《网管员世界》杂志社　编
飞思科技产品研发中心　监制

NetAdmin World

《网管员世界》2005超值精华本

特别赠送：

趋势科技防毒墙网络版 OfficeScan 7.0

Surfcontrol（美讯智）Web Filter试用版

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
URL:http://www.phei.com.cn

《网管员世界》2005
超值精华本

《网管员世界》杂志社　　编
飞思科技产品研发中心　监制

電子工業出版社
Publishing House of Electronics Industry
北京·BEIJING

内容简介

《网管员世界》月刊是目前国内唯一一本面向企业网络管理者的专业实用性网络技术管理媒体。本书是2005年《网管员世界》各期内容的精华汇集，按照栏目分类进行了汇总，分为管理维护、故障诊断、攻防实战、知识课堂、网管工具等5章，精选收录了二百余篇实用网络管理经验文章，内容详尽实用，保留价值高。同时，《网管员世界》又联系了著名网络安全公司趋势科技和美迅智，为读者提供了相关安全软件的试用版本。附书光盘内容为Surfcontrol Web Filter软件和趋势科技防毒墙网络版OfficeScan 7.0软件。

本书可作为网管员的日常工作手册，在工作中遇到问题时供随时查找；也可作为网络技术人员或者网络爱好者提高网络管理和维护水平的进阶读本。

图书在版编目（CIP）数据

《网管员世界》2005超值精华本 / 《网管员世界》杂志社编. —北京：电子工业出版社，2006.2
ISBN 7-121-02182-X

Ⅰ.网... Ⅱ.网... Ⅲ.计算机网络－管理 Ⅳ.TP393.07

中国版本图书馆CIP数据核字（2005）第157699号

责任编辑：武 嘉
印 刷：北京中科印刷有限公司
出版发行：电子工业出版社
北京海淀区万寿路173信箱 邮编：100036
经 销：各地新华书店
开 本：889×1194 1/16 印张：31.25 字数：900千字
印 次：2006年2月第1次印刷
印 数：6 000册 定价：49.80元（含光盘1张）

凡购买电子工业出版社的图书，如有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系电话：010-68279077。质量投诉请发邮件至zlts@phei.com.cn，盗版侵权举报请发邮件至dbqq@phei.com.cn。

FOREWORD 前言

《网管员世界》（http://www.netadmin.com.cn）是由中国电子信息产业发展研究院（CCID）主办的一个专业网络技术管理媒体，也是目前市场上惟一一个针对企业网络管理者的实用技术媒体。

创刊近五年来，《网管员世界》一直致力于提高企业网络管理技术人员的管理水平，进而提高企业 IT 基础设施的运营水平；在刊物内容上，坚持以技术应用为主、注重实用性和知识性，帮助网管员解决日常工作中碰到的实际问题，为网管员排忧解难。由于其内容非常契合广大网管员的实际工作需求，创刊以来迅速获得了网络界各方面人士的强烈认可，邮局订阅量直线攀升。许多近期刚刚接触到《网管员世界》的读者纷纷表示相见恨晚，希望能拥有已出版的全套《网管员世界》杂志。

为了方便网管员朋友从几十本刊物中寻找所需资料，便于收藏保管，从 2003 年开始，我们在电子工业出版社等单位的协助下，陆续编辑出版了《〈网管员世界〉精华本》、《〈网管员世界〉2004 超值合订本》等，得到了广大读者的热烈欢迎。

本书是《网管员世界》月刊 2005 年全年刊物精华内容的汇集。本书收集了《网管员世界》2005 年各期刊物中对网络管理技术人员关系比较密切而且比较优秀的数百篇文章；为了便于读者查阅，基本上仍然按照原栏目进行汇总、排序。同时，《网管员世界》又联系了著名网络安全公司趋势科技和美迅智，为读者提供了相关安全软件的试用版本。

本书可作为网管员的日常工作手册，在工作中遇到问题时供随时查找；也可作为网络技术人员或者网络爱好者提高网络管理和维护水平的进阶读本。

参加本书编写的人员有杨文飞、张碧薇、孙浩峰、孙红娜、翟振伟等，杨文飞和孙浩峰对全书进行了统稿。

由于时间紧张，加之编者水平所限，书中错误之处欢迎读者批评指正，以利于我们今后改进。

联系方式

咨询电话：（010）68134545　　88254160

电子邮件：support@fecit.com.cn

服务网址：http://www.fecit.com.cn　　http://www.fecit.net

通用网址：计算机图书、飞思、飞思教育、飞思科技、FECIT

《网管员世界》杂志社

飞思科技产品研发中心

CONTENT目录

第 1 章　管理维护

第 2 章　故障诊断

第 3 章　攻防实战

第 4 章　知识课堂

第 5 章　网管工具

NetAdmin World 2005

第 1 章　管理维护

“虚拟”的Web服务器

肇庆职业学校 卢江兴

在学校信息化的大潮中，各中小学校都要进行信息化建设。在现阶段，校园信息化对校园网的要求也比较简单：只要有对外的Web服务器、校园网内的计算机能上互联网、校园网有一定的管理功能即可。而中小学校的实际情况是：经费紧张、可用于信息化建设的资金都比较少、缺少专门的计算机人员对计算机及网络进行管理。

