一种基于UDP的IPv4 over IPv6的隧道方案

沈庆伟[1]，杨寿保[2]，孙伟峰[2]

(1. 安徽建筑工业学院计算机与信息工程系 合肥 230022; 2. 中国科学技术大学网络中心 合肥 230026)

【摘要】从IPv4向IPv6过渡，需要解决IPv4网络和IPv6网络之间的互联互通问题。为实现通过IPv6连接IPv4孤岛，利用IPv6高带宽的特点提出一种基于UDP协议的处理简单、处理开销小的IPv4 over IPv6隧道过渡方案BoIP。描述BoIP工作原理和具体实现，实验床测试结果表明，BoIP可以实现两个IPv4局域网通过IPv6网络透明连接。

关 键 词 IP层网桥; IPv4 over IPv6隧道; 过渡; 用户数据报协议
中图分类号 TP393.01 文献标识码 A

An IPv4 over IPv6 Tunnel Solution Based on UDP

SHEN Qing-wei[1]，YANG Shou-bao[2]，SUN Wei-feng[2]

(1. Dept. of Computer and Information Engineering, Anhui Institute of Architecture and Industry Hefei 230022;
2. Dept. of Computer Science, University of Science and Technology of China Hefei 230026)

Abstract The problem of interconnecting and communicating between IPv4 network and IPv6 network in need to be solved while transiting from IPv4 to IPv6. To connect IPv4 islands through IPv6 network, an IPv4 over IPv6 tunnel solution based on User Datagram Protocol (UDP) called BoIP is proposed. BoIP uses high bandwidth of IPv6 and runs simply and low-costly. Working processes and implementation are described. Experiment results on the test-bed show that BoIP can transparently connect two IPv4 networks through IPv6 network.

Key words bridge over IP; IPv4 over IPv6 tunnel; transition; user datagram protocol

IPv6协议解决了IPv4协议中地址枯竭、安全性不足以及移动性差等问题。从IPv4过渡到IPv6是一个渐进而漫长的过程，两者将共存相当长时间。为了实现平稳过渡，IETF对此进行了广泛研究，并针对不同的网络环境和应用要求提出了相应的过渡技术。它们可以分为三类：(1) 双协议栈(Dual Stack)；(2) 隧道(Tunnel)；(3) 地址/协议翻译(NAT-PT)。双协议栈在网络节点上安装IPv4和IPv6两种协议栈，使之能够同时支持两种协议的通信。双协议栈互通性好，易于理解；但是需要给每个网络设备和终端分配IPv4地址，主要和其他技术结合使用。NAT-PT是一种单栈IPv6节点和IPv4节点间的互通方式，实现方法比较复杂，处理开销较大。隧道技术在过渡初期主要用于IPv6孤岛通过IPv4网络互连，同时在IPv6占主导后，可反过来作为IPv4孤岛的连接方式。

随着IPv6的大规模发展，出现骨干IPv6网络，IPv6上引入大量业务，同时仍然有大量IPv4业务存在。如在CERNET2搭建了一个纯IPv6骨干网，已经有多所科研院所和高等院校部署了IPv6主干网络，但是还要保持原有IPv4网络，需要IPv4 over IPv6隧道技术或者协议转换技术。目前IPv6 over IPv4隧道技术应用较广，也较成熟，而IPv4 over IPv6隧道技术则不够成熟[1]，需要进行研究。本文研究IPv4 over IPv6隧道的封装机制，提出一种基于用户数据报协议(User Datagram Protocol，UDP)的IPv4 over IPv6的隧道方案BoIP。

1 隧道技术

隧道技术通过报文封装的方式连接被其他类型网络分隔的同一类型节点或网络。隧道有两个端点，隧道的入口和出口点。隧道的端点可以是主机或者路由器，必须是双协议栈的节点，它们连接两种网络，进行报文的封装与拆封[2]。隧道技术在IPv4向IPv6网络过渡初期是连接IPv6单独子网的基本手段。如图1所示，IPv6 over IPv4隧道在IPv4网络上建立隧道连接孤立的IPv6节点。在隧道入口处IPv6分组被封装在IPv4分组中，IPv4的源地址和目的地址分别是隧道的入口和出口的IPv4地址。封装后的分

收稿日期：2006 – 05 – 10
基金项目：安徽省教育厅科研资助项目(2004kj096；2005kj07)
作者简介：沈庆伟(1967 –)，女，副教授，主要从事网络过渡技术、QoS等方面的研究.

