

分享 提升技能的方法

探索 解决问题的关键

非常网管

网络管理

从入门到精通 (修订版)

■ 崔北亮 陈家迁 著

- **10**年资深网管员细致解读网络管理核心技术
- **64**个经典实验全面提升网络管理实战技能
- **4**大讨论主题涉及网络基础、服务器架设与管理、路由和交换、高级应用与故障排除
- 被众多院校选作网络管理课程教材，内容全新升级

 **人民邮电出版社**
POSTS & TELECOM PRESS

你可以通过本书掌握**64**个网管经典实验，快来体验吧！

- | | |
|--------------------------------|---------------------------------|
| 实验1-1 通过无线网卡共享ADSL上网 | 实验5-13 使用数字证书加密和签名电子邮件 |
| 实验1-2 查看局域网中的某台主机是否在线 | 实验6-1 Active Directory中的软件分发 |
| 实验1-3 查看ADSL上网获取到的IP地址 | 实验7-1 用户自定义命令级别 |
| 实验1-4 查看服务使用的端口号 | 实验7-2 配置日志服务器 |
| 实验1-5 使用Sniffer软件监控网络 | 实验9-1 配置单臂路由 |
| 实验1-6 IP子网计算 | 实验9-2 配置三层交换间路由 |
| 实验1-7 IP子网划分 | 实验9-3 环路的判断 |
| 实验1-8 IP路由汇总 | 实验10-1 配置基于TCP的单向访问 |
| 实验2-1 修改网卡的MAC地址 | 实验10-2 配置基于IP的单向访问（网络防火墙） |
| 实验2-2 网桥的工作方式 | 实验10-3 动态ACL |
| 实验2-3 双绞线制作的具体步骤 | 实验10-4 配置基于时间的ACL |
| 实验3-1 利用TCP/IP筛选技术配置计算机的防火墙 | 实验10-5 配置CBAC防火墙 |
| 实验3-2 快速切换IP地址 | 实验11-1 使用ACS对用户的等级进行授权 |
| 实验4-1 创建动态磁盘 | 实验11-2 使用AAA对用户可使用的命令进行授权 |
| 实验4-2 配置RAID-1和RAID-5 | 实验11-3 Cisco IOS认证代理（上网用户管理和计费） |
| 实验4-3 通过NTFS权限和用户管理确保计算机安全 | 实验11-4 基于802.1x的动态VLAN |
| 实验4-4 配置共享 | 实验11-5 配置PPPoE（电信级的用户管理和计费） |
| 实验4-5 在网络中实现打印机的安全共享 | 实验12-1 使用预共享密钥建立站点到站点VPN |
| 实验4-6 使用Netsh命令备份网络设置 | 实验12-2 使用SDM建立站点到站点VPN |
| 实验4-7 远程定期自动备份指定数据 | 实验12-3 使用SDM建立远程接入VPN |
| 实验4-8 Windows Server 2003的系统还原 | 实验13-1 分布式IP电话部署 |
| 实验5-1 备份和还原DNS服务 | 实验13-2 集中式IP电话部署 |
| 实验5-2 企业私有DNS | 实验A 路由器上配置DHCP |
| 实验5-3 巧用DNS实现上网管理 | 实验B 策略路由 |
| 实验5-4 DNS委派 | 实验C 路由器NAT实验 |
| 实验5-5 多Web站点服务器的安全配置 | 实验D 网关冗余 |
| 实验5-6 多邮件服务器间的邮件互发 | 实验E 交换端口分析 |
| 实验5-7 实现FTP服务 | 实验F 配置QoS |
| 实验5-8 代理服务器配置 | 实验G 网络负载平衡 |
| 实验5-9 提供公网服务的内部服务器 | 实验H 限制BT流量 |
| 实验5-10 管理上网用户 | 实验I ARP攻击的攻、判、防 |
| 实验5-11 VPN服务器配置 | |
| 实验5-12 实现网上电视直播 | |



ISBN 978-7-115-24059-0



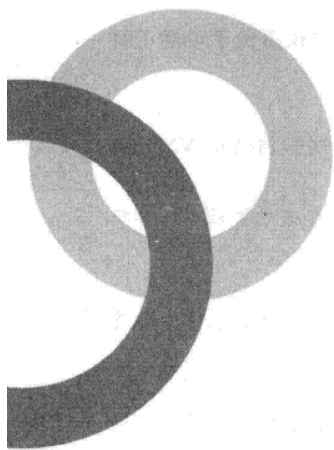
9 787115 240590 >

ISBN 978-7-115-24059-0

定价: 49.00 元

分类建议: 计算机 / 网络技术

人民邮电出版社网址: www.ptpress.com.cn



前言

Preface

随着网络技术的不断发展，人们的日常生活越来越离不开网络，小到家庭用局域网、网吧和小型办公网络，大到能够联通全球的 Internet，网络正在逐步改变着人们的生活方式，甚至是生活习惯。

为什么写本书

网络管理工作是计算机网络实践的重中之重，而本书正是基于这个市场热点编写的。

作者凭借多年高校教育、社会培训、网络咨询等方面的经验，发现社会上迫切需要那些懂得服务器架设和管理，熟悉路由器和交换机配置，能够快速排除网络故障的实用型人才。而本书就是服务于此的一本实用性极强的、提供综合网络实验环境的网络管理类图书。

本书特色

本书融入了作者10多年的工作心得和体会，并结合最新的网络技术，呈现给读者的不仅是一本教材，更是提供了一个综合的网络实验环境，便于读者在此之上深入领会网络管理技术的精髓。

仅仅通过一台计算机，便可以虚拟出多台计算机、路由器和交换机工作的情况，并能将它们完美地结合在一起，完成本书涉及的几乎所有服务器、路由器和交换机的实验配置及测试。

全书 65 个实验均是针对目前网络中的焦点问题和热门应用展开，包括各种服务器的架设、IP 语音电话、AAA 应用、VPN 配置、BT 流量限制、策略路由、PPPOE 计费、网络管理等。

主要内容

全书共分为 4 部分 14 章，65 个实验，主要内容介绍如下。
第 1 部分“网络基础篇”，包括第 1 章和第 2 章。

- 第1章主要介绍网络的基础、网络的体系结构、ISO/OSI参考模型、TCP/IP,以及无线网卡直接相连的配置,Sniffer软件的使用,IP地址的分类、计算、划分、汇总等。
- 第2章主要介绍网络硬件的相关知识,包括网络传输介质和网络硬件设备便于读者了解它们的工作原理和之间的区别,以便在工程中进行正确的选择。
- 第2部分“服务器架设和管理篇”,包括第3章至第6章。
 - 第3章主要介绍Windows Server 2003的安装和初始配置,重点讲述如何使用VMware软件在单台计算机上虚拟出各类网络实验环境。
 - 第4章主要介绍Windows Server 2003中用户和组的管理、磁盘和文件夹的管理、计算机的远程管理等内容。
 - 第5章主要介绍Windows Server 2003中常用服务的配置和管理。
 - 第6章主要介绍组策略的功能和工作方式,在AD(Active Directory,活动目录)中配置和应用组策略的方法,以及如何集中地管理用户和计算机。
- 第3部分“路由和交换篇”,包括第7章至第14章。
 - 第7章介绍路由器的硬件和软件,如“Dynamips”机架的搭建、路由器的基本硬件和软件、路由器的可选模块及其功能描述等。
 - 第8章通过介绍TCP/IP网络中路由器的基本工作原理,引出了静态路由协议和动态路由协议,以及内部网关协议和外部网关协议。同时介绍了目前最常见的直连路由、静态路由、默认路由和动态路由(包括RIP和OSPF)这几种路由协议,结合实验演示了这几种常见路由协议的配置。
 - 第9章介绍了冲突域和广播域,以便读者能够正确地配置VLAN来隔离广播,增强网络安全等。
 - 第10章介绍访问控制列表,内容包括标准、扩展、命名、自反、动态、基于时间/基于上下文的访问控制列表等项目。
 - 第11章讲解AAA的相关概念、Cisco Secure ACS软件的情况,以及如何使用Cisco Secure ACS软件在工程中对用户进行认证、授权和记账,如何结合AAA配置802.1x的动态VLAN、配置IOS认证代理和PPPoE,实现上网用户的管理。
 - 第12章介绍VPN的基础知识和IPSec VPN的技术原理与实现。
 - 第13章主要介绍VoIP的基础知识、VoIP模块接口类型、VoIP呼叫建立的过程。
 - 第14章主要介绍配置SolarWinds网管系统,完成复杂网络的管理。
- 第4部分“高级应用和故障排除篇”,共包括9个综合性的实验。
 - 实验A 配置DHCP,实现IP地址的自动分配。
 - 实验B 配置策略路由,实现数据包选路的灵活性。
 - 实验C 配置NAT,实现IP的共享上网。
 - 实验D 配置网关冗余,保障网络的高可用性。
 - 实验E 配置交换端口镜像,实现分析数据包监控和故障排除。
 - 实验F 配置QoS,实现有区分的服务。
 - 实验G 配置网络负载均衡服务器,实现服务的高可用性。
 - 实验H 配置路由器,限制BT流量。
 - 实验I 分析ARP的攻击原理,判断ARP攻击的存在,防止和排除ARP的存在。

读者对象

本书既可作为网络管理和维护人员实际工作中的自学和参考用书，也可作为高等院校计算机网络相关专业的教材和参考书，或社会培训机构相关领域的培训用书。

资源获取

读者如果需要书中涉及的相关软件及源代码，可以发邮件至computerbook@126.com索取，并请附上阅读本书的相关意见和建议。

本书主要由崔北亮、陈家迁编写，参加本书内容审校和绘图工作的还有庞松鹤、温剑锋、曹晶星、吴健、黄崇争、廖国葵、赵婧聪、吴永丰、孙宙、孙兰欣、莫恭乾、徐亮、陆芸、吴超等，在此一并表示感谢。

编 者
2010 年 10 月



目 录

Contents

第 1 部分 网络基础篇

第 1 章 网络基础知识回顾	2	2.1 网络传输介质	29
1.1 计算机网络基础	2	2.1.1 传导型介质	29
实验 1-1 通过无线网卡共享 ADSL 上网	5	2.1.2 辐射型介质	32
1.2 网络体系结构	9	2.1.3 传导型介质与辐射型介质的比较	33
1.3 ISO/OSI 参考模型	11	2.2 网络硬件设备	34
实验 1-2 查看局域网中的某台主机是否在线	12	2.2.1 网卡	34
实验 1-3 查看 ADSL 上网获取到的 IP 地址	15	实验 2-1 修改网卡的 MAC 地址	35
实验 1-4 查看服务使用的端口号	15	2.2.2 中继器	36
1.4 TCP/IP	17	2.2.3 集线器	36
1.4.1 TCP/IP 参考模型	17	2.2.4 网桥	37
实验 1-5 使用 Sniffer 软件监控网络	17	实验 2-2 网桥的工作方式	37
1.4.2 TCP/IP 参考模型与 ISO/OSI 参考模型比较	24	2.2.5 交换机	40
1.4.3 IP 地址划分	24	2.2.6 路由器	41
1.4.4 子网划分的具体方法	25	2.2.7 网关	41
实验 1-6 IP 子网计算	26	2.2.8 宽带路由器	42
实验 1-7 IP 子网划分	27	2.2.9 防火墙	42
实验 1-8 IP 路由汇总	28	2.3 双绞线的制作	43
第 2 章 网络硬件知识	29	2.3.1 双绞线的种类	43
		2.3.2 水晶头的针脚	44
		实验 2-3 制作双绞线的具体步骤	45

第 2 部分 服务器架设和管理篇

第 3 章 Windows Server 2003 安装和配置 .. 49	4.3 远程管理 .. 105
3.1 安装 Windows Server 2003 .. 49	4.3.1 配置服务端 .. 105
3.1.1 选择版本 .. 49	4.3.2 配置远程桌面连接 .. 105
3.1.2 安装前的准备工作 .. 50	4.3.3 配置远程桌面 .. 108
3.1.3 安装步骤 .. 51	第 5 章 配置常用服务器 .. 109
3.2 Windows Server 2003 的初始设置 .. 55	5.1 微软服务器可以实现的功能 .. 109
3.2.1 启用操作系统自带的防火墙 .. 55	5.2 DHCP 服务器 .. 110
实验 3-1 利用 TCP/IP 筛选技术配置	5.2.1 DHCP 常用术语 .. 111
计算机的防火墙 .. 56	5.2.2 DHCP 运行方式 .. 112
实验 3-2 快速切换 IP 地址 .. 58	5.2.3 DHCP/BOOTP 中继代理 .. 113
3.2.2 启动/停止默认的服务 .. 58	5.2.4 DHCP 服务器的安装与配置 .. 113
3.2.3 安装补丁程序 .. 60	5.2.5 DHCP 客户机的设置 .. 119
3.3 用单台计算机虚拟一个局域网 .. 61	5.3 DNS 服务器 .. 120
3.3.1 安装 VMware 虚拟机软件 .. 62	5.3.1 域名解析方式 .. 120
3.3.2 虚拟机的基本设置 .. 62	5.3.2 创建查找区域 .. 121
3.3.3 构建局域网 .. 69	5.3.3 添加资源记录 .. 123
3.3.4 测试局域网 .. 70	实验 5-1 备份和还原 DNS 服务 .. 124
第 4 章 计算机管理 .. 71	实验 5-2 企业私有 DNS .. 125
4.1 用户和组管理 .. 71	实验 5-3 巧用 DNS 实现上网管理 .. 126
4.2 磁盘和文件夹管理 .. 73	实验 5-4 DNS 委派 .. 127
4.2.1 磁盘管理 .. 73	5.4 WWW 服务器 .. 129
实验 4-1 创建动态磁盘 .. 75	5.4.1 IIS 的安装 .. 129
实验 4-2 配置 RAID-1 和 RAID-5 .. 79	5.4.2 Web 站点基本配置 .. 131
4.2.2 文件夹管理 .. 84	5.4.3 虚拟主机的实现 .. 134
实验 4-3 通过 NTFS 权限和用户管理	实验 5-5 多 Web 站点服务器的
确保计算机安全 .. 87	安全配置 .. 136
4.2.3 共享 .. 88	5.5 E-mail 服务器 .. 139
实验 4-4 配置共享 .. 88	5.5.1 安装 SMTP 和 POP3 服务 .. 139
实验 4-5 在网络中实现打印机的安全	5.5.2 注册邮件账号 .. 141
共享 .. 92	5.5.3 Outlook Express 设置 .. 143
4.2.4 卷影复制 .. 92	实验 5-6 多邮件服务器间的邮件互发 .. 144
4.2.5 EFS 加密和安全 .. 95	5.5.4 设置邮箱基本属性 (可选) .. 146
4.2.6 备份和还原 .. 101	5.5.5 设置邮箱安全属性 (可选) .. 146
实验 4-6 使用 Netsh 命令备份网络设置 .. 101	5.6 FTP 服务器 .. 148
实验 4-7 远程定期自动备份指定数据 .. 102	实验 5-7 实现 FTP 服务 .. 149
实验 4-8 Windows Server 2003 的系统	5.7 路由和远程访问服务器 .. 150
还原 .. 103	实验 5-8 代理服务器配置 .. 150

实验 5-9 提供公网服务的内部服务器	152
实验 5-10 管理上网用户	154
实验 5-11 VPN 服务器配置	157
5.8 架设视频服务器	160
5.8.1 安装 Windows Media 服务器	161
5.8.2 安装 Windows Media 编码器	162
5.8.3 转换文件格式	162
5.8.4 视频直播	164
5.8.5 实现网络教学	166
实验 5-12 实现网上电视直播	166
5.9 证书服务	170
5.9.1 数字证书	171
5.9.2 安装证书服务	171
5.9.3 管理证书	172

实验 5-13 使用数字证书加密和签名	
电子邮件	176
5.9.4 IIS 与数字证书	181
5.9.5 利用数字证书进行代码签名	186

第 6 章 组策略	187
6.1 组策略简介	187
6.1.1 组策略的功能	187
6.1.2 组策略的工作方式	188
6.1.3 应用组策略的要求	188
6.2 设置组策略	189
6.2.1 搭建域环境	189
6.2.2 组策略配置选项	192
实验 6-1 Active Directory 中的软件分发	194

第 3 部分 路由和交换篇

第 7 章 路由器的硬件和软件	206
7.1 搭建路由器和交换机实验机架	206
7.1.1 实验机架拓扑	207
7.1.2 安装 “Dynamips”	208
7.1.3 “Dynamips” 的使用方法	211
7.1.4 设计 “Dynamips” 的拓扑	212
7.2 路由器基本硬件	213
7.3 路由器基本软件	219
7.4 路由器的配置过程	220
实验 7-1 用户自定义命令级别	225
实验 7-2 配置日志服务器	233

第 8 章 路由	236
8.1 路由知识	236
8.1.1 网络互连	236
8.1.2 路由原理	238
8.1.3 路由协议	239
8.2 直连路由	241
8.3 静态路由	244
8.4 默认路由	246
8.5 动态路由协议	247
8.5.1 RIP 路由协议	247
8.5.2 OSPF 路由协议	251
8.6 管辖距离	253

8.7 路由选路	255
8.8 IP 主机表	256
8.9 辅助地址	258
第 9 章 交换机	259
9.1 交换概述	259
9.1.1 冲突域和广播域	259
9.1.2 局域网分段	261
9.1.3 交换机的分类	262
9.2 VLAN 的实现	264
9.2.1 VLAN 的概念	264
9.2.2 VLAN 的优点	265
9.2.3 动态 VLAN 和静态 VLAN	266
9.2.4 帧过滤与帧标记	267
9.2.5 VLAN 干线	267
9.2.6 VLAN 的封装和工作方式	269
9.2.7 配置 VLAN	271
9.2.8 VLAN 间路由	274
实验 9-1 配置单臂路由	274
实验 9-2 配置三层交换间路由	276
9.3 STP 的实现	277
9.3.1 冗余拓扑中存在的问题	277
实验 9-3 环路的判断	279
9.3.2 STP 的工作方式	281
9.3.3 生成树的端口状态	284

9.3.4 增强 STP 功能	284	11.5 配置 AAA 记账	322
9.4 链路聚合的实现	285	实验 11-3 Cisco IOS 认证代理 (上网	
9.4.1 聚合端口的要求	286	用户管理和计费)	323
9.4.2 配置链路聚合	286	实验 11-4 基于 802.1x 的动态 VLAN	329
第 10 章 访问控制列表	288	实验 11-5 配置 PPPoE (电信级的用户	
10.1 标准访问控制列表	288	管理和计费)	332
10.1.1 通配符掩码	289	11.6 ACS 中用户密码的修改	337
10.1.2 配置标准访问控制列表	290	第 12 章 VPN (虚拟专用网)	341
10.2 扩展访问控制列表	291	12.1 VPN 基础知识	341
10.2.1 配置扩展访问控制列表	291	12.1.1 VPN 优点	342
10.2.2 扩展访问控制列表的增强		12.1.2 IPSec VPN 分类	342
编辑功能	293	12.2 IPSec (IP 安全)	343
10.2.3 扩展 ACL 中的 Established	294	12.2.1 IPSec 功能	343
实验 10-1 配置基于 TCP 的单向访问	295	12.2.2 IPSec 工作模式	346
10.3 命名访问控制列表	295	12.2.3 IPSec 相关协议	347
10.4 配置标准访问控制列表的注意		12.3 IPSec 操作过程	348
事项	296	12.4 VPN 配置实例	350
10.5 反射 ACL	298	实验 12-1 使用预共享密钥建立站点	
实验 10-2 配置基于 IP 的单向访问		到站点 VPN	351
(网络防火墙)	299	实验 12-2 使用 SDM 建立站点到	
10.6 动态 ACL	302	站点 VPN	355
实验 10-3 动态 ACL	303	实验 12-3 使用 SDM 建立远程	
10.7 基于时间的访问控制列表	304	接入 VPN	361
实验 10-4 配置基于时间的 ACL	305	第 13 章 VoIP (IP 电话)	373
10.8 基于上下文的访问控制列表	306	13.1 IP 电话的基础知识	373
10.8.1 CBAC 功能	306	13.2 VoIP 模块的接口类型	374
10.8.2 配置 CBAC	307	13.3 呼叫建立的过程	375
实验 10-5 配置 CBAC 防火墙	308	13.4 VoIP 电话的配置	377
第 11 章 AAA (认证、授权、记账)	310	实验 13-1 分布式 IP 电话部署	378
11.1 AAA 简介	310	实验 13-2 集中式 IP 电话部署	384
11.2 Cisco Secure ACS	311	第 14 章 SolarWinds 网管系统	386
11.2.1 安装 ACS	311	14.1 功能简介	386
11.2.2 ACS 的基本配置	313	14.2 安装 SolarWinds	389
11.3 配置 AAA 认证	315	14.3 配置 SolarWinds	391
11.4 配置 AAA 授权	318	14.3.1 配置数据库	391
实验 11-1 使用 ACS 对用户的等级进行		14.3.2 配置 IIS	392
授权	319	14.3.3 设置服务	393
实验 11-2 使用 AAA 对用户可使用的		14.3.4 系统管理	393
命令进行授权	320	14.3.5 管理拓扑图	395

第 4 部分 高级应用和故障排除篇

实验 A 路由器上配置 DHCP	402
实验 B 策略路由	404
实验 C 路由器 NAT 实验	409
实验 D 网关冗余	411
实验 E 交换端口分析	416

实验 F 配置 QoS	419
实验 G 网络负载均衡	422
实验 H 限制 BT 流量	427
实验 I ARP 攻击的攻、判、防	430





溜客精神：

技術共享，資源共享，資料共享

不求最好，只求較好

做中國較好的網絡安全資料站

300G成套精品教程免费下载

每月网络期刊，黑客期刊发布

请将本站推荐给更多的好友

让大家都成为溜客一员

溜客資料共享群：

访问溜客安全网最下方
查看本站最新共享QQ群

溜客网络安全技术人才培养进行中

做一个通过正道可以养活自己的黑客

从我做起，不做伪黑客

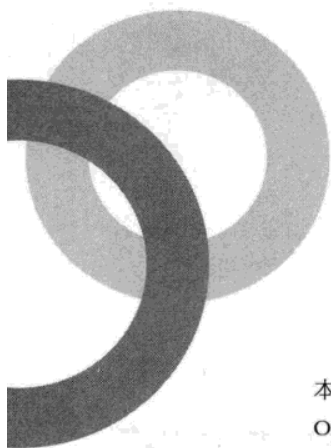
WWW.176KU.COM/VIP.HTM

Part

01

第 1 部分 网络基础篇

要成为一名称职的网络管理员，在进行服务器架设和路由交换配置之前，了解网络的基础知识是非常有必要的，掌握这部分内容有助于后续章节的学习和理解。



第1章 网络基础知识回顾

Chapter 1

古语云：“练武不练功，到老一场空”，学习网络的基础理论就像练功一样重要。本章主要介绍网络的基础、网络的体系结构、ISO/OSI（International Standard Organization/Open System Interconnection，国际标准化组织提出的开放系统互联）参考模型、TCP/IP（Transmission Control Protocol/Internet Protocol，传输控制协议/网际协议），其间穿插大量的实验和技巧，有助于加强读者对理论知识的理解，提高实际应用的能力。通过本章的学习，读者可以掌握无线网卡直接互连的配置，ISO/OSI 参考模型的7层结构以及每一层的功能，TCP/IP参考模型的4层结构以及每一层的功能，Sniffer软件的使用，IP地址的分类、计算、划分、汇总等。

1.1 计算机网络基础

在成为一名好的网络建设者之前，首先要成为一名好的网络使用者，正所谓“用然后知不足”。本节重点讲述计算机网络的功能，并陆续在以后的章节中实现该功能，最后演示无线网卡之间的互连。

1. 计算机网络的产生和发展

1969年12月，DARPA的计算机分组交换网ARPANET投入运行。ARPANET的成功，标志着计算机网络的发展进入了一个新纪元。ARPANET的成功运行使计算机网络的概念发生了根本性的变化。早期的面向终端的计算机网络是以单个主机为中心的星型网，各终端通过传输介质共享主机的硬件和软件资源。但分组交换网则以通信子网为中心，主机和终端都处在网络的边缘。主机和终端构成了用户资源子网。用户不仅共享通信子网的资源，还可以共享用户资源子网中丰富的硬件和软件资源。这种以资源子网为中心的计算机网络通常被称为第二代计算机网络。

在第二代计算机网络中，多台计算机通过通信子网构成一个有机的整体，既分散又统一，从而使整个系统性能大大提高；原来单一主机的负载可以分散到全网的各个机器上，使得网络系统的响应速度加快；而且在这种系统中，单机故障也不会导致整个网络系统的全面瘫痪。在网络中，相互通信的计算机必须协调工作，而这种“协调”是相当复杂的。为了降低网络设计的复杂性，

早在当初设计 ARPANET 时就有专家提出了层次模型。分层设计方法可以将庞大而复杂的问题转化为若干较小且易于处理的子问题。

有了网络体系结构,一个公司所生产的各种机器和网络设备就可以非常容易被连接起来。但由于各个公司的网络体系结构是各不相同的,所以不同公司之间的网络不能互连互通。针对上述情况,国际标准化组织于 1977 年设立了专门的机构研究来解决上述问题,并于不久后提出了一个使各种计算机能够互连的标准框架——开放系统互联参考模型 (Open System Interconnection/Reference Model, OSI/RM), 简称 OSI。OSI 模型是一个开放体系结构,它将网络分为 7 层,并规定每层的功能。OSI 参考模型的出现,意味着计算机网络发展到第三代。在 OSI 参考模型推出后,网络的发展道路一直走标准化道路,而网络标准化的最大体现就是 Internet 的飞速发展。现在 Internet 已成为世界上最大的国际性计算机互联网。Internet 遵循 TCP/IP 参考模型,由于 TCP/IP 仍然使用分层模型,因此 Internet 仍属于第三代计算机网络。如今,计算机网络从体系结构到实用技术已逐步走向系统化、科学化和工程化。

2. 计算机网络的功能

计算机网络自 20 世纪 60 年代末诞生以来,以异常迅猛的速度发展,并被越来越广泛地应用于政治、经济、军事、生产及科学技术的各个领域。计算机网络的主要功能包括如下几个方面。

(1) 信息通信。现代社会信息量激增,信息交换也日益增多,每年有几万吨纸质信件要传递。利用计算机网络传递信件则是一种全新的电子传递方式。电子邮件比现有的通信工具有更多的优点,它不像电话需要通话者同时在场,也不像广播系统只是单方向传递信息,而且在速度上比传统邮件快得多。另外,电子邮件还可以携带声音、图像和视频,实现多媒体通信。本书将在第 2 部分介绍如何在 Windows 环境下搭建邮件服务器。

(2) 资源共享。在计算机网络中,有许多昂贵的资源,如大型数据库和巨型计算机等,并非为每一用户所拥有,所以必须实行资源共享。资源共享包括硬件资源的共享,如打印机和大容量磁盘等,也包括软件资源的共享,如程序和数据等,本书将在第 2 部分介绍如何在 Windows 环境下实现资源共享。资源共享的结果是避免重复投资和劳动,从而提高了资源的利用率,使系统的整体性能价格比得到改善。

(3) 增加可靠性。在一个系统内,当单个部件或计算机暂时失效时,必须通过替换的办法来维持系统的继续运行,这将不可避免地造成服务的中断,而很多关键应用要求提供全天候(365×24)不间断的服务保障。在计算机网络中,每种资源(尤其程序和数据)可以存放在多个地点,用户可以通过多种途径来访问网内的某个资源,从而避免了单点失效对用户产生的影响。本书将在第 2 部分介绍在 Windows 环境下通过编写一个简单批处理文件(只需要 3 行代码),来实现任何时间任何地点任何文件的异机自动备份。

(4) 提高系统处理能力。单机的处理能力是有限的,且由于种种原因(如 CPU),计算机之间的忙闲程度是不均匀的。从理论上讲,在同一网络内的多台计算机可通过协同操作和并行处理来提高整个系统的处理能力,并使网内各计算机负载均衡。本书将在第 4 部分介绍如何实现服务器负载均衡。

(5) VoIP 服务。在 Internet 或 Intranet 上提供语音服务,因为其成本低廉而备受关注。本书将在第 3 部分介绍 VoIP 的相关配置,实现在个人计算机上轻松呼叫异地的语音电话。

(6) 数据的集中管理。计算机网络的另一个主要功能是访问远程数据库,集中处理数据信息,

保证数据库的一致性。现在遍布各地的车票代售点，大街小巷随处可见的银联 POS 机，在提供便利的同时，也维护着数据库的一致性。

(7) 其他功能。网络实时交谈（风靡全球的 MSN、QQ 提供的实时的文字、语音、视频服务已成为人们重要的通信手段）、视频点播、网络游戏（网络上的游戏应用尽有，如军棋、象棋、五子棋等）、网上教学（网上大学、视频下载、作业提交等）、网上书店、网上购物（贴近生活的“淘宝网”）、网上电视直播（PPLive、PPStream、PPMate 等，本书也将在第 2 部分介绍有线电视直播服务器的架设）、网上医院、网上证券交易（大大方便了股民，“炒股”不用再到证券大厅）、网络的远程管理（服务器的远程管理：Windows 2003 提供的远程桌面；设备的远程调试：针对设备的 Telnet、SSH、Web 管理）、虚拟现实以及电子商务正逐渐走进普通百姓的生活、学习和工作中。计算机网络作为信息收集、存储、传输、处理和利用的整体系统，将在信息社会中得到更加广泛的应用。随着网络技术的不断发展，各种网络应用将层出不穷，并将逐渐深入到社会的各个领域及人们的日常生活当中，改变着人们的工作、学习和生活乃至思维的方式。

3. 计算机网络分类

计算机连接所使用的介质可以是双绞线、同轴电缆或光纤等有线介质，也可以是激光、大地微波或卫星微波等无线介质。计算机之间的信息交换具有物理和逻辑上的双重含义。在计算机网络的最底层（物理层），信息交换体现为直接相连的两台机器之间无结构的比特流传输；而在物理层之上的各层所交换的信息便有了一定的逻辑结构，越往上层逻辑结构越复杂，也越接近用户真正需要的形式。信息交换在低层由硬件实现，而到了高层则由软件实现。如果一台计算机带有多台终端和打印机，这种系统通常被称为多用户系统，而不是计算机网络；而由一台主控机带多台从控机构成的系统，是主从式系统，也不是计算机网络。

计算机网络的分类标准很多，比如按拓扑结构、介质访问方式、交换方式以及数据传输速率等，但这些分类标准只给出了网络某一方面的特征，并不能反映网络技术的本质。事实上，确实存在一种能反映网络技术本质的网络划分标准，那就是计算机网络的覆盖范围。按网络覆盖范围的大小，可将计算机网络分为局域网（Local Area Network, LAN）、城域网（Metropolitan Area Network, MAN）、广域网（Wide Area Network, WAN）和互联网（Internet），如表 1-1-1 所示。

表 1-1-1 计算机网络分类

分布距离	覆盖范围	网络种类
10m	房间	局域网
100m	建筑物	局域网
1km	校园	局域网
10km	城市	城域网
100km	国家	广域网
1000km	洲或洲际	互联网

4. 无线网络的特点及连接方式

下面介绍一种新兴的网络——“无线网络”。无线网络是当前国内外的研究热点，无线网络的

研究是由巨大的市场需求驱动的。无线网络有很多优点,如易于安装和使用,可以使用户在任何时间、任何地点接入计算机网络,这一特性使其具有强大的应用前景。但无线网络也有许多不足之处:它的数据传输速率一般比较低,远低于有线网络;无线网络的误码率也比较高,而且站点之间相互干扰比较严重;再就是无线网络的安全问题也需要关注。

用户无线网络的实现有不同的方式。一些咖啡馆、茶馆、宾馆、大学等都安装了无线网络,如南京工业大学就在校园内安装许多无线 AP (Access Point, 接入点),学生坐在树底下也能查看图书馆的资料,这种情况是计算机直接通过无线 AP 接入互联网的。有的计算机通过配置 CDMA 上网卡,可以随时随地访问互联网,目前国内很多区域都提供了 CDMA 上网卡的包年服务。两台笔记本电脑之间还可以通过红外或无线网卡直接进行通信,而不需要有型的传输介质。

值得一提的是,两台计算机之间有线网卡的直接连接会被经常用到,而两台笔记本电脑之间无线网卡的直接连接却常常被忽视。一个错误的理解是,无线网卡只能与无线 AP 连接,而忽略了无线网卡与无线网卡之间也可以直接建立连接。下面举个例子来说明无线网卡的互连。

实验 1-1 通过无线网卡共享 ADSL 上网

家中有两台计算机(笔记本或台式机均可),各配置了一块无线网卡,其中有台计算机还配置了一块有线网卡。一般的笔记本电脑默认都配置了一块有线网卡和一块无线网卡,该实验更常用于笔记本电脑之间。如果只申请了一条 ADSL (Asymmetric Digital Subscriber Line, 非对称数字用户环路),如何实现两台计算机共享上网呢?

最简单经济的实现方法就是,不需购置任何设备,即可实现两台计算机同时上网的目的,下面是具体的操作步骤。

STEP 1 配置 ADSL 上网。把 ADSL 线路接入一台笔记本电脑的有线网卡,鼠标右键单击“网上邻居”,在快捷菜单中选择“属性”,打开“网上邻居”窗口,如图 1-1-1 所示。

单击如图 1-1-1 所示的“新建连接向导”图标,打开“新建连接向导”对话框;单击“下一步”按钮,接下来提示选择“网络连接类型”,这里选择第一个“连接到 Internet”,如图 1-1-2 所示。

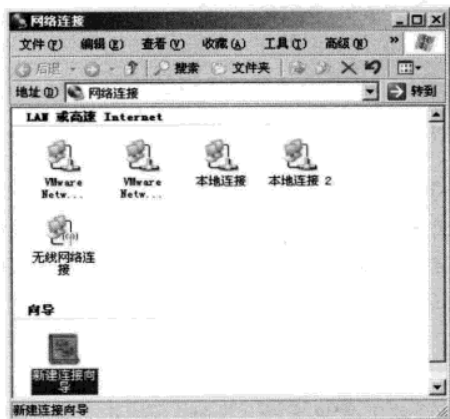


图 1-1-1 网上邻居窗口

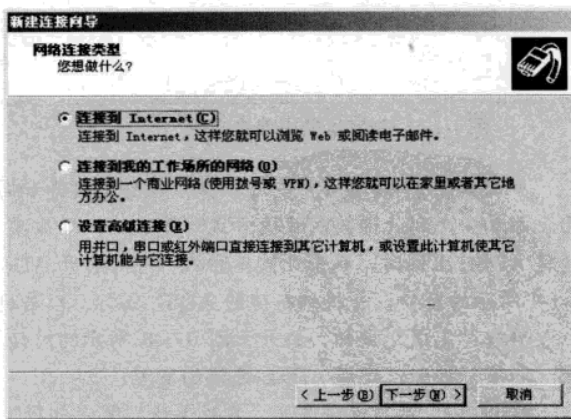


图 1-1-2 选择网络连接类型

单击“下一步”按钮，接下来的对话框中会询问怎样连接到 Internet，选择第二个“用要求用户名和密码的宽带连接来连接”，如图 1-1-3 所示。

单击“下一步”按钮，要求填入 ISP 的名称，这里随意填入一个，如“ADSL”，如图 1-1-4 所示。

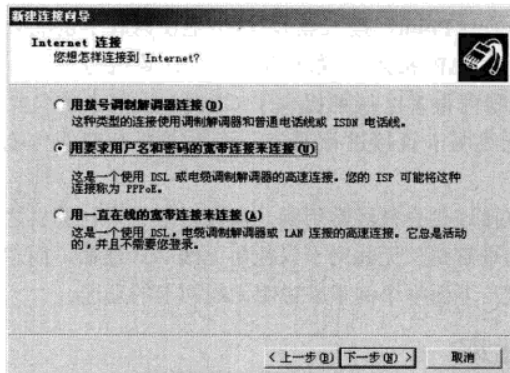


图 1-1-3 选择网络连接方式

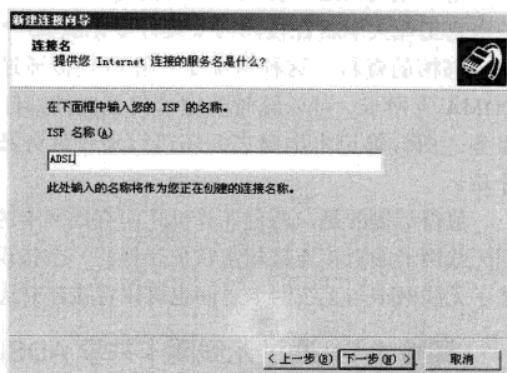


图 1-1-4 设置连接服务名

单击“下一步”按钮，保持默认的“任何人使用”选项，如图 1-1-5 所示。

单击“下一步”按钮，填入有效的 ADSL 用户名和密码，如图 1-1-6 所示。

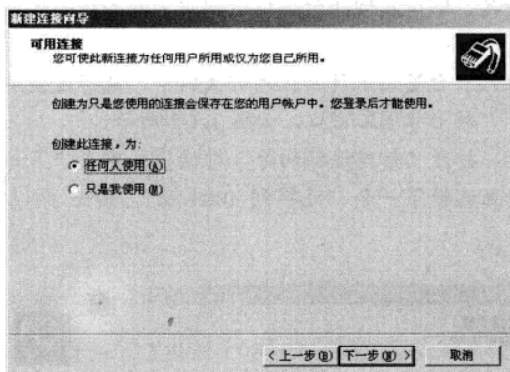


图 1-1-5 指定可使用连接的用户

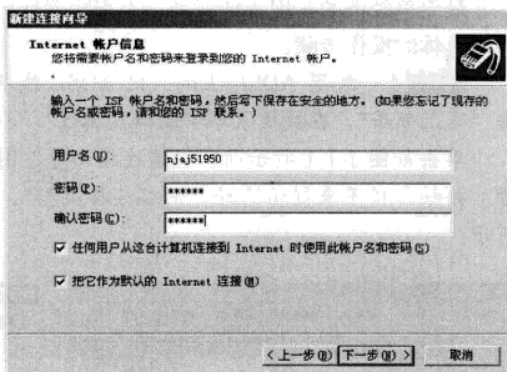


图 1-1-6 填入有效的 ADSL 用户名和密码

单击如图 1-1-6 所示的“下一步”按钮，打开如图 1-1-7 所示的对话框。如果选中“在我的桌面上添加一个到此连接的快捷方式”复选框，那么桌面上会新建一个到此连接的快捷方式，以后通过 ADSL 上网时，双击此快捷方式，即可打开 ADSL 连接；如果没有选中，以后需要打开如图 1-1-1 所示的窗口，并找到新建的 ADSL 图标，双击进行连接。

单击“完成”按钮，打开如图 1-1-8 所示的对话框，提示进行连接。这里暂不进行连接，单击“取消”按钮，完成 ADSL 连接的配置。

STEP 2 启用连接共享。右键单击“网上邻居”，在快捷菜单中选择“属性”，打开“网上邻居”窗口，如图 1-1-9 所示。右键单击刚才建立的“ADSL”连接，在快捷菜单中选择“属性”，

在“ADSL 属性”对话框中，选择“高级”选项卡，打开如图 1-1-10 所示的对话框。选中“允许其他网络用户通过此计算机的 Internet 连接来连接”复选框，在“家庭网络连接”下拉列表中，选择“无线网络连接”，单击“确定”完成配置。