要满足上述校园网的基本要求，一般可采用的方法有两种。

（1）申请少量静态IP，在互联网上架设Web服务器对外提供网页服务，并通过NAT方式使校园网内用户连接上Internet。这种方式对于架设在外网的Web服务器有一定的要求，至少要具有一定防病毒、防攻击的能力，所以要有专人进行管理和维护，包括购买杀毒软件、定期对系统打补丁、升级病毒库等。

（2）采用在互联网上申请虚拟主机的方式提供Web服务。而虚拟主机服务提供商所提供的服务有相当多的限制，缺乏灵活性。

下面提供一种简单可行、廉价、只需少量管理的方案来满足上述校园信息化的要求。

通过ADSL、NAT等方法使得校园内的用户可以上互联网，通过动态域名解析、虚拟主机重定向等方法，使得设置在校园网内的主机可以对外提供Web服务。由于Web主机在校园网内，使用何种类型的操作系统可由自己决定，具有相当的灵活性。

假定校内的计算机均联网，使用同一网段IP地址：192.168.10.X，设有一网控中心，架设ADSL电话线，要对外提供Web服务的计算机（IP地址：192.168.10.2）、提供NAT防火墙的计算机（IP地址：192.168.10.1）放在网控中心。网段内的其他计算机的IP地址可以使用DHCP服务器自动分配。

本来最简单的代理上网方式是，使用Windows 2000的共享连接，但是共享连接有一个限制：只能使用IP地址为192.168.0.X的网段，不利于内部网络的扩展。而使用RedHat 7.2操作系统配置iptables防火墙，则内网IP地址没有这个限制，可以在校园内部署多个网段（见图1）。

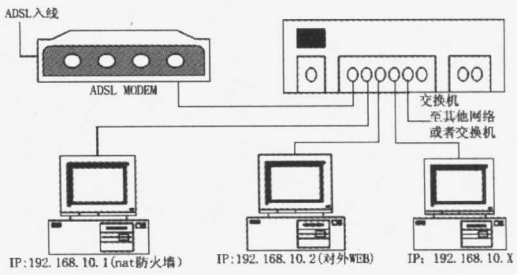

图1

配置NAT防火墙

硬件：赛扬667、128MB内存、RTL8139网卡一张、IP：192.168.10.1。

软件：安装RedHat 7.2操作系统、配置PPPOE拨号连接、iptables规则。

NAT计算机使用ADSL上网，从电信获得的是动态IP地址，需使用动态域名解析软件，现在有较多的公司提供这种服务，我选用的是希网（http://www.3322.org）的动态解析方案。希网提供Windows 、Linux、Unix等多种版本的解决方案。先从希网注册免费域名（如http://zqzy.3322.org），然后下载Linux版客户端软件（ez-ipupdate-3.0.10-linux-i386.tgz）。解压软件包，安装到NAT计算机/usr/local/目录，可以得到ez-ipupdate程序及qdns.conf配置文件，将注册的域名和密码写入qdns.conf文件，配置好qdns.conf文件后，运行（/usr/local/ezip/ez-ipupdate -c /usr/local/ezip/qdns.conf）语句，至此在互联网上可以通过域名http://zqzy.3322.org访问NAT计算机。

要对外提供Web、FTP等服务，一般的做法是：在NAT计算机上安装Web、FTP服务器软件。我认为这样做会使得NAT计算机负担过重，而且过多的服务集中在同一计算机上，打开太多的端口，会使得NAT计算机不安全。

基于以上考虑，决定在NAT计算机使用端口重定向技术，将从互联网上对动态域名http://zqzy.3322.org的访问重定向到内网的192.168.10.2计算机。这样做，无需在NAT计算机安装过多的服务，又可将Web服务器与互联网进行隔离，提高了安全性、灵活性。

为了开机就可以自动执行，实现主机重定向，把上述内容写到/etc/rc.d/rc.iptables文件，并在/etc/rc.d/rc.local最后加上以下语句，将访问本机（NAT计算机）8080端口的访问重定向到IP地址192.168.10.2的80端口，即Web服务器。

/etc/rc.d/rc.iptables

```
redir --lport=8080 --caddr=192.168.10.2 --cport=80 &
```

建立文件/etc/rc.d/rc.iptables 用于执行 iptables 规则，设置可执行权限，只要执行文件就可完成 iptables 防火墙规则的配置。

rc.iptables 文件如下：

```
#!/bin/sh
#这里加上清空、重置规则表语句 （略）
# ① 通过 /etc/rc.d/rc.ppp0 求得 ppp0 IP 存放在 /tmp/txt41 中
ppp_ip =`cat /tmp/txt41`
#以下进行重定向，其中 $ppp_ip 表示 ADSL 获得的动态 IP
#将对动态 IP $ppp_ip 80 端口的访问重定向到 8080 端口
iptables -t nat -A PREROUTING -j REDIRECT -p tcp -d $ppp_ip --destination-port 80 --to-ports 8080
#以下设置 NAT 代理
iptables -t nat -A POSTROUTING -s 192.168.10.0/24 -j MASQUERADE
#每当 IP 改变，更新动态域名服务
/usr/local/ezip/ez-ipupdate -c /usr/local/ezip/qdns.conf
```

