网管天下

张金荣　刘晓辉　编　著

- IP/MAC地址工具
- 网络查看和搜索工具
- 网络性能和带宽测试工具
- 网络安全测试工具
- 专业备份/恢复软件

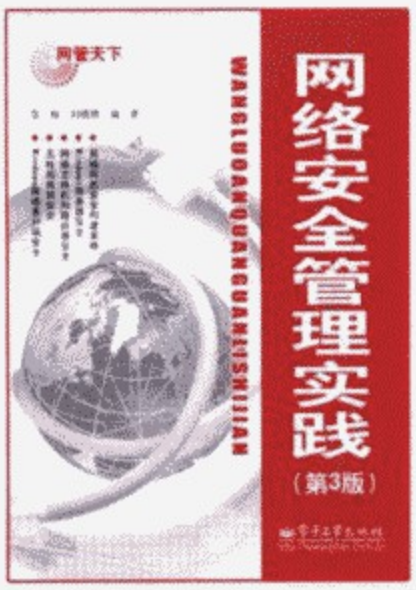
WANGLUOGUANLIGONGJU SHIYONGXIANGJIE

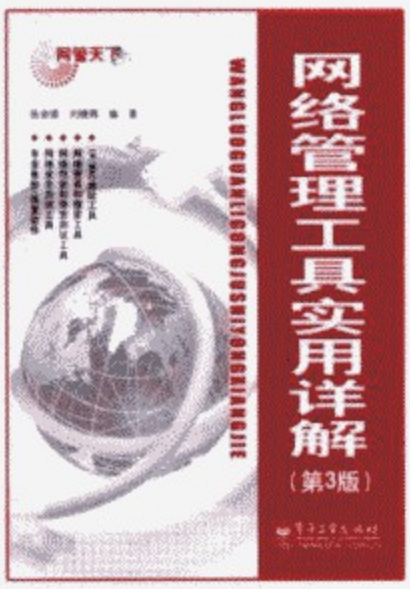
网络管理工具实用详解

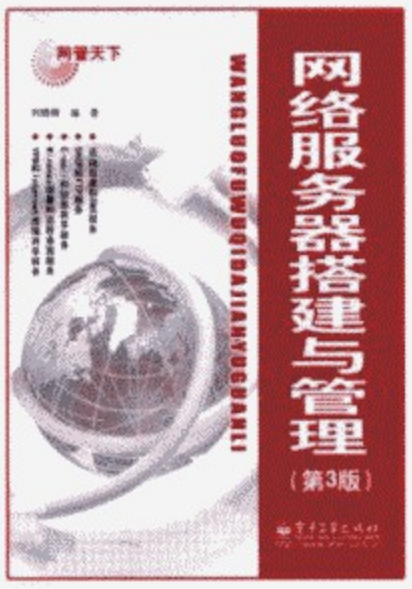
（第3版）

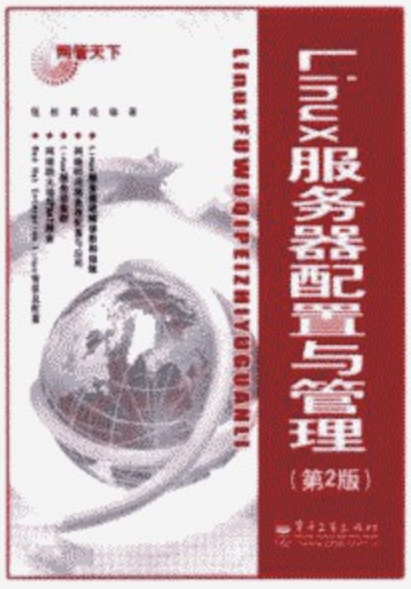
電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

网管天下









一套由国内资深网络专家写给网络建设与管理人员的应用实践手册，能够全方位地解决网络建设与管理中的各种实际问题。

上架建议 网络技术

PHEI

天启星
http://www.tqxbook.com

策划编辑：郭鹏飞
责任编辑：鄂卫华
封面设计：王　嵩

ISBN 978-7-121-14805-7

9 787121 148057 >

定价：59.80元

本书贴有激光防伪标志，凡没有防伪标志者，属盗版图书。

网管天下

网络安全管理实践（第3版）

WANGLUOGUANLIGONGJUSHIYONG

张金荣　刘晓辉　编　著

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

内 容 简 介

本书全面深入地介绍了局域网中最常用的安全管理技术及不同类型网络安全方案的规划与设计，主要内容包括服务器系统安全、用户账户安全、共享资源安全、局域网接入安全、局域网传输安全、Internet 接入安全、网络设备安全以及网络数据安全等，基本涵盖了当前主流局域网安全管理涉及的方方面面，可以满足不同领域用户快速打造安全网络的需求。

本书主要面向具有一定基础的中高级用户，尤其是热衷于系统安全和网络安全，喜欢探索尝试新技术的计算机爱好者。通过阅读本书，读者能够全面掌握局域网安全管理的方案设计与实施，提升网络安全技术水平，迅速成长为出色的网络安全管理员和网络安全工程师。

本书为“网管天下”系列《网络安全管理实践》的第 3 版，结合读者反馈意见和建议以及当前网络安全技术发展趋势，在原有基础上补充了大量的新内容、新技术和新案例。

未经许可，不得以任何方式复制或抄袭本书之部分或全部内容。
版权所有，侵权必究。

图书在版编目(CIP)数据

网络安全管理实践 / 张栋，刘晓辉编著. —3 版. —北京：电子工业出版社，2012.1
（网管天下）
ISBN 978-7-121-14806-4

Ⅰ. ①网… Ⅱ. ①张… ②刘… Ⅲ. ①计算机网络－安全技术 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2011)第 207906 号

策划编辑：郭鹏飞
责任编辑：鄂卫华
印　　刷：三河市鑫金马印装有限公司
装　　订：三河市鑫金马印装有限公司
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：787×1092　1/16　印张：31　字数：794 千字
印　　次：2012 年 1 月第 1 次印刷
定　　价：59.80 元

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。

前　言

关于《网管天下》丛书

《网管天下》丛书是一套由国内资深网络专家写给网络建设与管理人员的应用实践手册，其目的在于帮助初、中级网络管理员，全方位地解决网络建设与管理中的各种实际问题，包括综合布线设计、实施与测试，网络设计与设备选择、连接与配置，网络服务搭建、配置与监控，网络故障诊断、排除与预防，网络安全设计、配置与监视，网管工具选择、使用与技巧，网络设备、服务和客户管理的自动化等诸多方面；囊括了网络管理中几乎所有的内容，其目的在于将网络理论与实际应用相结合，提高读者分析和解决具体问题的能力，将所学变为所用，将书本知识变为操作技能。

《网管天下》前两版，取得了不错的销售业绩，在同类图书中名列前茅，受到了广大读者朋友的喜爱。《网络管理工具实用详解》一书，得到了中国台湾出版业同行的认可，在中国台湾也取得了不错的销售业绩。随着网络技术的不断进步，新的网络设备不断推出、新的网络技术不断成熟、新的管理软件不断升级、新的网络应用也不断丰富，原来图书中的有些内容已经不能适应新设备、新技术、新软件和新应用的需求。因此，在保留图书原有写作风格的基础上，对目录结构做了进一步优化，对过时的内容进行了大幅度的更新，隆重推出了《网管天下》第 3 版。

本丛书具有以下特点。

1. 授之以渔而不是授之于鱼。紧贴网络实际情况，从真实的网络案例入手，为网络管理员提供全面的网络设计、网络组建、网络管理和网络维护等解决方案，以提高读者的分析能力、动手能力和解决实际问题的能力。

2. 实用才是硬道理。为网络管理员提供彻底的、具有建设性的网络设计、网络组建和配置解决方案，真正解决网络建设和网络管理中的实际问题，突出实用性、针对性、技术性、经典性，举案说“法”、举一反三。

3. 理论新、技术新、设备新、案例新。所有的应用案例都发生在最近两年，而且案例中只涉及最主流的、最成熟的设备和技术，以及最新版本的软件，不再讨论那些已被淘汰或面临淘汰的东西，从而力求反映网络的新技术和新潮流。不仅让读者学了就能用，而且还可以拥有三年左右的“保鲜”期。

关于本书

网络在方便日常生活，提高工作效率、提升生活质量的同时，也有其危险的一面，轻则

使自己正常的工作、生活和学习受到影响，重则可能会危及财产和生命。由于网络安全事件，致使企业蒙受巨大经济损失的案例屡见不鲜，并且在最近几年正在朝着频率高、数额大的方向发展。相关专家曾经预言，应用与安全将成为网络技术发展的两大方向，网络安全问题已经引起了世界各国的普遍关注，我国正在逐步加大高等教育以及相关技术培训中有关网络安全技术知识的渗透与应用，从最初的专业化向普及化推广发展。

从技术上讲，网络安全是一门涉及计算机科学、网络技术、通信技术、信息加密、网络管理等多个领域的综合性学科。网络安全管理员的基本要求是能够根据既定网络架构给出相应的安全解决方案，随时掌握网络运行情况，能够熟练运用各种安全防护措施确保目标网络的稳定运行。在实际应用中，影响网络安全的因素有很多，除了网络自身的不安全性意外，病毒、人为因素、误操作等各种行为都可能导致漏洞的产生，如果恶意用户趁虚而入将直接威胁网络的安全运行，甚至造成数据丢失和网络瘫痪。

本书由张栋、刘晓辉编著，李海宁、陈志成、田俊乐、王淑江、王春海、赵卫东、刘淑梅、马倩、杨伏龙、李文俊、石长征、王同明、郭腾、白华、刘媛、莫展宏、由磊等也参与了部分章节的编写工作。笔者长期从事网络教学、实验和管理工作，规划、设计、论证、实施并验收过多个大中型网络建设项目，具有较高的理论水平和丰富的实践经验。曾经出版过近百部计算机类图书，均以易读、易学且实用的特点受到众多读者的一致好评。本书是笔者的又一呕心沥血之作，希望能对读者的网络搭建及管理工作有所帮助。

如果您在配置网络和管理网络时遇到了疑问或问题，或者对本书有什么看法，欢迎发送E-mail 至 hslxh@163.com，进行讨论或寻求支持。由于笔者水平有限，书中难免有疏漏之处，敬请专家和读者不吝赐教。

编著者

2011 年 7 月

目录

CONTENTS

第 1 章　网络安全规划与设计 1

1.1　网络系统安全风险分析 1
1.1.1　物理安全风险分析 1
1.1.2　网络平台的安全风险分析 2
1.1.3　系统的安全风险分析 2
1.1.4　应用的安全风险分析 2
1.1.5　管理的安全风险分析 3
1.1.6　其他安全风险 3
1.2　安全需求与安全目标 5
1.2.1　安全需求 5
1.2.2　网络安全策略 5
1.2.3　系统安全目标 6
1.3　网络安全规划 6
1.3.1　网络安全规划原则 6
1.3.2　网络安全技术规划 8
1.3.3　网络安全设备规划 10
1.4　网络安全体系结构 16
1.4.1　物理安全 16
1.4.2　网络结构规划 17
1.4.3　系统安全 19
1.4.4　信息安全 20
1.4.5　应用安全 20
1.5　安 全 管 理 21
1.5.1　安全管理规范 21
1.5.2　网络安全管理 22

第 2 章　Windows Server 2008 R2 系统安全 23

2.1　Windows Server 2008 R2 安装安全 23
2.1.1　Windows 安装安全指南 23
2.1.2　下载和安装更新程序 24
2.2　Windows Server 2008 R2 基本安全 26
2.2.1　Internet 防火墙 26
2.2.2　高级安全 Windows 防火墙 28
2.2.3　安全配置向导 32
2.2.4　安全配置和分析 39
2.3　Windows Server 2008 R2 被动防御安全 44
2.3.1　配置防病毒系统 44
2.3.2　配置防间谍系统 47
2.4　Windows Server 2008 R2 系统安全 49
2.4.1　应用程序安全 50
2.4.2　系统服务安全 50
2.4.3　禁止注册表远程访问 53
2.4.4　审核策略 54
2.5　Windows Server 2008 R2 系统漏洞安全 55
2.5.1　系统漏洞概述 55
2.5.2　MBSA 的主要功能 56
2.5.3　使用 MBSA 扫描本地

系统漏洞 57

第 3 章　网络用户账户安全 61

3.1　Active Directory 安全管理 61
3.1.1　全局编录 61
3.1.2　操作主机 63
3.1.3　功能级别 70
3.1.4　信任关系 71
3.1.5　权限委派 79
3.1.6　部署只读域控制器 83
3.2　系统管理员账户安全 85
3.2.1　更改超级管理员账户 85
3.2.2　禁用 Administrator 账户 86
3.2.3　设置陷阱账户 87
3.2.4　禁用 Guest 账户 87
3.2.5　减少管理员组成员 88
3.2.6　系统管理员口令设置 88
3.3　用户账户安全 90
3.3.1　重设用户密码与密码使用期限 90
3.3.2　限制用户登录时间 91
3.3.3　限制用户登录工作站 92
3.3.4　用户账户策略 92
3.3.5　审核策略 94
3.3.6　用户组安全 98
3.3.7　系统账号数据库 100
3.3.8　分配本地用户管理权限 101

第 4 章　文件系统与共享资源安全 105

4.1　NTFS 权限概述 105
4.1.1　NTFS 文件夹权限和 NTFS 文件权限 105
4.1.2　多重 NTFS 权限 107
4.1.3　NTFS 权限的继承性 109
4.2　设置 NTFS 权限 111
4.2.1　设置 NTFS 权限基本策略和规则 111
4.2.2　设置普通 NTFS 权限 112
4.2.3　设置高级 NTFS 权限 113
4.2.4　取消“Everyone”完全控制权限 114
4.2.5　NTFS 权限复制 115
4.3　文件审核 116
4.3.1　访问控制列表概述 116
4.3.2　启用审核策略 117
4.3.3　配置审核项目 117
4.3.4　选择审核项的应用位置 119
4.3.5　配置全局对象访问审核 119
4.4　磁盘配额 121
4.4.1　启动磁盘限额 121
4.4.2　为用户配置磁盘配额 122
4.4.3　监控每个用户的磁盘配额使用情况 123
4.5　共享资源安全 123
4.5.1　共享访问权限 124
4.5.2　共享访问权限与 NTFS 权限 126
4.6　默认共享安全 126
4.6.1　查看默认共享 126
4.6.2　停止默认共享 127
4.6.3　设置隐藏的共享 132

第 5 章　Internet 信息服务安全 133

5.1　IIS 安全规划 133
5.1.1　评估安全威胁 133

5.1.2 规划安全措施 134
5.2 Web 安全 137
5.2.1 用户控制安全 137
5.2.2 访问权限控制 139
5.2.3 IP 地址控制 141
5.2.4 端口安全 143
5.2.5 SSL 安全 144
5.2.6 审核 IIS 日志记录 148
5.2.7 设置内容过期 150
5.2.8 添加 MIME 类型 151
5.3 FTP 安全 152
5.3.1 设置 TCP 端口 152
5.3.2 连接数量限制 153
5.3.3 IP 地址访问限制 153
5.3.4 设置用户身份验证 155
5.3.5 设置授权规则 155
5.3.6 基于 NTFS 权限设置的访问控制 157
5.3.7 限制用户的上传空间 160

第 6 章 事件、日志和警报 161

6.1 事件查看器 161
6.1.1 事件查看器概述 161
6.1.2 查看事件信息 163
6.1.3 将任务附加到日志 165
6.1.4 导出和导入日志 166
6.1.5 订阅事件 168
6.1.6 分析日志和调试日志 172
6.2 安全性日志 172
6.2.1 启用审核策略 173
6.2.2 日志分析 174
6.2.3 审核日志 174
6.2.4 审核事件 ID 175
6.3 系统性能监控 184
6.3.1 系统监视器 184
6.3.2 性能监视器 187
6.3.3 数据收集器集 190

第 7 章 局域网接入安全 195

7.1 配置和管理 RADIUS 服务器 195
7.1.1 安装 RADIUS 服务器 195
7.1.2 配置 RADIUS 客户端 195
7.2 基于端口的认证安全 197
7.2.1 IEEE 802.1x 认证简介 197
7.2.2 配置 IEEE 802.1x 认证 201
7.2.3 配置交换机到 RADIUS 服务器的通信 203
7.2.4 配置重新认证周期 203
7.2.5 修改安静周期 204
7.2.6 用户计算机配置 205
7.2.7 客户端接入启用 802.1x 认证的网络 205
7.3 无线网络设备安全 206
7.3.1 无线接入点安全 206
7.3.2 无线路由器安全 216
7.3.3 无线局域网控制器安全 220
7.4 无线网络 IEEE 802.1x 身份认证 230
7.4.1 部署 IEEE 802.1x 认证 230
7.4.2 无线访问认证配置步骤 231
7.4.3 配置 Cisco 无线接入点 231
7.4.4 无线用户客户端计算机配置 232
7.4.5 无线客户端接入启用 802.1x 认证的网络 233

第 8 章　网络访问保护 235

8.1　NAP 系统概述 235
8.1.1　NAP 的应用环境 235
8.1.2　NAP 的强制模式 236
8.1.3　NAP 系统的功能 236
8.1.4　NAP 系统架构 236
8.2　强制方式 238
8.2.1　IPSec 强制 239
8.2.2　802.1x 强制 239
8.2.3　VPN 强制 239
8.2.4　DHCP 强制 240
8.2.5　RD 网关强制 240
8.3　网络访问保护的准备 240
8.3.1　相关服务组件的安装 241
8.3.2　更新服务器 242
8.3.3　网络策略服务器 243
8.4　DHCP 强制的配置与应用 244
8.4.1　网络环境概述 244
8.4.2　配置健康策略服务器 245
8.4.3　配置 DHCP 服务器 249
8.4.4　非 NAP 客户端测试 254
8.4.5　域中客户端计算机的测试 256
8.4.6　不健康 NAP 客户端的测试 260
8.5　VPN 强制的配置与应用 264
8.5.1　网络环境概述 264
8.5.2　配置健康策略服务器 265
8.5.3　VPN 服务器的配置 272
8.5.4　创建和配置 VPN NAP 客户端 275
8.5.5　测试受限 VPN 客户端的访问 277
8.6　配置 RD 网关强制 278
8.6.1　RD 网关服务器的配置 278
8.6.2　配置 RD 网关强制策略 279
8.6.3　配置 NAP 客户端 281

第 9 章　局域网传输安全 283

9.1　内部网络防火墙 283
9.1.1　内部防火墙规划与设计 283
9.1.2　内部防火墙的选择 284
9.1.3　内部防火墙配置实例 284
9.2　基于端口的传输控制 287
9.2.1　风暴控制 287
9.2.2　流控制 289
9.2.3　保护端口 290
9.2.4　端口阻塞 290
9.2.5　端口安全 291
9.2.6　传输速率限制 293
9.2.7　MAC 地址更新通知 294
9.2.8　绑定 IP 和 MAC 地址 298
9.3　VLAN 安全 298
9.3.1　VLAN 概述 299
9.3.2　VLAN 规划与设计 300
9.3.3　配置和管理 VLAN 301
9.3.4　配置 VLAN Trunk 306
9.4　私有 VLAN 安全 311
9.4.1　PVLAN 概述 311
9.4.2　配置 PVLAN 314
9.5　访问列表安全 318
9.5.1　访问列表概述 318
9.5.2　IP 访问列表 320
9.5.3　端口访问列表 326
9.5.4　创建并应用 VLAN 访问列表 327

第 10 章　网络设备系统安全.....329

10.1　网络设备登录安全.....329
10.1.1　登录密码安全.....329
10.1.2　配置命令级别安全.....332
10.1.3　终端访问限制安全.....333
10.1.4　SNMP 安全.....335
10.1.5　HTTP 服务安全.....339
10.2　系统安全日志.....341
10.2.1　日志信息概述.....342
10.2.2　启用系统日志信息.....344
10.2.3　设置日志信息存储设备.....345
10.2.4　定义消息严重等级.....346
10.2.5　配置 UNIX 系统日志服务器.....347
10.3　网络设备系统映像安全.....348
10.3.1　备份系统软件映像.....348
10.3.2　恢复或升级系统软件映.....350

第 11 章　Internet 接入安全.....353

11.1　网络边缘安全设备.....353
11.1.1　网络边缘安全设备类型与适用.....353
11.1.2　网络边缘安全设备选择.....355
11.1.3　网络边缘安全配置规划.....360
11.2　边缘网络防火墙安全配置.....364
11.2.1　网络防火墙基本配置.....365
11.2.2　配置 NAT 地址转换.....370
11.2.3　配置远程访问 SSL VPN 服务.....372
11.2.4　发布内部服务器.....381
11.3　代理服务器安全管理.....383
11.3.1　Microsoft TMG 安装.....383
11.3.2　Microsoft TMG 配置.....387
11.3.3　Internet 访问限制.....392

第 12 章　入侵检测系统.....401

12.1　入侵检测系统概述.....401
12.1.1　入侵检测系统架构.....401
12.1.2　入侵检测系统的功能.....402
12.1.3　入侵检测的一般步骤.....402
12.1.4　常用入侵检测工具.....403
12.2　Snort.....404
12.2.1　Snort 概述.....404
12.2.2　Snort 语法及参数.....405
12.2.3　部署 snort 入侵检测系统.....406
12.2.4　Snort 的 3 种工作模式.....418
12.2.5　Snort 应用实例.....424
12.3　Sniffer.....427
12.3.1　Sniffer 概述.....427
12.3.2　Sniffer 安装与配置.....428
12.3.3　Sniffer 的监控模式.....431
12.3.4　创建过滤器.....437
12.3.5　捕获数据.....440
12.3.6　分析捕获的数据.....441
12.3.7　Sniffer 应用实例.....446

第 13 章　网络客户端安全.....449

13.1　网络客户端安全规划.....449
13.2　组策略应用基础.....450
13.2.1　组策略概述.....450
13.2.2　将管理对象添加到域.....452
13.2.3　将用户添加到本地管理员组.....453
13.2.4　创建组策略.....456
13.2.5　编辑组策略.....457

13.2.6 添加管理模板 457
13.2.7 筛选管理模板 458
13.3 安全策略 459
13.3.1 账户策略和审核策略 460
13.3.2 设备限制安全策略 460
13.4 软件限制策略 462
13.4.1 软件限制策略概述 462
13.4.2 安全级别设置 463
13.4.3 默认规则 469
13.5 配置客户端环境 471
13.5.1 定制客户端主页 471
13.5.2 修改 Windows 防火墙设置 471
13.5.3 取消密码复杂性的要求 473
13.5.4 定制用户连接到的网络驱动器 474

第 14 章 网络安全方案示例 477

14.1 校园网安全方案 477
14.1.1 安全系统设计原则 477
14.1.2 网络安全需求分析 478
14.1.3 网络安全方案 479
14.2 企业网安全方案 481
14.2.1 安全系统设计原则 481
14.2.2 网络安全威胁 482
14.2.3 网络安全方案 482

第 1 章　网络安全规划与设计

网络安全已经成为企业管理者倍加重视的问题，其重要性是不言而喻的，尤其是知名企业更是如此。许多黑客甚至以攻破某企业网络为荣，尽管这种行为有时只是一场恶作剧，但是大多数网络入侵都意味着企业数据的丢失或网络瘫痪，对企业生产、声誉产生不利影响。计算机网络的安全体系，覆盖网络应用的每个细枝末节，是一套完整的综合应用系统，通常涉及安全风险分析、用户需求评估、安全技术规划和部署以及网络安全管理等方面。

1.1　网络系统安全风险分析

随着 Internet 网络急剧扩大和上网用户迅速增加，风险变得更加严重和复杂。原来由单个计算机安全事故引起的损害可能传播到其他系统，引起大范围的瘫痪和损失。另外加上缺乏安全控制机制和对 Internet 安全政策的认识不足，这些风险正日益严重。针对企业局域网中存在的安全隐患，在进行安全方案设计时，下述安全风险必须要认真考虑，并且要针对面临的风险，采取相应的安全措施。这些安全风险由多种因素引起，与网络结构和系统的应用、局域网内网络服务器的可靠性等因素密切相关。

计算机网络安全可以从以下几个方面来理解。

- 网络物理是否安全。
- 网络平台是否安全。
- 系统是否安全。
- 应用是否安全。
- 管理是否安全。

针对每一类安全风险，结合局域网络的实际情况，将具体的分析网络的安全风险。

1.1.1　物理安全风险分析

物理安全是涉及实现和维护计算机网络物理设备安全的措施，这意味着对管理人员、硬件以及控制信息，在所有状态下的支持系统元素和资源的物理保护，如果攻击者获得被控制设备的物理访问权，就可以绕过对此设备的大多数基于安全技术的控制。

计算机网络物理安全主要是指自然灾害事故、电源故障、人为操作失误或错误、设备被破坏或丢失、电磁干扰、线路截获等方面。除此之外，机房的物理环境及附属设施以及管理人员，也应归于网络物理安全风险范围。

物理安全是整个网络系统安全的前提，在局域网络内，由于网络的物理跨度不大，只要制定健全的安全管理制度，做好备份，并且加强网络设备和机房的管理，这些风险是完全可以避免的。

1.1.2 网络平台的安全风险分析

网络应用已经遍布我们生活的每一个角落，网络在给我们的生活带来便利的同时，也暴露其自身的弱点。众多网络功能的实现都是借助网络服务器实现的，而若想使每一个人都能享用这项服务，就必须将服务器放在公开的 Internet 上，每时每刻都可能遭受来自不同用户的攻击和入侵。

对于网络供应商而言，局域网络公开服务器区、特殊服务节点是与外界联系的枢纽，一旦不能运行或受到攻击，将影响集团的业务。同时公开服务器本身要为外界服务，必须开放相应的服务。因此，规模比较大网络的管理人员对 Internet 安全事故做出有效反应变得十分重要。有必要将公开服务器、内部网络与外部网络进行隔离，避免网络结构信息外泄；同时还要对外网的服务请求加以过滤，只允许正常通信的数据包到达相应主机，其他的请求服务在到达主机之前就应该遭到拒绝。

1.1.3 系统的安全风险分析

所谓系统的安全，是指整个局域网网络操作系统、网络硬件平台是否可靠且值得信任，安全只是一个相对的概念，绝对的安全是不存在的。

在日常应用中，用户可以通过对现有的操作平台进行安全配置、对操作和访问权限进行严格控制，从而提高系统的安全性。首先，不但要选用尽可能可靠的操作系统和硬件平台，而且必须加强登录过程的认证（特别是在到达服务器主机之前的认证），确保用户的合法性；其次，应该严格限制登录者的操作权限，将其完成的操作限制在最小的范围内。

1.1.4 应用的安全风险分析

应用系统的安全跟具体应用有关，涉及很多方面。应用系统的安全是动态的、不断变化的。应用的安全性也涉及到信息的安全性，同样包括很多方面。

1. 应用系统安全是动态的、不断变化的

应用的安全涉及面很广，以目前 Internet 上应用最为广泛的 E-mail 系统来说，其解决方案就有几十种，但其系统内部的编码甚至编译器导致的 BUG 是很少有人能够发现的，因此一套详尽的测试软件是必须的。但是应用系统是不断发展且应用类型是不断增加的，其结果是安全漏洞也是不断增加且隐藏越来越深。

2. 应用的安全性涉及到信息、数据的安全性

信息的安全性涉及机密信息泄露。未经授权的访问、破坏信息完整性、假冒、破坏系统的可用性等。由于局域网络跨度不大，绝大部分重要信息都在内部传递，因此信息的机密性和完整性是可以保证的。对于有些特别重要的信息需要对内部进行保密的（比如领导子网、财务系统传递的重要信息）可以考虑在应用级进行加密，针对具体的应用直接在应用系统开发时进行加密。

1.1.5 管理的安全风险分析

管理是网络中安全最为重要的部分。责权不明、管理混乱、安全管理制度不健全及缺乏可操作性等都可能会引起管理安全的风险。责权不明、管理混乱，使得一些员工或管理员随便让一些非本地员工甚至外来人员进入机房重地，或者员工有意无意泄露所知道的一些重要信息，而管理上却没有相应制度来约束。

当网络出现攻击行为或网络受到其他一些安全威胁时（如内部人员的违规操作等），无法进行实时的检测、监控、报告与预警。同时，当事故发生后，也无法提供黑客攻击行为的追踪线索及破案依据，即缺乏对网络的可控性与可审查性。这就要求必须对站点的访问活动进行多层次的记录，及时发现非法入侵行为。

建立全新网络安全机制，必须深刻理解网络并能提供直接的解决方案，因此，最可行的做法是管理制度和管理解决方案的结合。

1.1.6 其他安全风险

1. 黑客攻击

在计算机网络飞速发展的同时，黑客技术也日益高超。目前黑客能运用的攻击软件已有1000 多种。黑客自己开发或利用已有的工具寻找计算机系统和网络的缺陷和漏洞，并对这些缺陷实施攻击，如软件缺陷、硬件缺陷、网络协议缺陷、管理缺陷和人为的失误等。

发现并实现黑客技术通常要求这个人对计算机和网络非常精通，发现并证实一个计算机系统漏洞可能需要做大量测试、分析大量代码和长时间的程序编写。大部分黑客是利用已有的软件，这并不需要多么高超的技术。如今，Internet 上的黑客站点随处可见，黑客工具可任意下载，从而对网络的安全构成了极大的威胁。

2. 通用网关接口漏洞

黑客可以通用网关接口（CGI）脚本自身的漏洞，执行一些非法任务，通常情况下，这些CGI 脚本所在 WWW 服务器中寻找。要防止这类问题发生，应将这些 CGI 脚本设置为较低级用户特权。提高系统的抗破坏能力，提高服务器备份与恢复能力，提高站点内容的防篡改与自动修复能力。

3. 恶意代码

恶意代码主要利用本地主机上一些特殊的 Native API 函数和内核系统函数，进行感染、传播和隐藏，从而达到对系统进程、文件、注册表、系统服务和网络服务等进行控制的目的。新形式的恶意代码攻击，大量使用多重加密壳、驱动关联壳、变形壳等代码保护机制和多态和变形等新的技术，传统的恶意代码查杀技术遭到了严重的挑战。

从技术上进行分类，恶意代码使用的技术手段可以分为：

- 用户模式系统调用劫持。
- 核心模式系统调用劫持。

- 核心模式数据篡改。
- 核心模式中断处理程序劫持。

4. 病毒

计算机病毒一直是计算机安全的主要威胁。随着计算机技术的不断进步，计算机病毒的发展速度也是非常惊人的，每天网络上都会出现成千上万种新的病毒。大多数病毒都有一定的破坏性，严重的可能导致重要数据丢失、系统瘫痪，甚至硬件损毁。例如，被誉为“2006 年十大计算机病毒之首”的“熊猫烧香”，可以在极短的时间内感染本地计算机中所有的可执行文件。

5. 不满的内部员工

不满的内部员工（计算机人员、其他工作人员）熟悉服务器、小程序、脚本和系统的弱点。对于已经离职的不满员工，可以通过定期改变口令和删除系统记录以减少这类风险。但还有心怀不满的在职员工，这些员工比已经离开的员工能造成更大的损失，例如，可以传出至关重要的信息、泄露安全重要信息、错误地进入数据库、删除数据等。

6. 针对网络的其他手段

一般认为，目前对网络的攻击手段主要表现在如下几方面：

■ 非授权访问

没有预先经过同意，就使用网络或计算机资源被看作非授权访问，如有意避开系统访问控制机制，对网络设备及资源进行非正常使用，或擅自扩大权限，越权访问信息。非授权访问主要有以下几种形式：假冒、身份攻击、非法用户进入网络系统进行违法操作、合法用户以未授权方式进行操作等。

■ 信息泄露或丢失

信息泄露或丢失指敏感数据在有意或无意中被泄露出去或丢失，通常包括，信息在传输中丢失或泄露（如“黑客”们利用电磁泄露或搭线窃听等方式可截获机密信息，或通过对信息流向、流量、通信频度和长度等参数的分析，推出有用信息，如用户口令、账户等重要信息。），信息在存储介质中丢失或泄露，通过建立隐蔽隧道等窃取敏感信息等。

■ 破坏数据完整性

破坏数据完整性以非法手段窃得对数据的使用权，删除、修改、插入或重发某些重要信息，以取得有益于攻击者的响应；恶意添加，修改数据，以干扰用户的正常使用。

■ 拒绝服务攻击

拒绝服务攻击不断对网络服务系统进行干扰，改变其正常的作业流程，执行无关程序使系统响应减慢甚至瘫痪，影响正常用户的使用，甚至使合法用户被拒绝而无法进入计算机网络系统或不能得到相应的服务。

■ 利用网络传播病毒

网络是当今计算机病毒的主要传播途径之一，不仅后果严重，而且难于防范。这种传播

方式主要特点是：被病毒感染的计算机会自动扫描所在网络的其他计算机，如果这些计算机也存在这种漏洞，便会被入侵，这些被入侵的计算机会继续扫描攻击……此类病毒传播速度快，在很短时间内感染数台计算机。而且这种病毒会使得多台计算机同时扫描，占用网络的大量带宽，甚至阻塞整个网络的通信。要从根本上杜绝这种安全隐患，首先要在全网计算机中部署杀毒软件，并及时升级，同时必须配合在全网计算机中检查系统漏洞，及时做好系统补丁更新。

1.2 安全需求与安全目标

通过对网络结构、网络安全风险分析，再加上黑客、病毒等安全威胁日益严重。解决网络安全问题解决势在必行。针对不同安全风险，必须采用相应的安全措施来解决，从而使网络安全达到一定的安全目标。

1.2.1 安全需求

通过前面对局域网络结构、应用及安全威胁分析，可以看出其安全问题主要集中在对服务器的安全保护、防黑客和病毒、重要网段的保护以及管理安全上。因此，必须采取相应的安全措施杜绝安全隐患，应该做到以下几点：

- 公开服务器的安全保护。
- 防止黑客从外部攻击。
- 入侵检测与监控。
- 信息审计与记录。
- 病毒防护。
- 数据安全保护。
- 数据备份与恢复。
- 网络的安全管理。

针对局域网络系统的实际情况，在系统考虑如何解决上述安全问题的设计时应满足如下要求。

- 大幅度地提高系统的安全性（重点是可用性和可控性）。
- 保持网络原有的能特点，即对网络的协议和传输具有很好的透明性，能透明接入，无需更改网络设置。
- 易于操作、维护，并便于自动化管理，而不增加或少增加附加操作。
- 尽量不影响原网络拓扑结构，同时便于系统及系统功能的扩展。
- 安全保密系统具有较好的性能价格比，一次性投资，可以长期使用。
- 安全产品具有合法性，及经过国家有关管理部门的认可或认证。
- 分布实施。

1.2.2 网络安全策略

安全策略是指在一个特定的环境里，为保证提供一定级别的安全保护所必须遵守的规则，该安全策略模型包括了建立安全环境的 3 个重要组成部分。

- 法律规章。安全的基石是社会法律、法规、规章、制度与相应的制裁手段，这部分用于建立一套安全管理标准和方法。即通过建立与信息安全相关的法律、法规和单位的规章制度，使不法分子慑于法律，不敢轻举妄动。
- 先进技术。先进的安全技术是信息安全的根本保障，用户对自身面临的威胁进行风险评估，决定其需要的安全服务种类，选择相应的安全机制，然后集成先进的安全技术。
- 严格管理。各网络使用机构、企业和单位应建立相宜的信息安全管理办法，加强内部管理，建立审计和跟踪体系，提高整体信息安全意识。

1.2.3 系统安全目标

局域网络系统安全应该实现以下目标：

- 建立一套完整可行的网络安全与网络管理策略。
- 将内部网络、公开服务器网络和外网进行有效隔离，避免与外部网络的直接通信。
- 建立网站各主机和服务器的安全保护措施，保证系统安全。
- 对网络服务请求内容进行控制，使非法访问在到达主机前被拒绝。
- 加强合法用户的访问认证，同时将用户的访问权限控制在最低限度。
- 全面监视对公开服务器的访问，及时发现和拒绝不安全的操作和黑客攻击行为。
- 加强对各种访问的审计工作，详细记录对网络、公开服务器的访问行为，形成完整的系统日志。
- 备份与灾难恢复，强化系统备份，实现系统快速恢复。
- 加强网络安全管理，提高系统全体人员的网络安全意识和防范技术。

一个合格的网络系统应实现以下安全目标：

- 保护网络系统的可用性。
- 保护网络系统服务的连续性。
- 防范网络资源的非法访问及非授权访问。
- 防范入侵者的恶意攻击与破坏。
- 保护企业信息通过网上传输过程中的机密性、完整性。
- 防范病毒的侵害。
- 实现网络的安全管理。

1.3 网络安全规划

不同类型的计算机网络用户，对信息安全要求的级别也是有所不同的。网络安全性的提升是要以巨大的资金投入为基础的，因此，部署计算机网络安全之前，必须了解网络用户的需求，根据其实际情况确定安全系统的主体目标，只有这样才可以制定出一套可靠实用的网络安全系统。

1.3.1 网络安全规划原则

在对局域网络系统安全方案设计、规划时，应遵循以下原则。

1. 综合性、整体性原则

应用系统工程的观点、方法，分析网络的安全及具体措施。安全措施主要包括：行政法律手段、各种管理制度（人员审查、工作流程、维护保障制度等）以及专业措施（识别技术、存取控制、密码、低辐射、容错、防病毒、采用高安全产品等）。一个较好的安全措施往往是多种方法适当综合的应用结果。一个计算机网络，包括个人、设备、软件、数据等。这些环节在网络中的地位和影响作用，也只有从系统综合整体的角度去看待、分析，才能取得有效、可行的措施。即计算机网络安全应遵循整体安全性原则，根据规定的安全策略制定出合理的网络安全体系结构。

2. 需求、风险、代价平衡的原则

对于任何网络，绝对安全很难实现的，也不一定是必要的。通常情况下，需要对网络进行实际的研究（包括任务、性能、结构、可靠性、可维护性等），并对网络面临的威胁及可能承担的风险进行定性与定量相结合的分析，然后制定规范和措施，确定本系统的安全策略。

3. 一致性原则

一致性原则主要是指网络安全问题应与整个网络的工作周期（或生命周期）同时存在，制订的安全体系结构必须与网络的安全需求相一致。安全的网络系统设计（包括初步或详细设计）及实施计划、网络验证、验收、运行等，都要有安全的内容及措施，实际上，在网络建设的开始就考虑网络安全对策，比在网络建设好后再考虑安全措施，不但容易，且花费也小得多。

4. 易操作性原则

安全措施需要人为去完成，如果措施过于复杂，对人的要求过高，本身就降低了安全性。其次，措施的采用不能影响系统的正常运行。

5. 分步实施原则

由于网络系统及其应用扩展范围广阔，随着网络规模的扩大及应用的增加，网络脆弱性也会不断增加。一劳永逸地解决网络安全问题是不现实的。同时由于实施信息安全措施需相当的费用支出。因此分步实施，即可满足网络系统及信息安全的基本需求，亦可节省费用开支。

6. 多重保护原则

任何安全措施都不是绝对安全的，都可能被攻破。但是建立一个多重保护系统，各层保护相互补充，可以达到当一层保护被攻破时，其他层保护仍可保护信息的安全的目的。

7. 可评价性原则

如何预先评价一个安全设计并验证其网络的安全性，这需要通过国家有关网络信息安全测评认证机构的评估来实现。

1.3.2 网络安全技术规划

通常情况下，网络安全的部署和实施往往涉及多个方面甚至多个领域的应用技术，因此，规划网络安全管理工作中可能用到的安全技术也是非常有必要的。目前，常用的网络安全防御技术主要包括防火墙、防病毒、入侵检测、访问控制、安全扫描等，需要注意的是，每一种安全技术都必须被合理的部署在特定的网络环境或网络位置上，才能起到安全防御作用，否则，可能就会适得其反。

1. 防病毒技术

在所有计算机安全威胁中，计算机病毒是最严重的，不仅发生的频率高、损失大，而且潜伏性强、覆盖范围广。如今计算机病毒在形式上越来越狡猾，造成的危害也日益严重。这就要求网络防病毒产品在技术上更先进，在功能上更全面，并具有更高的查杀效率。

■ 单机防病毒

单机防病毒与专业的防病毒服务器配合，定期或自动通过 Internet 连接产品官方服务器获取最新病毒定义，以实现动态防御与静态杀毒相结合。单机防病毒最大的缺点就是功能单一，无法实现统一管理，因此要求防病毒产品必须可以更新病毒库和接受官方服务器的技术支持。

■ 网络防病毒

网络防病毒技术是目前主流安全防护技术之一，适用于各种规模的局域网。网络防病毒技术中主要包括服务器模块和客户端模块，其中服务器主要为客户端提供统一部署和管理，如病毒库升级、调度扫描、远程部署等，而客户端则工作相对简单，只需接受防病毒服务器的管理即可。

2. 防火墙技术

网络防火墙技术是一种用来加强网络之间访问控制，防止外部网络用户以非法手段通过外部网络进入内部网络，访问内部网络资源，保护内部网络操作环境的特殊网络互联设备。它对两个或多个网络之间传输的数据包如链接方式按照一定的安全策略来实施检查，以决定网络之间的通信是否被允许，并监视网络运行状态。

目前的防火墙产品主要有堡垒主机、包过滤路由器、应用层网关（代理服务器）以及电路层网关、屏蔽主机防火墙、双宿主机等类型。根据防火墙所采用的技术不同，可以将其分为4种基本类型：

- 包过滤型。防火墙通过读取数据包中的地址信息来判断这些"包"是否来自可信任的安全站点，一旦发现来自危险站点的数据包,防火墙便会将这些数据拒之门外。系统管理员也可以根据实际情况灵活制订判断规则。
- 网络地址转换-NAT。防火墙根据预先定义好的映射规则来判断访问请求是否安全。当符合规则时，防火墙认为访问是安全的，可以接受访问请求，也可以将连接请求映射到不同的内部计算机中。当不符合规则时，防火墙认为该访问是不安全的，不能被接受，防火墙将屏蔽外部的连接请求。网络地址转换的过程对于用户来说是透明的，不需要用户进行设置，用户只要进行常规操作即可。

- 代理型。代理型防火墙也可以被称为代理服务器,它的安全性要高于包过滤型产品,并已经开始向应用层发展。代理服务器位于客户机与服务器之间,由于外部系统与内部服务器之间没有直接的数据通道,外部的恶意侵害也就很难伤害到企业内部网络系统。
- 监测型。监测型防火墙能够对各层的数据进行主动的、实时的监测,在对这些数据加以分析的基础上,监测型防火墙能够有效地判断出各层中的非法侵入。同时,这种检测型防火墙产品一般还带有分布式探测器,这些探测器安置在各种应用服务器和其他网络的节点之中,不仅能够检测来自网络外部的攻击,同时对来自内部的恶意破坏也有极强的防范作用。

3. 网络访问控制

访问控制是网络安全防范和保护的主要策略，其主要功能就是保证网络资源不被非法使用和访问。访问控制涉及的技术也比较广，包括入网访问控制、网络权限控制、目录级控制以及属性控制等多种手段。

■ 连接访问控制

建立连接是用户获得资源的第一步，连接访问控制主要解决哪些用户能够登录到服务器并获取网络资源，控制允许用户登录的时间和工作站。用户的连接访问控制可分为 3 个步骤：

- 用户名的识别与验证。
- 用户口令的识别与验证。
- 用户账号的默认限制检查。

在上述 3 个步骤中只要任何一关未能通过，该用户便不能访问网络中的资源。

■ 访问权限控制

网络的访问权限控制是针对网络非法操作所提出的一种安全保护措施。用户和用户组被赋予一定的权限。网络控制用户和用户组可以访问哪些目录、子目录、文件和其他资源。可以指定用户对这些文件、目录、设备能够执行哪些操作。受托者指派和继承权限屏蔽可作为两种实现方式。受托者指派控制用户和用户组如何使用网络服务器的目录、文件和设备。继承权限屏蔽相当于一个过滤器，可以限制子目录从父目录那里继承哪些权限。

根据访问权限可以将用户分为以下几类。

- 特殊用户（即系统管理员）。
- 一般用户，系统管理员根据他们的实际需要为他们分配操作权限。
- 审计用户，负责网络的安全控制与资源使用情况的审计。

4. 入侵检测

入侵检测是防火墙的合理补充，主要用于应对潜在的网络攻击，扩展了系统管理员的安全管理能力（包括安全审计、监视、进攻识别和响应），提高了信息安全基础结构的完整性。入侵检测系统从网络系统中的若干关键点收集信息，并分析这些信息，看看网络中是否有违反安全策略的行为和遭到袭击的迹象。入侵检测被认为是防火墙之后的第二道安全闸门，在不影响网络性能的情况下能对网络进行监测，从而提供对内部攻击、外部攻击和误操作的实时保护。这些都通过它执行以下任务来实现：

- 监视、分析用户及系统活动。
- 系统构造和弱点的审计。
- 识别反映已知进攻的活动模式并向相关人士报警。
- 异常行为模式的统计分析。
- 评估重要系统和数据文件的完整性。
- 操作系统的审计跟踪管理，并识别用户违反安全策略的行为。

一个成功的入侵检测系统，不但可以使系统管理员实时了解网络系统（包括程序、文件和硬件设备等）的任何变更，还可以给网络安全策略的制订提供指南。更为重要的一点是，它应该管理、配置简单，从而使非专业人员非常容易地获得网络安全。此外，入侵检测的规模还应根据网络威胁、系统构造和安全需求的改变而改变。入侵检测系统在发现入侵后，会及时做出响应，例如自动断开网络连接、记录事件和报警等。

5. 安全扫描

安全扫描技术是一种重要的网络安全技术，与入侵检测系统类似，主要通过与防火墙、防病毒系统配合使用，达到增强网络安全的目的。通过对网络的扫描，网络管理员能够了解网络的安全配置和运行的应用服务，及时发现安全漏洞，客观评估网络风险等级。网络管理员能够根据扫描的结果更正网络安全漏洞和系统中的错误配置，在黑客攻击前进行防范。假如说防火墙和网络监控系统是被动的防御手段，那么安全扫描就是一种主动的防范措施，能够有效避免黑客攻击行为，做到防患于未然。

安全扫描技术主要分为两类：主机安全扫描技术和网络安全扫描技术。网络安全扫描技术主要针对系统中不合适的配置脆弱的口令，连同针对其他同安全规则抵触的对象进行检查等；而主机安全扫描技术则是通过执行一些脚本文档模拟对系统进行攻击的行为并记录系统的反应，从而发现其中的漏洞。

1.3.3 网络安全设备规划

局域网中常见的网络安全设备包括网络防火墙、入侵检测设备、入侵防御设备等。网络防火墙是必不可少的，用于拦截处理来自 Internet 的各种攻击行为，并且可以隔离内部网络有效避免内部攻击。入侵检测设备只能用于记录入侵行为，局域网中已经很少使用。通常情况下，可以在网络中部署入侵防御系统，保护内部服务器或局域网的安全。

1. 网络防火墙

防火墙的主要功能就是在不同网络之间创建一个阻塞点，用于过滤和控制不同网络之间的网络访问。根据用户需求的不同，可以将其部署在网络中的不同位置，实现对相应网络或子网的安全防护。

■ 连接局域网和 Internet

在局域网和 Internet 之间部署防火墙是最常用的应用方案，不过网络用户根据自己具体需要的不同，有两种连接方式可供选择。

部署方案 1：路由器做接入设备

如果用户网络原来已存在边界路由器，则此可充分利用原有设备，利用边界路由器的包过滤功能，添加相应的防火墙配置，这样原来的路由器也就具有防火墙功能了。然后再利用防火墙与需要保护的内部网络连接。对于 DMZ 区中的公用服务器，则可直接与边界路由器相连，不用经过防火墙。它可只经过路由器的简单防护。在这种网络环境中，边界路由器与防火墙就一起组成了两道安全防线如图 1-1 所示，并且在这两者之间可以设置一个 DMZ 区，用来放置那些允许外部用户访问的公用服务器设施。

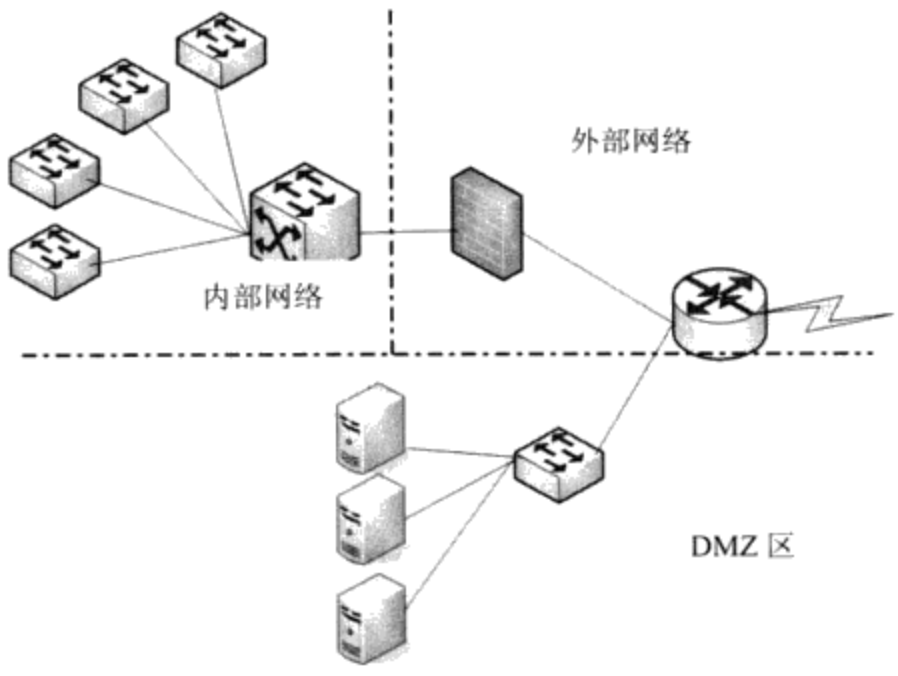


图 1-1　存在边界路由器网络连接

部署方案 2：防火墙做接入设备

网络防火墙也可以用作 Internet 接入设备，但是通常只支持以太网方式接入，这也是目前应用最多的接入方式。如果企业网络恰好采用以太网方式接入 Internet，则可以直接拿掉路由器，而直接借助防火墙实现 Internet 接入，如图 1-2 所示。

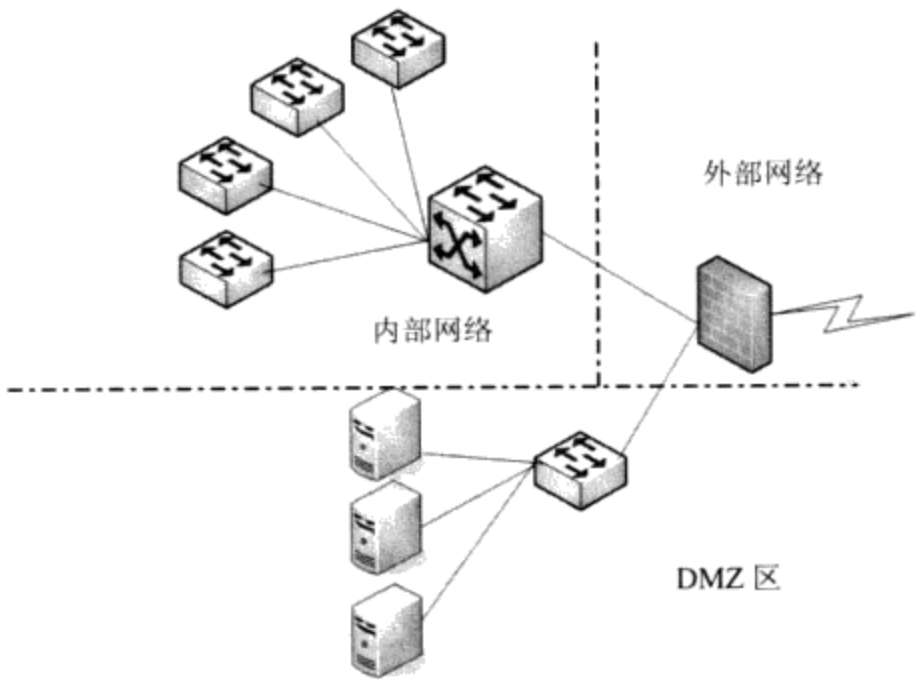


图 1-2　无边界路由器的网络连接

此时 DMZ 区域和需要保护的内部网络分别连接防火墙的不同局域网接口，因此需要对这两部分网络设置不同的安全策略。这种网络中虽然只有一道安全防线，但对于大多数中、小企业来说是完全可以满足的。不过在选购防火墙时就要注意，防火墙一定要有两个以上的局域网

接口。

■ **连接内部网络和第三方网络**

这种连接方式对于一般规模的网络而言应用不是很多，但是在大型企事业计算机网络中，往往有多个合作伙伴或者社会结构，此时就需要用到这种连接方式了，如图 1-3 所示。在这种网络环境中通常是将安全性要求较低的服务器直接连接在网络防火墙的 LAN 端口上，通过防火墙对这些服务器做一些简单的配置，可以提供第三方网络所需的功能即可。

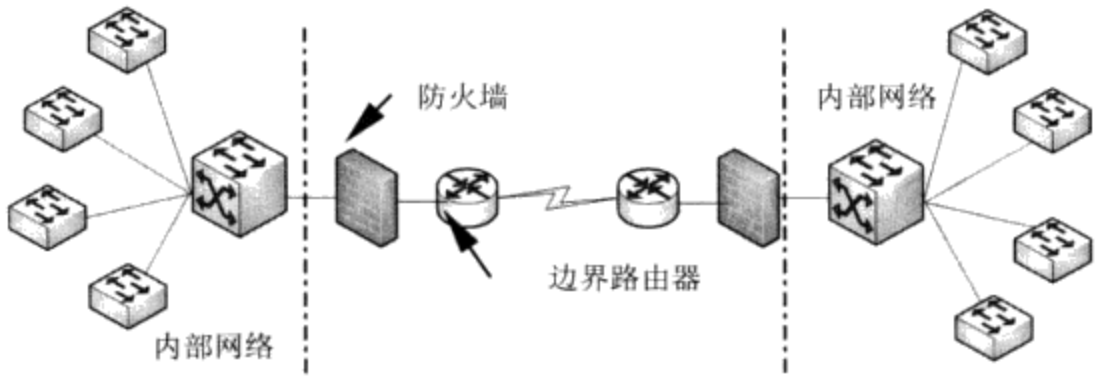


图 1-3 连接内部网络和第三方网络

■ **连接内部网络的不同部门**

这种连接方式在安全性要求较高的企业网络中比较常见，例如跨国公司等，公司内部网络包含多个部门的子网络，而有些局域网的数据是不允许其他用户随意访问的，因此，就要在这些局域网中设置防火墙进行隔离。在如图 1-4 所示的网络中，同是一个企业的内部网络，可以将需要受到保护的重要部门和一些服务器通过防火墙连接至其他网络。

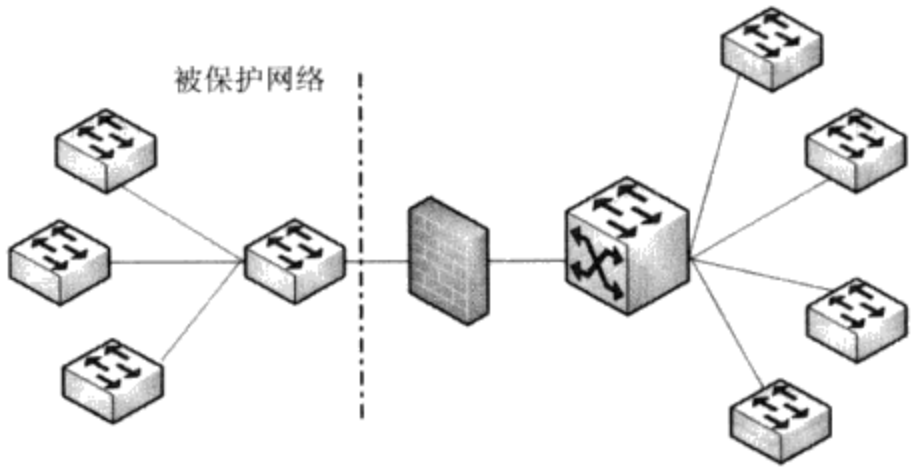


图 1-4 连接内部子网络

2. 入侵检测系统

入侵检测系统（Intrusion Detection Systems，IDS）是继“防火墙”、“信息加密”等传统安全保护方法之后的新一代安全保障技术。入侵检测技术是为保证计算机系统的安全而设计与配置的一种能够及时发现并报告系统中未授权或异常现象的技术。IDS 通过对计算机网络或计算机系统中的若干关键点收集信息并对其进行分析，从中发现网络或系统中是否有违反安全策略的行为和被攻击的迹象。

IDS 的主要功能就是对网络运行状况进行监测，与防火墙略有不同。假如防火墙是一幢大楼的门锁，那么 IDS 就是遍布这幢大楼的监视系统。因此在部署 IDS 时应尽量挂接在所有数据流量都经过的主干路上，或者直接靠近被监视的主要设备。如图 1-5 所示的是 IDS 通常

的位置。

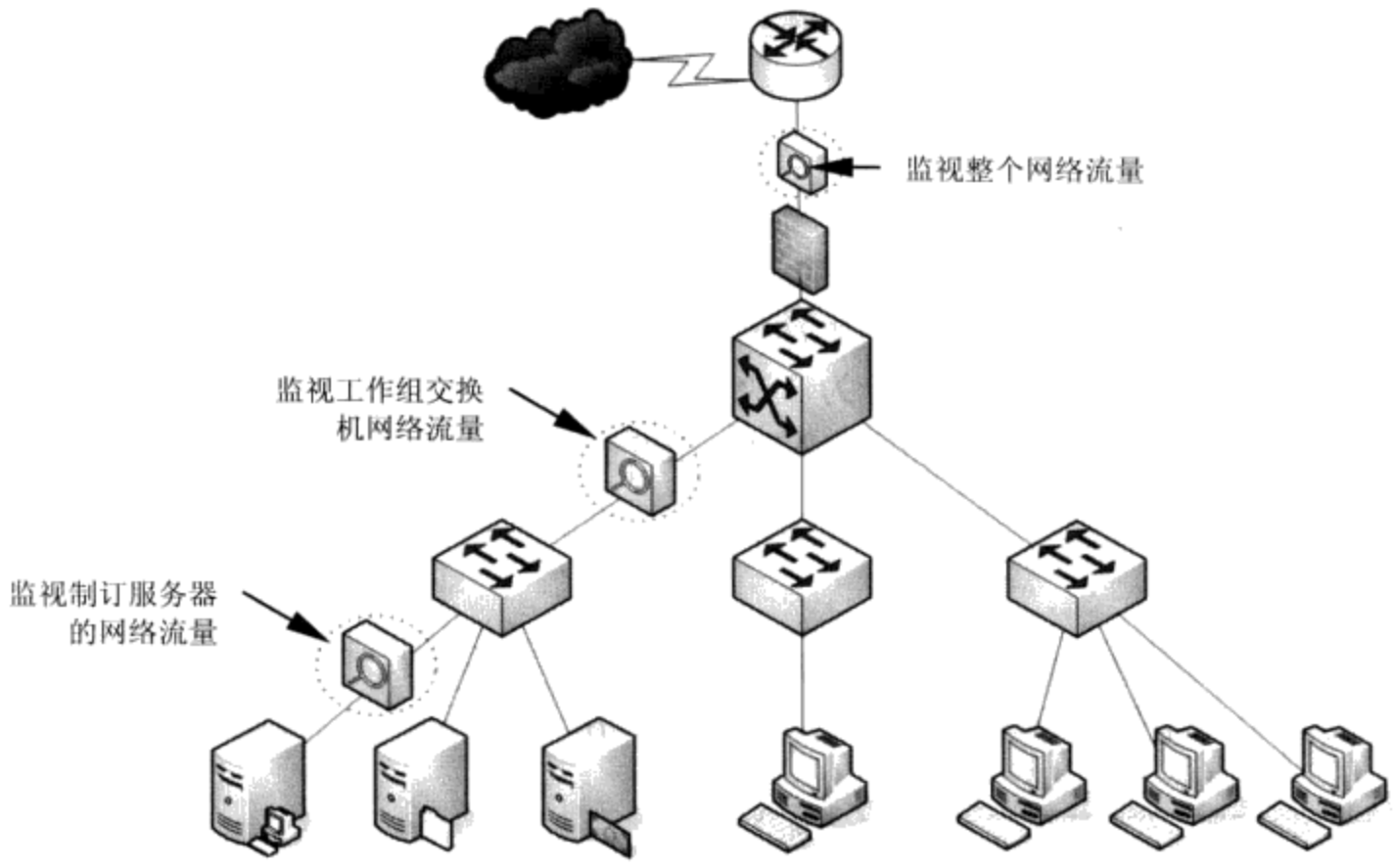


图 1-5　IDS 在网络中的位置

“IDS+防火墙”是目前应用较多的部署方式。防火墙是实施访问控制策略的系统，对流经的网络流量进行检查，拦截不符合安全策略的数据包。IDS 通过监视网络或系统资源，寻找违反安全策略的行为或攻击迹象，并发出报警。防火墙和 IDS 之间是互补的关系，两者协同工作，如图 1-6 所示。

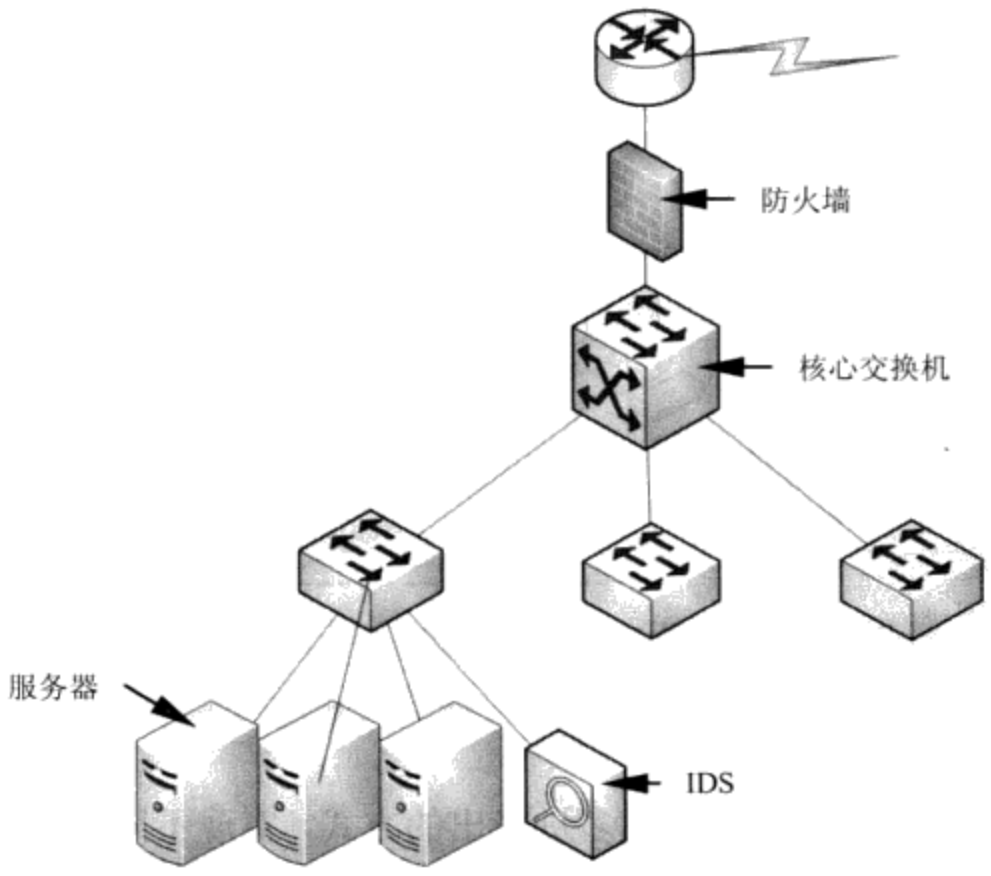


图 1-6　IDS 与防火墙协同工作

因为诸多不足，在目前而言，IDS 主要起的还是监听记录的作用。用个比喻来形容：网络就好比一片黑暗，到处充满着危险，冥冥中只有一个出口。IDS 就像一只手电筒，虽然手电筒不一定能照到正确的出口，但至少有总比没有要好一些。称职的网管，可以从 IDS 中得到一

些关于网络使用者的来源和访问方式，进而依据自己的经验进行主观判断对 IDS 的选择，跟上面谈到的防火墙的选择类似，根据自己的实际要求和使用习惯，选择一个自己够用的，会使用的就足够了。

3. 入侵防御系统

入侵防御系统（Intrusion Prevention System，IPS）是目前应用较多的网络安全防御设备，其主要功能就是拦截和处理传统网络防火墙无法解决的网络攻击，通常被部署在 Internet 接入区。根据 IPS 工作模式的不同，可以将其分为 3 类：基于主机的入侵防御（HIPS）、基于网络的入侵防御（NIPS）和基于应用的入侵防御（AIP）。IPS 在网络中的位置也非常灵活，简单的讲，只需将其部署在需要保护的链路上即可。

■ “路由防护”方案

路由防护，将 IPS 直接部署至路由器和核心交换机之间，借助网络的边界防护，实现 IPS 和防火墙功能，为整个网络提供网络安全保护，如图 1-7 所示。

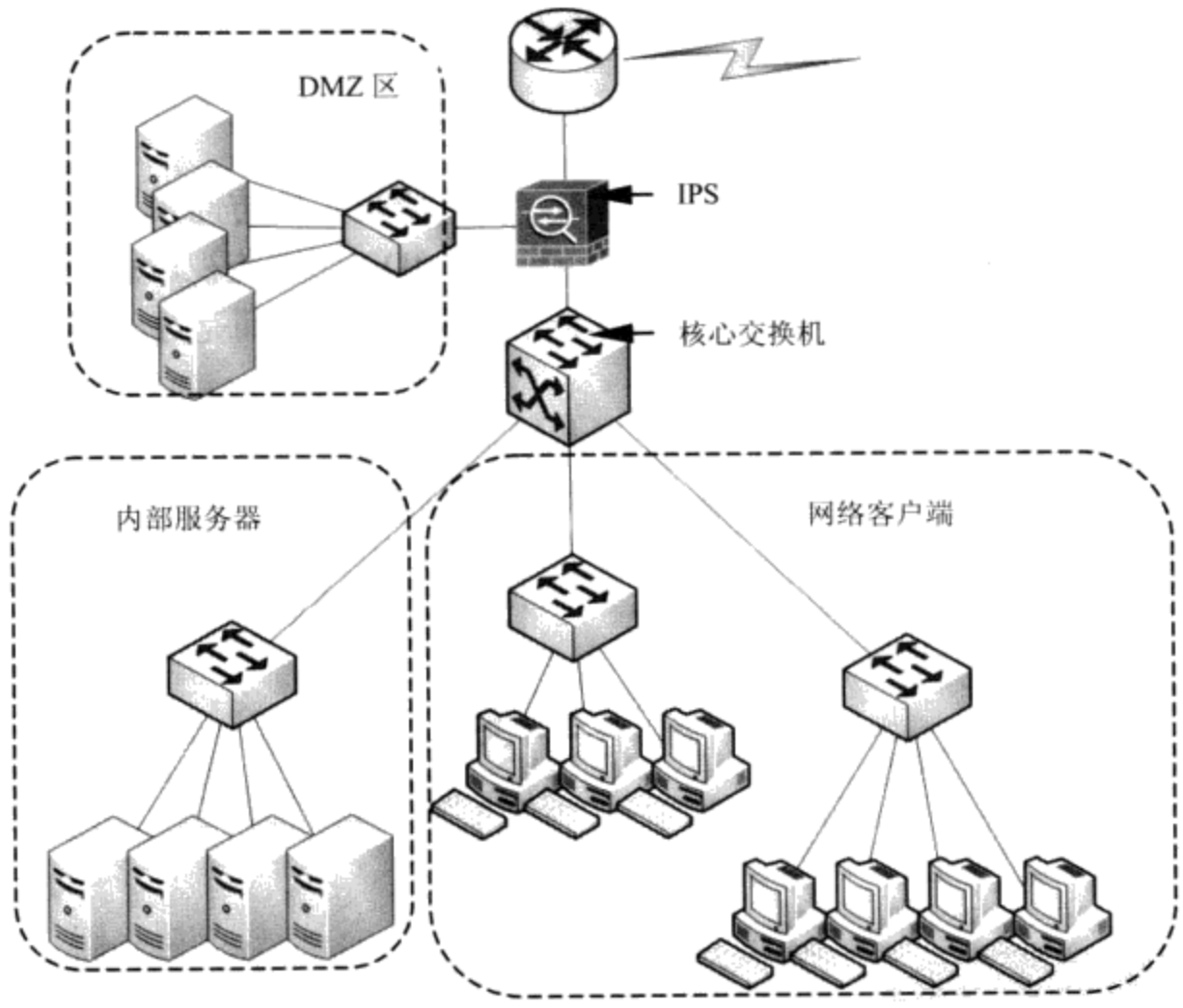


图 1-7 路由防护

■ “交换防护”方案

将 IPS 作为网络核心，采用一进多出或多进多出的方式，实现不同网段相互连接，进行数据交换，同时实现防火墙功能，如图 1-8 所示。

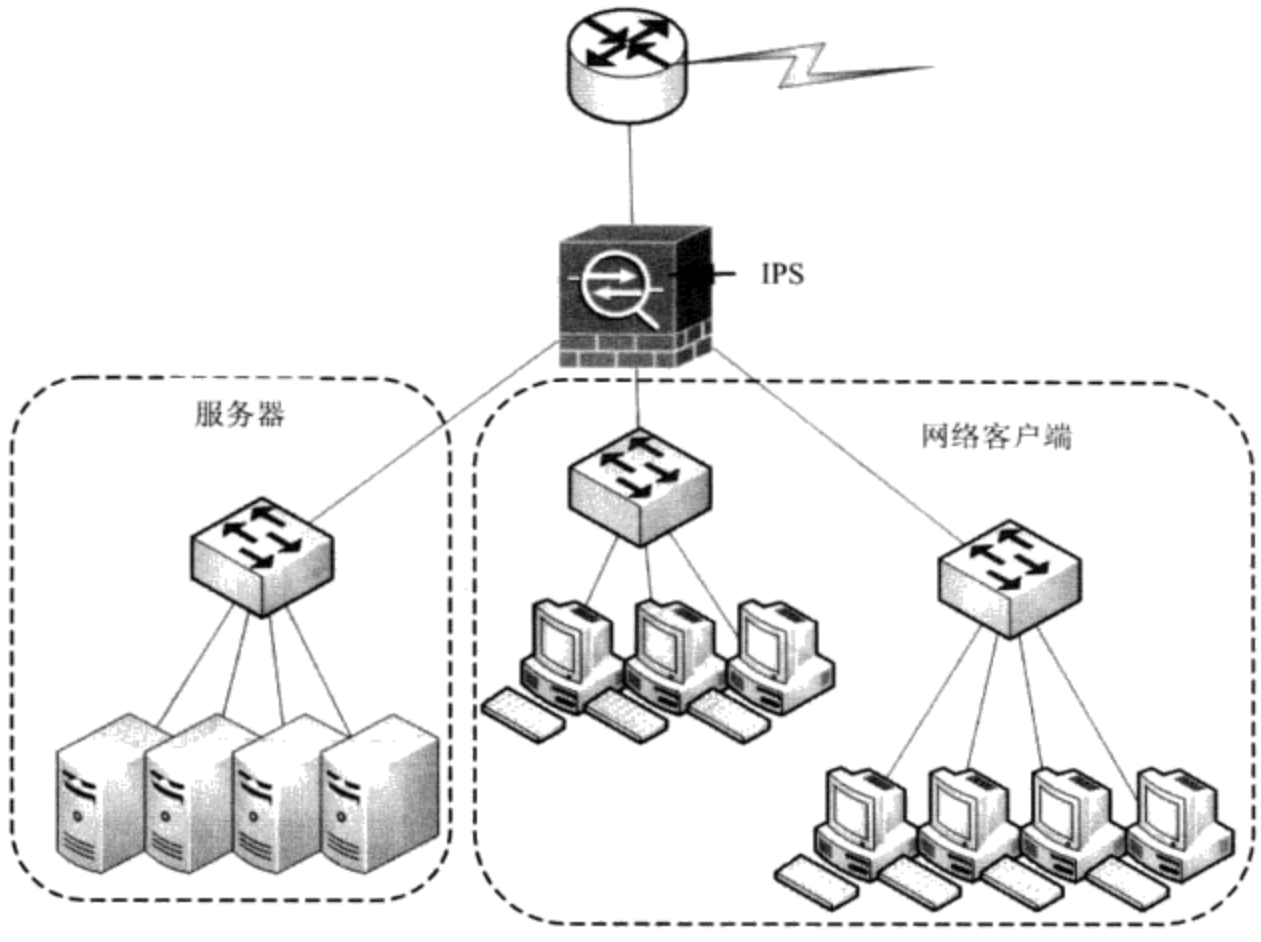


图 1-8　交换防护

■ **“多链路防护”方案**

采用多路 IPS 的连接方式，一路 IPS 防护一个 ISP 接入，各路 IPS 相互独立，彼此之间没有数据交换，互不干扰，如图 1-9 所示。

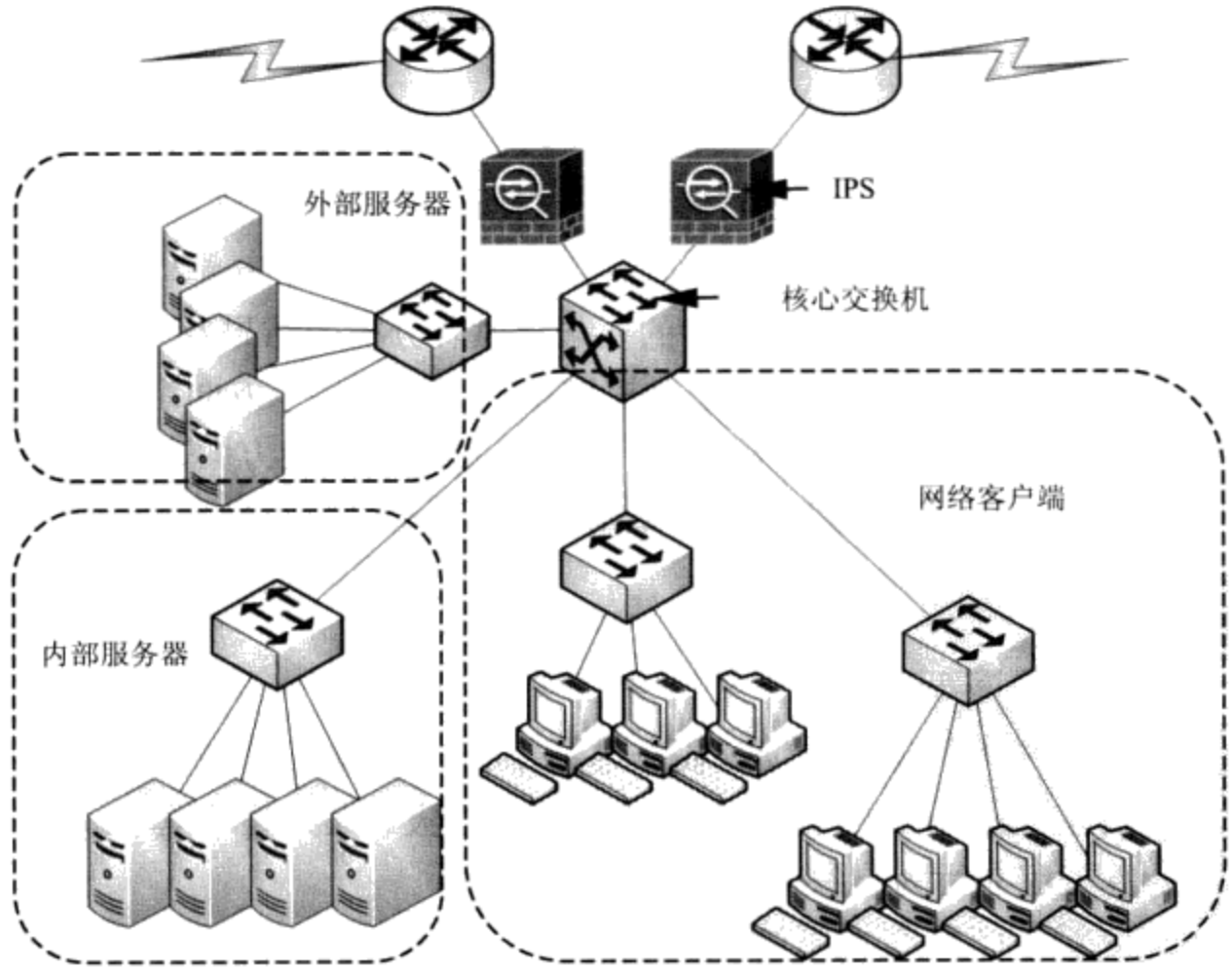


图 1-9　多链路防护

■ **“混合防护”方案**

多种模式分层防护，监控与防护相结合，更完善，在线 NIPS 模式、旁路 NIDS 模式相配合，如图 1-10 所示。

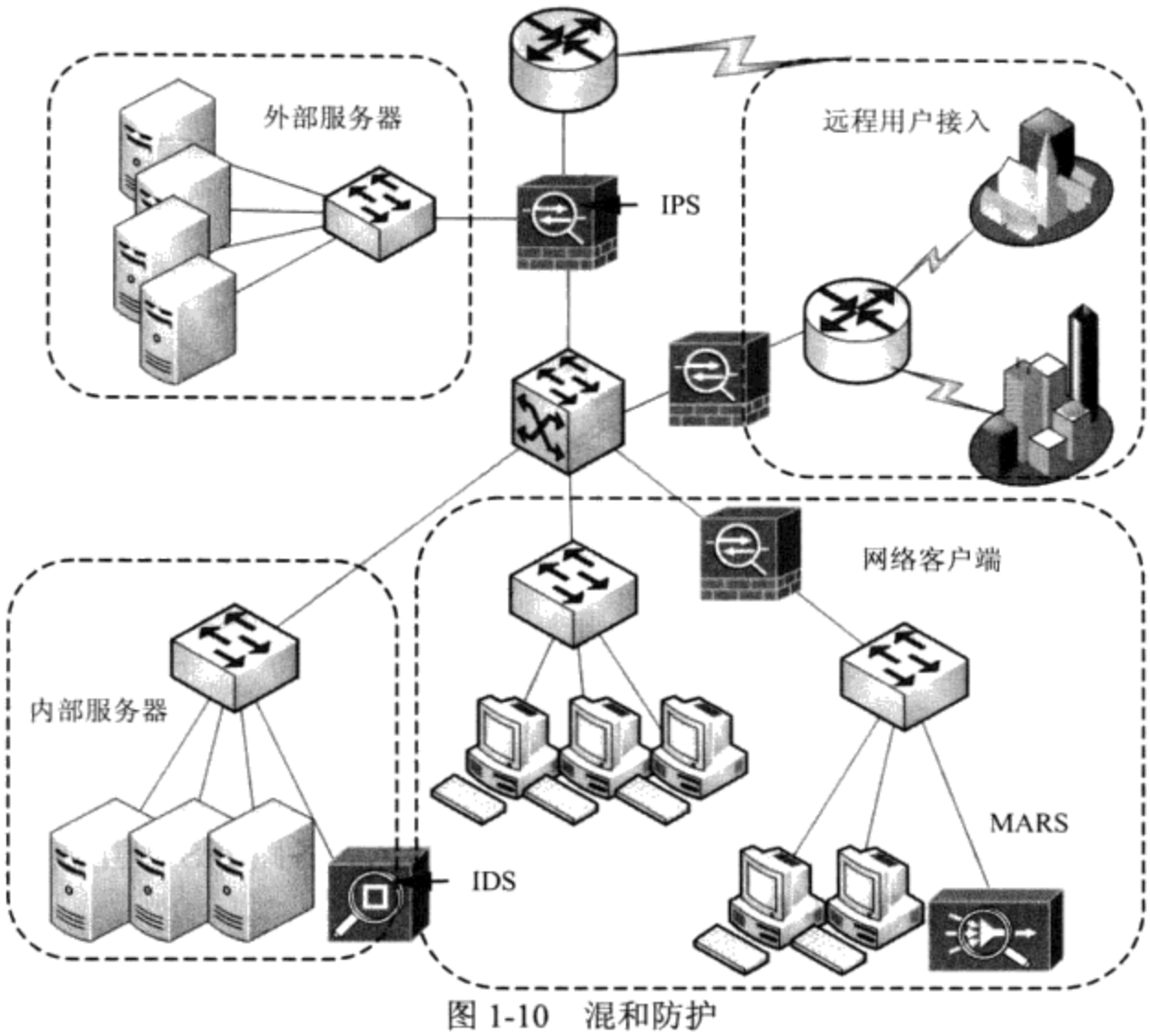


图 1-10 混和防护

1.4 网络安全体系结构

通过对网络的全面了解，按照安全策略的要求、风险分析的结果及整个网络的安全目标，整个网络措施应按系统体系建立。具体的安全控制系统由以下几个方面组成：物理安全、网络安全、系统安全、信息安全、应用安全和安全管理。在网络的安全方面，主要考虑两个大的层次：一是整个网络结构成熟化，主要是优化网络结构；二是整个网络系统的安全。

1.4.1 物理安全

保证计算机信息系统各种设备的物理安全是整个计算机信息系统安全的前提，物理安全是保护计算机网络设备、设施以及其他媒体免遭地震、水灾、火灾等环境事故以及人为操作失误或错误及各种计算机犯罪行为导致的破坏过程。

- 环境安全。对系统所在环境的安全保护，如区域保护和灾难保护；（参见国家标准 GB50173-93《电子计算机机房设计规范》、国家标准 GB2887-89《计算站场地技术条件》、GB9361-88《计算站场地安全要求》。
- 设备安全。设备安全主要包括设备的防盗、防毁、防电磁信息辐射泄露、防止线路截

获、抗电磁干扰及电源保护等。

- 媒体安全。媒体安全包括媒体数据的安全及媒体本身的安全。
- 网络临界点安全。网络临界点安全包括：防火墙、内外网互联的设备、无线设备、VPN 设备等。

1.4.2 网络结构规划

安全系统是建立在网络系统之上的，网络结构的安全是安全系统成功建立的基础。在整个网络结构的安全方面，主要是指网络结构、系统和路由的优化。网络结构的建立要考虑环境、设备配置与应用情况、远程联网方式、通信量的估算、网络维护管理、网络应用与业务定位等因素。成熟的网络结构应具有开放性、标准化、可靠性、先进性和实用性，并且应该有结构化的设计，充分利用现有资源，具有运营管理的简便性，完善的安全保障体系。网络结构采用分层的体系结构，利于维护管理，利于更高的安全控制和业务发展。网络结构的优化，在网络拓扑上主要考虑到冗余链路，防火墙的设置和入侵检测的实时监控等。

1. 网络系统安全

■ 访问控制

访问控制可以通过如下几个方面来实现：

- 制订严格的管理制度。例如《用户授权实施细则》、《密码及账户管理规范》、《权限管理制度》。
- 配备相应的安全设备。在内部网与外部网之间，设置防火墙实现内外网的隔离与访问控制是保护内部网安全的主要措施之一。防火墙设置在不同网络或网络安全域之间信息的唯一出入口。

■ 内外网络隔离

防火墙主要的种类是包过滤型，包过滤防火墙一般利用 IP 和 TCP 包的头信息对进出被保护网络的 IP 包信息进行过滤，能根据企业的安全政策来控制（允许、拒绝、监测）出入网络的信息流。同时可实现网络地址转换（NAT）、审计与实时告警等功能。由于这种防火墙安装在被保护网络与路由器之间的通道上，因此也对被保护网络和外部网络起到隔离作用。防火墙具有以下 5 大基本功能：

- 过滤进、出网络的数据。
- 管理进、出网络的访问行为。
- 封堵某些禁止的业务。
- 记录通过防火墙的信息内容和活动。
- 对网络攻击的检测和告警。

2. 内部网不同网络安全域的隔离及访问控制

在规模庞大的企业网络中往往存在多个功能不同的网络分支，如研发部门、营销部门、售后服务等，为了企业机密信息的外漏，就需要对不同部门用户的访问进行合理控制，例如可以借助交换机的 VLAN（Virtual Local Area Network，虚拟局域网络）功能实现网络隔离的访问

控制。

通过在交换机上划分 VLAN 可以将整个网络划分为几个不同的广播域，实现内部一个网段与另一个网段的物理隔离。这样，就能防止影响一个网段的问题传播到整个网络。在某些情况下，局域网的某个网段比另一个网段更受信任，或者某个网段比另一个更敏感。通过将信任网段与不信任网段划分在不同的 VLAN 段内，就可以限制局部网络安全问题对全局网络造成的影响。

3. 网络安全检测

网络系统的安全性取决于网络系统中最薄弱的环节，解决这一难题的有效方法就是定期对网络系统进行安全性分析，及时发现并修正存在的弱点和漏洞。网络安全检测工具通常是一个网络安全性评估分析软件，其功能是扫描分析网络系统，检查报告系统存在的弱点和漏洞，建议补救措施和安全策略，达到增强网络安全性的目的。检测工具应具备以下功能：

- 具备网络监控、分析和自动响应功能。
- 找出经常发生问题的根源。
- 建立必要的循环过程确保纠正隐患。
- 控制各种网络安全危险。
- 漏洞分析和响应。
- 配置分析和响应。
- 漏洞形势分析和响应。
- 认证和趋势分析。

具体体现在以下方面：

- 防火墙得到合理配置。
- 内外 WEB 站点的安全漏洞减为最低。
- 网络体系达到强壮的抗攻击性。
- 各种服务器操作系统，如邮件服务器、WEB 服务器、应用服务器，将受黑客攻击的可能降为最低。
- 对网络访问做出有效响应，保护重要应用系统（如财务系统）数据安全不受黑客攻击和内部人员误操作的侵害。

4. 审计与监控

审计是记录用户使用计算机网络系统进行所有活动的过程，是提高安全性的重要工具。审计不仅能够识别谁访问了系统，还能看出系统正被怎样地使用。同时，系统事件的记录能够更迅速和系统地识别问题，并且是后面阶段事故处理的重要依据。另外，通过对安全事件的不断收集与积累，并且加以分析，有选择性地对其中的某些站点或用户进行审计跟踪，以便对可能产生破坏性的行为提供有力证据。

除使用一般的网管软件和系统监控管理系统外，还应使用目前较为成熟的网络监控设备或实时入侵检测设备，以便对进出各级局域网的常见操作进行实时检查、监控、报警和阻断，从而防止针对网络的攻击与犯罪行为。

5. 网络防病毒

在网络环境下，计算机病毒有不可估量的威胁性和破坏力，计算机病毒的防范是网络安全性建设中重要的一环。

网络反病毒技术包括以下几种：

- 预防病毒技术。通过自身常驻系统内存，优先获得系统的控制权，监视和判断系统中是否存在病毒，进而阻止计算机病毒进入计算机系统和对系统进行破坏。这类技术有，加密可执行程序、引导区保护、系统监控与读写控制（如防病毒软件等）。
- 检测病毒技术。通过对计算机病毒的特征来进行判断的技术，如自身校验、关键字、文件长度的变化等。
- 清除病毒技术。通过对计算机病毒的分析，开发出具有删除病毒程序并恢复原文件的软件。
- 木马扫描技术。借助专业木马扫描软件，短时间内即可对本地计算机或网络中的主机进行专项扫描，发现存在的木马，并给出相应的防御和补救措施，将损失降到最低。
- 间谍软件扫描技术。间谍软件的主要目的是窃取用户机密信息，目前多个版本的 Windows 系统中已经集成了间谍软件扫描组件，并且可以自动按计划运行，以确保用户系统的安全。

6. 网络备份系统

备份系统的主要目的，就是尽可能快地恢复运行计算机系统所需的数据和系统信息。根据系统安全需求可选择的备份机制有：数据中心高速度、大容量自动的数据存储、备份与恢复；其他区域（备份区域）的数据存储、备份与恢复；对系统设备的备份。备份不仅在网络系统硬件故障或人为失误时起到保护作用，也在入侵者非授权访问或对网络攻击及破坏数据完整性时起到保护作用，同时亦是系统灾难恢复的前提之一。

在确定备份的指导思想和备份方案之后，就要选择安全的存储媒介和技术进行数据备份，有“冷备份”和“热备份”两种。

热备份是指“在线”的备份，即下载备份的数据还在整个计算机系统和网络中，只不过传到另一个非工作的分区，或另一个非实时处理的业务系统中存放。热备份的优点是调用快，使用方便，在系统恢复中需要反复调试时更显优势。热备份的具体做法是：可以在主机系统开辟一块非工作运行空间，专门存放备份数据，即分区备份；另一种方法是，将数据备份到另一个子系统中，通过主机系统与子系统之间的传输，同样具有速度快和调用方便的特点，但投资比较昂贵。

冷备份是指“不在线”的备份，下载的备份存放到安全的存储媒介中，而这种存储媒介与正在运行的整个计算机系统和网络没有直接联系，在系统恢复时重新安装，有一部分原始的数据长期保存并作为查询使用。冷备份弥补了热备份的一些不足，二者优势互补，相辅相成，因为冷备份在回避风险中还具有便于保管的特殊优点。

1.4.3 系统安全

系统的安全主要是指操作系统、应用系统的安全性以及网络硬件平台的可靠性。对于操

作系统的安全防范可以采取如下策略：

- 对操作系统进行安全配置，提高系统的安全性。系统内部调用不对 Internet 公开，关键性信息不直接公开，尽可能采用安全性高的操作系统。
- 应用系统在开发时，采用规范化的开发过程，尽可能的减少应用系统的漏洞。
- 网络上的服务器和网络设备尽可能不采取同一家的产品。
- 通过专业的安全工具（安全检测系统）定期对网络进行安全评估。

1.4.4 信息安全

信息是网络中最重要的安全对象。事实上，实施各种安全措施的最终目的，就是保护位于网络中各个位置的敏感信息。可以采取以下策略，实现对于信息安全威胁的防范：

- 在局域网络内，对不同的信息进行区域规划，执行严格的授权访问机制。将拥有不同安全访问权限的用户划分至不同的 VLAN，并在 Trunk 端口限制授权访问的 VLAN，将一些敏感信息与其他子网络相隔离。
- 将所有敏感信息都集中保存在网络内的文件服务器中，既可以有效保证敏感信息的存储安全，又可以保证在共享文件的同时，严格控制其访问权限。需要注意的是，应杜绝将敏感信息保存在个人计算机上。
- 制订严格的文件访问权限。敏感文件必须存储在 NTFS 系统分区，并且为不同用户或用户组设置严格的 NTFS 文件权限、NTFS 文件夹权限和共享文件权限。
- 将不同类型的用户划分于不同的用户组或组织单位，并为用户组和组织单位指定相应的访问权限，既可以减化文件权限管理的难度，又不会因疏忽大意导致访问权限划分错误。
- 安装 RMS 服务，严格限制对敏感文件的操作。权限管理服务（Windows Rights Management）作为组织内的权限策略管理系统提供一个平台，是在组织中搭建权限管理系统的重要组成部分。
- 其他基于交换机和路由器的安全措施。例如，采用 IEEE 802.1x 身份认证、IP 地址与 MAC 地址绑定、安全端口、IP 或 MAC 地址访问列表等技术，限制用户登录到网络，或者限制其对敏感区域的访问。

1.4.5 应用安全

在应用安全上，首先要考虑通信的授权，传输的加密和审计记录。这必须加强登录过程的认证（特别是在到达服务器主机之前的认证），确保用户的合法性；其次应该严格限制登录者的操作权限，将其完成的操作限制在最小的范围内。另外，在加强主机的管理上，除了上述的访问控制和系统漏洞检测外，还可以采用访问存取控制，对权限进行分割和管理。应用安全平台需要加强资源目录管理和授权管理、传输加密、审计记录和安全管理等内容。对应用安全，主要考虑确定不同服务的应用软件并紧密注视其漏洞；扫描软件不断升级。

1.5 安 全 管 理

为了保护网络的安全性，除了在网络设计上增加安全服务功能，完善系统的安全保密措施外，安全管理规范也是网络安全所必须的。安全管理策略一方面从纯粹的管理上（安全管理规范）来实现，另一方面从技术上建立高效的管理平台（包括网络管理和安全管理）来实现。安全管理策略主要有：定义完善的安全管理模型；建立长远的并且可实施的安全策略；彻底贯彻规范的安全防范措施；建立恰当的安全评估尺度，并且进行经常性的规则审核。当然，还需要建立高效的管理平台。

1.5.1 安全管理规范

面对网络安全的脆弱性，除了在网络设计上增加安全服务功能，完善系统的安全保密措施外，还必须花大力气加强网络安全管理规范的建立，因为诸多的不安全因素恰恰反映在组织管理和人员录用等方面，而这又是计算机网络安全所必须考虑的基本问题，所以应引起各计算机网络应用部门领导的重视。

1. 安全管理原则

网络信息系统的安全管理主要基于 3 个原则。

■ 负责原则

每一项与安全有关的活动，都必须有两人或多人在场。这些人应是系统主管领导指派的，忠诚可靠，能胜任此项工作，应该签署工作情况记录以证明安全工作已得到保障。具体的活动有：

- 访问控制使用证件的发放与回收。
- 信息处理系统使用的媒介发放与回收。
- 处理保密信息。
- 硬件和软件的维护。
- 系统软件的设计、实现和修改。
- 重要程序和数据的删除和销毁。

■ 有限原则

一般情况下，任何人最好不要长期担任与安全有关的职务，以免被误认为这个职务是专有的或永久性的。为遵循任期有限原则，工作人员应不定期地循环任职，强制实行休假制度，并规定对工作人员进行轮流培训，以使任期有限制度切实可行。

■ 分离原则

在信息处理系统工作的人员不要打听、了解或参与职责以外的任何与安全有关的事情，除非系统主管领导批准。出于对安全的考虑，下面每组内的两项信息处理工作应当分开：

- 计算机操作与计算机编程。
- 机密资料的接收和传送。
- 安全管理和系统管理。

- 应用程序和系统程序的编制。
- 访问证件的管理与其他工作。
- 计算机操作与信息处理系统使用媒介的保管。

2. 安全管理的实现

信息系统的安全管理部门应根据管理原则和该系统处理数据的保密性，制定相应的管理制度或采用相应的规范。具体工作是：

- 根据工作的重要程度，确定该系统的安全等级。
- 根据确定的安全等级，确定安全管理的范围。
- 制订相应的机房出入管理制度对于安全等级要求较高的系统，要实行分区控制，限制工作人员出入与己无关的区域。出入管理可采用证件识别或安装自动识别登记系统，采用磁卡、身份卡等手段，对人员进行识别、登记管理。
- 制订严格的操作规程。
- 操作规程要根据职责分离和多人负责的原则，各负其责，不能超越自己的管辖范围。
- 制订完备的系统维护制度。
- 对系统进行维护时，应采取数据保护措施，如数据备份等。维护时要首先经主管部门批准，并有安全管理人员在场，故障的原因、维护内容和维护前后的情况要详细记录。
- 制订应急措施。
- 要制定系统在紧急情况下，如何尽快恢复的应急措施，使损失减至最小。建立人员雇用和解聘制度，对工作调动和离职人员要及时调整响应的授权。

1.5.2 网络安全管理

网络安全管理的主要功能指对安全设备的管理；监视网络危险情况，对危险进行隔离，并把危险控制在最小范围内；身份认证，权限设置；对资源的存取权限的管理；对资源或用户动态的或静态的审计；对违规事件，自动生成报警或生成事件消息；口令管理（如操作员的口令鉴权），对无权操作人员进行控制；密钥管理，对于与密钥相关的服务器，应对其设置密钥生命期、密钥备份等管理功能；冗余备份，为增加网络的安全系数，对于关键的服务器应冗余备份。安全管理应该从管理制度和管理平台技术实现两个方面来实现。安全管理产品尽可能的支持统一的中心控制平台。

根据以上所述，针对网络的实际状况，应因地制宜，分布实施，指定和实现网络安全的纲要，将会极大的提高局域网络的安全性。

第 2 章　Windows Server 2008 R2 系统安全

Window Server 2008 R2 微软最新推出的服务器操作系统，与以往微软发布软件的 R2 版本略有不同，Window Server 2008 R2 不仅仅是在 Windows Server 2008 基础上的改进和扩充，甚至从功能集成、日常操作都有了明显的改变和创新。从安全性和可靠性角度讲，Windows Server 2008 R2 仍然保留了 NAP、AD RMS、RODC 等安全性能，除此之外还增加改进了 Windows Server Backup、组策略等功能角色，是企业服务器系统安全重要保证。

2.1　Windows Server 2008 R2 安装安全

对于普通个人用户而言，选择何种方式安装操作系统，并不会对系统安全产生太多影响，但是对于网络服务器而言，就要加倍注意了。企业网络中往往部署了专业存储网络或为服务器配置了专用存储设备，如果安装过程中操作不当，则可能影响系统运行的稳定性和日后的应用安全。除此之外，还应注意随时关注 Microsoft 的 Windows Update 站点，及时为 Windows Server 2008 R2 下载和安装更新程序。

2.1.1　Windows 安装安全指南

安装 Windows Server 2008 R2 时应注意以下几点：

- 使用正版 Windows Server 2008 R2 系统安装光盘，防止安装过程中被植入木马或间谍软件，影响系统安全性。另外，盗版系统安装光盘也可能影响计算机的兼容性，导致一些莫名其妙的问题。
- 保证硬件设备的可靠性。建议为重要服务器使用磁盘阵列技术，如 RAID0、RAID1 和 RAID 5 等，确保服务器存储系统硬件的稳定性和安全性。
- 尽量使用全新方式安装系统，即将操作系统安装在一个干净的系统分区中，并提前做好合理规划。例如，安装之前删除系统分区的所有文件，并重新格式化，确保磁盘完好无损。
- 使用 NTFS 文件系统格式化服务器所有磁盘分区，可以为系统分区、数据分区和日志文件分区提供更高的安全性。NTFS 是真正的日志型文件系统，使用日志和检查点信息，即使在系统崩溃或者电源故障的时候也可以保证文件系统的一致性。只有使用 NTFS 文件系统的分区，才能为文件配置 ACL（控制访问列表）访问权限控制，达到访问控制安全的目的。
- 没有进行任何安全配置的服务器，不要与任何公共设备或网络连接，必要时可以找一台可以确保安全性的服务器进行连接。
- 只为服务器安装必需的协议，如 TCP/IP 协议，避免其他网络协议给系统带来的漏洞。

- 通常情况下，不要将服务器加入到域，而安装成独立服务器模式。
- 为系统管理员设置一个安全性较高的密码。
- 不要在服务器上部署多操作系统，防止恶意用户通过其他系统控制权限获取重要信息，或对 Windows Server 2008 R2 系统进行破坏。

2.1.2 下载和安装更新程序

系统漏洞是 Microsoft 操作系统的致命弱点，让人欣慰的是其发布更新程序还是非常及时的，只要用户在第一时间安装了漏洞补丁程序，就可以避免由此招致的安全攻击。默认情况下，Windows Server 2008 R2 安装完成后，自动更新功能是未配置的，管理员必须开启并指定选择相应的方式，为系统下载、安装补丁更新，以保护系统的安全。

1. 通过 Internet 实现系统更新

以管理员账户登录到 Windows Server 2008 R2 系统，依次单击“开始”“所有程序”“Windows Update”选项，打开“Windows Update”窗口，单击“更改设置”链接，选择相应的更新方式即可，如图 2-1 所示。

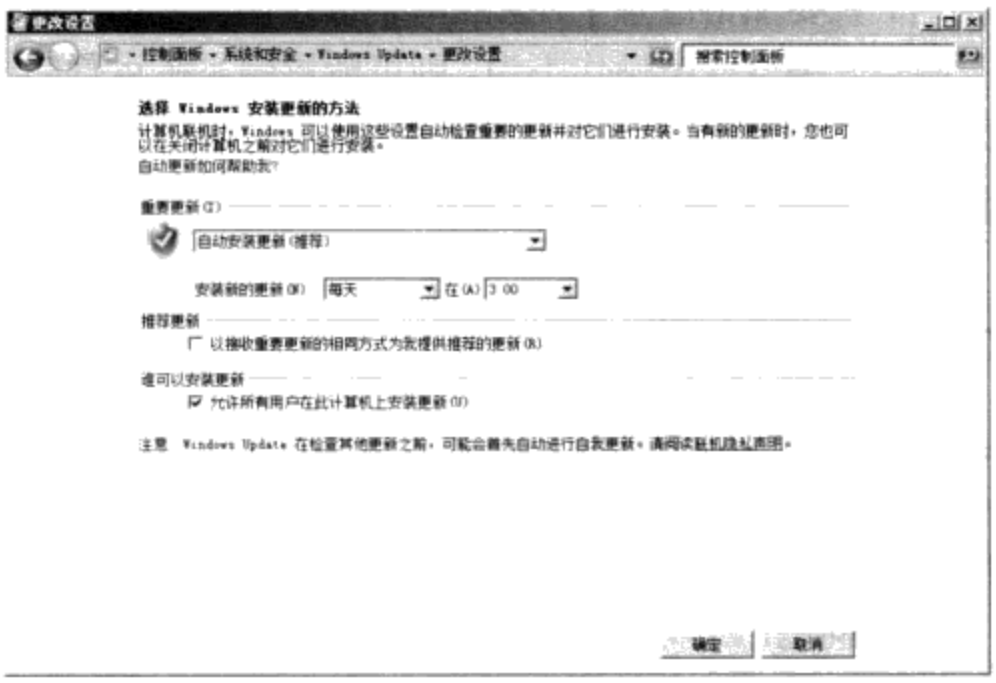


图 2-1 “Windows Update”窗口

Windows Server 2008 R2 系统对更新类型的划分更加详细，允许用户根据更新程序的重要程度选择操作方法。在“重要更新”下拉列表框中，包括如下几种选项：

- 自动安装更新（推荐）。服务器连接到 Internet 后，系统将自动检测 Microsoft Update 服务器是否有所需更新，如果有则将自动下载并安装这些更新。选择该单选按钮后还需要指定系统自动安装更新的具体时间。
- 下载更新，但是让我选择是否安装更新。仅下载所需的系统更新，完成后通知用户在合适的时间手动安装。
- 检测更新，但是让我选择是否下载和安装更新。仅检测 Microsoft Update 服务器上提供的更新项目，并以列表方式提示系统管理员，管理员可以根据实际情况选择需要下载的系统更新。建议使用这种方式，可以减少不必要的服务器资源和网络带宽浪费。
- 从不检查更新（不推荐）。关闭系统更新功能，建议不要选择此项。

另外，在“推荐更新”区域，用户可以选择对此类更新的操作。

2. 通过局域网中的 WSUS 服务器实现系统更新

如果网络中配置有 WSUS 服务器，那么，Windows Server 2008 R2 就可以从 WSUS 服务器上下载更新，而不必连接微软更新服务器。

第 1 步，打开“开始”菜单，在“所有程序”文本框中键入“gpedit.msc”命令，按 Enter 键，打开“本地组策略编辑器”窗口，依次展开“计算机配置”→“管理模板”→“Windows 组件”，如图 2-2 所示。

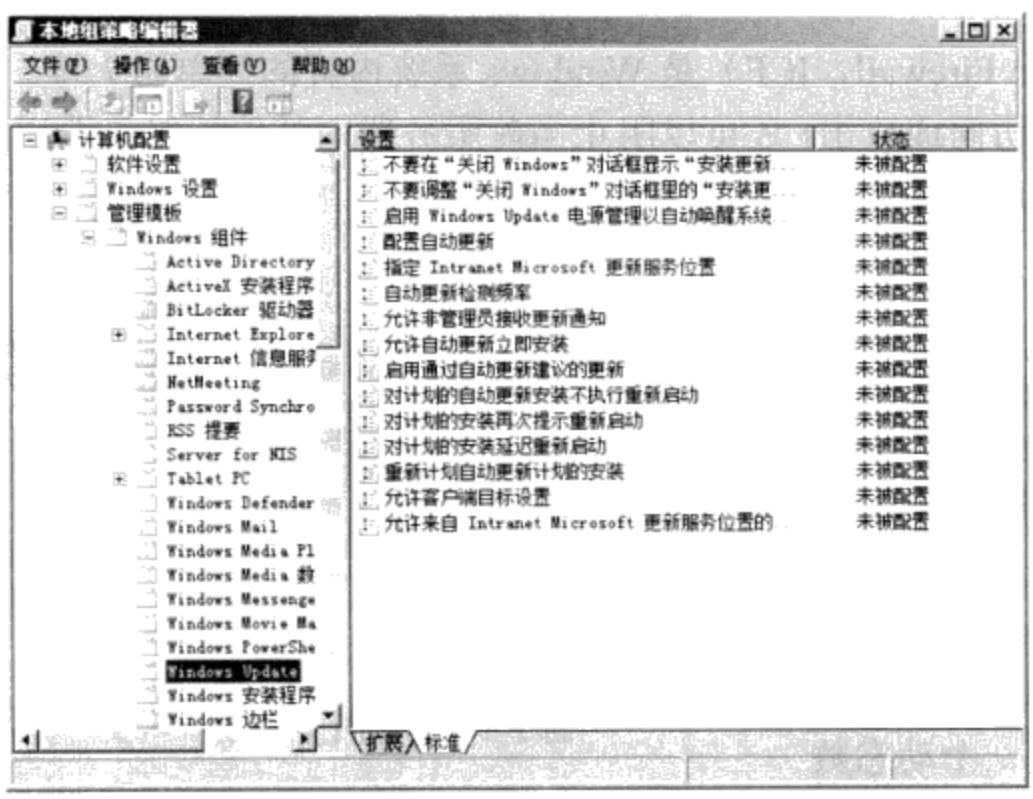


图 2-2 “Windows Update”窗口

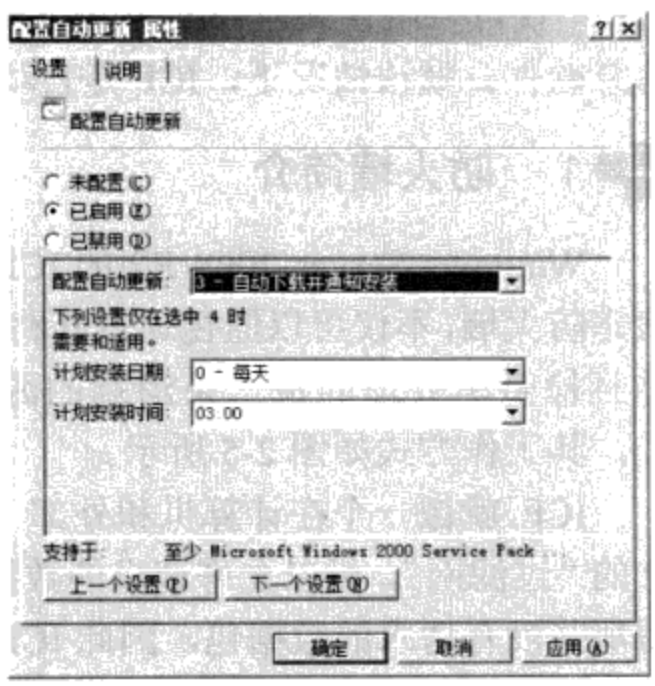


图 2-3 “配置自动更新 属性”对话框

第 2 步，双击“配置自动更新”选项，显示“配置自动更新 属性”对话框。选择“已启用”单选按钮，并在“配置自动更新”下拉列表框中选择下载更新的方式，如图 2-3 所示。单击“确定”按钮保存配置。

第 3 步，双击“指定 Intranet Microsoft 更新服务位置”选项，显示“指定 Intranet Microsoft 更新服务位置 属性”对话框。选择“已启用”单选按钮，并在“设置检查更新的 Intranet 更新服务”和“设置 Intranet 统计服务器”文本框中键入 WSUS 服务器的地址即可，如图 2-4 所示。单击“确定”按钮保存。

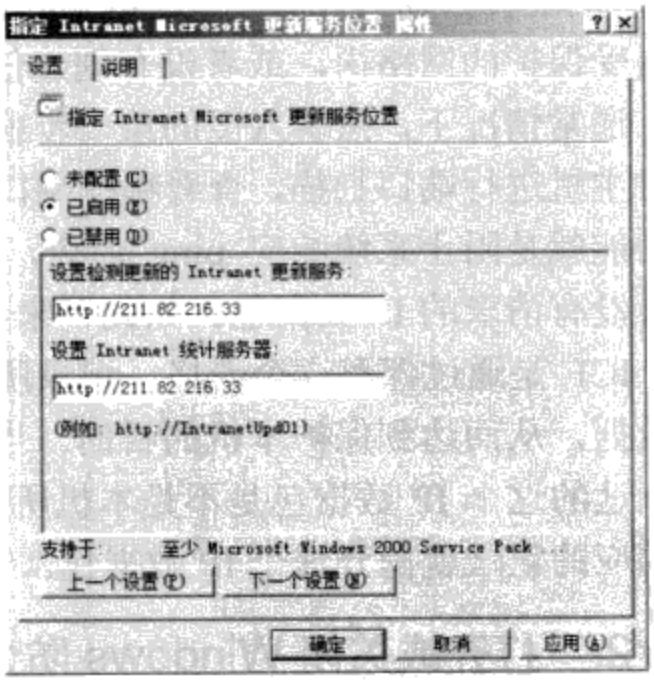


图 2-4 “指定 Intranet Microsoft 更新服务位置 属性”对话框

经过这样的设置，Windows Server 2008 R2 就可以自动从 WSUS 服务器上检测并下载更新程序了。

2.2 Windows Server 2008 R2 基本安全

Windows Server 2008 R2 系统防火墙，可以保护本地系统所有网络连接，并且允许用户针对不同的网络连接启用配置不同的安全策略。在安装网络服务或新的应用程序之后，防火墙安全配置向导，将提示对服务或应用程序访问网络要执行的操作，充分确保本地系统的安全。

2.2.1 Internet 防火墙

Internet 防火墙（Internet Connection Firewall，ICF）是 Windows 系统内置的简单防火墙。ICF 不仅可以阻止来自外部网络的恶意访问或攻击，还可以阻止当前服务器向其他计算机发送恶意软件。默认情况下，ICF 是自动开启的。

1. 防火墙简介

Windows Server 2008 R2 的 ICF 是一种典型的状态防火墙，不仅可以监视通过其路径的所有通信，并且检查所处理的每一条消息的源地址和目的地址，其工作方式如图 2-5 所示。

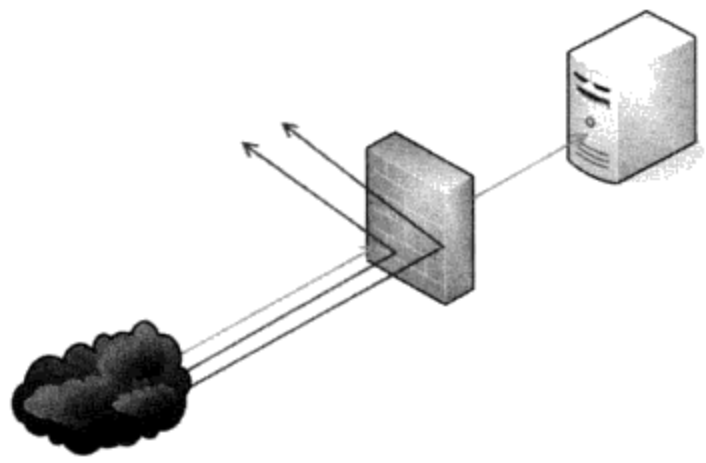


图 2-5 Internet 防火墙

ICF 就像一个在计算机和外部 Internet 之间建立的“过滤网”，可以允许请求的数据包通过，而阻碍那些没有请求的数据包，因此 ICF 是一个动态数据包过滤器。可以对直接连接 Internet 或连接在运行 ICF 的“Internet 连接共享主机”后的计算机提供保护。启用后，ICF 会禁止所有来自 Internet 的未经允许的连接。为此，防火墙使用“网络地址转换器（NAT）”逻辑来验证访问网络或本地主机的入站请求。如果网络通信不是来自受保护的网络内，或者没有创建任何端口映射，入站数据就被丢弃。

通常情况下，黑客入侵的第一步就是找到所要攻击主机的 IP 地址，再使用 ping 命令，然后对主机进行端口扫描，查看哪些端口是开放的，最后找出系统漏洞进行攻击。ICF 的一个重要功能就是阻止系统响应 ping 命令，而且，ICF 还禁止外部程序对本机进行端口扫描，丢弃所有没有请求的 IP 数据包。如此一来，可以极大地减少被黑客利用的系统漏洞。

ICF 是通过保存一个表格，记录所有自本机发出的目的 IP 地址、端口、服务以及其他一些数据，从而达到保护本机的目的。当一个 IP 数据包进入本机时，ICF 会检查这个表格，查看到达的这个 IP 数据包是不是本机所请求的，如果是就允许通过，如果在这个表格中没有找到相应的记录就抛弃这个 IP 数据包。

2. 打开或关闭 Windows 防火墙

在 Windows Server 2008 R2 的“控制面板”窗口中，双击“Windows 防火墙”打开 Windows 防火墙已启用。当前服务器上设置两个网络连接，分别用于连接私有网络和公用网络。

单击“打开或关闭 Windows 防火墙”链接，显示如图 2-6 所示“自定义每种类型的网络的设置”窗口，系统默认选择“启用 Windows 防火墙”单选按钮。如果同时选中“阻止所有传入连接，包括位于允许程序列表中的程序”复选框，则防火墙将阻止所有主动连接当前服务

器的尝试，当需要为该服务器提供最大限度的保护时，才使用该设置，启用该设置后将忽略“例外”列表中的所有设置。

图 2-6 “Windows 防火墙设置”对话框

提示 选中“Windows 防火墙阻止新程序时通知我”复选框，可以在防火墙阻止某应用程序或服务访问网络时，提示用户可以选择的操作。

3. 允许程序或功能通过防火墙

在“Windows 防火墙”窗口中，单击允许程序或功能通过 Windows 防火墙链接，显示如图 2-7 所示“允许程序通过 Windows 防火墙通信”窗口。在“允许的程序和功能”列表框中，选择该服务器欲提供的网络服务即可。通过选择其后面“家庭/工作（专用）”或“公用”对应的复选框，即可允许其通过哪种网络连接与网络通信。

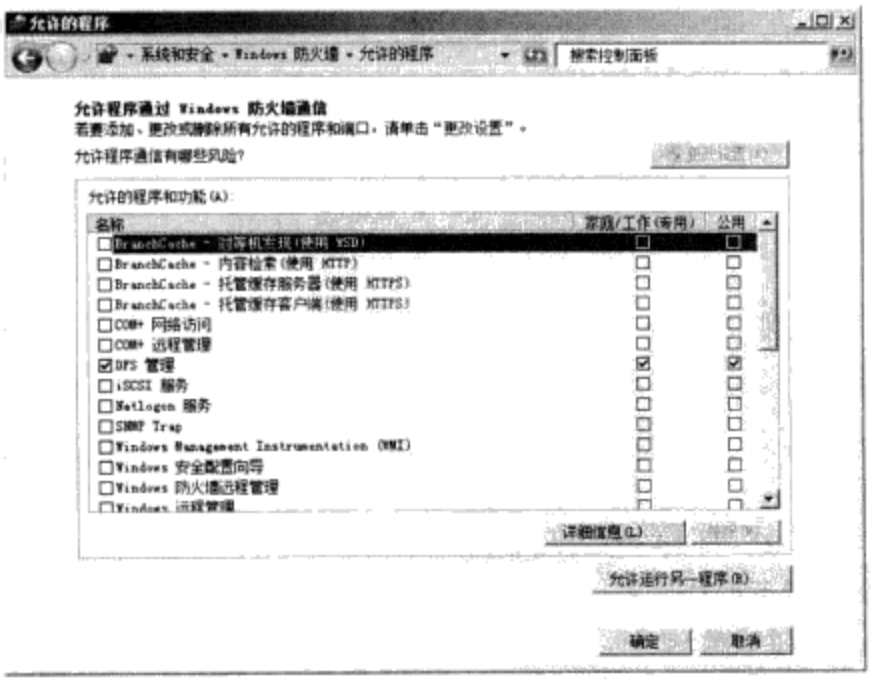


图 2-7 “允许程序通过 Windows 防火墙通信”窗口

提示 默认情况下，系统中安装需要访问网络的应用程序或功能后，将自动添加到“允许的程序和功能”列表中。

如果希望允许通过 Windows 防火墙访问网络的应用程序名称，没有出现在列表中，则可以单击“允许运行另一程序”按钮，显示如图 2-8 所示“添加程序”对话框。单击“浏览”按钮，选择希望添加的应用程序或功能对应的可执行文件即可

单击“添加”按钮，将选定应用程序添加到“允许的程序和功能”列表中。

4. 还原默认设置

单击“还原默认设置”超级链接，显示如图 2-9 所示“还原默认设置”窗口。单击“还原为默认设置”按钮即可撤销所有 Windows 防火墙设置，恢复至初始状态。需要注意的是，必须是本地计算机上 Administrators 组的成员，或者是被委派了适当的权限的用户，才可以还原 Windows 防火墙默认设置。如果计算机已经加入到域，则 DomainAdmins 组的成员可以执行该操作。

图 2-8 “添加程序”对话框

图 2-9 “还原默认设置”窗口

2.2.2 高级安全 Windows 防火墙

高级安全 Windows 防火墙是从 Windows Server 2008 系统开始加入的安全功能，它结合了主机防火墙和 IPSec，可以对穿过网络边界防火墙和发自企业内部的网络攻击进行防护，是网络边界防火墙的一个有益的补充。高级安全 Windows 防火墙还可以同时控制传入和传出连接，可以轻松实现端到端的安全连接和用户身份验证。

1. 高级防火墙概述

高级安全 Windows 防火墙使用两组规则，配置如何响应传入和传出流量，确定允许或阻止流量类型。而连接安全规则确定如何保护计算机和其他计算机间的通信，通过使用防火墙配置文件，可以应用这些规则以及其他设置，监视防火墙活动和规则。

■ **防火墙规则**

配置防火墙规则以确定阻止还是允许流量通过。传入数据包到达计算机时，高级安全 Windows 防火墙会检查该数据包，确定其是否符合防火墙规则中指定的标准。如果数据包与规则中的标准匹配，则高级安全 Windows 防火墙执行规则中指定的操作，即阻止连接或允许连接。如果数据包与规则中的标准不匹配，则高级安全 Windows 防火墙将丢弃该数据包，并在防火墙日志文件中创建条目（如果启用了日志记录）。

■ **连接安全规则**

连接安全规则可以用来配置本地计算机与其他计算机之间特定的连接的 IPSec 设置。高级安全 Windows 防火墙首先使用该规则评估网络通信，然后根据该规则中所建立的标准，阻止或允许消息。默认状态下，高级安全 Windows 防火墙将阻止通信。如果所配置的设置要求连接安全（双向），而两台计算机无法互相进行身份验证，则同样会阻止连接。

■ **防火墙配置文件**

防火墙配置文件是一种分组设置的方法，如防火墙规则和连接安全规则，根据计算机连接到的位置将其应用于该计算机。高级安全 Windows 防火墙中有 3 个配置文件，分别是域、专用网络（例如家庭网络）和公用网络，用户每次只能从中选择一个使用。

■ **监视**

监视节点显示有关当前所连接的计算机（本地计算机或远程计算机）的信息。如果使用管理单元来管理组策略对象而不是本地计算机，则不会出现该节点。

2. 配置防火墙规则

防火墙规则是防火墙执行安全防护任务的重要指导，而创建和编辑防火墙规则的工作必须在“高级安全 Windows 防火墙”控制台中完成。这里以配置关于 ICMP 通信的防火墙规则为例，介绍高级防火墙规则的配置。

在高级安全 Windows 防火墙控制台中，选择“入站规则”，右击“核心网络 – 需要目标不可访问的碎片 ICMPv4-In”选择快捷菜单中的“属性”选项，打开如图 2-10 所示对话框。在“常规”选项卡中，选中“已启用”复选框，表示启用该防火墙规则，然后选择“阻止连接”即可阻止来网络的此类网络请求。

图 2-10 “网络-路由器请求 属性”对话框

修改规则完成后，单击“确定”按钮应用并保存配置。

3. 创建防火墙规则

高级安全 Windows 防火墙使用出站和入站两组规则，配置其如何响应传入和传出的请求。默认情况下，管理员在该服务器上安装微软公司提供的网络服务后，将自动添加在高级防火墙的出站规则列表中，并允许通过防火墙。但是，如果安装的是第三方网络服务，则必须通过手动创建相关规则，才可以将服务法不到网络。例如，如果在当前服务器上配置基于 Serv-U 的 FTP 服务器，则必须同时创建提供上传和下载的入站规则。

第 1 步，在高级安全 Windows 防火墙控制台中，右击“入站规则”，选择快捷菜单中的“新规则”选项，即可启动“新建入站规则向导”。连续单击“下一步”按钮，在“规则类型”对话框中选择相应的方式，这里选择“端口”单选按钮。在“协议和端口”对话框。根据服务使用的协议类型选择“TCP”或者“UDP”单选按钮，本例中 FTP 服务使用的是 TCP 端口，选择“TCP”单选按钮即可。选择“特定本地端口”单选按钮，输入服务使用的端口号，如果在配置服务器时指定了非默认端口，则在这里也应指定相应端口，例如 2121，如图 2-11 所示。

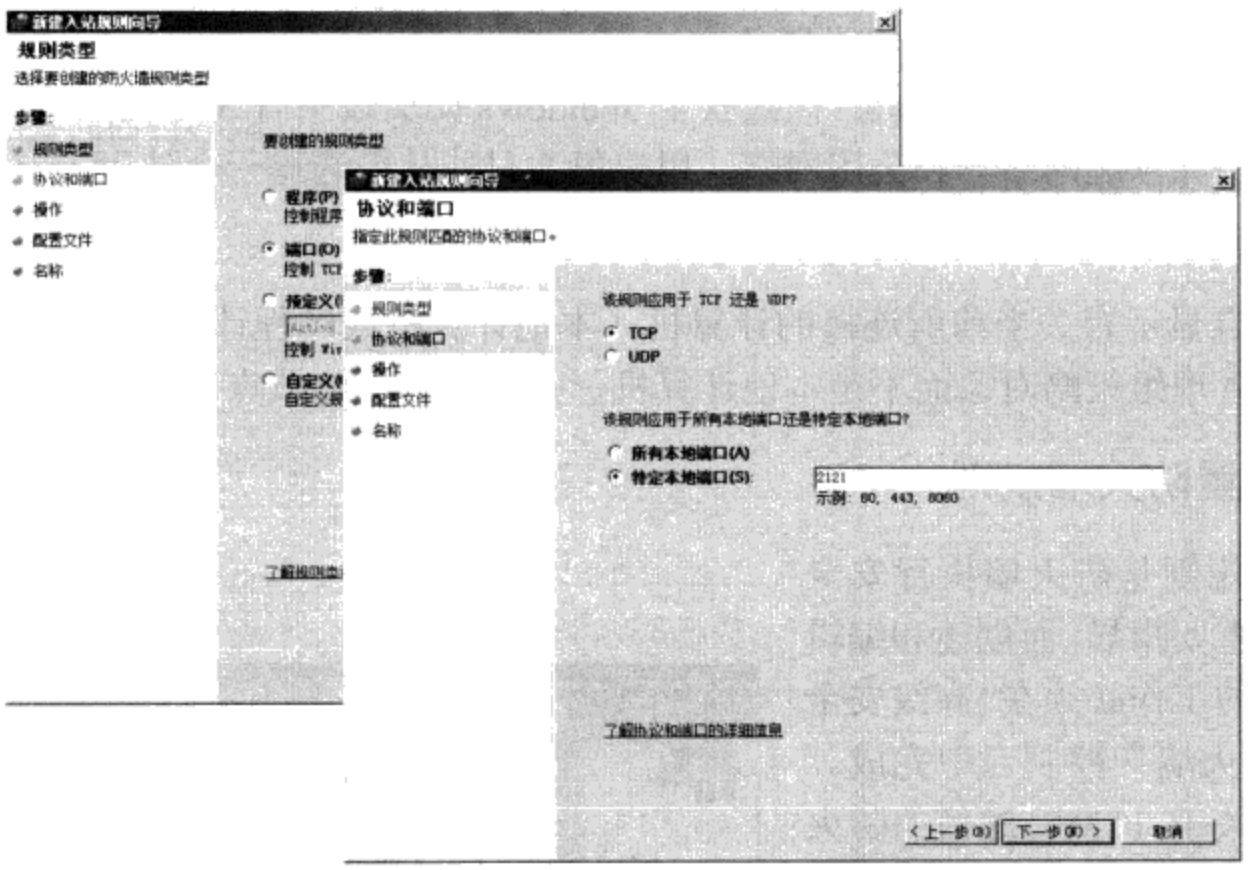


图 2-11 选择规则类型、协议和端口

第 2 步，连续单击“下一步”按钮，在“操作”对话框，选择“允许连接”单选按钮。如果选择“只允许安全连接”单选按钮，则高级防火墙只允许特定的安全用户访问服务器，即使用 IPSec 身份验证的用户。如果选择“阻止连接”单选按钮，则将阻止所有用户到服务器的连接。在“配置文件”对话框中，设置该规则的应用范围，如图 2-12 所示。例如，FTP 服务器仅对 Internet 用户提供服务，则选择“公用”复选框即可，内网用户对服务器的访问将不受防火墙保护。

第 3 步，单击“下一步”按钮，显示如图 2-13 所示“名称”对话框。在“名称”文本框中输入该入站规则的显示名称，便于识别。

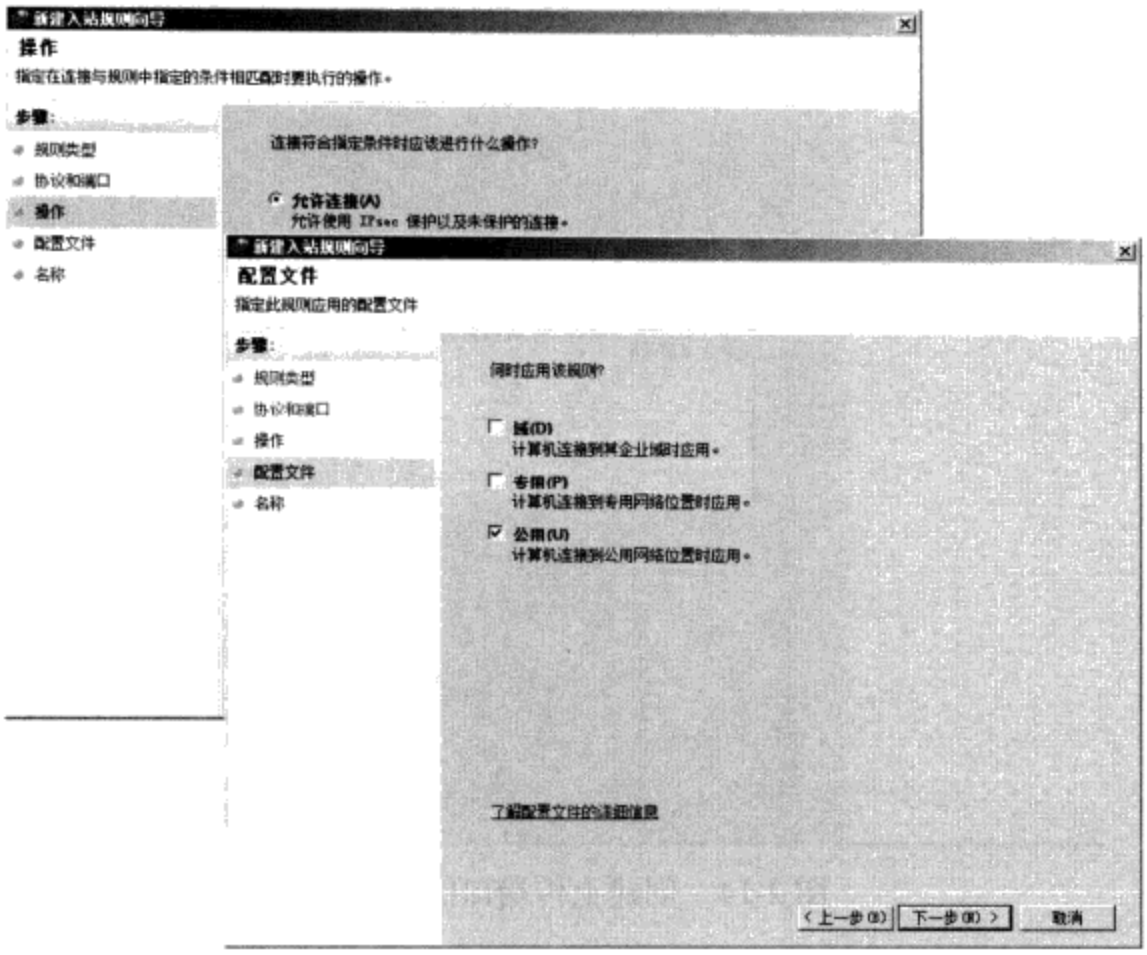


图 2-12　设置操作和配置文件

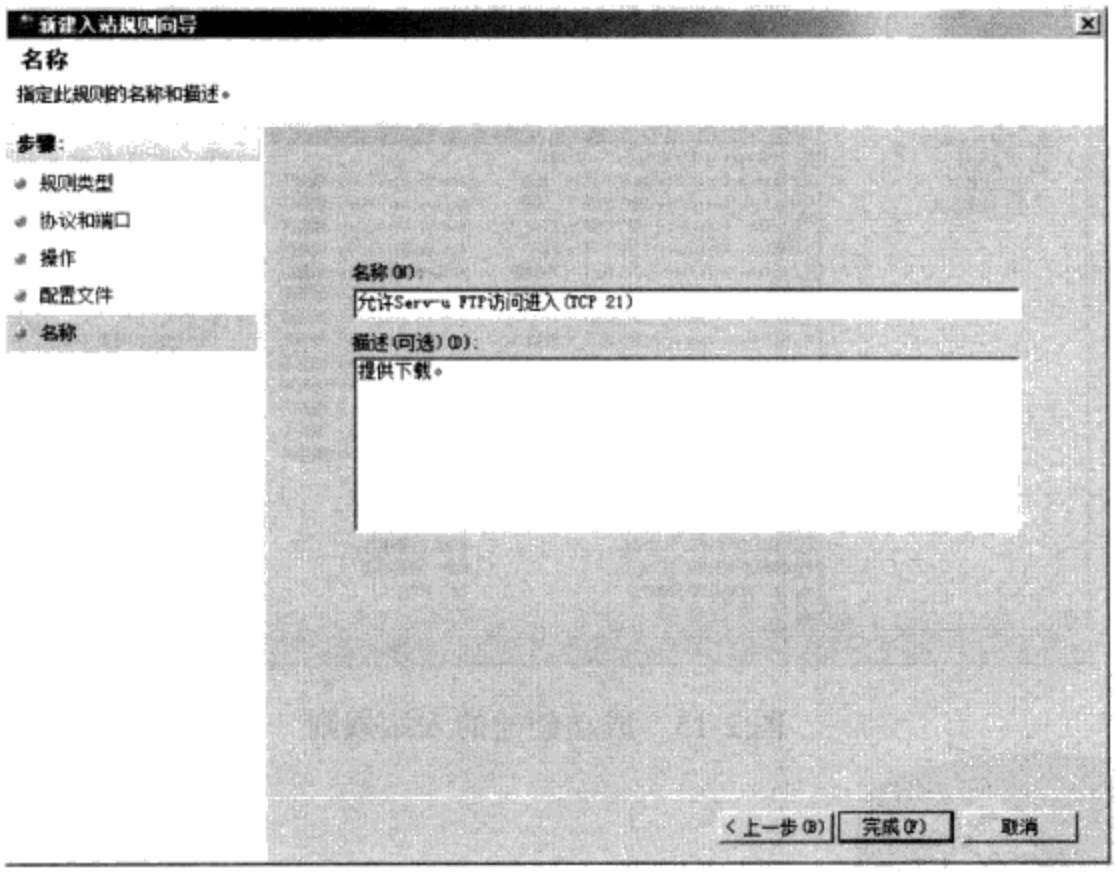


图 2-13　“名称”对话框

第 4 步，单击“完成”按钮，即可保存已创建的入站规则。FTP 服务器提供下载和上传服务时，需要使用不同的端口，因此还需要对用于发布上传服务的端口创建入站规则，如图 2-14 所示。详细操作过程，这里不再赘述。

第 5 步，默认情况下，成功创建的入站规则将自动启用，并显示在“入站规则”窗口中，如图 2-15 所示。

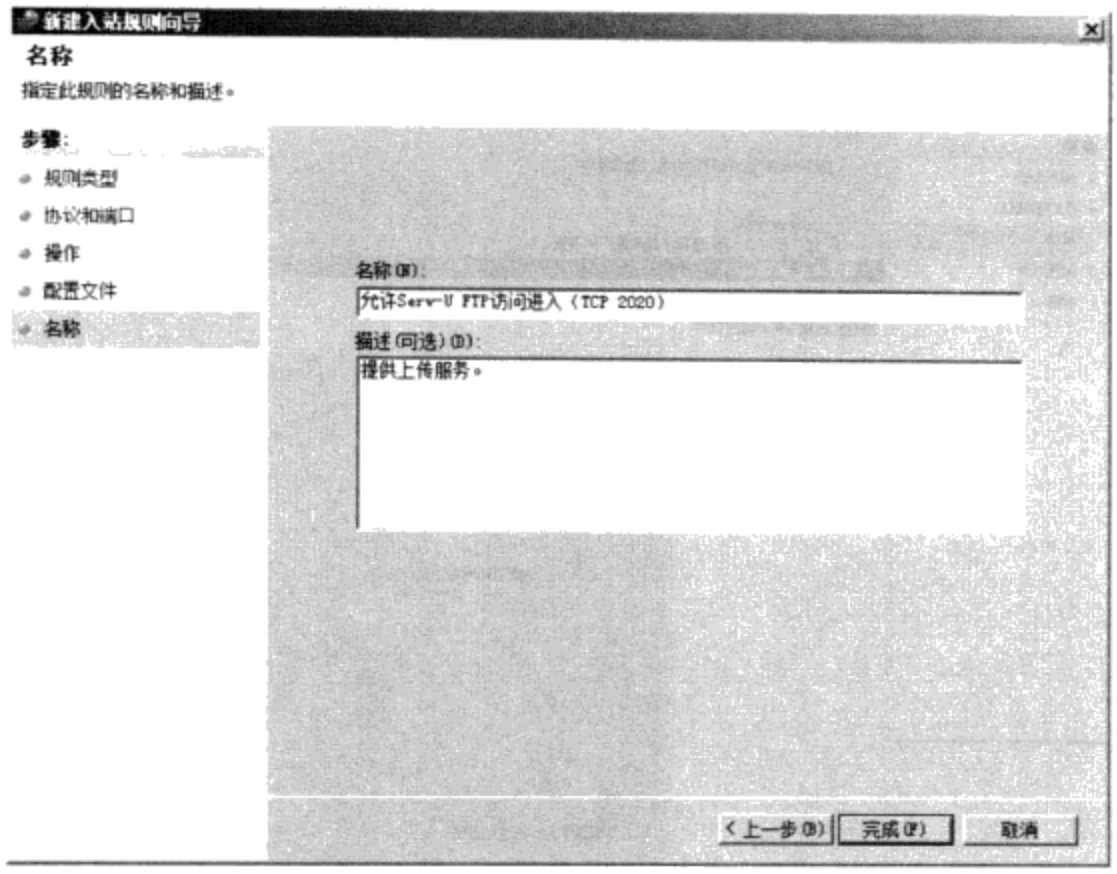


图 2-14　创建上传端口的入站规则

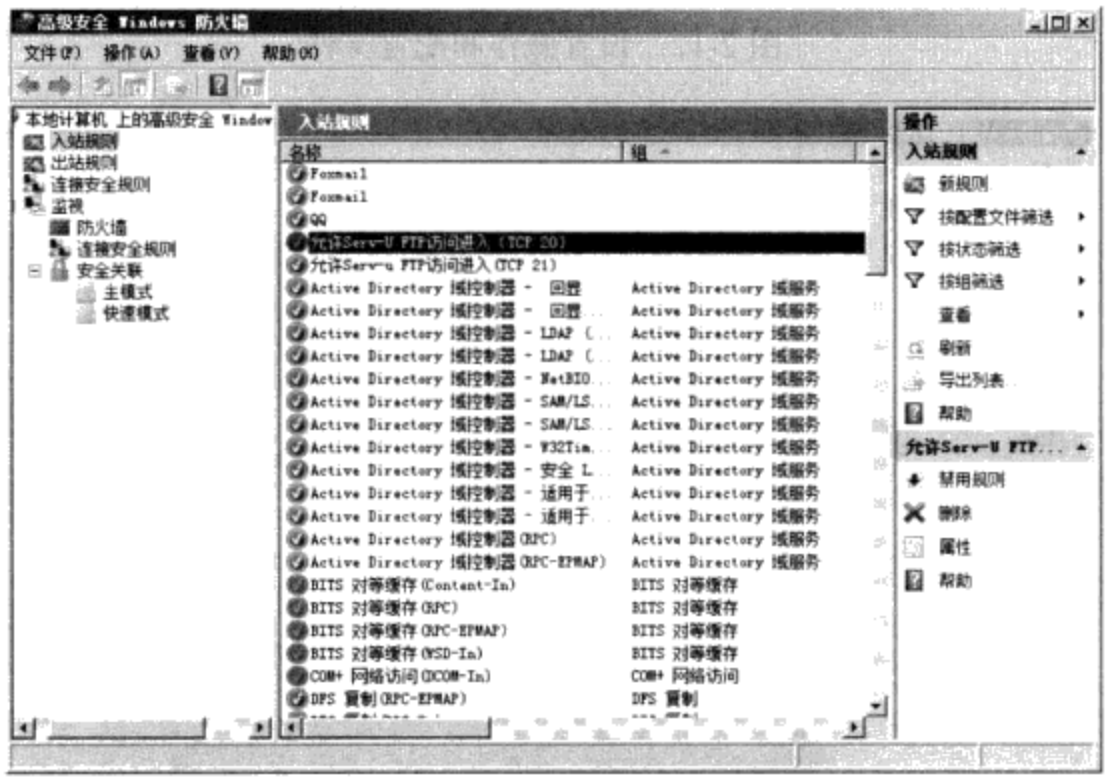


图 2-15　成功创建的入站规则

2.2.3 安全配置向导

安全配置向导（SCW）可以帮助管理员快速完成创建、编辑、应用和回滚安全策略操作。用户可以根据需要创建针对某个服务器角色的安全策略，并且可以将其应用到其他服务器上。配置和应用 SCW 时应注意以下几点：

- SCW 禁用不需要的服务并提供对具有高级安全性的 Windows 防火墙的支持。
- 使用 SCW 创建的安全策略与安全模板不同，其中前者扩展名为.xml，而后者扩展名为.inf。用户创建的安全策略源于安全模板，安全模板包含的安全设置可以应用于所有的服务器角色。

- 部署 SCW 安全策略后并不会影响服务器提供服务时所需的组件，并且应用之后，管理员仍可以通过服务器管理器安装所需的组件。
- 应用 SCW 安全策略之后，SCW 将自动选择所有从属角色。
- 创建和应用 SCW 安全策略时，应确保服务器的 IP 协议及端口配置完全正确。

1. 创建安全策略

第 1 步，依次单击“开始”→“管理工具”→“安全配置向导”，即可启动“安全配置向导”，用户也可以在“开始”菜单的“开始搜索”文本框中输入 SCW 命令，单击“确定”按钮来启动“安全配置向导”。单击“下一步”按钮，显示如图 2-16 所示“配置操作”对话框。安全配置向导提供了 4 种配置操作：

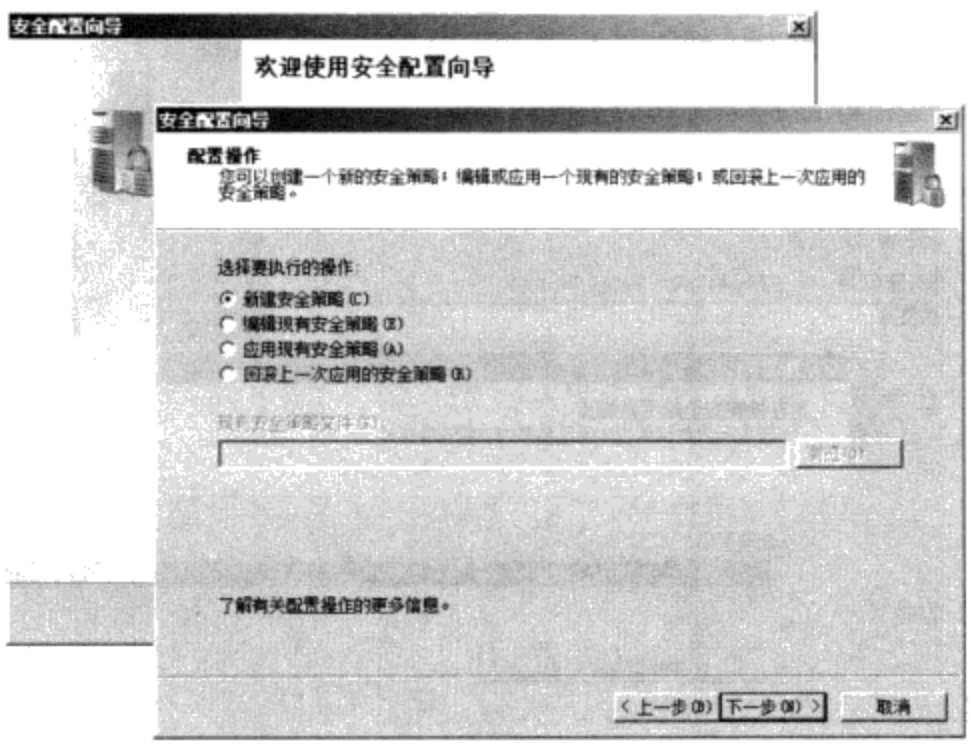


图 2-16 “欢迎使用安全配置向导”对话框

- 创建新的安全策略。可以创建用于配置服务、Windows 防火墙、Internet 协议安全（IPsec）设置、审核策略和特定注册表设置的安全策略。安全策略文件是 XML 格式文件，默认保存路径为%systemroot%\security\msscw\Policies。
- 编辑现有安全策略。可以编辑已使用 SCW 创建的安全策略。必须先选择“编辑现有安全策略”，才能浏览到要编辑的安全策略文件所在的文件夹。编辑的策略可存储在本地上或网络共享文件夹中。
- 应用现有安全策略。使用 SCW 创建安全策略后，可将其应用到测试服务器，或者应用到生产环境。

提示 在将新创建或新修改的安全策略应用到生产环境之前，首先进行测试，然后将安全策略部署到业务系统中，测试可使新策略在生产环境中导致意外结果的可能性降至最低。

- 回滚上一次应用的安全策略。如果使用 SCW 应用的安全策略使服务器功能达不到预期的效果，或者导致其他非预期结果，则可以回滚该安全策略，将自动从该服务器删除对应的安全策略。

注意　如果策略是在“本地安全策略”中编辑的，在应用策略后，这些更改就不能回滚到应用前的状态。对于服务和注册表值，回滚过程还原了在配置过程中更改的设置。对于 Windows 防火墙和 IPsec，回滚过程取消当前使用的任何 SCW 策略的分配，并重新分配在配置时使用的前策略。

第 2 步，单击“下一步”按钮，显示如图 2-17 所示“选择服务器”对话框。在“服务器”文本框中，输入需要进行安全配置的 Windows Server 2008 R2 服务器的主机名或 IP 地址。也可以单击“浏览”按钮，选择需要进行安全配置的目标计算机。单击“下一步”按钮，开始扫描配置数据库，主要包括已安装或运行的网络服务、IP 地址及子网信息等。

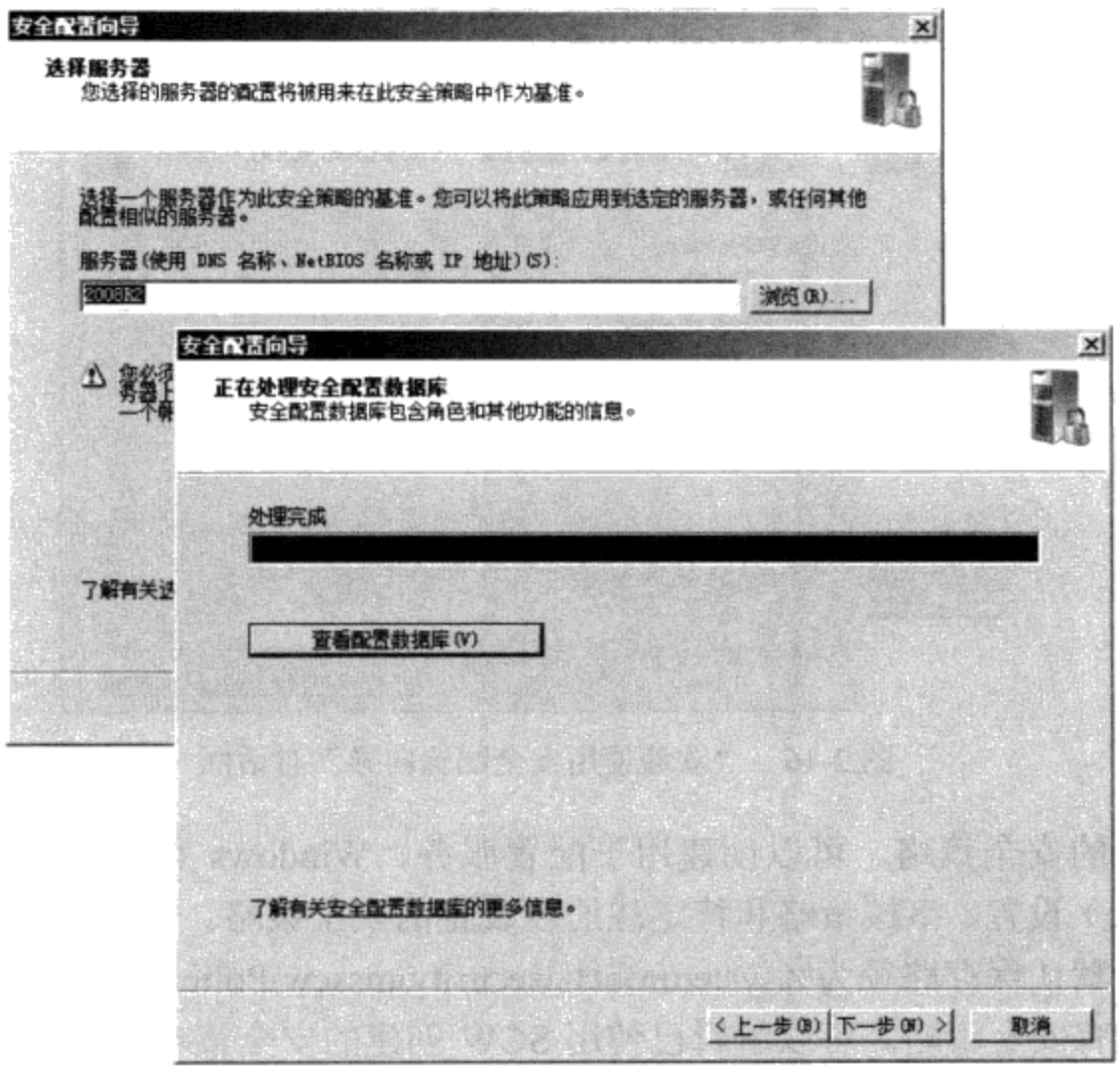


图 2-17　选择服务器并准备安全配置数据库

第 3 步，单击“下一步”按钮，显示“基于角色的服务配置”对话框，连续单击“下一步”按钮，分别为选定服务器安装的服务器角色、角色服务、功能以及其他系统服务配置安全策略，如图 2-18 所示。

第 4 步，单击“下一步”按钮，显示“网络安全”对话框。单击“下一步”按钮，显示“网络安全规则”对话框。系统默认，显示“所有规则”，即该服务器上目前开放的所有端口。也可以在“查看”下来列表中选择其他查看方式。单击安全规则前面的三角形按钮，还可以查看其详细信息，如图 2-19 所示。

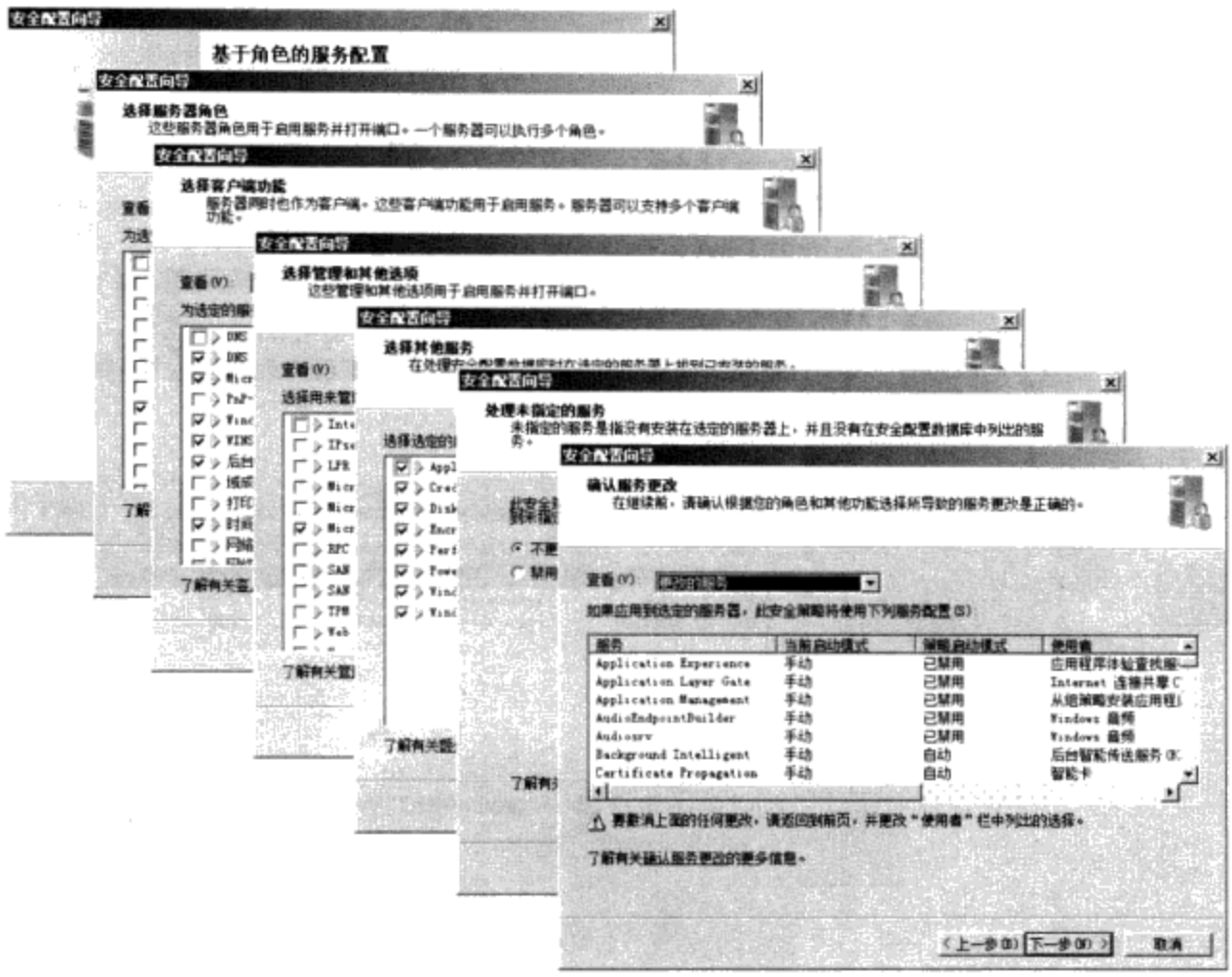


图 2-18　基于角色的服务配置

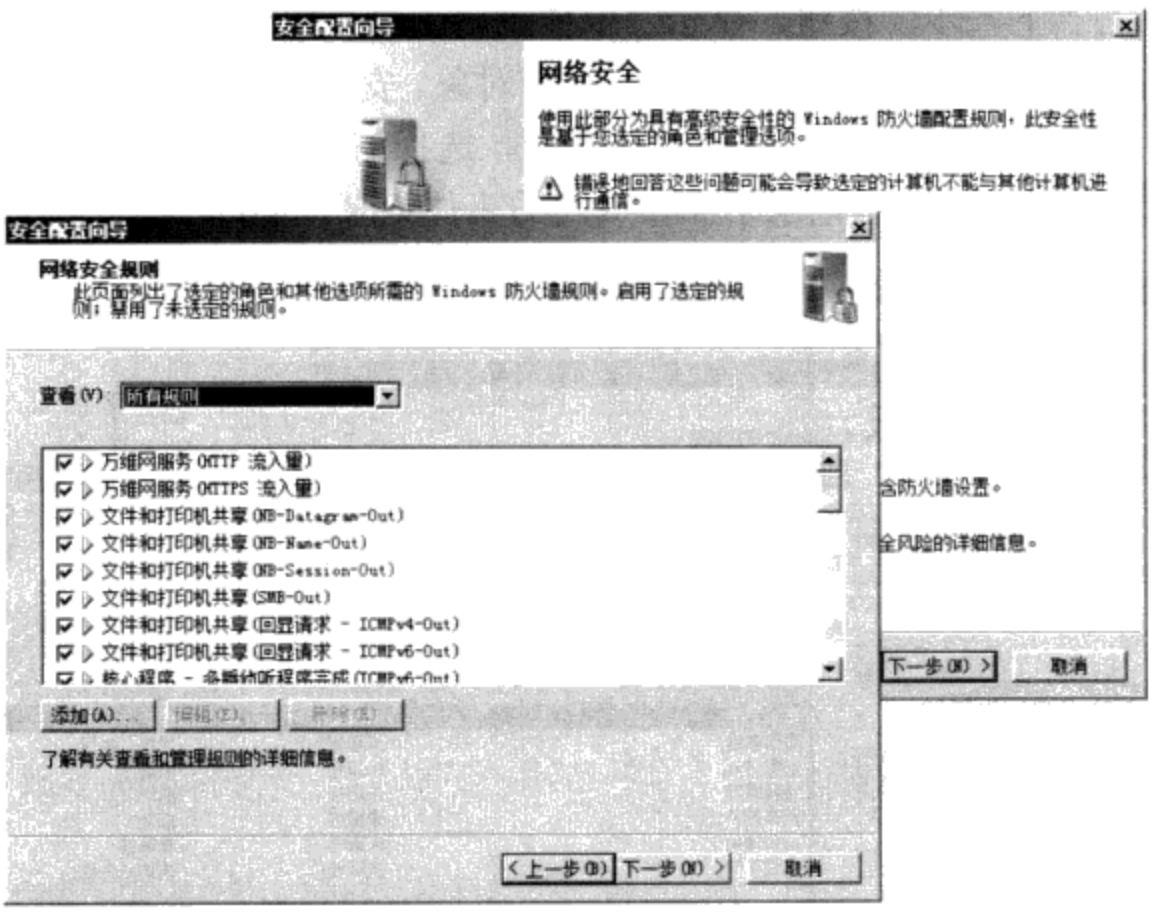


图 2-19　“网络安全”对话框

第 5 步，单击“下一步”按钮，显示“注册表设置”对话框。通过该设置可以修改 Windows Server 2008 R2 服务器注册表中一些特殊键值，从而严格限制用户的访问权限。建议用户不要跳过此步骤。单击“下一步”按钮，显示“要求 SMB 安全签名”对话框。设置选定的服务器和客户端的通信信息，保持系统默认的全部选择状态即可，如图 2-20 所示。

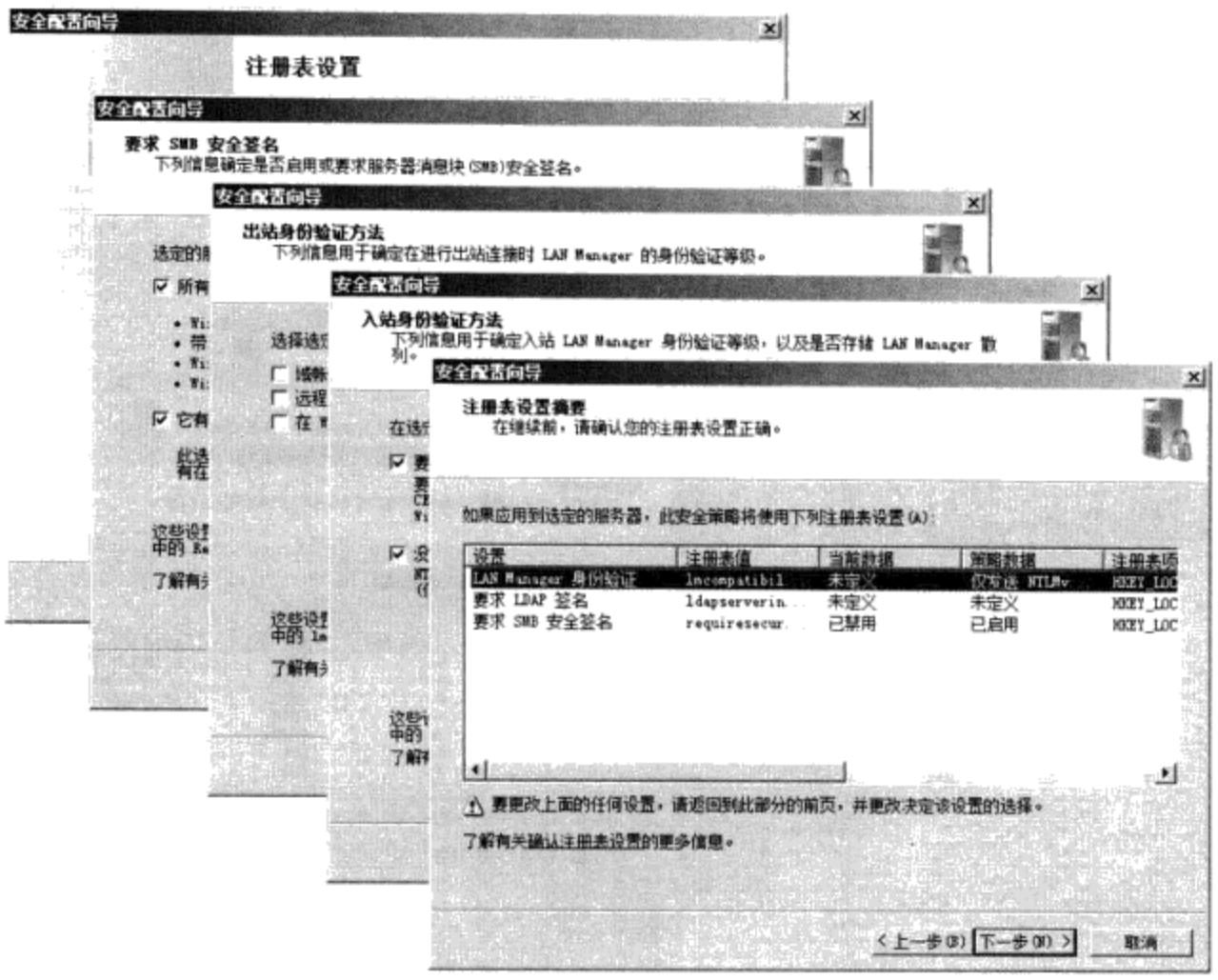


图 2-20 “注册表设置”对话框

第 6 步，单击“下一步”按钮，显示“审核策略”对话框。Windows 审核策略主要用于审核日志记录中的相关内容，并确定受影响的系统对象。安全策略回滚功能是无法回滚安全向导中的审核策略设置的。连续单击“下一步”按钮，选择需要审核的目标，选择“审核成功的操作”单选按钮，即只审核日志记录中操作成功的事件记录，如图 2-21 所示。

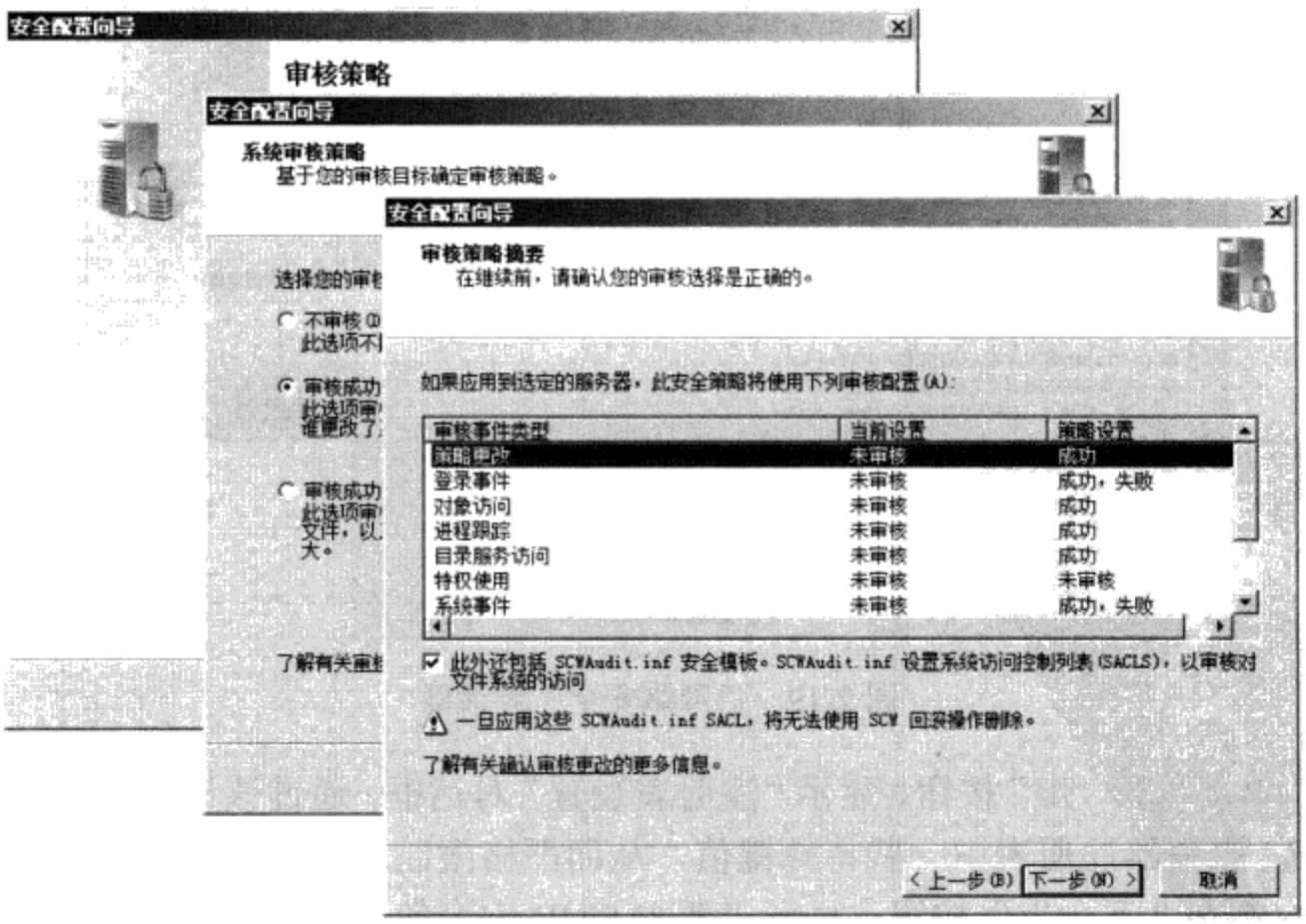


图 2-21 “审核策略”对话框

第 7 步，单击“下一步”按钮，显示“保存安全策略”对话框。保存之后，即可将该安全策略应用到当前或其他服务器上。单击“下一步”按钮，显示如图 2-22 所示“安全策略文件名”对话框。在保存安全策略文件的路径之后输入安全策略文件名，根据需要输入相关描述信息。

提示 单击“包括安全模板”按钮，还可以向当前安全策略中添加其他安全模板中的安全规则，这些规则将拥有较高的优先级。SCW 回滚功能将无法回滚已经应用的策略模板中的规则设置。

第 8 步，单击“下一步”按钮，显示如图 2-23 所示“应用安全策略”对话框。如果选择“现在应用”单选按钮，则可以将安全策略立即应用到当前服务器；建议选择“稍后应用”单选按钮，测试之后再应用到服务器。

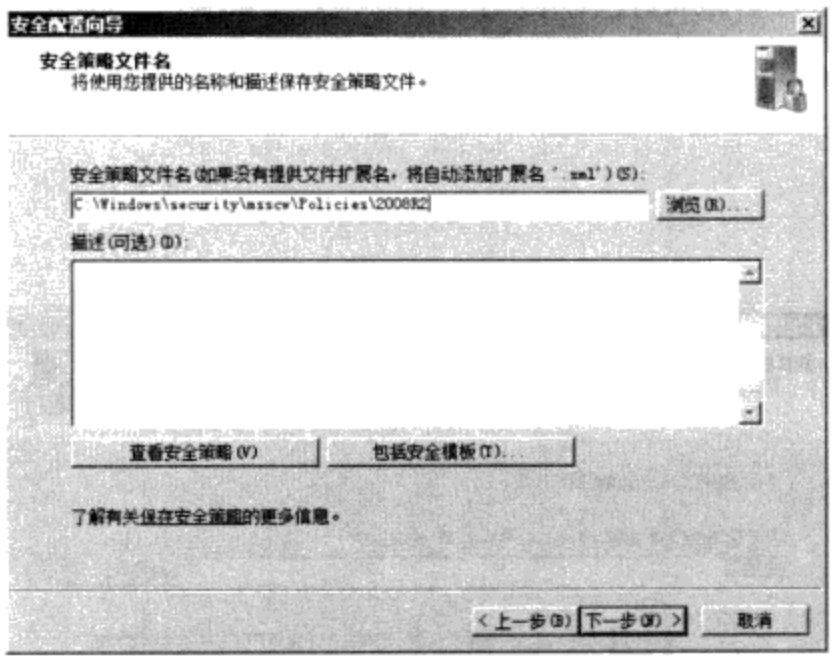


图 2-22 “安全策略文件名”对话框

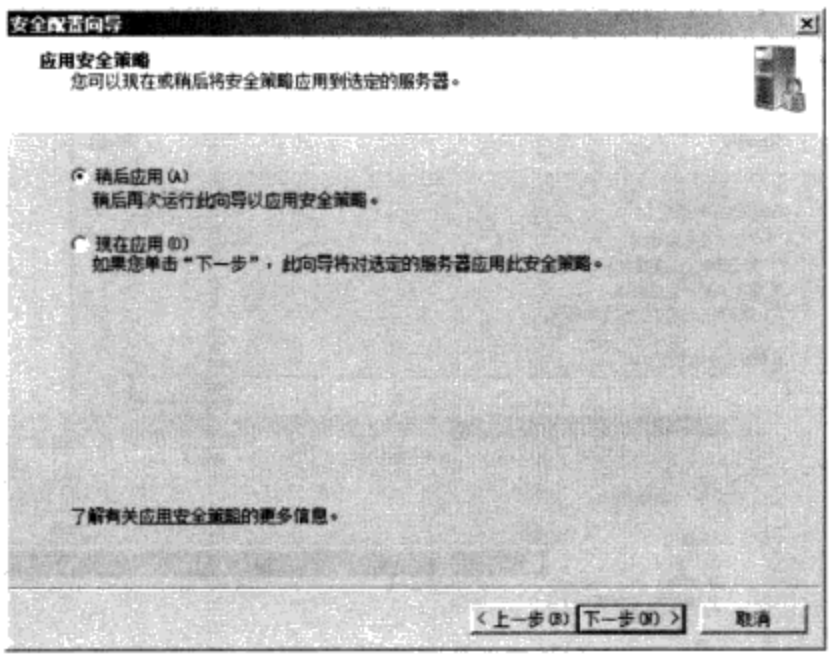


图 2-23 “应用安全策略”对话框

第 9 步，单击“下一步”按钮，显示如图 2-24 所示“正在完成安全配置向导”对话框。单击“完成”按钮，完成安全策略的设置。

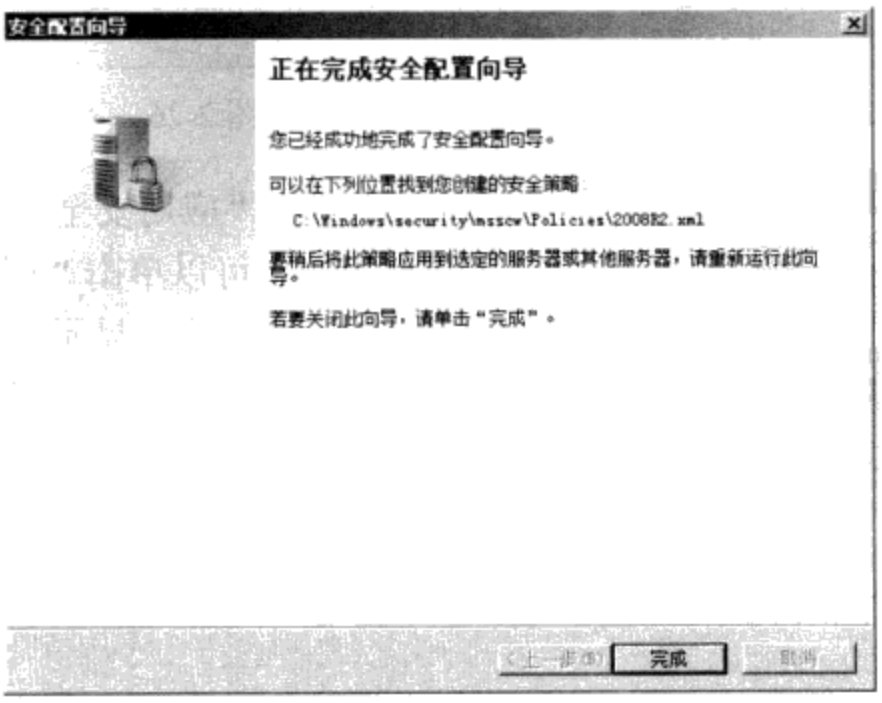


图 2-24 “正在完成安全配置向导”对话框

2. 应用安全配置策略

使用安全配置向导创建的安全策略，可直接应用于所有运行 Windows Server 2008 或者 Windows Server 2003 SP1/SP2/R2 操作系统的网络服务器。大规模应用安全策略之前必须经过严格测试，确认可行之后方可部署。应用安全配置策略之后，必须重新启动计算机才可以生效。应用安全策略的主要操作步骤如下：

第 1 步，依次单击“开始”→“管理工具”→“安全配置向导”，打开“安全配置向导”对话框，单击“下一步”按钮，在“配置操作”对话框中，选择“应用现有安全策略”单选按钮，在“现有安全策略文件”文本框中输入安全策略文件的路径，也可单击“浏览”按钮查找，如图 2-25 所示。

第 2 步，单击“下一步”按钮，显示如图 2-26 所示“选择服务器”对话框，在“服务器”文本框中，输入想要应用到的服务器名称或 IP 地址。如果目标服务器为远程主机，则应单击“指定用户账户”按钮，选择连接到指定主机部署安全策略使用的用户账户及凭证。

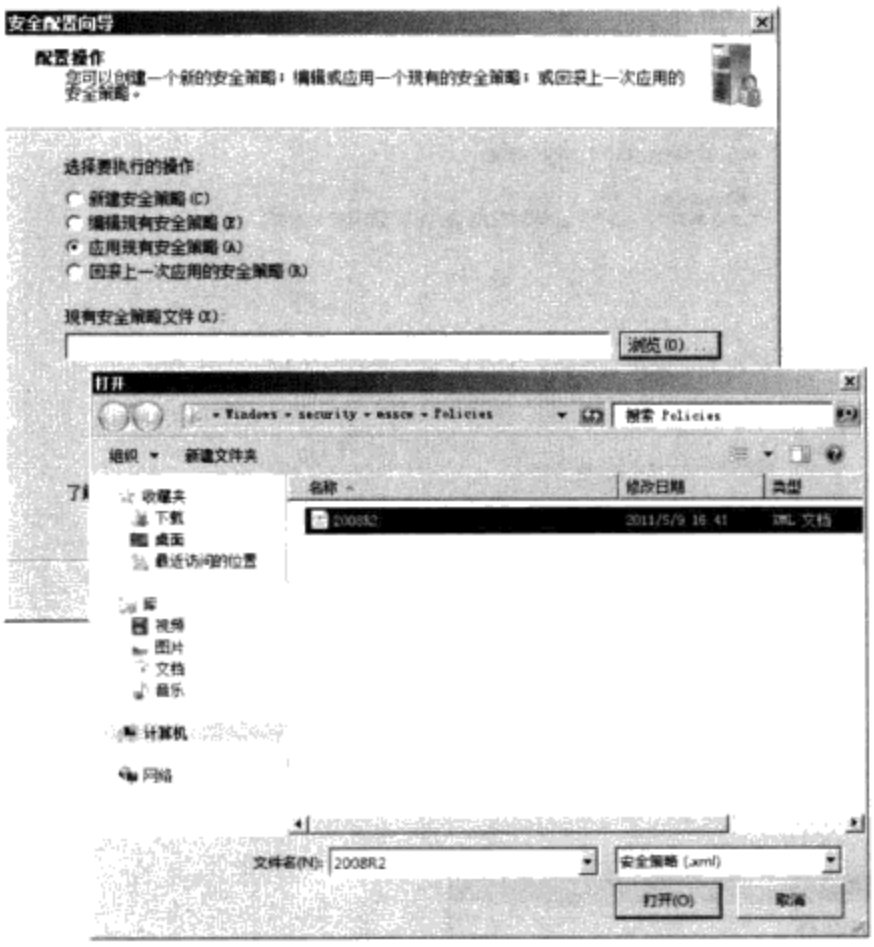


图 2-25 应用安全配置策略

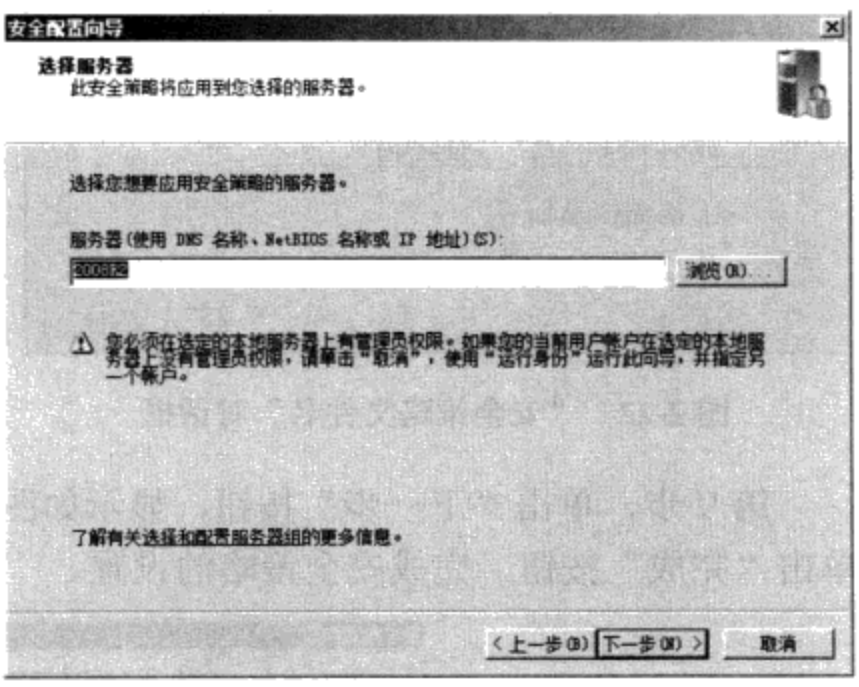


图 2-26 “选择服务器”对话框

第 3 步，单击“下一步”按钮，显示如图 2-27 所示“应用安全策略”对话框，在“安全策略描述”信息框中显示的是该策略的相关描述信息，也可以单击“查看安全策略”按钮打开“SCW 查看器”窗口，查看其详细信息。单击“下一步”按钮，显示“正在应用安全策略”对话框。将安全策略应用到本地计算机大概需要几分钟时间，应用到远程计算机时所需时间可能更长一些。应用完成之后将提示“应用完成”，单击“下一步”按钮，显示“正在完成安全配置向导”对话框。

第 4 步，单击“完成”按钮，关闭安全配置向导。重新启动计算机后，应用的安全策略即可生效。

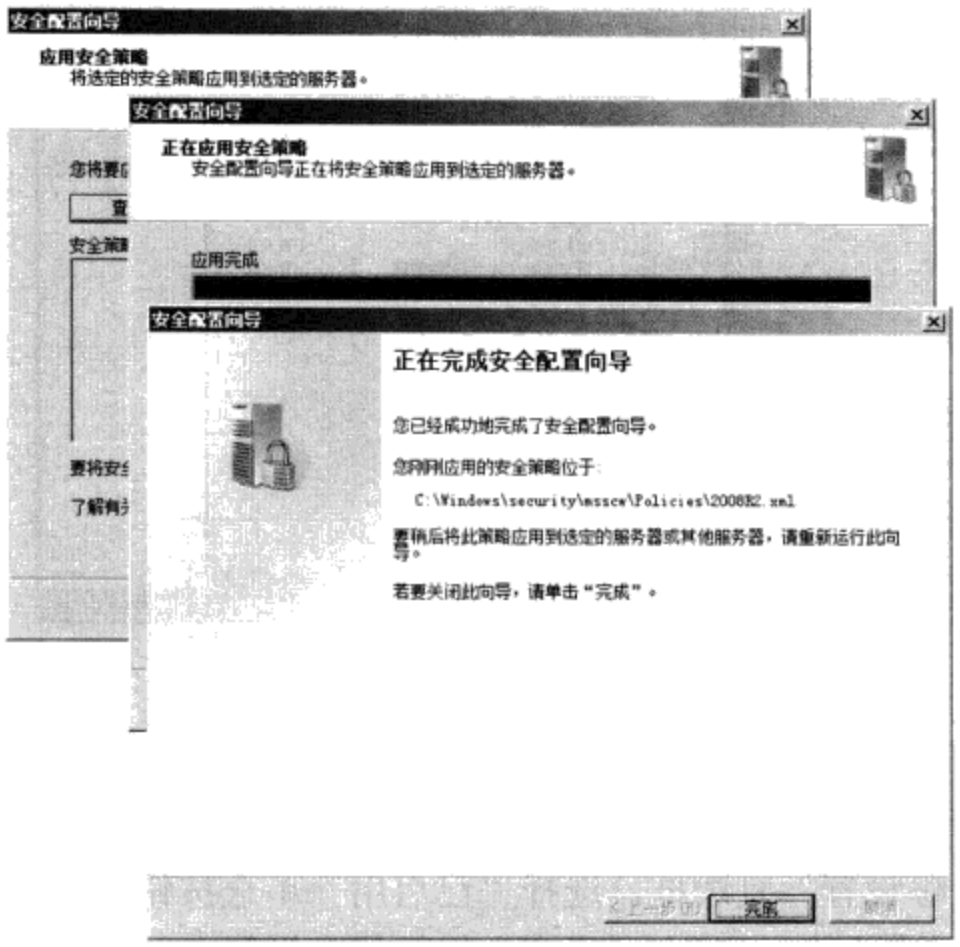


图 2-27 “应用安全策略”对话框

2.2.4 安全配置和分析

系统安全分析是指将当前系统配置状态与选定模板进行对比，通过查看分析结果，用户可以了解当前配置存在的问题。如果选定的模板是通过安全测试和验证的，则可以立即依据该模板对本地系统数据库进行快速配置。

1. 准备系统安全配置数据库

默认情况下，Windows Server 2008 R2 系统的所有安全配置信息都保存在系统默认的安全配置数据库中，其路径为 C:\Windows\security\database\secedit.sdb。由于当前策略正处于应用状态，所以用户无法使用任何安全模板对其进行分析和配置。此时，可以复制默认数据库，然后对数据库副本进行安全分析和配置，然后使用配置后的副本替代默认数据库，达到安全配置的目的。

除此之外，用户也可以通过新建系统安全配置数据库，然后使用选定模板对其进行配置，完成后在使其替代原有默认数据库，达到安全配置的目的。

2. 准备安全模板

默认情况下，Windows Server 2008 R2 系统是不提供安全模板的，但是安装 Active Directory 服务后将自动创建一个名称为 DC security.inf 的安全模板，用于对域控制器进行安全分析和配置。对于普通服务器系统建议使用新建的安全模板执行安全分析和配置。由于默认模板的安全策略都是未配置的，所以用户需要根据实际情况进行定义。

第 1 步，在控制台窗口的“安全模板”节点下，打开名称为 test.inf 的新建“安全模板”，显示如图 2-28 所示窗口，此时所有策略设置都是没有定义的。

图 2-28 打开安全模板

第 2 步，双击希望配置的策略（以“账户策略”→“密码策略”中的“密码必须符合复杂性要求”策略为例），显示如图 2-29 所示“密码必须符合复杂性要求 属性”对话框，选中“在模板中定义这个策略设置”复选框，选择“已启用”单选按钮（依实际需求而定，某些策略还需要设置相关数据或阀值），单击“确定”按钮保存设置。

第 3 步，使用相同的方法配置安全模板中的其他策略设置。为了便于演示，此处仅以配置“账户策略”中的“密码策略”为例加以介绍，具体配置结果如图 2-30 所示。

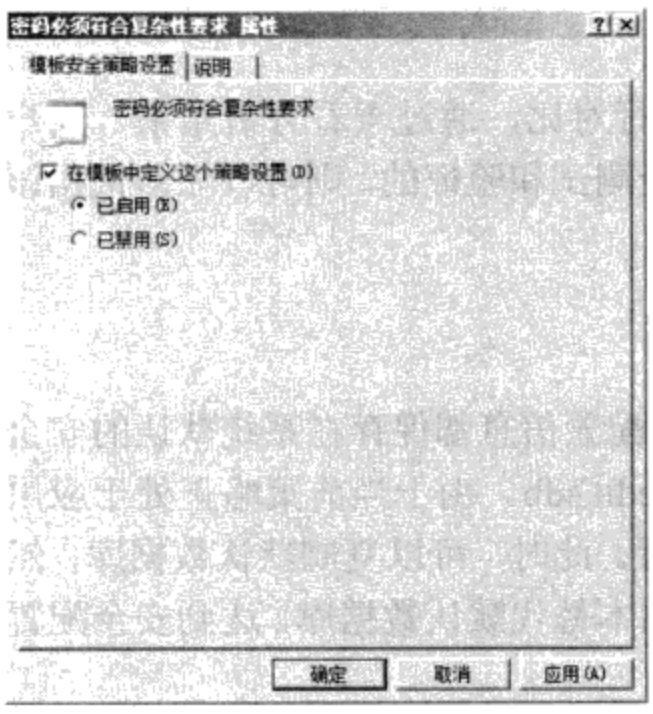


图 2-29 “密码必须符合复杂性要求 属性”对话框

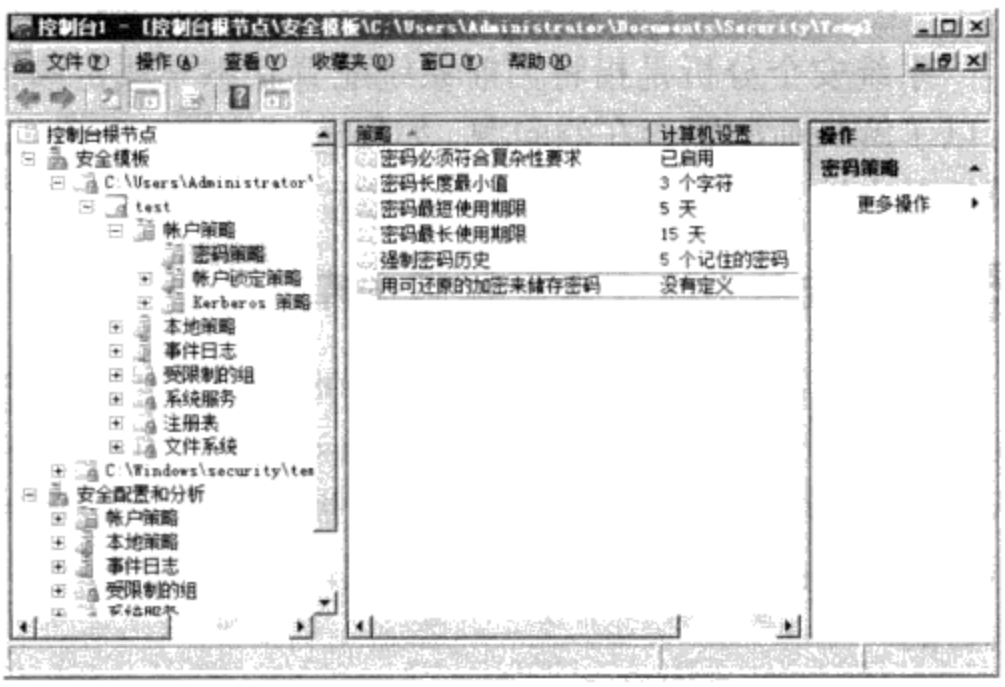


图 2-30 安全模板的配置状态

3. 执行安全配置和分析

添加“安全配置和分析”管理单元的过程与添加“安全模板”管理单元的过程类似。

第 1 步，在控制台窗口中，单击“文件”菜单选择“添加或删除管理单元”命令，显示“添加或删除管理单元”对话框，在“可用的管理单元”列表中选择“安全配置和分析”并单击“添加”按钮，将其天际到左侧“所选管理单元”列表中，如图 2-31 所示。

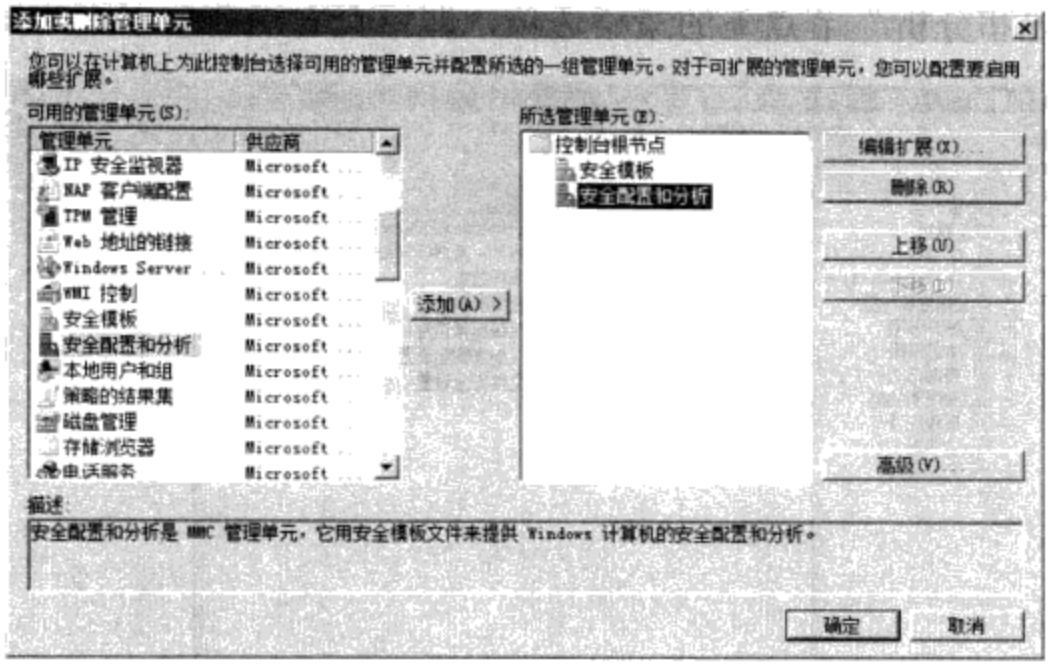


图 2-31 “添加或删除管理单元”对话框

第 2 步，单击“确定”按钮，将选定管理单元添加到控制台窗口中。右击“安全配置和分析”选择快捷菜单中的“打开数据库”命令，显示如图 2-32 所示“打开数据库”对话框，浏览到“C:\Windows\security\database”目录下，其中“secedit.sdb”是默认数据库，“secedit 副本.sdb”是后来创建的数据库副本，即安全配置和分析的对象。

图 2-32 “打开数据库”对话框

提示 如果不选择任何数据库文件，在“文件名”文本框中键入新的数据库文件名，单击“打开”按钮，即可创建新的数据库。默认情况下，新建数据库的所有策略选项都是未配置的。

第 3 步，选择“secedit 副本.sdb”数据库并单击“打开”按钮，显示如图 2-33 所示窗口。

依次展开“安全配置和分析”节点下的策略选项，即可查看当前数据库的安全配置状态。

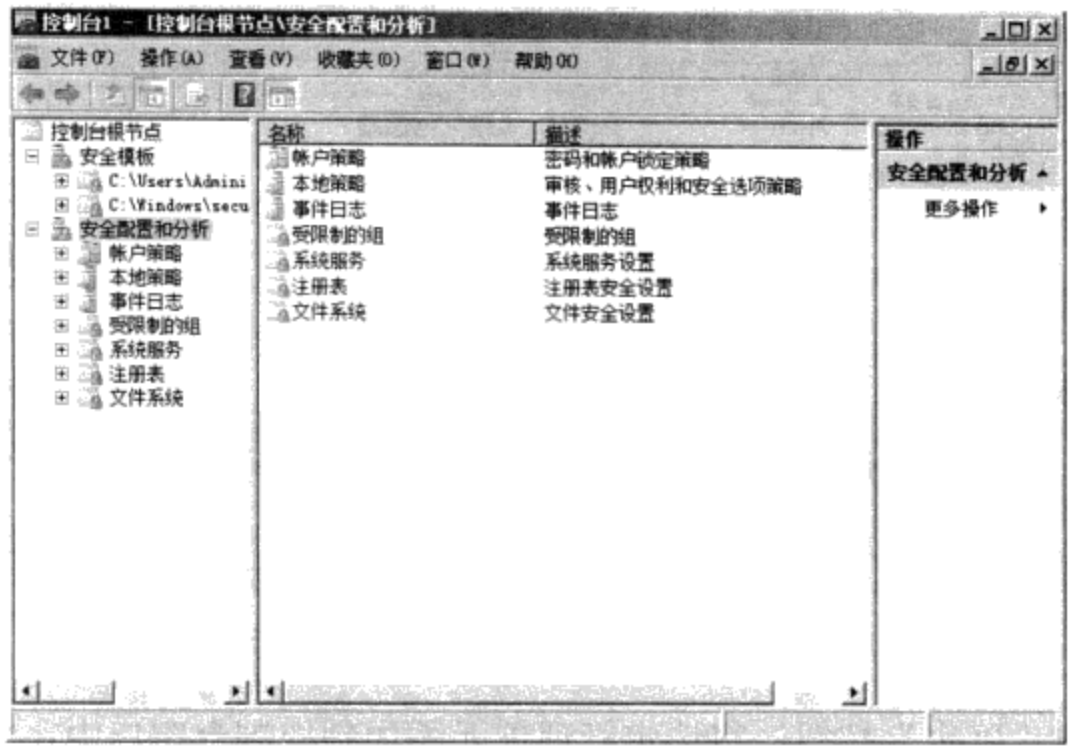


图 2-33 查看的开的数据库

第 4 步，右击“安全配置和分析”并选择快捷菜单中的“导入模板”命令，显示如图 2-34 所示“导入模板”对话框，选择定制好的新建安全模板即可。

第 5 步，单击“打开”按钮，返回控制台窗口。右击“安全配置和分析”并选择快捷菜单中的“立即分析计算机”命令，显示如图 2-35 所示“进行分析”对话框，选择用于保存错误日志的文件路径，系统默认为当前登录用户账户的配置文件夹。

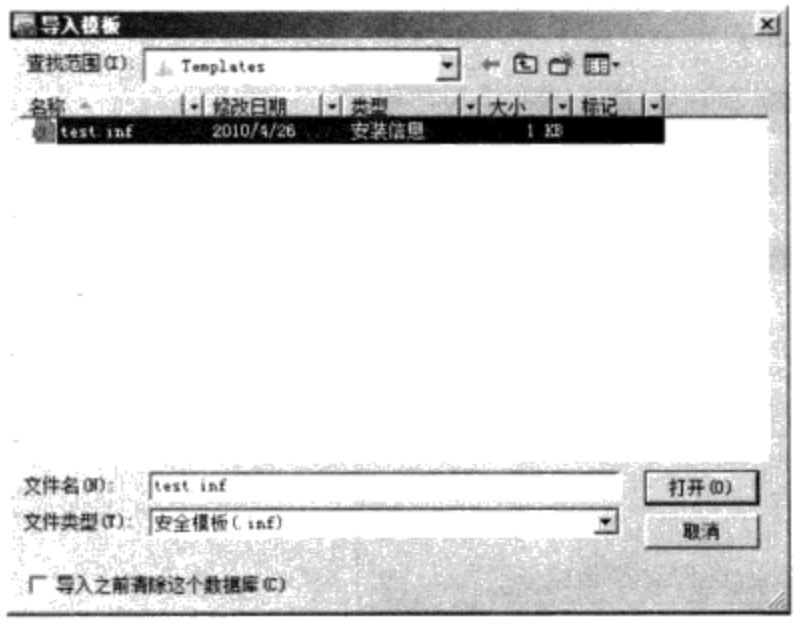


图 2-34 “导入模板”对话框

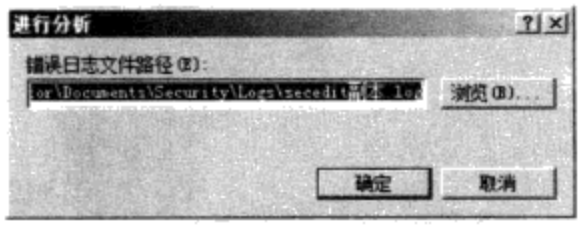


图 2-35 “进行分析”对话框

第 6 步，单击“确定”按钮，即可对选定数据库进行安全分析，依据选定策略模板的配置不同，执行分析所需的时间也会有所不同。如图 2-36 所示是分析结果，选定部分为安全模板中配置过的策略选项。

第 7 步，继续展开安全数据库，即可直观的查看分析结果。如图 2-37 所示是数据库中“密码策略”与安全模板中的“密码策略”对比结果。

第 8 步，右击“安全配置和分析”选择快捷菜单中的“立即配置计算机”命令，显示如图 2-38 所示“配置系统”对话框，设置保存错误日志文件的路径。

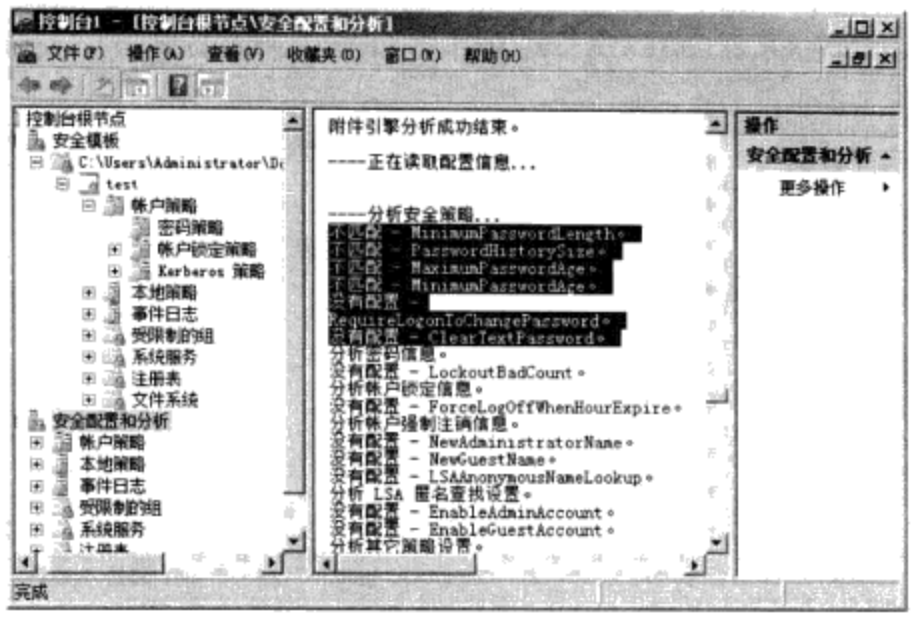


图 2-36　安全分析结果

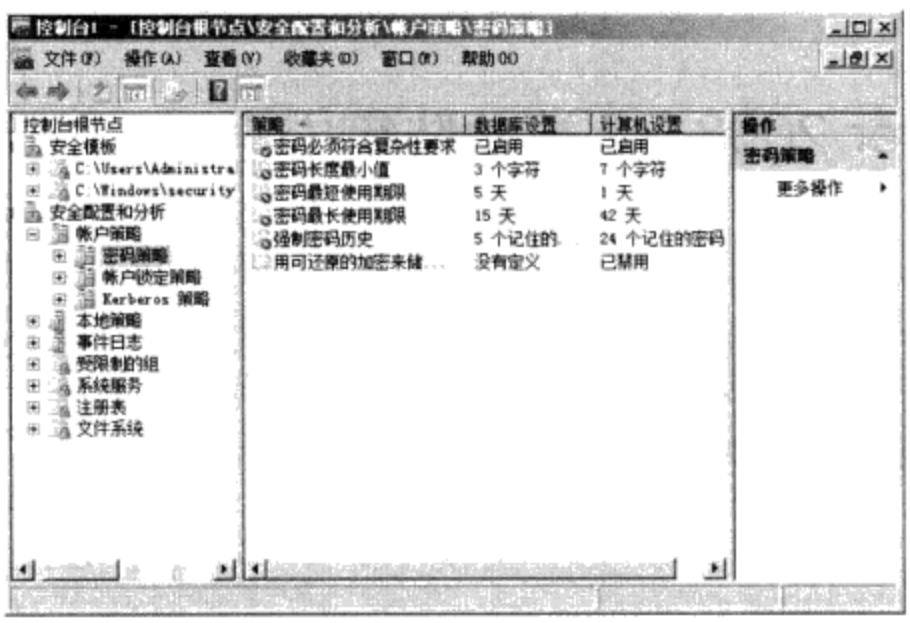


图 2-37　查看详细分析结果

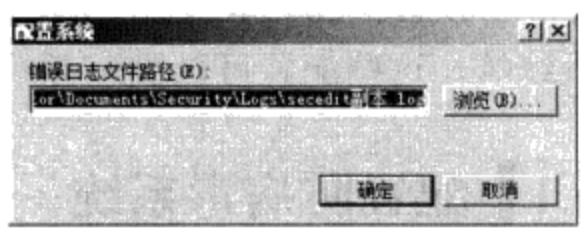


图 2-38　“配置系统”对话框

第 9 步，单击“确定”按钮，开始按照选定安全模板配置系统数据库，花费的时间比分析数据库要更长一些，完成后显示如图 2-39 所示配置结果。

图 2-39　配置结果

第 10 步，配置完成后，默认将自动关闭打开的数据库。可以重新打开数据库查看详细配置结果，如图 2-40 所示。数据库中的对应策略已经按照选定安全模板进行了重新配置。

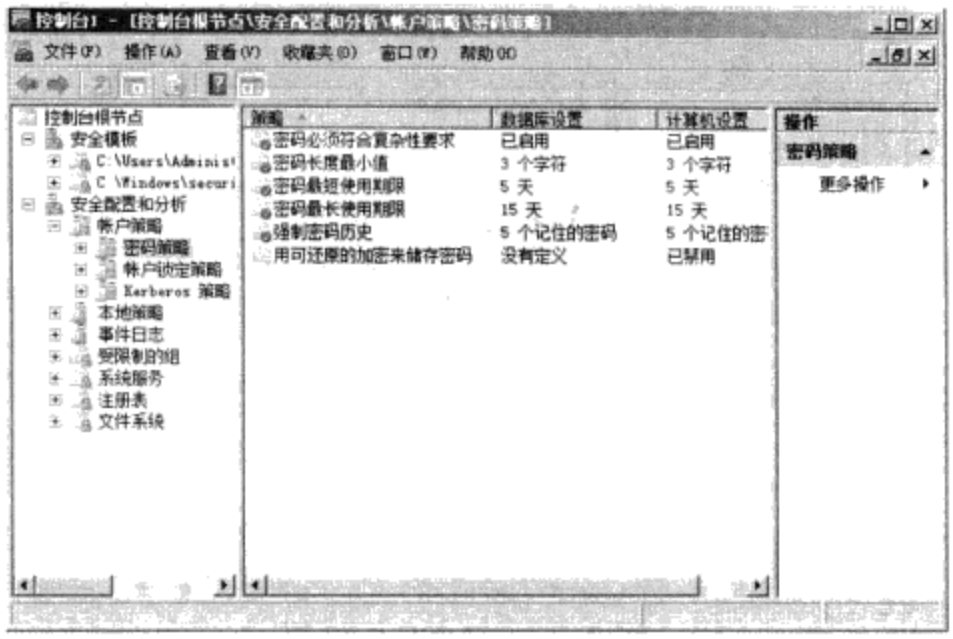


图 2-40 详细配置结果

2.3 Windows Server 2008 R2 被动防御安全

Windows 防火墙和安全配置向导都是主动防御系统，即主动阻止和过滤网络访问请求，但对于已经成功入侵到系统内部的病毒或恶意软件将起不到任何安全防御作用。因此，必须为 Windows Server 2008 R2 配置被动防御安全系统，如部署防病毒软件、设置 Windows 防间谍软件系统等，这些配置可以快速有效地处理进入系统的病毒或间谍软件。

2.3.1 配置防病毒系统

病毒对于计算机的危害性是不言而喻的，轻则造成应用程序出错、数据丢失，重则导致系统瘫痪、甚至波及到网络中的其他计算机。为了避免病毒对系统的破坏，应注意如下事项：

- 服务器投入应用之前必须安装防病毒软件，并升级最新的病毒库。
- 确认防病毒软件来源的合法性、完整性，以及可升级性。
- 应用过程中，应确保防病毒系统处于开启状态。
- 刚安装完成的操作系统，应进行一次完整的病毒扫描。
- 查看防病毒产生的日志文件。在系统运营后，经常查看病毒软件产生的日志文件。

1. 什么是计算机病毒

计算机病毒，是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码。病毒并非总是破坏文件或计算机，但它们通常会影响计算机的性能和稳定性。

计算机病毒通常具有如下特性：

- 传染性。
- 隐蔽性。
- 潜伏性。
- 破坏性。

- 表现性。

2. 单机防病毒系统

单机防病毒系统主要是指单个用户计算机上安装的病毒查杀软件，不必接受指定服务器的管理，通常都是通过 Internet 连接到官方服务器下载最新病毒库。单机防病毒系统成本相对较低，实现简单，易于管理，适用于小型企业局域网或 SOHO 网络。目前，针对单机用户的防病毒软件很多，建议用户通过正规渠道购买正版软件，或者登录相关软件的官方网站，下载试用版或共享版。

■ 瑞星

瑞星杀毒软件是国内反病毒软件中众多电脑生产商首选的杀毒软件，它集病毒防范、病毒扫描、查杀于一身，具有扫描速度快、识别率高、占用资源少等优点。瑞星杀毒软件不仅可以保护计算机系统不受病毒入侵，而且发现感染病毒后，还可以进行自动清除。瑞星杀毒软件可以运行于 Windows Server 2008 R2 或 Windows Server 2003 等服务器平台。

■ NOD32

NOD32 是 eset 公司的防病毒产品，以应用平台广泛著称，支持平台包括 DOS、Windows 9x/NT/2000/XP/2003/Vista/2008，到 Novell Netware Server、Linux、BSD 等。对于 Windows 版本，它同时支持 32 位和 64 位平台。NOD32 在线监测功能严密，占用内存资源较少，清除病毒的速度效果都令人满意。

■ Norton AntiVirus

诺顿杀毒软件由 Symantec 公司出品的一款杀毒软件，包括网络版和专业版，其中单机防病毒既可以使用网络版的客户端程序，又可以使用专业版。它可以为计算机提供全面的病毒防护，自动对计算机磁盘中的文件及 Internet 电子邮件进行监测、扫描，及时查杀病毒，以保证计算机的安全。今年的诺顿误杀系统文件事件，似乎并没有影响人们的热情，至今仍是众多用户的首选防病毒产品。

■ 趋势科技网络安全专家

趋势科技作为网络安全软件及服务领域的老牌厂商，以卓越前瞻和技术研发能力在业界推动了从桌面防毒到网络服务器和网关防毒的潮流。

趋势科技 Deep Security 产品可为物理、虚拟与云端服务器提供先进的安全防护，从而满足现今动态数据中心严格的运行安全要求。Deep Security 结合了入侵检测及预防、防火墙、一致性监控、记录文件检查以及无代理程序的恶意软件防护。用户只要使用具备集中管理的软件就能保护动态数据中心的安全。此外，Deep Security 是业界第一个也是唯一无代理程序的 VMware 环境防毒解决方案，可显著提高服务器整合率、效能及管理性。

■ Windows Live OneCare

Windows Live OneCare 微软公司推出的首款杀毒软件套件，包括反病毒防火墙、数据备份、反间谍、磁盘清理等功能，几乎可以覆盖所有的个人安全领域。随着时间的推移，相信会更加适合于 Windows 服务器。Windows Live OneCare 这项全面的服务可以帮助您保护计算机免受许多不同种类的威胁，还可以帮助用户在紧急情况下备份重要文档，并定期调整计算机从而帮

助计算机稳定运行。

3. 网络防病毒系统

网络防病毒系统主要应用于大、中型企业网络的病毒防御工作，相对于单机防病毒软件而言，不仅防御范围广、功能强大，而且可管理性强。目前，广泛应用的企业杀毒软件有Symantec AntiVirus 企业版、瑞星杀毒软件企业版、McAfee 网络防病毒等。网络防病毒系统主要由服务器和客户端两部分组成。主要特点就是客户端可以直接通过局域网从服务器获得最新的病毒库升级文件，并且管理员可以通过防病服务器客户端监控功能，及时了解客户端的运行情况，以便统一管理和部署。因此，部署企业杀毒软件系统不仅可以节省整个网络的带宽开销，还可以提高网络安全性。如图 2-41 所示是大多数企业杀毒软件的运行模式。

提示　有关网络防病毒系统部署的详细介绍，请参考本书“第 14 章 Windows 防病毒服务”中的相关内容。

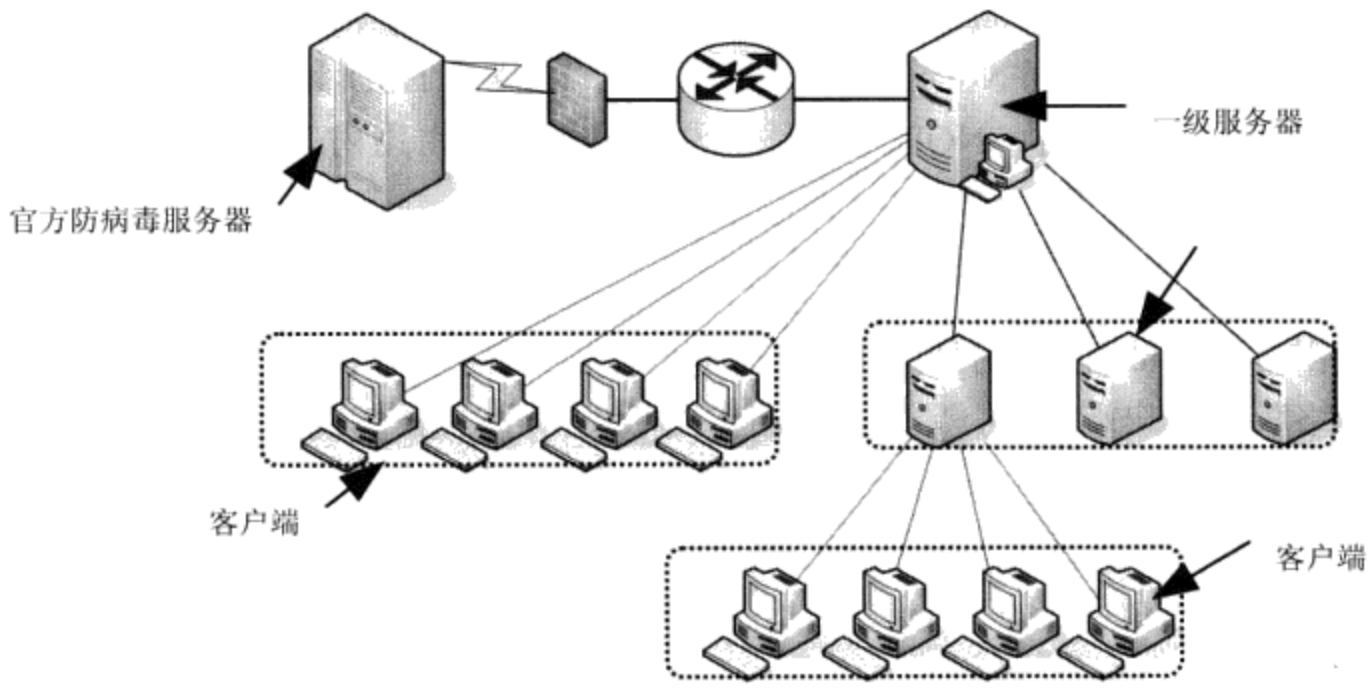


图 2-41　网络防病毒系统

■ 服务器端

企业杀毒软件系统中的服务器端是指安装服务器管理软件的计算机，可以直接登录杀毒软件官方升级服务器，快速下载最新病毒库文件。管理员可以通过服务器端对下属的二级服务器、客户端等进行统一管理，如分发升级文件、接收客户端病毒报警、实时状态监控等。另外，服务器端通常都集成适用于各种版本操作系统的客户端安装程序，管理员可以直接通过局域网安装客户端，免去一一安装的麻烦。

■ 客户端

客户端是指接受网络防病毒服务器管理的所有计算机，必须安装与服务器端配套的杀毒软件，并接受服务器的管理。客户端即可手动连接到局域网防病毒服务器，更新病毒库，也可以指定为自动接收来自服务器的病毒库文件。

2.3.2 配置防间谍系统

间谍软件与病毒程序最大的区别就是它不会产生直接的破坏性，而是偷偷的非法安装和运行，并从后台窃取当前计算机或网络中的某类信息，如管理员账户信息、企业信息、网络数据等。看似不会威胁服务器或网络的安全运行，实际上已经为企业长远发展埋下了隐患。Windows Defender 可以检测和清除 Windows 系统中的间谍软件和广告软件，以及其他具潜在危险性的软件，使 Windows 用户免受此类软件的威胁。

1. 防间谍软件系统概述

间谍软件通常是指自动安装，或者未提供足够通知、同意或控制的情况下，就在计算机上运行的应用程序。一般情况下，间谍软件在感染计算机后可能不会显示任何症状，但许多类型的恶意软件或不需要的程序都可以影响计算机的运行方式，如监视用户的实时行为、收集用户信息等。目前的防间谍软件产品很多，根据实际情况选择一款适合自己使用的防间谍软件产品，同时注意软件来源的合法性和安全性，以及间谍软件代码更新库的升级能力。

在安装防间谍软件时应注意如下事项：

- 建议配置成系统启动时自动启动防间谍软件。
- 定制自动更新间谍软件代码库。
- 定制在指定时间之内扫描系统的完整信息。
- 启动实施监视系统。
- 定制应用程序许可策略。
- 保存并定期察看日志信息。

为了应对网络中泛滥的木马、间谍等恶意软件对系统安全的挑战，微软也推出了反木马、间谍软件的专用程序 Windows Defender。Windows Defender 的前身是 Giant 公司的 Giant Antispyware，微软将该公司收购后便将其更名为 Windows Defender，并且已经成为 Windows Vista 系统的标准系统组件之一。

Windows Defender 具有如下主要功能：

- 提供完备的恶意软件清除功能。Windows Defender 在扫描查杀的同时，还会对恶意软件添加的文件以及修改的注册表内容进行同步检测和删除，清除比较干净。
- 与杀毒软件相得益彰。Windows Defender 是设计用来检测、删除或隔离用户电脑中的已知或可疑间谍软件的安全防御工具，针对的是杀毒工具无法处理的恶意软件，所以并不会和系统中安装的防病毒软件冲突，相反两者配合工作，安全防御效果会更好。
- 提供多种灵活扫描方式。Windows Defender 提供如下 3 种扫描方式，用户可根据实际需要选择。
  - Quick Scan：它可以扫描间谍软件常用的安装目录，可以在最短的时间里发现大多数间谍软件。
  - Full Scan：它可以扫描电脑中的全部硬盘分区以及全部文件夹。这种扫描方式非常彻底，但是耗时较多，具体的耗时根据用户的硬盘大小以及文件多少来决定。另外，扫描过程中，系统的整体运行速度会有所下降。

- Custom scan：在这种方式下，用户可以选择所要扫描的硬盘分区和文件夹。如果 Windows Defender 在这种模式下发现了间谍软件，将进而启动 Quick Scan 模式对间谍软件进行清除或隔离。

- 实时监控功能。Windows Defender 最大的特点在于当恶意软件试图入侵计算机时，会自动提醒用户。需要注意的是，只有当恶意软件是与其他软件捆绑安装时，Windows Defender 才会警报提醒，而当直接安装恶意软件时，则不会表现任何动作。
- 管理员可以监控用户行为。管理员可以允许用户使用 Windows Defender 扫描电脑，在发现可疑程序后选择相应的执行动作，以及查看 Windows Defender 的活动纪录。管理员还可以限制 Windows Defender 的管理权限。在默认情况下，任何用户都可以使用 Windows Defender。

2. 更新 Windows Defender 定义库

使用 Windows Defender 时，保持其定义库处于最新状态是非常重要的。定义是一些文件，其中包含了已知间谍软件和其他可能不需要的软件特称代码，类似于防病毒程序的病毒库。由于间谍软件在不断发展，Windows Defender 依靠更新定义来确定正尝试在计算机上安装、运行或更改设置的软件是否为可能不需要的或恶意软件。

在配置 Windows Defender 自动扫描时，如果选中“扫描前检查更新的定义”复选框，即可将其配置为自动更新定义。除此之外，用户还可以通过手动方式更新 Windows Defender 定义库。在“Windows Defender”窗口中，单击“帮助”按钮旁边的箭头，并选择“检查更新”即可。为确保计算机安全，Windows Defender 会在定义文件过期超过七天未更新时通知用户，此时直接单击“立即检查更新”按钮即可，如图 2-42 所示。

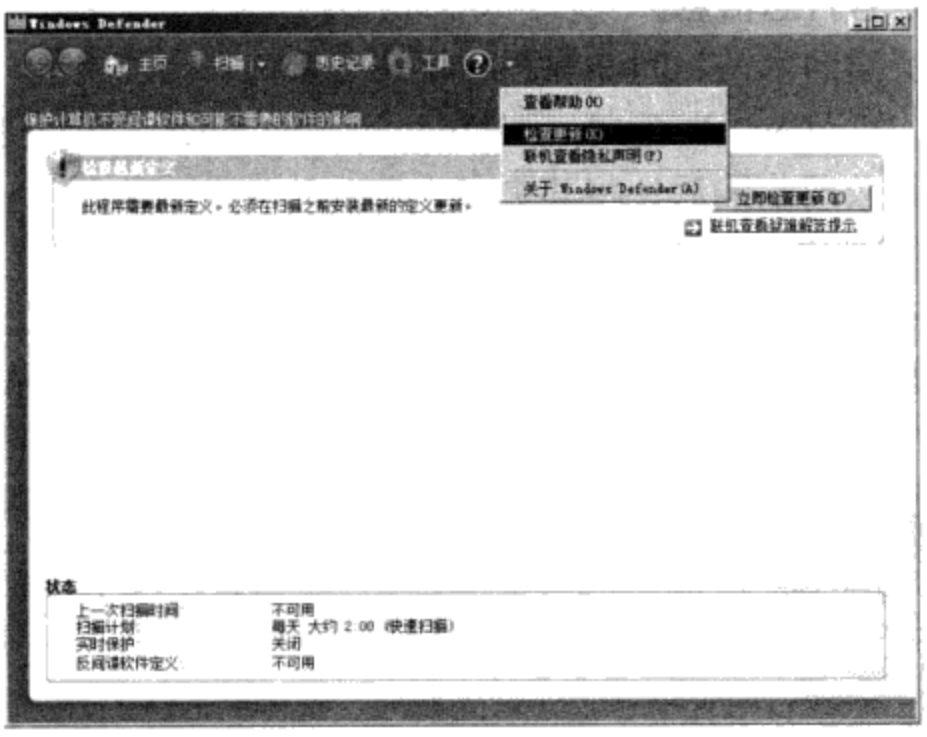


图 2-42 更新 Windows Defender

3. 执行系统扫描

在“Windows Defender”窗口中，单击“扫描”按钮默认将立即开始以“快速扫描”方式扫描本地计算机，如图 2-43 所示，扫描对象包括恶意软件、病毒程序、系统安全设置等。扫描方式包括快速扫描和完全扫描。快速扫描检查的是计算机上最有可能感染间谍软件的硬盘。

完整扫描检查硬盘上所有文件和当前运行的所有程序，但会引起计算机运行缓慢，直到扫描完成为止。

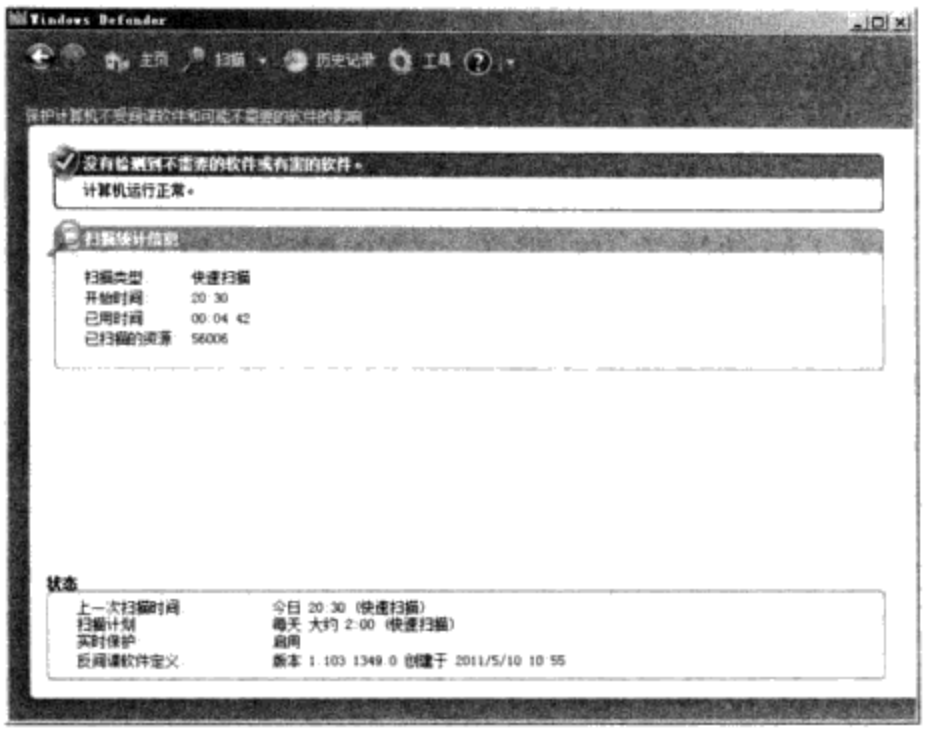


图 2-43　正在扫描计算机

如果发现计算机运行异常，怀疑可能被病毒或恶意软件感染，则可以通过“自定义扫描”方式只对可疑项目进行扫描。单击“扫描”按钮旁边的“向下箭头”，然后单击“自定义扫描”，打开如图 2-44 所示“选择扫描选项”对话框，选中“扫描选定的驱动器和文件夹”单选按钮。单击“选择”按钮，选择本地计算机上需要扫描的驱动器和文件夹，单击“确定”按钮关闭该对话框。然后单击“立即扫描”按钮，即可开始扫描。

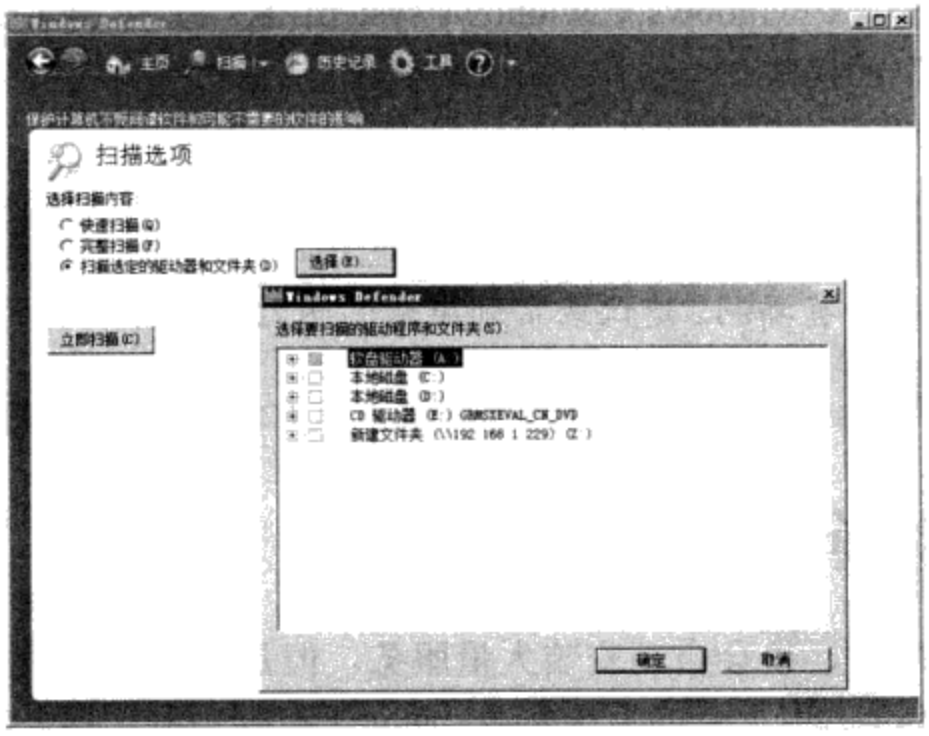


图 2-44　“选择扫描选项”对话框

2.4　Windows Server 2008 R2 系统安全

Windows Server 2008 R2 系统提供的系统安全涉及诸多方面，如应用程序安全、注册表安全、系统服务安全、文件权限安全、用户账户安全、活动目录安全、注册表安全、组策略安全、

端口安全、网络服务安全等等。任何一处隐藏的系统安全漏洞，都可能会招致整个系统安全的灭顶之灾。

2.4.1 应用程序安全

在服务器上安装正常使用的应用程序（包括更新的 IE 浏览器版本），同时安装配置选择好用来提供网络服务的程序（如微软的 IIS 服务、FTP 服务、SQL Server 数据库服务等）。非必要运行服务器操作系统的计算机不要登录到 Internet。

在配置系统应用程序时，应注意以下事项：

- 不要安装任何多余的程序。服务器仅提供网络服务，不是个人电脑，不需要安装任何服务以外的程序。
- 安装服务和应用程序，尽量选择最新的安装版本，这样，通常可以保证没有近期发布的程序漏洞。不需要的应用程序服务尽量不要安装，或者配置成禁止使用的模式。
- 通常不要在服务上运行系统提供的应用程序访问网络，服务器的漏洞有时会被恶意利用。
- 为安全起见，建议将系统“附件”中除写字板、记事本以外的所有应用程序卸载。
- 操作系统所在的服务器建议不要接入 Internet。
- 强烈建议删除甚至拒绝在服务器上安装 Microsoft Office 或者其他的日常办公软件。
- 不要在服务器上运行任何开发工具、软件调试器、扇区读写编辑器等可对操作系统底层进行操作的应用软件，可执行程序越少越好。
- 服务器设置严格的权限许可，共享文件的访问建议使用 ACL 权限控制。
- 对系统文件夹（x:\windows,x:\widnows\system 等）使用 ACL 控制，避免赋予系统文件夹“写入”的权限。
- 服务器的 IP 地址设置为静态 IP。

注意 了解要安装的程序是否存在缺陷，如 IE、Outlook、Media Player 等微软提供的程序可能含有漏洞。建议经常到微软的网站上查看最新的安全公告，或者接受微软的安全邮件列表。

2.4.2 系统服务安全

安装操作系统的同时，也会自动安装大量服务。但是，运行的服务越多，可能造成的安全漏洞也越多，同时还会占用大量的系统资源。而对于有能力利用服务特权和功能来访问本地 Web 服务器或其他网络服务器的不法入侵者来说，服务是最主要的漏洞点。不验证客户端身份的服务、使用不安全协议的服务、特权太多的服务等都将带来风险。服务越少、漏洞越少、系统越安全。

1. 服务账户

服务仅在登录到某一账户的情况下才能访问操作系统中的资源和对象。大多数的服务都

不更改默认的登录账户，更改默认账户可能导致服务失败。如果选定账户没有登录计算机服务的权限，Microsoft 管理控制台（MMC）的服务管理单元将自动为该账户授予登录服务的用户权限，但并不一定会启动服务。

（1） 本地系统账户

本地系统账户功能强大，它可对本地系统进行完全访问，并为网络中的计算机提供服务。如果某服务登录到域控制器使用的“本地系统”账户，则该服务可访问整个域。有些服务的默认配置使用的是“本地系统”账户，则不需要更改默认服务设置。本地系统账户名称是 LocalSystem，没有密码设置。

（2） 本地服务账户

本地服务账户是一种特殊的内置账户，类似于经过身份验证的用户账户。就访问的资源的对象而言，“本地服务”账户与“Users”（用户）组成员权限等同。这种限制性访问有助于在个别服务或进程受损时保障系统安全，以“本地服务”账户运行的服务使用有匿名凭据的空会话来访问网络资源。账户名称为 NTAUTHORITY\LocalService，该账户没有密码。

（3） 网络服务账户

网络服务账户也是一种特殊的内置账户，类似于经身份验证的用户账户。就访问的资源的对象而言，“网络服务”账户与“Users”（用户）组成员权限等同。这种限制性访问有助于在个别服务或进程受损时保障系统安全，以“网络服务”账户运行的服务可使用计算机账户的凭据来访问网络资源。账户名称为 NTAUTHORITY\NetworkService，该账户没有密码。

注意 如果更改默认服务设置，重要的服务可能无法正常运行。最重要的是，更改启动类型一定要谨慎，要使用配置了自动启动服务的设置来登录。

2. 服务权限

每个服务都有特定的权限，管理员可以将这些权限授予每一个用户或组，也可以从用户或组的权限中取消相应的服务权限。服务具有的权限及描述如表 2-1 所示。

表 2-1 服务权限

权　限	描　述
完全控制	执行所有功能。默认情况下，服务会自动授予登录用户完全控制权限
查询模板	确定与某个服务对象关联的配置参数
更改模板	更改服务的配置，如更改启动类型
状态查询	有关服务状态的访问信息
列举依存关系	确定依存于指定服务的所有其他服务
启动	启动服务
停止	停止服务
暂停和继续	暂停或继续服务
询问	报告服务的当前状态信息
用户定义的控制	将用户定义的控制请求或特定于服务的请求发送给该服务
删除	删除服务
读取权限	读取指派给服务的安全权限
更改权限	更改指派给服务的安全权限
取得所有权	更改安全密钥，或更改关于不为用户所有的服务的权限

3. 关闭和启动服务

默认情况下，Windows Server 2008 R2 已经自动安装并启动了大部分服务，用于辅助完成各项功能。需要注意的是，每项系统服务运行时需要开启不同的端口，而开启的端口越多，系统安全性就越差。因此，从系统安全角度而言，应关闭平时不需要的系统服务。以关闭 DHCP Client 服务为例，介绍如何关闭和启动服务。

第 1 步，依次选择“开始”→“管理工具”→“服务”选项，显示如图 2-45 所示“服务”控制台窗口。或者在“服务器管理器”窗口中，依次展开“配置”→“服务”选项，也可以打开“服务”窗口。

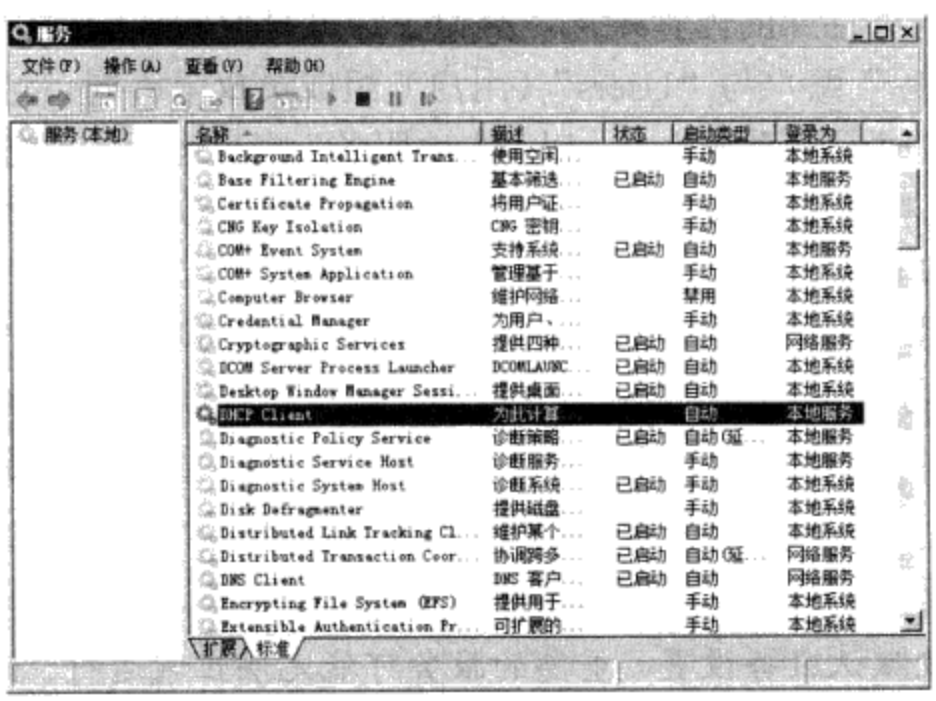


图 2-45　“服务”窗口

第 2 步，在右侧窗口中，双击“DHCP Client”服务，显示如图 2-46 所示“DHCP Client 的属性”对话框。目前该服务的状态是“已停止”。

第 3 步，单击“启动”按钮，即可启动该服务，如图 2-47 所示。此时，服务状态变为“已启动”，再次单击“停止”按钮，即可将其停止。

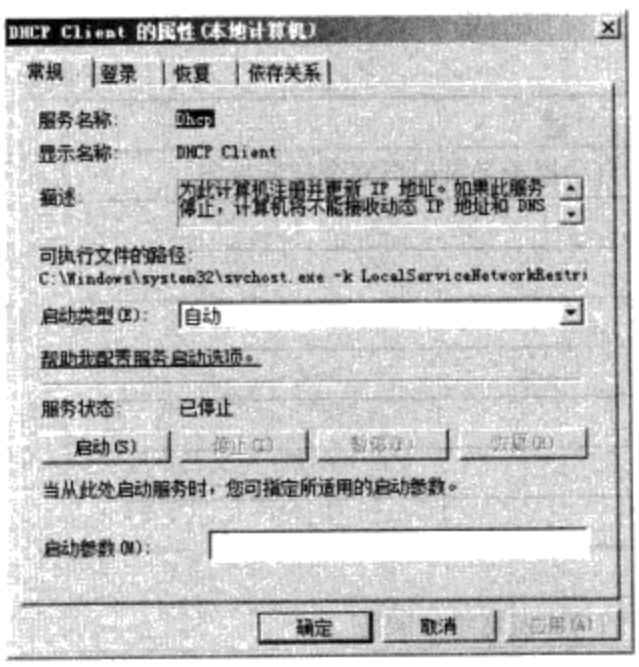


图 2-46　“DHCP Client 的属性”对话框

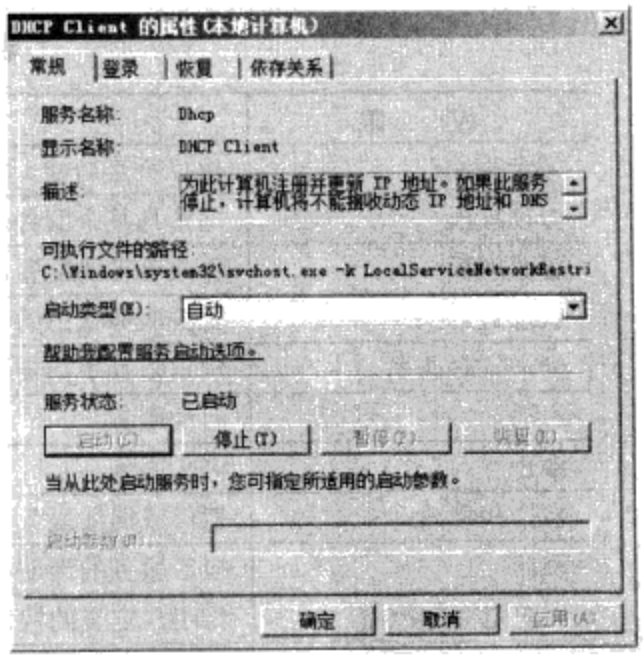


图 2-47　关闭服务

第 4 步，单击“确定”按钮，即可关闭 DHCP Client 服务对应的端口。

2.4.3 禁止注册表远程访问

注册表中包含了 Windows 系统运行时所需的信息，它作为 Windows 系统中重要的配置文件，对系统安全起着决定性的作用。Windows Server 2008 R2 在默认安装时启用了允许远程访问注册表。系统服务的启动、ACL 权限的修改、用户账户的创建，都可以在注册表中完成，因此开启此功能将会对系统安全带来极大的隐患，必须严格禁止使用远程注册表访问功能。该安全设置确定在网络上可访问哪些注册表路径和子路径。

第 1 步，打开组策略控制台，依次展开“计算机配置”→“Windows 设置”→“安全设置”→“本地策略”→“安全选项”，显示如图 2-48 所示窗口。

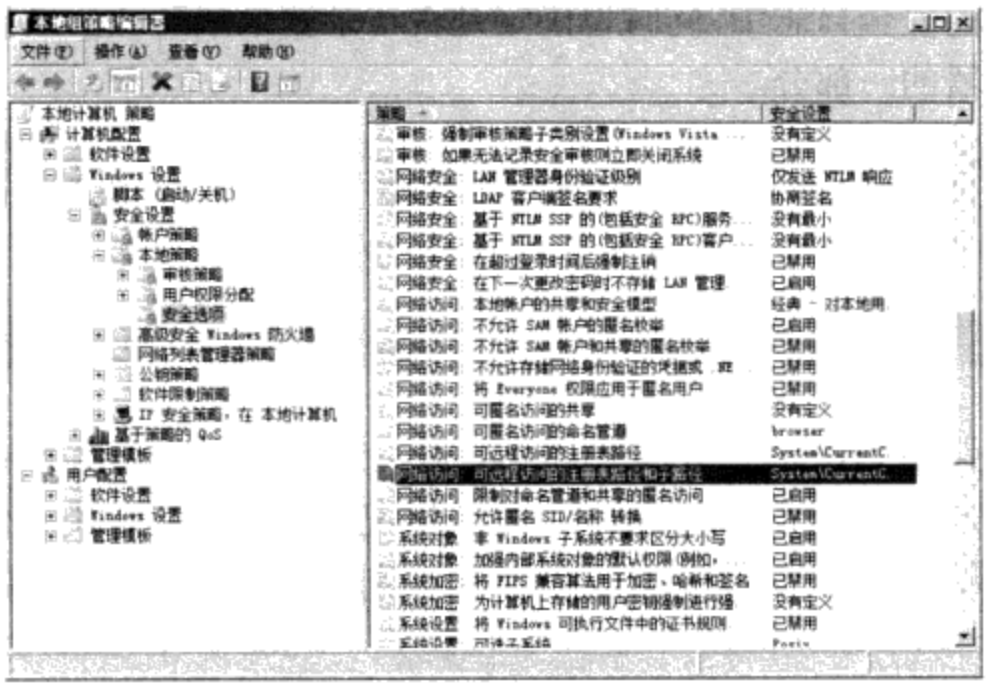


图 2-48 “本地组策略编辑器”窗口

第 2 步，在右侧的策略窗口中，双击“网络访问：可远程访问的注册表路径和子路径”策略，显示如图 2-49 所示“网络访问：可远程访问的注册表路径和子路径 属性”对话框。

第 3 步，删除列表框的所有数据，单击“确定”按钮保存设置。

第 4 步，双击“网络访问：可远程访问的注册表路径”策略，显示如图 2-50 所示“网络访问：可远程访问的注册表路径属性”对话框。

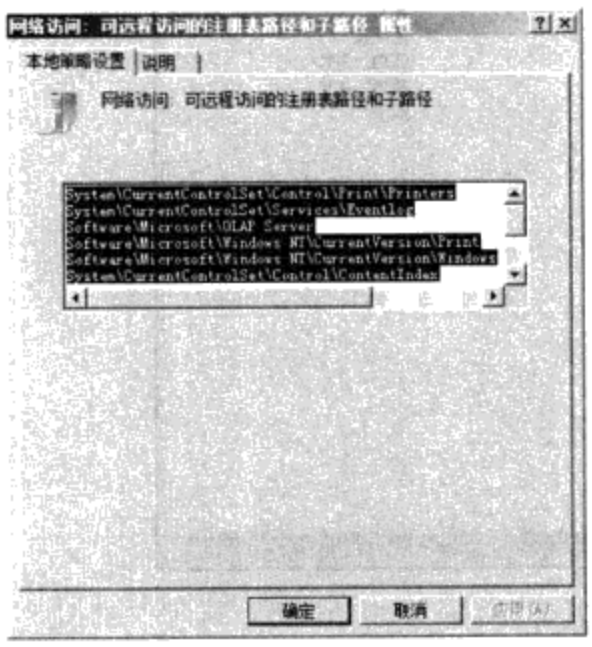


图 2-49 “网络访问：可远程访问的注册表路径和子路径 属性”对话框

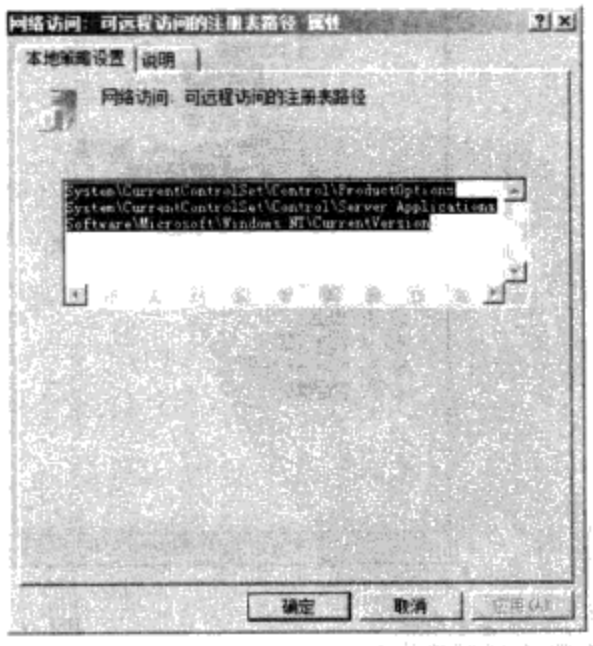


图 2-50 “网络访问：可远程访问的注册表路径属性”对话框

第5步，删除文本框的所有数据，然后单击“确定”按钮即可。

提示 编辑注册表不当可能会严重损坏的系统。在更改注册表之前，应备份计算机上任何有价值的数据。

2.4.4 审核策略

审核是Windows Server 2008 R2中本地安全策略的一部分，它是一个维护系统安全性的工具，允许跟踪用户以及系统的活动，这些活动称为事件。通过设置审核策略，确定是否将安全事件记录到计算机上的安全日志中，同时也确定是否记录登录成功或登录失败，或二者都记录。安全日志是事件查看器的一部分。

提示 要将某个审核策略的值设置为“无审核”，可在该策略设置的“属性”对话框中，选中“定义这些策略设置”复选框，然后清除“成功”和“失败”复选框即可。

执行审核策略前，必须决定要审核的事件类别。为事件类别选择的审核设置将定义审核策略。在加入域中的成员服务器和工作站上，默认情况下未定义事件类别的审核设置。在域控制器上，默认情况下审核关闭。通过为特定的事件类别定义审核设置，可以创建一个适合组织安全需要的审核策略。

依次打开“计算机配置”→“Windows 设置”→“安全设置”→“本地策略”→“审核策略”，显示如图2-51所示“审核策略”页面。

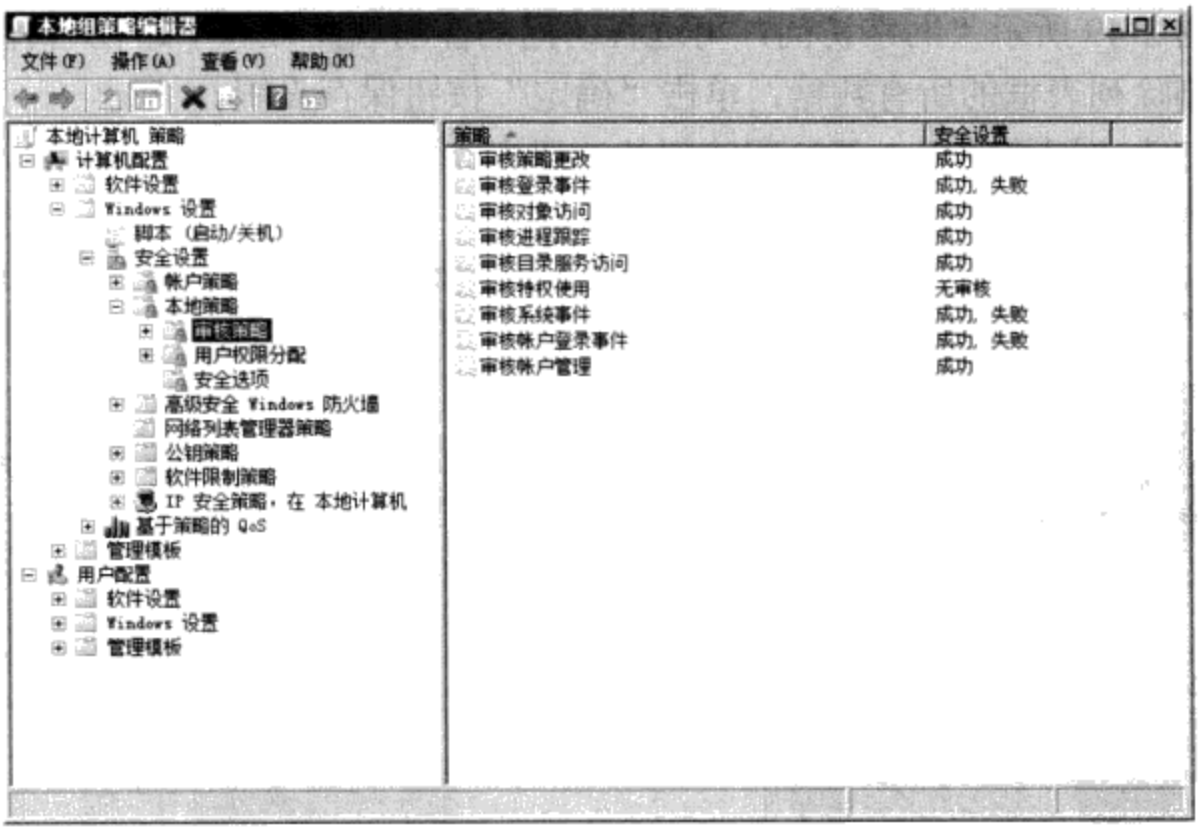


图2-51 “审核策略”窗口

2.5 Windows Server 2008 R2 系统漏洞安全

漏洞扫描是网络安全防御中的一项重要技术，其原理是采用模拟攻击的形式对目标可能存在安全漏洞进行逐项检查，其目标是工作站、服务器、数据库应用程序等。根据扫描结果向系统管理员提供周密可靠的安全性评估分析报告，从而为提高网络安全整体水平产生重要依据。MBSA 是 Microsoft 免费推出的系统漏洞扫描产品，支持类型涵盖了微软公司的大部分产品。

2.5.1 系统漏洞概述

硬件设备、应用程序、网络协议等都可能存在漏洞，攻击者借助这些漏洞，能够在未得到授权的情况下访问或破坏系统。客观地讲，系统漏洞是无法避免的，对于 Windows 操作系统而言，新版操作系统弥补旧版本中漏洞的同时，还会引入一些新的漏洞。应对系统漏洞最有效的方法就是指定详细的修补策略，及时发现并弥补漏洞。

1. 系统漏洞的特性

大多数用户都对系统漏洞的概念都有一定的了解，但这些了解只是局限于各大厂商的公布的漏洞，以及一些权威机构发布的漏洞公告。从信息安全的角度看，是先有漏洞和对漏洞的攻击的可能性，然后才会有补丁。漏洞是攻击者所要攻击的目标，而安装补丁是对漏洞的修补过程。漏洞是广泛存在的，不同的设备、操作系统、应用系统都会存在安全漏洞。

（1） 时间局限性

任何系统漏洞都是在用户的不断使用过程中被发现的，随之系统供应商采取新版本替代，或者发布补丁程序等方式弥补漏洞。但随着旧漏洞的消失，新环境下的新漏洞也将随时产生。因此，系统漏洞只是存在于特定时间和环境下的，即只能针对目标系统的系统版本、其上运行的软件版本，以及服务运行设置等实际环境。

（2） 隐蔽性

安全漏洞是最常见的系统漏洞类型之一。入侵者借助这些漏洞，可以绕过系统中的许多安全配置，从而实现入侵系统的目的。安全漏洞的出现，是因为在对安全协议的具体实现中发生了错误，是意外出现的非正常情况。而在实际的系统中，都会不同程度的存在各种潜在错误。因而所有系统中都存在安全漏洞，无论这些漏洞是否已被发现，也无论该系统的安全级别如何。在一定程度上，安全漏洞问题是独立于系统本身的理论安全级别而存在的。也就是说，并不是系统所属的安全级别越高，系统中所存在的漏洞就越少。

（3） 被发现性

漏洞是特定环境和时间内的必然产物，但必须发现后，才会被用来入侵系统或被弥补。在实际使用中，用户会发现系统中存在错误。入侵者会有意利用其中的某些错误，并使其成为威胁系统安全的工具，这时用户才会认识到这个错误是一个系统安全漏洞。系统供应商会尽快发布针对这个漏洞的补丁程序，纠正这个错误。这就是系统安全漏洞从被发现到被纠正的一般过程。

（4） 周期性

漏洞所造成的安全问题具备一定的时效性，也就是说每一个漏洞都存在一个和产品类似的生命周期的概念。只有对漏洞生命周期的概念进行研究并且分析出一定的规律，才能达到真正解决漏洞危害的目的。

2. 系统漏洞修补策略

大多数蠕虫病毒都是依靠系统漏洞进行传播的，同时网络扫描和利用系统漏洞也是“黑客”最常用的攻击手段之一。因此，做好网络的安全保障，必须做好漏洞补丁的安装管理工作。对于个人用户而言，系统漏洞修补无非就是安装官方网站发布的补丁而已，但是服务器或者网络中大规模部署补丁通常是一项非常重要的工作。安装之前，必须先在实验环境中进行测试和分析，然后才可以在网络中大规模部署。

（1） 环境分析

知己知彼，百战不殆。只有真正了解网络内部状况，才能有效的实施漏洞修补。例如，及时掌握网络资产情况、设备运行状态，包括网络中运行的设备型号、厂商、操作系统种类、版本等。同时还要了解企业的主要业务系统及重要的数据，根据需要划分安全等级，以确定补丁的紧急程度和修补时间。

（2） 补丁分析

用户计算机系统信息、硬件等变化，都可能导致无法正确安装官方发布的系统漏洞补丁，甚至安装后还会导致一系列的问题。因此，部署之前一定要针对用户系统环境进行测试，切不可盲目的安装补丁，否则将带来许多意想不到的问题，其中包括：

- 导致系统兼容性出现问题，甚至不能使用。
- 系统崩溃，无法正常工作。
- 部分功能无法使用。

在得到补丁以后，正确的做法应该是：

- 在测试环境中，测试对业务系统的影响，以及兼容性。
- 了解补丁自身的稳定性。
- 查看补丁是否还存在漏洞。
- 在大规模部署之前，进行小范围的短时间的联机测试。

在测试的过程中，应做好详细的测试记录，了解补丁程序和与其相关的组件对象之间的兼容性，对原有系统功能的影响，是否可以卸载，是否可以“回滚”等。

（3） 分发安装

对于网络用户而言，管理员可以通过组策略、SCCM、WSUS 等多种方法，将已获得的系统补丁分发到客户端。其中，WSUS 为微软公司提供的专用于补丁更新的服务组件，可以根据客户端实际情况，自动将补丁程序分发到用户或计算机，建议使用这种方法。

2.5.2 MBSA 的主要功能

MBSA（Microsoft Baseline Security Analyzer），此工具允许用户扫描一台或多台基于 Windows 系统的计算机，以及发现常见安全方面的配置错误，并检查操作系统和已安装的其他组件，及时通过推荐的安全更新进行修补。MBSA 的免费下载地址为：

http://www.microsoft.com/downloads/details.aspx?FamilyID=F32921AF-9DBE-4DCE-889E-ECF997EB18E9&displaylang=en。

MBSA 对在被扫描的计算机中 Windows 操作系统进行扫描，如表 2-2 所示列出了扫描过程中检测的项目。

表 2-2 MBSA 的扫描项目

检 测 项 目	描 述
Administrators 成员权限	确定并列出属于本地管理员组的用户账户。如果检测出的单个管理员账户数量超过两个，则该工具将列出这些账户名，并将该检查标记为一个潜在的安全漏洞
审核	确定在被扫描的计算机上是否启用了系统审核功能。Windows 系统的审核特性，可跟踪和记录系统上的特定事件，如成功的和失败的登录尝试。通过监视系统的事件日志，可以发现潜在的安全问题和恶意活动
自动登录	确定在被扫描的计算机上是否启用了“自动登录”功能，以及登录密码是在注册表中以密文方式存储。如果“自动登录”已启用而且密码以加密形式存储在注册表中，那么安全报表就会将这种情况作为一个潜在的安全漏洞标记出来。默认情况下，Windows Server 2008 禁止“自动登录”
自动更新	确定是否在被扫描的计算机上启用自动更新功能，以及详细的配置情况。当用户使用直接下载更新方式之外的其他方式时，扫描结果中可能会出现相关安全警告信息，提示自动更新没有正确配置，此时不必理会
域控制器	确定正在接受扫描的计算机是否为域控制器，这主要是针对 Windows Server 2003 和 Windows Server 2008 系统而言的。如果是域控制器，则同时检测是否采取了相应的操作来加强访问安全
文件系统	确定在每个分区使用的文件系统类型。NTFS 具有访问控制功能，是一个安全的文件系统，因此，服务器所有分区均使用该文件系统，如果使用 FAT32 文件系统，则扫描结果中将报警
guest 账户	确定在被扫描的计算机上是否启用了系统内置的 guest 账户。来宾账户主要视为临时用户提供的，默认情况下是禁用的。如果在 Windows NT/2000/XP/2003/Vista/2008 计算机上已启用来宾账户，则此时将在安全报表中作为一个安全漏洞标记出来
Windows 防火墙	确定是否在被扫描的计算机上对所有的活动网络连接启用 Windows 防火墙，这主要是针对 Windows XP/2003/2008 系统而言的。如果已经启用防火墙，则还将对其开放的入站端口进行检测。如果 Windows 防火墙没有开启，或者开放了存在安全漏洞的端口，则扫描结果中将出现警告信息
本地账户密码	确定被扫描计算机的本地用户账户密码是否为空或者简单密码。在 Windows Server 2008 系统中，必须设置符合相应复杂程度的安全密码，才允许启用管理员账户
密码过期	确定是否有本地用户账户设置了永不过期的密码。密码应该定期更改，以降低遭到密码攻击的可能性
限制匿名用户	确定被扫描的计算机上是否使用了 RestrictAnonymous 注册表项来限制匿名连接
共享资源	确定在被扫描的计算机上是否存在共享文件夹。扫描报告将列出在计算机上发现的所有共享内容，其中包括管理共享及其共享级别和 NTFS 级别的权限。扫描结果中将列出所有的系统默认共享，和用户后期设置的重要资源共享
检查是否存在不必要的服务	确定被扫描计算机上的 services.txt 文件的服务列表中，是否包含有已启用的非必要服务。services.txt 随 MBSA 的安装自动生成，并且是可配置的，默认情况下包括 MSFTPSVC（FTP）、TlntSvr（Telnet）、W3SVC（WWW）和 SMTPSVC（SMTP）。如果被扫描计算机上安装了列表中指定的服务，则扫描结果中将出现警告

2.5.3 使用 MBSA 扫描本地系统漏洞

第 1 步，依次选择“开始”→“所有程序”→“Microsoft Baseline Security Analyzer 2.1”，打开如图 2-52 所示 MBSA 主窗口。

第 2 步，单击“Scan a computer”链接，显示如图 2-53 所示“Which computer do you want to scan?”窗口。在“Computer name”文本框中，指定要扫描的计算机名，系统默认为本地计算机。用户可以根据需要，选择此次扫描的目标服务或应用程序，如 IIS、SQL、密码安全性等，这里只选择前两项扫描功能。

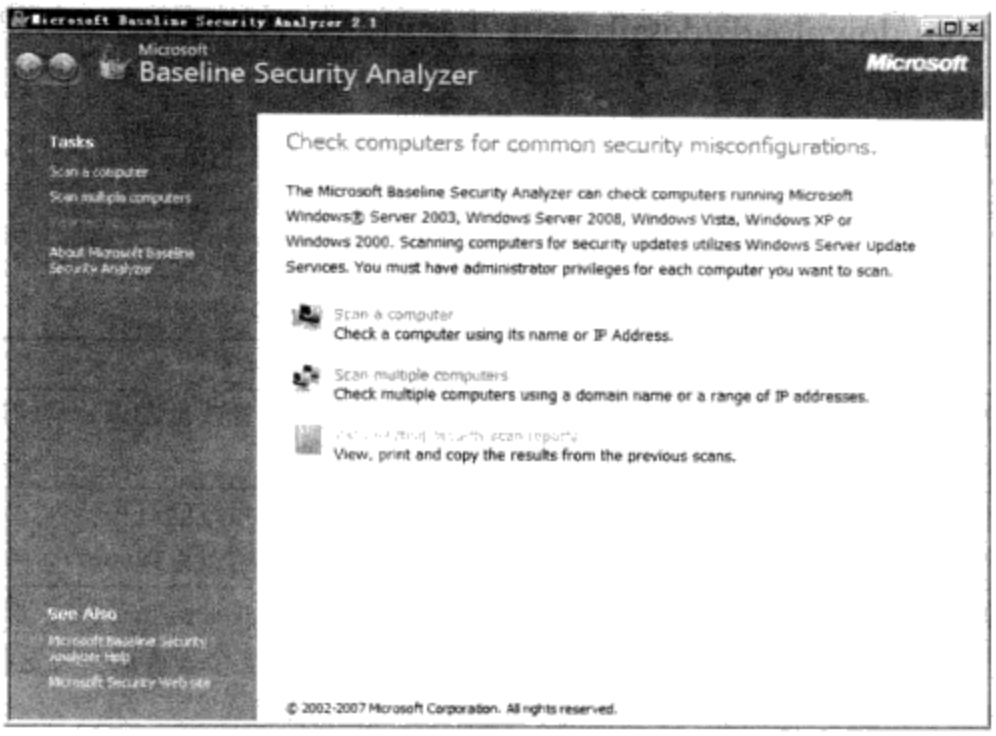


图 2-52　MBSA 主窗口

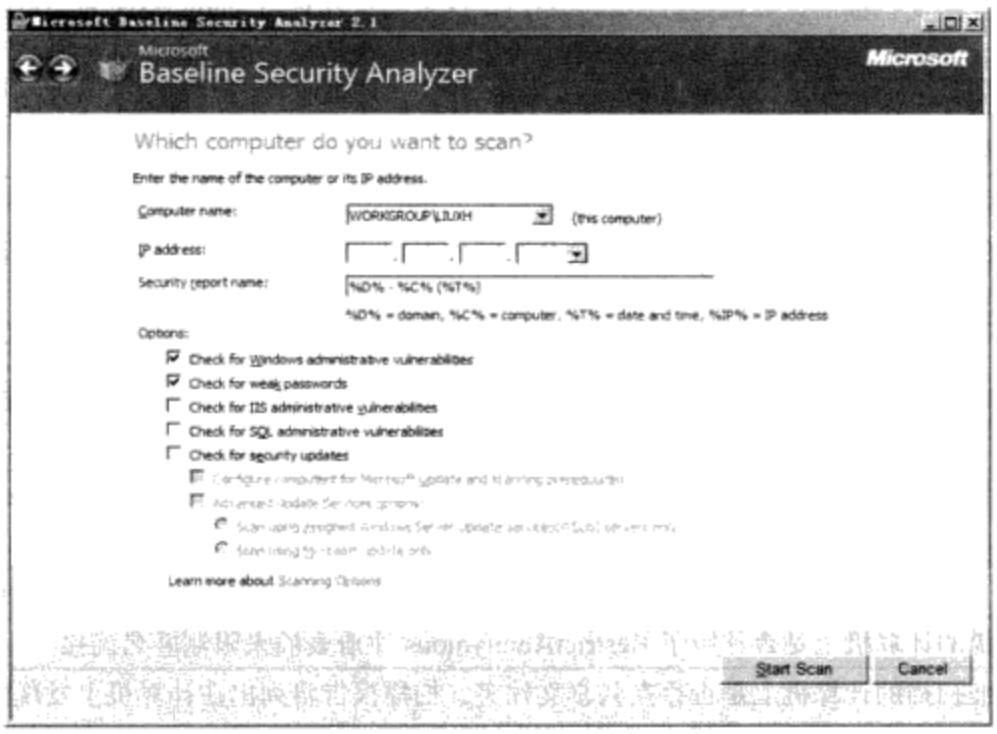


图 2-53　“Which computer do you want to scan?”窗口

提示

在“Security report name”文本框中显示的是系统默认的扫描结果名称格式，其中“%D%”表示域名称，“%C%”表示目标计算机名称，“(%T%)”表示扫描日期和时间，如果是基于 IP 地址的扫描任务，则还会出现%IP%，表示被扫描主机的 IP 地址。

