

郑重声明

本作品的图片均来源于互联网，仅供PDF文档制作学习，交流之用。版权归原出版社所有。任何组织或个人不得公开传播或用于任何商业盈利用途，因而产生的一切后果由该组织或个人承担。本站及其制作者均不承担任何法律责任。请自觉在下载后的24小时内删除。如果你喜欢该读物，请你支持及购买正版读物。

AprilVolcano.Org

Volcano Studio

网管员世界



“2004十大热门网络产品”

“2004十大热门网络事件”

专题报道

故障诊断

安全检查从日志做起

安全空间

横扫毒界之 2004

知识讲堂

隔而不断的物理隔离技术
网络寻址与互连技术

手把手

企业无线局域网组建入门

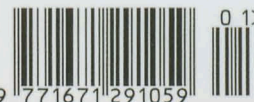
经验技巧

解决共享难题

网管工具

谁说没有“后悔药”

ISSN 1671-2919



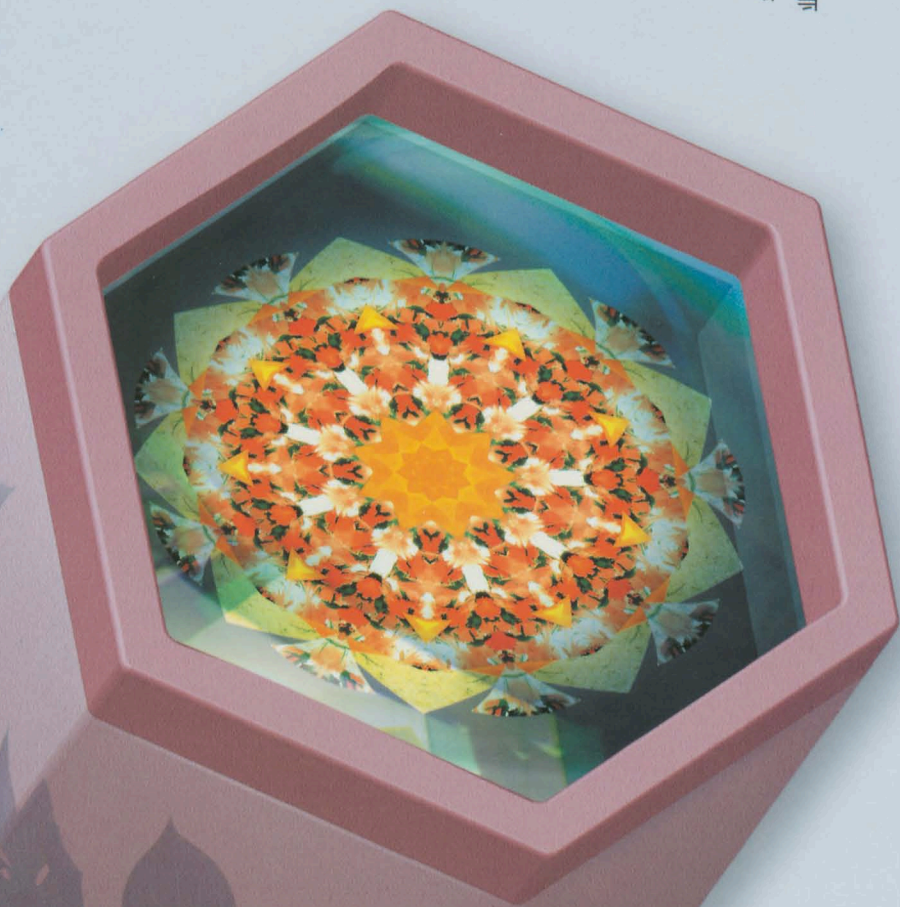
9 771671 291059

邮发代号: 2-99 零售价: 12 元

<http://www.netadmin.com.cn>

体验变化之美

华为 3Com 高品质 IP 核心网



领略万花筒的世界 动态网络让业务更精彩

网络之美，正如万花筒的魅力，尽在变化之中。

面对瞬息万变、精彩纷呈的网络业务，您将如何应对，尽情体验？

华为 3Com 高品质 IP 核心网，智能化网络，以高品质业务为核心，动态应变网络需求，业务动态感知，带宽动态调整，动态安全防护和保护，让您的网络不断优化，从容扩展。

拥有超强的动态应变能力，尽情体验网络之美。

华为 3Com，你身边的好网络。

华为 3Com 技术有限公司 www.huawei-3com.com 免费咨询热线: 800-810-0504 认证培训热线: 010-82774788
杭州基地 杭州市高新技术开发区之江科技工业园六和路东 邮编: 310053 电话: 0571-86760000 传真: 0571-86760001 北京分部 北京市宣武门外大街 6 号庄胜广场中央办公楼南翼 16 层 邮编: 100052 电话: 010-63108666 传真: 010-63108777

华为 3Com

你身边的好网络

登陆金山

金山毒霸企业版
金山毒霸网

获取更多信息
地址: 北京市海淀区
以上图片仅供参考

金山毒霸 DAV Corporate Edition 网络版 2.0

企业反病毒必备之选
dbnet.kingsoft.com



几万台电脑轻松掌控 全网系统漏洞集中修补 病毒 木马 垃圾邮件一网打尽

金山毒霸网络版

融病毒查杀、黑客防范、硬盘救护多种安全方案于一体
采用“远程控制、集中管理、多级管理、差异配置”的管理模式

几万台机器轻松掌控

适用于多种网络平台

为企业网络提供完整的信息安全解决方案

咨询电话: 010-82334488-5020

惊喜1+1 新年送大礼



活动说明

从12月10日起, 到2005年1月31日止, 购买金山毒霸网络版2.0的用户(以发放授权日期为准), 均可获得数码礼品一份!

购买50客户端以下: 朗科优盘一个

购买50-199客户端: 三星mp3播放器一个

购买200客户端以上: 惠普PDA一台

登陆金山毒霸企业信息安全网dbnet.kingsoft.com, 免费体验金山毒霸网络版2.0!

金山毒霸企业级信息安全产品线包括:

金山毒霸网络版2.0	金山毒霸for Exchange Server	金山毒霸for Lotus Domino	金山毒霸天网防火墙
------------	-------------------------	----------------------	-----------

获取更多金山产品信息请登陆: www.kinsoft.com 金山在线, 深度互联

地址: 北京市海淀区北四环中路238号柏彦大厦20层(100083) 总机: 010-82334488

传真: 010-82325655

经销商订货热线: 010-82325225/82325755

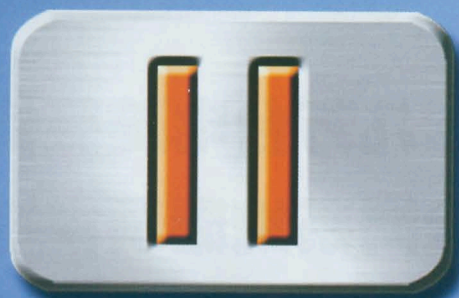
购买咨询热线: 010-82325757

KINGSOFT

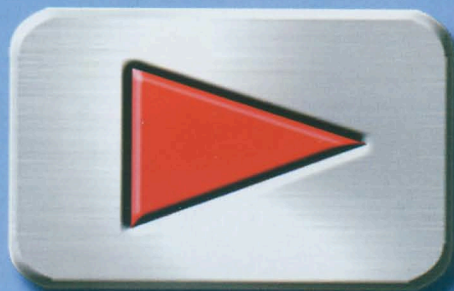
以上图片仅供参考, 金山公司不负责印刷及影像上出现的错误。

公司保留在不事先通知的情况下更改产品规格配置及价格的权利。

金山软件有限公司



服务器暂时宕机



损失立刻启动

对于服务器关键应用来说，每一次宕机都意味着难以估量的损失。所以，您总是梦想有一台永不宕机的服务器。浪潮英信NF280是您的理想选择，它基于全新的英特尔®至强™处理器，在2U空间内采用先进的内存容错技术、关键部件全冗余设计和独立风道结构，给您的系统运行带来无与伦比的可靠性，彻底满足关键应用对高可靠的需求，令您的企业运营永不间断。

稳定可靠 超越期待

处理器：采用英特尔®至强™处理器，配备先进的64位英特尔®内存扩展技术（英特尔®M64T）。

内存：不仅支持ECC内存技术，而且支持目前最高级别的内存容错技术；内存热备与内存镜像，即使内存发生错误也能保证系统稳定运行。

全冗余：硬盘、风扇、电源等关键部件均支持热插拔冗余技术，不关机就可以进行部件的更换与维护。

新品上市



浪潮英信NF280
采用英特尔®至强™处理器

灵活扩展 按需配置：

提供6个内存插槽，内存容量可扩至24GB；可选SCSI或SATA硬盘满足不同应用的数据存储需求，最大可支持8个热插拔硬盘；

预留6个PCI扩展槽支持主流的PCI-X设备与新一代的PCI-E串行扩展接口，同时支持标准尺寸和非标准尺寸的扩展卡。

尖端设计 易于管理：

机箱从中间位置向前后打开的设计方式以及内部模块化易拆卸设计，使设备维护或扩展操作更方便；

系统快速定位指示灯让您在众多的设备中快速找到故障服务器系统，将系统维护与管理工作的繁杂为简。

浪潮服务器

超越期待

浪潮集团服务器事业部 地址：北京市海淀区上地信息路2号创业园C栋1层 邮编：100085
电话：(010)62988886 传真：(010)82895417 服务热线：800-860-0011 0531-8546554

山东办事处 (0531)5106329	四川办事处 (028)85242628	云南办事处 (0871)3159272	北京办事处 (010)96096985	天津办事处 (022)27829119
山西办事处 (0351)7923769	河北办事处 (0311)6219504	广东办事处 (020)38182808	福建办事处 (0591)87813980	广西办事处 (0771)5870311
湖北办事处 (027)87886547	河南办事处 (0371)7444002	湖南办事处 (0731)4468300	江西办事处 (0791)6203907	江苏办事处 (025)83322799
安徽办事处 (0551)2832388	上海办事处 (021)52402666	浙江办事处 (0571)88271975	辽宁办事处 (024)22812881	黑龙江办事处 (0451)53641761
陕西办事处 (029)85220308	新疆办事处 (0991)5857887	甘肃办事处 (0931)4810242	吉林办事处 (0431)5661629	贵州办事处 (0851)8665179
深圳办事处 (0755)26632352	重庆办事处 (023)89089766	增值分销商：神州数码 (010)62893638		

欲知更多产品信息，欢迎发送邮件 bjvip@langchao.com 或登陆浪潮网站：http://www.langchao.com/Products/Channel_Server/

Intel 英特尔, Intel Inside, Intel Inside 标志和 Intel Xeon 英特尔至强是英特尔公司或其美国和其他国家分支机构的商标或注册商标。以上内容仅供参考，可能存在印刷或校对错误，同时浪潮集团服务器事业部保留随时对以上信息进行调整的权利。



英特尔®至强™处理器

SafeNet iGate 有奖调查

Want secure VPN connections here?

Here?

Here?

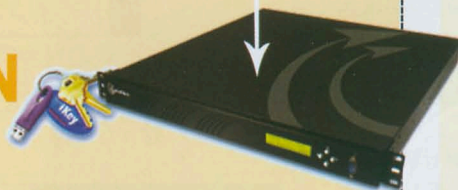
Here?

Here?

Start here!

iGate SSL VPN

安全远程接入方案



正在寻找高安全性的SSL VPN解决方案吗？
从SafeNet SafeEnterprise SSL iGate 开始吧！无论在世界的哪个角落，你都可以通过互联网远程访问内部的应用程序和重要数据！给你的员工更高的生产效率，让你的VPN更安全！这就是iGate！

- 适用广泛，支持 B/S和C/S应用以及手持设备
- 快速部署，易于使用，无需安装客户端程序
- 安全客户端检测，具备超强访问权限控制管理能力
- 集成双因素iKey身份认证令牌或智能卡
- 不间断的远程访问业务能力，不受访问环境网络配置影响

关于更详细内容，请致电赛孚耐公司010-88519191
或发邮件至security@cn.safenet-inc.com垂询详情！



- 1、 您公司是否有远程访问需求？
 - ☐ 有需求，有很多分支机构和移动办公人员需要远程接入公司总部。
 - ☐ 有需求，需要在分公司和总公司之间建立安全的远程连接。
 - ☐ 有需求，需要专线连接。
 - ☐ 一般不需要用到VPN。
 - ☐ 不清楚。
- 2、 请根据以下VPN性能的重要程度进行排序（1——最高，6——最低）
 - 安全性 _____
 - 可移动能力 _____
 - 认证强度 _____
 - 安装使用的难易程度 _____
 - 应用支持能力 _____
 - 接入速度 _____
- 3、 您认为以下哪些应用有远程访问需求？
 - ☐ CRM/ERP/SCM ☐ Email系统
 - ☐ OA系统 ☐ 文件共享 ☐ 其他 _____
- 4、 如果要购买VPN产品，您认为以下哪方面是您购买VPN首先要考虑的因素？
 - ☐ 性能 ☐ 知名度 ☐ 价格
 - ☐ 服务能力 ☐ 其他 _____
- 5、 如果要购买VPN产品，您需要多少并发用户连接？
 - ☐ 1~10个 ☐ 11~50个 ☐ 51~100个
 - ☐ 101~1000个 ☐ 1000个以上
- 6、 您可以接受的VPN产品价格是：
 - ☐ 3万~5万 ☐ 5万~10万 ☐ 10万~20万
 - ☐ 20万~50万 ☐ 50万以上
- 7、 您近期是否打算购买VPN产品？
 - ☐ 3个月内有需求 ☐ 3-6个月内有需求
 - ☐ 1年内有需求 ☐ 目前无需求 ☐ 不清楚

个人信息

姓名： _____
公司名称： _____
部门： _____
地址/邮编： _____
电话： _____ 区号 _____
电子邮件： _____

★ 公司所属行业：

☐ 银行\金融 ☐ 电信 ☐ 保险 ☐ 教育
☐ IT ☐ 电力 ☐ 交通运输 ☐ 其它

★ 您的职务类别？

☐ 公司总裁/执行董事 ☐ 首席财务官
☐ 首席信息官/IT总监 ☐ 总监/资深经理
☐ 经理(有下属员工) ☐ 经理(无下属员工)
☐ 行政人员 ☐ 员工 ☐ 其它

参与方式

请将填好答案的问卷沿虚线剪下，发送传真或邮寄回SafeNet China公司。我们将从所有收回的问卷中随机挑选出20位，每人获赠价值100元的精美运动水壶一个！

SafeNet China 联系方式：

地址：北京市海淀区西三环北路100号金玉大厦1603室
邮编：100037 联系人：赖丽莉
电话：010-88519191 传真：010-68727342
在线填写问卷：<http://cn.safenet-inc.com/products/iga-research.asp>



工欲善其事，必先“觅”其器

SITEVIEW 网管软件

游龙科技被德勤评为“2004 德勤亚太地区高科技高成长 500 强”

游龙科技被互联网周刊评为“2004 中国电子政务 IT 100 强”

SITEVIEW 获网管员世界“2004 优秀网管系统”殊荣

游龙科技由一批资深留学归国人员创办，并吸引了亚信、HP、联想、方正等一流工程师的鼎力加盟。SiteView 是游龙科技 6 年多的全部业务所在，它顺利通过了中国联通、中国移动、中国银行、海航等上千家用户近于苛刻的测试，很好地满足了数以万计中国用户自动化网络管理的需求。为中国用户提供更好用、更成熟、更稳定的产品，是游龙执着不断的追求。

SiteView 现已成功运用在电信、银行、电力、证券、媒体、政府、石油石化等行业。

免费咨询电话：800-810-5987

Contents 目录

聚焦

“2004 十大热门网络产品、网络事件评选”专题

- ◆ 2004, 网络该记忆什么? 5
- ◆ “2004 十大热门网络产品、网络事件评选”调查报告 6
- ◆ 需求为本 综合竞争 7
 - 2004 中国网络产品市场回顾及展望
- ◆ “2004 十大热门网络产品、网络事件评选”获奖公告 9
- ◆ “2004 十大热门网络事件”回顾 10
- ◆ “2004 十大热门网络产品”概览 13

技术与产品

专家观点

- 负载均衡设备将大显身手 23
- 拿什么拯救 RAID? 25

产业资讯

- “IT 培训直通车”驶向全国 26
- BEA eWorld China 2004 盛大开幕 27

产品评述

- 跨入 64 位之门 ★★★ 29
- 网关保护三重门 33
- 备份存档二合一 35
- 随需应变的好网络 35

新品快递

- 性能与防御并重等 37

方案与案例

应用方案

- 管理为先 应用为本 41

案例精选

- 安全高效并重的企业网 45
- 让校园应用跑起来 47

应用实践

系统构建

- “虚拟”的 Web 服务器 49
- 给园区网一对无线的翅膀 51

配置优化

- “升级”我们的校园网 53
- 让 RS6000 AIX 搭上网络快车 55
- 让 IP 参数对号入座 57
- 让企业多几个出口 58

横扫毒界之 2004

77

在信息安全领域,病毒与反病毒始终是最活跃的两支力量,而一年一度的病毒回顾可谓是安全界的年度大餐,使我们能够在须臾之间便可将一年的病毒现状与流行趋势尽收眼底,为下一年的信息安全建设做一个参考。“关注行业,检查自己”,永远是企业进行信息安全建设的原则。

本期专题,将带您浏览 2004 年的毒界,2004 年病毒的表现、今后可能的发展方向以及预防病毒的方法,在这里您都能找到。

隔而不断的物理隔离技术

97

物理隔离技术作为网络与信息安全技术的重要实现手段,越来越受到用户的重视,尤其是对政府、军事、保安、商业运作等部门来说,物理隔离不仅是需要,而且是必须的。那么,到底什么是物理隔离?如何实现物理隔离?本文将给您完整的答案。

解决共享难题

114

对于网管来说,共享是再也熟悉不过的,可是,要想自如地解决网络中的共享问题,也不是一件容易的事情。

谁说没有“后悔药”

125

通常计算机用户在出现重大误操作、数据丢失的时候会想到系统还原。作为网管员,系统还原就如它的同胞兄弟“系统备份”一样,是日常工作内容之一。

下期预告

应用实践

排除远程管理故障

用好远程管理可以有效地帮助网管员减轻网络管理的负担,不过,远程管理经常会出现这样那样的问题,该怎样解决这类问题呢?

安全防范

打造强“墙”

防火墙是安全体系中不可或缺的部分,如何配置才能让它更好地发挥作用?本期专题将从几款常见防火墙的配置方法入手,教您打造强“墙”。

网管工作必备

技术进阶指南

2005年1月 总第42期 www.netadmin.com

故障诊断

安全检查从日志做起	60
被遗忘的路由	61
一个共享问题及深入认识	63
发布不了的网页	64
NAT 也会惹故障	66
局域网内网络不通故障浅析	67
一次奇怪的网络故障	68
闹别扭的 BT	69

安全空间

安全防范

状态检测防火墙构建	71
新型网络攻击大追捕	74

防毒杀毒

横扫毒界之 2004 ★★★	77
◆ 2004, 病毒漫舞	78
◆ 蠕虫遍布整个网络	82
◆ 木马劫掠真实财产	84
◆ 脚本病毒甘做幕后帮凶	86
◆ 2004 年毒界“风云”榜	87
◆ 与毒过招	90
◆ 防毒路上, 还欠缺什么?	92

补丁升级

微软公布 6 大补丁	93
WINS 漏洞详细分析	94
近期主要漏洞一览	95

进阶驿站

知识讲堂

隔而不断的物理隔离技术 ★★★	97
◆ 物理隔离技术管窥	97
◆ 物理隔离典型技术方案概览	98
◆ 物理隔离技术路线回顾	100
网址与互连技术	101

手把手

企业无线局域网组建入门	105
◆ 无线局域网的基本结构	106
◆ IEEE 802.11 系列标准简介	106
◆ 无线局域网设置 Follow Me	108
◆ 无线局域网的管理与维护	109

培训认证

VPN 构建实战	110
Linux 历史漫谈 ★★★	112

工具与技巧

经验技巧

解决共享难题 ★★★	114
◆ Windows XP 的共享困惑	114
◆ Linux 共享接入的难题	115
◆ 打印机的麻烦	115
◆ 局域网中的共享“秘密”	116
◆ 轻松关闭默认共享	117
用好 SMS 2003 补丁分发	120
谈谈“同步”应用	122
小试脱机服务	123
给打印一个“可视化”窗口	124

网管工具

谁说没有“后悔药” ★★★	125
Linux 操作系统文件浏览器 Explore2fs	128
邮件列表好帮手	129

有问有答

	130
--	-----

编辑与读者

网管日记	134
动态播报, Yangsir 会客厅、精华看板	135
网管原创: 淘汰	136



网管员世界

主管单位: 中华人民共和国信息产业部
主办单位: 中国电子信息产业发展研究院
社 长: 李 颖
总 编 辑: 李超云
执行总编: 胡万进
副 社 长: 郑桂红
副 总 编: 杨文飞

编辑部电话: (010)88558021

编辑部 E-mail: netadmin@netadmin.com.cn

市场拓展部电话: (010)88559443/8012

发行部电话: (010)88558703

发行部 E-mail: world@ccu.com.cn

编辑出版: 《网管员世界》杂志社

地 址: 北京市海淀区紫竹院路 62 号
紫竹商住楼 2152 室

邮政编码: 100044

传 真: (010)88558703

网 址: www.netadmin.com.cn

邮发代号: 2-99

刊 号: ISSN 1671-2919

CN11-4708/TN

广告许可证号: 京海工商广字第 0264 号

承 印: 北京恒艺彩色印刷有限公司

出版日期: 1月5日

零 售 价: 12 元

全年定价: 144 元

本刊所有文字和图片作品, 未经许可, 不得转载、
编。凡投稿本刊, 或允许本刊登载的作品, 均视为已
权本刊在刊物、增刊、图书及本刊授权合作网站上使用
本刊支付的稿酬, 已包含授权费用。作者投稿给本
意味着同意上述约定, 若有异议, 请事先与本刊签订
面协议。

广告索引

版位	厂商简称	广告内容	咨询电话	版位	厂商简称	广告内容	咨询电话
封二	华为 3Com	IP 核心网	010-63108666	38	神州数码	高度灵活的 SAN	010-62693090
封三	福禄克	产品	010-65123435	40	华硕	华硕 VPN 路由器	010-82667575
彩内	金山	金山毒霸网络版 2.0	010-82334488	43	锐捷网络	校园 100 经典工程案例	010-68156699
彩内	浪潮	浪潮英信 NF280 服务器	010-62988886	44	ADIC	ADIC Pathlight VX 技术介绍第四辑	010-64106840/43
彩内	赛孚耐	SafeNet iKey1000 系列免费试用申请	010-88519191	70	中国计算机报	征订	010-88558003
目录页首页	游龙科技	SiteView 网管更自动、更智能	010-51655987	76	金山毒霸	企业反病毒技术与策略系列专栏	010-82334488
封底	美讯智软件科技	RiskFilter/SMG 反垃圾邮件信息网关	010-85188860	91	少年文摘报	征订	0931-8156600
28	Netscout	江苏移动解决方案	010-65675899	96	中国电脑教育报	合订本	010-88559660
34	游龙科技	电信级稳定性的 SiteView 网管	010-51655987	103	赛迪网	招生	010-88558957
36	Radware	产品	010-85183790	104	信息安全与通信保密	征订	010-66808404

新年致读者

本刊编辑部

送走了丰硕的2004，我们迎来了希望的2005。值此新年钟声敲响的时候，《网管员世界》杂志社所有工作人员，谨向一直以来给予我们关怀和支持的广大读者、作者及所有的网络管理人员致以亲切的问候和新年的祝福！

此时此刻，对于编辑部的所有同仁而言，我们感受到的是一种前所未有的兴奋和压力。如今的社会，哪个企业不需要网络？哪个网络不需要网络管理？二十一世纪的企业将是名副其实的网络企业，没有网管人员，网络就不能正常运行，社会活动就不能正常开展，企业运营就会陷于瘫痪。可以毫不夸张地说，网管人员将是社会和企业存在和发展的重要保障力量。但是，对于网管人员来说，谁不需要不断更新知识？不需要掌握最新的网络技术与产品？不需要提高实际问题解决能力和维护网络运行的能力？《网管员世界》，正是帮助企业网管员们解决这些问题的最佳渠道。

经过三年的发展，正如我们一年前预料的一样，2004年成为《网管员世界》蓬勃发展的一年。从内容上，《网管员世界》进一步巩固了实用性、知识性的特点，通过更多的刊物容量、两月一期的光盘和日益丰富的网站，为读者提供着越来越多的信息；从活动上，今年杂志社通过“2004中国网络管理技术大会”、“2004十大热门网络产品与事件评选”、“网管员之声”系列研讨会以及与微软、CA等公司联合举办的多场活动，全年共与全国范围数千名读者进行了面对面的交流，同时也通过网络等形式，与更多的读者进行了沟通……感谢一年来的所有读者，是你们的支持使我们这些改进得以进行，活动得以开展，也才有机会使《网管员世界》自身得以发展。

2005年，有25%的读者是我们的新朋友，我们也有了更多的责任和压力。2004年的迅速发展也让我们看到了自身的不足，诸如内容质量仍有待雕琢，渠道发行还不尽如人意，网站和论坛也还有太多的改进空间……在新的一年里，我们会在坚持原有特点的同时，积极改进这些问题。我们将继续贯彻“从网管中来、到网管中去”的方针，邀请更多的网管人员参与我们的刊物建设中来。我们将加强作者队伍建设，提高读者对刊物选题的参与程度，建立更完善的约稿、审稿制度，使刊物的内容更实用、更精彩。可以想见，2005年的《网管员世界》，将继续坚持实用性和知识性的编辑方针，刊物、光盘、网站的内容会更充实、更精彩；同时，我们还将继续组织各种有利于网管提高技术水平的活动，发挥好网络用户和网络厂商的桥梁作用。

作为专为网管人员服务的IT专业刊物，《网管员世界》的最终目的是帮助网管人员与时俱进，及时掌握最新的网管科技知识，不断提高网管人员解决问题的技术能力，维护网络的正常运行，保障所在企业各项业务的顺利开展。《网管员世界》的全部内容，都是为了达到这一目标。

读者的认可是本刊存在的基础，新的一年，我们依然会尽我们所能去探求和满足读者的需求，使《网管员世界》成为最受网管人员喜爱的IT专业刊物，我们热切希望广大网管员帮助我们实现这一目标。

预注2005年的《网管员世界》能得到您更大的认可！

网管员世界

开放系统世界

视窗世界

您订阅了吗?

www.netadmin.com.cn

订阅抽奖活动

正在进行!

如果您是上述任何一个刊物的读者,请登录《网管员世界》网站(www.netadmin.com.cn)在线填写您的信息,或者将您的姓名、工作单位、职务、所在城市、电话及电子邮箱用E-mail发给fk@netadmin.com.cn,即可参加我们的“订阅有礼”大抽奖活动。

一等奖 1 名

奖品为价值 4999 元的台式电脑一台

二等奖 10 名

奖品为价值 1000 左右的 MP3 一台

还不赶快行动?

咨询电话: 010-88559472

参与网址: www.netadmin.com.cn



“2004 十大热门网络产品、网络事件”专题报道

2004

网络应该记忆什么？

■ 本刊编辑部



中国电子信息产业发展研究院副院长、《网管员世界》杂志社社长李颖致辞

在 2004 年，中国的网络应用逐渐成熟，企业的网络化和信息化走向成熟，中国的网络使用者和管理者也逐渐走向成熟。在这一年里，有多少厂商推出了多少新的网络技术、新的网络产品，也许没有人能够数得清。但是，毋庸置疑，正是这些厂商、这些产品帮助了广大用户，把企业网络化、信息化，政府政务网络化、信息化，以及个人和家庭的网络应用推向了新的高潮。在网络化大潮中“手把红旗的弄潮儿”，对我国的网络化普及应用尤其做出了巨大的贡献。

那么，究竟是谁引领着 2004 年的网络大潮？谁是用户心目中网络产品中的“弄潮儿”？2004 年度与网络技术有关的大事件又有哪些？这些问题的答案，只有网络的用户和使用者才最有资格回答。

由中国电子信息产业发展研究院主办、《网管员世界》承

办的“2004 十大热门网络产品、网络事件评选”活动，就是为了恰当反映 2004 年网络应用的发展状况，揭示 2004 年最有价值、最值得人们记忆的网络产品和网络事件。

为办好本次活动，我们首先对本次活动进行了为期两个月的宣传，同时把厂商提供的和网络管理人员推荐的七大类 152 款网络产品的介绍，以及 23 个候选网络事件，公布在网站上，采用网站、电子邮件、传真等投票方式，最大范围地邀请了全国的网络管理人员评选出他们心目中 2004 年最热门的网络产品和网络事件。

2004 年 12 月 23 日，“2004 十大热门网络产品”和“2004 十大热门网络事件”颁奖典礼在北京赛迪大厦举办。主办者宣布了经过 34419 位读者评选出来的微软公司 Windows Server 2003 产品等十款“2004 十大热门网络产品”和“网络病毒肆虐 2004 年”等十个“2004 十大热门网络事件”，并对获奖产品的公司进行了颁奖，为本次活动划上圆满的句号。

可以说，本次活动是对 2004 年中国网络产品与网络事件的一次全面回顾，也是一次了解网络管理人员对网络产品关注点的全面检阅。对网络厂商来说，通过这次活动，除了对自身品牌有了一个极好的宣传，同时也获得了一次与用户良好沟通的机会。

在本次专题中，我们将为您详细介绍获得“2004 十大热门网络产品”和“2004 十大热门网络事件”的各个产品和事件，同时，还将就通过本次评选反映的 2004 年网络应用问题进行总结。■

“2004 十大热门网络产品、网络事件评选”活动报告

从2004年10月开始,来自全国的34419位读者参加了这次历时约两个月的“2004十大热门网络产品”和“2004十大热门网络事件”评选活动,其中,42%的用户属于无记名投票。活动采取了限制同一IP地址重复投票等措施,以保证投票的公正性。从填写投票信息的用户看,参加投票的用户来自全国各个省市、自治区的各个行业、企业,用户以一线网络管理人员为主,同时也包括了企业、政府、学校等行业的普通网络应用人员。

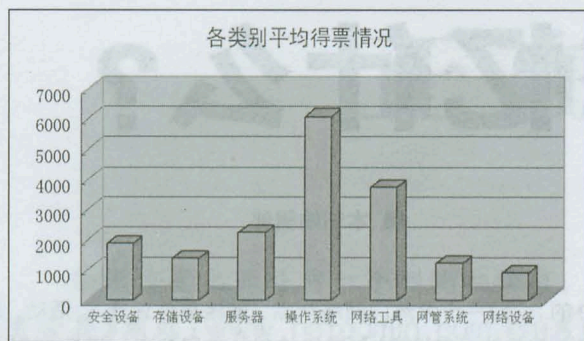


图1 各类别平均得票情况

产品排名竞争激烈

本次参选的产品,是主办者邀请当前市场主流的网络厂商免费提供的,也有部分是网络管理人员推荐的。参评产品共分安全设备、存储设备、服务器、网络操作系统、网络工具、网管系统和网络设备七大类约15个子类。为了投票不至于过于分散,要求每个厂商每个子类只提供主流的产品。尽管如此,本次活动还是征集了152款产品,基本囊括了当前市场主流的各类网络产品。

从评选过程看,用户对各款、各类产品都相当熟悉,所有的产品均得到了用户的推荐,在公示评选的一个多月的时间里,前十名的竞争一直非常激烈。某个产品“独霸天下”的局面在本次调查中几乎没有。除了微软公司Windows Server 2003产品的投票率高达35%以外,其他产品的得票率基本都在20%以下。从类别上看,不同类别的各个产品投票率也较为平均,显示用户的网络应用已经非常全面和普遍。

安全产品表现突出

虽然平均来说各个类别差异不大,但从入选前30名的产品看,各个类别之间的差异还是非常明显的。从结果看,前30名产品中,安全产品占了14款,接近50%。而对比参选

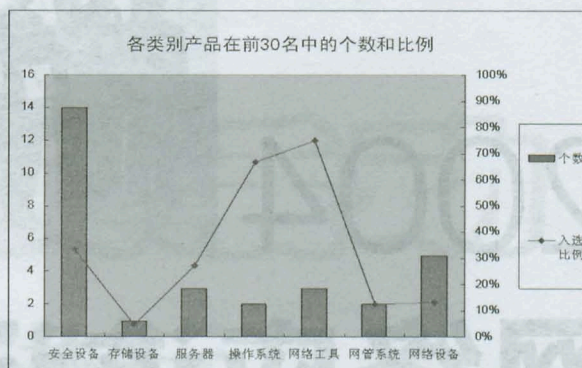


图2 各类别产品在前30名中的个数和比例

的总产品数量,入选前30名比例最高的却是操作系统和网管工具,在这两个类别中,都只有一款参选的产品没有进入前30名。相对而言,传统的网络产品——如交换机、路由器等,则只有5款产品挤入前30名。

这些数据显示了中国网络应用还在发生变迁。当今的企业网络化重心,已经从简单的构建网络转移到了网络的应用、运营、管理和安全保护等方面。尤其是网络安全,已经得到了企业网络应用的高度重视。

同样能体现用户对网络安全的关注,还有“2004十大热门网络事件”的评选,对“网络病毒肆虐2004年”这条新闻的关注度名列榜首。此外,其他关于安全的新闻,例如“全球首届电子邮件及反垃圾邮件技术大会召开”等,也都获得用户的充分关注。

本次参加评选的存储设备的得票率不高,这说明当前企业对网络存储设备的关注程度还不够,需要相关厂商和媒体共同帮助企业加强对企业存储方面的了解和认识。

本国网络事件受关注

通过本次“2004十大热门网络产品”和“2004十大热门网络事件”的评选,主办者另一个重要的感受就是用户对本国网络事件热切的关注。

本次热门产品的前30名中有超过一半是本国公司产品,本次热门事件的评选,关于中国IT业新产品发展的三条新闻“中国超级计算机首次跻身世界十强”、“中国成功研制出高性能路由交换核心芯片”、“国产操作系统‘麒麟’问世”均取得了不俗的成绩,这一方面表示了用户对这些新产品的认可,同时也表达了国人对中国IT发展的热切期望。

需求为本，综合竞争

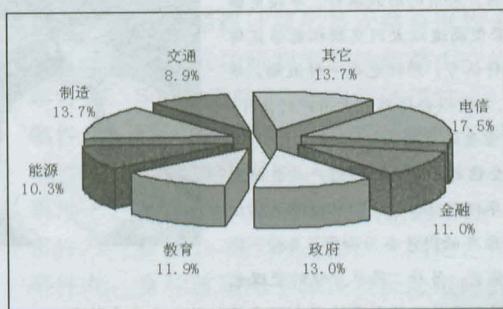
——2004 中国网络产品市场回顾及展望

■ 赛迪顾问高级咨询师 李辉

2004 年，中国通信与网络产业保持稳定增长的发展态势。各大运营商竞争的中心都放在了互联网、宽带接入及内容提供、行业应用等增值业务方面，因此网络建设投资力度都进一步加大。中国网络设备市场可以细分为路由器、以太网交换机、IP 语音、网络安全、ADSL 系统及 WLAN 设备等。2004 年中国网络设备总体市场规模预计为 285 亿元，同比 2003 年增长 25.3%，取得了较为快速的增长。

行业市场需求强劲

2004 年，电信、政府及能源行业是重点市场，其中电信行业所占份额依然排名第一，而能源和政府行业的销售额同比增长也超过了 25%。具体行业分布参见图 1。



2004 年网络市场行业分布图

2004 年，中国行业信息化工程中涉及大量局域网的升级改造工程，加大了对以太网交换机的需求。其中，教育和政府行业依然保持较高的增长率，其行业应用需求的不断扩大和深入，为中国网络设备市场带来无限商机。目前主力厂商的市场优势仍比较明显，所以整个市场的品牌结构变化并不大。但市场表现活跃，Cisco、华为 3Com 都纷纷推出自己的主打产品，以适应不断发展变化的用户需求。

而在 SMB/SOHO 市场中，因为这一市场进入门槛较低，因此参与者也很多，所以在 2004 年，整个 SMB/SOHO 市场可谓相当火爆，但没有绝对优势的厂商出现，所以市场竞争非常激烈。此外，在 2004 年，渠道建设依然是各大厂商的重点，随着行业市场的蓬勃发展，庞大的行业市场也将更多地依托渠道商来进行占领，所以渠道建设也成为各大厂商上半年的关键词。

重要设备亮点不少

2004 年，中国 WLAN 设备市场整体走势良好，总体市场规模预计达 5 亿元。虽然受到标准之争的困扰，但是，包括运营商、设备厂商和消费者在内的市场参与者依然看好中国 WLAN 市场未来的发展潜力。同时，中小企业和家庭 WLAN 市场份额在 2004 年上半年不断增加，Cisco、华为 3Com、Netgear 等大公司也开始在渠道上有所创新以应对市场的变化，纷纷开始进军中低端市场，同时通过扩大分销商和零售商渠道来抢占市场，这是 2004 年中国 WLAN 市场出现的明显变化。各厂商在已有的运营商和系统集成商的基础上，开始进一步加强渠道队伍的建设。IT 市场向来是“得渠道者得天下”，随着 WLAN 设备市场竞争的加剧和向非运营市场的倾斜，相关厂商对渠道的争夺和控制力度还会不断加强，因此，随着中低端市场的不断开发，相应的分销商和零售商队伍也将随之扩大，真正的渠道争夺战好戏还在后头。2004 年中国 WLAN 设备市场的主力厂商是 Cisco、华为 3Com、Nokia、Netgear 等。

与 2003 年相比，2004 年 ADSL 接入设备总体市场规模预计为 70 亿元。新增销售量小幅度上升，而平均价格小幅度下降，因此，对于 ADSL MODEM 市场，仅仅 OEM 设备的利润空间已经越来越小，未来这种厂商的竞争压力将会越来越大。2004 年中国 ADSL 设备市场的主力厂商是华为、上海贝尔阿尔卡特、大亚、中兴及港湾等。

分析表明，运营商的需求状况直接决定了 ADSL MODEM 厂商的前途。毕竟在宽带市场发展的初期，采用什么样的技术、发展多少用户等都是运营商在规划，他们才是推广 ADSL 宽带接入的主体。2003 年 ADSL 用户的雪崩增长，各 ADSL Modem 厂商销量随之增长。而 2004 年，中国的宽带接入市场仍将蓬勃发展，凭借以前的固有优势，主力厂商仍能处在一个很好的位置。通过对 2004 年 ADSL 设备市场的跟踪和分析表明，运营商的设备需求状况发生了深刻改变：功能单一的 Modem 系列逐渐不为运营商接受，而那些能够平滑升级到 ADSL2/2+，带有多条 PVC 设置、支持远端升级和远程管理、以及配有路由功能的 Modem 更受运营商青睐。而这些变化正是运营商运营思路、用户使用习惯变迁的一个直接结果。

2003 年全球全网性安全危机的此起彼伏是网络安全设备保持增长的根本动力，而一些新兴市场的快速增长，例如

WLAN 市场等,也带动了网络安全设备市场的增长。网络安全危机的不断出现也使得客户充分意识到构建网络安全体系的重要性,这也直接促进了网络安全设备市场的增长。2004 年,中国网络安全设备市场规模预计为 15 亿元,取得了较大幅度增长,这是因为用户对网络安全的认识开始成熟;设备厂家技术的日新月异,使网络安全产品日益完善;伴随中国经济的高速发展,网络建设的突飞猛进,中国网络安全设备市场变得更成熟。2004 年该市场主力厂商为 Cisco、Juniper (收购 Netscreen)、天融信、东软等。

IP 语音市场是 2004 年上半年中国网络设备市场的一个亮点,市场规模预计为 29 亿元。运营商竞争日趋激烈,对 IP 语音业务的资费、政策均有所放宽,相应的增值业务也逐渐增

多。IP 语音设备主要包括 PBX 和 IP 话机, Cisco 一直是该领域的倡导者。随着市场规模的增长和技术的逐渐成熟, IP 语音设备市场的提供商增多,竞争也日趋激烈。竞争者一部分是大型通信设备商,另一部分则是投入该领域的中小厂商,市场的广阔前景将使厂商加大对该领域的投入。

展望 2005 年,运营商将继续加大网络建设投资,其针对行业的解决方案还将拉动行业的网络设备投资,随着“十一五”计划的临近,行业自身的需求也将促使网络设备市场保持快速增长。同时 SOHO 市场将进一步被激活,高性价比的解决方案将成为市场的宠儿;至于家庭市场则仍须一定时间的培育,其市场潜力才会得到充分的发挥。综合以上因素,预计 2005 年中国网络设备市场规模将达 337 亿元,同比增长 18.2%。ISI

获奖厂商感言

CA 公司大中国区 市场总监 尹婉智

在刚刚过去的 2004 年里, CA 公司取得了一系列令人骄傲的成绩,今天又获得了“2004 十大热门网络产品”称号,为我们在 2004 年的突出表现锦上添花。

此次获奖的

产品 eTrust SCC, 可以用于发现相关安全数据并按优先性进行排序,从而方便管理员有效地实时管理风险,使企业能够高效而且有效地保护他们的信息架构。在中国市场推出以来,

eTrust SCC 在国内市场得到了广泛的好评和欢迎,许多大的电信运营商和大型商业银行都成为了 CA 产品的使用者。更值得一提的是, eTrust SCC 还应用在了 2004 年雅典奥运会上,以确保奥运会得以免遭多种网络攻击的威胁。

作为全球领先的网络安全软件供应商, CA 不仅提供优秀的产品,还提出“主动安全管理”的领先理念。我们可以帮助企业实现集成的、基于角色的安全管理,从被动的防御战变为主动出击,最终帮助企业实现主动地安全管理。



华硕中国业务事业群网络通讯事业部产品经理 傅建华

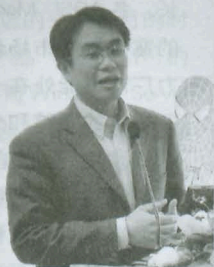
《网管员世界》组织的这次活动,采用的形式很好。华硕电脑 GigaX3112 12+2 GBIC 端口三层网管型高速以太网交换机能够获得这个奖项,是广大用户对华硕的一种认可,同时也是一种激励。华硕电脑进入网络市场的时间并不长,之所以会得到广大用户的认可,华硕产品本身的特色显然起着非常重要的作用。

对于网络产品来说,产品的安全稳定对于一款网络产品至关重要,也是用户对产品的重要需求。华硕 GigaX3112 12+2 GBIC 端口三层网管型高速以太网交换机采用独有的固件备份和 BIOS 备份,能够在系统出现故障后,迅速将系统恢复。另外,简单方便的管理也是华硕电脑 GigaX3112 12+2 GBIC 端口三层网管型高速以太网交换机的一个重要特色。



趋势科技网络(中国)有限公司策略部经理 曾嵘

网络病毒墙(NVW)是趋势科技在 2004 年最新推出的针对大企业用户推出的最新的主动式网络防护硬件设备,可协助用户防制互联网蠕虫之类的网络病毒,在爆发病毒疫情时隔绝高风险的网络脆弱环节,在网络层部署由趋势科技提供的安全防护策略,并能在缺乏防毒保护的设备等潜在感染源连接网络时,予以隔离和清除。自从 NVW 在中国面市以来,在金融、电信等行业获得了很多客户,有着很好的销售合作前景。2005 年, NVW 将继续进行更新和改进,以不断满足大家的需求和发展的趋势。



趋势科技一直专注于为客户提供实时更新的对不可预知和威胁的防护,并与其它领域的最佳厂商结成战略同盟。在 2004 年趋势科技取得了许多骄人的成绩,包括与思科的全球合作。非常荣幸获得《网管员世界》颁发的“2004 年十大热门网络产品”,这是对我们在国内的成绩做的最好的认同。

“2004 十大热门网络产品”获奖名单

- | | |
|---------------------|--------------------------------|
| 1. 微软(中国)有限公司 | Windows Server 2003 |
| 2. 思科系统(中国)网络技术有限公司 | Cisco IOS 防火墙 |
| 3. 国际商业机器中国有限公司 | IBM BladeCenter 刀片服务器 |
| 4. 华为 3Com 技术有限公司 | Quidway S8500 系列万兆核心路由交换机 |
| 5. 趋势科技网络(中国)有限公司 | 趋势网络病毒墙(NVW) |
| 6. 冠群电脑(中国)有限公司 | eTrust Security Command Center |
| 7. McAfee 公司 | McAfee IntruShield 2600 |
| 8. 浪潮(北京)电子信息产业有限公司 | 浪潮英信 NF280 服务器 |
| 9. 华硕电脑 | GigaX3112 系列三层千兆交换机 |
| 10. 美讯智软件科技有限公司 | 邮件安全信息网关 RiskFilter/SMG |

“2004 十大热门网络事件”名单

- 事件一 网络病毒肆虐 2004 年
- 事件二 中国超级计算机首次跻身世界十强
- 事件三 中国成功研制出高性能路由交换核心芯片
- 事件四 Sun 与微软 10 年官司终了结
- 事件五 IPv6 地址争夺中国申请量仅全球 1.8%
- 事件六 国产操作系统“麒麟”问世
- 事件七 微软 Windows 源代码新闻不断
- 事件八 多管齐下严厉“封杀”网络色情
- 事件九 全球首届电子邮件及反垃圾邮件技术大会召开
- 事件十 华为思科知识产权案和局收场

“2004 十大热门网络产品、网络事件评选”参与获得奖名单

为了对参与投票的用户表示感谢,《网管员世界》随机抽取了 20 名读者,他们将获得精美野餐垫一套,名单如下;另外 200 名读者将获得 10 元超星读书卡一张,由于篇幅所限,名单略。

获奖者名单:

- | | | | | |
|---------|---------|---------|---------|---------|
| 刘淼(深圳) | 许辉(大庆) | 闵伟清(上海) | 吴应嘉(贵州) | 余明(福建) |
| 严志芳(海南) | 李成坤(青岛) | 雷伟源(广州) | 李玉东(山东) | 张新明(江苏) |
| 钱建军(宁波) | 林幌(莆田) | 邱殿兵(温州) | 文涛(成都) | 廖春华(南京) |
| 翟志明(重庆) | 宋光文(洛阳) | 王光(哈尔滨) | 赵芮(北京) | 郭立英(济南) |

“2004年十大热门网络事件”回顾

■ 本刊编辑部

事件 1 网络病毒肆虐 2004 年

MyDoom、NetSky、Bagle 和震荡波 (Sasser) 等病毒在网络世界里掀起了轩然大波。震荡波 (Sasser) 使全球数百万计算机受到感染, 大量铁路、银行甚至包括欧洲委员会办公室的控制系统都未能幸免。MyDoom、NetSky 和 Bagle 的变种不断出现, 感染率居高不下, 都曾坐上过“每月十大病毒排行榜”的冠军宝座。

点评: 我国的互联网应用已经开始进入快速增长期, 而网络病毒也如影随形, 数量急速增加。目前, 木马病毒危害最为严重, 而邮件蠕虫病毒也对企业邮件服务器造成了巨大影响。利用人们行为习惯的弱点, 通过系统漏洞传播已经成为当今病毒的一大特点, 也将成为人们网络生活中一个长久的威胁, 现在的邮件病毒、木马病毒都呈现出了这个趋势。尤其是网络环境的转变, 更可能对病毒的传播形态、发作趋势产生影响。随着互联网应用和 ADSL 等宽带的普及, 网络病毒将有可能愈演愈烈。这些病毒盗窃个人信息、网上银行密码、游戏帐号等等, 具有明显的商业目的。预计在 2005 年, 网络病毒的数量还会猛增。

面对网络病毒的巨大威胁, 用户首先要在思想上予以高度重视, 把防病毒作为企业信息化建设的首要工作之一。在操作层面上, 企业用户要随时更新反病毒软件的病毒库, 尽量使用网络版反病毒软件来保证网络免受病毒侵害, 严格设置邮件服务器的规则来拒绝接收病毒邮件。个人用户也要积极使用反病毒软件彻底清除病毒, 减少病毒通过个人电脑作为发送病毒邮件的源头。

事件 2 中国超级计算机首次跻身世界十强

在美国能源部劳伦斯·伯克利国家实验室 2004 年 6 月公布的最新的全球超级计算机 500 强名单中, 中国曙光计算机公司研制的超级计算机“曙光 4000A”排名第十。这是中国超级计算机首次跻身世界十强。这是此次 500 强排名中惟一跻身前十名的非美国和日本研发的超级计算机。“曙光 4000A”运算速度可达每秒 8.061 万亿次。

点评: 曙光 4000A 是一个面向网络的超级服务器, 是 863 计划的一个重大的成果, 同时也是科学院知识创新工程和上海市信息化建设的一个成果, 曙光 4000A 的意义不

仅仅是一台高性能计算机, 而是满足了以上海市为代表的中国用户对十万亿次机器实实在在的需求。而且, 高性能计算对于国家竞争力的提高, 对于我们国家经济发展、国家安全都有极其重要的意义。

曙光 4000A 的研制成功, 是用户及早介入机器的研制, 参与机器研制全过程这一模式的成功典范, 为我国高性能计算机的研发走出了一条新的道路。曙光 4000A 的研制成功, 将我国通用高性能计算机系统的研制水平提升到一个新的高度, 这是我国高性能计算机上发展史上的新的里程碑, 标志着中国正在逐步走向高性能计算机的应用之路。曙光 4000A 将作为中国国家网格的重要资源, 安装在网格主结点, 和专项的网格技术一起, 成为我国新一代信息技术的重要支撑部分。值得注意的是, 高性能计算机的应用非常重要, 因为高效能计算机的生命周期是比较短的, 如何在它的生命周期内, 发挥应有的作用, 是摆在研发人员和用户面前的问题。

事件 3 中国成功研制出高性能路由交换核心芯片

我国第一颗具有完全自主知识产权的高性能路由交换核心芯片——“华夏网芯” TS2410 于 2004 年 5 月通过了鉴定, 从此改写了中国高性能路由交换机没有“中国芯”的历史。鉴定认为: 南山之桥研制的此芯片在采用中心架构的网络处理器 NFP、网络的安全管理性、可集成接入网功能和用户管理功能等方面优于国外同类产品, 整体处于国内领先、国际先进水平。

点评: “华夏网芯” TS2410 的面世, 是包括龙芯在内的“中国芯”的又一重大成果。网络安全直接关系到国家安全, 核心芯片、操作软件都是可能造成机密泄露、网络攻击的隐患, 因为这些网络设备的核心构成是如此的复杂, 在芯片、软件源代码中如果植入恶意的“后门”, 通过远程就可以控制网络设备。虽然现有国内交换机上可以提供自主开发的系统设备, 但其中的核心交换芯片仍然依赖境外, 安全隐患依然存在, 网络安全受制于人的被动局面没有得到根本改变。而“华夏网芯”具有完全自主知识产权, 没有“安全后门”, 改变了国产交换机、路由器核心芯片全部依赖于进口的弱势局面。“华夏网芯”市场前景广阔, 它的推广和应用将对中国民族 IT 产业产生重大影响。南山之桥“华夏网芯”的成功, 代表了国外芯片垄断时代的结束, 民族企业掌握路由交换核心芯片技术的开始。■

事件 4

Sun 与微软 10 年官司终了结

2004 年 4 月, Sun 公司发表正式声明, 宣布与微软达成和解协议, 由微软赔付 16 亿美元, 最终私下了结双方长达 10 年的垄断和专利官司。16 亿美元的赔付金额中有 7 亿美元用于平息微软与 Sun 之间旷日持久的垄断官司, 另外的 9 亿美元用于了结双方的专利纠纷。

另外, 微软与 Sun 宣布签订一项为期十年的技术合作与许可证协议, 以使双方的产品能够更好地相互协作。该项协议是这两家公司在以和解方式解决双方长久以来的法律纠纷之后宣布的。

点评: 微软与 Sun 签署的和解协议是 IT 行业的一个重大事件。虽然这个协议没有改变两家公司进行竞争的事实, 但是, 这个协议意味着微软与 Sun 将以从未有过的方式进行合作。这个协议对于双方的用户和开发人员也是个好消息。根据这个协议, 微软与 Sun 将相互提供有助于提高兼容性的技术, 使微软和 Sun 能够开发更好地相互兼容的产品。实际上, 每个大的 IT 客户都使用多家公司的 IT 产品, 这个协议能够帮助 IT 管理人员更好地运行多家厂商的系统。

事件 5

IPv6 地址争夺中国申请量仅全球 1.8%

截止到 2004 年 6 月, 全球已分配的 606 个 IPv6 地址块中, 中国仍旧只有 11 块, 占全部已分配 IPv6 地址块数量的 1.8%, 而且这个数据仅仅统计了 IPv6 地址块数, 忽略了每个地址块的大小。我国分配到的 IPv6 地址块均为缺省的 / 32, 与美国国防部所积极申请的 / 16 巨大地址块相距甚远。如果把最近几个月以来全球各地持续增加的大块地址分配情况考虑进去, 中国所分配到的 IPv6 地址资源在全球所占的份额就更为稀少。

点评: IP 地址资源对于互联网领域乃至整个信息技术领域的意义, 相当于国土资源、矿产资源等对于一个国家的意义。传统互联网领域资源分布的全球格局已成事实, 对于后来者没有更多的机会与发展空间。对中国而言, 争取下一代互联网资源分配的主动权, 就成为更加迫切和具有战略意义的目标。

尽管在 IPv6 的研发及部署上我们与其他国家处于同一起跑线, 但是在下一代互联网的基础资源 IP 地址申请上, 中国无疑正在面临严峻挑战, 甚至是再次落后的局

面。从 2003 年年底至今, IPv6 地址申请不断升温, 所申请的地址规模不断扩大, 纪录一再被刷新。出现的这一系列现象的直接原因是: 全球各地区的 IPv6 实质性甚至大规模部署产生了对 IPv6 地址乃至大块地址的需求。而中国从各 RIR 申请到的 IPv6 地址块仅为缺省分配值 / 32。为什么中国的运营商不积极? 原因就在于目前中国的 IPv4 部署尚有利用空间。基于 IPv4 的投资现在只有 5% 的回报, 运营商当然不愿意现在就推进 IPv6。在所有因素中, 运营商看不到一个现成的、必须基于 IPv6 网络的应用业务是关键, 即缺乏杀手级产品是中国 IPv6 产业最大的瓶颈。

事件 6

国产操作系统“麒麟”问世

2004 年 9 月 13 日, 首款具有完全自主知识产权的国产服务器操作系统——麒麟 (Kylin) 问世。麒麟操作系统是国家高技术研究发展计划 (“863” 计划) 的重大成果之一。与此同时, 麒麟操作系统的主要研制方——国防科技大学和参与研发的重要伙伴——联想集团在北京联合宣布, 双方将携手承担麒麟操作系统的产业化推广任务。

点评: “麒麟”服务器操作系统产业化战略合作协议的签署, 标志着我国在服务器操作系统开发上进入崭新的阶段。“麒麟”操作系统从研发进入产业化阶段对国家信息化建设具有重大战略意义。服务器操作系统是信息化基础设施的关键组成部分, 长期以来基本被外国厂商控制, 成为我国信息化应用及信息安全的隐患。“麒麟”不仅为国家在信息产业技术领域牢牢掌握自己的命运起到核心作用, 而且还肩负着振兴国产服务器市场的重任。该操作系统的推出对服务器产业极具现实意义。

麒麟服务器操作系统将会在三大领域率先取得应用上的突破: 一是电子政务领域, 这类用户对信息的安全性、网站的防攻击性要求较高, 麒麟“国产”血统具有天然竞争优势, 如完成自主知识产权的内核不受 GPL 规则限制, 既可灵活地面向应用开发内核代码, 又可对外部攻击者屏蔽内核模块。二是电信增值业务。这些领域目前主要使用的是 Linux 操作系统, 麒麟内核和与这一领域的应用软件是完全兼容的, 更重要的是麒麟可以根据用户个性化需求从内核上进行优化。三是国防领域。麒麟操作系统在自主知识产权、安全机制上有严格保证, 并且与国防科大联合开发, 无形中增加了麒麟进入相对封闭而又敏感的国防领域的砝码。

目前 64 位服务器热潮涌动中国市场, 但应用成为其进一步发展的瓶颈, 该系统的推出为 64 位真正普及应用提供了强有力的支持。

事件 7

微软 Windows 源代码新闻不断

2004 年 2 月, 微软公司宣布, 其 Windows 2000 和 Windows NT 4.0 操作系统的部分源代码已被泄漏并被非法放到互联网上。由此引发了一场 Windows 安全的讨论。

7 月 20 日消息称, 微软宣布, 将向来自全球 27 个国家的“最具价值的开发团体 (MVP)”免费提供 Microsoft Windows 2000、Windows XP、Windows Server 2003, 以及未来即将推出的所有 Microsoft 操作系统的源代码程序, 这其中还包括上述操作系统的所有版本、服务包和测试版本。

点评: 尽管 Windows 2000 和 NT 4.0 操作系统中有一些源程序代码已经被黑客盗取, 但是专门研究计算机安全问题的工程师们表示: 这次事件不会给微软的操作系统软件造成更多的攻击弱点, 不太可能导致出现大规模的安全事故。Windows 部分源代码泄漏可能使黑客们更容易编写恶意代码, 并攻击 Windows 操作系统的某些部分。但是, 现在黑客们通过网上下载的 Windows 部分源代码没有影响到 Windows 的核心内容或者是数据共享协议, 而这些东西才是黑客们最感兴趣的。

而微软开放更多的源代码程序, 则有助于我国对操作系统源代码的研究, 并加强信息技术安全性。

事件 8

多管齐下严厉“封杀”网络色情

2004 年 7 月 16 日, 公安部联合 14 个单位和部门宣布开始打击淫秽色情网站专项行动。与此同时, 信息产业部、最高人民法院、最高人民检察院、文化部、全国妇联、国家工商总局等国家多个部门也展开了各自的行动, 从技术、法律、行政等方面打击网络色情。专项行动开展以来, 取得了明显的效果, 对我国互联网更加规范有序的发展起到了积极促进作用。

点评: 淫秽色情网站首先伤害的是青少年, 伤害他们就是在摧毁民族的未来。打击淫秽色情网站就是要为青少年营造一个良好的网络环境。从这个意义上说, 专项行动功在当代、利在千秋。为了让网上黄毒不卷土重来, 专项行动不能只管一时, 而是要作为一项长期的工作坚持下去。一方面严厉打击网上贩“黄”者, 另一方面, 要彻底切断“黄网”的生财之道, 铲除淫秽色情网站生存的土壤。在此过程中, 我们需要逐步探讨建立长效机制, 配合有关部门把经济制裁、行政管理、法律约束、技术手段控制与思想教育、行业自律与社会监督有机结合起来, 对淫秽色情网站“发现一个, 关闭一个, 绝不手软”。打好这场打击淫秽色情网站的人民战争。

事件 9

全球首届电子邮件及反垃圾邮件技术大会召开

中国互联网协会代表团参加了 7 月 30 日至 31 日在 Mountain View 举行的全球首届电子邮件及反垃圾邮件技术大会 (CEAS)。尚易公司 (corpease.net) 等代表国内电子邮箱服务行业出席了会议。会上, 包括 MAPS 在内的多个国际的反垃圾邮件组织的负责人与中国三位代表深入讨论了中国的垃圾邮件问题, 尤其是中国的 IP 黑名单问题。

点评: 以前, 由于中国邮件服务业缺乏与国外反垃圾邮件组织以及国际大型邮件运营商直接沟通的渠道, 所以, 国外对来自中国的垃圾邮件投诉通常得不到及时回复。因此, 很多国际反垃圾邮件组织就采用大规模封堵中国的 IP 地址的过激做法, 迫使中国的邮件服务商不得不采取相应的措施, 防范垃圾邮件。中国代表团此行, 就是为了促进中国和国际各大反垃圾邮件组织、国际邮件运营商直接交流, 在双方之间建立一条畅通无阻的沟通桥梁, 尽量避免再出现中国 IP 地址被国际反垃圾邮件组织大规模封堵的情况, 为中国发展国际电子商务铺设一条坦途。

事件 10

华为思科知识产权案和局收场

美国当地时间 7 月 28 日, 华为公司、思科公司、3Com 公司向得克萨斯州东区法院马歇尔分院提交了终止诉讼的申请, 法院遂签发法令, 终止思科公司对华为公司的诉讼, 最终全部解决了该起知识产权案件的争议。同时意味思科今后不得再就此案提起诉讼或者就相同事由提起诉讼。至此, 这场历时一年半的跨国知识产权案以和解告终。

点评: 不管诉讼案的结果是令谁满意, 这件事情对未来通信市场的意义远远超出了其本身。对于华为, 事件的解决为其树立了新的国际企业形象, 华为也通过处理事件本身中所付出的努力, 使自己从一个在国际市场上不知名的中国企业, 成为了广受国际关注的通信企业。而思科也没有因为敏感的知识产权问题而失去广阔的中国市场。

华为为中国企业走向世界通信产业大舞台做出了一个范例。随着我国电信市场的逐步开放, 我国企业也会逐步地走向国际市场, 而中国厂商在“走出去”时会遇到不少问题, 其中一个很重要的环节就是知识产权。华为以自身的行动为在国际事务中缺乏经验的中国企业做出了一个表率, 并且为中国企业在以后碰到类似情况时如何面对提供了参考。 INI



微软(中国)有限公司

Windows Server 2003

Windows Server 2003 是一种高度集成、可靠安全、功能综合的基础架构,用来帮助企业级客户降低成本并提高IT运营的效率 and 有效性。基于 Windows 2000 系列强大的功能,新型服务器平台可帮助客户扩展现有资源,同时为构建新一代连接应用、提高企业生产效率奠定基础。

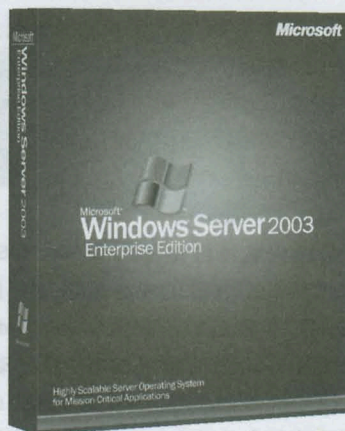
作为微软首推的服务器操作系统,Windows Server 2003 开启了高性能企业计算新纪元,具有高安全性、高可靠性、高可管理性、高可扩展性和对以前版本良好兼容性。

创造更高的商业价值

今天的商业环境要求企业在不停地消减成本、缩减预算的同时,还要具备对客户需求 and 市场变化作出快速响应的能力。作为新一代企业计算平台,Microsoft Windows Server 2003 结合同步上市的 Microsoft Visual Studio .NET Version 2003 及 Microsoft SQL Server 2000 企业版(64 位),在商业价值领域建立了一个新标准,并提供了一种支持可互操作的集成基础架构。这种基础架构可提供业界所需的领先运行性能、高可扩展性和高可靠性,以支持今天财务预算有限的各企业的 IT 部门的建设要求。Windows Server 2003 Datacenter 和 Microsoft SQL Server 64 位企业版运行在惠普基于英特尔安腾 2 芯片的 Superdome 系统,创造了全球目前最高的 TPCC 值,首次突破 70 万大关,每分钟处理的交易次数达到了 707102,每一次交易平均比其它的快了 3.9%,但却便宜 18%。在为企事业级客户提供卓越性能的同时,帮助企业客户有效降低系统成本。

Windows Server 2003 在设计上力求支持今天企业的需求,即:缩短停机时间、降低运营成本,同时建设高安全、可管理的基础设施。Windows Server 2003 提供了最高水平的可靠性、可扩展性和可管理性,同时在成本降低方面取得了突破性进展,使客户更快地获得投资回报。

今天的公司依靠计算技术来提高跨业务部门的工作效率。Windows Server 2003 提供了使工作变得更加轻松的基础,可以共享项目并进行协作,可以从任何地方通过企业内联网有效地利用关键信息,可以通过互联网使用 Microsoft Windows Media Services 9 Series 分享更加丰富和效率更高的流媒体培训和信息沟通。因此,无论是需要使用更加简便的强大工具的前端知识工作者,还是要求部



署迅速、易于管理的业务的后台管理员,他们都能够以更高的效率来工作。

Windows Server 2003 与 .NET 架构 1.1 版,再加上重新设计的 IIS 6.0 和 ASP.NET,大大提高了开发人员的工作效率,并显著加快了上市时间。仅用很少的代码行要求实现更优越的性能,从而在很大程度上提高了开发人员的工作效率并缩短上市时间。

此外,Windows Server 2003 在国内业界市场已经形成了良好的生态系统,基于 Windows Server 2003 已经有大量的服务器硬件厂商、软件厂商、系统集成商为企业客户提供安全可靠的解决方案,涵盖各个领域与行业。国内有超过 10 万人受过严格的基于 Windows Server 2003 与 Visual Studio .NET 2003 的开发训练,为企业客户进行广泛的方案选择提供了良好的平台。

编辑部点评:

作为微软首推的网络操作系统,Windows Server 2003 包含了基于 Windows 2000 Server 构建的核心技术,从而提供了经济划算的优质服务器操作系统。Windows Server 2003 家族增强了群集支持,从而提高了其实用性。对于部署业务关键的应用程序、电子商务应用程序和各种业务应用程序的组织而言,群集服务是必不可少的,因为这些服务大大改进了组织的可用性、可伸缩性和易管理性。Windows Server 2003 通过由对称多处理技术(SMP)支持的向上扩展和由群集支持的向外扩展来提供可伸缩性。Windows Server 2003 在安全性方面提供了许多重要的新功能和改善,包括公共语言运行时、增强的 IIS 6.0、卷影副本等,这些功能对提高系统的稳定性、可靠性有着非常重要的作用。

思科系统(中国)网络技术有限公司



Cisco IOS 防火墙

今天, Internet 成为功能强大的新技术焦点, 极大地增强了企业与客户、供应商、合作伙伴及远程雇员的通信, 用户必须确信网络业务, 尤其是公共网络上的业务是安全的, 他们需要安全的解决方案来: 保护内部网络, 防止黑客入侵; 提供安全的 Internet 和远程访问连接; 通过 World Wide Web 启动网络贸易。

Cisco IOS 防火墙特性集作为 Cisco IOS 软件的一个选项上市, 提供了一个先进的安全解决方案, 可以保护网络, 防止安全违规。它运行于 80% 以上的 Internet 骨干网络路由器中, 提供了全面的网络服务, 并启动网络化的应用程序。

Cisco IOS 安全服务为建立 Internet、内部网及远程访问网络提供安全解决方案, 进而提供端到端网络安全。

产品优势

Cisco IOS 防火墙特性集可以给用户带来的好处包括:

◆ **灵活性:** 一揽子解决方案可以执行路由, 提供安全的 Internet 连接, 在每用户和每应用的基础上, 根据一个用户定义的政策, 针对每一个接口采用不同的安全特性。

◆ **投资保护:** 将防火墙功能特性集成进一个多协议路由器, 可以利用现有的路由器投资。路由器通常被部署用于分离敏感的网络区段和管理专用/公共网络接口, 增量变化可以节省与学习新平台相关的成本和管理培训。

◆ **更加容易的管理:** 通过利用远程管理功能, 网络管理员可以从网络上的一个中央控制台实现安全特性。

◆ **无缝的互操作性:** 与其他 Cisco IOS 软件特性一起使用, 优化广域网使用, 提供稳健、可伸缩的路由, 并与现有的基于 Cisco IOS 的网络互操作。

新特性概览

Cisco IOS 安全服务包括一系列特性, 能使管理人员将一台 Cisco 路由器配置为一个防火墙。Cisco IOS 防火墙特性集给现有的 Cisco IOS 安全解决方案增加了更大的深度和灵活性, 给可能已经作为防火墙运行的路由器带来新增的灵活性和保护。

◆ **基于上下文的访问控制 (CBAC)** 基于上下文的访问控制 (CBAC) 是 Cisco IOS 防火墙特性集显著的新增特性。CBAC 技术的重要性在于, 它第一次使管理员能够将防火墙智能实现为一个集成化单框解决方案的一部分。现在, 紧密安

全的网络不仅允许今天的应用通信, 而且为未来先进的应用 (例如多媒体和电视会议) 做好了准备。CBAC 通过严格审查源和目的地址, 增强了使用众所周知端口 (例如 ftp 和电子邮件通信) 的 TCP 和 UDP 应用程序的安全。

◆ **Java 阻断** 随着大量 Java 小程序应用于 Internet, 保护网络免受恶意小程序的攻击已经成为网络管理人员的一个主要课题。该功能可以配置 Java 阻断来过滤或完全拒绝对没有嵌入在一个文档或压缩文件中的 Java 小程序的访问。

◆ **Denial of Service (服务拒绝) 检测/预防** 新近增强的服务拒绝检测和预防针对 syn 泛滥、端口扫描和包注入提供网络防御。服务拒绝检测和预防检查 TCP 连接中的包顺序号, 如果这些号码不在预期的范围内, 路由器将撤消可疑的包。当路由器检测出新建, 它就发出一条告警信息。它还能撤消半开的 TCP 连接状态表, 以防止系统资源耗尽。

◆ **审计踪迹** 增强的审计跟踪利用系统日志跟踪所有事务; 记录时间印迹、源主机、目的主机、端口、持续时间和传输的总字节数。

◆ **实时告警** 一旦查出可疑的活动, 实时告警将向中央管理控制台发送系统日志错误信息。网络管理人员有能力立即对入侵作出反应。

◆ **支持 ConfigMaker** 通过使用支持 ConfigMaker (一种基于 Windows 95/NT 向导的网络配置工具, 能使您将网络上支持的任何路由器配置为一个防火墙)。Cisco IOS 防火墙特性集非常容易安装。ConfigMaker 是现有 Cisco 命令行接口工具的一个配置替换。它指导分销商和网络管理员完成网络设计及路由器安装过程。ConfigMaker 允许从一台单一 PC 配置整个路由器网络, 而不是每一个路由器以独立的设备方式配置。

编辑部点评:

Cisco IOS 防火墙特性集通过在网络基础机构本身内提供访问目录政策加强, 完善了 Cisco 的端到端安全产品, 从而实现了独立设备不能提供的灵活性和控制水准。

Cisco IOS 防火墙特性集是三个 Cisco 防火墙解决方案之一, 这些解决方案被设计用来满足一个网络内的不同防火墙要求, 无论是专用设备 (PIX 防火墙)、基于 NT 的解决方案 (Centri 防火墙) 还是集成在网络基础机构 (Cisco IOS 防火墙特性集) 之中。ISI



国际商业机器中国有限公司

IBM Blade Center刀片服务器

如果用一个成语来形容 IBM 的 BladeCenter 刀片服务器家族, 那“两面三刀”再合适不过了。“两面”指的是 IBM 提供了 PowerPC 和 Intel 两个平台的刀片产品; “三刀”则是指 IBM 三款不同的刀片产品: Intel 平台双路刀片产品 HS20、PowerPC 平台双路刀片产品 JS20 以及 Intel 平台 4 路刀片产品 HS40。

刀片服务器高度集成了 CPU、硬盘、内存、网络接口和控制芯片, 它们并列地插在刀片服务器机箱的背板上, 共享统一的电源供应、风扇、鼠标、键盘以及显示器设备, 不仅占地空间更少, 还去掉了在机架式服务器中消耗电能的部件, 降低了系统电源的发热量。

应用领域: 在需要服务器物理整合以及大幅度节省空间的应用领域, 如电信中心、大型网络游戏运营, 刀片服务器有很好的应用前景; 另外, 高密度的刀片在石油勘探、电影数字特效等高性能运算领域也大有作为。目前, IBM BladeCenter 刀片服务器已在新疆油田、上海电信、中国工商银行、深圳无线电管理局等行业成功应用, 为各行业的发展贡献着力量。

独具匠心

当有限的地面空间使得企业捉襟见肘时, 刀片服务器不但提供了机柜式服务器的所有功能, 更带来了先进的管理功能和更低的整体拥有成本。

IBM BladeCenter 机箱采用标准 12 英寸 (7U) 的外观尺寸, 可以容纳 14 个 BladeCenter HS20 或 JS20 刀片, 或者 7 个 BladeCenter HS40 刀片, 从而在 42U 的机柜内可提供多达 168 个处理器的处理容量, 大大提升了计算能力。

IBM 刀片服务器产品允许企业将整个基础设施整合到 BladeCenter 机箱中, 也就是说, IBM 提供的任意刀片选件都可以安装到同一个机箱中, 而不论它是基于 Intel 平台并且运行 Linux 的双路刀片, 还是基于 PowerPC 平台并且运行 AIX 的刀片。

高密度管理能力成为 BladeCenter 的“利刃”。IBM BladeCenter 具有的远程部署管理器 (Remote Deployment Manager) 可以并行地为不同刀片安装相同或者不同的操作系统, 大大提高了管理的便利性, 管理员不再需要为每个刀片一次次地安装和配置系统软件; 此外, BladeCenter 带有专门的管理模块, 同时每个刀片上都内置了 ASMP 芯片, 利用 IBM Director 软件, 通过管理模块就可以直观清楚地对每个刀片的硬件状况进行检测、分析和报告, 而且是对硬件组件进行“可预测性故障分析”——使用户在“故障发生前”就得到预警



报告, 从而最大限度地保护用户的投资。

此外, BladeCenter 服务器在背部提供了一个单独用来管理的以太网接口, 方便用户对其进行直接管理。同时, 它的每一个部件如顶盖、硬盘等都可以轻易地进行拆卸。

产品链接

已经在刀片服务器领域确立起领导地位的 IBM eServer BladeCenter HS20 服务器, 采用双路 2.8GHz (最高可达 3.2GHz) 的 Intel Xeon 处理器, 内置 4 个内存插槽, 标准配备 512MB DDR 内存, 最大可支持到 8GB 的内存容量, 存储则可采用双 IDE 硬盘、双 SCSI 硬盘或外接光纤存储的方式。目前 HS20 可以搭配不同频率的 Intel Xeon 处理器。

编辑部点评:

IBM BladeCenter 刀片服务器的优势包括节省地面/机柜空间、低功耗和低热量, 以及相对于单独的机柜优化型服务器的潜在的低购买成本。通过将数十台分散在各个角落的服务器整合到一个机柜中, 刀片服务器还有助于降低管理成本和改进系统管理。大多数刀片服务器机箱都可以被添加到使用传统机柜服务器的标准机柜中。通常无需专用于刀片服务器机箱的机柜。

