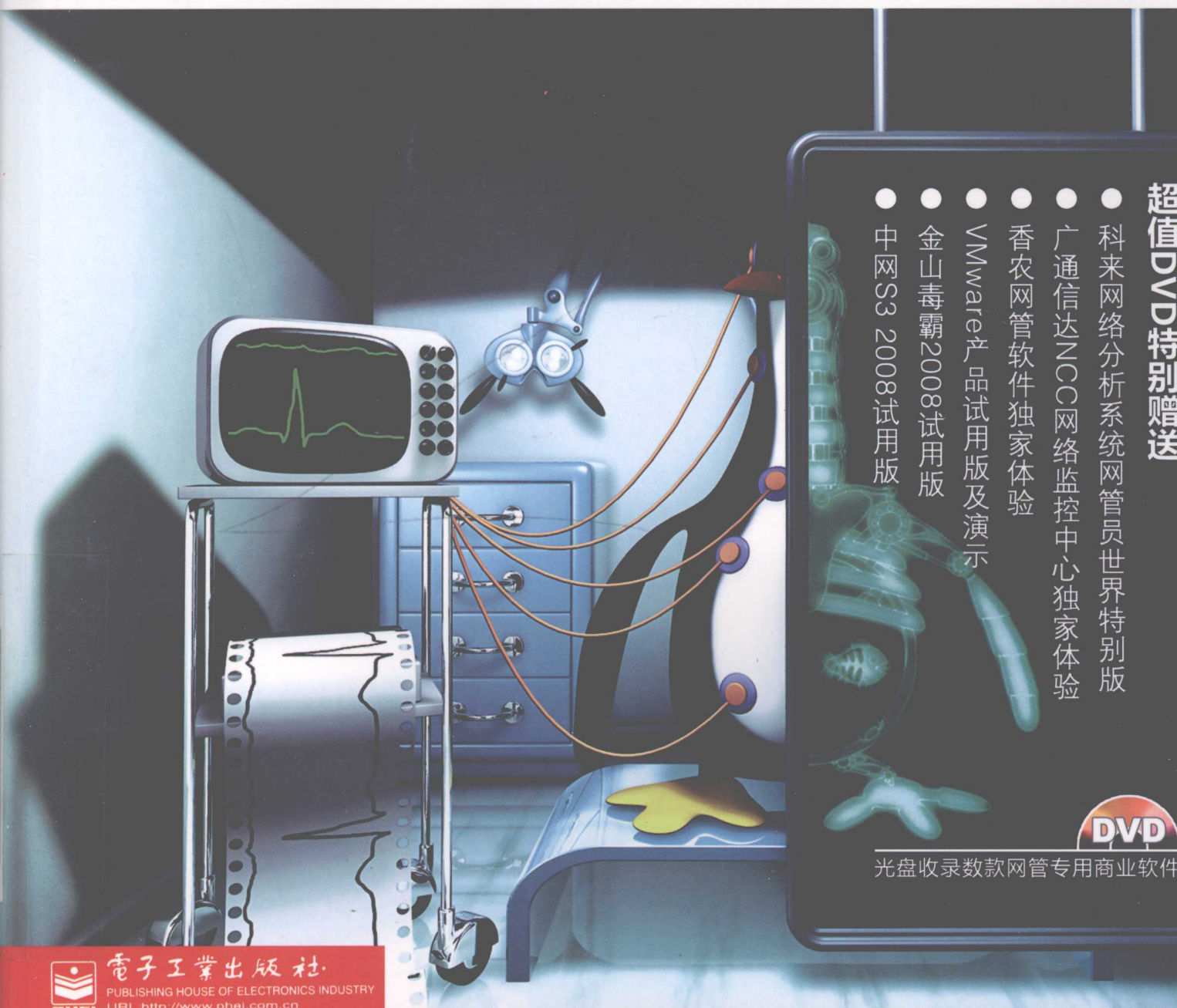
编与优选全年24期杂志内容　数百篇精华文章与专题大放送

网管员世界

NETADMIN WORLD MAGAZINE

2008 超值精华本

《网管员世界》杂志社
飞思科技产品研发中心　编
监制



超值DVD特别赠送

- 科来网络分析系统网管员世界特别版
- 广通信达NCC网络监控中心独家体验
- 香农网管软件独家体验
- VMware产品试用版及演示
- 金山毒霸2008试用版
- 中网S3 2008试用版