配置 Web 服务器

硬件：IP 地址为 192.168.10.2

软件：安装 Windows 2000 操作系统+IIS5.0+ASP

这样的选择是基于单位内的实际情况的，因为对于 Windows 会有更多人员使用它，况且 ASP 也易于编程。在 Web 服务器通过 ASP 编写网页，使用 Web 上传的方式上传文件，所以没有专门配置 FTP 服务器。

自动化问题

由于电信局故障、通信线路故障，NAT 计算机的 PPPOE 拨号连线发生中断，不能连上互联网的情况是会发生的。或者电信局设置 DHCP 租用时间较短，使得 NAT 计算机的 IP 频繁变动。这两方面原因都会使 NAT 计算机的 IP 发生变化，以至主机重定向不正确。为了让 NAT 计算机能自动处理这些问题，需要知道更新后的动态 IP 地址的值是多少，也就是上面 rc.iptables 文件中提到的变量 $ppp_ip。但由于 Linux 不直接提供获取这个变量的命令，Linux 只提供 adsl-status 、ifconfig ppp0 命令，虽然这些命令能显示较多的信息，但我们只需要 PPP0 的 IP 地址。可以编写一程序从 adsl-status 中获取地址信息。程序如下。

文件 /etc/rc.d/rc.ppp0

```
#!/bin/sh
/sbin/adsl-status |grep "inet" > /tmp/txt1
sed -e 's/[a-z|A-Z|:|-]//g' /tmp/txt1 > /tmp/txt2
sed -e 's/\(.*\) \(.*\) \(.*\)/ \1<\2 \3>/' /tmp/txt2 > /tmp/txt3
sed -e 's/<.*>//g' /tmp/txt3 > /tmp/txt41
```

运行/etc/rc.d/rc.ppp0 程序，将 ADSL 连线 ppp0 的 IP 地址写入到/tmp/txt41 文件。地址的形式是：XX.XX.XX.XX

在/etc/rc.d/rc.iptables 文件中①处，加上 /etc/rc.d/rc.ppp0 或直接加入以上指令。

在 /etc/rc.d/rc.iptables 文件最后，加上以下语句，使得每次 IP 地址改变都发 E-mail 到 is163@163.net 邮箱。

```
Ifconfig > /tmp/txtcron.txt
date >>/tmp/txtcron.txt
mail -s "ppp from 192.168.10.1" is163@163.net < /tmp/txtcron.txt
```

设置 CROND 服务，每小时执行一次/etc/rc.d/rc.iptables 文件。

在实际运行中，NAT 计算机代理全校七个机房 400 多台计算机上互联网，通过虚拟主机重定向对外提供 Web 服务，已经连续运行两年，也无需专门管理。

只要收到 E-mail 就表示计算机正常运行。在实际使用时，为了方便管理，Linux 计算机还开启了 ssh 服务，可以从收到的 E-mail 中得到 PPP0 连线的 IP，从互联网上对 Linux 计算机进行远程管理。内部网中的 Web 主机安装了 Windows 2000 的终端服务器，透过主机重定向，在互联网上也可以直接登录到内部网的 Web 主机进行远程管理。

给园区网一对无线的翅膀

中国科学院研究生院网络中心 史剑雄

中国科学院研究生院共有三个教学园区，其中 2003 年 9 月份启用的新教学大楼是中关村园区的主教学楼。该教学楼的功能定位为博士生教学和一些讲座性的课程，需要有远程实时和交互的功能，目前已与玉泉路园区的远程教育系统通过千兆光缆实现了互联。本文将简要地介绍该教学楼无线网络的设计、配置和使用的情况。

中科院研究生院中关村教学楼是一幢符合智能建筑 5A 标准的新型多媒体教学楼。其计算机网络系统的线缆主干部分采用 AVAYA 公司的万兆室内光缆，水平部分采用 AVAYA 公司六类非屏蔽双绞线。同时，每个教室均有光缆直接接入楼内的网络控制室，为适应将来的网络发展留出了空间，同时也为三网合一准备好了物质基础。作为有线网络的补充，整个大楼还进行了无线覆盖，使得学生们在楼内的任何地点均可以方便地使用无线网络。

由于目前无线网络的带宽只有 11Mb（802.11b），且其使用的方式为共享方式，因此，在设计无线网络时，为了保证

无线网络的使用效果，根据教室的分布、大小和使用情况，以及无线访问点 AP（Access Point）的有效容量，我们确定了每个教室内 AP 的数量，如 400 人教室放置了五个 AP，300 人教室放置了四个 AP，200 人教室放置了三个 AP，100 人教室放置了两个 AP，100 人以下的教室及教师休息室和走廊均放置了一个 AP。为了防止 AP 之间的互相干扰，我们采用跳频的方式，使得每个 AP 均有自己的频段。

