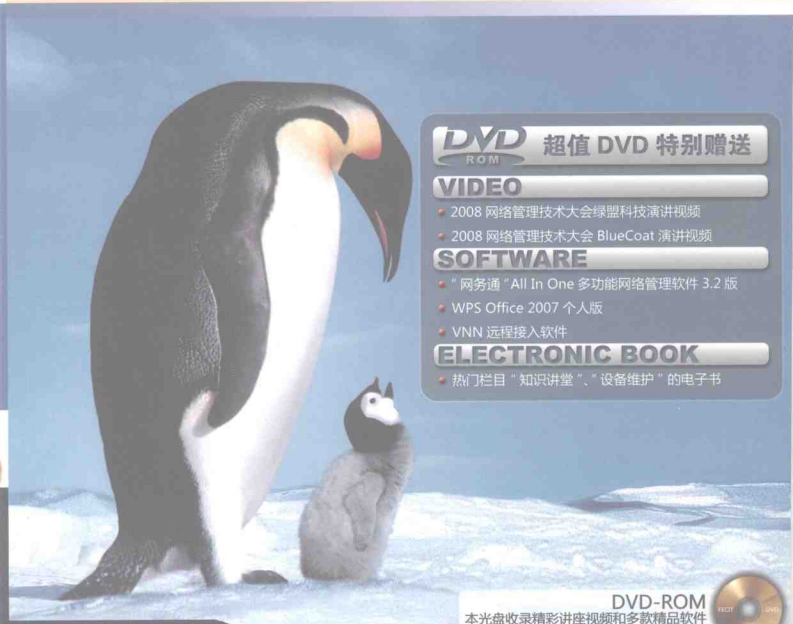
汇编与优选全年24期杂志内容　数百篇精华文章与专题大放送

网管员世界

NETADMIN WORLD MAGAZINE

2009 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



DVD ROM 超值 DVD 特别赠送

VIDEO

- 2008 网络管理技术大会绿盟科技演讲视频
- 2008 网络管理技术大会 BlueCoat 演讲视频

SOFTWARE

- “网务通”All In One 多功能网络管理软件 3.2 版
- WPS Office 2007 个人版
- VNN 远程接入软件

ELECTRONIC BOOK

- 热门栏目“知识讲堂”、“设备维护”的电子书

DVD-ROM
本光盘收录精彩讲座视频和多款精品软件

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

网管员世界

NETADMIN WORLD MAGAZINE

2009 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

电子工业出版社
Publishing House of Electronics Industry
北京·BEIJING

内容简介

《网管员世界》是国内一家专门面向网管员职业的刊物。本书是 2008 年《网管员世界》各期内容的汇集，内容权威、全面、时效性强，贴近应用实践，收藏价值高。本书按照栏目分类进行汇总，全书分为管理维护、桌面管理、开源系统、故障诊断、信息安全、升级改造 6 个部分，共精选收录了将近 400 篇实用、精彩的技术文章，是广大网管员不可多得的业务指导书。

随书光盘内容为《网管员世界》杂志“知识讲堂”和“设备维护”栏目的电子文档、2008 网络管理技术大会绿盟科技和 BlueCoat 演讲视频、WPS Office 2007 个人版、“网务通”All In One 多功能网络管理软件 3.2 版、VNN 远程接入软件等。

本书适合作为广大网络管理员入门和提高的技术参考用书。

图书在版编目（CIP）数据

网管员世界 2009 超值精华本 /《网管员世界》杂志社编.—北京：电子工业出版社，2009.5
ISBN 978-7-121-08447-8

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（2009）第 030112 号

责任编辑：王树伟　孙佳志
印　　刷：涿州市京南印刷厂
装　　订：涿州市桃园装订有限公司
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
开　　本：880×1230　1/16　印张：35.25　字数：1692 千字
印　　次：2009 年 5 月第 1 次印刷
印　　数：5 000 册　定价：65.00 元（含光盘 1 张）

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。
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。
服务热线：（010）88258888。

FOREWORD 前言

《网管员世界》是一本专门面向网络管理技术人员的专业杂志。长期以来，《网管员世界》杂志一直以帮助提高企业IT基础设施运营水平、提高企业网管人员的管理水平为目标和宗旨，为企业的网络技术人员提供了一个技术和经验交流的平台，成为在网络管理技术人员中颇具影响力的IT专业媒体。

为了更好地帮助广大网络技术人员提高网络管理技术水平，电子工业出版社与《网管员世界》杂志特别推出《〈网管员世界〉2009超值精华本》，内容来自于2008年全年《网管员世界》杂志“管理维护”、“桌面管理”、“开源系统”、“故障诊断”、“信息安全”、“升级改造”等栏目中精彩文章的汇总。对于这几百篇文章，本书进行了整合，全书共分为6章，包括管理维护、桌面管理、开源系统、故障诊断、信息安全、升级改造6个方面的内容：