组通过IPv4的路由体系传输，在隧道出口处恢复被封装的IPv6分组并转发至目的节点。

图1　IPv6 over IPv4隧道

IPv6 overIPv4隧道分为配置型隧道和自动型隧道两种。(1) 配置隧道是由隧道端点所在网络的管理员手工配置建立，隧道的端点地址由配置来决定，不需要为站点分配特殊的IPv6地址，适合用于经常通信的IPv6节点之间；(2) 自动隧道不需要预先配置隧道的目的地，隧道端点地址由兼容IPv4的IPv6目的地址所决定，适合用于单独的主机或不经常通信的节点之间。自动隧道通常有Tunnel Brokers[3]、6to4、ISATAP、6over4、Teredo等几种优化方式。

隧道技术只要求在隧道的入口和出口进行修改，对其他部分没有要求，因而技术实现非常容易。其优点在于隧道的透明性，IPv6主机之间的通信可以忽略隧道的存在。在过渡初期，它不需要大量的IPv6专用路由器和专用链路，可以明显减少投资成本[4]。

隧道技术不仅能让IPv6数据包在IPv4网络中传送，同样也适用于在IPv6网络中传送IPv4数据包。在IPv6占主导以后，可以IPv4 over IPv6隧道作为IPv4网络的连接方式，如图2所示。报文的封装与拆封所用IP协议与IPv6 over IPv4隧道相反。

图2　IPv4 over IPv6隧道

目前，隧道技术的报文封装与拆封大多在IP层，隧道端点需要对每一个进行判断、加隧道协议头、解隧道操作，解隧道后还要进行判断和转发的操作，对边缘路由器的性能要求高，边缘路由器可能会成为瓶颈。为简化隧道操作，本文提出一种基于UDP协议的隧道方案。

2　基于UDP的IPv4 over IPv6的隧道方案BoIP

2.1　BoIP的设计

IPv4 over IPv6隧道是把IPv4的分组封装在IPv6分组中，在IPv6网络中开辟隧道。考虑到IPv6网络的高带宽和对QoS的保证，为简化路由器根据每个数据包判断并进行封装与拆封的过程，采用IP层之上的UDP协议来实现隧道连接，避免对数据包的跨层判断和解析，把数据链路层的数据作为UDP的净荷。UDP只有8个字节固定长的头标，采用UDP协议构造的隧道增加的负荷小、效率高。IPv6的UDP头标包含校验和提供检测数据报内差错的功能，保证数据报本身无差错。图2中，路由器是隧道的端点，必须支持双栈协议，负责数据包的封装与拆封。路由器捕获IPv4网络的数据链路层报文，加IPv6 UDP报头，通过IPv6网络送往隧道的另一个端点；在出口路由器上将IPv6 UDP报头去掉，送往IPv4网络。由于是对链路层的数据进行操作，IPv6网络对IPv4网络内的主机类似透明网桥的功能，所以把这种方案称为BoIP(Bridge over IP)。

2.2　隧道方案的实现

目前IPv4网络多为以太网，BoIP中二层数据为以太帧。以太网的帧格式如图3所示，以太帧是可变长度的，但帧的长度不能小于64 B或大于1 518 B。

8 B	6 B	6 B	2 B	46～1 500 B	4 B
前同步码	目的地址	源地址	帧类型	帧数据	CRC

图3　以太网帧格式

在以太网上传输的每一帧中都包括源站和目的站的物理地址、一个前同步码、类型字段、数据字段和循环冗余校验码(CRC)。帧类型字段包括一个16b的整数，用来识别此帧上所载数据的类型。该字段非常重要，它意味着以太网的帧是自识别的。当一个数据帧到达路由器时，操作系统根据帧类协议，在数据链路层上不但可以抽取到IP数据包，还可以抽取其他链路层以上协议层的数据包。

BoIP的隧道端点抓取数据包及处理方法如图4所示。(1) 抓取链路层的数据包：用Socket(PF_ACKET，SOCK_RAW，htons (ETH_P_ALL))创建一个套接字，用来处理所有类型的帧。同时将网卡设置成混杂模式(Prosmiscuous Mode)，这样网卡能捕

获发送给其他主机的所有数据帧。只要得到数据链路层的数据，就可以得到包含其中的IP数据包以及其中的TCP数据或UDP数据；(2) 抓取所有链路层数据包，判断是否为进来的数据包：类型为“PACKET_OUTGOING”表示为出去的数据包，这样的数据包不做处理；(3) 判断是否含有UDP数据包 如果不是，说明这些链路层数据包是IPv4网内的数据，把这些数据加上IPv6 UDP报头，发送到IPv6网络指定地址的主机(隧道端点)；(4) 如果是UDP数据，还要判断是否为本机封装的UDP数据：如果不是则去掉UDP报头，发送到本地IPv4网络。LINUX环境下，使用send()、recv()、sendto()和recvfrom()函数，正确设置相应的参数就可实现上述功能[5]。

