智能DNS在多出口局域网中的应用研究*

侯冬青
(临沧师范高等专科学校,云南 临沧 677000)

【摘 要】在多出口局域网中合理配置策略路由实现了链路冗余,提高了内网用户访问Internet资源的速度。然而,该方法未能实现数据流的双向分配控制,外网用户访问内网资源的速度和可靠性难以保证。本文采用BIND软件实现域名的智能解析,满足按照请求者所在的网域对同一域名做出不同的解析。智能DNS结合NAT技术实现了数据流的双向分配控制,从而最大限度的提高了外网用户访问内网资源的速度。

【关键词】局域网;智能DNS;BIND;NAT
【中图分类号】TP393.18 【文献标志码】A 【文章编号】1673-1891(2015)01-0049-04
DOI:10.16104/j.cnki.xccxb.2015.01.016

引言

目前,大多数校园网都租用多家ISP的链路作为网络出口,以提高出口的稳定性,加快Internet的访问速度。临沧师专校园网也不例外,租用CERNET、中国联通和中国电信三家ISP的链路作为校园网的出口,网络拓扑如图1所示。

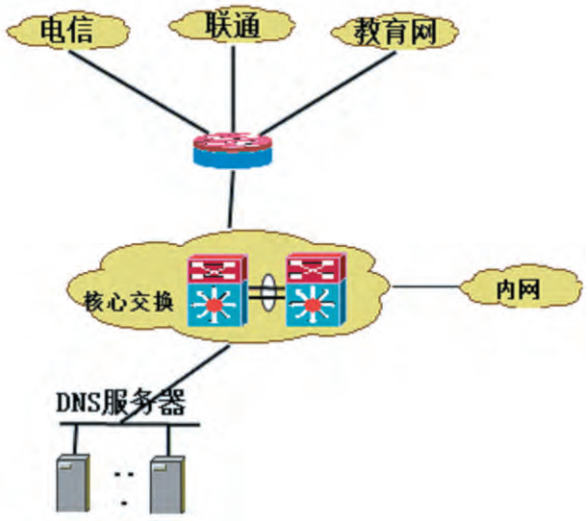

图1 校园网拓扑图

NAT技术和策略路由的配置实现,满足了校园网用户高速访问Internet资源的需求。当校园网用户访问的资源是由CERNET或联通提供时,将数据包从CERNET链路或联通链路转发出去;当校园网用户访问的资源是由其它ISP提供时,将数据包从电信链路转发出去。而且,实现了链路负载均衡,当CERNET或联通链路出现拥塞、断网时,可自动将流量分配至电信出口,有效的保证了网络出口的畅通。

然而,这些配置还不能解决公网用户访问校园网内部资源速度过慢的问题,因为不同运营商之间的网络存在着互连互通瓶颈。如果只将一个域名对应一个IP地址,不同ISP的用户访问学校内部资源时就会受到跨网访问的限制,影响访问速度。只有将内部服务器IP地址通过静态NAT分别连接到CERNET、联通和电信网络上,并采用动态DNS自动解析,将不同网域的用户访问校园网内部资源时解析到对应网域的IP地址,从而实现数据流的双向控制。

1 智能域名解析技术

1.1 智能DNS工作原理

DNS域名解析是运行在TCP协议之上,负责主机域名和主机IP地址之间的相互转换[1]。当用户在应用程序中输入主机域名时,DNS服务器可以将此域名解析为与之对应的IP地址,反之也成立。通常实现DNS域名解析是静态的过程,也就是将域名与IP地址进行一一对应。

智能DNS最基本的功能是DNS服务器可以智能的判断访问主机的用户,然后根据不同的访问者和事先设定的策略,把域名分别解析为不同的IP地址[2]。同样的域名www.lcnc.edu.cn,如果访问该域名的用户来自联通,会给用户返回一个指向联通服务器的IP地址;如果访问该域名的用户来自电信,会给用户返回一个指向电信服务器的IP地址;而如果是CERNET用户访问会返回一个指向CERNET服务器的IP地址。通过这种智能解析方式,尽可能避免CERNET用户去访问电信网络,电信用户去访问CERNET以及联通网络,因为,不同运营商之间的网络存在着互连互通瓶颈。动态DNS服务工作流程如图2所示。

