# 校园网双出口接入的实现与改造

刘丽萍[1,2],吴正畦[2],王 霖[2]
(1.四川大学 计算机学院,四川 成都 610065;2.成都纺织高等专科学校,四川 成都 611737)

【摘 要】随着网络技术的不断发展,Internet上的资源得到了不断丰富,但目前我国高校对此的利用率却不高。众所周知,我国CERNET与公众网的互连存在着带宽瓶颈问题,它们之间互访速度却很慢,这束缚了一些高校网络应用水平的提高。本文以我校实现校园网双出口接入Internet为实例,介绍如何采用双出口措施实现校内用户快速访问外部资源,校外访问者快速访问我校网站的策略与方法。本方法不仅解决了加快与公网互连速度问题,而且能够实现链路冗余和解决内网安全等问题。

【关键词】CERNET;双出口;网络地址转换(NAT)
【中图分类号】TP393.18 【文献标识码】A 【文章编号】1673-1891(2009)01-0053-03

## 1 引言

CERNET是中国最早的互联网络之一,其用户从CERNET地区主干节点接入Internet,主要以大专院校为主。随着网络的普及和用户数量的增多,人们的工作、学习对网络的依赖度不断提高,人们对上网的速度要求也越来越高,CERNET用户感觉是有些“网不从心”。众所周知,目前虽然在CERNET、CHINANET等互联网络其各自内部访问速度较快,但它们相互之间互访速度却很慢,均存在着互连的带宽瓶颈问题[1],而在人们的日常上网时,往往却是几个互联网间的互访。特别是在大专院校工作和学习的教师和学生,他们一部分是公众网用户(在家通过ADSL、小区宽带等上网,或在社会上的网吧上网等)访问校园网,比如访问学校的教务管理系统、图书借阅查询系统、学生管理系统等等,尤其值得一提的是在高考填报志愿期间,大量考生需要进入欲报考高校的校园网了解学校情况,这时校园网成为高校宣传展示自己的最好途径;大量的师生是作为教育网用户的,他们又经常因CERNET上的资源相对于公众网较少,不得不通过教育网访问公众网。许多高校为了解决这个问题,抛弃了过去仅从CERNET接入Internet的单一措施,相继采用了双出口接入的方案(如图1)。其思路是采用本地互联网服务提供商(ISP)和CERNET分别提供的两个出口,当校园网内用户访问目标是CERNET内部网站(如其他高校)时,便通过CERNET进行访问,其余所有访问目标均通过本地ISP提供线路对其直接访问,提高了校园网用户上网速度;同样地当外面的用户访问校园网时,如果是CERNET用户,便通过CERNET的链路进行访问,其余所有访问者均通过本地ISP的链路对校园网直接访问,同样提高了他们对校园网访问速度。也就是说通过采用双出口,不仅要解决校园网访问公网速度慢的问题,而且要解决非CERNET用户访问校园网慢的问题,甚至要实现出入口链路的冗余功能。同时由于CERNET的国际流量的计费方式是单独计费,将国际流量放在本地ISP提供链路上实现,可以降低网络使用费。这个思路很好,但在实施中部分高校却又面临经费困扰,或面临诸多技术难题,出现一些较难解决的问题,效果不甚理想。本文提供并探讨了我校双出口接入的解决方案,供一些高校参考和借鉴。

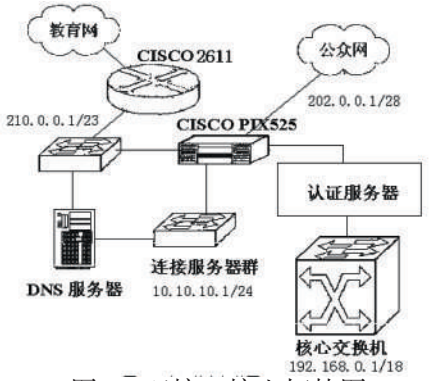

图1 双接口接入拓扑图

## 2 我校双出口接入方案的结构

我校考虑到学校师生对公众网的需要,在保留原有的CERNET链路的基础上,又申请了一条本地ISP的线路(CHINANET),实行双出口接入的办法。在建设时充分利用学校现有资源,基本没有增加什么新设备,较好地实现了校园网的双出双入的功能。其方案见图1,我们选择防火墙CISCO PIX525(以下称防火墙)作为主要的核心设备,在其上实现双出口接入功能,其DMZ口连接服务器群(网络中心的服务器,如WEB、FTP、DNS、EMAIL等服务器,