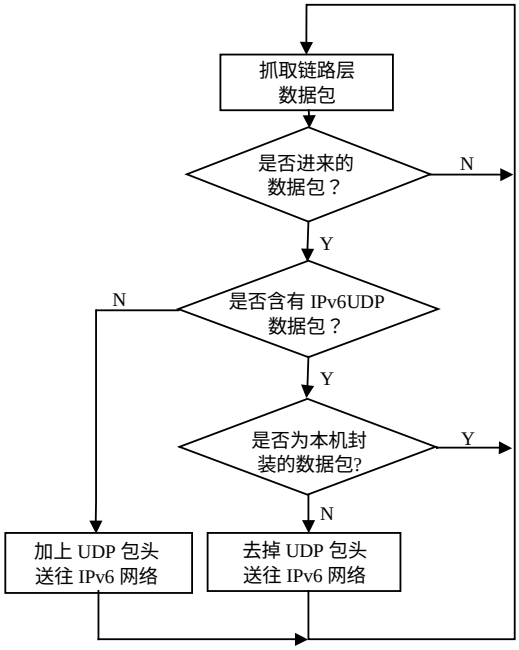

图4 隧道端点工作流程

3 BoIP的实验及结果分析

3.1 BoIP的实验

结合实际情况，设计实验场景如图5所示。双栈主机HA和HB分别作为隧道的端点，NIST为纯IPv6主机并运行NIST模拟IPv6的网络延迟。其中HB的eth1接入校园网，网段为202.38.64.0。MN运行的为Windows XP系统，HA、NIST、HB运行的是RedHat9操作系统，主机NIST运行软件NIST模拟IPv6网络，HA和HB运行本文编写的BoIP软件。编译后的可执行文件名为boip。实验床的地址配置如下：

NIST：eth0: (至HB)2001:250:5400::2/80
eth1: (至HA) 2001:250:5400:0:2::/80

HB：eth0: 202.38.64.185/25，属于202.38.64.0网络
eth1: (至NIST)2001:250:5400::/80

HA：eth0: (至NIST)2001:250:5400:0:2::1/80
eth1: (MN接入)10.2.0.254

HA主机运行命令：boip eth0 2001:250:5400:0:2::1 9001 2001:250:5400:: 9001

HB主机运行命令：boip eth0 2001:250:5400:: 9002 2001:250:5400:0:2::1 9002

其中，eth0为所要抓包的网卡设备；两个地址分别为本地IPv6地址和远端IPv6地址；9001和9002为socket的端口号。因为网卡设为混杂模式，MN的IPv4地址是多少并不相关，也可以设为IPv4局域网地址。

MN为IPv4主机，连接到HA的eth1，网卡配置使用DHCP协议。在此实验场景下，笔记本MN可以自动获取校园以太网的IP地址202.38.64.202，并同校园网内其他IPv4主机一样与校园网正常通信；可以进行Web浏览、视频点播等操作，速度没有受到影响。

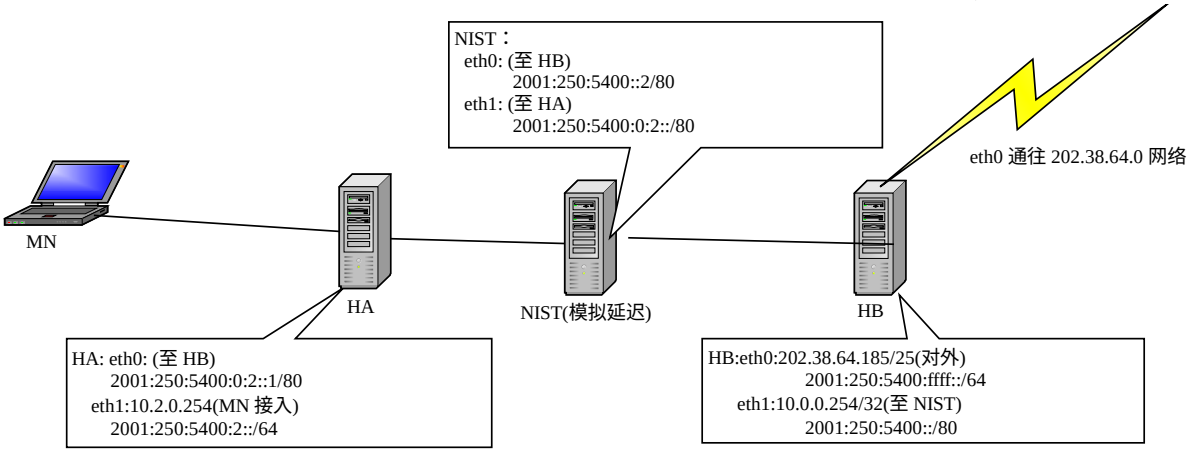

图5 IPv4 over IPv6隧道实验场景图

(下转第624页)

在大量的注册表数据中发现可疑内容，将是下一步研究的重点。此外，如何与其他检测方式，如进程检测相结合来进行全面的恶意程序检测和全面分析也是下一步研究的方向。

参 考 文 献

[1] CHRISTODORESCU M, JHA S. Testing malware detectors[C]//In Proceedings of the ACM SIGSOFT International Symposium on Software Testing and Analysis 2004(ISSTA'04). Boston USA: ACM SIGSOFT, ACM Press, 2004: 34-44.