第 3 步，根据需要选择需要检测的安全内容。然后窗口下方的“Start Scan（开始扫描）”按钮，系统开始进行扫描。完成后显示如图 2-54 所示扫描结果窗口。在“Potential Risk（潜在风险）”选项区域显示了被扫描主机的基本信息，包括主机名、IP 地址和扫描日期等；在“Windows Scan Results（Windows 扫描结果）”选项区域显示了扫描结果摘要信息。管理员，通过每项扫描结果前不同的图标，即可判断其安全状态。

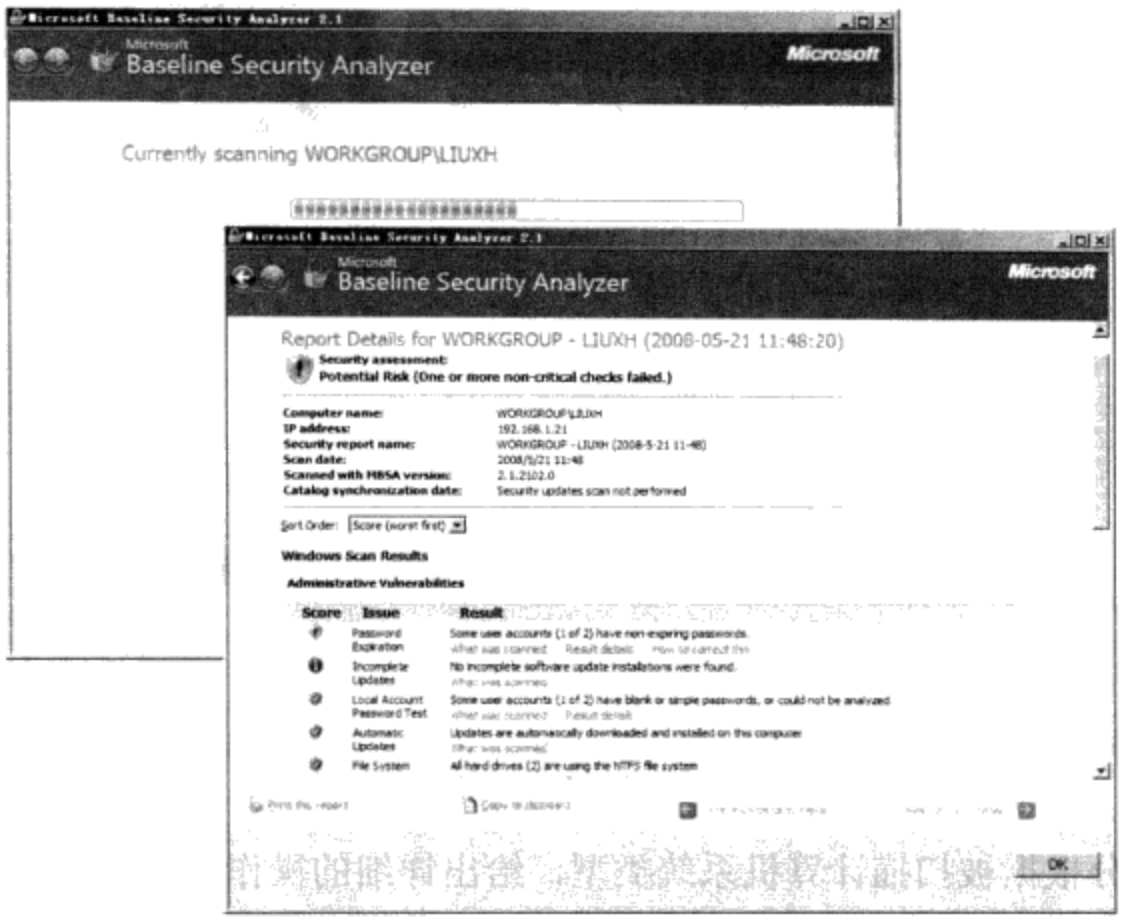


图 2-54　扫描结果

第 4 步，在“Issue（问题）”栏中列出了被扫描计算机存在的主要安全问题，这里以扫描结果中的“Password Expiration（密码过期）”问题为例。单击“What was scanned（扫描对象）”链接，打开如图 2-55 所示“Password Expiration”窗口，信息中提示该项检查将列出目标计算机系统中，所有密码过期或不符合要求的账户。

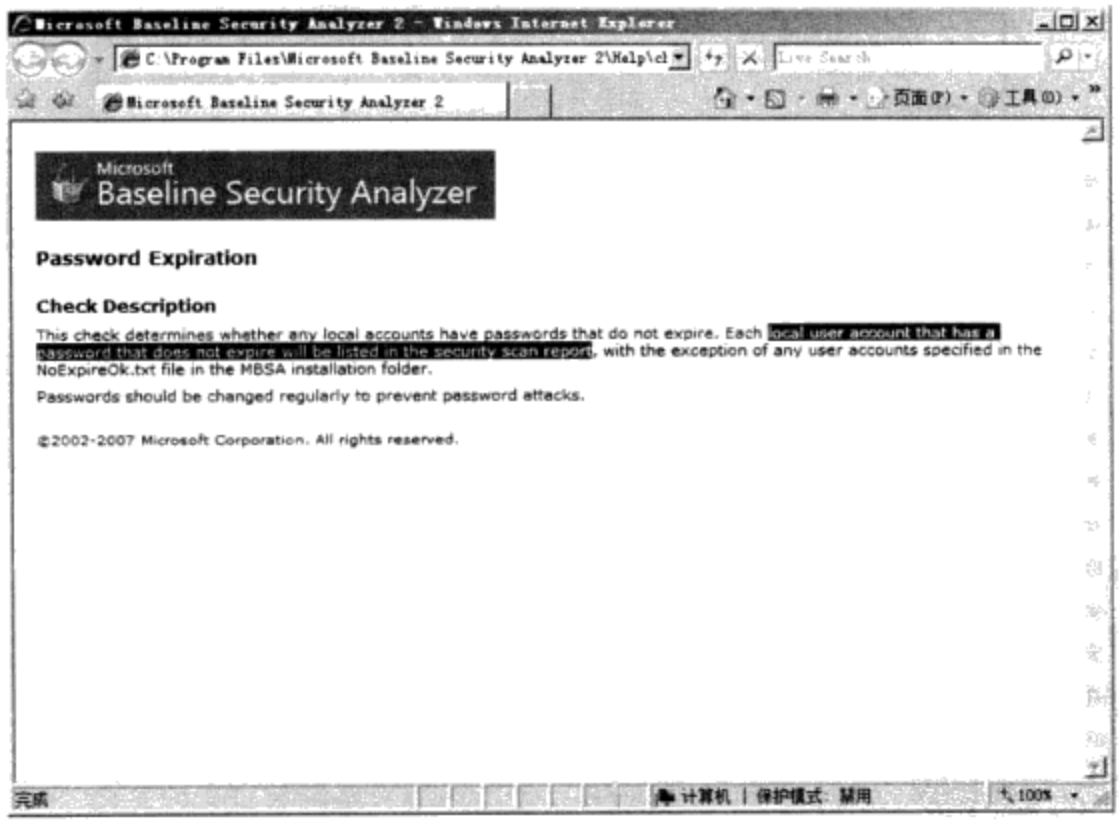


图 2-55　“Password Expiration”窗口

第 5 步，在扫描结果窗口中，单击“Result details（详细结果）”链接，打开如图 2-56 所示“Result Details”窗口，提示目标计算机的 Guest 账户密码已经过期。

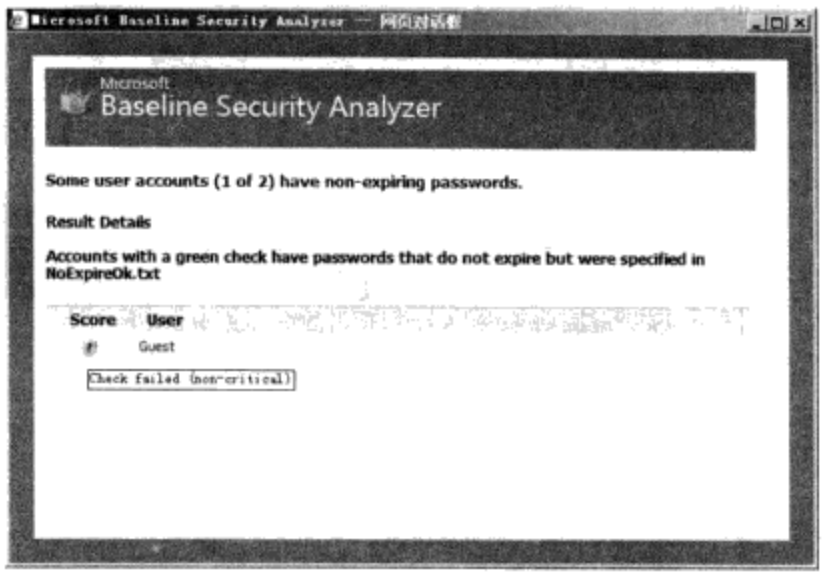


图 2-56 “Result Details”窗口

第 6 步，在扫描结果窗口中，单击“How to correct this（如何改正错误）”链接，打开如图 2-57 所示窗口。其中，在“Solution（解答）”部分将给出合理的解决方法；在“Instructions（操作步骤）”部分根据被扫描计算机系统类型，给出详细的操作流程。

提示 对于“Check passed（通过检查）”的扫描结果，则不会出现“How to correct this”链接。

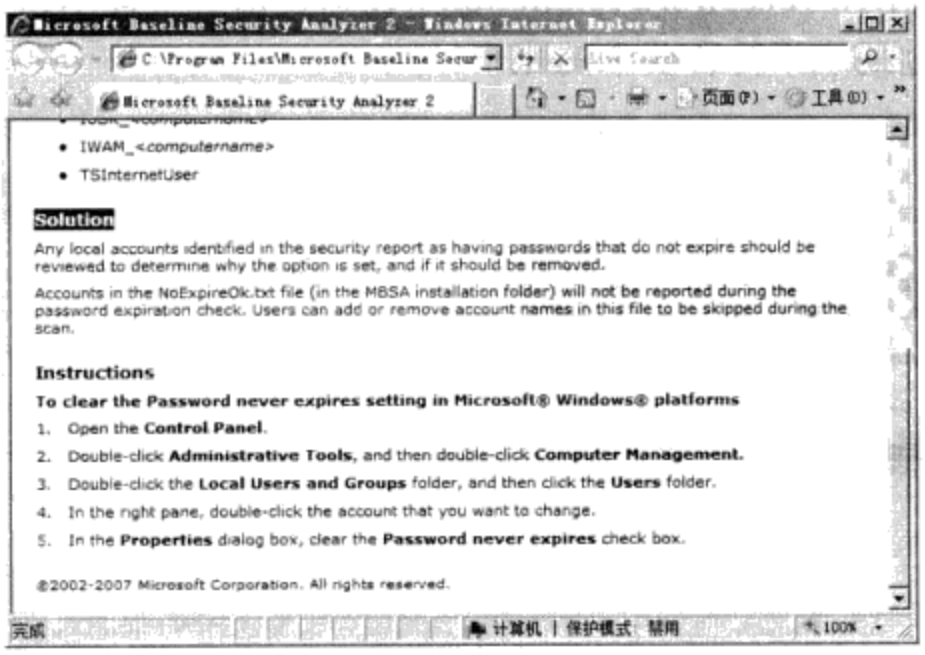


图 2-57 解决方法

第 7 步，在扫描结果窗口中，单击“OK”按钮结束此次扫描。

第 3 章　网络用户账户安全

网络用户账户信息通常是企业网络的重要资源，旺旺包含用户的私密性信息，并且用户账户是用户访问网络资源、接受统一管理的重要凭据，一旦失窃，后果不堪设想。因此，管理员必须为企业网络建立一套完善的用户账户管理机制，确保用户信息和企业网络的安全运行。目前，大多数企业网络都是通过 Active Directory 架构来管理网络资源，域管理员可以通过为用户创建对应的账户，然后为其分配不同的操作权限，来达到安全管理网络用户账户的目的。

3.1　Active Directory 安全管理

Active Directory 是 Windows Server 2008 R2 的默认服务器角色之一，主要用于管理企业网络的用户、计算机、文件等资源。Active Directory 是一个分布式数据库，它包含了网络中所有对象的信息，通过自身的安全认证和管理架构，为用户和网络资源提供身份认证和操作审核。同时，Active Directory 服务还是其他某些服务的基础，其安全性将直接影响其他网络服务的安全。

3.1.1　全局编录

“全局编录（Global Catalog，GC）”功能是 Active Directory 服务器提供的主要功能之一，主要存储林中主持域的目录中所有对象的完全副本，以及所有其他域中所有对象的部分只读副本。默认情况下，在活动目录中创建的第一个域控制器为全局编录服务器，其他域控制器也可以被指派为全局编录服务器，用于实现网络负载平衡和冗余。全局编录服务器负责响应网络中所有的全局编录查询，一旦出现问题，用户将无法查询和登录。建议网络安全要求较高的用户，配置多台全局编录服务器，以提高系统的可用性和可靠性。但需要注意的是，网络中 GC 之间的复制可能会增加一定的网络带宽开销。

> **注意**　当林中只有一个域时，则不必在登录时从全局编录获取通用组成员身份。因为 Active Directory 可以检测到林中没有其他域，并将阻止向全局编录查询此信息。

1. 概述

GC 服务器中存储的数据都是用户搜索操作中最常用的部分，可以为用户提供高效的搜索，避免再去调用域控制器中的 Active Directory 数据库对网络性能带来的影响。全局编录的主要功能如下：

- 查找对象。全局编录允许用户在林中的所有域中搜索目录信息，无论目标数据存储在什么位置，都将以最快的速度和最低的网络流量在林中执行搜索。
- 提供用户主体名称身份验证。当验证域控制器无法识别用户账户时，全局编录服务器

会解析主体名称（User Principal Name，简称 UPN），从而确定其属于林中的哪个域。例如，如果某账户属于 hs.coolpen.net，并且使用 liuxh@hs.coolpen.net 的 UPN 名称从一台位于 heb.coolpen.net 的计算机上登录，则此时 heb.coolpen.net 无法为该用户提供身份验证，必须与全局编录服务器联系，经确认后该用户账户方可顺利登录。

- 验证林内的对象引用。域控制器使用全局编录验证对林内其他域的对象的引用。当域控制器保留其属性包含对其他域中对象引用的目录对象时，域控制器将通过与全局编录服务器联系来验证引用的合法性。
- 提供多域环境中的通用组成员身份信息。域控制器可以始终发现其域中任何用户的本地组和全局组成员身份，并且这些组的成员身份信息是不被存储在全局编录服务器上的。在单域林环境中，域控制器可以始终发现通用组成员身份，但通用组可以包含来自不同域的成员，因此将通用组的成员身份信息复制到全局编录服务器，可以提供更广范围的账户身份信息验证。在多域林环境中的用户登录到允许通用组的域时，域控制器必须与全局编录服务器联系，以检索用户可能在其他域中具有的任何通用组成员身份。

提示 如果用户登录到通用组可用的域时，全局编录服务器不可用，则用户的客户端计算机可以使用缓存凭据登录；如果用户在此之前并未登录到过该域，则用户只能登录到本地计算机。

2. 添加全局编录服务器

默认情况下，每个域林中只有一台全局编录服务器，即根域控制器。但为了提升网络安全性，往往需要添加一台或者多台全局编录服务器，实现冗余和负载均衡。在根域控制器上进行如下操作，即可将其子域控制器或备份域控制器提升为全局编录服务器：

第 1 步，依次选择“开始”→“管理工具”→“Active Directory 站点和服务”选项，打开“Active Directory 站点和服务”窗口，依次展开“Sites”→“Default-First-Site-Name（系统默认站点名称）”→“Servers”→“TIANJL（子域控制器）”→“NTDS Settings”节点，如图 3-1 所示。

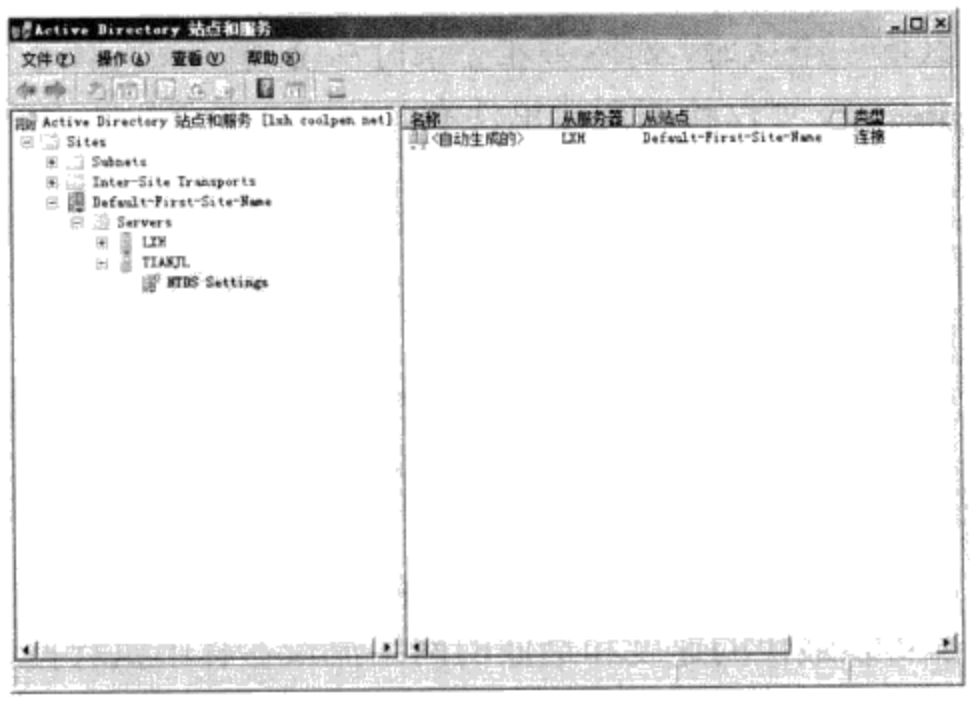


图 3-1 “Active Directory 站点和服务”窗口

第 2 步，右击“NTDS Settings”并选择快捷菜单中的“属性”选项，显示如图 3-2 所示“NTDS Settings 属性”对话框，选中“全局编录”复选框。

第 3 步，单击“确定”按钮，提示所选子域是当前域中的结构主机角色，不适宜用做全局编录服务器。单击“是”按钮确认，并单击“确定”按钮保存设置，即可将该子域提升为全局编录服务器。

如果在一台已经是全局编录服务器的控制器上，取消其“全局编录”身份之后，系统将立即停止对全局编录服务器服务端口（默认使用 3268 和 3269 端口）的监听。Windows Server 2008 R2 的 Active Directory 服务允许管理员删除全局编录服务器，但是不允许将全部全局编录服务器删除，否则用户账户将无法正常登录，Active Directory 将不能正常运行。

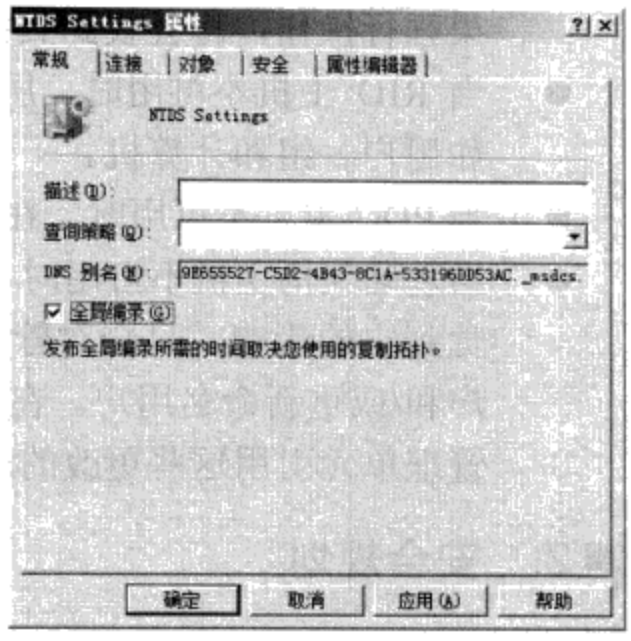


图 3-2 “NTDS Settings 属性”对话框

注意 设置完成，并不代表全局编录服务器已经提升完成，全局编录数据库同步需要时间。

3.1.2 操作主机

默认情况下，Active Directory 域中的第一台域控制器承载着整个林的所有操作主机（Operations Masters，OM）角色，也称为灵活单主机操作（Flexible Single Master Operation，FSMO）。操作主机是 Active Directory 数据库中的特殊对象，具备此类角色的域控制器肩负着 Active Directory 核心功能。Active Directory 域中有 5 种类型的操作主机，分别是：

- 架构主机（Schema Master）。
- 域命名主机（Domain Naming Master）。
- PDC 仿真器（PDC Emulator）。
- RID 主机（RIDMaster）。
- 基础架构主机（Infrastructure Master）。

其中，每个林中必须具备一个架构主机和一个域命名主机两种操作主机，并且这些角色是唯一的。而在林的每个域中都必须具备 RID 主机、PDC 主机和基础架构主机，并且均是唯一的。

1. 操作主机的重要性

操作主机在 Active Directory 环境中，肩负着重要的作用，如果操作主机出现问题，将会出现以下问题：

- 当架构主机不可用时，不能对架构进行更改。在大多数网络环境中，对架构更改的频率很低，并且应提前进行规划，以免由于使架构主机的故障，导致网络功能受到影响。

- 当域命名主机不可用时，不能通过运行 DCPROMO 向活动目录中添加或删除域，如果强行操作，将会收到类似“RPC 服务器不可用”提示信息。
- 当 RID 主机不可用时，所遇到的主要问题是不能向域中添加任何新的安全对象，例如用户、组和计算机。
- 当 PDC 主机不可用时，在本机模式环境中用户登录失败的可能性增大。
- 当基础架构主机不可用时，结构主机故障对环境的影响是有限的。最终用户并不能感觉到它的影响，只会对管理员执行大量组操作产生影响。这些组操作通常是添加用户和/或重新命名用户。在此情况下，结构主机故障只是会延迟通过 Active Directory 管理单元引用这些更改的时间。

2. 安全规划

鉴于操作主机在域中担负着如此重要的作用，转移或更改之前必须做好细致的规划。

■ 单域环境

Windows Server 2008 R2 或 Windows Server 2008 单域控制器上角色的初始配置，只能将所有 FSMO 主机角色部署在一台域控制器上，全局编录服务器也配置在此服务器上。在活动目录森林里，仅仅只有一个域的情况下，基础架构主机是不起作用的。

■ 多域环境

在多域环境中，存在多台域控制器和多台全局编录服务器，对性能的要求如下。

- 具有架构主机角色的域控制器上不需要高性能，通常情况下，只需保证其可用性即可，很少用于实际扩展。
- 具有域命名主机角色的域控制器不需要高性能，但是要保证高可用性。
- 具有 PDC 主机角色的域控制器是 FSMO 5 种角色里任务最重的，占用 PDC 模拟器的域控制器要保证高性能和高可用性。
- 具有 RID 主机角色的域控制器，不要求高性能，要保证高可用性。
- 具有基础架构主机角色的域控制器，可忽略性能和高可用性。

可以根据如下规则规划 FSMO 角色。

- 备用服务器与主要 FSMO 服务器位于同一站点中，以便在大的计算机组中获得更快的复制性能。
- 将 RID 角色和 PDC 模拟器角色放置在同一域控制器上。因为下级客户端和应用程序以 PDC 为目标，所以应保证从 PDC 到 RID 主机的良好通信。
- 在目录林级别上，架构主机角色和域命名主机角色应该放置在同一域控制器上。另外，域命名主机 FSMO 也应该是全局目录服务器。
- PDC 主机建议单独规划在一台域控制器。
- 域命名主机和全局编录服务器规划在一台域控制器上。
- 使用一个管理控制台可管理所有 FSMO 角色，并且确认所有的 FSMO 都是正常的。

“不要将结构主机放在全局目录服务器上”这一规则有以下两个例外。

- 单域目录林：在包含单个 Active Directory 域的目录林中没有跨域操作，因此没有需要结构主机完成的任务。在这种情况下，可以将结构主机放在域中的任一域控制器上。

- 多域目录林，其中的每个域控制器都包含全局目录：如果目录林中的每个域控制器承载全局目录，则没有需要结构主机完成的任务。在这种情况下，可以将结构主机放在目录林中的任一域控制器上。

3. 转移操作主机

在 Active Directory 环境中，如果具备操作主机角色的域控制器出现故障，在域控制器可用的情况下，可以使用“转移角色”的方式完成操作主机角色的转移。在域控制器不可用的情况下，可以使用“占用角色”的方式完成操作主机角色的转移。角色转移过程是可逆的，即可以从 A 域控制器转移到 B 域控制器，也可以从 B 域控制器重新转移到 A 控制器。

这里以域 coolpen.net 为例，介绍如何将操作主机角色从主域控制器（liuxh.coolpen.net）转移到额外域控制器（tianjl.coolpen.net），主要操作包括：

- 转移“Active Directory 用户和计算机”中的操作主机角色。
- 转移“Active Directory 域和信任关系”中的操作主机角色。
- 转移“Active Directory 架构”中的操作主机角色。

■ 转移“Active Directory 用户和计算机”中的操作主机角色

第 1 步，在主域控制器上，依次选择“开始”→“管理工具”→“Active Directory 用户和计算机”选项，将操作主机转移到额外域控制器之前，必须先连接到额外域控制器，即右击“coolpen.net”并选择快捷菜单中的“更改域控制器”选项，打开“更改目录服务器”对话框，选择“此域控制器或 AD LDS 实例”单选按钮，选中“tianjl.coolpen.net”选项，也可以选中“在此处键入目录服务器名称[:端口]”选项，输入域控制器或轻型目录服务器实例所在服务器的 IP 地址和端口号，如图 3-3 所示。

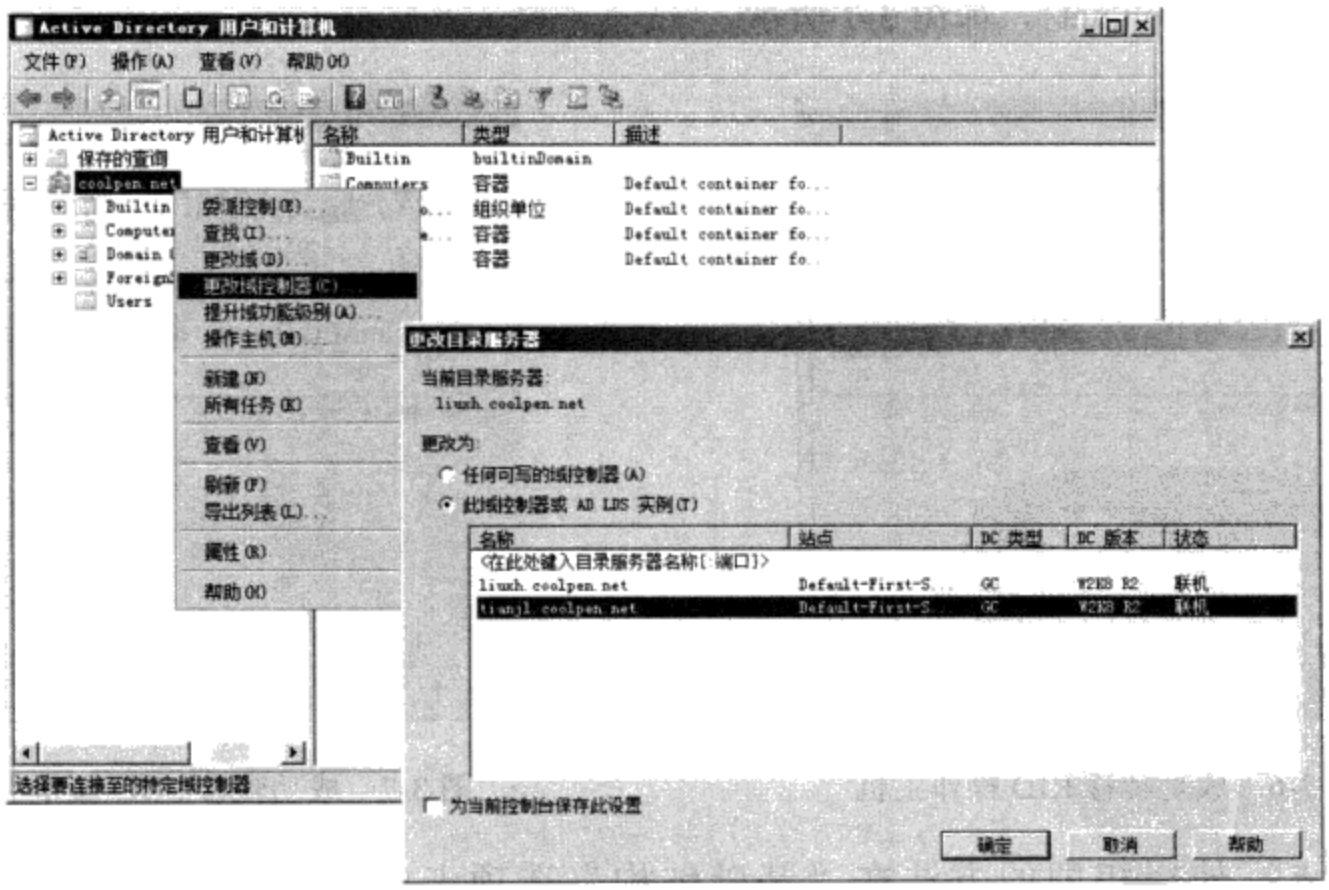


图 3-3 “更改目录服务器”对话框

第 2 步，单击“确定”按钮，返回到“Active Directory 用户和计算机”窗口。继续在主

域控制器上右击“coolpen.net”，选择快捷菜单中的“操作主机”选项，显示如图 3-4 所示“操作主机”对话框，默认显示“RID”选项卡。“操作主机”文本框中显示原主域控制器的主机名。

第 3 步，单击“更改”按钮，显示“Active Directory 域服务”对话框，即将更改 RID 主机角色到转移到额外域控制器上。单击“是”按钮，确认转移操作主机角色，提示：成功传送了操作主机角色，如图 3-5 所示。

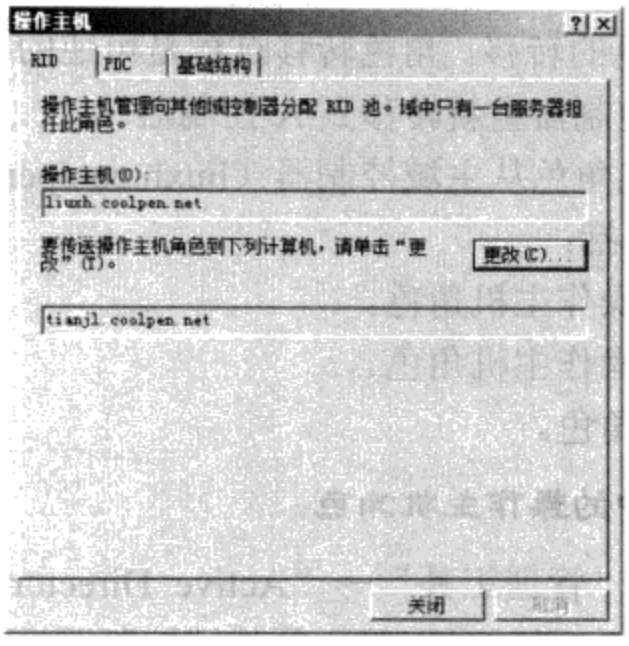


图 3-4 “RID”选项卡

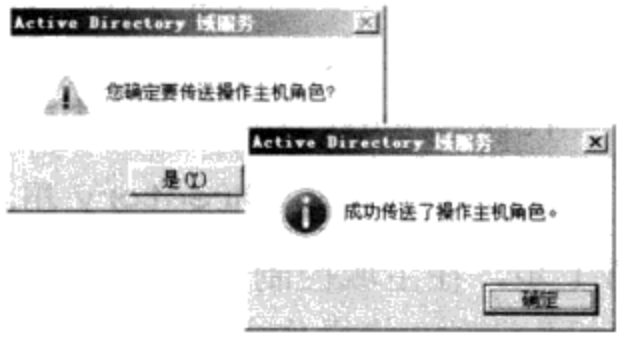


图 3-5 “Active Directory 域服务”对话框

第 4 步，单击“确定”按钮，返回到“操作主机”对话框的“RID”选项卡，如图 3-6 所示，“操作主机”文本框中已经转变为额外域控制器的主机名。

第 5 步，使用相同的方法在“PDC”选项卡中，将“操作主机”由原来的“liuxh.coolpen.net”更改为“tianjl.coolpen.net”，如图 3-7 所示。

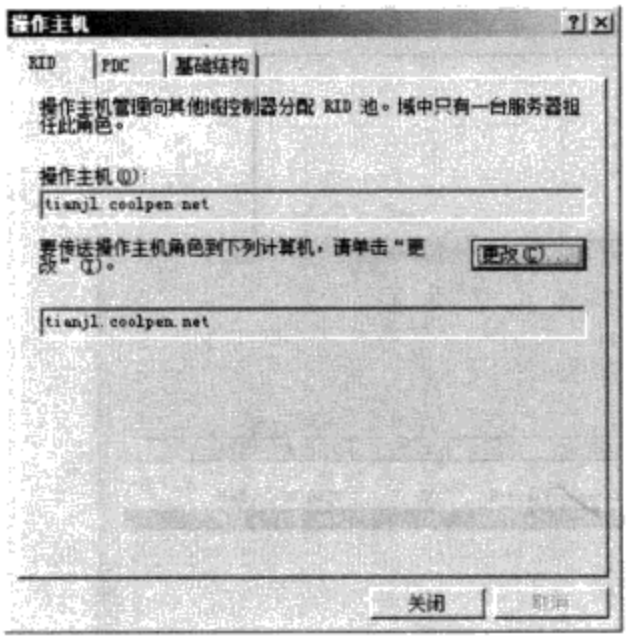


图 3-6 成功转移 RID 操作主机

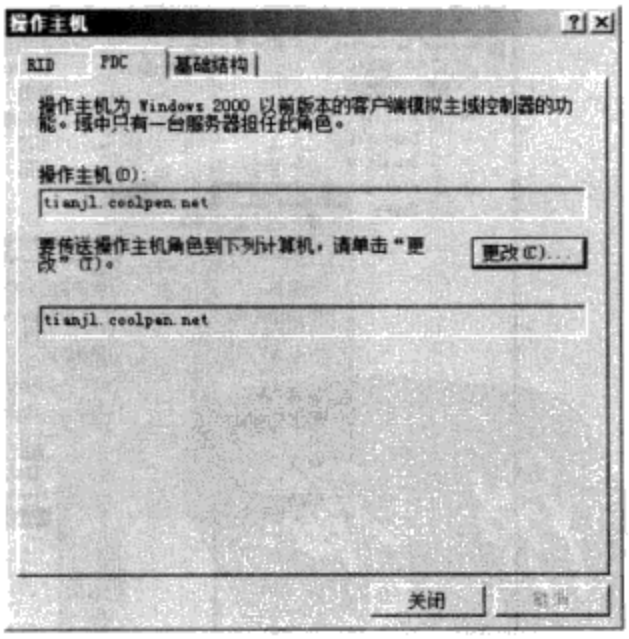


图 3-7 成功转移 PDC 操作主机

第 6 步，使用相同的方法在“基础结构”选项卡中，将“操作主机”由原来的“liuxh.coolpen.net”更改为“tianjl.coolpen.net”，如图 3-8 所示。

注意 “基础结构”角色的转移与当前额外域控制器是否同时担当“全局编录”角色有关，如果是则将提示如图 3-9 所示“Active Directory 域服务”对话框。但此时如果可以确保额外域控制器上“全局编录”服务的可用性，也可以单击“是”按钮强行转移。强行转移此角色并不会对其他角色功能产生影响。

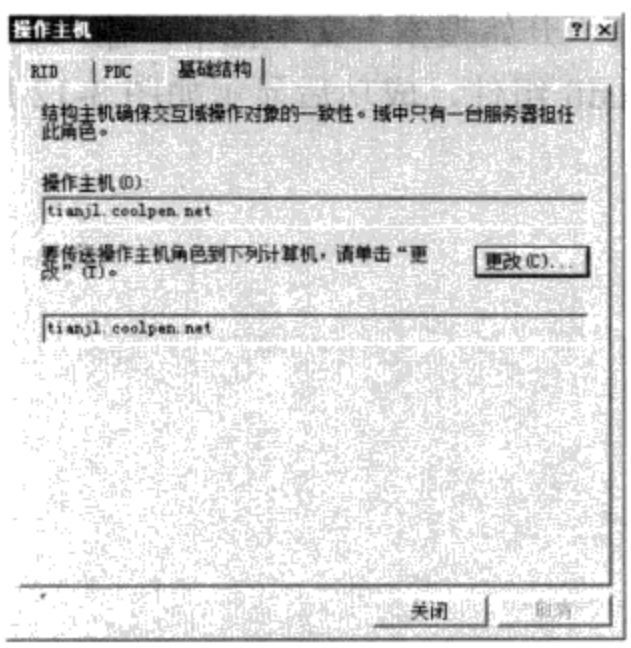


图 3-8 “基础结构”选项卡

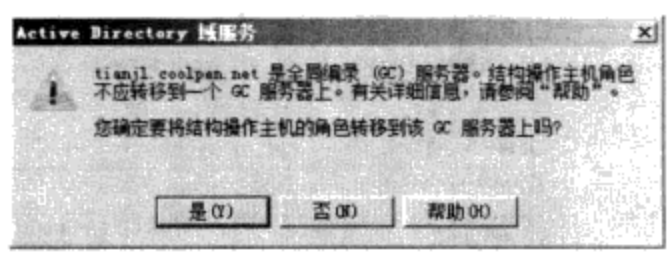


图 3-9 “Active Directory 域服务”对话框

■ 转移“Active Directory 域和信任关系”中的操作主机角色

第 1 步，在主域控制器上，依次选择“开始”→“管理工具”→“Active Directory 域和信任关系”选项，打开“Active Directory 域和信任关系”窗口。右击“Active Directory 域和信任关系”，选择快捷菜单中的“操作主机”选项，显示如图 3-10 所示“操作主机”对话框。“域命名操作主机”默认仍是原来的主域控制器名称。

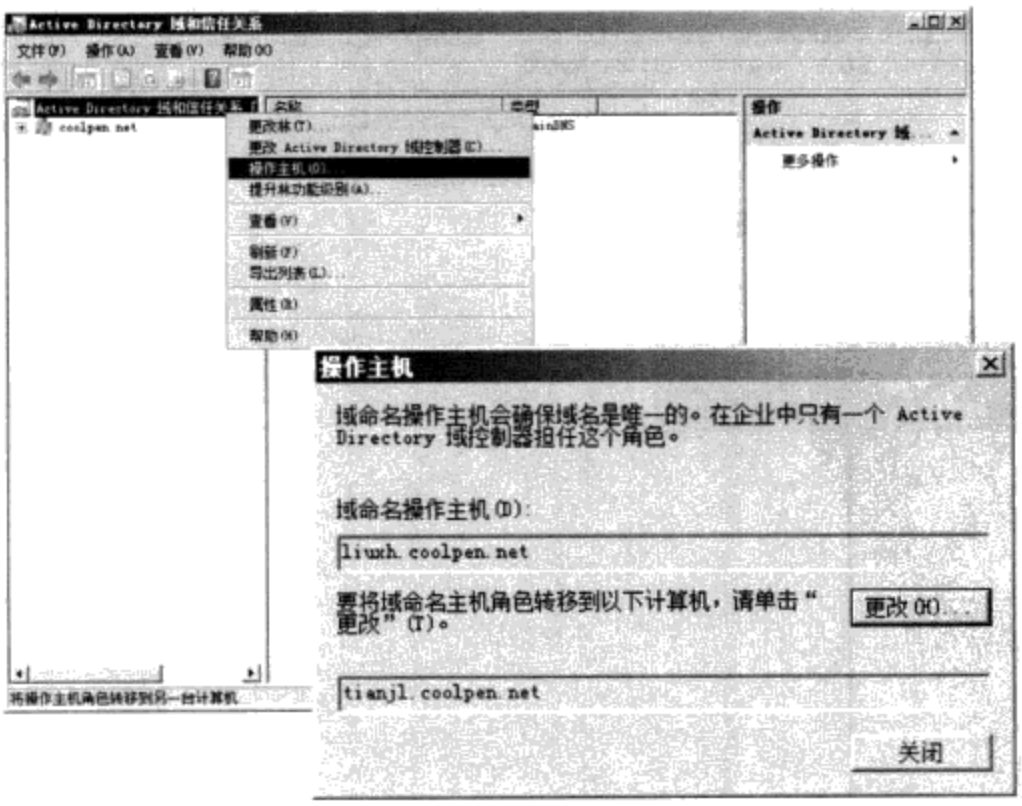


图 3-10 “操作主机”对话框

第 2 步，单击“更改”按钮，提示是否确实要移动操作主机，单击“是”按钮，确认即可成功转移域命名主机，显示如图 3-11 所示结果。

■ 转移“Active Directory 架构”中的操作主机角色

在 Windows Server 2003/2008 域中，默认情况下并没有将 Active Directory 架构注册到系统中，因此进行架构查看和操作之前，必须先进行注册。转移“Active Directory 架构”中的操作主机角色的主要操作步骤如下。

第 1 步，在主域控制器上，单击“开始”按钮，在“开始搜索”文本框中，输入 regsvr32 schmmgmt.dll 并按 Enter 键，在系统中注册 schmmgmt.dll 组件，成功后显示如图 3-12 所示的对话框。直接单击“确定”按钮关闭即可。

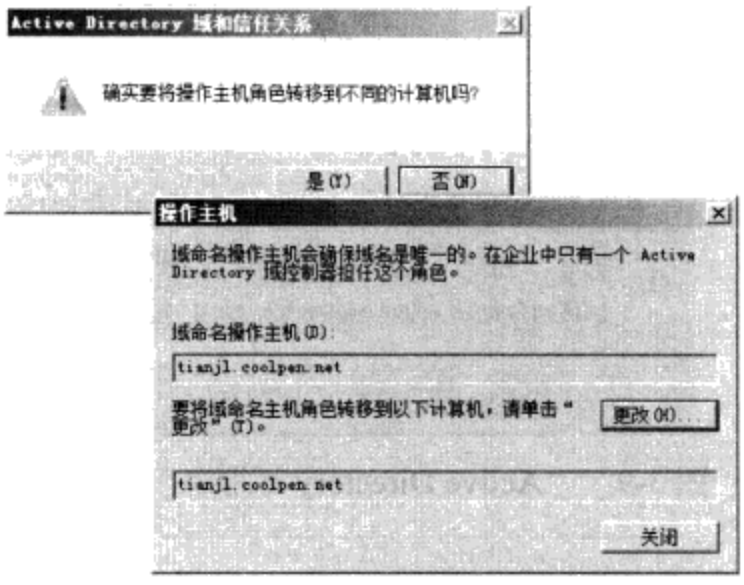


图 3-11 成功转移域命名角色

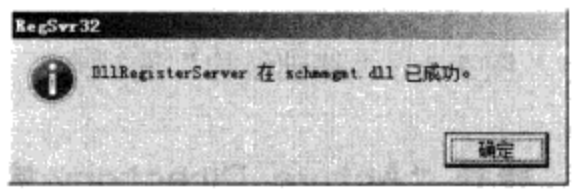


图 3-12 注册 schmmgmt.dll 组件

第 2 步，在“开始”菜单的“开始搜索”文本框中输入 mmc 并按 Enter 键，打开如图 3-13 所示“控制台”窗口，为了便于管理可以借助这种方法，将注册成功的“Active Directory 架构”添加到控制台中。

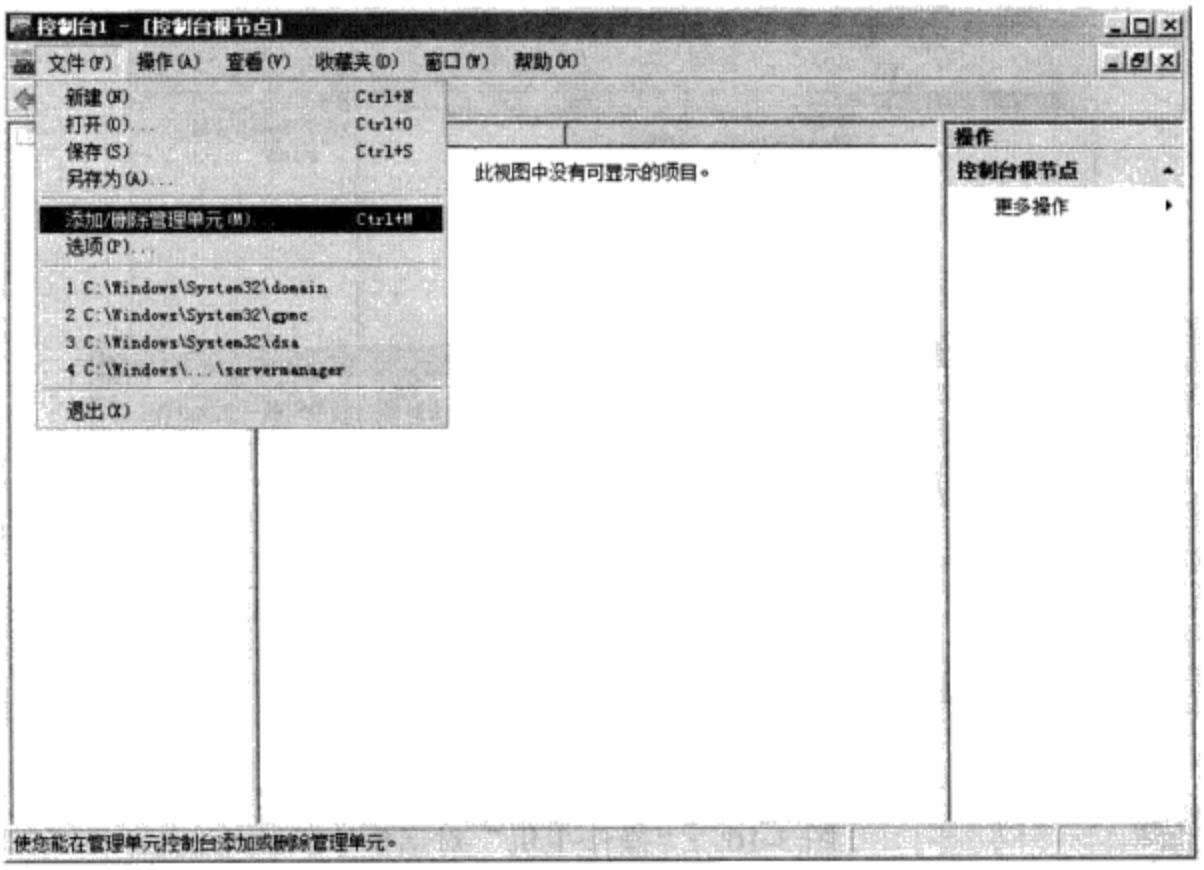


图 3-13 “控制台”窗口

第 3 步，依次选择“文件”→“添加/删除管理单元”选项，打开“添加或删除管理单元”对话框，在“可用的管理单元”列表框中选择“Active Directory 架构”组件，并单击“添加”按钮将其添加到“所选管理单元”列表框中，如图 3-14 所示。注册 schmmgmt.dll 组件之前，是不会出现该组件的。

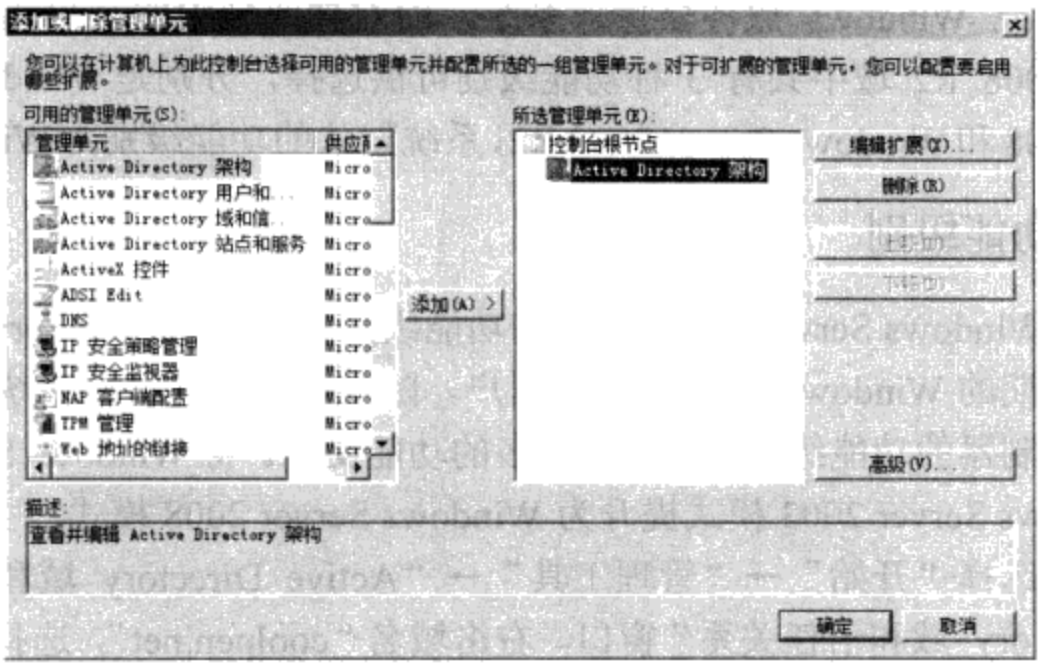


图 3-14 “添加或删除管理单元”对话框

第 4 步，单击“确定”按钮保存设置并退出，即可看到成功添加到控制台中的“Active Directory 架构”管理单元。右击“Active Directory 架构”，选择快捷菜单中的“更改 Active Directory 域控制器”选项，显示如图 3-15 所示“更改目录服务器”对话框。选择“此域控制器或 AD LDS 实例”单选按钮，并选择“tianjl.coolpen.net（额外域控制器计算机名称）”选项。单击“确定”按钮连接到额外域控制器。

第 5 步，再次右击“Active Directory 架构”，选择快捷菜单中的“操作主机”选项，显示如图 3-16 所示“更改架构主机”对话框。

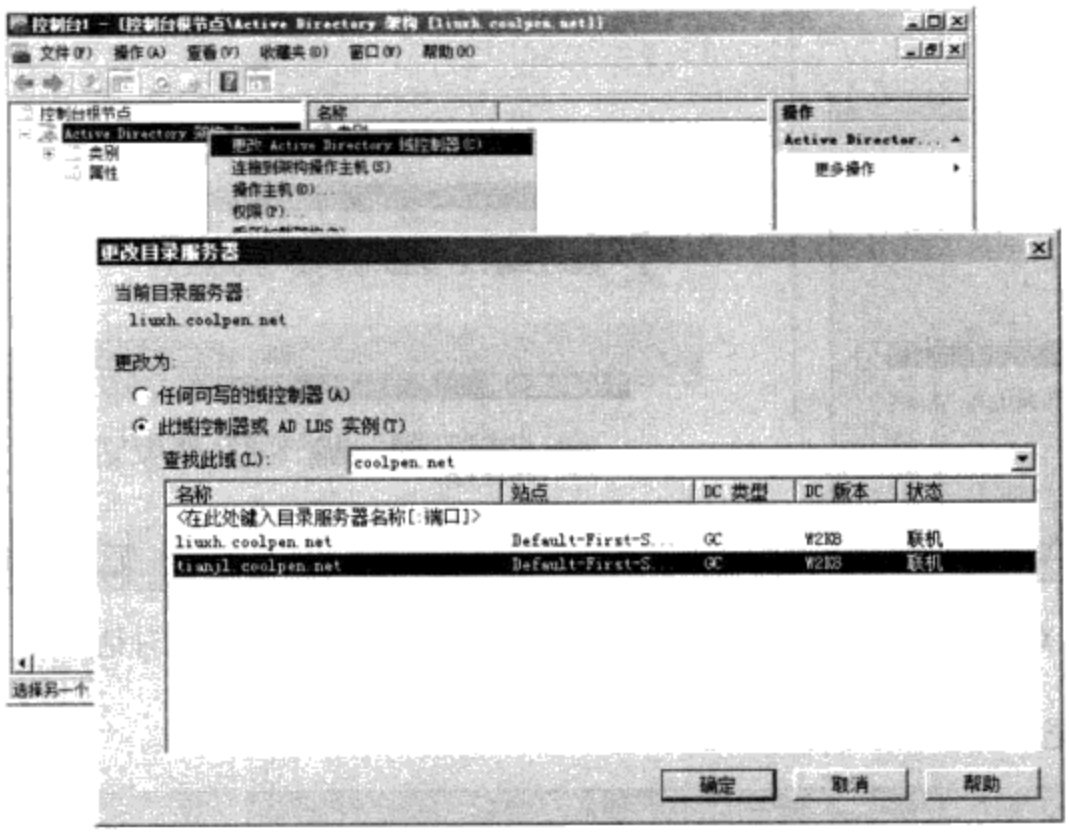


图 3-15 “更改目录服务器”对话框

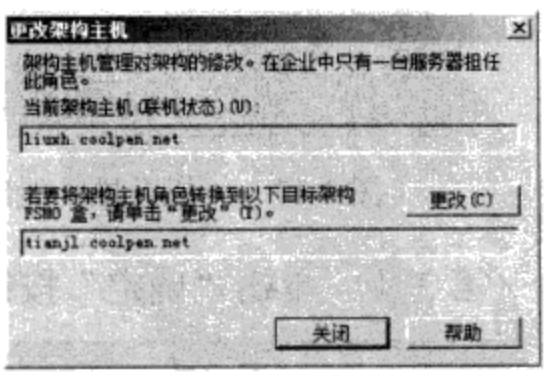


图 3-16 “更改架构主机”属性对话框

第 6 步，单击“更改”按钮，完成更改架构主机的转移。

3.1.3 功能级别

这里所介绍的功能级别包括林功能级别和域功能级别，分别用于定义可以在林或域中运行的域控制器类型或 Windows 服务器操作系统，而对林或域中的客户端不做任何定义。在 Windows Server 2008 R2 域中共有 3 种功能级别可供选择，分别是 Windows Server 2003、Windows Server 2008 和 Windows Server 2008 R2，系统默认的功能级别为 Windows Server 2003。

1. 提升域功能级别

默认状态下，Windows Server 2008 R2 域的功能级别都是 Windows Server 2003，这主要是为了兼容网络中早期的 Windows Server 2003 用户。随着网络中计算机系统的不断升级，可以根据需要提升域控制器的功能级别，以获得更多的功能支持。将 Windows Server 2008 R2 域功能级别，从 Windows Server 2003 模式提升为 Windows Server 2008 模式，主要操作步骤如下。

第 1 步，依次选择“开始”→“管理工具”→“Active Directory 域和信任关系”选项，显示“Active Directory 域和信任关系”窗口。右击域名“coolpen.net”，选择快捷菜单中的“提升域功能级别”选项，如图 3-17 所示“提升域功能级别”对话框，在“选择可用域功能级别”下拉列表框中，选择“Windows Server 2008”选项。由于当前级别模式为 Windows Server 2003 模式，所以只能选择“Windows Server 2008”或“Windows Server 2008 R2”。

第 2 步，单击“提升”按钮，提示当前更改存在的危险性，单击“确定”按钮，开始提升域 coolpen.net 的功能级别，提升完成显示如图 3-18 所示“提升域功能级别”信息提示框。

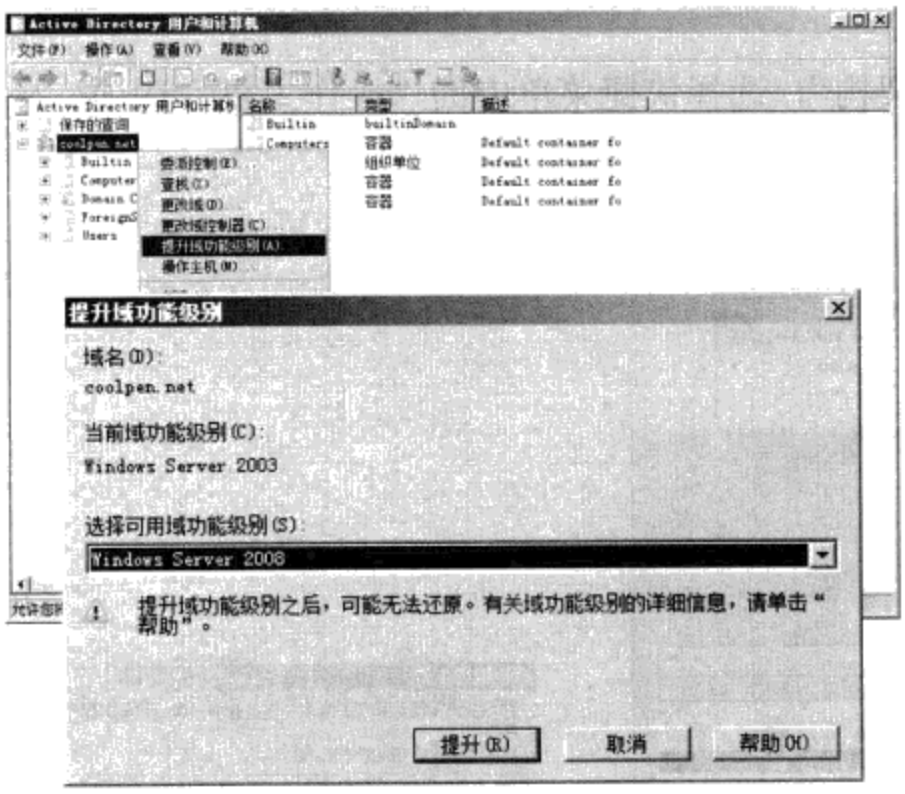


图 3-17 “提升域功能级别”对话框

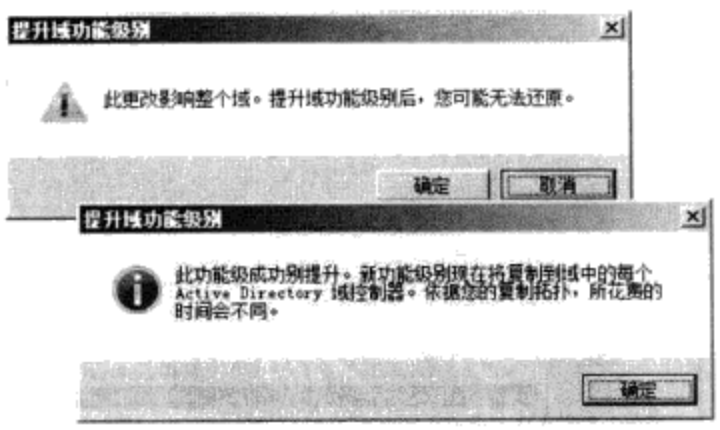


图 3-18 “提升域功能级别”对话框

第 3 步 单击“确定”按钮，完成域功能级别的提升。

注意 域功能级别提升是不可逆的，一旦提升到“Windows Server 2008”功能级别，将不能回退到“Windows Server 2003 模式”功能级别。

2. 林功能级别提升

林功能用于决定林中可以被激活的功能种类。默认状态下，Windows Server 2008 R2 的林功能级别是 Windows Server 2003 模式，如果要提升到 Windows Server 2008 或 Windows Server 2008 R2 林功能级别，必须先将网络的所有域控制器功能级别提升到 Windows Server 2008 或 Windows Server 2008 R2。

第 1 步，依次选择“开始”→“管理工具”→“Active Directory 域和信任关系”选项，打开“Active Directory 域和信任关系”窗口。右击“Active Directory 域和信任关系”，选择快捷菜单中的“提升林功能级别”选项，显示如图 3-19 所示“提升林功能级别”对话框。在“选择一个可用的林功能级别”下拉列表框中选择“Windows Server 2008”即可。

第 2 步，单击“提升”按钮，提示当前操作存在的危险性，是否继续更改。单击“确定”按钮，开始提升目录林 coolpen.net 的功能级别，提升完成后显示如图 3-20 所示“提升林功能级别”对话框。提示操作成功，并会将新的林功能级别复制到林中的每台域控制器上。

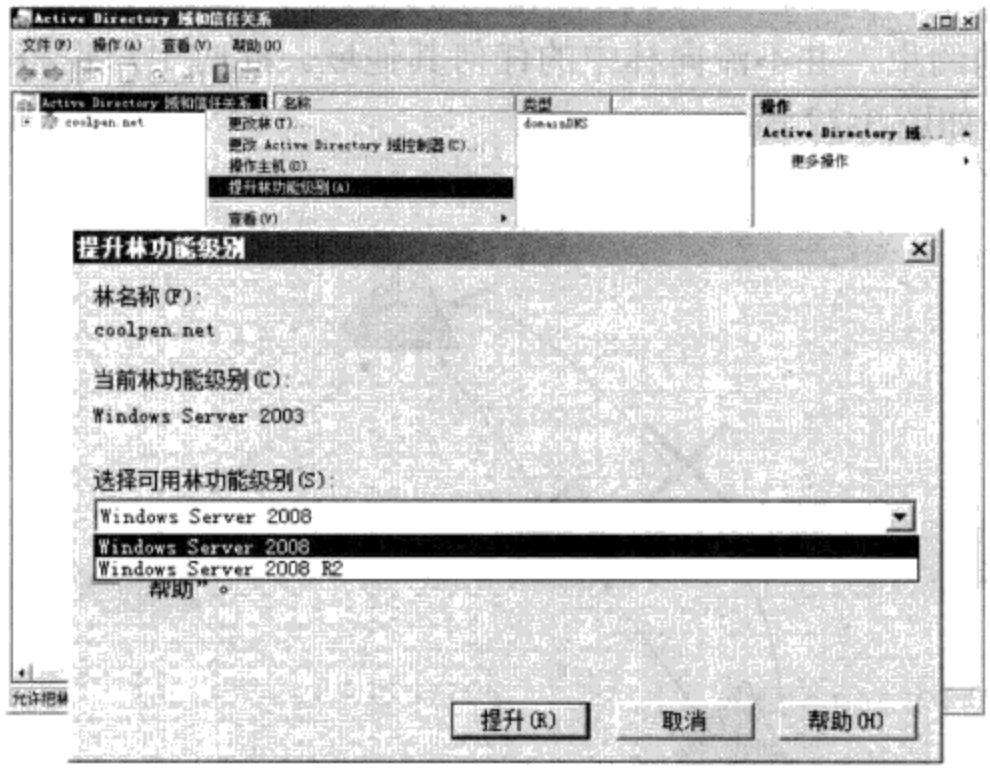


图 3-19 “提升林功能级别”对话框

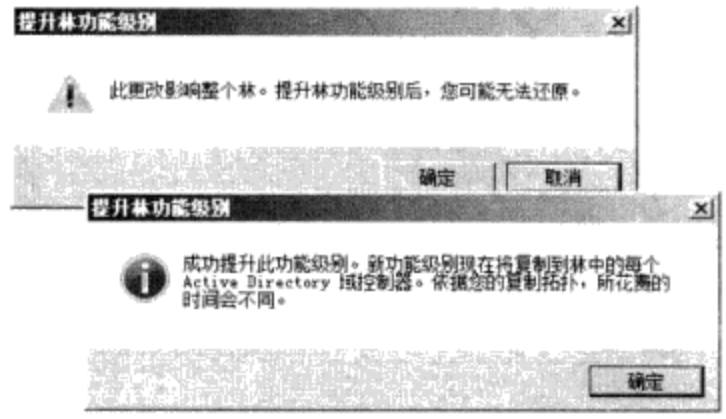


图 3-20 “提升林功能级别”对话框

第 3 步，单击“确定”按钮关闭对话框，完成目录林功能提升操作。

3.1.4 信任关系

域是网络中的安全边界，通常情况下不存在任何联系的域之间，是无法实现资源共享的。信任关系就是建立在域之间的逻辑关系，是彼此之间实现资源共享及互访的重要前提。通过信任关系的建立，可以将彼此的对象信息以某种方式相互传递，使分布于不同域的用户可以实现跨域登录。

1. 信任传递性

信任关系的传递性决定信任关系是否可扩展到建立信任的两个域之外，按照是否具有可传递性，信任关系分为可传递信任和非传递信任。可传递信任用于将信任关系扩展到其他域，

而非传递信任用于拒绝与其他域之间的信任关系。

■ **可传递信任**

任何一个 Windows Server 2008 R2 或 Windows Server 2008 域被加入到域目录树后，这个域会自动信任其父域，同时父域也会自动信任这个新域，并且这些信任关系是可以传递到以后加入到目录树中的其他域的。可传递信任关系将以域树形成时的方向沿域树向上流动，最终在域树中的所有域之间创建可传递信任。如图 3-21 所示是可传递信任关系及访问示意图。

由于这种信任关系都是建立在父域和子域之间的，所以也被称为父子信任关系。除以这种方式默认创建的可传递信任关系外，还可以通过手动方式创建如下 3 种类型的可传递信任关系：

- 快捷信任。在相同域目录树或域目录林中的域之间的可传递信任，用于缩短大型复杂的域树或林中的信任路径。
- 林信任。在林根域和第 2 个林根域之间的可传递信任。
- 领域信任。在 Active Directory 域和 Kerberos V5 领域之间创建可传递信任。

■ **非传递信任**

非传递信任受信任关系中的两个域的约束，并不流向林中的任何其他域。此时用户也将无法访问到没有直接建立信任关系的域，如图 3-22 所示。

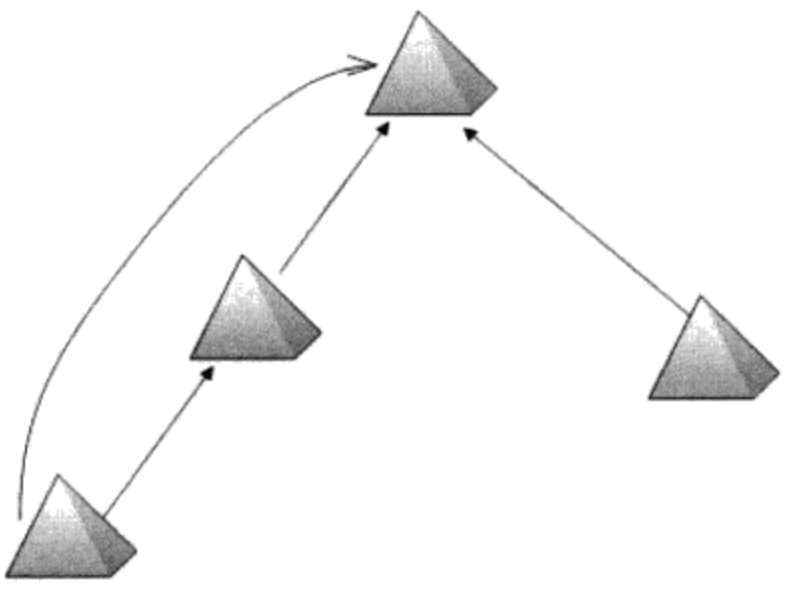


图 3-21 可传递信任关系

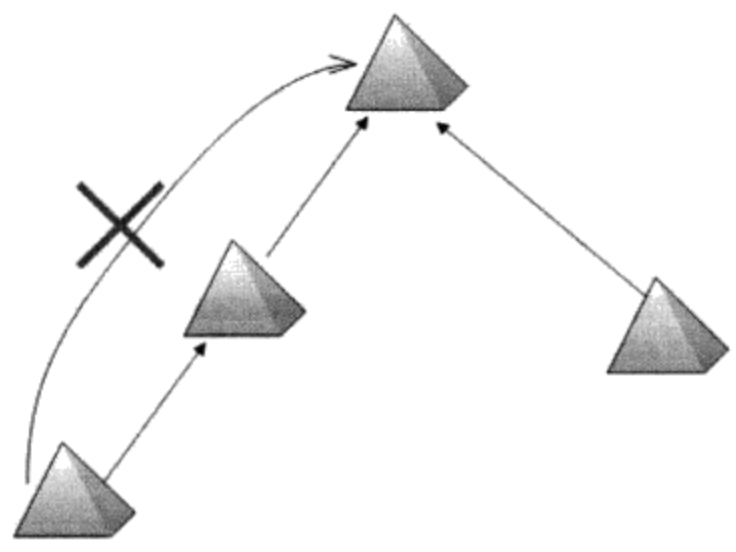


图 3-22 非传递信任关系

非传递域信任是以下各项之间唯一的信任关系形式：

- Windows Server 2008 R2 域、Windows Server 2008 域、Windows Server2003 域彼此之间。
- 一个林中的 Windows Server 2008 R2 域和其他林中的某个域（当没有被林信任联结时）。
- 管理员可以使用手动方式创建下列非传递信任：
- 外部信任。在单个 Windows 域之间，或不同林的 Windows 域之间创建的非传递信任关系。
- 领域信任。在 Windows Active Directory 域和 Kerberos V5 领域之间的非传递信任。

2. 信任方向

“信任域”和“受信任域”是信任关系中的两个主体，信任方向就是决定彼此之间的信任方式，通常以箭头表示。信任方向的分配将直接影响到用于身份验证的路径，信任路径则是身份验证请求必须符合域之间的一系列信任关系。信任方向可以分为单向信任和双向信任。

■ **单向信任**

单向信任是两个域之间创建的单向身份验证路径，即受信任域中的用户账户可以使用信任域上的身份验证方式，并访问域中的资源，但反之则无法实现。如图 3-23 所示是单向信任关系示意图。

■ **双向信任**

默认情况下，Windows Server 2008 R2 和 Windows Server 2008 林中的所有域信任关系都是双向、可传递的。创建新的子域时，双向可传递信任在新的子域和父域之间自动建立，这意味着身份验证求可按两种方向在两个域之间传递。如图 3-24 所示为双向信任关系示意图。

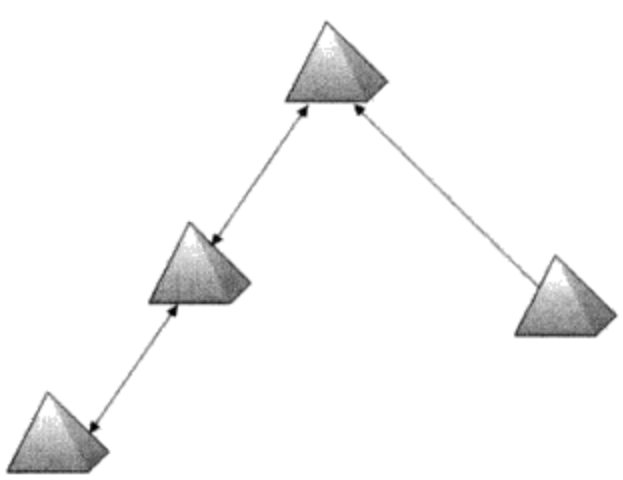


图 3-23 单向信任

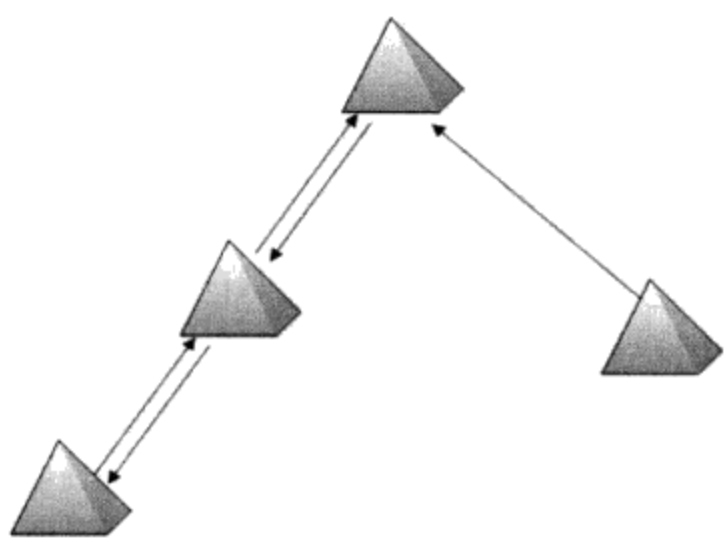


图 3-24 双向信任关系

Windows Server 2003 可以建立与下列各域之间的单向或双向信任：

- 同一林中的 Windows Server 2003 域。
- 不同林中的 Windows Server 2003 域。
- Windows NT 4.0 域。
- Kerberos V5 领域。

3. 信任安全规划

在默认状态下，在使用“Active Directory 安装向导”创建域的同时，系统会自动创建默认的信任关系，父子信任和域间信任。除此之外，用户根据需要创建信任关系之前，必须做好详细规划，以免实施之后导致不必要的网络安全威胁，通常应考虑如下因素：

■ **何时创建快捷信任**

快捷信任是当系统管理员需要优化身份验证过程时，可以使用单向或双向可传递信任。身份验证要求必须首先通过域树之间的信任路径，在复杂的林中，验证的时间会很长，执行的效率会很低。快捷信任可以缩短该信任验证的时间。信任路径是为了传递任何两个域之间的身份验证求而必须遍历的一系列的域信任关系。

当某个域中经常有许多用户登录林中的其他域时，有必要使用快捷信任。快捷信任可有效地缩短在两个不同树中的域之间进行身份验证所要经过的路径。

- 使用单向信任。建立在不同域树中的两个域之间的单向快捷信任，可以减少完成身份验证求所需的时间，但只能在一个方向上传递。

- 使用双向信任。建立在不同域树中的两个域之间的双向快捷信任，可以减少完成源自其中任一域的身份验证求所需的时间。

■ 何时创建林信任

只能在一个 Windows Active Directory 林的林根域和另一个 Windows Active Directory 林的林根域之间创建林信任，此时可以为目录林中的所有域控制器提供一种单向或双向的可传递信任关系。

- 使用单向林信任。两个林之间的单向林信任允许受信任林的成员使用信任林中的资源，但此信任只是单向的。
- 使用双向林信任。两个林之间的双向林信任允许任一个林的成员使用另一个林中的资源；每个林中的域隐式信任另一个林中的域。

4. 创建信任关系

创建信任关系可以帮助用户扩展网络应用范围，实现更广资源的集中管理和应用。当网络中有多个不同的域时，想要让每个用户可以自由的访问网络中的每台服务器（不管是否属于这个用户属于的域）时，这些域之间就需要创建信任关系。本案例的实验环境中包括两台彼此独立的主域控制器 coolpen.net 和 hsnc.cn，IP 地址分别为 192.168.1.21 和 192.168.1.25。在其中一台域控制器（本例为 coolpen.net）上执行如下操作：

第 1 步，依次选择“开始”→“管理工具”→“Active Directory 域和信任关系”选项，打开“Active Directory 域和信任关系”窗口，右击域名 coolpen.net，选择快捷菜单中的“属性”选项，打开“coolpen.net 属性”对话框，单击“信任”切换至如图 3-25 所示“信任”选项卡。目前，该域中包含一个子域 hengshui.coolpen.net，自动创建了信任关系，所以显示在列表中。

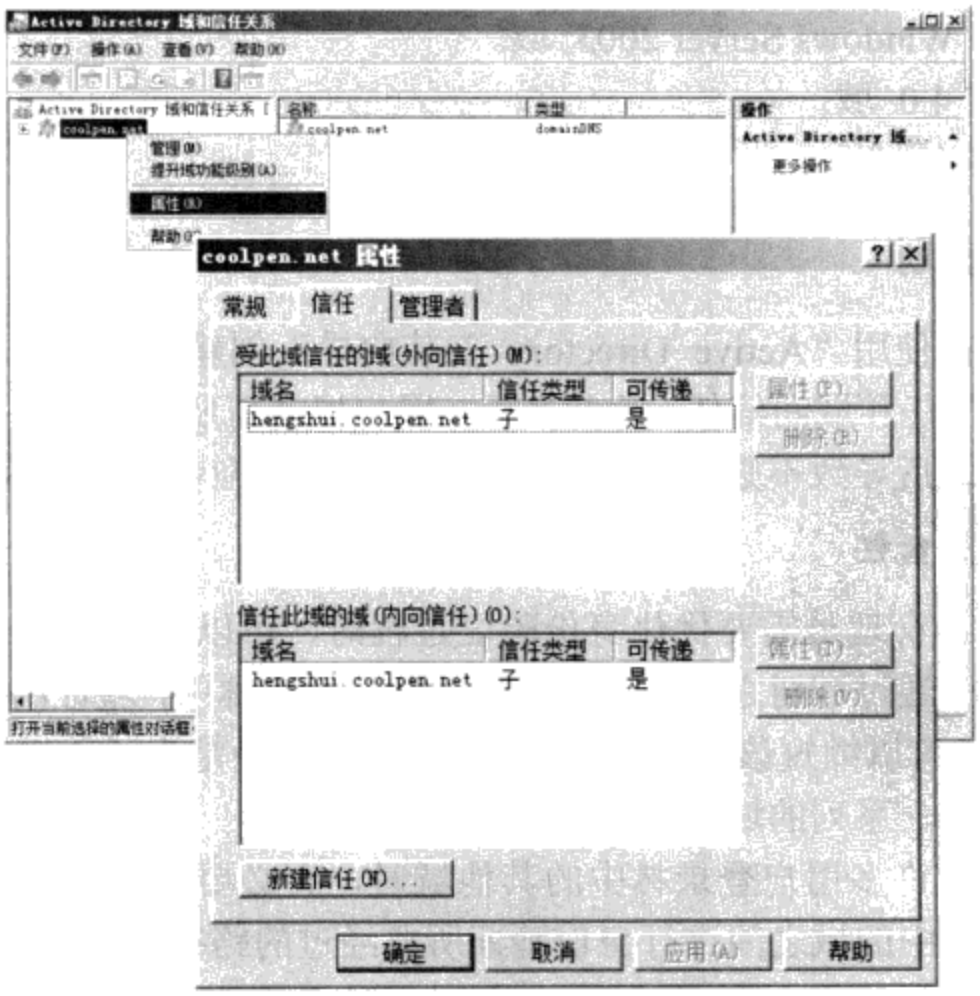


图 3-25 “信任”选项卡

第 2 步，单击“新建信任”按钮，启动“新建信任关系向导”，连续单击“下一步”按钮，在“信任名称”对话框的“名称”文本框中，键入想要与之建立信任关系的域控制器名称 hsnc.cn，也可以使用对方的 NetBIOS 名称 hsnc。在“信任方向”对话框中选择信任方向，系统默认选择“双向”单选按钮，如图 3-26 所示。

提示

如果两台域控制器的功能和安全级别有所不同，建议选择单向信任。单向信任可以划分为“单向：内传”和“单向：外传”，分别表示该域中的用户可以在指定的域、领域、域林中得到身份验证和指定域、领域或域林的用户可以在该域中得到身份验证，这两种情况均是单向信任。

第 3 步，单击“下一步”按钮，显示如图 3-27 所示“信任方”对话框。如果管理员具有每个域的管理权限，则可以通过选择“此域和指定的域”单选按钮，同时创建双方外部信任，否则选择“只是这个域”单选按钮，有对方域控制器的管理员完成相应操作即可。

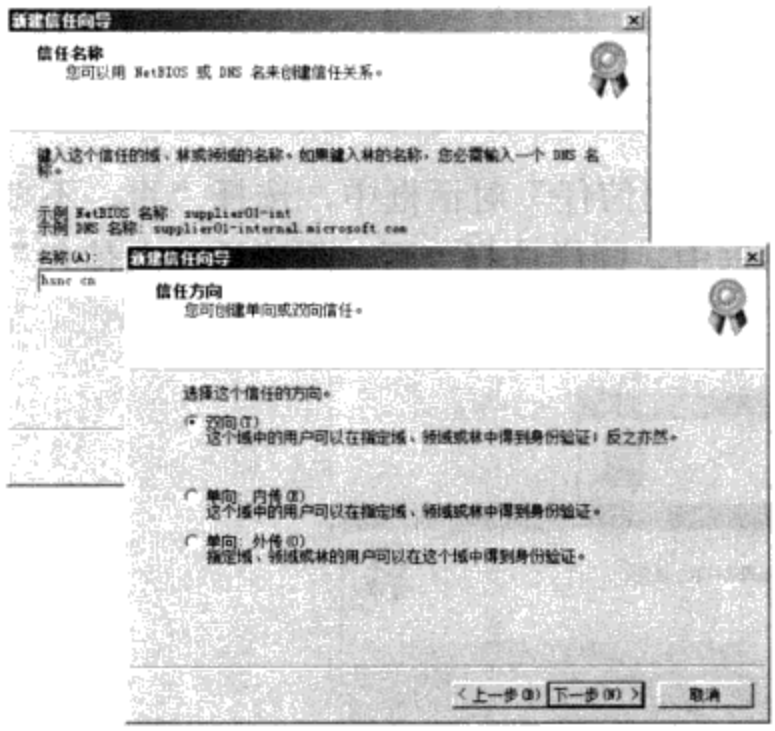


图 3-26　设置新人名称和信任方向

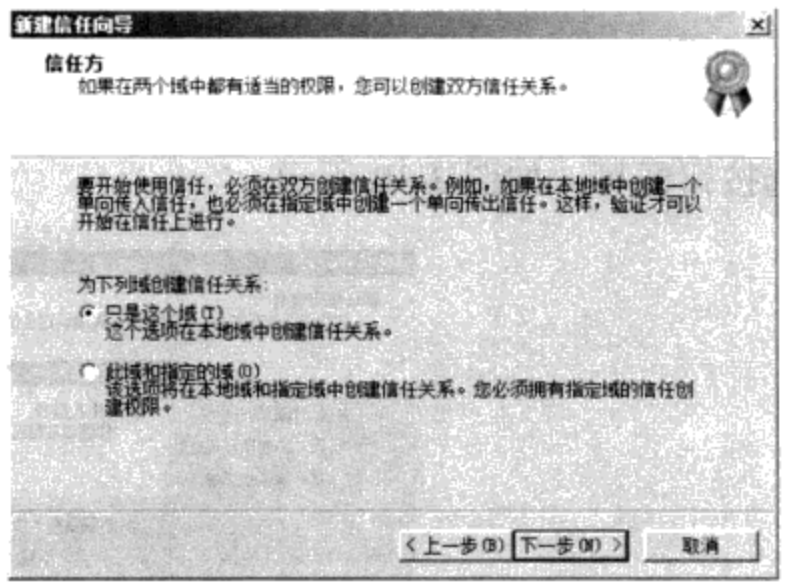


图 3-27　“信任方”对话框

第 4 步，单击“下一步”按钮，显示如图 3-28 所示“用户名和密码”对话框，在“用户名”和“密码”文本框中，分别输入域控制器 hsnc.cn 上的管理员账户及密码。

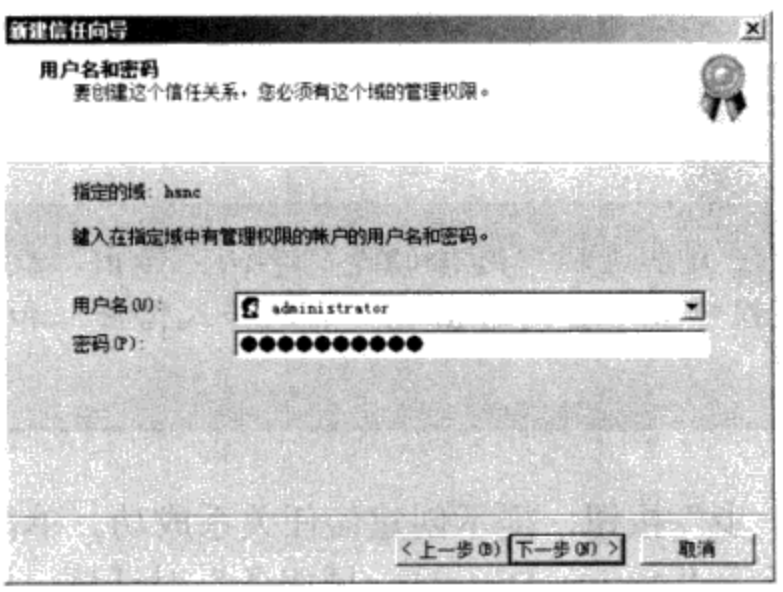


图 3-28　“用户名和密码”对话框

第5步，连续单击“下一步”按钮，完成信任关系的创建，如图3-29所示。创建完毕后，还可继续对该信任关系的某些选项进行配置，根据创建过程中选择选项的不同，配置选项也会有所不同。

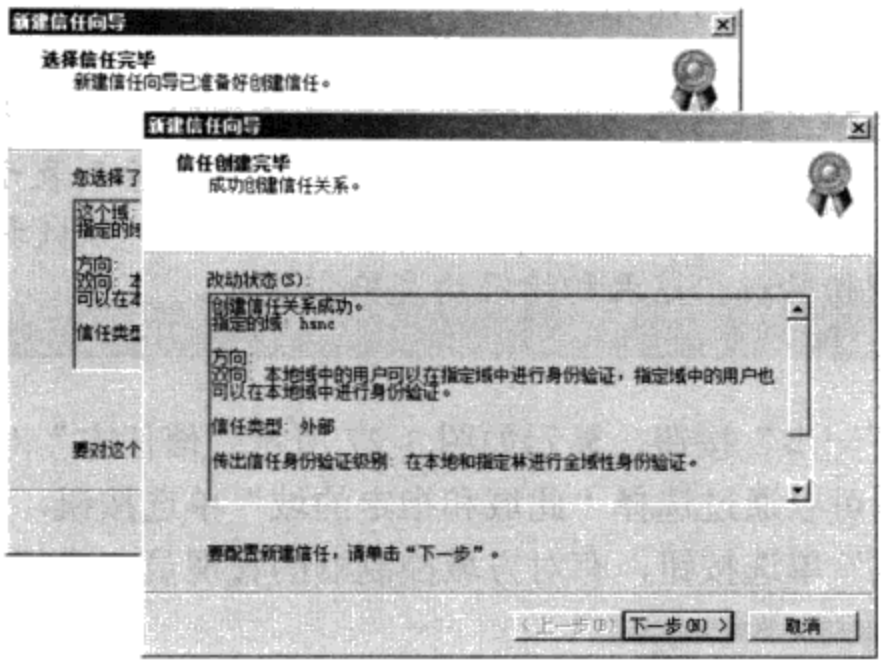


图3-29 信任创建完毕

第6步，连续单击“下一步”按钮，在“确认传出信任”对话框中，选择“否，不要确认传出信任”单选按钮。在“确认传入信任”对话框中，同样选择“否，不确认传入信任”单选按钮即可，如图3-30所示。

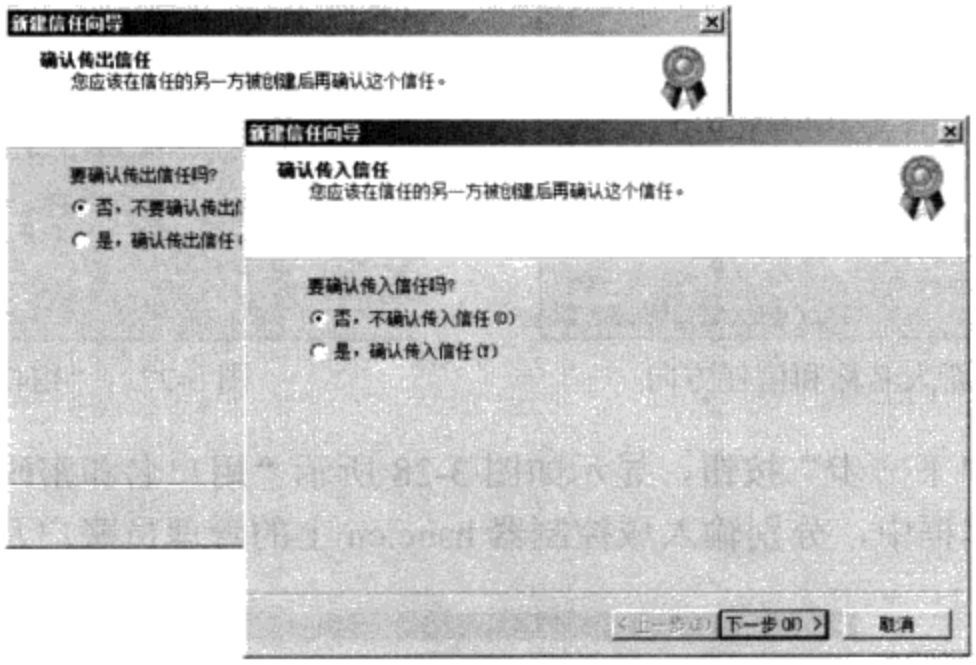


图3-30 确认传出和传入信任

提示 如果创建信任关系过程中选择的是“单向：传出”或者“单向：传入”信任方式，则配置过程中就不会同时出现“确认传入信任”和“确认传出信任”对话框。

第7步，单击“下一步”按钮，提示创建信任关系成功。单击“完成”按钮关闭新建信任向导，打开如图3-31所示“Active Directory域服务”对话框，提示已经启用SID（安全识别符）筛选功能。SID筛选用于防止可能试图将提升的用户权限，授予其他用户账户的恶意用

户攻击。强制 SID 筛选不会阻止同一林中的域迁移使用 SID 历史记录，而且也不会影响全局组的访问控制策略。对外部信任关系而言，SID 筛选功能会影响以下两个区域中的现有 Active Directory 基础结构：

- 将会从受信域发出的身份验证请求中删除 SID 历史数据，这些 SID 历史数据包含除该受信域外的所有域中的 SID。这会导致拒绝访问具有用户旧 SID 的资源。
- 林间通用组访问控制的策略将需要更改。

第 8 步，单击“确定”按钮，返回“coolpen.net 属性”对话框，新创建的信任关系已经显示在列表中，如图 3-32 所示。

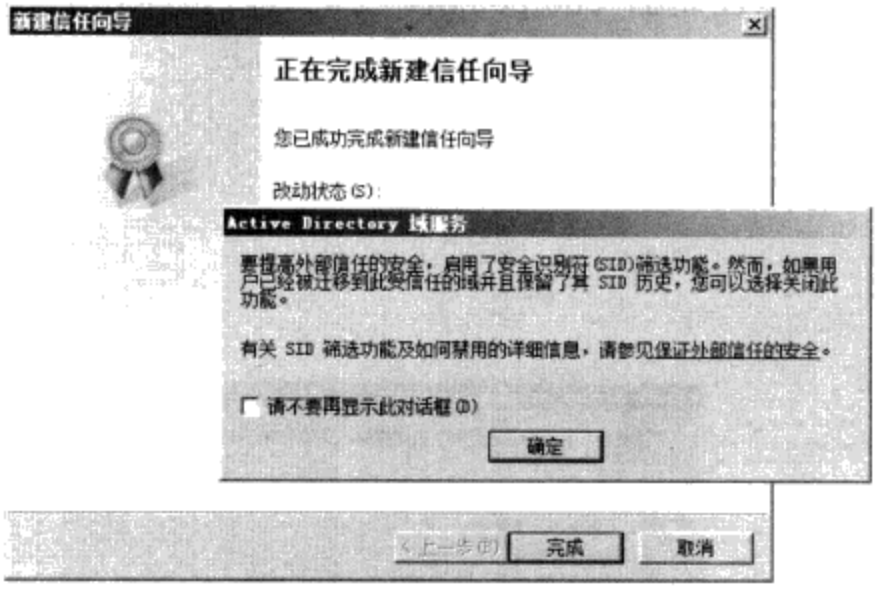


图 3-31 “Active Directory 域服务”对话框

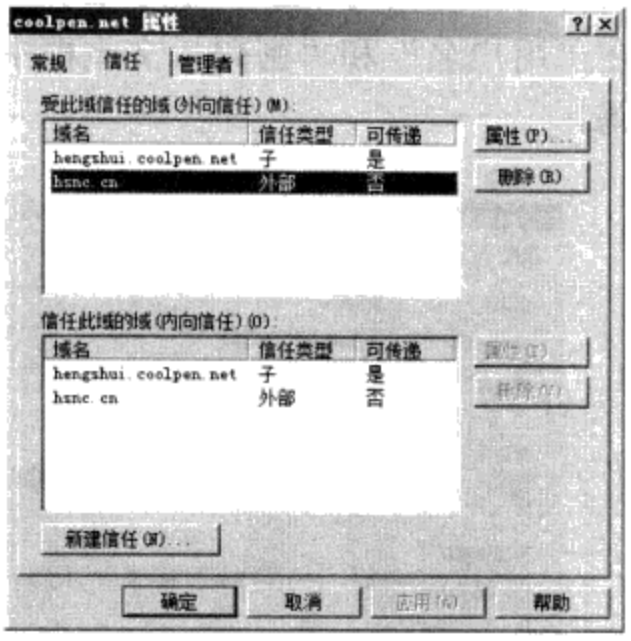


图 3-32 创建成功的信任关系

在另一台域控制器（本例中的 hsnc.cn）上，执行如下操作：

第 9 步，打开“Active Directory 域和信任关系”窗口，右击域名 hsnc.cn，选择快捷菜单中的“属性”选项，打开“hsnc.cn 属性”对话框，切换至如图 3-33 所示“信任”选项卡，默认已经显示了刚刚创建的信任关系。

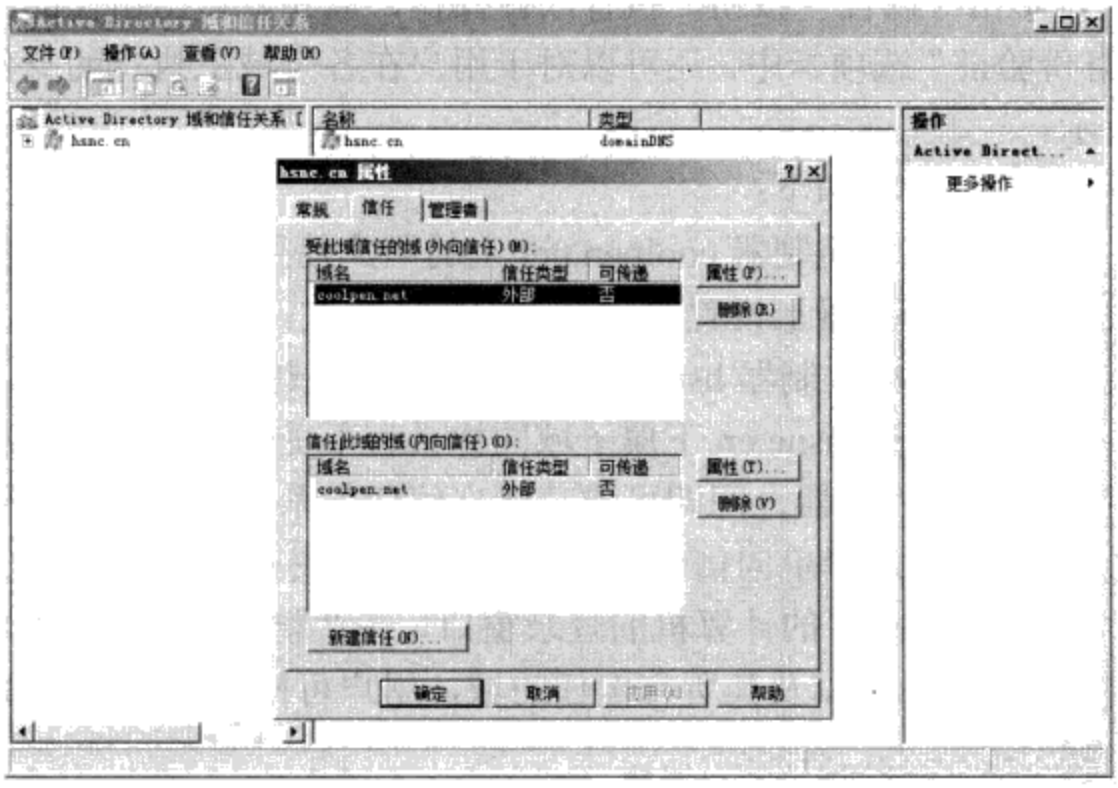


图 3-33 “hsnc.cn 属性”对话框

提示 如果创建的是单向信任关系，则已创建的信任关系只会出现在“受此域信任的域（外向信任）”或“此域信任的域（内向信任）”中的一个列表框中，但确认创建信任关系的操作步骤与双向信任完全相同。

第10步，在“受此域信任的域（外向信任）”列表框中，选择“coolpen.net”并单击“属性”按钮，打开“coolpen.net 属性”对话框，如图3-34所示。

第11步，单击“验证”按钮，显示如图3-35所示“Active Directory 域服务”对话框，验证信任传入方向时，必须有对方域控制器的管理员权限。选择“是，验证传入信任”单选按钮，并在“用户名”和“密码”文本框中，分别输入域控制器 coolpen.net 上的管理员账户名称和密码。

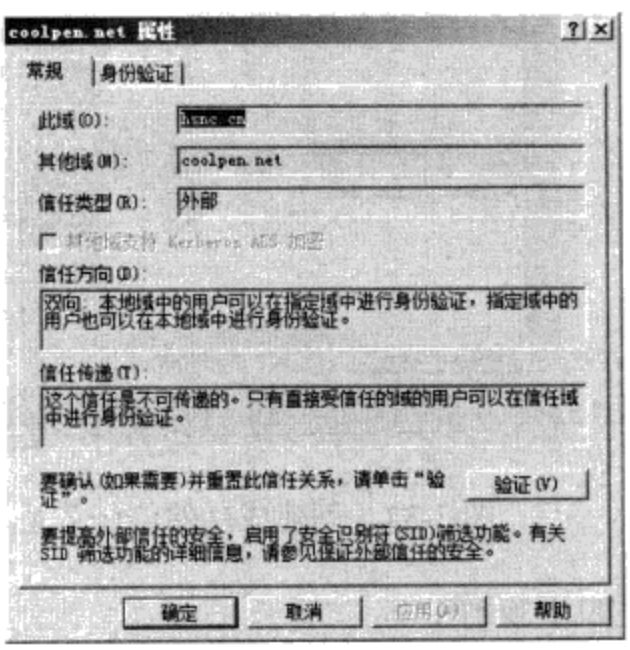


图3-34 “coolpen.net 属性”对话框

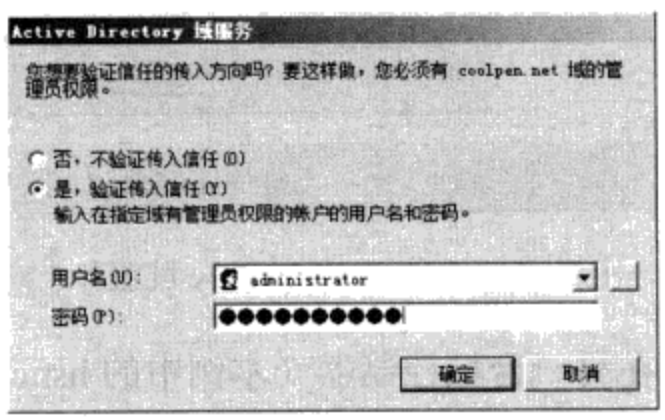


图3-35 “Active Directory 域服务”对话框

第12步，单击“确定”按钮，完成传入信任验证之后，还需要在“此域信任的域（内向信任）”选项框中，单击“属性”按钮，执行同样操作，以完成传出信任的验证。另外，在域属性对话框的“身份验证”选项卡中，还可以对于用户在各个域上执行的身份验证方式进行选择，如图3-36所示。

可供选择的身份验证方式如下：

- 全域性身份验证。域控制器 coolpen.net 上的用户使用域控制器 hsnc.cn 上的资源时，需要通过两台域控制器上设置的所有身份验证方式。
- 选择性身份验证。域控制器 hsnc.cn 将不会对来自域控制器 coolpen.net 的用户访问进行任何身份验证，对 hsnc.cn 下属子域同样具有不受身份验证的“特权”。

第13步，至此两台域控制器之间即可成功建立信任关系，这两个域的用户即可以自由访问另外一个域的信息（如果选择单向信任则另当别论）。如图3-37所示，是一台加入域控制器 coolpen.net 主机名为 coolpen-c8 的计算机的登录窗口，在“登录到”下拉列表框中显示了本地计算机、域控制器 coolpen.net 以及其所有信任的域，用户可根据需要选择登录到的对象。

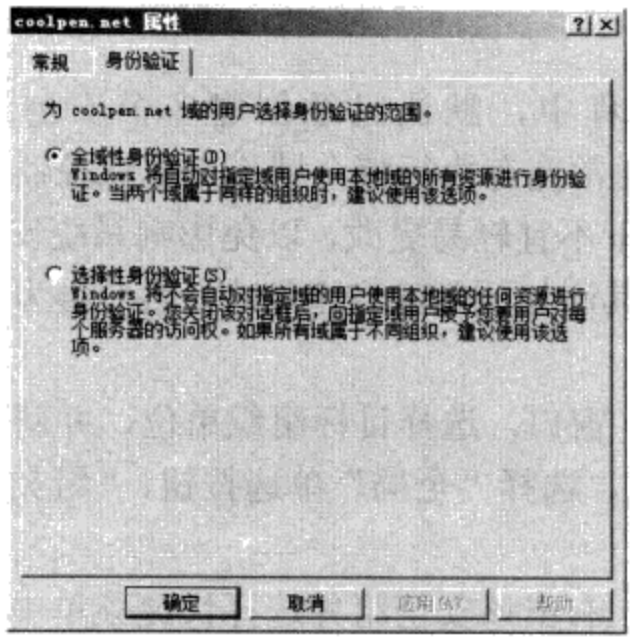


图 3-36 “身份验证”选项卡

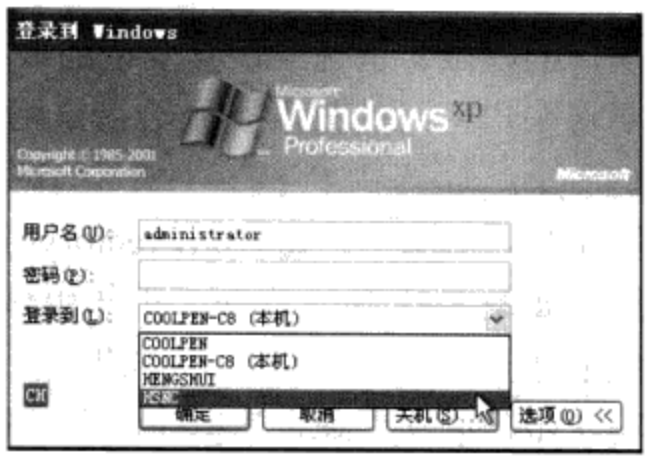


图 3-37 “登录到 Windows”窗口

3.1.5 权限委派

委派是 Active Directory 最重要的安全功能之一，将用于将某一功能的处理和管理的责任，分配给另一个用户、组或组织单位的权利。通过委派管理，可以使组织内的组更多地控制他们的本地网络资源。还可以通过限制管理员组的成员，保护网络不受意外或恶意的损伤。管理员可以通过两种方式将管理权限委派到指定的用户账户，一种是安全组权限委派，一种是 Active Directory 权限委派向导。此处以将重置账户密码权限委派到指定的用户账户为例进行介绍。

1. 权限委派概述

委派是 Active Directory 最重要的安全功能之一，将用于将某一功能的处理和管理的责任，分配给另一个用户、组或组织单位的权利。通过委派管理，可以为适当的用户和组指派一定范围的管理任务，这样不仅可以减少需要具有较高管理权限的管理员用户账户数量，还可以为普通用户和组指派基本管理任务，而让 Domain Admins 和 Enterprise Admins 组的成员执行域范围和林范围的管理。通过委派管理，可以使组织内的组更多地控制他们的本地网络资源。还可以通过限制管理员组的成员，保护网络不受意外或恶意的损伤。通过委派，让信任用户可以在一个特定容器内改变属性、创建或删除某种类型的对象以及更改某种类型对象的某些属性等。

通过在域中创建组织单位，并将特定组织单位的管理控制权委派给特定用户或组，可将管理控制权委派给域树的任何层次。通常情况下，可以向以下 Active Directory 容器委派管理权限。

- 组织单位。
- 域。
- 站点。

其中，向“域”和“组织单位”委派的管理权限包括将计算机加入域、管理组策略链接、重设用户账户的密码、读取所有用户信息以及管理硬件资源等。

2. 安全组权限委派

在 Windows Server 2008 R2 域控制器安装过程中，默认已经创建多个安全组，如 Administrators、Domain Admins 等，这些组中的成员通常拥有执行整个域或本地域控器上某些安全操作的权限。系统默认安全组的成员，通常情况下不宜轻易更改，以免影响系统安全。如果需要将账户密码的权限委派给指定用户，可以现将其添加到新建安全组中，然后再为其分配权限。

第 1 步，打开 “Active Directory 用户和计算机”窗口，选择目标组织单位，并新建一个安全组，如图 3-38 所示。在“组作用域”选项区域中，选择“全局”单选按钮，“组类型”选项区域中选择“安全组”单选按钮。

第 2 步，单击“确定”按钮，完成安全组的创建。右击该安全组并选择快捷菜单中的“属性”选项，打开安全组属性对话框，切换至如图 3-39 所示“安全”选项卡。

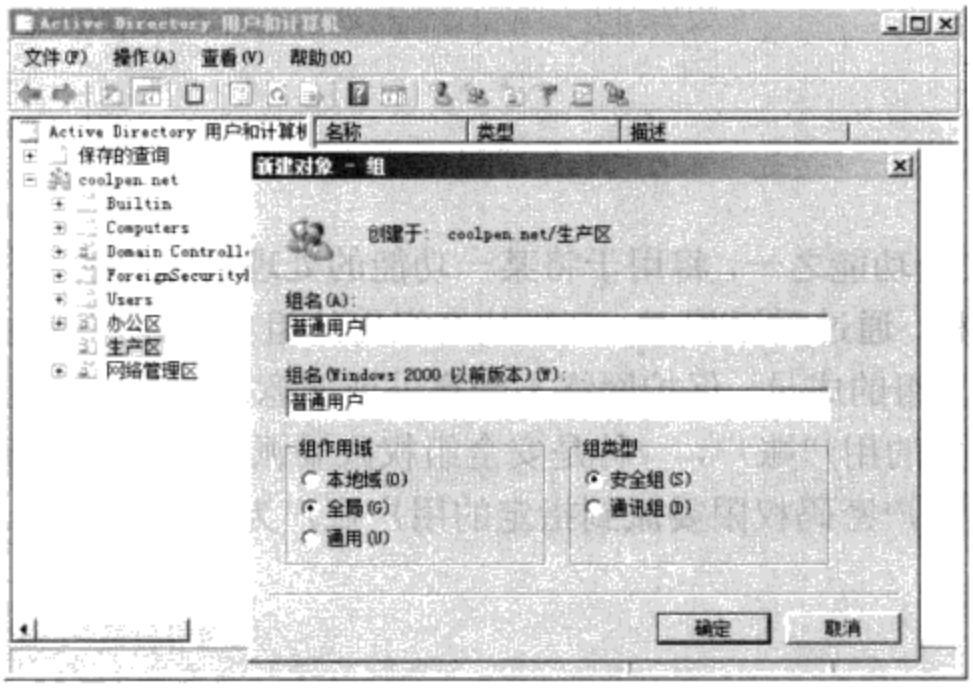


图 3-38　新建安全组

图 3-39　“普通用户 属性”对话框

提示　如果打开的组属性对话框中，没有“安全”选项卡，可以在“Active Directory 用户和计算机”窗口中，依次选择“查看”→“高级功能”选项使其显示，如图 3-40 所示。

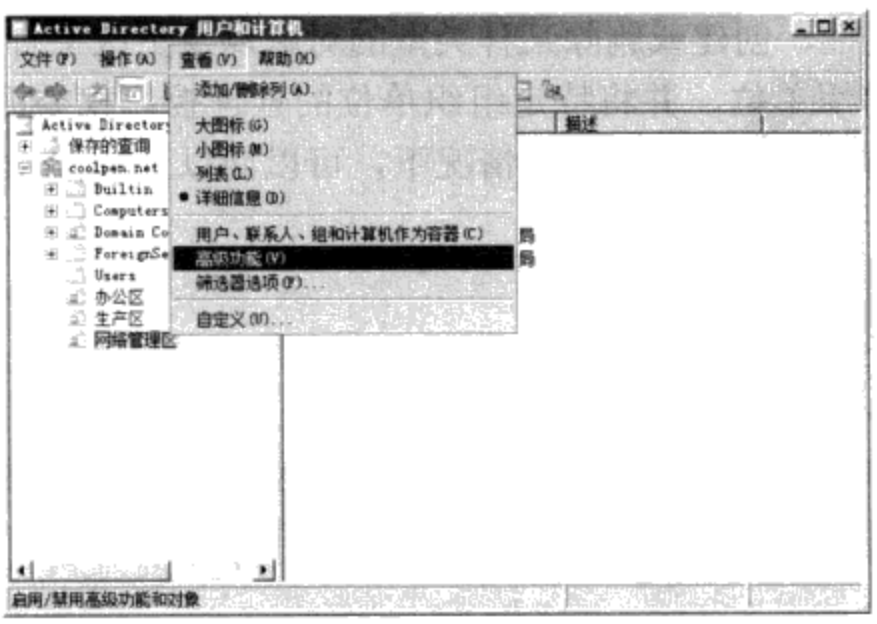


图 3-40　使用高级功能

第 3 步，单击“高级”按钮，显示如图 3-41 所示“普通用户 的高级安全设置”对话框，可以查看可用于该对象的所有权限项目。

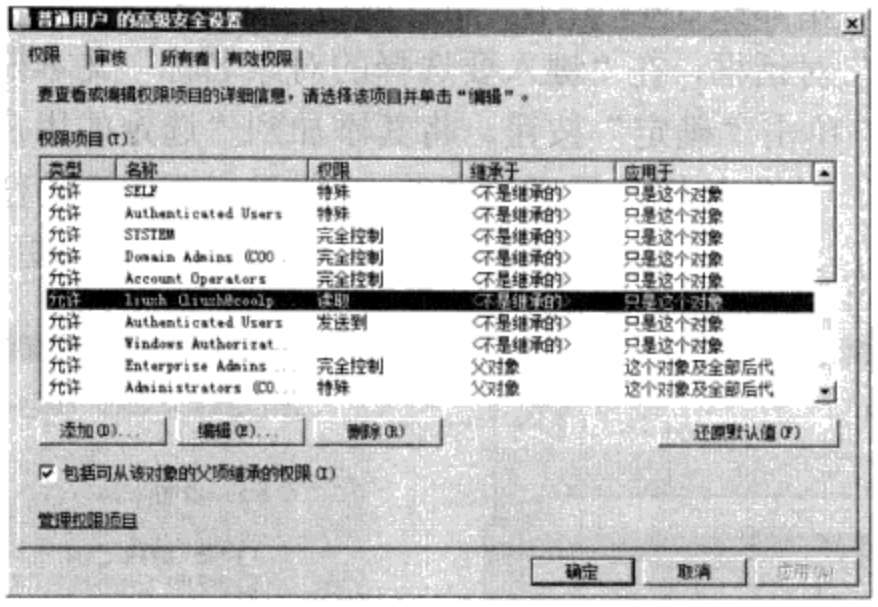


图 3-41 “普通用户 的高级安全设置”对话框

第 4 步，单击“添加”按钮，显示如图 3-42 所示“选择用户、计算机、或组”对话框，键入想要添加的组、计算机或用户的名称。

第 5 步，单击“确定”按钮，显示如图 3-43 所示“普通用户 的权限项目”对话框。此处需要委派的是针对用户账户安全管理的权限，如更改密码、重设密码等，所以需要在“应用于”下拉列表框中选择“后代 用户 对象”，并在“权限”列表中，选择“更改密码”和“重置密码”复选框。

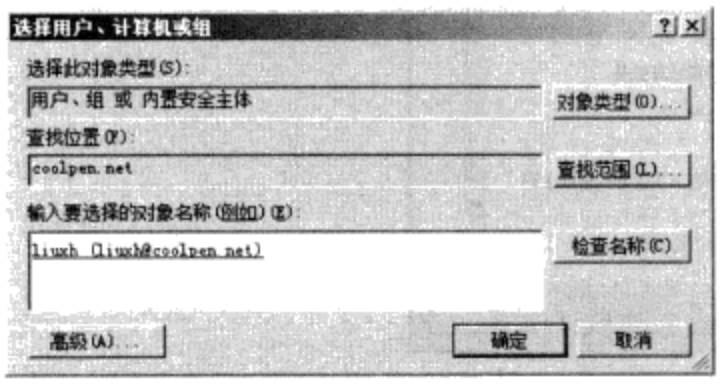


图 3-42 “选择用户、计算机、或组”对话框

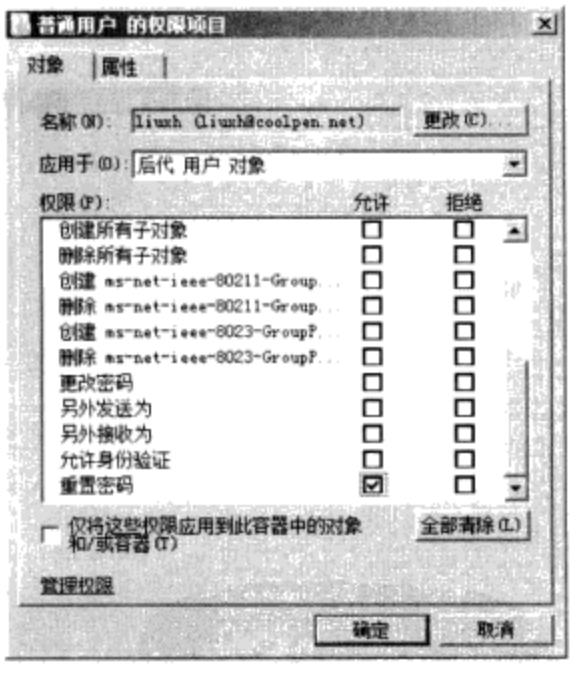


图 3-43 “普通用户 的权限项目”对话框

第 6 步，单击“确定”按钮，即可完成赋予用户对其后代账户的安全密码管理权限。如果需要设置其他的权限，根据需要设置相关的权限即可。切记，不要轻易赋予用户“完全控制”的权限。

3. 用户权限委派向导

权限委派向导是比较常用的权限委派方法之一。例如，同样将重置密码权限委派给 liuxh 用户账户，可以按照如下步骤操作：

第1步，打开“Active Directory 用户和计算机”窗口，右击需要委派管理权限对象所在的 OU（如“生产区”），选择快捷菜单中的“委派控制”选项，启动“控制委派向导”，直接单击“下一步”按钮，显示如图 3-44 所示“用户或组”对话框。单击“添加”按钮，显示“选择用户、计算机、或组”对话框，在“键入要选择的对象名称”文本框中输入接受权限的用户账户名称，如“liuxh”，单击“确定”按钮，将其添加到“选定的用户和组列表”中。

第2步，单击“下一步”按钮，显示如图 3-45 所示“要委派的任务”对话框。在“委派下列常见任务”列表中，选中“重置用户密码并强制在下次登录时更改密码”复选框。

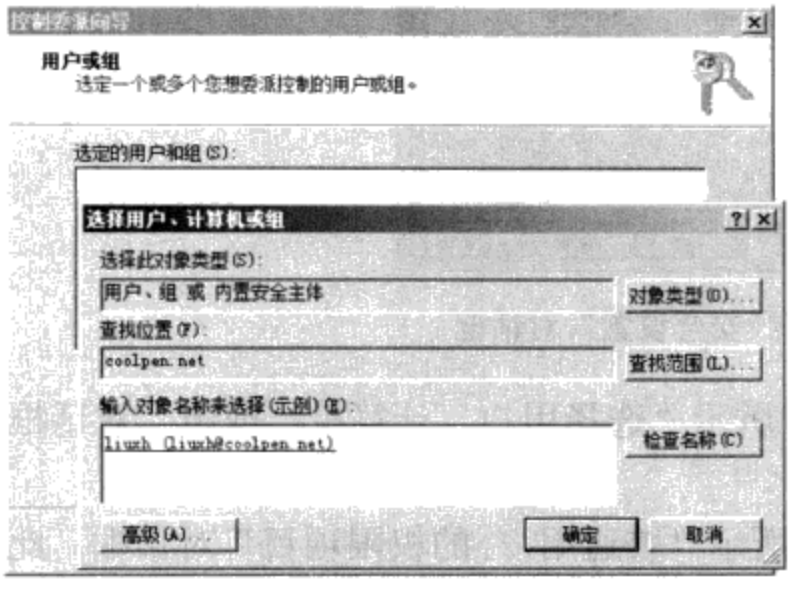


图 3-44 “用户或组”对话框

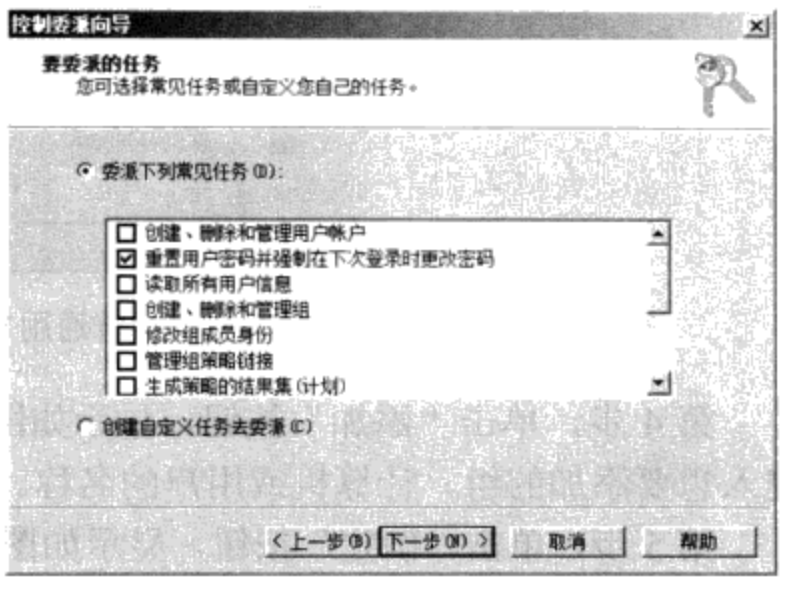


图 3-45 “要委派的任务”对话框

第3步，单击“下一步”按钮，显示如图 3-46 所示“完成控制委派向导”对话框，提示前面所设置的委派权限信息。

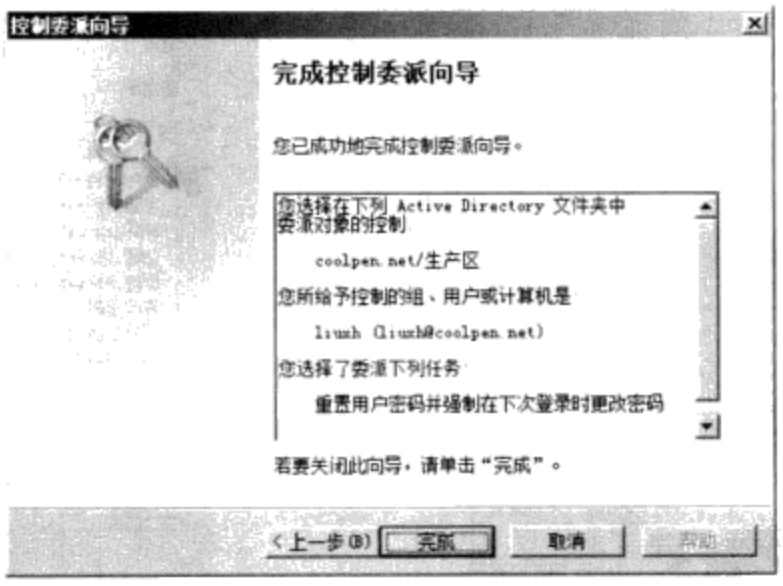


图 3-46 “完成控制委派向导”对话框

第4步，单击“完成”，即可完成委派任务操作。

4. 管理服务器测试

被委派管理权限的用户，可以通过登录管理服务器，或者已经安装管理工具的任意工作站上等用户账户，测试操作是否成功。例如，在管理服务器（Manager2008.coolpen.net）上登录 liuxh 用户账户，并重置“生产区”组织单位中的 test 账户的密码，显示如图 3-47 所示“重置密码”对话框，输入新的密码并单击“确定”按钮，即可保存设置。为 liuxh 用户账户委派

重置密码权限成功。

对于没有被委派到该用户账户的权限，则操作时将提示“访问特权不够，不能执行该操作。”的提示信息。例如，尝试禁用 test 用户账户，则显示如图 3-48 所示对话框。

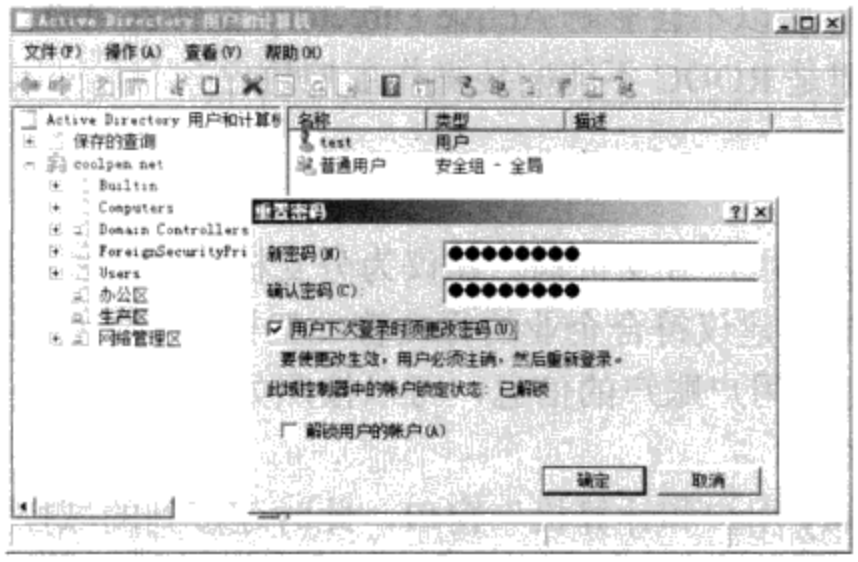


图 3-47 “重置密码”对话框

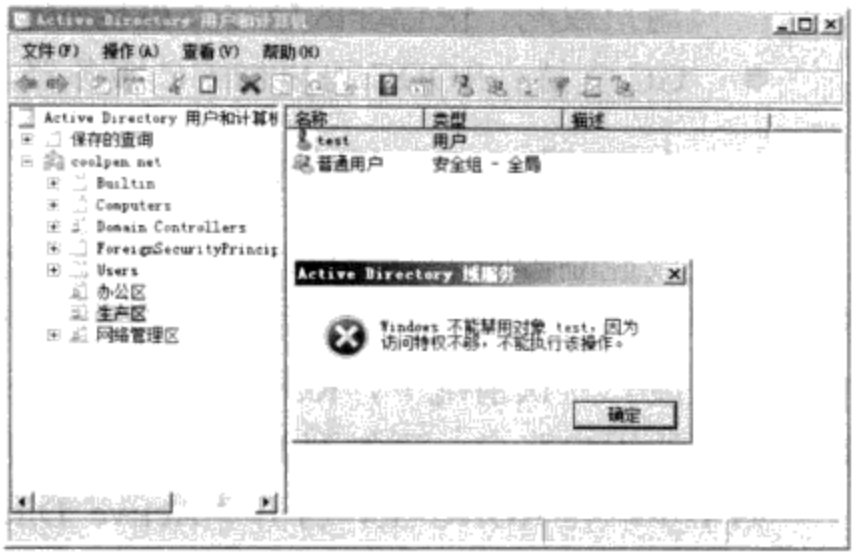


图 3-48 “Active Directory 域服务”对话框

3.1.6 部署只读域控制器

只读域控制器（RODC）是 Windows Server 2008 操作系统中的一种新型域控制器，在 Windows Server 2008 R2 系统中仍然保留。其主要功能有两点，一是缓存域控制器信息，便于无法连接到域控制器的用户进行身份验证；二是提高网络安全性。需要注意的是，RODC 只能配合 Windows Server 2008 或 Windows Server 2008 R2 的域控制器工作，无法独立运行，主要用于分支结构网络。

1. RODC 的优点

RODC 虽然是一个只读的域控制器，但本质上还是域控制器，具备域控制器的功能和优点，同时具有以下特点：

- 只读 Active Directory 数据库。RODC 上包含所有域对象和属性，与可读写域控制器不同的是，只能读取可读写域控制器中的数据，无法对 RODC 的 Active Directory 数据库进行更改。RODC 默认情况下，RODC 中不存储账户的密码。在不能保证域控制器安全性的情况下，可以通过 RODC 保证分支机构域安全性。
- 单向复制。可读写域控制器之间的复制是双向的，而 RODC 和可读写域控制器之间的复制是单向的，RODC 通过分布式文件系统（DFS）从可读写域控制器复制数据。
- 密码缓存。默认情况下，RODC 上只存储本地的计算机账户和一个用于 RODC 特殊的 Kerberos 票据授权（KRBTGT）账户，此账户被可读写域控制器用来验证 RODC 身份。在可读写域控制器上启用密码缓存功能，即可在 RODC 上缓存所有域用户账户。如果在 RODC 上启用密码缓存，只会影响缓存到本地计算机和用户账户。
- 只读 DNS。在 RODC 上可以安装 DNS 服务，RODC 可以复制 DNS 使用的所有应用程序目录分区中的数据，包括 ForestDNSZones 和 DomainDNSZones，支持客户端请求 RODC 进行名称解析。在 RODC 上的 DNS 不支持客户端直接更新 DNS 记录，因此 RODC 不会在其拥有的活动目录集成区域内注册任何 NS（Name Server）记录。

- RODC 管理。在可读写的域控制器中，本地管理员和域管理员，都可以管理域控制器。RODC 允许一个普通的域用户成为 RODC 的本地管理员，设置的域用户可以在 RODC 所在的区域执行管理任务，此用户在域中或者任何可读写的域控制器上没有用户权利，仅管理区域分支机构的权限，所以不会影响 Active Directory 整体安全性。
- GC 支持。RODC 可以做 GC 服务器，但是 RODC 不能安装操作主控角色。

2. 权限委派添加缓存账户

在主域控制器中，设置可以在 RODC 上缓存的用户分支机构。建议为分支机构创建单独的组织单位，在该组织单位下创建组，组的创建规则建议符合企业的行政管理架构，以降低管理的复杂度。默认情况下，RODC 并未保存所有域用户账户的信息，可以按照如下方法，将需要缓存的用户账户，添加到 RODC 的缓存策略中。

第 1 步，在 RODC 上，打开“Active Directory 用户和计算机”窗口，此时连接到的域控制器状态为“只读”。依次选择“coolpen.net”→“Domain Controllers”选项，双击“LIUXH-RODC”显示“LIUXH-RODC 属性”对话框，切换到如图 3-49 所示“密码复制策略”选项卡。

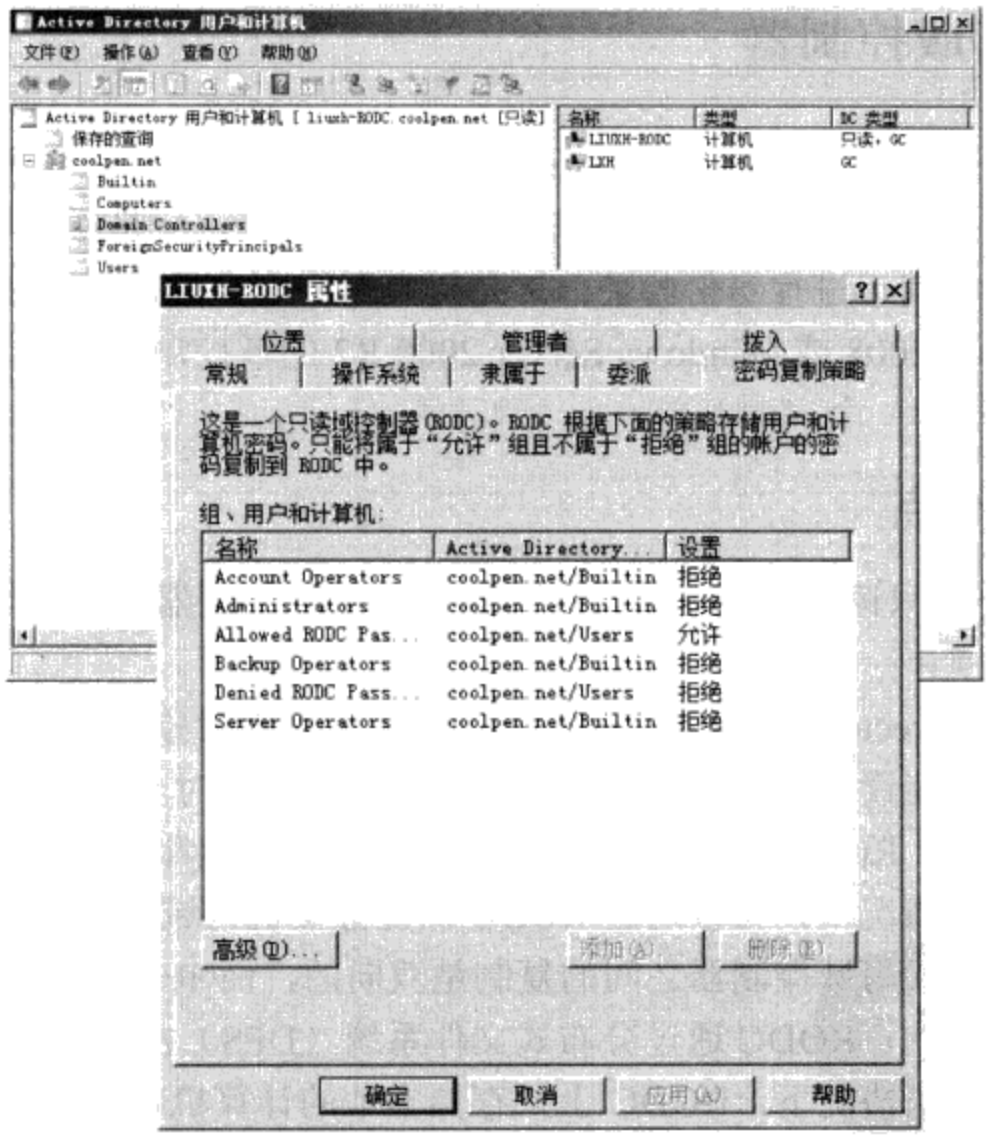


图 3-49 “密码复制策略”选项卡

第 2 步，单击“添加”按钮，显示“添加组、用户和计算机”对话框。设置 RODC 域控制器中允许或者拒绝缓存的组、用户和计算机，这里选择“允许该账户的密码复制到此 RODC 中”单选按钮。单击“确定”按钮，显示如图 3-50 所示“选择用户、计算机和组”对话框，在“输入对象名称来选择”文本框中，输入想要添加的域用户账户。

第 3 步，单击“确定”按钮，关闭“选择用户、计算机或组”对话框，返回到“LIUXH-RODC

属性”对话框，如图 3-51 所示，所选用户账户已被添加到列表中。

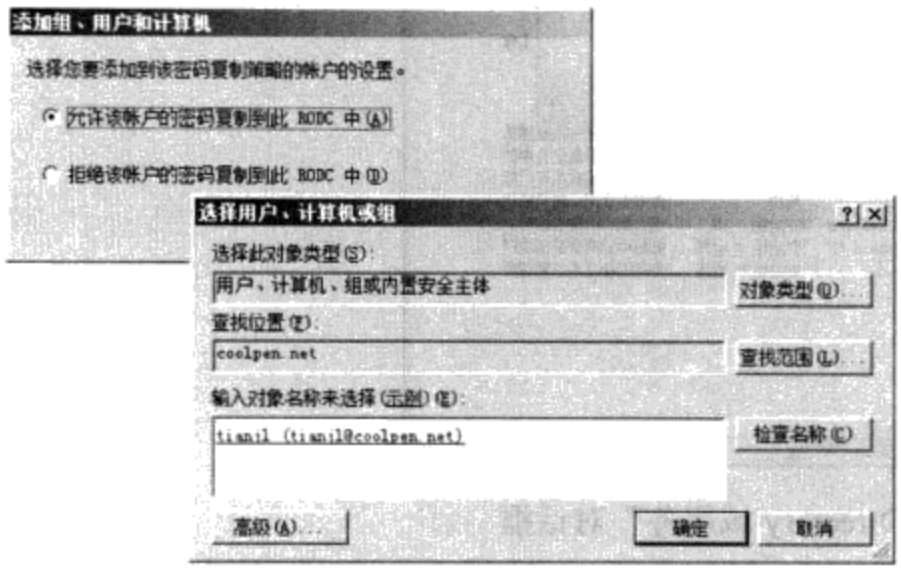


图 3-50 “选择用户、计算机和组”对话框

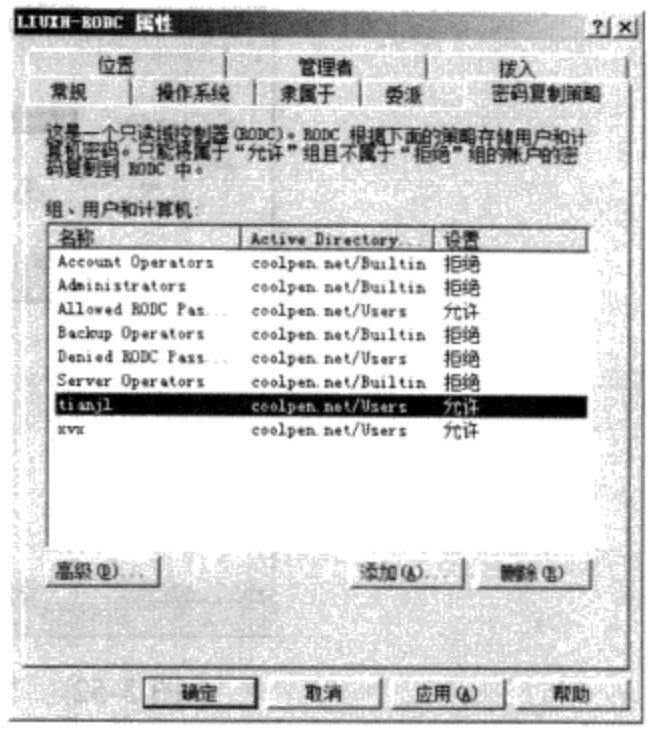


图 3-51 “LIUXH-RODC 属性”对话框

第 4 步，单击“应用”按钮，设置生效。

3.2 系统管理员账户安全

默认情况下，管理员账户是 Windows 系统中权限最高的账户，拥有管理员权限，也就相当于拥有了整个系统或网络。因此，管理员账户就成为黑客们的主要攻击目标。作为网络和计算机管理员，尤其应该做好管理员账户的安全管理，如更改账户名称、设置密码、创建陷阱账户等，避免被破解或盗取。

3.2.1 更改超级管理员账户

在 Windows Server 2008 R2 系统中，超级管理员账户的权限是至高无上的，因此管理员应加倍重视其安全性。系统默认的管理员账户名称是 Administrator，许多用户贪图一时方便，就直接使用系统管理员账户，因此，许多黑客攻击服务器时，总是试图破解 Administrator 账户的密码，如果此时密码安全性不高，后果不堪设想。通常情况下，可以通过更改管理员账户名称来避免此类攻击，提高系统安全性。

在“Active Directory 用户和计算机”窗口中，展开“Users”容器并右击 Administrator 账户，选择快捷菜单中的“重命名”选项，输入新的账户名并确认，显示如图 3-52 所示“Active Directory 域服务”对话框，建议更改之后立即注销并使用新的账户名登录，以避免出现访问冲突。单击“是”按钮，关闭该对话框，稍后注销当前用户账户即可。

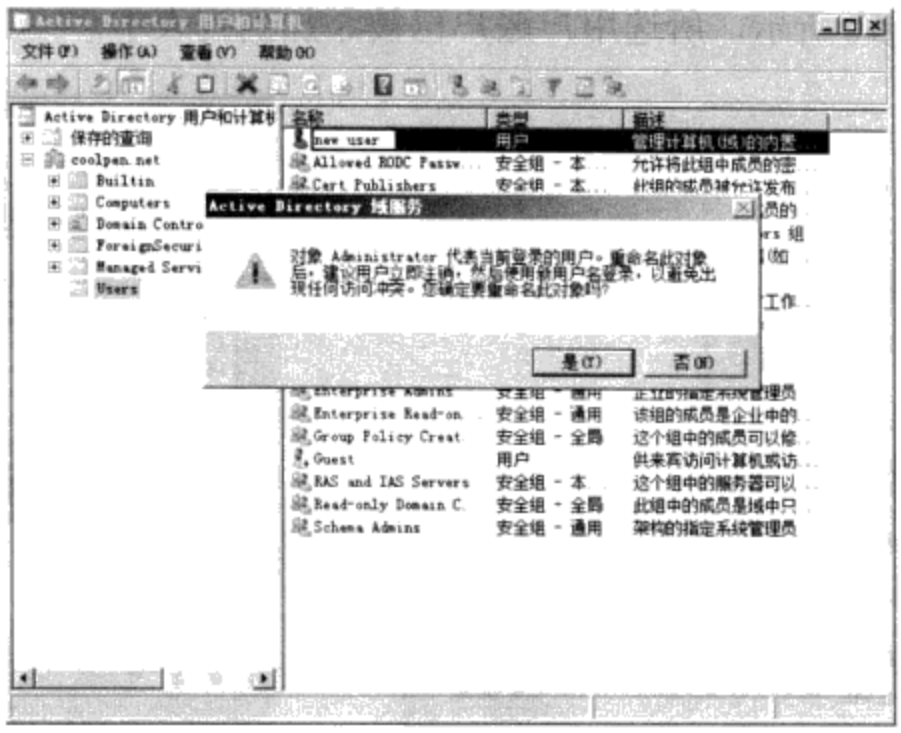


图 3-52 “Active Directory 域服务”对话框

3.2.2 禁用 Administrator 账户

如果更改账户名仍然无法达到安全需求，可以选择直接将其禁用，然后创建一个普通的管理员账户，用于实现基本的系统或者网络管理、维护功能。在“Active Directory 用户和计算机”的“Users”容器中，右击 Administrator 账户，选择快捷菜单中的“属性”命令，在打开的“Administrator 属性”对话框中切换到“账户”选项卡，在“账户选项”列表框中选中“账户已禁用”复选框即可，如图 3-53 所示。

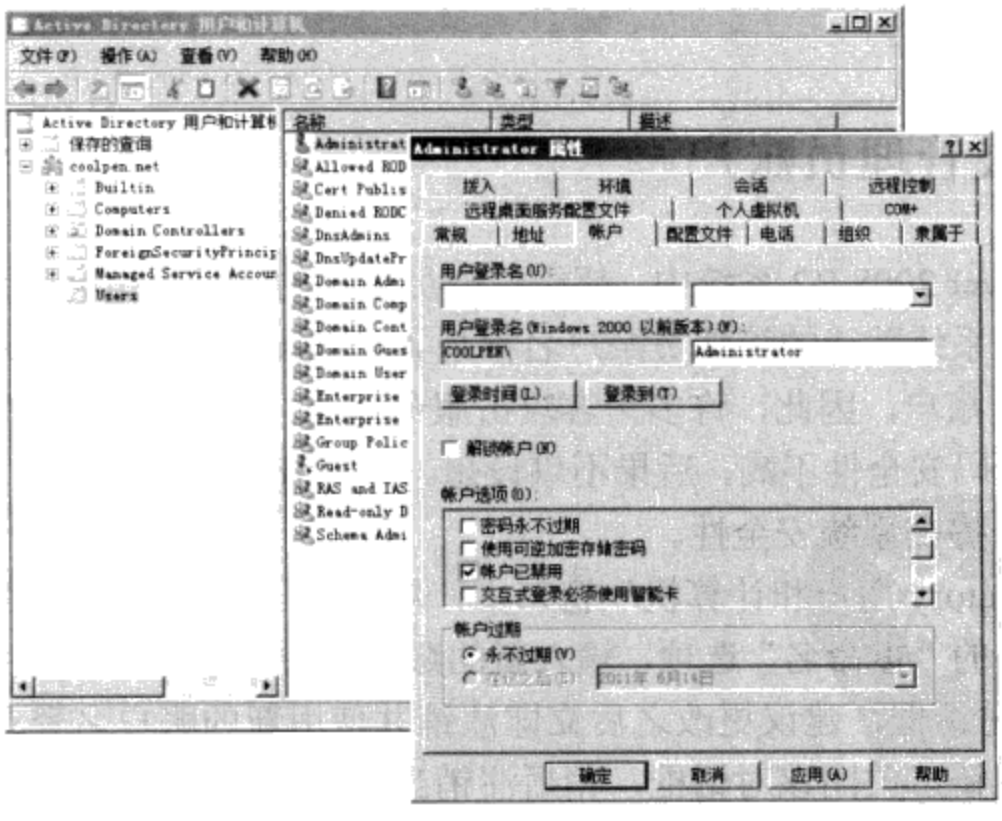


图 3-53 “Administrator 属性”对话框

禁用 Administrator 账户相对于为其更名而言，安全性更高。但是，当需要完成某些特殊管理任务而必须用到超级管理员账户时，必须先进入安全模式，重新启用该账户，如进行目录恢复和还原等。

提示 用户自定义的管理员，虽然同样属于某些系统管理员组，但却无法获得超级管理员的终极权限，功能方面仍有很大区别。

3.2.3 设置陷阱账户

所谓陷阱账户就是名称与默认管理员账户名称（Administrator）类似或完全相同，而权限却极低的用户账户。这种方法通常和“更改 Administrator 账户名称”配合使用，及将系统管理员账户更名后，再创建一个名称为 Administrator 的陷阱账户。最重要的是，一定要将陷阱账户的权限设置为最低。例如，在“拨入”选项卡中选择“拒绝访问”单选按钮，如图 3-54 所示。

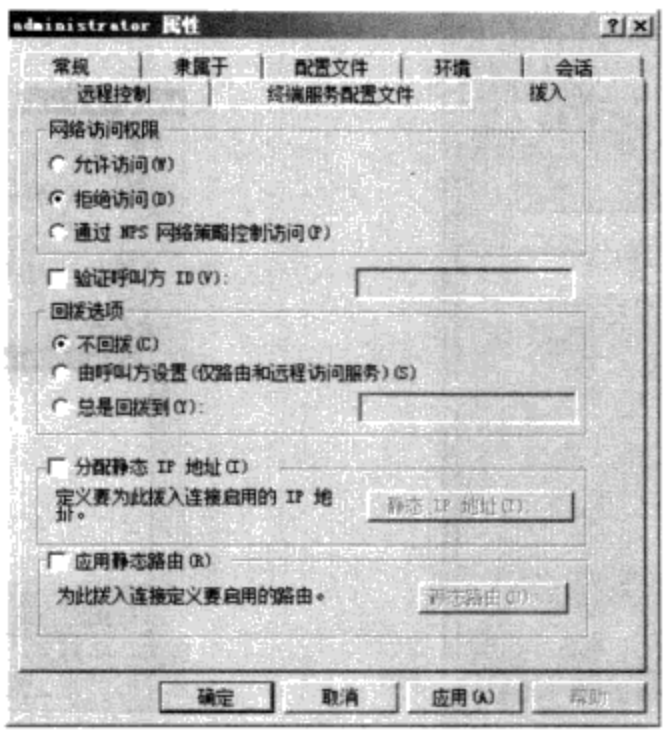


图 3-54 “拨入”选项卡

注意 除此之外，还可以在所有磁盘分区的 NTFS 权限列表框中一一删除陷阱账户的各种权限。总之，使其不具备任何操作权限，即使被盗用也无法进行任何破坏操作。

3.2.4 禁用 Guest 账户

Guest 账户是系统默认提供的来宾账户，主要是为了方便局域网中的陌生用户访问共享资源，在企业网络中通常为所有用户创建了对应的用户账户，如果继续启用 Guest 账户则可能成为系统安全的重大隐患，此时可以将其禁用。

在“计算机管理”窗口中，右击 Guest 用户账户，选择快捷菜单中的“属性”命令，显示如图 3-55 所示“Guest 属性”对话框，在“常规”选项卡中，选中“账户已禁用”复选框，单击“确定”按钮保存配置，即可禁用该用户账户。

3.2.5 减少管理员组成员

尽量减少管理员组成员的数量，也是最大限度保证网络安全的重要措施。由于管理员组成员拥有对系统的各种操作、配置和访问权限。因此，从某种意义上来讲，限制了管理员组的成员数量，也就限制了拥有较高权限的用户和密码管理的难度，减少易被识破的密码被用于系统密码的机会，从而避免使系统处于危险的境地。

对于独立计算机而言，可以在“计算机管理”→“本地用户和组”→“组”中，双击Administrators 打开如图 3-56 所示“Administrators 属性”对话框，选择“成员”列表框中想要删除的管理员账户，并单击“删除”按钮即可。如果是域控制器，则除减少 Administrators 组中的成员之外，还应严格控制添加到 DnsAdmins 组和 Enterprise Admins 组中的成员账户，这些组同样是 Administrators 组中的成员。

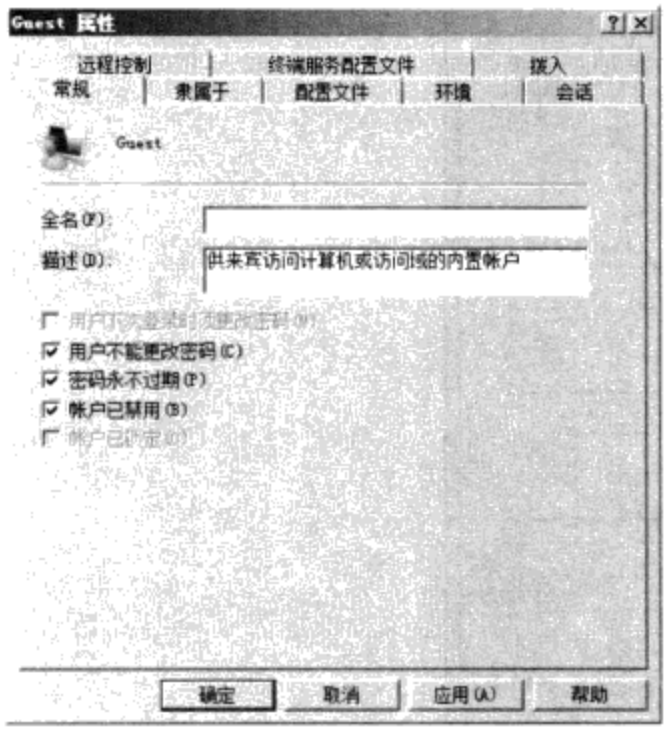


图 3-55 “Guest 属性”对话框

图 3-56 “Administrators 属性”对话框

系统管理员的数量越少，密码丢失或被猜到的可能性就越小，相对而言，系统也就越安全。因此，除非必要，否则不要将技术水平不高的用户添加为管理员组成员。

3.2.6 系统管理员口令设置

入侵者若想盗取系统内的重要数据信息或执行某项管理功能，就必须先获得管理员权限，即破解管理员账户密码。密码破解软件工作机制主要包括 3 种：巧妙猜测、词典攻击和自动尝试字符组合。从理论上讲，只要有足够时间，使用这些方法可以破解任何账户密码，破解一个弱密码可能只需几秒钟即可完成，而要破解一个安全性较高的强密码则可能需要几个月甚至几年的时间。因此，系统管理员账户必须使用强密码，并且经常更改密码。

1. 注意事项

在设置管理员账户密码时，应注意以下问题。

- 切忌账号与密码相同。如果将用户账号与密码设置为相同，许多系统扫描工具默认将

账户和密码作为相同的设置扫描系统，无疑会省去攻击者的很多力气。

- 切忌使用自己的姓名。使用自己的姓或名、甚至是姓名作为密码，实在是不堪一击，对于本单位和熟悉本单位的人来讲，姓名无疑是攻击的首选，因为这几乎谁都能猜得到。另外，在许多黑客编写的字典中，往往将百家姓一一列出，放在字典的前列。
- 切忌使用英文词组。一些常用或别致的英文单词往往是用户设置密码时的最爱，在他们看来，这类密码既便于记忆，又凸显自己的个性。但事实上，那些绝顶聪明的黑客们也早已猜到并详细地将其编入字典，因此，英文词组绝不可用。
- 切忌使用特定意义的日期。以具有特定意义的日期作为密码是任何人都十分喜爱的，这一类日期通常有自己生日、父母生日、儿女生日、朋友生日、重大节日、个人纪念日等等。不用说熟悉的人可以猜得到，即使是陌生人也可以通过穷举的方式而得手。在黑客字典中，几乎全部罗列以上所有的几个组合，实在令人惊骇不已。
- 切忌使用简单密码。越是字符数少、越是简单的密码，在破解时所用的时间也就越短。一个以穷举软件每秒钟可以重试 10 万次之多，字数越少，字符越简单化，排列组合的结果也就越少，也就越容易被攻破。

2. 安全密码原则

若欲保证账户密码的安全，应当遵循以下规则：

- 用户密码应包含英文字母的大小写、数字、可打印字符，甚至是非打印字符，将这些符号排列组合使用，以期达到最好的保密效果。
- 用户密码不要太规则，不要将用户姓名、生日和电话号码作为密码。不要用常用单词作为密码。
- 根据黑客软件的工作原理，参照密码破译的难易程度，以破解需要的时间为排序指标，密码长度设置时应遵循 7 位或 14 位的整数倍原则。
- 在通过网络验证密码过程中，不得以明文方式传输，以免被监听截取。
- 密码不得以明文方式存放在系统中，确保密码以加密的形式写在硬盘上并包含密码的文件是只读的。加密的方法很多，如基于单向函数的密码加密，基于测试模式的密码加密，基于公钥加密方案的密码加密，基于平方剩余的密码加密，基于多项式共享的密码加密，基于数字签名方案的密码加密等。经过上述方法加密的密码，即使是系统管理员也难以得到。
- 密码应定期修改，应避免重复使用旧密码，应采用多套密码的命名规则。
- 建立账号锁定机制。一旦同一账号密码校验错误若干次即断开连接并锁定该账号，经过一段时间才解锁。
- 由网络管理员设置一次性密码机制，用户在下次登录时必须更换新的密码。

3. 系统账户密码要求

在 Windows Server 2008 R2 系统中，安装系统的同时就要求管理员必须指定符合要求的安全密码，大大提高了用户账户和系统的安全性。通常情况下，Windows Server 2008 R2 网络中，对用户账户密码要求如下：

- 不包含全部或部分的用户账户名。
- 长度至少为 6 个字符。

- 包含来自以下4个类别中的3个的字符：
  - 大写英文字母（从 A 到 Z）。
  - 小写英文字母（从 a 到 z）。
  - 10个基本数字（从 0 到 9）。
  - 非字母字符（例如，!、$、#、%）。

对于未安装 Active Directory 服务 Windows Server 2003 计算机或修改了 Windows Server 203/2008 默认组策略的计算机，其用户账户密码可以随意设置。

强密码具有以下特征：

- 长度至少有7个字符。
- 不包含用户的生日、电话、用户名、真实姓名或公司名等。
- 不包含完整的词典词汇。
- 包含全部下列 4 组字符类型。大写字母（A,B,C...）、小写字母（a,b,c...）、数字（从0~9）、非字母字符（键盘上所有未定义为字母和数字的字符，如` ~ ! @ # $ % ^ & * ( ) _ + - = { } | [ ] \ : " ; ' < > ? , . / ）。

除此之外，管理员账户的密码应当定期修改，尤其是当发现有不良攻击时，更应及时修改复杂密码，以避免被破解。为避免密码因过于复杂而忘记，可用笔记录下来，并保存在安全的地方，或随身携带避免丢失。其实，最安全的方法就是不使用常规密码，而采用电子密钥等一些几乎无法破解的登录方式，确保系统安全性。

3.3 用户账户安全

网络中的每个用户都有一个与之身份对应的账户，如管理员维护计算机或网络时，通常会用到 Administrator 或其他被赋予管理权限的账户。除管理员账户之外，还应为其他用户创建一些普通账户，如来宾账户、其他个人用户账户等。为了确保系统或网络的安全，普通用户账户的安全设置也是不可小视的。

3.3.1 重设用户密码与密码使用期限

在域中，普通用户账户是无法重设自己密码的，只能由网络管理员或被赋予相关权限的用户账户完成。为了确保用户账户的安全，仅有足够强度的密码是不够的，理论上没有绝对的安全，因此应避免长时间使用一个密码。建议养成按时更改密码的习惯，例如可以每隔10天或30天更改一次。

1. 重设用户密码

以 Administrator 账户或拥有管理员权限的账户登录系统，或远程连接到域控制器，打开“Active Directory 用户和计算机”窗口。在“Users”容器中，右击想要重置密码的用户账户，并选择快捷菜单中“重置密码”选项，显示如图 3-57 所示“重置密码”对话框，在“新密码”和“确认密码”编辑框中输入新密码，单击“确定”按钮

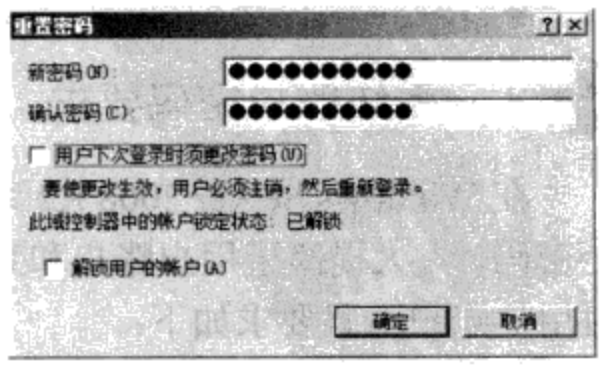


图 3-57 “重置密码”对话框

即可。

> **提示** 如果当前账户已被锁定，则可以选中“解锁用户的账户”复选框，使密码更改立即生效。由于系统配置的安全策略，可能会限制用户更改密码的次数或登录次数限制，如果超出策略限制，则立即锁定账户，并等待一定时间后自动解锁。此时，被锁定账户可以告知管理员，管理员可以登录到域控制器，通过这种方式更改密码和解锁账户。

2. 配置密码使用期限

管理员可以通过组策略配置与用户账户密码的使用期限。在域控制器上打开“组策略”管理窗口，新建一个关联到用户账户所在 OU 的组策略并编辑。在“组策略管理编辑器”窗口中，依次展开“计算机配置”→“策略”→“Windows 设置”→“安全设置”→“账户策略”→“密码策略”选项，双击“密码最长使用期限”策略打开如图 3-58 所示“密码最长使用期限 属性”对话框，选中“定义此策略设置”复选框，然后设置适当的天数即可。密码使用期限值的选择范围为 1~999 天之间，或将天数设置为 0，表示密码永不过期。

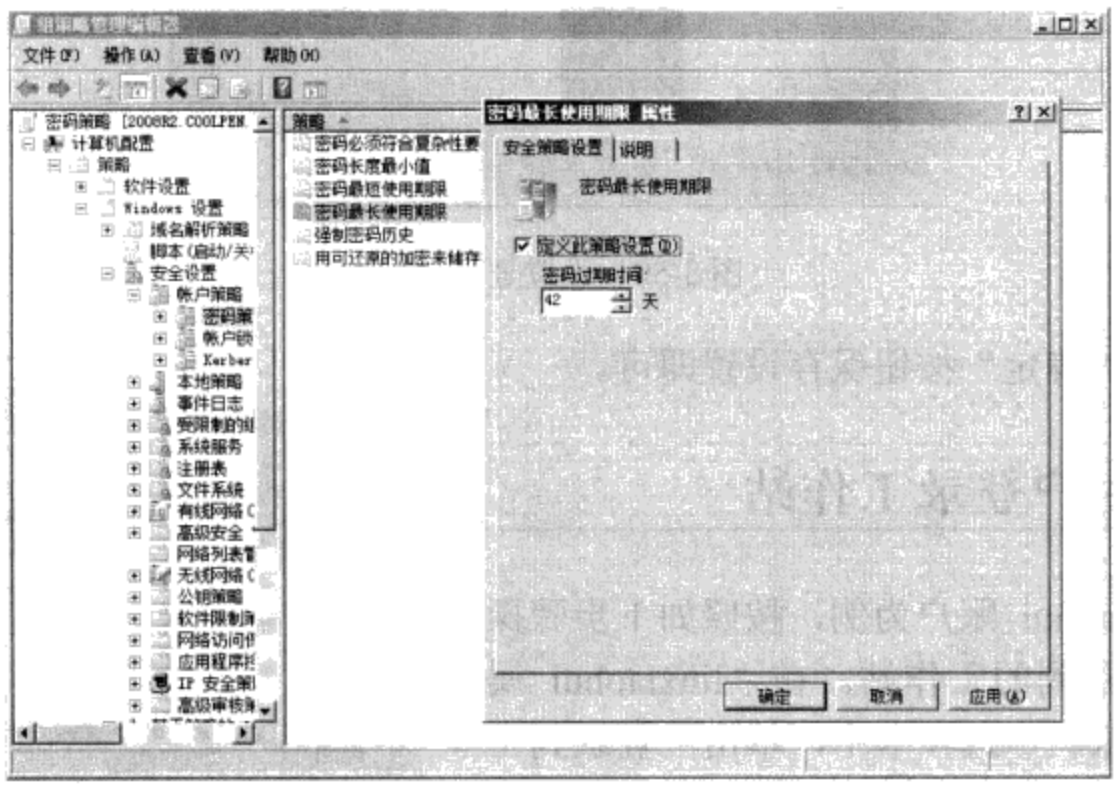


图 3-58 “密码最长使用期限 属性”对话框

> **提示** 启用此策略后，攻击者只能够在有限的时间内破解用户密码并访问的网络资源。建议对网络中的敏感用户密码最长使用期限设为 7 天。

3.3.2 限制用户登录时间

默认情况下，Windows 域中的中的常规用户账户允许登录网络中的所有计算机，并且不受时间限制。为了网络安全起见，可限制用户账户可以登录的工作站，使该用户只能在固定的

某台工作站上登录。

在“Active Directory 用户和计算机”窗口中，双击要设置的用户，打开用户属性对话框，切换到“账户”选项卡，单击“登录时间”按钮，显示“liuxiaohui 的登录时间”对话框，默认允许在任何时间登录。在登录时间分布表中，框选所有拒绝登录的时间，并选择“拒绝登录”单选按钮，如图 3-59 所示。例如，本例中设置的是 liuxiaohui 账户在每周星期一到星期五的 9 点至 17 点范围内登录。

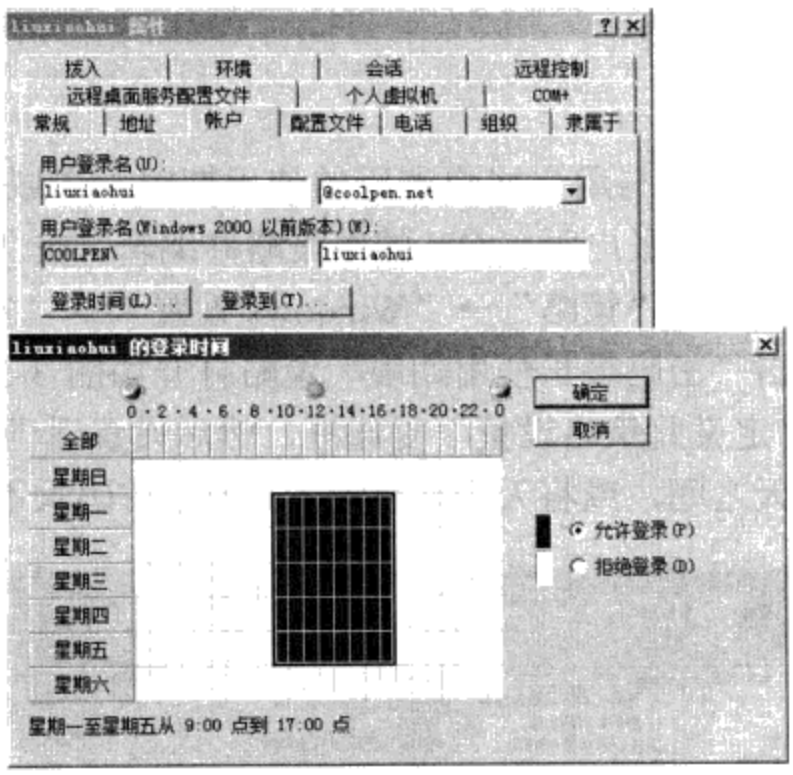


图 3-59　设置登录时间

最后，单击“确定”按钮保存设置即可。

3.3.3 限制用户登录工作站

仍然以 liuxiaohui 账户为例，按照如下步骤操作即可限制其登录到的工作站。在“liuxiaohui 属性”对话框的“账户”选项卡中，单击“登录到”按钮，显示如图 3-60 所示“登录工作站”对话框。默认选中“所有计算机”单选按钮，即允许用户登录网络中的所有计算机。

选择“下列计算机”单选按钮，并在“计算机名称”文本框中输入允许登录的工作站的 NetBIOS 名称。单击“添加”按钮添加到列表框中，可以添加多个允许登录的工作站。最后，单击“确定”按钮保存设置即可。

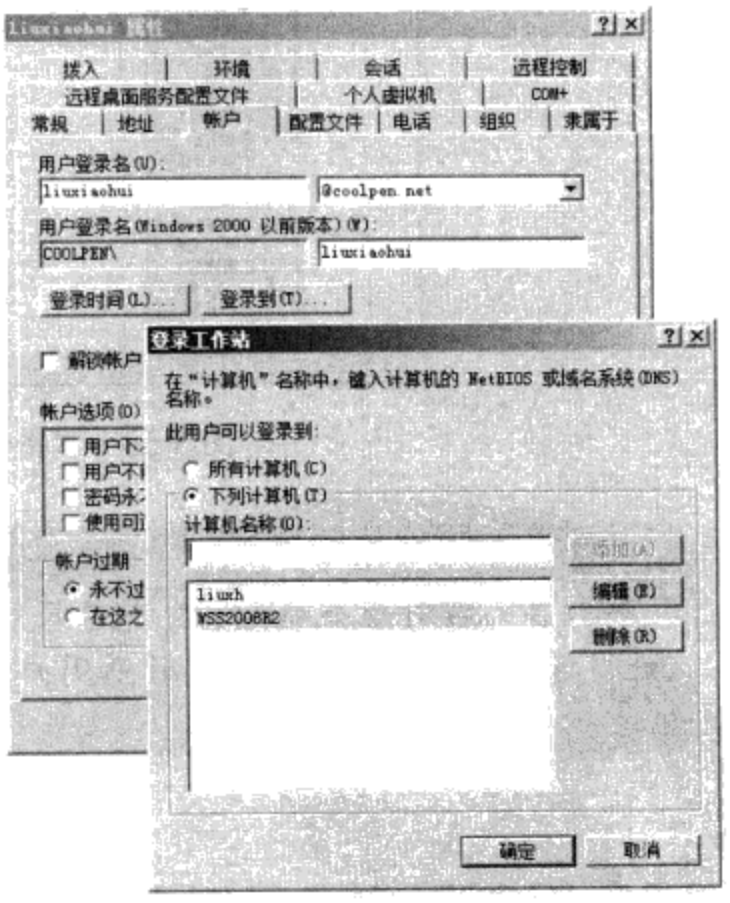


图 3-60　“登录工作站”对话框

3.3.4 用户账户策略

用户账户策略是组策略安全的一部分，主要包括账户密码策略和账户锁定策略。密码策

略用于确定密码设置（如强制执行和有效期限）。账户锁定策略确定某个账户被锁定在系统之外的情况和时间长短。

1. 密码策略

提高密码的破解难度主要是通过采用提高密码复杂性、增大密码长度、提高更换频率等措施来实现，但普通用户很难做到，对于企业网络中的一些敏感用户就必须采取一些相关的措施，以强制改变不安全密码的使用习惯。

密码策略包含以下 6 个策略。

- 密码必须符合复杂性要求。
- 密码长度最小值。
- 密码最长使用期限。
- 密码最短使用期限。
- 强制密码历史。
- 用可还原的加密来存储密码。

前面介绍的“配置密码使用期限”就是“密码策略”中的策略之一，其他策略的配置过程与之类似，此处不再赘述。

2. 账户锁定策略

账户锁定是指在某些情况下（账户受到采用密码词典或暴力破解方式的在线自动登录攻击等），为保护该账户的安全而将此账户进行锁定，使其在一定时间内不能再次使用此账户，从而挫败连续的猜解尝试。

Windows Server 2008 R2 系统在默认情况下，为方便用户起见，这种锁定策略并没有进行设置。因此对黑客的攻击没有任何限制。只要有耐心，通过自动登录工具和密码猜解字典进行攻击，甚至可以进行暴力模式攻击，破解密码只是一个时间和运气上的问题。账户锁定策略用于域账户或本地用户账户，用来确定某个账户被系统锁定的情况和时间长短。账户锁定策略包含以下 3 个策略。

- 复位账户锁定计数器。
- 账户锁定时间。
- 账户锁定阈值。

账户锁定策略设置的第一步就是指定账户锁定的阈值，即锁定前该账户无效登录的次数。一般来说，由于操作失误造成的登录失败的次数是有限的。在这里设置锁定阈值为 3 次（如图 3-61 所示），这样只允许 3 次登录尝试。如果 3 次登录全部失败，就会锁定该账户。

一旦该账户被锁定后，即使是合法用户也就无法使用了。只有管理员才可以重新启用该账户，这就造成了许多不便。为方便用户起见，可以同时设置锁定的时间和复位计数器的时间，这样以来在 3 次无效登录后就开始锁定账户，以及锁定时间为 30 分钟为限。以上的账户锁定设置，可以有效地避免自动猜解工具的攻击，同时对于手动尝试者的耐心和信心也可造成很大的打击。锁定用户账户常常会造成一些不便，但系统的安全有时更为重要。

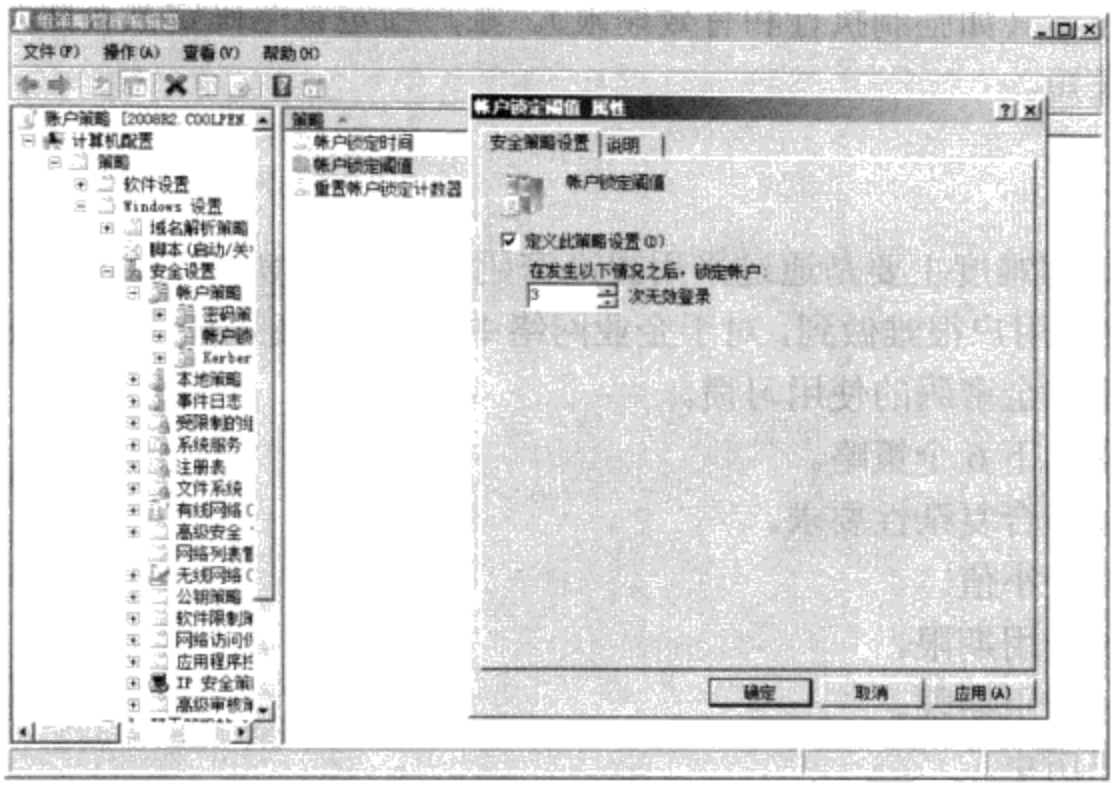


图 3-61　设置账户锁定阈值

3.3.5　审核策略

审核策略是 Windows Server 2008 R2 系统用户账户安全管理的一部分，其主要功能就是记录和审查域用户账户在什么时刻访问了哪些资源以及进行了哪些操作，即跟踪用户活动和系统活动。通过设置审核策略，确定是否将安全事件记录到计算机上的安全日志，同时也确定是否记录登录成功或登录失败，或二者都记录。

1.　审核策略的类别

执行审核策略前，必须决定要审核的事件类别。为事件类别选择的审核设置将定义审核策略。在加入域中的成员服务器和工作站上，默认情况下未定义事件类别的审核设置。在域控制器上，默认情况下审核关闭。通过为特定的事件类别定义审核设置，可以创建一个适合组织安全需要的审核策略。

（1）　审核策略更改

审核策略更改设置确定是否审核用户权限分配策略、审核策略或信任策略更改的每一个事件。

如果定义该策略设置，可以指定是否审核成功、审核失败，或根本不对该事件类型进行审核。对用户权限分配策略、审核策略或信任策略所作更改成功时，成功审核会生成审核项。对用户权限分配策略、审核策略或信任策略所作更改失败时，失败审核会生成审核项。

（2）　审核登录事件

审核登录事件设置确定是否审核每一个登录或注销计算机的用户实例。

在域控制器上将生成域账户活动的账户登录事件，并在本地计算机上生成本地账户活动的账户登录事件。如果同时启用账户登录和账户审核策略类别，那么使用域账户的登录将生成登录或注销工作站或服务器的事件，而且将在域控制器上生成一个账户登录事件。此外，在用户登录而检索登录脚本和策略时，使用域账户的成员服务器或工作站的交互式登录将在域控制

器上生成登录事件。

如果定义该策略设置，可以指定是否审核成功、审核失败，或根本不对事件类型进行审核。登录成功时，成功审核会生成审核项。登录失败时，失败审核会生成审核项。

（3） 审核对象访问

审核对象访问设置确定是否审核用户访问某个对象的事件，例如文件、文件夹、注册表项、打印机等，它们都有自己特定的系统访问控制列表（SACL）。

如果定义该策略设置，可以指定是否审核成功、审核失败，或根本不对该事件类型进行审核。当用户成功访问指定了合适 SACL 的对象时，成功审核将生成审核项。当用户访问指定有 SACL 的对象失败时，失败审核会生成审核项。

（4） 审核过程跟踪

审核过程跟踪设置确定是否审核事件（例如程序激活、进程退出、句柄复制和间接对象访问等）的详细跟踪信息。

如果定义该策略设置，可以指定是否审核成功、审核失败，或根本不对该事件类型进行审核。所跟踪的过程成功时，成功审核会生成审核项。所跟踪的过程失败时，失败审核会生成审核项。

（5） 审核目录服务访问

审核目录服务访问设置确定是否审核用户访问那些指定自己的系统访问控制列表（SACL）的 Active Directory 对象的事件。

默认情况下，在“默认域控制器组策略对象（GPO）”中该值设置为无审核，并且在该值没有任何意义的工作站和服务器中，它保持未定义状态。

如果定义该策略设置，可以指定是否审核成功、审核失败，或根本不对事件类型进行审核。用户成功访问指定了 SACL 的 Active Directory 对象时，成功审核会生成审核项。用户尝试访问指定了 SACL 的 Active Directory 对象失败时，失败审核会生成审核项。

注意 通过使用某个 Active Directory 对象“属性”对话框中的“安全”选项卡，可以设置该对象的SACL。该操作与审核对象访问相同，只不过它仅应用于 Active Directory 对象而不是文件系统和注册表对象。

（6） 审核特权使用

审核特权使用设置确定是否审核用户实施其用户权利的每一个实例。

如果定义该策略设置，可以指定是否审核成功、审核失败，或根本不对这种事件类型进行审核。用户权利实施成功时，成功审核会生成审核项。用户权利实施失败时，失败审核会生成审核项。

（7） 审核系统事件

当用户重新启动或关闭计算机时或者对系统安全或安全日志有影响的事件发生时，安全设置确定是否予以审核。

如果定义该策略设置，可以指定是否审核成功、审核失败，或根本不对该事件类型进行审核。系统事件执行成功时，成功审核会生成审核项。系统事件执行失败时，失败审核会生成审核项。

（8） 审核账户登录事件

审核账户登录事件设置确定是否审核在这台计算机用于验证账户时，用户登录到其他计算机或者从其他计算机注销的每个实例。当在域控制器上对域用户账户进行身份验证时，将产生账户登录事件。该事件记录在域控制器的安全日志中。当在本地计算机上对本地用户进行身份验证时，将产生登录事件。该事件记录在本地安全日志中，不产生账户注销事件。

如果定义该策略设置，可以指定是否审核成功、审核失败，或根本不对事件类型进行审核。当某个账户的登录成功时，成功审核会生成审核项。当某个账户的登录失败时，失败审核会生成审核项。

（9） 审核账户管理

审核账户管理设置确定是否审核计算机上的每一个账户管理事件。账户管理事件的例子包括：

- 创建、更改或删除用户账户或组。
- 重命名、禁用或启用用户账户。
- 设置或更改密码。

如果定义该策略设置，可以指定是否审核成功、审核失败，或根本不对事件类型进行审核。任何账户管理事件成功时，成功审核都会生成审核项。任何账户管理事件失败时，失败审核都会生成审核项。

2. 配置审核策略

此处以配置“审核策略更改”策略为例，介绍 Windows Server 2008 R2 审核策略的配置。

第 1 步，打开“组策略管理编辑器”控制台，依次展开“计算机配置”→“Windows 设置”→“安全设置”→“本地策略”→“审核策略”选项，在右侧窗口中可以查看系统默认的所有策略。双击“审核策略更改”策略，在“审核策略更改 属性”对话框中如图 3-61 所示，同时选中“成功”和“失败”复选框，系统即可同时记录所有“成功”和“失败”的策略更改事件。

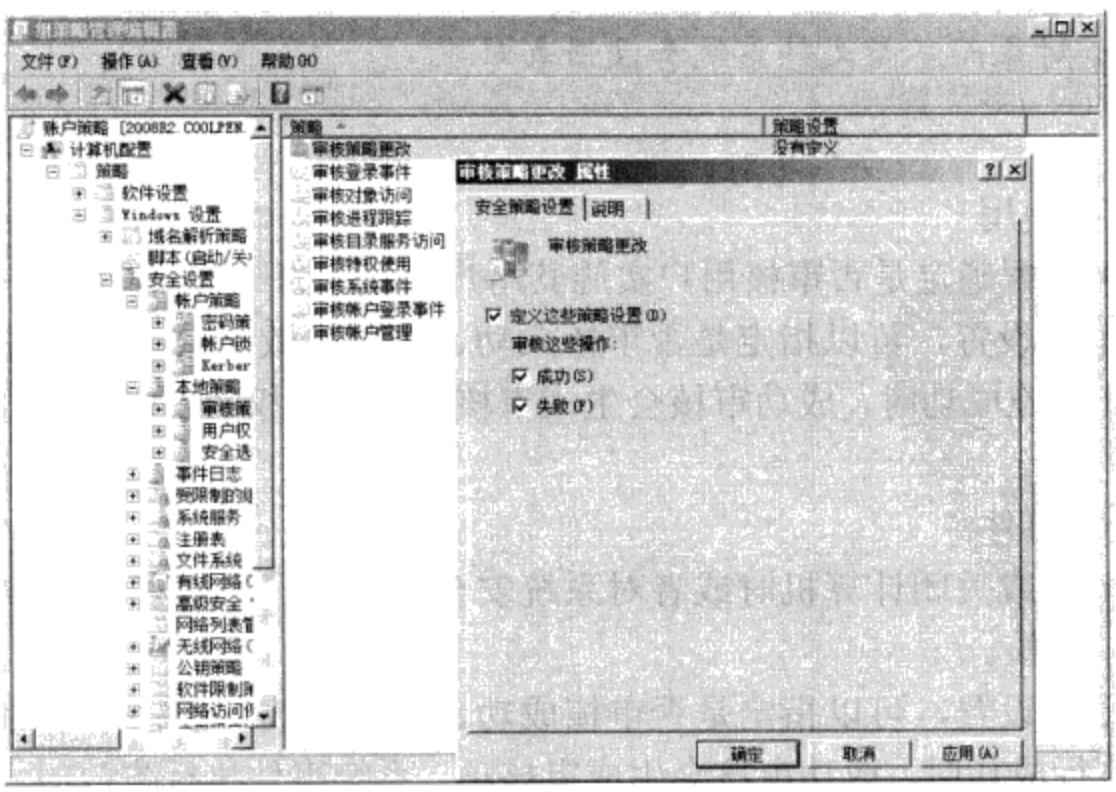


图 3-62　“审核策略”窗口

第 2 步，单击“确定”按钮，保存设置即可。配置其他审核策略的操作步骤与之完全相同，此处不复赘述。

3. 推荐的审核策略设置

推荐的审核策略配置目标为：

- 审核策略更改：成功+失败。
- 审核登录事件：成功+失败。
- 审核访问对象：失败。
- 审核目录服务访问：失败。
- 审核特权使用：失败。
- 审核系统事件：成功+失败。
- 审核账户登录事件：成功+失败。
- 审核账户管理：成功+失败。

4. 调整日志审核文件的大小

配置和启用审核策略后，系统将自动对指定事件进行审核和记录，默认情况下这些事件记录保存在 Windows 事件查看器指定的目录（%SystemRoot%\System32\Winevt\Logs\）下。在安装 Windows Server 2008 R2 系统时，系统默认的日志大小限制可能无法满足存储要求，必要时管理员可以适当调整其上限值。推荐的日志空间大小为：

- 应用程序日志，默认 20 MB，推荐设置为即 128 MB。
- 安全日志，默认 128 MB，推荐设置为 1000 MB。
- Setup 日志，默认 1 MB，推荐设置为 20 MB。
- 系统日志，默认 20 MB，推荐设置为 128 MB。
- 转发事件日志，默认 20 MB，依据被收集日志的服务器情况而定，该值只能在配置转发事件之后才能修改。

这里以“安全”日志审核文件为例，介绍如何调整 Windows 日志文件存储空间上限值。

第 1 步，在“事件查看器”窗口中，右击“安全”并选择快捷菜单中的“属性”选项，显示如图 3-63 所示“日志属性 – 安全”对话框。在“日志最大大小”文本框中，输入 1024000，即 1000 MB，并选择“日志满时将其存档，不覆盖事件”单选按钮，以免丢失旧的事件日志。

第 2 步，单击“确定”按钮，即可完成日志文件大小的修改。使用相同的方法即可更改其他类型日志审核文件大

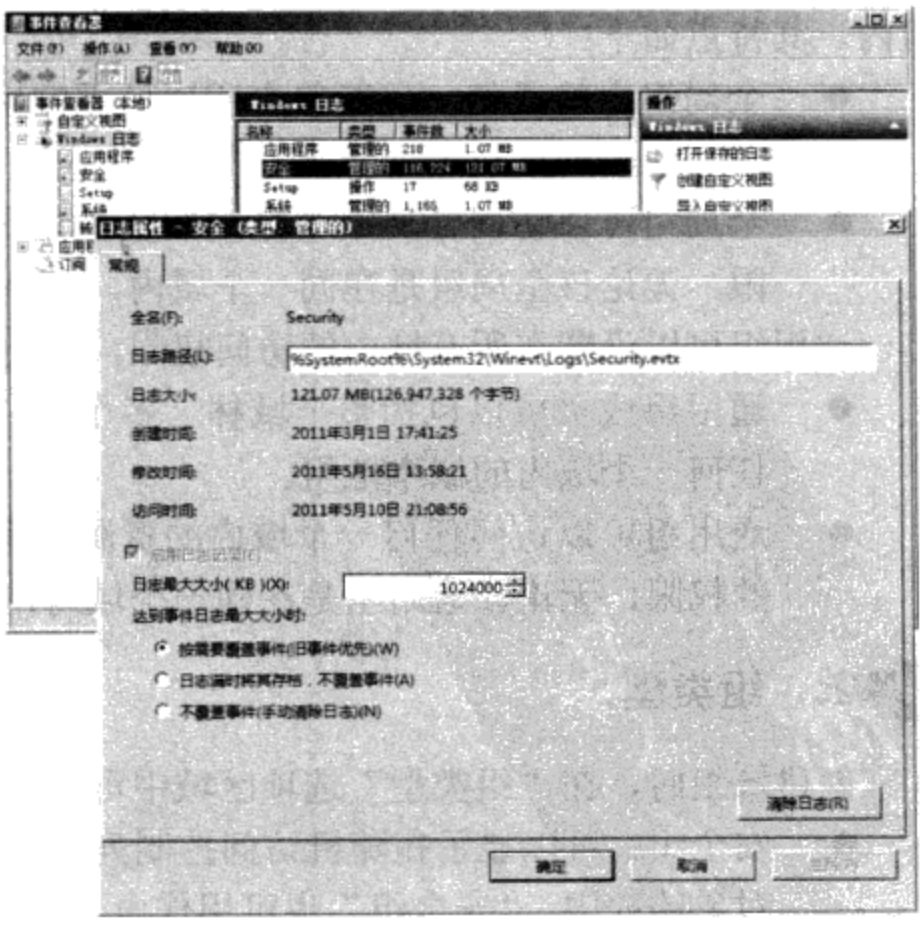


图 3-63 “日志属性 – 安全”对话框

小的最大值。

注意 日志文件的大小必须是 64 KB 的整数倍。

3.3.6 用户组安全

组是系统管理和网络管理中的常用功能之一。本地计算机中的组通常只用于管理本地计算机上的用户账户或组，不支持任何安全设置。而 Windows 域中的组，则可以帮助管理员统一设置某些对象的权限，简化操作的复杂性，降低管理难度。

1. 组作用域

在“组作用域”选项区域中可选择组的作用域，即该组可以在网络上的哪些地方使用。Windows 域中的组作用域包括 3 种：本地域、全局和通用。

本地域组主要用于指定其所属域内的访问权限，以便访问该域内的资源。对于只拥有一个域的企业而言，建议选择“本地域组”。其特征如下：

- 本地域组内的成员可以是任何一个域内的用户、通用组与全局组，也可以是同一个域内的域本地组，但不能是其他域内的域本地组。
- 域本地组只能访问同一个域内的资源，无法访问其他不同域内的资源。换言之，当在某台计算机上设置权限时，可以设置同一域内的域本地组的权限，但是，无法设置其他域内的域本地组的权限。

全局组主要用于组织用户，即可以将多个被赋予相同权限的用户账户加入到同一个全局组内。其特点如下：

- 全局组内的成员，只能包含所属域内的用户与全局组，即只能将同一个域内的用户或其他全局组加入到全局组内。
- 全局组可以访问任何一个域内的资源，即可以在任何一个域内设置全局组的使用权限，无论该全局组是在同一个域内，还是在另一个域内。

通用组可以设置在所有域内的访问权限，以便访问所有域资源。其特征如下：

- 通用组成员可以包括整个域林（多个域）中任何一个域内的用户，但是，无法包含任何一个域内的域本地组。
- 通用组可以访问任何一个域内的资源，也就是说，可以在任何一个域内设置通用组的权限，无论该通用组是在同一个域内，还是在另一个域内。

2. 组类型

创建域组时，在“组类型”选项区域中可选择组的类型：

- 安全组。可以显示在随机访问控制列表（DACL）中的组，该列表用于定义对资源和对象的权限。“安全组”也可用作电子邮件实体，给这种组发送电子邮件的同时也会将该邮件发给组中的所有成员。

- 通信组。仅用于分发电子邮件并且没有启用安全性的组。不能将“通信组”显示在用于定义资源和对象权限的随机访问控制列表（DACL）中。“通信组”只能与电子邮件应用程序（例如，Microsoft Exchange）一起使用，以便将电子邮件发送到用户集合。如果因为安全目的并不需要组，可以选择创建“通信组”而不要创建“安全组”。

3. 指定组管理员

默认情况下，每个系统管理员都可以管理任何用户组，并进行常规管理工作，如更新成员列表、指派用户权限等。域管理员也可以为组指定特定的管理者。需要注意的是，一旦指定了组管理员，将只有该管理者可以管理该组，域管理员都不允许。不过，独立服务器不具有此功能。指定组管理员的操作步骤如下：

第 1 步，在“Active Directory 用户和计算机”窗口中，右击要指定管理员的组（如 test），选择快捷菜单中的“属性”选项，显示如图 3-64 所示“test 属性”对话框，切换到“管理者”选项卡。

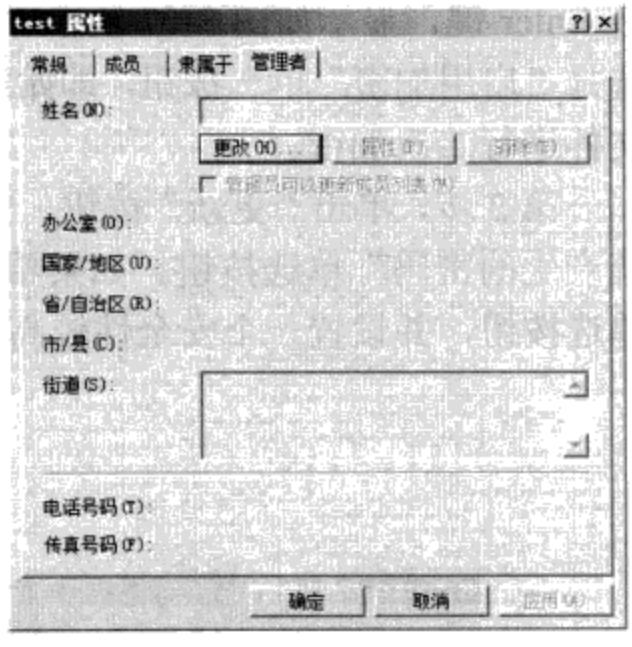


图 3-64 “管理者”选项卡

第 2 步，单击“更改”按钮，显示如图 3-65 所示“选择用户、联系人或组”对话框。在“输入要选择的对象名称”文本框中，输入要指派的管理者的用户名，或组名。被指定为组管理员的账户，可以不属于该组。

第 3 步，单击“确定”按钮返回“管理者”选项卡，在“姓名”文本框，显示了所添加的管理者账户名称，如图 3-66 所示。默认情况下，没有选中“管理员可以更新成员列表”复选框，为了方便域管理员工作，建议选中该复选框。

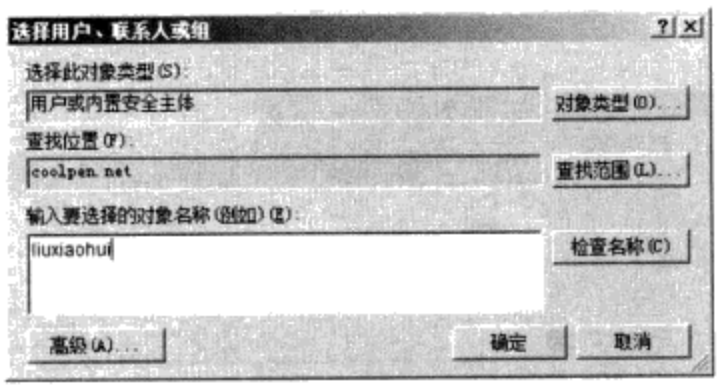


图 3-65 “选择用户、联系人或组”对话框

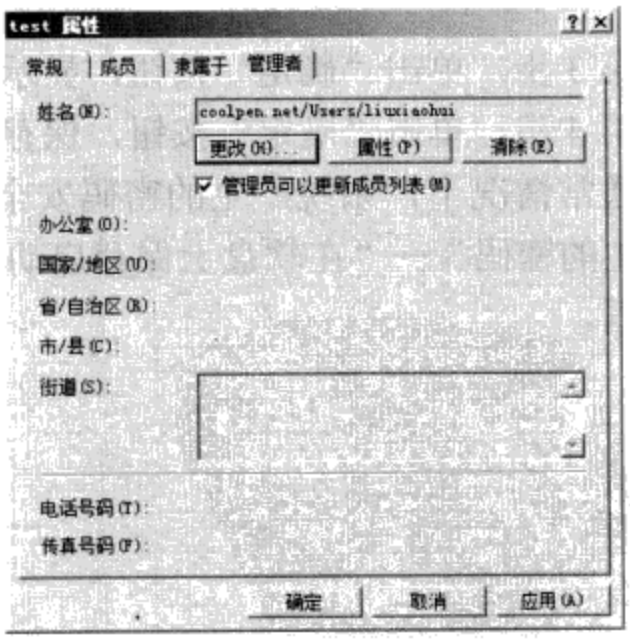


图 3-66 已指定管理者

第 4 步，单击“确定”按钮，完成组的管理者的指派。

3.3.7 系统账号数据库

默认情况下，Windows Server 2008 R2 系统中所有用户账户的登录信息，全部保存在%systemroot%\system32\config 目录下的 sma 文件中，该文件是 Windows 的系统账号数据库。做好 sma 文件的安全保护工作，也就间接保护了管理员账户的安全。Syskey 是 Windows 系统内置的账号数据库加密专用工具，加密之后，即使入侵者窃取了被加密的 sam 文件，也无法获取其中的用户名和密码信息。

第 1 步，单击“开始”按钮，在“开始”菜单的“开始搜索”文本框中，输入 syskey 并按 Enter 键，显示如图 3-67 所示“保证 Windows 账户数据库的安全”对话框。系统默认已经选择“启用加密”单选按钮，即始终执行对 sma 文件的加密。单击“确定”按钮，即可对 sam 文件进行二次加密。

第 2 步，单击“更新”按钮，显示如图 3-68 所示“启动密钥”对话框，系统默认选择“系统产生的密码”单选按钮。如果希望需要密码才能启动 Windows，则可以选择“密码启动”单选按钮，并设置一个安全性较高的密码，至少 12 个字符，最多可以 128 个字符。

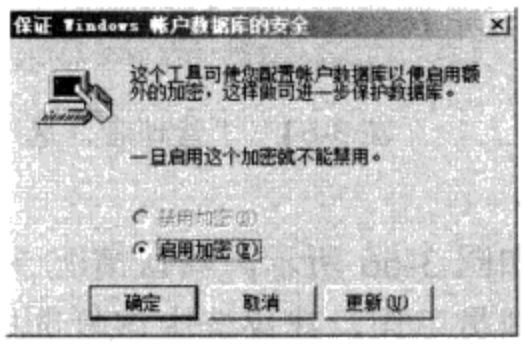


图 3-67 “启动密码”对话框

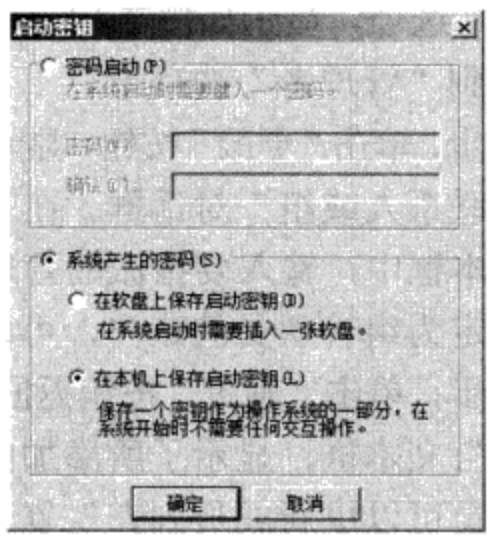


图 3-68 对话框

第 3 步，单击“确定”按钮，显示如图 3-69 所示“成功”对话框。

第 4 步，单击“确定”按钮，保存设置。

通常情况下，系统产生的密码安全性要高于人工输入的密码，用户也可以依次选择“系统产生的密码”→“在软盘上保存启动密钥”单选按钮，显示如图 3-70 所示“保存启动密码”对话框。

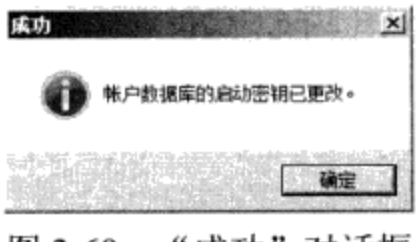


图 3-69 “成功”对话框

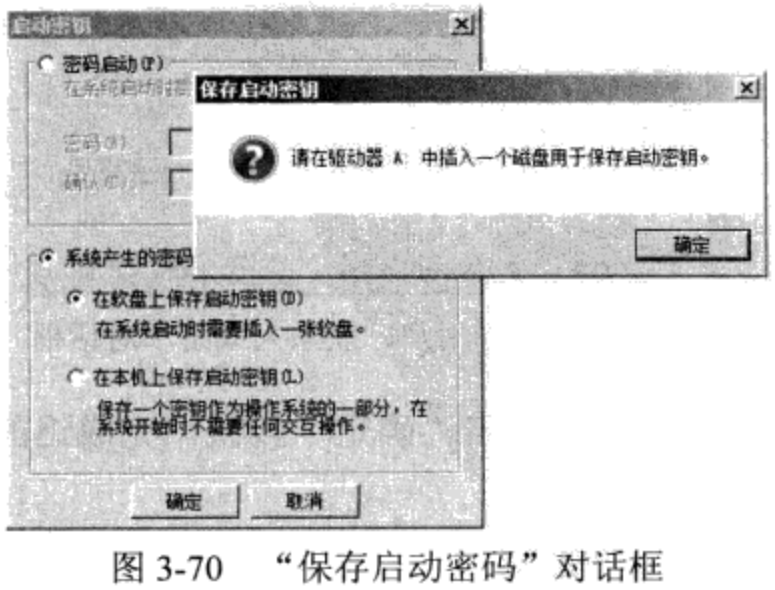


图 3-70 “保存启动密码”对话框

将已格式化好的空白软盘插入软驱并单击“确定”按钮，系统即可生成安全密码，并保存到软盘中。完成后提示如图 3-71 所示对话框，启动系统时将提示插入该软盘。软盘中的密码文件默认名称为 StartKey.Key。

如果将启动密码保存至软盘，则重新启动计算机时，显示如图 3-72 所示“启动密钥盘”对话框，提示插入保存启动密钥的软盘。

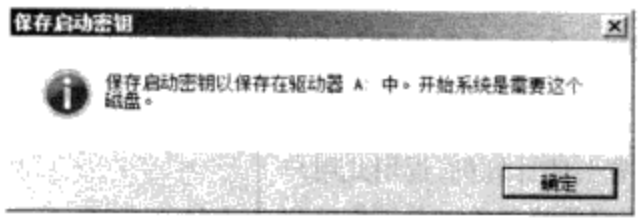


图 3-71　创建成功

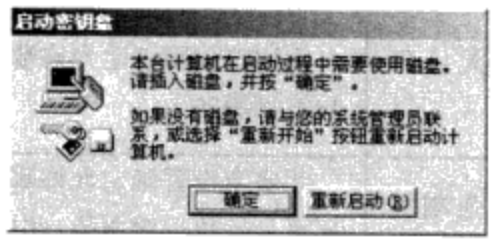


图 3-72　“启动密码盘”对话框

注意

账号数据库的加密操作是不可逆的，即一旦启用将无法停止。但是如果不希望每次都要输入启动密码或准备启动密码软盘，可以直接在“启动密码”对话框中，依次选择“系统产生的密码”→“在本机上保存启动密钥”单选按钮，将其恢复为默认状态即可。该选项是将保存一个密码作为操作系统的一部分，在系统开始时不需要用户进行任何交互操作，既安全又方便。

3.3.8 分配本地用户管理权限

通常情况下，服务器的管理工作涉及数据备份、系统配置、网络连接配置等多个方面，为了减轻管理员负担，可以将这些管理工作分配给不同的用户，这样还可以避免由于个别用户权限过高而给系统或网络带来的安全威胁。

1. 可分配的用户权限

管理员可以通过配置本地安全策略，为用户账户分配相应的操作权限。在 Windows Server 2008 R2 系统中，管理员可以为用户账户指派更为详细的安全管理权限，可分配权限及功能描述如表 3-1 所示。

表 3-1　用户权限分配策略及功能

策略	功能说明	默认用户账户和组
备份文件和目录	确定哪些用户可以绕过文件和目录、注册表和其他永久对象权限进行系统备份	Administrators 、 Backup Operators
创建符号链接	此权限决定用户是否可以从登录的计算机创建符号链接	Administrators
创建全局对象	此用户权限对于在终端服务会话过程中创建全局对象的用户账户是必需的。未分配此用户权限的用户仍可以创建特定于会话的对象	LOCAL SERVICE 、NETWORK SERVICE、Administrators、SERVICE
创建一个令牌对象	此安全设置确定进程可以使用哪些账户创建令牌，该令牌接着可以在进程使用内部应用程序编程接口（API，Application Programming Interface）创建访问令牌时用于获取任何本地资源的访问权限。此用户权限供操作系统内部使用。除非必要，建议不要将此用户权限分配给本地系统之外的用户、组或进程	没有任何用户账户
创建一个页面文件	此用户权限确定哪些用户和组可以调用内部应用程序编程接口（API）创建页面文件。此用户权限供操作系统内部使用，且通常不需要分配给任何用户	Administrators

（续表）

策略	功能说明	默认用户账户和组
创建永久共享对象	此用户权限确定进程可以使用哪些账户利用对象管理器创建目录对象。此用户权限供操作系统内部使用，且对于扩展对象命名空间的内核模式组件非常有用	没有任何用户账户
从扩展坞上取下计算机	此安全设置确定用户是否可以无需登录而从其扩展坞上移除便携式计算机	Administrators
从网络访问此计算机	此用户权限确定允许哪些用户和组通过网络连接到计算机。此用户权限不影响终端服务	Everyone、Administrators、Users、Backup Operators
从远程系统强制关机	此安全设置确定允许哪些用户从网络上的远程位置关闭计算机。误用此用户权限会导致拒绝服务。此用户权限是在默认域控制器组策略对象以及工作站和服务器的本地安全策略中进行定义的	Administrators
更改时区	此用户权限确定哪些用户和组可以更改计算机默认时区。这是 Windows Server 2008 的新增用户权限分配策略之一	LOCAL SERVICE、Administrators
更改系统时间	此用户权限确定哪些用户和组可以更改计算机内部时钟上的日期和时间。分配了此用户权限的用户可以影响事件日志的外观。如果已更改了系统时间，则记录的事件将反映此新时间，而不是事件发生的实际时间	LOCAL SERVICE、Administrators
关闭系统	此安全设置确定哪些在本地登录到计算机的用户可以使用关机命令关闭操作系统。误用此用户权限会导致拒绝服务	Administrators、Backup Operators
管理审核和安全日志	此安全设置确定哪些用户可以为单独的资源（如文件、Active Directory 对象和注册表项）指定对象访问审核选项	Administrators
还原文件和目录	此安全设置确定在还原备份的文件和目录时哪些用户可以绕过文件、目录、注册表和其他永久对象权限，以及确定哪些用户可以将任何有效的安全主体设置为对象的所有者	Administrators、Backup Operators
加载和卸载设备驱动程序	此用户权限确定哪些用户可以将设备驱动程序或其他代码动态加载和卸载到内核模式中。此用户权限不适用于即插即用设备驱动程序。建议不要将此权限分配给其他用户	Administrators
将工作站添加到域	此安全设置确定哪些组或用户可以将工作站添加到域。此安全设置仅对域控制器有效。默认情况下，任何已经过身份验证的用户都具有此权限并可以在该域中最多创建 10 个计算机账户	没有任何用户账户
拒绝本地登录	此安全设置确定要防止哪些用户在该计算机上登录。如果账户受制于此策略设置和“允许本地登录”策略设置，则前者会取代后者	没有任何用户账户
拒绝从网络访问这台计算机	此安全设置确定要防止哪些用户通过网络访问计算机。如果用户账户受限于此策略设置和“从网络访问此计算机”策略设置，则前者会取代后者	没有任何用户账户
拒绝通过远程桌面服务登录	此安全设置确定禁止哪些用户和组作为远程桌面服务客户端登录	没有任何用户账户
拒绝作为服务登录	此安全设置确定要防止哪些服务账户将进程注册为服务。如果账户受制于此策略设置和“作为服务登录”策略设置，则前者会取代后者	没有任何用户账户
拒绝作为批处理作业登录	此安全设置确定要防止哪些账户作为批处理作业登录。如果用户账户受限于此策略设置和“作为批处理作业登录”策略设置，则前者会取代后者	没有任何用户账户
配置文件单个进程	此安全设置确定哪些用户可以使用性能监视工具来监视非系统进程的性能	Administrators
配置文件系统性能	此安全设置确定哪些用户可以使用性能监视工具来监视系统进程的性能	Administrators
取得文件或其他对象的所有权	此安全设置确定哪些用户可以取得系统中任何安全对象（包括 Active Directory 对象、文件和文件夹、打印机、注册表项、进程以及线程）的所有权	Administrators
绕过遍历检查	此用户权限确定哪些用户即使在不具有对已遍历目录的权限时，也可以遍历目录树。此权限不允许用户列出目录的内容，仅允许遍历目录。此用户权限是在默认域控制器组策略对象以及工作站和服务器的本地安全策略中进行定义的	Everyone、LOCAL SERVICE、NETWORK SERVICE、Administrators、Users、Backup Operators

（续表）

策略	功能说明	默认用户账户和组
身份验证后模拟客户端	将此权限分配给用户使代表该用户运行的程序能够模拟客户端。此种模拟要求此用户权限可防止未经授权的用户说服客户端连接(例如，通过远程过程调用（RPC）或命名管道)到他们已创建的服务，然后模拟该客户端，这样会将未经授权的用户的权限提升至管理级别或系统级别	LOCAL SERVICE、NETWORK SERVICE、Administrators、SERVICE
生成安全审核	此安全设置确定进程可以使用哪些账户将项目添加到安全日志中。安全日志用于跟踪未授权的系统访问。如果启用了“审核: 如果无法记录安全审核，则立即关闭系统”安全策略设置，则误用此用户权限会导致生成许多审核事件，可能隐藏攻击证据或导致拒绝服务	LOCAL SERVICE、NETWORK SERVICE
锁定页内存	此安全设置确定哪些账户可以使用进程将数据保持在物理内存中，这样可以防止系统将数据分页到磁盘上的虚拟内存中。行使此权限会因降低可用随即村粗内存的数量而显著影响系统性能	没有任何用户账户
提高计划优先级	此安全设置确定哪些账户可以使用对另一个进程具有 Write Property 访问权限的进程来提高分配给其他进程的执行优先级。具有此权限的用户可以通过任务管理器用户界面更改进程的计划优先级	Administrators
替换一个进程级令牌	此安全设置确定哪些用户账户可以调用应用程序编程接口，从而使一个服务能够启动另一个服务。任务计划程序是使用此用户权限的进程的一个示例。有关任务计划程序的信息，请参阅任务计划程序概述	LOCAL SERVICE、NETWORK SERVICE
调试程序	此用户权限确定哪些用户可以将调试程序连接到任何进程或连接到内核。不需要将此用户权限分配给正在调试自己的应用程序的开发人员。调试新系统组件的开发人员将需要此用户权限来执行相应操作。此用户权限提供对敏感和关键系统组件的完全访问权限	Administrators
同步目录服务数据	此安全设置确定哪些用户和组有权同步所有目录服务数据，也称为 Active Directory 同步	没有任何用户账户
为进程调整内存配额	此权限确定谁可以更改进程可消耗的最大内存。此用户权限是在默认域控制器组策略对象以及工作站和服务器的本地安全策略中进行定义的	LOCAL SERVICE、NETWORK SERVICE、Administrators
信任计算机和用户账户可以执行委派	此安全设置确定哪些用户可以在用户或计算机对象上，设置“已为委派信任”设置	没有任何用户账户
修改固件环境值	此安全设置确定谁可以修改固件环境值。固件环境变量是在非基于 x86 的计算机的稳定 RAM 中存储的设置。该设置的效果依赖于处理器	Administrators
修改 一个对象标签	此权限决定哪些用户账户可以修改对象（例如文件、注册表项或其他用户所拥有的进程）的完整性标签。在用户账户下运行的进程可以将该用户所拥有的对象标签修改为没有此权限的更低级别	没有任何用户账户
以操作系统方式执行	此用户权限允许某个进程模拟任意用户而无须进行身份验证。因此该进程可以与该用户一样获得对本地资源的访问权限	没有任何用户账户
允许在本地登录	此登录权限确定哪些用户能以交互方式登录到此计算机。通过在连接的键盘上按 Ctrl+Alt+Del 序列启动的登录要求用户具有此登录权限。此外，可以登录用户的某些服务或管理应用程序可能要求此登录权限。如果为某个用户或组定义此策略，则还必须向 Administrators 组授予此权限	Administrators、Users、Backup Operators
允许通过终端服务登录	此安全设置确定哪些用户或组具有作为终端服务客户端登录的权限	Administrators、Remote Desktop Users
增加进程工作集	此安全设置确定允许那些用户增加运行进程时所需访问的页面数量	Users
执行卷维护任务	此安全设置确定哪些用户和组可以在卷上运行维护任务，如远程碎片整理。需要注意的是，具有此用户权限的账户可以浏览磁盘及将文件扩展到包含其他数据的内存中。当打开扩展的文件时，用户可能能够读取和修改获得的数据	Administrators
作为服务登录	此安全设置确定哪些服务账户可以将进程注册为服务	没有任何用户账户
作为批处理作业登录	此安全设置使用户能够通过批处理队列实用程序登录，并仅提供用于与旧版本的 Windows 的兼容性	Administrators、Backup Operators、Performance Log Users
作为受信任的呼叫方访问凭据管理器	此安全设置用于确定哪些远程访问账户可以访问本地服务器或网络上的凭据管理器，存在很大的风险，建议不要轻易使用	没有任何用户账户

2. 分配“备份文件和目录”权限

这里以“备份文件和目录”为例，介绍如何配置用户权限分配策略。

第1步，在“组策略管理编辑器”窗口中，依次展开“计算机配置”→“Windows 设置”→“安全设置”→“本地策略”→“用户权限分配”选项。在右侧窗口中双击“备份文件和目录”策略，显示如图3-73所示“备份文件和目录 属性”对话框，当前服务器是域控制器，某些操作权限只能在“组策略管理编辑器”中完成。

图3-73　用户权限分配策略

第2步，单击“添加用户或组”按钮，在“添加用户或组”对话框中单击“浏览”按钮，添加想要授予此操作权限的用户账户或组，如图3-74所示。

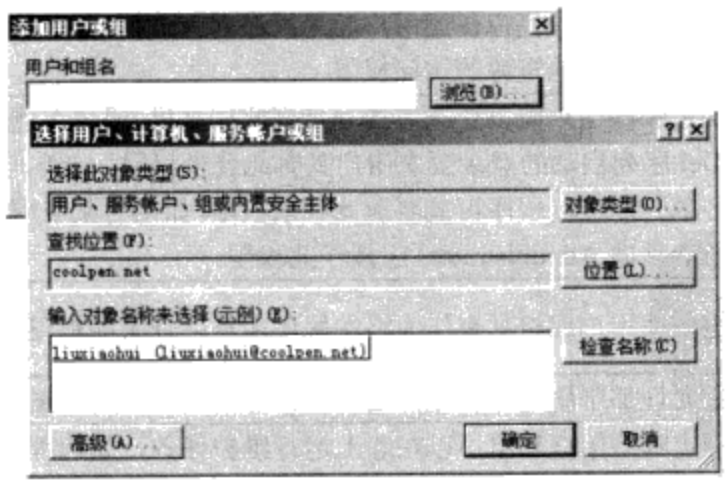


图3-74　添加用户账户或组

第3步，连续单击“确定”按钮，保存配置即可。

第 4 章　文件系统与共享资源安全

文件资源安全是网络安全的重要内容之一。基于 NTFS 文件系统的 Windows Server 2008 R2 系统默认已经支持多种安全功能配置，用户只需对其进行合理配置和使用即可。对于共享资源而言，由于暴露在相对开放的网络环境中，所以更要确保其安全性。本章主要介绍 NTFS 权限设置在文件访问安全方面的应用。

4.1　NTFS 权限概述

权限是指与计算机或网络上的对象（如文件和文件夹）关联的访问规则，用于确定用户是否可以访问某个对象以及可以执行哪些操作。本地计算机管理员或域管理员可以为普通用户和组分配权限。NTFS 是从 Windows NT 开始引入的文件系统，也是目前 Windows 服务器系统常用的文件系统。通过 NTFS，管理员可以实现对文件和文件夹的授权访问，从而确保服务器文件存储的安全。默认情况下，只有授予用户允许访问权限时，该用户才可以访问，否则是无法访问的。

4.1.1　NTFS 文件夹权限和 NTFS 文件权限

对于 NTFS 分区上的文件和文件夹，管理员可以通过 NTFS 权限限制不同用户账户的访问权限。文件和文件夹的 NTFS 权限有两种类型：显式权限和继承权限。其中，显式权限是系统创建对象时，默认赋予用户账户的访问和操作权限；继承权限是从父对象传播到当前对象的权限。继承权限可以减轻管理权限的任务，并且确保给定容器内所有对象之间的权限一致性。默认情况下，文件将自动继承来自其父文件夹的 NTFS 权限设置。

1.　NTFS 文件夹权限

NTFS 文件夹权限及允许用户完成的操作如下表 4-1 所示。

表 4-1　NTFS 文件夹权限

NTFS 文件夹权限	允许用户完成的操作
读取	查看该文件夹中的文件和子文件夹，查看文件夹的所有者、权限和属性
写入	在该文件夹内新建文件和子文件夹，更改文件夹属性，查看文件夹的所有者和权限
列出文件夹目录	查看该文件夹中的文件和子文件夹的名称
读取及运行	完成“读取”权限和“列文件夹目录”权限所允许的操作
修改	完成“写入”权限及“读取及执行”权限所允许的操作，删除文件夹
完全控制	完成其他所有 NTFS 权限允许的操作，更改权限，取得所有权和删除子文件夹和文件

设置 NTFS 文件夹访问权限的主要操作步骤如下：

第 1 步，以管理员账户登录系统，打开 Windows 资源管理器，右击欲设置 NTFS 权限的文件夹（本例以 test 文件夹为例），并选择快捷菜单中的“属性”选项，打开“test 属性”对

话框，切换至如图 4-1 所示“安全”选项卡。

第 2 步，在“组或用户名”列表框中选择想要配置权限的用户账户，如 hstjl，在下面的权限列表框中即可查看其当前权限。单击“编辑”按钮，显示如图 4-2 所示对话框。继续在“组或用户名”列表框中选择 hstjl，即可在下面的“hstjl 的权限”列表框中修改其权限。默认情况下，是没有对普通用户设置任何 NTFS 访问权限的，用户账户将自动继承来自其所属组的权限，文件夹将自动继承来自其父文件夹的 NTFS 权限。

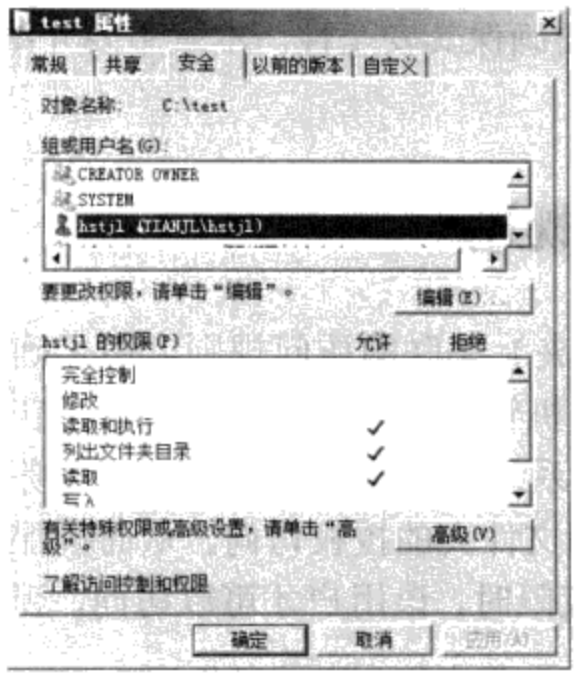


图 4-1 “test 属性”对话框

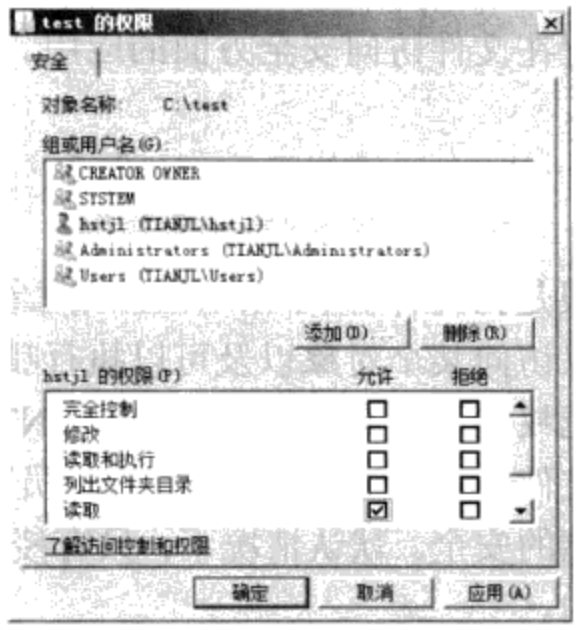


图 4-2 更改用户权限

提示

如果权限带阴影显示，说明这些权限是从父文件夹的权限继承过来的。

第 3 步，如果“组或用户名”列表框中默认没有需要的用户账户，则可以单击“添加”按钮，显示如图 4-3 所示“选择用户或组”对话框，在“输入对象名称来选择”文本框中，输入想要添加的用户账户名并单击“确定”按钮即可。在域控制器上还可以直接添加其他被信任域中的用户账户。

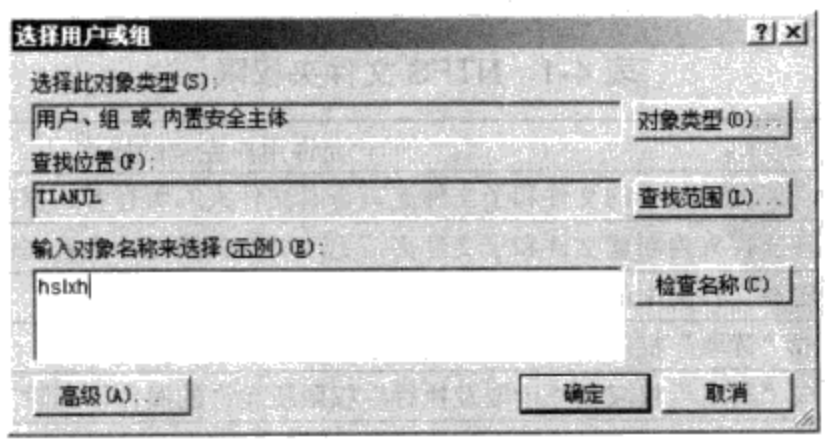


图 4-3 “选择用户或组”对话框

第 4 步，在“更改用户权限”对话框的“组或用户名称”列表框中，选择想要删除的用户或组，并单击“删除”按钮，即可将其从列表框中删除。如果此时该账户所属组未被删除，则该账户仍具有相应访问权限。

第 5 步，单击“应用”和“确定”按钮，保存设置即可。重复上述操作，可以为不同用户账户指定不同的 NTFS 文件夹权限。

2. NTFS 文件权限

NTFS 文件权限及允许用户完成的操作如表 4-2 所示。

表 4-2 NTFS 文件权限及允许用户完成的操作

NTFS 文件权限	允许用户完成的操作
读取	读该文件和查看文件属性、所有者及权限
写入	覆盖该文件，更改文件属性和查看文件的所有者和权限
读取及运行	完成“读取”权限所允许的操作。例如，运行应用程序
修改	完成“写入”权限和“读取及运行”权限所允许的操作。例如，修改和删除文件
完全控制	完成其他所有 NTFS 文件权限所允许的操作。例如，更改权限和取得所有权

设置 NTFS 文件权限与设置 NTFS 文件夹权限非常相似，如图 4-4 所示，此处不再赘述。NTFS 文件权限仅对目标文件有效，但建议用户尽量不要采用直接为文件设置权限的方式，而是应当将文件放置于文件夹中，然后对该文件夹设置权限。

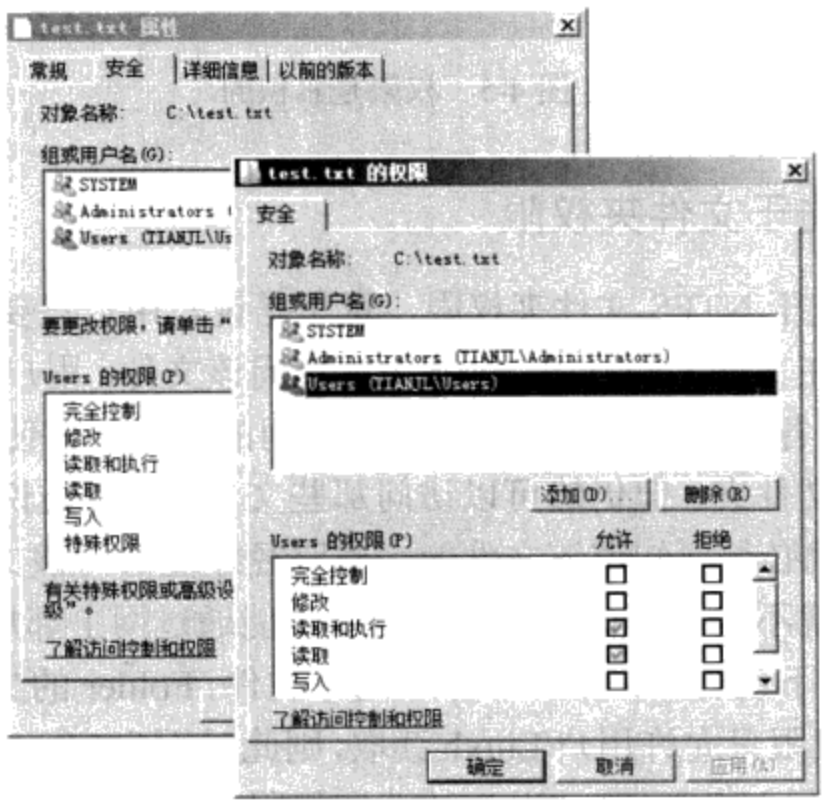


图 4-4 设置 NTFS 文件权限

4.1.2 多重 NTFS 权限

管理员可以根据需要为 NTFS 分区上的文件和文件夹同时设置 NTFS 权限，而文件夹和文件又有可能是包含与被包含的关系，所以必然会产生资源权限的重复，从而直接导致文件夹或文件最终的 NTFS 权限并非是管理员真正需要的结果。因此，配置 NTFS 权限之前必须明确以下几点：

1. 权限是累积的

用户对一个资源的最终权限是为该用户指定的全部 NTFS 权限和为该用户所属组指定的

全部 NTFS 权限之和。如果一位用户有一个文件夹的读取权限，同时又对该文件夹有写入权限的用户组的成员，则最终该用户对这个文件夹既有读取权限，也有写入权限。

例如，用户账户 Liuxh 隶属于 Manager 组，并且该用户本身对 Folder 文件夹具有读取权限，而其所在用户组 Manager 对 Folder 文件夹拥有写入权限，所以最终用户 Liuxh 对 Folder 文件夹的有效权限就是“读取+写入”，如图 4-5 所示。

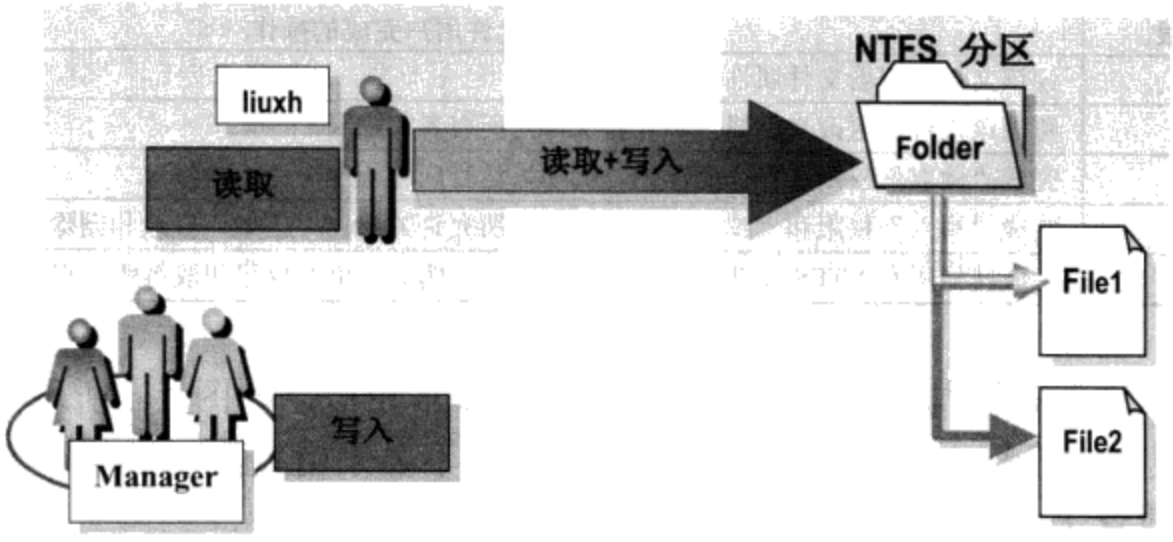


图 4-5 权限是累积的

2. 文件权限优先于文件夹权限

NTFS 文件权限优先于 NTFS 文件夹权限，意思是说，用户只要有访问一个文件的权限，即使没有访问该文件所在文件夹的权限，仍然可以访问该文件。用户可以通过用通用命令规则（UNC）或本地路径，从各自的应用程序打开有权访问的文件。即使该用户由于没有包含该文件夹的权限而看不到该文件夹，但仍然可以访问那些文件。也就是说，如果没有访问某个文件所在的文件夹的权限，就必须要知道该文件的完整路径才能访问该文件。也就是说，如果没有访问该文件夹的权限，就不能看到该文件夹，也就不能通过网上邻居等方式进行浏览访问。

例如，Folder 文件夹下包含 Files1 和 Files2 两个文件，Folder 的文件夹权限允许用户 Liuxh 写入，但 File2 的 NTFS 权限只允许用户 Liuxh 读取，则此时用户 Liuxh 的有效权限就是对 Folder 文件夹（包括 File1）的写入权限和对 File2 的读取权限，如图 4-6 所示。

3. 拒绝权限优先于其他权限

在 Windows 系统的所有 NTFS 权限中，拒绝权限优先于其他任何权限。即使用户作为一个组的成员有权访问文件或文件夹，一旦该用户被设置了拒绝访问权限，则最终将剥夺该用户可能拥有的任何其他权限。在实际使用中，应当尽量避免使用拒绝权限，因为允许用户或组进行某种访问，要比设置拒绝权限更容易做到。而事实上，只需巧妙地构造组和灵活组织文件夹中的资源，即可通过各种各样的“允许”权限满足访问控制的需求。

例如，User1 同时属于 Group B 组和 Group A 组。其中，User1 拥有对 Folder A 的读取权限，Group B 拥有对 Folder A 的读取和写入权限，Group A 则被禁止对 File2 的写操作。因此，User1 拥有对 Folder A 和 File1 的读取和写入权限，但对 File2 只有读取权限，如图 4-7 所示。

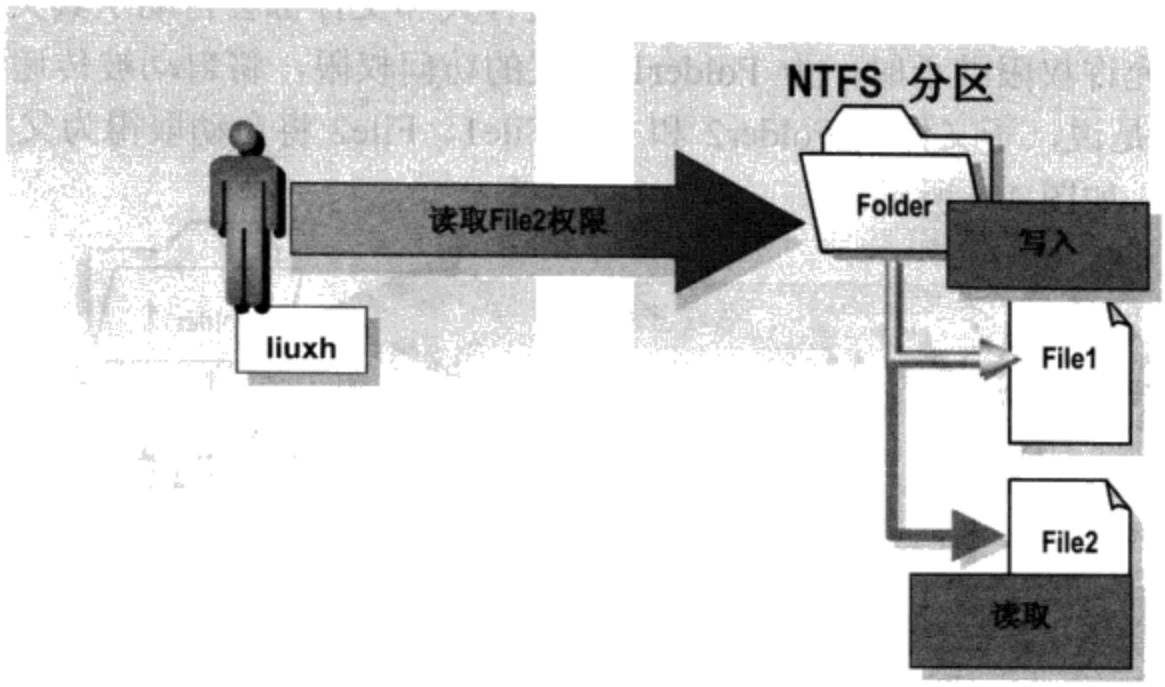


图 4-6　文件权限优先于文件夹权限

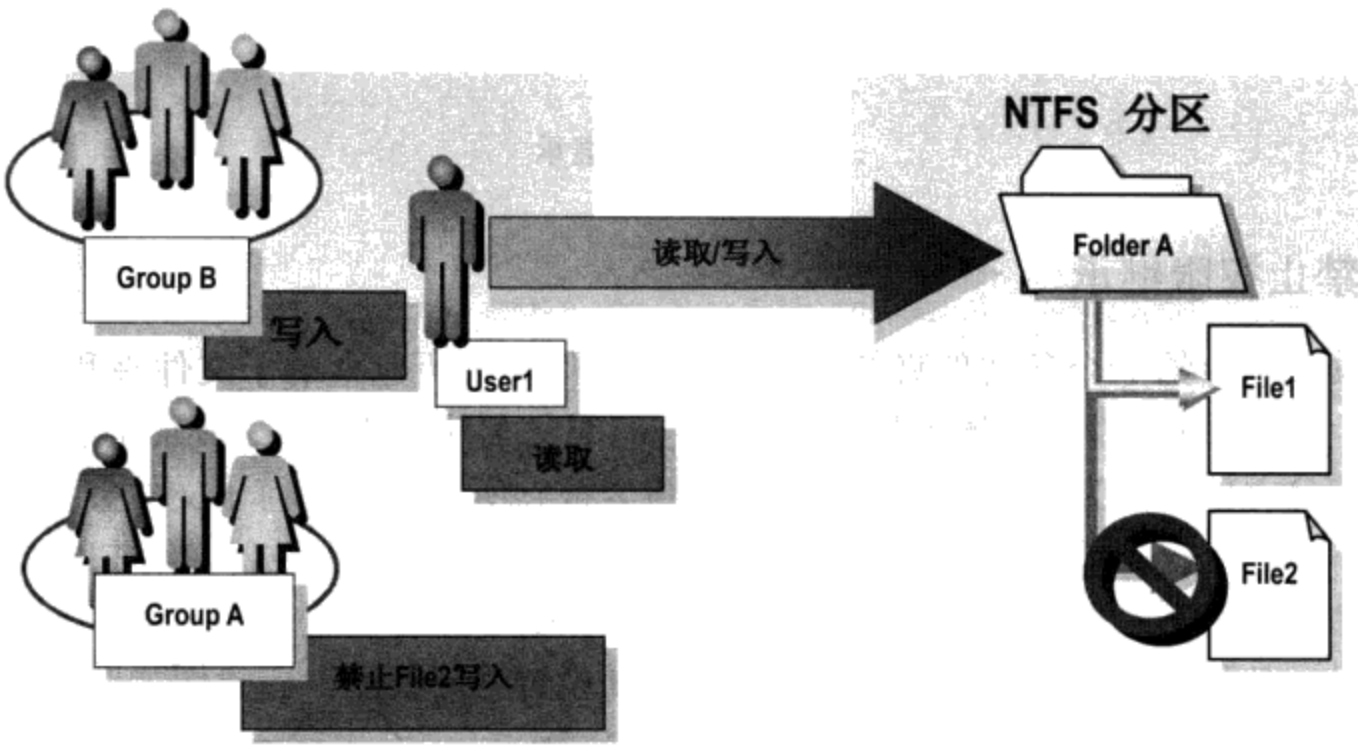


图 4-7　拒绝权限优先于其他权限

4.1.3 NTFS 权限的继承性

默认情况下，NTFS 权限是具有继承性的。所谓继承性，就是指 NTFS 权限自动从父对象传播到当前对象的过程，例如子文件夹继承来自其父文件夹的 NTFS 权限，文件继承来自文件夹的 NTFS 权限等。当然，正是因为 Windows 系统默认启用了 NTFS 权限继承，才会使用户不容易更加直观的判断对象最终的 NTFS 权限值。管理员可以根据实际情况，限制这种权限继承。

1. 权限继承

文件和子文件夹从其父文件夹继承权限，即管理员为父文件夹指定的任何权限，同时也适用于在该父文件夹中所包含的子文件夹和文件。当为一个 NTFS 文件夹指定权限时，不仅为该文件夹及其中所包含的文件和子文件夹指定了权限，同时也为将来在该文件夹中创建的所有

新文件和文件夹指定了权限。默认情况下，所有文件夹和文件都会自动从其父文件夹继承权限。

例如，当允许权限继承时，为 Folder1 设置的访问权限，将自动被传递给 File1、Folder2 和 File2。也就是说，子文件夹 Folder2 和文件 File1、File2 将自动取得为父文件夹 Folder1 设置的访问权限，如图 4-8 所示。

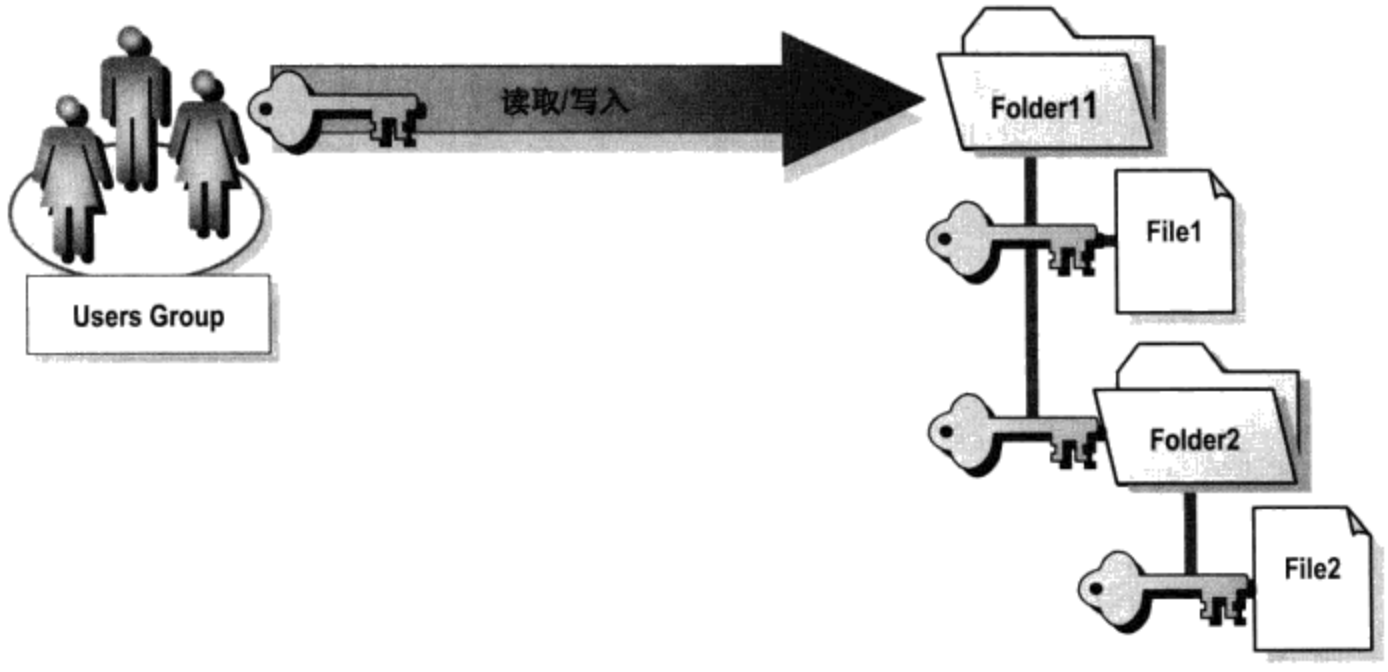


图 4-8　权限继承

2. 禁止权限继承

可以禁止指定给一个父文件夹的权限被这个文件夹中所包含的子文件夹和文件继承。也就是说，子文件夹和文件不会继承指定给包含它们的父文件夹的权限。被禁止继承权限的文件夹变成新的父文件夹，为该文件夹指定的权限将会被它所包含的任何子文件夹和文件继承。

例如，当禁止权限继承时，为 Folder1 设置的访问权限，将不被传递给 File1、Folder2 和 File2。也就是说，子文件夹 Folder2 和文件 File1、File2 不能自动取得为父文件夹 Folder1 设置的访问权限，必须一一为这些子文件夹和文件分别设置访问权限，示意图如图 4-9 所示。

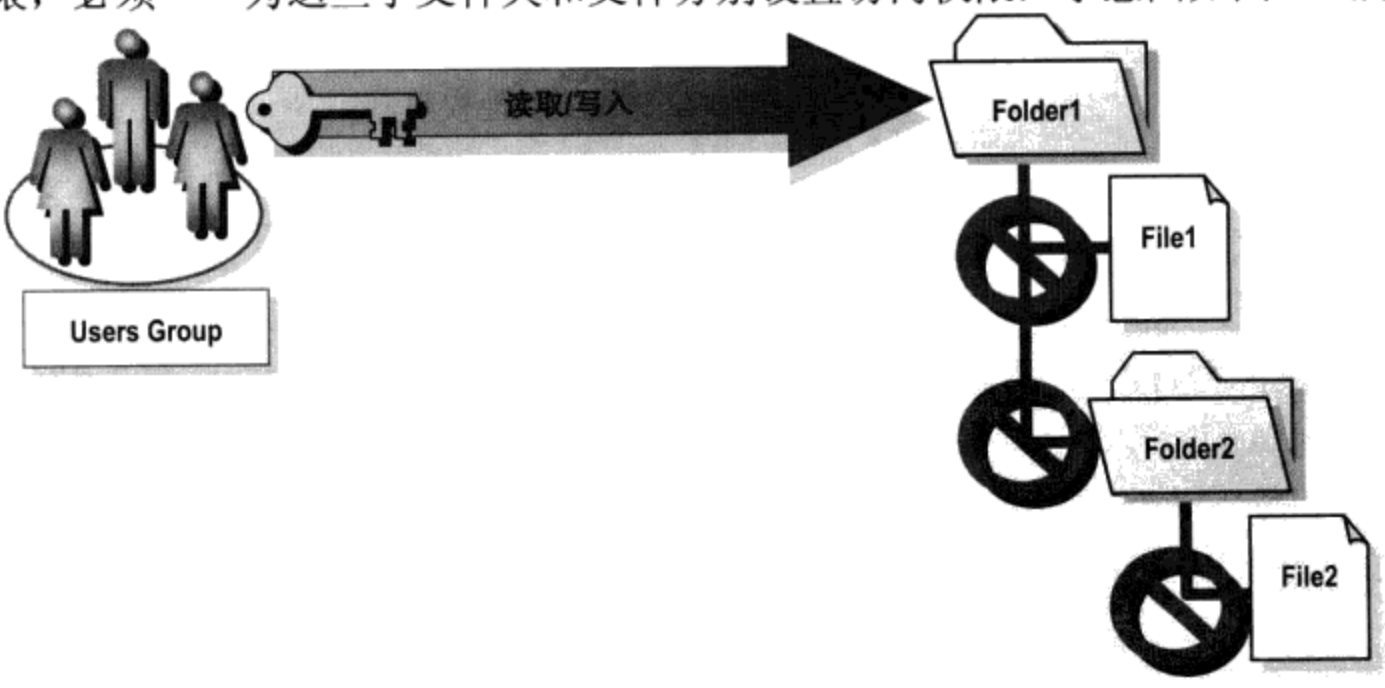


图 4-9　禁止继承权限

4.2 设置 NTFS 权限

NTFS 权限不仅在本地系统或本地域中有效，当目标资源在网络上共享时，这些权限设置同样有效，并且优先级高于共享权限设置。因此，从网络安全角度考虑，将资源设置为共享之前，应先配置其 NTFS 权限，以确保访问的安全性。

4.2.1 设置 NTFS 权限基本策略和规则

在设置 NTFS 权限时，必须遵循以下基本策略和规则：

- 为了简化管理，应事先对目标文件进行分类管理，将同一类别归于同一文件夹中，例如可以分为应用程序、数据和主目录文件夹等，并将主目录和公共文件夹集中在一个与应用程序和操作系统分开的独立卷上，从而只需为文件夹指定权限，而不必为单独的文件指定权限。另外，将所有历史数据保存在同一目录下，还减少了备份工作的复杂性。
- 在文件夹级指定需要的全部权限，而不是在文件级指定权限。对于希望限制用户访问的文件用单独的文件夹将文件分组，然后为该文件夹指定受限制的访问权限。
- 只允许用户拥有它们所需要的存取级别，也就是说，为用户或用户组指定最严格的 NTFS 权限，只要能够完成所需的任务即可，从而减少用户意外修改或删除重要文档和程序文件的可能性。如果用户只需要读取一个文件，那么，就只赋予其对该文件的读取权限。
- 按照组成员对资源的访问需要创建组，然后，为组指定适当的权限。只有必要时才为单独的用户指定权限。
- 对于全部应用程序的可执行文件，应当为 Administrators 组指定读取、执行权限和更改权限，但只为 Users 组指定读取和执行权限，从而有效防止应用程序文件被删除或破坏。
- 对于公共数据文件夹，应当为 Creator Owner 指定完全控制权限，使用户可以删除和修改其创建的文件和文件夹，从而完全访问在公共数据文件夹中创建的文件或文件夹。
- 对于公共文件夹，应当为 Everyone 组指定读取权限和写入权限，并为 Creator Owner 指定完全控制权限，使用户能够完全访问他们创建的文件，读取和修改其他用户创建的文件，并能够读取、修改和删除他们自己创建的文件和文件夹。同时，Everyone 组的成员只能读取该文件夹中的文件，并可向该文件夹中添加文件。
- 设置允许权限而不是拒绝权限。如果不希望让某个用户或用户组访问某个特定的文件夹或文件，就不要为其指定权限。拒绝权限应当是个例外，而不是经常使用的操作。只有在必须拒绝特定的用户账户或组的某种特定的访问类型时，才设置拒绝权限。
- 如果只是在这台计算机上访问资源，则使用描述性的长文件名。如果该文件夹将来要共享，则使用可被所有客户计算机访问的文件夹和文件名，建议采用短文件名的格式。

借助于文件服务器中设置的访问控制列表（ACL），不仅可以最大限度地保障重要数据存

储安全，保证数据不会由于计算机的硬件故障而丢失，而且还可以通过严格的权限设置，有效地保证数据的访问安全。

网络攻击的目的在于获取用户权限，而获取用户权限的目的，在于获取超级文件权限。因此，做好文件权限的访问控制，才是最重要和最有效的安全措施。在使用 NTFS 文件系统的基础上定制分区和文件访问条件，加强 Windows 2000/XP/2003 在默认状态下的访问权限，构建一个更加安全的系统。

4.2.2 设置普通 NTFS 权限

如果网络中的用户分类比较简单，则只需配置简单的 NTFS 访问权限即可，主要用于区别不同用户和组对文件的控制程度。管理员可以为 NTFS 卷上的文件夹和文件配置 NTFS 访问权限，这里仅以文件夹为例进行介绍。

以管理员账户登录系统，打开 Windows 资源管理器，右击欲设置 NTFS 权限的文件夹（以 test 文件夹为例），并选择快捷菜单中的“属性”选项，打开“test 属性”对话框，切换到“安全”选项卡。在“组或用户名”列表框中选择想要配置权限的用户账户，如 hstjl，在下面的权限列表框中即可查看其当前权限。单击“编辑”按钮，显示如图 4-10 所示对话框。继续在“组或用户名”列表框中选择 hstjl，即可在下面的“hstjl 的权限”列表框中修改其权限。默认情况下，是没有对普通用户设置任何 NTFS 访问权限的，用户账户将自动继承来自其所属组的权限，文件夹将自动继承来自其父文件夹的 NTFS 权限。

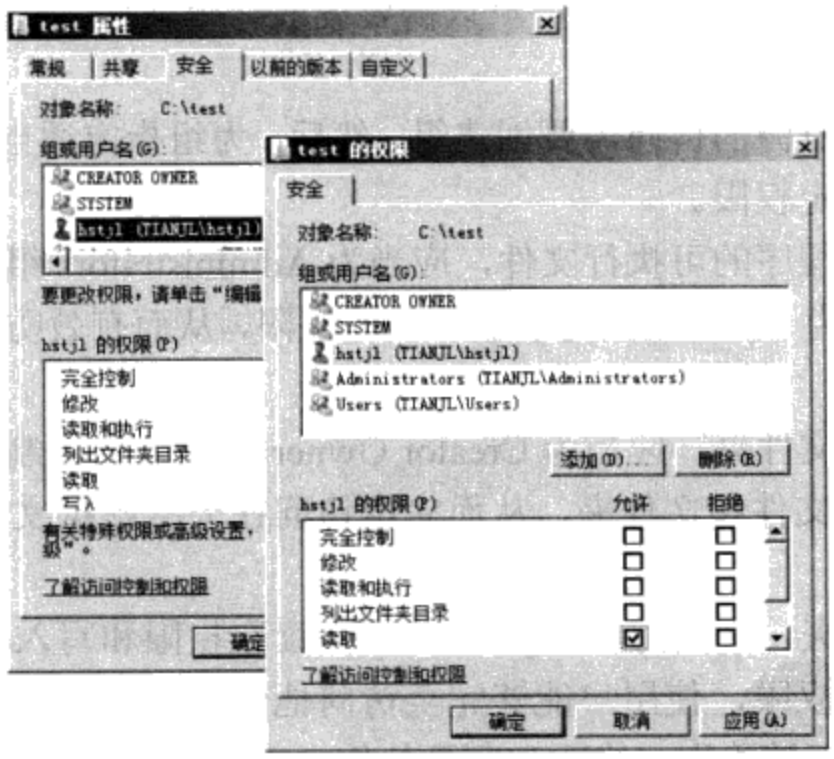


图 4-10 配置用户的 NTFS 访问权限

提示

如果权限带阴影显示，说明这些权限是从父文件夹的权限继承过来的。

4.2.3 设置高级 NTFS 权限

高级访问权限主要为管理员提供更为详细的权限值设定，实现更加严格的网络安全管理，一般用于用户划分复杂，且安全风险较高的网络环境。仍以 test 文件夹为例，设置高级权限的主要操作步骤如下。

第 1 步，在文件或文件夹属性的“安全”选项卡中，单击“高级”按钮，显示如图 4-11 所示“test 的高级安全设置”对话框，默认只能查看每个用户账户的高级访问权限设置。

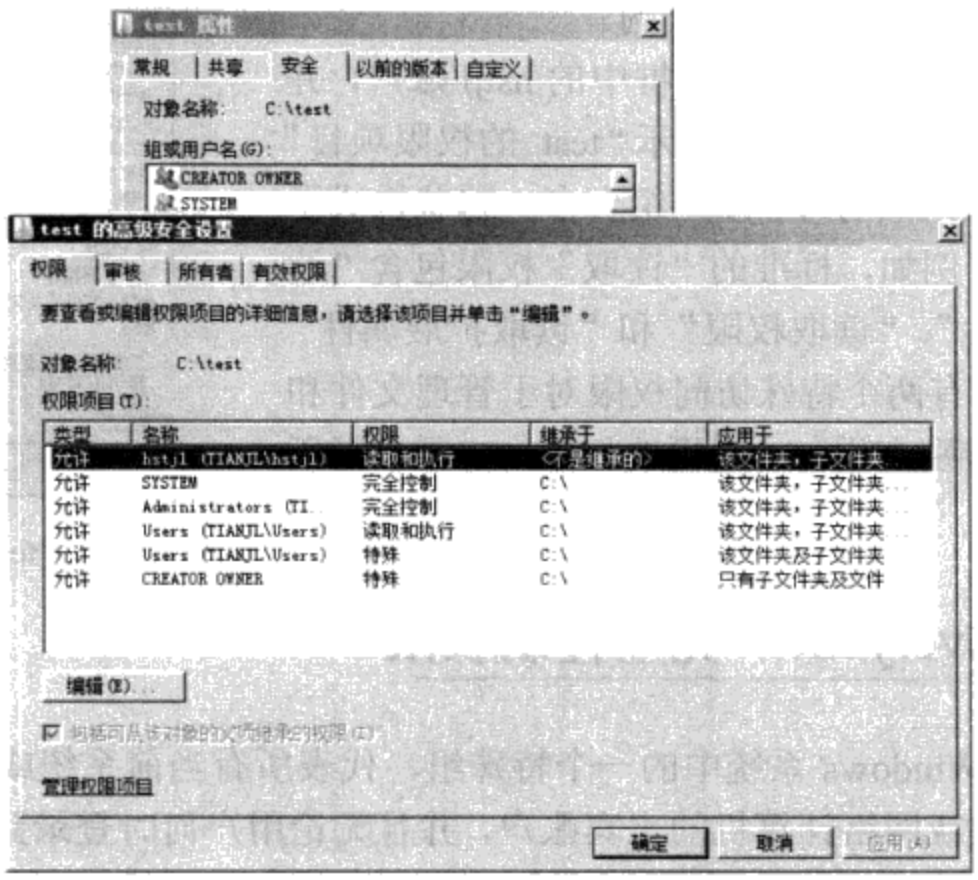


图 4-11 “test 的高级安全设置”对话框

第 2 步，在“权限项目”列表框中，选择想要设置高级权限的用户账户，如 hstjl。单击“编辑”按钮，显示如图 4-12 所示对话框，用于设置高级权限。

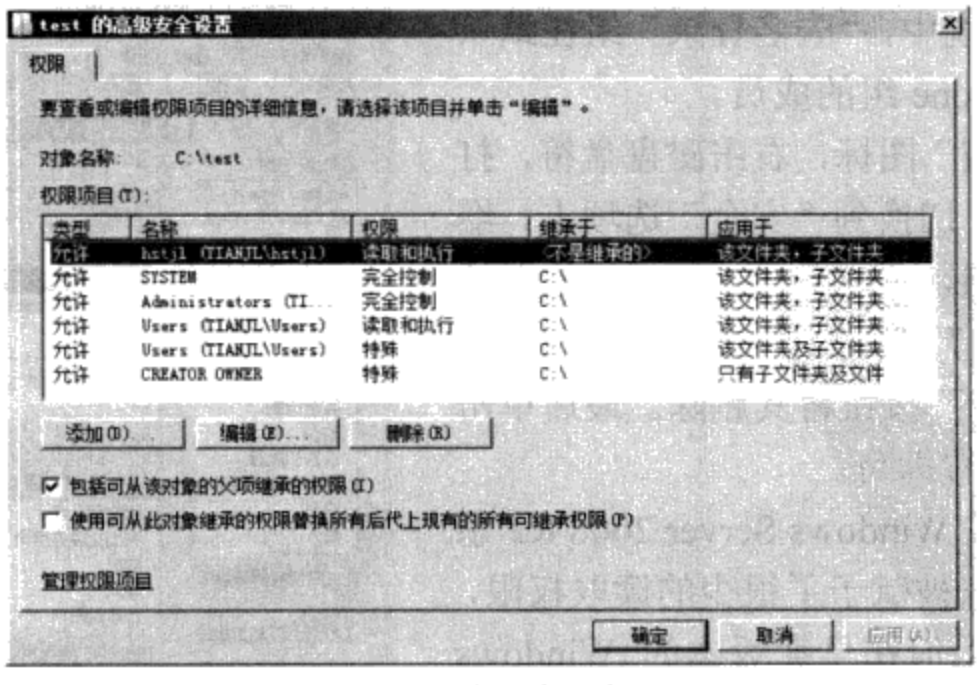


图 4-12 编辑高级权限

提示　系统默认已经选中“包括可从该对象的父项继承的权限”复选框，即自动继承来自父对象的高级权限，取消此复选框即可禁止 NTFS 权限的继承。

选中“使用可从对象继承的权限替换所有后代上现有的所有可继承权限”复选框后，该父对象上的权限将替换其子对象上的权限。如果取消，则每个对象上的权限（无论是父对象还是子对象）都将是唯一的。

第 3 步，选择“权限项目”列表框中的 hstjl 账户，并单击“编辑”按钮，显示如图 4-13 所示“test 的权限项目”对话框。高级访问权限共有 14 项，组合在一起就构成了标准的 NTFS 权限。例如，标准的“读取”权限包含“读取数据”、“读取属性”、“读取权限”和“读取扩展属性”4 种特殊访问权限。有两个特殊访问权限对于管理文件和文件夹的访问来说特别有用，一是更改权限，二是获得所有权。

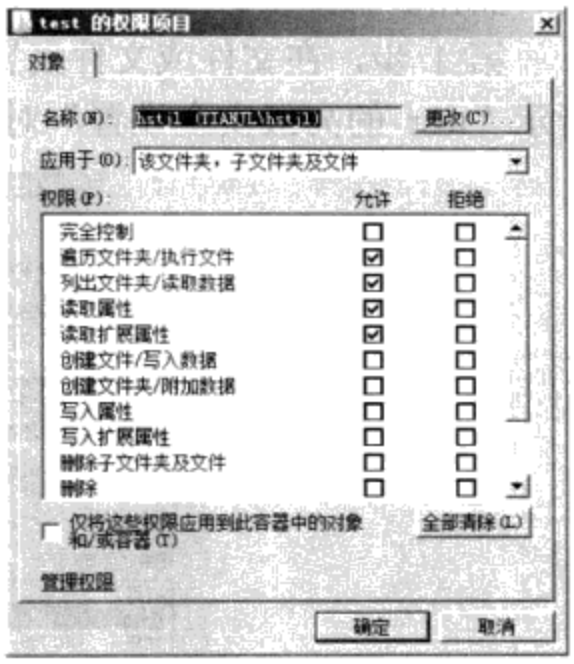


图 4-13　“test 的权限项目”对话框

4.2.4 取消“Everyone”完全控制权限

Everyone 组是 Windows 系统中的一个特殊组，代表所有当前系统或网络上的所有用户账户，包括来自其他域或网络计算机的来宾账户，并且无论用户何时登录到网络上，或通过网络访问本地计算机，都会自动将该用户添加到 Everyone 组中。如果为“Everyone”组赋予某种控制权限，则任何用户都可以对所涉及的文件夹或文件进行操作，严重影响系统安全，因此建议取消“Everyone”组的所有权限。需要注意的是，在早期版本的 Windows NT 系统中，匿名登录用户也是属于 Everyone 组的，但在 Windows Server 2003/2008 系统中，“匿名登录”组在默认情况下已不是 Everyone 组的成员。

打开“我的电脑”图标，右击磁盘盘符，打开磁盘属性对话框，切换到“安全”选项卡，继续单击“编辑”按钮，显示如图 4-14 所示对话框，在“组或用户名”列表框中选中“Everyone”选项，并单击“删除”按钮将其删除。最后单击“确定”按钮保存设置即可。

默认情况下，在 Windows Server 2008 R2 系统中，Everyone 组只被赋予了很少的读取权限，安全性以相对较高，但在早期版本的 Windows NT 系统中，该账户却拥有完全控制权限，很容易对系统安全造成威胁。

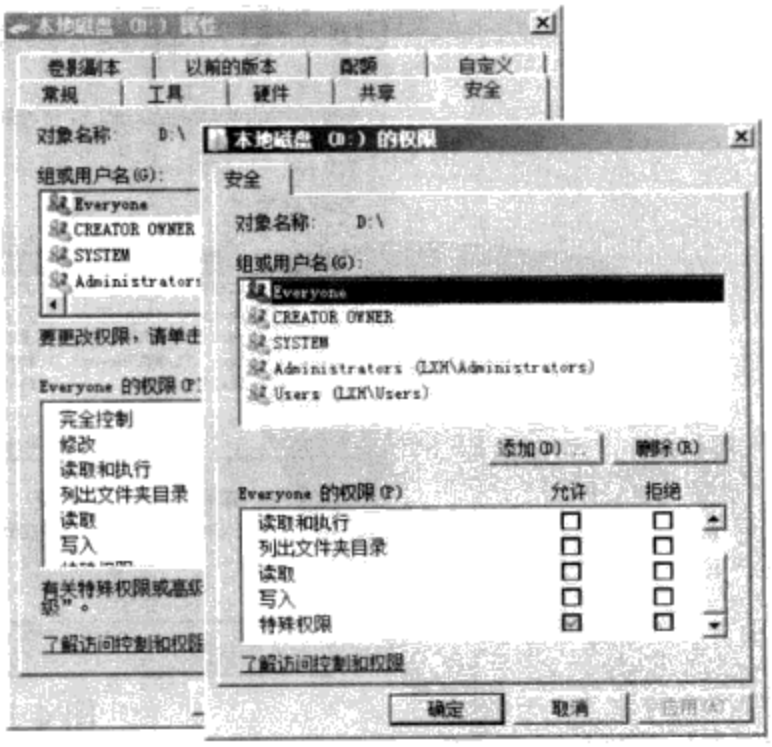


图 4-14　删除 Everyone 组

4.2.5 NTFS 权限复制

复制和移动已设置 NTFS 权限保护的文件或文件夹是在所难免的，但是操作之后往往会使原有的权限设置和当前的默认设置发生冲突，甚至产生安全漏洞。因此，在复制以配置 NTFS 权限保护的对象时，可以借助相关工具，达到联通权限配置一同复制的目的，如 robocopy、xcopy 等。

1. 复制和移动文件夹对权限的影响

在 NTFS 分区内和 NTFS 分区之间复制或者移动文件、文件夹时，Windows 系统会将其作为新文件或文件夹，因此，会对源文件或文件夹的 NTFS 权限产生影响。在复制文件和文件夹时，必须拥有源文件夹的“读取”权限，并且对目标文件夹具有“写入”权限。在移动文件或文件夹时，必须对目标文件夹拥有“写入”权限，并且对源文件夹拥有“修改”权限。

当从一个文件夹向另一个文件夹复制文件或文件夹时，或者从一个磁盘分区向另一个磁盘分区复制文件或文件夹时，复制文件或文件夹对 NTFS 权限产生下述影响：

- 当在单个 NTFS 分区内复制文件夹或文件夹时，文件夹或文件的复制将继承目的文件夹的权限。
- 当在 NTFS 分区之间复制文件夹或文件时，文件夹或者文件的复件将继承目的地文件夹的权限。
- 当将文件或文件夹复制到非 NTFS 分区时，因为非 NTFS 分区不支持 NTFS 权限，所以，这些文件夹或文件将丢失 NTFS 权限。

移动对 NTFS 权限的影响如下：

- 当在单个 NTFS 分区内移动文件夹或文件时，该文件夹或者文件保留其原来的权限。
- 当在 NTFS 分区之间移动文件夹或文件时，该文件夹或文件将继承目的地文件夹权限。当在 NTFS 分区之间移动文件夹或文件时，实际是将文件夹或文件复制到新位置，然后，将其从原来的位置删除。
- 当将文件或文件夹移动到非 NTFS 分区时，因为非 NTFS 分区不支持 NTFS 权限，所以，这些文件夹和文件将丢失其 NTFS 权限。

2. robocopy 权限复制

robocopy 命令行工具默认已集成在 Windows Server 2008 R2 系统中，此工具在命令行下可以简单高效的完成复杂的文件复制任务，同时支持对 NTFS 文件权限的复制。Robocopy 可以在复制文件时，将属性、用户权限、所有者都可以一并复制到目标文件夹中。

在命令提示符下键入如下命令：

```
robocopy c:\test c:\coolpen /e /copy:dat
```

按 Enter 键，运行后的结果显示如图 4-15 所示。

命令行中的 copy:dat 参数，表示将所有源文件夹的信息复制到目标文件夹中，其中 D：文件数据，A：文件属性，T：时间信息。

3. xcopy 权限复制

Xcopy 命令是 Windows Server 2008 R2 内置的命令行文件复制工具，支持 NTFS 权限的复制。例如，复制 test 文件夹到 coolpen 文件夹，同时复制目录以及文件 ACL 信息。