在设备选型上，我们采用了 3COM 公司的无线产品 AP8000，它能够提供现有的、强健的、多层可扩展安全解决方案。它支持 40 位 WEP 加密、128 位共享加密、IEEE 802.1x 和 RADIUS 验证。此外，它还支持可扩展验证协议（EAP），能够轻松地和网络基础设施进行集成。在没有集中 RADIUS 验证服务器的地方，3Com Access Point 8000 能够提供动态安全链路（Dynamic Security Link）技术，让用户安全地登录网络。该接入点的内嵌数据库可以支持多达 1 000 个用户名和口令。

在管理方面，Access Point 8000 支持 SNMP、HP Open View 和 3Com Network Supervisor，可以在一个中心点实现无缝的网络集成和完整的网络管理。其他的功能和特性可以通过 3Com 网站的 Live Update 轻松获得。

配置无线网络

在配置方面，3COM 的 Access Point 8000 采用友好的 Web 界面，配置非常简单，具体配置如下。

首先保证计算机与 AP8000 相通，打开 Internet Explorer，输入 AP8000 的 IP 地址，或者在 AP8000 随机光盘中安装 3Com Wireless Infrastructure Device Manager 软件，运行此软件，双击 AP8000 图标或单击配置按钮，可进入如图 1 所示的界面。

单击“Access Point properties”项，可以在“Device Name”对话框中对 AP 重命名，在“Device Location”对话框中描述 AP 所在的位置，在“Wireless LAN Service Area”对话框中命名无线局域网服务区域，单击“Save”按钮保存设置。选择“Network Properties”，可对 AP 进行网络设定，在“Network Setting”中选择“Obtain IP address automatically”，AP 将自动获得 IP 地址，选择“Specify an IP address”指定 AP 的 IP 地址、子网掩码和网关的地址。在“Wireless DHCP Server Setting”中选择“Enable”允许 AP 在网络中没有 DHCP 服务器时自动充当 DHCP 服务器，选择“Disable”则在任何网络环境下均不作为 DHCP 服务器分配地址。单击“Save”按钮保存设置。

进入“Data transmission properties”进行数据传输设定：在“Clear Channel Select”中可以选择 AP 对使用的频道设定，选择“On AP”将自动选择最好的频道进行无线连接，选择“Off”将手动指定 AP 使用的无线频道。在手动选择 AP 使用的频道时，在“Channel”中选择 AP 使用的频道，系统推荐使用 1、6、11 频道。在“Network Traffic Accelerate”中选择网络通信加速所采用的标准；选择“On”将采用 3COM 增强标准；选择“Off”将采用 Wi-Fi 标准；在“Data Preamble”中选择数据采用方式；选择“Short”将采用增强方式；选择“Long”将选择“WiFi”方式；在“Data Rate Management”中选择“Automatically set the best data rate AP”将自动采用自动变速方式否则将采用手动指定方式；在“Radio Antenna”中选择“Diversity On AP”将使用两个天线，否则 AP 将只使用左侧的天线；在“Transmit Power”中选择信号发射强度设定。单击“Save”按钮保存设置。

进入“Advanced settings”可进行高级设定，在“Load Balancing”选项中选择“On”可以限定无线用户数量（1~256），选择“Off”不限制用户数量，默认设置为“Off”；在“Client to Client Blocking”选项中选择“On AP”将进行用户隔离，即用户间不可通信，选择“Off”不进行用户隔离，默认设置为“Off”；在“Client List Timeout”中可以选择用户超时挂起的时间，默认设置为 60 分钟；在“Broadcast WLAN Service Area（ESSID）”选项中选择“On AP”将广播 ESSID，否则不广播 ESSID，默认设置为“On”。

