

骨干网IPv4/IPv6协议转换网关设计

张 鹏 , 杨国渝

(电子科技大学电子工程学院 成都 610054)

【摘要】阐述了骨干网上部署IPv6网络中,解决既要满足IPv4和IPv6网络互联互通的需要,同时减少IPv4地址消耗的问题。比较了几种比较成熟的IPv4/IPv6转换技术,提出了在IPv4/IPv6网络边界的协议转换网关上使用改进的NAPT-PT协议转换方案,指出了在城域网环境下采用NAPT-PT方案的不足和实现过程中的解决办法。

关键词 网络地址翻译端口扩展和协议转换; 骨干网; IPv4协议; IPv6协议

中图分类号 TN915.43; TP393.08 文献标识码 A

IPv4 /IPv6 Protocol Transition Mechanism on Backbone

ZHANG Peng , YANG Guo-yu

(School of Electronic Engineering, UEST of China Chengdu 610054)

Abstract In this paper, we analyze the problem that we must implement the interconnection of IPv4 and IPv6 network while decrease the consumption of the IPv4 addresses when we employed IPv6 on Backbone. Then, based on the comparison of several issues of IPv4/IPv6 transition, we provided a suggestion that we can integrate a NAPT-PT system in the gateway on the edge of IPv4 and IPv6 net. Additionally, we introduced the shortcoming of the NAPT-PT system on the MAN and the key to them in the realization.

Key words NAPT-PT; backbone; IPv4 protocol; IPv6 protocol

IPv4作为网络的基础协议而广泛地应用在Internet和难以计数的专用网络上,尽管它是一个令人难以置信的成功的协议,但是工程师和设计人员早在80年代初期就已经发现IP地址空间随着Internet的发展只能支持很短的时间。而且,随着联入Internet的主机数量的爆炸性增长,骨干路由器上的路由表项也以几何级数增大,骨干路由器逐渐成为网络性能的瓶颈。随着电信网络和数据通信网络的逐步融合,IPv4显示出不能满足服务质量保证、节点的移动性和安全性要求,因此对于IP协议的改进逐步显得必要。IETF在90年代初开始正式研究、讨论下一代IP(IPng)。最早的描述IPv6及其支持协议的RFC标准于1996年发表,经过完善,IPv6被选为下一代网络(NGN)的网络层核心协议^[1]。

据统计截至2003年6月,我国的上网计算机数量已达到2572万台,上网用户6800万,而分配到的IP地址却只有3000万个。加上各交换、路由设备和移动终端、特种设备对IP地址的消耗,以及在分配过程中几乎不可避免的地址浪费,实际上我国的IP地址数量是极其紧张的。我国人均分配的IP地址为:0.023,远低于美国(5.519)日本(0.815)等国家。IP地址的匮乏已经开始严重制约我国数据通信网络的进一步发展。

收稿日期:2003-10-09

基金项目:中国科学院知识创新工程“IPv6关键技术研究”项目

作者简介:张鹏(1979-),男,硕士,主要从事嵌入式网络系统及数字微波通信网络方面的研究;杨国渝(1947-),男,博士,教授,主要从事数字微波通信方面的研究。

1 问题的产生

由于现有Internet的巨大规模, 更换网络层协议将是一个庞大的工程。对于最终用户来说, 感受不到IP地址匮乏带来的问题; 对于网络管理者, 虽然为IP地址的短缺而苦恼, 但是网络层协议的升级要求为Internet上的每个主机和路由器都找到并安装新版本的网络软件, 考虑到目前已经有大量网络连接到Internet, 而且有很多不同的平台运行着IPv4, 因此整体切换式的升级是很难接受且难以实现的。

向IPv6过渡将是一个相对缓慢的过程。预计IPv4和IPv6将长期共存, 也许将永远共存。IETF注意到了这个问题, 在RFC 2893、RFC 2185、RFC 2071以及RFC 2072等文档中都涉及向IPv6过渡的讨论。这些过渡方案是为了实现在IPv4网络海洋中的各个IPv6岛屿之间的通信和实现IPv6与IPv4网络之间的互通。

IPv6对IPv4做了多个改进, 但其最大优势在于地址空间远大于IPv4。在骨干网上部署纯IPv6网络, 最关键在于能实现与传统IPv4网络的透明互通。由于现有IPv4地址不足, 不能保证给每个IPv6节点分配一个可用的IPv4地址, 因此, 在开发IPv6/IPv4边界网关时有必要选择一种合理的IPv4/IPv6协议转换方案。