在命令行模式下输入：

```
xcopy c:\test c:\coolpen /o
```

按 Enter 键，运行后的结果显示如图 4-16 所示。

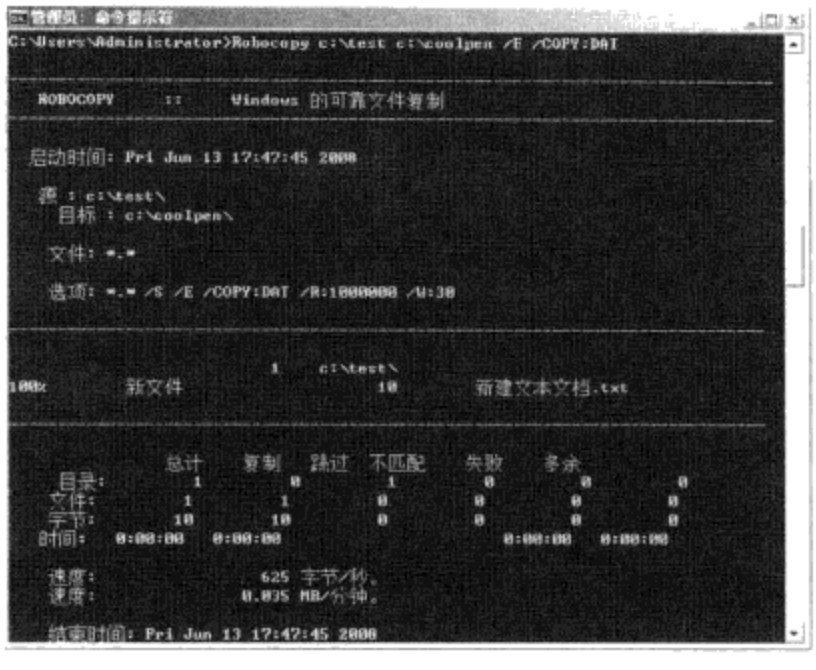


图 4-15 复制 NTFS 权限的文件夹

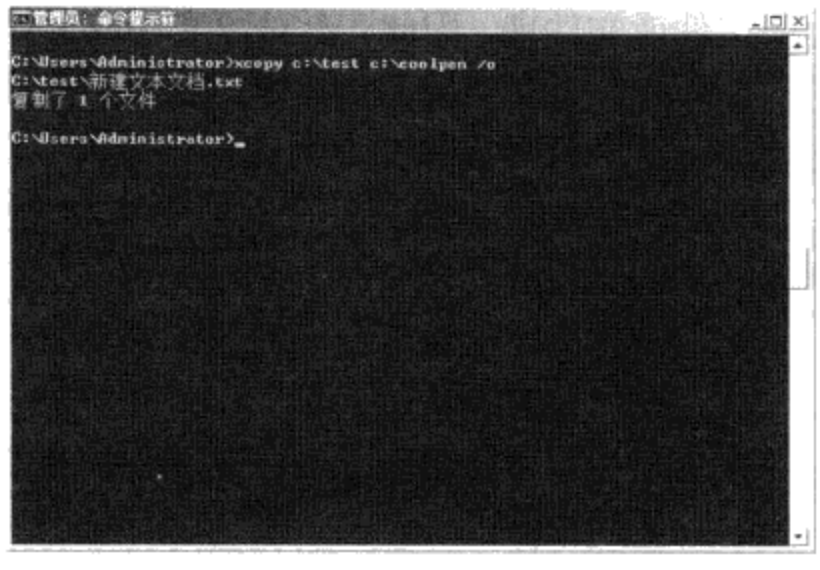


图 4-16 复制目录以及文件的 ACL 信息

命令行成功执行，将 rawdata 目录下的所有文件全部复制到目标目录中。同时复制目录以及文件的 ACl 信息到目标目录下的相应文件中。

4.3 文 件 审 核

通过配置 NTFS 权限审核策略，可以跟踪和记录用户对指定对象进行的操作，并生成可供管理员查阅的事件日志。默认情况下，Windows Server 2008 R2 系统并未开启任何审核策略，必要情况下，管理员可以打开和配置相应的审核事件类别，实现对客户端某些操作类型的审核。除了审核与安全有关的事件，还将生成安全日志，安全日志提供了查看日志中所报告的安全事件的方法。使用“事件查看器”可以查看安全日志。

4.3.1 访问控制列表概述

权限是与特定用户或组相关联的，或者是被管理员指派到用户和组的安全描述符。用户和组的每个权限的分配都会在系统中作为访问控制条目（ACE，Access Control Entries）显示，访问控制列表（ACL，Access Control Lists）就是这些访问控制条目的集合。如果 ACL 中不存在相应的 ACE，则系统将自动拒绝该用户账户访问相应资源。

访问控制列表有两种：任意访问控制列表（Discretionary ACL）和系统访问控制列表（System ACL）。任意访问控制列表包含用户和组的名称列表及其相应的权限，例如允许或拒

绝等。系统访问控制列表是为审核服务的，包含对象被访问的时间。

访问控制条目包含用户或组的 SID 以及对象的权限。访问控制项有两种：允许访问和拒绝访问，其中拒绝访问的优先级高于允许访问。当使用管理工具列出对象的访问权限时，列表的排序是以文字为顺序的，并不像防火墙的规则那样由上往下的顺次执行，访问控制条目中的权限是永远不会冲突的，并且拒绝访问总是优先于允许访问的。

用户通过验证后，登录进程会分配给用户一个访问令牌，该令牌相当于用户访问系统资源的票证，即当用户试图访问系统资源时，将访问令牌提供给 Windows Server 2008 R2 系统，系统将收到的访问令牌与目标资源的访问控制列表核对。如果用户被允许访问该对象，Windows Server 2008 R2 将会分配给用户适当的访问权限，否则用户将无法访问指定资源。

4.3.2 启用审核策略

配置文件审核之前必须先配置本地安全策略中的“审核策略”。以管理员账户登录文件服务器，打开“本地安全策略”窗口，依次展开“安全设置”→“本地策略”→“审核策略”选项，双击“审核对象访问”策略，显示“审核对象访问 属性”对话框，选中“成功”和“失败”复选框，如图 4-17 所示。

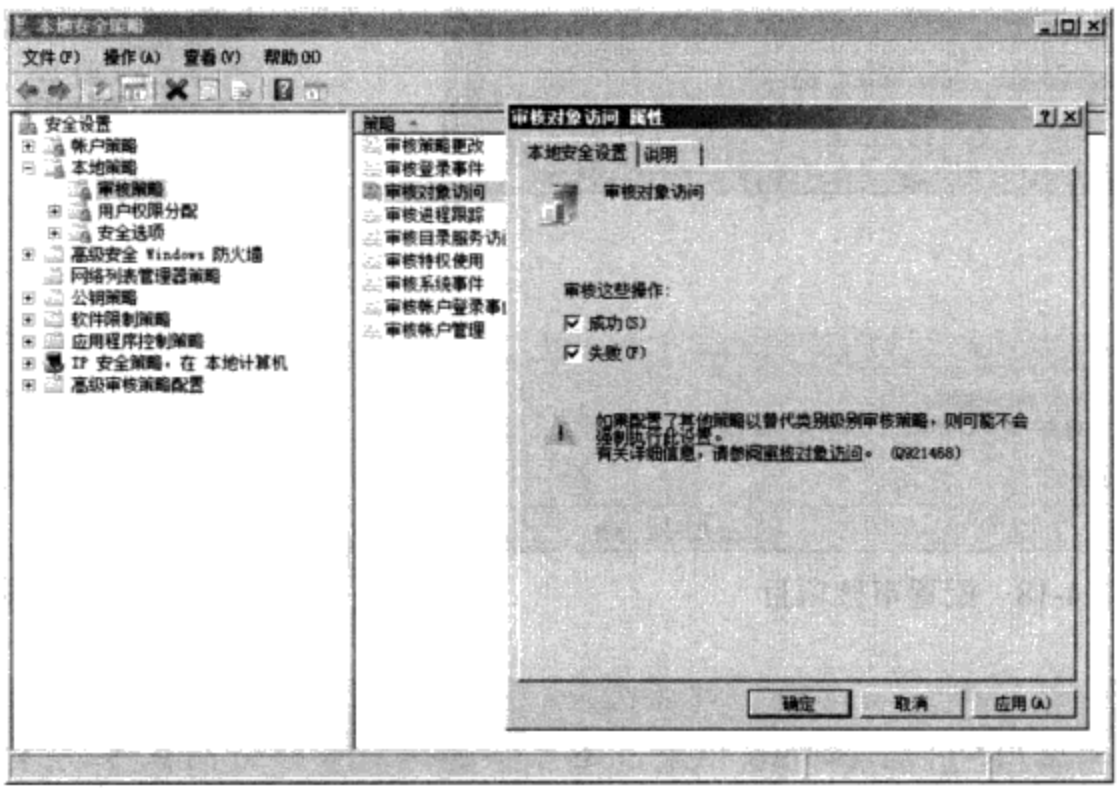


图 4-17 配置审核策略

最后，单击“确定”按钮，保存配置即可。

4.3.3 配置审核项目

管理员可以通过设置权限类型将审核策略应用于目标资源上，在安全日志中记录成功访问或失败访问尝试的系统事件，便于管理员更详细的了解用户对目标资源的访问情况。对文件和文件夹访问的审核，首先要求目标资源必须位于 NTFS 分区上，其次必须为对象访问事件设置审核策略。符合以上条件，即可对特定的文件或文件夹进行审核，并且设置对哪些用户或组指定哪些类型的访问事件进行审核。

第1步，在Windows资源管理器中，右击test文件夹并选择快捷菜单中的“属性”选项，打开“test 属性”对话框，切换到“安全”选项卡。单击“高级”按钮，打开“test 的高级安全设置”对话框，切换到“审核”选项卡。默认情况下，此时只能查看当前的审核项目设置情况，单击“编辑”按钮，才修改当前文件夹的审核项目，如图4-18所示。

第2步，单击“添加”按钮，在“选择用户或组”对话框中，输入希望被审核的用户账户或组。单击“确定”按钮，配置希望审核的用户权限，并选中“成功”或“失败”复选框，也可同时选择两者，主要用于设置系统审核日志的记录条件，如图4-19所示。例如，选择“读取属性”后的“成功”复选框，则系统将只审核用户账户hstjl读取目标资源成功的系统事件，而该读取失败的尝试或其他账户的访问均不会被审核。

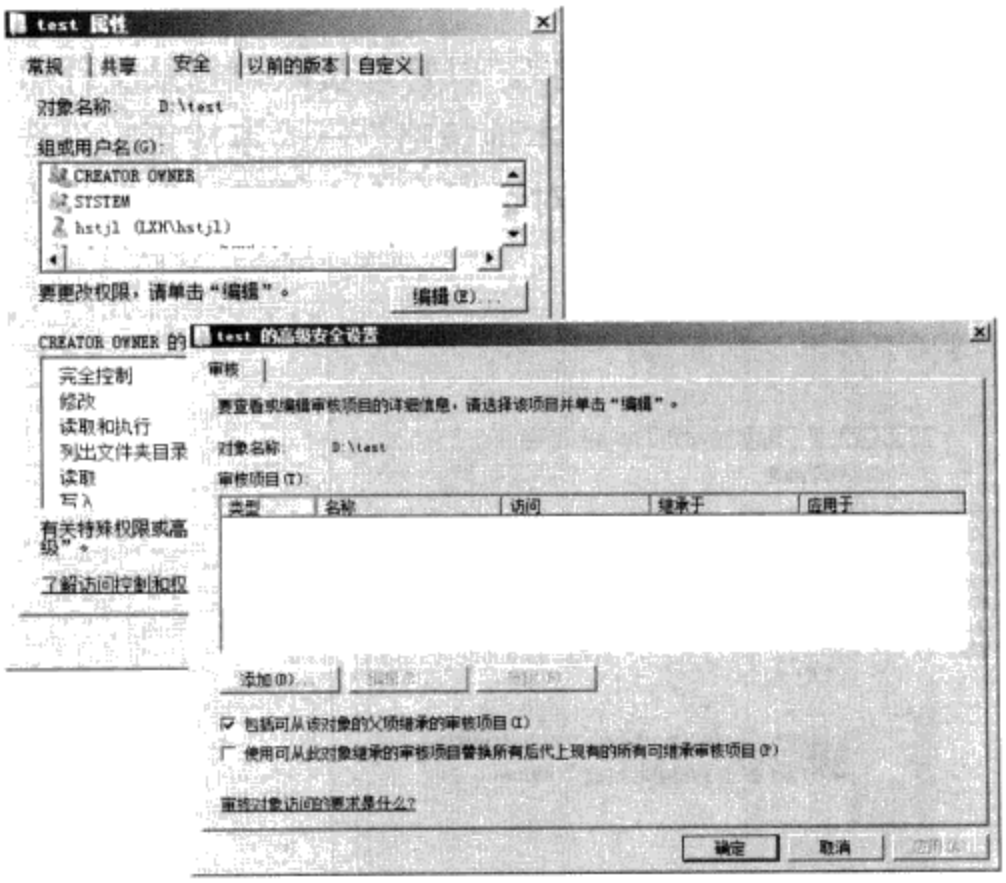


图4-18　配置审核项目

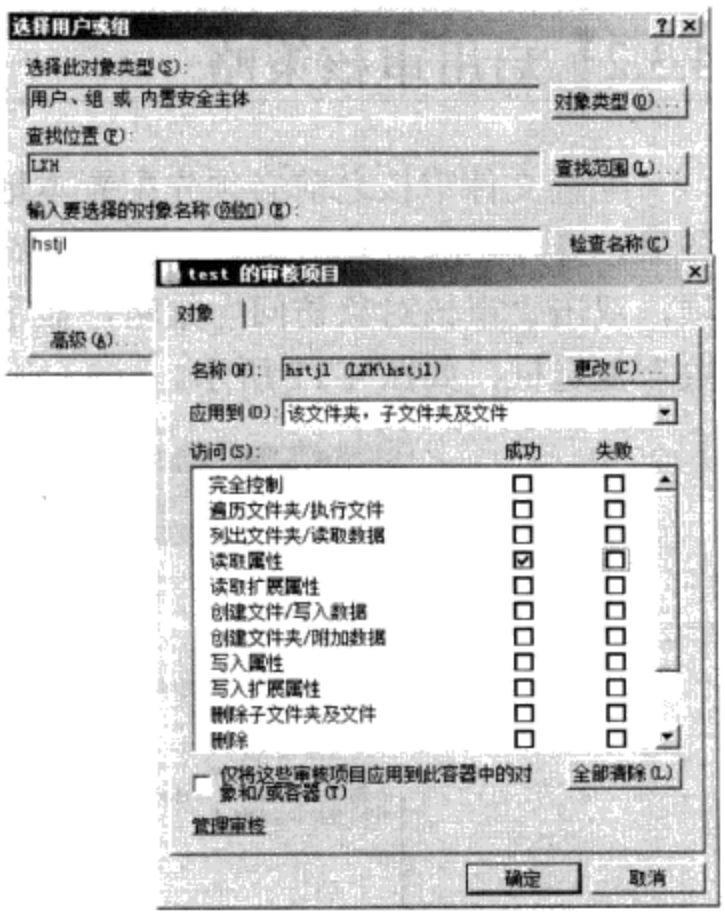


图4-19　设置审核的访问类型

提示

在“应用到”下拉列表框中，还可以选择被审核访问权限的作用目标，默认为“该文件夹，子文件夹及文件”，此处的可选项包括：

- 只有该文件夹。
- 该文件夹，子文件夹及文件。
- 该文件夹及子文件夹。
- 该文件夹及文件。
- 只有子文件夹及文件。
- 只有子文件夹。
- 只有文件。

第3步，连续单击“确定”按钮保存设置，即可完成审核设置。重复上述操作，可以设置用于其他账户或权限的审核。

注意

管理员可以通过“Windows 事件查看器”窗口，查看权限审核的日志。

4.3.4 选择审核项的应用位置

审核文件和文件夹时会出现“审核项目”对话框。在此对话框中，“应用到”列表显示了可以应用审核项目的位置。这些审核项应用的方式取决于是否选中了“将这些审核项目只应用到这个容器中的对象和/或容器上”。默认情况下，该复选框是清除的。

当“将这些审核项目只应用到这个容器中的对象和/或容器上”复选框未被选中时，审核目标如表 4-3 所示。

表 4-3 审核的应用范围

审核 / 应用到	当前文件夹	当前文件夹中的子文件夹	当前文件夹中的文件	所有后续子文件夹	所有后续子文件夹中的文件
仅此文件夹	Y	N	N	N	N
此文件夹、子文件夹和文件	Y	Y	Y	Y	Y
此文件夹和子文件夹	Y	Y	N	Y	N
此文件夹和文件	Y	N	Y	N	Y
仅子文件夹和文件	N	Y	Y	Y	Y
仅子文件夹	N	Y	N	Y	N
仅文件	N	N	Y	N	Y

当选中“将这些审核项目只应用到这个容器中的对象和/或容器上”复选框时，审核目标如表 4-4 所示。

表 4-4 审核的应用范围

审核 / 应用到	当前文件夹	当前文件夹中的子文件夹	当前文件夹中的文件	所有后续子文件夹	所有后续子文件夹中的文件
仅此文件夹	Y	N	N	N	N
此文件夹、子文件夹和文件	Y	Y	Y	N	N
此文件夹和子文件夹	Y	Y	N	N	N
此文件夹和文件	Y	N	Y	N	N
仅子文件夹和文件	N	Y	Y	N	N
仅子文件夹	N	Y	N	N	N
仅文件	N	N	Y	N	N

4.3.5 配置全局对象访问审核

在 Windows Server 2008 R2 系统中新增了多项审核策略，其中就包括“全局对象访问审核”，可以帮助管理员实现对全局对象访问的审核，审核范围更广泛。“全局对象访问审核”包括“文件系统”和“注册表”两条策略，可以为文件系统或注册表定义每种对象类型的计算机

SACL，然后将指定的 SACL 自动应用于该类型的每个对象。

第 1 步，在“本地安全策略”窗口中，依次展开“高级审核策略配置”→“系统审核策略”→“全局对象访问审核”选项，双击“文件系统”策略，打开如图 4-20 所示“文件系统 属性”对话框，选中“定义此策略设置”复选框即可启用该审核策略。

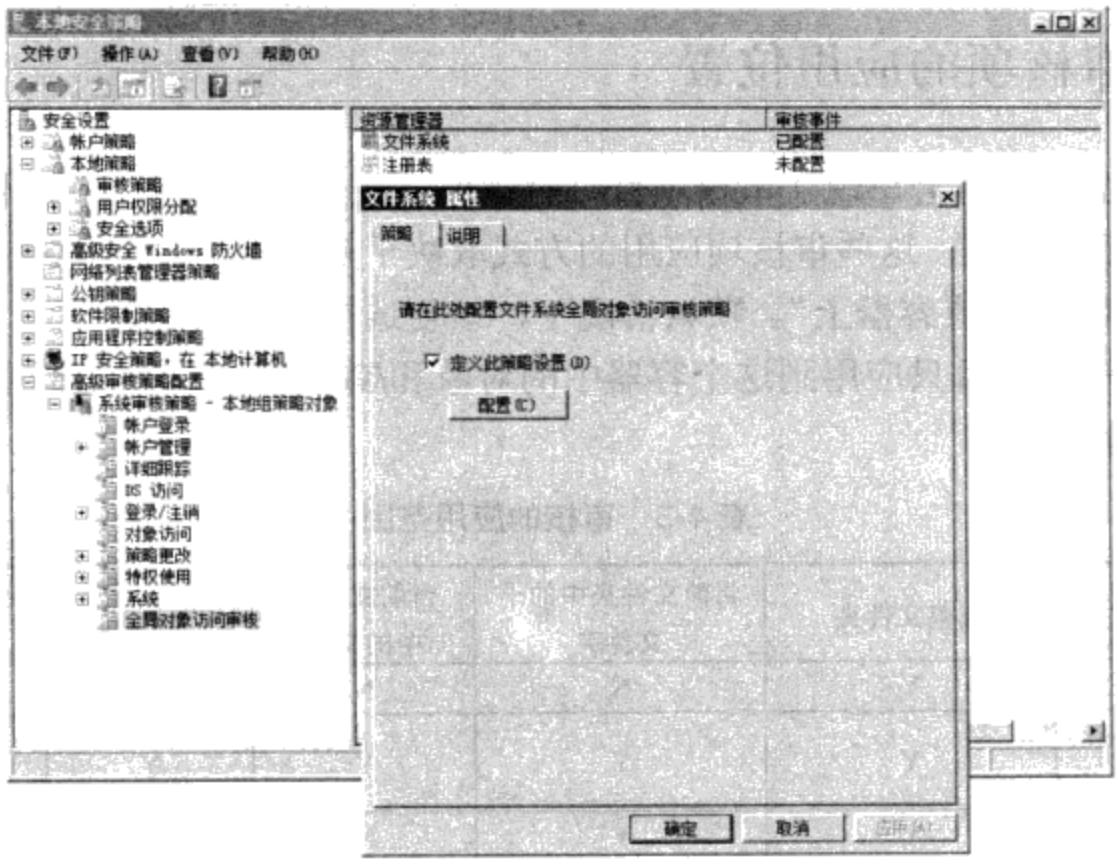


图 4-20 启用“全局对象访问审核”策略

第 2 步，单击“配置”按钮，显示“全局文件 SACL 的高级安全设置”对话框，系统默认没有任何审核项目。单击“添加”按钮，添加本地或域中相应的用户账户或组即可，如图 4-21 所示。

第 3 步，单击“确定”按钮，显示如图 4-22 所示“全局文件 SACL 的审核项目”对话框，设置需要进行审核的访问类型即可。与配置普通“审核对象访问”策略不同的是，这些审核项目仅能应用到选定的对象本身，而不涉及其包含的对象。

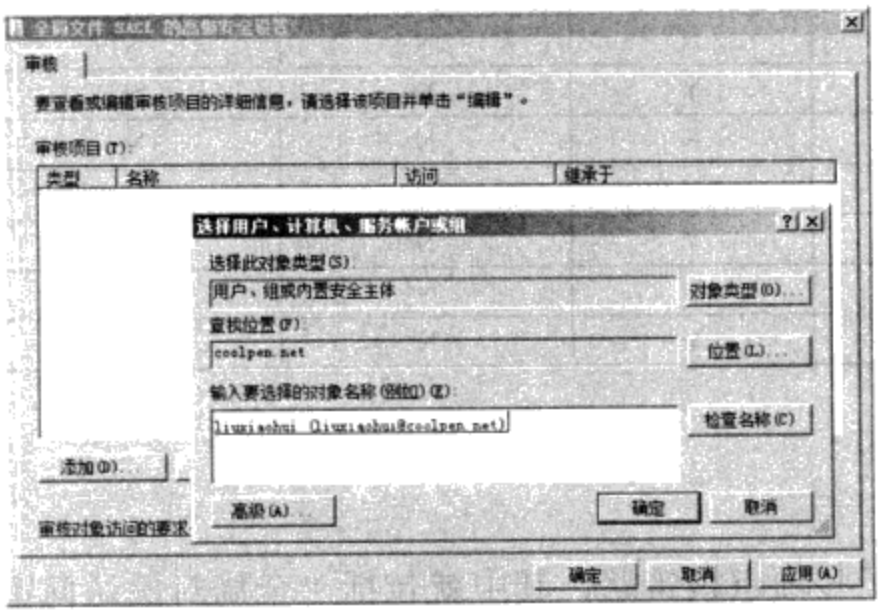


图 4-21 添加审核项目

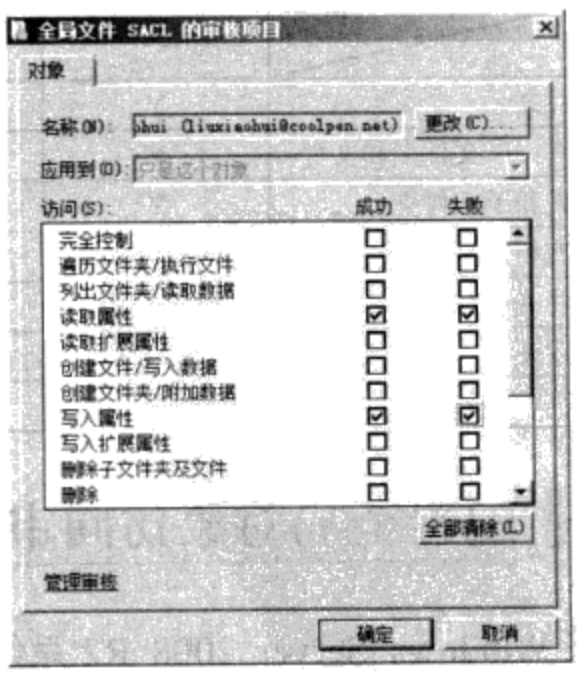


图 4-22 “全局文件 SACL 的审核项目”对话框

注·意 如果在计算机上同时配置了文件或文件夹 SACL 和全局对象访问审核策略，可能会造成意外的结果。因此，不应该将两组审核策略设置组合使用。配置高级审核策略之后，应启用“本地策略”→“安全选项”下的“审核：强制审核策略子类别设置（Windows Vista 或更高版本）替代审核策略类别设置”策略设置。这将通过强制忽略基本安全审核来防止类似设置之间的冲突。

4.4 磁盘配额

如果要在已经使用的磁盘中启用磁盘配额功能，Windows Server 2008 将计算到启动时间点为止，在该卷中复制文件、保存文件、或取得文件所有权的所有用户，使用的磁盘空间。根据统计结果，自动为每个用户 设置配额限度和警告级别。当然，管理员可以为某个或多个用户设置不同的配额或禁用配额。另外，也可以为还没有在卷上复制文件、保存文件和取得文件所有权的 用户设置磁盘配额，或者在一个新创建的卷上启用磁盘配额功能。

4.4.1 启动磁盘限额

在默认的情况下，磁盘配额是没有启用的。启动磁盘配额的操作步骤如下。

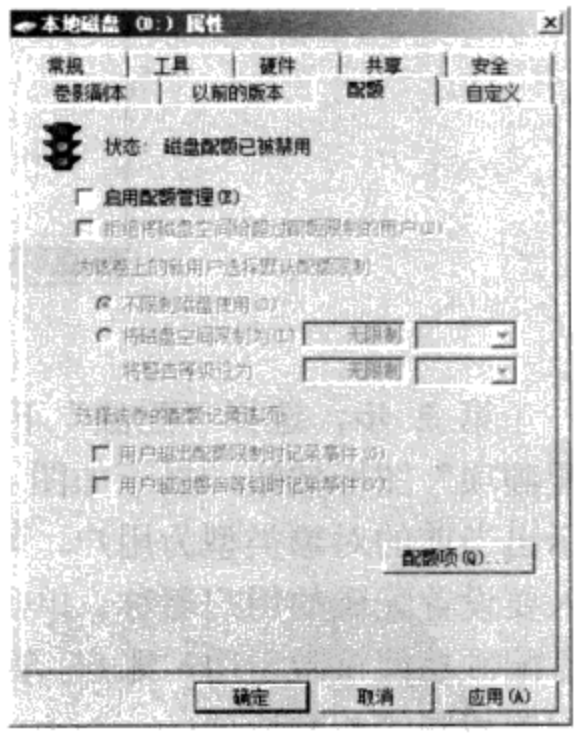


图 4-23 “配额”选项卡

第 1 步，在 Windows 资源管理器中，右击想要启用配额功能的 NTFS 卷（如本地磁盘 D:），并选择快捷菜单中的“属性”，打开“本地磁盘（D:）属性”对话框，切换到如图 4-23 所示“配额”选项卡，选中“启用配额管理”复选框，即可启用磁盘配额管理。

选择其中相应的各个选项，以配置系统的磁盘配额功能。

- 选中“拒绝将磁盘空间给超过配额限制的用户”选项，超过其配额限制的用户，将收到来自 Windows 的“磁盘空间不足”的错误信息，并且在没有从中删除和移动一些现存文件的情况下，无法将额外的数据写入卷中。如果清除该复选框，则用户可以超过其配额限制。
- 选中“将磁盘空间限制为”选项，并输入允许卷的新用户使用的磁盘空间数量，以及在将事件写入系统日志前已经使用的磁盘空间量。网络管理员可以在“事件查看器”中查看这些事件信息。在磁盘空间和警告级别中可以使用十进制数值，从下拉列表框中选择适当的单位（如 KB、MB、GB 等）。
- 选中“用户超出配额限制时记录事件”选项。此时如果启用配额，则只要用户超过其配额限制，事件就会写入到本地计算机的系统日志中。管理员可以用“事件查看器”，通过筛选磁盘事件类型来查看这些事件。默认情况下，配额事件每小时都会被写入

本地计算机的系统日志中。

- 选中“用户超过警告等级时记录事件”选项。此时如果启用配额，则只要用户超过其警告级别，事件就会写入到本地计算机的系统日志中。管理员可以用事件查看器，通过筛选磁盘事件类型来查看这些事件。默认情况下，配额事件每小时都会被写入本地计算机的系统日志中。

第2步，单击“确定”按钮，保存所做设置，启用磁盘配额完成。

第3步，启用磁盘配额管理后，所有的用户都使用磁盘配额启动时设置的默认配额限制和配额警告级别。使用配额项目管理可以为每一个用户设置适合的磁盘配额，对用户的磁盘配额设置进行维护，并且可以记录每一个用户对磁盘空间的使用情况。

4.4.2 为用户配置磁盘配额

若让某一个用户使用更多的空间，可以为该用户单独制定更大的磁盘配额。

第1步，在“驱动器属性”对话框中，打开“配额”选项卡，单击“配额项”按钮，显示如图4-24所示“（D:）的配额项”窗口。

图4-24 “（D:）的配额项”窗口

第2步，选择“配额”下拉菜单中的“新建配额项”命令，或者单击工具栏中的“新建配额项”图标按钮，显示如图4-25所示“选择用户”对话框。在“选择地对象类型”栏中显示出当前的对象类型为用户，可采用系统的默认值。在“输入对象名称来选择”文本框中，输入要设置配额的用户名称。单击“检查名称”按钮，检查输入的用户账户是否存在。注意，磁盘配额功能仅限于用户账户，管理员不能对用户组进行磁盘配额设置，但可以同时为多个用户配置相同的配额选项。

第3步，单击“确定”按钮，显示如图4-26所示“添加新配额项”对话框。选中“将磁盘空间限制为”单选按钮，并在其后文本框中为该用户设置访问磁盘的空间。

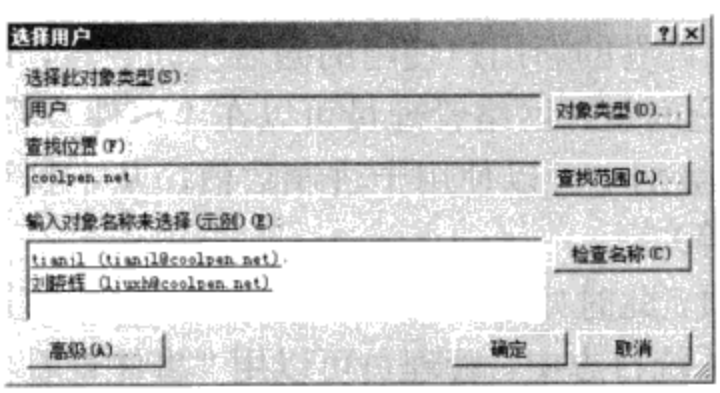


图4-25 “选择用户”对话框

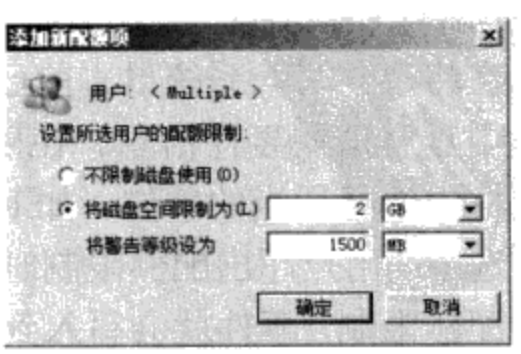


图4-26 “添加新配额项”对话框

第 4 步，单击“确定”按钮，保存用户的磁盘配额设置，提示启用配额系统会导致卷重新被扫描，如果已经存储的文件较多则可能需要几分钟的时间。

如果想删除指定用户的配额项，可选择用户名，右击并选择快捷菜单中的“删除”选项即可。

使用指定配额项具有以下优点：

- 登录到相同计算机的多个用户之间互不影响。
- 一个或多个用户不独占公用服务器上的磁盘空间。
- 在个人计算机的共享文件夹中，用户不使用过多的磁盘空间。

4.4.3 监控每个用户的磁盘配额使用情况

当为用户设置好磁盘配额以后，除了可以借助“日志查看器”浏览磁盘占用情况外，在配额项窗口中，也可以监视每个用户的磁盘配额使用情况，并可单独设置每个用户可使用的磁盘空间。也就是说配额项的主界面就是一个用户配额监控器。

若欲更改某一个用户的磁盘配额设置，可右击该用户，选择快捷菜单中的“属性”选项，显示如图 4-27 所示“刘晓辉（liuxh@coolpen.net）的配额设置”对话框，可以更改用户的磁盘空间限制及警告等级。

图 4-27 “刘晓辉（liuxh@coolpen.net）的配额设置”对话框

4.5 共享资源安全

共享资源是众多网络资源中的一部分，单位了确保这些资源的安全，只能允许网络上的部分用户在一定限度内访问和使用，这一限制就可以通过设置共享访问权限来实现。前面已经介绍过如何通过配置 NTFS 访问权限保护本地文件的安全，对于共享资源而言，完全可以借助 NTFS 权限和共享访问权限配合使用，配置更加安全的共享资源。

4.5.1 共享访问权限

共享资源提供对应用程序、数据或用户个人数据的访问。既可以直接设置共享权限，也可以使用 NTFS 文件系统上的访问控制，还可以将这些方法结合起来使用。直接设置共享权限时，易于应用和管理；借助 NTFS 权限时，可以对共享资源及其内容进行更详细的控制。结合使用时，将应用更为严格的权限。例如，如果共享权限设置为“Everyone=读取”（默认值）并且 NTFS 权限允许用户更改共享文件，则将应用共享权限，不允许用户更改文件。

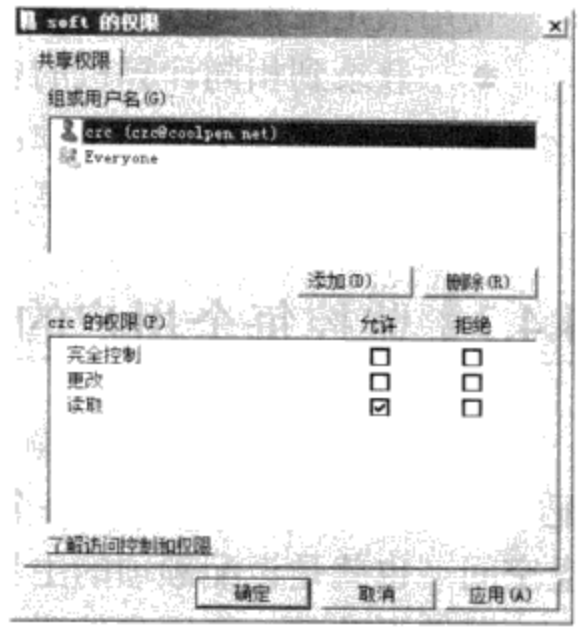


图 4-28 Soft 的权限

除了可以直接登录到服务器访问资源外，还可以通过共享文件夹访问网络远程共享资源。因此，除了设置 NTFS 权限外，还需要设置共享文件夹权限。在“高级共享”对话框中，单击“权限”按钮，即可显示“Soft 的权限”对话框，显示并设置该共享文件夹的权限，如图 4-28 所示。

提示 通常情况下，只有在想要覆盖已指派的特定权限时，才会使用拒绝权限。另外，当创建新的共享资源时，会自动指派 Everyone 组为读取权限，这种权限是最受限制的权限。

共享文件夹权限具有以下特点：

- 共享文件夹权限只适用于文件夹，不适用于单独的文件；只能为整个共享文件夹设置共享权限，而不能对该共享文件夹中的文件或子文件夹进行设置。所以，共享文件夹权限不如 NTFS 文件系统权限详细。
- 共享文件夹权限并不对直接登录到计算机上的用户起作用，只适用于通过网络连接该文件夹的用户。也就是说，共享权限对直接登录到服务器上的用户是无效的。
- 在 FAT/FAT32 系统卷上，共享文件夹权限是保证网络资源被安全访问的唯一方法。
- 默认的共享文件夹权限是读取，并被指定给 Everyone 组。

共享权限分为读取、修改和完全控制。不同访问权限以及对用户访问能力的控制如表 4-5 所示。

表 4-5 共享文件夹的权限以及对用户访问能力的控制

权限	允许用户完成的操作
读取	显示文件夹名称、文件名称、文件数据和属性，运行应用程序文件，以及改变共享文件夹内的文件夹
修改	创建文件夹，向文件夹中添加文件，修改文件中的数据，向文件中追加数据，修改文件属性，删除文件夹和文件，以及执行“读取”权限所允许的操作
完全控制	修改文件权限，获得文件的所有权。 执行“修改”和“读取”权限所允许的所有任务。默认情况下，Everyone 组具有该权限

共享文件夹权限的多重权限与 NTFS 文件系统权限相似，请参考上述相关内容。在管理共

享文件夹和指定共享文件夹权限时，应当注意以下几个方面的问题。

- 确定每个资源有哪些组需要访问，以及这些组对每个资源各自不同的权限级别。
- 为资源指定最严格的权限，只要允许用户完成所需要的任务即可。
- 在组织资源时，将对安全性要求相同的文件夹放在一个文件夹中。例如，如果用户需要拥有几个文件夹的读取权限，那么，最好将这些应用文件夹存放在同一文件夹，然后再共享这个文件夹，而不是单独地共享每个文件夹。
- 使用直观的共享名，便于用户识别并找到所需要的资源。
- 把权限指派给组而不是用户账户，既可简化对访问权限的管理难度，又可避免权限分配出现问题。把权限指派给组易于管理共享资源，因为不用重新指派权限，只需将用户从组中添加或删除即可。若欲拒绝对共享资源的所有访问，则拒绝完全控制权限即可。
- 指派最具限制的权限，该权限仍允许用户执行需要的任务。例如，如果用户仅需读取文件夹中的信息并且从不删除、创建或更改文件，应当指派“读取”权限。
- 如果用户通过网络远程登录主机访问共享资源（如终端服务器、远程桌面等），则用NTFS 文件系统权限或访问控制设置权限即可。
- 共享权限只适合通过网络访问共享资源的用户，并不适用于本机登录的用户。可以和NTFS 权限、访问控制等措施同时使用。
- 组织资源使安全性要求相同的对象定位于同一个文件夹中。例如，如果用户需要几个应用程序文件夹的“读取”权限，可将应用程序文件夹存储在同一个父文件夹中。然后，共享该父文件夹，而不是共享每个应用程序文件夹。需要注意的是，如果需要更改应用程序的位置，可能需要重新安装。
- 当共享应用程序时，将全部共享的应用程序组织在一个文件夹中。
- 将全部的应用程序组织在一个共享文件夹中可简化管理，因为这样仅有一个用来安装和升级软件的位置。
- 为了避免在访问网络资源时可能会出现的问题，建议不要为 Everyone 组设置“拒绝”权限。避免显式地给共享资源分配拒绝权限，只有在覆盖已分配的指定权限时，才有必要显式地分配拒绝权限。
- Everyone 组包括任何可以访问网络资源的用户（包括 Guest 账户），但不包括 Anonymous Logon 组。
- 限制 Administrators 组中授予其“完全控制”权限的成员数量，从而既保证管理员能管理应用软件和控制用户权利，又不会因为拥有较高权限的用户数量太多，而导致对访问权限的滥用。
- 通常情况下，建议不要更改 Everyone 组的默认权限（读取），也不要擅自更改共享资源的默认位置。
- 尽量使用域用户账户授予用户访问权限。
- 已加入域的计算机，尽量通过域用户账户授权访问共享资源，而不是通过本地用户账户，从而实现对共享权限的集中管理。
- 使用集中数据文件夹，可以方便地管理资源和备份数据。
- 为共享资源使用直观的注释，确保用户和所有客户端操作系统容易识别和访问共享资源。

- 使用防火墙，阻止来自 Internet 的恶意访问，保护共享资源的安全。

4.5.2 共享访问权限与 NTFS 权限

共享文件夹权限和 NTFS 权限是可以叠加的。共享文件夹权限为资源提供有限的安全性，而 NTFS 权限为共享文件夹提供最大的灵活性。不论是在本地访问访问资源，还是通过网络访问该资源，NTFS 权限都是非常有用的。因此，除了设置 NTFS 权限外，还需要设置共享文件夹权限。

当管理员对 NTFS 权限和共享文件夹的权限进行组合时，组合结果所产生的权限或者是组合的 NTFS 权限，或者是组合的共享文件夹权限，哪个范围更窄、更严格就是哪一个。

例如，Folder 文件夹是 NTFS 分区上的共享文件夹。共享文件夹权限为写入；NTFS 权限为读取。网络用户最终的访问权限即为读取，而不允许写入操作，如图 4-29 所示。这样可以更加有效地确保网络安全。

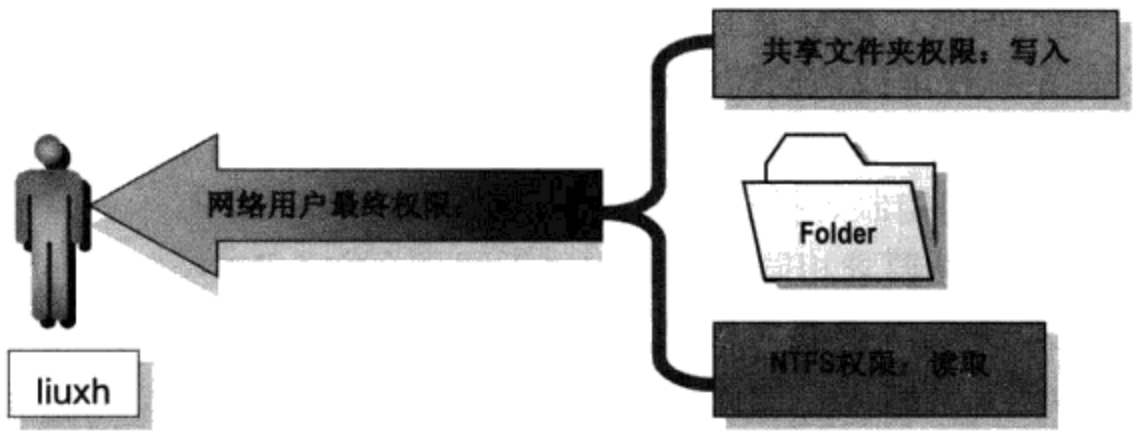


图 4-29 共享文件夹权限 NTFS 权限叠加

当在 NTFS 卷上为共享文件夹授予共享权限时，应当遵守下述规则：

- 可以对共享文件夹中的文件和子文件夹应用 NTFS 权限。可以对共享文件夹中包含的每个文件和子文件夹应用不同的 NTFS 权限。
- 除共享文件夹权限外，用户必须要有该共享文件夹包含的文件和子文件夹的 NTFS 权限，才能访问那些文件和子文件夹。在 FAT 卷上，共享文件夹权限是保护该共享文件夹中的文件和子文件夹的唯一权限。
- 在 NTFS 卷上必须要求 NTFS 权限。默认情况下，Everyone 组具有“完全控制”权限。

4.6 默认共享安全

默认共享主要是为了方便网络管理员管理网络中的计算机，特别是在基于域的网络中，专门有几个默认共享用于存储用户配置文件是非常方便的。但是，默认共享在方便管理的同时，也给计算机的安全埋下了重大安全隐患。如果知道了管理员账户和密码，任何人都能访问计算机，所以如果管理员账户密码恶意用户窃取，对于计算机的安全来说是非常不利的。

4.6.1 查看默认共享

默认共享是为了方便管理员远程管理而默认开启的共享（当然可以关闭它），即所有的逻

辑磁盘（C$，D$，E$……）和系统目录 Windows NT 或 Windows（Admin$），通过 IPC$连接可以实现对这些默认共享的访问。

1. 命令行方式

如果想要查看本地计算机目前所打开的默认共享，可以在本地计算机的命令提示符下，使用 Net Share 命令来查看系统目前所有的共享的目录。在这些所列出的共享目录中，不但包括默认共享，还包括系统除默认共享以外的所有共享目录。

具体操作过程如下。

在命令行提示符下，键入：

```
Net share
```

按 Enter 键，命令成功执行，如图 4-30 所示。

在这里所显示就是系统的所有共享目录，这里主要包括 IPC$默认共享、逻辑磁盘共享“D$、C$”，系统目录共享“ADMIN$”。

2. 图形窗口方式

如果用户对在命令提示符下的操作不是很熟悉的话，还可以使用图形方式，查看目前系统的默认共享目录。

第 1 步，以管理员账户登录系统，依次选择“开始”→“管理工具”→“计算机管理”选项，打开“计算机管理”窗口，依次展开“系统工具”→“共享文件夹”→“共享”选项，如图 4-31 所示。

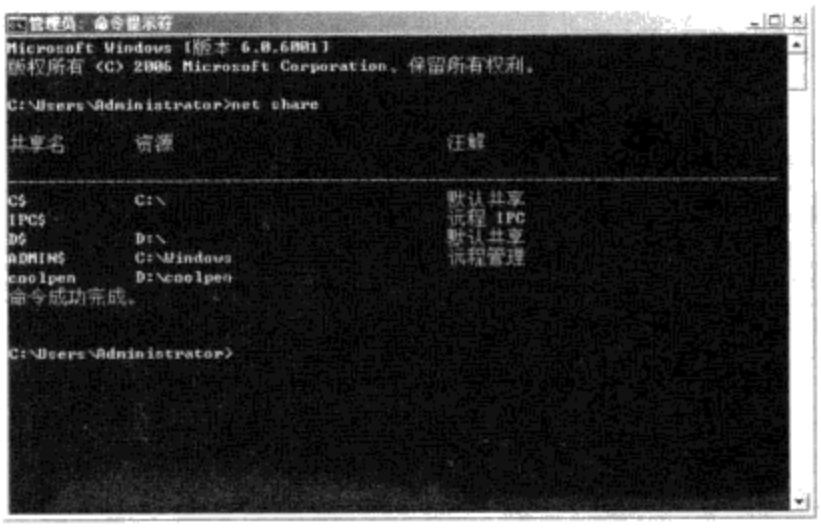


图 4-30 Net Share 的执行结果

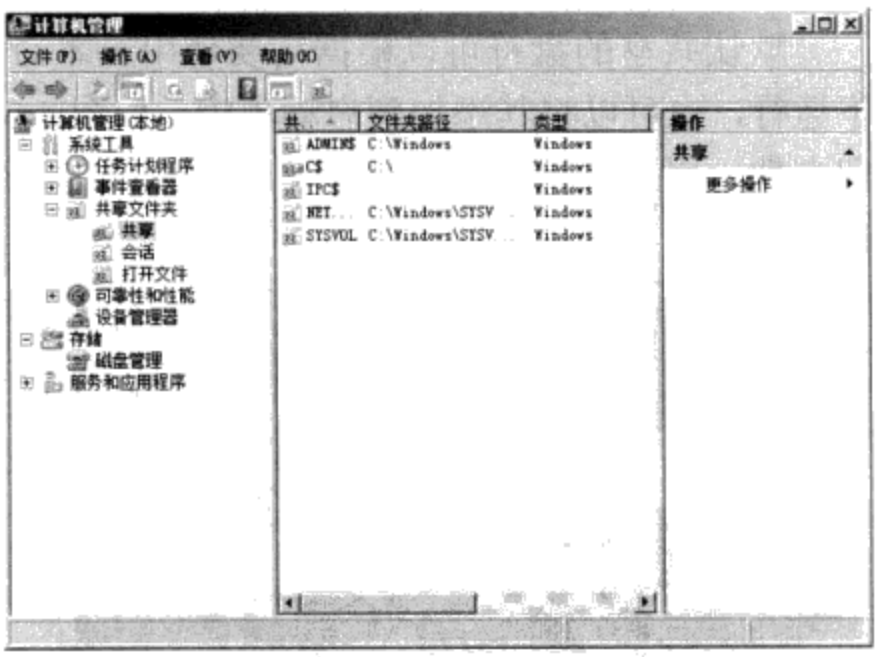


图 4-31 共享文件夹

第 2 步，选择“共享”选项，在右侧的共享列表框中，可以查看本地计算机上已经设置的默认共享。

4.6.2 停止默认共享

如果在网络中没有使用默认共享的必要，建议用户将系统的默认共享关闭，从而进一步

的保证计算机的安全。

1. 使用 Net share 命令

首先，介绍如何在命令提示符下，使用命令停止系统的默认共享，所使用的命令为“Net Share”。

具体操作过程如下。

在命令行提示符下，键入：

```
NET SHARE Admin$ /DELETE
```

按 Enter 键，命令成功执行，即可停止共享，如图 4-32 所示。

其中 D$表示系统默认共享 D 盘，其他如 C$、ADMIN$、IPC$等都可以使用此种格式删除。

在“/DELETE”前必须要有空格。可以使用“NET SHARE ADMIN$”或“NET SHARE IPC$”建立“ADMIN$”或“NET SHARE IPC$”共享（如果共享存在，则为显示共享），但需要注意的是，其他共享则不能使用该方法来建议默认共享。

如果需要删除所有的默认共享，可以使脚本命令（批处理文件方式）完成（即扩展名为“.bat”的文件）：

```
Net share IPC$ /delete
Net share Admin$ /delete
Net share C$ /delete
Net share D$ /delete
……
```

默认共享的盘符可以根据需要使用脚本命令分别删除，该批处理文件可以在命令提示符下运行，也可以将其添加到启动项中，如图 4-33 所示。这里创建一个名为“share.bat”的批处理文件，用以将系统的默认共享删除，并在命令提示符下运行。

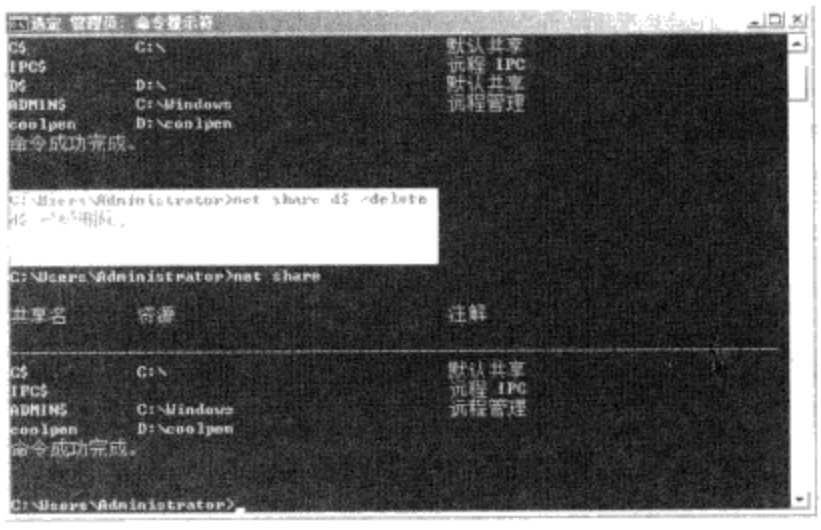


图 4-32 删除 D$默认共享

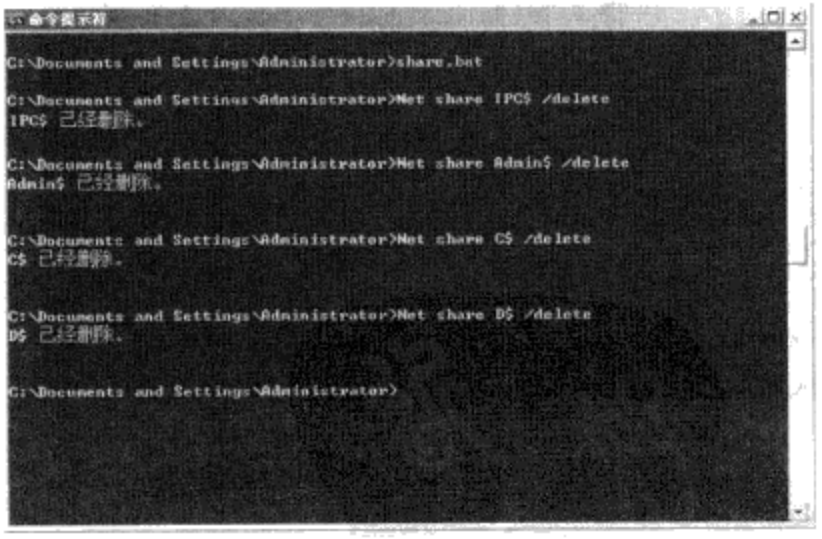


图 4-33 在命令提示符下运行批处理文件

2. 关闭 Server 服务

默认共享使用的是计算机系统的 Server 服务，如果将该服务直接关闭，就可以直接删除默认共享。

第 1 步，依次选择“开始”→“管理工具”→“服务”选项，打开“服务”窗口，双击“Server”服务，打开“Server 的属性（本地计算机）”对话框，如图 4-34 所示。在“启动类型”下拉列表框中，选择“手动”选项，以免再次重新启动系统时服务随之启动。

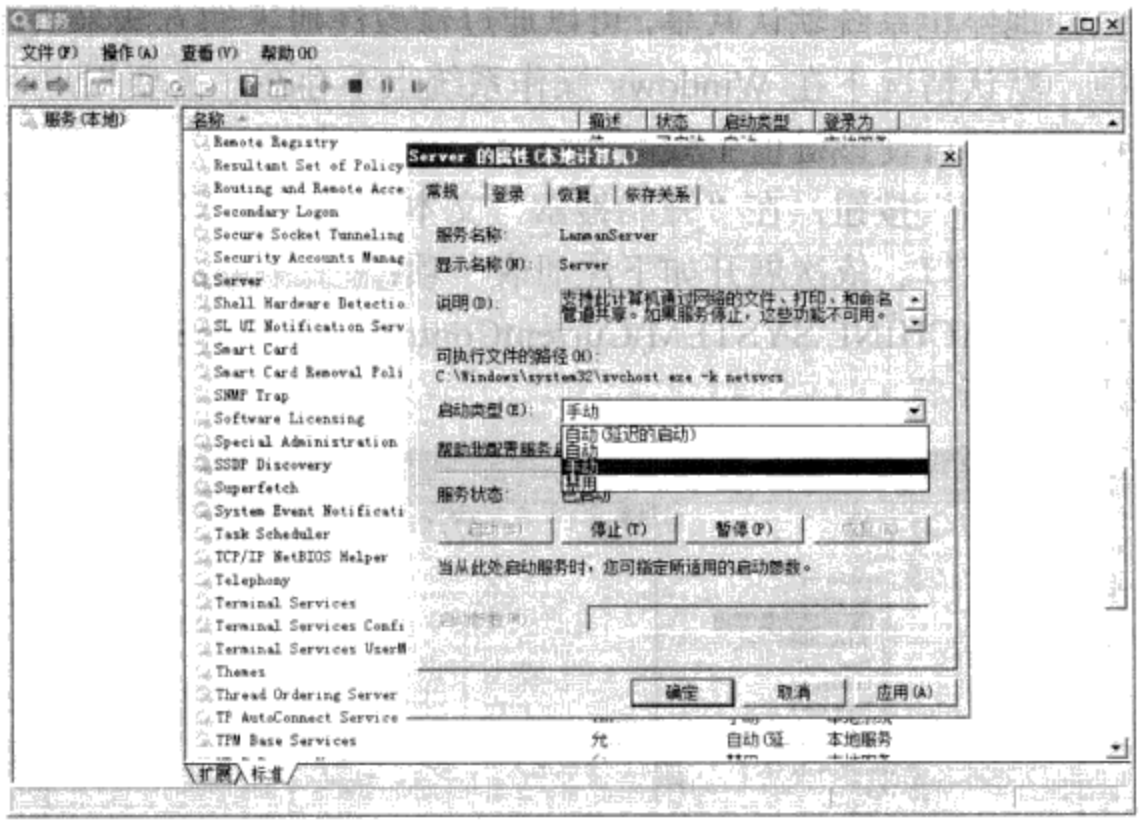


图 4-34 “Server 的属性”对话框

第 2 步，单击“停止”按钮，显示如图 4-35 所示“服务控制”对话框，开始停止“Server”服务。

第 3 步，单击“确定”按钮，即可停止 Server 服务。再次打开命令提示符窗口，输入如下命令：

```
Net share
```

按 Enter 键，显示如图 4-36 所示结果，提示 Server 服务没有启动，直接输入 n 并按 Enter 键即可。

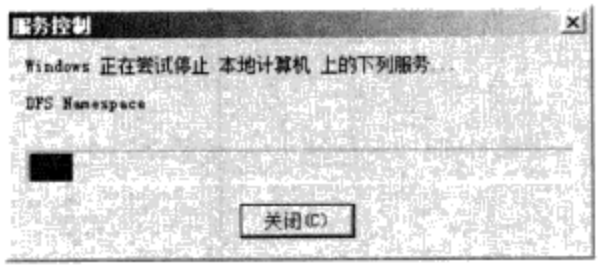


图 4-35 “服务控制”对话框

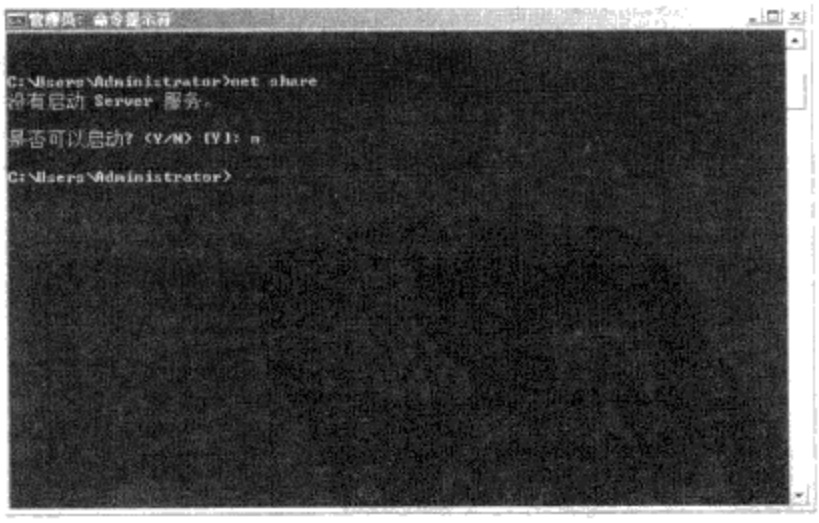


图 4-36 关闭 Server 服务后

使用这种方法停止默认共享后，其他共享也将同时被取消，应慎重选择。

3. 修改注册表

使用前面两种方法停止完成系统默认共享，当系统重新启动后，默认共享会重新恢复。如果用户需要永久性地停止系统默认共享，可以通过修改注册表的方法来实现该目的。停止系统默认共享的键值，默认情况下在 Windows 操作系统上不存在，需要用户手动添加该键值，修改后重新启动计算机即可使该键值生效。

第 1 步，单击“开始”按钮，在“开始搜索”文本框中，输入“regedit”并按 Enter 键，打开“注册表编辑器”窗口。依次展开如下注册表子项：

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Autotuned Parameters]，如图 4-37 所示。

图 4-37 展开的注册表项目

第 2 步，在右侧的空白窗口中，右击，在快捷菜单中选择“新建”选项，在子菜单中选择“Dword 值”选项，新建一个名为“AutoShareServer”的 DWORD 值，并将其赋值为：00000000，如图 4-38 所示。

图 4-38 创建 DWORD 值

4. Microsoft 网络的文件和打印机共享

除使用修改注册表的方法外，还可以使用卸载网卡相关属性的方法，同样也可以关闭默认共享。

第 1 步，在“控制面板”窗口中，打开如图 4-39 所示“网络和共享中心”窗口。

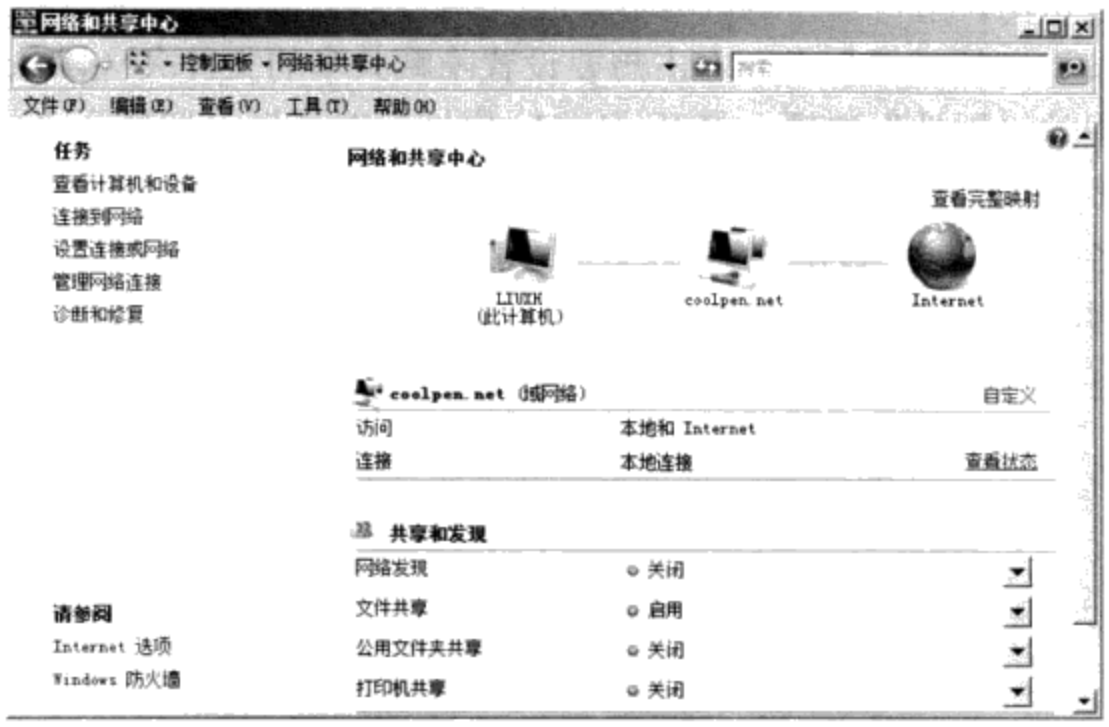


图 4-39 “网络和共享中心”窗口

第 2 步，单击“查看状态”按钮，打开“本地连接 状态”对话框，单击“属性”按钮，显示如图 4-40 所示“本地连接 属性”对话框。

第 3 步，选中“Microsoft 网络的文件和打印机共享”复选框，单击“卸载”按钮，系统提示确认删除信息，显示如图 4-41 所示“卸载 Microsoft 网络的文件和打印机共享”对话框。

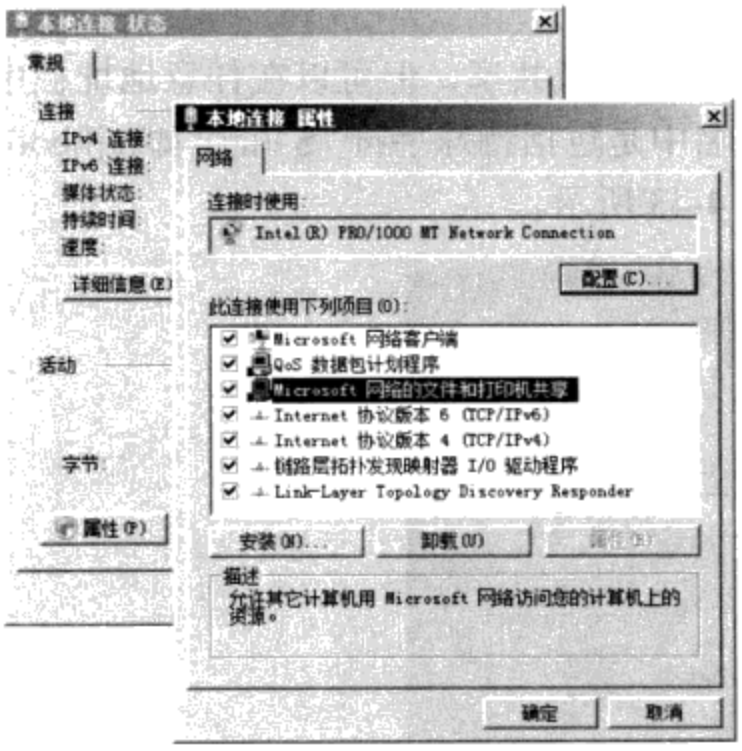


图 4-40 “本地连接 属性”对话框

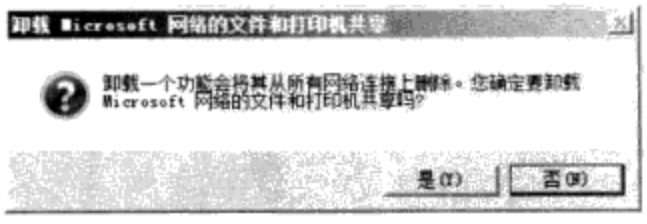


图 4-41 卸载信息提示

第 4 步，单击“是”按钮，即可完成“Microsoft 网络的文件和打印机共享”项目的卸载。

4.6.3 设置隐藏的共享

通常情况下，用户可以通过网上邻居查看或访问其他计算机上的共享资源，但其中并不包括隐藏共享。因此设置隐藏共享也是保护共享资源安全的一种常用方法，访问者必须使用准确的共享名才可以访问。

在“Windows 资源管理器”中，右击想要设置隐藏共享的文件夹（以 book 文件夹为例），并选择快捷菜单中的“属性”选项，打开“book 属性”对话框，切换至“共享”选项卡，单击“高级共享”按钮，打开如图 4-42 所示“高级共享”对话框。选中“共享此文件夹”复选框，并在“共享名”文本框中显示的默认名称后追加“$”，也可以设置其他共享名，但隐藏共享必须以“$”结尾。

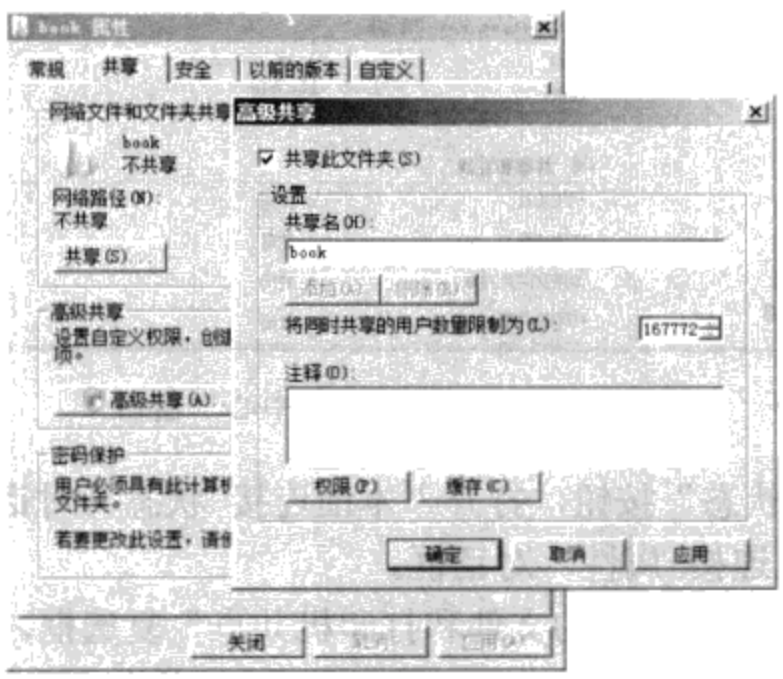


图 4-42　“高级共享”对话框

网络中的其他计算机无法直接通过资源管理器访问隐藏共享，但可以在任意地址栏中输入“\\服务器名\共享名”进行访问，注意此时的共享名中是包括特殊字符“$”的，如\\tjl\book$。此外，也可以通过映射网络驱动器直接访问，如图 4-43 所示。

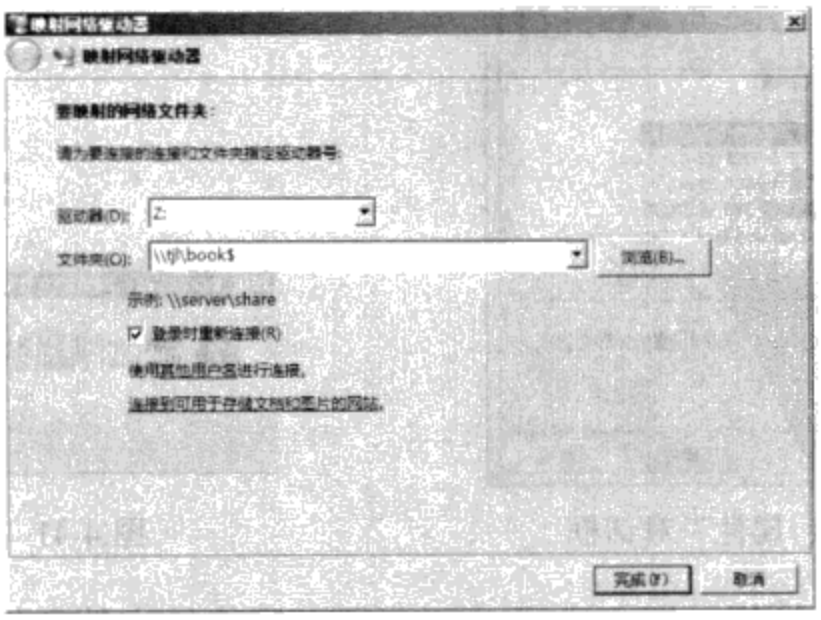


图 4-43　“映射网络驱动器”对话框

第 5 章　Internet 信息服务安全

Internet 信息服务（IIS）是企业网络中应用较多的服务，主要用于搭建 WWW 和 FTP 服务器，以及为其他网络服务提供所需的基础架构。Windows Server 2008 R2 系统中的 IIS 版本已经从 7.0 升级到 7.5，并且新增了多个功能模块。Web 和 FTP 站点往往都是暴露在开放的 Internet 环境中的，随时可能遭遇各种因素的安全威胁，因此，确保 IIS 服务器安全性的重要程度是可想而知的。

5.1　IIS 安全规划

尽管 IIS 7.5 本身已经提供多种安全功能，如果未能合理配置和应用，也无法确保 IIS 服务的安全。在实施 IIS 安全配置之前，应根据具体应用和实际环境进行合理规划，了解实际应用中将要面临的安全威胁，进而指定相应的安全策略。如果条件允许，应先在实验环境中试运行部署的安全策略，确认安全之后在应用到生产环境。

5.1.1　评估安全威胁

通常情况下，IIS 的主要功能就是搭建企业网站和文件传输，根据实际用途和应用环境的不同，可能面临的安全威胁也会有所不同。为了确保将来 Web 或 FTP 站点的安全运行，评估 IIS 安全威胁时应注意如下几点：

- 满足未来一段时期内应用业务的升级。根据企业为了纪念的发展规划，了解可能增加和升级的网络应用，是否对 Web 或 FTP 有新的需求等。
- 分清安全威胁的来源。根据安全威胁来源的不同，可以分为来自 Internet 的安全威胁和来自内部网络的安全威胁。针对不同的威胁来源，制订和实施的安全策略肯定是截然不同的。
- 划分威胁等级。为了确保制定和实施安全策略的顺利进行，应该依据潜在损失和恢复开销的不同，对安全威胁划分优先级。

1.　Windows 系统安全

Windows 系统是 IIS 服务运行的基础，如果系统本身就已经千疮百孔，为 IIS 制订的安全防护措施也会无济于事。尽管 Windows Server 2008 R2 系统在安全性方面的表现已经非常出色，但仍无法避免漏洞的产生。漏洞的来源是多方面的，如系统固有缺陷、用户误操作、错误管理方式、人为因素等。若想为 IIS 服务安全打下坚实基础，就必须从这些方面入手，确保 Windows 系统的安全。

2.　外部用户威胁

IIS 服务主要为暴露在 Internet 中的 Web 网站、FTP 站点或 E-mail 服务器提供服务，而

Internet 本身就是一个开放的平台，网络上的任何用户都可以从任何地点访问服务器上的资源。用户和 IIS 服务器之间连接的开放性，将直接影响会话连接的安全，不仅如此，用户和服务器之间的数据传输也是得不到任何保护的。因此，有非法企图的用户，就可以通过很多种方式达到入侵企业服务器，获取敏感资源的目的，如假冒合法用户、劫持网络连接等。

3. 内部用户威胁

外来用户并非企业站点的唯一威胁，内部用户威胁也是不容忽略的。某些情况下，内部威胁的严重性可能远大于来自 Internet 用户的威胁。通常情况下，内部用户掌握了大量的企业站点信息，了解日常网络管理的习惯和潜在漏洞，如果真的想要入侵 IIS 服务器或窃取机密信息，相比外部用户要简单的多，甚至，有可能无需通过网络防火墙即可完成。因此，来自企业内部的安全威胁才是最应重视的。

5.1.2 规划安全措施

任何安全措施都不是放之四海而皆准的，这也是进行前期安全评估的主要目的。规划和设计 IIS 安全防护措施时，应结合 IIS 服务在企业网络中的实际应用，以及可能存在的安全威胁因素，从多方面入手，制定尽善尽美的综合性安全防护体系。

1. Windows 系统安全

IIS 的安全功能是建立在 Windows Server 2008 R2 系统安全基础之上的。Windows 中的文件系统、用户账户和服务等设置将有助于 IIS 的安全。

在文件系统方面，推荐使用安全性较高的 NTFS 文件系统。对于站点中的可执行文件应存储在独立的目录中，以便于指定严格的访问权限和用户审核。基于 NTFS 权限的安全防护措施在本书其他章节已经详细介绍，另外，需要提醒管理员注意的是，默认情况下，Windows 系统在创建新的目录时，自动将“完全控制”权限指定给“Everyone”组，实际部署时必须将其删除。

在用户账户方面，应经常进行查看，确保不是由有效管理员创建的新账户，还应检查指派给 IUSR 账户的权限，所有能够匿名访问站点的用户都具有指派给 IUSR 账户的权限。在设置用户账户密码时，应选择复杂密码。作为 IIS 系统的管理员，不但要维护严格的账户策略和限制管理员组的成员，还要安全地设置管理员密码，并要经常修改密码，以免密码被盗用。

除了文件系统和用户账户外，还有一些 Windows 安全选项影响 IIS 系统的安全。系统的每一个服务都可能成为恶意攻击的入口，因此，在服务器上应运行最少的服务，对于那些不是十分必要的服务要及时停止或删除。

2. 配置 IIS 身份验证

Windows 安全是 Internet 信息服务安全的基本保证，但是 IIS 本身的安全措施可以为 Web 站点、FTP 站点以及其他附属服务提供前沿保护，这些措施包括验证和 Web 权限等。

Internet 信息服务提供与 Windows 完全集成的安全功能，在 IIS 7.5 中，支持以下 7 种身份验证方法，使用这些方法可以确认任何请求访问网站的用户的身份以及授予访问站点公共区域的权限，同时又可防止未经授权的用户访问专用文件和目录。IIS 7.5 支持的身份验证方式如下：

- ASP.NET 模拟身份验证。启用该身份验证方式后，ASP.NET 应用程序可以在两种环境中运行，即作为通过 IIS 身份验证的用户或作为管理员设置的任意账户。该身份验证方式需要 ASP.NET 扩展组件的支持。
- Forms 身份验证。使用 Forms 身份验证，可以为公共服务器上的高流量网站或应用程序提供身份验证。该身份验证模式，可以使用户在应用程序级别管理客户端注册，而无需依赖操作系统提供的身份验证机制。
- 基本身份验证。基本验证会“模仿”一个本地用户（即实际登录到服务器的用户），在访问 Web 服务器时登录。因此，若欲以基本验证方式确认用户身份，用于基本验证的 Windows 用户，必须具有“本地登录”用户权限。默认情况下，Windows 主域控制器（PDC）中的用户账户，不授予“本地登录”用户的权限。使用基本身份验证方法，将导致密码以未加密形式在网络上传输。蓄意破坏系统安全的用户，可以在身份验证过程中使用协议分析程序，破译用户和密码。
- 摘要式身份验证。摘要式验证只能在带有 Windows 域控制器的域中使用。域控制器必须具有所用密码的纯文本复件，以便完成散列操作结果与浏览器发送散列值的比较。
- 匿名身份验证。这是 IIS 7.5 默认使用的身份验证方式，允许任何用户访问任何公共内容，而不用向客户端浏览器提供用户名和密码质询。如果某些内容只应当由选定用户查看，而且准备使用匿名身份验证，则必须配置相应的 NTFS 文件系统权限，防止匿名用户访问这些内容。如果希望只允许注册用户查看选定的内容，则必须为这些内容配置适当的身份验证方法，如基本身份验证或摘要式身份验证。
- Windows 身份验证。集成 Windows 验证是一种安全的验证形式，需要用户输入用户账户和密码。用户名和密码在通过网络发送前会经过散列处理，因此可以确保安全性。当启用 Windows 验证时，用户的浏览器通过 Web 服务器进行密码交换。Windows 身份验证使用 Kerberos v5 验证和 NTLM 验证。如果在 Windows 域控制器上安装了 Active directory 服务，并且用户的浏览器支持 Kerberos v5 验证协议，则使用 Kerberos v5 验证，否则使用 NTLM 验证。
- 证书。可以用来建立安全套接字层（SSL）连接的数字凭据，也可以用于验证。

当不允许用户匿名访问时，还应当为 IIS 用户账户设置强密码，以实现 IIS 的访问安全。密码应该足够复杂且够长，可以通过使用数字、符号和英文字母（包括大小写）结合的方式来设置密码，长度一般在 6 位以上，并且通过经常修改密码，封锁失败的登录尝试，以及设定账户的有效期等方法对一般用户账户进行管理。

提示

如果 IIS 服务器是在 Windows 域环境中运行，则还将安装一种仅适用于域环境的身份验证方式，即“AD 客户证书身份验证”。允许用户使用 Active Directory 目录服务功能，将用户映射到客户证书，以便进行身份验证。将用户映射至客户证书可以自动验证用户的身份，而无需使用基本、摘要式或集成 Windows 身份验证等其他身份验证方法。

3. 为 IIS 目录配置 NTFS 访问权限

NTFS 文件系统可以为数据提供安全和访问控制，可以限制用户和服务对文件和文件夹的

访问。使用 NTFS 文件系统时，必须为用户账户授予相应的 NTFS 权限，该用户才能访问相应的文件或文件夹，否则就无法访问，从而在一定程序上保护了数据的安全。需要注意的是，NTFS 的安全性在本地计算机或网络中都是有效的。无论是以用户身份登录到服务器，还是通过网络访问共享文件夹，NTFS 安全性都有效。因此，从安全性角度考虑，应为 IIS 设置 NTFS 权限。

无论使用 IIS 搭建 Web 服务还是 FTP 服务，都应将文件存储在 NTFS 分区内，并利用 NTFS 权限来增加数据的安全性。

右击存储 Web 网站或 FTP 站点主目录所在的文件夹，在弹出的快捷菜单中选择“属性”选项，打开“属性”对话框，切换到“安全”选项卡；或者在“Internet 信息服务（IIS）管理器”窗口中，右击 Web 站点或 FTP 站点，并选择快捷菜单中的“编辑权限”选项（以 Default Web Site 默认站点为例），在打开对话框中切换到如图 5-1 所示“安全”选项卡，即可查看不同用户对应的 NTFS 权限，继续单击“编辑”按钮，还可以修改选定用户对文件或文件夹的访问权限。

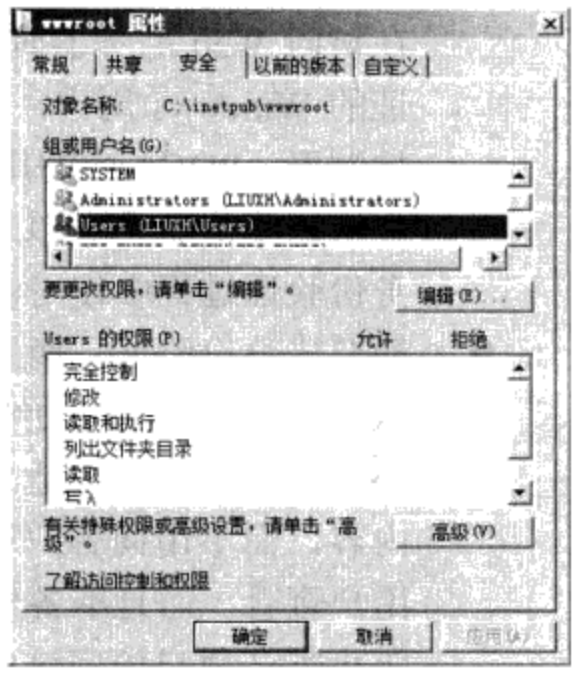


图 5-1 设置 NTFS 权限

需要注意的是，如果 NTFS 的权限设置与 IIS 权限设置发生冲突，以最严格的设置为准。例如，NTFS 的权限设置为只读，而 IIS 权限设置为完全控制，那么用户的访问权限将只能是“只读”。为了使服务器尽可能地安全，应该重新检查一下所有 IIS 文件夹的安全设置并进行适当的调整。

4. IIS 安装安全

在安装 IIS 时应注意以下问题：

- 选择非域控制器作为 IIS 服务器。安装 IIS 过程中，系统将自动创建“IUSR_计算机名”匿名账户，如果所选服务器是域控制器，则该用户账户将被添加到域用户组中（Users），从而把应用于组的访问权限，就会提供给访问 IIS 服务器的每个匿名用户，这不仅给 IIS 带来潜在危险，而且还可能威胁整个网络的安全。
- 选择非系统分区作为安装目录。把 IIS 安装在系统分区上，会使系统文件与 IIS 同样面临非法访问，容易使非法用户侵入系统分区，所以在安装 IIS 的 Web、FTP 等服务时，应尽量避免将 IIS 服务器安装在系统分区上。
- 安装在 NTFS 类型分区上。相对于 FAT32 分区而言，NTFS 分区拥有较高的安全性和可管理性，并且磁盘利用效率高，可以设置复杂的访问权限，以适应不同信息服务的需求。
- 只安装必需的组件。除非特别需要，否则，不要安装 Internet 打印以及 ASP.NET、CGI 等动态网站扩展组件，以避免恶意用户借助相应的组件漏洞或设置错误，实现对 IIS 服务器的攻击。
- 定制自己需要的安全功能组件。IIS 7.5 提供的更为丰富的安全功能设置，管理员可以根据 IIS 服务器的需求定制适当的安全限制。

5. 用户操作安全

在 IIS 服务的安全管理中，上述安全措施主要是从软件的角度并针对访问者来规划的。实

际上，用户操作安全也是服务器管理员应该考虑的问题。用户操作安全主要涉及到以下几个方面：

- 用户离开计算机前，应按快捷键 Ctrl＋Alt＋Delete，然后选择“锁定计算机”按钮，来锁定桌面。
- 使用带密码保护的屏幕保护程序，而且延迟时间应很短，以确保没有人能够在您离开很短的时间内使用计算机。屏幕保护程序应该设置为空，因为动画屏幕保护程序会降低服务器性能。
- 将计算机锁定在安全的房间，以减少危险用户的直接访问和物理破坏的机会。
- 如果需要多名管理员管理系统，应为具有管理员权限的每个人指派明显不同的用户账户和密码，这将易于跟踪所做的任何更改。
- 要降低用户账户信息受到危害的可能性，应定期为具有管理员或其他高级权限的人员指派新账户。
- 尽快删除无用的账户，这样可防止离职人员或供应商访问网络。

5.2 Web 安全

随着信息时代的进步，Web 网站已经成为树立企业形象的重要因素，通过 IIS 服务可以搭建信息发布、信息查询、电子商务、电子政务等各种用途 Web 网站。不仅如此，企业网络中常用的 E-mail 服务、办公系统、流媒体服务等也离不开 Web 网站的支持。因此，Web 服务器的安全性，将影响到本地系统，甚至整个网络的安全性，必须通过相应的安全机制，控制来访用户的访问。

5.2.1 用户控制安全

Web 服务器的主要功能就是为用户提供信息发布和查询平台，信息的面向对象不同，所以就需要对访问用户进行控制，通过设置适当的身份验证方式即可实现。例如，如果信息面向所有用户，则可以使用匿名身份验证；如果仅面向部分用户，则可以仅赋予这些用户对信息的访问权限。配置身份验证可以确保服务器的安全，同时还可以为来访用户提供身份验证并生成服务器日志。

第 1 步，依次选择“开始”→“管理工具”→“Internet 信息服务（IIS）管理器”选项，打开“Internet 信息服务（IIS）管理器”窗口，依次展开“SERVER2008”→“网站”→“XXX 有限公司”选项，在右侧主窗口中选择“身份验证”图标如图 5-2 所示。

提示

在“分组依据”下拉列表框中，可以选择适当的分类条件，包括类别、区域和不进行分组几种。所选分类条件的不同，布局也会有所不同。

第 2 步，在“操作”栏中单击“打开功能”链接，或者直接双击“身份验证”，显示如图 5-3 所示“身份验证”窗口。

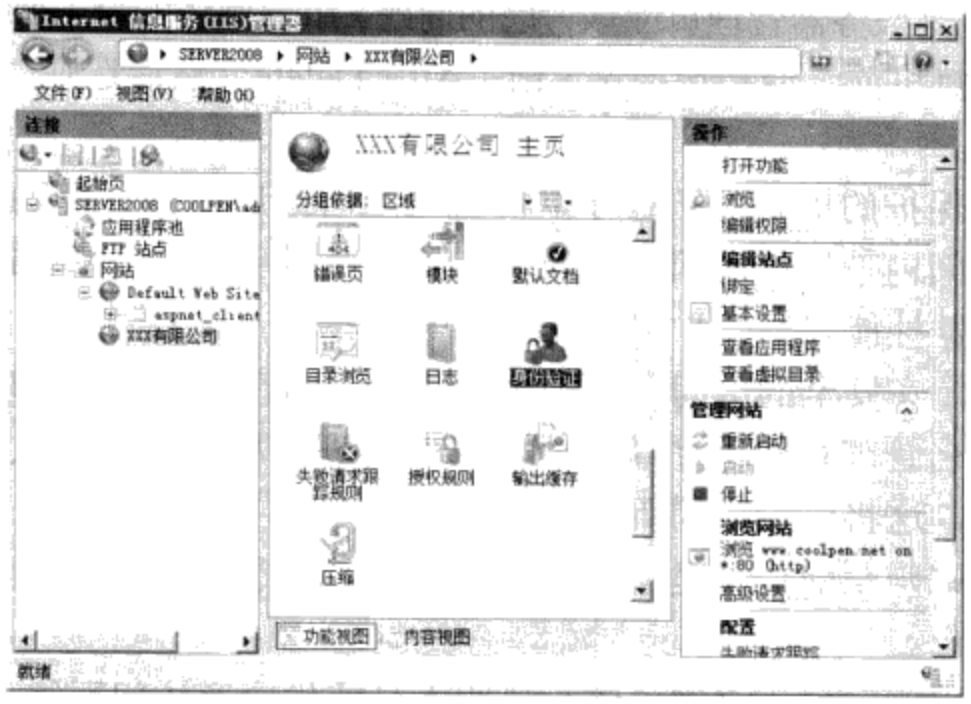


图 5-2 “Internet 信息服务（IIS）管理器”窗口

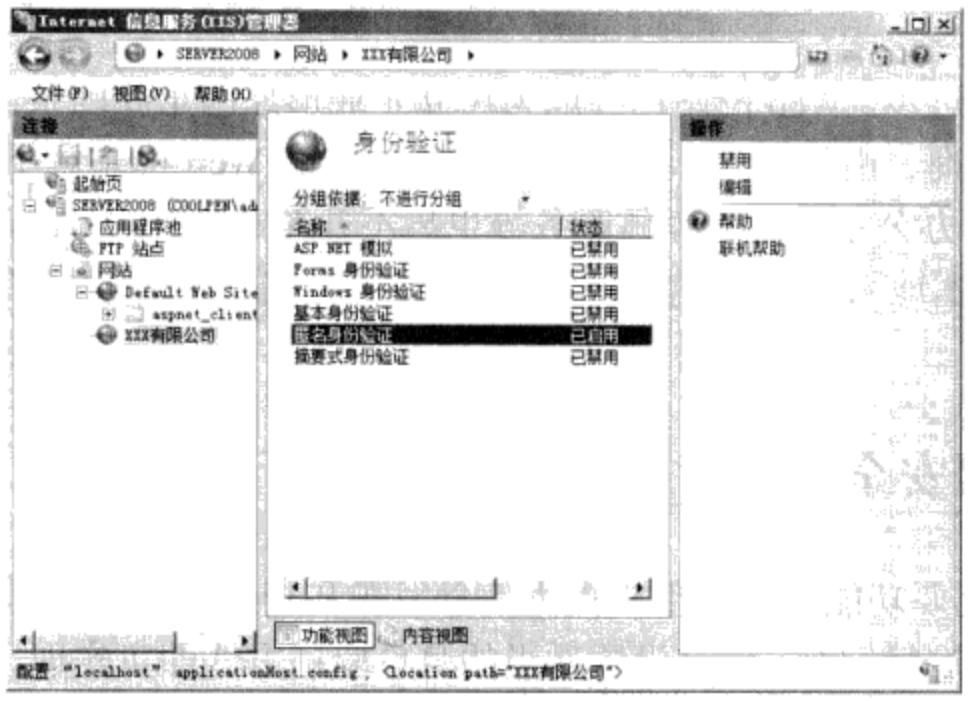


图 5-3 “身份验证”窗口

注·意 如果采用默认方式安装 Windows Server 2008 R2 中的 IIS 7.5，将只安装“匿名身份验证”组件，管理员也可以在安装过程中，根据需要选择希望安装的组件，或者在安装完成后，再次添加希望使用的身份验证安全组件。

第 3 步，在“身份验证”窗口中，选择“匿名身份验证”选项并单击“操作”栏中的“编辑”链接，显示如图 5-4 所示“编辑匿名身份验证凭据”对话框。默认选择“特定用户”单选按钮，IIS 7.5 默认使用安装过程中自动创建的 IUSR，作为用户名进行匿名访问。如果选择“应用程序池标识”单选按钮，则可以允许 IIS 进程，使用在应用程序池的属性页上指定的账户运行。

第 4 步，单击“设置”按钮，显示如图 5-5 所示“设置凭据”对话框。单击“确定”按钮，替换系统默认的 IUSR 账户，再次单击“确定”按钮，保存设置。使用相同的方法，还可以同时启用多种身份验证方式。

第 5 步，更改系统默认匿名访问账户，虽然可以起到一定的安全保护作用，但仍不能适

用于安全需求较高的 Web 服务器。在“身份验证”窗口中，选择“匿名身份验证”选项，单击“操作”栏中的“禁用”链接，即可禁用匿名访问。此时，来访用户必须使用有效的用户账户凭证，通过 Web 服务器的身份验证，才可以进行正常访问。在“身份验证”窗口中，选择希望使用的身份验证方式，单击“操作”栏中的“启用”链接即可。

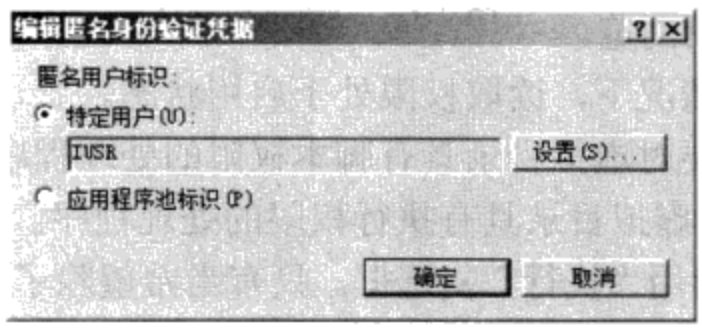


图 5-4 “编辑匿名身份验证凭据”对话框

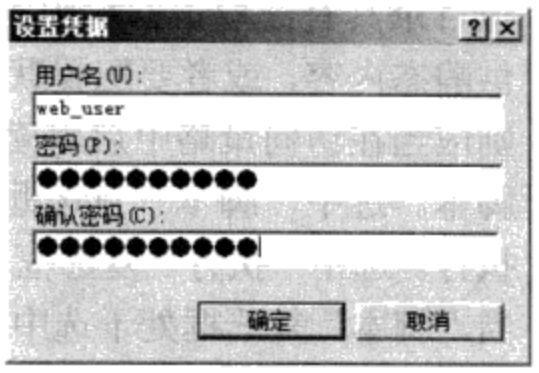


图 5-5 “设置凭据”对话框

5.2.2 访问权限控制

通过设置适当的访问权限，可以严格控制来访用户对于指定类型的文件的访问。管理员可以根据实际情况，为特殊文件类型设置访问策略，指定授予 IIS 中的 Web 服务器、网站、应用程序、目录或文件级别的处理程序的功能权限类型。

1. 编辑功能权限

通过配置功能权限可以设置访问策略，访问策略指定 IIS 中所有处理程序可以具有的权限类型。可以在访问策略中启用或禁用的功能权限包括读取、脚本和执行。处理程序能否运行由访问策略以及处理程序所需的访问设置共同决定。如果处理程序需要未在访问策略中启用的功能权限类型，该处理程序将被禁用，并且该处理程序（基于处理程序映射）处理的所有请求都将失败，除非请求可以由另一个处理程序处理。

第 1 步，在 IIS 管理控制台中，单击欲配置的服务器、站点或目录，在主页窗口中双击“处理程序映射”图标，显示如图 5-6 所示“处理程序映射”窗口。“已启用”列表框中显示的是当前站点支持的文件类型。

图 5-6 “处理程序映射”窗口

第2步，右击需要设置的文件类型（以ASPClassic为例），选择快捷菜单中的“编辑功能权限”选项，打开如图5-7所示“编辑功能权限”对话框。各权限的描述如下：

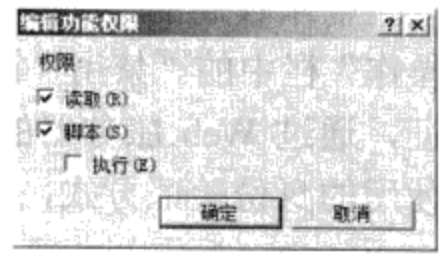


图5-7 “编辑功能权限”对话框

- 读取。选中“读取”复选框，可以启用需要对虚拟目录具有读取访问权限的处理程序。如果要提供静态内容，或者要配置默认的文档和目录浏览，则应当在访问策略中启用读取权限。默认情况下，读取权限处于启用状态。
- 脚本。选中“脚本”复选框，可以启用需要对虚拟目录具有脚本权限的处理程序。
- 执行。选中“执行”复选框，以启用需要对虚拟目录具有执行权限的处理程序。只有当“脚本”复选框处于选中状态时，才会启用“执行”复选框。只有当希望除了脚本之外，还允许运行可执行文件（如.exe、.dll和.com文件）时，才应当在访问策略中启用执行权限。

出于安全和性能方面的考虑，应当只对已经过测试、且应用程序需要的程序启用执行权限。

第3步，单击“确定”按钮，保存设置。

2. 设置请求限制

如果希望处理程序只响应对特定资源类型的请求（例如文件或文件夹，或者对特定谓词的请求），则可以为处理程序映射配置可选限制，也可以指定处理程序需要具有何种访问权限才能在虚拟目录中运行。处理程序所需的访问权限设置以及“处理程序映射”功能的访问策略，共同决定了处理程序能否运行。

第1步，在“处理程序映射”窗口中，双击希望设置请求限制的应用程序名称（以ASPClassic为例），打开如图5-8所示“编辑脚本映射”对话框。

第2步，单击“请求限制”按钮，打开“请求限制”对话框，默认显示如图5-9所示“映射”选项卡。如果希望处理程序仅响应针对特定资源类型的请求，则可以选中“仅当请求映射至以下内容时才调用处理程序”复选框，并选择以下选项之一。

- 文件。用于使处理程序仅在所请求的目标资源是文件时才做出响应。
- 文件夹。用于使处理程序仅在所请求的目标资源是文件夹时才做出响应。
- 文件或文件夹。用于使处理程序仅在所请求的目标资源是文件或文件夹时才做出响应。

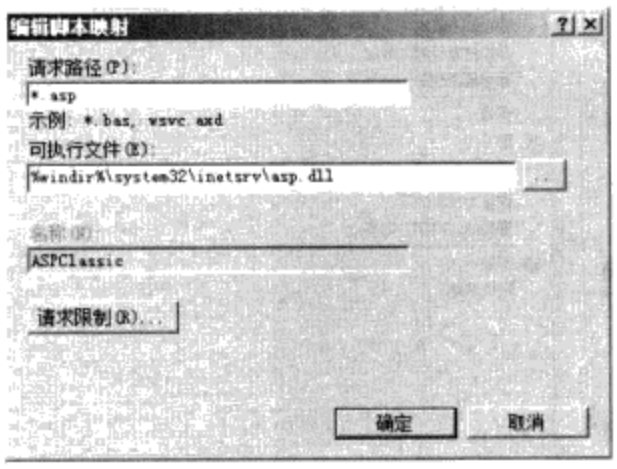


图5-8 “编辑脚本映射”对话框

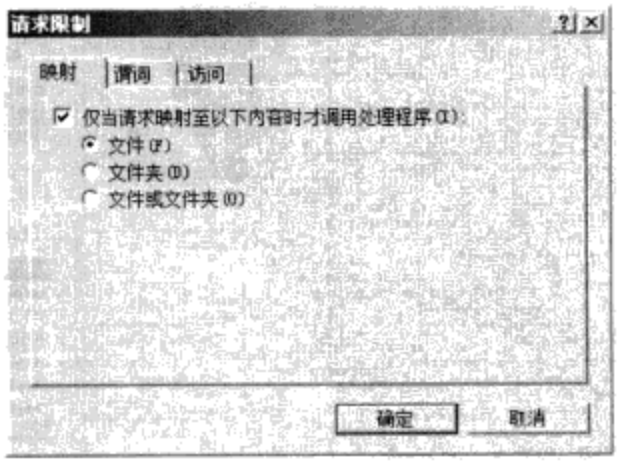


图5-9 “映射”选项卡

第 3 步，切换至如图 5-10 所示“谓词”选项卡，可以选择以下选项之一。

- 全部谓词。如果选择此选项，则不论请求中发送的谓词如何，处理程序均对请求做出响应。
- 下列谓词之一。如果选择此选项，则处理程序将响应包含特定谓词的请求。然后，请在对应的框中键入一个或多个谓词。

第 4 步，切换至如图 5-11 所示“访问”选项卡，可以选择下列选项之一。

- 无。如果选择此选项，在即使在未启用任何访问策略选项的情况下，处理程序也将运行。
- 读取。如果选择此选项，则处理程序会在访问策略中启用了“读取”的情况下运行。
- 写入。如果选择此选项，则处理程序会在访问策略中启用了“写入”的情况下运行。
- 脚本。如果选择此选项，则处理程序会在访问策略中启用了“脚本”的情况下运行。这是默认选项。
- 执行。如果选择此选项，则处理程序会在访问策略中启用了“执行”的情况下运行。

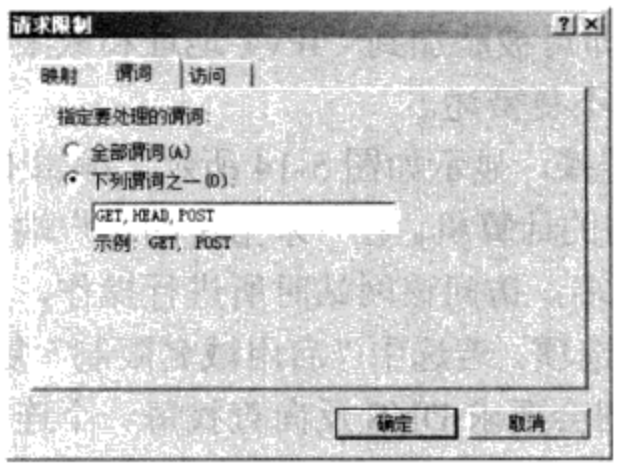


图 5-10 “谓词”选项卡

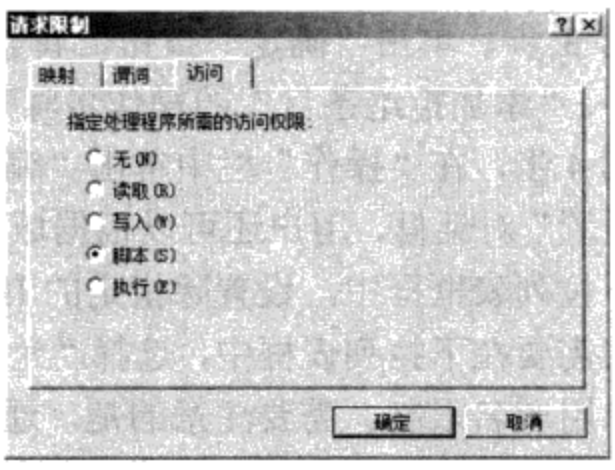


图 5-11 “访问”选项卡

请确保处理程序所需的访问权限设置正确无误，否则处理程序将可能在无意中运行。例如，如果为 ISAPI-dll 处理程序将处理程序所需的访问权限从“执行”更改为“读取”，那么，即使在功能的访问策略中仅启用了“读取”，ISAPI 扩展也将能够运行。

第 5 步，单击“确定”按钮，保存设置。

5.2.3 IP 地址控制

默认情况下，IIS 会自动检查每个来访者的 IP 地址，通过 IP 地址的访问来防止或允许某些特定的计算机、域，甚至整个网络访问站点。因此，通过 IP 地址限制来在 Internet 上排除未知用户是非常有效的方法。同时，IIS 7.5 还提供了基于 Windows 域的访问限制，管理员可以禁止或允许来自指定域的用户，访问站点或目录，该功能默认是未启用的。

第 1 步，在“Internet 信息服务（IIS）管理器”的站点主页中，双击“IPv4 地址和域限制”图标，显示如图 5-12 所示“IPv4 地址和域限制”窗口。

第 2 步，单击“添加允许条目”链接，打开“添加允许限制规则”对话框。系统默认选择“特定 IPv4 地址”单选按钮，在对应文本框中，输入想要允许访问的单个 IP 地址即可。建议选择“IPv4 地址范围”单选按钮，并输入相应的主机 IP 地址和“掩码”，如图 5-13 所示，可以同时添加多个被允许访问的主机 IP 地址。

图 5-12 “IPv4 地址和域限制”窗口

第 3 步，单击“确定”按钮，新创建的限制规则即可被添加到“IPv4 地址和域限制”列表框中。“添加拒绝条目”的操作步骤与之类似，此处不复赘述。

第 4 步，在“操作”栏中单击“编辑功能设置”链接，显示如图 5-14 所示“编辑 IP 和域限制设置”对话框，用户还可以根据域名来限制要访问的计算机。在“未指定的客户端的访问权”下拉列表框框中，设置除指定的 IP 地址外的客户端，访问该网站时所进行操作，用户可以根据需要在下拉列表框中，选择“允许”或“拒绝”选项。若选中“启用域名限制”复选框，即可启用域名限制。需要注意的是，通过域名限制访问会要求 DNS 反向查找每一个连接，这将会严重影响服务器的性能，建议不要使用。

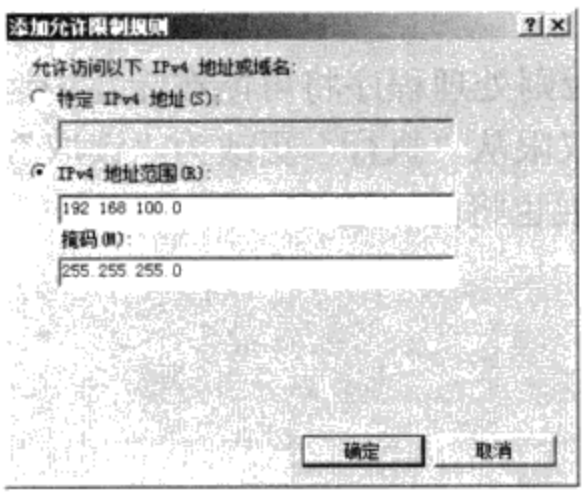


图 5-13 “添加允许限制规则”对话框

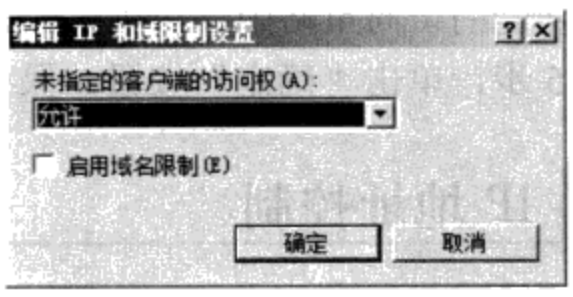


图 5-14 “编辑 IP 和域限制设置”对话框

第 5 步，在“操作”栏中单击“恢复为继承的项”链接，显示如图 5-15 所示“IPv4 地址和域限制”对话框，恢复功能以从父配置中继承设置，该操作将为当前功能删除本地配置设置（包括列表中的项目），应慎重使用。

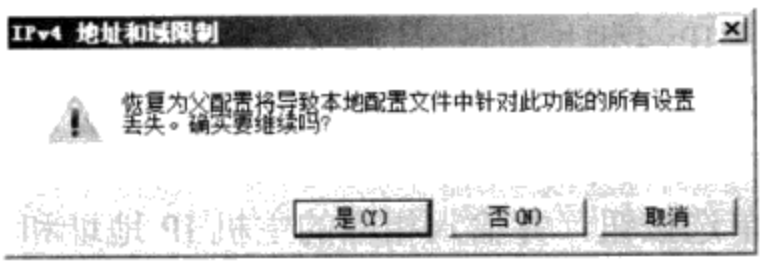


图 5-15 “IPv4 地址和域限制”对话框

第 6 步，在“操作”栏中单击“查看经过排序的列表”链接，显示如图 5-16 所示窗口。IIS 7.5 是按照限制规则列表中条目的顺序依次执行的。例如，当前规则列表中包括两条限制条目：拒绝 IP 地址为 192.168.100.229 的主机访问，允许整个 192.168.100.1 ~ 192.168.100.254 网段访问，即被拒绝的 IP 地址 192.168.100.229 又在被允许访问的网段内。此时，如果经过排序后拒绝在先，则将拒绝指定用户访问；如果允许在先则将允许该用户访问。

图 5-16　查看经过排序的列表

第 7 步，在经过排序的限制列表中，选择想要移动的限制条目，单击“上移”或“下移”链接，即可调整执行顺序。

5.2.4 端口安全

对于 IIS 服务，无论是 Web、FTP，还是 NNPT、SMPY 服务等都有各自侦听和接收浏览器请求的 TCP 端口号。一般常用的端口号为 Web 是 80，FPT 是 21，SMPT 是 25，SSL 是 443。通过修改端口号也可以提高 IIS 服务器的安全性。如果修改了端口设置，用户必须知道该服务的端口才能访问，不过用户在访问时需要指定端口号。

第 1 步，在“Internet 信息服务（IIS）管理器”窗口中，右击“Default Web Site”并选择快捷菜单中的“编辑绑定”选项，显示如图 5-17 所示“网站绑定”对话框。

第 2 步，选择需要设置端口安全的站点名称，单击“编辑”按钮，显示如图 5-18 所示“编辑网站绑定”对话框，默认使用的端口是 80，重新输入新的端口号即可。

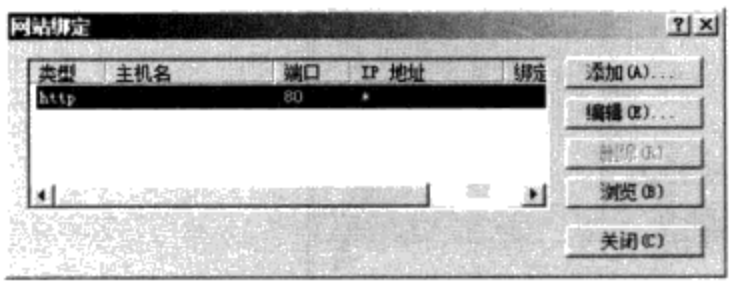


图 5-17　“网站绑定”对话框

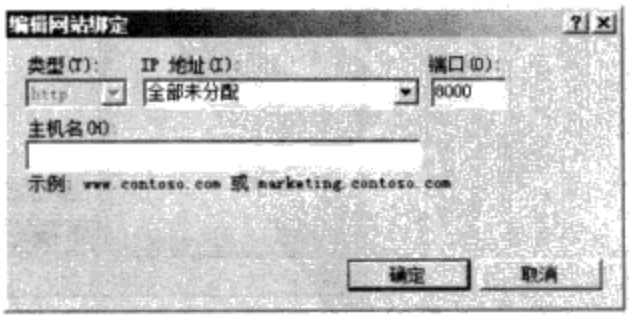


图 5-18　“编辑网站绑定”对话框

第 3 步，单击“确定”按钮，保存设置即可。

提示　使用默认值 80 端口时，用户只需通过 Web 服务器的地址即访问该网站，地址形式为：http:// 域名或 IP 地址，如 http://192.168.1.25 或 http://www.coolpen.net。而如果端口号不是 80，则访问服务器时就必须提供端口号，使用“http://域名或 IP 地址:端口号”的方式访问，如 http://192.168.1.25:8000 或 http://www.coolpen.net:8000。

5.2.5 SSL 安全

由于 Web 网站直接曝露于 Internet 中，因此，任何人都可以连接网站，这也使得网站很容易受到来自网络的攻击，并且网站数据在传输过程中很容易被人尝试截获。为了保护 Web 网站的安全，防止数据在传输过程中被截获和篡改，可以在 Web 服务器上配置 SSL（Secure Socket Layer，安全套接字层），对传输的数据进行加密，这样，即使数据被人窃取，也无法解密出数据内容，在一定程度上保护了数据的安全。

1. 创建 SSL 证书

如果要利用 SSL 实现加密传输，必须在 Web 服务器端安装用于 SSL 加密的证书。设置 SSL 证书可以使用三种方式：向证书服务器申请证书、创建域证书、创建自签名证书。其中，自签名证书是 IIS 7.5 自带的功能，不需向证书服务器申请。这里以向证书服务器申请证书为例，创建一个证书申请文件，然后向证书服务器申请。而客户端只需配置为信任证书服务器即可。

第 1 步，从证书服务器上下载证书链，配置 IE 浏览器信任证书颁发机构。

第 2 步，打开 IIS 管理器，单击 Web 服务器名，在主页窗口中双击“服务器证书”图标，显示如图 5-19 所示“服务器证书”窗口。默认还没有创建证书。

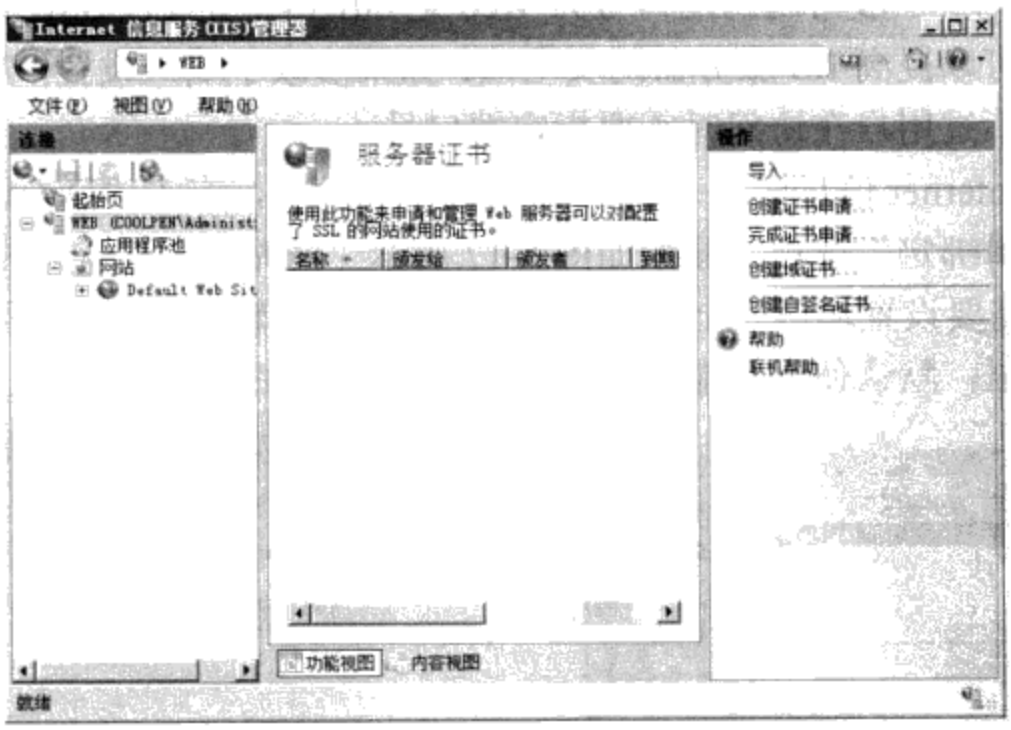


图 5-19　“服务器证书”窗口

第 3 步，单击右侧“操作”栏中的“创建证书申请”链接，显示如图 5-20 所示“可分辨名称属性”对话框，键入通用名称、组织、地点等证书信息。其中，“通用名称”文本框中必

须键入用户访问时使用的域名，否则客户端访问时，证书将无效。

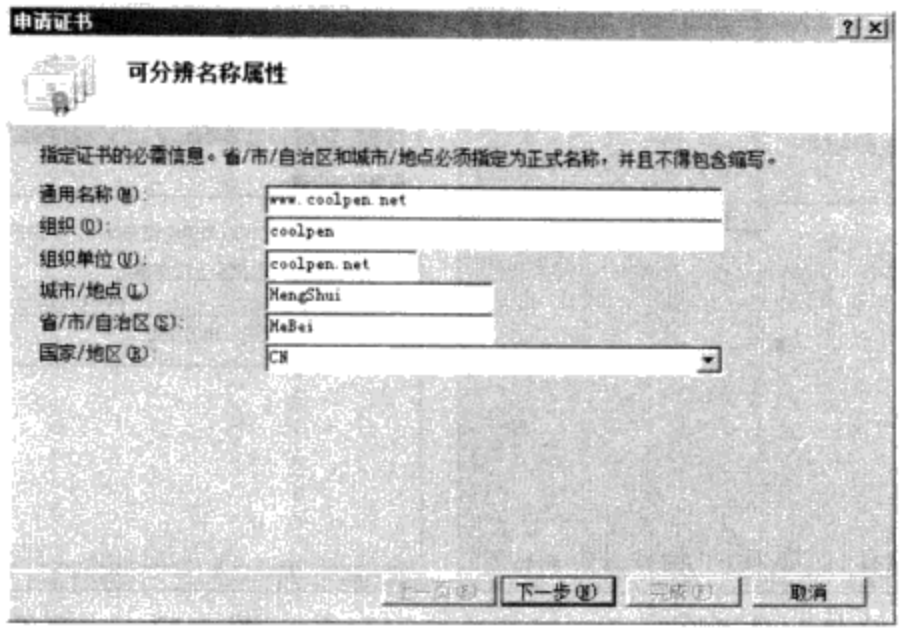


图 5-20 “可分辨名称属性”对话框

注意 此处的“通用名称”必须与该网站所使用的 DNS 域名相同，而且用户访问时也必须使用该域名，否则将会提示证书错误。

第 4 步，单击“下一步”按钮，显示如图 5-21 所示“加密服务提供程序属性”对话框。选择加密程序，并设置证书的位长，位长越大安全性也越强，但也会影响性能。

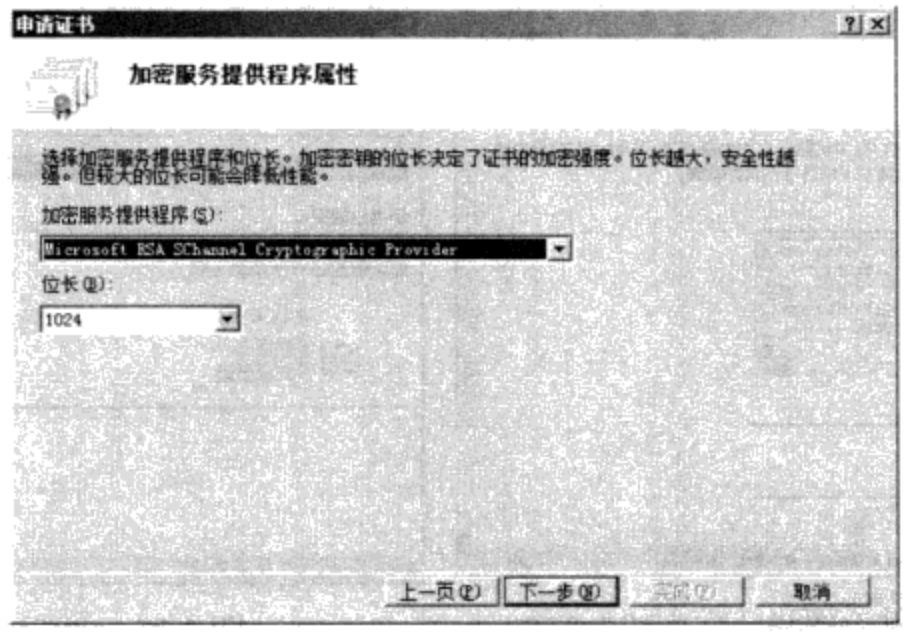


图 5-21 “加密服务提供程序属性”对话框

第 5 步，单击“下一步”按钮，显示如图 5-22 所示“文件名”对话框。在“为证书申请指定一个文件名”文本框中，指定证书申请文件的保存路径和名称，将需要使用该文件向证书服务器申请证书。

第 6 步，单击“完成”按钮，证书申请文件创建成功。

第 7 步，打开证书服务器申请页面，单击“申请证书”链接，显示“申请一个证书”窗口。单击“高级证书申请”按钮，显示“高级证书申请”窗口，如图 5-23 所示。

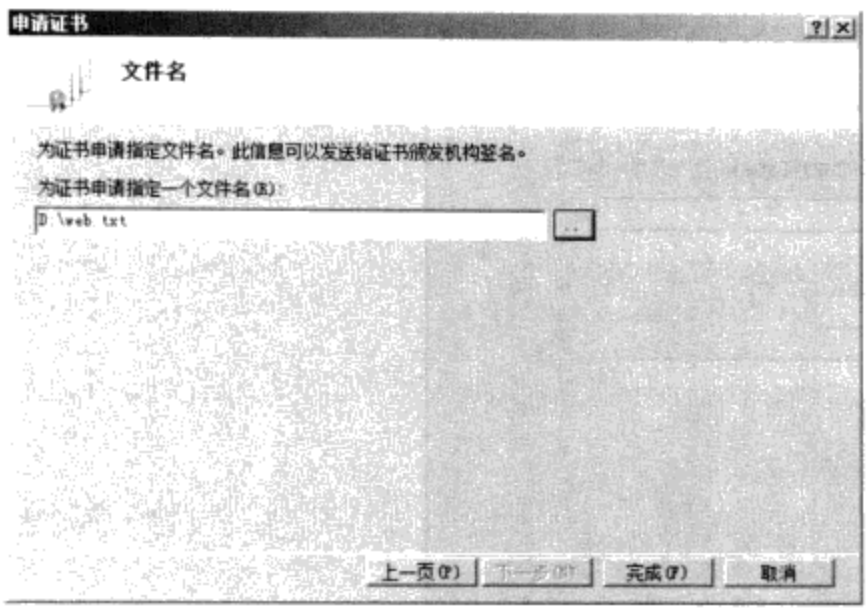


图 5-22 “文件名”对话框

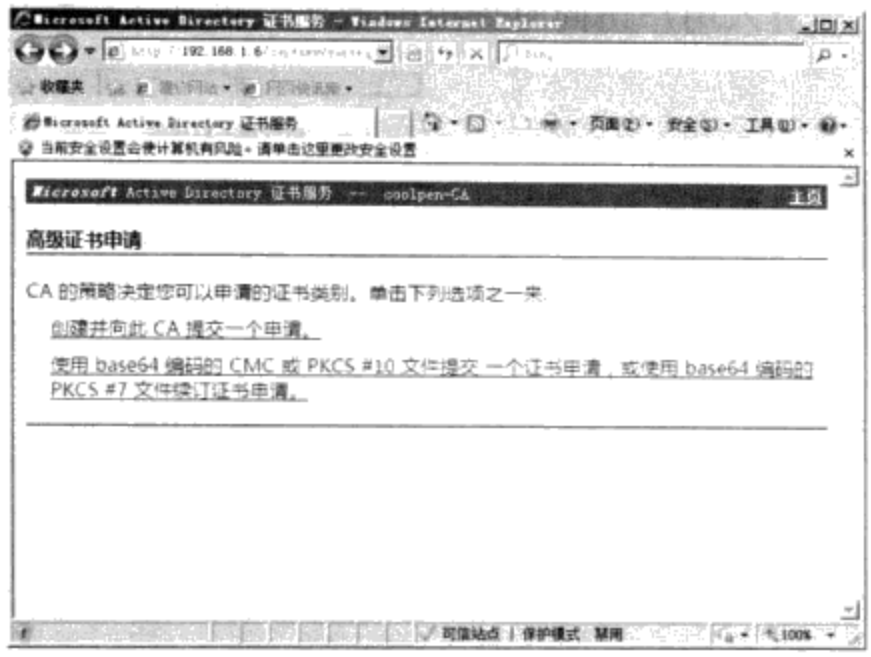


图 5-23 “高级证书申请”窗口

第 8 步，单击“使用 base64 编码的 CMC 或 PKCS #10 文件提交一个证书申请，或使用 base64 编码的 PKCS #7 文件续订证书申请”链接，显示如图 5-24 所示“提交一个证书申请或续订申请”窗口。在“保存的申请”文本框中，将所生成的证书申请文件中的内容粘贴进来；在“证书模板”下拉列表框中，选择“Web 服务器”选项。

第 9 步，单击“提交”按钮，申请成功，如图 5-25 所示。单击“下载证书”链接，将证书保存在本地计算机上。

图 5-24 “提交一个证书申请或续订申请”窗口

图 5-25 “证书已颁发”窗口

第 10 步，返回 IIS 管理器的“服务器证书”窗口，单击“操作”栏中的“完成证书申请”链接，显示如图 5-26 所示“完成证书申请”对话框。在“包含证书颁发机构响应的文件名”文本框中键入刚刚下载的证书文件路径，或者单击“..”按钮选择；在“好记名称”文本框中设置一个名称。

第 11 步，单击“确定”按钮，证书申请成功，并显示在“服务器证书”窗口中，如图 5-27 所示。

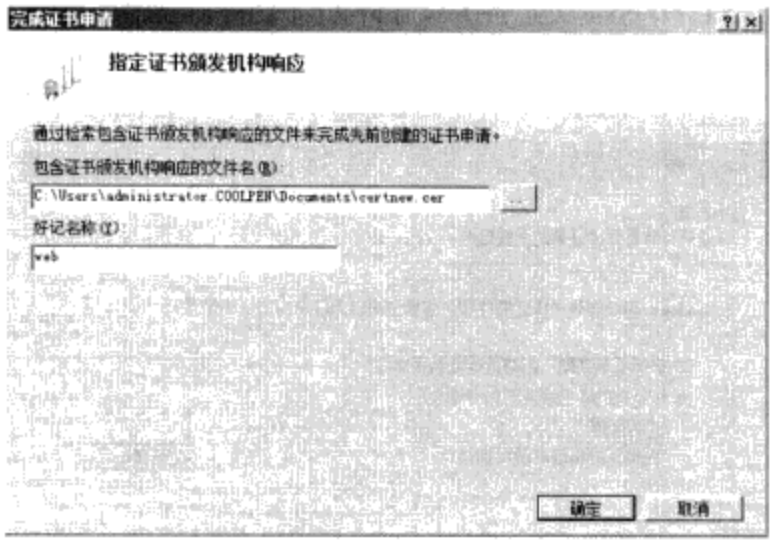


图 5-26 “完成证书申请”对话框

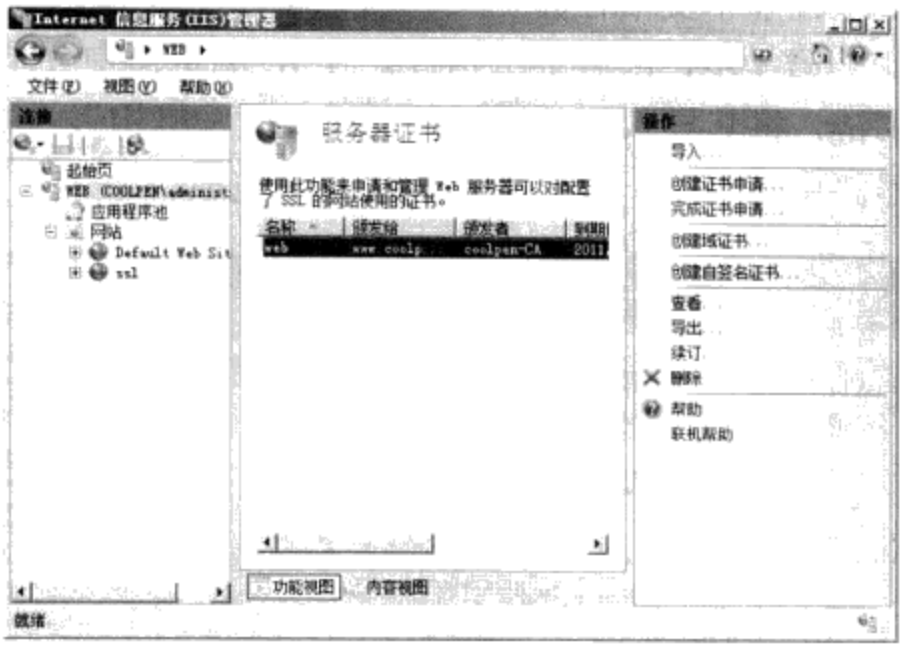


图 5-27 证书申请成功

至此，SSL 证书申请成功，即可用来创建 SSL 网站了。

2. 创建 SSL 网站

第 1 步，在 DNS 服务器上创建主机，设置 DNS 域名，并使其 IP 地址指向 SSL 网站的 IP 地址。

第 2 步，返回 Web 服务器，在 IIS 管理器中创建一个 SSL 网站。在“类型”下拉列表框中选择“https”，在“IP 地址”文本框中指定 IP 地址，“端口”文本框中使用默认的 443 即可。在“SSL 证书”下拉列表框中选择所申请的证书，如图 5-28 所示。

第 3 步，单击“确定”按钮，SSL 网站创建完成。

3. 访问 SSL 网站

第 1 步，在客户端计算机上，使用 IE 浏览器中打开 SSL 网站，首先会显示“此网站的安全证书有问题”，如图 5-29 所示。

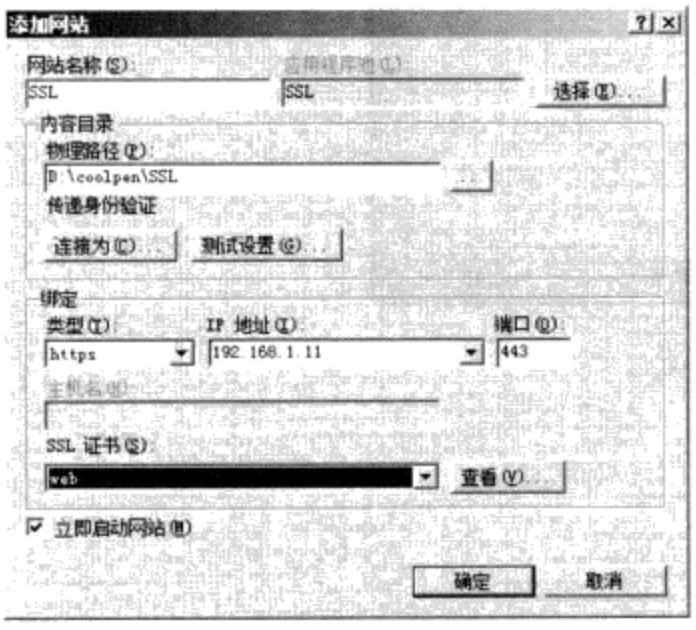


图 5-28 添加 SSL 网站

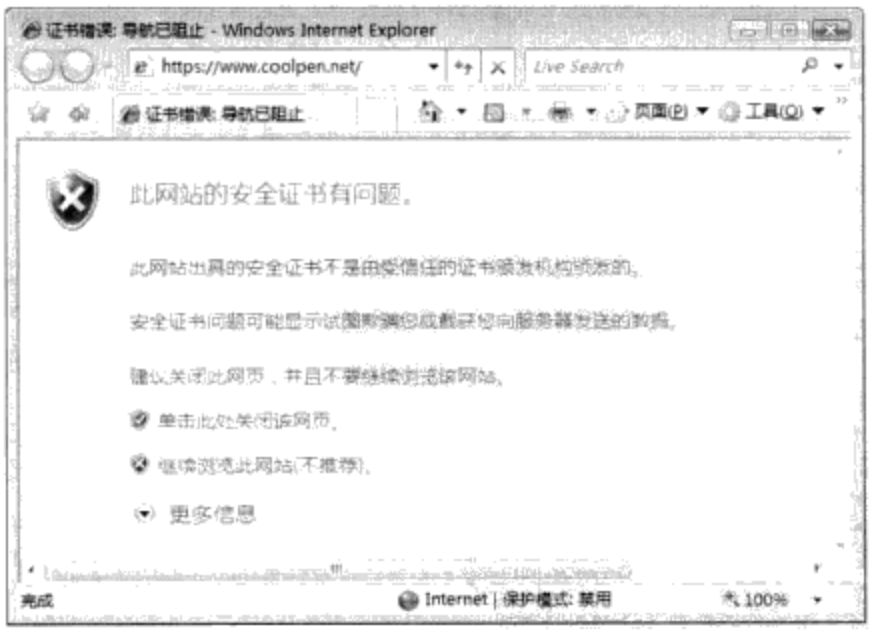


图 5-29 IE 浏览器

第 2 步，单击“继续浏览此网站（不推荐）”链接，可以打开此网站，但会提示证书错误，现在还不能使用证书加密传输数据。单击“证书错误”链接显示如图 5-30 所示对话框，提示

安全证书不受信任。

第3步，配置证书信任。在IE浏览器中登录“Active directory证书服务”主页，下载证书链，将其导入“受信任的根证书颁发机构”，如图5-31所示，使客户端计算机信任证书服务器。单击“下一步”按钮直接导入完成。

图5-30 证书错误

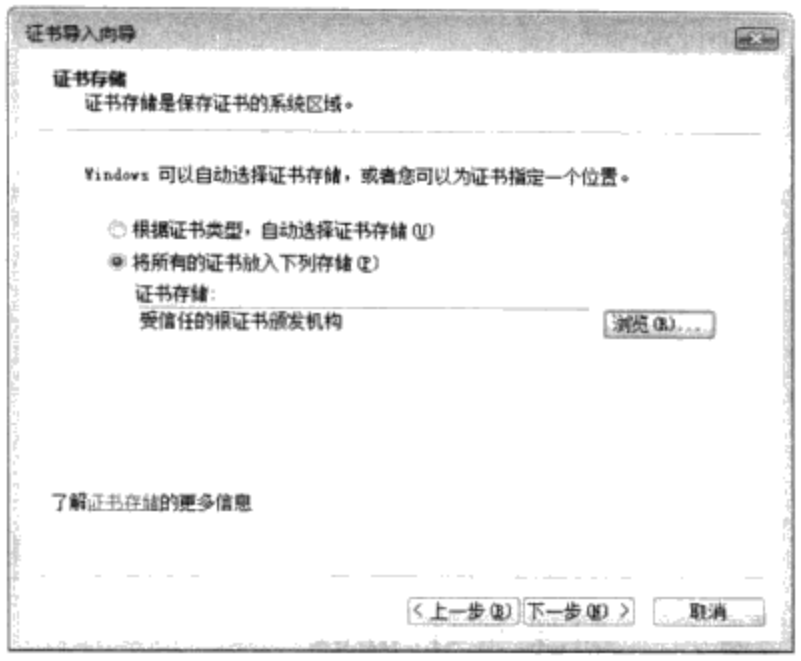


图5-31 配置证书信任

第4步，重新打开IE浏览器，再次以HTTPS方式打开网站，将不再提示证书错误，证书生效，证书图标也变为正常的锁状，如图5-32所示，表示访问网站的数据将在传输过程中被加密。

图5-32 网站访问正常

5.2.6 审核IIS日志记录

服务器上的每个Web站点，运行过程中都会产生相应的日志信息，用于记录服务器的运行情况、客户端访问情况等。IIS日志数据可以记录用户对站点内容的访问，确定哪些内容比较受欢迎，还可以记录有哪些用户非法入侵网站，确定计划安全要求和排除潜在的网站问题等。使用IIS的日志功能，可以配置IIS在Web服务器上记录请求的方式。

第 1 步，在“Internet 信息服务管理器”窗口的站点（以 Default Web site 站点为例）主页中，双击“日志”图标，显示如图 5-33 所示“日志”窗口。系统默认状态是为每个站点创建一个日志文件，管理员可以在服务器配置主页的“日志”窗口中，将其修改为：为每服务器创建一个日志文件。

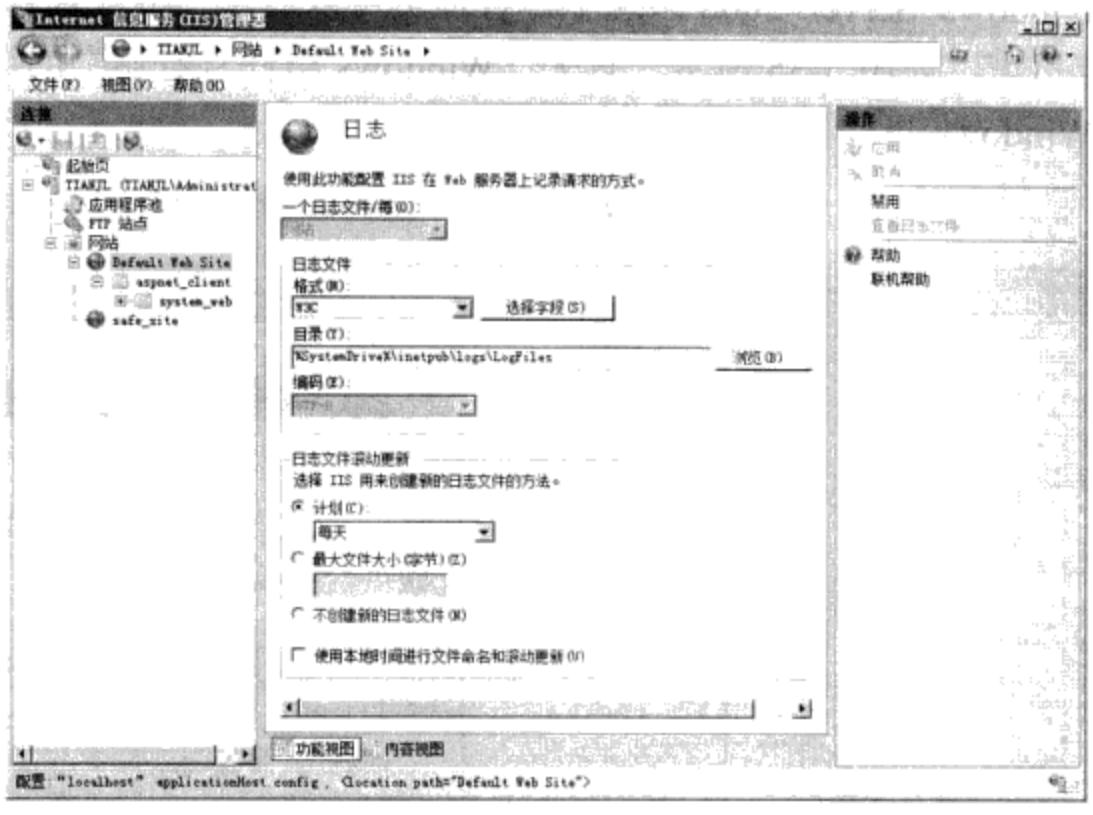


图 5-33 “日志”窗口

第 2 步，在“日志文件”选项区的“格式”下拉列表框中，选择“W3C”选项，IIS 7.5 可以提供 4 种日志文件格式。

- W3C。W3C 扩展日志文件格式，是一个包含多个不同属性、可自定义的 ASCII 格式，可以记录重要的属性，并通过省略不需要的属性字段来限制日志文件的大小。各属性字段以空格分开，时间以 UTC 形式记录。
- NCSA。NCSA 是美国国家超级计算技术应用中心公用格式，是一种固定的（不能自定义的）ASCII 格式，记录了关于用户请求的基本信息，如远程主机名、用户名、日期、时间、请求类型、HTTP 状态码和服务器发送的字节数。项目之间用空格分开，时间记录为本地时间。
- IIS。IIS 日志文件格式是固定的（不能自定义的）ASCII 格式。IIS 格式比 NCSA 公用格式记录的信息多。IIS 格式包括一些基本项目，如用户的 IP 地址、用户名、请求日期和时间、服务状态码和接收的字节数。另外，IIS 格式还包括详细的项目，如所用时间、发送的字节数、动作（例如，GET 命令执行的下载）和目标文件。这些项目用逗号分开，使得格式比使用空格作为分隔符的其他 ASCII 格式更易于阅读。时间记录为本地时间。
- 自定义。将 IIS 配置为对自定义的日志记录模块使用自定义格式。如果选择此选项，则“日志”页将被禁用，因为无法在 IIS 管理器中配置自定义日志。

第 3 步，单击“选择字段”按钮，显示如图 5-34 所示“W3C 日志记录字段”对话框，用户根据实际需要进行设置即可。

第 4 步，在“目录”文本框中，单击“浏览”按钮，设置日志文件的保存位置，默认保存目录为：%SystemDrive%\inetpub\logs\LogFiles。

第5步，在“日志文件滚动更新”选项区中，设置创建新日志文件的方式。包括：

- 计划。可以固定的时间更新日志，例如每天更新。
- 最大文件大小。当日志文件达到该大小时，自动更新日志文件。
- 不创建新的日志文件。将所有的网站日志记录全部记录到单个文件中。

第6步，在Windows Server 2008系统中，管理员可以通过“事件查看器”，管理和查看Web服务器和站点日志，如图5-35所示。有关“Windows事件查看器”的详细应用，请参考本书“第11章　Windows事件日志”中的相关内容。

图5-34　“W3C日志记录字段”对话框

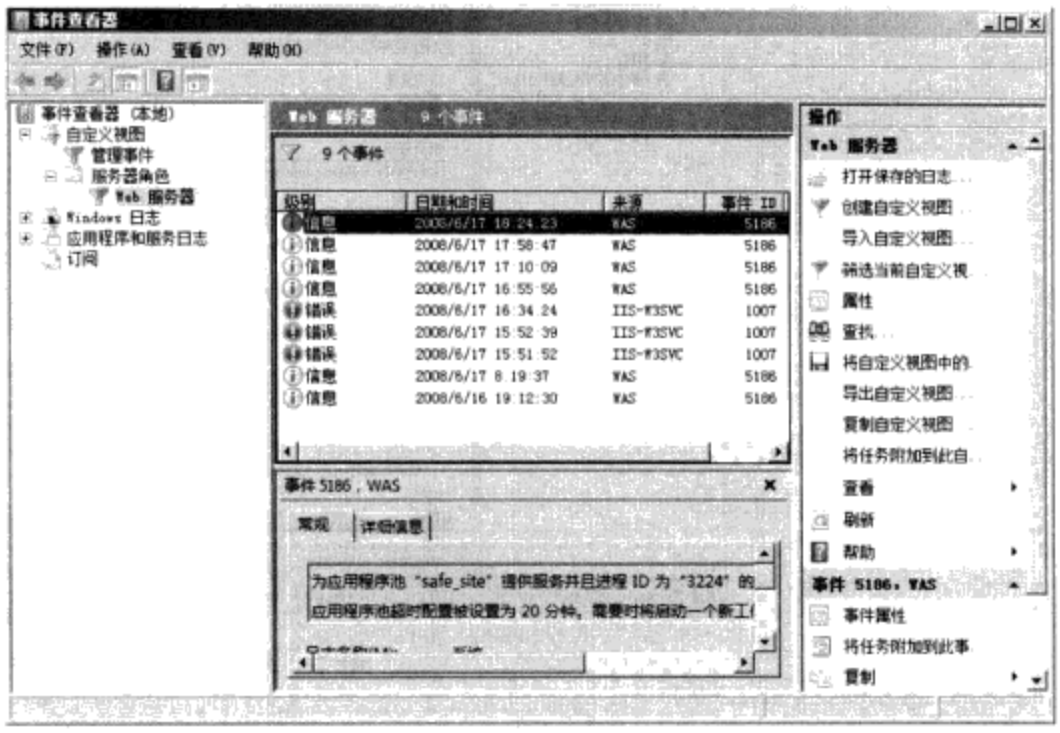


图5-35　查看Web服务器事件日志

第7步，设置完成后，在“操作”栏中单击“应用”链接，保存设置。

5.2.7 设置内容过期

“设置内容过期”是Web服务器重要的安全防护措施之一。对于一些比较敏感的数据（如特定的报价或事件公告），可以通过设置内容过期来更新所发布的内容。浏览器会自动比较当前日期与截止日期，如果发现内容已过期则不再发布该数据，客户端也不会显示缓存页而是从服务器更新。

第1步，在“Internet信息服务管理器”窗口的站点（以Default Web site站点为例）主页中，双击“HTTP响应标头”图标，显示如图5-36所示“HTTP响应标头”窗口。

第2步，在“操作”栏中，单击“设置常用标头”链接，显示如图5-37所示“设置常用HTTP响应头”对话框。系统默认并未设置内容过期，选中“使Web内容过期”复选框，并设置相应过期方式即可。包括：

- 立即。使内容在传送后立即过期，该选项适用于，包含不希望放入缓存或频繁更新的敏感信息的内容。
- 之后。设置内容在过期之前经过的时间，适用于定期更新的内容（如每日或每周更新的内容）。首先在对应的框中键入值，然后从列表中选择适当单位即可，如：“秒”、“分钟”、“小时”、“天”。
- 时间。设置内容过期时的准确日期和时间，适用于不希望频繁更改的内容。

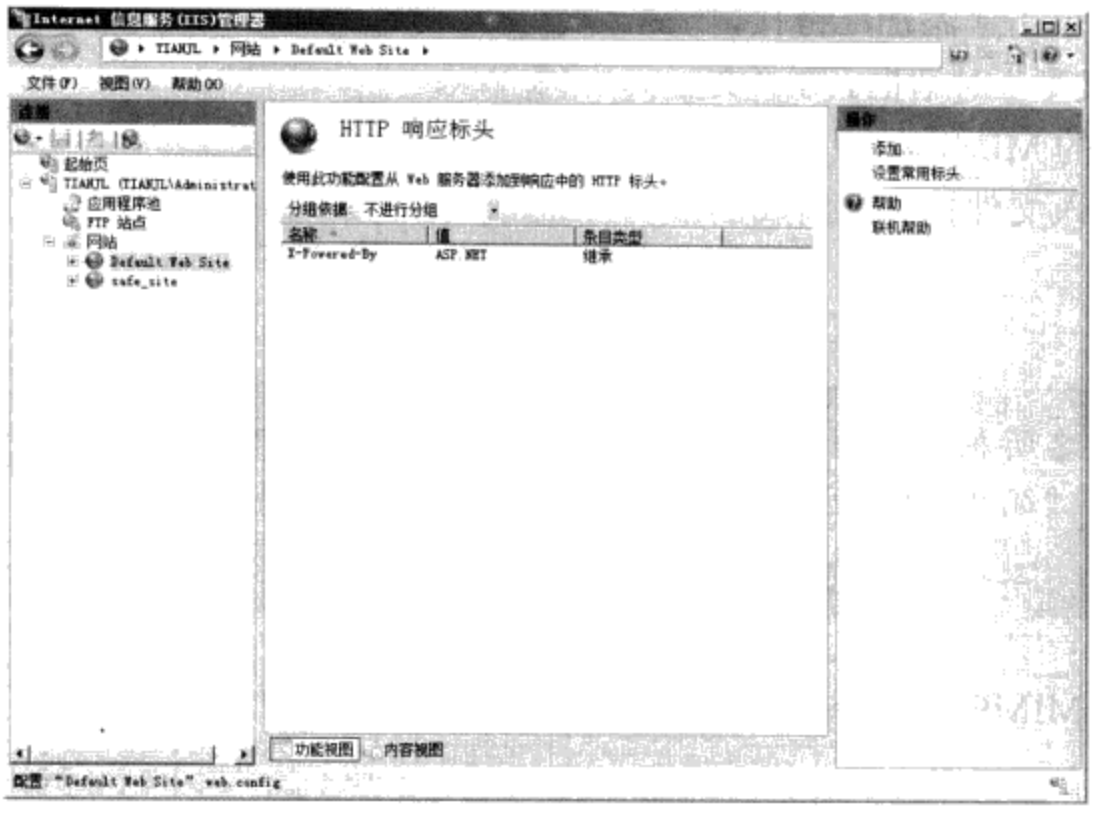


图 5-36 “HTTP 响应标头”窗口

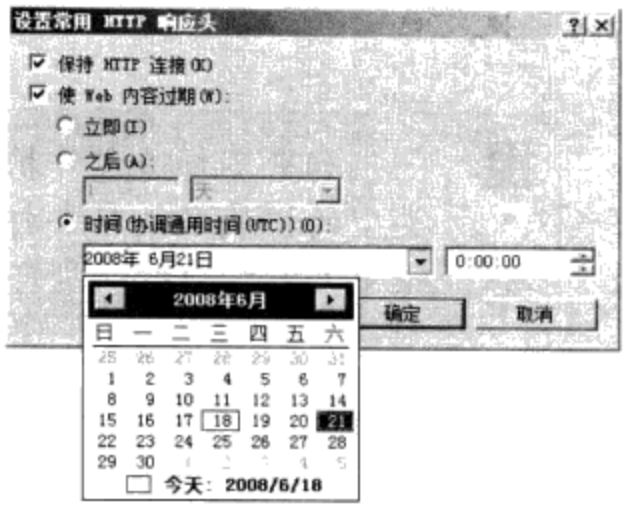


图 5-37 “设置常用 HTTP 响应头”对话框

第 3 步，单击“确定”按钮，保存设置。

5.2.8 添加 MIME 类型

IIS 中的 Web 网站默认支持大部分的文件类型。但是，如果文件类型不为 Web 网站所支持，则在网页中运行该类型的程序，或者从 Web 网站下载该类型的文件时，将会提示无法访问。此时，需要在 Web 网站添加相应的 MIME 类型，如 ISO 文件类型等。MIME（Multipurpose Internet Mail Extensions）即多功能 Internet 邮件扩充服务，可以定义 Web 服务器中利用文件扩展名所关联的程序。

第 1 步，在“Internet 信息服务（IIS）管理器”窗口中，选择希望配置的站点或目录，双击“MIME 类型”图标，显示如图 5-38 所示“MIME 类型”窗口，显示了系统已经集成的 MIME 类型。

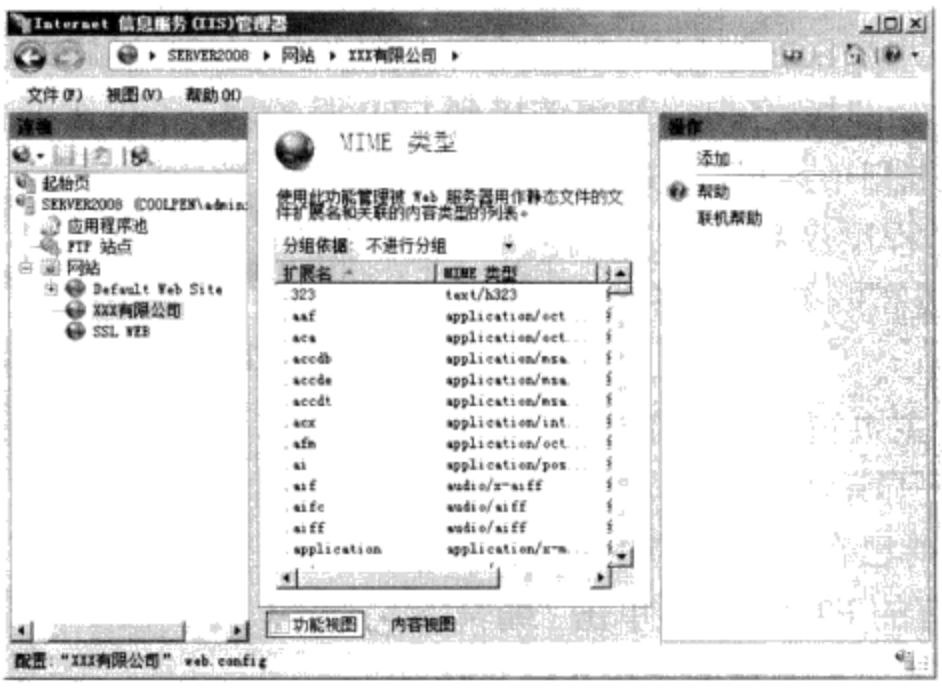


图 5-38 “MIME 类型”窗口

第2步，在“操作”任务栏中单击“添加”链接，显示如图5-39所示“添加MIME类型”对话框。在“文件名扩展名”文本框中键入欲添加的MIME类型，例如“.iso”，“MIME类型”文本框中键入文件扩展名所属的类型。

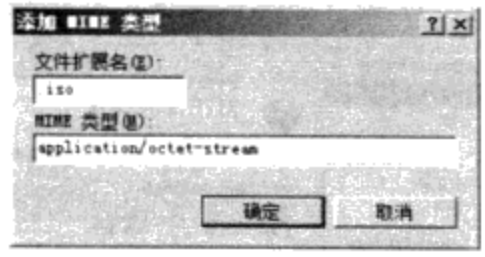


图5-39 “添加MIME类型”对话框

提示 如果不知道文件扩展名所属的类型，可以在MIME类型列表框中选择相同类型的扩展名，双击打开“编辑MIME类型”对话框。在“MIME类型”文本框中复制相应的类型即可。

第3步，单击“确定”按钮，MIME类型添加完成。如果还要添加其他MIME类型，可按如上步骤继续操作。

提示 如果希望处理所有文件而不考虑文件扩展名，则使用通配符“*”添加。

5.3 FTP安全

FTP（File Transfer Protocol，文件传输协议）服务既可以实现局域网文件传输，又可以实现Internet上的文件传输，在企业网络中广泛用于网站管理、协同工作、远程资源共享等。与IIS 7.0相比，IIS 7.5中的FTP服务已经无需单独安装“IIS 6.0管理兼容性”组件，用户可以在添加IIS服务器角色的同时选择安装FTP服务器组件。但是，默认情况下，系统并未创建FTP站点，用户需要手工添加。

5.3.1 设置TCP端口

FTP服务使用的默认TCP端口为21，同Web服务类似，通过修改服务端口也可以达到提高服务器安全的目的。此时，客户端若想链接到FTP服务器，不仅需要指定服务器的IP地址，还需要指定所使用的端口号，虽然访问过程有些繁琐，但可以从一定程度上拒绝客户端匿名链接。建议为安全需求较高的FTP服务器指定特殊TCP端口。

第1步，在FTP主页窗口中，单击“操作”栏中的“绑定”链接，显示“网站绑定”对话框。在列表框中显示了当前已存在的站点的IP地址和端口信息。选择现有的FTP站点，单击“编辑”按钮，显示如图5-40所示“编辑网站绑定”对话框。在“IP地址”下拉列表框中，可以为当前

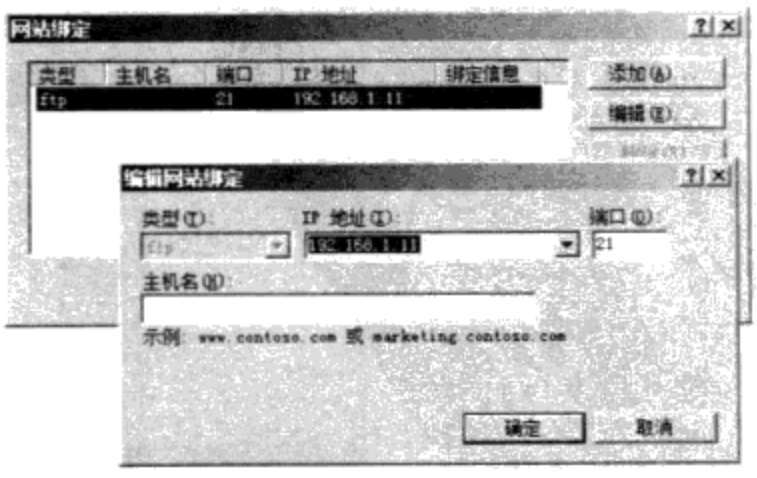


图5-40 “编辑网站绑定”对话框

FTP 站点指定一个 IP 地址；在“端口”文本框中则可指定 FTP 站点的端口，默认为 21。

第 2 步，编辑完成后，单击“确定”按钮保存即可。

> **提示** 在指定 FTP 服务端口时，应避免使用常用服务的 TCP 端口。

5.3.2 连接数量限制

FTP 服务器用来提供文件的上传和下载，但是，FTP 服务传输文件时占用的带宽较多，如果同时访问 FTP 服务器的用户数量比较多，就会占用大量带宽，影响其他网络服务的正常运行。尤其在一些中小型企业，往往一台服务器同时也提供其他多种网络服务，如 Web、Email 等，当并发访问数量较多时，更会因带宽被大量占用造成服务中断或超时。因此，应对 FTP 连接数量进行一定的限制。

在 FTP 主页窗口中，单击“操作”栏中的“高级设置”链接，显示“高级设置”对话框。展开“连接”节点，在“最大连接数”中即可设置允许同时连接的用户数量，如图 5-41 所示。完成后单击“确定”按钮保存即可。

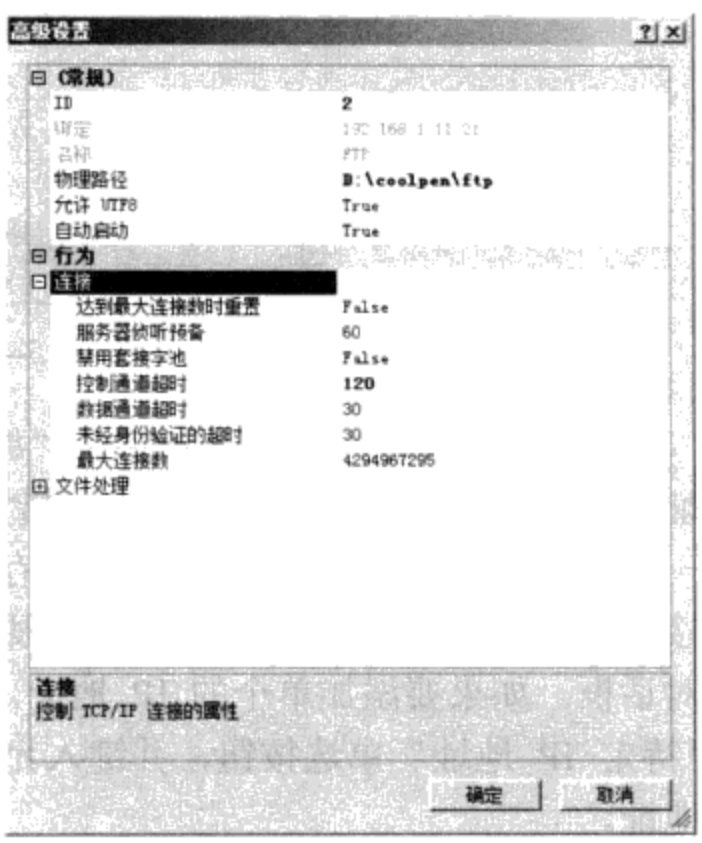


图 5-41 “高级设置”对话框

> **提示** 在该对话框中也可以设置 FTP 站点的主目录，即“物理路径”。

5.3.3 IP 地址访问限制

通过对 IP 地址的限制，可以只允许或拒绝某些特定范围内的计算机访问该 FTP 站点，从而可以在很大程度上避免来自外界的恶意攻击，同时还可以将授权用户限制在某一个特定访问范围内。将 IP 地址限制与用户认证访问结合在一起，可以进一步提高 FTP 站点访问的安全性。

1. 添加允许访问的 IP 地址

如果设置为只允许某一部分 IP 地址访问 FTP 服务器，其他所有 IP 都不允许访问。那么，需要先设置为拒绝所有 IP 地址访问，然后添加允许访问的 IP 地址。操作步骤如下：

第 1 步，在 FTP 站点的“主页”窗口中，双击“FTP IPv4 地址和域限制”图标，显示如图 5-42 所示“FTP IPv4 地址和域限制”窗口。

图 5-42　“目录安全性”选项卡

第 2 步，单击“操作”栏中的“编辑功能设置”链接，显示如图 5-43 所示“编辑 IPv4 地址和域限制设置”对话框。在“未指定的客户端的访问权”下拉列表框中选择“拒绝”选项。

第 3 步，单击“确定”按钮保存设置。然后，单击“操作”栏中的“添加允许条目”链接，显示如图 5-44 所示“添加允许限制规则”对话框。如果要添加单个的 IP 地址，可选择“特定 IP 地址”单选按钮，并键入允许的 IP 地址。

如果要添加一个 IP 地址段，可选择“IP 地址范围”单选按钮，并键入 IP 地址和掩码，如图 5-45 所示。

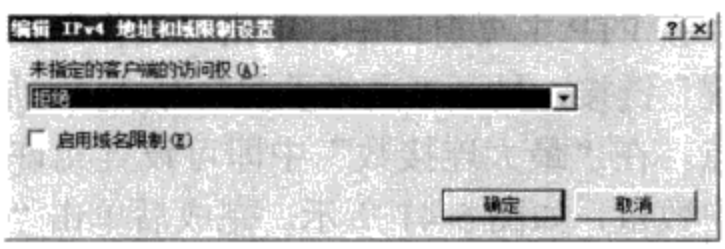


图 5-43　“编辑 IPv4 地址和域限制设置”对话框

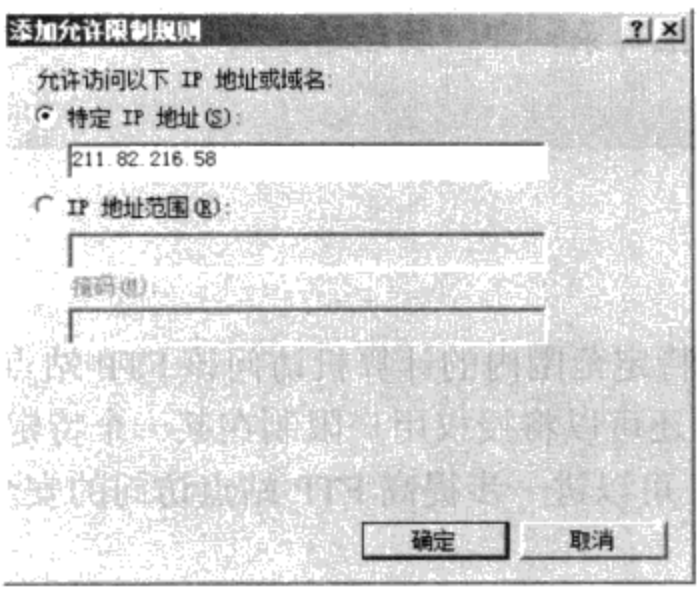


图 5-44　“添加允许限制规则”对话框

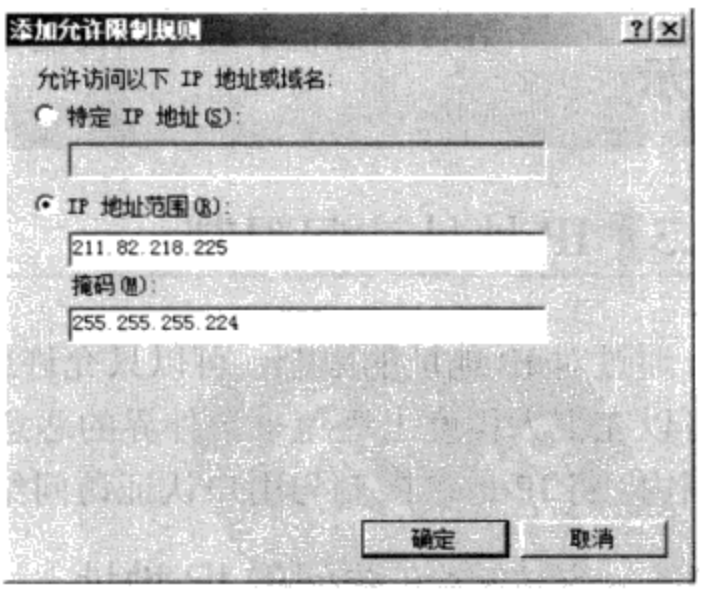


图 5-45　添加 IP 地址范围

第 4 步，完成后单击“确定”按钮保存即可。

2. 设置拒绝访问的 IP 地址

如果设置为拒绝某一部分 IP 地址访问 FTP 服务器，而其他所有 IP 都允许访问。那么，

需要先设置为允许所有 IP 地址访问，然后添加拒绝访问的 IP 地址，操作步骤如下。

第 1 步，单击“操作”栏中的“编辑功能设置”链接，在“编辑 IPv4 地址和域限制设置”对话框的“未指定的客户端的访问权”下拉列表框中，选择“允许”选项。

第 2 步，单击“操作”栏中的“添加拒绝条目”链接，显示如图 5-46 所示“添加拒绝限制规则”对话框，可以设置拒绝访问的 IP 地址或者 IP 地址段。

第 3 步，设置完成后单击“确定”按钮保存即可。

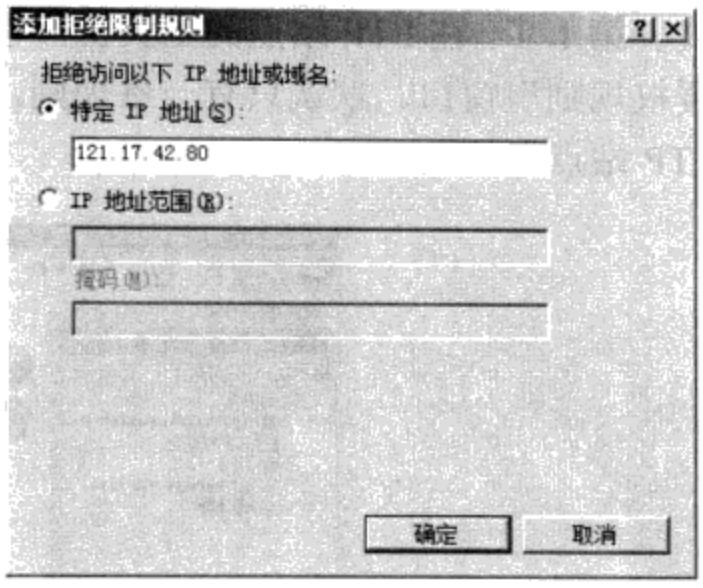


图 5-46 “添加拒绝限制规则”对话框

5.3.4 设置用户身份验证

如果 FTP 服务器上保存有比较重要的资源，不想被用户随意访问，就可以禁用匿名登录，启用身份验证，为特殊用户赋予访问 FTP 站点的权限。

在 FTP 站点的主页窗口中，双击“FTP 身份验证”图标，显示如图 5-47 所示“FTP 身份验证”窗口，可以设置基本身份验证和匿名身份验证。如果要启用身份验证，可选中并单击“操作”栏中的“启用”链接即可。

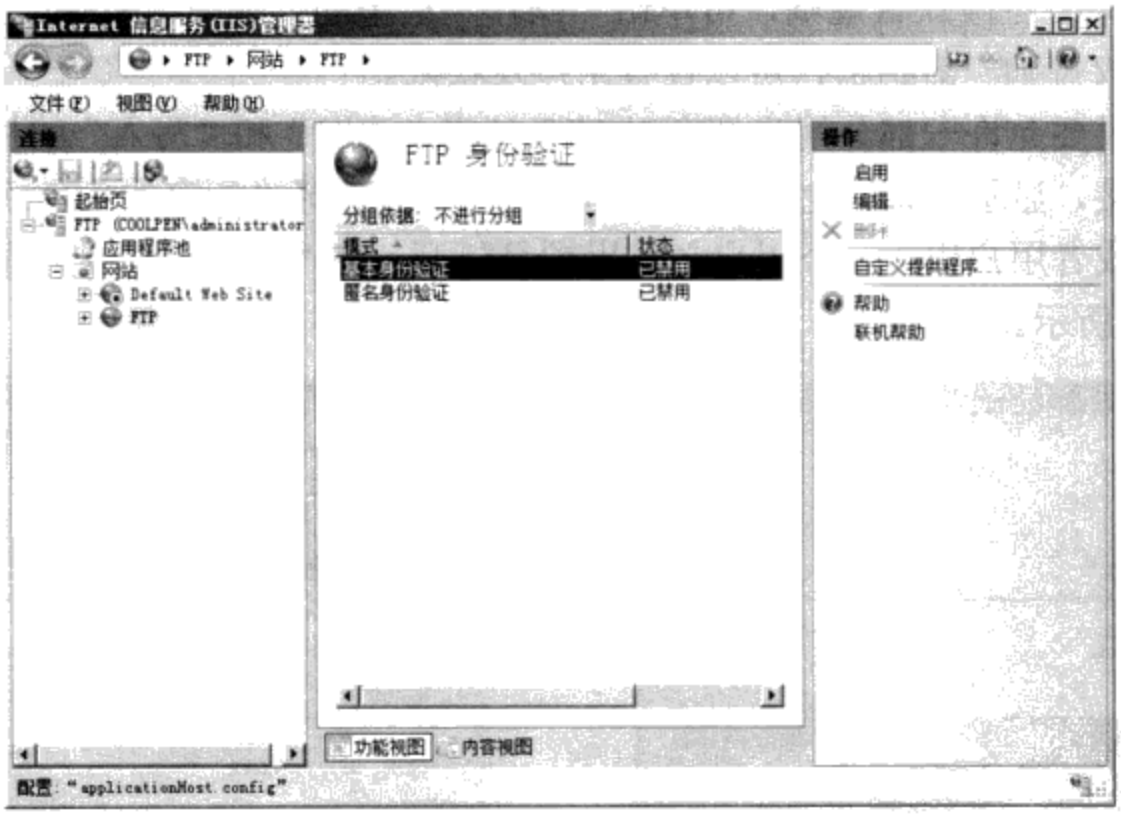


图 5-47 “FTP 身份验证”窗口

如果要允许所有用户匿名访问，可启用“匿名身份验证”；如果要使客户端必须登录才能使用，并且为不同的用户设置不同的权限，则需启用“基本身份验证”，并且该验证方式优先于“基本身份验证”。

5.3.5 设置授权规则

如果要为 FTP 站点指定允许访问的用户，可以通过配置“授权规则”来实现。不过，在

配置授权规则之前，应当禁用“匿名身份验证”，并启用“基本身份验证”功能。

第1步，在FTP站点的主页窗口中，双击“FTP授权规则”图标，显示如图5-48所示“FTP授权规则”窗口。默认只有一条规则，就是创建FTP站点时设置的规则，允许所有用户读取FTP站点上的文件。

图5-48　“FTP授权规则”窗口

第2步，如果要更改默认规则，可单击“操作”栏中的“编辑”链接，显示如图5-49所示“编辑允许授权规则”对话框，可以设置用户及权限。

第3步，如果要允许一部分用户拥有对FTP站点“读取”和“写入”的权限，可单击“添加允许规则”链接，显示“添加允许授权规则”对话框。选择“指定的角色或用户组”单选按钮，并键入用户或者用户组，多个用户之间用顿号隔开；在“权限”区域中选择读取或者写入权限，如图5-50所示。

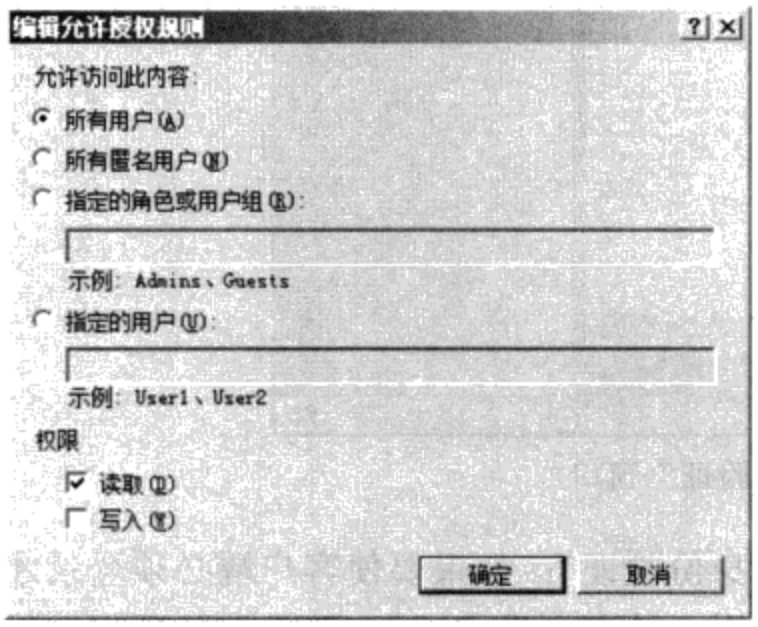


图5-49　“编辑允许授权规则”对话框

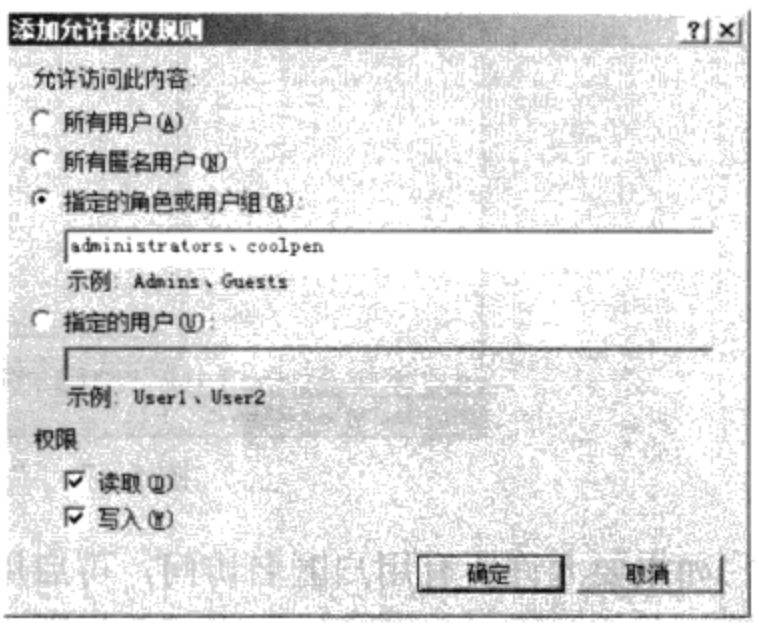


图5-50　指定角色或用户组

第4步，单击“确定”按钮即可添加该规则。如果要拒绝一部分用户访问该FTP站点，则可单击“添加拒绝规则”链接，显示如图5-51所示“添加拒绝授权规则”，设置拒绝访问的用户或用户组即可。

第5步，添加完成后的规则显示如图5-52所示，并且所做的设置会即时生效。

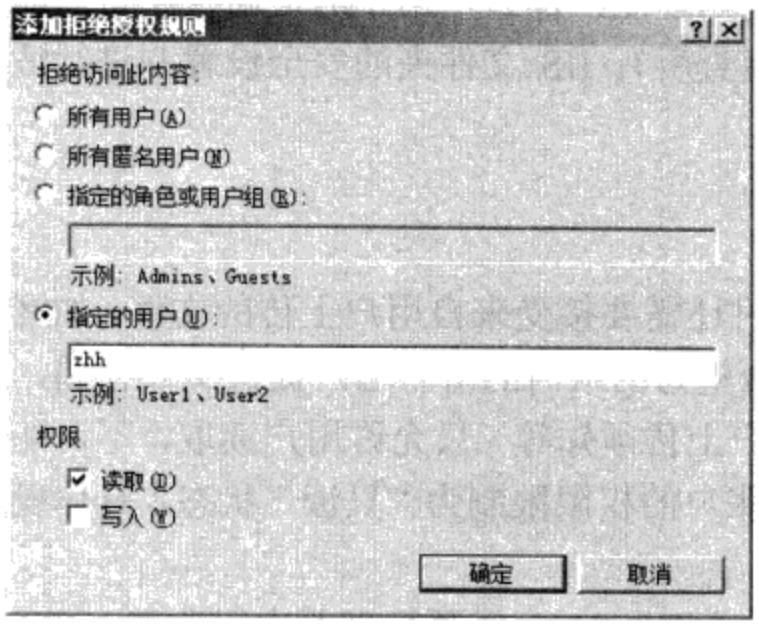


图 5-51　指定用户

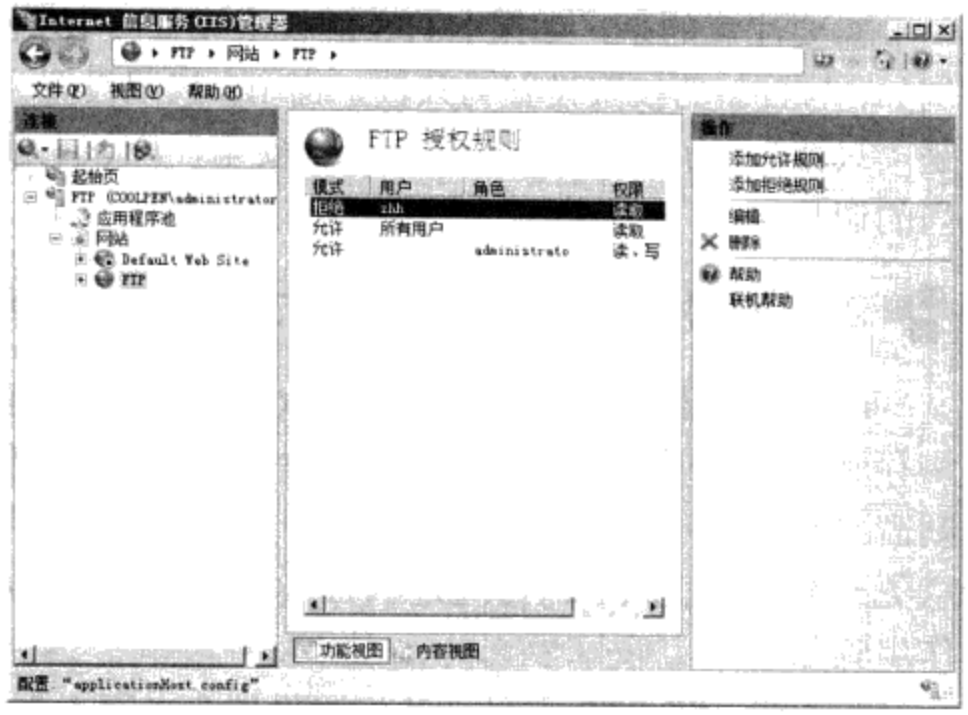


图 5-52　授权规则

5.3.6 基于 NTFS 权限设置的访问控制

使用 NTFS 文件系统时，必须为用户账户授予相应的 NTFS 权限，才能访问相应的文件或文件夹，在一定程序上保护了数据的安全。需要注意的是，NTFS 的安全性在本地计算机或网络中都是有效的。无论是以用户身份登录到服务器，还是通过网络访问共享文件夹，NTFS 安全性都有效。因此，从安全性角度考虑，应为 IIS 设置 NTFS 权限。

1. IIS 服务中的 NTFS 权限设置

无论使用 IIS 搭建 Web 服务还是 FTP 服务，都应将文件存储在 NTFS 分区内，并利用 NTFS 权限来增加数据的安全性。IIS 的默认安装文件夹为 inetpub，用户安装和配置的所有 Web 站点和 FTP 站点信息都被保存在这里。如果需要配置的 FTP 站点位于其他目录，则设置相应目录的 NTFS 权限即可，这里以默认目录为例进行介绍。

在 Windows 资源管理器中，右击 ftproot 并选择快捷菜单中的“属性”选项，打开“ftproot 属性”对话框，切换至“安全”选项卡，单击“编辑”按钮，显示如图 5-53 所示“ftproot 的权限”对话框。

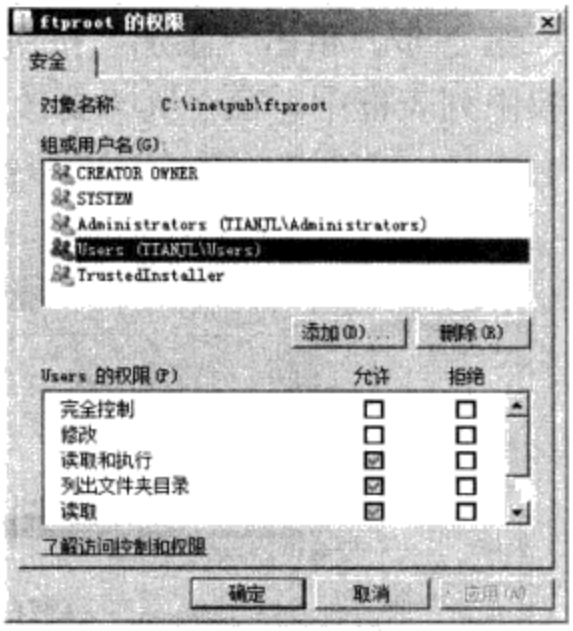


图 5-53　“ftproot 的权限”对话框

提示　在“Internet 信息服务（IIS）管理器”窗口中，右击 FTP 站点，选择快捷菜单中的“编辑权限”选项，也可以打开该对话框。

在“组或用户名称”列表框中，显示了可以访问该文件夹的用户账户，选择一个用户，会在下面的权限列表中，显示该用户所拥有的对该文件夹的访问权限。默认情况下，允许多个用户组的用户访问，可以修改用户账户相应的访问权限，也可以直接删除用户账户。

需要注意的是，如果NTFS的权限设置与IIS权限设置发生冲突，以最严格的设置为准。例如，NTFS的权限设置为只读，而IIS权限设置为完全控制，那么，用户的访问权限将只能是“只读”。为了使服务器尽可能地安全，应该重新检查所有IIS文件夹的安全设置并进行适当的调整。

2. 限制用户对主目录中子文件夹的访问

FTP服务器不仅要允许用户读取服务器数据，有时还需要接受来自用户上传的文件，如网络存储中的公用空间（以share文件夹为例），如果希望为网络内的所有用户提供文件存储，则需要赋予用户写入权限，但是其中有些内容（如用户上传须知等）只允许用户读取，不可随意更改或删除，此时即可通过NTFS权限将指定用户账户的权限限制为“只读”状态，具体操作步骤如下。

第1步，将FTP主目录的权限设置为“写入”，并在Windows资源管理器中修改其NTFS权限为：允许指定用于访问FTP的用户账户“写入”数据。右击“share”文件夹，选择快捷菜单中的“属性”选项，打开“share 属性”对话框，切换至“安全”选项卡，在“组或用户名”选项框中，单击“编辑”按钮，显示如图5-54所示“share 的权限”对话框。

提示 系统默认，只为SYSTEM组、Administrators组和TrustedInstaller组赋予了“写入”权限，如果FTP服务器登录账户不属于这些组，则必须为其赋予“写入”权限。

第2步，单击“添加”按钮，将用于FTP服务器访问的用户账户添加到列表框中，在用户权限列表框中，赋予其“修改”权限，如图5-55所示。

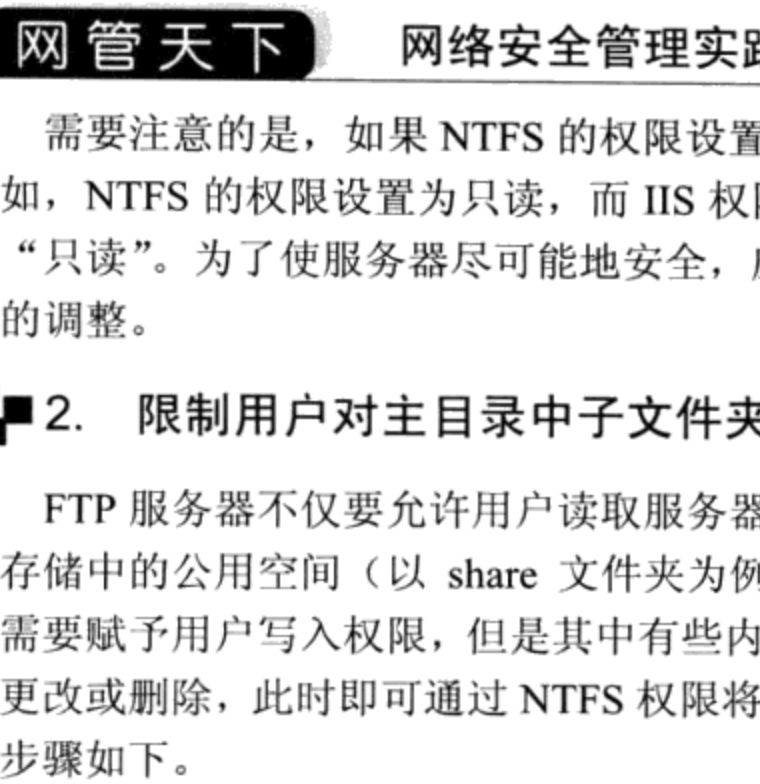


图5-54 “share 的权限”对话框

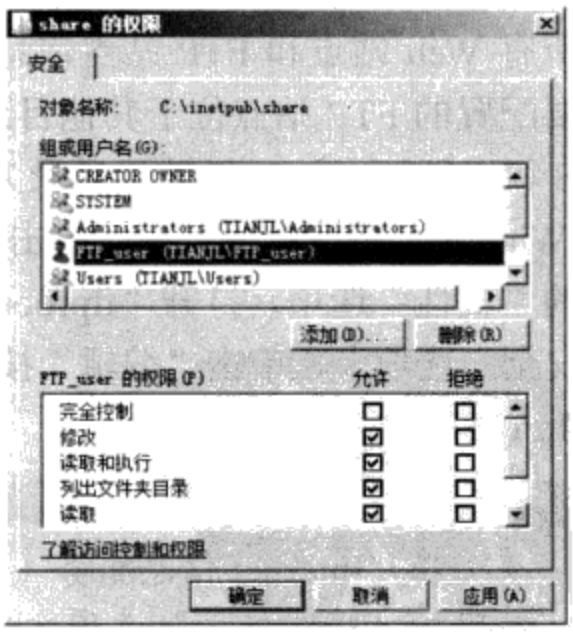


图5-55 添加用户账户并修改权限

第3步，单击“确定”按钮，关闭对话框。

第4步，在“share”文件夹下创建“用户上传须知”文件夹。默认情况下，该文件夹将自动继承“share”文件夹的NTFS权限，即仍然具有“写入”权限，如图5-56所示。

第5步，单击“编辑”按钮，显示如图5-57所示对话框，当前“权限项目”列表框中的

用户权限设置，都是继承的其父目录的权限设置。

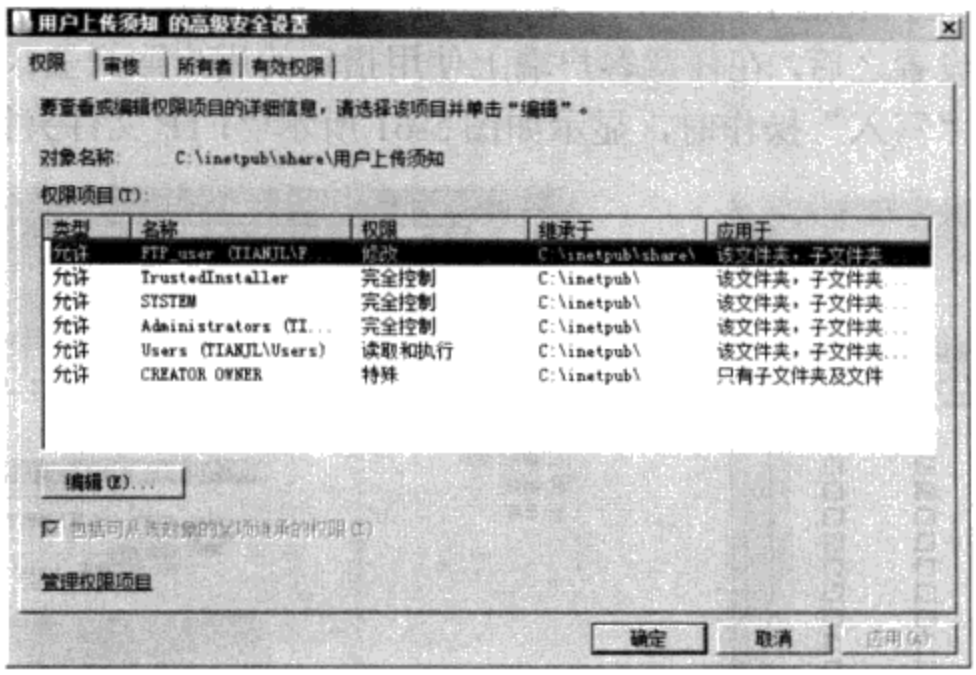


图 5-56 “用户上传须知 的高级安全设置”对话框

第 6 步，取消“包括可从该对象的父项继承的权限”复选框，显示如图 5-58 所示“Windows 安全”对话框，提示取消权限即成后可能出现的问题。

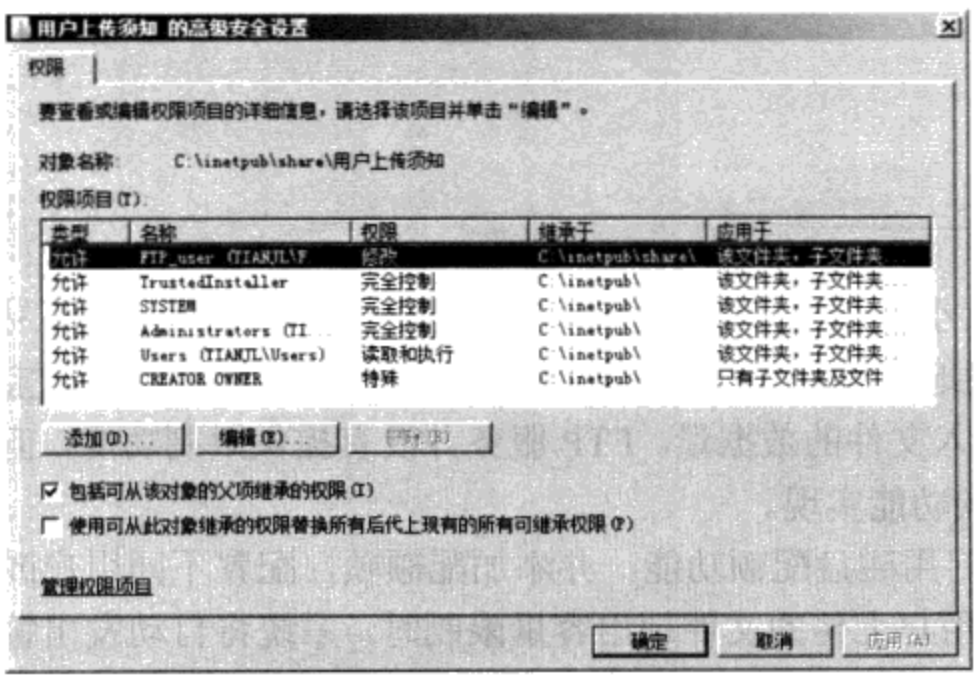


图 5-57 编辑文件加 NTFS 权限

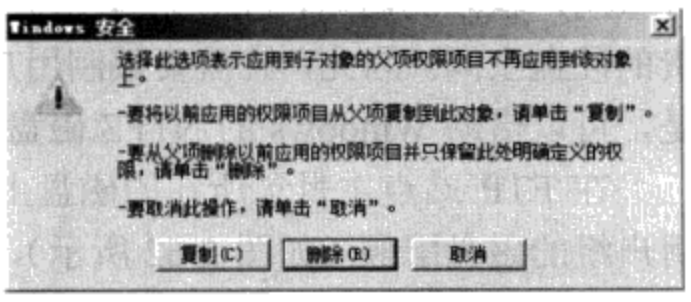


图 5-58 “Windows 安全”对话框

第 7 步，单击“删除”按钮，所有继承用户权限设置都将随之删除，如图 5-59 所示。

第 8 步，单击“添加”按钮，选择 FTP_user 账户，显示如图 5-60 所示“用户上传须知 的权限项目”对话框，在“应用于”下拉列表框中，选择“只有该文件夹”选项，在“权限”列表框中，选择“遍历文件夹/执行文件”、“列出文件夹/读取数据”、“读取属性”、“读取扩展属性”和“读取权限”后的“允许”复选框。

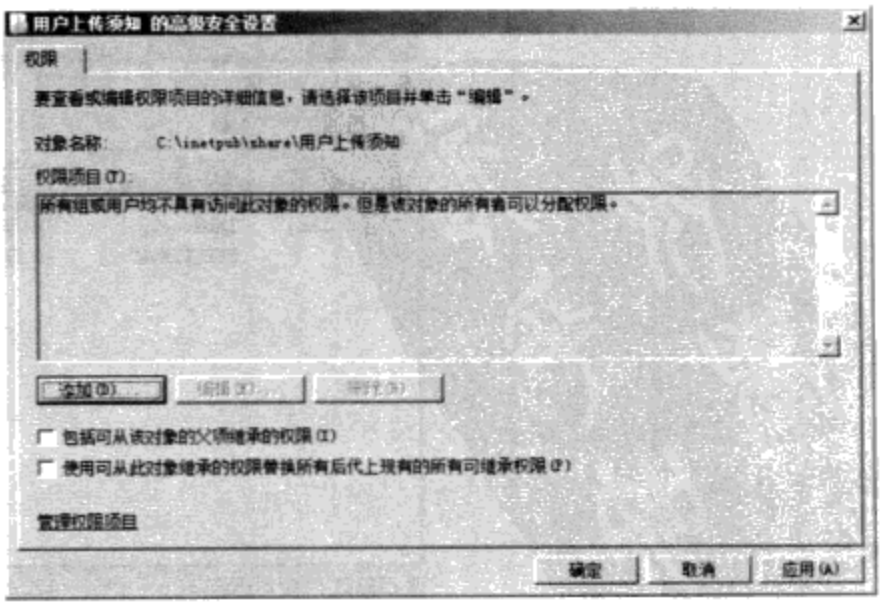


图 5-59 取消当前文件夹继承的父项权限

第 9 步，单击“确定”按钮，将其添加至“权限项目”列表框中。按照相同的方法，将 Administrators 组添加至列表框中，赋予“完全控制”权限，以便日后查看和管理。

完成 NTFS 权限设置之后，在任意客户端上使用指定的用户账户登录后，在“用户上传须知”文件夹中，执行“写入”操作时，显示如图 5-61 所示“FTP 文件夹错误”对话框。

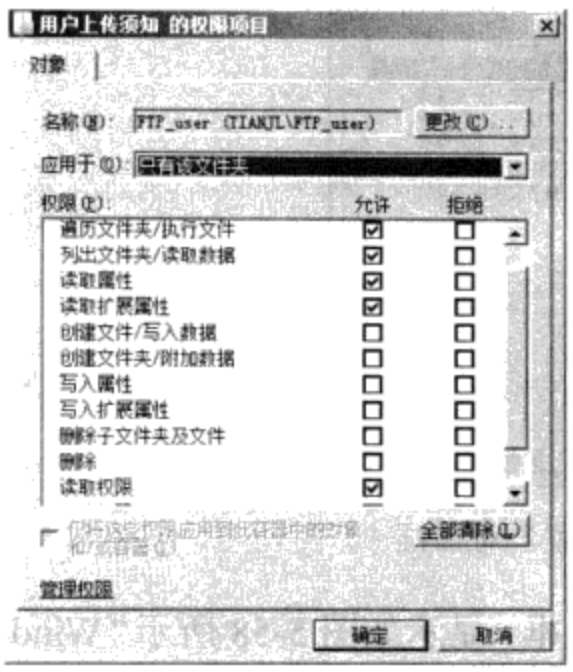


图 5-60 “用户上传须知 的权限项目”对话框

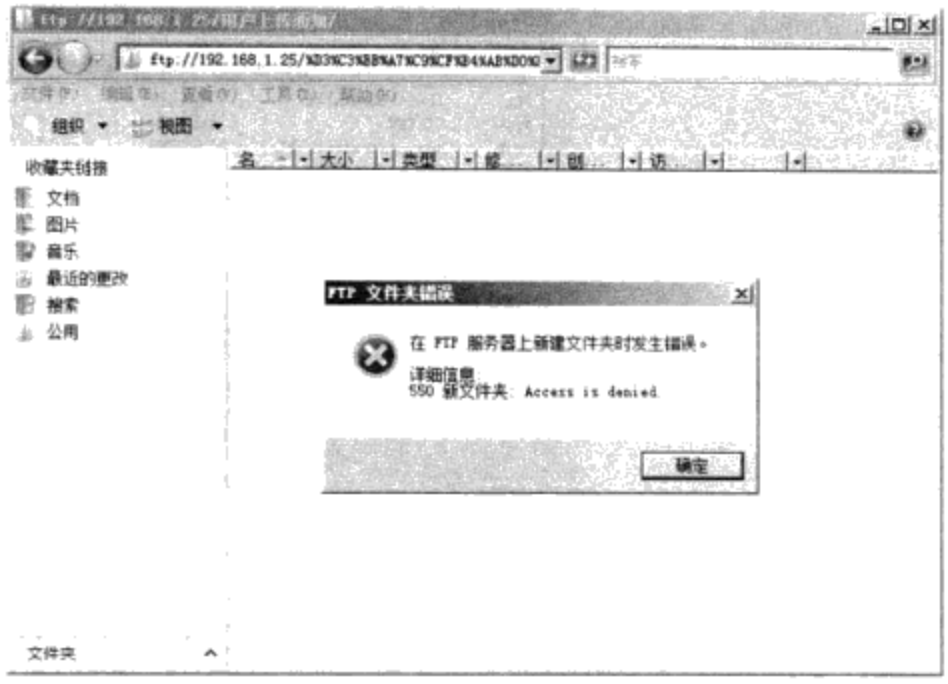


图 5-61 客户端测试结果

5.3.7 限制用户的上传空间

FTP 服务并不限制用户上传文件的大小，因此，当赋予了 FTP 用户写入权限时，就容易导致用户权限的滥用，用户可能会无限制地将大量文件保存在 FTP 服务器，从而占用大家宝贵的硬盘空间。因此，就需要限制用户写入文件的数据量。FTP 服务并没有提供限制功能，但是，可以借助 Windows 的 NTFS 磁盘配额功能实现。

在 FTP 站点主目录所在的磁盘上，启用磁盘配额功能，并添加配额项，配置不同用户或用户组的磁盘配额（如图 5-62 所示），当用户上传的文件超出容量限制时，系统将自动发出警告，提示用户超出空间配额，不能继续上传。当然，FTP 主目录必须位于 NTFS 系统分区，FAT32 格式的分区无法设置磁盘配额。

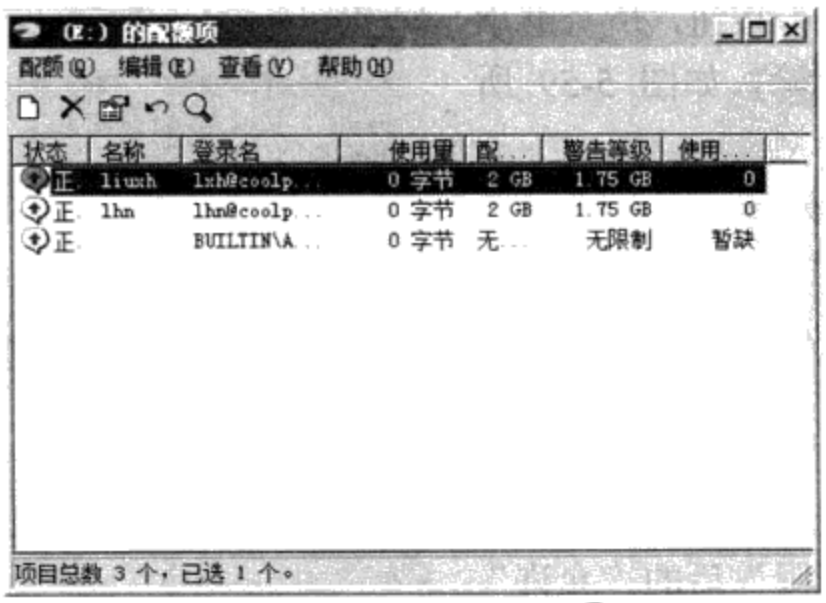


图 5-62 磁盘配额

第 6 章　事件、日志和警报

排除系统或网络故障时，管理员最想知道的就是最近有哪些用户访问，进行了哪些操作，而这些问题都要靠日志来解决。Windows Server 2008 R2 系统为管理员提供了迹象非常实用的功能，包括安全审核功能、性能日志、警报。安全审核可以用日志的形式记录好几种与安全相关的事件，可以使用其中的信息来生成一个有规律活动的概要文件，发现和跟踪可疑事件，并留下关于某一侵入者活动的有效证据。

6.1　事件查看器

Windows 事件查看器可用于浏览和管理事件日志，是监视系统的运行状况以及在出现问题时解决问题的必不可少的工具。管理员应该养成良好的习惯，经常查看日志，可以有效的避免突如其来的灾难。从 Windows Server 2008 R2 系统开始，新增了“自定义视图”和“应用程序和服务日志”功能，并且在“Windows 日志”中添加了“安装程序”和“转发的事件”查看功能，极大地提高了网络管理员的工作效率。

6.1.1　事件查看器概述

1.　事件基本信息

事件日志类似于日记，主要用于记录某一系统事件发生的日期、时间等基本信息，事件是操作系统在某一时刻对某一系统资源或者网路资源发生的访问操作，而记录的一系列行为，该行为包含当前的日期、时间、用户、计算机、来源、事件、类型、分类等信息。如表 6-1 中显示了事件的基本要素及描述。

表 6-1　事件基本信息

要素	描述
日期和时间	事件发生的日期和时间。事件的日期和时间以协调通用时间(UTC)存储，但始终按查看者的区域设置显示
用户	事件发生所代表的用户的名称。如果事件实际上是由服务器进程所引起的，则该名称为客户 ID；如果没有发生模仿的情况，则为主 ID。在可用时，安全日志条目包括主 ID 和模仿 ID。当该服务器允许一个进程采用另一个进程的安全属性时，则产生模仿
计算机	产生事件的计算机的名称。这通常是您自己的计算机的名称，除非您在另一台计算机上查看事件日志
来源	记录事件的应用程序，它可为程序名（如"SQLServer,"）、系统的组件（如驱动程序）或大程序的组件。例如，"Elnkii"指示 EtherLinkII 驱动程序。“来源”始终使用其原始语言
事件 ID	标识此来源的特定事件类型的数字。说明的第一行一般包含事件类型的名称。例如，6005 是在启动事件日志服务时所发生事件的 ID。这类事件说明的第一行是“事件日志服务已启动”。通过结合使用“来源”和“事件”的值，产品支持代理可解决系统问题
级别	事件严重性的分类，包括信息、警告、错误、关键、Success Audit、审核失败等 6 个级别。在“事件查看器”中的正常列表方式下查看，它们都由一个符号表示
操作代码	包含标识活动或应用程序引起事件时正在执行的活动中的点的数字值。例如，初始化或关闭
日志	已记录事件的日志的名称
任务类别	用于表示事件发行者的子组件或活动
关键字	可用于筛选或搜索事件的一组类别或标记，包括“网络”、“安全”或“未找到资源”

2. 事件的类型

Windows 操作系统中定义了 6 种事件类型，系统管理员可以根据关注的事件的性质筛选希望查看的事件。表 6-2 显示了 Windows 系统定义的事件类型，及每个事件类型的具体含义。

表 6-2 事件类型及描述

事件类型	描述
错误	指明出现了问题，这可能会影响触发事件的应用程序或组件外部的功能。例如，如果在启动过程中某个服务加载失败，将会记录“错误”事件
警告	指明出现的问题可能会影响服务器或导致更严重的问题（如果未采取措施）。例如，当磁盘空间不足时，将会记录“警告”事件
信息	指明应用程序或组件发生了更改，如操作成功完成、已创建了资源，或已启动了服务
关键	指明出现了故障，导致触发事件的应用程序或组件可能无法自动恢复
Success Audit	指明出现了故障，导致触发事件的应用程序或组件可能无法自动恢复
审核失败	指明用户权限练习失败

提示 “Success Audit”和“审核失败”类型事件属于严重安全级别，可能出现在安全日志中。

3. 事件日志分类

通常情况下，计算机存储的事件日志类型包括 Windows 系统日志、服务器角色日志、应用程序和服务日志。其中，Windows 系统日志是系统默认的，包括应用程序、安全、Setup、系统和转发的事件等 5 部分，服务器角色日志和应用程序日志则取决于当前服务器运行服务和应用程序。

■ Windows 系统日志

Windows Server 2008 R2 系统日志类包括如下 4 种：

- 应用程序日志。应用程序日志包含由应用程序或系统程序记录的事件。例如，数据库程序可在应用程序日志中记录文件错误。应用程序开发人员决定记录哪些事件。
- 安全日志。安全日志记录诸如有效和无效的登录尝试等事件，以及记录与资源使用相关的事件，如创建、打开或删除文件或其他对象。例如，如果已启用登录审核，登录系统的尝试将记录在安全日志中。
- 系统日志。系统日志包含 Windows 系统组件记录的事件。例如，在启动过程中加载驱动程序或其他系统组件失败将记录在系统日志中。服务器预先确定由系统组件记录的事件类型。
- Setup 日志。Setup 日志，记录在系统安装或者安装微软公司的产品时，产生的系列事件，如果安装出现错误，可以使用此日志分析出现的问题。

运行 Windows Server 2008 R2 操作系统且配置为域控制器的计算机以另外 3 种日志记录事件：

- 目录服务日志。目录服务日志包含 Active Directory 服务记录的事件。例如，在目录服务日志中记录服务器和全局编录间的连接问题。
- 文件复制服务日志。“文件复制”服务日志包含 Windows 文件复制服务记录的事件。例如，在文件复制日志中，记录着文件复制失败和域控制器（利用关于系统卷更改的信息）更新时发生的事件。运行 Windows 并配置为域名系统（DNS）服务器的计算机在其他日志中记录事件。
- DNS 服务器日志。DNS 服务器日志包含 DNS 服务记录的日志。

另外，根据所安装服务的情况，计算机可能会提供其他类型的事件和事件日志。

■ 应用程序和服务日志

应用程序和服务日志是一种新类别的事件日志，主要是来自单个应用程序或组件的事件。这类日志包括 4 种。

- 管理日志。理日志可以提供有关如何对事件做出响应的指南。管理事件主要以最终用户、管理员和技术支持人员为目标。管理通道中的事件指示问题以及管理员可以操作的良好定义的解决方案。
- 操作日志。操作日志主要面向 IT 专业人士。操作事件是用于分析和诊断问题或发生的事件，这些事件可以用于基于问题或发生的事件触发工具或任务。
- 分析日志。默认情况下，分析日志和调试日志都为隐藏和禁用状态，用户使用之前必须先将其启用。分析事件是大量发布的事件，这些事件描述程序操作并指示用户干预所无法处理的问题。
- 调试日志。调试日志由开发人员在调试应用程序时使用。

6.1.2 查看事件信息

通过 Windows Server 2008 R2 系统的事件查看器，可以管理服务器角色日志、Windows 系统日志和应用程序日志。事件日志中记录了事件发生的时间、事件来源、用户账户、操作代码及了解详细相关信息的超级链接，管理员通过这些信息可以快速判断服务器或应用程序是否存在故障或安全隐患。在 Windows Server 2008 R2 系统中，事件日志详细信息的基础结构完全符合 XML 架构，且可以访问代表给定事件的 XML。

第 1 步，打开“事件查看器”窗口，在左侧目录栏中展开希望查看和管理的事件日志类别，如“Windows 日志”→“安全”，如图 6-1 所示。系统默认已经启动“预览窗格”功能，即在事件列表中选择时间后，将自动显示相应预览信息。

第 2 步，双击其中的任何一个日志，便可查看详细信息。在日志属性窗口中，可以看到事件发生的日期，事件发生的源，事件发生的种类和 ID，以及事件的详细的描述，这些信息有助于帮助系统管理员解决安全问题。如图 6-2 所示是打开一个审核失败的安全事件。

第 3 步，单击“详细信息”切换至如图 6-3 所示“详细信息”选项卡，系统默认是以“友好视图”方式显示的。

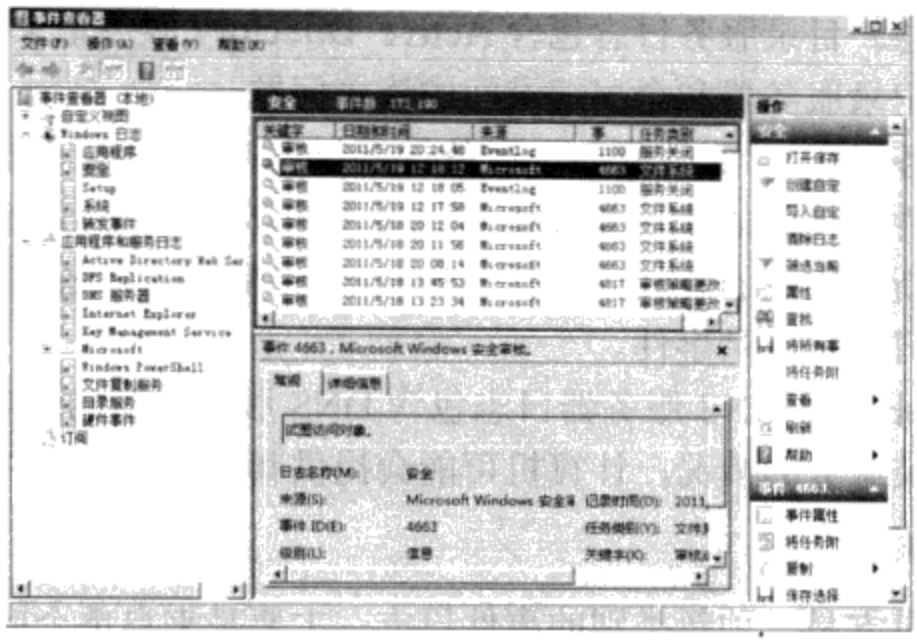


图 6-1　“事件查看器”窗口

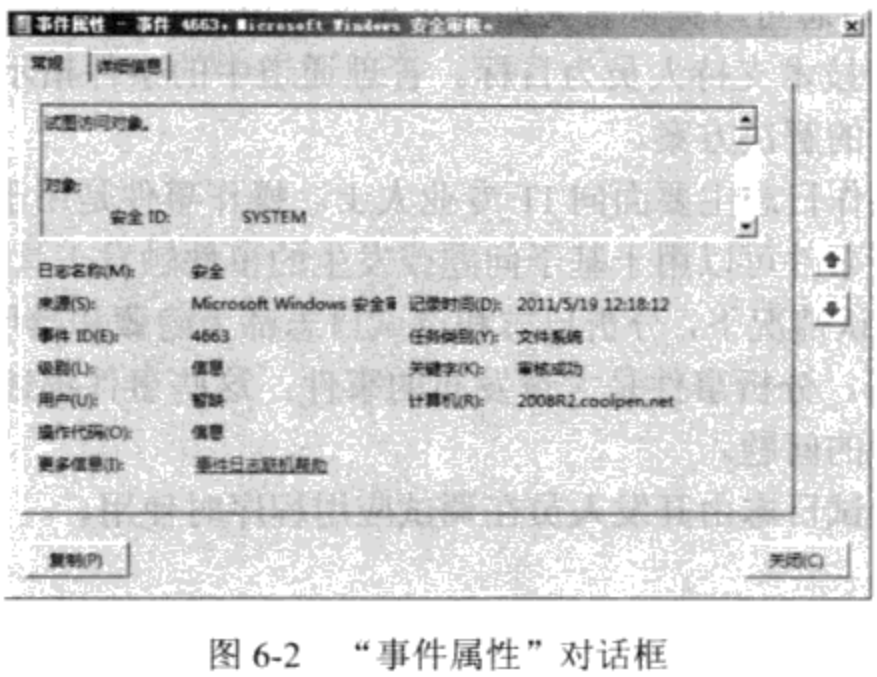


图 6-2　“事件属性”对话框

图 6-3　友好视图

提示　对于熟悉微软操作系统的用户而言，“友好视图”模式就可以看清事件的基本信息。在规模较大的网络中，管理员往往会借助专用的日志管理软件，了解事件信息，此时则可以选择“XML 视图”单选按钮，将 XML 格式的日志信息发送到日志管理软件即可。

6.1.3 将任务附加到日志

Windows Server 2008 R2 系统的事件查看器新增了通知、提醒功能，通过将计划任务附加到指定类型的事件，系统即可自动以某种方式通知用户，如发送 E-mail 邮件、弹出提示信息、开启程序等。可以选择一类系统事件作为关联对象，也可以选择单个事件进行关联。

第 1 步，在“事件查看器”窗口中，右击“Setup”（此处以“Setup”类别的 Windows 事件为例），并在快捷菜单中选择“将任务附加到日志”选项，启动“创建基本任务向导”界面。连续单击“下一步”按钮，在“创建基本任务”对话框中，设置任务名称和描述信息。在“操作”对话框中，定义当事件发生后，希望发生的操作，这里选择“发送电子邮件”单选按钮，如图 6-4 所示。

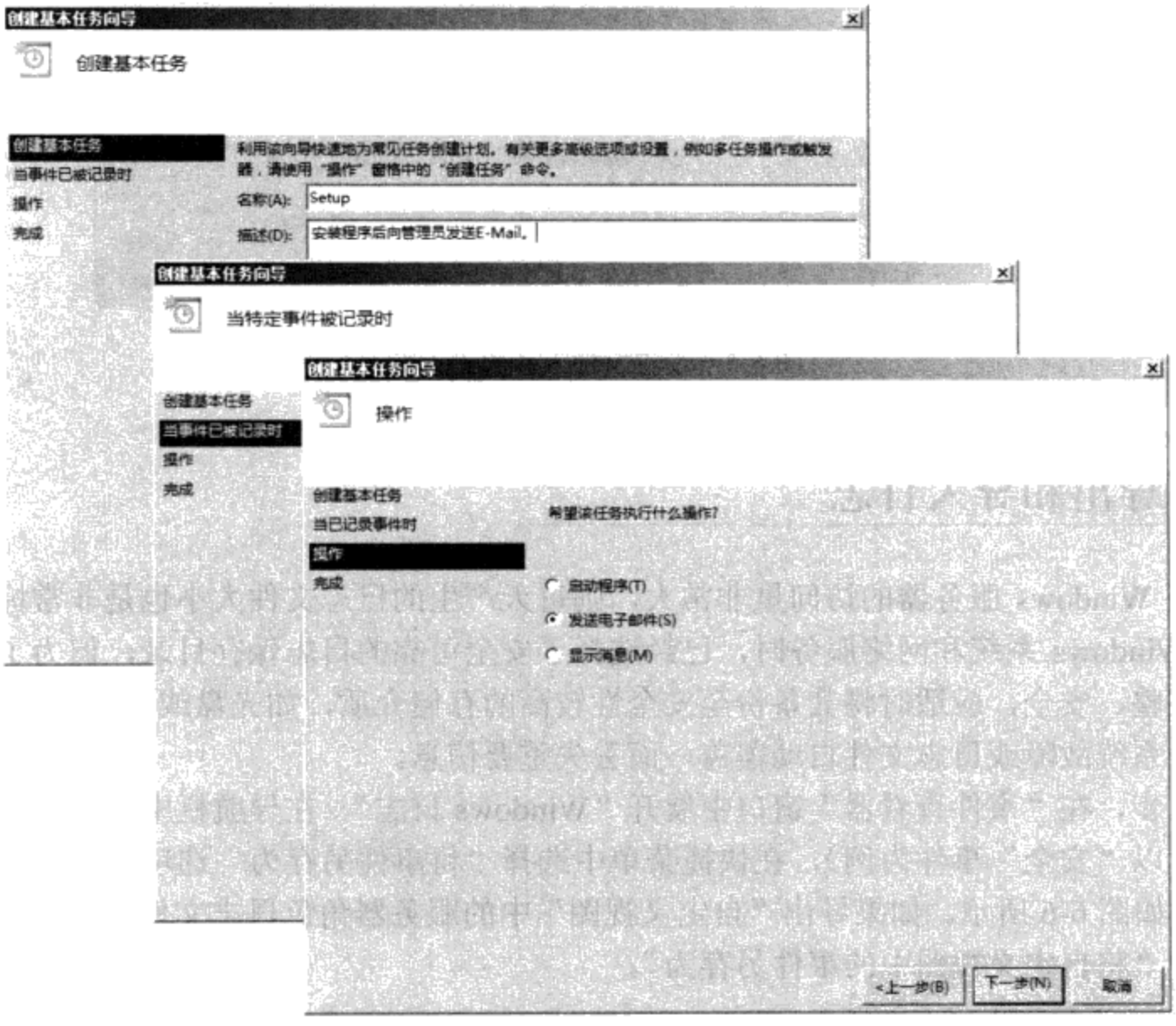


图 6-4　配置任务基本信息和操作

第 2 步，连续单击“下一步”按钮，在“发送电子邮件”对话框中，设置“发件人”和“收件人”的 E-mail 邮箱地址。在“摘要”对话框中，提示当前已做的所有设置，如图 6-5 所示。单击“完成”按钮，提示计划任务已创建完成，可以在“任务计划程序”中查看和编辑计划的任务。

第 3 步，单击“确定”按钮，关闭对话框即可。

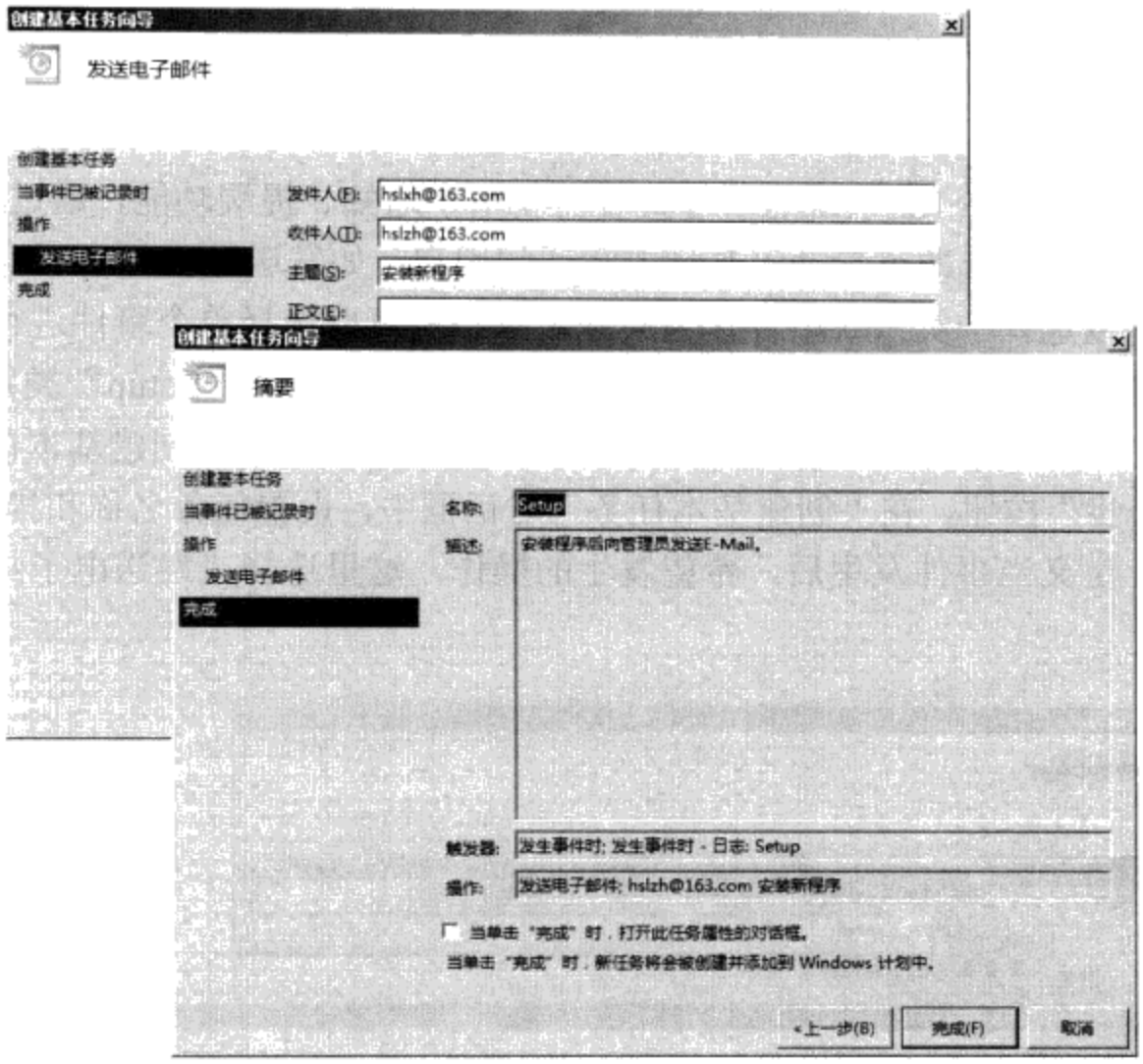


图 6-5 设置发件人和收件人信息

6.1.4 导出和导入日志

如果 Windows 服务器的访问量非常大，则每天产生的日志文件大小也是非常惊人的，尽管安装 Windows 系统和网络服务时，已经选择了安全可靠的日志保存目录，但为了确保日志文件的完整、安全，应适时将其备份至安全性较高的存储介质，如光盘或其他文件服务器等，以免由于系统故障或日志文件自动覆盖，而丢失重要信息。

第 1 步，在“事件查看器”窗口中展开“Windows 日志”，在导航栏中右击希望导出的时间类型（以“安全”事件为例），在快捷菜单中选择“将事件另存为”选项，显示“另存为”对话框，如图 6-6 所示。如果导出“自定义视图”中的服务器角色日志文件，则需要选择快捷菜单中的“将自定义视图中的事件另存为”。

提示 *.evtx 是 Windows Server 2008 R2 和 Windows Server 2008 系统的新文件格式，无法应用于 Windows Server 2003 以及 Windows XP 系统。

第 2 步，设置名称后单击“保存”按钮，打开如图 6-7 所示“显示信息”对话框，系统默认选择“没有显示信息”单选按钮，此时导出日志只能在本地计算机或与本地计算机语言类型相同的其他计算机上打开。如果希望此日志可以在其他系统中查看，则需要选择“显示这些语言的信息”单选按钮，并在列表框中选择与指定计算机系统匹配的语言类型。选中“显示所有

可用的语言”复选框，即可显示当前系统支持的所有语言类型。

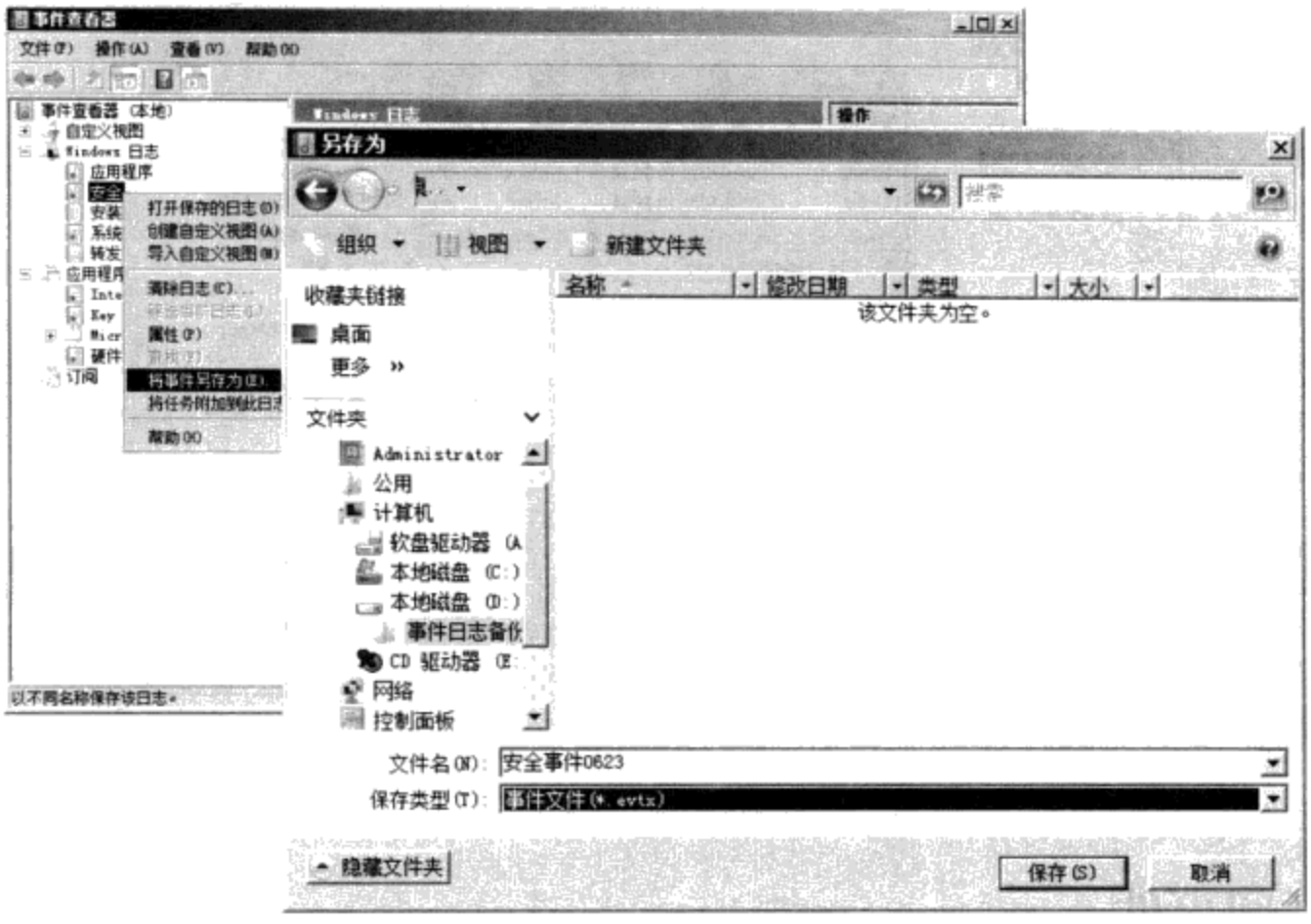


图 6-6　保存事件

第 3 步，单击“确定”按钮，保存日志。

第 4 步，在其他计算机的“事件查看器”窗口中，右击导航栏中的任意项目，并选择快捷菜单中的“打开保存的日志”，选择希望导入的目标文件，单击“打开”按钮，显示如图 6-8 所示“打开保存的文件”对话框，默认将在“事件查看器”导航栏中创建“保存的日志”项目，用于保存所有导入事件文件。选中“所有用户”复选框，则本地计算机上的所有用户均可以通过事件查看器查看当前文件，取消则只有本地管理员账户可以查看该文件。

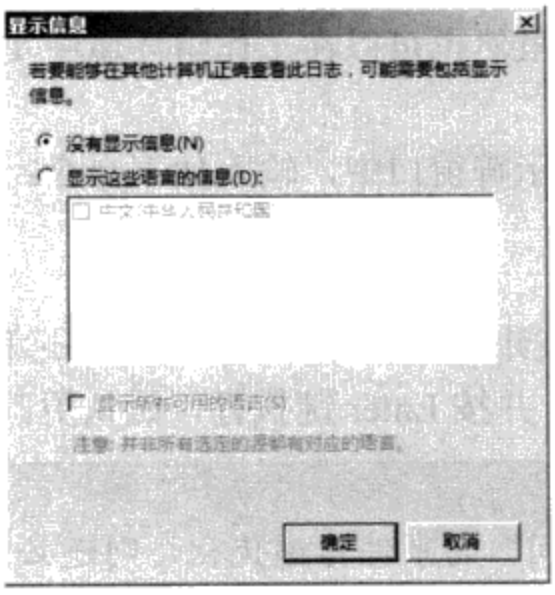


图 6-7　“显示信息”对话框

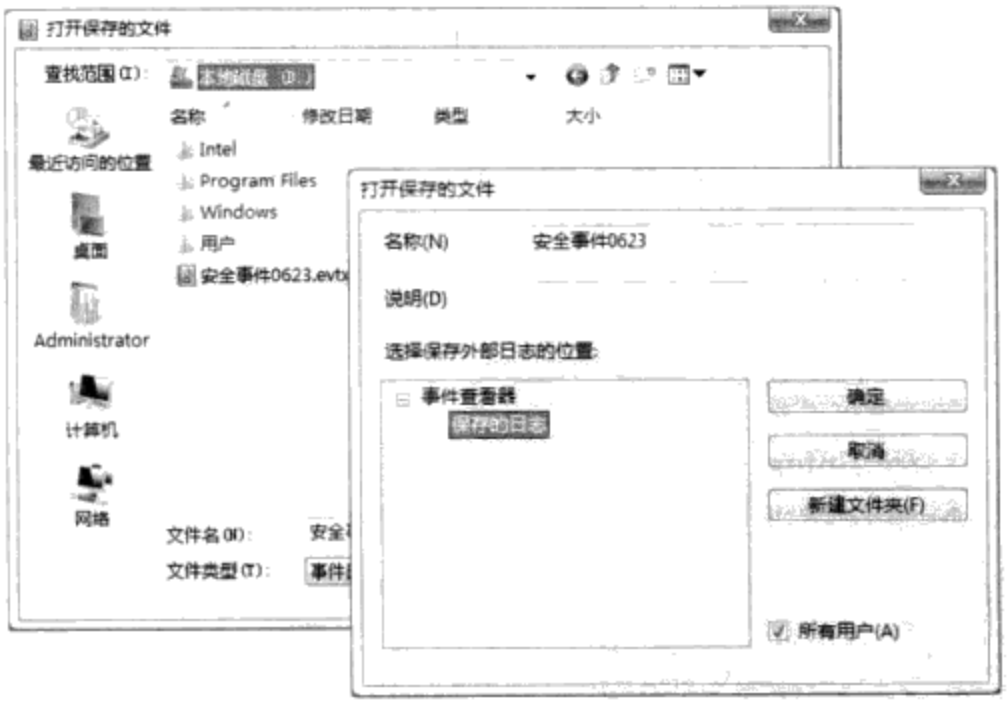


图 6-8　“打开保存的文件”对话框

第 5 步，单击“确定”按钮，即可添加到“事件查看器”窗口中，如图 6-9 所示。

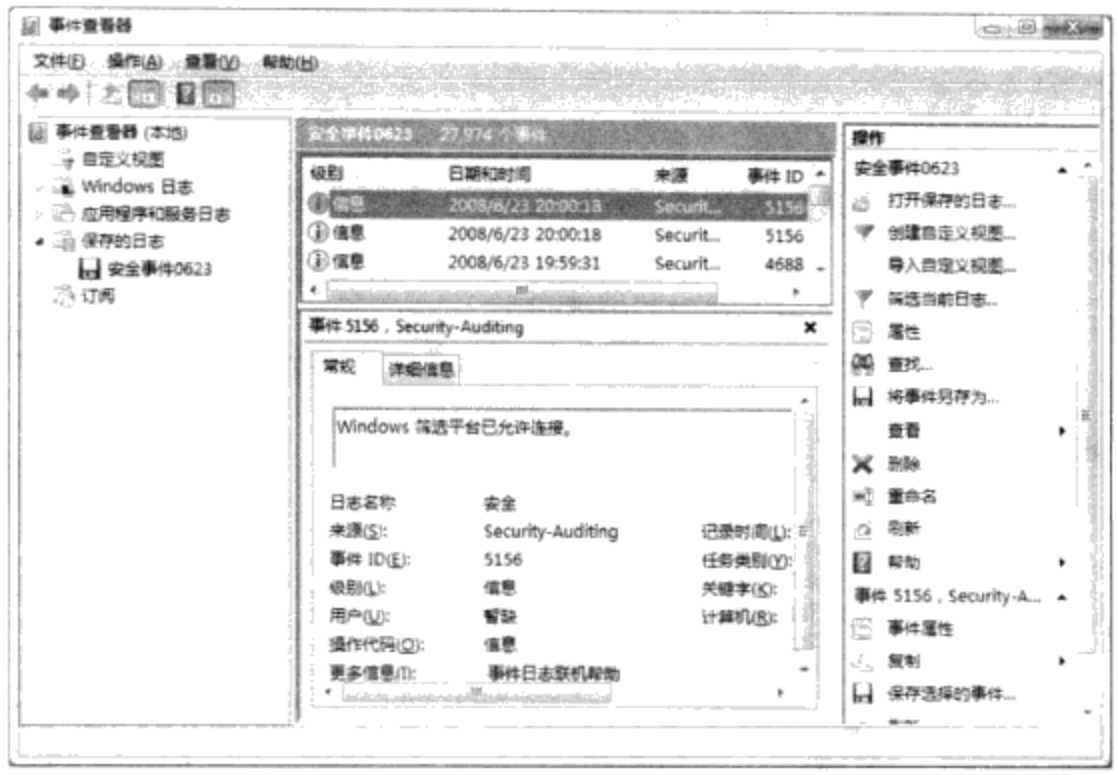


图 6-9 导入的事件日志

6.1.5 订阅事件

Windows Server 2008 R2 系统的事件查看器可以订阅来自其他 Windows 系统（Windows Vista/7 或 Windows Server 2008）的事件日志，管理员可以轻松做到集中分析和监控计算机的状态。订阅功能依赖于 Windows 远程管理（WinRM）服务和 Windows 事件收集器（Wecsvc）服务，这两项服务必须在参与转发和收集过程的计算机上运行。接下来以 Windows Server 2008 R2 系统为例，介绍如何使用管理服务器收集域控制器上的事件日志。

1. 配置计算机转发和接收事件

所谓源计算机就是指事件的真正来源。要配置订阅事件，首先要在源计算机上开启远程管理功能，即允许收集服务器通过网络登录并管理该计算机。需要注意的是，源计算机和事件收集服务器必须隶属于同一域，或建立信任关系的不同域中。虽然也可以在工作组环境中实现，但配置过于复杂，不推荐。

第 1 步，配置源计算机。以管理员登录系统，在命令提示符窗口中，输入如下命令：

```
winrm quickconfig
```

按 Enter 键执行，显示如图 6-10 所示结果。提示目前该计算机没有设置成为允许远程访问，执行更改后，即可接受远程访问，是否继续，输入“y”并按 Enter 键执行，确认更改。

注意 如果要制订“最小化带宽”或“最小化滞后时间”的事件传递优化，则还必须在收集器计算机上运行上述命令。

第 2 步，配置收集器计算机。在收集器计算机的命令提示符窗口中，输入如下命令：

```
wecutil qc
```

成功完成后，显示如图 6-11 所示结果。提示是否更改服务的启动模式，输入“y”并按 Enter 键即可。

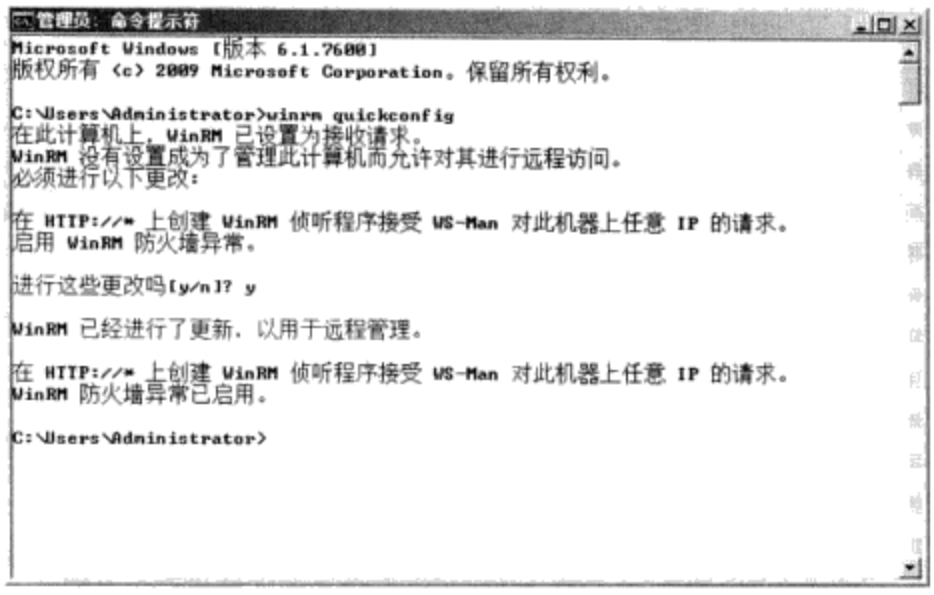


图 6-10　配置源计算机

第 3 步，将收集器计算机的计算机账户添加到源计算机的本地管理员组中，如图 6-12 所示。至此，源计算机和收集器计算机的配置。

图 6-11　配置收集器计算机

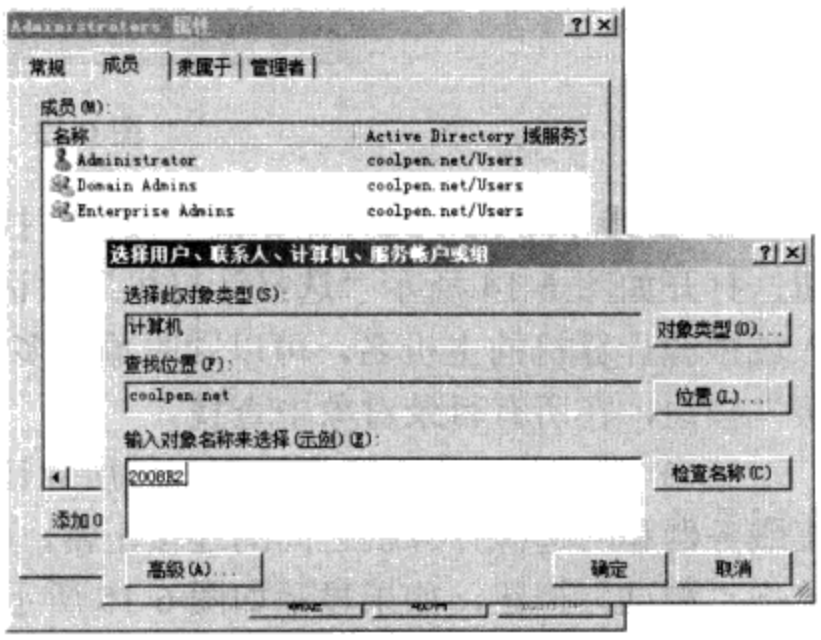


图 6-12　配置计算机账户

提示

重复操作，可以配置多台源计算机。

2. 创建订阅

若要在事件收集服务器上接收来自其他计算机的事件日志，必须创建一个或者多个事件订阅，在源计算机和事件收集服务器上做好上述准备工作之后，即可开始配置事件订阅。

第 1 步，在事件收集服务器上打开“事件查看器”窗口，右击“订阅”选择快捷菜单中

的“创建订阅”选项，显示“订阅属性”对话框。在“订阅名称”文本框中，输入该订阅的名称；在“描述”文本框中可输入相关的说明性文字，以便区分；“目标日志”是用于保存所收集事件的目录，默认目录为“Windows 日志”中的“转发的事件”；在“订阅类型和源计算机”选项区域，选择“收集器已启动”单选按钮，如图 6-13 所示。

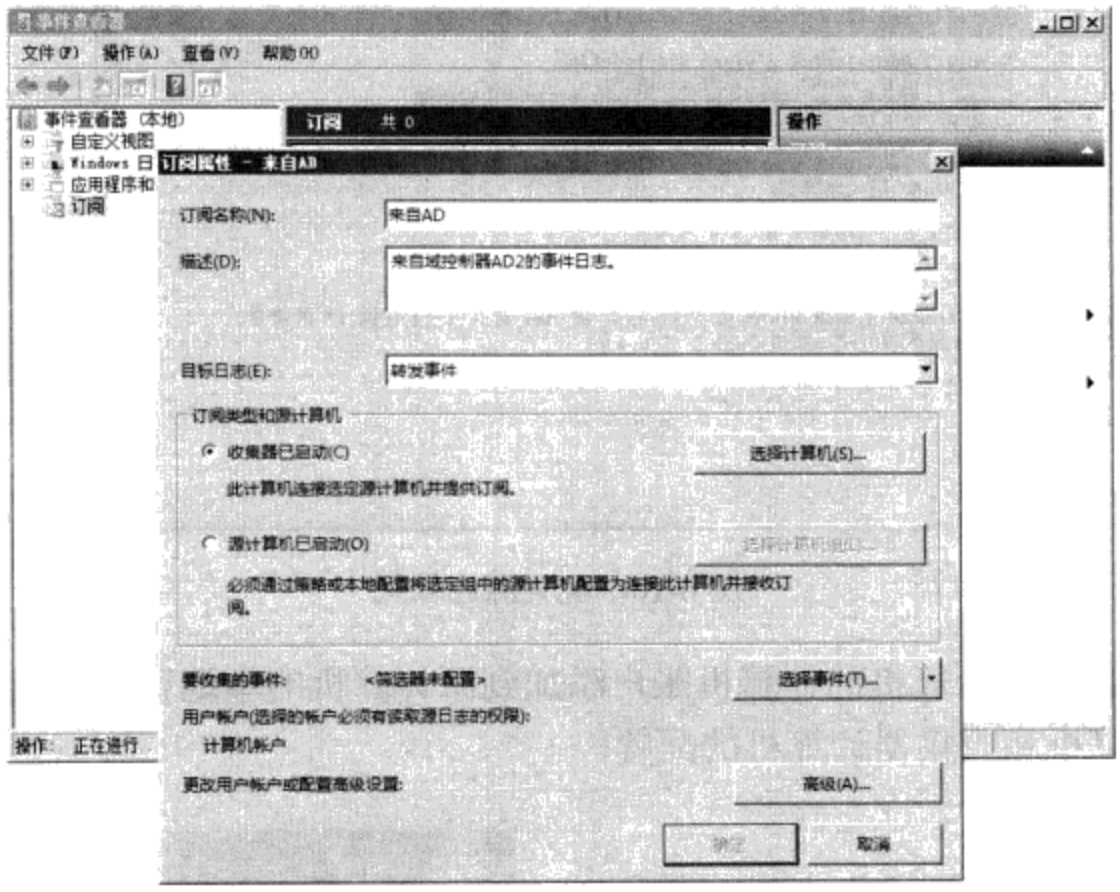


图 6-13 配置订阅属性

第 2 步，单击“选择计算机”按钮，打开“计算机”对话框，单击“添加域计算机”按钮，打开如图 6-14 所示“选择计算机”对话框。在“输入要选择的对象名称”文本框中，输入域中源计算机的主机名，可以同时输入多个，彼此之间以分号（;）隔开；也可以单击“高级”按钮，在所有目录对象中查找。

第 3 步，单击“确定”按钮，将所选计算机添加到“计算机”列表框中。为确保事件收集服务器和所选源计算机之间的连接正常，可以在“计算机”列表框中，选中源计算机名称并单击“测试”按钮，如果显示如图 6-15 所示“连接测试成功”的结果，则表示连接正常。

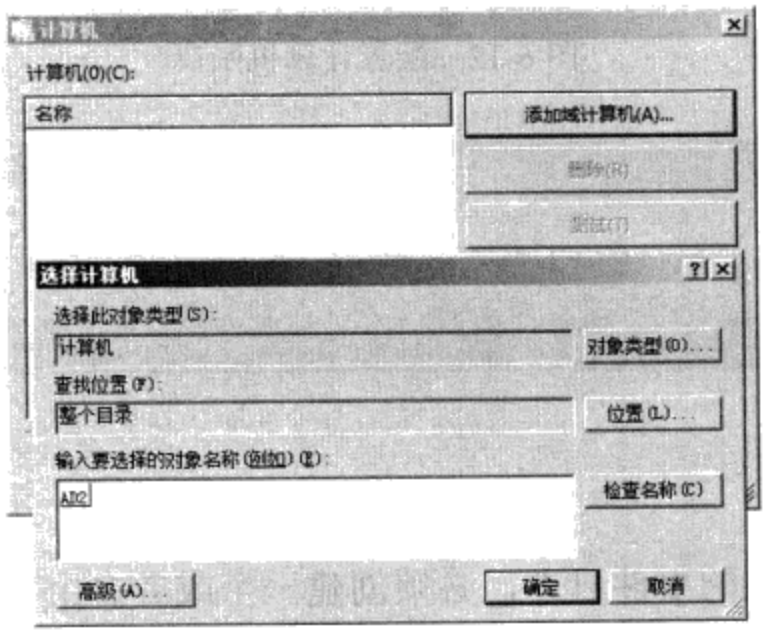


图 6-14 “选择计算机”对话框

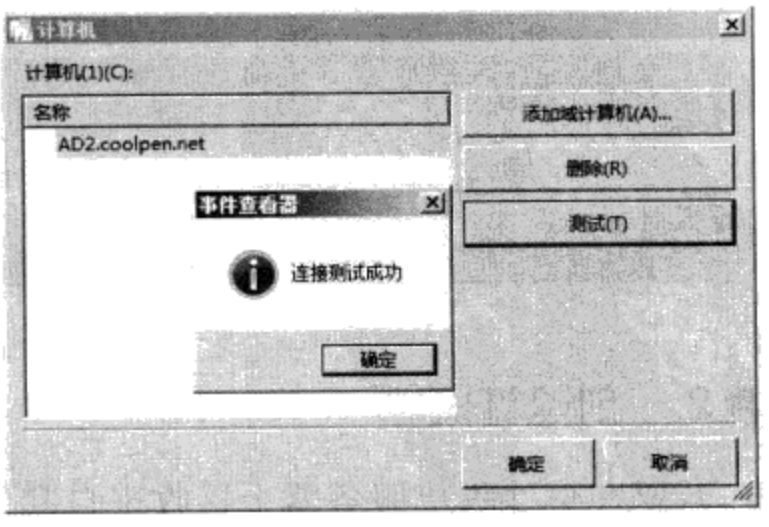


图 6-15 “连接测试成功”对话框

第 4 步，连续单击“确定”按钮返回至“订阅属性”对话框，单击“选择事件”按钮，打开如图 6-16 所示“查询筛选器”对话框。在“记录时间”下拉列表框中选择希望收集的事件产生的时间和日期来；在“事件级别”选项区域选择被收集事件的级别；选择“按日志”单选按钮，并在“事件日志”下拉列表框中，选择事件类型，需要注意的是，如果选择的事件类型过多，可能需要收集大量的事件，占用大量空间。

第 5 步，单击“确定”按钮，返回“订阅属性”对话框，单击“高级”按钮，打开如图 6-17 所示“高级订阅设置”对话框。由于已经将事件收集服务器的计算机账户添加到了源计算机的 Administrators 组中，所以选择“计算机账户”单选按钮即可。

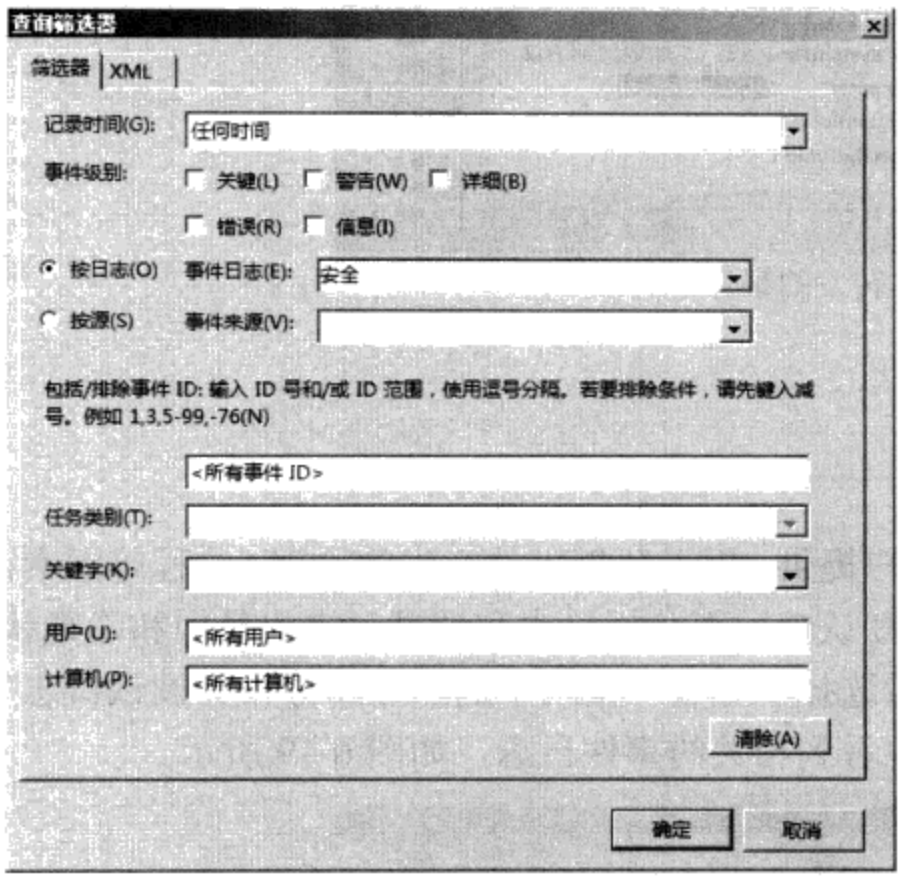


图 6-16 “查询筛选器”对话框

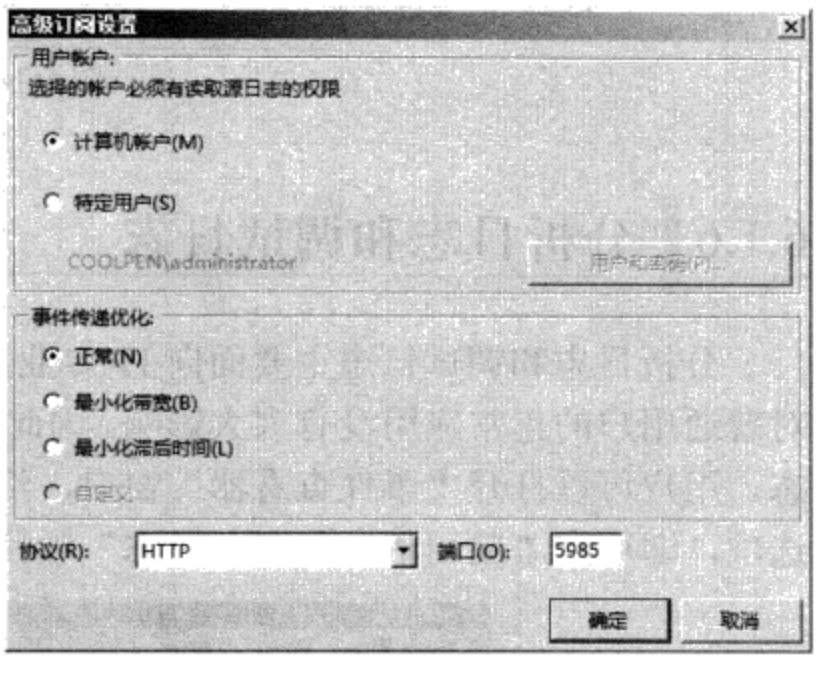


图 6-17 “高级订阅设置”对话框

提示 系统默认使用 HTTP 协议传出事件，用户也可以在“协议”下拉列表框中选择“HTTPS”协议，但此还必须在 Windows 防火墙的“例外”程序中添加“443 端口”。如果使用“正常”（PULL 模式）传递优化的订阅，则只需在源计算机的防火墙上设置例外；如果使用“最小化带宽”或“最小化滞后时间”（PUSH 模式）传递优化的订阅，则必须在源计算机和收集器计算机上同时设置例外。

第 6 步，单击“确定”按钮，关闭“订阅属性”对话框，返回“事件查看器”窗口，新创建的事件订阅已经显示在窗口中。通过事件查看器订阅的远程计算机日志，默认将显示在“Windows 日志”的“转发事件”项目中，如图 6-18 所示。需要注意的是，由于网络传输等多方面问题，远程计算机上产生的相关事件并不能立即转发到事件收集服务器上，通常会有一定时间的延迟。

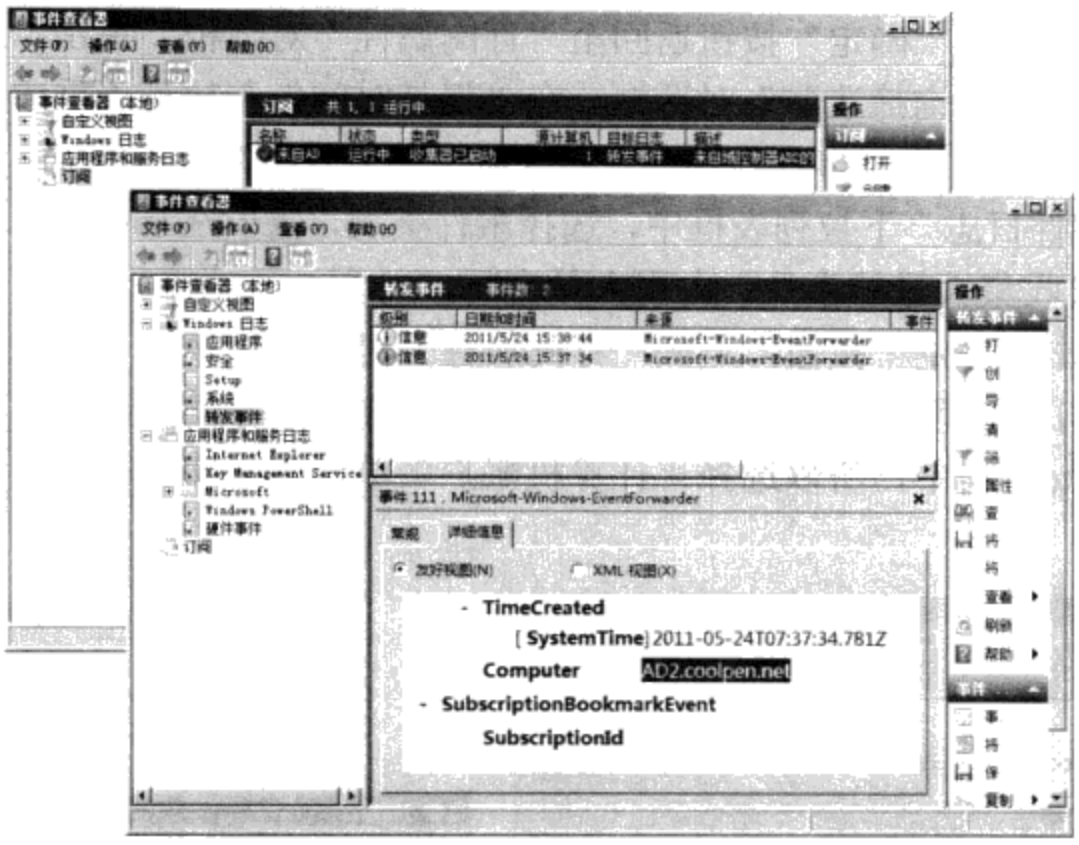


图 6-18　转发的事件

6.1.6　分析日志和调试日志

分析日志和调试日志主要面向 IT 专业用户提供，用于分析事件产生的原因、过程等因素，对普通用户的正常应用没有太大影响。因此，默认情况下分析日志和调试日志为禁用和隐藏状态。用户可以打开“事件查看器”窗口，然后选择“查看”菜单中的“显示分析和调试日志”选项，即可在“应用程序和服务日志”项目中看到相关的事件日志，如图 6-19 所示。

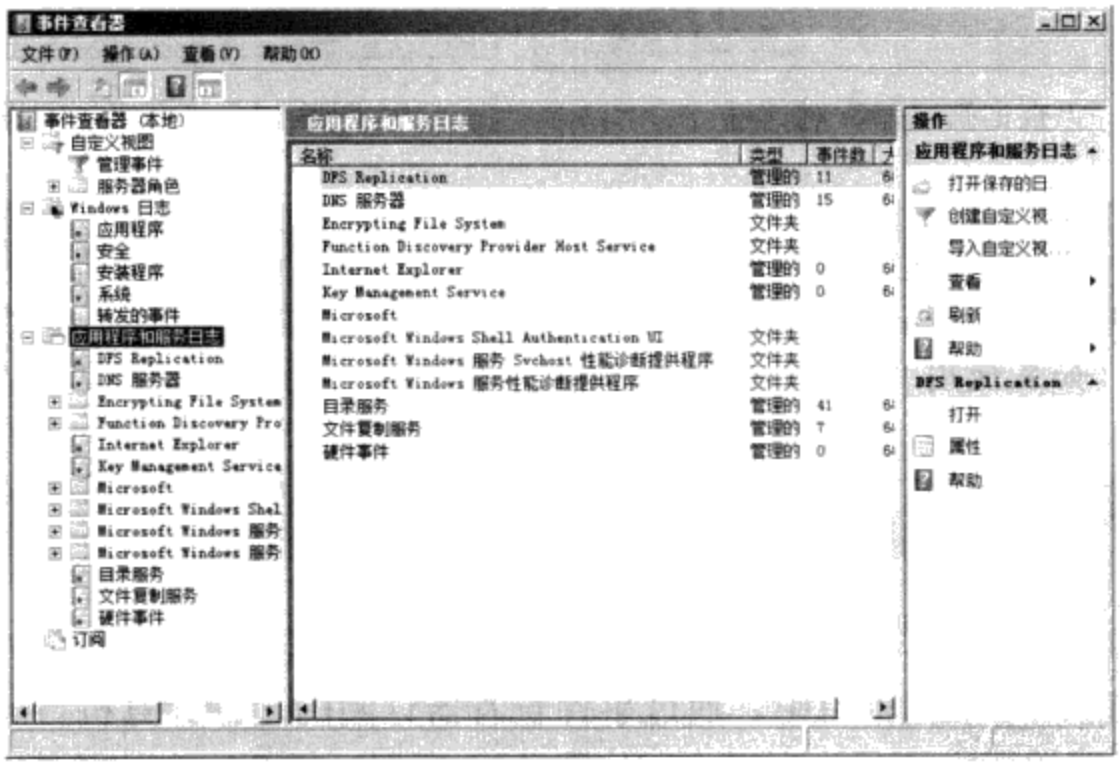


图 6-19　显示分析和调试日志

6.2　安全性日志

前面介绍“NTFS 文件权限访问审核”的时候已经介绍过部分审核策略的配置，以及相关

事件日志的处理。除此之外，Windows Server 2008 R2 系统其他审核策略也是非常实用的。正确配置和应用这些审核策略，可以帮助管理员快速检测黑客的渗透和攻击，及时防止非法用户的入侵，避免安全事件的发生。通常情况下，50%左右的网络入侵事件，都可以通过配置账户事件审核来发现。

6.2.1 启用审核策略

Windows 系统可以提供 9 类事件审核策略，对于每一类都可以指明是审核成功事件、失败事件，还是两者都审核。有关审核策略启动和配置的操作，请参考本书“第 4 章　文件系统与共享资源安全”中的相关内容。这里主要介绍一下，各种审核策略的功能。Windows Server 2008 R2 系统支持的事件审核策略如下。

- 审核策略更改。确定是否对用户权限分配策略、审核策略或信任策略做出更改的每一个事件进行审核。系统默认设置为“成功”，建议设置为“成功”和“失败”。
- 审核登录事件。确定是否审核用户登录到该计算机、从该计算机注销或建立与该计算机的网络连接的每一个实例。如果设定为审核“成功”，则可用来确定哪个用户成功登录到哪台计算机；如果设为审核“失败”，则可以用来检测入侵，但攻击者生成的庞大的登录失败日志，会造成拒绝服务（DoS）状态。建议保持系统设置的“成功”状态。
- 审核对象访问。确定是否审核用户访问某个对象，例如，文件、文件夹、注册表项、打印机等，都指定了自己的系统访问控制列表（SACL）的事件。建议设置为“失败”。
- 审核进程跟踪。确定是否审核事件的详细跟踪信息，例如，程序激活、进程退出、间接对象访问等。如果怀疑系统被攻击，可启用该项，系统默认设置为“成功”。
- 审核目录服务访问。确定是否审核用户访问那些指定有自己的系统访问控制列表（SACL）的 Active Directory 对象的事件。启用后会在域控制器的安全日志中生成大量审核项，因此只有在确实要使用所创建的信息时才应启用。系统默认设置为“成功”。
- 审核特权使用。确定是否对用户行使用户权限的每个实例进行审核，但除跳过遍历检查、调试程序、创建标记对象、替换进程级别标记、生成安全审核、备份文件和目录、还原文件和目录等权限。系统默认为“无审核”。
- 审核系统事件。用于确定当用户重新启动或关闭计算机时，或者对系统安全或安全日志有影响的事件发生时，是否予以审核。这些事件信息是非常重要的，所以建议设置为“成功”和“失败”。
- 审核账户登录事件。用于确定当用户登录到其他计算机（该计算机用于验证其他计算机中的账户）或从中注销时，是否进行审核。建议设置为“成功”和“失败”。
- 审核账户管理。用于确定是否对计算机上的每个账户管理事件，如重命名、禁用或启用用户账户、创建、修改或删除用户账户或管理事件进行审核。建议设置为“成功”和“失败”。

注意　审核项目应配置得当，如果审核项目过多，不仅会影响服务器的响应速度，而且还会产生大量的日志文件，加重管理员工作负担。如果审核项目不足，则无法准确记录恶意入侵和攻击情况，降低系统安全性。

6.2.2 日志分析

在基于NTFS格式的操作系统中使用审核策略，虽然不能对用户的访问进行控制，但是根据打开审核产生的安全日志，可以了解系统在哪些方面存在安全隐患以及系统资源的使用情况，从而为追踪黑客提供可靠依据，同时还有利于采取相应的防范措施将系统的不安全因素降到最低，从而营造一个更加安全可靠的基于NTFS格式的操作系统平台。经常查看和注意事件日志有助于预测和识别系统和安全问题的根源。

事件里的安全日志是系统安全审核的记录所在，应根据服务器的性能和选择的审核对象和记录产生速度定义好大小，一般建议为1024 MB，并定义处理方式为覆盖30天前的数据，这样日志中就可以保存30天的数据资料，如果选择了按需要覆盖，则系统记录满后将自动覆盖最早的数据（不建议），如果选择了手工清除，请确保的日志大小足够大。安全日志记录满后如果不能自动处理，将禁止用户使用计算机的。安全日志不能正确记录时，系统将立即关闭计算机。这些也可以在策略中修改。这里需要特别注意的是，当发现一个审核失败时，并不一定意味着是一个安全问题，在正常操作中，偶尔也会发生目录访问或特权使用失败的情况，应特殊问题特殊对待。

6.2.3 审核日志

管理员配置的所有审核策略产生的日志，默认都将保存在“Windows 日志”的“安全”目录下，双击相关审核日志，即可查看其详细信息，如图6-20所示。如果配置的“审核策略”过多，则可能产生大量的审核日志，此时可以通过筛选的方法，查看相关类型的审核事件日志。

