高速访问多出口局域网对外资源的方法研究*

肖 嵬,缪春莹
(重庆师范大学 网络管理中心,重庆 400047)

摘 要:由于中国电信、中国网通、中国教育科研网等各大 ISP 的网间数据交换几乎都要经过北京互联网交换中心,因此不同的 ISP 网络之间始终存在交互瓶颈,很难实现不同网络的用户同时高速访问多出口局域网的对外资源。本文介绍了一些常用的解决方法,包括双域名模式、反向代理以及智能域名结合 NAT 技术的方式,并重点研究和阐述了第三种方法的实现,利用此方法有效地解决了本校对外资源不能同时被多个 ISP 网络用户高速访问的问题。

关键词:域名系统;智能域名解析;NAT;iptables
中图分类号:TP393.07 文献标识码:A 文章编号:1672-6693(2008)03-0032-04

2000 年北京互联网交换中心的开通使我国主要互联网网间互通带宽由原来的不足 10 Mb/s 提高到 100 Mb/s,使得网络资源的访问速度大大提高。但随着最近几年互联网的高速发展,互联网上的应用越来越丰富,网间互通带宽已不能满足用户的需要,使得各 ISP 网络之间的交互瓶颈也越来越大。而对于一些拥有多出口的局域网来说,很难通过策略路由的方式实现不同网络的用户同时高速访问网内资源,各高校的校园网就是典型例子[1-2]。为了实现出口线路的冗余备份,很多高校都同时接入了教育科研网和其他 ISP 的网络。由于教育网与中国电信、中国网通等 ISP 之间存在交互瓶颈,绝大部分高校都优先保证教育网用户高速访问校园网对外资源,而其他 ISP 网络的用户发出的访问请求必须首先到达北京互联网交换中心,再转发到教育科研网,然后才能访问各高校的对外资源,因此访问速度非常慢,这在一定程度上影响了学校的正常工作。目前已有一些高校采用不同方法解决了上述问题,我校采用的是智能域名技术与 NAT 技术相结合的方法,大大提高了公网用户访问我校网内资源的速度。

1 常用解决方法

1.1 双域名模式

通常情况下,高校的域名都是由教育网解析的,而双域名模式要求向其他网络服务提供商再申请一个域名,并由服务商提供域名解析,校园网服务器由服务商托管,并使用服务商提供的公网 IP。此类解决方案的优点是简单易行,可完全交由网络服务商来实施;缺点是投入成本较高,管理不灵活,还需要双倍数量的服务器,且每次更新资源都要重复两次。

1.2 使用反向代理

反向代理也就是通常所说的 Web 服务器加速,它是一种通过在繁忙的 Web 服务器和 Internet 之间增加一个高速的 Web 缓冲服务器(即 Web 反向代理服务器)来降低实际的 Web 服务器的负载[3]。此方案将反向代理服务器放置在一台或多台 Web 服务器前端,或直接放置在公网入口处,当公网用户访问某个 Web 服务器时,实际上访问的是反向代理服务器的公网 IP,此时反向代理服务器逻辑上充当 Web 服务器。此方案的优点是只占用一个公网 IP 地址,内部 Web 服务器不用做任何调整;缺点是只能实现 Web 服务器的高速访问。

1.3 使用智能域名结合 NAT 技术

首先配置智能域名服务器,自动根据客户端 IP 地址来判断,当教育网用户访问时为内部服务器解析出教育网 IP 地址,当公网用户访问时解析出公网 IP 地址;然后配置 NAT 服务器,使用双网卡结构分别与公网和内部网连接,并分别设置公网 IP 和内部网 IP,同时在连接公网的网卡上绑定多个公网 IP 用于内部服务器地址转换。应用此方案时不用对内部服务器做任何调整,投入成本小,并可以实现外网对校园网内任何服务器以及任何端口的高速访问。

* 收稿日期:2007-12-03
资助项目:重庆市教委科研项目(No. KJ080828)
作者简介:肖嵬(1978-),男,实验师,硕士研究生,研究方向为计算机网络、GIS。

2 智能域名结合NAT技术的方法研究

2.1 智能域名解析

DNS是一个巨大的分布式数据库,其解析过程是首先由客户机提出域名解析请求,并将该请求发送给本地的域名服务器;当本地的域名服务器收到请求后,就先查询本地的缓存,如果有该纪录项则本地的域名服务器就直接把查询的结果返回,如果本地的缓存中没有该纪录,则本地域名服务器就直接把请求发给根域名服务器,然后根域名服务器再返回给本地域名服务器一个所查询域(根的子域)的主域名服务器的地址;本地服务器再向上一步返回的域名服务器发送请求,然后接受请求的服务器查询自己的缓存,如果没有该纪录则返回相关的下级域名服务器的地址,这样一直重复直到找到正确的记录;最后本地域名服务器把返回的结果保存到缓存,以备下一次使用,同时还将结果返回给客户机[4]。