- 管理维护：对于广大网络管理人员来说，网络管理和维护是他们的一项重要工作，网络管理维护章以大量精彩翔实的文章为广大网络管理人员管理和维护网络提供了鲜活的实例和参考，能够帮助网络管理技术人员完成从网络管理菜鸟到高手的转变。
- 桌面管理：针对网络管理人员需要了解的技术、技巧等方面进行全面介绍。
- 开源系统：针对开源软件和技术在网络管理工作中的应用进行了全面的介绍。
- 故障诊断：收集了《网管员世界》杂志社创刊以来在“故障诊断”栏目中的精华文章和优秀专题，既是网管员在日常工作中排障查错的工具手册，又是网管员提高网络管理水平的技术全书。
- 信息安全：专门针对网络安全而推出的网络安全专业手册，文章来自《网管员世界》杂志“信息安全”栏目，对网络管理人员增强网络安全意识、提高网络安全技能有着重要的指导作用。
- 升级改造：总结了实际升级改造项目中的宝贵经验，可以帮助网管员在项目中少走弯路、节省成本、变废为宝，达到事半功倍的效果。

随书光盘内容为《网管员世界》杂志“知识讲堂”和“设备维护”栏目的电子文档、2008网络管理技术大会绿盟科技和BlueCoat演讲视频、WPS Office 2007个人版、“网务通”All In One多功能网络管理软件3.2版、VNN远程接入软件等。

本书可作为网管员的日常工作手册，在工作中遇到问题时可以通过本书随时查阅，也可以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。

由于时间紧张，加之编者水平有限，书中不足之处欢迎读者批评指正，以利于我们今后改进。

《网管员世界》杂志社

飞思科技产品研发中心

联系方式

咨询电话：（010）88254160　88254161-67

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

光盘说明

一、超清晰独家视频

让您的安全变得更简单（Easy for your security）——绿盟科技

讲座主题：绿盟科技技术权威从性能、稳定性、实用性、及时性、易管理性等五个方面，系统介绍了UTM（统一威胁管理）产品作为最佳安全解决方案的实际功效与应用关键。

公司背景：绿盟科技是国内最早从事网络安全业务的企业之一，为客户提供及时、有效的本地化服务，建立并维护的全球最大的中文漏洞库已经成为业界广泛参考的标准。同时，在入侵防范技术、异常流量分析、检测与清洗、操作系统与应用安全、安全漏洞发掘技术、安全产品缺陷与检测、蠕虫及病毒原理与防范等领域，进行了深入的基础性研究。绿盟科技在国内率先开展专业安全服务业务，建立了完善的专业安全服务体系（NSPS），具备国内最高级安全服务资质，连续多年被评为“值得信赖的安全服务品牌”。

给广域网加速——BlueCoat

讲座主题：BlueCoat 公司资深专家针对提高广域网速度和安全性方面详尽阐述了自己的独到见解，彻底澄清过往在提高网速方面的认识误区。

公司背景：BlueCoat 公司专注于通过提供互联网安全代理专用设备来控制用户的 Web 访问。Blue Coat ProxySG 专用设备在不影响网络性能的前提下，集成了先进的代理功能和安全服务，如内容过滤、即时消息控制、Web 病毒扫描和 P2P 文件共享应用控制，已被许多世界上最具影响力的组织和机构所信任，用来确保 Web 环境的安全高效。

二、企业级精品软件

“网务通”All In One 多功能网络管理软件 3.2 版

北京无限精准软件技术有限公司推出的“网务通”All In One 多功能网络管理软件，不仅让企业用户把网络用起来，更重要的是把网络管起来，帮助企业用户真正做到事前预防、事中监控、事后追查，提高企业工作效率，从根本上降低企业网络运营成本和风险。

功能特点：不良网站及网页内容过滤；游戏、聊天、下载、炒股等应用程序管理；上网时间管理；带宽优化、流量分配；保护企业网络安全。

WPS Office 2007 个人版

北京金山软件有限公司出品的 WPS Office 2007 个人版对个人用户永久免费。

功能特点：28MB 超小体积，安全稳定——突破轻巧极限；看起来、用起来都一样——与 MS Office 双向深度兼容；独有金山词霸、PDF 格式直接输出等十余项功能；产品内含三大功能模块：WPS 文字、WPS 表格、WPS 演示。

VNN 远程接入软件

北京宇华亿欣科技有限公司出品的 VNN（虚拟本地局域网）是一款即插即用的 VPN 软件，用于远程接入。使用 VNN 进行连接的计算机之间的传输方式为点到点（P2P）传输，无任何服务器中转，数据传输过程使用 RC4 加密（可选 AES128 位或 AES256 位加密）压缩传输技术，以提高数据传输的速度。

功能特点：远程办公——共享文件，登录远程的计算机，访问公司的数据库；远程网管——数据备份，安装补丁包，远程查杀病毒和流氓软件，监控远程网络；远程监控——控制、查看远程的视频设备；网络加速——通过优化协议、最佳网络路由，解决跨运营商的速度瓶颈问题；文件加速网关——使大文件在互联网上传送的速度提高 3～10 倍。