收稿日期:2014-09-03
*基金项目:临沧师范高等专科学校2014年自然基金项目"临沧师范高等专科学校校园网集成方案研究(项目编号:LCSZL2014005)。
作者简介:侯冬青(1982-),男,云南江川人,讲师,主要从事网络技术及其教育等方面的教学与研究。

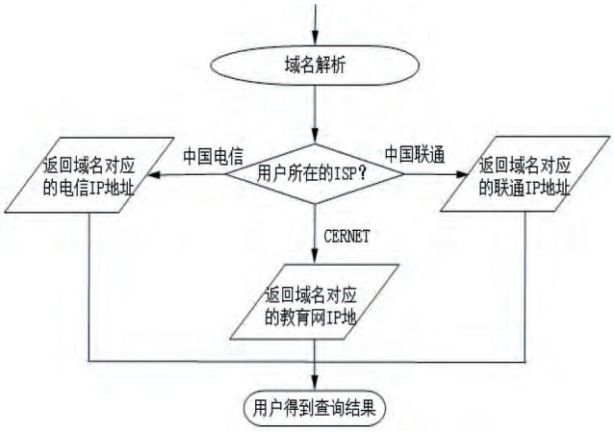

图2 智能DNS工作流程图

当用户在运用程序中输入域名时,程序会向本地DNS服务器提交域名解析请求;本地DNS服务器通过DNS解析的常规步骤查找到动态DNS服务器,并将用户请求转发至智能DNS服务器;智能DNS服务器根据请求者的IP地址确定客户端所属的网域,根据用户所属网域查找相应的域名解析地址池,找到域名所对应的IP地址;智能DNS服务器将域名解析结果返回给本地DSN服务器;本地DNS服务器将查询结果保存到缓存,以备下次查找使用,同时将最终结果返回给用户[3]。

1.2 Bind概述

目前,使用最为广泛的开元智能域名解析软件是由美国加州大学伯克利分校开发的BIND(Berkeley Internet Name Domain)[4]。在BIND中引入VIEW视图,通过VIEW的策略判断功能,可以将来自不同IP地址段的查询请求响应到不同的DNS解析。也就是说,当用户通过某个域名访问网络资源时,VIEW会根据请求者的IP地址在自己的列表里面进行匹配,然后把匹配的结果返回给用户[5]。但在实际解析过程中,VIEW判断用户来源的依据是本地DNS服务器的IP地址,而非用户自身的IP地址。

BIND有主配置文件、日志文件、解析文件三部分组成。当有DNS客户端需要进行域名解析时,守护进程Named读取主配置文件named.conf,通过解析文件查找到对应的IP地址,并将查询结果返回客户端[6]。服务器中BIND软件的组成如图3所示

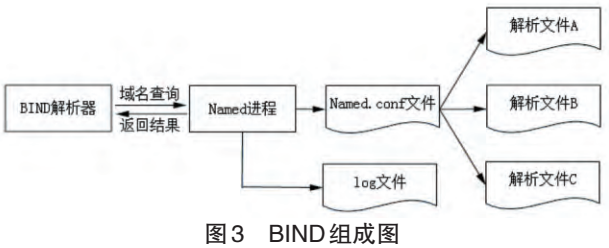

图3 BIND组成图

2 实现过程

在边界路由器上以静态NAT的方式将需要向公网提供服务的私有IP地址分别映射到三个公网IP地址上,从而使公网用户能通过这些IP地址访问内网资源。IP地址对应关系如表1所示。

表1 lcnc.edu.cn主机与不同ISP地址之间的对于关系

lcnc.edu.cn主机名	内网地址	CERNET地址	联通地址	电信地址
WWW	192.168.200.2	121.49.153.3	221.213.200.211	218.63.53.227
…….	…….	…….	…….	…….