智能域名解析是在原有域名解析技术基础上发展而来,其解析过程基本相同,主要的区别在于智能域名解析支持通过视图的方式来区分不同的IP地址,达到解析不同的IP地址的目的[5]。DNS服务软件Berkeley的Bind9版本已经提供了视图的功能。当网络上的客户端向域名系统发出解析请求时,域名系统会对源地址进行匹配,如果发现源地址来自教育网,域名系统会根据所请求的域名,找到该服务器对应的教育网IP地址,并返回给客户端;同样如果匹配到的源地址来自公网,域名系统根据所请求的域名返回给客户端该服务器对应的公网IP地址。然后客户端根据返回的地址从相应的网络线路访问该服务器。这样就实现了域名的智能解析。其原理如图1所示[6]。

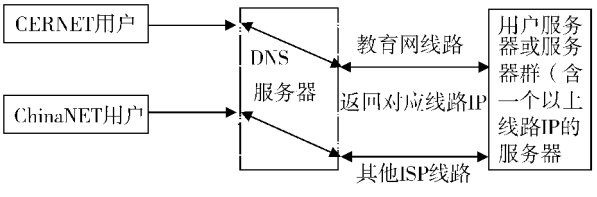

图1 智能域名解析原理图

下面以WWW服务器的解析为例,说明如何配置智能DNS服务器。设定域名为cqnu.edu.cn,WWW服务器的教育网IP地址为10.0.1.27,公网IP地址为219.10.6.57。下面简单列出/etc/named.conf中的主要相关部分[7]。

```
acl edu-nets {58.154.0.0/15;…};//Cernet地址列表
view“CerNet”{
    match-clients {edu-nets;};
    recursion yes;//递归解析
    zone“cqnu.edu.cn”{type master;
      file“cqnu.edu.cn.cernet”;
    };//教育网地址转向文件解析
};
view“ChinaNet”{
    match-clients {any;};
    recursion no;//不支持递归解析
    zone“cqnu.edu.cn”{type master;
      file“cqnu.edu.cn.chinanet”;
    };//非教育网地址转向文件解析
};
```

然后列出/var/named中的cqnu.edu.cn.cernet和cqnu.edu.cn.chinanet两个文件的主要相关部分,在cqnu.edu.cn.cernet中添加如下语句:

```
www IN A 10.0.1.27
```

在cqnu.edu.cn.chinanet中添加如下语句:

```
www IN A 219.10.6.57
```

2.2 用iptables实现NAT

NAT(Network Address Translation,网络地址转换)是一个IETF标准,顾名思义,它是一种把内部私有网络地址翻译成合法网络IP地址的技术,包括源NAT(SNAT)和目的NAT(DNAT)[8]。所谓SNAT就是改变转发数据包的源地址,如数据包伪装;所谓DNAT就是改变转发数据包的目的地址,如负载均衡、端口转发等。NAT的功能通常被集成到路由器、防火墙、ISDN路由器或者单独的NAT设备中,而且由于NAT在应用层以下进行处理,因此不但可以获得很高的访问速度,而且可以无缝支持任何新的服务或应用。

Linux下的NAT是基于iptables的。iptables内核空间包括3张表:filter、NAT和Mangle。filter表用来过滤数据包,Mangle不经常使用还在开发当中,而NAT表中存储了所有的NAT规则,并根据规则所处理的信息包类型,将规则分组在链中。要做SNAT的信息包被添加到POSTROUTING链中。要做DNAT的信息包被添加到PREROUTING链中。直接从本地出站的信息包的规则被添加到OUTPUT链中。其流程如图2所示[8]。

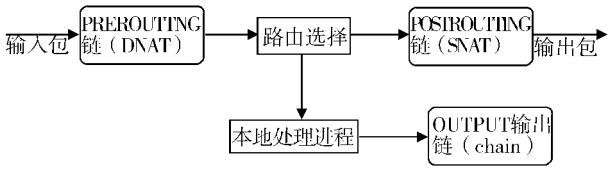

图 2　数据包穿越 NAT 表的流程图

1）DNAT:若包是被送往 PREROUTING 链的,并且匹配了规则,则执行 DNAT 或 REDIRECT 目标。为了使数据包得到正确路由,必须在路由之前进行 DNAT;

2）路由:内核检查信息包的头信息,尤其是信息包的目的地;

3）处理本地进程产生的包:对 NAT 表 OUTPUT 链中的规则实施规则检查,对匹配的包执行目标动作;

4）SNAT:若包是被送往 POSTROUTING 链的,并且匹配了规则,则执行 SNAT 或 MASQUERADE 目标。系统在决定了数据包的路由之后才执行该链中的规则。