DVD

光盘收录数款网管专用商业软件

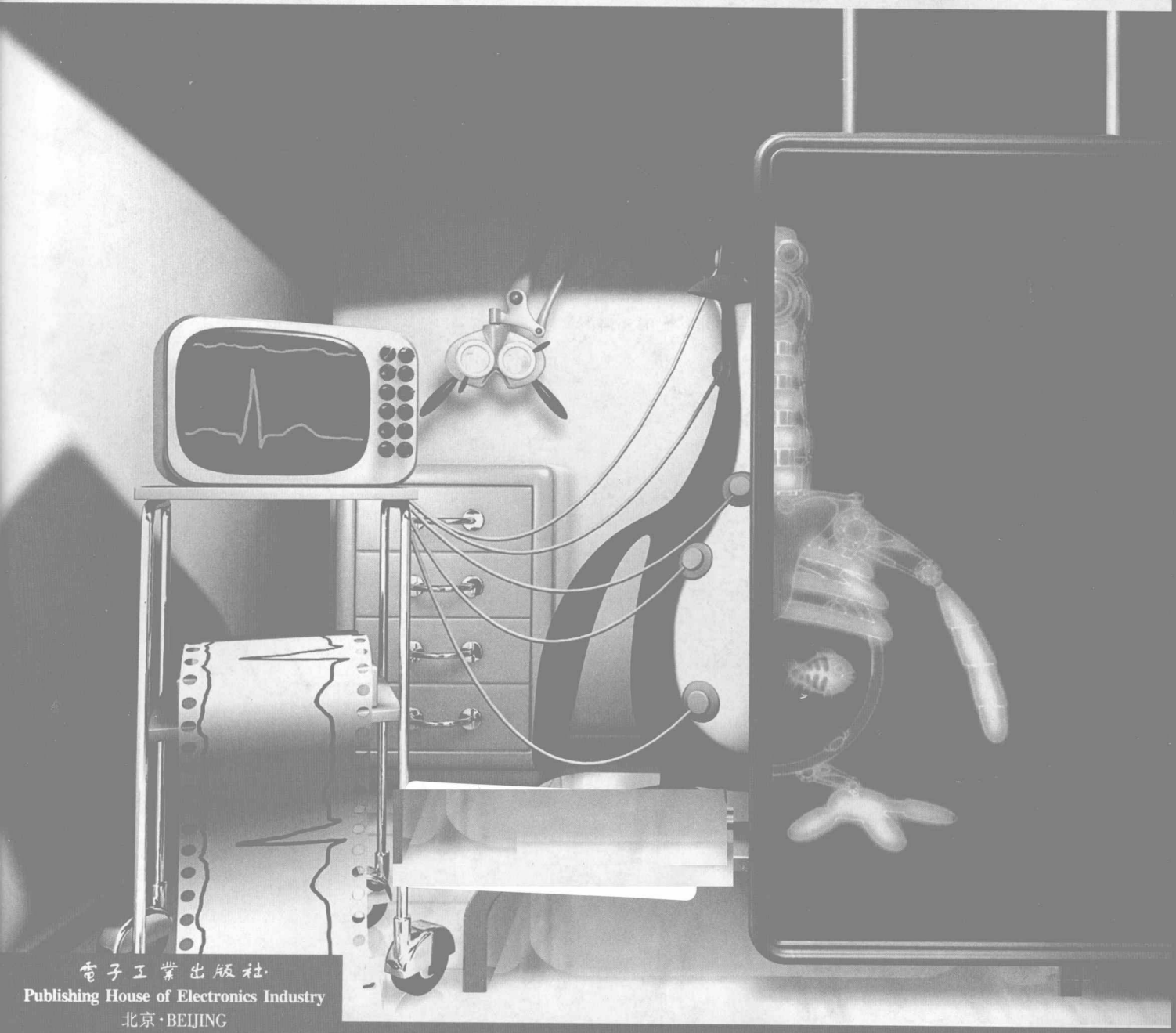
電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
URL:http://www.phei.com.cn

网管员世界

NETADMIN WORLD MAGAZINE

2008 超值精华本

《网管员世界》杂志社 编
飞思科技产品研发中心 监制



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

内容简介

《网管员世界》月刊是面向网络技术管理人员的实用性期刊。本书是2007年《网管员世界》各期内容的汇集，按照栏目分类进行汇总，内容详尽实用，保留价值高。全书分为管理维护、故障诊断、信息安全、桌面管理、有问有答5个板块，共精选数百篇实用、精彩的技术文章，是广大网管员不可多得的业务指导书。本书光盘内容包括金山毒霸2008试用版、香农网管软件试用版、广通信达NCC网络监控中心试用版、VMware产品试用版及演示、科来网络分析系统网管员世界特别版、中网S3 2008试用版。本书读者对象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应用与网络事业发展的人士。

本书适合作为广大网络管理员入门和提高的技术参考用书。

图书在版编目（CIP）数据

网管员世界2008超值精华本 / 《网管员世界》杂志社编.—北京：电子工业出版社，2008.4
ISBN 978-7-121-06214-8

I. 网… II.网… III.计算机网络－管理 IV.TP393.07

中国版本图书馆CIP数据核字（2008）第035634号

责任编辑：王树伟　李新承
印　　刷：北京智力达印刷有限公司
装　　订：三河市皇庄路通装订厂
出版发行：电子工业出版社
　　北京市海淀区万寿路173信箱　邮编：100036
开　　本：880×1230　1/16　印张：38　字数：1459.2千字
印　　次：2008年4月第1次印刷
印　　数：6 000册　　定价：59.80元（含光盘1张）

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

质量投诉请发邮件至zlts@phei.com.cn，盗版侵权举报请发邮件至dbqq@phei.com.cn。

服务热线：（010）88258888。

FOREWORD 前言

《网管员世界》作为一本专门面向网络管理技术人员的专业杂志，已经走过了 5 年的风雨历程，长期以来，《网管员世界》杂志一直以帮助企业提高企业 IT 基础设施运营水平、提高企业网管人员的管理水平为目标和宗旨，为企业的网络技术人员提供了一个技术和经验交流的平台，成为在网络管理技术人员中颇具影响力的 IT 专业媒体。为了更好地帮助广大网络技术人员提高网络管理技术水平，电子工业出版社与《网管员世界》杂志特别推出《〈网管员世界〉2008 超值精华本》，内容包括 2007 年全年《网管员世界》杂志“管理维护”、“故障诊断”、“信息安全”、“桌面管理”，“有问有答”等栏目中精彩文章的汇总。