2 现有的IPv4/IPv6转换技术的比较

目前已有的IPv6/IPv4互通策略主要有3种: 1) 地址映射方法, 就是将IPv4地址映射为IPv6地址, 或者相反, 如NAT - PT, NAPT - PT^[2]; 2) 双栈方法, 即主机在同一网络接口上运行IPv4/IPv6栈, 同时处理IPv4和IPv6包。这类技术包括有限双栈和双栈; 3) 代理方法, 就是源主机将服务请求发送给一个双栈代理服务器, 代理服务器建立与目的主机的连接, 再转发给源主机, 这种转换技术有: SOCK64, TRT。

双栈技术其核心在于节点的网络层协议采用双协议栈, 能同时处理IPv4/IPv6数据报, 应用可以根据要选择协议栈^[3]。采用双栈技术的节点必须各配置一个IPv4/IPv6地址。表面上看这是一个比较彻底的IPv4/IPv6互联解决方案, 但其缺陷仍很明显: 1) 它要求所有的网络节点都必须支持双协议栈, 这是一个庞大的工程, 难度巨大; 2) 它要求所有网络节点都同时配置IPv6和IPv4地址, 若IPv4地址不足, 将无法正常工作; 3) 双栈节点与IPv6主机互联, 必须升级涉及到IP地址的应用层协议和软件以支持IPv6, 代价巨大。虽然可以在IPv6终端上配合使用BIS(Bump-in-the- Stack)或者BIA(Bump-In-the- APD)解决, 但是需要升级IPv6主机的系软件, 一旦IPv6网络扩大, 将不再能满足需要, 因此不能用于骨干网, 只能用于早期小范围的过渡。

SOCK64(Socks-based IPv6/IPv4 gateway)是一种在IP层之上实现的双栈技术^[4]。SOCK64通过DNS欺骗和socket中继来实现IPv4/IPv6主机之间的通信。SOCK64替换了应用层API中部分函数, 当需要与IPv4网络通信时, 就建立一个与SOCK64代理服务器的socket连接, 由SOCK64向IPv4主机提出服务请求, 再将获得的数据转发给IPv6源主机。其最大优势在于, 不需要对客户端做大的修改, 只需升级到socks v5。但它的问题也很明显: 1) 它破坏了TCP/IP的分层体系, 因为源主机和目的主机是通过代理服务器实现一种虚连接, 不利于优化网络结构, 安全机制也无法实施; 2) 代理服务器在应用层实现, 因此负荷很重, 不能用于骨干网; 3) SOCK64使用UDP与代理服务器通信, 很难适应同时使用TCP/UDP的应用。

网络地址翻译、端口扩展及协议转换NAPT-PT是在传统的网络地址翻译NAT基础上发展起来的IPv4/IPv6协议转换技术^[5]。其核心是在一个边界网关上, 修改IP包头, 将IPv6会话号(地址、端口对)动态映射为IPv4会话号(地址、端口对), 记录相应的映射关系。在收到IPv4报文时, 检查是否有相应的映射关系存在, 如果存在就按照记录将其转换为IPv6报文, 否则丢弃。NAPT-PT使用了NAPT(Network Address and Port Translation)技术, 在转换网关上将源会话号(源IPv6地址:端口对)动态替换为IPv4会话号(IPv4地址:端口对)。由于每个IP地址拥有63 k个端口供用户使用, 因此, 使用NAPT-PT技术在协议转换过程中减少对IPv4地址的消耗。NAPT-PT不需要更改用户终端的软硬件, 对于用户是完全透明的。NAPT-PT本身也有一些不足, 但是都可以克服, 因此这是目前在骨干网上部署IPv6网络最好的与IPv4互通的转换技术。

3 NAPT-PT的实现

考虑到骨干网上的高吞吐量, 为了提高协议转换效率, 本文开发了一个专用的转换网关, 使用两片Intel IXP1200网络处理器, 可以提供全双工2 Gb/s的带宽, 足以满足边际骨干网接入的需要。其性能远远超过用