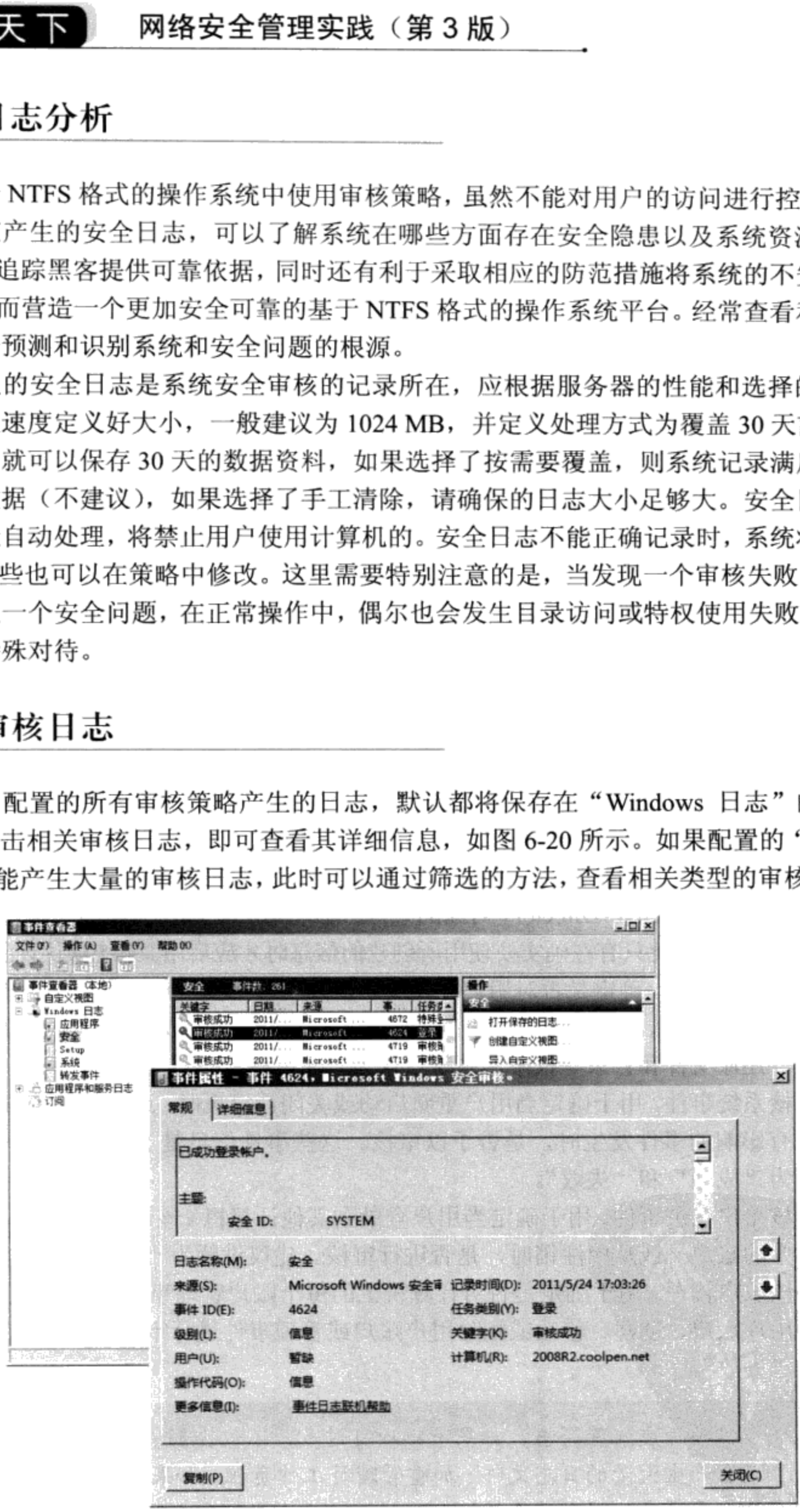


图6-20 查看审核日志

6.2.4 审核事件 ID

事件 ID 是 Windows 事件的基本属性之一，在 Windows 事件查看器中，管理员可以根据系统为不同类型事件定义的 ID 值，判断事件的类型和主要内容，筛选指定类型或 ID 的事件等。通过事件 ID 可以清楚地了解对服务器资源的非法访问和黑客的非法渗透。

1. 账户登录事件

如表 6-3 中列出了由“审核账户登录事件”安全策略设置所生成的安全事件。

表 6-3 审核账户登录事件

类别	事件 ID	内容
凭据验证类别	4774	使用被映射账户进行登录
	4775	无法使用映射账户进行登录
	4776	域控制器尝试验证凭据的账户
	4777	域控制器无法验证凭据的账户
Kerberos 身份验证服务类别	4768	请求 Kerberos 身份验证票证（TGT）
	4771	Kerberos 预身份验证失败
	4772	Kerberos 身份验证票证请求失败
Kerberos 服务票证操作类别	4769	Kerberos 服务票证请求
	4770	Kerberos 服务票证已续订

2. 账户管理事件

如表 6-4 中列出了由“审核账户管理事件”安全策略设置所生成的安全事件。

表 6-4 审核账户管理事件

类别	事件 ID	内容
应用程序组管理	4783	基本应用程序组已创建
	4784	基本应用程序组已更改
	4785	成员已添加到基本应用程序组
	4786	成员已从基本应用程序组删除
	4787	非成员已添加到基本应用程序组
	4788	成员被从基本应用程序组中删除
	4789	基本应用程序组已删除
	4790	已创建 LDAP 查询组
计算机账户管理	4742	计算机账户已更改
	4743	计算机账户被删除
通信组管理	4744	禁用安全的本地组已创建
	4745	禁用安全的本地组已更改
	4746	成员已被添加至禁用安全的本地组
	4747	成员已从禁用安全的本地组删除
	4748	禁用安全的本地组被删除
	4749	禁用安全的全局组已创建
	4750	禁用安全的全局组已更改
	4751	成员已添加至禁用安全的全局组

（续表）

类别	事件 ID	内容
通信组管理	4752	已从禁用安全的全局组删除成员
	4753	禁用安全的全局组已删除
	4759	禁用安全的通用组已创建
	4760	禁用安全的通用组已更改
	4761	成员已添加至禁用安全的通用组
	4762	已从禁用安全的通用组删除成员
其他账户管理事件	4739	更改域策略
	4782	访问账户密码哈希
	4793	密码策略检查 API 调用程序
安全组管理	4727	安全启用全局组已创建
	4728	成员已添加至启用安全的全局组
	4729	从安全启用全局组已删除成员
	4730	安全启用全局组已删除
	4731	安全启用本地组已创建
	4732	成员已添加至启用安全的本地组
	4733	成员已从启用安全的本地组删除
	4734	安全启用本地组被删除
	4735	安全启用本地组已更改
	4737	安全启用全局组已更改
	4754	安全启用通用组已创建
	4755	安全启用通用组已更改
	4756	成员已添加至启用安全的通用组
	4757	成员已从启用安全的通用组删除
	4758	安全启用通用组已删除
	4764	组类型已更改
用户账户管理	4720	创建用户账户
	4722	用户账户被启用
	4723	试图更改账户的密码
	4724	试图重置账户的密码
	4725	用户账户被禁用
	4726	用户账户被删除
	4738	用户账户已更改
	4740	用户账户被锁定
	4765	SID 历史添加到账户
	4766	账户添加 SID 历史的尝试失败
	4767	已锁定用户账户
	4780	这是管理员组的成员账户上设置 ACL
	4781	账户的名称已更改
	4794	被试图设置目录服务还原模式
	5376	凭据管理器凭据被备份
	5377	凭据管理器凭据已从备份还原

3. 详细跟踪事件

如表 6-5 中列出了由“审核详细跟踪事件”安全策略设置所生成的安全事件。

表 6-5　审核详细跟踪事件

类别	事件 ID	消息
DPAPI 活动	4692	尝试数据保护主密钥备份
	4693	尝试对数据保护主密钥恢复
	4694	尝试保护的审计保护数据
	4695	尝试未保护的审计保护数据
进程创建	4688	已创建一个新进程
	4696	主令牌被分配给处理
进程中止	4689	进程已退出
RPC 事件	5712	试图远程过程调用(RPC)

4. 目录服务访问事件

如表 6-6 中列出了由“审核目录服务访问事件”安全策略设置所生成的安全事件。

表 6-6　审核目录服务访问事件

类别	事件 ID	消息
详细目录服务复制	4928	建立 Active Directory 副本源命名上下文
	4929	删除 Active Directory 副本源命名上下文
	4930	修改 Active Directory 副本源命名上下文
	4931	修改 Active Directory 副本目标命名上下文
	4934	复制 Active Directory 对象的属性
	4935	开始复制失败
	4936	结束复制失败
	4937	从副本延迟对象删除
目录服务访问	4662	对象上进行操作
目录服务更改	5136	修改目录服务对象
	5137	已创建目录服务对象
	5138	目录服务对象是未删除
	5139	移动目录服务对象
	5141	删除目录服务对象
目录服务复制	4932	Active Directory 命名上下文的副本同步已开始
	4933	Active Directory 命名上下文的副本同步已结束

5. 登录/注销事件 ID

如表 6-7 中列出了“审核登录/注销事件”安全策略设置所生成的安全事件。

表 6-7　审核登录/注销事件

类别	事件 ID	消息
账户锁定	4625	账户无法登录。
IPSec 扩展模式	4978	在扩展模式协商，IPSec 收到一个无效协商数据包。如果问题仍然存在， 则可能说明网络问题或者试图修改或重播该协商
	4979	已建立 IPSec 主模式和扩展模式安全关联
	4980	已建立 IPSec 主模式和扩展模式安全关联
	4981	已建立 IPSec 主模式和扩展模式安全关联
	4982	已建立 IPSec 主模式和扩展模式安全关联
	4983	IPSec 扩展模式协商失败，相应的主模式安全关联已被删除
	4984	IPSec 扩展模式协商失败，相应的主模式安全关联已被删除

（续表）

类别	事件ID	消息
IPSec 主模式	4646	IKE 预防 DoS 攻击模式启动
	4650	已建立 IPSec 主模式安全关联，没有启用扩展模式，不使用证书验证
	4651	已建立 IPSec 主模式安全关联，没有启用扩展模式，证书用于身份验证
	4652	IPSec 主模式协商失败
	4653	IPSec 主模式协商失败
	4655	IPSec 主模式安全关联结束
	4976	在主模式协商过程中，IPSec 收到一个无效协商数据包
	5049	删除了 IPSec 安全关联
	5453	由于未启动 IKE 和 IPSec Keying 模块服务，IPSec 协商与远程计算机失败
IPSec 快速模式	4654	IPSec 快速模式协商失败
	4977	在快速模式协商过程中，IPSec 收到一个无效协商数据包
	5451	已建立 IPSec 快速模式安全关联
	5452	IPSec 快速模式安全关联结束
注销	4634	账户被注销
	4647	用户启动注销
登录	4624	已成功登录账户
	4625	账户无法登录
	4648	试图使用明确凭据登录
	4675	SID 被筛选
网络策略服务器	6272	网络策略服务器授予用户访问权限
	6273	网络策略服务器用拒绝户访问
	6274	网络策略服务器放弃对用户请求
	6275	网络策略服务器丢弃记账请求的用户
	6276	网络策略服务器隔离一个用户
	6277	网络策略服务器授予用户访问，但因为主机不符合定义策略而被阻止
	6278	主机满足网络策略服务器定义的状况策略，授予完全访问
	6279	由于重复验证失败，网络策略服务器锁定用户账户
	6280	网络策略服务器取消锁定用户账户
其他登录/注销事件	4649	检测重播攻击
	4778	重新会话已连接到窗口站
	4779	从窗口站会话被中断
	4800	锁定工作站
	4801	是锁定工作站
	4802	屏幕保护程序被调用
	4803	已关闭屏幕保护程序
	5378	请求凭据委派是允许通过策略
	5632	对到无线网络进行了请求
	5633	对到有线网络进行了请求
特殊登录	4964	特殊组已分配给新登录

6. 对象访问事件

如表 6-8 中列出了由“审核对象访问事件”安全策略设置所生成的安全事件。

表 6-8　审核对象访问事件

类别	事件 ID	消息
生成应用程序	4665	一个试图创建一个应用程序客户端上下文
	4666	应用程序尝试的操作
	4667	删除应用程序客户端上下文
	4668	初始化应用程序
证书服务	4868	证书管理员拒绝挂起证书请求
	4869	证书服务收到重复提交的证书请求
	4870	证书服务吊销证书
	4871	证书服务收到请求来发布证书吊销列表（CRL）
	4872	证书服务发行证书吊销列表（CRL）
	4873	更改证书申请扩展
	4874	一个或多个证书申请属性更改
	4875	证书服务接收到关闭请求
	4876	证书服务备份启动
	4877	证书服务备份完成
	4878	启动证书服务还原
	4879	证书服务还原完成
	4880	证书服务启动
	4881	证书服务停止
	4882	对于证书服务安全权限更改
	4883	证书服务检索存档密钥
	4884	证书服务导证书入其数据库
	4885	对于证书服务审核筛选器更改
	4886	证书服务收到证书请求
	4887	证书服务批准证书申请并颁发证书
	4888	证书服务拒绝证书申请
	4889	证书服务设置到挂起证书请求的状态
	4890	证书管理设置对于证书服务更改
	4891	证书服务中更改一个配置项
	4892	更改属性的证书服务
	4893	证书服务存档了密钥
	4894	证书服务导入和存档密钥
	4895	证书服务 CA 证书发行到 Active Directory 域服务
	4896	已从证书数据库删除一个或多行
	4897	角色分离启用
	4898	证书服务加载模板
文件共享	5140	访问网络共享对象
文件系统子类别	4664	一个试图创建硬链接
	4985	事务的状态已更改
	5051	文件被虚拟化
筛选平台连接	5031	Windows 防火墙服务阻止应用程序接受传入连接在网络上
	5154	Windows 过滤平台具有允许应用程序或服务以端口上监听传入连接
	5155	Windows 过滤平台已阻止应用程序或服务从端口上侦听传入连接
	5156	Windows 过滤平台具有允许建立连接
	5157	Windows 过滤平台已阻止建立连接
	5158	Windows 过滤平台具有允许绑定到本地端口
	5159	Windows 过滤平台已阻止绑定到本地端口

（续表）

类别	事件 ID	消息
筛选平台数据包过滤	5152	Windows 过滤平台阻止数据包
	5153	限制性 Windows 过滤平台筛选已阻止数据包
句柄	4656	请求句柄对象
	4658	关闭该控点来关闭对象
	4690	被试图复制句柄到对象
其他对象访问事件	4671	应用程序试图通过 TBS 访问阻止序号
	4691	请求对一个对象间接访问
	4698	创建计划任务
	4699	删除计划任务
	4700	已启用计划任务
	4701	计划任务被禁用
	4702	计划任务更新
	5888	修改 COM+目录中的对象
	5889	已从 COM+目录删除对象
	5890	对象被添加到 COM+目录
注册表	4657	修改注册表值
	5039	虚拟化注册表项
Multi-use 特殊子类别	4659	与意向来删除请求句柄对象
	4660	已删除对象
	4661	请求句柄对象
	4663	试图访问对象

7. 策略更改事件

如表 6-9 中列出了由“策略更改事件”安全策略设置所生成的安全事件。

表 6-9 策略更改事件

类别	事件 ID	消息
审核策略更改	4715	更改对象上审核策略 (SACL)
	4719	更改系统审核策略
	4902	创建用户审核策略表
	4904	被试图注册安全事件源
	4905	被试图注销安全事件源
	4906	CrashOnAuditFail 值已更改
	4907	更改审核设置对象上
	4908	修改特殊组登录表
	4912	每用户审核策略更改
验证策略更改	4706	新信任创建到域
	4707	删除对域信任
	4713	Kerberos 策略已更改
	4716	修改信任域信息
	4717	系统安全访问已授予账户
	4718	从账户删除系统安全访问
	4864	命名空间冲突检测
	4865	添加可信林中信息项
	4866	删除可信林中信息项
	4867	修改信任林信息项

（续表）

类别	事件 ID	消息
授权策略更改	4704	分配用户右侧
	4705	右用户被删除
	4714	更改加密数据恢复策略
筛选平台策略更改	4709	IPSec 服务已启动
	4710	IPSec 服务被禁用
	4711	可能包含下列之一： PAStore 引擎在计算机上应用 Active Directory 存储 IPSec 策略是本地缓存副本。 PAStore 引擎在计算机上应用了 Active Directory 存储 IPSec 策略。 PAStore 引擎在计算机上应用了本地注册表存储 IPSec 策略。 PAStore 引擎无法在计算机上应用 Active Directory 存储 IPSec 策略副本。 PAStore 引擎在计算机上应用 Active Directory 存储 IPSec 策略失败。 PAStore 引擎在计算机上应用本地注册表存储 IPSec 策略失败。 PAStore 引擎无法在计算机上应用某些规则的活动 IPSec 策略。 PAStore 引擎无法加载目录存储 IPSec 策略在计算机上。 PAStore 引擎加载目录存储 IPSec 策略在计算机上。 PAStore 引擎无法加载本地存储 IPSec 策略在计算机上。 PAStore 引擎加载本地存储 IPSec 策略在计算机上。 PAStore 引擎轮询以了解对活动 IPSec 策略更改，检测任何更改
	4712	IPSec 服务遇到可能严重错误
	5040	IPSec 设置已经更改。添加一个验证设置
	5041	IPSec 设置已经更改。验证设置了修改
	5042	IPSec 设置已经更改。验证设置一个被删除
	5043	IPSec 设置已经更改。添加连接安全规则
	5044	IPSec 设置已经更改。修改连接安全规则
	5045	IPSec 设置已经更改。删除连接安全规则
	5046	IPSec 设置已经更改。添加加密设置
	5047	IPSec 设置已经更改。加密设置被修改
	5048	IPSec 设置已经更改。加密设置被删除
	5440	下列标注为 Windows 筛选平台类别，在筛选引擎启动时显示
	5441	下列筛选器是 Windows 筛选平台类别，在筛选引擎启动时显示
	5442	下列提供程序是 Windows 筛选平台类别，在筛选引擎启动时显示
	5443	以下提供上下文是 Windows 筛选平台类别，在筛选引擎启动时显示
	5444	下列子层是 Windows 筛选平台类别，在筛选引擎启动时显示
	5446	Windows 过滤平台标注已更改
	5448	Windows 过滤平台提供程序已更改
	5449	Windows 过滤平台提供上下文已更改
	5450	Windows 过滤平台子层已更改
	5456	PAStore 引擎在计算机上应用了 Active Directory 存储 IPSec 策略
	5457	PAStore 引擎在计算机上应用 Active Directory 存储 IPSec 策略失败
	5458	PAStore 引擎在计算机上应用 Active Directory 存储 IPSec 策略是本地缓存副本
	5459	PAStore 引擎无法在计算机上应用 Active Directory 存储 IPSec 策略是本地缓存副本
	5460	PAStore 引擎在计算机上应用了本地注册表存储的 IPSec 策略
	5461	PAStore 引擎在计算机上应用本地注册表存储的 IPSec 策略失败
	5462	PAStore 引擎无法在计算机上应用某些规则的活动 IPSec 策略。使用 IP 安全监视器管理单元来诊断问题
	5463	PAStore 引擎轮询对活动 IPSec 策略更改，检测任何更改
	5464	PAStore 引擎轮询对活动 IPSec 策略更改，检测更改，并将其应用到 IPSec 服务
	5465	PAStore 引擎接收用于强制重新加载 IPSec 策略的控件和成功处理控件

（续表）

类别	事件ID	消息
筛选平台策略更改	5466	PAStore 引擎对 Active Directory IPSec 策略进行轮询，Active Directory 无法使用 Active Directory IPSec 策略的缓存副本更改。无法应用上次轮询后对 Active Directory IPSec 策略的任何更改
	5467	PAStore 引擎对 Active Directory IPSec 策略进行轮询，Active Directory 可以获得所有策略更改。Active Directory IPSec 策略的缓存副本不再被使用
	5468	PAStore 引擎通过轮询了解 Active Directory IPSec 策略更改，确定 Active Directory 可被访问，找到对策略，并应用这些更改。Active Directory IPSec 策略的缓存副本不再被使用
	5471	PAStore 引擎加载本地存储 IPSec 策略在计算机上
	5472	PAStore 引擎无法加载本地存储 IPSec 策略在计算机上
	5473	PAStore 引擎加载目录存储 IPSec 策略在计算机上
	5474	PAStore 引擎无法加载目录存储 IPSec 策略在计算机上
	5477	PAStore 引擎无法添加快速模式筛选器
MPSSVC 规则 - 级别策略更改	4944	Windows 防火墙启动时下列策略处于活动
	4945	Windows 防火墙启动时被列出规则
	4946	Windows 防火墙例外列表已被进行更改，添加规则
	4947	Windows 防火墙例外列表已被进行更改，修改规则
	4948	Windows 防火墙例外列表已被进行更改，删除规则
	4949	Windows 防火墙设置已还原到默认值
	4950	Windows 防火墙设置已经更改
	4951	规则已忽略因为通过 Windows 防火墙无法识别其主版本号
	4952	由于通过 Windows 防火墙无法识别其次要版本号部分规则已被忽略，将强制规则的其他部分
	4953	因为无法解析规则，已忽略通过 Windows 防火墙
	4954	Windows 防火墙组策略设置已更改，已应用新设置
	4956	Windows 防火墙已更改活动配置文件
	4957	Windows 防火墙未应用以下规则
	4958	由于规则引用此计算机上没有配置项目没有 Windows 防火墙采用以下规则
其他策略更改事件	4909	更改用于 TBS 本地策略设置
	4910	更改组策略设置 TBS
	5063	试图提供加密操作
	5064	试图加密上下文操作
	5065	试图加密上下文修改
	5066	试图加密函数操作
	5067	试图加密函数修改
	5068	试图为加密函数提供操作
	5069	试图加密函数属性
	5070	试图加密函数属性修改
	5447	Windows 过滤平台筛选已被更改
	6144	成功应用了组策略对象中安全策略
	6145	一个或多个处理安全策略组策略对象中时出错
Multi-use 特殊子类别	4670	更改对象上的权限

8. 特权使用事件

如表 6-10 中列出了由“审核特权使用事件”安全策略设置所生成的安全事件。

表 6-10　审核特权使用事件

类别	事件 ID	内容
敏感特权使用 / 非敏感特权使用	4672	特殊权限赋予新登录
	4673	特权服务调用
	4674	试图在特权对象操作

9. 审核系统事件

如表 6-11 中列出了由“审核系统事件”安全策略设置所生成的系统事件。

表 6-11　审核系统事件

类别	事件 ID	内容
IPSec 驱动程序	4960	IPSec 丢弃传入数据包完整性检查失败。如果问题仍然存在，则可能表明网络问题或该数据包被修改传输到此计算机中。验证从远程计算机发送数据包是否与由此计算机接收相同。此错误可能也表明其他 IPSec 实现互操作问题
	4961	IPSec 丢弃传入数据包重播检查失败。如果问题仍然存在，则可能表明本机重播攻击
	4962	IPSec 丢弃传入的数据包重播检查失败消息
	4963	IPSec 丢弃应该已被保护的入站明文数据包。这通常是由于到远程计算机更改其 IPSec 策略没有通知此计算机。这也可能是欺骗攻击尝试
	4965	IPSec 从远程计算机与一个正确安全参数索引(SPI)收到一个数据包。这通常由数据包被破坏，硬件故障。如果持续，这些错误验证从远程计算机发送数据包是否与由此计算机接收相同。此错误也可能表明其他 IPSec 实现互操作问题。这时，如果连接性是畅通的，这些事件可被忽略
	5478	IPSec 服务成功启动
	5479	IPSec 服务已成功关闭。关闭对 IPSec 服务可使计算机更危险的网络攻击或者将计算机暴露给潜在安全风险
	5480	IPSec 服务无法获取完整的计算机上网络接口列表。会因为某些网络接口的可能无法获得通过应用 IPSec 筛选器提供保护这带来潜在安全风险。使用 IP 安全监视器管理单元来诊断问题
	5483	IPSec 服务无法初始化 RPC 服务器。IPSec 服务无法启动
	5484	IPSec 服务遇到一个关键性失败，已关闭。关闭对 IPSec 服务可使计算机更危险的网络攻击或者将计算机暴露给潜在安全风险
	5485	IPSec 服务无法处理某些 IPSec 筛选器对即插即用事件对网络接口。 会因为某些网络接口的可能无法获得通过应用 IPSec 筛选器提供保护这带来潜在安全风险。使用 IP 安全监视器管理单元来诊断问题
其他系统事件	5024	Windows 防火墙服务成功启动
	5025	Windows 防火墙服务已停止
	5027	Windows 防火墙服务无法从本地存储器检索安全策略。服务将继续强制当前策略
	5028	Windows 防火墙服务无法分析新安全策略。服务将继续与当前实施策略
	5029	Windows 防火墙服务无法初始化驱动程序。服务将继续以强制当前策略
	5030	Windows 防火墙服务无法启动
	5032	Windows 防火墙无法通知用户它阻止应用程序接受传入连接在网络上
	5033	Windows 防火墙驱动程序成功启动
	5034	Windows 防火墙驱动程序已停止
	5035	Windows 防火墙驱动程序无法启动
	5037	Windows 防火墙驱动程序检测到关键运行错误。终止
	5058	密钥文件操作
	5059	密钥迁移操作

（续表）

类别	事件ID	内容
安全状态更改	4608	正在启动 Windows
	4609	关闭 Windows
	4616	更改系统时间
	4621	管理员从审核失败状态恢复系统。用户不是管理员用户现在允许进行登录。某些审核活动可能没有已记录
安全系统扩展	4610	通过本地安全机构验证包被加载
	4611	已使用本地安全机构注册可信登录过程
	4614	通知包被加载安全账户管理器
	4622	通过本地安全机构被加载安全程序包
	4697	系统中已安装服务
系统完整性	4612	已用内部资源分配给的审核消息队列通向丢失某些审核完
	4615	无效使用 LPC 端口
	4618	监视安全事件图案发生
	4816	RPC 检测解密传入消息时完整性冲突
	5038	代码完整性确定该图像的文件哈希无效。文件可能是因受到未经授权修改而损坏，或无效哈希运算错误
	5056	执行自检加密
	5057	加密基元操作失败
	5060	验证操作失败
	5061	加密操作
	5062	执行内核模式加密自检

6.3 系统性能监控

服务器的性能监视系统是网络管理和维护的重要组成部分，Windows Server 2008 R2 系统仍然保留了旧版本系统中的“系统监视器”和“性能日志和警报”等实用工具，管理员可以轻松监视系统性能以及系统吞吐量配置更改后的效果。最重要的一些性能监视衡量标准包括处理器利用情况、硬盘 I/O 传输率、内存利用率、页面文件的活动等。

6.3.1 系统监视器

并非所有的 Windows 系列操作系统都具有系统监视功能，在 Windows NT 4.0 中开始整合了系统监视器（即性能监视器），而如今系统监视器已属于核心管理工具之一，其功能强大，可以用来监视服务器活动或监视所选时间段内服务器的性能。系统监视器既可以在实时图表或报告中显示性能数据，又可以在文件中收集数据或在关键事件发生时生成警告。

1. 简单性能监视

不同用途的网络服务器管理方式和要求也会有所不同。通常情况下，管理员只需了解有关 CPU 和内存的实时数据时即可，使用任务管理器进行简单性能监视是个不错的选择。简单性能监视最大的特点就是灵活易用，占用系统资源少。任务管理器提供的 CPU 利用率、内存使用率等数据对于判断系统当前状态，初步了解系统繁忙程度等任务都是非常有用的。

在“任务管理器”窗口中切换到“性能”选项卡，即可显示如图 6-21 所示的图形窗口。任务管理器提供了 CPU 使用和内存使用（PF 使用）两个主要的实时图形窗口，以曲线的形式

显示当前的 CPU 使用率和内存占用数量。

双击 CPU 占用率窗口，以详细模式显示当前 CPU 占用情况，如图 6-22 所示。左侧柱型图标示实时 CPU 占用率，右侧曲线显示占用率的历史情况。

图 6-21　任务管理器的性能监视

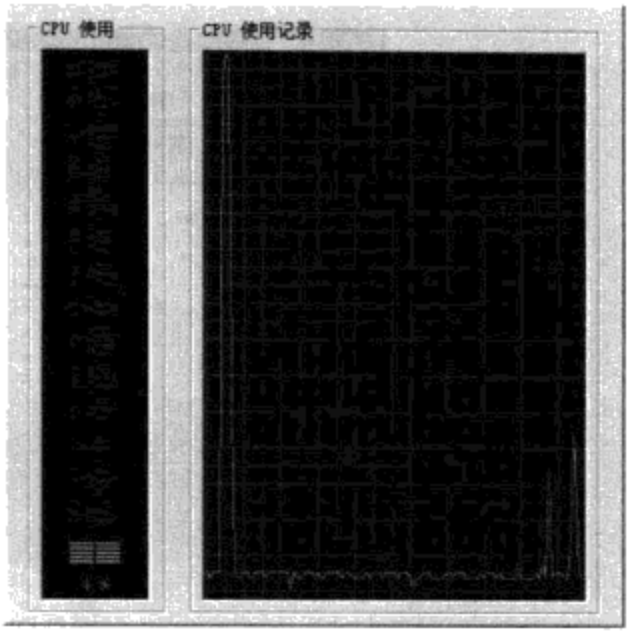


图 6-22　CPU 占用情况

在任务管理器的下部，显示了内存使用的详细信息，包括线程总数、物理内存、内存使用以及核心内存使用情况。这些数据为排错和性能分析提供了可靠依据，例如 CPU 或内存使用率经常性地居高不下，则系统内可能存在占用系统资源比较多的进程，可服务器的配置已经不能满足网络需求了。

2. 资源监视器

Windows 资源监视器是一个功能强大的工具，用于了解进程和服务如何使用系统淘汰。除了实时监视资源使用情况外，资源监视器还可以帮助分析没有响应的进程，确定哪些应用程序正在使用文件，以及控制进程和服务。

在“Windows 任务管理器”的“性能”选项卡中，单击“资源监视器”按钮，显示如图 6-23 所示“资源监视器”窗口。默认显示“概述”选项卡，其中包括 CPU、磁盘、网络和内存的基本信息。

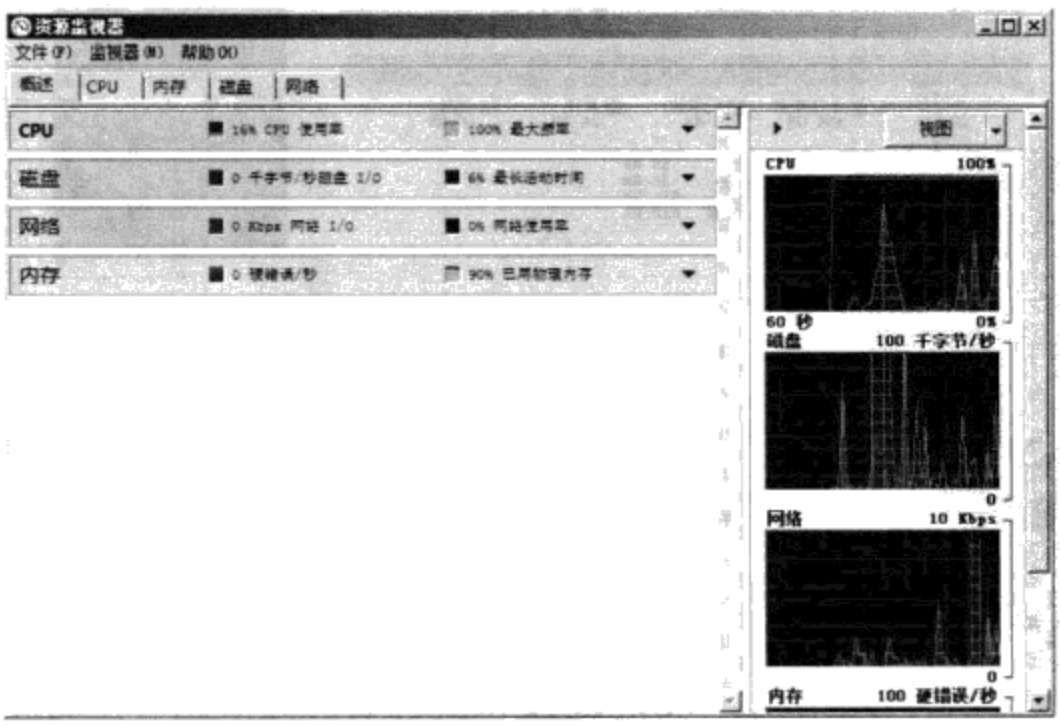


图 6-23　“资源监视器”窗口

切换到如图 6-24 所示“CPU”选项卡，监视当前 CPU 正在处理的进程、服务、关联的句柄和关联的模块等内容，单击想要查看的名称即可查看具体的使用情况。在窗口的右侧，以图形方式显示 CPU 的总的使用情况和服务对 CPU 的使用率。

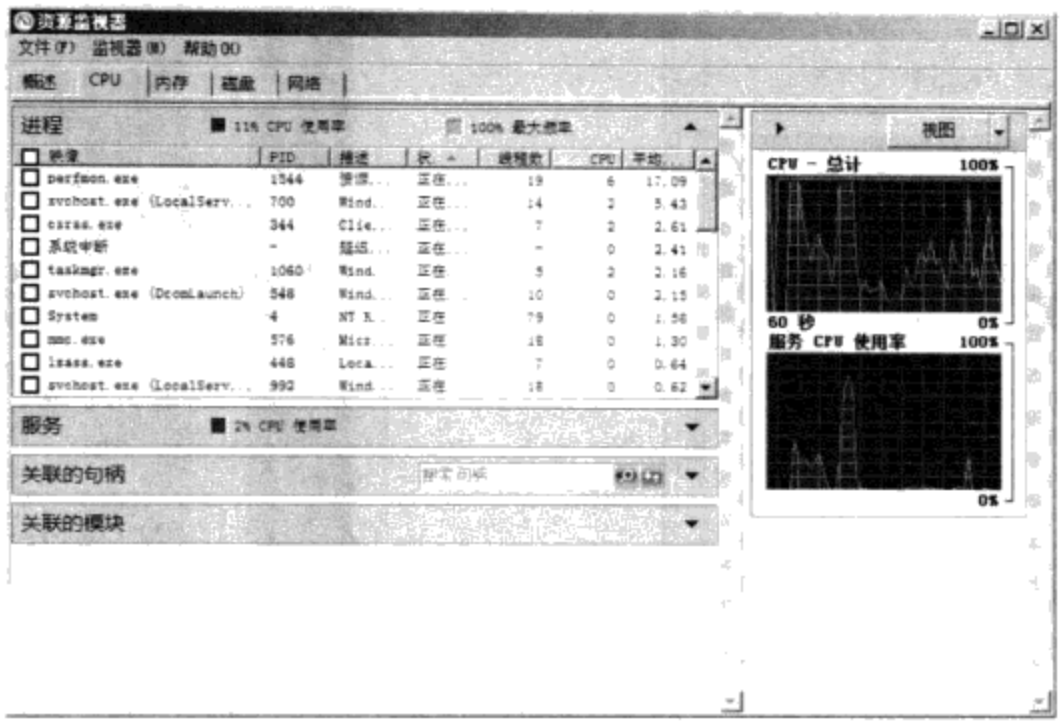


图 6-24 “CPU”选项卡

切换到如图 6-25 所示“内存”选项卡，监视当前内存的具体使用情况。在左侧窗口中，显示当前内存正在处理的进程，及物理内存的具体使用信息。在右侧窗口中，以图形方式显示使用的物理内存、60 s 内内存使用和硬错误/秒等。

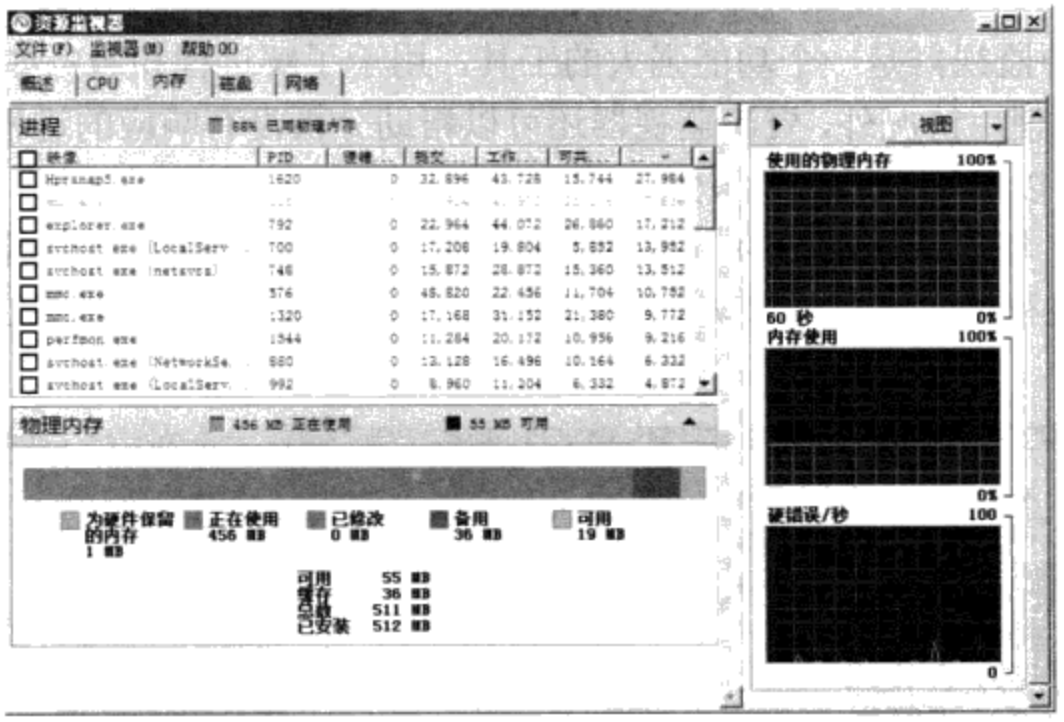


图 6-25 “内存”选项卡

切换到如图 6-26 所示“硬盘”选项卡，监视硬盘的使用信息。在左侧窗口中，显示当前硬盘活动的进程、磁盘活动和存储等内容。在右侧窗口中，以图形方式显示磁盘的实时使用情况。

切换到如图 6-27 所示“网络”选项卡，监视服务器的网络使用情况。在左侧窗口中，显示当前网络活动的进程、网络活动、TCP 连接和侦听端口等信息。在右侧窗口中，以图形方式，显示当前的网络使用率、60 s 内 TCP 连接、不同本地连接的网络使用情况。

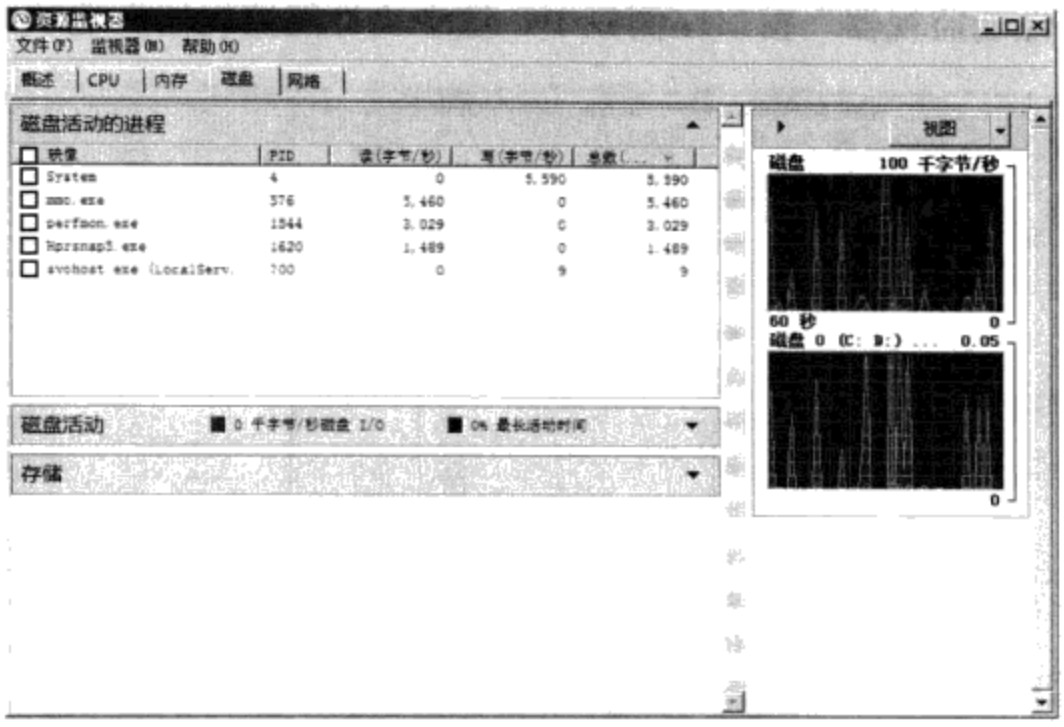


图 6-26 “硬盘”选项卡

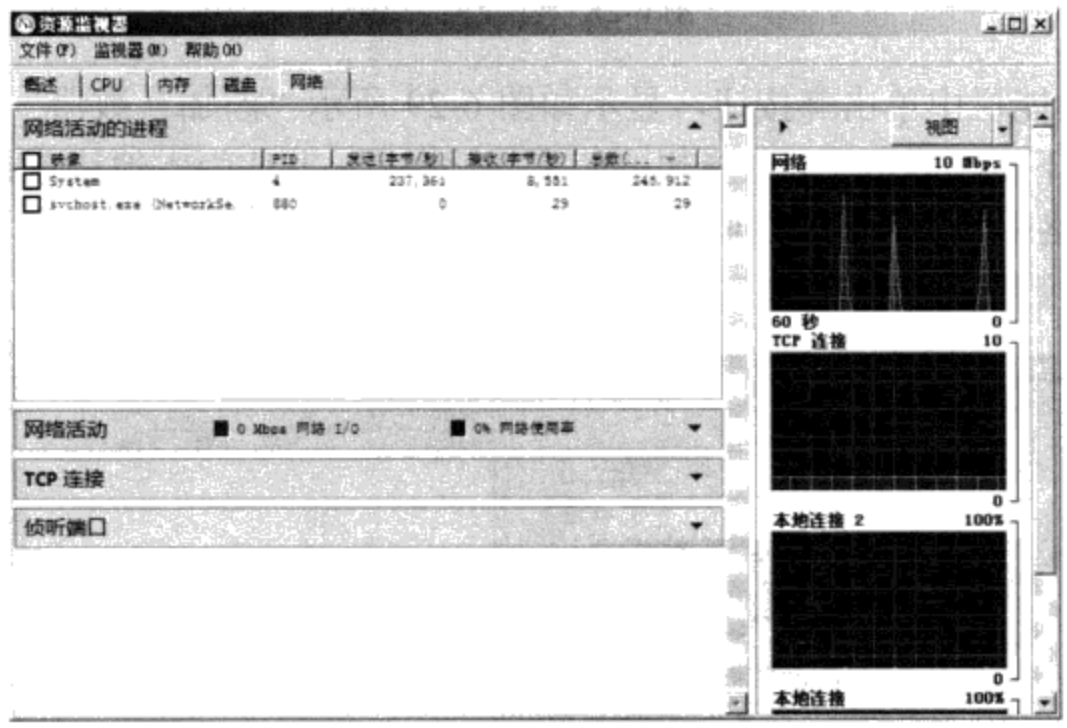


图 6-27 “网络”选项卡

6.3.2 性能监视器

性能监视器是一种简单而功能强大的可视化工具，用于实时以及从日志文件中查看性能数据。可以检查图表、直方图或报告中的性能数据。系统监视器监视的基本单位是“对象”，即特定的控制服务器资源的服务或机制，例如处理器对象，内存对象、Web 对象等。

1. 添加计数器

计数器是反映监视对象不同属性的工具，系统监视器真正记录的是这些计数器的值，例如处理器对象的%Processer Time 计数器，内存对象的 Pages Fault/Sec 计数器等。使用计数器监视服务器系统性能可以实时准确地反映服务器的运行状态，Windows Server 2008 R2 系统中提供了许多计数器，如安装 IIS 组件之后就会自动添加 IIS 计数器，包括 Web 服务计数器、FTP 服务计数器等。

第1步，在“性能监视器”窗口左侧栏中，选中“性能监视器”选项，如图6-28所示。

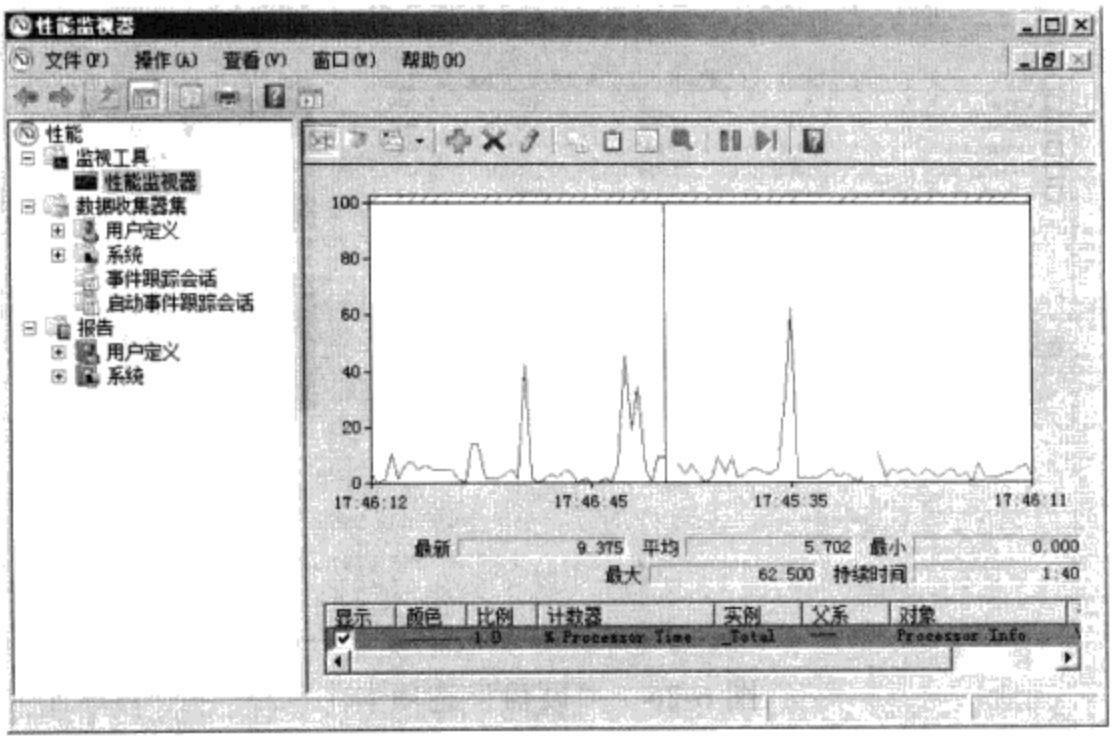


图6-28　性能监视器

第2步，在功能栏中单击按钮，显示如图6-29所示“添加计数器”对话框。在“从计算机选择计数器”下拉列表框中，选择想要监视的服务器，默认为本地计算机，也可以单击“浏览”按钮，浏览网络中的计算机。在监视的类别列表框中，选中想要监视的内容。然后单击“添加”按钮，将该计数器添加在右侧列表框中。重复操作，可添加多个计数器。

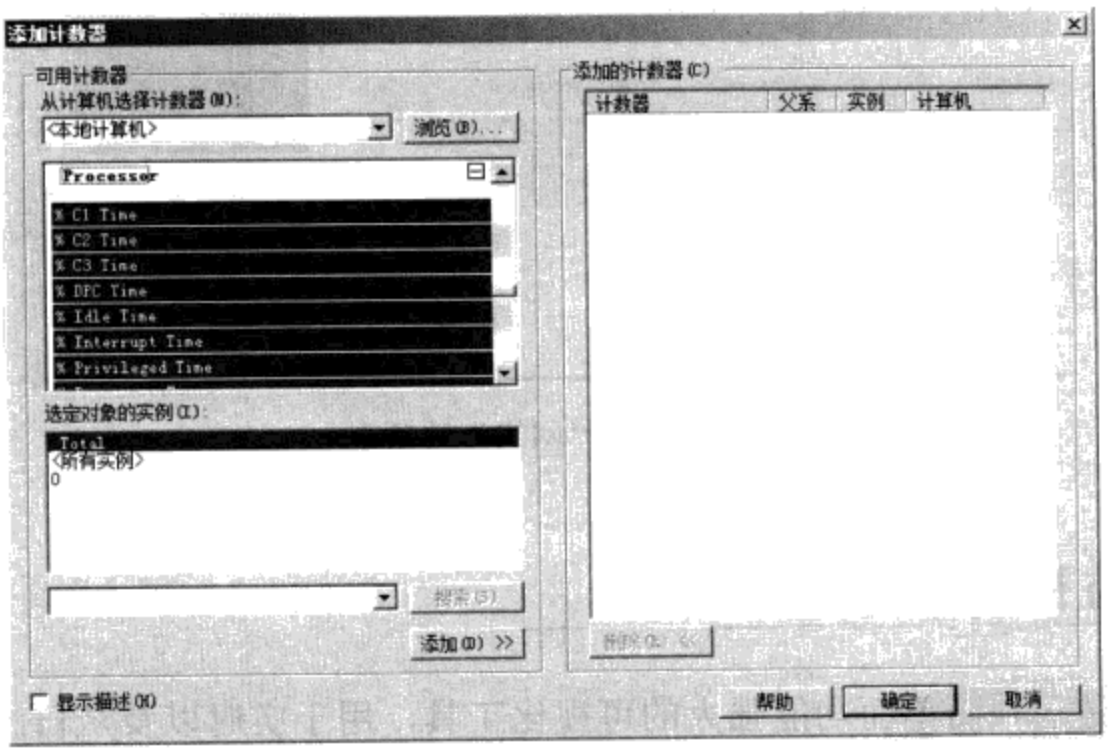


图6-29　“添加计数器”对话框

第3步，单击“确定”按钮，添加计数器成功，并开始进行监视，如图6-30所示。

2. 删除计数器

添加计算器过多，不仅会严重影响服务器运行速度，而且不容易分辨。必要时可以删除不常用的或非必要的计数器，在系统监视器的监视对象列表中，选中想要删除的计数器，然后按下“性能”工具栏中的“删除”按钮，或者直接按下“Delete”键。

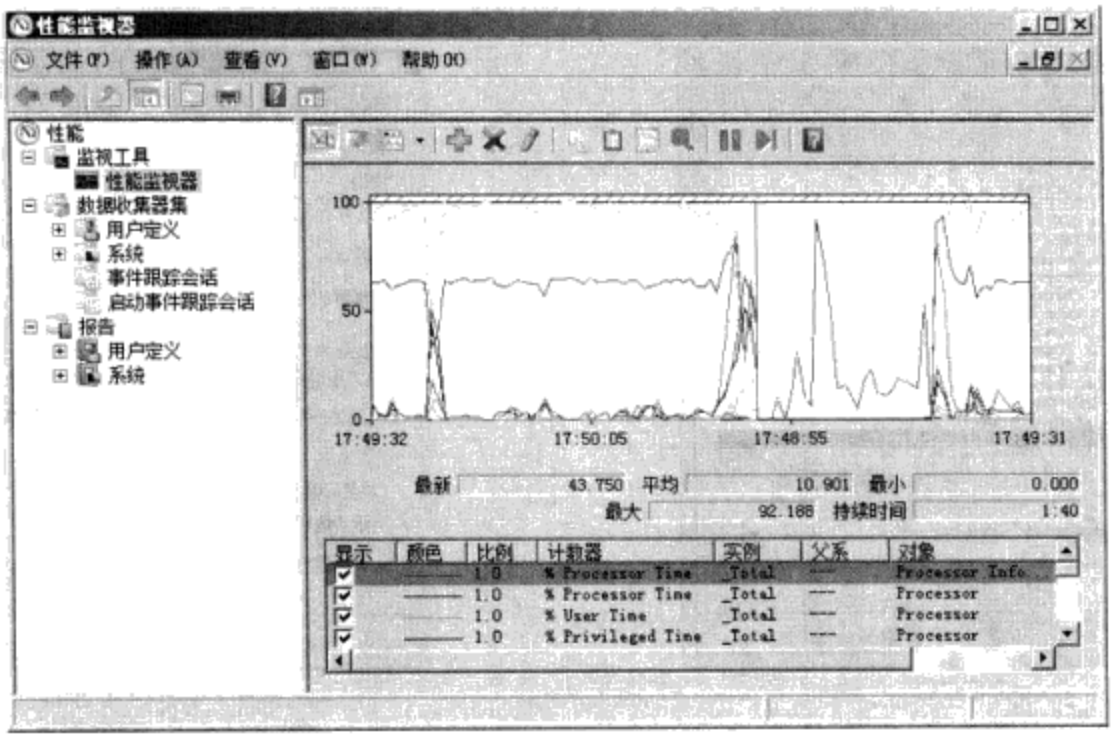


图 6-30　新计数器开始监视系统

3. 系统监视器的属性设置

系统监视器的默认设置通常可以满足大多数用户的应用，可以对其进行自定义。例如，需要监视的对象较多时，系统默认的曲线图看起来就会比较乱，而使用直方图就非常不错，此时就可以变更系统监视器的默认设置。在“系统监视器”窗口中，右击“系统监视器”并选择快捷菜单中的“属性”选项，打开“系统监视器 属性”对话框。

■ 常规设置

在“系统监视器 属性”对话框中，切换到如图 6-31 所示“常规”选项卡。其中，显示元素用于设置“系统监视器”主窗口中显示的元素类型，建议保持系统默认设置，即显示所有元素，便于比对和查看。

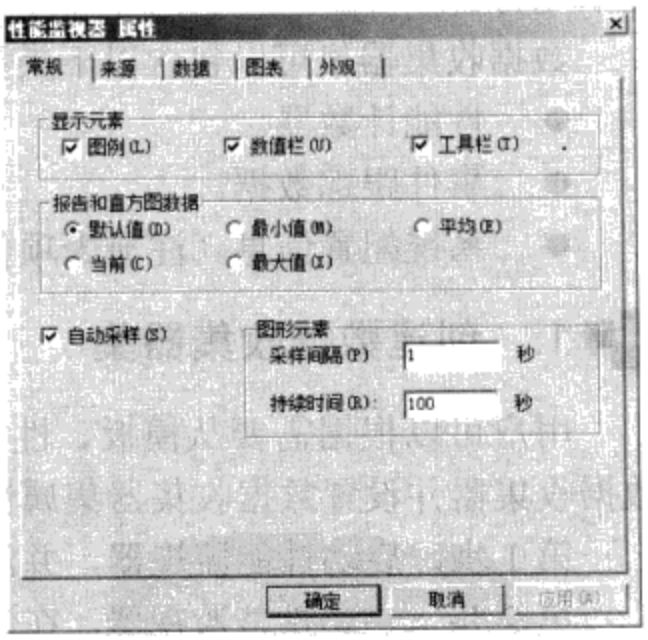


图 6-31　“常规”选项卡

■ 数据设置

在“系统监视器 属性”对话框中，切换到如图 6-32 所示“数据”选项卡。在“数据”选项卡中主要可以设置不同计数器的显示状态，如颜色、宽度、样式等，以适合个人感觉为宜。在“计数器”列表框中，选择相应的计数器后在下面即可显示其默认设置，颜色是区别计数器的显著标志，建议为不同的计数器设置不同的显示颜色和线条宽度。

■ 图表设置

在“系统监视器 属性”对话框中，切换到“图表”选项卡，如图 6-33 所示。在“图表”选项卡中可以设置“系统监视器”显示的“标题”和“垂直轴”标注等信息。为了查看更精确地结果还可以选择“垂直格线”和“水平格线”复选框。

图 6-32 “数据”选项卡

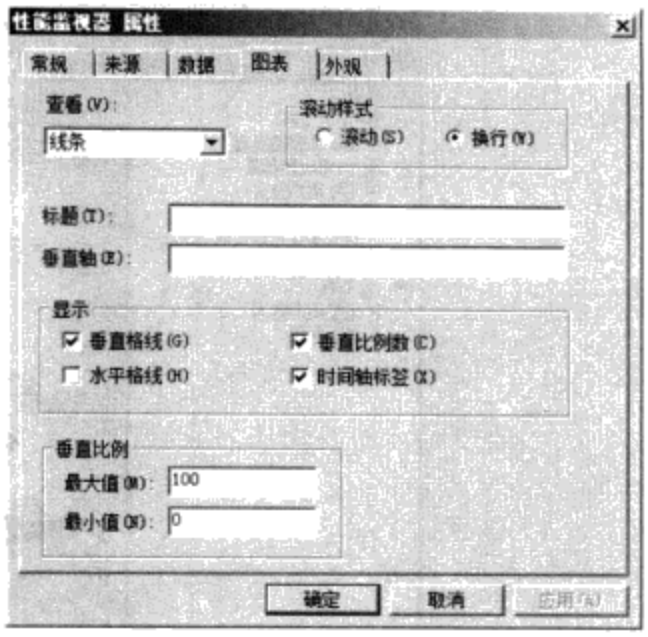


图 6-33 “图表”选项卡

6.3.3 数据收集器集

数据收集器集是 Windows 性能监视器中性能监视和报告的功能块，将多个数据收集点组织成可用于查看或记录性能的单个组件。可以创建数据收集器集，然后执行下列操作：逐个记录，与其他数据收集器集组合而且并入到日志中，在性能监视器中查看，配置为达到阈值时生成警报，或者由其他非 Microsoft 应用程序使用。可以将其与在特定时间收集数据的计划规则关联起来。可将 Windows Management Interface（WMI）任务配置为在数据收集器集收集完成之后运行。

数据收集器集可以包含以下类型的数据收集器：

- 性能计数器。
- 事件跟踪数据。
- 系统配置信息（注册表项值）。

1. 创建数据收集器集

用户可以根据需要从模板、性能监视器视图中现有的数据收集器集，或者通过选择单个数据收集器并设置数据收集器集属性中的每个单独选项来创建数据收集器集

第 1 步，启动性能监视器，并添加计数器以创建要保存为数据收集器集的自定义视图。

第 2 步，右击性能监视器，在快捷菜单中依次选择“新建”→“数据收集器集”选项，启动创建新数据收集器集向导，如图 6-34 所示。在“名称”文本框中，键入新创建的数据收集器集的名称。

第 3 步，单击“下一步”按钮，显示如图 6-35 所示“您希望将数据保存在什么位置？”对话框。在“根目录”文本框中，可以根据需要设置数据的保存路径。

第 4 步，单击“下一步”按钮，显示如图 6-36 所示“是否创建数据收集器集？”对话框。如果欲修改运行数据收集器集的用户身份，可单击“更改”按钮，根据提示键入用户名和密码即可。如果选择“立即启动该数据收集器集”单选按钮，则在完成操作后可立即收集数据。

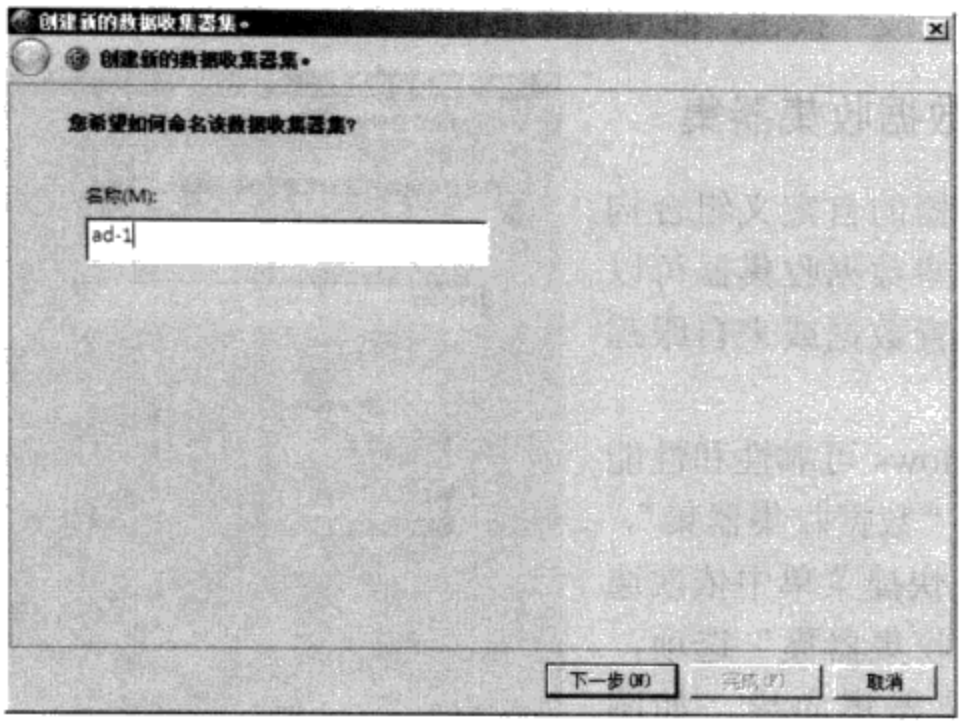


图 6-34　创建新数据收集器集向导

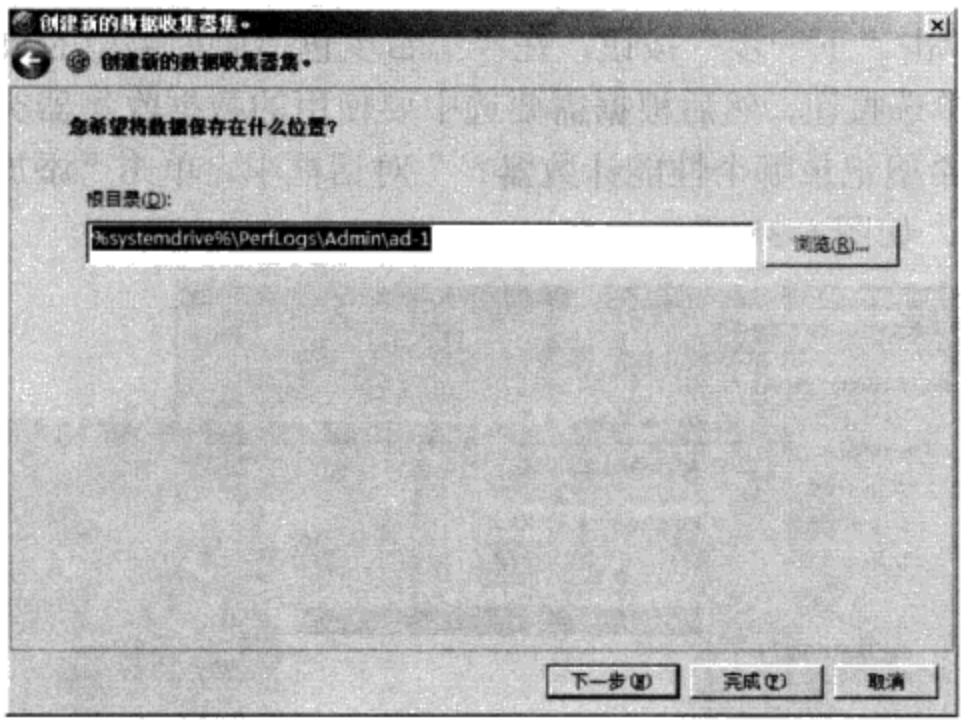


图 6-35　“您希望将数据保存在什么位置？”对话框

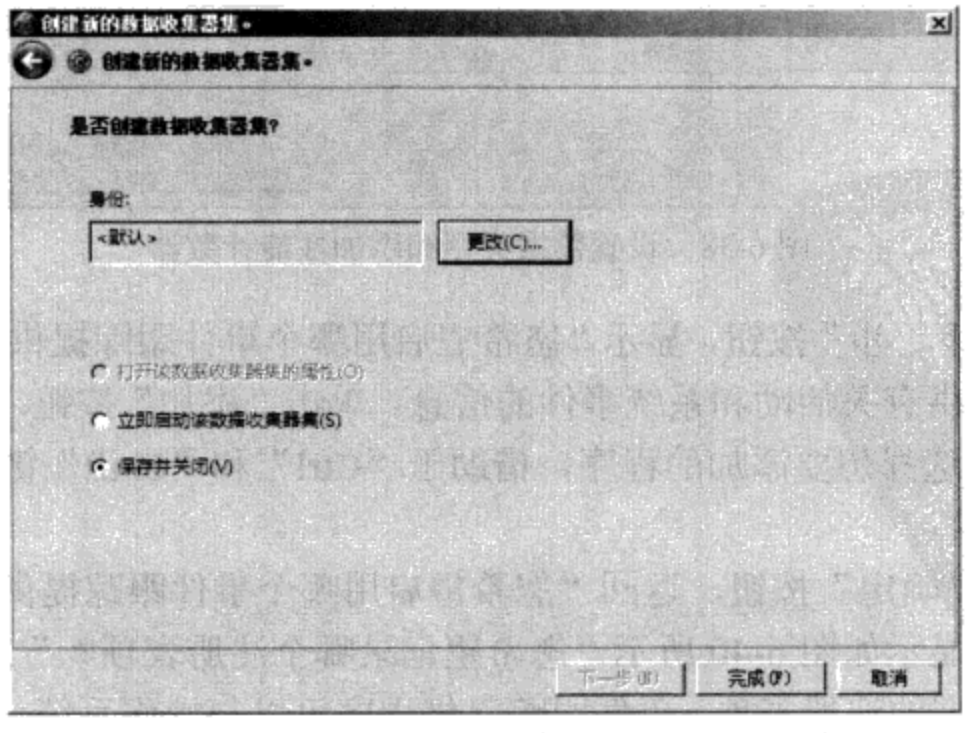


图 6-36　“是否创建数据收集器集？”对话框

第5步，单击“完成”按钮，即可完成数据收集器集的创建。

2. 手动创建数据收集器集

可以从数据收集器的自定义组合构建数据收集器集。这些数据收集器可以包括性能计数器、配置数据或来自跟踪提供程序的数据。

第1步，在Windows可靠性和性能监视器窗口中，展开“数据收集器集”，右击“用户定义”，在快捷菜单中依次选择“新建”→“数据收集器集”选项，启动创建新数据收集器集向导，如图6-37所示，设置数据收集器集名称和创建方式。

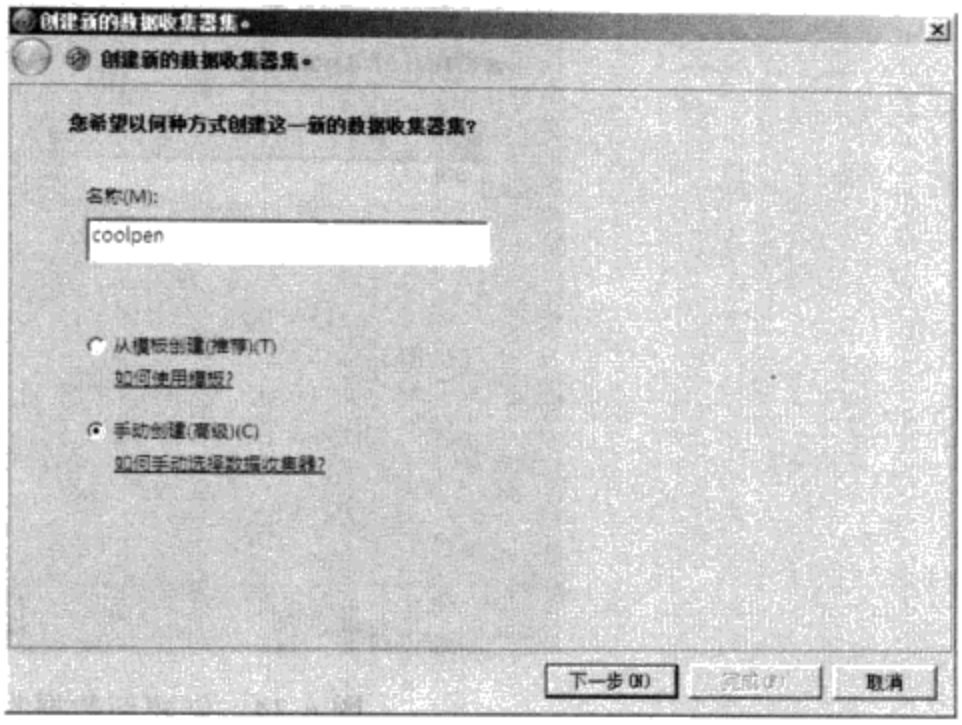


图6-37　创建新的数据收集器集向导

第2步，连续单击“下一步”按钮，在“您希望包括何种类型的数据？”对话框中，选择“创建数据日志”单选按钮，然后根据需要选中要使用的数据收集器类型的复选框即可，这里全部选中。在“您希望记录哪个性能计数器？”对话框中，单击“添加”按钮，根据需要添加相应的计数器即可，如图6-38所示。

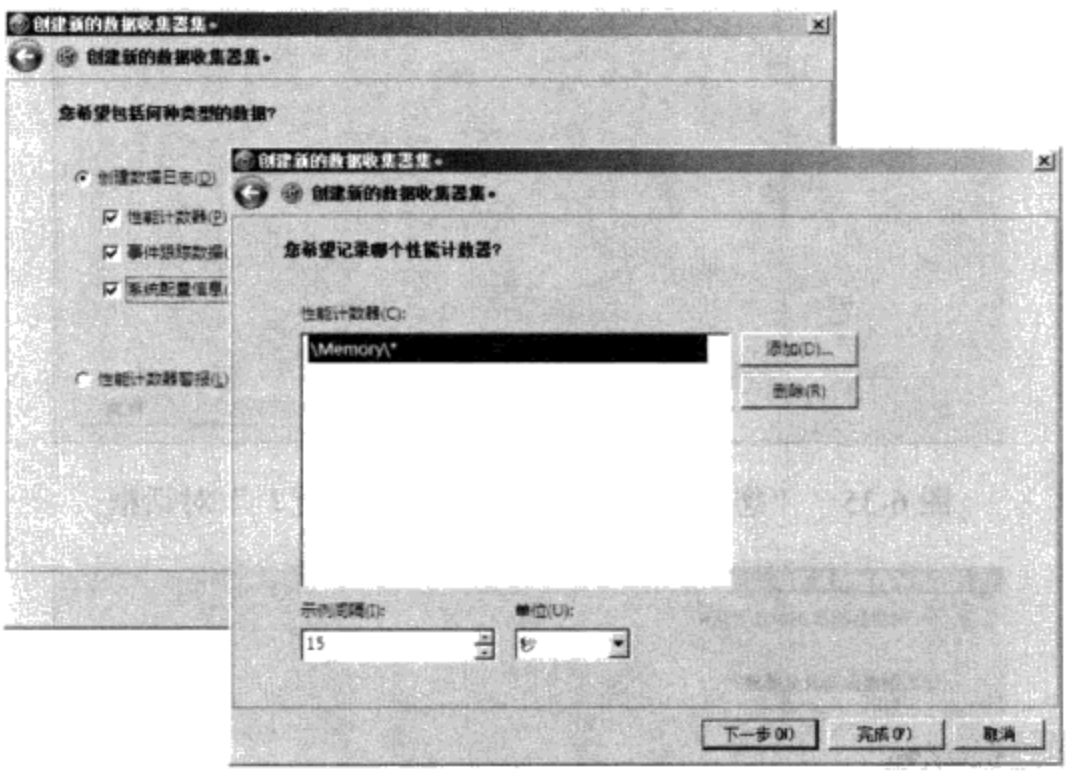


图6-38　设置数据类型和添加性能计数器

第3步，单击“下一步”按钮，显示“您希望启用哪个事件跟踪提供程序？”对话框。“事件跟踪数据”可以提供有关活动和系统事件的信息。单击“添加”按钮，在“选择事件跟踪提供程序”列表框中，选择想要添加的程序，借助于“Ctrl”和“Shift”键，可以同时选择多个程序，如图6-39所示。

第4步，单击“确定”按钮，返回“您希望启用哪个事件跟踪提供程序？”对话框。单击“下一步”按钮，显示如图6-40所示“您希望记录哪个注册表项？”对话框。单击“添加”按钮，可添加收集数据的注册表项。事件跟踪提供程序可以与操作系统一起安装，或者作为非Microsoft应用程序的一部分进行安装。

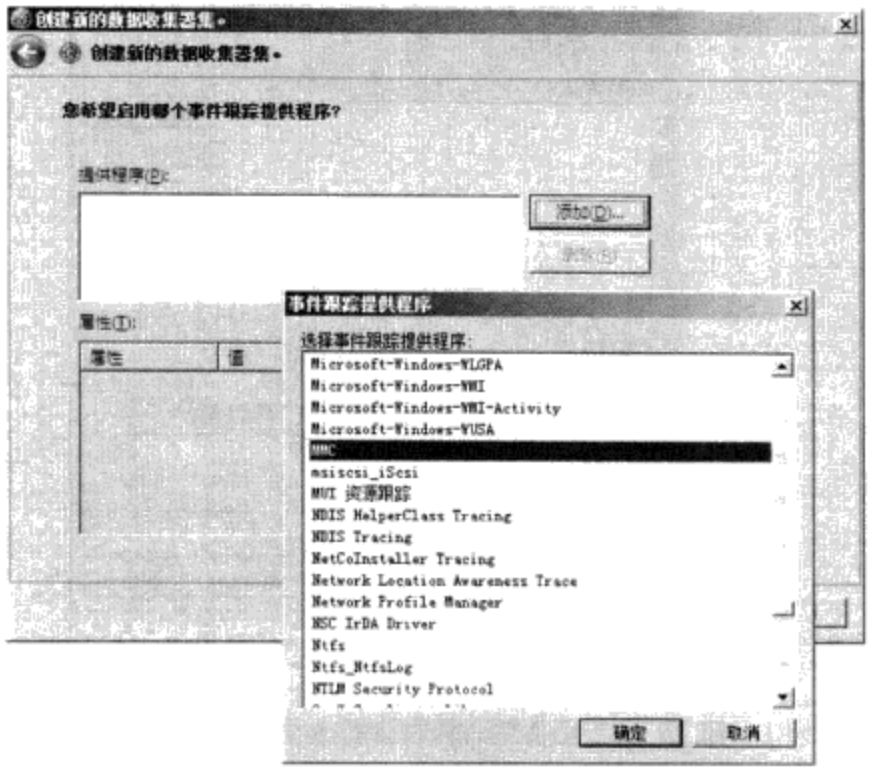


图 6-39　设置事件跟踪提供程序

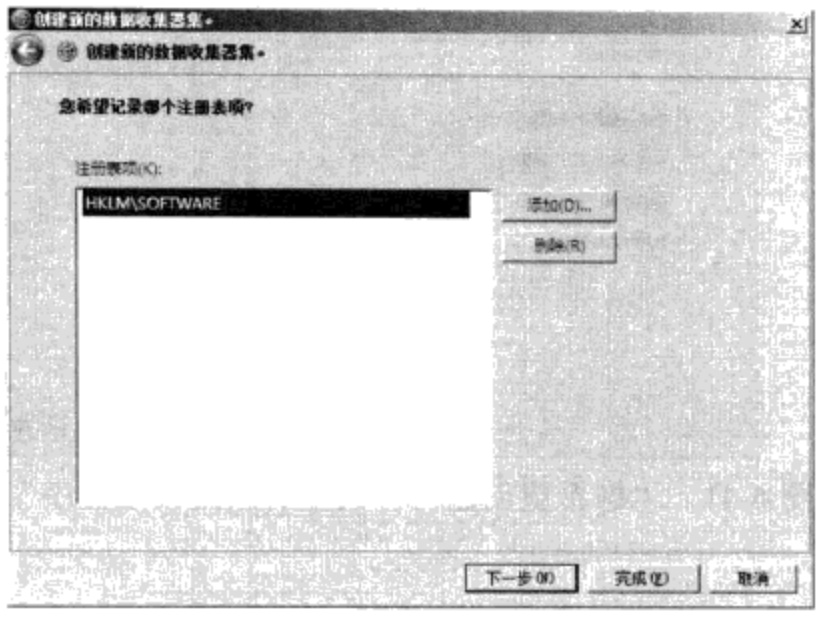


图 6-40　“您希望记录哪个注册表项？”对话框

第 5 步，连续单击“下一步”按钮，最后，单击“完成”按钮即可完成新数据收集器集的创建。

3. 创建数据收集器

在导航栏中，右击已创建的数据收集器集，并选择快捷菜单中的“新建”→“数据收集器”选项，打开如图 6-41 所示“您希望创建何种类型的数据收集程序”对话框。在“名称”文本框中输入数据收集器的名称，默认为“新的数据收集器”。然后选择希望创建的收集器类型，包括性能计数器数据收集程序、事件跟踪数据收集程序、培植数据收集程序和性能计数器警报 4 种。接下来的操作根据所选类型的不同，可能需要添加性能计数器、性能事件提供程序或注册表项等，只需按照向导提示逐步操作即可。

4. 添加性能计数器

创建数据收集器过程中已经添加了相关的性能计数器，数据收集器运行过程中，管理员可以按照如下操作步骤添加新的性能计数器。

第 1 步，在“性能监视器”窗口的“数据收集器集”目录中，展开相关的数据收集器集，并双击其中需要添加性能计数器的数据收集器，如“监视磁盘工作状态”数据收集器集中的“系统监视器日志”，打开如图 6-42 所示“系统监视器日志 属性”对话框。

第 2 步，在“性能计数器”选项卡中，单击“添加”按钮打开如图 6-43 所示对话框，从“可用计数器”列表框中选择需要添加的计数器，并单击“添加”按钮添加到右侧列表框中。

第 3 步，单击“确定”按钮，即可添加到“性能计数器”列表框中，如图 6-44 所示。

第 4 步，切换至如图 6-45 所示“文件”选项卡，在“日志文件名”文本框中可以重新输入新的文件名，在“文件名格式”文本框中单击右侧按钮，可以根据需要选择适当的命名格式，以便日后可以快速准确查询所需的日志，例如以日志文件创建的日期、时间作为文件名的结尾。

第 5 步，单击“确定”按钮，保存设置即可。

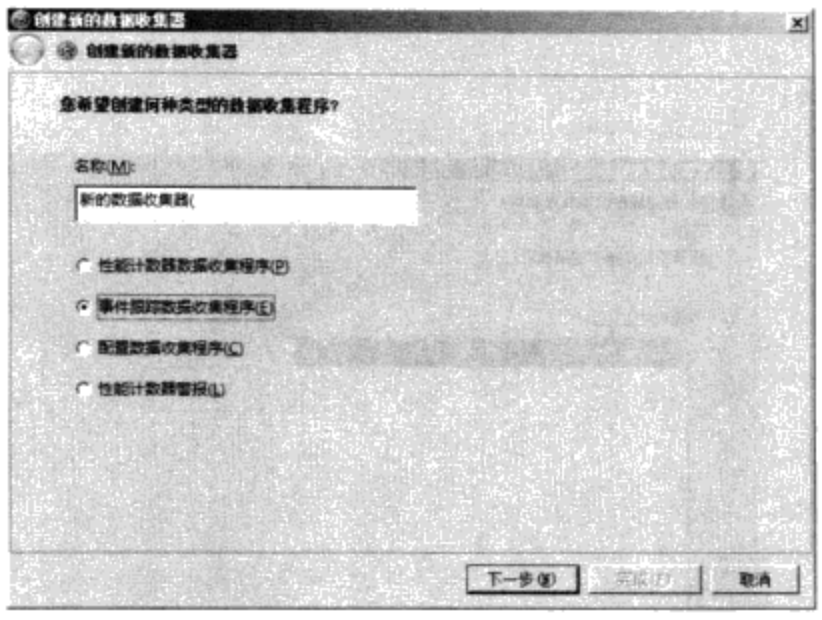


图 6-41　“您希望创建何种类型的数据收集程序”对话框

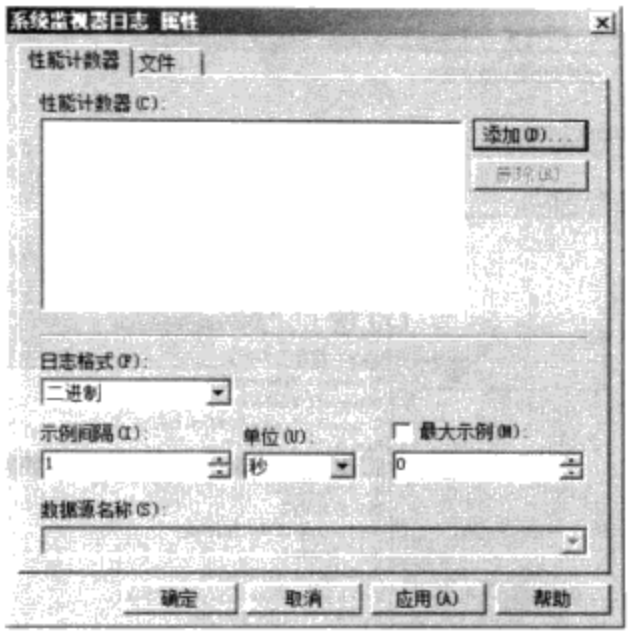


图 6-42　“系统监视器日志 属性”对话框

图 6-43　添加计数器

图 6-44　“性能计数器”选项卡

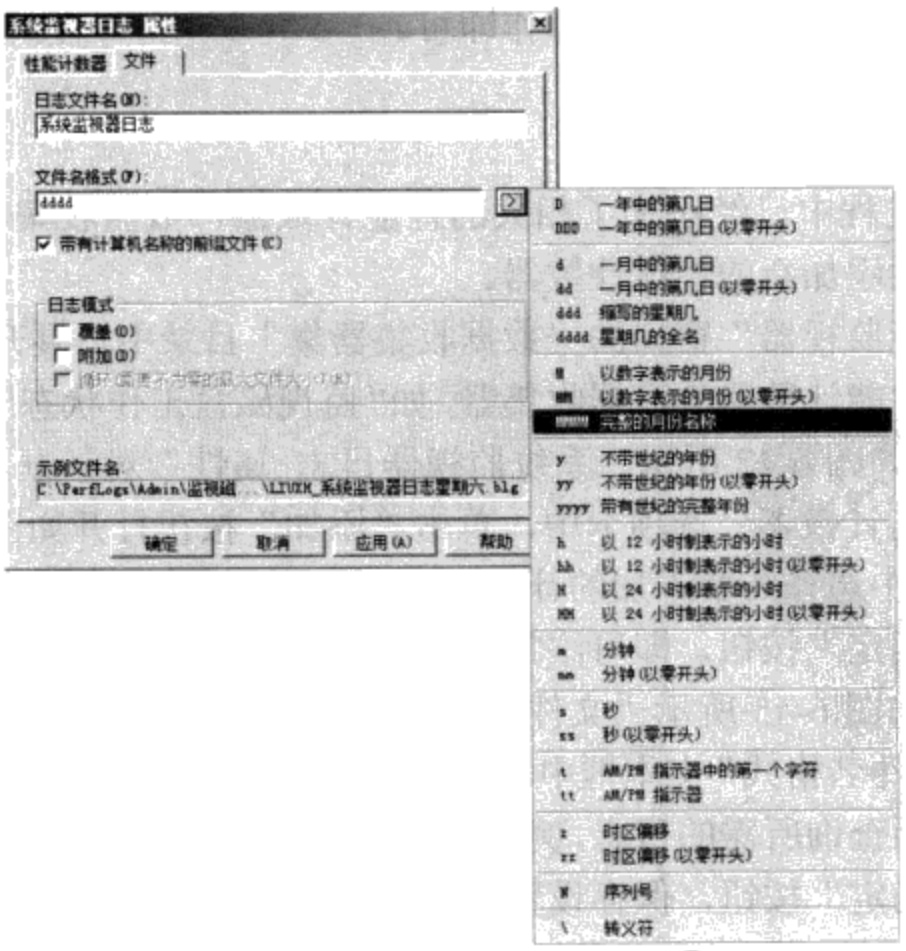


图 6-45　“文件”选项卡

第 7 章　局域网接入安全

随着局域网规模和功能的不断扩展，网络环境日益复杂，原本功能单一的计算机网络，现在还需要随时为移动用户、临时用户、手机用户等提供服务，在企业网络覆盖范围内，任何用户都可以随时随地接入局域网，甚至盗用合法用户身份信息访问内部共享资源。为了确保整个局域网的安全，必须对局域网接入进行严格控制，如身份验证、加密传输等，严防非法接入问题的出现。

7.1　配置和管理 RADIUS 服务器

RADIUS 是一种用于在需要认证其链接的网络访问服务器（NAS）和共享认证服务器之间进行认证、授权和记账信息的文档协议。从 Windows Server 2008 系统开始，RADIUS 服务就已经被集成在“网络策略”服务器角色中。局域网中的 RADIUS 服务器，主要用于接收和处理来自 RADIUS 客户端的用户身份验证请求，确保局域网的安全接入。

7.1.1　安装 RADIUS 服务器

在 Windows Server 2008 R2 系统中，将服务器配置网络策略服务器的同时，将自动配置为 RADIUS 服务器。网络策略服务器主要为接入局域网用户提供身份验证和系统状态评估，具体应用请参考本书“第 8 章　网络访问保护”中的相关介绍。而 RADIUS 服务器的用途是十分广泛的，主要包括认证（Authentication）、记账（Accounting）和授权（Authorization），可以概括为 AAA。

以管理员账户登录 Windows Server 2008 R2 系统，启动“添加角色向导”，在“选择服务器角色”对话框中选中“网络策略和访问服务”复选框，连续单击“下一步”按钮，在“选择角色服务”对话框中，选中“网络策略服务器”复选框即可，如图 7-1 所示。继续单击“下一步”按钮，即可完成 RADIUS 服务器的安装。

7.1.2　配置 RADIUS 客户端

在为网络用户提供 AAA 服务时，RADIUS 服务器并不是直接接收来自客户端的网络请求。在配置审核和记账的网络中，客户端首先向开启身份验证功能的服务器或网络设备发送身份验证请求，服务器或网络设备再将请求信息发送到 RADIUS 服务器，由 RADIUS 服务器完成请求信息的认证、授权和记账。因此，必须将用于转发用户请求信息的服务器或网络设备配置为 RADIUS 服务器的客户端。

在“网络策略服务器”窗口中，展开“RADIUS 客户端和服务器”节点，右击“RADIUS 客户端”并选择快捷菜单中的“新建”命令，启动“新建 RADIUS 客户端”对话框，如图 7-2 所示。首先选中“启用此 RADIUS 客户端”复选框；然后在“名称和地址”区域设置一个便

于识别的客户端名称，指定客户端设备的IP地址，如果不能确认是否正确，可以单击“验证”按钮进行验证；最后，选择共享密钥生成方式，建议选择“手动”单选按钮并输入共享密钥。

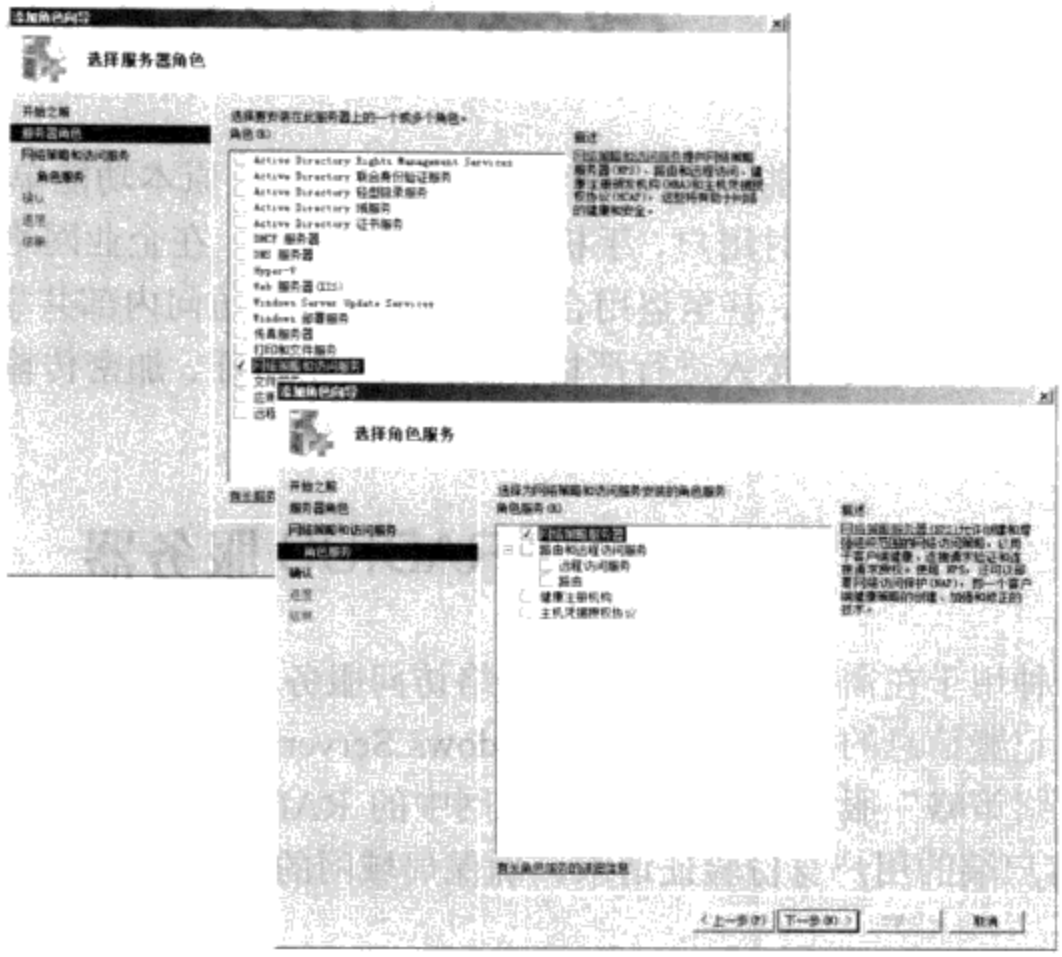


图 7-1 安装RADIUS服务器

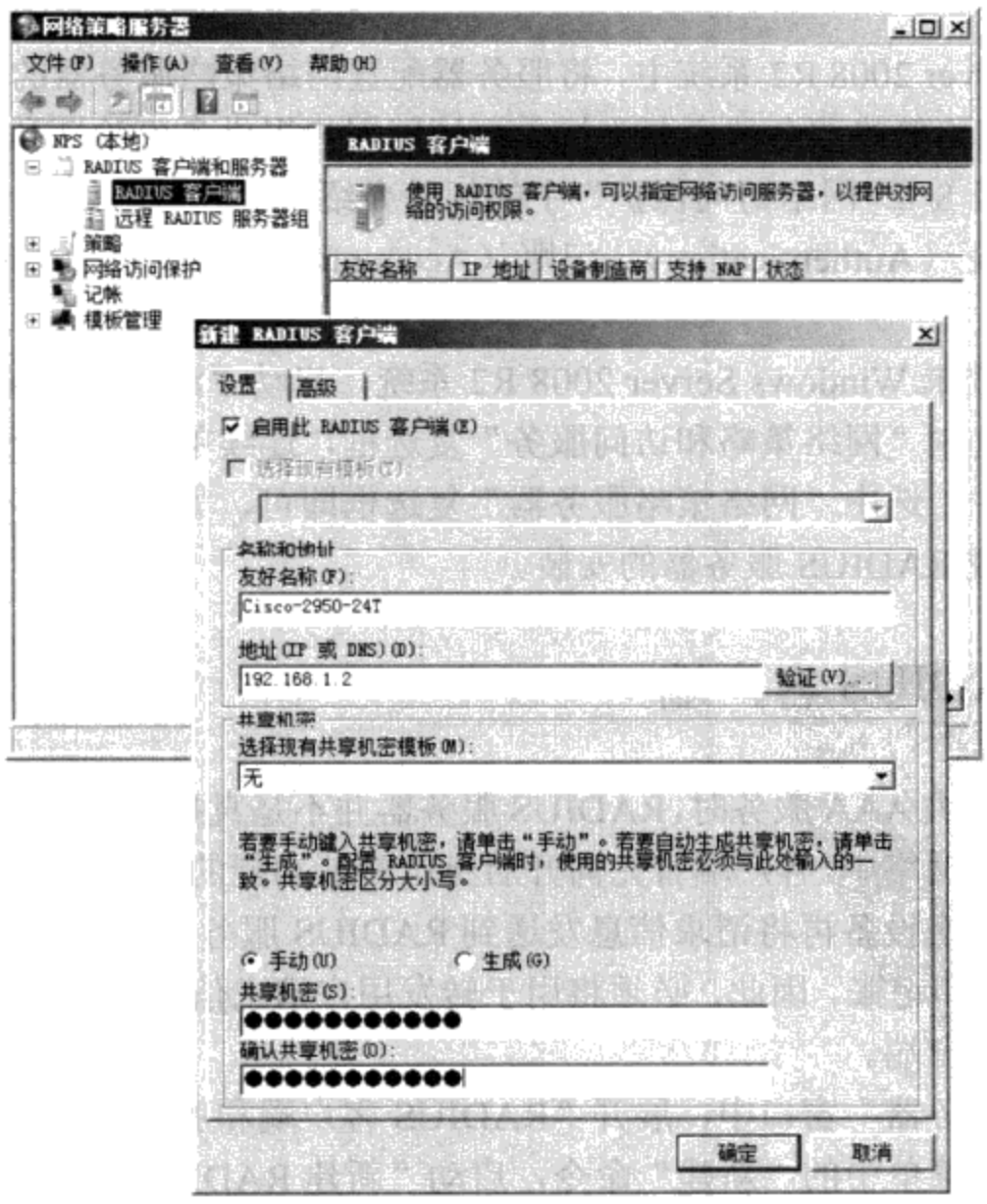


图 7-2 新建RADIUS客户端

注意 在启用身份验证的网络设备或服务器上配置到 RADIUS 服务器的连接时，必须指定与此处共享机密完全相同的密钥。

切换到“高级”选项卡，设置供应商名称及其他选项，如图 7-3 所示。这里以将 Cisco 交换机配置为 RADIUS 客户端为例，所以在“供应商名称”下拉列表框中应选择“Cisco”。

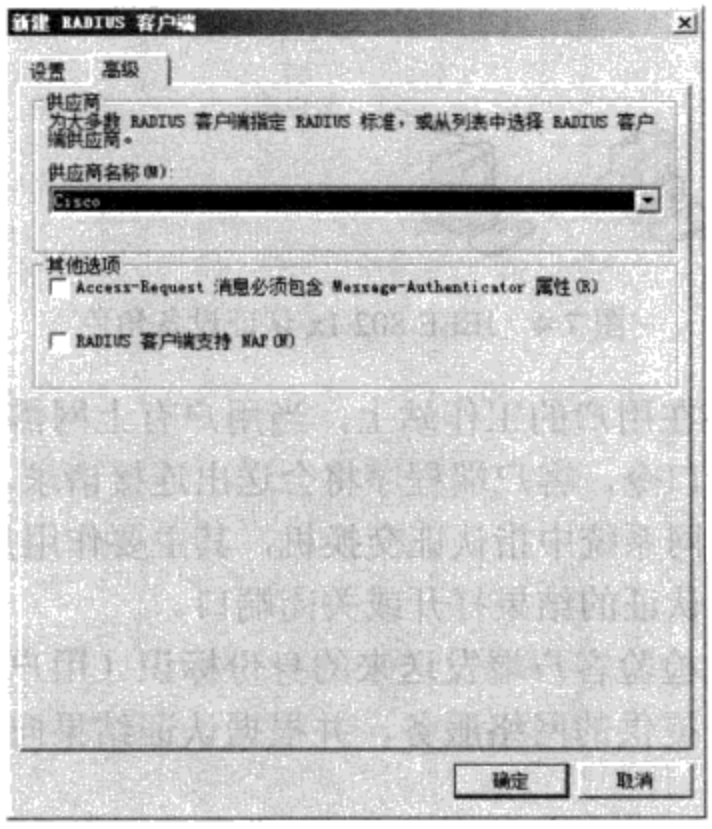


图 7-3 “高级”选项卡

7.2 基于端口的认证安全

有线网络仍是企业网络的主体，默认用户以有线方式接入网络时就必须连接到相应的网络接口，因此基于端口的安全认证措施是目前广泛应用的安全部署方案，如 IEEE 802.1x 认证等。目前，几乎所有网络设备都支持 IEEE 802.1x 认证，用户通过接口建立到网络设备的连接时，设备会要求其发送身份信息，通过验证和审核之后方可建立连接，否则将被断开网络连接，也就无法接入局域网。

7.2.1 IEEE 802.1x 认证简介

IEEE 802.1x 执行基于端口的网络访问控制。基于端口的网络访问控制使用交换的局域网(LAN)基础设施的物理特征来验证连接到 LAN 端口的设备，并防止访问身份验证进程已经失败的那个端口。IEEE 802.1x 身份验证用于对有线以太网和无线 IEEE 802.11 网络进行经过身份验证的网络访问。IEEE 802.1x 通过提供对集中式用户标识、身份验证、动态密钥管理和记账的支持来提高安全性和部署。

1. IEEE 802.1x 认证元素

在 IEEE 802.1x 协议中，只有具备了以下 3 个元素如图 7-4 所示，才能够完成基于端口的访问控制的用户认证和授权。

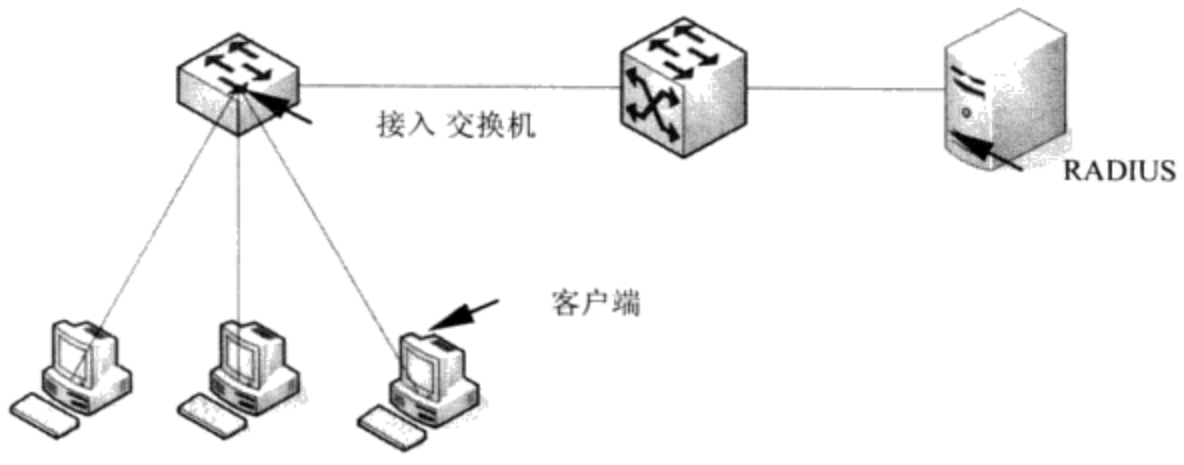


图 7-4 IEEE 802.1x 认证设备角色

- 客户端。一般安装在用户的工作站上，当用户有上网需求时，激活客户端程序，输入必要的用户名和口令，客户端程序将会送出连接请求。
- 认证系统。在以太网系统中指认证交换机，其主要作用是完成用户认证信息的上传、下达工作，并根据认证的结果打开或关闭端口。
- 认证服务器。通过检验客户端发送来的身份标识（用户名和口令）来判别用户是否有权使用网络系统提供的网络服务，并根据认证结果向交换机发出打开或保持端口关闭的状态。

802.1x 协议与 LAN 是无缝融合的。802.1x 利用了交换 LAN 架构的物理特性，实现了 LAN 端口上的设备认证。在认证过程中，LAN 端口要么充当认证者，要么扮演请求者。在作为认证者时，LAN 端口在需要用户通过该端口接入相应的服务之前，首先进行认证，如若认证失败则不允许接入；在作为请求者时，LAN 端口则负责向认证服务器提交接入服务申请。基于端口的 MAC 锁定只允许信任的 MAC 地址向网络中发送数据。来自任何“不信任”的设备的数据流会被自动丢弃，从而确保最大限度的安全性。

2. IEEE 802.1x 认证过程

配置 IEEE 802.1x 基于端口的认证，必须启用认证、授权、记账（AAA，Authentication Authorization Accounting）以及认证方法列表。认证方法列表描述了查询和认证用户的次序与认证方法。802.1x AAA 处理过程如图 7-5 所示。

第 1 步，当用户有上网需求时打开 802.1x 客户端，输入已经申请、登记过的用户名和口令，发起连接请求。此时，客户端程序将发出请求认证的报文给交换机，开始启动一次认证过程。

第 2 步，交换机收到请求认证的数据帧后，将发出一个请求帧要求用户的客户端程序发送输入的用户名。

第 3 步，客户端程序响应交换机发出的请求，将用户名信息通过数据帧送给交换机。交换机将客户端送上来的数据帧经过封包处理后送给 RADIUS 服务器进行处理。

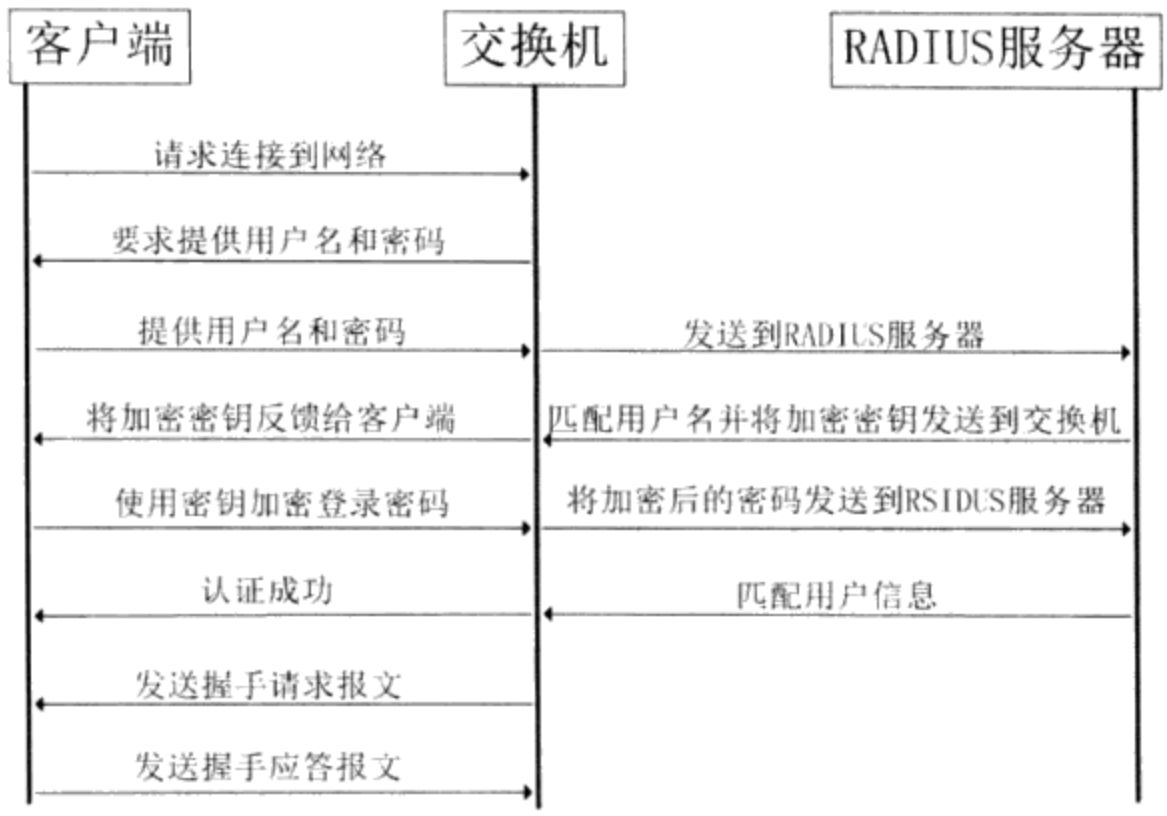


图 7-5　IEEE 802.1x 认证过程

第 4 步，RADIUS 服务器收到交换机转发的用户名信息后，将该信息与数据库中的用户名表相比对，找到该用户名对应的密码信息，用随机生成的密钥对其进行加密处理，同时也将此密钥发送给交换机，由交换机传给客户端程序。

第 5 步，客户端程序收到由交换机传来的密钥后，用该密钥对其密码部分进行加密处理，并通过交换机传给 RADIUS 服务器。

第 6 步，RADIUS 服务器将加密后的密码信息和自己经过加密运算后的密码信息进行对比，如果相同，则认为该用户为合法用户，反馈认证通过的消息。

第 7 步，交换机将端口状态改为授权状态，允许用户的业务流通过该端口访问网络。

提示　客户端也可以发送“请求退出”报文给交换机，主动终止已认证状态，交换机将端口状态从授权状态改变成未授权状态。

3. IEEE 802.1x 认证方案

方案 1：在接入层设备上启用 802.1x

接入层交换机采用支持 IEEE 802.1x 认证功能的设备，并在直接连接计算机的各端口启用 IEEE 802.1x 认证，从而实现对用户登录网络的限制。接入层交换机的 Uplink 端口、汇聚交换机和核心交换机，均不设置认证端口。拓扑结构如图 7-6 所示。

方案要求：

- 用户支持 802.1x，即要装有 802.1x 的客户端软件（Windows XP/Vista/7 系统内置，其他操作系统应当安装符合 IEEE802.1x 标准的客户端软件）。
- 接入层设备支持 IEEE 802.1x。
- 有一台（或多台）支持标准 RADIUS 的服务器作为认证服务器。

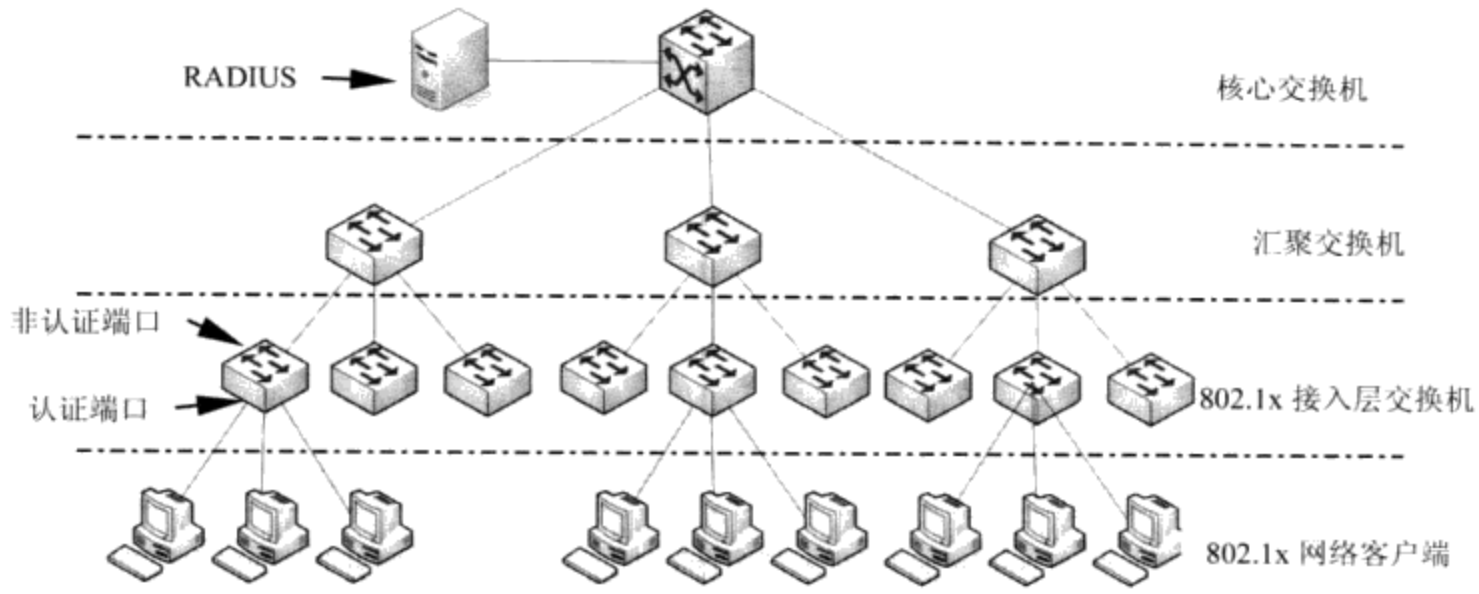


图 7-6　接入层采用 802.1x 设备

方案配置要点：

- 与 Radius Server 相连的口及上联口，配置成非受控口，以便交换机能正常地与服务器进行通信，以及使已认证用户能通过上联口访问网络资源
- 与用户连接的端口要设置为受控口，以实现对接入用户的控制，用户必须通过认证才能访问网络资源。

该方案的特点：

- 每台支持 802.1x 的交换机所负责的客户端少，认证速度快。各台交换机之间相互独立，交换机的重起等操作不会影响到其他交换机所连接的用户。
- 用户的管理集中于 RADIUS 服务器上，管理员不必考虑用户连接在哪台交换机上，便于管理员的管理。
- 管理员可以通过网络管理到接入层的设备。

方案 2：在汇聚层设备上启用 802.1x

接入层交换机无需支持 IEEE 802.1x 认证功能的设备，但是，汇聚交换机则必须采用支持 IEEE 802.1x 认证功能的设备，并在连接接入层交换机的各端口启用 IEEE 802.1x 认证，从而实现对用户登录网络的限制。接入层交换机、核心交换机和汇聚交换机的 Uplink 端口，均不设置认证端口。拓扑结构如图 7-7 所示。

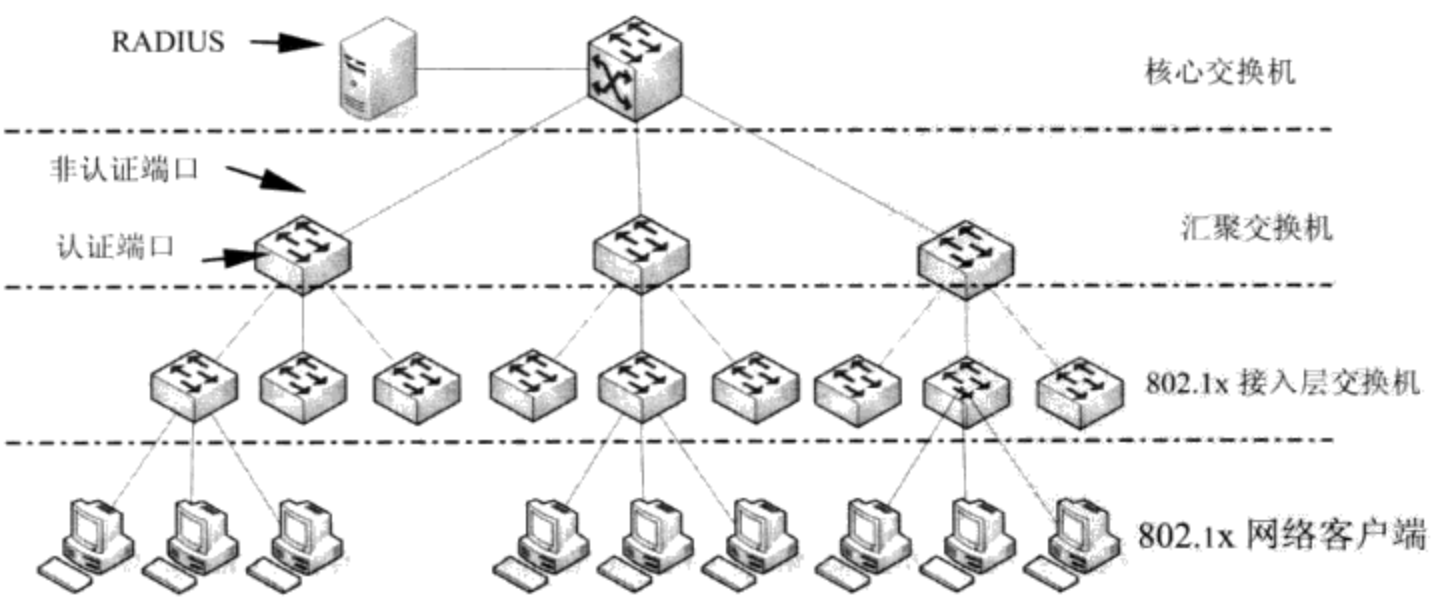


图 7-7　汇聚层采用 802.1x 设备

方案要求：

- 用户支持 802.1x，即必须安装 802.1x 的客户端软件。
- 接入层设备支持要能透传 IEEE 802.1x 帧（EAPOL）。
- 汇接层设备支持 802.1x（扮演认证者角色）。
- 有一台（或多台）支持标准 RADIUS 的服务器作为认证服务器。

该方案的配置要点：

- 与 RADIUS 服务器相连的口及上联口，配置成非受控口，以便交换机能正常地与服务器进行通信，以及使已认证用户能通过上联口访问网络资源。
- 与接入层交换机连接的端口要设置为受控口，以实现对接入用户的控制，用户必须通过认证才能访问网络资源。

该方案的特点：

- 由于 802.1x 认证由汇聚层设备完成，网络规模大，支持的用户数多，对设备的要求高，因为若该层设备发生故障，将导致大量用户不能正常访问网络。
- 用户的管理集中于 RADIUS 服务器上，网络管理员不必考虑用户连接在哪台交换机上，便于进行管理。
- 接入层设备可以使用较廉价的非网管型交换机（只要支持 EAPOL 帧透传）。
- 网络管理员不能通过网络直接管理到接入层设备。

4. 配置 IEEE 802.1x 的注意事项

配置 802.1x 认证时，应当注意以下几点：

- 当启用 802.1x 时，只有端口通过认证，其二层和三层功能才能被激活。
- 802.1x 协议支持二层静态访问端口、语音 VLAN 端口和三层路由端口，但是，不能支持 Trunk 端口、动态端口、动态访问端口和 EtherChannel 端口。如果尝试在这些类型的端口上启用 802.1x，将显示错误提示信息，802.1x 不能被启用。当尝试将启用 802.1x 的端口改变为这些类型的端口时，也将显示错误提示信息，并且端口模式也不会被改变。
- 虽然可以在 Switched Port Analyzer (SPAN) 和 Remote SPAN (RSPAN)目的端口上启用 802.1x，但是，在将端口从 SPAN 或 RSPAN 目的端口移除前，802.1x 将处于禁用状态。不过，可以在 SPAN 或 RSPAN 源端口启用 802.1x。
- 可以配置任意 VLAN，除了 RSPAN VLAN、private VLAN 或作为 802.1x 来宾 VLAN 的语音 VLAN。来宾 VLAN 功能不被 internal VLAN（路由端口）或 Trunk 端口所支持，只被访问端口所支持。
- 当在端口上启用 802.1x 时，不能配置端口 VLAN 为语音 VLAN。
- 可以在 private-VLAN 端口配置 802.1x，但是，不能在 private-VLAN 端口上同时配置安全端口、语音 VLAN、来宾 VLAN 或用户访问列表。
- 当配置来宾 VLAN 作为 802.1x 端口后，需要配置 DHCP 服务器的 IP 地址。

7.2.2 配置 IEEE 802.1x 认证

借助以下操作，可以指定的交换机上启用 IEEE 802.1x 认证，实现用户登录认证。

第1步，进入全局配置模式。

```
coolpen-2950-24T# configure terminal
```

第2步，在交换机上启用IEEE 802.1x认证。

```
coolpen-2950-24T (config)# dot1x system-auth-control
```

第3步，启用AAA。

```
coolpen-2950-24T (config)# aaa new-model
```

第4步，创建IEEE 802.1x AAA认证方式列表。如果在认证命令中没有指定列表名称，将创建并使用一个默认列表。默认情形下，将使用认证方式后的默认关键字。默认认证方式自动应用于所有接口。键入下列至少一个关键字，group radius使用列表中所有的RADIUS服务器认证；none不认证，客户端自动通过交换机认证，而无需使用客户端支持信息。

```
coolpen-2950-24T (config)# aaa authentication dot1x {default} method1 [method2...]
```

第5步，指定欲启用IEEE 802.1x认证的端口。

```
coolpen-2950-24T (config)# interface interface-id
```

第6步，将该端口指定为非中继、非标签的单一VLAN二层接口。

```
coolpen-2950-24T (config-if)# switchport mode access
```

第7步，在该端口以默认参数启用802.1x认证。

```
coolpen-2950-24T (config-if)# dot1x pae authenticator
Enables 802.1x authentication on the port with default parameters.
```

第8步，在该端口启用802.1x认证。

```
coolpen-2950-24T (config-if)# dot1x port-control auto
```

第9步，返回特权模式。

```
coolpen-2950-24T (config-if)# end
```

第10步，查看配置是否正确。

```
coolpen-2950-24T # show dot1x
```

第11步，保存配置。

```
coolpen-2950-24T # copy running-config startup-config
```

提示 若欲在多个端口启用IEEE 802.1x认证，应当重复指定端口和启用认证的操作。或者将相同配置的端口设置为一个端口组，然后，配置该端口组。

7.2.3 配置交换机到 RADIUS 服务器的通信

RADIUS 服务器维护了所有用户的信息，包括用户名、密码、该用户的授权信息，以及该用户的记账信息。所有的用户集中于 RADIUS Server 管理，而不必分散于每台交换机，便于管理员对用户的集中管理。

RADIUS 安全服务器通过主机名或 IP 地址、主机名和指定的 UDP 端口号，或者 IP 地址和批定的 UDP 端口号被识别。IP 地址和 UDP 端口号相结合构成惟一的标识符，在一个 IP 地址的服务器上，可以采用多 UDP 端口方式启用多个 RASIUS 请求。如果在同一 RADIUS 服务器上配置两个不同的主机条目，那么，第 2 个主机条目将担当第 1 条目失败后的备份。

交换机到 RADIUS 服务器的通信配置如下：

第 1 步，进入全局配置模式。

```
coolpen-2950-24T # configure terminal
```

第 2 步，配置 RADIUS 服务器参数。hostname | ip-address，指定 RADIUS 服务器的主机名或 IP 地址。auth-port port-number，指定认证请求的 UDP 目的端口。默认为 1812，可取值范围为 0～65536。key string，指定在交换机和 RADIUS 服务器之间的认证或加密密钥。这个密钥是一个字符串，必须与 RADIUS 服务器上使用的密钥相匹配。若欲使用多个 RADIUS 服务器，重复键入该命令。

```
coolpen-2950-24T (config)# radius-server host {hostname | ip-address}
auth-port port-number key string
```

第 3 步，返回特权配置模式。

```
coolpen-2950-24T (config-if)# end
```

第 4 步，校验当前设置。

```
coolpen-2950-24T # show running-config
```

第 5 步，保存当前配置。

```
coolpen-2950-24T # copy running-config startup-config
```

7.2.4 配置重新认证周期

可以实施对 802.1x 客户的定期重新认证，并且指定重新认证的周期。默认情况下，两次认证的间隔为 3600 秒。如果人员流行性较大，且对安全性要求较高，可以缩短重新认证的时间。

第 1 步，进入全局配置模式。

```
coolpen-2950-24T # configure terminal
```

第 2 步，指定欲配置的端口。

```
coolpen-2950-24T (config)# interface interface-id
```

第3步，启用定期重新认证。默认状态下，该功能被禁用。

```
coolpen-2950-24T (config-if)# dot1x reauthentication
```

第4步，设置两次重新认证之间的时间间隔，单位为秒。取值范围为1～65535，默认为3600秒。

```
coolpen-2950-24T (config-if)# dot1x timeout reauth-period seconds
```

第5步，返回特权配置模式。

```
coolpen-2950-24T (config-if)# end
```

第6步，校验当前设置。

```
coolpen-2950-24T # show dot1x interface interface-id
```

第7步，保存当前配置。

```
coolpen-2950-24T # copy running-config startup-config
```

7.2.5 修改安静周期

所谓安静周期，是指当客户端无法通过认证后，再次认证所需要等待的时间。为了使用户尽快得到再次重新尝试键入密码，以正确登录网络的机会，可以缩短安静周期。当然，应当在一些比较可靠的接口设置。

第1步，进入全局配置模式。

```
coolpen-2950-24T # configure terminal
```

第2步，指定欲配置的端口。

```
coolpen-2950-24T (config)# interface interface-id
```

第3步，指定认证失败后，可以重新认证所需等待的时间。默认状态为60秒，可取值范围为1～65535秒。

```
coolpen-2950-24T (config-if)# dot1x timeout quiet-period seconds
```

第4步，返回特权配置模式。

```
coolpen-2950-24T (config-if)# end
```

第5步，校验当前设置。

```
coolpen-2950-24T # show dot1x interface interface-id
```

第6步，保存当前配置。

```
coolpen-2950-24T # copy running-config startup-config
```

7.2.6 用户计算机配置

启动 802.1x 身份验证客户端功能。打开“服务”窗口，右击“Wired AutoConfig”服务并选择快捷菜单中的“启动”选项，启动该服务。如果希望此服务随系统自动启动，则可以将其启动类型修改为“自动”。另外，还要确保“Extensible Authentication Protocol”服务处于“启动”状态。如图 7-8 所示。

打开“网络连接”窗口，右击正在使用的本地连接（例如“本地连接”）并选择快捷菜单中的“属性”命令，显示“本地连接 属性”对话框，切换到如图 7-9 所示“身份验证”选项卡。选中“启用 IEEE 802.1X 身份验证”和“缓存用户信息以便随后连接网络使用”复选框。

图 7-8 启动相关服务

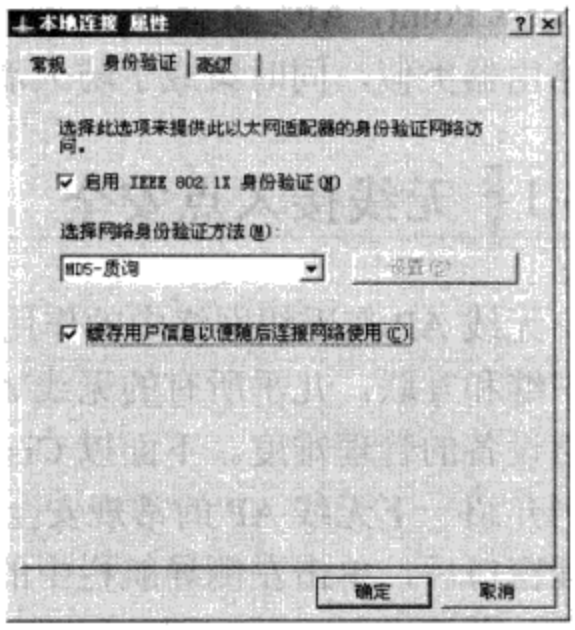


图 7-9 “身份验证”选项卡

最后，单击“确定”按钮，保存配置。

7.2.7 客户端接入启用 802.1x 认证的网络

第 1 步，网络用户完成计算机配置之后，即可开始向交换机发送身份验证请求，任务栏中的图标显示如图 7-10 所示状态，配置 802.1x 身份验证之前，网络连接是断开的。

第 2 步，当任务栏显示“需要其他信息以连接到网络”提示信息时，单击提示信息显示如图 7-11 所示“输入凭据”对话框。输入被 ACS 服务器授予访问权限的用户账户和密码，例如 user。

图 7-10 尝试连接到网络

图 7-11 “输入凭据”对话框

第3步，单击“确定”按钮，向交换机发送身份验证信息，交换机将身份验证请求转发到ACS服务器，如果通过ACS服务器身份验证，则成功建立网络连接，任务栏中的图标显示如图7-12所示状态。

图7-12 成功连接到网络

7.3 无线网络设备安全

随着无线网络用户队安全需求的日益严格，各种无线网络设备的安全功能也不断完善，通常包括WEP加密、SSID设置、802.11x身份认证、划分VLAN、MAC地址过滤等。如今，无线网络的安全程度已经远超过传统有线方式的计算机网络，一台功能强大的无线接入点（Access Point，AP）就像是一台可网管交换机，同时支持多种安全功能，而无限路由器和以太网路由器类似，同时集成了防火墙、VPN等附加安全功能。

7.3.1 无线接入点安全

无线AP在无线网络中的作用类似于以太网络中的集线器，用于实现无线客户端之间的信号中继和互联。几乎所有的无线AP都支持Web、Telnet已经图形窗口管理方式，从而简化了网络设备的管理难度。下面以Cisco Aironet 1300无线网桥（无线网桥也是无线AP的一种）为例介绍一下无线AP的常规安全设置，以管理员账户登录到Cisco Aironet 1300无线网桥Web管理窗口后，单击左侧导航栏中的“SECURITY”，即可查看当前的各项安全设置，如图7-13所示，继续进入下面的相关配置页面即可修改安全设置。

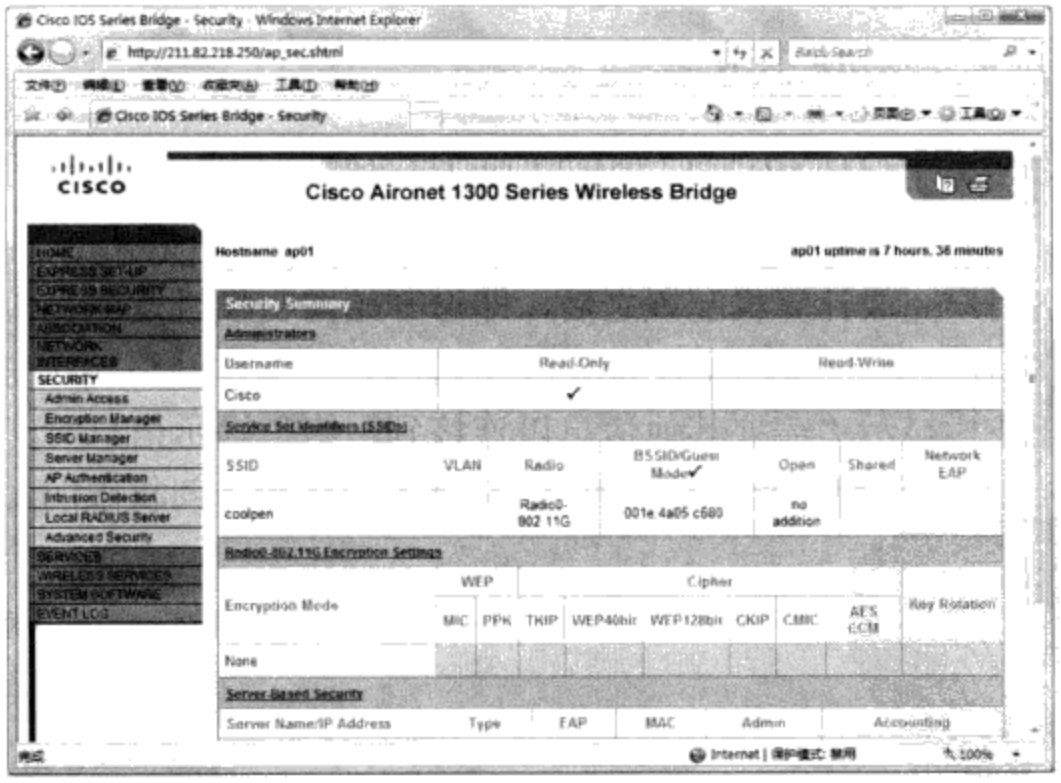


图7-13 当前安全设置

1. 修改admin密码

与其他网络设备一样，无线AP也提供了初始的管理员用户名和密码，通常情况下，Cisco产品的默认账户和密码均为“Cisco”，其他品牌产品的账户通常为“admin”，密码为空或者

“admin”。由此可见，同一厂商，甚至不同厂商的管理用户名和密码是完全一致的。如果不更改默认的账户和密码，恶意用户便有机可乘。只需通过简单的扫描工具，就能很容易找出这些设备的地址，并尝试用默认的用户名和密码去登录管理页面，如果成功则立即取得该无线网络的控制权。如图 7-14 所示是连接到 Cisco Aironet 1300 无线网桥时的登录对话框。

由于掌握了无线 AP 的管理密码即可访问设备甚至修改其配置，建议修改管理员账户名称，并设置高强度的安全密码。在安全设置窗口中，单击“Admin Access”显示如图 7-15 所示“Security: Admin Access”窗口，在 Default Authentication 选项区域设置新的密码即可。如果当前 AP 需要接受多管理员的管理，则可以在 Local User List 选项区域，创建多个用户账户，对于普通用户仅赋予其“Read-Only”权限即可，超级管理员则可以赋予“Read-Write”权限。

图 7-14 登录到无线 AP

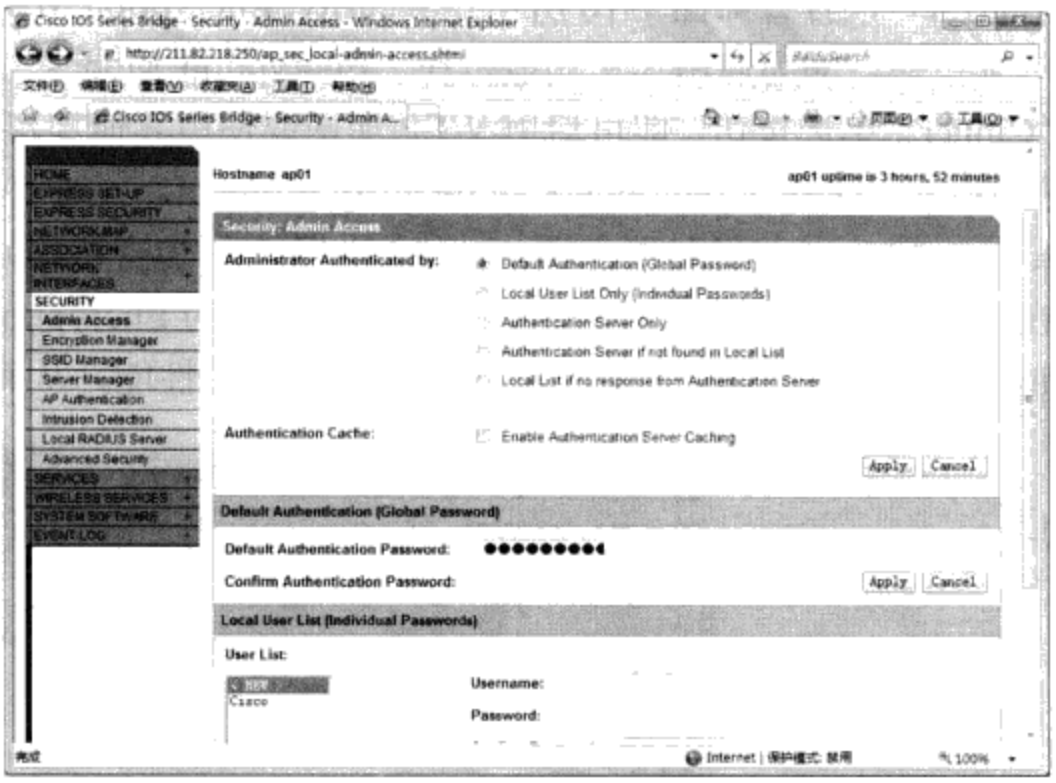


图 7-15 “Security: Admin Access”窗口

2. WEP 加密传输

IEEE 802.11 的安全性选项包括以 WEP 算法为基础的身份验证服务和加密服务。WEP 是一套安全服务，用来防止 IEEE 802.11 网络受到未授权用户的访问，例如偷听（捕获无线网络通信）等。利用自动无线网络配置，可以指定进入网络时用于身份验证的网络密钥。也可以指定使用哪个网络密码来对通过该网络传输的数据进行加密。启用数据加密时，生成秘密的共享加密密钥，并由源台和目标台用来改变帧位，因而避免泄露给偷听者。

（1） 开放式系统和共享密钥身份验证

IEEE 802.11 支持两个子类型的网络身份验证服务，即开放式系统和共享密钥。在“开放式身份验证”下，任何无线站都可请求身份验证。需要通过一个身份验证的无线站将包含发送站的身份验证管理帧发送出去。接收站然后将表明其是否识别发送站的身份的帧发送回去。在“共享密钥”身份验证下，每个无线站都被假定为具有安全频道的秘密共享密钥，该安全频道独立于 IEEE 802.11 无线网络通信频道。要使用“共享密钥”身份验证，必须具有一个网络密钥。

（2） 网络密钥

启用 WEP 时，用户可以指定用于加密的网络密钥。可为用户自动提供网络密钥（例如，

可能会提供在无线网络适配器上），用户也可以通过输入方式来亲自指定密钥。如果用户亲自指定密钥，还可以指定密钥长度（40 位或 104 位）、密钥格式（ASCII 字符或十六进制数据）和密钥索引（存储特定密钥的位置）。密钥长度越长，密钥越安全。密钥长度每增加一位，可能的密钥数量就会增加一倍。

在 IEEE 802.11 下，可用多达 4 个密钥（密钥索引值为 0、1、2 和 3）配置无线站。当访问点或无线站利用存储在特定密钥索引中的密钥传送加密邮件时，传送的邮件指明用来对邮件正文加密的密钥索引。然后接收访问点或无线站可以检索存储在密钥索引处的密码并使用它来对加密邮件正文进行解码。

以 Cisco Aironet 1300 无线网桥为例，在安全配置窗口中，单击导航栏中的“Encryption Manager”，打开如图 7-16 所示“Security: Encryption Manager”窗口。系统默认选择“None”单选按钮，即为启用加密功能。在“Encryption Modes”选项区域选择“WEP Encryption”或“Cipher”单选按钮，即可启用 WEP 加密或使用其他加密方法。Cisco Aironet 1300 无线网桥支持 WEP、TKIP（Temporal Key Integrity Protocol，暂时密钥集成协议）、CMIC（Cisco Message Integrity Check，思科消息完整性检测）等多种加密协议，或者多种协议配合使用加强安全性。在 Encryption Keys 选项区域，分别设置相应的 Encryption Key 值即可。需要注意的是，密钥越长，加密效果越好，但同时也将占用更多的性能，从而导致无线传输速率下降。

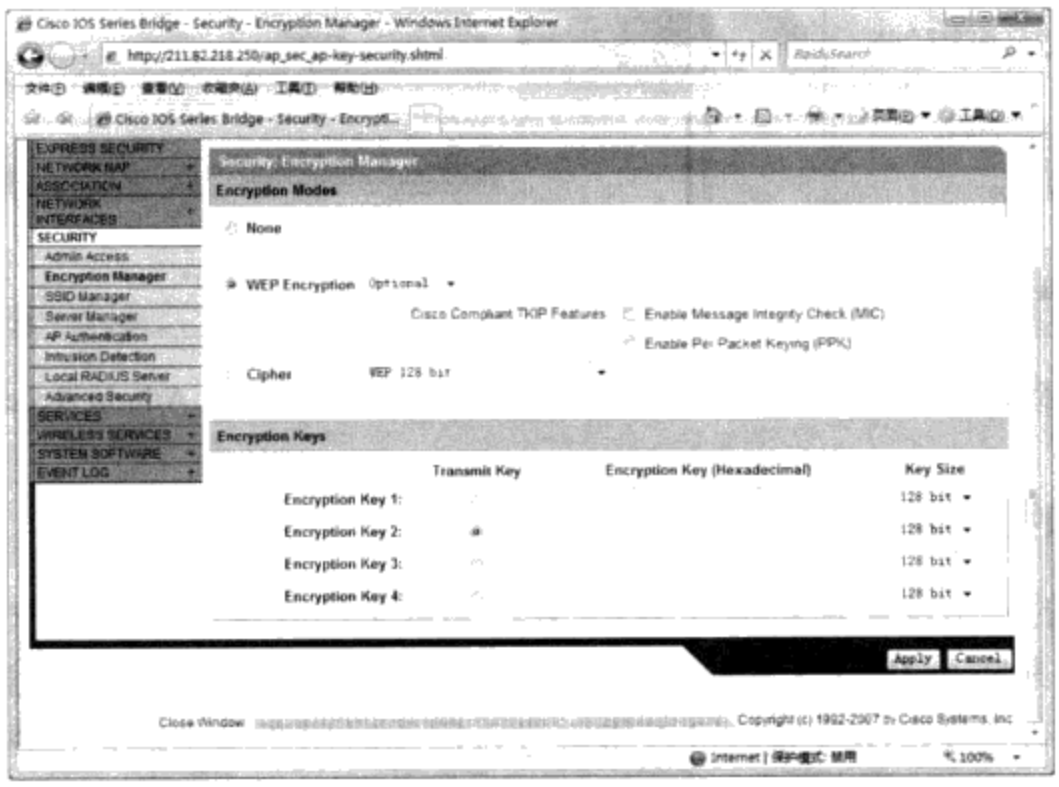


图 7-16 启用 WEP 加密

3. 修改 SSID 标识

默认状态下，无线 AP 生产商会利用 SSID（初始化字符串），来检验企图登录无线网络节点的连接请求，一旦检验通过，即可顺利连接到无线网络。由于同一厂商的产品都使用相同的 SSID 名称，从而给恶意攻击者提供了入侵的条件。一旦他们使用通用的初始化字符串来连接无线网络时，就很容易建成一条非授权链接，从而给无线网络的安全带来威胁。因此，必须修改默认的 SSID 初始化字符串，提高设备安全性。

第 1 步，在安全配置窗口中，单击左侧导航栏中的“SSID Manager”，打开如图 7-17 所示“Security: Global SSID Manager”窗口，在“SSID Properties”选项区域，选择“NEW”并在

左侧设置新的 SSID 即可。

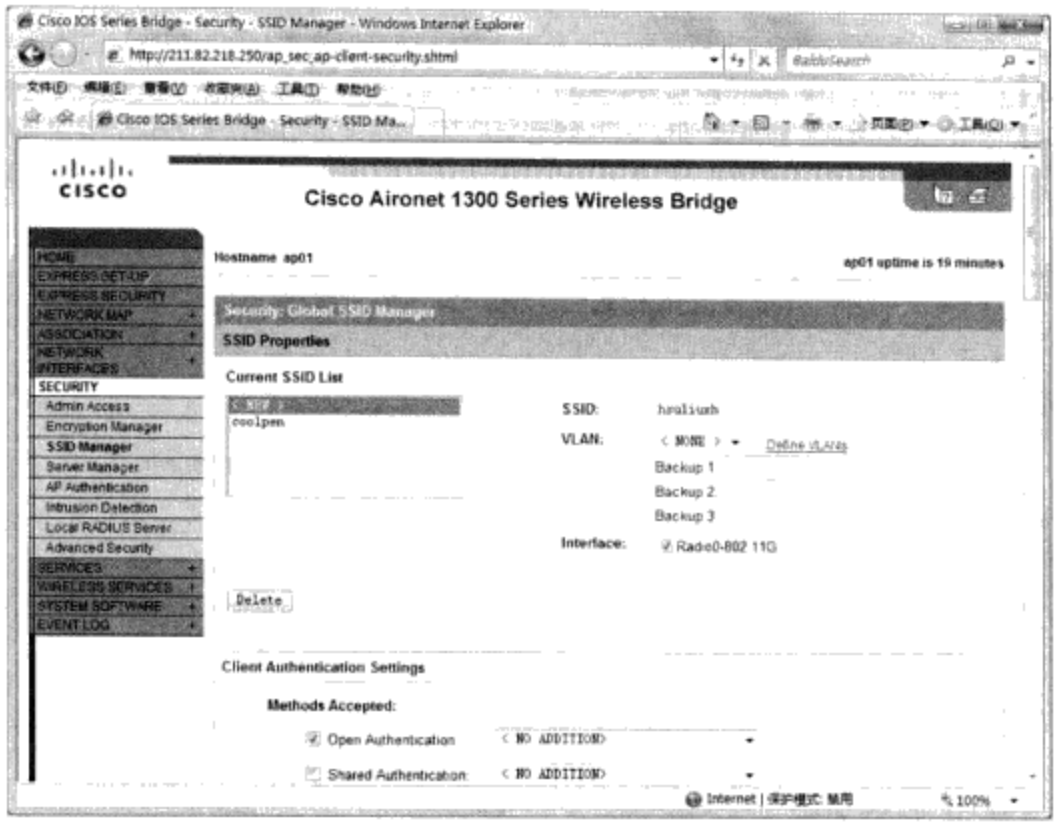


图 7-17 “Security: Global SSID Manager”窗口

第 2 步，在如图 7-18 所示“Client Authentication Settings”选项区域，可以设置客户端身份验证方法，首先选择希望使用的验证方法，选择“Open Authentication”复选框，并在后面的下拉列表框中选择具体验证方式即可，包括 MAC 地址、EAP 加密等。然后，在“Server Priorities（服务器优先级）”选项区域，选择所设置不同验证方式的执行顺序（必须同时使用多种验证方式才可设置），通常情况下都是使用默认设置。

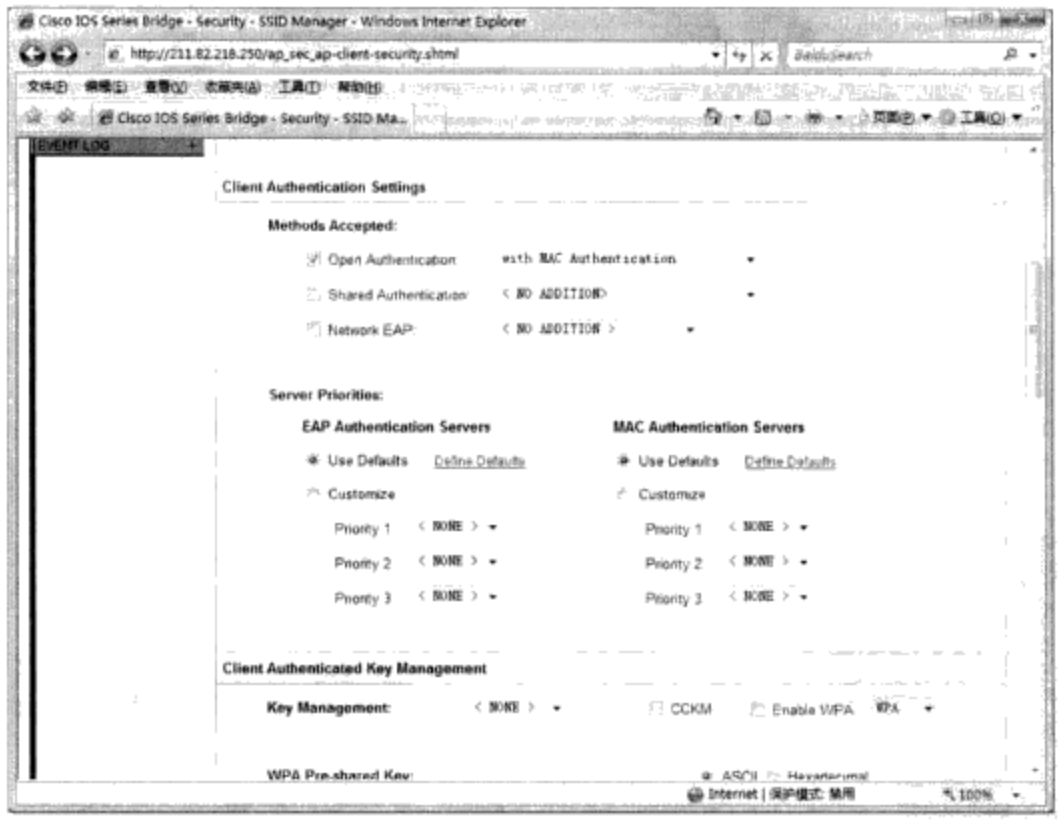


图 7-18 设置客户端验证方式

第 3 步，在如图 7-19 所示“Client Authenticated Key Management”选项区域，可以设置客户端验证密钥的管理方式，包括 mandatory（强制执行）和 optional（任意选择）两种方式，如果选择“Enable WPA”复选框启用“WPA”加密功能，则还必须设置相应的加密密码。

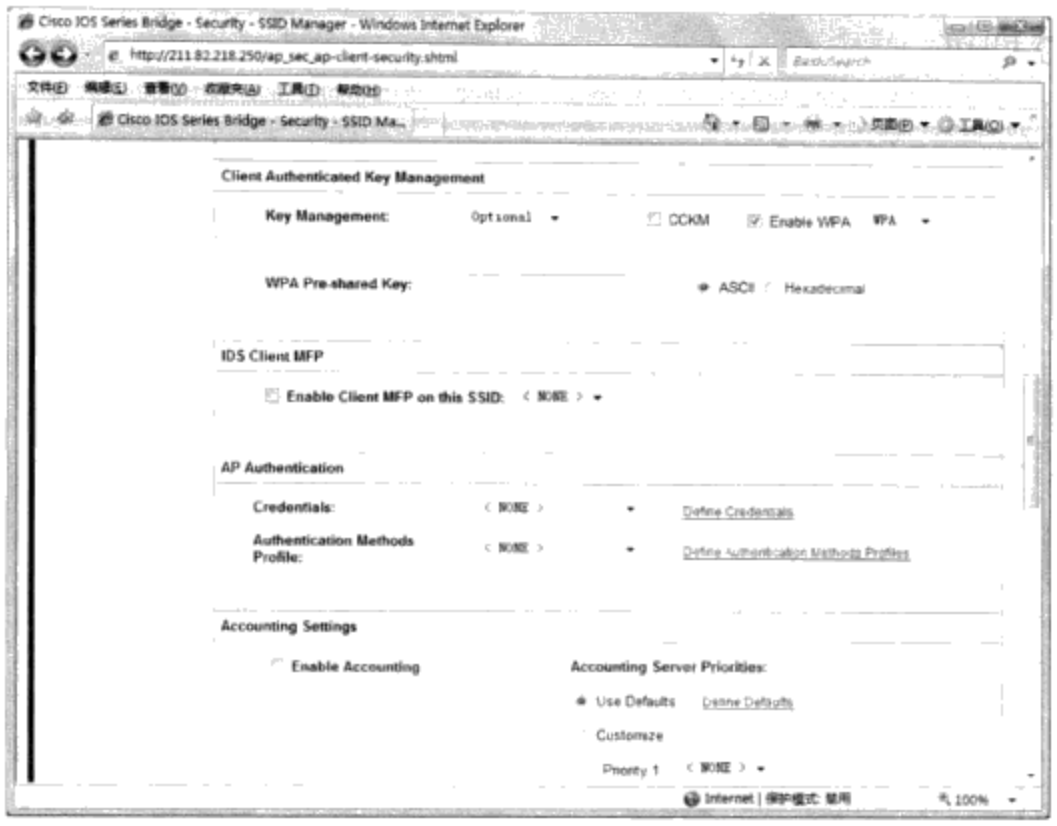


图 7-19　设置客户端验证密钥管理方式及其他

第 4 步，在如图 7-20 所示“Multiple BSSID Beacon Settings”选项区域，切忌不要选中“Set SSID as Guest Mode”复选框，所谓的 BSSID 是 SSID 的一种，SSID 是对 BSSID 和 ESSID 的缩写和统称。如果在无线网络只有一个无线路由器或 AP 发射源时，则各个客户端使用统一的 BSSID 名称和 AP 通信；如果在无线网络有多个无线路由器或 AP 发射源并相互通过 WDS（Wireless Distribution System，无线分布式系统）等方式连接时，各个客户端使用统一的 ESSID 信息和 AP 通信。

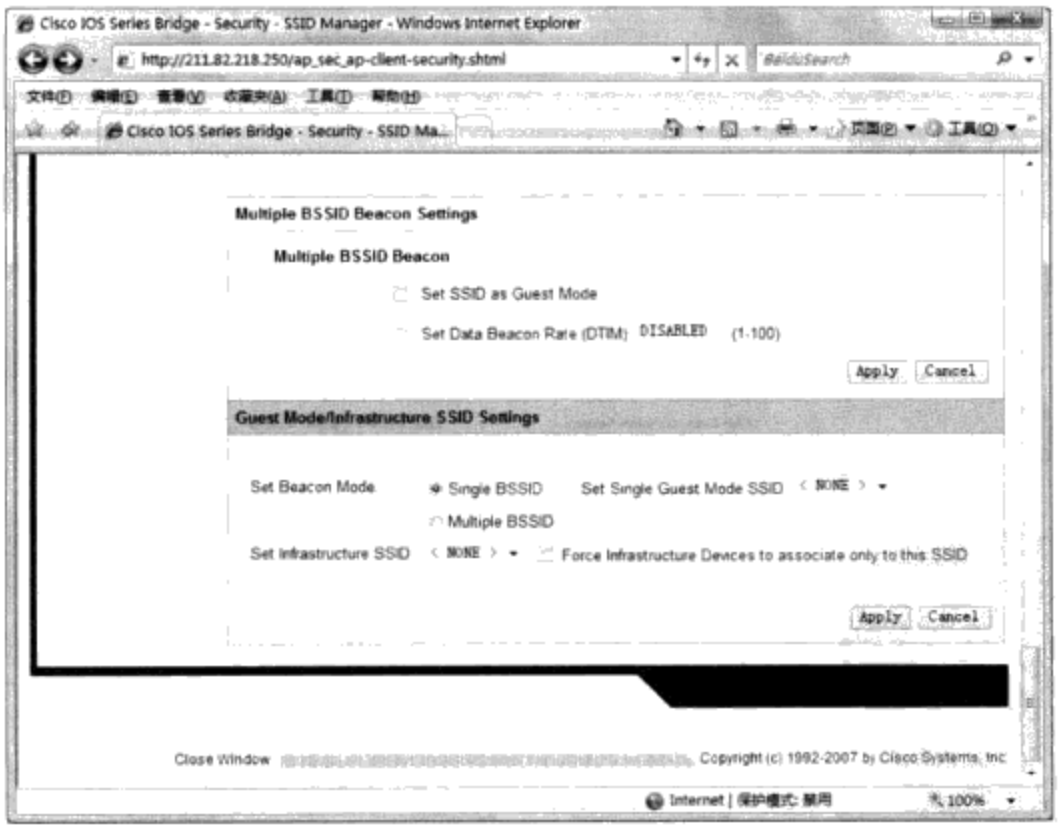


图 7-20　多重 BSSID 设置

第 5 步，在“Guest Mode/Infrastructure SSID Settings”选项区域，选择“Single BSSID”单选按钮即可，选择“Multiple BSSID”单选按钮后，无线客户端可以通过设置自己的 SSID 加入 AP 划分的不同 VLAN 中，可以提高网络安全性，普通用户不推荐配置此功能。

第 6 步，取消无线 AP 的 SSID 广播也是非常重要的，在 Cisco Aironet 1300 无线网桥的 Web 配置窗口中，单击左侧导航栏中的“EXPRESS SECURITY”，显示如图 7-21 所示“Express Security Set-Up”窗口，确认“SSID”文本框后的“Broadcast SSID in Beacon”复选框未被选中，即可阻止无线 AP 在覆盖范围内广播自己的 SSID。

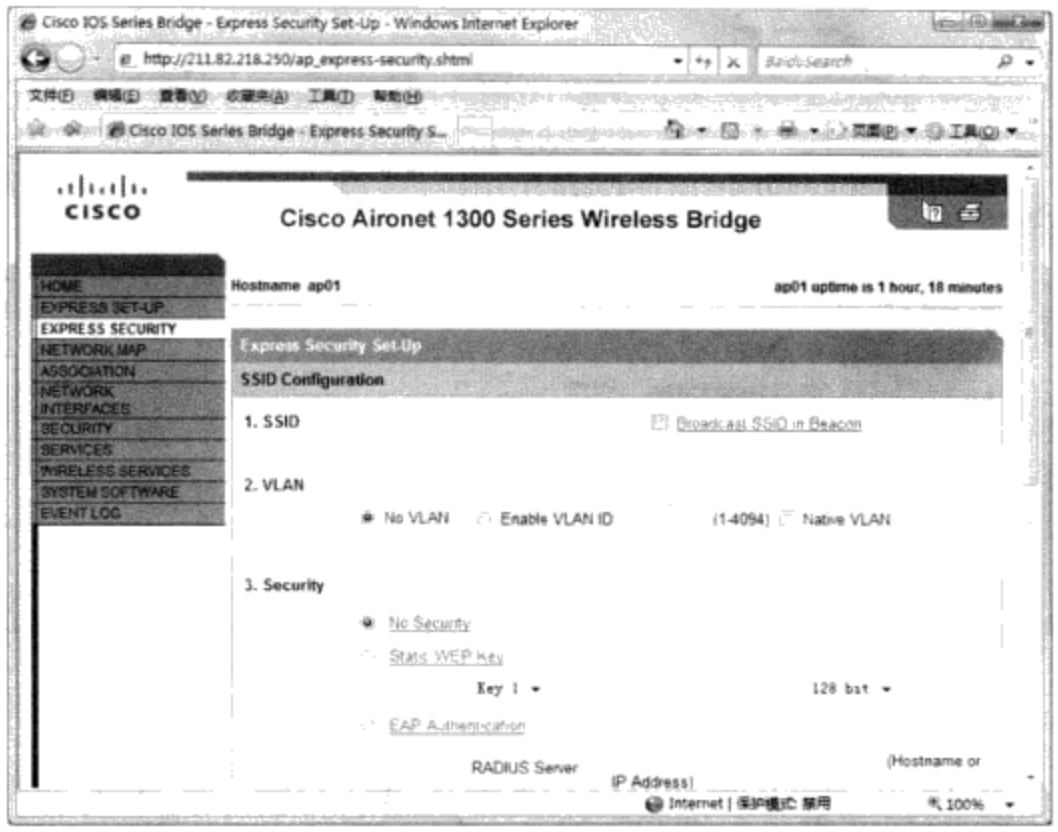


图 7-21 “Express Security Set-Up”窗口

提示 修改无线 AP 的 SSID 后，也必须在工作站的无线网络属性中作相应的设置，从而保持与无线 AP 的一致。在无线漫游网络中，所有无线 AP 的 SSID 必须保持相同。

4. 配置 RADIUS 服务器

RADIUS 身份验证服务器是身份验证中的重要环节，这里主要用来设置 RADIUS 备份服务器，即当主 RADIUS 服务器出现故障时，无线 AP 将自动把客户端请求身份验证的消息发送到指定的备份 RADIUS 服务器上，以确保网络正常运行。

在 Cisco Aironet 1300 无线网桥的安全配置窗口中，单击左侧导航栏中的“Server Manger”，打开如图 7-22 所示“Security: Server Manager”窗口。在“Backup RADIUS Server:”文本框中输入备份 RADIUS 服务器的主机名或 IP 地址，并在“Shared Secret:”文本框中，输入 RADIUS 服务器配置的共享密钥即可。

5. 无线 AP 身份验证

通常情况下，802.1x 身份认证都是网络设备同客户端之间的关系确认，即主要凭借预先为验证服务器指定的合法用户账户，来判断新接入网络的设备或用户是否可以获得相应的访问权限。在 Cisco 无线网络中，无线 AP 之间可以通过创建信任关系，而无需借助用户账户和密码即可快速得到目标网络的访问权限。当被信任的无线 AP 进入目标无线 AP 覆盖范围内时，

将自动被目标无线 AP 赋予相应的接入权限，并被作为当前目标 AP 的一个合法客户端。

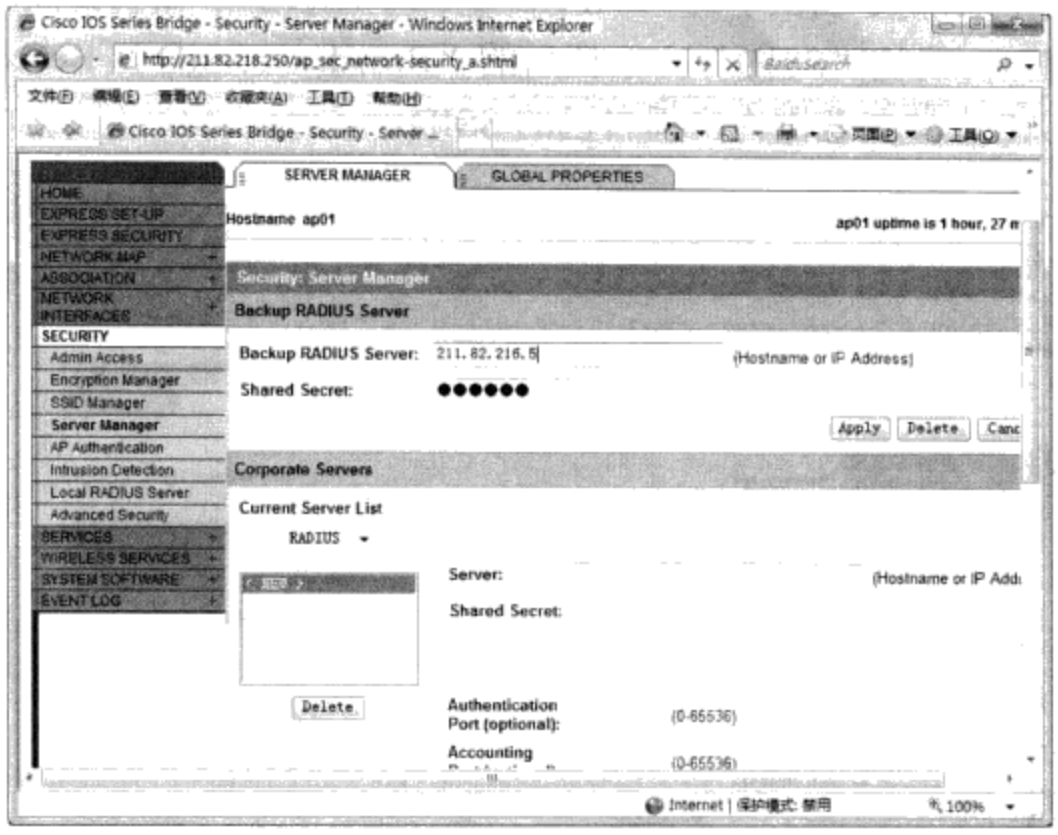


图 7-22 “Security: Server Manager”窗口

在 Cisco Aironet 1300 无线网桥的安全配置窗口中，单击左侧导航栏中的“AP Authentication”，打开如图 7-23 所示“Security: AP Authentication - General setup”窗口。在“Current Credentials”选项区域，选择“NEW”并在右侧输入当前 AP 的验证信息即可。

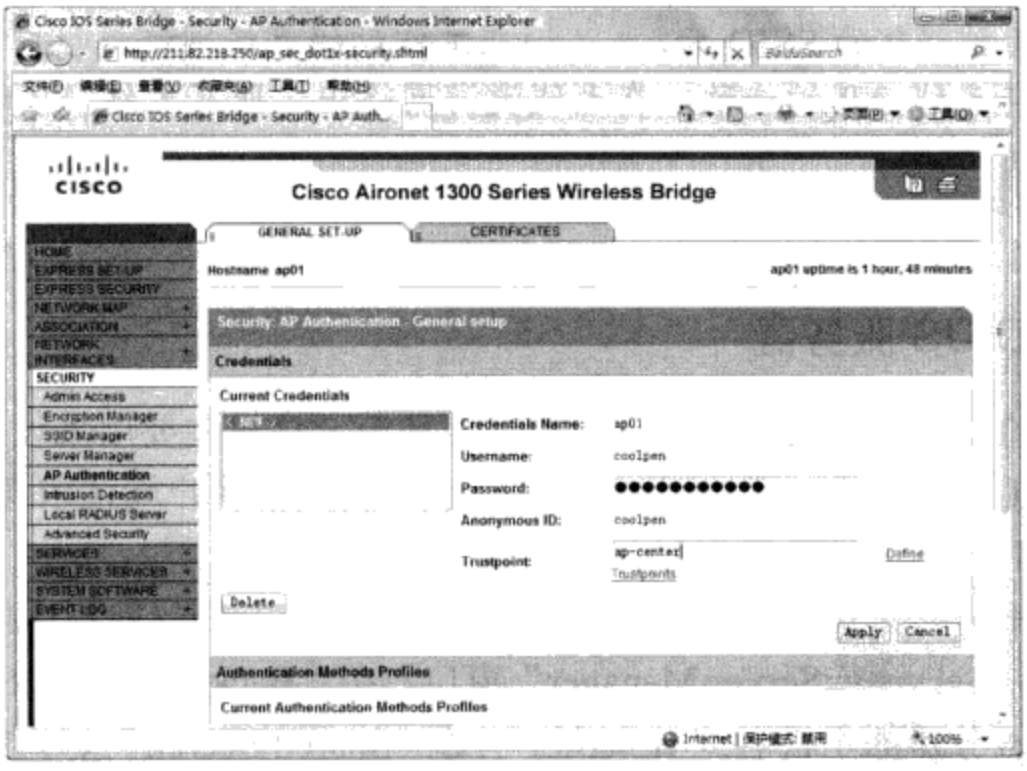


图 7-23 “Security: AP Authentication - General setup”窗口

6. 配置入侵检测功能

有些无线 AP 本身已经集成了简单的入侵检测功能，可以帮助网络管理员保护管理端口，在第一时间识别各种网络入侵。需要注意的是，启用该功能后，可能影响到设备 QoS，因此建议普通用户保持默认设置，即不启用该功能。

在 Cisco Aironet 1300 无线网桥的安全配置窗口中，单击左侧导航栏中的“Intrusion Detection”，打开如图 7-24 所示“Intrusion Detection: Management Frame Protection”窗口。如果选中“Transmit MFP Frames”复选框，则该 AP 向外发送信息时将自动对信息完整性进行保护和验证，同时要求接收端必须是当前 WDS 中的成员，否则将无法成功阅读消息。如果选中“Detect MFP Frames”复选框，则无线 AP 将对每一个传入连接进行验证，确保消息的完整性和有效性，抵御外来侵袭。

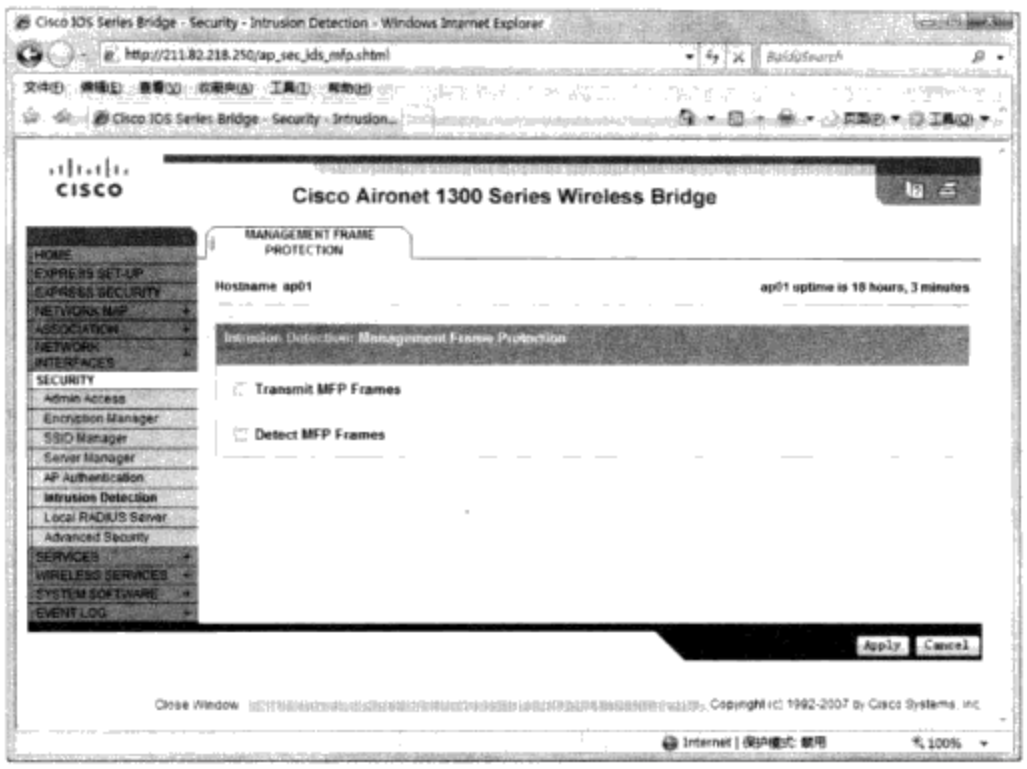


图 7-24 “Intrusion Detection: Management Frame Protection”窗口

7. 配置本地 RADIUS 服务器

本身集成 RADIUS 服务功能的无线 AP，则可以通过启用该功能，用于验证客户端或接入设备的可靠性，同时选择网络中的其他 RADIUS 服务器作为备份 RADIUS，确保身份验证的可用性。

在 Cisco Aironet 1300 无线网桥的安全配置窗口中，单击左侧导航栏中的“Local RADIUS Server”，打开如图 7-25 所示“Security: Local RADIUS Server - Statistics”窗口。这里只显示当前 AP 本地 RADIUS 服务器的配置情况，管理员可以在“GENERAL SET-UP”和“EAP-FAST SET-UP”选项卡中，设置具体的验证方式和密钥。

8. 高级安全设置

管理员可以通过高级安全设置，配置无线 AP 基于 MAC 地址验证客户端身份，类似于 Cisco 交换机中的基于 MAC 地址的 ACL。需要注意的是，如果在无线 AP 的 SSID Manager 中配置中设置了 EAP Client 的用户账户名和密码，则客户端访问该 AP 时，首先要通过 MAC 地址的验证，通过后才可继续进行 EAP 身份验证。

在 Cisco Aironet 1300 无线网桥的安全配置窗口中，单击左侧导航栏中的“Advanced Security”，打开如图 7-26 所示“Security: Advanced Security- MAC Address Authentication”窗口。在该选项卡中，管理员可以配置无线 AP 的 MAC 地址验证方式以及更改 MAC 地址列表。在“TIMERS”和“ASSOCIATION ACCESS LIST”选项卡中，可以对客户端连接空闲超时和

客户端 MAC 地址过滤功能进行设置。

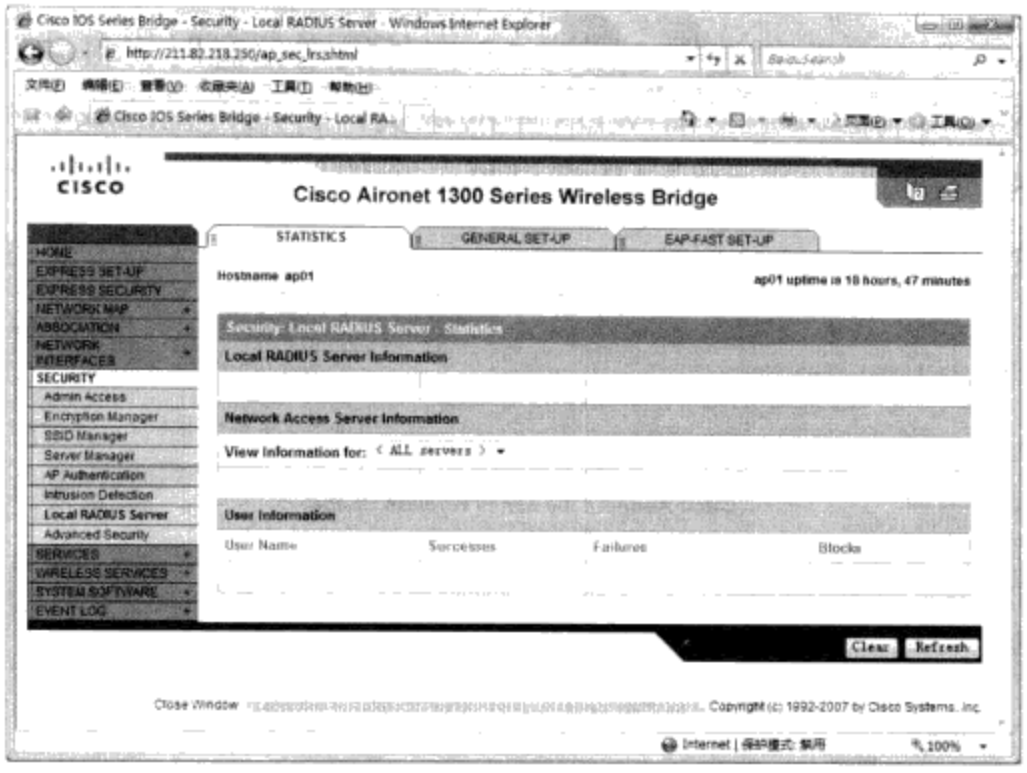


图 7-25 “Security: Local RADIUS Server - Statistics”窗口

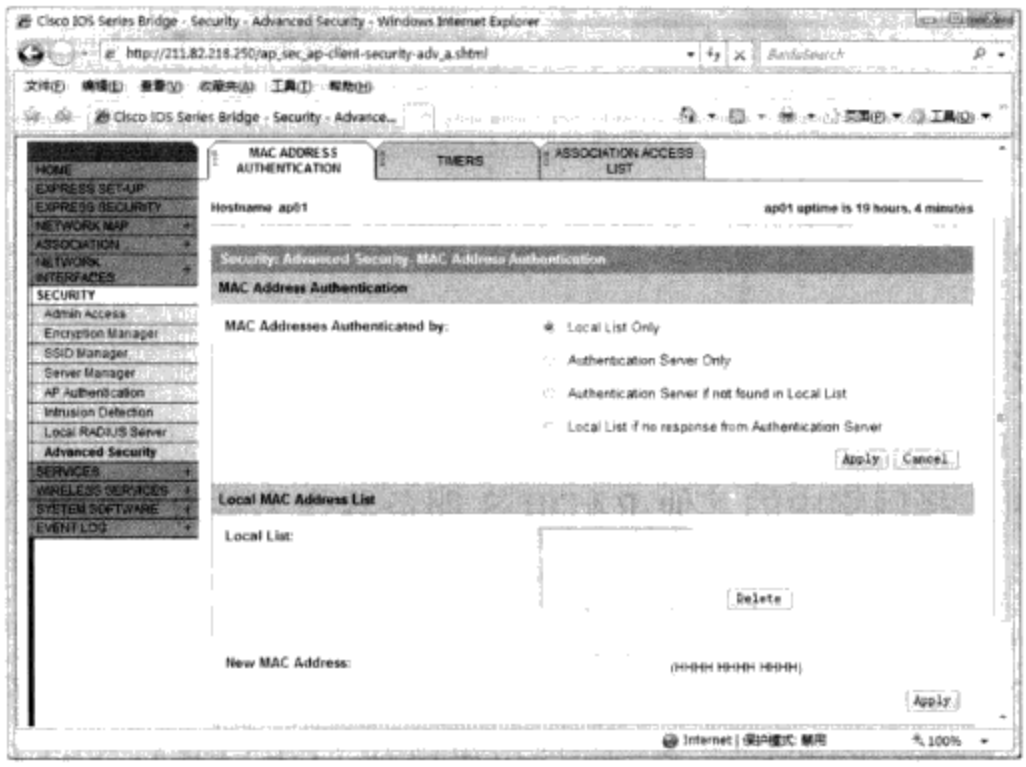


图 7-26 “Security: Advanced Security- MAC Address Authentication”窗口

9. 禁用多余服务

无线 AP 除提供基本的无线桥接功能外，还提供了多种附加服务功能。这些服务虽然可以满足不同用户的简单网络需求，但可能会对无线 AP 的安全带来严重威胁。在 Cisco Aironet 1300 无线网桥的管理窗口中，单击左侧导航栏中的“SERVICES”，打开如图 7-27 所示“Services Summary”窗口，显示当前无线 AP 提供的所有网络服务及运行情况。

单击服务的超级链接，即可打开相关的配置窗口，例如单击“DNS”超级链接，显示如图 7-28 所示“Services: DNS - Domain Name Service”窗口，选择“Disable”单选按钮即可将禁用该服务。

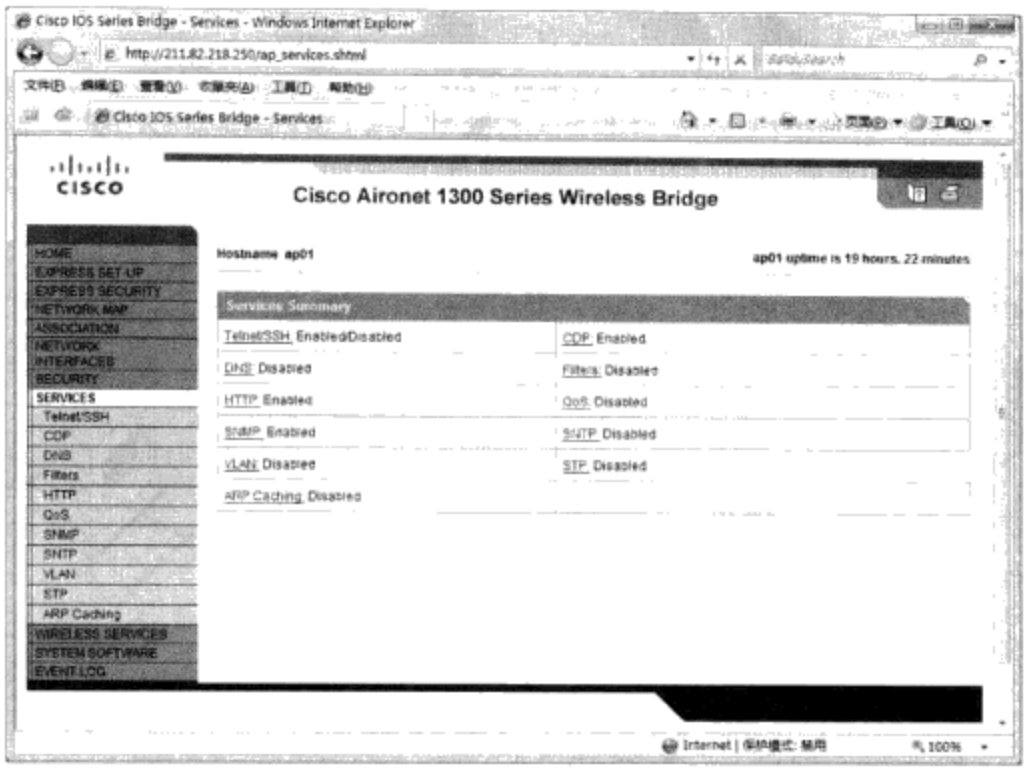


图 7-27 “Services Summary”窗口

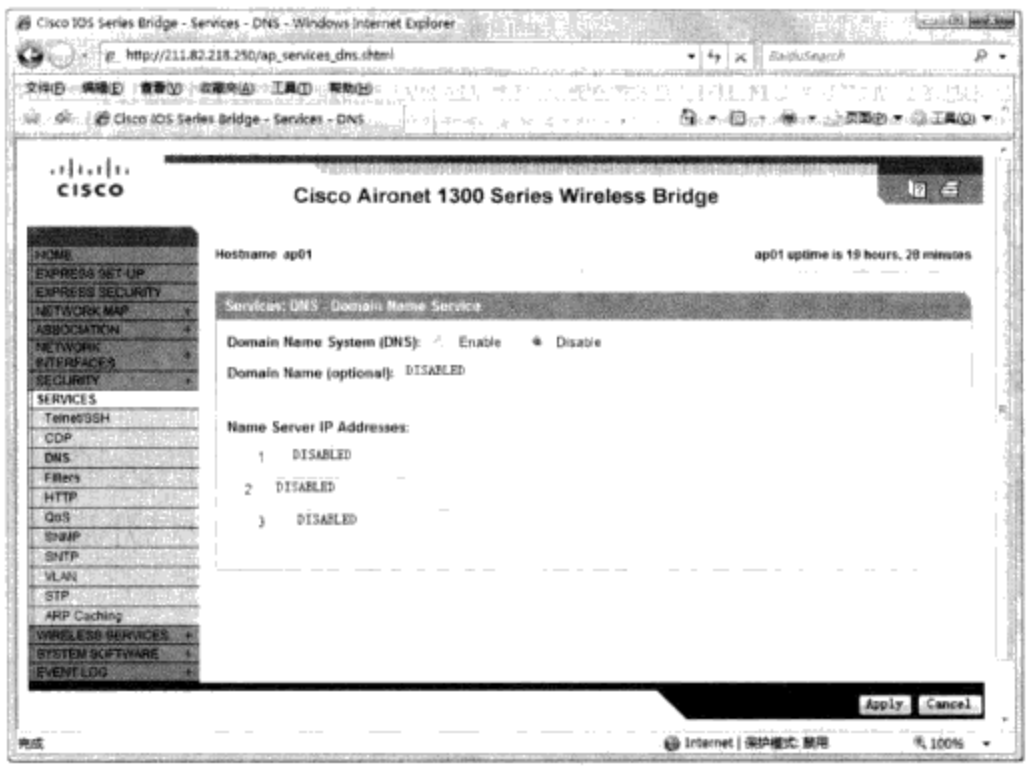


图 7-28 “Services: DNS - Domain Name Service”窗口

10. 合理放置无线 AP 和天线

由于无线 AP 是有线信号和无线信号的转换“枢纽”，无线 AP 以及无线的类型和位置，不但决定无线局域网的信号传输速度和通信信号强弱，而且还能影响无线网络的通信安全。因此，将无线 AP 摆放在一个合适的位置是非常有必要的。另外，在放置天线之前，一定要先搞清楚无线信号的覆盖范围有多大。然后，依据范围大小，将天线放置到其他用户无法“触及”的位置处。

例如，最好将无线网络节点放置在该空间的正中央（如图 7-29 所示），同时将其他工作站分散在无线网络节点的四周放置，使其他房间的工作站无法自动搜索到无线网络，也就不容易出现信号泄密的危险。倘若随便将无线网络节点放置在靠窗口或墙壁的位置处，不但会影响信号的对外发射，而且位于墙壁另一边的工作站用户，就能很轻易地搜索并连接，网络安全性就

会大大降低。

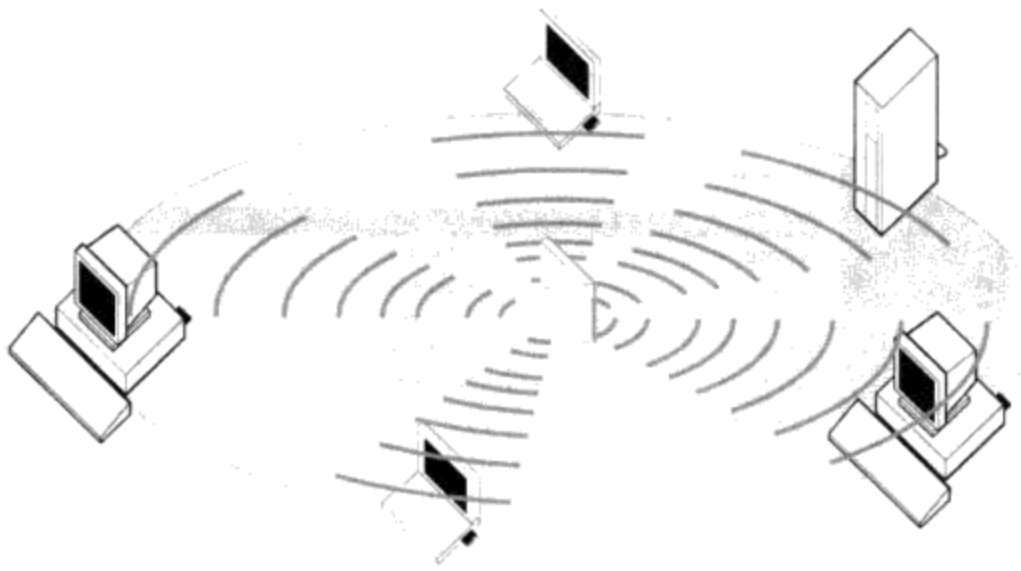


图 7-29 无线 AP 位置

7.3.2 无线路由器安全

无线路由器除了拥有无线 AP 的功能外，还集成了宽带路由器的功能，因此，可以实现小型网络的 Internet 连接共享。当然，由于无线路由器位于网络的边缘，承受着更多的安全威胁，因此，除了可以采用无线 AP 的安全策略外，还可以采用更多的安全策略，包括防火墙、IP 地址过滤、MAC 地址过滤等。

1. 防火墙设置

在 TP-LINK 主页中，单击“安全设置”超级链接，显示“防火墙设置”窗口，如图 7-30 所示。默认没有启用防火墙功能。如果要开启防火墙，只需选中“开启防火墙（防火墙的总开关）”复选框，并单击“保存”按钮即可。

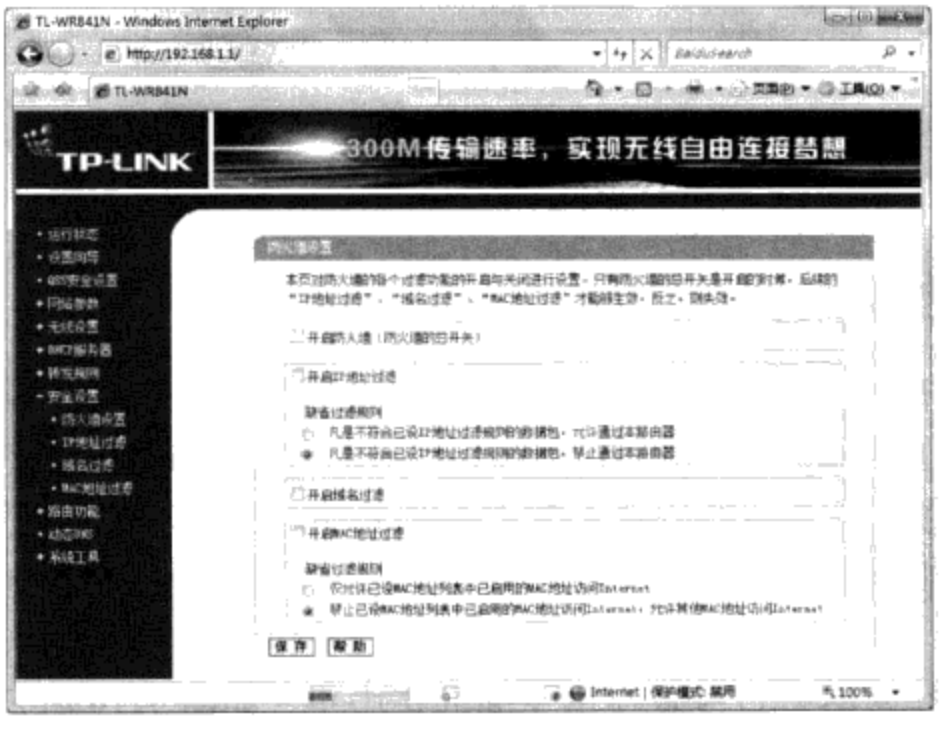


图 7-30 “防火墙设置”窗口

其中，IP 地址用来控制局域网内的计算机对广域网中特定 IP 地址及端口的访问；域名过

滤用来控制局域网计算机对 Internet 中特定网站的访问；MAC 地址过滤则用来控制局域网计算机对 Internet 的访问。要想启用相应的功能，必须选中相应的复选框。同时，也必须先开启防火墙。

2. IP 地址过滤

第 1 步，在“防火墙设置”窗口中，同时选中“开启防火墙”和“开启 IP 地址过滤”复选框，并在“默认过滤规则”选项区域中选择一种过滤规则（如图 7-31 所示）。

- 凡是不符合已设 IP 地址过滤规则的数据包，允许通过本路由器：也就是说，凡是符合规则列表中设置的 IP 地址规则，都不能通过该路由器，类似于防火墙的“黑名单”功能。
- 凡是不符合已设 IP 地址过滤规则的数据包，禁止通过本路由器：也就是说，只有符合规则列表中设置的 IP 地址规则，才能够通过该路由器，类似于防火墙的白名单功能。

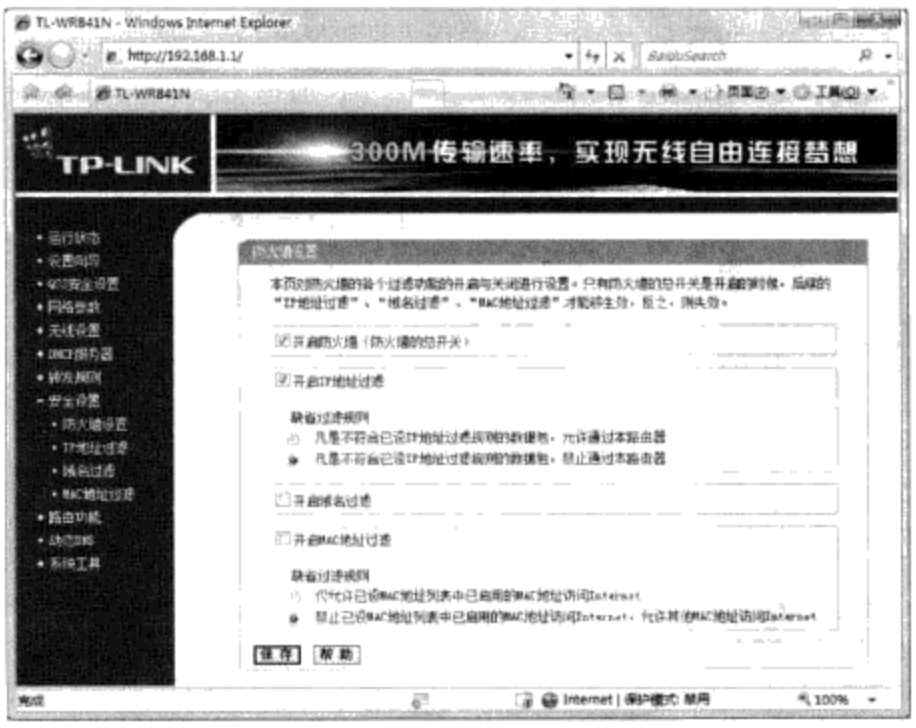


图 7-31　开启 IP 地址过滤

第 2 步，单击“IP 地址过滤”超级链接，显示如图 7-32 所示“IP 地址过滤”窗口，可以添加过滤规则。

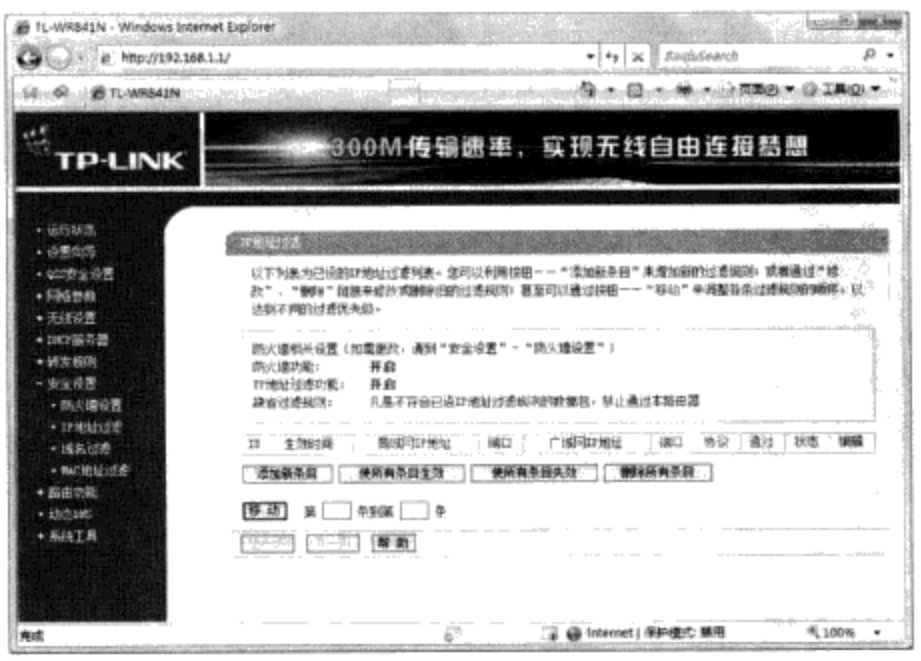


图 7-32　“IP 地址过滤”窗口

第3步，单击“添加新条目”按钮，显示如图7-33所示窗口，设置如下选项：

- 生效时间：设置该规则的有效时间范围，默认为从00:00到24:00。
- 局域网IP地址：局域网中被控制的计算机IP地址，可以是一个或一段IP地址。为空则表示控制局域网中所有的计算机。
- 局域网端口：局域网中被控制的计算机的服务端口，可以是一个或一段端口。为空表示控制该计算机的所有端口。
- 广域网IP地址：广域网中被控制的网站的IP地址，可以是一个或一段IP地址。为空表示控制整个广域网。
- 广域网端口：广域网中被控制的网站的服务端口，为空表示控制该网站所有端口。
- 协议：被控制的计算机所使用的协议，选择“ALL”则表示控制所有协议。
- 通过：选择“允许通过”选项，则符合该规则的数据都被允许通过，选择“禁止通过”选项则禁止符合规则的数据包通过。
- 状态：选择该规则是否生效。

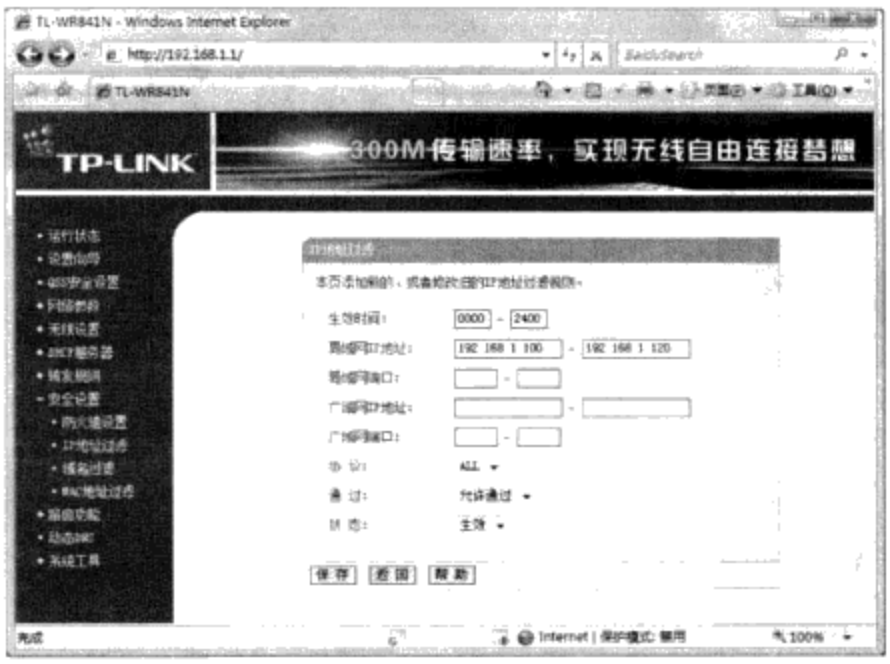


图7-33 添加过滤规则

第4步，单击“保存”按钮，一条新规则添加完成。按照同样操作步骤，可添加多条规则，如图7-34所示。

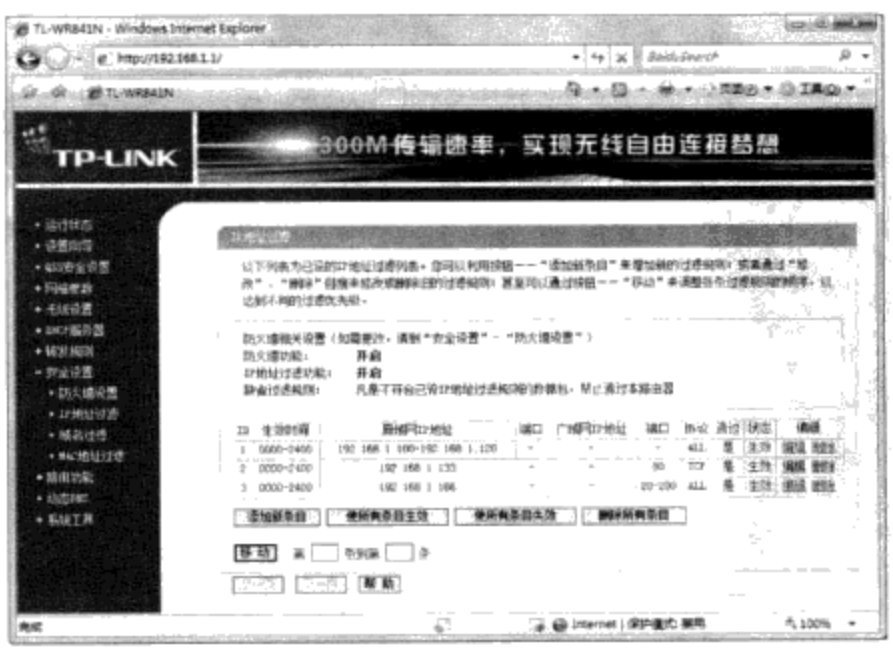


图7-34 已添加的规则

3. MAC 地址过滤

第 1 步，在“防火墙设置”窗口中，同时选中“开启防火墙”和“开启 MAC 地址过滤”复选框（如图 7-35 所示），并选择默认过滤规则。

- 仅允许已设 MAC 地址列表中已启用的 MAC 地址访问 Internet。只有添加到 MAC 地址列表中且已生效的地址，才能访问 Internet，未添加到列表中计算机不能访问。
- 禁止已设 MAC 地址列表中已启用的 MAC 地址访问 Internet，允许其他 MAC 地址访问 Internet。凡是添加到 MAC 地址列表中且已生效的地址将不能访问 Internet，只有未添加到 MAC 地址列表中的计算机才允许访问。

图 7-35　开启 MAC 地址过滤

第 2 步，单击“保存”按钮保存设置。然后，单击“MAC 地址过滤”超级链接，显示如图 7-36 所示“MAC 地址过滤”窗口。

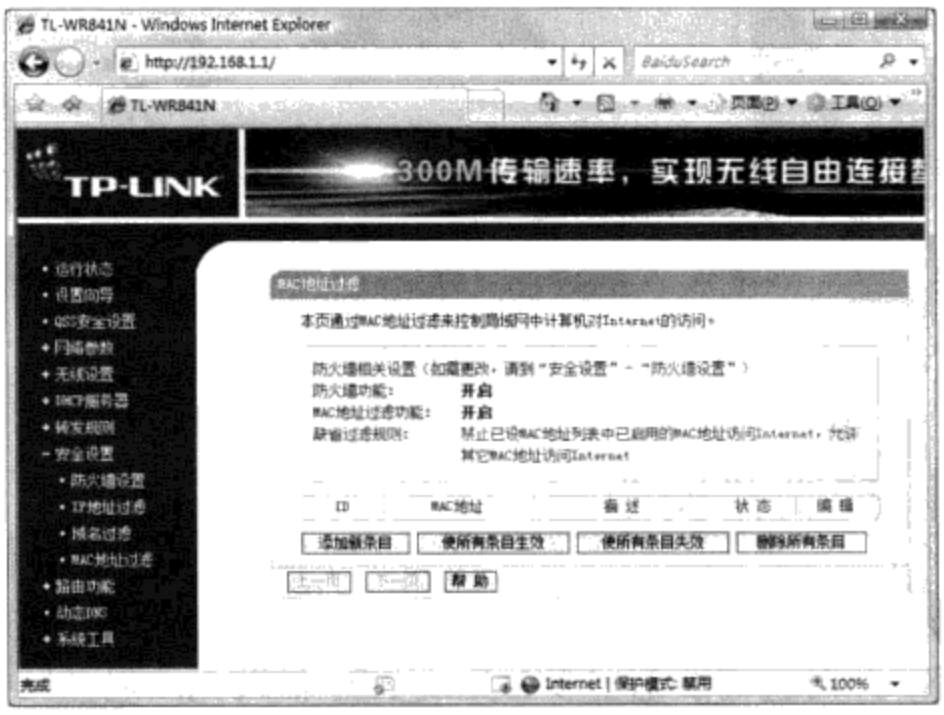


图 7-36　“MAC 地址过滤”窗口

第 3 步，单击“添加新条目”按钮，显示如图 7-37 所示窗口，在“MAC 地址”文本框中，

键入计算机的 MAC 地址，“描述”文本框中键入该计算机的描述信息，“状态”下拉列表框中选择是否生效。

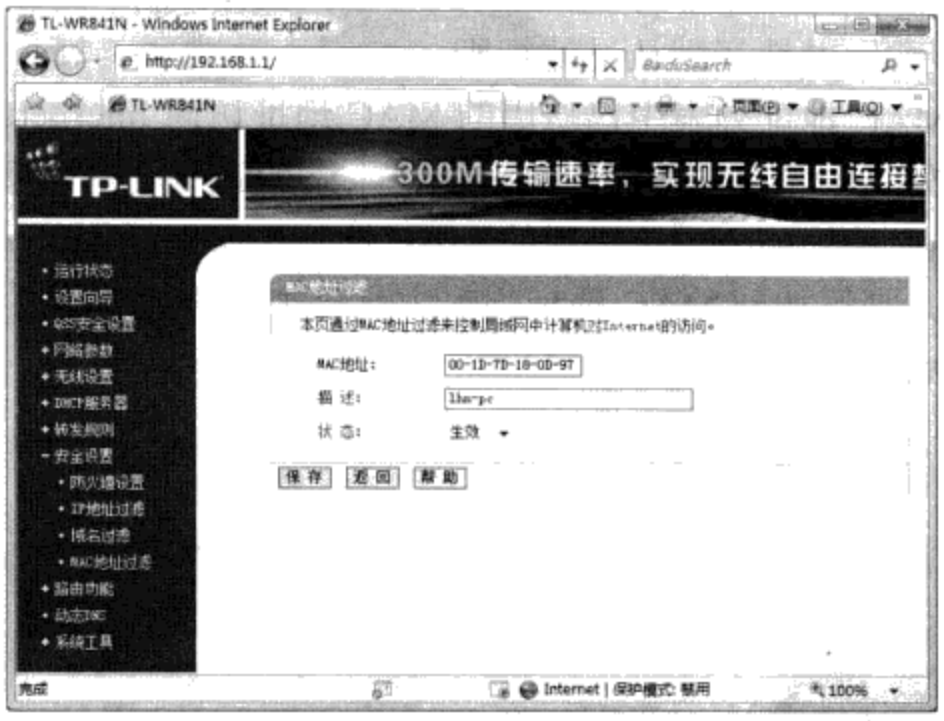


图 7-37　添加 MAC 地址过滤规则

第 4 步，单击“保存”按钮，一条新规则添加完成。按照同样操作步骤，可添加多条规则，如图 7-38 所示。

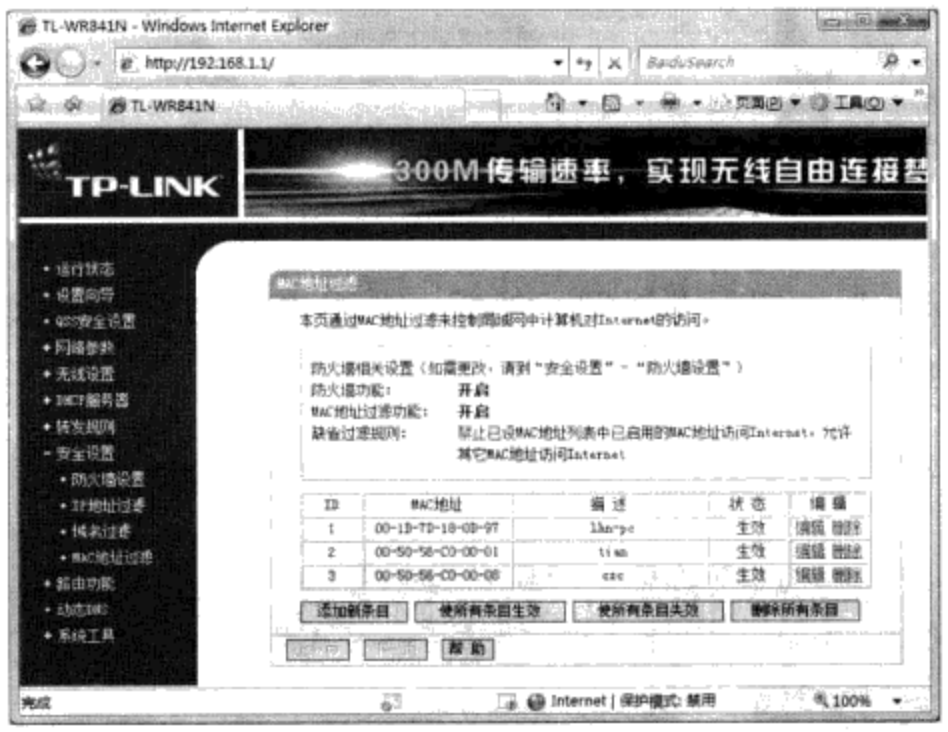


图 7-38　已添加的规则

7.3.3 无线局域网控制器安全

无线局域网控制器主要用于部署和管理网络中的无线 AP。在规模较大的企业网络中，往往会部署无线漫游网络，此时就需要部署多台无线 AP，借助无线局域网控制器进行统一配置、管理和监控，无疑可以实现省时、省力且高效率的目的。Cisco 的无线局域网控制器默认可作为独立无线入侵防御系统部署，管理员也可以为其添加无线局域网数据服务，以便可以环绕其 RF（Radio Frequency，电磁频率）域创建一个“防御屏障”， 抑制未授权无线活动，直到做

好部署无线局域网服务的准备为止。

1. 安全技术概述

Cisco 通过提供以下多个保护层来实现无线局域网安全。

- RF 安全。检测和避免 802.11 干扰。
- 无线局域网入侵防御和定位。Cisco 无线局域网系统不仅可发现恶意设备或潜在的无线威胁，而且能对这些设备定位。使系统管理员能快速评估威胁级别，立即按需采取措施来抵御威胁。
- 基于身份的联网。网络管理员必须在保护无线局域网的同时，支持大量不同的用户访问权限、设备格式和应用要求。Cisco 无线局域网系统使企业可为无线用户或用户组提供不同的安全策略。其中包括：
  - 第二层安全功能。IEEE 802.1x （PEAP，LEAP，TTLS）、WPA、IEEE 802.11i（WPA2）和 L2TP。
  - 第三层（和更高层次）的安全功能。IPSec、Web 验证。
  - VLAN 分配。
  - 访问控制列表（ACL）。IP 限制，协议类型，端口和差分服务代码点(DSCP)数值。
  - QoS。多个服务级别，带宽减少，流量整形和 RF 利用。
  - 验证、授权和记账（AAA）/RADIUS。用户连接策略和权限管理。
- 网络准入控制（NAC）。实施客户端配置和行为策略，以确保只有拥有适当安全工具的终端用户设备才能访问网络。
- 安全移动。在移动环境中保持最高安全水平。包括随用户移动而移动的 VPN，无需重新建立安全隧道。此外，Cisco 已开发了主动密钥缓存（PKC），这是 802.11i 标准的扩展、802.11r 标准的前身，可通过 AES 加密和 RADIUS 验证实现安全漫游。
- 访客隧道。为访客接入公司网络提供更高安全性。可确保访客如果不能通过公司防火墙，则无法接入公司网络。

2. 配置 WPA

第 1 步，依次单击“Wireless”→“WLANs”，显示“WLANs”界面。单击欲配置的无线网络，显示 “WLANs→Edit”界面。

第 2 步，依次单击“Security”和“Layer 2”标签如图 7-39 所示，在“Layer 2 Security”下拉列表框中选择“WPA+WPA2”。选中“WPA Policy”复选框启用 WPA1，选中“WPA2 Policy”复选框启用 WPA2，同时选中时则启用 WPA1 和 WPA2。

> **提示** 在“Layer 2 Security”下拉列表框中选择“CKIP”，则可以启用并设置 CKIP 加密。

第 3 步，选中“AES”或/和“TKIP”复选框，将为“WPA1”和“WPA2”启用“AES”或/和“TKIP”数据加密。

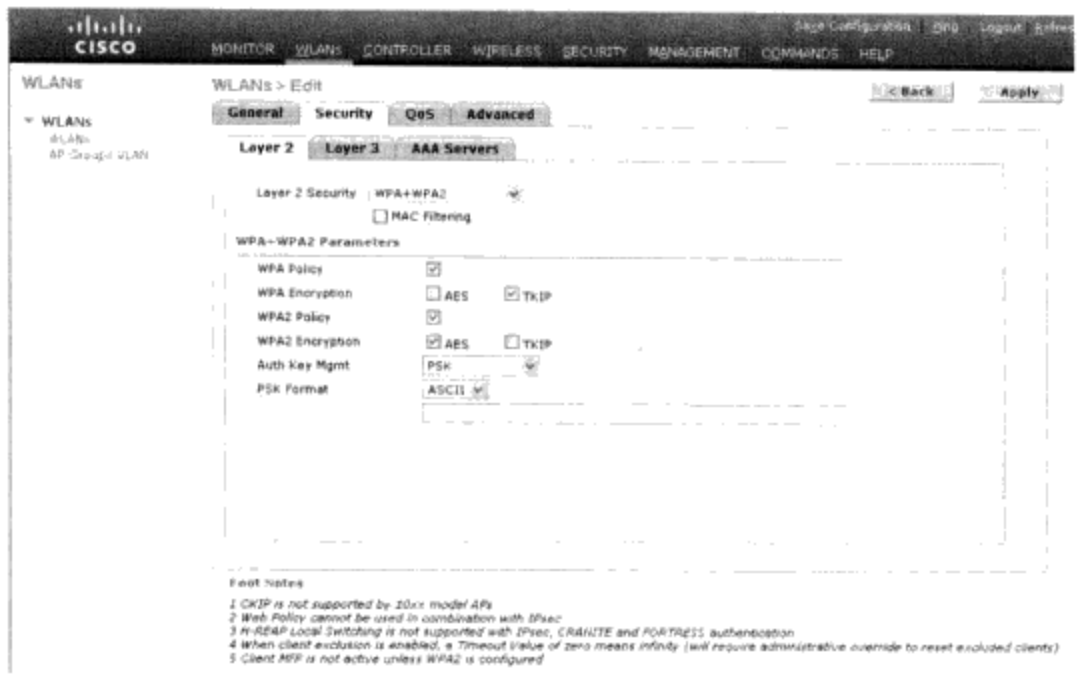


图 7-39 “Layer 2”标签

在“Auth Key Mgmt”下拉列表框中选择密钥管理方法，包括“802.1X”、“CCKM”、“PSK”和“802.1X+CCKM”。

如果选择了 PSK 密钥管理方式，从“PSK Format”下拉列表框中选择“ASCII”或“HEX”，并输入相应的预先共享密钥。预先共享密钥必须包含 8～63 个 ASCII 字符或 64 个十六进制字符。

第 4 步，依次单击“Apply”和“Save Configuration”按钮，保存设置。

3. 配置本地用户

第 1 步，依次选择“Security”→“AAA”→“General”选项，显示如图 7-40 所示 General 界面。在“Maximum Local Database Entries”文本框中，键入系统允许的本地数据库条目的最大值，其取值范围为 512 ～ 2048，默认值为 512。单击“Apply”按钮，保存设置，重新引导后该设置生效。

图 7-40 General 界面

第 2 步，依次选择“Security”→“AAA”→“Local Net Users”选项，显示如图 7-41 所示“Local Net Users”界面，显示已有的本地用户。

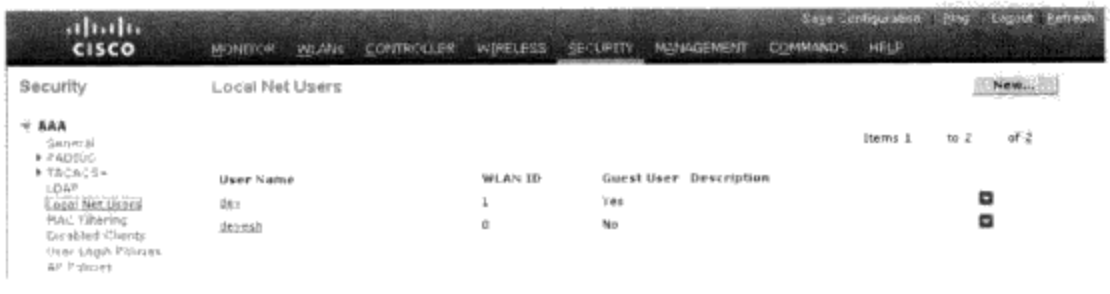


图 7-41 Local Net Users 界面

第 3 步，若欲编辑已有的用户，可直接单击“User Name”栏的用户名，显示“Local Net Users →Edit”界面，并进行修改即可；若欲删除用户，可单击用户名右侧的倒三角图标，选择“Remove”选项；若欲添加新用户，单击“New”按钮，显示如图 7-42 所示“Local Net Users →New”界面，依次设置新用户的信息。

图 7-42　Local Net Users → New 界面

4. 配置本地 EAP

依次选择“Security”→“Local EAP”→“Authentication Priority”选项，显示如图 7-43 所示“Priority Order” →“Local-Auth”界面。

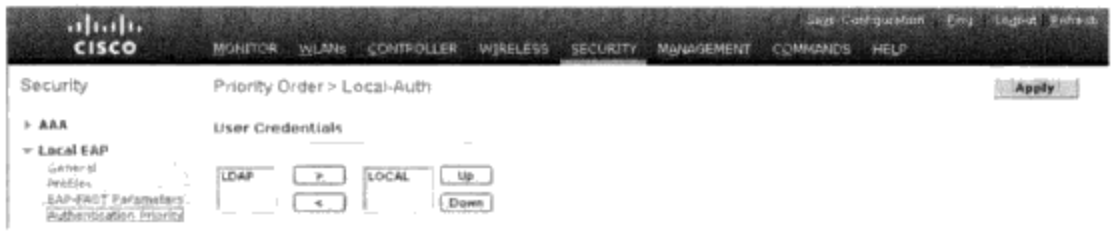


图 7-43　Priority Order→Local-Auth 界面

设置用于用户认证的后端数据库服务器顺序。高亮显示 LOCAL，单击“<”按钮将其移动至左侧的 User Credentials 列表框。高亮显示 LDAP，单击“→”按钮将其移动至右侧的 User Credentials 列表框。将 LDAP 作为优先使用的本地 EAP 认证的后端数据库服务器。当用户重新认证时，使用右侧显示在顶端的认证方式验证。单击“Apply”按钮，保存设置。

为本地 EAP 指定超时值。依次选择“Security”→“Local EAP”→“General”选项，显示“General”界面。在“Local Auth Active Timeout”文本框中，键入超时时间值。该值为使用本地 EAP 认证无线客户端时尝试连接 RADIUS 服务器失败的时间，其取值范围为 1 ~ 3 600 秒，默认值为 1 000 秒。单击 Apply 按钮，保存设置。

指定无线客户端支持的本地 EAP 认证类型。依次选择“Security”→“Local EAP”→“Profiles”选项，显示如图 7-44 所示 Local EAP Profiles 界面，显示已存在的 EAP 配置及其设置和指定的 EAP 类型。最多可以创建 16 个本地 EAP 配置。

图 7-44　Local EAP Profiles 界面

若欲编辑已有的 EAP 配置，可直接单击 Profile Name 栏的配置名称，显示如图 7-45 所示

“Local EAP Profiles”→“Edit”界面进行修改；若欲删除EAP配置，可单击该服务器右侧的倒三角图标，选择Remove选项；若欲添加新EAP配置，单击New按钮，显示“ Local EAP Profiles” →“New”界面。选中“LEAP”、“EAP-FAST”和“EAP-TLS”复选框，指定本地认证使用的EAP类型。最后，单击“Apply”按钮，保存设置即可。

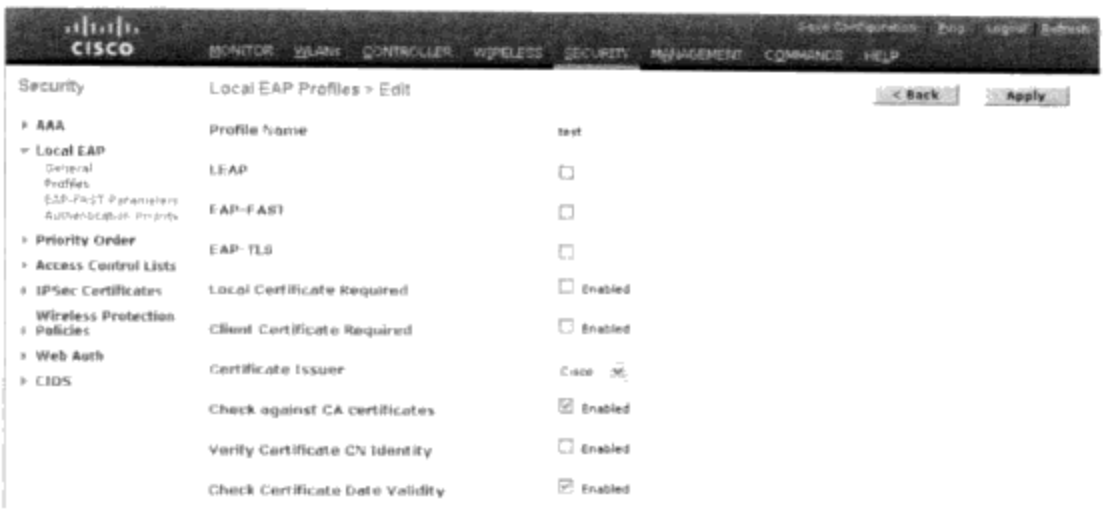


图7-45 Local EAP Profiles→Edit界面

配置EAP-FAST参数。依次选择“Security”→“Local EAP”→“EAP-FAST Parameters”选项，显示如图7-46所示EAP-FAST Method Parameters界面，设置EAP-FAST相应参数。单击“Apply”按钮，保存设置。

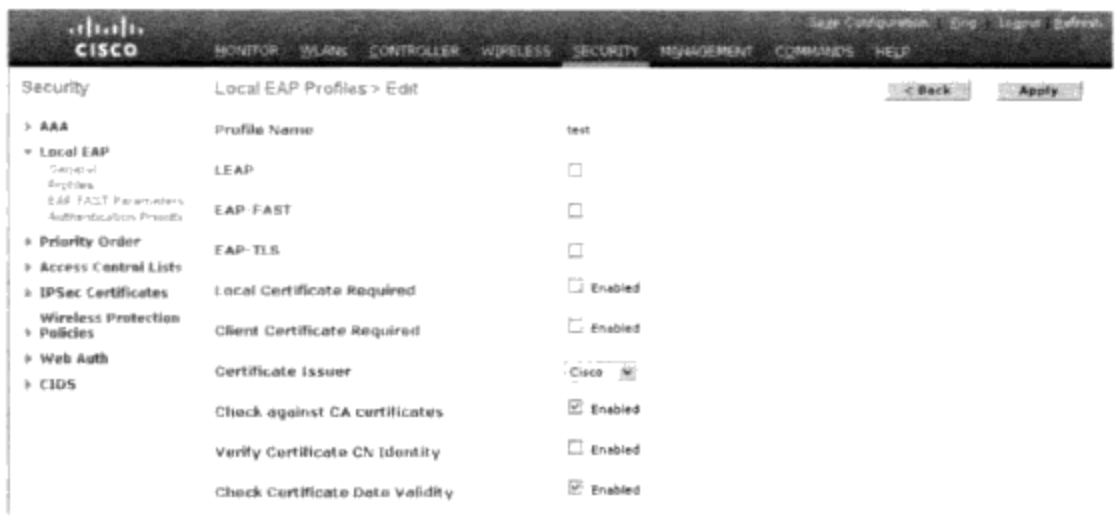


图7-46 EAP-FAST Method Parameters界面

在无线网络启用本地EAP。单击WLANs访问界面，单击欲设置WLAN的名称，显示“WLANs”→“Edit”界面。依次选择“Security”→“AAA Servers”标签，显示如图7-47所示“WLANs”→“Edit Security”→“AAA Servers”界面。

从LDAP服务器下拉列表框中，选择该WLAN欲使用的LDAP服务器。最多可以设置3个LDAP服务器。依次单击Apply和Save Configuration按钮，保存设置。

5. 配置访问列表

第1步，依次选择“Security”→“Access Control Lists”→“Access Control Lists”选项，显示如图7-48所示Access Control Lists界面，显示该无线网络控制器已经配置的所有访问列表。若欲删除访问列表配置，可单击该访问列表名称右侧的倒三角图标，选择Remove选项。

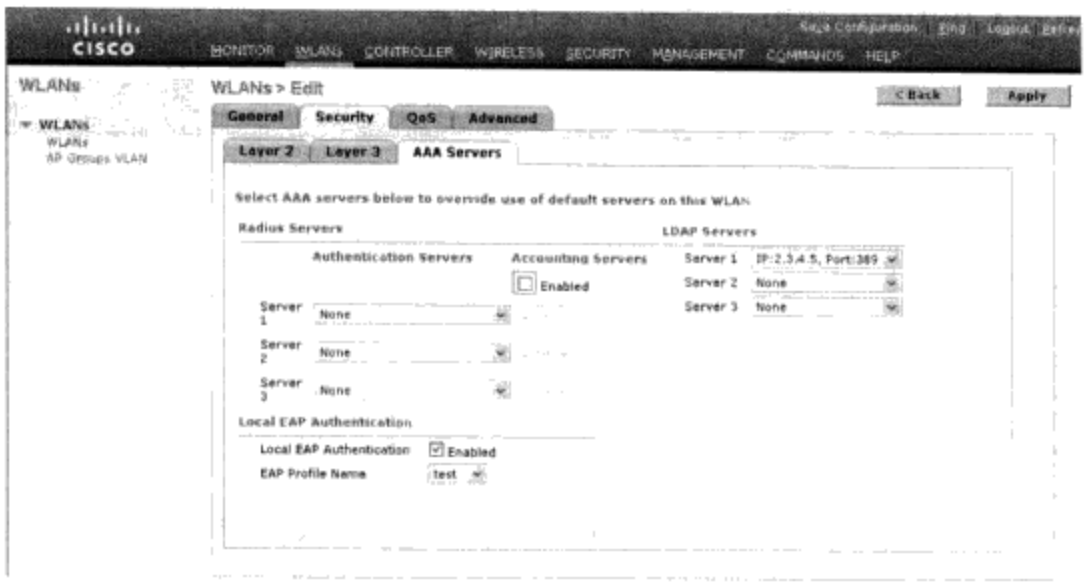


图 7-47　WLANs→Edit Security→AAA Servers 界面

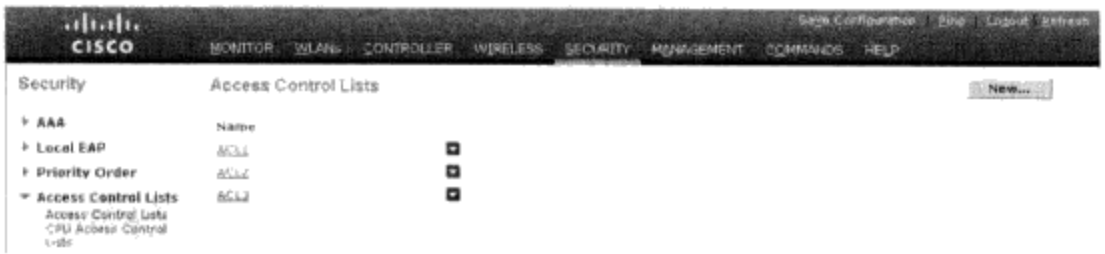


图 7-48　Access Control Lists 界面

第 2 步，创建访问列表。单击“New”按钮，显示如图 7-49 所示“Access Control Lists”→“New”界面，添加新的访问列表。键入新创建访问列表的名称，最长为 32 个字符。单击“Apply”按钮，访问列表创建完成。

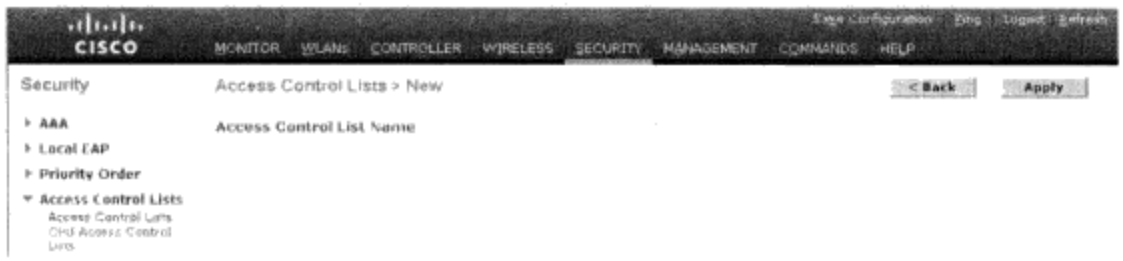


图 7-49　Access Control Lists→New 界面

第 3 步，单击欲修改的访问列表名称，显示如图 7-50 所示“Access Control Lists”→“Edit”界面。

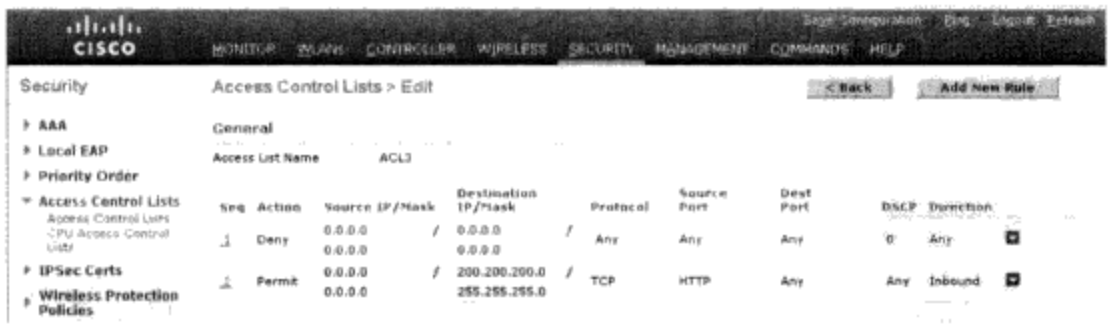


图 7-50　Access Control Lists → Edit 界面

第 4 步，创建访问列表条目。单击 Add New Rule 按钮，显示如图 7-51 所示“Access Control Lists”→“Rules”→“New”界面。根据需要设置访问列表条目，单击 Apply 按钮，保存创建的访问列表条目。重复该操作，可以创建多个访问列表条目。访问列表创建完成后，依次单

击“Apply”和“Save Configuration”按钮，保存设置。

图 7-51　Access Control Lists→Rules→New 界面

第 5 步，将访问列表应用至端口。依次选择“Controller”→“Interfaces”选项，显示 Interfaces 界面。单击欲使用该访问列表的端口名称，显示如图 7-52 所示“Interfaces”→“Edit”界面。在 ACL Name 下拉列表框中，选择该端口欲使用的访问列表名称，依次单击“Apply”和“Save Configuration”按钮，保存设置。

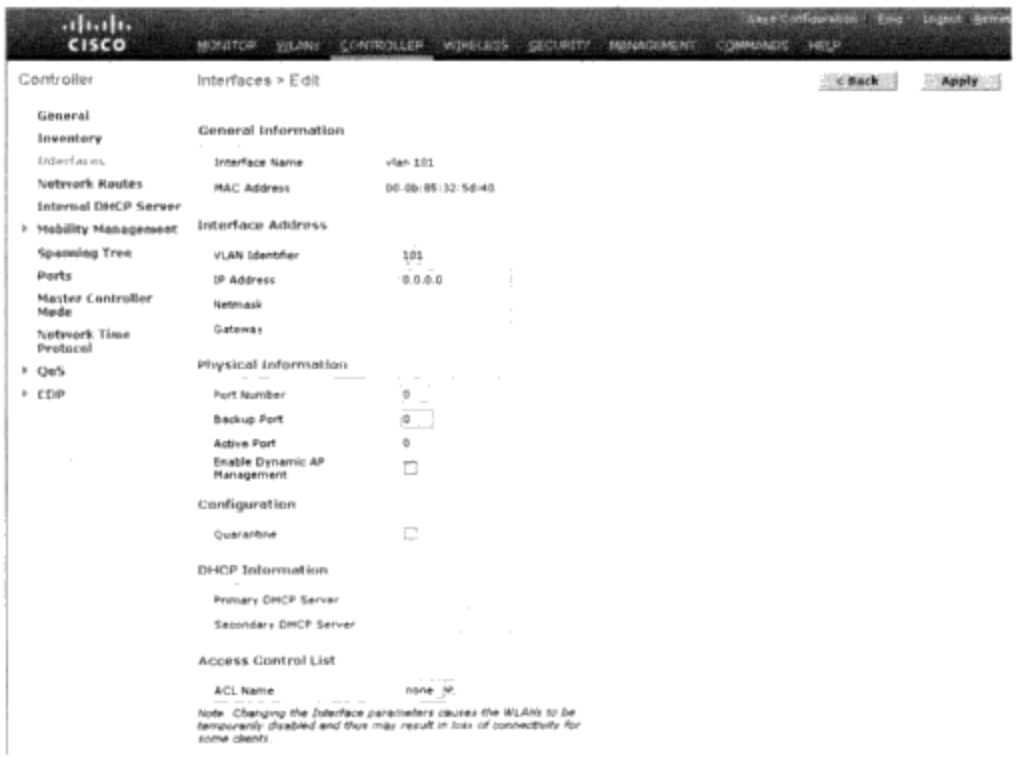


图 7-52　Interfaces→Edit 界面

第 6 步，将访问列表应用至 CPU。依次选择“Security”→“Access Control Lists”→“CPU Access Control Lists”选项，显示如图 7-53 所示“CPU Access Control Lists”界面。选中“Enable CPU ACL”复选框，从“ACL Name”下拉列表框中，选择欲使用的访问列表，将选择的访问列表指定至无线网络控制器传输，从而控制 CPU 的利用率。依次单击“Apply”和“Save Configuration”按钮，保存设置。

图 7-53　CPU Access Control Lists 界面

第 7 步，将访问列表应用至无线网络。单击“WLANs”按钮访问“WLANs”页面，单击欲应用访问列表的无线网络的配置名称，显示如图 7-54 所示“Advanced”选项卡。从“Override Interface ACL”下拉列表框中，选择欲应用至该无线网络的访问列表名称。依次单击“Apply”和“Save Configuration”按钮，保存设置。

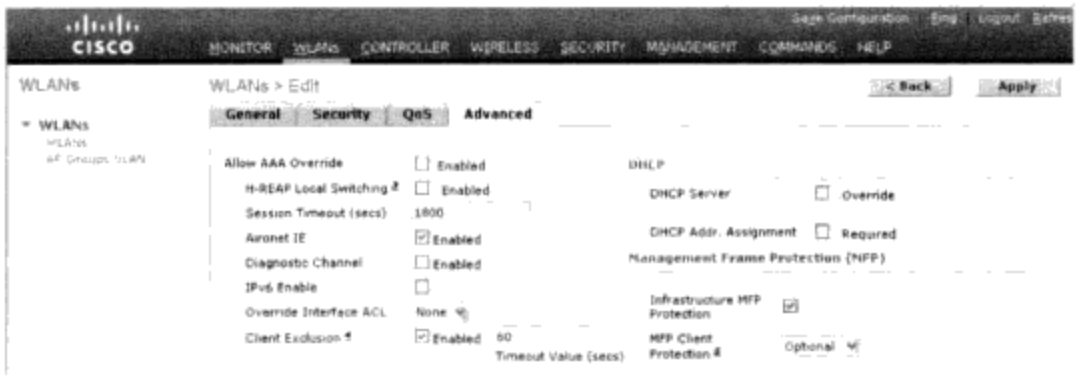


图 7-54　Advanced 选项卡

第 8 步，将认证访问列表（Preauthentication Access Control List）应用至 WLAN。单击“WLANs”按钮，打开“WLANs”页面，单击欲应用访问列表的无线网络的配置名称，显示如图 7-55 所示“WLANs”→“Edit”界面。依次选择“Security”→“Layer 3”选项，选中“Web Policy”复选框。依次单击“Apply”和“Save Configuration”按钮，保存设置。

图 7-55　WLANs→Edit 界面

6. 配置 RF 组

Cisco 无线局域网控制器所管理的特定智能 RF 功能包括：

- 动态信道分配。802.11 信道可根据不断变化的 RF 情况进行调整，以优化网络覆盖范围和性能。
- 干扰检测和避免。该系统可检测干扰并重新调整网络，以避免性能问题。
- 负载均衡。此系统对多个接入点提供了自动的用户负载均衡，即使负载量很大，也能获得最优网络性能。
- 覆盖盲区检测和修复。无线资源管理(RMM)软件可发现覆盖盲区，并尝试通过调整接入点的功率输出来修复它们。
- 动态功率控制—该系统可动态调整各接入点的功率输出，来适应不断变化的网络情况，以确保达到预期的无线性能和可靠性。

依次选择 Controller → General 选项，显示图 7-56 所示的 General 界面。在 RF-Network Name 文本框输入无线组名称，最多允许 19 个 ASCII 字符。依次单击 Apply 和 Save Configuration 按钮，保存对设置的修改。

依次选择 Wireless → 802.11a 或 802.11b/G. → RRM → Auto RF 选项，显示图 7-57

所示的 802.11a (或 802.11b/g) Global Parameters → Auto RF 界面，可以查看 RF 组的相关信息。

图 7-56 General 界面

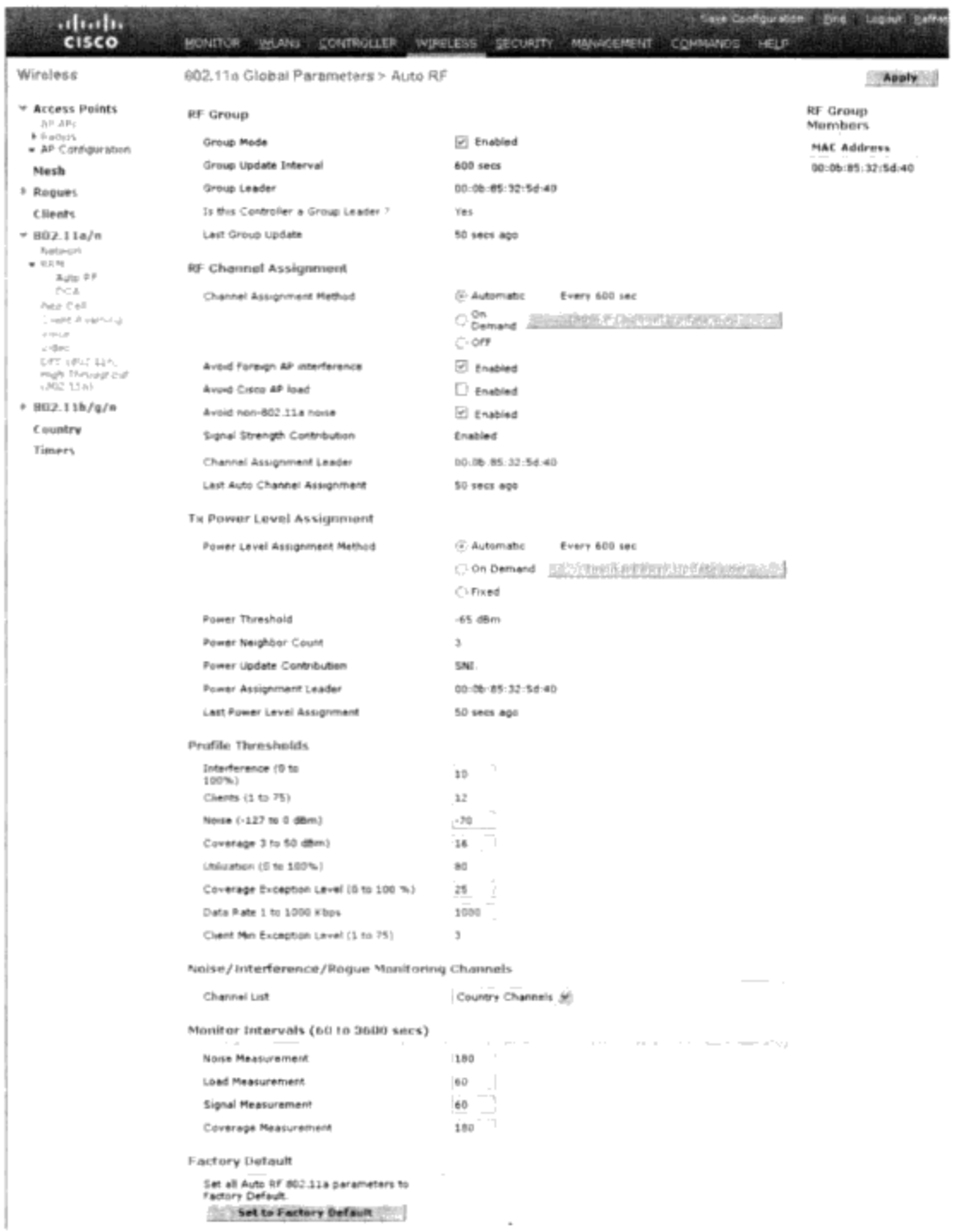


图 7-57 802.11a Global Parameters → Auto RF 界面

7. 侦测流氓 AP

单击 Wireless 按钮，显示图 7-58 所示 All APs 界面。

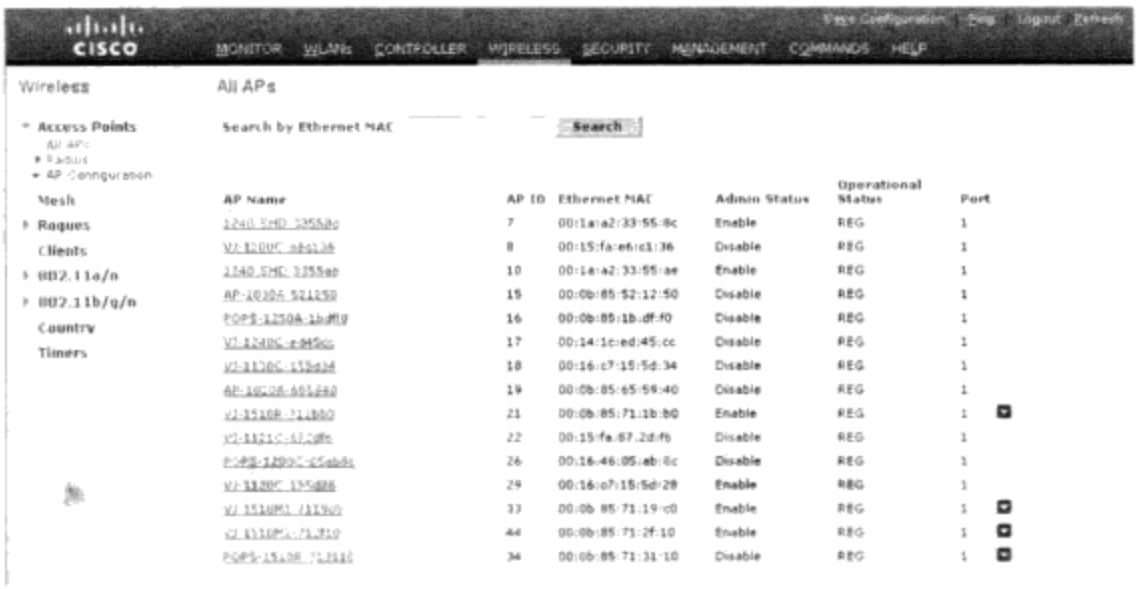


图 7-58 All APs 界面

单击 AP Name 栏中无线 AP 的名称，显示图 7-59 所示 All APs → Details 界面。在 AP Mode 下拉列表框中选择 local 或 monitor，设置无线 AP 的工作模式。依次单击 Apply 和 Save Configuration 按钮，保存对设置的修改。

图 7-59 All APs → Details 界面

重复操作，将所有的 AP 都连接至无线网络控制器。

依次选择 Security → Wireless Protection Policies → AP Authentication/MFP 选项，显示图 7-60 所示的 AP Authentication Policy 界面，列出属于该控制器的 RF 组名称。从 Protection Type 下拉列表框中选择 AP Authentication 启用流氓 AP 侦测功能。在 Alarm Trigger Threshold 文本框中输入发现流氓 AP 后发送的警报数量。依次单击 Apply 和 Save Configuration 按钮，保存对设置的修改。

在 RF 组中的每个控制器上重复上述操作。

图 7-60 AP Authentication Policy 界面

7.4 无线网络 IEEE 802.1x 身份认证

IEEE 802.1x 是实现无线网络认证的最佳手段之一。IEEE 802.1X 依赖于 RADIUS（远程身份验证拨入用户服务）网络身份验证和授权服务来验证网络客户端的凭据。802.1X 使用 EAP 来打包解决方案不同组件间的身份验证会话，并生成保护客户端与网络访问硬件畅通的密钥。部署 RADIUS 并不困难。如果用户采用 Microsoft 产品，那么，可以利用 Internet 认证服务器（IAS）来帮助部署 RADIUS。

7.4.1 部署 IEEE 802.1x 认证

对于无线网络而言，若欲实现 WPA 用户认证，就必须设置 IEEE 802.1x 身份认证。WPA 强迫用户使用 802.1x 基于端口的网络访问控制，从而防止在用户身份认证完成之前访问到全部网络。

1. 为小型网络部署 802.1x

对于小型网络而言，即使没有一个完整的公共密钥基础构架，也不需要很多工作，就可以部署 IEEE 802.1x。简单地说，需要设置 Windows XP SP 1 或更新版本的客户端来使用 PEAP，然后，设置至少一台计算机运行 Windows Internet 身份验证服务 (IAS)，该服务将提供 RADIUS 连接性。每个 IAS 服务都必须拥有一个由自己签署或从第三方证书颁发机构（CA）购买的数字证书。

2. 为大型企业部署 802.1x

对于至少拥有一个域控制器的 Windows 2000/2003 网络，可以设置一个更灵活有力的 802.1x 基础构架，充分利用 Active Directory 和 Windows 2000/2003 对远程访问策略的支持。首先，为客户端获得数字证书。在域网络中，可以很方便地通过创建组策略来获得这些证书，组策略能够自动地为域中的计算机请求机器证书。然后，部署所需基础结构（包括 IAS）的剩余部分，将无线 AP 配置为使用 RADIUS 来与 IAS 服务器进行通信。至此，WLAN 流量已经被安全地保护起来。

7.4.2 无线访问认证配置步骤

若欲借助 IAS 服务器实现无线接入的访问认证，主要配置步骤如下：

第 1 步，将无线访问点添加为主 IAS 服务器上的 RADIUS 客户端。

第 2 步，使用新建远程访问策略向导创建用于无线访问的公用策略。

第 3 步，如果正通过受保护的可扩展的身份验证协议使用安全密码身份验证，应为远程访问策略配置身份验证方法。

第 4 步，如果要使用受保护的可扩展的身份验证协议对客户端和服务器证书进行身份验证，应为远程访问策略配置身份验证方法。

第 5 步，如果要使用 PEAP-EAP-TLS 对客户端和服务器进行身份验证，应在无线客户端上从软盘安装证书，或者部署智能卡。

第 6 步，如果正在使用带有 EAP-TLS 的证书身份验证，并通过无线连接在无线客户端初始安装用户证书，应启用来宾身份验证。

第 7 步，如果正在使用带有 EAP-TLS 的证书身份验证，并通过无线连接在无线客户端初始安装用户证书，应创建名为“Guests”的组，并将 Guest 账户添加为成员。

第 8 步，如果正在使用带有 EAP-TLS 的证书身份验证，并通过无线连接在无线客户端初始安装用户证书，应使用新建远程访问策略向导为新的无线客户端（不包含用户证书的客户端）创建自定义策略。将“NAS-Poot-Type”条件设置为“Wireless-IEEE802.11”和“Wireless-Other”，并将“Windows-Groups”条件设置为“来宾”。在配置文件的“拨入限制”选项卡上，将最大会话时间限制为 10 分钟。在配置文件的“高级”选项卡上，添加带有“虚拟 LAN(VLAN)”的值的“Tunnel-Type”属性，然后，添加带有与来宾无线客户端相应的 VLANID 值的“Tunnel-Pvt-Group-ID”属性。

第 9 步，从主 IAS 服务器将 IAS 配置复制到备份 IAS 服务器。

第 10 步，在适当的 Active Directory 域中注册主服务器和备份 IAS 服务器。

第 11 步，验证无线访问点的配置。确保用于无线访问点的身份验证和记账的 RADIUS 服务器是 IAS 服务器计算机。

7.4.3 配置 Cisco 无线接入点

借助以下操作，可以指定 RADUIS 服务器，并配置 RADIUS 登录认证。

第 1 步，进入全局配置模式。

```
CiscoAP# configure terminal
```

第 2 步，启用 AAA 认证。

```
CiscoAP(config)# aaa new-model
```

第 3 步，指定 RADIUS 服务器的 IP 地址或名称。

```
CiscoAP(config)# radius-server host {hostname | ip-address} [auth-port port-number] [acct-port port-number] [timeout seconds] [retransmit retries] [key
```

string]

第4步，创建登录认证方法列表。

CiscoAP(config)# **aaa authentication login {default | list-name} method1 [method2...]**

第5步，进入Line配置模式，并指定欲适用的认证列表。

CiscoAP(config)# **line** [**console** | **tty** | **vty**] *line-number* [*ending-line-number*]

第6步，适用认证列表。

CiscoAP(config)# **login authentication {default | list-name}**

第7步，配置访问点发送其系统名称。

CiscoAP(config)# **radius-server attribute 32** *include-in-access-req* **format** *%h*

第8步，返回特权模式。

CiscoAP(config)# **end**

第9步，查看配置是否正确。

CiscoAP# **show running-config**

第10步，保存配置。

CiscoAP# **copy running-config startup-config**

7.4.4 无线用户客户端计算机配置

客户端计算机默认并未启用802.1x身份验证功能，若想连接到启用802.1x身份验证的无线AP，必须进行如下配置。

第1步，在“网络连接”窗口中，右击“无线网络连接”并选择快捷菜单中的“属性”命令，显示如图7-61所示的“无线网络连接 属性”对话框，切换到“无线网络配置”选项卡。

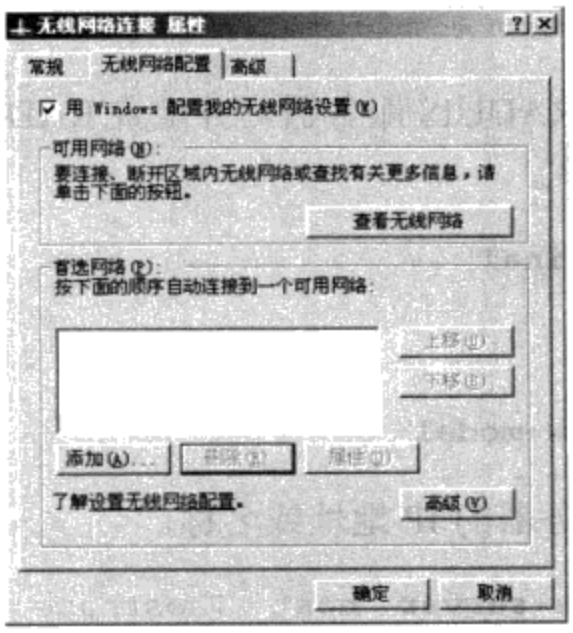


图7-61 “无线网络连接 属性”对话框

第 2 步，单击“查看无线网络”按钮，显示如图 7-62 所示“无线网络属性”对话框，在“关联”选项卡中，输入无线网络的 SSID 名称，必须与无线 AP 的配置完全相同。

第 3 步，单击“验证”切换到如图 7-63 所示“验证”选项卡，选中“启用此网络的 IEEE 802.1x 验证”复选框，在“EAP 类型”下拉列表框中选择“受保护的 EAP（PEAP）”选项，必须与无线 AP 的配置完全相同，取消“当计算机信息可用时验证为计算机”复选框。

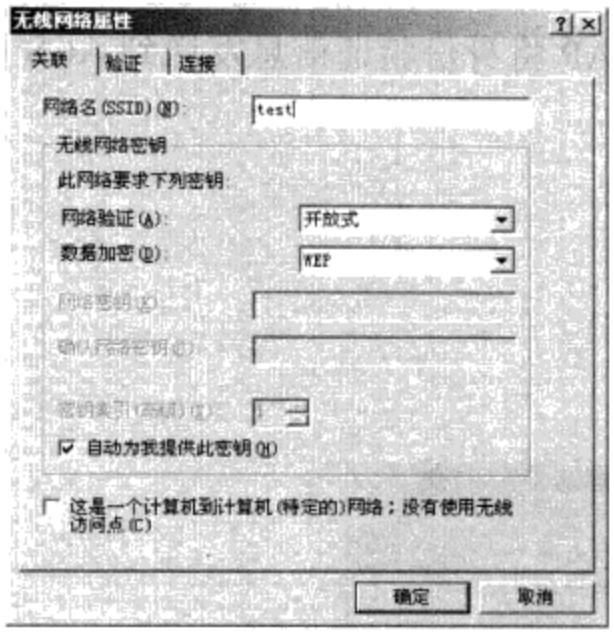


图 7-62 “无线网络属性”对话框

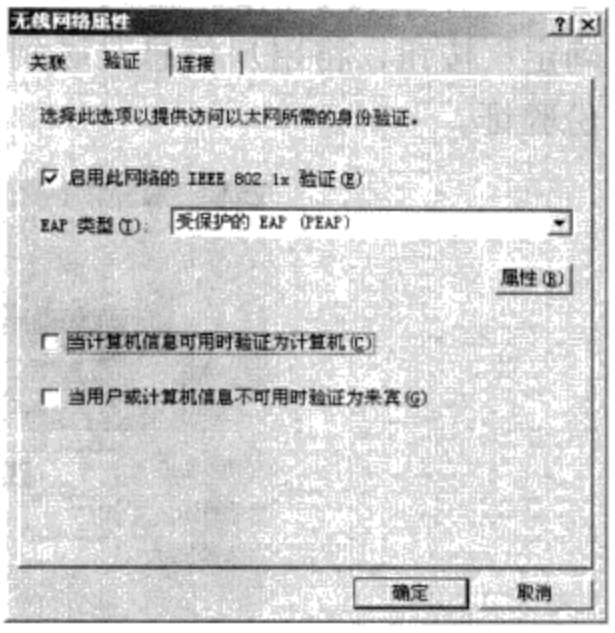


图 7-63 “验证”选项卡

第 4 步，单击“属性”按钮，显示如图 7-64 所示的“受保护的 EAP 属性”对话框，取消“验证服务器证书”复选框，在“选择验证方法”下拉列表框中，选择“安全密码（EAP-MSCHAP v2）”选项。

第 5 步，单击“配置”按钮，显示如图 7-65 所示“EAP-MSCHAPv2 属性”对话框，取消“自动使用 Windows 登录名和密码（以及域，如果有的话）”复选框。

图 7-64 “受保护的 EAP 属性”对话框

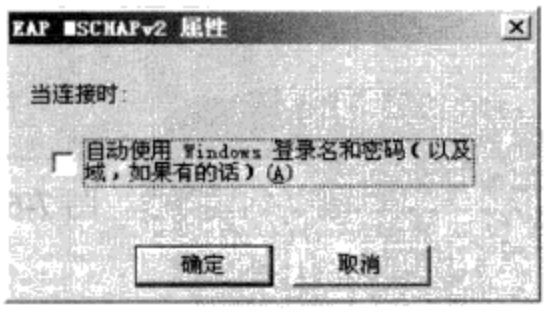


图 7-65 “EAP-MSCHAPv2 属性”对话框

7.4.5 无线客户端接入启用 802.1x 认证的网络

第 1 步，用户计算机完成基本配置后，任务栏中的无线网络连接将提示如图 7-66 所示信息，要求提供凭据才可以连接到指定的无线网络。

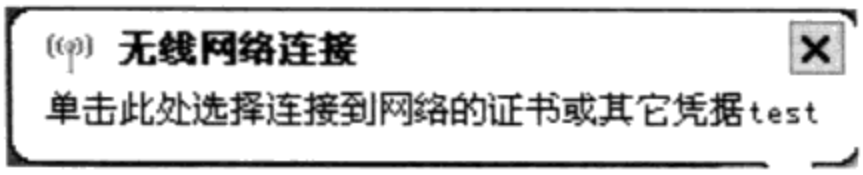


图 7-66　提示需要凭据

第 2 步，单击提示信息，显示如图 7-67 所示“输入凭据”对话框，输入用户名和密码，单击“确定”按钮，将用户信息发送到无线 AP，无线 AP 将身份验证信息发送到 ACS 服务器进行身份验证。

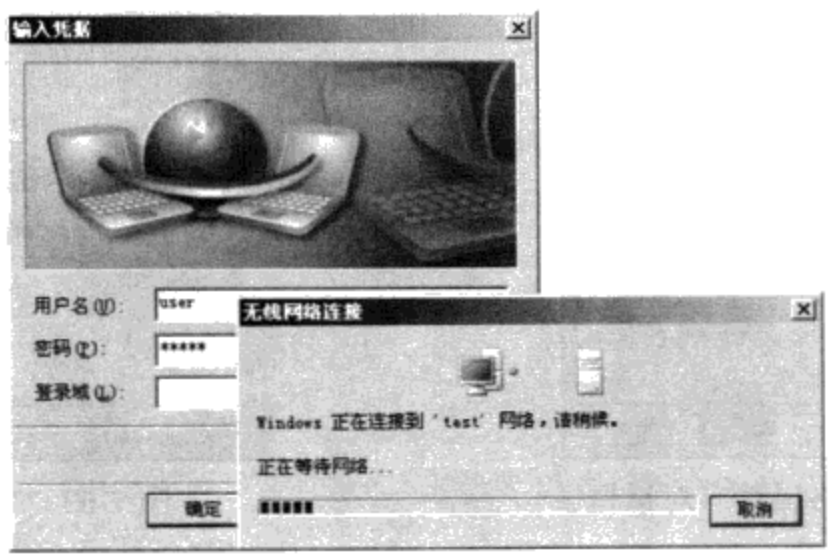


图 7-67　“输入凭据”对话框

第 3 步，成功连接到无线 AP 后，显示如图 7-68 所示窗口，test 就是启用 802.1x 身份验证的无线 AP。

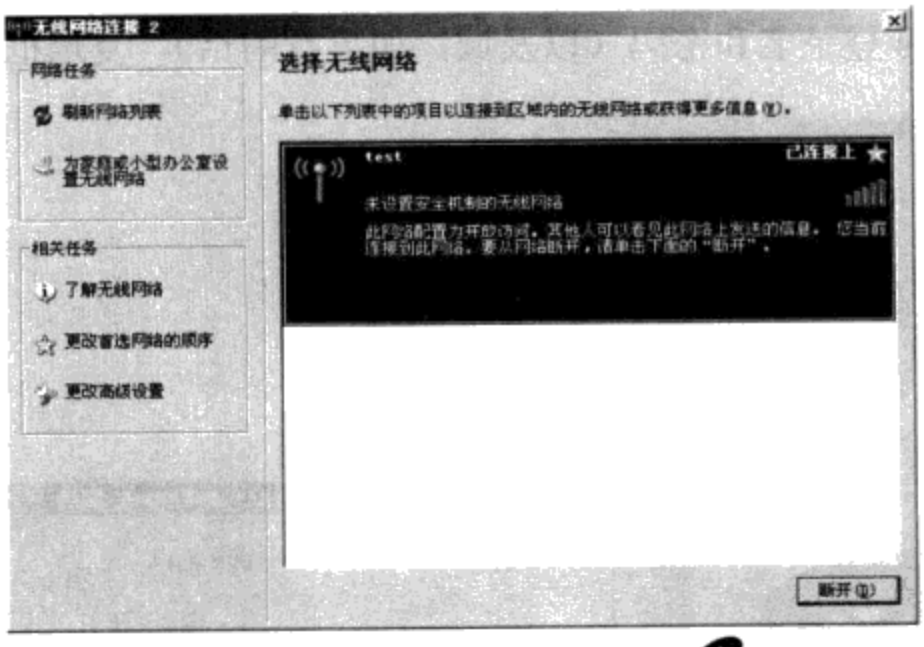


图 7-68　成功连接到无线 AP

第 8 章　网络访问保护

网络访问保护是当今网络安全领域的一项重要突破。简言之，就是通过访问控制技术将存在安全隐患的计算机或用户对象隔离在网络外部，使其不会威胁内部网络安全。目前，在此领域中比较突出的技术包括 Microsoft 的 NAP 和 Cisco 的 NAC 等，由于 NAP 易于部署和应用，而且实现成本低，所以应用非常广泛。默认情况下，NAP 组件已经集成在 Windows Server 2008 和 Windows Server 2008 R2 中，用户无需单独购买，而且默认支持主流的 Windows 客户端系统，可以实现对 IPSec、VPN、远程桌面等服务的安全防护。

8.1　NAP 系统概述

网络访问控制技术是网络安全领域的新技术之一，对访问进行“控制”的目的就是使用户按照管理员既定的策略访问网络，降低网络安全事件的发生。NAP 是一种基于软件的网络访问控制技术。在企业网络中部署 NAP 系统，可以使用定义的客户端计算机健康策略，对有网络访问需求的用户计算机进行状态评估，如果不符合健康策略要求，则拒绝进入网络，从而避免将风险因素引入网络。

8.1.1　NAP 的应用环境

网络内部安全已经成为网络安全的重点，用户水平参差不齐，使用习惯各不相同。例如，如果网络中有没有安装软件更新或者防病毒软件的客户端，则很可能导致整个网络遭受攻击。NAP 就可以很好地解决这一难题，通常情况下，它可以应用于如下保护环境。

1.　保护漫游计算机的健康

网络中应用笔记本移动办公的用户越来越广泛，例如，需要经常携带笔记本出差的用户，笔记本需要经常连接不安全的外部网络，没有安装更新补丁，没有更新病毒库，或者已经感染病毒，一旦连接到公司网络，需要进行安全检查。

2.　保护桌面计算机的健康

网络中相对比较固定的工作站，虽然可以受到网络防火墙的保护和安全策略限制，但是由于经常接入 Internet，连接移动设备，收发电子邮件等，也可能存在一定的安全隐患，有必要接受补丁包获得更新，并更新病毒库。

3.　保护来访用户计算机的健康

有时候来访用户的计算机需要连接到内部网络，但是，很难保证这些计算机符合网络内部的安全策略，如果强行接入网络，则可能会有安全威胁。此时，可以通过网络访问保护功能在技术层面进行访问限制。当客户计算机连入内部网络之后，NAP 可以将客户计算机重定向

到一个隔离的网段，会自动连接到修正服务器，对客户计算机实施制定的安全策略，例如进行自动更新，修复漏洞等，在修复安全之后，客户计算机可以自动连接到内部网络，以上操作自动完成，不耽误业务的进展。

4. 保护家庭计算机的健康

网络中的用户有时候会将工作带到家中处理，需要通过 VPN 等方式将家中的计算机连接到公司内部网络访问资源，此时家中的计算机就有可能对公司内部网络造成安全威胁。使用 NAP 功能可以设置检查家庭计算机，可以将连接入的家庭计算机限制到隔离网段，进行健康修复，直到安全为止。

8.1.2 NAP 的强制模式

在实际应用中，可以根据需要选择合适的策略模式，决定安全策略如何以策略中的配置文件评估客户端、制作 NAC Manager 中的通报信息，并判定是否向用户发送信息、进行校正或采取强制执行策略等。网络访问保护策略的模式包括如下 3 种。

- Report Only（仅报告）：在该模式下，安全策略会以配置文件对客户端进行评估，而在 NAC Manager 内会制作报告信息，但在客户端点上不会显示任何信息，并进行校正动作，并且强制执行动作也不会执行。
- Remediate（校正）：在该模式下，安全策略会以配置文件对客户端进行评估，而在 NAC Manager 内会制作报告信息，并在客户端上显示信息，并执行校正动作，而存取样本也会依适当的存取或策略状态而套用。
- Enforce（强制执行）：在该模式下，安全策略会以配置文件对客户端进行评估，而在 NAC Manager 内会制作报告信息，并在客户端上显示信息，并执行校正动作，而存取样本也会依适当的存取或策略状态而套用。

8.1.3 NAP 系统的功能

NAP 系统的主要功能就是保护内部网络安全，确保用户访问不会对内网完全造成不利影响。确切的说，企业网络中的 NAP 系统提供如下功能：

- 确认健康状态。确认尝试连入或与企业网络通信的计算机其健康状态。
- 网络访问限制。限制不符合企业计算机健康策略需求的计算机，其对企业网络的访问能力。
- 自动修复。自动提供不符合企业计算机健康策略需求的计算机，其所需要的“更新（例如，启动 Windows 防火墙功能）”，且不需使用者手动修复处理。
- 持续的符合。“持续的符合”代表需提供自动化的更新机制，让目前已符合企业计算机健康策略需求的计算机能够持续符合更新后的计算机健康策略需求。

8.1.4 NAP 系统架构

本书中介绍的 NAP 系统主要用于实现对基于微软组件的网络访问保护为例。此外，NAP

还允许其他第三方与其整合，以建立一个使用系统健康状态作为控制访问企业网络基础的平台。NAP 系统的基础架构如图 8-1 所示。

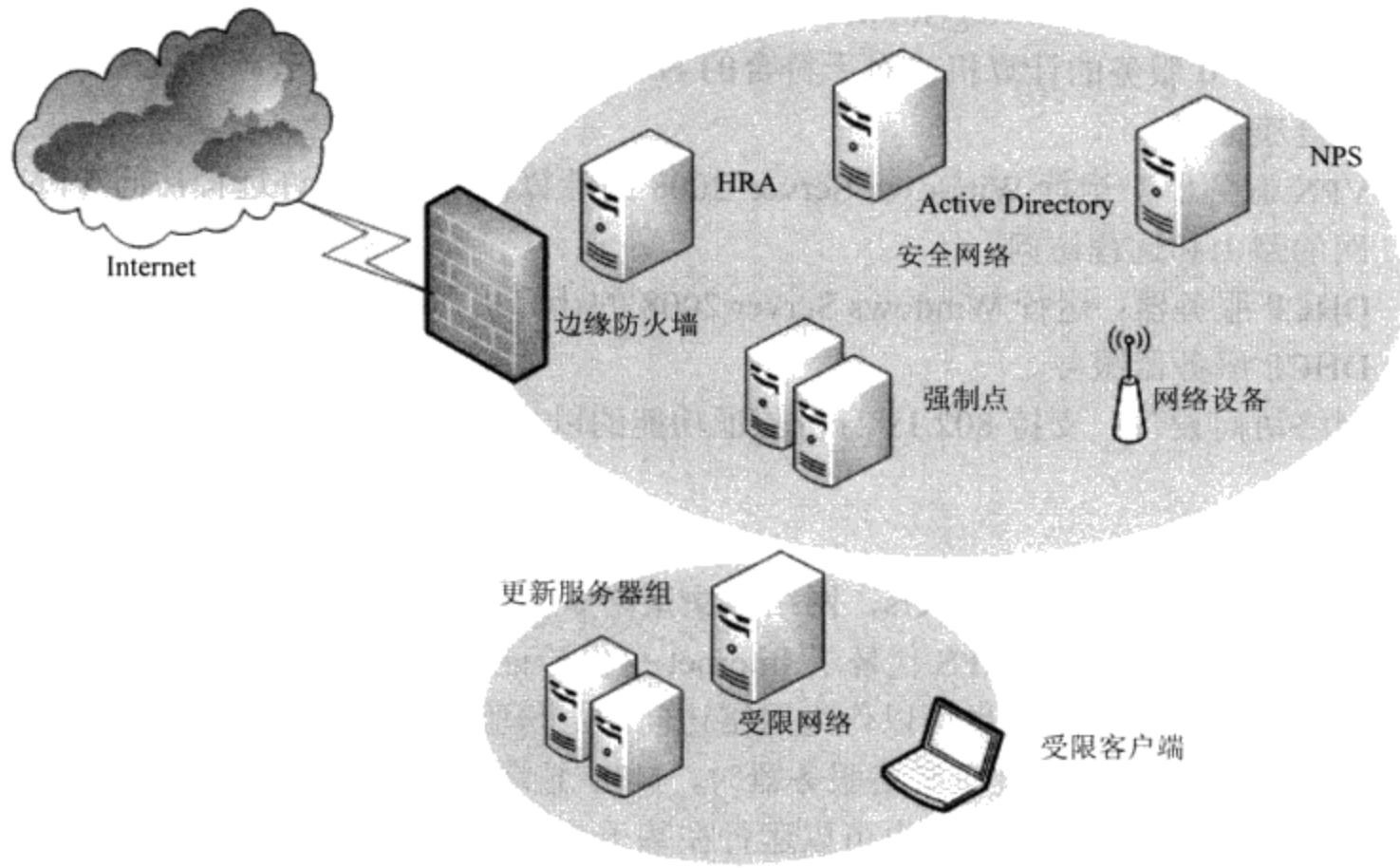


图 8-1　启用 NAP 的网络基础结构的组件

1. NAP 客户端

支持 NAP 平台功能用以确认计算机系统健康状态为控制网络访问方法的计算机或网络访问装置。例如，安装 Windows Vista、Windows XP with Service Pack 3、Windows Server 2008 等系统的计算机。而 NAP 客户端由如下部分组成。