至此，AP 已经可以正常运行了，接下来就要对其进行安全设置，如图 1 所示。

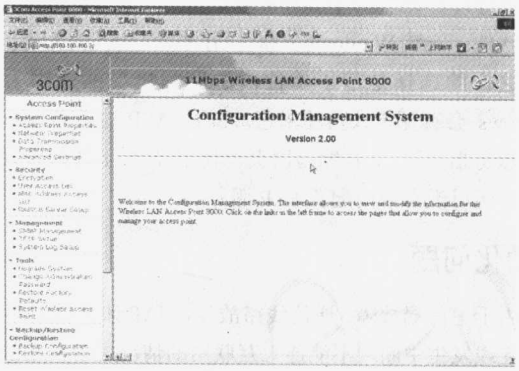

图 1

安全设置

打开 Security 下的 Encryption 您将会看到如图 2 所示界面。

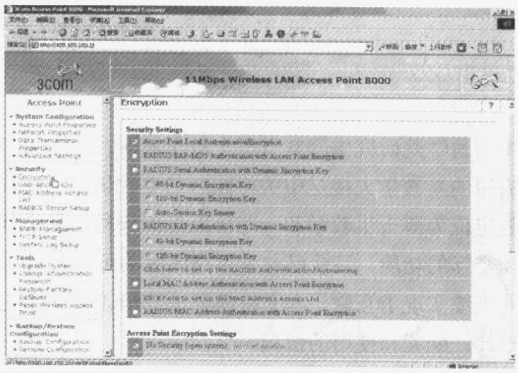

图 2

在此处可以对 AP 进行加密设置，其中包括 40 位加密、128 位加密以及 128 位动态加密、针对 MAC 地址的加密，或其他第三方加密程序加密。

在安全设置中：

选择“Access Point Local Authentication/Encryption”将指定 AP 使用 AP 本身的加密与认证机制。

选择“RADIUS EAP-MD5 Authentication with Access Point Encryption”将指定 AP 使用 AP 的加密和 RADIUS EAP-MD5 认证机制。

选择“RADIUS Serial Authentication with Dynamic Encryption Key”将指定 AP 使用动态加密的 RADIUS 认证机制，在此方式下可以选择 40 位或 128 位动态加密，并指定是否自动更新。

选择“RADIUS EAP Authentication with Dynamic Encryption Key”将指定 AP 使用动态加密的 RADIUS EAP 认证机制，在此方式下可以选择 40 位或 128 位动态加密。单击“Click here to set up the RADIUS Authentication/Accounting”可以进行 RADIUS 服务器的设定。

选择“Local MAC Address Authentication with Access Point Encryption”将指定 AP 使用 AP 本身的 MAC 地址认证与加密机制。单击“Click here to set up the MAC Address Access List”可以设置 MAC 地址的存取列表。

选择“RADIUS MAC Address Authentication with Access Point Encryption”将指定 AP 使用 RADIUS 的 MAC 地址认证与 AP 本身加密机制。

在加密设置中：

选择“No Security （open system）”AP 将没有加密，单击其后的“more information”可以看到此项内容的具体说明。

选择“40-bit Encryption Shared Key （Wi-Fi），AP”将使用 40 位共享加密方式，单击其后的“more information”可以看到此项内容的具体说明。在此方式下可以选择“Enter a string to generate the shared keys”指定一个 6~30 位的字符串作为密钥或选择“Specify shared keys and which key to use”单击“Modify Keys”按钮输入四组 10 位十六进制字符。

选择“128-bit Encryption Shared Key”，AP 将使用 128 位共享加密方式，单击其后的“more information”可以看到此项内容的具体说明。在此方式下可以选择“Enter a string to generate the shared keys”指定一个 6~30 位的字符串作为密钥或选择“Specify shared keys and which key to use”单击“Modify Keys”按钮输入四组 22 位十六进制字符。

选择“128-bit Dynamic Security Link”，AP 将使用 128 位动态加密方式，单击其后的“more information”可以看到此项内容的具体说明。单击“Click here to set up or modify the User Access List”可以设置用户的存取列表。选择“Require Windows user authentication”可以让 AP 使用 Windows 的用户认证。

可以通过“User access list”来指定用户存取；通过“MAC Address access list”来观察及指定可以与 AP 进行通信的 MAC 地址；通过“RADIUS SERVER SETUP”对 RADIUS 服务器进行设定与配置。

在管理页面中包括简单网络管理协议管理（SNMP Management）、一般文件传输协议管理（TFTP Setup）以及系统记录设置（SYSTEM Log setup）。

其页面分别为：设置 SNMP 管理的各项参数；设置 TFTP 服务器的 IP 地址和使用的端口；设置系统登录信息的存储方式及地址。

在工具页面中包括系统升级（Upgrade system）、更改管理员密码（Change administrator password）、恢复系统默认值（Restore factory default）以及重新启动 AP（reset wireless access point）。

单击“Change”按钮设定 TFTP 服务器的 IP 地址，TFTP 软件可在 AP8000 的随机光盘中找到，在文件名栏中填入要升级的固件的文件名，单击“Upgrade Now”按钮即可进行固件的升级。

备份以及恢复配置（Backup/Restore configuration）可进行 AP 设置的备份与恢复。

数据统计页面可以对 AP 中的射频、以太网、接口、信道选择的转发进行统计。

系统情况（System Status）页面能够让用户对当前连接用户情况（Currently Associated Clients）和系统摘要（System Summary）有所了解。

目前，中关村教学楼的无线网络运行稳定，达到了设计的要求，用户反应良好。

“升级”我们的校园网

南京　吉翔　朱爱兵

目前，在高校中已经建立起了规模大小不等、技术水平各异的校园网络体系，并相应地开展了一系列架构在校园网络上的各类服务；随着各种应用服务的深入、网络覆盖范围的扩大，早期所设计、建设的校园网中，无论带宽、拓扑、设备、服务等均越来越不能满足当前学校发展的需要，一些管理、运行中的问题也逐步暴露出来。作者根据南京农业大学浦口校区校园改扩建工程中所进行的规划、设计，对在新的网络技术、管理手段及新的设备不断涌现的形势下，解决