三、PDF 电子杂志

光盘中收录 2008 年《网管员世界》热门栏目“知识讲堂”和“设备维护”的全部内容。

CONTENTS 目录

第 1 章　管理维护

第 2 章　桌面管理

CONTENTS

第 3 章　开源系统

第 4 章　故障诊断

CONTENTS

CONTENTS

第 6 章　升级改造

NetAdmin World 2009

第 1 章　管理维护

802.1x 认证管理宿舍网

安徽财经大学现代教育技术中心 吴秋兵

IEEE 802.1x 解决安全认证

最近，我校将校园网延伸到学生宿舍区。学生对网络的使用存在极高的热情，对网络技术也有很浓厚的兴趣。这种热情和兴趣一方面推动了校园网络迅速发展，另一方面也产生了各种极具破坏性的尝试。在学生宿舍区网络管理中，经常发生 IP 地址盗用、IP 地址冲突、使用代理、非法设备接入等情况。随着用户数的急剧增加，网络的安全性问题日益突出。

由于 PPPoE 和 Web/Portal 等传统认证方式对用户数据包烦琐的处理，造成了网络传输瓶颈，并且通过增加网络设备来解决传输瓶颈势必造成网络成本的提升，因此无法满足用户对网络安全性、高效性和低成本的要求。

IEEE 802.1x 协议通过对认证方式和认证体系结构进行优化，有效地解决了传统认证方式带来的问题，消除了网络瓶颈，减轻了网络封装开销，降低了建网成本，成为我校学生宿舍网络管理的首选。

802.1x 标准和 Radius 扩展原理

Radius 基本原理是，用户接入 NAS，NAS 向 Radius 服务器使用 Access-Request 数据包提交用户信息，包括用户名、密码等相关信息。其中，用户密码是经过 MD5 加密的，双方使用共享密钥，这个密钥不经过网络传播。Radius 服务器对用户名和密码的合法性进行检验，必要时可以提出一个 Challenge，要求进一步对用户认证，也可以对 NAS 进行类似的认证。如果合法，给 NAS 返回 Access-Accept 数据包，允许用户进行下一步工作；否则返回 Access-Reject 数据包，拒绝用户访问。

如果允许访问，NAS 向 Radius 服务器提出计费请求 Account-Request，Radius 服务器响应 Account-Accept，对用户开始计费，同时用户可以开始进行自己的相关操作。

Radius 具有以下特点：

客户端/服务器结构，采用共享密钥保证网络传输的安全性，具有良好的可扩展性，认证机制灵活。图 1 中详细说明了在 Radius 系统下用户的认证过程：

（1）由客户端向接入设备发送一个 EAPOL-Start 报文，开始 802.1x 认证接入请求。

（2）接入设备收到客户端的 EAPOL-Start 报文后，向客户端发送 EAP-Request/Identity 报文，要求客户端将用户名送上来。

（3）客户端向接入设备回应 EAP-Response/Identity 报文，其中包括用户名信息。

（4）接入设备将客户端送上来的“用户名”信息封装到 Radius Access-Request 报文中，发送给认证服务器。

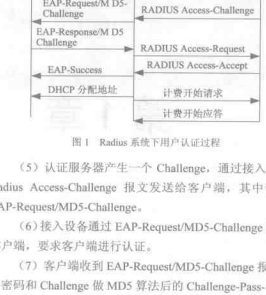


图 1 Radius 系统下用户认证过程

（5）认证服务器产生一个 Challenge，通过接入设备将 Radius Access-Challenge 报文发送给客户端，其中包含有 EAP-Request/MD5-Challenge。

（6）接入设备通过 EAP-Request/MD5-Challenge 发送给客户端，要求客户端进行认证。

（7）客户端收到 EAP-Request/MD5-Challenge 报文后，将密码和 Challenge 做 MD5 算法后的 Challenge-Pass- Word，在 EAP-Response/MD5-Challenge 回应给接入设备。

（8）接入设备将 Challenge、Chanllenge Password 和用户名一起送到 Radius 服务器，进行认证。

（9）Radius 服务器根据用户信息，做 MD5 算法，判断用户是否合法，然后回应认证成功/失败报文到接入设备。若认证成功，则携带协商参数及用户的相关业务属性给用户授权；若认证失败，则流程到此结束。

（10）如果认证通过后，用户通过标准的 DHCP 获取规划的 IP 地址。

（11）如果认证通过后，接入设备发起计费开始请求给 Radius 用户认证服务器。

（12）Radius 服务器回应计费开始，请求开始报文，用户上线完毕。

系统网络体系结构设计

我校原来用两台 Cisco 7609 作为东西校区核心，并采用双万兆互连，由东校的 7609 连至联想网御的防火墙，通过教育网、电信和网通上 Internet。我校原有亿邮的计

费网关，用户采用静态分配 IP 地址，但面对学生区管理中频繁出现的 IP 地址盗用、IP 地址冲突、使用代理、非法设备接入等问题，该计费方案有些无能为力。因此，我校对学生区采用了安全、高效、基于 802.1x 协议的 Sam 认证计费系统，并通过 DHCP 对学生区的 IP 地址进行动态分配。