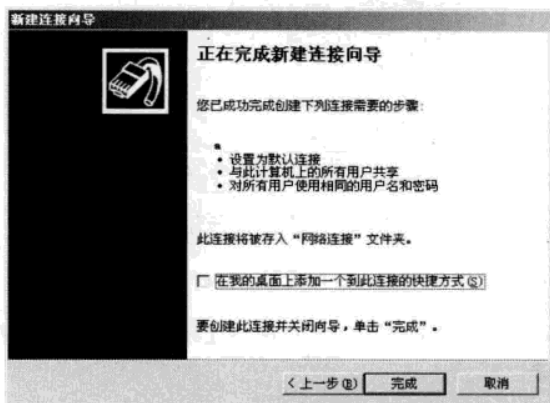


图 1-1-7 完成连接向导

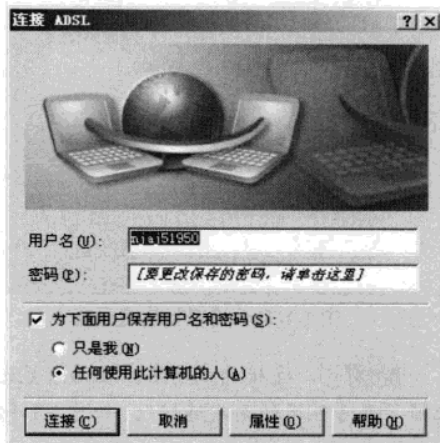


图 1-1-8 连接 ADSL

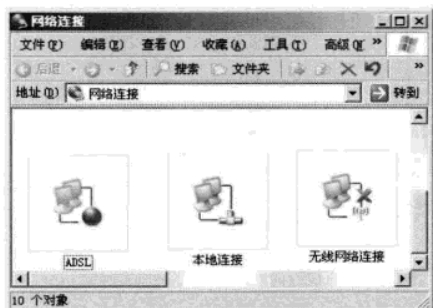


图 1-1-9 网络连接对话框

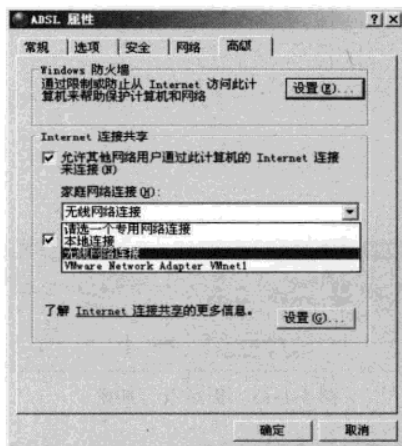


图 1-1-10 设置连接共享

STEP 3 配置无线网卡连接。如图 1-1-9 所示，右键单击“无线网络连接”，在快捷菜单中选择“属性”，打开“无线网络连接属性”对话框，选择“无线网络配置”选项卡，如图 1-1-11 所示。

再单击如图 1-1-11 所示的“添加”按钮，打开如图 1-1-12 所示的对话框。

如图 1-1-12 所示进行操作，添加 SSID 名字，如填入“network-lab”；“网络身份验证”保持默认的“开放式”；“数据加密”选择“已禁用”，选中“这是一个计算机到计算机（特定的）网络”；没有使用“无线访问点”复选框，单击“确定”按钮，此时会提示不加密可能会不安全，如图 1-1-13 所示。由于是作为家庭共享上网使用，这里继续单击“仍然继续”按钮，完成无线网卡配置。

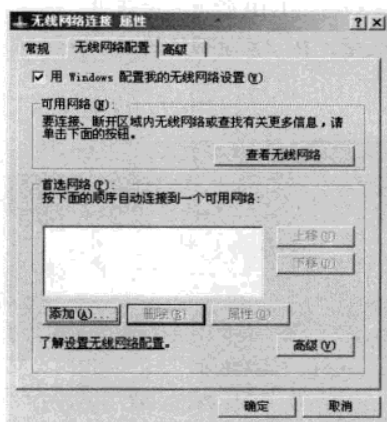


图 1-1-11 设置无线网卡属性

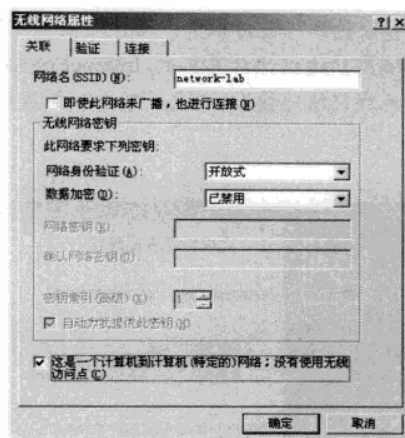


图 1-1-12 添加 SSID

STEP 4 连接无线网络。在两台笔记本电脑上右键单击“无线网络连接”，在快捷菜单中选择“查看可用的无线连接”，如图 1-1-14 所示。

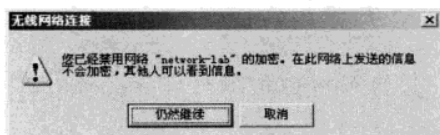


图 1-1-13 提示没有加密

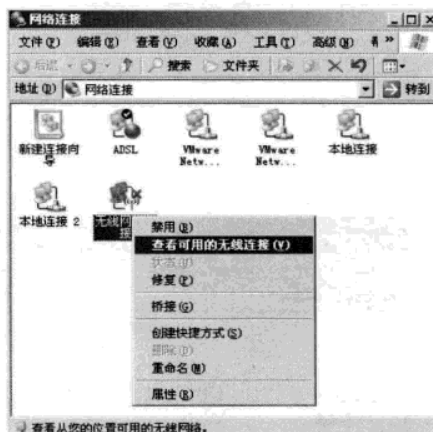


图 1-1-14 搜索无线信号

将可以搜索到无线网络“network-lab”，如图 1-1-15 所示。单击“连接”按钮进行连接，两台笔记本电脑都连接成功后，将提示网络已连接。

STEP 5 配置 IP 地址。连接成功后再配置两台计算机无线网卡对应的 IP 地址，选择有 ADSL 线路的那台笔记本电脑，右键单击“无线网络连接”，在快捷菜单中选择“属性”，打开“无线网络连接 属性”对话框，选中“常规”选项卡中的“Internet 协议 (TCP/IP)”复选框，如图 1-1-16 所示。

单击图 1-1-16 中的“属性”按钮，打开 IP 配置对话框，在“IP 地址”中填入“192.168.0.1”，“子网掩码”中填入“255.255.255.0”，“默认网关”和下面的 DNS 栏中都保留为空，如图 1-1-17 所示。单击“确定”按钮，完成 IP 地址配置。继续配置第二台笔记本电脑的无线网卡，在“IP 地址”中填入“192.168.0.2”，“子网掩码”中填入“255.255.255.0”，“默认网关”中填入“192.168.0.1”，

“首选 DNS 服务器”中填入一个有效 DNS 服务器的 IP 地址，比如“218.2.135.1”。

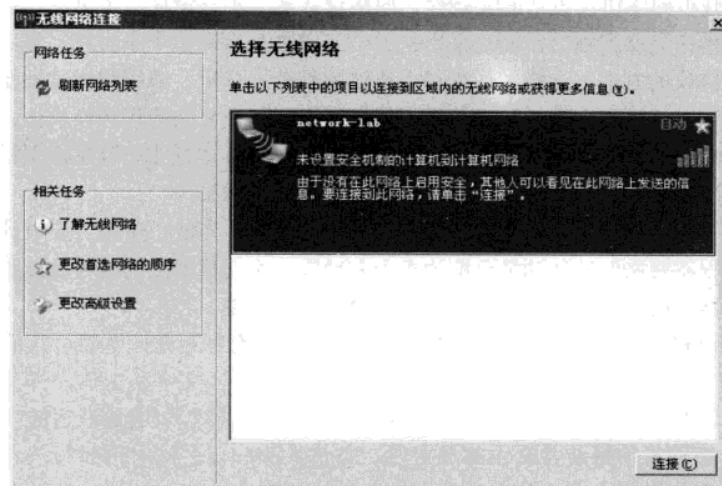


图 1-1-15 无线网卡充当的 AP

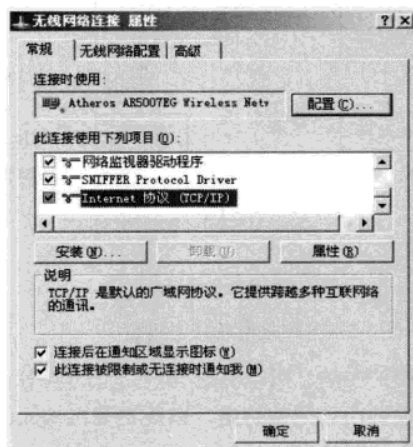


图 1-1-16 无线网络连接属性

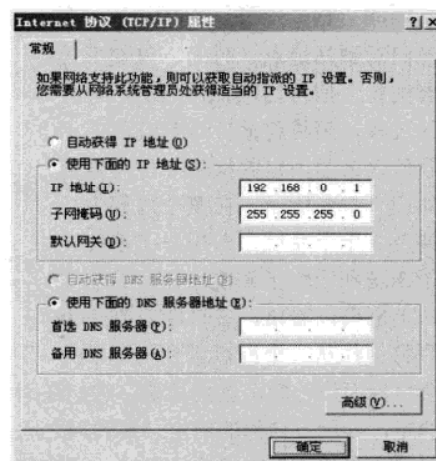


图 1-1-17 配置 IP 地址

经过上述配置，当第一台笔记本电脑 ADSL 连接成功后，则两台笔记本电脑都可以访问 Internet。如果还有第三台有无线网卡的计算机，可以按照第二台笔记本电脑的设置方式进行设置，只需要把 IP 地址设成“192.168.0.3”，其他设置不变。依此类推，仅通过一根 ADSL 线路，可实现很多台有无线网卡的计算机共享上网。

1.2 网络体系结构

两台计算机进行通信时，必须采用相同的信息交换规则。在计算机网络中，用于规定信息的

格式以及发送和接收信息的规则称为**网络协议** (Network Protocol) 或**通信协议** (Communication Protocol)。为了减少网络协议设计的复杂性, 网络设计者并不是设计一个单一、巨大的协议来为所有形式的通信规定完整的细节, 而是采用把通信问题划分为许多个小问题, 然后为每个小问题设计一个单独的协议的方法。这样做使得每个协议的设计、分析、编码和测试都比较容易, 正如编程一样, 通过编写“过程”和“函数”以方便调用, 把一个复杂的程序模块化、简单化。分层模型 (Layering Model) 是一种用于开发网络协议的设计方法。本质上, 分层模型描述了把通信问题分为几个小问题 (称为层次) 的方法, 每个小问题对应于一层。

为了减少网络设计的复杂性, 绝大多数网络采用分层设计方法。所谓分层设计方法, 就是按照信息的流动过程将网络的整体功能分解为多个功能层, 不同机器上的同等功能层之间采用相同的协议, 同一机器上的相邻功能层之间通过接口进行信息传递。

为了便于理解接口和协议的概念, 首先以邮政通信系统为例进行说明。人们平常写信时, 对信件的格式和内容都有约定。写信必须采用双方都懂的语言文字和文体, 开头是对方称谓, 最后是落款等。这样, 对方收到信后, 才可以看懂信中的内容, 知道是谁写的, 什么时候写的等。信写好后, 必须将信封装并交由邮局寄发, 寄信人和邮局之间对信封写法和邮票的贴法也有约定。在中国寄信必须先写收信人地址、姓名, 然后再写寄信人的地址和姓名。邮局收到信后, 首先进行信件的分拣和分类, 然后交付有关运输部门进行运输, 如航空信交民航、平信交铁路运输或公路运输等。这时, 邮局和运输部门对到站地点、时间、包裹形式等也有约定。信件运送到目的地后进行相反的过程, 最终将信件送到收信人手中, 收信人依照约定的格式才能读懂信件。如图 1-2-1 所示, 在整个过程中, 主要涉及 3 个子系统, 即用户子系统、邮政子系统和运输子系统。

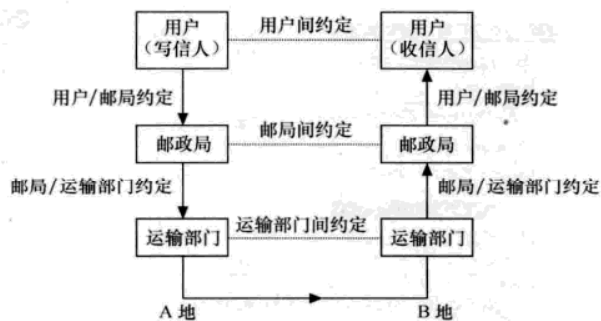


图 1-2-1 邮政系统分层模型

从上例可以看出, 各种约定都是为了达到将信件从一个源点送到一个目的点这个目标而设计的, 这就是说, 它们是因信息的流动而产生的。可以将这些约定分为同等机构间的约定, 如用户之间的约定、邮政局之间的约定和运输部门之间的约定, 以及不同机构间的约定, 如用户与邮政局之间的约定以及邮政局与运输部门之间的约定。

虽然两个用户、两个邮政局和两个运输部门分处甲、乙两地, 但它们都分别对应同等机构, 同属一个子系统; 而同处一地的不同机构则不在一个子系统内, 它们之间的关系是服务与被服务的关系。很显然这两种约定是不同的, 前者为部门内部的约定, 而后者是不同部门之间的约定。在计算机网络环境中, 两台计算机中两个进程之间进行通信的过程与邮政通信的过程十分相似。

为了减少计算机网络设计的复杂性, 人们往往按功能将计算机网络划分为多个不同的功能层。网络中同等功能层之间的通信规则就是该层使用的协议, 如有关第 N 层的通信规则的集合, 就是第 N 层的协议。而同一计算机不同功能层之间的通信规则称为接口 (Interface), 在第 N 层和第 $(N+1)$ 层之间的接口称为 $N/(N+1)$ 层接口。总的来说, 协议是不同机器同等功能层之间的通信约定, 而接口是同一机器相邻功能层之间的通信约定。不同的网络, 分层数量、各层的名称和功能以及协议都各不相同。然而, 在所有的网络中, 每一层的目的都是向它的上一层

提供一定的服务。

协议层次化不同于程序设计中模块化的概念。在程序设计中，各模块可以相互独立，任意拼装或者并行，而层次则一定有上下之分，它是依数据流的流动而产生的。组成不同计算机同等功能层的实体称为对等进程。对等进程不一定必须是相同的程序，但其功能必须完全一致，且采用相同的协议。

分层设计方法将整个网络通信功能划分为垂直的层次集合后，在通信过程中，下层将向上层隐藏下层的实现细节。但层次的划分应首先确定层次的集合及每层应完成的任务。划分时应按逻辑组合功能，并具有足够的层次，以使每层小到易于处理。同时层次也不能太多，以免产生难以负担的处理开销。

计算机网络体系结构是网络中分层模型以及各层功能的精确定义。对网络体系结构的描述必须包括足够的信息，使实现者可以为每一功能层进行硬件设计或编写程序，并使之符合相关协议。需要注意的是，网络协议实现的细节不属于网络体系结构的内容，因为它们隐含在机器内部，对外部说来是不可见的。

1.3 ISO/OSI 参考模型

上一节对协议分层和网络体系结构进行了概述。接下来，本节介绍一些具体的网络体系结构，首先介绍一个重要的网络体系结构，即 OSI 参考模型。

在网络发展初期，许多研究机构、计算机厂商和公司都大力发展计算机网络。从 ARPANET 出现至今，已经推出了许多商品化的网络系统。这种自行发展的网络，在体系结构上差异很大，以至于它们之间互不相容，难于相互连接以构成更大的网络系统。为此，许多标准化机构积极开展了网络体系结构标准化方面的工作，其中最为著名的就是国际标准化组织 ISO 提出的开放系统互连 OSI 参考模型。OSI 参考模型是研究如何把开放式系统（即为了与其他系统通信而相互开放的系统）连接起来的标准。

OSI 参考模型将计算机网络分为 7 层，如图 1-3-1 所示。下面将从最底层开始，依次介绍模型的各层所要完成的功能。

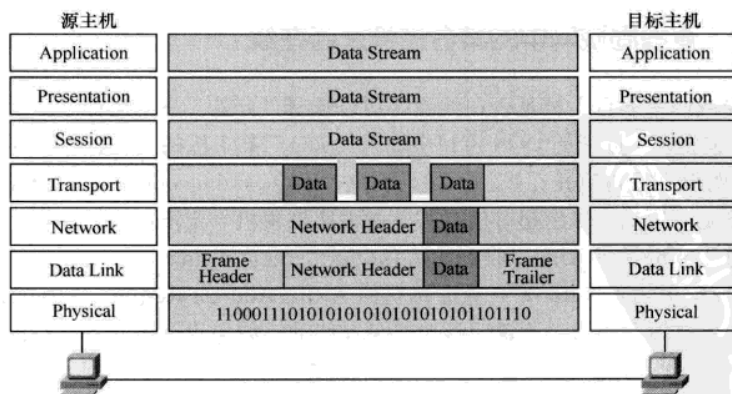


图 1-3-1 OSI 七层模型

1. 物理层

物理层 (Physical Layer) 的主要功能是完成相邻节点之间原始比特流的传输。物理层协议关心的典型问题是, 使用什么样的物理信号来表示数据“1”和“0”, 一位持续的时间多长, 数据传输是否可同时在两个方向上进行, 最初的连接如何建立以及完成通信后连接如何终止, 物理接口 (插头和插座) 有多少针以及各针的用处。物理层的设计主要涉及物理层接口的机械、电气、功能和过程特性, 以及物理层接口连接的传输介质等问题。物理层的设计还涉及通信工程领域内的一些问题。物理层常用的网络设备有中继器 (Repeater) 和集线器 (Hub)。

2. 数据链路层

数据链路层 (Data Link Layer) 的主要功能是在不可靠的物理线路上进行数据的可靠传输。数据链路层完成的是网络中相邻节点之间可靠的数据通信。为了保证数据的可靠传输, 发送方把用户数据封装成帧 (Frame), 并按顺序传送各帧。由于物理线路的不可靠, 因此发送方发出的数据帧有可能在线路上发生出错或丢失, 从而导致接收方不能正确接收到数据帧。为了保证能让接收方对接收到的数据进行正确性判断, 发送方为每个数据分块计算出 CRC (Cyclic Redundancy Check, 循环冗余校验), 并把 CRC 添加到帧中, 这样接收方就可以通过重新计算 CRC 来判断数据接收的正确性。一旦接收方发现接收到的数据有错, 则发送方必须重传这一帧数据。然而, 相同帧的多次传送也可能使接收方收到重复的帧。例如, 接收方给发送方的“确认帧”被破坏后, 发送方也会重传上一帧, 此时接收方就可能接收到重复帧。数据链路层必需解决由于帧的损坏、丢失和重复所带来的问题。

数据链路层要解决的另一个问题是, 防止高速发送方的数据把低速接收方“淹没”。因此需要某种信息流量控制机制使发送方得知接收方当前还有多少缓存空间。为了控制的方便, 流量控制常常和差错处理一同实现。

在局域以太网中, 数据链路层通过 MAC (Media Access Control, 介质访问控制) 地址负责主机之间数据的可靠传输。数据链路层的设备必须能识别出数据链路层的地址, 如局域网交换机能构造 MAC 地址表, 基于 MAC 地址进行数据转发; 网卡本身具有 MAC 地址, 能根据 MAC 地址判断数据包是否是发往本机的数据包。网桥、交换机和网卡都属于数据链路层的设备。

实验 1-2 查看局域网中的某台主机是否在线

如何查看局域网中某台主机是否在线呢? 可以选择“开始”→“运行”命令, 输入“cmd”后单击“确定”按钮, 在打开的 DOS 窗口中输入“ping 某主机的 IP 地址”。如果收到“Reply from ...”, 则说明该主机肯定是在线的; 如果收到“Request time out”, 是否能说明该主机一定不在线呢? 回答是否定的, 收到超时信息并不能说明该主机一定不在线, 因为如果该主机运行防火墙软件, 禁止 ping 命令回应, 收到的信息也是“Request time out”。ping 执行完以后, 可以通过在 DOS 窗口中输入“arp -a”, 查看本机的 ARP (Address Resolution Protocol, 地址解析协议) 缓存, 如果有缓存条目, 则说明该主机是在线的, 如果没有缓存条目, 则说明该主机不在线。

为了更形象地说明这个问题, 请参照图 1-3-2。第一次执行“ping 192.168.1.220 -n 1”命令,

尝试去 ping 192.168.1.220 这个 IP 地址, 其中的“-n 1”是 ping 命令的参数, 表示只 ping 一个数据包, ping 命令默认发送的是 4 个包。结果收到了 192.168.1.220 的应答包, “Reply from 192.168.1.220: bytes=32 time<1ms TTL=128”, 其中“byte=32”表示收到的字节数, ping 的应答包默认大小是 32 字节; “time<1ms”, 表示从发出 ping 包到收到应答, 花费的时间小于 1ms, 这个值可以用来简单地判断网络的健康状况; “TTL=128”, TTL 表示生存周期, 每经过一台路由器, 这个值至少减 1。这个值和具体的操作系统以及从 ping 的源主机到 ping 的目标主机之间经过的路由器数量也有关, 因不同的操作系统默认的初始值不同, 可能的初始值是 64、128、255。假如操作系统的默认初始值是 128, 则上面的结果表示, 没有经过任何一台路由器就到达目标了, 假如操作系统的默认值是 255, 则经过的路由器可能就是 $255-128=127$, 这是不可能的情况, 因为 Internet 上没有任何两台主机之间的路由器会达到这个数值。

确定源和目标之间的路由器数量, 可使用“tracert”命令, 如图 1-3-3 所示。使用 ping 命令测试从 www.263.net 返回的包的 TTL (Time To Live, 生存时间) 是 49, 源主机和 www.263.net 主机之间经过的路由器数量大概是 $64-49=15$, 说“大概”是因为每经过一台路由器, TTL 至少减 1, 有时减的不止是 1, 这和具体的网络有关。接下来使用 tracert 命令测试。其中“-d”是附加参数, 如果不加这个参数, tracert 命令执行的速度会比较慢, 因为计算机尝试把每台路由器的 IP 地址解析成域名, 这会花很多的时间, 而且意义不大。“-d”参数表示计算机不执行 IP 到域名的反向解析, 这会大大加快执行速度。结果显示, 经过 14 台路由器到达目标, 第 15 跳已经是目标地址了。由此可见, ping 命令中的 TTL 可以用来粗略判断源主机和目标主机之间经过的路由器的数量, ping 只能测试计算机的连通情况, 无法定位到中间出故障的某一台路由器上, 而 tracert 可以更准确地

```

C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>ping 192.168.1.220 -n 1
Pinging 192.168.1.220 with 32 bytes of data:
Reply from 192.168.1.220: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.1.220:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\Documents and Settings\Administrator>ping 192.168.1.3 -n 1
Pinging 192.168.1.3 with 32 bytes of data:
Request timed out.
Ping statistics for 192.168.1.3:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),
C:\Documents and Settings\Administrator>ping 192.168.1.4 -n 1
Pinging 192.168.1.4 with 32 bytes of data:
Request timed out.
Ping statistics for 192.168.1.4:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),
C:\Documents and Settings\Administrator>arp -a
Interface: 192.168.1.200 --- 0x3
Internet Address      Physical Address      Type
192.168.1.3           00-8c-29-76-7c-56    dynamic
192.168.1.220         00-16-35-00-ff-5c    dynamic
C:\Documents and Settings\Administrator>

```

图 1-3-2 测试主机是否在线

```

D:\>ping www.263.net -n 1
Pinging www.263.net [211.150.96.51] with 32 bytes of data:
Reply from 211.150.96.51: bytes=32 time=89ms TTL=49
Ping statistics for 211.150.96.51:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 89ms, Maximum = 89ms, Average = 89ms
D:\>tracert www.263.net -d
Tracing route to www.263.net [211.150.96.51]
over a maximum of 30 hops:
  0  <1 ms  <1 ms  <1 ms  210.28.203.1
  1  24 ms  25 ms  26 ms  10.255.20.2
  2  34 ms  32 ms  32 ms  192.168.3.1
  3  39 ms  43 ms  42 ms  218.2.134.149
  4  32 ms  31 ms  28 ms  218.2.132.13
  5  32 ms  35 ms  37 ms  221.231.206.213
  6  36 ms  37 ms  34 ms  221.231.191.193
  7  40 ms  43 ms  45 ms  221.231.191.177
  8  63 ms  66 ms  68 ms  202.97.41.189
  9  88 ms  87 ms  84 ms  202.97.34.73
 10  90 ms  91 ms  90 ms  219.141.131.54
 11  90 ms  92 ms  89 ms  219.142.9.102
 12  88 ms  91 ms  90 ms  211.150.127.18
 13  90 ms  87 ms  87 ms  211.150.125.54
 14  88 ms  86 ms  86 ms  211.150.96.51
Trace complete.
D:\>

```

图 1-3-3 tracert 命令

定位到某台出故障的路由器上。

开启计算机“192.168.1.3”的防火墙。在计算机“192.168.1.3”上，右键单击“网上邻居”，在快捷菜单中选择“属性”，打开“网络连接”窗口，右键单击“本地连接”，在快捷菜单中选择“属性”，如图 1-3-4 所示。

在打开的“本地连接 属性”对话框中，选择“高级”选择卡，选中“通过限制或阻止……”复选框，启用计算机的防火墙，如图 1-3-5 所示。



图 1-3-4 设置以太网卡属性

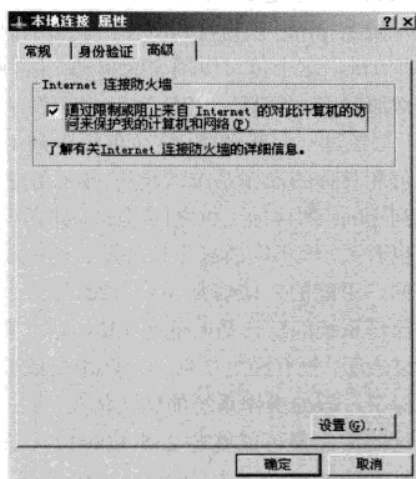


图 1-3-5 启用防火墙

在计算机“192.168.1.3”上启用防火墙后，如图 1-3-2 所示，ping 192.168.1.3 时，收到了超时的提示，原因是防火墙阻止了 ping 包。再 ping 一个不存在的 IP 地址“192.168.1.4”，也收到了超时的提示，如何准确判断出哪一个 IP 地址是在线的呢？图 1-3-2 中所示的“arp -a”命令用来显示本机保存的 ARP 缓存，可以看到两个条目“192.168.1.220”和“192.168.1.3”，却没有看到“192.168.1.4”的条目，由此可以判断“192.168.1.220”和“192.168.1.3”主机在线，“192.168.1.4”主机不在线。由此也可以得知，防火墙对 ARP 是阻止不了的。IPv4 中，针对局域网的 ARP 攻击危害巨大，很难防御，本书第 4 部分通过分析 ARP 攻击原理，具体介绍一些防御攻击的切实可行的解决办法。

3. 网络层

网络层（Network Layer）的主要功能是完成网络中主机间的报文传输。在广域网中，这包括产生从源端到目的端的路由，根据采用的路由协议，选择最优的路径，本书将在第 3 部分介绍路由的相关知识。

当报文不得不跨越两个或多个网络时，又会产生很多新问题。例如，第二个网络的寻址方法可能不同于第一个网络，第二个网络也可能因为第一个网络的报文太长而无法接收，两个网络使用的协议也可能不同。网络层必须解决这些问题，使异构网络能够互连。

网络层涉及的协议有 IP、IPX 等，网络层的设备必须能识别出网络层的地址，如路由器、三层交换机等都可以根据 IP 地址做路径选择，它们都属于网络层设备。

实验 1-3 查看 ADSL 上网获取到的 IP 地址

如图 1-1-17 所示, 查看给计算机静态分配的 IP 地址。如果通过 ADSL 上网, 计算机将会动态获取到一个 IP 地址, 如何查看获取的 IP 地址呢?

可以在 DOS 窗口中执行 “ipconfig” 命令, 查看计算机静态分配的 IP 地址或动态获取的 IP 地址、使用 “ipconfig /all” 命令除了可以查看计算机的 IP 地址外, 还可以查看计算机网卡的 MAC 地址, 以及 DNS 服务器地址。如图 1-3-6 所示, ADSL 显示的结果与图 1-3-6 所示类似, 但 IP 地址是动态获取的。

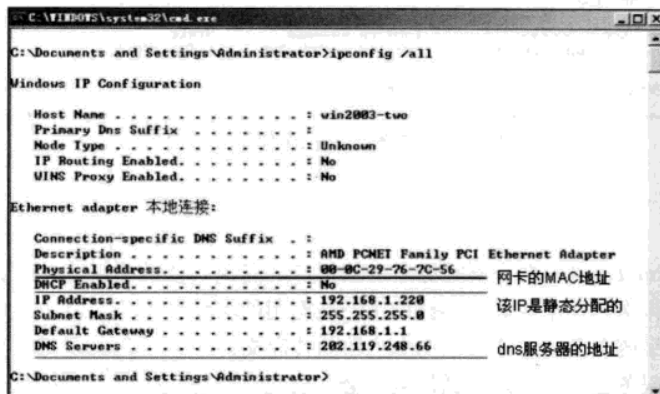


图 1-3-6 查看 IP 地址

4. 传输层

传输层 (Transport Layer) 的主要功能是完成网络中不同主机上的用户进程之间可靠的数据通信。最好的传输连接是一条无差错的、按顺序传送数据的管道, 即传输层的连接是真正端到端的连接。换言之, 源端主机上的某进程是利用报文头和控制报文与目标主机上的对等进程进行对话。

由于绝大多数主机都支持多任务操作, 因而机器上有多个进程, 这意味着多条连接将进出主机, 因此需要以某种方式区别报文属于哪条连接。识别这些连接的信息可以放入传输层的报文头中。除了将几个报文流多路复用到一条通道上, 传输层还必须管理跨网连接的建立和拆除。这就需要某种命名机制, 使机器内的进程能够说明它希望交谈的对象。另外, 还需要有一种机制来调节信息流, 使高速主机不会过快地向低速主机传送数据。

传输层相关的协议有 TCP、UDP (User Datagram Protocol, 用户数据报协议), 它们涉及服务使用的端口号, 主机根据端口号识别服务 (常用的 WWW 服务端口号是 80, FTP 服务端口号是 21 等) 和区分会话 (源 IP、源端口号、目标 IP、目标端口号, 四者共同唯一标识一个会话)。对一些常用的服务, 在文件 “C:\WINDOWS\system32\drivers\etc\services” 中记录了服务名、所使用的协议 (TCP 或 UDP)、默认端口号。

实验 1-4 查看服务使用的端口号

对一些不常使用或用户自己开发的服务程序, 用户可以先建立到服务端的连接, 然后在 DOS

窗口中输入命令“netstat -n”，查看服务所对应的端口号。此方法也适用于一些常用服务。先连接主机“192.168.1.220”的远程桌面（有关远程桌面的使用，本书将在第 2 部分介绍），然后执行“netstat”命令来查看远程桌面所使用的协议和端口号，如图 1-3-7 所示。可以看出远程桌面使用的协议是 TCP，本地主机的 IP 地址是 192.168.1.200，使用的端口号是 1756，该端口号是一个大于 1024（包括 1024）以上的随机值；外部主机的 IP 地址是 192.168.1.220，端口号是 3389，3389 是远程桌面默认使用的端口号。

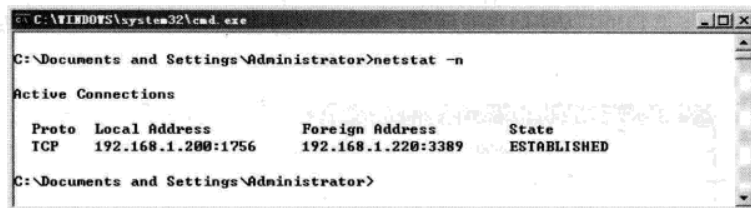


图 1-3-7 查看服务程序使用的端口

5. 会话层

会话层（Session Layer）允许不同机器上的用户之间建立会话关系。会话层允许进行类似传输层的普通数据的传送，在某些场合还提供了一些有用的增强型服务。会话层允许用户利用一次会话在远端的分时系统上登录，或者在两台机器间传递文件。

会话层提供的服务之一是管理对话控制。会话层允许信息同时双向传输，或任一时刻只能单向传输。如果属于后者，则类似于物理信道上的半双工模式，会话层将记录此时该轮到哪一方传输数据。一种与对话控制有关的服务是令牌管理（Token Management）。有些协议保证双方不能同时进行同样的操作，这一点很重要。为了管理这些活动，会话层提供了令牌，令牌可以在会话双方之间移动，只有持有令牌的一方可以执行某种关键性操作。另一种会话层服务是同步。如果在平均每小时出现一次大故障的网络上，两台机器间要进行一次两小时的文件传输，则会出现严重的问题。每一次传输中途失败后，都不得不重新传送这个文件。当网络再次出现大故障时，可能又会半途而废。为了解决这个问题，会话层提供了一种方法，即在数据中插入同步点。每次网络出现故障后，仅仅重传最后一个同步点以后的数据。

6. 表示层

表示层（Presentation Layer）完成某些特定的功能，对这些功能，人们常常希望找到普遍的解决办法，而不必由每个用户自己来实现。值得一提的是，表示层以下各层只关心从源主机到目标主机可靠地传送比特，而表示层关心的是所传送信息的语法和语义。表示层服务的一个典型例子是用一种大家一致选定的标准方法对数据进行编码。

网络上计算机可能采用不同的数据表示，所以需要在数据传输时进行数据格式的转换。例如，在不同的机器上常用不同的代码来表示字符串（ASCII 和 EBCDIC）、整型数（二进制反码或补码）以及机器字的不同字节顺序等。为了让采用不同数据表示法的计算机之间能够相互通信并交换数据，在通信过程中使用抽象的数据结构来表示传送的数据，而在机器内部仍然采用各自的标准编码。管理这些抽象数据结构，并在发送方将机器的内部编码转换为适合网络上传输的传送语法，

以及在接收方做相反的转换等，都是由表示层来完成的。

另外，表示层还涉及数据压缩和解压、数据加密和解密等工作。

7. 应用层

网络的目的在于支持运行于不同计算机的进程之间的通信，而这些进程则是为用户完成不同任务而设计的。应用层（Application Layer）包含大量人们普遍需要的协议，如 HTTP（Hyper Text Transfer Protocol，超文本传输协议）、FTP（File Transfer Protocol，文件传输协议）、SMTP（Simple Message Transfer Protocol，简单邮件传输协议）、DNS（Domain Name Service，域名解析服务）等。

对于需要通信的不同应用来说，应用层的协议都是必需的。例如，当某个用户想要获得远程计算机上的一个文件拷贝时，要向本机的文件传输软件发出请求，这个软件与远程计算机上的文件传输进程通过文件传输协议进行通信，这个协议主要处理文件名、用户许可状态和其他请求细节的通信。远程计算机上的文件传输进程使用其他特征来传输文件内容。

由于每个应用有不同的要求，应用层的协议集在 ISO/OSI 模型中并没有定义，但是有些确定的应用层协议，包括虚拟终端、文件传输和电子邮件等，都可作为标准化的候选。值得注意的是，OSI 模型本身不是网络体系结构的全部内容，这是因为它并未确切地描述用于各层的协议和实现方法，而仅仅规定每一层应该完成的功能。不过，ISO 已经为各层制定了相应的标准，但这些标准并不是模型的一部分，它们是作为独立的国际标准被发布。

在 OSI 参考模型中，有 3 个基本概念：服务、接口和协议。OSI 模型的最重要的贡献是将这 3 个概念区分清楚。

OSI 参考模型是在其协议开发之前设计出来的。这意味着 OSI 模型不是基于某个特定的协议集而设计的，因而它更具有通用性。但另一方面，也意味着 OSI 模型在协议实现方面存在某些不足。实际上，OSI 协议过于复杂，这也是 OSI 从未真正流行开来的原因所在。

虽然 OSI 模型和协议并未获得巨大的成功，但是 OSI 参考模型在计算机网络的发展过程中仍然起到了非常重要的指导作用，作为一种参考模型和完整体系，它仍对今后计算机网络技术标准化、规范化方向发展具有指导意义。接下来介绍目前广泛使用的 TCP/IP。

1.4 TCP/IP

TCP/IP 是目前最成功、使用最频繁的互连协议。虽然现在已有许多协议都适用于互联网，但只有 TCP/IP 最突出，因为它在网络互连中用得最为广泛。

1.4.1 TCP/IP 参考模型

TCP/IP 参考模型是 4 层结构，下面结合 Sniffer 软件来介绍 TCP/IP 模型的 4 层结构。

实验 1-5 使用 Sniffer 软件监控网络

Sniffer 软件是 NAI 公司推出的功能强大的协议分析软件，具有捕获网络流量进行详细分析、实时监控网络活动、利用专家分析系统诊断问题、收集网络利用率和错误等功能。Sniffer 的工作

方式就是通过将网卡置为混杂模式,对网卡上接收到的数据包进行侦听、捕获和分析。这里需要注意,只有网卡收到的包才会被捕获,如在集线器的环境中,Sniffer 能捕获到所有的包;而在交换环境中,Sniffer 仅仅只能捕获到流经本网卡的包,包括广播包和本主机发送及接收的包,其他主机间的通信将捕获不到。但通过使用某些方法也可以捕获其他主机间的通信,如进行 ARP 欺骗或在交换机端口上进行端口镜像,这些技术在后面会陆续介绍。从“<http://www.router.net.cn/network.rar>”或“<http://blcui.njut.edu.cn/network.rar>”下载压缩包,该压缩包中包括了本书使用到的所有软件。有关 Sniffer 的安装,请参考软件包中的“补充资料\1Sniffer 软件的安装.pdf”,下面简单介绍 Sniffer 的几个常用功能。

(1) 实时监控网络。

STEP 1 启动 Sniffer 后,单击 Sniffer 中的“Matrix”(矩阵)图标,如图 1-4-1 中箭头所指。

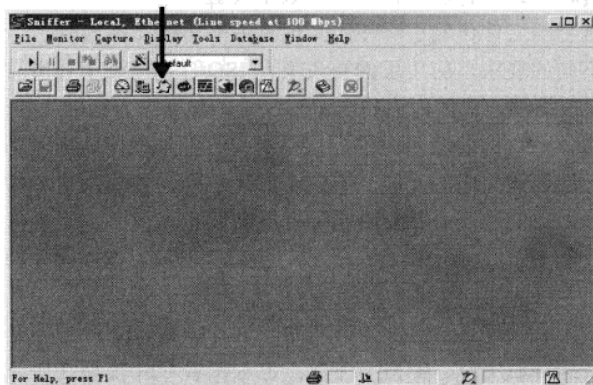


图 1-4-1 Sniffer 监控网络

这里显示网卡接收到的数据包,默认是以 MAC 地址的形式显示,如图 1-4-2 所示。

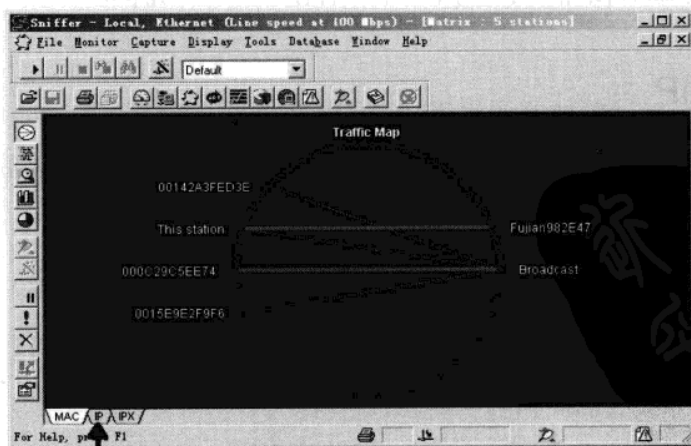


图 1-4-2 监控 MAC 地址发送的数据包

STEP 2 数据包以 MAC 地址形式显示时,感觉不是很直观。单击如图 1-4-2 所示的“IP”选项卡(如箭头所指),将会以 IP 的形式显示网卡收到的数据包,从这里可以直观地看出每个 IP 发送数据包的情况,如图 1-4-3 所示。

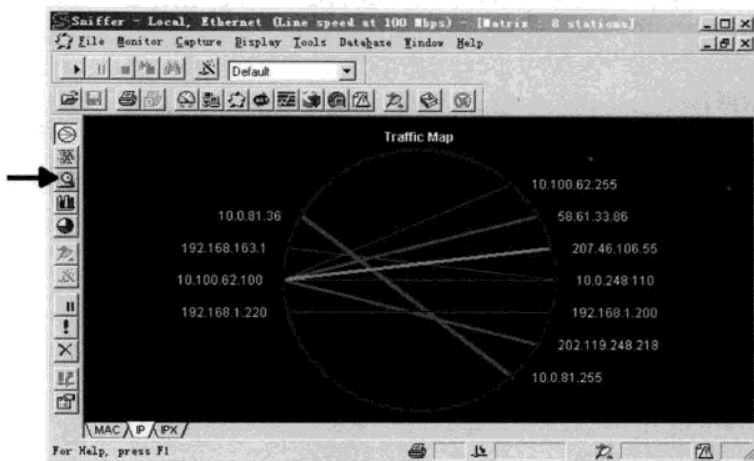


图 1-4-3 监控 IP 地址发送的数据包

注意



如果连接到一个新的网络环境,在查询该网络使用的 IP 地址段时,那么可以使用该功能。如图 1-4-3 所示,捕获的包中可以显示该网段使用的 IP 地址,至于子网掩码,一般局域网中使用的都是 255.255.255.0,网关一般都是 1 或 254, DNS 可以随便配置。

STEP 3 单击如图 1-4-3 所示的“Detail”图标(如箭头所指),查看报文的详细情况。如图 1-4-4 所示,单击标题栏(箭头所指的那一行)中的“Protocol”、“Host 1”、“Packets”、“Bytes”、“Bytes”、“Packets”、“Host 2”等,可以分别实现以该列进行升序/降序排列。

