多出口校园网中策略路由技术的研究与应用

Applying the Policy Based Routing Technology in Multi-exports Campus Network

摘　要：本文提出了在当今校园网多出口环境下利用策略路由技术（PBR）整合CERNET和本地ISP的资源优势的技术方案，达到减少CERNET国际流量费用的目的，在淮阴师范学院校园网中进行了典型应用，实践证明这是行之有效的减少校园网国际流量费用的解决办法。

关键词：策略路由　多出口校园网　流量费用

庄永龙　（江苏淮安淮阴师范学院信息中心 223001）

当今高校校园网的ISP基本均是中国教育和计算机网（CERNET），由于CERNET按照国际流量的计费策略既增加了各校的经费负担，又限制了用户对国际网络资源的自由访问。有鉴于此，相当一部分高校相继看中了电信、网通等其他ISP可以不按照流量的计费优势，相继开通了校园网的本地第二出口，由此就产生了路由的策略问题。

目前，关于策略路由的研究多限于网络负载均衡的角度，很少研究CERNET特有的流量费用问题，本文通过对目前高校校园网多出口现状的调查分析，提出在校园网多出口应用策略路由（PBR）的方法，整合CERNET丰富的教育资源及本地ISP提供的高速出口带宽、国际资源优势，在适应CERNET网络环境的策略路由上有所突破。

1　淮阴师范学院校园网出口现状

淮阴师范学院校园网上联CERNET江苏淮安主接点，由于CERNET在苏北主干带宽仅为155M，故实际出口带宽只有10M左右，全院2000多个网络终端上网速度不甚理想，随着学院信息化的大力开展，网络招生、科研信息资料网络化、学生信息系统、VOD视频点播等服务均要求较高的网络出口带宽，而CERNET按照国际流量的计费策略又大大加重了学院的网络经费负担，某种程度上也限制了用户对国际网络资源的访问。

我们经过研究分析，发现本地ISP具有较高的接入带宽且接入费用较低，可以有效提高校园网网络出口带宽，于是在本地ISP中进行比较后决定选择电信作为学院的第二出口。在校园网多出口环境下，如何合理分配网络资源，达到增加网络速度、减少CERNET国际流量费用的目的，是一个值得研究的重要问题。

2　策略路由技术介绍

策略路由英文翻译为Policy Based Routing，简称PBR。它不仅可以根据数据包的目的IP地址来进行路由选择，而且可以根据数据包的源IP地址、数据包类别等条件，在路由器中根据自己的需求进行控制数据包的路由，这就是策略路由的功能。通常策略路由技术主要有以下几种方式：

（1）基于源IP地址的策略路由；

（2）基于数据包协议类别的策略路由；

（3）基于数据包大小的策略路由；

（4）基于应用的策略路由。

3　淮阴师范学院校园网多出口环境下策略路由需求分析

淮阴师范学院校园网络有Cisco 3640主路由器和Cisco PIX525防火墙，中心交换为具有三层路由功能的Cisco Catalyst 6509交换机。学院现有16个C类的教育网IP地址，因此我们决定在校园网内使用CERNET提供的合法C类IP地址，这样用户在CERNET线路端无须转换可以直接上网，于是利用具有强大访问控制列表功能的Cisco 3640路由器上联CERNET淮安地区主节点；在电信接口端由于只有一个合法IP地

表 1

比较类别	CERNET	电信网络
速度	在高校、科研机构等联网单位站点内访问速度较快	在公共资源、娱乐等信息站点内部访问速度较快
资源	教育站点中诸多教育资源共享	资源相当广泛，国际资源的无限制访问
安全	本身网络信息已经过管理、净化，用户访问较安全，可以“绿色上网”	信息资源可用性缺乏保障
费用	国际资源按流量收费	电信可以采取包月的方式

址可以对外连接使用，因此我们选择在电信接口端使用具有超强NAT（Network Address Translation，网络地址翻译）功能的PIX525进行地址转换上网。

CERNET和电信网络的各自资源优势不尽相同，具体比较结果如表1。

根据CERNET和电信网络的各自资源优劣，结合学院实际情况，制定如下的策略需求：

(1) 学院公共服务器（WWW服务器、DNS服务器、E-mail服务器等）由于使用的是CERNET合法IP地址，外部路由指向使得外部对此类服务器的访问只能通过CERNET的线路进行，否则会造成路由包文丢失，所以公共服务器和所有外部网络的通信都得通过CERNET出口进行；