高校校园网的改扩建进行探讨和分析，试图推出一套指导性的应用准则。

南京农业大学浦口校区现有在校生 4 000 人，教职员工 800 人，占地 650 亩；校区内的 35 幢主要建筑分为三个区域：教学行政区、学生生活区和教工生活区；校园网于 2000 年完成第一期的建设，范围覆盖校区中主要的 20 幢楼宇。校园网主干采用了千兆以太网的技术，网络的逻辑拓扑为星型结构，在网络中心安装了一台 Nortel 的 PassPort8610 十槽三层核心交换机，在教学行政区建立了九个接入点，均采用 BayStack420-24T 与核心交换机以 GE 相连。在学生生活区安装了一台 Nortel 的 Accelar1150 千兆全光三层交换机作为汇聚结点（可提供两个千兆单模光口和六个千兆多模光口），在学生住宿区每幢楼中以堆叠的 Bay420-24T 为接入层设备上连 Accelar1150；在教工生活区的两幢楼中安装了两台 BayStack450 作为汇聚，均以千兆单模光纤上连核心交换机，以百兆多模光纤收发器下连实达 S1924F+至每幢住宅楼；至 2002 年底，校园网信息点共 1 400 个，接入用户达 600 个。

校区共有八个 C 类 IP 地址，一律采用分配公有地址给用户，除学生生活区外，开放全部访问，学生生活区及校区的校外访问通过一台富士通公司的 MS610（PIIIX700/1GM/108GSCSI HD）服务器完成。网络拓扑图如图 1 所示。

根据校区的发展规划，在 2008 年前，在校生将达到 8 000 人（其中研究生 1 000 人），学生生活区共建设 10 幢住宿楼，教学区新建图书馆、新实验楼、行政办公楼，全区信息点达到 3 500 个。

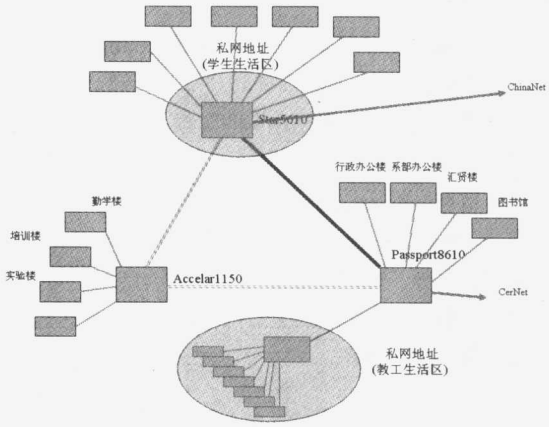

图 1

存在的问题及矛盾

现有校园网在建设完成后近两年的运行中，虽然取得了良好的社会效益和经济效益，但也暴露了许多思路、结构、管理中存在的问题，主要表现在以下几点。

（1）网络设计定位有误：由于建设中一方面片面追求校园网的性能指标，一方面限于经费的制约，部分设备选购不当；如千兆堆叠交换机数量购置得较多（达 30 台），但三层可控制设备只购置了两台，造成管理、安全方面的极大欠缺；Bay420-24T 为一款千兆可二层交换机（支持 802.1Q、MAC 地址绑定，IGMP，最大可堆叠到 192 个 100M 端口）无法进行有效的网络安全管理，特别在学生生活区，盗用 IP 地址、利用 ARP 欺骗、私设代理等情况日益严重。

（2）网络通信考虑得多，应用服务考虑得少：在设计、规划进行调研时，将大部分力量均放在网络设计、产品选型，而网络服务及应用考虑得不够，认为这是校园网建成以后的事；当有了应用需求时，网络无法提供所需的环境；例如当建设远程视频会议系统时，要求在网络链路中提供全链路的 QoS 质量保证，普通的网络设备无法满足；在校园网建设时，由于未考虑到具体的应用，平均分配了设备配置资金，部分地区，如学生生活区千兆堆叠交换机 60%以上的性能被浪费，而部分地区设备的指标达不到要求。

（3）网络扩容能力不够：由于对学校发展的速度缺乏足够的认识，思想上不够解放，对网络结构、设备的可扩充性考虑不够，如在学生生活区的 Accelar1150 最多只能提供八个千兆光纤接口，新增的宿舍楼只能以百兆接入，随着新的图书馆、实验楼及学生宿舍的建成，原有规模的校园网设备更是严重缺乏。

（4）网络管理难度加大：随着接入用户的增加，无论是维护、收费还是管理难度越来越大，对于用户拖欠通信费用，网络中心只能采用禁用端口的方法来处理；而某些地区，多台设备上网是采用 Hub 或 Switch 接入的,所以不能全部禁用；对于某些情况，网络中心的工作人员疲于应付。