- 管理维护：对于广大网络管理人员来说，网络管理和维护是他们重要的工作，网络管理维护的内容以大量精彩翔实的文章为广大网络管理人员管理和维护网络提供了鲜活的实例和参考，能够帮助网络管理技术人员完成从网络管理菜鸟到高手的转变。
- 故障诊断：收集了《网管员世界》杂志社创刊 5 年来在故障诊断栏目中的精华文章和优秀专题，既是网管员在日常工作中排障查错的工具手册，又是网管员提高网络管理水平的技术宝典。
- 信息安全：专门针对网络安全而推出的网络安全专业手册，文章来自《网管员世界》杂志攻防实战栏目，对网络管理人员增强网络安全意识，提高网络安全技能有着重要的指导作用。
- 桌面管理：针对网络管理人员需要了解的技术、技巧等方面进行全面介绍。
- 有问有答：汇集了网络管理、维护、排障方面遇到的典型问题，可以帮助网络管理技术人员迅速解决一些常见的网络问题，是网络管理人员可以随时随地查阅的问答宝典。

《网管员世界》杂志社

飞思科技产品研发中心

联系方式

咨询电话：（010）88254160　88254161-67

电子邮件：support@fecit.com.cn

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

通用网址：计算机图书、飞思、飞思教育、飞思科技、FECIT

CONTENTS 目录

第 1 章　管理维护

CONTENTS

第 2 章　故障诊断

CONTENTS

第 3 章　信息安全

CONTENTS

第 4 章　桌面管理

CONTENTS

第 5 章　有问有答

NetAdmin World 2008

第1章 管理维护

机房网吧两不误

河北/袁景涛

单位机房原来只对本单位的用户开放，使用“美萍网管大师”作服务器上的管理系统，工作站上安装“美萍电脑安全卫士”作客户端，实现对机房的管理工作。征得本地文化和公安部门的许可，休息期间，单位机房可对外开放。

按照要求，服务器上必须安装任子行 NET110 网吧安全管理系统、吉胜网络妙管服务端和刷卡器，工作站要安装任子行万象 2004 客户端软件，让所有外来人员实名刷卡才能上机。那么如何改造网络系统，让机房同时兼顾内外两种应用呢？

伪双系统解决用户登录问题

在服务器上同时安装“美萍网管大师”和“吉胜网络妙管家服务器端”软件，可以使用一台服务器作为两套管理系统的服务器。当在工作站同时安装“美萍电脑安全卫士”和“任子行万象 2004 客户端”软件时，出现了冲突现象，两种管理软件互相锁定，要逐一输入用户名和密码才能登录桌面，造成外来刷卡上机人员和本单位上机人员登录时都很不方便。

本打算在工作站上同时安装 Windows 98 和 Windows XP 两套系统来解决两种用户的登录问题，可是工作站大部分采用的是联想 AMD 闪龙品牌机，安装的是 Windows XP 操作系统，如果安装 Windows 98 操作系统，则兼容性和运行速度都不够理想。其他兼容机配置较低，安装的是 Windows 98 操作系统，如果安装 Windows XP 操作系统，运行速度又太慢，并且工作站的硬盘都只有区区的 40GB，剩余空间捉襟见肘，重新分区安装双操作系统工作量又很大，所以只能另想办法。

解决思路

“美萍电脑安全卫士”和“万象 2004 客户端”都是以程序的方式安装的，通过写入系统文件和修改注册表达到管理的目的，而这些关键修改都是在 C:\Windows 目录中进行的。如果在安装好 Windows XP 系统以后，把 Windows 目录重新复制一份，开机建立双启动菜单，使 Windows XP 系统进入不同的 Windows 目录，就相当于安装了两个 Windows XP 系统，在每个 Windows XP 系统中分别安装“美萍电脑安全卫士”和“任子行万象 2004 客户端”软件就不会出现冲突现象了。

所需软件

建立双启动菜单程序：maxdos，下载地址：www.maxdos.net。

修改注册表程序：Registry Workshop，下载地址：http://www.21hh.com/soft/29688.htm。

Windows XP 客户端解决方法

1. 优化系统

首先在 Windows XP 客户端安装好操作系统及所需要的软件，添加必要的通信协议，修改 IP 地址、DNS 和网关，连入局域网，保证局域网互通。接入 Internet，安装最新的 Flashplayer 播放插件，最后对系统进行彻底的优化。

2. 安装 MaxDos，添加多重启动菜单

运行 MaxDos 的安装程序，输入 Windows 菜单的启动等待时间，把默认的 2 秒钟修改为 30（MaxDos 最大只能设置 30 秒），给初次上机人员充足的阅读时间进行选择，再修改 MaxDos 的启动密码，不要留空，这样可以给网管人员留下 DOS 入口，方便进入 DOS 环境，对系统进行备份和恢复，或进行网络硬盘的克隆操作。

3. 修改多重启动菜单

在桌面上用鼠标右键单击“我的电脑”，从弹出的快捷菜单中选择【属性】命令，切换到“高级”选项卡，在“启动和故障恢复”栏中单击【设置】按钮，再单击“系统启动”栏中的【编辑】按钮，就会打开多重启动菜单。