Protocol	Host 1	Packets	Bytes	Bytes	Packets	Host 2
HTTP	10.100.62.100	41	9,077	8,463	22	207.46.106.44
	10.100.62.39	0	0	229	1	10.100.62.100
	10.100.62.100	1	255	0	0	10.100.62.255
NetBIOS_DGM_U	192.168.1.220	16	3,868	0	0	192.168.1.255
	10.100.62.25	1	247	0	0	
	10.100.62.39	5	1,208	0	0	10.100.62.255
	10.100.62.100	1	96	0	0	
	10.100.62.39	1	108	0	0	10.100.62.100
NetBIOS_NS_U	192.168.1.220	33	3,600	0	0	192.168.1.255
	10.100.62.39	361	34,925	0	0	10.100.62.255
	10.100.62.100	6	296	0	0	10.0.248.110
NetBIOS_SSN_T	192.168.163.1	5	330	0	0	
	10.100.62.39	4	256	0	0	224.0.0.22
Others	10.100.62.100	16	3,070	1,368	9	202.119.248.218
		6	462	0	0	10.0.248.110
	10.100.62.39	3	537	0	0	239.255.255.250

图 1-4-4 查看数据包的详细情况

注意



如果局域网是通过交换机互连的, 要捕获局域网中所有与外部通信的包, 则可以配置端口镜像, 把上连端口的包镜像到连接 Sniffer 主机的交换机端口, 详见第 4 部分的实验 E 交换端口分析。

(2) 捕获数据包。

STEP 1 在 Sniffer 中单击 “Start” 按钮, 启动数据包捕获, 如图 1-4-5 所示。

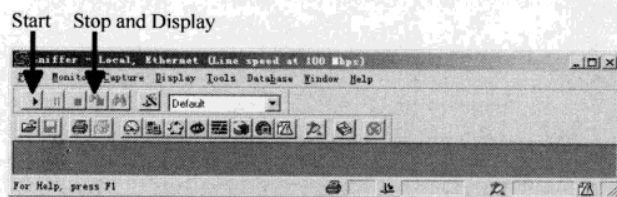


图 1-4-5 Sniffer 捕数据包

STEP 2 在计算机的 IE 浏览器的地址栏中输入 <http://www.njut.edu.cn>, 访问南京工业大学主页。

STEP 3 在图 1-4-5 中, “Stop and Display” 按钮变亮, 表示已经捕获到数据包了。单击此按钮停止捕获并显示数据包, 如图 1-4-6 所示。

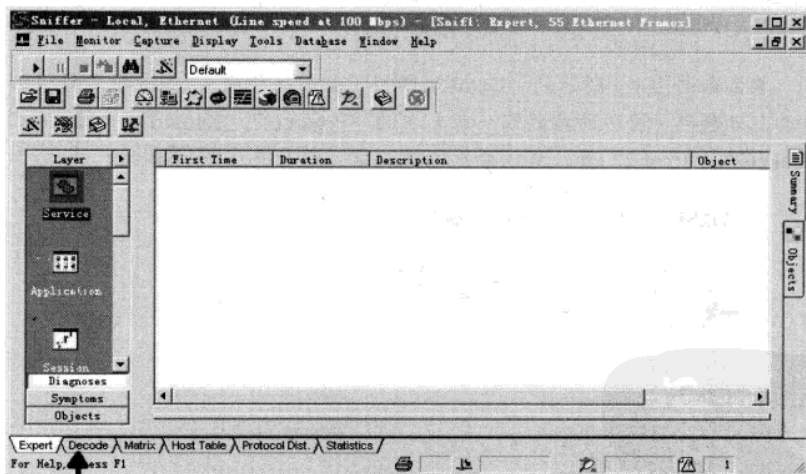


图 1-4-6 Sniffer 抓包

单击图 1-4-6 中的 “Decode” 选项卡, 显示捕获包的详细情况, 如图 1-4-7 所示。

STEP 4 最初的两个数据是 DNS 的包, 第一个包是客户机 192.168.1.200 去往 DNS 服务器 218.2.135.1 的 DNS 查询包, 客户机需要从 DNS 服务器获知 “www.njut.edu.cn” 所对应的 IP 地

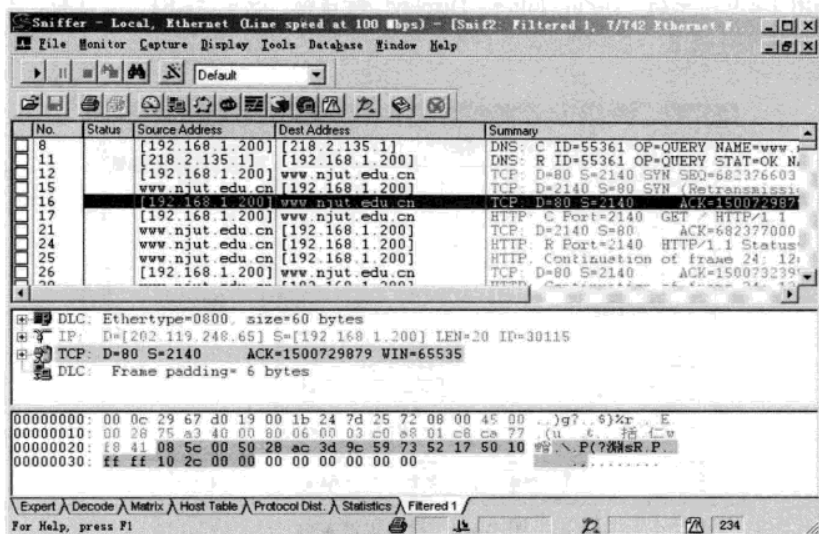


图 1-4-7 Sniffer 捕获包的详细情况

址，才能继续后面的访问。第二个包是 DNS 服务器返回给客户机的 DNS 应答包，其中“STAT=OK”说明域名解析已经成功。接下来就是“www.njut.edu.cn”这台服务器与客户机之间的直接对话了。

(3) 过滤数据包。

在如图 1-4-7 所示的窗口中，经常会捕获到很多数据包，但大多数都是无关的数据包，需要采用过滤技术才能过滤出有用的数据包。过滤数据包分为两个步骤：定义过滤条件和应用过滤条件。这里以过滤 ARP 包为例进行讲解。

STEP 1 定义过滤条件。如图 1-4-7 所示的数据包捕获窗口中，单击右键，在快捷菜单中选择“Define Filter”命令，如图 1-4-8 所示。

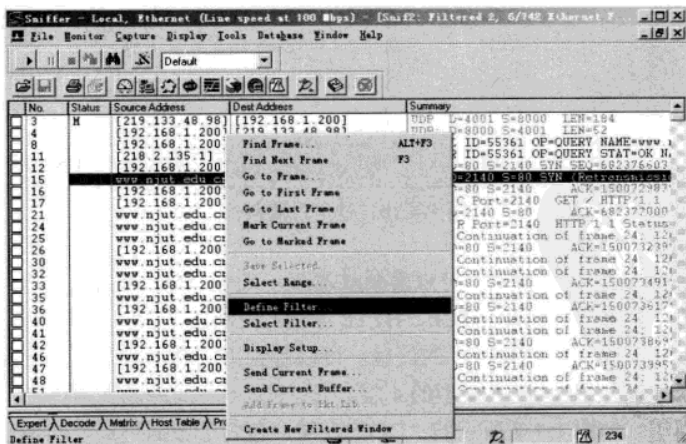


图 1-4-8 打开过滤对话框

打开如图 1-4-9 所示的“Define Filter - Display”对话框，选中“ARP”复选框，单击“确定”按钮，完成过滤条件设置。

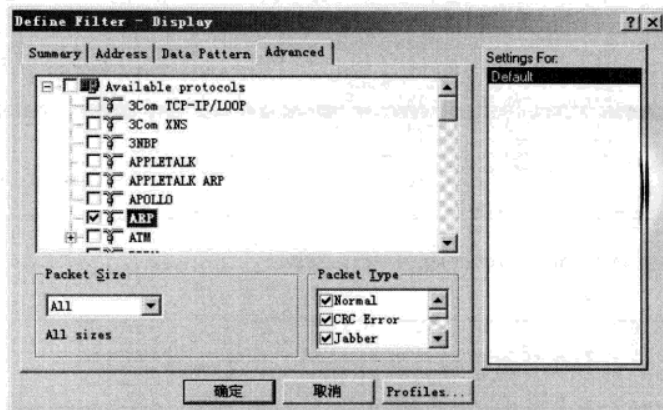


图 1-4-9 设置过滤条件

STEP 2 应用过滤条件。在如图 1-4-8 所示的快捷菜单中选择“Select Filter”，打开如图 1-4-10 所示的对话框，选择“Display”下的“Default”，右边显示该项是针对 ARP 进行过滤的。单击如图 1-4-10 所示的“确定”按钮，进行过滤。

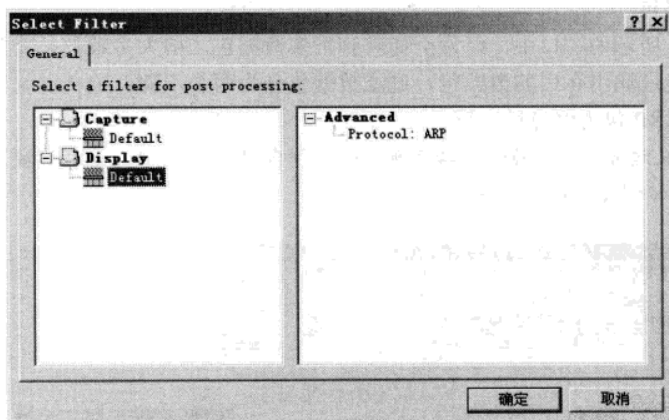


图 1-4-10 使用过滤条件

过滤后的窗口如图 1-4-11 所示，可以看到过滤后，只有 ARP 的包被显示。与此类似，还可以基于 MAC 地址、IP 地址、UDP、TCP、HTTP 等进行过滤。

如图 1-4-7 所示，任选一条 HTTP 的信息，可以看到第二个子窗口中显示此 HTTP 信息由 4 个层组成。接下来详细介绍 TCP/IP 模型的 4 层。

(1) 网络访问层。如图 1-4-7 所示的“DLC:”层，包含了数据链路层的地址，如用在以太网就是 MAC 地址。展开此层，可以看到数据包的源 MAC、目的 MAC 地址。此层是 TCP/IP 模

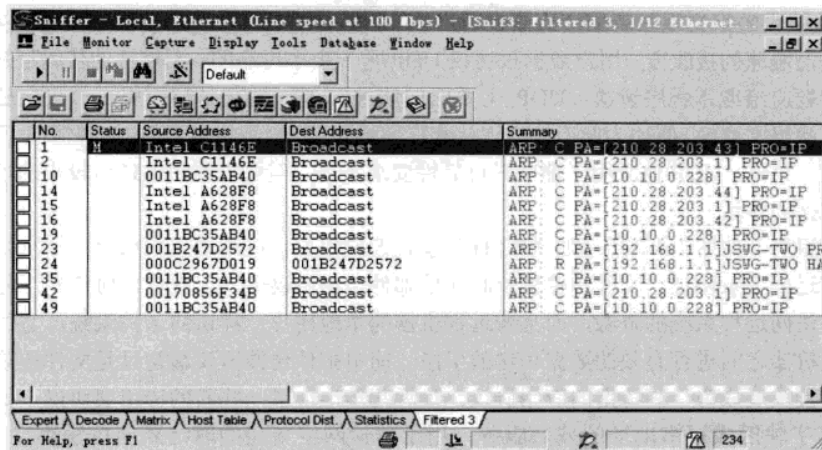


图 1-4-11 过滤出 ARP 的包

型的最低层，负责接收从 IP 层传来的 IP 数据报，并将 IP 数据报通过低层物理网络发送出去，或者从低层物理网络上接收物理帧，解封装出 IP 数据报，交给 IP 层处理。需要注意，当一台主机访问外网的某台服务器时，目的 MAC 并不是目标服务器的 MAC 地址，而是路由器局域网接口的 MAC 地址。因为 MAC 地址仅用于局域网内的寻址，假设目的 MAC 就是目标服务器的 MAC，当路由器收到这样的报文，通过比较目的 MAC 地址，发现不是发往本接口时，便把报文丢弃，这样数据报文也就无法通过路由器，更无法到达目标服务器了。因为目的 MAC 地址是路由器接口的 MAC 地址，路由器接收下这个报文并解封装后，交给上一层处理，路由器查询路由表，决定转发接口，把数据包交换到外出端口，再重新封装后发出去。如图 1-4-7 所示，验证目的 MAC 地址。

(2) 互联网层。如图 1-4-7 所示的“IP:”层，包含了网络层的地址，展开此层，可以看到数据包的源 IP、目的 IP 地址。它的主要功能包括 3 个方面。第一，处理来自传输层的分组发送请求。将分组装入 IP 数据报，填充报头，选择去往目的节点的路径，然后将数据报发往适当的网络接口。第二，处理输入数据报。首先检查数据报的合法性，然后进行路由选择，假如该数据报已到达目的节点（本机），则去掉报头，将 IP 报文的数据部分交给相应的传输层协议；假如该数据报尚未到达目的节点，则转发该数据报。第三，处理 ICMP（Internet Control Message Protocol，网际控制信息协议）报文。即处理网络的路由选择、流量控制和拥塞控制等问题。TCP/IP 网络模型的互联网层在功能上非常类似于 OSI 参考模型中的网络层。

(3) 传输层。如图 1-4-7 所示的“TCP:”层，包含了传输层的端口号，展开此层，可以看到数据包的源端口、目的端口。TCP/IP 参考模型中传输层的作用与 OSI 参考模型中传输层的作用是一样的，即在源节点和目的节点的两个进程实体之间提供可靠的端到端的数据传输。为保证数据传输的可靠性，传输层规定接收端必须发回确认，如果没有收到确认则假定分组丢失，再次发送，若干次重传后，仍然失败，则认为目标不可达，放弃重传。

TCP/IP 模型提供了两个传输层协议：传输控制协议 TCP 和用户数据报协议 UDP。TCP 是一个可靠的面向连接的传输层协议，它将某节点的数据以字节流形式无差错投递到互联网的另

机器上。发送方的 TCP 将用户交来的字节流划分成独立的报文并交给互联网层进行发送，而接收方的 TCP 将接收的报文重新装配交给接收用户。TCP 同时处理有关流量控制的问题，以防止快速的发送方淹没慢速的接收方。用户数据报协议 UDP 是一个不可靠的、无连接的传输层协议，UDP 将可靠性问题交给应用程序解决。UDP 主要面向请求/应答式的交易型应用，一次交易往往只有一来一回两次报文交换，假如为此而建立连接和撤销连接，开销是相当大的。这种情况下使用 UDP 就非常有效。另外，UDP 也应用于那些对可靠性要求不高，但要求网络的延迟较小的场合，如话音和视频数据的传送。

(4) 应用层。如图 1-4-7 所示的“HTTP”层，即应用层，应用层包括所有的高层协议。早期的应用层有远程登录协议、文件传输协议和简单邮件传输协议等。远程登录协议允许用户登录到远程系统并访问远程系统的资源，而且像远程机器的本地用户一样访问远程系统。文件传输协议提供在两台机器之间进行有效的数据传送的手段。简单邮件传输协议最初只是文件传输的一种类型，后来慢慢发展成为一种特定的应用协议。最近几年出现了一些新的应用层协议，如用于将网络中主机名字映射成网络地址的域名服务；用于传输网络新闻的网络新闻传输协议（NNTP，Network News Transfer Protocol）和用于从 WWW 网上读取页面信息的 HTTP。本书将在第 2 部分介绍有关 DNS、FTP、SMTP、HTTP 等服务器的搭建。

在 TCP/IP 网络中，IP 采用无连接的数据报机制，对数据进行“尽力而为的传递”，即只管将报文尽力传送到目的主机，无论传输正确与否，不做验证，不发确认，也不保证报文的顺序。TCP/IP 的可靠性体现在传输层，传输层协议之一的 TCP 提供面向连接的服务（传输层的另一个协议 UDP 是无连接的）。因为传输层是端到端的，所以 TCP/IP 的可靠性被称为端到端可靠性。

1.4.2 TCP/IP 参考模型与 ISO/OSI 参考模型比较

ISO/OSI 参考模型是在其协议被开发之前设计出来的。这意味着 ISO/OSI 模型并不是基于某个特定的协议集而设计的，因而它更具有通用性。但另一方面，也意味着 ISO/OSI 模型在协议实现方面存在某些不足。而 TCP/IP 模型正好相反，先有协议，模型只是现有协议的描述，因而协议与模型非常吻合。问题在于 TCP/IP 模型不适合其他协议栈。因此，它在描述其他非 TCP/IP 网络时用处不大。下面介绍两种模型的具体差异。其中显而易见的差异是两种模型的层数不一样：ISO/OSI 模型有 7 层，而 TCP/IP 模型只有 4 层。两者都有传输层和应用层，但其他层是不同的，两种模型之间的对应关系如图 1-4-12 所示。

ISO/OSI	TCP/IP
7 Application	Application
6 Presentation	
5 Session	
4 Transport	Transport
3 Network	Internet
2 Data Link	Network Access
1 Physical	

图 1-4-12 模型对照表

1.4.3 IP 地址划分

IP 地址是用来标识网络中的一个通信实体，如一台主机，或者是路由器的某一个端口。而在基于 IP 协议网络中传输的数据包，也都必须使用 IP 地址来进行标识，如同写一封信，要标明收

信人的通信地址和发信人的地址，邮政工作人员通过该地址来决定邮件的去向。

在计算机网络里，每个被传输的数据包也要包括一个源 IP 地址和一个目的 IP 地址。当该数据包在网络中进行传输时，这两个地址要保持不变（有网络地址转换和代理的情况例外，本书第 2 部分及第 4 部分都会介绍网络地址转换的配置实例），以确保网络设备总能根据确定的 IP 地址，将数据包从源通信实体送往指定的目的通信实体，以及数据包从目的通信实体返回源通信实体。

目前，IP 地址使用 32 位二进制地址格式，为方便记忆，通常使用以点号分隔的十进制数来表示，如 202.119.248.65。一个 IP 地址主要由两部分组成：一部分是用于标识该地址所从属的网络号；另一部分用于指明该网络上某个特定主机的主机号。网络号由 Internet 权力机构分配，主机地址由各个网络的管理员统一分配。因此，网络地址的唯一性与网络内主机地址的唯一性确保了 IP 地址的全球唯一性（其中保留给私网使用的地址段除外，私网使用的地址段有 10.0.0.0~10.255.255.255、172.16.0.0~172.31.255.255、192.168.0.0~192.168.255.255）。

为了给不同规模的网络提供必要的灵活性，IP 地址的设计者将 IP 地址空间划分为 5 个不同的地址类别，如表 1-4-1 所示，其中 A、B、C 三类最为常用，D 类用于组播，E 类用于科研。

表 1-4-1 IP 地址分类表					
IP 地址类型	第一字节十进制范围	二进制固定最高位	二进制网络位	二进制主机位	每个网络中可容纳主机数
A	0~127*	0	8 位	24 位	$2^{24}-2$
B	128~191	10	16 位	16 位	$2^{16}-2$
C	192~223	110	24 位	8 位	2^8-2
D	224~239	1110	组播地址使用		
E	240~255	1111	保留实验使用		

*规定 A 类中的 0 不允许使用，127 作为测试 TCP/IP 的环回地址，也不可以使用，因此 A 类实际可用的地址是 1~126。

如表 1-4-1 所示，A 类地址的网络位是 8 位，在子网掩码的二进制格式中，前面的 8 位是“1”，子网掩码中“1”表示的是网络位，“0”表示的是主机位，所以 A 类地址的默认子网掩码是 255.0.0.0。同理，B 类地址的默认子网掩码中，“1”的位数是 16 位，换成十进制就是 255.255.0.0；C 类地址的默认子网掩码中，“1”的位数是 24 位，换成十进制就是 255.255.255.0。

1.4.4 子网划分的具体方法

在讲述子网划分之前，先来看一个实例，如图 1-4-13 所示，4 台计算机接在一个 Hub（集线器）上，IP 和子网掩码配置如图中所示。图中的“/24”表示的是计算机 IP 地址的网络位有 24 位，主机位是 8 位（32-24=8），相当于子网掩码是 255.255.255.0。哪些计算机之间可以通信？判断的依据是什么？如何才能让它们全部都可以互访？

结果是 PC1 和 PC2 为一组，PC3 和 PC4 为一组，组内计算机之间可以通信，组间计算机之间不能通信。判断的依据是：同一子网的计算机可以直接通信，

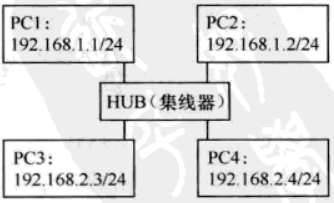


图 1-4-13 计算机互访图

不同子网的计算机不可以直接通信,处在不同子网中的计算机间如需通信,需要通过一个三层设备(也就是有路由功能的设备)。

那么如何判断计算机是否在同一个子网呢?先把 IP 地址和子网掩码换算成二进制,然后进行“与”运算,也就是二进制的按位取小运算,得出一台计算机所在的网络号,如果两台计算机的网络号相同,则它们处在同一子网;如果网络号不同,则它们处在不同子网。把每台计算机的 IP 地址与子网掩码进行按位“与”运算,得出 PC1 的网络号 192.168.1.0/24,PC2 的网络号是 192.168.1.0/24,PC3 的网络号 192.168.2.0/24,PC4 的网络号 192.168.2.0/24,PC1 和 PC2 处在同一子网,PC3 和 PC4 处在同一子网。如果 192.168.1.0 网络中的计算机需要访问 192.168.2.0 网络中的计算机,那么就需要通过一个三层设备,而 Hub 处于 OSI 七层模型中的第一层,即物理层,不具备路由功能,无法为不同子网中的计算机提供路由功能。

如何才能让 4 台计算机相互都可以通信呢?方法有很多种,这里简单列举 3 种。方法一,修改 PC3、PC4 的 IP 地址为 192.168.1.3、192.168.1.4,这样 4 台计算机就处在同一子网中,相互之间可以直接通信;方法二,修改 4 台计算机的子网掩码为“/22”,即 255.255.252.0,这样 4 台计算机就都处在 192.168.0.0/22 子网中了;方法三,把集线器换成三层交换机,并把接 PC1、PC2 的交换机端口划到一个 VLAN(虚拟局域网,在本书第 3 部分会更详细深入地介绍 VLAN 的配置),并给此 VLAN 分配 IP 地址 192.168.1.254,把 PC1 和 PC2 的网关设成 192.168.1.254,把连接 PC3、PC4 的交换机端口划到另一个不同的 VLAN,并给此 VLAN 分配 IP 地址 192.168.2.254,把 PC3 和 PC4 的网关设成 192.168.2.254,这样 4 台计算机之间也可相互通信了。

需要注意,在做子网划分的时候,主机位全“0”、全“1”的 IP 地址都不可以使用,全“0”的是子网地址,全“1”的是子网广播地址,如 192.168.1.0/24 和 192.168.1.255/24 这两个 IP 地址就分别代表网络地址和广播地址,都不可以配置给计算机使用,192.168.1.0/24 网络中可用的 IP 地址数是 $256-2=254$ 个,即每个子网中可用的 IP 地址数量是: $2^{\text{主机位数}}-2$ 。

为了便于初学者理解子网的计算,在这里列举 3 个例子。

实验 1-6 IP 子网计算

一台计算机的 IP 地址和子网掩码是 172.16.2.160/26,如何计算出该计算机所在的子网地址、子网广播地址、该子网中第一个可用的 IP 地址、该子网中最后一个可用的 IP 地址以及该子网中共有多少个 IP 地址可用?

如何对上述问题进行解答,许多专家一眼就能看出答案,但对于初学者却非易事。如图 1-4-14

172	16	2	160		
172.16.2.160	10101100	00010000	00000010	10100000	Host ①
255.255.255.192	11111111	11111111	11111111	11000000	Mask ②
172.16.2.128	10101100	00010000	00000010	10000000	Subnet ④
172.16.2.191	10101100	00010000	00000010	10111111	Broadcast ⑤
172.16.2.129	10101100	00010000	00000010	10000001	First ⑥
172.16.2.190	10101100	00010000	00000010	10111110	Last ⑦

图 1-4-14 子网的计算

所示,给出了一个通用的解法,虽然有点繁琐,但却易于理解,不会出错,随着对“与”运算的了解,还是可以再做精简。下面对上述几个问题解释如下。

STEP ① 把 IP 地址转换成二进制,不要使用一般常用的“除 2 取余”法,这特别容易搞错。建议使用凑数字法,IP 地址的每个十进制数是由 8 个二进制数组成的,最大是 $128+64+32+16+8+4+2+1=255$,如 $192=128+64$,则转换成二进制数就是 11000000。最后会发现,本例中的 172.16.2 是没有必要转换成二进制的,因为,任何数与 255 与运算的结果一定是它本身。

STEP ② 把子网掩码转换成二进制。

STEP ③ 在子网掩码二进制表示法中“1”的结束处,画一条竖线,竖线左边表示的是网络位,竖线右边表示的是主机位。本例中网络位是 26 位,主机位是 6 位。

STEP ④ 主机位全是“0”的地址是子网地址。

STEP ⑤ 主机位全是“1”的地址是广播地址。

STEP ⑥ 子网地址加 1 得到的是本子网中第一个可用的 IP 地址。

STEP ⑦ 子网广播地址减 1 得到的是本子网中最后一个可用的 IP 地址。

STEP ⑧ 把 IP 地址在竖线左边的网络位部分照抄下来,把各个地址部分补充完整。

STEP ⑨ 把二进制转换成十进制,就得出本子网地址是 172.16.2.128,本子网广播是 172.16.2.191,本子网中第一个可用的 IP 是 172.16.2.129,本子网中最后一个可用的 IP 是 172.16.2.190,本子网可用的 IP 地址数量是 $2^6-2=62$ 个。

实验 1-7 IP 子网划分

某单位申请到了一个 C 类的网络地址 192.1.1.0/24,该单位共有 5 个部门,每个部门最多有 28 台计算机。为了增强安全性,使用路由器来限制部门之间只能进行有限的访问。问子网掩码设成多少比较合适?

分析 C 类地址的特征,24 位网络位,8 位主机位,因为网络位是 IP 地址分配商提供,是固定分配的,单位内部可调整的只能是主机位。从 8 位主机位中如果借出一位,只能划分成 $2^1=2$ 个子网(有些老式系统不支持全 0、全 1 的子网,也就是如果是借 1 位,将没有子网可用,但新的系统基本都不存在这个限制),满足不了 5 个部门的需要;借 2 位,可以划分成 $2^2=4$ 个子网,还是满足不了 5 个部门的需要;借 3 位,可以分成 $2^3=8$ 个子网,可以满足 5 个部门使用的需要。网络位本来有 24 位,又从主机位借走了 3 位作为子网位,还剩下来 5 位主机位,每个子网可容纳的主机数量是 $2^5-2=30$,大于每个部门最多的主机数量 28;借 4 位,虽然子网数量满足了,可主机位只剩下 4 位,每个子网中最多只能有 $2^4-2=14$ 个可用 IP 地址,还要去除网关占用的一个 IP 地址,每个子网最多只能容纳 13 台计算机,小于每个部门最多有 28 台计算机的需求。故本例的正确划分方法只有一种,从主机位中借出 3 位作为子网位,则网络位变成了 $24+3=27$ 位,换成十进制就是 255.255.255.224。

本实验把一个 C 类地址分成了 8 个子网,而单位只需有 5 个子网,拿出前 5 个子网,后面的 3 个子网预留给将来的升级使用。假设每个子网都是把第一个可以使用的 IP 地址用做网关,则 IP 地址的分配范围、网关和子网掩码的配置、路由器接口的 IP 地址配置,以及每个子网的网络号和未使用的网络号,如图 1-4-15 所示。

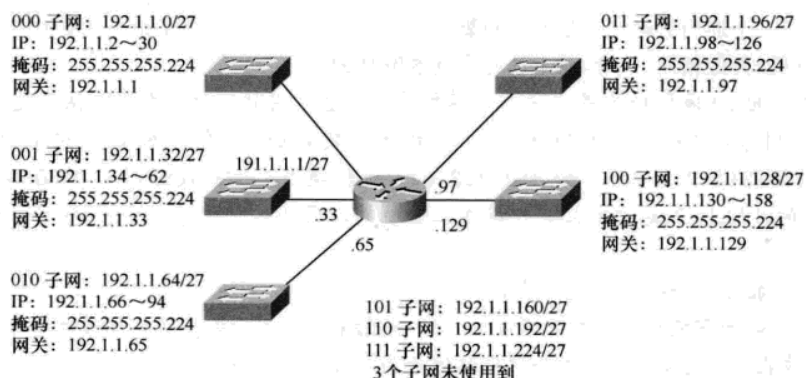


图 1-4-15 子网的划分

实验 1-8 IP 路由汇总

如图 1-4-16 所示, 路由器 R1、R2、R4 上均有 4 个 C 类的地址, 路由器 R3 能学到所有的路由条目 (本书第 3 部分会介绍路由的配置)。R3 的路由表中有 $12+3$ (路由器中的互连网段) = 15 个条目, 过多的路由表条目会占用更多的内存, CPU 的负载也会更大, 还会带来网络的不稳定性。可以使用路由汇总技术来减小 R3 路由表的大小。对于一个网络管理人员来说, 掌握正确的路由汇总技术必不可少。

把所有明细路由条目转换成二进制, 把共同的部分取出来, 如果不会带来误解, 即可实现路由的汇总。这里以 R1 上的 4 个条目为例, 如图 1-4-17 所示进行操作。

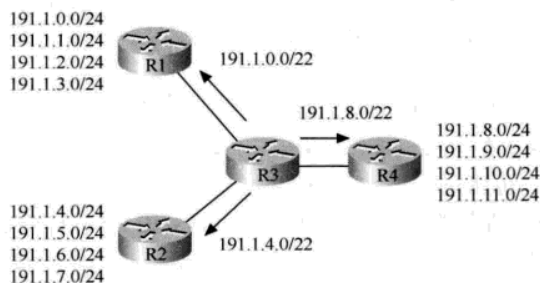


图 1-4-16 路由条目分布

191.1.0.0	10111111	00000001	00000000	10100000	①
191.1.1.0	10111111	00000001	00000001	11000000	②
191.1.2.0	10111111	00000001	00000010	10000000	③
191.1.3.0	10111111	00000001	00000011	10111111	④
⑤	191.1.0.0/22				

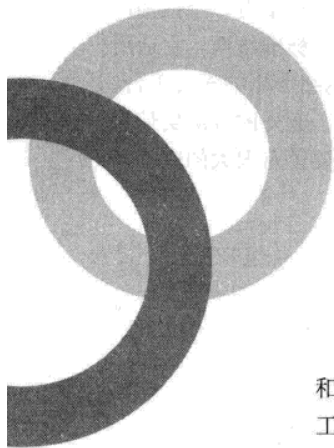
图 1-4-17 路由汇总算法

STEP 1 ①②③④ 个步骤把 4 个明细路由条目转换成二进制。

STEP 2 ⑤ 在所有明细条目都具备的共同部分后面画一条竖线。

STEP 3 ⑥ 取出共同的部分, 后面的位补 “0”, 这里是 191.1.0.0。再数一数竖线左边的位数是 22, 得出汇总后的网络地址是 191.1.0.0/22。同理可以得出去往 R2 的路由汇总条目是 191.1.4.0/22, 去往 R4 的路由汇总条目是 191.1.8.0/22。这 3 个路由汇总条目之间互不影响, 不会产生路由转发的误解。

STEP 4 在 R3 上取消明细条目, 只保留汇总后的条目。路由表条目从汇总前的 15 条变成汇总后的 3 (汇总后的路由) + 3 (路由器中的互连网段) = 6 条, 路由表大大减小。



第2章 网络硬件知识

Chapter 2

第一章介绍了网络的基础理论，本章将介绍网络的基础硬件，包括网络传输介质和网络硬件设备。通过本章的学习，读者可以了解各种网络传输介质及特点，以便在工程中正确选择传输介质；还可以了解网络硬件设备的工作原理和它们之间的区别，以便在工程中正确选择网络设备；还可以掌握双绞线的制作和应用场合。

2.1 网络传输介质

网络传输介质是网络中传输数据、连接各网络站点的实体。网络传输介质分为两大类：传导型介质和辐射型介质。

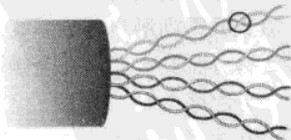
2.1.1 传导型介质

信号通过电路传输时，传导型介质利用导体传导，即承载信号。金属导体被用来传输电信号，通常由铜线制成，双绞线和大多数同轴电缆就是如此。玻璃纤维通常用于传导光信号的光纤网络。

1. 双绞线

双绞线可分为非屏蔽双绞线和屏蔽双绞线。

非屏蔽双绞线（Unshielded Twisted Pair，UTP），如图 2-1-1 所示，价格低廉、容易安装及重新配置，是最常见的传输介质，它由两股线规很细的铜线（通常为实心）组成，互相绝缘，以固定间隔彼此绞合在一起，绞合的作用是为抵消电脉冲传输过程中所形成的电磁场。现在，UTP 被广泛应用于局域网领域，以便把终端与集线器、交换机和路由器连接起来。在传输距离（100m）范围内，五类 UTP 的数据传输速率可以达到 100Mbit/s，甚至 1000Mbit/s。



铝箔屏蔽的双绞线（Foil Twisted Pair，FTP），如图 2-1-2

图 2-1-1 非屏蔽双绞线

所示, 带宽较大、抗干扰性能强。但屏蔽线比非屏蔽线的价格及安装成本要高一些, 线缆弯曲性能稍差。

屏蔽双绞线 (Shielded Twisted Pair, STP), 如图 2-1-3 所示, 每一对双绞线都有一个铝箔屏蔽层。4 对双绞线合在一起, 还有一个公共的金属编织屏蔽层, 这是七类线的标准结构。它适用于高速网络, 提供高度保密的传输, 支持未来的新型应用, 有助于统一当前网络应用的布线平台, 使得从电子邮件到多媒体视频的各种信息, 都可以在同一套高速系统中传输。额外的屏蔽层使得七类线有一个较大的线径, 这些特点要求在设计安装和端接时要特别小心, 要留有很大的空间和较大的弯曲半径。

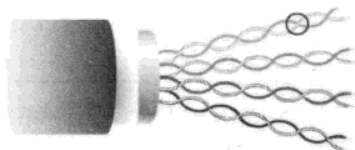


图 2-1-2 铝箔屏蔽的双绞线

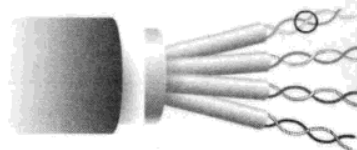


图 2-1-3 独立屏蔽双绞线

屏蔽双绞线需要一层金属铝箔, 即覆盖层, 把电缆中的每对线包起来, 有时候利用另一覆盖层把多对电缆中的各对线包起来或利用金属屏蔽层取代这层包在外面的金属铝箔。覆盖层和屏蔽层有助于吸收环境干扰, 并将其导入地下以消除这种干扰。这意味着金属铝箔和屏蔽层在焊接时必须与焊接导体时同样小心, 而且确保导入地下的机制安全可靠。与 UTP 相比, STP 和 FTP 的成本高得多, 而且安装过程也难得多。

2. 同轴电缆

如图 2-1-4 所示, 与 UTP 相比, 同轴电缆含有线规较粗的单层实心导体。导体一般由铜或覆以铜的铝制成。

中间的导体外面覆以一层绝缘材料, 这有助于把中间的导体和外面的金属铝箔屏蔽层隔开来。外面通常会包一层金属网, 再包一层保护皮对电缆加以保护。中间的导体可支持高频信号, 几乎不会出现困扰 UTP 及其同类电缆的信号衰减问题。

有线电视系统传统上使用同轴电缆, 支持高达 500~750MHz 的信号, 传输距离相当远, 信号通常被细分成 6MHz 的频率信道, 用于下行电视传输。当前的系统还越来越多地划分不同带宽的信道, 以实现双向数据甚至语音传输。

同轴电缆传输系统目前在国内外有线电视网络中仍占有重要地位, 它是由多级干线放大器级联, 1 级桥接放大器和 2 级分配放大器组成。干线放大器大都采用压铸铝合金机盒安装在干线上, 对信号进行放大, 以补偿干线电缆的损耗, 使传输线路进一步延伸。

桥接放大器是干线放大器的派生品种。干线桥接放大器除放大干线中的信号外, 还分出几路支线信号传输到用户分配系统。而桥接放大器则对干线中的信号不放大, 仅对分出的几路信号进行放大并送到用户分配系统。为了能支持更多的用户, 在更高频有线电视系统中可在支线上再串接 2 台分配放大器, 在全频道系统中则只能串接 1 台分配放大器, 分配放大器的输出可直接驱动用户分配网。

在电缆传输的有线电视系统中, 从前端发出的射频电视信号是用同轴电缆传输给用户的。由于所传输的射频信号都在高频段, 因而需要使用比较粗的同轴电缆以降低损耗, 以传输较远

的距离。

对于同轴电缆传输系统,虽然国内外各种放大器的性能已达到相当高的水平,而且在减少同轴电缆衰减、减少温度系数、提高同轴电缆寿命等方面做了不少工作,实现在同样的电强度下能传输更远的距离和提高系统的可靠性,但是由于同轴电缆传输系统离不开放大器和同轴电缆,系统本身存在一些难以克服的缺陷,不能无限地级联干线放大器来增加传输的距离,因而,同轴电缆传输系统的发展受到了限制。

以太网及其他 LAN 技术早期使用同轴电缆是因为它能支持高频信息,而且不受电磁干扰影响。然而,面对迅猛发展的数据级 UTP,成本高昂加上安装困难导致同轴电缆退居双绞线之后。

同轴电缆根据粗细程度不同,分为粗缆和细缆,粗缆的传输距离是 500m,细缆的传输距离是 185m。

3. 光纤

光导纤维简称光纤,它的特点是传输距离远,不易受到电磁干扰。光纤是细如头发般的透明玻璃丝,可用来传导光信号。光纤由纤芯和包层组成。由于纤芯的折射率大于包层的折射率,故光波在界面上形成全反射,使光只能在纤芯中传播,实现通信。

光纤按组成成分来分,有以 SiO_2 (二氧化硅) 为主要成分的石英纤维,有多种组成成分的多组分纤维,有以塑料为材料的塑料纤维等。

工程中使用最多的分法是按光纤横截面上折射率来分,有单模光纤和多模光纤。单模光纤纤芯直径较小,采用激光作为光源,传输的方向是沿光纤直径方向,如图 2-1-5 所示,故单模光纤数据传输速率较高,传输距离较远,价格相对较贵;多模光纤纤芯直径较大,采用发光二极管作为光源,传输的方向是全反射,如图 2-1-5 所示,故多模光纤数据传输速率较低,传输距离较近,价格相对较便宜。

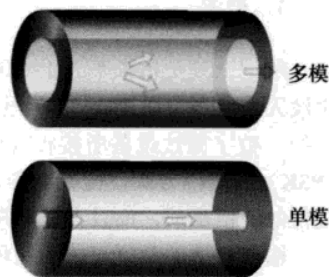


图 2-1-5 光在多模和单模光纤中的传输方向

光纤的主要特性有两项,即损耗和色散。光纤每单位长度的损耗或衰减 (dB/km),关系到光纤传输系统的传输距离和中继站的间隔距离,这是一个首要的特性,对数字信号的传输尤其重要。色散使光纤中的光脉冲在传输过程中发生展宽和畸变,由于脉冲宽度与频带宽度成反比,脉冲宽度越大,带宽越窄,脉冲展宽的程度(即带宽的宽窄)直接关系到光纤传输系统的信息容量,决定了在给定传输距离和误码条件下的码速率上限(即信息传输容量)。

目前常用的石英光纤的损耗已接近理论极限,短波段的损耗可达 2.1dB/km ,长波段的损耗可达 0.2dB/km 。光纤的带宽可达数十 GHz/km ,并在 $1.3\text{ }\mu\text{m}$ 波长左右可实现“零散色区”,光纤传输正向长波段、单模光纤发展。

光纤传输系统主要由光纤(或光缆)和中继器组成。在短距离传输系统中,一般不需要中继器,从发送部分输出的已调光波经耦合器进入光纤。光纤是光纤传输系统的主要组成部分,其特性好坏对光纤传输系统的性能有很大的影响。为了增加光纤传输系统的传输距离和传输容量,对光纤传输特性总的要求是损耗尽可能低和带宽尽可能宽。虽然光纤的损耗和带宽限制了光波的传输距离,由于光纤损耗很低,故光纤传输的中继距离通常比其他有线通信,甚至比微