纯软件实现的协议转换网关的性能。

在具体实现过程中,在边界转换网关上,维护一个存放可分配的IPv4地址、端口对的地址池和一个源IPv6地址、端口与分配的IPv4地址、端口的对应状态表。收到的IPv6数据报,首先检查其目的地址是否为兼容IPv4的IPv6地址,否则丢弃报文。然后将目的为IPv4网络的IPv6报文头按照SIIT(Stateless IP/ICMP Translator)转换为IPv4报文头,其传输层以上的包净荷保持不变。查找状态表,如果已有对应的表项,根据其映射关系,用表中的IPv4地址和端口替换原报文的IPv6地址和端口;否则,从转换网关的IPv4地址池中分配一个IPv4地址和端口,替换源报文IPv6地址和端口,将源报文的IPv4兼容IPv6地址转换为IPv4地址,完成IP层报文的协议转换。当IPv4主机的返回报文到达时,查表,找到相应的IPv6地址和端口,替换其目的地址和端口,将其源地址转换为IPv4兼容IPv6地址。如果没有对应的表项,则丢弃报文。这样就完成了整个转换过程。地址映射状态如表1所示。

表1 地址映射状态表

IPv6地址	IPv6端口	IPv4地址	IPv4端口
3ffe:8330::9fe2:2701	2341	159.226.39.1	5001
3ffe:8330::9fe2:2701	2345	159.226.39.1	5003
3ffe:8330::9fe2:2705	5678	159.226.39.2	5034

从表中得知:

- 1) IPv6主机向IPv6 DNS服务器提出域名解析请求;
- 2) IPv6 DNS服务器向其返回目的主机IPv6地址,如果是IPv4网络主机,则返回IPv4兼容IPv6地址;
- 3) IPv6路由器解析收到的报文,将目的地址是IPv4兼容IPv6地址的报文选路到NAPT-PT网关;
- 4) NAPT-PT网关完成IP报文的协议头部转换和地址更改,将转换后的报文发向IPv4网络;
- 5) 返回的IPv4报文被选路到NAPT-PT网关,经过报文头部修改和地址转换,选路到目的IPv6主机。

NAPT-PT转换网关的网络环境如图1所示。

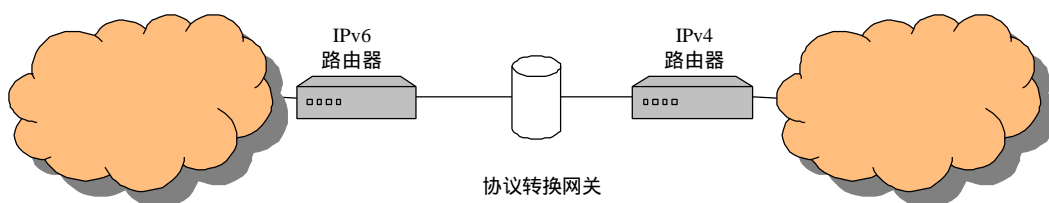


图1 转换网关的网络环境

注:如果没有IPv6 DNS服务器,就需要在协议转换网关上建立DNS应用级网关(Application Level Gateway, ALG),将IPv6终端的DNS服务器地址配置为IPv4 DNS服务器的兼容IPv6地址,NAT-PT的具体工作流程如图2所示。所有表项都应该有一个计时器,当计时器到达设定的门限时,就删除表项,回收IPv4地址和端口。该门限值如果过大,可能造成地址池的IPv4地址资源迅速枯竭,无法满足新的IPv6会话的转换服务请求;如果过小,又可能造成已连接会话频繁被中断,服务质量下降。因此,应该根据具体网络大小、会话数、可用IPv4地址数量、数据流量、应用类型,在试验、测试的基础上,设定一个优化值。同时,为了保证正在进行的会话不被中断,当有某表项对应的数据报穿越网关时,对该表项的计时器值进行刷新。

由于NAPT-PT继承自NAT,因此也具有其固有的一些问题为:1) 它只支持由IPv6端主动发起的会话,禁止由IPv4端发起的会话,这不利于IPv6服务器对IPv4网络提供服务;2) 由于报文在转换网关上修改了IP地址和报文头,一些在报文中夹带了IP地址的应用层协议(如,DNS,FTP,SIP)将会失败;3) 由于对IP头的修改,任何传输层以下的安全协议(如,IPsec)将无法实施。

对于问题1),目前采取在转换网关上预留地址和端口的方法加以部分解决。其具体做法是:在转换网关上预留部分IPv4地址和端口,作为IPv6服务器对IPv4网络提供服务用的保留地址、端口,在其上静态绑定与