收稿日期:2008-12-11
作者简介:刘丽萍(1974- ),女,河北石家庄人,讲师,四川大学在读硕士。研究方向:多媒体技术及网络应用。

不含部门级的服务器,因部门级的服务器分布在局域网内各部门的机房中,如教务管理系统等,这是我校的管理模式),原来的两个以太网口分别连接内网(通过接认证服务器,见图1)和公众网,再在其上增加一个网络模块来连接教育网。连接教育网时,从防火墙出来先通过一个普通交换机连接路由器CISCO 2611(以下称路由器)到教育网,交换机的其中一个接口连接学校的DNS服务器(在DNS服务器上增加一块网卡,另一个网卡连到服务器群交换机,相当于有两个DNS服务器)。

为了便于后面的分析,我们就在结构中仿照我校的IP地址情况假定几个IP地址段。

公众网IP地址段:202.0.0.1/28(相对较少);教育网IP地址段:210.0.0.1/23;服务器群IP地址段:10.10.10.1/24(从安全考虑,采用私用IP地址);校园网内IP地址段:192.168.0.1/18(我校IP资源已显不足,网内采用私有IP地址)。

## 3 双出口接入的实施分析

通过这次改造,校园网内用户访问教育网和公众网的速度都明显加快,同样外部访问学校网站速度也都明显加快,还具有了出入口链路冗余的作用。

### 3.1 访问Internet分析

众所周知,对Internet的访问,用户都必须使用各自目标认为是合法的IP地址才能出去实现访问。但校园网采用双出口接入后,在校园网出口处由于教育网的地址不能被ISP的公众网路由,因此教育网地址不能直接通过ISP的出口出去访问,同样ISP提供的IP地址通过教育网出口出去访问亦然,这些都是需要解决的问题;另一方面实际上对我校来说,ISP提供的IP地址很有限,无法满足学校众多用户直接访问公众网的需求;同时,又发现随着学校网络的发展,教育网地址也不能满足学校用户的需求,因此目前情况下在内网只能使用私有IP地址。方案是:分别在CERNET和ISP提供的公众网两个接入口处采用NAT技术[2]。具体如下:访问公众网时,在防火墙的公众网接入口将内网地址192.168.0.1/18转换为202.0.0.1/28中的部分地址,访问教育网时,在防火墙的CERNET接入口将内网地址192.168.0.1/18转换为210.0.0.1/23中的部分地址。但由此产生的NAT列表过大,所以实现NAT功能不能放在路由器上[3],这样势必会造成路由器CPU资源占用率过高,甚至产生宕机;如果放在核心交换机上实现,则需要两台客户认证服务器(四川高校要求有客户认证功能)分别放在两个接入口,势必会增加投入。因此选择在防火墙上实现NAT的功能。

由于防火墙不支持策略路由的功能,我们采用了静态路由的方式,路由表中的地址为CERNET的地址(从教育科研网中获取),其指向的路由为路由器的端口地址(即教育网链路,见图1),访问教育网通过该链路进行;访问公众网使用默认路由,即访问路由表中未被列出的IP地址都通过ISP提供的链路进行。其配置见文献[4]。

通过以上方式就实现了校园网内用户访问教育网和访问公众网分流的功能,又发挥它们在各自其内部较快相互访问的优势。当校园网内用户出去访问时,从核心交换机出来,通过客户认证服务器,首先在防火墙上作路由选择(判断是否是路由表中列出的地址),如果目的地址是教育网地址(即路由表中列出的地址),防火墙则在CERNET接入口处将内网地址转换为210.0.0.1/23中的一个合法IP地址,再经过路由器进入教育网;否则防火墙在公众网接入口将内网地址转换为202.0.0.1/28中的一个合法IP地址,然后进入公众网。本方案还实现了出口冗余功能。当教育网链路和ISP提供的链路中其中一条故障时,可以通过在防火墙上简单改变路由设置实现出口冗余功能,比如教育网链路故障,设置成所有的访问都通过ISP提供的链路。