为此，我校新加了两台 Cisco 6509，分别作为东西校区学生宿舍的核心汇聚，用锐捷的 5750 作为每栋学生宿舍楼的楼宇汇聚，用锐捷的 2126 作为接入设备。东西校区的 6509 分别通过千兆光纤与 7609 和各楼宇汇聚交换机相连。而各楼宇汇聚通过千兆光纤跟各楼层的接入交换机相连，并在东校区核心 Cisco 7609 连接了一台服务器和一台 SamDHCP 服务器，作为学生区的认证计费和动态 IP 地址分配（如图 2 所示）。

图 2　网络拓扑图

架设校园宿舍网

硬件平台

鉴于 Cisco 6509 路由的健壮性较好，物理设计充分考虑冗余可靠性，并且在用户面前很透明，有 NetFlow 和大量 MIB 及监控手段，因此我校核心汇聚新加了两台 Cisco 6509。楼宇交换机选用锐捷 5750，它是锐捷网络推出的融合了高性能、高安全、多智能、易用性的新一代万兆机架式多层交换机。

楼层接入交换机选用锐捷 2126。RG-S2126S 是一款全线速可堆叠千兆智能交换机，提供智能的流分类和完善的服务质量（QoS）及组播管理特性，并可以实施灵活多样的 ACL 访问控制。可通过 SNMP、Telnet、Web 和 Console 口等多种方式提供丰富的管理。并且 2126 具有极高的性价比。我校 28 栋学生宿舍需要大量的接入设备，考虑多方因素，RG2126 是我校接入层设备的首选。

Sam 认证计费服务器和 DHCP 服务器选用两台曙光 A620r-F。曙光天阔 A620r-F 型服务器系统，配以最新推出的 nVidia nMCP55 Professional 和 NEC uPD720400 芯片组，集成双通道千兆网卡控制器、SATA RAID 控制器、SCSI 控制器、IDE 控制器，ATI ES1000 图形控制器。nVidia nMCP55 Professional 芯片组支持两个 PCI-E X8 接口（x8 速率）的扩展，提供 4Gbps 的高速带宽，为高端的扩展提供了便利。nVidia nMCP55 Professional 芯片组支持 SATA RAID 功能，提供了人性化的 RAID 管理界面，集成 USB 2.0 高速接口。AMD64 位皓龙 2000 系列处理器集成 DDRII 内存控制器，最高可提供 21.33GBps 的内存带宽。在存储方面支持 6 个热插拔 SCSI 硬盘，最大 1.8TB 内部存储空间。该服务器的配置完全满足我校学生的认证计费要求，并为以后的升级留有余地。

数据库平台

在 Windows 2000 Server 系统平台的基础上，架设 SQL Server 2000 数据库服务器。数据库中建立了大量数据表用来记录、保存用户的详细信息，以及用户使用和费用情况。数据库中有接入控制表、账务流水表、上网记录及费用、账号模块表、接入控制属性表、账号相关联服务表、用户卡批次信息表、充值卡信息表、充值卡表、充值卡收入登账表、充值卡批次信息表、系统配置表、黑名单、管理员表、接入交换机表、用户在线表、缴费提示条件表、用户缴费记录表、操作权限列表、计费册列表、注册用户表、用户表、服务属性列表。

下面就以表 T_ ACCTRECORD（上网记录及费用表）举例说明，该表详细记录了用户上网的详细信息（如表 1 所示）。

表 1　上网记录及费用表

名　称	含　义
ACCTRECORDID	计费记录 ID，系统自动生成
USERID	用户登录名
NASIP	NAS 的地址
NASPORT	NAS 接入端口
SERVICE	用户访问服务
USERIP	用户分配 IP
USERMAC	用户主叫 MAC
ACCTSTART	计费开始时间
ACCTSTOP	计费结束时间
ACCTTIME	时长
INPUTBYTES	流入 M 字节
OUTPUTBYTES	流出 M 字节
FEE	无折扣费用
DISCOUNT	折扣
REALFEE	折扣后费用
NASNAME	NAS 名称
NASLOCATION	NAS 本地位置
NASTYPE	NAS 类型

（续表）

名　称	含　义
DNS	DNS
NETMASK	子网掩码
GATEWAY	网关
TERMINATECAUSE	用户记账结束原因

系统功能实现

我校原有网络基础是将东西校区的 Cisco 7609 采用 Trunk 互连，并在东校区的 Cisco 7609 采用三层 VLAV 交换，校园网的所有用户流量都流向东校区的 Cisco 7609 进行路由选择。由于学生大多都玩局域网游戏、局域网共享及基于 P2P 的下载等，这些将会产生巨大的网络流量，从而对东校区 Cisco 7609 是一个很大的压力。因而，我校又重新规划了网络体系结构，在核心层、楼宇汇聚层启用 OSPF 路由，将局域网内部的流量控制在汇聚层，从而减轻学生上网所产生的流量对校园网出口核心交换机的压力。而对于计费认证，则主要在接入层交换机 RG2126 上进行。