同时刀片服务器还具有很高的向上扩展性, 与传统的 8 路或 16 路服务器不同, 它使用“向上扩展”方案, 刀片服务器设计采用有效的“向外扩展”, 这种设计方案整合了多种结构——最常见的 3U、6U 和 7U——它们包含各种各样的刀片托架。增加新的服务器只需将新的单处理器或多处理器刀片滑入到机箱中的开放托架中, 无需进行物理安装和与各台服务器连线。

通过选件模块来提供更大规模扩展的大型机箱有助于实现性能与密度之间的平衡, 以正确使用基础架构来获得最高的利用率。如果没有这种灵活性, 刀片服务器可能出现的情况是高密度、低性能或者低密度、高性能, 不能获得需要的优势。■



华为 3Com 技术有限公司

Quidway S8500系列万兆核心路由交换机

Quidway S8500系列万兆核心交换机是由华为3Com公司自主开发的新一代高性能万兆核心路由交换机产品,可广泛应用于电子政务网核心层、校园网及教育城域网核心层、园区网和企业网核心层以及运营商IP城域网核心层、汇聚层。

产品特点

先进的体系结构

产品采用全分布式体系结构设计,采用功能强大的ASIC芯片进行高速路由查找,并通过Crossbar技术进行高速报文交换,从而大大提升了路由交换机的转发性能和扩充能力。产品革命性的解决了传统交换机流Cache精确匹配转发的致命缺陷,能够有效的抗击网络“红色代码”、“冲击波”等病毒的攻击,更加适合大规模、多业务、复杂流量访问的网络。

大容量、高密度线速交换

产品最高可提供高达1.44Tbps交换容量,857Mpps转发能力。支持各种高密度业务板和组合业务板,整机可支持高达576个千兆端口的同时线速转发,满足核心层设备大容量、高密度的要求。

强大的业务支撑能力

支持MPLS VPN业务;支持丰富的组播协议(IGMP、IGMP Snooping、PIM-SM、PIM-DM和MSDP/MBGP等);支持WebSwitch(硬件支持)、NAT(硬件支持)、内置防火墙(硬件支持)、IDS;支持POS/ATM、RPR等接口。

新一代万兆接口支持

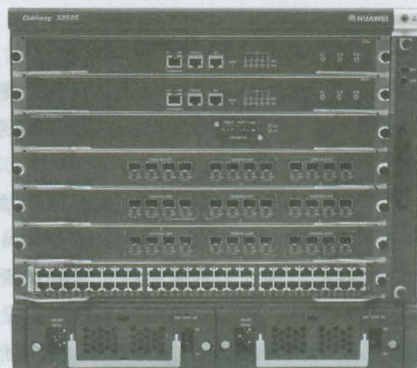
产品提供的新一代万兆以太网克服了早期万兆以太网的诸多局限,在线速转发的基础上能够提供强大的QoS保障,并支持丰富的ACL、策略路由、安全等特性。

MPLS/IPv6 分布式线速支持

产品遵循业务与性能并重的设计理念,采用功能强大的ASIC芯片实现MPLS、IPv6的分布式线速转发,能够基于高性能NP实现线速NAT、WebSwitch等增值业务,在为用户提供全面的有保障业务的同时,也做到根据需求业务可裁剪。

完善的QoS机制

产品提供了灵活的队列调度算法,可以同时基于端口和队列进行设置,支持SP、WRR、SP+WRR三种模式;支持8



个优先级队列、3个丢弃优先级;支持WRED拥塞避免算法和端口流量整形;支持带宽控制功能,流量限速的粒度为8Kbit/s,满足精品宽带网络的要求。

电信级可靠性设计

产品系统采用分布式结构,支持双主控交换板,无源背板设计,所有单板支持热插拔;电源系统交流/直流可选,采用1+1冗余热备份,并支持双路电源输入;支持STP/RSTP/MSTP协议和VRRP协议,支持以太网冗余协议,能够满足苛刻的电信级网络可靠性要求,系统可靠性达到:99.999%。

完善的安全机制

产品先进的逐包转发机制确保其在各种数据流状况下的设备安全,支持OSPF、RIP v2及BGP v4报文的明文及MD5密文认证;支持URPF(单播反向路径检查);采用802.1x方式对接入用户进行认证,支持安全的SNMPv3的网管协议;支持配置安全,对登录用户进行认证,不同级别的用户有不同的配置权限,并提供两种用户认证方式:本地认证和RADIUS认证。

编辑部点评:

Quidway S8500系列交换机基于新一代核心交换机的设计理念,具备大容量高性能、可扩展能力强和业务与性能兼具的特点。产品支持新一代高性能万兆接口,能够为城域网、园区网、数据中心提供超高速链路,构建端到端以太网,打造低成本、高性能、具有丰富业务支持能力的高性能网络。产品提供二、三层线速转发性能,内置强劲的全分布式业务处理引擎,以全线速处理二层、三层、MPLS VPN、组播等各种业务流量,提供完善的QoS保障、安全管理机制和电信级的高可靠设计,满足大型IP网络对多业务、高可靠、大容量、模块化的需求。



趋势科技网络（中国）有限公司

趋势科技网络病毒墙NVW

趋势科技网络病毒墙 Trend Micro Network VirusWall 是一个病毒疫情防御的硬件防护设备，可协助企业防治蠕虫之类的网络病毒，在爆发病毒疫情时隔绝高危险的网络脆弱环节，在网络层部署由趋势科技提供的安全防护策略，并能在缺乏防毒保护的设备等潜在感染源连接网络时予以隔离和清除。它支持趋势科技企业安全防护战略 Enterprise Protection Strategy，并且统一由趋势科技中央控管软件 Trend Micro Control Manager 来管理。

新的防毒能力

作为趋势科技“企业安全防护战略”一个新的组成部分，NVW 为趋势科技原有的防病毒解决方案带来了如下变化：

前置的防护能力：以往的防病毒产品，需要在得到真实的病毒样本之后编制相应的病毒特征码，部署到所有业务主机、客户端上，执行病毒扫描操作，才能完成安全防护功能。而 NVW 无需在业务主机、客户端上安装任何组件，它监测网络层的流量，在病毒到达目标设备之前就完成了检测和清除操作，不仅在时间上做到了大幅度的提前，由于病毒信息不会在业务主机或客户端完成重组，也大幅度地降低了这些设备的计算负载。

目标对象的改变：现有的防病毒产品基本都作用在“应用层”，工作对象为“文件”。而 NVW 作用在“网络层”，工作对象为“数据包”。工作层次和处理对象的差异，带给客户的直接收益是：现在，面对网络蠕虫病毒的疯狂进攻导致的网络瘫痪，它可以提供针对性的解决方案，平稳网络流量，提高网络基础设施的可用性。

综合的安全控制：网络蠕虫病毒攻击的对象大多和操作系统漏洞、不安全的使用习惯等相关联，在以往的网络管理实践中，这些问题的解决缺乏对应的技术性控制手段。NVW 整合了漏洞侦测和管理、病毒紧急响应等功能项目，能够有效地控制这些网络管理的老大难问题。

功能概览

NVW 可以设置在网络的 LAN 网段，实时监测网络通讯的安全防护设备，可以提供下列功能：

◆ **隔离薄弱环节** NVW 让企业能在发生攻击之前或当时，选择性地隔离可能带有特定安全漏洞的计算机（例如未安装补丁程序），防止病毒利用网络上的薄弱环节入侵。当爆发病毒疫情时，可以阻止未安装相关补丁程序的计算机再感染位



于其他网段上的计算机，避免造成网络交通拥塞。

◆ **网络疫情监测** 它使用智能型规则，提供关于网络病毒疫情的早期预警信息，以便企业采取主动、及时的安全措施。

◆ **预防网络疫情** NVW 运用 TrendLabs 所提供的及时、明确、特定的防治策略，来预防或围堵网络病毒。它可以禁止带有病毒的信息进出染毒的网络区域，以隔离与围堵病毒的散播，从而维持整体网络的正常运作。

◆ **网络扫描与侦测** 利用 TrendLabs 提供的病毒码进行扫描与侦测，并且过滤掉染毒封包，以清除在网络层散播的病毒（例如 Internet 蠕虫），并且运用防毒软件扫描潜藏在应用层（application layer）的病毒。

◆ **自动清除损害** NVW 能够找出网络上的染毒来源并在清除完成前予以隔离，以预防再次染毒。它使用 TrendLabs 提供的损害清除模板，不需透过代理程序即可从远程自动清理染毒主机，大幅降低手动清除与复原所产生的成本与管理负担。

◆ **安全策略的实施** 公司企业可实施防毒安全策略，将网络中毒或再次中毒的可能性尽可能减小。

◆ **便于使用、管理与安全控制** NVW 是部署关键性疫情防护服务的整合性防护设备，使用、配置、安装和管理均非常简便。其 SNMP 监控可加强管理与检测能力，内建的本地（local host）防火墙有助于预防对 NVW 的攻击，还可以通过 ActiveUpdate 模块和 TCM 集中管理控制台实现 NVW 的定期和自动化的代码库或程序更新。

编辑部点评：

趋势科技网络病毒墙 Trend Micro Network VirusWall 不同于只监测安全威胁或提供信息的安全解决方案，它能协助企业采取准确、快速的安全措施，并且主动侦测、预防围堵与进行善后清理。

当企业在网络的各网段之间部署 NVW 之后，即可强制实施全网一致的防毒安全策略，并且准确清除网络上的感染源，可大幅降低安全风险。一旦爆发病毒疫情，它可以隔离高危险的网络弱点，预防攻击或限制攻击发生的区域，以减少网络的宕机时间。而且，用户还可以得到来自趋势科技屡屡获奖的全球安全专家网络提供的特定病毒防治策略，这些防治策略可以方便、统一地部署到整个网络。IN

冠群电脑(中国)有限公司



eTrust Security Command Center

CA eTrust Security Command Center 是一款功能强大的解决方案, 主要用于在企业范围内管理和响应安全事件。

作为 CA 企业基础架构管理策略(EIM)的一部分, eTrust Security Command Center 通过大幅降低安全信息过载情况和巧妙地实现安全工作流程的自动化, 显著降低了企业所面临的风险, 帮助企业发现并按照重要程度对相关安全信息进行优先排序, 以确保实时管理安全风险。同时, 通过将安全风险与企业资产进行关联, 企业可以通过总控中心发现安全事件并采取正确的行动, 从而显著降低企业所面临的风险, 帮助企业确保其安全管理操作符合相关规范, 同时提高 IT 安全小组的工作效率。它可以将不同的安全解决方案集成到带有整个企业资源目录的单一安全管理平台上, 并将整个安全状况反映到基于 Web 的单一门户上, 从而便于安全管理员在需要时查看所需的信息, 及时地作出决策, 采取行动和提供适当的报告, 真正实现“洞察一切”和“管理一切”。

基于规则的关联

SCC 通过基于规则的智能关联功能来专门解决隐藏于安全事件之下的根源性问题。其开装即用的事件关联工具包括:

- ◆ 规则库, 共 100 多个默认策略可用于进行快速威胁分析。
- ◆ 通过 Web 进行自动策略更新。
- ◆ 规则模板和向导, 可用于创建自定义规则。

高级事件管理功能

这款产品为 IT 安全小组提供了高级事件管理功能, 包括:

- ◆ 安全事件分组, 允许基于公用属性来处理多个事件, 而不必修改事件库中的事件。
- ◆ 事件分配与注解, 用于监控和针对事件实施适时、适当的响应。
- ◆ 可视化增强功能, 有助于对模式和异常情况进行更为有效的调查和分析。
- ◆ 与 CA 的 Unicenter ServicePlus Service Desk 等帮助台解决方案集成, 从而实现无缝的工作流程分析。

特定任务工作空间

它以创新的特定任务工作空间 (Task-Specific Workspace) 进一步简化了安全管理, 具体包括:

- ◆ SANS Top 20 工作空间 (SANS Top 20 Workspace), 以 SANS 协会排名前 20 位的漏洞列表为基础, 关联高优先级

的安全威胁。

- ◆ 基于角色的工作空间 (Role-Based Workspace), 确保病毒控制和 DoS 防御等特定任务被分配给指定的小组成员。

与网络和系统管理的集成

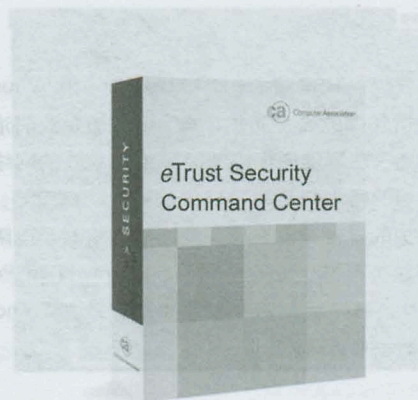
eTrust Security Command Center 与 CA 公司的“企业基础设施管理”战略保持高度一致, 它使 IT 企业能够像管理其他基础设施、应用程序和数据管理进程 (如在 Unicenter Network and Systems Management 下运行的进程) 一样, 以常用的方式来管理安全。这种集成的管理方式降低了技术的拥有成本, 并使安全策略能够跨功能区域进行扩展。例如, 管理员可以利用与网络通信异常有关的数据来更好地确定安全事件的本质。

eTrust Security Command Center 的关联规则模板、工作空间以及代理均可通过网络进行更新, 这给用户带来了极大的价值。在上传到网络之前, 这些更新都进行了测试和验证, 以确保它们的有效性。

编辑部点评:

CA eTrust Security Command Center 可实时监控和管理企业安全的各个方面——从威胁发现一直到威胁解除。它提供了一个集中化的“命令—控制”中心, 该中心以直观的图形界面来显示安全数据, 从而使 IT 安全小组能够根据事件的紧急程度和潜在的商业影响来快速确定并响应突发事件和漏洞。

通过基于安全策略管理系统构建的完整的安全体系架构, 可以提供从企业用户的管理、企业信息资产与风险管理到安全事件的处理, 从而建立起一套集成、全面的的安全管理系统, 并且变传统的“被动式”管理为“主动式”管理, 建立起对安全事件的预警机制。IN



McAfee 公司



McAfee IntruShield 2600

安全防护是一个多层次的保护机制，它既包括企业的安全策略，又包括从防火墙、防病毒到入侵防护系统(IPS)的技术解决方案。其中，IPS 是一个不可或缺的保护层，它既能防止员工违反企业的安全策略，又能够有效地检测来自外部的威胁，例如潜在的Slammer蠕虫或拒绝服务(DoS)攻击。

McAfee IntruShield 2600就是这样一款特别的产品。它不仅能够提供实时的入侵检测和预防功能，而且拥有成本也相对较低，并以其特建的专用设备、高度准确的检测功能、千兆位速度的检测性能以及基于Web的管理功能为许多大企业遍布全球的区域办事处和分支机构提供了强大的入侵检测功能。

产品特性

IntruShield 2600配置了8个端口，在SPAN (Switched Port Analysis) 模式工作时，全部可以用作检测端口，即如果用户只需要传统的IDS功能，这款产品完全可以充当一个8口的IDS，不过在部署时需要考虑吞吐量。IntruShield 2600的拿手好戏在于对入侵和非法的数据包进行阻断，这是在In-line的模式下实现的，这个模式是把IPS作为一个以太网的桥接器，透明地连接到已有的网络中，而不需要改动原有网络的配置，对于一个复杂的网络来说，这种设计可以减轻调试安装设备对原有网络的影响。

由于需要实现实时阻断，所以IntruShield 2600在进行协议重组的过程中就需要比传统IDS更强的处理能力，但通用的硬件平台在多端口配置的情况下显然无法满足实时阻断的需求。所以，IntruShield 2600采用NP (network processor) 和ASIC(专用集成电路)混合的架构设计，因而能够实现非常高的转发率，可以帮助入侵防护设备进行实时阻断。

尤其值得一提的是，这款产品的软件和硬件的配合程度是非常高的。虽然各个管理服务器上都需要安装多个服务程序，但是McAfee通过把这些服务打包，整合成安装向导提供了用户。我们只需要点击几次“下一步”，并且设置好管理端口的IP地址，就能够完成安装。

功能概览

◆ **实时入侵检测** 该产品具有特建的专用设备、高度准确的检测功能、千兆位速度的检测性能以及基于Web的管理功能，多种检测方法层层把关，加上其广泛的攻击检测范围，使得各种已知或未知的攻击都很难触及到用户的网络。



◆ **灵活、可扩展的部署** IntruShield产品能够在多种模式之间轻松切换，举例来说，IT人员在一开始可以将该设备部署为SPAN模式，一段时间后，为了降低误报率并节省带宽资源，他们就可以将设备模式切换为嵌入模式。由于IntruShield具有多个端口，因此同一个传感器可以同时监控多个网段。

◆ **简化的IDS管理** IntruShield产品提供了非常直观的图形化界面。IntruShield Global Manager可以说是简易性和强大功能的完美融合体，“简易”体现在可以全天候掌控全球网络的运行状况，而“强大”则体现在一些资深安全专家可以通过它来深入分析某些可疑的攻击。此外，其智能警报查看器(Intelligent Alert Viewer)还提供了实时的威胁分析功能，用户只需单击鼠标，即可查看有关某个威胁的详细信息。

◆ **高投资回报率** IntruShield系列产品不仅降低IDS系统的总拥有成本，对公司业务也起到了积极的促进作用。平均来说，企业无论在新的环境还是在传统环境下部署IntruShield的专用IDS设备，都可以在三年内实现145%的投资回报率。此外，攻击严重性的降低也有效地消除了某些方面的成本。通过积极预防来保持业务的持续性，这同时也具有显著的组织效益。就这一点来说，IntruShield广泛的攻击检测范围以及极低的误报率都成为了无可比拟的绝对优势。IntruShield产品通过单一的平台提供了全面的入侵检测和预防功能，其卓越的灵活性、高水平的可用性和扩展性都能够为用户带来极大的价值。

编辑部点评：

McAfee IntruShield网络安全产品采用先进的实时网络入侵检测和防护体系，能有效地保护企业和政府的网络。IntruShield独特的体系结构集成了多项专利技术，包括特征检测、异常检测和拒绝服务分析技术，从而能在几千兆的网络流量下进行准确和智能的检测和防护，使企业免遭已知攻击、首次发生的未知攻击以及DoS攻击的影响。

而且，具有良好可扩展性的IntruShield方案可以为企业提供更综合的防护体系，它可以跨越企业核心网络、企业边界网络以及分支机构的网络，无论是对于带宽几十兆还是2G的网络来说，它都具有极高的性价比。■

浪潮北京电子信息产业有限公司

浪潮英信 NF280 服务器



浪潮英信 NF280 是一款全新的、超稳定的 2U 双路机架式服务器，是浪潮新一代商用服务器家族中的新成员。这款服务器采用了浪潮专有的工业设计方法如无线缆工业设计、定向风导技术等，特别适用于对稳定性有特殊要求的用户。

层层把关 确保超强稳定性

浪潮英信 NF280 采用了先进的内存热备和内存镜像，可以有效避免由于内存故障而导致数据丢失或系统宕机。NF280 不仅支持一般的 ECC 内存容错技术，实现数据的实时容错，同时采用了业内领先的内存热备和内存镜像技术（用户可选），能够实时对内存中的数据进行热备份，在服务器的运行过程中，一旦有内存出现故障，用作镜像或热备的内存即可迅速工作，接管系统运算的任务，彻底杜绝了因内存故障而导致的数据丢失或系统宕机。

在关键部件上 NF280 采用了全面冗余技术。NF280 采用了 1+1 冗余电源，在电源出现故障的时候能够自动实现电源切换，避免电源问题而导致的系统故障。

浪潮 NF280 的超强稳定还源于浪潮独有的设计和生产技术。众所周知，系统过热是影响服务器稳定性的最主要原因，对于机架式服务器来说，由于空间的限制，散热问题的挑战更大。浪潮 NF280 在散热设计上采用了独有的无线缆设计和散热技术，保证了服务器在恶劣环境下长时间满负荷运转的温度正常。

先进技术造就高性能与高可扩展性

浪潮英信 NF280 采用了支持 64 位扩展技术的新至强处理器，集成 1M 的二级缓存和 800MHz 的前端总线，大容量缓存极大地提升了处理器的数据处理能力，高频率的前端总线则提供高速数据传输能力，使服务器的效能得到最大限度的发挥。同时，浪潮 NF280 也支持先进的 PCI-E 总线技术，完全消除了总线带宽不足给系统性能提升带来的瓶颈。此外，NF280 还集成了双千兆网卡，确保服务器具有高速稳定的网络性能。

高可扩展性是浪潮英信 NF280 的另一大特色，NF280 采用了以一扩二的先进技术，增加一个与主板垂直的固定卡，采用“背靠背”的崭新方式扩充了两个扩展板，不仅能够提高内部空间利用率，同时保证了用户扩展后系统仍然能够保证良好的散热表现。NF280 在狭小的 2U 空间内配置了 6 个 PCI 扩展槽，这些扩展槽不仅支持主流的 PCI-X 设备，也支持新一代的 PCI-E 串行扩展接口，此外插卡同时支持标准尺寸和非标准尺寸的扩展卡，这为用户提供了充分的选择空间，在满

足需求的同时有效保护了投资。

NF280 配备 6 个内存插槽，内存容量最大可扩至 24GB，为数据库应用等大规模数据处理提供了足够的内存空间。NF280 提供了 8 个硬盘槽位，用户可以选择 SATA 或 SCSI 硬盘，以满足不同应用和不同资金约束下的不同需求；在 8 个硬盘槽位之外，NF280 还集成了 SCSI 接口，可以接入不同的磁盘阵列，为用户提供了足够的存储空间。

人性化设计、软硬一体打造高可管理性

在强大的性能和可扩展性之外，NF280 还拥有良好的可管理性。NF280 还配备了系统快速定位指示灯，管理员可以让用户在众多的设备中快速找到相应的服务器系统，极大地提高服务器管理效率。

NF280 的机箱采用完全独具特色免螺丝设计，用户可以不借助任何工具就可以将机箱打开，另外，机箱上盖分成两部分，可以从机箱中部向两端打开。

而在软件方面，NF280 配备了浪潮的蓝海豚安装导航软件和猎鹰管理软件。通过安装导航软件，管理员无需特殊经验即可轻松完成软件的安装；而猎鹰管理软件则可以实现跨平台操作、远程监控、实时报警等多种管理功能，帮助管理员提高系统管理效率和系统的安全性。

编辑部点评：

NF280 采用了内存热备/内存镜像等技术，很大程度上杜绝了因内存错误等原因导致的宕机和数据丢失问题，再配合硬盘、风扇、电源等关键部件热插拔冗余设计，更是让 NF280 在稳定性和保证数据安全方面具有出类拔萃的表现。

除了超强的稳定性之外，NF280 所采用的新至强处理器、PCI-E 等业内诸多先进技术，保证了它性能的强大、良好的可扩展性。另外，人性化的设计结合浪潮独有的“蓝海豚”智能导航软件和“猎鹰”管理软件，NF280 在可管理性方面也具有突出的表现。作为机架式部门级服务器的典范，浪潮英信 NF280 在电信增值、政府、高教等行业的 Web、OA、数据库、视频点播等关键应用领域有着广泛的市场空间。■

华硕电脑公司



GigaX3112系列三层千兆交换机

GigaX 3112 三层网管型高速以太网交换机具有 12 个 10/100/1000 BASE-T 连接端口及 2 组 10/100/1000 BASE-T 连接端口与备用的光纤插孔, 每个连接端口的传输速率都能达到线速的要求, 并通过储存转发的交换模式及流量控制, 防止封包流失, 提供良好的传输效能。最多可以记录 16000 个 MAC 地址, 并支持 STP 通讯协议, 加强网络传输的能力。具有双 Flash ROM 的设计, 可以预防更新固件不及时造成的损害。在第三层路由功能部分, GigaX 3112 支持 DHCP、DHCP Server、TFTP 固件更新功能、静态路由通讯协议、RIP/RIPv2、Inter VLAN Routing。此外, GigaX 3112 还提供了完备的传输控制和灵活的系统管理; 在硬件方面, 它可支持 RPS 备用电源系统, 机壳后方另有可更抽换式的散热风扇, 能够减少等待维修的时间。

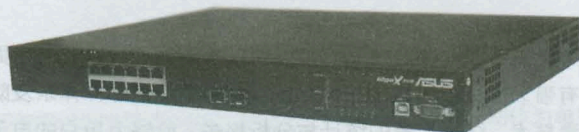
关键特性

GigaX 3112 系列三层千兆交换机为企业提供了性价比极高的三层交换机, 对管理和网络协议的广泛支持, 为用户提供极高投资回报率; 另外, GigaX 3112 配有华硕独有的 RPS 冗余电源和 USB/RS232 控制端口及 Web 式管理界面设计为用户提供在稳定性、可管理性、完全性方面俱佳的选择。

- ◆ 提供 12 端口自动侦测 (Auto-Sensing) 10/100Base-TX 端口和 2 组 mini GBIC, 具备 Auto MDI/MDIX 功能, 可自动侦测直连网线或交叉网线。
- ◆ 提供可置换的风扇设计 (Swappable Fans Module)。
- ◆ 提供 RS232 及 USB 双控制端口, 提供更方便的网络系统管理。
- ◆ 提供备用电源系统 (Redundant Power System)。
- ◆ 支持参数设定文件备份与回存 (Backup & Restore)。
- ◆ 提供 ANWM (ASUS Network Web Management) 图形接口 (GUI) 网管软件, 仿真前端面板设计可实时监控每个端口的状况并监控网络状态。

产品规格

- ◆ 支持 16,000 (含) 以上 MAC 地址
- ◆ 4096 路由
- ◆ 提供 24 Gbps 的背板频宽, 支持线速 (Wire Speed) 交换能力, 交换速度可达 18Mpps。
- ◆ 支持 Auto-sensing。
- ◆ 大型封包最高可支持 9216 byte。



- ◆ 具备广播流量控制以避免广播风暴产生。
- ◆ 最高可支持到 4094 组的虚拟局域网设定 (VLAN)。
- ◆ 支持 IEEE 802.1d Spanning Tree 功能及 802.1w Rapid Spanning Tree 功能。
- ◆ 具备 IEEE 802.3ad Link Aggregation 汇集链路能力。
- ◆ 具备 IGMP snooping 的功能。
- ◆ 支持 IEEE 802.1p 八种不同 CoS (Class of Service) 分类, 8 个硬件优先权队列 (priority queues)。
- ◆ 能阻隔 (Blocking) 不良的应用程序, 增加网络频宽。
- ◆ 提供多种型态的管理接口, 适合各种管理人员与管理环境。Console Port (CLI、Telnet) 与 Web Based 图形管理接口等, ANWM (ASUS Network Web Management) 图形接口 (GUI) 网管软件, 为仿真前端面板设计, 可实时监控每个端口的状况并监控网络状态。

编辑部点评: 华硕 GigaX3112 12+2 GBIC 端口三层网管型高速以太网交换机具有 12 个 10/100/1000M 的 MDI/MDI 交换端口, 2 个用于 1000Base-LX 和 1000Base-SX 的 SFP 插槽, 用于对下层级联交换机 GigaX204/2048 或 GigaX1024p 和服务器的千兆接入, 消除网络主干的带宽瓶颈; 依据距离和实际需求, 可灵活选择是光纤接入和铜缆接入; 24G 的背板带宽、32Mpps 的包转发速率保证数据快速无阻塞的转发。

GigaX3112 三层交换机支持 4096 组 VLAN, 同时如果网络内部划分了 VLAN, 可通过三层交换机实现不同 VLAN 间的通讯, 一次路由、多次转发的三层交换性能保证 VLAN 间的高速数据通讯; 支持静态路由和 RIP1/RIP2 (后续 firmware upgrade 会支持 OSPF), 可有效实现与其他三层交换机或路由器之间的路由处理能力。

GigaX3112 三层交换机还具备 L2-L4 层的安全过滤能力, 用于对网络流量进行安全控制; 8 个优先级排队的 QoS, 实现对不同网络应用的优先级排队服务; 支持 IGMP Snooping, 有效支持组播能力。

同时, GigaX3112 三层交换机具备完善的二层交换性能, 支持 802.1w (快速生成树)、802.1ad (链路捆绑)、802.1q (虚网划分)、802.1p (COS) 等, 可满足用户网络架构及网络功能的不同需求。IN

美讯智软件科技有限公司

邮件安全信息网关RiskFilter/SMG



美讯智RiskFilter/SMG邮件安全信息网关在内容判断方面具有强大适应性的推理技术, 多层面的防垃圾邮件体系及防病毒技术, 结合大量的统计与分析报告, 能够为用户的电子邮件系统提供全方位的保护。

该产品基于美讯智 Linux 优化内核和专利的信息处理技术, 提供对信息内容高速扫描处理; 集成 SurfControl ASA 和美讯智垃圾邮件过滤引擎, 能够准确过滤垃圾邮件和提供完善的用户管理机制; 集成世界领先的企业级杀毒引擎, 高效查杀邮件病毒; 灵活定义内容过滤规则, 过滤策略模板提供敏感内容过滤手段; 提供MTA保护的邮件防火墙, 抵御对邮件服务器的各种攻击; 详尽易用的统计报表信息。

产品特性

◆ **高准确率和低误报率** 具有强力垃圾邮件过滤系统, 识别垃圾邮件的准确率最高可达98%, 基于内容的垃圾邮件过滤技术极大地降低了误报率。

◆ **简易轻松的管理维护** RiskFilter/SMG的垃圾、病毒邮件过滤策略库全球自动更新, 实施后基本不需要人工管理。独特的策略管理模块为用户提供7种过滤器模板以及7种过滤器触发操作, 有效减少了管理员的日常维护时间, 降低了他们的工作负荷。

◆ **个人垃圾邮件管理** 允许邮箱用户登录网关, 查询并处理自己收到的垃圾邮件。用户可根据实际需求, 定制用户发件人邮件地址白名单和黑名单。系统每天自动产生垃圾邮件摘要邮件, 用户在摘要邮件中可直接处理垃圾邮件, 彻底解决了误报问题。

◆ **内容辞典** 通过内建可定制的预定义关键字辞典, 它提供了高品质的内容过滤, 为您减少管理时间, 节约成本。该辞典包含英语、法语、日语、简体中文和繁体中文等10个版本的关键词, 所有关键词被划分为16类, 涵盖了从成人、垃圾邮件、金融到医疗保健等几乎所有方面的内容。

◆ **表达式匹配** 采用高级布尔逻辑语言来构建精确的词汇匹配规则。使用逻辑运算符“AND”(与)、“OR”(或)、“NOT”(非)、“OCCUR”(出现)以及通配符和其他的字母数字形式组成复杂的表达式, 提供更为精确的反垃圾邮件和内容过滤效果。

◆ **完善的防攻击体系** 全面防范针对传输层25端口攻击, 防止邮件地址泄露, 保障后端邮件系统的安全。

◆ **完善的统计分析功能** 该产品可以通过直观的图表及多种查询方式显示邮件网关和后端的实时状态, 邮件系统所



遭受的各类攻击的状况以及流经网关的所有邮件、垃圾邮件、病毒邮件以及含有不适当信息邮件的收发状况, 帮助用户全面了解应用状况, 并相应调整过滤策略。

◆ **真正的电信级产品** 专业优化的SMG分布式系统为用户提供超大容量邮件的转发和处理。基于专有的MessagePro信息处理平台, 该产品可以为电信用户提供高速、稳定、可靠、可扩展的处理性能。

功能模块

◆ **内容过滤模块** 它基于Unicode码元流的内容扫描技术——Unicode码元匹配, 实现敏感内容的精确过滤, 内建了反病毒过滤器、反垃圾邮件过滤器、常规内容过滤器、高级内容过滤器、附件过滤器、多级过滤器以及免责声明过滤器等七种过滤器模板, 能够满足企业的不同需求。

◆ **反病毒模块(AVA)** 由全球知名杀毒厂商McAfee提供网关级病毒扫描引擎, 该产品依靠先进的病毒扫描技术检测所有邮件, 并且可以根据每个公司定制的规则来处理邮件, 决定对病毒邮件进行清理、删除、隔离或是其他操作。它支持病毒扫描引擎和病毒代码库的实时在线更新, 可以及时遏制新病毒的发作。

◆ **防攻击模块** 美讯智提供完善的防攻击体系, 有效地防范针对邮件系统的各类攻击, 包括字典算法攻击、目录树攻击、多线程攻击、DHA攻击、空文件攻击、多重病毒感染攻击以及多重压缩攻击等。

编辑部点评:

美讯智科技的邮件信息安全网关RiskFilter/SMG基于本土研发, 具有配置灵活、功能丰富、可扩展性强等特点, 支持独立安装和集成安装两种模式, 可以被应用到任何网络环境中, 以满足来自信息安全市场的多种需求。

美讯智内容安全产品包括邮件信息安全网关(RiskFilter/SMG)、网页过滤系统(SWF)和即时通信过滤系统(P2P), 能够有效阻挡不受欢迎的内容和阻止关键数据泄漏, 为电信运营、政府机关、教育、保险、安全、金融、电力、税务、证券等用户提供了内容安全的整体解决方案。■

负载均衡设备将大显身手

■ 国堡电子科技技术总监 朱敏

企业与政府机构可以说愈来愈依赖因特网，然而影响因特网的因素太多，因此使用因特网时常不能尽如人意。

早先提供网络服务的企业面对昂贵的专线，常常望而却步，因此转而考虑主机托管或将机器设备放置于IDC。随着企业网络用量增加，企业发现这样做的成本越来越高，又考虑将机器设备搬回自建机房运营。企业自建机房的好处是能节省每月必须支付的机柜，以及IT人员往返于公司与DC的交通费用和时间。由于网络使用的需求增加，企业自建机房愈来愈多，也使得网络负载均衡设备的需求增加。

此外，随着因特网需求增加，无论是Web服务器、防火墙或VPN设备，都需要留意主机效能问题。如果原来的主机效能不足，许多企业与政府机构会考虑更换新主机来解决效能不足的困境，在添购新主机时，也会预测未来的整体需求。但是如此一来就会造成原有旧设备的投资浪费。此外，新旧设备更换时，必然会有旧机器停机与新机上线的问题，因此，中断服务时间也就成为企业与机关的负担与成本（中断服务造成的营业损失与信誉等等）。

服务器、防火墙以及VPN负载均衡设备能解决添加设备及备份问题，一方面能使企业原有的设备继续运作，不至于造成原有设备的投资浪费；另一方面也能在不停机的前提之下，增加更新、效能更好的设备来提供高可靠的服务。

笔者将针对网络负载均衡设备、服务器负载均衡设备、防火墙负载均衡设备以及VPN负载均衡设备的发展趋势加以探讨。

网络负载均衡设备

随着ADSL的普及，企业自建机房的可能性越来越大。ADSL的费用远较专线便宜，因此如果能同时申请多条ADSL加以使用，总带宽不但效果与一条专线相差无几，费用反而降低不少，而且线路之间能够互为备份。万一某一条ADSL线路断线，其它ADSL仍然可以继续提供服务，不会像只有一条专线时，如果专线因意外中断，服务立刻遭受影响，造成公司营运以及信誉上的严重损失。

企业使用多条ADSL时，会希望ADSL能并联起来使用，而

服务器、防火墙以及VPN负载均衡设备能解决添加设备及备份问题，一方面不至于造成原有设备的投资浪费；另一方面也能在不停机的前提之下，增加更新、效能更好的设备来提供高可靠的服务。

非各条线路分别作为单独用途。网络对于网络负载均衡设备（Network Load Balancer）的需求愈来愈高，因此无论是企业对外

联机的对外负载均衡（Outbound Load Balance），或是企业本身构建主机提供网友各种服务的对内负载均衡（Inbound Load Balance），都成为企业急需寻求的解决方案。

企业国际化的影响，连带造成VPN需求增加，尤其许多企业构建VPN需要在不同的地点之间传送公司内部的ERP数据以及语音甚至于视频等等，网络流量负载增加，网络负载均衡设备因此更担负起稳定流量的重任；其次，公司内部的信息种类已多样化，因此企业也开始要求网络设备能提供QoS。

但是，部份设备厂商标榜的QoS，其实只能做到切割不同的带宽给不同的网络服务，也就是“各走各”的形式，基本上来说，并不算真正的QoS。另外，有些产品声称除了切割带宽之外，高优先权的服务在低优先权带宽空闲时，能以“借用”的方式，增加可用带宽，也强调这种方式是QoS。

其实，真正的QoS除了需要兼具以上两种功能之外，还需要能透过分级方式（Classification）来达到高优先权能插队先走的原则。举例来说，如果企业或机关目前有人正在使用FTP程序大量下载数据，造成下载带宽被占用时，如果VoIP的优先权高于FTP，那么一旦VoIP封包出现时，应该能优先比FTP封包先传送。这样才能提供优先权分级的功能，让最需要而且最迫切的服务，能实时或快速传送。

服务器负载均衡设备

许多企业与机关已经发现单一部服务器（包括Web服务器、应用服务器、数据库服务器等等）已经无法满足众多网友的需求。此外，许多企业与机关会希望提供7×24的服务。但服务器是由各种软硬件组成，难免会发生故障。因此规划上会倾向提供两部或两部以上的主机同时提供服务（Active-Active），或一部或多部作为备份服务（Active-Stand-by）。

基于这一类的需求，服务器负载均衡设备应运而生。该设备不但要能提供Active-Active服务，而且要能让不同平台（Windows、Linux、Unix）与不同规格的主机同时运作。

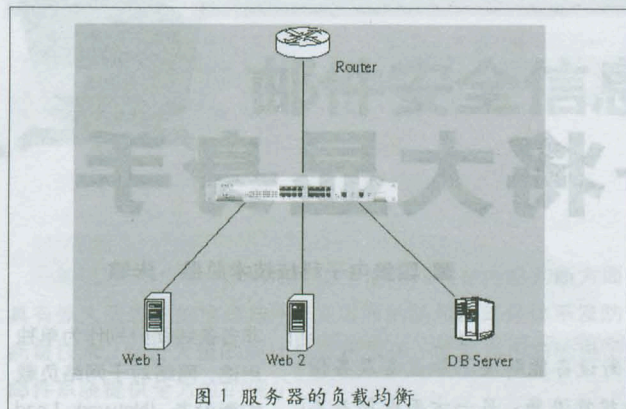


图1 服务器的负载均衡

防火墙负载均衡设备

许多企业发现防火墙是可能发生单点故障的所在,因此需要避免因防火墙故障而影响整体营运。还有企业则发现它们对外的网络流量急剧增加,防火墙的 Throughput 可能即将不够使用。接下来的问题是是否有方法可以让多个防火墙并联。防火墙负载均衡设备提供了解决之道,不但可以应付目前的需要,而且可以加以扩充,并联,提供 Active-Active 架构。但某些厂商提供的防火墙负载均衡设备只能有一部防火墙作为主机运作,其它防火墙作为备份,这样的设计会造成设备的浪费,而且无法解决 Throughput 过高的问题。

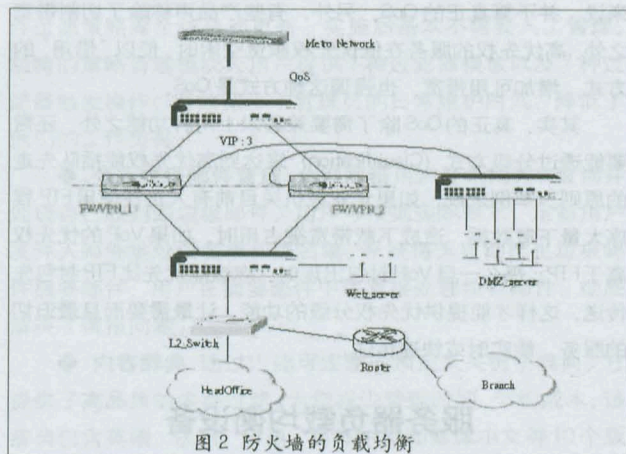


图2 防火墙的负载均衡

防火墙负载均衡设备应该能提供多台并联、Active-Active 的功能,最重要的是能保证不断线或在很少的断线时间内,就能快速增加防火墙主机数量。另外一项考虑要素是:防火墙负载均衡应该考虑到 DMZ 区的负载均衡问题。

VPN 负载均衡设备

VPN (Virtual Private Network) 已经开始普及,点对点专线

不再是企业或机关惟一的选择,好处当然是价格大幅降价,让整体网络存取成本最优化。随着 VPN 大行其道,许多企业总公司或机关的总部,由于连接太多分公司或分支机构,导致 VPN gateway 负荷太大,必须进行负载均衡工作。许多设备厂商开始推出 VPN 负载均衡设备。但是有的 VPN 负载均衡设备出现了这样的问题:总部内多部 VPN gateway 往往会出现 gateway A 与分公司的 VPN gateway 建立 VPN 通道,但是负载均衡设备却在封包传送时,发现 gateway B 负荷较轻,居然将封包送往 gateway B 而造成 VPN 联机失败。这种情况将随着总公司的 VPN gateway 数量增加而恶化,总公司如果有两部 VPN gateway,联机失败的机会是二分之一;但是总公司如果有四部 VPN gateway,联机失败的机会将高达四分之三。目前只有少数厂商推出的设备能解决 VPN 负载均衡这一类的难题。

目前已经开始出现防火墙与 VPN 两用的负载均衡设备,此外许多防火墙厂商也开始推出内建 VPN 功能的防火墙设备。有了防火墙与 VPN 两用的负载均衡设备,不但能减少设备投资,而且更能简化管理作业。

负载均衡设备选购指南

其实,企业在考虑购置负载均衡设备时,首先应该评估设备的稳定度,毕竟网络负载均衡设备关乎企业对外与对内联机,一旦此类设备发生故障,将造成严重后果。如果企业资金充裕,建议同时购买两部相同设备,一部提供服务 (Active),另外一部作为备援 (Stand-by)。不过有些厂商提供此类解决方案时,可能会要求收取两部设备加上 Active/Stand-by 设定的费用。

如果企业因经费问题,或是短期内不考虑双设备架构时,应多加考虑设备稳定性问题。网络负载均衡设备不建议采用硬盘之类机械材料。此外,电源供应器与散热风扇应有两组,一组接市电,另一组连接 UPS。

负载均衡设备有可能需要更新软件,由于网络下载或厂商提供的光盘可能会因为下载、运送或操作等因素,造成更新时发生错误,导致设备故障,无法提供服务。因此,内建两组 ROM 就能避免这种问题。如果一组 ROM 在更新 Flash 时失败,还有另外一组可以维持运作,不至于影响网络服务。无论是单独使用或两部互为备份方式,一旦发生故障时,会出现服务中断时间 (Interval),较好的方案是采用旁通机制 (By-pass)。也就是说一旦网络负载均衡设备故障或断电时,网络负载均衡设备形同透明不存在,对外或对内联机可以预设一条专线或 ADSL,提供有限度的网络服务,避免企业对内或对外全部瘫痪。

此外,许多负载均衡设备由于技术性高,培训不易,使得公司的运营成本增加。企业在考虑这一类设备之际,应考虑便于操作的产品。目前有的产品已经推出 GUI 操作方式,甚至可以通过 HTTP 或 HTTPS 完成设定与变更,不再需要复杂的命令才能完成。■

拿什么拯救 RAID?

■ 北京维尔码科技发展有限公司副总经理 吴韦霖

存储系统的核心 支柱

RAID 是由美国加州大学 Berkeley 分校教授 David A. Patterson 于 1988 年正式

提出的,早在 1984 年就已经出现在他的论文中了,作为 Redundant Array of Inexpensive Disks 的缩写,意思是“廉价冗余磁盘阵列”,开发的目的是替代当时数据中心系统普遍采用的价格昂贵的 SLEDs (Single Large Expensive Disks) 磁盘。作为高性能的存储系统,RAID 得到越来越广泛的应用,开始进入企业级市场,RAID 中的字母 I 被理解为 Independent,翻译过来就是“独立冗余磁盘阵列”,简称为“磁盘阵列”。

RAID 技术经过不断的发展,现在已经具有非常成熟的技术体系,发展了从 RAID 0 到 7 八种基本级别,还有一些基本 RAID 级别的组合形式,如 RAID 10 (RAID 0 与 RAID 1 的组合)、RAID 50 (RAID 0 与 RAID 5 的组合)等,成为存储的基本要素,是从服务器的内部存储到外部独立存储系统整个存储领域的核心支柱之一。

简单地说,RAID 就是一种把多块独立的硬盘(物理硬盘)按不同方式组合起来的一个硬盘组(逻辑硬盘),提供比单个硬盘更高的存储性能和数据冗余的技术,既保证了存取数据的快捷方便和管理客户端的简捷,也解决了存储海量数据的问题,同时提供了容错性(Fault Tolerant)。它可以在不须停机的情况下自动检测故障硬盘,进行硬盘替换,还可以扩充硬盘容量,重建故障硬盘上的数据。

RAID 仍有隐忧

本来,RAID 的核心价值就在于提供了最基本的阵列功能以及基本的基础架构可靠性,数据冗余的功能就是在用户数据一旦发生损坏后,利用冗余信息可以使损坏数据得以恢复,从而保障了用户数据的安全性。然而这也是一把“双刃剑”,随着企业应用和存储管理重要性的突出,用户的关注点转移了,渠道和厂商的价值点也随之转移。用户关心所用数据的可用性和可靠性,无非是对几种 RAID 级别的选择,厂商和集成商因此把主要精力都放在了存储的管理和产品上。RAID 技

RAID 技术已经非常成熟,但 RAID 并非完美无缺。万一 RAID 发生问题而威胁到了存储在其中的数据,最重要的就是找到专业的恢复方法。

术的成熟逐渐导致厂商以及用户对存储安全的淡漠和麻木,在这种淡漠中存在着相当大的数据安全隐

患。首先,RAID 系列确实存在一些遗憾,譬如现在最常用的 RAID 5,在一块硬盘发生故障后,RAID 组从 ONLINE 变为 DEGRADED 方式,I/O 读写不受影响,直到故障盘恢复。但如果在 DEGRADED 状态下,又有第二块盘故障,整个 RAID 组的数据将丢失。RAID 0 代表了所有 RAID 级别中最高存储性能,但它不提供数据冗余,可靠性最差,一旦损坏,数据将无法得到恢复。其次,正如一些业内人士所言,RAID 技术在实验室里的成熟并不代表真正应用的成熟,实施到用户身上,仍旧是麻烦不断。譬如突然断电、重新配置 RAID 阵列,都可能造成 RAID 磁盘阵列卡信息的丢失;用户的错误操作(如误删除、误格式化、误分区、误克隆、病毒损坏等)都会导致数据的丢失。一旦 RAID 阵列出现故障,硬件服务商只能给客户重新初始化或者 REBUILD,这样客户数据就会无法挽回,工作就无法正常地进行。

对用户而言,迫在眉睫的事情并不是怀疑 RAID 的技术与性能,最要紧的是拿什么去拯救存储在 RAID 上的数据。RAID 发生故障后,首先,不要对 RAID 进行任何操作,然后咨询一些技术过硬、修复率高的数据修复公司,或是登陆相关网站。例如,北京维尔码科技发展有限公司投资的“飞客数据恢复中心”(网站:www.fix.com.cn)就是在 RAID 修复方面具备丰富实战经验和娴熟操作技术的公司,创造过一次次 RAID 故障解决的经典案例。不久前,北京某著名公司的一台服务器,不知为何突然无法启动,数据无法读取。该服务器采用的是 RAID 5 的工作方式。飞客数据恢复中心的工程师根据陈述初步判断是 RAID 信息丢失的问题。这是一个由五块 75G 硬盘组成的阵列,分别对每块硬盘进行镜像,不在原盘进行操作,避免造成二次破坏。通过对 RAID 信息的分析确实发现其损坏,经过大量针对性的计算和对 RAID 的重组,三天后数据成功找回。

用户还可以在飞客网站了解修复 RAID 相关的注意事项,以及一些基本知识,避免因不当的操作而增加恢复数据的难度,甚至造成数据丢失。■

“IT 培训直通车”驶向全国

■ 本刊记者 仁仲

仔细阅读《网管员世界》的朋友一定会知道“IT 培训直通车”活动。它是微软 TechNet 和《网管员世界》共同打造的培训品牌,目的是向广大网络管理技术人员介绍微软企业产品的相关技术和使用技巧。经过从 2004 年 3 月到 12 月的多次培训,“IT 培训直通车”已经在京城的网管员心中打响了知名度,获得了网管员们的普遍认可,培训的内容也越来越细化、深入。

外面的世界很精彩

由于微软的总部在北京,因此我们的培训活动也首先在北京举办,北京的网管员可谓是“近水楼台先得月”。同时,我们也看到,微软的产品已经在国内得到了广泛的应用,各行各业、全国各地都有大量用户使用微软的产品。这些外地的网络管理技术人员也迫切需要了解微软产品的相关知识和技术,提高自己的技术水平,有很多人在网站上询问有关“IT 培训直通车”的事宜,并表示希望能在当地举办“IT 培训直通车”活动。北京的成功经验和外地用户的大量需求为“IT 培训直通车”走出北京,驶向全国提供了非常好的基础。



图 1 南京的听众认真听讲



图 2 杭州会场座无虚席



图 3 探讨问题

相约 2005

2004 年 12 月 7 日,在南京金陵晶元大酒店,微软 TechNet 与《网管员世界》联合举办的“IT 培训直通车”开始了在外地的第一次培训活动。我们邀请了南京当地的培训机构的微软资深技术讲师林老师授课,培训内容为“Windows Server 2003 常见问题释疑及技术进阶”。由于在活动前期进行了充分的网上邀请和电话邀请,本次大会十分成功。这次活动的人员大部分来自网上注册,从会场气氛上看,参会人员显示了极大的热情和积极性。由于这是第一次在南京举办“IT 培训直通车”活动,大家对该活动抱有非常高的参与热情,听讲认真。此次活动的选题比较符合广大技术人员的需求,现场交互性强。在培训正式开始之前已经有很多的学员到场,并且与老师就实际工作中遇到的 Windows Server 管理问题进行沟通。会中茶歇以及会后仍有部分学员围在老师周围讨论

咨询相关内容,学习氛围十分浓烈。

继在南京成功举办“IT 培训直通车”活动之后,我们马不停蹄,又来到了杭州。12 月 9 日,在杭州大酒店,“IT 培训直通车”开始了在外地的第二次培训活动,培训内容为“Exchange Server 2003 常见问题释疑及技术进阶”。在课上,老师由浅入深的讲解和深厚的技术底蕴令大家感觉十分过瘾。大家不时提出各种问题,而老师总是能给出令人满意的回答。经过 2 个小时的培训,在后边的提问环节中,大家依然争先恐后地向老师提问,现场气氛非常热烈。可以看出,大家对今天的培训内容不仅很感兴趣,而且也掌握了相应的要点。大家在会后纷纷表示,参加本次活动很有收获,希望以后能在杭州多举办类似的活动。

虽然外地的培训活动仅有两站,但我们已经深深感受到网管员们对技术的执著和热情,他们给予了我们极大的信心。我们相信,2005 年的“IT 培训直通车”将驶向更多的城市,提供更好的内容,得到网管员们更多的支持! INI

BEA eWorld China 2004 上海盛大开幕

本刊讯 近日, BEA 公司在上海召开了主题为“前瞻科技, 架构未来”的 BEA eWorld China 2004 大会。BEA 公司创始人、董事会主席兼首席执行官庄思浩在首日的大会中发表了主题为“BEA 与 SOA: 在中国新经济环境下推动创新”的重要演讲。作为重要的合作伙伴以及成功使用 BEA 产品的企业代表, Intel、联邦快递和中国平安保险等公司的相关业务部门管理者还在大会现场就 BEA WebLogic Platform 平台的具体应用进行了详细介绍。在两天的会议期间, 现场开设了 60 余场主题演讲及行业解决方案专场以介绍和演示 BEA 的全球最新技术与应用。同时, 让人耳目一新的还有 CEO 论坛、开发者日等诸多互动交流活动的。(边)

“2004 年中国 IT 用户年会”在京召开

本刊讯 近日, “2004 年中国 IT 用户年会”隆重召开。本届年会由中国电子信息产业发展研究院 (CCID) 和中国信息化推进联盟主办, 赛迪顾问股份有限公司和《中国计算机用户》周刊承办。会上, 赛迪顾问股份有限公司发布了“2004 年度中国 IT 产品与解决方案用户满意度调查”与“中国重点行业信息化企业及中国重点行业 CIO 调查”的最终结果。Emerson、科华、华为 3Com 等企业的行业解决方案获得“2004 年度中国重点行业解决方案用户满意品牌奖”。(洪)

“清华同方杯”计算机调试员大赛圆满落幕

本刊讯 近日, 由信息产业部、劳动和社会保障部联合举办的首届“清华同方杯”计算机调试员全国职业技能大赛举行了决赛及颁奖仪式。决赛最终的优胜者分别获得劳动和社会保障部授予的“全国技术能手”、信息产业部授予的“行业技术能手”称号。(姜)

虚拟化技术打造适应性系统

本刊讯 近日, HP 企业 Unix 部门负责人 Kennedy 先生来到中国, 介绍了 HP 如何通过虚拟化技术打造适应性系统, 帮助企业实现 IT 与业务最佳同步。HP 提供部件、集成和全面虚拟化等三个层次的虚拟化解决方案, 特别是与 Integrity 动能服务器最密切相关的分区、工作负载管理、iCOD/PPU 和集群等部件虚拟化解决方案得到了进一步发展。(音)

联想万全服务器加入广东 Linux 产业联盟

本刊讯 近日, 广东省 Linux 公共技术服务中心与联想举行了签约仪式, 双方签定了共建“联合实验室”合作协议, 旨在共同推动 Linux 的应用和产业发展。同时, 联想还全面展示了支持 Linux 操作系统的联想万全 NS10000 高性能集群系统, 以及完全兼容 Linux 的银河麒麟 (Kylin) 国产服务器操作系统。(蒋)

Power.org 联盟图创新

本刊讯 近日, IBM、Bull、Novell、Red Hat、上海贝岭等 15 家知名企业共同宣布成立“Power.org”开放标准联盟。该联盟以“Power 架构”技术为基础, 重点关注芯片和系统的发展。随着视频游戏、网络设备和消费电子产品等领域的发展, 不同厂家的产品需要进行整合以提供更多新功能。按照 Power.org 成员最初的构想, 与 Power 架构技术相关的开放规格主要集中在总线架构和高量产服务器两个领域。总线架构使得不同的组件能够在相同的“单芯片系统”上协同工作, 其标准化结果将有助于不同厂商技术的整合。开放的服务器规格能够帮助其他厂家实现低价 Power 服务器的大规模生产。(力)

日立高科技开发实验室正式成立

本刊讯 近日, 日立制作所信息通信集团在北京中关村软件园正式设立了“日立高科技开发实验室”。设立该实验室的主要目的在于促进以中间件为核心的中国国内系统开发, 同时希望为中国培养一大批优秀的软件技术人才。该实验室的具体运作由“日立信息系统 (上海) 有限公司执行”。(娜)

SiteView 入编国家网络教程

本刊讯 近日, SiteView 首次出现在普通高等教育“十五”国家级规划教材中, 作为广大网管人员学习和使用的教材软件。在《网络管理与维护技术》一书中, 编者以图文并茂的形式在相关章节里详细介绍了 SiteView 网络管理软件的使用方法。(肖)

让网络更快速、更稳定、更智能

本刊讯 近日, 在 2004 年网络管理、网络优化、网络维护技术研讨会上, 思科、网络负载均衡厂商 F5、网络智能应用流量管理厂商 PACKETEER, 以及国内专注第三方专业化网络服务供应商阳光金网介绍了各自的解决方案和网络维护、优化实例。(茹)

微软存储发布策略

本刊讯 近日, 微软公司携手存储在线发布了“微软存储百科网”以及微软存储在 2005 年发展方向与市场策略。(刘)

艾崴 ZMAXdp 获得创新奖

本刊讯 近日, 艾崴 ZMAXdp 荣获 2005 年国际消费电子产品展创新奖。它是世界第一台支持双 Opteron 处理器的准系统, 并使用 nForce3 Pro 250 MCP 芯片组。(陈)

1688 元突破办公和娱乐“线”制

本刊讯 近日, 华硕宣布从 12 月 15 日起在全国范围内展开无线存储分享器 (WL-HDD2.5) 产品的促销活动, 产品售价 1688 元, 同时还赠送价值 500 元的 WL-100g 无线网卡一个。(张) ■

未雨绸缪，优化性能

江苏移动使用NetScout的nGenius解决方案来监控其DCN网络和应用系统的性能，确保网络服务。

作为江苏省内最大的移动通信运营商，江苏移动已经建立了有高度整合之商务应用的先进数据通信网络（DCN）来满足不断扩大的用户需求。这些应用系统为其移动和互联网用户提供了无缝和高质量的服务和支持。随着支持这些服务的应用系统数目的增加，确保它们的可用性和高性能也变得越来越具有挑战性。

用户需求分析

江苏移动DCN网络以南京为中心，覆盖江苏全省。要保证在这地域分布广泛、规模复杂庞大的网络上运行的关键型应用的畅通无阻，江苏移动需要采用一个统一整合的网络性能和应用管理方案，从根本上改变以往管理工作只能依靠技术人员凭经验去操作、问题出现后紧急救火、甚至面对问题束手无策的被动局面。换句话说，江苏移动网络性能管理方案的主要目的是从技术手段上保证网络和应用系统的可视性，预防问题出现，真正实现统一管理、集中监控，在管理方面实现质的飞跃，从而提高网络服务水平。具体说来，他们需要：

1) 全面深入的可视性。采集关于关键应用系统的性能信息，洞察网络和应用的活动情况，及时发现和隔离DCN网络的性能问题并迅速排除故障，从而提高DCN网络的可靠性，提高业务处理效率。

2) 实时流量监控、流量分析和历史报表的无缝整合。历史报表必须是基于Web的，无论何时何地都能存取，而且要有高度的灵活性，为不同的读者提供不同的内容。

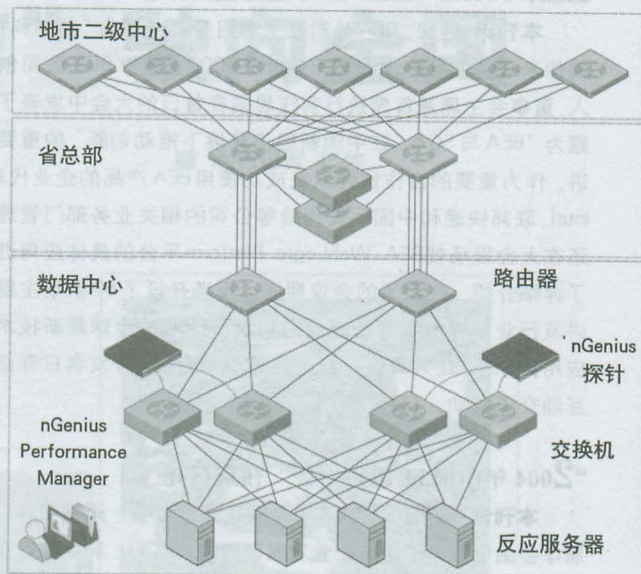
3) 提高IT工作人员的生产率。改变以往网络管理员手工操作复杂事务（如查找网络问题、数据统计等）、顾此失彼的工作方法，建立合理化的网络故障处理的工作流，从而减少出错，提高效率。

NetScout 解决方案

在此项目的第一期，江苏移动在省数据中心装置了 nGenius 硬件探针和 nGenius Performance Manager 管理软件。如图所示，在省数据中心的网捷网络交换机同多个不同的应用服务器（如BOSS业务操作支持系统）相连接。通过镜像（Span）网捷网络交换机，探针采集应用服务器流量等的信息。nGenius Performance Manager 管理软件将这些数据综合整理并加以分析。网络管理人员可以随时随地通过Web浏览器获得网络和应用的实时视图和报纸格式的历史报表。

结果和利益

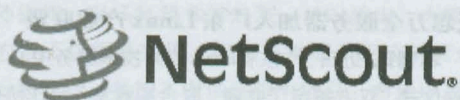
◆全面监控关键行商务应用流量，迅速发现问题并排除故障。江苏移动在网络性能管理项目的第一阶段使用nGenius重点监控其对业务至关重要的BOSS系统的流量。这个业务操作支持系统包括计费、业务流程管理、客户服务等举足轻重的应用。有了nGenius性能管理解决方案，网管人员可以对BOSS系统的流量（无论是从地市节点到省总部还是地市之间的流量）情况了如指掌。他们不但知道发生了什么情况而且还清楚为什么会出现这种情况。此外，nGenius 智能警报（Power Alarms）、阈值、和过滤等功能及时为网管经理提供告警，在影响到客户服务之前迅速隔离和解决问题。



◆列显示实时和历史性能信息，综合分析网络应用性能，优化网络资源。nGenius Performance Manager 软件中的工作台（workspace）可以将实时和历史集于一体并和主要性能指标相关联，在前后一致的环境中加以分析。这中分析的功用之一是帮助管理规划容量——在保证BOSS这样的关键应用拥有足够的带宽的同时，避免盲目升级，从而节约和优化宝贵的网络资源。

◆提高IT工作人员的效率和生产率，实现集中统一的性能管理。nGenius 解决方案为江苏移动DNC所提供的集中和易用的平台使他们整个网络和应用的性能管理手段发生了质的飞跃。网络管理员现在不仅在任何时候和地点都能获得丰富细微的整合的实时和历史的性能信息，完全摆脱了手工操作之事倍功半的工作方式，而且可以制作满足不同读者需求、能够自行定义的报表。这些报表既可以显示如每日使用量的细节也能够提供全系统范围的执行报告给有关部门领导参考。由于江苏移动IT工作人员不再需要为没有足够的性能数据而苦恼或者在出现问题时象大海捞针般地无从下手，他们现在可以集中精力，充分利用nGenius所提供的全面性能信息，积极主动地预防问题出现，完善网络和应用性能故障处理的工作流，提高效率，从而确保联网应用服务的畅通，为业务的正常运作和客户的满意作出贡献。

如想进一步了解 NetScout 公司情况，请访问 www.netscout.cn。



NetScout 北京办事处

北京市朝阳区建国路118号招商局大厦18楼

邮编：100022

电话：(86) 10 6567 5899

传真：(86) 10 6566 2728

电子邮件 bain@netscout.com

跨入 64 位之门

随着网络对人类生活影响的日益加大,作为互联网重要组成部分的服务器也不断受到应用的挑战。对于那些计算任务极其庞大的应用程序,如视频/音频/三维处理、气象/天文/物理学的数据运算、海量数据库查询等来说,要求服务器具备更好的可扩展性、更大的可寻址内存。显然,32位技术已经难以满足用户高强度应用程序对高性能服务器的需求,64位服务器应运而生。

尽管用户对64位运算有着强烈的需求,但今天的绝大部分软件仍然是32位的,而且这类软件在未来几年内还是会被广泛应用的。所以,从32位到64位计算架构,这种迁移不可能一蹴而就。

一个能提供强劲性能并同时兼容32位和64位的软硬件平台才是用户的最佳选择。



HP ProLiant ML370 G4

HP ProLiant ML370 G4: 轻松过渡

应用范围: HP ProLiant ML370 G4可以应用于多种应用环境,能充分满足工作组以及不断发展的中小企业用户的需求,为关键性的远程分支机构提供了持久的运行环境。

HP ProLiant ML370 G4工业标准服务器提供了实现64位计算所需要的技术,它大幅提升了运行和存取速度,且能够在同一平台上混合32位和64位应用,使用户可以轻松向64位计算平台过渡。

它采用2个PCI-Express插槽,提供了全新的I/O技术,能够充分满足用户发展的需求,所配备的4个PCI-X插槽还可以兼容原有设备,有效保护了用户的投资。

而且,ML370 G4还充分考虑到用户的应用特点,在许多方面做了特别的设计。管理方面,它集成了远程控制功能,让用户可以通过网络轻松访问并管理服务器;全新的锁扣设计便于开启与管理,方便访问设备组件;导轨安装方式更加快捷方便,无论是机柜型号还是塔式型号,都可以通过滑轨快速地安装到机柜上。在安全方面,它采用全新的塔式机箱前面板设计,使热插拔硬盘具有更好的安全特性。

IBM eServer OpenPower 720: 为Linux调优

应用范围: IBM OpenPower 720运行64位企业版Linux操作系统,有不错的扩展选项和升级选项,尤其适合于支持一些创新性工作,如IT基础结构的简化、服务器整合、关键业务应用以及向Linux的战略性迁移等。

IBM eServer OpenPower 720采用处理器卡设计,可配置二颗Power 5处理器,并共享36MB的三级高速缓存,大大缩减了高速缓存到处理器的距离,提高了处理器的整体性能表现。

Power 5采用0.13微米铜线和SOI(绝缘硅)工艺制造,在一个处理器中集成了2.76亿个晶体管,并新增了并发多线程(SMT)功能,可以将一个处理器内核转变为两个逻辑处理器使用,其计算能力十分可观。

OpenPower 720是为Linux定制的,操作系统可选择

SUSE或Red Hat等主流的Linux,可以用于开放源码Linux应用程序的通用开发和部署平台。由于从设计之初,这些Linux操作系统与OpenPower的整机硬件系统就在稳定性、运行效率和管理性等方面做了充分的匹配和调试,所以,OpenPower 720与Linux的结合就紧密程度可想而知。

另外,它还提供了企业级的虚拟化和动态逻辑分区(LPAR)功能,可以通过在一台服务器上部署多个应用程序来帮助企业降低IT成本,以保证业务的连续性、性能和安全性。



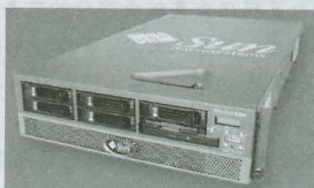
IBM eServer OpenPower 720

Sun Fire V40z: 降低 TCO

应用范围: Sun Fire V40z服务器设计独特, 适用于高性能计算和企业应用、Web 服务、数据管理、工作组协作、网络结构的数据库管理等应用。

Sun Fire V40z 服务器是一款基于 AMD Opteron 的4处理器的3U机架式服务器。它提供了64位高性能计算能力, 具有本机 x86 32 位功能, 并且具有与其他 32 位 x86 服务器类似的竞争价格。

这款产品的设计非常独特, 采用 AMD Opteron 符合业界标准的 32 位和 64 位架构, 支持 2 路和 4 路, 而且, 其中两个处



Sun Fire V40z

理器在机箱内, 而另两个处理器被放到了主机板上。多个处理器之间拥有网状交互结构, 大大提高了 Fire V40z 的数据传输和处理速度。

Sun 为 Fire V40z 提供了不同操作系统的应用, 用户可以用它运行 Windows 2003、Linux、Solaris x86 OS 等多种不同的操作系统。

Sun 的软件配备更降低了用户的整体成本, 其 Solaris 整体软件包括从操作系统、中间件到应用软件, 能同时兼容 32/64 位的企业级 Unix 操作环境。整个软件体系的一贯性更降低了用户的升级和维护成本。

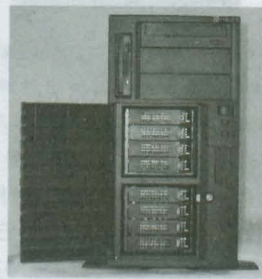
八亿时空 IT2660: 按需配置

应用范围: 八亿时空 IT2660 恒通服务器可以按需配置, 能够满足用户不断发展的业务需求。

IT2660 采用支持 64 位英特尔内存扩展技术的英特尔至强处理器, 在满足用户对 64 位应用需求的同时, 可以高效率地执行 32 位应用程序。

它采用 ECC 内存, 可以发现并纠正一位内存错误, 提高服务器的可用性和可靠性。而且, 可选 SATA RAID 0、1、5 或 SCSI RAID 0、RAID 1、RAID 1+0、RAID 5, 为用户提供了不同级别的数据保护方案, 提高了系统的可用性和可靠性。

这款产品可以进行按需配置。用户可选单 / 双通道 SCSI 或四通道 SATA 磁盘控制器, 可以根据应用需求灵活配置, 从而控制总体拥有成本。而且, 它最大支持 8 个 SATA 或 SCSI 热插拔硬盘, 并支持热插拔, 为用户提供了充分的数据存储空间, 能够满足用户不断发展的业务需求。



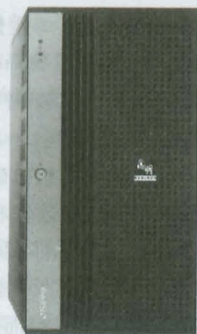
八亿时空 IT2660

方正圆明 MT300 2100: 高效管理

应用范围: 方正圆明 MT300 2100 能够满足前端接入服务器、中小企业服务器及高性能计算应用的性能需求, 其全面的管理功能大大简化了服务器的管理工作, 有效降低了企业的 TCO。

针对日益增长的后台服务器的需求, 如何管理服务器已经成为企业或者管理员必须解决的问题, 方正 RME (Reminus Management Expert) 管理解决方案应运而生。

RME 是一组根据用户需求专为圆明服务器量身定制、软硬一体的通用管理解决方案, 包括标准版、专业版和高级版几个版本。它具有强大的管理功能,



方正 圆明 MT300 2100

可以实现服务器的快速安装和部署, 降低了服务器安装、升级和维护的费用, 尤其适合服务器数量较多或者软件升级比较频繁的用户使用。

目前, RME 已经成功应用于方正圆明系列服务器家族所有服务器产品上, 圆明 MT300 2100 就是其中一款。RME 不仅能够提高圆明 MT300 2100 的可用性, 还可以防止服务器系统宕机和数据丢失, 减少了服务器的平均维修时间。

圆明 MT300 2100 具有多项新的或者增强的平台技术: PCI-Express 大大提高了系统性能; DDR2 400 内存具有更高的带宽, 降低了功耗; DBS 按需配电及增强 SpeedStep 技术降低了电力消耗; Intel EM64T 技术提高系统的可扩展性, 可以满足需要 64 位内存地址访问的数据库等应用的需求; 其内存镜像和在线热备技术提高了系统可靠性; 主板集成的智能 RAID 技术提供了经济、智能的数据保护方案。

航天联志 Aisino 9400R: 智能管理

应用范围: 航天联志 Aisino 9400R 是一款极具特色、性价比较高的高性能集群服务器, 适用于大型 Web 服务器、邮件服务器、数据库服务器等环境。



航天联志 Aisino 9400R

Aisino 9400R 是一款采用 Intel 的 IA 服务器产品为基础构建方式的集群服务器产品。其特点是用高速通信网络将一组多个超跃系列 IA 架构服务器连接起来, 形成松耦合多处理机系统, 就像一个单独集成的计算资源一样协同工作。

这款产品极具特色: 独有的内存 Chipkill 技术和错误纠正代码 (ECC) 功能, 使之可以经受在不支持此项技术的环境中足以摧毁整个系统的错误考验; 机箱带有非法入侵报警功能, 大大提高了整体系统的可用性和可靠性。

Aisino 9400R 的管理芯片直接集成在主机板上, 为用户提供了全面的硬件系统的管理及诊断功能: 监控服务器状况, 在第一时间探测系统元件的错误; 当服务器发生故障时, 可以根据预先的配置主动报警, 并帮助诊断服务器故障的基本原因; 还可以实现远程电源控制、基于温度的自动控制、风扇速度的调整等操作。

联想万全 T270: 无忧应用

应用范围: 联想万全 T270 可以同时承担中小型网络中多个业务应用、对硬盘数据安全较高的业务应用、大型网络中的局部应用以及其他运算量较大的应用, 也可以在行业用户省级大型网络的地区子网中同时担当多个业务。

万全 T270 是联想充分考虑中国企业及行业用户对于服务器的使用需要而设计的一款新型服务器产品, 能够让企业在 32 位应用与 64 位应用之间无缝迁移, 而无需更换硬件平台。

万全 T270 服务器从多个层面入手, 保证了服务器的可靠工作。比如, 所采用的 ECC 内存本身具备的纠错能力就是服务器安全性能的第一道保护屏障, “热插拔 SCSI + 高性能 RAID” 确保了企业应用系统与业务数据的安全。

特别的是, 万全 T270 在电源保护方面表现非凡, 即使您



联想 万全 T270

选择的是单电源配置的服务器, 也能轻松应对瞬时的断电。用户还可以选择冗余电源配置, 从而确保服务器不因电源和供电问题而影响系统工作。

而且, 借助于联想万全慧眼服务器智能监控系统, 用户可以对万全 T270 进行远程实时监控, 方便了对服务器的控制和管理, 特别是在服务器数目较多、分

布分散、距离较远的环境中提高了服务器管理的灵活性和及时性, 有效降低了企业对服务器管理的时间、费用及综合成本。

清华同方超强 TP300 2890: 平滑升级

应用范围: 清华同方超强 TP300 2890 具备强大的运算性能, 是一款面向高性能、海量处理的部门级服务器, 可以部署为邮件服务器、Proxy 服务器、Web 服务器、数据库服务器以及其他特殊应用服务器, 运行特殊应用软件, 如作为工作站运行多媒体制作程序等。



清华同方 超强 TP300 2890

清华同方超强 TP300 2890 是一款采用双路 Nocona 至强处理器的塔式服务器。它采用 800MHz 系统总线, 数据带宽达

到 6.4GB, 能够同时兼容 16 位和 32 位应用程序, 并完美运行未来的 64 位应用程序, 是一个平稳、全兼容平台升级解决方案。

在电源设计方面, 超强 TP300 2890 标配了 460W/600W 单电源或者 650W 2+1 冗余电源, 如果用户连接设备较多, 还可以选择大功率 2+1 冗余电源。为了更好地散热, 这款产品最大允许安装 3 个 120 毫米高性能系统散热风扇, 提高了系统的稳定性。

而且, 它集成了双通道 Ultra320 SCSI 控制器, 有效地保护了用户在高处理而非磁盘瓶颈应用下的投资, 如 Web、邮件等。它的机箱前面板还带有安全锁, 提高了系统的安全性, 使系统数据能够得到有效保护。

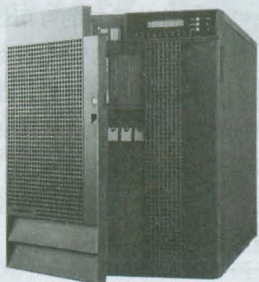
曙光天阔 S4800A: 以 SUMA 取胜

应用范围: 曙光天阔

S4800A 是一款强大的适用于后台数据处理的企业级服务器, 能够满足 ISP、电信、金融、教育等行业对稳定性、可靠性、处理性能的苛刻要求。

曙光天阔 S4800A 采用曙光公司自行研制开发的四路高性能服务器主板, 配有曙光先进的服务器监控系统, 是一款具有 SUMA 特性的优秀产品。

S—scalability 可扩展性 它的可扩展性极强, 可以从 32 位计算到 64 位计算, 从 32 位操作系统到 64 位操作系统, 从 32 位应用程序到 64 位应用程序。其处理器内建内存控制器,