“timeout=30”表示菜单等待时间为 30 秒，可以把它改得更长一些，如 180 秒。“operating systems”项表示可选择进入的不同操作系统，为了方便上机者把 multi(0)disk(0)rdisk(0)partition(1)\WINDOWS=“Microsoft Windows XP Professional” /noexecute=optin /fastdetect 中的“Microsoft Windows XP Professional”改为“持卡用户刷卡登录”。复制此字段中的 multi(0)disk(0)rdisk(0)partition(1)\WINDOWS=“持卡用户刷卡登录”到它的下一行，修改为 multi(0)disk(0)rdisk(0) partition(1)\WINDOWS1=“本单位美萍用户登录”。修改最后一行 C:\grldr=MaxDOS v5.7s 为 C:\grldr=管理人员 DOS 登录。最后选择【文件】→【保存】命令。修改前与修改后的 boot.ini 启动文件如图 1 所示。

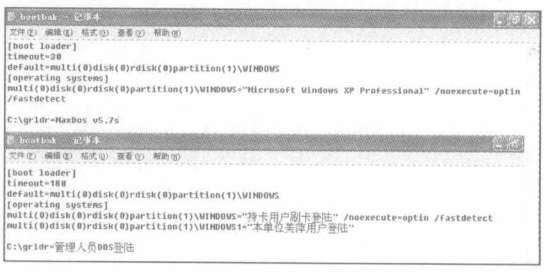


图 1　修改前后的 boot.ini 文件

4．复制 Windows 目录

拆下硬盘挂接到另一台计算机上，把挂接硬盘上的 C:\Windows 目录（大概 1.3GB 左右）进行原地复制粘贴。最后把“复件 Windows”改名为“Windows1”。

修改注册表建立第二个 Windows XP 系统。

把硬盘挂回原来的计算机，启动计算机后就会出现双重启动菜单。选择第二项“本单位美萍用户登录”进入 Windows XP 系统。安装注册表修改程序：RegistryWorkshop，并立即运行，选择【搜索】→【查找】命令，在“查找内容”中输入“c:\windows”（不含引号），然后进行“查找”，很快就会找到 1 000 个左右的项目。再选择【搜索】→【在查找结果 1 中替换】命令，在“替换为”栏中输入“c:\windows1”（不含引号），最后单击【替换】按钮完成第二个 Windows XP 注册表的修改。

5. 在两个 Windows XP 系统分别安装客户端软件

重新启动计算机，选择“持卡用户刷卡登录”进入 Windows XP 系统，安装“任子行万象 2004 客户端”软件。重新启动计算机，选择“本单位美萍用户登录”，安装“美萍电脑安全卫士”软件。

至此，两套客户端软件全部安装完毕。重新启动计算机，就会出现多重启动菜单，不同的上机人员可以自由地选择不同的登录方式。

Windows 98 客户端解决方法

Windows 98 工作站也可以参照 Windows XP 的方法进行修改。通过分析“美萍电脑安全卫士”和“任子行万象 2004 客户端”for Windows 98 版发现，并不像 for Windows XP 版本那样对系统文件及注册表修改得太多，它们只是简单地在注册表的启动项中添加键值，调用客户端主程序 smenu.exe（美萍安全卫士）和 client.exe（任子行万象 2004）达到开机自动运行的目的。

由于启动 Windows 98 系统时，会执行根目录下的 Autoexec.bat 文件，而进入桌面时又会运行程序组中“启动”栏中的项目，所以可以通过修改 Autoexe.bat 文件，有选择地把其中一个客户端主程序的快捷方式复制到程序组的“启动”项，达到自动运行的目的。

（1）首先安装 Windows 98 系统，再安装好各项驱动、DX9.0C 和 Flashplayer 插件，添加必要的通信协议，设置好 IP 地址、网关及 DNS 等。

（2）安装“美萍电脑安全卫士”，进入设置状态，选择【管理】→【启动】命令，再选择“取消 Windows 自动运行”，这样美萍电脑安全卫士就不会在注册表中添加自动运行项了。同时设置好相关的参数，如机器号和密码等，保存设置参数，退出美萍管理系统。打开 C:\smenu 目录，创建主程序 Smenu.exe 的快捷方式 Smenu.lnk。

（3）安装“任子行万象 2004 客户端”软件，进入设置状态，在“一般设置”中取消选择“客户端随系统同时启动”，同时还要设置好其他相关的选项。打开 C:\Octopus 文件夹，创建主程序 Client.exe 的快捷方式 Client.lnk。

（4）编辑 Autoexec.bat 文件。在 C 盘根目录下找到 Autoexe.bat 文件，取消其隐藏和只读属性。双击并用记事本打开进行编辑。

```
@echo off
c:\windows\command\pbios
c:\windows\command\font16
c:\windows\command\hzvio95

echo
****************************************
******
echo      *              欢      迎
光      临                *
echo      *如果您有任子行磁卡，请在键盘上按“Y”
键刷卡登录。*
echo      *如果您没有磁卡，请在键盘上按“N”键
进入美萍登录。*
echo
****************************************
******

choice /c:y，n /n /t:y，180
if errorlevel 2 goto no
if errorlevel 1 goto yes

:yes
Del c:\Windows\StartM~1\ Programs\启动\ Client.lnk
Del c:\ Windows\StartM~1\ Programs\启动\ smenu.lnk
copy C:\Octopus\Client.lnk C:\ Windows \StartM~1\
Programs\启动
goto end

:no
Del c:\Windows\StartM~1\ Programs\启动\ smenu.lnk
Del c:\ Windows\StartM~1\ Programs\启动\ Client.lnk
copy C:\smenu\smenu.lnk C:\ Windows \StartM~1\
Programs\启动
goto end
:end
```