RG2126 配置：

```
hostname 1#SSL-2F-1/S2126S
vlan 1
（创建 VLAV1、VLAN 501）
vlan 501
radius-server host 10.10.200.100
（设置 Radius Server IP 地址）
aaa authentication dot1x
（启用 802.1x 认证功能）
aaa accounting server 10.10.200.100
（设置记账服务器的 IP 地址）
aaa accounting
（记账）
aaa accounting update
（配置记账更新功能）
enable secret level 1 5 +TYC,tZ[Q-ZD+S(\X2YG1X)s-S5UH.Y*T
（配置交换机的 Telnet 密码）
enable secret level 15 5 +TY1u_：CQ-Z8U0<DX2Yŋ9=G-S5U7R：>H
（配置交换机的特权密码）
port-security arp-check
（开启交换机 ARP 报文检查功能）
service dhcp
（交换机开启 DHCPRELAY 功能）
ip helper-address 10.10.200.200
（设置 DHCP 服务器的 IP 地址）
interface fastEthernet 0/1
switchport access vlan 501
（将交换机的端口划到 VLAN 501 中）
dot1x port-control auto
（将此端口设置成受控端口）
interface gigabitEthernet 1/1
switchport mode trunk
（将交换机端口配置成 Trunk 模式）
interface vlan 501
no shutdown
ip address 10.10.101.1 255.255.255.0
（配置交换机的管理地址）
dot1x client-probe enable
（打开客户端在线探测功能）
dot1x probe-timer alive 250
（配置交换机的 Alive Interval，单位为秒）
aaa authorization ip-auth-mode dhcp-server
（配置 IP 授权模式为 DHCP-Server 模式）
radius-server key star
（设置 Radius Server 认证密码）
ip default-gateway 10.10.101.254
snmp-server community public ro
（配置交换机 SNMP 管理）
end
```

经验总结

通过一段时间的实际运行，可以看到：

（1）由于采用了 DHCP 动态分配 IP 地址，没有出现一例学生抱怨 IP 地址冲突、IP 地址被盗用的情况。同时，Sam 认证计费的实施，也杜绝了部分学生使用代理和接入非法设备，如交换机路由器的情况。

（2）通过一段时间观察发现，即使在晚上学生上网高峰段，也没有出现一例因认证服务器繁忙而无法认证，或由于网络繁忙而通信失败的情况。

（3）近期，网络中出现的 ARP 病毒干扰，让网络管理人员大为头疼。但学生公寓网络至今没有一例因为 ARP 病毒而导致学生无法上网的情况发生，这是因为我们在学校的学生公寓的接入层交换机（锐捷 2126）启用了 ARP 报文检查功能。

虽然利用 IEEE 802.1x 认证技术能够比较好地解决现阶段校园网所面临的一系列安全问题，增强了网络的可控性和安全性，但正如大家所共知的，任何一项技术都不可能解决目前所面临的所有问题。因此，仅仅依靠 802.1x 这项技术来解决用户身份认证和应用终端所面临的所有安全问题是不现实的。只有将多项技术和相关的管理规定有机结合起来，采用全局化、智能化的安全体系来替代陈旧、孤立的安防措施，才能构建一个真正安全、可靠的网络环境。

高质量传输大流量数据

福建广播电视大学　黄晶慧
福建信息职业技术学院 张冬

在通信和计算机技术日益成熟的今天，诸如视频会议、实时音频和视频的多点组播等应用程序，对数据吞吐量和网络延时等因素的要求大大高于传统的如电子邮件和远程文件访问等异步应用程序。应用 QoS 技术，可以实现高质量传输大流量、多类型的数据，实现海量数据实时、高效传输。

笔者单位局域网的主干速度为 1000Mbps/100Mbps 到桌面，基本上实现各种多媒体应用，诸如视频新闻、VOD 点播、网络会议、网络教育等，但局限于非对称式、小数据量的应用。

比如，在视频点播这样的多媒体系统中，上行链路和下行链路传输的信息量不同，从用户到信息源的信息量小，从信息源到用户的信息量大。因此这是一种不对称的交互方式。

通常利用高速缓存技术，首先将服务器端的数据下载到用户端，然后由客户端软件播放存在本地系统内的数据。这种做法有效地节约了带宽，使服务器可以同时响应大量的请求，也节约了服务器系统资源。但是，一旦传输海量数据时，目前的网络配置存在一定的问题。主要的问题集中在核心设备——路由器 PassPort 8600 承担着实验室和外网的连接重任，处理局域网内部之间的数据传输和局域网与外部之间数据传输，因而在同一时刻，如果产生较大的并发数据量，目前的设置很难确保端到端的大数据量快速、准确地传输。

为此，我们利用现有设备 PassPort 8600 及 QoS 技术，实现了高质量传输大流量、多类型的数据，满足海量数据实时、高效传输的要求。

Passport 8600 实施 QoS

Passport 8600 执行 QoS 是基于区分服务体系的。区分服务具有良好的可扩展性，它可以根据应用或业务类型排出不同的优先级别。业务区分结构使用 IPv4 包头中的业务类型（ToS）字段，并将 8 位 ToS 字段重新命名。作为 DS 字段，其中 6 位可供目前使用，剩余 2 位以备将来使用。通过该字段的标记，下行结点可以获取足够的服务质量信息，以对到达该端口的数据包做出相应的“处理”，将它们正确地转发给下一跳的路由器。