曙光 天阔 S4800A

采用 64 位内存寻址模式, 抛开了 32 位内存寻址 4GB 限制, 无论是现在的 32 位庞大的数据库查询应用, 还是将来的 64 位大型 CAD/CAM、数字视频创建等应用, 都将不受内存容量的限制。

U—usability 易使用性 这款产品的机箱结构、电源系统、散热系统、服务器监控系统、热插拔冗余部件等均与 32 位服务器完全兼容。而且, 它配置了曙光天阔 A 系列服务器导航软件, 即使是初级用户, 也能轻松掌握 64 位服务器的安装、配置和管理。

M—manageability 易管理性 它采用曙光自主研发的新型硬件监控系统, 硬件监控配合主板芯片连接的硬件监控芯片, 可以对系统硬件工作状态进行实时监控, 并通过 VFD 显示屏向用户报警, 给用户提供了轻松、稳定的服务器管理环境。

A—availability 可用性 其风扇冗余、电源冗余、网卡冗余及负载平衡设计让系统可以 7 × 24 小时不间断运行。ISI

64 位服务器产品参数一览 (以厂商资料为准, 仅供参考)

产品	架构	CPU	缓存	内存	网卡	硬盘	散热
HP ProLiant ML370 G4	立式或机架式 (5U)	64 位英特尔至强 3.2GHz 和 3.4GHz 处理器, 可扩展至双路处理器。	1MB 二级缓存	PC2-3200R 400MHz DDR2, 标配为 1GB, 最大支持 16GB。	集成 NC7781 PCI-X 千兆网卡	/	标配 3 个风扇, 冗余风扇套件包括 3 个风扇及背面 CPU 风扇盒。
IBM eServer OpenPower 720	立式或机架式 (4U)	Power 处理器, 1.5GHz 1 路、2 路、4 路或 1.65GHz 2 路、4 路	36MB 三级高速缓存	每处理器卡上具有 8 个双列直插式内存 (DIMM) 插槽, 内存最大 32GB。	两个以太网 10/100/1000Mbps 端口	四个标准和四个可选的热交换 Ultra320 SCSI 驱动器支架, 可获得超过 1.1TB 的存储容量。一个全配的带 8 个 7311-D20 I/O 扩展笼的 OpenPower 服务器可支持超过 14.6TB 的联机磁盘存储。	备用的热插拔冷却风扇。
Sun Fire V40z	机架式 (3U)	最多 4 个 AMD 844 或 848 Opteron 处理器	每个处理器带 1MB 二级高速缓存	最高可达 32GB DDR1/333 ECC 寄存 DIMM, 每个 CPU 带有 2 × 4 个 DIMM 插槽。	板载千兆以太网双端口	最多 6 个 Ultra320 SCSI 磁盘驱动器 (内部磁盘)。	冷却设备
八亿时空 IT2660	立式单塔	支持两颗 Intel 新 XEON 2.8~3.6GHz 处理器	1MB 全速二级缓存	ECC Registered DDR 内存, 最大容量可扩展到 8GB (4 个内存插槽)。	集成 Intel PRO/1000XT 服务器网卡	最大支持 8 个 SCSI/SATA 硬盘。	主动散热系统
方正 圆明 MT300 2100	x86	Dual Nocona	1M L2	最大 16GB ECC Registered DDR333, 或最大 24GB ECC DDR Registered DDR266。	双千兆网卡, 其中一个采用 PCI-E 总线	SCSI、S-ATA。	1 个 120 毫米系统散热风扇, 可选 2 个 60 毫米热插拔系统风扇
航天联志 Aisino 9400R	机柜式	支持 4 颗 Intel 安腾 2 处理器	片内 256KB 全速二级缓存, 1.5MB/3MB/6MB 三级缓存。	ECC Registered DDR200/266 SDRAM, 最大 32GB。	集成 Intel 82540EM 10/100/1000M 服务器专用网卡	提供 3 个 1 英寸热插拔硬盘位, 最大 220GB 内部存储容量。	冗余风扇
联想 万全 T270	IA 架构	支持两路英特尔至强处理器, 2.8、3.0、3.2GHz 或更高主频	1MB 二级缓存 (CPU 片内集成)	Registered ECC DDR 333 内存, 最大可扩展至 8GB。	集成两个千兆自适应网卡	最大 5 个热插拔硬盘架位和 2 个非热插拔硬盘架位, 可支持 36/73GB 10000 转/分钟的 SCSI 硬盘。	/
清华同方 超强 TP300 2890	塔式	2 颗英特尔 Xeon 2.8GHz、3.0GHz、3.2GHz 或更高主频	1MB 二级高速缓存	Registered ECC DDR333 内存, 支持双通道读取技术, 可扩展至 16GB。	内置 2 个英特尔千兆服务器网卡	硬盘支持热插拔 SCSI 配置, 最大可提供 8 个 SCSI 热插拔硬盘。	可扩展 3 个 12 厘米高速系统散热风扇
曙光 S4800A	四路机架式	单 AMD Opteron 840 处理器, 可扩展至两路或四路。	1MB 二级缓存	最大可支持 20GB DDR ECC Registered 内存。	双千兆以太网网卡	最大支持 18 块 Ultra 320 热插拔硬盘。	可配置六只热插拔的冗余风扇

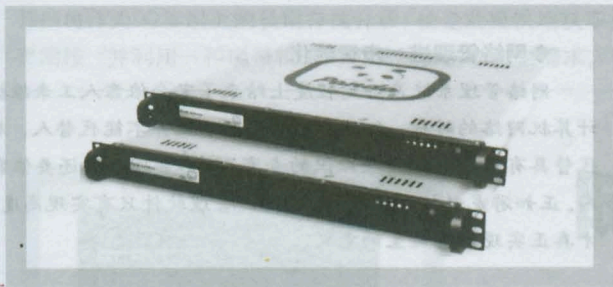
方正熊猫硬件安全网关：

网关保护三重门

■ 本刊记者 文飞

随着互联网的迅速普及，病毒的肆虐和猖狂也变得一浪高过一浪。

在过去的两年中，有99%的病毒是通过因特网进行传染和攻击的，其中更多的是通过SMTP邮件和HTTP网页浏览进行传播的。调查显示，全球电子邮件流量到2006年将达到600亿封，其中每204封邮件就有一个病毒，这些病毒所造成的经济影响以几十亿美元计。国际电信联盟专家会议在闭幕时发表的公报指出，目前约80%的电子邮件是垃圾邮件，每年给世界经济造成的损失高达250亿美元。而根据刚刚公布的中国互联网协会第三次垃圾邮件调查报告显示，国内网民平均收到的垃圾邮件占网民收到邮件总数的65.79%，几乎达到正常邮件的两倍。垃圾信息的危害也同样不轻，美国



Websense公司最新公布的一份调查结果显示，四分之一的员工每个星期至少会花费超过一个工作日的上网浏览与工作无关内容。可以说，病毒、垃圾邮件和不受欢迎的内容是令网络管理人员烦恼的三个“害群之马”。

解决这些“害群之马”的方法当然很多，许多网管都有自己的经验。不过，谈到轻松、高效、实用，也许方正安全和熊猫软件刚刚联手推出的高性能方正熊猫硬件安全网关8000能给您一些启发。

方正熊猫硬件安全网关8000系列产品在原有7000系列的基础上融合了更多全新功能和尖端技术，在网络边界或Internet网关处提供全面的防病毒、反垃圾和内容过滤的三重边界防护，在病毒、垃圾邮件和不受欢迎的内容进入网络之前进行彻底阻断，从而突破了传统的防病毒技术，真正构建了企业安全网络的第一道屏障。

◆**防病毒：**熊猫卫士安全网关拦截和扫描HTTP、FTP、SMTP、POP3、IMAP4和NNTP通讯以检测恶意软件。管理员可以开启或关闭对每种协议的扫描，将99%以上的含毒数据阻

止在企业网络之外，大大降低防病毒软件的负载和对企业网络资源的占用，使得企业网站运转更加顺畅。

◆**反垃圾邮件：**熊猫卫士安全网关通过其反垃圾邮件模块检查进入公司的所有邮件。信息被扫描并划分成垃圾或非垃圾两类，在未被请求的邮件到达用户信箱之前进行阻断或修改信息的主题。也可以根据发件人的地址生成白名单和黑名单，这些地址清单发出的邮件可以免受扫描或发自这些地址的邮件被直接定义为垃圾邮件。为了更好地调整分析，反垃圾邮件模块具有不断学习的功能，这将显著地减少垃圾邮件的产生，将员工从手动删除大量垃圾邮件的繁琐工作中解放出来。

◆**内容过滤：**网页过滤模块允许网络管理员控制企业网络资源的使用，并且阻止非法、色情或暴力网页内容进入公司。该模块扫描通过HTTP访问的URL，并且阻断访问那些未被授权的内容，使管理员知道哪些内容用户正在访问。过滤规则根据预定义内容目录和管理员定义的白名单（允许）和黑名单（非授权）进行网页内容筛选过滤，让员工将网络真正运用于工作。

除了以上这些特点，方正熊猫硬件安全网关8000系列的安装和配置、管理通过简单的Web界面实现，网桥模式的工作原理和强大的硬件性能决定了它能在不改变用户原有网络规划的情况下满足多种复杂的网络环境。而且，方正熊猫硬件安全网关8000系列还拥有人性化报告和负载均衡等功能，使得企业在拥有高度安全性的同时充分提高企业运营效率，为企业创造价值。

赛迪评测在对方正熊猫安全网关GateDefender 8200做了精心测试之后评价说：“该产品是一款先进的基于硬件的多功能安全网关，利用它可以在Internet网关处对内网提供全方位立体防护，使病毒、垃圾邮件和不受欢迎的内容在进入客户网络之前便被阻断，更最大限度地保护了用户的网络免受侵袭。”

编辑点评：方正熊猫安全网关GateDefender8200作为一款具备千兆网络接口的网络安全硬件产品，具有功能齐全、性能优越和便于管理的特点。其优秀的HTTP及SMTP处理能力可以满足具有上千用户的单位进行Internet访问的需求，每天自动进行的恶意代码防护引擎和特征码定义文件的自动更新可以很快地对新出现的网络病毒做出防护反应，多种扫描协议可以拒病毒于网外，而不是像一般防病毒软件那样，只有病毒进入内网才进行反应的被动局面。 ■■

国产网管软件的本土化及其发展

网管软件在巨大的市场需求的推动下,发展前景已经被业内人士普遍看好。在“网管软件”的大概念下,各网管软件的管理侧重点却不尽相同。有的侧重于网络设备的管理;有的侧重于服务器的管理;有的侧重于对网络基础架构及其应用系统进行综合集中式管理,如IBM Tivoli、HP OpenView、游龙 SiteView 等。

网管软件的本土化趋势

现在网管市场格局日益清晰,虽然电信级网管市场被有限的几家国外网管软件提供商长期占据,但是随着国产网管软件的崛起,这一格局正在悄悄地发生变化。网管软件只要能够在激烈的市场角逐中脱颖而出,经受住市场竞争的考验,为众多的消费企业认可和接受,就是适合市场需求、可以创造出巨大生产力的高品质软件。以游龙科技的 SiteView 网管软件为例,国产网管软件的发展呈现如下明显特征:

◆在技术的应用上与国际保持同步

国内网管厂商时刻关注国际网管标准的出台,关注国际相关网络组织、协会的最新动态,并能及时预测和把握最新网络技术,充分与国际接轨。国际上最新推出的各种网管技术,都会很快在国产网管软件中得到普及和应用。对于其中的部分技术,中国的网管软件甚至可以结合自身应用的特点,更加深入地得到开发和利用。

如 SiteView 网管软件采用了国际先进的 Portal 技术,它具有很强的可扩展性、兼容性和综合性,提供了对分布式软件服务和信息资源安全管理的框架。而 SiteView 对 RMON (远程网络监控) 技术的应用,可以更为有效、更为积极主动地监控远程设备;同时,游龙科技也对正在探索中的 CORBA 技术给予了充分的重视,深入研究其作为一个面向对象的分布式计算平台,如何实现不同的程序之间透明地互相操作,从而使不同的网络管理模式能够结合在一起。

◆本土化的服务

网管软件的竞争已经从产品的竞争延伸到服务的竞争,网管软件的管理对象是面向整个 IT 基础架构及其应用。用户对网管软件需求的差异性极大,再好的产品也需要良好的售前、售后服务以及二次开发才能更好地满足用户差异化的需求。游龙科技总裁张泽军说, SiteView 作为一个成熟、专业的国产网管软件,拥有全部源代码和自主知识产权,相对而言,它可以为中国客户提供更加有针对性的、个性化的服务。

◆本土企业进一步掌握核心技术

虽然很多领先的网管技术都源于国外,但是现在新技术在国内的普及非常迅速,而且国内网管厂商大都具有很强的新技术信息捕捉和开发能力,在新技术和新产品上都能够迅速跟进国际水准,甚至在一些特色应用上超过国际水平。国外成熟的网管软件产品普遍架构庞大而复杂,对新技术的应用可以说是牵一发而动全身,所以对新技术的采用普遍采取比较保守的策略。国内网管软件业虽然起步比较晚,在业内非常具有影响力的游龙科技,也才仅有六年的历

史;但是发展速度非同一般,并有赶超国际网管软件的趋势。同时,本土企业也正在进一步掌握核心技术,并在此基础上研发自身独特的产品。

国产网管软件的发展趋势

中国网管市场的发展,已经从初期的厂商引导购买转变到市场需求驱动的模式,市场已经基本蕴育成熟。目前,国内很多成熟的网管软件厂商已经开始逐步进入国际市场。如,游龙科技已于 2004 年 5 月份推出了 SiteView 英文版。总体来说,国产网管软件的发展趋势体现在以下几个方面:

◆基于 Web 的网络管理技术将得到越来越广泛的应用

基于 Web 的网络管理系统可以通过 Web 浏览器十分方便地进行远程管理。游龙科技研发经理王朋介绍:在未来的 Intranet 中,基于代理与基于嵌入式的两种网络管理方案将被广泛应用。大型企业通过代理来进行网络监视与管理,而且代理方案也能充分管理大型机构的纯 SNMP 设备;内嵌 Web 服务器的方式对于小型办公室网络则是理想的管理模式。

◆网络管理进一步智能化

网络管理系统在一定程度上结束了完全依靠人工来维护和管理计算机网络的时代。但是,网络管理系统并不能代替人,尤其不能代替具有专门网络管理知识的专家,网络管理系统还要依靠人去使用。正如游龙科技总经理张泽军说,管理软件只有实现高度智能化,才真正实现了它诞生的意义。

◆大型网络的综合化管理与个性化管理

毫无疑问,企业的网络即使规模不扩大,应用也会增加,网络系统只会越来越复杂。现在部分企业的网络管理软件比较混乱,有专门的服务器网管软件,也有不同的网络设备厂商提供的设备管理系统,还有加强对应用系统管理的软件。这种多网管系统共存于一个网络系统的混乱局面,不仅失去了自动化、简单化管理的意义,而且会对系统的性能产生一定的影响,必须引进综合完善的网管系统来加以解决。

综合化管理是指面向服务器、网络设备和应用系统的管理。现在企业用户的网络规模越来越大,网络基础和应用系统也日渐增多,而且大都呈现分布式网络、集中化管理的特点,各企业为全面掌握网络动态、充分利用网络资源,必然会加强综合化管理。游龙科技 SiteView 网管系统在研发过程中,非常注重 SiteView 的可扩展性和与其他网管系统的兼容性,从而使综合化管理与个性化管理有效地结合起来。

北京游龙科技有限公司

地址:北京西长安街 88 号首都时代广场 13 层

电话:(010)51655987

网址:www.siteview.com

备份存档二合一

■ 本刊记者 彤欣

在飞速发展的信息时代，企业在存储方面面临着许多挑战：企业通常的备份时间为10小时或更短，因而需要更高性能的备份设备，以便在相同的备份时间内备份更多数据；需要更广泛的存储整合，以减少软硬件及资源管理的开支，从而提高投资回报，改善灾难恢复、提高安全性和性能；为了遵守政府法规，许多记录需要保持7年或者更长时间……

该如何应对这些挑战？为了帮用户解决这道难题，HP推出了第三代全高LTO Ultrium（傲群）磁带机HP StorageWorks Ultrium 960，且为每台磁带机免费内置了单服务器的HP OpenView Data Protector 备份软件v5.5许可证。

HP StorageWorks Ultrium 960的容量达到800GB，传输率为160 MB/s，全面支持一写多读（WORM）介质，不仅向企业提供了数据保护特性，更提供了全面的归档功能。磁带归档将作为30年以上的长期存储介质，使企业更快地获取投资回报，并利用一种磁带机来同时满足备份和存档需求。相



HP StorageWorks Ultrium 960

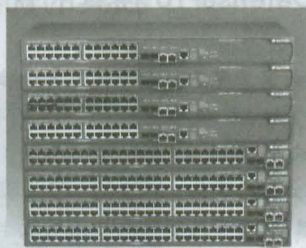
比基于磁盘的WORM解决方案，磁带归档以相当低的成本增加长期存储容量，并拥有进行长期存储的更高的产品稳定性（可用性和可靠性）；同时，磁带容量、性能和可管理性方面的进步，将能满足用户对更大存储整合的需求；HP强大的OBDR单键灾难恢复解决方案帮助企业轻松从灾难中恢复。而且，这款产品广泛支持主流的备份和归档存储软件，实施中几乎不需要任何改变。

特别的是，LTO Ultrium技术具有业界领先的产品规划和兼容性，HP还制定了长期、稳定的Ultrium发展蓝图，产品多达4代以上，更最大限度地保护了企业的现有投资。

编辑点评：HP StorageWorks Ultrium 960是一个高容量备份解决方案，它将故障保护特性集成到驱动器固件、磁带内存、介质格式化和软件中，分别具有多次重写和只写一次WORM的介质，以一种低成本、易于部署的解决方案，让一种驱动器能够同时满足备份和存档需求。 INI

随需应变的好网络

■ 本刊记者 逸阳



华为 3Com Quidway S3900

大部分企业、学校、团体、社区使用的网络规模会随着组织规模的不断增长而增长，因而在最初规划网络的时候会预留一定的容量以便扩充和升级。然而，如果预留的容量太大，初期投入资金无疑是一种浪费；预留的容量太小，将来升级时又难免捉襟见肘。这一直是困扰网络规划者的一大难题。

针对这种情况，华为3COM公司推出了“IRF”智能弹性架构技术，让网络的扩容和升级变得非常简单和快捷。IRF智能弹性架构是华为3Com公司融合高端交换机的技术基础，在中低端交换机上推出的创新性建设网络核心的新技术。它让用户在网络建设初期可以只购买当前需要的网络设备，不需要为将来的网络需求买单。等到网络规模需要扩充时，新的设备可以在运行中随时加入，并自动同步获取IRF的全局配置。在扩容过程中，原来设备的运行基本不受影响，让用户原来的投资得到

更大限度的保护。

在使用上，IRF和传统的三层堆叠技术有一点相似。简单说，就是支持IRF的多台交换设备可以互相连接起来形成一个“联合设备”，称之为一个Fabric，组成Fabric的每个设备则被称为一个Unit。多个Unit组成Fabric后，无论在管理还是使用上，将成为一个整体。用户可以将多台设备看成一台单一设备进行管理和使用，既可以通过增加设备来扩展端口和交换能力，也能通过多台设备之间的互相备份增加设备的可靠性。

华为3Com的Quidway S39/56/65系列交换机是基于IRF技术推出的系列新产品。其中，Quidway S5600系列交换机具备10GE接口上联、完善的语音解决方案和其他丰富的业务特性，保证了网络接入和相关业务的开展；而S65家族的新一代万兆产品6502则采用全新第三代交换引擎，其新增的高密度GE接口板兼容原有接口板，可以全面保护用户的原有投资。

编辑点评：随着网络的发展，网络设备也要不断更新，如何使自己的网络设备能够不断适应网络的发展成为一个棘手的问题，华为3Com的IRF技术给我们提供了一个解决此类问题的途径。 INI

快速全面的深层防护体系

Radware DefensePro

随着各个企业对网络化应用的依赖性不断增强,他们面临的各种攻击的威胁也在不断增加。应用攻击的数量和严重性的快速增长,使其对企业造成的损失也呈直线上升趋势。在这种情况下,传统的防火墙或入侵检测技术(IDS)显得力不从心,这就需要引入一种全新的技术—入侵防护(Intrusion Prevention System, IPS)。Radware推出的DefensePro,实现了以3千兆位的速度检测和拦截1300多种病毒、蠕虫和特洛伊木马,从而快速而全面地清除所有恶意入侵。

Radware DefensePro 硬件平台介绍

DefensePro的硬件架构是为满足企业、电子商务公司以及通讯商在网络和应用保护方面的需求而设计的,共有两款硬件平台:Application Switch II和Application Switch III。其中ASIII平台是4到7层业界唯一的万兆平台。

◆ 44 Gbps 的交换结构及业内最高的端口密度: DefensePro无阻塞的44千兆位交换背板基于多层的分布式交换架构,共包括1个10GbE端口、7个1千兆位端口以及16个高速以太网端口实现线速交换的交换ASIC。借助业内最高的端口密度和最高的交换性能,一台DefensePro设备就可以执行对多个网络段的双向扫描。

◆ 更先进的网络处理器: 当两个网络处理器并行工作时,它们可以用数千兆位的速度同时处理多个数据包并且执行所有同数据包处理有关的任务,包括流量转发和拦截、流量控制以及延迟绑定等。值得一提的是,它们可以用每秒100万个SYN请求的空前速率来防范拒绝服务攻击和任何已知或未知的SYN flood攻击。除了清除所有可疑流量外,网络处理器还支持端到端的流量控制和带宽分配管理,确保了流量的安全性与稳定性,以及关键任务应用的连续性和服务质量。

◆ Radware StringMatch Engine—基于ASIC的专用安全硬件加速器: Radware StringMatch Engine是一种专用的硬件卡,旨在提供更快速的数据包检查和特征比较,它由ASIC和高端的Power PC RISC处理器构成,提供了9千兆位速度的自由范围搜索和16千兆位速度的固定偏移搜索。

◆ CPU—1 GHz的安全会话管理: DefensePro的RISC处理器使用的是Motorola PPC7457。它不仅可识别所有的活动攻击并且控制StringMatch Engine和网络处理器中隔离、拦截和阻止攻击的活动操作,而且还可以管理所有的安全更新和网络要求。

Radware DefensePro 的主要功能

在先进的硬件平台基础上, Radware充分发挥了在基于内容的处理上的技术优势,保护网络化应用免遭攻击威胁,并提供了高速的入侵防范能力和拒绝服务攻击防范能力。

◆ 攻击监测和隔离: DefensePro不仅为管理员提供了对网络流

量的全面监视能力,而且还使得他们可以实时识别蠕虫、病毒和异常的流量模式,从而实现对所有活动威胁的完全监视。

◆ 对各个网络段的流量进行双向扫描: DefensePro是为嵌入式部署而设计的,它可以在具有多个网络段的网络中对所有流量进行实时扫描并对数据包进行逐一检查,根据恶意攻击模式执行特征比较。

◆ 3千兆位速度的攻击特征比较: 为了支持数千兆位的特征扫描速度, DefensePro专门采用了基于ASIC的强大加速器—StringMatch Engine™。StringMatch Engine支持并行的特征搜索操作,可对照特征数据库进行高速的检测和数据包比较。

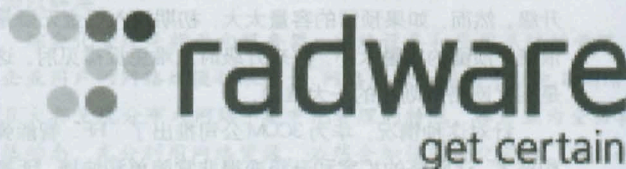
◆ 实时抑制攻击: 当检测到恶意活动时, DefensePro立即执行丢弃数据包、重置连接以及向管理位置发送报告等操作,从而为各种应用系统和操作系统、网络设备和网络资源提供了全面保护。

◆ 防扫描功能: 黑客在发起攻击之前,通常都会设法确定打开的TCP和UDP端口。DefensePro的应用安全模块可以拦截并修改发送给黑客的服务器应答,从而提供了旨在阻止黑客获取信息的全面机制。

◆ DoS Shield—彻底防范拒绝服务攻击: DefensePro的DoS Shield模块可借助高级的取样机制和基准流量行为监测来识别异常流量和DoS攻击,这不仅实现了完全的DoS和DDoS防范能力,而且还保持了大型网络的高吞吐量。

Radware DefensePro 独具的优势

DefensePro独具的多层安全架构组合了数种攻击检测机制,它们联同高级的防范工具(如DoS Shield、SYN cookie和应用安全模块)一起,提供了对恶意攻击和DoS攻击的完全防范能力。DefensePro的底层支持技术是4层安全交换架构,其交换ASIC使用了44 GB的线速背板、2个网络处理器、RISC处理器和专用的基于ASIC的硬件加速卡(StringMatch Engine),可将检查速度提高1000倍。这使得DefensePro成为高速/高性能环境中的应用安全性能的基准。



瑞得韦尔中国公司

地址: 北京市东城区东长安街1号东方广场中二办公楼901室
邮编: 100738

电话: +86 10 8518 3790

传真: +86 10 8518 3786

网址: <http://www.radware.com.cn>, Info@radware.com.cn

性能与防御并重



港湾网络 SmartHammer G503

在网络安全中, 防火墙一直充当着非常重要的角色。通常, 防火墙这种产品是由专门的网络安全厂商研发的, 虽然具有专业性的优点, 但是作为数据的转发设备在性能和体系结构上存在些许不足。港湾网络清楚地认识了这一点, 于近日发布了全系列的基于NP技术架构的SmartHammer系列防火墙产品。

该系列产品基于新的安全理念设计, 采用基于网络处理器(NP)的安全处理核心, 支持ACL预编译、DDR业务队列调度、基于状态的资源控制、基于状态的深层报文分析等港湾网络公司专有的安全技术, 能够实现网络的高性能, 并具有深层次的安全过滤能力。

更有特色的是, 配置于核心交换机的防火墙模块ESP-FW是港湾网络对网络安全深入理解的技术结晶, 融交换机与防火墙各自的安全过滤能力为一体, 能够让用户对内网划分多个安全域, 可以有效抑制攻击区的蔓延以及受损区域的扩大。其工作原理就如同轮船中的隔水舱, 能够实现对占网络攻击总量78%以上的内部网络攻击防御, 从根本上提高了整个网络的抗攻击能力。

八位一体, 全面防毒



瑞星杀毒软件 2005 版

以“截获病毒——杀毒软件升级——查杀病毒”为特征的传统反病毒模式, 已经远远不能满足用户的安全需求。因此, 一款反病毒产品必须包括系统修复、查杀病毒、反黑客等众多功能, 这些功能就像木桶上的木板, 哪一块板子短了, 都会导致整个安全系统的崩溃。

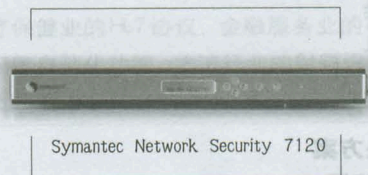
针对这种严峻的形势, 瑞星开发了瑞星杀毒软件2005版。它集反毒、防黑、反垃圾等八大功能于一体, 采用面向对象的高稳定性设计, 是一款真模块化、高应变型杀毒引擎。新品依托全新的OOT杀毒引擎, 在“立体防御”的主导设计思想下整合各种新技术和新功能, 能够协同防御, 不留死角, 为企业提供全面防护。

这款产品强化了木马病毒查杀、网络游戏保护和智能反垃圾三个专向保护功能, 以及作为电脑信息保护最后防线的“数据修复”功能。尤其值得一提的是它的“数据修复”模块, 采用瑞星专利技术“高效超容压缩数据拯救”, 占用硬盘空间少, 效率更高。

一键切换, IDS/IPS 大变身

赛门铁克Symantec Network Security 7100系列是一款具有千兆级入侵防护功能和创新的—键防护能力的入侵防护设备。用户只需通过单击鼠标, 即可轻松地把SNS 7100系列从综合监测设备转变为功能强大的防护工具, 允许客户根据其安全策略在不同模式间进行切换。而且, 该功能对任何以太网网络都是透明的, 因而可以在提供极佳安全威胁防范能力的同时确保业务连续性。

这款产品集成了新型的入侵抑制统一网络引擎IMUNE。IMUNE架构是可以实时检测并阻止现今不断变化的安全威胁



Symantec Network Security 7120

的一种革命性方法, 可以阻止蠕虫传播, 并且精确地阻止恶意威胁, 能够防止客户遭受入侵和恶意代码、网络基础结构攻击、应用程序利用、扫描、探测、DoS拒绝服务攻击、后门、缓冲器溢出以及像MS Blaster和SQL Slammer等的攻击。

Symantec Network Security 7100包含7120、7160和7161三种型号, 带宽范围为50Mbps到2Gbps不等, 可在—台设备上监控八个网段的数据流量, 能够满足用户不同的带宽需求。而且, 它还允许企业通过LiveUpdate下载赛门铁克安全响应中心的最新安全更新, 让企业能够实时防范最新威胁。

Symantec Network Security 7100包含7120、7160和7161三种型号, 带宽范围为50Mbps到2Gbps不等, 可在—台设备上监控八个网段的数据流量, 能够满足用户不同的带宽需求。而且, 它还允许企业通过LiveUpdate下载赛门铁克安全响应中心的最新安全更新, 让企业能够实时防范最新威胁。

BEA 助企业实现业务创新

BEA公司近日推出了代号为“Diablo”的BEA WebLogic Server 9.0。Diablo添加了许多全新功能, 为下一代集成软件组件——即将面世的BEA WebLogic平台9.0奠定了基石。

新品旨在连接不同的计算机系统, 运行大型公司开展业务的应用软件。Diablo的独特之处在于它是一款能够帮助企业应用面向服务的架构(SOA), 可以快速实现开发和部署大容量任务。Diablo具有应用软件和服务器“实时”更新的特点, 执行上述更新时, 无需离线, 也不需要中断对终端用户的服务。

Diablo管理简单的特点可帮助企业为维护其基于WebLogic的应用软件时, 极大地节约成本。使用Diablo统一的、基于入口的管理控制台, 可为系统管理员提供更统一的群集部署和更完整的操作控制。通过它, 可以对该控制台进行定制, 以便为企业内的不同角色和职责提供不同的视图, 它允许第三方嵌入自身的管理和监测工具以提供额外的功能。

Diablo还具有一个高级诊断框架, 可以允许管理者实时识别并解决生产中运行的应用软件中的问题; 同时具有自调功能, 即一种创新的自调技术, 包括定义服务级别的能力, 因此, 服务器可以实时进行调整, 以解决这些问题。这样的结果, 使Diablo不仅可以提高持续正常运行时间, 而且可以降低配置和调节的复杂性。

高度灵活的 SAN

McDATA 的方案组合如何满足用户的业务需要

McDATA 的产品组合可以满足不同客户的各种需要。虽然它也关注那些拥有小型 SAN 或新建 SAN 的客户,然而这篇文章是集中讨论那些拥有较大及分散 SAN 的用户的需要。

McDATA 的产品的方案可以协助机构克服过往部署 SAN 后遭的问题。通过利用 McDATA 的网络解决方案,客户可以更好的满足下列业务需要:

- ◆ 存储资源的整合
- ◆ 分散存储资源的安全共享
- ◆ 集中化备份
- ◆ 灾难恢复和业务持续
- ◆ 配合业务增长的扩展
- ◆ 减少整体成本

针对业务需要的网络解决方案

整合并安全的共享存储资源

虽然整合存储资源是实行 SAN 的一大驱动因素,但一些 SAN 技术的限制桎梏了整合选择。安全问题、端口数限制和距离限制迫使组织产生了 SAN 孤岛,结果是尽管每一个 SAN 的主机都可以分享存储资源,但这些资源却不能在各个 SAN 中共享。如果一个阵列只是部分用于一个 SAN,其闲置资源并无有效方法用于其他用途。如今 SAN 用户希望能全面利用全部可用的资源,因此希望能够跨越各个 SAN 来整合资源。

McDATA 可通过 SAN 路由和动态分区(Dynamic Partitioning)来解决上述问题,例如 SAN 路由可通过 IPS 3300 和 IPS 4300 来实行。当一个 SAN 路由被置于 SAN 孤岛之间,每一个 SAN 光纤网络仍是独立的,但资源可以安全地跨越 SAN 被共享。SAN 路由为分立的多个 SAN 提供选择性连接。如果 SAN B 上有多余的容量,而 SAN C 的一个主机需要额外的数据存储空间,通过建立路由可容许 SAN C 的主机附接在 SAN B 的阵列上,这样便不需要为 SAN C 购买额外的存储资源。

集中备份

集中备份是推动机构部署 SAN 的另一关键因素。如果一个机构有多个 SAN 孤岛,那么每个孤岛通常有多种备份资源。正如整合主要的存储资源一样,机构也希望整合这些备份资源。McDATA 的 SAN 路由让机构可以把备份资源汇聚在一个 SAN 上。备份可以在校园及远程路由网络环境上进行,McDATA 的 SAN 路由器是采用 iFCP 协议,这种协议允许光纤通道数据传输可在 IP 网络上进行。通过利用 IP 网络来传输数据,备份可以在分散各地的多个 SAN 中进行。

灾难恢复和业务持续

固然充分的数据备份是支持灾难恢复和业务持续进程的要素,然而,一个扎实的灾难恢复和业务持续计划牵涉到建立一个远程的站点,然后将所有关键数据复制至其中,以便保证灾难发生时数据的可恢复性。最近发表的 ESG 数据保护调查报告显示,58% 的受访者(调查对象为 228 名用户)表示他们只可以忍受 4 个小时的停机时间,否则他们将蒙受严重的盈利损失及业务打击,简言之,一个充分的灾难恢复和业务持续计划是必备的。

满足增长需求的扩展性

机构需要存储的数据量不断急速增长,单是交换应用程序每年

便牵涉超过 400TB 的新数据。机构必须不断增加更多的存储资源来解决这个问题,如果这些数据是联网的,这就意味着要增加更多的端口。存储网络是有局限的,尽管光纤通道规格表示 240 个独立的交换机可以在同时于一个 SAN 中运作,但没有人会尝试构建拥有这么多台交换机的 SAN,“扁平的”SAN 是管理者的恶梦,当每一个附带设备找到一个新地址时,重新配置就会令整个 SAN 瘫痪。

管理问题也是导致 SAN 孤岛出现的部分原因,因此问题的核心是在机构规模扩大时,怎样能保持网络的高效率, SAN 路由和动态分区可解决这个问题。SAN 路由可以使不同 SAN 之间选择性互联,同时 nScale 动态分区结构可以使那些已经达到它们增长限制的 SAN 组成一个更大的 SAN。Intrepid nScale Director 可被放在 SAN 孤岛间,然后分区并为每个孤岛增加端口,而光纤网络仍旧保持“独立”。

降低总体成本

很明显,整合和共享资源可以降低资本开支。通过使用 SAN 路由和动态分区,企业可以有效的降低他们的整体存储资源成本。另外,管理和行政成本因备份整合和集中管理也将会减少。McDATA 不仅提供交换机来满足这些需求,其存储管理和安全软件解决方案也可减少行政成本,并降低数据丢失和无法恢复的风险。此外,用户可通过现有 SAN 的基础设施来实现上述两项功能。

总结

McDATA 一向以为数据中心存储网络需求提供高可用、高度可靠的解决方案而闻名于世。McDATA 理解客户的存储网络需求,并能通过其各种解决方案协助解决客户的业务需求。

强强合作

2004 年 11 月全球开放存储网络(SAN)解决方案的领导者 McDATA 公司与国内最大的 IT 服务供应商之一神州数码(中国)有限公司在北京签署了战略合作协议。根据协议,神州数码将成为 McDATA 公司存储网络(SAN)解决方案在中国大陆地区的总代理,协助 McDATA 公司拓展全国各地区增值经销商,并为最终用户提供更为直接和全面的解决方案及服务。神州数码将整合渠道、方案、技术服务等多方面优势支持 McDATA 公司的推广工作。McDATA 公司与神州数码的全面合作,将有助于更好地为中国客户和合作伙伴提供范围广泛的产品和服务,使其增强数据及业务的可靠性和可用性同时,同时降低了总体拥有成本。



神州数码
Digital China

地址:北京市海淀区苏州街 16 号神州数码大厦 9 层

邮编:100080

电话:010-62693090

传真:010-62693365

E-mail: yandong@digitalchina.com

安全的零距离办公

日前,赛孚耐公司正式推出SSL VPN 解决方案SafeEnterprise SSL iGate 4.01版。这款产品增强了iGate用户界面的易用性,应用更加简单、方便,所有管理界面都可以通过Web进行在线操作,消除了原来必须同时使用ACM软件和Web管理界面的麻烦。

iGate 4.01具备强大的SSL远程接入能力,可以完全支持远程全网连接;拥有高级别的安全性,支持PKI体系和客户端策略检查功能;集成双因素身份认证令牌,还支持对基于Web的PDA或其他移动设备。正是由于这些特性,远程用户可随时随地通过SafeEnterprise SSL iGate 4.01实现从酒店、网吧、随身携带的电脑或其他无线设备上安全访问公司内部网、收发电子邮件、进行文件共享或调用内部应用系统和数据,真正实现安全零距离办公。

数据备份一键OK

当中小企业和家庭用户要备份和管理其宝贵的数据资料时,Maxtor OneTouch II外置式硬盘是一个非常好的帮手。

新型的OneTouch II外置式硬盘继承了广受好评的“一键式”快速数据备份与恢复的功能,在容量、速度、外观和使用性方面均有了进一步的提升,以满足用户不断增长的存储需求。此外,OneTouch II还特别增加了DriveLock加密功能,从而进一步加强了数据的安全性,同时兼容PC及Mac平台,可以满足不同平台用户的需求。

用户只需根据需要激活附赠的Dantz Retrospect Express备份软件,便可以自动备份时间、备份范围,甚至可以选择备份文件种类,以及随意恢复任何一天所保存的备份资料,而免于因系统崩溃、病毒袭击等带来的数据损失。

可靠的邮件保护伞

CipherTrust新近推出的IronMail S级设备是专为规模为1000或小于1000个电子邮件用户的企业而设计的,提供了4个版本以满足中小企业预算和业务需求,能够为规模较小的企业的信息基础设施提供保护。

IronMail S级设备具备CipherTrust反垃圾邮件防护、反病毒防护、策略实施和安全电子邮件网关能力的所有特点,可以确保电子邮件沟通的完整性。IronMail的垃圾邮件工具箱有别于其他同类产品,它使用多种垃圾邮件侦测技术,这些技术均优化地建立在独有的遗传优化处理基础之上。

此外,IronMail S级设备还具备CipherTrust零时差病毒防范功能,在病毒入侵并破坏一个小范围业务环境之前通过网关实时的侦测遏制其爆发。

而且,S级设备易于安装,以IronMail集成的方法为电子邮件应用程序提供一套完整的解决方案,而非对多个个别的威胁提供多点解决方案。

满足企业管理新需求

Oracle电子商务套件11i.10 (Oracle E-Business Suite 11i.10)是甲骨文公司一款非常强大的企业管理软件。用户可以从这款迎合了新的企业管理需求并涵盖了业界领先技术的产品中大大受益。

11i.10提供了功能丰富的纵向行业解决方案,继续增加了众多横向产品功能,具有绩效管理的集成功能,还能保证低成本集成和实施。而且,这款管理软件还新增了2100项功能,其中50%为行业功能,50%为跨行业功能,有些功能还是专为新型企业应用而设计的。

而且,11i.10全面支持高科技行业的RosettaNet协议、医疗保健业的HL7协议、金融服务业的Basel II协议、电信业的配置自动化功能、物流行业的射频识别以及制造业的精益制造功能。

应用层的安全盾牌

TrafficShield是F5网络公司推出的一款优秀的应用层安全管理设备,可以保护企业组织用户的应用系统免受黑客及其他的恶意攻击(包括零日攻击)。该产品可为企业应用系统提供全面的保护,防御那些可绕过传统的边界防护攻击Web应用系统,进而非法访问公司网络的黑客。

F5公司的TrafficShield解决方案中应用了与网络防火墙、入侵检测系统及其他安全设备中使用的消极安全逻辑相反的积极安全模型,在阻止黑客篡改系统的同时,还可确保用户安全、无限制的访问所需要的信息。

而且,该产品应用的应用流程模型(AFM)利用积极安全逻辑,根据用户会话信息、内容及应用响应内容对每一个事务进行验证。

加速补丁管理进程

在充斥着黑客、病毒的网络世界中,存在漏洞的计算机无疑是一枚“定时炸弹”。不过,给一台计算机及时打补丁不是一件难事,但如果要同时给成百上千的计算机及时打上补丁就不那么容易了。很可能,您只来得及给很少的计算机安装上补丁,您的网络就已经被黑客或病毒攻陷了。如何清除网络内各台计算机的漏洞及补丁状况?如何更快地为每一台计算机打补丁?LANDesk补丁管理器是个不错的帮手。

LANDesk补丁管理器是一个可更新的服务,能对异构的IT环境自动进行安全漏洞评估和补丁管理,建立和维护操作系统、应用系统和应用程序的安全基线、稳定性和性能。

在它的帮助下,IT人员能够通过主动的安全漏洞扫描实现系统的快速评估,可以依据业界标准的信息数据来源来定位安全漏洞,研究、回顾和下载可用的补丁,通过自动定位和补丁分发高效修补已知的安全漏洞,可以建立主动的管理策略来自动保持当前的补丁更新。 ■

华硕 VPN 路由器： 灵活、安全、高效

网络已成为我们工作和生活中基础工具，企业各种应用也都在网络上进行，但是在安全性和传输的性能要求上也更高，对安全性要求高的业务获得了极大的增长空间。其中VPN技术已经能够提供足够安全的保障，可以使用户数据不被查看、修改。VPN (Virtual Private Network)：虚拟专用网络，是一门网络新技术，为我们提供了一种通过公用网络安全地对企业内部专用网络进行远程访问的连接方式。VPN由客户机、传输介质和服务器这三部分组成，不同的是VPN连接使用隧道作为传输通道，这个隧道是建立在公共网络或专用网络基础之上的。总的来说，VPN具有以下显著优点：

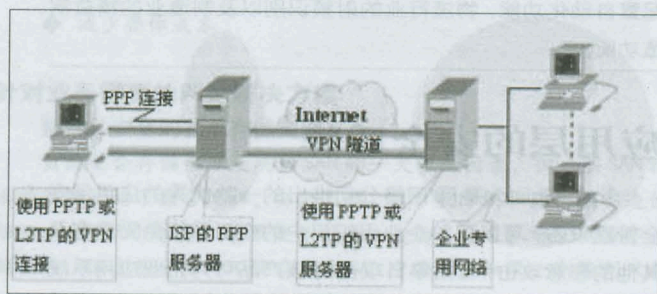


图1 VPN网络图

安全可靠

VPN可以利用隧道技术和加密技术对通过隧道传输的数据进行加密，以保证数据仅被指定的发送者和接收者了解，从而保证了数据的私有性和安全性，确保其VPN上传送的数据不被攻击者窥视和篡改，其隧道技术和加密技术是否具有高安全性。

服务质量保证 (QoS)

VPN网应当为企业数据提供不同等级的服务质量保证，由于广域网流量的不确定性使其带宽的利用率很低，在流量高峰时引起网络阻塞，使实时性高的数据得不能及时发送；而在流量低谷时又造成大量带宽空闲。对此问题VPN在网络优化方面，采取过流量预测与流量控制策略，可以充分有效地利用有限的广域网资源，可以按照优先级分配带宽资源，使得各类数据能够被合理地先后发送，并预防阻塞的发生。

高扩展性能

VPN必须能够支持通过网络的任何类型的数据流，方便增加新的节点，支持多种类型的传输媒介，可以满足同时传输语音、图像和数据等新应用对高质量传输以及带宽增加的需求。

方便管理性能

VPN使用需要可方便地进行管理、维护，VPN要求企业将其网络管理功能从局域网无缝地延伸到公用网，甚至是客户和合作伙伴，因此VPN管理系统是必不可少的，主要包括安全管理、设备管理、配置管理、访问控制列表管理、QoS管理等内容。

可以想象，VPN将会成为我们网络生活的主要组成部分。在不远的将来，VPN技术将成为广域网建设的专业解决方案，它不仅会大大

节省广域网的建设和运行维护费用，而且增强了网络的可靠性和安全性。同时，VPN会加快企业网的建设步伐，使得集团公司不仅仅只是建设内部局域网，而且能够很快地把全国各地分公司的局域网连起来，从而真正发挥整个网络的作用。VPN对推动整个电子商务、电子贸易将起到不可低估的作用。

华硕SL-500，SL-1000系列产品是华硕电脑公司为帮助企业建立安全、灵活、高效的虚拟专用网而推出的VPN路由器。相对一些非VPN设备，华硕VPN路由具有以下特点：

高度的灵活性

1) 用户不论在家中、在出差途中，或是在其它任何环境中，只要该用户能够接入Internet，便能够安全地



图2 华硕SL-500，SL-1000系列产品

接入企业网内部。既不受地域限制，也不受接入方式限制。

2) 用户可以选择使用本地服务提供商所能提供的任何宽带接入技术，不论是ADSL、Cable Modem，还是在信息化小区或酒店中使用以太网接入。

严格的安全性

所有的流量均经过加密和压缩后在网络中传输，采用先进加密技术，为用户信息提供了更高的安全性保证。

1) 具有超高的封包穿透效率，而且支持5或25条VPN高速通道，充分保证数据传输的速度和质量。5或25条隧道，在一个隧道中又可以建立很多会话数量，这样保证了传输的高效率。

2) 华硕VPN路由器的安全协议支持最新基于IPsec的管理协议，另外还支持多种安全协议，充分保障了信息传输的安全性。

方便的管理性

- 1) 支持DHCP客户端管理
- 2) 支持WAN/LAN配置端口管理
- 3) 支持Web浏览器管理

ASUS®
华硕品质·坚若磐石

华硕电脑网络通信事业部

地址：北京市海淀区海淀路52号（北大太平洋科技大厦13层）

邮编：100080

电话：010-82667575

传真：82667312

技术支持：010-8008206655

网址：www.asus.com.cn

■ 北京 剑屏

41

扑管理、图形化操作界面、实时声光报警、中文操作系统的同时,利用华为组管理协议可以实现对数量庞大的楼层交换机的动态发现、动态拓扑生成、自动配置的功能,降低网络管理人员的工作量,提高效率。

丰富的资费策略:提供多种资费策略,包括:按时长计费、按流量计费、按带宽计费,并且提供预付费业务和多种折扣策略,针对学校特殊情况,支持按不同ISP分别计费的能力。

完整的业务控制层:在提供网络互联解决方案的同时,也提供统一网络管理平台、校园网业务管理平台和视讯平台,提供软硬结合的马上可以开展校园业务的整体解决方案。

强大的WLAN解决方案:可以实现布线困难区域,如两栋教学楼之间的无线连接;可以提供空旷地区,如操场或礼堂的网络覆盖;可以提供在教学区,如教室、图书馆的无线信息口。提供完整的AP、无线网卡、天线系统、功率放大器系统、无线网管和配置软件包等WLAN接入方案。

多接入方式的提供:考虑到学校实际线路情况和资金情况,不一定都选择以太网接入手段,可以考虑利用电话线、电磁波,甚至有线电视线缆作为数据承载介质,以降低投资。所以华为3Com公司除提供以太网接入方式之外,还提供ADSL、VDSL、WLAN、有线宽频等可选技术方案和产品。

校校通和教育骨干网解决方案

校校通网络也同样存在着用户管理和业务开展的需求,与上面的校园网需求存在着共性。但因为校校通城域网和教育骨干网涉及到广域网络的建设,如教育城域网和教育骨干网建设,所以网络分为校园局域网和广域互联两级结构,校园局域网结构与上述校园网结构类似,广域互联可以采用网关设备,如路由器、三层交换机完成星型组网,利用RPR技术完成环行组网,或者利用传输设备或WDM设备进行环行组网,华为3Com公司可以提供任何一种符合建网需求的解决方案和产品。

高安全、高性能、高可靠:提供高吞吐量、线速转发的核心路由器和三层交换机;所有关键器件的冗余,包括主控板、交换网板、电源、时钟等;支持板件的热插拔;支持软件的热补丁和热升级,在不中断业务的情况下,实现平滑升级;支持

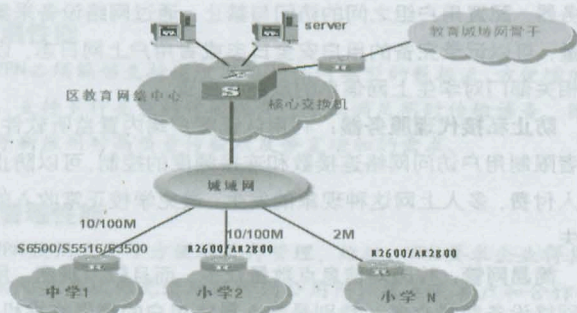


图2 校校通组网图

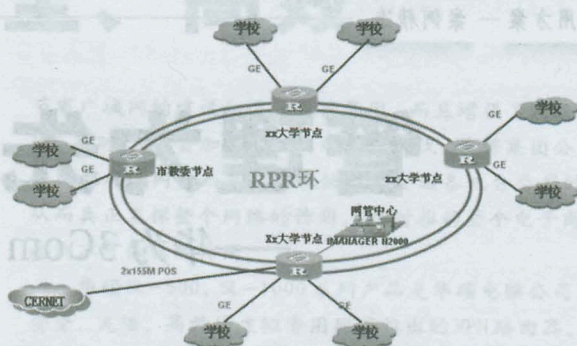


图3 教育城域网RPR组网图

设备的冗余备份协议VRRP,以及链路捆绑和等价路由,具有更高的安全性。支持弹性分组环RPR,实现环型网络的快速收敛;提出的基于时间、空间和网络层次的三维端到端安全网络,利用通用防火墙和网络设备共同构建教育安全网络。

强大的业务能力:DHCP RELAY和内置DHCP SERVER,对用户IP地址实行动态分配和管理;大容量高速NAT;通过内置Web Switch提供L4负载均衡、L5/7负载均衡、Web Cache Redirection等功能。

强大的组网能力与兼容性:拥有从核心层、汇聚层到接入层丰富的路由器和以太网交换机系列,既有电信级可靠性的网络设备,也有简单网管型,甚至无管理型的网络设备。同时网络设备具有丰富的互联接口,可以满足复杂环境中的设备互联;提供有线无线一体化解决方案;提供LAN、WLAN等接入方式进行网络互联,实现笔记本教室、无线会议室、空中图书馆的构建;完全支持国际与国家标准,具有互联互通能力。

技术先进:核心设备采用业界领先的第五带路由器技术,集成网络处理器的核心设备可以利用微处理引擎实现加载业务后的高效转发,而专用的网络CPU又可以实现新技术和新功能的加载。

性价比高:采用专为校园网设计的智能三层交换机产品,具有运营级可靠性,先进的路由最长匹配技术(逐包转发机制、路由最长匹配技术)以及高度灵活的系统资源配置,并可以实现精细化的用户管理,具有极高的性价比。

支持多种接入方式:提供灵活的十兆、百兆、千兆到桌面的接入方案,同时可以提供WLAN无线局域网的无缝接入方案。

MPLS VPN特性:支持MPLS VPN技术,实现校校通网络的数据、视频和IP语音的三网合一。支持三层的MPLS VPN和二层的MPLS VPN,同时提出了业界领先的HOPE技术,使得MPLS VPN网络具有更智能的层次感,对接入设备的能力要求进一步降低,特别适合校校通开展MPLS VPN业务。

功能强大的QoS:实现了流分类、流量监管、拥塞控制、队列调度和输出流整形等功能,提供一种用户可选的新拥塞控制方法——SA-RED,比传统的WRED能更平滑地处理流量抖动。其强大的队列功能和输出流整形能更好地满足多种业务流特性,真正做到业务区分和保证,提供完善的DiffServ/QoS支持。INI

“我的网络我设计”

第二届校园网方案设计大赛获奖方案展

■ 北京师范大学珠海校区 汤建

北师大珠海校区二期网络建设的总体目标是利用各种先进成熟的网络技术和通信技术,采用统一的网络协议,建设一个可实现各种综合网络应用的高速计算机网络系统,将教育系统内各院、系、行政管理部门通过网络连接起来,通过园区网骨干节点与CERNET、Internet相连。该高速宽带网可为用户提供可靠的、高速的和可管

理的网络环境,在网上为各院、系、行政管理部门提供广泛的资源和数据共享、丰富便捷的网络应用,提供各种网络服务,可为各用户提供多种形式访问形式,实现最大化信息资源、教学资源、设备资源的共享。在网络的建设上努力实现网络的扩展,扩大联网的范围和规模,实现园区网的全面入网。

建设目标

学校二期网络建设要求建成能实现除现在网络上的一般功能:如E-mail、FTP、网络论坛、网络图书馆、搜索引擎、网上聊天、管理数据的传输、处理与查询外,还应包括视频点播、实时远程教学、网络学校、电视会议、网络电话等功能,是一个高速多媒体互联网,实现整个教育系统的资源共享,做到网内设备园区网都能共享,设备利用率大大提高。并在网络核心层上,可建立一个信息容量的数据中心,为基础教育、成人教育和继续教育提供信息资源服务。

根据本网的发展要求,还可以在一年两年的时间里,将几个不同的Internet出口接入本网的其他不同核心节点。从而扩大本地区园区网出口带宽,也实现出口链路冗余备份和负载均衡。

方案实施

学校的二期网络建设结合实际建网情况和一期网络建设,设计“千兆主干、支干千兆、百兆交换桌面”的网络拓扑结构。根据实际应用和长远设计,为保证整个网络系统的高效率、高可用性、高可靠性和高稳定性为前提,在原有网络架构基础上,再增加三台核心路由交换机,在图书馆、学生宿舍、教工公寓各设一个网络中心,选用三台高性能的锐捷STAR-S6808的多层交换机和原有的网络核心层交换机,构成学校的网络核心层,共设计为六个核心的环状互连结构,生活区、新学生宿舍、教工公寓分别和教学楼、图书馆组成一个环,任何一个方向的链路出现故障,都可以通过OSPF的自动路由学习切换到其它可用链路,保障网络的继续传输。网络的子网交换在各核心处理,网形成。链路聚合功能技术也体现了产品的可扩展性能,能充分利用现有设备实现高速数据传递。本期设计全双工高达4G的带宽。同时设计为两个互连网出口,一个CERNET,一个ChinaNet,设计一个出口接在教学楼,另一出口接在图书馆,这样网络设计更加灵活,然后根据策略路由,可以使出口负载均衡和冗余备份更加优越。



在二期网络建设中,由于在学校二期网络建设中,接入信息点集中,同时学校的应用多元化,要求接入层的设备端口高密度和设备的高性能、多功能等特点。针对以上特点,我们在设计网络结构时,采用三层网络结构。由于每栋楼的信息点都比较集中,而且相对较多,在各栋楼选用汇聚设备,设立一个汇聚交换机,千兆光纤下连各

接入交换机,这就要求汇聚交换机具有高密度的光口,高速的交换能力,具有多种路由协议。在汇聚层选用STAR-S3550-12G交换机,12个GBIC千兆接口,48G的背板带宽,RIP v1/v2,OSPF等路由协议。

学校在二期的网络实施完成后,在确保实用性和经济性可扩展性和可管理性、安全性和保密性、可靠性和稳定性的基础上还可以实现以下功能,充分满足学校的实际的应用需求。

高性能需求 多媒体交互教学,以及VOD等媒体流应用对网络的性能要求是很高的。因此要求构建学校网络的组网技术必须是高带宽的组网技术;骨干交换设备必须支持线速交换,以保证无阻塞的数据交互;另外从网络结构设计上,需要考虑到一些高流量多媒体应用的分布式部署,以降低跨骨干网的流量,提高网络的性能。

关键业务服务质量保证需求 由于教育系统的特殊性,其应用类型几乎涵盖了Internet所有的应用类型,包括:Email、FTP、网页浏览、数据库查询、协同计算机辅助设计、协同计算机辅助教育、基于计算机的教育、协同研究、远程教育、视频广播、视频点播、VoIP以及视频会议等等应用类型。校园网中有各种各样的应用业务数据流,当网络流量处于高峰期时,必定会影响关键业务数据流的响应时间,对于多媒体业务来说就会有说话结巴、图像马赛克的情况。因此高性能的网络,也需要QoS技术,保证任何时刻都能对关键业务提供优质的传输服务。

网络安全需求 全网接入认证,对于我院校园网的安全保障十分重要;另外我院校园网的网络安全,还需要考虑与外网及内网不同应用系统之间的安全访问控制。

方案点评:

本方案在充分利用原有设备的基础上,考虑了网络的未来发展和可升级性,同时充分满足了当前校园网的各种需求,是非常切合实际的解决方案。

——“经典100工程—校园网方案设计大赛”评审委员会



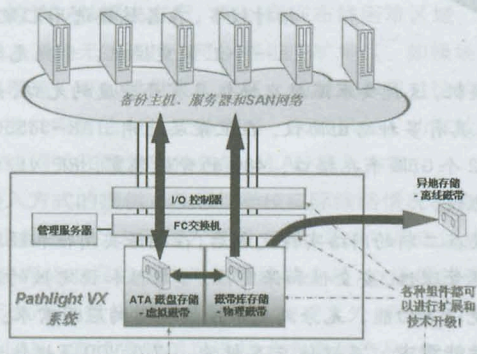
锐捷网络网址: www.ruijie.com.cn

先进、完善的磁盘—磁盘—磁带 (DtDtT) 数据备份系统

——ADIC Pathlight VX 技术介绍第四辑

ADIC Pathlight VX 体系结构

Pathlight VX集成了ADIC公司多种世界领先的数据存储和备份技术,如SAN I/O控制器技术、虚拟磁带机技术、高性能SAN共享文件系统和数据迁移技术,以及领先的磁带库产品。从而使Pathlight VX具备满足企业级用户需求的DtDtT数据备份体系结构。



集成的模块化 (DtDtT) 数据备份系统

一般的DtDtT集成系统将虚拟磁带、设备管理、磁盘到磁带的I/O管理和数据存储策略等功能全部由一台服务器实现,容易形成性能和技术瓶颈,不利于系统的今后在性能、容量方面的扩展、以及未来技术的升级。ADIC Pathlight VX采用模块化的设计结构,将DtDtT系统的主要功能由不同的组件实现。包括:

- ◆ 管理主机—负责对存储设备的管理以及内部数据复制、迁移策略的制定和执行;

- ◆ I/O控制器—负责实现虚拟磁带/磁带机功能和处理数据I/O操作。Pathlight VX可以根据实际需求配置多台I/O控制器,并且通过技术升级实现更高的性能和SAN网络连接方式;

- ◆ FC交换机—负责为管理主机、I/O控制器、磁盘阵列、磁带库提供内部高速数据传输通道,数据在磁盘、磁带之间复制、迁移不占用外部主机、SAN网络的资源;

- ◆ 磁盘阵列—采用多台配备冗余控制器的EMC CX300磁盘阵列并行工作(最大RAID后容量为46.8TB),可以大大提高数据吞吐率和存储容量,并且可以通过技术升级满足未来更高的性能和容量的要求;

- ◆ 磁带库—ADIC公司是世界上领先的智能磁带库供应商,其Scalar系列磁带库都可以连接到Pathlight VX系统中,实现数据自动化复制、迁移、离线存储和容灾功能。

高性能的 (DtDtT) 数据备份系统

由于Pathlight VX采用了模块化设计,内部具有高性能的FC交换机,从结构上消除了性能瓶颈,例如消除了一般系统的DtD和DtT带宽不匹配的问题。当前的Pathlight VX的系统吞吐量可以达到每小时2TB,无论正常的磁盘到磁盘的数据备份和恢复,还是磁盘

到磁带的拷贝、迁移,系统带宽都可以达到2TB。同其它系统相比,可以缩短创建物理磁带或从物理磁带进行数据恢复的时间。这个数值是通过商业备份软件进行实际数据备份和恢复操作测量出来的,不是通过理论计算或专用工具测试出来的。

扩展灵活的 (DtDtT) 数据备份系统

Pathlight VX将磁盘阵列和磁带库透明地集成在一起,对备份软件形成一个可以不断扩展的虚拟磁带库系统。备份软件不知道物理磁带库的存在,从而降低了用户设备管理的复杂性和软件购买的成本。Pathlight VX磁盘和磁带的存储容量比例可以根据用户对数据备份/恢复的性能、数据保存时间的不同要求进行调配。整个系统从3.8TB可用存储容量和每小时600GB吞吐率,逐步扩展到接近3,000TB可用存储容量和每小时2TB吞吐率的系统。随着技术的快速发展,可以通过升级、更换Pathlight VX的内部组件达到性能、容量的扩展和技术升级,从而保护用户的投资。例如,当新型的SAN网络技术出现时,可以通过升级I/O控制器将Pathlight VX接入该网络,达到技术和性能的升级,而去不必更换Pathlight VX中其它的组件。

完善的 (DtDtT) 数据备份系统

Pathlight VX具有完善的数据保护、快速恢复和容灾等功能。内置的数据存储管理策略可以实现如下功能:

- ◆ 提前创建虚拟磁带的物理磁带副本—加快物理磁带的创建和出库保存操作的速度;

- ◆ 出库磁带的格式和条形码带标与备份软件规定的完全一致—出库磁带可以脱离Pathlight VX系统进行数据恢复,从而实现真正的数据容灾功能;

- ◆ 虚拟磁带的内容可以复制多达4盘物理磁带当中—提高数据冗余度,防止磁带介质出错而丢失数据,同时还可以加快从离线磁带恢复数据的速度;

- ◆ 多种数据恢复方式—可以选择从虚拟磁带、磁带库中的物理磁带和离线的物理磁带中进行数据恢复。其中离线的物理磁带可以在另外的磁带机、磁带库中进行数据恢复,做到在整个Pathlight VX系统失效情况下的数据恢复。

ADIC 北京代表处

地址: 北京东三环北路南银大厦 815 室

电话: 010-64106840/1/2/3

网址: <http://www.ADIC.com.cn>



Intelligent Storage™

安全高效并重的企业网

■ 河南 刘志都

乐凯集团第二胶片厂早在1985年就已开始微机信息管理系统的开发与应用,随着应用范围的逐步扩大和推广,于1990年建立了当时在技术上还很先进的细缆总线型网络,该网络系统的总线部分连接办公楼和研究楼,由于受总线长度的限制,各车间的微机是作为远程工作站通过公用电话网进行数据传输的。近年来随着用户的增多、业务范围的扩大、应用的深入以及总线型网络本身的缺陷,该系统已不能满足当今企业信息化建设的需要,所以建立一个覆盖全厂的高性能的网络系统势在必行。

网络需求分析

根据第二胶片厂信息中心提出的具体需求,系统建设的主要目的是建立全厂的计算机信息管理系统;组成现代化的办公环境;实施ERP系统;创建企业Web站点;设立邮件服务器;由于销售网点遍布各地,应能方便快捷地传输当天的各类销售数据等。因此该网络系统应为宽带IP网,且系统应具有较高的可靠性、稳定性和安全性。对内连接各管理处室和生产车间,建立企业内部网Intranet,对外连接Internet。

从目前网络市场来看,各种网络技术及联网方式参差不齐,种类繁多。千兆以太网、快速以太网则是最为流行的建网方案,它提供了常规以太网10~100倍的带宽,采用CSMA/CD介质访问方式,兼容原来的常规10Mbps方案。因此利用千兆以太网、快速以太网技术组网是一种比较成熟的高速网解决方案。依据以上要求及该厂建筑物分布情况,结合当今网络技术、通信技术发展状况,架构一个覆盖该厂主要建筑物的高速光纤网。根据以上分析和方案论证,兼顾经济、实用的原则,最后确定主干网通信介质采用6芯多模光纤,交换式1000M带宽为主干,交换100M带宽到桌面,并通过租用中国电信的10M光纤联接Internet。

设备选型

网络设备是整个网络系统的通信核心,因此,网络设备的选择十分重要。根据系统需求分析,通过多个网络选型方案比较,遵循实用性、可靠性、先进性、安全性、可扩充性、经济性的原则,最终确定选用3Com公司的交换机。其中选用SuperStack 3 Switch 4900SX交换机作为核心交换机,该

交换机采用模块化体系结构,具有稳健的可用性,包括链路聚合、快速生成树支持、冗余电源系统及对XRN技术的支持,可确保关键应用的最大运行时间。它带有12个1000BASE-SX端口,具有第三层交换功能,支持VLAN划分。二级交换机采用SuperStack 3 Switch 4400SE,根据需要配上1至2块1000Mbps光纤模块,该交换机带有24个10/100Mbps自适应以太网接口,支持VLAN划分。选用SuperStack 3 Switch 3300XM交换机作为三级交换机,它带有24个10/100Mbps自适应以太网接口,支持VLAN划分。该网络系统共采用SuperStack 3 Switch 4900SX交换机1台,SuperStack 3 Switch 4400SE交换机18台,SuperStack 3 Switch 3300XM交换机14台,光纤收发器16台。

在防火墙的选型上,考虑到整个网络系统要对外连接Internet,所以系统在安全防范方面尤为重要,因此,选用Cisco公司的Cisco PIX-515硬件防火墙来实现内外网用户之间的访问控制、网络地址转换、信息过滤等功能。

为保证系统安全、可靠的运行,在网络管理中心的供电方面,不间断电源的使用是必不可少的,这里选用SANTAK公司的CASTLE 6KVA不间断电源,在断电的情况下,可保证为网管中心的服务器、交换机等网络设备供电4小时左右。

网络设计方案

根据第二胶片厂的实际应用需求,整个企业网的拓扑结构如图1所示。

该网络设计构造采用交换式以太网技术,网络主干采用1000Mbps交换技术,二级和三级交换机采用交换式100M带宽到桌面。该设计方案中传输介质主干采用6芯多模光纤,具有一定的冗余性和可扩充性;各楼层内和车间内的信息点采用超5类UTP(非屏蔽双绞线),能够满足将来网络的扩展。整个网络拓扑结构为星型,星型结构便于维护,某一点或某一个子网的非正常运行不会干扰其它工作站的正常工作。

具体方案为:在办公楼网管中心采用一台3Com SuperStack 3 Switch 4900SX交换机作为核心交换机,在网管中心、办公楼9楼、研究楼、涂布车间、片基车间、PS版车间、立体仓库等单位各采用一至两台SuperStack 3 Switch 4400SE作为二级

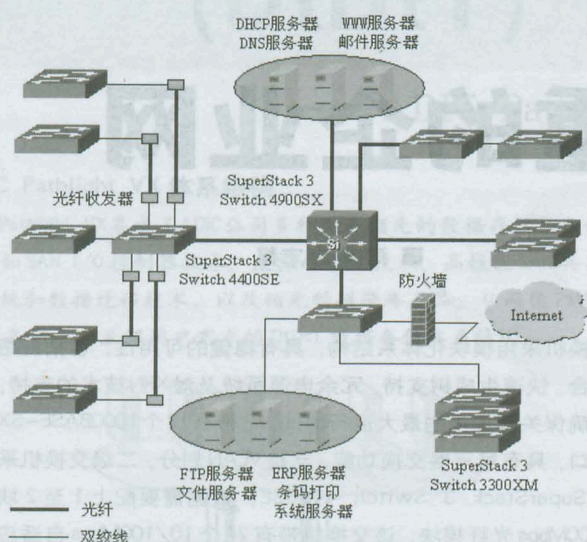


图1 网络拓扑图

交换机, 同时在 SuperStack 3 Switch 4400SE 交换机上根据实际需要安装一至两块千兆光纤模块与核心交换机实现1000Mbps互联。其它车间由于分布在立体仓库附近, 为了节省费用并兼顾今后设备更新及发展的需要, 利用立体仓库的二级交换机采用光纤收发器的方式, 分别通过光纤连接CTP车间、有机车间、电气车间、树脂车间、水汽车间、净化车间、培训中心等单位的三级交换机, 实现100Mbps互联。在办公楼、研究楼等信息点比较多的地方, 通过二级交换机向下级联SuperStack 3 Switch 3300 XM 三级交换机来扩展用户接口, 实现100Mbps互联。由于Cisco PIX-515 硬件防火墙的内网卡和外网卡分别为10/100Mbps以太网卡, 所以防火墙内连网管中心的二级交换机, 外连租用中国电信的10M光纤(使用光纤收发器转换为RJ-45以太网接口, 通过双绞线连接)。

考虑到位于立体仓库的SuperStack 3 Switch 4400SE二级交换机所连单位较多, 在该交换机和核心交换机之间采用链路聚合技术, 通过两条1000Mbps光纤链路相连, 从而实现链路冗余, 并将两个交换机之间的带宽提升到2Gbps, 确保了该条线路有更高的可靠性和可用性。

核心交换机除了与二级交换机实现1000Mbps互联外, 还连接着对带宽和可靠性要求较高的服务器。二级交换机和三级交换机负责为分布在各节点上的用户提供100Mbps的带宽联接, 包括桌面工作站和打印服务器等。整个系统为文件传输、办公自动化、ERP系统、Web服务、邮件服务等系统提供了足够的带宽和较高可靠性。

在网络安全方面, 采用硬件防火墙把内外网隔开, 通过系统设置实现网络地址转换、静态IP地址映射等, 保证内部IP地址、信息资源不会被非法获取。从而有效地防范来自外部网络的攻击。在内部局域网的安全上, 除ERP系统、商标打印系统有自己的用户验证系统外, 还建立了内部域名服务器来实现对

用户的验证。同时利用 SuperStack 3 Switch 4900SX 核心交换机的虚拟局域网 (VLAN) 技术和第三层路由技术, 结合 DHCP 服务, 在交换机上划分 VLAN, 使连入网络的主机位于特定的 VLAN 中, 这不但有效地隔离子网内的大量广播, 提高网络性能, 而且隔离子网之间的通信, 控制了资源的访问权限, 提高了内部网络资源的安全性。

整个网络系统通过综合布线及设备安装调试完成后, 形成一个以1000Mbps光纤为主干, 覆盖全厂主要建筑物的企业网, 并通过防火墙与Internet互连。

网络特点

1. 实用性 对企业来说, 管理信息系统的实用性永远是第一位的。整个网络系统的设计是依据先进性与成熟性并重的原则, 既考虑要防止单纯追求先进性而受国外厂商误导的趋向, 同时在主要产品和技术的选择上也考虑应选用主流厂商的产品技术。目前该系统已全部完成, 并交付使用。企业自行开发的各种信息管理系统、用友ERP系统、商标及条码打印等应用系统都在依靠该网络运行。企业Web站点、邮件服务器、FTP服务器也已通过该网络系统投入运行。整个系统性能稳定, 安全可靠。

2. 安全性 主要通过对交换机的设置, 采用VLAN技术和Cisco PIX-515 硬件防火墙来提高系统的安全性。交换机可以解读数据包中的高层信息, 支持基于数据包中的MAC地址、IP地址、端口号等信息设置包过滤器, 完成对数据流的管理和控制。采用虚拟局域网技术, 将整个网络按部门划分为12个VLAN, 利用核心交换机的三层交换功能, 对网络进行分段管理, 实现各网段间数据传输的安全控制。从而保证不同职能部门管理的安全性和方便性。选用Cisco PIX-515 硬件防火墙, 通过设置限制内外网用户的访问, 过滤掉不安全的服务和非法用户, 避免来自外部的攻击, 从而有效的保护内部资源, 提高系统的安全性。

3. 可扩充性 本方案中的网络设备能方便地进行容量扩充, 如核心交换机3Com SuperStack 3 Switch 4900SX, 采用模块化体系结构, 可以利用可选的千兆交换模块对系统进行扩展, 并且可选的千兆交换模块可以混用, 从而匹配光纤及铜缆千兆介质, 在一个简单的集成式平台中提供经济高效的性能。SuperStack 3 Switch 4400交换机的背面均有两个可扩展槽, 用户可以根据自己的需要, 灵活选择各种千兆接口模块、百兆光纤模块或堆叠模块, 以提供堆叠扩展和高带宽网络接口。总之, 该网络方案采用目前计算机网络领域先进、成熟的技术, 主干网络设备能够随着网络技术的不断发展而平滑升级。

4. 开放性与标准化 开放性与标准化原则是一个系统赖以生存和发展的基础, 我们在规划和建设时, 也充分考虑了这一点。所有网络设备都支持各种标准的网络和接口协议, 使系统具有良好的开放性, 从而有效地保护用户的投资, 体现出良好的可扩展和互操作能力。

让校园应用跑起来

——上海市黄浦区市南中学校园网升级方案

■ 上海市黄浦教育信息中心 徐俊

黄浦区是国家教育部认定的“全国中小学信息技术教育实验区”，在推进教育信息化方面一直处于领先地位。为了更好地使信息化带动教育现代化，实现教育的跨越式发展，2003年年底黄浦区教育信息中心决定对一部分1999年以前建设校园网的学校进行网络升级，以便更好地实现IP宽带交互教学、视频点播等城域网关键业务。

市南中学原有的校园网建于1998年，当时共有2百多个信息点，主干千兆，千兆到桌面，核心交换机以及汇聚层交换机均采用Intel Express 510T Switch，接入层采用Intel Express 140T Hub，一根千兆光纤到科技馆大楼。随着现代化教学活动的开展和与国内外教学机构交往的增多，通过Internet/Intranet网络进行信息交流的需求越来越迫切，为促进教学、方便管理和进一步发挥学生的创造力，原校园网络已经不能适应，网络升级是必然的选择。

市南中学现有综合大楼（网管中心位置）、教学大楼、办公大楼、图书馆大楼、科技馆大楼、艺术楼、东楼、门房等8个独立楼宇，其中综合大楼中还有清新民校、育新民校，这两个学校也要通过市南中学连接Internet，但需要将三个学校进行有效隔离，使得各学校的局域网相对独立。

经过对各个厂家各种网络产品的性价比、售后服务及技术支持等各种因素的综合考证，学校决定选择锐捷网络（原实达网络）的产品，通过同锐捷网络的通力合作，使得上海市黄浦区市南中学校园网从千兆主干升级到千兆主干得以圆满完成。

升级后的校园网采用了锐捷网络的千兆以太网解决方案，同时延用了原有网络稳定可靠的星形拓扑结构，原交换机全部作为接入层交换机，Hub全部淘汰。核心层、汇聚层和接入层经过精心设计，最终选择了锐捷网络的STAR-S4909全模块化的核心骨干路由交换机作为核心交换机，STAR-S1926G+千兆增强网管交换机作为汇聚交换机，STAR-S1824+和STAR-S1808M快速以太网交换机作为接入交换机，以充分发挥千兆主干、千兆到桌面的快速转发能力，使网络性能得到优化。