简要说明：首先执行 C:\windows\command 目录中的 pbios、font16 和 hzvio95 文件，调入 Windows 98 系统自带的 Windows 95 中文系统，以便显示中文说明。然后显示“欢迎光临”及登录说明文字。系统预留 180 秒的时间等待输入“Y”或“N”（超时将自动执行“Y”选项）。输入“Y”，则执行 Yes 字段，删除 C:\ WINDOWS\StartM~1\Programs\启动中原

来可能存在的 Client.lnk 和 smenu.lnk 快捷方式，再复制 C:\Octopus\Client.lnk 到“启动”组中，进入系统时就会启动“任子行万象 2004”软件的管理系统；输入“N”，则执行 No 字段，同样先删除 C:\WINDOWS\StartM~1\ Programs\启动中可能存在的 Client.lnk 和 smenu.lnk 快捷方式，再复制 C:\smenu\smenu.lnk 到“启动”组中，进入系统时就会启动“美萍电脑安全卫士”软件的管理系统。

最后保存修改过的 Autoexec. Bat 文件，并恢复其隐藏和只读属性。

重新启动 Windows 98 系统，画面闪过之后就会出现登录说明（见图 2），输入“Y”或“N”即可登录相应的管理系统。

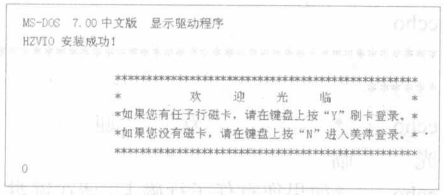


图 2 登录说明

注意事项

（1）Windows XP 系统并不是真正意义上的两个独立的操作系统，它们有共用的桌面和程序组，也有相对独立的注册表和系统文件。所以以后安装软件时可以先在一个 Windows XP 系统中安装成功，重启进入另一个 Windows XP 系统中直接运行新软件的主程序。如果不能直接运行，可再次运行安装程序，安装路径选择原来 Windows XP 系统中的安装位置。

（2）在装有 Windows XP 系统的计算机中，如果进入桌面时无法加载输入法图标，可以打开注册表编辑器，依次展开HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ Windows \CurrentVersion\Run，在 RUN 键下新建字符串值“ctfmon.exe”，数据数值输入 c:\Windows\system32\ctfmon.exe 即可解决输入法图标丢失的问题。

（3）两套管理软件都会在桌面上创建快捷方式，可直接删除这些快捷方式，防止用户误点击而进入另一套管理系统。

（4）如果要安装“还原精灵”等还原类的软件，要把 Windows XP 系统看做多个系统，分别进入两个 Windows XP 系统中进行安装。而 Windows 98 系统只需看做一个操作系统。

（5）“美萍电脑安全卫士”和“任子行万象 2004”软件都有各自的系统漏洞，要防止上机人员及第三方软件对管理系统进行破坏。

IPSec 与 NAT 共存

无锡/陶琦 初怀远

NAT 通常是将内部私有地址转换为全球公有地址，一般位于网络边缘的路由器和防火墙设备都支持这种功能。它有两种映射方式，一种是私有地址对公有地址间的一对一或多对一映射，另一种是多个私有地址到一个公有地址和其端口间的映射，称为 NAPT。

IPSec（IP Security Protocol）是保证企业网资源安全的一种技术，通过在 IP 层实现加密和认证等多种安全技术，极大地提高了 TCP/IP 的安全性。与其他技术相比，由于 IPSec 整个协议在 IP 层上实现，上层应用不必进行任何修改，加上 IPSec 在实现安全策略上的灵活性，使 IPSec 的通用性更好，实施效率更高，后期维护工作量和成本更低，从而广泛地应用于路由器及安全网关上。

IPSec 提供了两种安全机制：认证和加密。认证机制使 IP 通信的数据接收方能够确认数据发送方的真实身份及数据在传输过程中是否遭到篡改。加密机制通过对数据进行编码来保证数据的机密性，以防数据在传输过程中被窃听。IPSec 协议组包含 Authentication Header（AH）、Encapsulating Security Payload（ESP）和 Internet Key Exchange（IKE）协议。

（1）Authentication Header（AH）协议结构：AH 协议为 IP 通信提供数据源认证、数据完整性和反重播保证，它能保护通信免受篡改，但不能防止窃听，适用于传输非机密数据。AH 的工作原理是在每一个数据包上添加一个身份验证报头。AH 报头位置在 IP 报头和传输层协议报头之间。

（2）Encapsulating Security Payload（ESP）协议结构：ESP 为 IP 数据包提供完整性检查、认证和加密，可以看做是“超级 AH”，因为它提供机密性并可防止篡改。ESP 可以单独使用，也可以和 AH 结合使用。一般 ESP 不对整个数据包加密，而是只加密 IP 包的有效载荷部分，不包括 IP 头。但在端对端的隧道通信中，ESP 需要对整个数据包加密。ESP 报头如图 1 所示。