波通信远得多。

2.1.2 辐射型介质

辐射型介质并不利用导体,如图 2-1-6 所示,确切地说,信号完全通过空间从发射器发射到接收器。辐射介质有时被称为无线电波系统,更准确地说,是空间波或自由空间系统。只要发射器和接收器之间有空气,就会导致信号减弱及失真。

在广泛使用的辐射传输系统类别中,无线电系统最常见,这里着重介绍微波和卫星。还有一系列针对特定应用的变种,包括传呼、蜂窝、无绳电话和各种分组无线系统。自由空间激光系统最常见的就是红外线 (Ir),它从本质上来说基于光技术,且不依赖玻璃或塑料导体,信号完全通过空间发射。

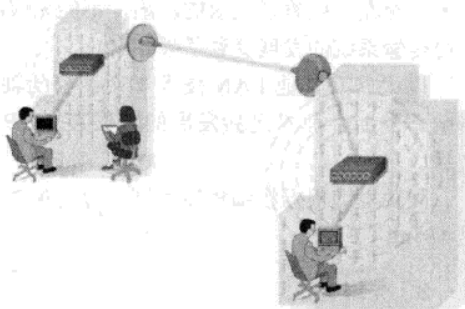


图 2-1-6 无线传输

1. 微波

所谓微波是指频率大于 1GHz 的电波。如果应用较小的发射功率 (约 1W) 配合定向高增益微波天线,再每隔 10~50 英里 (约为 16~80km) 的距离设置一个中继站就可以架构起微波通信系统。数字微波设备所接收与传送的是数字信号,数字微波采用正交调幅 (QAM) 或相移键控 (PSK) 等调幅方式,传送语音、数据或是影像等数字信号。与模拟微波比较起来,数字微波具有较佳的通信品质,而且在长距离的传送过程中相对不会有杂音累积。

微波传播的类型可分为两种,一种是自由空间传播,也就是在收发二地之间没有任何阻隔,也没有任何其他的影响下 (包括反射、折射、绕射、散射或吸收) 传播,不过这种环境在现实生活中很少出现;另一种则是视线传播。在完美的状况下,视线传播与自由空间传播并无显著的差别,不过因为视线传播将大气层折射与地面物反射等影响因素考虑在内,所以在现实环境中使用时就会与自由空间传播产生极大的差异。

自由空间传播是假设微波传输的两点之间没有物体阻挡,而且除了两点直线间不能有阻碍物体外,直线附近的某一个范围内也必须避免物体存在,因为微波天线虽具有良好的指向性,但它所发射的信号路径不是一条单纯的直线,它所发射的波面会逐渐扩大,若这些散逸的电波遇到物体阻挡,就会经由反射路径达到接发点,反射路径与直线路径因为长度不等,所以到达接收点的相位自然有差异,这就是“干扰”的形成。这种干扰偶尔会对传播有利,但通常都是有害的,所以若是以自由空间传播的方式进行,则电波传播路径的直线周围必须预留相当大的空间,这些空间被称为“空域”。

但是视线传播则不然,当两地相距数十千米时,其中有无山林房屋阻挡常常无法凭视觉决定,再加上地面本身就是弯曲的视线,视线是否会被地弧所阻也是问题之一。不过上述这些问题都可以借由精确的地面测量图及实地现场勘测后绘制的地图来解决,在预定收发两点间画一条直线即可判断二地之间会受到多少阻碍。

2. 卫星

卫星其实就是非地面微波,有些情形下工作在与地面系统相同的频率范围上。在20世纪70年代和20世纪80年代,卫星通信一般使用大型地面站,通过直径10~30m的天线进行通信,那时用户在全球或远距离上打电话、接收电视或其他任何信号时,需要这样的大型地面站和大天线。在20世纪80年代末90年代初,当卫星技术进一步发展时,情况发生了相当大的变化,用户可以从很多地方接收卫星信号。如航行在大海的舰船、以800km/h以上的速度飞行的飞机、运行速度大于7~8km/s的空间飞行器和卫星、处于困境中的飞机或船只、行人和行进中的汽车等。

卫星在多种轨道中提供通信,使人们进行有效的沟通联络。各种普通的卫星通信业务包括电话、电视广播、数据接收与分发、直播电视、灾害预警、气象监测、航空器跟踪和指令、星际链路、电子邮件传递、互联网接入、数据采集、GPS(Global Positioning System,全球定位系统)定位和定时、移动车辆跟踪等。卫星通信网络是推动社会各个领域发生变化的重要基础设施。除了传统的地面链路、光纤链路可以把通信网络迅速延伸到人迹罕至的偏远地点,卫星通信也将起着举足轻重的作用。

在未来的社会生活中,最常见的通信方式是移动个人通信,即用户在任何地点、任何时间,与他人交换各种信息,如话音、数据、视频和图像。构成这种移动通信的基础的关键要素是小型廉价的手持式通信机,且使用不受地点、地界束缚的单一电话号码。卫星通信可以发挥重要作用。

卫星具有诸多优点,包括覆盖区域广泛。由于距离地面相当高,它们所能发射及接收信号的范围很大。因此,卫星在点对多点和广播应用中具有很大优势。

然而与所有微波系统一样,卫星的性能随天气的变化而有所不同。此外,传播延迟也是卫星的重要问题,因为信号要在发射器和接收器之间通过长达几万千米的距离,所以即使以光速传输也需要一段时间。

3. 红外线

红外线及其他自由空间光学系统用于短程应用,在可以获得直接视线的场合最有效。一些WLAN利用红外线,例如,两台笔记本电脑就可以通过红外线进行数据传输。有些手机也支持红外线功能,可以通过红外线与笔记本电脑进行数据交互。

2.1.3 传导型介质与辐射型介质的比较

就最基本的方面而言,传导系统与辐射系统有着明显区别。

传导系统使用绝缘和覆盖材料(有时是屏蔽层)包起来的导体,因此不会受外部因素的干扰。如果绝缘、覆盖和屏蔽材料没有受到钉子、老鼠、挖土机、打桩机或其他破坏工具的损坏,一旦合理安装,预计传导系统就会正常工作。合理安装意味着要获得地方政府的批准、挖沟、埋管道以及铺设电缆(在不同点进行焊接)、设置检修孔、将当地电力输送到放大器和中继器、安放交叉连接设备等。此外,架空系统需要立杆、架设电缆,这比地理线缆更加快速方便,但仍然耗时、成本高。

辐射系统的部署常常速度快得多,成本也相对较低。虽然要为发射及接收天线获得许可权或者屋顶架设权,但相关的成本、难度和耗时常常比传导系统低得多。卫星需要难度更大、成本更

高的部署过程,但对一系列特殊应用而言它具有优点。

辐射系统存在几大问题。首先,视线总是更可取,而且常常是必需的。其次,无线电波的质量会因天气出现很大变化,天气对传输性能具有重大影响,完全不受人的控制。最后,射频频谱资源有限,而且受到严格管制,在当今供不应求的现状下,获得成本将会非常高。

有些系统所用的免许可证频谱随处可得,但需要与其他系统和用户共享。当然,辐射系统的一大优点是不用线缆,因而大大简化了配置和重新配置。其次,辐射系统具有移动性。蜂窝、传呼和各种无线系统也具有移动性优点,而有线系统不具备这些优点。

网络信息依靠传输介质来承载,网络的发展离不开传输介质的发展,在网络高速发展的今天,应该高度重视传输介质的研究,同时在组网时应该认真比较和论证,以确定最适合的网络传输介质。

2.2 网络硬件设备

组成网络的主要硬件设备有网卡、中继器、集线器、网桥、交换机、路由器、网关、宽带路由器和防火墙等,下面对这些网络设备进行介绍。

2.2.1 网卡

网卡(Network Interface Card, NIC)也叫做网络适配器,是连接计算机与网络的硬件设备,网卡的主要工作是整理计算机发往网线的的数据,并将数据分解为适当大小的数据包,然后向网络发送出去。对于网卡而言,每块网卡都有一个唯一的网络节点地址,它是网卡生产厂家在生产时烧入ROM(Read Only Memory,只读存储器)中的,通常把它叫做MAC地址,且保证绝对不会重复,本书的实验1-3中介绍过如何查看MAC地址。用户可以人为地修改MAC地址的显示(并没有更改ROM中的内容,当计算机重新安装操作系统后,MAC地址还是出厂时的MAC地址),具体操作参见实验2-1。网卡插在计算机或服务器扩展槽中,通过网络线(如双绞线、同轴电缆或光纤)与网络交换数据、共享资源。选购网卡需考虑以下几个因素。

(1) 速度。网卡的速度表示网卡接收和发送数据的快慢,10Mbit/s的网卡价格较低(基本被淘汰,现在市面上很难买到);在传输频带较宽的信号或交换式局域网中,应选用速度较快的100Mbit/s网卡;1000Mbit/s网卡现在也越来越普遍,最新购买的服务器几乎都配备了1000Mbit/s的网卡。

(2) 总线类型。常见网卡按总线类型可分为ISA网卡、PCI网卡等。ISA网卡以16位传送数据,速度较慢,现在已基本淘汰。PCI网卡以32位传送数据,速度较快。目前市面上大多是100Mbit/s和1000Mbit/s的PCI网卡,建议不要购买过时的ISA网卡,除非用户的计算机没有PCI插槽。

(3) 接口。常见网卡接口有BNC接口、RJ-45接口和光纤接口。接口的选择与网络布线结构有关,在小型共享式局域网中,BNC口网卡通过同轴电缆直接与其他计算机和服务器相连;RJ-45口网卡通过双绞线连接集线器或交换机,再通过集线器或交换机连接其他计算机和服务器;提供光纤接口的网卡,多为1000Mbit/s的网卡,主要是出于连接速度方面的考虑。

实验 2-1 修改网卡的 MAC 地址

前面介绍到,网卡在生产时 MAC 地址被烧入 ROM 中,不能够被改变,但网卡 MAC 地址在操作系统中的显示却是可以修改的。一个有趣的现象是,当把同一个局域网中的两台计算机配置成相同的 IP 地址,两台计算机都提示 IP 地址冲突,并且后配置的计算机的 IP 地址无效。修改网卡 MAC 地址的方法如下。

右键单击“网上邻居”,在快捷菜单中选择“属性”,打开“网络连接”窗口,右键单击“本地连接”,在快捷菜单中选择“属性”,如图 2-2-1 所示。

打开“本地连接 属性”对话框,如图 2-2-2 所示。

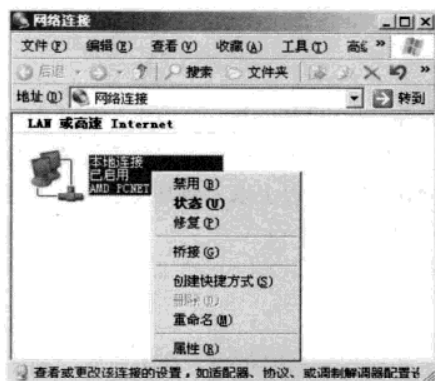


图 2-2-1 网络连接窗口

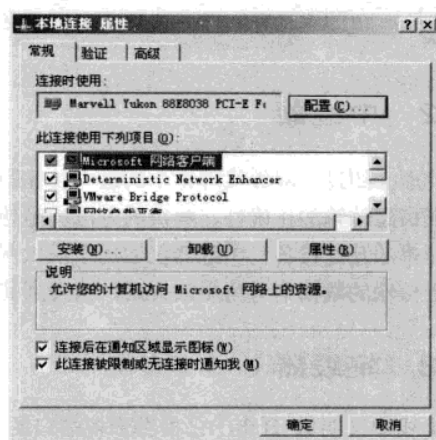


图 2-2-2 本地连接属性

单击如图 2-2-2 所示的“配置”按钮,打开网卡属性对话框,如图 2-2-3 所示。

选择如图 2-2-3 所示的“高级”选项卡,在左边的“属性”栏中选择“网络地址”,在右边的“值”中填入网卡新的 MAC 地址,如填入“001B247D2511”,如图 2-2-4 所示。

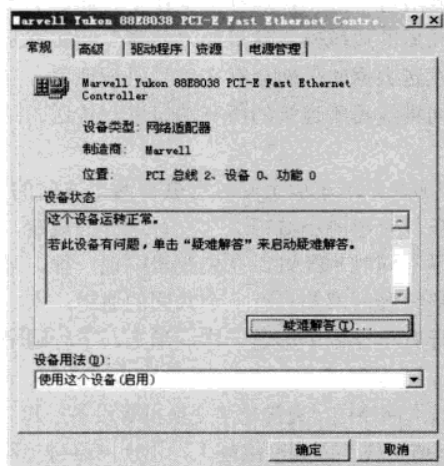


图 2-2-3 网卡属性

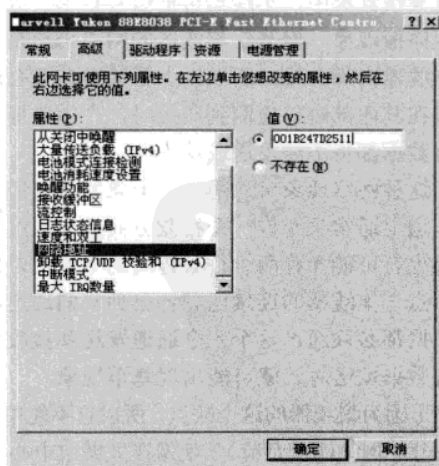


图 2-2-4 更改网卡的 MAC 地址

必须以十六制的格式填入 12 位数据,中间不加任何分隔符号,组成新的 MAC 地址。如果填写错误,MAC 地址更改将无效,网卡继续使用先前的 MAC 地址。随意填入 12 位十六制编码,生成的 MAC 地址并不一定有效,最好的办法是前 6 位保持不变(前 6 位是厂商编码),更改后 6 位(后 6 位是厂商生产的网卡编号),单击“确定”按钮返回。使用实验 1-3 的方法,在 DOS 窗口中输入“ipconfig/all”,验证网卡新的 MAC 地址。

如图 2-2-4 所示,网卡除了可以更改 MAC 地址属性外,还可以更改其他参数,如“速度和双工”、“流控制”、“接收缓冲区”等。

注意



如果把两台计算机的 IP 和 MAC 地址都配置成一样,则不会提示 IP 地址冲突,并且都可以上网。

2.2.2 中继器

前面介绍过,双绞线理论上的最大传输距离是 100m,如果超过 100m,由于信号的衰减,很难保证信息传输的正确性,解决的办法就是使用中继器(Repeater)。中继器又称重发器,是一种最为简单的互连设备。中继器仅适用于以太网,可将两段或两段以上以太网互连起来。中继器对电缆上传输的数据信号再生放大后,重发到其他电缆段上。

2.2.3 集线器

集线器又叫做 Hub,它相当于多端口的中继器,也可以把信号整形、放大后发送到所有节点上。

在环型网络中只存在一个物理信号传输通道,所有信号都是通过一条传输介质来传输的,这样就存在各节点争抢信道的矛盾,传输效率较低。引入集线器这一网络设备后,每一个工作站是用它自己专用的传输介质连接到集线器,各节点间不再只有一个传输通道,各节点发出去的信号通过集线器集中,集线器再把信号整形、放大后发送到所有节点上,这样至少在上行通道上不再出现碰撞现象。但基于集线器的网络仍然是一个共享介质的局域网,这里的“共享”其实就是共享集线器内部总线,所以当上行通道与下行通道同时发送数据时仍然会存在信号碰撞现象。当集线器在其内部端口检测到碰撞时,产生碰撞强化信号向集线器所连接的所有端口进行传送。这时所有数据都将不能发送成功。

这种网络现象可以用一个形象的现实情形来说明,那就是单车道上同时行驶有两个方向的车。单车道上通常只允许一个行驶方向的车通过,但是在条件有限的小城镇通常没有这样的规定,单车道也有可能允许两个行驶方向的车通过,但是必须是不同时刻经过。在集线器中也一样,虽然各节点与集线器的连接已有各自独立的通道,但是在集线器内部却只有一个共同的通道,上、下行数据都必须通过这个共享通道发送和接收数据,这样有可能像单车道一样,当上、下行通道同时有数据发送时,就可能出现塞车现象。

正因为集线器的这个缺点,所以它不能单独应用于较大网络中(通常是与交换机等设备一起分担小部分的网络通信负荷),就像在大城市中心不能有单车道一样,因为网络越大,出现网络碰撞现象的机会就越大。也正因如此,集线器的数据传输效率是比较低的,因为它在同一时刻只能有一个方向

的数据传输，也就是所谓的“单工”方式。生活中最常见的使用“单工”方式工作的设备有对讲机，按下通话键时，可以讲话，但不能接收；松开通话键，可以接收，但不能说话。而生活中的电话采用的是“双工”工作方式，可以同时说话和听话。如果网络中要选用集线器作为单一的连接设备，那么网络的规模最好在 10 台以内，而且集线器带宽应为 10Mbit/s 以上。

集线器除了共享带宽这一缺点，还有另一个缺点必须要考虑，那就是它的广播工作方式。因为集线器属于 OSI 七层模型的物理层，基本上不具有“智能”的能力，更别说“学习”功能了。它也不具备交换机所具有的 MAC 地址表，所以它发送数据时都是没有针对性的，因此采用广播方式发送。也就是说当它要向某节点发送数据时，不是直接把数据发送到目的节点，而是把数据包发送到与集线器相连的所有节点，如图 2-2-5 所示。所有通过集线器互连的网络属于同一个子网，只有一个广播域、一个冲突域。

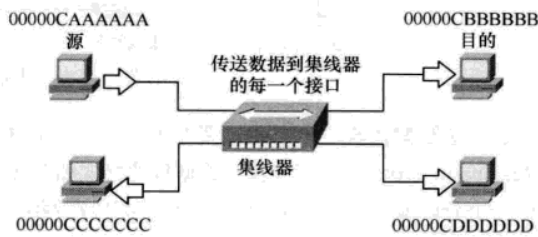


图 2-2-5 集线器的工作原理

这种广播发送数据的方式有两方面不足。第一，用户数据包向所有节点发送，很可能带来数据通信的不安全因素，一些别有用心的人很容易就能截获他人的数据包。第二，由于所有数据包都是向所有节点同时发送，加之以上所介绍的共享带宽方式，就更加可能造成网络拥塞现象，降低网络执行效率。

2.2.4 网桥

网桥工作在数据链路层，用于将两个 LAN 连接在一起并按 MAC 地址转发帧。网桥用于扩展 LAN，连接两个网段的网桥能从一个网段向另一个网段传送完整而且正确的帧，不会传送干扰或有问题的帧。任何一对在桥接 LAN 上的计算机都能互相通信，但是它们并不知道是否有网桥将其分开。根据路由选择方法，可将网桥分为两种类型。

1. 透明网桥

透明网桥主要用于互连以太网分段。这种网桥用来传输需在两个不同以太网分段间传输的信息，但是阻断局部分段内的信息，因此减少了网络上的通信总量。

实验 2-2 网桥的工作方式

如图 2-2-6 所示，有两台集线器，4 台计算机，一台网桥。网桥的工作方式如下。

STEP ① 每个网桥保存一个动态的 MAC 地址表（由站点的 MAC 地址和网桥的端口号组成）。

STEP ② 初始时，该 MAC 地址表为空，以后通过逆向自学习方法获取 MAC 地址信息。逆向自学习方法是当一个数据帧到达网桥时，网桥根据其源 MAC 地址以及到达的端口号，向 MAC 地址表中增加或刷新一条记录。

刚刚启动加电时，网桥的 MAC 地址表是空的，假设计算机 A（192.168.1.1）要发送数据给计算机 B（192.168.1.2），发送数据之前，计算机 A 要对数据包进行封装。计算机 A 仅知道计算机 B 的 IP 地址，却不知道计算机 B 的 MAC 地址，因此无法完成数据包的封装。

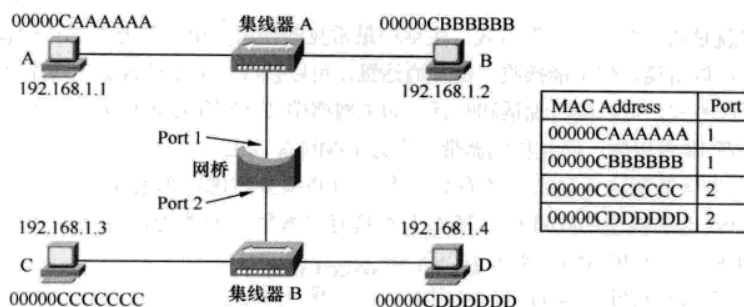


图 2-2-6 网桥工作方式图

发送数据之前, 计算机 A 要首先获知计算机 B 的 MAC 地址, 计算机 A 发送一个 ARP (Address Resolution Protocol) 请求包, 数据包的格式如图 2-2-7 所示。数据包在传输层被分段 (Segment), 其中一个分段被交给下一层 (网络层); 数据段在网络层被封装成包 (Packet), 源 IP 地址是“192.168.1.1”, 目的 IP 地址“192.168.1.2”, 封装后的数据包被交给下一层 (数据链路层); 在数据链路层被封装成帧 (Frame), 源 MAC 地址是“00000CAAAAAA”, 因不知道 B 的 MAC 地址, 要先发一个 ARP 查询包, 来获取计算机 B 的 MAC 地址, ARP 查询包是广播包, 目的 MAC 地址是“FFFFFFFFFFFF”, 封装后的数据帧被交给下一层 (物理层); 物理层把数据帧转变成二进制的比特 (bit) 流。

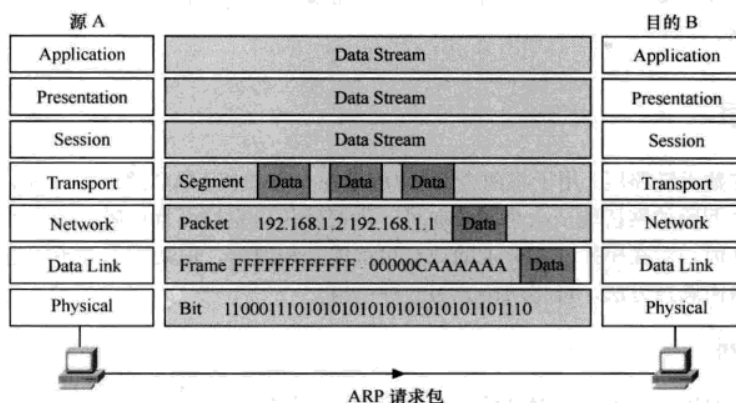


图 2-2-7 ARP 请求包格式

比特流到达集线器 A, 集线器把比特流发往除接收端口以外的所有端口 (计算机 B 和网桥)。计算机 B 收到这个比特流, 物理层把比特流接收下来, 交给数据链路层。因目的 MAC 地址是广播 MAC 地址“FFFFFFFFFFFF”, 计算机 B 接收这个帧, 执行解封装, 把解封装后的包交给网络层。计算机 B 发现目的 IP 地址与本机的 IP 相同, 继续处理这个包, 发现是 ARP 请求包, 计算机 B 对计算机 A 的 ARP 请求包进行应答。网桥也接收到这个比特流, 网桥是数据链路层的设备, 可以查看帧的格式, 网桥看到数据帧中的源 MAC 地址是“00000CAAAAAA”, 并且网桥的 MAC 地址表中没有该项, 网桥把该 MAC 地址及对应的端口加入到 MAC 地址表中。网桥查看数据帧的目的 MAC 地址, 发现是广播 MAC 地址, 网桥把该比特流从除接收端口 (Port 1) 以外的所有端口 (Port 2) 发出去。网桥把 ARP 请求包发往如图 2-2-6 所示的集线器 B。

集线器 B 收到网桥转发过来的比特流后, 把比特流发往除接收端口以外的所有端口 (计算机

C 和计算机 D)，计算机 C 收到这个比特流，物理层把比特流接收下来，交给数据链路层，因目的 MAC 地址是广播 MAC 地址“FFFFFFFF”，计算机 C 接收这个帧，执行解封装，把解封装后的包交给网络层。计算机 C 发现目的 IP 地址与本机的 IP 不同，从而丢弃这个 ARP 请求包。类似地，计算机 D 也丢弃这个 ARP 请求包。

STEP 3 MAC 地址表中的每一项都设置一个超时计时器，若超时，则删除该项，以适应拓扑结构的变化。

STEP 4 当某一帧到达网桥时，查询 MAC 地址表，若找到目的 MAC 地址，则向对应的端口转发。接着 **STEP 2** 的操作继续分析，计算机 B 收到计算机 A 的 ARP 请求包后，计算机 B 要发送 ARP 应答包，包格式的内容如图 2-2-8 所示。计算机 B 发出这个数据包。

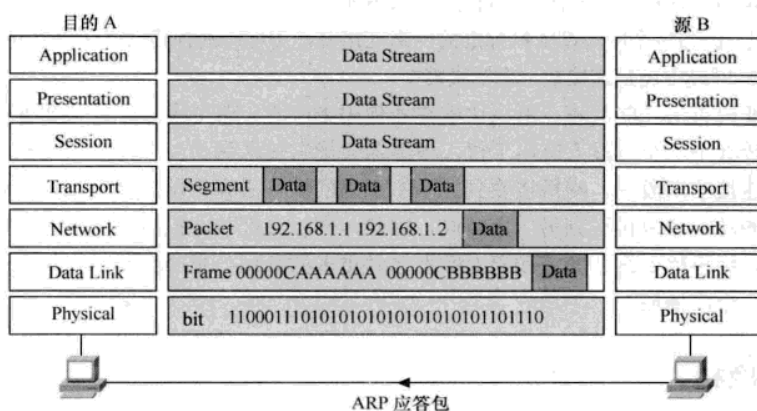


图 2-2-8 ARP 应答包格式

集线器 A 收到这个数据包，然后把数据包广播出去，计算机 A 和网桥都收到这个 ARP 应答包。计算机 A 从包的内容中可以看到计算机 B 对应的 MAC 地址，完成 ARP 的请求工作。网桥也收到计算机 B 的 ARP 应答包，查看数据帧的源 MAC 地址，发现 MAC 地址“0000CBBBBB”并没有出现在网桥的 MAC 地址表中，网桥添加该 MAC 地址和对应的端口到网桥的 MAC 地址表中。网桥继续查看数据帧的目的 MAC 地址，发现目的 MAC 地址“0000CAAAAA”已经存在于网桥的 MAC 地址表中，对应端口是 Port 1，这个数据帧来源的端口也是 Port 1。由于该数据帧的源和目的端口是网桥的同一个端口，网桥不转发这个数据帧到其他端口。计算机 C 和计算机 D 收不到这个数据包。

注意



如果网桥收到一个未知单播帧（在 MAC 地址表中找不到目的 MAC 地址），那么网桥向所有的端口（除了它接收端口外）广播该帧。

最后，网桥会学到所有 MAC 地址和端口的对应，如图 2-2-6 中的表所示。表中记录了计算机 A 和计算机 B 在网桥的 Port 1，计算机 C 和计算机 D 在网桥的 Port 2。

STEP 5 当网络拓扑结构出现环路时，应阻塞某些网桥的某些端口以消除环路，使网络呈现出生成树（Spanning Tree）结构，本书将在第 3 部分介绍生成树协议。

2. 源路由网桥

源路由网桥通常用于互连令牌环分段, 这种网桥实际中很少见。源路由网桥与透明网桥的工作原理不同。透明网桥使连网的主机表现出有连续网络分段的假象。源路由网桥不用决定在什么地方发送分组, 也不用建立主机 MAC 地址表。源路由网桥要求主机决定所有路由信息和路由发现。这意味着更多的通信路由信息产生, 假设网路上有比网桥更多的主机。

同中继器一样, 网桥也是连接两个网段的设备。但不同之处在于, 网桥能处理一个完整的帧, 并使用和计算机相同的接口设备。网桥以一种随机方式侦听每个网段上的信号, 当它从一个网段接收到一个帧时, 网桥会检查并确认该数据帧是否已经完整地到达, 并根据需要把该数据帧传送到其他网段。这样, 两个 LAN 网段通过网桥连接后, 就像一个 LAN 一样, 网中任何一台计算机可发送数据帧到任何其他计算机。因为每个网段都支持标准的网络连接并使用标准的帧格式, 计算机并不知道它们是连接在同一 LAN 网段中还是连接在一个桥接网中。

因为网桥能检查出一些故障, 所以比中继器使用更广泛。两个通过中继器相连的网段, 如果由于闪电而导致其中一个网段上有电干扰, 中继器会把它传送到另一个网段。相反, 如果干扰发生在通过网桥连接的网段中, 网桥接收到一个不正确的帧, 丢弃该帧。类似地, 网桥不会把从一个网段传送来的冲突信号传送到另一个网段。因此, 网桥会把故障控制在一个网段中而不会影响到另一个网段。网桥比中继器和集线器对数据包做更多的处理, 延时也相对增加, 一个网桥包括两个冲突域、一个广播域。

2.2.5 交换机

与网桥一样, 交换机也按每一个数据帧中的 MAC 地址相对简单地决定信息转发, 转发过程如图 2-2-9 所示。源主机“00000CAAAAAA”发送一个数据帧给目的主机“00000CBBBBBB”, 交换机收到这个数据帧后, 查找交换机的 MAC 地址表, 发现目的 MAC 地址在交换机的端口 2, 交换机从端口 2 把数据帧转发出去, 端口 3 和端口 4 端口不受影响。

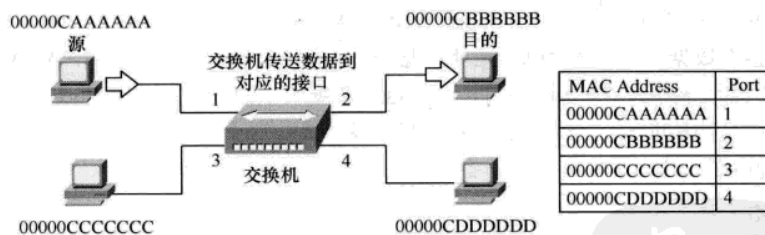


图 2-2-9 交换机的转发过程

类似传统的网桥, 交换机提供了许多网络互连功能。交换机的每个端口都是一个独立的冲突域, 可以为每个工作站提供更高的带宽。协议的透明性使得交换机在软件配置简单的情况下直接安装在多协议网络中; 交换机使用现有的电缆、中继器、集线器和工作站的网卡, 不必作高层的硬件升级; 交换机对工作站是透明的, 这样管理开销低廉, 简化了网络节点的增加、移动和网络变化的操作。

交换机根据功能来分, 可分为如下几种类型。

- (1) 传统的二层交换机与集线器相比, 仅是多了 MAC 地址表的功能。二层交换机属于 OSI

七层模型的数据链路层、有一个广播域、多个冲突域（每个端口就是一个冲突域）。

(2) VLAN 型交换机，可网管型交换机，比传统型交换机增加了 VLAN 的功能。它仍属于数据链路层，有多个广播域（每个 VLAN 就是一个广播域）、多个冲突域（每个端口就是一个冲突域），并可配置 IP 地址，方便远程管理。

(3) 三层交换机，比 VLAN 型交换机增加了路由功能，可以把三层交换机想象成路由器 + VLAN 型交换机，但三层交换机的数据包转发性能要比路由器 + VLAN 型交换机的性能高出许多倍。它属于 OSI 七层模型的网络层，具有多个广播域、多个冲突域。工程中出于安全的考虑，有时需要把 IP 和 MAC 进行绑定，这就需要三层以上的交换机才能完成，因为普通的二层交换机处在 OSI 七层模型的第二层，识别不了三层的 IP 地址，也就无法完成绑定。

有关交换机的更多介绍和配置，可参阅本书第 3 部分交换机的配置。

2.2.6 路由器

路由器是一种连接多个网络或网段的网络层设备，它能将不同网络或网段之间的数据信息进行“翻译”，以使它们能够相互“读懂”对方的数据，从而构成一个更大的网络。它不是应用于同一网段的设备，而是应用于不同网段或不同网络之间的设备。路由器之所以能在不同网络之间起到“翻译”的作用，是因为它不再是一个纯硬件设备，而是具有相当丰富路由协议的软、硬结构设备，如 RIP、OSPF、EIGRP、IPv6 协议等。这些路由协议就是用来实现不同网段或网络之间的相互“理解”。

路由器有两大典型功能，即数据通道功能和控制功能。数据通道功能包括转发决定、背板转发以及输出链路调度等，一般由特定的硬件来完成；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。

路由器具有判断网络地址和选择路径的功能，它能在多网络互联环境中，建立灵活的连接，可用完全不同的数据分组和介质访问方法连接各种子网。路由器属网络层的一种互连设备，有隔离广播的作用，它每个端口都是一个单独的广播域，也是一个单独的冲突域。

在局域网接入广域网的众多方式中，通过路由器接入 Internet 是最为普遍的方式。使用路由器互联网络的最大优点是各互联网仍保持各自独立，每个子网可以采用不同的拓扑结构、传输介质和网络协议，网络结构层次分明。通过路由器与互联网相连，则可完全屏蔽公司内部网络，有些路由器内部还集成了入侵防御和防火墙功能，因此使用路由器上网可以防御攻击，保护内部网络的安全。

从本质上说，路由器也是一台计算机，其操作系统是在计算机引导时从 FLASH 中装入内存的。随着 Internet 和企业网络的不断普及，路由器这种网络设备也被大量地采用。目前，市场上的路由器品牌很多，其中 Cisco 路由器使用广泛。不过我国的华为，经过近 20 年的发展，也已经非常强大，在一定程度上它几乎成为了 Cisco 公司最具有竞争力的对手之一。近年来锐捷公司也是异军突起，该公司的产品配置命令行与 Cisco 路由器相仿，熟悉 Cisco 设备的工程师易于上手。有关 Cisco 路由器的更多介绍和配置，可参阅本书第 3 部分路由器的配置。

2.2.7 网关

网关 (Gateway) 是在连接两个协议差别很大的计算机网络时使用的设备。它可以将具有不同体系结构的计算机网络连接在一起。在 OSI 七层模型中，网关属于最高层（应用层）的设备。

网关的实现非常复杂,工作效率也很难提高,一般只提供有限的几种协议转换功能。常见的网关设备都是用在网络中心的大型计算机系统之间的连接上,为普通用户访问更多类型的大型计算机系统提供帮助。

当然,有些网关可以通过软件来实现协议转换操作,并能起到与硬件类似的作用。但它是以降低机器的运行效率作为代价的。

网关在概念上与网桥相似,它与网桥的不同之处就在于网关是用来实现不同局域网的连接;网关建立在应用层,网桥建立在数据链路层;网关比起网桥有一个主要的优势,它可以将具有不相容的地址格式的网络相连起来。

2.2.8 宽带路由器

多功能宽带路由器是专门为满足小型企业办公和家庭上网需要而设计的,它性能优越且配置简单,提供多方面的管理功能,可对系统、DHCP (Dynamic Host Configuration Protocol, 动态主机配置协议) 服务器、虚拟服务器、DMZ (Demilitarized Zone, 隔离区或非军事化区) 主机、防火墙、上网权限管理、静态路由表等进行管理。同时用户界面友好,配置简单易用,最主要的是价格便宜(最便宜的宽带路由器只需要 100 多元)。常用的一款宽带路由器产品是 TP_LINK, 它的 Web 管理界面如图 2-2-10 所示。

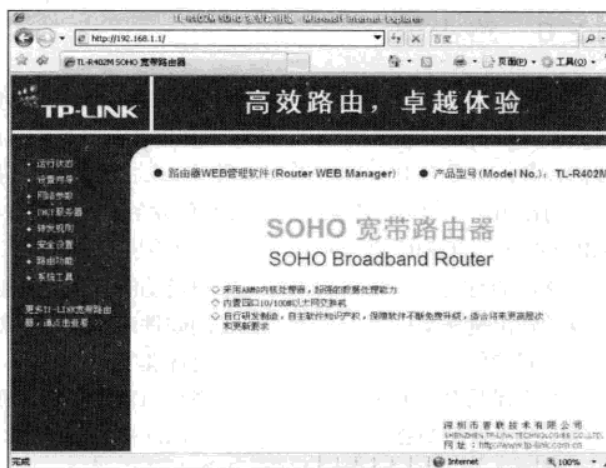


图 2-2-10 TP_LINK 无线宽带路由器 Web 管理界面

2.2.9 防火墙

防火墙是指设置在不同网络(如可信任的企业内部网和不可信的公共网)或网络安全域之间的一系列部件的组合。它是不同网络或网络安全域之间信息的唯一出入口,能根据企业的安全政策控制(允许、拒绝、监测)出入网络的信息流,且本身具有较强的抗攻击能力。它是提供信息安全服务,实现网络和信息安全的基础设施,可以有效地监控内部网和 Internet 之间的任何活动,保证内部网络的安全。防火墙的功能主要有如下几点。

(1) 防火墙是网络安全屏障。一个防火墙(作为阻塞点、控制点)能极大地提高一个内部网络的安全性,并通过过滤不安全的服务而降低风险。由于只有经过精心选择的应用协议才能通过防火墙,所以网络环境变得更安全。如防火墙可以禁止诸如众所周知的不安全的 NFS 协议进出受保护网络,这样外部的攻击者就不可能利用这些脆弱的协议来攻击内部网络。防火墙同时可以保护网络免受基于路由的攻击,如 IP 选项中的源路由攻击和 ICMP 重定向中的重定向路径。防火墙可以拒绝所有以上类型攻击的报文并通知防火墙管理员。

(2) 防止内部信息的外泄。通过利用防火墙对内部网络的划分,可实现内部网中重点网段的隔离,从而限制了局部重点或敏感网络安全问题对全局网络造成的影响。隐私是内部网络非常关心的问题,一个内部网络中不引人注意的细节可能包含了有关安全的线索而引起外部攻击者的兴趣,甚至因此而暴露了内部网络的某些安全漏洞。使用防火墙就可以隐蔽那些透漏内部细节的服务,如 Finger、DNS 等。

除了安全作用,防火墙还支持 NAT(Network Address Translation)、VPN(Virtual Private Network)等。通过 NAT 可实现企业共享上网。通过 VPN 将企事业单位在地域上分布在各地的 LAN 或专用子网有机地连成一个整体,不仅省去了专用通信线路,而且为信息共享提供了安全保障。

2.3 双绞线的制作

制作双绞线是练习计算机网络动手能力的的第一步,掌握双绞线的制作是组建星型结构以太网的必要技术之一,同时也是日常网络维护的内容之一。

2.3.1 双绞线的种类

双绞线根据应用场合不同有 3 种制作方法。

1. 直通线

双绞线两端接入 RJ-45(水晶头)的线序相同,即橙白(与橙色绞在一起的那根白色)、橙、绿白、蓝、蓝白、绿、棕白、棕,这种线序标准为 T568B,还有一种线序标准为 T568A,如图 2-3-1 所示。目前,中国普遍使用的是 T568B 标准。这种线主要用于不同种设备的互连,如计算机—交换机、计算机—集线器、交换机—路由器之间的互连等。

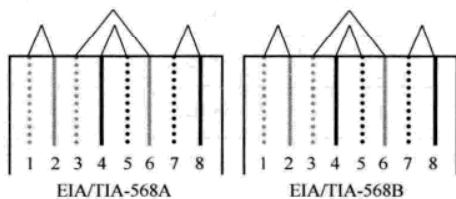


图 2-3-1 EIA/TIA-568 标准分类

2. 交叉线

双绞线两端接入 RJ-45 的线序不同,一端保持 T568B 的线序,另一端使用 T568A 标准(也就是把 T568B 标准中 1 和 3、2 和 6 互换)。双绞线中有 8 根,为何只交叉其中的 4 根呢?在要求不高的情况下,真正用于数据传输的只有 1、2、3、6 这 4 根线,剩下 4、5、7、8 这 4 根线主要起到屏蔽等辅助作用。而且有些工程中只有一根双绞线接入,计算机和电话却都可以使用,这是因为施工人员为图方便,偷工减料,把双绞线中不用的 4 根挪用出两根给了电话。这种线主要用于同种设备的互连,如计算机—计算机、路由器—路由器、集线器—集线器、交换机—交换机、交换机—集线器之间,尤其值得注意的是“计算机—路由器”也用此种线缆,因为路由器起源于计算机,从工作原理到硬件配置都非常相似。

3. 全反线

双绞线两端接入 RJ-45 的线序完全相反,这种线主要用于对路由器和交换机进行初始配置之

用，有时也用于异步传输。

随着技术的发展，现在有些新款集线器或交换机能自动识别所接设备的类型，并调整接口状态，自动适应线缆的类型。

2.3.2 水晶头的针脚

实际应用中要注意区分 RJ-45 和 RJ-11，RJ-11 只有 4 根针脚，用于电话线接头，而 RJ-45 有 8 根针脚，用于以太网连接。RJ-11 连接器在形状上明显小于 RJ-45 连接器。