### 3.2 访问校园网分析

本方案从网络安全考虑,校园网内所有服务器的IP地址均使用私有地址,其中网络中心服务器群的地址用10.10.10.0/24,各部门级的服务器由于分布在各部门的机房中,只能使用192.168.0.1/18内网地址中的地址。但若要能被外部访问,必须把校园网内各个服务器的地址转换为Internet上合法的IP地址,同样也需要快速。我们同样采用了教育网用户和公众网用户分别通过CERNET和ISP提供的公众网的链路访问校园网,分别在防火墙的两个接入口上对各服务器做静态端口重定向,在CERNET接入口上各服务器(除DNS服务器外,因为在本链路上它已有合法的CERNET地址,见图1)IP映射到教育网地址210.0.0.1/23,专门接受教育网用户的访问;在公众网接入口上各服务器IP映射到公众网地址202.0.0.1/28,专门接受公众网用户的访问,配置参见文献[5]。这样外部用户各自通过校园网映射出来的合法IP地址/端口穿过防火墙访问到校园网内各服务器。

高校的域名依托教育网,因此将学校的DNS服务器其中的一个网络接口(相当于一台DNS服务器)放在教育网链路上路由器与防火墙之间(见图

1),作为是首选DNS服务器;DNS服务器的另一个网络接口(相当于第二台DNS服务器)连到服务器群交换机上,作为备用DNS服务器。在教育网链路正常的情况下,首选DNS服务器工作,它既在校园网内部,却又不受防火墙静态路由表的限制,不论是CERNET用户还是公众网用户都能通过CERNET链路得到域名解析。两个接入都正常的情况下,首选DNS服务器在解析域名时采用策略域名解析[6]的方式,根据来访者所在的网络地址,DNS服务器返回不同的解析结果。即在DNS服务器解析校内服务器域名(建议对校内所有服务器在学校DNS服务器上注册域名,以便在学校网页上它们之间的链接时使用,如果直接使用IP地址链接,可能会造成不能访问的情况,原因见上一个部分)时,分CERNET用户(我校设置把校园网内用户也看作CERNET用户)、公众网用户两种策略进行解析,配置参见文献[6]。其配置文件内的源地址列表1中的地址为防火墙静态路由表中的地址(注意两个表的地址内容一定要一致,否则将造成部分用户不能访问的情况,分析略),当来访者所在网络的地址与源地址列表1匹配时,就解析为教育网地址210.0.0.1/23中的一个地址;配置文件的源地址列表2中的地址为any(其含义是除源地址列表1中地址外的所有地址),当来访者所在网络的地址与源地址列表1不相匹配时,就解析为公众网地址202.0.0.1/28中的一个地址。这样就实现了教育网用户通过CERNET、公众网用户通过ISP提供的公众网链路访问校园网的分流功能,发挥它们各自在其内部相互访问网速较快的优势。

同样也实现了冗余功能,当只有公众网链路正常时,启用备用DNS服务器,修改DNS服务器设置,将配置文件内的源地址列表1中的地址改设为空,这样所有校内服务器的域名都被解析为公众网地址,同时修改防火墙静态路由表,允许Internet上的所有用户都通过公众网来访问;同样当只有教育网链路正常时,也需修改首选DNS服务器设置,将所有校内服务器域名都解析为教育网地址,修改防火墙静态路由表,允许Internet上的所有用户都通过教育网来访问(这也是建议需对校内所有服务器在学校DNS服务器上注册域名,在学校网页上不直接使用IP地址链接的原因)。