需要注意的是，ToS 字段和 DS 字段的定义是不同的。边缘路由器可以将 ToS 字段映射到 DS 字段，而且区分服务可以识别网络流量大小。这种体系能够优化微流量或者累积流量，并且提供可升级的 IP QoS。

在区分服务网络中，根据标记，标记包被放置在队列里。举例来说，如果视频流被标记为最高优先级，它会被放在高优先级队列里，当标记包通过该类网络时，视频流将优先于其他包通过。

Passport 8600 已定义了默认的 QoS 参数，一般能够满足千兆网的应用要求。如果网络中有海量数据的应用，可以通过修改 Passport 8600 的默认值，同时利用 access port 和 core port 优化网络数据流量对网络带宽的占有率，使其具有更好的 QoS 性能。

Passport 8600 的 QoS 功能

1. 端口类型

Passport 8600 通过存取端口和核心端口处理数据流量。

1）存取端口（access port）

在区分网络边缘的端口称为存取端口。数据包的 IP 头包含着 DS 域（也称为 DSCP），用以识别服务等级。另外，标记为 IEEE 802.1q 的数据包也包含用以识别服务等级的 IEEE 802.1p 位。因此，数据包的 DSCP 或者 IEEE 802.1p 位可以被置位，也可以保持不变。在 DS 的存取端口，数据包将被分配基于区分标准的 QoS 性能。

2）核心端口（Core Port）

在网络中的端口被称为核心端口。当数据包通过存取端口时，数据包被打上标记，然后，这些数据包通过网络的时候，由核心端口处理这些被存取端口做过标记的数据包，将包放到适当的 QoS 队列里。

2. 基于各种机制的 QoS

Passport 8600 可以基于不同的机制设置 QoS 级别。包括：

基于 VLAN——可以给某个 VLAN 中的数据流量定义 QoS；

基于端口——即根据存取端口或者核心端口定义；

基于 MAC——针对某个 MAC 地址定义其 QoS。

3. 队列与 QoS 级别

Passport 8600 有 8 个队列，对应着 8 种不同的 QoS 服务级别。第 7 队为网络控制所保留。第 6 队具有最高优先级，即便在第 0 队被允许传输的时候，第 6 队中的数据包仍能传输或者路由。举例来说，音频和视频流量需要放在第 6 队里，因为它们必须无延时地传输；而 Web 数据则仅需放在第 1 队里，因为这种数据流允许有一定的延时。

QoS 应用实例

基于端口的 QoS 设置

假设来自子网一的大多数数据包是关于多媒体数据包的，我们使用基于端口的 QoS 配置方案。

网络结构图如图 1 所示。

图 1　网络结构图

基于端口的 QoS 配置非常简单，只需在 Port 菜单中启用区分服务，同时指明区分服务的类型和 QoS 级别即可。详细设置步骤如下：

（1）选择端口。

（2）从 Device Manager 菜单上选择【Edit】→【Port】命令。

（3）在 Interface Windows 中的 QoS 部分，启用 DiffServEnable 为 True。

（4）指定 DiffServType 为 access。

（5）指定 QoS Level 为 Level 6，即最高优先级。

默认设置如图 2 所示。

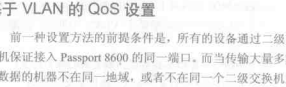


图 2　Passport 8600 默认设置

这样，无论是网络内部的数据传输，还是网络外部的数据传输，来自于同一的数据包都将以最高优先级通过，保证了多媒体数据的传输效率。

基于 VLAN 的 QoS 设置

前一种设置方法的前提条件是，所有的设备通过二级交换机保证接入 Passport 8600 的同一端口。而当传输大量多媒体数据的机器不在同一地域，或者不在同一个二级交换机上时，可以采用基于 VLAN 的方式保证某一个虚拟子网内的数据包在指定的 QoS 级别上。

比如，不仅子网一需要使用实时交互系统，包括子网二和子网三的部分机器也需要使用实时交互系统。因此，首先将这些设备划分在同一个 VLAN 中，然后再进行 QoS 级别的设置（如图 3 所示）。配置过程如下：

（1）选择指定的 VLAN。

（2）从 Device Manager 菜单中选择【VLAN】→【VLAN】。

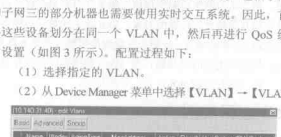


图 3　基于 VLAN 的 QoS 设置

其中 QosLevel 便是当前 VLAN 的 QoS 级别，将其修改为我们所需要设定的 QoS 级别即可，这样便实现了不同地域、同种类型应用的机器享有同样的 QoS 级别。

以上两例仅是为了进一步说明 QoS 的实现方式，在具体应用的时候，还要权衡路由器的承载能力和网络性能，以及操作系统接受和发送数据的极限速度等多方面因素，以便使千兆网更好地为不同应用提供服务。