BIND能够在Unix、Linux或Windows环境下运行,因此,本方案以Windows Server 2003作为支撑平台,采用BIND9.4.2软件实现动态域名解析功能。安装配置过程如下:

(1)安装BIND

下载BIND9.4.2.zip,解压后双击BINDInstall.exe进行安装,默认安装路径是"C:\WINDOWS\system32\dns"。安装完成后将named账号设置比较复杂的密码,并授予named账号具有对DNS目录的读写权限。

(2)配置BIND

以命令模式进入C:\WINDOWS\system32\dns\bin目录,执行rndc-confgen-a命令在\dns\etc目录生成rndc.key文件,并执行rndc-confgen > ..\etc\rndc.conf在同一目录下生成rndc.conf文件。

进入etc目录,用notepad命令分别生成named.conf、cernet.conf和cnc.conf文件。其中,cernet.conf和cnc.conf两个文件列出教育科研和联通IP地址段,并生成ACL库,这两个库文件用于判断用户所在的网域。通过文本编辑器修改、编辑named.conf、cernet.conf和cnc.conf文件,具体内容如下。

```
#cernet.conf                    #cnc.conf
acl "CERNET" {                  acl "CNC" {
1.51.0.0/16;                    58.16.0.0/16;
1.184.0.0/15;                   58.17.0.0/17;
…                               …
#教育网地址列表,可以从网上下载。  #联通地址列表,可以从网上下载。
};                              };
```

```
#named.conf
options {
directory "C:\WINDOWS\system32\dns\etc";  //文件存放位置
pid-file  "C:\WINDOWS\system32\dns\etc\named.pid";
};
include "cernet.conf";  //定义教育网地址列表。
```

#判断如果是教育网的地址范围,则执行此处,调用教育网解析文件进行地址解析。

```
view "view_cernet" {
match-clients { CERNET; };
zone "." {
type hint;          //根域名服务器
file "named.root";   // 根域名服务器文件,可从网站下载。
};
zone  "0.0.127.in-addr.arpa" {
type master;
file  "named.local";
};
zone  "localhost" {
type master;        //指定本机为DNS服务器。
file  "localhost.zone";
};
include"C:\WINDOWS\system32\dns\etc\master\cernet.def";  //CERNET网域对应解析文件的位置和名称。
};
include "cnc.conf";  //定义联通网地址列表。
```

#判断如果是联通网的地址范围,则执行此处,调用联通网解析文件进行地址解析。

```
view "view_cnc" {
match-clients { CNC; };
… //同上,省略。
};
include"C:\WINDOWS\system32\dns\etc\master\cnc.def";  //CNC网域对应解析文件的位置和名称。
};
view "view_any" {
match-clients { any; };
#any;  //表示其它所有外网地址域都解析为电信IP地址。
…    //同上,省略。
include"C:\WINDOWS\system32\dns\etc\master\telecom.def";  //其它网域对应解析文件的位置和名称。
};
```

在master文件夹中创建cernet.def、cnc.def和telecom.def三个解析文件,cernet.def具体内容如下,其它两个文件内容类似。

```
$TTL 3600
$ORIGIN lcnc.edu.cn.
@ IN SOA dns1.lcnc.cn. root.lcnc.edu.cn.(
2006111520 ;Serial
3600 ; Refresh ( seconds )
900 ; Retry ( seconds )
68400 ; Expire ( seconds )
15 );Minimum TTL for Zone ( seconds )
;
@ IN NS dns1.lctc.edu.cn
dns IN A 121.49.153.5    //dns服务器IP地址。
www IN A 121.49.153.3  //cen.def和telecom.def文件的www服务IP地址分别为221.213.200.211和218.63.53.227。
```