## 4 结语

我校校园网改造后,效果比较明显,取得了预期的效果,但也发现在访问高峰时防火墙的负荷较重,经过测试和分析,问题出在两个地方,一是校园网内部用户每次访问做域名解析时,都需通过防火墙进行NAT转换,才能到DNS服务器上;二是校园网内部用户在访问校园网内的服务器时也需要通过防火墙进行NAT转换,这两个方面都大大增加了防火墙的负荷。针对这个问题我们再次做了改造,在核心交换机下直接再增加一台DNS服务器,负责校园网内部用户访问的域名解析工作(由于负荷分摊,两个DNS服务器都可以用一般PC机来实现),并在这台DNS服务器上把学校里所有服务器的域名都解析为它的私有地址,这样不仅域名解析不需要频繁通过防火墙进行NAT转换,访问校园网内的服务器时也不需要通过防火墙进行NAT转换,并且对校园网内核心交换机下各部门服务器访问只需到核心交换机就可完成,根本不需要经过防火墙。通过这次改造后,发现防火墙的负荷大大减少了,优化了校园网的结构,提高了访问效率。

**注释及参考文献:**

[1]钱爱增,谢延红,陈德山,等.双出口校园网的设计与实现[J].德州学院学报,2004, 20(4):59-60.
[2]刘伟,崔永锋.基于防火墙和策略路由的校园网双出口实现[J].周口师范学院学报,2006,23(2):101-102.
[3]刘伟,崔永锋.校园网双出口实施中的问题及解决方案[J].计算机时代,2006,7(7)19-21.
[4]李磊,刘秋鸣,章志勇,等.校园网双出口路由的设计与实现[J].教育信息化,2006(15):37-38.
[5]郭强.使用 cisco firewall pix 实现局域网络双出口[J].吉林师范大学学报(自然科学版) ,2006(1):72-73.
[6]崔骋宇.解决双出口校园网瓶颈[J].网管员世界,2006(3):74-75.

# Reform and Implementation of Double-Export-Links Campus Network

LIU Li-ping[1,2], WU Zheng-qi[2], WANG Lin[2]
*(1. College of Computer Science, Sichuan University, Chengdu, Sichuan 610065;*
*2.Chengdu Textile College, Chengdu, Sichuan 611737)*

**Abstract:** With the development of network technology, the resources provided by internet are being enriched constantly. Whereas, in our country, university's utilization ratio of resources on internet is low currently. (下转60页)

[5]牛星,欧名豪.青岛市开发区土地集约利用评价与研究[J].中国农业资源与区划,2007,28(5):47-51.
[6]陈成,吴群,王楠君.开发区土地集约利用研究—以徐州市开发区为例[J].国土资源科技管理,2005,4(5):46-50.
[7]翟文侠,黄贤金,杜文星.开发区土地集约利用研究--以江苏省为例[J].区域研究与开发,2006,26(1):101-105.
[8]刘庆.开发区土地持续集约利用与对策研究一一以江苏省为例[D].南京农业大学,2006.

# Study on the Evaluation for the Intensive Use of Development Region Land

## ——A Case of TEDA

XU Song-qing

*(College of Geographical Science, Fujian Normal University, Fuzhou, Fujian 350007)*

**Abstract:** The intensive use of urban land is an objective requirement for sustainable development. As a case study on Tianjin Economic Development Area(TEDA), the evaluation system and the weight of intensive use of land are studied in this paper. And as the Hsinchu Science-based Industrial Park in Taiwan for reference, this paper discussed the level of intensive land use of the Tianjin Economic Development Area at this stage, and on the basis of this put forward the suggestions for improving level of intensified development region land use.

**Key words:** Development region; Intensive use; Evaluation

(上接55页)

It is well known that there is a bottleneck between public network and CERNET, which causes the very slow velocity to access each other and limites the enhancement of network application's level in some universities. Through example of double-export-links campus network in our college,this paper introduced how to access outer resources for inner users or to access our college's webserver for outer guests at a high speed by using double-export-links. This method not only solved the problem of speeding the velocity of connection between campus network and public network but also realized the chain circuit redundancy and inner network's safety.

**Key words:** CERNET; Double-export; NAT