相关IPv6服务器地址的对应关系,允许外部IPv4主机对这些地址、端口发起主动会话。2)和3)都可以通过在转换网关上建立ALG加以解决。由于采用网络处理器为硬件解决方案,可以很方便的在其上建立新的ALG或其他应用而不至于对系统做大的修改。同时NAPT-PT还有很大的改进余地。由于其来源于传统的NAT,任何对NAT的改进方案都能很容易的移植到NAPT-PT上。比如,进一步可以考虑在转换网关和IPv6 DNS服务器上集成改进的RSIP(Real Specific IP)。RSIP是目前IETF NAT工作组正在开发一个新的协议。采用它可以解决在转换网关上建立各种ALG造成的工作量较大,而且系统的转换效率下降的问题。同时,IPv4主机不能主动发起会话的问题也不再成立。实现方案中要求改进RSIP,支持IPv6,同时终端应用层必须支持从兼容IPv4的IPv6地址中自动获取IPv4地址。RSIP最大的问题在于需要用户终端系统的支持。但是RSIP是一个很彻底的解决应用层协议透明穿越NAT的方案,如果被采用为网络系统标准,终端对他的支持就不会成为问题。至于3),由于现在的安全协议主要是在应用层完成的,在网络层及以下的安全协议并不多,可以在转换网关上集成ALG来解决。

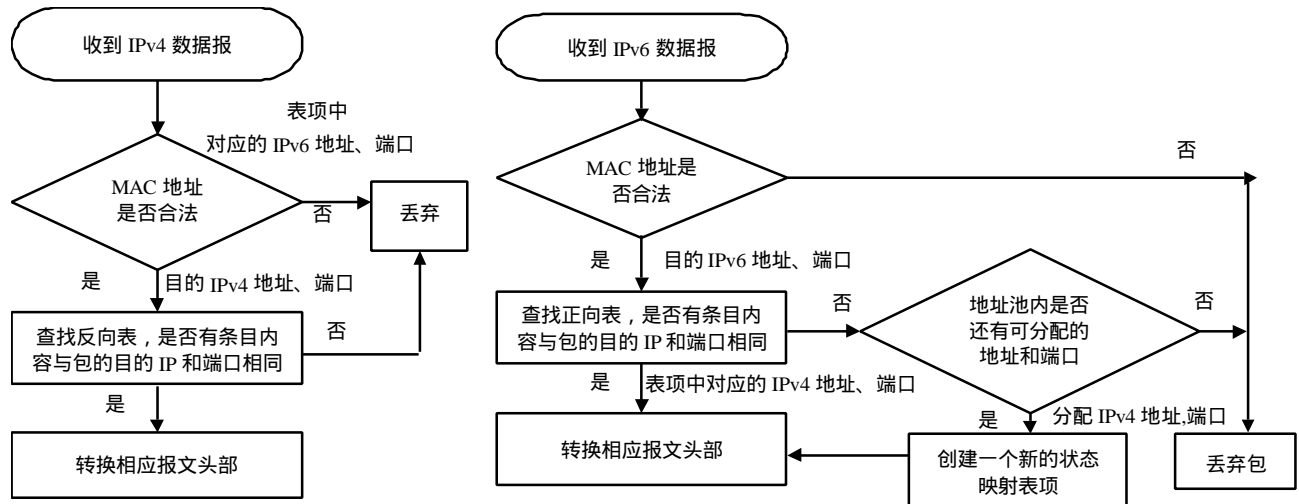


图2 协议转换网关处理流程

4 结束语

采用IPv6协议,建设IPv6网络可以有效解决我国IPv4地址匮乏的问题,对于我国数据通信技术的发展有着重要意义。本文比较了目前比较流行的几种IPv4/IPv6互通转换技术,提出NAPT-PT方案是最适合我国国情的协议转换模型,描述了在实施过程中需要考虑的问题和解决方法。采用NAPT-PT技术方案的试验网关,在城域高速光纤网络项目的测试中实现了两网的线速转发和正确互通。

参 考 文 献

- [1] Kaat M, Overview of 1999 IAB network layer workshop, rfc2956[S]. Internet Engineering Task Force, 2000
- [2] Tsirtsis G, Srisuresh P. Network address translation - protocol translation (NAT-PT), RFC 2766[S]. Internet Engineering Task Force, 2000
- [3] Alain D. Draft-durand-v6ops-dualstack-vs-natpt-00[S]. Internet Engineering Task Force, 2003
- [4] Egevang K, Francis P. The IP network address translator(NAT), RFC1631[S]. Internet Engineering Task Force, 1994
- [5] Kitamura H. A SOCKS-based IPv6/IPv4 gateway mechanism, RFC3089[S]. Internet Engineering Task Force, 2001

编 辑 刘文珍