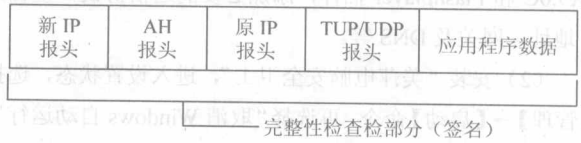


图 1 ESP 报头形式

（3）Internet Key Exchange（IKE）协议结构：Internet 密钥交换（IKE）协议是 IPSec 安全关联（SA）在协商它们的

保护套件和交换签名或加密密钥时所遵循的机制。IKE 定义了双方交流策略信息的方式和构建并交换身份验证消息的方式。IKE 是由另外三种协议（ISAKMP：Internet 安全关联和密钥管理协议、Oakley 和 SKEME）混合而成的一种协议。

IKE 使用了两个阶段的 ISAKMP。第一阶段，协商创建一个通信信道（IKE SA），并对该信道进行验证，为双方进一步地 IKE 通信提供机密性、消息完整性及消息源验证服务。第二阶段，使用已建立的 IKE SA 建立 IPSec SA。

IPSec 与 NAT 冲突分析

IPSec 的设计和 NAT 存在冲突，它主要表现在以下几点。

（1）IPSec 中的 AH 协议和 NAT 存在冲突。AH 用验证算法保护包括 IP 头在内的整个 IP 报文不被修改，如果到达执行 NAT 功能的网关，NAT 需要修改 IP 报文，经过修改的报文到达对方后因无法通过验证会被丢弃。ESP 协议由于只保护 IP 载荷，所以如果修改 IP 地址不会影响通信。

IPSec 和 NAT 的校验也存在冲突。TCP/UDP/SCTP 中的校验都是依赖于 IP 源目的地址的，它需要计算“伪头”（即 IP 源、目的地址加上 TCP 头），通过 NAT 和 NAPT 后由于地址和端口被修改，校验要重新计算。如果对源报文进行了完整性或密码保护，报文到达对方后，验证就会出现不一致，对方 IPSec 将丢弃此报文，除非 IPSec 使用通道模式、IPSec/GRE 模式或不计算校验才能避免报文丢弃。即使这样也仍然存在问题，在 IKE 中最普遍、最基本的验证方法就是预共享密钥，这种方法依赖于源 IP 地址，所以也与 NAT 冲突，解决办法就是使用另外的验证方法，如 X.509。

（2）IKE 的协商端口固定为 500，这与 NAPT 有冲突。当多个主机在一台 NAT 设备后与同一目的主机协商 IKE SA 时，从这一目的主机来的报文需要由 NAPT 分路到不同的源主机，典型的做法是转换内部主机 IKE 的 UDP 源端口。但是在重建密钥时会出现不可知错误，除非修改的源端口在重建密钥时用作目的端口。

（3）当多个主机在一个 NAT 设备后与同一个目标主机协商安全策略库（SPD）的内容时，很可能发送到错误的 SA（安全关联）中，因为对目标主机来说，这些 SA 好像是相同的，它们都是存在于同一对主机间的。

IPSec 和 NAT 共存解决方案

NAT 广泛应用于家庭、宾馆和网吧，如果不解决该问题，许多使用 IP 隧道模式的 VPN 客户就无法从家庭或办公室接入因特网。同样，使用 IPSec 通道模式保护的 TCP / UDP 流，也无法进行对等体到对等体、Server 到 Server 的交换。解决方法有以下几种。

方案 1：如果能够在一个设备中实现 IPSec 和 NAT，那么将 NAT 放在前面处理，而 IPSec 放在后面处理，就可以避免冲突。但有些情况下，NAT 不能放在 IPSec 前处理。

方案 2：用 RSIP 替代 NAT 解决 IP 地址短缺的问题。RSIP 是将一个拥有合法 IP 的服务器放在私有地址域内，与 NAT 工作原理不同，它不是采用替换 IP 来工作，而是允许域内主机直接在几个地址域内同时通信。在通信过程中，RSIP 对 IP 载荷进行的修改不会削弱 IPSec 这类对 NAT 敏感的协议的功能，当一个 RSIP 客户机想要在自己所在的地址域外通信时，首先在 RSIP 网关上登记，RSIP 网关给它分配一个合法的 IP 地址（或一个 IP 地址和端 E1），RSIP 客户使用该地址为源地址和外部设备通信，直到该地址过期或被更新。

实际处理起来并不是这么简单，RSIP 还要将此数据报文封装在源地址为其私有 IP 的报头内，封装方式可以用 IP-in-IP，GRE 或 L2TP。数据报文首先传给 RSIP 网关，网关将外面的报头脱掉，然后将报文发出去。

然而，RSIP 也存在一定的问题，RSIP 使用的是一个公有端口分路进来的报文流，当多个内部主机使用一个 RSIP 网关和同一个外部主机传送 ESP 时，由于 ESP 流是加密的，会出现分路冲突问题，所以，必须要使用另外的标识。幸运的是每个安全联盟都有不同的 SPI，由于 SPI 的唯一性只针对一个主机，为了确保对一个 RSIP 网关的唯一性，选用 SPI+协议（AH 或 ESP）+目的 IP 作为标识。

同样的问题会出现在 IKE 协商安全联盟时，由于使用知名端口 500，当多台主机使用一个 RSIP 网关时，可能发生冲突，所以，这里使用另外的一个新标识：初始化 Cookie+目标端口+目标地址。在重建密钥时可能仍然会出现问题，因为通常重建密钥用到的 Cookie 与以前数据流中所用的不同。

