试验阶段已经过去，很多国家和地区已陆续开始建设 IPv6 骨干网。在教育科研网方面，美国的 Abilene 和欧洲的 GEANT 等都在建设大型纯 IPv6 骨干网络；而作为 CNGI 骨干网之一的 CERNET2 实验网也于 2004 年 3 月开通，CERNET 将迎来 IPv6 网络建设与应用的快速发展时期。因此，在以往 IPv4 接入和管理的经验基础之上，研究探讨校园网的 IPv6 接入十分必要。

本文其余部分作如下安排：第一节介绍基本的迁移技术，第二节分析校园网接入环境和需求，第三节给出具体的接入方式，第四节进行分析和讨论，最后对全文进行总结。

2　基本迁移技术

目前存在的迁移技术大致分为两类[1]:一类是隧道技术，致力于穿越 IPv4 主干实现 IPv6 间的通讯，一类是协议翻译以及双栈技术，致力于 IPv4/IPv6 间的互操作。

隧道的基本思想是报文的封装，其建立方式有以下几种：一是手工建立；二是半自动隧道，如 Tunnel Broker 服务[2]；三是全自动隧道，如 6to4[3]，ISATAP，Teredo。双栈技术在节点的 IP 层完全实现 IPv6 和 IPv4，使其能同时处理两种报文，是 IPv4 和 IPv6 最简单的共存方式。但隧道和双栈都不能让纯 IPv4 节点和纯 IPv6 节点进行通信，此时需使用协议翻译，它实现了网络层，传输层或者应用层的协议转换，主要的协议翻译技术有 NAT-PT，TRT，BIS/BIA 以及 Socks64。

成功部署 IPv6 的关键是在不损害现有 IPv4 架构和服务的基础上进行逐步集成。在 CERNET 地区接入网环境下，实现双栈网络需要升级所有的路由器设备，一次性投资巨大，在目前不具有普遍性；而纯 IPv4 和纯 IPv6 节点之间的通信需求则更加稀少。因此，采用隧道技术来部署 IPv6 网络更有代表性。

3 校园网接入环境和需求

CERNET2 的骨干网为纯 IPv6，CERNET 的骨干网为纯 IPv4，两者构成了一个并行的双主干核心网络；而地区接入网被两个主干所共享，且现阶段大多数接入路由器为 IPv4，即校园网不能直接连接到 IPv6 主干。在这样的环境中，校园网除了保持原有的 IPv4 接入外，有两个新的需求：一是接入到 IPv6 主干，以便校内用户进行 IPv6 科研或开展新应用，二是根据策略分流特定应用的 IPv4 流量至负载相对较轻的 IPv6 主干，以充分利用其高带宽。对于带宽需求量大、跨域传输数据的网络应用来说，绕开负载较重的 IPv4 主干是提高其服务质量最直接的方法。

4 隧道接入平台

针对上述校园网在双主干环境中的接入需求，本文给出了一个针对教育网的隧道接入平台，以期为校园网提供高效、通用的接入服务。该平台的具体架构图如下：

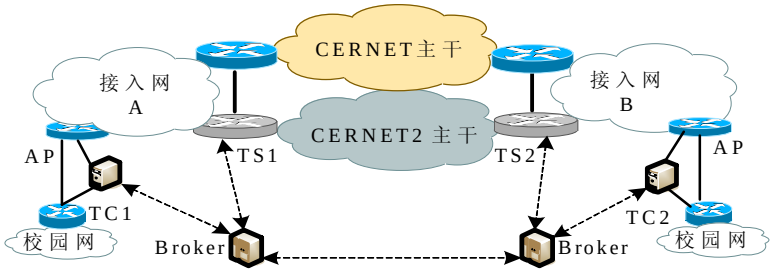

图 1 隧道接入平台架构

如图 1 所示，以两个地区接入网 A、B 为例，每个接入网内部署相应的隧道服务器(TS)和代理(Broker)，在校园网边界与其接入点(AP)之间部署隧道客户端(TC)。

4.1 IPv6 接入服务

该服务主要体现在 TS 和用户间 IPv6 over IPv4 隧道的创建，参与实体为 Broker、TS 和用户。用户有两种：一是可管理用户(USER)，如校园网，为其提供长期稳定的隧道服务；二是不可管理用户(ADHOC)，如校园网内尝试使用 IPv6 的主机，为其提供临时隧道服务。对于可管理用户，可以参考传统 TB 模型，由 Broker 作为服务的主要执行实体，在 Broker 上建立数据库，存储所有可管理用户的信息，并由 Broker 负责用户身份的注册和认证、IPv6 地址前缀分配以及隧道的建立；而对 ADHOC 用户，则首先通过某种机制去发现并选择可用的 TS，然后不通过 Broker 而直接向 TS 发出隧道请求，由 TS 负责隧道的创建。

4.2 IPv4 流量分流服务

分流在校园网边界进行，包含两个动作，一是根据策略筛选出需要分流的 IPv4 报文，二是采用 IPv4 over IPv6 隧道技术对选出的报文执行分流。其中策略应由校园网管理员制定，并以策略路由或 ACL 列表的方式配置在校园网边界路由器上，从而将特定应用(如视频流、大规模数据传输)的报文转发至 TC 而不是 AP 上。而 TC 和 Broker 则在执行分流的过程中起主要作用。

以图 1 为例，在接入网 A 中，当初始 IPv4 报文到达 TC1，TC1 首先通过某种机制找出该报文目的地址所在校园网的 TC(假设为接入网 B 中的 TC2)的 IPv6 地址，并以此作为 IPv6 目的地址对原始 IPv4 报文作 IPv6 封装。封装后的 IPv6 报文通过 TC1 和 TS1 之间的 IPv6 over IPv4 隧道到达 TS1，进入 IPv6 主干后被路由至接入网 B 中的 TS2。TS2 根据其 IPv6 路由表将报文通过 IPv6 over IPv4 隧道送至 TC2 并执行解封装，原始 IPv4 报文被正确送至目的主机。