- NAP EC：NAP EC（Enforcement Client，强制客户端组件）是用来强制客户端的审核机制的，每一个 EC 都被定义不同类别的网络访问或沟通方法，例如 DHCP 强制客户端组件、VPN 强制客户端组件等。
- SHA：SHA（System Health Agent，系统健康代理）用于检查客户端所传回的健康状态，例如，系统更新状态、病毒特征更新版本，以及系统设置状态等，而隔离代理组件则与 SHA 和 EC 协同运行。
- NAP 代理：用于收集并维护 NAP 客户端目前的健康状态信息，协助 NAP EC 和 SHA 两个组件之间的正常沟通。
- SHA API：SHA API（SHA Application Programming Interface，SHA 应用程序接口）NAP 平台所提供，且内置于 NAP 平台的 SDK（Software Development Kit）中，负责提供允许 SHA 向 NAP 注册及指出“系统健康状态（System Health Status）”、响应 NAP Agent 查询系统健康状态需求。

2. NAP 强制点

使用 NAP 或可以使用 NAP 的计算机与网络设备要求 NAP 客户端的健康状态评估，并提供受限的网络访问或通信。NAP 强制点使用网络策略服务器（NPS）作为 NAP 健康策略服务

器来评估客户端的健康状态信息，网络访问或通信是否被允许，以及对不符合的NAP客户端必须执行的修正动作的设置。典型的NAP强制点示例如下。

- HRA：HRA（Health Registration Authority，健康注册机构）运行Windows Server 2008和IIS 7.0服务的计算机，对于符合的NAP客户端都具有证书颁发机构（CA）颁发的健康证书。
- VPN服务器：运行Windows Server 2008的计算机，以及允许远程访问VPN连接内网的路由和远程访问。
- DHCP服务器：运行Windows Server 2008的计算机，以及提供动态IPv4地址配置的DHCP服务器服务。
- 网络访问设备：支持802.1x身份验证功能的以太网交换机或无线访问点等。

3. NPS

NPS（NAP Health Policy Servers，网络健康策略服务器）负责存储NAP使用的健康需求策略，并提供健康状态确认。NPS代替了Internet身份验证服务、RADIUS服务器和Windows Server 2003提供的代理。NPS也可以作为网络访问的身份验证、授权和记账（AAA）服务器。当作为AAA服务器或NAP健康策略服务器时，NPS通常为网络访问和健康要求策略的集中配置使用单独的服务器。NPS服务也可以运行在基于Windows Server 2008的NAP强制点上，如HRA或DHCP服务器。但在这些配置中，NPS服务是用于RADIUS代理与NAP健康策略服务器交换RADIUS消息的。

4. Active Directory域服务

Active Directory域服务用于存储账户证书和属性以及组策略设置。虽然不需要健康状态验证，但在IPSec强制、802.1x强制以及远程访问VPN强制应用中，Active Directory域服务都是必不可少的。

5. 受限网络

受限网络是一个单独的逻辑或物理网络包含如下部分。

- 更新服务器组　网络基础结构服务器和NAP用来修正不符合状态的健康更新服务器。例如，网络基础结构服务器包括DNS服务器和活动目录域控制器。健康更新服务器包括病毒库服务器和软件更新服务器。
- 受限客户端　对于不满足健康要求策略的计算机将会被放置在受限网络中。
- 不支持NAP的计算机　不支持NAP的计算机将会被放置在受限网络中。

8.2 强制方式

所谓强制方式就是指可以通过NAP系统为哪些网络连接提供保护，这与NPS服务器的操作系统以及NAP客户端操作系统有关。Windows Vista、Windows XP SP3和Windows Server 2008中的NAP支持如下类型的网络访问和通信包括IPSec连接、802.1x网络连接、VPN连接和DHCP连接请求。而Windows Server 2008和Windows Vista中除此之外还包括TS网关服务器的远程连接。在Windows Server 2008 R2中TS网关已更名为RD网关，但强制方式并无太

大变化。

8.2.1 IPSec 强制

使用 IPSec 强制，计算机必须符合使用内网中服务器隔离或域隔离的其他符合计算机初始化的通信，这就要求入站通信受到 IPSec 的保护。因为 IPSec 强制利用 IPSec，用户可以为受保护的通信在每个 IP 或每个 TCP/UDP 端口号上指定要求。IPSec 强制在成功连接和获取有效 IP 地址配置后，为符合的计算机限制通信。IPSec 强制是 NAP 中限制网络访问或通信的最强形式之一。

IPSec 组件包括运行于 Windows Server 2008 的 HRA 上的 IPSec ES 和 Windows Vista、Windows XP SP3 和 Windows Server 2008 上的 IPSec EC。当 NAP 客户端证明符合要求时，HRA 包含基于 X.509 健康证书。当 NAP 客户端使用其他符合的 NAP 客户端初始化 IPSec 保护的通信时，这些健康证书需要与 IPSec 策略设置一同来验证 NAP 客户端。

8.2.2 802.1x 强制

使用 802.1x 强制，计算机必须可以通过 802.1x 身份验证的网络连接来获取不受限的网络访问，网络连接包括认证的以太网交换机或 IEEE 802.1x 无线 AP。对于不符合的计算机，通过以太网交换机或无线 AP 中的受限访问配置文件来限制网络访问。受限访问配置文件可以指定访问控制列表（ACL），必须符合以太网交换机或无线 AP 上配置的 IP 数据包过滤器的设置，或者符合受限网络 VLAN ID。使用 802.1x 强制，健康策略要求在每次计算机尝试 802.1x 身份验证网络连接时都要进行强制。802.1x 强制也可以监视连接的 NAP 客户端的健康状态，以及当客户端变为不符合时应用受限访问配置文件到连接上。

802.1x 强制组件包括 Windows Server 2008 中的 NPS 和 Windows Vista、Windows XP SP3 和 Windows Server 2008 上的 EAPHost EC。802.1x 为所有通过 802.1x 身份验证连接访问网络的计算机提供受限的网络访问。

8.2.3 VPN 强制

使用 VPN 强制，计算机必须可以通过远程访问 VPN 连接获取不受限的网络访问。对于符合的计算机，通过 VPN 服务器应用在 VPN 连接上的 IP 数据包过滤器的设置来限制网络访问。使用 VPN 强制，健康策略要求在每次计算机尝试获取远程访问 VPN 连接时，都要进行强制。VPN 强制也可以监视连接的 NAP 客户端的健康状态，以及当客户端变为不符合时，为到 VPN 连接的受限网络访问应用 IP 数据包过滤器。

VPN 强制组件包括 Windows Server 2008 中的 NPS 和 Windows Vista、Windows XP SP3 和 Windows Server 2008 远程访问客户端上的 VPN EC。VPN 强制为所有通过远程访问 VPN 连接访问网络的计算机提供受限的网络访问。

8.2.4 DHCP 强制

使用 DHCP 强制，计算机必须可以从 DHCP 服务器上，获取受限网络访问的 IPv4 地址配置。对于不符合的计算机，网络访问受到 IPv4 地址配置的限制，该配置只允许到受限网络的访问。使用 DHCP 强制，健康策略要求在每次 DHCP 客户端尝试租借或续借 IPv4 地址配置时都要进行强制。DHCP 强制也可以监视连接的 NAP 客户端的健康状态，以及当客户端变为不符合时，只允许访问受限网络续借 IPv4 地址配置。

DHCP 强制组件包括 Windows Server 2008 DHCP 服务器中的 DHCP ES 和 Windows Vista、Windows XP SP3 和 Windows Server 2008 DHCP 客户端中的 DHCP EC。因为 DHCP 强制依赖于受限 IPv4 地址配置，可以被管理员任意修改，所以该强制是 NAP 中受限网络访问中较弱的形式。

8.2.5 RD 网关强制

在 Windows Server 2008 R2 中，远程桌面服务替换了 Windows Server 2008 中的终端服务。通过使用 RD 网关，授权的用户可以从任何连接到 Internet 的设备连接到组织网络中的终端服务器和远程桌面。此外，还可以使用 NAP 来强制并监视作为远程桌面客户端的客户端计算机的健康状况。

RD 网关的 NAP 强制是使用运行 NPS 的服务器和 RD 网关服务器来部署的。若要使用 RD 网关部署 NAP，必须进行下列配置。

- 安装和配置 RD 网关。
- 在 NPS 中，配置连接请求策略、网络策略和 NAP 健康策略。可以使用 NPS 控制台分别配置这些策略，也可以使用“新建网络访问保护”向导进行配置。
- 配置 WSHV 或安装并配置其他 SHA 和 SHV。
- 如果使用的是带智能卡或证书的受保护的可扩展身份验证协议-传输层安全（PEAP-TLS）或可扩展身份验证协议-传输层安全（EAP-TLS），则使用 Active Directory 证书服务部署公钥基础结构（PKI）。
- 如果使用的是受保护的可扩展身份验证协议（PEAP-MS-CHAP v2），则使用 Active Directory 证书服务颁发服务器证书，或向一个受信任的根证书颁发机构购买服务器证书。
- 使用“RD 网关管理器”管理单元在 RD 网关服务器上启用 NAP 健康策略检测。
- 在支持 NAP 的客户端计算机上启用 NAP RD 网关强制客户端、EAP 强制客户端和 NAP 服务。

8.3 网络访问保护的准备

在网络访问保护（NAP）前，需要进行一些准备工作，包括评价当前的网络基础结构和配置独立于NAP强制方式的NAP组件的设计。在正式进行部署前，需要用户理解基于Windows的身份验证基础结构的活动目录的角色、PKI、组策略和 RADIUS 和 NAP 组件和 NAP 强制方式。

8.3.1 相关服务组件的安装

不同类型的 NAP 强制，所需的网络组件有所不同，不仅需要相应的服务器角色，还需要提供辅助验证工作的组件，如证书服务器、域控制器等。通常情况，在网络中应用 NAP 强制之前，首先需要安装或配置相应的服务器角色，然后准备所需的网络环境。

1. 域控制器

域控制器的主要功能就是为内网用户和计算机提供基本的身份认证。在网络中部署和应用 NAP 强制之前，首先应在域中创建相应的用户账户或组，例如，NAP 免除安全组、测试用户组等。

NAP 免除安全组用于存储网络中的非 NAP 客户端，如 Windows Server 2003、Windows XP（非 SP3）系统用户等。这些用户无法应用各种 NAP 强制，管理员为符合安全策略和不符合安全策略的客户端设置访问权限后，必需单独为这些客户端指定是授权访问，还是限制访问。

测试用户组则用于存储广泛应用 NAP 强制之前的测试工作。不同的 NAP 强制分别限制不同类型的网络访问。如果由于应用了网络健康评估策略，而影响了正常的网络应用，就得不偿失了。因此，应用 NAP 强制之前必须在小范围内进行测试。

2. 证书服务器

数字证书是最常用的网络安全保护手段之一。在部署 NAP 强制的网络中，证书服务器的主要作用，就是为网络中的各种服务器角色或客户端颁发数字证书，实现彼此之间的身份验证。证书服务器在 IPSec 强制的网络中是必需的，而在其他 NAP 强制的网络中则是可选的。例如，在 VPN 强制网络中，如果用户选择了特定的加密传输协议和身份验证方式，则就可能需要准备数字证书，验证 VPN 服务器和 VPN 客户端身份的有效性。

3. 网络策略服务器

网络策略服务器（NPS）是任何 NAP 强制都必需的，提供各种安全健康评估、记账等功能，是 Windows Server 2008 系统的新增功能之一。NPS 允许用户通过 RADIUS 服务器、RADIUS 代理和网络访问保护策略服务器，集中配置和管理网络策略。

■ RADIUS 服务器

从 Windows Server 2008 系统开始，RADIUS 服务器已经被集成在 NPS 中。作为 RADIUS 服务器，NPS 为许多类型的网络访问（包括无线、身份验证切换、VPN 远程访问，路由器到路由器的连接）执行集中化的连接身份验证、授权和记账。

RADIUS 服务器具有对用户账户信息的访问权限，并可以检查网络访问身份验证凭据。如果用户的凭据是真实的，并且连接尝试获得授权，RADIUS 服务器将根据指定条件向用户授予访问权限，并将网络访问连接记录到记账日志中。使用 RADIUS 允许在一个中心位置（而不是在每台访问服务器上）收集并维护网络访问用户身份验证、授权和记账数据。

■ RADIUS 代理

作为 RADIUS 代理，NPS 将身份验证和记账消息转发到其他 RADIUS 服务器。使用 NPS，

各组织还可以在保留对用户身份验证、授权和记账活动控制的同时，将远程访问基础结构外包给服务提供商。

■ NAP 策略服务器

NAP 包含在 Windows Vista 和 Windows Server 2008 中，并通过确保按照组织网络健康策略配置客户端计算机后才允许其连接到网络资源，从而有助于保护对专用网络的访问。此外，计算机连接到网络时，NAP 会监视客户端计算机对管理员定义的健康策略的遵从性情况。使用 NAP 自动更新，可以自动更新不符合要求的计算机，以使其遵从健康策略，从而使它们能够连接到网络。

系统管理员可以定义网络健康策略，并使用 NPS 中或其他公司（取决于 NAP 部署）提供的 NAP 组件创建这些策略。

健康策略可以包含软件要求、安全更新要求和所需的配置设置等内容。NAP 通过检查和评估客户端计算机的健康，在认为客户端计算机不健康时限制网络访问以及修正不健康的客户端计算机以进行充分的网络访问，来强制运行健康策略。

8.3.2 更新服务器

当用户配置健康要求策略来强制受限访问时，更新服务器是不符合健康要求策略的 NAP 客户端可以访问的内网的子集。更新服务器包括网络基础结构服务器和健康更新服务器。不符合的 NAP 客户端，使用这些服务器或服务器上的资源来自动或手动执行更新。健康要求策略也可以为不支持 NAP 的客户端强制受限访问。

如果使用报告模式，则不需要更新服务器。在报告模式下，不符合的 NAP 客户端的访问不受限制。但是，为了避免不符合健康要求策略的计算机为内网带来的威胁，必须最终转换到强制模式，即需要建立更新服务器。

在 VPN 和 DHCP 模式下不符合健康要求策略的 NAP 客户端，可以访问的更新服务器列表，需要与 NAP 客户端健康评估匹配的网络策略的 NAP 强制设置中，指定的更新服务器组相符合，更新服务器组是一个 IPv4 和 IPv6 地址的列表。该列表应该包括网络基础结构服务器和健康更新服务器。

基础结构服务器包括如下部分：

- DHCP 服务器，为不符合健康要求策略的 NAP 客户端分配 IPv4 地址和其他配置参数，保证其可以访问更新服务器。如果用户正使用 DHCP 强制方式，则不需要添加支持 NAP 的 DHCP 服务器作为更新服务器。
- DNS 和 WINS 服务器，为不符合的 NAP 客户端提供名称解析，保证其可以解析名称，并访问其他更新服务器。
- 活动目录域控制器，保证不符合的 NAP 客户端可以执行域登陆，访问基于域的资源如文件共享。
- Internet 代理服务器，保证不符合健康要求策略的 NAP 客户端可以访问 Internet。
- HRA，保证不符合健康要求策略的 NAP 客户端可以在 IPSec 强制模式下获取健康证书。

更新 NAP 客户端系统健康需要健康更新服务器，包括如下部分。

- 疑难解答 URL 服务器：在“更新服务器和疑难解答 URL”对话框中的疑难解答 URL

文本框中，指定 Web 服务器。

- 反病毒更新服务器：这些服务器可能位于 Internet 上。如果用户拥有 Internet 代理服务器作为更新服务器，则不需要包含基于 Internet 的反病毒更新服务器。如果在内网中拥有反病毒更新服务器，则应该将其作为更新服务器，因为在尝试连接访问基于 Internet 的反病毒服务器前，通常会首先在这些服务器上检查更新。
- 反间谍更新服务器：如同反病毒服务器一样，如果在内网中配置了反间谍更新服务器，则需将其作为更新服务器。如果只存在于 Internet 上，确保 Internet 代理服务器包含在更新服务器组中。
- 软件更新服务器：如同反病毒服务器一样，如果在内网中配置了软件更新服务器，则需将其作为更新服务器。如果只存在于 Internet 上，确保 Internet 代理服务器包含在更新服务器组中。

更新 NAP 客户端所需要的健康更新服务器的设置依赖于用于健康评估的 SHV。

8.3.3 网络策略服务器

网络策略服务器（NPS）是 NAP 系统中的重要角色，集成 RADIUS、健康策略等服务，主要完成对客户端接入请求的验证、系统健康评估、记账和访问授权。Windows Server 2008 或 Windows Server 2008 R2 服务器都可以作为网络策略服务器。部署 NPS 之前应对网络架构进行合理规划，尽量避免与 Active Directory 等重要服务使用同一台服务器。

在本书“第 7 章局域网接入安全”中已经介绍过 RADIUS 服务器的安装，NPS 的部署过程与之完全相同，并且可以根据需要选择其他相关组件的安装，如图 8-2 所示。

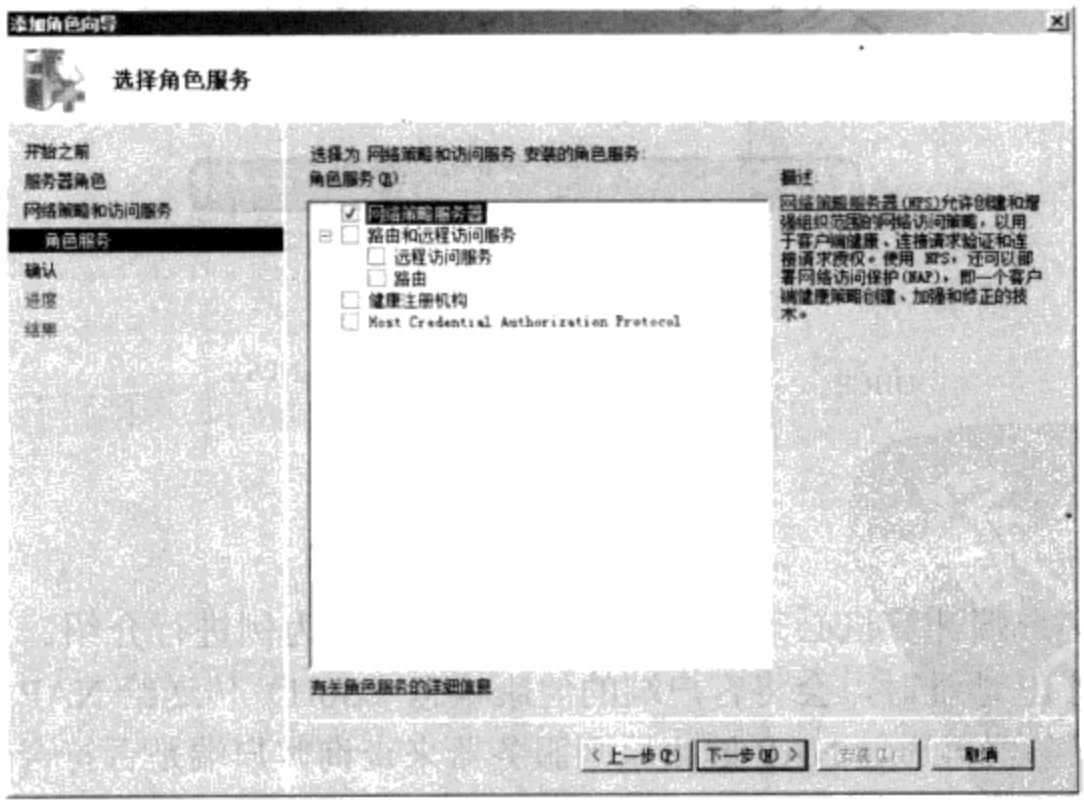


图 8-2 安装网络策略服务器

提示 角色服务中的“路由和远程访问服务”、“健康注册机构”和“Host Credential Authorization Protocol”，只有在特殊环境中才会用到，通常情况下不会用到。

8.4 DHCP 强制的配置与应用

NAP DHCP 强制的目的是在 DHCP 客户端租借或续订其 IP 地址时，执行客户端健康检查，根据评估结果为其分配相应作用域的 IP 地址。通常情况下，需完成下列配置：

- 在 NPS 中，配置连接请求策略、网络策略和 NAP 健康策略。可以使用 NPS 控制台单独配置这些策略，也可以使用新建网络访问保护向导。
- 在可用 NAP 的客户端计算机上启用 DHCP 强制客户端和 NAP 服务。
- 在 DHCP 控制台中，为各个作用域或在 DHCP 服务器上配置的所有作用域启用 NAP。
- 配置网络策略服务器上的 SHV。
- 配置更新服务器组。

8.4.1 网络环境概述

本章 DHCP 强制实例的网络环境如图 8-3 所示。NPS 服务器和 DHCP 服务器均已经加入域中，域控制器同时担当 DNS 和 CA 角色。DHCP 服务器同时被配置为 RADIUS 代理服务器，通过 RADIUS 协议将 NAP 客户端的请求发送给 NPS。NPS 服务器同时也是 RADIUS 服务器，用于接收和处理 DHCP 服务器发送过来的 NAP 客户端健康状态验证请求。NAP 客户端系统为 Windows Vista，自动从 DHCP 服务器获得 IP 地址。

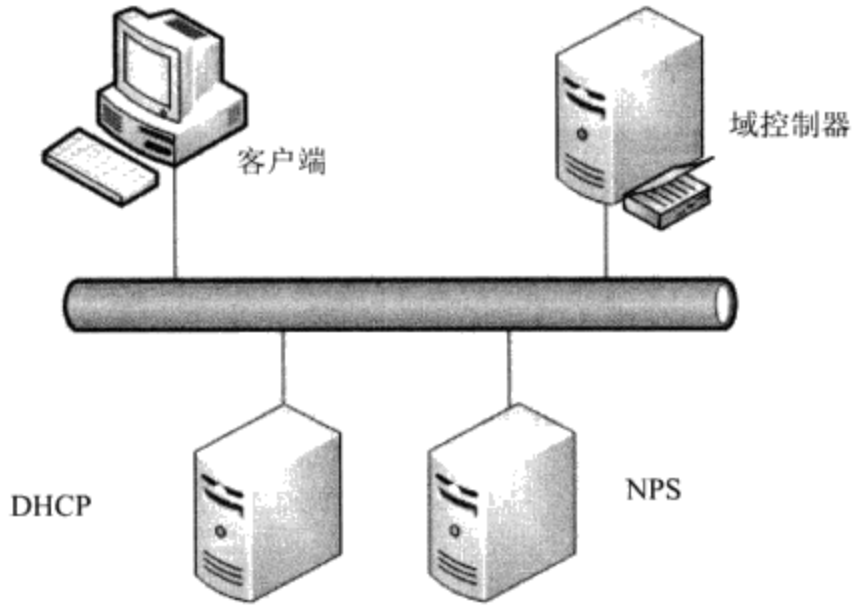


图 8-3 DHCP 强制网络环境

实验以要求客户端计算机必须开启 Windows 防火墙为例进行介绍。当 NAP 客户端向 DHCP 服务器租用 IP 地址时，会将客户端的健康状态（SoH）传送给 NAP 强制执行点 DHCP 服务器，DHCP 服务器再通过 NAP 健康原则服务器来查询客户端是否符合健康原则的要求：

- 如果 NAP 客户端已启用 Windows 防火墙的话，则会根据网络原则的设定来给予客户端具备完整网络访问权限的 IP 组态与路由设定。
- 如果 NAP 客户端尚未启用 Windows 防火墙的话，则会根据网络原则的设定来给予客户端不同的 IP 组态与路由设定，让该客户端仅能存取受限制的网络资源。
- 不符合健康要求的客户端可以在受限网络中访问更新服务器，最终成为符合策略要求的健康客户端。

实验环境中所需的各种服务器角色的配置过程，这里不做详细介绍，只介绍每个服务器角色需要完成的配置。

8.4.2 配置健康策略服务器

配置 DHCP 强制所需的健康策略服务器需要完成的操作包括系统健康状态验证（SHA）设置、健康策略设置、网络策略设置以及连接请求策略设置等，可以借助 NAP 配置向导来完成。

1. 配置健康策略

第 1 步，在 NPS 服务器上，打开“网络策略服务器”窗口。单击“NPS（本地）”并在右侧窗口“标准配置”的下拉列表框中选择“网络访问保护（NAP）”选项，如图 8-4 所示。

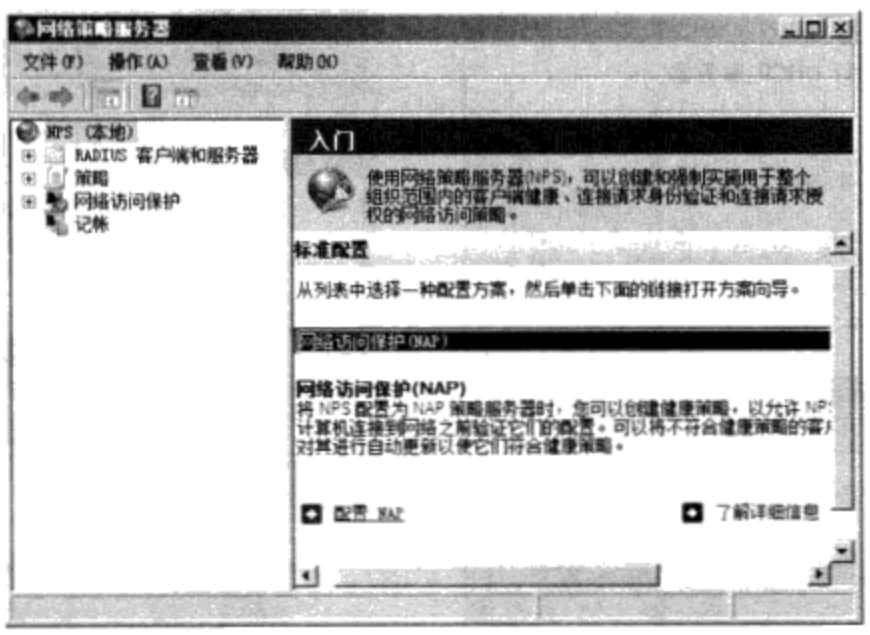


图 8-4 “网络策略服务器”窗口

第 2 步，单击“配置 NAP”链接，显示如图 8-5 所示“选择与 NAP 一起使用的网络连接方法”对话框，在“网络连接方法”中，选择“动态主机配置协议（DHCP）”选项，在“策略名称”文本框中，默认名称为 NAP DHCP，用户也可以自定义。

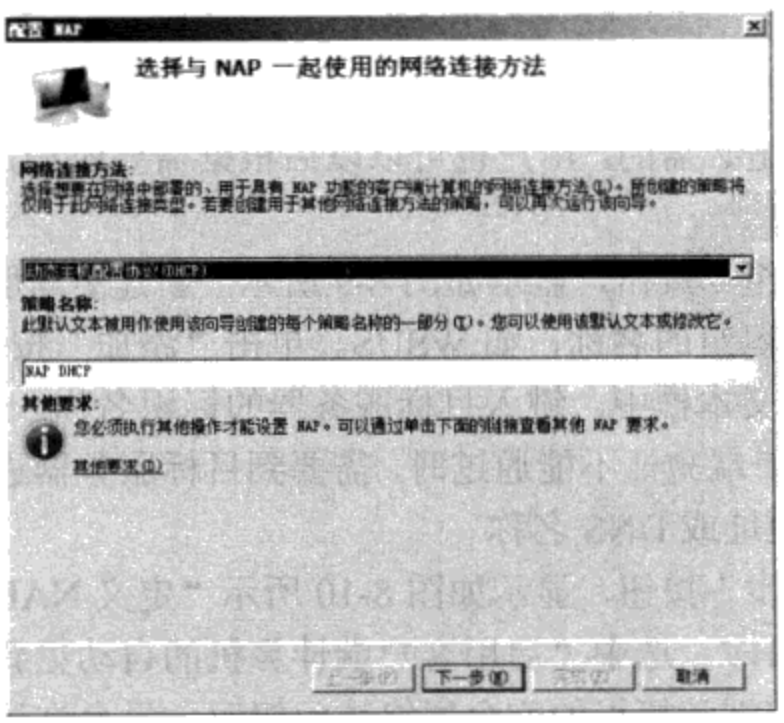


图 8-5 “选择与 NAP 一起使用的网络连接方法”对话框

第3步，单击“下一步”按钮，显示如图8-6所示“指定NAP强制服务器运行DHCP服务器”对话框，将DHCP服务器配置为NPS的RADIUS客户端。单击“添加”按钮，在“新建RADIUS客户端”对话框，为该客户端命名、指定其IP地址（DHCP服务器的IP地址）并创建“共享机密”。注意，在RADIUS客户端也必须设置相同的密码，否则无法进行RADIUS通信。此处选择“手动”方式创建共享机密，也可以选择“生成”单选按钮自动创建改密码。单击“确定”按钮返回NAP配置向导。

第4步，连续单击“下一步”按钮，在“指定DHCP作用域”对话框，即通过此作用域租用IP地址的客户端将会受到NAP系统的限制，系统默认将NAP强制应用于所有作用域。在“配置用户组和计算机组”对话框，根据需要选择计算机或组，如图8-7所示。

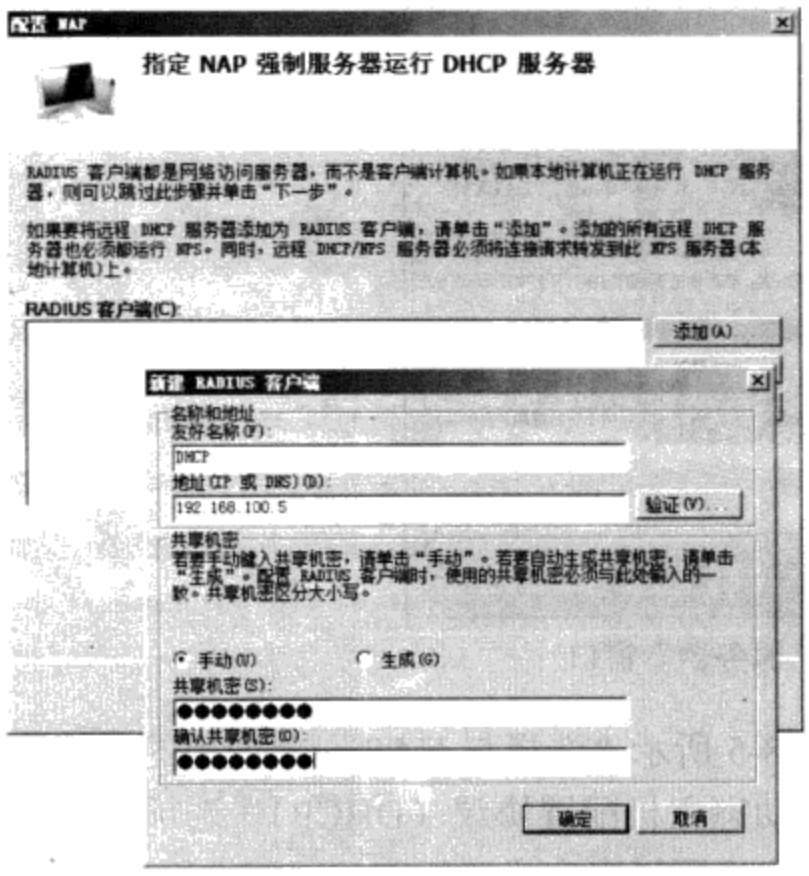


图8-6 指定DHCP的NAP强制和配置RADIUS客户端

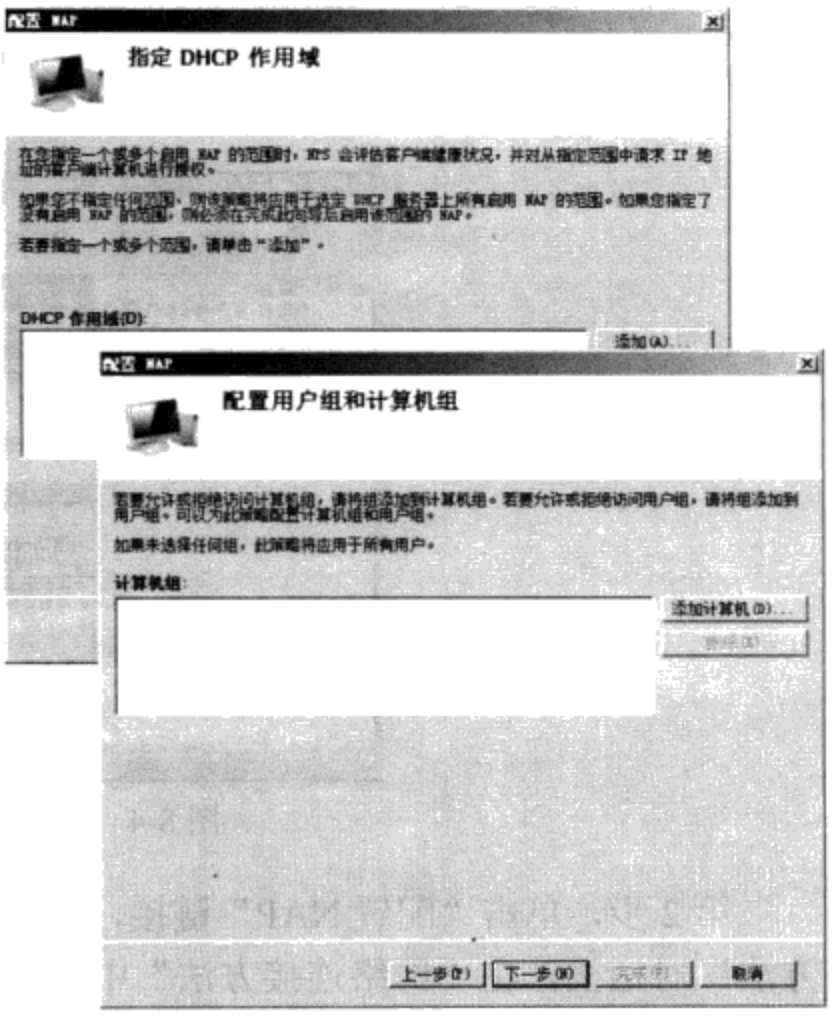


图8-7 指定DHCP作用域和对象组

第5步，单击“下一步”按钮，显示如图8-8所示“指定NAP更新服务器组和URL”对话框，更新服务器组并不是必需的，用户也可以以后根据需要添加，在这里我们立即创建更新服务器组。

第6步，单击“新建组”按钮，显示如图8-9所示“新建更新服务器组”对话框。在“组名”文本框中，键入服务器组的名称，如WSUS。单击“添加”按钮，显示“添加新服务器”对话框。在“友好名称”文本框中，键入目标服务器的标识名称。在“IP地址或DNS名称”文本框中，键入当验证客户端验证不能通过时，需要到目标服务器进行处理或者暂时访问的目标服务器，可以使用IP地址或DNS名称

第7步，单击“下一步”按钮，显示如图8-10所示“定义NAP健康策略”对话框，选择DHCP强制需要评估的SHV。选中“启用客户端计算机的自动更新”复选框，并选择“拒绝对不具有NAP功能的客户端计算机的完全网络访问权限。只允许访问受限网络。”单选按钮，即配置为强制模式。如果网络中非NAP客户端数量较多，也可以更改为“报告”模式，即允

许这些客户端完全访问网络同时报告其状态。

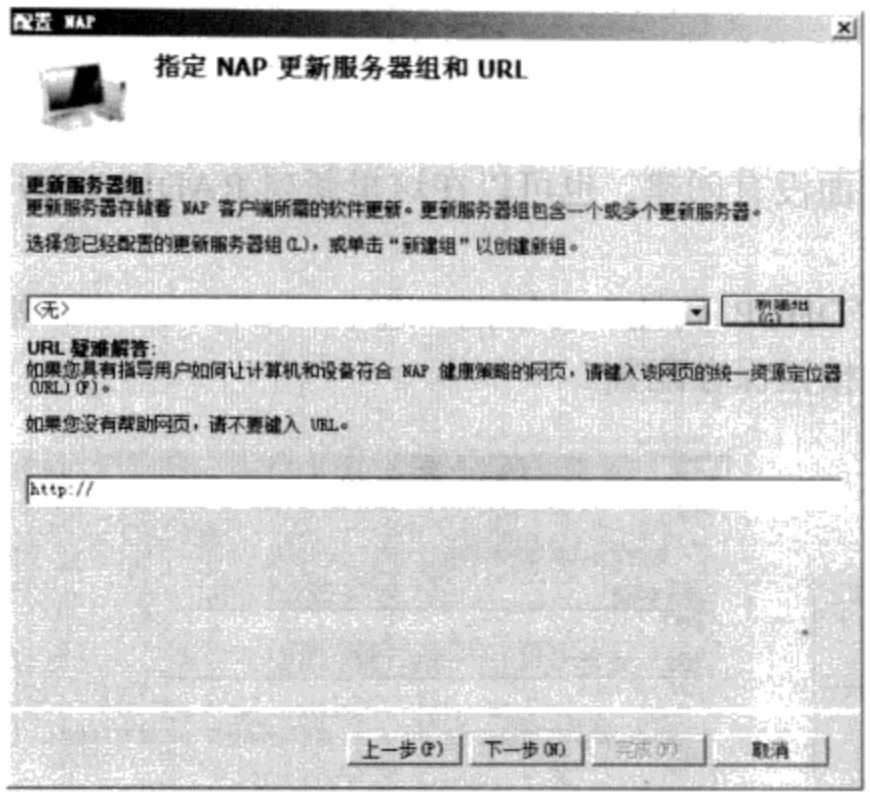


图 8-8 "指定 NAP 更新服务器组和 URL"对话框

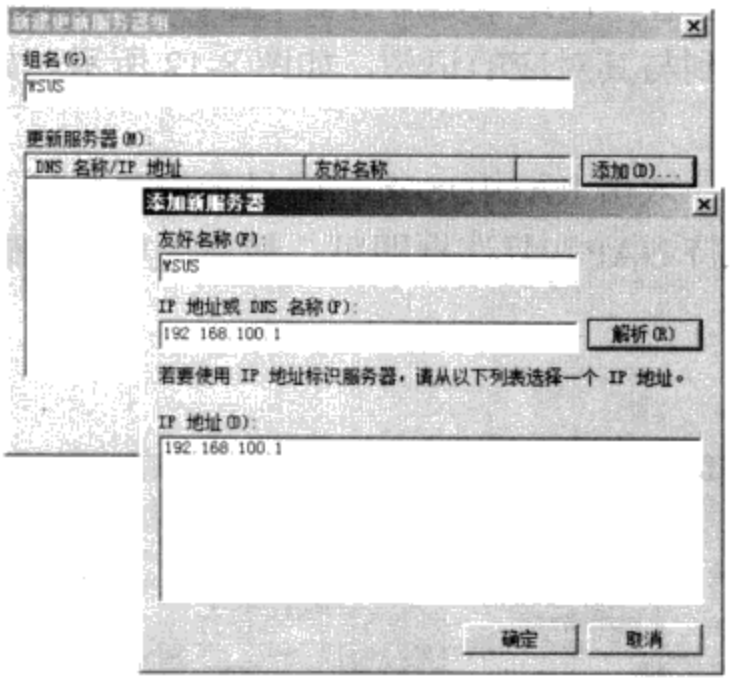


图 8-9 "新建更新服务器组"对话框

第 8 步，单击"下一步"按钮，显示如图 8-11 所示"正在完成 NAP 增强策略和 RADIUS 客户端配置"对话框，提示由该向导创建的各种策略以及 RADIUS 客户端和更新服务器组。

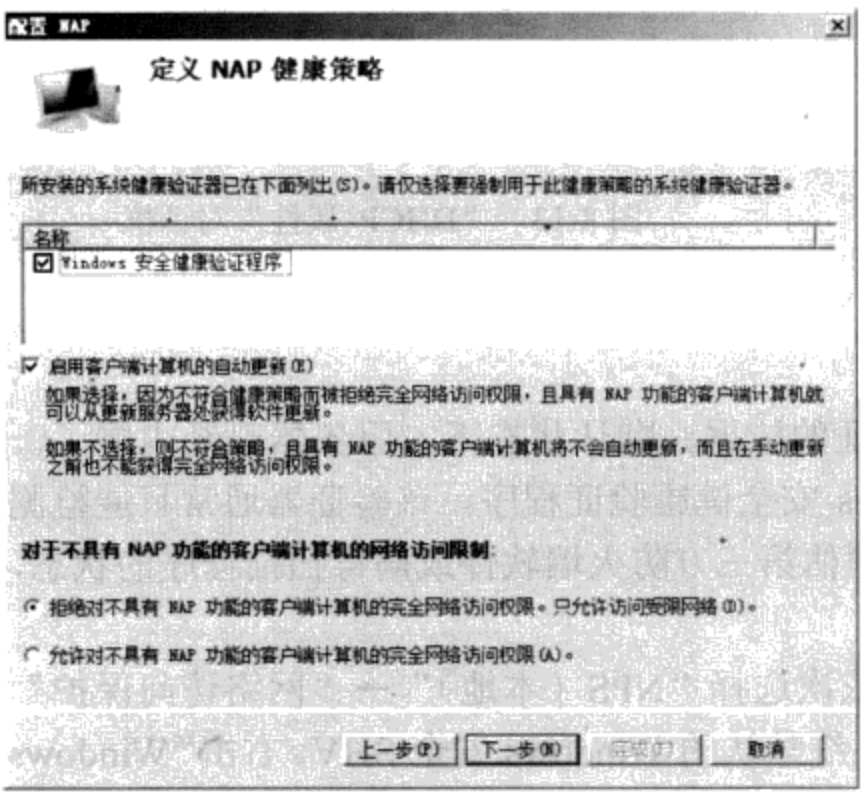


图 8-10 "定义 NAP 健康策略"对话框

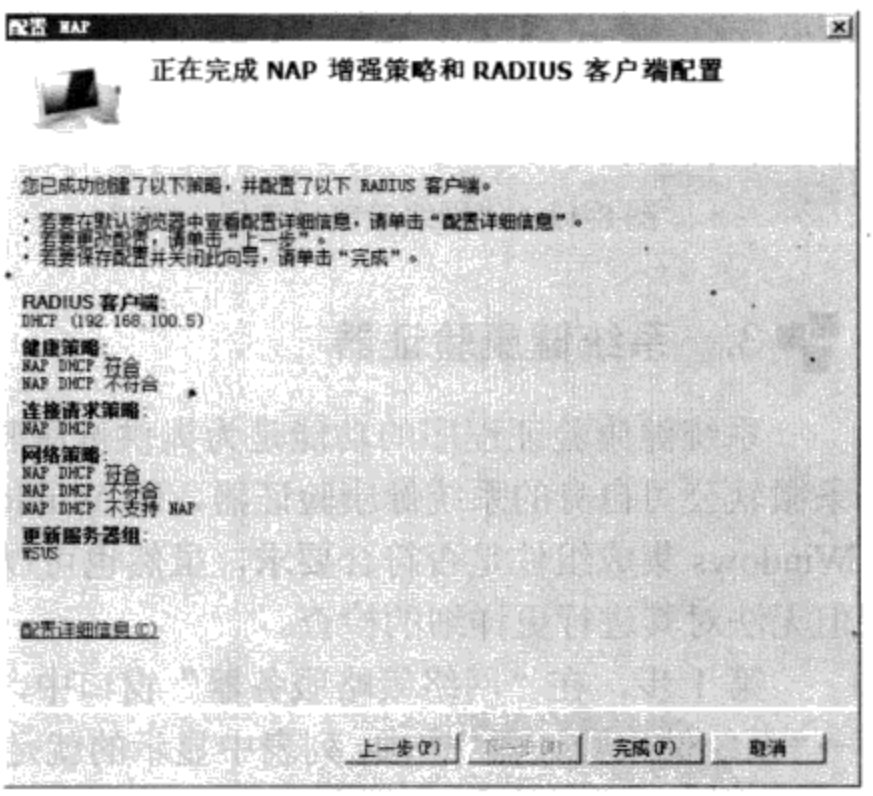


图 8-11 "正在完成 NAP 增强策略和 RADIUS 客户端配置"对话框

第 9 步，单击"完成"按钮，关闭"配置 NAP"向导即可。

"配置 NAP"向导创建的连接请求策略和网络策略位于各自顺序列表的底部。由于不符合健康要求策略的 NAP 客户端网络策略默认情况下只允许受限访问（强制模式），用户必须修改该策略使之允许报告模式下的不受限访问。

2. 配置 RADIUS 客户端

由于在配置 DHCP 强制策略过程中已经将 DHCP 服务器配置为 NPS 的 RADIUS 客户端，所以在“网络策略服务器”窗口的“RADIUS 客户端和服务器”→“RADIUS 客户端”中可以看到与其对应的记录，如图 8-12 所示。如果前面没有创建，也可以在这里新建 RADIUS 客户端。

双击 RADIUS 客户端显示如图 8-13 所示“DHCP 属性”对话框，选中“RADIUS 客户端支持 NAP”复选框即可。最后，单击“确定”按钮保存配置。

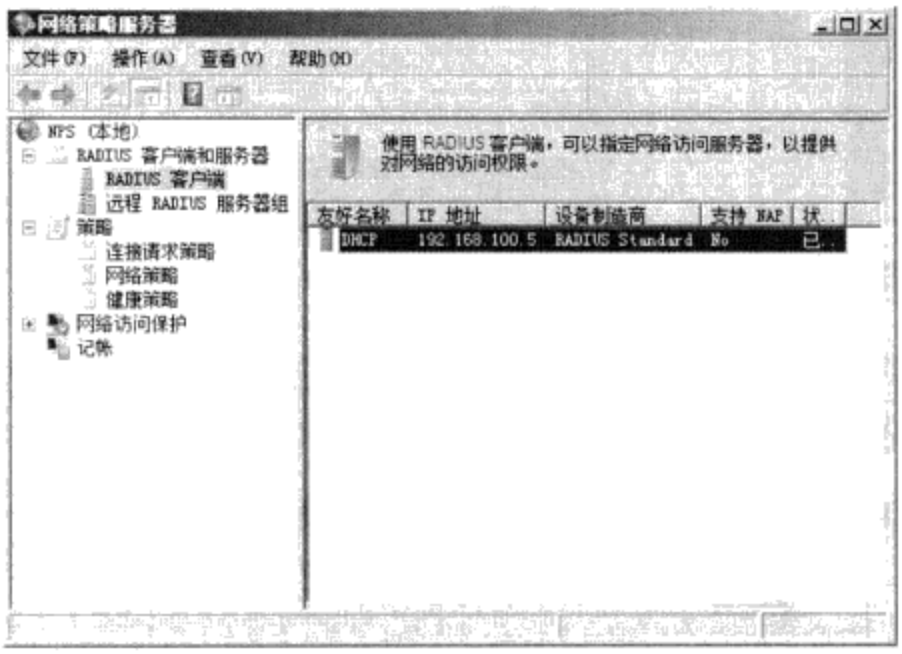


图 8-12 “网络策略服务器”窗口

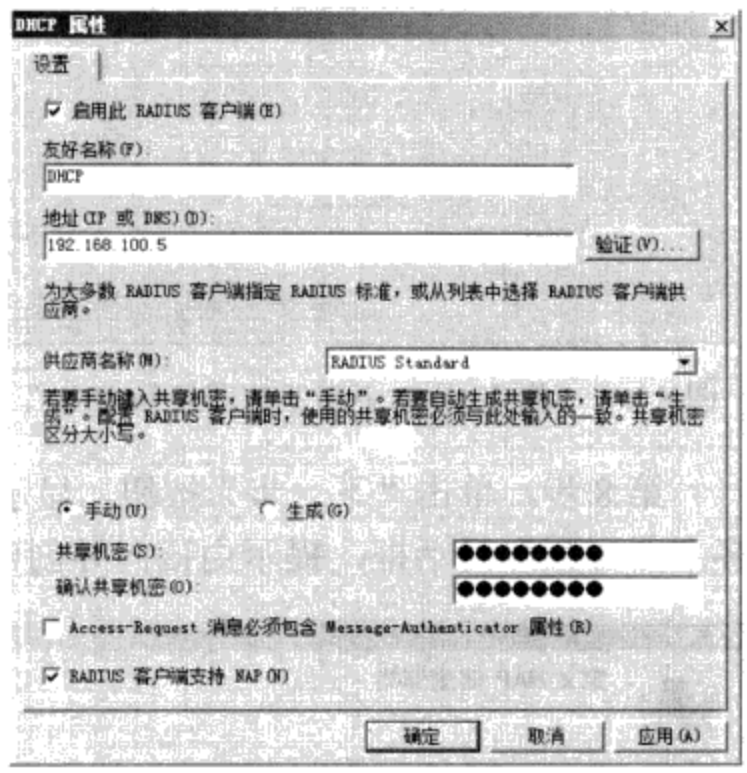


图 8-13 “DHCP 属性”对话框

3. 系统健康验证器

系统健康验证程序的功能是为提供健康验证的依据。默认状态下，服务器已经内置了一条微软公司自身的系统健康验证器，即 Windows 安全健康验证程序。该验证器通常只能检测 Windows 集成组件是否符合要求，虽然也可以评估第三方防火墙软件或病毒扫描程序的状态，但无法对其进行更详细的检查。

第 1 步，在“网络策略服务器”窗口中，依次选择“NPS（本地）”→“网络访问保护”→“系统健康验证器”选项，列表中显示的就是系统默认的 Windows 安全 SHV。右击“Windows 安全健康验证程序”，选择快捷菜单中“属性”选项，打开如图 8-14 所示的“Windows 安全健康验证程序 属性”对话框。

第 2 步，单击“配置”按钮，显示如图 8-15 所示“Windows 安全健康验证程序”对话框。默认显示的是“Windows Vista”选项卡，这里可以设置适用于所有 Windows Vista 客户端的验证功能，包括防火墙、病毒防护、间谍软件保护和自动更新等，这里选中“已为所有网络连接启用防火墙”复选框。切换到“Windows XP”选项卡，还可以设置对运行 Windows XP 系统客户端的健康要求。

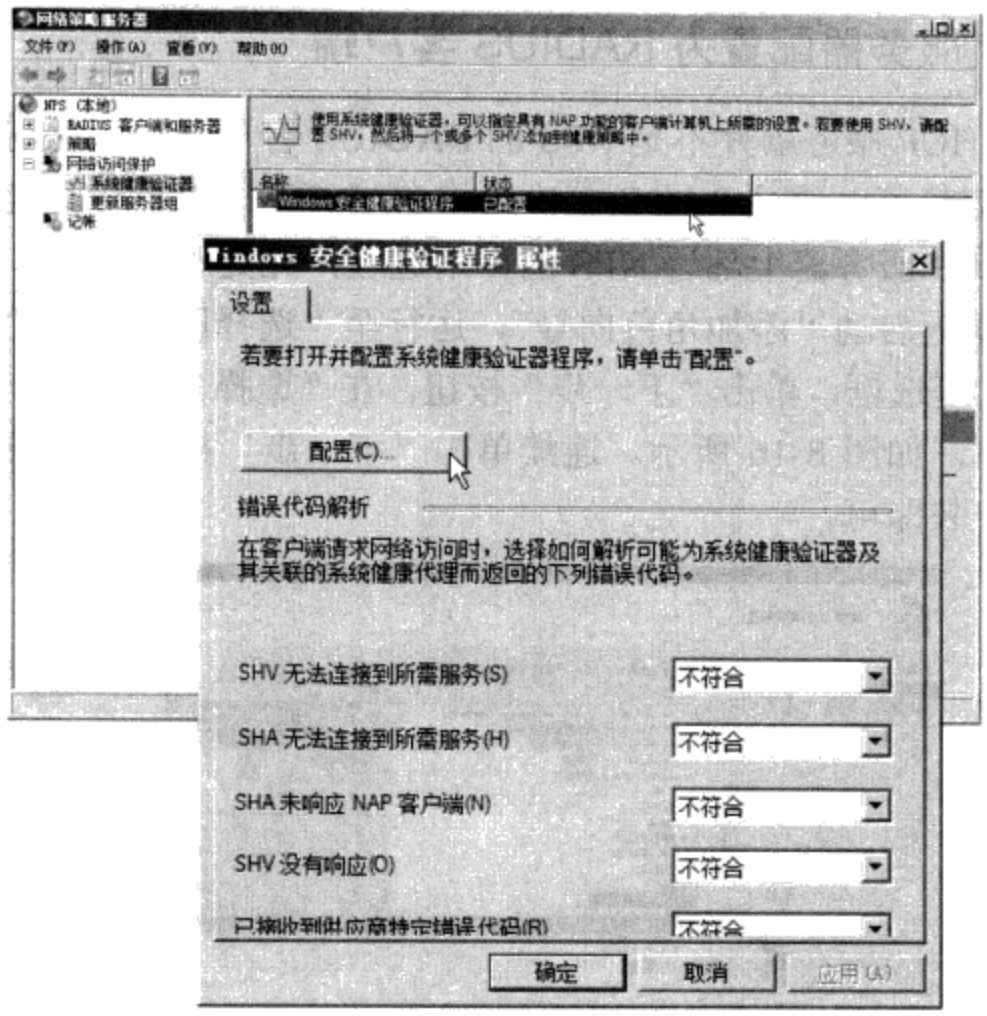


图 8-14 “Windows 安全健康验证程序 属性”对话框

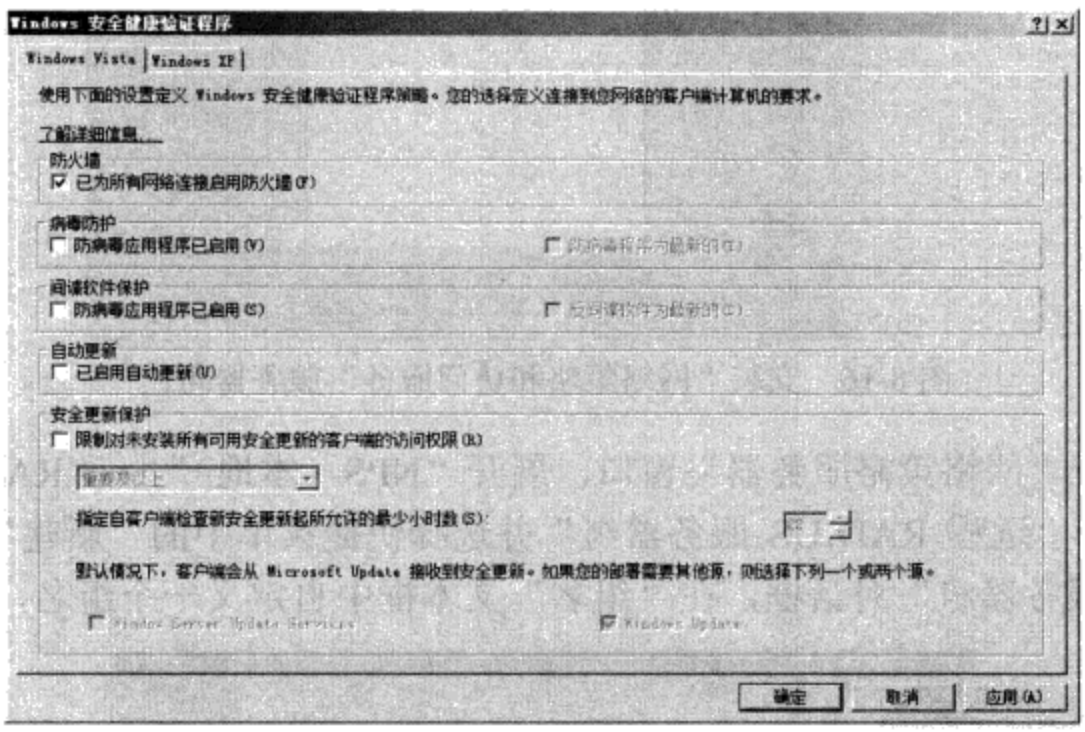


图 8-15 “Windows Vista”选项卡

第 3 步，单击“确定”按钮，保存配置。

8.4.3 配置 DHCP 服务器

当 DHCP 服务器被配置为 NPS 服务器，或者所在网络中新增 NPS 服务器后，原有 DHCP 服务将被新的包含 NPS 功能的组件所取代，管理员需要对 NPS 涉及的 DHCP 选项进行重新配置。默认状态下，NPS 关联的组件没有启用。

1. 将 DHCP 服务器配置为 RADIUS 客户端

默认情况下，DHCP 服务器并不是 NPS 的 RADIUS 客户端，因此需要安装“网络策略和访问”服务器角色，使其可以通过 RADIUS 协议将 NAP 客户端的健康状态（SoH）发送给 NPS。

第 1 步，在 DHCP 服务器上部署 NPS 的详细过程，此处不复赘述。

在 DHCP 服务器上启动“添加角色向导”，运行至“选择服务器角色”步骤时，选中“网络策略和访问服务”复选框，单击“下一步”按钮，在“选择角色服务”对话框中选中“网络策略服务器”复选框，如图 8-16 所示。连续单击“下一步”按钮，完成“网络策略和访问服务”服务器角色的安装即可。

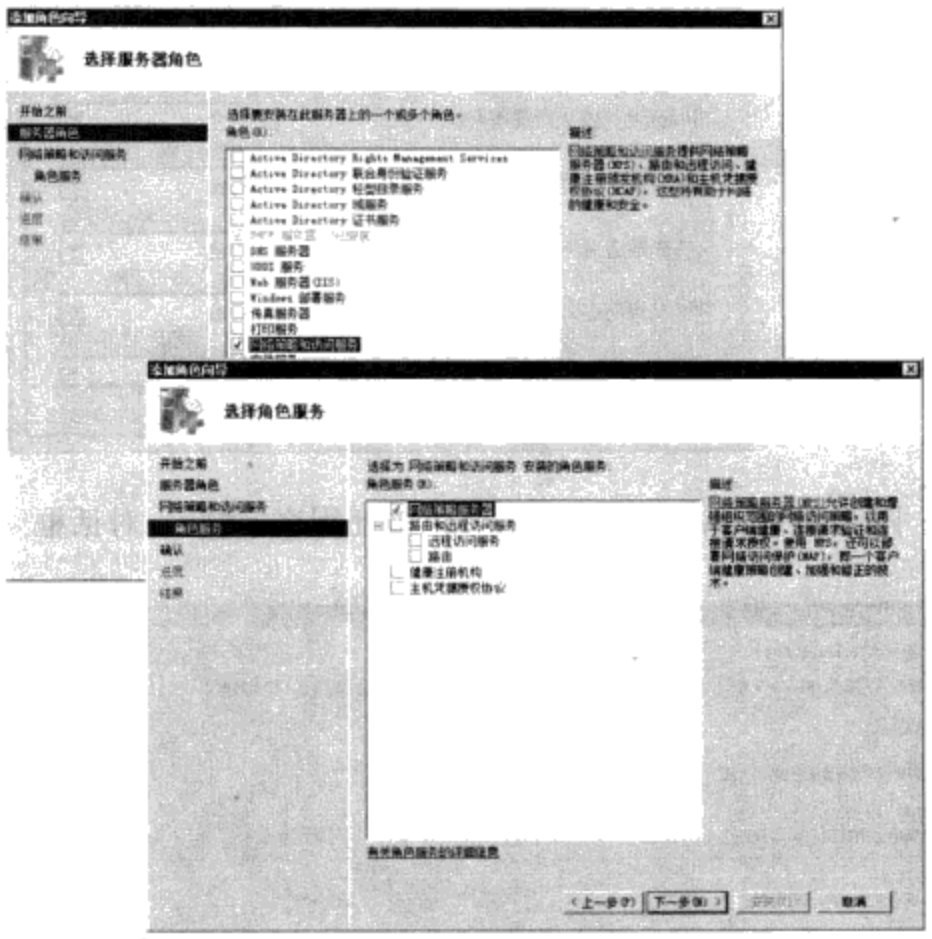


图 8-16　安装“网络策略和访问服务”服务器角色

第 2 步，打开“网络策略服务器”窗口，展开“NPS（本地）”→“RADIUS 客户端和服务器”选项，右击“远程 RADIUS 服务器组”并选择快捷菜单中的“新建”命令，显示“新建远程 RADIUS 服务器组”对话框，在“组名”文本框中自定义一个组名，如图 8-17 所示。

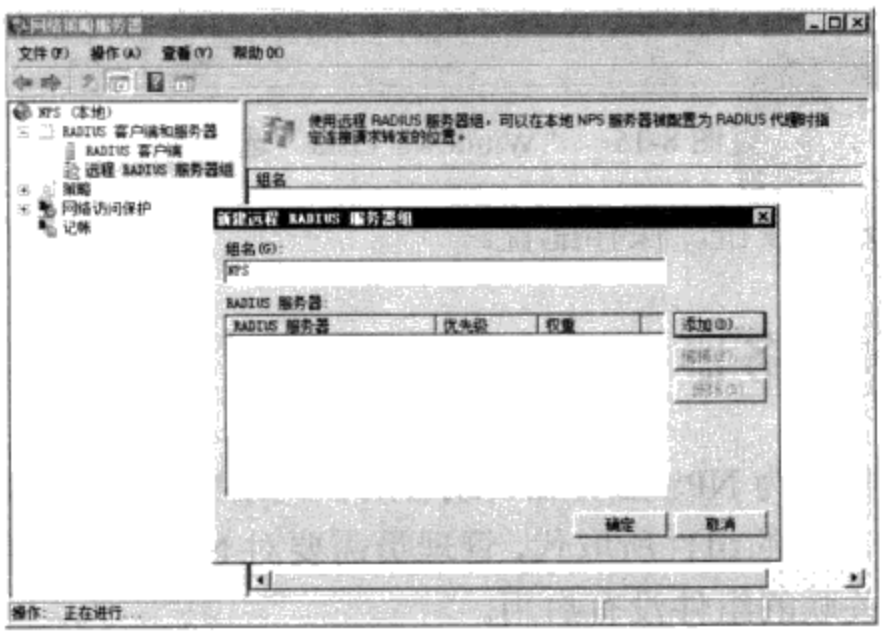


图 8-17　新建远程 RADIUS 服务器组

第 3 步，单击“添加”按钮，显示“添加 RADIUS 服务器”对话框，在“地址”选项卡的“服务器”文本框中输入远程 RADIUS 服务器（本例中 NPS 服务器就是 RADIUS 服务器）的主机名或 IP 地址即可。如果输入主机名，则可以单击“验证”按钮，查看解析所得的 IP 地址是否与主机名对应。切换到“身份验证/记账”选项卡，在“共享机密”和“确认共享机密”文本框中输入 NPS 端完全相同的密码，其他选项保持默认值即可，如图 8-18 所示。

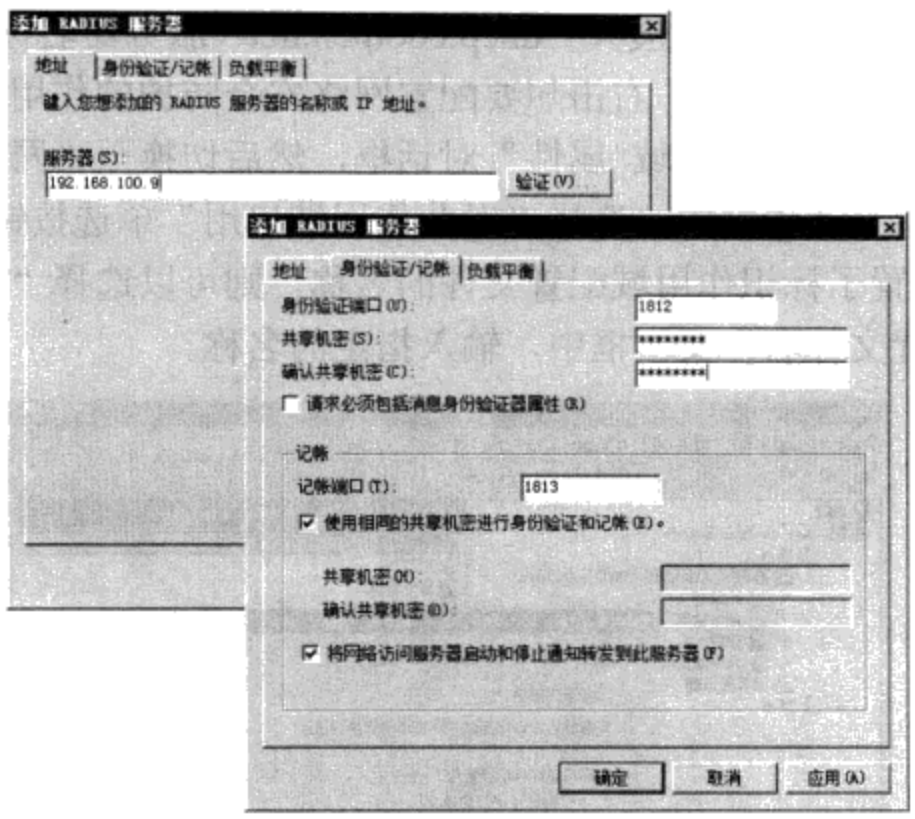


图 8-18 “添加 RADIUS 服务器”对话框

第 4 步，连续单击“确定”按钮保存配置。在“网络策略服务器”窗口中，展开“策略”→“连接请求策略”选项，双击“所有用户使用 Windows 身份验证”策略，显示如图 8-19 所示“所有用户使用 Windows 身份验证 属性”对话框，切换到“设置”选项卡，在“设置”列表框中单击“身份验证”选项，在右侧窗口中选择“将请求转发到以下远程 RADIUS 服务器组进行身份验证”单选按钮，同时在下拉列表框中选择刚刚创建的远程 RADIUS 服务器组。

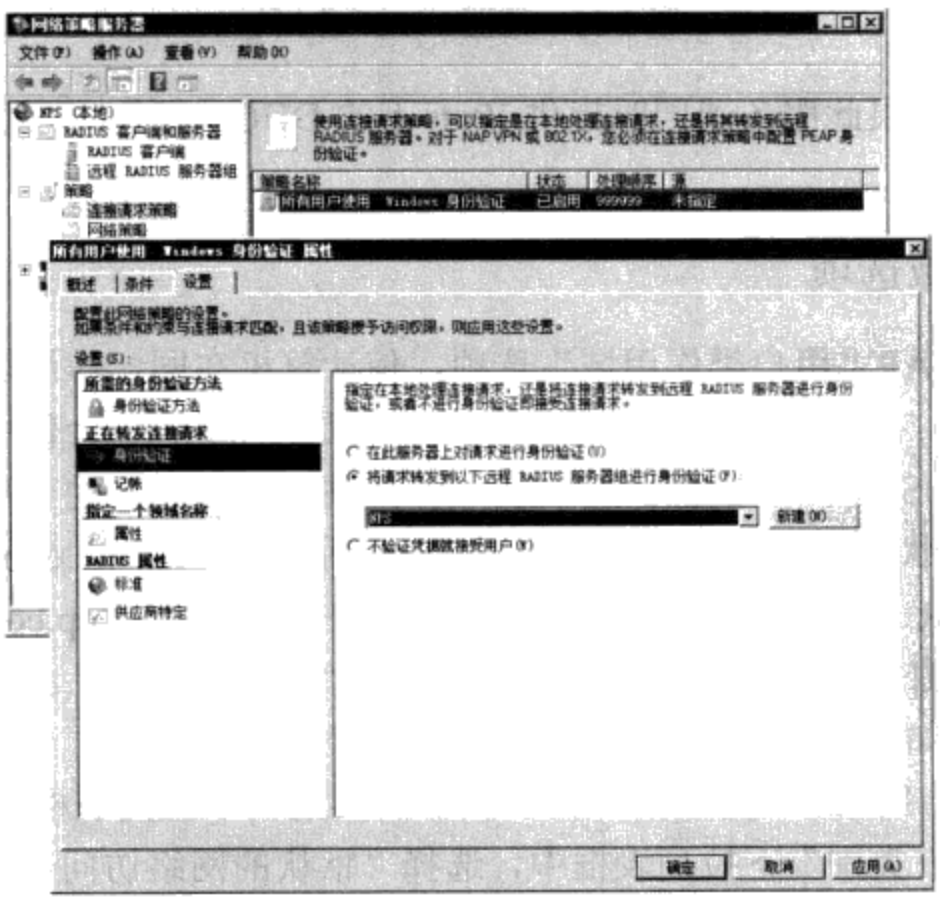


图 8-19 “所有用户使用 Windows 身份验证 属性”对话框

第5步，单击“确定”按钮，保存配置。

2. 配置强制作用域

NPS 安装完成后，在 DHCP 作用域属性中，添加了一项“网络访问保护”选项卡，默认情况下，该设置没有启用，需要网络管理员启用该设置。

在 DHCP 控制台窗口中，依次展开“dhcp.coolpen.net（服务器名称）”→“IPv4”，显示当前 DHCP 上的所有作用域。首先，右击想要配置网络安全防护的作用域并在弹出的快捷菜单中选择“属性”选项，打开“作用域 属性”对话框，然后切换至“网络访问保护”选项卡。在“网络访问保护设置”选项框中，选择“对此作用域启用”单选按钮，如图 8-20 所示。如果在 NPS 服务器上设置了标识作用域配置文件的名称，则可以选择“使用自定义配置文件”单选按钮，并在“配置文件名”文本框中，输入指定的名称。

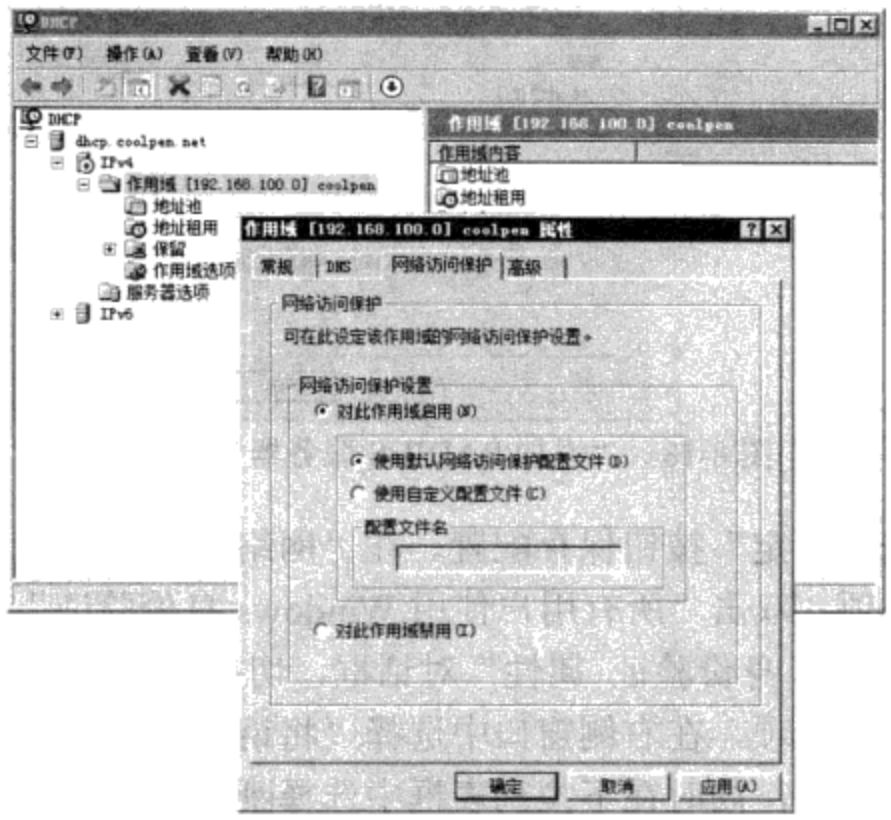


图 8-20 配置 DHCP 作用域

需要注意的是，如果此服务器同时提供 IPv6 下的 DHCP 服务，则还需要在 IPv6 的所有作用域中，执行相同操作。

3. 配置作用域选项

NAP 通过新的 NAP“用户类作用域”选项，使计算机在同一作用域内的受限网络和不受限网络访问之间切换。在为状态不良的客户端计算机提供租约时，会使用这组特殊的作用域选项（DNS 服务器、DNS 域名、路由器等）。例如，提供给状态良好的客户端的默认 DNS 后缀为“coolpen.net”，而状态不良的客户端提供的 DNS 后缀为“unsafe.coolpen.net”。

第 1 步，在“DHCP”管理窗口中，依次展开“DHCP”→“dhcp.coolpen.net（服务器名）”→“IPv4”→“作用域[192.168.100.0] coolpen”，右击“作用域选项”并选择快捷菜单中的“配置选项”选项，显示如图 8-21 所示“作用域 选项”对话框。

第 2 步，切换至“高级”选项卡，在“供应商类别”下拉列表框中，选择“DHCP 标准选项”选项；在“用户类别”下拉列表框中，选择“默认的网络访问保护级别”选项。在“可用选项”列表框中，选择“006 DNS 服务器”复选框，在“IP 地址”文本框中，输入网络中

DNS 服务器使用的 IP 地址，单击“添加”按钮。如果网络中有多个 DNS，可以逐次添加。如果发现 DNS 服务器的顺序错误，则可以单击“向下”或者“向上”按钮，调整 DNS 服务器的顺序，如图 8-22 所示。

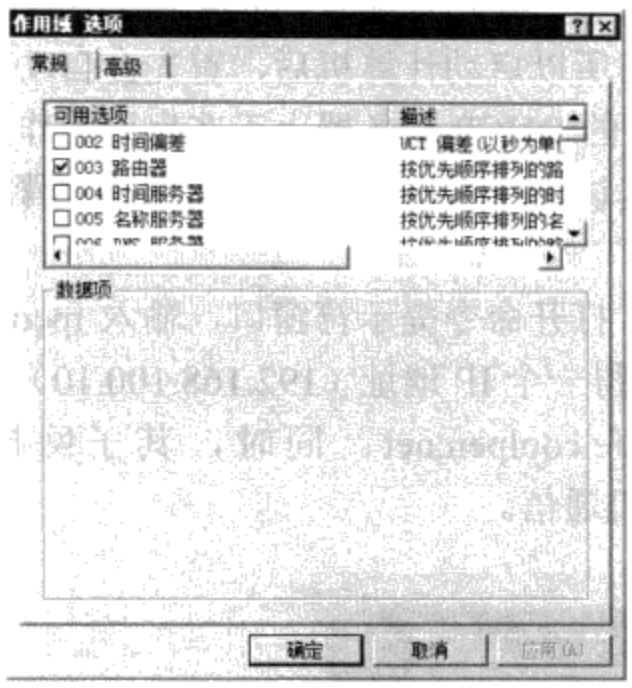


图 8-21 “作用域 选项”对话框

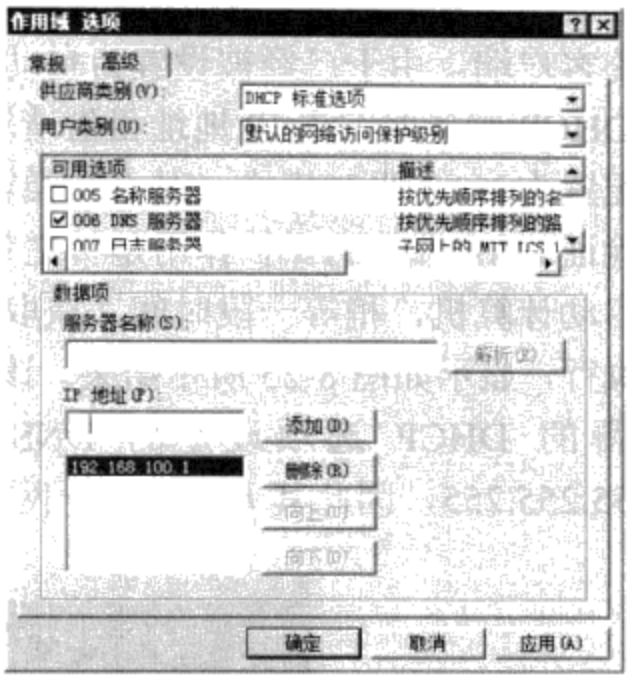


图 8-22 “高级”选项卡

第 3 步，在“可用选项”列表框中，选择“015 DNS 域名”复选框，在“数据项”选项区的“字符串值”文本框中，输入临时的 DNS 域名，如图 8-23 所示。

提示 临时域的域名和 DHCP 安装过程创建的域名不同，没有实际的作用，只是方便网络管理员区分连到网络中的计算机，哪些是安全的，哪些是不安全的。例如，如果计算机是安全的，则使用 coolpen.net 域名；如果计算机不是安全的，则使用这里指定的 unsafe.coolpen.net 域名。

第 4 步，单击“确定”按钮，完成服务器选项的设置，如图 8-24 所示。

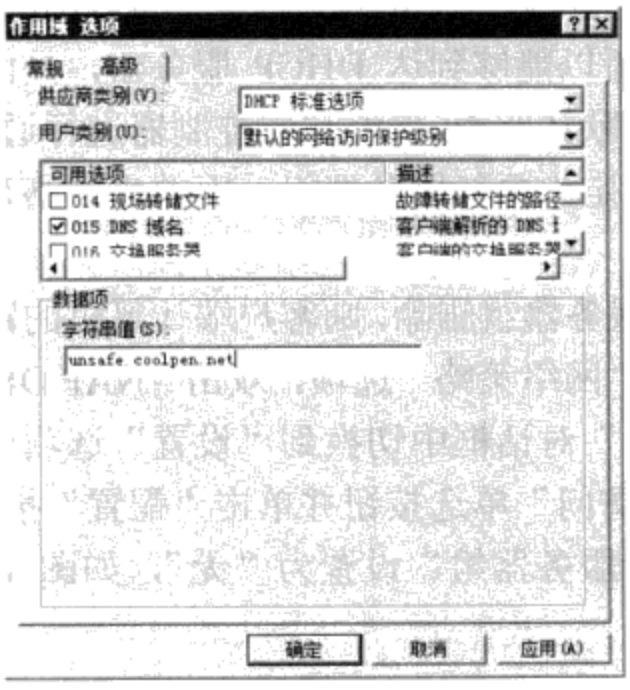


图 8-23 配置 DNS 域名选项

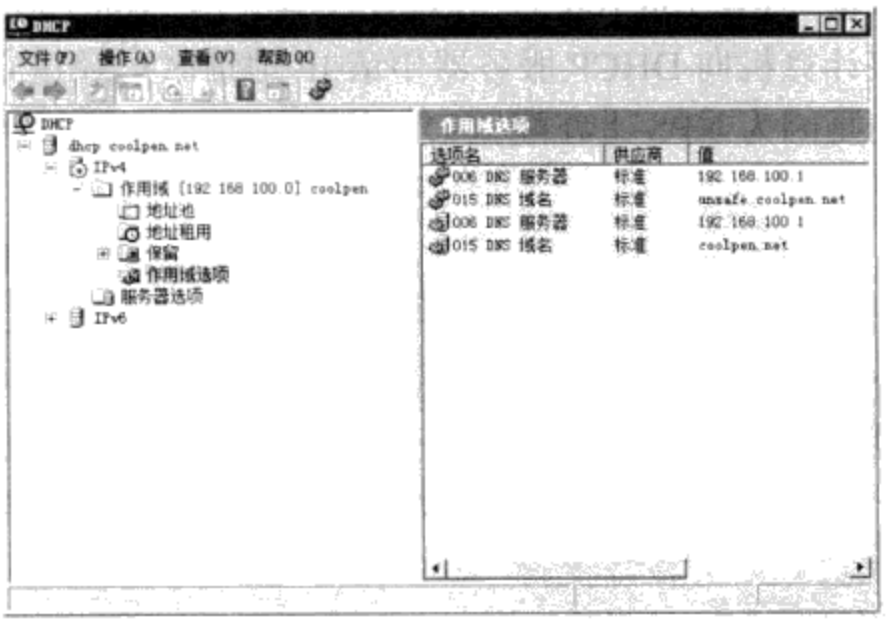


图 8-24 配置完成后的作用域选项

8.4.4 非 NAP 客户端测试

此时用于实验的客户端计算机尚未进行任何 NAP 客户端选项配置，即是一台不支持 NAP 功能的客户端。由于已经被设置为自动获取 IP 地址，所以启动计算机后，首先会自动向网络中的 DHCP 服务器发送 IP 地址租借请求，实验环境中的 DHCP 服务器上正在启用的作用域已经被配置为 NAP 强制模式，对于此类客户端只允许其访问受限网络，按照下面的步骤操作，即可验证 NAP 系统的保护作用是否生效。

启动计算机，稍等一段时间（获取 IP 地址）后，打开命令提示符窗口，输入 ipconfig 命令并执行，显示如图 8-25 所示结果。该计算机已经获得一个 IP 地址（192.168.100.10）但是它所获得的 DHCP 选项设定的 DNS 后缀是 unsafe.coolpen.net。同时，其子网掩码为 255.255.255.255，因此其无法和同一网络中其他计算机通信。

图 8-25 成功获取 IP 地址

继续输入“route print -4”命令并执行，显示如图 8-26 所示结果，可以查看当前计算机的所有 IPv4 路由表信息。从结果中可以看出，目前该计算机可以到达的远程主机包括 DHCP 服务器（192.168.100.5）和域控制器（192.168.100.1）。之所以能够到达 DHCP 服务器，是因为该计算机向 DHCP 服务器申请 IP 地址时已经建立了一条默认路由。能够与域控制器进行通信，则是因为 NPS 上在配置 DHCP 强制策略时将域控制器指定为更新服务器组，而首先网络是可以访问更新服务器组的。

如果在 NPS 上将非 NAP 客户端强制策略中的更新服务器组删除，则客户端计算机的路由表信息也会发生相应的变化。在 NPS 上展开“策略”→“网络策略”选项，双击“NAP DHCP 不支持 NAP”策略，在“NAP DHCP 不支持 NAP 属性”对话框中切换到“设置”选项卡，单击“NAP 强制”选项，在右侧窗口中选择“允许受限访问”单选按钮并单击“配置”按钮，在“更新服务器和疑难解答 URL”对话框中，将“更新服务器组”设置为“无”，如图 8-27 所示。

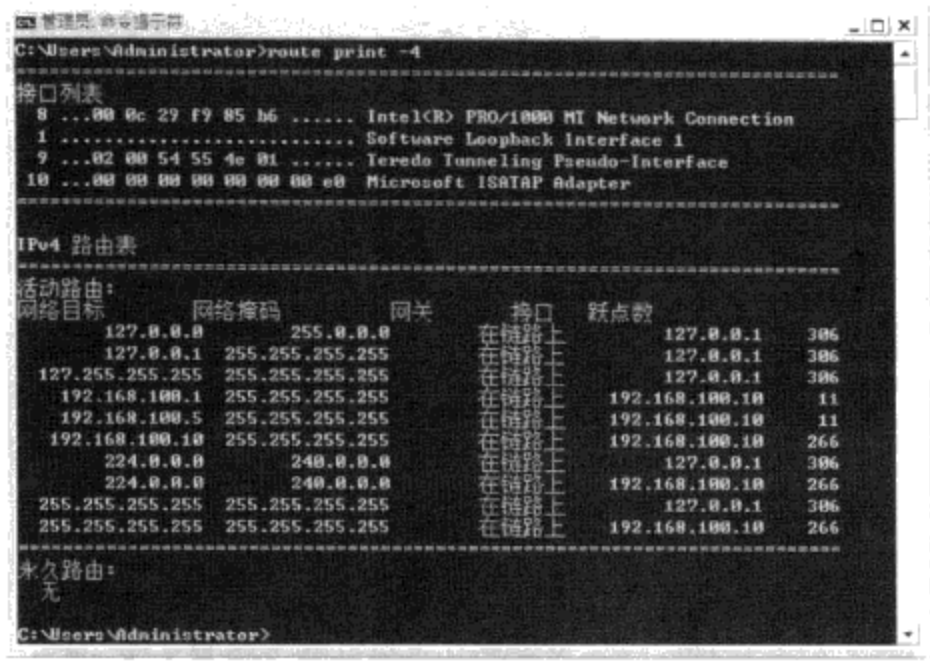


图 8-26　查看路由表信息

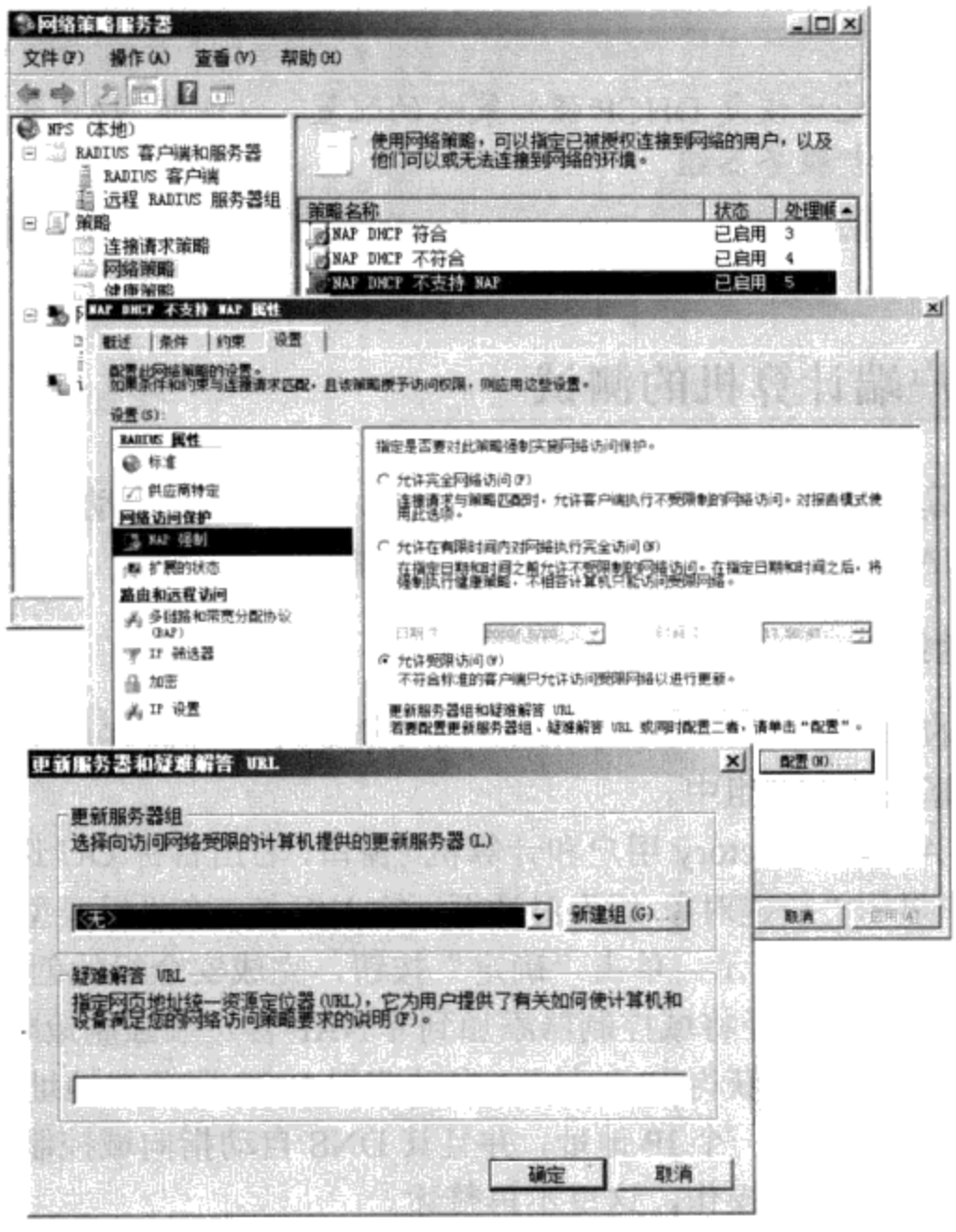


图 8-27　暂时取消更新服务器组

此时再返回到 Vista 客户端计算机，首先运行“ipconfig -renew”命令重新获取 IP 地址，虽然还可以从 DHCP 服务器获得相同的 IP 地址，但是此时的路由表中已经删除了到域控制器的路由，如图 8-28 所示。

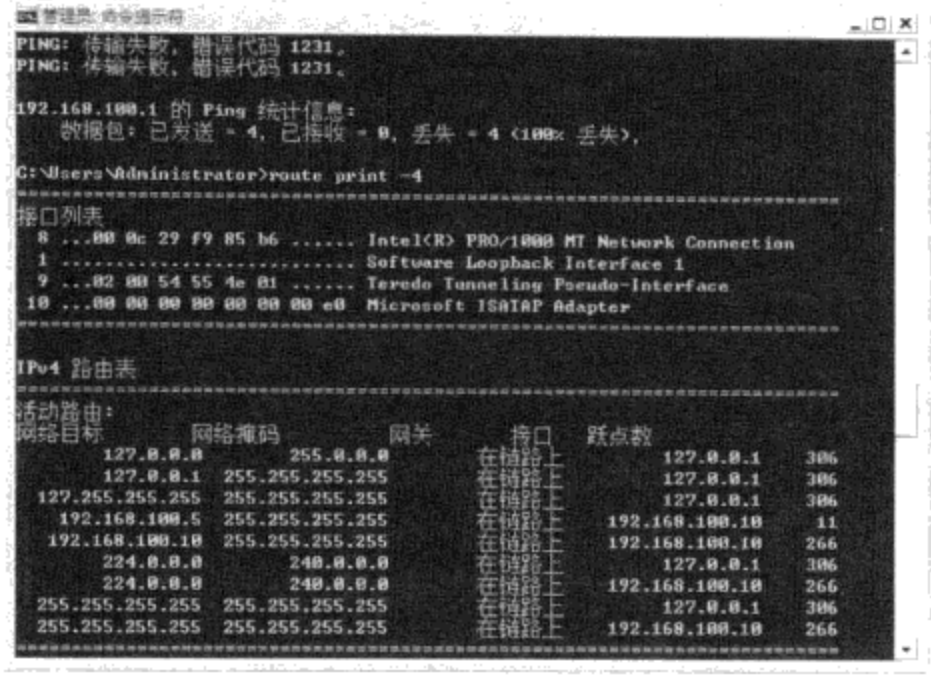


图 8-28 无法与域控制器通信

提示 测试完毕之后恢复 DHCP 强制策略的配置，以便非 NAP 客户端可以在受限网络中访问更新服务器组。

8.4.5 域中客户端计算机的测试

如果客户端计算机已经加入到域，则管理员可以通过组策略自动配置 NAP 客户端，使支持 NAP 功能的非 NAP 客户端自动配置为 NAP 客户端。

1. 建立安全组

为了便于管理 NAP 客户端，可以在域控制器上创建用于存储客户端计算机的安全组，然后将域中的指定计算机加入到组中。

第 1 步，打开“Active Directory 用户和计算机”窗口，右击目标 OU 选择快捷菜单中的“新建”→“组”命令，显示“新建对象-组”对话框，输入组名，在“组类型”选项区域选择“安全组”单选按钮，如图 8-29 所示。单击“确定”按钮，完成安全组的创建。

第 2 步，由于在 NPS 上已经将域控制器添加到非 NAP 客户端强制策略的更新服务器组中，所以局域网中被设置为“自动获得 IP 地址”“自动获得 DNS 服务器地址”的所有客户端计算机，都可以从受限网络中获得一个 IP 地址，并且其 DNS 自动指向域控制器，因此是可以加入域的。客户端计算机加入域的操作，这里不再赘述。

第 3 步，将客户端计算机添加到安全组。在“Active Directory 用户和计算机”窗口中，双击新创建的“NAP 客户端”安全组，在“NAP 客户端 属性”对话框的“成员”选项卡中，单击“添加”按钮，显示如图 8-30 所示“选择用户、联系人、计算机或组”对话框，在“输入对象名称来选择”文本框中，输入客户端计算机的名称，单击“检查名称”按钮以确认计算机是否存在。

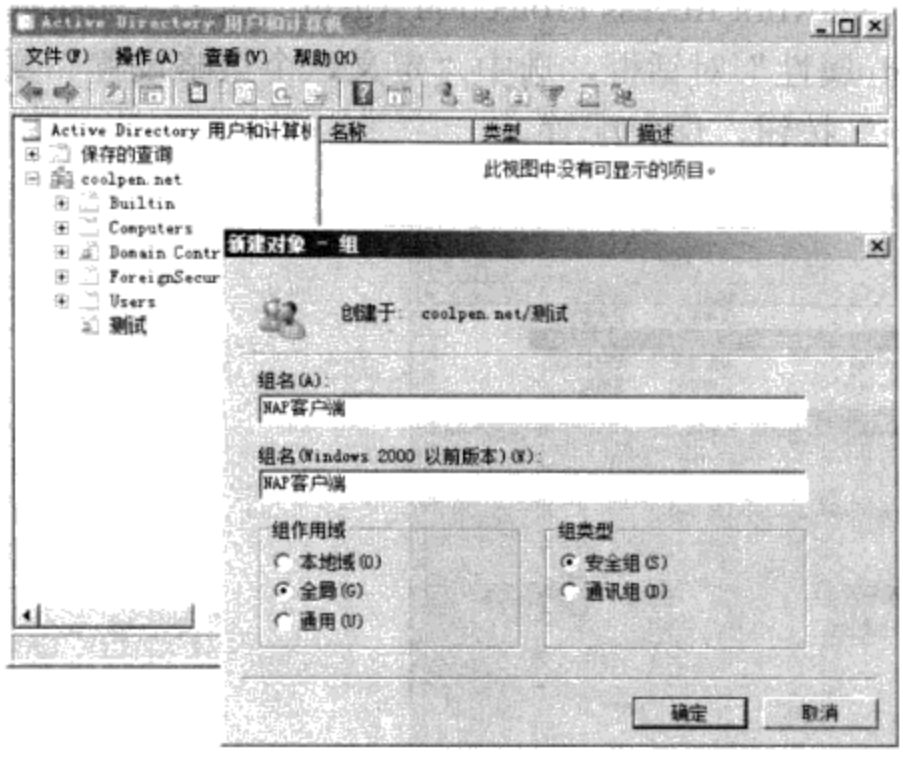


图 8-29 创建安全组

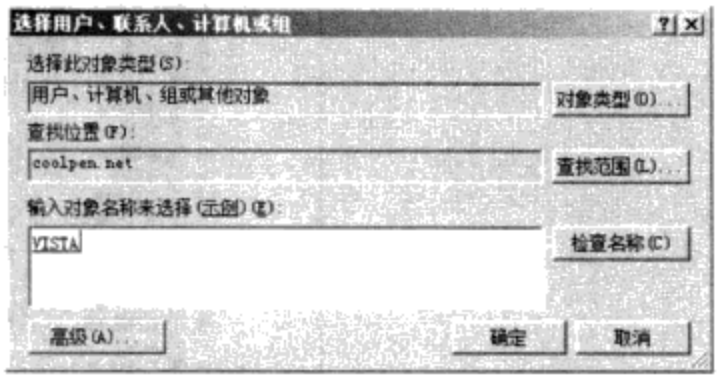


图 8-30 “选择用户、联系人、计算机或组”对话框

提示 默认情况下可能无法选择“计算机”对象，此时可以单击“对象类型”按钮，选中“对象类型”列表中的“计算机”复选框即可。

第 4 步，单击“确定”按钮，即可将客户端计算机添加到安全组中，继续单击“确定”按钮，保存配置。

2. 使用组策略配置 NAP 客户端

第 1 步，在域控制器上依次打开“开始”→“管理工具”→“组策略管理”选项，显示“组策略管理”窗口，新建作用域客户端计算机安全组所在 OU 的组策略对象，如图 8-31 所示。

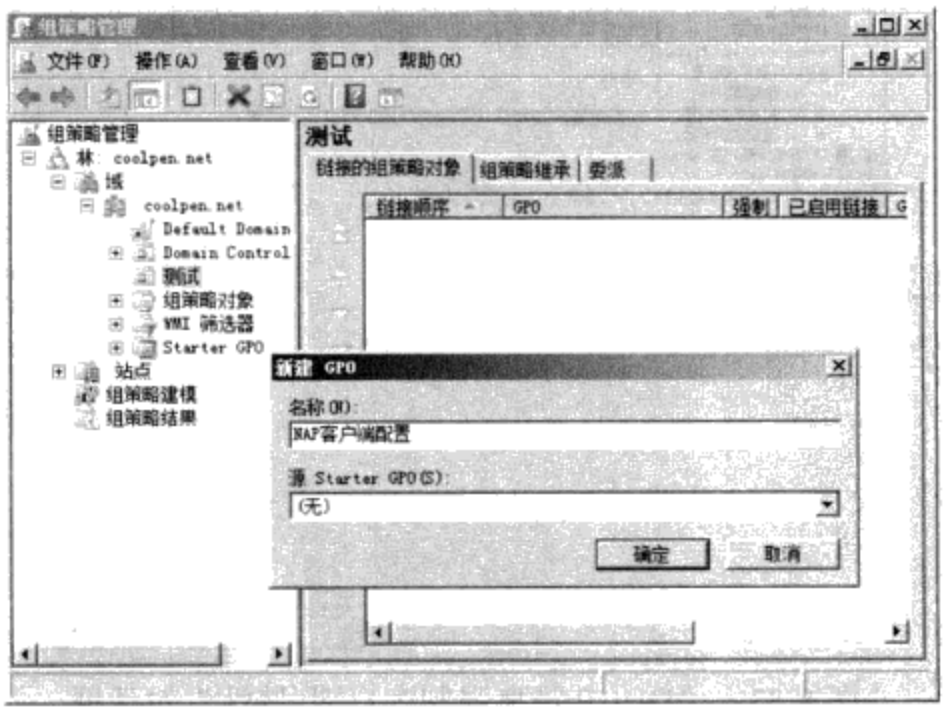


图 8-31 新建组策略对象

第 2 步，直接编辑新建组策略，依次展开“计算机配置”→“策略”→“Windows 设置”

→“安全设置”→“系统服务”选项，双击“Network Access Protection Agent”服务，显示如图 8-32 所示“Network Access Protection Agent 属性”对话框，选中“定义这个策略设置”复选框，并选择“自动”单选按钮。单击“确定”按钮，保存配置。

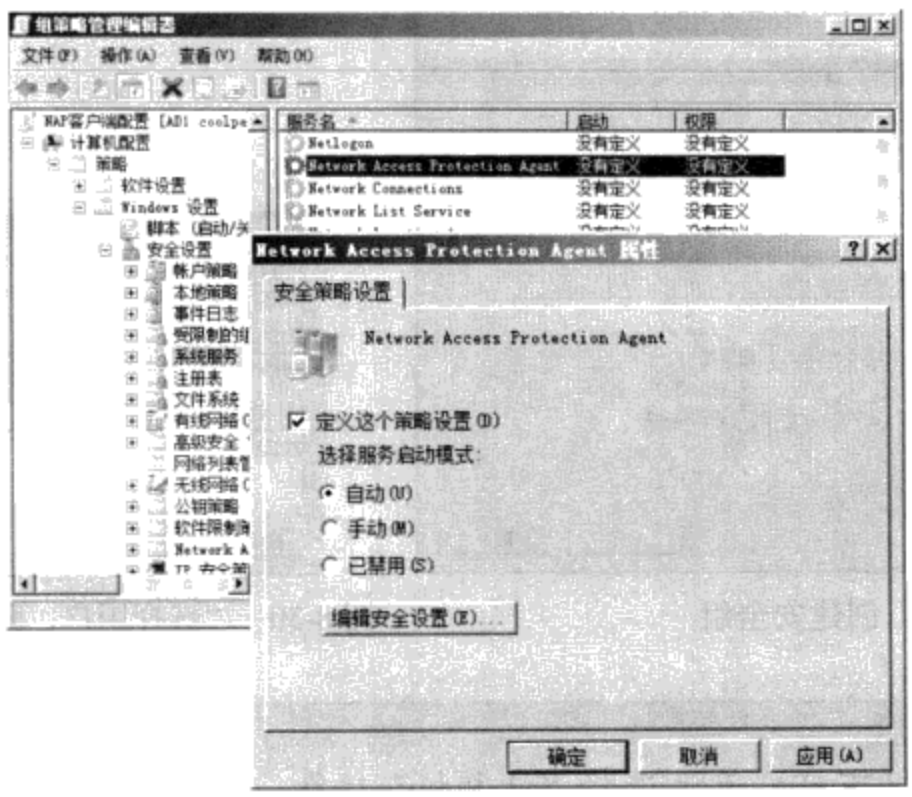


图 8-32　“Network Access Protection Agent 属性”对话框

第 3 步，依次展开“计算机配置”→“策略”→“Windows 设置”→“安全设置”→“Network Access Protection”→“NAP 客户端配置”→“强制客户端”选项，双击“DHCP 隔离强制客户端”显示如图 8-33 所示“DHCP 隔离强制客户端 属性”对话框，选中“启用此强制客户端”复选框。

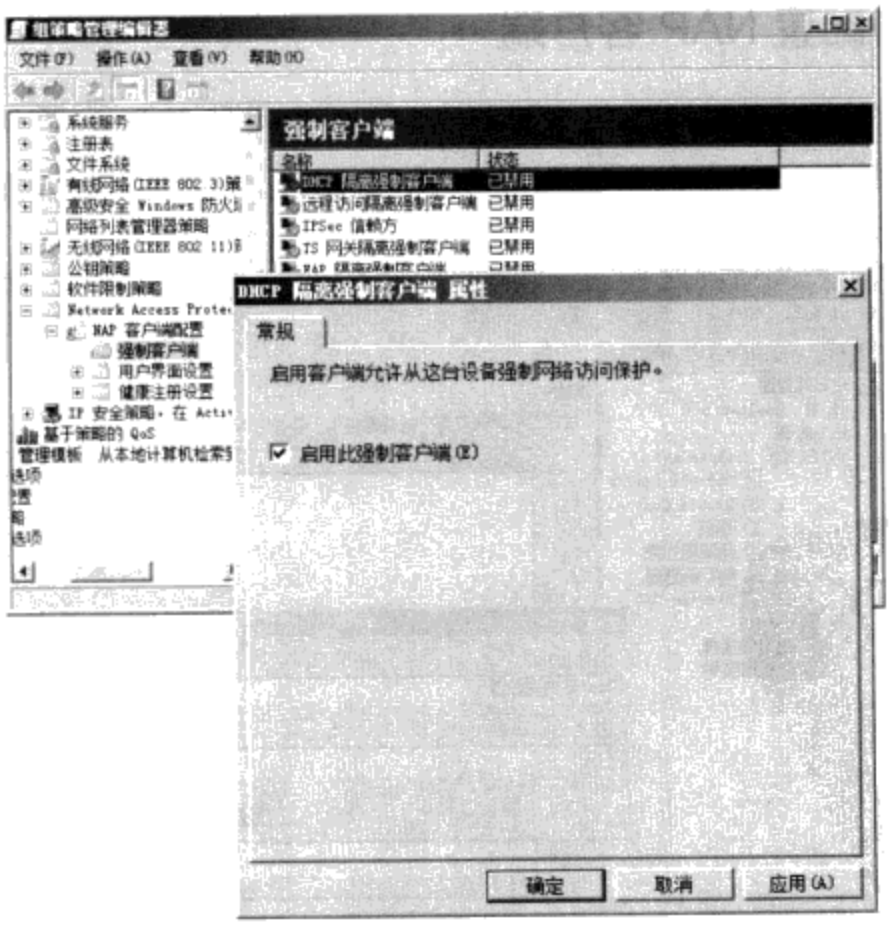


图 8-33　“DHCP 隔离强制客户端 属性”对话框

第 4 步，单击“确定”按钮，保存配置。关闭“组策略编辑器”窗口时显示如图 8-34 所示“NAP 客户端配置”对话框。单击“是”按钮即可。

第 5 步，在“组策略管理”窗口中配置组策略对象的“安全筛选”，以确保该策略只部署在 NAP 客户端计算机上，而不会对其他用户或计算机造成影响。选择“NAP 客户端配置”选项，在“作用域”选项卡的“安全筛选”区域内选中系统默认的“Authenticated Users”对象，单击“删除”按钮将其删除，如图 8-35 所示。

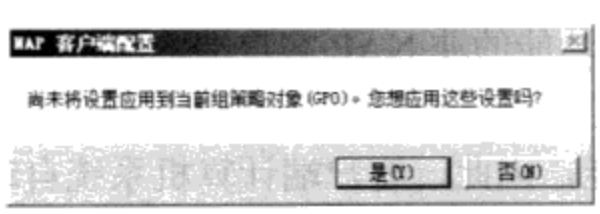


图 8-34 “NAP 客户端配置”对话框

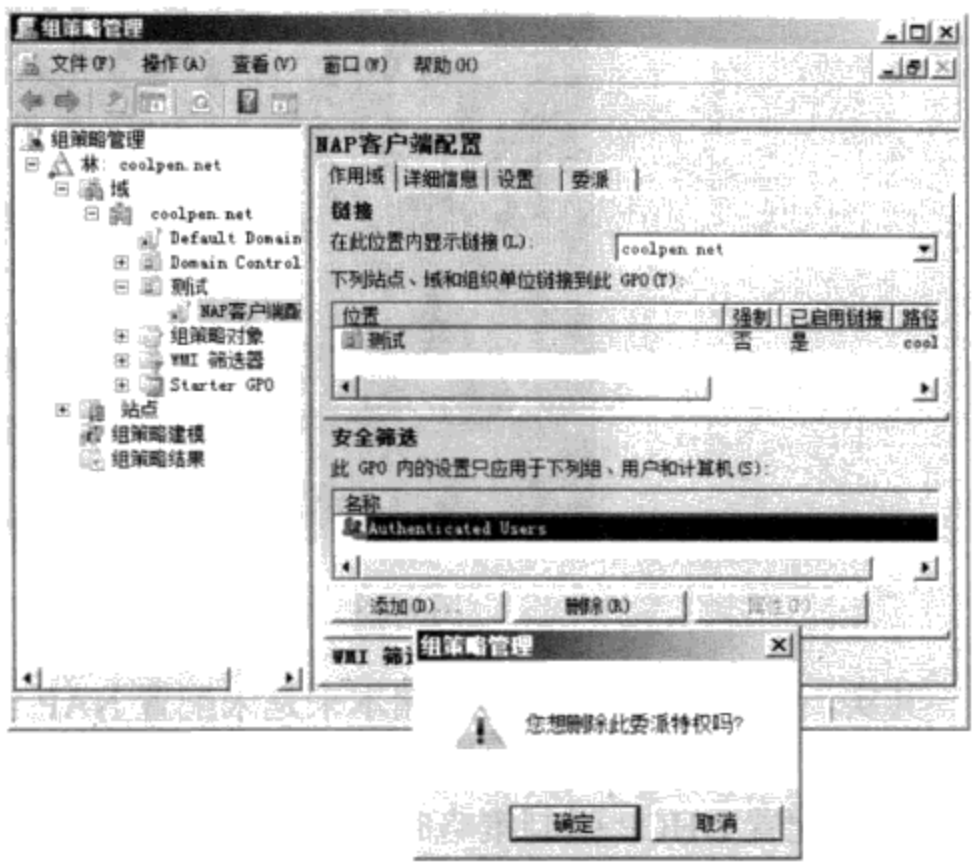


图 8-35 从作用域中删除其他对象

第 6 步，单击“添加”按钮，显示如图 8-36 所示“选择用户、计算机或组”对话框，将已创建的“NAP 客户端”安全组，添加到“安全筛选”列表框中。

3. 检查 NAP 客户端状态

重新启动客户端计算机或者使用“gpupdate –force”命令强制刷新策略，即可成功应用域控制器上部署的 NAP 客户端策略。如果成功应用，计算机将自动被配置为 NAP 客户端。打开命令提示符窗口，输入并执行如下命令，即可检查客户端配置是否成功，执行结果如图 8-37 所示，可以看到“DHCP 隔离强制客户端”已经成功启用。

```
netsh nap client show grouppolicy
```

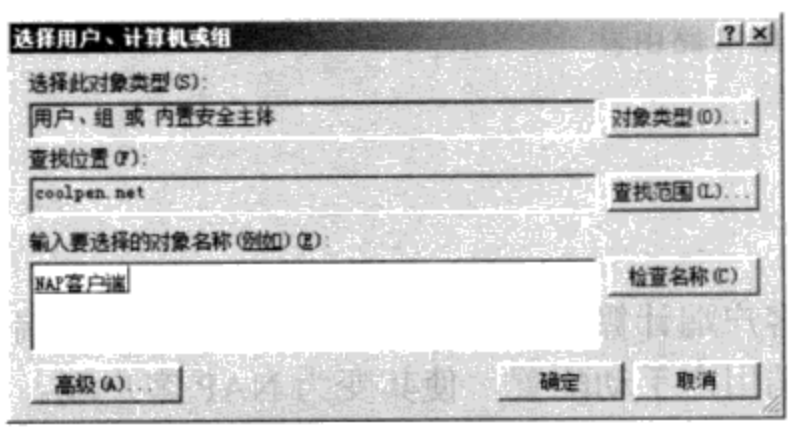


图 8-36 “选择用户、计算机或组”对话框

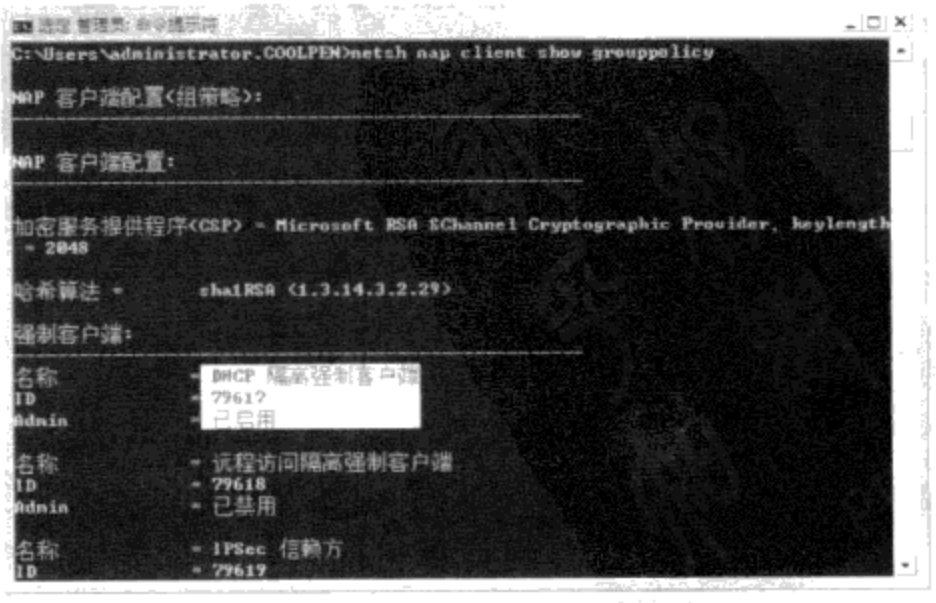


图 8-37 检查 NAP 客户端状态

继续输入“ipconfig”命令，检查此时获得的 IP 地址及 DNS 后缀的状态变化，显示如图 8-38 所示结果。此时获得的 IP 地址仍为 192.168.100.10，但是子网掩码已经变为 255.255.255.0，即可以和网络的计算机正常通信。

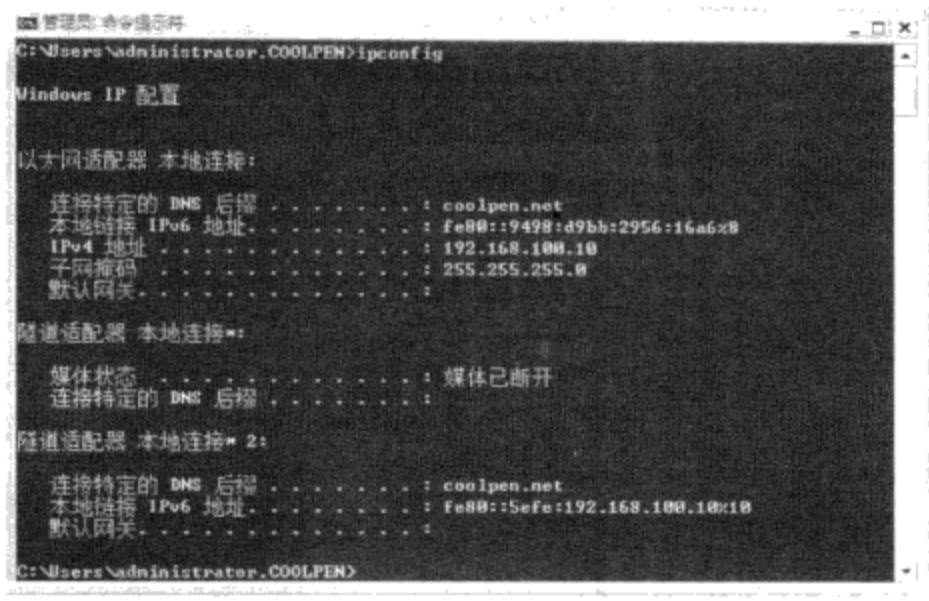


图 8-38　健康状态下获得的 IP 地址信息

其实，加入域的 Vista 客户端本来是未配置 NAP 客户端功能的非 NAP 客户端，但是客户端登录到域后将自动应用域控制器上部署的组策略，因此会自动被配置为 NAP 客户端。另外，在 NPS 上配置 DHCP 强制策略时启用了客户端自动更新功能，因此，客户端计算机系统自动开启了 Windows 防火墙，符合了健康策略的要求，所以此时的 DNS 后缀已经变为正常状态——“coolpen.net”。

此时，运行“route print -4”命令检查路由信息，显示如图 8-39 所示结果，已经建立到 192.168.100.0 网络的路由。

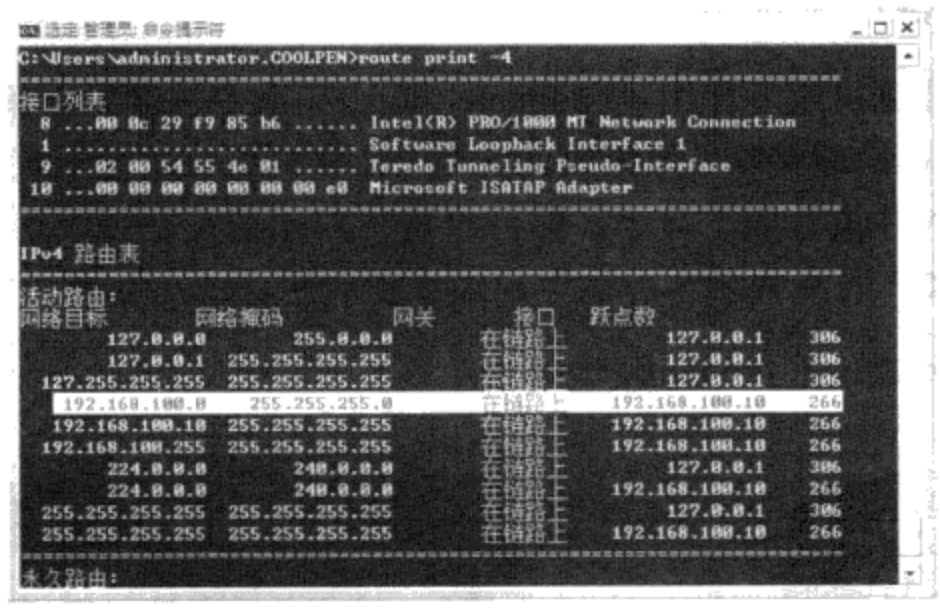


图 8-39　健康客户端的 IPv4 路由表

8.4.6 不健康 NAP 客户端的测试

无论是 Windows Vista/7 还是 Windows XP SP3 客户端计算机，默认均为启用 NAP 客户端功能，对于独立工作组计算机而言，则只能由客户端用户手动配置，使其变为 NAP 客户端。

1. 手动配置 NAP 客户端

将一台运行 Windows Vista 系统的计算机配置为 NAP 客户端，需要依次进行修改计算机策略、配置 NAP 客户端组件和配置 NAP 客户端代理组件等操作。如果客户端计算机已经加入域，则可以通过组策略统一部署；工作组方式的客户端计算机则可以通过手动方式逐一配置。这里已手动配置为例加以介绍。

■ 配置 NAP 客户端

Windows Vista 操作系统中，默认已经内置了 NAP 客户端组件，用户只需进行简单配置即可。

第 1 步，单击“开始”按钮，在“开始搜索”文本框中，输入“napclcfg.msc”并按 Enter 键，显示“NAP 客户端配置”窗口。依次选择“NAP 客户端配置（本地计算机）”→“强制客户端”选项，在右侧“强制客户端”窗口中，右击“DHCP 隔离强制客户端”，选择快捷菜单中的“启用”命令，如图 8-40 所示。

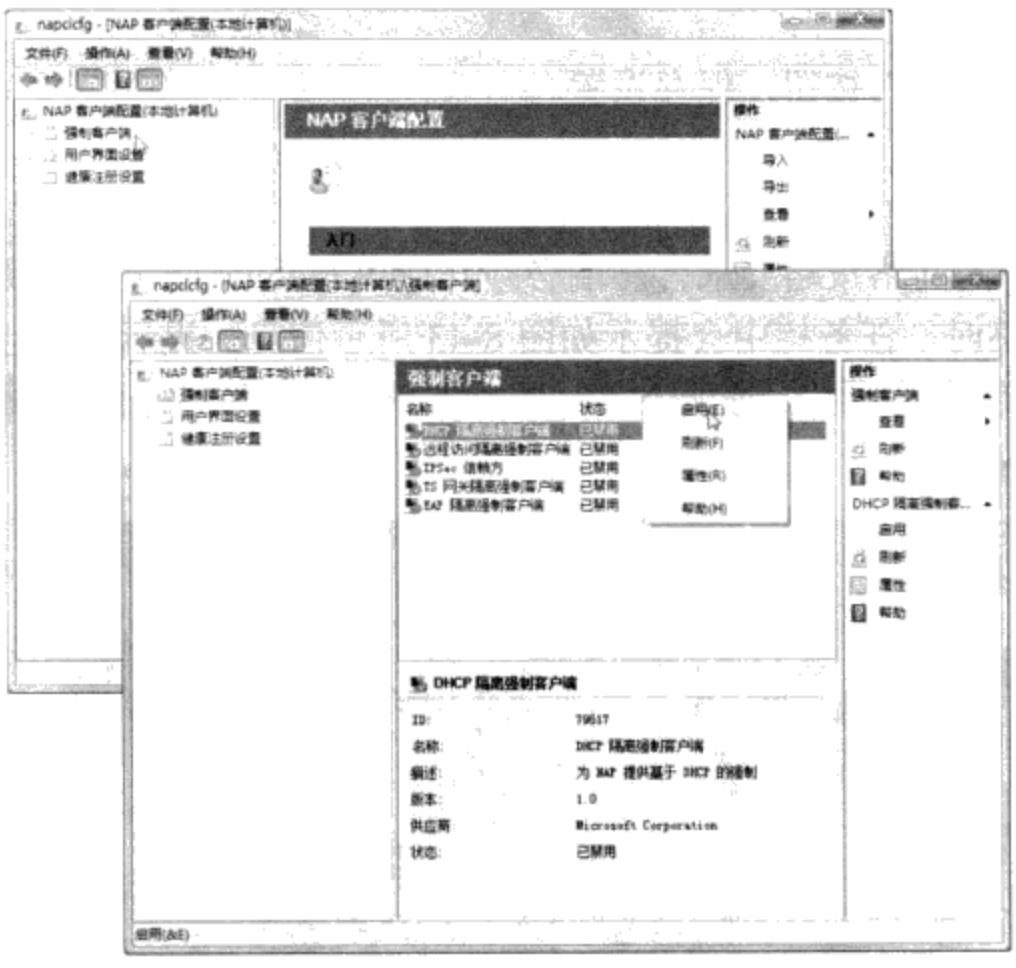


图 8-40 启用“DHCP 隔离强制客户端”

第 2 步，将“DHCP 隔离强制客户端”设置为启用状态后，关闭窗口即可。

■ 配置 NAP 代理服务

NAP 代理服务全称为“Network Access Protection Agent”服务，在默认情况下禁止使用，建议将其设置为随系统自动启动。

第 1 步，依次选择“开始”→“控制面板”→“管理工具”→“服务”选项，打开“服务”窗口。Network Access Protection Agent 服务的默认状态是未启动的，如图 8-41 所示。

第 2 步，右击“Network Access Protection Agent”服务，选择快捷菜单中的“属性”选项，显示如图 8-42 所示“Network Access Protection Agent 的属性”对话框。在“启动类型”下拉

列表框中选择“自动”方式，单击“启动”按钮，启动该服务。

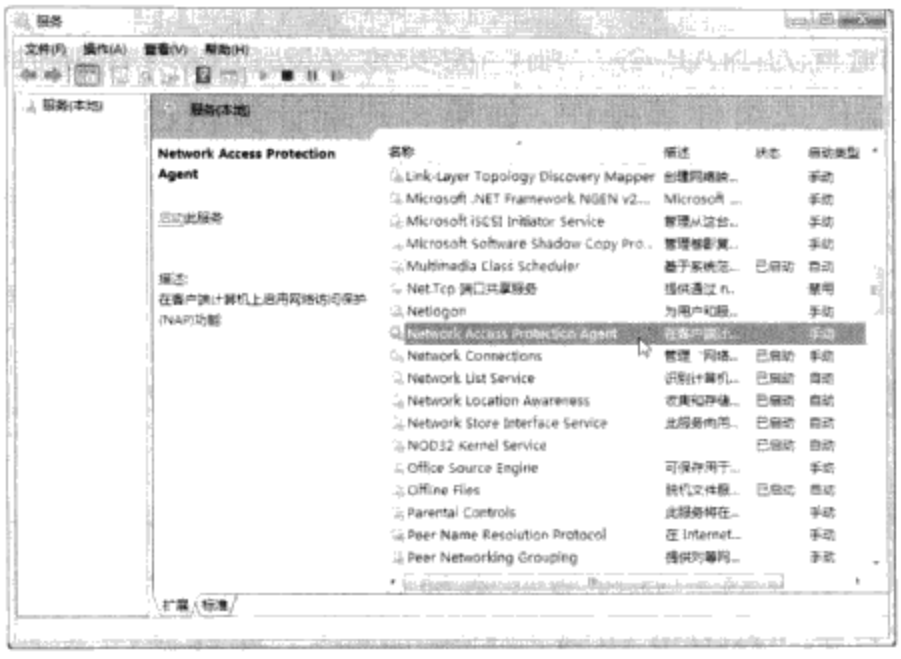


图 8-41　“服务”窗口

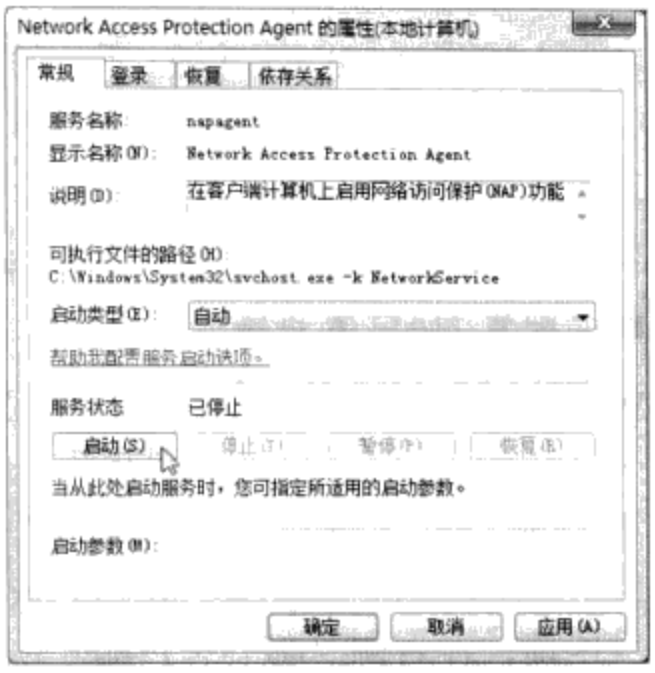


图 8-42　“Network Access Protection Agent 的属性”对话框

第 3 步，单击“确定”按钮，保存设置。

2. 客户端测试

由于本例实验中的网络策略要求客户端必须开启 Windows 防火墙，所以当禁用防火墙的 NAP 客户端访问网络时，任务栏中会提示如图 8-43 所示信息，提示“此计算机不符合该网络的要求，网络访问权限受限制”。证明 NAP 服务器开始发挥作用。此时如果查看已获得的 IP 信息，会发现其子网掩码为 255.255.255.255，即无法正常访问网络。

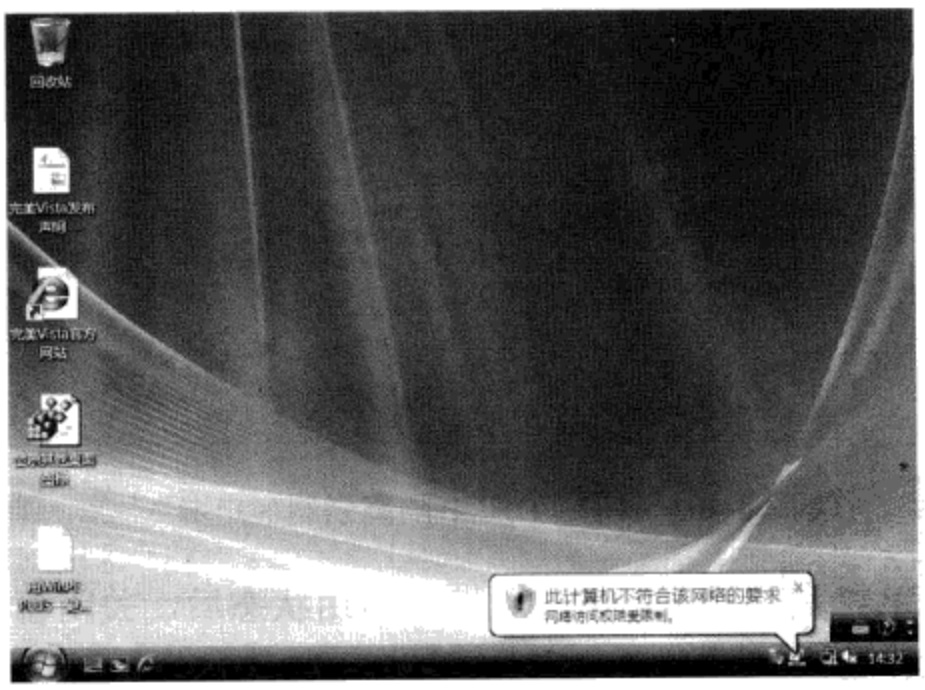


图 8-43　不符合策略要求的客户端

如果仅对防火墙状态进行评估，而 NPS 上的不健康 NAP 客户端的 DHCP 强制策略中启用了客户端自动更新功能，则 Windows 将自动启用防火墙，使其达到健康状态。这里为了便于演示客户端手动配置计算机的过程，暂时取消客户端自动更新功能，即取消“自动更新”区域内的“启用客户端计算机的自动更新功能”复选框，如图 8-44 所示。

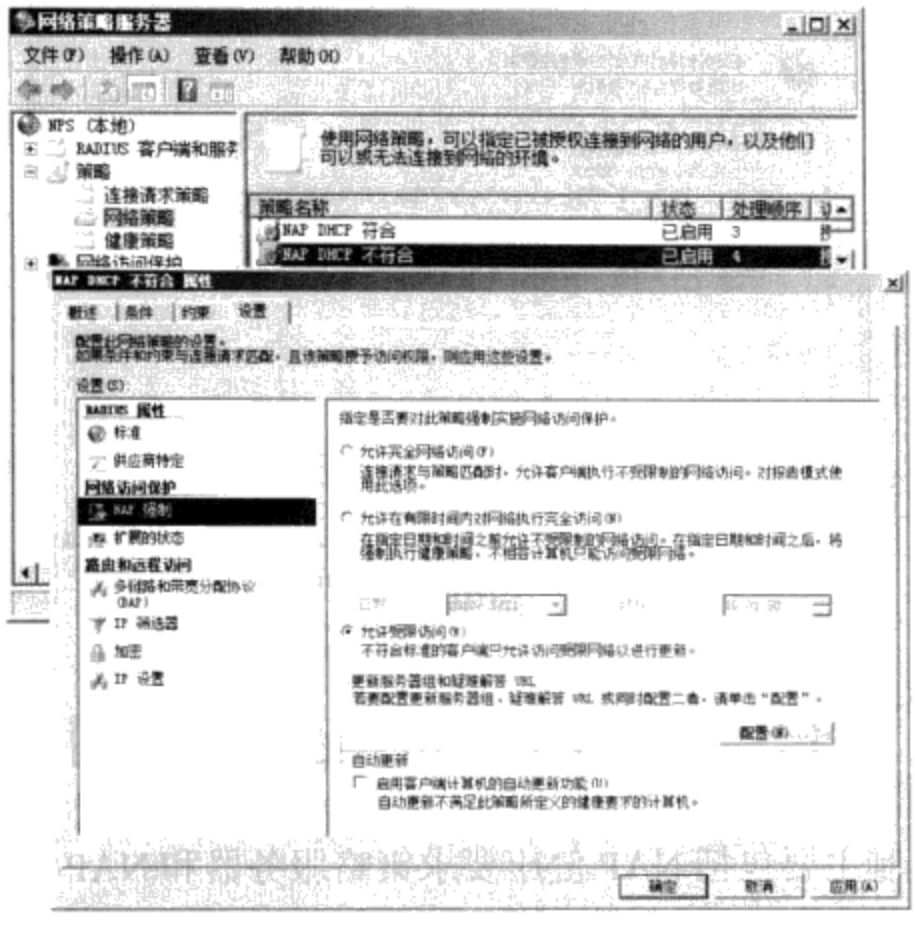


图 8-44　暂时取消客户端自动更新功能

此时该客户端不能继续访问网络中的某些服务器或计算机。单击提示信息，打开如图 8-45 所示“网络访问保护”窗口。该窗口中提示当前客户端未能通过网络策略检测的原因，并给出解决问题的方案。这些提示方法就是系统健康策略模板中管理员设定的处理操作。

用户可以根据提示信息尝试解决相关问题，本例中只针对系统防火墙状态进行评估，开启 Windows 防火墙即可。处理完毕后，任务栏中会出现如图 8-46 所示提示信息。

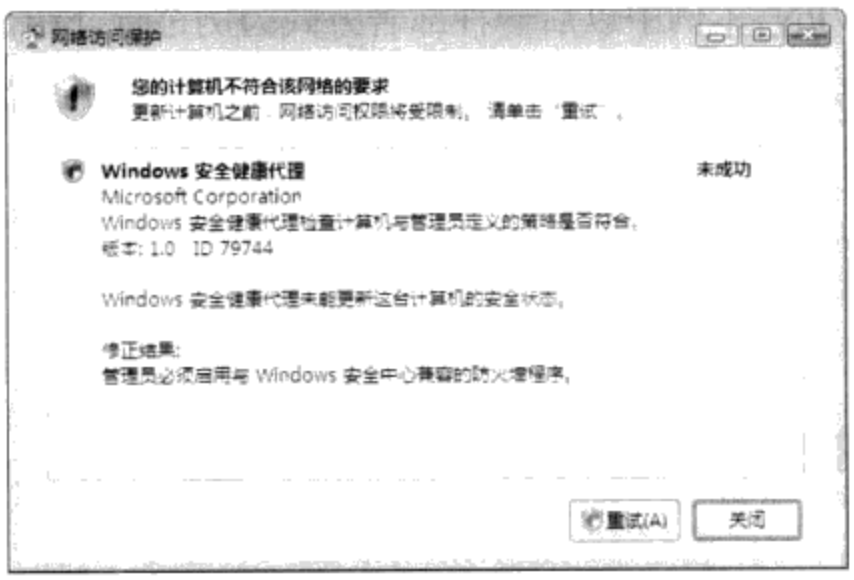


图 8-45　“网络访问保护”窗口

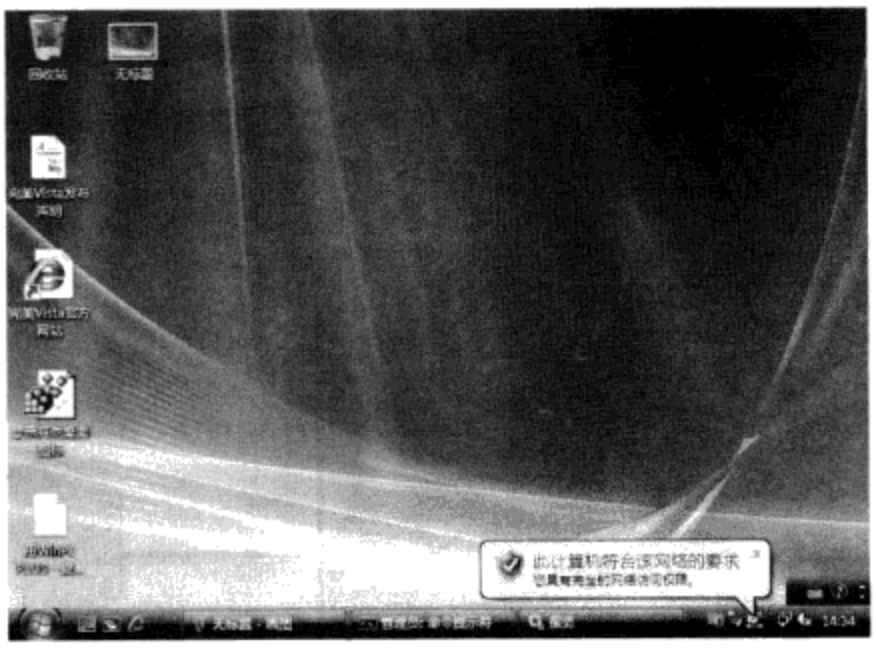


图 8-46　符合网络策略要求

此时，单击“此计算机符合该网络的要求”提示信息，会显示如图 8-47 所示“网络访问保护”窗口，已具有完全的网络访问权限。

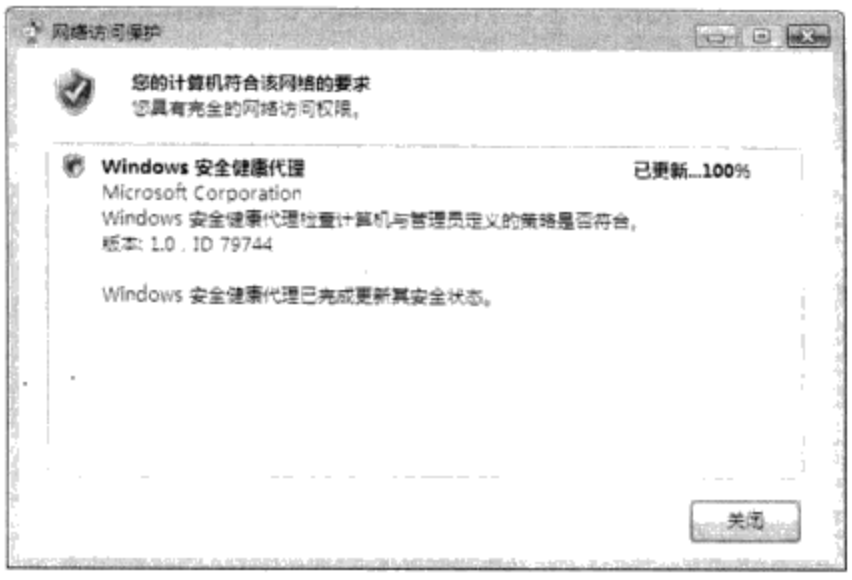


图 8-47　“网络访问保护”窗口

8.5　VPN 强制的配置与应用

NAP 中的 VPN 强制主要包括 NAP 健康要求策略服务器和 NAP 客户端上的远程访问隔离强制客户端。NAP 健康要求策略服务器评估 NAP 客户端的健康，并且指示远程访问 VPN 服务器限制不符合健康要求的策略的 NAP 客户端的访问。安装 NPS 过程中，安装向导会提示安装本地 CA，即在 NPS 服务器上安装 CA，这种模式偶尔会产生无法颁发证书的错误，建议，提前在域中部署专用的 CA。如果服务器资源紧张，也可以在域控制器上部署 CA。

8.5.1　网络环境概述

远程访问 VPN 服务器的部署方案有多种，如果使用硬件防火墙作为 Internet 接入设备，则可以在内网部署 VPN 服务器，然后将其发布到 Internet，如果使用 TMG 作为 Internet 接入代理服务器，则可以直接在 TMG 服务器上部署 VPN。本例中以后一种部署方式为例进行介绍，网络连接示意图如图 8-48 所示。

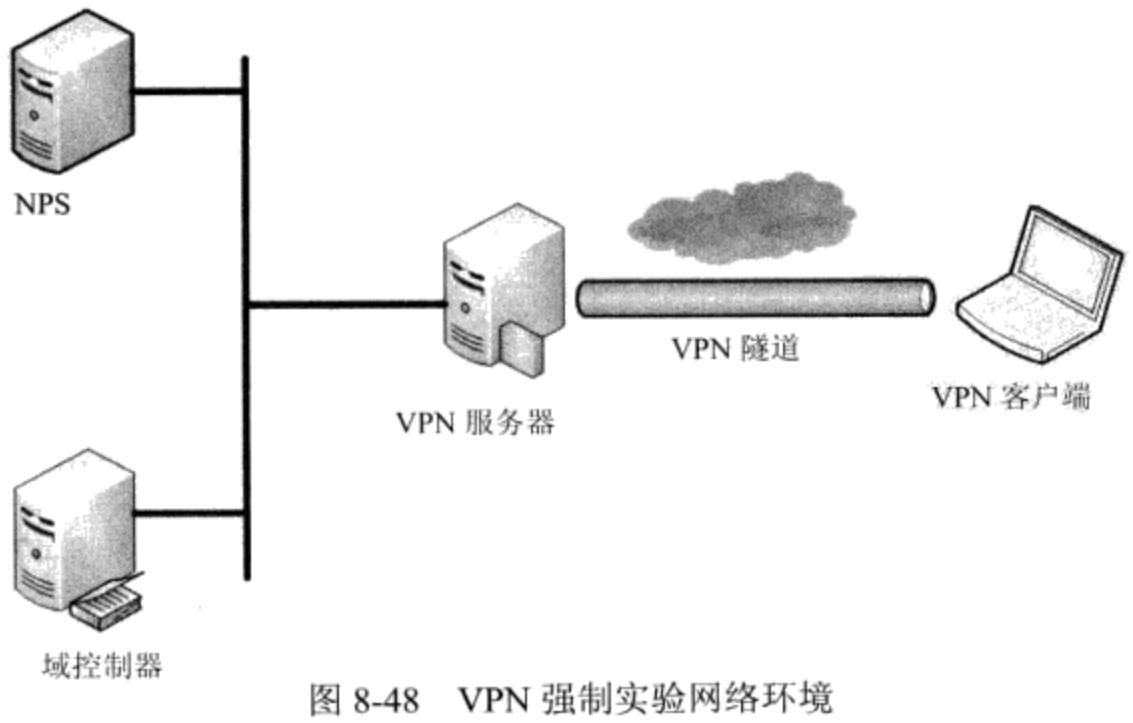


图 8-48　VPN 强制实验网络环境

1. 域控制器

域控制器除提供 Active Directory 域服务外，还提供 DNS 域名解析服务，同时还是企业证书颁发机构。由于 VPN 连接的 NAP 强制需要采用 PEAP 通信协议，因此，NPS 需要安装服务器证书，证书颁发机构是必不可少的。

2. VPN 服务器

VPN 服务器是 VPN 连接 NAP 强制系统的强制点，已经加入到域。由于需要将 VPN 客户端发送过来的请求发送给 NPS，因此必须配置 RADIUS 客户端，借助 RADIUS 协议将 VPN 客户端的健康状态（SoH）发送到 NPS。给 NAP 健康原则服务器。本例中使用部署在网络边缘的 TMG 服务器作为 VPN 服务器，其外网网卡 IP 地址为 211.82.218.242，内网网卡 IP 地址为 192.168.100.2。

3. NPS

NPS 已经加入到域，同时也是 RADIUS 服务器，用于接收并处理 VPN 服务器发送过来的 NAP 客户端健康状态（SoH）。

4. VPN 客户端

VPN 客户端计算机是运行 Windows Vista 系统的计算机，并且已经启用 NAP 客户端计算机的相关设置。

8.5.2 配置健康策略服务器

1. 为 NPS 申请计算机证书

计算机证书是进行 PEAP 通信必需的，由于 NPS 已经加入到域，所以可以通过“证书注册”向导向企业根 CA 申请计算机证书。

第 1 步，在 NPS 服务器上，打开“控制台”窗口。依次选择“文件”→“添加或删除管理单元”选项，打开“添加或删除管理单元”对话框，在“可用的管理单元”列表框中，选择“证书”单元。单击“添加”按钮，在“证书管理单元”对话框中，选择“计算机账户”单选按钮。然后单击“下一步”按钮，在“选择计算机”对话框中，选择“本地计算机”单选按钮，如图 8-49 所示。

第 2 步，依次单击“完成”和“确定”按钮，返回“控制台”窗口。依次展开“证书（本地计算机）”→“个人”选项，右击“个人”并选择快捷菜单中“所有任务”→“申请新证书”选项，显示“在您开始前”对话框。单击“下一步”按钮，显示如图 8-50 所示“申请证书”对话框，选中“计算机”复选框。

第 3 步，单击“注册”按钮，开始向网络中的 CA 提交证书申请，稍等即可成功。单击“完成”按钮，返回“控制台”窗口，如图 8-51 所示，即可看到成功注册的计算机证书。

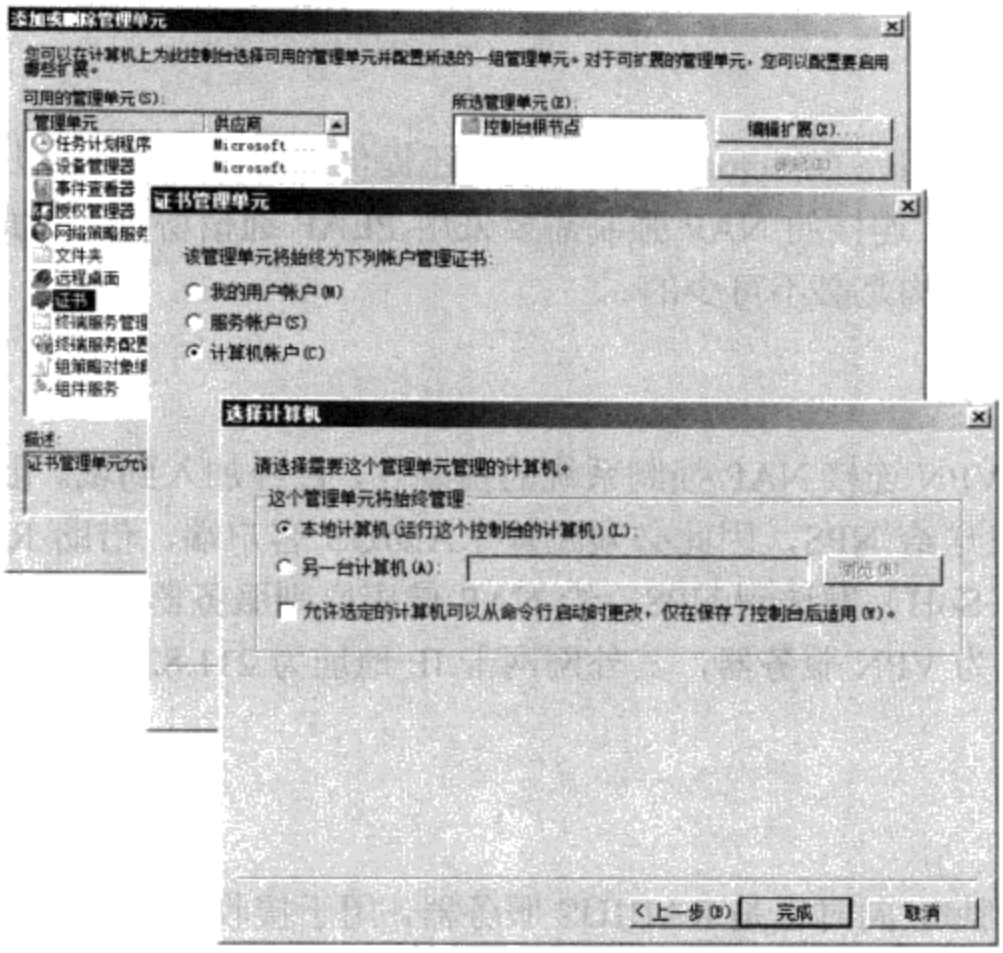


图 8-49　添加计算机证书控制台

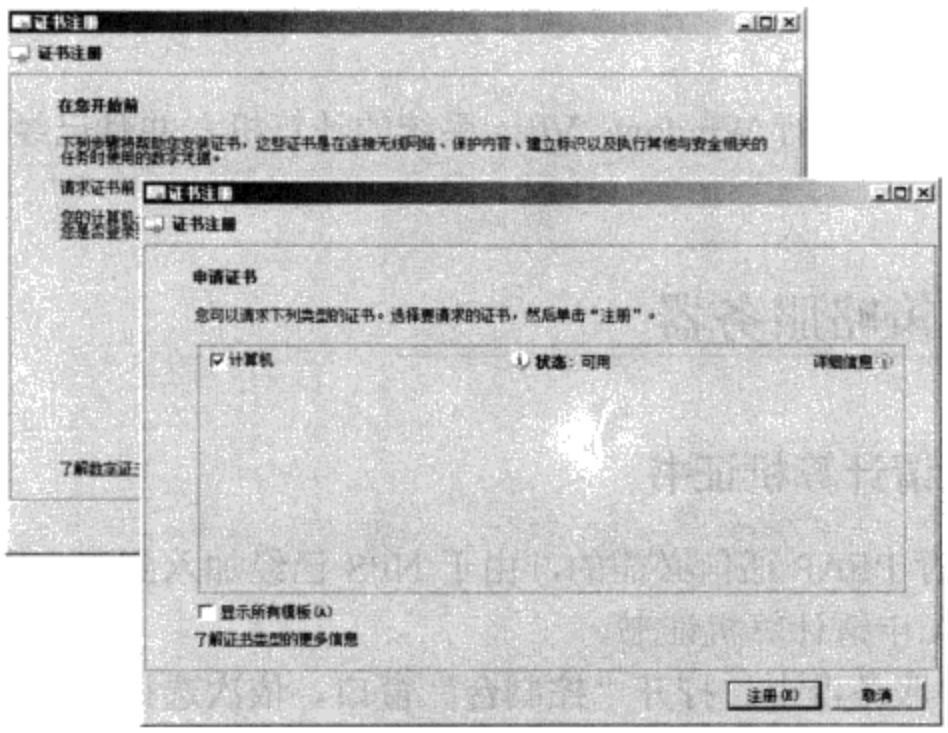


图 8-50　“申请证书”对话框

图 8-51　“控制台”窗口

2. 配置 VPN 强制策略

VPN 强制策略的配置方法与步骤同 DHCP 强制策略配置过程大同小异，这里只介绍重点操作步骤和不同之处。

第 1 步，在 NPS 上打开“网络策略服务器”窗口。展开“NPS”选项，在“标准配置”下拉菜单中选择“网络访问保护（NAP）”选项，单击“配置 NAP”超级链接，显示如图 8-52 所示“选择与 NAP 一起使用的网络连接方法”对话框。在“网络连接方法”中，选择“虚拟专用网络（VPN）”，在“策略名称”文本框中，输入对应的名称，建议使用默认名称。

第 2 步，单击“下一步”按钮，显示如图 8-53 所示“指定 NAP 强制服务器运行 VPN 服务器”对话框，由于 NAP 健康要求策略服务器已经是一个 RADIUS 服务器，本例中配置 VPN 服务器时，已经将 RADIUS 服务器指向该服务器。需要注意的是，必须在该服务器上设置与之对应的 RADIUS 客户端，双方才可以建立连接。

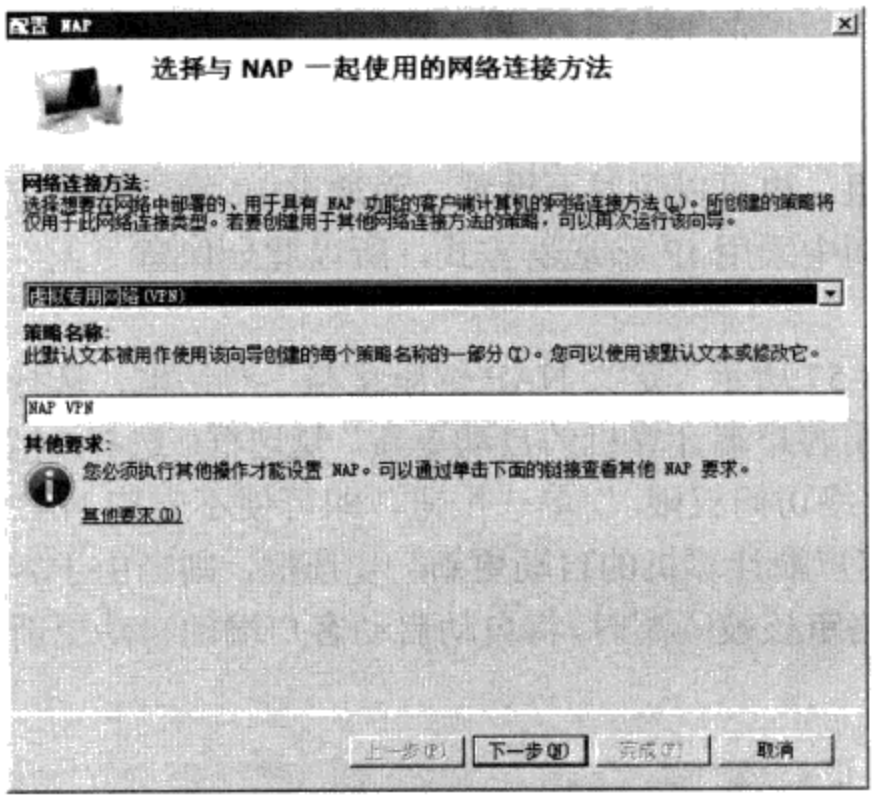


图 8-52 “选择与 NAP 一起使用的网络连接方法”对话框

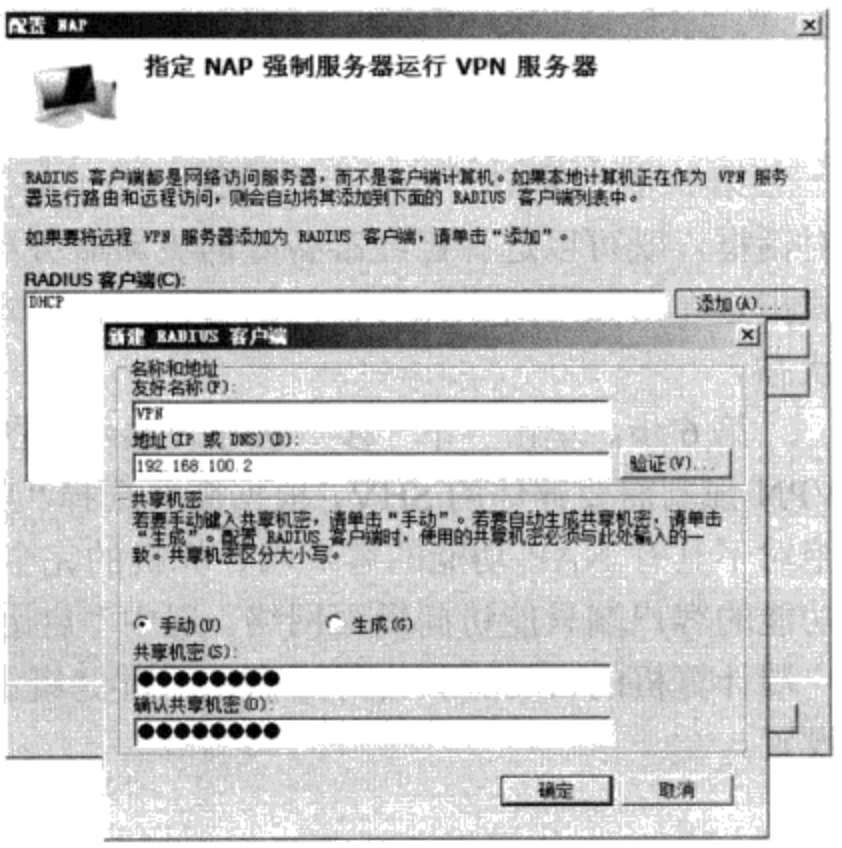


图 8-53 “指定 NAP 强制服务器运行 VPN 服务器”对话框

第 3 步，单击“确定”按钮，返回“指定 NAP 强制服务器运行 VPN 服务器”对话框。单击“下一步”按钮，显示如图 8-54 所示“配置用户组和计算机组”对话框，根据需要配置组。如果不选择，则将对所有计算机组和用户组有效。

第 4 步，单击“下一步”按钮，显示如图 8-55 所示“配置身份验证方法”对话框，为 PEAP 身份验证选择 NPS 所使用的计算机证书，即上述操作中申请的验证证书。选中“安全密码（PEAP-MS-CHAP v2）”或者“智能卡或其他证书（EAP-TLS）”复选框，需要注意的是，VPN 服务器、NPS 和客户端必须设置完全相同的身份验证方式，否则无法建立连接。本例中选中“安全密码（PEAP-MS-CHAP v2）”复选框。

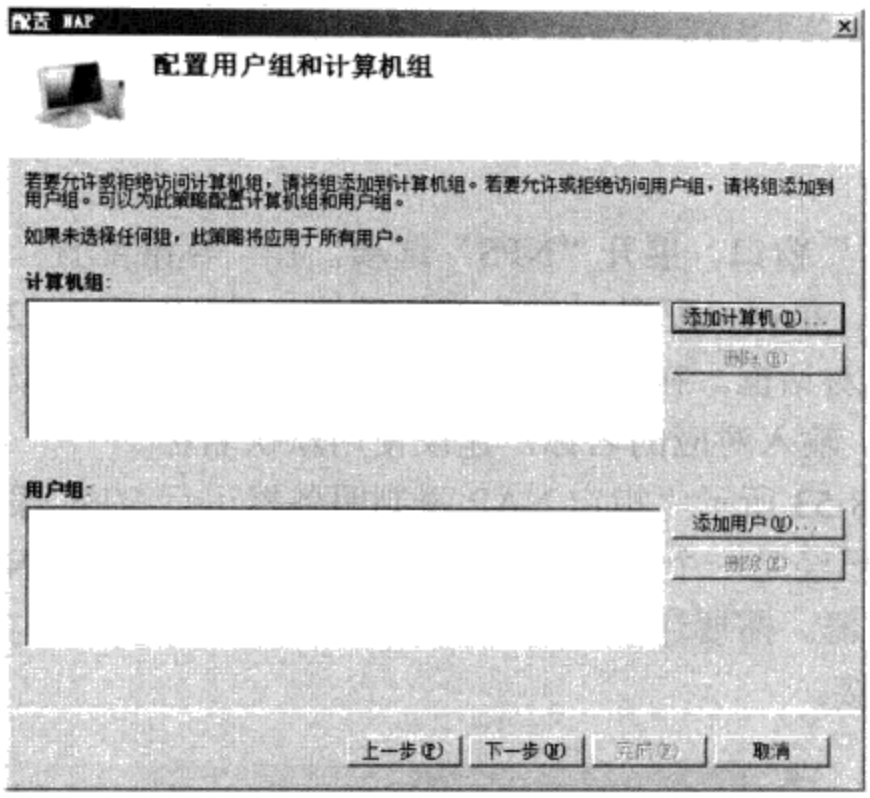


图 8-54 “配置用户组和计算机组”对话框

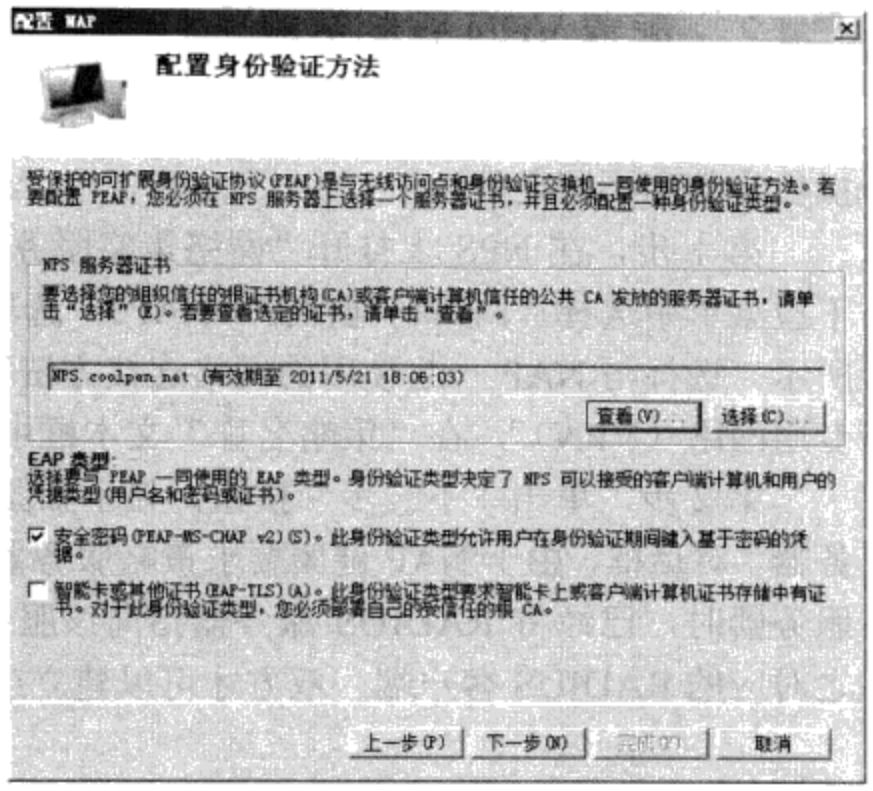


图 8-55 “配置身份验证方法”对话框

第 5 步，单击“下一步”按钮，显示如图 8-56 所示“指定 NAP 更新服务器组和 URL”对话框，既可以选择已经准备好的更新服务器组，也可以暂时不设置，而通过 IP 筛选器的方式指定在受限网络中允许访问的目标主机。本例中采用 IP 筛选器方式，所以此处保留“无”状态。

第 6 步，单击“下一步”按钮，显示如图 8-57 所示“定义 NAP 健康策略”对话框，选择 VPN 强制需要评估的 SHV，根据需要选择“启用客户端计算机的自动更新”复选框。选择“拒绝对不具有 NAP 功能的客户端计算机的完全网络访问权限。”单选按钮，即可使不支持 NAP 功能的客户端只能访问受限网络。选中“启用客户端计算机的自动更新”复选框，则当由于客户端计算机的自动更新为开启而未通过健康策略审核被隔离时，将自动启动客户端的自动更新设置。

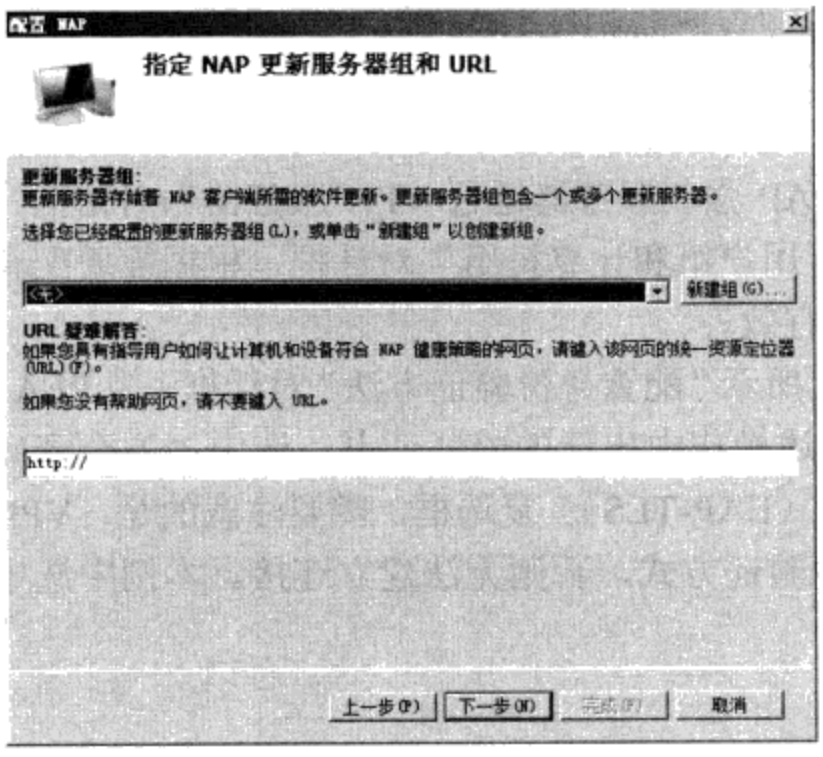


图 8-56 “指定 NAP 更新服务器组和 URL”对话框

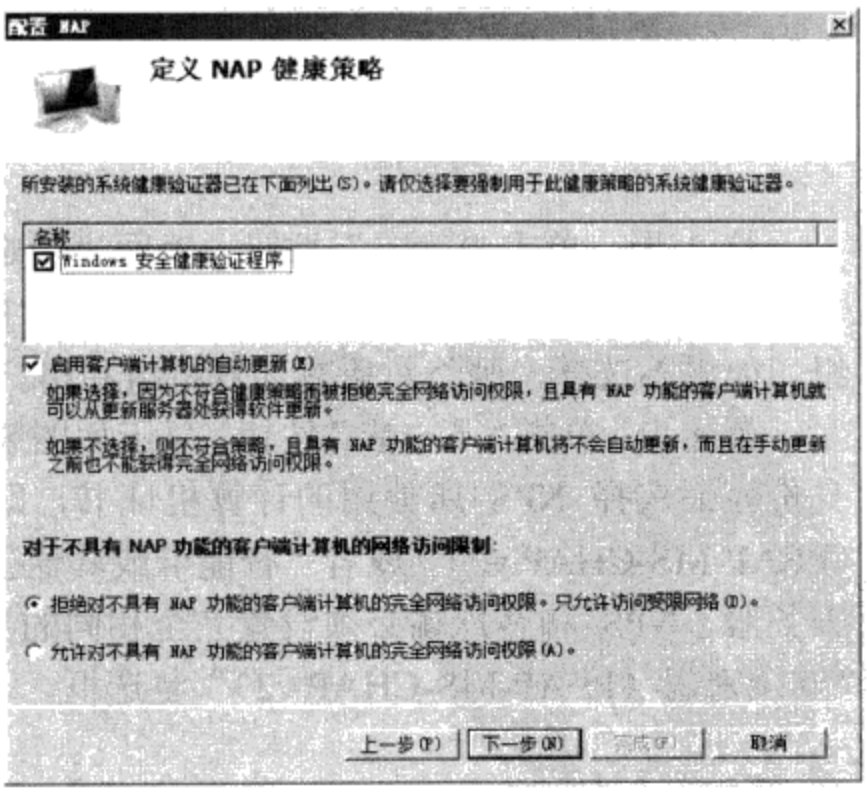


图 8-57 “定义 NAP 健康策略”对话框

第 7 步，单击“下一步”按钮，显示如图 8-58 所示“正在完成 NAP 增强策略和 RADIUS 客户端配置”对话框，当前“配置 NAP”向导创建了如下策略：

- 符合的 NAP 客户端的健康策略。
- 不符合的 NAP 客户端的健康策略。
- 基于 NAP 的远程访问 VPN 连接的连接请求策略。
- 不受限访问的符合的 NAP 客户端的网络策略。
- 受限访问的不符合的 NAP 客户端的网络策略。
- 不具有 NAP 功能的客户端的网络策略。

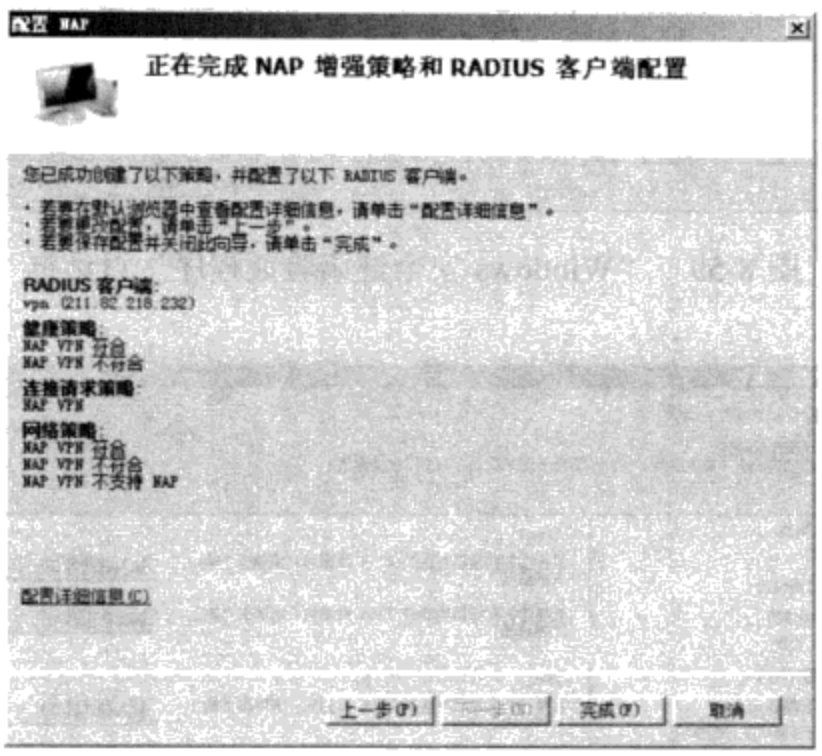


图 8-58 “正在完成 NAP 增强策略和 RADIUS 客户端配置”对话框

第 8 步，单击“完成”按钮，关闭“配置 NAP”向导。

“配置 NAP”向导创建的连接请求策略、健康策略和网络策略位于各自顺序列表的底部，直到用户删除或改变现有远程访问 VPN 网络策略，“配置 NAP”向导创建的网络策略才会用于基于 VPN 的远程访问连接的身份验证或健康评估。

3. 配置系统健康验证器

由于本例中 VPN 强制与 DHCP 强制使用的是同一个系统健康验证程序，即“Windows 安全健康验证程序”，所以这里不再详细介绍配置过程。在“Windows Vista”选项卡中选中“已为所有网络连接启用防火墙”复选框即可，如图 8-59 所示，即只对运行 Windows Vista 系统的 VPN 客户端是否开启 Windows 防火墙进行健康评估。

4. 通过 IP 筛选器配置受限网络中允许访问的主机

受限网络主要是针对非 NAP 客户端和不符合策略要求的 NAP 客户端而言的，因此需要同时更改“网络策略”中的“NAP VPN 不符合”和“NAP VPN 不支持 NAP”两条策略。

第 1 步，打开“网络策略服务器”窗口，展开“策略”→“网络策略”选项，双击“NAP VPN 不符合”显示如图 8-60 所示“NAP VPN 不符合属性”对话框，切换到“设置”选项卡，单击“IP 筛选器”链接，即可开始配置 IPv4 筛选器和 IPv6 筛选器，本例中仅设置 IPv4 筛选器。

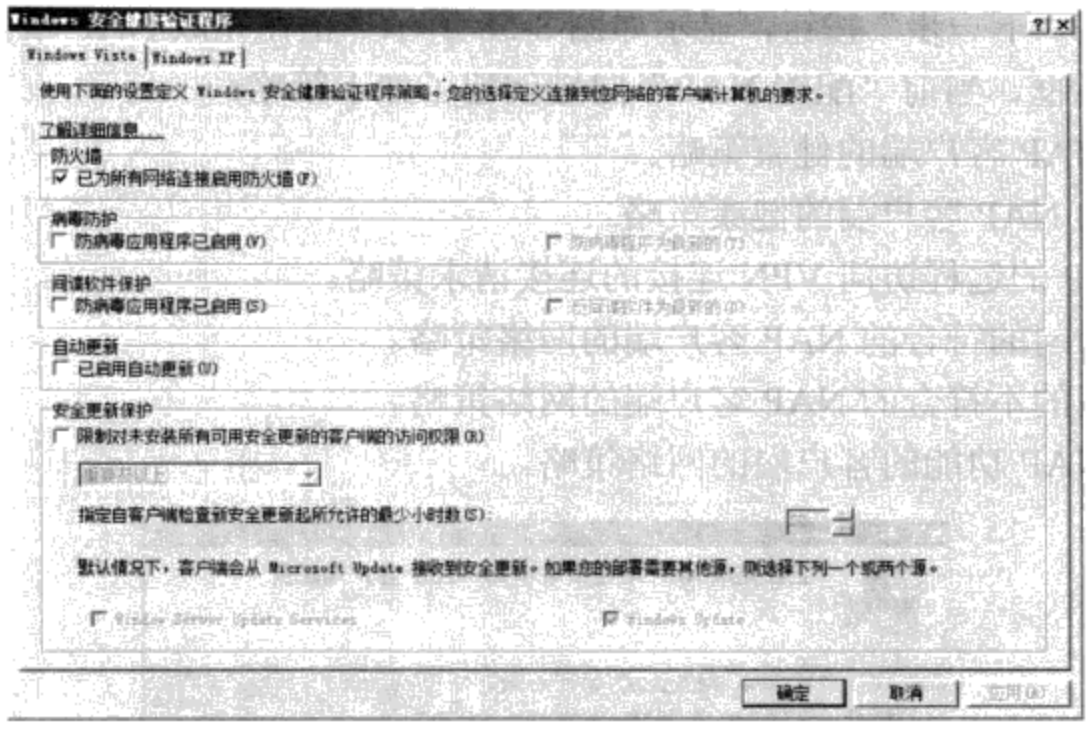


图 8-59　“Windows 安全健康验证程序”对话框

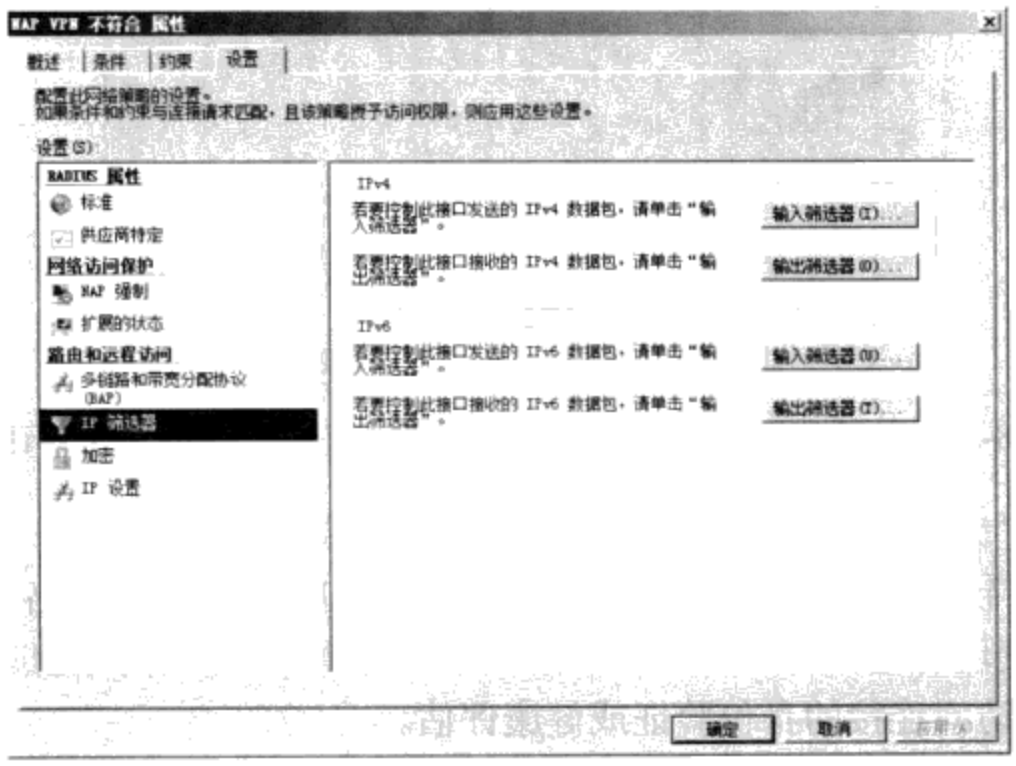


图 8-60　“NAP VPN 不符合属性”对话框

第 2 步，在 IPv4 区域内单击“输入筛选器”按钮，显示“入站筛选器”对话框，单击“新建”按钮，显示“添加 IP 筛选器”对话框。选中“目标网络”复选框，输入受限网络中允许访问的主机 IP 地址和子网掩码，注意，必须将子网掩码设置为 255.255.255.255，以确保是一台主机。这里以允许受限网络访问域控制器（IP 地址为 192.168.100.1）为例，如图 8-61 所示。

第 3 步，单击“确定”按钮，返回到如图 8-62 所示“入站筛选器”对话框，选择“仅允许下面列出的数据包”单选按钮即可。

第 4 步，单击“确定”按钮保存设置。继续在“IPv4”选项区域单击“输出筛选器”显示“出站筛选器”对话框，单击“新建”按钮显示如图 8-63 所示“添加 IP 筛选器”对话框，选中“源网络”复选框，设置 VPN 客户端计算机所属 IP 地址范围即可，如果 IP 地址和子网掩码分别设置为 0.0.0.0 和 0.0.0.0，则表示来源于任何网络。

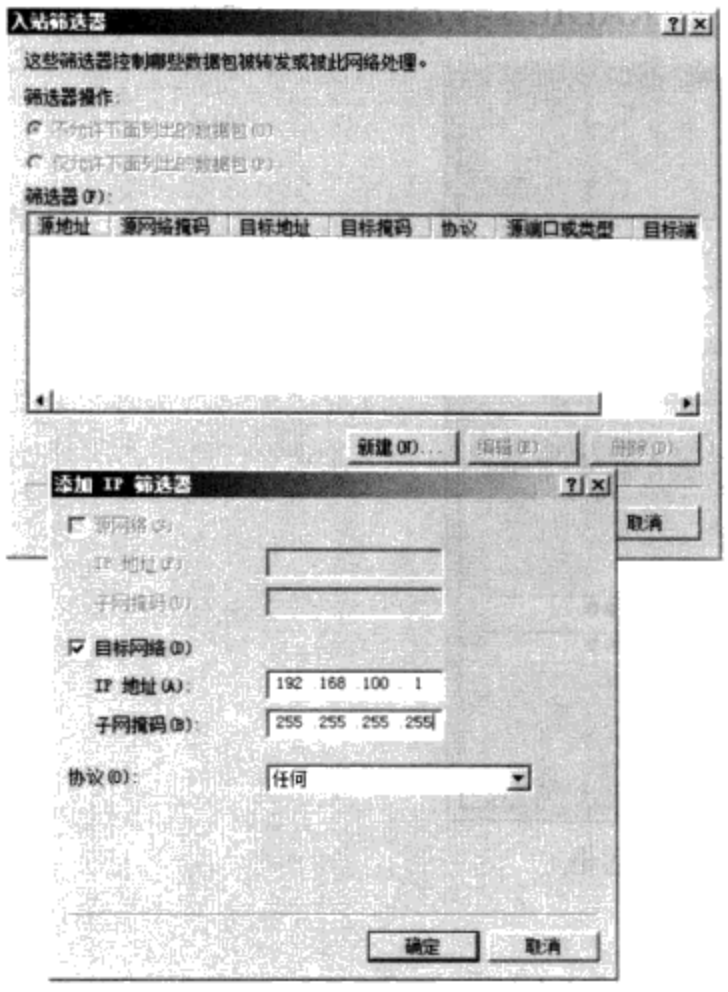


图 8-61　设置允许访问目标主机

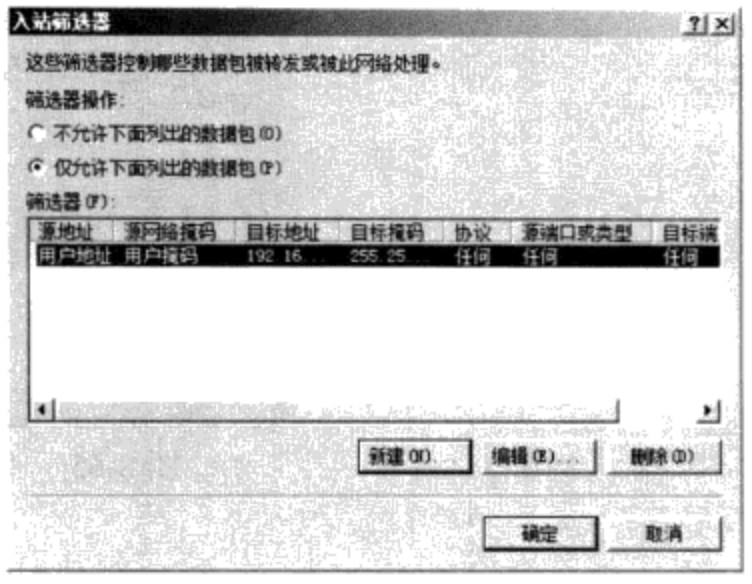


图 8-62　“入站筛选器”对话框

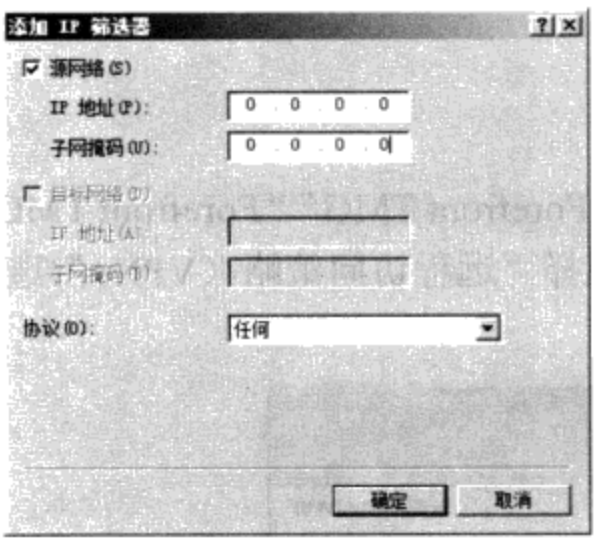


图 8-63　“添加 IP 筛选器”对话框

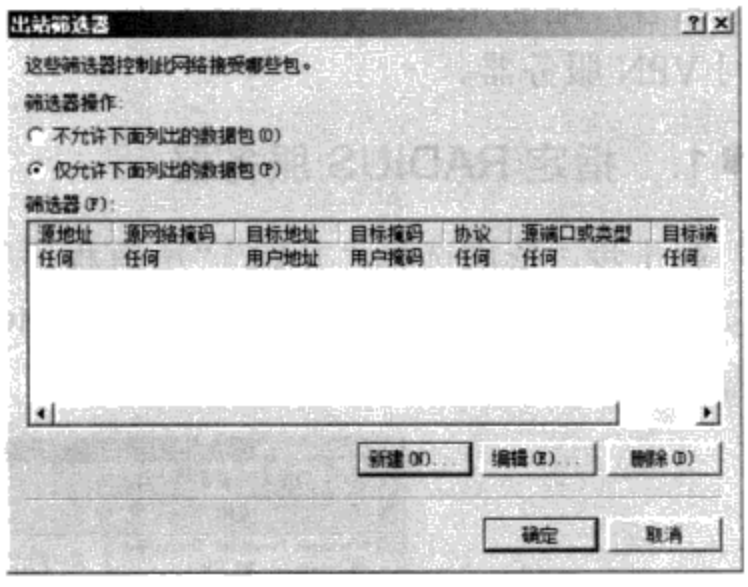


图 8-64　“出站筛选器”对话框

提示　“NAP VPN 不支持 NAP”网络策略同样需要配置 IP 筛选器，操作过程完全相同，此处不再赘述。

5. 为 RADIUS 客户端配置 NAP 支持

在“网络策略服务器”窗口中，依次展开“NPS（本地）”→“RADIUS 客户端和服务器”→“RADIUS 客户端”选项。右击名称为“VPN”的 RADIUS 客户端，选择快捷菜单中的“属性”

选项，显示如图 8-65 所示“VPN 属性”对话框，选中“RADIUS 客户端支持 NAP”复选框。

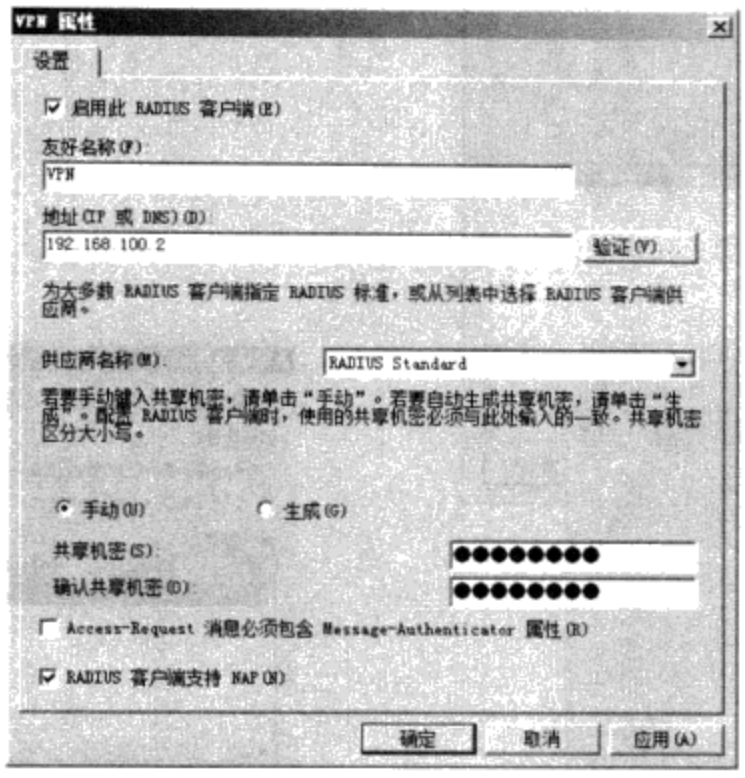


图 8-65 “VPN 属性”对话框

8.5.3 VPN 服务器的配置

默认情况下 VPN 服务器并没有启用 NAP 强制机制，只需提供有效的用户账户和密码即可建立 VPN 连接。因此，管理员需要重新配置 VPN 服务器的相关选项，启用 NAP 强制，并能够将客户端的系统健康状态信息发送到 NPS。本例中使用部署在网络边缘的 TMG 作为远程访问 VPN 服务器。

1. 指定 RADIUS 服务器

第 1 步，依次选择“开始”“所有程序”“Microsoft Forefront TMG”“Forefront TMG 管理”选项，显示如图 8-66 所示“Forefront TMG”窗口。选择“远程访问策略（VPN）”选项即可查看和配置 VPN 服务器相关的内容。

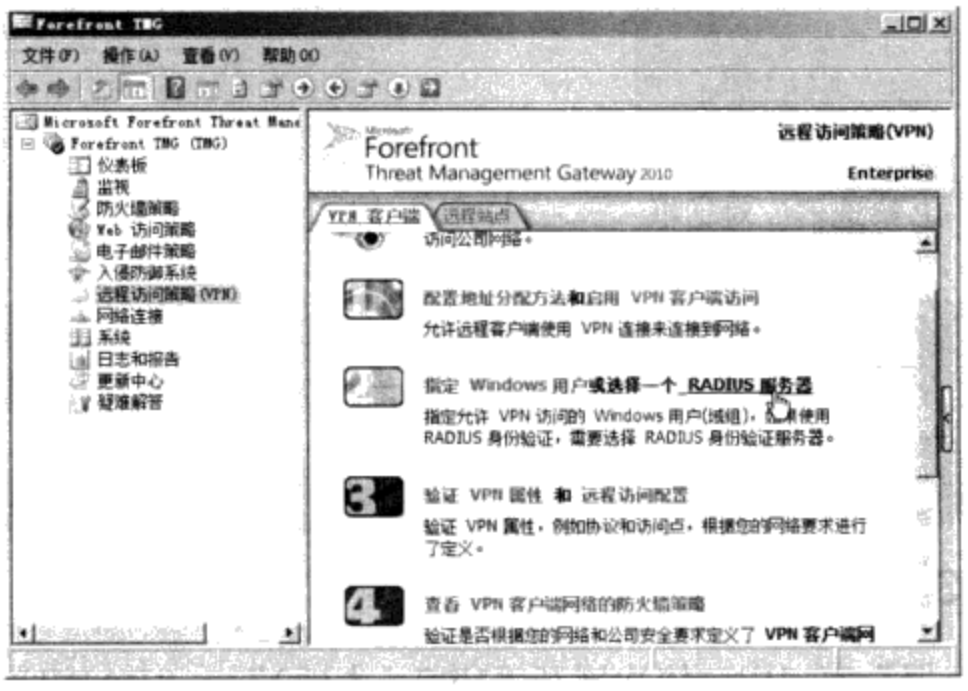


图 8-66 “Forefront TMG”窗口

第 2 步，单击“RADIUS 服务器”链接，显示“远程访问策略（VPN） 属性”对话框，默认显示如图 8-67 所示“RADIUS”选项卡。选中“使用 RADIUS 进行身份验证”和“使用 RADIUS 记账（记录）”复选框。

第 3 步，单击“RADIUS 服务器”按钮，显示“RADIUS 服务器”对话框，单击“添加”按钮显示“添加 RADIUS 服务器”对话框，输入 RADIUS 服务器的名称和简要描述信息，本例中 NPS 就是 RASIUS 服务器，所以输入 NPS 服务器的 IP 地址或主机名即可。单击“更改”按钮，设置与 NPS 上配置 VPN 强制策略中完全相同的共享密码，如图 8-68 所示。

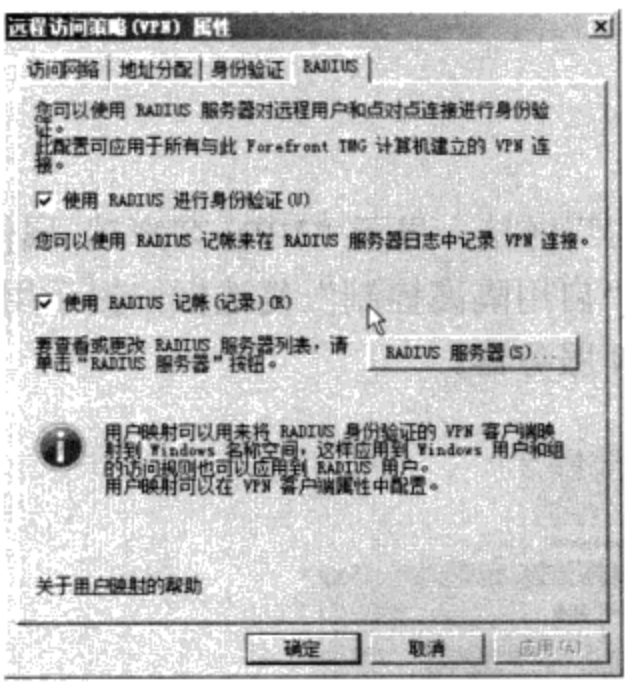


图 8-67 “RADIUS”选项卡

图 8-68 设置 RADIUS 服务器信息

第 4 步，连续两次单击“确定”按钮，返回到如图 8-69 所示“RADIUS 服务器”对话框，即可看到成功添加的 RADIUS 服务器。

第 5 步，单击“确定”按钮，保存配置。注意，此时 TMG 服务器并未应用新的配置，可以待全部完成后再保存和应用配置。

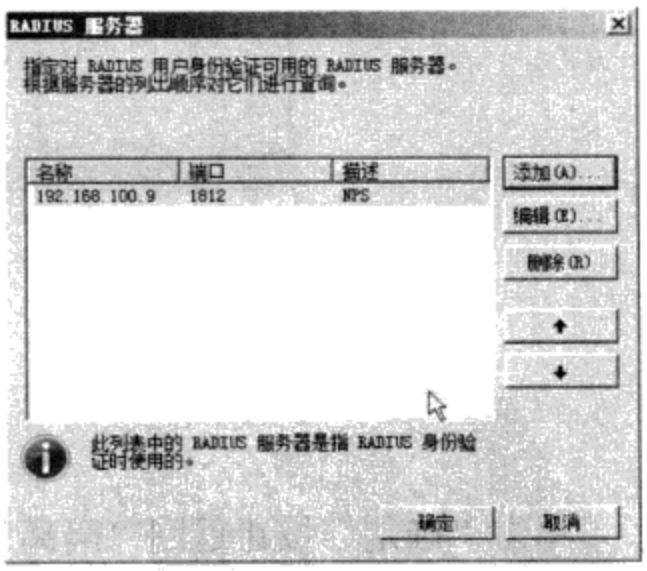


图 8-69 “RADIUS 服务器”对话框

2. 配置身份验证协议

在“远程访问策略（VPN） 属性”对话框中，切换到如图 8-70 所示“身份验证”选项卡，选中“Microsoft 加密的身份验证版本 2（MS-CHAPv2）”和“可扩展的身份验证协议（EAP），使用智能卡或其他证书”复选框，此时会提示“Microsoft Forefront Threat Management Gateway”对话框，直接单击“确定”按钮即可。最后，单击“确定”按钮，保存配置。

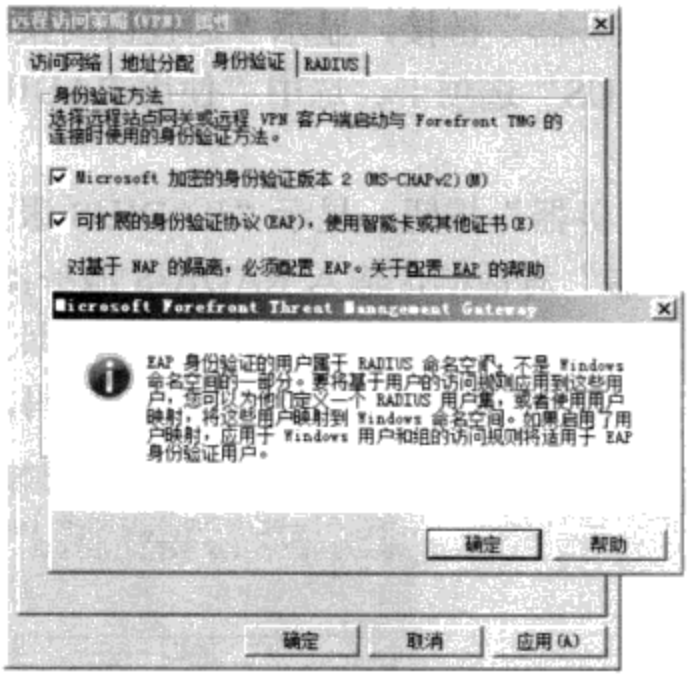


图 8-70　“身份验证”选项卡

3. 启用 NAP 隔离控制

在“Forefront TMG”窗口中，单击“配置隔离（可选）”链接，显示“VPN 客户端 属性”对话框，默认显示如图 8-71 所示“隔离”选项卡。选中“启用隔离控制”复选框，提示用户启用该配置后默认策略将阻止所有客户端计算机访问 VPN 服务器。

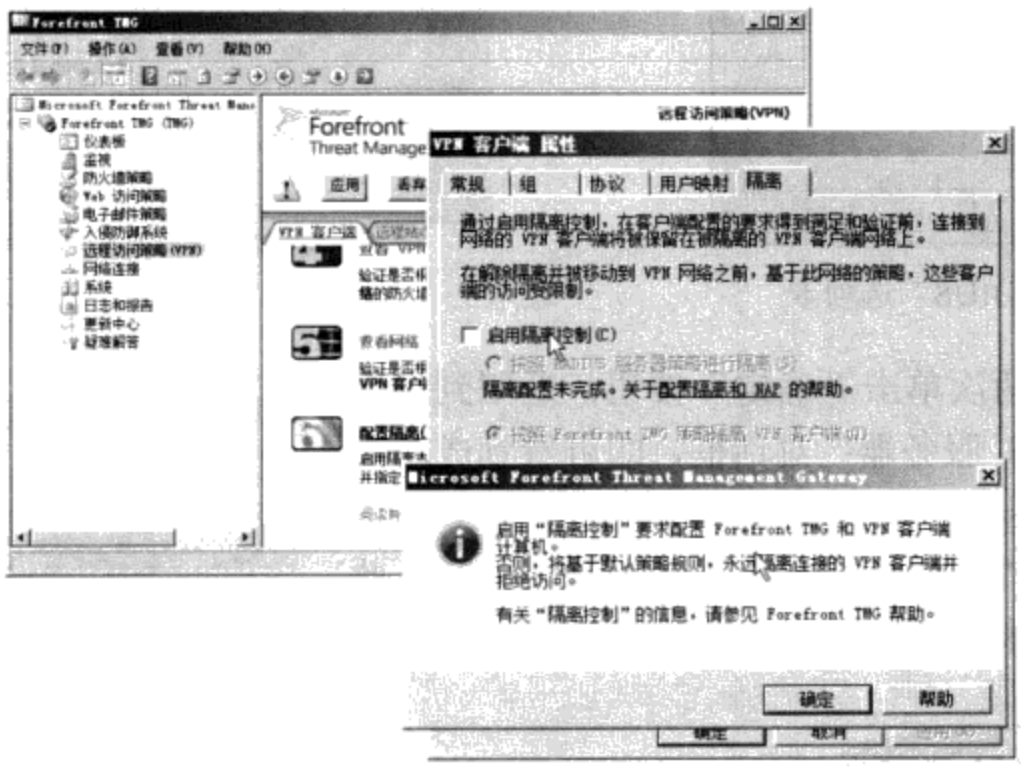


图 8-71　“隔离”选项卡

单击“确定”按钮返回“隔离”选项卡，选择“按照 RADIUS 服务器策略进行隔离”单选按钮，如图 8-72 所示。系统默认将使用 Forefront TMG 的 VPN 隔离策略。最后，单击“确定”按钮，保存配置。

4. 应用策略

所有配置完成后，即可在“Forefront TMG”窗口中，单击“应用”按钮保存并应用配置，此时会显示如图 8-73 所示“配置更改描述”对话框，输入相关的描述信息。

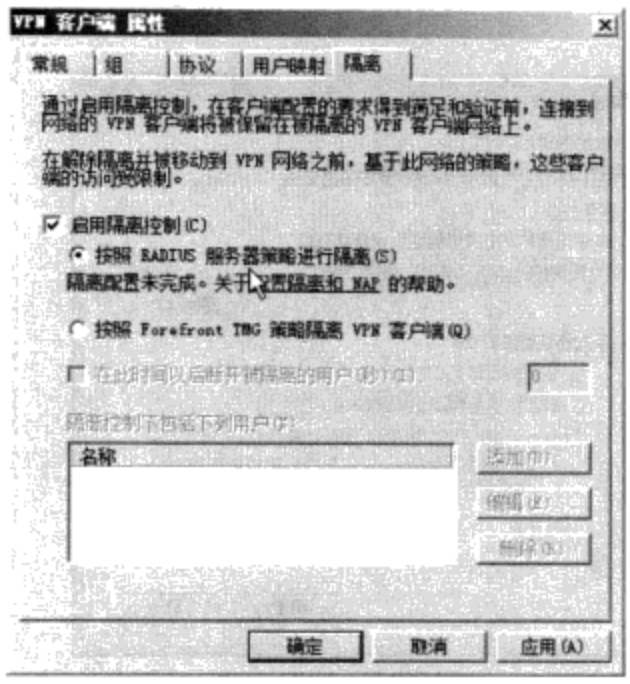


图 8-72　启用 NAP 隔离机制

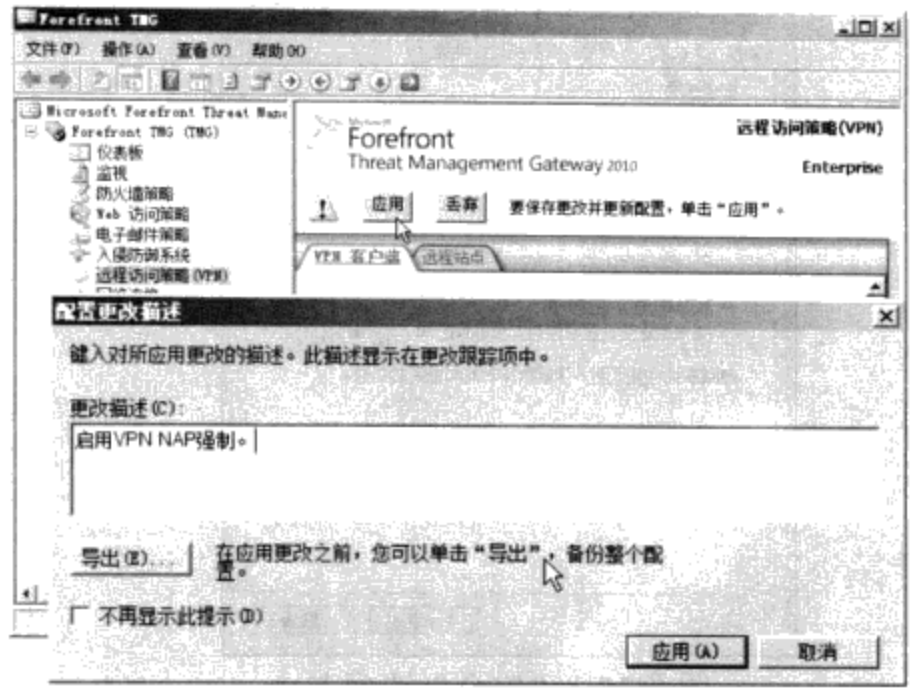


图 8-73　“配置更改描述”对话框

单击“应用”按钮，即可开始保存并应用配置更改，完成后显示如图 8-74 所示结果。单击“确定”按钮，关闭对话框。

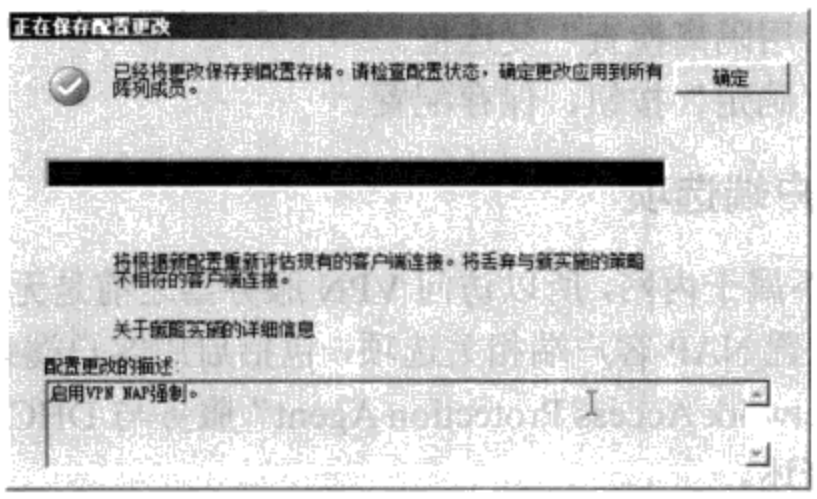


图 8-74　“正在保存配置更改”对话框

8.5.4 创建和配置 VPN NAP 客户端

1. 配置 VPN 客户端

VPN 客户端连接的创建比较简单，详细操作过程，请参考本书第 10 章中的相关介绍，此处不再赘述。配置 VPN 强制时，应注意客户端身份验证协议是否正确，确保与 VPN 服务器完全一致，否则将无法建立连接。

第 1 步，在“网络连接”窗口中，右击创建的 VPN 连接，选择快捷菜单中的“属性”对话框，打开“VPN 连接 属性”对话框。切换至“安全”选项卡，选择“高级（自定义设置）”单选按钮，如图 8-75 所示。

第 2 步，单击“设置”按钮，显示如图 8-76 所示“高级安全设置”对话框，在“数据加密”下拉列表框中选择“需要加密（如果服务器拒绝将断开连接）”选项，选择“使用可扩展的身份验证协议（EAP）”单选按钮，选择下拉列表框中的“受保护的 EAP”选项。

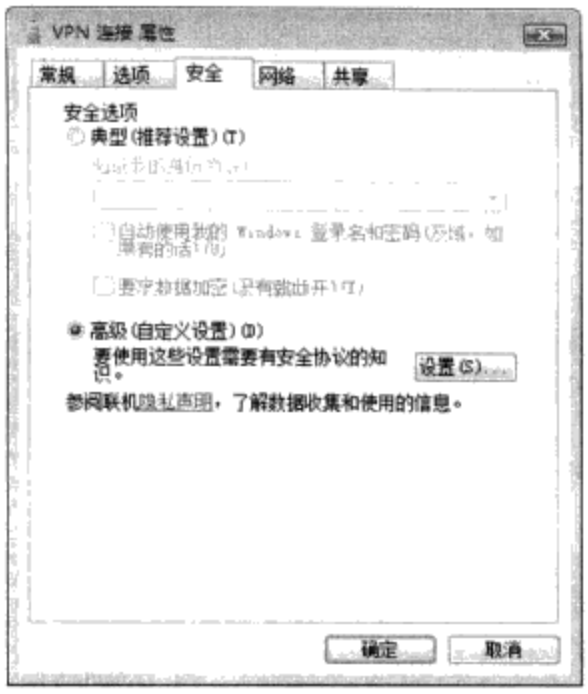


图 8-75 “安全”选项卡

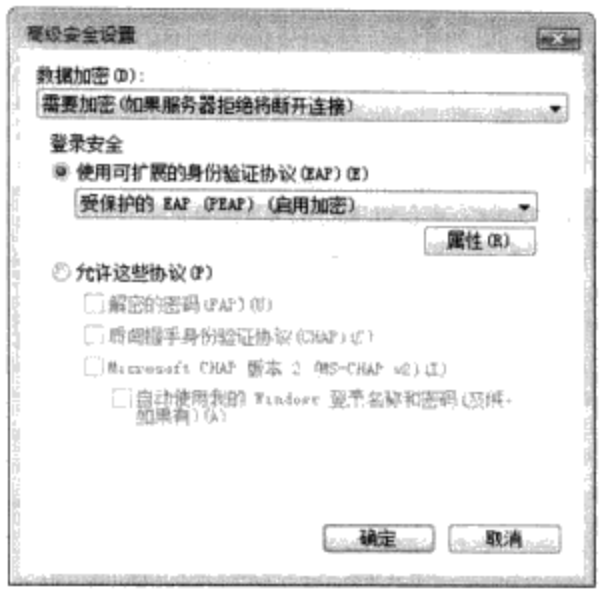


图 8-76 “高级安全设置”对话框

第 3 步，单击“属性”按钮，显示如图 8-77 所示“受保护的 EAP 属性”对话框，取消 “连接到这些服务器”复选框。选中“验证服务器证书”复选框，在“受信任的根证书颁发机构”列表框中，会发现已经安装的证书颁发机构。在“选择身份验证方法”下拉列表框中，选择“安全密码”选项。选中“启用隔离检查”复选框。

第 4 步，连续单击“确定”按钮，保存配置。

2. 配置 NAP 客户端选项

VPN 客户端计算机不属于内网，所以访问 VPN 服务器之前是无法应用域控制器的组策略的，只能通过手动方式配置 NAP 客户端相关选项，包括启用客户端系统服务、启用 NAP 客户端隔离等。其中启用“Network Access Protection Agent”服务与 DHCP NAP 客户端手动配置方式完全相同，这里不再赘述。

用户需要在“NAP 客户端配置”窗口中，启用“远程访问隔离强制客户端”，如图 8-78 所示。

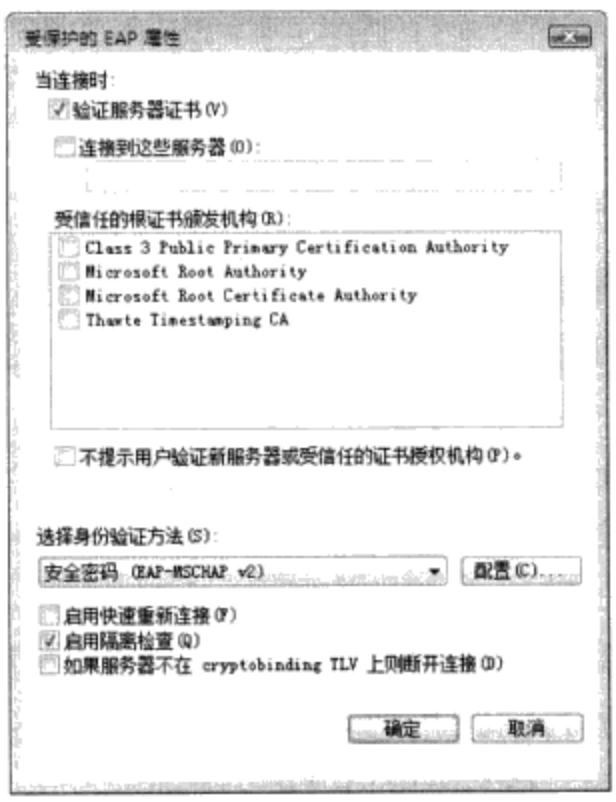


图 8-77 “受保护的 EAP 属性”对话框

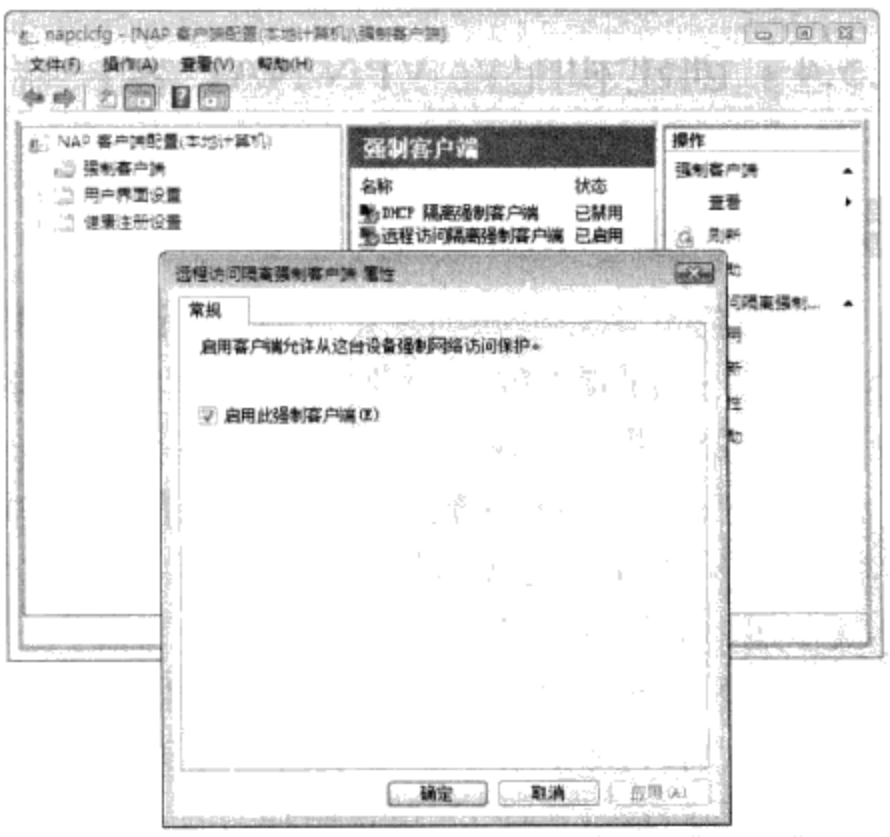


图 8-78 “远程访问隔离强制客户端 属性”对话框

8.5.5 测试受限 VPN 客户端的访问

在启用强制模式之前，用户必须测试不符合健康要求策略的 NAP 客户端的受限访问，以确保其可以被提示未通过评估的原因，并且只能访问受限网络中的补救服务器。

第 1 步，在“网络连接”窗口中，双击 VPN 链接，输入用户名和密码并单击“确定”按钮，即可尝试连接到 VPN 服务器。此时，由于防火墙设置不符合健康策略要求，任务栏中显示“此计算机不符合该网络的要求”信息，如图 8-79 所示。

第 2 步，单击信息提示框，显示如图 8-80 所示“网络访问保护”窗口。当前验证结果为“未成功”，修正结果为“管理员必须启用与 Windows 安全中心兼容的防火墙程序”。

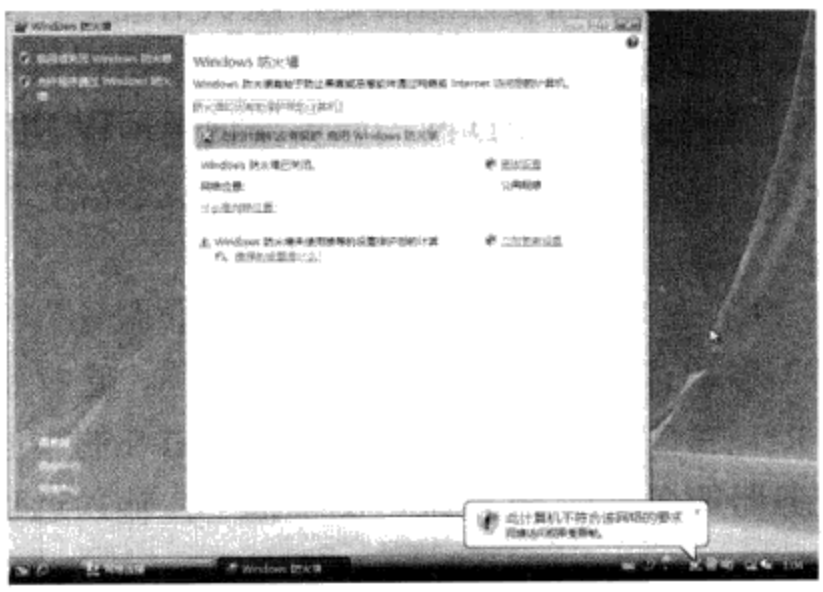


图 8-79　此计算机不符合该网络的要求

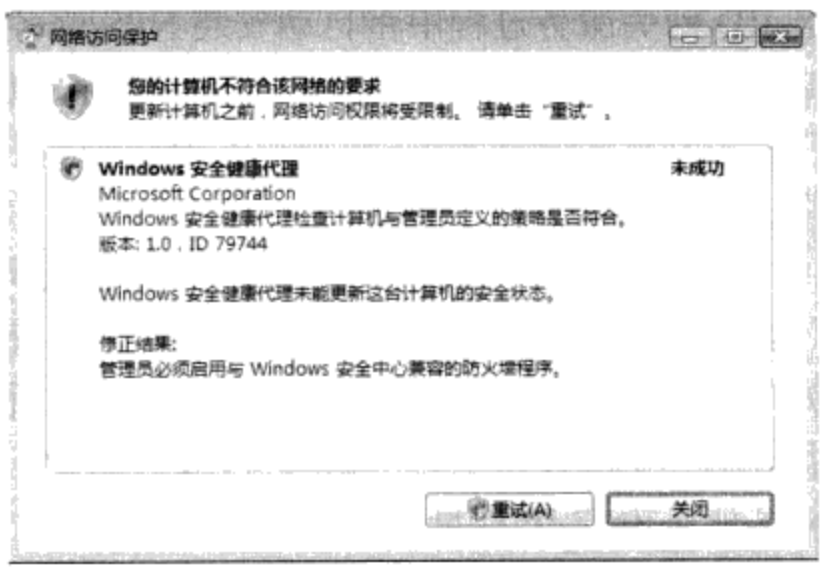


图 8-80　“网络访问保护”窗口

第 3 步，根据提示信息，启用 Windows 防火墙后，任务栏中将自动显示如图 8-81 所示提示信息“此计算机符合该网络的要求”。

第 4 步，此时单击信息框，显示如图 8-82 所示“网络访问保护”窗口，即完全符合健康策略的要求。

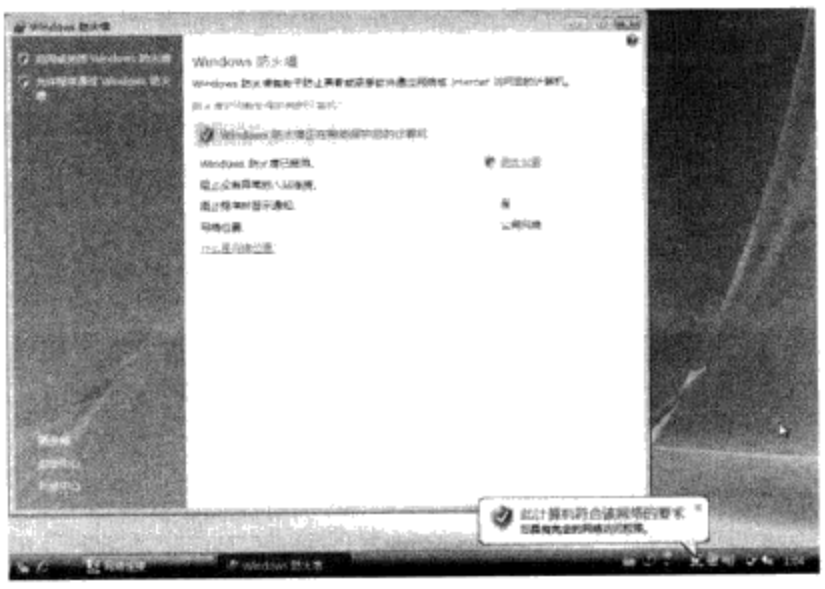


图 8-81　此计算机符合该网络的要求

图 8-82　“网络访问保护”窗口

8.6 配置 RD 网关强制

远程桌面是平时应用最多的远程管理方式之一，在 Windows Server 2008 R2 系统中，其安全性大大增强，通过与网络中的 NAP 系统协同工作，评估实施远程桌面连接的远程计算机系统的健康程度，避免将不安全因素引入网络，从而确保内部网络的安全性。

8.6.1 RD 网关服务器的配置

若要通过 NPS 服务器为 RD 网关连接进行保护，首先必须部署 RD 网关服务器，具体操作过程可以参照本书“Windows 远程管理”中的相关介绍。需要注意的是，默认情况下，安装 RD 网关服务过程中将自动安装 NPS 服务器，即默认使用本地 NPS 服务器存储连接授权策略和资源授权策略。如果网络中已经部署其他 NPS 服务器，希望 RD 网关服务器使用远程 NPS 服务器存储和管理策略，则可以在 RD 网关服务安装完成后进行配置，安装过程中无法取消“网络策略服务器”角色服务。

第 1 步，RD 网关安装完成后，依次选择“开始”→“管理工具”→“远程桌面服务”→“远程网关管理器”选项，打开“RD 网关管理器”窗口，右击 RD 网关服务器名称，选择快捷菜单中的“属性”命令，显示如图 8-83 所示“RD 属性”对话框，选择“运行 NPS 的中心服务器”单选按钮，在“输入正在运行 NPS 的服务器的名称或 IP 地址”文本框中，输入远程 NPS 服务器的 IP 地址。

第 2 步，单击“添加”按钮，显示如图 8-84 所示“共享机密”对话框。若要建立 RD 网关服务器到远程 NPS 服务器的连接，必须设置共享机密。默认情况下，NPS 服务器是未配置该共享机密的，因此必须先在 RD 网管服务器上生成新的共享机密，然后在 NPS 服务器上创建 RADIUS 客户端时，在输入相同的共享机密。在“输入新的共享机密”文本框中，输入共享机密，并牢记该字符串。

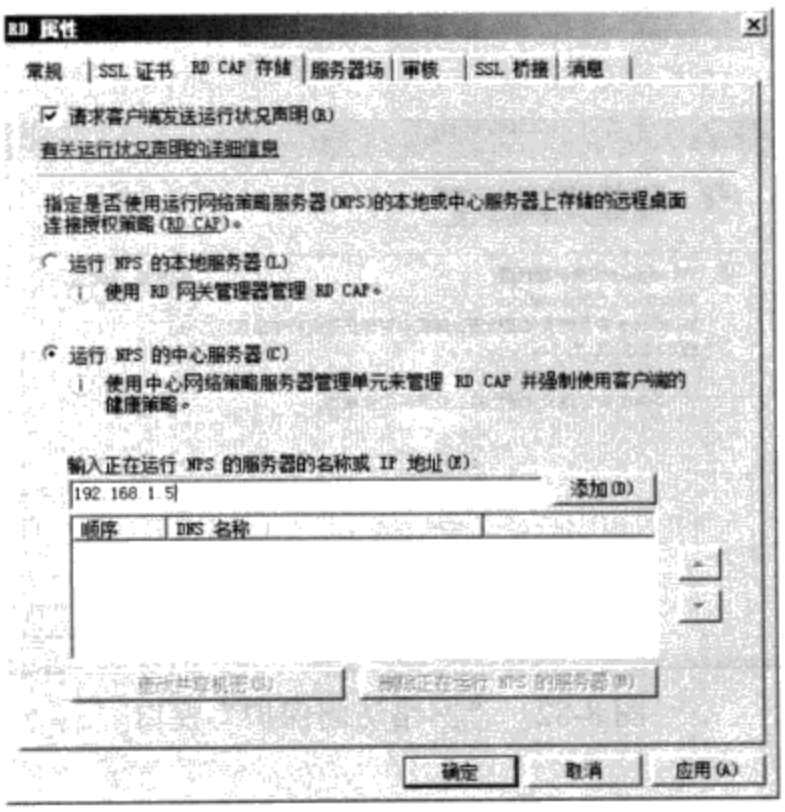


图 8-83 “RD 属性”对话框

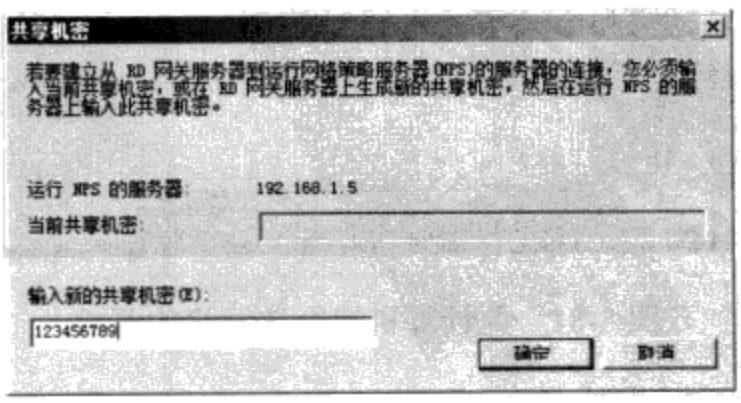


图 8-84 “共享机密”对话框

第 3 步，连续单击“确定”按钮，完成 RD 网关服务器的配置。

8.6.2 配置 RD 网关强制策略

RD 网关强制策略的配置与其他类型网络连接的强制策略类似，可以通过“配置 NAP”向导快速生成各种策略。进行系统健康状态评估时使用的 SHV 仍为 WSHV。

1. 将 RD 网关服务器配置为 RADIUS 客户端

默认情况下，RD 网关连接使用本地 NPS 服务器，若想建立到远程 NPS 服务器的连接使用完全相同的共享机密。在此之前，配置 RD 网关服务器时，已经设置了共享机密，所以在将 RD 网关服务器配置为 RADIUS 客户端时，只需使用相同的共享机密即可。

在 NPS 服务器上打开“网络策略服务器”窗口，右击“RADIUS 客户端”并选择快捷菜单中的“新建”命令，显示如图 8-85 所示“新建 RADIUS 客户端”对话框，选中“启用此 RADIUS 客户端”复选框，在“友好名称”文本框中输入便于识别的名称，在“地址”文本框中，输入 RD 网关服务器的 IP 地址或 DNS 名称。在“共享机密”区域，选择“手动”单选按钮，输入与 RD 网管服务器端完全相同的共享机密即可。另外，在“高级”选项卡中还应选中“RADIUS 客户端支持 NAP”复选框，操作方法与“配置 IPSec 强制”完全相同，此处不再赘述。

2. 创建 RD 网关强制策略

第 1 步，在“网络策略服务器”窗口中，单击“NPS”节点，在右侧主窗口中，单击“配置 NAP”链接，启动“配置 NAP”向导。在“选择与 NAP 一起使用的网络连接方法”对话框中，选择“远程桌面网关（RD 网关）”连接方法，并设置希望使用的策略名称，如图 8-86 所示。

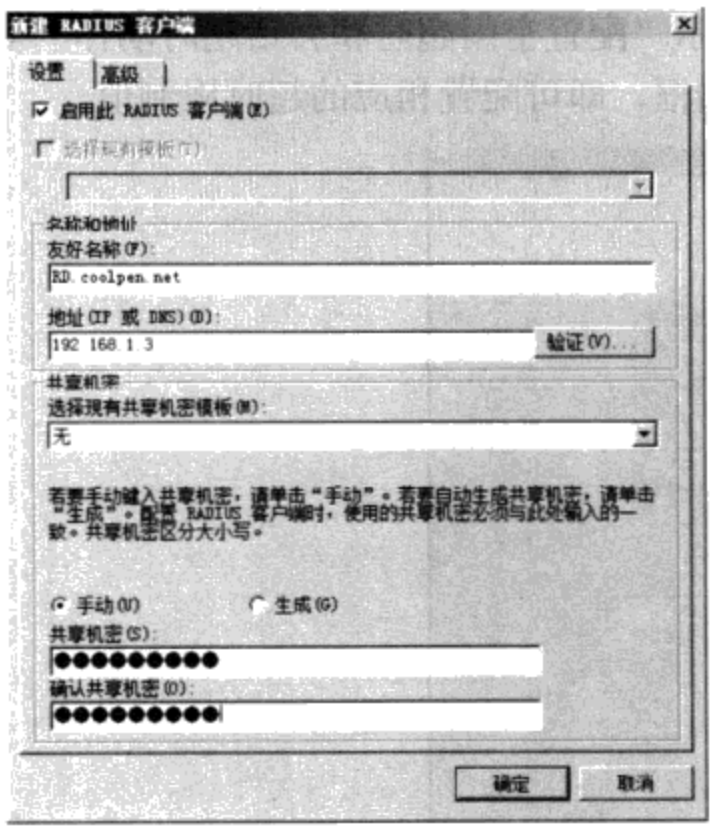


图 8-85 “新建 RADIUS 客户端”对话框

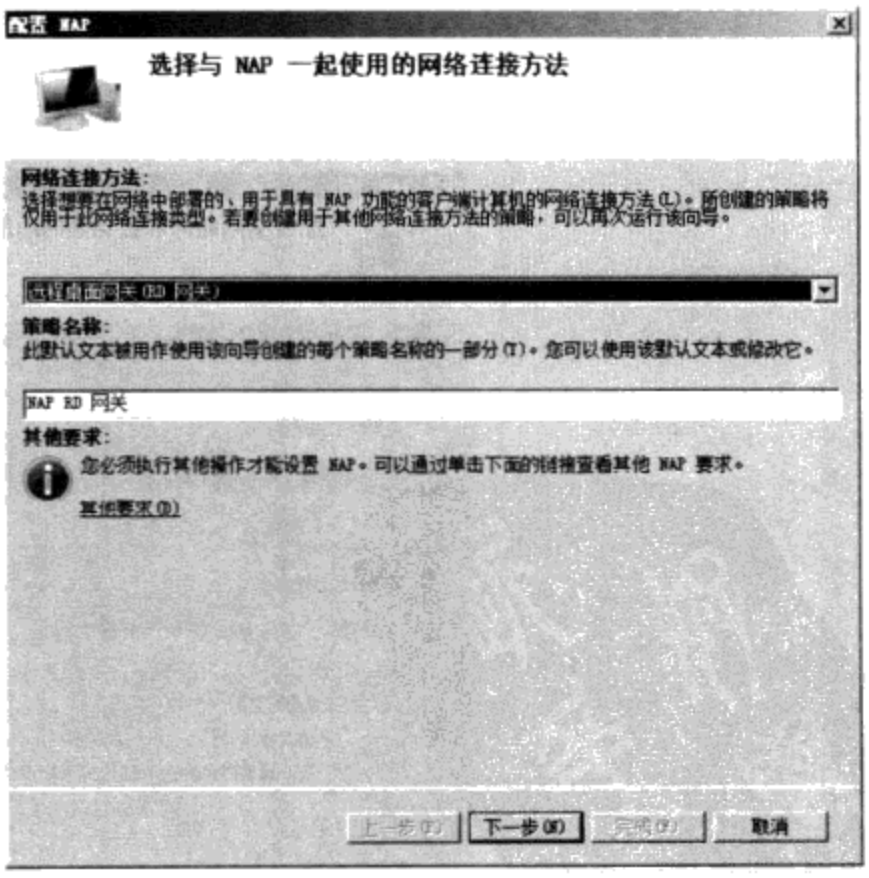


图 8-86 “选择与 NAP 一起使用的网络连接方法”

第 2 步，单击“下一步”按钮，显示如图 8-87 所示“指定 NAP 强制服务器运行 RD 网关”对话框，由于已经将 RD 网关服务器配置 RADIUS 客户端，所以 RD 网关服务器将自动显示在

“RD网关服务器”列表框中。

第3步，单击“下一步”按钮，显示如图8-88所示“配置客户端设备重定向和身份验证方法”对话框，所谓“客户端设备重定向”是指当客户端通过RD网关访问内部服务器的远程桌面时，是否可以使用相关功能和设备，包括驱动器、打印机、剪贴板等，建议选择“启用所有远程客户端设备的重定向”单选按钮。在“身份验证方法”区域，根据实际环境选择相应的方法。

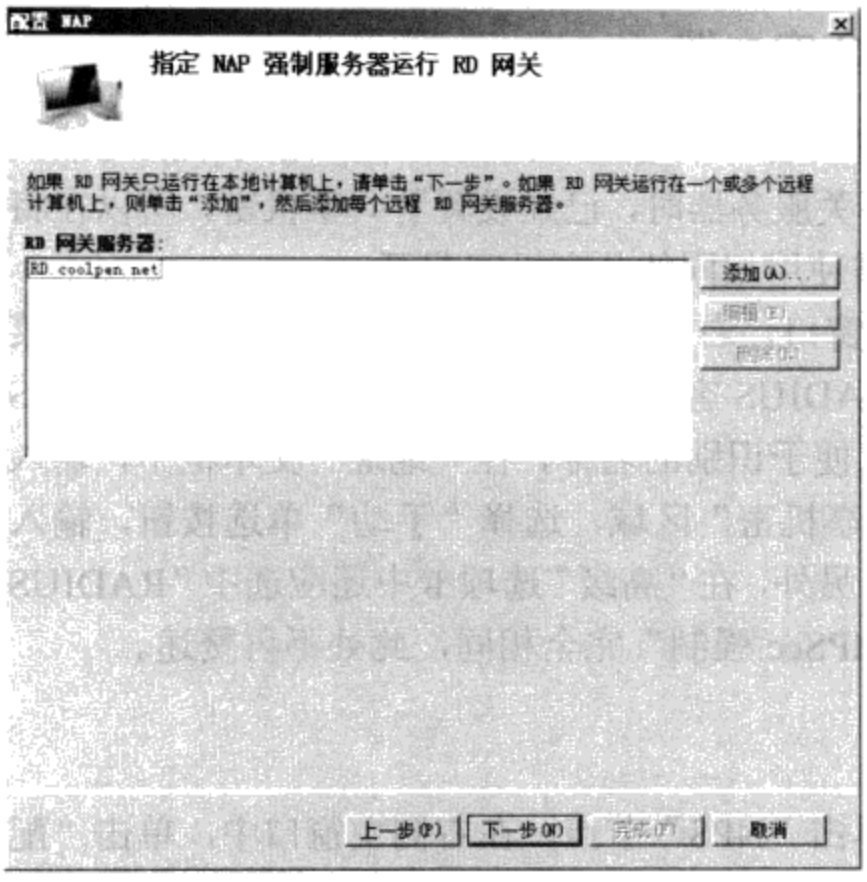


图8-87 “指定NAP强制服务器运行RD网关”对话框

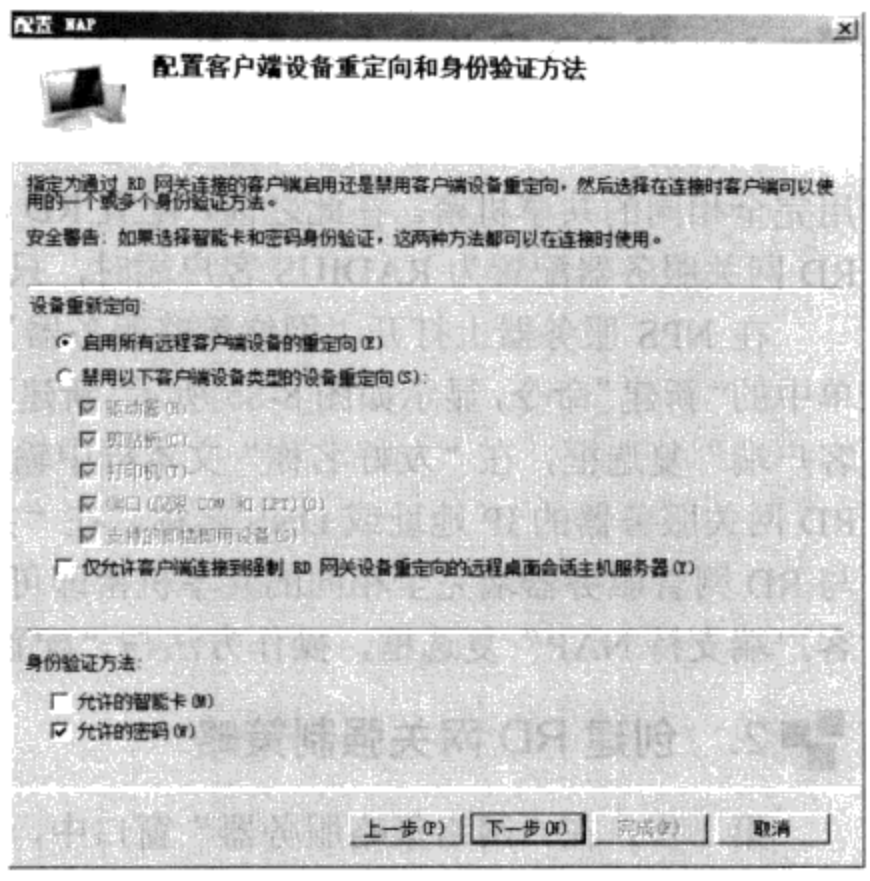


图8-88 “配置客户端设备重定向和身份验证方法”对话框

第4步，单击“下一步”按钮，显示如图8-89所示“配置空闲超时和会话超时动作”对话框，选中“启用空闲超时”和“启用会话超时”复选框，即可配置相应的超时限制值。

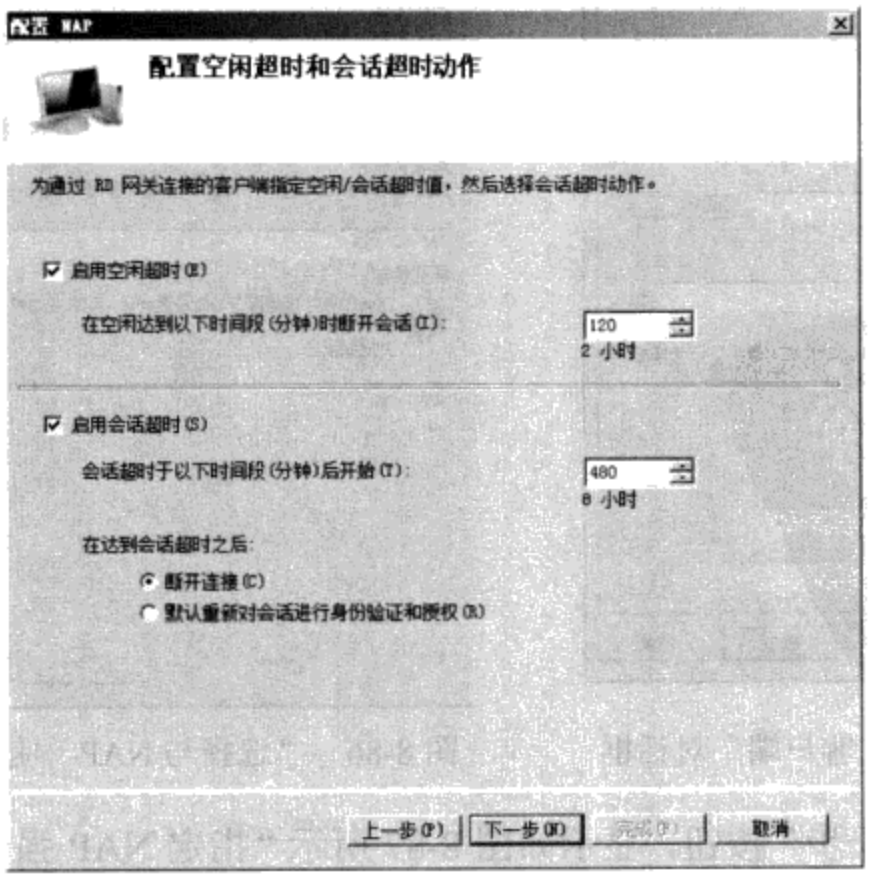


图8-89 “配置空闲超时和会话超时动作”对话框

第 5 步，单击“下一步”按钮，显示如图 8-90 所示“配置用户组和计算机组”对话框，设置允许远程用户使用哪些用户账户，通过 RD 网关访问网络中哪些计算机的远程桌面。其中，“用户组”是必须指定的，单击“添加”按钮，输入希望指定的用户组名，并单击“检查名称”按钮进行核实，最后单击“确定”按钮，返回“配置用户组和计算机组”对话框。如果不指定任何“机器组”，则表示允许通过 RD 网关连接到网络中的所有计算机。

第 6 步，单击“下一步”按钮，显示如图 8-91 所示“定义 NAP 健康策略”对话框，指定使用 SHV，并对非 NAP 客户端的访问限制进行设置，建议选择“允许客户端访问运行远程桌面的远程桌面会话主机服务器和计算机”单选按钮，以确保非 NAP 客户端可以进行正常网络连接。

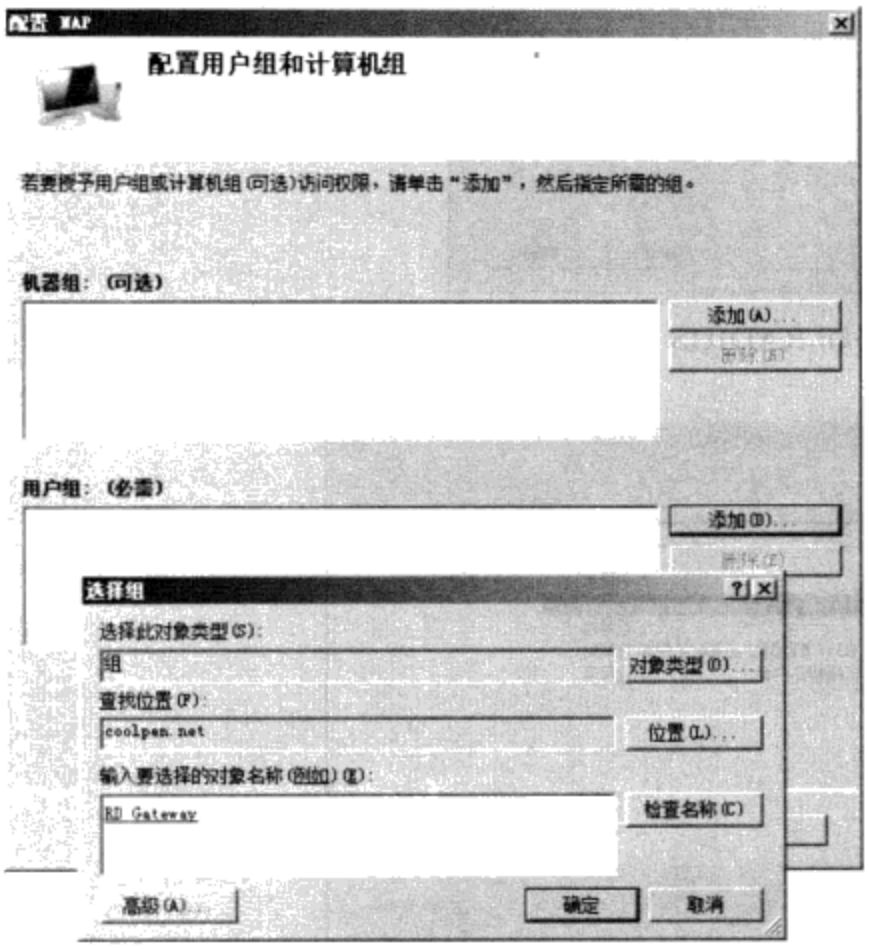


图 8-90 “配置用户组和计算机组”对话框

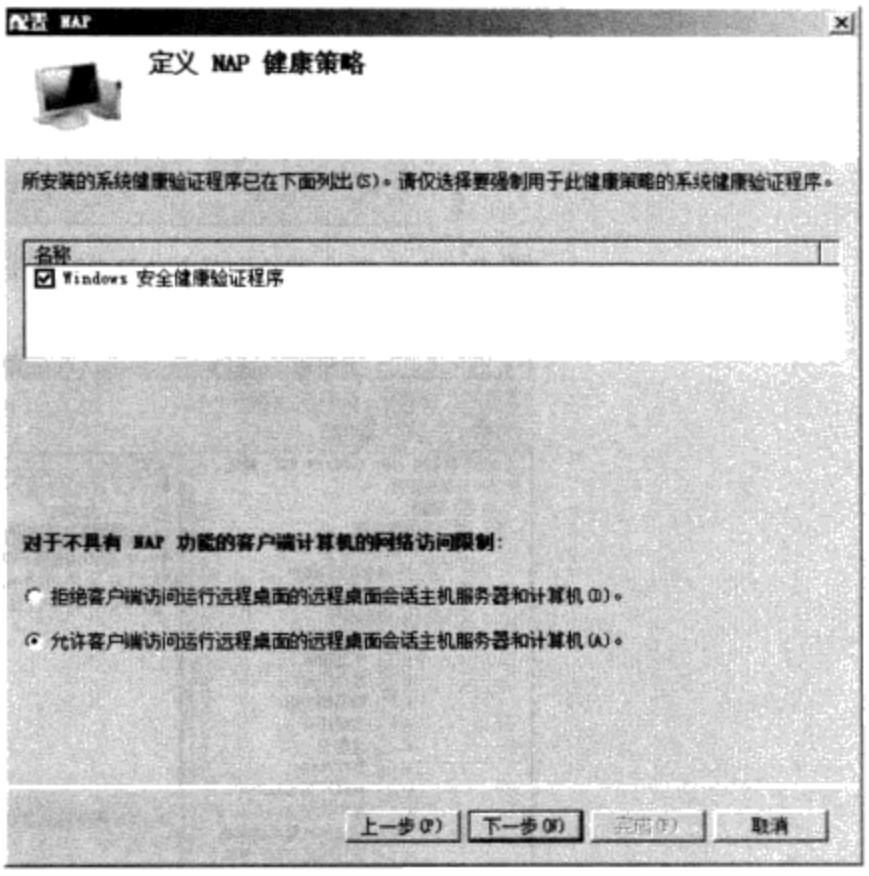


图 8-91 “定义 NAP 健康策略”对话框

第 7 步，单击“下一步”按钮，显示如图 8-92 所示“正在完成 NAP 增强策略和 RADIUS 客户端配置”对话框，显示该向导完成后将生成的所有策略。

3. 配置 SHV

RD 网关强制的 SHV 配置与其他类型的强制完全相同，根据需要分别对“NAP RD 网关 符合”和“NAP RD 网关 不符合”进行配置即可，此处不再赘述。

8.6.3 配置 NAP 客户端

客户端的配置与其他类型强制类似，推荐使用组策略统一配置 NAP 客户端。在“组策略管理编辑器”窗口中，启用“RD 网关隔离强制客户端”策略即可，如图 8-93 所示。其他操作，请参考 IPSec 强制客户端的配置。

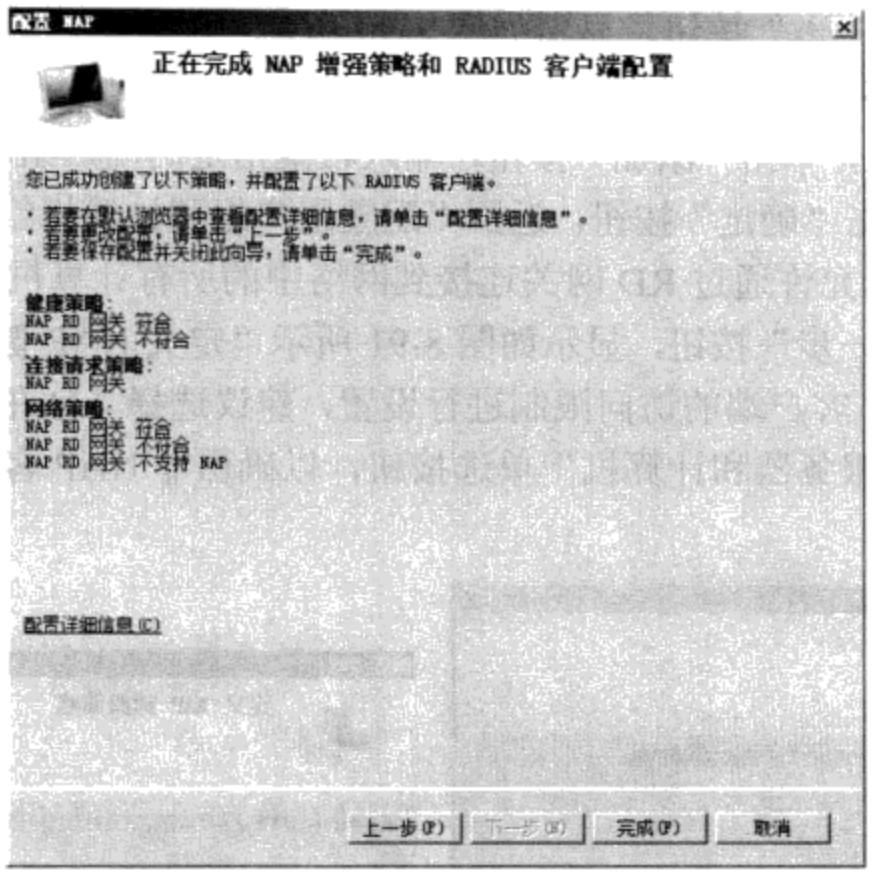


图 8-92 “正在完成 NAP 增强策略和 RADIUS 客户端配置”对话框

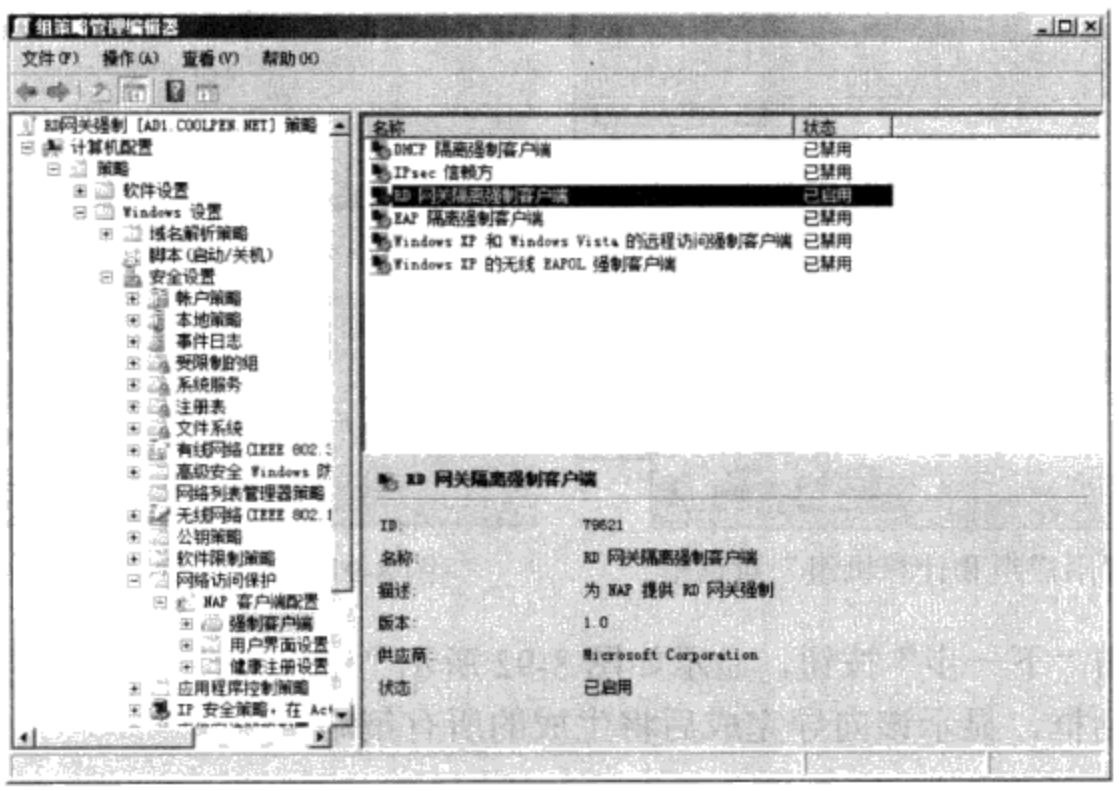


图 8-93 启用“RD 网关隔离强制客户端”策略

需要注意的是，在实施 RD 网关强制时，运行 Windows Server 2008 和 Windows Server 2008 R2 的计算机不能用做 NAP 客户端，只有运行 Windows XP/Vista/7 的计算机可以用做 NAP 客户端。

第 9 章　局域网传输安全

数据传输是组建局域网的主要目的之一，传输文件、共享本地资源几乎是每个用户天天都要用到的。在具有一定规模的局域网中，如果不能对局域网中的数据传输进行有效控制，确保资源传输和网络连接的安全，则网络传输故障的出现只是迟早的事情。在局域网中，管理员通常可以借助内部防火墙隔离和控制不同子网或部门之间的数据传输，还可以通过配置用户接入的交换机端口、划分 VLAN、部署访问列表等，控制用户之间的传输安全。

9.1　内部网络防火墙

防火墙是每个企业网络必备的安全设备，主要用于隔离两个或几个信任度不同的网络，最常见的就是部署在网络边缘的边缘防火墙。另外，在许多大中型企业网络安全需求较高的局域网中，往往会在不同的部门或子网之间部署内部防火墙。内部防火墙与边缘防火墙的功能和应用有所不同，因此在选购设备和规划网络结构时应区别对待。

9.1.1　内部防火墙规划与设计

连接不同内部网络是网络防火墙的重要应用之一。这种应用环境就是在一个企业内部网络之间，对一些安全性要求较高的部门（如人事管理或财务管理等）进行隔离保护，使内部网络中敏感部门的资源不被非法访问。在这些部门的网络主机中的数据对于企业来说是非常重要的，它的工作不能完全离开企业网络，但其中的数据又不能随便供网络用户访问。

一种有效的方法就是采用防火墙进行隔离，在防火墙上进行相关的配置（比起划分 VLAN 来简单许多）。通过防火墙隔离后，尽管同属于一个内部局域网，但是其他用户的访问都需要经过防火墙的过滤，符合条件时才能访问。这类防火墙不仅要通过包过滤来筛选数据包，而且还要对用户身份的合法性（在防火墙中可以设置允许哪些用户访问）进行识别，通常为自适应代理服务器型防火墙；同时它具有日志记录功能，对网络管理员了解网络安全现状及改进非常重要。在如图 9-1 所示的网络中，同是一个企业的内部网络，可以将需要受到保护的重要部门和一些服务器通过防火墙连接至其他网络。

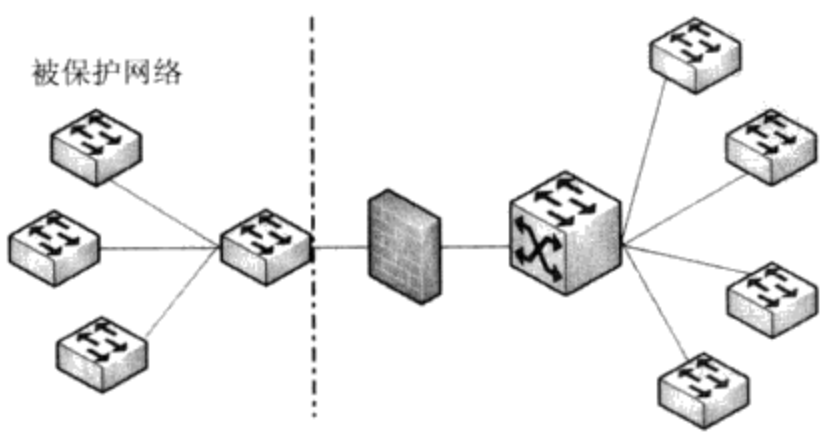


图 9-1　连接内部子网络

9.1.2 内部防火墙的选择

内部防火墙部署在企业网络中安全需求较高的网络分支上，如财务部、研发部、人事部等，为了控制普通内网用户对这些敏感部门的访问，就可以在这些部门的网络边缘部署一道防火墙，位于内网之间的防火墙也被称为二级防火墙。

通常情况下，内部防火墙在企业网络中应用并不多，因为很多网络访问控制措施都可以基于支持网络管理的汇聚层交换机实现，并且大中型网络中汇聚层交换机都是三层的，管理员只需配置 ACL 即可实现不同 VLAN 之间的访问行为。但是这种基于三层交换机的网络访问隔离，都是粗略的控制，不可能像防火墙那样通过动态包过滤机制来实现访问策略的控制，因此只适用于中等安全需求的内部网络分支。

如果网络中某些部门安全需求较高，则必须部署内部防火墙，并进行合理配置。由于内部防火墙只需对某一网络分支的网络流量进行过滤和控制，所以一般负载较轻，无需追求过高的硬件配置。通常情况下，可以使用基于核心交换机或核心路由器的防火墙模块，作为内网络部门间的防火墙。如图 9-2 所示是可以在 Cisco Catalyst 6500 系列交换机和 Cisco 7600 系列路由器中提供状态防火墙功能的 FWSM 模块，本身并不带任何外部端口，只能通过在交换机或路由器上进行相应配置，使某些网络的流量通过此设备，以接受防火墙的安全保护。因此，这类防火墙更适合于内部网络。

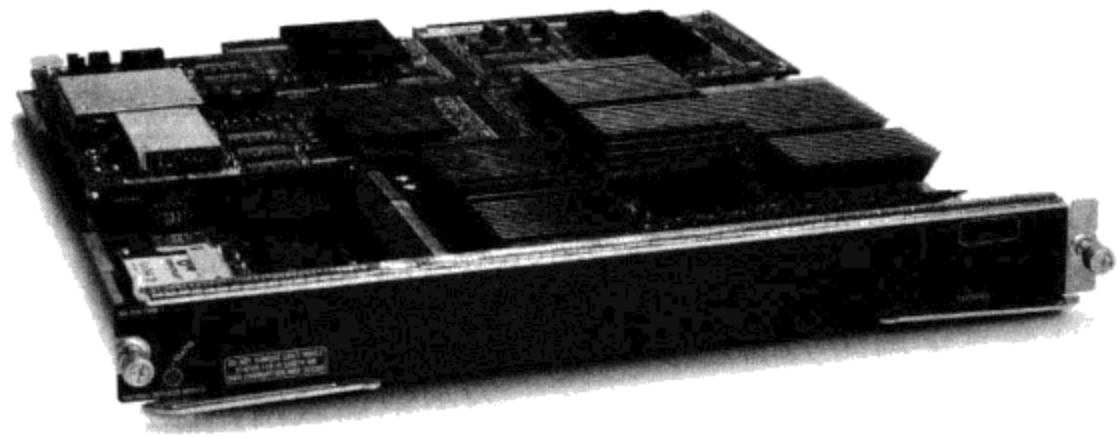


图 9-2 Cisco FWSM 模块

9.1.3 内部防火墙配置实例

1. 网络环境概述

在中等规模的局域网中往往会采用 Cisco 6509 或同等级别的模块化交换机，作为核心交换机，并且通常会同时配置两台互为备份。例如，如图 9-3 所示是某局域网的核心部分，两台 Cisco 6509 交换机作为核心主干，两块 FWSM 卡板部署为 Failover 模式，受保护网络的汇聚交换机为 Cisco 3750G，通过两条链路连接至两台 Cisco 6509。

其中，VLAN10 是防火墙的内部接口，VLAN20 是防火墙的外部接口，用于和 Cisco 6509 通信。Cisco 6509 的 G3/23 口连接到 Cisco 3750 的上连端口。需要注意的是防火墙的链路冗余和三层交换机或路由器有所不同，是二层链路上的冗余。所以即使是 A/A（Active\Active，两者都处于活动状态）对于同一个虚拟防火墙而言，也不是负载均衡的，只不过如果虚拟墙很多，

可以互相调整主和备，使两台防火墙同时工作。如果是 A\S（Active\Standby，活动/待机）模式，则不能。VLAN10 和 VLAN20 之所以都是 29 掩码，是因为内部接口需要 3 个地址，外部接口需要 5 个地址。为了保证更高的冗余性，外部接口采用 HSRP（热备份路由器协议），用以保证外部网关的更高的可靠性。

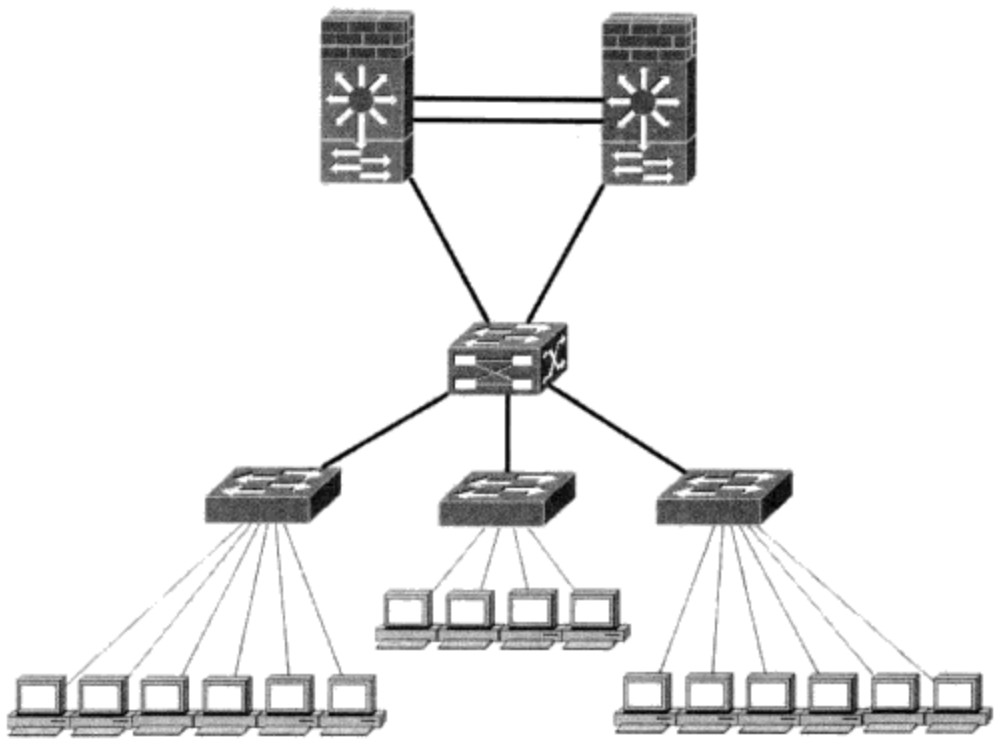


图 9-3　实例拓扑图

2. Cisco 6509 的配置

在 Cisco 6509 上面配置需要的逻辑接口 VLAN，需要注意的是，防火内部的 VLAN 也是在外面定义的，而并不是在防火墙里面定义。

第 1 步，将需要划分进入防火墙的 VLAN 划入不同的组，如果虚拟防火墙较少，可以都划分到一个组中，也可以分类别划分组。

```
Router(config)# firewall vlan-group firewall_group vlan_range
```

第 2 步，将 VLAN 组添加到防火墙模块中，这里的 module_number 是你防火墙卡板的槽位，例如防火墙卡板在第 2 槽，则 module_number 就是 2。注意，每次添加 VLAN 进入 VLAN 组时，都要执行一次该命令，否则新增加的 VLAN 不会划分进入防火墙内。

```
Router(config)# firewall module module_number vlan-group firewall_group
```

第 3 步，将 VLAN10 和 VLAN20 划分进入防火墙后外部配置基本完成。

2. 防火墙模块的配置

第 1 步，登录防火墙模块。

```
6509#session slot 2 processor 1
```

第 2 步，将防火墙设置为网络模式。

```
FWSM(config)# no firewall transparent
```

第 3 步，将防火墙设置为 multiple 模式，用以支持 A/A 模式。

```
FWSM(config)# mode multiple
```

提示 执行此命令后，将重新启动防火墙板卡。

3. 定义在 A/A 模式下的故障转移

■ 主防火墙配置

第 1 步，定义此卡板为主。

```
FWSM(config)# failover lan unit primary
```

第 2 步，定义 Failoverlink VLAN 为 30，其作用是同步故障转移信息，如 hello 包等。

```
FWSM(config)# failover lan interface failoverlink vlan 30
```

第 3 步，定义 Failoverlink 的 IP 地址，要求主和备必须是同一个网段内。

```
FWSM(config)# failover interface ip failoverlink 10.75.0.1 255.255.254 standby
10.75.0.2
```

第 4 步，定义 Statelink VLAN 为 31，用以同步数据。如果不定义 Statelink，则同步的数据是通过 Failoverlink 传输。

```
FWSM(config)# failover link statelink vlan 31
```