（5）网络结构不合理：由于校园网采用星型结构,当光纤链路或中心光接口出现故障时,一些地区不可避免地中断网络服务，部分地区的网络扩展无法实现。边界路由器负荷过高，由于校园网在特殊时刻寻根性很强，如下午 4:00 以后，晚上 9:00 以后，访问 Internet 的访问流量大幅增长，由于我们的虚网划分在主干交换机上进行，默认路由均指向边界路由器，边界路由器（SSR2000 的 CPU 负荷）在上述时间段内负荷超过 60%~70%。

校园网改造升级目标

根据此种情况，校区计划在近期进行校园网的改造升级，由此我们对如何改造校园网的设计进行了一些探讨，充分分析了在一期工程中的经验和教训，得出了以下共识。

（1）校园网是服务应用为主的一项基本信息资源基础建设工程：校园网应将其基本目的定位在为教学、科研、管理及生活服务上，以满足学校事业发展为第一目的；在建设过程中注重投资效益。

（2）要对网络技术进行充分理解和认识：当前各类新的网络技术层出不穷，在非研究性校园网中，是否可采用超前的技术一直是大家争论的焦点；比如万兆以太网、六类综

合布线的问题。对此，我们认为，既然校园网是以用为主，当然应当采用性价比较高、技术较为成熟的技术和设备，同时在通过对网络技术发展前景理解的基础上，为今后升级换代留有足够的余地。

（3）校园网的改造升级必须紧紧依托于现有网络总体结构和设备、光纤路由，保证前期所投入的光纤线路、网络设备仍能发挥其应有的作用，节约资金，以最少的投入获得最大的收益。

（4）充分发挥管理手段：一个校园网，建设重要，管理更重要。要管理好校园网，除了网管人员的专业素质和道德水准外，网络规划和设计以及网络设备的选择是非常重要的。

校园网改造方案

以此为依据，我们提出了全网的改造方案。

（1）原有的星型结构的校园网架构更改为冗余的环型核心层；以 PassPort8610（新图书馆网络中心）、Accelar1150 和实达公司的 S5610 三层核心交换机构成了环型的三个节点，其间以 GE 构成主干；只购置了一台新的核心设备 S5610（配置了 16 个 GBIC 端口），原有设备得到充分利用。

（2）原有在学生生活区中的 Bay420 交换机全部撤换到新图书馆、新实验楼等注重性能而对安全性要求不高的环境中；在学生生活区购置了 10 台实达公司的 S3550-24T 三层交换机和 25 台二层交换机（包括 S2024 系列、S1916F+/S1924F+/1926F+系列，以上设备均支持 802.1X/Q，支持带宽管理），论证、计费系统相应采用了实达公司的 SAM Radius 系统。

（3）针对教育网境外访问流量较大造成的费用较高的问题，我们向中国电信申请了一条 Mb/s 级带宽的干线，解决境外访问费用及境内公网的访问速度问题；另外也可在单一链路失效时，互为备份，保证校园网对外出口的畅通无阻；我们未采用一般的将所有出口均置于网络中心的做法，而是放在对外访问量较大的学生生活区汇聚中心，一是充分利用 S5610 的 55Mb/s 的三层包转发率和 128Gb/s 的背板带宽，二是使自 S5610 中 NAT 出来的流量不需经过环网链路，直接通过电信的边界路由器出去，大大降低了网络中心的边界路由压力。

（4）在学生生活区和教工生活区全部采用 DHCP 分配地址，一来节约了大量 IP，二来通过 Radius 计费系统进行交换机、端口、用户名的绑定，提高了网络系统的安全性。网络拓扑图如图 2 所示。

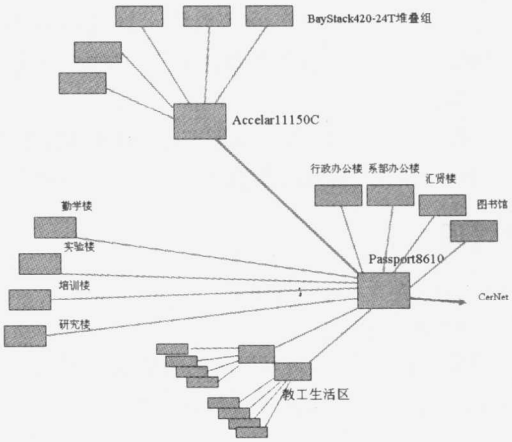

图 2

方案特点

该方案的特点如下。

（1）在原校区的光纤链路不作大规模更改的情况下，拓展网络结构，扩大校园网覆盖面，保证原有光纤的冗余。

（2）用实达公司的 SAM 系统，加强校园网的论证、计费管理，规范上网用户行为。

（3）充分利用硬件 NAT 功能，减轻节点交换机压力及服务器投入，节约合法 IP 地址，强化管理。

（4）充分利用原有网络设备的资源，保证在校园网升级改造的过程中没有浪费，并为网络进一步的扩展保证足够的可扩充余地。

让 RS6000 AIX 搭上网络快车

西安电子科技大学　吴文华

AIX（Advanced Interactive Executive）是 IBM 公司为其 RS6000 小型机配置的操作系统，因其采用的是 UNIX 内核，所以俗称“Advanced IBM UNIX”，完全符合 X/open、XPG4、UNIX 98、Spec1170、CORBA、OpenDoc、IEEE POSIX1003.1c 等工业标准，RS6000 在全球的装机量已经超过一百万套，目前我国银行、证券、航空、邮电、通信等各行业都有采用。