[2] JAMES R, BUTELER I I. Detecting compromises of core subsystems and kernel functions in windows NT/2000/XP [D]. Baltimore USA: University of Maryland, 2002.

[3] CONOVER M. 恶意代码剖析和Rootkit检测[EB/OL]. www.xfocus.net/projects/Xcon/2005/Xcon2005_Shok.pdf, 2005-06-15.

[4] Microsoft Knowledge Base. Description of the Microsoft Windows registry[DB/OL]. http://support.microsoft.com/kb/256986/en-us, 2006-02-21.

[5] Clark. Security accounts manager[DB/OL]. http://www.beginningtoseethelight.org/ntsecurity, 2006-03-02.

[6] HOGLUND G. Nt rootkit - the original and first public NT ROOTKIT[DB/OL]. https://www.rootkit.com/vault/hoglund/ rk_044.zip, 2006-03-02.

[7] Fireworker. Kernel-mode backdoors for windows NT [DB/OL]. http://www.phrack.org/archives/62/p62-0x06_Kernel_Mode_Backdoors_for_Windows_NT.txt, 2006-03-02.

[8] HOGLUND G, Butler J. Rootkits: subverting the mindows kernel[M]. Boston, USA: Addison Wesley Professional, 2005.

[9] PJF. The homepage of iceSword[DB/OL]. http://pjf.blogone.net, 2006-03-02.

[10] HAGEN P N, OFFLINE N. TPassword & registry editor [DB/OL]. http://home.eunet.no/-pnordahl/ntpasswd/, 2006-01-13.

编 辑 孙晓丹

(上接第610页)

实验证明，BoIP的隧道技术可实现IPv4孤岛的连接，并没有出现延迟增大、连接次数增多的现象。

3.2 分析与讨论

目前，IPv4 over IPv6隧道技术还没有统一的标准，国际IETF组织正在为该技术建立专门标准工作组，制定相关的国际系列标准。对比已经成熟的IPv6 over IPv4隧道技术，BoIP改进了报文的封装方式，简化了报文的封装操作。基于IPv6网络高带宽、安全和QoS等功能，BoIP采用UDP协议构造隧道，具有简单、高效的特点。

BoIP能使IPv4孤岛透明地通过IPv6主干网互连，并不失端到端的连接性。对于带宽需求量大、跨域传输数据的IPv4网络应用，它还可以作为分流IPv4网络的数据至负载相对较轻的IPv6主干网以利用IPv6高带宽的一种方法，实现IPv4端到端的高性能连接。

4 结 束 语

IPv4 over IPv6隧道技术是一种重要的IPv4网络向IPv6网络过渡的技术。随着大规模IPv6主干网的建设，会出现IPv4网络孤岛，需要通过IPv4 over IPv6隧道互连，从而实现最后的过渡。本文提出了基于UDP协议的IPv4 over IPv6隧道方案BoIP，描述了该方案的工作原理和实现过程，并以通过IPv6网络连接两个IPv4以太网为例做了实验。实验结果表明，BoIP具有透明(Transparent)、轻量(Lightweight)、支持单播组播和IPv4地址的动态分配等优点。该方案可进一步扩展成为支持多个IPv4孤岛连接的情况，并可用作无线网络接入有线网络的解决方案，具有较大的应用前景和实用价值。

参 考 文 献

[1] 吴建平. CNGI核心网CERNET2的设计[J]. 中兴通讯技术, 2005, 11(3): 17-20.

[2] 张云勇. 基于IPv6的下一代互联网[M]. 北京: 电子工业出社, 2004.

[3] DURAND A, FASANO P, GUARDINI I, et al. IPv6 Tunnel Broker, RFC3053[S]. 2001.

[4] TATIPAMULA M, GROSSETETE P, ESAKI H. IPv6 Integration and coexistence strategies for next-generation networks[J]. IEEE Communications Magazine, 2004, (1): 88-96.

[5] STEVENS W R, Fenner B, Andrew M. UNIX network programming[M]. Beijing: China Machine Press, 2003.

编 辑 孙晓丹