RJ-45 水晶头包括两端，一端是插头，另一端是插孔。插头可以接入机器、交换机或路由器的以太网接口上，而插孔和连接导线（现在最常用的就是采用非屏蔽双绞线的 5 类线）相连。EIA/TIA（电子工业协会 EIA 和电信工业协会 TIA 开发了一个叫做 EIA/TIA-568 商用建筑布线标准的商业建筑电信布线标准）制定的布线标准规定了 8 根针脚的编号。

将 RJ-45 的插头端面对眼睛，并使带有 8 个铜质接触点的一面在下方，那么最左边是①，最右边是⑧，如图 2-3-2 所示。

在 10Mbit/s 和 100Mbit/s 以太网中只使用两对导线，也就是说，只使用 4 根针脚。标准规定使用的 4 根针脚是 1、2、3 和 6，1 和 2 用于发送，3 和 6 用于接收，如表 2-3-1 所示。

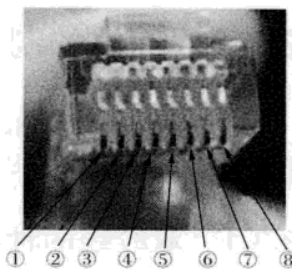


图 2-3-2 RJ-45 针脚编号

表 2-3-1 RJ-45 针脚作用表

针 脚 编 号	作 用
针脚 1	发送+
针脚 2	发送-
针脚 3	接收+
针脚 4	不使用
针脚 5	不使用
针脚 6	接收-
针脚 7	不使用
针脚 8	不使用

不同颜色的 4 对双绞线与针脚连接。EIA/TIA-568 标准规定了两种连接标准（并没有实质上的差别），即 EIA/TIA-568A 和 EIA/TIA-568B，如图 2-3-1 所示，上方的折线表示这两根针脚连接的是一对双绞线。结合图 2-3-2 所示，每个引脚对应线的颜色如下。

T568A 规定的线序如下。

- ①——绿白（白色的外层上有些绿色，表示和绿色的是一对线）
- ②——绿色
- ③——橙白（白色的外层上有些橙色，表示和橙色的是一对线）

- ④——蓝色
- ⑤——蓝白（白色的外层上有些蓝色，表示和蓝色的是一对线）
- ⑥——橙色
- ⑦——棕白（白色的外层上有些棕色，表示和棕色的是一对线）
- ⑧——棕色

T568B 规定的线序如下。

- ①——橙白
- ②——橙色
- ③——绿白
- ④——蓝色
- ⑤——蓝白
- ⑥——绿色
- ⑦——棕白
- ⑧——棕色

这里特别要强调一下，线序是不能随意改动的。例如，从上面的连接标准来看，1 和 2 是一对线，而 3 和 6 又是一对线。但如果将以上规定的线序弄乱，例如，将 1 和 3 用做发送的一对线，而将 2 和 4 用做接收的一对线，那么这些连接导线的抗干扰能力就要下降，误码率就可能增大，就不能保证以太网的正常工作。

实验 2-3 制作双绞线的具体步骤

上面介绍了 RJ-45 连接器 8 根针脚的编号规定和不同颜色的 4 对双绞线应当连接到哪一个针脚的规定。下面介绍 RJ-45 连接器的制作。

STEP 1 准备好五类线、RJ-45 插头和一把专用的压线钳，如图 2-3-3 所示。

STEP 2 用压线钳的剥线刀口将五类线的外保护套管划开，小心不要将里面的双绞线的绝缘层划破，刀口距五类线的端头至少 2cm，如图 2-3-4 所示。

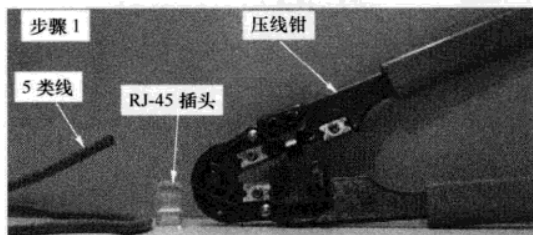


图 2-3-3 做线工具

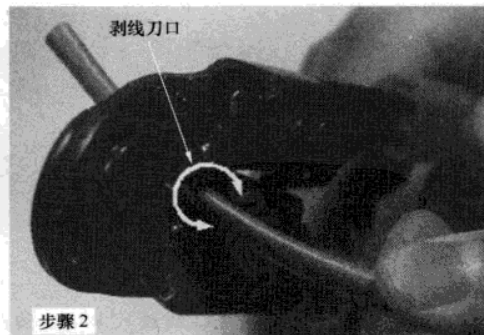


图 2-3-4 剥线

STEP 3 将划开的外保护套管剥去（旋转、向外抽），如图 2-3-5 所示。

STEP 4 露出五类线电缆中的 4 对双绞线，如图 2-3-6 所示。

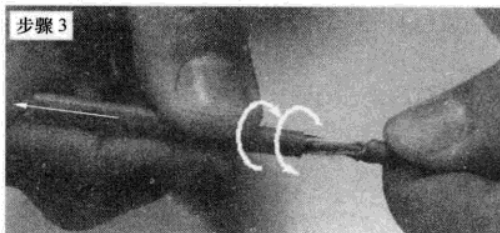


图 2-3-5 去线

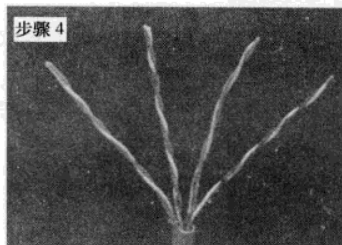


图 2-3-6 剥去保护层的双绞线

STEP 5 按照 EIA/TIA-568B 标准和导线颜色将导线按规定的序号 (橙白、橙色、绿白、蓝色、蓝白、绿色、棕白、棕色) 排好, 如图 2-3-7 所示。

STEP 6 将 8 根导线平坦整齐地平行排列, 导线间不留空隙, 如图 2-3-8 所示。

STEP 7 准备用压线钳的剪线刀口将 8 根导线剪断, 如图 2-3-9 所示。

STEP 8 剪断电缆线。注意一定要剪得很整齐。剥开的导线长度不可太短 (10~12mm), 也不可太长。不要剥开每根导线的绝缘外层, 如图 2-3-10 所示。

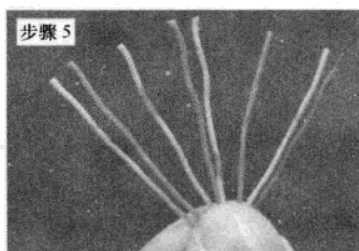


图 2-3-7 排线序

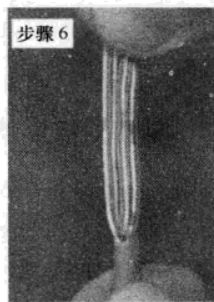


图 2-3-8 理线

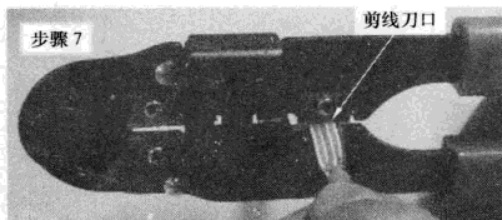


图 2-3-9 剪线

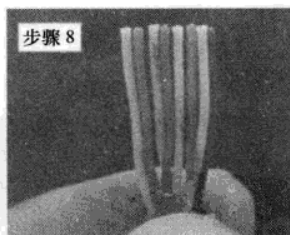


图 2-3-10 剪好的线

STEP 9 将剪断的电缆线放入 RJ-45 插孔中, 试试长短, 要能插到底, 确保每一根线都能接触到铜片, 电缆线的外保护层最后应能够在 RJ-45 插头内的凹陷处被压实, 以便使做好的线更牢固, 如图 2-3-11 所示。

STEP 10 在确认一切都正确后 (特别要注意不要将导线的顺序排反), 将 RJ-45 插头放入压线钳的压头槽内, 准备最后的压实, 如图 2-3-12 所示。

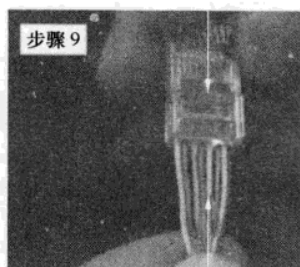


图 2-3-11 把线按序插入 RJ-45

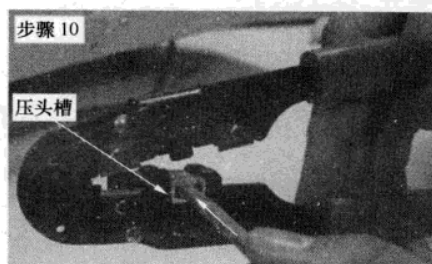


图 2-3-12 准备压线

STEP 11 双手紧握压线钳的手柄，用力压紧，如图 2-3-13 所示。注意，在这一步骤完成后，插头的 8 个针脚接触点就穿过导线的绝缘外层，分别和 8 根导线紧紧地压接在一起。

STEP 12 完成后的双绞线如图 2-3-14 所示。



图 2-3-13 压线

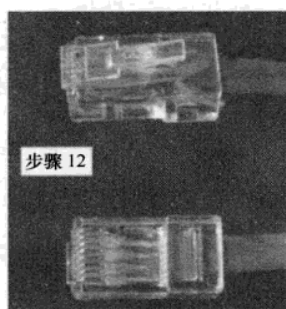


图 2-3-14 完成后的双绞线

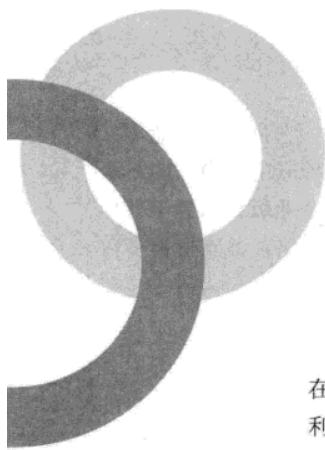
至此，就完成了双绞线一端的制作，另一端的线序需根据应用场合，选择直连、交叉或全反线序。

Part

02

第 2 部分 服务器架设和管理篇

上一篇介绍了网络的基础知识和常用的网络设备，相信大家“功”练得不错了，接下来就要开始习武，本篇主要介绍微软服务器平台上各种服务的搭建和应用。通过学习本篇，读者可以管理 Windows Server 2003 服务器，并能配置 DHCP、DNS、WWW(World Wide Web)、E-mail、视频、证书等基于 Windows Server 2003 的服务。



第3章 Windows Server 2003 安装和配置

Chapter 3

本章主要介绍 Windows Server 2003 的安装和初始配置,重点讲述使用 VMware 软件在单台计算机上虚拟搭建本篇要使用到的网络实验环境。成功搭建本章实验环境是顺利完成本篇后续章节学习的前提条件。尽管更新的服务器操作系统 Windows Server 2008 已经面世,本书仍以 Windows Server 2003 为系统平台,介绍各种服务和应用的配置,因为该版本经过几年的完善和考验,是目前使用最多的服务器操作系统,也是最稳定的服务器操作系统。掌握 Windows Server 2003 中的各种应用和配置,将来也可以很容易地上手 Windows Server 2008。

3.1 安装 Windows Server 2003

Windows Server 2003 是微软公司开发的新一代网络服务器操作系统,与以前的同类操作系统相比,它更加安全、性能更加稳定,而操作和使用却更加轻松。它不仅能够被安装和部署到服务器,担当域控制器服务器、文件服务器等各种服务器,也能安装在局域网的普通计算机上,成为更加稳定、更加安全、更容易使用的个人操作系统。本节主要介绍 Windows Server 2003 操作系统版本的选择和操作系统的安装步骤。

3.1.1 选择版本

如果将 Windows Server 2003 作为服务器来使用,那么建议用户选择英文版,因为英文版对某些计算机病毒具有天生的免疫力,且中文版补丁的推出一般要滞后英文版补丁的推出一周左右,也就是说在漏洞出现后一周左右的时间,中文版操作系统都是高度危险的。Windows Server 2003 与以往的 Windows 2000 Server 一样,也推出了几个不同版本,即标准版、企业版、数据中心版、Web 版,它们可以支持不同的硬件设备,具备不同的性能特点,并提供不同的网络服务,用户可以根据自己的网络需求进行选择。

1. Windows Server 2003 Standard (标准版)

Windows Server 2003 标准版是一个可靠的网络操作系统,可迅速灵活地提供各种不同的企业

解决方案。这种灵活的服务器版本是小型企业和部门应用的理想选择。标准版最多可支持 4 个处理器, 主要用于提供文件和打印共享, 以及安全的 Internet 连接, 并且它允许集中化的桌面应用程序部署。但是需要注意的是, 该版本并不支持集群服务。

2. Windows Server 2003 Enterprise (企业版)

Windows Server 2003 企业版是为满足各种规模企业的一般用途而设计的, 它是一种功能丰富的服务器操作系统, 可提供高可靠性、高性能和出色的商业价值, 是构建各种应用程序、Web 服务和基础结构的理想平台。企业版最多能支持 8 个 CPU 和 64 位计算平台。企业版在功能上与标准版基本相同, 只是提供了对更高硬件系统的支持, 因此可用于更大规模的网络, 并支持更多数量的用户和更为复杂的网络应用。

3. Windows Server 2003 Data Center (数据中心版)

Windows Server 2003 数据中心版是企业所需的应用程序而设计的, 这些应用程序需要高的可伸缩性和可用性, 是微软所开发的功能非常强大的服务器操作系统。它可支持高达 32 路的 SMP (Symmetrical Multi-Processing, 对称多处理) 和 64GB 的 RAM (Random Access Memory, 随机存取内存), 提供 8 节点集群和负载均衡服务等标准功能, 可用于支持 64 位处理器和 512GB 内存的 64 位计算机平台。

4. Windows Server 2003 Web 版

Windows Server 2003 Web 版是 Windows 系列中的新产品, 它主要作为 Web 服务器来使用, 用于生成和承载 Web 应用程序、Web 页面以及 XML Web 服务, 提供一个快速开发和部署 XML Web 服务和应用程序的平台, 以实现 Web 服务和托管。Web 版有较大的功能限制, 无法单独用于执行强大的管理功能, 但优点是成本较低。与标准版相同的是, 它也不支持服务器的集群服务。

本篇将以 Windows Server 2003 企业版为例, 介绍 Windows Server 2003 的安装、管理、配置。

3.1.2 安装前的准备工作

首先要保证系统配置符合要求。Windows Server 2003 对系统硬件的要求并不高, 建议计算机的 CPU 主频不低于 550MHz (支持的最低主频为 133MHz); 建议系统内存在 256 MB 以上 (最小支持 128MB, 最大支持 32GB); 硬盘分区要具有足够的可用空间, 最小要在 2GB 以上; VGA 或更高分辨率的监视器 (建议使用 SVGA 800×600 或更高); 配备键盘和鼠标; 对于大多数用户来说, 由于要通过光驱来安装操作系统, 所以用于读取安装光盘的 CD-ROM 或者 DVD-ROM 是必不可少的。

其次确保切断 UPS 设备。如果目标计算机与不间断电源 (UPS) 设备相连, 那么在运行安装程序之前断开正在连接的串行电缆。因为安装程序将自动检测连接到串行端口的设备, 而 UPS 设备可能导致在检测过程中出现问题。

断开任何网络连接。计算机在安装过程中, 可能存在大量系统漏洞, 防护系统比较脆弱, 尤其易受病毒感染和黑客攻击。

3.1.3 安装步骤

无论是服务器还是普通计算机，安装 Windows Server 2003 都是非常轻松的。具体的步骤如下。

STEP 1 设置光盘引导。放入 Windows Server 2003 安装光盘，启动计算机时进入 CMOS 设置，把光盘引导调整到硬盘引导之前，如图 3-1-1 所示。保存配置后，重新启动计算机，计算机从光盘引导。

STEP 2 开始安装。系统首先要读取必需的启动文件，接下来询问用户是否安装此操作系统，按“Enter”键确认安装，按“R”键进行修复，按“F3”键退出安装，如图 3-1-2 所示。这里按“Enter”键继续。

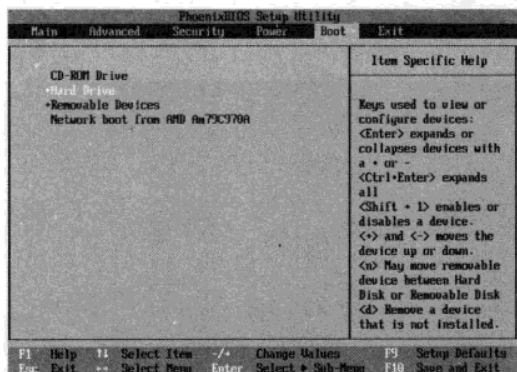


图 3-1-1 设置光盘引导

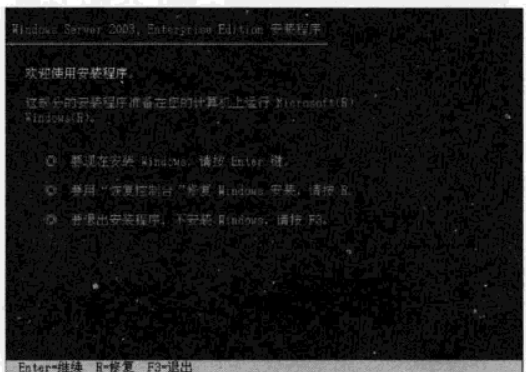


图 3-1-2 开始安装

STEP 3 授权许可。接下来出现软件的授权协议，必须按“F8”键，同意微软协议才能继续进行。

STEP 4 分区选择。安装程序搜索系统中已安装的操作系统，并询问用户将操作系统安装到计算机的哪个分区中。如果是一块没有分区的硬盘，会询问是否直接安装，还是创建磁盘分区，如图 3-1-3 所示。如果按“Enter”键直接安装，则硬盘只有一个分区，这里建议至少建立两个分区，前者用作系统分区，后者用作应用程序分区。

如果是一块没有分区的硬盘，建议按“C”键，选择“创建磁盘分区”，打开如图 3-1-4 所示的窗口，在“创建磁盘分区大小（单位 MB）：”栏中输入第一个分区的大小，如 4000MB。

图 3-1-4 中，按“Enter”键返回分区选择界面，依上面的方法再创建第二个分区，结果如图 3-1-5 所示。

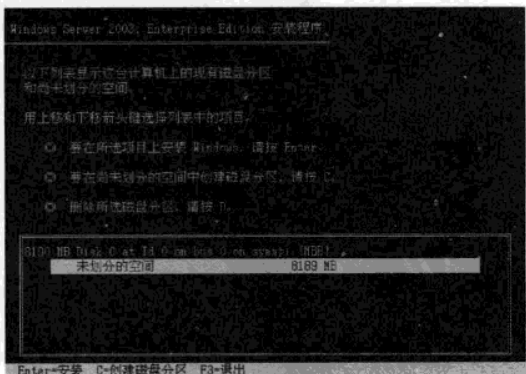


图 3-1-3 选择磁盘分区



图 3-1-4 创建磁盘分区大小



图 3-1-5 创建完成的分区

在图 3-1-5 中，选择“C:”分区后，按“Enter”键，系统提示选择的磁盘分区没有经过格式化，选择“用 NTFS 文件系统格式化磁盘分区”，如图 3-1-6 所示。选择使用 NTFS 分区主要是为了获得高安全性能。系统开始格式化 C 分区，格式化完成后开始从光盘复制安装文件到 C 分区，文件复制完成后，系统自动重启。

STEP 5 区域和语言选项。保持默认，直接单击“下一步”按钮继续。

STEP 6 提供个人信息。在姓名和单位栏中输入相关信息。

STEP 7 提供产品序列号。在光盘的封套或者说明书中找到这个序列号，输入到如图 3-1-7 所示的“产品密钥”输入框中，单击“下一步”按钮继续。



图 3-1-6 格式化磁盘分区

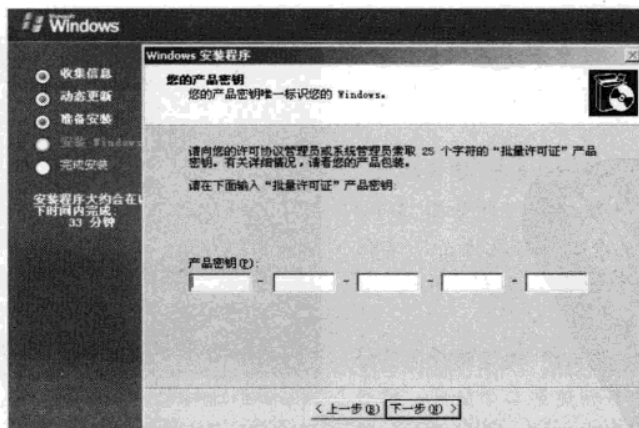


图 3-1-7 输入产品序列号

STEP 8 选择授权模式。如图 3-1-8 所示，保持默认选项，单击“下一步”按钮继续。

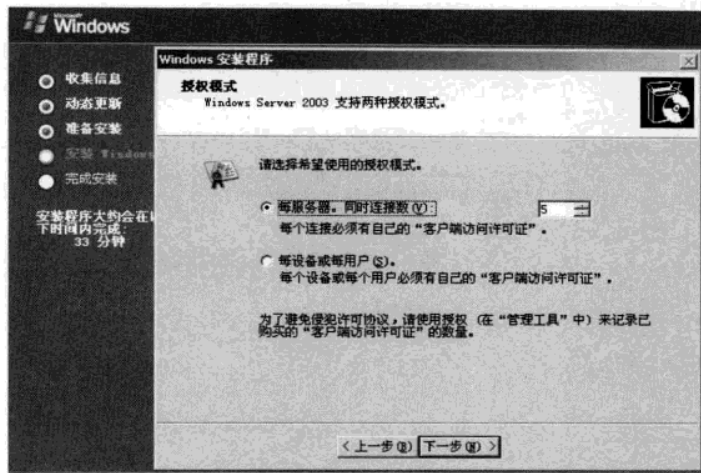


图 3-1-8 选择授权模式

STEP 9 设置计算机名称和管理员密码。如图 3-1-9 所示，设置计算机的名称和系统管理员的密码，计算机的名称不能与局域网内其他计算机的名称相同，管理员的密码设置要安全，最好是数字、大小写字母、特殊字符相结合，然后单击“下一步”按钮继续。

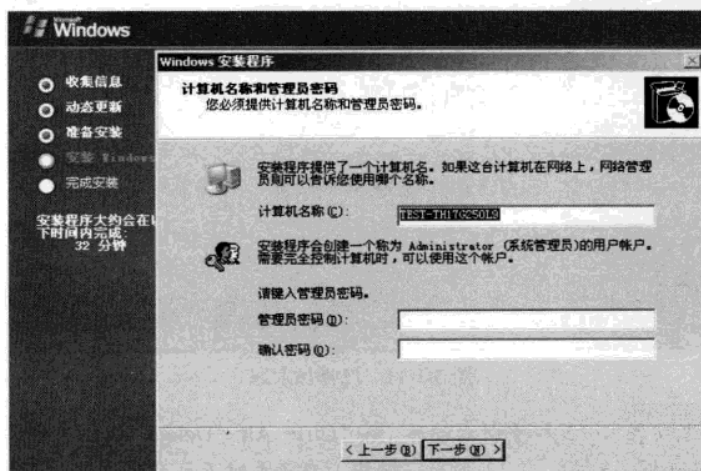


图 3-1-9 设置计算机名和管理员密码

STEP 10 设置时区、日期和时间。保持默认，单击“下一步”按钮继续。

STEP 11 网络的设置。如图 3-1-10 所示，可以选择“典型设置”，在安装完后再进行调整。

STEP 12 域选项。询问该计算机是否需要加入域，这里选择不要加入域，如图 3-1-11 所示。如果需要加入域时，可以再进行相关配置。单击“下一步”按钮继续。接下来，系统将安装开始

菜单项、对组件进行注册、保存设置等操作，这些都无需用户参与，所有的操作完成后，系统进行第二次自动重启。

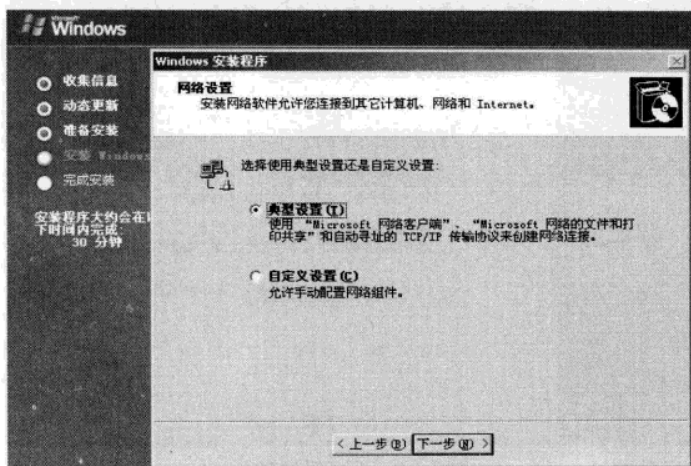


图 3-1-10 网络设置

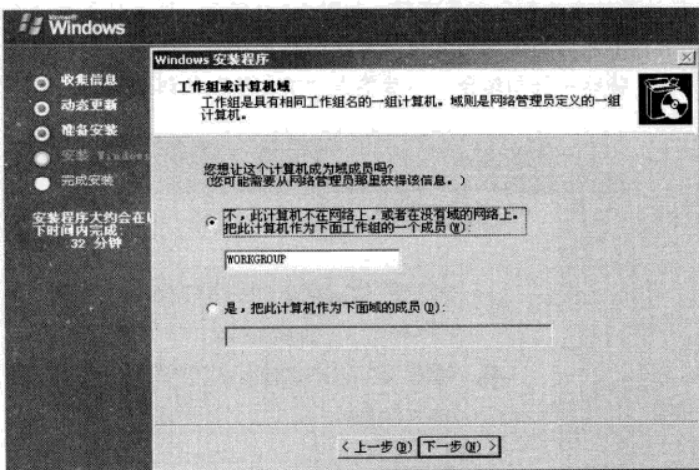


图 3-1-11 选择加入域

STEP 13 完成安装。计算机重新启动后，按“Ctrl + Alt + Delete”组合键登录系统。弹出“管理您的服务器”对话框，如图 3-1-12 所示。选中“在登录时不要显示此页”，并关闭该对话框，这里暂不进行相关服务的配置。至此，完成了 Windows Server 2003 的安装。

注意



如果计算机厂商没有提供针对 Windows Server 2003 的硬件驱动（尤其是笔记本电脑，一般厂商都不提供针对 Windows Server 2003 的硬件驱动），在多数情况下，用户可以使用厂商提供的针对 Windows XP 的硬件驱动来替代。

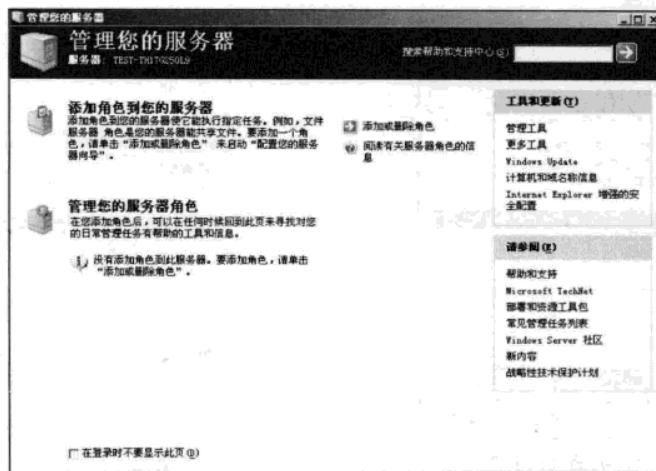


图 3-1-12 管理服务器

3.2 Windows Server 2003 的初始设置

3.2.1 启用操作系统自带的防火墙

Windows Server 2003 自带了简易的基于包过滤的防火墙——ICF (Internet Connection Firewall)，如果仅作为个人操作系统用，建议用户启用 ICF，防火墙能有效的防止黑客的主动攻击。右键单击“网上邻居”→“属性”，在“网络连接”窗口中，右键单击对应网卡，在弹出的快捷菜单中选择“属性”，打开如图 3-2-1 所示的对话框。在“高级”选项卡中选中复选框，启用操作系统的 Internet 连接防火墙。

如果服务器需要运行某些服务的时候，就需要对 ICF 进行一些简单的配置，使防火墙对外开放相应的服务端口。

一般情况下，启用 ICF 时并没有开放 80 端口，为什么用户还是能够访问外部的网站呢？启用防火墙后本机将封闭所有端口，不接受外部主动发起的连接，也不能对外提供服务，但并不意味着本机不可以访问外网，实际上启用防火墙的计算机和没有启用防火墙的计算机访问网络几乎没有差别。如图 3-2-1 所示，当启用了 Internet 连接防火墙后，再单击图 3-2-1 右下脚的“设置”按钮，即可对 ICF 进行配置。如果该计算机还需对外提供 WWW 服务，需要选中“Web 服务器 (HTTP)”来对外开放 80 端口，如图 3-2-2 所示。

当然用户也可以自定义一个对外开放的端口并给它命名。如图 3-2-2 所示，单击“添加”按钮，打开如图 3-2-3 所示对话框。

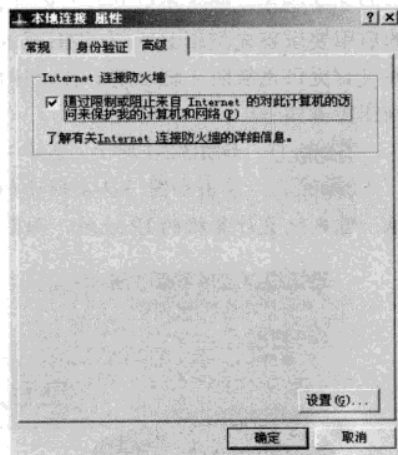


图 3-2-1 启用防火墙

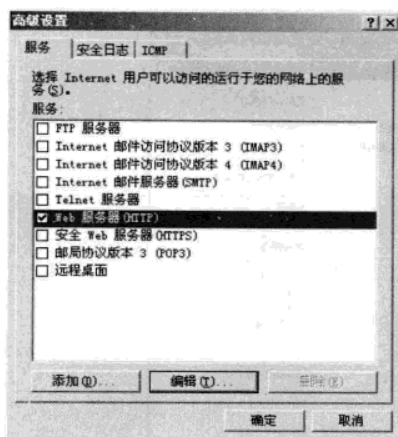


图 3-2-2 防火墙高级设置

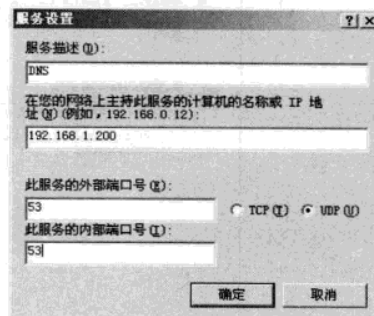


图 3-2-3 防火墙的服务设置

依次填入服务描述、本计算机的 IP 地址、此服务使用的外部和内部端口号，以及选择该服务使用的是 TCP 还是 UDP。最后单击“确定”按钮，完成对特殊端口的设置。

实验 3-1 利用 TCP/IP 筛选技术配置计算机的防火墙

虽然 Windows Server 2003 内置的防火墙配置简单，但它是基于后台的 ICF 服务得以运行的，可能和某些系统服务不能共存。例如，RRA (Routing & Remote Access，路由与远程访问) 服务的启用要求首先禁用 ICF。有些旧版本的系统，如 Windows 2000 Server、Windows 2000 Professional 并没有提供系统防火墙功能。在上述情况下，通过配置 TCP/IP 筛选技术，可以实现防火墙功能，操作步骤如下。

STEP 1 如图 3-2-1 所示，选择“常规”选项卡，选中“Internet 协议 (TCP/IP)”，如图 3-2-4 所示。

STEP 2 单击如图 3-2-4 所示的“属性”按钮，打开“Internet 协议 (TCP/IP) 属性”对话框，首先配置计算机的 IP 地址，如图 3-2-5 所示。

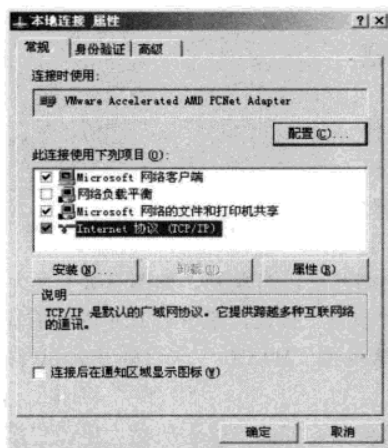


图 3-2-4 配置 Internet 协议

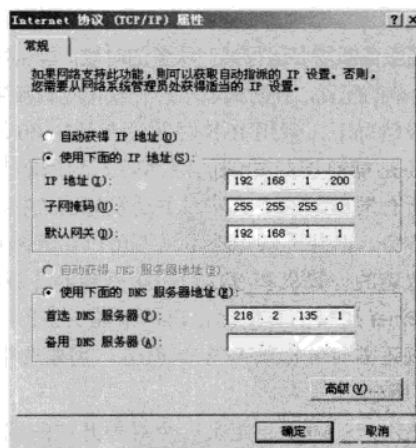


图 3-2-5 Internet 协议对话框

STEP 3 单击如图 3-2-5 所示的“高级”按钮，打开“高级 TCP/IP 设置”对话框，如图 3-2-6 所示。

STEP 4 选择如图 3-2-6 所示的“选项”选项卡，如图 3-2-7 所示。

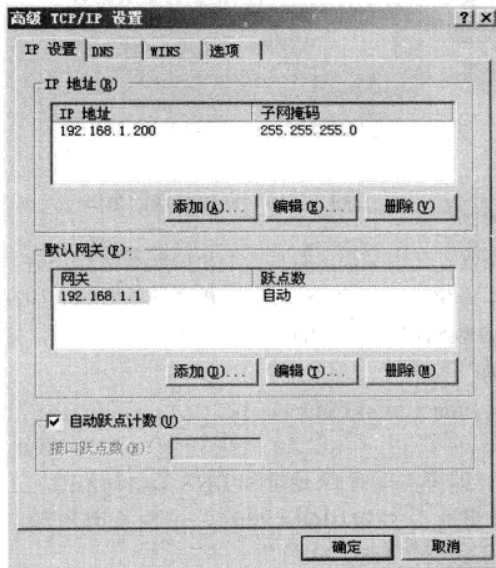


图 3-2-6 高级 TCP/IP 设置

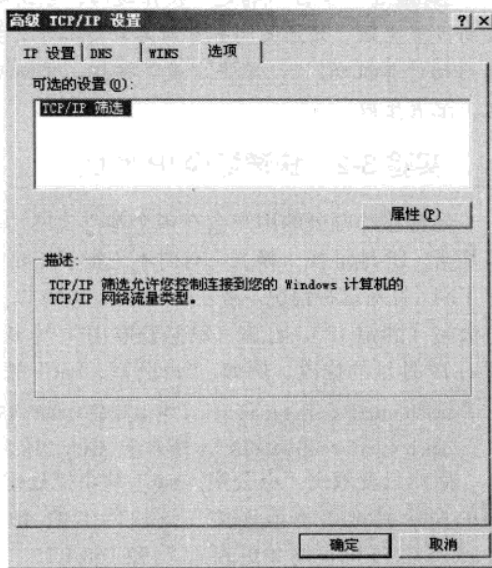


图 3-2-7 高级 TCP/IP 设置的选项

STEP 5 单击如图 3-2-7 所示的“属性”按钮，打开“TCP/IP 筛选”对话框，如图 3-2-8 所示。默认情况下，计算机不启用 TCP/IP 筛选，所有 TCP 和 UDP 的端口均对外开放。

STEP 6 启用防火墙。如图 3-2-9 所示操作，选中“启用 TCP/IP 筛选（所有适配器）”复选框，并选中 TCP 端口上方的“只允许”，这样该计算机的所有 TCP 端口均对外关闭，但对外界的访问不受影响。如果不需要进行域名解析，还可以把所有的 UDP 端口也关闭，但一般的计算机都需要使用域名访问网络，UDP 端口保持默认的“全部允许”。

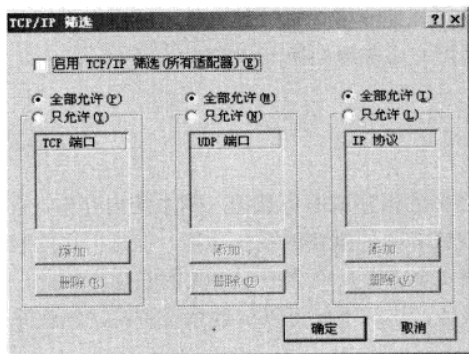


图 3-2-8 TCP/IP 筛选对话框

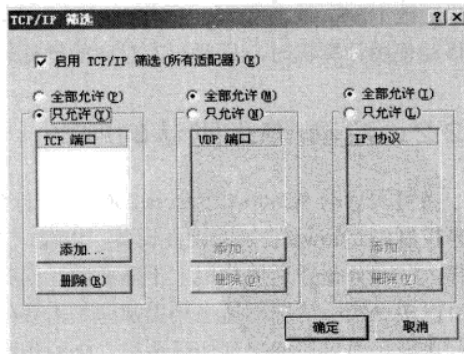


图 3-2-9 关闭所有 TCP 端口

STEP 7 开放特殊的端口。假如该计算机需要对外提供 WWW 服务，如图 3-2-9 所示，单击

TCP 端口下的“添加”按钮，打开“添加筛选器”对话框，在对话框中输入“80”端口，如图 3-2-10 所示。如果还有其他的服务，则依次添加相应的端口。

STEP 8 单击“确定”按钮返回。系统提示“要使新设置生效，必须关闭并重新启动计算机。要立即重新启动计算机吗？”，单击“是”按钮，重新启动计算机，配置生效。

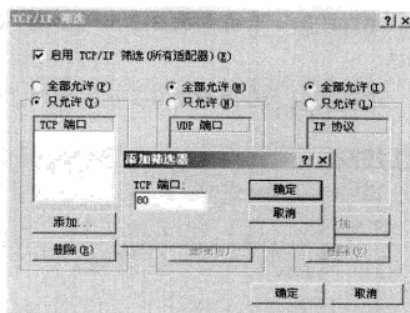


图 3-2-10 开放特殊的端口

实验 3-2 快速切换 IP 地址

经常移动办公的用户会在多个地点上网，笔记本随身携带，IP 地址换来换去，有时不记得了还要咨询网管、查询文档，而且一不小心配置错误还会上不了网。针对这种情况，微软 Windows 2000 以上版本提供了采用命令行修改 IP 地址的方法，如在办公室（固定 IP）、在家（动态获取 IP）等多个地方频繁移动，就可以建立多个批处理文件，实现对 IP 地址的修改。例如，“办公室.bat”的内容如下。

```
netsh interface ip set address "本地连接" static 192.168.1.200 255.255.255.0 192.168.1.1 1
netsh interface ip set dns "本地连接" static 218.2.135.1
```

用户只要双击“办公室.bat”这个批处理文件，即可实现对 IP 地址和 DNS 的自动修改。上面的命令将把“本地连接”这块网卡的 IP 地址更改为“192.168.1.200”，子网掩码更改为“255.255.255.0”，网关更改为“192.168.1.1”，DNS 更改为“218.2.135.1”。

注意



网关后面的那个“1”，是指从计算机到网关有一跳，配置时不要遗漏。

“家.bat”的内容如下。

```
netsh interface ip set address "本地连接" dhcp
netsh interface ip set dns "本地连接" dhcp
```

只要双击“家.bat”这个批处理文件，即可把 IP 和 DNS 都设置为自动获取。如果只更改 IP 或只更改 DNS，文件中写一行就可以了。类似的方法可以建立多个批处理文件，以后在不同的场所移动使用计算机时，只要双击对应的批处理文件即可完成快速切换 IP 地址。

3.2.2 启动/停止默认的服务

当每次启动 Windows Server 2003 时，总会有相当多的程序或服务被调入到系统内存中，它们用来控制 Windows 系统的硬件设备、内存、文件管理或者其他重要的系统功能。但是，这些服务有很大一部分是普通用户根本不需要的，同时在系统安全方面反而会造成很大的隐患。因此，完全可以根据实际情况，适当禁用那些不需要的系统服务，这样不仅可以节约系统资源，加快系统运行速度，而且还能起到加强系统安全的作用。

首先以管理员或 Administrators 组成员身份登录，单击“开始”→“运行”命令，在出现的对话框中键入“Services.msc”并按下回车键，即可打开“服务管理控制台”，如图 3-2-11 所示。也