今天的局域网与外界的联系必不可少，所以对系统管理人员来说，掌握网络设置也是必需的。大多数 UNIX 系统上用命令设置 TCP/IP，例如 Ipconfig 和 Route，然后通过初始化文件使配置永久生效。AIX 也可以这样做，但 AIX 还可以使用一条简单的命令通过菜单方式实现 TCP/IP 设置，这个命令就是 mktcpip，在进行 TCP/IP 设置之前，对于您的系统首先要知道以下信息：IP Address、Host Name、Domain Name、Subnetmask、Name Server、Gateway Address。

进行设置时，在命令提示行下输入：

#smit mktcpip

首先在“Available Network Interfaces”屏幕选择适当的网络接口，这个接口在系统启动时由 cfgmgr 认出，并且设置到 ODM 数据库里。接着屏幕会出现“Minimum Configuration & Startup”菜单，然后把相关的信息填入即可。如果对有的信息不清楚，您可以不填，系统会采用默认值，但至少要填写“Hostname”和“Internet Address”，在菜单屏幕里您还可以设置子网掩码、网络接口、名字服务、网关和电缆类型等，在“CABLE TYPE”选择的参数含义分别为 bnc-细缆、dix-粗缆、tp-双绞线。

在进行设置时，可以随时按下 F1 键打开联机帮助，如果还需要进一步地设置或修改 TCP/IP，可用以下命令。

路由管理

（1）增加路由，输入命令：

smit mkroute

按照菜单填写目标地址和默认网关地址，目标类型可以选择“net”或“host”，MeTRIC 域默认值为 1。

（2）删除路由

输入命令：

smit rmroute

然后在各个域填写适当的值即可。

（3）刷新路由

输入命令：

smit rmroute

屏幕显示如下：

Flush routing Table

TYPE or select values in entry fields.

Press Enter AFTER making all desired changes.

[Entry Fields]

Flush routing Table in the Current Running System yes

Flush routing Table in the Configuration Date Base no (effective in the next system restart)

如果只想暂时刷新路由表，而保持 ODM 数据库中的路由信息，就接受默认值。如果还要清除 ODM 中的路由表信息，“Flush Routing Table in the Configuration Data Base”域就要选“yes”。

网卡配置

（1）改变网卡的配置

输入命令：

smit chinet

（2）删除网卡配置

输入命令：

smit rmroute

然后在各个域填写适当的值即可。

SMIT 删除网络接口没有确认提示！

配置域名服务器

AIX 有三种类型的 DNS：主域名服务器（Primary）、次域名服务器（Secondary，主域名服务器的备份）、代理域名服务器（Cache，自己不进行域名解析，只将请求发到上层域名服务器）。域名服务 DNS 的守护进程是 named，它要用到一些配置文件，编辑这些文件，然后启动守护进程 named 即可。

主域名服务器

（1）编辑 etc/named.boot 文件，确认包括以下内容，例如：

/etc/named.boot

directory/etc

domain win-service.com （默认域名）

primary win-service.com named.date (域内其他主机名和地址转换信息文件名)

primary 0.168.192. in-addr.arpa named.rev (主机名和地址转换信息文件名)

primary 0.0.127. in-addr.arpa named.local (本机主机名和地址转换信息文件名)

cache named.ca

（2）编辑 etc/named.ca 文件，确认包括上层域名服务器的主机名和 IP 地址，例如：

/etc/named.ca

9999999 IN NS dns.xb.sx.cn

dns.xb.sx.cn 9999999 IN 201.101.99.55

（3）编辑 etc/named.[domain_name]local 文件，确认包含域名服务器（NS）记录和指针（PTR）记录，例如：

/etc/named.local

@ IN NS r24.win-service.com

1 IN PTR localhost.win-service.com

（4）编辑/etc/named.[domain_name]data 文件，包含更新时间、地址转换信息、服务器的记录等，也可用下列命令生成：

/usr/samples/tcpip/addrs.awk

/etc/hosts>/etc/named.data

（5）编辑/etc/named.[domain_name]rev 文件，也可用下列命令生成：

/usr/samples/tcpip/addrs.awk

/etc/hosts>/etc/named.rev

（6）创建空文件 /etc/resolv.conf ，用下列命令生成：

touch /etc/resolv.conf

这个文件如果不存在，表示本机的域名服务由/etc/hosts 提供，如果存在且空，表示本机是域名服务器，如果存在且非空，表示本机是由域名服务器提供域名解析的客户机。

（7）启动 named 守护进程，为客户机提供域名解析服