(3)启动服务

在服务器开始菜单的【运行】对话框中输入services.msc命令打开【服务】窗口,找到ISC BIND服务,将该服务的登录用户改为本地系统用户,启动方式设置为“自动”,配置完成启动服务即可。

3 测试验证

(1)分别在校园网、教育网、联通网和电信网中找一客户端作为采样点,采用nslookup命令测试对www.lcnc.edu.cn域名的解析,测试结果如表2所示。结果表明,在出口静态NAT工作正常的情况下,智能DNS服务器均能返回给用户正确的域名解析结果。

表2　www服务的解析结果

用户所在网络	返回IP
校园网	192.168.200.2(内网地址)
教育网	121.49.153.3(教育网地址)
联通网	221.213.200.211(联通网地址)
电信网	218.63.53.227(电信网地址)

(2)在前一测试的基础上,采用ping命令分别对以上IP地址进行测试,对比响应时间,测试结果如表3所示。结果表明,校园网用户访问校内资源时响应时间最短,用户和访问的地址在同一网域时次之,跨网域访问响应时间最长。由此得出,在访问同一域名时,如果解析到的IP地址和用户在同一网域,访问速度最快。

表3　访问www服务的响应时间

采用点	192.168.200.2	121.49.153.3	221.213.200.211	218.63.53.227
校园网用户	<1ms	<1ms	<1ms	<1ms
教育网用户	超时	2ms	80ms	60ms
联通网用户	超时	120ms	8ms	30ms
电信网用户	超时	53ms	36ms	6ms

通过以上测试可以看出，校园网智能DNS服务器的智能解析功能有效、可靠，可以针对用户不同的访问线路，返回对应线路的IP地址，响应时间大幅缩短，访问速度大幅提升，达到方案设计的预期目标。

4 结语

该方案采用BIND9的VIEW功能实现了域名的智能解析，弥补了策略路由的不足。策略路由提高了校园网用户访问Internet的速度，而智能DNS方案为不同ISP用户解析到同一网域的对应IP地址，避免了跨网域访问，提高了Internet用户访问校园网内部资源的速度，从而实现了多出口网络环境下数据流的双向分配控制。

BIND判断时是根据请求者的本地DNS服务器IP地址，而不是用户自身IP地址。因此，为了避免由于本地DNS服务器设置错误而造成的跨网访问，影响访问速度，用户在进行网络参数设置时要明确自己所属的网域，并设置对应的本地DNS服务器。

注释及参考文献：

[1]Tanenbaum A S.Computer Networks(Fourth Edition)[M].北京:清华大学出版社,2008.

[2]Thomson P S.Dynamic Updates inthe Domain Name System(DNS UPDATE)[R].RFC 2136,1997.

[3]王亮.基于智能DNS技术下的多ISP校园网服务质量优化[J].科技信息,2011(33):102-103.

[4]Internet Systems Consortium.BIND 9 Administrator Reference Manual(9.3.2)[EB/OL].(2005).http://www.bind9.net/manuals.

[5]杨柯,陈纪豪,卢春,等.基于Linux智能DNS系统的研究和实现[J].信息安全与通信保密,2011(10):72-75.

[6]李馥娟.智能域名解析技术在多出口校园网中的应用[J].计算机与数字工程,2009(11):91-94.

The Application of Intelligent DNS in Multi-outlet LAN

HOU Dong-qing

(Lincang Teachers' College, Lincang, Yunnan 677000)

Abstract: In the multi-outlet LAN routing strategy to achieve a rational allocation of link redundancy, which improves network users to access Internet resources speed. However, this approach failed to achieve two-way data flow distribution control, speed and reliability within the extranet users to access network resources is not guaranteed. This paper puts forward that using BIND software achieve domain name intelligent analysis, in order to satisfy the domain requesters on the same domain to make a different parsing. Intelligent DNS NAT technology achieves a two-way combination of distribution control data flow, which maximize improves the speed of extranet users accessing network resources.

Key words: LAN; intelligent DNS; BIND; NAT