(2) 所有校园网IP在访问CERNET及其联网单位网络时均通过CERNET出口进行；

(3) 学生机房IP只能访问CERNET免费列表中的网络，且出于负载均衡目的限定从CERNET出口进行；

(4) 所有其他的校园网IP在访问CERNET联网单位之外网络时均通过本地电信出口进行。

CERNET是以校园网国际入流量统计国际流量的，在实施以上路由策略需求后，除了学院公共服务器对CERNET免费列表以外资源（即CERNET定义的国际资源）访问的回应包文可以产生国际流量以外，其他用户在访问国际资源时将经PIX525进行NAT转换后从本地电信ISP出口路由，请求的相应返回包文也自然经过电信路由，如此即可实现减少校园网国际流量费用的目的。

4 策略路由结合地址翻译的技术方案

在实际运用中，我们决定选择基于源IP地址的策略路由方式，根据源IP地址的不同决定是否应用策略路由，在Catalyst 6509中采用策略路由技术，在PIX525中采用NAT技术。如果是服务器和学生机房IP（包括访问CERNET及其联网单位网络的源IP）则不需地址转换直接从CERNET出口进行访问；否则需要利用PIX525进行地址转换后从电信出口进行访问。本例假设学院IP地址范围为192.168.0.0——192.168.15.255，合计16个C类地址；本地电信ISP分给我们可用的IP地址为172.16.0.2，路由下一跳地址为172.16.0.1；Cisco3640连接CERNET的以太网接口IP为192.168.10.5，路由下一跳地址为192.168.10.6；Cisco3640连接6509交换机的以太网接口IP为192.168.100.10（校园网络拓扑如图1所示）。

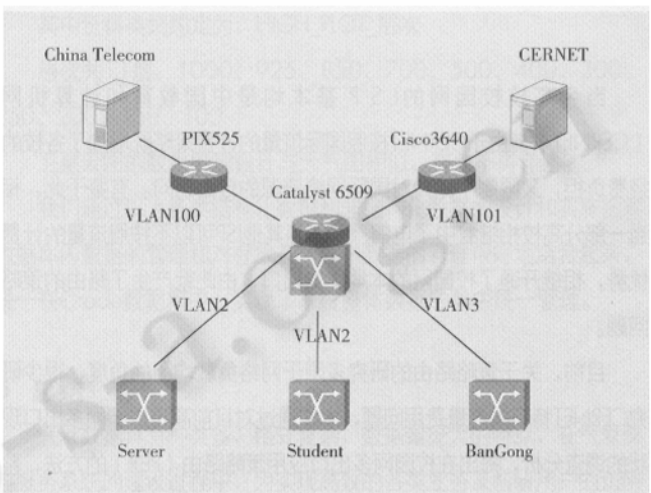

图 1 多出口校园网络拓扑图

根据制定的策略需求在Catalyst6509上划分如下VLAN：

5 策略路由和 NAT 配置实例

5.1 在 Catalyst6509 上定义路由策略

route-map hytc permit 10

表 2

VLAN ID	描述	IP地址范围	VLAN网关	VLAN子网掩码
1	Server	192.168.0.0—192.168.0.255	192.168.0.1	255.255.255.0
2	Student	192.168.1.0—192.168.1.255	192.168.1.1	255.255.255.0
3	BanGong	192.168.2.0—192.168.2.255	192.168.2.1	255.255.255.0

```
match ip address server&student
set ip default next-hop 192.168.100.10 192.168.100.6
```

如果匹配访问列表server&student即如果是公共服务器或学生机房用户，则由CERNET出口访问，否则从电信出口访问。

5.2 Catalyst6509 上的 VLAN 配置

```
interface Vlan1
description server
ip address 192.168.0.1 255.255.255.0
ip policy route-map hytc
interface Vlan2
description student
ip address 192.168.1.1 255.255.255.0
ip policy route-map hytc
interface Vlan3
description bangong
ip address 192.168.2.1 255.255.255.0
interface Vlan100
description TO_PIX525
ip address 192.168.100.5 255.255.255.252
ip access-group 110 out
interface Vlan101
description To_CISCO3640
ip address 192.168.100.9 255.255.255.252
```

公共服务器、学生机房用户VLAN应用路由策略，VLAN100是6509和PIX525间的管理VLAN，VLAN101是6509和PIX525间的管理VLAN。

5.3 在 Catalyst6509 上配置路由策略在电信出口的 ACL 访问控制列表

```
ip access-list extended server&student
permit ip host 192.168.0.11 any (WWW服务器)
permit ip host 192.168.0.12 any (MAIL服务器)
permit ip host 192.168.0.13 any (主DNS服务器)
permit ip host 192.168.0.14 any (辅DNS服务器)
permit ip host 192.168.0.15 any (FTP服务器)
permit ip 192.168.1.0 0.0.0.255 any （学生机房用户）
access-list 110 permit ip 192.168.2.0 0.0.0.255 any （办公用户）
access-list 110 permit ip any 61.28.0.0 0.0.15.255
access-list 110 permit ip any 61.48.0.0 0.7.255.255
..... （CERNET定义的免费访问列表，下载地址http://www.nic.edu.cn/RS/ipstat/internalip/）
```