可以选择“开始”→“管理工具”→“服务”来启动该控制台。

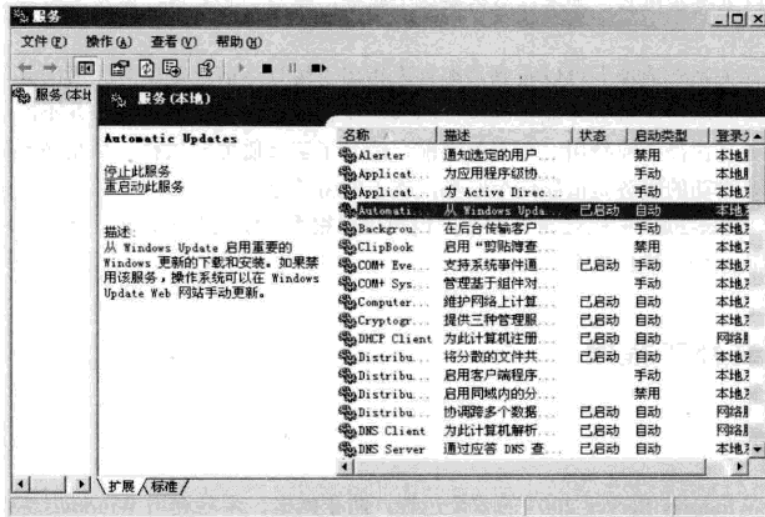


图 3-2-11 服务控制台

然后在服务控制台中，双击任意一个服务，就可以打开该服务的属性对话框，如图 3-2-12 所示。在这里可以对服务进行配置、管理，也可更改服务的启动类型。

在“常规”选项卡中，“服务名称”是指服务的“简称”，并且也是在注册表中显示的名称；“显示名称”是指在服务配置界面中每项服务显示的名称；“描述”是为该服务作的简单解释；“可执行文件的路径”是指该服务对应的可执行文件的具体位置；“启动类型”是整个服务配置的核心。对于任意一个服务，通常都有 3 种启动类型，即自动、手动和禁用，只要从下拉菜单中选择就可以更改服务的启动类型。“服务状态”是指服务的现在状态是启动还是停止，用户通常可以利用下面的“启动”、“停止”、“暂停”、“恢复”按钮来改变服务的状态。下面具体介绍 3 种不同类型的启动状态。

● 自动：此服务随着系统启动时启动，它将延长系统启动所需要的时间。有些服务是必须设置为自动的，如 Remote Procedure Call (RPC)。由于依存关系或其他影响，其他的一些服务也必须设置为自动，这样的服务最好不要去更改它，否则系统可能无法正常运行。

● 手动：如果一个服务被设置为手动，那么可以在需要时再运行它，这样可以节省大量的系统资源，加快系统启动。

● 禁用：此类服务不能再运行。这个设置一般在提高系统安全性时使用。如果怀疑一个陌

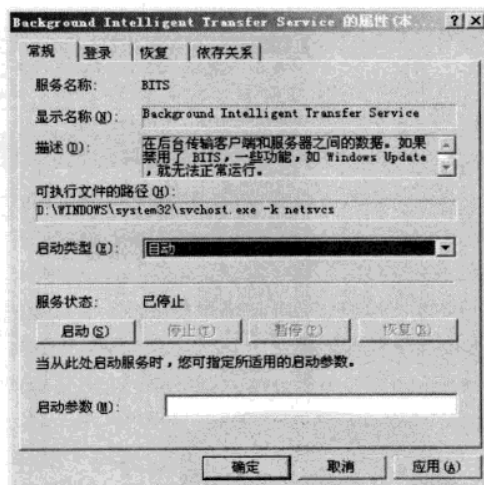


图 3-2-12 服务属性设置

生的服务会给系统带来安全上的隐患，可以先尝试停止它，观察系统能否正常运行，如果一切正常，那么就可以直接禁用它。如果以后需要这个服务，在启动它之前，必须先将启动类型设置为自动或手动。

单击“依存关系”选项卡可以看到顶端列表指出了运行当前选定服务所需的其他服务，底端列表则指出了需要运行此服务才能正确运行的其他服务。它说明了一些服务并不能单独运行，必须依靠其他服务。在停止或禁用一个服务之前，清楚了解该服务的依存关系是必不可少的步骤，如果有其他需要启动的服务是依靠这个服务，就不能将其停止。

Windows Server 2003 的服务有上百个，用户可以根据系统的需要，停止一些不必要的服务，以减少系统资源占用，增加安全。

3.2.3 安装补丁程序

1. 在线更新

为了保证 Windows Server 2003 的安全运行，防止病毒、木马利用 Windows 系统漏洞进行攻击和传播，需要定期为计算机安装最新的补丁修复程序。通过安装补丁程序，可以大幅提高操作系统的安全性以及稳定性。访问 <http://windowsupdate.microsoft.com/> 可以在线更新。如图 3-2-13 所示，单击“查看以寻找更新”，此时会检测当前配置，寻找最新更新。如果使用正版软件，将显示可以安装的补丁列表，直接选择所需要的补丁进行安装即可。



图 3-2-13 安装补丁

2. 自己提供系统更新服务

刚安装和部署的企业内部服务器，如果立即连接到 Internet 上进行系统更新，无疑是把系统

存在的漏洞暴露在各种病毒和恶意攻击的威胁之下，即便是访问微软更新网站也是很很不安全的；另外还存在着是否能够免费访问微软更新站点的问题（如教育网用户需根据流量付费）；如果企业内有很多台计算机，所有的计算机都要到微软的网站下载同样的补丁，下载速度慢且要重复多遍，浪费大量的时间。基于以上考虑，可以在企业内部搭建一台 SUS（Microsoft Software Update Services）服务器，企业 SUS 服务器定期从微软服务器下载最新的补丁包，企业内部用户可以从企业的 SUS 服务器获得系统的更新补丁包，这样即经济又高效。有关 SUS 服务器的更多配置请参考微软网站。

3.3 用单台计算机虚拟一个局域网

既然是学习网络管理，只有一台计算机是远远不够的，可不管是学校机房，还是网吧或者家庭用户，往往都是单人单机，这样的环境可以抽象成图 3-3-1 所示的网络环境。

如图 3-3-1 所示的拓扑中，一般用户仅拥有内部网中的一台计算机，与真实的环境相差甚远。作为一名网管，至少要拥有图 3-3-1 中所有设备。这里需要借助于虚拟机软件 VMware（本书以 5.5 版为例）或类似的虚拟机软件来模拟出多台计算机，搭建出如图 3-3-1 所示的网络环境。虚拟的计算机在功能上与真实计算机几乎没有

差异。第 3 部分会通过另一个模拟软件 dynamics 模拟出路由器和交换机。dynamics 是一款功能强大的路由器和交换机模拟软件，甚至可以把它当成真实的设备，在真实的网络中使用。图 3-3-2 所示方框中的所有设备均由一台计算机模拟出来，这样就拥有了 3 台计算机，

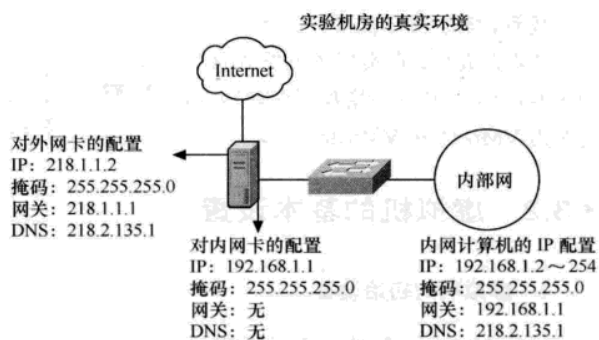


图 3-3-1 机房的真实网络拓扑

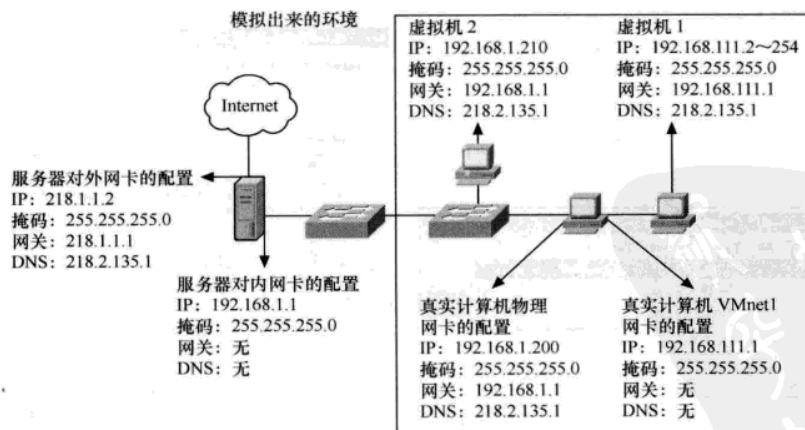


图 3-3-2 模拟的网络拓扑

其中真实机安装 Windows Server 2003，虚拟机 1 和虚拟机 2 也安装 Windows Server 2003，由它们一起构建出图 3-3-2 所示的网络环境。

3.3.1 安装 VMware 虚拟机软件

为了能顺利地完成本书中的大部分实验，建议计算机的配置越高越好，推荐最低配置为：CPU 至少 1500MHz，最好是 3000MHz 以上，双核的更好；内存至少 512MB，最好是 1GB，2GB 更好；空闲硬盘空间至少 6GB。

VMware 软件可以在下载的软件包中找到，安装比较简单，在此不作介绍。安装完成后，真实机的网络连接如图 3-3-3 所示，其中新增加了两块网卡，简称为 VMnet1 和 VMnet8。

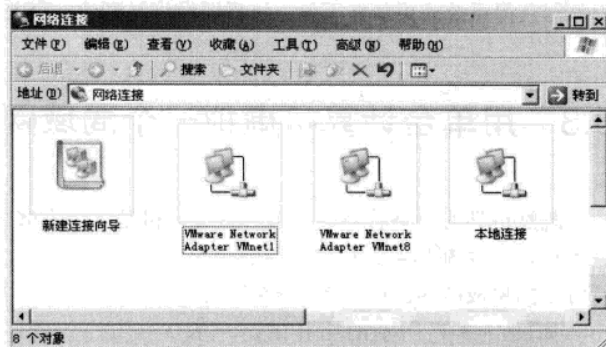


图 3-3-3 VMware 安装完成后的网络连接

3.3.2 虚拟机的基本设置

1. 虚拟机的初始设置

运行 VMware 软件，选择“File”→“New”→“New Virtual Machine”命令，如图 3-3-4 所示。弹出“New Virtual Machine Wizard”虚拟机安装向导对话框，直接单击“下一步”按钮继续。

弹出“Virtual machine configuration”对话框，如图 3-3-5 所示。保持默认的“Typical”选项，直接单击“下一步”按钮继续。

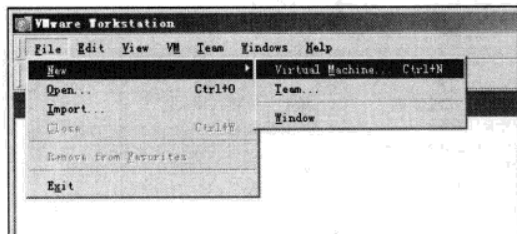


图 3-3-4 新建虚拟机

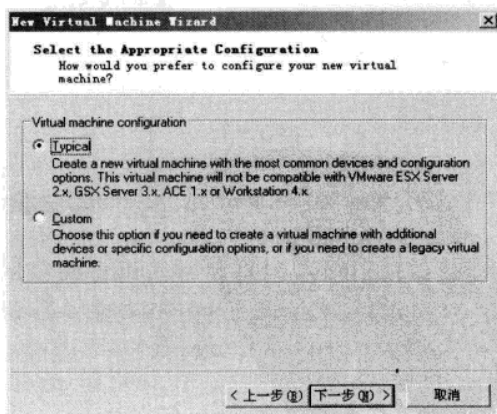


图 3-3-5 新建虚拟机向导

弹出“Select a Guest Operating System”对话框,如图 3-3-6 所示。这里选择“Windows Server 2003 Enterprise Edition”,单击“下一步”按钮继续。

弹出“Name the Virtual Machine”对话框,如图 3-3-7 所示。注意“Location”是 Windows Server 2003 将要安装的路径,选择一个空闲空间比较大的硬盘分区,至少要达到 3GB 以上。

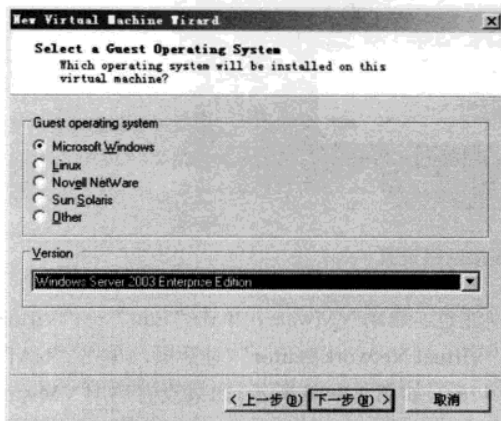


图 3-3-6 选择要安装的操作系统

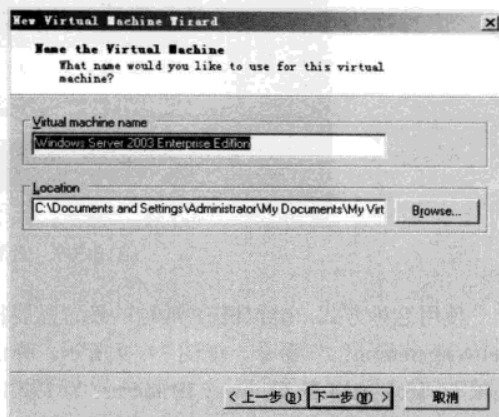


图 3-3-7 选择虚拟机的保存路径

单击“下一步”按钮继续,弹出“Network Type”选择对话框,如图 3-3-8 所示。该对话框中提供了 4 个选项,具体解释如下。

● Use bridged networking: 这种方式最简单,直接将虚拟网卡桥接到真实机的物理网卡上,相当于在真实机的前面连接了一台交换机,虚拟出来的计算机和真实的计算机都接在交换机上。在这种模式下,虚拟机的网卡直接连到了真实机物理网卡所在的网络上,可以想象为虚拟机和真实机处于同等的地位,在网络关系上是平等的,没有谁在谁后的问题。使用这种方式很简单,前提是需要得到 1 个以上的 IP 地址。图 3-3-2 所示虚拟机 2 的网卡使用这个选项,网卡类型可以随时改变,即使虚拟机启动后也可实时改动并立即生效。安装完成后按如图 3-3-2 中所示配置 IP 地址。

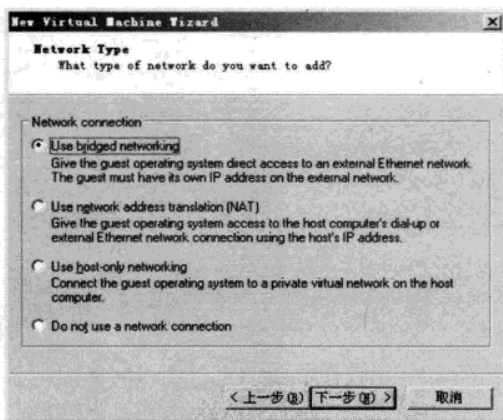


图 3-3-8 网卡类型选择

● Use network address translation (NAT):

安装 VMware 后,可以在“服务管理控制台”中找到“VMware DHCP Service”服务,该服务自动为配置成 NAT 和 Host-only 类型的虚拟机分配 IP 地址信息,这样虚拟机就可以使用 DHCP 服务。更为重要的是,配置为 NAT 类型的虚拟机可以借助真实计算机的合法 IP 访问外部网络, NAT 提供了从虚拟机私有 IP 到真实计算机合法 IP 之间的地址转换。这种情况相当于有一个 NAT 服务器在运行,只不过这个 NAT 配置集成到 VMware 中了,不需要用户配置。很显然,如果只有一个公网地址,这种方式很合适。

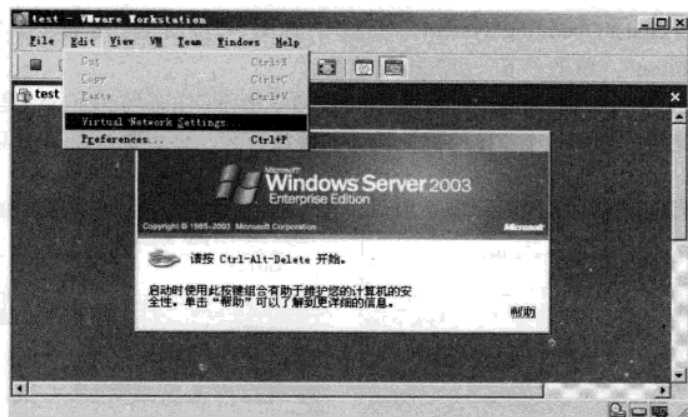


图 3-3-9 查看虚拟网络设置

使用这种方式,虚拟机 IP 地址的设置需要特别注意。启动 VMware,单击“Edit”→“Virtual Network Setting...”命令,如图 3-3-9 所示。弹出“Virtual Network Editor”对话框,单击“NAT”选项卡,记录 NAT 的 Gateway IP address 为 192.168.126.2,如图 3-3-10 所示。如果没有启用 VMware 的 DHCP 服务,可以手工设置虚拟机的 IP 地址为 192.168.126.5 (与 192.168.126.2 在同一个网段的不同地址),子网掩码为 255.255.255.0 (与 192.168.126.2 的掩码相同),网关为 VMware 中的 NAT 网关 192.168.126.2, DNS 设置成真实机的 DNS。配置完成后,虚拟机即可通过 NAT 服务访问外部网络。

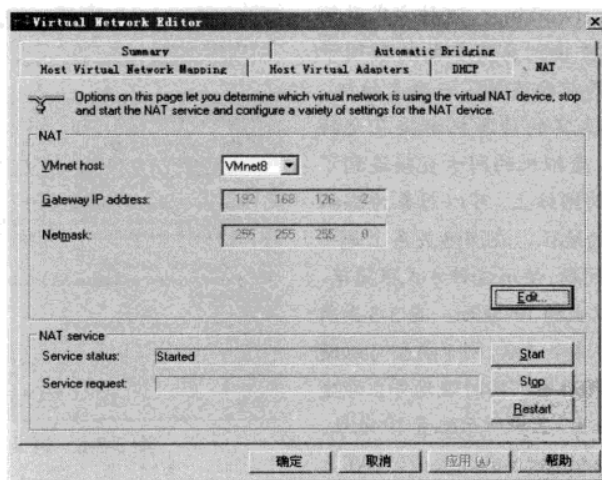


图 3-3-10 虚拟网卡中的 NAT 地址

注意



虽然 NAT 是借助于 VMnet8,但却和真实计算机上 VMnet8 网卡无关,随意配置真实计算机 VMnet8 网卡的 IP 地址,或者禁用 VMnet8 网卡,对虚拟机访问外部网络没有任何影响。

● **Use host-only networking:** 和 NAT 不同的是, 此种方式下没有地址转换服务。因此, 默认情况下, 虚拟机只能访问到真实计算机, 这也是 host-only 名字的意义。默认情况下, 也会有一个 DHCP 服务加载到 VMnet1 上, 这样连接到 VMnet1 上的虚拟机仍然可以设置成 DHCP, 方便系统的配置。是不是这种方式下, 虚拟机就没有办法连接到外网呢? 当然不是。事实上, 这种方式更为灵活, 用户可以手工配置 NAT。在 Windows Server 上实现 NAT 的方法很多, 简单的有“Internet 连接共享”, 复杂的有“路由和远程访问中的 NAT 服务”。Use host-only networking 这种模式和图 3-3-1 所示的情形类似, 可以方便地进行与之有关的实验。图 3-3-2 所示虚拟机 1 的网卡使用这个选项。

注意



Use host-only networking 需要借助真实计算机的 VMnet1 网卡, 真实计算机的 VMnet1 网卡不能禁用, 虚拟机的网关要指向 VMnet1 网卡的 IP 地址。

- **Do not use a network connection:** 不使用网络, 虚拟系统为一个单机。

每种网络类型都有自己的优势和特点, 用户可以根据实际需要进行选择。

如图 3-3-8 所示, 单击“下一步”按钮, 设定虚拟的硬盘, 如图 3-3-11 所示。虚拟机硬盘默认是 8GB, 用户也可以调整。“Allocate all disk space now”表示立即从物理硬盘中划出虚拟机使用的硬盘空间, 如果不选择此复选框, 虚拟机的硬盘空间是动态变化的。“Split disk into 2GB files”表示把虚拟机硬盘文件分成 2GB 的多个文件。这里保持默认设置, 单击“完成”按钮, 完成 VMware 虚拟机的初始设定。

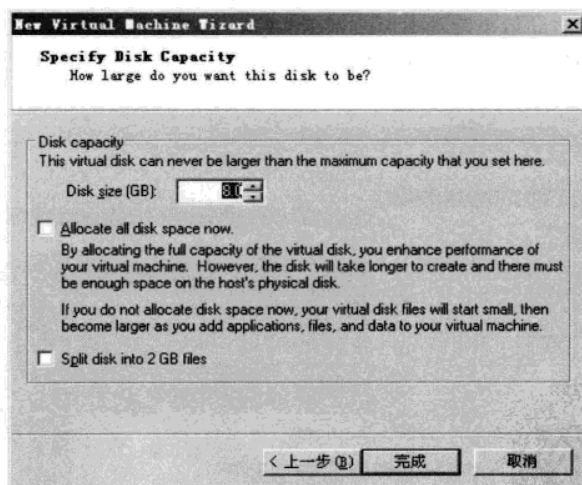


图 3-3-11 设置虚拟机的硬盘

2. 更改虚拟机的配置

完成虚拟机的初始设置后, 如对虚拟机的默认硬件配置不满意, 可以单击如图 3-3-12 所示的“Edit virtual machine settings”对虚拟机的内存大小、网卡数量及类型、光盘来源(如没有系统光

盘, 可以用 ISO 代替) 等进行更改。

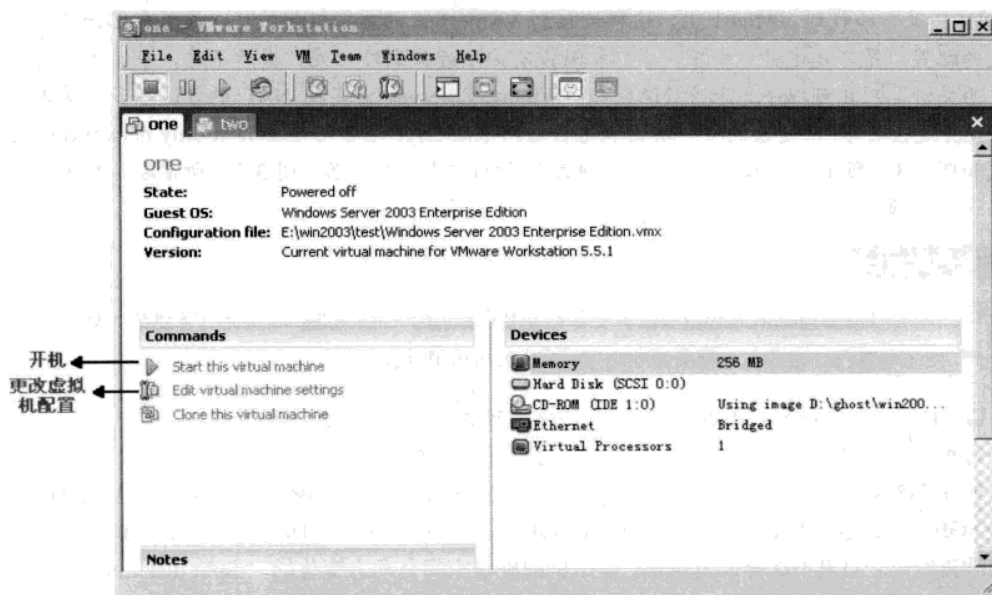


图 3-3-12 更改虚拟机配置

虚拟机安装完成, 启动后也可动态更改网卡类型, 单击菜单 “VM” → “Removable Devices” → “Ethernet” → “Edit” 命令, 如图 3-3-13 所示。

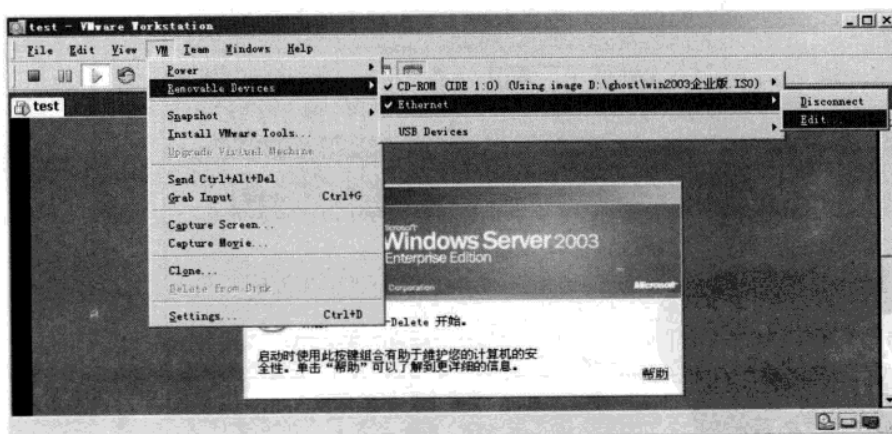


图 3-3-13 编辑虚拟机设备

在打开的如图 3-3-14 所示的对话框中, 更改网卡的类型后可立即生效。从图 3-3-13 中可以看到 “CD-ROM” 也支持随时更改。

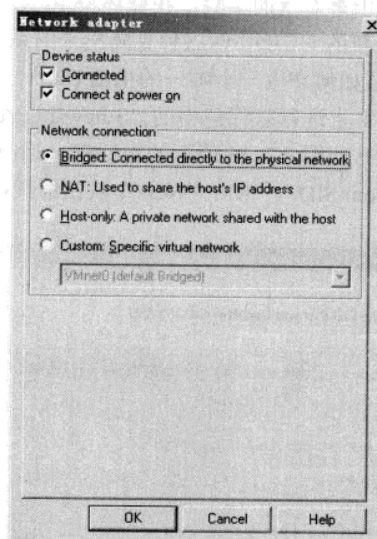


图 3-3-14 修改虚拟机网络类型

3. 安装虚拟机的操作系统

VMware 只是提供了虚拟机的硬件，接下来还需要给虚拟机安装操作系统。首先安装虚拟机 1，可以从光盘直接安装，如果没有光盘，使用 Windows Server 2003 的 ISO 文件也可以，具体的安装步骤请参照本章 3.1.3 小节。接下来安装虚拟机 2，步骤与安装虚拟机 1 相同。还有一种快速安装的方法，那就是复制虚拟机 1 的安装文件夹，然后在 VMware 中单击菜单“File”→“Open”，定位到复制文件夹下的“Windows Server 2003, Enterprise Edition.vmx”文件，第一次运行复制的系统时，会弹出图 3-3-15 所示的提示界面，选择“Create”或“Always Create”，创建一个唯一用户标识（UUID），这样网卡 MAC 地址和新的机器 ID 都会被重置。启动后，修改虚拟机 2 的主机名、网卡类型、IP 地址。

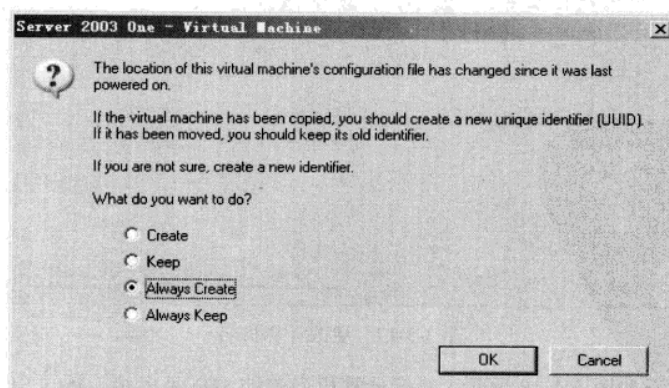


图 3-3-15 创建一个新的 UUID

这种克隆的系统默认不能用于第 6 章的实验，在域环境中，所有计算机都要求有唯一的机器 ID，尽管图 3-3-15 中创建了一个新的 UUID，但这种克隆出来的系统，在 Windows Server 2003 中的机器 ID 是一样的。接下来介绍如何产生一个唯一的机器 ID。

虚拟机 2 启动后，在虚拟机 2 上运行软件包中的“3\newsid.exe”文件，在弹出的“NewSID”对话框中单击“Next”按钮，打开如图 3-3-16 所示的对话框，询问是产生一个随机的 SID，还是复制一个 SID，这里选择“Random SID”，单击“Next”按钮继续。

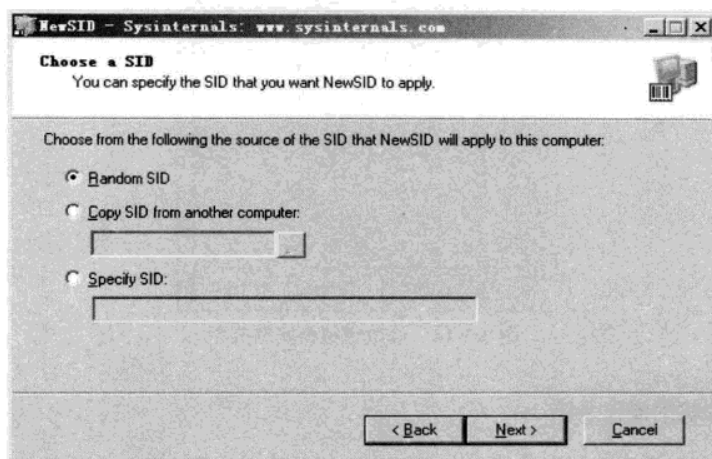


图 3-3-16 产生一个随机的 SID

接下来询问是否要更改计算机名，如图 3-3-17 所示，这里随便填入一个不同于虚拟机 1 的计算机名。单击“Next”按钮继续。

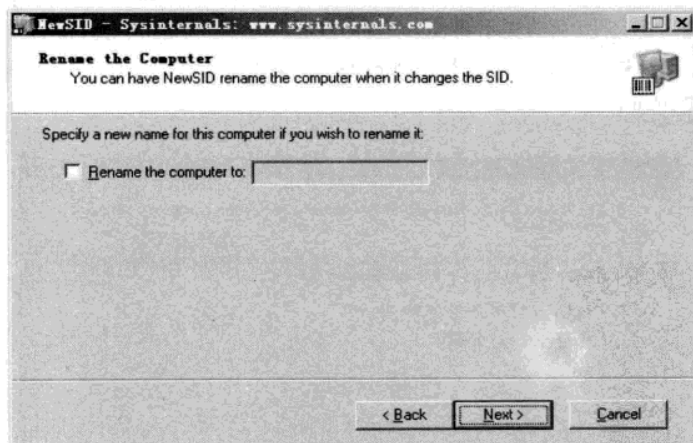


图 3-3-17 更改计算机名

接下来的对话框如图 3-3-18 所示，显示计算机当前的 SID 是多少，新的 SID 将是多少。单击“Next”按钮应用新的 SID，单击“Cancel”按钮，取消更改。读者在虚拟机 1 上运行 newsid.exe，

可以发现两台虚拟机的 SID 相同,这样的两台计算机无法同时工作在域的环境中。这里单击“Next”按钮产生新的 SID,至此克隆出来的虚拟机 2 和虚拟机 1 可以共存于域的环境中,不影响完成第 6 章的实验。

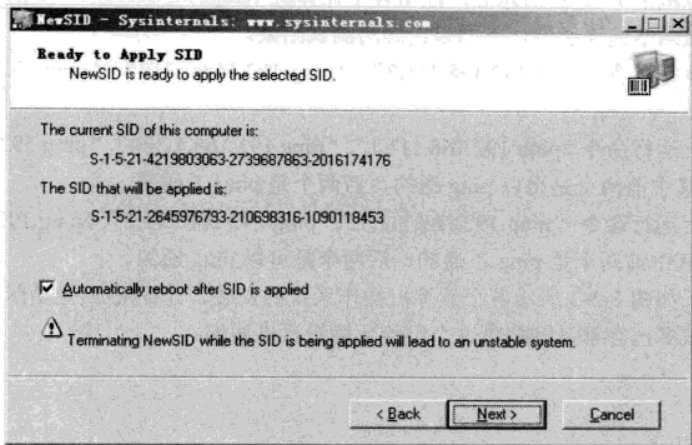


图 3-3-18 使用新的 SID

注意



本书提供了众多的实验,需要在虚拟机 1 和虚拟机 2 上完成,有些实验相互影响,甚至是冲突,为了能随时把操作系统还原到刚初始状态,请备份“Windows Server 2003 Enterprise Edition.vmdk”文件。这个文件相当于是虚拟机的硬盘,备份该文件相当于克隆硬盘,需要还原操作系统时,只要用备份文件覆盖安装目录下的同名文件即可。

操作系统安装完成后,会发现鼠标移进 VMware 中的虚拟机后,需按“Ctrl + Alt”组合键才能移出,这样的操作很是不便,这个问题可以通过安装 VMware Tools 来解决。选择菜单“VM”→“Install VMware Tools”命令,安装完成后,可以发现鼠标可以自由地移进移出,还可更改适配器的模式,调整屏幕的分辨率和色彩等。

3.3.3 构建局域网

按图 3-3-2 配置各计算机的网络地址信息,如表 3-3-1 所示。

表 3-3-1 各计算机的网络配置

	网卡名称	网卡类型	IP 地址	子网掩码	网 关	DNS
真实机	本地连接	物理网卡	192.168.1.200	255.255.255.0	192.168.1.1	218.2.135.1
真实机	VMnet1	虚机网卡	192.168.111.1	255.255.255.0	无	无
虚拟机 1	本地连接	Host-only	192.168.111.2	255.255.255.0	192.168.111.1	218.2.135.1
虚拟机 2	本地连接	Bridged	192.168.1.210	255.255.255.0	192.168.1.1	218.2.135.1

3.3.4 测试局域网

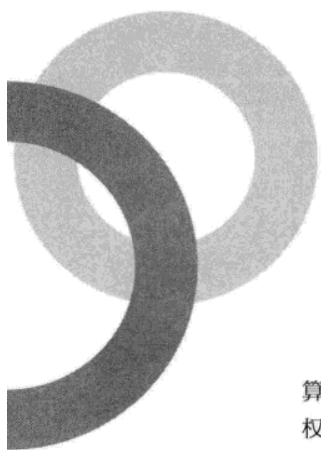
配置完各计算机的 IP 地址信息后, 停用各个计算机 Windows Server 2003 的防火墙, 分别在各个计算机上测试网络的连通性, 下面是正确的测试结果。

在真实机上运行命令 “ping 192.168.111.2”、“ping 192.168.1.210”、“ping 192.168.1.1”, 全部都可以 ping 通。

在虚拟机 1 上运行命令 “ping 192.168.111.1”、“ping 192.168.1.200”、“ping 192.168.1.1”、“ping 192.168.1.210”, 其中前两个是可以 ping 通的, 后两个是 ping 不通的。

在虚拟机 2 上运行命令 “ping 192.168.111.1”、“ping 192.168.111.2”、“ping 192.168.1.1”、“ping 192.168.1.200”, 其中前两个是 ping 不通的, 后两个是可以 ping 通的。

至此, 完成了如图 3-3-2 所示各个计算机操作系统的安装、计算机 IP 地址配置、网络连通性测试。接下来的很多内容都是围绕着这个实验环境进行讲述的。



第4章 计算机管理

Chapter 4

本章主要介绍 Windows Server 2003 中用户和组的管理、磁盘和文件夹的管理、计算机的远程管理等内容。通过学习本章，读者能够配置打印和文件共享，配置 NTFS 权限保证文件的安全，配置软 RAID 实现硬盘的冗余，配置卷影复制实现共享文件的冗余，配置 EFS 加密保护文件的安全，并能实现远程数据的定期自动备份。

4.1 用户和组管理

Windows Server 2003 作为一个多用户的操作系统，允许多个用户共同使用一台计算机，而账号就是用户进入系统的凭证。用户组的存在主要是为了方便用户的管理。

1. 用户管理

作为一名服务器管理员，必须经常查看服务器有无异常，检查本地用户账号就是其中一项工作。黑客攻入一台服务器后，最想做的一件事一般就是建立一个超级用户。通过检查本地用户，可以发现是否有非法用户的存在。Windows Server 2003 安装完成后，一般会存在以下用户账号。

- Administrator: 本地计算机中拥有最高权限的用户，可以对它重命名及更改密码，但不能删除。
- Guest: 只拥有相对较低的权限，默认情况下是被禁止的。
- SUPPORT_388945A0: Windows XP 和 Windows Server 2003 中新增的一个用户账号，可以通过 Windows 中的 HELP AND SUPPORT CENTER (求助与支持中心) 提供远程支持，默认情况下是被禁用的。
- IUSER_MACHINENAME: 如果系统安装了 IIS，客户端就能使用这个账号来匿名访问 IIS，它是 Guests 用户组中的成员。
- IWAM_MACHINENAME: 如果安装了 IIS，各种 IIS 应用程序就将运行在这个账号下，它是 IIS_WPG 用户组的成员之一。

管理员可以添加新的用户，单击“开始”→“程序”→“管理工具”→“计算机管理”命令，在打开的对话框中展开“本地用户和组”，右键单击“用户”，如图 4-1-1 所示。

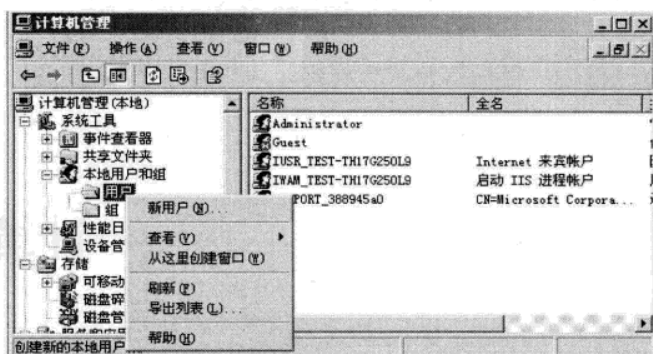


图 4-1-1 用户管理

选择“新用户”，打开“新用户”对话框，如图 4-1-2 所示。在“用户名”中填入用户名，如“test”；“全名”和“描述”是选填项；再填入用户的密码和确认密码；如果不让用户自行更改密码，可以取消“用户下次登录须更改密码”复选框，选中“用户不能更改密码”；密码使用一段时间后会要求更换，否则密码会失效，选中“密码永不过期”复选框，使密码永不过期；如果临时性停用账号，可选中“账号已禁用”复选框。

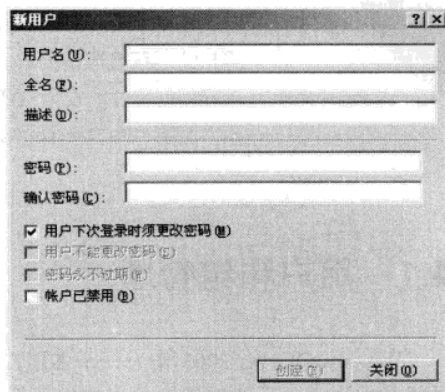


图 4-1-2 添加新用户

2. 组管理

用户组是为简化用户管理而存在的，它们就像是一些容器，每个容器里是一些拥有同样权限的用户，下面介绍一些常见的组和权限。

- Administrators: 该用户组里的成员在本地机器上拥有最高权限。
- Users: 本地机器上所有的用户账号，这是一个低权限的用户组。
- Guests: 本地来宾组。
- Remote Desktop Users: Windows Server 2003 中新增的用户组，有权使用远程桌面。
- Network Configuration Operators: Windows Server 2003 新增的用户组，这个用户组有足够的权限去管理网络配置状况。
- Backup Operators: 虽然没有 Administrators 组成员的权限大，但相差不多。
- Power Users: 拥有的权限比 Users 组成员所拥有的大，但比 Administrators 组成员所拥有的小。
- IIS_WPG: Windows Server 2003 中新增的用户组，如果安装了 IIS，Web 应用进程的账号将被容纳在这个用户组里。

管理员可以把刚才新添加的用户“test”提升为计算机的系统管理员。在如图 4-1-1 所示的右边子窗口中，右键单击新添加的“test”用户，在快捷菜单中单击“属性”命令，打开用户属性对话框，选择“隶属于”选项卡，如图 4-1-3 所示。

单击“添加”按钮，打开如图 4-1-4 所示的对话框。在打开的文本框中直接输入“administrators”

或者单击“高级”按钮，然后再单击“立即查找”按钮，选中“administrators”组后，单击“确定”按钮返回。如图 4-1-3 所示的列表框中添加了一个“administrators”，单击“确定”按钮，完成添加。至此，“test”用户也变成了管理员组中的一员。