下面同样以 WWW 服务器的地址转换为例,说明如何配置 NAT 服务器。设定 NAT 服务器的内网卡地址为 10.0.1.2,网卡介质为 eth0;外网卡地址为 219.10.6.2,网卡介质为 eth1。在 linux 中用户使用 iptables 命令在用户空间设置 NAT 规则,下面简单列出主要的配置命令。

```
ip addr add 219.10.6.57 dev eth1
modprobe ip_tables
echo 1 > /proc/sys/net/ipv4/ip_forward
iptables -t nat -A PREROUTING -i eth1 -d 219.10.6.57 -p tcp--dport 80 -j DNAT--to 10.0.1.27
iptables -t nat -A POSTROUTING -o eth0 -d 10.0.1.27 -p tcp--dport 80 -j SNAT--to 10.0.1.2
iptables -A FORWARD -o eth0 -d 10.0.1.27 -p tcp--dport 80 -j ACCEPT
iptables -A FORWARD -i eth0 -s 10.0.1.27 -p tcp--sport 80 -m state--state ESTABLISHED -j ACCEPT
```

以下是对配置命令的简单解释。

1）在外网卡上绑定 WWW 服务器的公网 IP 地址;

2）要使用 NAT 表必须先载入相应模块;

3）打开转发功能,让包可以通过 NAT 服务器转发;

4）从 eth1 进来的包被重写目标地址后伪装出去;

5）从 eth0 出去的包被重写源地址后伪装出去;

6）转发 WWW 服务器到任何地方去的包;

7）允许通过有连接状态的包。

3 效果与结论

重庆师范大学采用的是教育网和中国电信双出口线路连接 Internet,对外服务器都是使用策略路由到教育网,长期以来教育网以外的用户访问校内资源的速度都很慢。在使用智能域名解析以及 NAT 技术后,作者对服务器进行了公网客户端 ping 测试,测试结果为延时 100 ms 左右,几乎没有出现掉包现象;而以前的测试延时为 400 ~ 500 ms,且掉包现象严重。从测试结果可以看出,公网访问校园网的速度至少提高了 4 ~ 5 倍,稳定性也大大增加。因此将智能域名技术与 NAT 技术结合用于实现不同 ISP 网络的用户同时高速访问多出口校园网的对外资源,方法是完全可行的,而且效果显著。并且此方法还可以推广到企业、公司、研究机构等内部局域网。

参考文献:

[1] 肖嵬,肖丹燕. 基于 Linux 操作系统的 Socks 代理服务[J]. 重庆师范大学(自然科学版),2004,21(1):89-90.

[2] 缪春莹. 基于校园网的远程访问和用户认证[J]. 重庆师范大学学报(自然科学版),2004,21(1):91-92.

[3] IT 公社. 详细解析用 Squid 实现反向代理的方法[EB/OL]. (2007-05-12). http://www.itqoo.com/Linux/cy/200705/42989.html.

[4] 计算机之家. 域名解析基础知识及配置过程[EB/OL]. (2007-03-30). http://hi.baidu.com/farhill/blog/item/835709080b1423d063d9866a.html.

[5] 常潘,沈富可. 使用域名负载均衡技术实现校园网对外服务器的高速访问[J]. 计算机应用,2007,27(7):1585-1590.

[6] ORAY. 域名双线路智能 DNS 负载均衡[EB/OL]. (2007-08-03). http://www.oray.cn/Ask/Question-11673.html.

[7] OK LINUX. 解决双出口校园网瓶颈[EB/OL]. (2006-03-22). http://www.oklinux.cn/html/network/wlgl/20070324/5059.html.

[8] 服务器安全讨论区. Linux 下的 NAT 服务器架设实战[EB/OL]. (2007-03-30). http://old.fuan7.cn/Html/2007-3/30/17015011223.shtml.

Research into High Accessing Speed to Resources of Exports LAN

XIAO Wei, MIAO Chun-ying

(Network Management Center, Chongqing Normal University, Chongqing 400047, China)

Abstract: The net data exchange between ISP, like CTC、CNC、CERNET, almost all pass through Beijing Internet Exchange Center, so the bottlenecks between different ISP networks always exist and high accessing speed to resources of exports LAN is hardly realized for the users of different networks. This article describes a few solutions to common use. The first way is Dual-mode domain. It requires other network service providers to apply for a domain name provided by the analytical services, campus network servers hosted by service providers and the use of the services to provide the public and IP. The second way is reverse agent. It is also known as the Web server acceleration. It is busy through the Web server and the Internet to increase between a high-speed Web server buffer (that is, web reverse proxy server) to reduce the actual Web server load. This programme will place reverse proxy server in one or more front-end Web servers or directly at the entrance to the network. When the network users to access a Web server, the reverse is in fact the visit of the proxy server network IP, then reverse proxy server logic as Web server. The third approach is to use smart domain technology with NAT. According to automatic client IP address to judgement, the network users access to education for internal analysis to education network server IP address, the network user access to public networks, analytical IP address and then configuration NAT server, the internal network and public network are connective in a dual-card structures, and the network are set in public network IP and internal network IP. At the same time in the card of public network connecting bundled on a number of public networks IP for internal server IP address conversion. The article mainly researches and explains the third way, and effectively solves the problem which the users of different ISP networks can not access to campus resources in high speed.

Key words: domain name system; intelligent domain resolution; NAT; iptables

(责任编辑 游中胜)