第 5 步，定义 Statelink 的主和备

```
FWSM(config)# failover interface ip statelink 10.75.0.5 255.255.255.254
standby 10.75.0.6 #定义。
```

第 6 步，登录 group 1。

```
FWSM(config)# failover group 1
```

第 7 步，将 group 1 设置为主。

```
FWSM(config-fover-group)# primary
```

第 8 步，进入 group 2。

```
FWSM(config)# failover group 2
```

第 9 步，将 group 2 设置为备。

```
FWSM(config-fover-group)# secondary
```

第 10 步，创建虚拟防火墙 NC

```
FWSM(config)# context NC-Security
```

第 11 步，将此防火墙加入 group 1。

```
FWSM(config -ctx)# join-failover-group 1
```

第 12 步，启用 failover。

```
FWSM(config)#failover
```

■ **备防火墙配置**

第 1 步，定义此卡板为备

```
FWSM(config)# failover lan unit secondary
```

第 2 步，定义 failoverlink vlan。

```
FWSM(config)# failover lan interface failoverlink vlan 30
```

第 3 步，定义 failoverlink 的 IP 地址，与主防火墙相同即可。

```
FWSM(config)# failover interface ip failoverlink 10.75.0.1 255.255.254 standby
10.75.0.2
```

第 4 步，启用 failover。

```
FWSM(config)#failover
```

第 5 步，定义虚拟防火墙，与主防火墙完全相同。

```
FWSM(config)# context NC
```

第 6 步，将 VLAN10 和 VLAN20 划入此虚拟防火墙。

```
FWSM(config-ctx)# allocate-interface vlan 10 20
```

第 7 步，登录逻辑防火墙 NC。

```
FWSM# changeto context NC
```

接下来即可开始定义访问列表、访问控制策略、NAT 等。

9.2 基于端口的传输控制

目前，几乎所有企业网络中部署的都是可网管交换机，其实很多传输安全控制和防护措施都可以基于交换机完成。借助对交换机端口传输控制的配置，既可以有效杜绝广播风暴对整个网络的冲击，从而保证网络的正常通信。同时，又可以拒绝未被授权的计算机接入网络，或者限制某个端口接入计算机的数量，从而保证网络的接入安全，避免网络被个别用户滥用。

9.2.1 风暴控制

当端口接收到大量的广播、单播或多播包时，就会发生广播风暴。转发这些包将导致网络速度变慢或超时。借助于对端口的广播风暴控制，可以有效地避免因硬件损坏或链路故障而导致的网络瘫痪。默认状态下，广播、多播和单播风暴控制被禁用。

1. 启用风暴控制

第1步，进入配置模式。

```
Switch# config terminal
```

第2步，指定欲配置的接口。

Switch(config)# interface interface-id

第3步，配置广播、多播或单播风暴控制。默认状态下，风暴控制被禁用。

- level，指定阻塞端口的带宽上限值。当广播、多播或单播传输占到宽带的多大比例（百分比）时，端口将阻塞传输。取值范围为0.00~100.00。如果将值设置为100%，将不限制任何传输；如果将值设置为0%，那么该端口的所有广播、多播和单播都将被阻塞。
- level-low，指定启用端口的带宽下限值。该值应当小于或等于下限值，当广播、多播或单播传输占用带宽的比例低于该值时，端口恢复转发传输。取值范围为 0.00 ~ 100.00。
- bps，指定端口阻塞的传输速率上限值。当广播、多播或单播传输达到每秒若干比特（bps）时，端口将阻塞传输。取值范围为0.0 ~ 10 000 000 000.0。
- bps-low，指定端口启用的传输速率下限值。该值应当小于或等于下限值，当广播、多播或单播传输低于每秒若干比特（bps）时，端口将恢复传输。取值范围为0.0 ~ 10 000 000 000.0。如果数值较大，也可以使用K、M或G等词头单位表示。
- pps，指定端口阻塞的转发速率上限值。当广播、多播或单播传输速率达到每秒若干包（pps）时，端口将阻塞传输。取值范围为0.0~10 000 000 000.0。
- pps-low，指定端口启用的传输速率下限值。该值应当小于或等于下限值，当广播、多播或单播转发速率低于每秒若干包（pps）时，端口将恢复传输。取值范围为0.0~ 10 000 000 000.0。如果数值较大，也可以使用K、M或G等单位表示。
- Switch(config-if)# storm-control {broadcast | multicast | unicast} level {level [level-low] | bps bps [bps-low] | pps pps [pps-low]}

第4步，指定风暴发生时如何处理。默认状态下，将过滤外出的传输，并不发送SNMP陷阱。选择“shutdown”关键字，在风暴期间将禁用端口；选择“trap”关键字，当风暴发生时，产生一个SNMP陷阱，向网络管理软件发出警报。

```
Switch(config-if)# storm-control action {shutdown | trap}
```

第5步，返回特权配置模式。

```
Switch(config-if)# end
```

第6步，显示并校验该接口当前的配置。

```
Switch# show storm-control [interface] [{broadcast | history | multicast | unicast}]
```

第7步，保存风暴控制配置。

```
Switch# copy running-config startup-config
```

2. 禁用风暴控制

第 1 步，进入配置模式。

```
Switch# config terminal
```

第 2 步，指定欲配置的接口。

```
Switch(config)# interface interface-id
```

第 3 步，禁用端口风暴控制。

```
Switch(config-if)# no storm-control {broadcast | multicast | unicast}
```

第 4 步，禁用指定的风暴控制动作。

```
Switch(config-if)# no storm-control action {shutdown | trap}
```

第 5 步，返回特权配置模式。

```
Switch(config-if)# end
```

第 6 步，显示并校验该接口当前的配置。

```
Switch# show storm-control [interface] [{broadcast | multicast | unicast}]
```

第 7 步，保存配置。

```
Switch# copy running-config startup-config
```

9.2.2 流控制

流控制只适用于 1000Base-T、1000Base-SX 和 GBIC 端口。在千兆位端口启用流控制后，可以在拥塞期间暂停其他终端的连接。当端口处于拥塞状态，无法接收到数据流时，将通知其他端口暂时发送，直到恢复正常状态。当本地设备发现任何终端发生拥塞时，将发送一个暂停帧，以通知其连接伙伴或远端拥塞设备。收到暂停帧后，远程设备将停止发送任何数据包，以防止在拥塞期内丢失任何数据包。

第 1 步，进入全局配置模式。

```
Switch# configure terminal
```

第 2 步，选择欲配置的端口，进入接口配置模式。

```
Switch(config)# interface interface-id
```

第 3 步，设置端口的流控制。

```
Switch(config-if)# flowcontrol {receive | send} {on | off | desired}
```

第 4 步，返回特权配置模式。

```
Switch(config-if)# end
```

第5步，显示接口状态。

```
Switch# show interfaces interface-id
```

第6步，保存配置。

```
Switch# copy running-config startup-config
```

9.2.3 保护端口

保护端口可以确保同一交换机上的端口之间不进行通信。保护端口不向其他保护端口转发任何传输，包括单播、多播和广播包。传输不能在第二层保护端口间进行，所有保护端口间的传输都必须通过第三层设备转发。保护端口与非保护端口间的传输不受任何影响。

第1步，进入配置模式。

```
Switch# config terminal
```

第2步，指定欲配置的接口。

```
Switch(config)# interface interface-id
```

第3步，将接口配置为保护端口。

```
Switch(config-if)# switchport protected
```

第4步，返回特权配置模式。

```
Switch(config-if)# end
```

第5步，显示并校验该接口当前的配置。

```
Switch# show interfaces interface-id switchport
```

第6步，保存配置。

```
Switch# copy running-config startup-config
```

若欲禁用保护端口，可以使用“no switchport protected”接口配置命令。

9.2.4 端口阻塞

默认状态下，未知目的MAC地址的泛洪包被允许从端口向外传输。如果未知的单播和多播通信被转发到保护端口，将导致安全问题。可以采用阻塞端口的方式，防止未知的单播和多播通信被转在端口间转发。

第1步，进入配置模式。

```
Switch# config terminal
```

第2步，指定欲配置的接口。

```
Switch(config)# interface interface-id
```

第 3 步，禁止未知多播从该端口向外传输。

```
Switch(config-if)# switchport block multicast
```

第 4 步，禁止未知单播从该端口向外传输。

```
Switch(config-if)# switchport block unicast
```

第 5 步，返回特权配置模式。

```
Switch(config-if)# end
```

第 6 步，显示并校验该接口当前的配置。

```
Switch# show interfaces interface-id switchport
```

第 7 步，保存配置。

```
Switch# copy running-config startup-config
```

9.2.5 端口安全

借助安全端口，可以只允许指定的 MAC 地址或指定数量的 MAC 地址访问某个端口，从而避免未经授权的计算机接入网络，或限制某个端口所连接的计算机数量，从而确保网络接入的安全。当配置端口安全时，应当注意以下问题：

- 安全端口不能是 Trunk 端口。
- 安全端口不能是 Switch Port Analyzer（SPAN）的目的端口。
- 安全端口不能是属于 EtherChannel 的端口。
- 安全端口不能是 private-VLAN 端口。

1. 配置安全端口

第 1 步，进入全局配置模式。

```
Switch# configure terminal
```

第 2 步，指定欲配置端口安全的接口。

```
Switch(config)# interface interface_id
```

第 3 步，将接口设置为访问模式。

```
Switch(config-if)# switchport mode access
```

第 4 步，在接口启用端口安全。

```
Switch(config-if)# switchport port-security
```

第 5 步，（可选）在接口设置安全 MAC 地址的最大数量，以限制该端口所连接的计算机数量。取值范围为 1~3072，默认值是 1。

```
Switch(config-if)# switchport port-security maximum value
```

第6步，（可选）设置违例发生后的处理模式。当安全违例事件发生时，将端口置于restrict或shutdown模式。选择restrict模式，当非法MAC地址或太多MAC连接至该接口时，将丢弃数据包，并向网管计算机发送SNMP陷阱通知。选择shutdown模式时，发生安全错误的端口将被置于error-disable状态，除非网络管理员使用“no shutdown”命令手工激活，否则该端口失效。

```
Switch(config-if)# switchport port-security violation {restrict | shutdown}
```

第7步，设置坏包速率限制。

```
Switch(config-if)# switchport port-security limit rate invalid-source-mac
```

第8步，（可选）为该接口指定安全MAC地址。也可以使用该命令指定最大安全MAC 地址数。如果指定的MAC地址数量少于安全地址的最大数量，动态学习的MAC地址将被保留。

```
Switch(config-if)# switchport port-security mac-address mac_address
```

第9步，在端口启动sticky learning。

```
Switch(config-if)# switchport port-security mac-address sticky
```

第10步，返回特权EXEC模式。

```
Switch(config-if)# end
```

第11步，查看并校验配置。

```
Switch# show port-security address interface interface_id
Switch# show port-security address
```

第12步，保存当前配置。

```
Switch# copy running-config startup-config
```

注意 使用no switchport port-security mac-address mac_address命令，可以从地址表中删除MAC地址。

2. 设置端口安全老化

当为端口指定最大MAC地址数时，为了保障该端口能够得以充分利用，可以采用设置端口安全老化时间和模式的方式，使系统能够自动删除长时间未连接的MAC地址，从而不必手工删除，减少网络维护的工作量。

第1步，进入全局配置模式。

```
Switch# configure terminal
```

第2步，指定欲配置端口安全老化的接口。

```
Switch(config)# interface interface_id
```

第 3 步，为安全端口设置老化时间和老化类型。老化时间的取值范围为 0~1440 min。采用 absolute 模式时，一旦到达指定的老化时间，即将其从安全地址列表中移除。采用 inactivity 时，即使到达指定的老化时间，如果没有其他数据通信，那么，MAC 地址仍然被保留在安全地址列表中。

```
Switch(config-if)# switchport port-security  [ aging time aging_time | type {absolute | inactivity} ]
```

第 4 步，返回特权 EXEC 模式。

```
Switch(config-if)# end
```

第 5 步，查看并校验配置。

```
Switch# show port security [interface interface_id] [address]
```

第 6 步，保存当前配置。

```
Switch# copy running-config startup-config
```

9.2.6 传输速率限制

网络传输速率变慢的主要原因往往是某些用户对网络的滥用。当使用 MRTG 等流量监控软件检测到流量来源于某个端口时，可以在核心交换机、汇聚交换机，甚至接入交换机上，对相应的端口作必要的处理，限制其传输带宽，从而限制每个用户所允许的最大流量，以便使其他网络用户能够恢复正常的网络应用服务。

第 1 步，进入配置模式。

```
Switch# config terminal
```

第 2 步，指定欲配置的接口。

```
Switch(config)# interface interface-id
```

第 3 步，配置端口带宽控制。其中，input/output 表明在输入和输出方向应用该带宽限制，通常情况下，应当进行双向限制。access-group acl-index 用于定义使用该带宽限制的访问列表。bps 用于定义限制带宽，以 bps 为单位，并采用 8 Kbps 的增量。burst-normal 用于定义所允许的普通突发速率，burst-max 用于定义所允许的最大突发速率。conform-action conform-action 用于指定在规定最大带宽时所执行的操作，通常为“transmit”即允许发送。exceed-action exceed-action 则用于指定在规定最大带宽时所执行的操作，通常为“drop”即丢弃。

```
Switch(config-if)# rate-limit {input | output} [access-group acl-index] bps burst-normal burst-max conform-action conform-action exceed-action exceed-action
```

第 4 步，返回特权配置模式。

```
Switch(config-if)# end
```

第5步，显示并校验该接口当前的配置。

```
Switch# show interface interface-id
```

第6步，保存带宽限制配置。

```
Switch# copy running-config startup-config
```

例如，若欲限制GigabitEthernet4/4带宽为128 Kbps，当连接的普通突发速率、最大突发速率在8 KBps（即64 Kbps）、9 KBytes（即72 Kbps）范围内时，所执行的操作是“transmit”（传输即发送）。当超出该范围时，则相应的操作就是“drop”。其中，128 000用于限制最大带宽，8000和9000则用于限制突发连接，保证不因个别用户的大量传输而使整个链路性能大幅度下降。限制输入和输出速率后，该端口配置如下：

```
interface GigabitEthernet4/4
no switchport
description tushuguan
ip address 211.82.220.9 255.255.255.248
ip access-group 120 in
ip access-group 120 out
rate-limit output access-group 102 128000 8000 9000 conform-action transmit
exceed-action drop
rate-limit input access-group 102 128000 8000 9000 conform-action transmit
exceed-action drop
!
```

IP访问列表只需设置应用带宽限制的IP地址范围（192.168.0.0～192.168.255.255）即可，内容如下：

```
access-list 102 permit ip 192.168.0.0 0.0.255.255 any
```

提示 启用宽带限制之前，必须先在全局模式下执行“ip cef”命令，启用交换机的快速转发技术。

9.2.7 MAC地址更新通知

MAC地址是交换机进行快速转发和传输的重要依据，但是交换机的MAC地址表的容量是有限的，随着新用户的接入，原有老用户的MAC地址可能会被清除。当使用交换机的用户较多时，可能在短时间内会有大量的MAC地址变化产生（如计算机机房开放时）。因此，为了减少网络流量，可以设置发送MAC地址通知的时间间隔。系统会将指定的时间间隔地址通知信息加以捆绑，这样在每条地址通知信息中，就包含了若干个MAC地址变化的信息，这样就会有效地减少网络流量。

1. 设置MAC地址通知

当MAC地址通知产生时，通知信息同时会记录到MAC地址通知历史记录表中。如果没

有配置接收 Trap 的 NMS（网络管理服务器）或没有及时接收 MAC 地址变化的 Trap，可以通过查看 MAC 地址通知历史记录表来了解最近 MAC 地址变化的消息。MAC 地址通知功能是基于端口的，但 MAC 地址通知有一个全局开关。在全局开关打开的情况下，如果打开某个端口上的 MAC 地址通知功能，那么该端口上 MAC 地址的变化将会产生通知，而没有打开该功能的端口的 MAC 地址变化将不会产生通知。可以让端口仅仅发送地址增加或减少的通知，也可以两者都发。如果 MAC 地址通知全局开关关闭，则所有端口上均不会产生 MAC 地址通知。

提示 MAC 地址通知功能仅针对动态地址，对于静态配置的地址的变化将不会产生通知信息。默认情况下，MAC 地址的全局开关是关闭的，所有端口的 MAC 地址通知功能也均被关闭。

交换机 MAC 地址通知功能配置如下：

第 1 步，进入全局配置模式。

```
Switch# configure terminal
```

第 2 步，配置接收 MAC 地址通知的 NMS。其中，host-addr 用于指明网管工作站的 IP 地址。Version 用于指明发送哪种版本的 Trap。community-string 用于指明发送的 Trap 上附带的 SNMP 字符串。

```
Switch(config)# snmp-server host host-addr {traps | informs} {version {1|2c}}
community-string notification-type
```

第 3 步，允许交换机发送 MAC 地址通知的 Trap。

```
Switch(config)# snmp-server enable traps mac-notification
```

第 4 步，打开 MAC 地址通知功能的全局开关。

```
Switch(config)# mac-address-table notification
```

第 5 步，设置 MAC 地址通知的时间间隔和 MAC 记录表的最大个数。interval value（可选）用于设置产生 MAC 地址通知的时间间隔。时间间隔的单位为秒，范围为 0~3 600，默认为 1 s。history-size value 用于设置 MAC 通知历史记录表中记录的最大个数，范围 0~200，默认为 50。

```
Switch(config)# mac-address-table notification {interval value | history-size
value}
```

第 6 步，进入端口配置模式，指定具体哪个端口上打开 MAC 地址通知功能。

```
Switch(config)# interface interface-id
```

第 7 步，打开端口的 MAC 地址通知功能。added 用于表明当地址增加时通知，removed 用于表明当地址被删除时通知。

```
Switch(config-if)# snmp trap mac-notification {added | removed}
```

第 8 步，返回特权 EXEC 模式。

```
Switch(config-if)# end
```

第9步，查看并校验配置。

```
Switch# show running-config
Switch# show mac-address-table notification interface
```

第10步，保存当前配置。

```
Switch# copy running-config startup-config
```

可以在全局配置模式下通过命令 no snmp-server enable traps mac-notification 来禁止交换机发送 MAC 地址变化通知的 Trap，使用命令 no mac-address-table notification 来关闭 MAC 地址通知的全局开关。此外，可以在接口配置模式下，使用命令 no snmp trap mac-notification {added | removed}来关闭指定接口的相应 MAC 地址通知功能。

例如，打开 MAC 地址通知功能，并以 public 为认证名向 IP 地址为 211.82.214.58 的 NMS 发送 MAC 地址变化通知的 Trap，产生 MAC 地址变化通知的间隔时间为 60 s，MAC 地址通知历史记录表的大小为 100，打开接口 fastethernet 0/4 上当 MAC 地址增加和减少时进行通知的功能（如图 9-4 所示）。

图 9-4 启用 MAC 地址通知

相关配置过程如下：

```
Switch# configure terminal
Switch(config)# snmp-server host 211.82.214.58 traps public
Switch(config)# snmp-server enable traps mac-notification
Switch(config)# mac-address-table notification
Switch(config)# mac-address-table notification interval 60
Switch(config)# mac-address-table notification history-size 100
Switch(config)# interface fastethernet 0/4
Switch(config-if)# snmp trap mac-notification added
Switch(config-if)# snmp trap mac-notification removed
Switch(config-if)# end
```

```
Switch# copy running-config startup-config
```

2. 查看 MAC 地址变化通知信息

在特权模式下，可以使用下表所列的命令来查看交换机的 MAC 地址表信息：

查看 MAC 地址变化通知功能的全局配置信息（如图 9-5 所示）。

```
Switch# show mac-address-table notification
```

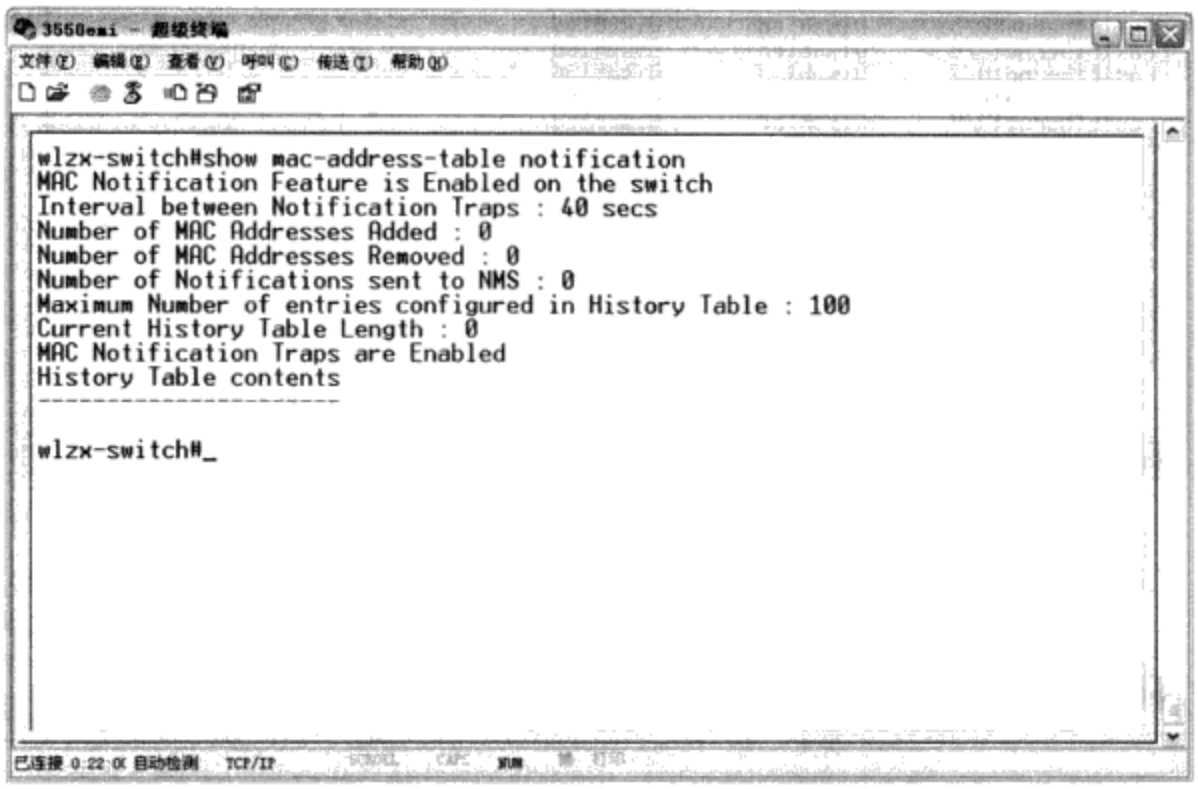


图 9-5 MAC 地址变化通知功全局配置信息

查看指定接口 MAC 地址变化通知功能状况（如图 9-6 所示）。

```
Switch# show mac-address-table notification interface interface-id
```

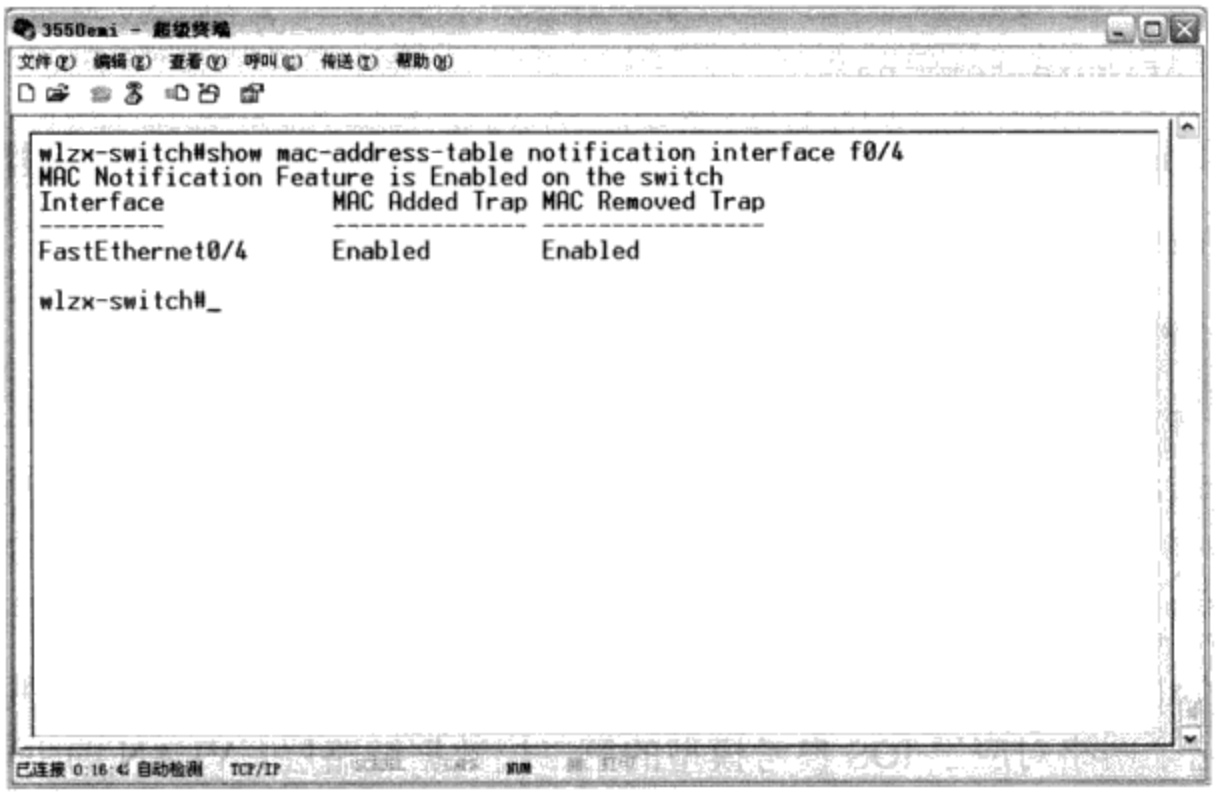


图 9-6 指定接口 MAC 地址变化通知功能状况

查看所有接口 MAC 地址变化通知功能状况（如图 9-7 所示）。

```
Switch# show mac-address-table notification interface
```

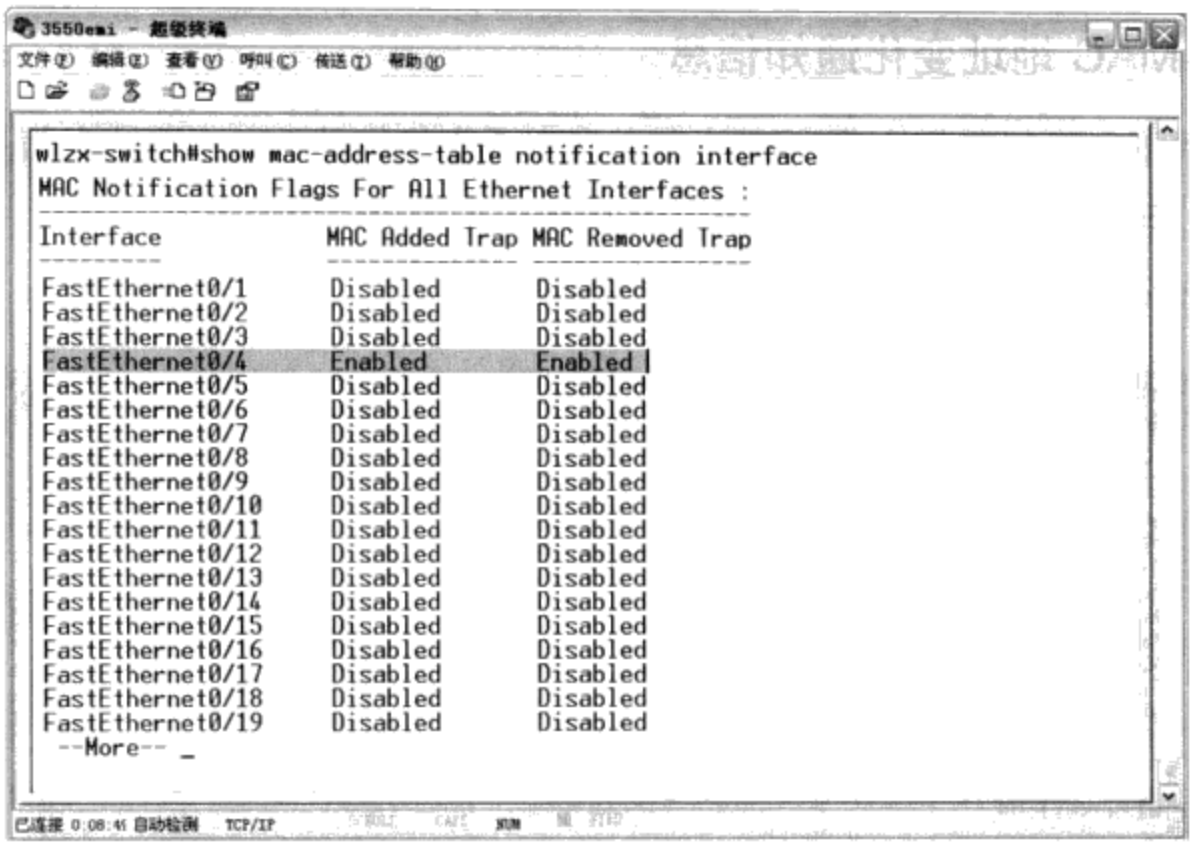


图 9-7 所有接口 MAC 地址变化通知状况

9.2.8 绑定 IP 和 MAC 地址

许多安全设置都是基于 IP 的，而用户的 IP 地址却可以自己随意设置。因此，还应当同时采取另外一种安全措施，即在交换机中将 IP 地址与 MAC 地址绑定在一起。这样，即使用户设置了 IP 地址，也由于 MAC 地址不同而不能获得相应的权限，从而保证网络的安全。

使用下述命令，可将 MAC 地址与 IP 地址绑定在一起：

第 1 步，进入全局配置模式。

```
Switch# configure terminal
```

第 2 步，绑定 IP 地址与 MAC 地址。若欲绑定若干 IP 地址，需要重复该操作。

```
Switch(config-if)# arp ip-address mac-address arpa
```

第 3 步，保存当前配置。

```
Switch# copy running-config startup-config
```

9.3 VLAN 安全

VLAN（Virtual Bridged Local Area Network，虚拟局域网）是在一个物理网络上划分出来的逻辑网络。这个网络对应于 IOS 参考模型的第二层数据链路层。VLAN 的主要作用有两点，一是提高网络安全性，阻止未经授权的 VLAN 访问；二是提高网络传输效率，将广播隔离在子网之内。因此，VLAN 在网络安全性和稳定性方面，都起着非常重要的作用。

9.3.1 VLAN 概述

VLAN 有着和普通物理网络同样的属性，除了没有物理位置的限制外，它和普通局域网是一样的，第二层的单播、广播和多播帧可以在一个 VLAN 内转发、扩散，而不会直接进入其他的 VLAN 之中。所以，如果一个 VLAN 端口所连接的主机想要和另外一个 VLAN 端口的主机通信，则必须通过一个三层设备进行转发，如路由器或者三层交换机等。

1. 划分 VLAN 的意义

在局域网络中使用 VLAN，具有以下重要意义：

- 降低移动和变更的管理成本。VLAN 中的成员与其物理位置无关，既可连接至同一台交换机，也可连接至不同交换机。当需要把一台计算机从一个子网转移到另一个子网时，迁移工作将只是由网络管理员在用作网络管理的计算机上重新定义一下 VLAN 成员即可。
- 控制广播。由于所有的广播都只在本 VLAN 内进行，而不再扩散到其他 VLAN 上，将大大减少广播对网络带宽的占用，提高带宽传输效率，并可有效地避免广播风暴的产生。
- 增强安全性。VLAN 的一个重要好处就是提高了网络安全性。由于交换机只能在同一 VLAN 内的端口之间交换数据，不同 VLAN 的端口不能直接相互访问。因此，通过划分 VLAN，就可以在物理上防止某些非授权用户访问敏感数据。
- 网络监督和管理的自动化。由于网络管理员可以通过网管软件，查到 VLAN 间和 VLAN 内通信的数据报的细目分类信息，以及应用数据报的细目分类信息，而这些信息对于确定路由系统和经常遭到访问的服务器的最佳配置十分有用。通过划分 VLAN，可以使网络管理变得更简单、更轻松、更有效。

基于端口的 VLAN 是最常使用的划分 VLAN 的方式，几乎被所有的交换机所支持。所谓基于端口的 VLAN，是指由网络管理员使用网管软件或直接设置交换机，将某些端口直接地、强制性地分配给某个 VLAN。除非网管人员重新设置，否则，这些端口将一直保持对该 VLAN 的从属性，即属于该 VLAN，因此这种划分方式也称为静态 VLAN。这种方法虽然在网络管理员进行 VLAN 划分操作时会比较麻烦，但相对安全，并且容易配置和维护。同时，由于不同 VLAN 间的端口不能直接相互通信，因此每个 VLAN 都有自己独立的生成树。此外，交换机之间在不同 VLAN 中可以有多个并行链路，以提高 VLAN 内部的交换速率，增加交换机之间的带宽。

2. VLAN 的划分方式

从技术角度讲，VLAN 的划分可依据不同原则，常用的划分方式有以下 3 种：

- 基于端口的 VLAN 划分。这种划分是把一个或多个交换机上的几个端口划分一个逻辑组，这是最简单、最有效的划分方法。该方法只需网络管理员对网络设备的交换端口进行重新分配即可，不用考虑该端口所连接的设备。
- 基于 MAC 地址的 VLAN 划分。MAC 地址其实就是指网卡的标识符，每一块网卡的 MAC 地址都是惟一且固化在网卡上的。MAC 地址由 12 位 16 进制数表示，前 8 位

为厂商标识，后4位为网卡标识。网络管理员可按MAC地址把一些站点划分为一个逻辑子网。

- 基于路由的VLAN划分。路由协议工作在网络层，相应的工作设备有路由器和路由交换机（即三层交换机）。该方式允许一个VLAN跨越多个交换机，或一个端口位于多个VLAN中。

其中最常用的就是基于端口和路由来划分VLAN两种方式，基于MAC地址的划分方式仅作辅助之用。

9.3.2 VLAN规划与设计

1. VLAN设计原则

由于VLAN自身的一些特性，如果划分不当，很可能会导致网络无法正常通信或安全性降低，因此在规划和设计VLAN时必须全面考虑各种因素，并遵循一定的划分原则。

- 对于联网计算机或用户数量较多的部门，可根据用户接入信息点的分布划分为多个VLAN。
- 对网络数据安全要求较高的部门（如财务）可以单独划分一个VLAN。
- 对计算机或用户数量较少，且对数据安全要求不高的部门，可以多个部门划分一个VLAN。
- 对于一些使用范围涉及多个部门的服务器等，根据业务内容的不同和其上业务数据的安全要求的高低，划分为多个VLAN。以便更好地对服务器的访问和安全进行控制和管理。
- 对于局域网中的网络设备，各区域的网络设备统一划分到一个VLAN中。

2. VLAN配置策略

在配置VLAN时，应当遵循以下策略。

- 在VTP客户端、服务器和透明模式中，交换机支持1005个VLAN。
- 标准序列VLAN的ID号为1~1001。VLAN号为1002~1005是Token Ring和FDDI VLAN。
- VLAN 1~1005通常被保存在VLAN数据库中。如果VTP模式是透明的，VTP和VLAN配置也保存在交换机运行配置文件中。
- 在VTP透明模式（VTP禁用）中，交换机也支持VLAN ID 1006~4094。该扩展序列VLAN和配置选项被限制。扩展序列VLAN不能被保存在VLAN数据库。
- 在创建VLAN之前，交换机必须处于VTP服务器模式或VTP透明模式。如果交换机是VTP服务器，必须定义VTP域。
- 交换机支持128个生成树实例。如果交换机有太多的活动VLAN，超过所支持的扩展树，扩展树将在128个VLAN启用，并且禁用其他的VLAN。

3. VLAN默认配置

以太网VLAN默认配置和范围如表9-1所示。

表 9-1　以太网 VLAN 默认配置和范围

属　性	默　认	有效值
VLAN ID	1	1~4094。扩展范围 VLAN(ID 6~4094)不能被保存在 VLAN 数据库
VLAN 名称	VLANxxxx，其中 xxxx 表示为与 VLAN ID 相同的数字，包括 0 开头的 VLAN ID	没有范围
IEEE 802.10 SAID	100001（100000 加 VLAN ID）	1~4294967294
MTU 大小	1500	1500~18190
VLAN 状态	活动	活动，挂起，禁用

9.3.3 配置和管理 VLAN

创建 VLAN 共需要两个步骤，先是创建 VLAN，然后再将相关接口指定至该 VLAN。这个过程相似于先划分若干部门，然后再将人员一一分配至不同部门。

1. 创建 VLAN

■ 配置命令

第 1 步，进入全局配置模式。

```
Switch# configure terminal
```

第 2 步，键入 VLAN ID，进入 VLAN 配置模式。以太网 VLAN ID 的取值范围为 1~1001。其中，VLAN 1 为系统默认 VLAN，不能被创建，也不能被删除。

```
Switch(config)# vlan vlan_id
```

提示　如果键入的 VLAN ID 不存在，那么，此时将自动创建该 VLAN。因此，首次进入某个 VLAN 的过程，也是创建该 VLAN 的过程。

第 3 步，VLAN 命名，便于区分、查看和管理 VLAN。如果不为 VLAN 命名，默认在 VLAN ID 前添加 0 作为 VLAN 名称。例如，VLAN0004 是 VLAN 4 的默认名称。

```
Switch(config-vlan)# name vlan-name
```

提示　为 VLAN 命名后，使用 show vlan 命令，可以方便地查看该 VLAN 所属的部门或用户群，便于对 VLAN 进行后期的配置和管理，因此，建议为每个 VLAN 命名。

第 4 步，返回全局配置模式。

```
Switch(config-vlan)# exit
```

提示　若欲创建多个VLAN，并将端口指定至VLAN，必须一一重复执行上述命令。

第5步，查看并检验VLAN配置。

```
Switch# show vlan [id | name] vlan_name
```

第6步，保存VLAN配置。

```
Switch# copy running-config startup-config
```

■ **配置示例**

在核心交换机Catalyst 4506上创建VLAN 2～VLAN 12和VLAN 100。

```
Hexin_4506# configure terminal
Hexin_4506(config)# vlan 2
Hexin_4506(config-vlan)# name Wangluo
Hexin_4506(config-vlan)# exit
Hexin_4506(config)# vlan 3
Hexin_4506(config-vlan)# name Lingdao
Hexin_4506(config-vlan)# exit
Hexin_4506(config)# vlan 4
Hexin_4506(config-vlan)# name Bangong
Hexin_4506(config-vlan)# exit
Hexin_4506(config)# vlan 5
Hexin_4506(config-vlan)# name Shiyan
Hexin_4506(config-vlan)# exit
Hexin_4506(config)# vlan 6
Hexin_4506(config-vlan)# name Wenke
Hexin_4506(config-vlan)# exit
Hexin_4506(config)# vlan 7
Hexin_4506(config-vlan)# name Like
Hexin_4506(config-vlan)# exit
Hexin_4506(config)# vlan 8
Hexin_4506(config-vlan)# name Jisuanji
Hexin_4506(config-vlan)# exit
Hexin_4506(config)# vlan 9
Hexin_4506(config-vlan)# name Keyan
Hexin_4506(config-vlan)# exit
Hexin_4506(config)# vlan 10
Hexin_4506(config-vlan)# name Tushugan_guanli
Hexin_4506(config-vlan)# exit
Hexin_4506(config)# vlan 11
Hexin_4506(config-vlan)# name Tushugan_yulan
Hexin_4506(config-vlan)# exit
Hexin_4506(config)# vlan 12
Hexin_4506(config-vlan)# name WAN
Hexin_4506(config-vlan)# exit
Hexin_4506(config)# vlan 100
Hexin_4506(config-vlan)# name Fuwuqi
Hexin_4506(config-vlan)# end
Hexin_4506# copy running-config startup-config
Hexin_4506#
```

2. 将端口指定至相应的 VLAN

指定欲配置至该 VLAN 的接口。创建 VLAN 之后，接下来就需要根据规划将相应的端口指定至该 VLAN。

■ 配置命令

第 1 步，进入全局配置模式。

```
Switch# configure terminal
```

第 2 步，指定欲配置的端口或端口范围。

```
Switch(config)# interface {fastethernet | gigabitethernet | tengigabitethernet} slot/port
```

或

```
Switch(config)# interface range interface-range
```

提示 若欲将多个端口指定至同一 VLAN，建议采用指定端口组的方式，一次将多个端口指定至同一 VLAN。

第 3 步，在配置完成之前禁用该端口。

```
Switch(config-if)# shutdown
```

第 4 步，将该接口指定为二层访问模式。

```
Switch(config-if)# switchport mode access
```

注意 在将交换机端口指定至某个 VLAN 之前，必须将该端口设置为二层接口。尤其是对于三层交换机而言，默认状态下，所有接口都是三层接口，因此，将指定端口设置为二层交换端口就显得更为必要。

第 5 步，将该端口指定至相应的 VLAN。

```
Switch(config-if)# switchport access vlan vlan_num
```

第 6 步，重新激活该接口，使其恢复转发状态。

```
Switch(config-if)# no shutdown
```

第 7 步，退出接口配置状态。

```
Switch(config-if)# end
```

第 8 步，查看该接口的运行状态。

```
Switch# show running-config interface {fastethernet | gigabitethernet}
slot/port
```

第9步，显示该接口的交换端口配置。

```
Switch# show interfaces [{fastethernet | gigabitethernet | tengigabitethernet}
slot/port] switchport
```

第10步，保存VLAN配置。

```
Switch# copy running-config startup-config
```

提示 若欲将多个端口指定至不同VLAN，必须一一重复执行上述命令。当然，不能将一个端口指定至多个VLAN。当将一个端口指定至一个新的VLAN后，该端口将只属于新指定的VLAN。

■ 配置示例

在核心交换机Catalyst 4506上按照规划将G2/1～G2/16　指定至VLAN 100，将G2/19~G2/20指定至VLAN 2，将G3/1指定至VLAN 5，将G3/3指定至VLAN 6，将G3/4指定至VLAN 9。

```
Hexin_4506# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Hexin_4506 (config)# interface range g2/1 ~ g2/16
Hexin_4506 (config-if-range)# shutdown
Hexin_4506 (config-if-range)# switchport mode access
Hexin_4506 (config-if-range)# switchport access vlan 100
Hexin_4506 (config-if-range)# no shutdown
Hexin_4506 (config-if-range)# exit
Hexin_4506 (config)# interface range g2/19 ~ g2/20
Hexin_4506 (config-if-range)# shutdown
Hexin_4506 (config-if-range)# switchport mode access
Hexin_4506 (config-if-range)# switchport access vlan 2
Hexin_4506 (config-if-range)# no shutdown
Hexin_4506 (config-if-range)# exit
Hexin_4506 (config)# interface g3/1
Hexin_4506 (config-if)# shutdown
Hexin_4506 (config-if)# switchport mode access
Hexin_4506 (config-if)# switchport access vlan 5
Hexin_4506 (config-if)# no shutdown
Hexin_4506 (config-if)# exit
Hexin_4506 (config)# interface g3/3
Hexin_4506 (config-if)# shutdown
Hexin_4506 (config-if)# switchport mode access
Hexin_4506 (config-if)# switchport access vlan 6
Hexin_4506 (config-if)# no shutdown
Hexin_4506 (config-if)# exit
Hexin_4506 (config)# interface g3/4
Hexin_4506 (config-if)# shutdown
Hexin_4506 (config-if)# switchport mode access
```

```
Hexin_4506 (config-if)# switchport access vlan 9
Hexin_4506 (config-if)# no shutdown
Hexin_4506 (config-if)# end
Hexin_4506# copy running-config startup-config
Hexin_4506#
```

3. 管理 VLAN

如果交换机处于 VTP 透明模式，VLAN 配置被保存在运行配置文件时，也被保存至 VLAN 数据库。这里只是将当前配置保存至启动配置。

■ 删除指定 VLAN

使用 no vlan vlan_id 命令，可删除指定的 VALN。

第 1 步，进入全局配置模式。

```
Switch# configure terminal
```

第 2 步，删除指定的 VLAN。

```
Switch(config-vlan)# no vlan vlan_id
```

第 3 步，更新 VLAN 数据库，并返回特权配置模式。

```
Switch(config-vlan)# end
```

第 4 步，校验 VLAN 的改变。

```
Switch(config-vlan)# show vlan brief
```

第 5 步，保存 VLAN 配置。

```
Switch# copy running-config startup-config
```

提示 删除 VLAN 后，所有指定至 VLAN 的端口将不再可用，直到将其指定至新 VLAN 时止。若欲一次性删除所有创建的 VLAN，则必须借助删除 vlan.dat 数据库的方式。

■ 清除接口配置

将指定接口恢复为默认值，即可清除该接口的所有配置，当然也包括 VLAN 设置。

第 1 步，进入 VLAN 配置模式。

```
Switch# config terminal
```

第 2 步，清除某接口的所有配置。

```
Switch(config)# default interface {fastethernet | gigabitethernet | tengigabitethernet} slot/port
```

第 3 步，返回特权配置模式。

```
Switch(config)# end
```

第4步，保存对配置的修改。

```
Switch# copy running-config startup-config
```

提示 若欲将接口指定至其他VLAN，只需直接将其指定至新VLAN ID即可，而不必先清除接口配置再指定至新VLAN。

9.3.4 配置 VLAN Trunk

当在交换机上划分有多个VLAN时，若欲借助一条链路实现与其他交换机的通信，就必须创建Trunk（中继）。默认状态下，第二层接口自动处于动态的Switchport模式，当相邻接口（即借助于双绞线或光纤连接在一起的两个端口）支持Trunk，并且配置为Trunk或动态匹配模式时，该链接即可作为Trunk链接。

1. Trunk封装协议与适用

可以借助IEEE 802.1Q、ISL（Inter-Switch Link Protocol，交换链路协议）和DTP（Dynamic Trunking Protocol，动态中继协议）等3种不同的封装协议创建中继。

其中，

802.1Q作为IEEE标准适用于在任意交换机之间创建中继。因此，无论是在Cisco交换机之间，还是在Cisco交换机与其他品牌的交换机创建Trunk，802.1Q封装协议无疑都是最佳选择。

ISL是Cisco私有协议，主要用于维护交换机和路由器间的通信流量等VLAN信息。DISL（Dynamic Inter-Switch Link Protocol，动态交换链路内协议）则简化了两台相互连接的快速以太网设备上ISL中继的创建过程。

DTP用于管理Trunk协商，支持在ISL和802.1Q中继间自动协商。

两个接口的Trunk模式、Trunk封装类型和硬件能力决定了连接创建为ISL中继还是802.1Q中继。

以太网Trunk封装类型如表9-2所示。

表9-2 以太网Trunk封装类型

封装类型	封装命令	描述
ISL	switchport trunk encapsulation isl	在Trunk链路上指定ISL封装
802.1Q	switchport trunk encapsulation dot1q	在Trunk链路上指定802.1Q封装
Neighboring	switchport trunk encapsulation negotiate	指定接口与相邻接口协商，根据相邻接口的配置和能力，创建ISL或802.1Q中继

Cisco Catalyst交换机平台支持的中继协议如表9-3所示。

表 9-3　Cisco Catalyst 交换机平台支持的中继协议

平台	802.1Q	ISL	DTP
Catalyst 6500/6000 (CatOS)	是	是	是
Catalyst 6500/6000 (Cisco IOS)	是	是	是
Catalyst 5500/5000	是	是	是
Catalyst 4500/4000 (CatOS), 包括 2948G/2980G/4912G	是	否	是
Catalyst 4500/4006 (Cisco IOS)	是	是	是
Catalyst 3750	是	是	是
Catalyst 3560/3550	是	是	是
Catalyst 2970	是	是	是
Catalyst 2960	是	否	是
Catalyst 2950/2955	是	否	是
Catalyst 2940	是	否	是
Catalyst 2948G-L3/4908G-L3/4840G	是	是	否
Catalyst 8500	是	是	否

二层接口模式及其相应的特性如表 9-4 所示。

表 9-4　二层接口模式及特性

模式	特性
switchport mode access	将接口置于非 Trunk 模式，并且协商将接口转换至非 Trunk 链路。即使相邻接口不做改变，也将接口改变为非 Trunk 接口
switchport mode dynamic desirable	接口尝试将链路转换为 Trunk 链路。当相邻接口设置为 trunk、desirable 或 auto 时，接口将改变为 Trunk 接口
switchport mode dynamic auto	当相邻接口设置为 Trunk 或 desirable 时，接口将改变链路为 Trunk 链路。该模式是所有以太网接口的默认模式
switchport mode trunk	将接口置于 Trunk 模式，并协商将链路转换为 Trunk 链路。即使相邻接口不做改变，也将接口改变为 Trunk 接口
switchport nonegotiate	将接口置于 Trunk 模式。不过，必须手动配置相邻接口为 Trunk 接口，以建立 Trunk 链路

若欲在相邻交换机之间创建 Trunk，必须将相邻的交换端口置于相应的状态。如表 9-5 所示为相邻端口之间可以创建 Trunk 的匹配状态。

表 9-5　相邻端口之间可以创建 Trunk 的匹配状态

Catalyst 平台之间推荐的 Trunk 模式		相邻 Catalyst 交换机(连接到该交换机)			
		6500/6000, 4500/4000, 5500/5000 (CatOS)	6500/6000, 500/4000, 5500/5000 (Cisco IOS)	3750, 3560, 3550, 2955, 2950,2960	2948G-L3, 4908G-L3, 4840G
本地 Catalyst 交换机	Catalyst 6500/6000, 4500/4000, 5500/5000 (CatOS)	本地: desirable 相邻: desirable	本地: desirable 相邻: dynamic desirable	本地: desirable 相邻: dynamic desirable	本地: nonegotiate 相邻: 查看注释*
	Catalyst 6500/6000, 4500/4000, 5500/5000 (Cisco IOS)	本地: dynamic desirable 相邻: desirable	本地: dynamic desirable 相邻: dynamic desirable	本地: dynamic desirable 相邻: dynamic desirable	本地: nonegotiate 相邻: 查看注释*
	Catalyst 3750, 3560, 3550, 2955, 2950,2960	本地: dynamic desirable 相邻: desirable	本地: dynamic desirable 相邻: dynamic desirable	本地: dynamic desirable 相邻: dynamic desirable	本地: nonegotiate 相邻:查看注释*

* Catalyst 2948G-L3, 4908G-L3, 4840G 是三层交换机，并且没有 Trunk 模式。因此，配置这些交换机时应当采用类似路由连接至交换机的模式，并将路由配置为中继。

2. 二层以太网接口默认配置

二层以太网接口默认配置如表 9-6 所示。

表 9-6 二层以太网接口默认配置

特性	默认值
接口模式	switchport mode dynamic auto
Trunk 封装	switchport trunk encapsulation negotiate
允许 VLAN 范围	VLAN 1–1005
VLAN 修剪合格范围	VLAN 2–1001
默认 VLAN（访问端口）	VLAN 1
本地 VLAN（802.1Q 中继）	VLAN 1
STP	在所有 VLAN 启用
STP 端口优先级	128
STP 端口开销	10 Mbps 端口为 100 10/100 Mbps 端口为 19 100 Mbps 端口为 19 1000 Mbps 端口为 4 10 000 Mbps 端口为 2

3. Trunk 配置策略

在配置 Trunk 时，应当遵循以下策略或限制：

- 在由 Cisco 交换机连接创建的 IEEE 802.1Q 中继中，交换机将为中继所允许的每个 VLAN 都保持一个实例，而非 Cisco 设备可能只支持一个扩展树实例（为所有 VLAN）。将借助 802.1Q 中继连接 Cisco 交换机和非 Cisco 交换机时，Cisco 交换机合并非 Cisco 交换机扩展树实例。
- 确认 Trunk 连接两端的 IEEE 802.1Q 中继的本地 VLAN 是相同的。如果两端的本地 VLAN 不同，可能会导致扩展树环。
- 建议不启用 Trunk 中的本地 VLAN 的扩展树，或者在网络中的每个 VLAN 中禁用扩展树。在禁用扩展树前，一定要确认网络中不存在拓扑环。
- Trunk 端口不能是安全端口。
- Trunk 端口可以被添加至 EterChannel 端口组，但是，所有组中的所有 Trunk 必须拥有相同的配置。当组首次创建，所有端口参数都与每一个添加至组的端口相同。如果修改以下任何一个参数配置，交换机都将向组中的所有端口传播。
  - 允许 VLAN 列表
  - 每个 VLAN 的 STP 端口优先级
  - STP Port Fast 配置
  - Trunk 状态。如果端口组中的一个端口停止作为 Trunk，所有端口都将停止作为 Trunk
- 在 PVST 模式中，建议配置不超过 24 个 Trunk 端口。在 MST 模式中，建议不超过 40 个 Trunk 端口。
- 在 Trunk 端口尝试启用 IEEE 802.1x，将显示错误信息，并且 IEEE 802.1x 不会被启用。同样，尝试将启用了 IEEE 802.1x 的端口改变为 Trunk 端口，端口模式也不会改变。

4. 配置 Trunk 端口

■ 配置命令

第 1 步，进入全局配置模式。

```
Switch# configure terminal
```

第 2 步，在配置完成之前禁用该端口。

```
Switch(config-if)# shutdown
```

第 3 步，指定欲设置为 Trunk 的接口。当然，Trunk 应当在交换机级联端口上配置。

```
Switch(config)# interface interface_id
```

第 4 步，指定 Trunk 采用的封装模式。建议选择使用 dot1q 封装，以获得最大的兼容性。

```
Switch(config-if)# switchport trunk encapsulation {isl | dot1q | negotiate}
```

第 5 步，将接口配置为第二层 Trunk。dynamic auto，是指如果相邻接口被设置为 trunk 或 desirable 模式，将该接口置为 Trunk 连接。dynamic desirable，是指如果相邻接口设置为 trunk、desirable 或 auto 模式，将该接口置为 Trunk 连接。trunk，是指将接口设置为永久 Trunk 模式，即使相邻接口不是 Trunk 接口，也会与之协商将连接转换为 Trunk 连接。建议相邻接口均使用 trunk 关键字，以保证 Trunk 创建成功。

```
Switch(config-if)# switchport mode {dynamic {auto | desirable} | trunk}
```

提示

只有接口是第二层访问接口，或者指定 Trunk 模式时，才需要使用该命令。

第 6 步，（可选）指定默认 VLAN，即当 Trunk 失效后，允许哪一个 VLAN 使用 Trunk 链路继续通信。既可指定某一个 VALN，也可以指定一个 VLAN 范围。访问 VLAN 不能作为本地 VLAN 使用。

```
Switch(config-if)# switchport access vlan vlan_id
```

第 7 步，（可选）为 802.1Q Trunk 指定本地 VLAN。若不指定本地 VLAN，默认将使用 VLAN1。

```
Switch(config-if)# switchport trunk native vlan vlan_id
```

第 8 步，配置 Trunk 上允许的 VLAN 列表。默认状态下，Trunk 端口允许所有 VLAN 的发送和接口传输。当然，根据需要，也可以拒绝某些 VLAN 通过 Trunk 传输，从而限制该 VLAN 与其他交换机的通信，或者拒绝某些 VLAN 对敏感数据的访问。需要注意的是，不能从 Trunk 中移除默认的 VLAN1。使用 add（添加）、all（所有）、except（除外）和 remove（移除）关键字，可以定义允许在 Trunk 上传输的 VLAN。VLAN 列表既可以是一个 VLAN，也可以是一

个 VLAN 组。当同时指定若干 VLAN 时，不要在“,”或“-”间使用空格。

```
Switch(config-if)# switchport trunk allowed vlan {add | all | except | remove}
vlan-list
```

第 9 步，返回至特权配置模式。

```
Switch(config-if)# end
```

第 10 步，查看并校验配置。

```
Switch# show interface interface_id switchport
Switch# show interfaces interface_id trunk
```

第 11 步，保存 VLAN 配置。

```
Switch# copy running-config startup-config
```

若欲将接口恢复至默认值，可以使用 default interface interface_id 接口配置命令。若欲将 Trunk 接口中的所有特征恢复为默认值，可以使用 no switchport trunk 接口配置命令。若欲禁用 Trunk，可以使用 switchport mode access 接口配置命令，端口将作为一个静态访问端口。

若欲允许所有 VLAN 都通过该 Trunk，可以使用 no switchport trunk allowed vlan 接口配置命令。

提示 Trunk 应当在相互连接的两台交换机上分别设置，否则 Trunk 将无法生效。也就是说，当在接入交换机的级联端口上设置了 Trunk 端口后，还应当在汇聚交换机的相应端口上设置 Trunk。同时，在汇聚交换机上必须创建 Trunk 中所包含的全部 VLAN ID。

■ 配置示例

将 Catalyst 4506 的 G3/2 和 G3/5 插槽配置为 Trunk 端口，用于理科楼和图书馆接入交换机中多个 VLAN 借助一条上行链路与核心交换机进行通信。网络拓扑结构如图 9-8 所示。

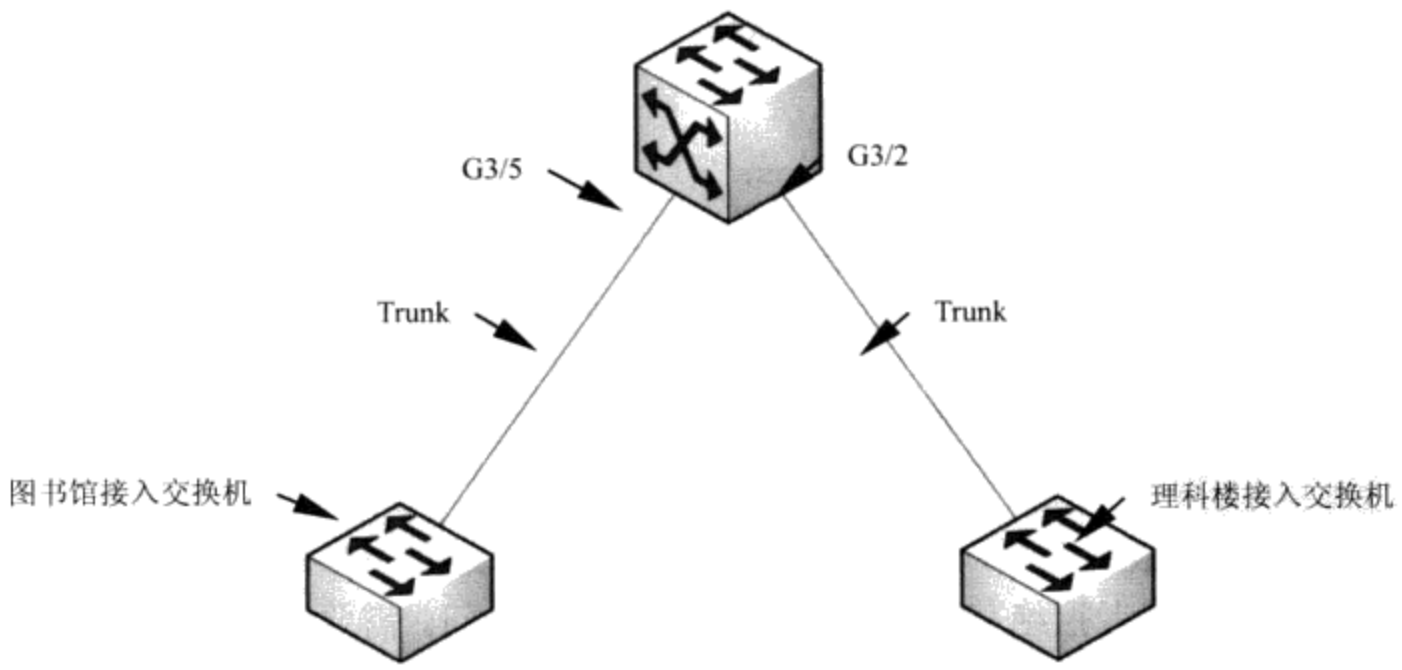


图 9-8 Trunk\拓扑结构

```
Hexin_4506# configure terminal
Hexin_4506 (config)# interface gigabitethernet 3/2
Switch(config-if)# shutdwon
Hexin_4506 (config-if)# switchport trunk encapsulation dot1q
Hexin_4506 (config-if)# switchport mode trunk
Switch(config-if)# no shutdwon
Hexin_4506 (config-if)# exit
Hexin_4506 (config)# interface gigabitethernet 3/5
Switch(config-if)# shutdwon
Hexin_4506 (config-if)# switchport trunk encapsulation dot1q
Hexin_4506 (config-if)# switchport mode trunk
Switch(config-if)# no shutdwon
Hexin_4506 (config-if)# end
Hexin_4506 #
```

9.4 私有 VLAN 安全

与 VLAN 不同，私有 VLAN（Private Virtual Local Area Network，PVLAN）端口之间相互隔离，不能实现相互之间的通信，仅可通过上联端口访问到企业网络。若用户希望端口之间通信，必须借助三层交换机或路由器进行路由转发。PVLAN 技术在解决通信安全、防止广播风暴和浪费 IP 地址方面的优势是显而易见的，而且采用 PVLAN 技术有助于网络的优化。另外，PVLAN 的配置也相对简单，不必占用 VLAN 资源。

9.4.1 PVLAN 概述

私有 VLAN 可以实现端口之间的相互隔离，满足宽带接入用户的安全性要求，避免用户信息和数据的泄露，防止非法攻击和窃取。在使用私有 VLAN 时，各接入端口间不可以相互通信，仅可通过上联端口来访问网络资源。需要注意的是，二层交换机和三层交换机都可以创建 PVLAN。

1. VLAN 的局限性

随着企业网络应用的不断丰富，对网络数据通信的安全性也提出了更高的要求，诸如防范黑客攻击、控制病毒传播等，都要求保证网络用户通信的相对安全。传统的解决方法是给每个客户分配一个 VLAN 和相关的 IP 子网，通过使用 VLAN，每个用户被从第二层隔离开，可以防止任何恶意的行为和网络信息探听。然而，这种分配每个客户单一 VLAN 和 IP 子网的模型造成了巨大的可扩展方面的局限。这些局限主要表现在以下几个方面。

- VLAN 的限制。交换机固有的 VLAN 数目的限制，导致企业网络不能划分太多数量的 VLAN，限制了网络应用。
- 复杂的 STP。对于每个 VLAN，每个相关的 Spanning Tree 的拓扑都需要管理，管理复杂繁琐。
- IP 地址的紧缺。IP 子网的划分势必造成一些 IP 地址的浪费，加之 IP 地址资源紧张，使 IP 地址的分配变得更加困难。

- 路由的限制。每个子网都需要相应的默认网关的配置，管理起来非常麻烦，而且增加了路由的负担，影响网络传输效率。

2. PVLAN 技术

采用 PVLAN 技术，同一 PVLAN 内的计算机彼此相互隔离，虽然它们位于同一 IP 地址段，拥有相同的子网掩码和默认网关，却无法实现彼此之间的通信。它们之间的通信，只能经过默认网关，在第三层交换机中才能实现。PVLAN 的应用对于保证接入网络的数据通信的安全性是非常有效的，用户只需与自己的默认网关连接，一个 PVLAN 不需要多个 VLAN 和 IP 子网就提供了具备第二层数据通信安全性的连接。所有用户都接入 PVLAN，从而实现了所有用户与默认网关的连接，而与 PVLAN 内的其他用户没有任何访问。PVLAN 功能可以保证同一个 VLAN 中的各个端口相互之间不能通信，但可以穿过 Trunk 端口。这样即使同一 VLAN 中的用户，相互之间也不会受到广播的影响。

■ PVLAN 端口

PVLAN 端口有 3 种类型。

- Promiscuous：Promiscuous 端口可以与所有接口通信，包括同一 PVLAN 内的 Isolated 端口和 Community 端口。
- Isolated：同一 PVLAN 内的 Isolated 端口与其他端口在二层相互隔离，但是，仍然可以与 Promiscuous 端口通信。PVLAN 阻塞所有到 Isolated 端口的传输，但来自 Promiscuous 端口的通信除外。来自 Isolated 端口的信号传输将只被转发到 Promiscuous 端口。
- Community：Community 端口可以在彼此之间、以及与 Promiscuous 端口进行通信。这些端口与其他 PVLAN 内的 Community 端口或 Isolated 端口在二层被隔离，相互之间不能进行通信。Trunk 支持 VLAN 在 Isolated、Community 和 Promiscuous 端口间的数据传输，

Isolated 端口属于 Isolated PVLAN，Community 端口属于 Community PVLAN，而代表一个 Private VLAN 整体的是 Primary VLAN，前述两类 PVLAN 必须和它绑定在一起，同时它还包括 Promiscuous 端口。在 Isolated PVLAN 中，Isolated 端口只能和 Promiscuous 端口通信，彼此不能交换流量；在 Community PVLAN 中，Community 端口不仅可以和 Promiscuous 端口通信，而且彼此也可以交换流量。Promiscuous 端口与路由器或第三层交换机接口相连，它收到的流量可以发往 Isolated 端口和 Community 端口。

■ PVLAN 域

PVLAN 可以将正常的 VLAN 域划分为子域。子域表现为 VLAN 对——Primary VLAN 和 Secondary VLAN。PVLAN 可以由多所 VLAN 对组成，一个对即为一个子域。PVLAN 内的所有 VLAN 对共享同一 Primary VLAN。每一个子域的 Secondary VLAN ID 与其他子域都不相同。Primary VLAN 与 Secondary VLAN 的关系如图 9-9 所示。

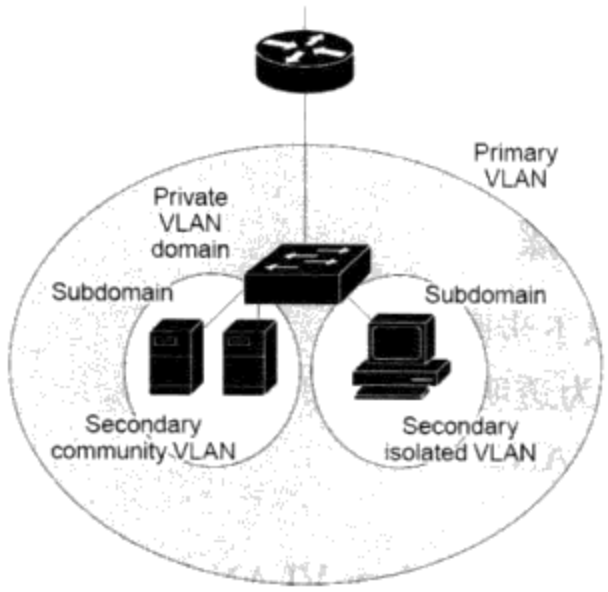


图 9-9　Primary VLAN 与 Secondary VLAN

Primary VLAN 和 Secondary VLAN 具有下述特征。

- Primary VLAN：一个 PVLAN 只能有一个 Primary VLAN。所有端口只能实现单向的向下传输，即从 Promiscuous 端口到（Isolated 和 Community）主机端口和其他 Promiscuous 端口。
- Isolated VLAN：一个 PVLAN 只能有一个 Isolated VLAN。Isolated VLAN 属于 Secondary VLAN，所有端口只能实现单向的向上传输，即从主机端口到 Promiscuous 端口和网关。
- Community VLAN：Community VLAN 属于 Secondary VLAN，所有端口只能实现单向的向上传输，即从 Community 端口到 Promiscuous 端口和网关，以及同一 Community VLAN 内的其他主机端口。

Secondary VLAN 有两种类型。

- Isolated VLAN：同一 Isolated VLAN 内的端口在二层相互隔离，必须借助于三层交换机才能实现相互通信。
- Community VLAN：同一 Community VLAN 内的端口可以与其他端口通信，但是与其他 Community VLAN 端口在二层相互隔离。

多交换机之间 PVLAN 的连接，也是借助 Trunk 实现。Trunk 不仅可以实现多 VLAN 的传输，而且还可以实现多 PVLAN 的传输，如图 9-10 所示。

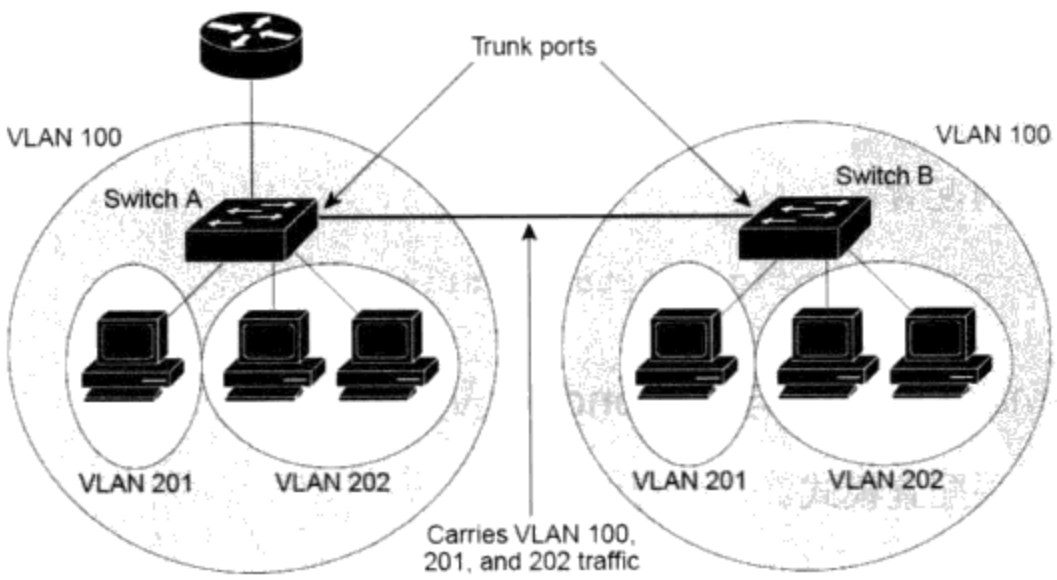


图 9-10　Trunk 实现 PVLAN 传输

9.4.2 配置 PVLAN

1. 配置 PVLAN 一般步骤

配置 PVLAN 时，需经过以下步骤。

第 1 步，将 VTP 模式设置为透明模式，即禁用 VTP。

第 2 步，创建 Secondary VLAN。

第 3 步，创建 Primary VLAN。

第 4 步，为 Primary VLAN 与 Secondary VLAN 建立关联。一个 Isolated VLAN 可以与一个 Primary VLAN 关联，多个 Community VLAN 可以与 Primary VLAN 关联。

第 5 步，将接口配置为 Isolated 或 Community 端口。

第 6 步，将 Isolated 端口或 Community 端口关联为 primary-secondary VLAN 对。

第 7 步，将接口配置为 Promiscuous 端口。

第 8 步，将 Promiscuous 端口映射为 primary-secondary VLAN 对。

2. 将 VLAN 配置为 PVLAN

第 1 步，进入全局配置模式。

```
Switch# configure terminal
```

第 2 步，指定欲设置为 PVLAN 的 VLAN。

```
Switch(config)# vlan vlan-ID
```

第 3 步，将指定 VLAN 设置为 PVLAN，并指定 PVLAN 类型。在退出 VLAN 配置模式时，该配置命令不会生效。

```
Switch(config-vlan)# private-vlan {isolated | primary}
```

第 4 步，返回特权配置模式。

```
Switch(config)# end
```

第 5 步，校验当前设置。

```
Switch# show vlan private-vlan [type]
```

第 6 步，保存当前配置。

```
Switch# copy running-config startup-config
```

3. 关联 Primary VLAN 与 Secondary VLAN

第 1 步，进入全局配置模式。

```
Switch# configure terminal
```

第 2 步，指定 Primary VLAN，进入 VLAN 配置模式。

```
Switch(config)# vlan primary-vlan-ID
```

第 3 步，建立 Secondary VLAN 与 Primary VLAN 的关联。该列表只能包括一个 VLAN。

```
Switch(config-vlan)# private-vlan association {secondary-vlan-list | add
secondary-vlan-list | remove secondary-vlan-list}
```

第 4 步，返回特权配置模式。

```
Switch(config)# end
```

第 5 步，校验当前设置。

```
Switch# show vlan private-vlan [type]
```

第 6 步，保存当前配置。

```
Switch# copy running-config startup-config
```

当关联 Secondary VLAN 和 Primary VLAN 时，注意以下几点。

- secondary-vlan-list 参数只能包含一个 Isolated VLAN ID。
- 使用 remove 关键字可以清除 Secondary VLAN 与 Primary VLAN 的关联。该列表包括一个 VLAN。
- 只有退出 VLAN 配置模式时，键入的命令才会生效。

4. 配置 PVLAN Promiscuous 端口

第 1 步，进入全局配置模式。

```
Switch# configure terminal
```

第 2 步，指定欲配置的二层端口。

```
Switch(config)# interface interface-id
```

第 3 步，将二层接口配置为 PVLAN Promiscuous 端口。

```
Switch(config-if)# switchport mode private-vlan {host | promiscuous | trunk}
```

第 4 步，将 PVLAN Promiscuous 端口设为 Primary VLAN，并选择 Secondary VLAN。

```
Switch(config-if)# switchport private-vlan mapping primary-vlan-id
{secondary-vlan-list | add secondary-vlan-list | remove secondary-vlan-list}
```

第 5 步，返回特权配置模式。

```
Switch(config)# end
```

第 6 步，校验当前设置。

```
Switch# show interfaces infterface-id switchport
```

第 7 步，保存当前配置。

```
Switch# copy running-config startup-config
```

在将二层接口配置为 PVLAN Promiscuous 端口时，注意以下几点。

- secondary-vlan-list 参数不能有空格，也不能包括由多个“,”分隔开的条目。每个条目只能包括一个 PVLAN ID 或一个带有“-”的 PVLAN ID 范围。
- 键入 secondary-vlan-list 或使用 add 关键字，将 Secondary VLAN 映射到 PVLAN Promiscuous 端口。
- 使用 remove 关键字可以清楚 Secondary VLAN 和 PVLAN Promiscuous 端口的关联。

5. 配置 PVLAN Host 端口

第 1 步，进入全局配置模式。

```
Switch# configure terminal
```

第 2 步，指定欲配置的二层端口。

```
Switch(config)# interface interface-id
```

第 3 步，将二层接口配置为 PVLAN Host 端口。

```
Switch(config-if)# switchport mode private-vlan {host | promiscuous} | trunk
```

第 4 步，将二层接口关联至 PVLAN。

```
Switch(config-if)# switchport private-vlan host-association primary-vlan-id
secondary-vlan-id
```

第 5 步，返回特权配置模式。

```
Switch(config)# end
```

第 6 步，校验当前设置。

```
Switch# show interfaces infterface-id switchport
```

第 7 步，保存当前配置。

```
Switch# copy running-config startup-config
```

6. 配置 PVLAN Trunk 端口

第 1 步，进入全局配置模式。

```
Switch# configure terminal
```

第 2 步，指定欲配置的二层端口。

```
Switch(config)# interface interface-id
```

第 3 步，将二层接口配置为 PVLAN Trunk 端口，实现多 Secondary PVLAN 在一条链路上的传输。

```
Switch(config-if)# switchport mode private-vlan {host | promiscuous | trunk}
```

第4步，建立Primary VLAN与Secondary VLAN的关联，将PVLAN端口作为一个PVLAN。使用该命令，可以指定多个PVLAN对，从而使PVLAN Trunk端口实现多个Secondary VLAN的传输。如果关联被指定至一个已有的Primary VLAN，现有关联将被替换。如果没有创建Trunk关联，Secondary VLAN上接收的任何包都将被丢弃。

```
Switch(config-if)# switchport private-vlan association trunk primary-vlan-id
secondary-vlan-id
```

第5步，在PVLAN Trunk端口配置普通VLAN的允许列表。

```
Switch(config-if)# switchport private-vlan trunk allowed vlan vlan-list all
| none | [add | remove | except] vlan-atom[,vlan-atom...]
```

第6步，将VLAN配置为非标签包。如果没有本地VLAN，所有非标签包将被丢弃。如果本地VLAN是Secondary VLAN，并且端口没有与Secondary VLAN关联，非标签包也将被丢弃。

```
Switch(config-if)# switchport private-vlan trunk native vlan vlan-id
```

第7步，返回特权配置模式。

```
Switch(config)# end
```

第8步，校验当前设置。

```
Switch# show interfaces infterface-id
```

第9步，保存当前配置。

```
Switch# copy running-config startup-config
```

7. 将Secondary VLAN映射为Primary VLAN三层VLAN接口

若欲借助三层交换机实现PVLAN间的路由，必须为Primary VLAN配置SVI（Switch Virtual Interface，交换机虚拟接口），并将Secondary VLAN映射至SVI。

第1步，进入全局配置模式。

```
Switch# configure terminal
```

第2步，指定欲配置的Primary VLAN，进入接口配置模式。

```
Switch(config)# interface vlan primary-vlan-id
```

第3步，将Secondary VLAN映射至三层VLAN接口，从而允许PVLAN在三层交换机上实现数据传输。

```
Switch(config-if)# private-vlan mapping primary-vlan-id {secondary-vlan-list
| add secondary-vlan-list | remove secondary-vlan-list}
```

第4步，返回特权配置模式。

```
Switch(config)# end
```

第5步，校验当前设置。

```
Switch# show interface private-vlan mapping
```

第6步，保存当前配置。

```
Switch# copy running-config startup-config
```

9.5 访问列表安全

访问控制列表（ACL，Access Control List）是Cisco IOS提供的一种访问控制技术，被广泛应用于路由器和三层交换机。借助ACL，可以有效地控制用户对网络和Internet的访问，从而最大限度地保障网络安全，并使得企业网络不被滥用。

9.5.1 访问列表概述

ACL 使用包过滤技术，在路由器上读取第三层及第四层包头中的信息。如源地址、目的地址、源端口、目的端口等，根据预先定义好的规则对包进行过滤，从而达到访问控制的目的。不过，由于ACL是通过使用包过滤技术来实现的，过滤的依据又仅仅只是第三层和第四层包头中的部分信息，这种技术具有一些固有的局限性。如无法识别到具体的人，无法识别到应用内部的权限类别等。因此，要达到“端到端”的权限控制目的，需要和系统级及应用级的访问权限控制结合使用。

1. 交换机支持的访问列表

交换机支持IP访问列表和Ethernet（MAC）访问列表。

- IP访问列表。过滤IP通信，包括TCP、User Datagram Protocol (UDP)、Internet Group Management Protocol (IGMP)和Internet Control Message Protocol (ICMP)。
- Ethernet访问列表。过滤非IP通信。

交换机支持三种访问列表的应用过滤传输：

- 端口访问列表。也称MAC访问列表。对进入二层接口的通信实施访问控制。交换机不支持外出访问的访问列表。在二层接口可以应用IP访问列表和端口访问列表。
- 路由访问列表。对VLAN之间以及三层接口之间的通信实施访问控制，并且可以控制进、出双向通信。
- VLAN访问列表。也称VLAN映射，对所有包实现访问控制。在同一VLAN的设备之间，可以采用VLAN ACL实施访问控制。VLAN访问列表的配置与访问控制均基于IP地址，不支持基于MAC地址的访问控制。

可以在同一交换机上实施端口访问列表、路由访问列表和VLAN访问列表。不过，端口访问列表优先于路由访问列表和VLAN访问列表。

2. 访问列表的类型

Cisco 支持 3 种类型的访问列表，即标准 IP 访问列表、扩展 IP 访问列表和命名访问控制列表。

■ 标准 IP 访问控制列表

标准 IP 访问列表只允许过滤源地址，且功能十分有限。当我们要想阻止来自某一网络的所有通信流量，或者允许来自某一特定网络的所有通信流量，或者想要拒绝某一协议簇的所有通信流量时，可以使用标准访问控制列表来实现这一目标。标准访问控制列表检查路由的数据包的源地址，从而允许或拒绝基于网络、子网或主机的 IP 地址的所有通信流量通过路由器的出口。

■ 扩展 IP 访问列表

扩展 IP 访问列表允许过滤源地址、目的地址和上层应用数据。因此，可以适应各种复杂的网络应用。扩展 IP 访问列表既检查数据包的源地址，也检查数据包的目的地址，还检查数据包的特定协议类型、端口号等。扩展 IP 访问列表更具有灵活性和可扩充性，即可以对同一地址允许使用某些协议通信流量通过，而拒绝使用其他协议的流量通过。

■ 命名访问控制列表

在标准与扩展 IP 访问列表中均要使用表号，而在命名访问控制列表中使用一个字母或数字组合的字符串来代替前面所使用的数字。使用命名访问控制列表可以用来删除某一条特定的控制条目，这样可以在使用过程中方便地进行修改。

3. 配置访问列表应当注意的问题

在设置访问列表时，应当遵循最小特权原则，即只给受控对象完成任务所必需的最小的权限，从而最大限度地保障网络传输安全。所谓最小特权（Least Privilege），是指在完成某种操作时所赋予网络中每个主体（用户或进程）必不可少的特权。最小特权原则，则是指应限定网络中每个主体所必需的最小特权，确保可能因事故、错误、网络部件的篡改等原因造成的损失最小。最小特权原则一方面给予主体必不可少的特权，保证所有的主体都能在所赋予的权限内完成自己的任务或操作；另一方面，只给予主体必不可少的特权，从而限制每个主体所能进行的操作，以确保企业网络安全。

■ 自上而下的处理过程

访问列表包含一个访问控制条目（ACE，Access Control entry）规则列表。每个 ACE 都指定“permit”（允许）或“deny”（拒绝），以及应用条件。包会逐个条目顺序匹配 ACE。访问列表表项的检测按自上而下的顺序进行，并且从第一个表项开始。这意味着必须特别谨慎地考虑访问列表中语句的顺序。

■ 添加表项

新增加的表项被追加到访问列表末尾，这就意味着不能改变已有的访问列表的功能。如果要改变，就必须创建一个新的访问列表，并删除已经存在的访问列表，并且将新的访问列表应用于接口上。

■ **标准 IP 访问列表过滤**

标准 IP 访问列表只限于过滤源地址，所以，需要使用扩展的 IP 访问列表来满足企业的特殊需求。

■ **访问列表位置**

应当将扩展 IP 访问列表尽量放在靠近过滤源的位置，这样创建的过滤器就不会反过来影响其他接口上的数据流。而标准访问 IP 列表则应当尽量靠近目的地位置。由于标准 IP 访问列表只使用源地址，因此将阻止报文流向其他端口。

■ **语句的位置**

由于 IP 协议包含 ICMP、TCP 和 UDP，所以应当将具体的表项放在不太具体的表项前面，以保证位于另一个语句前面的语句不会否定表中后面语句的作用效果。

■ **访问列表应用**

使用 Access-group 命令应用访问列表。需要注意的是，只有访问列表被应用于接口上时，才执行过滤操作，从而真正产生作用。

■ **过滤方向**

通过接口的数据流是双向的。过滤方向定义了欲检查的是流入还是流出的报文。所以，访问列表要应用到接口的特定方向上。向外的（outbound）表示数据流从三层设备流出；向内的（inbound）表示数据流流向三层设备。

4. 访问列表配置步骤

- 分析需求，找清楚需求中要保护什么或控制什么；为方便配置，最好能以表格形式列出。
- 分析符合条件的数据流的路径，寻找一个最适合进行控制的位置。
- 编写 ACL，并将 ACL 应用到接口上。
- 测试并修改 ACL。

9.5.2 IP 访问列表

1. 创建标准 IP 访问列表

第 1 步，进入全局配置模式

```
Switch# configure terminal
```

第 2 步，使用源地址或通配符定义标准 IP 访问列表。

```
Switch(config)# access-list access-list-number {deny | permit} source
[source-wildcard]
```

access-list-number ACL 号。相同的所有 ACL 形成一个组。在判断一个包时，使用同一组中的条目从上到下逐一进行判断，一遇到满足的条目就终止对该包的判断。1~99 或 1300~1999

为标准的 IP ACL 号。

deny | permit 当条件匹配时，确定是允许包通过，还是将包丢弃。

Source 源地址。发送包的网络或主机地址，使用点分十分进制数表示。当表示一组主机时，使用通配符屏蔽码。

source-wildcard 通配符屏蔽码。Cisco 访问列表所支持的通配符屏蔽码与子网掩码的方式是相反的。也就是说，二进制数“0”表示一个匹配条件，“1”表示一个不关心条件。

Any 表示任何主机。源地址和源通配符 0.0.0.0 255.255.255.255 的缩写。例如，若欲拒绝从源地址 192168.1.100 发出的报文，但又允许发自其他源地址的报文，应当使用下述语句：

```
Access-list 1 deny host 192.168.1.100
Access-list 1 permit any
```

需要注意这两条语句的顺序。访问列表语句的处理是由上至下的。如果将两个语句顺序颠倒，将 Permit 语句放在 Deny 语句前面，则不能过滤来自主机的报文，因为 Permit 语句允许所有报文通过。访问列表中的语句顺序非常重要，不合理的语句顺序将会在网络中产生安全漏洞，或者使用户不能很好地利用公司的网络策略。

Host 表示一台主机，是源和源通配符 0.0.0.0 的缩写。例如，若欲允许从 192.168.1.200 发出的报文，则应当使用下述语句：

```
Access-list 1 permit 192.168.1.200 0.0.0.0
```

上述语句也可以使用下面的语句代替：

```
Access-list 1 permit host 192.168.1.200
```

第 3 步，返回特权配置模式。

```
Switch(config)# end
```

第 4 步，校验当前设置。

```
Switch# show access-lists number
```

第 5 步，保存当前配置。

```
Switch# copy running-config startup-config
```

使用“no access-list access-list-number”全局配置命令，可以删除全部访问列表。需要注意的是，不能从指定的访问列表中删除某个 ACE。

2. 创建 IP 扩展访问列表

标准 IP 访问列表只能控制源 IP 地址，不能控制到端口。若欲控制企业用户的网络应用，就需要使用扩展 IP 访问列表。

第 1 步，进入全局配置模式

```
Switch# configure terminal
```

第 2 步，定义扩展 IP 访问列表，取值范围为 100 ~ 199 或 2000 ~ 2699。

```
Switch(config)# access-list access-list-number {deny | permit} protocol source
source-wildcard [operator port] destination destination-wildcard [operator port]
```

或者

```
access-list access-list-number {deny | permit} protocol any [operator port]
any [operator port]
```

或者

```
access-list access-list-number {deny | permit} protocol host source [operator
port] host destination [operator port]
```

protocol 欲过滤的协议，如 IP、TCP、UDP、ICMP 等。默认过滤所有协议，若欲根据特殊协议进行报文过滤，需指定协议。

destination destination-wildcard 目的地址和通配符屏蔽码。

operator 端口操作符，在协议类型为 TCP 或 UDP 时支持端口比较。支持的比较操作有：等于（eq）、大于（gt）、小于（lt）、不等于（neq）或介于（range）。如果操作符为 range，则后面需要跟两个端口。

Port 端口号，可以用几种不同方法指定。可以显式地指定，数字或使用一个可识别的助记符。例如，可以使用 80 或 http 指定超文本传输协议，使用 21 或 ftp 指定文件传输协议。例如，若欲允许来自任何地址的包含有 SMTP 数据的报文到达 192.168.10.10 主机，可以在访问列表中添加下述语句：

```
Access-list 101 permit tcp any host 192.168.10.10 eq smtp
```

第 3 步，返回特权配置模式。

```
Switch(config)# end
```

第 4 步，校验当前设置。

```
Switch# show access-lists number
```

第 5 步，保存当前配置。

```
Switch# copy running-config startup-config
```

3. 创建 IP 访问列表名称

命名 IP 访问列表有两个主要优点：一是可以解决 ACL 号码不足的问题；二是可以自由地删除 ACL 中的一条语句，而不必删除整个 ACL。而主要不足之处在于无法实现在任意位置加入新的 ACL 条目。

■ 创建标准 IP 访问列表名称

第 1 步，进入全局配置模式。

```
Switch# configure terminal
```

第 2 步，利用名称定义标准 IP 访问列表，进入访问列表配置模式。名称可以是 1~99。

```
Switch(config)# ip access-list standard name
```

第 3 步，定义一个或多个 permit 或 deny 条件，以确定对包实施转发或是丢弃。

```
Switch(config-std-nacl)# deny {source [source-wildcard] | host source | any}
```

或者

```
Switch(config-std-nacl)# permit {source [source-wildcard] | host source | any}
```

第 4 步，返回特权配置模式。

```
Switch(config-std-nacl)# end
```

第 5 步，校验当前设置。

```
Switch# show access-lists name
```

第 6 步，保存当前配置。

```
Switch# copy running-config startup-config
```

■ **创建扩展 IP 访问列表名称**

第 1 步，进入全局配置模式。

```
Switch# configure terminal
```

第 2 步，利用名称定义扩展 IP 访问列表，进入访问列表配置模式。名称可以是 100~199。

```
Switch(config)# ip access-list extended name
```

第 3 步，定义一个或多个 permit 或 deny 条件，以确定对包实施转发或是丢弃。

```
Switch(config-ext-nacl)# {deny | permit} protocol {source [source-wildcard]
| host source | any} {destination [destination-wildcard] | host destination | any}
```

第 4 步，返回特权配置模式。

```
Switch(config-std-nacl)# end
```

第 5 步，校验当前设置。

```
Switch# show access-lists name
```

第 6 步，保存当前配置。

```
Switch# copy running-config startup-config
```

例如，借助扩展 IP 访问列表，可以在 VLAN 或端口上阻止蠕虫端口，从而避免蠕虫在网络中的蔓延，保证网络的传输效率。

```
access-list 110 deny   tcp any any eq 135
access-list 110 deny   tcp any any eq 445
access-list 110 deny   tcp any any eq 593
access-list 110 deny   tcp any any eq 1029
```

```
access-list 110 deny   tcp any any eq 4444
access-list 110 deny   tcp any any eq 5000
access-list 110 deny   tcp any any eq 5554
access-list 110 deny   tcp any any eq 7955
access-list 110 deny   tcp any any range 9995 9996
access-list 110 deny   udp any any range netbios-ns netbios-dgm
access-list 110 deny   udp any any eq tftp
access-list 110 deny   udp any any range 995 999
access-list 110 deny   udp any any eq 1434
access-list 110 deny   udp any any eq 8998
access-list 110 permit ip any any
```

然后，再将该访问列表应用至端口或 VLAN，在入和出双向上启用该列表。

```
ip access-group 110 in
ip access-group 110 out
```

4. 基于时间的访问列表

借助基于时间的访问列表，可以控制用户在某个时间段的访问权限。

第 1 步，进入全局配置模式。

```
Switch# configure terminal
```

第 2 步，为指定的时间范围命名一个有意义的名称。名称不能包括空格和引号，并且必须以字母开头。

```
Switch(config)# time-range time-range-name
```

第 3 步，指定时间范围。

```
Switch(config-time-range)# absolute [start time date] [end time date]
```

或者

```
periodic day-of-the-week hh:mm to [day-of-the-week] hh:mm
```

或者

```
periodic {weekdays | weekend | daily} hh:mm to hh:mm
```

absolute 指定绝对时间范围。该关键字之后紧跟着 start 和 end 关键字。若欲访问列表中相关的 permit 或 deny 语句生效，则 start 和 end 之后应当紧跟开始和结束的时间。需要注意的是，时间以 24 小时格式表示，日期以“日/月/年”格式表示。

periodic 尽管每个时间范围只能有一个 absolute 语句，但却可以有多个 periodic 语句。另外，absolute 语句只拥有开始和结束时间，以及日期等少数几个参数，而 periodic 语句可以使用大量参数，范围可以是一星期中的某一天或几天的组合，或者使用关键字 daily、weekdays 和 weekend 等。表 9-7 列出了在语句中可以使用的周日期天数的参数。

表 9-7　periodic 语句中可以使用的周日期天数的参数

参　数	意　义
Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday	某一天或某几天的组合
daily	从星期一至星期天
weekdays	从星期一至星期五
weekend	星期六和星期日

第 4 步，返回特权配置模式。

```
Switch(config-time-range)# end
```

第 5 步，校验当前设置。

```
Switch# show time-range
```

第 6 步，保存当前配置。

```
Switch# copy running-config startup-config
```

例如，若欲限制所有员工在周一至周五的 8:00~18:00 使用 QQ 和 MSN 聊天，可以在访问列表中添加下述语句：

```
time-range deny-qq
!---定义时间范围名称为“deny-qq”
periodic weekdays start 8:00 end 18:00
!---时间范围为周一至周五的 8:00~18:00
ip access-list extend internet_limit
!---定义扩展 IP 访问列表，名称为“qq_limit”
deny tcp 10.1.0.0 0.0.255.255 any eq 1863 time-range deny-qq
deny tcp 10.1.0.0 0.0.255.255 any eq 8000 time-range deny-qq
deny tcp 10.1.0.0 0.0.255.255 any eq 1080 time-range deny-qq
deny udp 10.1.0.0 0.0.255.255 any eq 8000 time-range deny-qq
deny udp 10.1.0.0 0.0.255.255 any eq 4000 time-range deny-qq
deny udp 10.1.0.0 0.0.255.255 any eq 1080 time-range deny-qq
!---定义 QQ 和 MSN 聊天使用的协议和端口号
permit ip any any
!---其余访问不予限制
```

需要注意的是，网络应用程序所使用的端口号，大多都可以在下述下文件中找到：

```
Win9x:%windir%\services
WinNT/2000/XP：%windir%\system32\drivers\etc\services
Linux：/etc/services
```

如果在 services 文件中找不到端口的应用，可以在运行程序前后，运行 netstat －ap 比较并找出应用所使用的端口号。

5. 将 IP 访问列表应用到接口

如果不将 IP 访问列表应用到接口，那么该访问列表将不会发生作用。

第 1 步，进入全局配置模式。

```
Switch# configure terminal
```

第2步，指定欲应用该IP访问列表的接口。该接口既可以是二层接口（端口访问列表），也可以是三层接口（路由访问列表）。

```
Switch(config)#interface interface-id
```

第3步，将访问控制应用到指定的接口。二层接口（端口访问列表）不支持out关键字。

```
Switch(config-if)# ip access-group {access-list-number | name} {in | out}
```

第4步，返回特权配置模式。

```
Switch(config-if)# end
```

第5步，校验当前设置。

```
Switch# show running-config
```

第6步，保存当前配置。

```
Switch# copy running-config startup-config
```

9.5.3 端口访问列表

在VLAN或二层接口上，可以使用MAC地址和MAC扩展ACL名称过滤非IP地址通信，从而保障企业网络访问安全，拒绝非授权用户对敏感部门的访问。配置过程与其他扩展名称ACL相似。

1. 创建端口扩展访问列表名称

第1步，进入全局配置模式。

```
Switch# configure terminal
```

第2步，为扩展MAC地址列表定义一个名称，进入扩展MAC地址列表配置模式。

```
Switch(config)# mac access-list extended name
```

第3步，定义允许或拒绝的源MAC地址或目的MAC地址。使用Host，可以指定特定主机的MAC地址；使用掩码，可以指定多个主机MAC地址。

```
Switch (config-ext-macl# {deny | permit} {any | host source MAC address | source MAC address mask} {any | host destination MAC address | destination MAC address mask}
```

第4步，返回特权配置模式。

```
Switch(config-ext-mac)# end
```

第5步，校验当前设置。

```
Switch# show access-lists name
```

第 6 步，保存当前配置。

```
Switch# copy running-config startup-config
```

2. 将端口访问列表应用到二层接口

第 1 步，进入全局配置模式。

```
Switch# configure terminal
```

第 2 步，指定欲应用该 IP 访问列表的二层接口。

```
Switch(config)#interface interface-id
```

第 3 步，将 MAC 访问列表应用到二层接口。注意，该命令不适用于 EtherChannle。

```
Switch(config-if)# mac access-group {name} {in}
```

第 4 步，返回特权配置模式。

```
Switch(config-if)# end
```

第 5 步，校验当前设置。

```
Switch# show mac access-group [interface interface-id]
```

第 6 步，保存当前配置。

```
Switch# copy running-config startup-config
```

9.5.4 创建并应用 VLAN 访问列表

1. 创建 VLAN 访问列表

第 1 步，进入全局配置模式。

```
Switch# configure terminal
```

第 2 步，创建 VLAN 映射，并给该 VLAN 访问列表定义一个名称和序号，进入 VLAN 访问列表配置模式。

```
Switch(config)# vlan access-map name [number]
```

第 3 步，为 VLAN 映射设置动作，默认为转发（forward）。

```
Switch (config-access-map)# action {drop | forward}
```

第 4 步，借助一个或多个标准，或扩展访问列表匹配包（使用 IP 或 MAC 地址）。IP 包只能被标准或扩展 IP 访问列表匹配；非 IP 包只能被 MAC 扩展访问列表匹配。

```
Switch (config-access-map)# match {ip | mac} address {name | number} [name | number]
```

第5步，返回特权配置模式。

```
Switch(config-if)# end
```

第6步，校验当前设置。

```
Switch# show running-config
```

第7步，保存当前配置。

```
Switch# copy running-config startup-config
```

2. 将VLAN访问列表应用到VLAN

第1步，进入全局配置模式。

```
Switch# configure terminal
```

第2步，将VLAN映射应用至一个或多个VLAN。可以使用“-”或“,”指定若干VLAN。需要注意的是，“-”或“,”前后必须键入空格。

```
Switch(config)# vlan filter mapname vlan-list list
```

第3步，校验当前设置。

```
Switch# show running-config
```

第4步，保存当前配置。

```
Switch# copy running-config startup-config
```

第 10 章　网络设备系统安全

可网管的网络设备本身就是一台功能简化的计算机，有自己的硬件系统和软件系统。网络设备的操作系统主要为用户日常管理和维护提供相应的操作平台和接口。以 Cisco 网络设备为例，其操作系统通常为 IOS，允许用户通过命令行、图形窗口、远程等多种方式实现对设备的配置与管理。从安全的角度考虑，IOS 自身也会存在一些漏洞，这些底层的安全隐患很可能对网络设备及网络系统造成致命的打击。

10.1　网络设备登录安全

登录网络设备是实施设备配置与管理的第一道关卡，管理员通常都会配置用户名密码或加密传输等安全防御措施。以 Cisco 的可网管设备为例，可以通过配置登录密码、配置命令安全级别、用户访问权限、HTTPS 传输、SNMP 字符串等，来预防非法登录和管理设备等情况的发生。

10.1.1　登录密码安全

Cisco 的 Enable 密码与 Windows 的 Administrator 密码的作用和重要性完全相同。任何人只要知道了 Enable 密码，就可以对交换机进行任意配置和管理，其重要性不言而喻。

1.　配置 Enable 密码

Cisco 的 Enable 密码有两种类型，即“secret password”和“password”，其中，前者被加密存储，安全性较强，后者则未被加密，安全性较差。因此，从安全的角度考虑，应当使用更加安全的“secret password”。

> **提示**　“secret password”较“password”的级别高，当设置了 secret password 后，将不能再使用 password。两种口令对大小写都敏感。也就是说，它们认为大写字母“A”与小写字母“a”是两种不同的符号，所以，必须牢记该密码。

默认状态下，Cisco 设备的 Enable 密码为空，所以，在对交换机进行初始配置时，必须为其设置 Enable 密码。

Enable 密码配置过程如下。

第 1 步，进入全局配置模式。

```
Cisco# configure terminal
```

第 2 步，为特权模式指定新的 Enable 密码。Enable 密码可包括 1~25 个大写或小写字母，也可以包括数字。密码长度应当大于 6 个字符，并且应当是包含大小写字母和数字的无意义的

字符串。访问级别（level）可取值范围为 0 ~ 15， 级别 1（Level 1）是 normal user EXEC 模式，拥有最低权限。级别 15 是 privileged EXEC 模式，拥有最高权限。默认级别是 15。

```
Cisco(config)# enable secret [level level] password
```

或

```
Cisco(config)# enable password [level level] password
```

提示 密码的第 1 个字符不能是数字。当有多个网络管理员时，可以为不同的级别分别设置不同的访问密码，这样，既可以让他们查看网络配置，诊断网络故障；同时，又可以保障网络设备的配置安全。

第 3 步，设置新的密码。

```
Cisco(config)# service password-encryption
```

第 4 步，返回特权模式。

```
Cisco(config)# end
```

第 5 步，保存修改后的配置。

```
Cisco# copy running-config startup-config
```

2. 配置 Telnet 密码

远程管理是网络设备的重要管理方式，因为在日常管理中不可能每次对设备进行配置和管理时，都需要与设备“面对面”，即需要配置 Telnet 管理方式从远程管理设备。当为网络设备设置了管理 IP 地址后，就可以借助“超级终端”或“Telnet”以 IP 地址远程访问和管理该设备了。默认情况下，没有为 Telnet 设置密码。因此，为了网络设备的安全管理，必须设置 Telnet 密码，如图 10-1 所示。

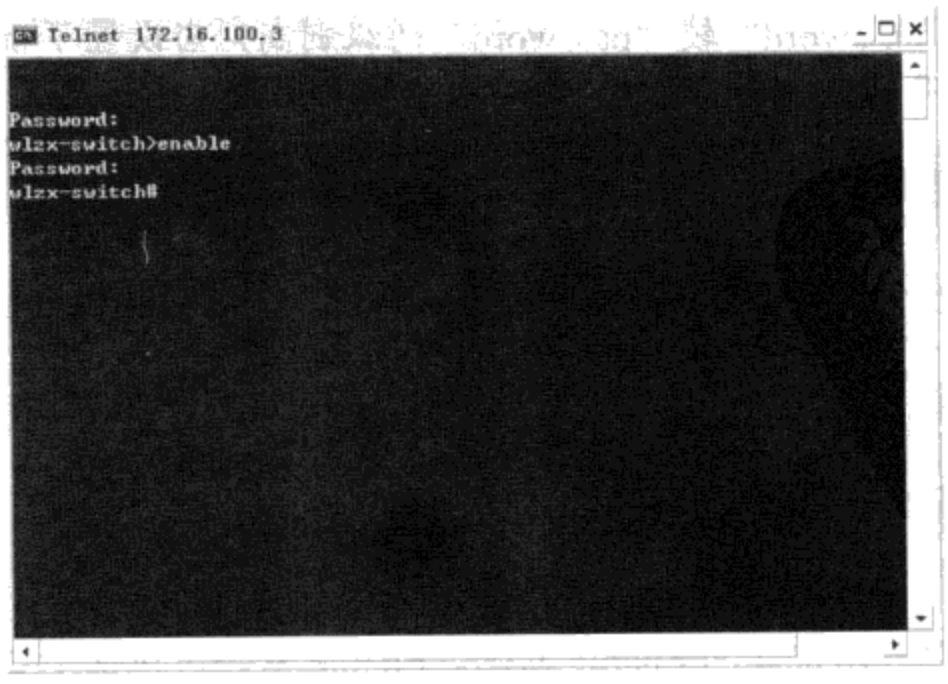


图 10-1 Telnet 密码

Telnet 密码的配置过程如下。

第 1 步，进入全局配置模式。

```
Cisco# configure terminal
```

第 2 步，输入 Telnet 进程号，进入 Line 配置模式。在一台交换机和路由器上，最多可以实现 16 个 Telnet 进程，方便多个用户同时查看和管理。“0 15”表明配置所有的可能的 16 个进程。

```
Cisco(config)# line vty 0 15
```

第 3 步，指定 Telnet 密码。Telnet 密码设置要求与 Enable 相同。

```
Cisco(config)# password password
```

第 4 步，返回特权模式。

```
Cisco(config)# end
```

第 5 步，保存修改后的配置。

```
Cisco# copy running-config startup-config
```

3. 配置管理用户

除了可以为 Admin 超级用户设置密码外，还可以自己创建若干管理用户（如图 10-2 所示），并为这些用户分别指定不同的级别，从而实现对网络设备的分级管理。

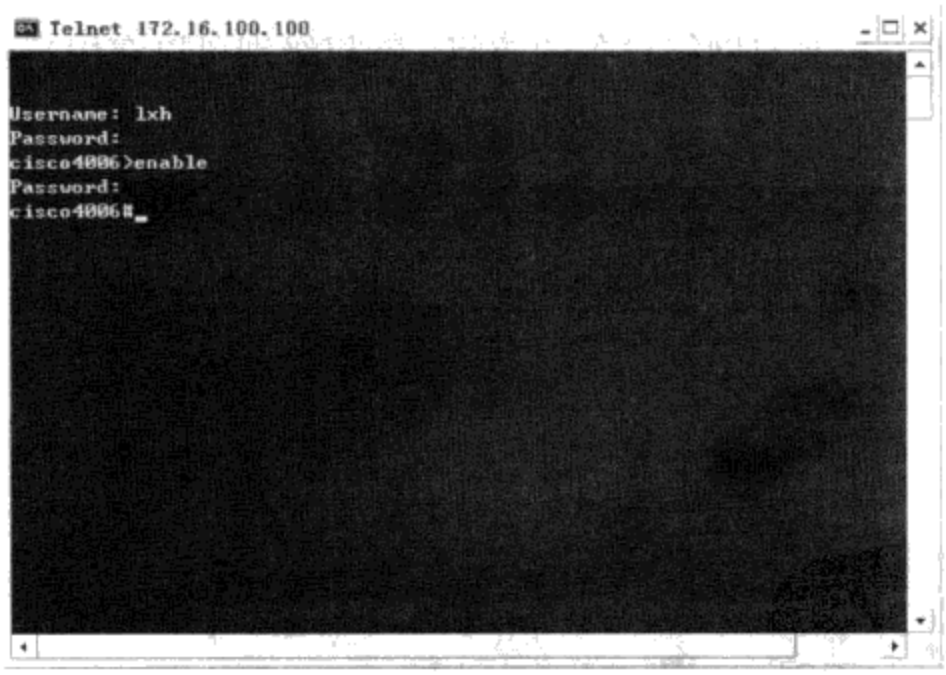


图 10-2　用户登录

管理用户配置过程如下。

第 1 步，进入全局配置模式。

```
Cisco# configure terminal
```

第 2 步，设置管理用户，并为其指定级别。用户名中间不能有空格和引号。级别（Level）的可取值范围为 0 ~ 15，15 拥有特权模式访问权限，而 0 只拥有普通用户权限。用户密码

（Password）设置要求与 Enable 密码相同。

```
Cisco(config)# username name [privilege level] {password password}
```

第 3 步，进入 Line 配置模式，配置 Console（Line 0）或 VTY Line（Line 0 ~ 15）。

```
Cisco(config)# line console 0
```

或

```
Cisco(config)# line vty 0 15
```

第 4 步，用户登录到设备时，启用本地密码检查。

```
Cisco(config-line)# login local
```

第 5 步，返回特权模式。

```
Cisco(config)# end
```

第 6 步，保存修改后的配置。

```
Cisco# copy running-config startup-config
```

10.1.2 配置命令级别安全

控制网络上的终端访问交换机的一个简单办法，就是使用口令保护和划分特权级别（如图 10-3 所示）。口令可以控制对网络设备的访问，特权级别可以在用户登录成功后，控制其可以使用的命令。

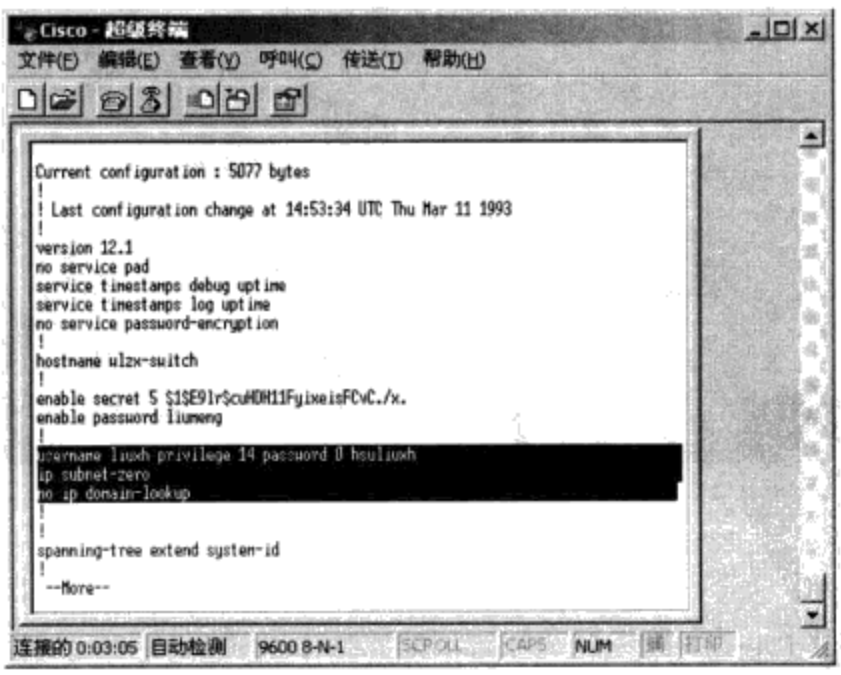


图 10-3 用户级别

在默认情况下，系统只有 2 个受口令保护的授权级别，即普通用户级别和特权用户级别。不过，可以为每个模式的命令划分 16 个授权级别。通过给不同的级别设置口令，就可以使不同的授权级别使用不同的命令集合。例如，想让更多的授权级别使用某一条命令，则可以将该

命令的使用权授予较低的用户级别。而如果想让命令的使用范围小一些，则可以将该命令的使用权授予较高的用户级别。

1. 配置多个用户级别

为某个配置命令设置多个用户级别时，配置过程如下。

第 1 步，进入全局配置模式。

```
Cisco# configure terminal
```

第 2 步，设置命令的级别划分。mode 用于指定命令的模式，其中，configure 表示全局配置模式，exec 表示特权命令模式，interface 表示接口配置模式，line 表示 Line 配置模式。level 用于授权级别，取值范围为 0~15，level 1 是普通用户级别，level 15 是特权用户级别，在各用户级别间切换可以使用 enable 命令。command 则用于指定欲授权的命令。

```
Cisco(config)# privilege mode level level command
```

> **提示** 当将一条命令的权限授予某个级别时，则该命令的所有参数和子命令都同时被授予该级别，除非该授权被收回。

第 3 步，返回特权模式。

```
Cisco(config)# end
```

第 4 步，保存修改后的配置。

```
Cisco# copy running-config startup-config
```

若要恢复一条已知的命令授权，可以在全局配置模式下使用“no privilege mode level level command”命令。

2. 登录和离开授权级别

在特权命令模式下，可以登录到指定的授权级别，或者离开某个授权级别。登录到指定的授权级别。Level 用于指定级别，取值范围为 0~15。

```
Cisco# enable level
```

离开到指定的授权级别。

```
Cisco# disable level
```

10.1.3 终端访问限制安全

通过限制对交换机、路由器等网络设备的访问，可以最大限度地避免可能来自内部或外部的恶意网络攻击，并可有效地预防未授权用户或权限较低的网络管理员修改网络配置，从而

保护网络传输的稳定和安全。

1. 控制虚拟终端访问

默认状态下，可以通过任何网络中的任何一台计算机登录到交换机或路由器。因此，必须将访问列表应用于虚拟终端线路上，使得拥有特定 IP 地址的用户才有权访问网络设备，建立 Telnet 会话。当其他非指定 IP 地址的用户访问该设备时，将提示“不能打开到主机的连接……”，如图 10-4 所示。

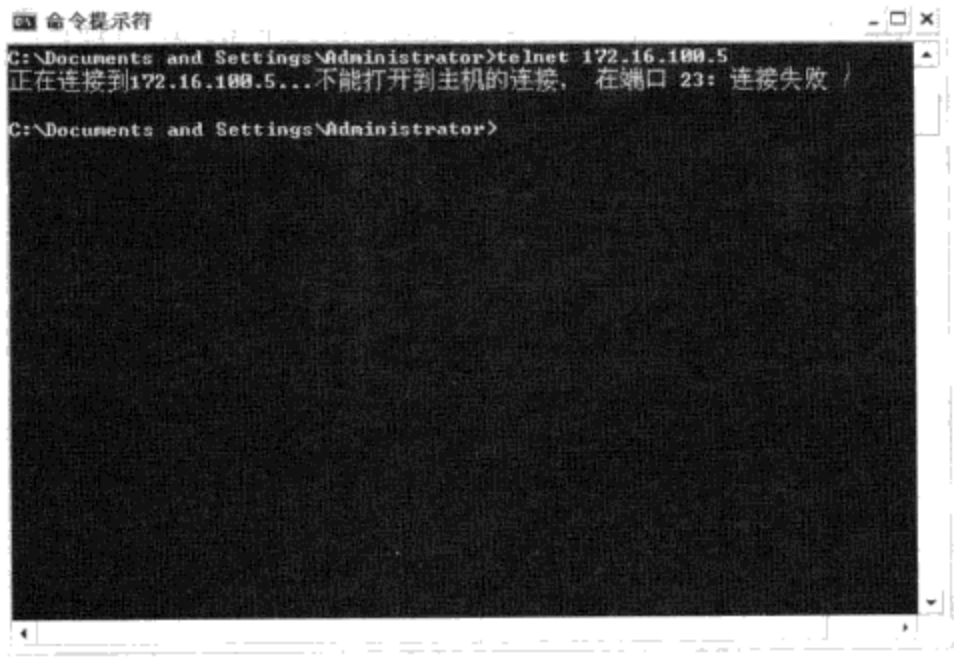


图 10-4 不能打开到主机的连接

控制虚拟终端访问配置过程如下。

第 1 步，进入全局配置模式。

```
Cisco# configure terminal
```

第 2 步，配置 IP 访问列表。

```
Cisco(config)# access-list access-lis-number permit ip-address
```

第 3 步，进入 Line 配置模式。

```
Cisco(config)# line vty 0 4
```

第 4 步，启用 IP 访问列表。

```
Switch(config-line)# access-class access-class-number in
```

第 5 步，返回特权模式。

```
Cisco(config-line)# end
```

第 6 步，保存修改后的配置。

```
Cisco# copy running-config startup-config
```

有关 IP 访问列表的设置，请参见其他相关内容，这里就不再赘述。

2. 控制会话超时

当网络管理员远程登录到路由器或交换机的控制台后，如果在特权模式下因事外出，就会使控制台处于无人看管状态，此时，任何用户都可以修改网络设备的配置。因此，对空闲会话必须进行超时设置，使得控制台在一段时间的空闲后自动断开与网络设备的连接（如图 10-5 所示），从而可提供额外的安全保障。默认超时限制值为 10 分钟。

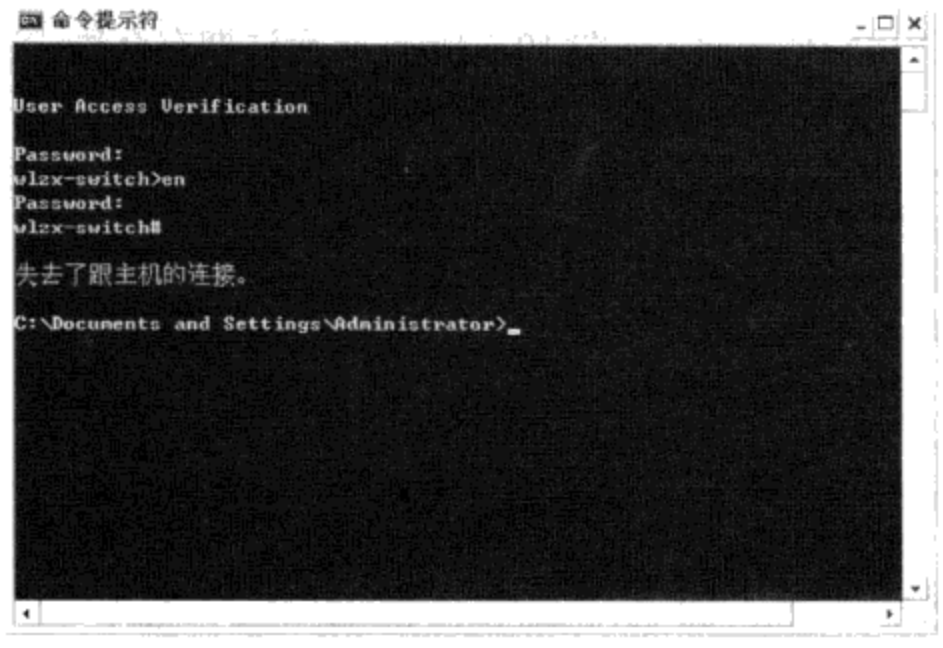


图 10-5 会话超时

要改变默认超时值，配置过程如下。

第 1 步，进入全局配置模式。

```
Cisco# configure terminal
```

第 2 步，进入 Line 配置模式。

```
Cisco(config)# line vty 0 4
```

第 3 步，设置超时连接的时间。取值范围为 0~35791，建议采用 180。

```
Switch(config-line)# exec-timeout seconds
```

第 4 步，返回特权模式。

```
Cisco(config-line)# end
```

第 5 步，保存修改后的配置。

```
Cisco# copy running-config startup-config
```

10.1.4 SNMP 安全

SNMP 是一种应用协议，为 SNMP 管理者和代理间的通信定义了协议消息格式。SNMP 管理者可以是网络管理系统的一部分，代理和管理信息库（MIB）包含在交换机上，通过配置交换机上的 SNMP，可以规定管理者同代理之间的联系。SNMP 代理包含 SNMP 管理者能够

请求或更改的管理变量。管理者能够从代理那里获得管理变量值或者向代理设置管理变量值。代理从 MIB（包含设备的参数和网络数据信息）中收集管理信息。代理也能够响应管理者发出的设置或请求操作。代理能够向管理者主动发出 TRAP 信息。TRAP 信息是用来向管理者通告网络中的某种事件的发生。TRAP 信息能够通告认证失败、重启动、连接状态和拓扑改变等重要的事件的发生。

1. 配置 SNMP 字符串

SNMP 字符串的作用类似密码（如图 10-6 所示），允许拥有合法认证名的用户同交换机上的代理通信。因此，对 SNMP 字符串的保护，应当像对待 Windows 的 Administrator 密码一样。

图 10-6　SNMP 字符串

为了更加安全地使用 SNMP，可以指定以下一个或者几个属性同认证名绑定：

IP 地址。通过指定 IP 地址，只允许该 IP 地址的管理者有权同代理通信。

读写权限。通过指定读写权限，限制管理者的操作。

第 1 步，进入全局配置模式。

```
Cisco# configure terminal
```

第 2 步，设置 SNMP 字符串。string 用于定义字符串，应当使用较长的、没有意义的、不容易被猜到的字符。ro 表示定义只读字符串，只享有配置读取权限；rw 表示可写字符串，享有配置修改权限。access-list-number 用于指定 IP 标准访问列表号，取值范围为 1～99 和 1300～1999。

```
Cisco(config)# snmp-server community string [ro | rw] [access-list-number]
```

第 3 步，如果在上面指定了 IP 访问列表，那么，就应当在这里创建它。需要时，可以重复执行该命令，以创建多条访问列表项。access-list-number 应当与上述所引用的访问列表号相同。deny 关键字将禁止与之匹配的访问，permit 关键字则允许与之匹配的访问。Source 用于指定 SNMP 管理的 IP 地址。source-wildcard（可选）键入用于指定 IP 地址范围的反码。从安

全的角度考虑，只需设置 Permit 允许特定 IP 地址即可。

```
Cisco(config)# access-list access-list-number {deny | permit} source
[source-wildcard]
```

第 4 步，返回特权模式。

```
Cisco(config)# end
```

第 5 步，保存修改后的配置。

```
Cisco# copy running-config startup-config
```

2. 配置 SNMP 组和用户

第 1 步，进入全局配置模式。

```
Cisco# configure terminal
```

第 2 步，为每个本地或远程 SNMP 复制配置名称。engineID-string 是一个 24 字符的 SNMP 复制 ID 字符串，不过，为“0”的部分不需要输入。例如，当要配置的本地设备的引擎 ID 为“123400000000000000000000”时，只需输入“snmp-server engineID local 1234”即可。如果选择的是远程设备，那么，应当指定其 SNMP 复制的 IP 地址和 UDP 端口号即可。默认端口号为“162”。

```
Cisco(config)# snmp-server engineID {local engineid-string | remote ip-address
[udp-port port-number] engineid-string}
```

第 3 步，在远程设备上配置新 SNMP 组。Groupname 用于指定组的名称。v1、v2c 和 v3 用于指定安全模式，其中，v1 安全模式最低，v3 安全模式最高。Auth 用于启用 Message Digest 5（MD5）和 Secure Hash Algorithm（SHA）包认证。Priv 用于启用 Enables Data Encryption Standard（DES）加密。Noauth 用于启用 noAuthNoPriv 加密级别。

```
Cisco(config)# snmp-server group groupname {v1 | v2c | v3 {auth | noauth | priv}}
[read readview] [write writeview] [notify notifyview] [access access-list]
```

第 4 步，为 SNMP 组添加新用户。Username 用于指定该主机上的用户名称，groupname 用于指定将该用户加入的用户组。Remote 用于指定用户所属的远程 SNMP 条目，其中，host 用于指定其主机名和 IP 地址，udp-port 用于指定端口号（默认值为 162）。v1、v2c、v3 用于指定 SNMP 版本。access-list 用于指定访问列表。如果指定为 v3，那么，还需要指定相应的认证方式。

```
Cisco(config)# snmp-server user username groupname {remote host [udp-port port]}
{v1 [access access-list] | v2c [access access-list] | v3 [encrypted] [access
access-list] [auth {md5 | sha} auth-password]}
```

第 5 步，返回特权模式。

```
Cisco(config)# end
```

第 6 步，保存修改后的配置。

```
Cisco# copy running-config startup-config
```

3. SNMP 配置实例

■ 示例 1

允许所有管理者使用“public”字符串，以只读权限访问所有对象。同时，交换机使用SNMPv1 发送 Linkup 陷阱到主机 192.168.1.111 和 192.168.1.112，使用 SNMPv2C 发送至主机 192.168.1.113。

```
Cisco(config)# snmp-server community public
Cisco(config)# snmp-server enable traps linkup
Cisco(config)# snmp-server host 192.168.1.113 version 2c public
Cisco(config)# snmp-server host 192.168.1.111 version 1 public
Cisco(config)# snmp-server host 192.168.1.112 version 1 public
```

■ 示例 2

允许访问列表 10 中指定的计算机，使用字符串“hsupublic”，以只读权限访问所有对象。其他 SNMP 管理员将被拒绝访问任何对象。SNMP 认证失败陷阱时，使用字符串“public”，以 SNMPv2C 方式发送至 192.168.100.100。

```
Cisco(config)# snmp-server community hsupublic ro 10
Cisco(config)# snmp-server enable traps snmp authentication
Cisco(config)# snmp-server host 192.168.100.100 version 2c public
```

■ 示例 3

发送 Entity MIB 陷阱到主机 192.168.100.120，字符串为“coolpen”。其中，第 1 行用于将发送 Entity MIB 的陷阱添加至以前发送的陷阱中，第 2 行用于指定陷阱的目的地，并且覆盖以前所有 SNMP 服务器主机（192.168.100.110）命令。

```
Cisco(config)# snmp-server enable traps entity
Cisco(config)# snmp-server host 192.168.100.110 restricted entity
```

■ 示例 4

使用字符串“public”将交换机中的所有陷阱发送至 192.168.100.100。

```
Cisco(config)# snmp-server enable traps
Cisco(config)# snmp-server host 192.168.100.100 public
```

■ 示例 5

将 authgroup 用户组 authuser 用户关联到一个远程设备（192.168.100.130），当用户进入全局配置模式时，发送 auth 认证级别通知。

```
Cisco(config)#     snmp-server     engineID     remote     192.168.100.130
800000090300000AF45812C1
Cisco(config)# snmp-server group authgroup v3 auth
Cisco(config)# snmp-server user authuser authgroup remote 192.168.100.130 v3
```

```
auth md5 mypassword
    Cisco(config)# snmp-server user authuser authgroup v3 auth md5 mypassword
    Cisco(config)# snmp-server host 192.168.100.130 informs version 3 auth authuser
config
    Cisco(config)# snmp-server enable traps
    Cisco(config)# snmp-server inform retries 0
```

10.1.5 HTTP 服务安全

Cisco IOS 允许通过 Web 浏览器管理交换机和路由器，所需的 HTTP 服务器软件可在 IOS 11.0 及以后的版本中找到。这虽然使网络配置变得更加简单，但也可能由此而产生安全漏洞。因此，如非特别需要，建议关闭 HTTP 服务。

1. 关闭 HTTP 服务

若欲关闭 HTTP 服务，可使用如下命令：

```
Cisco# configure terminal
Cisco(config)# no ip http server
Cisco(config)# end
Cisco# copy running-config startup-config
```

使用“show running-config”命令查看时，HTTP 服务已经被关闭，如图 10-7 所示。

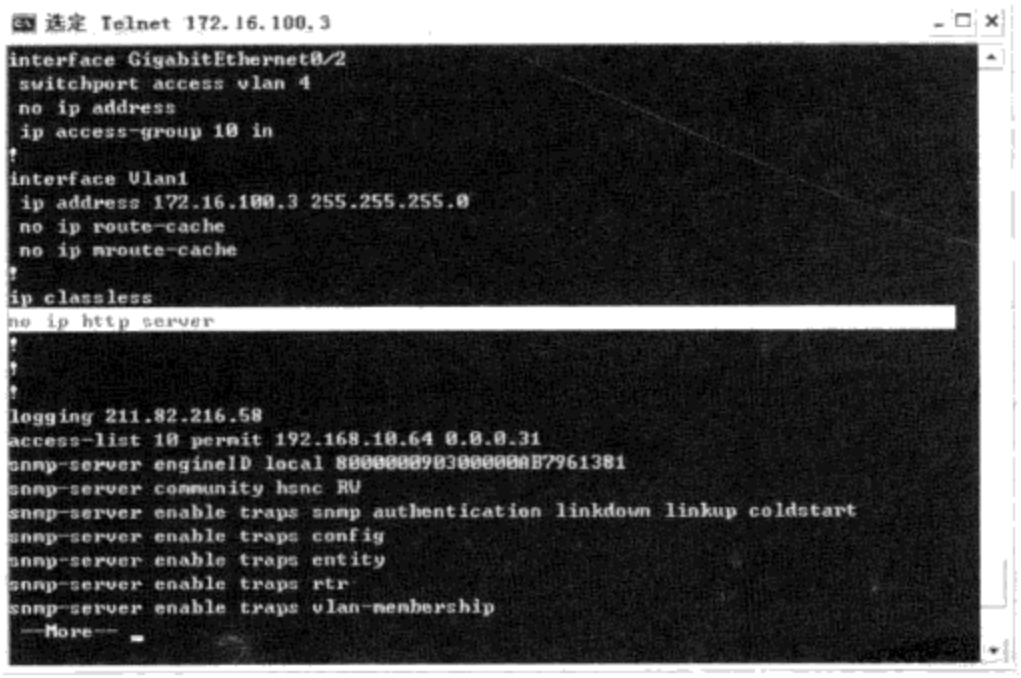


图 10-7 HTTP 服务被关闭

若需启用 HTTP 访问，则使用如下命令：

```
Cisco# configure terminal
Cisco(config)# ip http server
Cisco(config)# end
Cisco# copy running-config startup-config
```

然后，再通过访问控制列表过滤允许访问网络设备的计算机。

2. 配置安全 HTTP 服务

可以将网络设备设置为 HTTPS 服务，让交换机和路由器作为认证服务器，从而提高网络传输的安全性。

第 1 步，查看 HTTP 服务状态。如果网络设备支持安全 HTTP 服务，将显示信息“HTTP secure server capability: Present”或“HTTP secure server capability: Not present”。

```
Cisco# show ip http server status
```

第 2 步，进入全局配置模式。

```
Cisco# configure terminal
```

第 3 步，启用安全 HTTPS 服务。默认状态下，HTTPS 服务是被启用的。

```
Cisco(config)# ip http secure-server
```

第 4 步，（可选）指定 HTTPS 服务的端口号。默认端口号为 443，有效取值范围为 1025～65535。建议采用系统默认值 443。

```
Cisco(config)# ip http secure-port port-number
```

第 5 步，（可选）为 HTTPS 连接指定 CipherSuites 加密算法。如果不指定加密算法，HTTPS 服务器与客户端将协商所采用的算法。默认为不指定加密算法。

```
Cisco(config)#ip http secure-ciphersuite {[3des-ede-cbc-sha] [rc4-128-md5]
[rc4-128-sha] [des-cbc-sha]}
```

第 6 步，（可选）在连接处理期间，配置 HTTP 服务从客户端请求 X.509v3 证书。默认情况下，客户端将从服务器请求证书，但是，服务器不会尝试从客户端获取证书。

```
Cisco(config)# ip http secure-client-auth
```

第 7 步，指定 CA 信任点（Trustpoint）使用得到的 X.509v3 证书认证客户端连接。

```
Cisco(config)# ip http secure-trustpoint name
```

第 8 步，（可选）为 HTTP 服务指定主目录。该路径通常位于网络设备本地的 Flash 闪存中。

```
Cisco(config)# ip http path path-name
```

第 9 步，（可选）指定一个允许访问 HTTP 服务的访问列表。

```
Cisco(config)# ip http access-class access-list-number
```

第 10 步，（可选）设置访问 HTTP 服务的并发最大数。取值范围为 1~16，默认值为 5。如果网络内只有一个网络管理员，那么，该值不妨设置为 1。

```
Cisco(config)# ip http max-connections value
```

第 11 步，（可选）指定在几种情形下，能够与 HTTP 服务保持多长时间的连接。idle 用于指定在没有数据发送或接收时所允许连接的最长时间，取值范围为 1 ～ 600 秒，默认值为 180

秒。life 用于指定所允许的连接持续的最长时间，取值范围为 1～86400 秒，默认值为 180 秒。requests 用于指定在一个连接上所允许的请求处理最大数，最大值为 86400，默认值为 1。从安全的角度考虑，idle 取值应当在 120～180 秒，life 取值应当在 180～300 秒，requests 取值为 1。

```
Cisco(config)# ip http timeout-policy idle seconds life seconds requests value
```

第 12 步，返回特权模式。

```
Cisco(config)# end
```

第 13 步，保存修改后的配置。

```
Cisco# copy running-config startup-config
```

3. 配置安全 HTTP 客户端

如果没有配置 CA 信任点，那么，当远程 HTTPS 服务器请求客户端认证时，到该 HTTP 客户端的连接将失败。因此，必须配置安全 HTTP 客户端。

第 1 步，进入全局配置模式。

```
Cisco# configure terminal
```

第 2 步，（可选）指定远程 HTTP 服务器请求客户端认证时使用的 CA 信任点。使用该命令的前提是已经配置了 CA 信任点。当然，如果客户端无需认证，或者根信任点已经存在，那么，该命令并非必需。

```
Cisco(config)# ip http client secure-trustpoint name
```

第 3 步，（可选）为 HTTPS 连接指定 Ciphersuites 加密算法。如果不指定加密算法，HTTPS 服务器与客户端将协商所采用的算法。默认为不指定加密算法。

```
Cisco(config)#ip http secure-ciphersuite {[3des-ede-cbc-sha] [rc4-128-md5]
[rc4-128-sha] [des-cbc-sha]}
```

第 4 步，返回特权模式。

```
Cisco(config)# end
```

第 5 步，保存修改后的配置。

```
Cisco# copy running-config startup-config
```

10.2 系统安全日志

网络设备的 Syslog 日志功能可以将某些重要事件信息（如系统错误、系统配置、状态变化、状态定期报告和系统退出等）或用户设定的期望信息传送给日志服务器，网管人员依据这些信息掌握设备的运行状况，及早发现问题，及时进行配置设定和排障，保障网络安全稳定地运行。

10.2.1 日志信息概述

1. 日志信息格式

日志信息将以以下格式显示：

```
seq no:timestamp: %facility-severity-MNEMONIC:description
```

日志信息中各个要素的描述如表 10-1 所示。

表 10-1 日志信息要素

要 素	描 述
seq no	标记日志信息序号。只有执行“service sequence- numbers”配置命令后，才显示该序号
timestamps 格式如下：*mm/dd hh:mm:ss* 或 *hh:mm:ss*（短时间运行时）或 *d h*（长时间运行时）	日志信息的产生时间。只有执行“service timestamps log [datetime | log]”配置命令后，才显示该部分
facility	日志信息要点
serverity	日志信息的级别，取值范围为 0～7
MNEMONIC	日志信息类型描述
description	日志信息详细描述

下面是 Cisco Catalyst 3550 交换机系统日志信息的一部分（如图 10-8 所示）。

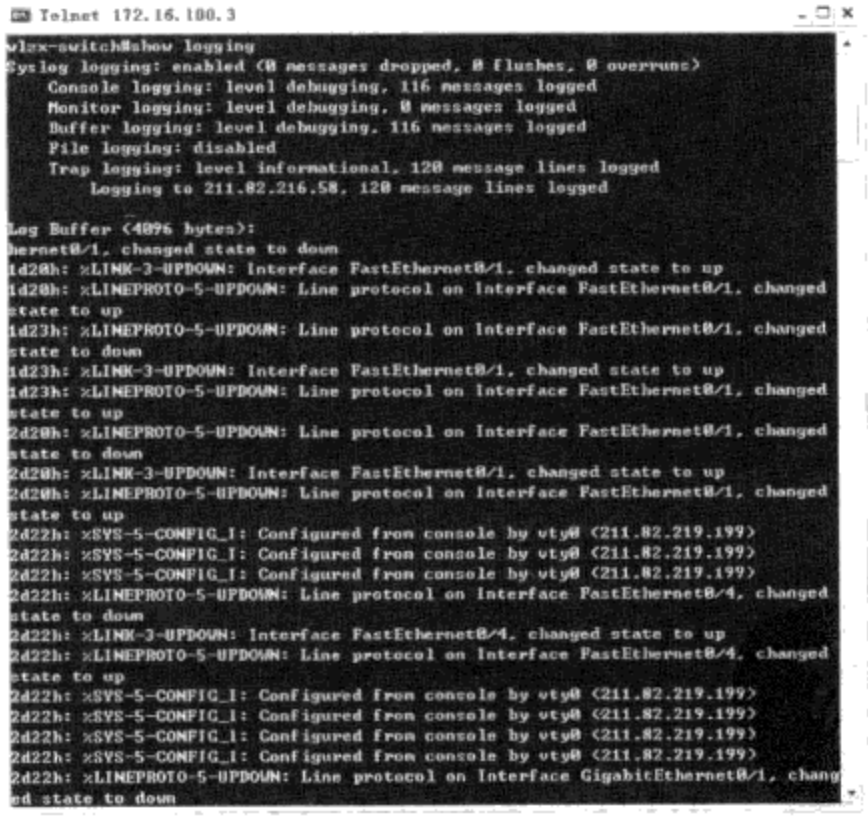


图 10-8 系统日志信息

```
    3d18h: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed
    state to down
    3d18h: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
    3d18h: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed
```

```
    state to up
    3d19h: %SYS-5-CONFIG_I: Configured from console by vty0 (211.82.219.199)
    3d20h: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4,
changed
    state to down
    3d20h: %LINK-3-UPDOWN: Interface FastEthernet0/4, changed state to up
    3d20h: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4,
changed
    state to up
    3d20h: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed
    state to down
```

2. 日志信息等级

可以根据需要决定向管理界面发送的日志信息。根据事件严重程度的不同，日志信息等级定义为 0~7 共 8 级，如表 10-2 所示。

表 10-2 日志信息等级关键字

关 键 字	等 级	描 述	系统日志定义
Emergencies	0	紧急情况	LOG_EMERG
Alerts	1	应该被立即改正的问题	LOG_ALERT
Critical	2	重要情况	LOG_CRIT
Errors	3	错误	LOG_ERR
Warnings	4	警告	LOG_WARN
Notifications	5	不是错误情况但可能需要处理	LOG-NOTICE
Informational	6	普通信息	LOG_INFO
Debugging	7	调试信息	LOG_DEBUG

3. 日志信息类别

日志信息类别及描述如表 10-3 所示。

表 10-3 日志信息类别

日志信息	描 述
@5-COLDSTART: System coldstart	系统冷启动
@5-WARMSTART: System warmstart	系统热启动
@5-CONFIG:Configured from [chars] by [chars]	系统配置改变。第一个 chars 指明管理类型，第二个 chars 指明管理者的 IP
@5- LINKUPDOWN Interface [chars] changed state to [chars]	端口状态改变。第一个 chars 指明对应的接口，第二个 chars 指明接口当前的状态
@4-TOPOCHANGE: Topology is changed	网络拓扑结构改变
@4-NEWROOT：New root is produced	网络中有新的根桥产生
@4-AUTHFAILURE: Authenticate failed	用户认证失败。
@2-STORMGENERATE: Broadcast（Unicast,Multicast） storm has happend in [chars]	接口上有帧（广播，单播，多播）风暴产生。chars 表示对应的接口
@2-PORTSECURVIOLATED: Security has be violated of [chars].	端口安全被违反。chars 表示对应的接口
@4-HWCHANGE: Module [chars] has been plugged into slot [chars] @4-HWCHANGE: Module [chars] in slot [chars] has been pulled out	系统的硬件发生变化，模块插入/移除

4. 系统日志默认配置

系统日志的默认配置如表 10-4 所示。

表 10-4 系统日志默认配置

属 性	默认设置
系统日志开关	打开
在 telnet 界面显示日志信息	打开
telnet 信息等级	7 级
在 telnet 界面显示信息	关闭
telnet 界面显示信息等级	7 级
向缓冲区发送日志信息	打开
缓冲区日志信息等级	7 级
将日志信息记录到文件	关闭
文件记录日志信息等级	5 级

10.2.2 启用系统日志信息

默认情况下，日志信息功能是被启用的。但是，当系统日志信息被关闭后，可以借助以下操作，重新启用日志信息。

第 1 步，进入全局配置模式。

```
Cisco# configure terminal
```

第 2 步，启用系统日志信息。

```
Cisco(config)# logging on
```

第 3 步，返回特权模式。

```
Cisco(config)# end
```

第 4 步，查看日志信息状态。

```
Cisco# show running-config
Cisco# show logging
```

第 5 步，保存修改后的配置。

```
Cisco# copy running-config startup-config
```

如图 10-9 所示为重新启用日志信息，并显示其工作状态的操作过程。

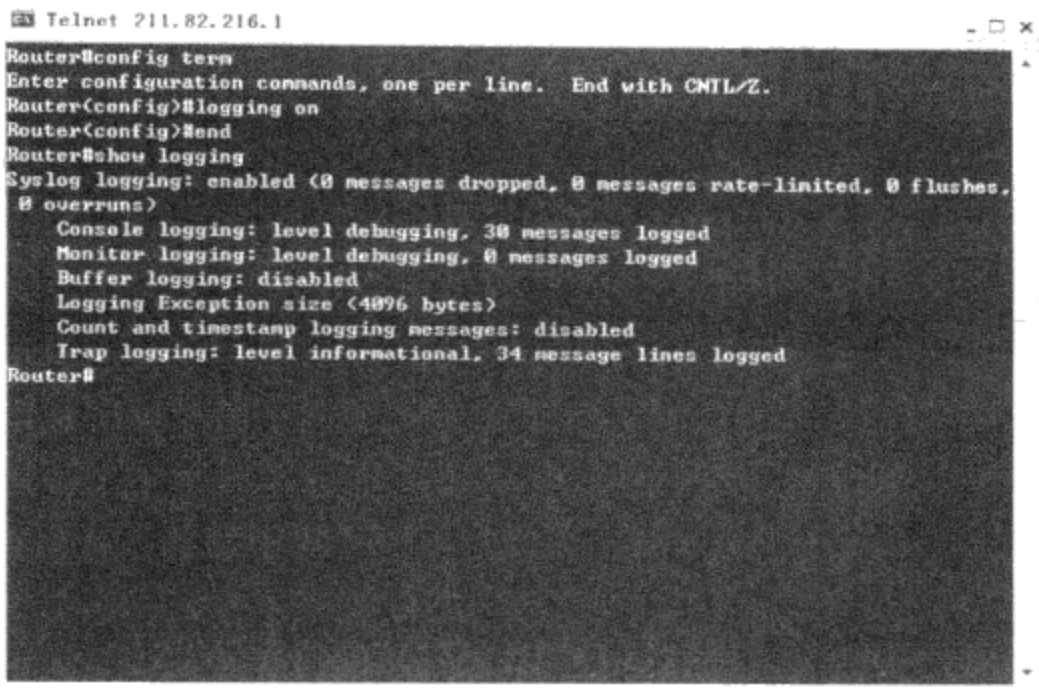


图 10-9　重新启用日志信息

10.2.3 设置日志信息存储设备

当系统日志信息功能被启用后，默认状态下将存储在网络设备的缓存中。而网络设备一旦瘫痪，缓存中的日志文件将全部丢失，除非事先将其保存至闪存中。因此，若要借助日志文件分析故障和安全事件，必须将日志信息存储在其他目的设备。

设置日志信息存储设备配置过程如下。

第 1 步，进入全局配置模式。

```
Cisco# configure terminal
```

第 2 步，将日志信息记录到设备内置的缓存。默认缓存大小为 4096，可取值范围为 4096 ~ 2147483647 字节。

> **提示**　不要将缓存设置得太大，因为交换机的其他任务也需要使用该缓存。使用“show memory”命令可以查看交换机中空闲的内存。Size 的设置值一定要小于最大可用值。

```
Cisco(config)# logging buffered [size]
```

第 3 步，将日志记录到 UNIX 系统日志服务器。Host 可以是系统日志服务器的计算机名称或 IP 地址。如果有多台 UNIX 系统日志服务器，应当重复执行该命令。

```
Switch(config)# logging host
```

第 4 步，将系统日志保存在设备闪存中。max-file-size 用于指定日志文件的最大尺寸，取值范围为 4096 ~ 2147483647，默认值为 4096 字节。min-file-size 用于指定日志文件的最小尺寸，取值范围为 1024 ~ 2147483647，默认值为 2048 字节。severity-level-number | type，用于指定每个日志的严重级别或日志类型，取值范围为 0 ~ 7。

```
Cisco(config)#logging file f lash:filename [max-file-size [min-file-size]]
[severity-level-number | type]
```

提示 将日志保存在设备闪存中是个不错的选择。特别是当没有专门的 UNIX 系统日志服务器时。

第 5 步，返回特权模式。

```
Cisco(config-line)# end
```

第 6 步，校验配置。

```
Cisco# show running-config
```

第 7 步，保存修改后的配置。

```
Cisco# copy running-config startup-config
```

10.2.4 定义消息严重等级

可以限制将某种级别的消息发送至某种目的设备。在特权 EXEC 模式下开始，借助以下步骤可以定义消息的严重等级及目的设备。

第 1 步，进入全局配置模式。

```
Switch # configure terminal
```

第 2 步，限制将消息发送到控制台。

```
Switch (config) # logging console level
```

第 3 步，限制将消息发送到终端。

```
Switch (config) # logging monitor level
```

第 4 步，限制将消息发送到日志服务器。

```
Switch (config) # logging trap level
```

第 5 步，返回特权 EXEC 模式。

```
Switch (config-if) # end
```

第 6 步，校验配置。

```
Switch # show running-config
```

或者

```
Switch # show logging
```

第 7 步，保存修改后的配置。

```
Switch # copy running-config startup-config
```

禁用控制台上的日志，使用“no logging console”全局配置指令。禁用到终端或其他控制台的日志，使用“no logging monitor”全局配置指令。禁用系统日志陷阱，使用“no logging trap”全局配置指令。

10.2.5 配置 UNIX 系统日志服务器

1. 将消息发送至 UNIX 系统日志 Daemon

将消息发送到 UNIX 系统日志服务器之前，必须在一个 UNIX 服务器上配置系统日志后台程序。

第 1 步，添加一个类似下面文件的行到文件/etc/syslog.conf。关键字“local7”指定被使用的日志工具，关键字“debug”指定系统日志的等级，系统 log 在这个等级或一个更严重的等级下发送消息。这个文件首先必须存在，并且系统 log 后台程序必须允许读。

```
local7.debug /usr/adm/logs/cisco.log
```

第 2 步，创建一个日志文件。

```
$ touch/var/log /cisco.log
$ chmod 666/var/log/cisco.log
```

第 3 步，确保系统日志后台程序读改变后的新文件。

```
$ kill -HUP ` cat/etc/syslog.pdi`
```

2. 配置 UNIX 系统日志工具

当将系统日志消息发送到外部设备时，可以在交换机上标识将这些信息发送至哪个 UNIX 系统日志工具。

在特权 EXEC 模式下开始，下面的步骤是配置 UNIX 系统日志工具。

第 1 步，进入全局配置模式。

```
Switch # configure terminal
```

第 2 步，使用 IP 地址让日志消息到一个 UNIX 系统服务器主机。

```
Switch (config) # logging host
```

第 3 步，限制消息到日志服务器。

```
Switch (config) # logging trap level
```

第 4 步，配置系统日志工具。

```
Switch (config) # logging facility facility-type
```

第5步，返回特权EXEC模式。

```
Switch (config-if) # end
```

第6步，校验配置。

```
Switch # show running-config
```

第7步，保存修改后的配置。

```
Switch # copy running-config startup-config
```

移除一个系统日志服务器，使用“no logging host”全局配置指令，并指定系统日志服务器的IP地址。禁用系统日志服务器的日志，输入“no logging trap”全局配置指令。

表10-5显示了UNIX系统被软件支持的工具。

表10-5 UNIX系统被软件支持的工具

工具类型关键字	描 述
auth	授权系统
cron	Cron工具
daemon	系统后台程序
kern	核心
local0-7	本地定义消息
lpr	行打印系统
mail	邮件系统
news	USENET news
sys9-14	系统使用
syslog	系统日志
user	用户进程
uucp	UNIX-to-UNIX复制系统

若要显示日志配置和日志缓冲的内容，可以使用“show logging”特权EXEC指令。

10.3 网络设备系统映像安全

IOS是Cisco拥有的核心软件数据包，主要在Cisco路由器和交换机上实现。IPS则是包括Cisco路由器在内的许多网络产品具有的保护功能，能够实时阻止未经授权的网络访问和恶意代码。然而，Cisco最近连续公布了几个严重的系统漏洞。黑客可以利用其中一个漏洞在未被IOS IPS（入侵防御系统）察觉的情况下侵入系统；同时可以利用另外的漏洞使IOS IPS设备瘫痪，导致“拒绝服务”情况发生。因此，路由器和交换机（尤其是路由器）必须及时为IOS安装升级补丁封堵漏洞。

10.3.1 备份系统软件映像

为了保证网络设备系统映像在意外损坏（如误删除、闪存故障或被恶意攻击者破坏），和保障系统映像升级后遇到问题时可以迅速恢复，应当及时备份系统软件映像，特别是在执行IOS系统升级之前，必须要执行该项操作。系统映像的备份需要借助TFTP服务器完成。下面，

以 Cisco 3640 系统映像的备份为例介绍。

第 1 步，运行 Cisco TFTP 服务器，通过 Console 端口、超级终端或 Telnet 登录至需要备份系统映像的网络设备。

提示

充当 TFTP 服务器的计算机必须关闭网络防火墙，开启 TFTP 服务端口。并且交换机的 IP 访问列表中不能限制 TFTP 端口。

第 2 步，进入全局配置模式。

```
Cisco# configure terminal
```

第 3 步，查看当前闪存中的 IOS 系统版本，如图 10-10 所示。

```
Cisco# show version
```

图 10-10　查看 IOS 系统版本

第 4 步，查看闪存中的文件夹和系统映像文件名称，如图 10-11 所示。确认系统文件名称为“c3640-d-mz.120-4.bin”。IOS 映像文件的扩展名为 bin。

```
Cisco# dir flash:
```

图 10-11　查看闪存文件系统

提示 如果系统文件位于子文件夹中，可以使用“cd sub_dir”命令进入该子文件夹，然后，再使用“dir”命令查看系统文件映像名称。

第5步，将软件映像上传至TFTP服务器，如图10-12所示。在提示符下，指定源IOS文件名、TFTP服务器地址、目的IOS文件名和系统映像将被上传至TFTP服务器。

```
Cisco# copy flash tftp
```

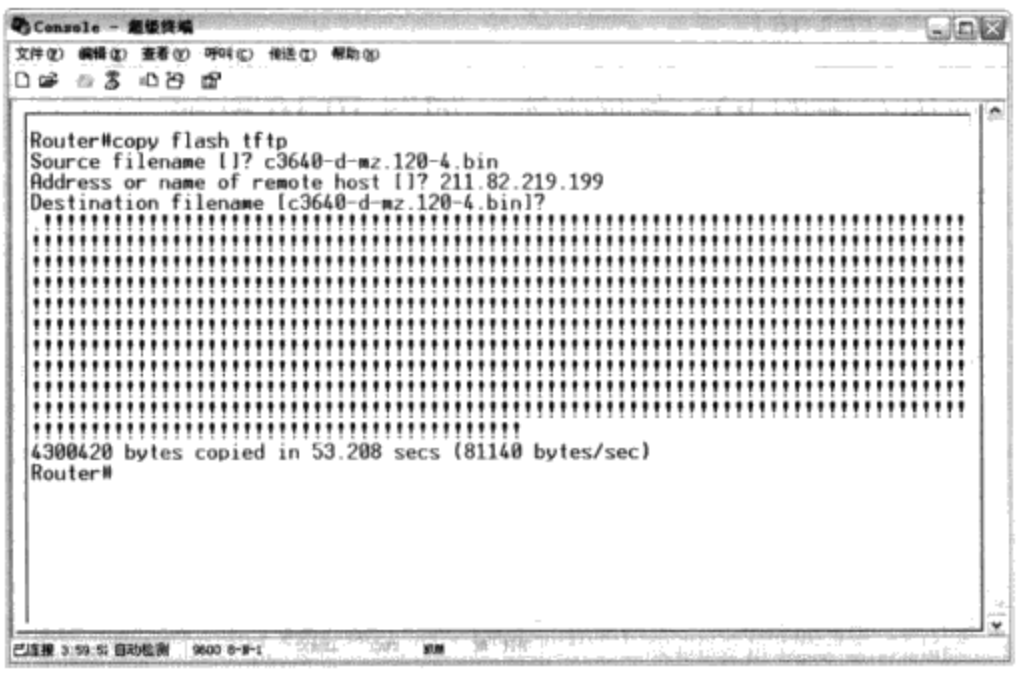


图10-12 将IOS上传至TFTP服务器

10.3.2 恢复或升级系统软件映

使用TFTP服务器，可以通过网络将系统软件映像下载到网络设备。当软件映像下载时，该映像文件被下载至超级引擎闪存中。如果闪存的容量够大，可以在其中保存多个映像文件，并选择用于引导的映像文件。

第1步，将下载的软件映像复制至Cisco TFTP服务器默认目录（C:\program files\Cisco Systems\Cisco TFTP Server）。通过Console端口、超级终端或Telnet登录至交换机。如果使用Telnet登录交换机，那么，当交换机运行新软件而重新启动时，将断开连接。

提示 同时使用Console端口和以太网端口连接管理用计算机和需要升级系统映像的网络设备，将大大提高系统映像的复制速度。

第2步，查看网络设备闪存容量，确认系统映像小于或等于该值（如图10-13所示）。

```
Cisco# show flash:
```

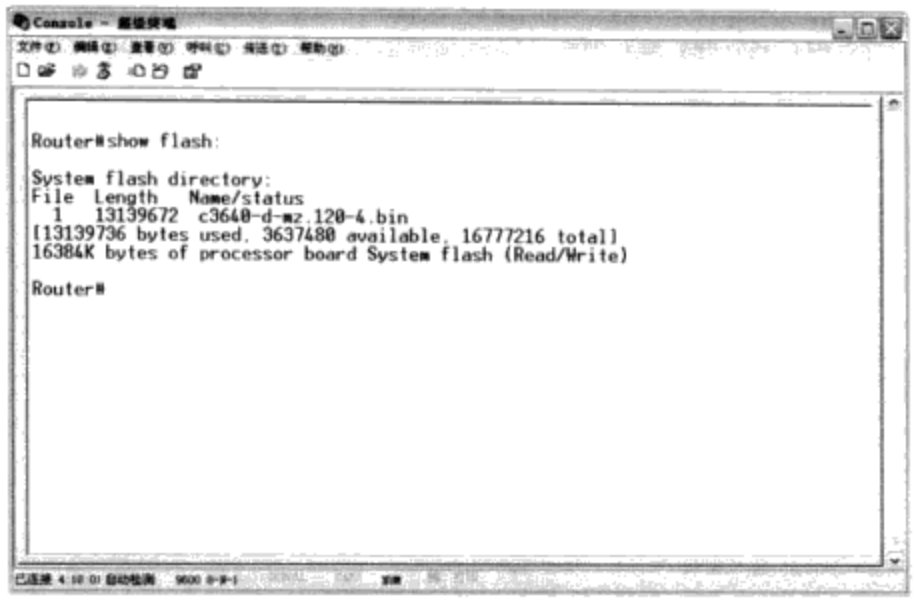
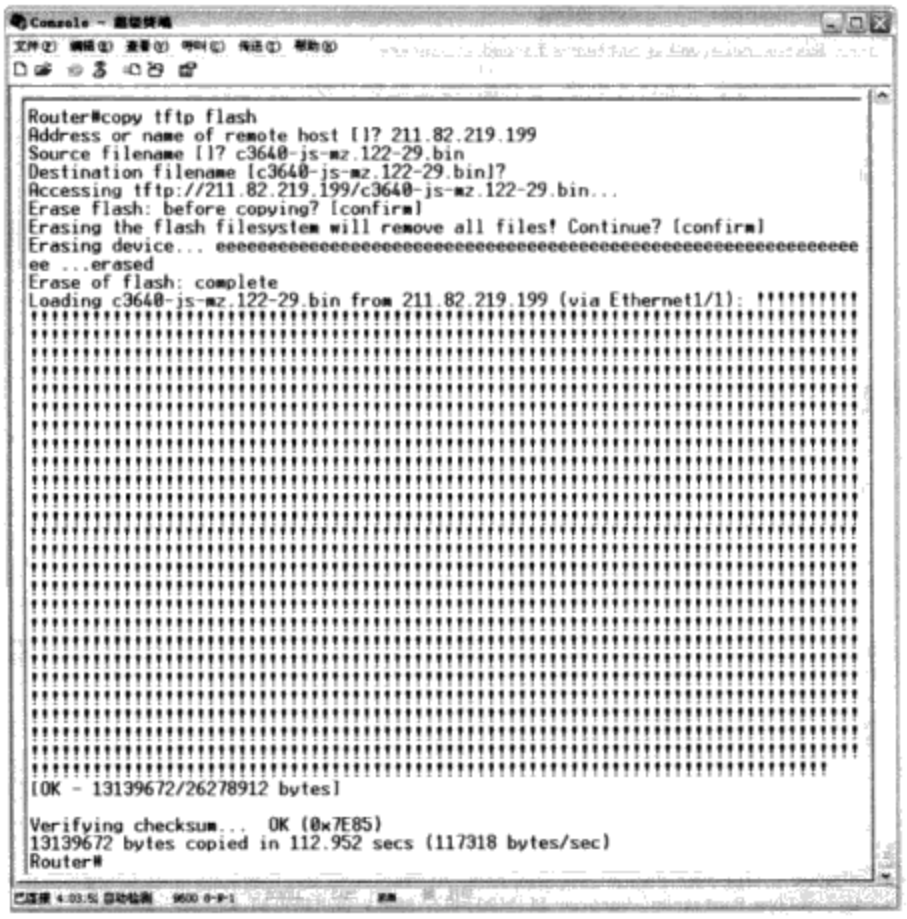


图 10-13　查看闪存容量

第 3 步，从 TFTP 服务器下载软件映像，如图 10-14 所示。在提示符下输入 TFTP 服务器的 IP 地址或主机名，以及要更新升级的 IOS 文件名，并确认删除原有的系统映像。网络设备将从 TFTP 服务器下载映像文件，并将映像复制至引导闪存。

```
Cisco# copy tftp flash
```


Router#copy tftp flash
Address or name of remote host []? 211.82.219.199
Source filename []? c3640-js-mz.122-29.bin
Destination filename [c3640-js-mz.122-29.bin]?
Accessing tftp://211.82.219.199/c3640-js-mz.122-29.bin...
Erase flash: before copying? [confirm]
Erasing the flash filesystem will remove all files! Continue? [confirm]
Erasing device... eeee

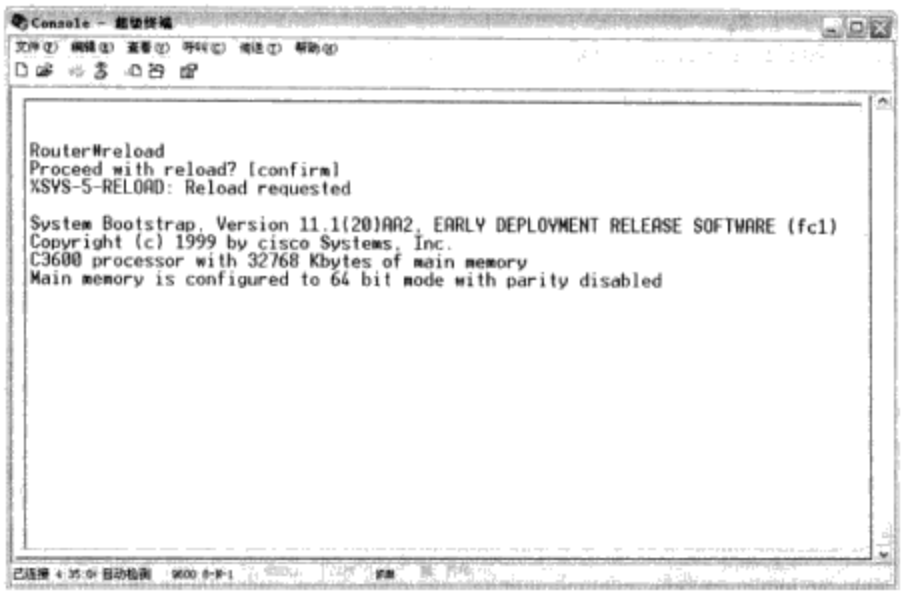


图 10-15　重新引导 IOS

图 10-16　进入 rom 监视模式

第 6 步，重新引导 IOS 系统。

```
Cisco# reset
```

第步，重新引导后，查看更新的 IOS 版本（如图 10-17 所示）。

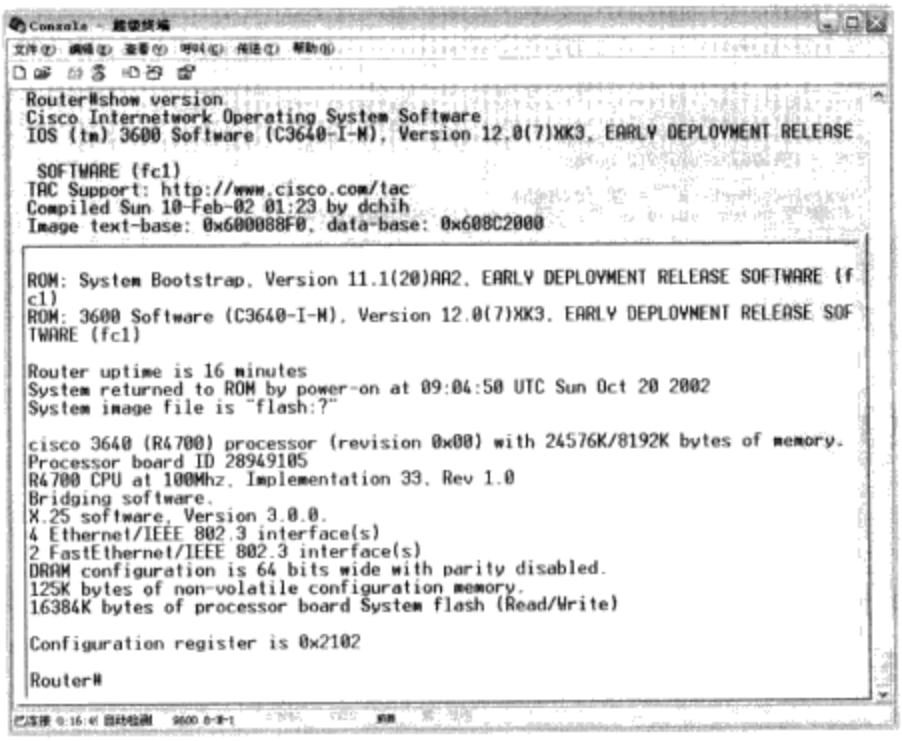


图 10-17　查看更新的 IOS 版本

第 11 章　Internet 接入安全

接入 Internet 是局域网的重要功能之一，其主要目的就是实现更广范围的资源共享与信息传输。但是，相对于局域网内部而言，Internet 连接和传输往往是没有任何安全保障的，这也是许多企业内部重要部门禁止接入 Internet 的主要原因。其实，Internet 接入的安全并非防不胜防，如果能够正确部署和配置安全设备或部署边缘安全防御系统，完全可以保证基本 Internet 连接和传输的安全进行。

11.1　网络边缘安全设备

若要构建一个真正牢固、强大的网络，任何环节都不容忽视。在危机四伏的 Internet 世界中，部署在局域网边缘的安全设备必然首当其冲的成为众矢之的。因此，边缘安全设备的安全性和性能将直接影响整个网络的安全。如今，在许多局域网中边缘安全设备往往要身兼数职，不仅要配置安全筛选策略，还要实现共享接入、发布服务器等。本小节主要介绍边缘安全设备的选型与配置规划。

11.1.1　网络边缘安全设备类型与适用

边缘网络设备通常包括路由器、防火墙、代理服务器等，也有些网络甚至直接通过集成多业务的核心路由器作为 Internet 接入设备，这种接入方式的危险性是显而易见的，一旦核心设备遭到入侵，不仅 Internet 接入收到影响，就连内部交换也可能无法顺利实现。除此之外，其他几种接入方式各有千秋，用户可以依据实际环境，选择适当的接入方式。

1.　多业务路由器

“路由器”向来以接口丰富和稳定的处理能力而著称，其主要功能就是以各种方式实现网络互连，如实现局域网与 Internet 的互连等。目前，单纯用路由器实现 Internet 接入的情况已经很少，但是，如果局域网需要实现安全防御、VPN、VoIP、分支结构互连等应用，则在边缘部署多业务路由器是非常不错的选择。

如图 11-1 所示是 Cisco 3945 集成多业务路由器，不仅集成丰富的接口，而且提供多个插槽，允许用户根据需要选择相应的业务板卡。路由器的信息信道功能一般由硬件来完成，包括转发决定、转发以及输出数据链路调度等；传输控制功能一般用软件来实现，包括与相邻路由器之间的信息交换、系统配置、系统管理等。由于它强大的网络翻译和互连功能，因此，被广泛应用于网络地址转换、Internet 接入、网络互连等各个方面。

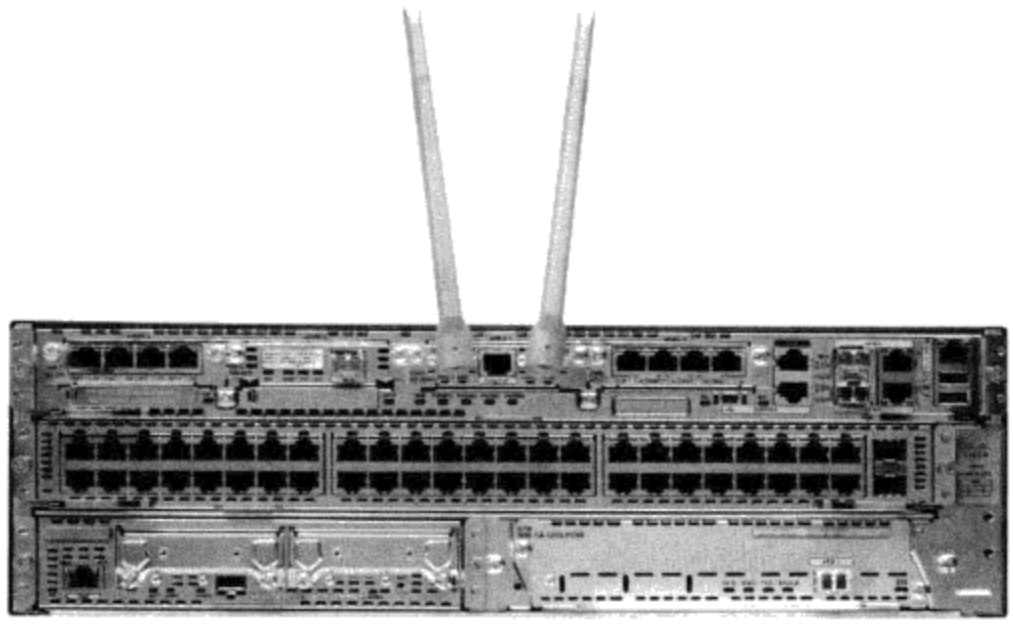


图 11-1 Cisco 3945 集成多业务路由器

2. 边缘防火墙

防火墙是最重要且最常用的网络边缘安全设备，既可以同时提供安全防护和网络互连功能，也可以仅提供安全防护功能。相对于网络边缘的路由器而言，防火墙不仅可以提供常用的网络互连方式，而且可以提供强大的安全防护功能。网络边缘接入路由器的安全防护功能通常是基于软件实现的，这一点是无法与网络防火墙同日而语的。但是，由于边缘防火墙通常只提供以太网接口，因此只能以太网方式实现网络互连，即便如此已经可以满足大部分用户的 Internet 接入和安全防护的双重需求。

如图 11-2 所示 Cisco ASA 5500 系列安全设备。防火墙最初的设计思想是，对内部网络总是信任的，对外部网络总是不信任的，所以当初的防火墙只能对外部进入的通信数据进行过滤，而对内部网络用户发出的信息不做任何限制。目前，最新的分布式防火墙系统在过滤机制上有所改变，不仅对外部网络发送过来的数据进行过滤，对内部网络用户发出的部分连接请求和数据包同样需要过滤，但防火墙仍然只是让符合安全策略的数据包通过。

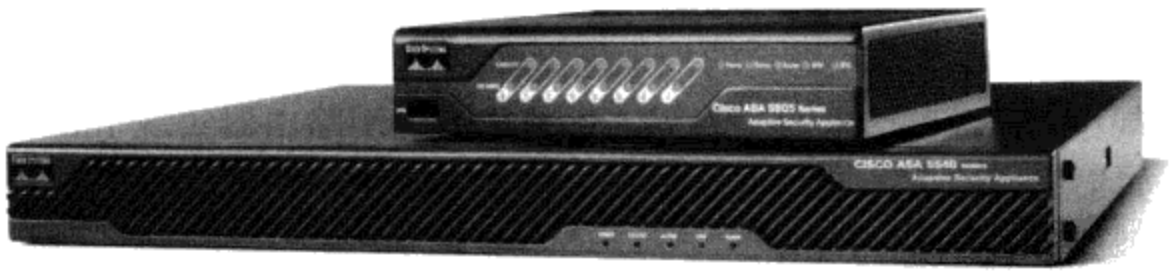


图 11-2 Cisco ASA 5500 系列

3. 代理服务器

代理服务器，是一种最简单、最常用、也最廉价的 Internet 连接共享方式。对于小型网络或 SOHO 网络而言，只需要一台服务器或普通 PC，即可实现所有网络用户的 Internet 连接共享。当网络规模较大、用户数量较多时，可以采用群集代理服务器的方式，提高服务器的处理能力和稳定性。

部署在网络边缘的代理服务器不仅需要提供 Internet 连接功能，还需要提供可靠的安全防

护，因此，选购服务器和代理软件也就成了重点。例如，在计算机数量不超过 10 台的小型办公网络中，可以直接使用普通 PC 和 Windows 系统的 ICS（Internet 连接共享）实现安全接入，如果计算机数量超过上百台，则需要部署单独的代理服务器和专业代理服务器软件（如 Microsoft 的 Forefront TMG 等）实现安全接入。

11.1.2 网络边缘安全设备选择

Internet 接入区的实际应用情况不同于局域网内部或某个分支子网，只需处理内部用户与外网之间的访问请求和数据传输即可，但是，边缘设备往往是局域网唯一的出口，因此要求其具备较高的可靠性，甚至采用链路冗余或双机热备技术，达到增强可靠性和稳定性的目的。不同边缘安全设备的功能及适用环境也有所不同，选购之前必须进行合理规划，以免造成投资浪费或网络传输瓶颈。

1. 边缘安全路由器的选择

边缘安全路由器通常位于企业网络的边缘，主要用于提供与分支机构网络的互连、VPN 接入、视频语音系统互连、安全防护等功能。相对于核心路由器而言，接入路由器的通常要身兼数职，因此选购策略也有所不同。

■ 多业务支持

接入路由器最重要的工作就是把各种方式接入的用户汇聚到网络中，每种接入方式的用户数量都不会太多，所以对其处理能力的要求相对较低，关键是对每种接入方式的支持。远程访问 VPN 是大多数企业都广泛应用的远程互联方式，如分支机构同企业本部之间的安全互连、出差用户到企业网络的安全连接等。除此之外，企业中常见的附加业务还包括网络电话、视频会议、网络传真等。

■ 多协议支持

多种网络接口的支持、多种协议的支持是体现接入路由器网络多面手的基础。开放标准的协议是设备互连的前提，所支持的协议也意味着设计上的灵活和高效，一般路由器都能够对多种链路层的协议进行支持，例如 PPP、MP、LAPB、X.25、SLIP、HDLC、SDLC 等，可以很好地提供广域网的连接。

■ 语音支持

大多数接入型路由器都提供语音功能，即支持 IP 电话，可以大大降低企业本部与分支机构之间的语音通话成本。由于 IP 电话对网络连接实时性要求比较高，因此，如果想很好的利用 IP 电话为企业服务，路由器还必须支持 QoS 功能，以保证 IP 语音的通话质量。

■ 投资保护

边缘路由器一般服务于企业的分支机构或合作伙伴，通常不会承载企业关键业务，因此对于一般企业用户而言，无需花费高额资金购买高端产品，大多数普通中低端产品就可以胜任。另外，在选购时应根据企业发展规划，选择硬件支持能力较强，且留有足够升级空间的产品，以便在将来需要扩展接入业务时，只需购置相应业务的板卡，而无需更换新设备。

2. 边缘防火墙的选择

边缘防火墙位于企业网络的边界，用于隔离内部网络和外部网络，过滤 Internet 用户对内部网络的访问请求。边缘防火墙对于整个企业网络的安全起着重要的保护作用，其性能优劣预选性是否得当，将直接影响企业网络的安全管理。选购边缘防火墙时应注意下因素。

■ 产品类型

边缘防火墙负责整个网络的安全防御工作，对于中等规模的企业网络而言，毫无疑问应选择硬件防火墙产品。根据结构的不同，硬件防火墙又可以分为路由器集成式防火墙和独立式防火墙两种。前者无论是采用软件系统集成还是硬件模块集成，其最基本的运算系统仍是基于路由器的，相对于独立式硬件防火墙而言，其安全性和可靠性要略输一筹。

■ 自身安全性

防火墙本身就是一个用于安全防护的设备，当然其自身的安全性也就显得更加重要了。防火墙的安全性能取决于防火墙是否采用了安全的操作系统和是否采用了专用的硬件平台。目前，市场上的主流防火墙产品不再依靠用户操作系统，而是采用专用的操作系统。应用系统的安全性能是以防火墙自身操作系统的安全性能为基础的，同时，应用系统自身的安全实现也直接影响到整个系统的安全性。在硬件配置方面，提高防火墙的可靠性通常是通过提高防火墙部件的强健性、增大设计阀值和增加冗余部件进行的。

就硬件防火墙运行的操作系统而言，一些安全软件厂商所提供的硬件防火墙通常都是在硬件服务器厂商定制硬件，然后再把 Linux 系统与自己的软件系统嵌入，最终提供安全防御功能的是软件系统，所以不再是真正意义的硬件防火墙。而一些专业硬件防火墙生产商则可以提供与硬件设备配套的专用的操作系统，减少了黑客利用操作系统 BUG 攻击的可能性，如 Cisco 公司的 Pix、ASA、FWSM 等防火墙产品。

■ LAN 端口类型和数量

防火墙的端口虽然不像路由器那样复杂，但也因具体的应用环境不同，所用的接口类型也不一样。主要表现在内部网络接口类型上，防火墙的 LAN 端口类型要符合应用环境的网络连接需求。主要的 LAN 端口类型有以太网、快速以太网、千兆位以太网、ATM 等主流网络类型。在企业局域网中，通常只需要能支持以太网、快速以太网，浸透数新型的防火墙还支持千兆位以太网。

LAN 端口的数量也是设备选型的重要因素。如果企业只有一个网络需要保护，则可选择提供 1 个 LAN 端口的防火墙，而需组建多宿主机模式，则需要选择能提供多个 LAN 端口的防火墙（如 4 个或 4 个以上的 LAN 端口），以实现保护不同内网的目的。

Cisco ASA 5500 系列防火墙可以提供 4 个 10/100/1000 Mbps 的 LAN 端口（如图 11-3 所示），足以满足大中型企业的网络需求。

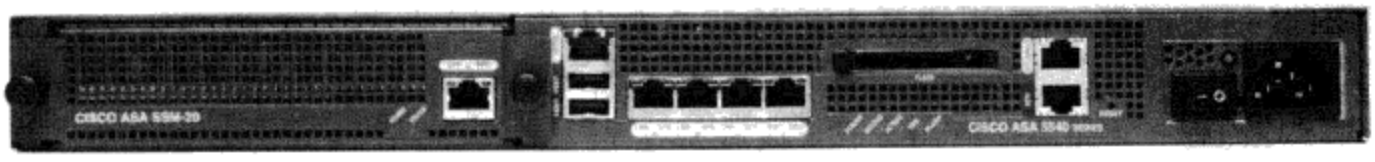


图 11-3　Cisco ASA 5500 防火墙的 LAN 端口

提示 硬件防火墙提供的 LAN 端口类型丰富，或端口数量越多，相应的价格也会越高。

■ 数据处理能力

边缘防火墙位于网络接入 Internet 的干路上，需要对进入网络的所有数据包进行过滤，这就要求防火墙能以最快的速度及时对所有数据包进行检测，否则就可能造成比较大的延时，甚至死机。如果因为防火墙的数据处理能力低，而导致整个网络的 Internet 访问速率下降，显然是每个用户都不愿看到的结果。

就防火墙的工作方式而言，包过滤型防火墙的速度最快，对网络传输性能影响最小，但是，相对于先进的动态包过滤自适应代理防火墙而言，简单的静态包过滤防火墙仍有许多不足，不宜在安全性要求较高的网络中使用。所以，用户应以自身网络的安全需求级别，考虑选择相应工作方式的网络防火墙。

■ NAT 功能

如今几乎所有的网络防火墙都支持 NAT 功能，即可以帮助用户完成内部 IP 地址到公网 IP 地址的转换，从一定程度上发挥接入路由器的功能，如果网络规模不大，完全可以使用边缘防火墙作为 Internet 接入设备。NAT 实现方式有 3 种：静态 NAT（一对一）、动态 NAT（多对多）和端口多路复用 PAT（多对一）。

静态 NAT 是 NAT 最基本的实现形式，可以把内部 IP 地址映射到不同的公网 IP 地址。动态 NAT 是将其他网络上几组不同的 IP 地址映射成内部或公网 IP 地址。如果用户准备把一组 DHCP 作用域映射到另一组 DHCP 作用域，这就需要采用多对多 NAT 寻址。端口多路复用 PAT 则是把多个内部地址转化为一个外部地址（通过端口来区别），这个外部地址可以是定义的只包括一个地址的地址池；也可以是使用外部接口的 IP 地址。

■ 管理方式

尽管网络设备的功能越来越强大，但管理方式却越来越简便。对于网络防火墙而言，为了达到控制或阻止指定类型的网络访问通过，管理员可能会经常配置防火墙规则、设置安全参数、查看防火墙的日志以及调整网络部署等。因此，防火墙的管理最好要适合网管员的管理习惯，如 Telnet、FTP、HTTP、Console、GUI 工具等。GUI 类管理器作为防火墙的管理工具，为网管员提供了有效、直观的管理方式，如图 11-4 所示是使用 Cisco ASDM 管理工具配置 Cisco PIX 防火墙。

在规模较大的网络中，肯能需要部署多个防火墙，此时还需要考虑防火墙是否支持集中管理，通过集成策略集中管理多个防火墙可以大大减轻网络管理负担。另一方面，还要考虑防火墙是否提供基于时间的访问控制以及是否支持 SNMP 监视和配置。

■ 访问控制配置

访问规则是防火墙的一项重要而又基本的功能。在防火墙中的访问规则列表中，不同的防火墙有不同的配置方式，也就体现了不同防火墙系统的安全策略完善程度。一款功能强大的防火墙其访问规则应涵盖所有出入防火墙的数据包的处理方法，对于没有明确定义的数据包，

也应有一个默认处理方法。同时要求过滤规则应易于理解，易于编辑修改，并具备一致性检测机制，防止各条规则间相互冲突，而不起作用。

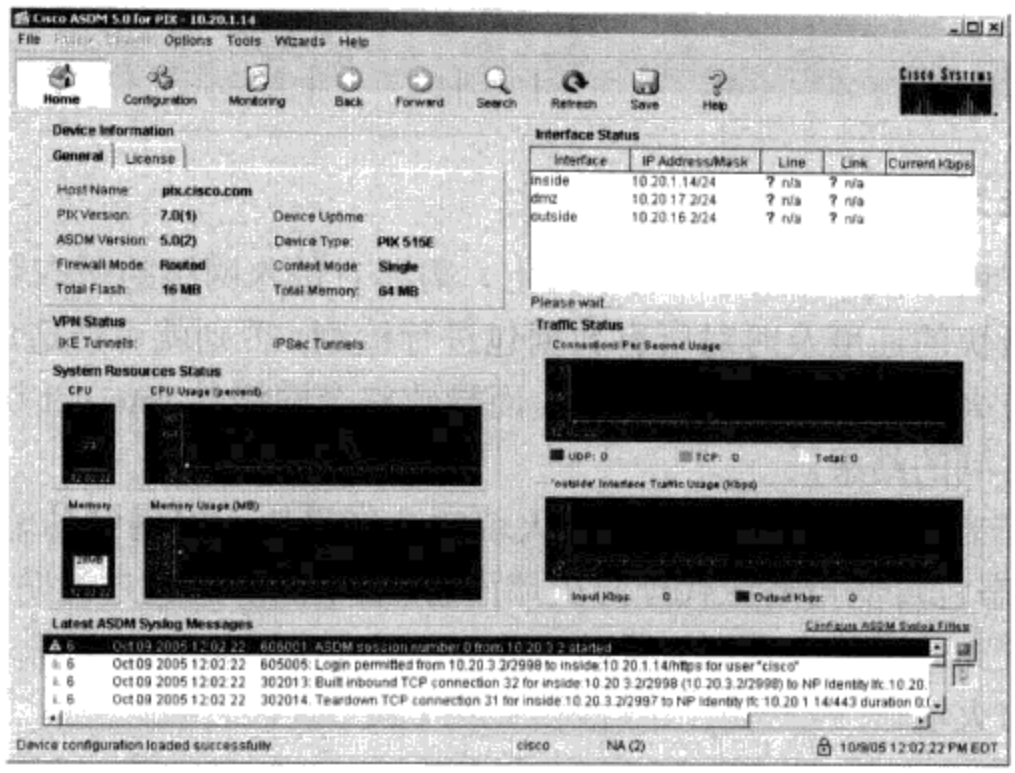


图 11-4 使用 Cisco ASDM 管理工具配置 Cisco PIX 防火墙

防火墙能否在应用层提供代理支持也是非常重要的，如 HTTP、FTP、Telnet、SNMP 代理等，在传输层是否可以提供代理支持，是否支持 FTP 文件类型过滤，允许 FTP 命令防止某些类型文件通过防火墙；在应用级代理方面，是否具有应用层高级代理功能，如 HTTP、POP3。

在安全策略上，防火墙应具有相当的灵活性。首先防火墙的过滤语言应该是灵活的，编程界面对用户是友好的，还应具备若干可能的过滤属性，如源和目的 IP 地址、协议类型、源和目的 TCP/UDP 端口及入出接口等。只有这样用户才能根据实际需求采取灵活的安全策略保护自己企业网络的安全。另外，防火墙除应包含先进的鉴别措施外，还应采用尽量多的先进技术，如包过滤技术、身份识别及验证、信息的保密性保护、信息的完整性校验、系统的访问控制机制、授权管理等技术等，这些都是防火墙安全系统所必须考虑的。

在身份认证支持方面，一般情况下防火墙应具有一个以上认证方案，如 RADIUS、Kerberos、TACACS、TACACS+、口令方式、数字证书等。防火墙能够为本地或远程用户提供经过认证与授权的对网络资源的访问，防火墙管理员必须决定客户以何种方式通过认证。列出防火墙所能支持的认证标准和 CA 互操作性（厂商可以选择自己的认证方案，但应符合相应的国际标准），以及实现的认证协议是否与其他 CA 产品兼容互通。

■ 防御能力

发生网络攻击或黑客入侵时，处于网络边缘的防火墙不免要首当其冲，因此其自身的抗攻击能力也是非常重要的。在网络攻击中，拒绝服务攻击（DoS）是使用频率最高的手段。DoS 就是攻击者过多地占用共享资源，导致设备超载或系统资源耗尽，而使其他用户无法享有服务或没有资源可用。防火墙通过控制、检测与报警等机制，应可有效地防止或抵御黑客的 DoS 攻击。

随着网络技术的不断发展，新的网络入侵手段也不断出现，如基于 ActiveX、Java、Cookies、JavaScript 程序的入侵。防火墙应该能够从 HTTP 页面剥离 Java Applet、ActiveX 等小程序及从

Script、PHP 和 ASP 等代码检测出危险代码或病毒，并向浏览器用户报警。同时，能够过滤用户上载的 CGI、ASP 等程序，当发现危险代码时，向服务器报警。

在提供病毒扫描功能的防火墙中，要验证其扫描的文档类型，如是否会对电子邮件附件中的 DOC 和 ZIP 文件、FTP 中的下载或上载文件内容进行扫描，以发现其中包含的危险信息。

■ 记录和报表功能

为了便于管理员实时了解网络安全状态，边缘防火墙必须能够详细记录网络安全事件信息，并能以报表的形式通知管理员。在防火墙的日志记录和报表功能上，主要考虑以下几个方面：

- 处理完整日志的方法。防火墙应该规定对于符合条件的报文进行日志记录，同时还需提供日志信息管理和存储方法。
- 自动日志扫描。指防火墙是否具有日志的自动分析和扫描功能，对于帮助 管理员进行有效的管理非常重要，通过防火墙的自动分析和扫描功能，管理员可以获得更详细的统计结果，以便管理员有针对性地进行相应方面的完善。
- 警告通知机制。防火墙应提供警告机制，在检测到网络入侵及设备运转异 常情况时，通过警告信息来通知管理员采取必要的措施，警告方式包括 E-mail、状态显示、声音报警、呼叫报警等。
- 简要报表。这是防火墙日志记录的一种输出方式，即可以按照用户 ID 或源/目标 IP 地址排列记录，具有这种功能的防火墙可按管理员要求提供相应的报表分类或打印。
- 实时统计。这也是防火墙日志记录的一种输出方式，通过实时统计状态显示，管理员可及时分析当前网络安全状态，发现和排除安全隐患。实时统计结果通常是以图标的形式显示的。

■ 可扩展性

随着企业的发展，网络规模也会不断扩大，因此，用户在选购网络防火墙时应注意其可扩展性，一边在网络功能升级后仍能继续胜任。在条件允许的情况下，建议用户购买模块化网络防火墙，便于产生新的网络需求时安装相应的业务板卡，而不再购置专用设备。Cisco ASA 5500 系列自适应安全设备均采用模块化设计，支持接口扩展和功能业务扩展，如图 11-5 所示是 Casco ASA 5540 及其对应的扩展模块。

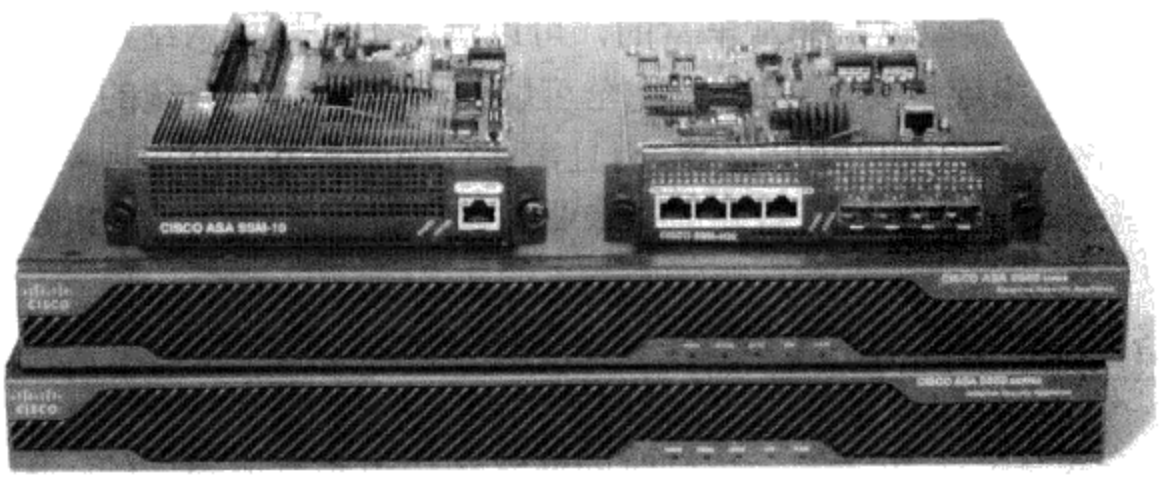


图 11-5　Cisco ASA 5540 的可选扩展模块

■ 协同工作能力

网络防火墙只是企业网络中最基本的网络安全设备，并不是网络安全防护体系的全部。

通常情况下，除部署网络防火墙之外，还需要部署入侵检测系统、入侵防御系统、网络防病毒系统等。这就要求，网络防火墙必须能够与其他安全产品很好的协同工作，才能从根本上保证整个系统的安全。因此，在选购防火墙时通常要注意看它是否支持 OPSEC（开放式安全平台）标准。

■ 品牌和知名度

品牌和知名度可能是决定用户选购方向的重要因素，其实网络防火墙采用的技术和运行机制都具有一定的通用性，所以只需注意不要选购一些杂牌产品即可。目前，国外在防火墙产品的开发、生产中比较著名的品牌有 Cisco、NetScreen、Check Point 等，国内开发、生产防火墙的品牌主要有联想、天网、实达、东软、天融信等。通常情况下，国外品牌的防火墙比国产防火墙要贵一些，但功能更强大，安全性更高，一般适用于大中型企业网络。

3. 代理服务器的选择

如果采用代理服务器作为网络边缘安全设备，则要依据不同的网络规模和需求，选择不同性能的服务器硬件和代理服务器软件。

■ 服务器硬件的选择

看似简单的代理服务器，实则起着极其重要的作用，如实现 Internet 连接共享、服务器发布、VPN 接入、防火墙策略等，因此在选购服务器硬件时应注意如下几个方面。

- 代理服务器承载着整个企业的外部网络访问，为了保障企业用户外网访问的持续性，需要选择具有区别于 PC 的高稳定特性的专业服务器。
- 企业员工都是通过代理服务器来访问外部网络，对于外网资源如网页、软件、图片、文档等资源的访问与本地调用比较频繁的，视网络资源调用的频繁度选择 4GB 或更高的内存。
- 网络资源的访问与调用，都是需要通过服务器下载到本地缓存，然后才能在客户端看到，而所有这些工作都需要代理服务器的大内存来完成网络资源传输的缓冲支持，辅以相对高的处理性能回复响应。

■ 代理服务器软件的选择

代理服务器软件的类型也是非常丰富的，可以满足不同规模网络用户的需求。例如，用户数量较少，而且对网络连接要求较低，则完全可以使用 Windows 系统的 ICS、Sygate、CCproxy 等免费软件，如果网络中的用户数量较多，而且需要代理服务器同时实现网络访问缓存、NAT、VPN、发布内部服务器等功能，则需要选择专业的代理服务器软件，如 Forefront TMG 等。

11.1.3 网络边缘安全配置规划

采用不同安全设备实现边缘安全防御时的网络结构也是有所不同的，因此在部署网络边缘安全之前，应结合内部用户的 Internet 访问需求、接入方式等实际因素，进行合理规划，尽量避免投资浪费。

1. 边缘路由器连接规划

许多路由器产品都拥有防火墙功能，能够起到基本的防火墙作用。也可以通过防火墙功能起到屏蔽内部网络的 IP 地址的功效，使得内部网络用户可以自由设定 IP 地址、通信端口过滤，充分保障网络的安全。此时，当再使用路由器作为接入设备时，则不再需要另外设置安全设备，可直接使用路由器共享接入 Internet，如图 11-6 所示为使用路由器作为共享接入 Internet 的网络拓扑图。

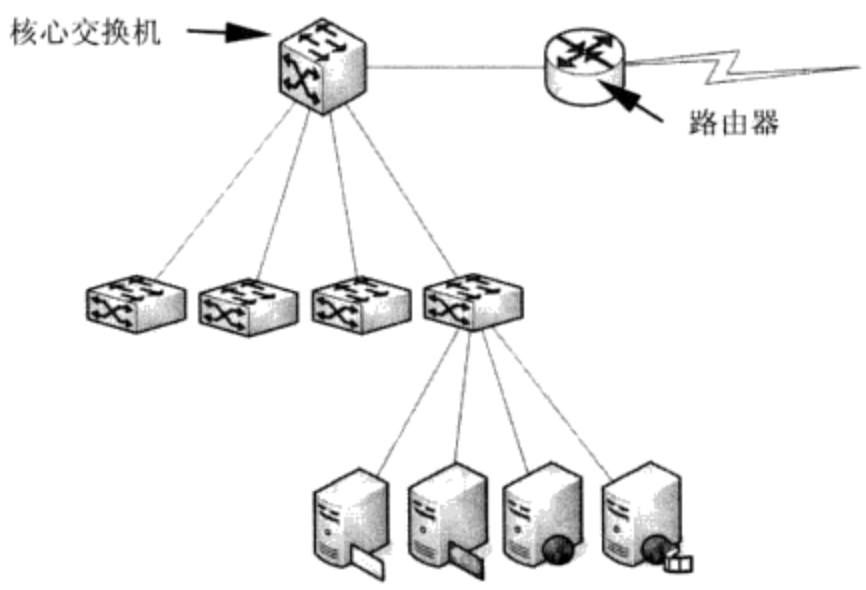


图 11-6　使用路由器共享接入网络拓扑图

因为不同的网络提供商之间的网络通信速度，与同一网络提供商内的速度相差很多，为了能够更加流畅的访问网络，可能会接入不同的网络提供商。使用双链路或者多链路接入 Internet 的方式，可以使用户访问网络更加流畅，也可使网络上的用户访问企业网更加的流量。当使用路由器实现双链路接入时，最少需要 3 个网络接口，一个用于连接局域网，两个连接不同的 ISP，如图 11-7 所示为使用路由器实现双链路 Internet 接入共享的拓扑图。

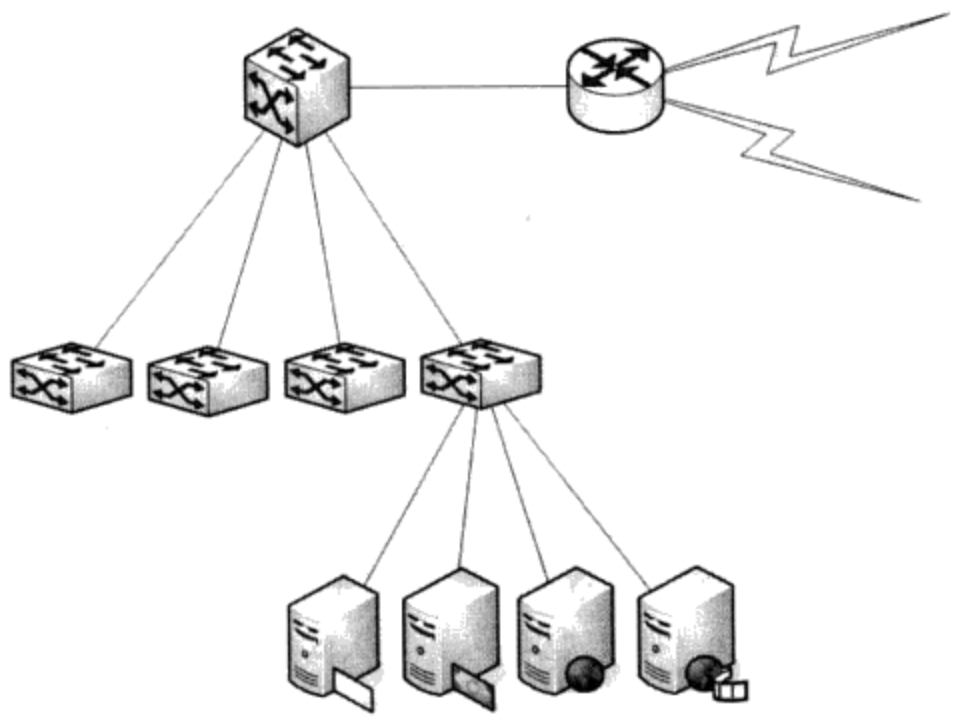


图 11-7　使用路由器实现双链路 Internet 接入共享的拓扑图

在一些大小型网络中，通常会存在比较复杂的网络接入，会将路由器与防火墙等安全设备混合使用。例如，使用路由器使用 Cisco ASA 作为双链路网络的接入设备，而使用路由器作

为 VPN 接入设备，如图 11-8 所示。

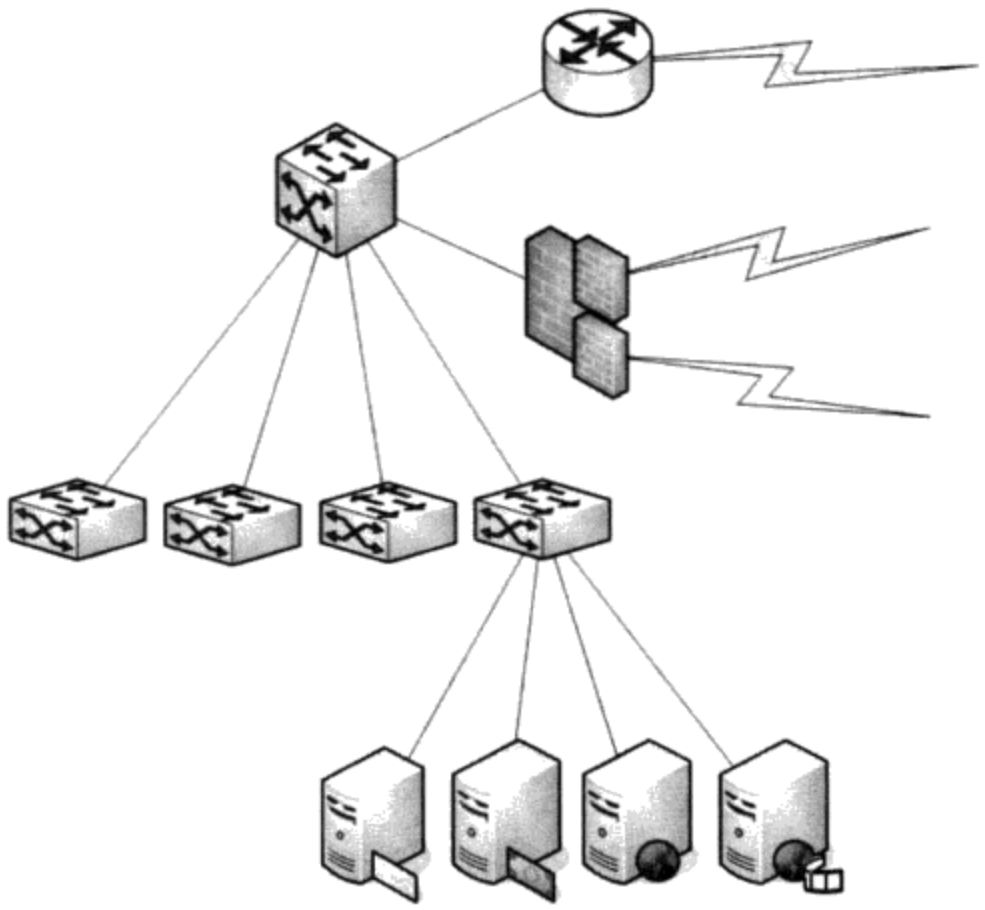


图 11-8　复杂路由器接入

2. 边缘网络防火墙的规划

当使用防火墙作为共享网络接入的设备时，因为网络防火墙同样可以实现路由表的配置、网络地址转换和访问控制列表等配置，因此将不再需要再使用路由器，可以直接使网络防火墙分别连接核心交换机和 Internet，如图 11-9 所示。

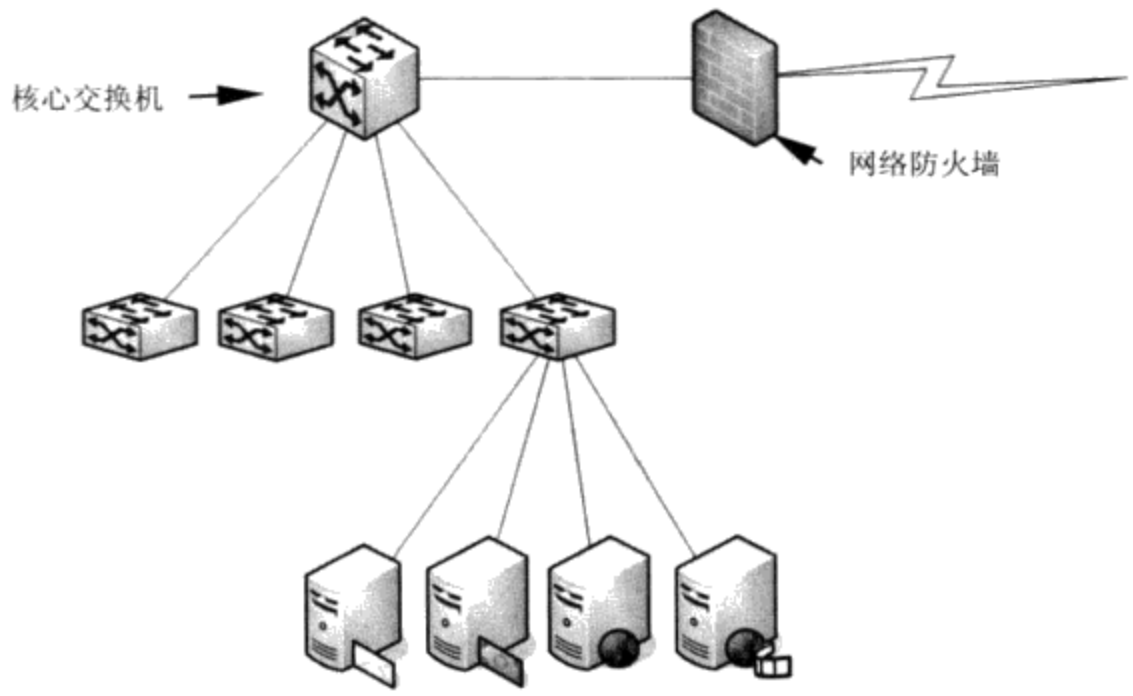


图 11-9　使用网络防火墙接入网络拓扑图

当防火墙只提供一个连接端口时，一般采用如图 11-10 所示的连接方式，即将防火墙直接连接至工作组交换机上即可。

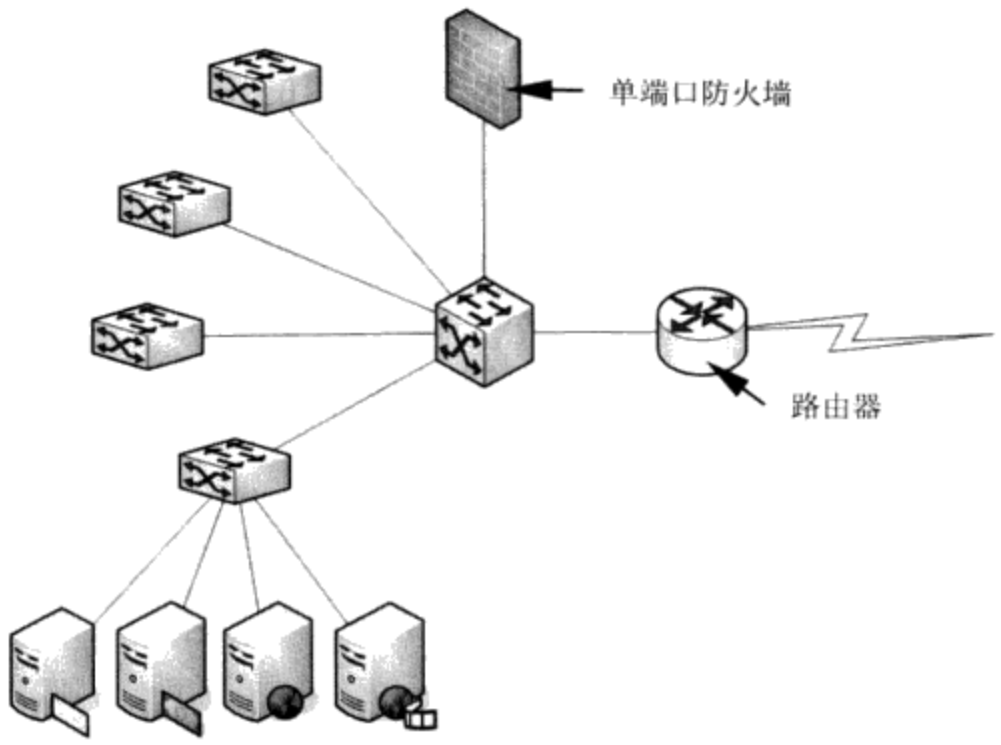


图 11-10　单端口防火墙连接

3. 代理服务器的连接规划

除 Windows Server 2003/2008 本身拥有 NAT 转换模块，可以实现简单的 Internet 连接共享。此外，还有许多专用的代理服务器软件，不仅可以实现 Internet 共享接入，还同时拥有软件防火墙的功能。

> **提示**　对于不同规模的网络所需要的服务器的性能要求也是不相同的，对于大中型网络而言，需要使用专业的服务器作为代理服务器。而对于中小型网络而言，则对代理服务器的性能要求稍低一些，可以使用普通计算机来完成。

如果局域网采用 FTTX 方式接入城域网或 Internet，那么，代理服务器将是性价比最高的 Internet 共享方式。

在使用单链路接入 Internet，并对网络的稳定性要求不是特别高的网络，可以在投入较少资金的前提下，使用单台代理服务器共享接入 Internet。如图 11-11 所示为采用单链路单代理服务器共享 Internet 接入的网络拓扑图。

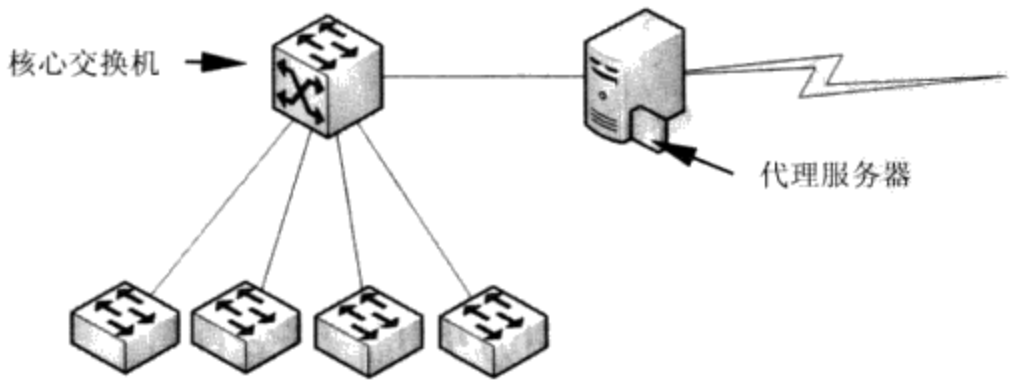


图 11-11　单链路代理服务器

在使用单链路接入 Internet，并对网络的稳定性要求比较高的网络，可以考虑采用代理服务器群集方式保证网络的稳定性。此时，如果其中一台代理服务器发生故障，另一台代理服务

器可立即接管发生故障的服务器的工作。并且在群集内的服务器都完全正常时，还可实现网络负载平衡功能。如图 11-12 所示为单链路群集代理服务器的拓扑图。

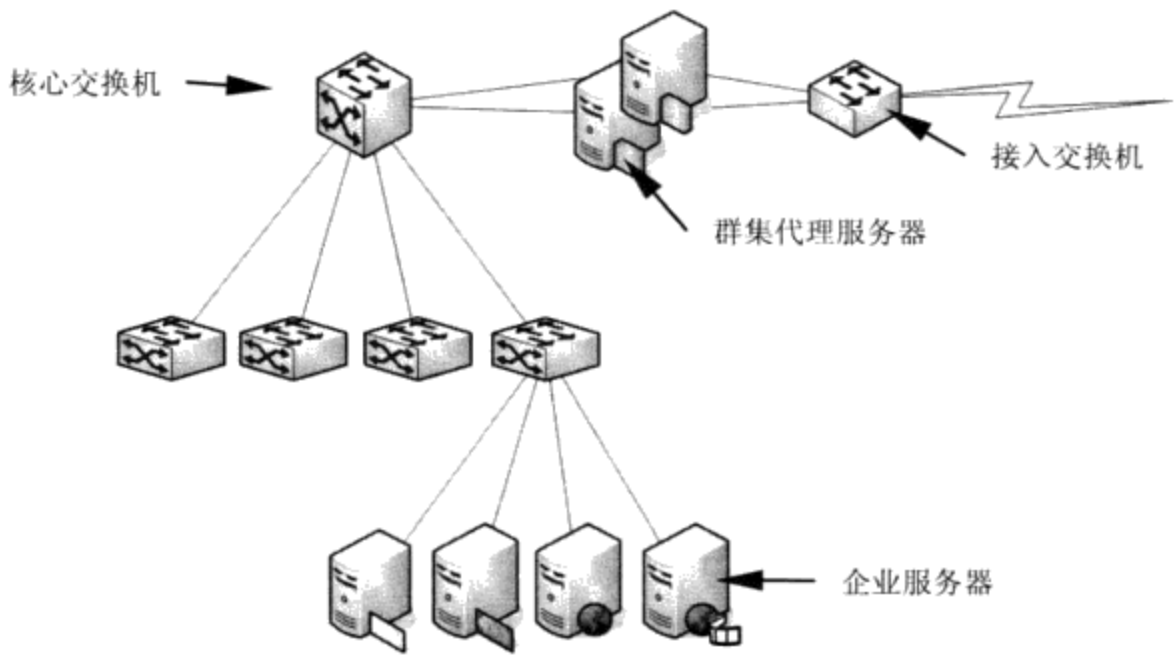


图 11-12　群集代理服务器

另外，现在有很多的网络采用双链路的接入方式，即网络会同样接入不同的电信提供商。此时，则需要为每条接入线路分别设置代理服务器，如图 11-13 所示为采用电信、联通双链路接入 Internet 的网络拓扑图。需要注意的是，为了使局域网内的用户在接入网络时，可以自动识别所应连接的网络，需要在核心交换机上配置相应的访问列表和路由表，具体内容请参见本书的相关内容，这里就不再赘述。

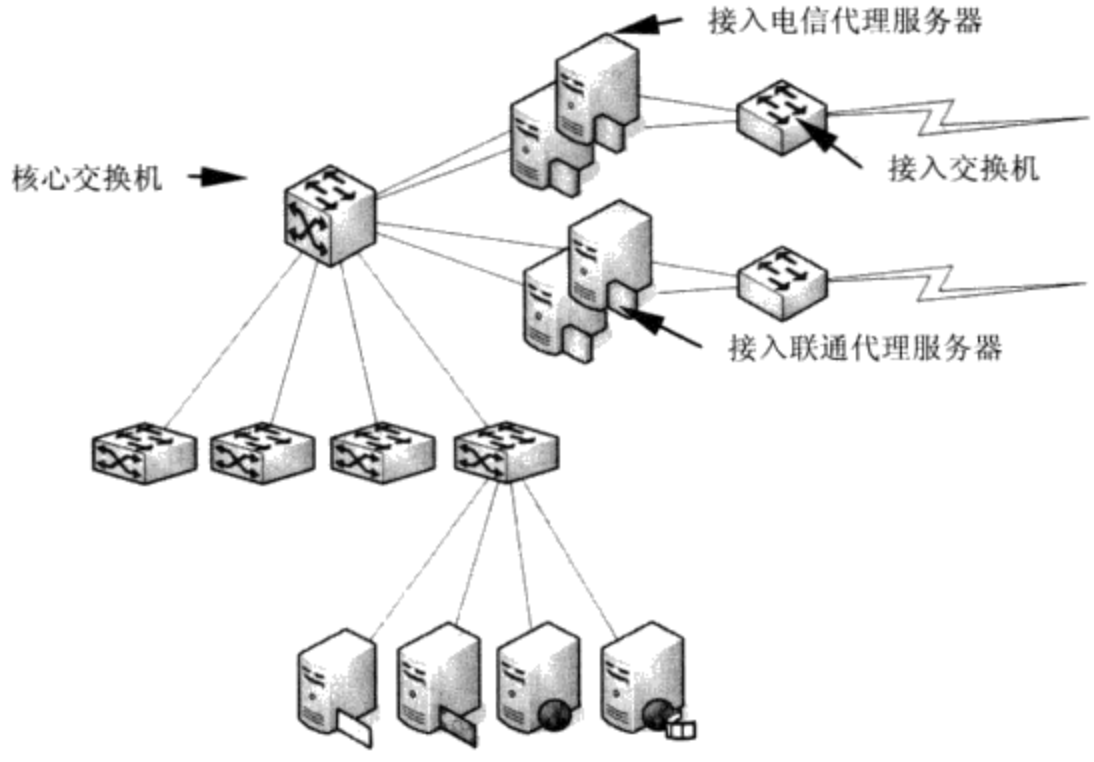


图 11-13　双链路代理服务器

11.2　边缘网络防火墙安全配置

网络防火墙是局域网中最重要的网络安全防护设备，并且随着以太网 Internet 接入方式的逐步普及，在某些环境中已经取代接入路由器的地位。网络防火墙的主要功能就是抵御外来非法用户的入侵，就像是矗立在内部网络和外部网络之间的一道安全屏障。Cisco ASA 5500 系列

自适应安全产品是比较出色的网络防火墙，不仅可以通过 NAT 实现 Internet 接入共享，还可以发布内部服务器、配置 VPN 等。

11.2.1 网络防火墙基本配置

由于网络防火墙默认禁止所有的通信，因此，只有对其进行适当配置后，才能实现正常的网络通信。在初始化设备的过程中，不仅可以使用传统的超级终端方式进行操作，还可以使用思科针对不同的设备提供的管理工具进行相应的初始化操作。

1. 设备初始化

Cisco ASA 5500 系列自适应安全设备为机构的关键信息资产提供了无与伦比的保护，在一个易于部署的平台中集成了最佳防火墙和 VPN 的功能。

ASA 基本配置方法如下：

第 1 步，进入全局配置模式。

```
ciscoasa# configure terminal
```

第 2 步，选择欲作为网络防火墙外部接口的网络接口。

```
ciscoasa(config)# interface interface-id
```

第 3 步，为该接口指定 IP 地址和网掩码。

```
ciscoasa(config-if)# ip address ip-address subnet-mask
```

第 4 步，将该接口指定为外部接口。

```
ciscoasa(config-if)# nameif outside
INFO: Security level for "outside" set to 0 by default.
```

第 5 步，激活该外部接口。

```
ciscoasa(config-if)# no shutdown
```

第 6 步，返回至全局配置模式。

```
ciscoasa(config-if)# exit
```

第 7 步，选择欲作为网络防火墙内部接口的网络接口。

```
ciscoasa(config)# interface interface-id
```

第 8 步，为该接口指定 IP 地址和网掩码。

```
ciscoasa(config-if)# ip address ip-address subnet-mask
```

第 9 步，将该接口指定为内部接口。

```
ciscoasa(config-if)# nameif inside
INFO: Security level for "inside" set to 100 by default.
```

第10步，激活该外部接口。

```
ciscoasa(config-if)# no shutdown
```

第11步，返回至全局配置模式。

```
ciscoasa(config-if)# exit
```

第12步，启用Web VPN。

```
ciscoasa(config)# webvpn
```

第13步，允许VPN对外访问。

```
ciscoasa(config-webvpn)# enable outside
```

第14步，指定SSL VPN客户端（SSL VPN Client，SVC）文件位置。

```
ciscoasa(config-webvpn)# svc image disk0:/sslclient-win-1.1.2.169.pkg
```

第15步，使安全设备能够将SVC文件下载到远程计算机。

```
ciscoasa(config-webvpn)# svc enable
```

第16步，返回至全局配置模式。

```
ciscoasa(config-webvpn)# end
```

第17步，保存配置。

```
ciscoasa# copy startup-config running-config
```

2. 配置接口地址

Cisco ASA默认会集成多个接口，用于连接Internet和局域网，在安全设备进行初始化操作时，通常会对当前所要使用的接口进行配置，例如IP地址信息等。当接口发生变化，需要修改IP地址信息时，则需要重新配置接口地址。

第1步，使用ASDM登录Cisco ASA，在窗口任务栏中单击“Configuration”，并在左侧栏中依次选择“Device Setup”→“Interfaces”，在右侧窗口中即可显示当前Cisco ASA的接口配置情况，如图11-14所示。

第2步，在接口列表中，选择所要配置的接口，单击“Edit”按钮，显示如图11-15所示“Edit Interface”对话框。默认显示“General”选项卡，根据需要配置接口名称（Interface Name）、安全级别（Security Level）和IP地址信息（IP Address）等。如果选中“Enable Interface”复选框，则可以在配置完成后，立即启用接口。切换到“Advanced”选项卡，可以配置其他高级选项，例如MTU等。

第3步，单击“OK”按钮，确认配置，并将配置发送到安全设备，此时，该配置即可生效。使用相同操作，可以配置其他接口。如果在Cisco ASA主窗口中，单击“Save”按钮，可以将配置保存到安全设备的NVRAM中。

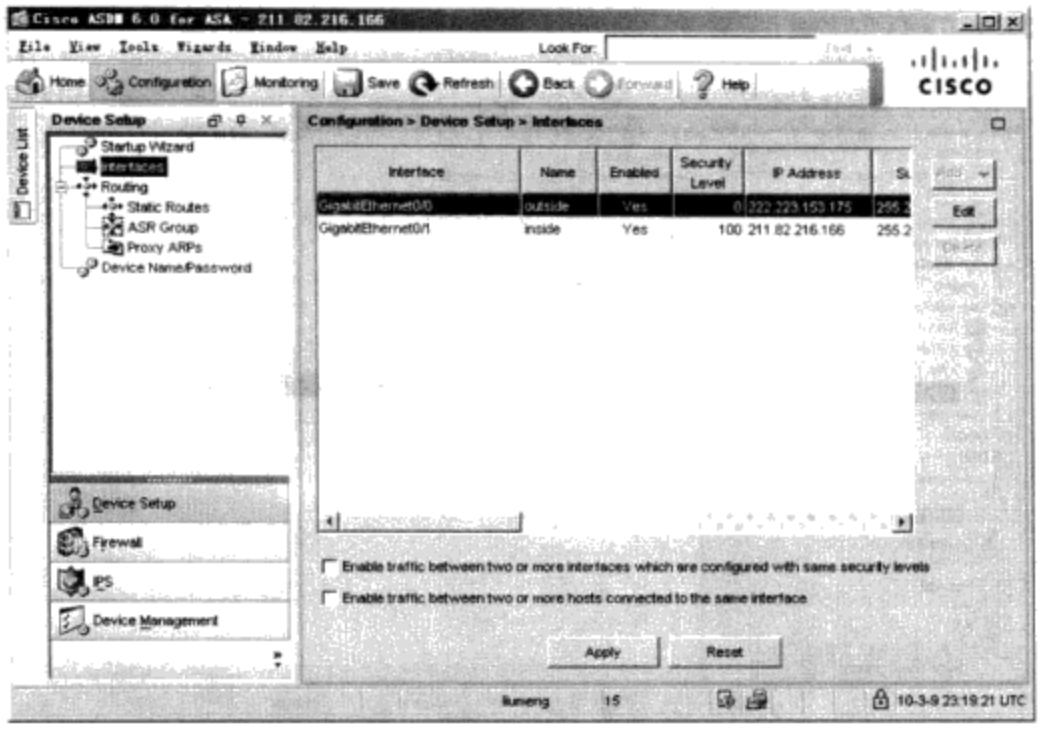


图 11-14　配置接口

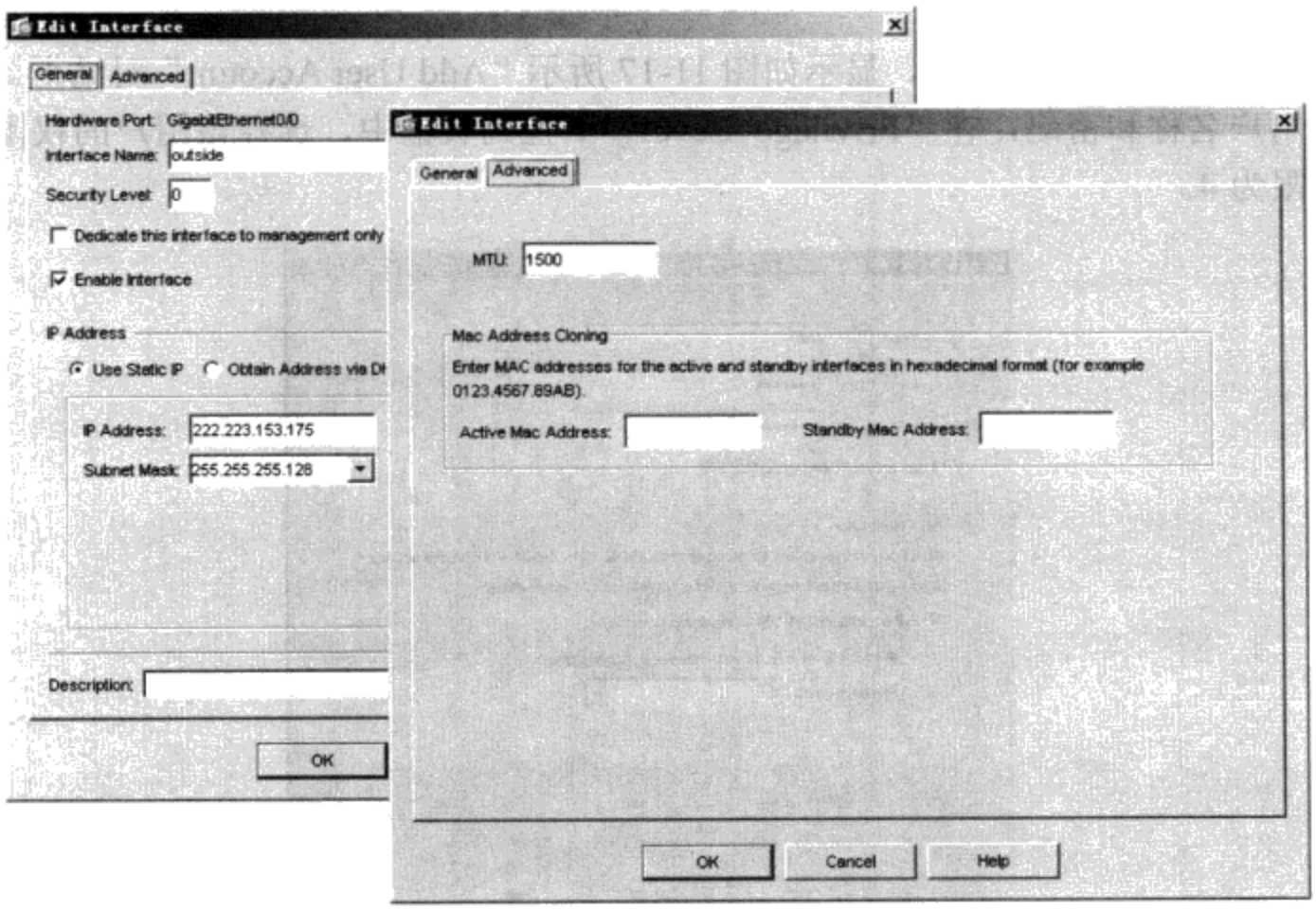


图 11-15　“Edit Interface”对话框

3. 创建用户

默认情况下，安全设备拥有一个管理员用户，并且在初始化安全设备时，也可以创建用户。但这些并不能满足网络管理的需求，尤其是网络中存在多个管理员，并且各管理员承担不同的管理任务时，则需要为每个管理员创建不同权限的管理员账户。

第 1 步，使用 ASDM 登录 Cisco ASA，在窗口任务栏中单击“Configuration”按钮，并在左侧栏中依次选择“Device Management”→“User Accounts”，在右侧窗口中即可显示当前所有用户的配置情况，如图 11-16 所示。

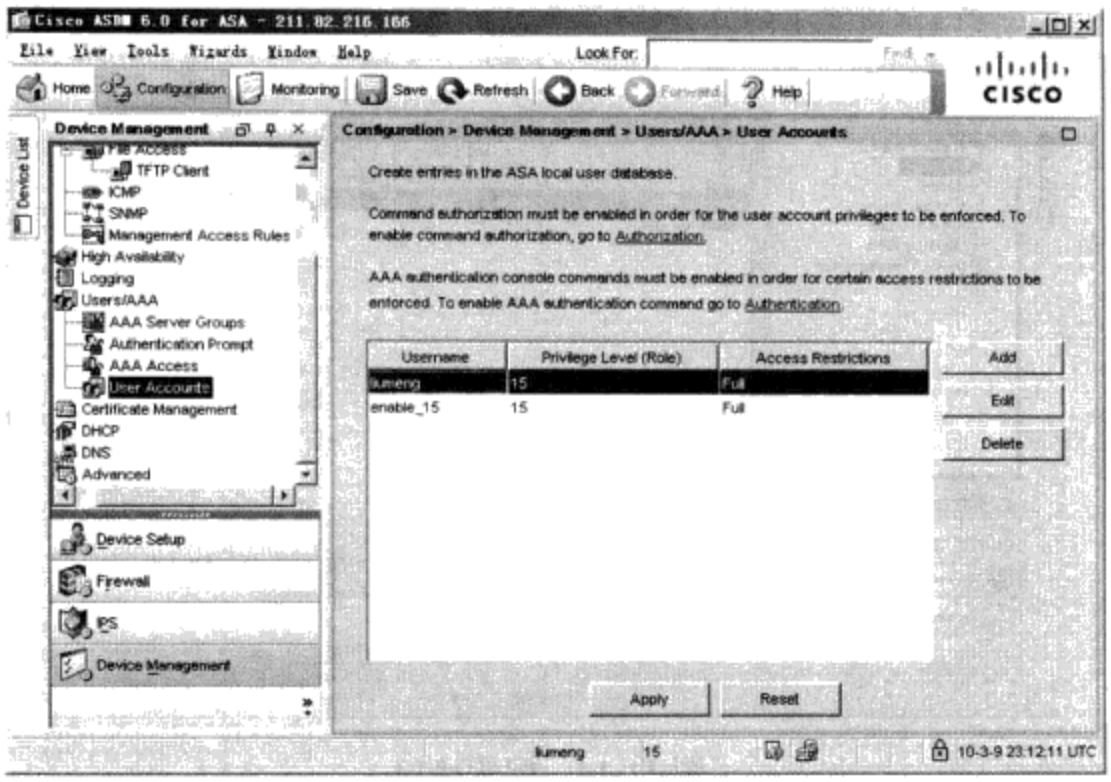


图 11-16　配置用户

第 2 步，单击“Add”按钮，显示如图 11-17 所示“Add User Account”对话框。根据需要分别键入用户名称和密码，在“Privilege Level”下拉列表框中，选择该用户的权限，这里设置用户权限为 4。

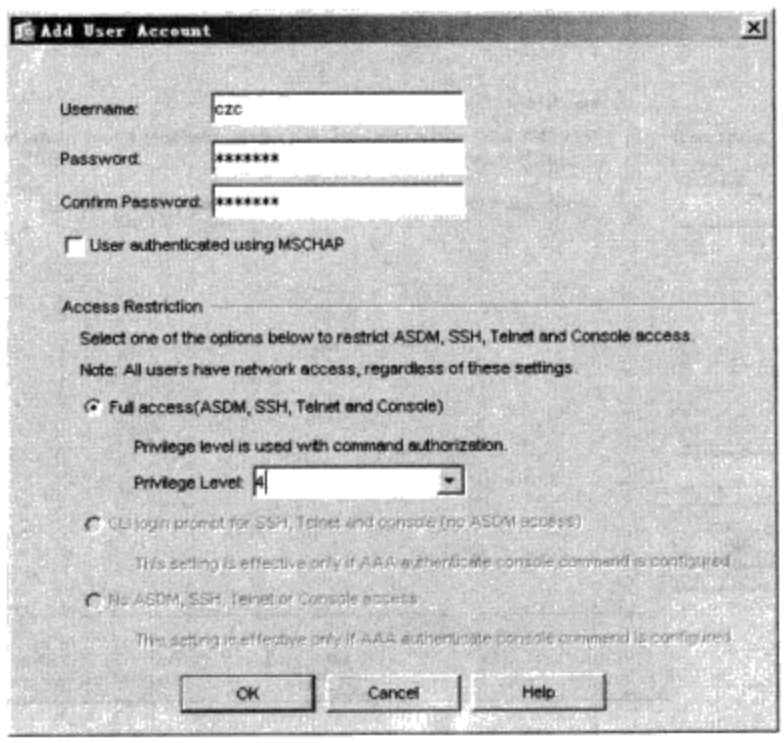


图 11-17　“Add User Account”对话框

第 3 步，单击“OK”按钮，确认并发送配置到安全设备。重复操作，可创建多个用户。

4. 配置 ASDM 访问的地址

默认情况下，Cisco ASA 允许局域网内的所有计算机使用 ASDM 访问，这无疑降低了设备的安全性，因此，推荐的做法是只允许管理员所在的 Vlan 对安全设备进行配置和管理，这里将修改默认条目。

第 1 步，依次选择“Configuration”→“Device Management”→“ASDM/HTTPS”，在右侧窗口中，选中默认允许访问条目，如图 11-18 所示。

第 2 步，单击“Edit”按钮，显示如图 11-19 所示“Edit HTTP Configuration”对话框。在“Interface Name”下拉列表框中，选择允许接入的接口。在“IP Address”文本框中，键入允许访问的网络号。在“Mask”下拉列表框中，选择该网络号所使用的子网拔码。

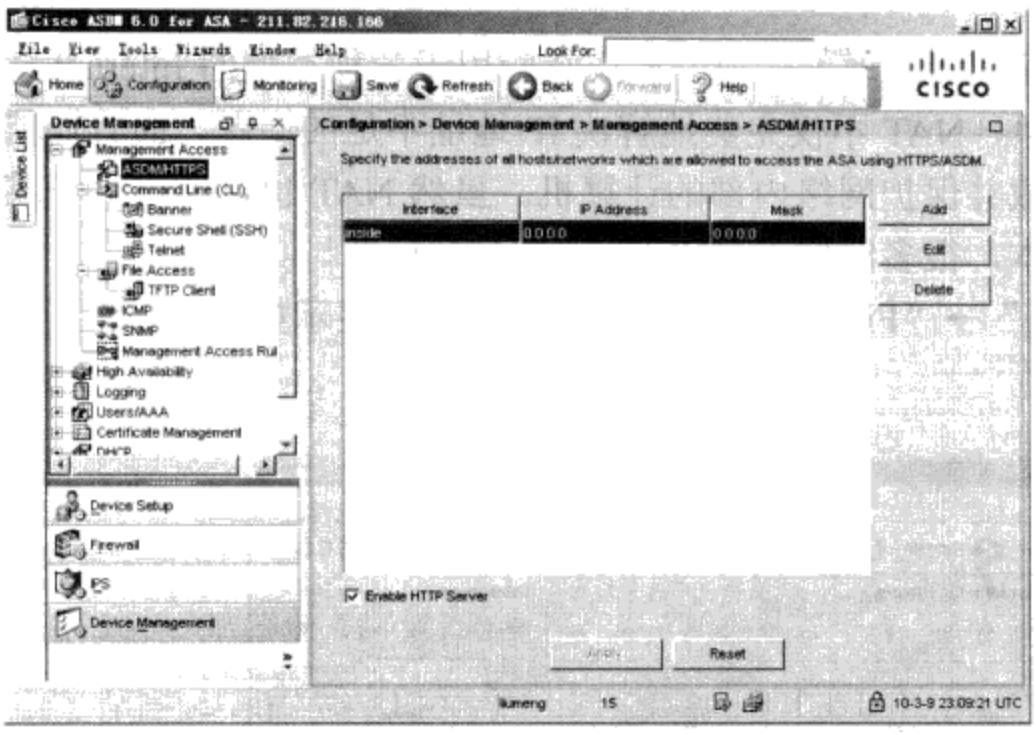


图 11-18　配置 ASDM 访问的地址

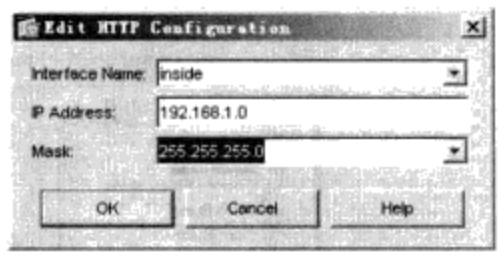


图 11-19　“Edit HTTP Configuration”对话框

第 3 步，依次单击“OK”、“Apply”按钮，确认并发送配置到设置即可。

5. 配置 Telnet 访问地址

与允许 ASDM 访问设备相同，对于 Telnet 方式，同样需要限制访问的 IP 地址。

第 1 步，依次选择“Configuration”→“Device Management”→“Telnet”，在右侧窗口中，选中默认允许访问条目，如图 11-20 所示。

第 2 步，单击“Edit”按钮，显示如图 11-21 所示“Edit Telnet Configuration”对话框。在“Interface Name”下拉列表框中，选择允许接入的接口。在“IP Address”文本框中，键入允许访问的网络号。在“Mask”下拉列表框中，选择该网络号所使用的子网拔码。

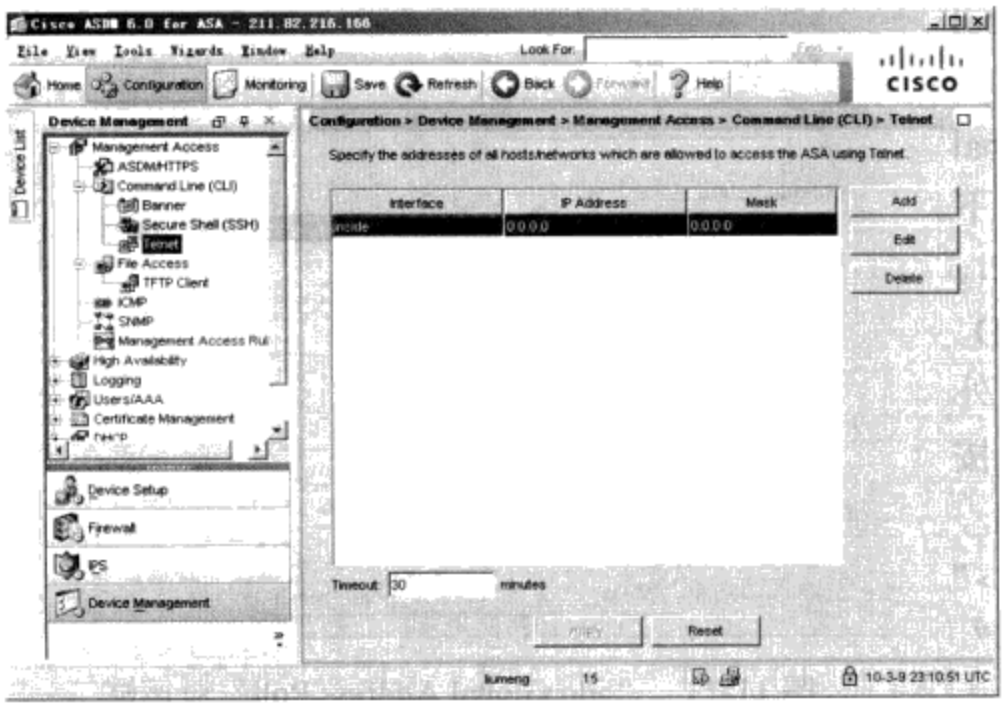


图 11-20　配置 Telnet

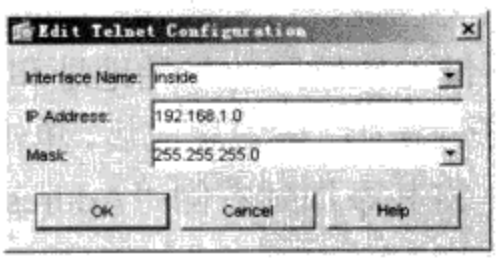


图 11-21　“Edit Telnet Configuration”对话框

第3步，依次单击“OK”、“Apply”按钮，确认并发送配置到设置即可。

11.2.2 配置NAT地址转换

NAT（Network Address Translation，网络地址转换）被广泛应用于各种类型的Internet接入方式和各种类型的网络。原因很简单，NAT不仅完美地解决IP地址不足的问题，而且还能有效地避免来自网络外部的攻击，隐藏并保护网络内部的计算机。虽然NAT也可以借助于某些代理服务器实现，但考虑到运行成本，很多时候都是在路由器上实现。

第1步，依次选择“Configuration”→“Firewall”→“NAT Rules”，显示如图11-22所示“NAT Rules”窗口。

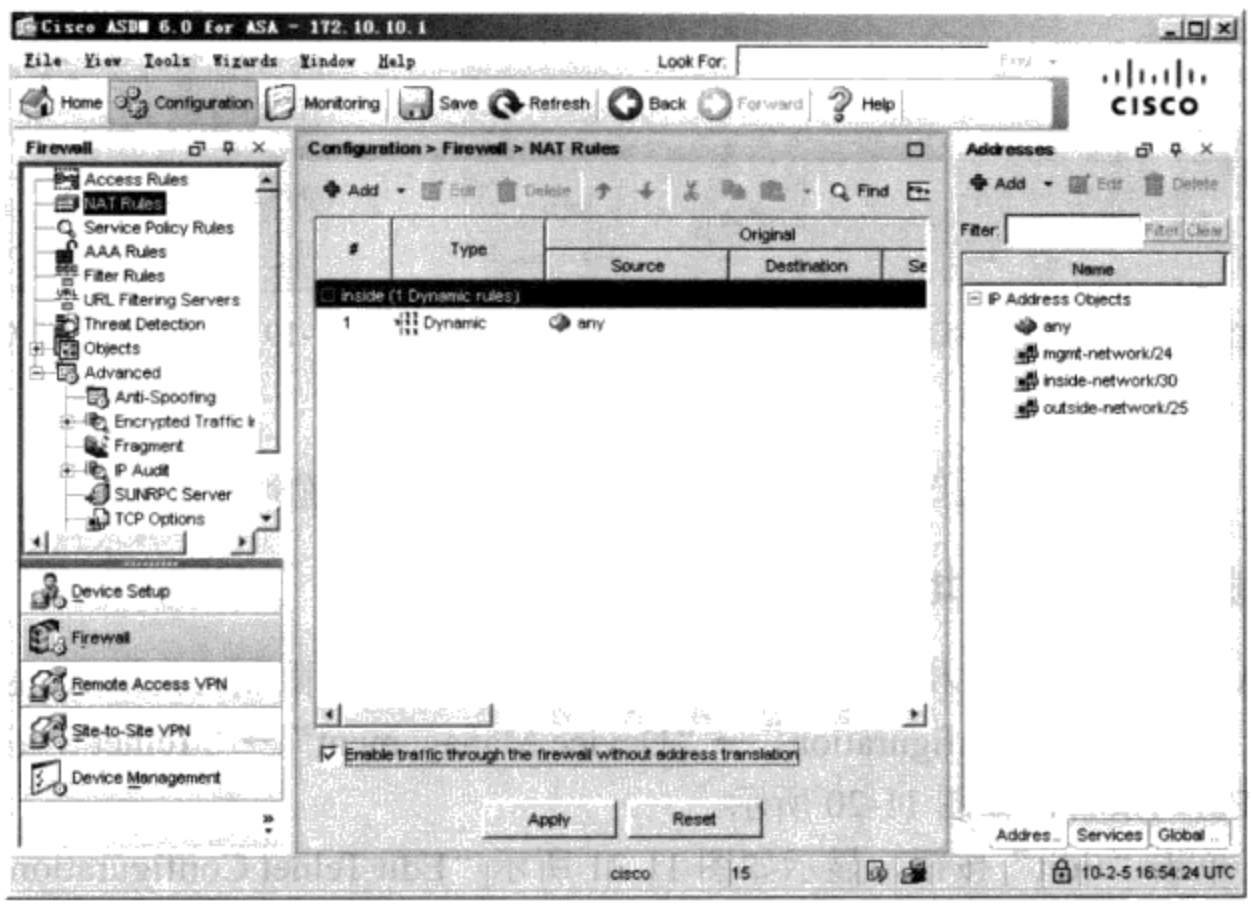


图11-22 “NAT Rules”窗口

第2步，在右侧栏的下方，打开“Global Pools”选项卡，然后在该栏上方单击“Add”按钮，显示如图11-23所示“Add Global Address Pool”对话框。在“Interface”下拉列表框中，选择连接ISP提供商的接口。在“Pool ID”文本框中，键入该地址的ID。因为这里需要将局域网地址转换为多个外网地址，因此，这里选择“Range”单选按钮，并键入地址段的起始地址和结束地址，以及子网掩码。设置完成后，单击“Add>>”按钮，将其添加到右侧“Addresses Pool”列表框中。

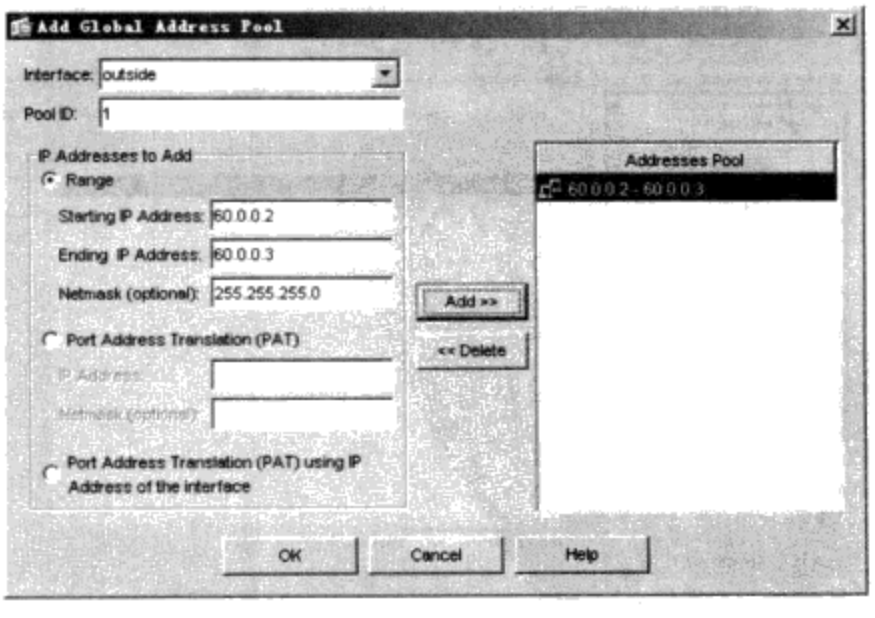


图11-23 “add Global Address Poll”对话框

第3步，单击“OK”按钮，确认配置并发送到设备，如图11-24所示。

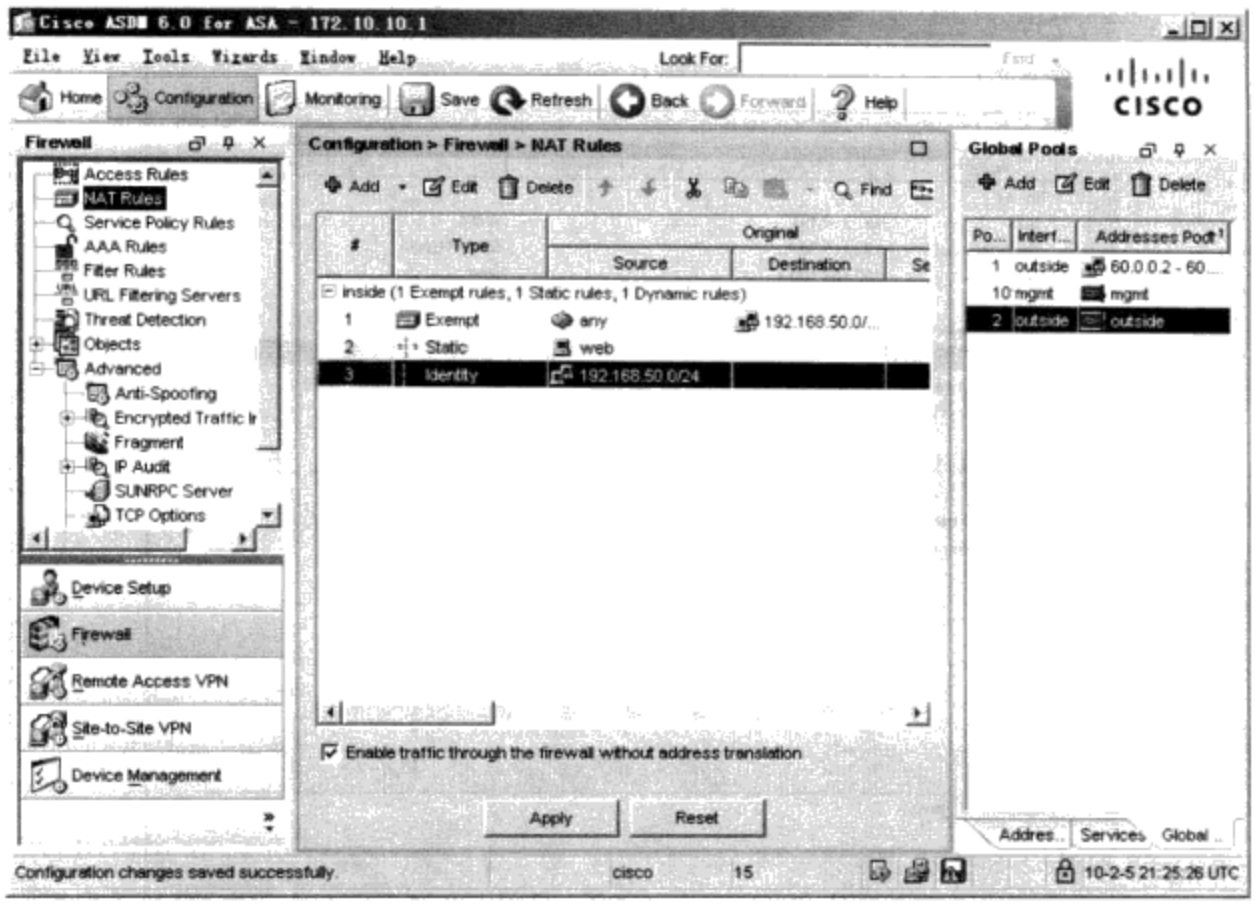


图 11-24　完成地址池的配置

第 4 步，在窗口中间栏的“Add”列表框中，选择“Add Dynamic NAT Rule...”选项，显示如图 11-25 所示“Add Dynamic NAT Rule”对话框。在“Interface”下拉列表框中，选择连接局域网的接口。

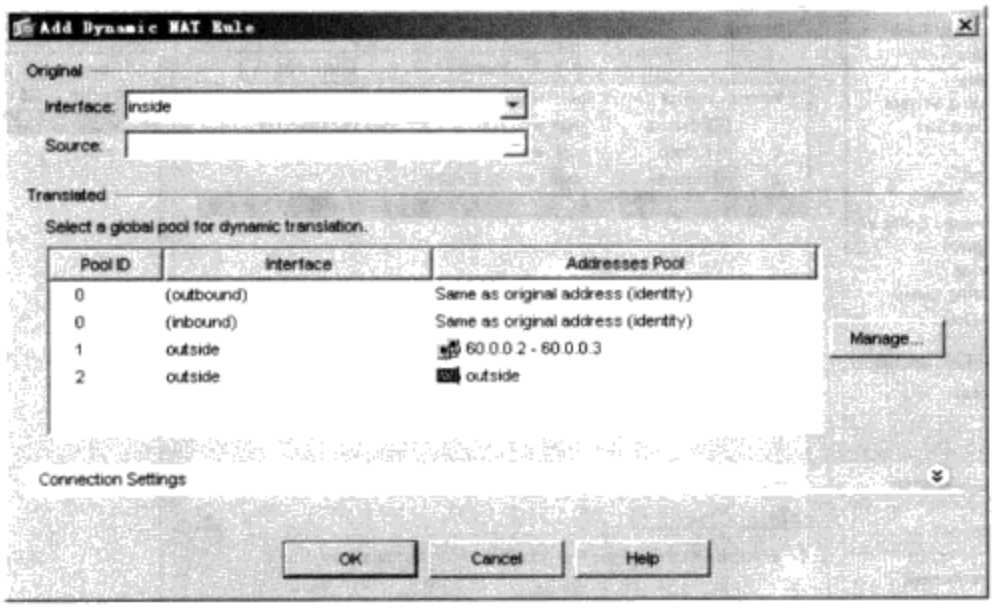


图 11-25　“Add Dynamic NAT Rule”对话框

第 5 步，单击“Source”右侧的…按钮，显示如图 11-26 所示“Browse Source”对话框，在“IP Address Objects”列表框中，选择“any”选项，即允许所有的数据通过。

第 6 步，单击“确定”按钮，返回“Add Dynamic NAT Rule”对话框，再单击“OK”按钮，确认并发送配置到设备即可，如图 11-27 所示。此时，局域网内的计算机即可通过该设备连接 Internet。

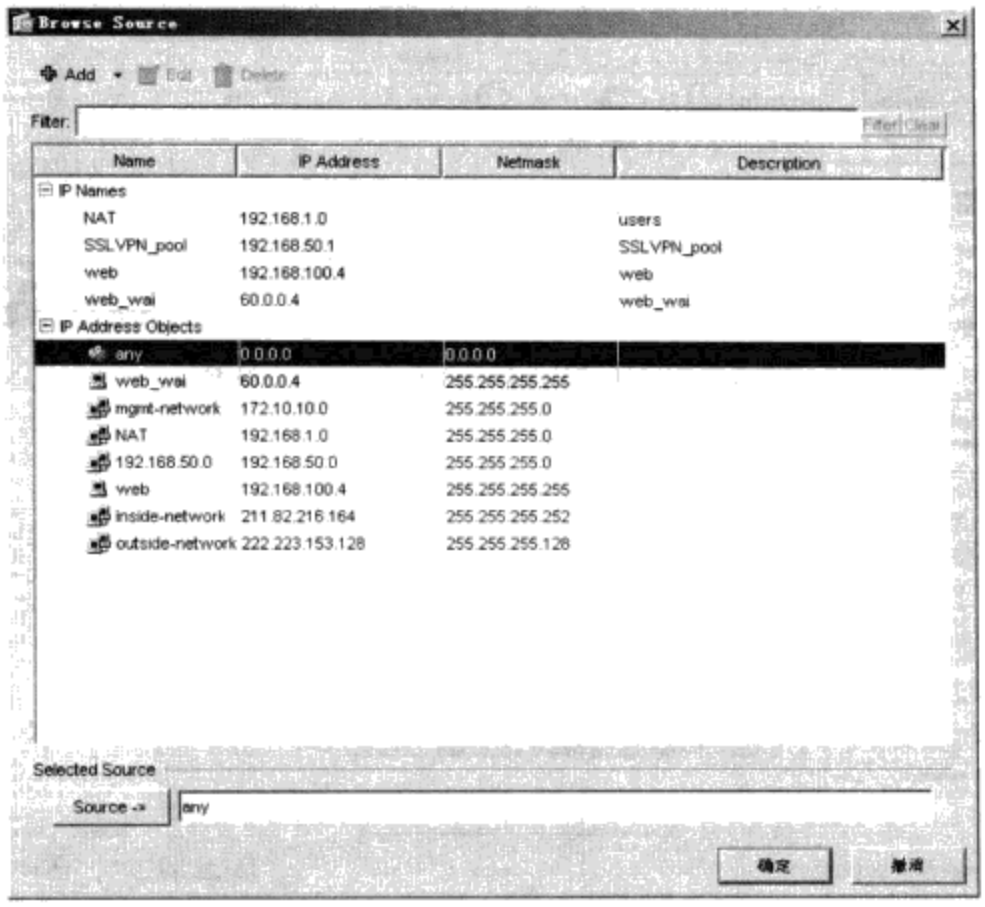


图 11-26 “Browse Source”对话框

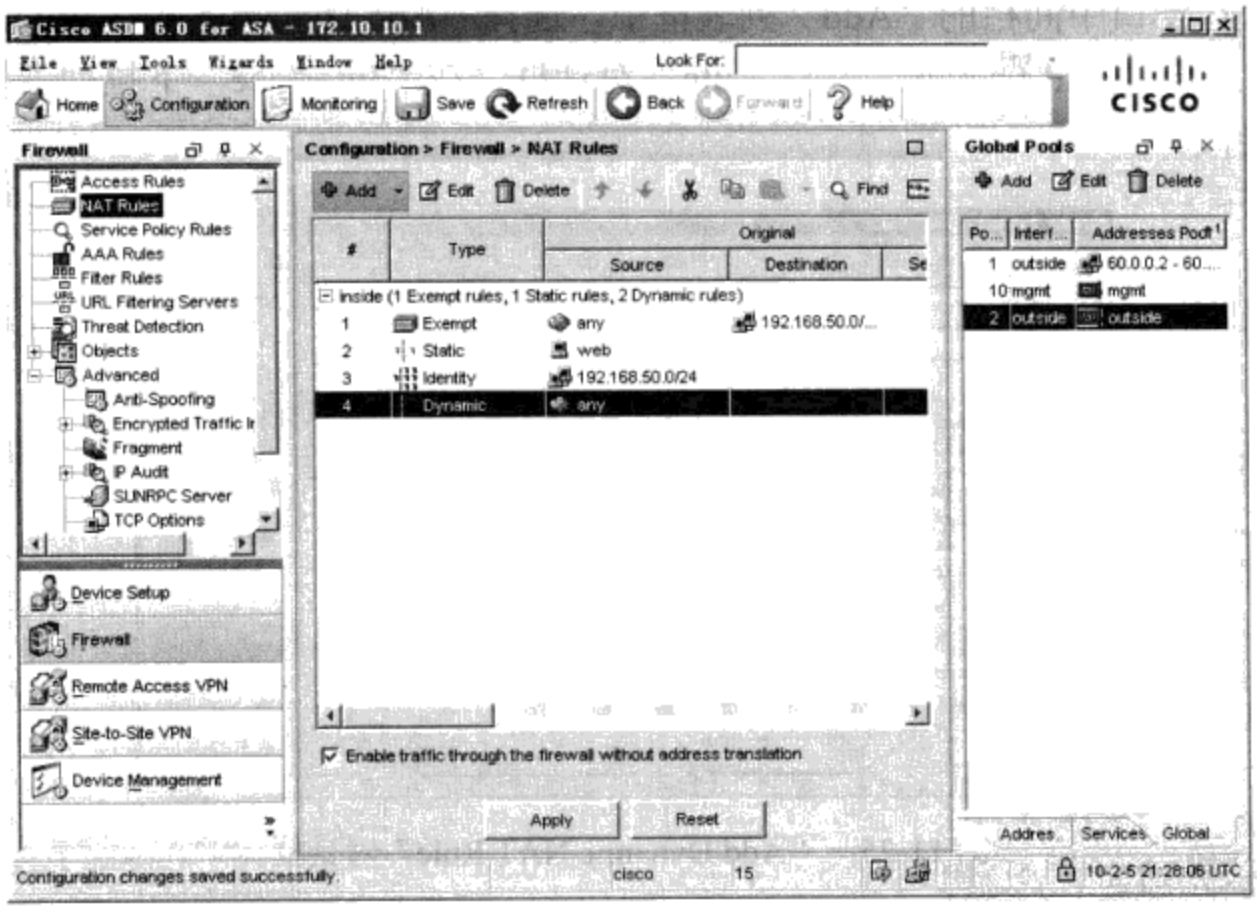


图 11-27 完成 NAT 配置

11.2.3 配置远程访问 SSL VPN 服务

基于 Cisco ASA 5500 安全产品的 VPN 连接方案，使用户不需要降低企业网络安全策略的完整性，即可实现远程安全接入。由于 Cisco ASA 5500 将安全套接字层（SSL）和 IP Security（IPSec）VPN 服务与全面威胁防御技术有机地结合在一起，因此，它不但能按照各种部署环境的要求提供高度定制的网络接入，还能提供高级端点和网络层安全性。

1. 网络连接规划

使用 Cisco ASA 作为 VPN 接入设备时的网络连接示意图如图 11-28 所示。目前，使用安全设备作为局域网 Internet 接入设备已经成为最常用的连接方式之一，Cisco ASA 同时提供接入功能，但是 ASA 不能同时用作 Internet 接入设备和 VPN 接入设备，所以需要在网络边缘同时部署分别用于 Internet 接入和 VPN 接入的 Cisco ASA，或者使用路由器作为 Internet 接入设备。VPN 客户端可以通过 Internet 或其他公用网络，实现与公司网络的安全连接。

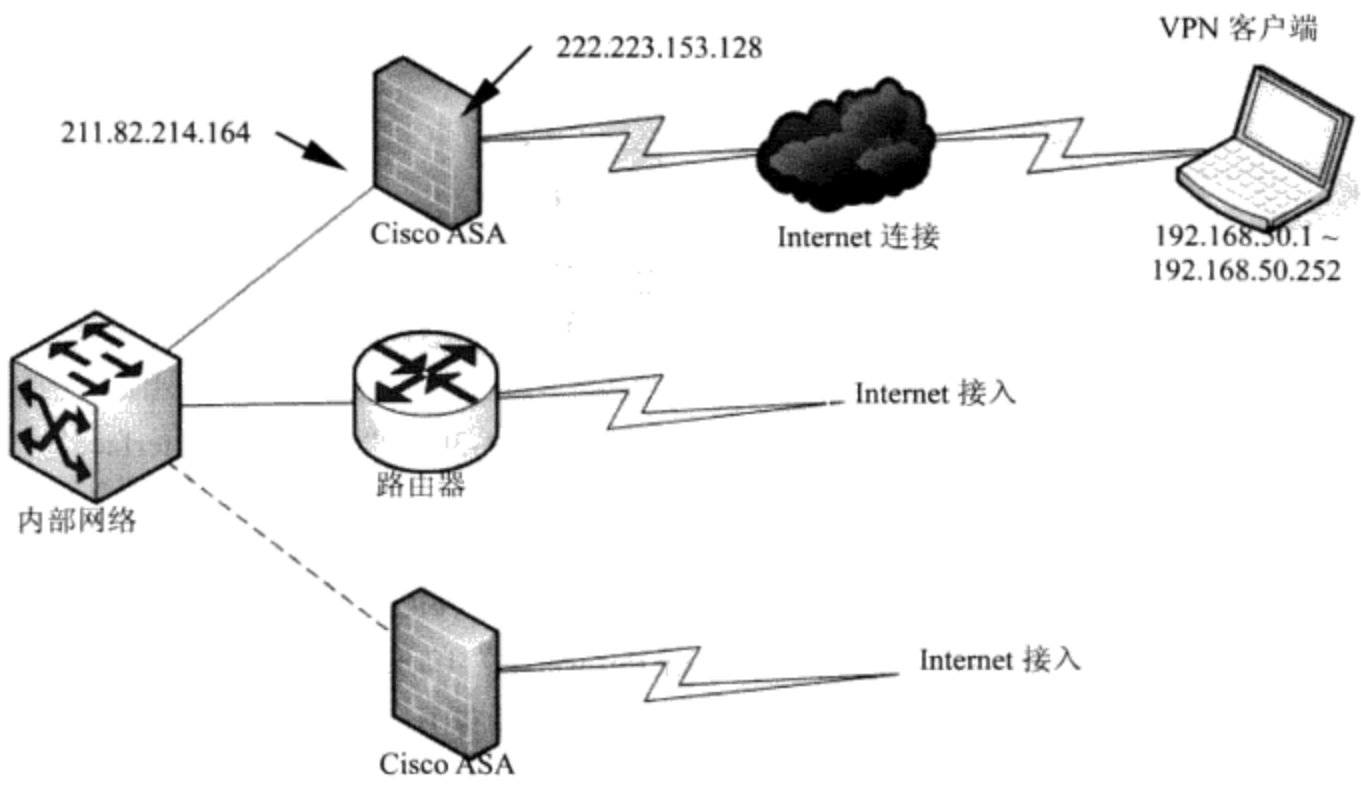


图 11-28 在 Cisco ASA 上配置远程访问 VPN

用作远程访问 VPN 服务器 Cisco ASA 外部接口 IP 地址为 222.223.153.128，内部接口 211.82.214.164，为 VPN 客户端创建的 IP 地址范围 192.168.50.1~192.168.50.252，客户端使用 ASA 上创建的本地用户账户和密码访问 VPN 服务器。

在配置 IPSec VPN 远程访问之前，确认已经准备好以下信息：

- IPSec VPN 远程客户端使用的 IP 地址池。
- 在本地认证数据库中创建用户列表，或者使用 AAA 服务器实现认证。

当 VPN 连接时，远程客户端使用的网络信息，包括：

- 主 DNS 服务器和辅助 DNS 服务器的 IP 地址。
- 默认域名。
- 认证远程客户端可访问的本地主机、组和网络的 IP 地址列表。

2. 运行 SSL VPN 配置向导

第 1 步，SSL VPN 配置向导的启动方式与启动向导类似，打开“Remote Access VPN”对话框，并在“Wizard”菜单栏中选择“SSL VPN Wizard...”命令，显示如图 11-29 所示“SSL VPN Connection Type”对话框。系统默认选中“Clientless SSL VPN Access”复选框，即只为通过基于浏览器（Windows 内置客户端）访问 VPN 的客户端启用 SSL 加密传输。如果网络中存在使用 Cisco 专用客户端（AnyConnect VPN Client）的用户，建议同时选中“Cisco SSL VPN Client”

复选框。

第2步，单击“Next”按钮，显示如图11-30所示“SSL VPN Interface”对话框，在“Connection Name”文本框中输入VPN连接名称，在“SSL VPN Interface”下拉列表框中选择“outside”，即用户访问此VPN时使用的接口。