解析 QoS

QoS 定义

QoS 是指 IP 的服务质量，也是指 IP 数据流通过网络时的性能。它的目的就是向用户提供端到端的服务质量保证。QoS 能够对数据包进行合理的排队，对含有内容标识的数据包进行优化，并对其中特定的数据包赋以较高的优先级，从而加速传输的进程，并实现实时交互。

QoS 在可预测、可测量性方面比传统 IP 有了很大的提高，基本解决了多媒体类应用或者大数据优先传输的需求，并且可提高带宽的使用率。

服务质量不仅仅是网络的事情，而是应用程序、用户终端、网络、服务器各部分的综合效应。例如，一个用于远程视频播放的端到端活动，从媒体服务器获得视频，在源地进行压缩，在目的地进行解压缩，并根据播放窗口的大小对视频按比例进行调整，最后在视频窗口播放。在端到端路径上，任何一个环节不符合 QoS 的要求，都会影响播放的完整性。

对于一个带宽与交换速率已经固定的网络，有两种方法实现 QoS 支持：第一种方法是沿着特定应用的数据流所经过的路径保留端到端的资源；第二种方法是不必为具体的流在网络中保留特定的资源，但是要对分组做标记，并在结点中提供特殊处理。比如“区分服务（DiffServ，Differentiated Services）”，是先把分组的 DS 域标记以具体的权值，然后将结点做适当的配置，使得被标记的分组在传送它们的结点中能做预期的处理。

IP QoS 结构分析

IP QoS 主要是对第二层的以太网帧头加入了优先级字段，以区分不同的优先级。

这种解决方案是根据对 IEEE 802.1p/q 协议字段的处理来区分不同优先级业务的。IEEE 802.1p/q 同属于一个子集，它在传统的以太网帧头中加入了 4 个字节，其中 802.1p 占 3 位。802.1p 延伸了 802.1d 的协议，利用 3 位优先级位可以最多提供 8 个优先等级。而 802.1q 利用 VI（VLAN Identifier，虚拟网标识）位识别传送的帧究竟属于哪一个虚网。

VI 位共有 12 位，最大可以支持的虚网个数不会超过 4096 个。802.1p/q 的具体定义可以参见图 4。

图 4　802.1p/q 的定义

IP QoS 实现机制

1. 队列管理机制（Queue Management Mechanism）

在网络发生拥塞时，路由器必须丢弃一些分组，这个问题的解决首先必须实施有效的队列管理机制（或缓冲区管理策略）。

目前，已经出现的队列管理机制有：PPD（Partial Packet Discard）、EPD（Early Packet Discard）、RED（Random Early Discard）、FRED（Flow RED）、RIO（RED with In and Out）、BLUE 等算法。比较起来，RED 算法具有较低的排队时延、较高的分组通过度和较好的公平性。

2. 队列调度机制（Queueing Scheduling Mechanism）

不论在 IntServ 还是在 DiffServ 里，都涉及到队列调度问题。简言之，队列调度的功能就是路由器如何从多个（或一个）队列中选择下一个待转发的分组，这与队列管理机制有着本质的区别。根据不同的服务规则，队列调度算法可以分为以下几种：先到先服务、循环调度、处理机共享、优先级服务、随机服务等。

3. 基于约束的路由（Constrained -Based Routing）

基于约束的路由源自 QoS Routing，只是对 QoS 的限制参数进行了一定的扩充。CBR 的有效实现需要各个路由器之间的相互配合，比如相互通知各自所知道的网络的一些状态信息（如链路的剩余带宽）。

4. 业务量工程（Traffic Engineering）

其主要目的在于尽量避免网络拥塞的发生，以保证 QoS。

让静态路由使用多网关

湖北　邓海英

我校有如下网络环境：全校 450 个结点划分成 5 个子网，各子网的网络号为 192.168.1.0～192.168.5.0，网关均为 192.168.1.1，各个子网通过华为 S2026B 二层交换机接入烽火 R2600 出口路由器，出口通过光纤以 100Mbps 的带宽接入 Internet。

现全县组建电子政务网，要求全县各个单位处室以上领导干部的计算机必须能直接访问县电子政务网服务器 192.168.20.6/24，县电子政务网办公室给我校划分的子网号为 10.1.26.0，掩码为 255.255.255.192，网关为 10.1.26.1，电子政务网不能访问 Internet。

由于县电子政务网的服务器在电信局托管，所以电信局给我校又开通一条 10Mbps 的光纤连接电子政务网。电信局的建议是，给我校需要直接访问电子政务网的计算机安装两张网卡，分别设置两个网络的网关，来达到同时访问电子政务网和 Internet 的目的。

手动添加静态路由

以上的网络需求实际就是要解决两个子网 192.168.0.0 及 10.1.26.0 访问不同目标的问题。由于我校办公大楼在建设时就已将连接各个办公室到网络中心的网线埋入墙内，如果为每个需要直接访问县电子政务网的计算机再安装一张网卡，就需要再单独铺设一根网线，无论从铺设的难度及办公大楼的布局来说，都不是一个很好的办法。