使用 RSIP 替代 NAT 解决了分路和 SPD 重叠问题，并且与类似隐藏 IP 地址这样的协议都兼容，所以既适合于企业，也适合于家庭使用。通过将 IKE 和 IPSec 封在隧道里，RSIP 避免了对 IKE 和 IPsec 协议的修改，既适合现有的 AH 和 ESP 协议，也适合隧道和传输两种方式。但是，为了解决 IKE 重建密钥时的分路传输问题，RSIP 需要改动 IKE 的源端口，这就不能保证与现有的 IPSec 实现兼容。

方案 3：这种方法的核心思想是使用 UDP 封装 ESP。当报文交给网关后，网关照旧进行 NAT、NAPT 转换，它不会破坏 ESP 的加密或验证。之所以使用 UDP 是因为 UDP 提供了最小标准的封装，8bit 就够了。如果换成 TCP 封装，则需要 20bit，而且 UDP 是面向无连接协议的，TCP 的建链和拆链过程会引入诸如 RESET 攻击这类影响 IPSec 性能的负效果。

这种方法只适用 ESP 协议，既然 ESP 被 UDP 封装了，就要求网关到网关、客户到客户、网关到客户都能相互识别并将 UDP 头脱去，对于同一厂家的产品可能还可以实现，但是对不同厂家在实现上会有些困难。解决的方法是 IKE 对等体将交换一个定义好的值，来确定对方是否支持 UDP ESP 封装，如果双方都支持，对等体就会探测负荷中是否运用了这种封装。

由于 IKE 对等体已经使用了 UDP 的 500 号端口，所以

这里也沿用这一端口，可以避免在防火墙的过滤规则中再多开一个漏洞。发送者会将 UDP 后的第一个 8bit 设置为 0，该位置在 IKE 中是初始 Cookie 的位置。接收者就可以在都使用 500 号端口的情况下，区分是 IKE 还是 UDP 封装下的 ESP。

综上所述，为了解决 IPSec 和 NAT 的共存问题，主要有三种解决方法，一种是对 IPSec 协议或 NAT 进行一定的修改，但实现要很小心，因为很容易引入实现带来的错误。第二种是使用 NAT 的替代协议 RSIP，这种方法较为全面地解决了 IPSec 和 NAT 的兼容问题，但是它的实现相对较复杂，而且需要对原有设备进行较大的改动。第三种是使用 UDP 封装 ESP 载荷，这种方法不需要对 IPSec 或 IKE 进行修改，实现最为简单。

加固 Web 服务器

新疆/沈兵　张静

在系统默认配置下，IIS 使用的是“HTTP”以明文形式传输数据，没有采用任何加密手段，传输的重要数据很容易被窃取。这对于一些安全性要求高的网站来说，是远远不够的。如何保证网站数据的安全呢？

为了保证重要数据的万无一失，IIS 提供了 SSL 安全加密机制。SSL（Security Socket Layer）的中文全称是“加密套接字协议层”，基于 TCP，位于 HTTP 协议层和 TCP 协议层之间，使用 HTTPS 能够对信用卡和个人信息提供较强的保护。SSL 在客户和服务器之间建立一条加密通道，确保所传输的数据不被非法窃取。

应用了 SSL 加密机制后，IIS 服务器的数据通信过程如下：首先客户端与 IIS 服务器建立通信连接，接着 IIS 把数字证书与公用密钥发给客户端。然后使用该公共密钥对客户端的会话密钥进行加密后，传递给 IIS 服务器，服务器端接收后用私人密钥进行解密，这时就在客户端和 IIS 服务器间创建了一条安全数据通道，只有被 IIS 服务器允许的客户才能与其进行通信，从而实现 Web 服务器与客户端建立安全通信。

下面以 Windows 2003 系统环境为例进行实验，其中安装 Internet 信息服务（IIS）管理器略。

生成证书请求文件

选择【控制面板】→【管理工具】→【Internet 信息服务（IIS）管理器】命令，展开“网站”目录，建立自己的站点（本人建立了站点 myweb），并将站点的主目录设置为 E:\SSLWEB，将站点的默认文档设置为 E:\SSLWEB 目录下的 Test.asp（网站主页）文件。用鼠标右键单击站点 myweb，选择【属性】命令，在“目录安全性”中单击【服务器证书】按钮。选择“新建证书”，单击【下一步】按钮。

选择“现在准备证书请求，但稍后发送”，在“名称”栏中为该证书起个名称，在“位长”下拉列表框中选择“密钥的位长”选项。接着设置证书的单位、部门和地理信息，在站点“公用名称栏”中输入该网站的域名，然后指定证书请求文件的保存位置，这里笔者将该证书请求文本文件保存在“e:\ SSLWEB\certreq.txt”中。这样就完成了证书请求文件的生成。

注意

密码位长不能设置得过大，否则会影响通信质量。

申请 IIS 网站证书

完成了证书请求文件的生成后，就可以开始申请 IIS 网站证书了。但该过程需要证书服务 CA（Certificate Services）的支持。

1. 安装证书服务 CA

在“控制面板”中运行“添加或删除程序”，单击【添加/删除 Windows 组件】按钮，在“Windows 组件向导”对话框中选择“证书服务”复选框，接下来选择 CA 类型，这里笔者选择了“独立根 CA”，然后为该 CA 服务器起个名称（本实验中为 wlaqlab），设置证书的有效期限，建议使用默认值“5 年”即可。最后指定证书数据库和证书数据库日志的位置后，就完成了证书服务的安装。