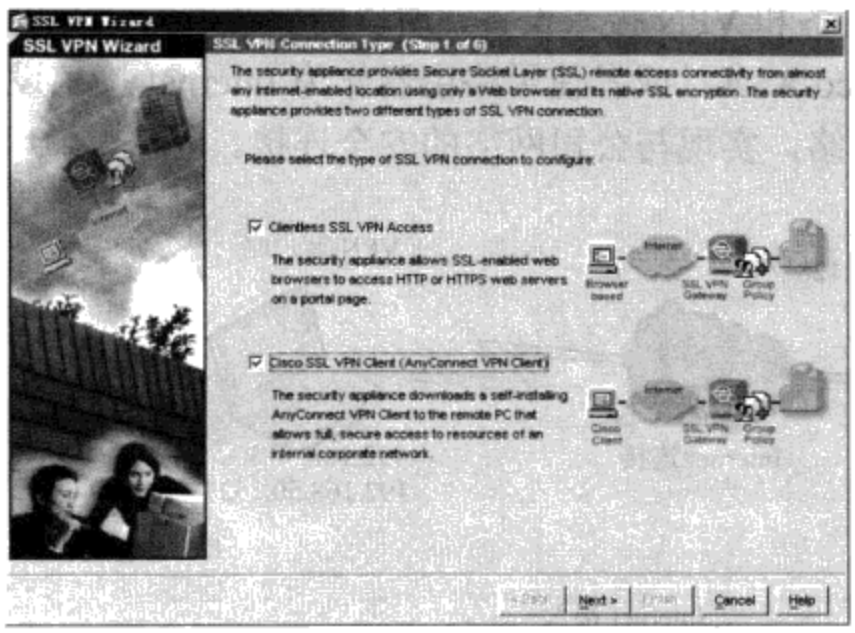


图11-29 “SSL VPN Connection Type”对话框

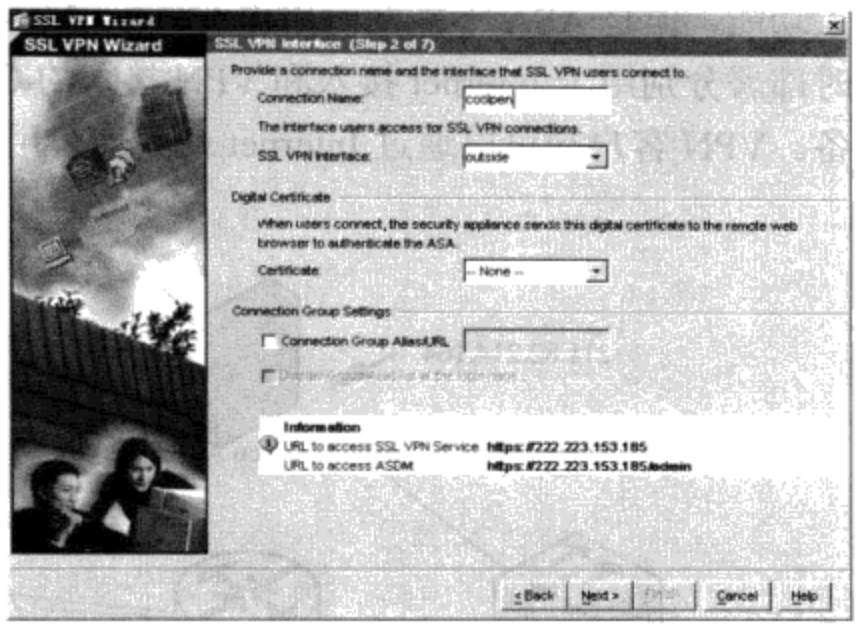


图11-30 “SSL VPN Interface”对话框

第3步，单击“Next”按钮，显示如图11-31所示“User Authentication”对话框，系统默认选择“Authenticate using a AAA server group”单选按钮，即使用AAA服务器验证来访用户身份。如果选择“Authenticate using the local user database”单选按钮，即使用本地用户账户数据库验证，则既可以在这里创建新用户账号，也可以稍候使用ASDM配置界面添加用户。在“Username”、“Password”和“Confirm Password”中分别输入用户名、密码、确认密码，单击“Add”按钮，即可向本地用户数据库中添加新的用户。重复操作，可添加多个用户。

第4步，单击“Next”按钮，在“Group Policy”对话框中，选择“Create new group policy”单选按钮，并在对应文本框中输入名称，即可创建新的组策略。单击“Next”按钮，在“Clientless Connections Only - Bookmark list”对话框中，设置VPN客户端访问页面中的链接列表，即用户登录VPN后可以快速访问的Web站点或网络资源，如图11-32所示。

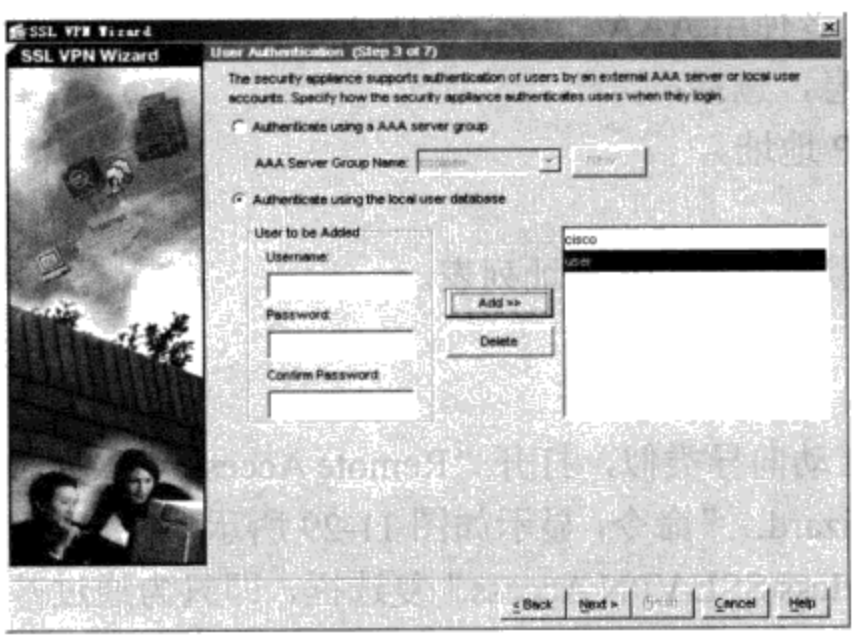


图11-31 “User Authentication”对话框

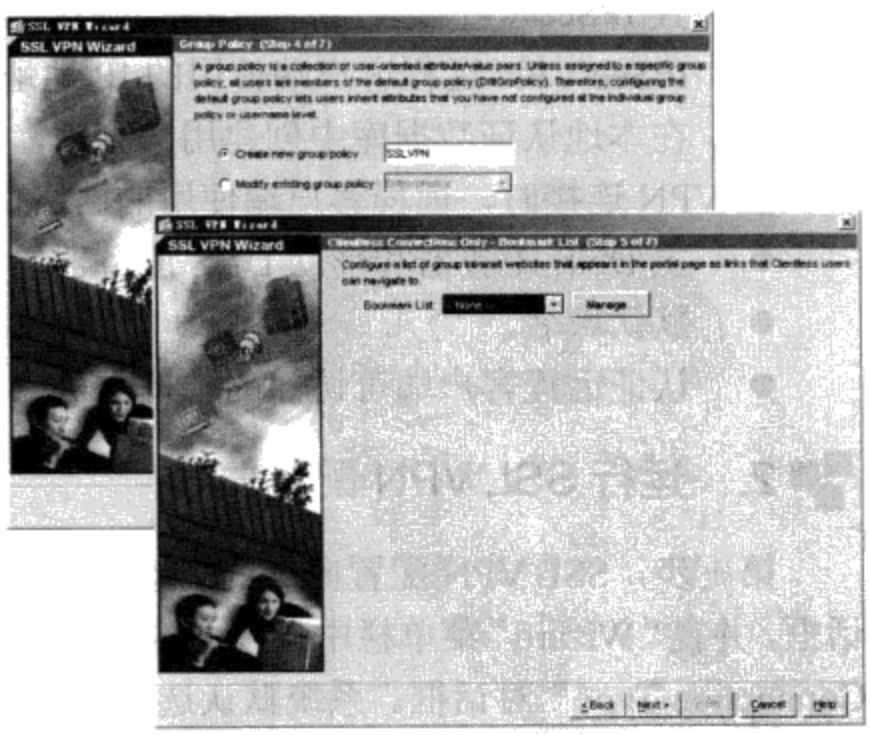


图11-32 设置策略名称和资源列表

提示

建议不要修改系统默认策略，以免影响到其他访问功能的应用。

第 5 步，单击“Manage”按钮，在“Configure GUI Customization Objects”对话框中，配置 SSL VPN 门户网站页面显示的可用资源或站点书签列表。单击“Edit”按钮，在“Add Bookmark List”对话框中，编辑现有书签列表，在“Name”和“URL”栏中分别可以设置显示名称和对应的 URL 路径。单击“Add”按钮，显示如图 11-33 所示“Add Bookmark Entry”对话框，添加书签项。

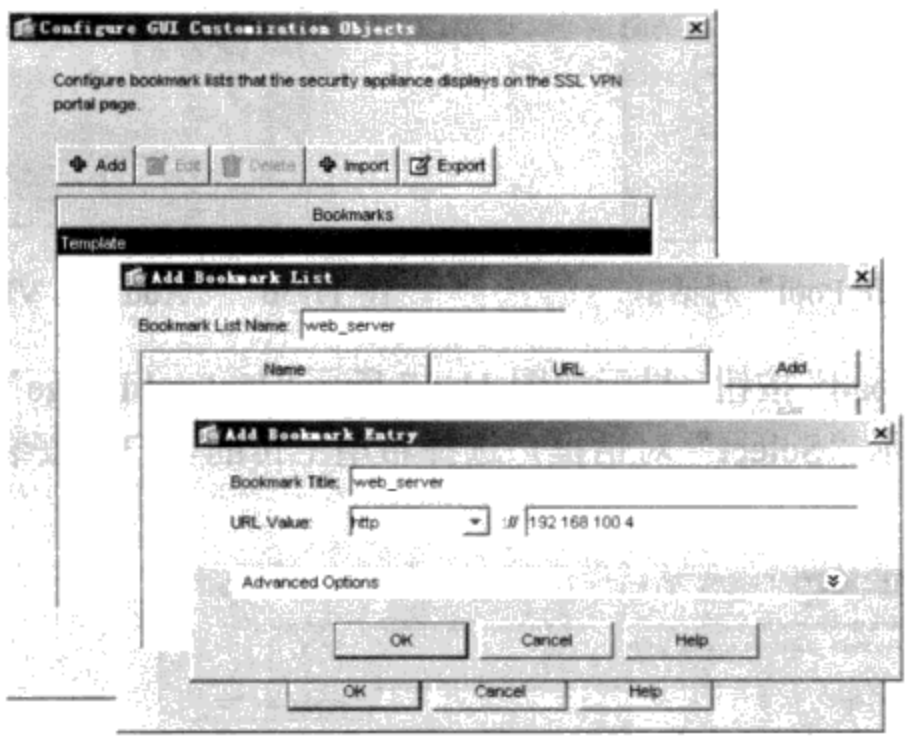


图 11-33　指定 VPN 客户端可以访问的网络资源

第 6 步，连续单击“OK”按钮，返回“Clientless Connections Only - Bookmark list”对话框，所选对象已经显示在下拉列表框中。单击“Next”按钮，显示如图 11-34 所示“IP Address Pools and Client image – AnyConnect VPN Client Connections Only”对话框，为通过 SSL VPN 拨入的用户创建 IP 地址池，并为其提供 VPN 客户端安装程序。

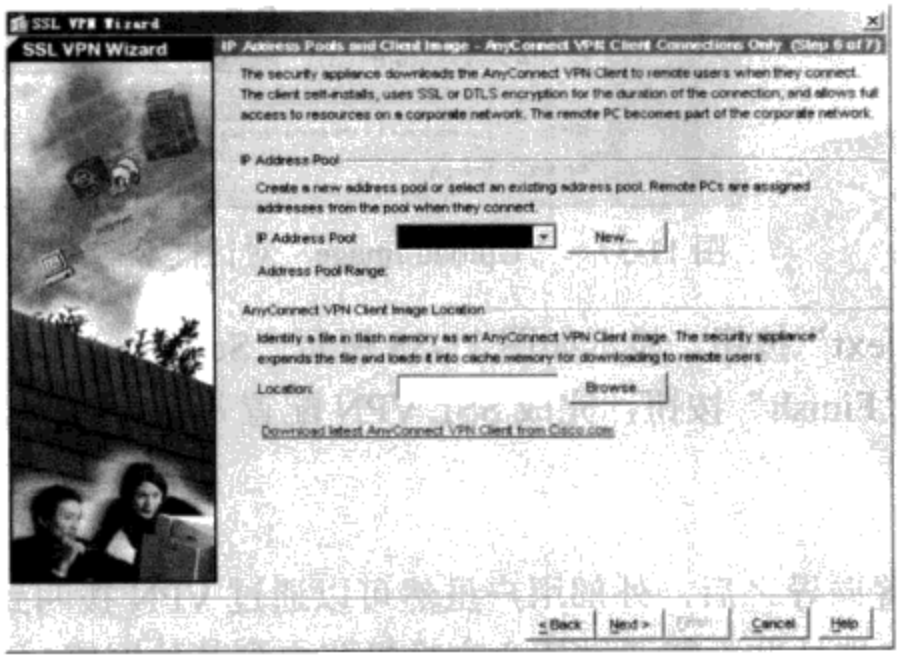


图 11-34　“IP Address Pools and Client image–AnyConnect VPN Client Connections Only”对话框

第7步，单击“IP Address Pool”选项后的“New”按钮，显示如图11-35所示“Add IP Pool”对话框，输入地址池名称和起止IP地址即可，单击“OK”按钮返回到SSL VPN配置向导。

第8步，在“IP Address Pools and Client image – AnyConnect VPN Client Connections Only”对话框中，单击“Browse”按钮，显示如图11-36所示“Add SSL VPN Client Image”对话框，选择将要为拨入用户提供的客户端安装程序。如果ASA缓存中已经包含VPN客户端程序，则可以单击“Browse Flash”按钮查找，否则可以上传本地计算机上的客户端安装程序。

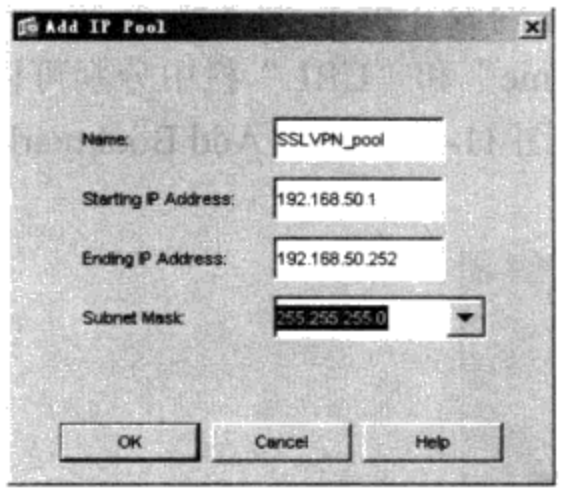


图11-35 “Add IP Pool”对话框

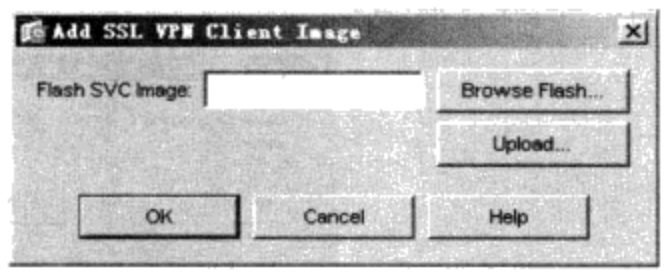


图11-36 “Add SSL VPN Client Image”对话框

第9步，单击“Upload”按钮，显示如图11-37所示“Upload Image”对话框，单击“Browse Local Files”按钮，显示“Select”对话框，选择希望上传的客户端安装程序并单击“Select”按钮即可。

图11-37 “Upload Image”对话框

第10步，单击“Next”按钮，显示如图11-38所示“Summary”对话框，显示已创建SSL VPN摘要信息。单击“Finish”按钮，完成SSL VPN配置并保存。

3. 配置NAT

完成SSL VPN配置向导之后，外部用户虽然可以通过VPN拨叫到内网，但由于ASA地址池为客户端分配的IP地址并不能通过核心交换机路由到其他网络，因此还必须通过NAT将其转换为能够访问内部网络资源的IP地址。

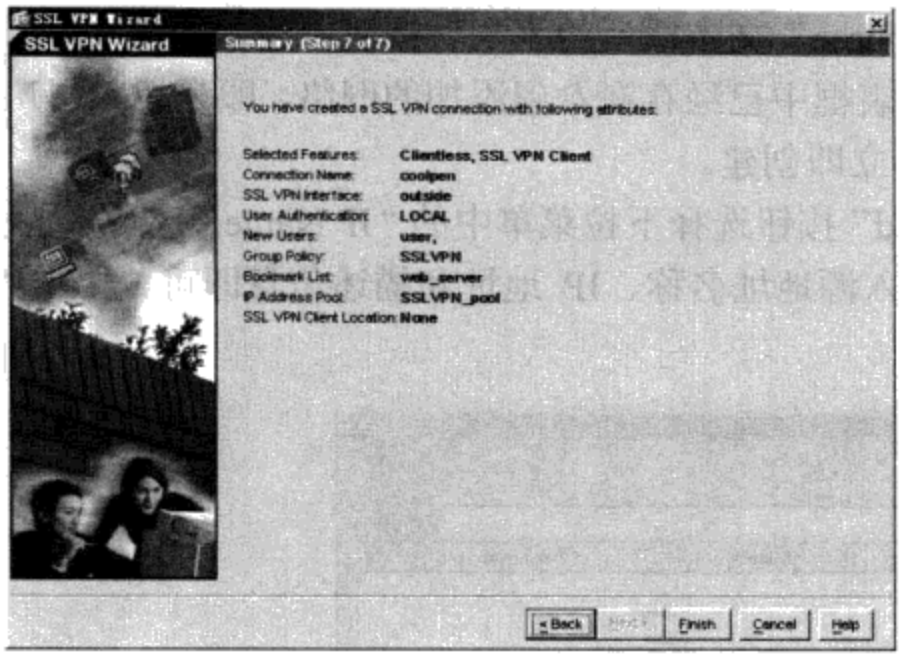


图 11-38 “Summary”对话框

第 1 步，在 ASDM 管理窗口中单击“Configuration”按钮，在左侧导航栏中单击“Firewall”按钮，选择“Firewall”分支下选择“NAT Rules”选项，显示如图 11-39 所示窗口。

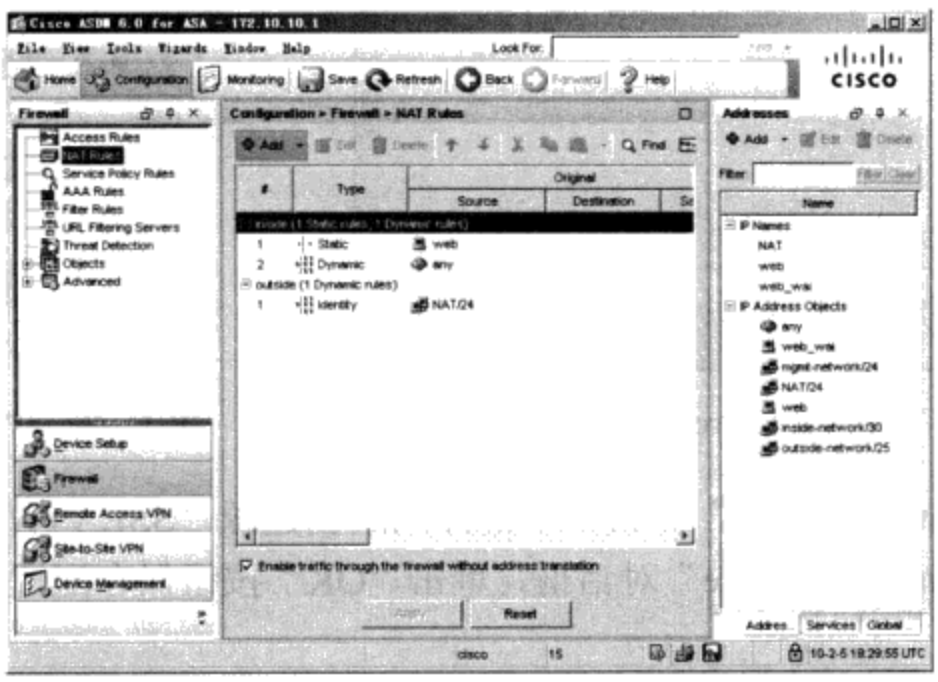


图 11-39 ASDM 管理窗口

第 2 步，单击“Add”按钮并选择下拉菜单中的“Add Dynamic NAT Rule”选项，显示如图 11-40 所示“Add Dynamic NAT Rule”对话框，在“interface”下拉列表框中选择“inside”选项。

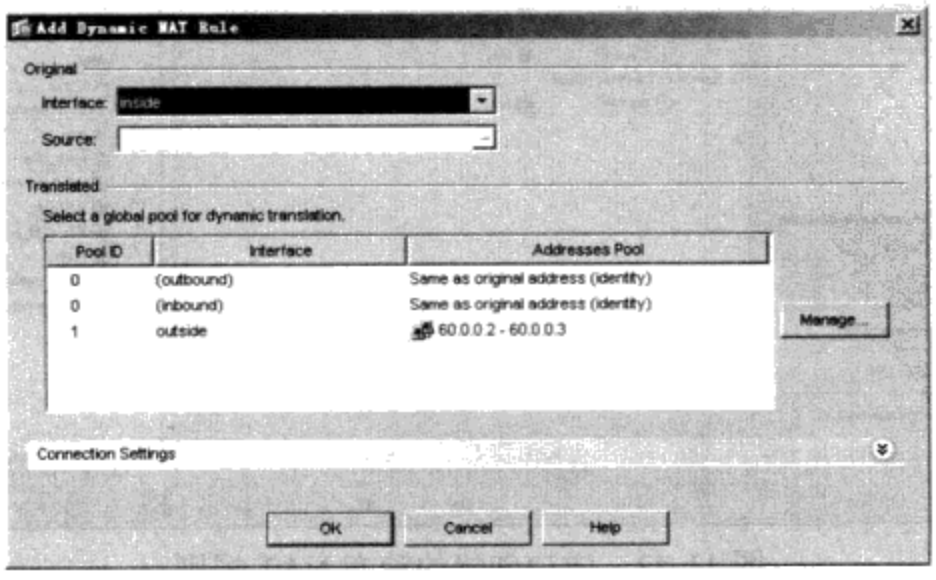


图 11-40 “Add Dynamic NAT Rule”对话框

第3步，单击“Source”文本框后的“...”按钮，显示如图11-41所示“Browse Source”对话框，如果源地址列表框中已经存在希望添加的网络，即为拨入用户创建的地址池，则可以直接选择。否则，需要立即创建。

第4步，单击“Add”按钮选择下拉菜单中的“IP Name”选项，显示如图11-42所示“Add IP Name”对话框，输入源地址名称、IP 地址和描述信息即可。单击“OK”按钮，将其添加到源列表框中。

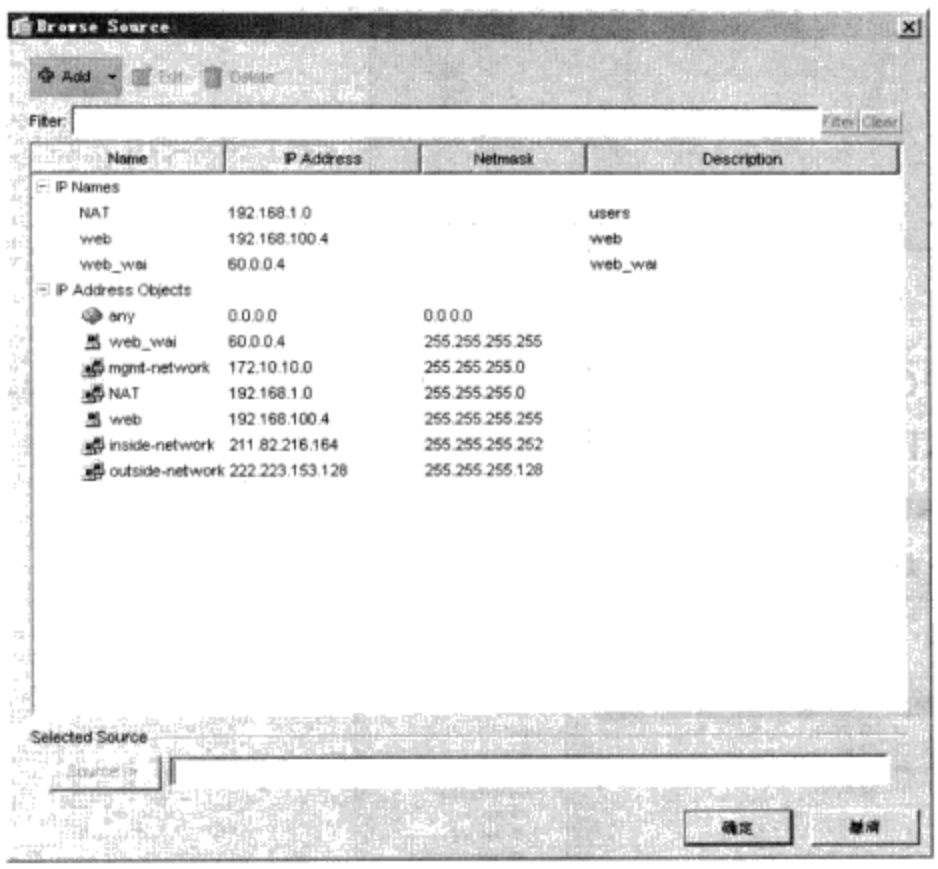


图11-41 “Browse Source”对话框

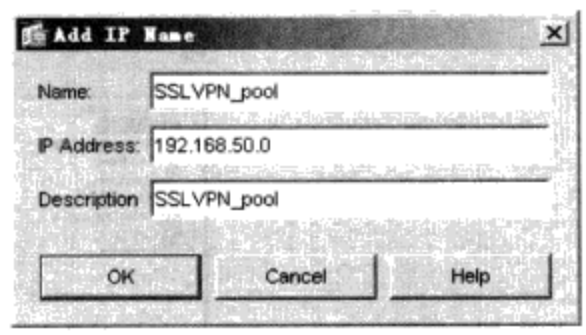


图11-42 “Add IP Name”对话框

第5步，在“Browse Source”对话框中选择刚刚创建源“SSL VPN_Pool”，单击“确定”按钮返回“Add Dynamic NAT Rule”对话框，单击“OK”按钮保存配置，配置结果如图11-43所示。

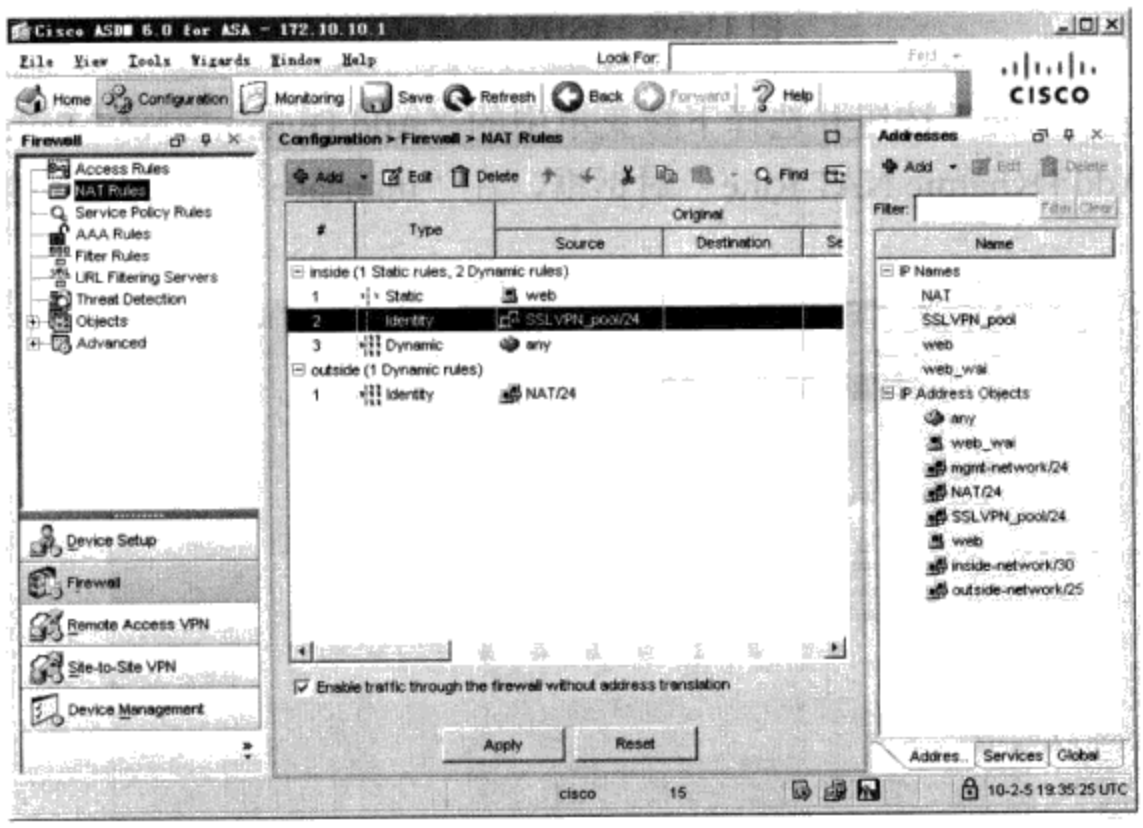


图11-43 成功创建的动态NAT规则

第 6 步，在右侧边栏底部单击“Global”按钮，在“Global”选项卡中单击“Add”按钮，显示如图 11-44 所示“Add Global Address Pool”对话框，在“interface”下拉列表框中选择“outside”选项，默认情况下此时“Pool ID”文本框中将自动输入 1，如果在此之前已经创建过全局地址池，则此处的需要将以此类推。选择“Port Address Translation（PAT） using IP Address of the interface”单选按钮即可。

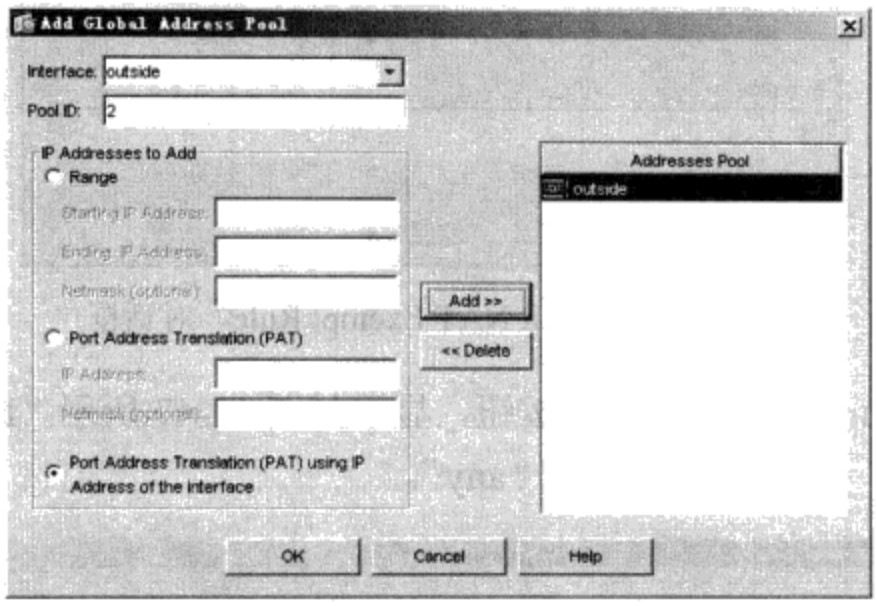


图 11-44 “Add Global Address Pool”对话框

第 7 步，单击“OK”按钮，保存配置并返回 ASDM 管理窗口，配置结果如图 11-45 所示。

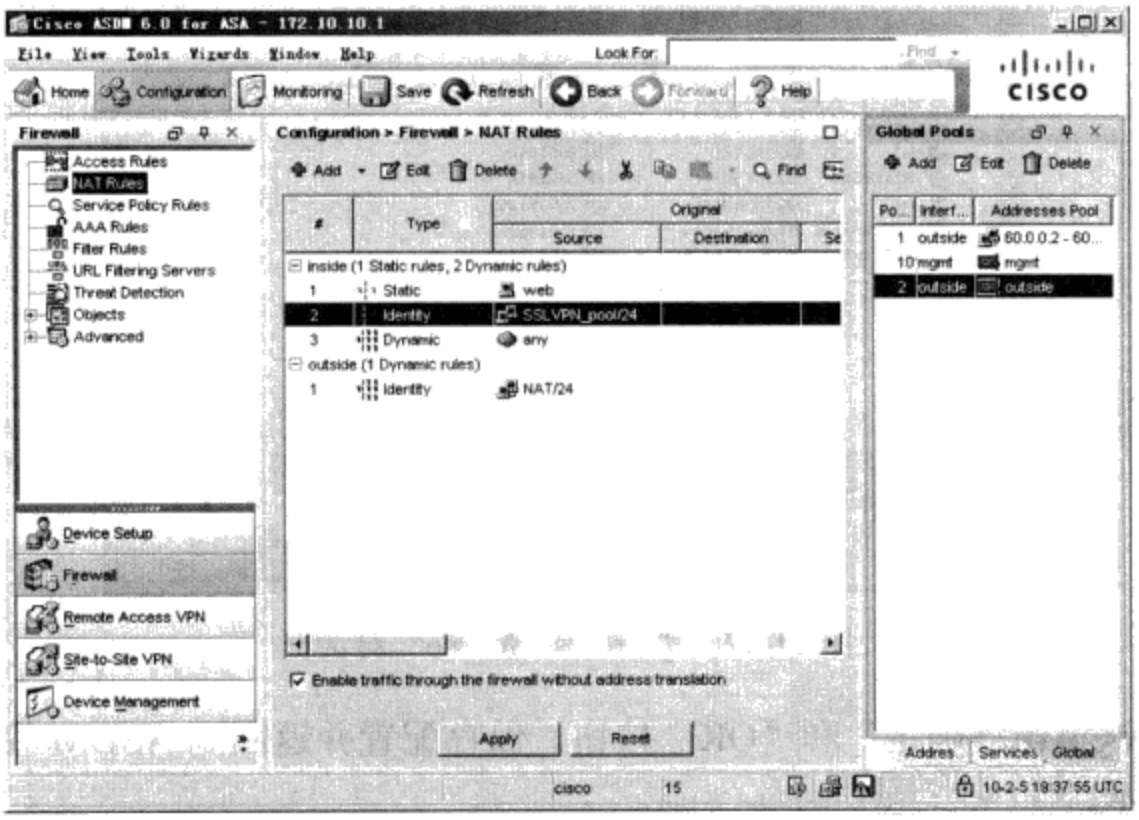


图 11-45 成功创建的全局地址池

4. 配置非转换 NAT

创建非转换 NAT 规则的过程与创建动态 NAT 规则基本类似。

第 1 步，单击“Add”按钮并选择下拉菜单中的“Add NAT Exempt Rule”选项，显示如图 11-46 所示“Edit NAT Exempt Rule”对话框，选择“Exempt”单选按钮，在“interface”下拉列表框中选择“inside”。

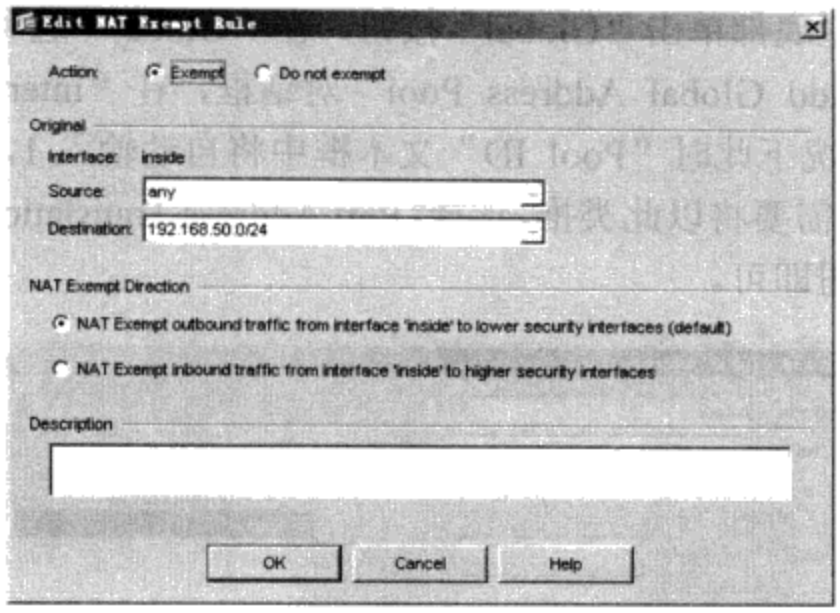


图 11-46 “Edit NAT Exempt Rule”对话框

第 2 步，单击“Source”后的“...”按钮，显示如图 11-47 所示“Browse Source”对话框，在“IP Address Objects”选项区域内选择“any”。

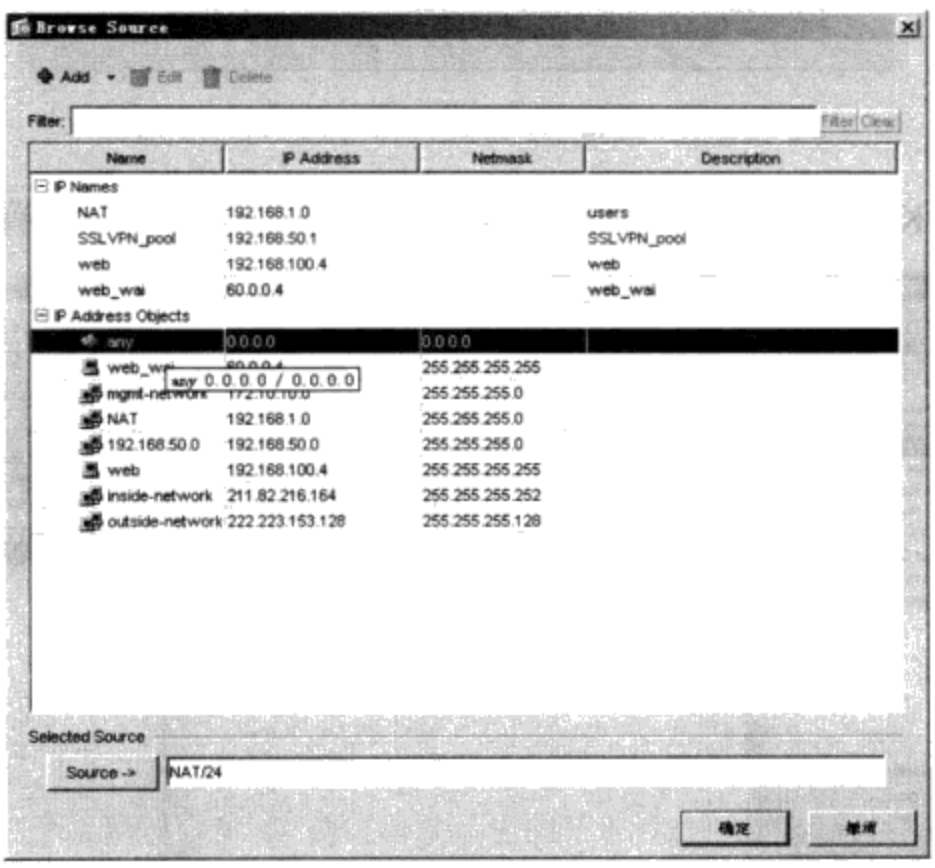


图 11-47 “Browse Source”对话框

第 3 步，依次单击“确定”和“OK”按钮，保存配置并返回到 ASDM 管理窗口，配置结果如图 11-48 所示。

5. Cisco AnyConnect VPN 客户端

在 IE 浏览器地址栏中输入 VPN 服务器的地址，如 https://222.223.153.128，正确输入用户名和密码后即可登录，显示如图 11-49 所示窗口。在客户端下载页面中单击“Start AnyConnect”超级链接即可开始下载，并自动安装，在此过程中用户需注意浏览器上方的信息栏，安装向导会提示安装 Active 控件。

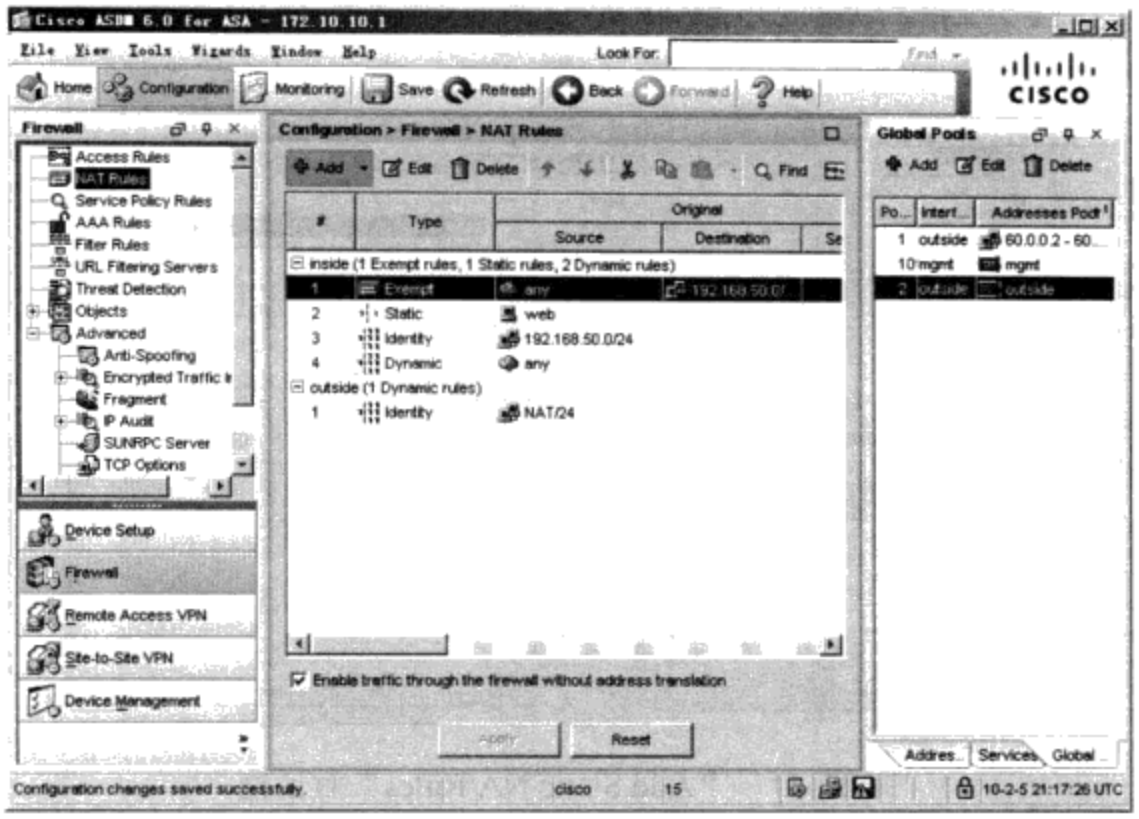


图 11-48　成功创建的非转换 NAT 规则

安装完成后将自动连接到远程 VPN 服务器，并在系统任务栏中显示相应提示信息，如图 11-50 所示。

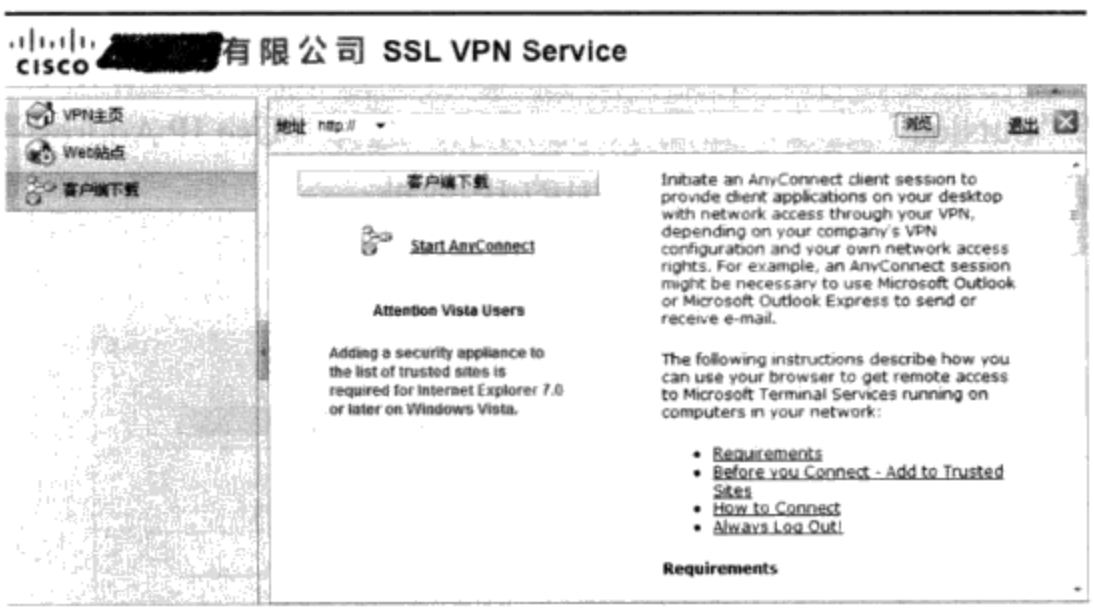


图 11-49　下载并安装 AnyConnect VPN 客户端

图 11-50　连接到 VPN 服务器

11.2.4 发布内部服务器

当服务器处于局域网内，而又需要 Internet 上的计算机可以些服务器时，因为这些服务器使用的是局域网地址，外部的计算机是无法进行访问的，例如 Web 服务器。此时则需要将服务器发布出去，将服务器的局域网地址转换为 Internet 地址。

第 1 步，依次选择“Configuration”→“Firewall”→“NAT Rules”，显示“NAT Rules”窗口。在中间“Add”列表框中，选择“Add Static NA Rules”选项，显示如图 11-51 所示“Add Static NA Rules”对话框。在“Original”区域的“Interface”下拉列表框中，选择内部接口，这里选择“inside”选项。

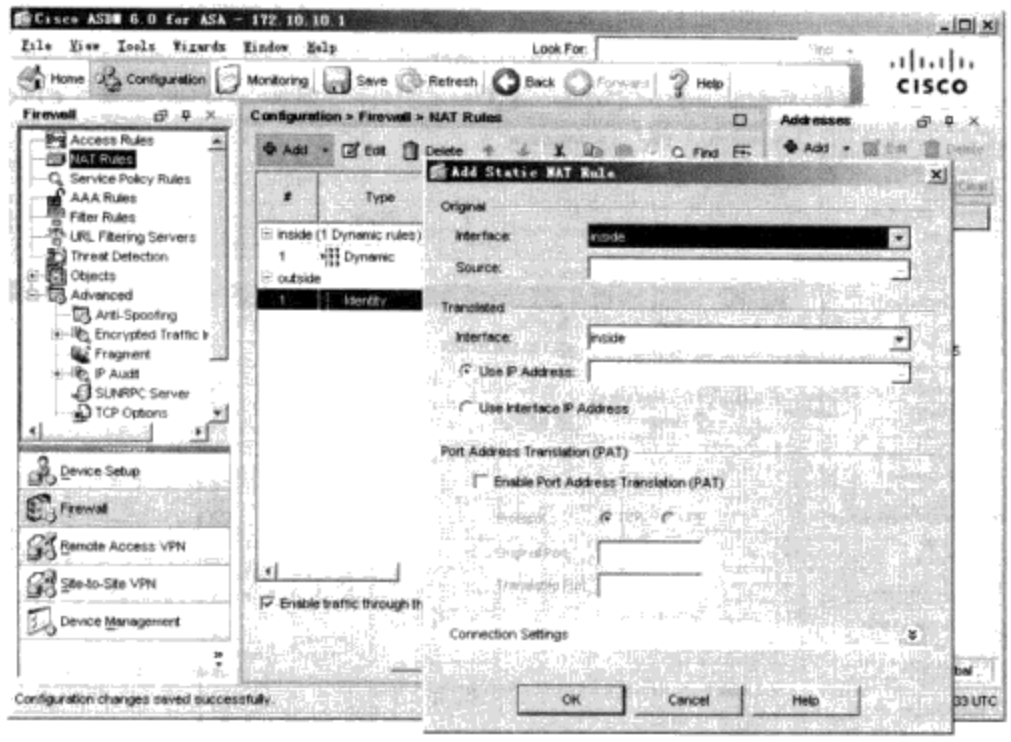


图 11-51　“Add Static NA Rules”对话框

第 2 步，单击…按钮，显示如图 11-52 所示“Browse Source”对话框，在列表框中显示当前所创建的地址类型。依次单击“Add”→“IP Name”，显示“Add IP Name”对话框。在“Name”文本框中，键入该 IP 名称的名称，在“IP Address”和“Description”文本框中，分别键入所在发布的服务器的 IP 地址和描述信息。

第 3 步，依次单击“OK”、“确定”按钮，返回“Add Static NA Rules”对话框。并在“Translated”区域的“Interface”列表框中，选择“outside”选项，如图 11-53 所示。选择“Use IP Address”单选按钮并单击…按钮，设置服务器在发布到 Internet 时所使用的 IP 地址。

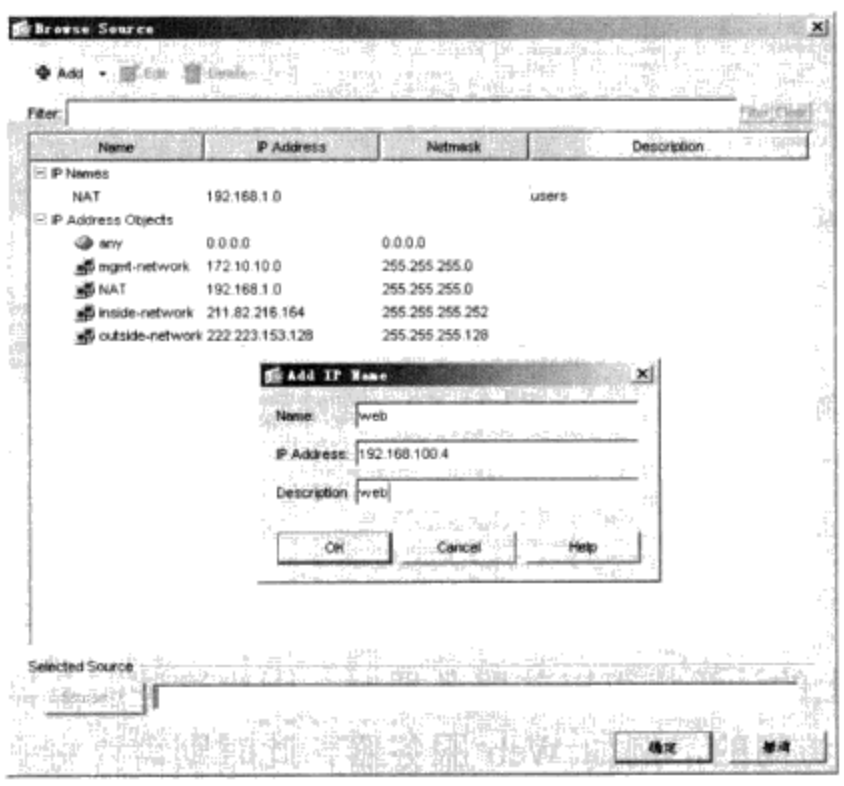


图 11-52　“Browse Source”对话框

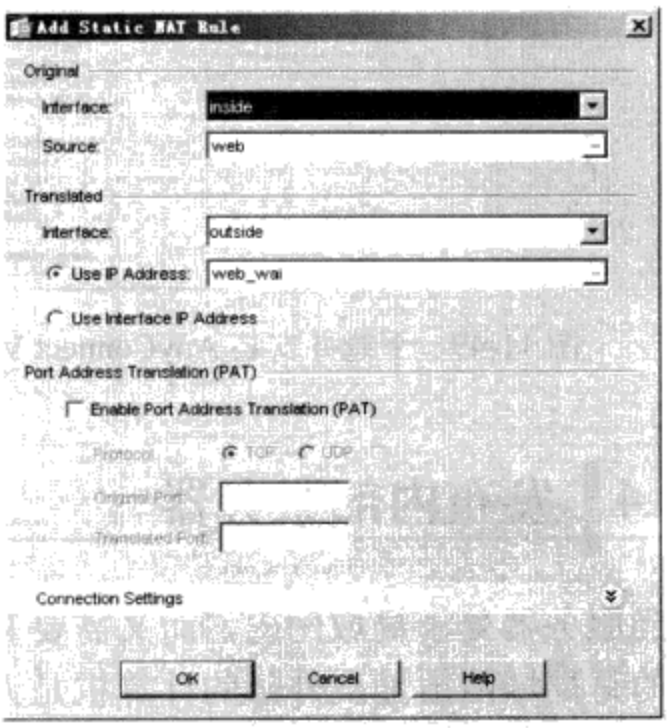


图 11-53　设置连接外网接口

第 4 步，设置完成后，单击“OK”按钮，确认并发送配置到设备即可。

第 5 步，此外，还需要配置接入策略，依次选择“Configuration”→“Firewall”→“Access Rules”。在中间窗口中的“Add”列表框中选择“Add Access Rule”选项，显示如图 11-54 所示“Add Access Rule”对话框。在“Interface”下拉列表框中，选择“outside”选项。在“Action”

栏中，选择“Permit”单选按钮。在“Source”和“Destination”下拉列表框中，选择“any”选项。在“Service”下拉列表框中，选择“ip”选项。如果想要启用日志记录功能，可选中“Enable Logging”复选框即可。

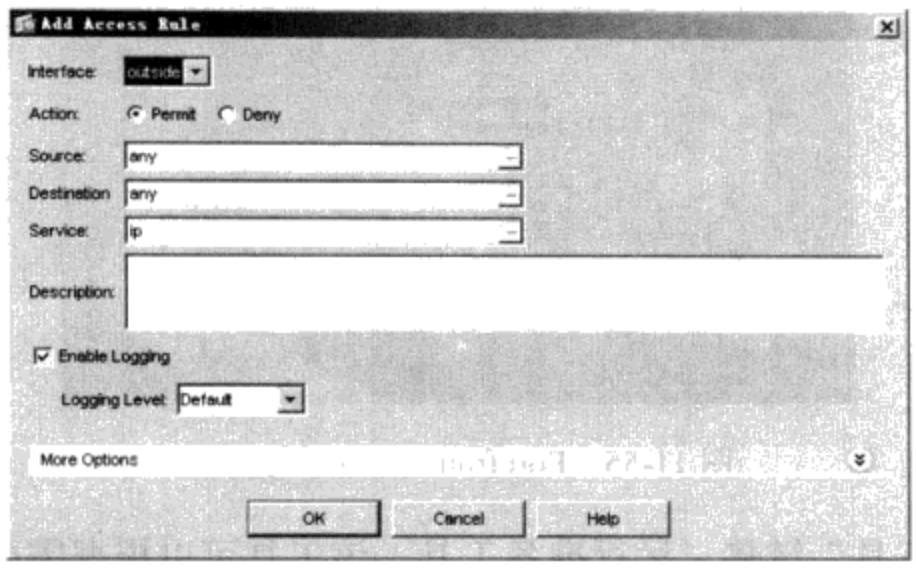


图 11-54 “Add Access Rule”对话框

第 6 步，设置完成后，单击“OK”按钮，确认并发送配置到设备即可。

11.3 代理服务器安全管理

代理服务器方案无疑是所有接入方案中实现成本最低的，在保证服务器硬件性能满足需求的下，关键是选择适用的代理服务器软件。Forefront TMG 是 Microsoft Forefront 系列中的产品，全名为 Forefront Threat Management Gateway，是 ISA Server 的升级版本。Forefront TMG 主要提供代理服务器、防火墙和 Web 缓存三大功能，通过制定策略、规则，控制网络内部与外部的通信，防范外来网络的攻击，提高网络性能和安全性。

11.3.1 Microsoft TMG 安装

Forefront TMG 的安装过程很简单，只需指定局域网的 IP 地址段即可，而且安装完成后还可以利用“入门向导”来配置网络设置、系统设置、部署选项及 Web 访问策略。尤其是当配置完 Web 访问策略以后，就可以直接为局域网中的计算机提供 Internet 共享，不需再另行创建其他策略，从而降低了管理的难度。

1. 运行准备工具

安装 Forefront TMG 之前，必须运行准备工具，验证计算机是否满足其安装要求，并自动安装所需的组件。如果在未首先运行准备工具的情况下运行 Forefront TMG，并且如果计算机未包含所需应用程序，Forefront TMG 安装可能会失败。这些应用程序包括：

- Windows 角色和功能。
- .NET 3.5 Framework SP1。
- Windows Web 服务 API。

将 Forefront TMG 2010 安装光盘插入光驱，自动运行如图 11-55 所示界面。

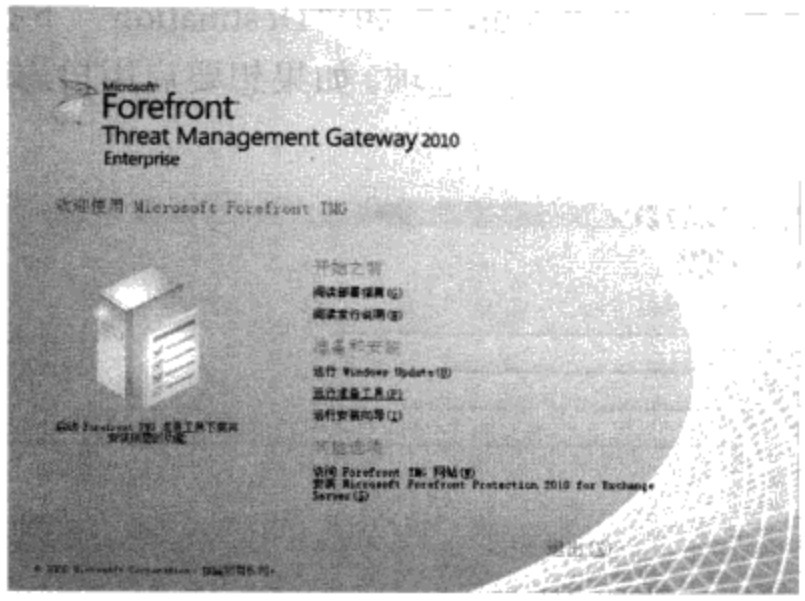


图 11-55　Forefront TMG 欢迎界面

单击“运行准备工具”链接，运行准备工具，该工具可以根据需要安装某些或所有需要的功能。在如图 11-56 所示“安装类型”对话框中，根据需要选择当前服务器 Forefront TMG 的安装类型，这里选择“Forefront TMG 服务和管理”选项。单击“下一步”按钮，准备工具即可开始对服务器进行检测和功能安装，并安装完成后自动重新启动计算机。

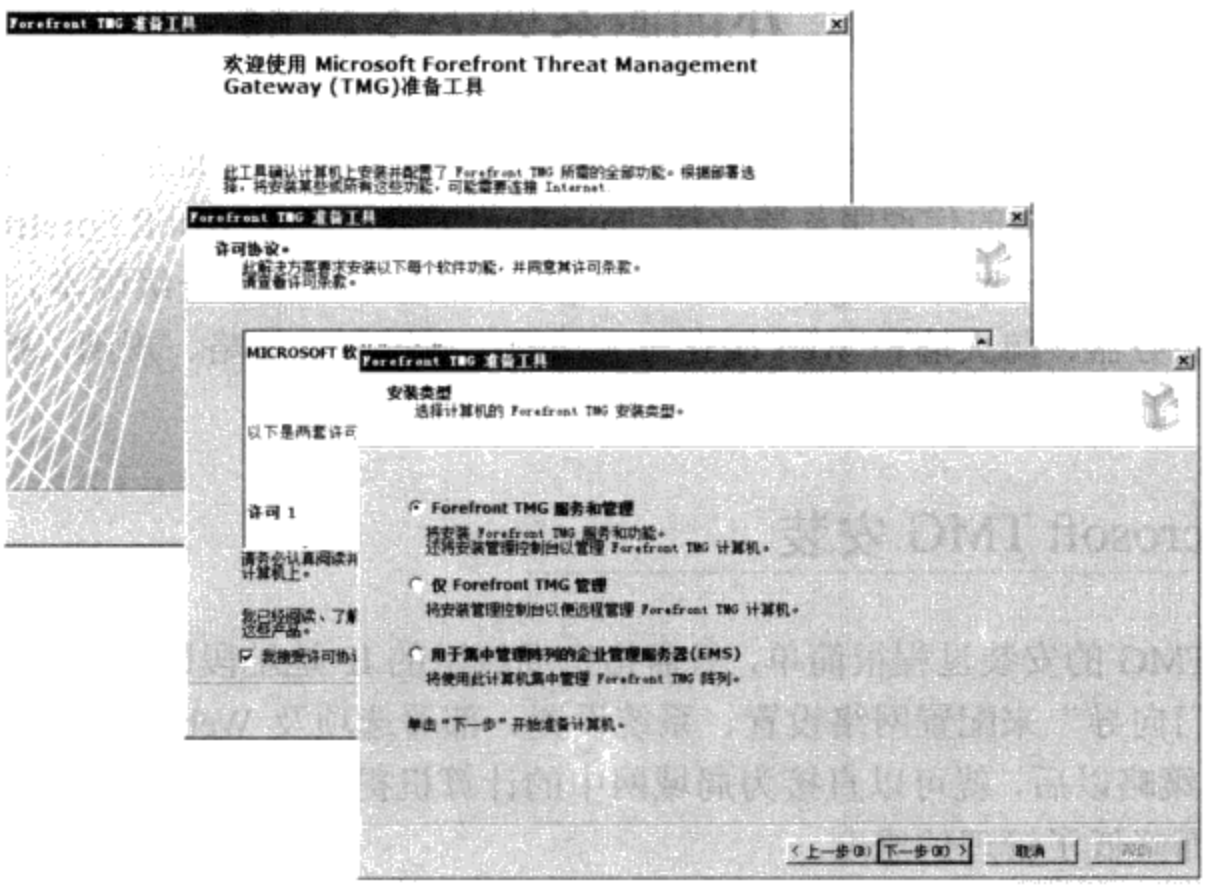


图 11-56　“安装类型”对话框

2. 安装 Forefront TMG

第 1 步，重新启动计算机后，再次运行 Forefront TMG 安装光盘，在欢迎界面中，单击“运行安装向导”链接运行安装向导。连续单击“下一步”按钮，在“客户信息”对话框中输入用户名、单位和产品序列号，如图 11-57 所示。

第 2 步，单击“下一步”按钮，显示如图 11-58 所示“安装方案”对话框。根据需要选择安装的类型，包括 Forefront TMG 服务和管理、仅 Forefront TMG 管理和用于集中管理阵列的企业管理服务器三项，这里选择“安装 Forefront Threat Management Gateway”单选按钮。

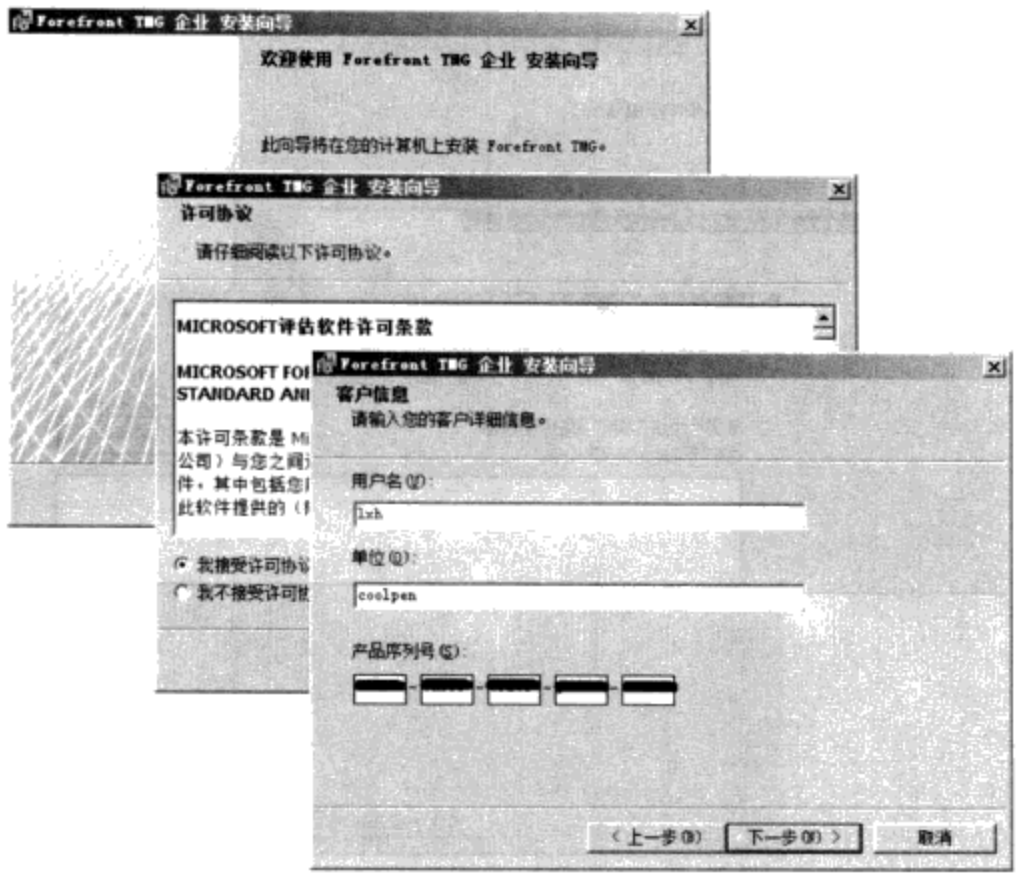


图 11-57 “客户信息”对话框

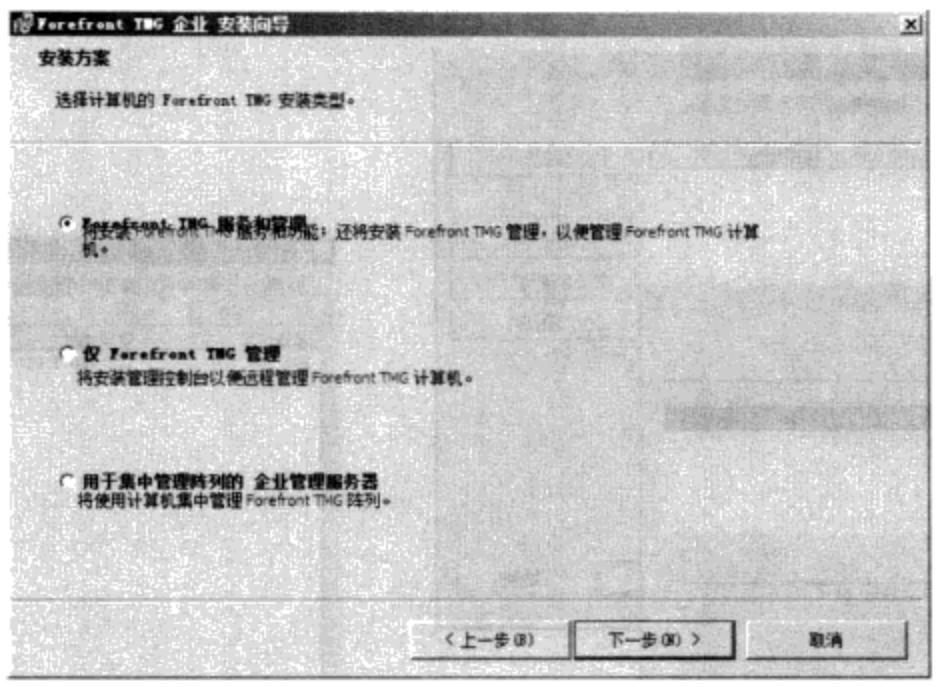


图 11-58 “安装方案”对话框

第 3 步，单击“下一步”按钮，显示如图 11-59 所示“安装路径”对话框，可根据需要修改程序的安装路径，这里保持默认安装路径。单击“下一步”按钮，显示“定义内部网络”对话框，需要根据网络实际情况，将用于连接内部网络的网卡，或内部网络的 IP 地址添加到列表框中。

第 4 步，单击“添加”按钮，显示“地址”对话框，用来添加内部网络的 IP 地址范围。如果要根据网卡添加，可单击“添加适配器”按钮，显示如图 11-60 所示“选择网络适配器”对话框，选择连接内部网络的网卡，即可自动添加相应的 IP 地址段。

如果网络内还包含有其他类型的 IP 地址段，可单击“添加专用地址”按钮，在下拉列表框中选择相应的私有 IP 地址段，如图 11-61 所示。

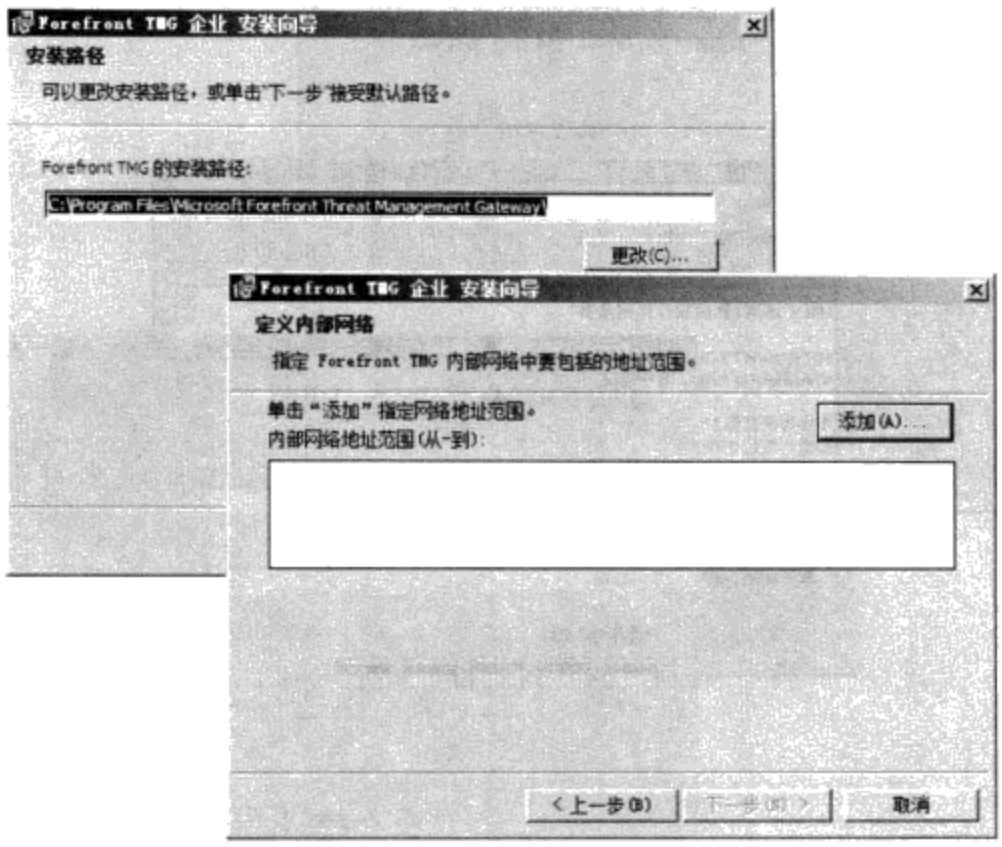


图 11-59 “安装路径”对话框

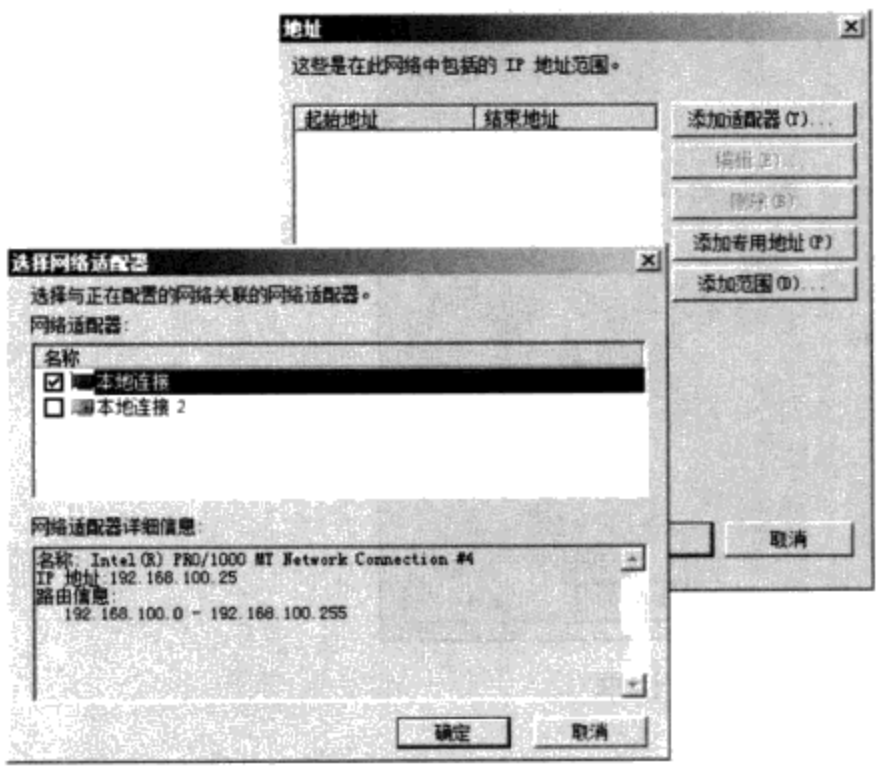


图 11-60 添加地址范围

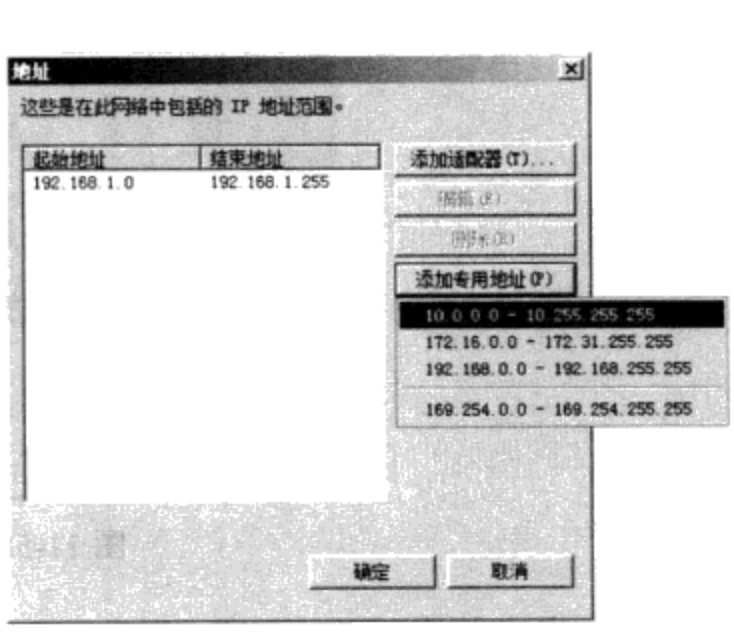


图 11-61 添加专用地址

提示 如果添加专门的 IP 地址段，可单击“添加范围”按钮，在“IP 地址范围属性”对话框，键入起始地址和结束地址即可。

第 5 步，连续单击“确定”按钮，返回“内部网络”对话框。单击“下一步”按钮，显示如图 11-62 所示“服务警告”对话框，列出了在安装过程中将需要重新启动和停止的服务。单击“下一步”按钮，显示“为安装程序做好准备”对话框。单击“安装”按钮即可开始安装。

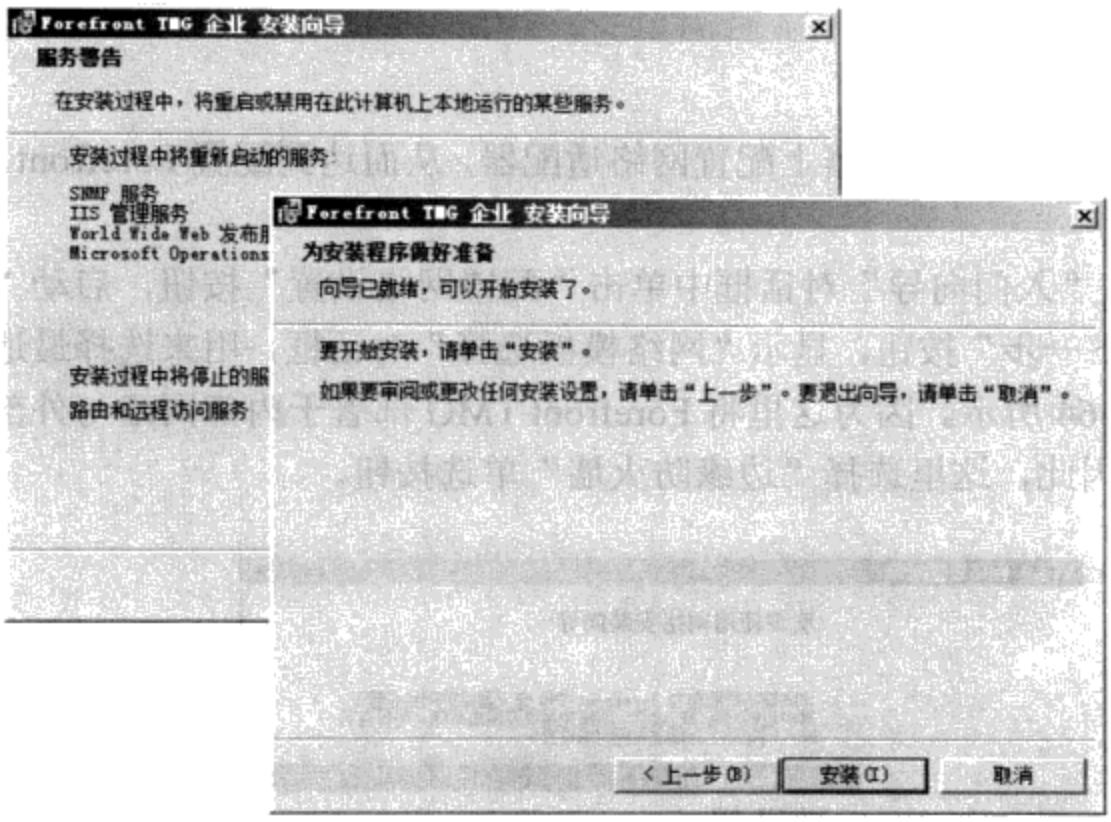


图 11-62 “服务警告”对话框

第 6 步，完成后显示“安装向导完成”对话框，Forefront TMG 安装完成。单击“完成”按钮退出安装向导，显示“保护 ISA 服务器计算机”窗口，并启动 Forefront TMG 控制台。会显示如图 11-63 所示“入门向导”对话框，可用来简单而快速地配置 Forefront TMG，如果不运行向导，将其关闭即可。

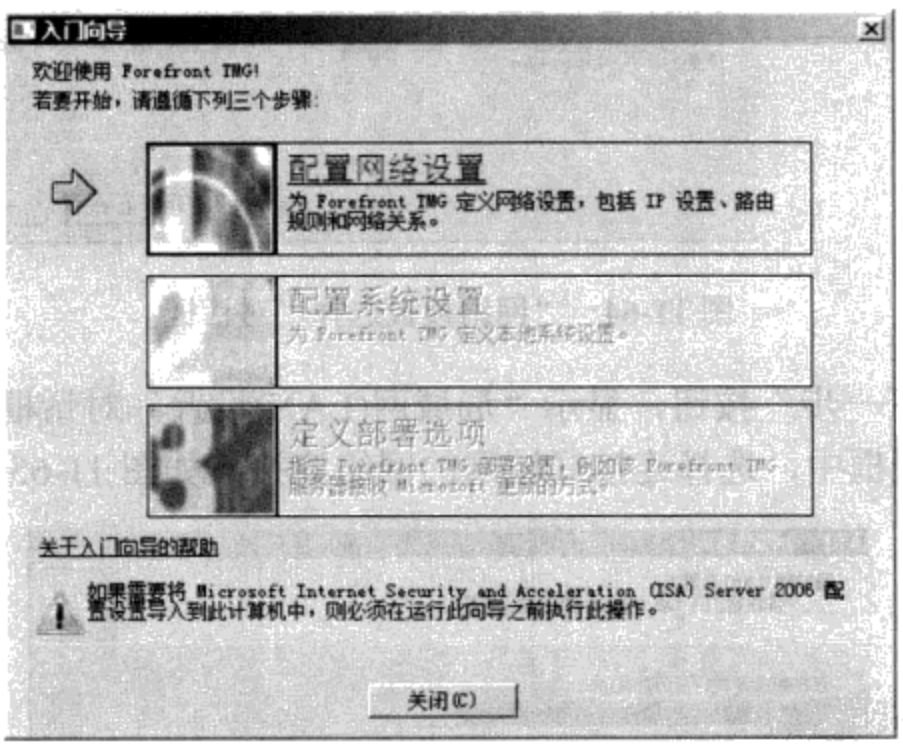


图 11-63 入门向导

11.3.2 Microsoft TMG 配置

在第一次运行 Forefront TMG 时，会自动启动入门向导，可以完成配置网络设置、配置系统设置和定义部署选项，并可配置 Web 访问策略。不过，这三个向导是按顺序依次进行的，在首次使用时，必须先配置完前一个向导，才可配置下一个向导。

1. 配置网络设置

配置网络设置用于在服务器上配置网络适配器，从而达到配置 Forefront TMG 拓扑结构的目的。

第 1 步，在“入门向导”对话框中单击“配置网络设置”按钮，启动“网络设置向导”对话框。单击“下一步”按钮，显示“网络模板选择”对话框，用来选择最适合当前网络的拓扑结构，如图 11-64 所示。因为这里将 Forefront TMG 部署于内部网络与外部网络之间，即处于网络的边缘，因此，这里选择“边缘防火墙”单选按钮。

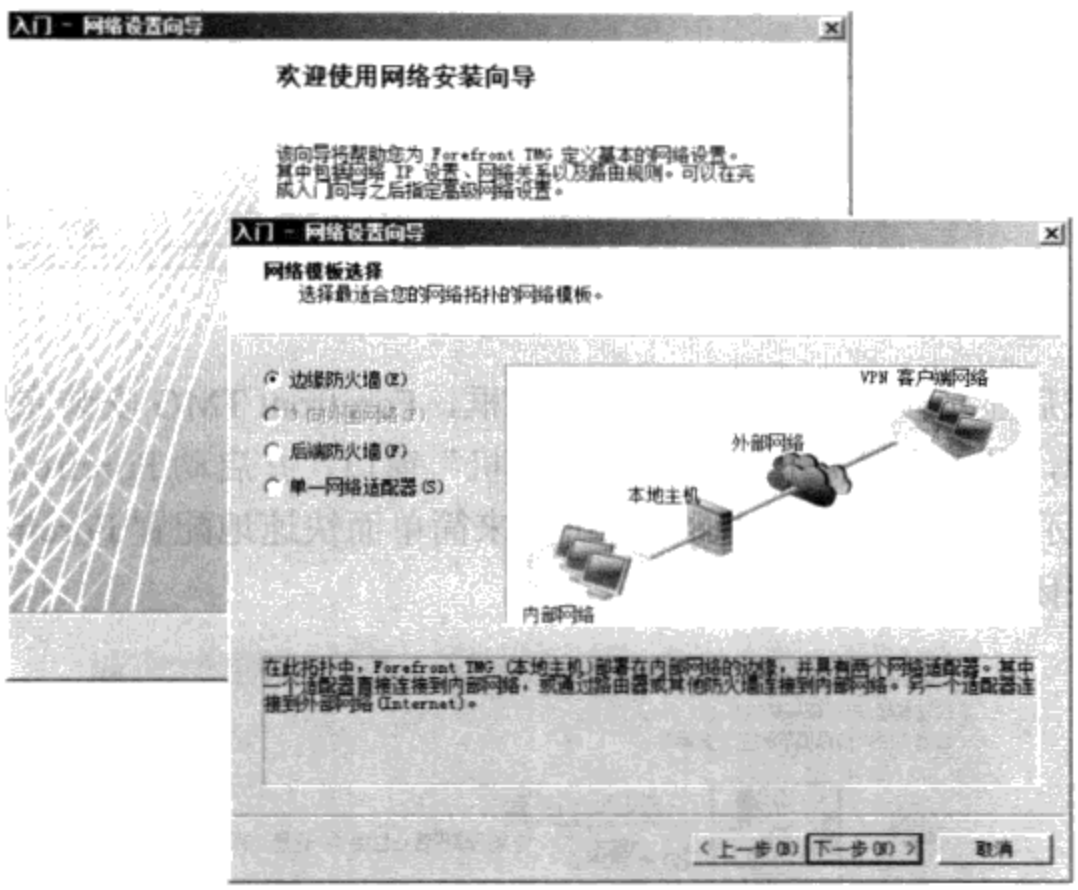


图 11-64 “网络模板选择”对话框

第 2 步，单击“下一步”按钮，显示“局域网(LAN)设置”对话框。在“连接到 LAN 的网络适配器”下拉列表框中，选择连接局域网的网络连接，如图 11-65 所示。

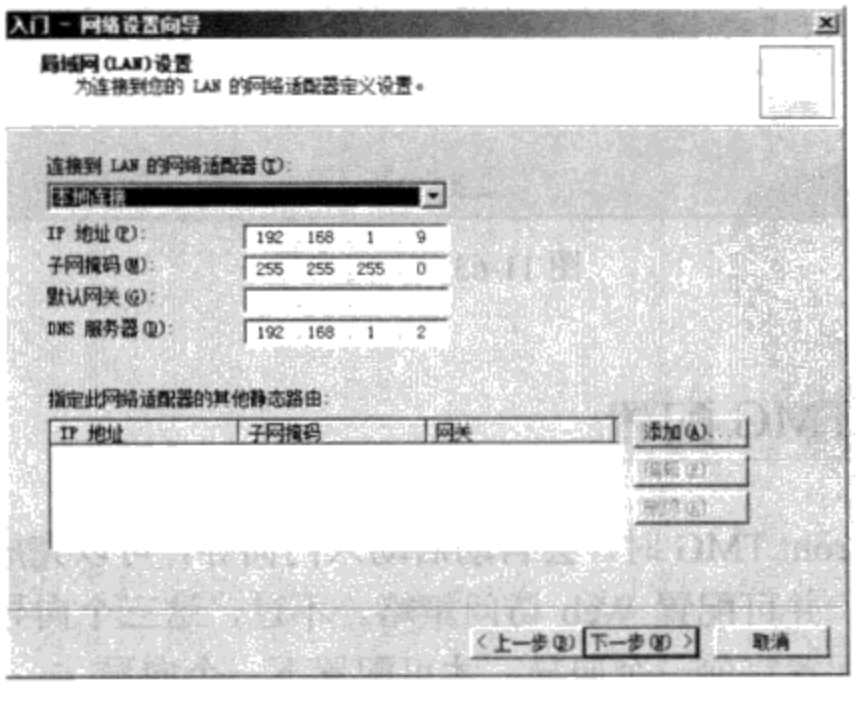


图 11-65 “局域网(LAN)设置”对话框

第 3 步，单击“下一步”按钮，显示“Internet 设置”对话框。在“连接到 Internet 的网络适配器”下拉列表框中，选择连接 Internet 的网络连接，如图 11-66 所示。

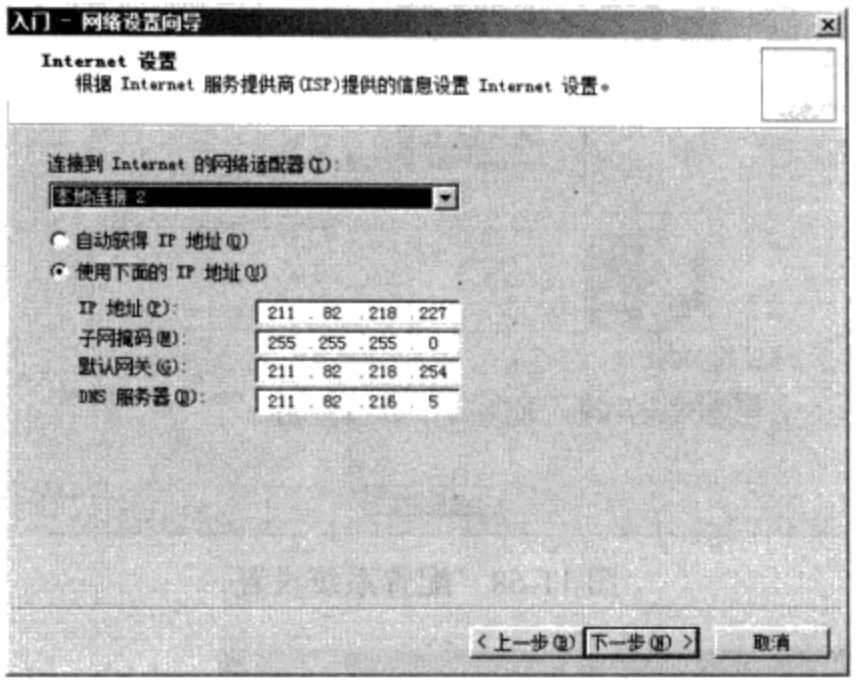


图 11-66 “Internet 设置”对话框

第 4 步，单击“下一步”按钮，网络设置向导完成，如图 11-67 所示。单击“关闭”按钮关闭即可。

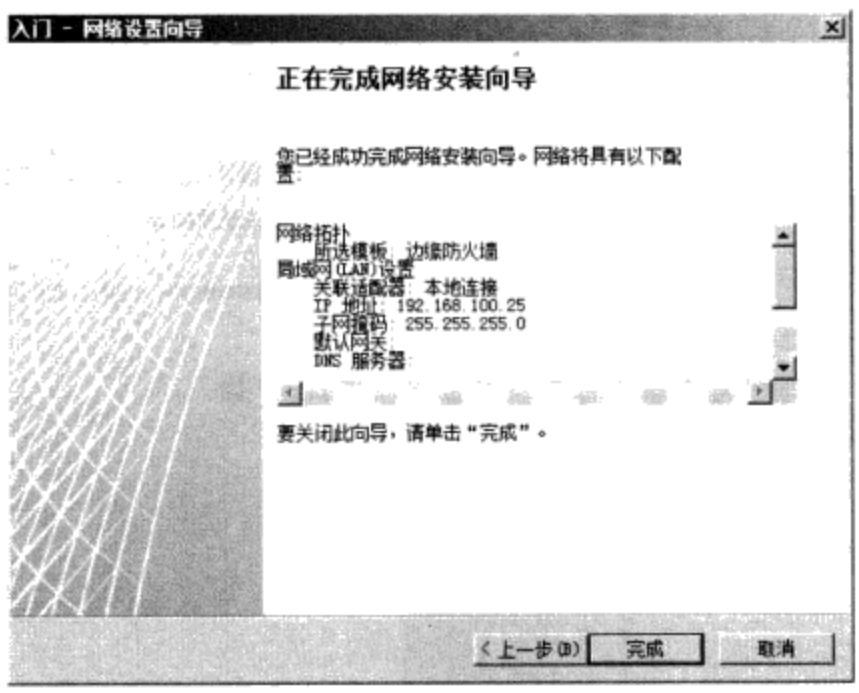


图 11-67 完成网络设置向导

2. 配置系统设置

当“网络设置向导”完成以后，“配置系统设置”选项变为可用状态，可以用来定义本地系统设置了，如图 11-68 所示。

单击“配置系统设置”按钮，打开“系统配置向导”对话框。连续单击“下一步”按钮即可配置完成，如图 11-69 所示。

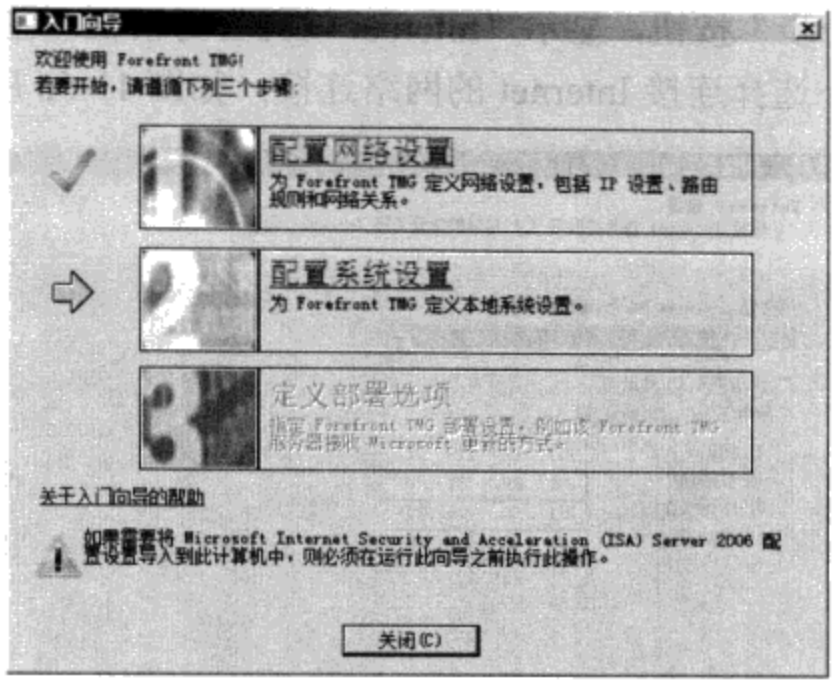


图 11-68　配置系统设置

图 11-69　系统配置向导

3. 定义部署选项

当“系统配置向导”运行完成以后，“定义部署选项”就会变为可用状态，如图 11-70 所示，用来配置 Forefront TMG 的部署设置。

第 1 步，单击“定义部署选项”按钮，打开“部署向导”对话框。连续单击“下一步”按钮，在“定义更新设置”对话框中，选择恶意软件的检查方式和自动更新的轮询频率，如图 11-71 所示。

第 2 步，连接单击“下一步”按钮，完成部署向导，如图 11-72 所示。单击“完成”按钮返回“入门向导”对话框。

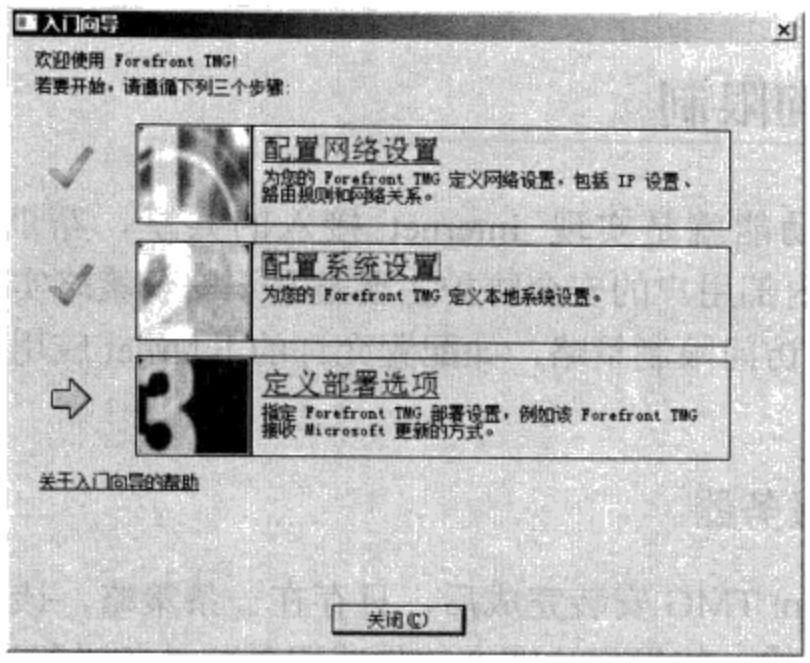


图 11-70　定义部署选项

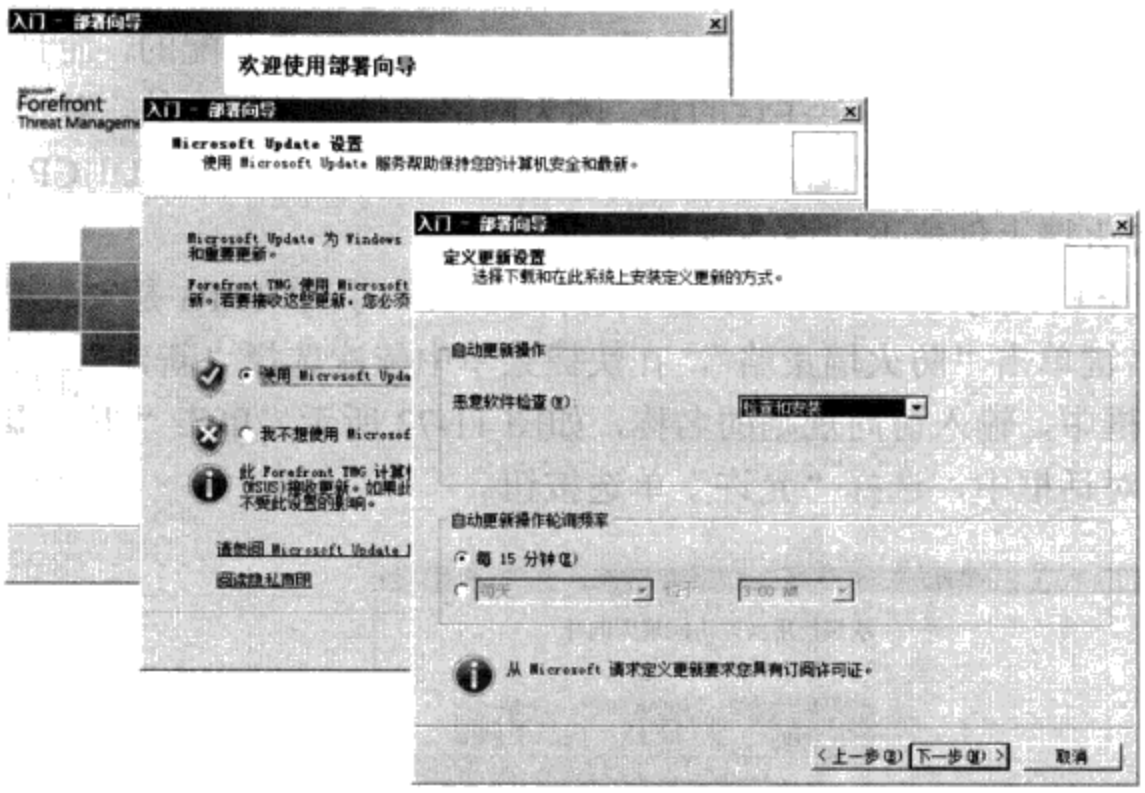


图 11-71　部署向导

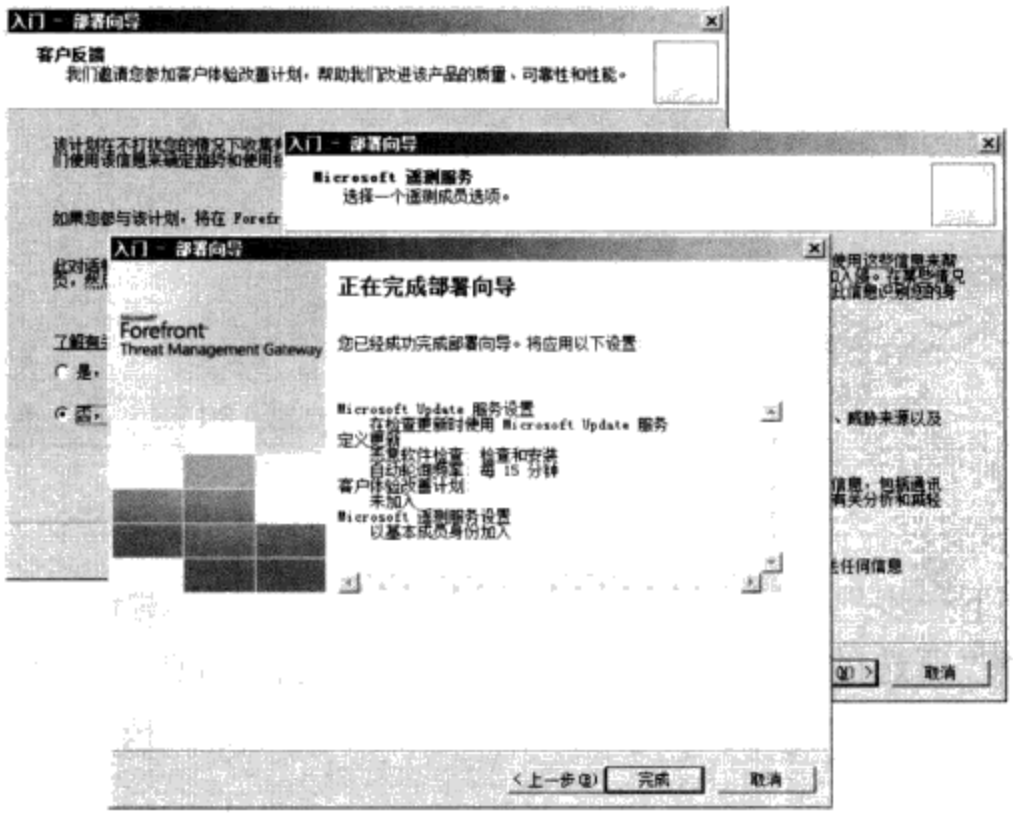


图 11-72　完成部署向导

11.3.3 Internet 访问限制

代理服务器的主要功能就是实现 Internet 接入的共享，帮助内部用户安全的接入到 Internet。TMG 服务器对内部用户的安全防护主要是基于安全策略实现的，管理员可以根据内部网络安全需求配置用户访问限制策略，如配置允许的 Internet 应用、禁止访问指定站点、阻止相应类型的文件等。

1. 配置 DHCP 服务器

默认情况下，Forefront TMG 安装完成后，只存在一条策略，该策略规定所有的关于服务器的网络通信都是被禁止的，如果想让哪个软件或服务与外部进行通信，则必须在 Forefront TMG 中将这个软件或服务所使用的端口打开。

假如一个企业中，计算机的 IP 地址是通过 DHCP 服务器来分配的，而且 DHCP 是安装在了 Forefront TMG 服务器上。需要注意的是，因为网络通信都是双向的，对于 DHCP 服务器而言，不仅需要能够接受客户端的 DHCP 服务请求，更需要能够回复 DHCP 请求，即需要在 Forefront TMG 防火墙上创建下面两条规则。

第 1 步，打开 Forefront TMG 对话框，展开“TMG（其中 TMG 是安装 Forefront TMG 计算机的名称）”右键单击“防火墙策略”，在快捷菜单中依次选择“新建”→“访问规则”，在打开的欢迎对话框中，输入访问规则的名称，如图 11-73 所示。单击“下一步”按钮，在打开的“规则操作”对话框中，选择“允许”单选按钮。

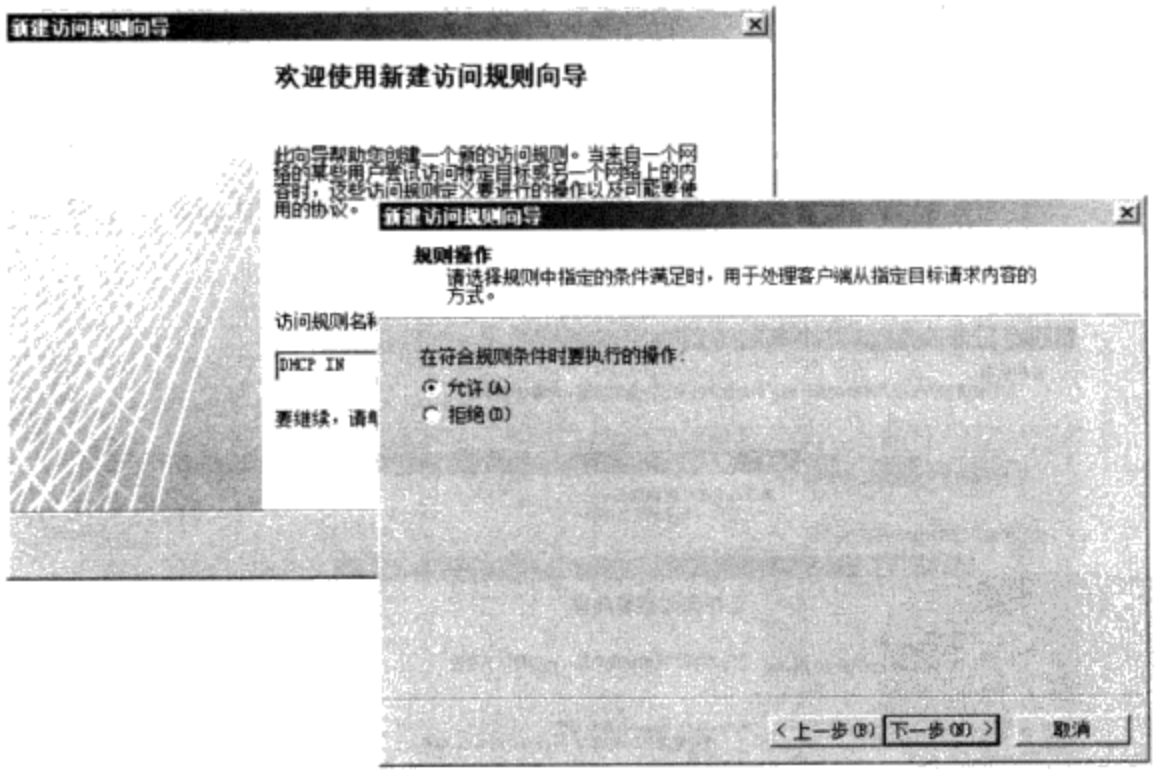


图 11-73　访问规则名称

第 2 步，单击“下一步”按钮，显示如图 11-74 所示“协议”对话框。在“此规则应用到”下拉列表框中，选择“所选的协议”选项，然后单击“添加”按钮，在打开的“添加协议”对话框中，从“结构”中选择“DHCP 请求”协议，单击“添加”按钮，然后单击“关闭”按钮返回即可。

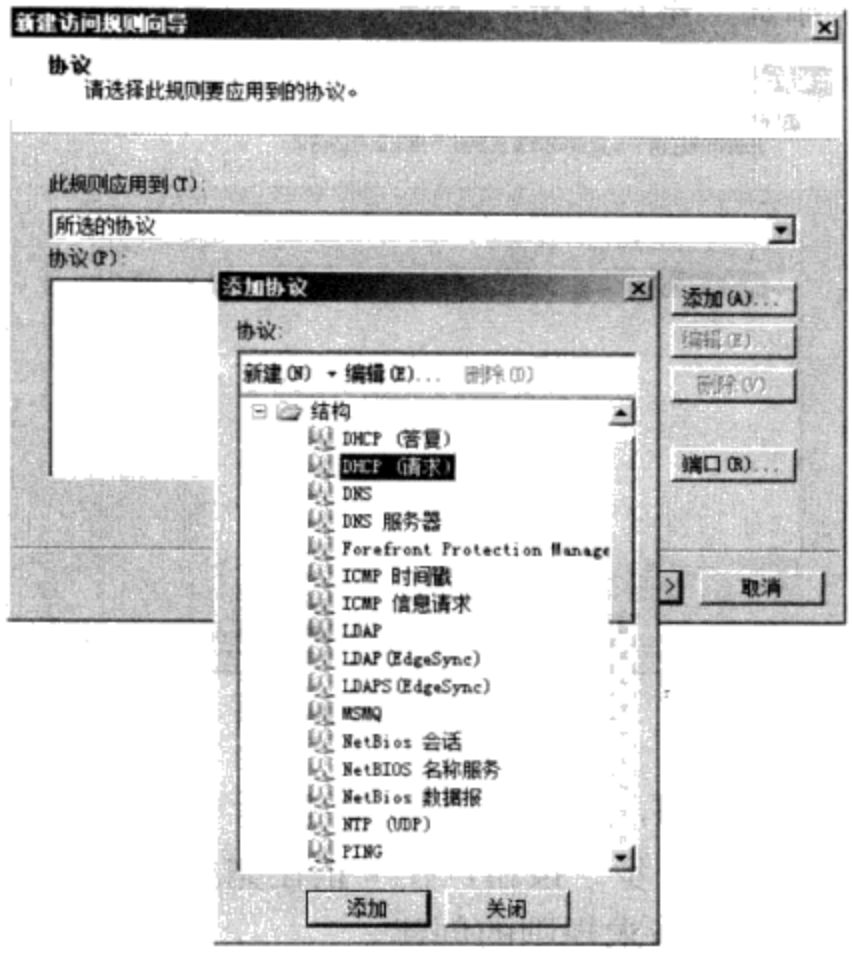


图 11-74 “协议”对话框

第 3 步，单击“下一步”按钮，显示如图 11-75 所示“访问规则源”对话框。单击“添加”按钮，在打开的添加网络实体的“网络”中选择“内部”选项，单击“添加”按钮，然后单击“关闭”按钮返回即可。

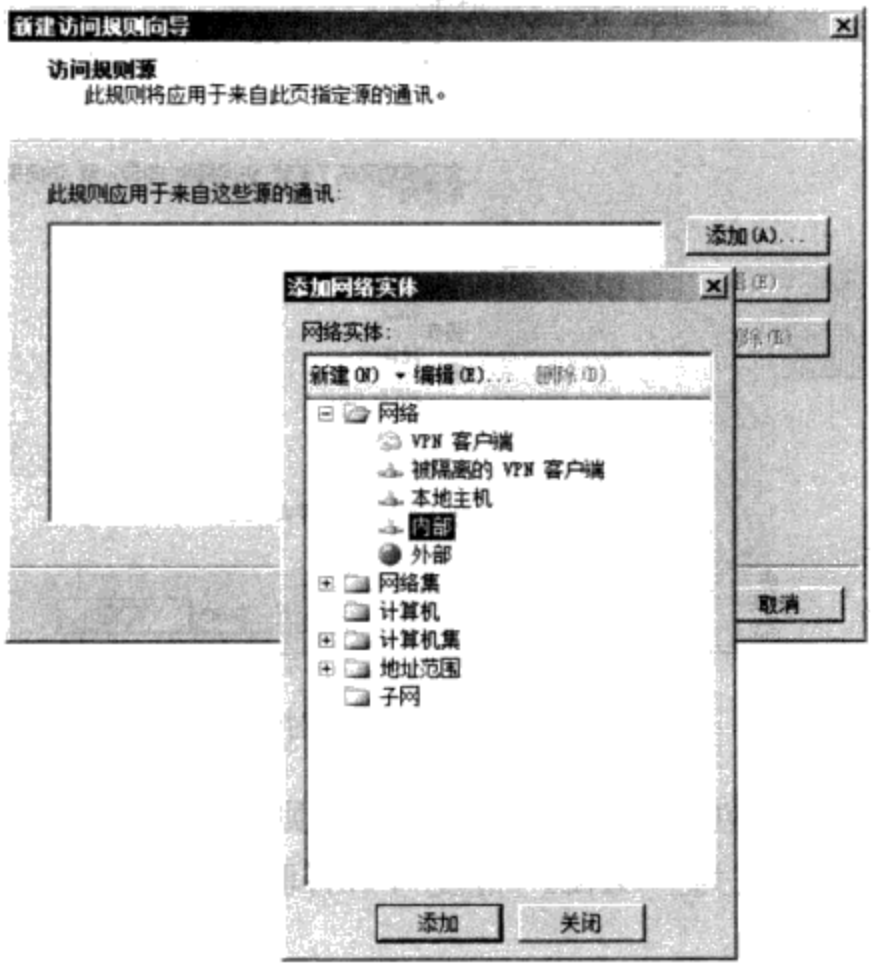


图 11-75 访问规则源

第 4 步，单击“下一步”按钮，显示如图 11-76 所示“访问规则目标”对话框，使用与添

加内部网络相同的操作，添加“本地主机”选项。

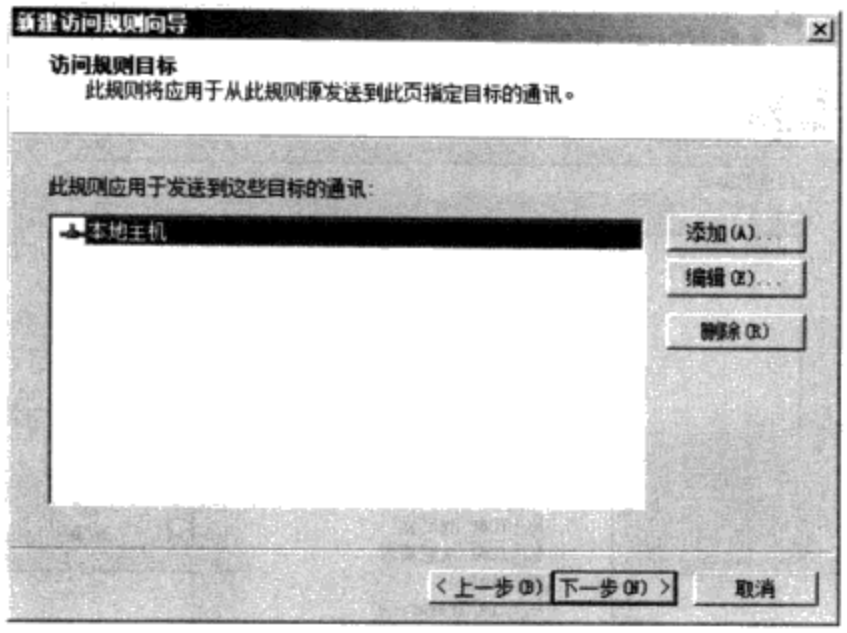


图 11-76 访问规则目标

第 5 步，单击“下一步”按钮，显示如图 11-77 所示“用户集”对话框，保持默认设置，即允许所有用户通信。单击“下一步”按钮，在“正在完成新建 访问规则 向导”对话框中，单击“完成”按钮，完成 DHCP 请求规则的创建。

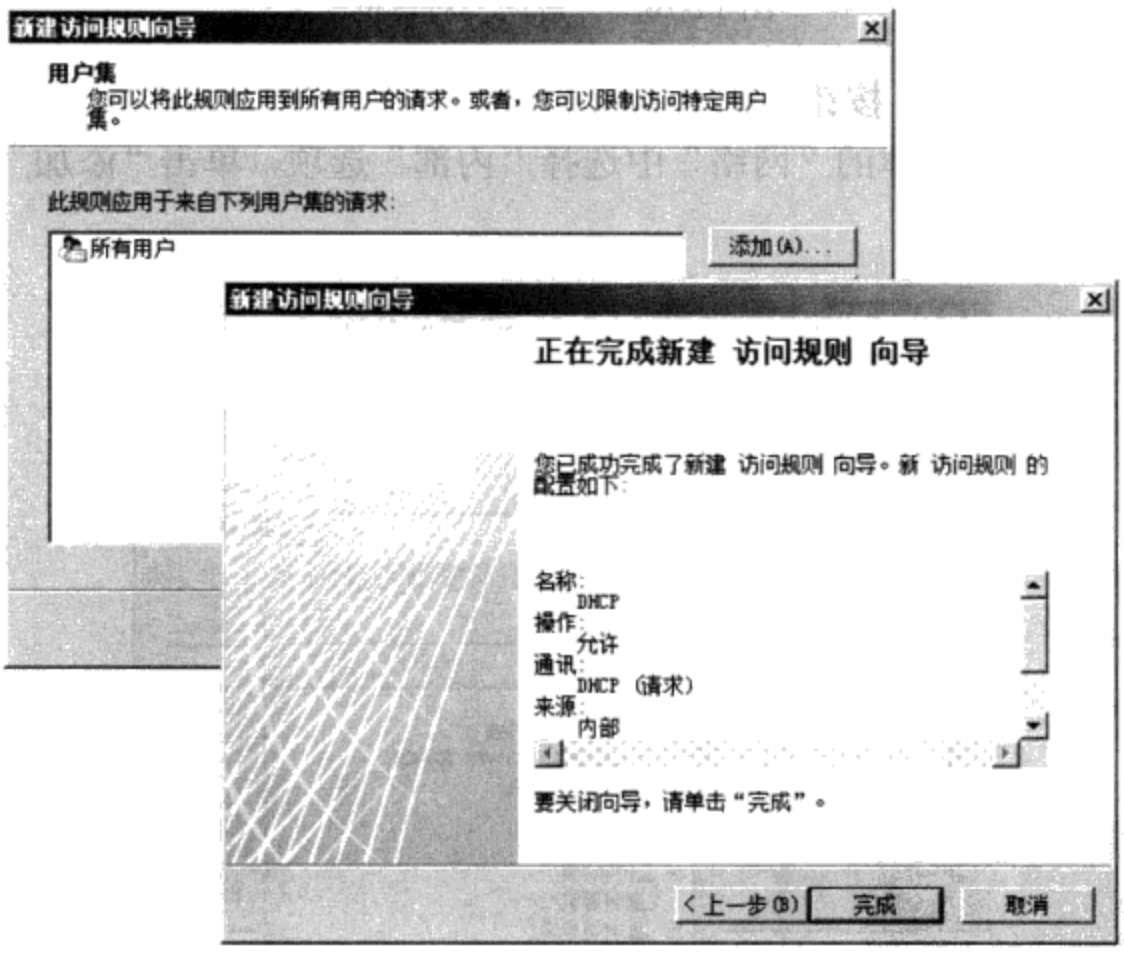


图 11-77 “用户集”对话框

第 6 步，使用相同操作再创建一条 DHCP 答复规则，与 DHCP 请求规则所不同的是，在“协议”中，设置所使用的协议为“DHCP 答复”，访问规则源为“本地主机”，而访问规则目的为“内部”，如图 11-78 所示。

第 7 步，最后在 Forefront TMG 的主窗口中单击“应用”按钮，使规则生效即可，如图 11-79 所示。

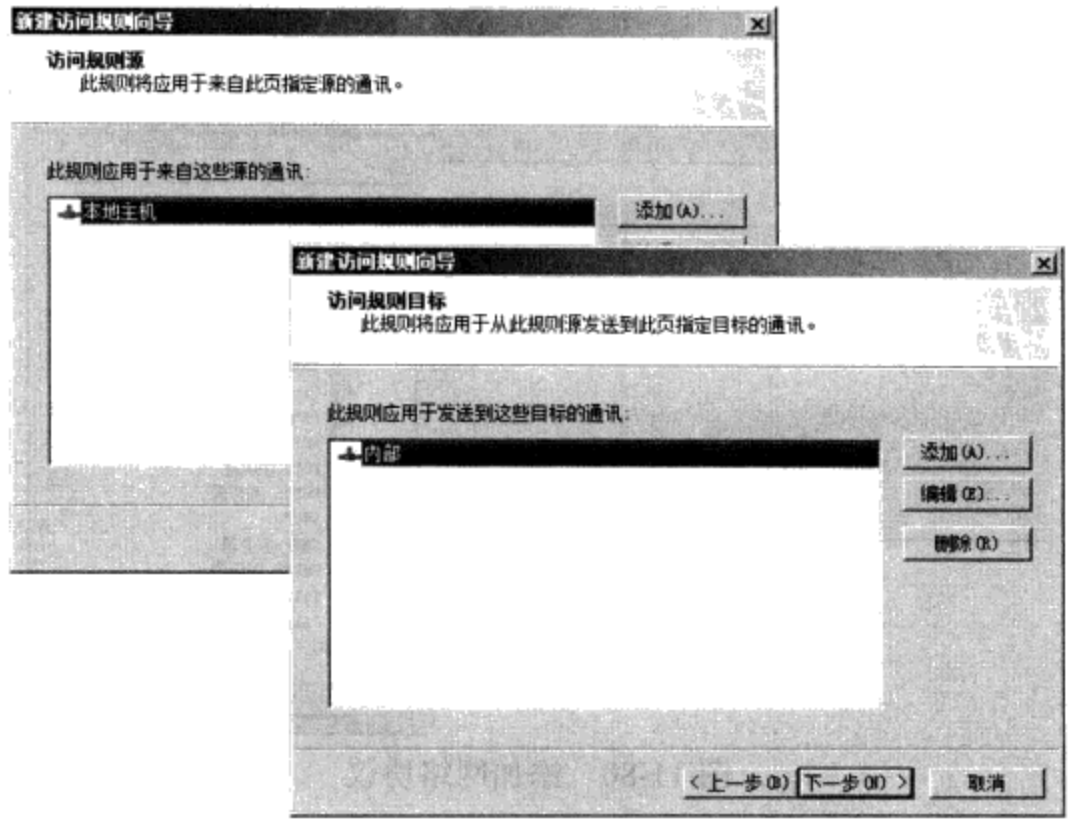


图 11-78　DHCP 答复规则

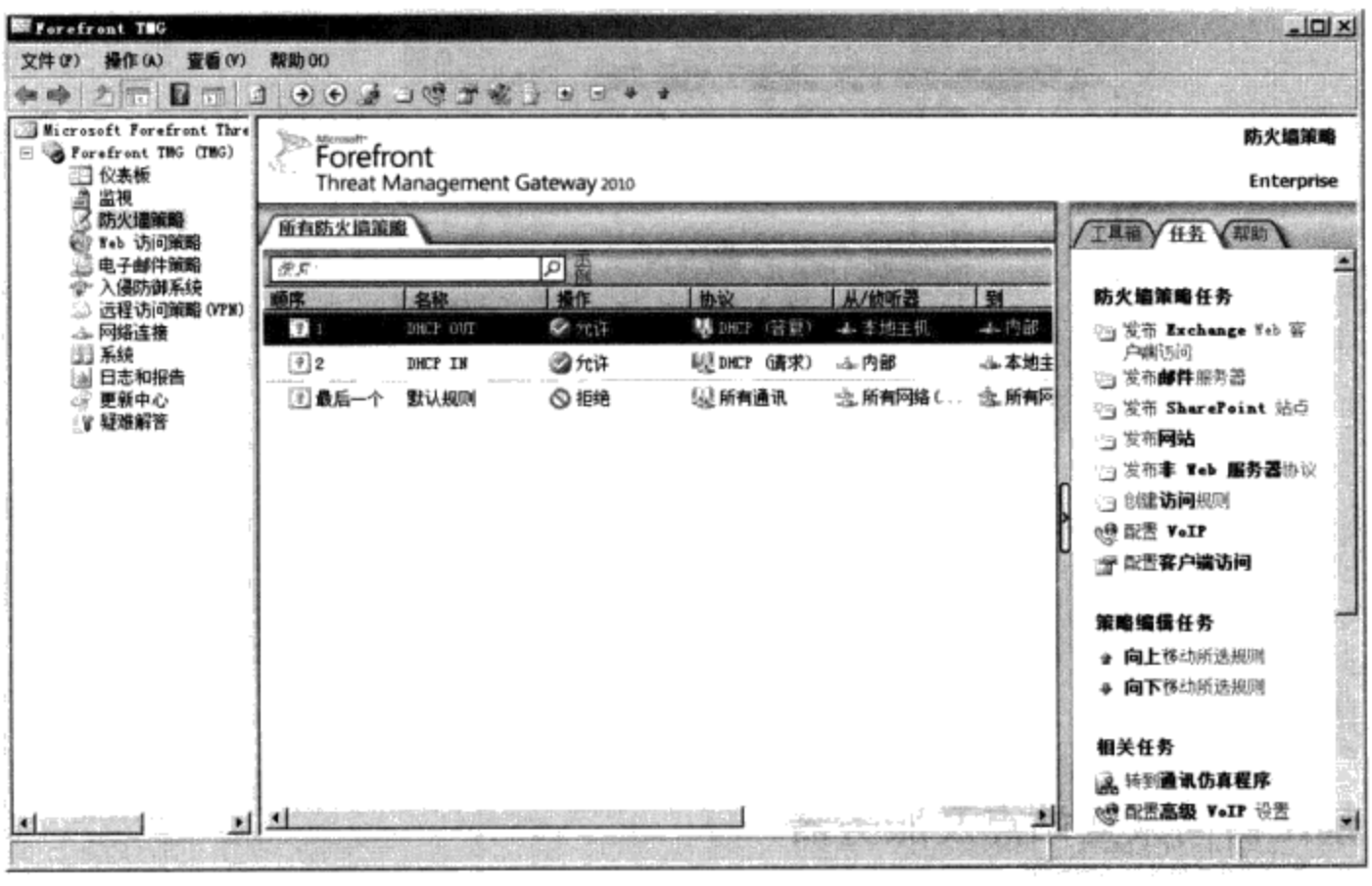


图 11-79　DHCP 服务规则

2. 配置允许的 Internet 应用

默认情况下，Forefront TMG 是不允许内部网络访问外部网络的，要实际使用中需要根据网络需要添加允许的 Internet 应用规则。具体配置操作与配置 DHCP 服务器相似，需要注意的是，在“协议”对话框需要根据允许的 Internet 应用添加相应的协议，如图 11-80 所示。

在“访问规则源”中添加“内部”，在“访问规则目标”中添加“外部”，如图 11-81 所示。

在完成规则的创建后，单击“应用”按钮，使新建的规则生效。

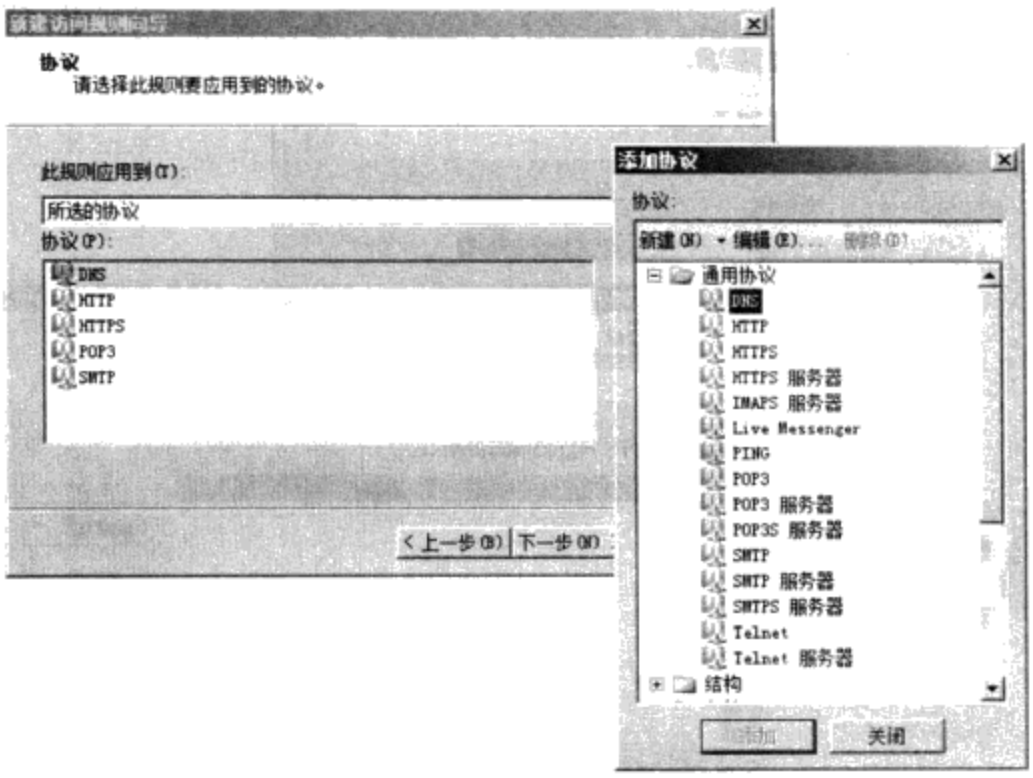


图 11-80　添加网络协议

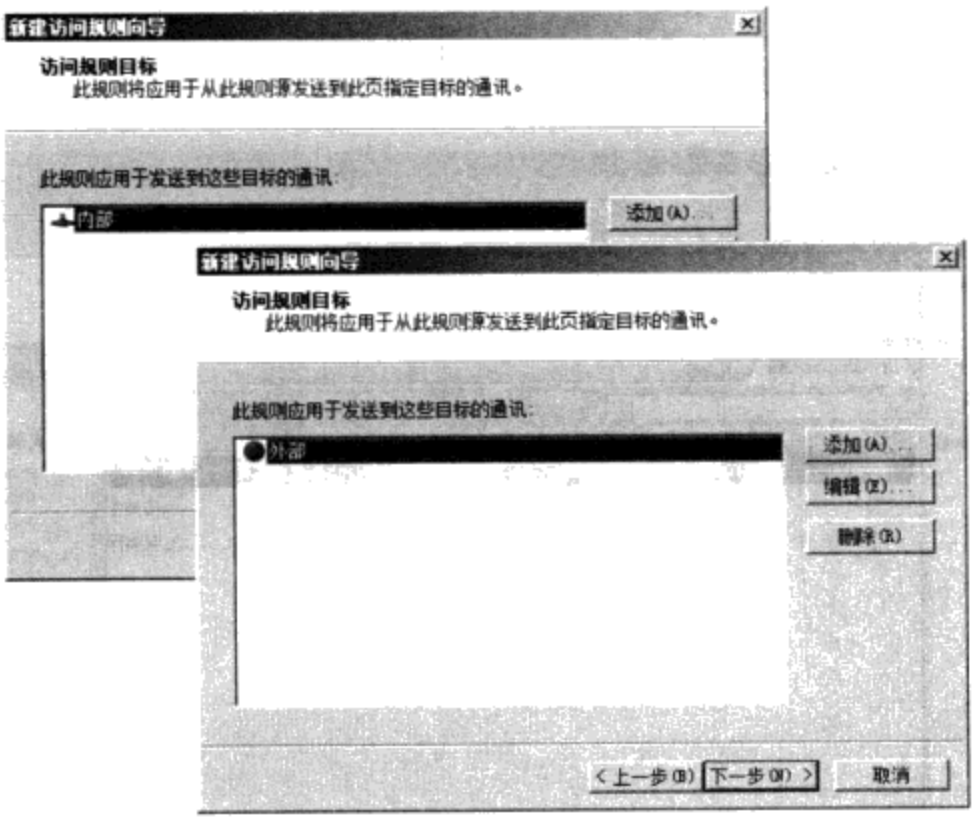


图 11-81　访问规则

3. 禁止访问某些站点及服务器

在当前网络环境下，有很多网站中被黑客植入的了病毒，这些网站显然是禁止访问的。另外，对于某些娱乐网站、门户网站，可能也是禁止访问的网站之内。这里以禁止讯雷网站和搜狐网站为例进行介绍。

第1步，打开 Forefront TMG 防火墙，右击“防火墙策略”，在快捷菜单中依次选择“新建”→“访问规则”，在打开对话框的访问规则名称中输入“禁止网站”。

第 2 步，单击“下一步”按钮，在“规则操作”对话框中，选择“拒绝”单选按钮，在“协议”对话框中选择“所有出站通信”。

第3步，单击“下一步”按钮，在“访问规则源”中单击“添加”按钮，添加“内部”，在“访问规则目标”对话框中，单击“添加”按钮，在“添加网络实体”中，单击“新建”按

钮，在打开的菜单中选择“URL 集”，如图 11-82 所示。在打开的“新建 URL 集规则元素”对话框中，输入 URL 集的名称，然后在下面单击“添加”按钮，将要禁止的站点加入其中。

第 4 步，添加完成后，单击“确定”返回到“添加网络实体”对话框，然后在对话框中选择“URL 集”下面新建的“禁止访问站点地址”，单击“添加”按钮，如图 11-83 所示。添加完毕后单击“关闭”按钮，然后在“访问规则目标”对话框中，单击“下一步”按钮继续。

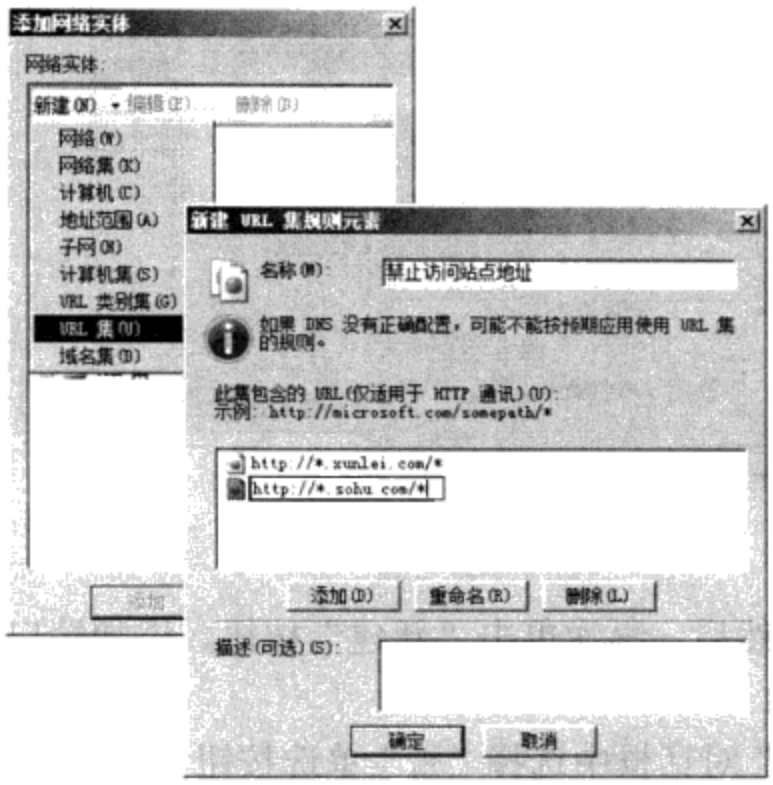


图 11-82　新建 URL 集

图 11-83　添加网络实体

第 5 步，在“用户集”对话框中，保持默认设置，即对所有用户有效。单击“下一步”按钮继续，最后单击“完成”按钮。

第 6 步，在 Forefront TMG 窗口中，单击“应用”按钮使规则生效。

这样 Forefront TMG 内部的计算机就不能访问这些站点了，如果还有其他要禁止访问的站点可以在“新建 URL 集规则元素”中一并加入。

4. 禁止某些通信软件

随着网络的盛行，很多人都喜欢使用聊天软件。但在企业中，为了不影响用户的工作，往往禁止在上班时上网聊天。这可以在 Forefront TMG 中进行限制。Forefront TMG 默认提供了 AOL、ICQ、IRC、Net2Phone、MSN Messenger 等软件的协议，而对于一些国内即时通信软件却没有提供，如 QQ、UC 等，需要由用户手动添加。

■ 添加 QQ 和 UC 协议

QQ 使用 UDP 和 TCP 协议的 4000～4001 和 8000 端口。而 UC 使用 UDP 协议，端口为 3001 到 3002。需要在 TMG 中添加 QQ 和 UC 的协议，准备创建禁用规则。

第 1 步，打开 TMG 的“防火墙策略”窗口，在右侧列表中切换到“工具箱”选项卡，并选择“协议”选项组，如图 11-84 所示。单击“新建”按钮，选择下拉菜单中的“协议”选项。

第 2 步，在“首要连接信息”对话框中，用来设置端口号和协议。单击“新建”按钮，显示如图 11-85 所示“新建/编辑协议连接”对话框，各选项配置如下：

- 协议类型：在下拉列表框中选择“UDP”选项。
- 方向：在下拉列表框中选择“发送接收”选项。

- 端口范围：分别键入4000和4010。

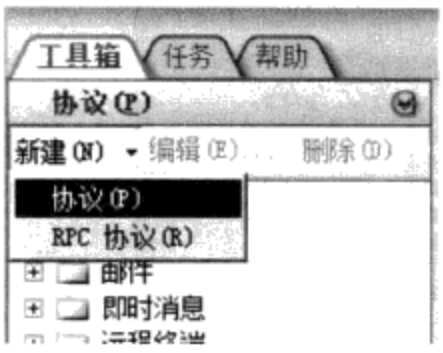


图 11-84 “协议”选项组

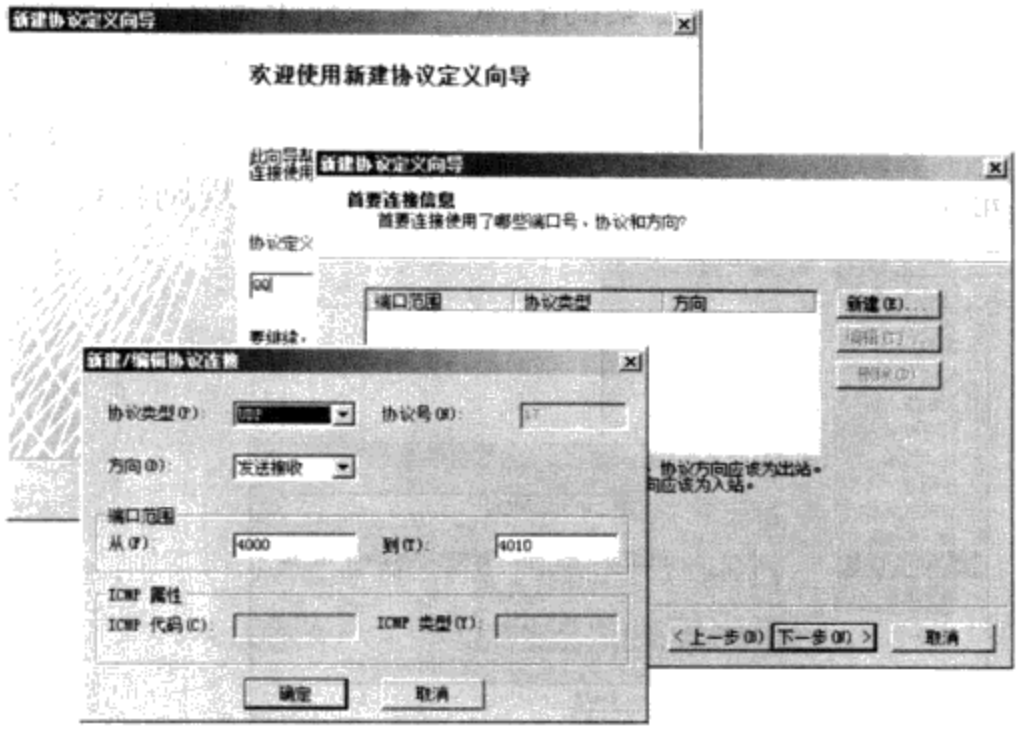


图 11-85 新建 QQ 协议

第 3 步，单击“确定”按钮，确认并返回。然后，再次单击“新建”按钮，添加端口范围为 8000~8010 的“UDP”协议。

第 4 步，单击“下一步”按钮，在“辅助连接”对话框中选择“否”单选按钮，如图 11-86 所示。在“正在完成新建协议定义向导”对话框中，单击“完成”按钮即可。

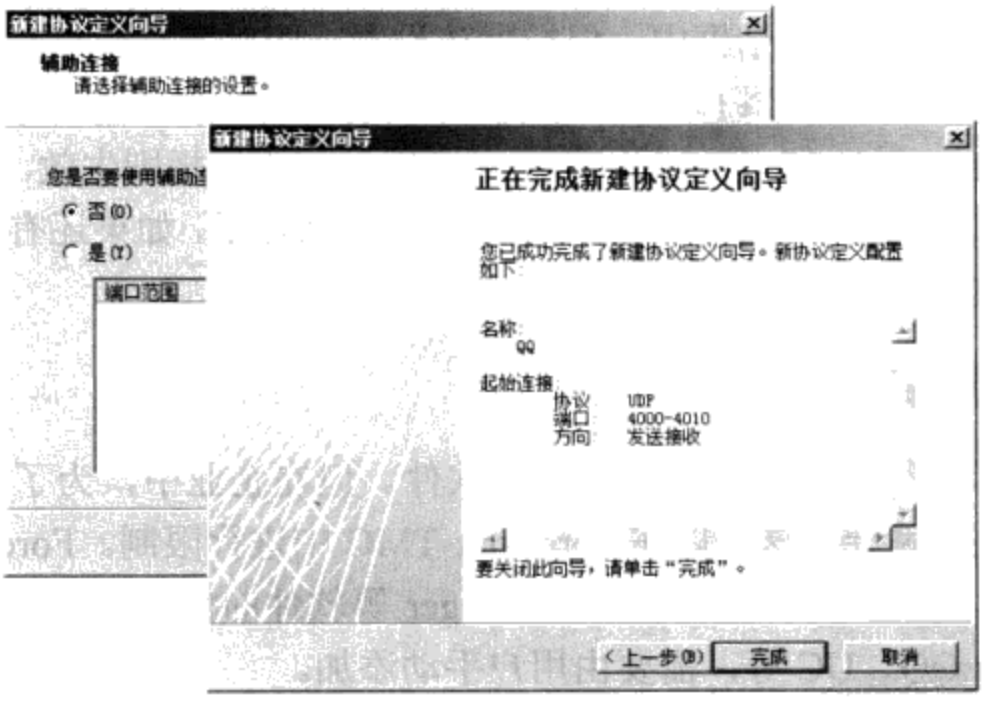


图 11-86 “辅助连接”对话框

第 5 步，再次运行“新建协议定义向导”，添加 UC 协议。UC 协议的“协议类型”为 UDP，“方向”为“发送接收”，“端口范围”为 3000 到 3002。添加完成的 QQ 和 UC 协议将显示在“防火墙策略”的“用户定义”列表框中。

■ 添加防火墙规则

要限制内网用户使用 QQ、UC 等即时通信软件，还需要添加一条规则，拒绝所添加的 QQ 和 UC 协议的通信，从而使内网中的用户无法登录 QQ 和 UC。

第 1 步，在“防火墙策略”窗口中，运行“新建访问规则向导”。在“规则操作”对话框

中选择“拒绝”单选按钮；在“协议”对话框中，单击“添加”按钮，在“通用协议”列表框中选择“Live Messager”选项，在“用户定义”列表框中选择 QQ 和 UC 协议，如图 11-87 所示。

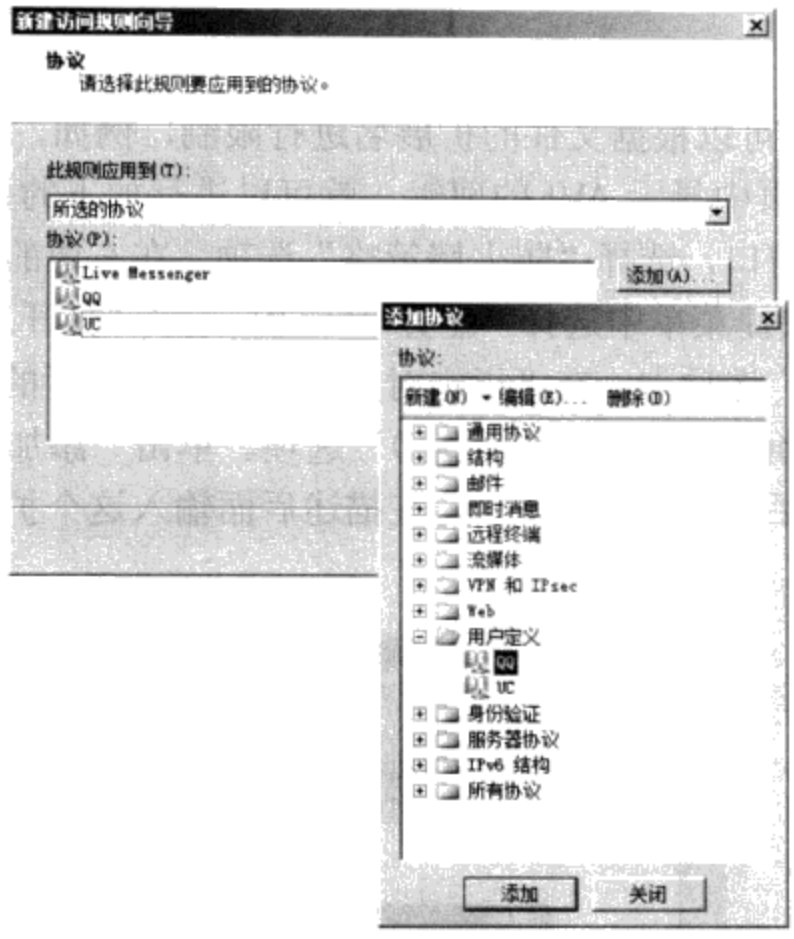


图 11-87　添加 QQ 和 UC 协议

第 2 步，连续单击“下一步”按钮，在“访问规则源”对话框中添加“内部”选项；在“访问规则目标”对话框中添加“外部”选项。

第 3 步，规则创建完成以后，还可设置时间计划，设置为只在上班时间禁用 QQ 和 UC。右击规则在快捷菜单中选择“属性”选项，并切换到“计划”选项卡。默认情况下，在“计划”下拉列表框中已经提供了常用的时间列表，如果符合用户要求可直接使用。也可单击“新建”按钮，创建新的时间表。打开“新建计划”对话框，在“名称”文本框中，键入所要创建的时间表名称，在下方时间设置中根据实际需要进行设置即可，如图 11-88 所示。

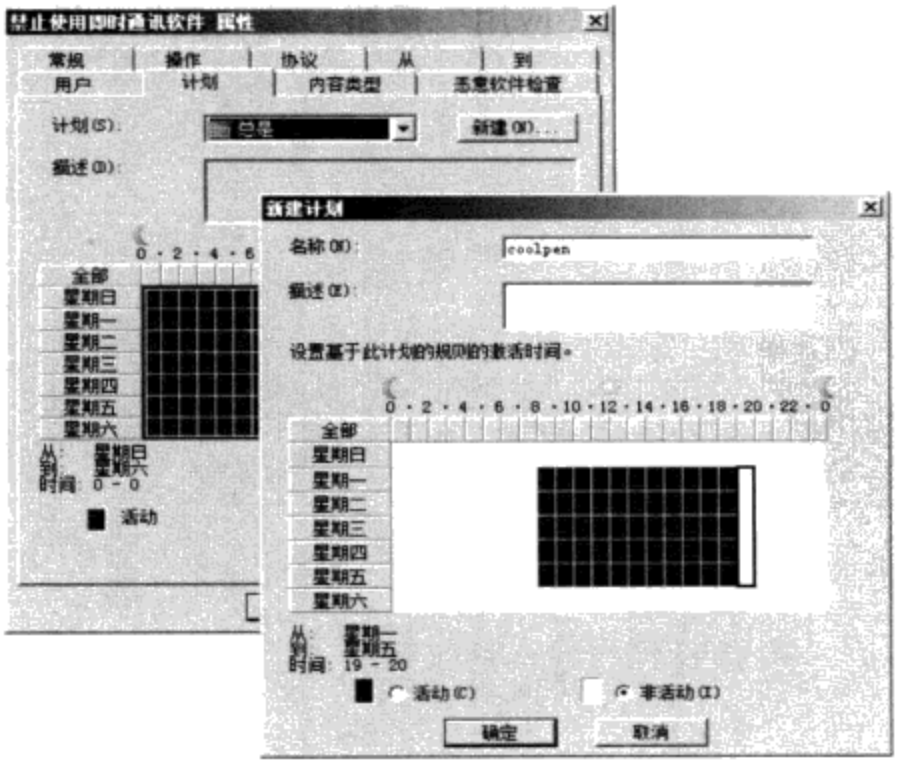


图 11-88　“计划”选项卡

第 4 步，依次单击“确定”按钮保存，并单击“应用”按钮使规则生效。这样，在上班时间，用户就不能使用 QQ 和 UC 软件了。

5. 阻止某些文件

使用 HTTP 过滤器，可以根据文件的扩展名进行限制，例如，不想在网页中显示 Flash 动画，或者不想在当前网页中显示 AVI 的剪辑，就可以进行如下的操作来限制这些文件。

打开 Forefront TMG 窗口，选择“防火墙策略”选项，在右边的窗口中，右击创建的允许访问 Internet 的规则，在快捷菜单中选择“配置 HTTP”选项，打开“为规则配置 HTTP 策略”对话框，切换到“扩展名”选项卡。在“指定对文件扩展名要执行的操作”下拉列表框中，选择“阻止指定的扩展名（允许所有其他扩展名）”选项。单击“添加”按钮，在打开的“扩展名”对话框中，在扩展名后面输入“.SWF”，在描述后面输入这个扩展名的简单描述文字，如图 11-89 所示。

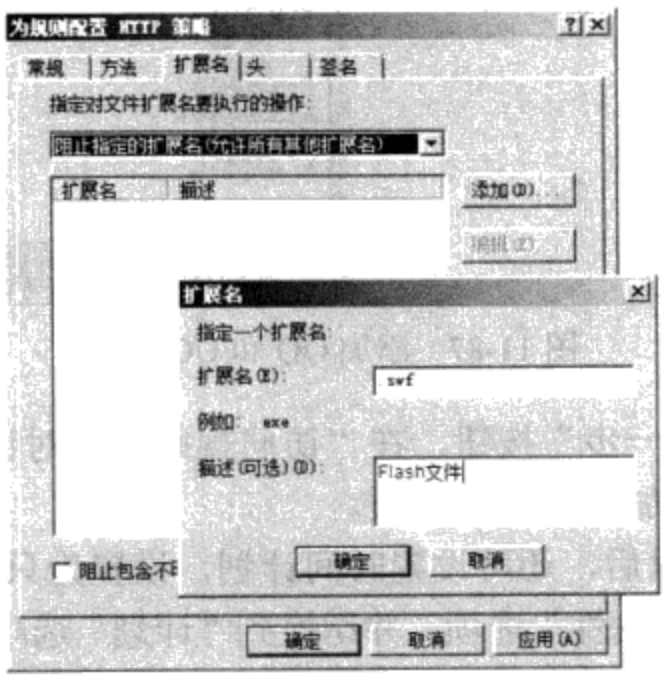


图 11-89　设置阻止的扩展名

设置完成后单击“确定”按钮，如果想添加其他扩展名可以使用如上操作添加，添加完成后，在 Forefront TMG 窗口中，单击“应用”按钮，使设置生效即可。

第 12 章　入侵检测系统

入侵检测系统是局域网安全的重要组成部分，其主要功能就是发现入侵行为，并及时向管理员发出报警。这种检测既可以基于专业的入侵检测设备（如 Cisco IDS）实现，也可以基于软件（如 Snort 等）实现。随着入侵防御设备、网络防火墙等安全设备功能的不断完善，入侵检测设备正在逐渐消失，而基于软件的实现方式则比较灵活，且实现成本低。本章主要介绍如何借助 Snort 和 Sniffer 来帮助管理员快速发现网络入侵情况。

12.1　入侵检测系统概述

入侵检测系统（Intrusion Detection Systems，IDS）是网络安全体系的一部分，是网络防火墙的合理补充，可以扩展系统管理员的安全能力（包括安全审计、监视、攻击识别和响应）、提高网络安全基础结构的完整性。入侵检测通过迅速地检测入侵，在可能造成系统损坏或数据丢失之前，识别并驱除入侵者，使系统迅速恢复正常工作，并且阻止入侵者进一步的行动。同时，收集有关网络入侵的信息，用于改进和增强系统抵抗入侵的能力。

12.1.1　入侵检测系统架构

入侵检测涵盖的内容非常广泛，专业的入侵检测设备、入侵检测软件可以称为入侵检测系统，Windows 事件查看器、网络服务运行日志等都可以视为入侵检测系统的一部分，本章中介绍的入侵检测系统主要是指专业化的网络入侵检测软件，如 Snort、Sniffer 等。根据应用环境和被保护目标的不同，入侵检测系统分为多种架构。

1.　基于网络的 IDS

基于网络的 IDS 一般安装在需要保护的网段中，利用网络侦听技术实时监视网段中传输的各种数据包，并对这些数据包的内容、源地址、目的地址等进行分析和检测。如果发现入侵行为或可疑事件，IDS 就会发出警报甚至切断网络连接。

基于网络的 IDS 具有以下优点：

- 检测速度快。于网络的监测器通常能在微秒或秒级发现问题，检测精度非常高。
- 易于安装和实施。常只需要将程序在主机上安装一次，即可用来保护本网段内的所有主机。

基于网络的 IDS 尤其适合阻止扫描和拒绝服务攻击。但是，在扫描大型网络时会使主机的性能急剧下降。

2.　基于主机的 IDS

基于主机的 IDS 安装在被保护的计算机上，通常用于保护运行关键应用的服务器。它通过监视与分析主机的审计记录和日志文件来检测入侵行为。

基于主机的IDS具有以下优点：

- 性价比高。主机数量较少的情况下，这种部署方式可以在满足应用需求的情况下，减少企业开支。
- 更加细致。种方法可以很容易地监测一些活动，如对敏感文件、目录、程序或端口的存取，而这些活动很难在基于协议的线索中发现。
- 视野集中。旦入侵者得到了一个主机用户名和口令，基于主机的代理是最有可能区分正常的活动和非法的活动的。
- 对网络流量不敏感　用代理的方式一般不会因为网络流量的增加而丢掉对网络行为的监视。

3. 分布式IDS

分布式入侵检测系统是由分布在网络中的多个入侵检测系统所构成，该系统中的IDS通过彼此间的通信和协调来协同展开各种数据采集、分析和事件检测活动，共同实现对整个网络全面有效的监控。分布式IDS能够在数据收集、入侵分析和自动响应方面最大限度地发挥系统资源的优势，其设计模型也具有很大的灵活性。

12.1.2 入侵检测系统的功能

通常情况下，一个入侵检测系统由4部分组成：事件产生器（Event generators）、事件分析器（Event analyzers）、响应单元（Response units）和事件数据库（Event databases）。

事件产生器的功能是从整个计算环境中捕获事件信息，并向系统的其他组成部分提供该事件数据。事件分析器分析得到的事件数据，并产生分析结果。响应单元则是对分析结果做出反应的功能单元，它可以做出切断连接、改变文件属性等有效反应，当然也可以只是报警。事件数据库是存放各种中间和最终数据的地方的统称，用于指导事件的分析及反应，它可以是复杂的数据库，也可以是简单的文本文件。

入侵检测系统能主动发现网络中正在进行的针对被保护目标的恶意滥用或非法入侵，并能采取相应的措施及时中止这些危害，如提示报警、阻断连接、通知网管等。

其主要功能是监测并分析用户和系统的活动、核查系统配置中的安全漏洞、评估系统关键资源与数据文件的完整性、识别现有已知的攻击行为或用户滥用、统计并分析异常行为、对系统日志的管理维护。

12.1.3 入侵检测的一般步骤

1. 入侵数据获取

主要是为系统提供数据，提取的内容包括系统、网络、数据及用户活动的状态和行为。入侵检测数据提取可来自以下4个方面：

- 系统和网络日志。
- 目录和文件中的改变。
- 程序执行中的不期望行为。

- 物理形式的入侵信息。

2. 入侵数据分析

主要作用在于对数据进行深入分析，发现攻击并根据分析的结果产生事件，传递给事件响应模块。常用技术手段有：模式匹配、统计分析和完整性分析等。入侵数据分析是整个入侵检测系统的核心模块。

3. 入侵事件响应

事件响应模块的作用在于报警与反应，响应方式分为主动响应和被动响应。

被动响应型系统只会发出报警通知，将发生的不正常情况报告给管理员，本身并不试图降低所造成的破坏，更不会主动地对攻击者采取反击行动。

主动响应系统可以分为对被攻击系统实施保护和对攻击系统实施反击的系统。

12.1.4 常用入侵检测工具

在本地计算机或网络实施入侵检测并不难，关键是选对适用与检测目标和本地环境的入侵检测工具。

1. Snort

Snort 是最常用的入侵检测工具之一，适用于 Linux、Windows 等多种系统平台，其代码完全开源，倍受众多用户青睐。Snort 采用灵活的基于规则的语言来描述通信，将签名、协议和不正常行为的检测方法结合起来。通过协议分析、内容查找和各种各样的预处理程序，Snort 可以检测成千上万的蠕虫、漏洞利用企图、端口扫描和各种可疑行为。需要注意的是，用户需要检查免费的基础数据库来分析 Snort 的警告。

2. OSSEC

OSSEC 是一款基于主机的入侵检测工具，它可以执行日志分析、完整性检查、Windows 注册表监视、rootkit 检测、实时警告以及动态的适时响应。除了其 IDS 的功能之外，通常还可以被用作一个 SEM/SIM 解决方案。因为其强大的日志分析引擎，倍受 ISP、大型校园网、企业网络和数据中心用户的欢迎，以监视和分析其防火墙、IDS、Web 服务器和身份验证日志。

3. Sguil

Sguil 是一款被称为网络安全专家监视网络活动的控制台工具，它可以用于网络安全分析。其主要部件是一个直观的 GUI 界面，可以从 Snort/barnyard 提供实时的事件活动。还可借助于其他的部件，实现网络安全监视活动和 IDS 警告的事件驱动分析。

4. Sniffer

Sniffer 是一种基于被动侦听原理的网络入侵检测工具，可以监视网络的状态、数据流动情况以及网络上传输的信息。当信息以明文的形式在网络上传输时，便可以使用网络监听的方式来进行攻击。将网络接口设置在监听模式，便可以将网上传输的源源不断的信息截获。Sniffer

技术被广泛地应用于入侵检测分析、故障诊断、应用性能分析和网络安全保障等各个领域。

12.2 Snort

Snort是一款开源式入侵检测软件，用于监视网络传输量的网络型入侵检测系统。其主要工作是捕捉流经网络的数据包，一旦发现与非法入侵的组合一致，便向管理员发出警告。Snort同时适用于Linux系统和Windows系统，可以帮助用户实施基于各种网络协议的入侵检测。

12.2.1 Snort概述

1. Snort主要功能及特点

Snort具有很好的扩展性和可移植性，主要提供3种功能，即数据包嗅探器、数据包记录器和网络入侵检测。其特点如下：

- Snort是一个跨平台、轻量级的网络入侵检测软件。
- Snort采用基于规则的网络信息搜索机制，对数据包进行内容的模式匹配，从中发现入侵和探测行为。
- Snort具有实时数据流量分析和监测IP网络数据包的能力，能够进行协议分析，对内容进行搜索/匹配。它能够检测各种不同的攻击方式，对攻击进行实时报警。它还可以用来截获网络中的数据包并记录数据包日志。
- Snort的报警机制丰富。
- Snort的日志格式既可以是二进制格式，也可以解码成ASCII字符形式，便于用户检查。
- Snort使用一种简单的规则描述语言，能够很快对新的网络攻击做出反应。
- Snort支持插件。可以使用具有特定功能的报告、检测子系统插件对其功能进行扩展。

2. 基于Windows系统的Snort环境需求

在Windows Server 2008系统中部署Snort入侵检测系统前，必须确保已经完成如下准备工作：

- 安装IIS服务组件。
- 安装SQL Server服务器。
- 配置IIS支持PHP。

3. Snort的组成

Snort入侵检测系统由以下4部分组成：

- 数据包解码器。据包解码器主要是对各种协议栈上的数据包进行解析、预处理，以便提交给检测引擎进行规则匹配。
- 检测引擎。nort用一个二维链表存储其检测规则，一维称为规则头，另一维称为规则选项。规则匹配查找采用递归的方法进行，检测机制只针对当前已经建立的链表选项进行检测。

- 日志子系统。nort 可供选择的日志形式有 3 种：文本形式、二进制形式和关闭日志服务。
- 报警子系统。警形式有 5 种：报警信息可发往系统日志、用文本形式记录到报警文件中去、用二进制形式记录到报警文件中去、通过 Samba 发送 WinPopup 信息、以及关闭报警。

12.2.2 Snort 语法及参数

Snort 安装完成后，在其安装目录的“bin”子目录中“snort”的执行文件，即是 Snort 的可执行文件。使用“./snort –h”命令，可以查看该可执行文件的详细帮助信息。snort 命令的命令格式为：

snort [选项]

Snort 命令行选项的作用如下。

- -A <记录模式>：括 full、fast 和 none 三种模式。其中，“full”模式是以标准模式记录到 alert 文件中；“fast”模式只写入时间戳、messages、IPs、ports 到文件中；“None”模式的功能则是关闭报警。
- -a：示 ARP 包。
- -b：LOG 的信息包记录为 TCPDUMP 格式，所有信息包都被记录为两进制形式，建议与 fast 记录模式配合使用，这样不需要花费时间将包的信息转化为文本。
- -c <配置文件>：个配置文件将为系统指定信息要 LOG、报警等配置。
- -C：用 ASCII 码显示信息包信息，而不是 hexdump。
- -d：码应用层。
- -D：守护进程的方法来运行“snort”，默认情况下“ALERT”记录发送到“/var/log/snort.alert”文件中。
- -e：示并记录 2 个信息包头的数据。
- -F <bpf 文件>：指定的<bpf>文件中读 BPF 过滤器。
- -h <网络地址>：定网络地址，启用这个选项后，会使用箭头的方式表示数据进出的方向。
- -I <if>：用网络接口参数<if>。
- -l <ld>：LOG 信息包记录到<ld>目录中去。
- -M <wkstn>：送 WinPopup 信息到<wkstn>文件中所列出的工作站。
- -n <num>：定在处理<num>个数据包后退出。
- -N：闭 LOG 记录。
- -o：变记录文件的方式，默认采用 Alert->Pass->Log order 的顺序记录文件，当使用“-o”选项后，则采用 Pass->Alert->Log order 的顺序记录文件。其中，Pass 为允许通过的规则而不记录和报警，ALERT 是不允许通过的规则，LOG 指 LOG 记录。
- -p：闭混杂模式嗅探方式，此时可更安全的调试网络。
- -r <tf>：取 tcpdump 方式产生的文件<tf>。
- -s：LOG 报警记录到 syslog 中，在 Linux 操作系统中，这些警告信息会出现在“/var/log/secure”文件中，在其他操作系统中将记录到“/var/log/message”文件中。

- -S <n=v>：置用来在命令行定义“Snort rules”文件中的变量，如果要在“Snort rules”文件中定义变量“HOME_NET”，则可在命令行中预定义变量值。
- -v：用“verbose”模式，把信息包显示在屏幕上。需要注意的是，该选项后会使计算机速度变慢，在记录比较多时还可能出现丢包现象。
- -V：示“snort”命令的版本并退出。
- -?：示“snort”命令帮助信息。

12.2.3 部署 snort 入侵检测系统

用户可以通过多种方式在 Windows 系统中部署 snort 入侵检测系统，它可以基于不同的数据库、系统环境以及数据分析平台，例如“IIS+SQL Server+PHP”环境、“Apache+MySQL+BASE”环境、“Apache+MySQL+ACID”环境等。本例中的环境为“Apache+MySQL+ACID”，部署 snort 之前，必须做好相应的准备工作。

1. 准备所需工具

在 Windows Server 2008 系统中部署 Snort 入侵检测系统需要用到如下软件：

- Apache。供 Web 管理方式，通过浏览器查看入侵检测分析结果。
- Acid。基于 PHP 的入侵检测数据库分析控制台。
- ADodb。提供 PHP 所需的 ADodb 数据库。
- JPGRAPH。PHP 环境中的图形库。
- MySQL。提供 Windows 平台下的 PHP 脚本环境支持。。
- PHP。为数据分析平台提供运行环境。
- WinPcap。Windows 平台的 PCAP，配置网络适配器的工作模式。
- SnortRules。为入侵检测提供分析和判断依据。

提示 为了便于配置和管理，建议将所有工具安装在同一目录下，如 C:\IDS\等。

2. 安装 Apache 服务器

Apache 服务器的安装过程比较简单，只需根据向导提示完成相应操作即可，这里不做详细介绍。另外，用户也可以直接下载 Apache 服务器的绿色版本，解压缩后即可使用。

3. 安装 PHP

PHP 环境广泛应用于 Linux、Windows 等各种系统平台，因此下载时应注意选择适用的版本。本实例中采用的是“Apache+PHP”配合使用，所以选择 VC6 版本，如果是 Windows 平台下“IIS+PHP”配合使用，建议下载 VC9 版本。另外，VC6 版本又分为 NTS（Non Thread Safe）和 TS 两种版本，建议下载 TS 版本。

第 1 步，将下载的 PHP 压缩包解压缩到 C:\ids\php5\目录下，如图 12-1 所示。在该目录下，将 php5ts.dll 文件到 C:\Windows\system32\目录下，将 php.ini-dist 文件到 C:\Windows\目录下并

重命名为 php.ini。

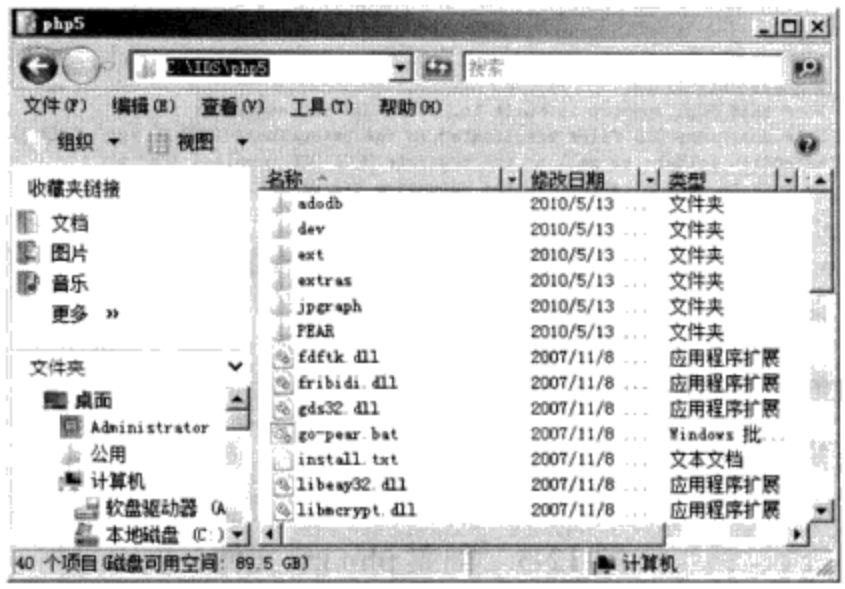


图 12-1 PHP 的安装路径

第 2 步，配置 Apache 对 PHP 的支持。使用记事本或者写字板，打开 C:\ids\apache\conf\httpd.conf 文件，在如图 12-2 所示位置分别插入如下语句。

```
loadmoudle php5_module c:\ids\php5\php5apache2_2.dll
addtype application/x-httpd-php .php
```

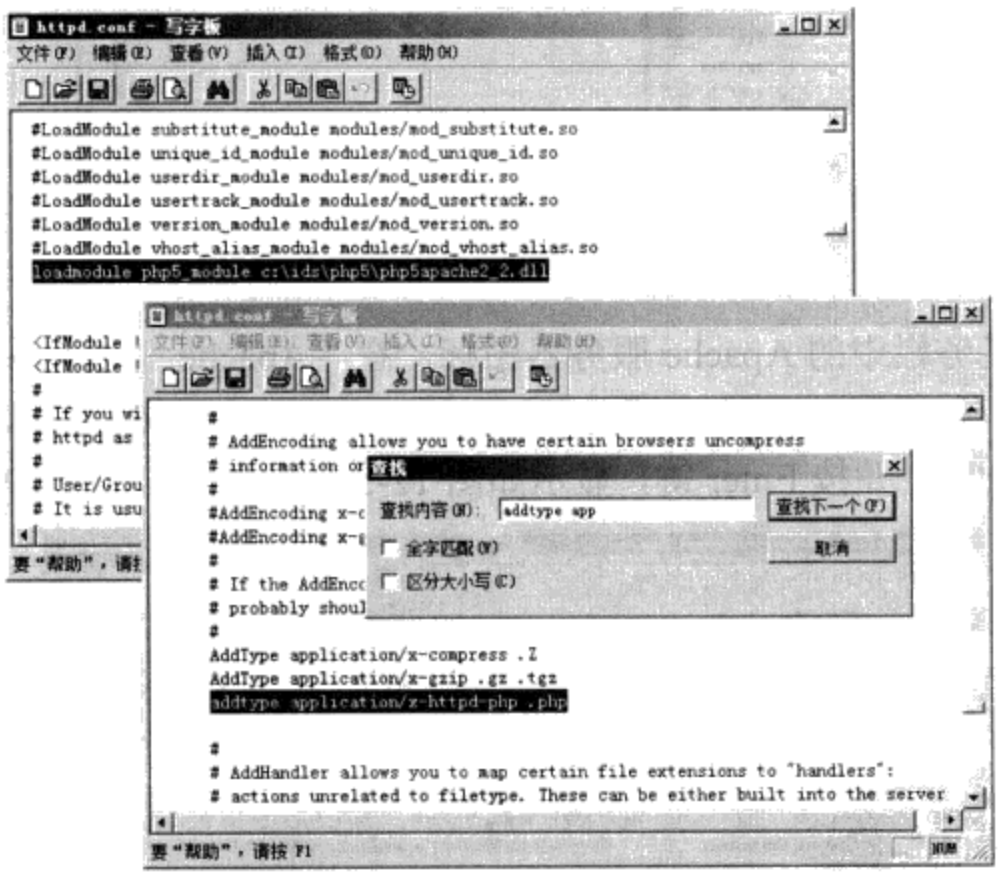


图 12-2 配置 Apache 对 PHP 的支持

第 3 步，修改 C:\Windows\php.ini 文件，激活“extension=php_gd2.dll”语句，即删除其前面的分号，如图 12-3 所示。另外，将 C:\ids\php5\ext\目录下的 php_gd2.dll 复制到 C:\Windows\目录下。

第 4 步，配置 PHP 测试页。在 C:\ids\apache\htdocs\目录下，打开 test.php 文件，将其内容修改为“<?php phpinfo(); ?>”，如图 12-4 所示。

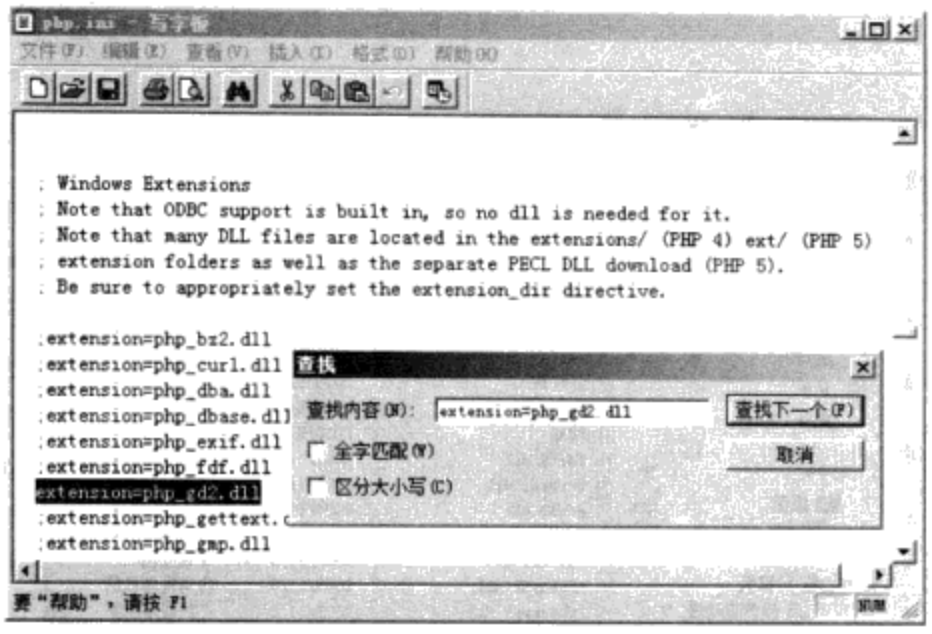


图 12-3　配置 php.ini 文件

图 12-4　配置 PHP 测试页

第 5 步，双击任务栏中的 Apache 服务器图标，在“Apache　Services Monitor”窗口中，单击“Restart”按钮重新启动 Apache 服务器。打开 IE 浏览器，在地址栏中输入“http://127.0.0.1/test.php”并按 Enter 键，显示如图 12-5 所示窗口，即 PHP 环境配置成功完成。

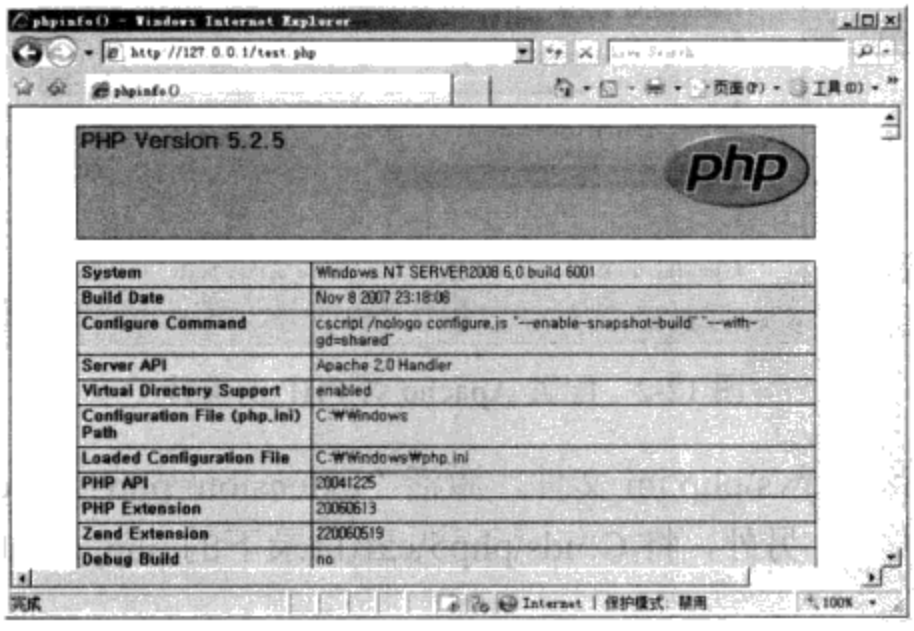


图 12-5　测试 PHP 环境

4. 安装 WinPCAP

WinPCAP 的主要功能在于独立于主机协议而发送和接收原始数据包。WinPCAP 不能阻

塞、过滤或控制其他应用程序数据包的发收，只是监听共享网络上传送的数据包。基于 Windows 平台的 Snort 入侵检测系统中的 WinPCAP 安装非常简单。需要注意的是，在如图 12-6 所示“Installation options”对话框中，选中“Automatically start the WinPcap driver at boot time”复选框，使 WinPcap 能够开机自动运行。

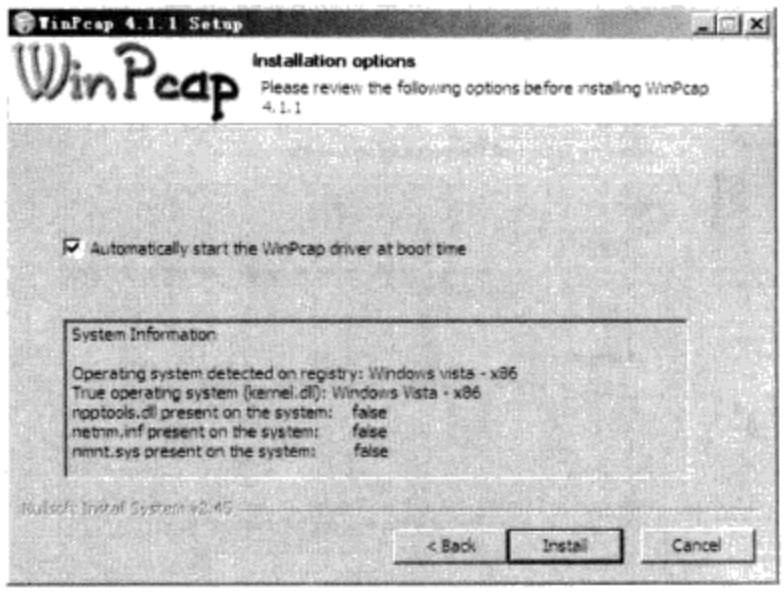


图 12-6 “Installation options”对话框

安装完成后，还必须向 Windows 系统中增加新的与之对应的用户环境变量并赋值。打开“系统属性”对话框，在“高级”选项卡中单击“环境变量”按钮，显示“环境变量”对话框。在“Administrator 的用户变量”选项区域单击“新建”按钮，显示“新建用户变量”对话框，在“变量名”文本框中输入“PCAP_FRAMES”，在“变量值”文本框中输入“MAX”，连续单击“确定”按钮，保存设置。配置结果如图 12-7 所示。

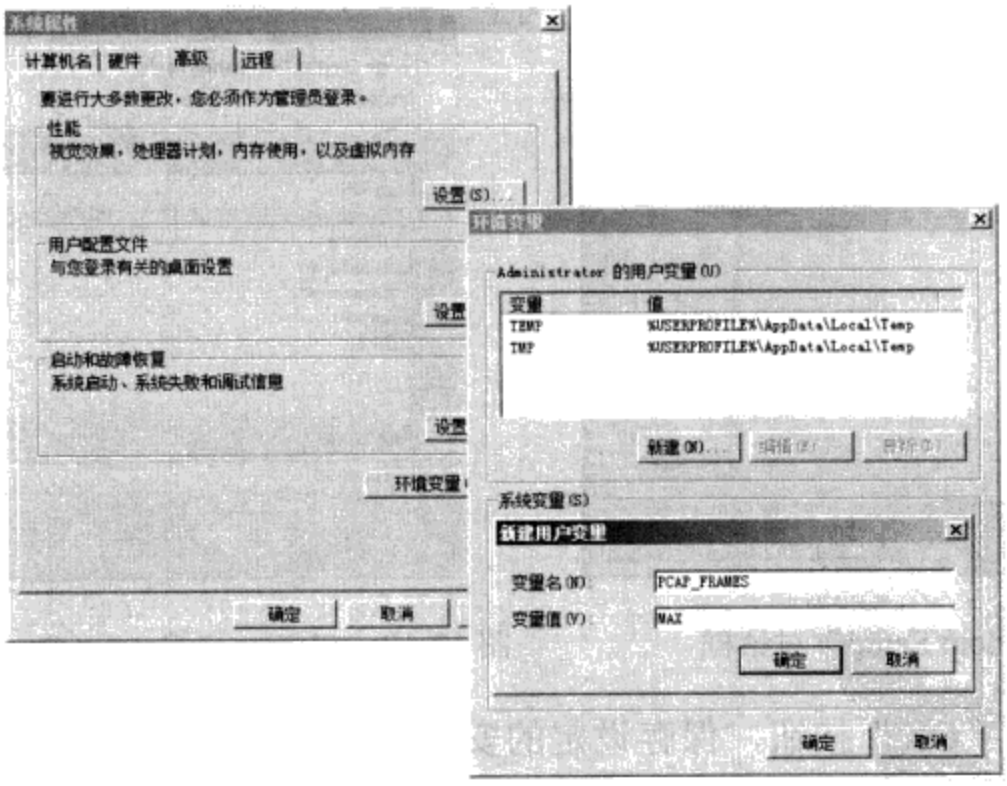


图 12-7 配置用户环境变量

5. 安装与配置 MySQL

MySQL 数据库有多种格式，建议下载安装格式的 MySQL，以便通过向导完成基本配置任务。

第1步，运行MySQL Server安装文件，启动“MySQL Server 5.0 – Setup Wizard”向导，直接单击“Next”按钮，显示如图12-8所示“Setup Type”对话框，选择“Custom”单选按钮，即采用自定义安装类型。

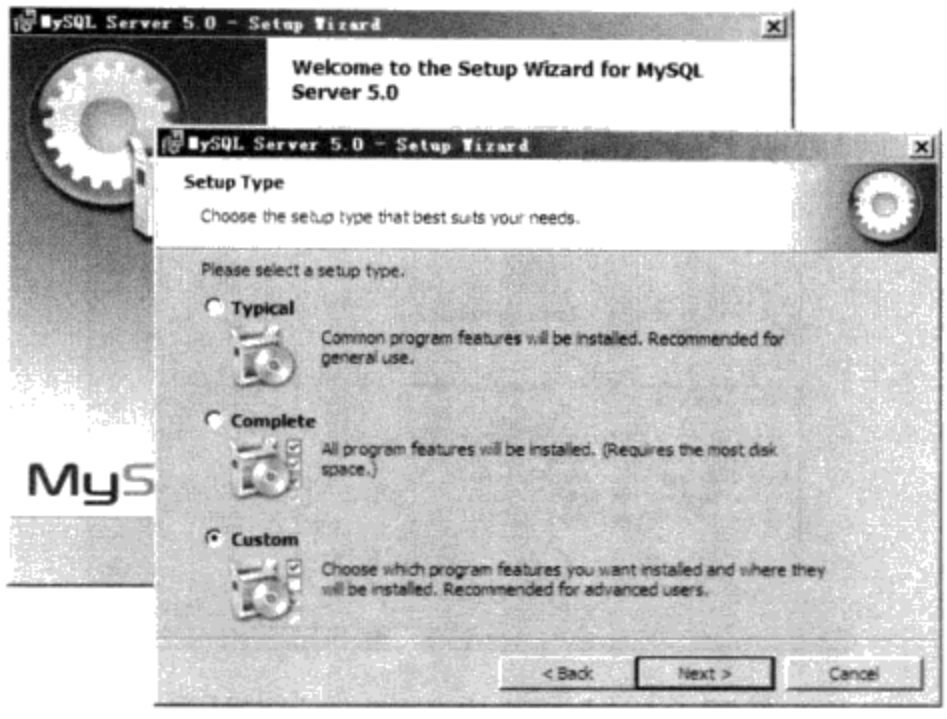


图12-8 “Setup Type”对话框

第2步，单击“Next”按钮，显示如图12-9所示“Custom Setup”对话框，选择希望安装的组件，建议全部安装。

第3步，单击“Change”按钮，显示如图12-10所示“Change Current Destination Folder”对话框，将安装路径设置为C:\ids\mysql\。

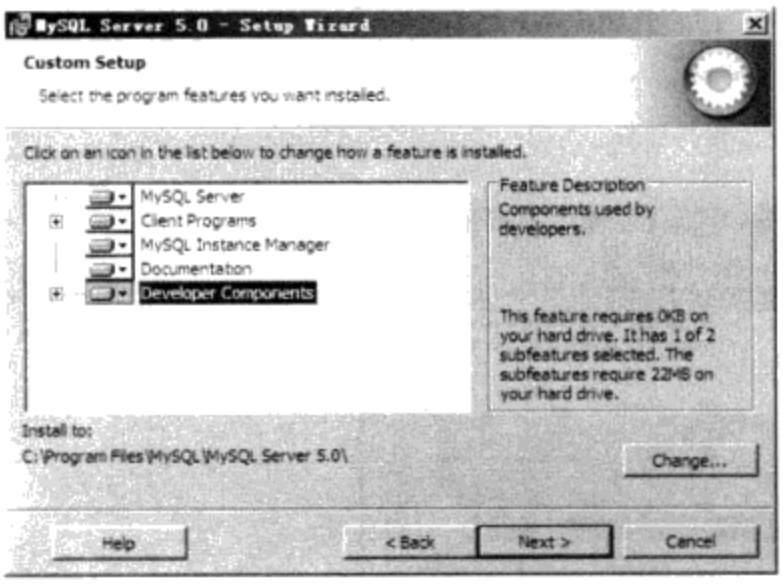


图12-9 “Custom Setup”对话框

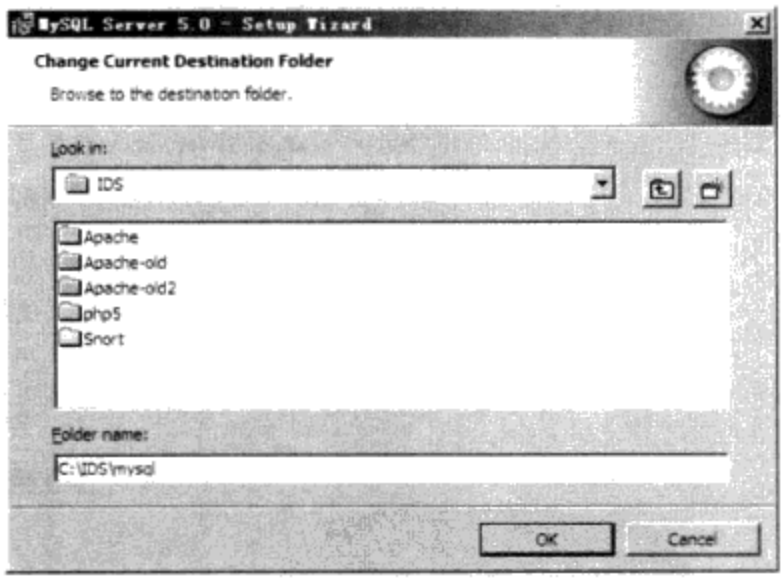


图12-10 “Change Current Destination Folder”对话框

第4步，单击“OK”按钮，保存设定的安装路径。连续单击“Next”按钮，开始安装MySQL。完成后，显示如图12-11所示“Wizard Completed”对话框，选中“Configure the MySQL Server now”复选框，可以立即配置MySQL数据库。

第5步，单击“Finish”按钮，完成MySQL的安装，并启动“MySQL Server Instance Configuration Wizard”向导，直接单击“Next”按钮，显示如图12-12所示对话框，选择“Standard Configuration”单选按钮，采用标准配置模式。

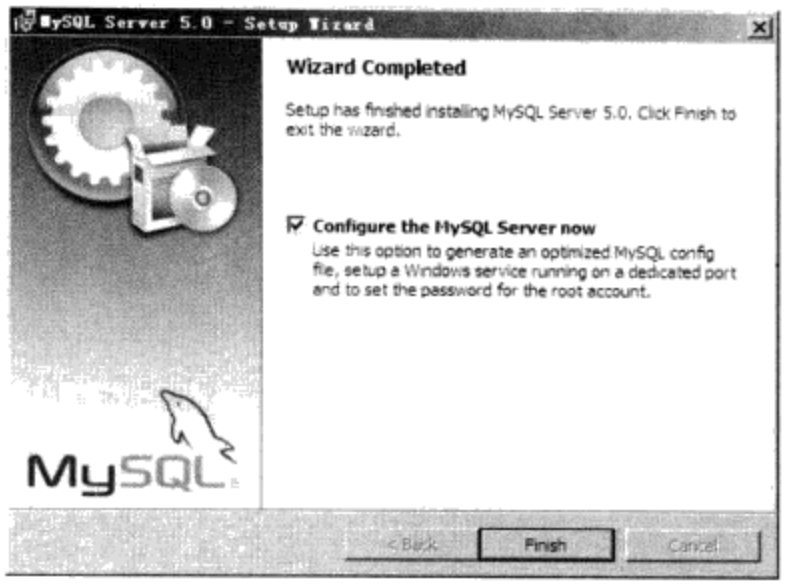


图 12-11 “Wizard Completed”对话框

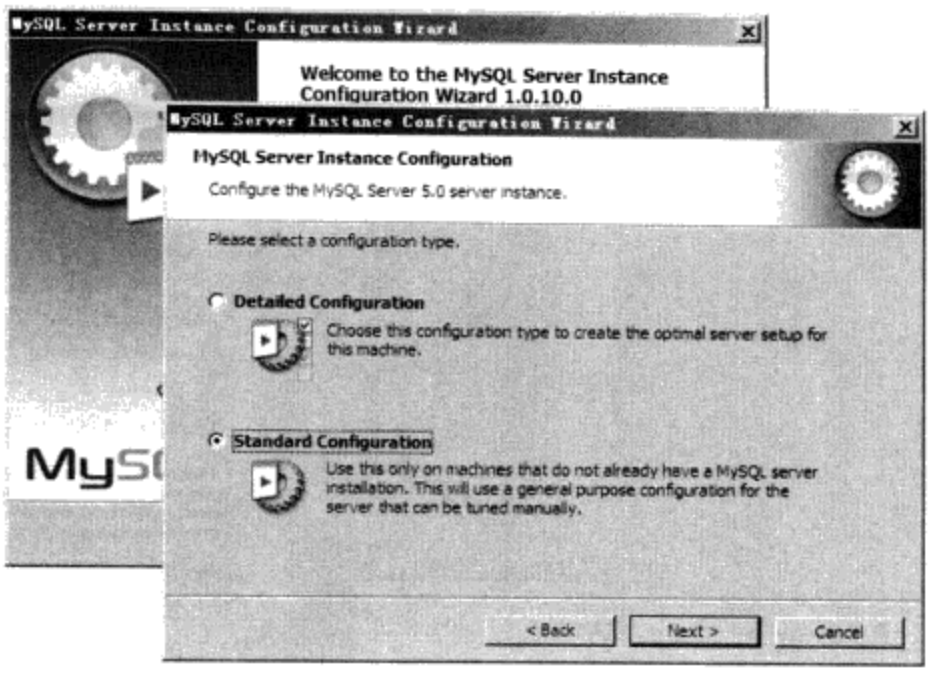


图 12-12 选择配置模式

第 6 步，单击“Next”按钮，显示如图 12-13 所示对话框，设置 MySQL 与 Windows 系统相关的选项，选中“Install As Windows Service”复选框，将 MySQL 作为 Windows 系统的一项服务运行。同时选中“Launch the MySQL Server automatically”复选框，使 MySQL 服务可以自动运行。

第 7 步，单击“Next”按钮，显示如图 12-14 所示对话框，设置 MySQL 的安全选项。选中“Modify Security Settings”复选框，设置 root 账户的密码。

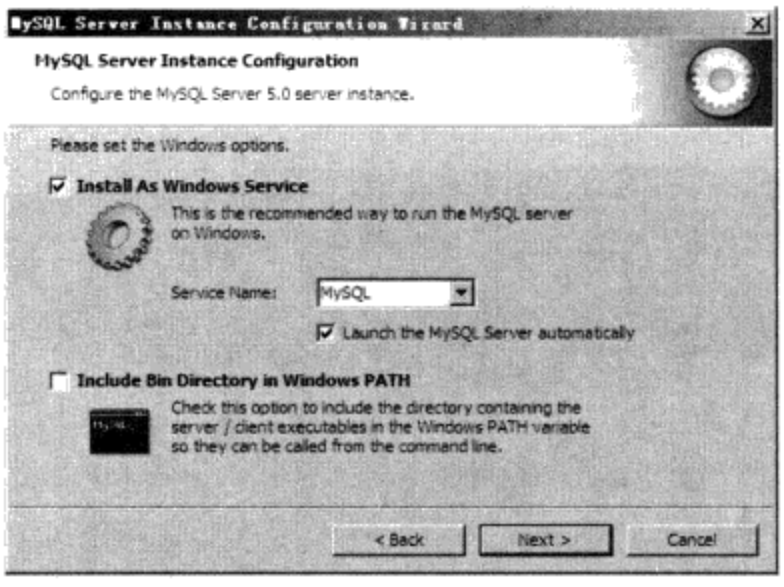


图 12-13 设置 MySQL 与 Windows 系统相关的选项

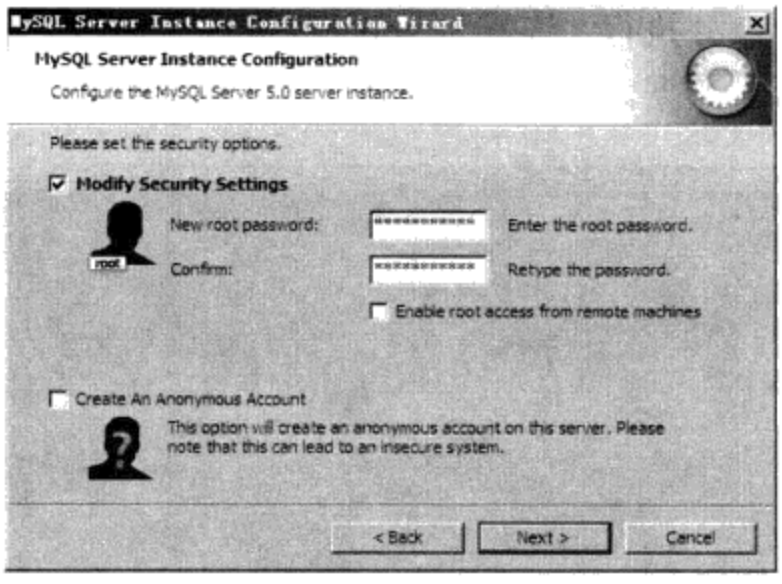


图 12-14 设置 MySQL 的安全选项

第 8 步，单击“Next”按钮，提示将要配置的 MySQL 选项，单击“Execute”按钮，即可开始配置，完成后显示如图 12-15 所示结果。

第 9 步，单击“Finish”按钮，完成 MySQL 数据库的配置。

6. 创建和配置 snort 数据库

成功安装和配置 MySQL 数据库之后，即可开始创建 snort 入侵检测系统所需的数据库。首先将 C:\ids\snort\schames\目录下的 create_mysql，复制到 C:\ids\mysql\bin\目录下，然后使用 MySQL 客户端配置程序进行如下配置。

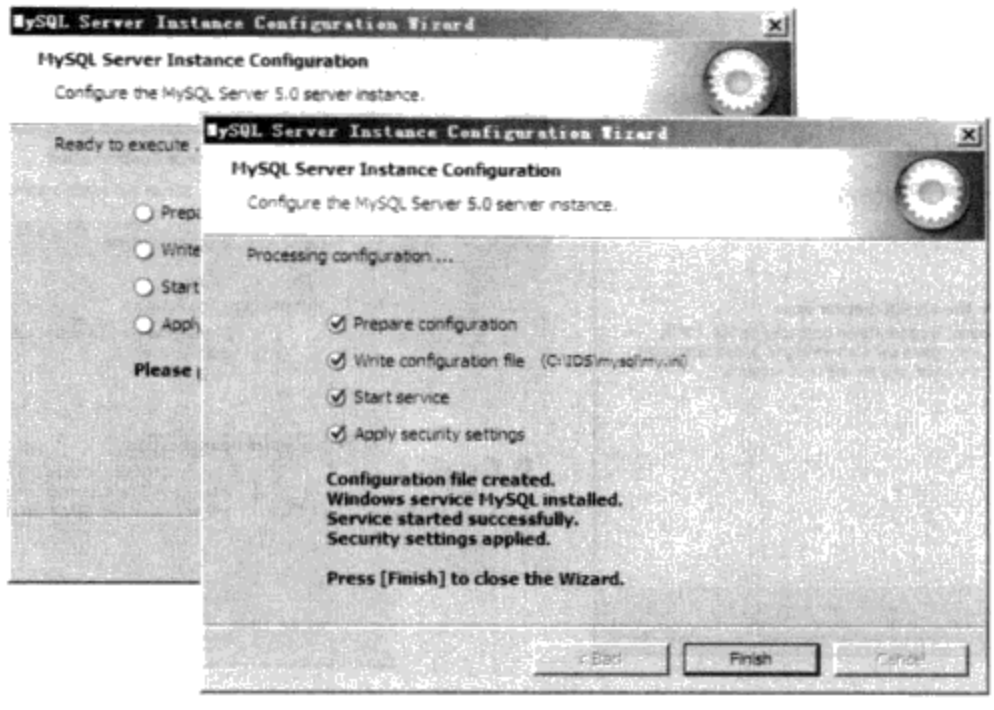


图 12-15　完成 MySQL 配置

第 1 步，依次打开“开始”→“所有程序”→“MySQL”→“MySQL Server 5.0”→“MySQL Command Line Client”选项，启动 MySQL 命令行配置程序，显示如图 12-16 所示窗口，默认以 root 账户登录，提示输入登录密码。

第 2 步，输入配置 MySQL 数据库时设置的账户密码，按 Enter 键执行即可成功登录 MySQL 服务器。输入“create database snort;”命令并执行，创建名称为 snort 的数据库。输入“create database snort_archive;”命令并执行，创建名称为 snort_archive 的数据库。输入“use snort;”命令并执行，连接到 snort 数据库。输入“source create_mysql;”命令并执行，向当前数据库中写入数据。执行结果如图 12-17 所示。

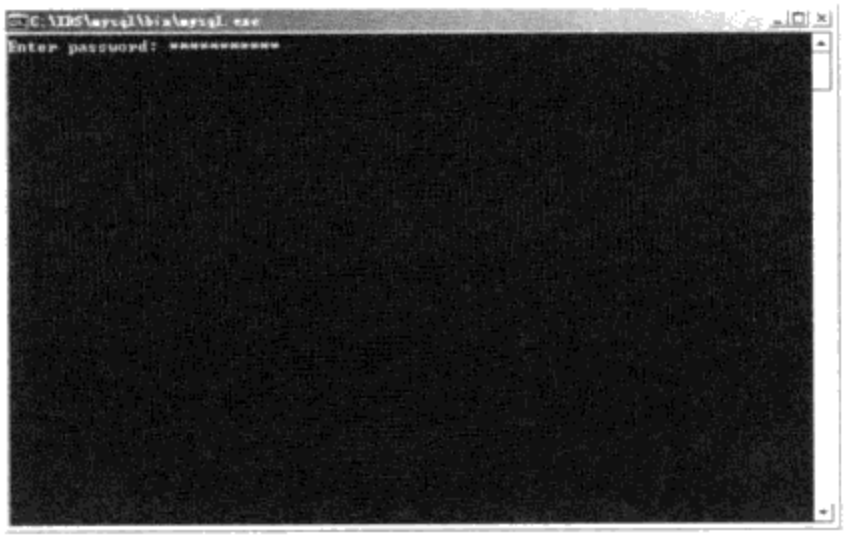


图 12-16　输入 root 账户登录密码

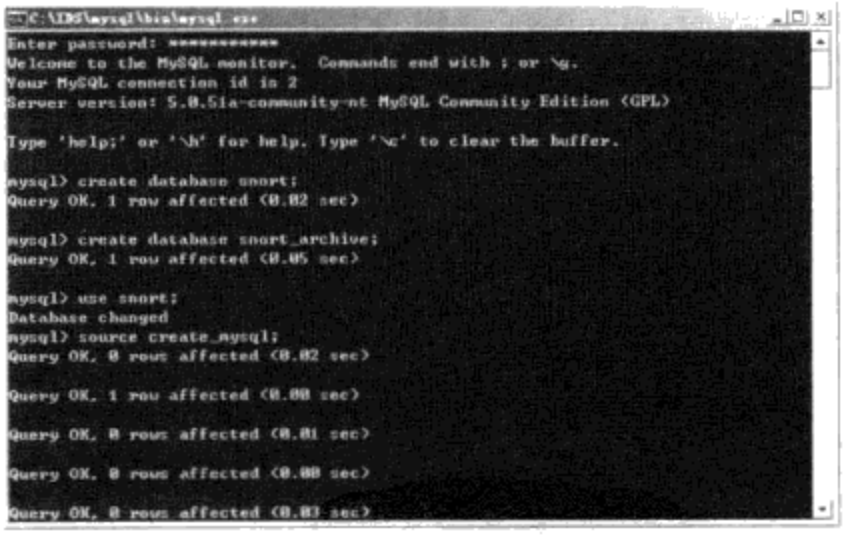


图 12-17　创建并配置 snort 数据库

第 3 步，继续输入“use snort_archive;”命令并执行，连接到 snort_archive 数据库。输入“source create_mysql;”命令并执行，向当前数据库中写入数据。执行结果如图 12-18 所示。

第 4 步，输入“grant all on *.* to root@localhost;”命令并执行，授予用户对数据库的所有操作权限，如图 12-19 所示。默认情况下，root 账户已经拥有该权限，如果配置 MySQL 数据库时创建了其他用户账户，则需要使用该命令授予其对所创建数据库的所有操作权限。

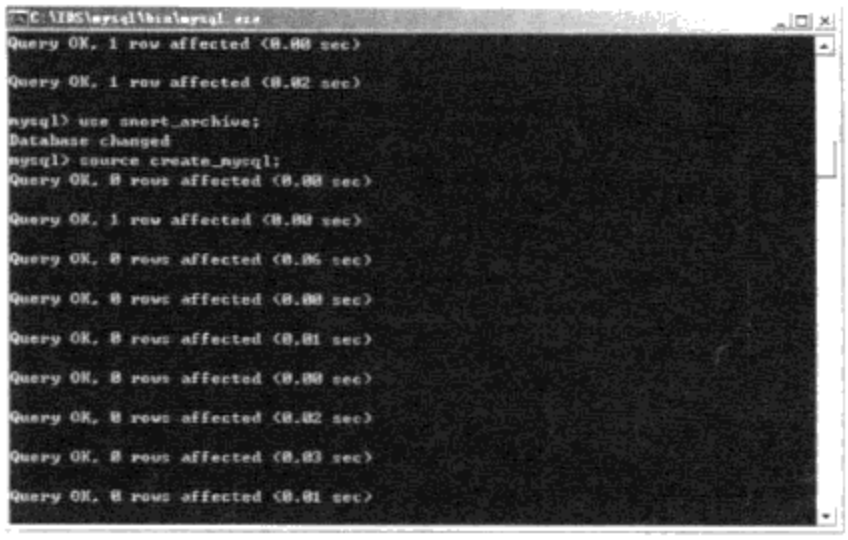


图 12-18　创建并配置 snort_archive 数据库

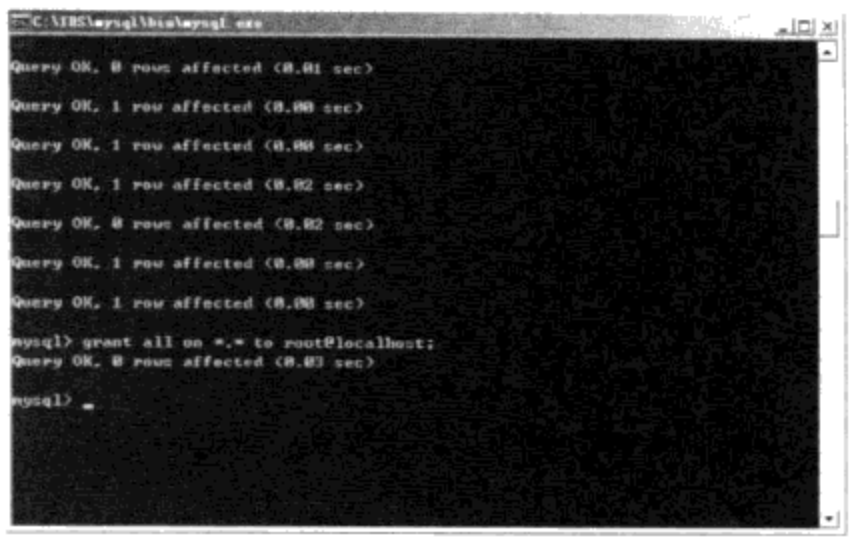


图 12-19　授予用户对数据库的所有权限

第 5 步，输入“exit”命令并执行关闭 MySQL 客户端配置窗口。

7. 安装和配置 Acid

将 Acid 解压到 C:\ids\apache\htdocs\acid\目录下，并修改当前目录下“acid_conf.php”文件中的相关代码，创建数据库与 Acid 之间的关联。

以记事本或写字板方式打开 acid_conf.php，将文件中的如下位置替换为相应的内容，如图 12-20 所示。需要配置的内容如下：

图 12-20　创建数据库与 Acid 之间的关联

- $DBlib_path = "c:\ids\php5\adodb";　# 指定 adodb 数据库路径。
- $DBtype = "mysql";　#指定数据库类型。
- $alert_dbname = "snort";　#指定数据库名称。
- $alert_host = "localhost";　#指定数服务器名称。

- $alert_port = "3306"; #指定通信端口。
- $alert_user = "root"; #指定数据库管理员账户。
- $alert_password = "coolpen.net"; #指定通信账户使用的密码。
- $archive_dbname = "snort_archive"; #指定 Archive 数据库名称。
- $archive_host = "localhost";
- $archive_port = "3306";
- $archive_user = "root";
- $archive_password = "coolpen.net";
- $ChartLib_path = "c:\ids\php5\jpgraph\src"; #指定图形数据库路径。

8. 安装 ADodb 和 JPGRAPH

ADodb 和 JPGRAPH 都是压缩包格式的，分别将其解压到 C:\ids\php5\adodb\ 和 C:\ids\php5\jpgraph\目录下，如图 12-21 所示。

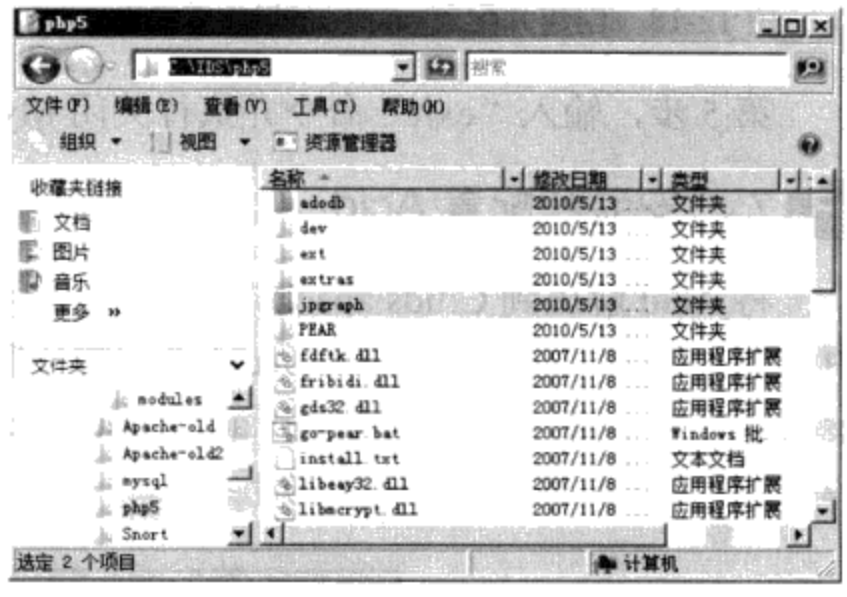


图 12-21 安装 ADodb 和 JPGRAPH

9. 安装 snort

第 1 步，运行 Snort 安装文件，启动“Snort 2.8.6 Setup”向导，显示“License Agreement”对话框，直接单击“I Agree”按钮，显示如图 12-22 所示“Installation Options”对话框，选择 Snort 使用的数据库类型，本例中选择“I do not plan to log to a database, or I am planning to log to one of the database listed above.”单选按钮。

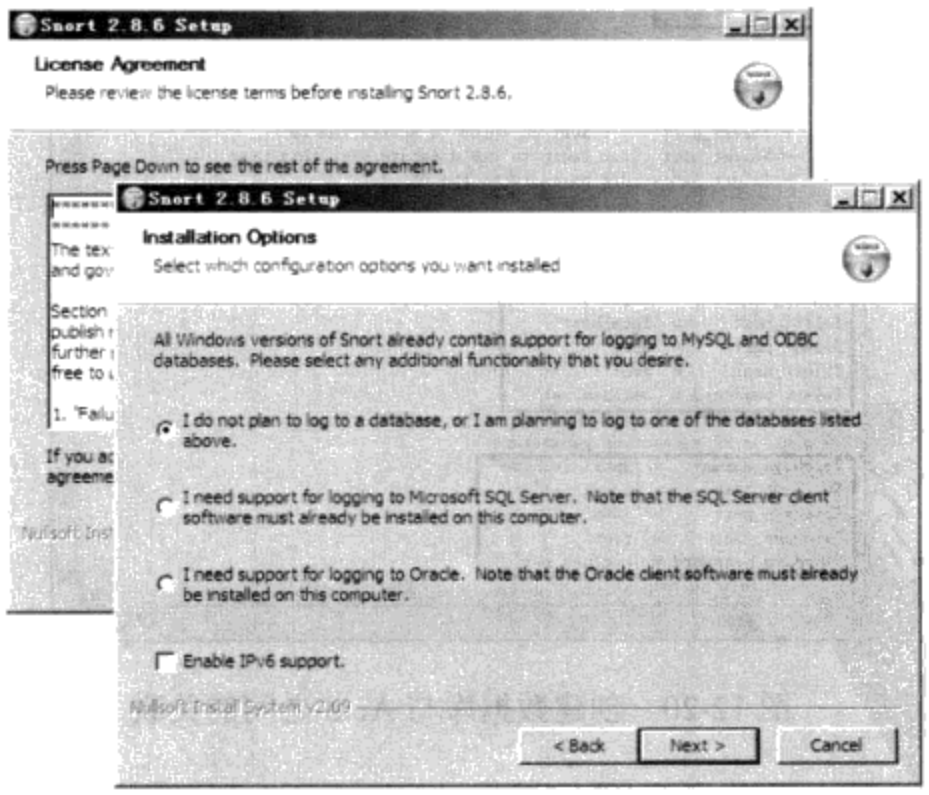


图 12-22 “Installation Options”对话框

第 2 步，单击“Next”按钮，显示如图 12-23 所示“Choose Components”对话框，选择将要安装的 snort 组件，建议全部安装。

第 3 步，单击“Next”按钮，显示如图 12-24 所示“Choose Install Location”对话框，设置 snort 的安装路径，单击“Browse”按钮将其安装路径设置为 C:\ids\snort。

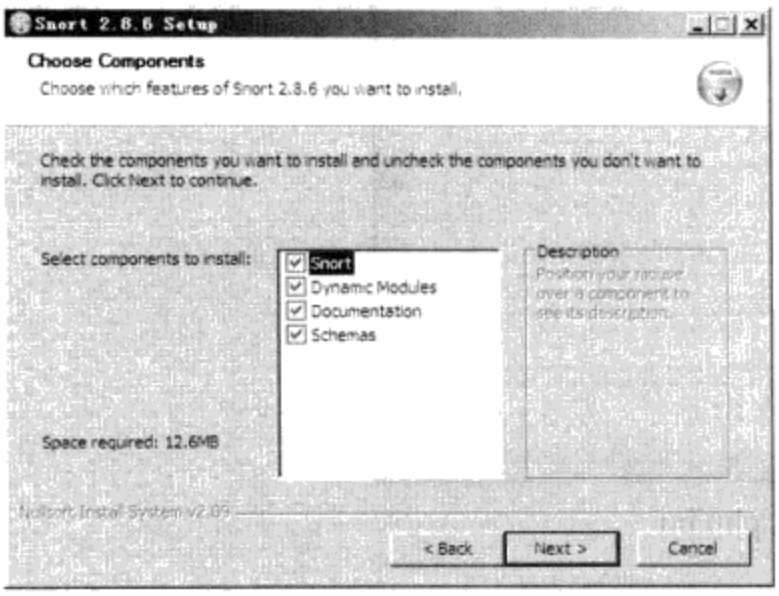


图 12-23 “Choose Components”对话框

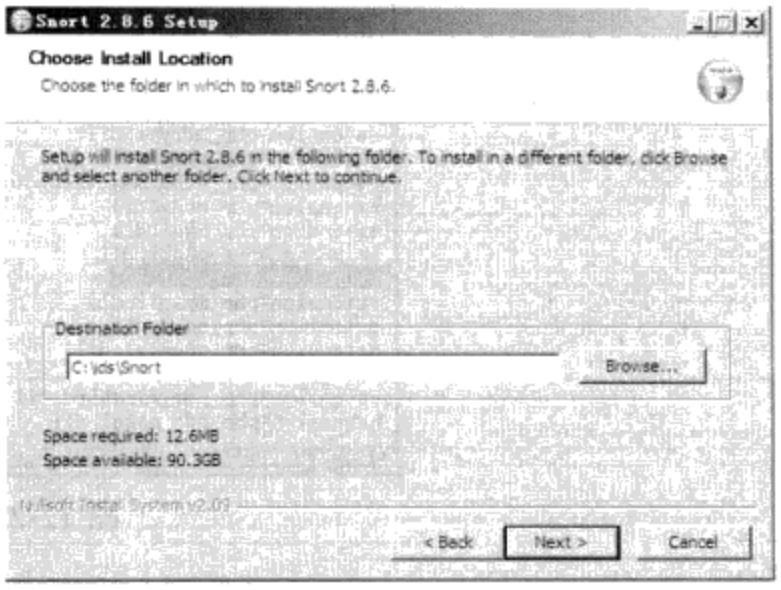


图 12-24 “Choose Install Location”对话框

第 4 步，单击“Next”按钮，开始安装，完成后显示“Completed”对话框，单击“Close”按钮，显示如图 12-25 所示对话框，提示 Snort 已经成功安装。

第 5 步，测试 snort 安装是否正确。单击“确定”按钮，关闭“Snort 2.8.6 Setup”向导。打开命令提示符窗口，转入 Snort 的安装目录，运行“snort -W”命令，显示如图 12-26 所示结果，表示 snort 已经正确安装。

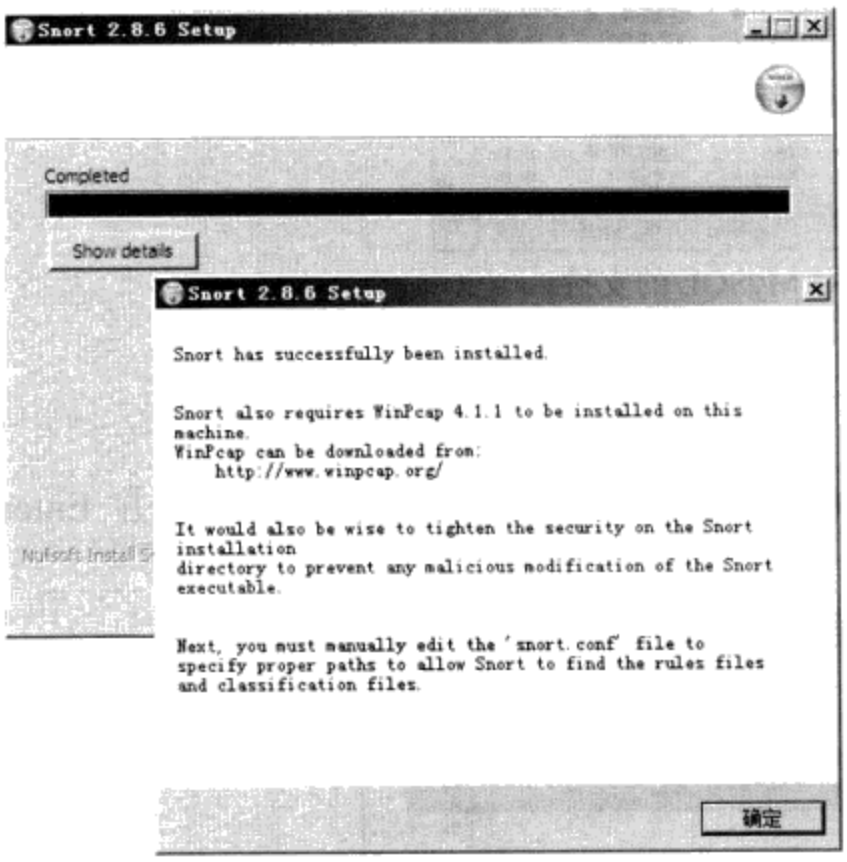


图 12-25 snort 成功安装

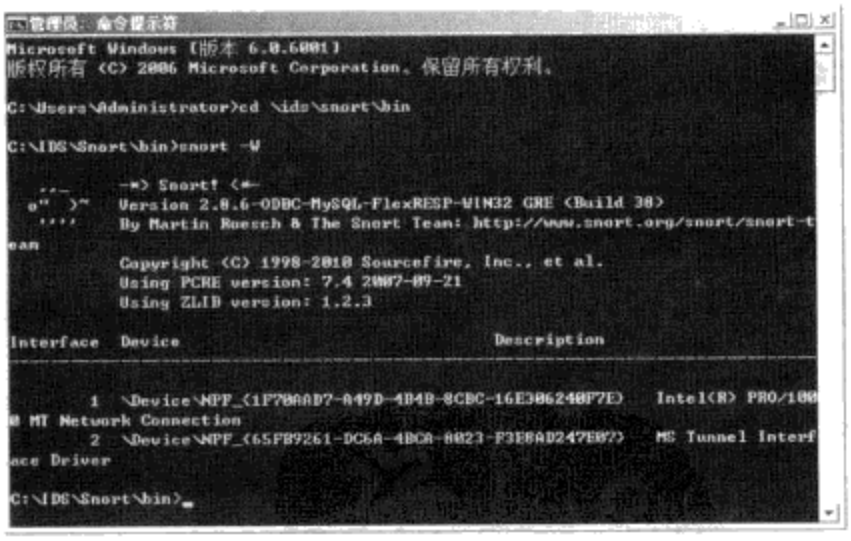


图 12-26 测试 snort 安装是否正确

10. 配置 PHP 对 MySQL 的支持

第 1 步，激活 C:\Windows\php.ini 中的“extension=php_mysql.dll”语句，删除其前面的分号，如图 12-27 所示。

第 2 步，将 C:\ids\php5\ext\目录下的 php_mysql.dll 复制到 C:\Windows\目录下，将 C:\ids\php5\目录下的 libmysql.dll 复制到 C:\windows\system32\目录下，如图 12-28 所示。

图 12-27　配置 php.ini

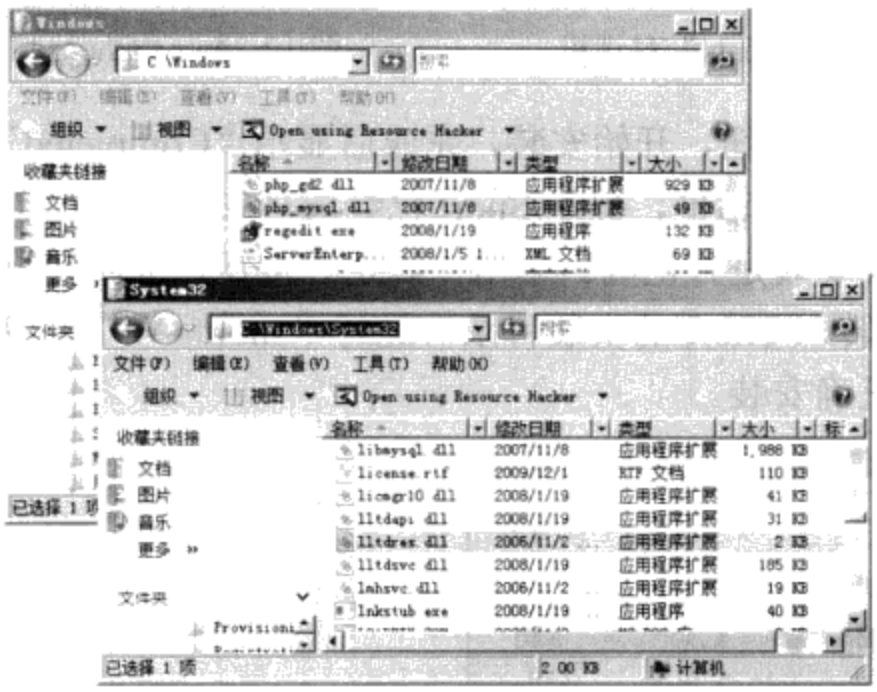


图 12-28　配置 PHP 对 MySQL 的支持

11. 初始化 Acid 数据库

第 1 步，在 IE 浏览器地址栏中，输入“http://127.0.0.1/acid/acid_db_setup.php”并 Enter 键，显示如图 12-29 所示窗口。

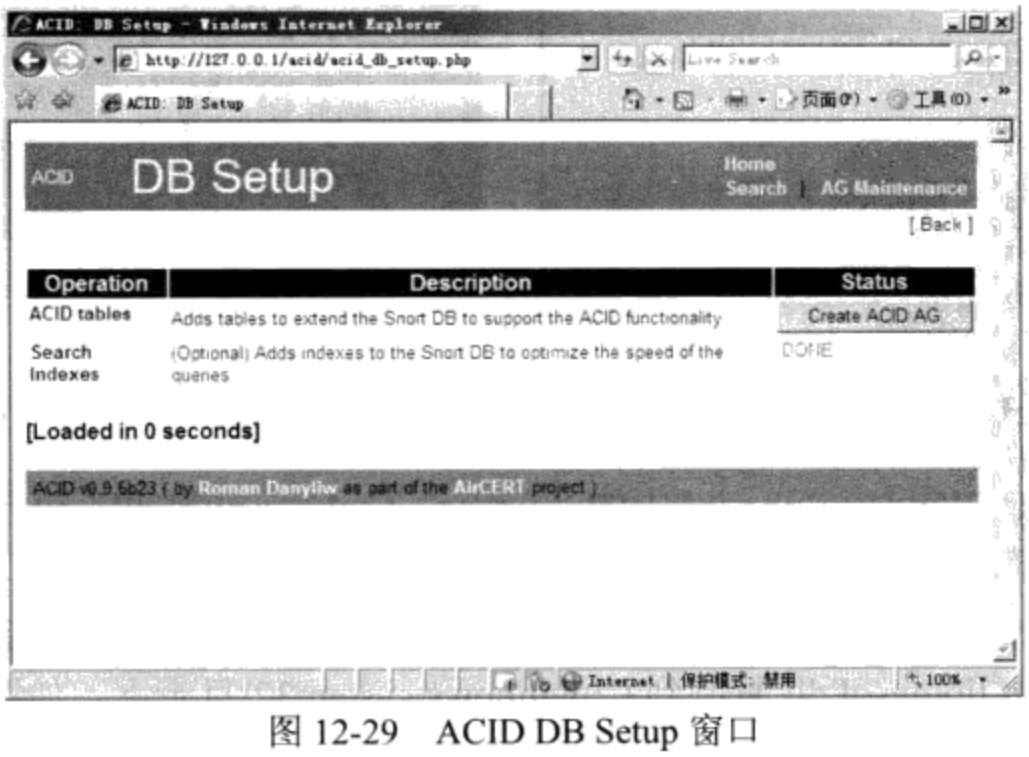


图 12-29　ACID DB Setup 窗口

第 2 步，单击“Create ACID AG”按钮，显示如图 12-30 所示窗口，成功初始化 ACID 数据库。

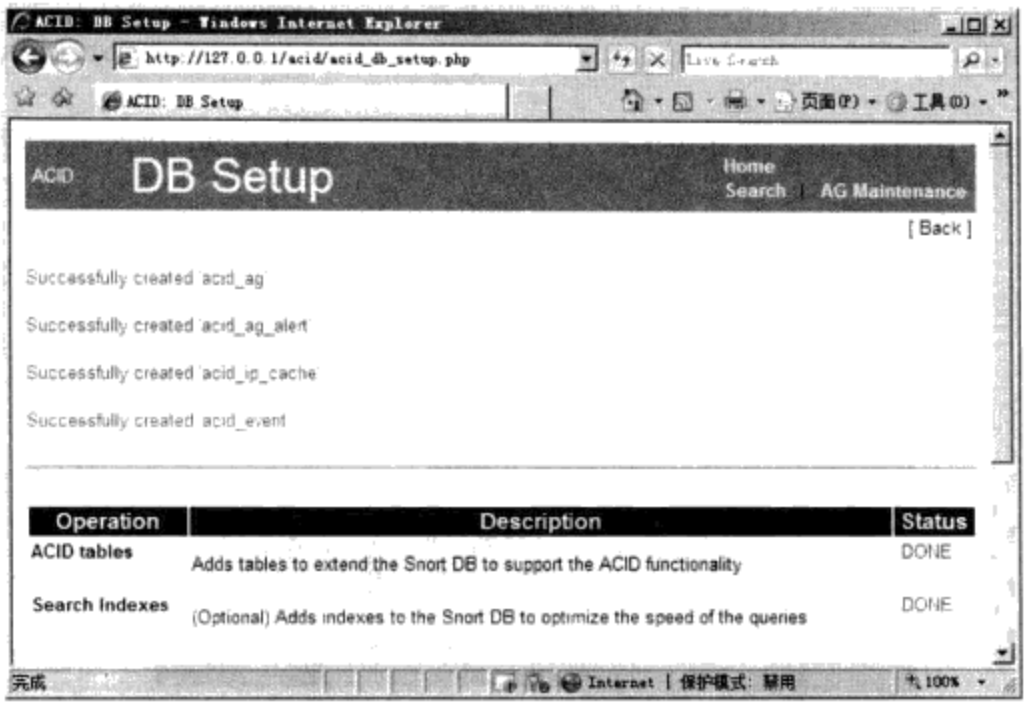


图 12-30　创建 ACID AG

12.　配置 snort rules

用户必须注册为 www.snort.org 网站会员，才能获取 snortrules。下载 snortrules 时应注意与所安装的 snort 版本匹配。

第 1 步，将下载的规则包解压缩到 C:\ids\snort\目录下，覆盖目标目录下的原有文件和文件夹即可。

第 2 步，配置 snort.conf 文件。将原文中“# metadata reference data.　do not modify these lines”下的内容替换为如下代码，如图 12-31 所示。

```
include c:\ids\snort\etc\classification.config
include c:\ids\snort\etc\reference.config
```

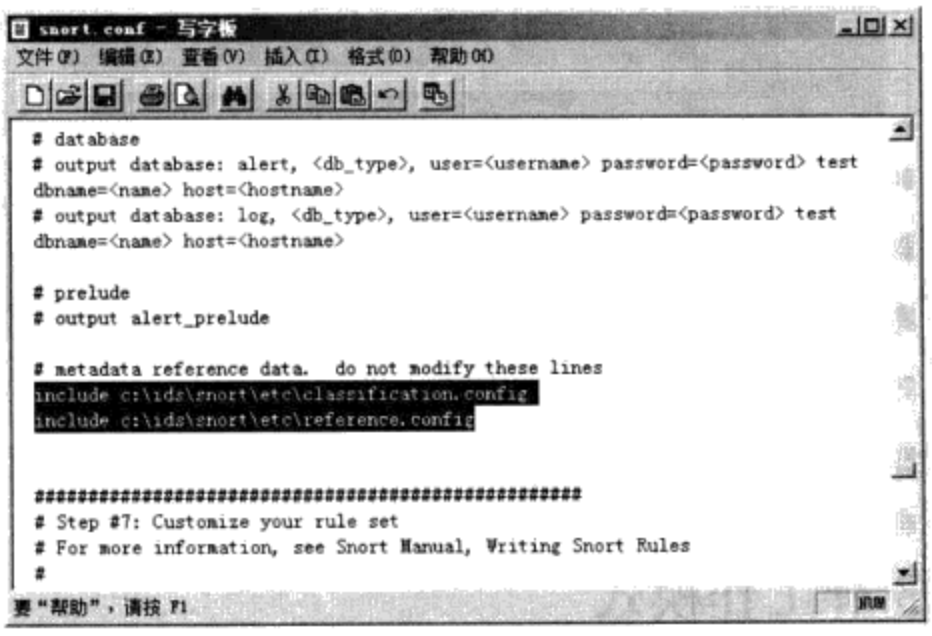


图 12-31　配置 snort.conf 文件（1）

将原文“# path to dynamic preprocessor libraries”下的内容替换为如下代码：

```
dynamicpreprocessor file C:\ids\snort\lib\snort_dynamicpreprocessor\sf_dcerpc.dll
dynamicpreprocessor file C:\ids\snort\lib\snort_dynamicpreprocessor\sf_dns.dll
dynamicpreprocessor file C:\ids\snort\lib\snort_dynamicpreprocessor\sf_ftptelnet.dll
dynamicpreprocessor file C:\ids\snort\lib\snort_dynamicpreprocessor\sf_smtp.dll
dynamicpreprocessor file C:\ids\snort\lib\snort_dynamicpreprocessor\sf_ssh.dll
```

在“# path to base preprocessor engine”下，将原文替换为如下代码，如图 12-32 所示。

```
dynamicengine C:/ids/Snort/lib/snort_dynamicengine/sf_engine.dll
```

图 12-32 配置 snort.conf 文件（2）

将原文“# database”下的内容，替换为如下代码，如图 12-33 所示。

```
output database: alert, mysql, user=root password=coolpen.net dbname=snort
host=localhost
    output database: log, mysql, user=root password=coolpen.net dbname=snort
host=localhost
```

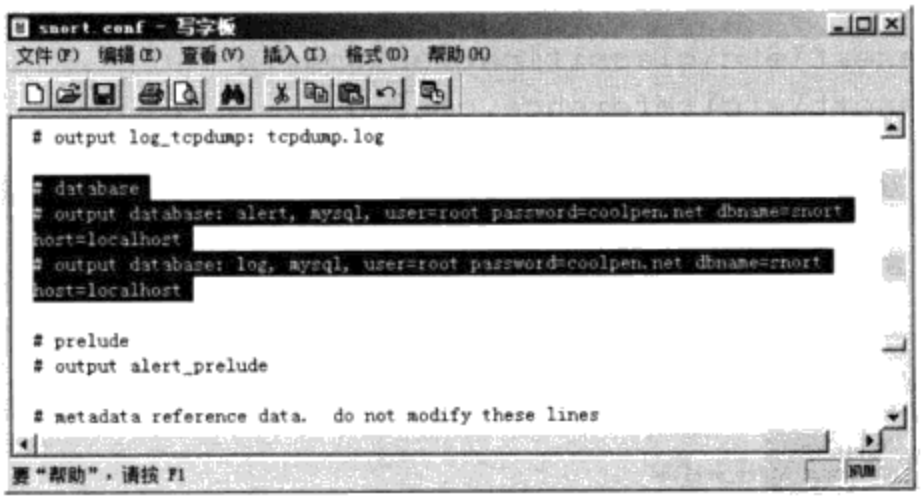


图 12-33 配置 snort.conf 文件（3）

第 3 步，单击“保存”按钮，保存配置。

12.2.4 Snort 的 3 种工作模式

Snort 有嗅探器、数据包记录和网络入侵检测 3 种工作模式，这 3 种工作模式都是通过“Snort”命令的不同选项来完成的。

1. 嗅探器

嗅探器模式是利用 snort 从网络上读取数据包，然后再将其显示在控制台上。例如，用户需要刺探网络中所有的数据包。在命令提示符窗口中，运行 snort –v 命令，输入如下结果：

```
c:\IDS\Snort\bin>snort -v
Running in packet dump mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Network Interface \Device\NPF_{1F70AAD7-A49D-4B4B-8CBC-
16E306240F7E
}
Decoding Ethernet on interface \Device\NPF_{1F70AAD7-A49D-4B4B-8CBC-
16E306240F7E
}

        --== Initialization Complete ==--

      ,,_     -*> Snort! <*-
     o"  )~   Version 2.8.6-ODBC-MySQL-FlexRESP-WIN32 GRE (Build 38)
      ''''    By Martin Roesch & The Snort Team: http://www.snort.org/snort/
snort-t
eam
           Copyright (C) 1998-2010 Sourcefire, Inc., et al.
           Using PCRE version: 7.4 2007-09-21
           Using ZLIB version: 1.2.3

Using PCAP_FRAMES = MAX
05/14-18:44:38.128525 123.134.66.6:80 -> 211.82.218.229:57622
TCP TTL:52 TOS:0x0 ID:19153 IpLen:20 DgmLen:1420 DF
***AP*** Seq: 0xA40BD2A9  Ack: 0xB5785C07  Win: 0xD8  TcpLen: 20
=+=+=+
```

```
Outstanding:          1 (25.000%)
===================================================================
Breakdown by protocol (includes rebuilt packets):
      ETH: 3          (100.000%)
  ETHdisc: 0           (0.000%)
     VLAN: 0           (0.000%)
     IPV6: 0           (0.000%)
  IP6 EXT: 0           (0.000%)
  IP6opts: 0           (0.000%)
  IP6disc: 0           (0.000%)
     IP4: 3          (100.000%)
  IP4disc: 0           (0.000%)
    TCP 6: 0           (0.000%)
    UDP 6: 0           (0.000%)
   ICMP6: 0           (0.000%)
  ICMP-IP: 0           (0.000%)
     TCP: 2           (66.667%)
     UDP: 1           (33.333%)
    ICMP: 0           (0.000%)
  TCPdisc: 0           (0.000%)
  UDPdisc: 0           (0.000%)
  ICMPdis: 0           (0.000%)
    FRAG: 0           (0.000%)
   FRAG 6: 0           (0.000%)
     ARP: 0           (0.000%)
    EAPOL: 0           (0.000%)
  ETHLOOP: 0           (0.000%)
      IPX: 0           (0.000%)
IPv4/IPv4: 0           (0.000%)
IPv4/IPv6: 0           (0.000%)
IPv6/IPv4: 0           (0.000%)
IPv6/IPv6: 0           (0.000%)
      GRE: 0           (0.000%)
   GRE ETH: 0           (0.000%)
  GRE VLAN: 0           (0.000%)
  GRE IPv4: 0           (0.000%)
  GRE IPv6: 0           (0.000%)
 GRE IP6 E: 0           (0.000%)
  GRE PPTP: 0           (0.000%)
   GRE ARP: 0           (0.000%)
   GRE IPX: 0           (0.000%)
  GRE LOOP: 0           (0.000%)
     MPLS: 0           (0.000%)
    OTHER: 0           (0.000%)
   DISCARD: 0           (0.000%)
InvChkSum: 0           (0.000%)
    S5 G 1: 0          (0.000%)
    S5 G 2: 0          (0.000%)
     Total: 3
===================================================================
Action Stats:
ALERTS: 0
```

```
LOGGED: 0
PASSED: 0
===============================================================================
Snort exiting
```

如果用户不进行干预，Sonrt 将会一直执行下去，因此，需要按组合键“Ctrl+C”，结束操作并显示刺探统计信息。从统计结果可知，本次总共嗅探到 4 个数据包，其中有 3 个数据包通过分析，被丢弃的数据包为 0，未分析的数据包 1 个。

以上显示只是显示了数据包的包头信息，若需要查看到应用层的数据，则可以在“snort”命令后面再添加“-d”选项，其操作方法如下：

```
snort -vd
```

如果需要显示链路层中的数据信息，则应在 Snort 后增加“-e”选项，其操作方法如下：

```
snort -vde
```

提示 在 Snort 命令的后面添加多个选项时，可只输入一个“-”，如“snort -d -v -e”命令可直接表示为“snort -dev”。

2. 数据包记录器

在嗅探器显示刺探到的数据包时，都是通过显示屏幕显示的，若数据包较多时，则需要将数据信息保存到文件中，并通过文本编辑器查看并分析数据。例如，在其他操作系统中利用“Ping”命令向本地计算机机发出 ICMP 请求，此时再利用 Snort 刺探其数据包，并将其记录到日志文件中。

第 1 步，在运行 snort 的计算机上启动数据包记录器。在命令提示符窗口中，输入如下命令并执行，启动 snort，如图 12-34 所示。

```
snort -vde -l c:\ids\snort\log
```

第 2 步，在网络中其他计算机上使用 ping 命令试探与 snort 主机之间的连接，如图 12-35 所示，发送数据包数量为 4 个。

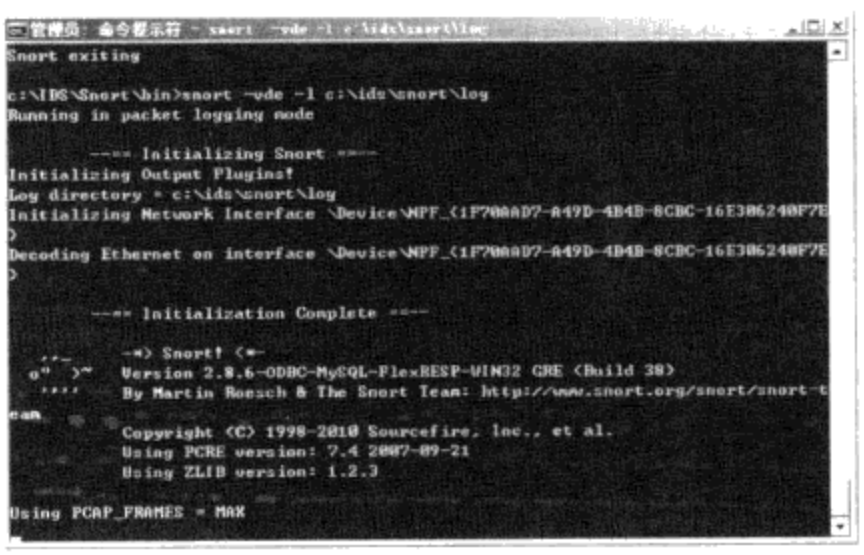


图 12-34 启动 snort

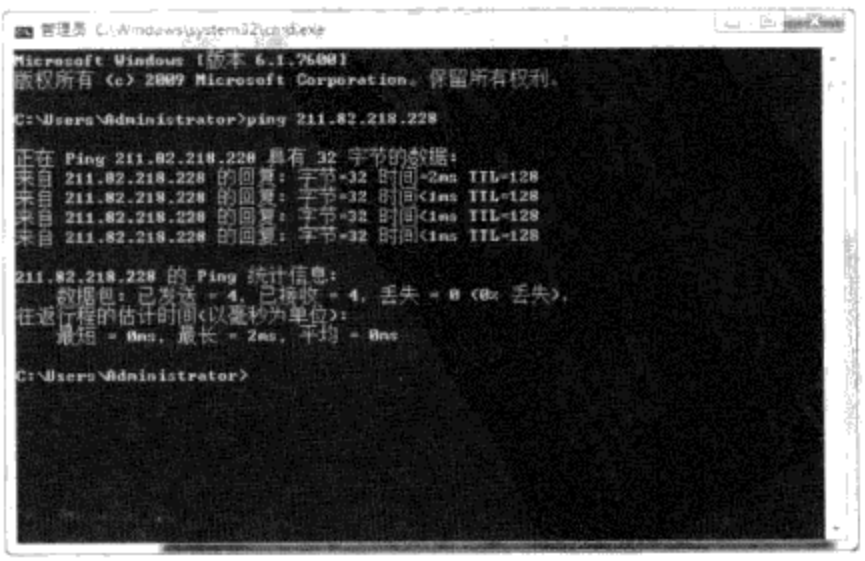


图 12-35 使用 ping 命令试探 snort 主机

第3步，在snort主机上中断snort程序的运行，如图12-36所示。

第4步，在snort主机上打开保存运行日志的目录，找到刚才生成的日志文件，记录下文件名，如图12-37所示。

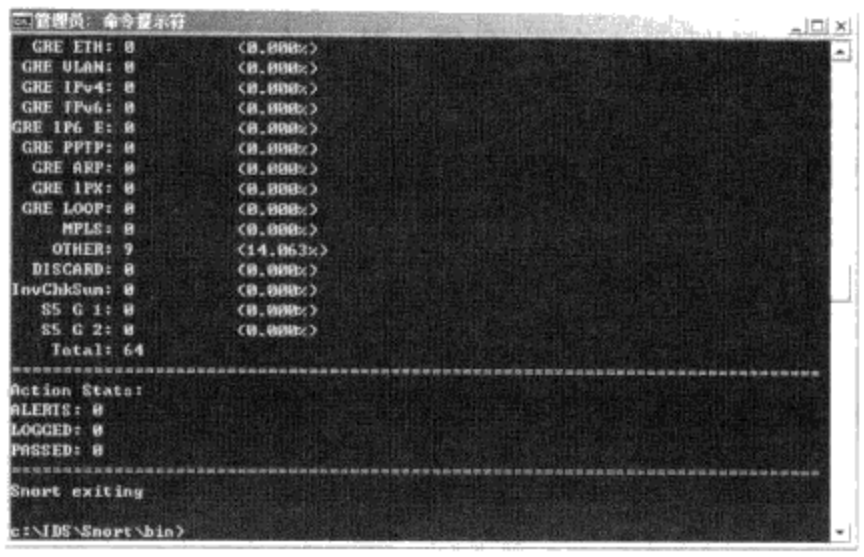


图12-36 退出snort程序

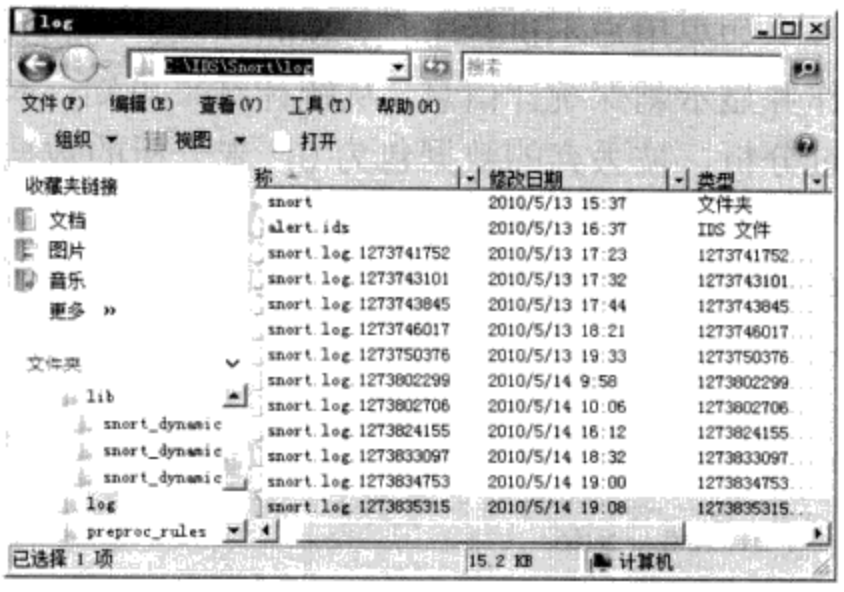


图12-37 记录日志文件名

在命令提示符窗口中，进入snort命令所在目录，输入如下命令即可查看日志的详细内容。

```
snort -dv -r <filename>
```

用户也可以根据需要只查看日志中指定通信协议的数据包，例如查看日志中的ICMP数据包处理情况，输入并执行如下命令即可。

```
snort -dv -r c:\ids\snort\log\snort.log.1273835315 icmp
05/14-19:08:38.652688 211.82.218.229 -> 211.82.218.228
ICMP TTL:128 TOS:0x0 ID:21617 IpLen:20 DgmLen:60
Type:8  Code:0  ID:1   Seq:23  ECHO
61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70  abcdefghijklmnop
71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69  qrstuvwabcdefghi
=+=+=+
```

```
05/14-19:08:40.665109 211.82.218.229 -> 211.82.218.228
ICMP TTL:128 TOS:0x0 ID:21630 IpLen:20 DgmLen:60
Type:8  Code:0  ID:1   Seq:25  ECHO
61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70  abcdefghijklmnop
71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69  qrstuvwabcdefghi
=+=+=+
```

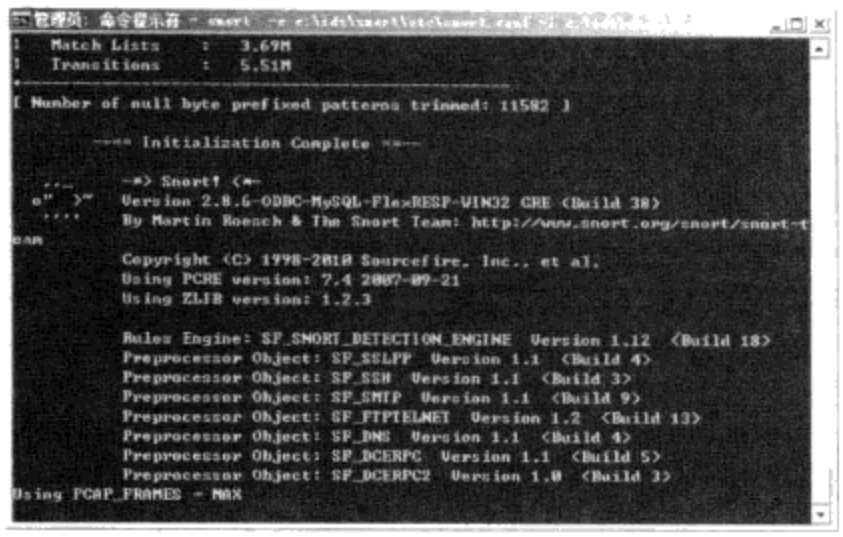


图 12-38　启动入侵检测模式

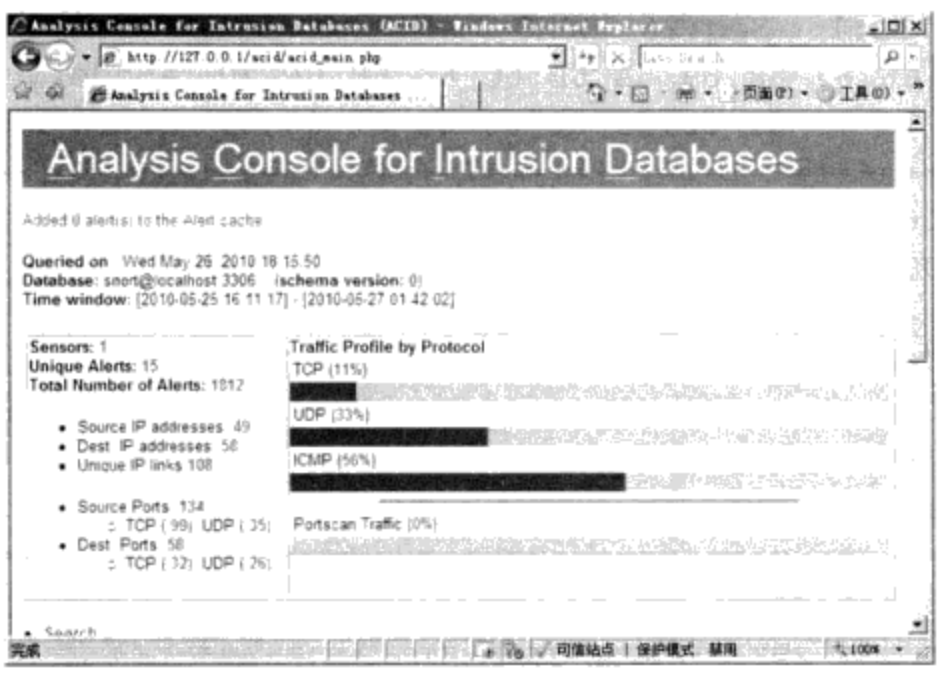


图 12-39　查看详细分析结果

12.2.5 Snort 应用实例

1. 防御 ICMP 攻击

洪水 ping 攻击虽然是老的攻击方式，但仍有恶意使用这种方式扰乱目标网络的正常运行。因此，大多数企业网络中的服务器和接入设备已经配置为禁 ping 状态，以阻止用户的扫描和攻击。在运行 snort 的代理服务器上，查看监测结果时发现连续几个小时内 ICMP 流量非常大，占到总流量的 90%，同时内网访问 Internet 的速度受到严重影响，如图 12-40 所示。

单击“ICMP”后的百分数，显示如图 12-41 所示结果，发现大量源地址为外网 IP 地址，目标地址为代理服务器外网网卡地址的 ICMP 连接。

单击其中一条记录的 ID 显示如图 12-42 所示窗口，查看 ICMP 连接的详细信息。在“length”区域可以查看 ICMP 数据包的大小。恶意用户为了达到攻击目标主机的目的，往往会增大 ICMP 数据包，以耗费目标主机的处理器资源。从图中可以看出，此次，攻击源使用的 ICMP 数据包大小为 60028，单位为字节（Byte）。

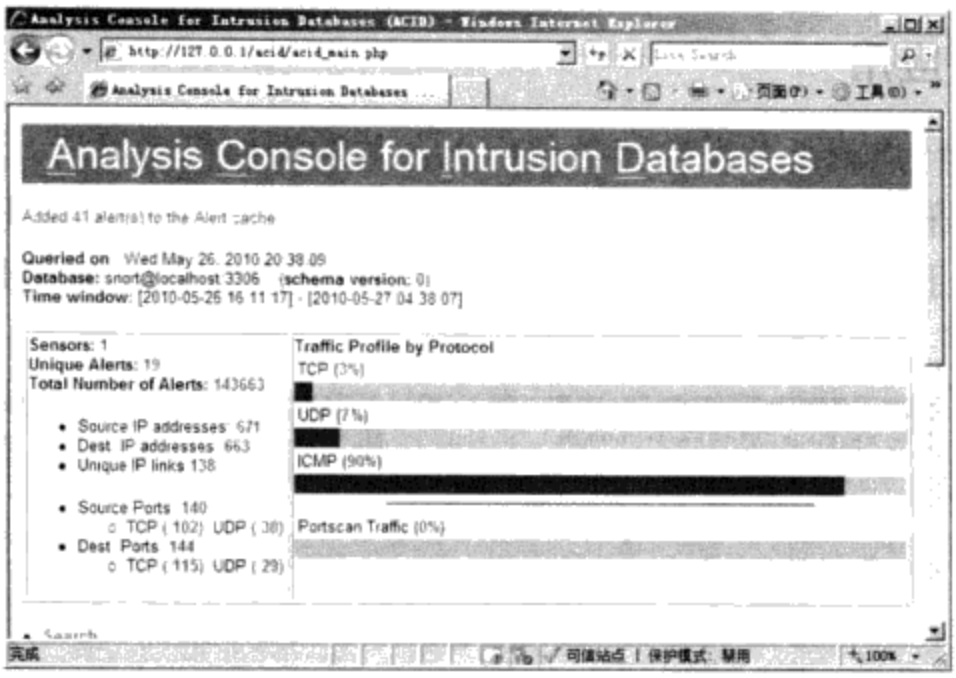


图 12-40　ICMP 流量异常

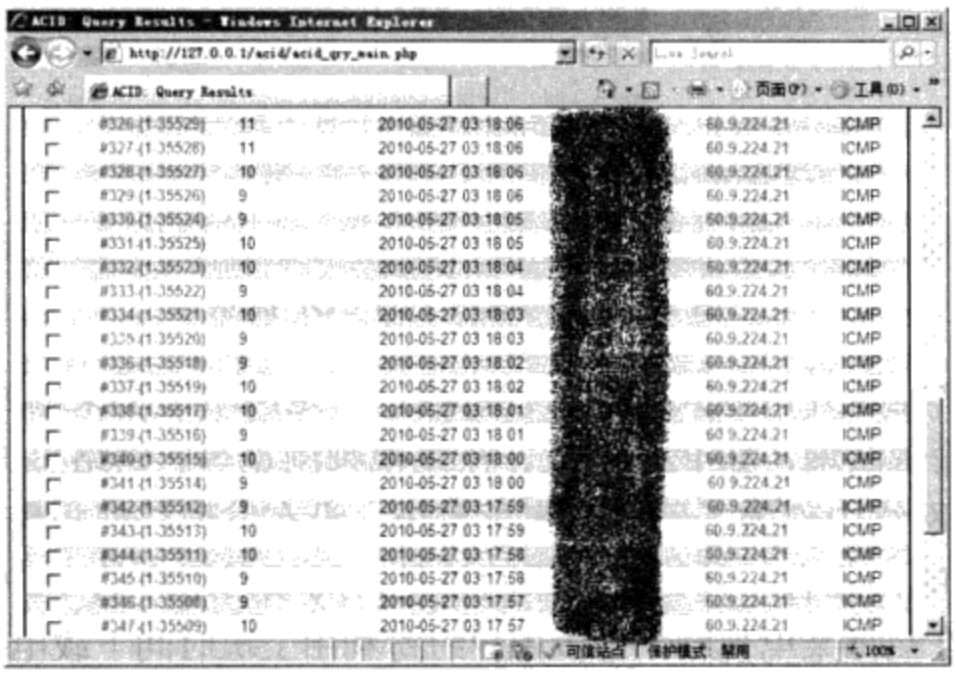


图 12-41　查看 ICMP 源地址和目标地址

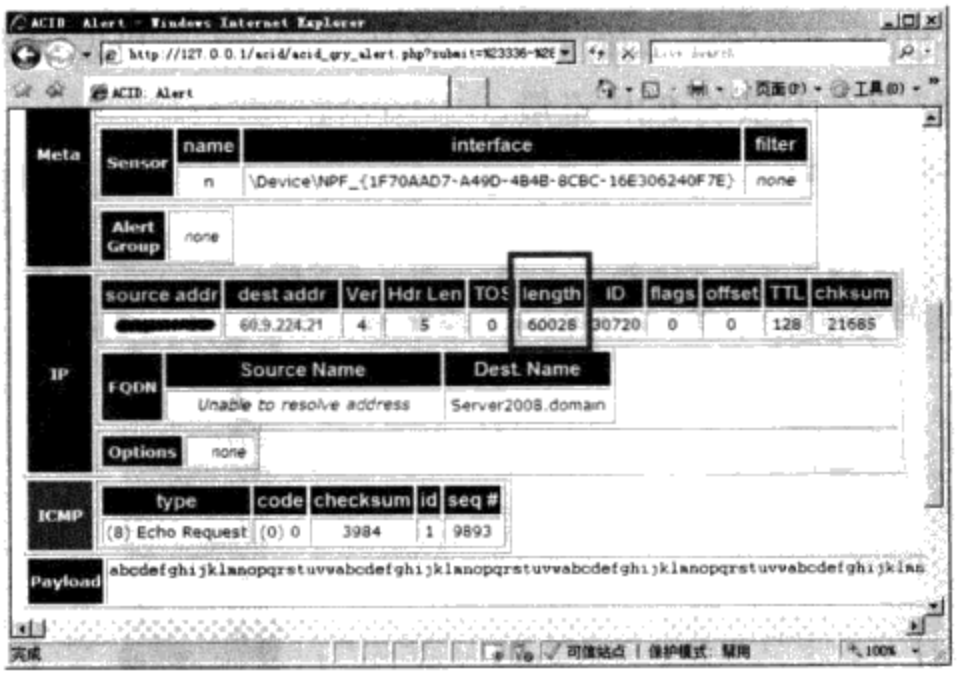


图 12-42　查看 ICMP 连接详细信息

因此，为了防止服务器遭遇来自 Internet 的 ICMP 攻击，可以通过配置 Internet 防火墙，禁止本地服务器响应 ICMP 连接。

2. 封杀 P2P 应用

P2P 应用的主要特点就是并发连接数量巨大，传输端口机动灵活，难于防范。Snort 代理服务器所在局域网，采用共享方式接入 Internet。最近几天，网络传输速度非常慢，查看 snort 监测结果时，发现基于 UDP 协议的网络流量巨大，占到总流量的 90%上，显然是不正常，如图 12-43 所示。

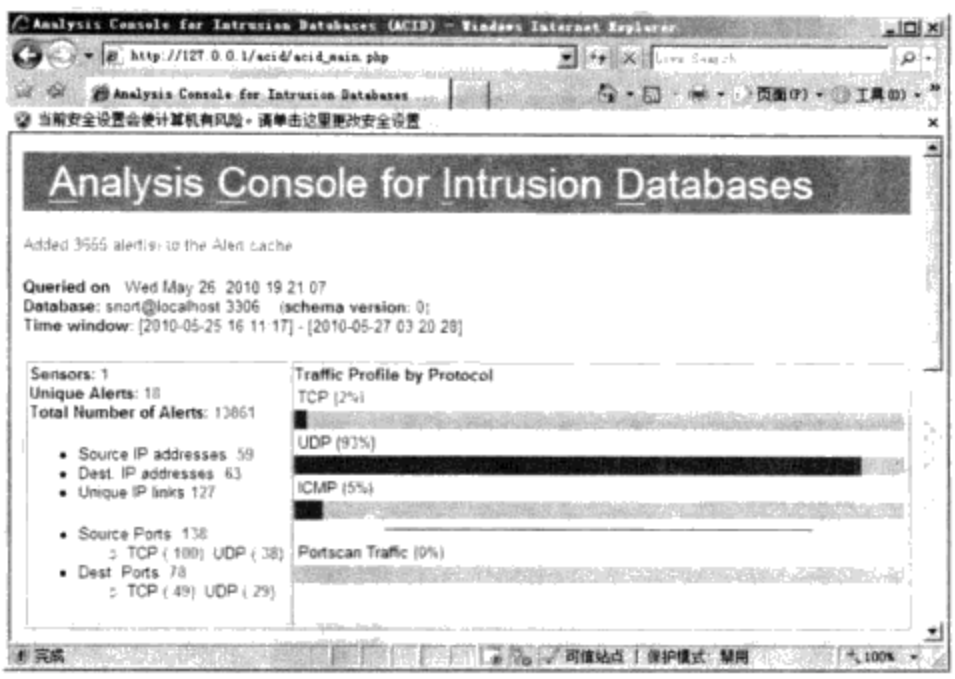


图 12-43 局域网中的 UDP 流量

导致网络中 UDP 流量异常放大，有两种可能，一是网络中感染蠕虫病毒；二是，网络中基于 UDP 的数据传输量激增，如 P2P 下载、在线视频浏览等。网络感染蠕虫病毒显然会导致这种情况出现，但是网络中部署了网络防病毒系统，没有发现任何报警信息，运行状态正常，所以可以排除这种可能。还有一种可能的原因就是，局域网用户的 P2P 下载导致这种情况。据了解，最近几天正在热播某电视剧，许多用户纷纷利用上班时间下载电视剧，甚至有些用户直接在线观看。而网络运行状态异常，也正是从最近几天开始的，所以第二种原因的可能性更大了。

继续单击“UDP”后的百分数显示如图 12-44 所示结果，局域网中的大量计算机在向 Internet 上的其他计算机发送 UDP 数据包，同时也有许多从 Internet 主机发送到局域网计算机的数据包，进一步证实，网络存在大量的 P2P 流量。

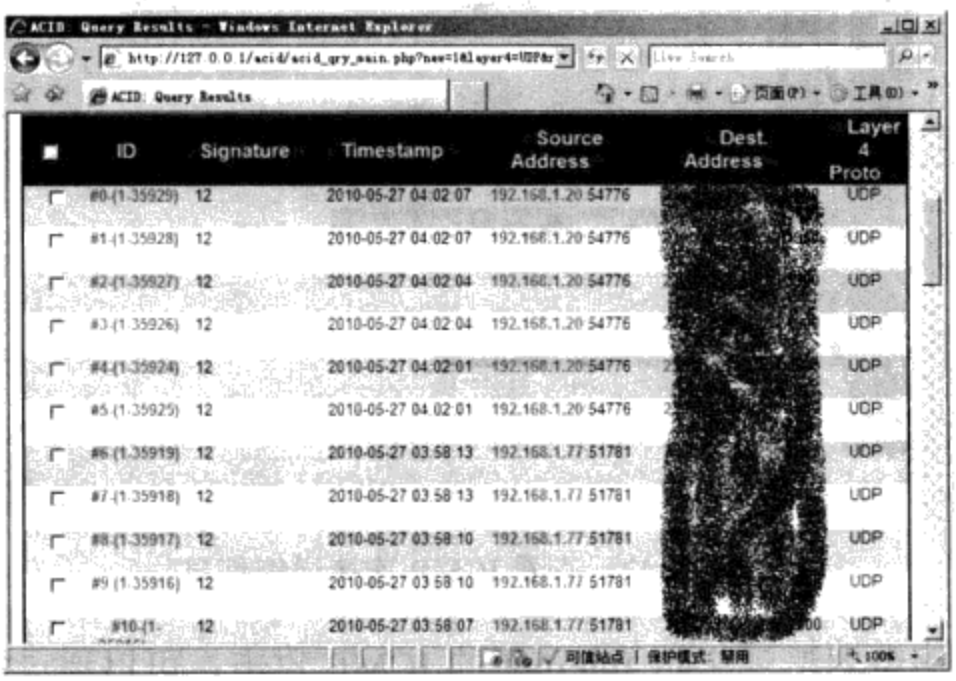


图 12-44 网络中存在大量 P2P 流量

由于 P2P 连接远程源主机和目标主机都不固定，所以很难通过 IP 地址达到封杀的目的。虽然其端口也是不断变化，但通常仍采用封端口的方式防止 P2P 泛滥。因此，可以在网络中的核心交换机上部署 IP 访问列表，阻止 P2P 连接常用的端口。IP 访问列表内容如下：

```
access-list 110 deny   tcp any any eq 135
access-list 110 deny   tcp any any eq 139
access-list 110 deny   udp any any range netbios-ns netbios-dgm
access-list 110 deny   tcp any any eq 445
access-list 110 deny   tcp any any range 3076 3077
access-list 110 deny   udp any any range 3076 3077
access-list 110 deny   tcp any any eq 3389
access-list 110 deny   tcp any any eq 4001
access-list 110 deny   udp any any eq 4004
access-list 110 deny   tcp any any range 4661 4672
access-list 110 deny   tcp any any range 6881 6890
access-list 110 deny   tcp any any eq 8008
access-list 110 deny   tcp any any gt 8081
access-list 110 deny   udp any any gt 8081
access-list 110 deny   icmp any any
access-list 110 permit ip any any
```