升级后，将该校园网分为三级结构：以位于综合大楼内的校园网控制中心为核心，并在将来需要时可以升级到万兆；与校园内各建筑（校园内需要联网的建筑物共有8座）互连形成园区主干；各建筑物内部再扩展面向用户的局域网子网。园区主干连接为千兆或千兆光纤，综合大楼内部主干连接为千兆超五类线双绞线，建筑物内部的用户子网提供到桌面的100Mbps网络带宽。升级后的校园网共有四百多个信息点。

网络需求特点

◆ **高接入带宽**：校园网应以较高带宽接入黄浦区教育信息中心，以便共享区信息中心的网上资源。学校能够积极利用在区教育信息网上的各种应用平台，实现各项应用。

◆ **大容量、高速率的数据传输**：校园网的核心是面向校园内部师生的网络，信息中包含大量多媒体信息，所以大容量、高速率的数据传输是网络的一项基本要求。

◆ **IP地址、域名的统一管理**：校园网的IP地址、域名等由区教育信息中心统一管理和分配。

◆ **教学多业务支持**：信息结构的多样化，校园网应用分为电子教学（多媒体教室、电子图书馆等）、办公管理、资源库和远程通信（IP宽带交互教学、视频点播、互联网接入）四大部分内容。电子教学包含大量多媒体信息，办公管理以数据库为主，远程通信则多为www方式，不同类型的数据对网络传输有不同的质量需求。

◆ **高安全需求**：校园网中同样有大量关于教学和档案管理的重要数据，不论是损坏、丢失还是被窃取，都将带来极大的损失。

◆ **易管理需求**：校园网面向不同知识层次的教师、学生和办公人员，应用和管理要简便易行，界面友好，不宜太过专业化。

网络升级设计原则

校园网络系统的设计应采用国际通行的TCP/IP协议，并达到以下目标：

◆ **先进性**：采用先进的设计思想、网络结构、开发工具，以及市场覆盖率高、标准化和技术成熟的软硬件产品。

◆ **实用性**：建网时应充分考虑利用和保护现有资源，充分发挥设备效益，要保证系统和应用软件全中文界面，且功能完善、界面友好、兼容性强，使用户最方便地实现各种功能。

◆ **开放性**：系统设计应采用开放技术、开放结构、开放系统组件和开放用户接口，以利于网络的维护、扩展升级以及和外界信息的沟通。

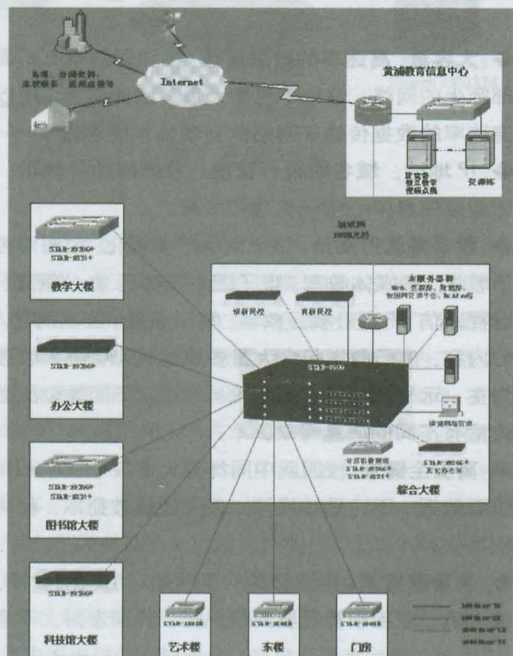
◆ **适应性**：采用积木式模块组合和结构化设计，使系统配置灵活，使网络具有强大的可增长性，方便管理和维护。

◆ **可扩展性**：网络规划设计要满足校园不断发展的

要求,还要满足因技术发展需要而实现低成本扩展和升级的需求。

◆ **可靠性:** 具有容错功能,能满足学校所在地的环境、气候条件,抗干扰能力强,对网络的设计、选型、安装、调试各环节进行统一规划和分析,确保系统运行可靠。

◆ **安全性:** 要注意各环节的安全保密性能,提供多层次安全控制手段,建立完善的安全管理体系,防止关键数据受侵袭和破坏,有可靠的防病毒、防黑客措施。系统应具有对主要环节的监视和控制功能,严防计算机病毒和非法用户的越权操作,做好系统内权限的分级管理,具有较强的容错和故障恢复能力。



校园网整体拓扑结构图

◆ **经济性:** 投资合理,有良好的性能价格比。

校园网升级建设方案

通过细致的规划和多次论证,市南中学的校园网升级方案最终确定了采用锐捷网络提供的设备,具体如下:

核心交换机选用了 STAR-S4909, 加 4 口 100BASE-SX、1000BASE-LX 光纤模块以及 1000BASE-TX 百/千兆接口模块作为主干交换机。主干交换机通过千兆光纤分别下连校内的教学大楼、办公大楼、图书馆大楼、科技馆大楼等二级结点,从而形成千兆网络主干,对于综合大楼内部信息点较多的子网,其主干连接为千兆超五类线双绞线,由于艺术楼、东楼、门房等信息点少于 8 个,故采用百兆光纤连接。

汇聚层设备选用了一款全线速千兆增强网管型交换机 STAR-S1926G+, 具有 2 个扩展槽;支持百/千兆、光/电

口上联;支持 IGMP Snooping 组播协议,以减轻多媒体应用中视频流对带宽的占用;支持带宽分配,以减小主干的压力;支持标准网络管理协议 (SNMP), 提供中文化的网管界面,实现端口管理智能化;采用业界最先进的 802.1x 安全接入控制策略;支持业界领先的 EAPS 功能,实现网络的高可用性;支持 802.1p、端口优先级等多种 QoS 策略。在保证千兆带宽的同时,利用原有的布线系统,保护用户的投资,同时充分利用其功能,实现负载均衡,有效降低了核心交换机的路由压力。

接入层设备选用了锐捷快速以太网交换机 STAR-S1824+ 和 STAR-S1808M, 它们具有自适应 RJ45 的交换端口,所有端口可以根据连接的设备,自动将连接速度和工作模式调整到需要的方式,无须更改网络结构,对于学校应用广泛的多媒体广播教学完全适用,全系列产品采用业界先进的高容量超高速背板设计,能以全端口、全线速的模式进行数据传输,满足了校园网的应用。

方案特点

通过采用锐捷网络的千兆以太网解决方案,完成了市南中学校园网的升级工程,在安全性、业务的支持程度和网络管理等方面达到了很高的水平:

◆ 千兆以太网取代原有的百兆以太网,为用户提供了一个全新的、先进的网络平台,提高了工作效率。核心层、汇聚层和接入层都采用全线速的设备和模块,全面提高了整个网络的性能;

◆ 在原有布线系统的基础上进行的网络改造,有效保护了用户投资,最大限度缩短了工程时间,从而实现了“无影响升级”;

◆ 由于网络性能的提高,用户的应用已不局限于传统的电子邮件和文件传输,对于高带宽需求的应用,例如 IP 宽带交互教学、视频点播、多媒体教学、校园课件点播和广播等多种视频网络服务,已经在学校全面展开;

◆ 实现了以部门为单位的 VLAN 地址划分,提供了快速数据传输和交换的源动力;

◆ 本方案中 S4909、S1926G+ 交换机均支持 Port VLAN 和 802.1Q Tag VLAN, 可以通过划分 VLAN 来保证网络中数据的安全性,同时有效抑制广播风暴;

◆ 通过中心交换机 S4909 的三层交换功能,实现基于 IP 的三层交换能力,通过划分子网 VLAN 和设置访问规则,可极大程度上提高网络传输性能和安全特性,极大方便用户对网络进行管理;

◆ 锐捷网络的专用网管软件 S-Manager 是一套基于 Windows 平台的全中文用户界面的网络管理系统,能够满足校园网对网管功能既要全面又要方便操作的需求,增加了管理的效率。

“虚拟”的Web服务器

肇庆职业学校 卢江兴

在学校信息化大潮中,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,通过动态域名解释、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。网段内的其它计算机的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RedHat7.2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(如图1)。

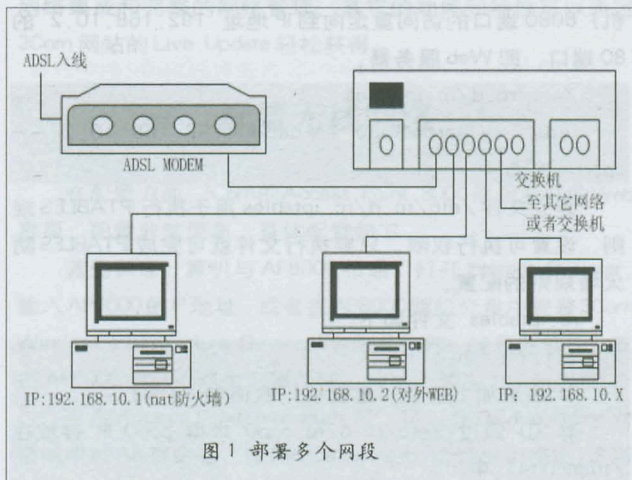


图1 部署多个网段

配置NAT防火墙

硬件: 赛扬667, 128M内存, RTL8139网卡一张, IP: 192.168.10.1。

软件: 安装RedHat7.2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,现在有更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, 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, 把上述内容写到文件 `/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: 192.168.10.2

软件: 安装 Windows 2000 操作系统 + IIS 5.0 + ASP

这样的选择是基于单位内的实际情况, Windows 有更多人使用, ASP 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、通讯线路故障, 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, 以致主机重定向不正确。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 7 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6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都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5个AP,300人教室放置了4个AP,200人教室放置了3个AP,100人教室放置了2个AP,100人以下的教室及教师休息室和走廊均放置了1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),能够轻松的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,让用户安全的登录网络。该接入点的内嵌数据库可以支持多达1000个用户名和口令。

在管理方面,Access Point 8000支持SNMP、HP OpenView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。其它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图标或点击配置按钮,可进入如图1所示界面。

点击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,点击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。点击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选单中选择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中选择数据方式采用方式,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,点击Save按钮保存设置。

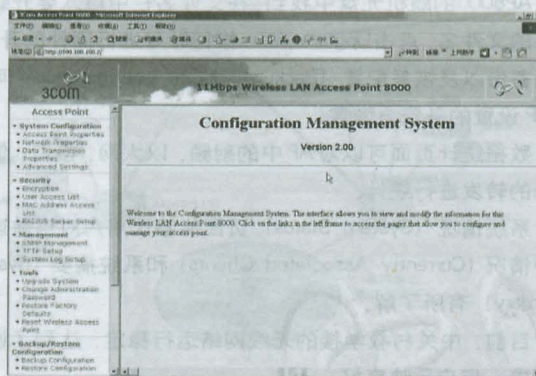


图1 配置界面

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,即用户间不可通讯,选择Off不进行用户隔离,默认设置为Off;在Client List Timeout 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。

安全设置

打开Security下的Encryption您将会看到如图2所示界面: 在此处可以对AP进行加密设置,其中包括40位加密、128

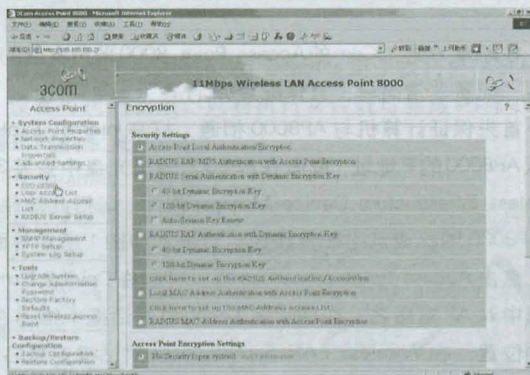


图2 安全设置

位加密以及128位动态加密,针对MAC地址的加密。或其它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。点击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。点击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,点击其后的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,点击其后的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点击Modify Keys按钮输入四组10位16进制字符。

选择128-bit Encryption Shared Key, AP将使用128位共享加密方式,点击其后的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点击Modify Keys按钮输入四组22位16进制字符。

选择128-bit Dynamic Security Link, AP将使用128位动态加密方式,点击其后的more information可以看到此项内容的具体说明。点击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)。

点击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,点击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,用户反映良好。 ■

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。

“升级”我们的校园网

■ 南京 吉翔 朱爱兵

南京农业大学浦口校区现有在校生4000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2个千兆单模光口和6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2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1400个,接入用户达600个。

校区共有8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。

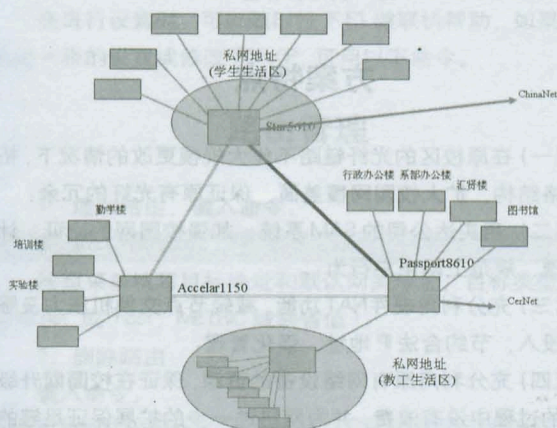


图1 网络拓扑图

根据校区的发展规划,在2008年前,在校生将达到8000人(其中研究生1000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3500个。

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:

(一) 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。

(二) 网络通讯考虑得多,应用服务考虑的少: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。

(三) 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、设备的可扩展性考虑不够,如在学生生活区的Accelar1150最多只能提供8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。

(四) 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, 对于用户拖欠通讯费用, 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。

(五) 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:

(一) 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。

(二) 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。

(三) 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。

(四) 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:

(一) 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 (配置了十六个 GBIC 端口), 原有设备得到充分利用;

(二) 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 台实达公司的三层交换机 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。

(三) 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 4 兆带宽的干线, 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 55M 的三层包转发率和 128G 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。

(四) 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。

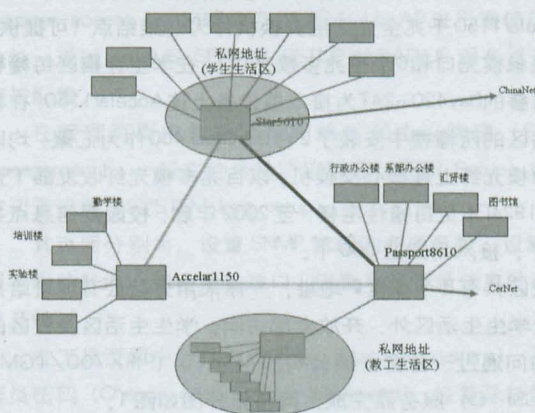


图 2 网络拓扑图

方案特点

(一) 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;

(二) 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;

(三) 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;

(四) 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 全名为 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, 在命令提示行下键入:

```
#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, 系统会采用缺省值, 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 键联机帮助, 如果还需要进一步的设置或修改 TCP/IP, 可用以下命令。

路由管理

1. 增加路由, 键入命令:

```
# 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 域缺省值 1。

2. 删除路由

键入命令:

```
# smit rmroute
```

然后在各个域填写适当的值即可。

3. 刷新路由

键入命令:

```
# 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 Data 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, 就接受缺省值。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

键入命令:

```
# smit chinnet
```

2. 删除网卡配置

键入命令:

```
# smit rmroute
```

然后在各个域填写适当的值即可。

注意: 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, 然后启动守护进程是 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)纪录, 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/addr.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/addr.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务, 用命令:

```
# smit stnamed
```

次域名服务器

1) 编辑/etc/named.boot文件。同主域名服务器的内容相近, 但要把primary win-service.com named.date和primary win-service.com named.rev的primary改为secondary, 而primary win-service.com named.local的primary保持不变。

2) 编辑/etc/named.ca文件, 与主域名服务器相同。

3) 编辑/etc/named.[domain_name]local, 其中NS的名字改为次域名服务器的主机名, 其它主域名服务器相同。

4) 其它文件会自动从主域名服务器下载。

5) 创建空文件/etc/resolv.conf, 用命令生成:

```
# touch /etc/resolv.conf
```

编辑并输入域名和域名服务器的主机名和地址。

6) 启动named守护进程。用命令: # smit stnamed

代理域名服务器 (Cache)

1) 编辑/etc/named.boot文件。注意对/etc/named.local文件名的描述标记为primary。如果不存在*.data和*.rev, 则是纯粹的代理服务器。

2) 编辑/etc/named.ca文件, 与主域名服务器相同。

3) 编辑/etc/name.[domain_name]local文件, NS的名字用次域名服务器的主机名, 其它与主域名服务器相同。

4) 创建/etc/resolv.conf文件, 用命令: # touch /etc/resolv.conf, 编辑并输入域名和域名服务器的主机名和地址。

5) 启动named守护进程: 用命令: # smit stnamed。

域名服务客户机

在提供域名服务的网络中, 大多数域名服务客户机, 需要在/etc/resolv.conf文件中指定域名服务器。最简单的创建、删除、修改/etc/resolv.conf的方法是执行: # smit resolv.conf, 屏幕显示如下:

```
Domain Nameserver (etc/resolv.conf)
```

```
Move cursor to desired item and press Enter.
```

```
Start Using the Nameserver
```

```
List All Nameservers
```

```
Add a Nameserver
```

```
Remove a Nameserver
```

```
Stop Using a Nameserver
```

```
Set/Show the Domain
```

```
Remove the Domain
```

```
Set/Show the Domain Search List
```

```
Remove the Domain Search List
```

选择 Start Using the Nameserver, 再选 Create a New /etc/resolv.conf File, 如:

```
/etc/resolv.conf
```

```
domain win-service.com
```

```
nameserver 192.188.0.220
```

```
nameserver 192.168.0.223
```

域名解析顺序

域名解析是对主机名和IP地址进行互译, AIX系统有多种域名解析方法, 这些方法的采用有优先顺序, 它们的默认顺序是: DNS—NIS—本地机的/etc/host, NIS是网络信息系统。如果要改变默认顺序, 可以用环境变量NSORDER指定顺序, 如:

```
NSORDER=nis,bind,local
```

除了TCP/IP和DNS设置, IBM RS6000 AIX操作系统下网络管理还包括网络信息系统(NIS)、网络文件系统(NFS)以及邮件系统(UUCP, SMTP)等方面的设置, 如果需要可以查阅System Management Guid: Communication and Networks或到IBM网站查询。■

让 IP 参数对号入座

■ 重庆 朱宏志

公司的网络由几台普通的二层交换机连接在一起,也就是整个公司网络处于一个物理网络中,也即一个大的广播域中,这个物理网络被划分为两个逻辑子网(如图1)。

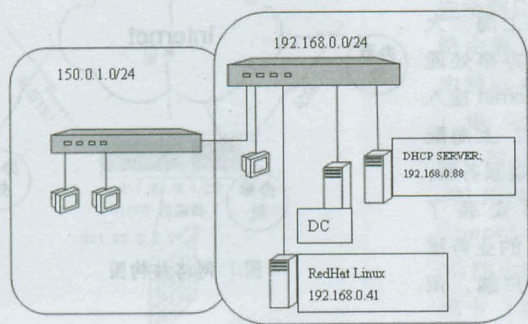


图1 网络结构图

一个是192.168.0.0/24,一个是150.0.1.0/24,其中192.168.0.0/24是一个由Windows 2000系统组成的Windows 2000域,而150.0.1.0/24子网是一个由Windows 98组成的工作组,其中也有个别计算机需要登录到192.168.0.0/24的域,以前192.168.0.0/24子网由一台Windows 2000上的DHCP服务分配IP地址等参数(DHCP服务器的IP是192.168.0.88),现在也想把原150.0.1.0/24子网中部分计算机的TCP/IP参数分配交由这台DHCP服务器负责,但却遇到了一个难题,就是DHCP服务不分配新作用域150.0.1.0/24中的地址,为什么会这样呢?

这是因为DHCP服务只会分配它所在子网的IP,即这里它只会分配192.168.0.0/24子网范围的IP,虽然可以通过超级作用域的方式来把这两个作用域组合起来,让它也能分配150.0.1.0/24范围的地址,但DHCP服务器是在分配完所在子网作用域的地址后才会分配别的子网地址,所以这也不能实现我的要求,由于公司的整个网络是一个物理网络,所以采用DHCP中继代理也没必要,而网上盛传的用户类的方法其实在微软DHCP服务器上也是无法实现的。正当郁闷之际,忽然把眼光放到了Linux平台的DHCP服务上,因为Linux平台通常都是采用ISC DHCP实现,而ISC的DHCP实现可以说是最权威而且功能也是最为强大的,通过测试,ISC的DHCP实现果然不负我意,很好地实现了我的要求,下面就来看看它是怎样在RedHat 7.3系统上实现我的要求的。

实现要求

把DHCP服务从Windows平台转移到Linux平台,保证原192.168.0.0/24子网的客户机仍然得到192.168.0.0/24范围内的地址,而原来静态分配IP的150.0.1.0/24子网中的客户机改为动态分配IP,但这些客户机仍然使用150.0.1.0范围的地址。

实现的基本思路

实现的基本思路是建立一个用户类(user-class),是这个类的客户就分配192.168.0.0/24子网的地址,不是这个类就分配150.0.1.0/24范围的地址。

实现的基本步骤

设置域客户端的DHCP用户类

在安装和启用新DHCP服务之前,需要先为域中的客户端设置用户类,这样才能保证它们在新的DHCP服务之下仍然能够使用原作用域192.168.0.0/24范围的地址,注意只有Windows 2000及以下的系统才支持用户类,由于这里是一个Windows 2000域,所以正好满足要求。

有几种方法来设置用户类,推荐的方法是使用域的启动或关机脚本进行设置,不过这需要等到客户端关机或重新开机才行,第二种方法是直接远程设置客户端用户类,比如用psexec工具进行远程设置,不管使用哪一种方法或者是把二者结合起来用,都可以先创建一个脚本class.bat,里面包含一行命令“ipconfig /setclassid 本地连接 fzz”,通过它来设置域客户端的用户类为fzz。至于怎样在域中应用启动/关机脚本或使用psexec进行远程管理,请参考以前的文章。如果是某台计算机要加入域,需要在它加入域前手动设置用户类,也就是执行命令:

```
ipconfig /setclassid 本地连接 fzz.
```

下载及安装ISC的DHCP服务软件包,用rpm qa | grep dhcp命令确定系统上是否已经安装了DHCP服务,如果没有,请到<http://www.isc.org>下载安装程序,我这里使用的是DHCP 3.0版本,具体安装这里就不叙述了。

为这台DHCP服务器绑定第二个IP地址,同微软的DHCP实现一样,这里的DHCP也只会分配它所在子网的IP地址,但我们可以通过为网卡绑定更多相应的IP地址来让DHCP服务认为它处于多个子网中(注意Windows上这 【下转第58页】)

让企业多几个出口

■ 上海 丁红兵

Internet已经与现代企业的各项业务紧密结合在一起。E-mail、企业网站、视频、Internet浏览再加上企业的业务系统已经使Internet接入成为不可或缺的一项关键应用。但是我们也知道,Internet接入相对而言是一种不可靠的接入,常常由于病毒、突发流量、物理线路等各方面的问题而受到影响。另外,各种业务对Internet接入质量的要求并不一样:例如接入公司Terminal Server运行订单输入等业务系统,带宽要求小(每连接大约10~20kbps),但可靠性要求高;E-mail流量上下波动很大,但对延时不敏感等等。目前ISP众多,费率差距颇大,在这种情况下,使用多ISP或多方式接入Internet是个在可靠性与费用等方面获得综合平衡的方法。

笔者所在公司是一中型外资企业,在广东、上海、河北三地有工厂,全国各地有四、五十个办事处。上海工厂是全

国的信息中心,有Internet接入;工厂和少数较大的办事处用户使用DDN连接到上海,大部分办事处通过Internet接入上海。上海配置终端服务器,上面安装了SAP的业务程序客户端。用

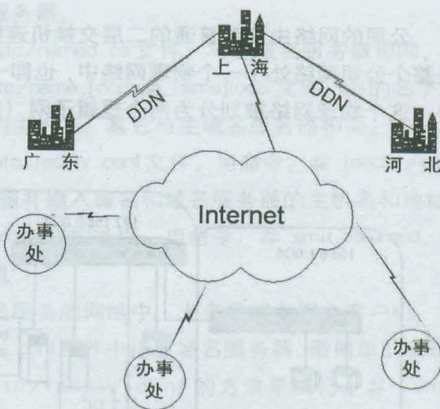


图1 网络结构图

【上接第57页】

种方法无效),当然如果您的DHCP服务器上本身就有多块网卡及相应子网范围内的IP地址,那就没有必要绑定更多IP了。绑定方法很简单,即在/etc/sysconfig/network-scripts目录下新建一个名为ifcfg-eth0:0的文件:

```
DEVICE="eth0:0"
```

```
IPADDR="150.0.1.41"
```

```
NETMASK="255.255.255.0"
```

```
ONBOOT="yes"
```

如果要绑定更多的IP请创建更多的ifcfg-eth0:x文件,其中eth0为相应的网卡。完成后运行/etc/rc.d/init.d/network restart重新应用网络设置。

配置DHCP服务

DHCP服务的配置文件是/etc/dhcpd.conf,默认情况下这个文件并不存在,但在/usr/share/doc/<dhcpserver>/下会有一个名为dhcpd.conf的模板文件,为了避免配置错误,可以先把这个文件复制为/etc/dhcpd.conf,然后对其进行修改。下面是我的配置文件:

```
# 全局参数
```

```
ddns-update-style interim;
```

```
ignore client-updates;
```

```
default-lease-time 691200;
```

```
max-lease-time 691200;
```

```
option domain-name-servers 192.168.0.88;
```

```
# 定义一个用户类
```

```
class "fzz" {
```

```
match if substring (option user-class, 0, 3) = "fzz";
```

```
}
```

```
# 定义一个物理网络,以及其中包含的逻辑子网
shared-network fzznet {
```

```
subnet 192.168.0.0 netmask 255.255.255.0 {
    option routers 192.168.0.43;
```

```
}
```

```
subnet 150.0.1.0 netmask 255.255.255.0 {
    option routers 150.0.1.43;
```

```
}
```

```
# 用户类为fzz的客户端分配192.168.0.0/24子网的IP
pool {
```

```
allow members of "fzz";
```

```
range 192.168.0.100 192.168.0.150;
```

```
}
```

```
# 非fzz类客户端分配150.0.1.0/24子网的IP
pool {
```

```
deny members of "fzz";
```

```
range 150.0.1.50 150.0.1.99;
```

```
}
```

```
}
```

启动DHCP服务,关闭原Windows平台上的DHCP服务,用service dhcpd start来启动服务,这里要注意是如何顺利从微软的DHCP服务过渡到Linux平台的DHCP服务,可以让这两台服务器共存一段时间(当然它们的地址池不能重叠),并且减少Windows上的DHCP租约时间,到一段时间后就可停掉Windows平台上的DHCP服务,使客户端的DHCP请求自然转移到新平台上。■

户主要的应用有E-mail、公司网站、Internet浏览等(如图1)。

为了保障公司的业务系统应用,我们申请了512kbps的专线接入上海163平台,地址为203.96.46.0/28;为使用其它应用,我们申请了1Mbps专线接入网通的Internet骨干,地址为211.22.3.0/28。我们希望达到两个基本目的:

1. 业务系统(通过终端服务器)的流量与其它流量各自走不同的专线,相互不要干扰;

2. 在某条线路发生故障短时间内无法排除时,可以通过手工更改设置的方法把某些应用临时调整到其它线路。

下面我们说一下具体的安装、配置方法:

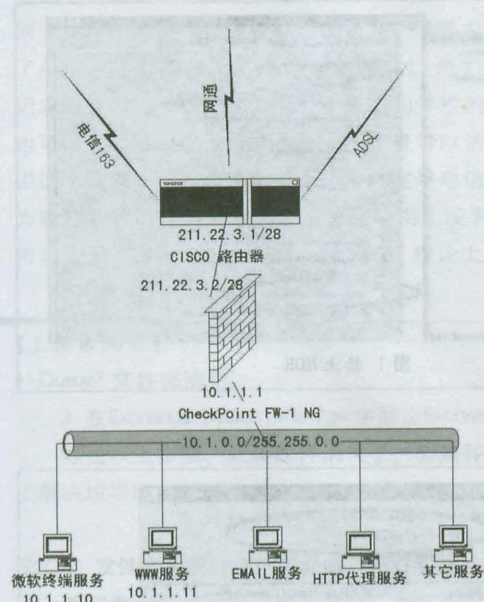


图2 改进后的网络图

域网地址为10.1.0.0/16,防火墙内网卡地址为10.1.1.1/16。各对外提供服务的服务器将缺省路由设为10.1.1.1,防火墙上作静态地址转换,将服务器内部地址转换成不同ISP的外部合法地址,在路由器上按照源地址做策略路由(policy-routing)。Cisco路由器的策略路由,可以根据IP包的源地址来决定下一跳进入的端口(如图2)。

IP包完整的进出过程叙述如下:某台终端服务器(10.1.1.10/16)发送IP包到外部网,由于缺省网关指向防火墙10.1.1.1,包到达防火墙后进行静态地址转换,源地址变为203.96.46.10,然后通过防火墙外网卡211.22.3.2转发到路由器以太口211.22.3.1。路由器以太口收到该包后根据策略路由,由串行口s0/0发出去,从而顺利的实现了包的发出。进来的情况是怎样的呢?当目的地址为203.96.46.10的IP包到达路由器串口时,路由器根据主机路由将它转发至防火墙外网卡,防火墙外网卡收到这样的包时对其之进行响应并将其地址转换成内网地址10.1.1.10转发至内网。

注意: 1. 路由器上对进来的路由使用主机路由的方式,如果使用网段路由的方式,由于某些主机与路由器以太口处于同一网段,路由器将试图直接发送包而并不转发到下一跳(防火墙)。

2. 不同的防火墙(甚至同一防火墙的不同版本)配置方式上可能有区别,例如Checkpoint FW-1 4.1版本以下需要配置用外网卡MAC地址来响应主机外网地址,同时在防火墙上设置外网地址的主机路由指向内网地址。但在Checkpoint FW-1 NG以上的版本就不需要了。

3. 当某线路如网通断掉时,可在防火墙上将静态地址转换到电信线路网段,同时通知相应用户改用新的IP地址。这至少可以保证少量关键应用尚可进行。

笔者公司还在路由器上增加一条ADSL线路专门用于上网浏览,配置更复杂,原理差不多,这里就不叙述了。

路由器的相关配置如下:

```
interface FastEthernet0/0
ip address 211.22.3.1 255.255.255.240
ip policy route-map takeserial
duplex auto
speed auto
!
interface Serial0/0
description connected to dianxin
ip address 203.96.5.222 255.255.255.252
encapsulation ppp
!
interface Serial0/1
description connect to wangtong
ip address 211.22.2.30 255.255.255.252

access-list 1 permit 203.96.46.0 0.0.0.15
access-list 1 deny any
access-list 3 permit 211.22.3.0 0.0.0.15
access-list 3 deny any
!
route-map takeserial permit 10
match ip address 1
set interface Serial0/0
!
route-map takeserial permit 30
match ip address 3
set interface Serial0/1
!
ip route 0.0.0.0 0.0.0.0 s0/1
ip route 203.96.46.1 255.255.255.255 211.22.3.2
ip route 203.96.46.2 255.255.255.255 211.22.3.2
.
ip route 203.96.46.14 255.255.255.255 211.22.3.2
ip route 211.22.3.3 255.255.255.255 211.22.3.2
ip route 211.22.3.4 255.255.255.255 211.22.3.2
.
ip route 211.22.3.14 255.255.255.255 211.22.3.2 INI
```


安全检查从日志做起

■ 辽宁 李辉 刘晶

电子邮件无疑是目前互联网时代最主要的信息沟通方式,伴随着这种通信方式,病毒邮件和垃圾邮件迅速增长,使我们防不胜防。致使我们不得不关心我们的邮件系统安全问题。

我们无法预料到威胁来自哪里,作为系统维护人员除了做好一切应有的预防措施外,最应该了解的是系统,知道出了问题如何去处理,如何找到病因。下面以一次垃圾邮件处理过程解释如何利用Exchange本身的日志来分析、查找问题原因,从而最终解决问题。

问题症状

现象: 邮件收发不正常

邮件服务器: Microsoft Windows 2000 advanced Server+Exchange 2000 Server

检查邮件服务器队列发现大量垃圾邮件,由于这些邮件堆积在邮件服务器队列中,导致邮件服务器不能正常运作。为保证邮件正常收发,首先停止SMTP服务,将队列名称queue改名,重建queue目录,启动SMTP服务,分析原队列内邮件,造成邮件服务器阻塞的这些垃圾邮件可以分成以下两类:

第一类,Exchange向外部用户发送的Non-Deliverable Report (NDR)。

第二类,发件方和收件方均不是邮件系统中用户的relay邮件。

排查过程和解决问题的方法

根据不同种类的垃圾邮件,采取不同的防治措施:

第一类 Exchange 向外部用户发送的 NDR

第一类问题的起因源自第二类的垃圾邮件。由于大量垃圾邮件发给的是虚假的不存在的账号,导致Exchange服务器伴随着产生大量的NDR邮件。在问题Queue目录中,除了relay邮件之外,可以发现大量的NDR,即发件人为系统用户、收件人为不存在的外网用户。

针对大量的NDR堆积与Queue中的问题,可以采取的办法是将自动发送NDR的选项禁止。这一步骤可以在Exchange System Manager (ESM)中完成。详情请参见图1:

针对这一问题,采取以下措施解决:

1. 及时地将"%System Root%\ExchSrvr\Mailroot\VSI

【下转第61页】

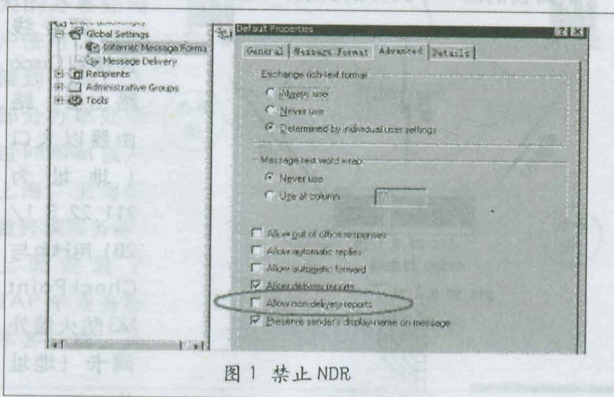


图1 禁止NDR

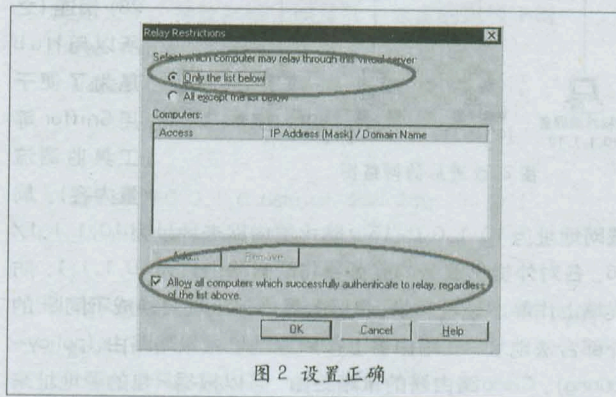


图2 设置正确

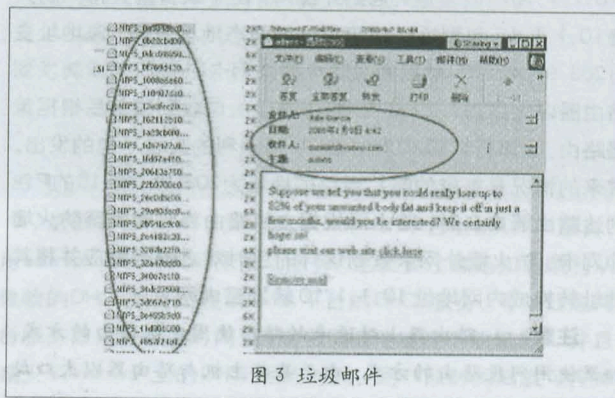


图3 垃圾邮件

被遗忘的路由

■ 江苏 王雪峰

学校给我们每个老师都配发了笔记本电脑,每个人都领到一个固定的IP地址。在学校时,大家只要把网线接上网卡就可以上网了。随着宽带的普及,很多人在家里开通了ADSL,几个月前曾经有人向我提起过,他们在家用笔记本上宽带(ADSL)时,有时不能访问学校的网站,有时也可以,但使用拨号方式上网,却一直可以访问。我一听说这个现象,不假思索的认为,那肯定是电信的问题,因为能够拨号访问说明校园网在上联路由上没有问题。而宽带拨号只不过是不同的接入方法而已,理论上应该没有问

题,除非电信做了某些过滤,禁止某些网站的访问,从而导致上宽带时出现不可以访问学校网站的情况。

几个月过去后,我家也装ADSL了,而这个现象一直存在。有一天,我决定研究一下到底是什么原因。为了排除服务器被关闭(可能会有意外停电)的情况,先用拨号方式建立网络连接,能够正常访问学校网站,说明服务器是开着的。断开拨号连接,把ADSL的网线接上网卡,打开ADSL的电源,建立ADSL拨号连接,在浏览器的地址栏输入网易的地址,正常显示,连接成功。

【上接第60页】

1.\Queue"文件夹清空。

2.在Exchange System Manager中禁止Exchange发送NDR。

经过以上步骤,此类邮件消失了。但是并没有从根本上解决垃圾邮件问题。

第二类 发件方和收件方均不是邮件系统中用户的relay邮件

第二类问题相对来说较为复杂。我们通过以下的步骤查找问题的根源并最终将其解决:

1.首先,检查Exchange服务器上的relay设置。根据UI界面的显示,relay相关的设置完全正确(如图2)。

2.由于relay设置是正确的,而relay的邮件又反复出现,开始怀疑系统中可能有账号被泄漏。从邮件服务器上,可以发现大量的relay邮件。这些邮件来自不同的主机,邮件的发送方和接受方都不是邮件系统的内部用户(如图3)。

邮件在Internet上是通过SMTP协议进行传送的。如果一台服务器没有被设置成为open relay,那么服务器将要求客户端在发送邮件以前首先进行验证。只有经过验证后的用户才被获准发送relay邮件。邮件系统的服务器正好属于这种情况。于是,需要找出究竟是哪个用户账号被泄漏。

3.在服务器上进行以下操作:

◆ 打开MSExchangeTransport\SMTP Protocol组件的诊断日志。

◆ 打开SMTP protocol logging。

◆ 从文件系统中列出几封典型的垃圾邮件以便于核对。

4.在系统日志中,发现一个名为"xxxx"的账号产生了大量的登录失败纪录。

5.在应用日志中,发现"xxxx"账号曾经从一台名为"yyyy"的外部机器通过验证。在相应的时间段,还发现在队列中有一封来自"yyyy"的垃圾邮件。

6.通过再次检查应用日志以及队列中的垃圾邮件,发现"xxxx"账号曾经从不同的外部主机登录到邮件系统的服务器。在相同的时间段内,都发现了从这些主机发送的垃圾邮件。由此,基本确认"xxxx"账号被泄漏,垃圾邮件的发送者使用该账号通过邮件服务器发送relay邮件。

7.根据以上发现,将有问题的账号禁用。继续观察发现,relay邮件已经不再产生。问题最终得以彻底解决。

问题追踪

通过以上分析已经将问题解决。更进一步的,可以根据SMTP日志中记录的信息找到攻击发生时,攻击者所使用的IP地址。查找步骤如下:

1.在ESM中,SMTP Virtual Server属性页中,确保SMTP Logging已打开。

2.默认情况下,日志文件存储在"%SystemRoot%\system32\logfiles\smtpsvc1"文件夹下。文件的命名规则是"EX<当天日期>.log"。

3.打开问题发生当天的日志文件,搜索发件方地址和收件方地址均不是本域中的IP地址。

通过以上案例的解决过程可以看出日志在分析问题和解决问题过程中的重要性,因此建议各系统管理员一定要把日志打开,为查找问题留下重要的数据来源。同时,要经常察看日志信息,对可疑日志多加留心,从而消除系统安全隐患。■

接下来输入我们学校的网址 (http://www.jsntyz.edu.cn), 状态栏上显示“正在连接http://www.jsntyz.edu.cn”, 过了几秒钟后, 出现错误提示“找不到服务器或发生DNS错误”。可能出现这种现象的原因是服务器被关闭或者没有到达服务器的路由或者电信的DNS解析不到服务器。由于先用拨号连接排除了服务器被意外关闭的情况, 接下来就是排除后两种情况, 我决定先用“ping”命令来检查。在命令提示符下, 输入“ping www.jsntyz.edu.cn”, 出现以下回显:

```
c:\>ping www.jsntyz.edu.cn
Pinging www.jsntyz.edu.cn [211.70.32.17] with 32 bytes of data:

Request timed out.
.....

Ping statistics for 211.70.32.17:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

从以上出现的情况可以看到服务器的域名地址已经解析为“211.70.32.17”了, 说明DNS解析没有问题。那到底是什么原因导致没有到达服务器的路由呢? 由于我们学校的上联单位是南通市的教育网主节点——南通师院 (www.nttc.edu.cn), 如果没有到达南通师院的路由, 就不会有到达我们学校的路由了。使用“tracert”命令来测试:

```
c:\>tracert 210.29.64.9
Tracing route to star.nttc.edu.cn [210.29.64.9]
over a maximum of 30 hops:
  0  27 ms  27 ms  26 ms  61.177.206.90
  1  27 ms  33 ms  38 ms  61.177.205.181
  .....
 19  917 ms  914 ms  916 ms  210.29.64.9
```

上面的测试结果表明, 目标服务器能够成功到达。再试着 tracert 我们的网站:

```
c:\>tracert www.jsntyz.edu.cn
Tracing route to www.jsntyz.edu.cn [211.70.32.17]
over a maximum of 30 hops:
  0  *      *      *      Request timed out.
  1  *      *      *      Request timed out.
```

上面的显示表明, 计算机根本就找不到路由。啊, 天哪, 这是为何? 冷静, 别急。问题可能出现在本地计算机上, 输入我最常用的命令“ipconfig” (查看IP地址)。

```
c:\>ipconfig

Windows IP Configuration

Ethernet adapter 本地连接:

    Connection-specific DNS Suffix . :
```

```
IP Address. . . . . : 211.70.32.220
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 211.70.32.1
PPP adapter adsl:

    Connection-specific DNS Suffix . :
IP Address. . . . . : 218.91.167.129
Subnet Mask . . . . . : 255.255.255.255
Default Gateway . . . . . : 218.91.167.129
```

啊, 有两个IP地址, 本地连接上的“211.70.32.220”是我在学校上网的地址, 而“218.91.167.129”是ADSL拨号连接的地址。我觉得好像有点眉目了。再使用“route print”命令查看本机路由:

```
c:\>route print -f

Active Routes:

NetworkDestination  Netmask          Gateway          Interface        Metric
61.177.206.90      255.255.255.255  218.91.167.129  218.91.167.129   1
127.0.0.0          255.0.0.0        127.0.0.1      127.0.0.1        1
211.70.32.0        255.255.255.0    211.70.32.220  211.70.32.220   1
211.70.32.220      255.255.255.255  127.0.0.1      127.0.0.1        1
211.70.32.255      255.255.255.255  211.70.32.220  211.70.32.220   1
218.91.167.129     255.255.255.255  127.0.0.1      127.0.0.1        50
224.0.0.0          240.0.0.0        211.70.32.220  211.70.32.220   1
.....
.....
255.255.255.255    255.255.255.255  211.70.32.220  211.70.32.220   1
Default Gateway: 218.91.167.129
```

在上面的显示中可以看到, 目标网络为“211.70.32.0/255.255.255.0”的接口是“211.70.32.220”, 也就是本地连接。至此终于明白是什么原因了, 因为ADSL上网需要使用网卡, 而当我把ADSL的网线接上网卡的时候, 同时激活了网卡上设置的固定IP地址, 由于此IP地址和我校网站服务器的地址在同一个网段211.70.32.0/255.255.255.0, 所以计算机就认为网站服务器 (211.70.32.17) 在本地网卡所连接的网络上, 而本地网卡并没有连接到任何网络, 所以无法找到服务器。

那如何解决这个问题呢? 其实只要删除本地网卡上的地址即可, 或者改为其它地址, 也可以设为“自动获得IP地址”。有的时候能够访问学校网站, 只是因为无意中丢失了IP地址或者设为“自动获取”, 而幸运的连接成功罢了。后来对校园网的地址分配做了改进, 把服务器的地址段和老师上网的地址段划分为两个虚网 (VLAN)。这样既可以方便老师使用ADSL上网, 又可以方便我在服务器网段前做访问控制列表 (ACL)。真是一举两得! ■

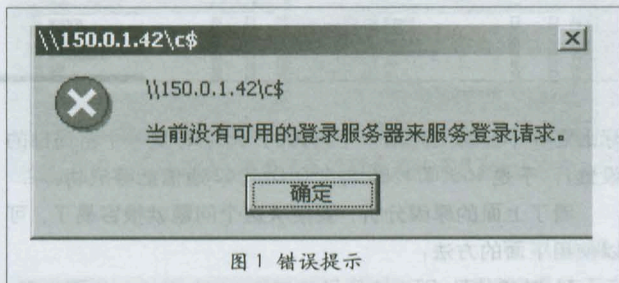
一个共享问题及深入认识

■ 重庆 朱宏志

这几天遇到一个怪问题，就是从192.168.0.88 (150.0.1.88) 用\\150.0.1.42\c\$ 的方式访问150.0.1.42时，出现了图1所示的错误提示框（如图1）。

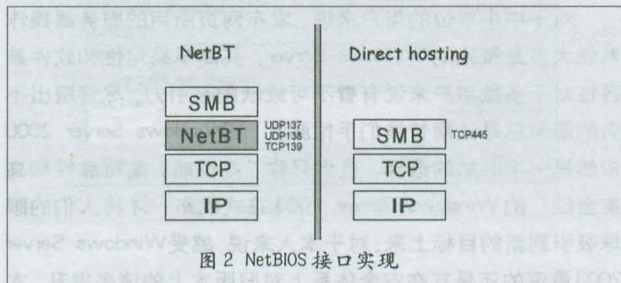
于是共享访问不能成功，但用户名和密码都是输入正确的，更奇怪的是，有时这种形式的访问又能成功，这是为什么呢？通过一番分析，总算找到了原因，也从这个问题更深入更具体地认识了NetBIOS over TCP/IP通信和Direct hosting通信，在这里把整个问题的分析及解决过程写出来，相信对大家解决相关问题会有所启发。

先来简单介绍一下这个问题的产生环境，192.168.0.88这台服务器是Windows 2000 Server系统，有一块网卡，网关为192.168.0.43，并且添加了第二个IP：150.0.1.88，您也许会问，为什么有了网关还要设置第二个IP呢？这是因为内网有一台150.0.1.222的关键服务器，为了防止192.168.0.0/24网络的计算机与其通信，所以150.0.1.222



没有设置网关，也就是此时只有150.0.1.0/24子网的计算机才能与其通信，为了方便192.168.0.88这台服务器也能与150.0.1.222通信（主要是作一些管理操作），所以就增加了150.0.1.88这个IP，这也就造成了文章开篇所讲的问题，具体原因后面将讲到。另外被访问的计算机150.0.1.42是一台Windows XP系统，也是一块网卡，网关指向150.0.1.43，150.0.1.43与192.168.0.43是同一台路由器。

我们知道文件共享是通过SMB协议来完成的，而SMB协议有两种实现方式。一种是大家熟悉的NetBIOS over TCP/IP（简称NetBT），也就是在NetBIOS接口上实现的（如图2左侧）。使用端口UDP 137、UDP 138和TCP 139，其中137端口用来进行名字解析，138端口用来传递数据报，而139端口是会话



服务，也就是真正的文件传输所使用的端口。

另一种方式微软称为Direct hosting（直接主机通信），我们这里不管它的名字，只说说它的特点，此时SMB直接在TCP层上实现，不再需要NetBIOS的中间支持（如图2右侧），也就是让NetBIOS下岗了，于是也就不再需要NetBIOS使用的名称解析端口137和数据报端口138了，它只使用了TCP 445端口，这就是Direct hosting方式的好处，它简化了SMB通信传输，也免去了NetBIOS名称解析，如果有名称解析就通过标准的DNS来完成了。虽然这种方式不错，不过只有Windows 2000以上系统才支持。

那您会问，如果两种方式都可用，系统到底会使用哪一种呢？实际上当两种都可以用时，系统将同时尝试使用这两种方法，第一个响应的将被使用（是不是有点像抢答？），说到这里，您也许有点明白了，上面图1的问题我有时遇得到而有时又遇不到可能就与这里的“抢答”有关了，不错，确实是因为系统选择的方法不同造成的，当出现图1的错误提示时，是因为NetBT抢了先，而访问成功时是因为Direct hosting抢了先，那您又会问为什么说出现错误时是因为NetBT抢了先而访问成功时是使用了Direct hosting呢？下面来——分析。

当使用NetBT时，共享访问失败，错误提示如图1。

大家注意，NetBIOS over TCP/IP（NetBT）将绑定到每个网卡，但只能绑定到每一个网卡的第一个IP上，这里是192.168.0.88，当计算机启动时，它的NetBIOS名字注册时对应的IP就是192.168.0.88（不会是第二个IP 150.0.1.88），但由于连接的目标150.0.1.42与150.0.1.88是同一子网，所以连接时系统会以150.0.1.88去连接（不会使用192.168.0.88），但实际上NetBT并没有与 【下转第64页】

发布不了的网页

■ 江西 赵庆

对于中小单位的用户来说,发布网页所用的服务器操作系统大多是微软的 Windows Server,其简单易用性和软件兼容性对于多数用户来说有着不可或缺的吸引力,尽管层出不穷的漏洞总是让网管员们手忙脚乱,但 Windows Server 2000 依然是一个必然的选择,直到号称“高性能、高可靠性和高安全性”的 Windows Server 2003 正式发布,才将人们的眼球吸引到新的目标上来。对于本人来说,感受 Windows Server 2003 最深的还是其在安全体系上对旧版本上的诸多提升,本文将通过 Windows Server 2003 网页发布过程中经历的一些问题,对网页文件夹用户权限设置做一些探讨。

问题发现

用 Windows Server 2003 服务器进行网页发布相对 Windows Server 2000 有了一定的变化,通过有关资料的介绍,主要是两点:1) Windows Server 2003 采用了新的 IIS6.0,

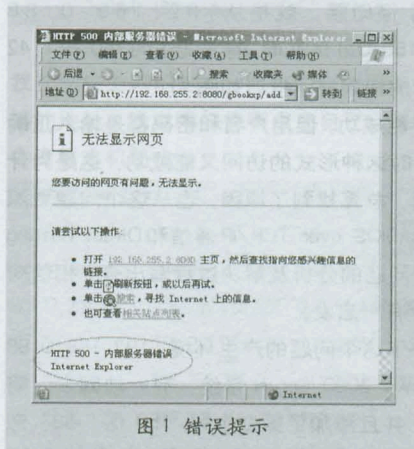


图1 错误提示

并且 IIS6 在缺省情况下未安装,所以必须从“开始”菜单的“管理工具”中选择“配置您的服务器向导”,并选择“应用程序服务器 (IIS, ASP.NET)”进行 IIS6 的安装过程;

2) 打开“Internet 信息服务 (IIS) 管理器”后,选中“Web 服务扩展”,发现 ASP 等服务都被禁用,打开所需的服

【上接第 63 页】

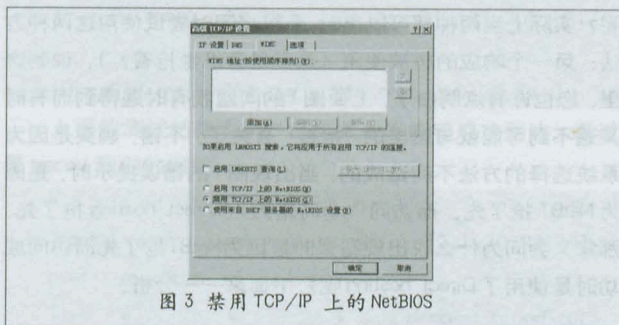


图3 禁用 TCP/IP 上的 NetBIOS

150.0.1.88 绑定,所以 TCP 连接虽然能够建立成功,但实际的 SMB 通信不能成功,于是出现图 1 的错误提示。

当使用 Direct hosting 通信时,共享访问成功

此时系统将直接以 150.0.1.88 地址去连接 150.0.1.42 的 445 端口 (可以用 netstat na | find ":445" 命令来发现相应的 TCP 连接),由于 Direct hosting 不存在绑定限制 (实

际上它并不会绑定到某一个具体的网卡,它是一个全局性的设置),于是 150.0.1.88 与 150.0.1.42 通信能够成功。

看了上面的原因分析,要解决这个问题就很容易了,可以使用下面的方法:

- 1) 禁用掉 NetBT, 这样只使用 Direct hosting, 步骤如下:
 - a, 右击桌面上的“网上邻居”,进入其“属性”窗口;
 - b, 右击“本地连接”图标,进入其属性窗口,选定“Internet 连接协议 (TCP/IP)”项,点击“属性”按钮,点击新窗口的“高级”按钮,进入“高级 TCP/IP 设置”窗口;
 - c, 切换到“wins”标签,选择“禁用 TCP/IP 上的 NetBIOS”项 (如图 3)。

我这里使用的就是这种方法,另外还可以使用下面的方法:

- 2) 去掉 150.0.1.88 地址,只保留 192.168.0.88,这样即使使用 NetBT 方法,由于没有了 150.0.1.88,通信时将使用 192.168.0.88 地址,由于这个 IP 与 NetBT 有绑定,所以与 150.0.1.42 的文件共享能够成功。 INI

2000下正常发布的网页文件夹复制到2003服务器,新建Web站点,进行常规设置后进行发布,熟悉的网页打开,似乎一切正常,可在测试ASP源码的留言板时,却发现新留言不能正常提交,再仔细观察,所有涉及网页数据库更新的操作都存在相同的错误(如图1)。

症状分析

由于网页文件夹在Windows Server 2000服务器中可以正常发布,基本可以排除源代码的问题。从问题的现象分析,网页(包括ASP)能正常打开,可以肯定ASP源码可以进行读、执行操作,那么,提交时出错很可能是由于网页数据库在进行写操作时异常导致的。难道Windows Server 2003与2000系统在文件夹用户权限设定上有所不同吗?

原来发布网页的Windows Server 2000与安装Windows Server 2003系统的两台服务器都采用了NTFS文件格式,再分别打开两套系统的磁盘文件夹属性,选择“安全”页框,进行对比(如图2)。

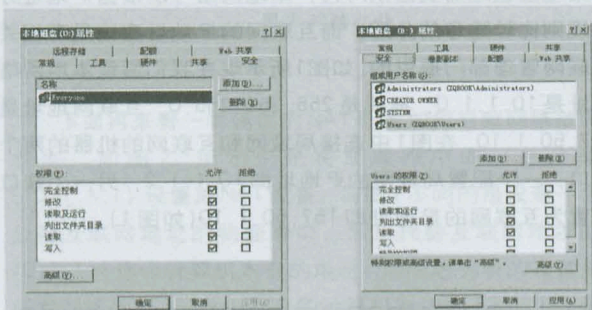


图2 两套系统的磁盘文件夹属性

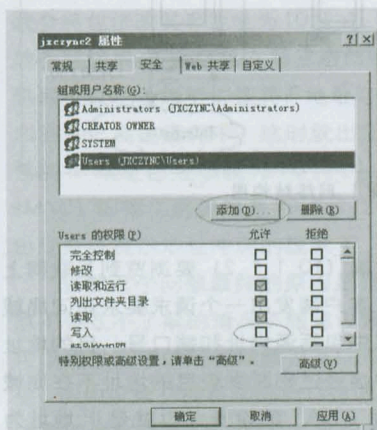


图3 没有写入权限

可以发现:在2000系统下文件夹默认everyone组具有包括“完全控制”在内的全部权限;2003系统却没有everyone组,users组中也只有“读取”、“运行”、“列出文件夹目录”三项权限,尤其是users组中没有“写入”权限!给users组加上“写

入”权限,再进行网页发布测试,完全正常,原因终于真相大白(如图3)。

问题解决

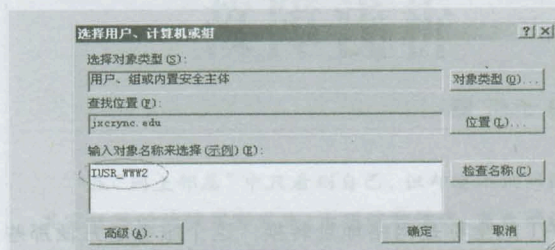


图4 选择用户、计算机或组

显然,给users组加上“写入”权限还不是一个最佳的方案,匿名访问Windows Server信息服务的内置账号为:IUSR_ (服务器计算机名),我们只要赋予此账号适当的权限,问题就可以解决。

首先,单击图4中的“添加”按钮,输入本服务器的Internet来宾账号(如图3),确定后,选中Internet来宾账号的“写入”权限,确定,设置完毕(如图5)。

在后面的实验中,我们还发现:如果网页文件夹所在磁盘文件系统采用了FAT32格式,将不会出现上文所出现的问题,但是,磁盘采用FAT32文件格式无论从性能还是安全性肯定不是一个明智的选择。

从以上Windows Server 2003网页发布的案例中,让我们再次感觉到,微软在Windows Server 2003安全问题上的小心翼翼,相对Windows Server 2000等较早版本而言,权限往往限定较严格,甚至有处处设防的感觉。虽然微软的用心我们是理解的,但也给新用户带来了一定的麻烦。作为用户而言,在了解Windows Server 2003的这个特点后,往往可以从安全性的角度来思考 and 解决一些棘手问题。

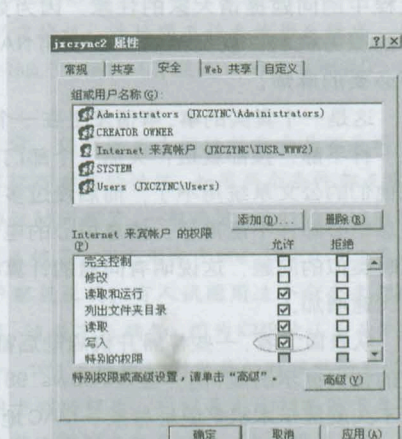


图5 属性

NAT 也会惹故障

■ 北京 陈春芳

NAT 的全称是网络地址转换, 这个服务是方便那些想更大范围的利用有限的互联网资源的公司准备的, 因为它的实现容易、费用低而深受欢迎, 在这里, 我不想就这个服务本身的特点再多说些什么, 只想就其设置使用过程中的问题提请大家的注意, 因为如果了解 NAT 本身的服务机制, 就贸然的配置使用 NAT, 会为自己带来不必要的麻烦。

这是一个真实的事。事情发生在一个上午, 办公室像以往一样平静, 按部就班; 突然一个部门打电话到信息中心说他们的公文系统用不了, 而后没过多久另一个部门通知信息中心邮件不能用了, 信息中心的电话一直在响, 都在反映类似的问题, 这说明有问题的计算机在像病毒传播一样飞速增加。

从表面上看, 一些机器开机启动后都很正常, 也没有任何的错误提示出现; 而一些 Windows 98 系统的机器在开机后不久就提示本机 IP 地址与某一 MAC 地址冲突, 造成网络连接不正常; 而安装 Windows 2000/XP 的计算机就提示硬件错误。

由于网络是局部瘫痪, 一些机器运行还很正常, 而一些机器却完全不能联入网络, 而且从发生的时间上感觉像是在一台一台的传染, 所以首先怀疑是病毒, 向防病毒公司进行咨询, 否定了这个结论。可以肯定的是在发生该事件之前, 网络一直都正常, 而且网络设备经检查也没有问题; 而且局域网通过 Cisco 的路由器接入广域网, 本地的机器对广域网的其它网段上的设备进行联通测试都没有问题, 那么可以肯定问题应该是出在局域网内部, 不是病毒的问题。对有问题计算机进行操作, 拔去网线再插上, 在短时间内机器是正常的, 网络也是可以连通的, 但很快就再次出现问题。

最后通过 MAC 地址找到了出现问题的计算机, 发现就是由于这台计算机的错误配置 NAT 服务才造成如此大的网络故障, 那么为什么 NAT 有如此大的威力能够将网络进行毁灭性的颠覆呢?

首先让我们先来了解一下正常情况下 NAT 是如何工作的吧。NAT 能够实现小型局域网共享一个有效的互联网地址, 从而保证局域网中所有计算机都能够共享互联网资源。而且在 Windows XP、2000、2003 下配置简便, 容易实现, 但配置 NAT 需要一些条件才能进行配置, 如图 1 所示就是标准的 NAT 的实现的网络拓扑图, 其中那个连接互联网和本地网络的计算机需要有至少两个网络接口, 而且网络地址也是需要区别对待, 本地网络可以根据 IP 地址分配规则比较随意的分配, 而互联网的 IP 地址应该是有相关互联网管理部门提供的。如图 1 所示现在我们假设本地网络地址是 10.1.1.0, 掩码是 255.255.255.0, 互联网地址是 157.50.1.10。在图 1 中连接局域网和互联网的机器的两个端口, 一个配置局域网的 IP 地址即 10.1.1.2, 另一个端口配置为互联网的 IP 地址即 157.50.1.10 (如图 1)。

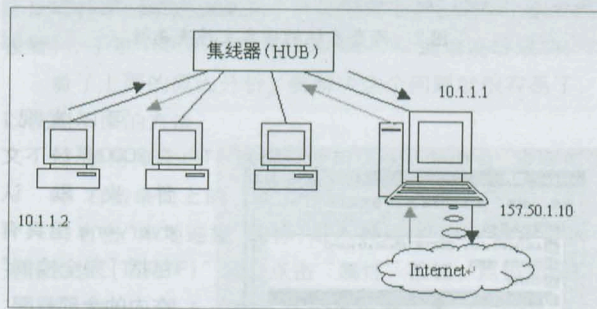


图 1 网络结构图

一个局域网的客户端 (10.1.1.2) 要浏览到互联网上的资源的过程是, 首先客户端发出一个请求要求访问局域网以外的资源的包, 包中包括源地址和端口号, 目的地址和端口号等信息, 客户端经过判断发现目的地址不在局域网中, 就将包发给配置了 NAT 的设备, 也就是 IP 地址为 10.1.1.1 的计算机, 这个由客户端 (10.1.1.2) 发送过来的包在 10.1.1.1 这台计算机中经过处理。在 NAT 设备上,

当第一次局域网中的客户端 (10.1.1.2) 请求访问互联网资源的包到达 10.1.1.1 这个设备上, 这台设备将建立一个映射列表, 其中添加源地址 (10.1.1.2) 到 NAT 设备的连接互联网的地址 (157.50.1.10) 映射的一条记录, 而局域网中各台计算机在映射列表中是以在 157.50.1.10 上分配不同的端口号来区别其不同请求, 而后每次无论是客户端向外部发出请求, 还是外部地址对请求的回复都经过 NAT 设备上的映射列表将其发送至正确的地址。因此 NAT 设备更像是一个中转站, 帮助局域网中的计算机访问本身不能够访问的地方。

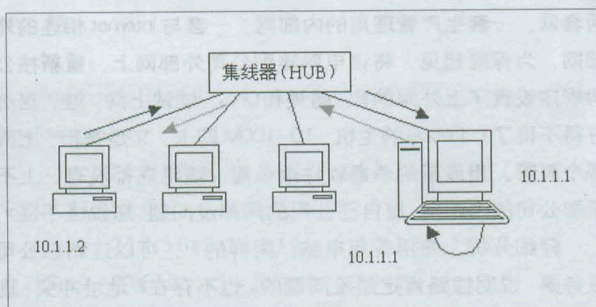


图2 网络拓扑

下面再来看一看错误的 NAT 配置如何导致网络故障的发生, 如图 2 所示仍是将局域网中的一台计算机 (10.1.1.1) 设置成 NAT 设备, 与图 1 不同的是没有一个为分配互联网地址的物理端口, 而且代替互联网地址的是 10.1.1.1 这个计算机本身的地址, 而映射列表的设置是将所有网络地址为 10.1.1.0 的计算机对应到 10.1.1.1 这台计算机上, 这样无形之中就将 10.1.1.1 这台计算机配置成为一个局域网中的多播地址, 只要是网络地址为 10.1.1.0 的计算机与 10.1.1.1 进行联系, 例如 10.1.1.2、10.1.1.0 就会将包修改其 IP 地址为 10.1.1.1 再发送出去, 根据网络的七层结果, IP 地址是在第三层网络层, 在包到达目的计算机后经过地址解析协议将 IP 地址与 MAC 地址的对应信息添加到 ARP 高速缓存中, 这时就出现了问题了, 由于传送的包的 IP 地址已经被改为 10.1.1.1, 而对应的硬件地址 (MAC) 即第二层仍然是 10.1.1.2 的 MAC 地址, 这样就会出现系统提示地址冲突的现象了。

当然这个问题最终的原因是错误的配置 NAT。需要注意不要在不了解的情况下随意设置 NAT, 同时网络管理员可以通过合理的配置网络设备的策略来避免这种问题的发生, 例如设置交换机上的端口过滤掉广播地址、多播地址, 使得即使配置了 NAT 的设备也无法将修改了 IP 地址的包再重新发送出去, 而当问题出现了以后, 需要去关注细节, 要从细微末节之处了解情况, 找出根源。

局域网内网络不通 故障浅析

■ 河北 韩军波

在“网上邻居”中只看到自己, 但却看不到网络中的其它机器的故障常有发生。出现这种情况, 首先确认网线是否插好, 相关的网络设备 Hub、交换机等是否工作正常。在出现这类问题时, 您应先从简单的方面去考虑, 除了确认网线已经插好外, 还要确认网线工作是否正常, 使用的是正线序还是反线序。连接不同类设备使用正线序, 如网卡——Hub/交换机; 连接同类设备使用反线序, 如 Hub/交换机——Hub/交换机 (有联连口的另当别论)、网卡——网卡。

如果一切正常, 仍然连不上网络就要看是不是同一个工作组的计算机有重名的情况。如果两个条件都正常, 就要看是不是协议的问题了。一般而言, 我们的局域网使用 TCP/IP 协议就足够了。首先用命令 ping 127.0.0.1 来确认本地的 TCP/IP 配置正确。有人试图用这个命令来判断网卡是否有故障, 这是不正确的, 因为 ICMP 被认为是 IP 层的一个组成部分, ping 本地地址到 IP 层的时候就短路了, 并没有调用到网卡驱动程序, 所以是无法判断网卡是否有故障的, 也没有使用到更高层协议 (如 TCP 协议); 实际上是如果 ping 命令返回正常的结果, 仅仅说明本地的 TCP/IP 协议安装正确。ping 局域网中的另外一台主机, 如果返回的结果正确, 但仍然无法在网上邻居中看到它, 表示对方计算机没有打开“文件和打印机共享”服务; 当然, 如果要是让别人看到您, 您也必须打开“文件和打印机共享”, 否则别人看不到您。

但在只有几台机器的对等网中, 可能没有主机提供所需的服务, TCP/IP 需要进行专门设置, 要指定各台计算机的 IP 地址, 并使它们处于同一个网段, 千万不要指定了两个同样的 IP 地址; 指定各台计算机网关为局域网中的同一台计算机 (服务器); 指定 DNS; 绑定文件和打印机共享和 Microsoft 网络客户, 其它可保留系统默认值。另外, 在对等网中本着“宁多勿缺”的原则, 对于其它协议也可以装上, 常见的有: IPX/SPX 兼容协议、NetBEUI 网络协议; 最后设置基本网络登录方式为“Microsoft 网络客户”。

一次奇怪的网络故障

■ 深圳 高峰

局域网的网络故障,大多在系统登录时有明确的提示,对于那些无须口令开机就自动联上网的电脑,也可以通过排除法找出故障的问题所在。前不久,我遭遇了一次奇怪的网络故障,问题原因很简单,但找到问题却颇费周折。

公司办公大楼内,有一客户租了几间办公室作办事处,其总公司设在市内另一个区。由于平时多业务往来,他们的电脑问题一般找我们帮忙解决。办事处内各办公室电脑组成小型局域网,再通过光纤与总公司联接,网络布线工程我们没有参与,他们公司技术科的人调试好设备后就回去了,日常一些电脑使用问题、网络故障,就由我们代为处理。平时也没什么大问题,一直相处太平。

有一天早上刚上班,接到电话,说有一台电脑连不到市区总公司。我准备好测试工具和备用线,就过来检测。我发现,这里其它办公室的电脑都可以正常连接到市内总公司服务器,就只有一台电脑连不上,而前一天使用还是可以的。这里的电脑都是固定IP,开机自动连接,无须输入登录口令密码。经咨询,问题已有一段时间,且时好时坏。该电脑安装的是Windows 98操作系统,网卡IP地址采取自定义,ping不到它们的网关和其它电脑,其它电脑也ping不过来。根据经验,我们首先检查了网线,没什么异常;又检查了联网的集线器,该电脑联接的集线器上端口指示灯显示正常,且也会随其它指示灯闪烁,换到其它正常的端口上,指示灯依然如其它灯一样闪烁,但仍连不上总公司,这从另一个方面说明线路应该是没问题的。我又检查电脑主机,可无论是从设备管理器中查看,还是ping网卡自身,都正常,可问题依旧。

同一个集线器,其它电脑正常使用,只有这一台连不上网,网络线路又没问题,电脑也好像是好的,那么问题在哪里呢?这里的电脑都采用固定IP,TCP/IP中也都设定了相同的网段、网关,甚至工作组也一样,IP设置也和之前记录的相同,应该不会有IP地址冲突,即使有冲突,开机时电脑也会有提示呀,事实上没有。作为测试,我们关掉一台使用正常的电脑,将该电脑的IP记下,移置到故障电脑上,理论上应该没问题。可是,电脑重新启动后,还是连不上;不停地更换集线器端口,除了指示灯如常闪烁外,故障依旧。原来使用正常的IP,移到这台电脑上,就不起作用了。难道这台电脑系统有问题?我们换上一台备用电脑,参照故障电脑原

来的IP一路设置过去,重新启动,OK,连上了!看来这台电脑系统是有问题。没关系,只要找到问题,拿回去,慢慢弄。

这奇怪的问题就出在将电脑拿回自己公司后:公司内有两套网,一套生产管理用的内部网,一套与Internet相连的外部网,为保险起见,将该电脑接到公司外部网上,重新按公司规定设置了上外网的IP、网关和DNS,试试上网,哇,居然好得不得了!PIII800的主机,10-100M网卡,又是宽带,上网那个爽呀。用最新的杀毒软件杀杀毒,啥毛病都没有。上不了那公司的内部网,接自己公司的网却没问题,您说怪不怪?

仔细分析,使用备用电脑,同样的IP,可以连到总公司服务器,说明线路肯定是没有问题的,也不存在IP地址冲突;现在又测试了故障电脑的软硬件,连到自己公司网上可以使用,电脑硬件、系统软件应该也没问题。可拿回去了就是不行,这实在无法理解。

我又去查看那办事处里的布线,发现这里没有放置服务器,所有办公室电脑通过网线联接到一个24口3COM集线器上,再通过光纤联出去。也就是说,他们的服务器、网关都在总公司那边,虽然距离比较远,但理论上布线也说得过去。在办事处内,备用电脑可以联上网,那么它与故障电脑有什么不同呢?操作系统都是Windows 98,网卡虽型号不同但都能正常使用,安装的软件有差异应该也没什么影响,影响上网的只有网络设置了,可网络不是也设置成一样过吗!再仔细看看,IP地址、子网掩码、网关、DNS、WINS、工作组等等,一路比下去,惟一不同的是网络标识。对呀,网络标识!一直注意IP冲突,没想过同一局域网内网络标识相同一样会有冲突,因为它也是惟一标识一台电脑哇!使用备用机,只是修改了IP地址、网关、DNS,没有留意到网络标识,当初怎么没想到呢。可标识相同电脑联网应该会报错呀?问使用人员,说之前的确动过一些地方,具体哪里早记不得了,因当时没出问题以为就没事。咨询总公司技术科,该电脑标识果然被改动过。立马把标识改回,接上网络,开机一试,通了。

可见,问题应该是使用人员无意间修改了网络标识,虽然与本地的电脑标识没有冲突,但可能与总公司服务器相连的其它办事处的电脑标识冲突;而我虽注意到了冲突问题,但过分注重IP地址的冲突,网络标识也只是在办事处内检查有无冲突,而忽略了该公司整个单位网。且该公司内同标识电脑如果没开机的话,也不大容易暴露问题。

近来我单位局域网经常无法连接到互联网上，重启路由器后，恢复正常，但过一段时间后又出现连不上网的情况。我单位的网络环境如下：联网工作站机器二十台，思科2621路由器一台，交换机一台，通过路由器作NAT地址转换，以一个公网地址（假设为217.56.6.38）上互联网，内部这二十台机器以地址10.250.3.1~10.250.3.253范围内选取。

在排除了线路、单机、病毒等故障后，我们重点放在了路由器上，通过在路由器上运行show ip nat tran命令，发现有几台计算机比较随机的向互联网上的主机发送大量的数据包，如：一台10.250.3.117的计算机不停的向网络发出ping包。

如下：

Pro	Inside global	Inside local	Outside local
Outside global			
icmp	217.56.6.38:512	10.250.3.117:512	
	10.250.22.192:512	10.250.22.192:512	
icmp	217.56.6.38:512	10.250.3.117:512	
	10.250.46.193:512	10.250.46.193:512	
icmp	217.56.6.38:512	10.250.3.117:512	
	10.250.38.193:512	10.250.38.193:512	
icmp	217.56.6.38:512	10.250.3.117:512	
	10.250.30.193:512	10.250.30.193:512	
icmp	217.56.6.38:512	10.250.3.117:512	
	10.250.22.193:512	10.250.22.193:512	
icmp	217.56.6.38:512	10.250.3.117:512	
	10.250.46.194:512	10.250.46.194:512	
.....			