2. 申请 IIS 网站证书

完成了证书服务的安装后，就能开始申请 IIS 网站证书了。运行 Internet Explorer 浏览器，在地址栏中输入“http://localhost/CertSrv/default.asp”。接着在“Microsoft 证书服务”欢迎窗口中单击“申请一个证书”链接，在证书申请类型中单击“高级证书申请”链接，在高级证书申请窗口中单击“使用 BASE64 编码的 CMC 或 PKCS＃10 文件提交…”链接，接着将证书请求文件（e:\zhjlab\certreq.txt）的内容复制到“保存的申请”文本框中，最后单击【提交】按钮。

颁发 IIS 网站证书

虽然完成了 IIS 网站证书的申请，但这时它还处于挂起状态，需要颁发后才能生效。在“控制面板→管理工具”中运行“证书颁发机构”程序，在“证书颁发机构”左侧展开目录，选择“挂起的申请”选项，在右侧找到刚才申请的证书，用鼠标右键单击该证书，选择【所有任务】→【颁发】命令。

将证书导出为 IIS 可导入的证书

在 CA 中选择“颁发的证书”目录，打开刚刚颁发成功的证书。在“证书”对话框中切换到“详细信息”选项卡。

单击【复制到文件】按钮，弹出证书导出对话框，一路单击【下一步】按钮。在“要导出的文件”栏中指定文件名，这里笔者保存证书路径为“e:\ SSLWEB\webex.cer”。最后单击【完成】按钮。

导入 IIS 网站证书

在 IIS 管理器的“目录安全性”选项卡中，单击【服务器证书】按钮，这时弹出“挂起的证书请求”对话框，选择“处理挂起的请求并安装证书”，单击【下一步】按钮，指定刚才导出的 IIS 网站证书文件的位置，接着指定 SSL 使用的端口 443，最后单击【完成】按钮。

配置 IIS 服务器

完成证书的导入后，IIS 网站还没有启用 SSL 安全加密功能，需要对 IIS 服务器进行配置。

在“目录安全性”选项卡中，单击安全通信栏的【编辑】按钮，选择“要求安全通道（SSL）”和“要求 128 位加密”，单击【确定】按钮即可。如果需要验证客户端，则需要在 CA 中申请一个 Web 浏览器证书。

接着单击“身份验证和访问控制”栏中的【编辑】按钮，在对话框中取消选择“启用匿名访问”和“集成 Windows 身份验证”，单击【确定】按钮。

实验结果

现在已经大功告成了，在浏览器地址栏中输入 https://202.117.10.170/ （别忘了将 IP 换成自己的 IP），出现的界面如图 1 所示。在图 1 所示中可以看见窗口下方有一把锁的标记，说明已经成功建立 SSL 连接。

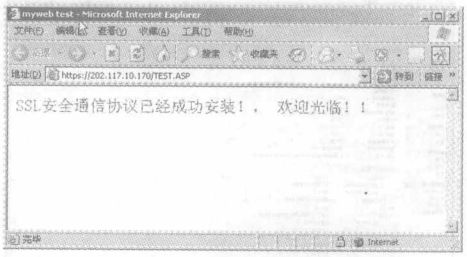


图 1　登录界面

一台 PC 建集群

贵州/肖荣江

服务器集群允许客户端在出现故障和计划中的暂停时，依然能够访问应用程序和资源。如果集群中的某一台服务器无法使用，资源可转移到其他集群节点。运用 Virtual Server 2005 R2，只需要一台高性能的 PC，就可以构建出虚拟集群系统。

由于集群系统的费用高昂，很少有人能够拥有一个完整的集群调试环境。而实际工作中的集群系统又与普通的独立服务器系统有很多不同之处。应用微软虚拟服务器技术，只需一台普通 PC，就可以搭建一个虚拟的集群系统。该虚拟集群系统可用于旧应用系统的迁徙、学习集群技术及支持集群的软件系统的开发和测试等。

集群环境

在这个简单的集群中（见图 1）只有两个节点，即两台虚拟机，均配置为成员服务器。两个节点都连接到一个虚拟的、共享的集群存储设备上。每个节点有两块虚拟网卡，分别设置两个 IP 地址，其中一个地址用于外部通信，连接局域网中的其他计算机。另一个地址则用于集群节点间的内部通信，两个集群节点构成一个内部网络，节点之间相互传递心跳信号，向对方通告自身的状态。

为了降低复杂程度，域控制器使用局域网中已经配置好的服务器。也可以用第三台虚拟机作为域控制器，构建一个独立的集群应用环境。

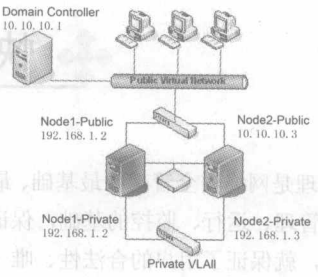


图 1　集群环境

搭建过程

1. 创建共享仲裁磁盘

在 Virtual Server 2005 R2 中，集群的仲裁盘必须使用固定大小的虚拟硬盘。此外，对于 NTFS 文件系统，仲裁盘的最佳大小为 500MB。

2. 创建并配置虚拟集群节点 1

创建一台虚拟机，命名为 Node1，并为其分配 256MB 内存。

然后创建一个虚拟网络，起名为 Private。该虚拟网络就是由两台集群虚拟机所组成的。注意，应禁用虚拟 DHCP 服务器，默认情况下是启用的。

接着添加两个虚拟网络适配器，一个选择“External