12.3 Sniffer

Sniffer 是 Network Associates 公司推出的功能强大的协议分析软件，广泛应用于入侵检测、流量统计与分析、网络故障与性能管理等领域。当信息以明文的形式在网络上传输时，便可以使用网络监听的方式来进行攻击。将网络接口设置在监听模式，便可以将网上传输的源源不断的信息截获。

12.3.1 Sniffer 概述

Sniffer 的主要作用是收集网络流量，通常部署在网关处的代理服务器上，可以统计网络中某台计算机的网络使用情况，包括使用的网络协议、数据流量、目标计算机等。数据分析系统可以对收集到的网络流量进行详细分析，帮助管理员快速定位与网络入侵相关的网络访问。

Sniffer 的功能主要包括如下几方面：

- 捕获网络流量进行详细分析。
- 利用专家分析系统诊断问题。
- 实时监控网络活动情况。
- 监控单个工作站、会话或者网络中任何一部分的详细的网络利用情况和错误统计。
- 支持主要的 LAN、WAN 和网络技术（包括高速与超高速以太网、令牌环、802.11b 无线网、SONET 传递的数据包、T-1、帧延迟和 ATM）。
- 提供在位和字节水平过滤数据包的能力。

12.3.2 Sniffer 安装与配置

Sniffer 的安装位置的选择，是使 Sniffer 发挥其作用的关键。通常情况下，Sniffer 应该安装在内部网络与外部网络通信的中间位置，例如代理服务器。也可以安装在局域网内的任意一台计算机上，但此时只能对局域网内部的通信进行分析。

1. 准备网络环境

如果希望使用 sniffer 收集和分析来自整个网络的数据流量，则需要将部署 sniffer 的代理服务器直接连接到核心交换机的某个端口上，然后通过配置端口镜像，将所有流量镜像到代理服务器所在端口，即可实现对整个网络的流量监测与分析。Cisco 的端口镜像叫做 SWITCHED PORT ANALYZER，简称 SPAN。端口镜像仅适用于以太网交换端口。

Cisco 交换机的 SPAN 端口配置过程如下：

第 1 步，进入全局配置模式。

```
Cisco# configure terminal1
```

第 2 步，为该进程移除任何已经存在的 SPAN 配置。

```
Cisco # no monitor session {session_number | all | local | remote}
```

第 3 步，指定 SPAN 进程和侦听源端口。

```
Cisco (config)# monitor session session_number source {interface interface-id
| vlan vlan-id} [, | -] [both | rx | tx]
```

session_number 可取值范围为 1~66，interface-id 端口号有效取值范围为 1~48。vlan-id 可取值范围为 1~4094。both 表示同时监视进/出双向流量，rx 表示仅监控入口流量；tx 表示仅监控出口流量。

第 4 步，指定 SPAN 进程与侦听目的端口。

```
Cisco (config)# monitor session session_number destination {interface
interface-id [, | -]
```

第 5 步，返回特权配置模式

```
Cisco (config)# end
```

第 6 步，校验 SPAN 配置。

```
Cisco # show monitor [session session_number]
Cisco # show running-config
```

第 7 步，保存 SPAN 配置。

```
Cisco # copy running-config startup-config
```

例如，若欲将 g1/0/1 端口的所有收发流量全部映射至 g1/0/2 端口，配置过程如下：

```
Cisco (config)# no monitor session 2
```

```
Cisco (config)# monitor session 2 source gigabitethernet1/0/1 rx
Cisco (config)# monitor session 2 destination interface gigabitethernet1/0/2
Cisco (config)# end
```

提示

所谓端口镜像，是指把交换机一个或多个端口（或 VLAN）的数据镜像到一个或多个端口的方法。简单地说，端口镜像就是把交换机一个（数个）端口（源端口）的流量完全复制一份，从另外一个端口（目的端口）发出去。网络管理人员在目的端口通过软件分析源端口的流量，从而找出网络存在问题的原因。

2. 安装 Sniffer

在使用 Sniffer 捕获数据时，由于网络中传输的数据量特别大，如果安装 Sniffer 的计算机内存太小，这些数据会被系统交换到磁盘，从而导致计算机性能下降。如果没有足够的物理内存，很容易造成安装有 Sniffer 的计算机死机或崩溃。因此，网络中捕获的流量越多，Sniffer 系统就应该运行得更快、功能更强。因此，建议为运行 Sniffer 的代理服务器配备高速处理器，至少应安装 1GB 以上的物理内存。

第 1 步，运行 Sniffer 安装程序，启动 Sniffer 安装向导，单击“Next”按钮，安装程序开始检查计算机硬件，检查是否满足 Sniffer 的最低安装需要，如图 12-45 所示。如果显示为均显示为“Passed”，则表示测试通过。如果其中某项没有通过检测，则不能进行安装。

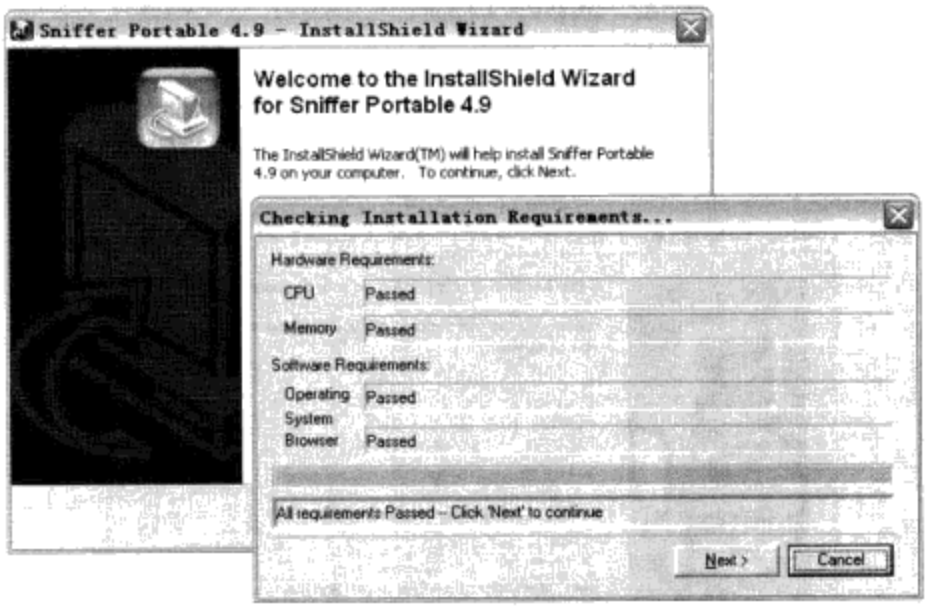


图 12-45 硬件测试结果

第 2 步，单击“Next”按钮，显示“Software License Agreement”对话框，显示该软件许可协议。单击“Yes”按钮，显示如图 12-46 所示“Choose Destination Location”对话框。单击“Browse”按钮，可以根据需要设置 Sniffer 的安装目录，通常情况下保持默认即可。

第 3 步，单击“Next”按钮，开始安装 Sniffer，安装完成后打开“Setup Complete”对话框。选中“View the Sniffer Portable Release Notes”复选框，可以在安装完成后，查看 Sniffer 的说明文件。单击“Finish”按钮，显示如图 12-47 所示“Sniffer Portable Install”对话框。提示 Sniffer 已经安装完成，需要重新启动计算机，才能使用该软件。

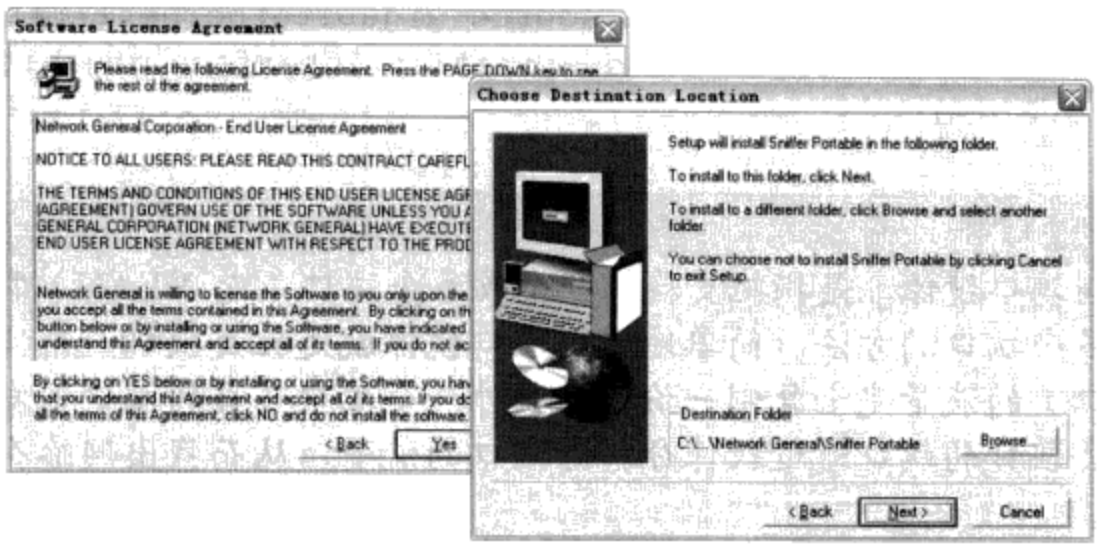


图 12-46 “Choose Destination Location”对话框

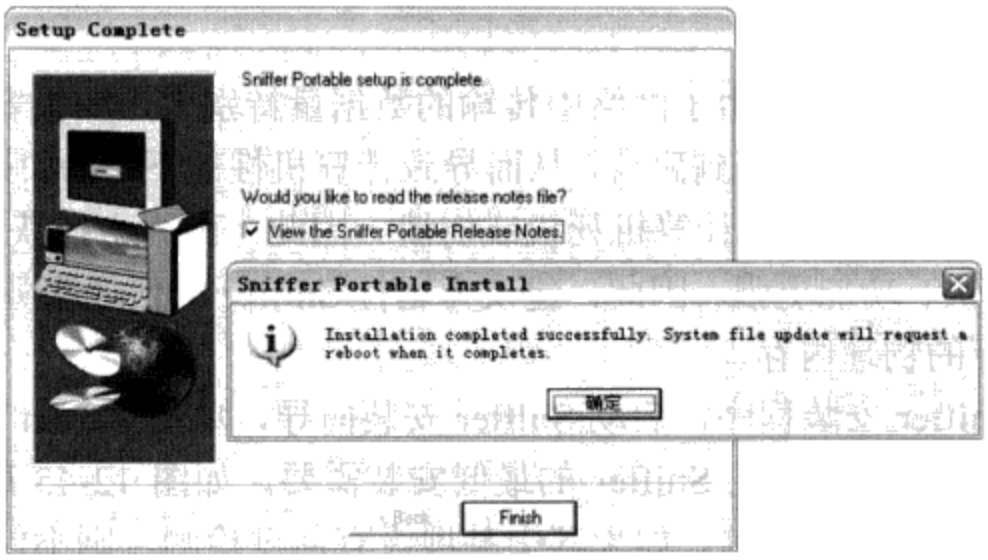


图 12-47 “Sniffer Portable Install”对话框

第4步，单击“确定”按钮，显示如图12-48所示“Setup Complete”对话框。选择“Yes, I want to restart my computer now.”单选按钮，安装完成后，立即重新启动计算机。

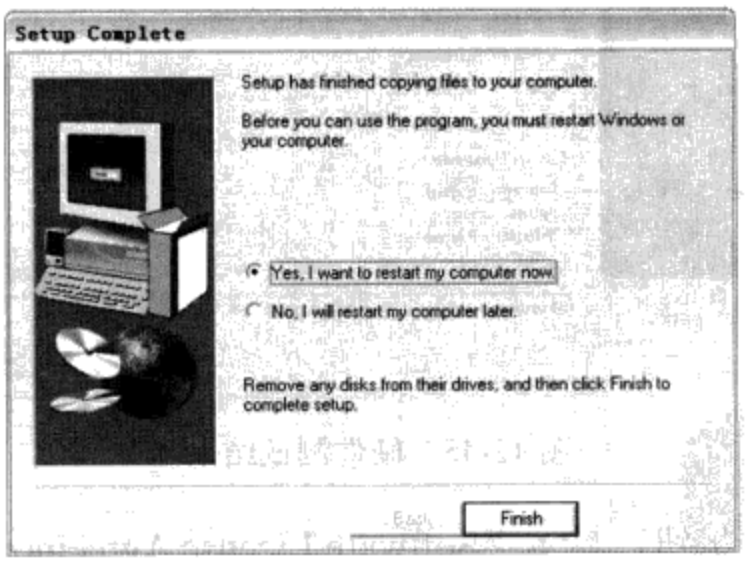


图 12-48 “Setup Complete”对话框

第5步，单击“Finish”按钮，即可重新启动计算机完成安装。

3. 配置网络适配器

通常情况下，代理服务器会安装多块网卡，以实现Internet共享，而Sniffer默认只监控一块网卡上的数据流。因此，在使用Sniffer捕获网络数据流前，需要指定所监控的网卡。另外，使用Sniffer实例功能，可以实现同时捕获多块网卡，但多个Sniffer实例的“Settings”窗口不

能同时打开。

第 1 步，依次打开“开始”→“所有程序”→“Network General”→“Sniffer Portable”→“Sniffer Portable”，启动 Sniffer 程序。如果当前计算机上安装有多块网卡，会显示如图 12-49 所示“Settings”对话框，需要选择要监视的网卡。

第 2 步，为了使 Sniffer 能够监控多个不同的网络，可以设置多个代理。在“Settings”对话框中单击“New”按钮，显示如图 12-50 所示“New Settings”对话框。在“Description”对话框中键入网卡描述信息，在“Network Adapter”下拉列表框中选择要使用的网卡。

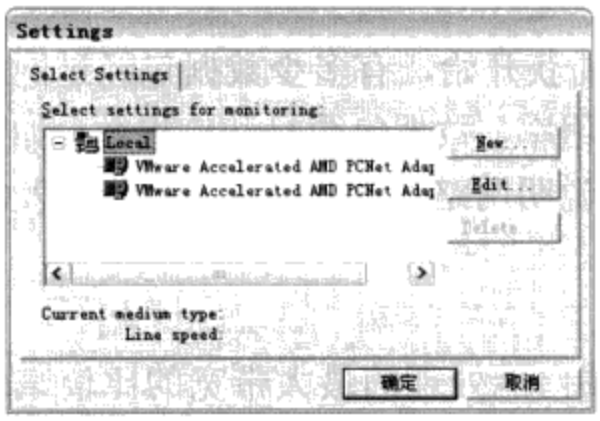


图 12-49　设置网络适配器

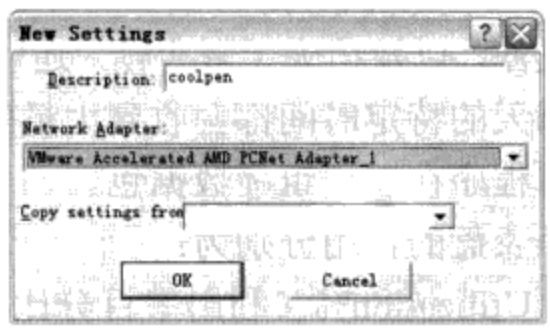


图 12-50　“New Settings”对话框

第 3 步，单击“OK”按钮，保存设置即可。

第 4 步，配置完成后，单击“确定”按钮，显示如图 12-51 所示主窗口。依次打开“File”→“Settings”选项，选择不同的网卡，即可监控不同的网络。

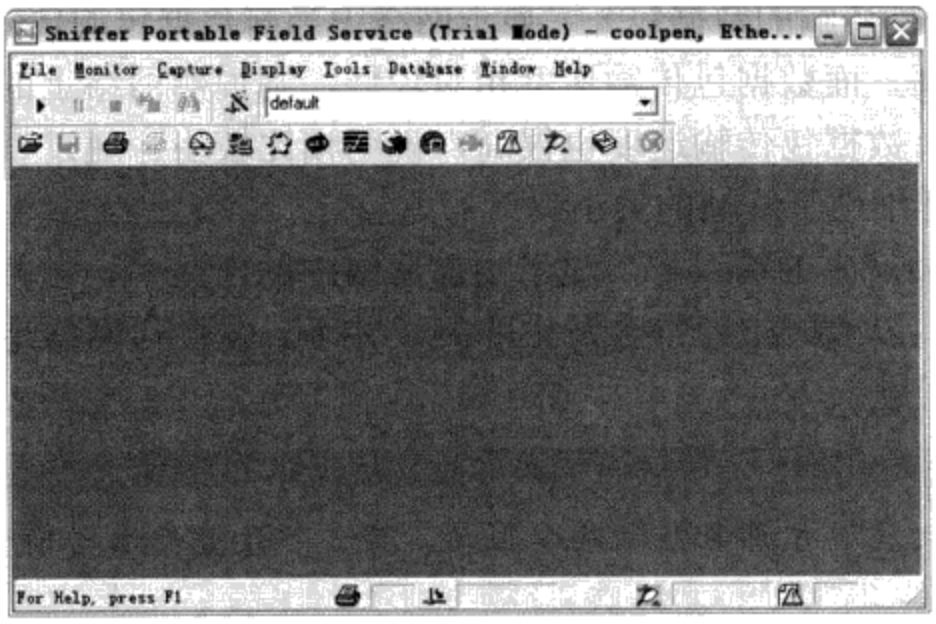


图 12-51　Sniffer 主窗口

12.3.3 Sniffer 的监控模式

Sniffer 的监控功能可以查看当前网络中的数据传输情况。Sniffer 具有 7 大监控功能，包括：Dashboard（仪表）、Host Table（主机列表）、Matrix（矩阵）、ART（Application Response Time，应用响应时间）、Protocol Distribution（协议分类）、History Sample（历史采样）和 Global Statistics（全局统计）。这些功能可以实时显示当前网络中传输的数据，便于网络管理员及时发现故障并解决。

1. Dashboard（仪表）

Sniffer的仪表盘使用图形化界面，可以直观地观测到网络的利用情况。

在Sniffer窗口中，依次选择“Monitor”→“Dashboard”选项，或单击工具栏上的仪表盘按钮，显示如图12-52所示仪表盘窗口，以后每次启动Sniffer时都会自动打开该仪表盘。这里共有3个仪表盘，分别为“Utilization%”、“Packets/s”和“Errors/s”，分别用来显示网络利用率、传输的数据和错误统计。其中，表盘的红色区域表示警戒值，下方的两个数字分别表示当前和最大的利用率。

通过这3个仪表盘，管理员可以很容易地看到从捕获开始，有多少数据包经过网络、多少帧被过滤，以及遗失了多少帧。还可以看到网络的利用率、数据包数目和广播数，如果发现网络在每天的特定时间都会收到大量的组播数据包，这说明网络可能出现了问题，需及时分析哪个应用程序在发送组播数据包。

各个表盘的作用分别为：

- Utilization%（利用率百分比） 使用传输与端口能处理的最大带宽的比值来表示网络占用带宽的百分比。由于网络数据流通常都是突发的，一个几秒钟内爆发的数据流和能长期保持活性数据流的重要性是不同的，因此，表示网络利用率的理想方法要因网络不同而改变，而且很大程度上要取决于网络的拓扑结构。在以太网端口，利用率为40%，效率可能已经很高了，但是在全双工可转换端口，80%的利用率才是高效的。
- Packets/s（每秒传输的数据包） 显示网络中当前数据包的传输速度。例如，如果网络利用率很高，而数据包传输速度相对较低，则说明网络上的帧比较大。如果网络利用率很高，数据包传输速度也很高，说明帧比较小。通过查看规模分布的统计结果，可以更详细地了解帧的大小。
- Errors/s（每秒产生的错误） 显示当前网络中的出错率。但并非所有的错误都产生故障。例如，以太网中经常会发生冲突，并不一定会对网络造成影响，但过多的冲突就会带来问题。

提示 每个仪表盘下方都会显示两个数值，前一个数值表示当前值，后一个数值表示最大值。

如果想查看详细的传输数据，可单击仪表盘下方“Detail”（详细）按钮，显示如图12-53所示表格，以数值形式显示网络的使用信息。

其中，“Network”表格中显示了当前网络的使用情况。

- Packets：网络中传输的数据包总数。
- Drops：网络中遗失的数据包数量（在网络活动高峰期经常会遗失数据包）。
- Broadcasts：网络中广播帧的数量。子网或VLAN上所有的组件都必须处理所有的广播数据包，过多的广播会使网络上所有系统的性能整体下降。
- Multicasts：网络中组播帧的数量。
- Bytes：数据包的总字节数。

- Utilization：当前网络的利用率。
- Errors：网络中存在的错误的总数。

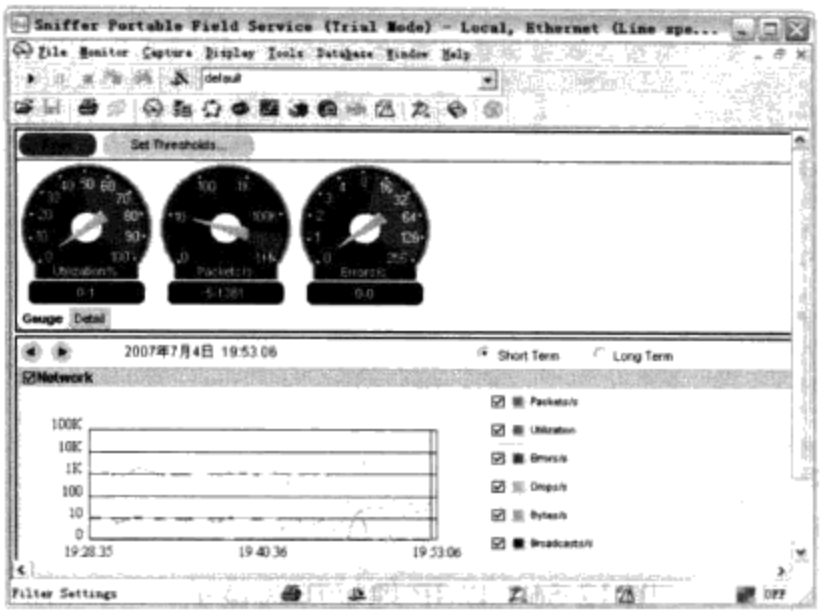


图 12-52　Sniffer 主界面

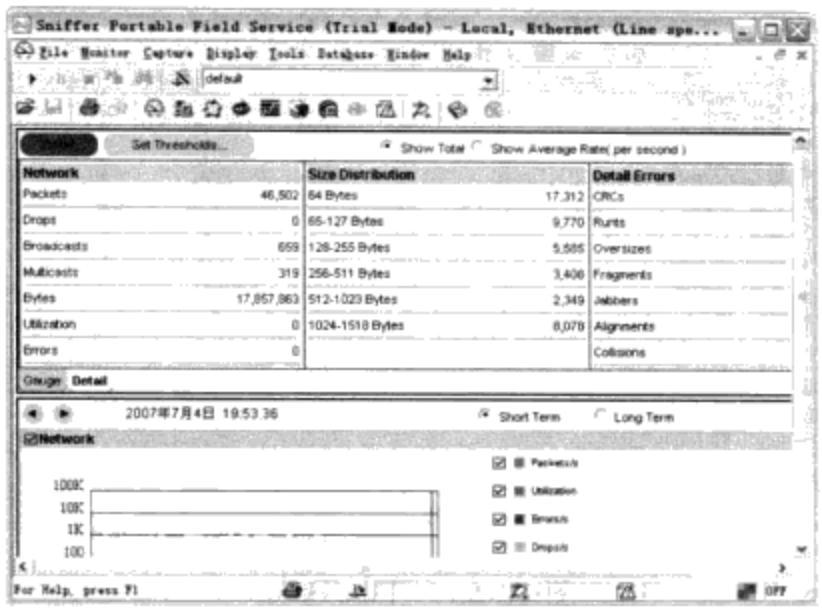


图 12-53　表格形式

在“Size Distribution”表格中列出了网络中数据包（包括 4 字节的 CRC）的分布状态，包括 64 字节、65～127 字节、128～255 字节等各种不同字节的数据包总数。“Detail Errors”表格中列出了错误出现率，即“Errors/s”表盘中显示的错误的详细情况。

Sniffer 的很多网络分析结果都可以设定阈值，若超出阈值，报警记录就会生成一条信息，并在仪表盘上以红色来标记阈值的警告值。网络管理员可根据警告信息，通过对超过阈值的次数和超出阈值的频率进行分析，从而让判断网络的健康状况。

单击仪表盘上的“Set Thresholds（设定阈值）”按钮，显示如图 12-54 所示“Dashboard Properties”对话框，根据网络状况配置仪表阈值即可，以保证仪表能准确的显示网络情况。

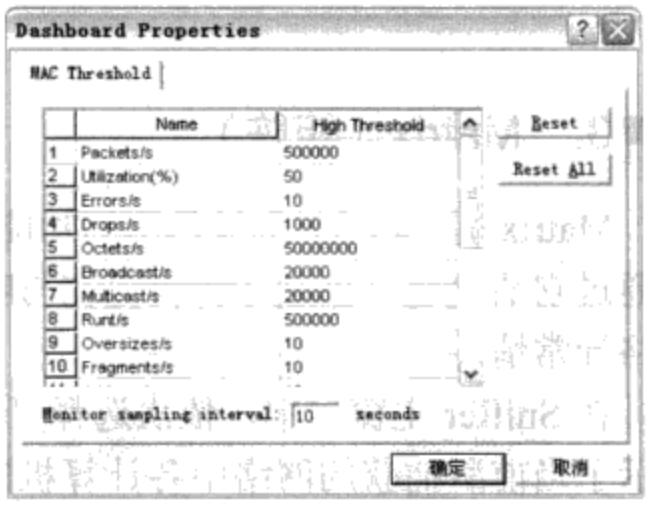


图 12-54　“Dashboard Properties”对话框

2. Host Table（主机列表）

Sniffer 的主机列表功能是以列表形式显示当前网络上计算机的流量信息。

依次选择“Monitor”→“Host Table”选项，显示如图 12-55 所示窗口，列出了当前所捕获的网络上的各个主机的流量信息。

- Hw Addr（硬件地址）：以 MAC 地址形式显示计算机。
- In Pkts（传入数据包）：网络上发送到此主机的数据包。
- Out Pkts（传出数据包）：本地主机发送到网络上的数据包。
- In Bytes（传入字节数）：网络上发送到此主机的字节数。
- Out Bytes（传出字节数）：本地主机发送到网络上的字节数。

在查看网络主机信息时，默认以 MAC 地址形式显示网络中的计算机。如果计算机处于局域网中，可以清楚地显示计算机的 MAC 地址。如果计算机处于 Internet 中，则不能获得计算机的 MAC 地址，此时会以 IP 地址形式显示。单击窗口下方的“IP”标签，如图 12-56 所示，

即可显示计算机的IP地址。

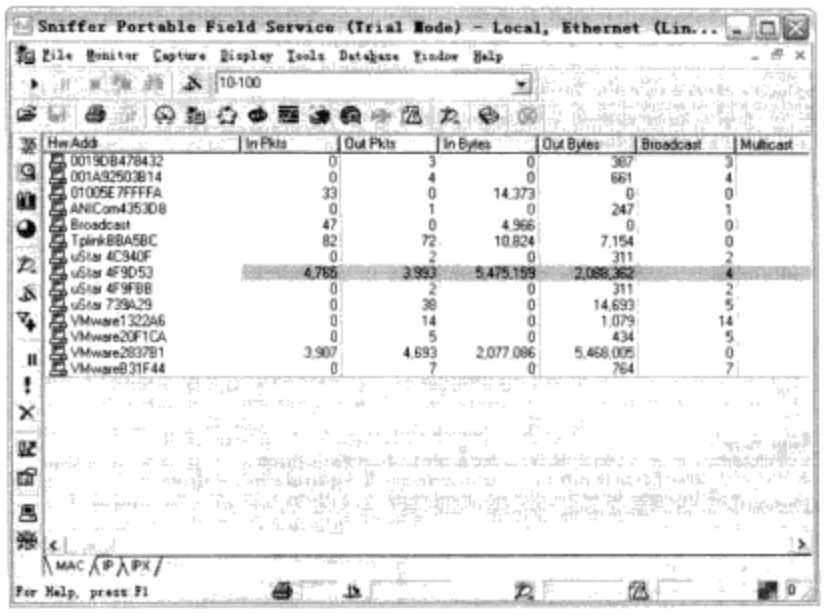


图12-55　主机列表

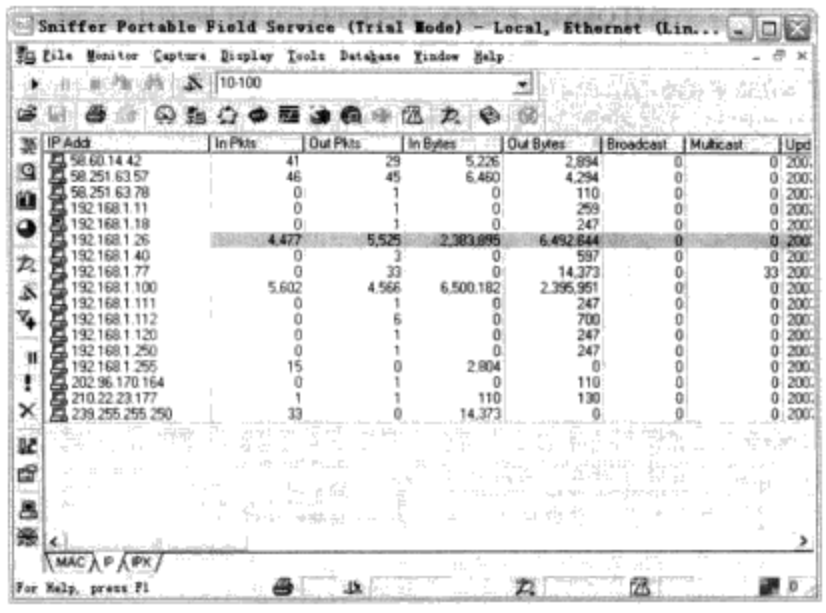


图12-56　以IP地址形式显示

提示　通过主机列表功能，可以查看某台计算机所传输的数据量。如果发现某台计算机在某个时间段内发送或接收了大量数据，例如某用户一天内就传输了数GB的数据，则说明该用户很可能在使用BT、PPLive等P2P软件。

3. Matrix（矩阵）

Matrix是Sniffer中最常用的功能之一，它以矩阵方式列出当前网络中的连接情况。管理员通过它清楚地掌握某计算机正在与哪些地址进行连接，并可查看因蠕虫、BT软件等造成的网络异常情况。

在Sniffer主窗口中，依次选择“Monitor”→“Matrix”选项，显示如图12-57所示窗口，显示了当前所捕获的网络中各计算机的连接情况。单击窗口下方的“IP”标签，可以以IP地址方式显示各主机。

在窗口空白处右击，在快捷菜单中选择“Zoom”选项，在子菜单中选择100%、200%、300%等选项，可以放大显示比例，以解决因为连接过多或连接太密集而无法查看具体连接情况的问题。

如果要详细查看某台主机的连接情况，可以在该窗口中只显示该主机的连接。右击要查看的主机IP地址，在快捷菜单中选择“Show Select Nodes”选项，显示如图12-58所示，此时可以清楚地看到该计算机正在与哪些地址连接。如果将鼠标指针放在连线上，还会显示出该主机所传输的数据大小。右击窗口并选择快捷菜单中的“Show All”选项，即可返回查看所有主机的连接情况。

提示　通过“Matrix”功能，管理员可以发现网络中使用BT等P2P软件或中了蠕虫病毒的用户。如果某个用户的并发连接数特别多，并且不断地向其他计算机发送数据，这就说明该计算机很可能中了蠕虫等病毒。此时，网络管理员应及时封掉该计算机所连接的交换机端口，并对该计算机查杀病毒。

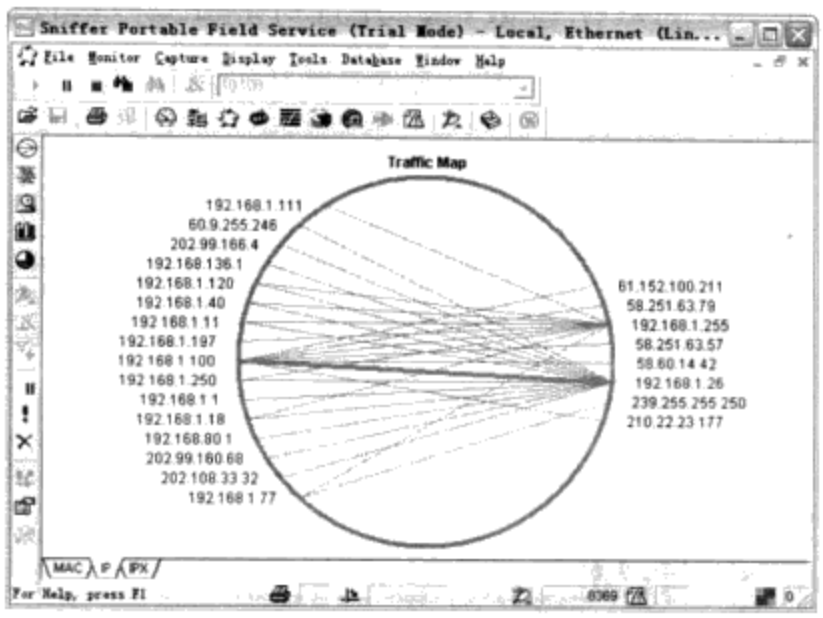


图 12-57　矩阵对话框

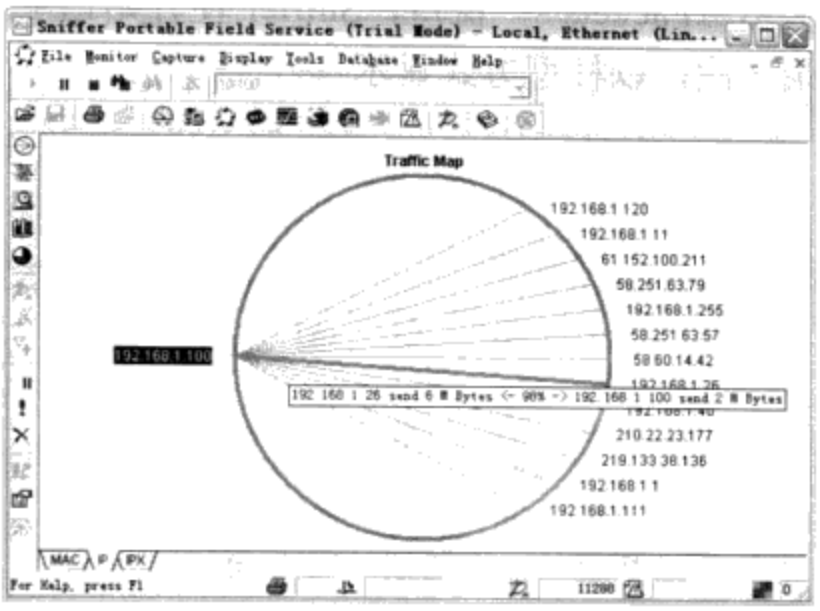


图 12-58　显示单个主机的连接情况

4. Application Response Time（应用响应时间）

Sniffer 的“Application Response Time”功能主要用来显示网络中 Web 网站的连接情况，可以看到局域网中有哪些计算机正在上网，浏览的是哪些网站等。

在 Sniffer 主窗口中，依次选择“Monitor”→“Application Response Time”选项，显示如图 12-59 所示“Application Response Time”对话框。该列表框中显示了局域网内的通信及数据传输大小，并且显示了本地计算机与 Web 网站的 IP 地址。

通过单击左侧工具栏中的图标，可以以柱形图方式显示网络中计算机的数据传输情况。不同顺序的图形柱代表右侧列表中的相应的连接，并以柱形的长短显示传输量的大小，如图 12-60 所示。

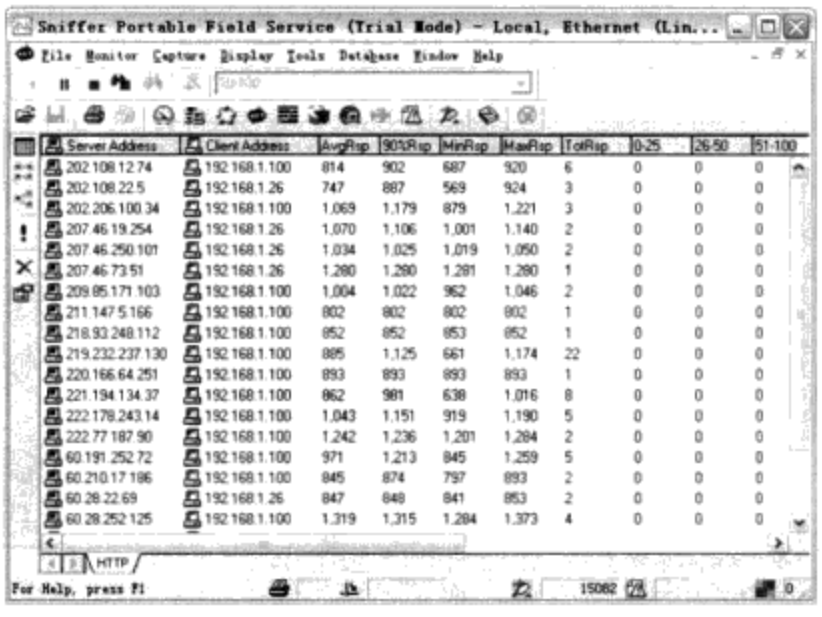


图 12-59　“Application Response Time”对话框

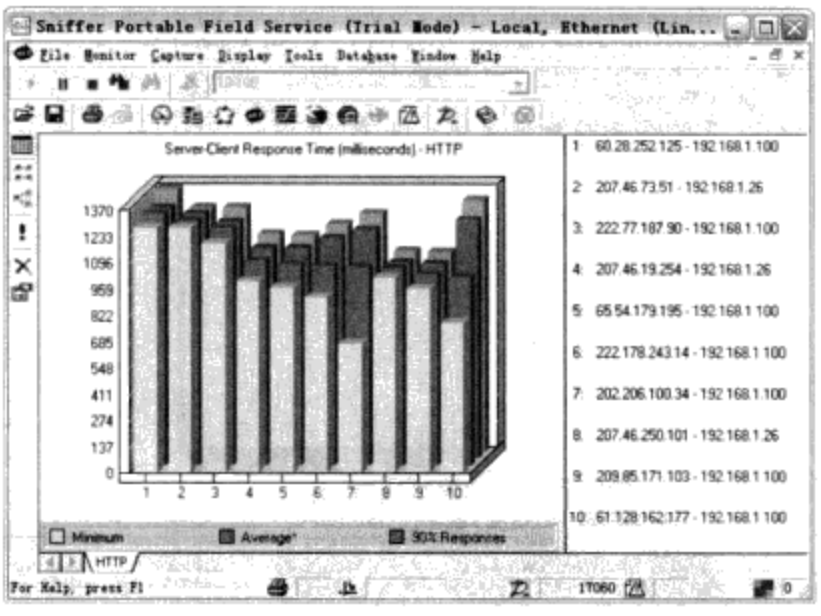


图 12-60　服务器-客户响应时间柱形图

5. History Samples（历史采样）

Sniffer 的历史采样功能记录了捕获过程中各个时间段的网络利用情况。在 Sniffer 主窗口中，依次选择“Monitor”→“History Samples”选项，显示如图 12-61 所示“History Samples”窗口，包括了多种记录。

现在我们来看一个网络中每秒发送的数据包数。双击“Packets/s”图标，显示如图 12-62

所示“Packets/s”窗口，Sniffer 便开始记录每秒所发送的数据包数量，并且每隔 15 秒钟便记录一次，以柱型方式显示。

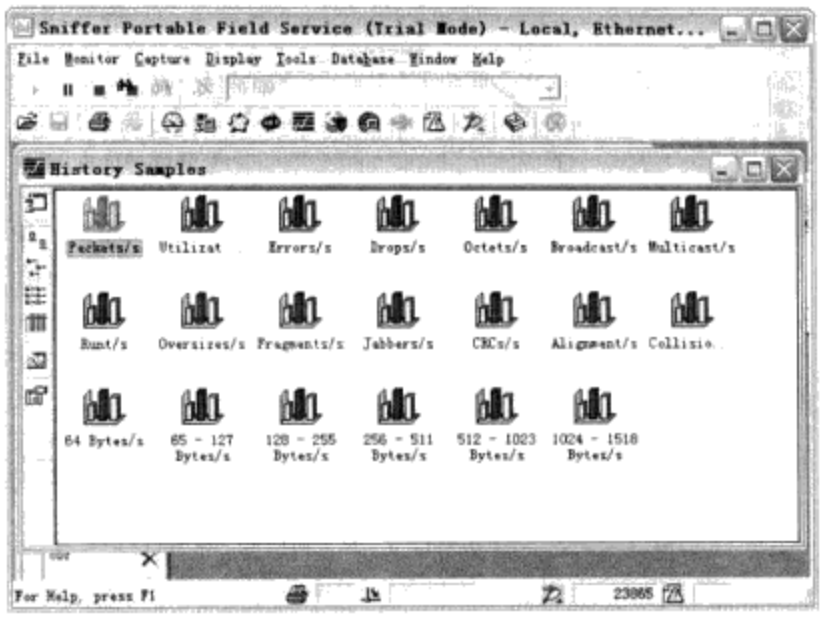


图 12-61　“History Samples”窗口

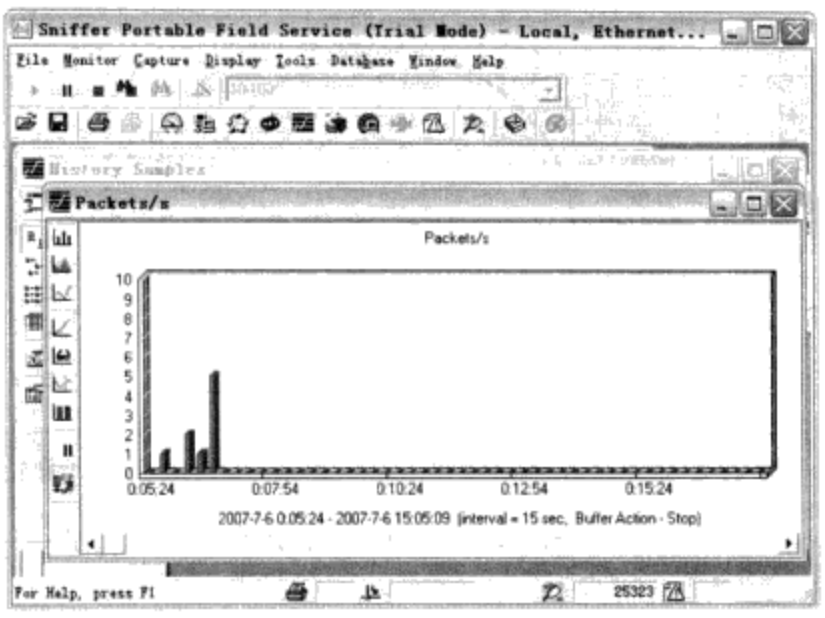


图 12-62　“Packets/s”窗口

经过一段时间的记录后，便可以将记录结果保存起来，便于管理员分析各个时间段的数据流量。依次选择“File”→“Save”选项保存即可。

6. Protocol Distribution（协议分类）

在 Sniffer 主窗口中，依次选择“Monitor”→“Protocol Distribution”选项，显示如图 12-63 所示窗口，以不同颜色的柱形显示网络中不同协议的使用情况。

通过单击左侧工具栏上饼型、表格型图标，还可以分别以饼型、表格等方式显示。如图 12-64 所示以表格方式显示。

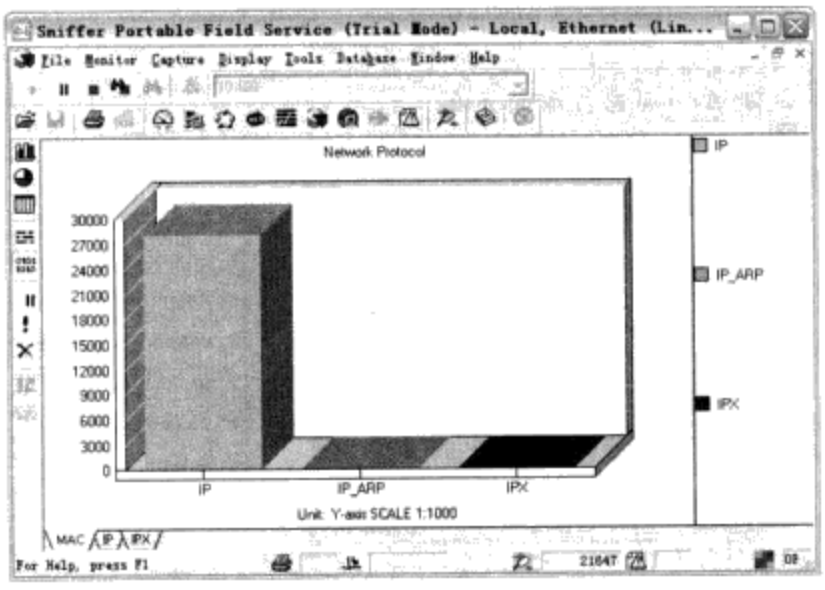


图 12-63　协议分布状况

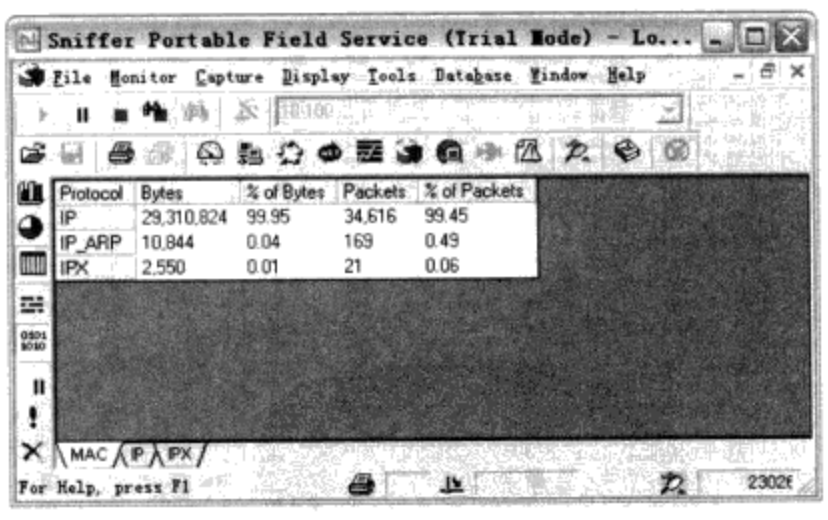


图 12-64　以表格方式显示

7. Global Statistics（全局统计）

Sniffer 的“Global Statistics”功能用来显示不同大小数据包的使用情况。

在 Sniffer 主窗口中，依次选择“Monitor”→“Global Statistics”选项，显示如图 12-65 所示“Global Statistics”对话框，默认以柱型方式显示不同大小数据包的使用情况。也可以单击左侧工具栏中的柱型图标，以柱型方式显示。

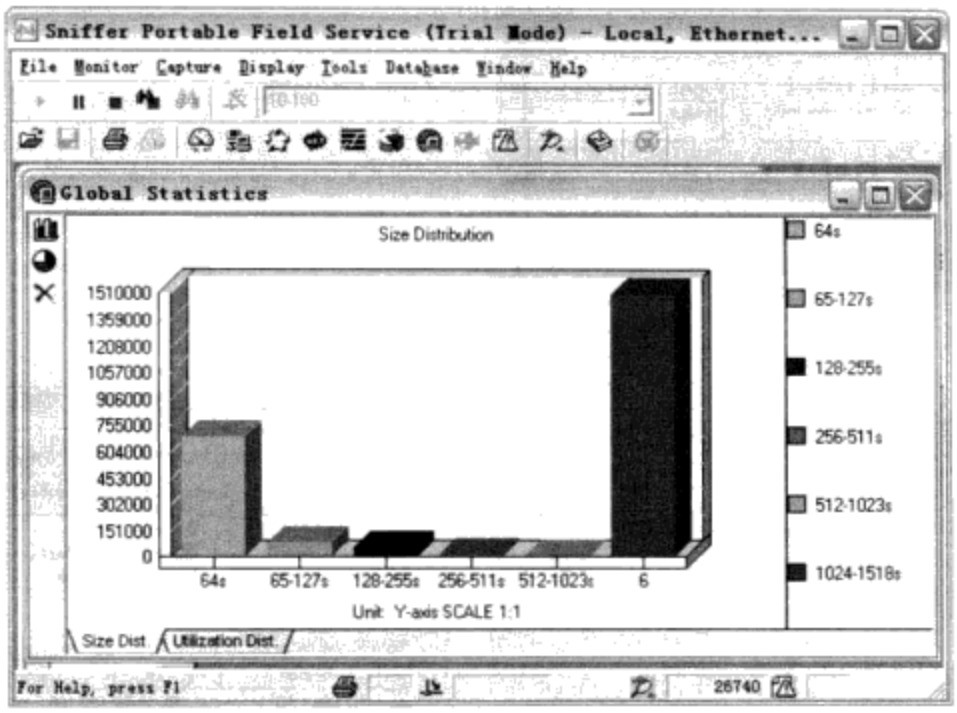


图 12-65 “Global Statistics”对话框

12.3.4 创建过滤器

默认情况下，Sniffer 会监控网络中所有传输的数据包，但在分析网络协议、查找网络故障时，有许多数据包并不是管理员所关心的。通过定义过滤器，管理员可以设定捕获条件，Sniffer 只接收与问题或事件相关的数据，从而便于进行数据分析。Sniffer 提供了捕获数据包前的过滤规则的定义，过滤规则包括 2、3 层地址的定义和几百种协议的定义。

1. 过滤 IP 地址

这里创建一个过滤器，使 Sniffer 只捕获 IP 地址段为 192.168.1.10 到 192.168.1.100 范围内传输的数据。

第 1 步，在 Sniffer 主窗口中，设置过滤方式，依次选择“Capture”→“Define Filer”选项，显示“Define Filter – Capture”对话框。在“Settings For”列表框中显示过滤器名，默认只有“default”，该过滤器对所有经过网卡的数据全部捕获。单击“Profiles”按钮，显示“Capture Profiles”对话框，单击“New”按钮，显示如图 12-66 所示“New Capture Profile”对话框，在“New Profile Name”文本框中键入新过滤器的名称如 10-100。最后，单击“OK”按钮返回“Capture Profiles”对话框，一个新的过滤器创建完成。

第 2 步，在“Settings For”列表框中，选择过滤器“10-100”，切换到“Address”选项卡，在“Station”列表框中用来设定要监视的 IP 地址范围。分别在“Station 1”和“Station 2”中键入 IP 地址 192.168.1.10 和 192.168.1.100，如图 12-67 所示。

第 3 步，单击“确定”按钮，过滤器创建完成。

在网络管理过程中，应设定多个过滤器，根据不同的监控用途进行选择。在 Sniffer 窗口中，依次选择“Capture”→“Select Filter”选项，显示“Select Filter”对话框，在左侧列表框中即可选择要使用过滤器，并可看到过滤器设定的条件，如图 12-68 所示。单击“确定”按钮，应用所选择的过滤器，Sniffer 会根据过滤器所设置的条件来捕获网络中特定的数据。

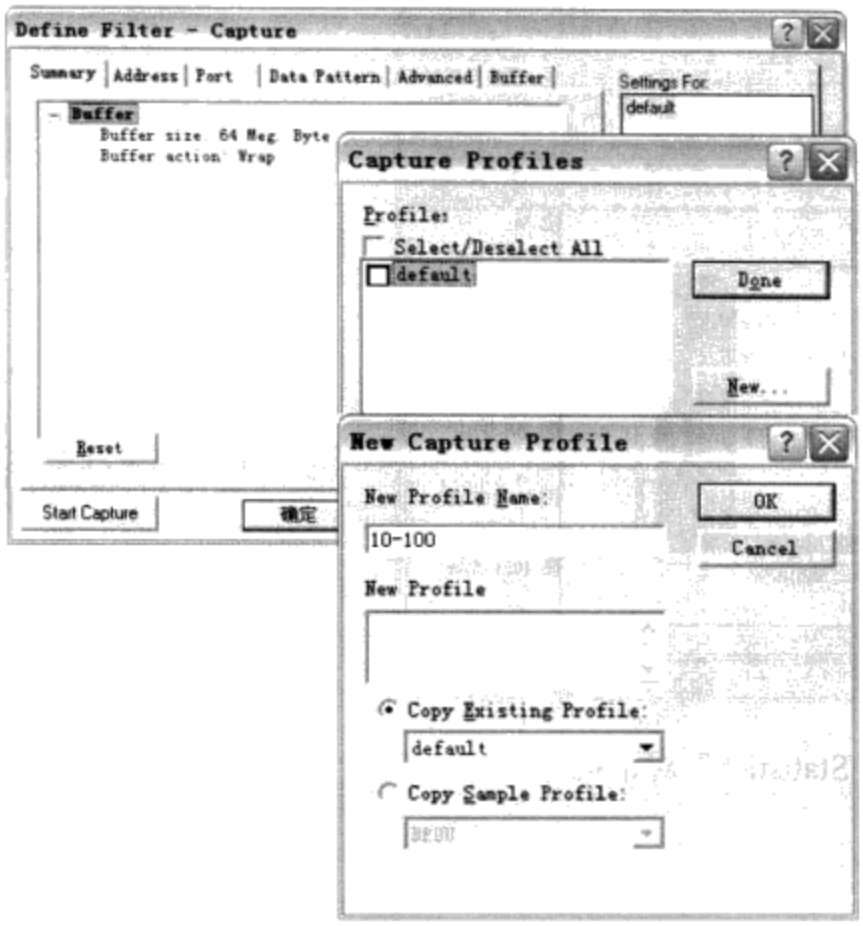


图 12-66 创建过滤器

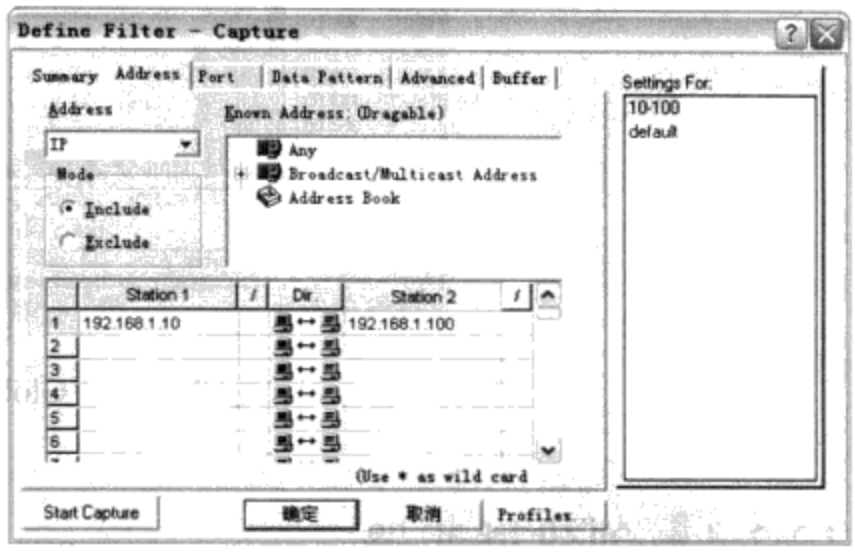


图 12-67 “Address”选项卡

图 12-68 “Select Filter”对话框

2. 过滤端口

Sniffer 4.8/4.9 中增加了端口过滤功能，可以让 Sniffer 只捕获特定端口内传输的数据，可以是固定的一个或几个端口，也可以是一个端口范围。这里创建一个过滤器，只捕获 80 和 445 端口所传输的数据，来监控网络中访问 Internet 网页和网络共享的数据。

第 1 步，先创建一个过滤器，如“80-445”。在“Define Filter- Capture”对话框中，切换到“Port”选项卡，在“Port 1”的 1 和 2 文本框中分别键入 80、445，“Port 2”中为“Any”即可，如图 12-69 所示。

第 2 步，单击“确定”按钮，只捕获 80 和 445 端口数据的过滤器创建成功。在选择使用该过滤器监控网络时，Sniffer 就会只捕获网络中通过 80 和 445 的数据，从而了解网络资源的占用情况。

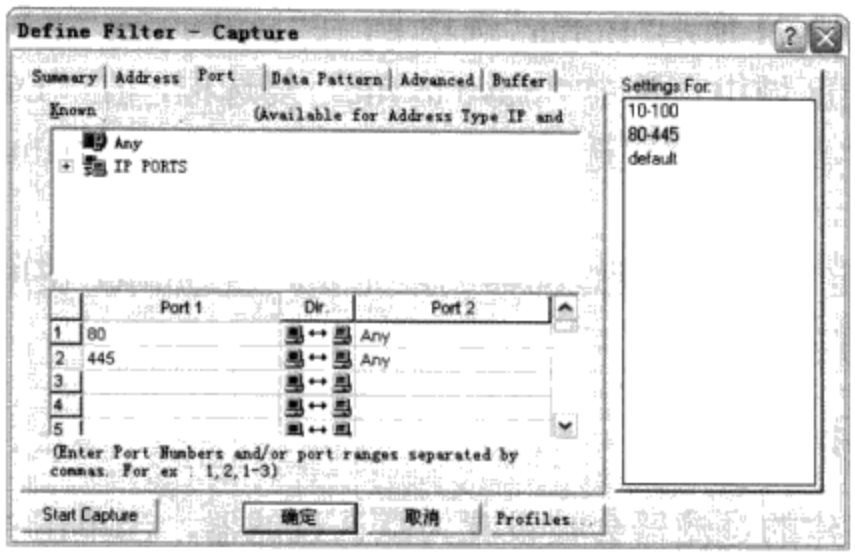


图 12-69 “Port”选项卡

3. 过滤网络协议

虽然 Sniffer 可以通过 IP 地址、端口等形式捕获数据，但如果客户端更改了 IP 地址，或一些软件使用随机端口，如 BT、PPLive 等软件，每次都使用不同的端口，那么 Sniffer 将很难捕获到相应的数据。此时，可以根据网络协议进行捕获，Sniffer 支持网络中大部分的网络协议，无论客户端怎样改，软件所使用的协议是不会变的，通过监控协议，可以使各种软件无所遁形

这里创建一个过滤器，只捕获网络中使用 FTP 协议传输的数据，来查看有多少人在通过 FTP 下载文件。

第 1 步，创建一个新过滤器，例如 FTP。

第 2 步，选择“FTP”过滤器，切换到“Advanced”选项卡，依次展开“Available”→“Protocols”→“IP”→“TCP”，选中“FTP”复选框，如图 12-70 所示，使该过滤器只捕获使用 FTP 协议传输的数据。

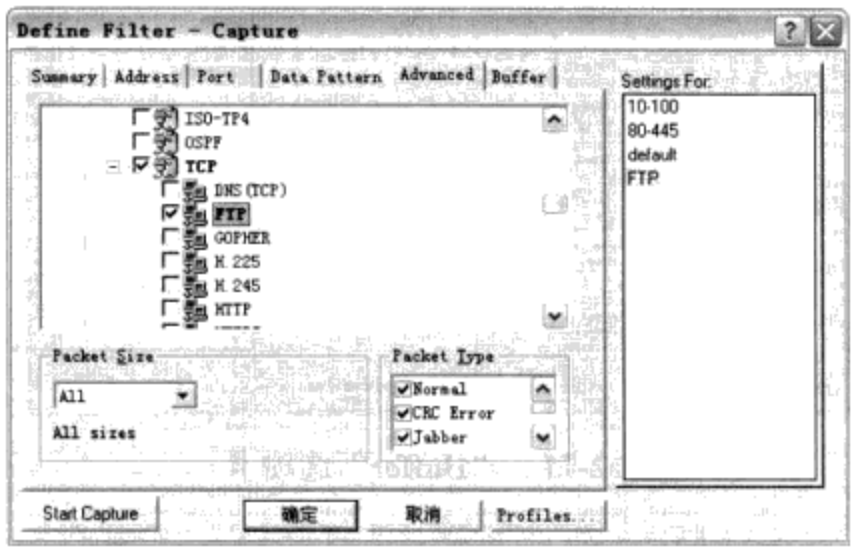


图 12-70 “Advanced”选项卡

第 3 步，单击“确定”按钮保存，即可使 Sniffer 使用该过滤器只捕获使用 FTP 协议传输的数据。

4. 设置缓冲器

缓冲器用来临时保存 Sniffer 捕获的数据，它占用的是计算机的内存。当缓冲器已满后，Sniffer 就会自动停止捕获，但缓冲器中的内容不会自动保存，当重新捕获或关闭 Sniffer 时，缓冲器会自动清空。Sniffer 4.9 的缓冲器大小默认为 64 MB，比以前版本大了许多。网络管理员可以创建一个过滤器，自定义缓冲器的大小，并可设置将缓冲器中的数据保存到文件中，以备日后进行分析。

这里创建一个捕获网络中使用 HTTP 协议数据的过滤器，设置缓冲区大小为 40 MB，缓冲器中的数据保存到 E:\sniffer 文件夹下。

第 1 步，创建一个过滤器如“new buffer”，切换到“Advanced”选项卡，依次选择“IP”→“TCP”→“HTTP”。

第2步，切换到如图12-71所示“Buffer”选项卡，在“Buffer size”下拉列表框中选择“40 MB”，在“Capture buffer”选项区域中，选中“Save to file”复选框，在“Director”文本框中键入地址：E:\sniffer\，或单击“浏览”按钮选择保存目录即可，在“Filename”文本框中设置保存的文件名。

第3步，单击“确定”按钮，新过滤器创建完成。当Sniffer使用该过滤器捕获时，即可将捕获的数据保存到文件中。

5. 过滤器的使用

在Sniffer中，新创建的过滤器会被设置为默认过滤器，当单击“Start”时就会自动使用新过滤器捕获数据。如果要使用其他过滤器，则需要选择。

第1步，依次选择“Capture”→“Select Filter”选项，显示如图12-72所示“Select Filter”对话框，在左侧的列表框中显示了所有的过滤器。其中，“Capture”列表框中显示的是用户自定义的过滤器，而“PreDefined”列表框中则是Sniffer内置的过滤器。当选择一个过滤器后，在右侧窗口中会显示该过滤器定义的详细信息。

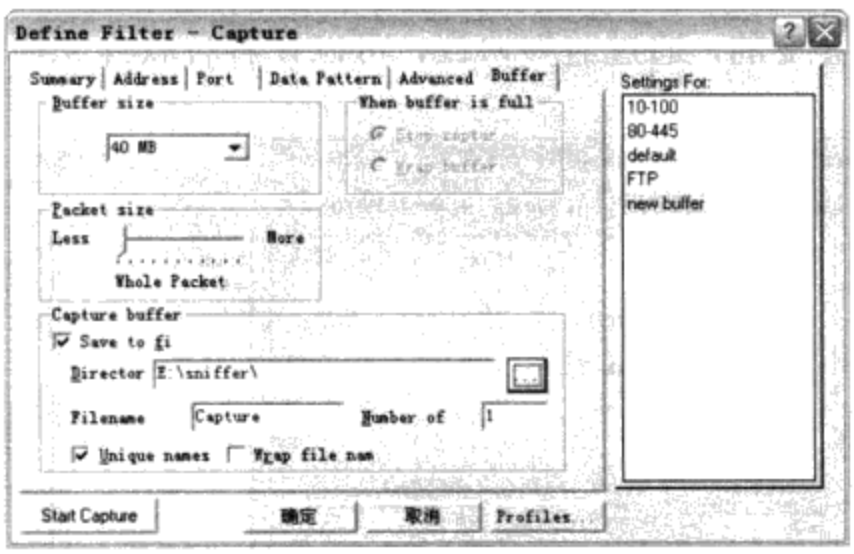


图12-71 “Buffer”选项卡

图12-72 “Select Filter”对话框

第2步，单击“确定”按钮即可应用。

第3步，单击“Start”按钮，即可根据所选择的过滤器中定义的条件捕获网络中的数据。

另外，Sniffer中所有的过滤器都会显示在工具栏上的下拉列表框中，在该下拉列表框中单击要使用的过滤器，然后单击“Start”按钮，即可根据选择的过滤器捕获数据。

12.3.5 捕获数据

通过Sniffer进行网络和协议分析，需要先捕获网络中的数据。默认状态下，由于Sniffer没有进行过滤设置，会捕获网络中所有的数据。

第1步，单击工具栏上的▶按钮，或依次选择“Capture”→“Start”选项，显示“Expert”窗口，Sniffer开始捕获网络中的数据，并显示所捕获到的数据的概要信息，如图12-73所示。

第2步，如果要查看当前捕获的各种数据，单击对话框左侧的“Service”、“Connection”等选项，在右侧即可显示相应数据的概要信息。单击窗口左侧“Objects”选项卡，可显示出当前所监视对象的详细信息，如图12-74所示。

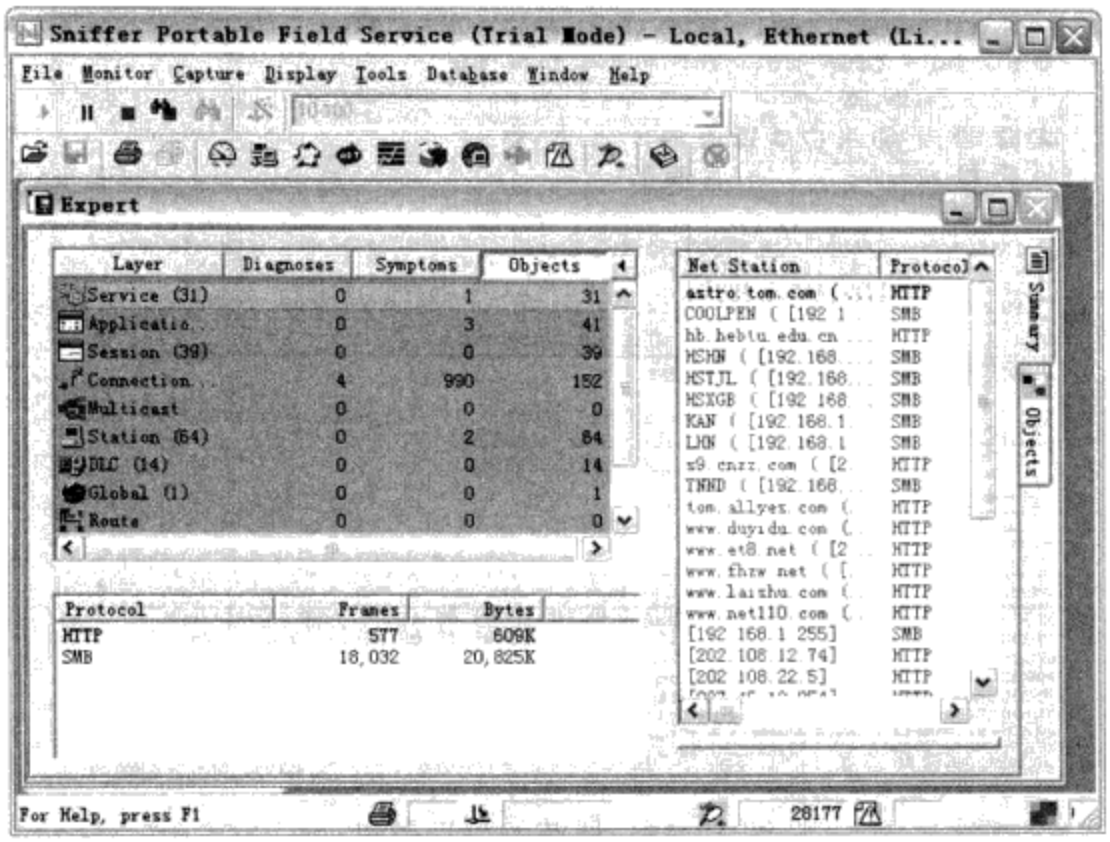


图 12-73 “Expert”对话框

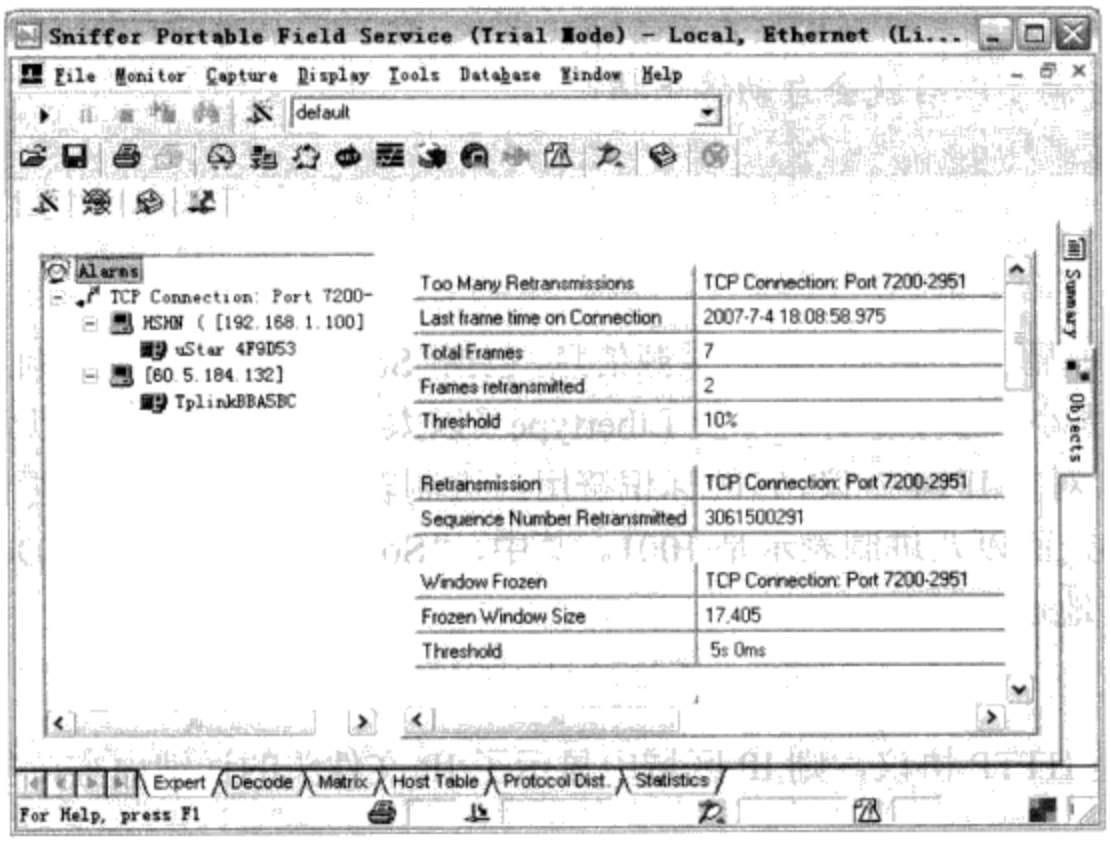


图 12-74 “Objects”选项卡

第 3 步，当 Sniffer 捕获了一定的数据，就可以停止捕获并进行分析。单击工具栏上■快捷按钮，或依次选择“Capture”→“Stop”选项，即可停止捕获。此时，管理员就查看并分析所捕获的数据，从而了解网络的使用状况。

12.3.6 分析捕获的数据

依次选择“Capture”→“Display”选项，即可查看所有捕获的内容了。选择该窗口下方的“Decode（解码）”选项卡，显示如图 12-75 所示窗口，该窗口共分为 3 个部分，由上到下依次为：总结、详细资料和 Hex 窗格的内容，可以查看所捕获的每个帧的详细信息。

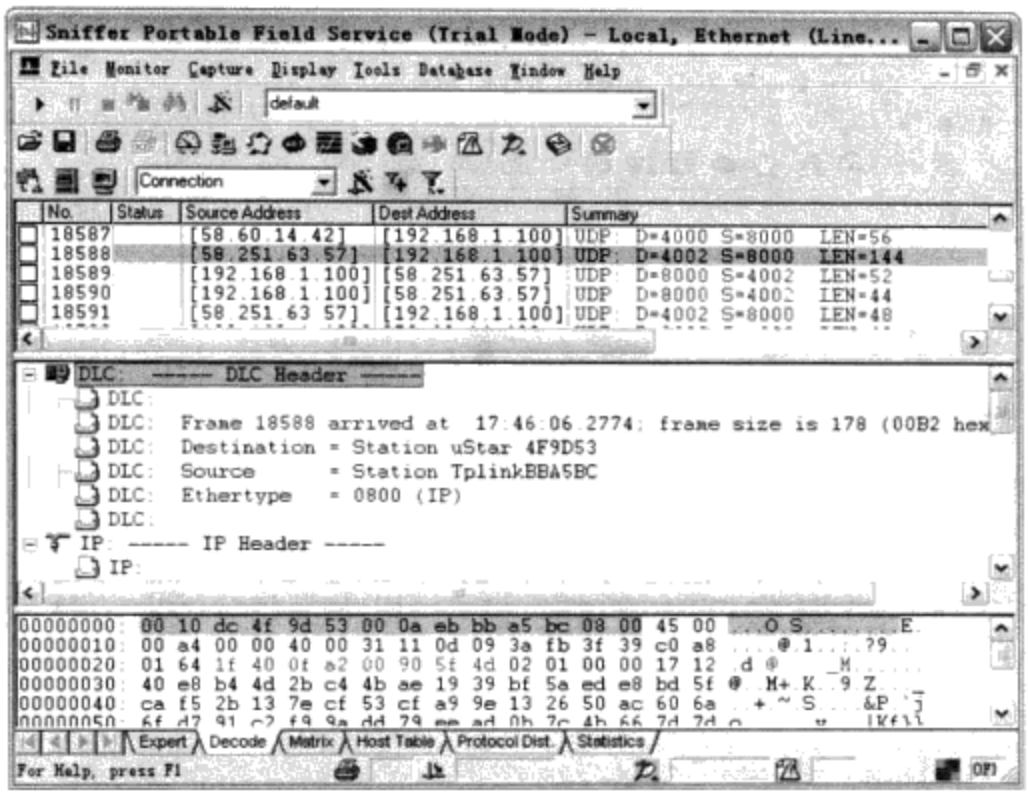


图 12-75 捕获的数据信息

提示 Sniffer所捕获的数据保存在缓冲区中。Sniffer 4.9的缓冲区大小默认为64 MB，当缓冲区满了以后就会自动停止捕获。

■ DLC

在DLC区域中显示了捕获的帧的来源信息，包括“Source Addess（源地址）”、“Dest Address（目标地址）”、帧大小（以字节计）以及Ethertype（以太类型）。在这里，以太类型值为0800，表示是IPv4协议。对于IPv4协议，它的标识符用二进制表示是2048，十六进制表示就是0800，十进制表示是513，而以八进制表示是1001。其中，“Source Addess”或“Dest Address”中会显示网卡的MAC地址。

■ IP

如果捕获的是HTTP协议，则IP区域中显示了IP文件头的详细内容，如图12-76所示，各内容含义如下。

- Version（版本）：版本序号为4，代表IPv4。
- Header length：Internet文件头长度，为20个字节。
- Type of service（服务类型值）：该值为00，会看到Tos下面一直到总长的部分都是0。这里可以提供服务质量（QoS）信息。每个二进制数位的意义都不同，这取决于最初的设定。例如，正常延迟设定为0，说明没有设定为低延迟，如果是低延迟，设定值应为1。
- Total length（总长度）：显示该数据的总长度，为Internet文件头和数据的长度之和。
- Identification 该数值是文件头的标识符部分，当数据报被划分成几段传送时，发送数据的主机可以用这个数值来重新组装数据。
- Flag（标记）：数据报的“标记”功能，例如，数据报分段用0标记，未分段用1标记。

- Fragment offset（分段差距）：分段差距为 0 个字节。可以设定 0 代表最后一段，或者设定 1 代表更多区段。这里这个值为 0。分段差距用来说明某个区段属于数据包的哪个部分。
- Time to live（保存时间）：表示 TTL 值的大小，说明一个数据包可以保存多久。
- Protocol（协议）：显示协议值，在 Sniffer 中代表 TCP 协议。文件头的协议部分只说明要使用的下一个上层协议是什么，在这里为 TCP。
- Header checksum（校验和）：这里显示了校验和（只在这个文件头中使用）的值，并且已经做了标记，表明这个数值是正确的。
- Source address（来源地址）：显示了数据的来源地址。
- Destination address（目的地址）：显示了数据访问的目的地址。

■ UDP

IP 文件头（如图 12-77 所示）下面为 TCP 或 UDP 文件头，这里为 UDP 文件头，包括下列信息。

- Source port（源端口）：显示了所使用的 UDP 协议的源端口。
- Destiantion port（目的端口）：显示了 UDP 协议的目的端口。
- Length（长度）：表示 IP 文件头的长度。
- Checksum（校验和）：显示了 UDP 协议的校验和。
- Byep（s）of date：表示有多少字节的数据。

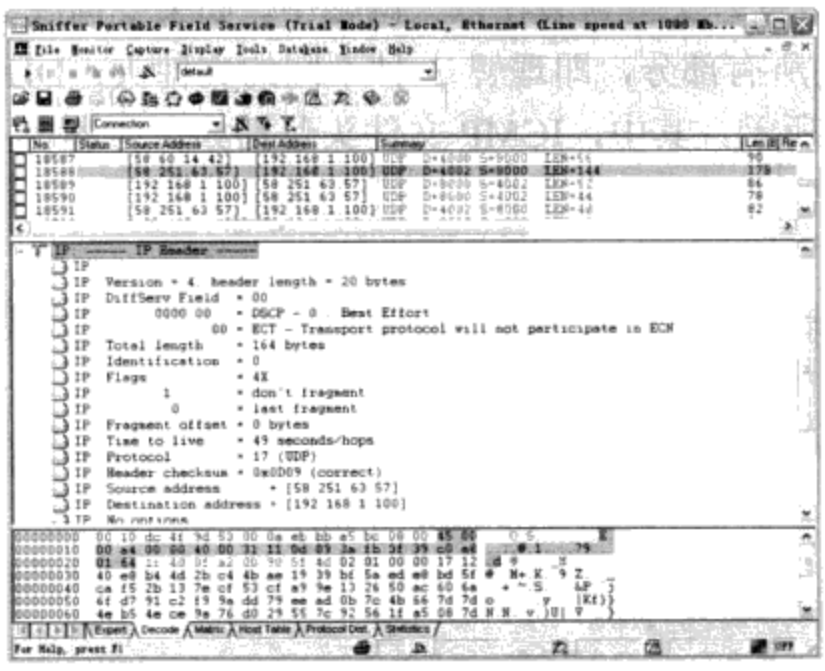


图 12-76　IP 文件头信息

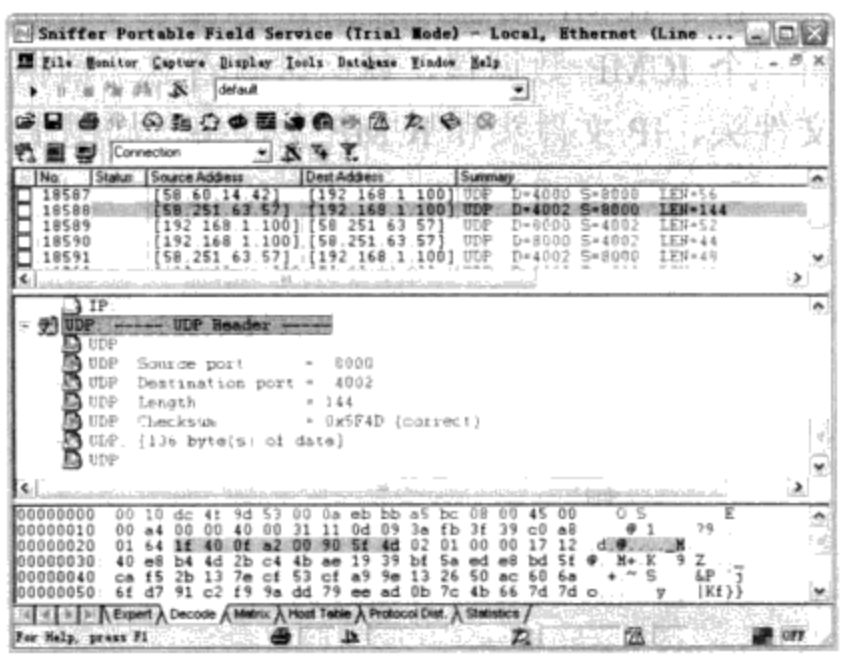


图 12-77　UDP 文件头信息

■ ARP

ARP 构架（如图 12-78 所示）中具有如下的一些信息。

- Hardware type（硬件类型）：这是一个 16 比特字段，用来定义运行 ARP 的网络的类型。每一个局域网基于其类型被指派给一个整数。例如，以太网是类型 1。ARP 可使用在任何网络上。
- Protocol type（协议类型）：这是一个 16 比特字段，用来定义协议的类型。例如，对 IPv4 协议，这个字段的值是 0800。ARP 可用于任何高层协议。
- Length of hardware address（硬件长度），这是一个 8 比特字段，用来定义以字节为单

位的物理地址的长度。例如，对以太网这个值是6。

- Length of Protocol address（协议长度）：这是一个8比特字段，用来定义以字节为单位的逻辑地址的长度。例如，对IPv4协议这个值是4。
- Opcode（操作） 这是一个16byte的字段，用来定义分组的类型。已定义了两种类型：ARP请求① ARP回答第2步。
- Sender's Hardware address（发送站硬件地址）：这是一个可变长度字段，用来定义发送站的物理地址的长度。例如，对以太网这个字段是6字节长。
- Sender's Protocol address（发送站协议地址）：这是一个可变长度字段，用来定义发送站的逻辑（例如IP）地址的长度。对于IP协议，这个字段是4字节长。
- Target Hardware address（目标硬件地址）：这是一个可变长度字段，用来定义目标的物理地址的长度。例如，对以太网这个字段是6字节长。对于ARP请求报文，这个字段是全0，因为发送站不知道目标的物理地址。
- Target Protocol address（目标协议地址）：这是一个可变长度字段，用来定义目标的逻辑地址（例如，IP地址）的长度。对于IPv4协议，这个字段是4字节长。

■ ICMP

ICMP协议即Internet控制信息协议，是TCP/IP协议栈的一部分。ICMP是一种非常强大的工具，允许报告 20 种以上不同的网络状况。首先需要创建一个新的 ICMP 过滤器，即在“Advanced”选项卡中选中“IP”列表中的“ICMP”协议，捕获足够数据后便可以进行分析。

由于ICMP信息封装在IP数据包中，而IP数据包又会封装在以太网帧中，如果要彻底分析一个 ICMP 数据包，就必须查看这个数据包的所有部分，即理解 3 种不同的文件头：DLC文件头、IP文件头和ICMP文件头，如图12-79所示。其中，ICMP文件头包括如下内容。

- Type=8（Echo）：ICMP Echo有两种类型，类型8是请求，而类型0是响应。
- Coad：该代码现在在ICMP Echo信息中并不常用，经常设定为0。
- Checksum：IP文件头校验和不能用来证明高层协议数据的完整性，所以ICMP信息用自己的校验和来确保数据在传输过程中没有被中断。
- Identifier与Sequence number：这些数字由发送方式生成，用来将响应与请求匹配在一起。

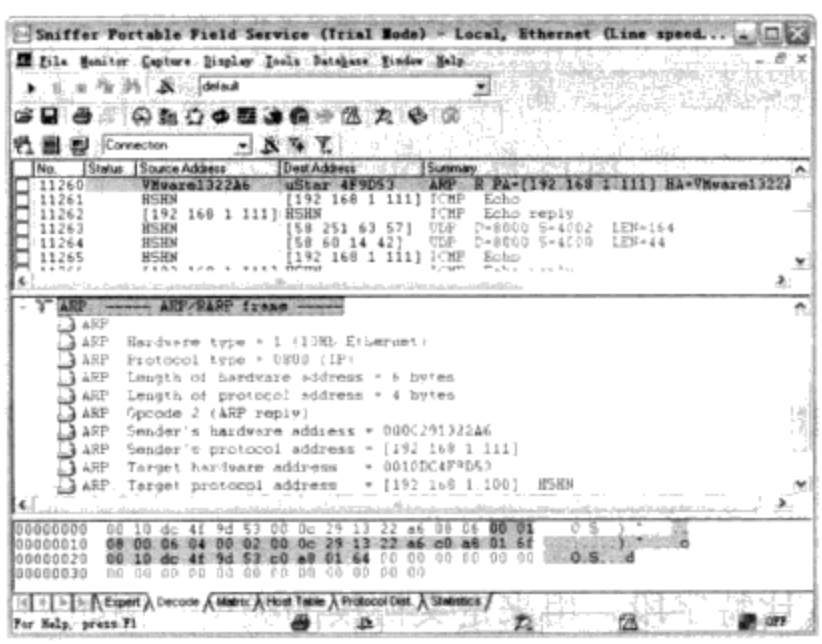


图 12-78 ARP 文件头信息

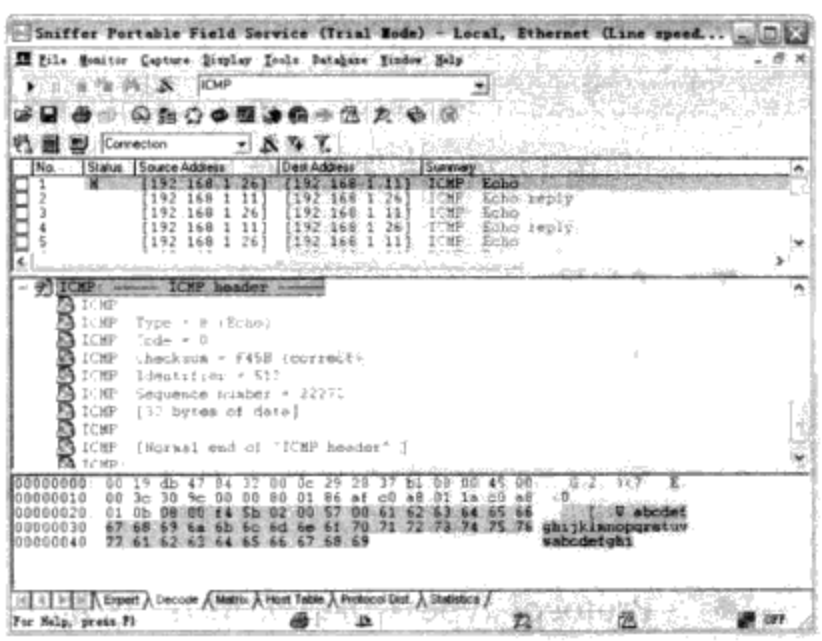


图 12-79 ICMP 文件头

■ Hex

“Decode”窗口最下方为“Hex 窗格”，这里显示的内容最直观，但也难以理解。“Hex 窗格”中的信息是十六进制代码的信息集合。数据的传输是按照二进制系统为基本标准进行的，二进制数据还可以转换为十六进制、十进制和八进制的格式，在“Hex 窗格”中查看数据时，看到的就是处于传输状态的原始 ACS II 格式的数据。

■ Matrix

Sniffer 的矩阵功能可以直观地显示网络中各计算机之间的连接。单击窗口下方的“Matrix”标签，显示如图 12-80 所示，以“Matrix”方式显示了网络中各计算机之间的连接情况，默认以 MAC 地址代表计算机。这里的图型界面类似于 Sniffer 监视功能中的“Matrix”界面。所不同的是，此处显示的是固定数据，即曾经捕获到的数据，而“Monitor”中的“Matrix”是不断变化的，并会随时添加即时捕获的数据。

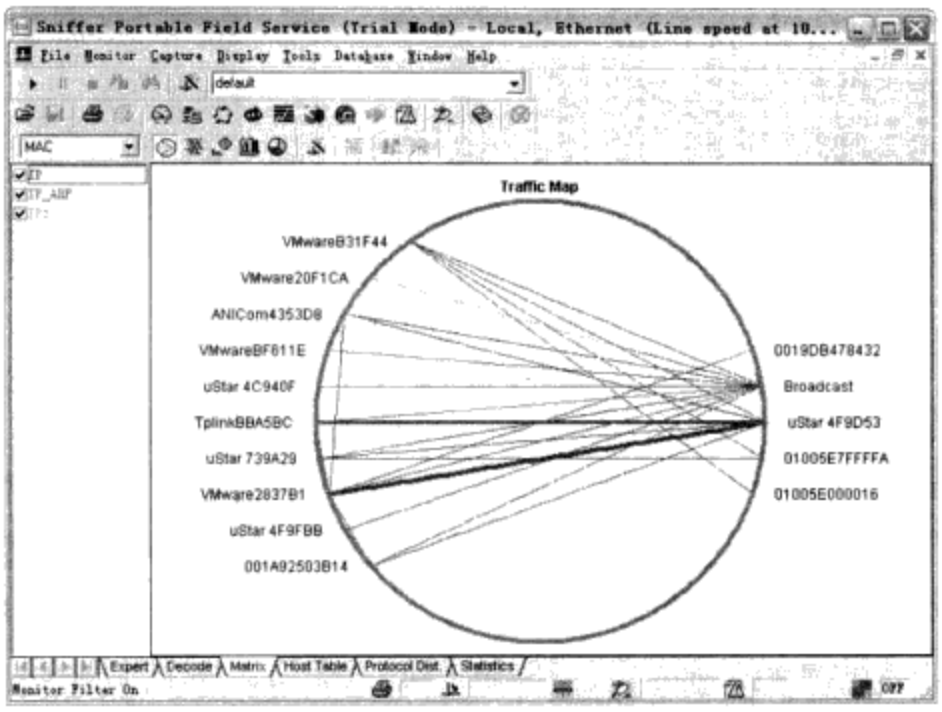


图 12-80 “Matrix”图表

为便于查看，可以以 IP 地址形式显示计算机。在“MAC”下拉列表框中选择“IP”选项，即可显示各计算机的 IP 地址，并使用不同颜色的连线来显示各连接所使用的不同协议，如图 12-81 所示。

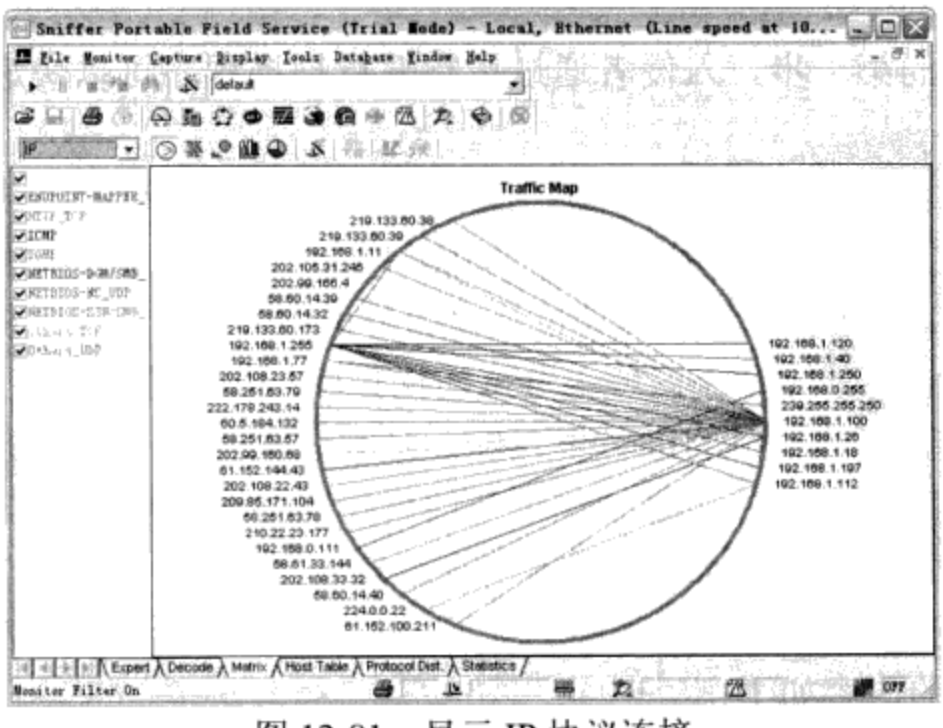


图 12-81 显示 IP 协议连接

■ Host Table

主机列表是一个很有用的功能，如图 12-82 所示。该功能可以清楚地显示出在该捕获过程中各计算机所传输的数据，并且可以根据所传输数据多少按顺序排列。与“Matrix”结合使用，网络管理员可以轻松分析出各计算机的使用情况。

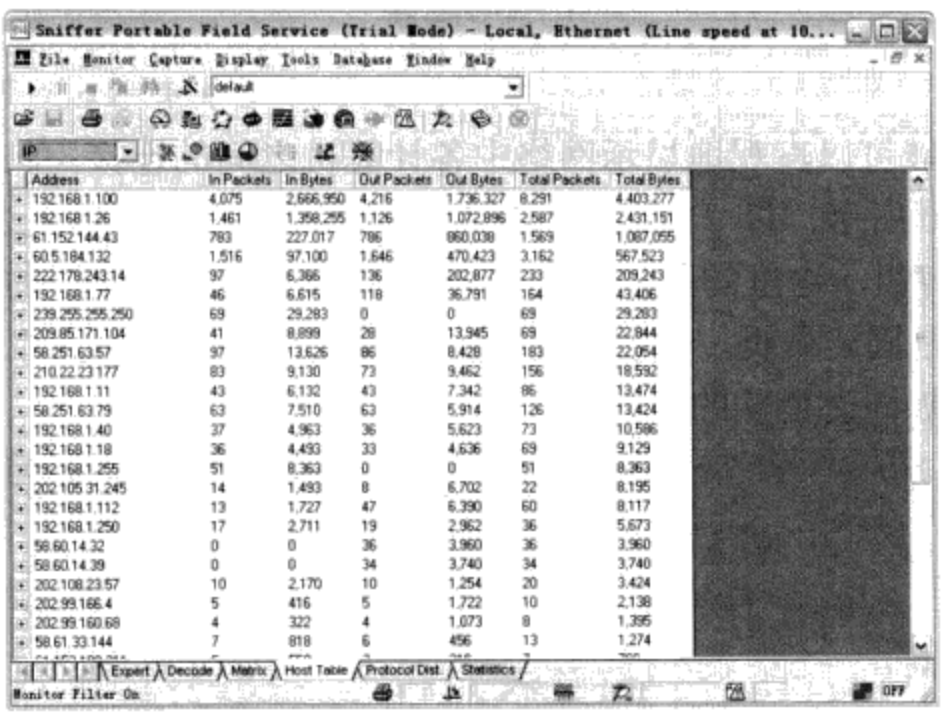


图 12-82 “Host Table”窗口

例如，当管理员发现上网速度特别慢，而服务器又运行正常，即可通过 Sniffer 的“HostTable”和“Matrix”功能进行分析。如果在“Host Table”中发现有计算机在某段时间内传输的数据特别多，并且在“Matrix”中显示该计算机有大量的并发连接，由此可以得出结论：该计算机很可能在使用 BT 等 P2P 软件下载文件。为避免该用户过多占用带宽，管理员即可中止该用户的下载。

12.3.7 Sniffer 应用实例

1. 发现并阻止外部主机恶意扫描网络

扫描是网络入侵的第一步，入侵者通过运行恶意扫描程序可以快速发现目标主机存在的漏洞，以便实施入侵。

使用 sniffer 在代理服务器 VLAN 监控网络传输状况时，发现有一个 IP 地址（219.248.188.130）的并发连接数量非常多，如图 12-83 所示。由于局域网的 IP 地址范围为 211.82.214.0～211.82.223.0，显然该 IP 地址是来自外网的。同时，该主机与局域网内的大部分计算机建立连接，所以很可能是正在使用恶意扫描程序扫描网络。

为了防止该用户对本地网络的进一步入侵，必须立即阻断其与本地网络的所有通信，可以通过创建 IP 访问列表解决这一问题。如果使用代理服务器共享接入 Internet，则可以在核心交换机上部署访问列表，如果使用路由器或防火墙接入 Internet，则可以直接在网络接入设备上部署该访问列表。注意，新的访问列表条目一定要部署在该 IP 访问列表的“permit ip any any”之前。访问列表条目的内容如下：

```
access-list 180 deny   ip any host 219.248.188.130
access-list 180 deny   ip host 219.248.188.130 any
```

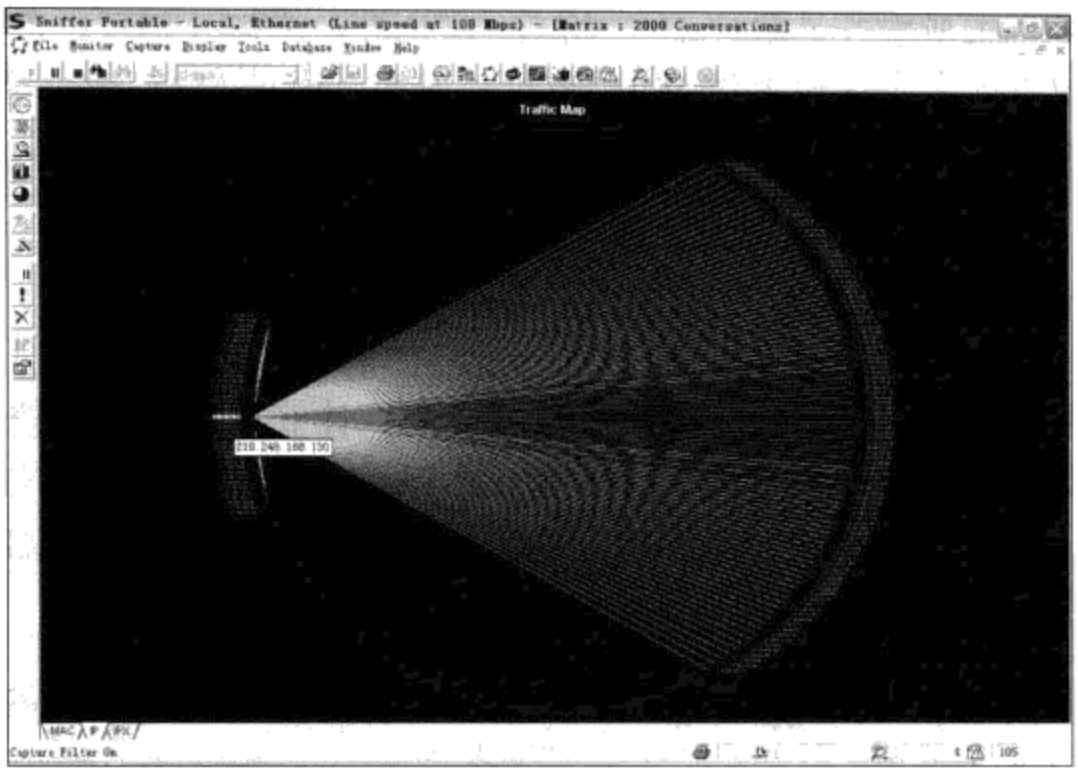


图 12-83　恶意扫描

2. 查找盗用 IP 地址的计算机

在企业网络中，通常使用 DHCP 服务器为客户端计算机分配 IP 地址，IP 地址被盗用的情况时有发生，如果管理员在网络正常运行时创建了客户端计算机的 MAC 地址列表，则可以通过 ping 和 arp 命令解决这一问题。但是，如果局域网中禁止运行 ping 命令，则只能通过 sniffer 捕获目标 IP 地址的数据并分析，获得其 MAC 地址，然后再与 MAC 地址对照表，找出盗用别人 IP 地址的计算机。

第 1 步，启动 Sniffer 并创建一个过滤器，用来监听被盗用的 IP 地址上传输的数据。

第 2 步，单击“Start”按钮开始捕获数据，当捕获到一定数据后停止并显示，开始解码所捕获到的数据。此时，在“DLC”区域的“Station”字段中，即可看到盗用 IP 地址的计算机网卡的 MAC 地址，如图 12-84 所示。

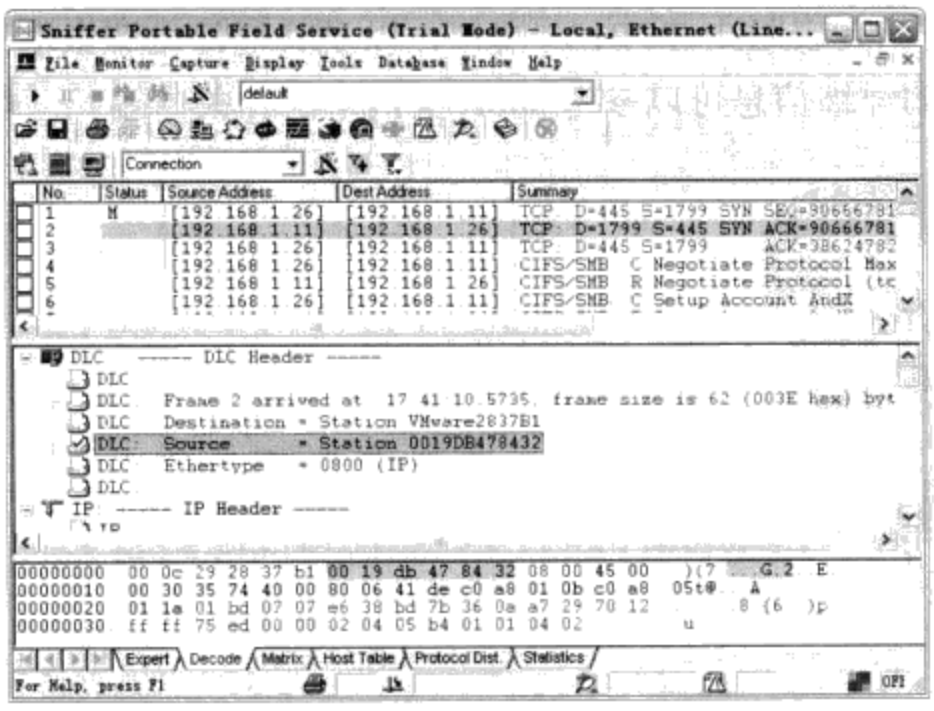


图 12-84　“Expert”窗口

第3步，找到MAC地址后，查看MAC地址登记表，即可找到盗用IP地址的计算机了。

提示 虽然记录所有计算机网卡的MAC地址有些麻烦，不过，用户可以更改IP地址，但很少会更改网卡的MAC地址。因此，通过MAC地址来识别计算机也是一个不错的方法。

3. 阻止蠕虫泛滥

蠕虫泛滥的主要特征就是网络运行速度急剧下降，计算机的反应也较为迟缓。例如，在使用Sniffer Pro监控代理服务器所在VLAN时，发现许多计算机同时与网络内部的许多计算机通信（如图12-85所示）。经进一步查看，发现使用的端口为TCP 135端口，由此可见，是蠕虫病毒导致该故障的发生。

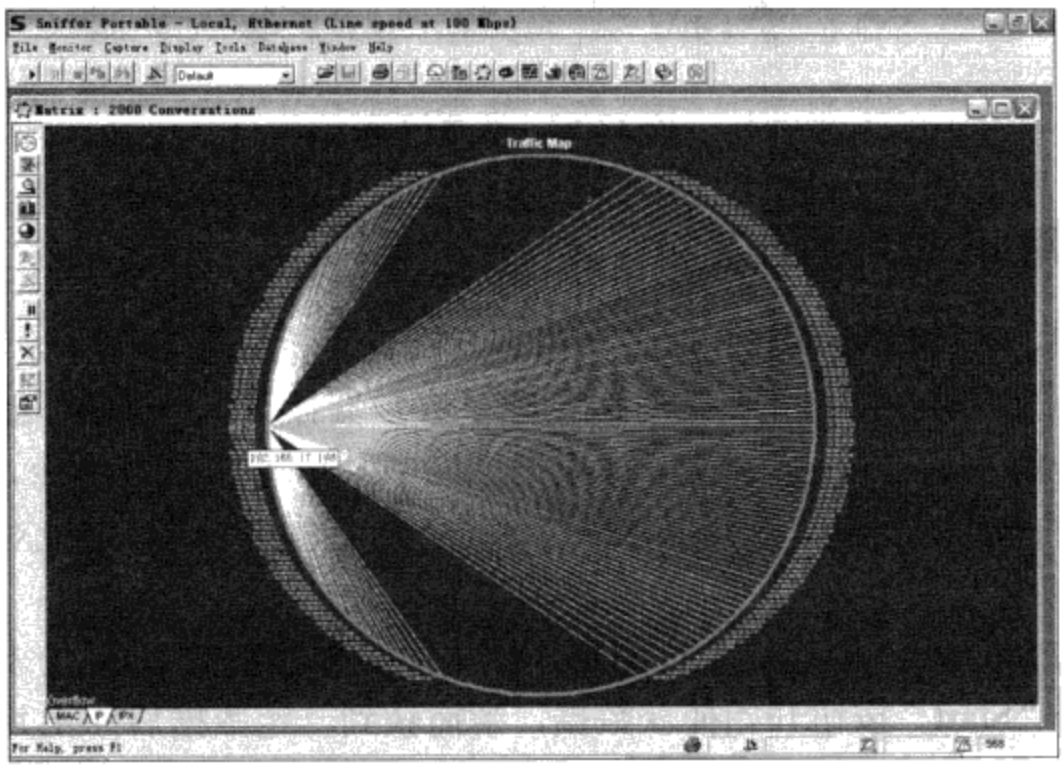


图12-85 大量的并发连接

于是，设置IP访问列表阻止TCP135端口，以及其他常见蠕虫端口，并将其应用于所有VLAN。IP访问列表的详细信息可以参考snort实例中的相关内容。

第 13 章　网络客户端安全

客户端安全往往是局域网安全管理工作的重点，其根本原因是普通用户网络安全意识较差，网络应用复杂多样，更重要的是一旦个别用户感染病毒或遭到其他威胁，无法及时阻断向其他客户端的蔓延，从而导致大面积的网络故障。实现客户端安全的关键在于网络管理方式的变革，如果管理员能够实现对客户端的统一部署和集中控制，就可以减少客户端安全漏洞的出现，降低网络安全事件的发生频率。

13.1　网络客户端安全规划

随着局域网规模的扩大，客户端数量将不断增加，由此引发的网络通信和安全问题也会越来越多，如果不能实施有效控制和管理，网络阻塞、蠕虫病毒泛滥、网络性能下降将是不可避免的。目前，客户端操作系统以 Windows 为主，还是比较容易实现统一部署和管理的。管理员可以从如下几个方面着手，规划和部署客户端安全管理。

1.　采用 Windows 域管理模式

按照微软官方的说法，网络中客户端数量超过 10 台，就需要采用 Windows 域管理模式，因此，“域”已经成为大多数管理员的制胜法宝。首先，采用“域”管理模式更容易实现集中管理，域中可以创建 OU，OU 中可以创建对象分组等，更重要的是管理员可以对不同的 OU 应用不同的管理策略，实现客户端快速部署。其次，采用域管理模式可以提升网络安全性，集中控制用户访问权限，必要时还可以将部分管理权限委派给不同用户账户，既可以减轻管理员负担，又可以增加网络安全性。有关 Windows 域的相关操作和应用请参考本书“第 3 章　网络用户账户安全”中的详细介绍。

2.　借助组策略实现自动化管理

随着网络内计算机数量的不断增加，软件安装、系统安全以及文件夹共享等基本操作都会成为系统管理员的“累赘”，系统维护和安全维护的工作量也会越来越大。组策略是系统管理员为计算机和用户所定义的，用来控制应用程序、系统设置和管理模板的一种机制。通过组策略管理可以完成网络环境中客户端的统一软件部署、安全设置、脚本设置、软件限制、客户端桌面环境部署以及浏览器功能统一设置等功能，同时根据策略的不同需求可以分为计算机配置策略和用户策略。

借助于组策略的应用，管理员可以通过域控制器，让系统自动而高效地完成许多重复、繁琐的系统管理与安全管理工作，提高网络管理工作的效率和网络的安全性，保持系统和网络的稳定运行。

3.　基于网络设备的访问控制措施

交换机特别是接入层交换机作为客户端连接网络的接口和网络传输的通道，在限制客户

访问时起着非常重要的作用。交换机中的访问限制可以概括为3个方面：

- 限制非授权用户访问网络，包括802.1x身份认证、安全端口、MAC地址绑定和禁用/启用端口；
- 限制用户滥用网络，包括时间访问限制、网络协议和端口访问限制、IP/MAC地址访问限制和连接带宽限制。
- 网络用户的隔离，包括VLAN访问限制、PVLAN访问限制和Trunk中继访问限制。

下面给出其中几种常用的访问限制方法。

提示 有关基于网络设备的客户端访问控制部署与应用，请参考本书“第9章 局域网传输控制”中的详细介绍。

4. 集中的客户端资产管理平台

选择一款得心应手的网络管理工具可以使管理员的工作事半功倍。在局域网客户端管理方面，由于客户端系统平台多为微软的Windows系统，可以采用微软推出的客户端管理工具，集中控制和管理客户端资源，如SCCM、SCOM等统一管理平台。借助统一管理平台可以及时获取客户端的硬件系统和软件系统资源清单，并能生成报表发送给管理员，帮助管理员制定相应的维护策略。

5. 统一安装系统更新

正确配置和安装系统更新可以有效避免由系统漏洞引发的网络攻击。以Windows系统为例，有些用户认为开启Windows Update功能是个累赘，其实这是完全错误的。Windows系统漏洞可谓屡见不鲜、层出不穷，令人欣慰的是微软官方可以在最短的时间内公布解决方案，发布相应的补丁程序，如果能够立即安装，即可弥补系统漏洞。在局域网管理中，管理员可以通过Windows Server 2008 R2系统集成的WSUS服务，实现客户端系统更新的集中管理。

13.2 组策略应用基础

应用组策略管理网络客户端之前，首先应做好准备工作，创建OU、组并将被管理对象添加到OU中。如果想要管理员之外的其他用户通过组策略管理网络，则还应先将管理权限委派给其对应的用户账户。

13.2.1 组策略概述

组策略设置定义了系统管理员需要管理的用户桌面环境的多种组件，例如，用户可运行的程序、用户的桌面环境、“开始”菜单选项、任务栏选项等。允许系统管理员为特定用户组创建特殊的桌面配置，允许使用的特定的管理单元。指定的组策略设置包含在组策略对象中，而组策略对象又与选定的Active Directory对象（即站点、域或组织单位）相关联。

1. 组策略的功能

基于活动目录的组策略不仅应用于用户和客户机，还应用于成员服务器、域控制器以及管理范围内的任何 Windows 2000 以上操作系统的计算机。默认情况下，应用于域（即，在域级别应用，在 Active Directory 用户和计算机管理单元的根目录之上）的组策略会影响域中的所有计算机和组织单位下的用户。Active Directory 用户和计算机管理单元还提供内置的域控制器组织单位。如果将在那里保存域控制器账户，则可以使用组策略对象“默认域控制器策略”将域控制器与其他计算机分开管理。

组策略内包含计算机配置与用户配置两部份，其中计算机配置只对计算机环境有影响，而用户配置只对使用者工作环境有影响。管理员可以通过如下两个途径配置和应用组策略：

- 本机计算机策略。可用来配置单一计算机上的组策略，用户所做的计算机配置只会应用到本地计算机，而用户配置会被应用到本地计算机上的所有用户账户。
- 域组策略。在域控制器上可以针对站点、域或 OU 来配置组策略，其中域组策略内的配置会被应用到域内的所有计算机与用户上，而 OU 的组策略会被应用到该 OU 内的所有计算机与用户。对加入域的计算机而言，如果其本机计算机策略的配置与域或 OU 的组策略配置冲突，则以域或 OU 组策略的配置优先，也就是此时本机计算机策略的配置无效。

2. 组策略的组件

组策略组件包括组策略对象组件、组策略模板组件、组策略容器组件、客户端扩展组件、组策略编辑器组件、计算机策略和用户策略组件、组策略和本地策略组件。

■ 组策略对象组件

在 AD 中，包括站点、域和 OU 在内的容器对象都可以连接到一个 GPO 中。通过连接，可以将 GPO 设置的应用于所指定容器中的用户和计算机。GPO 由两部分组成：

- 组策略模板组件（GPT，Group Policy Template）。组策略的 GPT 组件中包含了一系列的指令集。例如，对注册表进行更新的策略存储在一个名为 Registry.pol 的 GPT 文件中。标准 GPT 文件存储在每个域控制器的 Sysvol 文件夹中。
- 组策略容器组件（GPC，Group Policy Container）。GPC 是一个活动目录对象，包含一个与特定 GPO 关联的 GPT 名称。Windows 客户端使用一个 GPC 的信息来确定要下载和处理 GPT 信息。

■ 客户端扩展组件

客户端扩展组件称为 Client Side Extension（CSE）。在一个 Windows 客户端，有许多功能都是由组策略来管理的。这些功能具备相应的服务，他们知道如何获取和处理指向它们的组策略，这些服务器被称为“客户端扩展组件”，它们采取动态链接库的形式存在。

■ 组策略编辑器组件

组策略编辑器组件称为 Group Policy Editor（GPE）。GPE 是一个 MMC 管理单元，用于创建和管理 GPO。

■ **计算机策略和用户策略组件**

一个 GPO 的策略设置即可以用于计算机对象也可以用于用户对象。计算机在启动时下载所属的策略，用户在登录到域控制器时下载所属的策略。

■ **组策略和本地策略组件**

并不是所有的策略都是从域中下载的。每个客户端都有自己的本地策略。如果用户不是一个域成员，那么在启动时将使用本地的策略，而不使用域策略。

3. Windows Server 2008 R2 中组策略的新特性

在 Windows Server 2008 系统中对原有的系统策略进行了扩展，Windows server 2003 SP1 中提供了约 1700 条组策略设置，但是在 Windows Server 2008 系统中已增加至 2400 条组策略，管理功能更加丰富。在 Windows Server 2008 和 Windows Server 2008 R2 系统中，组策略管理控制台提供了更多元化的组策略管理方式，主要有以下新特点：

- 支持新的策略应用范围，包括无线和有线网络，Windows 防火墙和 IPSec 策略，支持电源管理和 USB 设备限制策略。
- 客户和域控制器之间慢速链接检测已经有所改进，现在可以有一个更稳定的机制，来判定客户是否通过慢速链接到域控制器，从而决定所应用的组策略行为。
- 组策略更新现在是基于域控制器的可用性，也就是说，当客户远程通过 VPN 链接到网络的时候，组策略更新会更加及时。
- 支持多个本地策略对象（LGPO）以及针对不同的用户组或用户设置不同的组策略对象。
- 支持基于 XML 的管理模板文件格式化（ADMX），更好的支持多语言模板。
- 支持 per-GPO 和 per-GP 的设置。
- GPMC 和组策略编辑器都有了改进，并且增加了新功能。
- 增加了通过收购 Desktop Standard 所获得的工具，也就是现在被称为 Group Policy Preferences 的工具，用它来实现组策略的自动创建。
- 组策略的 Windows PowerShell Cmdlet。Windows PowerShell 是一种 Windows 命令行界面和脚本语言，可用于自动化许多相同的任务（使用组策略管理控制台在用户界面中执行这些任务）。Windows Server 2008 R2 中的组策略提供了 25 个 cmdlet。每个 cmdlet 都是一个简单的单一功能命令行工具。通过组策略的 Windows PowerShell Cmdlet 可以完成如下任务：
  - □ 维护 GPO。创建、删除、备份和导入 GPO。
  - □ 将 GPO 与 Active Directory 容器相关联。创建、更新和删除组策略链接。
  - □ 在 OU 和域中设置继承标志和权限。
  - □ 配置基于注册表的策略设置和组策略首选项注册表设置。更新、检索和删除。
  - □ 创建和编辑 Starter GPO。

13.2.2 将管理对象添加到域

组策略管理的对象主要包括用户和计算机，部署组策略之前，首先应将其添加到域，并

移动到指定的 OU，如图 13-1 所示是添加到“网管区”的所有用户账户，具体操作可以参考本套教材的其他章节，此处不复赘述。Windows 2000 Professional、Windows XP Professional、Windows 2000 Server、Windows Server 2003 、Windows Vista、Windows 7 或 Windows Server 2008 或等客户端均可被添加到 Active Directory 域中。需要注意的是，添加计算机之前必须在客户端上以本地管理员身份登录，然后将客户端的 DNS 地址设置为域控制器的 IP 地址。

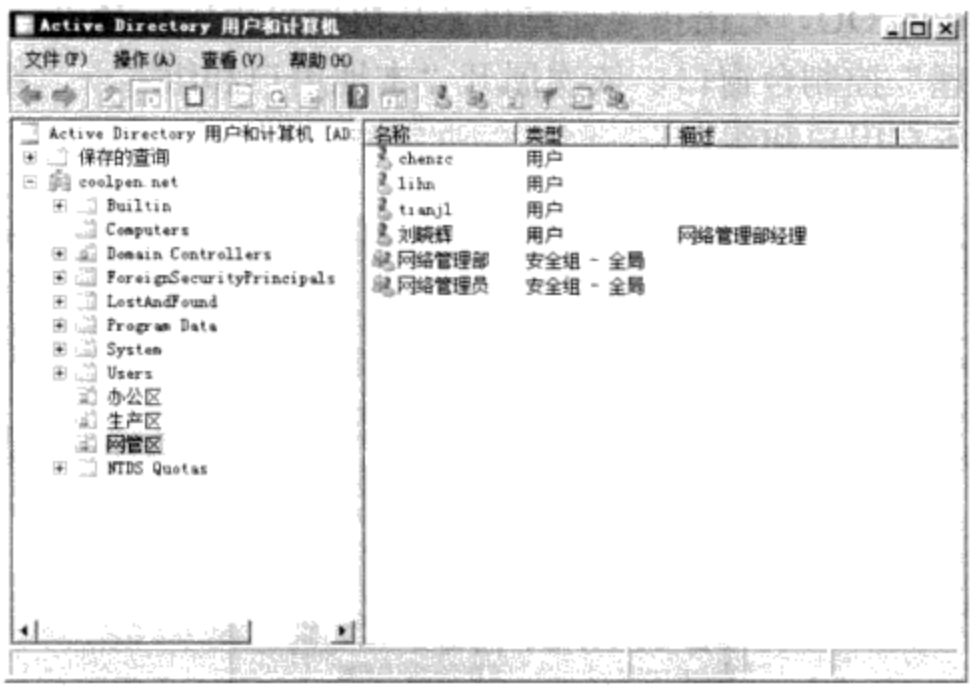


图 13-1 将用户和计算机移动到 OU

13.2.3 将用户添加到本地管理员组

已加入域的计算机登录系统时，可以根据自己的需要选择登录到“域”，还是登录到“本机”。两者的区别在于：

- 当登录到“本机”时，就是一台连接到网络的“单机”，这种方式不能使用网络中提供的服务。当然，此时使用分配给用户的域用户名及密码，还是可以使用网络中的“文件和打印”共享服务的。
- 只有登录到“域”的用户，才能使用 Active Directory 及其提供的各项服务，例如使用组策略部署软件、使用 Exchange 提供的邮箱等。

建议选择“登录到域”，否则组策略将不会起作用。为了让组策略生效，必须使用域用户登录到每台计算机。

通常情况下，普通域用户账户（域的管理员用户除外），不能在登录计算机上安装软件，可能会给个别用户带来不便。其实这个问题很容易解决，只要将计算机使用者的“域用户名”添加到当前计算机的“本地管理员组”即可。将普通的域用户添加到“本地管理员”组，有 3 种方法：

- 使用域管理员账户登录到工作站，然后进入“计算机管理”→“本地用户和组”中进行添加。
- 由管理员在“Active Directory 用户和计算机”窗口，从 Computer 组中选择用户的计算机并右击，从快捷菜单中选择“管理”选项，打开工作站的“计算机管理”对话框，然后从“用户”中添加。
- 由“本地计算机”管理员自己登录到计算机添加。

前两种方法，都需要有“域”管理员权限。如果工作站的使用者对计算机操作不熟悉，可以由管理员“代劳”。如果网络中有大量的计算机，为了减轻管理员负担，应该让每个用户都掌握这项“技术”。其中前两种方法非常类似，这里只介绍以管理员身份登录到域控制器的操作方法。

第1步，在服务器上，以管理员身份登录，打开“Active Directory 用户和计算机”窗口，展开客户端计算机所在的 OU，右击指定计算机名从快捷菜单中选择“管理”选项，显示如图 13-2 所示“计算机管理”控制台窗口。依次展开“本地用户和组”→“组”，在右侧窗口中即可查看本地计算机的所有用户和组。

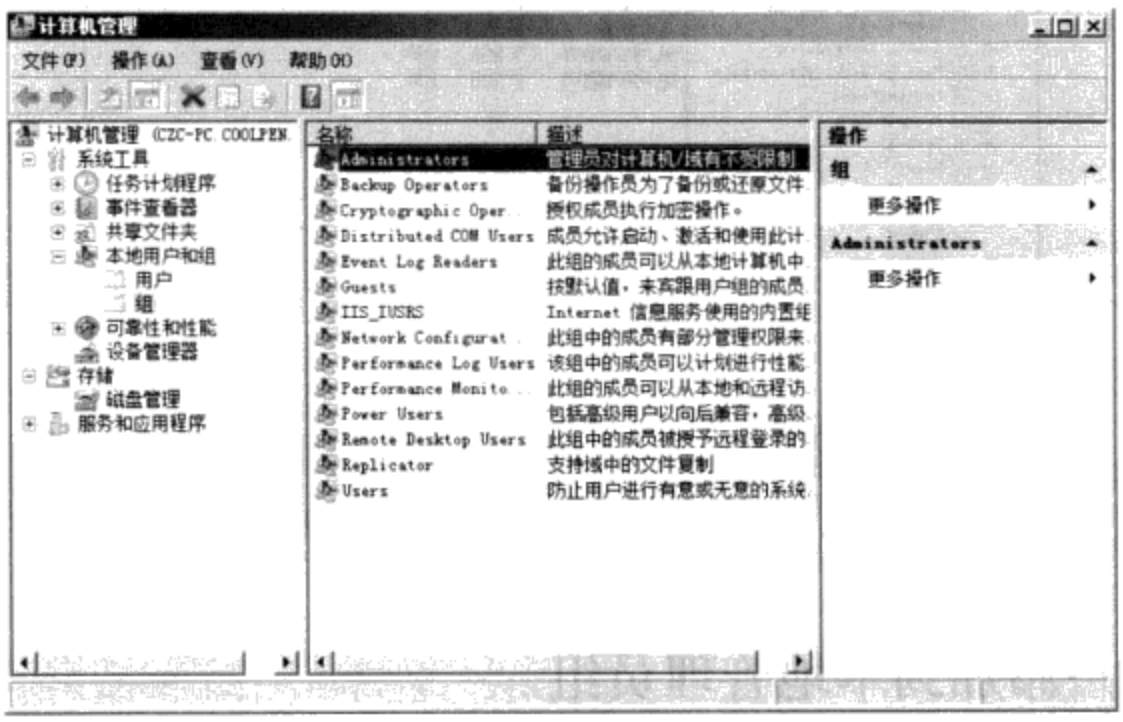


图 13-2 “计算机管理”窗口

提示 如果客户端计算机启用了防火墙，则可能导致无法正常连接，建议先关闭所有防火墙。

第2步，右击 Administrators，从快捷菜单中选择“属性”选项，显示如图 13-3 所示的组属性对话框，已经成功添加的用户账户将显示在成员列表框中。

第3步，单击“添加”按钮，显示如图 13-4 所示“选择用户、计算机或组”对话框。在“输入对象名称来选择”文本框中键入登录域控制器的用户账户，如果不清楚用户账户全称，也可以查找添加。

第 4 步，单击“高级”按钮，进入“高级查找”功能，单击“立即查找”按钮，将查找当前域中的所有用户、用户组和计算机，如图 13-5 所示。

第 5 步，从查找到的列表框中，选择与管理的计算机相对应的使用者的用户名（可以选择一个、多个或者选择一组用户）。连接单击“确定”按钮，保存设置即可。

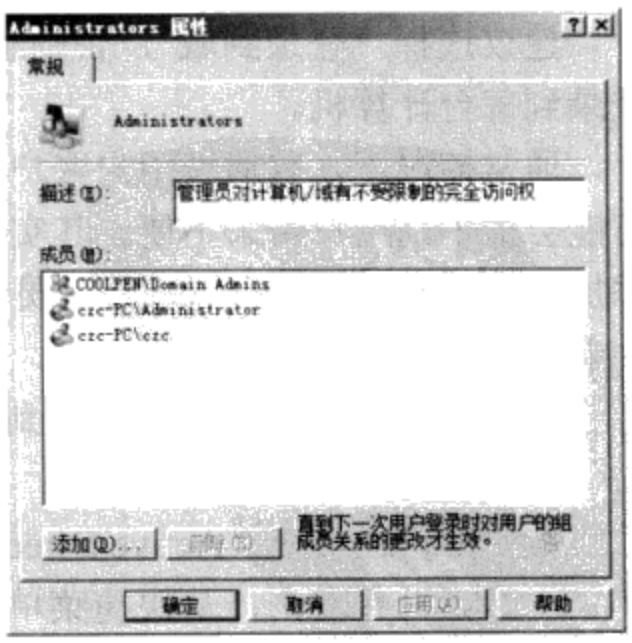


图 13-3 组属性

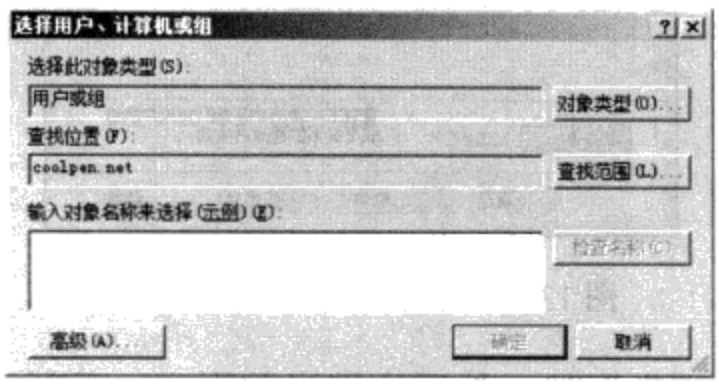


图 13-4 “选择用户、计算机或组”对话框

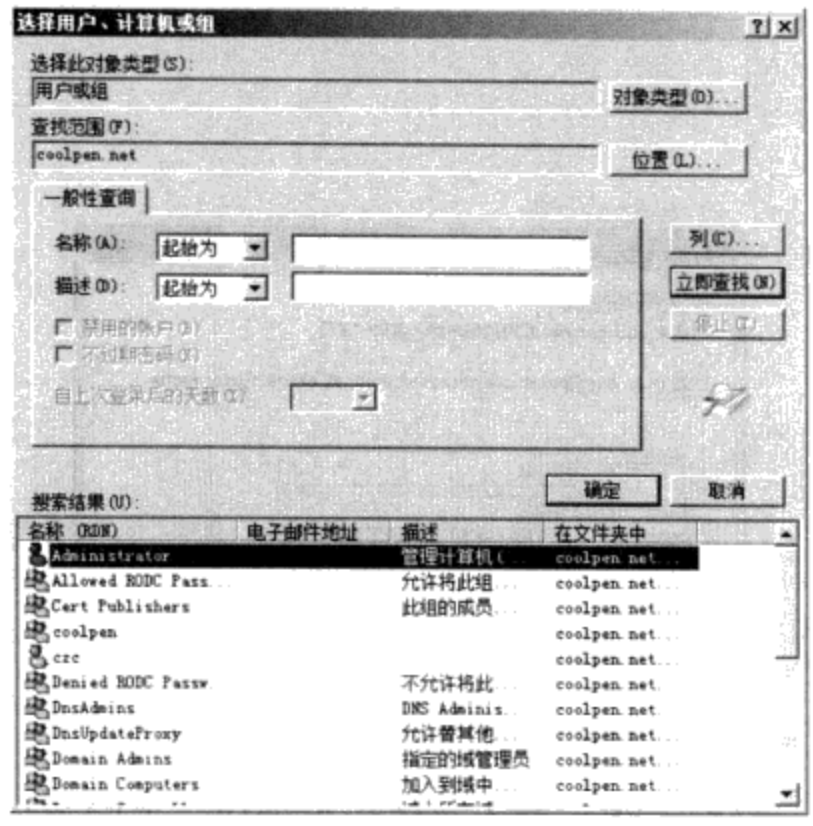


图 13-5 选择用户

接下来介绍第 3 种方法的实现过程。

第 1 步，当计算机添加到 Active Directory 并重新启动，在登录 Windows 时，使用本地管理员账户登录到本机。

第 2 步，在“计算机管理”窗口中展开“本地用户和组”，双击主窗口中的 Administrators 组，打开“Administrators 属性”对话框。

第 3 步，单击“添加”按钮，显示“选择用户、计算机或组”对话框，在“输入对象名称来选择”文本框中，输入使用这台计算机的用户名，如图 13-6 所示。

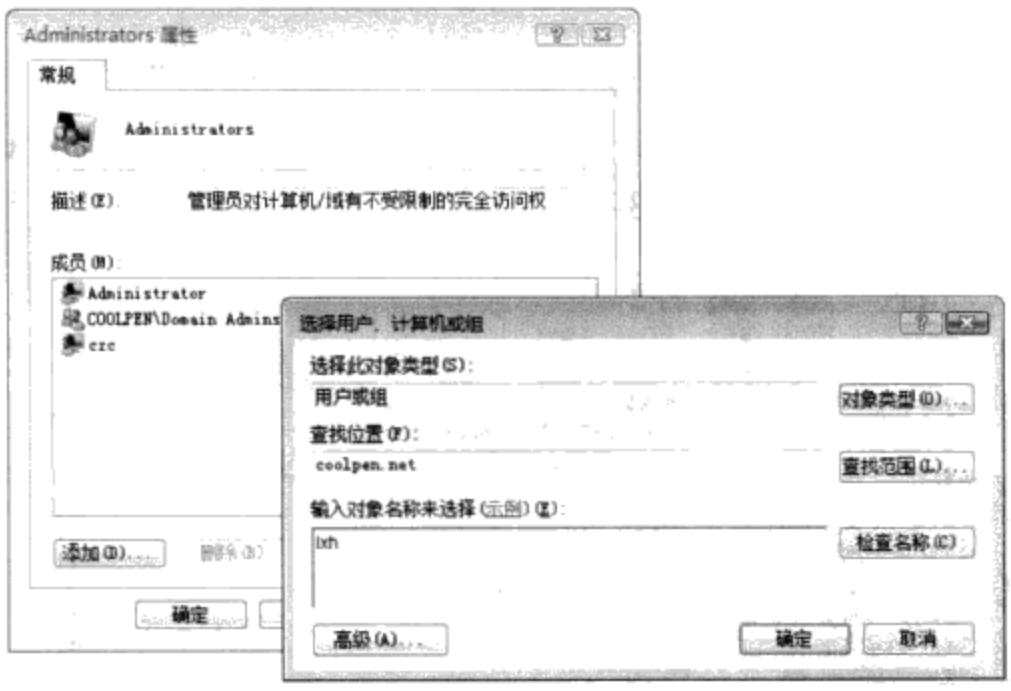


图 13-6 将用户添加到管理员组

第 4 步，单击“确定”按钮，显示如图 13-7 所示“输入网络密码”对话框，输入将计算机加入到域的用户名及密码。

第 5 步，单击“确定”按钮，该用户即被添加到管理员组，如图 13-8 所示。继续单击“确定”按钮返回“计算机管理”窗口，然后注销当前用户，重新登录到域控制器即可。

图 13-7 “输入网络密码”对话框

图 13-8 将用户添加到管理员组

第 6 步，单击“确定”按钮，返回“计算机管理”窗口，然后注销当前用户，重新登录到域控制器即可。

13.2.4 创建组策略

用户可以在组织单位或站点上创建组策略，默认情况下，其子对象也将继承父对象的策略配置。所以，通常将公共的任务设置在最上级的组织单位上，将专用的任务设置在具体应用的组织单位上，避免不同策略之间的冲突。在 Windows Server 2008 系统中，使用“组策略管理”控制台部署策略，在“Active Directory 用户和计算机”的组织单位属性中，则不支持组策略管理。

第 1 步，依次选择“开始”→“管理工具”→“组策略管理”选项，显示“组策略管理”窗口。依次展开“组策略管理”→“林：coolpen.net”→“域”→“coolpen.net”→“网管区”（需要应用组策略的 OU）选项，如图 13-9 所示。

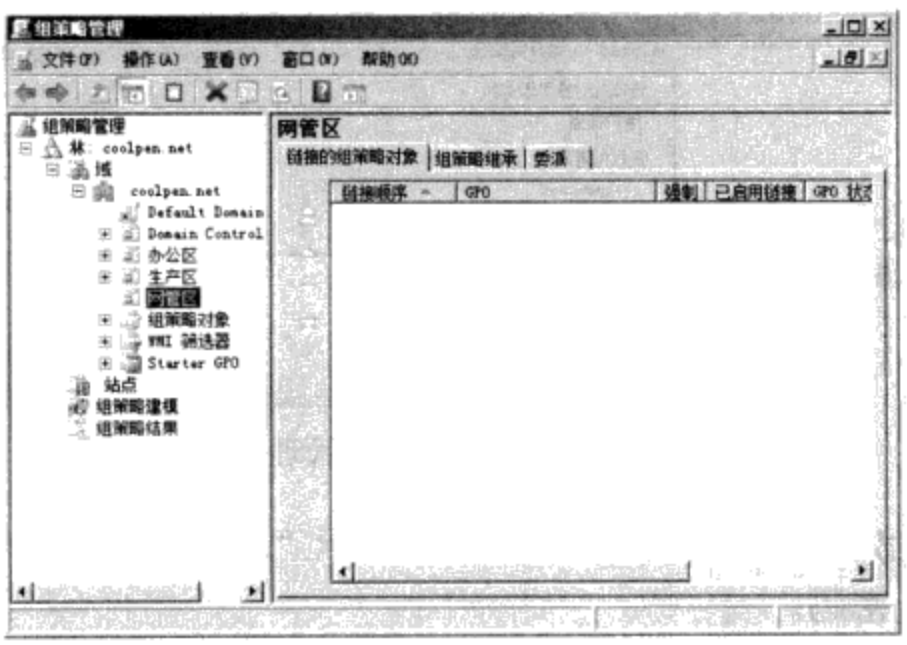


图 13-9 “组策略管理”窗口

第 2 步，右击“网管区”并选择快捷菜单中的“在这个域中创建 GPO 并在此处连接”选

项，显示如图 13-10 所示“新建 GPO”对话框，在“名称”文本框中，键入新建的创建名称，例如“测试”。

第 3 步，单击“确定”按钮，关闭“新建 GPO”对话框，返回到“组策略管理”窗口，如图 13-11 所示。

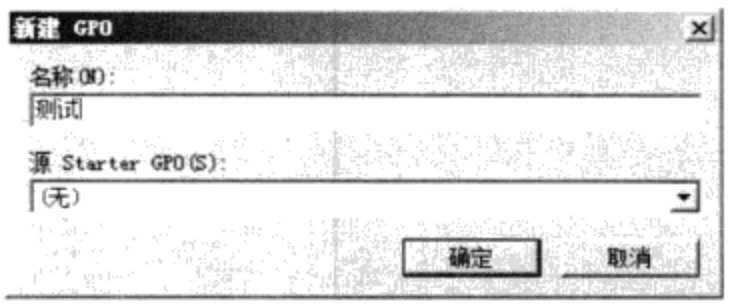


图 13-10 “新建 GPO”对话框

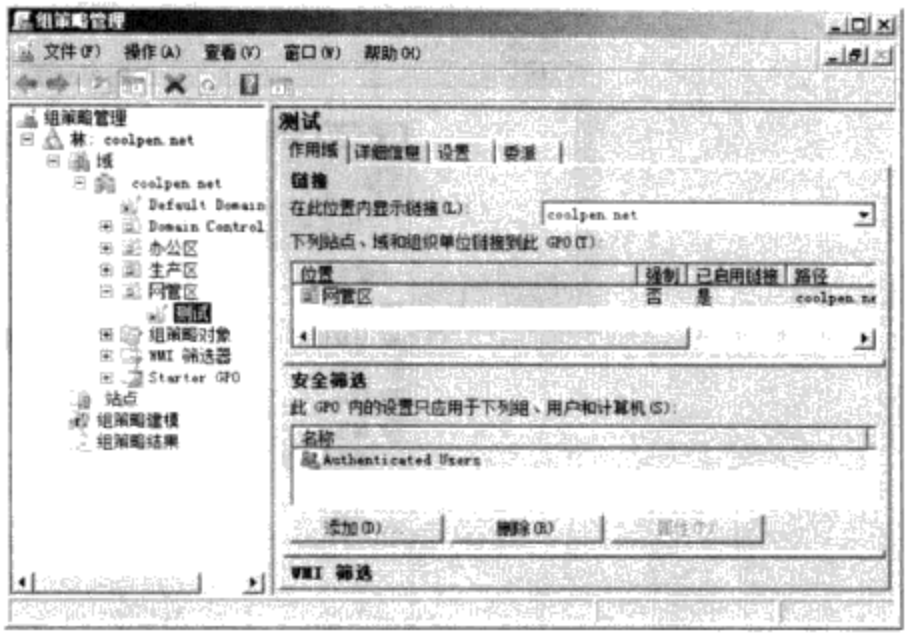


图 13-11 “组策略管理”窗口

13.2.5 编辑组策略

默认情况下，新创建的策略并没有进行任何配置，为了达到某些功能或安全要求，必须对组策略进行编辑。这里以编辑新建的策略为例进行介绍。

在“组策略管理”窗口中，右击“测试”策略，在快捷菜单中选择“编辑”选项，显示如图 13-12 所示“组策略管理编辑器”窗口。在该窗口中，根据需要对组策略进行编辑即可。

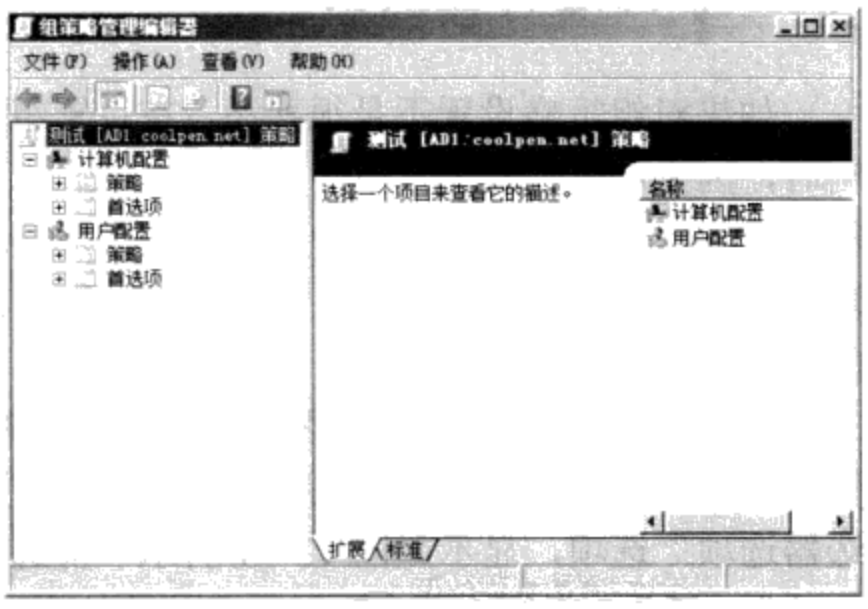


图 13-12 “组策略编辑管理器”窗口

在每个组策略配置窗口中，均有“计算机配置”和“用户配置”两项，其中“计算机配置”主要应用于所编辑组策略的 OU 中的计算机，而“用户配置”应用于 OU 中的所有用户。通常，新创建的组织单位中默认是不包含计算机的，只包含用户。只有域的组策略中才包含计算机。

13.2.6 添加管理模板

每次评估 GPO 时，也会评估 GPO 内的所有设置，以确定如何影响用户或计算机。评估的设置越多，计算机启动或用户接收到登录对话的时间也就越长。因此，默认情况下，并没有将所有可用的管理模板全部添加在组策略结构中。换句话说，在实际使用中，只需要添加所必

需的管理模板即可。

在“组策略管理编辑器”窗口中，右击“管理样板”，在快捷菜单中选择“添加/删除模板”选项。显示如图 13-13 所示“添加/删除模板”对话框，单击“添加”按钮，浏览并选择所要添加的模板即可。

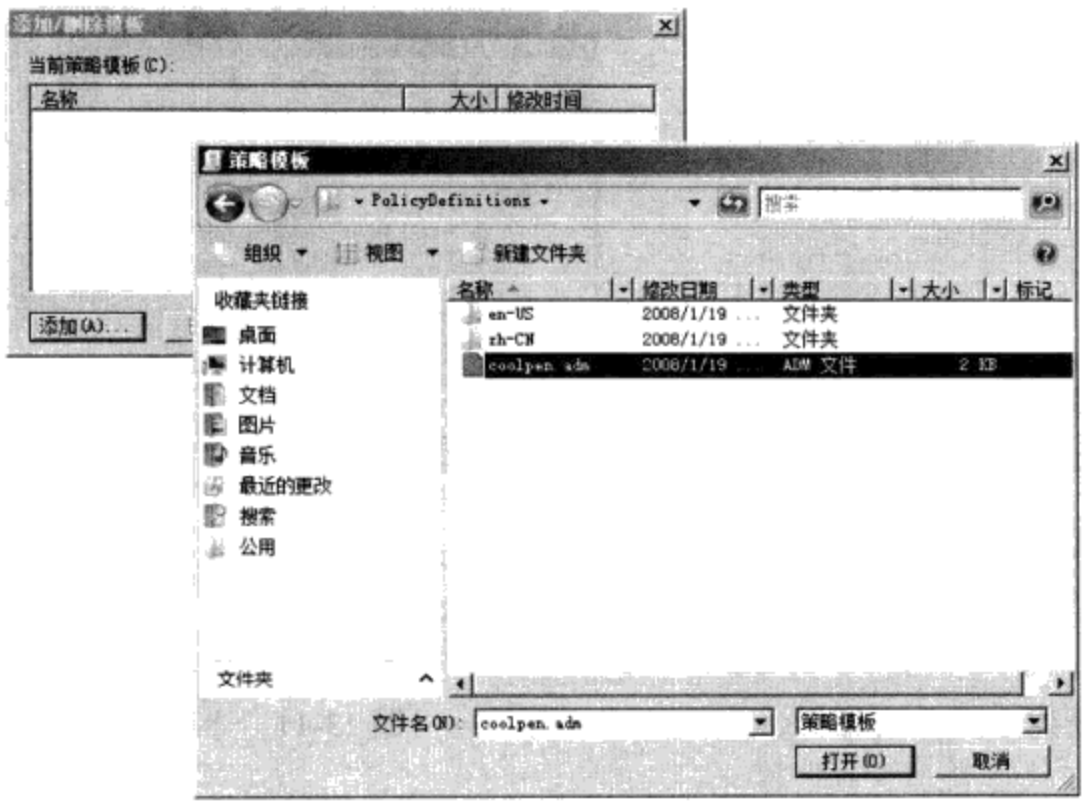


图 13-13 添加模板

13.2.7 筛选管理模板

如果对组策略设置不是很熟悉，在设置组策略时，因为可配置的设置很多，所以查找起来可能会比较困难。为了解决这个问题，在组策略管理器中，可以使用筛选功能，筛选掉所有不匹配的选项。

第 1 步，右击“计算机配置”或“用户配置”管理模板下的任一容器，在快捷菜单中选择“筛选器选项”选项，显示如图 13-14 所示“筛选器选项”对话框。根据需要，设置所要筛选的类别。例如选中“启用需求筛选器”复选框，并在列表框中选中“Windows Server 2008 家族”和“Windows Vista 家族”复选框。

第 2 步，单击“确定”按钮，保存筛选配置。

第 3 步，再次右击模板节点，在快捷菜单中选择“打开筛选器”选项，即可启动筛选器，如图 13-15 所示为筛选后结果。此时，根据需要设置策略模板即可。

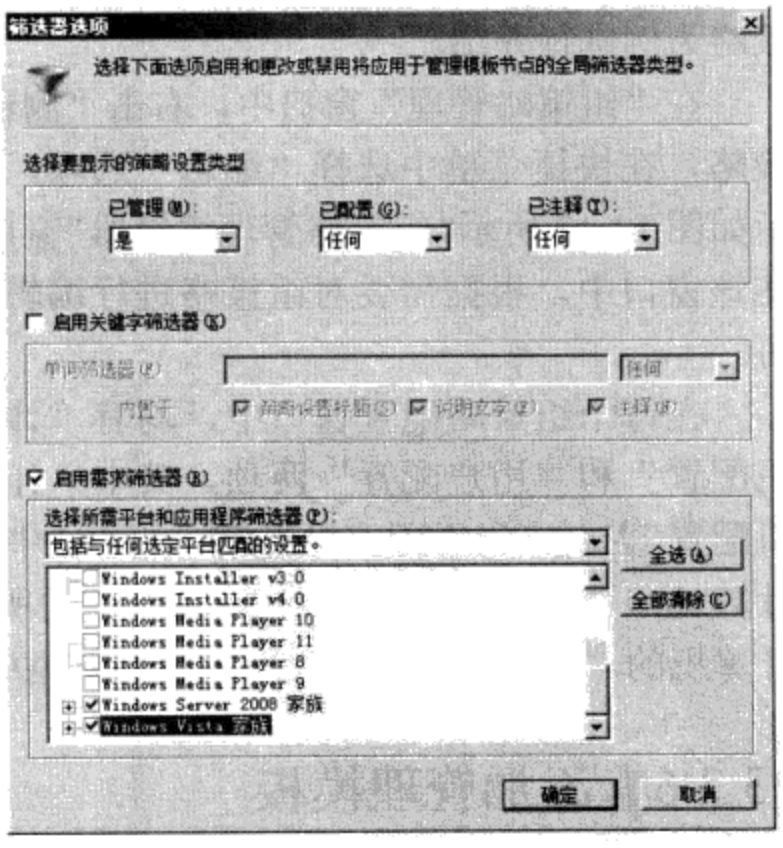


图 13-14 “筛选器选项”对话框

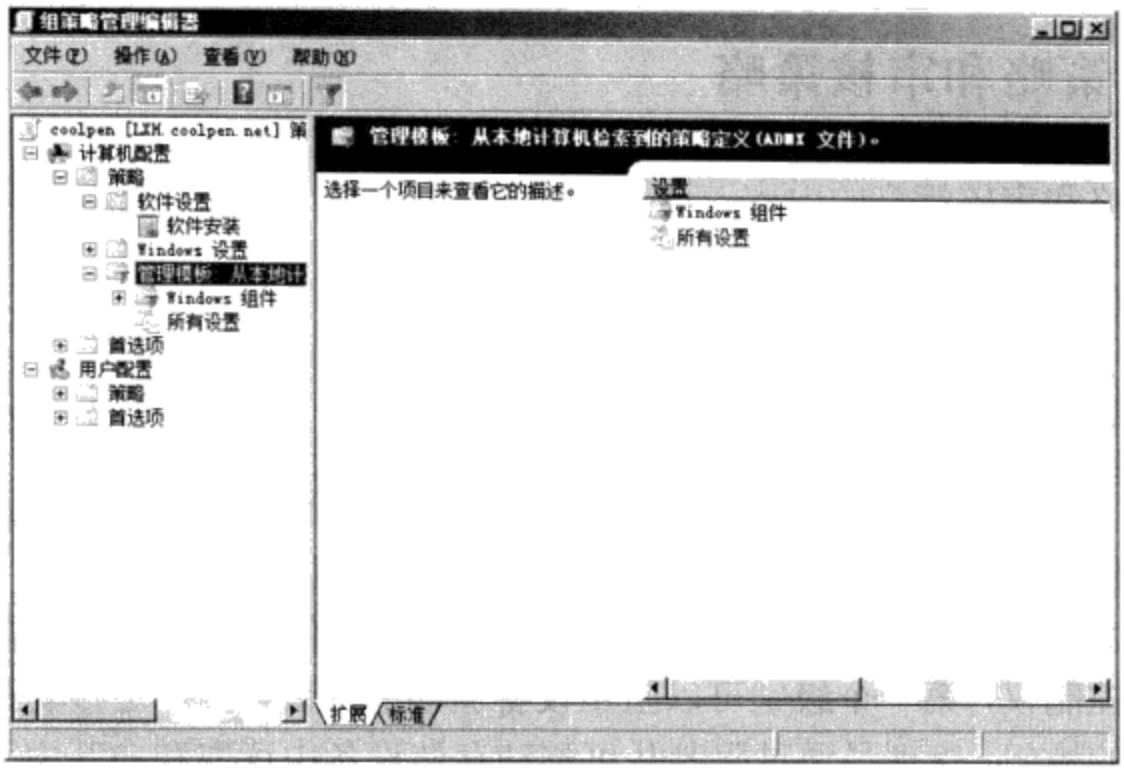


图 13-15　筛选后管理模板

筛选器的缺点是只能应用在管理模板上，组策略其他区域的设置不会受到影响，也不会被筛选掉。但是，这些设置被更新和修改的频率不如管理模板。

13.3　安 全 策 略

所有安全策略都是基于“计算机配置”的策略，本地计算机上的用户账户或登录计算机的域用户账户无关。Windows Server 2008 R2 系统的安全机制更加完善，但默认情况下并未配置，因此起不到任何保护作用，必须根据需要启用并配置这些安全策略，以确保系统安全。打开“本地组策略编辑器”窗口，并依次展开“本地计算机 策略”→“计算机配置”→“Windows 设置”→“安全设置”选项，即可开始配置相应策略，如图 13-16 所示。

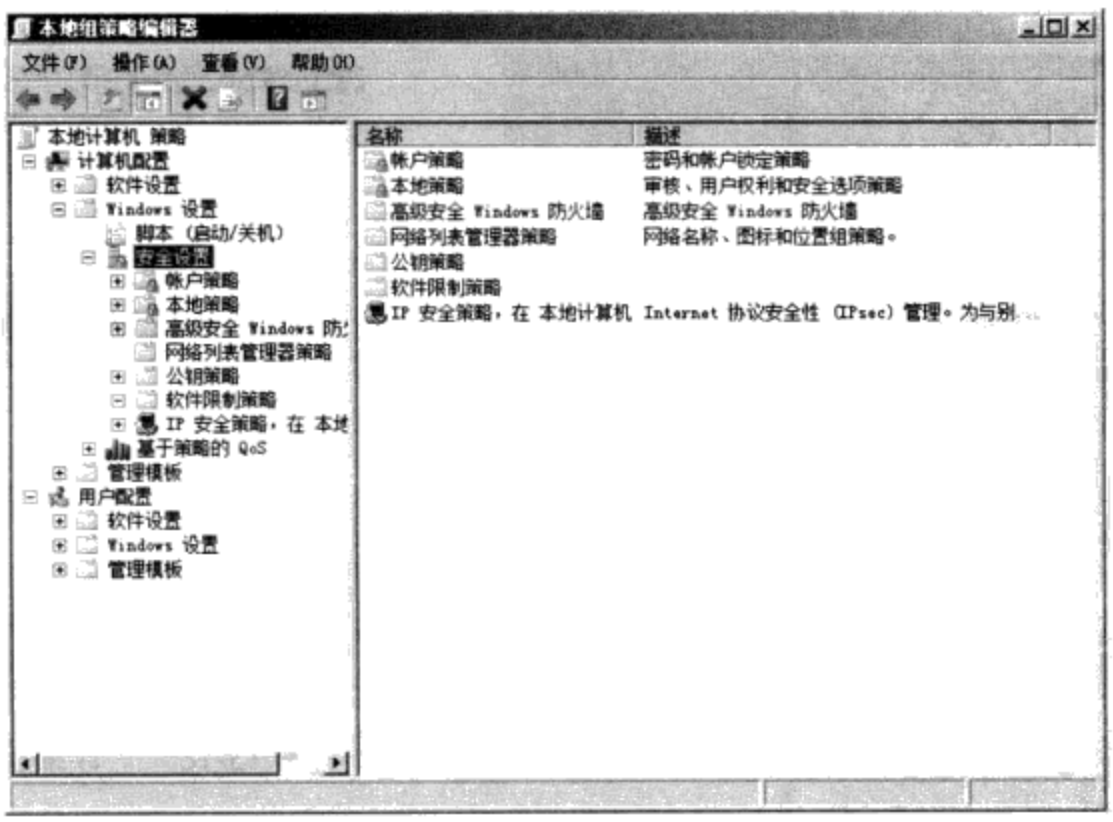


图 13-16　“本地组策略编辑器”窗口

13.3.1 账户策略和审核策略

有关账户策略和审核策略的内容，请参考本书“第3章 网络用户账户安全”中的相关介绍。

13.3.2 设备限制安全策略

通过在所有客户端计算机上部署硬件设备安装限制安全策略，可以阻止用户随便在计算机上安装任何硬件设备，导致不必要的系统安全问题。例如，通过限制使用U盘等可移动存储设备，不仅可以阻止部分病毒的传播，还可以避免重要的信息失窃。组策略中的管理模板策略有两个级别的控制权，第一个级别可以阻止设备驱动的安装，特别是移动存储设备。第二个级别控制对资源的访问。管理员通过限制从可移动存储设备中读取和向其中写入的数据，就可以保护内部数据安全。

提示 此处以硬件设备的GUID为例，禁止安装指定的硬件设备。

第1步，将任意U盘插入计算机的USB接口，打开“计算机管理”→“设备管理器”窗口，展开“磁盘驱动器”选项，显示如图13-17所示窗口。

第2步，右击U盘对应的设备名称，在弹出的快捷菜单中选择“属性”选项，在打开的对话框中切换至如图13-18所示“详细信息”选项卡。在“属性”下拉列表框中选择“设备类GUID”选项，在“值”列表框中，显示的就是U盘类设备对应的GUID，将此值复制到粘贴板即可。

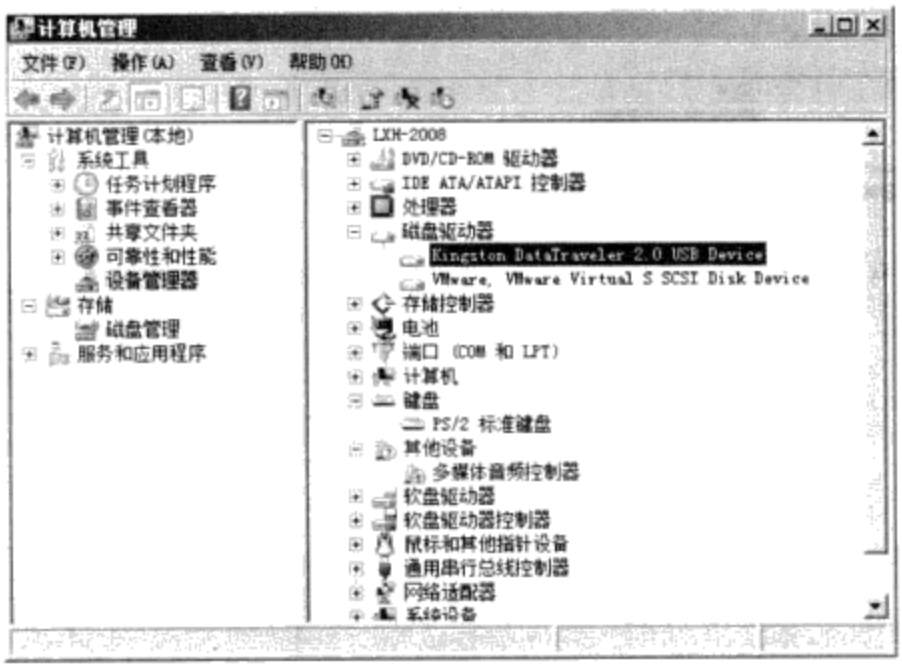


图13-17 “计算机管理”窗口

图13-18 “详细信息”选项卡

第3步，单击“确定”按钮，关闭对话框。

第4步，在“组策略管理编辑器”窗口中，依次展开“计算机配置”→“管理模板”→

“系统”→“设备安装”→“设备安装限制”，显示如图 13-19 所示窗口。

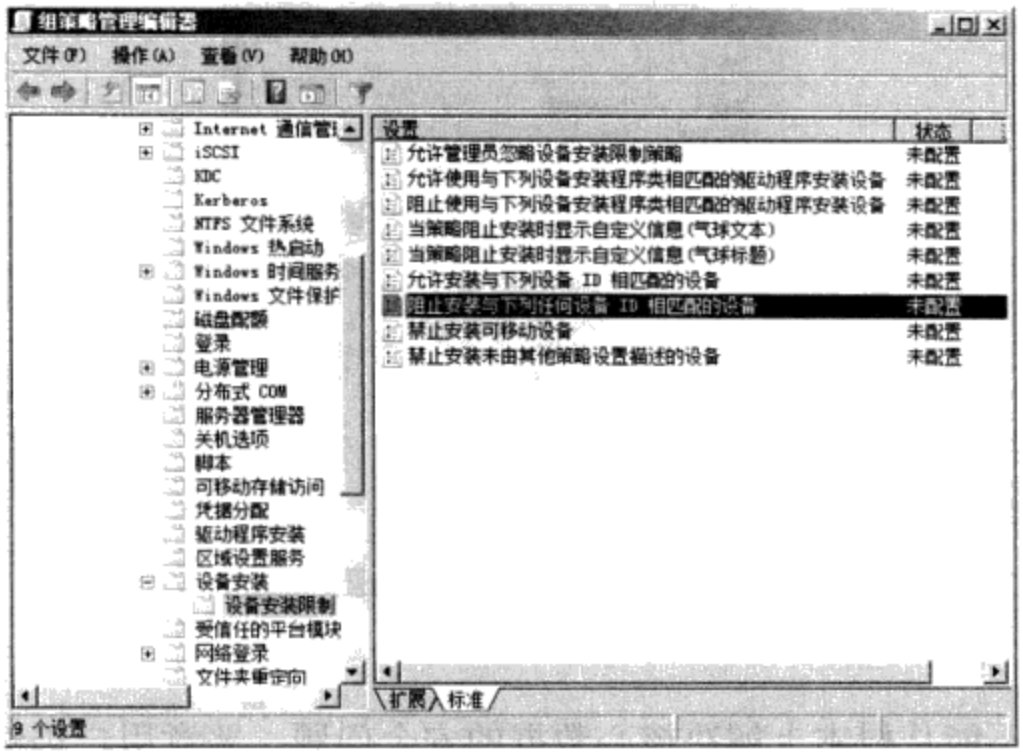


图 13-19 “组策略管理编辑器”窗口

第 5 步，双击“阻止安装与下列任何设备 ID 相匹配的设备”策略，显示如图 13-20 所示对话框，选择“已启用”单选按钮。

第 6 步，单击“显示”按钮，显示“显示内容”对话框，默认此列表框为空白。单击“添加”按钮，显示“添加项目”对话框，将复制到粘贴板的 U 盘类设备 GUID，粘贴到“输入要添加的项目”文本框中即可，如图 13-21 所示。

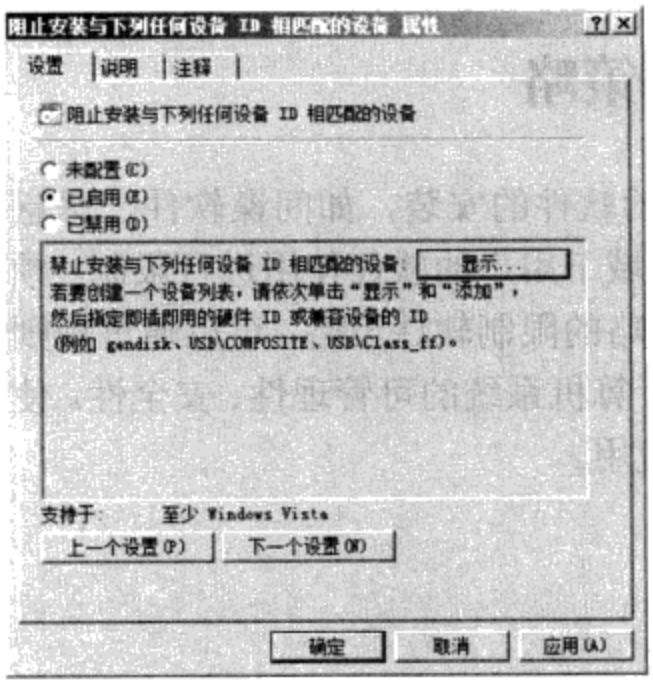


图 13-20 “阻止安装与下列任何设备 ID 相匹配的设备 属性”对话框

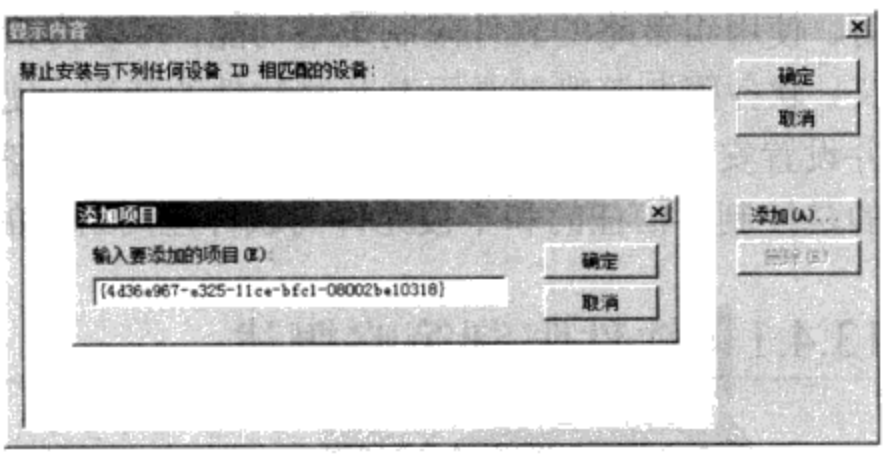


图 13-21 “添加项目”对话框

第 7 步，连续单击“确定”按钮，保存设置即可。由于以上策略只是阻止使用 U 盘类设备，所以应用此策略后，用户仍可以将 U 盘插入 USB 接口，并且系统会自动为其安装驱动程序，但是在资源管理器中打开时，会发现 U 盘对应的可用磁盘空间为 0，不会显示任何数据，如图 13-22 所示。

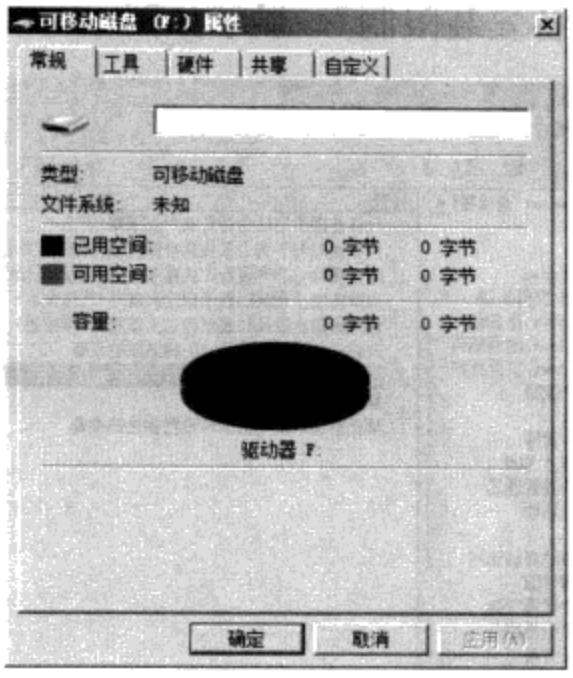


图 13-22 U 盘当前不可用

这些措施，并不能从根本上解决核心数据的安全问题。恶意用户仍然可以通过电子邮件发送数据，并且，如果管理员的话，具备工作站或服务器的物理操作权限，则盗取数据更是易如反掌。所以说，最完美的解决方案是，确保核心数据的访问权限，而不是仅仅依靠组策略。

注意 如果在应用设备限制策略之前，用户已经将移动设备安装到系统中，则不能阻止用户的正常应用，该策略会在用户取下设备并再次安装移动设备时生效。

13.4 软件限制策略

软件限制策略的主要功能在于控制未知或不信任的软件的安装，如间谍软件、恶意程序等。使用组策略的软件限制策略功能，可以为策略作用域下用户的软件使用进行限制。顾名思义，软件限制策略就是限制某些软件的使用。使用组策略的限制软件策略，可以通过规则标识并设置安全级别来指定软件是否运行从而达到客户端计算机系统的可管理性、安全性。使用目的是控制不信任的和不被允许的软件在网络内的非法使用。

13.4.1 软件限制策略概述

使用软件限制策略，可通过标识并指定允许运行的软件来保护计算机环境免受不信任软件的侵袭。可以为组策略对象定义“不受限的”或“不允许的”的默认安全级别，从而决定是否在默认情况下允许软件运行。通过为特定软件创建软件限制策略规则，可以相对于默认安全级别做出例外安排。软件限制策略使用规则来标识和控制软件的运行方式。可以通过软件程序的哈希、证书、路径或其所驻留的 Internet 区域对其进行标识。对软件进行了标识后，可以决定是否允许运行。

软件限制策略可应用于计算机或用户，这取决于是修改了“计算机配置”中的设置还是“用户配置”中的设置。软件限制策略是通过组策略得以应用的。需要将策略设置应用于组策略对象，该对象与本地计算机、站点、域或组织单位相连。如果应用了多个策略设置，将遵循

以下的优先级顺序（从低到高）：

- 本地计算机策略。
- 站点策略。
- 域策略。
- 组织单位策略。

所有策略设置在重新启动计算机后都会被刷新。修改策略设置时，在工作站或服务器上将每 90 分钟刷新一次，而在域控制器上将每 5 分钟刷新一次。不管是否更改了策略设置，它们都会每 16 小时刷新一次。通过先运行强制刷新组策略命令 gpupdate /force，然后注销计算机并重新登录来刷新策略设置。

软件限制策略中的规则标识一个或多个应用程序，以指定是否允许其运行。

软件限制策略使用下列 4 个规则来标识软件：

- 哈希规则：使用可执行文件的加密密钥。
- 证书规则：用软件发布者为 .exe 文件提供的数字签名证书。
- 路径规则：使用 .exe 文件位置的本地路径、通用命名约定（UNC）路径或注册表路径。
- 区域规则：使用可执行文件源自的 Internet 区域。

使用软件限制策略可以实现以下目的：

- 控制软件在系统中的运行能力。
- 允许用户在多用户计算机上仅运行特定文件。
- 决定可以在计算机中添加信任的发布者的用户。
- 控制软件限制策略是作用于所有用户，还是仅作用于计算机上的某些用户。
- 阻止任何文件在本地计算机、组织单位、站点或域中运行。

13.4.2 安全级别设置

使用软件限制策略可以标识并指定允许运行的软件，以便保护计算机环境不会受到不可信代码的攻击。使用软件限制策略时，可以为组策略对象（GPO）定义系统默认的安全级别的一种，不受限的、不允许的或基本用户，使得在默认情况下或者允许软件运行，或者不允许软件运行，或者以用户账户身份而定。

1. 创建软件限制策略

Windows Server 2003/2008 默认情况下，并没有配置软件限制策略，在“本地组策略编辑器”窗口中，依次展开“计算机配置”→“Windows 设置”→“安全设置”→“软件限制策略”，显示如图 13-23 所示窗口。如果是在 Windows 域控制器上编辑作用于站点或组织单位的组策略，则在“用户配置”→“策略”→“Windows 设置”→“安全设置”→“软件限制策略”分支中同样可以创建软件限制策略（以 Windows Server 2008 域控制器为例）。

右击“软件限制策略”并选择快捷菜单中的“创建软件限制策略”选项，系统将自动完成策略类型的构建，右侧窗口中即可显示可以配置的策略项目，如图 13-24 所示。

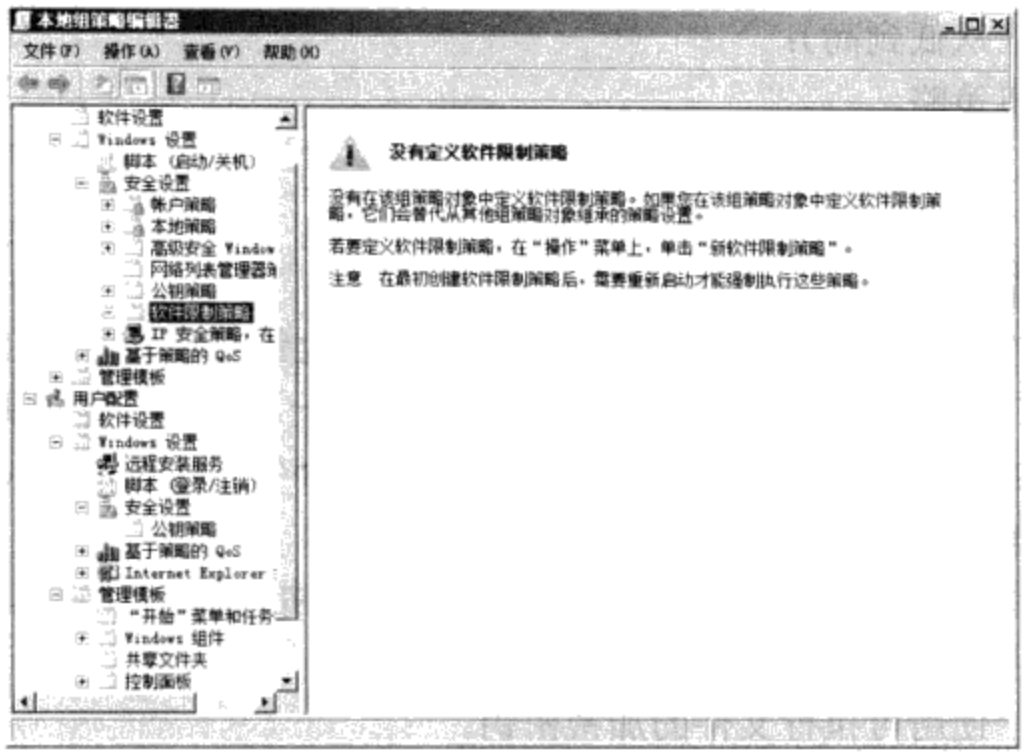


图 13-23 软件限制策略

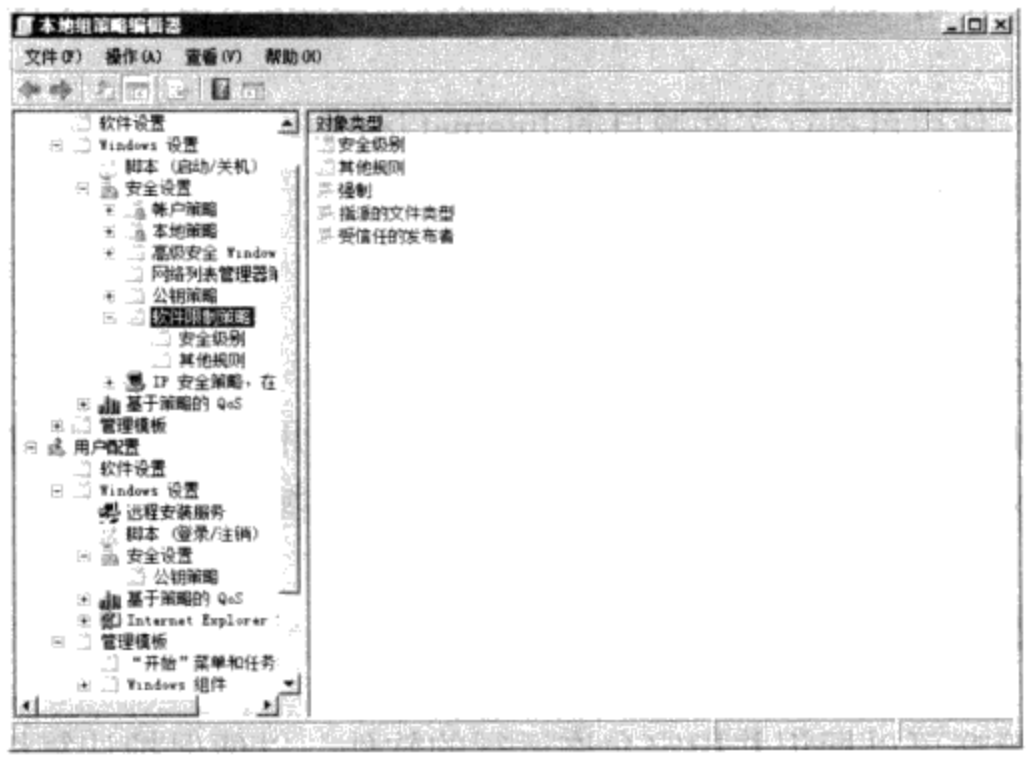


图 13-24 创建软件限制策略

2. 设置安全级别

安全级别指的是操作系统对应用策略所具备的访问级别，创建软件限制策略后，继续展开“安全级别”，显示如图 13-25 所示窗口。默认情况下，Windows Server 2008 系统中包括如下 3 种安全级别。

- 不允许的：无论用户的访问权如何，软件都不会运行。
- 基本用户：允许程序访问一般用户可以访问的资源，但没有管理员的访问权。
- 不受限的：软件访问权由用户的访问权来决定。

其中，“基本用户”是 Windows Server 2008 系统新增的安全级别。Windows Server 2003/2008 的默认设置均为“不受限的”，即软件访问权限由用户账户自身的权限决定。

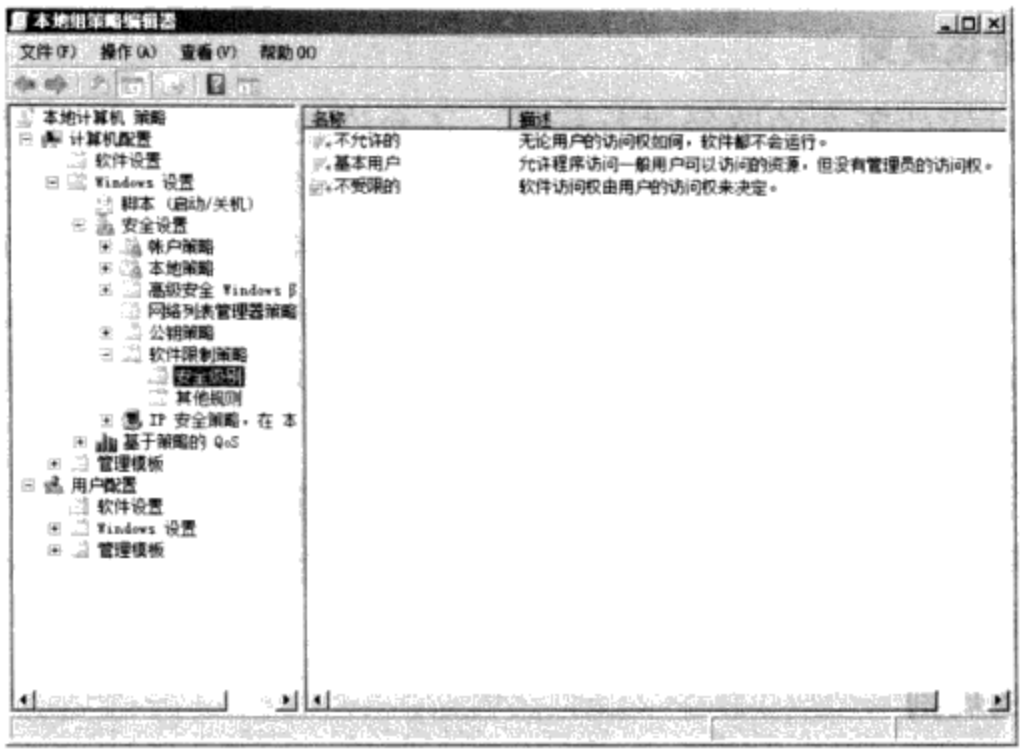


图 13-25　设置安全级别

Windows 系统的默认安全级别为“不受限的”，管理员可根据需要修改其他默认安全级别，主要操作步骤如下。

第 1 步，双击“不允许的”显示如图 13-26 所示“不允许的 属性”对话框，当前状态为：不是默认级别。

第 2 步，单击“设为默认”按钮，显示如图 13-27 所示“软件限制策略”对话框，提示所选择的默认等级比当前默认等级还要严格，更改后可能会导致一些应用程序停止工作。

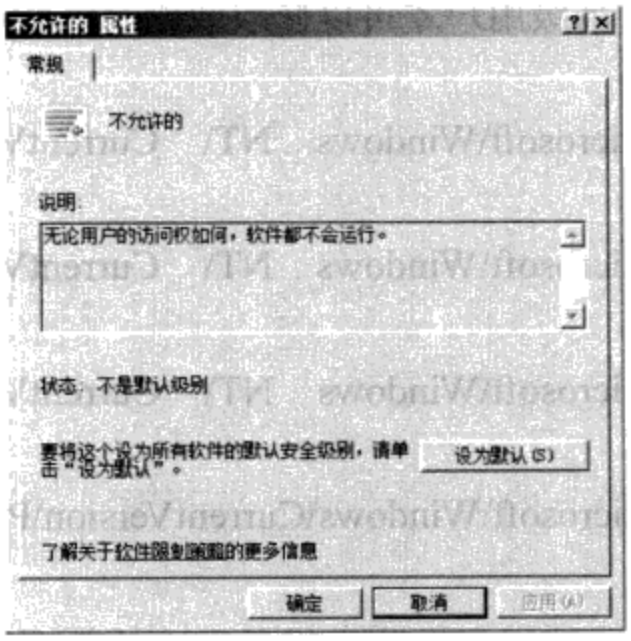


图 13-26　“不允许的 属性”对话框

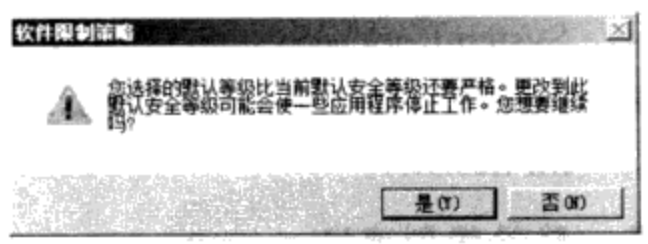


图 13-27　“软件限制策略”对话框

第 3 步，单击“是”按钮，确认设置即可。返回“不允许的 属性”对话框，单击“确定”按钮，保存设置。

3. 设置路径规则

路径规则用于指定程序的文件夹路径或完全限定路径。当路径规则指定文件夹时，将匹配该文件夹中包含的任何程序以及相关子文件夹中包含的任何程序。路径规则既支持本地路径也支持 UNC 路径。

■ 应用程序路径规则

路径规则允许对软件所在的路径进行标识，还允许使用软件的注册表路径规则。由于路径规则软件限制策略是按照软件所在的路径指定的，路径移动后，该软件限制策略将不再适用。

管理员必须在路径规则中定义用于启动特定应用程序的所有目录。例如，如果管理员在桌面上创建了一个用于启动应用程序的快捷方式，则在路径规则中，用户必须能够同时访问可执行文件路径和快捷方式路径才能运行该应用程序。试图仅使用这两个路径之一来运行应用程序将触发“Software Restricted”警告。

默认情况下，所有应用程序使用%ProgramFiles%变量作为安装目录，如果将该变量设置为不同驱动器上的其他目录，某些应用程序仍会将文件复制到原来的%Program Files%子目录中。因此，最好将路径规则定义到默认目录位置。

■ 注册表路径规则

许多应用程序将其安装文件夹或应用程序目录的路径存储在系统注册表中。有些应用程序可以安装在文件系统中的任何位置，管理员可以创建路径规则来查找这些应用程序对应的注册表项。

使用特定文件夹路径或环境变量可能不会很容易地标识这些位置。但是，如果程序将其应用程序目录存储在注册表中，则可以创建一个路径规则，该路径规则将使用注册表中所存储的值，格式为：%<Registry Hive>\<Registry Key Name>\<Value Name>%

如果将默认规则设置为“不允许的”，将设置4个注册表路径，以便操作系统能够访问系统文件以执行正常操作。创建这些注册表路径规则是为了避免将自己和所有其他用户锁定在系统之外。这些注册表规则被设置为“不受限的”。只有高级用户才可以修改或删除这些规则。注册表路径规则设置如下所示：

- %HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\ CurrentVersion\ SystemRoot%
- %HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\ CurrentVersion\ SystemRoot%*.exe
- %HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\ CurrentVersion\ SystemRoot%\System32*.exe
- %HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProgramFilesDir%

■ 路径规则建议

使用表13-1可以确定最适合于应用程序的用户和环境的路径规则。

表13-1 任务与推荐规则

任务	推荐规则
允许或不允许特定程序版本	哈希规则 浏览到文件以创建哈希
标识始终安装在同一位置的程序	带有环境变量的路径规则 %ProgramFiles%\Internet Explorer\iexplore.exe

（续表）

任务	推荐规则
标识可以安装在客户端计算机上的任何位置的程序	注册表路径规则 %HKEY_LOCAL_MACHINE\SOFTWARE\ ComputerAssociates\InoculateIT\6.0\Path\HOME%
标识中央服务器上的一组脚本	路径规则 \\SERVER_NAME\Share
标识一组服务器上的一组脚本	带有通配符的路径规则
例如，DC01、DC02 和 DC03	\\DC??\Share
禁止所有 .vbs 文件，但登录脚本目录中的 .vbs 文件除外	带有通配符的路径规则 *.VBS 设置为“允许的” \\LOGIN_SRV\Share*.VBS 设置为“不受限的”
不允许由病毒安装的名称始终为 flcss.exe 的文件	路径规则 flcss.exe 设置为“不允许的”
标识一组可以在任何位置运行的脚本	证书规则 使用证书对脚本进行数字签名
允许从受信任的 Internet 区域站点安装软件	区域规则 将“受信任的站点”设置为“不受限的”

■ 注册表路径限制实施

第 1 步，单击“开始”按钮，在“开始搜索”文本框中，输入 regedit 并按 Enter 键，打开“注册表编辑器”窗口，找到想要设置路径规则的应用程序对应的注册表项，如 MMC。依次展开“HKEY_LOCAL_MACHINE”→“SOFTWARE”→“Microsoft”→“MMC”，右击 MMC 并选择快捷菜单中的“复制项名称”选项，如图 13-28 所示。

图 13-28 “注册表编辑器”窗口

第 2 步，在“本地组策略编辑器”窗口中，展开“软件限制策略”中的“其他规则”，如图 13-29 所示，系统默认已经设置了“%SystemRoot%”和“%ProgramFilesDir%”的路径规限制，并且默认软件访问规则为“不受限的”。

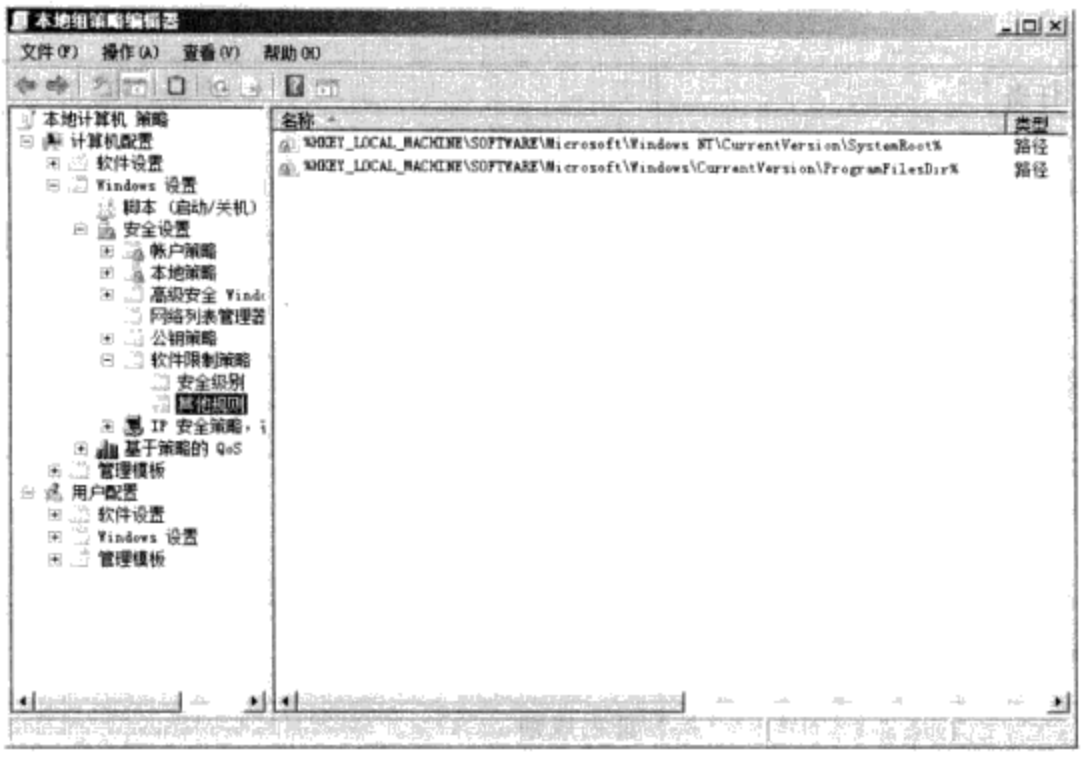


图 13-29　其他规则

第3步，右击“其他规则”并选择快捷菜单中的“新建路径规则”选项，显示如图13-30所示“新建路径规则”对话框，在“路径”文本框中，粘贴已复制的注册表项，并在首位加上“%”符号。在“安全级别”下拉列表框中，选择想要设置的安全级别，如“不允许的”，为了便于区分还可以在“描述”文本框中，输入相关描述信息。

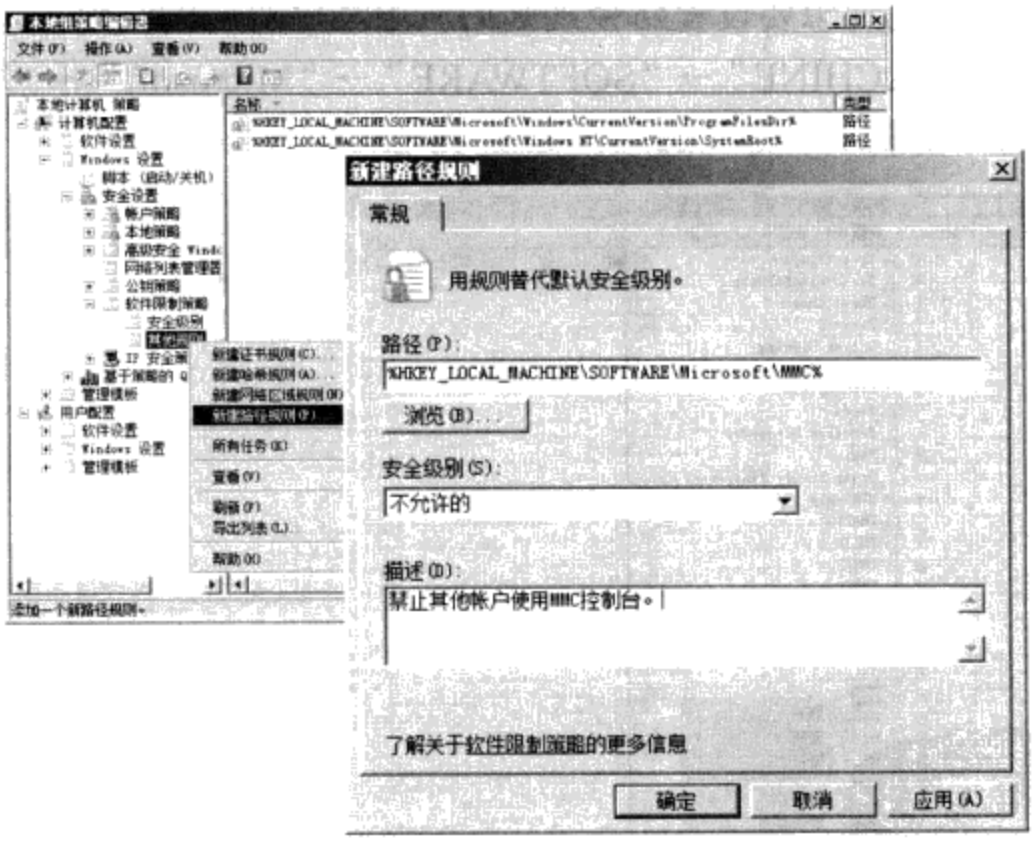


图 13-30　“新建路径规则”对话框

提示　也可以单击“浏览”按钮，为本地计算机上的制定文件夹设置访问规则。

第4步，单击“确定”按钮，保存设置即可。

13.4.3 默认规则

创建软件限制策略的同时，Windows 系统已经默认安装了部分安全规则，包括强制、指派文件类型和受信任的发布者。

1. 强制

除非为组策略指定一个明显的强制规则，否则策略将对组下的所有用户生效。组策略允许对默认的安全级别做其他安排。如果默认的安全级别是“不允许的”，则可以为他指定一个新的规则，允许软件运行。对同一个软件可以使用多个规则，将由具备最高优先权的规则来指定软件是否运行。在“软件限制策略”右侧窗口中，双击“强制”显示如图 13-31 所示“强制 属性”对话框。

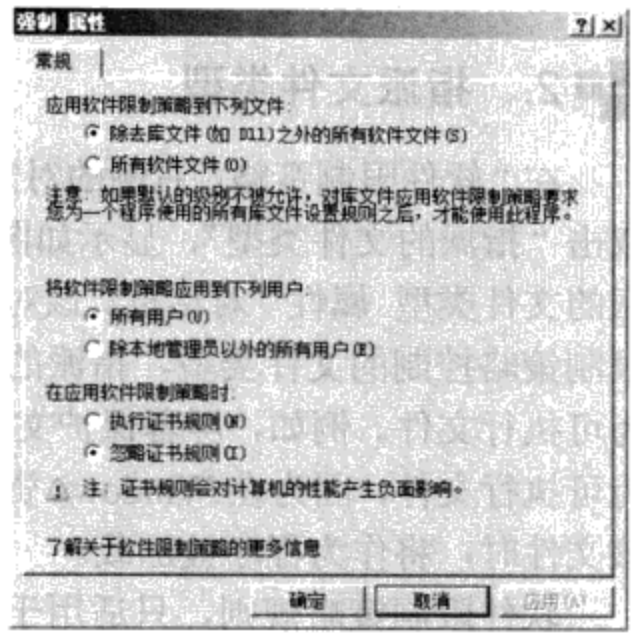


图 13-31 “强制 属性”对话框

■ 应用软件限制策略到下列文件

在该选项区域，管理员可以对目标文件的类型进行限制，系统默认选择“除去库文件（如 DLL）之外的所有软件文件”单选按钮。一个应用软件，可能涉及到很多后台的 DLL 文件，如果选择对所有软件文件进行限制，其他软件调用的时候可能会产生程序关联错误，建议使用除去库文件之外的所有软件文件，即保持系统默认设置。

大多数程序都由可执行文件和许多支持 DLL 组成。默认情况下，不会对 DLL 强制实施软件限制策略规则。这是针对大多数客户的推荐选项，下面列出了这样做的 3 个原因：

- 不允许主要可执行文件可以阻止程序运行，因此无需再阻止构成程序的 DLL。
- 由于 DLL 检查必须检查链接到应用程序的所有库，因此会降低系统性能。例如，如果用户在登录会话中运行了 10 个程序，则软件限制策略将评估每个程序。打开 DLL 检查后，软件限制策略将评估每个程序中的每个 DLL 负载。如果每个程序使用 20 个 DLL，这将导致 10 个可执行程序检查以及 200 个 DLL 检查，因此软件限制策略必须执行 210 次评估。Internet Explorer 之类的程序由可执行文件、iexplore.exe 和多个支持 DLL 组成。
- 将默认安全级别设置为“不允许的”，将强制系统不仅要标识主要可执行文件（在允许该程序运行之前），还要标识作为.exe 文件组成部分的所有 DLL，这将加重系统负担。

■ 将软件限制策略应用到下列用户

在该选项区域，管理员可以设置软件限制策略应用到的用户账户，默认为所有账户，但由于软件策略的应用可能会影响到管理员正常的系统管理和维护操作，因此，建议选择“除本地管理员以外的所有用户”单选按钮。

如果在链接到 Active Directory 中的对象的 GPO 中创建了软件限制策略，则建议拒绝将此 GPO 上的“应用组策略”权限授予 Administrators 组。

■ **在应用软件限制策略时**

在该选项区域，管理员可以设置应用软件限制策略时，是否执行证书规则，系统默认是不执行的。如果本地计算机或所在网络中配置了证书服务器，则可以选择“执行证书规则”单选按钮，即执行软件限制策略的同时执行证书规则中的权限限制。需要注意的是，此时可能会占用过多的系统资源。

2. 指派文件类型

在“软件限制策略”右侧的对象类型列表框中，双击“指派的文件类型”，显示如图 13-32 所示“指派的文件类型 属性”对话框。该对话框列出了软件限制策略控制的文件类型，指派的文件类型将被视为可执行文件。例如，屏幕保护文件（.scr）便被视为可执行文件，因为在 Windows 资源管理器中双击该文件时，将作为程序被加载。

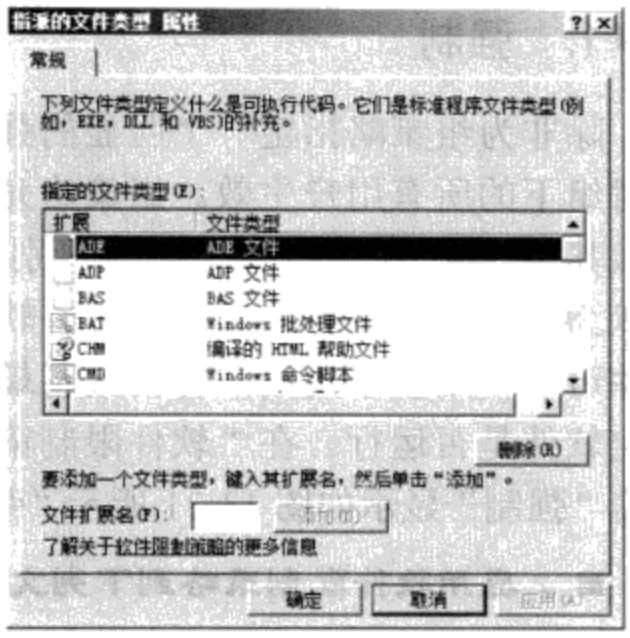


图 13-32 “指派的文件类型 属性”对话框

软件限制策略规则，只适用于“指派的文件类型 属性”对话框列出的文件类型。如果环境使用要应用规则的文件类型，将该文件类型添加到列表中。例如，在“文件扩展名”文本框中输入 docx，并单击“添加”按钮，即可将其添加至“指定的文件类型”列表框中。

3. 受信任的发布者

在“软件限制策略”右侧的对象类型列表框中，双击“受信任的发布者”显示如图 13-33 所示“受信任的发布者 属性”对话框。选中“定义这些策略设置”复选框，管理员可以在这里配置哪些用户可以选择受信任的发布者，还可以确定在信任发布者之前执行哪些证书吊销检查（如果存在证书颁发机构）。系统默认设置为“允许所有管理员和用户管理用户自己的受信任的发布者”，即普通用户账户也可以管理自己受信任的发布者。在域环境中，管理员可以选择“仅允许企业管理员管理受信任的发布者”单选按钮，避免普通擅自更改自己受信任的发布者信息。

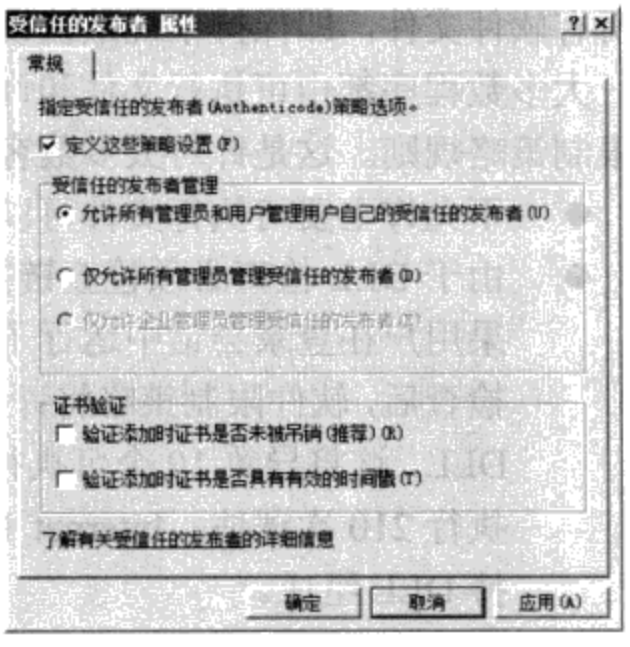


图 13-33 “受信任的发布者 属性”对话框

在“证书验证”选项区域，管理员可以根据需要并结合自己的实际情况，选择相应的验证方式。启用证书规则后，软件限制策略将检查证书吊销列表（CRL），以确保软件的证书和签名有效，这样可能会造成签名程序启动时系统性能的下降。通过验证功能，可以配置与 ActiveX 控件以及其他签名内容相关的设置。

如表 13-2 所示显示了与 ActiveX 控件以及其他签名内容相关的受信任发布者选项。

表 13-2　受信任发布者选项

设置名称	任务
企业管理员	用于只允许企业管理员进行有关签名活动内容的决策
本地计算机管理员	用于允许本地计算机管理员进行有关签名活动内容的所有决策
最终用户	用于允许用户进行有关签名活动内容的决策
发布者	用于确保软件发布者使用的证书未被吊销
时间戳	用于确保组织用于对活动内容加时间戳的证书未被吊销

13.5　配置客户端环境

所谓用户环境就是用户根据自己的工作需要和应用习惯，对系统选项或应用程序进行配置并保存，以便下次登录时能够快速应用自己的配置。在企业网络中，管理员可以借助组策略为用户定制所需的配置环境，如输入法、桌面、应用程序、连接到的网络驱动器等。

13.5.1　定制客户端主页

在“组策略管理编辑器”窗口中，依次展开“用户配置”→“策略”→“Windows 设置”→“Internet Explorer 维护”→“URL”选项，如图 13-34 所示。

在右侧双击“重要 URL”选项，显示如图 13-35 所示“重要 URL”对话框。在此有 3 个文本框，分别是主页 URL、搜索栏 URL 和联机支持页的 URL。分别选中“自定义主页 URL”、“自定义搜索栏 URL”、“自定义联机支持页 URL”复选框，然后在文本框输入相应的主页地址即可。需要注意的是，输入的地址必须以“http://”开始。

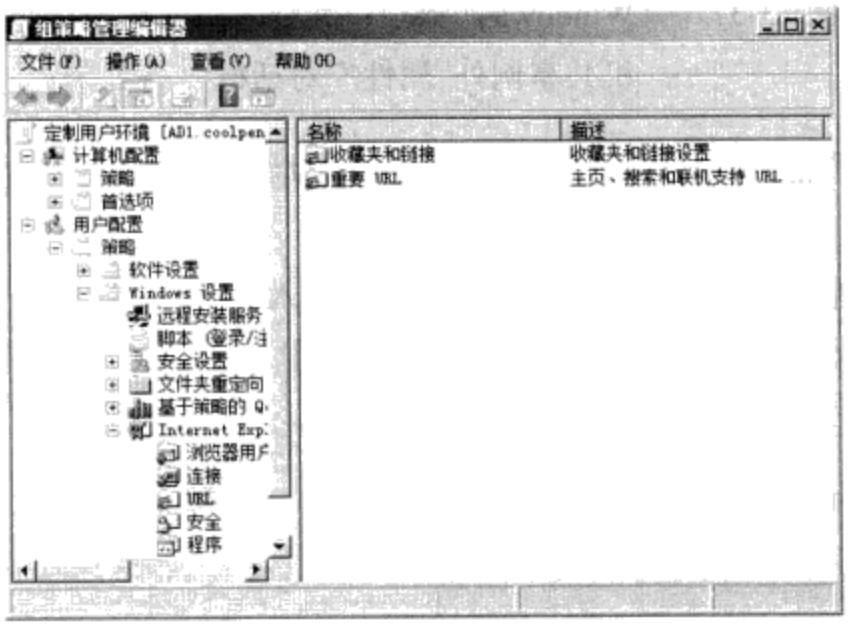


图 13-34　使用组策略对 IE 的进行定制

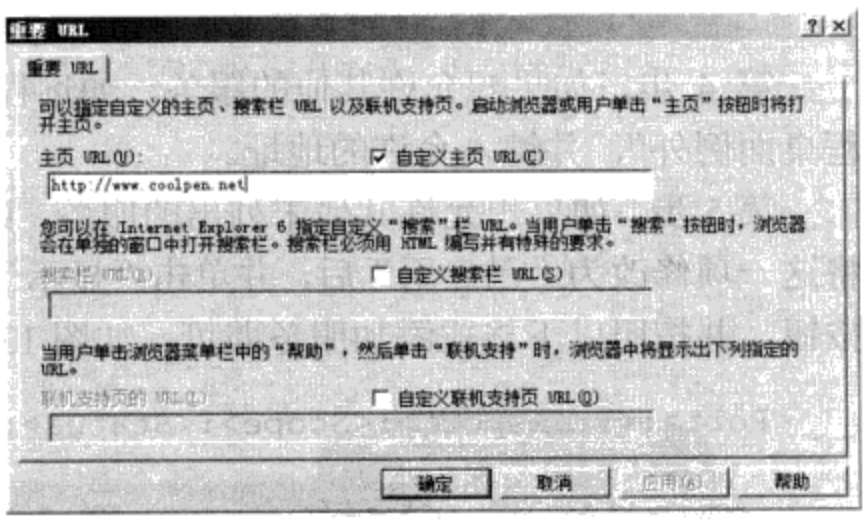


图 13-35　“重要 URL”对话框

13.5.2　修改 Windows 防火墙设置

Windows XP 内置了防火墙，对于“单机上网”的计算机来说，这是一个很方便的事情。但对于企业内部网络来说，如果大家互相共享计算机使用，并且对计算机的防火墙设置不是很熟悉的话，将无法使用文件和共享打印服务。通过修改组策略的方法，修改 Windows XP 的防

火墙设置，为终端计算机启用文件和打印共享，也可以为防火墙打开其他的端口。

第 1 步，在“组策略管理编辑器”窗口中，依次展开“计算机配置”→“管理模板：从本地计算机检索到的策略定义。”→“网络”→“网络连接”→“Windows 防火墙”→“域配置文件”分支，将“Windows 防火墙：不允许例外”策略的值修改为“已禁用”。

第 2 步，将“Windows 防火墙：允许入站远程管理例外”修改为“已启用”，并且在“允许来自这些 IP 地址的未经请求的传入消息”文本框中键入“localsubnet”，如图 13-36 所示。

第 3 步，将“Windows 防火墙：允许入站文件和打印机共享例外”修改为“已启用”，并在“允许来自下列 IP 地址的未经请求的传入消息”文本框中键入“localsubnet”，如图 13-37 所示。

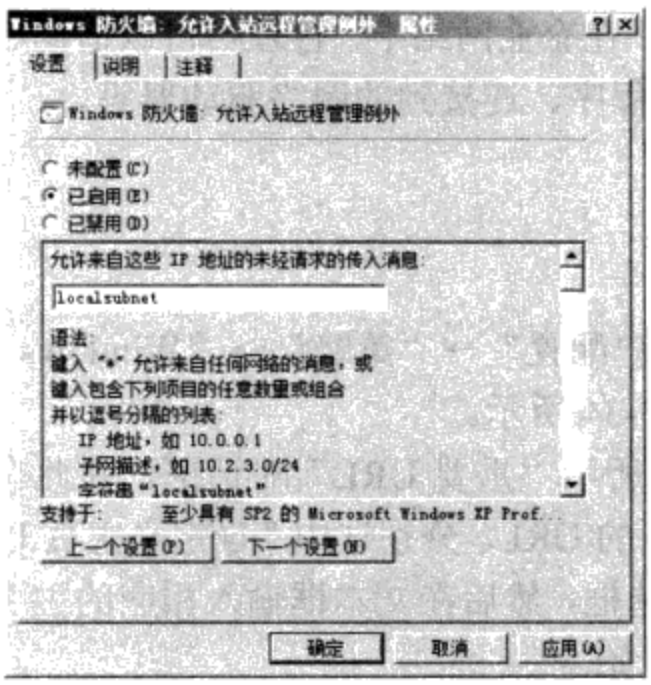


图 13-36 “Windows 防火墙: 允许入站远程管理例外 属性”对话框

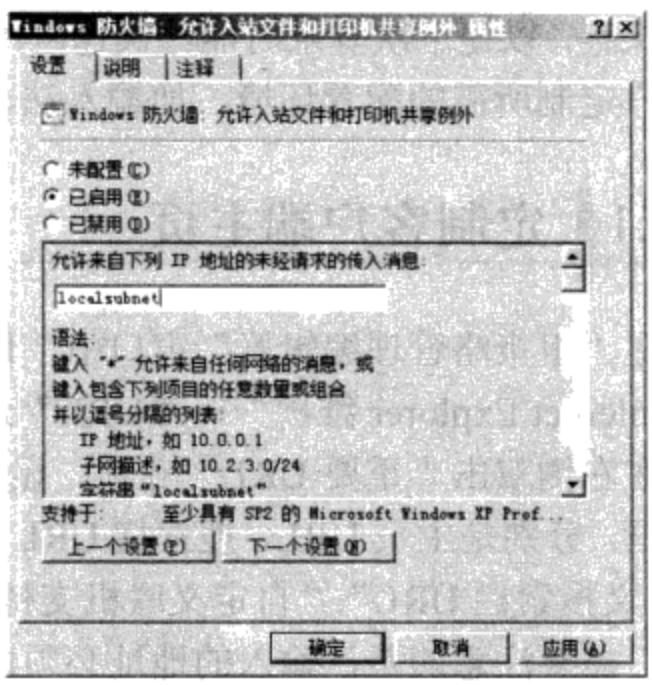


图 13-37 “Windows 防火墙：允许入站文件和打印机共享例外 属性”对话框

第 4 步，如果想允许其他的服务，如远程桌面，则启用“Windows 防火墙：允许入站远程桌面例外”，并键入允许的地址。

第 5 步，如果想允许其他未列出的服务，则启用“Windows 防火墙：定义入站端口例外”，将这一项修改为“已启用”后，并单击“显示”按钮，在“显示内容”对话框中，单击“添加”按钮，并按照以下格式添加服务即可，如图 13-38 所示。

```
<Port>:<Transport>:<Scope>:<Status>:<Name>
```

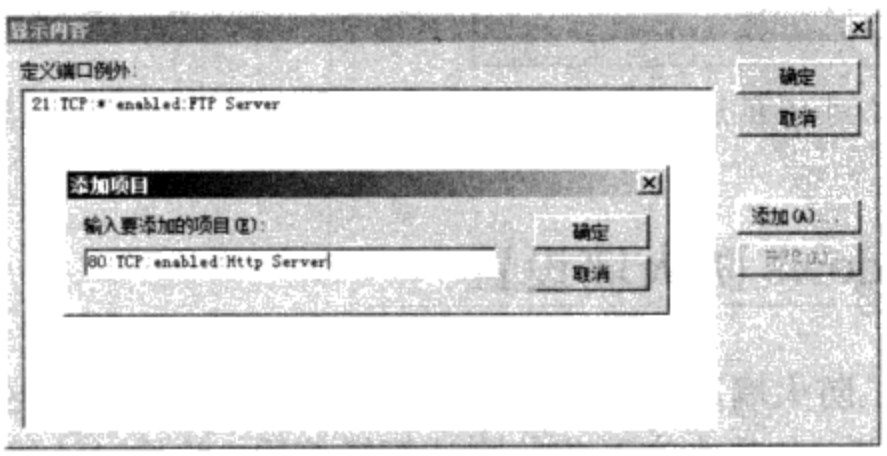


图 13-38 添加其他端口

其中<Port>是十进制的端口号，<Transport>是“TCP”或“UDP”，<Scope>是“*”作用范围包括（*用于所有网络和 IP 地址或子网），例如，在 Windows XP 的计算机上安装了 Web 服务器，想允许外网的用户使用，则需要键入：

```
80:TCP:*:enabled:Http Server
```

第 6 步，依次单击“确定”按钮，保存设置。

说明　虽然可以在这一项禁止 Internet 连接防火墙，但如果计算机的本地管理员，在域策略生效之后（即禁用 Internet 连接防火墙之后），手动启用了 Internet 连接防火墙，则本地管理员的操作将覆盖组策略的设置（只对当前计算机有效）。

13.5.3 取消密码复杂性的要求

在 Windows Server 2008 系统中，要求为用户账户设置符合复杂性要求的密码，这是因为越复杂的密码其安全性越高，但越复杂的密码其记忆难度也越大。因此在企业网络中，很多用户都会抱怨密码太长，不便于记忆和使用。此时，可以通过修改域控制器的安全策略，取消密码的复杂性要求，从而使用简单的密码。具体操作如下：

打开“组策略管理编辑器”窗口，依次选择“计算机配置”→“策略”→“Windows 设置”→“安全设置”→“账户策略”→“密码策略”。根据实际需要，修改右侧窗口中的策略即可，如图 13-39 所示。

默认情况下，所有密码策略都是未配置的。由于系统默认已经继承了来自站点的组策略，所以仍然对用户账户密码有严格要求，在这里需要将相应的策略禁用。双击“密码必须符合复杂性要求”策略，显示如图 13-40 所示“密码必须符合复杂性要求属性”对话框。选中“定义这个策略设置”复选框，选择“已禁用”单选按钮，单击“确定”按钮，保存配置。

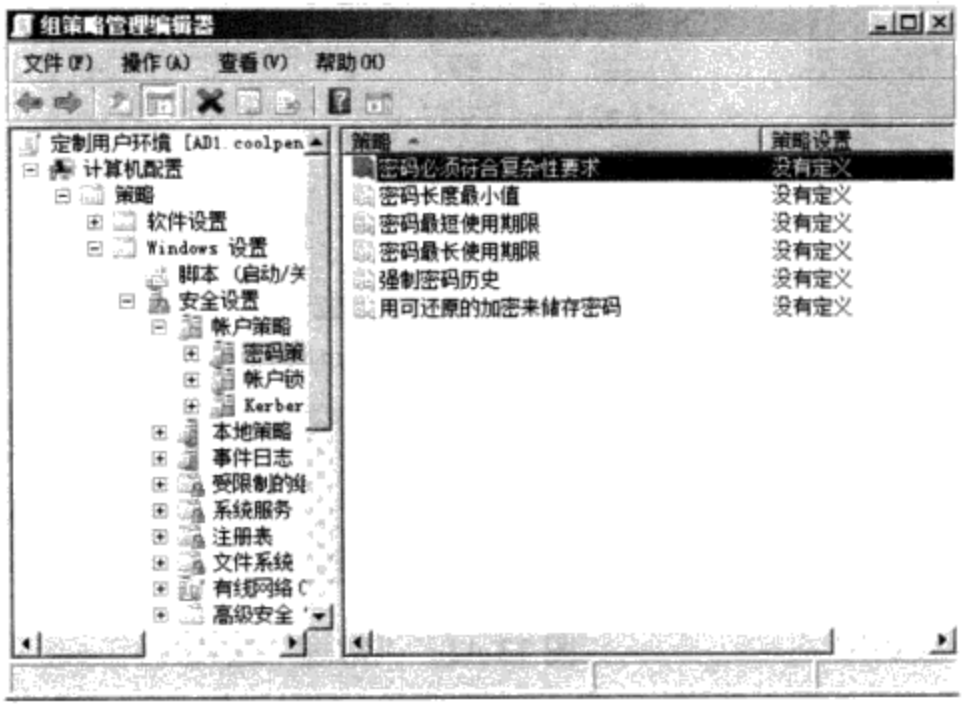


图 13-39　默认密码策略

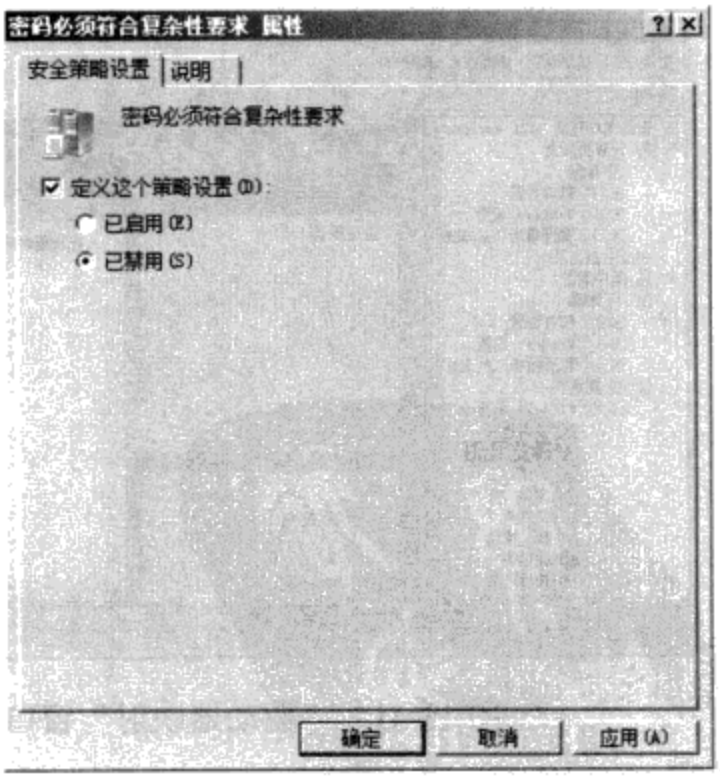


图 13-40　“密码必须符合复杂性要求”对话框

13.5.4 定制用户连接到的网络驱动器

映射网络驱动器是网络管理与应用的一项常用任务。不同类型的用户可能需要随时访问网络中的某些共享资源，如共享文件夹、打印机等。此时，管理员就可以通过组策略为其用户账户定制相关策略，使其无论何时何地登录都可以自动连接到网络驱动器，提高工作效率。

第1步，将希望连接到网络驱动器的用户账户保存到准备好的OU中。在“组策略管理”窗口中，右击该OU选择快捷菜单中创建GPO并开始编辑，打开“组策略管理编辑器”窗口。依次展开“用户配置”→“首选项”→“Windows设置”→“驱动器映射”选项，如图13-41所示。

第2步，在窗口空白处单击鼠标右键，依次选择快捷菜单中的“新建”→“映射驱动器”选项，打开“新建驱动器属性”对话框，默认显示如图13-42所示“常规”选项卡。在“操作”下拉列表框中选择“更新”选项；在“位置”文本框中指定共享文件夹的网络路径；选中“重新连接”复选框，确保用户每次登录时都会自动连接到网络驱动器；在“驱动器号”区域，设置使用的驱动器号；在“连接身份”区域，设置连接共享资源时使用的用户账户凭据，依共享资源的访问权限设置而定，如果指明只有特定账户拥有访问共享资源的权限，则此处必须指定有效凭据。在“操作”下拉列表框中包含如下选项：

- 创建。在客户端计算机建立用来连接此共享文件夹的Z:磁盘（以Z盘为例，下同）。
- 替换。如果客户端已存在网络驱动器Z:，则将其删除后改以此处的设置来替换。若客户端不存在Z:磁盘，则新建Z:磁盘。
- 更新。修改客户端的Z:磁盘设置。例如，修改客户端连接共享文件夹时所使用的用户账户与密码。若客户端不存在Z:磁盘，则新建Z:磁盘。系统默认选择该选项。
- 删除。删除客户端的Z:磁盘。

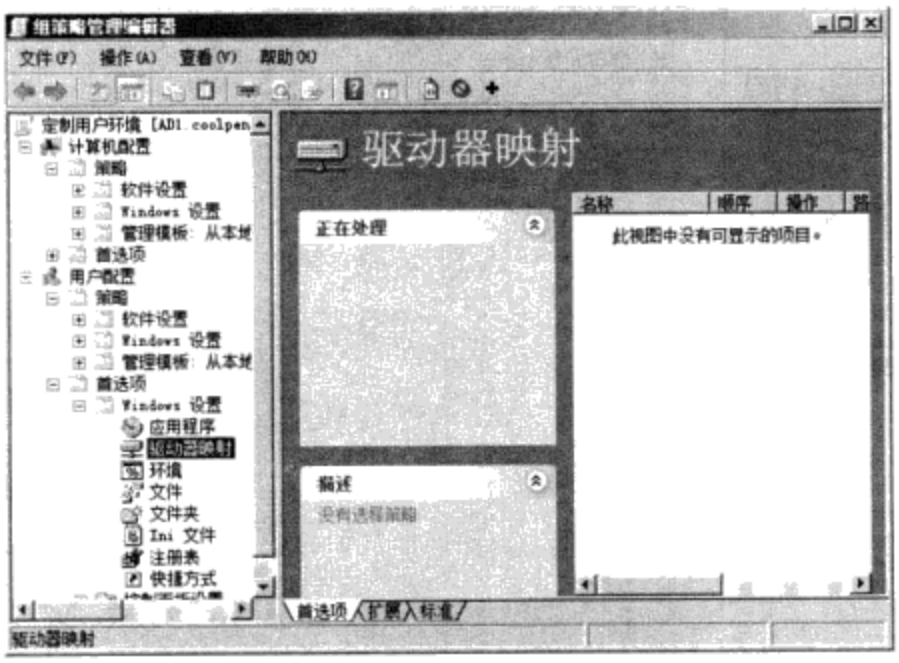


图13-41　“驱动器映射”窗口

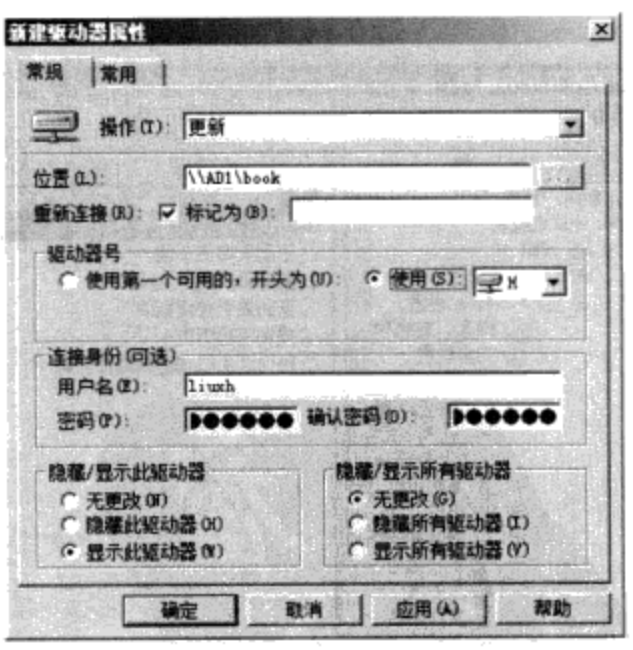


图13-42　“常规”选项卡

第3步，切换至如图13-43所示“常用”选项卡，设置所有项目通用的选项，包含下列项目：

- 如果发生错误，则停止处理该扩展中的项目。如果选择此选项，则失败的首选项会阻止处理扩展中的剩余首选项。此更改行为限于主持的GPO，不扩展到其他GPO。

- 在登录用户的安全上下文中运行（用户策略选项）。如果选择此选项，将更改在其下处理首选项的安全上下文。首选扩展在登录用户的安全上下文中处理首选项。这允许首选扩展以用户而不是计算机形式访问资源。当使用计算机可能没有权限访问资源的驱动器映射或其他首选项时，或使用环境变量时，该设置尤其重要。在非登录用户的安全上下文中评估时，许多环境变量的值会有所不同。
- 当不再应用项目时删除此项目。如果选择此选项，首选扩展确定首选项是否应用于目标用户或计算机（作用域之外）。如果首选扩展确定首选项超出作用域，它将删除与首选项相关的设置。
- 应用一次且不重新应用。如果选择此选项，首选扩展将首选项的结果应用于用户或计算机的次数仅为一次。当用户不希望重复应用首选项的结果时，此选项非常有用。
- 项目级别目标。组策略提供筛选器以控制应用于用户和计算机的策略设置和首选项。如果选中“项目级别目标”复选框并单击“目标”按钮，则可以设置更为详细的附加筛选层，例如，设置是否将首选项应用于指定的用户或计算机组。

第 4 步，单击“确定”按钮，保存设置即可。coolpen OU 中的用户账户，登录到域后即可看到自动创建的网络驱动器 H:盘，如图 13-44 所示。

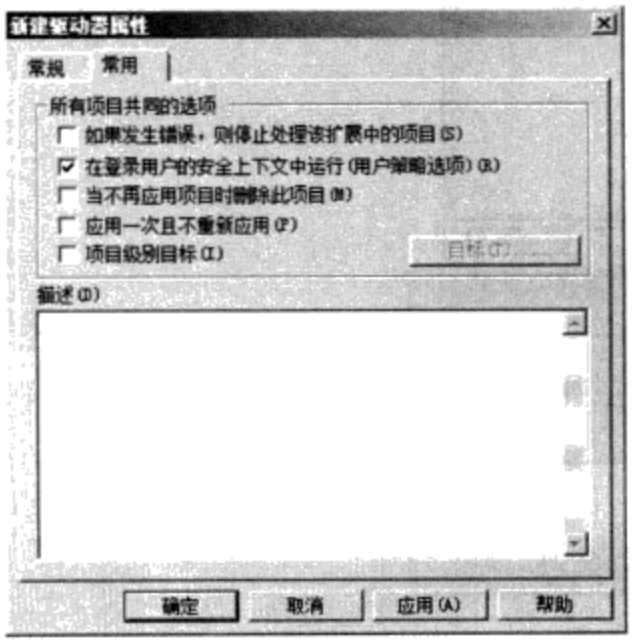


图 13-43 “常用”选项卡

图 13-44 将设置应用到客户端

如果希望为当前 OU 中的部分用户进行特殊配置，则可以按照如下操作步骤进行。

第 1 步，再次新建映射驱动器，为了区别于前面创建的映射驱动器，可以为当前映射驱动器指定其他的盘符和共享文件。在“新建驱动器属性”对话框的“常用”选项卡中，选中“项目级别目标”复选框，单击“目标”按钮，显示“目标编辑器”窗口，默认情况下没有任何项目。单击“新建项目”按钮，即可从级联菜单中选择希望添加的项目，本例选择“用户”选项，如图 13-45 所示。

第 2 步，单击“...”按钮，添加想要指定的用户账户，如图 13-46 所示。此设置将确保只有被选中的用户可以看到指定的映射驱动器。

第 3 步，连续单击“确定”按钮，保存设置即可。在客户端上使用指定的用户账户（此处以 liuxh 账户为例）登录时，即可看到特殊指定的映射驱动器，由于该账户属于 coolpen OU，所以仍可以看到为 coolpen OU 指定的映射驱动器，如图 13-47 所示。

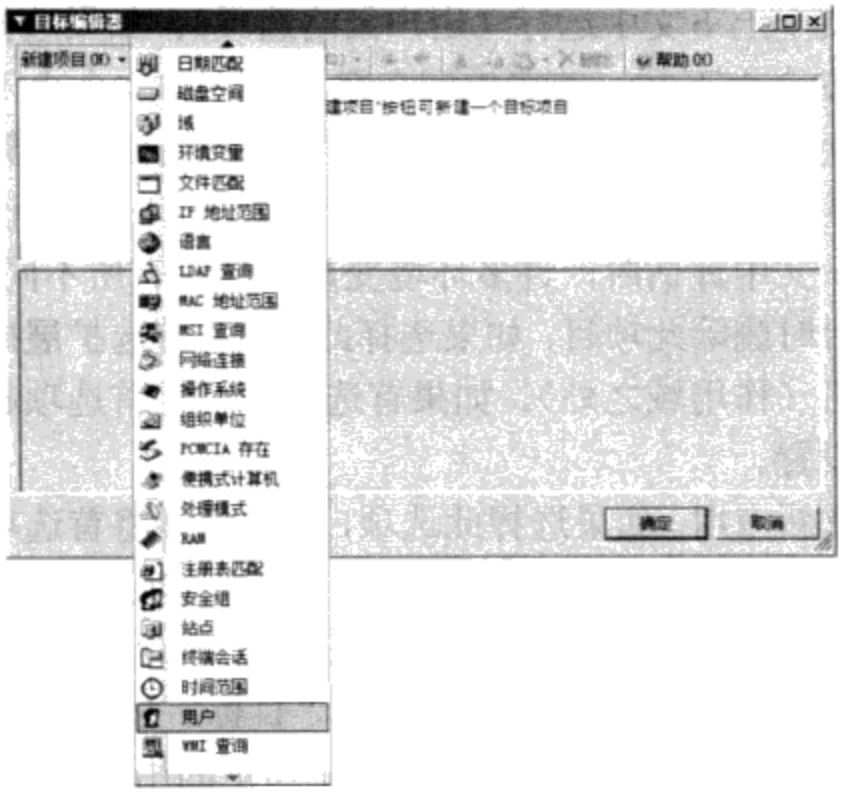


图 13-45 “目标编辑器”窗口

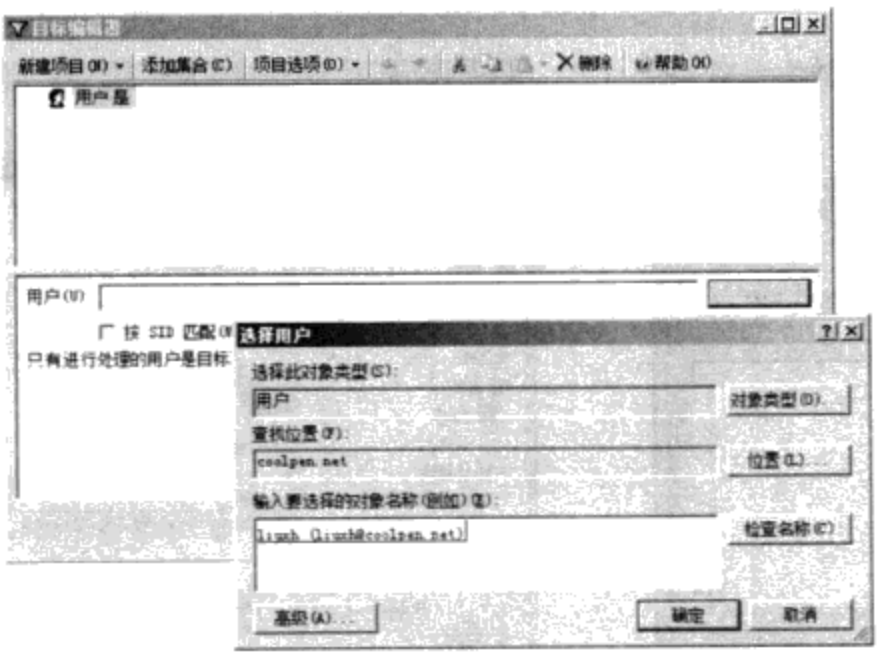


图 13-46 添加需要映射驱动器的用户账户

图 13-47 为个别用户账户映射驱动

第 14 章　网络安全方案示例

网络安全虽然贯穿局域网的每个分支，但是依据网络类型、功能应用、用户需求的不同，也应采取灵活的解决方案。客观的讲，任何安全防御措施的部署，都会在一定程度上影响正常的网络应用，因此规划和设计网络安全系统时必须综合考虑用户需求、应用类型、主要业务等多方面因素。本章主要以示例的方式，简要介绍不同类型网络安全方案的设计。

14.1　校园网安全方案

校园网已经成为院校的一面旗帜，合理使用校园网不仅能够促进院校现代化教学改革、提高教学质量、改善教学环境，还可以加强院校与其他院校和社会互通交流。但是，如果不能确保网络系统的安全，作用就会适得其反。对于校园网而言，网络安全管理的关键在于保护内网重要资源的安全和合理控制用户上网行为。

14.1.1　安全系统设计原则

在规划高校校园网安全系统时，应重点关注以下几个方面：

- 前瞻性。确保网络安全系统能够满足未来 3~5 年网络升级的需求。安全设备性能的降低往往会成为整个网络传输的瓶颈，因此在规划安全系统时，应充分考虑现有网络用户数量、网络带宽、应用类型等因素，尽量做到既要保证校园网的安全运行又要保护学校投资。
- 内部资源安全。网络教学课件、公共资源、公开课、精品课等重要资源，往往会保存在校园的内部服务器上，网络安全系统首先应保证这些宝贵资源不被窃取、篡改和丢失，其次应严格控制内部用户对这些资源的访问和使用。
- 上网行为管理。学生可能会对校园网和 Internet 上的大量资源产生兴趣，但是为了确保大家能够安全、文明的使用网络，必须对内部用户的访问行为进行管理和控制，例如，限制对某些站点的访问和浏览等。另外，还可以借助流控设备、防火墙等对学生经常访问的站点进行统计和分析，及时了解学生的学习和生活动向，为将来教学方案的制定提供翔实素材。
- 网络接入安全。校园网相对于企事业单位的办公网络而言，开放性较高，为了防止非法用户通过公共场所的网络接口进入网络，可以在接入层交换机上部署局域网接入身份验证措施，确保只有符合身份验证条件的用户才能进入校园网。
- 全程网络访问安全。用户的网络访问行为可以分为 3 个阶段，包括访问网络前、访问网络的时候、访问网络后。对应着每一个阶段，都应该有严格的安全控制措施。
- 全局网络安全。
- 网络安全绝非某一个设备或某一项功能的安全，应当让网络中的所有设备都发挥其安全功能，互相协作，形成一个一个全民皆兵、无懈可击的网络，最终从全局的角

度把控网络安全。

14.1.2 网络安全需求分析

1. 局域网病毒传播

校园网最明显的一个特征就是用户数比较多，会有很多的客户端计算机缺乏有效的病毒防范措施，访问 Internet 陌生站点、打开邮件、局域网传输文件、使用 U 盘复制文件等都可能感染计算机病毒，并且会在短时间内传播到服务器、网络设备等，最终导致整个网络性能下降。

一旦计算机病毒感染校园网的某个分支甚至全网，万兆、千兆、百兆的网络带宽都被大量的病毒数据包所消耗殆尽，势必会造成用户正常的网络访问得不到响应，办公平台不能使用，资源库、VOD 不能点播，Internet 无法连接等。

2. 地址盗用

在校园网中，IP 地址、MAC 地址盗用的事情屡见不鲜，在用户看来这些都是微不足道的小事，但却给管理者带来了不小的麻烦。一旦发生地址冲突，将直接导致用户无法接入网络，如果对方是普通用户的话，影响还小一点，如果发生冲突的是服务器或网络设备 IP 地址，则后果不堪设想。另外，地址盗用还是许多恶意用户的惯用伎俩，通过地址欺骗可以轻松窃取内部网络上传输的机密信息，如用户账户、密码、银行卡账户等，后果不堪设想。

3. 对安全事件的溯源

国家相关规定要求，各大 Internet 运营机构（包括高校）必须要保存 60 天的用户上网记录，以待相关部门审计。对于校园网而言，必须明令禁止学生通过网络从事非法活动或散布各种违禁信息，对于管理者而言，一旦发现此类事件，必须能够准确定位到相应的用户和计算机，避免由学校或网络中心成为替罪羔羊。

4. 上网时间控制

如果缺乏有效的机制来限制用户的上网时间，学生可能会利用一切机会上网，会旷课。学生家长会对学校产生强烈的不满，会认为学校及其的不负责任，不是在教书育人。这对学校的声誉以及学校的长期发展是及其不利的。

5. 访问权限控制

在校园网中，不同用户的访问权限应该是不一样的，比如学生应该只能够访问资源服务器、访问 Internet，不能访问办公网络、财务网络。办公网络的用户因该不能访问财务网络。因此，需要对用户网络权限进行严格的控制。

6. 屏蔽网络攻击

校园网中常见的网络攻击比如 MAC FLOOD、SYN FLOOD、DoS 攻击、扫描攻击、ARP 欺骗攻击、流量攻击、非法组播源、非法 DHCP 服务器及 DHCP 攻击、窃取交换机的管理员密码、发送大量的广播报文，这些攻击的存在，会扰乱网络的正常运行，降低了校园网的效率。

14.1.3 网络安全方案

综合分析校园网可能存在的安全威胁和用户安全需求等因素之后，即可开始制定网络安全部署方案。如图 14-1 所示是某高校校园网的拓扑结构，一般可以从物理安全、系统安全、网络互连安全、应用安全、管理安全等 5 个方面进行分析和设计。

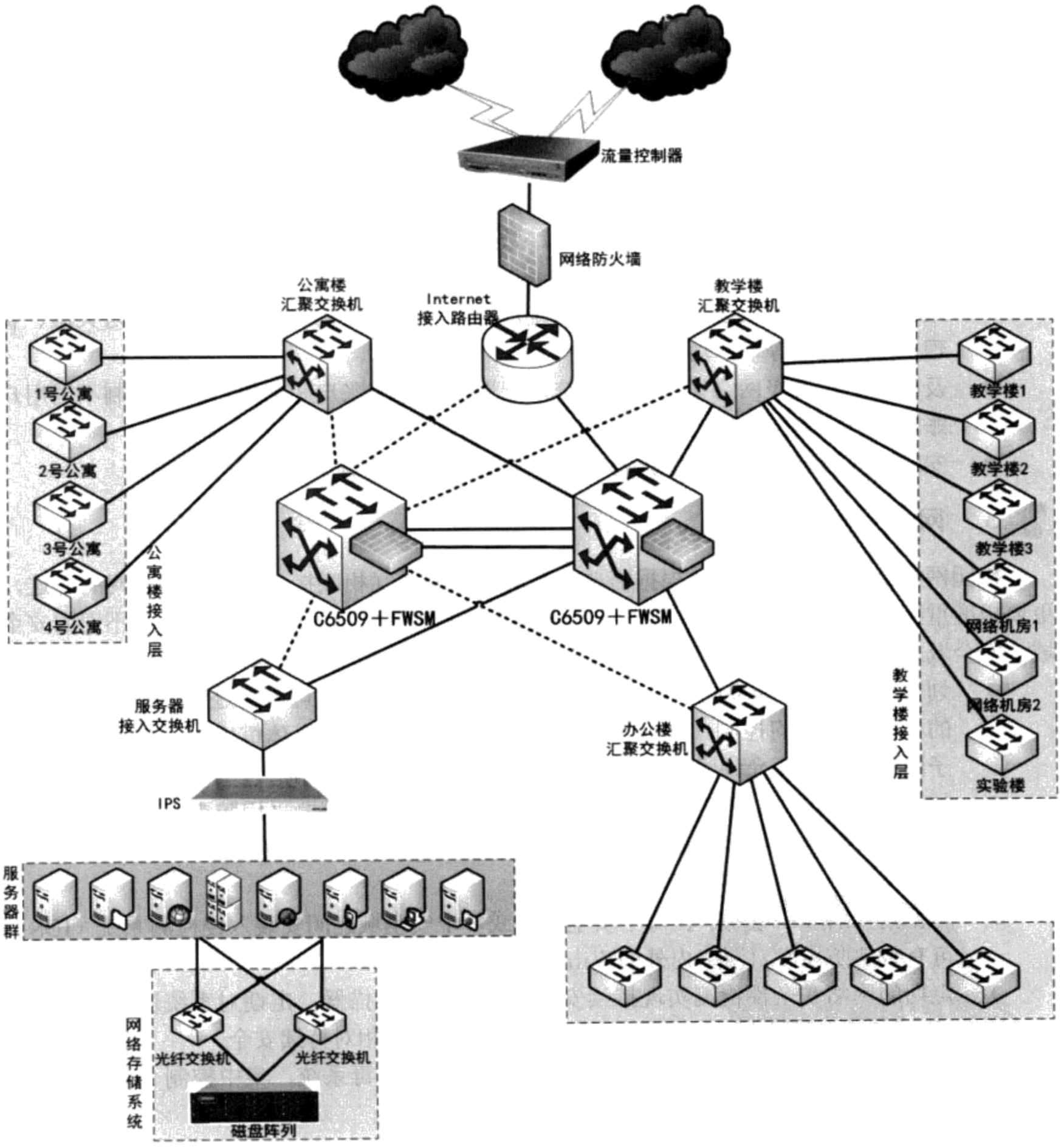


图 14-1　某校园网网络拓扑

1. 物理层安全

物理层的安全主要包括环境、设备及线路的安全：

- 物理环境安全。系统中心或机房的建设应遵照 GB50173-93《电子计算机机房设计规范》、GB2887-89《计算机站场地安全要求》及 GB2887-89《计算机站场地技术条件》的要求，在设备集中的管理间安装干扰器防止由于设备辐射造成的信息泄露。同时，要注意保护线路的安全，防止用户的搭线窃听行为。
- 设备安全。主要包括设备的防盗、防毁、防电磁信息辐射泄露、防止线路截获、抗电磁干扰及电源保护等。
- 媒体安全。包括媒体数据的安全及媒体本身的安全。

2. 系统安全

系统层主要解决的是由于各种操作系统、数据库、及相关产品的安全漏洞和病毒造成的威胁。解决的技术手段主要有以下几种：

- 采用正确的方式安装和配置操作系统，并开启服务器系统的自动更新、防火墙、管理员账户安全等基本功能。
- 及时更新和升级网络设备操作系统，配置各种登录账户和密码，严格控制不同用户账户的访问和操作权限，关闭不必要的服务。
- 安装防病毒程序，定时更新病毒库，定期进行病毒扫描和查杀。

3. 网络互连安全

校园网中局域网数目较多，根据需要多个网络可能要互相联接。正是这种多网的互连，更要极度重视网络层的安全管理。定义一个网络或各网络内不同安全等级的部分为不同的安全域，安全域之间的连接处叫网络边界。用户可以从以下几个方面配置网络互连安全：

- 划分安全子网。如果同一局域网内有不同等级的安全域，可以通过划分子网及 VLAN 的方法加以访问控制。如在教学局域网中学生机房和多媒体机房之间可以通过划分子网来控制，不允许学生机房的机器访问多媒体机房的机器。
- 加强网络边界的访问控制。安全等级差别较大的边界需要采用防火墙来控制。如校园内网、校园外网和 Internet 之间，利用防火墙进行访问控制和内容过滤。可有效地解决需求中提到的多种威胁。
- 防止内外的攻击威胁。在每个安全域内或多个安全域之间安装入侵检测系统（IDS），可有效地防止来自网络内外的攻击。
- 定期的网络安全性检测实现持续安全。利用漏洞扫描器，定期对系统进行安全性评估，及时发现安全隐患并实施修补，可达到网络的相对持续安全。
- 建立网络防病毒系统。在校园网中安装网络版的防毒系统，集中控制、管理查杀网络中服务器、终端的病毒，保护全网不被病毒侵害。

4. 应用安全

网络应用安全设计网络应用的放放面面，一般可以从如下几个方面考虑：

- 各应用系统自身的加固。几乎所有的网络应用和部署都是建立在系统基础上的，因此，必须确保系统自身的安全性和可靠性。
- 建立身份认证系统。校园网内用户数量众多，必须实施统一的网络管理，确保只有拥有合法身份信息的用户才可以进入网络或使用网络资源。
- 建立安全审计系统。安全审计系统的功能是记录用户在网络中进行的操作，一是为了便于管理员跟踪用户的网络应用情况，及时制定相应的网络策略，二是可以在发生网络安全事件或网络故障时，提供解决问题的重要依据。
- 建立备份系统。校园网中的数据量往往是非常惊人的，确保这些数据能够正常使用的重要前提就是建立完善的备份和恢复系统，以便在由于用户非法操作或设备故障而导致数据丢失时，能够尽快恢复，将损失降到最低。

5. 管理安全

网络管理安全主要涉及以下几个方面：

- 建立统一安全管理平台。对于管理员而言，建立统一的网络安全管理平台是非常重要的。网络安全管理工作通常覆盖服务器、网络设备、客户端等各个方面，而管理员不可能时时刻刻守在每台设备旁边，这就需要用到统一的安全管理工具，能够同时远程管理和监控网络中的服务器、客户端以及网络设备的运行状态。
- 建立、健全安全管理体制。校园网用户较多，一定要建立一套合理可行的安全管理制度。只有制度和设备的完美结合才能真正提高校园网的安全水平。
- 加强用户网络安全意识。管理员和重要部门用户的网络安全意识也是非常重要的，应定期对这些人员进行相关培训和技能强化。

14.2 企业网安全方案

企业网络的主要特点就是部门多、部门之间限制多，企业对网络的需求主要集中在局域网资源共享、用户之间的协作、部门之间的信息交流等方面。企业用户人群的网络应用相对比较集中，一般不会尝试或涉及一些与正常工作无关的功能，这是企业网络与校园网明显区别之一。另外，企业网络中某些重要应用往往会与经济利益直接关联，这也是众多管理者不惜重金打造安全网络的初衷。

14.2.1 安全系统设计原则

在对企业局域网网络系统安全方案设计、规划时，应遵循以下原则：

- 综合性和整体性。企业网络的应用虽然并不复杂，但它对企业形象和利益的影响确实非常大的，因此必须综合考虑系统集成工程及应用的各方面因素，既要做到网络安全，又要将安全措施给用户带来的不便降到最低。必要时可以综合应用行政法律、规章制度以及专业措施等多项技术，来打造安全网络。例如，在重要部门或场所采用生物识别技术、门禁系统、高安全产品等，既实现网络安全，又树立了企业形象。
- 需求、风险、代价之间的平衡。绝对安全的计算机网络是不存在的，也不一定是必

要的。对于企业网络而言，能够满足大多数用户的应用需求和安全需求即可，切不可一味追求安全，而将最关键的网络应用束之高阁。

- 一致性。一致性原则主要是指网络安全问题应与整个网络的工作周期（或生命周期）同时存在，制定的安全体系结构必须与网络的安全需求相一致。安全的网络系统设计及实施计划、网络测试、验收、运行等，都要有安全的内容及措施。实际上，在网络建设的开始就考虑网络安全对策，比在网络建设好后再考虑安全措施，不但容易，且花费也小得多。
- 易操作性。安全系统的部署与维护都要由管理员人为完成，如果操作过于复杂，势必会要求管理员具备较高的技术水平，加大管理难度，也会从一定程度上降低安全系统的安全性和可用性。另外，安全措施的采用不应影响系统的正常运行。
- 分步实施。由于网络系统及其应用扩展范围广阔，随着网络规模的扩大及应用的增加，网络脆弱性也会不断增加。一劳永逸地解决网络安全问题是不现实的。同时由于实施信息安全措施需要大量的费用支出。因此分步实施，即可满足网络系统及信息安全的基本需求，亦可节省费用开支。
- 多重保护。任何安全措施都不是绝对安全的，都可能被攻破。但是建立一个多重保护系统，各层保护相互补充，当一层保护被攻破时，其他层保护仍可保护信息的安全。

14.2.2 网络安全威胁

影响企业局域网的稳定性和安全性的因素是多方面的，主要表现在以下几个方面：

- 外网安全。黑客攻击、病毒传播、蠕虫攻击、垃圾邮件泛滥、敏感信息泄露等，都可能影响企业网络的安全运行，并且可能使企业蒙受经济损失。
- 上网行为控制。如果在网关上不能有效掌握和控制内部用户的上网行为，则无法避免内部员工使用公司网络处理私人事务，这不仅会耗费企业网络资源、降低生产效率，更重要的是还可能引入病毒、间谍等安全威胁。
- 部门之间的安全连接。随着企业的发展壮大，逐渐形成了企业总部、各地分支机构、移动办公人员这样的新型互动运营模式。如何处理总部与分支机构、移动办公人员的信息共享安全呢，既要保证信息的及时共享．又要防止机密的泄露，这已经成为企业成长过程中不得不考虑的问题，各地机构与总部之间的网络连接安全直接影响企业的高效运作。

14.2.3 网络安全方案

如图 14-2 所示是某企业计算机网络的拓扑结构，依据不同部门进行了简单的区域划分，包括生产区、办公区、会议室、展示厅、网管区、服务器区和 Internet 接入区。为了实现全网安全，必须在每个网络分支、每个区部署相应的安全措施。

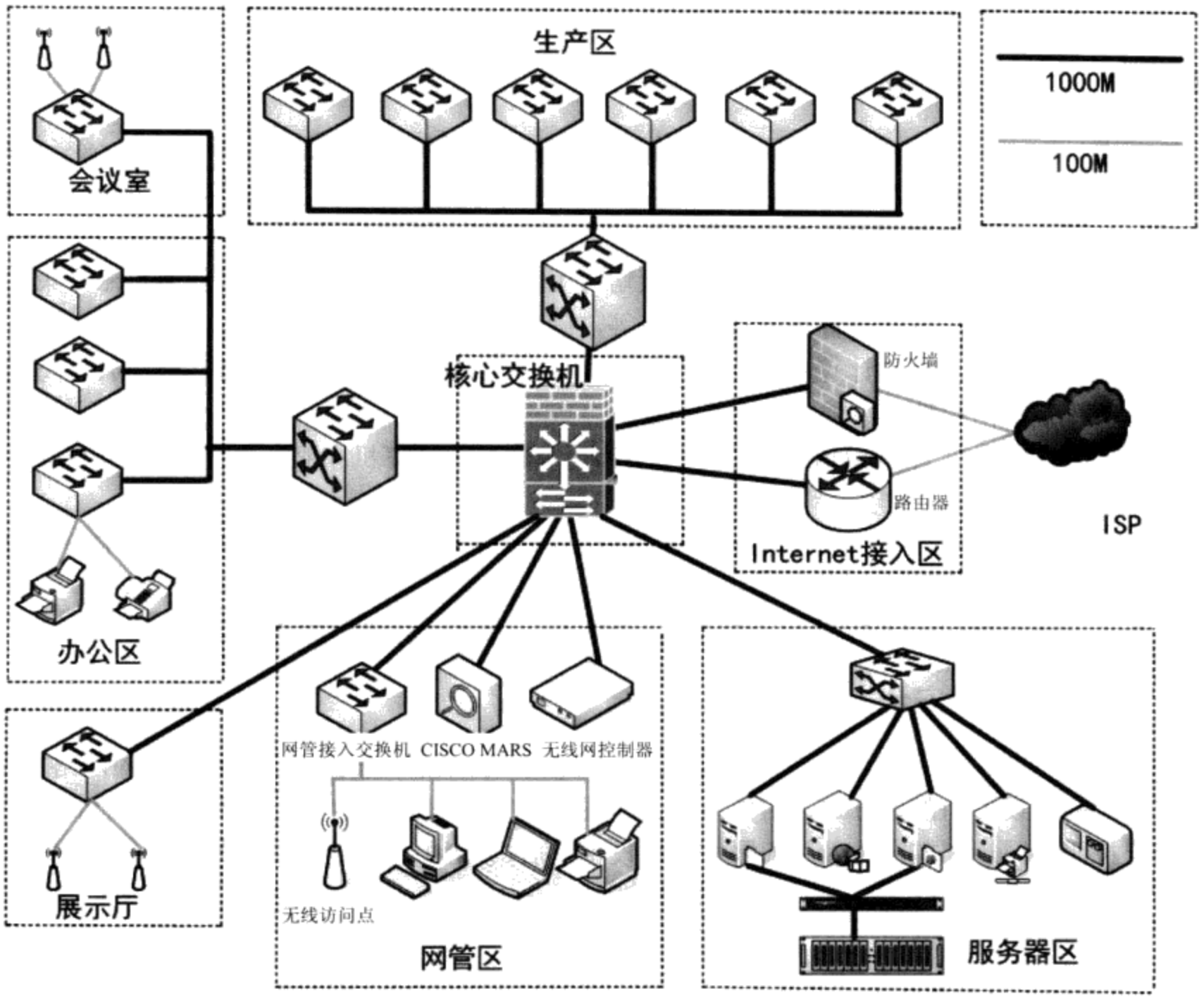


图 14-2　某企业计算机网络拓扑

1. 服务器安全

服务器是企业网络的重要基础，其安全性将直接影响企业网站以及网络应用的安全，甚至会影响企业的生存与发展。服务器的大部分应用都是基于网络操作系统等软件实现的，因此，无论是应用程序出错，还是硬件故障都可能导致服务器瘫痪。若想做好服务器安全防护工作，必须从多方面入手。

- 服务器硬件安全。服务器硬件设备的维护主要包括增加和卸载设备、更换设备、工作环境维护等。因为服务器的运行是不间断的，因此这些维护工作必须在确保服务器正常运行的状态下进行。
- 操作系统安全。服务器操作系统的安全是指操作系统、应用系统的安全性以及网络硬件平台的可靠性。常用的服务器安全措施包括开启防火墙、运行安全配置向导、禁用多余服务和端口、安装安全补丁程序、定期进行漏洞检测和系统安全评估等。
- 网络应用服务安全。局域网中常用的网络服务包括 WWW 服务、FTP 服务、DNS 服务、DHCP 服务、Active Directory 等，随着服务器提供的服务越来越多，系统也容易混乱、安全性也将降低，因此，就需要对网络服务的相关参数进行设置，以增强其

安全性和稳定性。

2. 客户端安全规划

目前，Windows XP 和 Windows 7 是首选客户端操作系统，为了便于统一管理，应将相对固定的客户端计算机加入域，接受域控制器的统一管理。通常情况下，可以从如下方面做好客户端计算机的安全防御工作：

- 对于加入域的计算机可以通过组策略等工具统一部署安全策略，例如用户账户策略、密码策略、硬件设备安装限制策略等，确保客户端的安全。
- 对于未加入域的计算机，应提高用户网络安全的意识，通过设置登录密码、计算机锁定、防火墙等方式，确保系统安全。
- 在网络中部署 WSUS 服务器，负责为所有客户端计算机和服务器提供系统更新，避免系统漏洞的产生。
- 在所有客户端上部署 Symantec 网络防病毒客户端软件，并接受服务器端的统一管理，开启自动更新病毒库功能。
- 灵活部署和运用 Windows 防火墙、Windows Defender 等系统集成安全防护程序。

3. 网络设备安全

局域网中的主要网络设备包括路由器、交换机和防火墙，分别用于提供不同的网络功能和应用。网络设备的部署方式、工作环境、配置管理等，都可能影响其安全性。通常情况下，当用户按照组网规划方案购入并部署好网络设备之后，设备中的主要组成系统即可在一段时间内保持相对稳定的运行。但是，网络设备本身就有一定的脆弱性，这也往往会成为入侵者攻击的目标。用户可以通过如下措施加固设备安全：

- 禁用不必要的网络服务。
- 利用最小特权原则严格对设备的访问控制。配置用户访问安全级别，为不同的管理账户赋予不同的访问和管理权限。
- 及时对系统进行软件升级。IOS 的系统漏洞是不可避免的，用户可以通过安装补丁或升级 IOS 版本的方法避免由于系统漏洞导致的网络攻击。
- 提供符合 IPP（Information Protection Policy，信息保护策略）要求的物理保护环境。
- 配置登录密码，主要包括 Enable 密码和 Telnet 密码，必要时可以以加密方式存储密码，以确保其安全性。

4. 无线网络安全

无线接入不仅是企业发展的需要，更是企业形象的代表。无线局域网是有线网络的扩展，主要用于为移动终端用户提供网络接入。该公司中的 AP（Access Point，无线接入点）主要分布在产品展示区和会议室，方便移动用户随时随地访问公司网络。如今许多笔记本、掌上电脑、手机等都提供无线接入功能，在无线网络覆盖范围内“蹭网”已经成为一种时尚，对于管理员而言无线网络安全自然也就成了管理重点。

在无线局域网管理中，可以采用如下措施确保网络安全：

- 确保桌面计算机和服务器系统实现尽可能的安全。这种保护提高了攻击的门槛，即使攻击者进入了 WLAN，仍然很难渗透进用户的计算机。

- 启用无线 AP 和工作站所支持的最强 WEP。同时，确保拥有一个强健的 WEP 密码，这个密码应该符合有线网络中所应用的相同的密码强度规则。
- 确保无线网络的网络名称（SSID）不是可以轻松识别的。不要使用公司名称、自己的姓名或者地址作为 SSID。
- 如果无线 AP 支持 SSID 广播，应当关闭。这个措施可以创建一个封闭网络，这样，新的客户端必须在连接之前输入正确的 SSID。
- 使用 IEEE 802.1x 身份验证协议保护无线网络的安全。
- 在网络中部署无线网络控制器，统一管理和部署网络中的所有无线接入点，实时监测无线网络攻击情况。

5. 内网访问控制与隔离

企业网络不同部门有着严格的职能界限划分，在网络应用上也应有所体现。一般可以从如下几个方面实现内部用户之间的访问控制与隔离：

- 制订严格的管理制度。管理者可以制定的相应《用户授权实施细则》、《口令字及账户管理规范》、《权限管理制度》等相关规章制度，以约束网络用户的日常行为。
- 部署安全设备。在内部网与外部网之间，设置防火墙实现内外网的隔离与访问控制是保护内部网安全的最主要、同时也是最有效、最经济的措施之一。防火墙设置在不同网络或网络安全域之间信息的唯一出入口。
- 划分 VLAN。划分 VLAN 的主要目的在于隔离内部网络不同的安全区域。通过在交换机上划分 VLAN 可以将整个网络划分为几个不同的广播域，实现内部一个网段与另一个网段的物理隔离。这样，就能防止影响一个网段的问题穿过整个网络传播。另外，通过将不同信任度的网段划分在不同的 VLAN 内，还可以限制局部完全威胁对全局网络造成的影响。

6. 局域网接入安全

根据拓扑结构，可以将局域网分为核心层、汇聚层和接入层 3 个层次。接入层是最终面向用户的，是局域网用户进入网络的接入点，在该层应用保障安全的策略，能为局域网安全运行提供保障。为防止企业网络资源浪费，应避免非法用户的随意接入：

- 有线网络接入安全。在传统有线网络中，通常可以采用 802.1x 认证确保局域网接入的安全，但需要交换机支持和后台的 RADIUS 服务器，同时必须采用国内某些网络厂商提供的 802.1x 解决方案，可以实现用户名、IP 地址、MAC 地址、端口、VLAN、交换机 IP 等的绑定，从而有效避免网络设备、用户等的非法接入。除此之外，防水墙类的产品也可以控制局域网接入，但需要额外投资，并且可靠性不是很高。
- 在无线局域网中，管理员可以通过设置 SSID 加密、WEP 加密、MAC 地址绑定、802.1x 认证等措施确保接入安全。
- 网络访问保护技术。NAP（Network Access Protection，网络访问保护）是为微软 Microsoft 在 Windows Vista 和 Windows Server 2008 提供的全新系统组件，它可以在访问私有网络时提供系统平台健康校验。NAP 平台提供了一套完整性校验的方法来判断接入网络的客户端的健康状态，对不符合健康策略需求的客户端限制其网络访问权限。

7. 审计与监控

审计是记录用户使用计算机网络系统进行所有活动的过程，它不仅能够识别谁访问了系统，还能看出系统正被怎样使用。对于确定是否有网络攻击的情况，审计信息对于去定问题和攻击源很重要。同时，系统事件的记录能够更迅速和系统地识别问题，并且它是后面阶段事故处理的重要依据。另外，通过对安全事件的不断收集与积累并且加以分析，有选择性地对其中的某些站点或用户进行审计跟踪，以便对发现或可能产生的破坏性行为提供有力的证据。

因此，除使用一般的网管软件和系统监控管理系统外，还应使用目前较为成熟的网络监控设备或实时入侵检测设备，以便对进出各级局域网的常见操作进行实时检查、监控、报警和阻断，从而防止针对网络的攻击与犯罪行为。

8. 网络防病毒

在开放的网络环境下，计算机病毒有不可估量的威胁性和破坏力，计算机病毒的防范是网络安全性建设中重要的一环。网络反病毒技术包括预防病毒、检测病毒和消毒3种技术：

- 预防病毒。它通过自身常驻系统内存，优先获得系统的控制权，监视和判断系统中是否有病毒存在，进而阻止计算机病毒进入计算机系统和对系统进行破坏。这类技术有，加密可执行程序、引导区保护、系统监控与读写控制（如防病毒软件等）。
- 检测病毒。它是通过对计算机病毒的特征来进行判断的技术，如自身校验、关键字、文件长度的变化等。
- 清除病毒。它通过对计算机病毒的分析，开发出具有删除病毒程序并恢复原文件的软件。

在部署企业网络防病毒系统时，应依据网络安全需求选择主要面向 E-Mail 服务器、Web 服务器或文件服务器，并且支持统一部署和管理的产品，以便管理员能够通过中心控制台向多个目标分发防病毒客户端程序、升级病毒库、扫描客户端等。

9. 网络可靠性

对于企业网络而言，许多金融、贸易、电子商务等活动都是通过网络完成的，这就要求企业网络具备很高的可靠性。提高网络可靠性的方法有很多，最常用的就是冗余和容错。

在硬件设备方面，可以通过配置交换机生成树、链路汇聚和链路冗余技术，来提高局域网线路连接的可靠性。其中生成树协议可以帮助管理员快速检查网络连接。当主链路发生故障时，便可以自动接通备份链路，确保网络正常工作。链路汇聚技术可以将多条链路聚合为一组干路，还可以提高网络带宽，更重要的是，链路汇聚可以实现负载均衡，从而大大提高了网络的可靠性。局域网接入区域的路由器虽然仅提供路由选择功能，但其重要性也是不容忽视的。可以通过配置路由冗余充分保证 Internet 连接的可靠性。

在软件方面则可以通过服务器群集技术和网络负载均衡技术，来提高重要服务器的可靠性。除此之外，常规的数据备份也是必不可少的，包括服务角色状态信息备份、服务器系统备份、数据库备份、网络设备配置备份等。

[General Information]
书名=网络安全管理实践　第3版
作者=张栋，刘晓辉编著
页数=486
出版社=北京市：电子工业出版社
出版日期=2012.01
SS号=12865998
DX号=000008198686
URL=http://book.szdnet.org.cn/bookDetail.jsp?dxNumber=000008198686&d=EEA379797C212D779ED886718 2D36027