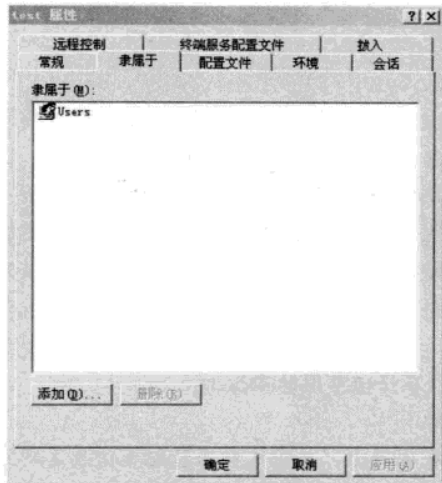


图 4-1-3 用户属性对话框

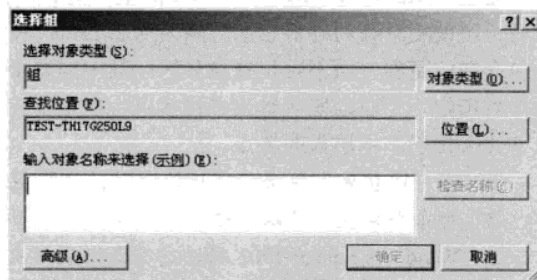


图 4-1-4 把用户加入组

4.2 磁盘和文件夹管理

Windows Server 2003 中的磁盘、卷和文件管理功能使其成为文件服务器的灵活平台，并可使用户更方便地查找和访问信息。此外，本节还介绍卷影复制、共享、EFS 加密功能，并编写一个批处理文件实现文件夹的异机或异地定时自动备份。

4.2.1 磁盘管理

Windows Server 2003 在磁盘管理方面提供了许多新的功能，包括简化的任务和直观的用户界面、基本和动态磁盘存储、本地和远程磁盘管理，支持 MBR（Master Boot Record，主引导记录）和 GPT（Globally unique identifier Partition Table format，全局唯一识别分区表格式）磁盘，支持 SAN（Storage Area Network，存储区域网络）等功能。

硬件 RAID（Redundant Array of Independent Disks，独立磁盘冗余阵列）解决方案具有存取速度快、稳定性好的优点，但居高不下的价格让用户可望而不可及。值得庆幸的是，Windows Server 2003 提供了内嵌的软件 RAID 功能，并且软 RAID 可以实现 RAID-0、RAID-1、RAID-5。软 RAID 不仅实现上非常方便，而且还节约了大量的资金，是 Windows Server 2003 中一个很实用的功能。

RAID-5 卷是数据和奇偶校验间断分布在 3 个或更多物理磁盘上的容错卷，如果物理磁盘的某一部分出错，用户可以用余下的数据和奇偶校验重新创建磁盘上出错的那一部分上的数据。对于多数由读取数据构成的计算机环境中的数据冗余来说，RAID-5 卷是一种很好的解决方案。可使用基于硬件或基于软件的解决方案来创建 RAID-5 卷，Windows Server 2003 操作系统提供基于

软件的 RAID，其中 RAID-5 卷中磁盘上的信息创建和重新生成将由“磁盘管理”来处理，数据将跨磁盘阵列中的所有成员进行存储。当然，软 RAID 的性能和效率是不能与硬 RAID 相提并论的。下面首先从动态磁盘的创建开始介绍，然后说明在 Windows Server 2003 中如何实现软 RAID，最后讲述一下软 RAID 的管理。

1. 创建动态磁盘

在安装 Windows Server 2003 时，硬盘将自动被初始化为基本磁盘。用户不能在基本磁盘分区中创建新卷集、条带集、RAID-5 组，而只能在动态磁盘上创建类似的磁盘配置。也就是说，如果想创建 RAID-0、RAID-1 或 RAID-5 卷，就必须使用动态磁盘。在 Windows Server 2003 安装完成后，可使用升级向导将它们转换为动态磁盘，将一个磁盘从基本磁盘转换为动态磁盘后，磁盘上包含的将是卷，而不再是磁盘分区。其中的每个卷是硬盘驱动器上的一个逻辑部分，还可以为每个卷指定一个驱动器字母或者挂接点，但是要注意的是只能在动态磁盘上创建卷。动态磁盘有以下几个优于基本磁盘的特点。

- 卷可以扩展到包含非邻接的空间，这些空间可以在任何可用的磁盘上。
- 对每个磁盘上可以创建的卷的数目没有任何限制。
- Windows Server 2003 将动态磁盘配置信息存储在磁盘上，并将这些磁盘配置信息复制到所有其他动态磁盘中。因此，单个磁盘的损坏将不会影响到访问其他磁盘上的数据。

一个硬盘既可以是基本的磁盘，也可以是动态的磁盘，但不能二者兼是，因为在同一磁盘上不能组合多种存储类型。但是，如果计算机有多个硬盘，就可以将各个硬盘分别配置为基本的或动态的磁盘。下面以有 4 块硬盘配置的计算机为例，介绍软 RAID 的技术。硬盘的配置如图 4-2-1 所示。

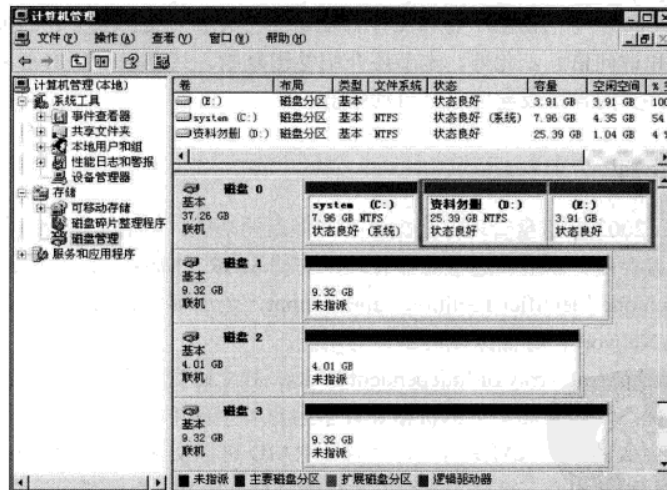


图 4-2-1 多硬盘计算机的磁盘管理

如图 4-2-1 所示的计算机配置了 4 块硬盘，磁盘 0 为基本磁盘，分成了 3 个分区，其中 C 分区安装的是 Windows Server 2003 操作系统，D 分区存储的是重要资料，E 分区暂未使用；磁盘 1、磁盘 2、磁盘 3 都是新加入磁盘，目前它们也是基本磁盘。进行软 RAID 实验之前，首要的工作就是把基本磁盘转换成动态磁盘。

实验 4-1 创建动态磁盘

软 RAID 必须在多磁盘系统中才能实现。实现 RAID-1 最少需要两块硬盘，而实现 RAID-5 则最少需要 3 块硬盘。一般情况下，操作系统所在磁盘采用 RAID-1，而数据所在磁盘采用 RAID-5。为了不影响操作系统，本小节的实验把操作系统所在的硬盘除外，也就是说需要 4 块硬盘。由于一般计算机上都没有配置 4 块硬盘，为了能顺利完成本小节实验，这里借助如图 3-3-2 所示的“虚拟机 1”来构造出多块硬盘，下面是操作步骤。

STEP 1 虚拟出多块硬盘。启动 VMware，选择虚拟机 1，单击“Edit virtual machine settings”，编辑虚拟机的硬件配置，打开如图 4-2-2 所示的对话框。

在图 4-2-2 中单击“Add”按钮，打开添加硬件向导，单击“下一步”按钮，打开选择硬件类型对话框，如图 4-2-3 所示。

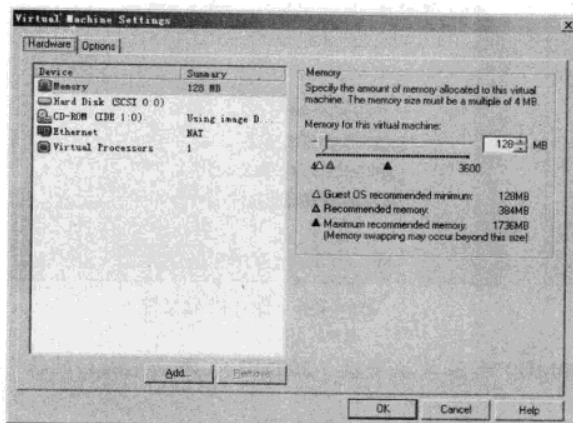


图 4-2-2 更改虚拟硬件配置

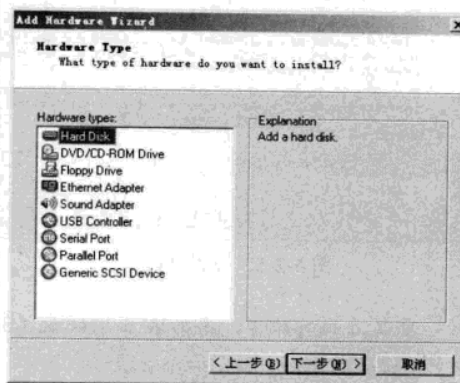


图 4-2-3 添加虚拟机硬盘

在图 4-2-3 中选中“Hard Disk”（硬盘）后，单击“下一步”按钮继续。接下来会要求选择一

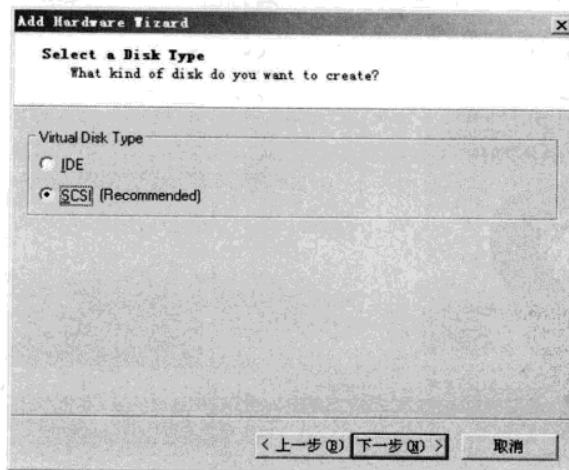


图 4-2-4 选择虚拟硬盘类型

个硬盘，这里保持默认的选项“Create a new virtual disk”（创建一个新的虚拟硬盘），单击“下一步”按钮继续。接下来要求选择虚拟硬盘的类型，如图 4-2-4 所示，保持默认的“SCSI”选项，单击“下一步”按钮继续。

接下来询问硬盘的大小，这里填入 0.3，也就是 300MB，如图 4-2-5 所示，单击“下一步”按钮继续。

接下来询问这个硬盘文件的名字和保存的位置，如图 4-2-6 所示，单击“完成”按钮，完成一块新硬盘的添加。

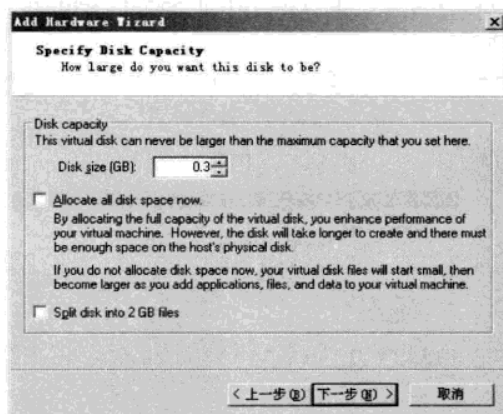


图 4-2-5 设置硬盘大小

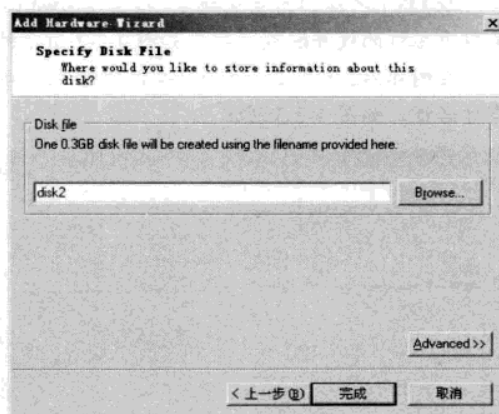


图 4-2-6 保存硬盘文件

重复上面的操作，添加第 3 块硬盘（300MB）和第 4 块硬盘（200MB），添加完成后的状态如图 4-2-7 所示。

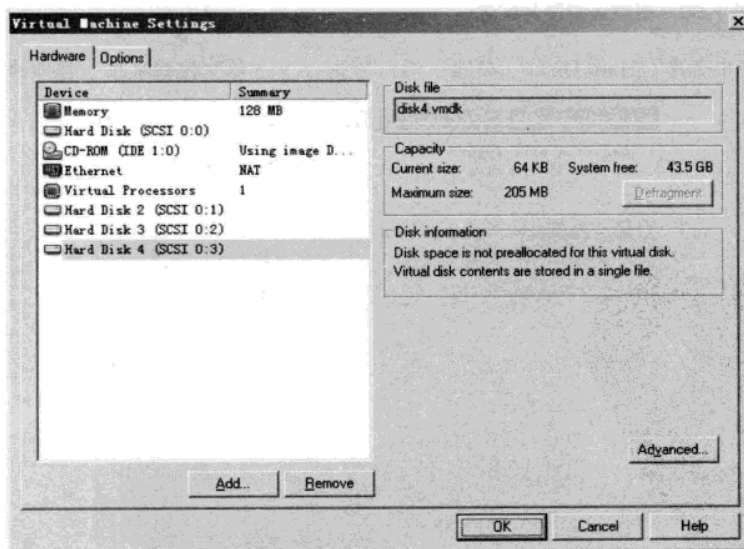


图 4-2-7 有 4 块硬盘的虚拟机

STEP 2 执行磁盘初始化和转换向导。启动虚拟机 1，选择“开始”→“程序”→“管理工具”→“计算机管理”命令，在“计算机管理”窗口中展开“存储”→“磁盘管理”，弹出“磁盘初始化和转换向导”对话框，如图 4-2-8 所示，单击“下一步”按钮继续。

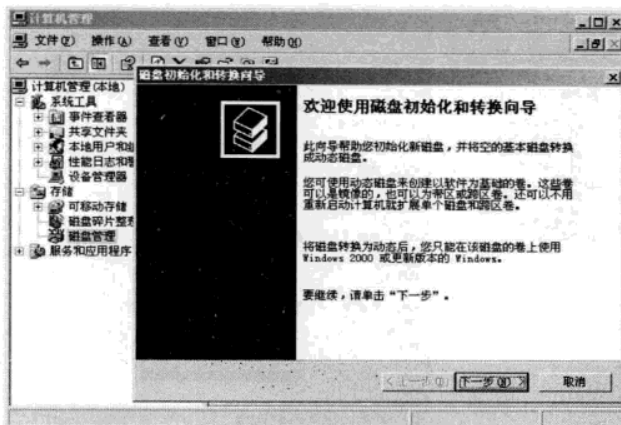


图 4-2-8 磁盘初始化向导

STEP 3 初始化磁盘。磁盘必须经过初始化才能使用，选中新添加的 3 块硬盘，如图 4-2-9 所示，单击“下一步”按钮继续。

STEP 4 转换磁盘。如图 4-2-10 所示，选中磁盘 1、磁盘 2、磁盘 3，将它们转换成动态磁盘，单击“下一步”按钮继续。

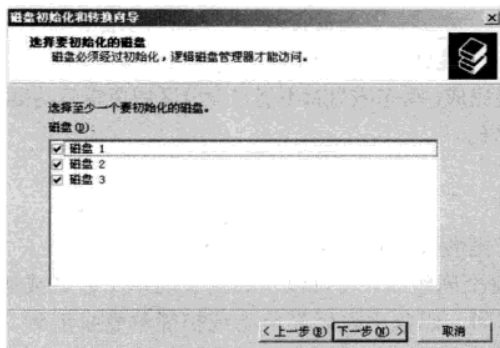


图 4-2-9 初始化磁盘

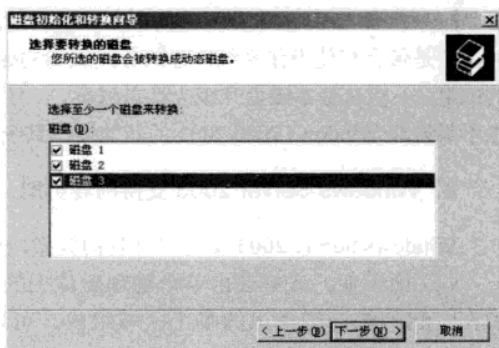


图 4-2-10 转换动态磁盘

STEP 5 完成转换。单击“完成”按钮，将磁盘 1、磁盘 2、磁盘 3 转换成动态磁盘。

这里转换的是 3 块没有初始化的硬盘，如果是把基本磁盘转换到动态磁盘，如把安装操作系统的第一块硬盘转换到动态磁盘，操作要麻烦得多，需多次确认。第一次，系统要求用户对要转换为动态磁盘的硬盘进行确认，这样做的原因很简单，因为这一升级操作是不可逆的，也就是说，基本磁盘可以升级为动态磁盘，但动态磁盘却不能恢复为基本磁盘。第二次，系统再次要求用户对磁盘升级予以确认，提示当将该磁盘升级为动态磁盘后，无法从这些卷上启动其他已安装的操作系统。第三次，系统要求用户确认操作，提示要升级磁盘上的文件系统将被强制卸下，并要求

用户对该操作进一步予以确认。基本磁盘到动态磁盘转换完成后，提示系统需要重新启动。图 4-2-11 显示全部 4 块磁盘都转换成动态磁盘。在本小节的实验中，“磁盘 0”可以不必转换成动态磁盘。

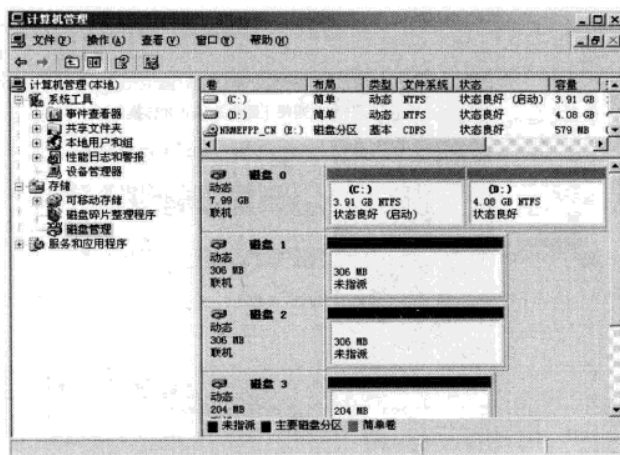


图 4-2-11 完成动态磁盘转换

在升级到动态磁盘时，必须以管理员或管理组成员的身份登录才能完成该过程。将基本磁盘升级到动态磁盘后，就不方便将动态卷改回到基本分区，唯一的方法就是必须删除本磁盘上的所有动态卷。删除卷时，这个卷上所有的数据都会丢失。全部卷被删完后，再使用“还原为基本磁盘”命令。在升级磁盘之前，应该关闭在那些磁盘上运行的程序。为保证升级成功，任何要升级的磁盘都必须至少包含 1MB 的未分配空间，在磁盘上创建分区或卷时，“磁盘管理”工具将自动保留这个空间，但是带有其他操作系统创建的分区或卷的磁盘上可能就没有这个空间。扇区大小超过 512 字节的磁盘，不能从基本磁盘升级为动态磁盘。一旦升级完成，动态磁盘就不能包含分区或逻辑驱动器，也不能被非 Windows 2000/2003 的其他操作系统所访问。

2. Windows Server 2003 支持的卷类型

Windows Server 2003 支持多种卷的类型，可以提供用户更大的选择空间。

(1) 简单卷。简单卷由单个物理磁盘上的磁盘空间组成，它可以由磁盘上的单个区域或链接在一起的相同磁盘上的多个区域组成。可以在同一磁盘中扩展简单卷或把简单卷扩展到其他磁盘。如果跨多个磁盘扩展简单卷，则该卷就是跨区卷。只能在动态磁盘上创建简单卷。简单卷不能包含分区或逻辑驱动器，也不能由 Windows Server 2003 以下的其他 Windows 操作系统访问。如果网络中的计算机还在运行 Windows 98 或更早版本，那么应该创建分区而不是动态卷。如果想在创建简单卷后增加它的容量，则可通过磁盘上剩余的未分配空间来扩展这个卷。要扩展一个简单卷，则该卷必须使用 Windows Server 2003 中所用的 NTFS 版本格式化。同时不能扩展基本磁盘上作为以前分区的简单卷。也可将简单卷扩展到同一计算机的其他磁盘的区域中，当将简单卷扩展到一个或多个其他磁盘时，它会变成一个跨区卷。在扩展跨区卷之后，不删除整个跨区卷便不能将它的任何部分删除。要注意的是，跨区卷不能是镜像卷或条带卷。

(2) 条带卷。利用条带卷,可以将两个或者更多磁盘(最多为 32 块硬盘)的空余空间组成为一个卷。在向条带卷中写入数据时,数据被分割为 64KB 的块,并均衡地分布在阵列中的所有磁盘上。一个阵列是两个或者多个磁盘的集合。条带卷可以有效地提高磁盘的读取性能,但是它并不提供容错功能,任何一块硬盘的损坏都会导致全部数据的丢失。条带卷类似于 RAID-0。

(3) 跨越卷。利用跨越卷,也可以将来自两个或者更多磁盘(最多为 32 块硬盘)的空余磁盘空间组成为一个卷。与条带卷所不同的是,将数据写入跨越卷时,首先填满第一个磁盘上的空余部分,然后再将数据写入下一个磁盘,依次类推。虽然利用跨越卷可以快速增加卷的容量,但是跨越卷既不能提高对磁盘数据的读取性能,也不提供任何容错功能。当跨越卷中的某个磁盘出现故障时,存储在该磁盘上的所有数据将全部丢失。

(4) 镜像卷。利用镜像卷(RAID-1 卷),可以将用户的相同数据同时复制到两个物理磁盘中。如果其中的一个物理磁盘出现故障,虽然该磁盘上的数据将无法使用,但系统能够继续使用尚未损坏而仍继续正常运转的磁盘进行数据的读写操作。镜像卷通过在另一磁盘上保留完全冗余的副本,保护磁盘上的数据免受介质故障的影响。由此可见,镜像卷的磁盘空间利用率只有 50% (即每组数据有两个成员),所以镜像卷的成本相对较高。要创建一个镜像卷,必须使用另一磁盘上的可用空间。动态磁盘中现有的任何卷(甚至是系统卷和引导卷),都可以使用相同的或不同的控制器镜像到其他磁盘上大小相同或更大的另一个卷。最好使用大小、型号和制造厂家都相同的磁盘作镜像卷,以避免可能产生的兼容性错误。

镜像卷可以大大地增强读性能,因为容错驱动程序同时从两个磁盘成员中同时读取数据,所以读取数据的速度会有所增加。当然,由于容错驱动程序必须同时向两个成员写数据,所以它的写性能会略有降低。镜像卷可包含任何分区(包括启动分区或系统分区),但是镜像卷中的两个硬盘都必须是 Windows Server 2003 动态磁盘。

(5) RAID-5 卷。在 RAID-5 卷中,Windows Server 2003 通过给该卷的每个硬盘分区中添加奇偶校验信息来实现容错。如果某个硬盘出现故障,Windows Server 2003 便可以用其余硬盘上的数据和奇偶校验信息重建发生故障的硬盘上的数据。

由于要计算奇偶校验信息,所以 RAID-5 卷上的写操作要比镜像卷上的写操作慢一些。但是,RAID-5 卷可以提供比镜像卷更好的读性能。其中的原因很简单,Windows 2003 可以从多个磁盘上同时读取数据。与镜像卷相比,RAID-5 卷的性价比较高,而且 RAID-5 卷中的硬盘数量越多,冗余数据带区的成本越低。但是 RAID-5 卷也有一些限制:第一,RAID-5 卷至少需要 3 个硬盘才能实现,但最多也不能超过 32 个硬盘;第二,RAID-5 卷不能包含根分区或系统分区。

实验 4-2 配置 RAID-1 和 RAID-5

虚拟机 1 的 3 块新加磁盘容量分别为:磁盘 1 是 0.3GB,磁盘 2 是 0.3GB,磁盘 3 是 0.2GB。在磁盘 1、磁盘 2、磁盘 3 这 3 个动态磁盘上创建 RAID-5。RAID-5 以最小的硬盘空间为参考,从每个磁盘上分配相同的空间,也就是说从 3 块磁盘上都分配 0.2GB 空间。磁盘 1 和磁盘 2 各剩下 0.1GB 空间,刚好可以继续配置 RAID-1。本实验在实验 4-1 的基础上继续,操作步骤如下。

STEP 1 新建卷。右键单击“磁盘管理”,在快捷菜单中选择“新建”→“卷(V)”,如图 4-2-12 所示。打开“新建卷向导”对话框,单击“下一步”按钮继续。

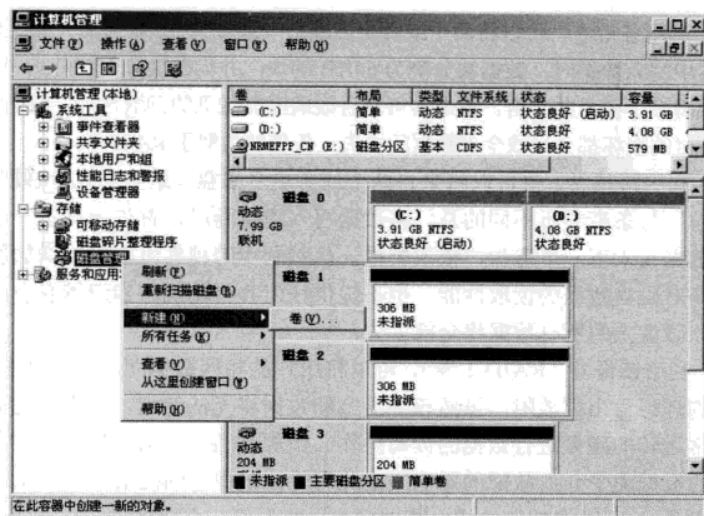


图 4-2-12 新建卷

- STEP 2** 选择卷类型。如图 4-2-13 所示，根据需要选择要创建的卷类型，这里选择 RAID-5 卷。
- STEP 3** 选择磁盘。单击“下一步”按钮，将显示“选择磁盘”对话框，如图 4-2-14 所示。

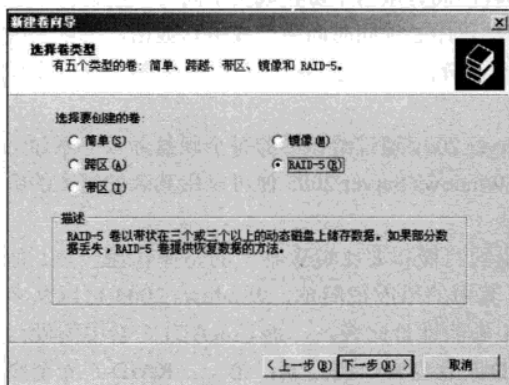


图 4-2-13 新建 RAID-5 卷

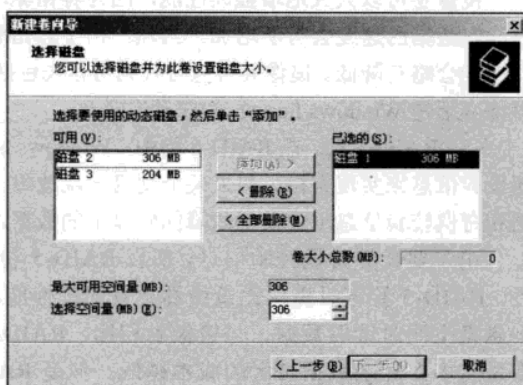


图 4-2-14 RAID-5 选择磁盘对话框

在左侧所有“可用”的动态磁盘列表框中选择要添加的磁盘，并单击“添加”按钮，即可将其添加至该 RAID-5 卷，并显示在“已选的”动态磁盘列表框中。选择“磁盘 2”，把磁盘 1 和磁盘 2 都加到 RAID-5 中，可以发现“下一步”按钮仍是灰色的，因为 RAID-5 至少需要 3 块硬盘。添加磁盘 3 后，“下一步”按钮此时可操作，如图 4-2-15 所示。

用户可以发现，磁盘 1 和磁盘 2 的容量都为 0.3GB，但添加到 RAID-5 中的却只有 0.2GB，这是因为 RAID-5 在每个磁盘中所占空间大小是相同的，即磁盘中最小磁盘的容量。还可以发现整个 RAID-5 卷的大小是 0.4GB，并不是 0.6GB ($0.2 \times 3 = 0.6$)，这是因为 RAID-5 卷采用奇偶校验的存储方式。假设要保存的数据是二进制的“101110”，从左边顺序保存“101110”中的每一位，顺序读出二进制串中的第一位“1”写入第一块磁盘；顺序读出二进制串中的第二位“0”写入第

二块磁盘；因第一块磁盘中的数据是“1”，第二块磁盘中的数据是“0”，为了保证3块磁盘中“1”的个数是奇数，第三块磁盘被写入“0”；接下去重复这样的过程，直到把数据写完。数据全部写完后的结果如图4-2-16所示。有用的比特数是6，写到磁盘上比特数是9，最后一块磁盘上写的全是校验数据。也就是说不管用多少块磁盘组成RAID-5卷，都需要用一块磁盘来做奇偶校验，都要因此占用一块磁盘的空间，RAID-5卷的空间大小应该是 $(n-1) \times$ 最小磁盘的容量，因此 $(3-1) \times 0.2\text{GB}=0.4\text{GB}$ 证实了这个结论。如果第二块磁盘故障，根据奇校验，RAID-5可以反过来推出第二块磁盘上的数据应该是“010”，所以在RAID-5卷，单一磁盘的故障，不会引起数据的丢失。如果同时两块磁盘损坏，那么RAID-5卷失败，保存的所有数据将丢失。

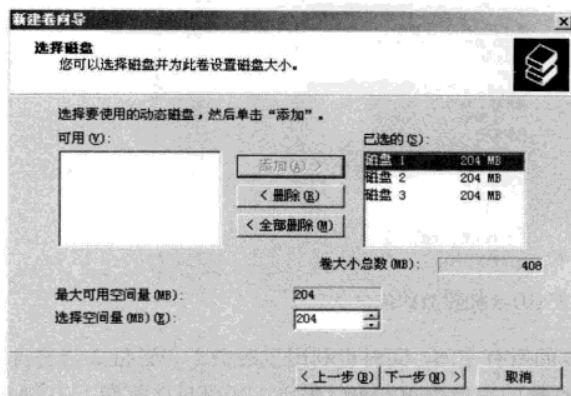


图 4-2-15 RAID-5 磁盘配置

将要写入的二进制串	101110
第一块磁盘中的数据	111
第二块磁盘中的数据	010
第三块磁盘中的数据	010

图 4-2-16 RAID-5 存储

STEP 4 指派驱动器号和路径。磁盘添加完毕后，单击“下一步”按钮，显示“指派驱动器号和路径”对话框。选中“指派以下驱动器号”选项，并为该RAID-5卷指派驱动器号，以便于管理和访问，如图4-2-17所示。

STEP 5 卷区格式化。单击“下一步”按钮，显示“卷区格式化”对话框，如图4-2-18所示，采用默认的设置。

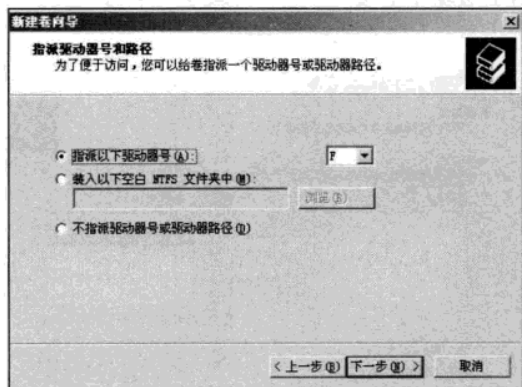


图 4-2-17 指派驱动器号

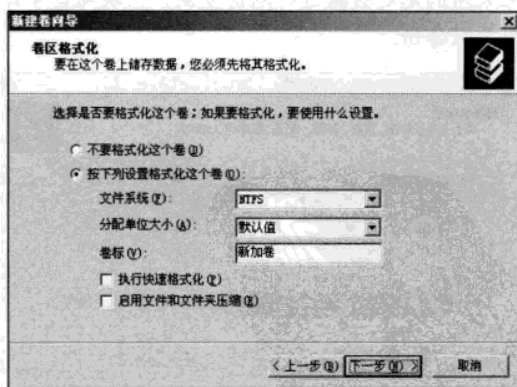


图 4-2-18 卷区格式化

STEP 6 完成RAID-5卷。单击“下一步”按钮，显示“完成创建卷向导”对话框，单击“完

成”按钮，系统格式化新创建的卷。至此，RAID-5 卷已创建完成，如图 4-2-19 所示。

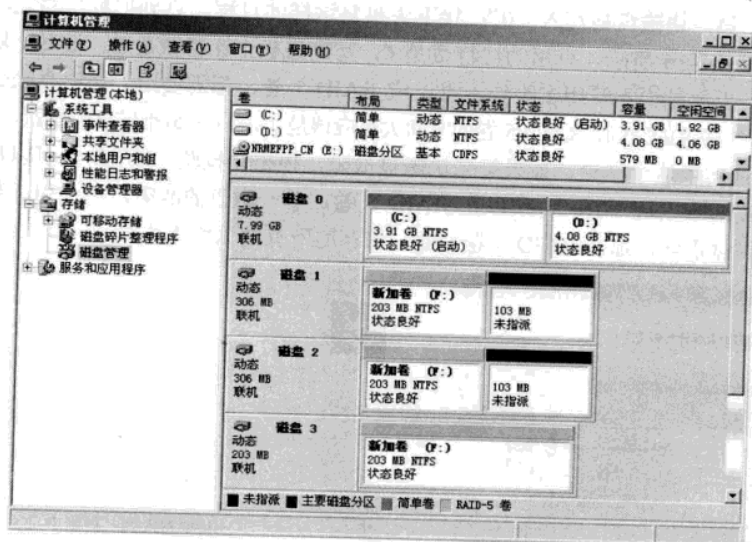


图 4-2-19 完成 RAID-5 配置后的磁盘状态

这里可以发现，RAID-5 卷利用了磁盘 3 的所有空间，同时也利用了磁盘 1 和磁盘 2 与磁盘 3 容量相等的空间，本实验环境中新建的 F 驱动器的容量为 406MB。磁盘 1 和磁盘 2 都剩下 103MB 的空间，刚好可以做一个 RAID-1 的卷，即镜像卷。

STEP 7 创建 RAID-1 卷。在磁盘管理中再次新建卷，选择卷类型，这里选择“镜像”，如图 4-2-20 所示。因为只有两块磁盘有未分配的空间，RAID-5 选项为灰色，处在不可用状态。

STEP 8 选择磁盘。单击“下一步”按钮，将显示“选择磁盘”对话框，如图 4-2-21 所示。把磁盘 1 和磁盘 2 都添加进来，图中显示镜像卷的空间大小与单块磁盘上未分配的空间相同。镜像采用的是对数据进行双份复制，两块磁盘中保存的数据完全相同，这样将耗费一半的磁盘空间用来做备份。

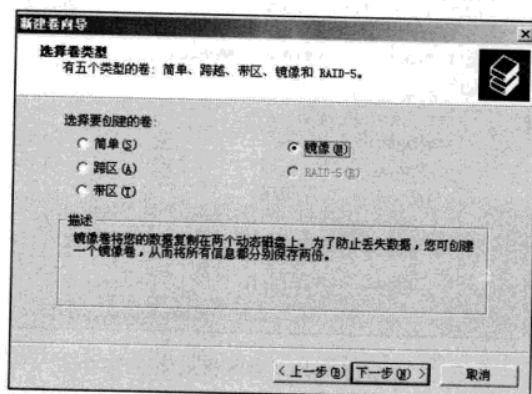


图 4-2-20 具有 RAID-1 和 RAID-5 的卷

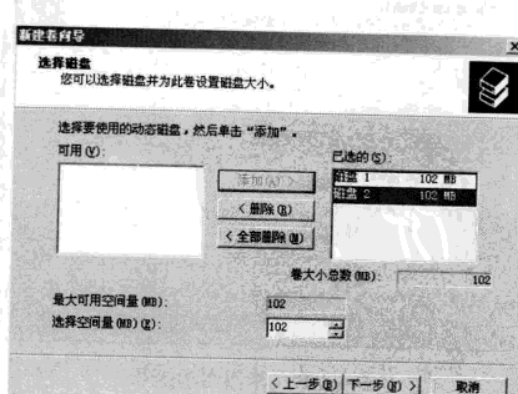


图 4-2-21 配置镜像卷

STEP 9 完成配置。RAID-1 和 RAID-5 都配置完后，磁盘管理的显示如图 4-2-22 所示。

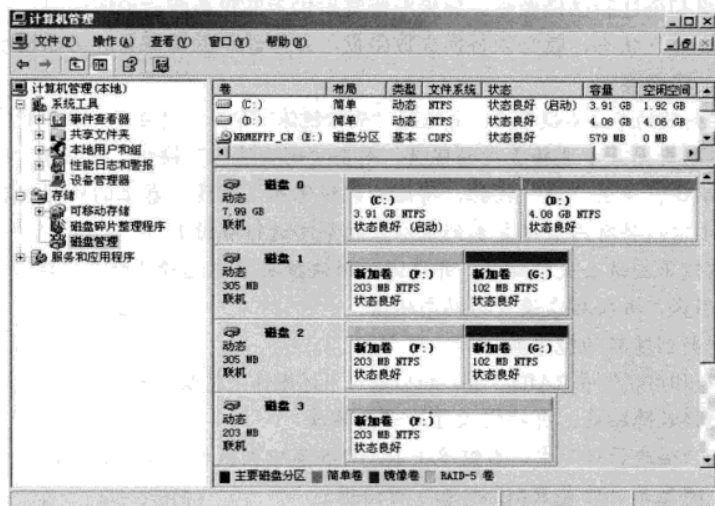


图 4-2-22 配置 RAID-1 和 RAID-5 的磁盘管理

3. RAID 卷的管理

● **添加镜像卷。**对于已有的动态磁盘，可以简单地通过添加镜像卷的方式来提高数据的安全性。在“磁盘管理”中，右键单击要添加镜像磁盘的动态磁盘，并在快捷菜单中选择“添加镜像”命令，此时将显示“添加镜像”对话框。在磁盘列表中选择要设置为镜像的动态磁盘，然后单击“添加镜像”按钮，至此镜像添加完成。需要注意的是，添加为镜像的磁盘空间必须大于或等于现存卷。

● **重新激活 RAID-5 磁盘。**如果 I/O 错误是暂时的，则可以尝试重新激活磁盘。在控制台中单击“磁盘管理”，然后右键单击局部出现故障的磁盘，然后单击“重新激活磁盘”命令，RAID-5 卷的状态应变为“正在重新生成”，最后变为“良好”。

● **软 RAID 的恢复。**磁盘冗余的目的就在于当磁盘出现故障时，系统能够保证数据的完整性。虽然在 RAID-1 和 RAID-5 中某个磁盘成员的失败不会导致数据丢失，其他成员仍然可以继续运转，但是如果失败不能得到及时恢复，那么磁盘卷将不再拥有冗余的特性。因此，必须及时恢复失败的 RAID-1 和 RAID-5。下面是针对“修复镜像卷和 RAID-5 卷”、“替换磁盘和创建新的镜像卷”、“替换磁盘和重新生成 RAID-5 卷”3 种情况给出操作步骤，但不作具体的演示。

(1) **修复镜像卷和 RAID-5 卷。**在“磁盘管理”中，失败卷的状态将显示为“失败的冗余”，磁盘之一将显示为“脱机”、“丢失”或“联机（错误）”。可以通过下述操作来恢复镜像卷。

首先确保该磁盘已经连接到了计算机，并且已经加电，然后在“磁盘管理”中，右键单击标识为“脱机”、“丢失”或“联机（错误）”的磁盘，然后在快捷菜单中单击“重新激活磁盘”命令，此时该磁盘的状态应当回到“良好”，同时镜像卷应该自动重新生成。如果磁盘被严重破坏或者不可能修复，在弹出的快捷菜单中将只能看到“删除”命令，此时 Windows Server 2003 将无法再修复该镜像卷。另外，如果磁盘连续显示“联机（错误）”，则有可能表明该磁盘很快就要发生故障

了,应当尽可能快地替换该磁盘。

(2) 替换磁盘和创建新的镜像卷。如果经修复后仍未能重新激活镜像磁盘,或者镜像卷的状态没有恢复到“良好”状态,就必须替换失败磁盘,并创建新的镜像卷。可以通过下述操作来替换磁盘和创建新的镜像卷。

STEP 1 在失败的卷上右键单击,并选择“删除镜像”命令,将显示“删除镜像”对话框。

STEP 2 从磁盘列表中选择丢失的磁盘,单击“删除镜像”按钮,将显示“磁盘管理”警告框,以提示用户确认,单击“是”按钮,将删除该镜像卷(注意:卷上的所有内容将消失,为安全起见,删除卷之前请将有用数据复制到卷以外的空间进行备份)。

STEP 3 右键单击该丢失的磁盘,并在弹出的快捷菜单中选择“删除磁盘”选项,将该磁盘删除。更换新的磁盘,并将磁盘设置为动态磁盘。

STEP 4 重新创建新的镜像卷。

(3) 替换磁盘和重新生成 RAID-5 卷。可以通过下述操作来替换磁盘和重新生成 RAID-5 卷。

STEP 1 更换故障磁盘,并将它设置为动态磁盘。

STEP 2 在“磁盘管理”中,右键单击 RAID-5 卷中失败的磁盘,在弹出的快捷菜单中选择“恢复卷”命令,将显示“修复 RAID-5 卷”对话框。

STEP 3 选择要在 RAID-5 卷中替换失败磁盘的磁盘,并单击“确定”按钮。此时 RAID-5 卷开始自动修复。

STEP 4 右键单击失败的磁盘,并在弹出的快捷菜单中选择“删除磁盘”命令,从系统中删除该磁盘。

● 测试镜像系统或启动卷。关闭计算机,然后断开或关闭某个磁盘以模拟磁盘故障,使用剩余镜像来重新启动计算机。验证 Windows 可正确启动后,关闭计算机然后重新连接磁盘,重新启动计算机。启动菜单出现时,选择仍保持连接状态的磁盘上的镜像。在控制台中单击“磁盘管理”,右键单击任何标有“失败的重复”的卷的磁盘,然后单击“重新激活磁盘”命令。有兴趣的读者可以在 RAID-1 卷和 RAID-5 卷中写入一些内容,关闭计算机,编辑虚拟机 1 的硬件配置,删除磁盘 2,重新启动计算机,观察保存的配置文件是否仍然存在。重新添加磁盘,恢复 RAID-1 卷和 RAID-5 卷。

4.2.2 文件夹管理

1. 查看文件和文件夹属性

文件夹属性包括文件夹所处的位置、文件夹大小、占用的磁盘空间、创建时间等。

文件属性包括文件类型、打开方式、文件夹位置,以及文档的创建时间、修改时间及上次访问时间。

在资源管理器中,用鼠标右键单击想要查看属性的文件或文件夹,选择“属性”命令,打开文件夹对话框,如图 4-2-23 所示。

【快问快答】如果服务器几天前被黑客攻入,如何查看黑客在服务器上新建了哪些文件?