在上述过程中，TC1 和 TC2 之间自动创建了 IPv4 over IPv6 隧道，而创建该隧道的前提是得到原始 IPv4 报文的目的地址与 TC2 的 IPv6 地址之间的映射。可以用校园网地址范围注册分发机制来解决这一问题：由 TC 向本地 Broker 注册其校园网 IPv4 地址范围与 TC 的 IPv6 地址之间的对应关系，各地区网的 Broker 之间动态交换该信息并保持一致性；当 TC 得知 IPv4 目的地址时，向本地区的 Broker 查询便可获取对端 TC 的 IPv6 地址。

4.3 隧道的管理

IPv6 over IPv4 隧道由 Broker 负责管理，而 IPv4 over IPv6 隧道的管理则由 TC 负责。对于前者，某些隧道具有长期性，譬如校园网与 TS 之间建立的隧道，而有些具有临时性，如 ADHOC 用户与 TS 之间建立的隧道，Broker 会对此区别对待，并以合理的机制进行垃圾处理工作，控制系统资源的使用；对于后者，通常一个特定网络应用的会话就会导致一条隧道的建立，隧道生灭周期频繁，因此 TC 上对隧道资源的管理则显得更加重要。

5 分析和讨论

5.1 可扩展性问题

在部署 IPv6 接入服务时，用户总量可能会非常大，如果不采取相应措施，所带来的结果是资源耗尽和服务失效，因此必须考虑可扩展性问题。由于 TS 承受去往该地区网的所有 IPv6 流量，因此解决问题的关键是以负载均衡的方式来部署多台 TS。由 Broker 实时检测每台 TS 的负载信息，通过算法为可管理用户选择合适的 TS；而由于 TS 需要直接接收 ADHOC 用户的请求，该负载均衡策略必须使得 ADHOC 用户能找到合适的 TS 为其服务。可以考虑基于 Anycast 或 DNS 的负载均衡方式，使得该 TS 集群的服务以统一方式提供给用户，其内部负载平均分布，不存在单一失效点。

5.2 与 6to4 方案比较

除了使用上述所提出的隧道平台为校园网提供 IPv6 接入服务外，还有 6to4 方案可供考虑。6to4 作为一种全自动的隧道技术，在路径优化和系统管理方面有优势，但针对教育网双主干的环境，存在以下不足。首先，6to4 要求使用专有地址，站点内主机的 IPv6 地址依赖于 IPv4 地址，降低了其可扩展性；而且由于机制本身的原因，6to4 不支持组播。第二，6to4 的规范指出当 6to4 站点和纯 IPv6 站点通讯时需要 6to4 relay 的支持，但这会导致报文往返的路径不对称，即源自 6to4 站点、前往纯 IPv6 站点的报文所经过的 relay 与返回 6to4 站点的报文所经过的 relay 不能保证是同一个。路径不对称会引发不容易检测通信故障、不能保证端到端 QoS、用户没有选择可信 relay 的自主性等问题。[4]提出一种可行方法，即在所有的 relay 之间建立 BGP4+连接，并且 6to4 站点向其缺省 relay 注册地址前缀，但这样大大增加了配置的复杂性，除此之外，目前没有更好的解决办法。第三，6to4 只是针对 IPv6 over IPv4 隧道的一种技术方案，并没有考虑在双主干环境下使用 IPv4 over IPv6 隧道进行流量分流的要求，因此无法为特定应用提供分流服务。

而本文提出的隧道平台在诸多方面有优势。它能以不同的策略服务于不同类型的用户，而且由于服务结构简单，不存在 relay 的概念，有利于端到端 QoS 的保证和故障的监测排除；

另外，该平台集成了 IPv4 流量分流服务，与 IPv6 接入服务一起以统一的接口提供给校园网用户；同时，由于采取了负载均衡措施，可扩展性较强。其不足之处在于，提供分流服务时，由于地址映射机制限于教育网，因此网络会话的两端只能都位于教育网内。但这一点并不影响分流服务的部署，因为完全可以让往返教育网外的流量通过 IPv4 主干进行传输。

6 结语

IPv6 网络正开始进入全面部署时期，对不同的网络环境应采取不同的部署策略和技术。本文则针对 CERNET 环境和校园网需求提出了一种隧道接入平台，该平台具有简单、通用、可扩展性强等优点。但目前在教育网内大规模部署 IPv6 还没有经验可以参考，因此在具体实践时还需要进行更详尽的考虑。

参考文献：

[1] Tatipamula M, Grossetete P, Esaki H. IPv6 Integration and Coexistence Strategies for Next-Generation Networks. IEEE Communications Magazine, Jan. 2004:88-96.

[2] Durand A, Fasano P, Guardini I, etc. IPv6 Tunnel Broker. RFC3053, 2001.

[3] Carpenter B, Moore K. Connection of IPv6 Domains via IPv4 Clouds. RFC3056, 2001.

[4] Yuichiro Hei, Katsuyuki Yamazaki. Traffic Analysis Worldwide Operation of Open 6to4 Relays for IPv6 Deployment. IEEE SAINT'04, 2004:265-268

作者简介：

周渔（1980 -），男，江苏泰兴人，东南大学计算机系硕士生，主要研究方向为 IP 组播和下一代互联网。

龚俭（1957-），男，上海人，东南大学教授、博士生导师，CERNET 专家委员会委员，主要研究领域为网络安全、网络体系结构。