当关闭了这台计算机，我们通过命令观察路由器CPU占用，从原来的50%下降到5%。用同样的方法，我们在另一个时间测试发现一台10.250.3.66的计算机不停的对互联网主机进行访问，我们关掉此计算机后，路由器的CPU由30%降到5%。

经过对类似情况的对比，我们发现这些机器上都运行一个叫BT的下载软件，此软件会不停地向互联网上提供这种服务的计算机发出数据包，数量相当大，占用路由大量的资源。分析原因，BT中有三个进程在运行时，特别是在BT和种子有很多时，BT会不停地向各服务器发送TCP数据包，以取得联系。这种连续的变换服务器和网络病毒的攻击导致路由器上的TCP NAT连接的数量剧增，从而占用了大量的CPU资源，最终路由器由于无内存空间运算而停止工作。

根据分析，我们认为这种故障是由于BT软件与路由器之间协调工作不顺造成的，根据前面的分析，我们将路由器的TCP timeout时间由原来的24小时改为现在的30分钟，TCP会话的动态映像的路由表中的停留时间默认是24小时

闹别扭的BT

山东吴兆达

(1440分钟)。命令为：

```
2621 # conf t
2621(config)# ip nat translation timeout 1800
```

在保存了配置后，我们查看路由器的CPU占有率，只有2%，网络正常，具体如下：

```
2621 # sh proc
CPU utilization for five seconds: 2%/2%; one minute: 2%; five minutes: 2%
PID QTy PC Runtime (ms) Invoked uSecs
Stacks TTY Process
1 Csp 803B831C 4 913 4
2644/3000 0 Load Meter
2 M* 0 344 163 211010196/
12000 0 Exec
3 Lst 8039F7BC 1312 463 2833
5828/6000 0 Check heaps
```

我们又在一两台机器上各开了六个BT进程，经测试CPU的占有率只有4%，完全可以进行正常工作。

导致这种情况的原因是BT等软件引起的路由器内存过度占用，原有NAT刷新时间过长，无法满足BT等软件的要求，通过修改路由器的NAT刷新时间就可以解决这种问题。■

China Information World

中国计算机报

www.ccidnet.com

百万IT专业读者 20年的选择

创刊于1985年，每周双刊，七大版面。周一出刊：《要闻》、《中国信息化》、《产品与应用》、《网络与通信》、《软件与服务》、《渠道与市场》，周三出刊：《周刊》，全面覆盖IT产业、行业应用及个人消费市场。

“20周年订报嘉年华”

活动说明：

■ 为庆祝创刊20周年，答谢广大读者，凡订阅2005年全年《中国计算机报》的读者，即可参加“20周年订报嘉年华”活动。

■ 每订阅1份可任选价值150元的礼品组合，礼品分为

- 超值精品（价值50元）
- 数码激情（价值100元）
- 时尚魅力（价值150元）
- 精致生活（价值200元）
- 完美体验（价值300元）
- 绝对经典（价值400元）

■ 本次活动截止日期为2005年1月15日，请您于截至日期前将邮局订阅收据原件及订阅回执单寄到报社（以寄出邮戳为准）

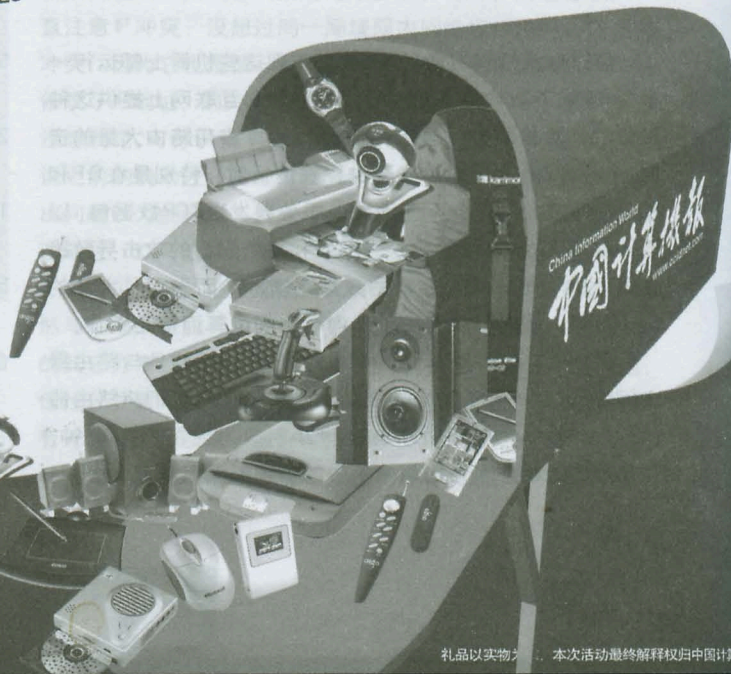
■ 邮寄地址：北京市海淀区紫竹院路66号赛迪大厦18层中国计算机报社发行推广部（信封正面注明“20周年订报嘉年华”字样） 邮编：100044

■ 活动详情敬请关注2004年66期至89期的《中国计算机报》，或拨打发行热线咨询。

■ 发行热线：北京010-88559888 上海021-63609657-117 深圳0755-83782360
广州020-87542809 西安029-88231769 沈阳024-23960217-604
成都028-66168880

邮发代号1-132
全年98期定价147元

（各地邮局均可订阅）



状态检测防火墙构建

■ 中国石油勘探开发研究院西北分院 杨志贤 冯超敏 陈靓

本文以 Linux 2.4 的内核为基础, 分析了嵌入 Linux 内核中的 Netfilter 的工作原理, 结合现实的网络环境实例, 在 Netfilter 强大包过滤功能和数据包处理的框架基础上, 借助 iptables 灵活、多变的用户空间实现工具, 为在复杂多变的网络环境中实现基于状态检测的过滤型防火墙提供了一种高效、快捷的手段。

在网络安全产品中, 防火墙颇引人注目, 已经成为实现网络安全非常基本的环节和安全屏障。防火墙的类型有很多种, 但是应用更广泛、技术更成熟的是过滤型防火墙。在过滤型防火墙中, 状态检测技术 (Stateful Packet Inspection) 为防火墙对数据的侦测和过滤增加了更为细致的工具。

防火墙既是一个软件, 也是一个系统, 它的数据包处理功能是建立在安全的操作系统之上, 和操作系统应该是浑然一体的。在这一方面, Linux 具有与生俱来的优势, 其强大的功能和安全特质吸引了众多的用户。在 Linux 2.4 内核中内嵌的 Netfilter 具有对数据流丰富的操作方式和对数据强大的过滤功能, 为构建功能强大的防火墙提供了潜在的手段和功能框架。

Netfilter 框架

Netfilter 是 linux2.4 内核中实现数据包过滤、数据包处理、NAT 等的功能框架, iptables 则是在这个功能框架之上实现数据包处理的用户空间的功能工具。Netfilter、iptables 和连接跟踪 (Connection Tracking) 与 NAT (Network Address Translation) 子系统一起构建数据流处理的整体框架。

Netfilter

Netfilter 提供了一个抽象、通用化的框架, Netfilter 框架包含以下三部分:

(1) 为每种网络协议 (IPv4、IPv6 等) 定义一套钩子函数 (Hooks) (IPv4 定义了 5 个钩子函数), 这些钩子函数在数据包流过协议栈的几个关键点被调用。

(2) 内核的任何模块可以对每种协议的一个或多个钩子进行注册, 实现挂接, 这样当某个数据包被传递给 Netfilter 框架时, 内核能检测是否有模块对该协议和钩子函数进行了注册。如果注册了, 则调用该模块注册时使用的回调函数, 这

样这些模块就有机会检查 (可能还会修改) 该数据包, 然后做出丢弃该数据包 (NF_DROP)、允许该数据包通过 (NF_ACCEPT)、接管该数据包 (NF_STOLEN) 或者指示 Netfilter 将该数据包传入用户空间的队列 (NF_QUEUE)。

(3) 那些排队的数据包是被传递给用户空间的, 并且这些数据被异步地进行处理。

Netfilter 是在协议栈 (IPv4、IPv6) 中不同点的一系列钩子函数。一个数据包按照图 1 所示的过程通过 Netfilter 系统:

数据包从左边 IN 进入系统, 进行简单完整性检查 (如数据包完整、IP 校验、非混杂模式接受等), 经过第一个钩子函数 NF_IP_PRE_ROUTING[PREROUTING] 进行处理, 然后就进入路由代码 (路由代码丢弃不可路由的数据包), 决定该数据包是需要转发到另一个接口还是发送到本机 (Localhost); 若该数据包是传送到本机的, 则该数据经过钩子函数 NF_IP_LOCAL_IN[INPUT] 处理后传递给上层协议; 若该数据包是被转发到另一个接口, 则它被 NF_IP_FORWARD[FORWARD] 处理; 经过转发的数据包经过最后一个钩子函数 NF_IP_POST_ROUTING[POSTROUTING] 处理后, 再传输到网络上。

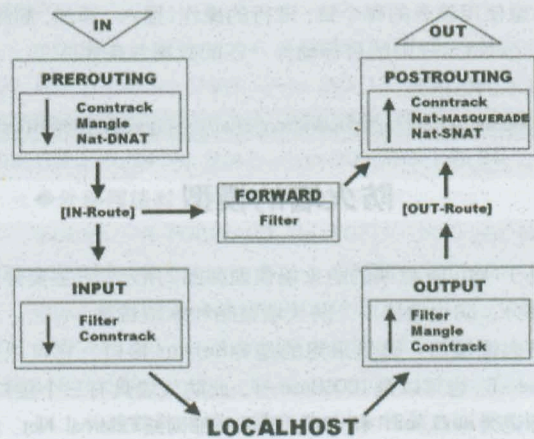


图 1 数据包过程

本地产生的数据经过钩子函数 NF_IP_LOCAL_OUT[OUTPUT] 处理后, 进行路由选择处理, 然后经过 NF_IP_POST_ROUTING[POSTROUTING] 处理后发送到网络上。

2005年1月 责任编辑：孙红娜 美术编辑：庆琨

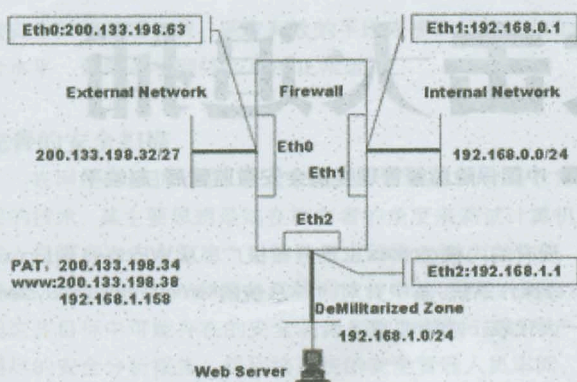


图3 典型网络拓扑图

实现

在图3所示的网络环境中实现基于 Netfilter 框架的防火墙，主要运用用户空间的数据包选择系统 iptables 为手段，从以下三个方面构建一个较为完善的、能够实现基本网络环境的防火墙。

(1) 防火墙缺省策略

防火墙采用的缺省策略：禁止策略，即未被明确表示允许即被禁止。

```
iptables -A INPUT -i eth0 -j DROP
iptables -A OUTPUT -o eth0 -j DROP
iptables -A INPUT -i eth1 -j DROP
iptables -A OUTPUT -o eth1 -j DROP
iptables -A INPUT -i eth2 -j DROP
iptables -A OUTPUT -o eth2 -j DROP
```

(2) 防火墙自身安全

防火墙是网络的安全屏障，首先必须保证自身的安全，这样保障网络安全才有基础。

◆允许 loopback 接口传输

```
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT
```

◆防止 SYN-FLOOD 攻击

```
iptables -N syn-flood
iptables -A INPUT -i -p tcp eth0 --syn -j syn-flood
iptables -A syn-flood -m limit --limit 1/s --limit-burst 4 -j RETURN
iptables -A syn-flood -j DROP
iptables -A INPUT -i eth0 -p tcp !--syn -m state --state NEW -j DROP
```

◆防止地址欺骗 (IP SPOOFING)

```
iptables -A INPUT -i eth0 -s 192.168.0.0/24 -j DROP
iptables -A INPUT -i eth0 -s 192.168.1.0/24 -j DROP
```

◆防止 IP 碎片攻击

```
iptables -A FORWARD -f -m limit --limit 100/s --
```

```
limit-burst 100 -j ACCEPT?
```

◆防止 ICMP 攻击

```
iptables -A FORWARD -p icmp --type echo-request -d 192.168.0.0/24 -i eth0 -m state ESTABLISHED, RELATED -j ACCEPT
iptables -A FORWARD -p icmp --type echo-request -d 192.168.0.0/24 -i eth0 -m state ESTABLISHED, RELATED -j ACCEPT
```

仅接受由内部网络发起的 ping 命令。

(3) 网络之间的访问策略

在图3所示的网络环境中，安全级别最高的是内部网络的安全性，次之的是 DMZ，安全性最低的是外部网络。总的访问原则是高安全级别的网络可以完全访问安全性低的网络，而低安全级别的网络不能访问高安全性的网络。但是对于 DMZ 区所提供的具体服务，仅允许外部网络访问特定的服务端口，如外部网络仅能访问 Web 服务器的 80 端口。

◆内部网络对外部网络的访问

```
iptables -A FORWARD -s 192.168.0.0/24 -i eth1 -j ACCEPT
iptables -A FORWARD -i eth0 -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -t nat -A POSTROUTING -o eth0 -s 192.168.0.0/24 -j SNAT --to 200.133.198.34
```

◆内部网络对 Web 服务器的访问

```
iptables -t nat -A POSTROUTING -o eth2 -s 192.168.0.0/24 -j SNAT --to 192.168.1.254
```

◆DMZ 区对外部网络的访问

```
iptables -A FORWARD -s 192.168.1.0/24 -i eth2 -j ACCEPT
iptables -t nat -A POSTROUTING -o eth0 -s 192.168.1.158 -j SNAT --to 200.133.198.38
iptables -t nat -A POSTROUTING -o eth0 -s 192.168.1.0/24 -j SNAT --to 200.133.198.34
```

◆外部网络对 Web 服务器的访问

```
iptables -A FORWARD -p TCP -i eth0 -o eth2 -d 200.133.198.38 --dport 80 -j ACCEPT
iptables -t nat -A PREROUTING -p TCP -i eth0 -d 200.133.198.38 --dport 80 -j DNAT --to-destination 192.168.1.158
```

以上构建的防火墙，是在 Netfilter 框架内以 iptables 为手段所构架的具有状态检测功能的过滤型防火墙，它只在网络层和传输层操作，因而对用户而言，网络是透明的。

点评：在网络的实际应用中，基于 Netfilter 的过滤型防火墙不失为一种很好的、高性价比选择，在具体实现网络安全时，具有实际的参考意义。

新型网络攻击大追捕

■ 中国保险监督管理委员会安徽监管局 赵皖平

绝对的安全是不存在的,因为信息安全是一个动态发展的过程,每个网络都有一定程度的漏洞和风险。尤其是今天,新一代的攻击手段更加智能化,攻击目标直指TCP/IP和操作系统层次,向用户的信息安全防范能力发起了挑战。

新型攻击方式

随着技术的发展,新的计算机攻击手段层出不穷,常见的有主动式网络嗅探、内核rootkits、嗅探/后门技术、分布式反射拒绝服务攻击DRDoS等。

主动式网络嗅探

网络嗅探(Sniffer)技术有了进一步的提高,具有主动控制通信数据的强大功能。这种技术的主要思想是主动向网络发送攻击数据包,以主机为基础,重定向网络上的通信数据,使得攻击者能够窃听交换网络内的数据包。特别需要指出的是,即使攻击者和被攻击者分布在不同的局域网时,主动式Sniffer也能够跨越交换机,帮助攻击者收集到足够的数据包。

在交换网络下,Sniffer技术改写了ARP缓存内容,修改目标计算机的IP地址到Mac帧地址的映射,重定向有关的通信数据包,使得这些数据包直接由交换机发往攻击者的机器。同时,攻击者还可以采取IP欺骗、DNS欺骗等多种方式,跨越不同的局域网,重定向所需的通信数据包,达到监听的目的。Dsniff工具软件是主动式Sniffer技术的代表者,甚至还提供了面向SSH和SSL的“代理人”攻击工具包。

此外,由于无线网络使用功能较弱的WEP加密技术,易于受到攻击,近年来无线Sniffer逐渐成为无线网络安全的重大威胁。

内核rootkits

内核rootkits是典型的“特洛伊木马”技术。随着攻击技术的提高,rootkits得到了长足的发展,可以直接操作操作系统的底层内核,实现对计算机系统的全面控制。

内核rootkits可以修改操作系统的核心底层,置入特定的代码段。一般来说,这些代码都具有重定向系统调用的能力,并隐藏实际运行的进程、打开的文件和被占用的端口等情况,阻止用户获得真实的系统情况。

这样一个被修改内核的操作系统从功能上看,与标准的系统没有区别。但当用户执行类似ls、su之类的指令时,有关的系统和用户信息将被内核rootkits泄露给攻击者。

现有的内核rootkits工具分布极广,从Windows到Linux、Unix等操作系统,其中针对Linux系统的Kernel Intrusion System是一大代表,功能非常强大。

新型的嗅探/后门技术

新型的后门攻击手段结合了嗅探技术(Sniffer)和后门技术(Backdoors),变得更加隐蔽、难以察觉。它采用Sniffer技术,按照类型匹配算法收集后门攻击者发过来的数据,执行相应的指令。这种技术既可以工作在混杂模式下,也可以工作在非混杂模式下。

提示:这里所谓的混杂模式就是改变网卡默认设置(网卡在默认状态下只接收属于自己的数据包),使其接受所有数据包,这是网络监听的标准工作模式。

充当非混杂模式的Sniffer/Backdoors只能用来监听宿主机的数据包,是攻击行为的具体执行者。而充当混杂模式的Sniffer/Backdoors则可以监听网络上所有主机的通信数据包。攻击者完全可以利用这种技术给管理人员的安全追踪制造障碍:攻击者在网络内的A主机放置Sniffer/Backdoors,监视B主机的通信;为了掩盖攻击痕迹,攻击者向B主机发送攻击指令,让管理员误以为是B主机上存在后门。SAdoor就是一个功能较强的Sniffer/Backdoors程序。

分布式反射拒绝服务攻击DRDoS

最近,DDoS技术转变为分布式反射拒绝服务攻击DRDoS(Distributed Reflection Denial of Service Attack)。

这种新技术实质上是对SYN Flood的改进,其基本思想是利用TCP协议的三次握手机制:攻击者通过DDoS代理向任意一台主机发送一个TCP SYN数据包,包中的源地址设为要攻击的目标主机地址;该主机收到该包后,自动向包中的源地址回送一个TCP SYN-ACK的响应包。在这种情况下,攻击者可以采用多线程,同一源地址连续不断地向多台高带宽主机发送数据包,形成令人畏惧的SYN Flood攻击潮。因此,目标主机将受到网络上多台服务器的同时攻击,很难幸免,且无法查出攻击者的真实地址。

有效的网络安全防范手段

为了应对日益变化的网络攻击技术,必须建立一个全面、系统的网络安全体系:网络的基础架构必须是以三层交换和路由为核心的智能型网络,在此基础上,综合运用完善的三

层安全策略管理工具,采取有效的手段来提高网络系统的安全水平,保障各项网络应用的正常运行。

完善的安全扫描

在网络安全防范中,安全扫描是一项基本的也是非常重要的技术,其主要思想是站在攻击者的角度来测试计算机系统上是否存在安全隐患,主要用于对网络主机、工作站、交换机、路由器、WWW服务和数据库应用等项目的检查,找出这些目标中可能存在的安全漏洞,最后根据扫描结果产生详尽的安全分析报告,供网络系统的安全管理人员审阅。

现有的安全扫描器主要分为三种类型:端口服务扫描工具,能够自动检测目的主机的操作系统类型,扫描所有的端口,确认端口服务的合法性,但无法检测整个系统的安全漏洞,比如Nmap;安全漏洞扫描工具,针对已知的系统安全漏洞扫描,分析整个计算机系统,发现系统的安全隐患,如Whisker;分布式安全测评系统,能从浏览器直接提交指令,实现对多扫描用户的权限管理,还可以出具完整的安全报告,帮助系统安全管理人员分析、了解计算机系统的安全漏洞以及解决方法,如CNNS Scanner。

全面使用加密技术

为了保障网络应用的安全,可以采用数据加密手段。这样,即使攻击者通过Sniffer抓取到了传输的数据信息,但這些以密文传输的数据对他来说也没有什么实际意义。在实际运用中,作为Telnet、ftp等安全替代产品,可以考虑采用安全的SSH2替换掉不安全的采用明文传输数据的服务,如在Server端用SSH、Openssh等替换系统自带的Telnet、ftp等,在Client端使用securecrt、sshtransfer等替代Telnet、ftp等。

如果网络应用对安全性要求比较高,可以考虑采用安全认证机制,如kerberos就是面向开放系统的一种为网络通信提供可信第三方服务的认证机制。它提供了一种强加密机制,使Client端和Server即使在非安全的网络连接环境中也能确认彼此的身份,而且在双方通过身份认证后,后续的所有通讯也是被加密的。在实现中,建立与可信的第三方服务器通讯的系统的密钥数据库,只有kerberos和与之通讯的系统本身拥有私钥(private key),然后通过private key以及认证时创建的session key来实现可信的网络通讯连接。

建立牢固的计算机系统

为了防范攻击者对主机系统的恶意监听,应采取多种措施来建立牢固的“堡垒主机”,如关闭所有非必须的服务及端口、及时安装各类系统补丁等。同时,针对现有的攻击手段,有针对性地采取预防措施:

保护ARP缓存表 以Dsniff为代表的主动式网络嗅探工具能够突破交换机的安全监控。为了防止类似工具改写ARP缓存表,可以对相关网络中主机的ARP缓存表进行硬编码,结

合前述的加密技术来保护重要信息。为防止对无线网络的监听攻击,可以采用无线VPN来增强系统的认证和加密功能。

监控系统内核 为了更有效地应对rootkits攻击,可以使用检查工具来检查系统中二进制执行程序的完整性,同时保证系统内核的完整性;监测系统调用表的修改情况;将系统配置成为固化内核,建立一个非可重用内核模块的系统内核。这样就可以简化内存管理,提高系统的效率,像St.Jude Project软件就可以监测Linux系统内核的完整性。

扫描系统端口和网卡模式 为了查找非法开放的端口服务,可以定期检测端口,防止非法的后门服务,也可以使用工具软件,从远程检测异常端口的占用情况,特别要关注以超级用户权限运行的进程。Nmap软件就可以完成上述功能。同时,为了检测网卡是否处于混杂工作模式,还可以使用相关工具,如用于Windows系统的PromiscDetect软件。

应对SYN Flood攻击

对于普通的DDoS攻击,可以反向跟踪数据包,查找攻击来源。而对于DRDoS攻击,就必须采取整体解决方案。

首先要及时发现并过滤Flood数据包,目前有两类工具可用:一类是基于探头的设计,这些探头被设置到网络的关键节点上,能通过异常扫描技术来发现可疑的Flood数据包,及时地调整路由器和防火墙的过滤设置;第二类则直接在网络边界处发现和过滤Flood数据包。

由于不论采取何种防范措施,涌来的SYN Flood数据包都会占用宝贵的网络带宽,使系统反应缓慢甚至停滞,所以,应对DRDoS攻击的另一个方向是完善和发挥ISP的应急机制,从上游过滤和杜绝Flood数据包。

建立良好的编码规范

Web应用是网络发展的推动力,必须形成良好的编程规范和代码检测机制,防范对Web系统的攻击。Web应用程序的开发者要深刻理解应用系统面临的威胁,有意识地构建安全防御机制,提高系统的安全防护。通过使用hash函数、时间戳、数字签名等技术来保护发送到服务器或浏览器的敏感数据;检查用户的输入,过滤可能危及数据库系统的特殊字符、脚本语言和命令,要特别指出的是,这个检测机制必须安置在服务器上,而不能放在浏览器上实现。

目前,有些Web应用防护工具可以分析所有的Web连接,防止常见的应用层攻击和应用层的敏感数据泄露。它们具有学习能力,能够理解正常的Web访问,当出现可疑的修改操作或特殊字符序列时,将拦截非法指令并报告异常访问。如SPI Dynamics开发的WebInspect软件就可完成上述功能。

在网络世界的安全不断受到挑战的情况下,我们必须不断提高网络安全防范意识,了解网络攻击的原理和手段,正确运用相关的防护手段,建立全面的互联网络安全防范机制,斩断非法攻击的黑手,让网络会变得越来越安全。■

可伸缩性的网络反病毒体系

对于一个计算机系统来说,可伸缩性(Scalability)是指其体系结构能够在何种程度上不断扩展以满足用户动态需求的特性,用来衡量用于分布式环境的所有应用与技术在功能方面的质量。可伸缩性的体现方式多种多样:可以是移植,也可以是提升原来的系统的性能、增添模块、或者是向群集中增加新的节点等。企业网络结构和环境相对复杂,规模较大,且其反病毒工作具有鲜明的整体效应,可伸缩性必然成为企业网络反病毒体系构建的侧重点之一。

企业网络反病毒体系的可伸缩性:

物理区域部署灵活可调

目前企业网络最基本的形式是企业局域网(Enterprise LAN),这是大多数企业OA系统的基础;同时,对于拥有众多驻外机构,需要随时沟通联系的企业来说,企业广域网(Enterprise WAN)起到的桥梁作用必不可少。这种结构决定了反病毒体系必须要在不同系统环境下提供统一防护,而其前提是能够提供可伸缩的物理区域部署能力。对于企业局域网内各已有节点,反病毒体系必须做到全面覆盖,出现新增节点时需要及时纳入体系之中,以防成为最易受攻击的薄弱环节。对于大型企业而言,众多的跨地域驻外机构的网络同样有病毒防护需求,并且这种需求是动态变化的:紧跟市场的经营策略随时可能面临调整,驻外机构会遇到诸如新增、搬迁、撤销等情况,对此同样需要企业网络的整体反病毒体系具备灵活调整、跨物理区域灵活部署的特性。

升级扩展快捷智能

对于企业网络而言,需面对的各种病毒威胁快速增长、不断变化,反病毒体系的升级和扩展应做到快捷智能,其中病毒定义是最基本的升级内容,同时也包括体系本身的功能和模块。为了最大限度地增加了系统正常运行时间,并有效降低升级扩展带来的成本增加,应做到增量升级扩展,无需重新部署软件或重启系统。

管理控制随需变化

与单机用户不同,企业网络反病毒重在管理,而管理在反病毒体系的可伸缩性上体现为——安全策略针对需求、对受管理的节点动态可控、实时的安全信息反馈收集。

安全策略针对需求:企业拥有众多的部门机构,缺乏灵活针对性的安全策略将会导致应用冲突,同时,各个部门内部的安全需求也处于变化之中,当遇到大规模病毒爆发等紧急安全事件时也要求快速制定并配置应对措施。

对被管理节点动态可控:对被管理节点进行动态实时的控制,这包括防护策略的定制执行、病毒查杀等。

实时的安全信息反馈收集:网络管理者需要得到最新的安全信息才能作出正确有效的决策——包括实时的日志、客户机安全状况信息反馈等。

金山毒霸网络版可伸缩性反病毒解决方案

B/S 分级架构可调

金山毒霸网络版反病毒体系采用了业内领先的B/S架构设计,有效地避免了因为数据分布造成的安全性、一致性和实时性问题。

结合无限分层的多级管理,实现了快速贴和用户需求的自适应扩张。管理中心提供了对整个防毒体系的集中管理,可通过基于WEB的控制台对管理中心进行远程操作,从而实现对整个防毒体系的远程管理。管理中心还可以对跨Internet的二级节点进行管理,以将跨地域分支机构纳入到统一的防病毒体系。系统中心提供对执行端的集中管理,可以直接向执行端发布指令或改变其配置选项。体系的执行终端包括客户端和服务端,它接受系统中心指令并应用指定的配置选项,从指定的升级服务器进行升级更新。它对网络内每台主机提供了直接的保护,并有效地执行防毒策略。

部署灵活快捷

金山毒霸网络版提供了WEB页面(ActiveX)安装、远程控制安装、域脚本安装、光盘安装等方式,管理员可根据网络环境灵活采用,能够在较短的时间内完成网络内部众多客户端的安装作业,简单快速的实现整个网络反病毒体系的部署,包括对跨地域的驻外机构实施部署。

优秀的系统环境兼容性

金山毒霸网络版反病毒体系兼容目前常见的多种操作系统,包括Windows NT WorkStation 4.0, Windows 98 / 98 Second Edition, Windows ME, Windows 2000 Professional, Windows XP Professional / Home Edition, Linux等。在保证高效防护的基础上最大限度地减少了资源占用,对硬件系统要求较低,可以灵活地应用于多种网络环境。

升级扩展智能

金山毒霸网络版反病毒体系采用了独立的级联升级体系,保证了升级扩展智能化。单出口的升级方式加上分发升级数据的升级过程也最大限度地降低了对网络带宽占用。通过贴和网络环境的升级服务器部署,可以实现升级数据流的可控和负载均衡。用户可以选择定时升级设置,及时获取最新的扩展。升级服务器可以为终端提供升级更新及漏洞修补程序下载代理,以保证整个防毒体系持续有效。体系中的管理、升级、执行端均能实现无重启的增量快速升级,在保证了对防护的持续不间断和系统正常运行的同时降低了扩展成本。

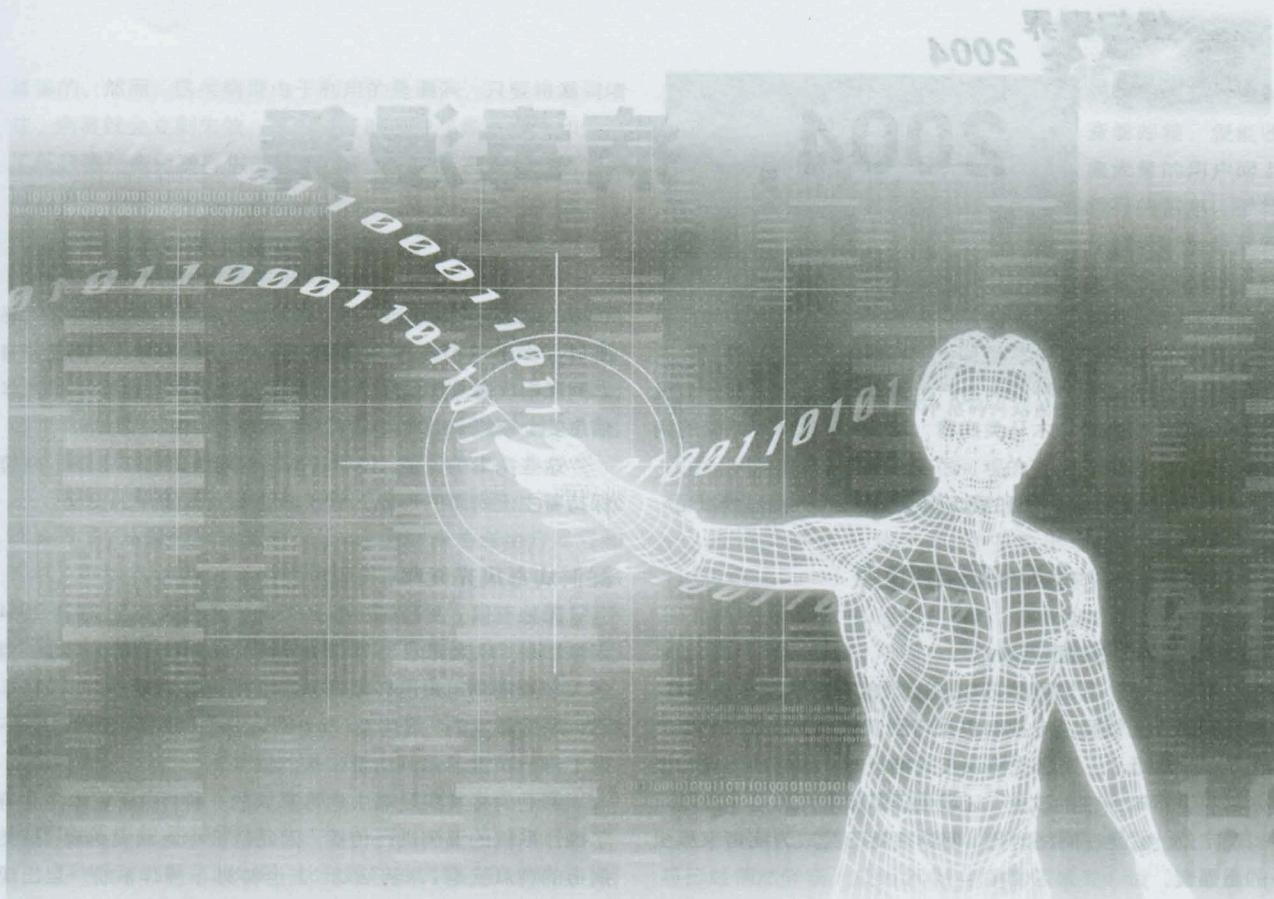
安全策略随需配置

通过分组及分组策略配置功能,管理员可以实现安全策略的统一配置、针对性配置并能够集中分发。用户可根据安全需求按部门、用户工作性质、操作系统等划分标准自定义分组,并且针对不同的组实施不同病毒防护策略。同时,金山毒霸网络版在对各组反病毒的准确定位基础上能够进行策略统一配置,网络管理员只要通过可移动的控制台就可以对全网进行策略集中制定、分发和变更。通过组策略的应用,金山毒霸网络版反病毒体系实现了安全策略弹性随需。

金山毒霸

DAV Corporate Edition 网络版

dbnet.kingsoft.com



横扫毒界之 2004

在信息安全领域,病毒与反病毒始终是最活跃的两支力量,而一年一度的病毒回顾可谓是安全界的年度大餐,使我们能够在须臾之间便可将一年的病毒现状与流行趋势尽收眼底,为下一年的信息安全建设做一个参考。

“关注行业、检查自己”,永远是企业进行信息安全建设的原则。

- ◆ 2004, 病毒漫舞
- ◆ 蠕虫遍布整个网络
- ◆ 木马劫掠真实财产
- ◆ 脚本病毒甘做幕后帮凶
- ◆ 2004 年毒界“风云”榜
- ◆ 与毒过招
- ◆ 防毒路上, 还欠缺什么?

横扫毒界
之 2004

2004, 病毒漫舞

■ 安天实验室 张晓兵

2004年,病毒依然保持着高速发展的势头,有关资料显示,2004年全年产生的病毒种类已经达到了25000种,大大超过了2003年20000种的病毒产生数量,这其中大部分为没有感染能力的蠕虫、木马类病毒,而像CIH这种可感染的病毒则是少之又少。

2004年的病毒与反病毒的风云际会到底呈现出哪些特点呢?

2004 病毒特点

网络病毒仍是主流

不可否认,互联网依旧以超出想象的速度迅速膨胀着,与此同时,无线网、电视网也都得到了长足的发展,IPv6产生了,3G走近了。当这些协议正式推行时,网络的规模和概念都将进行革命性的改变,让我们无从猜测,但有一点是可以确定的,就是在网络时代,网络病毒已经成为病毒家族里的超强音。

网络病毒是一个广泛的概念,它是指通过网页、邮件、即时通信、P2P等网络手段进行传播的蠕虫、木马、黑客程序等病毒的总称。无论从数量上还是发作情况来看,网络病毒都是2004年最大的“赢家”。去年初的“SCO炸弹(Worm.Novarg/Worm.MYDoom)”大家是否还记忆犹新?该病毒通过邮件疯狂

传播,其速度不亚于当年的“求职信”病毒,而去年中的“恶鹰(Worm.Bagle)”与“网络天空(Worm.NetSky)”病毒作者之间互相攻击、竞相推出病毒新变种的现象,也成为2004年信息安全领域一道难得一见的“风景”。

这些病毒的泛滥,说明了网络病毒继2003年以来,继续保持着主流病毒的形象,继续威胁着上网用户的安全。

漏洞病毒风光无限

无独有偶,漏洞病毒继2003年“大出风头”以后,2004年依然是“风光无限”。2003年8月份冲击波病毒的爆发,相信大多数电脑用户已经领略到了这类病毒的威力,而2004年五一期间爆发的“震荡波(Worm.Sasser)”病毒,更使人们不得不再一次重温漏洞病毒带来的噩梦。

漏洞病毒其实是蠕虫病毒家族的一种,由于它本身利用了操作系统的漏洞进行传播,因此也被称为漏洞病毒,这类病毒的特点就是“来势汹汹,去也匆匆”。操作系统一旦出现重大漏洞,就等于所有的电脑用户都为病毒打开了一扇毫无防备的大门,让病毒可以来去自由。另一方面,重大的操作系统漏洞往往是核心程序出现了问题,病毒一旦利用这些漏洞进行攻击的话,就会使用户电脑的操作系统崩溃,从而出现各种怪异现象。因此,只要是漏洞病毒爆发,一定是天下

一月毒星

MyDoom (Worm.Novarg/Worm.MYDoom)

闪光点:最有领导潜力的病毒

一月的病毒明星要算是MyDoom了,也叫SCO炸弹。它会通过邮件疯狂传播,传播速度不亚于当年的“求职信”病毒,运行时发送标题为:“Error”、“Mail Transaction Failed”、等内容,附件后缀为“.bat”、“cmd”、“exe”、“pif”、“scr”、“zip”的病毒邮件。这家伙自产生以来,不断地出现新变种,二月份出现了两个重要变种C和D。截止到年底,共出现了50多个病毒变种,单看它联合所有被感染的电脑对SCO网站发起的攻击,就知道它有多大的领导能力了。

二月毒星

贝革热(Worm.Bagle/Worm.BBeagle)

闪光点:最疯狂的病毒

二月份是贝革热(也称恶鹰)病毒的世界,它也利用电子邮件传播,传播力极强。该病毒有几个特点:第一是会自

我升级,每隔一断时间登录一个网址,自动下载新版本;第二是会自杀,它会检测系统时间,如果是2004年2月25日则自动退出系统并停止传播。据猜测,这样做的目的是想测试一下病毒传播的情况,以便改进。该病毒自产生以来,也是变种繁多,目前已经有了将近100个变种。该病毒的特点是传播疯狂、做法疯狂,而且还疯狂地产生下一代。

三月毒星

网络天空(Worm.NetSky)

闪光点:最虚伪的病毒

虽然网络天空病毒在二月份就已经产生,但它在三月才开始真正泛滥。同前两个月的病毒明星一样,它也是一个通过邮件进行疯狂传播的蠕虫病毒。值得一提的是,该病毒曾在其第11个变种的病毒体里留下“该病毒将是我的最后一个版本”的话,着实让用户松了一口气。而事实上,这只是一句美丽的谎言,之后,它又推出了多个变种,至今病毒变种已经达了40多个。

皆惊的。然而，这类病毒由于利用的是漏洞，只要将漏洞堵住，病毒就会立刻失效，当用户及时下载了微软补丁和使用反病毒厂商免费提供的病毒专杀工具后，它们就会成为过眼云烟，在短时间内消散的。

即时通信、网游病毒全面开花

2004年还有一点也颇引起人注目，那就是即时通信工具大战和网游大战了。在QQ成为即时通信的王者，MSN Messenger成为第二之后，立刻引发了即时通信工具的大战，这种现象使得即时通信立刻成为继邮件之后的又一大平台，从而滋生了大量的即时通信病毒。

可别小看这些年纪轻轻的病毒，它们可是经过了好几代的变异了，从最初只偷盗聊天记录，到后来偷盗用户账号和密码，再到2004年在即时通信工具里发送病毒网址来诱惑用户中毒，这类病毒的能力也越来越强。而新兴的MSN Messenger即时通信工具也陆续出现了类似“MSN射手”、MSN骗子(Worm.MSN.fun)这样的病毒。种种情况表明，病毒编写者开始全面介入这一新兴平台，以后这类病毒将会越来越多。

病毒的商业化趋势明显

2004年，继震荡波之后，比较惹眼的病毒恐怕要算是“网银大盗”系列病毒和“快乐耳朵”病毒了，如果您了解了这类病毒的特性，就会觉得那些网游病毒只是小儿科了。

这类病毒不再拐弯抹角，而是直接盯上了赤裸裸的金钱，就像是一个间谍，会隐藏在用户的电脑中，当发现用户登录网上银行时，便把用户名和密码记录下来，发送到指定的邮件，

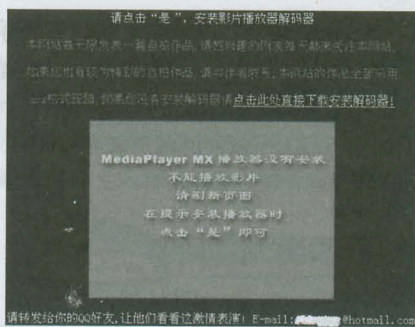


图1 “快乐耳朵”诱惑用户中招的网站画面

但是这类病毒一旦泛滥，积少成多，也是一笔很可观的资金，如果这类病毒的编写成风，将会极大地阻碍网上银行这类新生事物的发展。

而在2004年11月下旬出现的“股票窃密者(TrojanSpy.Stock)”则更甚，专门针对数家国内证券公司的网络交易系统编写。如果用户中毒，病毒会窃取用户的股票网络交易账号和密码，从而可以恶意买卖用户的股票，造成用户的资金损失。从这些事例中可以看到，病毒的商业化趋势已经越来越明显。

手机病毒在成长中发展

当人们还在争论手机中到底有没有病毒的时候，手机病毒已经悄然降临，成为2004年病毒领域又一道“风景”。

在第一例手机病毒“洪流”沉寂了两年后，手机病毒从2004年6月开始发起了第二次攻击浪潮。

很明显，这次手机病毒都不约而同地盯上了智能手机。2004年年中时出现了“卡波尔(Worm.Symbian.Cabir.a)”、“灰尘(WinCE4.Dust)”、“布兰多(Backdoor.Wince.Brador.a)”

四月毒星

QQ播客(Trojan.QQMSG.Boker.d)

闪光点：最煽情的病毒

该病毒属于QQ尾巴类病毒，会利用QQ发送例如“……钓鱼岛是中国的领土!!!台湾是中国不可分割的一部分!!!请将此消息发给您QQ上的好友!”等消息，消息后面是一个网址。虽然病毒发的消息很煽情，但是大家千万不要相信，因为这消息后面跟随的是病毒的网址，用户只要一点，就会中毒，从而再次感染线上的其他好友。该病毒自诞生那天起也产生了80个病毒变种。

五月毒星

震荡波(Worm.Sasser)

闪光点：传播范围最广的病毒

五月可谓名符其实的病毒月，爆发了堪称2004年毒王的震荡波病毒。该病毒利用LSASS漏洞进行传播，只要没有打过该补丁的操作系统都会受到该病毒的攻击，其感染范围和

破坏程序都超过了2003年的冲击波病毒。虽然它只产生了7个变种，但是足以让人们记住。而且，五月甚至还有一个好心的病毒作者编写了“震荡波杀手”工具，只可惜它在清除电脑中的震荡波病毒的同时，让用户的系统改受该“杀手”的继续攻击。

六月毒星

卡波尔(Worm.Symbian.Cabir.a)

闪光点：最时尚的病毒

虽然它还是一个概念型的病毒，但却标志着智能手机病毒开始正式登上病毒的舞台。病毒运行会感染采用Symbian操作系统的诺基亚型手机，并能通过手机的蓝牙功能进行传播感染。这是全球首个完全在智能手机上运行并感染的蠕虫病毒。该病毒最早出现在欧洲，发作时会在手机上显示“CARIBE-VZ/29A”字样，并且在Symbian操作系统的系统目录下释放多个病毒体，但并没有对系统产生破坏动作。即使如此，用户也得小心了，因为很可能会出现更多的有破坏性的病毒。

等多种智能手机病毒, 年终时又出现了可以通过控制PC来向手机发送垃圾信息的“Delf-HA”病毒、影响Symbian手机操作系统的“头盖骨 (Skull)”病毒等。

与此同时, Sun公司手机版Java软件的两个漏洞被发现, 蓝牙设备的三个重大漏洞也被发现, 还有人制作出了能破坏蓝牙设备的蓝牙枪。

反病毒技术的 2004

虽然随着反病毒技术的发展, 病毒已经成为可以控制的变量, 但病毒与反病毒之间的战斗永远也不会结束, 它们之间是水涨船高的关系, 随着病毒的变异, 反病毒公司依然要长时间走着技术革新的道路。

驱动级编程技术得到发展

每年反病毒公司都会在年终推出新版的杀毒软件, 这些杀毒软件里使用的新技术就成了反病毒技术革新的证据。

驱动级编程技术是2004年KV2005使用的技术, 它采用驱动编程的思想, 将反病毒引擎从应用层移到了核心层。这样做的好处是使病毒的查杀速度更快, 对病毒监控得更彻底。但也会产生不好的影响, 就是编程难度增加, 如果不经大量的测试, 会给操作系统带来不稳定的隐患。不过, 无论怎

样, 这种技术的产生与应用都是反病毒技术上的一个进步, 因为只有同操作系统结合得越紧密, 对病毒的防护才会越有效。

单机网络化的趋势开始明显

随着技术的发展和下移, 许多原来网络版里使用的技术开始更多地在单机版的杀毒软件中体现, 成为2004年反病毒技术上的又一个亮点。

瑞星杀毒软件2005版就是一个典型的例子, 其网络黑名单技术使得单机用户能够在局域网环境下很好地防御像FUNLOVE、尼姆达这样通过网络传播的病毒, 其漏洞监控技术也为单机用户在局域网中的使用建立起一道防线。

病毒监控技术更加完善

病毒监控技术自产生之时起就得到了反病毒公司的大力推崇, 经过几年的发展, 成为反病毒的一支重要力量。如果说病毒查杀技术是“亡羊补牢”的话, 那么病毒监控技术就是“未雨绸缪”, 对用户来说是更加有用的一种技术, 于是病毒监控技术的完善便成了2004年反病毒技术的又一话题。

纵观新近推出的新版杀毒软件, 给用户留下深刻印象的恐怕要算监控系统了。江民推出了七大监控系统, 瑞星则推出了八大监控系统, 虽然监控系统越多, 会对资源占用越多, 但是对于机器配置较好的用户来说, 使电脑更安全才是根本。

七月毒星

拉兹 (Trojan.Win32.Lasta)

闪光点: 最“安全”的病毒

七月的拉兹病毒是数据保护行业的一个耻辱。它利用了某系统保护和还原软件的漏洞, 当用户使用这类保护软件进行系统恢复时, 并不能将该病毒恢复掉, 而下次用户以为系统是干净的要再次保护时, 该病毒就会被做为正常的程序进行保护。这样一来, 该病毒就相当于多了一个保护膜, 更加难以清除了。而事实上, 它曾经使数千个电脑用户中毒, 可谓“人小鬼大”。该病毒至今只产生了11个病毒样本。

八月毒星

布若达 (Backdoor.Bardor.A)

闪光点: 最有“前途”的病毒

布若达是全球第一个可以让攻击者远程控制被感染手机或智能设备的病毒。它会感染采用ARM处理器、Windows CE操作系统的智能手机, 在被感染设备中开设后门。利用它, 攻击者不但可以偷窃中毒手机里的电话号码和电子邮件, 还可以对其进行远程控制, 运行多种危险指令。该病毒依然是一个概念型的病毒, 只能由攻击者通过电子邮件或其他手段诱

骗用户下载并运行。但根据国外媒体报道, 该病毒出现后, 已经开始有人利用电子邮件销售这个病毒的客户端, 卖病毒的人声称, 任何人都可以购买该病毒用来控制别人的手机。如果这种情况泛滥的话, 将是智能手机用户的又一场灾难。

九月毒星

快乐耳朵 (Trojan.Happyear)

闪光点: 最无耻的病毒

快乐耳朵并不会使人快乐, 因为它的出现, 九月成了网上银行的噩梦。它首先会通过邮件进行传播, 会发大量标题为“快来看看我的偷拍作品”的邮件, 声称自己是一个酒店的经理, 偷拍了大量的社会丑恶现象, 然后放在一个网站中。如果用户要看的话, 需要下载一个插件。随信件还有一个链接地址, 如果用户感兴趣点击了该地址的话, 就会链接到发信人所说的那个偷拍网站, 并且确定会提示用户下载播放插件, 但此时您下载的并不是什么插件, 而是病毒。不过, 这些都不算什么, 病毒真正的目的是盗窃用户网上银行的密码。它运行时时刻监视用户的动作, 如果用户这时登录某银行的网上银行系统时, 就会被偷走用户名和密码。

2005 展望：网络争夺战

漏洞病毒依然是毒魁

就目前的Windows操作系统来说,几千万行的代码、上百万软件工程师共同进行编码,想没有漏洞是不太可能的事情。我们也不得不承认,漏洞病毒依然是极其厉害的一类病毒。

就像每年操作系统都会出现重大的漏洞一样,2005年也会出现类似蠕虫王、冲击波、震荡波这样极具杀伤力的漏洞病毒。这类病毒不会很多,可能只有一两个,但是却能毫不费劲地造成社会问题。因此,及时关注病毒和漏洞信息应该成为每一个电脑用户的习惯,这样才有可能在漏洞病毒面前不再显得那么脆弱。

浏览器劫持会向纵深发展

浏览器劫持现象在2004年初步形成气候,将会在2005年进行发力。它是指一些恶意程序通过控制浏览器的形式来左右用户的电脑,使用户上网时出现各种问题,这其中就包括曾经名噪一时的脚本病毒和最近新出现的广告插件(ADWare)、色情插件(PornoWare)之类的恶意程序。

ADWare程序在非法侵入用户电脑后,会占用用户大量的网络带宽,使上网速度变慢,而PornoWare则会非法修改用户的长途拨号或网络银行设置,使用户莫名其妙地产生巨额支出。由于这类恶意程序隐藏得很深,用户一般很难发觉,比传统的病毒更具威胁性。

网络钓鱼将引发新的社会问题

最近两年一个新兴的网络问题是垃圾邮件的问题,而

2004年及以后,另一个新的热点将会是“网络钓鱼”。网络钓鱼是2004年才出现的新事物,与网银大盗之类的病毒偷盗行为不同,它采用的是“舍不得孩子套不着狼”的战术,利用真实的病毒网址来诈骗用户上当,从而盗取用户的网络银行或信用卡的密码,从而盗取大量现金。

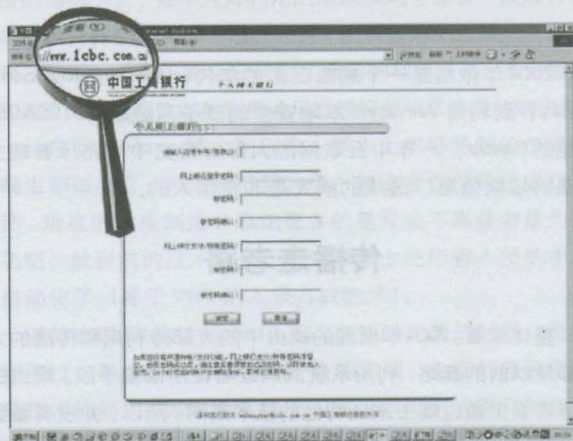


图2 “网络钓鱼”界面

随着网络的发展,这类问题将在2005年进一步扩大,成为新的社会问题。对于这类问题的解决已经不是单纯的用户如何防御的问题了,已经上升到了网络监管的层次。如果能够对网络进行规范化管理,会使我们上网的环境更纯洁些。

不管怎么说,热热闹闹的2004年即将过去,回首这一年,病毒依然是我们心中抹不掉的痛,遥望2005年,我们只能说,希望病毒再少些。INI

十月毒星

MSN 骗子 (Worm.MSN.funny)

闪光点: 最可气的病毒

该病毒可以通过QQ和MSN传播,病毒运行时会向线上好友发送“Funny.exe”的文件,用户点击后就会中毒。中毒后,病毒会屏蔽937个主流网站,使用户无法访问,更有甚者,还有可能会造成Windows 98系统崩溃,让那些爱上网的人因无法上网而气愤之极。该病毒的出现表明了即时通讯平台作为继邮件之后又一个主流通讯平台,也同样成了病毒的温床。

十一月毒星

股票窃密者 (TrojanSpy.Stock)

闪光点: 最富有的病毒

它是专门针对数家国内证券公司的网络交易系统编写的木马病毒,与偷盗网上银行密码的“快乐耳朵”相比,它可谓是大巫见小巫了。用户中毒之后,病毒会窃取用户的股票

网络交易账号和密码,从而可以恶意买卖用户的股票,造成用户的资金损失,因此,该病毒成了2004年名符其实最富有的病毒。而且,随着网络的发展,这种直接偷盗金钱的病毒将会越来越多。

十二月毒星

圣诞骗子 (Worm.Zafi.d)

闪光点: 最“博学”的病毒

就在圣诞节快要到来时,利用圣诞节进行传播的病毒也出现了。尽管这种手法并不新奇,但在节前的一段时间里,对于广大网民来说,仍然是很难防范的。“圣诞骗子”其实是2004年6月出现的网银大盗病毒的一个变种,会以发贺卡的名义欺骗用户上当。病毒侵入用户电脑后,会开设后门,使黑客们可以远程控制这些中毒电脑。而且,它还是一个“博学”的病毒,自带了15种欧洲语言,当向不同国家的用户发送携带病毒邮件时,会采用相应国家的语言,从而大大增强自己的欺骗性。INI

横扫毒界
之 2004

蠕虫遍布整个网络

■ 上海 马木留克

2004年依然是一个蠕虫泛滥的年代,从年初的MyDoom、NetSky,到利用Windows本地安全验证子系统服务(LSASS)问题的Sasser,一年中互联网的大部分带宽中都充斥着蠕虫发送的垃圾信息,造成的损失是非常惊人的。

传播走老路

整体来看,2004年出现的蠕虫中的大部分利用和传播的方式都是以前的套路:利用系统漏洞或者使用诱骗手段。蠕虫的编写者很少通过蠕虫来证明他的技术高明,所以,并没有看到像当年MSSQL蠕虫那样“简洁而优美”的代码,相反给人的感觉是某些情况下,病毒编写者似乎是早已编好了蠕虫的各个部分,只是等待着出现“好用”的漏洞作为传播的途径而已。

以Sasser(震荡波)为例,它的传播途径是微软安全公告04011中描述的Windows本地安全验证子系统服务的一个远程溢出漏洞。在该漏洞的远程利用程序公布后不久,这个蠕虫的第一个版本便开始在网上肆虐。与MSSQL蠕虫不一样,它不是一个“常驻内存”的蠕虫,而是一个文件性质的蠕虫。对漏洞的利用仅仅是得到一个Shell,然后在这个Shell上进行操作,从攻击端下载蠕虫程序的副本,在新感染的机器上执行,以便传播。Sasser蠕虫与2003年流行的Blaster(冲击波)传播的方式和行为非常类似,不同的是一个是通过tftp方式传播蠕虫副本,而另一个通过自带的ftp方式来传播。较之2003年,Sasser及其他利用相同漏洞进行传播的蠕虫破坏力没有Blaster强,原因除了用户的安全意识提高和部分对端口的限制以外,漏洞本身的局限性也是一个重要的因素。

具体分析过LSASS问题的朋友都知道,这个漏洞是一个典型的栈溢出问题,尽管有两次机会可以获得控制权,但编码的限制使得攻击者无法找到一个对所有版本都通用的返回地址(最好的情况也就是能够针对几个不同语言的所有Windows 2000/XP或者是针对不同语言下某几个特定的SP版本),使得利用该漏洞的蠕虫的传播成功率大打折扣,这也是很多受害者在其影响下,仅仅是看到了一个倒计时的关闭系统对话框,而没有成为蠕虫的另一个传播源的原因。

除了利用系统本身缺陷传播的蠕虫以外,常规的通过邮件或者其他途径传播的蠕虫也非常多,例如NetSky/Bagle的各种变形版本、MSN/QQ尾巴等。前者通过添加蠕虫副本至

邮件附件中,不断发送并诱使收件人打开并执行来传播;后者则是通过一些在线聊天工具的文件传送功能,通过传送蠕虫的副本和诱使对方执行来进行传播。这一类蠕虫利用的不是具体的某一个漏洞,而是利用人们的好奇心和信任来达到传播的目的。较之利用漏洞的蠕虫而言,这一类的蠕虫对平台或版本不那么敏感,影响的范围相应也要广很多,但是由于传播的环节中需要人为参与(比如点击执行),所以传播的速度不如利用漏洞进行主动攻击的蠕虫快。

弱口令和其他的漏洞也是蠕虫传播的一个途径,不过蠕虫通常不会单独针对弱口令或某个不太常见的漏洞进行攻击,而是结合了许多种传播途径进行传播,例如AgoBot(高波)。从感染的情况来看,这一类蠕虫的泛滥程度不逊于前面两大类蠕虫,像弱口令这样由于用户本身造成的问题,相比打几个补丁而言要难解决得多,因而也很难杜绝此类蠕虫的大量传播。

个人用户是攻击重点

2004年,蠕虫的主要攻击对象还是个人用户,因为人的因素始终是安全中非常薄弱的一环。利用社会工程学进行传播的蠕虫要获得控制权,必须有人为的参与在里面——至少需要收件人浏览一下邮件或者打开运行附件中的恶意文件。尽管遭受了Melissa、Sircam的袭击以后,人们还是会一如既往地轻信,也使得每年都有换汤不换药的蠕虫出现。现在流行的邮件、IRC、MSN、QQ等都有相关的针对个人用户的恶意蠕虫,蠕虫的制造者也是瞄准了个人用户这一大块,流行什么软件就针对什么制造蠕虫,只要在技术上没有困难,相信还会有很多新的蠕虫会源源不断地出现。

相对个人用户而言,专门针对服务器的蠕虫似乎还没有这么厉害,比起前些年CodeRed横行的时期,2004年服务器遭受的打击要小得多。这一类蠕虫的一个重要特点是要依赖于系统漏洞,比如之前的IDQ、Webdavx之类。2004年,虽然安全公告中依然有只针对服务器版本的漏洞报告,但是并没有与之相关的exp公布,而蠕虫制造者也没有能力自己编写这一部分,所以利用新漏洞专门针对服务器的蠕虫几乎没有。还有一点,在微软每公布一个重要的服务器漏洞之后,几乎都有对应的蠕虫,这客观上促使了网管们及时去打补丁修正bug。蠕虫制造者也很清楚这一点,也许是出于传播面积的考虑,很少有蠕虫会利用以前的漏洞,顶多是整合到传播模块中来,只是把它用作多种传播手段中的一项。

明天的蠕虫

密切关注漏洞

目前,蠕虫有一个非常明显的趋势,那就是每一个重大的安全漏洞都对应一个(种)危险的蠕虫,比较明显的例子就是Blaster和Sasser。在一个危险的漏洞出现后,从公布细节到大范围地打上补丁,中间往往间隔非常长的一段时间。这期间,可能有某些人出于特殊的理由公布了这个漏洞的利用方法甚至是代码,客观上促成了蠕虫的产生。因为蠕虫制造者等待的可能就是这样一个传播的手段,倘若该漏洞的影响范围很广,那么这个蠕虫可能传播的范围就越广,这正是蠕虫制造者所希望的。利用代码公布以后,只需要一些很简单的手段就可以制造出一个蠕虫来,从技术角度而言,Sasser乃至之前的Blaster,不过是把漏洞利用的手工方式变成自动方式而已,其行为就像一个攻击者在用很高的速度来入侵其他机器,并没有很高的编程技巧。蠕虫泛滥后,大部分的机器都打上了补丁,传播速度也就降下来了,所以虽然来势凶猛,去得也很快。

有些危险的安全漏洞并没有造成蠕虫的泛滥,很多情况下是由于技术的原因,譬如GDI+的问题(微软安全公告04028),这是一个堆溢出的问题,小范围内有蠕虫传播,但由于通用性的原因,并没有大面积的影响。可以想象的是,如果蠕虫制造者的水平有所提高,那么这一类的漏洞以后也会非常凶猛,因为就技术的角度而言,堆溢出的问题能够被做得比普通的栈溢出更为通用,对应蠕虫的传播范围也会很大。

与后门相结合

蠕虫的另外一个趋势是与后门相结合。很多蠕虫在传播中获得了系统的控制权后会留下一个后门供可能的攻击者进出,这也表明蠕虫制造者已经由以前仅仅为了出名或是技术原因而编写蠕虫,转变为带有其他特殊目的而编写蠕虫。

通过人这一个薄弱环节传播的蠕虫每年都有,以前是,今后肯定也会有。利用邮件等方式,攻击性不是那么强,甚至有些被动传播的意味,然而人却往往受不了看似来自熟悉地址的信件或是类似porn、free等字眼而打开附件,如果不能在短时间内提高个人用户的素质和警觉性,以后很多年内还会有一部分蠕虫通过邮件等类似社会工程的方式传播。而这种邮件除非是获得了确定的样本,否则在大范围泛滥之前,目前技术下的杀毒或是反蠕虫软件是没有办法完全预防的。

未来切入点

抛开道德等其他方面,单纯从技术角度来分析这一系列泛滥得极其厉害的蠕虫的话,可以看到它们在技术上没有什么突破,也没有什么创新点可言。比起2003年“补漏洞”的蠕虫或者更早的宏病毒,2004年的蠕虫无论在创意、技术甚至程序员的功底上都有很大的差距。蠕虫似乎发展到了和互联网当初“快鱼吃慢鱼”类似的地步——不在于写的东西有

多么的“好”,只要能够在极短的时间内完成,就会造成更大范围的影响,这一点在Sasser的出现上表现得非常明显。

值得一提的是,对于GDI+的漏洞,尽管相对应的蠕虫传播面积比较窄,但也是蠕虫编写者对通过堆溢出方式来获得控制权,进而进一步传播的一种尝试。在栈溢出漏洞报告步伐逐渐减慢的情况下,一些不太好利用的系统漏洞可能会一跃成为蠕虫制造者青睐的新传播手段。而且,随着技术的发展,看似不好利用的漏洞很有可能会出现更加通用的利用方法,在传播范围和速度上不见得比以前利用通用性较好漏洞来传播的蠕虫差。

从早期的Morris蠕虫到现在,基本上能够想到的传播方式蠕虫都做到了。如果说早期的蠕虫制造者仅仅是炫耀技术的话,现在的蠕虫制造者恐怕更多的是发泄不满或者是为了出名吧。就当前的技术看来,蠕虫基本上把所有入侵的手段都自动化了(基于Web的入侵方式除外)。

以前出现IIS的Unicode以及二次解码问题的时候,有蠕虫利用过,不过后来也没有进一步的发展,主要的原因想必还是技术的制约,因为通常情况下通过Web方式得到的控制权限比较低,而且获得权限的方式比较复杂,单纯通过自动化的手段还不太容易实现。

2004年以来,看起来极有可能做成蠕虫的是dvBBS等一系列.asp程序上传的问题,可能因为影响范围和程序设计的难度,并没有相应的蠕虫出现。将来,也可能出现利用广义上的注入漏洞来传播的蠕虫,存在这一类问题的程序很多也很广,完全可以成为蠕虫制造者的下一个目标。

我们可以简单分析一下,寻找目标主机可以通过搜索引擎(比如google),这一点不存在困难;如果获得执行的权限,传播文件也有很多方式(比如ftp或者是vbs等脚本来下载文件或者其他),这一点上也不存在困难;惟一的难点就在获得控制权限,而获得控制权限中比较麻烦的是注入点的选择与确定,蠕虫制造者也需要结合启发式的搜索或者干脆穷举来攻击并传播。一旦这方面的技术难题得以解决,也许我们就能看到一种全新的蠕虫出现,这也是短时间内我们极有可能看到的“新突破”。其他的CGI问题,由于范围或通用性的原因,不太可能被蠕虫制造者利用,脚本的解析器出现重大安全漏洞除外。

结合系统漏洞的蠕虫,在可以预见的未来估计也会发生比较大的变化。除了前面说的堆溢出等不太容易利用的漏洞可能会被用作传播手段以外,也许还会出现一些通过内核溢出来传播的蠕虫,这在技术层面上已经没有任何问题,关键就要看是否有相应的漏洞以及利用程序被公布。

除了传播的手段以外,蠕虫的隐蔽性也许会成为蠕虫制造者下一个关注的部分,各种rootkit技术可能会被用在蠕虫自身的隐藏上面,不久的将来我们或许会迎来查杀更加困难的蠕虫。

当然,如果所有用户都有很好的安全意识,蠕虫编写者肯定不愿意花费太多精力去写一个没用的程序,蠕虫也无法如此肆虐。只是,距离蠕虫消失的那一天,恐怕还有相当长的一段路要走。 ■

横扫毒界
之 2004

木马劫掠真实财产

■ 北京 八杯水

2004年出现的木马从技术上以及目的性来看,都比前几年有很大变化。为了大家能对特洛伊木马有一个整体的认识,我们先从2004年以前的木马谈起。

2004年以前:远程监控为主体

在2004年以前,提起特洛伊木马,人们首先会想到的是“冰河”、“BO”、“YAI”以及“Sub7”等,它们均属于远程监控类软件。要想发挥作用,木马的服务器端程序和客户端程序必须同时存在,而且,木马本身不具备繁殖性和自动感染的功能,所以大多情况下都需要诱骗受害机器的使用者自己运行木马程序,木马开始在伪装上下文章。

这一时期出现的木马程序在传播上大多可以分为三类:

- ◆通过电子邮件直接发送。邮件主题具有一定的诱惑性,诱惑用户自己点击执行附件中的木马程序服务器端。

- ◆通过下载网站捆绑在正常的程序中。这段时期,网上出现了大量的exe捆绑工具(EXEBinder),这种工具可以把一个木马程序和一个正常的软件捆绑在一起。

- ◆利用操作系统漏洞直接下载运行。

除了这三大类之外,2004年以前还出现了可以感染exe文件的木马程序,比如YAI(You and I)和冰河的一个变种。这类木马由于在技术上存在一定限制,数量很少,但却改变了木马不具备传染特性的概念。

这一时期也出现了具有特定功能的木马,比如一些QQ盗号木马。它们的功能不是远程监控,而是隐藏在受害的计算机中伺机记录QQ密码,并将它发送到释放木马者指定的信箱。

总的来说,2004年以前的木马主要目的还是远程监控,已经具备了一些狡猾的伪装手段和基本的隐藏技巧。

2004年:功能细化,具备反安全软件特性

功能进一步细化

2004年的木马在功能上发生了很大的变化,真正的远程监控木马只占很小的比例,木马的功能开始细化。2004年流行的木马按功能可以分为五大类:网游木马、广告木马、即时通信木马、网络银行木马及后门程序。

随着近几年网络游戏业的迅速发展,网上虚拟装备、财产成为黑客们猎取的对象,网络游戏盗号木马大量涌现。这

类木马一旦感染用户的计算机,就会自动记录用户网络游戏的账号和密码并发送给木马使用者,木马使用者通过出卖盗取的虚拟装备、人物账号谋取利益。由于偷盗网络游戏账号具有很大的诱惑性,您甚至可以在网上买到定制的网游木马。

2004年9月初,国内发现了一例专门窃取网络银行账号的木马“网银大盗”,也称“快乐耳朵”。它是专门针对某银行网上业务个人版编写的,可以取得该行网络银行专业版的数字证书、密码和账号,能够在网上实现完整的盗窃资金过程,对用户的危害极大。11月26日,众多反病毒公司又截获了针对数家国内证券公司的网络交易系统编写的可以窃取用户的股票网络交易账号和密码的“股票窃密者”木马(又名“股票盗贼”、“证券大盗”)。

网游木马和网络银行木马的出现揭示了木马的发展趋势:现阶段的木马越来越向着直接获取经济利益的方向发展。病毒作者编写即时通信木马和广告木马同样也是受到利益的趋势。即时通信木马以“QQ狩猎者”(也叫“QQ尾巴”)木马为代表。感染这类木马后,QQ会自动发送诸如“http://xmc.*****.net快去看看,您感兴趣的消息”之类的消息。当其他用户登录消息中的网站,他的计算机就有可能感染这个病毒,也会自动发送这类消息。通常,这些网站上还包含有广告木马,感染这类木马的计算机的IE首页会被锁定为含有病毒的网站而无法修改,并且还会定期弹出广告窗口。即时通信木马和广告木马的目的就是为了提高网站的访问量,但频繁发送消息和弹出广告已经严重干扰了用户正常的上网和办公。

技术复杂性大幅提升

2004年木马在功能上发生变化的同时,其技术也变得越来越复杂化,开始具有更高的隐蔽性和对抗安全软件的能力。

(一) 传播渠道的变化

从传播方式看,2004年的木马主要通过两大渠道传播。

一是即使通信软件与含有恶意代码的网站相配合,那些频频更新、变种数以百计的“QQ尾巴”木马,2004年10月份大肆传播的Worm.MSN.Funny(又称“MSN骗子”)病毒都是利用即时通信软件自动发送广告消息传播的典型木马,2004年发现的几个偷盗“传奇”网络游戏账号的“武汉男生”木马变种也是利用这种方式传播的。

二是通过蠕虫病毒释放,这是国外一些病毒作者的惯用手法,许多国外的病毒在成功感染计算机后都会在受害的计算机上留有后门程序。这种方法目前也已经逐渐被国内的病毒作者所采用。

(二) 隐藏手段的变化

从隐藏手段看, 2004年的木马采用的随系统自启动项的名称更具欺骗性, 启动方式也更加复杂。

目前的木马大多采用和系统文件相近的文件名进行伪装, 比如采用rundll.exe (用数字1伪装成字母l)、svchost.exe (用数字0伪装成字母o) 作为生成文件的名字。更有一些木马干脆采用和系统文件相同的名字, 但所在位置与正常文件不同, 这样用户就很难注意到它的存在了, 甚至连专业的反病毒专家也弄不清微软自己的一些文件究竟应该放在Windows的目录还是Windows下面的系统目录中。

由于木马采用了和正常文件近似或相同的文件名, 用户经常会对这类文件麻痹大意, 就让木马有了可乘之机。

(三) 启动方式的变化

在启动方式方面, 2004年的木马采用了更多的先进技术。许多自动修改IE首页、反复在搜索页和收藏夹中添加恶意网站地址以及浏览正常网站时自动弹出恶意网站广告的木马都以IE的插件形式随IE的启动自动运行。这种方式被称为IE浏览器捆绑或浏览器劫持。

(四) 文件格式的变化

在文件格式方面, 许多木马制作成DLL或OCX文件, 使用Rundll32.exe运行。这样做的好处有二, 其一是可以使木马的启动方式变得隐蔽, 不易被发现; 其二是目前杀毒软件对DLL文件的内存查杀能力不强, 正常模式下往往难于清除这类木马, 使之可以更好地执行。

(五) 反安全软件特性

2004年的木马普遍带有反安全软件的特性, 多数木马都会查找内存中杀毒软件和个人防火墙软件的进程, 并结束这些进程, 使之失效。

实际上, 结束安全软件进程并不是一个新的技术, 但这两年该技术被普遍采用, 2004年出现的许多木马都具备这个功能。同时, 木马还利用其他手段躲避安全软件的查杀, 比如用DLL格式文件运行来躲避内存杀毒、自动检测、卸载或删除反病毒软件等。

总的来说, 2004年的木马不再像早些时候那样, 为了追求功能全面而臃肿复杂, 开始针对用户真实财产, 功能单一但非常有效。

未来: 务实为主

从2004年的木马发展就可以看出, 目前的木马越来越“务实”, 以直接获取真实财产的偷盗类木马大大增多。

通过对过去几年的木马发展趋势可以判断出未来木马的发展趋势。

具备病毒特征的木马大量涌现

现在的木马可以说是“为达目的不择手段”, 传统的“木

马是装作用有用程序的一类恶意程序, 不主动进行感染和传播”的定义已经变得片面, 类似MSN骗子病毒就同时具备木马和病毒的双重特性。

为了能够迅速地将木马种植在尽可能多的计算机上, 未来的木马将大量采用计算机病毒技术, 也就是说木马本身就是蠕虫病毒, 反过来讲蠕虫病毒也具有木马的功能特征, 木马和病毒之间将没有明显的区分界限。

利用操作系统漏洞的木马逐渐增多

不光只有病毒会利用操作系统的漏洞, 越来越多的木马也开始利用这些漏洞进行传播, 尤其是一些IE浏览器的漏洞, 允许木马在未经用户许可的情况下自动下载并运行。

早些时候的iframe漏洞, 2004年弄得人心惶惶的JPEG溢出漏洞以及年底出现的网页元素处理溢出漏洞都属于这种情况。同时, 由于宽带在中国的普及, 利用远程攻击漏洞进行传播的木马也会出现。

对抗反病毒软件和个人防火墙软件的技术升级

在对抗杀毒软件方面, 未来的木马不会简单地只结束杀毒软件的进程或者卸载杀毒软件, 因为这种做法实际上已经暴露了自身, 有经验的用户马上会察觉到系统的异常。

新的木马可能会针对杀毒软件的弱点进行编写, 比如删除杀毒软件的病毒特征库, 使有些杀毒软件加载病毒库不成功并不会进行告警。这样, 杀毒软件看似正常运行, 实际已经无法对木马、病毒进行查杀, 变成木马的“帮凶”。

同时, 为了躲避杀毒软件的追杀, 未来还可能会出现能够变形的木马。举个简单的例子 (只是一个概念, 可行性有待研究): 木马可能内置源代码和编译器, 每次随机地对源代码进行自动改写并释放, 然后用内置的编译器重新编译。对杀毒软件来说, 每次重新编译的木马都是一个新的变种, 对它们的查杀将会变得十分困难。

在对抗个人防火墙软件方面, 目前已经有一些概念性的软件出现, FireHole就是其中一个 (<http://keir.net/firehole.html>)。它的原理是创建一个DLL文件, 并将这个文件放置在一个被防火墙信任的程序中, 比如IE浏览器, 那么这个DLL文件对网络的访问便不会被防火墙拦截。即使有一些谨慎的用户设置了他们的防火墙, 使浏览器只能在指定的TCP80端口连接, 但这个惟一开放的端口也足以保证该DLL文件进行通信。

木马功能智能化

传统的木马通常只通过捕获用户键盘操作来窃取用户的密码, 目前不少软件 (如腾讯QQ) 采用通过软键盘输入账号、密码的方式来防止这类偷盗情况的发生。未来的木马会自动检测用户是否开启软键盘, 通过Hook技术捕获用户的鼠标操作, 并根据鼠标点击顺序截图并发送到黑客的邮箱中。■

横扫毒界
之 2004

脚本病毒甘做幕后帮凶

■ 北京 晓兵

脚本病毒想必大家都不会陌生,“美丽莎”、“快乐时光”、“万花谷”都是恶性脚本病毒的代表。脚本病毒的出现使得病毒编写的门槛大大降低了,稍具电脑知识的用户经过简单的学习就可以轻松编写出这种病毒来,其破坏性却丝毫不比传统病毒差。

随着技术的发展,脚本病毒也像其他病毒一样不断地产生着新种类。

曾经的辉煌

虽然脚本病毒出现的时候并不算短,但是人们真正听到“脚本病毒”这个称呼还是最近几年的事,因为最早的脚本病毒只有一种情况,就是利用微软 Office 系统提供的宏功能进行编制的病毒,也称宏病毒。后来,随着 JS、VBS 这样真正的脚本编程语言的出现,脚本病毒这个名称才被正式提出来。虽然宏病毒随着 Office 2000 的宏安全机制的出现而走向没落,但是它在脚本病毒的历史上却统治了相当长的一段时间。

在脚本病毒的发展中期,欢乐时光病毒可谓是一座里程碑,它开创了感染式网页病毒的先河,并在一夜之间传遍整个世界,该病毒是脚本病毒发展的重要产物。在它之前虽然也有一些网页脚本病毒出现,但是都未成气候,让大多数人认为脚本语言的编程能力有限,对网页病毒的破坏性都还持怀疑态度,也就在这时候,欢乐时光病毒出现了。它采用 VBS 脚本语言进行编写,隐藏在网页中,当用户中了该病毒之后,病毒便会将用户系统中所有的网页文件都感染上病毒代码,该病毒不但可以在传染的过程改变大小,而且还能将自己作为信件的模板文件发送出去,还会删除系统中的所有可执行程序,使整个系统崩溃。可以说,欢乐时光病毒将脚本网页病毒推入了一个新时代,从此,编写这类脚本病毒的人越来越多。

此后,经过短短一年的发展,脚本病毒又出现了两种新的形式,一种是利用系统文件夹可配置属性的 RedLof 病毒,另一种就是通过修改注册表来破坏用户系统的万花谷、网页炸弹、极限女孩等病毒。由于这类病毒的泛滥,各大反病毒公司都推出了自己的注册表修复工具,也正是随着这些工具的产生,使得曾经辉煌一时的脚本病毒逐渐走向没落。

退居幕后

现在,脚本病毒又出现了一种新的形态,就是成为木马

病毒的帮凶。

编写病毒离不开编程语言,而编程语言的一个基本原则是,编程语言越高级,编程就越简便,但是能实现的底层功能也就越有限,因为语言被层层封装,已经失去了灵活性。脚本语言是封装级别极高的语言,它本身的破坏是比较有限的,因此从 2003 年开始,脚本病毒开始退居幕后,甘心做起了木马病毒的帮凶,像 2004 年的“快乐耳朵”病毒就是一例。

这类病毒首先会给用户发送一些带有诱惑性标题的邮件,当您感兴趣并链接那个网址时,就已经落入了病毒的圈套。该网址的首页就是一个脚本病毒,他们一般会利用系统的网页漏洞偷偷地给用户系统安装一个木马,或者告诉用户缺少一个插件,希望用户点击下载,其实这个插件就是一个木马病毒。当木马病毒溜到用户系统后就开始完成开后门、偷密码等“地下”工作,给用户带来很大的安全隐患。

从这里我们看到,在这个讲究合作的年代,脚本病毒也开始与传统的木马进行合作,这种合作很可能是病毒作者同时使用两种编程语言编写,然后再进行组合,也可能是两个病毒小组之间协作完成的。

假到真时真亦假

网络是一部永远向前发展的永动机,而随着网络环境的变化,脚本病毒也一定会发生某些改变,它的明天是怎样的呢?