5.4 在 Cisco3640 上配置路由策略在 CERNET 出口的 ACL 访问控制列表

```
interface FastEthernet0/0
ip address 192.168.10.5 255.255.255.252
ip access-group 110 out
interface FastEthernet0/1
ip address 192.168.100.10 255.255.255.252
ip route 162.105.0.0 255.255.0.0 192.168.10.6
ip route 166.111.0.0 255.255.0.0 192.168.10.6
..... （校园网用户在访问CERNET及其联网单位网络时由CERNET出口进行）
access-list 110 permit ip host 192.168.0.11 any
..... （公共服务器可以不限制访问）
access-list 110 permit ip any 61.28.0.0 0.0.15.255
access-list 110 permit ip any 61.48.0.0 0.7.255.255
..... （CERNET定义的免费访问列表）
```

5.5 在 PIX525 上配置 NAT

```
ip address outside 172.16.0.2 255.255.0.0 （设定外部端口地址）
ip address inside 192.168.100.6 255.255.255.252 （设定内部端口地址）
global (outside) 1 interface （为所有地址做NAT,转换地址为外部的接口地址）
nat (inside) 1 0.0.0.0 0.0.0.0 0 0 （定义需要转换的地址为从内部端口来的所有地址）
access-group acl_out in interface outside
route outside 0.0.0.0 0.0.0.0 172.16.0.1 1 （为外部接口指定下一级路由）
route inside 192.168.0.0 255.255.0.0 192.168.100.5 1 （静态路由把对应内部地址指向5505）
route inside 192.168.0.0 255.255.240.0 192.168.100.5 1 （静态路由把对应内部地址指向5505）
```

如此进行应用策略路由，就实现了我们制定的路由策略需求。

6 关键的动态路由切换技术

在应用以上的策略路由技术后，虽然完美地解决了路由策略需

求，但是在两个校园网出口中有一个中断后却不能及时地进行路由切换，此时就不能体现出两个出口的冗余性，为了能够高效管理校园网络，我们选择OSPF动态路由技术来达到动态路由切换目的。具体实现如下：

```
router ospf 1
network 192.168.100.8 0.0.0.3 area 0
ip route 0.0.0.0 0.0.0.0 192.168.100.6
ip route 0.0.0.0 0.0.0.0 192.168.100.10 60
```

以上在6509上配置，以下在3640上配置

```
router ospf 1
redistribute static subnets
network 192.168.100.0 0.0.0.255 area 0
network 192.168.10.4 0.0.0.3 area 0
ip route 0.0.0.0 0.0.0.0 192.168.10.6
ip route 0.0.0.0 0.0.0.0 192.168.100.9 50
```

如此就实现了两个校园网出口之间在其中一个中断后路由的动态切换。

7 结束语

通过在校园网出口应用策略路由，使多出口接入Internet的优势得到最大程度的发挥，具体表现在如下几个方面：

(1) 最大限度地减少国际流量：统计数据表明以前我校流量费用约为8000元/月，在应用策略路由技术后只有500元/月，扣除增加电信出口费用3000元/月，可以直接每月为学校节约经费4000元以上；

(2) 提高网络访问速度：以前我校用户平均网络访问速度只有10Kbps左右，在应用策略路由技术后一般均能达到50Kbps到80Kbps之间，实现了网络的高速访问；

(3) 实现网络负载均衡：在应用策略路由技术后，公共服务器和学生机房用户通过CERNET出口访问，其他所有用户在访问CERNET及其联网单位以外网络时均通过电信出口进行，实践证明有效实现了网络的负载均衡；

(4) 增加网络安全：校园网内部用户在通过电信出口访问时，由于其IP地址经由NAT转换，此时外部主机实际上无法访问到他们，增加了网络的安全性。

参考文献

1 美国Chris Lewis著，Cisco交换式网络互连[M]，机械工业出版社，2000。

2 国Syngress Media公司著，韩存兵、张秀丽、刘今朝等译，CCNA 2.0[M]，机械工业出版社，2001。

3 国Chris Lewis著，潇湘工作室译，Cisco TCP/IP路由管理专业参考[M]，机械工业出版社，2000。

4 ttp://www.cisco.com/,2003-8.