如果沿用原来校园网的网线，在需要连接电子政务网的计算机上设置两个网关，就需要人为地切换网关，这对于计算机应用水平不高的人来说，也是一个不小的麻烦。因此，我们决定不采纳电信局的建议，而采用手动添加静态路由的方式来实现两个网关的无缝切换。

（1）将连接电子政务网的光纤接入原有的 S2026B 交换机。

（2）在需要接入电子政务网的计算机上添加网络号为 10.1.26.0 的 IP 地址，例如：10.1.26.2，掩码为 255.255.255.192。

具体操作步骤是：选择【Internet 协议（TCP/IP）】→【属性】→【高级】→【IP 设置】→【添加】命令，添加好 IP 地址后，要特别注意的是，不能添加 10.1.26.1 这个网关，具体原因见后文的进一步分析。

（3）进入 DOS 命令方式，在提示符后输入：ip route add 192.168.20.0 mask 255.255.255.0 10.1.26.1，从而手动添加一条静态路由。

（4）为了能使每次开机时都自动执行这个命令，可以将其写成一个批处理文件，因为建立批处理文件的方法比较

简单，此处略去不提。

经过以上 4 个步骤的操作后，在命令行方式中可以用 route print 命令看到本地路由表中新增了一条到 192.168.20.0 网络的静态路由，此时本地计算机既可以访问 Internet，也可以访问电子政务网，用户在使用过程中完全感觉不到网关切换的过程。

方案原理

通过以上的介绍可以看出，本方法中有两个亮点：

一是同一个交换机可以连接不同的网络，在平常使用过程中，普遍的固定思维是一个交换机只能接同一个网络。其实我们从交换机的原理就可以知道，这种思维方式是不正确的，因为交换机处于 OSI 参考模型的数据链路层，属于网桥，起着桥接的作用，因此交换机可以接入多个不同的网络。上述方案中正是利用了这一点，从而免去了不必要的硬件投入。

二是不设 10.1.26.0 这个网络的网关，而采用静态路由的方式，免去了额外的组网开销。

那么为什么不能设置两个网关呢？这就要从网关的作用说起，在设置网关时，本地计算机的路由表中添加了一条默认路由：

0.0.0.0 0.0.0.0　网关 IP 地址本地接口跃点数。

其含义是，如果在路由表中无法找到到达目标网络的路径时，就把数据包发送到这条默认路由中的网关，如果删除了本机对应的网关，则这条默认路由也将在路由表中删除。如果本机设置了两个 IP 地址，并且分别对应了两个网关，则会在本机的路由表中添加了两条默认路由，它们分别是：

0.0.0.0　0.0.0.0　192.168.1.1　192.168.1.88　1

0.0.0.0　0.0.0.0　10.1.26.1　192.168.1.88　1

此时，本机在发送数据时就不知道该如何处理了，而手动添加静态路由与直接设置网关产生路由路径不同，数据在发送过程中会根据本地路由表中指明的路径传输。

通过以上的方法，完全可以实现单张网卡对不同网络的无缝访问。

配置 DNS 转发器

山东沃华医药科技股份有限公司　张鲁峰

转发器是网络上的域名系统（DNS）服务器，通过让网络中的其他 DNS 服务器将它们在本地无法解析的查询转发给网络上的 DNS 服务器，该 DNS 服务器即被指定为转发器。

使用转发器可以管理网络外的名称解析（例如 Internet 上的名称），并提高网络中的计算机名称解析效率。

将 DNS 服务器指定为转发器时，转发器将负责处理外部通信，从而可以将 DNS 服务器有限地暴露给 Internet。转发器将建立外部 DNS 信息的巨大缓存，因为网络中的所有外部 DNS 查询都是通过它解析的。在很短的时间内，转发器将使用该缓存数据解析大部分外部 DNS 查询，从而减少网络 Internet 通信与 DNS 客户端的响应时间。

配置标准转发器

单击【开始】按钮，找到管理工具，然后单击 DNS。

鼠标右键单击 ServerName，其中 ServerName 是服务器的名称，然后单击转发器选项卡。选择“接口”，在以下地址侦听选项中选“所有的 IP 地址”（如图 1 所示）。

单击 DNS 域列表中的一个 DNS 域，或者单击【新建】按钮，在 DNS 域框中输入希望转发查询的 DNS 域名称，然后单击【确定】按钮。这里使用系统默认的选项“所有其他 DNS 域”。在所选域的转发器 IP 地址框中，键入我们希望转发到的第一个 DNS 服务器的 IP 地址，然后单击【添加】按钮。重复上述步骤，可以添加希望转发到的 DNS 服务器（如图 2 所示）。

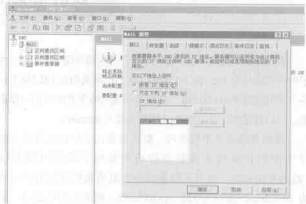


图 1　选择所有的 IP 地址

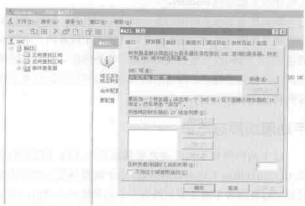


图 2　添加 DNS 服务器