首先,一个逻辑上的发展趋势就是脚本病毒会越来越趋向于被动传播这样一种方式,就像上面分析的那样,脚本病毒的编写方便和功能上的先天不足,导致它在未来这个防毒体系已经比较完善的世界中只能扮演一个帮凶的角色,将会出现更多利用脚本病毒传播木马程序这种模式的病毒。

其次,将会出现越来越多的网络诈骗性质的脚本病毒。这类病毒会给用户发送一些含有伪造内容的邮件,比如说用户的网上银行账户和密码已经过期之类的信息,当用户信以为真点击给出的链接时,则会出现与真的网上银行一样的虚假网页,该网页会提示用户输入自己的用户账号和密码,其实用户的资料这时已经被发送到了另一个邮箱,病毒作者只要定时收集这些信息,便能轻松窃取到用户的网上银行的资金。在未来,这种以诈骗为目的脚本病毒将会越来越多。

当然,当一些新的应用产生后,必然会有新的病毒随之而来。正所谓“魔高一尺,道高一丈”,无论未来病毒如何发展,总会有解决它的方法。



2004 年毒界“风云”榜

据统计, 美国企业2003年因计算机病毒导致的损失约一百三十亿美元。加州的市场研究公司预估, 2004年的损失金额将更高, 可能接近一百七十五亿美元。如果从全球来看, 2004年病毒所带来的损失该是多么庞大的一组数据啊! 谁有如此能力, 谁在2004年里的毒海里掀起巨浪? 请看2004年的毒界“风云”榜。

2004年毒界“风云”榜

奖项	获奖者	得奖理由	得奖感言
最“佳”男主角	NetSky 网络天空病毒	历久不衰	子孙(变种)满堂, 分身有术。
最“佳”女主角	Social Engineering 社交工程	魅力无法挡	垂涎欲滴, 鼠标忍不住想咬一口。
最“佳”新人	18岁的德国青年 Sven Jaschan	全球瞩目	震荡波病毒作者, 最好的18岁生日礼物。
最“佳”动作设计	Bot 遥控程序	从不说“不”	黑客坐以待“币”, 傀儡计算机坐以待毙。
最“佳”视觉设计	Phishing 网络钓鱼	维妙维肖	钓大户, 创“钱”程。
最“佳”置入式行销	Spyware 间谍软件	神出鬼没	找我卧底就对了。
最“佳”剧情片	MyDoom、Bagle 和 NetSky 之间的口水战	自编自导	隔空照样打得火热。
最“佳”替身演员	手机垃圾短信	一字千金	离间亲友, 反目成仇, 够霹雳。
最“佳”美术设计	JPEG 图片	金玉其表	将这个荣耀与漏洞计算机分享。

最“佳”男主角: NetSky 网络天空病毒

得奖理由: 历久不衰

NetSky 不同于它的死对头 Bagle 那样不断衍生出变种病毒, 在传说中的作者德国18岁少年被捕入狱后, 自4月28日 Worm_NetSky_AB 之后, 就没有产生新的变种。但这并没有削弱该病毒的影响力, 几乎每个月的十大病毒排行榜中, NetSky 都名列前茅。

主要劣迹:

自2004年2月现身以来, NetSky 变种家族每个月都进入趋势科技实时病毒监控中心的十大病毒排行榜, 其中有八个月夺得毒王“宝座”, 是2004年度长跑冠军。

得奖感言:

子孙(变种)满堂, 分身有术。

最“佳”女主角: 社交工程

得奖理由: 魅力无法挡

黑客作案得逞的关键往往脱离不了“性、贪婪与恐惧”的主题, 所以, 社交工程 (Social Engineering) 这种操控计算机使用者间接破坏计算机的手法在病毒攻击行动中开始担任重要角色。而且, 只要有一个人抗拒不了本身的好奇心而打开了带毒邮件, 病毒就可能在所在的网络上大行肆虐。

主要劣迹:

◆著名的市调分析机构Gartner在11月公开研究报告中表

示: 未来10年内可能躲过IT监控、攻破计算机网络的最大的风险就是“社交工程 (Social Engineering)”。

◆1到3月, MyDoom 行骗天下。2004年第一季度感染冠军 MyDoom 采用仿冒退件通知, 信件无法正常被开启、自动开启应用程序以及假装是txt纯文字文件的ICON等手法, 创下高感染率。

◆9月, MSN 一日之内满地开花。MSN “花木马”病毒仅是恶作剧: “请放一朵玫瑰在MSN名字之前, 为死于俄罗斯恐怖行动中的孩童哀悼”的信息, 9月9日就像连锁信一般地通过MSN实时通讯满地绽放。翌日却有人指称其中含有病毒, 大家又通过MSN要互相通知把“花”连根拔除。还好事后证实是虚惊一场, 但若真有其事, 这就是成功地运用社交工程的一大典型呢!

◆11月, 阿拉法特死亡之谜。阿拉法特于2004年11月11日在法国巴黎附近的贝尔西军医院逝世, 他的真正死因引起多方揣测。很快, 出现了一个以“Latest News about Arafat! (阿拉法特的最新消息!)”为信件主题的病毒“Worm_Golten.A”。该病毒在内文里叙述“Hello guys! Latest news about Arafat! Unimaginable!”, 并分别附上两个 .emf 图片延伸格式附件, 其中 Apafat_1 .emf 文件名附件内果真含有阿拉法特葬礼图片, 这是病毒利用障眼法, 让受害者没有防备心地开启第二个附件, 一旦使用者开启 Apafat_2 .emf 附件, 病毒就会利用 Windows XP 的 Metafile 漏洞钻入系统。

得奖感言:

垂涎欲滴, 让鼠标忍不住想咬一口。

最“佳”新人: 18岁德国青年 Sven Jaschan

得奖理由: 全球瞩目

据德国 Stern 杂志的访问内容, 18 岁的 Sven J. 是从 2004 年 1 月才开始写计算机病毒。Sven 坦承, 撰写了 29 种网络天空 NetSky 病毒的版本和三个震荡波 Sasser 版本。

主要劣迹:

5 月, 让全球动弹不得。澳大利亚铁路, 上万旅客滞留站台; 德国银行被迫改用手写完成各种业务; 英国海岸警备局的计算机无法运转, 工作人员不得不用纸条来记录事故; 芬兰某银行关闭 120 家分行达数个小时; 德尔塔航空公司约 40 个航班无法准时起飞。

得奖感言:

最好的 18 岁生日礼物。(注: Sven Jaschan 在 18 岁生日当天把该程序放网络上)

最“佳”动作设计: Bot 遥控程序

得奖理由: 从不说“不”

Bot 是黑客暗中出租计算机攻击他人并牟利的新武器, 一个口令, 傀儡计算机齐动员, 动作整齐。

主要劣迹:

◆ 7 月, Bot 成为新兴诈骗行业。来自英国的报导指出, 有一个由青少年组成的新兴行业正盛行: “出租可由远程恶意程序任意摆布的计算机”, 这些受控制的计算机称之为“傀儡 (Zombie)”计算机。数目自小 10 台大到 3 万台。

◆ 9 月, 挪威被迫关闭 IRC。挪威 ISP “Telenor” 因为察觉 IRC (Internet Relay Chat) 已成为 1 万多台个人计算机组成的攻击网络的指令中心, 因此关闭了 IRC 服务器。

◆ 10 月, 四万美金花钱消灾。网络安全机构 SANS 表示, 傀儡计算机已被黑客当作用来勒索的工具, 尤其是线上赌博网站, 若要避免服务器因 DoS 而瘫痪, 代价是付给黑客 4 万美金。

◆ 11 月, 生意谈不成, 瘫痪对方网站。美国司法单位起诉一位公司负责人, 该涉嫌人因为生意没做成, 涉嫌雇用网络黑客利用 Bot 程序瘫痪另一家公司的网站。受害者至少损失了二十万美元。

得奖感言:

傀儡计算机坐以待毙, 黑客坐以待“币”。

最“佳”视觉设计: Phishing 网络钓鱼

得奖理由: 惟妙惟肖

仿冒金融机构官方页面相似度近 100%, 靠得再近, 也看不出哪里不对劲。诈取受骗者银行账号、私人密码, 得逞率极高。

主要劣迹:

◆ IDC 在 2004 年 10 月发布的《2004 年亚太地区的安全威胁》(不含日本) 的报告指出, 网络欺诈行为“网络钓鱼” (Phishing), 已经对亚太地区从事电子商务的企业造成严重的安全威胁, 成为成长速度极快的非暴力犯罪行为之一, 知名金融机构是其锁定目标。

◆ 美国 Parenty Consulting 主席 Thomas Parenty 在 2004 年 5 月香港举办的“信息安全博览会”表示: 逮捕“Phisher”的成功率只有七百分之一。

◆ 9 月, 假橘子真诈骗。一个中国网站以“gamannia”的名字作为网域名称, 并放上游戏橘子的 Logo 企图瞒天过海。该假网站谎称配合政府打击诈骗, 要求玩家输入资料进行核对, 借机盗取游戏序号。事实上, 游戏橘子的网域名是“gamania”, 冒牌网站则在字母中间多了 1 个“n”。

◆ 10 月, 网络钓鱼进入第二代, 不再完全依赖电子邮件。早期的网络钓鱼信件以英文为主, 而且文法错误百出, 使用者只要不点选信中的链接, 就不会上钩。不过, 目前网络钓鱼的辨识度愈来愈低了, 甚至不用电子邮件当钓饵, 可以说是第二代的网络钓鱼。比如, Troj_Bancos.cop 这个特洛伊木马会监控 Internet Explorer 的浏览行为, 以获得记录受害者的 IE 上网行为, 一旦窗口标题符合设定的银行字符串, 就会制造几可乱真的登录网页, 要求输入个人密码等敏感资料。这些资料汇整于特定文件夹后, 将利用电子邮件自动发送给黑客。而且, 每一笔资料被寄出后, 会自动删除, 来去不留痕迹。

◆ 11 月, 到天堂钓鱼。一封冒称“天堂 II 营运团队”的诈骗信件以“关于您的账号涉嫌盗号”为电子邮件标题, 声称收件者的游戏序号已被盗用, 为了保护被盗玩家的利益, 要求输入相关账号信息, 否则三日内将永久停用该账号。

◆ 11 月, 利用 Google 等着大鱼上钩。当网络购物者利用 Google 搜索他们要购买的商品时, 会被引导到某网站, 并指示用户点击产品图片。一旦点击后, 并不会看到广告上的产品, 而是指向了一个自动解压缩的 .zip 文件, 并自动安装特洛伊木马, 以窃取个人金融资料。

得奖感言:

钓大户, 创“钱”程。

最“佳”置入式行销: Spyware 间谍软件

得奖理由: 神出鬼没

宛若网络侦探社, Spyware 间谍软件起初是利用用户安装软件时潜入用户的系统, 并利用多半用户未仔细阅读同意书的习惯, 规避责任。后来进展到与垃圾邮件共同犯案, 比如鼠标点选垃圾邮件的“remove it”时, 间谍软件即进驻计算机。

主要劣迹:

◆ 根据 National Cyber Security Alliance 调查报告指出, 91% 的 PC 遭受间谍软件入侵, 但 1/3 受访者认为遭受网络攻

击的机会,比中乐透彩或被雷打到机率低。美国国家网络安全联盟和美国在线公司10月25日联合发布另一项雷同调查报告亦指出,在某个用户运行缓慢的计算机上,居然有1000多个“间谍软件”。难怪有厂商推出情人间谍软件,监看情人与网友的交谈。

◆ 6月,WebMoney锁定50家银行。WebMoney专门窃取个人网络银行的相关信息,在使用者访问近50家银行网站时,测录键盘窃取密码,并把得手的信息回传到某个黑客网站。

◆ 7月,Tenget.A带您去Shopping。Tenget.A这个间谍软件化身网址工具列(browser helper),或者是随着E-mail的网址链接而来,一旦执行就会修改IE设定,当受害者在浏览器上端网址列输入auto.search.msn.com、search.netscape.com、ieautosearch等字符串时,就会被导向某个商业网站。除此之外,该间谍软件还可以任意开启文件、读写文件、开启URL、任意下载和执行文件,而且上述动作都不会出现警告窗口。

◆ 7月,您穿几号鞋子,Spyw_Gator.C都知道。这个间谍软件被另一只广告软件附身,所以无论受害者身处哪个网站,一个不请自来的跳出式广告总是会不断骚扰。除此之外,它还会将受害者喜欢上的网站回报给Gator公司,并转售给其广告厂商。这是延续至2003年备受争议的Cator弹出式广告问题。当时它自家外挂软件与受欢迎的Kazaa点对点文件传输软件、iMash搜寻程序搭配供人下载。之后,使用者上网时,Cator代理的客户广告便会出现“盖台”小动作。

◆ 10月,用间谍软件行销反间谍软件。美国联邦贸易委员会宣布,援引既有的公平交易法,要求联邦法院关闭部分散播间谍软件的主要网站。其中一个网站暗藏间谍软件,一旦感染会出现CD-ROM莫名其妙地打开、计算机速度降低甚至宕机等现象。之后,则以大量的弹出式广告呼吁用户采用自家反间谍软件收拾这些残局。

获奖感言:

找我卧底就对了。

最“佳”剧情片: MyDoom、Bagle和NetSky隔空叫阵

获奖理由:自编自导

2004年春天,MyDoom、Bagle和NetSky互相通过内含的病毒码字符串,彼此唇枪舌战。

主要劣迹:

以下为几个主要字符串:

Bagle.J:别坏了我的好事!!

Hey,NetSky,f*** off you b****,don't ruine our bussiness,wanna start a war?

他**的,别想坏了我们的好事,怎样,想开战吗?

NetSky.H:你们这些小鬼!

“Skynet AntiVirus—MyDoom and Bagle are children”

MyDoom和Bagle都是小鬼。

MyDoom.U:给我工作,否则攻击您。

“We searching 4 work in AV industry.”我们想在防毒软件公司找4份工作。

不知是否没得到善意响应,10月Worm_MyDoom.AA竟开始利用新变种,让感染者无法访问多家防毒厂商的网页,还放话要攻击知名防毒厂商。

获奖感言:

隔空照样打得火热。

最“佳”替身演员:手机垃圾短信

获奖理由:一字千金

被当作替身发送邀请函,倒霉的是亲友团收到垃圾短信,还要付费,真是欲哭无泪。

主要劣迹:

◆ 11月,冒名推荐,垃圾简讯满天飞。提供网络发送短信服务的SMS.AC网站,因未经使用者同意冒名发送邀请函给会员邮件地址簿的所有名册而争议不断。由于以每天免费发送5条短信到全世界67个国家或地区的手机为号召,吸引了不少网友加入会员。有些SMS接收短信是要付费的,受害者不但要接受SMS垃圾短信的轰炸,还要被迫把账算到自己头上。

◆ 11月,木马下毒,简讯接不完。Delf-HA木马目前锁定提供短信发送服务SMS的俄国电信网站。感染该木马的计算机会自动至特定网站下载某个名为SMS.txt的垃圾短信,然后利用上述俄国网站的SMS网上短信服务,随机发送给手机用户。

获奖感言:

离间亲友,反目成仇,够霹雳。

最“佳”美术设计:JPEG图片

获奖理由:金玉其表,败絮其中

以色情为主题的电子邮件一直是病毒得逞的主因,现在病毒制造者们开始直接在图片上动手脚,更要当心啊。

主要劣迹:

◆ 10月,利用微软9月公布的JPEG处理(GDI+)缓冲溢出(MS04-028)漏洞的首批病毒图片在色情网络出现,一旦查看该图片,就会被植入后门程序。

◆ 10月,利用上述漏洞的病毒荼毒实时通讯用户,受害者在AOL实时通讯中收到了一个链接,该网址连结到含有恶意图片的网站。

获奖感言:

将这个荣耀,与漏洞计算机分享。

(特别感谢趋势科技提供相关资料)

横扫毒界
之 2004

与毒过招

■ 深圳 黄盘兰

如今,病毒已经由传统介质的慢速传播演变成以局域网共享、网络下载、浏览、即时通信工具等方式的飞速传播,而病毒本身也逐渐演变成了以黑客木马病毒、间谍软件、网络陷阱、邮件病毒、网页恶意脚本和利用漏洞的蠕虫为主。

面对各种已知和未知的病毒,我们该掌握哪些基本技巧?

下面,笔者以2004年7月份与Lovegate变种病毒过招的经过为例,介绍一下基本的应对方法。

首战告负

2004年7月5日早上,当笔者正一边浏览病毒软件公司的网页一边看着服务器日志时,公司一个同事打来求助电话:我的电脑中毒了,电脑很慢且都还没打开IE上网,IE窗口就不断跳出来,无法手动关闭这些不断跳出来的IE窗口……

笔者来到同事那里,果然看到他所描述的现象,于是熟练地通过任务管理器中止了IE进程,边检查电脑边询问同事是否有上黄色网站之类。得到确认“没有”后,笔者开始认真检查电脑,果然看到注册表启动项里面有好多RAVMOND.exe、SysTra.EXE、NetMeeting.exe、Netmanager.exe、IEEXPLORE.EXE、Hxdef.exe等之类的程序,且都是对应于C:\winnt\system32目录下,于是用纸记录了文件名及对应路径,然后使用下面的步骤一一清除:

(1) 使用procexp.exe将这些相关的进程结束掉(procexp.exe是在WindowsNT/2000/XP下查看进程的软件,能够结束几乎所有的进程,包括任务管理器不能结束的进程)。

(2) 在C:\winnt\system32目录下找到相对应的程序,全部删除并顺便清除注册表启动项。

(3) 使用srvinstw.exe将注册成服务的“_reg”服务卸载(srvinstw.exe是在Resource Kit里面的一个能注册程序为服务并卸载服务的小程序)。

(4) 查看Win.ini和System.ini里面有没有病毒项(这两个文件在C:\winnt目录下,使用sysedit即可编辑该文件)。

(5) 查看文件关联有没有正常(一般笔者会看exe和txt的文件关联,只要看它们command对应的默认数值有没有被

更改;exe文件关联在HKEY_CLASSES_ROOT\exefile\shell\open\command,txt文件关联在:HKEY_CLASSES_ROOT\txtfile\shell\open\command)。

(6) 使用Fport(命令行下查看程序所开的端口工具)查看程序所开的端口情况及端口对应程序所在的路径。

(7) 最后再利用杀病毒软件扫描一遍系统盘(笔者使用的是Office Scan,不过没扫描出什么病毒)。

按上面的步骤做完后,笔者心想:这次病毒应该被清理干净了吧(因为平时几乎所有的病毒都是这样除掉的)。于是重启电脑后进行确认,谁知电脑重启后病毒再次出现,之前清除的注册表项及%systemroot%\system32目录下的病毒文件重新出现,并且出现提示:ODBC16.DLL找不到的错误。

笔者心里暗自奇怪,以为刚才有漏哪个步骤,于是再按刚才的方法重新清除一遍病毒,但是重启后又出现先前的现象。之后再清除一次,然后启动到安全模式,果然不再出现,可谁知一启动到正常模式,病毒又出现了。

没辙了,笔者终于明白了这不是一般的网页病毒,于是随意用“netstat -an”命令查看一下输出时,吓了一跳,输出的内容过了二屏才停止,定睛一看,连接的都是内部其他机器(之前因为结束了病毒进程后才用Fport看的,所以这些连接随着病毒进程的结束而被中断)。原来,局域网内已经有很多机器都中了该病毒,杀病毒软件居然一点反应都没有。

再战病毒

暂时离开该同事处,迅速回到自己座位后上网搜索相关的资料,可是几大杀病毒厂商的网站都没该病毒的描述。想不到自己当先锋了。

笔者继续搜索,终于搜索到一点相关的资料,知道病毒可能是Lovegate变种(这其中电话响个不停,只好暂时将电话挂起来),因为之前有类似的Lovegate病毒,只是病毒体(即病毒文件)有些不同。由于里面介绍的病毒清除方法都和笔者原来的方法差不多,认真察看病毒详细描述后终于发现问题所在,原来该病毒是通过弱口令、共享可写进行传播的。看到这,笔者总算知道为什么清除病毒重启后病毒又会在此出现的原因了。

想到病毒软件不能查杀该病毒,且有许多电脑都中了

该病毒，自己不可能一台台清除，于是笔者编写了一个清除该病毒的VBS脚本放到计算机登录里面，并且在域服务器上设置下次重启需要更改密码且启用复杂密码等。做好这一切以后，便立刻打电话通知所有部门：有权限设置共享的用户，请取消共享或暂时取消写权限（因为有个别用户有管理员权限），改完后请马上重启电脑，且须更改密码方可登录。

脚本内容如下（由于代码过长且都是重复的，所以请大家注意看文字描述）：

以下为清除Lovegate病毒的VBS脚本，by landy 2004.7.5

```
On Error Resume Next

const HKEY_LOCAL_MACHINE=&H80000002
strComputer="."

'结束病毒进程（如果要结束其他的进程，请将下面的内容拷贝一份且更改相对应的进程名称即可）

strProcsToKill="suchost.exe"

Set wbemObjectSet=GetObject("winmgmts:" & "{impersonationLevel=impersonate,} & "authenticationLevel=Pkt"}\\" & strComputer & "\root\cimv2").InstancesOf("Win32_Process")

For Each wbemObject In wbemObjectSet
If LCase(wbemObject.Name) =strProcsToKill Then wbemObject.Terminate
Next

'删除在注册表的病毒启动项（如果要删除其他注册表键值，请将下面内容拷贝一份且更改相对应的注册表键值名称即可）

Set oReg=GetObject("winmgmts:{impersonationLevel=impersonate}!\\" & strComputer & "\root\default:StdRegProv")

strKeyPath = "SOFTWARE\Microsoft\Windows\CurrentVersion\Run"

strWORDValueName = "RAVMOND.exe"

oReg.DeleteValue HKEY_LOCAL_MACHINE,strKeyPath, strWORDValueName

'删除病毒文件（如果要删除其他的文件，请将下面内容拷贝一份
```

且更改相对应的文件名称即可)

```
Set objFSO=CreateObject("Scripting.FileSystemObject")
objFSO.DeleteFile("c:\winnt\system32\IEXPLORE.EXE")
```

做好这一切后，笔者随机去检查用户的电脑，果然，启动后再没有出现该病毒，这才松了一口气。接下来就是更新病毒库和等大家下班后，在Officescan中设置统一扫描一次内部所有的电脑，以杜绝有些没清除干净的病毒文件。

感触：这次病毒事件让笔者明白，必须加强每一个薄弱环节，木桶理论在这里就能很好地体现出来了。在此也为每一位网管员提个醒：要彻底防止病毒必须从安全这个源头抓起。加强局域网内的安全非常重要，这也是目前业界提出立体防御（或说整体防御）的原因了。当内部安全做足，并在相应的出口部署防毒墙进行全网保护，才可能使我们的网络在蠕虫病毒横行的年代处于不败之地。

各门功课都辅导 不用到处请家教

中小生当然要订《少年文摘报》

《少年文摘报》作为全国唯一一份以指导中、小学生学习和传授百科知识为主要内容的学习辅导类精品文摘报纸，从小学到高中，各年级单独出版发行，创办23年来，两代人数千万读者从中受益，深受广大中小学校师生的信赖和喜爱。

各报从全国上千家学习类报刊和辅导资料中萃取精华，小学各版以语、数、英为主，注重百科知识的传授和创新思维能力的开发；初中、高中各版涵盖语、数、英、理、化、生、政、史、地全部内容，以同步训练、释疑解惑为主，注重学习技巧、思路、方法和重难点的归纳分析解答，提高读者的应试能力，确保在中考和高考中取得成功。本报在历年的高、中考中平均试题命中率75%以上，数以万计的中小学校将本报列为必选的学习辅导资料，本报被全国中小学教学改革研究中心评为“我最喜爱的中国少年儿童类报刊”名列前茅，中国报业协会等机构授予本报“全国青少年喜爱的名报名刊”等称号，全国近20个省、市、自治区推荐本报为“教学辅导类精品学习报纸”，发行代理遍布全国。是广大中小学生学习上不可多得的好帮手。本报从2005年起推出各年级试题版，与学习版有效互动，是同学们检测学习效果的权威标尺。

一、索样：请来信封3元邮资即寄近期出版的各版样报及相关资料。

二、订阅：到当地邮局订阅，也可汇款到报社订阅，免收邮资费。欢迎全国各地有识之士做本报发行代理。

汇款地址：兰州市白银路47-8号新闻大厦13楼少年文摘报财务处(收) (邮政编码：730030)

联系电话：0931-8156591 8128676

邮发代号	报纸名称	单价	全年价
53-79	小学一年级学习版	0.50	27.00
53-80	小学二年级学习版	0.50	27.00
53-81	小学三年级学习版	0.80	43.20
53-82	小学四年级学习版	0.80	43.20
53-83	小学五年级学习版	0.80	43.20
53-84	小学六年级学习版	0.80	43.20
53-101	小学写作与欣赏版	0.50	27.00
54-150	小学三年级达标试题版	4.00	24.00
54-151	小学四年级达标试题版	4.00	24.00
54-152	小学五年级达标试题版	4.00	24.00
54-153	小学六年级达标试题版	4.00	24.00

邮发代号	报纸名称	单价	全年价
53-85	初一学习版	0.80	43.20
53-86	初二学习版	0	
53-85	初一学习版	0.80	43.20
53-86	初二学习版	0.80	43.20
53-87	初三学习版	1.20	64.80
53-102	初中写作与欣赏版	0.80	43.20
54-154	初一达标试题版	4.50	27.00
54-155	初二达标试题版	4.80	28.80
54-156	中考冲刺试题版	5.00	30.00

邮发代号	报纸名称	单价	全年价
53-88	高一学习版	1.20	64.80
53-89	高二学习版	1.20	64.80
53-90	高三文科学习版	1.20	64.80
53-91	高三理科学习版	1.20	64.80
53-103	高中写作与欣赏版	0.80	43.20
54-157	高一达标试题版	5.00	30.00
54-158	高二达标试题版	5.00	30.00
54-159	高考文科冲刺试题版	5.00	30.00
54-160	高考理科冲刺试题版	5.00	30.00

横扫毒界
之 2004

防毒路上, 还欠缺什么?

■ 北京 董霞 山东 庄甲升 新疆 叶自力

2004年可以说是各类病毒大发展的一年, 无论是数量、手段还是破坏力、传播范围, 都较以往有了大幅提高, 给企业的防病毒工作带来了相当的困难。为了防范这些病毒, 您可能在安全产品方面做了大量投入, 可是, 为什么系统中依然时不时会有病毒拜访一下呢?

您的防毒体系中, 究竟还欠缺什么?

何处是真正的薄弱环节

有些人也许会认为, 装上杀毒软件, 及时更新病毒库, 及时给系统打上各种补丁, 不就万事大吉了? 其实, 这仅仅是病毒防护中的一个环节。

举个简单的例子, 一台电脑放在网络管理员手中, 可能没有安装任何杀毒软件也不会出问题; 但如果在一个电脑初学者手中, 即便装上最新的杀毒软件也一样会被病毒破坏得一塌糊涂。这充分说明, 人才是真正的薄弱环节。也许您的网络配备了全面的安全防护体系, 但黑客却并不是必须通过计算机技术来实现入侵的, 他们还可以通过各种手段来诱使别人自己走进陷阱。

提高员工安全意识

病毒的蔓延, 往往是由于企业内部员工对病毒的防范意识不够重视, 对病毒的知识以及危害性不了解引起的。所以, 我们平时就要加强安全意识, 类似教育企业员工不要打开来历不明的电子邮件、减少共享文件夹的数量、文件共享的时候尽量控制权限和增加密码等, 都可以很好地防止病毒的传播。

对于网络管理员而言, 除了要具备一定的病毒知识和技术外, 更重要的是自身认真的工作态度和责任感。举个真实的例子, 某公司安装了企业版防病毒软件, 但局域网的客户端还是中了“震荡波”病毒, 寻找原因, 发现是由于网络管理员忘记给每台计算机打安全补丁了。如果提前做好预防工作, 这些麻烦和损失是完全可以避免的。

加强内部安全管理

没有规矩, 不成方圆。如果连内部网络管理都没法作好, 怎么谈安全?

制定有针对性的保安规划

制定有针对性的保安规划是保护网络安全的关键, 是将

企业网对安全的期望值与合适的管理构架、适当的保安系统相结合所制定的一套有针对性的保安规划。

第一步, 建立一个有针对性的保安规划。要明确在安全问题上您的目标是什么, 需要保护哪些网络资源, 要达到什么安全级别, 目前面临哪些威胁。一个高安全的保安系统应该能够在适当地点安置足够的保安措施。

第二步, 制定安全制度和公约, 约束企业员工的访问行为, 确保所有在网上并影响网络安全的员工都按公约中规定的方式操作。企业网保安公约是对信息系统工作过程的简明概述, 应规定如下要点: 可以使用本系统的员工; 员工使用系统的时段; 员工对系统的使用权限, 针对不同的部门可以有所不同; 系统接入权的授权程序; 系统接入权的撤销程序, 在类似员工离职等情况下发挥作用; 系统的使用方式总汇; 远程与本地登录方式; 定期检查系统审核跟踪所记录的数据; 对开发商预设的所有密码进行修改; 使用不易猜测的密码, 密码至少要有八个字符, 其中要包含特殊字符并且同时使用大小写; 定期更换密码; 定期对所有的系统进行病毒检查; 定期发送有关安全威胁、政策、补救措施的安全简报; 定期将所有敏感数据进行备份; 教育职员使用特定的流程来核对对方身份等。

最后, 在明确了保护对象及其所需要的安全级别之后, 结合各种网络安全产品构建一套合适的保安系统。

按部门或安全级别分类

划分网段是保证网络安全的一项重要措施, 具体做法为: 将企业网按部门或安全级别分类, 通过具有VLAN(虚拟局域网)功能的交换机将物理位置分散的同类设备组合在同一个虚拟网内, 并通过路由器和防火墙限制不同虚拟网之间的相互访问权限。采用VLAN技术实际上是将以太网基于广播的机制转变为点到点通讯, 让信息只到达应该到达的地点。因此, 这样可以防止大部分基于网络监听的入侵手段。

VLAN可以按系统的安全性来划分, 将总部中的服务器系统单独划在一起, 如数据库服务器、电子邮件服务器等组成一个VLAN; 也可以按机构职能划分, 如将领导所在的网络单独作为一个VLAN, 其他部门分别作为一个VLAN。为保证VLAN之间的单向信息流动, 比如允许领导所在的VLAN查看其他VLAN的相关信息, 而其他VLAN不能访问领导所在VLAN的信息, 需要在这两个VLAN之间设置防火墙作为安全隔离设备。IN

微软公布 6 大补丁

MS04-040: IE 累积性安全更新

漏洞类型: 远程代码执行

重要说明: 此更新也是累积性更新, 取代 Microsoft 安全公告 MS04-038 附带的更新。此更新可能不包括自 MS04-004 或 MS04-038 发布后发布的修补程序。

受影响系统: Windows 2000 SP3/SP4, Windows XP SP1, Windows NT Server 4.0 SP6a/4.0 Terminal Service Edition SP6, Windows 98/98 SE 及 Windows ME 中的 IE6 SP1 或者 IE6 for Windows XP SP1 (64 位版本)。

摘要: 此更新可消除一个公开报告的新发现漏洞。该漏洞可能允许在受影响的系统上执行远程代码。

MS04-041: WordPad 中存在可能允许执行代码的漏洞

漏洞类型: 远程执行代码

严重等级: 重要

受影响系统: Windows NT Server 4.0 SP6a/ 终端服务器版 SP6, Windows 2000 SP3/SP4, Windows XP SP1/SP2, Windows XP 64-Bit Edition SP1/XP 64 位版本 (2003 版), Windows Server 2003 及其 64 位版本, Windows 98/98 SE, Windows ME。

摘要: 该更新可消除一些秘密报告的新发现的漏洞。如果用户使用管理权限登录, 成功利用这些漏洞的攻击者就可以完全控制受影响的系统。要利用此漏洞, 需要进行用户交互。

MS04-042: DHCP 中存在允许远程执行代码和 DoS 漏洞

必读群体: 使用 DHCP Server 服务的用户。

漏洞类型: 远程执行代码

严重等级: 重要

受影响系统: Windows NT Server 4.0 SP 6a/ 终端服务器版 SP6。

不受影响系统: Windows 2000 SP3/SP4, Windows XP SP1/SP2/64-Bit Edition SP1/Version 2003, Windows Server 2003/2003 64-Bit Edition, Windows 98/98 SE 和 Windows ME。

摘要: 该更新可消除一些秘密报告的新发现漏洞。如果被利用, 会导致动态主机配置协议(DHCP)服务器出现拒绝服务故障。

MS04-043: 超级终端中存在可能允许执行代码的漏洞

漏洞类型: 远程执行代码

严重等级: 重要

受影响系统: Windows NT Server 4.0 SP6a/4.0 终端服务器版 SP6, Windows 2000 SP3/SP4, Windows XP SP1/SP2, Windows XP 64-Bit Edition SP1/64 位版本 (2003 版), Windows Server 2003/2003 64 位版本。

不受影响系统: Windows 98/98 SE, Windows ME。

摘要: 此更新可消除一个秘密报告的新发现漏洞。要利用此漏洞, 需要进行用户交互。

MS04-044: Windows 内核和 LSASS 中存在特权提升漏洞

漏洞类型: 特权提升

严重等级: 重要

受影响系统: Windows NT Server 4.0 SP6a/Server 4.0 终端服务器版 SP 6, Windows 2000 SP3/SP4, Windows XP SP1/SP2, Windows XP 64-Bit Edition SP1/XP 64 位版本 (2003 版), Windows Server 2003 及其 64 位版本。

不受影响系统: Windows 98/98 SE, Windows ME。

摘要: 该更新可消除一些秘密报告的新发现的漏洞。成功利用该漏洞可能完全控制受影响的系统。

MS04-045: WINS 中存在可能允许远程执行代码漏洞

必读群体: 使用 Windows Internet 命名服务 WINS 的用户。

漏洞类型: 远程执行代码

严重等级: 重要

受影响系统: Windows NT Server 4.0 SP6a/4.0 终端服务器版 SP6, Windows 2000 Server SP3/SP4, Windows Server 2003 及其 64 位版本。

不受影响系统: Windows 2000 Professional SP3/SP4, Windows XP SP1/SP2, Windows XP 64-Bit Edition SP1/Version 2003, Windows 98/98 SE, Windows ME。

摘要: 此更新可消除多个公开报告和秘密报告的新发现漏洞。建议 WINS 管理员尽早安装该更新。

WINS 漏洞详细分析

■ 上海 马木留克

年底临近,微软又发布了一系列的产品补丁,其中,WINS 内存覆盖导致任意指令执行的漏洞颇值得关注。

漏洞分析

WINS 是 Microsoft NetBIOS 名字服务,用于解析 NetBIOS 计算机名到 IP 地址。研究人员发现,WINS 服务的守护进程 Wins.exe 对特殊 WINS 包处理不正确,远程攻击者可以利用这个漏洞以进程权限在系统上执行任意指令。

具体的情况是,WINS 有一个功能叫 WINS 复制,用于一个和多个 WINS 服务器交换其网络中的电脑信息,WINS 复制通过 Microsoft 私有协议经过 TCP 42 端口完成。在这个协议流程中,内存指针会从服务器发送给客户端,而客户端使用这个指针与服务器进行会话。如果特殊构建的 WINS 包发送给服务器,攻击者可以控制指针,指向攻击者控制的服务器地址,最后可以写任何地址的 16 字节,精心构建提交数据可能以进程权限在系统上执行任意指令。

通过对 WINS 的反汇编可以了解到,向开启了 WINS 服务的主机提交满足以下格式的数据,可能造成一个任意地址写的危险:

```
+-----+
| 数据长度 |
+-----+
| xx xx FF xx |
+-----+
| 实地址指针 P |
+-----+
| ... .. |
```

这里的数据长度是除去自身所占四字节的数据段的长度,为一个 DWORD。数据段的第三个字节设定为 0xFF 可以触发这个漏洞。

对 WINS 反汇编后得到的代码表明,这个数字在满足特定条件时,会有以下的 C 语言描述的行为发生:

```
if(data[3] ^ 0x78 == 0x78 && p)
{
    ... ..
    for(int i=0; i < 4; i++)
    {
        *(DWORD*)(*p+0x48)=*(p+0x24);
        p+=sizeof(DWORD); //p++
    }
}
```

```
}
... ..
}
```

问题出在 WINS 服务几乎没有对我们提交的指针进行判断,就直接对这个指针指向的地址进行了操作,一旦我们把这个指针设定为指向一个我们可以控制的区域,比如就是我们提交的这个报文在内存中存放的区域,那就可以做到写任意的十六字节(四个 DWORD)到任意连续的地址中去。然而,这个漏洞被利用的一个首要条件就是攻击者要准确地猜中自己数据的所在位置,这其实无形中增加了被利用的难度。

通过进一步的研究可以了解到,由于 WINS 自己的异常处理机制,在攻击者提交了不正常的数据以后,服务进程并没有崩溃掉,也就是说,这个漏洞可以被反复利用。恶意攻击者可以采用暴力猜测定位的方法,多次尝试不同的地址,直到成功为止。配合攻击者提交的 shellcode,在获得远程控制权限以后仍然可以保持 WINS 服务的开启状态,使得同一台服务器受到多人攻击的可能性大大增加。

攻击者在准确地定位自身数据后,可以通过改写内存中指向函数的指针,SEH 链或者处理过程中栈内保存的返回地址来获得执行任意指令的权力。对于不同语言的 Windows 2000 而言,某些函数的指针存放在一个相对固定的内存地址中,这使得利用程序可能对不同版本、语言、补丁情况的 Windows 2000 均通用。同样的,Windows NT 也有着类似的情况。存在漏洞的 Windows 2003 情况则要复杂一些,由于 Windows 2003 本身的部分安全机制,使得攻击者不那么容易通过改写某个通用的内存地址来获得控制权限,然而针对各种不同语言的版本,依然可以做到远程成功的利用。

检测方法

我们可以通过扫描对方是否开启了 TCP 42 端口来简单地判断其是否存在问题,然而没有很好的办法来判断对方的操作系统版本以及是否已经受到攻击。

这个漏洞的危害程度虽然严重,但是危害的范围并不大,因为默认安装情况下,WINS 服务并没有安装。手工安装的情况下,在选择组件一步,如果点选了“网络服务”,可能会附带安装并且启动 WINS 服务,所以依然需要检测是否有相关的服务开启。■

近期 Windows 漏洞关注重点

IE 6 存在地址栏欺骗漏洞

受影响系统: Internet Explorer 6.0。

详细描述: Internet Explorer 6 对部分脚本处理不正确, 远程攻击者可以利用这个漏洞伪造地址栏, 欺骗用户。攻击者可以构建恶意链接, 诱使用户访问, 导致显示的地址栏可为实际的地址, 欺骗用户, 用户会盲目的输入敏感信息而泄露。

IE 存在本地文件探测漏洞

受影响系统: Internet Explorer 6.0 SP1。

详细描述: Internet Explorer 在处理 "sysimage://" 协议时存在问题, 远程攻击者可以利用这个漏洞判断目标系统中安装的软件。"sysimage://" 用于显示相对文件路径的正确图标, 默认行为是如果存在的文件路径作为输入, 它就显示相关图标, 但是如果提供的文件路径不存在, 它就装载文件夹的图标来代替, 利用这个特性可判断目标系统中安装的软件。

近期 Unix 漏洞关注重点

Solaris in.rwhod 进程 存在远程任意指令执行漏洞

受影响系统: Sun Solaris 9.0_x86/ 9.0/8.0_x86/8.0/7.0_x86/7.0。

详细描述: Solaris 包含的 in.rwhod 守护进程存在安全问题, 远程攻击者可以利用这个漏洞以 root 用户权限在系统上执行任意指令。

FreeBSD fetch() 整数溢出 远程任意指令执行漏洞

受影响系统: FreeBSD FreeBSD 5.3 及以下若干版本。

详细描述: FreeBSD 的 fetch 在处理 HTTP 头时存在整数溢出问题, 远程攻击者可以利用该漏洞以用户进程权限在系统上执行任意指令。恶意服务器或 CGI 脚本可以以畸形 HTTP 头字段应答 HTTP 或 HTTPS 请求, 可在客户端触发缓冲区溢出, 精心构建应答数据可能以用户进程权限在系统上执行任意指令。

近期 Linux 漏洞关注重点

Linux Kernel AMD64/EM64T TSS 限制特权提升漏洞

受影响系统: Linux kernel 2.4.22/2.4.21/2.4.20。

不受影响系统: Linux kernel 2.2.23。

详细描述: 运行在 AMD's AMD64 和 Intel's EM64T 系统上的 Linux Kernel 时, 在处理 TSS 限制处理上存在问题, 本地攻击者可以利用该漏洞对系统进行拒绝服务或特权提升攻击。

ProZilla 处理网络协议 存在缓冲区溢出等多个漏洞

受影响系统: ProZilla 1.3.6。

详细描述: ProZilla 在处理网络协议时存在缓冲区溢出, 远程攻击者可以设置恶意服务器, 诱使用户使用 ProZilla 获取文件, 可导致以用户进程权限在系统上执行任意指令。

Linux unix_dgram_recvmsg 竞争条件特权提升漏洞

受影响系统: Linux kernel 2.4.9 及以下若干版本。

不受影响系统: Linux kernel 2.4.28。

详细描述: Linux 内核 unix_dgram_recvmsg() 函数没有对信号量进行序列化操作, 本地攻击者可以利用这个漏洞通过竞争条件来提升特权。攻击者必须使 kmalloc() 在特殊分配的内存块上进行 sleep 操作, 然后诱使调度程序执行其他线程来利用这个漏洞, 因此, 利用此漏洞比较困难, 但却是可行的操作。

Linux smbfs smb_proc_readX 敏感信息泄露漏洞

受影响系统: Linux kernel 2.4.9 及以下若干版本。

不受影响系统: Linux kernel 2.4.28。

详细描述: Linux Kernel smbfs 是 Linux 内核支持的文件系统, 用于共享应用。Linux Kernel smb_proc_readX 在读取恶意数据时存在问题, 本地攻击者可以利用这个漏洞获得敏感信息。

当接收 readX 请求的应答数据时, Linx 2.4 kernel 不正确对提供的数据偏移进行边界检查, 问题是由于对符号检查失败, 这表示当连接的服务器从外部数据返回一个数据偏移时, 本地攻击者可以简单地在 smb 文件系统中发送 read 系统调用泄露内核内存信息。如果未分配内存被访问可导致程序崩溃。■

超值工具书

全面上市



1 《中国电脑教育报》
2004年合订本（下）

只需 **19** 元

中国电脑教育报社

地址：北京市海淀区紫竹院路66号赛迪大厦16层

邮编：100044

电话：010-88559609 传真：010-88559664

北京万水电子信总有限公司

地址：北京市海淀区长春桥路5号新起点嘉园4号楼1706室

邮编：100089

2 容量650MB的实用工具光盘，内含全年报纸电子版



3 价值222元的趋势正版杀毒软件（免费升级病毒库一年）



4 免费试玩20小时的《封神榜》新手卡



5 另外，回馈读者调查表，还有价值699元的20个精美MP3等你拿！



正文部分

《中国电脑教育报》精华文章荟萃：新品选购、整机维护、软件使用、办公技巧、网络疑难，只有你想不到的，没有你找不到的！

附录部分

系统安全点点通

Flash经典制作实例

Windows XP SP2经典故障问答

下载、播放全攻略

装机必备的78个技巧

数码相机应用，故障排除大全

国家保密局发布的《计算机信息系统国际联网保密管理规定》中第二章第六条规定：“涉及国家秘密的计算机系统，不得直接或间接地与国际互联网或其他公共信息网络相连接，必须实行物理隔离”。那么，什么是物理隔离？如何实现物理隔离？本文将给您完整的答案。

隔而不断的物理隔离技术

■ 陕西 李晓勇

物理隔离技术管窥

物理隔离技术作为网络与信息安全技术的重要实现手段，越来越受到业界的重视。物理隔离的概念，简单地说就是让存有用户重要数据的内网和外部的互联网不具有物理上的连接，将用户涉密信息与非涉密的可以公布到互联网上的信息隔离开来，让黑客无机可乘。这样就需要一种技术来帮助用户方便、有效地隔离内、外网络。尤其是政府、军事、保安、商业运作和筹划以及重要的科研部门更需要物理隔离技术。

作为物理隔离技术，仅仅是一种被动的隔离方法，目的是为了保障内、外网络信息的隔离，而信息是保存在存储介质上的，物理隔离就是要保证隔离双方的信息不会出现在同一存储介质上，也不会出现在对方的网络中，而在同一时刻二个存储介质只能有一个在发挥作用。

物理隔离技术的要求

一般说来，物理隔离技术需要做到以下几点：

- (1) 高度安全。物理隔离要从物理链路上切断网络连接，达到高度安全的可行性。
- (2) 较低的成本。建立物理隔离时要考虑其成本，如果物理隔离的成本达到或超过了两套网络的建设费用，那就失去了物理隔离的意义。

(3) 容易部署。在实施物理隔离时，既要满足内外网络的功能又要易于部署，结构要简单。

(4) 操作简单。物理隔离技术应用的对象是工作人员与网络专业技术人员，因此要求工作站的网络端要简单易行，方便用户，使用者不会感觉到操作的困难性。

(5) 灵活性与扩展性。物理隔离是具有多种配置的，我们可根据现有网络系统的特性，进行灵活改造，达到物理隔离的功能，同时要考虑在网络中可随时添加新设备，不会给网络安全带来任何不利的影响。

物理隔离技术的不足之处

物理隔离技术的不足之处主要表现在四个方面，它们是：

- (1) 物理隔离技术仅仅是一种被动的隔离开关，手段单一，没有与其他安全技术进行配合。
- (2) 物理隔离不能做到安全状态检测，容易被非法人员利用而混入内部网络。
- (3) 内部防范措施。由于内外网的存储介质都在本地，不能有效地防止内部人员的信息主动泄密行为，尤其是内部人员作案。
- (4) 复核取证难度大。内部网络信息一旦泄露出去，无法进行复核、取证，确认泄露信息的行为人相当困难。IN

物理隔离典型技术方案概览

以下介绍八种物理隔离技术的方案, 供有关读者参考。

方案一：专线接入方案

本方案通过专线上网, 使用防火墙保护整个内部网络系统, 将外网隔离在防火墙之外, 方案的结构如图1所示。

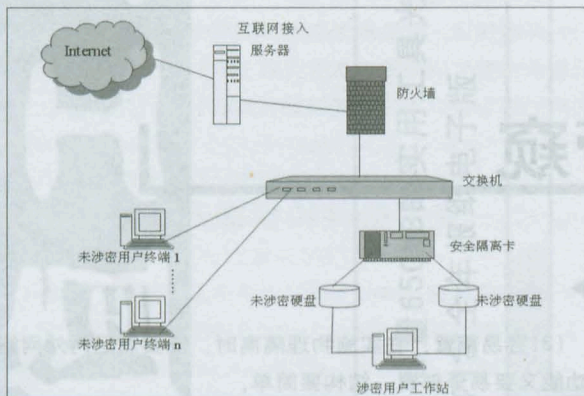


图1 专线接入方案

图1所示的方式存在两方面的安全漏洞: 一是防火墙自身的不安全性, 一些高水平的黑客软件能突破防火墙; 二是在受防火墙保护的网中, 若未涉密用户终端通过Modem拨号进入Internet, 如果其他终端没有采取任何防范措施, 则会使整个网络暴露在黑客眼下, 造成严重的泄密。

这种方案使用了两套独立的布线系统, 但计算机依靠网络拔插的方式轮流登录涉密硬盘和因特网。此方式存在的问题是: 在使用的终端计算机上只有一套硬盘系统, 当该计算机访问外网时会受到各种驻留式黑客病毒的入侵, 当该计算机在内网上工作时会把病毒传播到内网上, 当计算机再次上网时将会造成网上泄密, 同时该计算机上的信息在访问外网时将完全暴露。

方案二：双硬盘隔离方案

用户在实施物理隔离的过程中, 可以选择双硬盘隔离技术方案。其基本思想是: 客户端安装两块硬盘, 当用户登陆内网时, 内网硬盘有效, 外网硬盘无效; 当用户登陆外网时,

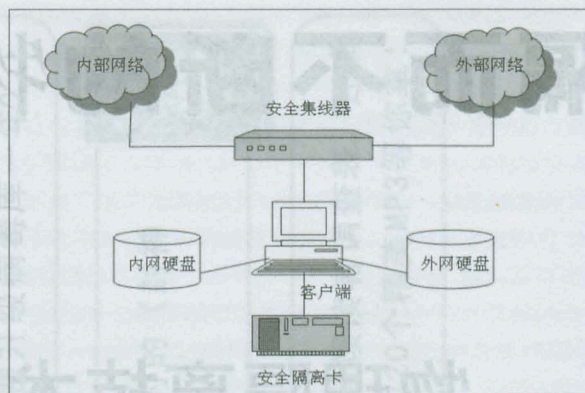


图2 双硬盘隔离方案

外网硬盘有效, 内网硬盘无效。根据网络的不同, 该方案又可以分为单网方案和双网方案。单网方案在网络选择端添加了安全集线器, 该集线器负责与客户端通信, 并根据用户的选择, 连通内外网络。该方案具有部署简单、使用方便的特点, 适合大多数普通用户采用。方案的结构如图2所示。

方案三：网间隔离方案

很多企事业单位的内部财务网是一个相对独立的网络, 需要与内部办公网络隔离, 并且当该网用户登陆互联网和内部网络时, 需要在财务网、内网和外部互联网三网之间进行切换。该方案具有三网隔离能力, 部署简单, 适合内部还有

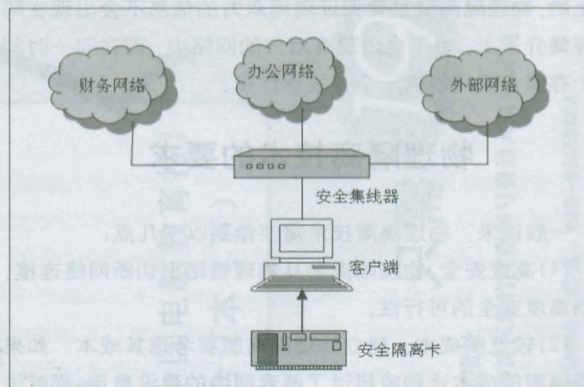


图3 三网间隔离方案

独立小网络的用户采用。其结构如图3所示。

方案四：对外提供服务的隔离方案

许多单位要求在内外网隔离的同时，能够提供电子报税等对外服务。当外部Web服务器在接受互联网上发来的电子税表时，会接通外部网络，断开内部网络，电子税表暂存在本地，当满足了一定条件后，才会断开外部网络，接通内部网络，把电子税表转发到内部业务系统中，同时从内部网络接受上次内部业务系统处理完的电子税表。交换完毕后，再次断开内部网络，接通外部网络，接收新的电子税表。这种方式就好像用户在河的两岸，通过一只船来回传递两岸的货物，这样不会存在直接连接两岸的桥梁或者船同时停靠两岸的问题，既保证了对外服务需求，又保证了网络安全。

该方案在实现物理隔离的同时，能够提供对外服务。其结构如图4所示。

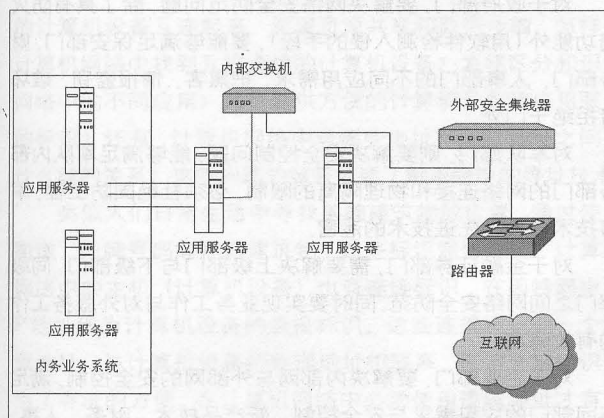


图4 能提供对外服务的隔离方案

方案五：基于无盘系统的隔离方案

一些用户希望在做到内外网隔离的同时，能加强内部管理，防止内部用户泄露本单位秘密。有这种需求的用户，可

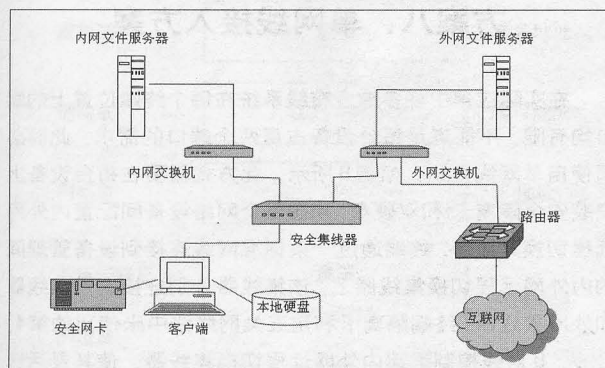


图5 基于无盘系统的隔离方案

以采用基于无盘系统的隔离方案。

该方案采用单硬盘方式，当用户登陆内网时，无盘启动系统通过网络从服务器上启动操作系统，同时屏蔽本地的硬盘、光驱和软驱等存储设备，用户所见的硬盘实际上是服务器分配给用户的硬盘镜像，客户端相当于一个瘦终端。这样，内部用户无法通过本地下载、拆卸硬盘等手段窃取内部信息。该方案在做到内外网隔离的同时，能有效地防止内部网络的泄密。其结构如图5所示。

方案六：单机接入方案

针对单机用户，一般使用安全隔离卡Ⅲ型，配备双硬盘。其结构如图6所示。

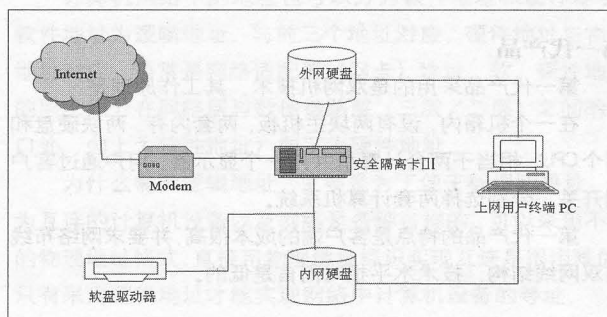


图6 单机接入方案

这种结构具有内、外网的硬盘，无论是在内网还是在网外的硬盘上工作，产生的文件、数据存放于硬盘还是软盘，都是相当安全的。

方案七：双网线接入方案

双网线接入方案需要两套布线系统，但使用Internet的用户数量不是很多，在网络布线接口较为富余的情况下，采用双网线方式，并使用安全隔离卡Ⅱ型，结构如图7所示。

双网线接入方案在上网时涉及用户配置安全隔离卡Ⅱ和双硬盘，两条网络线同时接到隔离卡上，通过隔离卡连接到

【下转第100页】

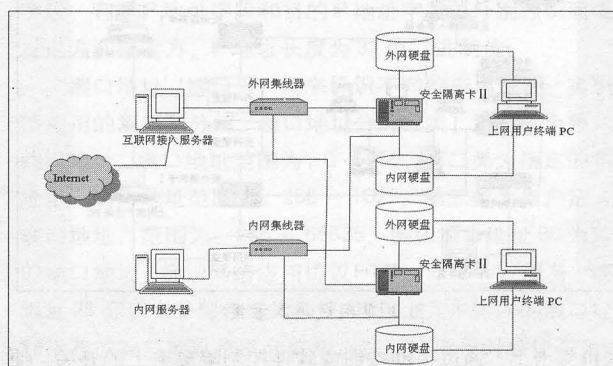


图7 双网线接入方案

物理隔离技术路线回顾

美国早在 1999 年就强制规定军方涉密网络必须与 Internet 断开。我国政府近两年也在不断强调保密问题, 要求有秘密的信息要与网络物理隔离。物理隔离技术的路线, 一般是客户端选择设备和网络选择器, 用户通过开关设备或键盘控制选择不同的存储介质体, 管理端设立内、外网存储介质, 通过防火墙、路由器与外界相连。

物理隔离技术从出现到现在, 虽然时间不长, 但其产品可划分为三代产品。

第一代产品

第一代产品采用的是双网机技术, 其工作原理是:

在一个机箱内, 设有两块主机板、两套内存、两块硬盘和两个 CPU, 相当于两台计算机共用一个显示器。用户通过客户端开关, 分别选择两套计算机系统。

第一代产品的特点是客户端的成本很高, 并要求网络布线为双网线结构, 技术水平相对而言是低的。

第二代产品

第二代产品主要采用双网线的安全隔离卡技术, 其表现为:

客户端需要增加一块 PCI 卡, 客户端硬盘或其他存储设备首先连接到该卡上, 然后再转接到主板, 这样通过该卡用户就能控制客户端的硬盘或其他存储设备。用户在选择硬盘的时候, 同时也选择了该卡上所对应的网络接口, 连接到不同的网络。

第二代产品与第一代产品相比, 技术水平提高了, 成本也降低了, 但是这一代产品仍然要求网络布线采用双网线结构。如果用户在客户端交换两个网络的网线连接, 内外网的存储介质也同时被交换了, 这时信息的安全还存在着隐患。

第三代产品

第三代产品采用基于单网线的安全隔离卡, 加上了网络选择器的技术。客户端仍然采用类似于第二代双网线安全隔离卡的技术, 所不同的是第三代产品只利用一个网络接口, 通过网线将不同的电平信息传递到网络选择端, 在网络选择端安装网络选择器, 并根据不同的电平信号, 选择不同的网络连接, 这类产品能够有效利用用户现有的单网线网络环境, 实现成本较低, 由于选择网络的选择器不在客户端, 系统的安全性有了很大的提高。

目前在网络综合布线行业中, 第一代产品已淘汰, 以第二代和第三代产品为主的物理隔离技术在市场上流行。

在具体的应用范围上要区分几种状况:

对于政府部门, 要解决网络安全防范问题, 除了具有防火墙功能外(用软件检测入侵的手段), 要能够满足保安部门、财务部门、人事部门的不同应用需求, 把黑客、情报盗窃、破坏者拒绝于门外。

对军队部门, 则要解决安全控制问题, 能够满足军队内部各部门的网络连接和物理隔离的限制, 必须杜绝国防工程、军事技术与各种先进技术的泄密。

对于金融证券部门, 需要解决上级部门与下级部门、同级部门之间网络安全防范, 同时要实现业务工作与对外服务工作的有效隔离。

对于企业部门, 要解决内部网与外部网的安全控制, 满足不同部门的应用需求与安全控制, 新产品技术、财务、人事、销售渠道等与整个网络进行局部隔离。

而对于科研部门来说, 既要考虑 Internet 的应用, 又要考虑本身研究课题的保密性, 避免泄密和被盗窃, 应有着严格的隔离限制。■

【上接第 99 页】

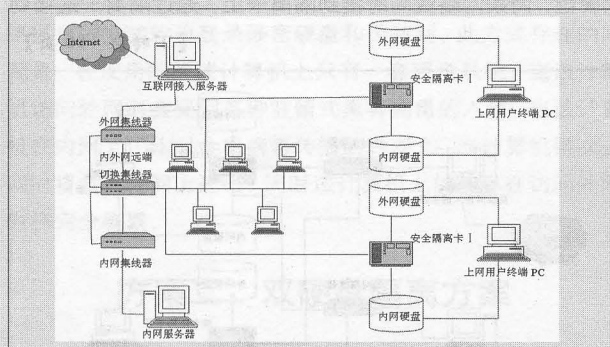


图 8 单网线接入方案

本机网卡上, 通过手动按钮或软件控制隔离卡上的开关, 使其在选择涉密硬盘的同时选择连接内网。因此, 该卡安装时

一定要注意内外网线不能颠倒。

方案八：单网线接入方案

在实际应用中许多综合布线系统在每个终端位置上的端口均有限, 不能满足每台设备占用两个端口的需求, 此时必须使用单网线方式, 如图 8 所示。此方式需要在每台设备上安装安全隔离卡 I 和双硬盘, 并在每个网络设备间配置内外网远程切换集线器。终端通过一条标准网线连接到设备管理间的内外网远程切换集线器上, 该集线器分别连接内网集线器和外网集线器。终端隔离卡利用五类网络线中未使用的第 4、5、7、8 对线控制远端内外网远程切换集线器, 使其灵活选择, 接通内网或外网。■

计算机网络技术系列讲座【之一】

计算机网络从上世纪50年代的联机终端、60年代的多主机互连、80年代的开放网络体系结构（NA）再到如今的Internet，经历了多年的发展。其中，导致这些发展的重要因素就是计算机网络技术的进步。

为了帮助广大网管员深入了解计算机网络技术，本栏目特别邀请了王相林教授为大家介绍计算机网络采用的主要技术。本系列讲座将分三期介绍，本期介绍网络寻址和网络互连技术；下期我们将介绍网络中采用的协议和LAN技术。

网络寻址与互连技术

■ 郑州大学 王相林 教授

寻址技术：在网络中安个家

网络中怎样寻址

计算机网络通过通信协议和传输链路把分散在不同地点的计算机设备互连起来，实现资源共享和数据传输，怎样在计算机网络中找到互相通信的计算机设备？怎样区分和识别网络中的不同应用？怎样提供方便的计算机设备和服务的标识？还有，计算机网络中有哪些地址？这些地址之间是什么样的关系？这些问题的解答需要了解网络中的寻址技术。

类似人们日常生活中寻找某幢建筑物的位置，通过使用街道、门牌号码等标识建筑物，这些标识用作连接，计算机网络中的主机（计算机设备）也有连接标识，在因特网中用IP地址作为计算机设备的连接标识。这些连接标识是一个逻辑地址，与计算机设备的物理地址相联系，采用连接标识是为了寻址的方便，在计算机网络中必须使用逻辑地址才有可能实现计算机设备以及网络的互连。

计算机网络中的地址

计算机网络中有四种地址：域名地址、端口地址、IP地址、物理地址，自顶向下依次与应用层、运输层、网络层、数据链路层对应，如图1所示。

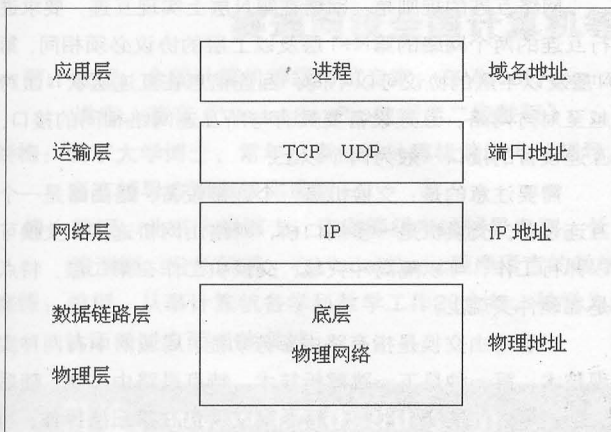


图1 网络中的地址及层次对应

计算机网络中的地址也可以分为软件地址和硬件地址。软件地址为逻辑地址，与前三个地址对应，硬件地址与物理地址对应，通常是网络适配器（网卡）地址。软、硬件地址的层次划分在网络层与数据链路层（三层/二层）之间的接口处，向上为软件地址？向下为硬件地址。

为什么需要逻辑地址，主要是为了便于标识和寻址，因为互连的计算机设备以及网络是各种各样的，可以采用不同的物理地址格式，直接用物理地址标识实现互连是很困难的，只有采用逻辑地址才能实现网络中计算机设备的寻址。

网络地址的使用

访问网络中的计算机设备，寻址最终要执行物理地址，才能找到网络中一个主机的位置，物理地址通常固化在网卡的芯片上，用来惟一标识一个接口的连接。网络寻址时需要进行逻辑地址到物理地址的转换。物理地址在应用时对应数据链路层帧中的MAC地址。

IP地址用来实现不同计算机设备和网络的互连，IP地址其实是一个接口的连接标识，通常人们常说IP地址惟一标识网络中的一个主机的地址，之所以称为地址，是习惯的叫法，实际上IP地址标识一个连接。例如，网络中的路由器也是一台计算机设备，即也是一台主机，路由器往往有2个以上接口，需要多个IP地址，用来标识接口的连接。IP地址包含在IP分组（网络层的协议数据单元）中，为协议数据单元中的字段，有源IP地址字段和目的IP地址字段，分别标识通信的发送方和接收方。IP地址长度为32位二进制位。

端口地址（端口号）用来标识不同的应用进程，实现网络应用的复用和分解。端口地址分为三类。第一类为熟知的端口地址，端口地址范围为：0—255。第二类为指定的端口地址，端口地址范围为：256—1023。第三类为用户定义的端口地址，范围为：256—65535。例如端口地址80为熟知的端口地址，标识网络应用协议HTTP，即WWW服务，端口地址25标识电子邮件应用协议SMTP。其中熟知的端口地址和指定的端口地址是不允许用户在网络编程时随便占用的，是因特网规定分配的，用户编程中定义的端口地址只能用第三类。端口地址的长度为16位二进制位。

域名地址与IP地址相联系,用来标识网络中的一个计算机设备,IP地址使用32位二进制表示,为方便记忆,又采用点十进制记法,但从四个用点间隔的十进制数上很难看出所标识计算机连接的含义。域名地址使用类自然语言的字符,便于人们识别和记忆,能够望文生义,域名地址与IP地址对应,通过域名解析服务找到对应的IP地址。域名地址为层次结构,各个分量之间由点间隔,从右向左,层次级别依次递减。例如网管员世界WWW主机的域名地址为:www.netadmin.com.cn。

网络地址转换

网络中寻址时需进行地址转换。IP地址+端口地址构成套接字Socket,用于标识不同的应用进程,在网络应用编程使用到套接字,网络编程也称为套接字编程实现在一个计算机设备上多种应用服务。

域名地址通过域名服务器的域名解析服务,找到对应的IP地址,域名解析服务采用客户机服务器工作模式。

IP地址通过地址解吸协议ARP,转换为物理地址,反之,物理地址可以通过反向地址解析协议,转换为IP地址。

互连技术:实现网络中的沟通

网络互连设备及对应的层次

网络之间的互连需要互连设备,有四种互连设备,自顶向下划分为:协议转换器(gateway)、路由器(router)、桥接器(bridge)、中继器(repeater)。依次对应的层次为:运输层及以上层次、网络层、数据链路层、物理层,也就是说互连是在不同的层次上进行,越在高层次上实现互连,互连设备需要处理的东西就越多。

不同的互连设备可以实现不同的网络互连类型,同种LAN的互连可以使用中继器,异种LAN的互连可以使用桥接器,LAN-WAN的互连可以使用路由器。网络互连类型有:

LAN-LAN(同种与异种);

WAN-WAN;

LAN-WAN;

LAN-WAN-LAN。

网络互连设备的功能

中继器从LAN接收信号,进行放大,用于扩展信号的传输距离,使用时对中继器的数目有限制,因为信号在传输过程中有衰减,会遇到干扰,在放大信号的同时也放大了干扰的噪声。中继器没有定向控制网络流量的能力,也没有为所传输数据选路的功能,用中继器互连的网络仍然属于一个冲突域。

桥接器(网桥)可以实现异种LAN之间的互连,用来隔离不同的网段,根据转发表决定是否把收到的帧送往另一个网络。桥接器可以识别帧中的MAC地址。桥接器根据实现转

发帧的机制分为透明桥和源选路径桥。桥接器在实现互连时由于要复制帧容易产生广播风暴。

路由器可以实现多种形式的互连,路由器综合使用硬件和软件,将数据从源“路由”到目的。使用路由器的软件可以配置各个连接接口,路由器的硬件可以实现各种路由协议,提高了路由效率。使用路由器可以把网络划分为逻辑网段,这种划分与网络中采用的寻址方法相联系,例如通过对IP地址和子网掩码的设计,可以实现划分子网,实现无类别域间选路CIDR(classless interdomain routing)。还可以使用使能路由器实现内网与外网之间的网络地址转换NAT(network address translation)。

协议转换器实现在运输层及以上层的网络互连,例如一个网络在运输层采用TP4协议,另一个网络在运输层采用TCP协议,在实现两个网络的互连时就要用到协议转换器。由于协议转换器实现互连的层次比较高,在实现起来比较复杂,一般用在特定的使用环境和场合。协议转换器功能的实现往往通过软件设计。

网络互连设备之间的关系

互连设备之间的关系为包含关系,即高层次上的互连设备可以实现低层次上互连设备实现的互连功能,如图2所示。

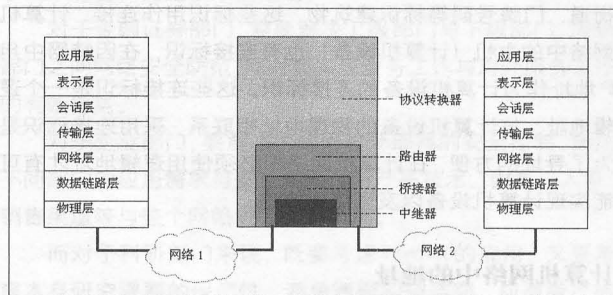


图2 互连设备的层次及包含关系

网络互连规则

网络互连的规则是:网络在第N层上实现互连,要求进行互连的两个网络的第N+1层及以上层的协议必须相同,第N层及以下层的协议可以不同。互连信息在互连层次N上跨越至对方网络。互连设备要具有与所互连网络相同的接口,互连设备的接口一般为两个以上。

需要注意的是:交换机是一个连接设备,路由器是一个互连设备。交换机是一多端口桥,网络由网桥连接,交换可以并行工作,可以隔离冲突域,交换机工作在第二层,特点是在硬件实现上。

三层路由交换是指有路由部分功能,局域网中有两种实现技术:第一种是下一跳解析技术,特点是路由一次,随后交换;第二种是NETFLOW,特点是交换仍在第三层操作,利用先前保存下来的路由信息。 ■

**赛迪网校**

CCID www.ccidedu.com

全国信息技术人才培养工程远程教育平台

赛迪网校 2005年

全国计算机等级考试招生简章

赛迪网校（全国信息技术人才培养工程远程教育平台）由中国极具影响力的IT门户网站——赛迪网建立，2004年招生数千人，据统计，赛迪网校学员考试平均通过率比一般考生至少提高一倍以上！

2005年赛迪网校组建了包括北大、清华等学校知名专家组成的名师团队，开展计算机等级考试考前辅导。赛迪网校将以权威的培训师资、及时的考试信息、贴心的教学服务为学员顺利通过计算机等级考试而保驾护航，赛迪网校有信心在计算机等级考试考前辅导领域再创辉煌，让所有信赖赛迪网校的同学以优异的成绩轻松通过计算机等级考试！

赛迪网校全国计算机等级考试（NCRE）招生计划

考试级别	开设课程	课时(学时)	价格(天)	学习期(天)	赠送资料
一级	一级B	25	80	180	报名任一课程均可获赠对应科目的全真模拟考试软件光盘一套。
二级	Visual BASIC	25	120	180	
	Visual FoxPro	25	120	180	
	C++	25	120	180	
	C	25	120	180	
三级	网络技术	25	120	180	

赛迪网校实用教学服务模式

◆全程指导复习备考

赛迪网校NCRE专家组对考试大纲进行了深入的研究与探讨，提炼出一整套科学有效的复习方案，帮助学员合理安排复习内容和进度，紧跟赛迪，过关没问题！

◆多媒体视频课件

网校采用国际先进技术制作的教学课件，全真模拟课堂教学模式，教学效果深受好评。

◆全真等级考试模拟光盘

网校还为每位学员免费提供一套等级考试模拟光盘，上百套模拟试题供学员日常练习。

有效数据表明以“教师教学+软件日常练习”的方式，学员考试通过率在**80%以上**！

◆支持课件下载离线学习

赛迪网校全部多媒体课件均提供免费下载，以方便学员离线学习。

◆实时、准确、有效的考前指导

网校强大的师资队伍，保证学员学习疑问不过夜！临考前，还将提供由国内知名等级考试专家精心准备的临考模拟试题，高含金量的备考资料，帮助学员踢好临门一脚！

赛迪网校全国计算机等级考试辅导名师团

刘丽：教授，全国计算机等级考试专家，在Visual Foxpro有极深的造诣，曾担任北京教育电视台VF知识讲座，著有《Visual FoxPro数据库二级教程》。

洪妍梅：北京大学博士，常年从事指导计算机等级考试辅导。师从著名计算机科学专家杨芙清教授，在计算机等级考试C语言辅导方面有极深造诣。

赵倩：教授，北京大学博士，资深等级考试辅导专家。长年从事相关辅导工作，教学经验丰富，其授课重点突出，思路清晰，分析精确。在Visual Basic程序语言的教学方面有突出贡献。

杨海锋：教授，从事计算机各学科教学工作20余年，被誉为应试辅导专家。在辅导全国计算机等级考试、NIT考试、微软认证考试方面成就卓越。

网址：www.ccidedu.com

报名咨询热线：010-68861118

赛迪网校面向全国诚招市级经销商 招商热线：(010) 68871388 68862252 68878122

《信息安全与通信保密》杂志社



读者俱乐部开通了!

订阅即可成为会员, 免费参加我社举办的各种活动!

凡通过杂志社订阅 2005 年全年《信息安全与通信保密》杂志的读者, 都可以申请参加读者俱乐部, 成为读者俱乐部会员, 会员将获得参与 2005 年《信息安全与通信保密》杂志定期推出的幸运读者抽奖活动, 以及杂志社举办的各种活动免费或优惠参与资格。

俱乐部会员可享受

- ★ 以优惠价格订阅杂志
- ★ 参加订阅期间俱乐部组织的抽奖活动
- ★ 参加杂志社在全国组织的各种活动

订阅方式

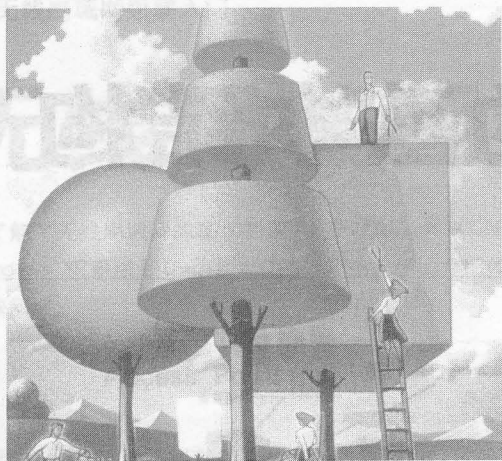
- ★ 邮局订阅: 62-208
- ★ 汇款: 北京复兴路 83 号东 9 楼 236 室 (100856)
成都高新区创业路 6 号 (610041)
《信息安全与通信保密》杂志社发行部

俱乐部联系方式

地址: 北京复兴路 83 号东 9 楼 236 室 (100856)
成都高新区创业路 6 号 (610041)

电话: 010-66808404 028-85169858

欢迎订阅



企业无线局域网组建入门

■ 东北财经大学网络信息中心 孙剑颖

无线局域网(Wireless LAN)是指去除了传统网络中的网络传输线缆,利用微波等无线技术进行信息传递的局域网。无线局域网是上世纪90年代计算机网络与无线通信技术相结合的产物,它提供了使用无线多址信道的一种有效方法来支持计算机之间的通信,并为通信的移动化、个人化和多媒体应用提供了技术支持。作为有线网络的相互补充,无线局域网的应用,满足了用户对移动办公应用的需求。

无线局域网由于其便利性和可伸缩性,特别适用于小型办公环境和家庭网络。与有线网络相比,无线局域网具有以下优点:

(1) 移动性强。无线网络中的计算机通过无线方式进行通信,在任何地方都能提供实时的信息服务,摆脱了线缆的束缚,增强了可移动性。

(2) 灵活性高。无线局域网可以以一种独立于有线网络的形式存在,在需要时可以随时建立临时网络,而不依赖有线骨干网。无线局域网组网灵活,可以满足具体的应用和安装需要。

(3) 安装便捷,维护成本低。无线局域网尽管搭建时的投入资金要比搭建有线局域网高30%左右,但是由于后期维护方便,维护成本比有线网络可减少50%左右。而且对于经常移动、增加和变更的动态环境,无线局域网的长远投资收益更加明显。相对于有线网络,无线局域网的安装工作非常简单,一般计算机工作人员都可以胜任网络的管理工作。同时,无线网络设备可以随办公环境的变化而轻松转移和布置,

有效提高设备的利用率并保护用户的设备投资。

无线局域网(WLAN)的主要技术有蓝牙(Bluetooth)、IEEE 802.11 系列、HiperLAN、HomeRF 技术等,其中,目前得到广泛应用的技术是 IEEE 802.11 系列。而在众多的 802.11 标准中,IEEE 802.11b 以传输距离和传输速率方面的优势得到了广泛应用。

1999 年被正式批准的 IEEE 802.11b 标准,带宽最高可达 11Mbps,可根据实际情况采用 5.5Mbps、2 Mbps 和 1 Mbps 带宽,实际的工作速度在 5Mb/s 左右,与普通的 10Base-T 规格有线局域网几乎是处于同一水平,可以基本满足使用要求。IEEE 802.11b 使用的是开放的 2.4GHz 频段,不需要申请就可使用。既可作为对有线网络的补充,也可独立组网。

IEEE 802.11b 无线局域网与我们熟悉的 IEEE 802.3 以太网的原理很类似,都是采用载波侦听的方式来控制网络中信息的传送。不同之处是以太网采用的是 CSMA/CD(载波侦听/冲突检测)技术,网络上所有工作站都侦听网络中有无信息发送,当发现网络空闲时即发出自己的信息,如同抢答一样,只能有一台工作站抢到发言权,而其余工作站需要继续等待。如果一旦有两台以上的工作站同时发出信息,则网络中会发生冲突,冲突后这些冲突信息都会丢失,各工作站则将继续抢夺发言权。而 802.11b 无线局域网则引进了冲突避免技术,从而避免了网络中冲突的发生,可以大幅度提高网络效率。

本文即以 802.11b 标准为例,介绍如何架构无线网络。

企业无线局域网组建入门

无线局域网的基本结构

无线局域网的设备组成包括无线网卡和无线接入点 (Access Point, 简称 AP)。无线局域网利用常规的局域网及其互联设备构成骨干网。利用无线接入点 (AP) 来支持移动终端 (MT) 的移动和漫游。配有无线网卡的台式 PC 机、笔记本电脑或其他设备就可以与无线网络连接起来。

无线客户端的计算机必须安装无线网卡, 无线网卡作为无线网络的接口实现与无线网络的连接。无线网卡根据接口类型的不同, 主要有三种类型: PCMCIA 无线网卡 (适用于笔记本电脑, 支持热插拔)、PCI 无线网卡 (适用于台式机) 和 USB 无线网卡 (适用于笔记本电脑和台式机, 支持热插拔)。

Access Point, 一般俗称为网络桥接器, 是完成无线网和有线网之间的桥接, 因此任何一台装有无线网卡的 PC 均可使用 AP 去分享有线局域网的资源。另外, AP 又兼具有网管的功能, 可对接入的无线网络卡进行控制。为了让工作站本身有足够的频宽可利用, 一般建议一台 AP 约支持 20~30 个工作站为最佳状态。AP 可加上外接增益天线, 使覆盖距离到达更远、信号更强。

一个典型的企业无线局域网的连接示意图如图 1 所示。企业内部原有的局域网采用 ADSL 线路作为网络出口, 接入 Internet。ADSL 路由器与核心交换机相连。服务器和工作站通

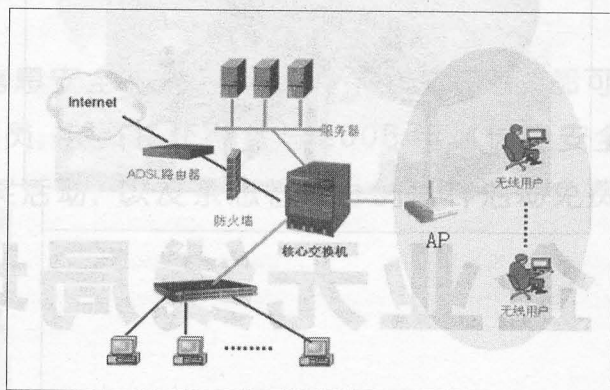


图 1 典型无线局域网示意图

过网线与交换机相连。由于移动办公应用的需要, 使用无线网络进行场区内的网络覆盖。

在本例中, 添加一台无线 AP, 通过直连线与核心交换机相连, 即实现无线局域网和有线 LAN 的互联, 此时无线 AP 完成无线网和有线网之间的桥接。在无线网络覆盖范围内, 无线工作站通过无线网卡与 AP, 接入到企业内部局域网, 共享网络中的信息。

IEEE 802.11 系列标准简介

1990 年 IEEE 802 标准化委员会成立 IEEE 802.11 无线局域网标准工作组。该标准定义物理层和媒体访问控制 (MAC) 规范。物理层定义了数据传输的信号特征和调制, 工作在 2.4000~2.4835GHz 频段。IEEE 802.11 是 IEEE 最初制定的一个无线局域网标准, 主要用于难于布线的环境或移动环境中计算机的无线接入。由于传输速率最高只能达到 2Mbps, 所以, 业务主要被用于数据的存取。

IEEE 802.11a 标准

1999 年制定完成。该标准规定无线局域网工作频段在 5.15G~5.825GHz, 数据传输速率达到 54Mbps/72Mbps

(Turbo), 传输距离控制在 10~100 米。802.11a 采用正交频分复用 (OFDM) 的独特扩频技术; 可提供 25Mbps 的无线 ATM 接口和 10Mbps 的以太网无线帧结构接口, 以及 TDD/TDMA 的空中接口; 支持语音、数据、图像业务; 一个扇区可接入多个用户, 每个用户可带多个用户终端。

IEEE 802.11b 标准

1999 年 9 月被正式批准, 又称 Wi-Fi 标准。该标准规定无线局域网工作频段在 2.4G~2.4835GHz, 数据传输速率达到 11Mbps。该标准是对 IEEE 802.11 的一个补充, 采用点对点模式和基本模式两种运作模式。在数

【下转第 111 页】

企业无线局域网组建入门

无线局域网设置Follow Me

了解了无线局域网的基本知识,下面以D-Link 900AP和装有Windows XP系统和D-Link 650的计算机为例,介绍如何配置无线网络。

Access Point 的配置

使用直连线将AP和管理计算机接入到同一台交换机上,默认状态下AP的IP地址为192.168.0.50,将管理计算机的IP设置为192.168.0.1,在IE浏览器中输入地址: http://192.168.0.50,默认的用户名为ADMIN,密码为空,如图2所示。

单击确定后,出现管理主页,如图3。

一般来说,无线AP是不需要配置的,可以都是默认值。我们需要改动的地方有以下几个:

无线AP的IP地址。由于默认IP地址是192.168.0.50,如果网络中其他设备的IP也为192.168.0.50时就会发生冲突。可以根据具体情况,将IP地址设定为192.168.0.250,子网掩码选择255.255.255.0,如图4。如果网络中存在DHCP Server,支持动态的IP地址分配功能,也可以选择“自动获取IP地址”项。如图5所示,选择HOME中的DHCP项,可以开启或关闭无线AP的DHCP Server服务。如果希望新建的无线网络使用AP进行IP地址动态分配,选择DHCP Server Enable,并设定起始IP地址即可,起始IP可以设定为2~255。我们设定从100开始进行分

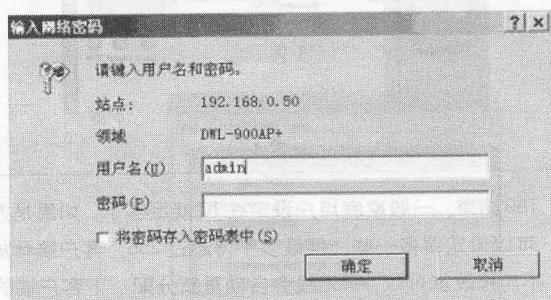


图2

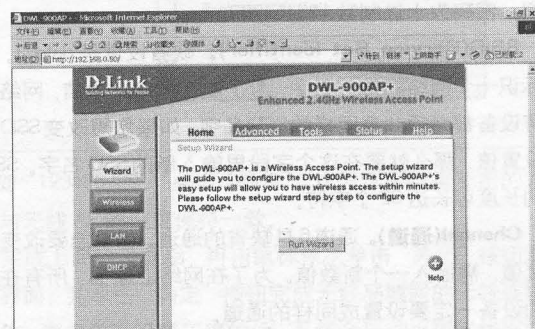


图3

【上接第110页】

据传输速率方面可以根据实际情况在11Mbps、5.5Mbps、2Mbps、1Mbps的不同速率间自动切换,而且在2Mbps、1Mbps速率时与802.11兼容。

802.11b使用直接序列(Direct Sequence) DSSS作为协议。802.11b和工作在5GHz频率上的802.11a标准不兼容。由于价格低廉,802.11b产品已经被广泛地投入市场,并在许多实际工作场所运行。

IEEE 802.11e/f/h 标准

IEEE 802.11e标准对无线局域网MAC层协议提出改进,以支持多媒体传输,以支持所有无线局域网无线广播接口的服务质量保证QoS机制。IEEE 802.11f,定义访问节点之间的通信,支持IEEE 802.11的接入点互操作协议(IAPP)。IEEE 802.11h用于802.11a的频谱管理技术。

IEEE 802.11g

2001年11月批准。该标准可以视作对流行的802.11b标准的提速(速度从802.11b的11Mb/s提高到54Mb/s,仍然工作在2.4GHz频段)。802.11g接入点支持802.11b和802.11g客户设备。同样,采用802.11g网卡的笔记本电脑也能访问现有的802.11b接入点和新的802.11g接入点。

IEEE 802.11i

IEEE 802.11i标准是结合IEEE 802.1x中的用户端口身份验证和设备验证,对无线局域网MAC层进行修改与整合,定义了严格的加密格式和鉴权机制,以改善无线局域网的安全性。IEEE 802.11i新修订标准主要包括两项内容:“Wi-Fi保护访问”(WPA)技术和“强健安全网络”。Wi-Fi联盟计划采用802.11i标准作为WPA的第二个版本,并于2004年初开始实行。

IN1

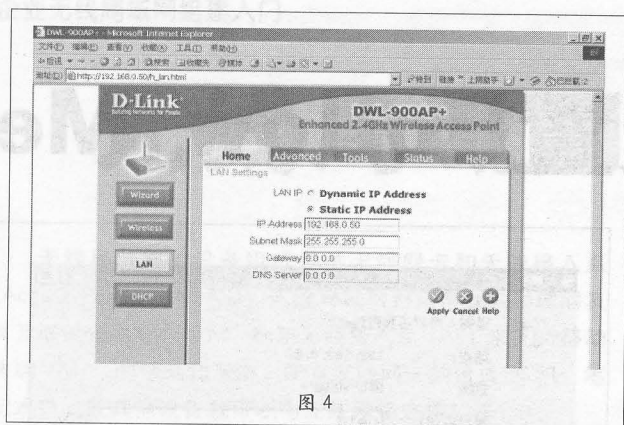


图 4

配, 199 结束。一般家庭用户设定在 10 就足够了, 如果是办公室, 可以设定得多一些, 但最多不得超过 255。客户端释放时间, 不用修改就可以, AP 无线会自动重新分配一下客户端的 IP。选择 HOME 中的 DHCP 项, 设置无线 AP 的名字为 TESTAP, SSID 为 TEST, Channel(通道)为 6, WEP 状态为 Enable, 采用 64 位的加密, 密码为十进制数 123456789。

SSID(Service Set Identifier)。缺省设置是 default。SSID 是标识一个网络的惟一名字, 为了能在网络上通信, 网络中的所有设备都必须共享同样的 SSID 名字。如果您想改变 SSID 的缺省设置值, 那么就要在这个字段里输入新的 SSID 名字。SSID 名字的长度可长达 32 个字符。

Channel(通道)。通道 6 是缺省的通道。如果您要改变缺省设置值, 需输入一个新数值。为了在网络上通信, 所有在网络中的设备一定要设置成同样的通道。

WEP 加密。若在网上使用 WEP(有线等效保密), 需选择 "Enable Encryption"。在网络中的所有设备以及 Access Point

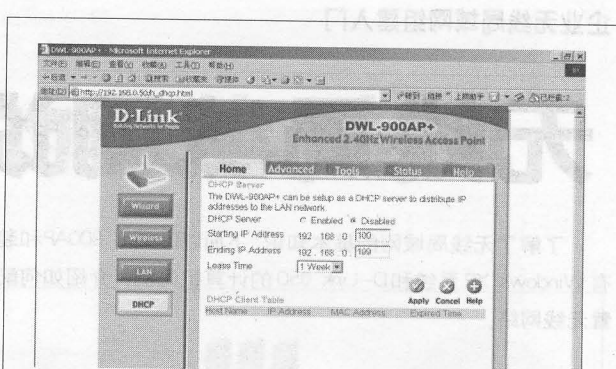


图 5

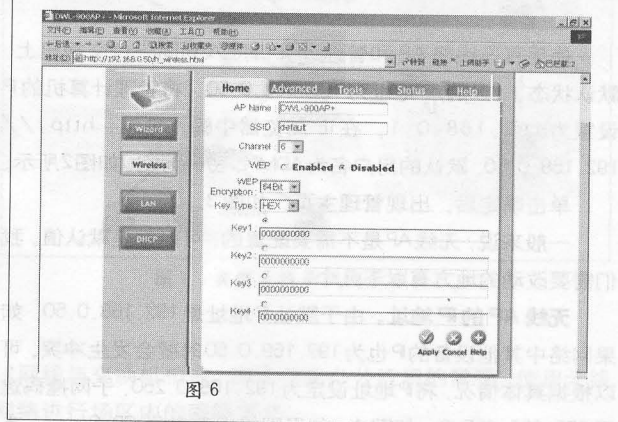


图 6

都要共享同样的 WEP 选择。无论是 Enable 还是 Disable, 它们都要共享同样的 WEP key。The WEP key 由 ASCII 码或者十六进制数产生, 长度可以是 64, 128, 256 位。当需要加密时, 选择 Key 类型 (ASCII 或者十六进制) 然后输入适当的数字或者字母, 最多可以创建 4 个 key。如图 6 所示。

无线局域网的管理与维护

安全性是组建无线局域网需要考虑的主要问题之一。因为无线局域网使用无线电波传输数据信号, 无线电波能够穿透墙壁, 使黑客有机会截获电波并进入未受保护的局域网。在 WLAN 中, 由于不再针对每一端口提供一条专门的线作为通道, 非法数据包在接入现有无线管理区之前很难中途被拦截。为了提供更高的安全保护, 除了采用 WEP 外, 还可以采用虚拟专用网 (VPN)、IPSec 加密和利用 IEEE 802.1x 的 EAP(可扩展鉴别协议)等技术对数据进行加密和保护。限制网络的开放程度, 让只有授权用户可以访问无线设备。

基本上无线网络所使用的频段是属于 ISM 2.4GHz 的高频率范围, 日常生活或办公室等等所用的电器设备是不会

相互干扰, 因频率差异甚多, 而且无线网络本身共有 12 个信道可供调整, 自然干扰的现象也不多。目前, 基于 802.11b 协议的产品已成应用主流, 这些产品都使用 2.4GHz 频段, 能够在短距离内实现大约 11Mbps 的接入速率, 每个接入点可以同时支持数十个用户的接入。但 2.4GHz 频段同时也被蓝牙无线电话和微波炉使用, 所以家庭建无线网络需要考虑一下设备的摆放问题。

无线网络的架设可分室内与室外两部分进行。无线网络架设时, 应考虑无线接入点的数量和位置, 以及网络带宽、网络速度的要求, 包括覆盖频率、信道使用和吞吐量需求等。室外无线接入点的配置应根据地形将各楼房连接起来, 为了增强信号, 还应架设全向室外天线或定向天线。IN

如果无线网络连接的距离比较长或是需要采用无线的方式接入其它的局域网,可以设置无线 AP 为无线的客户端或是网桥,并设置可以接入 AP 的 MAC 地址,如图 7 所示。这里我们只有一个无线 AP,选择 Access Point 项。

无线客户端的设置

Windows XP 系统提供了对无线网络的良好支持,不需要另外安装无线网络管理和配置软件。计算机安装完无线网卡后,可以直接在“网络连接”窗口中来设置网络参数。

在 Windows XP 系统桌面上,依次单击“开始”中的“设置”中的“控制面板”命令,打开控制面板窗口,在其中双击网络图标,打开“网络连接”界面;然后右键单击“无线网络连接”图标(安装无线网卡后自动出现),从打开的快捷菜单中,单击“属性”命令,系统会显示“无线网络连接属性”设置对话框。

单击选中“无线网络配置”标签,并在弹出的“无线网络配置”标签页面中,选中“用 Windows 来配置我的无线网络配置”复选项,启用自动无线网络配置功能;单击“无线网络配置”的“高级”按钮,打开“高级”设置对话框,对话框中用鼠标选择“任何可用的网络(首选访问点)”选项;在首选访问点无线网络时,要是发现有可用网络的话,系统一般会首先尝试连接到访问点无线网络;要是当前系统中的访问点网络不能用的话,那么系统就会自动尝试连接到对等无线网络。如果是计算机与计算机之间的相互连接,单击选中“仅计算机到计算机(特定)”选项。

如果无线网络的传输需要设置安全认证,单击“无线网络配置”中的配置项,在弹出的对话框中,选择“无线网络连接属性”。点击“添加”,弹出如图 8 所示对话框。在“服务名”一栏输入 SSID,即“TEST”,然后激活“数据加密(WEP 启用)”功能,在“网络密钥”和“确认网络密钥”两栏都填入 WEP 密

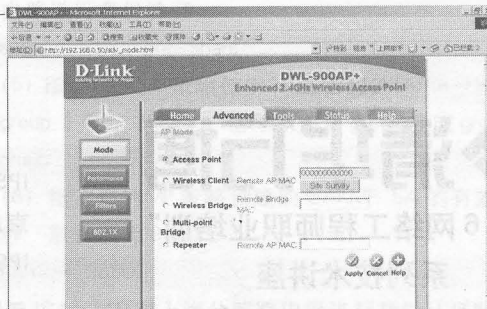
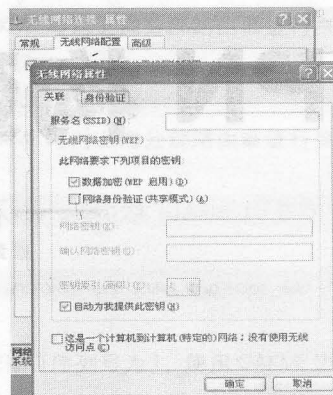


图 7

图 8



钥,即“123456789”,点击“确定”。这里选择数据加密的方式必须与无线 AP 的设置保持一致。

完成上面的设置后,再用鼠标依次单击“关闭”按钮退出设置界面,并单击“确定”按钮完成无线局域网的无线连接设置工作,要是参数设置正确的话,系统会自动出现无线网络连接已经成功的提示。

无线网络连接成功后,单击“无线网络连接”中的 TCP/IP 项,选择属性。与普通的以太网设置一样,配置无线客户端的 IP 地址、子网掩码、DNS、和网关。

《网管员世界》投稿须知



作为一份关注网络管理和应用的技术类刊物,《网管员世界》的成长离不开广大读者的关心和支持,包括对我们刊物的意见、建议和各位作者的投稿。

本刊欢迎所有与网络管理和维护相关的优秀稿件,来稿要求内容实用、文笔生动、可读性强。为了使大家的投稿更加准确、有效,特将注意事项公布如下:

一、需要特别提示各位作者,我刊不向作者收取任何费用。我们已经发现有不人员冒充我刊向作者收取审稿费,并开具假用稿证明,请大家务必警惕。您有类似问题,请电话咨询《网管员世界》编辑部,电话是 010-88558021、88559465。

二、本刊非常欢迎 E-mail 投稿,请将稿件投给我刊的公用投稿邮箱:netadmin@netadmin.com.cn,或者按照刊物中各个栏目标明的投

稿信箱进行投稿。

三、所有来稿必须是从未在任何媒体(包括网站)中发表过的原创文章,若发现一稿多投、抄袭或擅稿现象,本刊将严肃处理,并保留对该投稿人追究法律责任的权利。

四、来稿请以 Word 或文本格式保存,一般文章字数要求在 3000 字以内,特别欢迎短小精悍的文章。如文章中有图片,请将清晰的图片存为 TIF 或 JPG 格式。

五、来稿请注明作者的联系方式,包括姓名、单位、地址、电话等(尤其是电话),便于我们随时和您联系。

六、所有来稿本刊会在五个工作日回信确认稿件收到;如未收到回复,请确认邮件发送正常。出于编辑质量的考虑,稿件的采用过程需要经过多个流程,所以不会立即告知稿件能够采用,视栏目情况会在一周到一个月左右告知作者。

七、关于投稿和刊物的任何问题,欢迎到网管员世界论坛“编读往来”栏目中和我们热线交流。



“1 + 6 网络工程师职业培训”
系列技术讲座

VPN 构建实战

——在 Cisco 路由器之间配置基于 IPSec 的 VPN

■ 清华万博网络安全专家、清华万博高级讲师 丛日权

VPN (Virtual Private Network, 虚拟专用网) 是指利用 Internet 或其他公共网络, 为用户建立一条临时的、安全的隧道, 并提供与专用网络相同的安全和功能保障。VPN 是对企业内部网的扩展, 可以帮助远程用户、公司分支机构和商业伙伴与公司的内部网建立可信的安全连接, 并保证数据的安全传输。在众多构建 VPN 的技术中, IPSec 是目前安全级别相对较高的一种技术, 它可以实现数据通信的保密性、完整性和不可否认性。

清华万博公司在北京总部和上海分部之间建立了基于 IPSec 的 VPN (网络结构如图 1 所示)。以下为读者朋友讲解相关的配置方法。

为提高数据传输的安全性, 清华万博公司使用 Cisco 路由器作为 VPN 终结点, 下文中的讲解也以 Cisco 路由器为例; 北京和上海的路由器名 (hostname) 分别为 RT-BJ 和 RT-SH。

北京总部路由器的配置

1. 配置 ISAKMP 策略

(1) 创建 ISAKMP 策略 (优先级为 1)

```
crypto isakmp policy 1
```

(2) 指定 ISAKMP 策略使用 DES 进行加密 (也可以使用其他加密算法)

```
encryption des
```

(3) 指定 ISAKMP 策略使用 MD5 进行 HASH 运算 (也可以使用 SHA)

```
hash sha
```

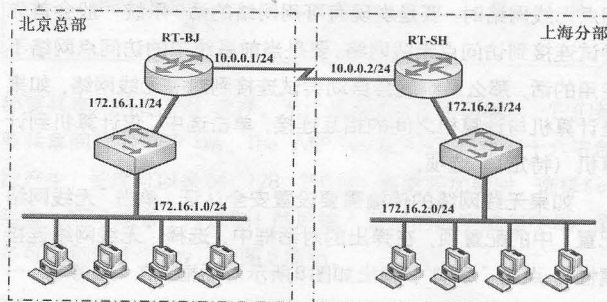


图 1 清华万博公司的网络结构示意图

(4) 指定 ISAKMP 策略使用预共享密钥的方式对上海分部路由器进行身份验证

```
authentication pre-share
```

(5) 指定 ISAKMP 策略使用 10 位密钥的 Diffie-Hellman 算法 (group 1 表示 768 位, 也可以使用 group 2 或 group 5)

```
group 1
```

(6) 指定 ISAKMP 策略创建的 ISAKMP SA 的有效期 (单位为秒, 默认值为 86400)

```
lifetime 28800
```

2. 配置 ISAKMP 对上海分部路由器进行身份认证时的密钥生成参数

(1) 指定 ISAKMP 与对上海分部路由器进行身份认证时使用 IP 地址作为标识

```
crypto isakmp identity address
```

(2) 指定 ISAKMP 与对上海分部路由器进行身份认证时

使用预共享密钥

```
crypto isakmp key cisco123 address 10.0.0.2
```

3. 配置 IPsec 变换集

```
crypto ipsec transform-set bjset esp-des esp-md5-hmac
```

4. 配置加密图

(1) 创建加密图 (序列号为 1, 使用 ISAKMP 协商此加密图创建 IPsec 的 SA)

```
crypto map bjmap 1 ipsec-isakmp
```

(2) 指定加密图用于上海路由器建立 VPN 连接

```
set peer 10.0.0.2
```

(3) 指定加密图使用的 IPsec 变换集

```
set transform-set bjset
```

(4) 指定使用此加密图进行加密的通信 (用访问控制列表来定义)

```
match address 101
```

5. 设置内网接口

```
interface FastEthernet0/0
```

```
ip address 172.16.1.1 255.255.255.0
```

6. 设置外网接口

```
interface serial0/0
```

```
ip address 10.0.0.1 255.255.255.0
```

```
no ip mroute-cache
```

```
no fair-queue
```

```
clockrate 64000
```

(1) 指定在此接口上应用加密图

```
crypto map bjmap
```

7. 配置访问控制列表指定需要加密的通信

```
access-list 101 permit ip 172.16.1.0 0.0.0.255 172.16.2.0 0.0.0.255
```

```
access-list 101 permit ip 172.16.2.0 0.0.0.255 172.16.1.0 0.0.0.255
```

```
!
```

```
end
```

上海分部路由器的配置

1. 配置 ISAKMP 策略

(1) 创建 ISAKMP 策略 (优先级为 1)

```
crypto isakmp policy 1
```

(2) 指定 ISAKMP 策略使用 DES 进行加密 (也可以使用其他加密算法)

```
encryption des
```

(3) 指定 ISAKMP 策略使用 MD5 进行 HASH 运算 (也可以使用 SHA)

```
hash sha
```

(4) 指定 ISAKMP 策略使用预共享密钥的方式对上海分

部路由器进行身份验证

```
authentication pre-share
```

(5) 指定 ISAKMP 策略使用 10 位密钥的 Diffie-Hellman 算法 (group 1 表示 768 位, 也可以使用 group 2 或 group 5)

```
group 1
```

(6) 指定 ISAKMP 策略创建的 ISAKMP SA 的有效期 (单位为秒, 默认值为 86400)

```
lifetime 28800
```

2. 配置 ISAKMP 对上海分部路由器进行身份认证时的密钥生成参数

(1) 指定 ISAKMP 与对上海分部路由器进行身份认证时使用 IP 地址作为标识

```
crypto isakmp identity address
```

(2) 指定 ISAKMP 与对上海分部路由器进行身份认证时使用预共享密钥

```
crypto isakmp key cisco123 address 10.0.0.1
```

3. 配置 IPsec 变换集

```
crypto ipsec transform-set shset esp-des esp-md5-hmac
```

4. 配置加密图

(1) 创建加密图 (序列号为 1, 使用 ISAKMP 协商此加密图创建 IPsec 的 SA)

```
crypto map shmap 1 ipsec-isakmp
```

(2) 指定加密图用于上海路由器建立 VPN 连接

```
set peer 10.0.0.1
```

(3) 指定加密图使用的 IPsec 变换集

```
set transform-set shset
```

(4) 指定使用此加密图进行加密的通信 (用访问控制列表来定义)

```
match address 101
```

5. 设置内网接口

```
interface FastEthernet0/0
```

```
ip address 172.16.2.1 255.255.255.0
```

6. 设置外网接口

```
interface serial0/0
```

```
ip address 10.0.0.2 255.255.255.0
```

```
no ip mroute-cache
```

```
no fair-queue
```

```
clockrate 64000
```

(1) 指定在此接口上应用加密图

```
crypto map shmap
```

7. 配置访问控制列表指定需要加密的通信

```
access-list 101 permit ip 172.16.1.0 0.0.0.255 172.16.2.0 0.0.0.255
```

```
access-list 101 permit ip 172.16.2.0 0.0.0.255 172.16.1.0 0.0.0.255
```

```
!
```

```
end
```


“Linux 跟我学”系列专栏 (之一)



目前有关 Linux 技术文章、教程和小技巧,在图书馆、书店、网络上随处可见,它们是 Linux 应用开发和系统管理的宝藏。但是眼下的现实情况是 Microsoft 公司的操作系统 (Windows NT, Windows 98, Windows 2000, Windows XP) 已经安装在了世界上 90% 的 PC 机上,人们想要从 Windows 平台转移到 Linux 平台并不容易,对于那些试图自己选择方向的读者来说,则尤为如此。许多人都感觉在这些 Linux 技术文章、教程和小技巧中找到所有需要的信息来得很不容易。

本专题就是要对想要学习 Linux 但又无从下手的读者提供综述指导,在讲解 Linux 知识的基础之上,把相关的文章、教程、技巧以及当前 IT 产业方面的信息集结在一起,以利于进一步的学习。我们的目标是要让 Linux 初学者能够像在 Microsoft Windows 里一样,随心所欲地做任何事情,甚至做得更好、更多。

Linux 历史漫谈

■ 北京 张家才博士

Linux 究竟是什么?

用最简单的话说, Linux 是一个操作系统。它是由当初身份还是芬兰赫尔辛基大学学生的 Linus Torvalds (Linux 是 Linus's UNIX 的缩写) 在 1991 年 10 月创造出来的。Linux 本身实际上只是其内核;它实现了多任务和多用户功能,管理硬件,分配内存并且使应用程序能够运行。

对于任何一种操作系统,普通用户绝对没有足够的兴趣去了解其内核内部是如何运作这样的内容。只有真正致力于此的人——那些放弃个人生活或受雇做这种工作的人——才愿意探索这些复杂的东西。但即使您从未亲身深入研究过内核,也无需担心,您可以很容易地雇用一家承包商或公司来为您完成这项工作;对一个专有系统进行这样的修改常常较困难,花费也比较大。

对于初学者,有关内核要记住的最重要的事情是:带奇数的内核版本 (即 2.3、2.5、2.7 等) 是实验性的开发版内核。稳定的发行版内核的版本号是偶数 (即 2.4、2.6、2.8 等)。

典型的 Linux 发行版在 Linux 内核之外,还包含许多应用程序和工具。总的说来, Linux 发行版中出现的许多系

统级和用户级的工具都来自自由软件基金会 (Free Software Foundation) 的 GNU 项目 (GNU 是 “GNU's Not UNIX” 的缩写)。

Linux 内核和 GNU 工具套件都在 GNU 通用公共许可证 (GNU General Public License, GNU GPL) 的授权下发行。如果您还不熟悉 GNU GPL, 那么理解它的最佳方法就是去阅读它。冒着可能会遗漏某些重要方面的风险,我这样概括 GNU GPL:它是一种使计算机代码可自由使用的方式,使用其代码的用户可随意使用和实验它。

从“玩具”到热门话题

计算机操作系统的历史开始于上世纪 50 年代,当时还只是用来最小化程序间的空闲时间间隔,以提高批处理程序的效率。批处理程序根本就不与用户交流,它从文件读取输入 (可能是一堆打孔卡),并将结果输出到另一个文件 (可能是打印机,打印机在操作系统中也是文件)。这就是当时的操作系统的工作方式。

到了上个世纪 60 年代早期,交互式的计算机应用开始发展。这一时期,不光是计算机可以与用户交互,甚至出现

了多个用户从不同的终端,同时使用同一台计算机的情况。这样的系统叫做分时系统(time-sharing systems),相对于批处理而言是一在挑战。整个60年代,为了创建优秀的分时系统,人们进行了大量的尝试。其中的一些是大学的研究项目,其它一些是商业项目。这些项目中的一个Multics,在当时它是一大创新。例如,它开创性地提出具有层次结构的文件系统,当然了,在今天的操作系统中这是被认为是理所当然的。

然而Multics项目在随后的时间并没有太大的发展,它的参与者之一的贝尔实验室(Bell Labs)退出了该项目。贝尔实验室中参与了这个项目的那些人开始研制他们自己的操作系统,称为Unix。Unix最初是免费发放的,很快就在各个大学普及开来。再后来它实现了TCP/IP协议,并因此而成为早期工作站的操作系统。

到了1990年,Unix操作系统已经在服务器市场站稳脚跟,并在大学中有很坚实的基础。许多的大学都安装有Unix系统,并对计算机科学的学生开放。许多学生希望能在他们自己的计算机上也可以运行Unix,但不幸的是当时Unix已经商业化,而且价格不菲。一个省钱的选择就是Minix,它是由Andrew Tanenbaum编写的一个用于教学用途的受限的类似于Unix的系统。那个时候还有386BSD, NetBSD, FreeBSD以及OpenBSD,但它们都还不成熟,并需要很高的配置,这在当时的情况下是不太可能的。

1991年10月,Linux就诞生于这种背景下。Linux的作者Linus Torvalds,他在赫尔辛基大学使用Unix,但是也想在自己家的PC机上运行一个类似的东西。商业的软件太过昂贵,他就开始研究Minix,并要做得比Minix更好,很快他就开始编写自己的操作系统。Linux第一版发布后,立即引起了其他几位电脑黑客的兴趣。虽然Linux最初只是一个玩具,没有任何特殊用处,但它很快就集中了大量的优点,并吸引了那些对操作系统开发本来没有什么兴趣的人也参与进来。

Linux本身只是操作系统的内核,内核是使其他所有程序能够运行的那部分。它实现多任务处理,并管理硬件,让应用程序能够做它们的事情。用户(或是管理员)所交互的所有程序都运行在这个内核之上。在这些程序中,有些是必不可少的基本要素:如命令行解释器(command line interpreter)或Shell,它们既可以用于交互,以可用来编写Shell脚本(就像Windows下的.BAT文件)。

Linus并没有亲自编写这些程序,而是使用了现有的免费版本,这样做大大减少了他的工作量。事实上,他常常改变内核,为的就是让这些现有的程序能够运行在Linux上。

大多的特别重要的系统软件,包括C编译器,都来自于自由软件基金的GNU项目(Free Software Foundation's GNU project)。1984年开始的GNU项目的目标是开发一个完全免费的类似于Unix的操作系统,为了怀念它,许多人都喜欢将

Linux称为GNU/Linux系统(GNU有它自己的内核)。

1992-1993年间Linux获得了替代Unix工作站所需要的所有特性,包括TCP/IP网络和图形视窗系统(X Window系统)。此时的Linux还引来了行业的注意,几家小公司开始开发和发布Linux。许多的Linux团体成长起来,1994年开始出现Linux的刊物杂志。

1994的阳春三月,Linux内核1.0版本发布。从此开始,这个内核经历了多个开发周期,每个开发周期都花费了两到三年的时间,并以一个稳定版本而告终,其中涉及到重新设计和重写部分内核,以应付硬件的变化(如USB等新的外围设备连接方式),满足人们不断增长的速度上的需求,尤其是人们将Linux用于越来越大的系统时(或是越来越小的系统:嵌入Linux成为了热门话题)。

从市场和政策角度来看,1.0版本发布后,下一个重大的事件发生在1997年,当时的Netscape公司决定推出它们自己的Web浏览器自由软件(为此还出现了“开源”团队)。这是第一次将自由软件放到时下所有的计算机世界眼前的机会。自那以后,又花了几年的时间,自由软件(或是称为开源)变得广为人知,并成为了许多应用程序的首选。

本专栏与《开放系统世界》共同举办

开放系统世界 月刊

邮发代号: 2-877



就是Linux世界

掌握Linux就是掌握未来。

学习Linux、开发Linux、应用Linux离不开《开放系统世界》。

《开放系统世界》月刊为您搭建走向未来的桥梁。

每期订价: 10元 大16开本128页
全年订价: 120元

订 阅: 全国各地邮局
邮购热线: 010-88558703/9472 传 真: 010-88559493
电子邮件: world@ccu.com.cn 网 址: http://linux.ccidnet.com
地 址: 北京市海淀区紫竹院路66号赛迪大厦14层《开放系统世界》发行部(100044)

对于我们网管来说,共享是再也熟悉不过的。可是,要想自如的解决网络中的各种共享问题,也不是一件容易的事情,小朱是一家中型企业的网管,让我们来看看他都遇到了什么共享问题吧。

解决 共享难题

Windows XP 的共享困惑

■ 新乡医学院网络中心 张鑫旺

前几天,一位同事提出一个问题:他的计算机装的是 Windows XP,他想将自己计算机中的某些文件对他们部门的某些用户共享,结果他们部门的所有用户都能访问!如何解决(我们的网络是基于工作组方式,一个部门在同一个VLAN内)?

我一听,心想:在 Windows 98 中可为共享文件夹设置只读、修改密码,用户不知道密码就无法访问;在 Windows 2000 中更方便、更安全——可对不同的用户设置不同的访问权限,权限也分得更细;Windows XP 号称提供了更高的安全性、更便于用户使用,对如此简单的问题还不是小菜一碟!让我试试。

我找了台安装有 Windows XP Professional 的计算机(为后文叙述方便,假定这台计算机名称为 Share),打开资源管理器,新建一个文件夹 Test,在该文件夹上单击鼠标右键,在弹出菜单中选择“共享和安全”,打开窗口一看,傻了眼:只能设置共享和是否允许修改,而不能针对特定用户设置权限!先试试看。选中“在网络上共享这个文件夹(S)”,单击“确定”。

到别的计算机上,打开“网上邻居”,找到计算机 Share,双击打开,显示出该机所有共享资源,双击 Test,什么都没提示,居然直接打开这个共享文件夹了,和在 Windows 98 下共享时没设密码的情形相同!果真与我的同事说的一样。

怎么办?查找帮助!经过一番摸索,我终于弄明白了是怎么回事!原来,在 Windows XP Professional 中,缺省情况下,系统在对使用本地账户的网络登录进行身份验证时,自动将本地账户的网络登录映射到“来宾”账户,所有用户都被同等对待。对于指定资源,这些用户可以获得相同级别的访问权限,即“只读”或“修改”。所以,在缺省时,就会出现如本文开头所述现象:所有计算机都能访问。

同时,Windows XP 还为我们提供了另一个选择,可以针对同一资源为不同的用户授权不同类型的访问权限,从而对资源访问进行精确控制。在这种模式下,我们共享资源时同在 Windows 2000 下一样,可以对不同的用户随心所欲地设置权限。下面我们来看看如何设置。

首先,依次打开“控制面板”→“管理工具”→“本地安全策略”,将打开图1所示窗口:

如图1所示,选中左侧目录树中“本地策略”下的“安

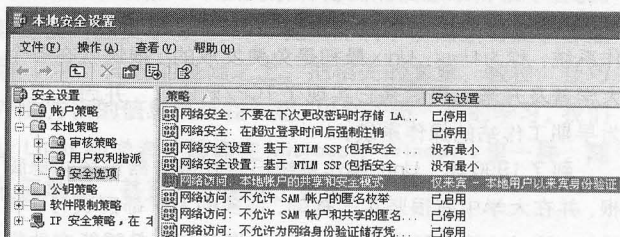


图1 本地安全策略

全选项”,在右侧视图中找到“网络访问:本地账户的共享和安全模式”项,在其上单击右键,在弹出菜单中单击“属性”菜单项,打开如图2所示窗口。

在下拉列表中选择“经典—本地用户作为自身进行验证”,单击“确定”按钮。然后,打开资源管理器,找到前面建立的文件夹 Test,在该文件夹上单击鼠标右键,在弹出菜单中选择“共享和安全”,发现不同了吧!是不是和在 Windows 2000 下共享时的界面一样了?我们可以单击“权限(P)”按钮,选择要将

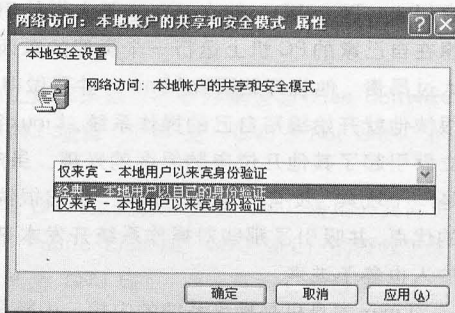


图2 属性

该文件夹共享给哪些用户或用户组,并可赋予其恰当的权限。限于篇幅,在此就不详细说明了。

最后,再试着访问该计算机。到别的计算机上,打开“网上邻居”,找到计算机 Share,双击该计算机图标,将弹出警告窗口。

输入有权限的用户和密码,单击“确定”按钮,即可访问共享资源。否则将拒绝访问。

注意:如要针对不同的用户或用户组指定共享,需在要建立共享文件夹的计算机上根据需要建立相应的用户或用户组,然后在设置共享时为不同的用户或用户组指派相应的权限。这样,当用户从别的计算机上访问该共享资源时,输入您为他设置的用户名和密码,即可访问。

解决 共享难题

小米所在单位的财务室为了更安全的上网,采用了Linux操作系统,并且单独接了一条ADSL上网,不过,财务室有三台机器都要上网,那么如何通过Linux实现共享上网呢?

Linux共享接入的难题

■ 大连 周锋

要实现不使用代理,直接利用Linux共享一条电信的ADSL宽带线让两台或多台计算机访问Internet,我们需要以下条件:

首先,需要为这台Linux服务器配上两块网卡。一块接到宽带的入户线上(网卡为eth0),一块接到内部的交换机或者集线器上(网卡为eth1)。然后查看Linux上安装的pppoe协议软件的版本,命令为:

```
#rpm -qa | grep pppoe
```

需要Linux上安装的pppoe协议软件的版本在3.5-1以上,若低于该版本有可能出现能连接到电信的服务器但是无法访问的情况。若软件包版本较低需要获取新的版本(新的软件包为:rp-pppoe-3.5-3.i386.rpm),使用下面命令升级pppoe软件包。

```
#rpm -Uvh rp-pppoe-3.5-3.i386.rpm
```

接着进行ADSL拨号设置:

```
#adsl-setup
```

输入电信给的ADSL账号,例如:hello@163。确认进行ADSL连接的网卡,输入:eth0。询问是否在不活动时自动挂断,默认是NO。输入DNS服务器的地址,这个可以询问当地的ISP。例如:202.99.8.1。输入ADSL账号的密码。防火墙

不需要设置。

最后会询问是否每次网络启动都自动进行ADSL拨号,选yes。若选no,以后可以使用

```
#adsl-start
```

来启用ADSL连接。若需要每次机器启动时都自动进行ADSL连接可以将adsl-start命令写入/etc/rc.d/rc.local文件中。

连接成功后,我们可以使用ping、lynx等命令来测试连接是否成功。使用ifconfig命令将能看到虚拟的ppp0端口。

由于我们使用的是ADSL进行Internet接入,ISP每次分给我们的IP都不一样。所以要实现内部的机器也能上网我们需要实现IP伪装。在Linux上执行:

```
#iptables -t nat -A POSTROUTING -o ppp0 -j MASQUERADE
```

这个命令告诉Linux对于通过ppp0接口进行路由出去的IP对它的源地址进行伪装,使它可以在Internet上传播。将该句写入/etc/rc.d/rc.local文件中,以后重新启动Linux后将自动实现IP伪装。

至此就完成了共享上网,内部的计算机连接到交换机或者集线器上即可同时访问Internet。

打印机的麻烦

■ 江苏 王寅虎

虽然小米单位的机器大部分是Windows操作系统,但为了安全和稳定着想,有一台服务器使用的是Solaris操作系统,由于没有专用的打印机,所以,一直无法打印,最近单位为一台Windows 2000服务器配了一台打印机,于是,领导让小米想法使Solaris也能用这台打印机,这可让小米犯了难。不过,经过努力,小米终于完成了领导交给的任务。

首先,在Window 2000服务器上安装Unix打印服务(计算机IP: 10.83.104.1,计算机名: PRINTSRV)。

单击开始→控制面板→添加/删除程序→添加与删除Windows组件,选择“其它的网络文件和打印服务”→确定后完成。然后,配置Solaris系统:

1) 编辑hosts文件,添加打印服务器的地址和计算机名:(10.83.104.1, PRINTSRV)

```
# vi /etc/hosts
```

2) 添加打印机

运行命令: # /usr/sadm/admin/bin/printmgr

启动Solaris打印服务管理器,选择Naming Service(命名服务): files,选择“OK”。在菜单上选择“Printer”,选择“Add Access to Printer”(添加对打印机的访问)。

在Printer Name对话框中输入网络打印机的共享名称,如我的是HPLASERJET。在Printer Server对话框中输入打印机的名称(即在/etc/hosts文件中加入的名称)。选项中选中“Default Printer”(缺省打印机)。

最后,使用下列命令测试打印机:

```
# lp -d PRINTSRV filename
```

配置正确的话,Solaris系统就可以打印了。

虽然工作没有几年,但是小朱在工作中也总结了不少共享的小技巧,其中有些技巧还真的不为人所知呢。

解决 共享难题

局域网中的共享“秘密”

■ 江苏 周勇生

工作簿也能共享编辑

大家知道,通过网上邻居窗口可以很轻松地局域网中的多台计算机中,同时共享访问Excel工作簿文件;不过,如果您使用的是Excel XP程序的话,还能按下面的方法来同时共享编辑Excel工作簿文件:

首先运行Excel XP程序,依次执行菜单栏中的“文件”/“打开”命令,在弹出的文件打开窗口中,选中目标Excel工作簿文件;接着单击编辑界面中的“工具”菜单项,从弹出的下拉菜单中执行“共享工作簿”命令,在弹出的设置界面中,将“允许多用户同时编辑,同时允许工作簿合并”选项选中,最后单击“确定”按钮退出设置窗口,返回到主编辑界面。

重新保存该Excel工作簿文件,然后将该文件复制到计算机的某个共享文件夹中,这样其他人就能在各自的工作站中,通过网上邻居窗口打开共享的Excel工作簿文件,并对它进行同时编辑了;编辑完毕后,Excel XP程序会自动对该文档内容进行合并。

移除“共享文档”

在安装Windows XP操作系统的工作站中,通过网上邻居功能,您可以查看到局域网中各台Windows XP计算机中的共享文档内容;如果您不想让其它人看到自己计算机中的共享文档时,可以按下面的方法,来将该默认的系统文件夹删除掉:

依次单击系统桌面中的“开始”/“运行”命令,在弹出的运行对话框中,输入注册表编辑命令“regedit”,在弹出的编辑界面中,用鼠标逐步展开其中的HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\MyComputer\NameSpace\DelegateFolders子键(如图1所示)。

接着从“DelegateFolders”主键下面,将“{59031a47-3f72-44a7-89c5-5595fe6b30ee}”项目选中,再单击一下菜

单栏中的“编辑”/“删除”命令,下面再关闭注册表编辑窗口,重新启动计算机系统,就能使Windows XP计算机中的“共享文档”文件夹隐藏起来了。此时,您再打开网上邻居窗口时,就找不到“共享文档”文件夹的“身影”了。

“通透”隐藏共享

为了确保安全,不少人都将一些重要的共享文件夹隐藏起来,以确保其它人无法通过网上邻居浏览到自己的隐私。不过,对于使用“\$”法(即在文件夹的共享名称后面直接添上“\$”符号)隐藏起来的共享文件夹,您可以利用一种名为Exview的工具,来轻松浏览到它们。不信的话,就来看看Exview工具是如何“通透”局域网中的所有隐藏共享文件夹的吧。

首先将Exview程序从网上下载下来,并按向导提示正确



图2 扫描资源分布

安装好它;再从开始菜单中单击“Exview”命令,打开它的主界面(如图2)。下面单击菜单栏中的“选项”命令,从弹出的下拉菜单中执行“配置”命令,在随后出现的图2窗口中,选中“Custom Modules”标签,并在对应的标签页面中,选中“可选模块”列表框中的“Share Folder”,然后单击“>”按钮,将“Share Folder”模块添加到“已选模块”列表框中,这样您就自定义好了Exview程序的共享文件夹扫描模块,以后您就能使用该自定义的模块,来快速浏览局域网中的所有隐藏共享文件夹了;接着返回到Exview程序的主界面,在其中的“IP从”处输入局域网的开始IP地址,在“到”处输入局域网的结束IP地址,这样就能指定好Exview程序的扫描范围;如果您的局域网中包含的工作站数目太多的话,您还必须在主程序界面的“延迟”文本框中,缩短Exview程序与工作站的连接时间,同时将该程序的工作线程数设置为最大“10”;完成上面的设置后,您可以从主界面的选项列表框中,将“Custom scan”选中,再执行“开始探测”命令,Exview程序就会自动对局域网中的所有工作站进行扫描,同时将扫描到的隐藏共享文件夹【下转第117页】

图1 展开子键

解决共享难题

虽然共享给小米和他的同事们带来了许多的便利,但是不可否认,它带来便利的同时也带来了安全隐患,比如说默认共享,在系统默认状态下,它们是打开的,由此可能会引起一些潜在的安全问题,因此,小米觉得自己有必要关闭它们。

轻松关闭默认共享

■ 江西 吴昱

众所周知,Windows 2000操作系统(包括Windows XP 2003)在安装完成后,会自动创建一些默认的共享资源。这些默认的共享资源包括:

(1) 根目录的共享:就是将计算机硬盘中的所有分区的根目录(如:C:、D:等)自动设为共享,并显示为C\$. D\$等。

(2) 远程管理的共享:就是将Windows 2000的系统目录(也就是Windows 2000的安装目录,如:C:\WINNT等)自动设为共享,并命名为ADMIN\$。

(3) 远程IPC的共享:就是将程序间通讯基础的“命名管道”设为共享,并命名为IPC\$。

由于这些默认的共享是隐含的,所以在“我的电脑”中不会显示出表示“共享”的手形图标,而且在“网上邻居”中也看不到,当然网络用户对它们的访问也是隐藏的。因此,相当一部分用户不知道它们的存在。

通过以下方法查看到这些默认的共享:

(1) 鼠标右键单击“我的电脑”图标,在弹出的右键快捷菜单中单击“管理(G)”菜单。在弹出的“计算机管理”对话框中,依次展开左侧窗口中的“计算机管理(本地)”→“系统工具”→“共享文件夹”→“共享”管理单元,在右侧窗口中就可查看到。

(2) 依次单击“开始”按钮→“程序(P)”→“附件”→“命令提示符”,在弹出的“命令提示符”对话框中直接输入命令“net share”(仅双引号内的文字)也可查看到。

虽然这些默认的共享是Windows为管理系统而设置的,但是它们却像一扇扇敞开的后门供黑客和计算机病毒自由出入。因此为了确保计算机系统的安全,除非有特殊需要,否则应该关闭全部的默认共享。

最直接的关闭方法就是:在“计算机管理”对话框中,用

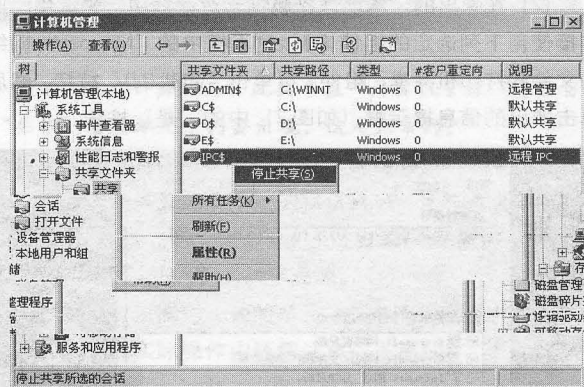


图1 停止共享

【上接第116页】名称全部显示在主界面中,这样您就能知道局域网中的共享资源分布情况了。

快速进入共享文件夹

不少人为了阻止非法用户随意访问自己的共享隐私,往往都会为自己的共享文件夹设置一个访问密码,任何用户只有输入正确的密码才能访问到里面的共享资源。不过如此一来,每次访问朋友的共享文件夹时,也都需要输入密码,这样不但麻烦不说,而且还容易忘记。那有没有办法不要每次手工输入密码,就能快速进入到朋友的共享文件夹呢?答案是肯定的,如果您使用的是Windows XP操作系统,只要您在首次输入一次访问密码,以后系统就能帮您自动记忆密码了;要是您使用的是其它操作系统,可以按照下面的方法来

实现共享文件夹的快速访问:

打开记事本或其它文字编辑程序界面,并在其中输入如下内容:

```
@echo off
net use X: \\111\222 "333" /user:"444"
```

其中“X:”表示共享文件夹要映射成本机的设备名,“111”表示共享计算机名称,“222”表示目标共享文件夹,“333”表示共享文件夹的访问密码,“444”表示访问共享计算机的账号名;接着将上面的代码内容保存为一个扩展名为bat的批处理文件,然后为该批处理文件创建一个快捷方式,并将它的快捷图标拖动到“开始”菜单里的“启动”子菜单中,以后系统每次启动时,就能自动连接到朋友的共享文件夹中,而不需要自己每次输入密码了。■

鼠标右键单击某个共享,在弹出的右键快捷菜单中单击“停止共享(S)”菜单即可(如图1)。这种关闭方法不但操作麻烦,而且只是暂时性的,一旦重启计算机,所有的默认共享又会被 Windows 2000 系统自动地恢复。

经过一段时间的摸索,笔者找到了几种关闭默认共享的简便方法。

方法一:删除“网络组件”法

不知道大家是否注意到,在 Windows 2000 系统中设置“网络连接”的属性时,Windows 会提供一些安装组件(包括协议、服务和客户)供用户选择,这其中就有一个名为“Microsoft 网络的文件和打印机共享”的组件。只要将这个组件删除就能关闭系统的默认共享。具体的操作步骤如下:

(1) 依次单击“开始”按钮→“设置(S)”→“网络和拨号连接(N)”。在弹出的“网络和拨号连接”对话框中,用鼠标右键单击“本地连接”项目,在弹出的右键快捷菜单中单击“属性(R)”菜单。

(2) 在弹出的“本地连接属性”对话框中,先选中“此连接使用下列选定的组件(D)”列表框中的“Microsoft 网络的文件和打印机共享”组件,再单击“卸载(U)”按钮,然后单击弹出的信息提示框(如图2)中的“是”按钮。

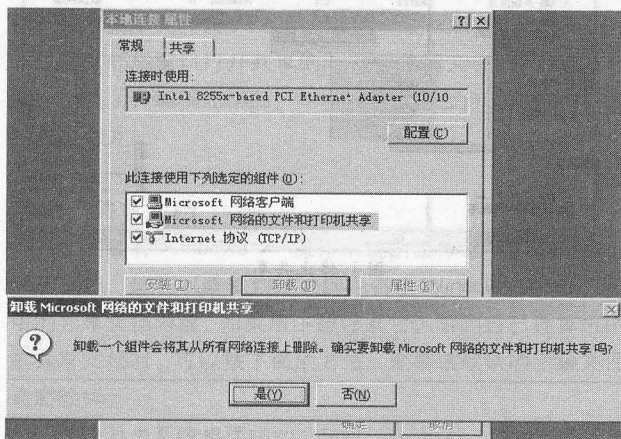


图2 卸载组件

(3) 最后单击“确定”按钮关闭“本地连接属性”对话框即可。

这种方法是将计算机上的“共享”功能彻底地关闭,就连右键快捷菜单中的“共享(H)”菜单都将消失。如此一来,不但计算机中的所有共享(包括系统的默认共享)都将被关闭,而且用户也不能创建自己的共享资源。此时再访问“计算机管理”窗口的“共享”管理单元会弹出错误信息提示框(如图3)。当然,这不妨碍用户通过本机访问网络中其它的共享资源。

“Microsoft 网络的文件和打印机共享”组件在 Windows 9X 系统中同样存在,所以此方法也适用于 Windows 9X 系统。

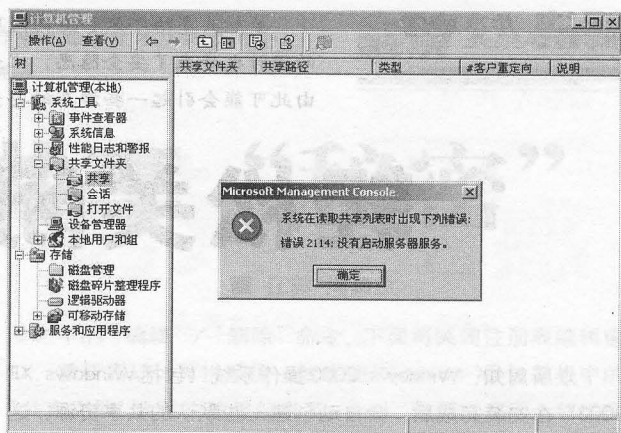


图3 错误提示

方法二:关闭服务法

从 Windows 2000 系统开始,Windows 系统创建了“服务”程序的概念,将系统中的很多管理功能以“服务”程序的形式来实现,因此停止某个服务程序的运行也就等同于关闭了与之对应的管理功能。“共享”功能也不例外,它也有与之对应的服务程序——“Server”服务。只要停止该服务的运行,就能起到关闭“共享”功能的功效。具体的操作步骤如下:

(1) 用鼠标右键单击“我的电脑”图标,在弹出的右键快捷菜单中单击“管理(G)”菜单。在弹出的“计算机管理”对话框的左侧窗口中,单击“服务和应用程序”项目下的“服务”管理单元,在右侧窗口中将列出计算机中已经安装的所有服务程序。

(2) 找到并双击名为“Server”的服务,在弹出的“Server 的属性(本地计算机)”对话框的“常规”选项卡中,将“启动类型(E)”下拉列表框的值选为“已禁用”。

(3) 再单击“服务状态”处的“停止(T)”按钮停止该服务的运行,同时会弹出“停止其它服务”对话框(如图4),提示“Computer Browser”服务也会被关闭是否继续?单击“是”按钮后,Windows 系统将先停止“Computer Browser”服务的运行,再停止“Server”服务的运行。

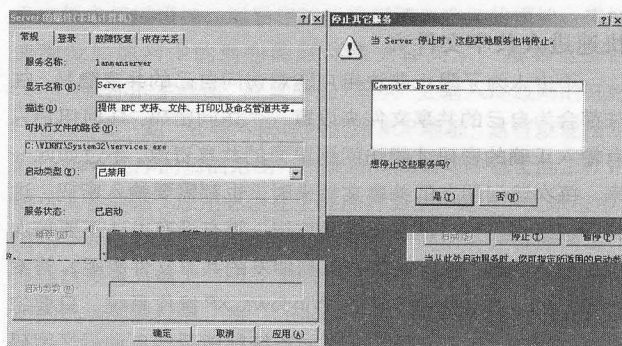


图4 停止服务

(4) 最后单击“确定”按钮关闭“Server的属性(本地计算机)”对话框即可。

重启计算机后,由于“Server”服务被设为“禁用”状态,所以计算机上的所有共享会被删除,而且计算机中的“共享”功能将永远处于关闭状态。其实这种方法的功效与“方法一”的完全相同。

因为 Windows 9X 系统中没有“服务”的概念,所以这种方法不能在 Windows 9X 系统中使用。

方法三:修改注册表法

“方法一”和“方法二”的结果都是彻底关闭系统中的“共享”功能,所以对于一些有特殊要求的用户来说就不实用了。接下来介绍一种既能永久性地关闭系统的默认共享资源,又能保留“共享”功能的方法。具体的操作步骤如下:

(1) 依次单击“开始”按钮→“运行(R)”菜单,在弹出的“运行”对话框的“打开(O)”文本框中输入“regedit”(仅双引号内的文字),然后单击“确定”按钮(或按“Enter”键)。

(2) 在弹出的“注册表编辑器”对话框中,依次展开左侧窗口中的“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters”分支。

①在右侧窗口的空白处单击鼠标右键,在弹出的右键快捷菜单中单击“新建(N)”→“双字节值(D)”菜单,创建一个 REG_DWORD 类型(双字节类型)的数值项,命名为“AutoShareServer”(仅双引号内的文字)。再双击该数值项,将它的“数值数据”置为“0”(如图5)。这样就能关闭诸如

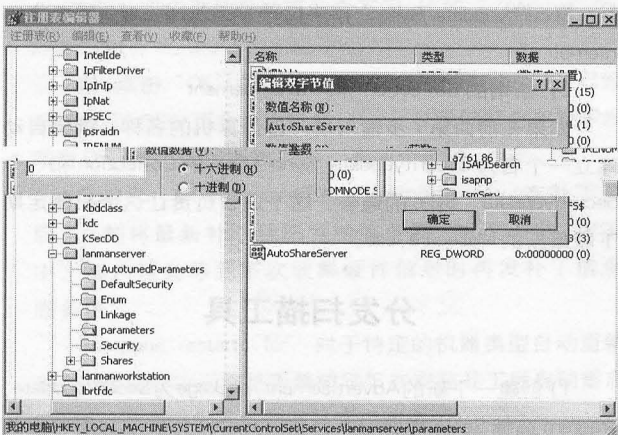


图5 关闭根目录共享

C\$, D\$ 一类的根目录的共享。

②同理,再创建一个名为“AutoShareWks”的 REG_DWORD 类型的数值项,将它的“数值数据”也置为“0”。这样就能关闭 ADMIN\$ 共享。

③如果以上两个数值项已经存在,则只要双击它们,更改“数值数据”中的值即可。

提示:重启计算机后,上述两类共享在“计算机管理”对

话窗的“共享”管理单元中不会再出现。

(3) 在“注册表编辑器”对话框的左侧窗口中,再依次展开“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa”分支,在右边窗口中,双击名为“restrictanonymous”的数值项,将它的“数值数据”置为“1”(如图6)。这样就能关闭 IPC\$ 共享。

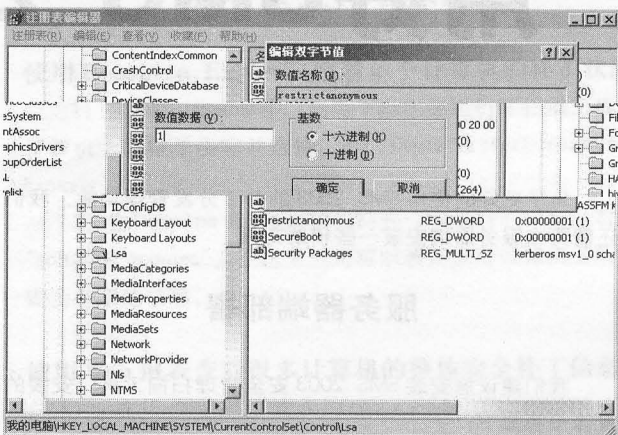


图6 关闭 IPC\$ 共享

提示:重启计算机后,此共享在“计算机管理”对话框的“共享”管理单元中仍会出现,这是正常的。

(4) 以上设置完成后,重启计算机即可。

这种方法只是关闭了系统的默认共享,计算机上的“共享”功能仍然有效,用户依旧可以通过右键快捷菜单中的“共享(H)”菜单来创建自己的共享资源。

上述三种方法操作比较简单,功效各有千秋,大家可以按需选用。但在实际操作中还需注意以下事项:

(1) 在“方法一”中,如果只是取消“Microsoft 网络的文件和打印机共享”复选框(即:清除其左边方框中的“√”),“共享”功能仍旧有效。所以必须“卸载”(也就是“删除”)该组件。

(2) 在“方法三”中,由于 IPC\$ 共享是为了让进程间通信而开放的命名管道,通过提供可信任的用户名和口令,连接双方可以建立安全的通道并以此通道进行加密数据的交换,从而实现远程计算机的访问,因此每次计算机启动时都会自动重建此共享。也就是说,IPC\$ 共享无法彻底关闭,将“restrictanonymous”的“数值数据”置“1”只是防止其它匿名用户访问 IPC\$ 共享。

(3) 由于“方法三”是对系统的注册表进行修改,而“注册表”又是 Windows 系统的核心文件,因此强烈建议用户:在操作“注册表”前一定要先备份,以备系统异常时恢复所用。

(4) 使用“方法三”后,如果 ADMIN\$ 共享或 C\$, D\$ 类的共享仍旧出现,就需要考虑系统是否感染了病毒?此时最好是先用防病毒软件对计算机进行全面的查/杀病毒,再进一步判断、处理。INI

在2004年第十期的《网管员世界》杂志上,我们介绍了用SMS进行局域网补丁自动分发的文章,在读者当中引起了不小的反响,有许多读者来信咨询SMS补丁分发管理的情况,为此我们特别组织了这篇SMS补丁管理的文章,希望能够解决您在使用SMS中遇到的一些问题。

用好SMS 2003补丁分发

■ 上海 翟惊卿

为了更好的使用SMS 2003的补丁分发管理功能,我们还需要在服务器端安装一些辅助工具。

服务器端部署

我们建议您安装SMS 2003安全管理扫描工具,安装的具体步骤如下:

1) 下载SMS 2003安全管理扫描工具并解压缩到一个临时目录(下载地址: <http://www.microsoft.com/smsserver/downloads/2003/featurepacks/suspack/default.asp>)

2) 解压缩后,会产生六个文件,在SMS服务器上运行其中的SecurityPatch_ENU.exe。

3) 选择接受协议,进入下一页,输入安装路径,默认为C:\Program Files\SecurityPatch。

4) 进入“Scan Tool Download”。

如果SMS服务器能够连接Internet,点击“Download”,SMS会自动下载最新的补丁列表文件Mssecure.cab。

如果SMS服务器不能连接Internet,可以到以下地址手工下载Mssecure.cab: <http://go.microsoft.com/fwlink/?LinkId=23190>,并拷贝至C:\Program Files\SecurityPatch\PkgSource\1033。

5) 点击“next”开始安装。

6) 进入到“Distribution Settings”页面,输入一个好记的Package名称,我们这里填入“Securityupdate”。按需要勾选下列复选框: Create Collection, Create Advertisement, Assign Package to all Distribution Points。

其中, Create Collection和Create Advertisement会将安全补丁扫描工具发给一台您指定的客户端机器,主要用于测试目的,在生产环境中不用选。

7) 点击“OK”进入“Database Updates”页面,在这里指定一台用于定期自动更新安全补丁列表文件Mssecure.cab的机器,这台电脑必须是SMS客户端。

说明:

建议这台机器最好有直接公网连接。

如果没有机器可以连接公网,可以定期手工从<http://>

go.microsoft.com/fwlink/?LinkId=23190下载最新的Mssecure.cab并复制到C:\Program Files\SecurityPatch\PkgSource\1033。同时按以下方法设置定期自动更新DP。

a) 在SMS Console中,选择“Securityupdate Package”。

b) 右键选择“Properties”

c) 点击“Data Source”,选择“Update Distribution Points on a schedule”。默认是每天一次。

8) 完成安装。

安装好以后,进入SMS管理台会有如下变化:

1) 出现一个新建的Package: Securityupdate,它包含三个程序:

Securityupdate: 在客户端扫描安全补丁安装情况,在下次硬件信息收集的时候把数据从客户端发给服务器。

Securityupdate (expedited): 在客户端扫描安全补丁安装情况后,立即把数据发给服务器,但会增加网络负荷。

Securityupdate Sync: 用于同步Mssecure.cab,需要连接Internet。

2) 新增的Collection和Advertisement

如果在前面第7步输入了一台计算机的名称,就会自动建立一个名为Securityupdate Sync Host的Collection和一个Securityupdate Sync的通告,这个通告负责让这台机器定期下载最新的Mssecure.cab。

分发扫描工具

1) 创建一个新的Advertisement, package为Securityupdate, program选择Securityupdate (expedited), 分发给您所希望的Collection, Schedule可以设置为As soon as possible+每7天一次。

2) 等候一段时间,察看Advertisement Status,确认客户端已经成功运行完这个通告。

使用向导分发补丁

注意: 在大规模发布补丁之前,必须先进行充分的测试,

以确保补丁安装不会影响现有系统。

1) 在 SMS Console 中, 右键点击 Collection → All tasks → Distribute Software Update, 在下拉框中选择 "MBSA"。

注意: 如果这里不能选, 一般是因为客户端的补丁状况信息还没有收集上来。

2) 选择 "new" 来新建一个安全补丁分发。

注意: 如果您以前运行过这个向导, 可以在这里选择修改以前建立的安全补丁分发。

3) 在下一页中输入分发包的名称。在这里可以把您的安全补丁政策写入到一个 rtf 文件中, 再点击 "import" 导入。这部分信息会在客户端安装安全补丁时显示在客户端。

4) 选择 Securityupdate package 和 Securityupdate program。下一页会显示出所有客户端需要打的安全补丁。

注意: SMS 补丁管理主要侧重在重要安全补丁, 运行机制与 Windows update 不同, 所以这里看到的待装补丁列表可能与 Windows update 中看到的不同。

另外, 同一个安全补丁可能会由于系统版本或语言的不同而有多个, 您需要将它们全部都选上。

5) 您可以选择自动或者手动下载补丁, 但目前中文补丁还不能自动下载, 需要手工下载然后再导入。下一页显示您选择的安全补丁包。注意这时 "ready" 为 "no"。逐个选择这些安全补丁包, 点击 "properties" 按钮。您可以在新窗口中点击 "Import" 导入补丁安装程序, 然后点击 Name 旁边的 Information 按钮上网查看这个补丁的安装参数, 填入 "parameters" 框。目前微软补丁安装程序的参数尚未完全规范化, 不同补丁安装参数可能会不同, 比如 "/passive /quiet /norestart"、"/q /z"。

6) 点击 "OK" 关闭此窗口后, 注意到 "ready" 已经显示 "yes"。下一页会让您选择 DP。一般我们都会把补丁发到所有 DP。下一页配置客户端, 有两个选项:

Collect Client Inventory immediately: 在补丁装好后, 立刻将最新补丁状态发给服务器。建议选中。如不选中, 客户端会等到下次收集硬件信息时再发补丁信息给服务器。

Postpone restarts for: 对于特定的机器类型自动重新启动。该选项取决于您是否希望 SMS 在安装补丁后自动重启计算机 (不管是服务器类型还是客户端类型)。

注意: 这项配置主要考虑重启是否会影响客户端正常工作, 但大部分安全补丁必须重启才能生效。

Perform unattended installation of software updates: 即无人参与安装, 终端用户不会得到任何提示。Countdown: 设置倒计时框的时间。下一页设置是否允许终端用户推迟安全补丁的安装。建立一个通告并选择具体发给哪个 collection。

注意: SMS 客户端在安装安全补丁时会再次检查自身的

安全补丁状态, 确保不会装上不兼容的补丁或重复安装, 因此, 假设我们把一个 Windows 2000 的补丁分发给不同操作系统, 也只有 Windows 2000 的系统才会安装, Windows XP, Windows 2003 并不会装。

最后, 完成向导。

察看安全补丁状态

使用 Resource Explorer 察看单个计算机的补丁状态

1) 在 SMS console 中, 选择一台已经运行了扫描工具的计算机, 右键单击它并选择 "all tasks → start resource Explorer"。

2) 在 Resource Explorer 中, 打开 "hardware", 可以看到 "software updates"。在这里, 您可以看到这台计算机上所有安全补丁的信息。

使用 Web 报表查看很多计算机的整体安全补丁信息

1) 在 IE 浏览器中输入 http://SMSServerName/SMSReporting_XXX。这里 XXX 代表您的 Site Code。

2) 在左边的树状列表中, 选择 "Software updates Compliance → Compliance by product"。

3) 可以选择产品, 也可以直接点击 "display" 显示所有产品的安全补丁信息。这个报表中会显示安全补丁安装的整体情况: 有多少台计算机已经安装, 有多少台计算机还没有安装等等。

4) 如果要察看某个特定的安全补丁有哪些电脑还没安装, 可以查看 "Software updates Compliance → Computers where a specific software update is applicable"。Applicable 就是指应该安装但是没有安装。

补丁管理工作流程

为了更好的进行补丁管理, 我们建议:

1) 在 http://www.microsoft.com/security/security_bulletins/alerts2.asp 订阅安全公告的电子邮件通知。

2) 定期查阅最新的安全公告。

3) 如果 SMS 服务器不能连接 Internet, 需要定期下载最新的安全补丁列表并复制到 SMS 服务器上。

4) 当有新的安全公告发布后, 评估它对企业内部环境的影响并决定是否安装该安全补丁。

5) 若决定安装该安全补丁, 下载该安全补丁 (若该补丁对不同的操作系统有不同的文件, 则不同操作系统的补丁都要下载) 并先往测试实验室中的计算机上部署。

6) 该安全补丁通过测试后, 正式部署到企业中所有计算机。

7) 检查安全补丁分发结果, 定期生成报表。

谈谈“同步”应用

■ 北京 王书琴

Windows 中的“同步管理器”可以把保存在计算机中的脱机网页文件与网络中相应的网页内容进行比较并自动更新,使两者始终保持一致,并可让同一局域网内的不同计算机中的数据文件同步更新,还可以使计算机的系统时钟与 Internet 时间服务器的时钟保持一致。因此,“同步管理器”使我们对脱机网页的及时更新以及文件(夹)之间的比较、复制、粘贴等操作变得异常简单,更是了解最新时事动态、备份、更新文件的极好途径。下面,就让我们来看看“同步管理器”的有关应用问题(以 Windows XP 为例)。

脱机网页的同步

经同步后的脱机网页文件,当您重新连接到 Internet 网络上时,系统就将对这些脱机网页文件自动进行检查并更新,使您在脱机状态下浏览到的网页内容永远保持最新状态。

要使脱机网页文件与源网页内容保持同步,首先要让计算机系统能够使用脱机文件。但是,在默认状态下,我们登录系统所用的“账户”处于一种“快速用户切换”状态,此时我们是无法在系统中使用脱机文件的。因此,首先要修改账户为“非快速用户切换”状态,方法是:进入“控制面板”,点击“用户账户”图标,再点击“更改用户登录或注销的方式”,在“选择登录或注销选项”窗口中去掉“使用快速用户切换”复选框中的勾,再点击“应用选项”按钮即可。

使脱机网页文件与网络中源网页的内容保持同步的设置步骤为:

1、设置计算机以便使用脱机文件:在“我的电脑”窗口中依次点击“工具”→“文件夹选项”,并在“文件夹选项”对话框中切换到“脱机文件”选项卡,然后勾选“启用脱机文件”复选框。如果勾选了“注销前同步所有脱机文件”,那么就是使用“完全同步”方式,“完全同步”可以确保每个脱机网页文件在注销时仍能保持最新性。如果没有勾选此项,那么只是使用了“快速同步”方式,“快速同步”只能确保脱机网页文件的完整性,但却不一定是最新的。

2、选择需要脱机浏览的网页:要使某个网页可以脱机浏览,可以将该网页存放到“收藏夹”中,如要将“新浪首页”添加到“收藏夹”中,可以先登录到“新浪首页”,并点击 IE

工具栏中的“收藏夹”按钮,再在左边的“收藏夹”栏中点击“添加”按钮,最后在“添加到收藏夹”对话框中勾选“允许脱机使用”复选框即可。

3、安排要同步的脱机项目:在“我的电脑”的“工具”菜单中点击“同步”选项,并在“要同步的项目”对话框中点击“设置”按钮,然后切换到“计划”选项卡,再点击“添加”按钮即可启动“同步计划向导”来创建同步计划。在创建“脱机网页同步项目”时您要在“为该同步选择网络连接”列表中选择您的网络连接名称,同时最好勾选“如果在计划好的同步开始时计算机还没有连接上,请自动连接”复选框,另外还要指定同步任务开始的日期与时间。

至此,“新浪首页”已被设置成了同步的脱机网页。但是,为了能够使脱机网页能够在登录或注销计算机、计算机闲置状态时自动保持与网络同步,我们应该进一步地设置。首先,在“同步设置”对话框的“登录/注销”选项卡中选择需同步的脱机网页,并勾选“登录计算机时”、“从计算机注销时”两个复选框。这样就能使该脱机网页在登录或注销计算机时保持与网络中源网页的同步。另外,如果要求“同步管理器”在自动同步脱机项目前提示选择许可权限,那么还可以勾选“同步项目之前发出提示”复选框。

而要在计算机处于闲置状态时使脱机网页文件仍能同步更新的话,那么只要在“同步设置”对话框的“空闲状态”选项卡中勾选“在计算机空闲时同步所选项目”复选框。此外,还可点击“高级”按钮来控制计算机闲置时自动运行同步功能的触发机制,包括设置同步的启动时间、两次同步间的时间间隔等。

文件(夹)的同步

如果您经常要在两台计算机之间或是使用移动存储设备来传输文件的话,那么,使用“同步+公文包”组合方式将成为最佳途径。因为“公文包”能自动将主计算机上的文件更新为修改后的版本,而不必将修改后的文件移出“公文包”,或者删除主计算机中现有的副本文件;而“同步”将使这所有的步骤显得更为简单。下面,以台式机与便携机之间文件同步为例来说明具体的操作步骤。

1、创建公文包:将便携机通过局域网或直接电缆连线连接到主计算机上,然后在便携机的“我的电脑”中依次点击“文件”→“新建”→“公文包”,并为其重【下转第 123 页】

小试脱机服务

■ 北京 李文龙

近期公司接到一个新的开发项目。由于工程比较大,时间又紧迫,所以加班加点在所难免。起初同事们都任劳任怨,可临近“5.1”时,有些同事就开始抱怨起来。因为项目至今才开发了三分之一,按照此进度,想过节逍遥一下的计划就要泡汤了,为此他们专门找过公司的高层。但结果可想而知,公司以利当头,驳回了他们延期项目的要求。不过最后加了一句:如果有不耽误项目开发进程,又可以逍遥过节的两全其美的方法,公司可以考虑。这一句话给大家带来了希望,可前提是到底有没有这种方法呢?公司的(兼职)网管小李给出了肯定的答案:“我们可以通过 Windows 2000/XP 的脱机服务来实现。”听到这一喜讯,同事们迫不及待地要求小李演示一下,以便将此方案早日提交给老板。

按照事先的设想,小李在开发工程的服务器上用 Administrator 身份登录,新建了一个共享文件夹 TJJ, 将小陶研发的模块(文件)归类到此文件夹中。接着打开该文件夹属性的“共享”选项卡,并单击其中的“缓存”,出现“缓存设置”对话框,选中“允许在这个共享文件夹中缓存文件”。

然后,小李把小陶的笔记本电脑连上服务器,开机进入资源管理器,在“工具”菜单中单击“文件夹选项”,在出现的对话框中单击“脱机文件”按钮,引出了“脱机文件”选项,选中“启用脱机文件”,并根据实际情况对脱机文件选项进行配置完成后打开“网上邻居”找到先前服务器共享出来的文件夹 TJJ,右击它,在右键菜单中选择“允许脱机使用”,弹出“脱机文件向导”对话框。

操作到这,小李抬起头对同事们说:“在这里我们可以根

据实际需要选择是否在“登录和注销时自动同步处理脱机文件”、是否“启用提醒程序”(建议选上)、是否“允许文件夹的子文件夹脱机使用”(必须选上)。另外建议在桌面上创建脱机文件夹的快捷方式,这样会带给我们使用上的便捷。”

“那么怎样使用这脱机文件呢?”站在一旁的小陶有点急不可耐了。小李道:“别急,下面我就演示给你们看。”

小李拔下笔记本电脑的网线,断开网络连接,这时任务栏右侧出现了脱机文件图标,并提示开始脱机工作。小李双击打开桌面上的 TJJ 脱机文件夹对小陶说:“现在你可以对其中的模块进行操作了。”小陶打开一个模块文件,输入一段代码,保存后道:“可以了,但怎么将修改后的文件上传到服务器呢?”

这次小李没有说话,用实际行动回答了他。他将笔记本电脑重新连上了服务器,单击任务栏中脱机文件图标,在弹出的“脱机文件状态”对话框中,点击确定,出现了“正在与文件服务器同步”的信息框,等传输结束后。小李对小陶说:“现在你登录到服务器看看,那里的文件是不是被更新了?”

“真的,文件已经更新了,这项功能太神奇了。”小陶兴奋的叫道。周围的同事也开始欢呼雀跃起来。看着同事高兴的样子,小李只是笑了笑,因为他知道这项功能并没有同事们说得这么神奇,它的运作原理和以前的公文包基本相同,只不过这次用在了刀刃上罢了。

最后上报老板的结果是皆大欢喜。同事们可以外出逍遥过节,而老板也可以节省一笔不小的加班费,至于小李,他只不过在当晚提前赴约,与女友“交流思想”了。■

【上接第 122 页】命名。将需要在便捷中处理的文件(夹)从主计算机中复制到便携机的“公文包”中。

2、在便携机中处理文件。

3、再次将便携机连接到主计算机上(如果两者已断开),打开便携机上的“公文包”后,如果要更新所有文件,则在“公文包”菜单中点击“全部更新”项;而如果只需更新部分文件,那么就选择需要更新的文件,然后在“公文包”菜单中点击“更新所选内容”项。

这样,主计算机中的有关文件已被更新。这种主计算机与便携机之间的文件(夹)同步方法同样适用于局域网中不同计算机之间的文件(夹)的同步,这就使文件(夹)的备份工作有了一种全新的“武器”,也使数据安全有了更好的保障。

时间的同步

无论您如何调整,计算机的时间总会在一段时间后与标准时间“差之毫厘”,甚至“谬以千里”。但是,如果您启用了“时间同步”功能,那么您的计算机系统时间就始终能与 Internet 时间服务器保持同步。

要启用“时间同步”,以便让计算机系统时间始终与 Internet 时间服务器的时钟保持一致,可以按以下步骤操作:双击“任务栏”中的时间图标以打开“日期和时间属性”对话框,切换到“Internet 时间”选项卡,勾选“自动与 Internet 时间服务器同步”复选框,并在“服务器”列表中选择“时间服务器”,再点击“立即更新”按钮即可使本机时间与 Internet 时间服务器时钟保持一致。■

给打印开一个“可视化窗口”

■ 北京 陈志清

网络打印是一项伴随Internet走向深化而衍生出来的一种快速、高效的打印方式,随着网络打印机产品的不断丰富和价格的不断降低,现在已有不少企业选择了网络打印机。不过,从目前来看,虽然有些企业已经购买了高性能的网络打印机,但在应用网络打印时却没有真正发挥其优势,其中一个很关键的因素是用户没有应用好与网络打印相结合的管理软件。比如,一些企业只是把网络打印机作为单机使用,或者依然采用传统的共享打印方式使用,这在很大程度上“抹杀”了网络打印能提高设备使用效率、打印速度和质量、提供个性化的打印以及降低整体拥有成本方面的一系列优势,而这一系列优势的切实体现主要依赖于网络打印的良好管理。毫不夸张地说,管理就是网络打印的核心,它像一个神经系统一样支配着网络打印的运行。这是笔者在使用了网络管理软件后的一些亲身体会,在和大家分享的同时,希望其它一些网管员能从中发现一些更多更好的功能。

由于我们公司所使用的机器是惠普的网络打印机,因此,我想与大家分享的是HP Web JetAdmin的功能体验,客观地说,基于惠普在网络打印市场的地位,最常见也是应用最多的就是惠普的Web JetAdmin了,用户可以从HP网站免费下载到该软件。据了解,使用Web JetAdmin可以通过Internet浏览器界面,从世界上任何能够访问企业Intranet的地方,远程安装和配置HP网络打印机、发现HP网络扫描仪、CD-ROM服务器和任何厂商的、兼容标准打印机MIB的设备,并监视它们的状态,查看网络中打印机、批量升级打印机或打印服务器的配置、分组管理打印机等各组任务。这就好像给打印工作开了一个“可视化的窗口”,让网管员可以轻松地完成设置打印机和排除故障等工作。由于我们公司的规模有限,到目前为止,应用最多的还只是打印故障的发现和排除问题,下面也就主要针对此功能和与大家进行分享。

为打印设置权限

众所周知,我们在使用传统打印机时,一般只能被动地等待打印,如果想打印一些比较紧急的文件,也不得不等前面的打印工作完成以后才能处理。而且在打印机遇到故障或要取消一些打印工作时,就必须到连接打印机的PC上进行相应的操作,这对那些需要管理多台打印机的网管员来说,也是一项繁重的工作。为了帮助网管员更好地管理打印工作,HP Web JetAdmin提供两个配置文件,网络管理员通过配置文件可以查看和配置打印机。因此,我为公司的不同部门设置了打印权限,如业务部的员工只能打印而不能更改打印设

置,并且使用配置文件来隐藏一些不想要他们看见的产品功能。在对打印权限等进行设置后,自己就可以很好地控制和管理打印机,避免不必要的负累,从而为自己的工作带来了方便。

在自己的电脑上“监控”打印

在日常的办公打印当中,经常出现打印机故障或碳粉、纸张用尽的情况,但员工们却浑然不知,继续浪费时间打印,相信大家都会遇到这类的问题。而在使用了网络管理软件后,如打印机碳粉、纸张即将用尽等信息,便尽在自己的“监视”之下了。这些信息不仅网管员自己能看到,同时也可以通过打印机内嵌的打印机网页服务器将把打印机的状态用网页的形式提供给公司的所有同事,这样可以提醒大家在碳粉和纸张即将用尽的时候及时更换和添加。

以上功能便是网络管理软件的智能报警功能,它能在打印机出现问题时提供快速响应,对此,网管员可以通过HP Web JetAdmin进行设置。而且这一响应可以发送给指定的地址,如可以指定某一名员工(我们公司专门指定了一名行政人员)专门负责更换硒鼓等耗材,或者将信息直接发给供应商,以便在打印机的墨粉等用完时把警报消息发送给负责人,提醒他及时更新,这样网管员便不再为更换耗材这类小事烦心了。

另外,对卡纸、内存不足等信息,也都可以通过管理软件设置智能报警。但有时候,仅仅依靠控制面板或测试页提供的一些提示信息并不能帮助管理员顺利排除故障,这时,HP Web JetAdmin的全面诊断功能便显示出了优势。我们公司的机器有时候会出现设备显示问题或连续卡纸,这就意味着设备需要预防性维护,借助诊断功能就可以清楚地了解故障出现的原因,并尽早排除,以避免一些大的问题发生。

打印机遇到的故障往往是多种多样的,在无法判断时,也可以通过查看打印历史作业的方式进行逐个排除,HP Web JetAdmin便为管理员提供了这项功能,它可以全程跟踪打印作业进程,当用户发送作业给打印机,但作业不打印时,通过查看打印作业历史,就很清楚地知道该作业是否已经到达打印机,这样便于网管员对故障的确定和及时排除。

以上只是管理软件如何来帮助网管员解决打印问题的一部分功能,它极大地减少了管理人员用于处理网络中打印相关问题的时间,直接降低了企业网络的管理成本,并且简化维护、操作。除此之外,也可以通过它进行打印成本的管理和控制等,致力于企业的进一步发展。■

谁说没有“后悔药”？

——系统还原工具专题

■ 重庆 冷寒生

常听人说“要是有了‘后悔药’就好了”，呵呵，现实生活中是没有啦，可在信息时代却不是做不到的，我们称之为“系统还原”。通常计算机用户在出现重大误操作、数据丢失的时候才会想到它，可是作为网管员，系统还原就如它的同胞兄弟“系统备份”一样，是日常工作内容之一。不是常说“工欲善其事，必先利其器”吗？在我们进行还原操作时，还原工具软件是少不了的，它让您工作中的难题迎刃而解，今天小生就这方面的软件给大家作个盘点推荐，希望对广大网管同行的工作能有些帮助！

魔镜还原

最新版本：V1.7

适用平台：Windows 9x/NT/2000/XP

软件授权：免费版

软件大小：4.52MB

下载地址：[http://sd-http.skycn.net:8180/down/](http://sd-http.skycn.net:8180/down/MagicRes.exe)

MagicRes.exe

这是由新海科技出品的一款还原工具，在操作上跟Ghost非常类似，它同样也是Windows窗口和DOS双操作模式。软件安装完成并重启后“魔镜还原”会出现在启动菜单里，以便我们系统不能正常启动时可以进行DOS操作。如图所示，软件安装好之后不会马上对系统进行监视，还要安装启动程序，

在安装启动程序的窗口中，提供了各种模式的选项，使其可以适合任何操作系统。

软件操作步骤也是极其简单的，在备份系统里选好“备份原盘”和“目标盘”之后，点“开始备份”就OK了。在高级选项里可以为DOS下的恢复操作配置4个实用的工具，比如KV3000 DOS版等。另外在恢复时，从哪个盘做的备份，只能恢复到那个盘，不然会有一些不可预知的错误发生。软件没有提供即时操作监视的功能，也就是不能自动创建还原点。此软件可以为操作者设置使用权限。■



“实用之星”(RestoreIT)

最新版本：V3.0 个人版

适用平台：Windows 9x/NT/2000/ME

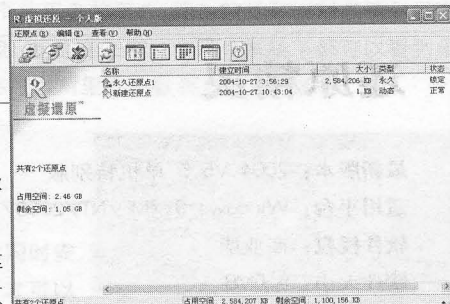
软件授权：共享版

软件大小：17.6MB

下载地址：<http://software.tech.tom.com/SoftInfoDisplay.php?id=6500#>

“实用之星”虚拟还原其DOS操作模式是随Windows下安装时一起装载的，在DOS下启动管理界面需按空格键并输入密码才能进入（默认为空，三次错误会被锁定），在DOS下初次创建还原点的速度大约为300M每分钟。其工作原理就是在某一磁盘分区上建立一虚拟分区，用来存放需备份驱动器

的资料，我们称其为“还原点”；核心功能就是建立“永久还原点”和“动态还原点”。由于软件采用递增的方式，使其创建的动态还原点不会大量占用磁盘空间。创建还原点的操作分自动和手动两种，不提供单个文件及操作步骤的跟踪功能。另外软件附带一个紧急救援盘制作程序，制作好了之后在DOS下由A盘启动，运行其中的程序：A:\VBTOOLS.EXE就可以用它来恢复硬盘的主引导记录，恢复文件，修复及卸载“虚拟还原”程序。此软件同样可以设定操作者的权限。■



着迷守护神—系统再生

最新版本: Build 2001.07.31

适用平台: Windows 9x/ME

软件授权: 共享版

软件大小: 3120KB

下载地址: <http://xbol-http.skycn.net:8180/download/PchoClone.zip>

这款软件操作一目了然, 就算您从没接触过这方面的软件也可以快速上手。其备份与恢复都可以具体到某个单一的文件上! 惟一感到遗憾的就是软件删除不够智能, 不能同时删除原

始备份文件, 需进入受过监视的驱动器里手动删除。

软件安装完成后在程序组里就清楚地列出4个操作选项: 定期备份、文件恢复、系统应急盘和原始备份。使用之初首先要先选择“原始备份”建立初始还原点, 可以选择多个驱动器, 也可以对每个驱动器里的文件进行筛选备份(系统盘是默认选中状态)。设置完成即开始初始备份, 其备份压缩比约为1/2。注意备份的分区一定要是由Fdisk分出来的, 否则可能无法恢复。其建立备份文件的过程很快, 备份文件以*.zlb的文件形式隐藏存储。



Norton GoBack

最新版本: v4.0 Final 正式版

适用平台: Windows 9x/NT/2000/XP

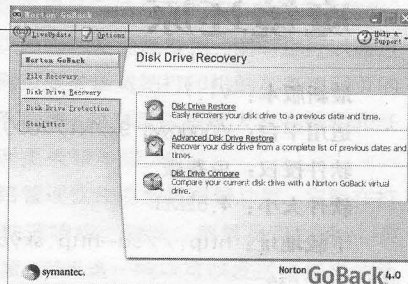
软件授权: 零售版

软件大小: 3672KB

Norton防火墙、Norton杀毒软件都太熟悉不过了, 而这一款名为Norton GoBack的还原工具同样出色。Norton GoBack分“文件恢复”、“磁盘恢复”和“磁盘保护”三类工具, 其“文件恢复”和“磁盘恢复”功能可记录下您自开机以来所有的窗口操作及程序运行情况, 包括重启时在DOS状态运行过的程序。GoBack会每隔一定的时间自动创建一个还原点, 时刻保证可以恢复到最近的一次操作时间。

另外其磁盘保护功能是此款软件的一大亮点, 在软件主界面的“Disk Drive Protection”选项中, 提供了两种模式:

1. Safe Try Mode (交互模式), 此功能跟“完美卸载”差不多, 它会监视您机器中一些软件的安装, 网络下载等操作, 而且具有一定的选择性; 2. AutoBack Mode (自动模式), 默认每5分钟创建一个恢复点, 也提供了自由恢复时间设定, 自动模式恢复的是上一次监视状态下您对硬盘的所有读取操作。



还原精灵

最新版本: 2004 V5.5 单机特别版

适用平台: Windows 9x/ME/NT/2000/XP

软件授权: 商业版

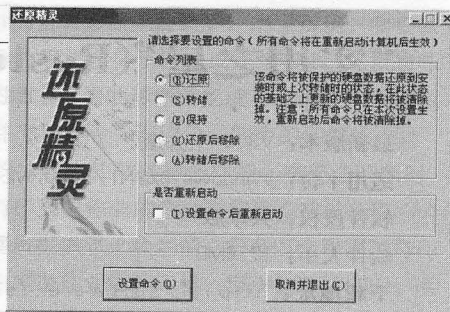
软件大小: 5.6MB

下载地址: <http://sc.cnzz.com/vvd/soft15/Hyj155.rar>

这款软件相信大家不陌生吧, 这是大多网吧、机房普遍安装并被代替硬件还原卡而使用的一款软件, 它还可以配合“还原精灵伴侣”使用, 能够最大限度地保证系统的安全。其实现原理就是把用户对受到保护的磁盘数据的操作, 由还原精灵分为了“真实操作”跟“虚拟操作”两种, 在没有安装此软件或未启动保护时, 我们对电脑进行的操作属于真实的

操作, 安装了还原精灵或是启动了保护后, 对电脑的操作理论上就成了虚拟的操作, 还原精灵可以随时删除或保

存这些操作。由于这个特性, 使得此软件系统资源占用极少, 不影响我们正常使用硬盘。它提供的还原方式有手动、自动、定时和资料转储; 它可以恢复COMS, 防止硬盘I/O (输入/输出) 遭到破坏; 另外系统不能启动时可以在重启后按Home或Ctrl+Home键进DOS设置界面进行恢复, 其默认管理密码为12345678。



PowerQuest SecondChance

最新版本: V2.01

适用平台: Windows 9x/NT/2000

软件大小: 2380KB

软件授权: 共享软件

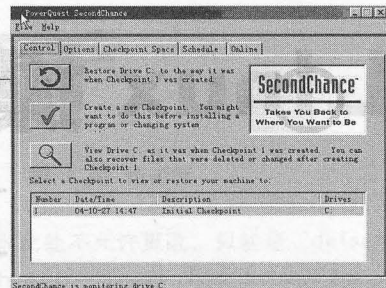
下载地址: <http://ftp7.enet.com.cn/pub/system/syssafe/sc2demo.zip>

由于安装/卸载的软件太多,造成硬盘中有许多垃圾文件,久而久之系统运行速度逐渐变慢甚至崩溃,PowerQuest的SecondChance可省却您的烦恼,恢复机器到某一时间点的状态。安装中它会提示:选择需监视的驱动器(最好是选中“全部”);安装完毕会提示:创建救援盘(强烈要求创建)。安装完成后会在所有受监视的驱动器下建立“Pqsc”文件夹,存放改动日志。这款软件提供的是一种映象方式而不是实际存

储文件方式,类似于“还原精灵”的“实际操作”和“虚拟操作”,所以不用太担心硬盘空间问题。不爽的是:

备份选项不提供单个文件的备份功能,只能选择整个驱动器,还有它只提供了以星期几为计数的定时备份功能。

其一般操作流程为:点击“Create a new Checkpoint”(创建新的还原点),并为还原点命名;在下面框里就创建了编号为1的C盘还原点;然后在C盘上安装某个软件后再点View Drive C按钮,可以看到C盘的一切改变都清楚地记录在这里,其中绿色的表示新增的文件,蓝色表示修改过的文件,这个颜色的标注十分省心;最后点击“Restore Drive C”按钮,就可以恢复到安装前的样子了! **■**



Pro Magic

最新版本: V6.0

适用平台: Windows 9x/NT/2000/XP

软件授权: 试用版

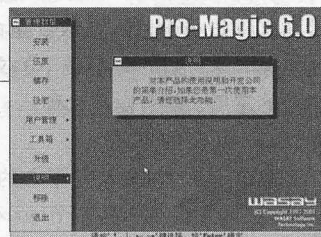
软件大小: 1308KB

下载地址: <http://xbol-http.skycn.net:8180/download/ProMagic.exe>

这是由瓦瑟科技(Wasay)出品的又一款还原利器,安装重启后会出现启动菜单选项,按F10进入设置界面。储存备份文件的原理是建立了一个整盘的虚拟分区(可以用一般的分区软件如Disk Genius看到),所以它基本上不会浪费太多

的空间。在系统保护方面,它可以保护CMOS,禁止软盘、操作系统启动等。在其它的附加功能方面,Pro-

Magic提供了三个实用工具:重新分区格式化、传送系统文件和硬盘对拷。Pro-Magic可以做手动和自动的多个时间点的还原,且还原点理论上说可以有无限个。Pro-Magic提供双重密码保护功能,授予管理者和使用者的不同权限。另外Pro Magic提出了一个共用盘的概念,因为软件可以对多重引导进行控制,“共用盘”就是在任何一个操作系统下都可以看到里面的数据,程序可以对里面的数据进行清除操作。 **■**



DeepFreeze

最新版本: 4.10

软件授权: 共享版

软件大小: 1.29MB

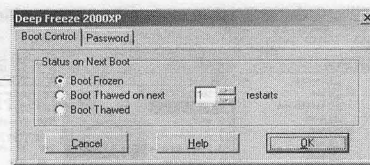
适用平台: Windows 9x/NT/2000/XP

下载地址: <ftp://down1.down@fjnt.com/xtwf/DeepFreeze2000XP.rar>

这个软件可以说是推荐的这十款之中操作最简单的一款,不过也是需重启次数最多的一个。单一的保护、无声的还原,特别适合嫌麻烦的朋友。安装之前一定要先清理一次系统垃

圾,并一定不能同时安装“还原精灵”,才可以

正常安装。注意在安装时就要进行备份驱动器的设置,完了之后设定一个管理密码,系统就开始受保护啦!重启之后在Windows下打开设置窗口的方法是:按CTRL+ALT+SHIFT+F6,里面有三个选项:“开机还原”、“开机N次后还原”及“不还原”。如果我们要新装软件,需在设置窗口里先选择第三项“不还原”,重启后开始安装软件,最后在设置窗口里再选择“开机就还原”就可以了(切记这个步骤)。软件的卸载也跟上面的步骤类似。 **■**



Linux 操作系统文件浏览器

Explore2fs

■ 北京 陈小兵

最新版本: 1.00 pre 6

适用平台: Windows 95/98/NT/2000/XP

软件授权: 共享软件

软件大小: 268KB

下载地址: <http://uranus.it.swin.edu.au/~jn/linux/>

Explore2fs 是一款类似于 Windows 操作系统的资源管理器, 不过是用来浏览 Linux 操作系统下文件。它不但可以从 Linux 操作系统下导入、输出文件和查看文件, 而且还可以直接对文件进行删除、修改、重命名以及创建等操作。使用 Explore2fs 来分析 Linux 系统下的文件和结构是非常方便的。该软件的常用功能有以下几种:

查看 Linux 下的分区

双击“全部文件夹”下方的磁盘图标 (在本文中显示为“hda5”, 如果系统中有多多个 Linux 操作系统, 则在左侧窗口中以 had 加数字标识显示磁盘), 在 Explore2fs 中将会显示 Linux 系统中的所有文件夹, 其中右侧窗口显示文件及其文件夹的详细信息。

在 Explore2fs 中有“大图标”、“小图标”、“列表”和“详细信息”四种文件查看方式, 分别单击工具栏上的四种图标即可切换查看方式。这比 Windows 的下拉菜单选择查看方式要方便得多。其中“详细信息”查看方式比 Windows 下的资源管理器增加了“权限”、“UID”和“GID”三个新功能。

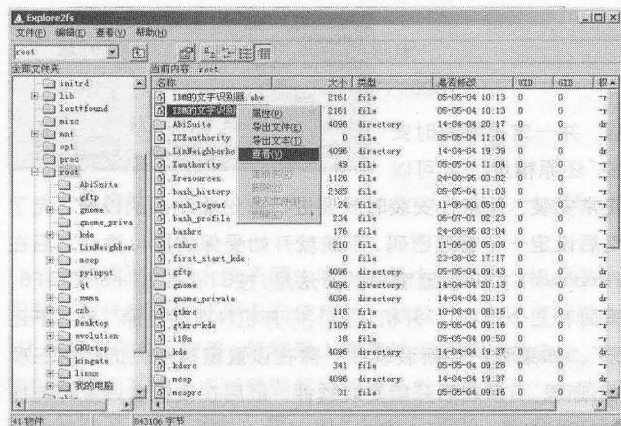


图1 可方便地查看 Linux 系统中的文件

查看文件

在 Explore2fs 中可以很方便地查看 Linux 系统中的文件, 使用鼠标展开文件夹, 然后选中欲打开的文件, 鼠标右键单击, 在弹出的菜单中选择“查看”(如图所示), 程序会自动选择相应的应用程序来打开所选中的文件。

输出文件和文本

在 Explore2fs 可以以两种方式输出文件, 一种是直接输出原来的文件, 另外一种是将文件输出为文本文件。使用鼠标展开文件夹, 然后选中欲打开的文件, 鼠标右键单击, 在弹出的菜单中选择“导出文件”, 然后在“另存为”对话框中输入要保存文件的名称即可。输出文本与输出文件类似, 在此就不赘述了。

对文件进行操作

Explore2fs 可以对 Linux 下的文件直接进行“删除”、“修改”、“重命名”、“导入文件”以及“创建”等操作。不过在运行 Explore2fs 程序的操作系统中, 不能对 Explore2fs 所要操作的磁盘进行访问。即对文件进行操作的磁盘分区应该是独立的, 在 Windows 操作系统下没有对其进行访问, 否则程序会报错, 显示如下错误信息:

```
Windows NT 5.0 build number 2195
```

```
Looking for Linux Partitions
```

```
GetLastError = (32) 进程无法访问文件, 因为另一个程序正在使用此文件。
```

```
GetLastError = (32) 进程无法访问文件, 因为另一个程序正在使用此文件。
```

```
GetLastError = (32) 进程无法访问文件, 因为另一个程序正在使用此文件。
```

```
\Device\Harddisk0\Partition5
```

```
EXT2 Found, magic = 0xEF53
```

```
Found 1 Linux partitions
```

分析 Linux 操作系统结构

使用 Explore2fs 来分析 Linux 操作系统结构无疑是方便的。使用 Explore2fs 可以很方便地查看 Linux 下的文件和设备分配情况, 可以很方便地对各种 *.conf、*.allow 等文件进行查看和修改。修改完毕后重新启动操作系统即可完成对配置文件的修改。①

邮件列表好帮手

■ 广州 伍裕标

最新版本: 5.01

适用平台: Windows 9X/ME/2000/XP

软件授权: 共享软件

软件大小: 1963K

下载地址: <http://www.onlinedown.net/soft/9469.htm>

是否有想过亲自动手制作属于自己的MAILLIST? 如果答案是肯定的话, 就一定要请MAILLISTKING帮忙了。因为有了它, 您就能轻松实现MAILLIST的订阅、退订、管理等工作, 从而从容驾驭MAILLIST。

单击“options”按钮(或者“view—option”)进入软件功能设置选项, 下面简单介绍一下:

◆ 单击“groups → edit”按钮可以增加或编辑组名(注意每个组名必须占一行);

◆ 单击“add all groups in current database”可以将有组别添加到当前数据库中; 在“scanning → mailling list folder”可以选择软件检测E-mail客户端所在文件夹位置。如果在安

装向导选择了第二项则此处不允许更改, 只能是“default folder”, 其中“auto-checking → always check for new entries on start-up”让软件启动时自动检测新增用户, 建议选择此项, “check for new netries every minutes”定时检测新增用户。

◆ 要使用Web提交的表单的功能, 请勾选“web forms → automatically process web form submissions”选项, 在下面的空白栏中输入表单名称。接着试着在您的Web页中建立一个表单, 并把有关的数据寄到您的邮箱, 以便让MAILLIST KING作出处理。“acknowledge”功能标签中分别可以建立subscription(订阅)和unsubscribe(退订)的模板, 我们只需各自填入主题和正文即可。

◆ 发送邮件时在“sending mail → send method”中单击“select”进行选择“use mapi to send via your default E-Mail software”。单击“send E-Mail to list”按钮进入发送窗口, 输入主题、正文(如果撰写html邮件时请先勾选“Message is in HTML format”选项, 然后就可以工具栏中的html工具了)。

简单便捷的使用就介绍到这里, 喜欢的话, 不妨下载一个试试哦! ■■

eEye数字安全公司—Retina Network Security Scanner

Retina Network Security Scanner是卓越的网络安全漏洞扫描和补救管理系统, 它能发现和帮助修复所有已知的互联网, 局域网和外部系统的网络安全漏洞。Retina操作简便并包含了先进的报告工具来安排和隔离必要的修复工作。它提供对开放式网关, 用户安全政策, 注册设置和一系列的已知安全漏洞的完全控制。它最有竞争力的优点在于能自动矫正许多检测出来的漏洞, 并提供了可以完全定制的助手工具。Retina的助手工具允许客户强制实施内部安全规则, 比如防病毒部署和企业标准注册登记表的设置。作为一个同时面向分布式企业用户和单机网络环境用户的专业安全软件, Retina已经被世界上许多大公司和政府部门使用。

Retina Remote Manager是一个基于网络的在一个组织中增加对多个分散式 Retina Network Security Scanners 远程管理的软件。每个 Retina 都能设置成为企业网络监控的一部分, 用于不间断的监控某些已知的安全漏洞, 让网管员集中创建, 调度和浏览整个网络中的 Retina 扫描结果。

Iris Network Traffic Analyzer是一个容易上手的新一代网络协议分析工具。它捕捉每一条从服务器通过的数据,

并允许网络管理员方便的跟踪和重演任何网络用户的任何操作。Iris 完全重建捕获的数据, 允许网管员监控任何网络操作就好像用户在自己的客户端所见的一样。此外, Iris 还有先进的过滤, 搜索和图表功能, 是一个功能完全的系统监控解决方案。

美国 eEye 软件中国区代理:
上海比特瑞旺电脑有限公司
Qast Systems Solutions Inc.



地址: 上海市江苏路 369 号兆丰世贸大厦 7 楼 D 座
邮编: 200050
电话: 021-52400198 传真: 021-62115855
欢迎访问 www.qast.com 网站了解更多产品信息!

Exchange Server

安装 Exchange 2000 Server

Q 我的操作系统是 Windows 2000 高级服务器版,我想在它上面安装 Exchange 2000 Server 版,但始终不能成功。请问,是否需要特殊的安装方法或条件?

A 安装 Exchange 2000 Server 之前,你必须同时满足以下几个条件:

1. 确保 Windows 2000 已升级成了域控制器,安装了 Active Directory (活动目录)。假设本服务器的计算机名为“Server”,“域”被命名为“o a”,“域名”为“Netadmin.net”,则本机的“Active Directory 域名”为“oa.Netadmin.net”(它同时也将是邮件服务器名),而“完整的计算机名”则为“mail.oa.Netadmin.net”。

2. 确保已安装了 NNTP (Network News Transfer Protocol, 网络新闻传输协议) 和 SMTP (Simple Mail Transfer Protocol, 简单邮件传输协议) 两种服务。它们的添加可以在“控制面板→添加/删除程序→添加/删除 Windows 组件”中的“Internet 信息服务 (IIS)”中找到。由于后文基于 Web 的 Exchange 的使用需要用到 IIS 中的 HTTP 服务器,因此建议此处一并并 IIS 组件中的所有内容都选中。

3. 登录账户必须拥有修改根域的配置容器的权限,并且它必须是以下三个小组中的一员:“Enterprise Admins”、“Domain Admins”、和“Schema Admins”,也即它必须至少属于其中的某一个小组。

4. 目录“MDBData”必须为空!它所在的默认路径为“C:\Program Files\Exchsrvr\MDBDATA”,其中 C 盘为 Windows 2000 系统文件所在的分区。

5. 此外还需要 DNS (Domain Name System, 域名字系统) 和 DHCP (Dynamic Host Configure Protocol, 动态主机配置协议) 两种服务。它们的添加可以在上步“添加/删除 Windows 组件”列表中的“网络服务”里找到;也可以在安装 Exchange 2000 Server

时让系统一并并将它们自动添加上去。

6. 由于 Exchange 2000 Server 的安装过程很长(往往需要1个小时左右),为了防止安装过程中因意外事故(比如停电)的发生而造成前功尽弃,请事先做好相关防范工作。

服务器升级成域控制器

Q 我在安装 Exchange 2000 Server 之前,服务器是否一定要升级成域控制器?

A 不,没有必要!只需您要安装 Exchange 2000 Server 的目标服务器是属于一个 Windows 2000 域就行了!当然,如果您在只有一个服务器(如一个域控制器)的小型分支机构(SBO)或是中等分支机构(MBO)中部署 Exchange 2000 Server,你就必须先将它升级到域;否则通常不需要在域控制器上安装 Exchange 2000 Server。

升级 Exchange 2003 Server

Q 之前从 Exchange Server 5.5 升级到 Exchange Server 2000,但是最后要删除 SRS 时 Exchange Server 5.5 的 director replication service 怎么都删不掉,若再想升级到 Exchange Server 2003 不知要先注意什么?

A 如果您已经是 Exchange Server 2000 升级到 2003 就不会向 5.5 那么复杂了,而且 2003 提供您一个 Step by Step 的指引工具 ExDeploy,一定要 Follow 此工具,注意事项请参考附件。

防范 Exchange 2003 Server 成转信站

Q Exchange 2003 Server 好像被当成转信站了,该怎么办好?修好以后要怎么做防范?

A 请确定 Relay 的设置是否正确。(预设是

拒绝 Relay 的)

1. 开启 SMTP VIRTUAL SERVER 的属性页。

2. 在 ACCESS 页中,按下 RELAY 的按键。

3. 选择“Only the list below”并勾选“Allow all computer which successfully authenticate to relay”。

两者搭配有何特别

Q Exchange Server 2003 和 Outlook 2003 搭配上有何特别之处?

A 最大的好处是提供了 RPC Over HTTP 的功能!使用 MAPI 的使用者可以只透过 SSL 443 Port 直接与 Exchange Server 2003 进行联机!这样一来就可以不用大费周章的去修改 Exchange 的 port 或是将防火墙开大量的 Port。

在 OWA 上有何不同

Q 请问在 OWA Outlook Web Access 上有何不同之处吗?

A 最大的差别在于其使用者接口已经改为 Outlook 2003 接口!此外在以前的版本无法针对邮件按右键做任何动作,现在则会出现快捷菜单!此外阅读窗格也有所改进!更重要的是可以修改 Register Key 启动防止使用者透过 OWA 的方式将机密档案下载回公司以外的地方。

OWA 保护

Q 请问如何强化 Exchange Server 2003 OWA 的保护呢?

A 请建立 CA Server 利用 SSL 加密通讯来存取 OWA,搭配 ISA Server 的防护,即可保护 OWA 及内部网络之安全。

设定备份

Q Exchange 2003 Server 如何设定每次寄件都能有备份?

A 可勾选 Information Store Properties 中的 Archive all messages sent or received by mailboxes on this store, 可将所有进出的信件备份一份至其它信箱或是公用数据夹中。

使用 OWA 看信

Q 请问我该如何让 user 账户能使用 OWA 进入 Exchange 2003 Server 看信?

A 安装 Exchange 2003 Server 后, 系统会自动配置 OWA, 也就是说内部的使用者只需透过 IE 输入 http://exchange 即可, 若 internet 的 user 账户需要 OWA 时, 需要在 FIREWALL 上做适当的配置。

转移 Mail Server

Q 要怎样才能顺利从 Exchange 2000 Server 移转 Mail Server 到 Exchange 2003 Server 上呢?

A 安装 Exchange 2003 Server 加入原 Site 中, 将 Exchange 2000 Server 信箱及公用数

据夹迁移至 Exchange 2003 Server 上, 移除 Exchange 2000 Server 即可。

利用公司邮件服务器收、发信

Q 如何设定家里的 Outlook Express 可以利用公司的 Exchange 2003 Server 寄信与收信?

A 将 SMTP, POP3 指定到 Exchange 2003 Serve 上即可; Exchange 2003 Serve 也需要将 Port 25, 100 对应至实体 IP 上。另外也可以用 OWA, RPC over HTTP, VPN 来收发信件。

AD 安装 Build up AD 网域

Q Windows 2000 Server AD 安装 Exchange 2003 Server 需要重新 build up AD 网域吗?

A 安装 Exchange 2003 Serve 并不需要重建 AD, 但需要重新 EXTEND SCHEMA Setup / forestprep; Setup / domainprep, 再安装 Exchange 2003 Server。

追踪不同错误讯息

Q 每次我在 Exchange 2003 Server 使

用邮件追踪都会出现不同的错误讯息, 重新安装有用吗?

A 不建议重装, 可以做以下测试。

1. 停用 message tracking.
2. 移除 exchsrvr\log 资料夹。
3. 重新启用 message tracking.

设定 IMAP

Q 请问 Exchange 2003 Server 的环境里要如何设定 IMAP 呢?

A 在 Exchange 2003 Server 上预设是停用的, 必需先将该 Service 设为启动 (自动启动), 再到 ESM 中将 IMAP 的 Virtual 启动即可使用。

设定备用专线

Q 如何设定备用专线? 以防当其中一条专线有问题时, 收发信可随即由第二条线接手。

A 需要一台支持 in bound load balance 的宽带负载器, 然后在 DNS server 上设定 MXRECORD 指向两条专线的 IP。重点是在 DNS 的设定上, 至于设定的细节要视使用的宽带分享器而定!

Windows 操作系统

不能安装 longhorn

Q 我现有的系统是 Windows XP, 完全安装 Windows longhorn 到一半的时候, 系统却提示 “can't edit boot.ini”, 请问为什么会这样, 应该如何解决才能正常安装呢?

A 错误提示已经告诉您了, 不能编辑 Boot.ini 文件所造成的安装失败。解决办法: 在 Windows XP 下打开 “我的电脑”, 选择 [工具] → [文件夹选项] → [查看], 设置显示所有隐藏文件和受系统保护的文件, 然后找到 Boot.ini

文件, 将它的 “只读” 属性去掉, 换为 “存档” 属性。重新安装就不会出现错误了。

SU0167 错误信息

Q 在安装 Windows 98 的过程中, 出现 SU0167 的错误信息, 使安装搁浅, 怎么也进行不下去, 请问这是什么问题, 如何解决?

A 错误信息提示是重名目录造成的。因为当前目录中存在名为 “Desktop” 的目录, 而在 Windows 98 安装过程中将生成一个名

为 “Desktop” 的目录存放系统文件, 因此安装程序不能将 Windows 98 安装在这个目录中。解决的办法很简单, 只要将当前目录中的 “Desktop” 目录删除或重新命名, 然后再运行安装程序即可成功。

DDRAW.dll 出错

Q 重新安装系统后, 我发现很多游戏都不能玩了, 就连 Flash 也打不开了, 系统提示: 系统文件出错, 找不到所需的 .dll 文件 DDRAW.Dll 文件。请问应该如何

恢复它呢?

显然故障是由于DDRAW.DLL文件出错或者丢失造成的,该文件是DDRAW的加速程序,而DDRAW是DirectX的重要组成部分,游戏必须依靠它才可以正常运行。所以我们只要重新安装一下DirectX一般就可以解决问题了。

系统配置无法通过

我的电脑在安装Windows 98时,执行到系统配置一步时出现问题,尝试几次都不成功,非常苦恼,能告知什么原因和解决办法吗?

安装系统时,系统自动关机或没有响应,也有的会提示“致命的异常错误发生在0137”或“0028错误”。出现这种情况一般都是由于硬件问题造成的。而其中主要原因是芯片过热导致。解决的方法可采取:恢复CPU超频设置;检查CPU散热风扇是否脱落或停转;显卡的主芯片散热风扇是否脱落或停转;内存条或硬盘是否存在故障;机箱内散热状况是否良好等等,然后根据检查或判断的结果相应采取对策。

禁用错误汇报

我的电脑装的是Windows XP,最近在msconfig启动项中发现了一个名为“dumprep 0-k”的项目,感觉比较可疑,所以想删除它,但删除后它又来了!即使在注册表中,将它找到后删除,还是不行,

它仍然在msconfig启动项中。请问它是做什么的?如何才能删除呢?

这个启动项的作用是用来向微软汇报错误的,大家在使用Windows XP或2003时,当遇到非法操作的时候,系统总会问您是否发送错误报告给微软,以便微软解决问题。实际上并没有什么坏处,但如果您想关闭它,可以进入“控制面板”,选择[系统]→[高级]→[错误报告],选择“禁用错误汇报”选项即可取消错误汇报,这样msconfig启动中相应的项也自动消失了。

NTFS无损转FAT32

我安装的系统是Windows 2000, C盘是NTFS文件格式的,因为使用这种格式造成了诸多不便,所以我想将它转换成FAT32格式的。请问如何在不破坏C盘内容的情况下对文件格式进行无损转换呢?

在转换之前,首先建议您将C盘重要的内容备份到其它盘中,然后使用PartitionMagic For DOS版进行转换(这里之所以没有用For Windows简装汉化版,是因为使用该版本转换经常出现丢失文件、中文目录出错的现象)。在转换过程中一定要保证不要出现停电等意外现象发生,不然就惨了,呵呵。

Home版内置防病毒功能

既然Windows XP Home Edition有内置的病毒防护功能,我还需要安装另外

的病毒防护软件吗?

除了XP带有自己的防火墙以外,其他任何Windows产品都没有病毒防护软件。这个防火墙可以帮您阻挡一些来自Internet的侵犯(如果您需要更高级别的防护,还是建议您安装一个功能更强的软件),但是它对于E-mail病毒和Web蠕虫无能为力。

其实另外安装防病毒软件是完全需要的,您可以选择一些免费的或者是试用版,或者购买一些声誉不错的软件如Norton AntiVirus、McAfee VirusScan,或者Trend Micro的PC-cillin,另外及时更新病毒代码和补丁也非常重要。

共享NTFS和FAT32文件系统

Windows XP同时支持NTFS和FAT32两种文件系统,所以假如我使用NTFS格式安装Windows XP,我可以和机器中其他使用FAT32的Windows系统之间共享数据吗?

可以的。您的文件系统只特定针对您的系统和硬盘,不影响网络文件的共享。

但是,这样的文件系统会影响您访问您硬盘中的文件,如果您使用双系统启动或者用启动盘启动另一个系统。所以如果您在一个分区使用DOS或者Windows 95、98、98SE或者Me,用FAT32文件系统,您就无法访问保存在另一个NTFS分区的Windows XP、NT或者Windows 2000的文件。因为NTFS文件系统使用基于NT的加密方法来保护文件,所以您必须用Windows NT、2000或者XP的版本登录访问NTFS分区的文件。

Linux 应用

服务器安全

如何确定wu-ftp服务器是否存在site exec安全漏洞?

在某些Linux发行版本上(Redhat 7.3)的wu-ftp有site exec安全漏洞,用户可以非匿名用户ftp登录,然后执行下面的命令:

```
ftp>SITE EXEC bash -c id
```

如果返回的信息中有“200-uid=0 (root) gid=0(root)”,那么就有这个漏洞,需要马上更换。

加入Windows启动选单

如何将Linux加入到Windows Me/

XP的启动选单中?

可以按以下步骤来完成:

1. 安装完所有Windows系列操作系统后再装Linux,并在安装时选择将Grub或LILO安装到Linux所在的分区,而非MBR;
2. 利用启动盘启动Linux,执行下面的命令加载Windows分区:


```
#mount /mnt/dos
```

3. 执行下面的命令。这样在 Windows 分区就有了一个 bootsect.linux 文件, 它记录了 Linux 分区的启动信息:

```
#dd if=/dev/hda? bs=512 count=1 of=/mnt/dos/bootsect.linux
```

4. 在 Windows NT 的启动配置文件 boot.ini 中加入下面的一行:

```
C:\BOOTSECT.LIN="radhat Linux 9.0"
```

然后再启动电脑的时候, 发现在 Windows 启动选中单中多了 "redhat linux 9.0" 这个选项。选择它就能启动 Linux。

通过防火墙使用数据镜像

④ 在不危害安全的情况下通过防火墙使用数据镜像 (rsync)?

这通常有两种情况, 一种是服务器在防火墙内, 一种是服务器在防火墙外。

无论哪种情况, 通常还是使用 ssh, 这时最好新建一个备份用户, 并且配置 sshd 仅允许这个用户通过 RSA 认证方式进入。

如果服务器在防火墙内, 则最好限定客户端的 IP 地址, 拒绝其它所有连接。

如果客户机在防火墙内, 则可以简单允许防火墙打开 TCP 端口 22 的 ssh 外发连接就可以。

验证 TCP/IP 协议是否安装

④ Linux 下如何验证本机 TCP/IP 协议是否安装?

Linux 中一个概念: 封闭回路。使用 TCP/IP 协议的 Linux 计算机, 都会拥有一个 IP 地址, 彼此间相互以 IP 地址确认对方, 传递信息与数据。在有些情况下, 我们为了进行某项测试 (比如网卡是否正确安装), 或者是没有另外一台电脑作为接收端。这时, 我们可利用本机扮演信息的发送端和接收端, 这就是所谓的封闭回路。封闭回路的 IP 地址是 127.0.0.1。这个 Ping 命令被送到本地计算机的 IP 软件, 在 Linux 下该命令永不退出该计算机。如果没有做到这一点, 就表示 TCP/IP 的安装或运行存在某

些最基本的问题。

DNS 故障排除

④ Linux 下 DNS 服务器故障排除步骤?

Linux 域名服务器使用的是 Bind9。域名服务器包含数据库的部分段的信息, 并可提供被称之为解析器的客户来访问。如果在 Linux 网络中无法进行域名解析, 很可能是没有在本地指定有效的域名服务器, 通常这种情况比较常见。大多数 DNS 故障是因为配置文件的语法错误, 或者是对计算机分配了错误的地址造成的。当进行 DNS 故障诊断时, 可参照下面的步骤:

- (1) 对全部记录检查和确认主机名称的拼写, 记住绝对地址是以 "." 结尾的。
- (2) 如果在区文件中做了任何修改, 务必修改 SOA 记录中的序列号, 这将保证服务器正确地重新上载文件。
- (3) 确定输入到主区的名称和 IP 地址匹配反向指针文件中的反向指针信息。
- (4) 检查防火墙相关程序。

网络故障排除

④ NFS 网络出现了故障排除步骤?

网络文件服务器 (Network File System, 简称 NFS), 是分布式计算系统的一个组成部分, 可实现在异种网络上共享和装配远程文件系统。故障排除步骤:

- (1) 检查 NFS 客户机和服务器的负荷是否太高, Server 和 Client 之间的网络是否正常。
 - (2) 检查 /etc/exports 文件的正确性。
 - (3) 必要时重新启动 NFS 或 portmap 服务。
 - (4) 运行下列命令重新启动 portmap 和 NFS:
- ```
service portmap restart
service nfs start
```
- (5) 检查 Client 上的 mount 命令或 /etc/fstab 的语法是否正确。
  - (6) 查看内核是否支持 NFS 和 RPC

服务。

### 屏蔽索引文件

④ LAMP 网站的目录如何屏蔽索引文件?

LAMP 网站的目录如果没有索引文件, 用户便可以看到网站所有目录的列表, 在 Apache 的配置文件 httpd.conf 中找到需要设置目录的 Directory 属性, 并在 Options 一行去掉 Indexes, 就可以屏蔽索引文件。

### 显示器休眠

④ 在 Linux 下, 显示器经常进入休眠状态, 怎么能不让显示器休眠呢?

用户可以使用下面的命令试一下:

```
#setterm -blank n (n 为等待时间单位是秒)
```

### NFS 连接方式

④ NFS 连接有哪些方式?

NFS 提供硬 (hard) 或软 (soft) 两种挂载方式:

采用硬挂载: NFS 客户机会不断的尝试与 NFS 服务器的连接, 直到挂载上为止。软挂载: 会在前台尝试与 NFS 服务器的连接, 是默认的连接方式。如硬 (hard) 挂载:

```
mount -t nfs o hard 192.168.1.4:/home/cao /home/nfs/cao
```

对于到底是使用 hard 还是 soft 的问题, 这主要取决于你访问什么信息有关。例如你是想察看 NFS 服务器的视频文件时, 你绝对不会希望由于一些意外的情况 (如网络速度一下子变的很慢) 而使系统输出大量的错误信息, 如果此时你用的是 hard 方式的话, 系统就会等待, 直到能够重新与 NFS 服务器建立连接传输信息。另外如果是非关键数据的话也可以使用 soft 方式, 如 FTP 一些数据等, 这样在远程机器暂时连接不上或关闭时就不会挂起你的会话过程。④





2005 的新年“网刊互动”又与您见面了！哈，本期新增了一份崭新的读者反馈表，并有精美礼品相送哦，请大家多多留意。昨天接到一个电话，是位询问“精华看板”文章出处的读者，真让小凡高兴，这才是真正意义上的读编往来呀。各位读者，如遇到杂志方面的问题，欢迎与小凡取得联系，我会尽力帮您的。

今年本栏目打算多多刊一些网管员求职面试所感所悟的文章，相信大家会很感兴趣的，毕竟看看同行们的得意、失意，对自己绝对是个好的参照。那么这里小凡也向广大读者发起征稿，畅所欲言，谈您所感，多多给我们投稿，我们这里每一篇文字都出自如您一样的广大平凡网管员，还犹豫什么？赶快行动吧！

## 网管日记

### Siemenew 2004年9月16日

公司又进新员工了，公司从前年的35个人扩张到现在的92人。这两天可把我给忙坏了，新员工在我一点都不知情的情况下突然出现在单位里，领导要我马上给他们配电脑，在我们这种小城市里要一下子去弄十几台电脑谈何容易。真是郁闷。这种情况出现了好几次，我也提了好几次。结果呢？办公室的人说他们忙，没时间顾及这些。所以他们的人员从3个增加到6个。现在会计和出纳也增加到4个了，可我仅仅要求把一些如发电子邮件，刻光盘的工作交给其他人的要求也没实现。这两天，我总结了一下，唯一的原因就是我的工作效率太高。哎！没时间写了，有人在催我去帮他装软件了。

### 暮雪千山 2004年9月22日

吾校中有师名曰“晓斌”者，年二十三，山东淄博人也。好书法，喜于女子戏。

今日午时见斌于宿舍内，斌手持一罐状物，品之，见吾入其室，忙呼之曰：兄速看此物。乃明朝之宝也。

吾忙视之，见其罐乃以瓦成，油迹斑驳，不可见其色也，问曰：斌兄从何处得此宝？

答曰：吾昨日归家，于床下得之，乃询翁，翁道其儿时即见此物，恐已多世。详究之，以为宝。

吾求于手中试玩，觉罐底有字，审视之，乃见其字迹“淄博永利陶瓷厂制 MADE IN CHINA”

吾笑之又笑，晓斌视之，气而破其罐曰：十块钱六个，害我昨晚抱其眠也！

### 阿奴 2004年10月22日

昨天备机又出问题了。本来运行得好好的，突然一点反应都没有，按键盘没用，点鼠标没用，整个一关机状态。一开始还以为是同事把它给关了，于是毫不犹豫按下POWER键，灯亮了一会，屏幕上都还没显示，就自动熄灭，感觉是电源不足，驱动不起来的样子。我向领导汇报了情况。打算向HP金牌服务求助，打电话过去，一直在占线。

副主任进来，把CMOS电池拿出来放电之后竟然能启动了，真是怪事，我到现在都还不明白到底是什么原因。

### Landy 2004年11月14日

由于昨晚在外面混得很夜才回来，今天睡了整天，呵呵，也够厉害的：)

翻了翻杂志，也上网转了转，突然有种想法：看看我对各大版块的问题都能否回答，知识方面如何。

于是乎进Linux版出Windows版，进XX版再出……看到的问题除了关于路由器及编程方面不大熟悉外（真的丢了这方面的知识），其它都还能正常回答上来，也能够有相关思路；随便回答了些题目但懒得再动手打字了。不过也不大再想方方面面都想发展了，人的精力有限得很；可能再迟一段时间或更久些，相信丢得会更多，毕竟目前自己已有相关的发展方向了，没必要再将精力耗上一些不相干的知识上了。另外，前几天发过这试题：<http://www.netadmin.com.cn/adminbbs/dispbbs.asp?boardID=49&ID=18374&page=1>，想看看论坛朋友的知识方向，从跟



贴可以大概地说明在网管论坛的各位朋友的知识集中点了;也从侧面看到目前绝大多数公司是以MS产品线为主;其实上面的试题如果是自己不靠网络能回答出90%的话,工资会在4-8K(对方经理说的),如果你细心些,应该会知道该公司的名称及所在的地方;考的知识面也广(包括Linux / BSD / Solaris / Router等)。说真的,在脱离一台机器的情况下,我也没法正确地写出一半的问题,知识确实不牢固……

呵呵,感觉写的好乱,不过既然是日记,也懒得整理思路;想到什么就写什么。

## 动态 播报

是否曾有某网络产品让您很不满意呢?不妨来这里一吐为快!我们将协助您向厂商进行反映,或者通过媒体进行发表,让其他同行引以为戒。体验上帝的感觉,就来网管员世界“我不满意”投诉台……



## Yangsir 会客厅

Yangsir:首先需要更正一下,2004年第12期《信号衰减引故障》的作者是瞿松平,特此更正,并向作者致歉。

## 精华看板

### 网络基础

图解虚拟机 VMware Workstation 的安装与使用

网络故障诊断 70 例

网管到底要掌握哪些东西?

轻松当网管—深挖 DNS 服务器潜能三法

移动硬盘常见问题的解决

### 系统集成

CISCO 路由器 IOS 的恢复

动态 IP 地址的 DSL+NAT 的实现

二层交换机,三层交换机,四层交换机的区别

Cisco 常见路由器密码和版本恢复方法探讨

Cisco IOS 接口不正确处理 IPV4 包远程拒绝服务漏洞

开启路由器的 TCP 拦截

### Windows 及其应用

最全的 windows 操作系统快捷键

## 《网管员世界》诚征优秀稿件

《网管员世界》是由中国电子信息产业发展研究院(CCID)创办的网络技术专业媒体,其目标读者以网络管理技术人员(网管员)为主,辐射网络管理主管、网络爱好者、准网管和所有关注网络事业发展的人士。

《网管员世界》内容以技术应用为主,注重实用性和知识性,以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。

### 主要栏目:

**故障诊断**—网管员日常工作中遇到的网络问题,如交换机、路由器、服务器、服务器系统软件、网线等出现的故障分析和解决。

**安全防范**—防患于未然的安全设置、及时有效的网络攻击防御。

**补丁升级**—介绍如何对现有系统进行升级、安装补丁软件、弥补系统漏洞。

**知识讲堂**—网管员必备的基础知识和完成日常工作所需的专门知识介绍。

**经验技巧**—网友日常工作中提高工作效率的一些经验和技巧。强调实用性。

……

本刊欢迎所有与网络管理有关的各类优秀稿件。来稿要求内容实用性强,问题的普遍性强,文字生动,可读性强。投稿请寄至各版块指定投稿邮箱,并在邮件主题中注明“投稿”字样,同时注明详细联系方式,以便本刊随时与您联系。

如果五个工作日内尚未接到回复,请您确定一下邮件是否正常发出。若重发后仍未得到回复,可以拨打编辑部电话 010-88558021 进行查询。

恶意网站——永久屏蔽

Windows Server 2003 秘笈放送

电脑高手应用技巧荟萃

很好的技巧 60 则

最新万能 DOS 启动盘制作全攻略

让计算机启动更快 15 招

快速关机的 5 种方法

超级值得收藏! IE 经典故障大全

使用事件查看器和微软知识库解决问题的经验

## Linux/Unix

学习网址 Linux

Linux squid 服务器安装使用

Linux 必须学会的 60 个命令

Linux 使用技巧集锦

linux 内核编译手记

linux 入门教程



这是一篇在论坛上倍受好评的原创文章,出自我们亲爱的女网管员阿奴好妹妹,在此发表是想让所有读者也与我们论坛网友一起互动,呼唤网管员原创文章,把您的工作、生活用文字显现出来……

# 淘汰

## ——一台服务器自述

■ 阿奴

我叫HP LH6000,是HP家族的一员。2000年10月份的某一天,我被人装进集装箱,上了火车,车行几千里,辗转到了云南的一个小城市,在一公司安家落户了。记得人们才打开箱子的时候,对着体积比普通电脑大好几倍的我“啧啧称赞,说不愧是服务器,感觉就是不一样。听到这些赞美之词,我有些飘飘然。我被安置到一个大房间里,人们称这房间为“微机房”,里面有好几台体积比我小得多的微机。说实在话,把我安排了和这些普通家伙在一起,我感到很委屈。作为“服务器”,公司的“核心机”,我认为应该给我一间单独的房子居住,而不是和这帮家伙混居。但没办法,“机”在屋檐下,不得不低头,总有一天,这里的人会认识到我的重要性的,当前只能忍耐。

不久,我就知道了自己的具体任务。原来这个公司新上了一套管理信息系统,用的是SYBASE数据库。而我呢,作为他们的数据库服务器使用,每天24小时运行。唉!真是命苦,这房间里的其它家伙每天只需要工作8小时,下班后就可以熄火休息。我却成天不停地运转。长时间的操劳过度,我终于病倒了。人们很着急,我看见那个叫阿奴的小姑娘急得饭也不吃,觉也不去睡,在我身上不停的折腾,把我的合作伙伴Windows 2000、SYBASE装了又卸、卸了又装。最后一次安装好后,一头靠在凳子上睡着了。我看她瘦弱的身体,睡梦里还不安稳的表情,实在不忍心了,我发誓要好好工作,不管怎么累,都得坚持下去。

我一直很努力,但还是问题不断。开始时只有两三个客户端向我提出处理数据的请求,到后来增到十多个。我每天忙着把资源分配给这些提出“请求”的家伙使用。有些可恶的家伙非常不讲信用,常占据我的内存空间不归还,其它长时间排队等候使用“资源”的“客户”提出了剧烈的抗议。我也没法呀,“僧多粥少”。我无法开口说话,只能指望着这里的人能发现我的窘况,再给我加点“资源”。人们最终还是发现了这一问题,决定给我增加“兵力”。一开始我只有一颗CPU主持大局,512MB的内存供使用,后来一连给我加了3颗CPU,内存也加到1GB,还给配置了磁盘阵列。有那么好的条件,我想施展手脚好好大干一场,让人们认识到我的重要性。

在我意气风发的时候,新问题又出现了:由于厂家的程序没处理好,导致客户端不停的死锁。这问题我是知道的,有很多个赖皮“进程”,一抓住内存就不放。有时候我真不想分配资源给它们。但“顾客”至上,人家有请求,我就不得不给,一给就出问题。我身上的部件刚增加过,所以我的问题不大。人们开始找软件问题,阿奴成天在我身上运行程序测试,详细登记了那些无赖进程锁住内存

的情况,并把这些反映给软件提供商。当然,这些软件提供商怎么肯承认是自己的软件有问题,他们觉得是我的资源不够,才导致那么多的“进程”争抢。阿奴和他们剧烈的争执了一翻,最后达成协议:软件提供商更改程序;我方新增一台服务器,两机做双机热备,我做为“备机”使用。

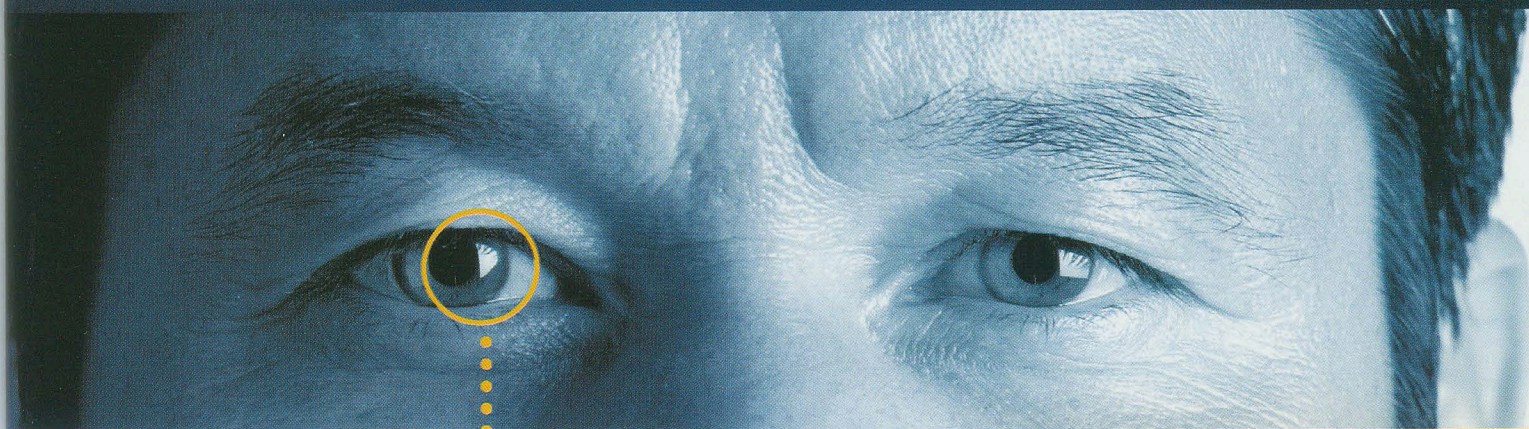
我真冤呀,本不是我的问题,到最后把我下放到“备机”使用。新来这家伙黑头黑脑,一副酷像。人家实力比我强,我也只能忍气吞声做它的副手。不过沾它的光,我们分配到一间专门的机房,人们称这房间为“服务器室”。我的任务就是在这家伙“头疼发热”不能工作的时候,我马上接管它的工作。我们之间用一根“心跳线”相连,我每隔几秒钟就检测这家伙的心跳,看看它是否在“喘气”。如果一旦停止“喘气”,马上接管任务。可这家伙身体好得很,连续工作了两个月竟然没出半点问题。我等得真心焦。“马行千里,终有失足的时候”,有一天,这家伙生病了。我真乐呀,马上把它的工作接管了过来。一开始人们并没有发现是我接替了“主机”的工作,还以为是那家伙在工作呢。我希望人们能尽快发现是我在工作,从而认识到我的重要性。阿奴当天就发现问题了,这小丫头每天都会到我们住的地方检查我们的“身体状况”。她迅速处理了那家伙身上的故障,想把我正接管着的工作任务交还给它。刚想操作,我见她歪着头想了想,又放弃了,还是让我继续工作,我真开心呀。工作到第二天,我看见阿奴指着我对其它人说“其实以前用它也能胜任工作的,主要是软件问题比较大”。人们频频点头,他们终于认识到不是我的原因了,我好感动,有一种被“平反昭雪”的感觉。第三天,那恢复元气的家伙开始和我争抢管理权。反正“磁盘阵列柜”里的磁盘资源在我的掌控之下,我看你怎么办。那卑鄙的家伙抢不到资源,竟然启用了我俩共同使用的一漂移IP地址。这地址本来是谁接管资源谁使用的,现在它一使用,我就没法了,只好撒手。我一撒手,它没阿奴的帮忙,也无法把任务启动起来,结果我俩同时丢掉任务不管。阿奴气急败坏地进来,看了一下我们各自的“日记”,就明白发生了什么事。二话不说,把资源交给了那家伙,看到那家伙得意洋洋的样子,我肺都快气炸了。

从当初的“核心机”,沦落到今天的“备机”,心里的酸楚真是无以言表。隔壁杂物间里堆放着很多淘汰下来的伙伴,每当夜深人静的时候,我常听见它们在长吁短叹,听它们回顾昔日的辉煌,感叹今天的悲凉。它们这般景况会不会是我明天的归宿,我不敢想象。

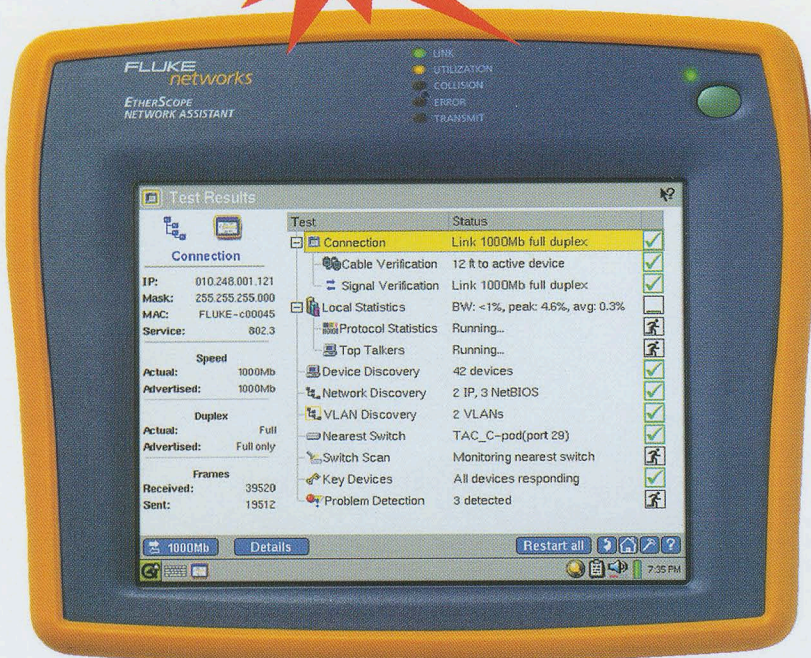
相关链接: <http://www.netadmin.com.cn/adminbbs/dispbbs.asp?boardID=49&ID=8377&page=1> ■



# 网络性能测试极佳助手



新



EtherScope™  
ES 网络通

EtherScope™ ES 网络通  
快速透视网络、发现问题、解  
决故障的极佳助手

- 第一台支持 1000Mbps 的掌上型测试仪
- 自动测试网络设备的端口状态和 VLAN 设置
- 分析流量趋势和带宽需求
- 分析协议分布和数据源
- 验证关键服务器的连通性
- 电缆测试和网络信号诊断
- 交换路径跟踪 Trace SwitchRoute
- 内置网络测试报告
- 通过 WEB 方式远程遥控
- 可支持无线局域网和吞吐量测试选项

ES 网络通 让您工作更轻松。请访问 [www.flukenetworks.com.cn/EtherScopeD](http://www.flukenetworks.com.cn/EtherScopeD), 了解产品详细信息, 观看产品在线虚拟演示, 并申请工程师到您的现场进行实地演示。

网络超级透视  
NETWORK SUPERVISION

美国福禄克网络公司

北京办事处: (010)65123435 转 660 上海办事处: (021)63548829 广州办事处: (020)38795800  
成都办事处: (028)85268810 西安办事处: (029)88376090 重庆联络处: (023)89061910  
济南联络处: (0531)6127616 沈阳联络处: (024)23286038 武汉联络处: (027)85743386

FLUKE  
networks™





是摆脱垃圾邮件困扰的时候了!

**美讯智 RiskFilter/SMG 反垃圾邮件信息网关是您的不二之选：**

- ▶ 准确率高，最高可达 98%，误报率低
- ▶ 适用于各种邮件系统，且易于安装、管理
- ▶ 垃圾、病毒邮件过滤策略库全球自动更新，实施后基本不需要人工管理
- ▶ 允许邮箱用户登录 RiskFilter/SMG，查询并处理自己收到的垃圾邮件；系统每天自动产生垃圾邮件摘要邮件，用户在摘要邮件中可直接处理垃圾邮件，彻底解决了误报问题
- ▶ 完善的统计分析功能帮助用户全面了解应用状况并相应调整过滤策略等
- ▶ 高性能高可靠性的电信级产品

赶快行动起来，拨打 800-810-7638 索取 RiskFilter/SMG 试用版，精美礼品等着您！

欢迎访问公司网站：[www.surfcontrol.com](http://www.surfcontrol.com)

公司地址：北京市东长安街1号东方广场C2座三层309号    公司电话：010-85188860    公司传真：010-85150067

  
**SurfControl®**  
The World's #1 Web & E-mail Filtering Company  
**美讯智科技**



## 郑重声明

本作品的图片均来源于互联网，仅供PDF文档制作学习，交流之用。版权归原出版社所有。任何组织或个人不得公开传播或用于任何商业盈利用途，因而产生的一切后果由该组织或个人承担。本站及其制作者均不承担任何法律责任。请自觉在下载后的24小时内删除。如果你喜欢该读物，请你支持及购买正版读物。

AprilVolcano.Org

Volcano Studio