答:一般黑客都会在服务器上安装服务,放置木马,只要查看指定日期内有哪些文件是被新建的,再加以排查,就可找出隐患。如果对每个文件都查看属性,其工作量可想而知,当然也是不可行的,这时可以使用 Windows 操作系统提供的强大的搜索筛选功能。打开搜索对话框,

展开“什么时候修改的”选项，选中“指定日期”，再选中“创建日期”，并填入日期范围，然后开始搜索，如图4-2-24所示。管理员根据搜索结果很快就可找出可疑的木马文件。

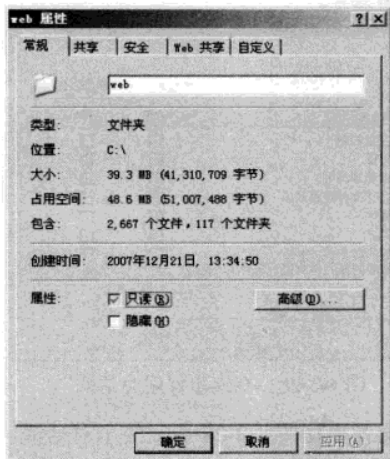


图 4-2-23 文件夹属性对话框



图 4-2-24 文件和文件夹高级搜索对话框

2. NTFS 分区的权限设置

为了确保用户能够按照所希望的进行操作，并减少破坏行为的发生，NTFS 的权限设置至关重要。NTFS 分区是 Windows Server 2003 推荐的系统分区格式，它比 FAT32 分区有更好的性能和更高的安全性，有关两者的比较这里不再多叙，仅对 NTFS 的权限进行介绍。如图 4-2-25 所示，选择“安全”选项卡，只有处在 NTFS 分区上的文件和文件夹才有“安全”选项卡。选中“组或用户名称”列表框中的对应用户，就可在下面窗口中设置该用户或组对此文件或文件夹的权限。如果欲操作的用户或组没有“在组或用户名称”列表框中出现，则需单击“添加”按钮把该用户或组添加进来。下面针对文件夹的 NTFS 权限进行介绍。

● 完全控制：指用户对该对象具有所有的权限，包括下面列出的所有权限和夺取该文件夹所有者的权限。

● 修改：具有“完全控制”中除夺取所有权以外的权限。

● 读取及运行：能查看该文件夹以及子文件夹

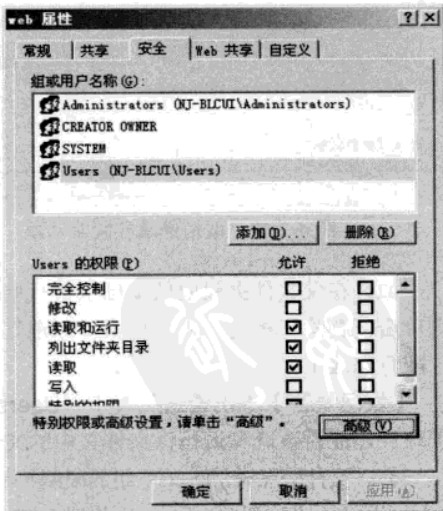


图 4-2-25 文件和文件夹的“安全”选项卡

下的内容,能执行文件,如 EXE 文件等,此权限也包括了“列出文件夹目录”和“读取”权限。

● 列出文件夹目录:只能浏览该文件夹以及子文件夹下的内容,但不能查看文件具体内容,当然也无法复制。

● 读取:能查看文件内容。

● 写入:能新建文件或文件夹,如果只具有此权限,其结果是用户可以在此文件下添加内容,但无法浏览此文件夹下的内容,更无法查看文件的具体内容。

【快问快答】为何不能取消 DATA 文件夹“安全”选项卡中“Users”用户组的“读取和运行”复选框的选中状态?

答:如图 4-2-26 所示,“安全”选项卡中的复选框不能取消是因为该文件夹的权限是从父文件夹中继承而来的,所以不能取消。如需特殊设置,可以先取消文件夹权限的继承,操作如下。

单击“高级”按钮,弹出如图 4-2-27 所示的对话框。取消“允许父项的继承权限传播到该对象……”复选框,此时会弹出如图 4-2-28 所示的子对话框。

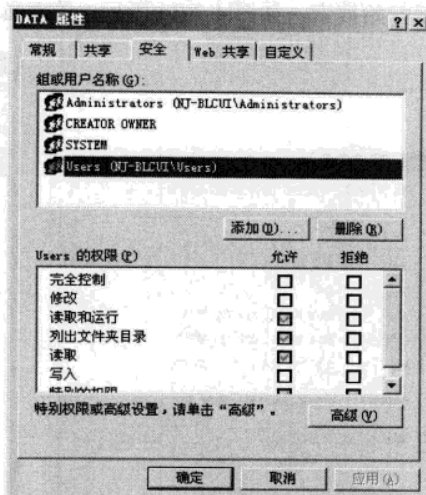


图 4-2-26 有继承权限对话框

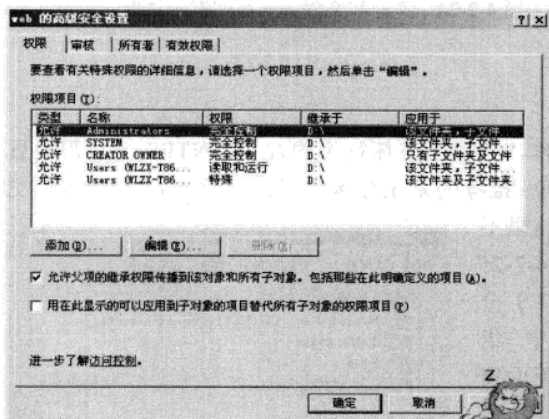


图 4-2-27 取消继承权限对话框

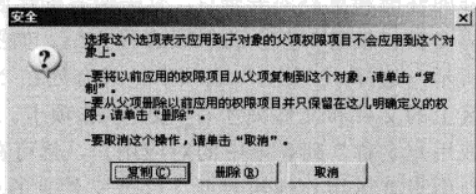


图 4-2-28 取消继承权限的子对话框

如果在父文件夹权限的基础上进行修改,可以单击“复制”按钮;如果重新设置该文件夹,则单击“删除”按钮,否则单击“取消”按钮。删除继承权限关系后,就可以对文件夹的权限进行随意修改了。

【快问快答】本机管理员属于“Users”组,如果清除“Users”组的“读取和运行”权限,管理员还能否读取和运行该文件夹中的文件?

答:这种情况对“Users”组的限制并不会影响管理员,原因是管理员既属于“Users”组,也属于 Administrators 组,Administrators 组对 DATA 文件夹具有完全控制的权限。当一个用户属于多个组时,用户的权限是多个组权限的累加,即用户权限具有累加性,管理员对 DATA 文件夹具有完全控制的权限。

【快问快答】取消或拒绝“Users”组的允许“读取和运行”权限，两者有何区别？

答：两者有本质性的区别，如果是选中了拒绝“读取和运行”权限，则管理员也无法对此文件夹进行读取和运行等操作。虽然管理员属于 Administrators 组，Administrators 组有“完全控制”的权限，而且用户权限具有累加性，按理说管理员仍可完全控制文件夹，但有一个特例，那就是“拒绝”权限具有最高的优先级，不管一个用户属于多少个组，只要其中一个组被拒绝某项权限，即使其他组都授予此项权限，该用户仍无法拥有此项权限。这也给用户提供一个方便，如果限制某个用户对某个文件或文件夹的操作，不需要对该用户属于的所有组进行操作，只要简单地拒绝该用户的此项权限即可。

实验 4-3 通过 NTFS 权限和用户管理确保计算机安全

如果别人要临时借用自己的计算机，而计算机上有一些重要或隐私的资料担心被删除或看到时，可以使用下面介绍的一种方法，执行的步骤如下。

STEP 1 新建普通用户。在虚拟机 1 中，选择“开始”→“程序”→“管理工具”→“计算机管理”，新添加一个用户，如“friend”，该用户默认是“Users”组中的成员，不要改变隶属关系。

STEP 2 限制用户权限。假设重要的数据保存在 D 盘，右键单击 D 盘，在快捷菜单中选择“属性”命令，打开 D 盘“属性”对话框，选择“安全”选项卡，如图 4-2-29 所示。

在“组或用户名称”列表框中添加“friend”用户，拒绝“friend”用户的所有权限，结果如图 4-2-30 所示。



图 4-2-29 “安全”选项卡

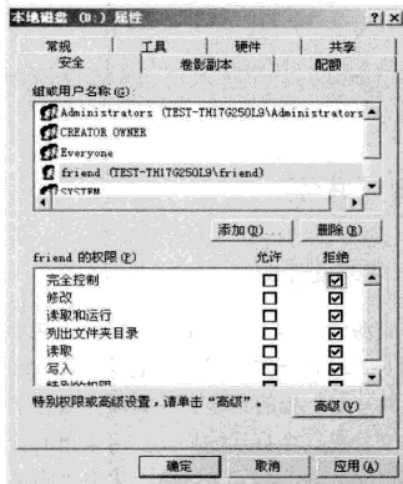


图 4-2-30 拒绝 friend 访问

单击“确定”按钮，系统提示拒绝权限的注意事项，单击“是”按钮，确认修改，如图 4-2-31 所示。

STEP 3 测试。单击“开始”→“关闭计算机”→“注销 administrator”，使用 friend 账号登录。打开资源管理器，当 friend 账号访问 D 盘时，遭到拒绝，如图 4-2-32 所示。

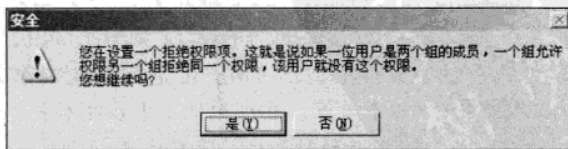


图 4-2-31 拒绝权限提示

friend 账号除了不能访问 D 盘外, 还有其他方面的限制, 如不能删除系统文件, 不能修改系统配置, 当尝试修改 IP 地址时, 屏幕提示没有权限执行这个操作, 如图 4-2-33 所示。

STEP 4 外借。经过上面的测试, friend 作为一个普通账号, 其功能受到限制, 把这个账号告诉借用自己计算机的人就可以了。

注意



这种方式的安全还是很脆弱的, 如果借用者把计算机的硬盘挂接在其他能识别 NTFS 的系统上可以读取 D 分区中的内容。此外使用 WinPE (Microsoft Windows Preinstallation Environment, Windows 预先安装环境, 简称 Windows PE 或 WinPE) 光盘或 U 盘引导系统, 也可以识别和复制 D 分区中的内容。本章 4.2.5 小节介绍的 EFS 加密, 可以有效阻止这种威胁。

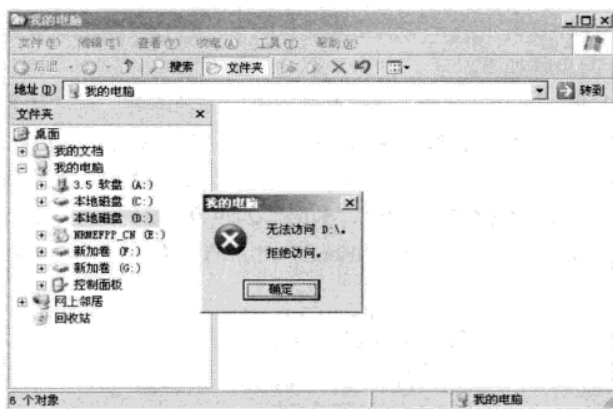


图 4-2-32 拒绝访问提示

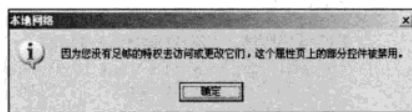


图 4-2-33 禁止访问或修改提示

4.2.3 共享

1. 共享文件夹

在资源管理器中, 右键单击任何想共享的文件夹, 在快捷菜单中选择“共享和安全”命令, 打开如图 4-2-34 所示的对话框。选中“共享该文件夹”单选按钮。选中后, 下面的一些选项即可设置, 其中“共享名”指的是该文件夹以什么名字出现在网络中, 不一定要与实际的文件名相同; “描述”是对该文件夹一个直观的描述, 用来帮助管理员识别该共享存在的目的或用途, 而且“描述”是可选项。只要填入“共享名”后, 单击“确定”按钮, 该文件夹就被成功共享。

实验 4-4 配置共享

默认情况下, 所有用户都能读取共享文件夹, 如果限制一些用户从网络上访问该文件夹或者允许一部分人有更高的特权, 则需额外的设置。如配置虚拟机 1, 实现除“friend”以外的用户都可以读取此共享文件夹, 并且只有管理员组的用户能完全控制该共享文件夹, 实现步骤如下。

STEP 1 设置共享。在虚拟机 1 中右键单击“d:\test”文件夹, 选择“共享和安全”命令, 弹出如图 4-2-34 所示的对话框, 设置共享。

STEP 2 设置权限。单击图 4-2-34 所示的“权限”按钮，弹出如图 4-2-35 所示的共享文件夹权限设置对话框。在此对话框的“组或用户名称”中默认只有 Everyone，被授予的权限是读取。为达到共享要求，单击“添加”按钮，把 Administrators 组加入，并允许“完全控制”。

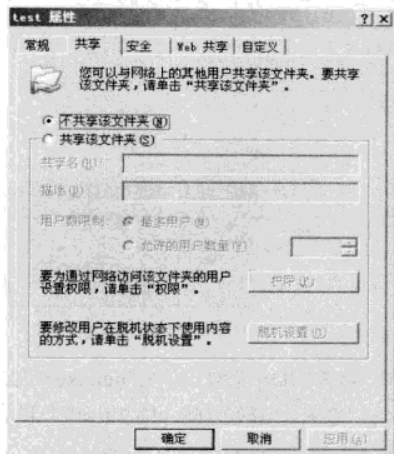


图 4-2-34 文件夹共享对话框

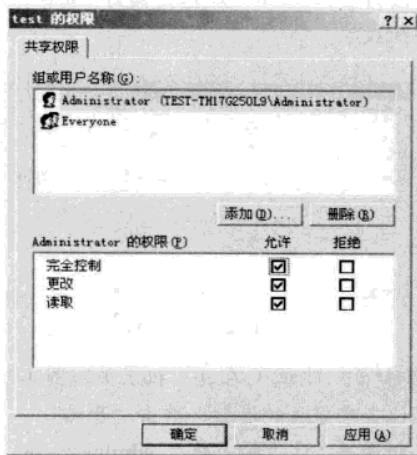


图 4-2-35 共享文件夹权限设置对话框

STEP 3 测试 1。在真实机上，单击“开始”→“运行”命令，输入“\\192.168.111.2\test”，提示输入用户名和密码，以 friend 账号登录，系统提示登录失败，如图 4-2-36 所示。既然允许 Everyone 读取，friend 账号又是 Everyone 中的一员，为何却不能读取呢？原因是从网络上访问共享资源的最终权限是本地安全权限和共享权限二者的交集，在实验 4-3 中，在本地安全权限中，拒绝了 friend 账号对 D 盘的访问，因为“d:\test”文件夹继承了根目录的权限，也拒绝 friend 账号的访问。最终导致 friend 账号从网络上无权访问共享文件夹“d:\test”。

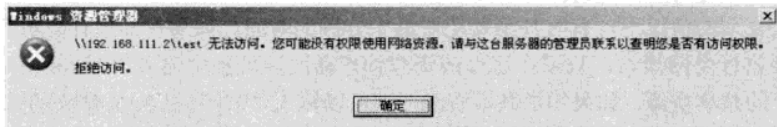


图 4-2-36 访问共享资源失败提示

STEP 4 测试 2。在真实机上关闭如图 4-2-36 所示的信息提示框，在打开的 DOS 窗口中输入“net use * /delete”，删除测试 1 中建立的连接，如图 4-2-37 所示。

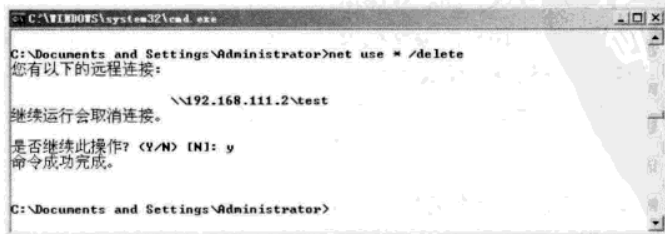


图 4-2-37 删除已建立的连接

在真实机上,单击“开始”→“运行”命令,输入“\\192.168.111.2\test”,提示输入用户名和密码,以虚拟机1上的一个普通账号,如“user1”登录,可以打开共享资源,如图4-2-38所示。

在如图4-2-38所示的窗口中,单击右键,选择“新建”→“文件夹”命令,系统提示拒绝访问,如图4-2-39所示。原因是因为“user1”属于Everyone中的一员,有读取的权限,但没有写入文件的权限。

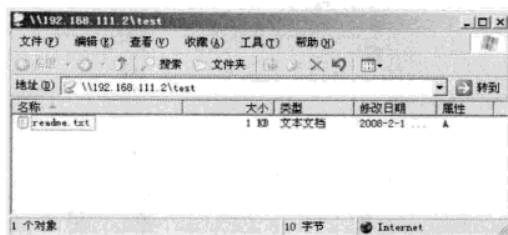


图 4-2-38 访问共享资源

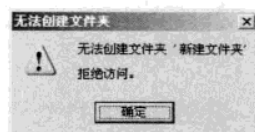


图 4-2-39 拒绝写入

STEP 5 测试3。在真实机上关闭图4-2-38所示窗口,打开DOS窗口,输入“net use * /delete”,删除测试2中建立的连接。单击“开始”→“运行”命令,输入“\\192.168.111.2\test”,提示输入用户名和密码,这次输入账号 administrator。再次打开图4-2-38所示窗口,单击右键选择“新建”→“文件夹”命令,文件夹被成功创建,如图4-2-40所示,因为 administrator 组成员有完全控制的权限。

【快问快答】 如何通过网络快速定位要访问的共享资源?

答:一些用户习惯双击网上邻居,再单击对应的计算机,然后再打开对应的共享资源,这种方法往往要浪费很长的时间,尤其是在网络庞大复杂的情况下,有时甚至要花费近十分钟的时间。如果在知道计算机名的情况下,完全没有必要进行全网搜索,只需在运行或资源管理器的地址栏中输入“\\计算机名”即可访问到该计算机上的共享资源。如果知道共享资源,则可以输入“\\计算机名\文件夹的共享名”,直接访问到共享文件夹,节省大量的时间。如果要访问的计算机不在本地网络内,通过计算机名搜索的效率就大打折扣,此时可以把计算机名换成对应的IP地址,就可以访问被授权的远程共享资源。共享在广域网上一概不可用,主要是因为大多数广域网路由器都阻止了网络共享服务。

【快问快答】 已把一个用户的共享权限设成“完全控制”,为何远程访问此共享文件夹时,仍只能查看,而不能进行添加、修改、删除等操作?

答:用户从远程访问共享文件夹的最终权限是“共享权限”和“本地安全权限”两者中最严格的,虽然把此用户的“共享权限”设成了允许“完全控制”,但在“本地安全权限”中,该用户的权限只是读取,取两者中最严格的权限,交集是“读取”,所以该用户从网络上只能读取此文件夹,而无其他特权。

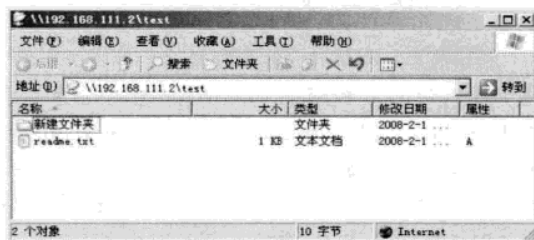


图 4-2-40 共享写入

2. Windows Server 2003 中存在的特殊共享资源

根据计算机的配置,系统将自动创建下列部分或所有特殊共享资源,以便于管理和系统本身

使用。在资源管理器中这些共享资源是不可见的，但在计算机管理中可以查看它们，如图 4-2-41 所示，不同配置的计算机看到的共享会有所不同（一些应用程序可能会产生额外的特殊共享资源）。

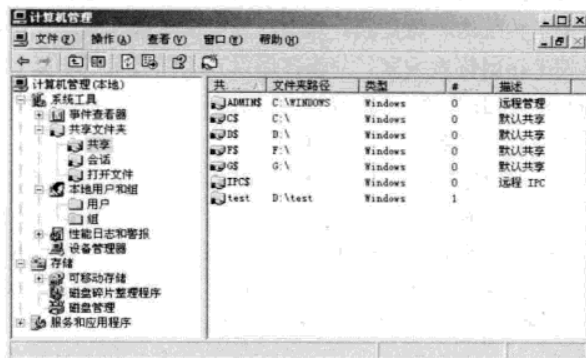


图 4-2-41 计算机中存在的共享

如图 4-2-41 所示，不难发现有些特殊的共享之所以不能从网上直接被发现，它们存在一个共同的特点，就是共享名的最后都有一个“\$”符号，共享名的最后加一个“\$”就表示此共享是隐藏共享。只有在明确知道此共享名的情况下才能访问，用户可以在任意文件夹共享名的最后加上“\$”来隐藏该共享。远程客户访问服务器的管理共享，如“D\$”，则需输入“\\此服务器的 IP 地址\d\$”，如果客户计算机的登录用户名和密码在此服务器中不存在或不是管理员的情况下，继续弹出验证窗口，只有输入合法的账号和密码（用户账号必须隶属于此服务器的管理员组）才能访问此类特殊共享。默认情况下 Windows Server 2003 的所有硬盘驱动器都是隐藏共享的，只有管理员组的用户才有权访问计算机的管理共享。除此之外还有“ADMIN\$”共享，它是计算机远程管理期间使用的资源，该资源的路径总是系统根目录路径（安装操作系统的目录，例如 C:\Windows）；“IPC\$”为共享命名管道的资源，在程序之间的通信过程中，该命名管道起着至关重要的作用，在计算机的远程管理期间，以及在查看计算机的共享资源时，使用“IPC\$”。

3. 管理和查看共享资源

如图 4-2-41 所示可以看到本机所有存在的共享，包括隐藏的共享（试图在资源管理器中找出本机所有的共享是不现实的），也可在此新建共享、更改共享、停止共享。还可以在“会话”中查看有哪些用户正在访问本机的共享资源，进一步在“打开文件”中可以看到这些用户在对哪些文件进行什么样的操作。

同时，微软提供了命令行下查看本地共享的方式。使用“net share”命令可以方便地查看到本机上的所有共享。

【快问快答】为了安全起见，停止所有的管理共享，即“C\$”、“D\$”等，可计算机每次重启后这些共享又出现了，如何才能停止这些默认的管理共享呢？

答：停止默认的管理共享，需在注册表添加双字节项“AutoShareServer”，并把值设成“0”，如下所示：

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters]
AutoShareServer = DWORD: 00000000
```

实验 4-5 在网络中实现打印机的安全共享

网络的出现改变了人们的生活,网络打印机的使用,不仅节约办公成本,同时也方便了人们的操作。网络打印,避免了传统的软盘复制。然而,随着微软操作系统的不断推陈出新,不同操作系统之间的打印共享越来越困扰着大家。共享打印设置不当会造成不必要的浪费。甚至还会被恶意利用,尤其是 Internet 日益普及的当今,实现网络打印机的安全共享更是显得尤为重要。Windows Server 2003 作为打印服务器的设置步骤如下。

STEP 1 配置服务器。默认情况下 Windows Server 2003 的 Guest 账户是被禁用的,最简单的方法就是启用 Guest 账户,但不安全因素随之出现。当 Windows Server 2003 启用 Guest 账户并将打印机设成共享后,默认权限是 Everyone 都可打印,也就是说任何能连接到打印服务器的用户都可以使用共享打印机,因此这样的做法不可取。实现安全共享的方法是不要启用 Guest 用户,在 Windows Server 2003 中新建一个普通用户,并设置密码。

STEP 2 Windows 98 客户端设置。Windows 98 客户端每次以刚刚新建的用户名和密码登录 Windows 98 系统,当 Windows 98 的客户端试图访问 Windows Server 2003 的共享打印机时就会用登录时的用户名和密码去验证,刚好 Windows Server 2003 中有这样的用户名和密码,验证通过,可以正常使用打印机。

STEP 3 Windows Server 2003 系列(包括 Windows 2000 和 Windows XP 的操作系统)客户端设置。Windows Server 2003 系列客户端访问网络打印服务器时,提示输入用户名和密码,Windows Server 2003 客户端输入打印服务器上的普通用户名和密码,成功访问打印服务器。如果不想每次访问打印服务器时都需要输入用户名和密码,可以选择记住密码。

经过上面的设置,不仅实现了网络打印机的安全共享,而且充分利用网络打印的灵活和方便。

4.2.4 卷影复制

在以往的 Windows 文件服务器资源共享中,当客户端不小心将共享文件删除或覆盖时,管理员就必须重建共享文件,以便共享资源能够恢复正常。在 Windows Server 2003 中,这种问题都随着“共享文件夹的卷影复制”功能的出现,而有了彻底的解决。卷影复制服务(Volume Shadow Copy Service, VSS)是 Microsoft 在 Windows Server 2003 中开始引入的服务,实质上就是可以对现有的共享资源进行复制的技术,在使用卷影复制功能后,服务器会按指定的时间自动(也可以使用手工方式)、不断地按时(默认状态为两天进行一次卷影复制操作)对共享文件夹的属性进行复制。当客户端对服务器中的共享资源进行了删除、更改、覆盖等操作后,如果想恢复原来的共享资源,就可以调用这些共享资源在服务器上使用“卷影复制”功能后产生的“版本”进行恢复了。它能让用户在没有 IT 专业人员协助的情况下,更轻松地恢复丢失的共享文件。

此外, VSS 还提供了更灵活的备份方案。结合了良好的规划以及最新的备份和恢复技术,卷影复制服务将对灾难恢复计划的增强很有帮助。VSS 甚至让小企业也有恢复丢失数据的能力。其实, VSS 也为大企业提供更比基本工具更多的恢复选项,并帮助其减少数据恢复任务中 IT 专业人员的数量。

1. 卷影复制服务能做什么

通过使用 VSS, 可以在特定卷上建立数据复制时间点, 并在将来的某一时刻把数据恢复到任何一个曾创建的时间点的状态。VSS 可以帮助客户恢复意外删除的文件, 使一般员工也能轻松完成, 并且不需要创建高效备份策略。

对于 IT 技术支持人员来说, 最常见的问题一般是恢复人为原因造成的数据丢失。用户不经意地存储了有错误信息的文件, 不小心删除文件, 或是其他的数据意外都是经常发生的。当用户需要重新找回数据的时候, 经常需要请技术支持人员拔出备份磁带, 进行人工恢复, 这个工作相当浪费时间。

VSS 让管理员能够在服务器上发布共享文件夹, 在一定的时间间隔内做时间点的备份 (在指定时间内最多可以存在 65 份拷贝)。这让最终用户能够安全地处理文件并随时恢复到早前的版本, 而不需要 IT 部门的人工支持。

2. 应用卷影复制服务时的注意事项

这一服务唯一的缺点就是需要为每一个卷影留出更多的磁盘空间, 因为必须在某处存储这些拷贝。不过, 因为 VSS 使用指针数据, 这些拷贝占用的空间要比想象的小得多, Windows Server 2003 可以有效地存储这些拷贝。

用户还可以将复制与备份工具和 VSS 配合使用, 将拷贝移动到另一个 VSS——其他站点的可用服务器。因此, 如果原始服务器在灾难中崩溃了, 最终用户还是可以访问他们的数据。由于 VSS 在一定时间间隔内做一次快照, 并且在母文件使用时并不锁定它们, 因此开放文件锁定并不会影响到复制与备份工具。除了复制开放文件以外, 还可以在最终用户处理文件的时候备份 VSS 快照。这一功能通过消除备份窗口、开放文件锁定和其他的障碍, 显著地提高了备份能力。

实际应用中也许还将遭遇 CPU 利用问题 (在运行备份代理的时候) 和 LAN 利用问题 (在跨越网络进行数据备份的时候), 不过这并不妨碍最终用户使用文件。

备份 VSS 快照产生干净的数据镜像以及恢复时间点拷贝的能力。既可以恢复整个快照, 还可以使用 VSS 备份工具来恢复单独的文件和文件夹。

因为基于时间点来备份文件拷贝, 所以可以很轻松的使用复制工具即时地将 VSS 快照移动到另一台灾难恢复站点中的服务器上, 并在那里进行备份, 创建脱机的默认备份。通过将备份保存在脱机位置会发现实施灾难恢复系统变得相当简单, 而且备份系统能平滑地协同工作。

3. 如何在服务器上配置卷影副本

前提条件必须是使用 NTFS 分区的磁盘分区才能使用共享文件夹的卷影复制功能, 在真实机的资源管理器中选中要启用“卷影副本”的驱动器, 在驱动器的属性窗口中选择“卷影副本”选项卡, 如图 4-2-42 所示。

单击“启用”按钮, 启用 C 盘的卷影副本功能, 再单击“设置”按钮, 如图 4-2-43 所示, 进一步设置卷影副本存放的位置和大小、以及创建卷影副本的计划安排。

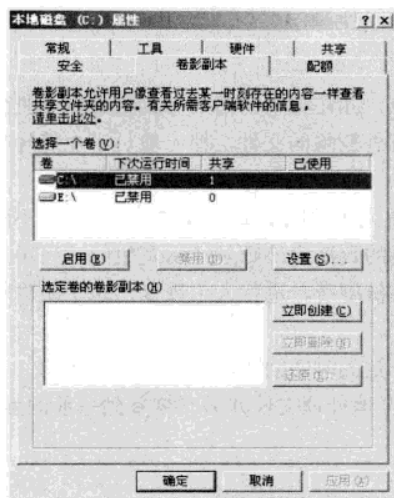


图 4-2-42 启用卷影副本

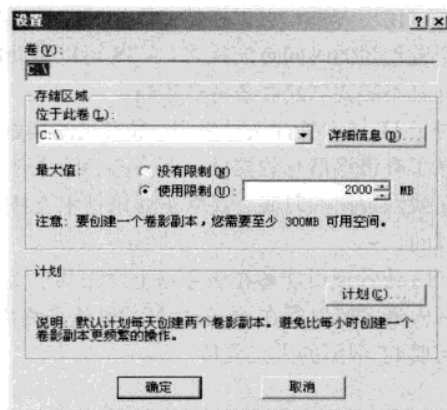


图 4-2-43 配置卷影副本

4. 卷影副本的客户端软件

要使用卷影副本功能，需在客户端上安装卷影副本客户端程序，它位于 Windows Server 2003 服务器的“%systemroot%\system32\clients\twclient\x86\twcli32.msi”中，只能安装在 Windows XP 或更新版本的操作系统上。这里在虚拟机 1 上安装卷影副本的客户端软件。

5. 共享资源的还原

客户端软件安装完成后就可以使用卷影副本功能了。在虚拟机 1 上找到要还原的服务器共享文件夹，右键单击，在快捷菜单中选择“属性”命令，选择“以前的版本”选项卡，如图 4-2-44 所示。接着在“文件夹版本”列表框中根据时间选择一个需要的副本文件，单击“还原”按钮，稍候将弹出一个名为“以前的版本”提示框，根据提示单击“是”按钮后，系统将开始执行共享文件的还原操作。

因为还原操作实际上是在服务器中进行的，所以还原过程十分迅速。当客户端看到弹出“已将文件成功还原到上一个版本”的提示框后，该文件夹就恢复到原来的状态了。有兴趣的读者不妨在真实机和虚拟机 1 上完成该实验。

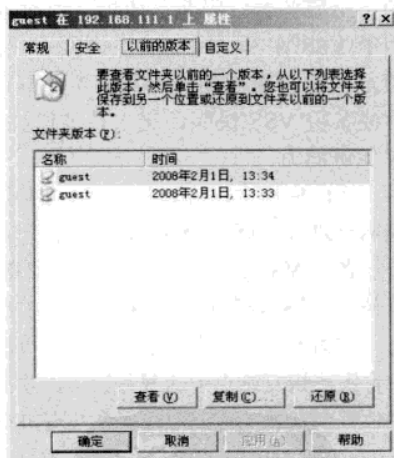


图 4-2-44 恢复以前的版本

注意

远程用户对共享文件夹要有修改的权限。

4.2.5 EFS 加密和安全

Windows 2000, Windows XP, Windows Server 2003 等操作系统的文件加密功能强大并且简单易用,因而许多用户都使用它来保护自己的重要文件,但由于大部分用户对该功能了解不足,在使用过程中经常出现问题,如不做任何准备就重装操作系统,那很可能导致以前的加密数据无法解密。下面对 EFS 的使用和安全性问题进行介绍。

1. EFS 加密

EFS (Encrypting File System, 加密文件系统) 是 Windows 2000/XP/2003 等所特有的一个实用功能,对于 NTFS 卷 (FAT、FAT32 卷并不支持加密) 上的文件和数据,都可以直接被操作系统加密保存,在很大程度上提高了数据的安全性。

EFS 加密是基于公钥策略的,在使用 EFS 加密一个文件或文件夹时,系统首先会生成一个由伪随机数组成的 FEK (File Encryption Key, 文件加密密钥),然后将利用 FEK 和数据扩展标准 X 算法创建加密后的文件,并把它存储到硬盘上,同时删除未加密的原始文件。随后系统利用公钥加密 FEK,并把加密后的 FEK 存储在同一个加密文件中。而在访问被加密的文件时,系统首先利用当前用户的私钥解密 FEK,然后利用 FEK 解密出文件。在首次使用 EFS 时,如果用户还没有公钥/私钥对 (统称为密钥),则会首先生成密钥,然后加密数据。如果用户登录到域环境中,密钥的生成依赖于域控制器,否则它就依赖于本地机器生成。

2. EFS 加密的优点

首先,EFS 加密机制和操作系统紧密结合,用户不必为了加密数据安装额外的软件,这节约了使用成本。

其次,EFS 加密系统对用户是透明的。这也就是说,如果加密了一些数据,那么对这些数据的访问将是完全透明的,并不会受到任何限制。EFS 加密的用户验证过程是在登录 Windows 时进行的,只要登录到 Windows,就可以打开任何一个被登录用户加密过的文件。

最后,EFS 加密是安全的。其他非授权用户试图访问加密过的数据时,就会收到“访问拒绝”的错误提示。即使非法用户取得了数据的存取权,仍无法浏览文件内容。

实验 4-3 中,计算机被别人借用,虽然没有告诉他们超级用户的密码,并且限制他们对 D 盘的浏览,但这并不能保证数据不会泄露,如果他们把计算机的硬盘挂接到另一台能识别 NTFS 分区的系统上,所有的数据将暴露无遗。如果采用了 EFS 加密,即使把硬盘挂接到其他操作系统上,也无法读取 EFS 加密过的文件。

3. 使用 EFS 加密/解密

鼠标右键单击需要加密的文件或文件夹,然后选择“属性”命令,在文件或文件夹属性窗口中,单击“常规”选项卡中“高级”按钮,在“高级属性”窗口中选中“加密内容以便保护数据”,如图 4-2-45 所示,然后单击“确定”按钮,等待片刻数据就加密完成。

如果加密的是一个文件夹,系统还会询问是否把这个加密属性应用到该文件夹还是该文件夹以及内部的所有子文件夹和文件,如图 4-2-46 所示,用户可以根据需要进行选择。

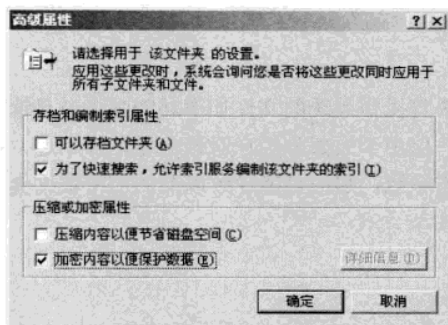


图 4-2-45 加密文件夹

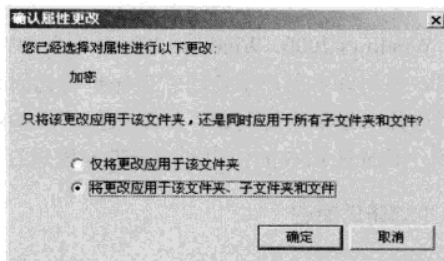


图 4-2-46 加密文件夹提示

解密数据也很简单的，同样是按照上面的方法，取消对“加密内容以便保护数据”复选框，然后单击“确定”按钮，即完成解密。

4. EFS 保障数据的安全

在 EFS 加密体系中，数据是依靠 FEK 加密的，而 FEK 又会和用户的公钥一起加密保存。解密的时候顺序刚好相反，首先用私钥解密出 FEK，然后用 FEK 解密数据。可见，用户的密钥在 EFS 加密中起了很大作用。

密钥又是怎么来的呢？在 Windows 2000/XP/2003 中，每一个用户都有一个 SID (Security Identifier, 安全标示符) 以区分各自的身份，每个人的 SID 都是不相同的，并且有唯一性。可以这样理解，把 SID 想象成人的指纹，虽然世界上已经有几十亿人（同名同姓的也有很多），可是理论上还没有哪两个人的指纹是完全相同的。因此，这具有唯一性的 SID 就保证了 EFS 加密的绝对安全和可靠。在第一次加密数据的时候，操作系统就会根据加密者的 SID 生成该用户的密钥，并把公钥和私钥分开保存起来，供用户加密和解密数据。因为理论上没有 SID 相同的用户，因而用户的密钥也就不会相同，即使在同一台计算机上删除用户后再新建一个同名的用户，他们的 SID 也是不同的。这一切都保证了 EFS 机制的可靠。

5. 做好 EFS 的灾难恢复

如何避免不慎使用 EFS 加密带来的损失？EFS 机制在设计的时候就考虑到了多种可能的突发情况，如操作系统瘫痪，加密文件的所有者离开等，有两种方法用来解决突发事件，那就是使用“备份密钥”和“恢复代理”。

(1) 备份密钥。有许多用户在系统发生故障或重新安装系统以后，无法再访问以前他们加密过的文件，也没有任何办法恢复以前的数据。因为 Windows 内建的加密功能与用户的账户关系非常密切，同时用于解密的用户密钥也存储在系统内，任何导致用户账户改变的操作和故障都有可能带来灾难，要避免这种情况的发生，必须未雨绸缪，在使用加密功能后马上备份加密密钥。

备份密钥的操作并不复杂。首先以要备份加密密钥的用户的身份登录，单击“开始”→“运行”命令，输入“certmgr.msc”打开证书管理器，在左边窗口中单击“证书—当前用户”下的“个人”中的“证书”，然后在右边窗口中用鼠标右键单击“预期目的”是“加密文件系统”的证书（如果右边窗口中没有出现登录用户的账户名，则是因该账户从未进行过加密文件的操作），右键单击

对应的账户，选择“所有任务”→“导出”命令，如图 4-2-47 所示。

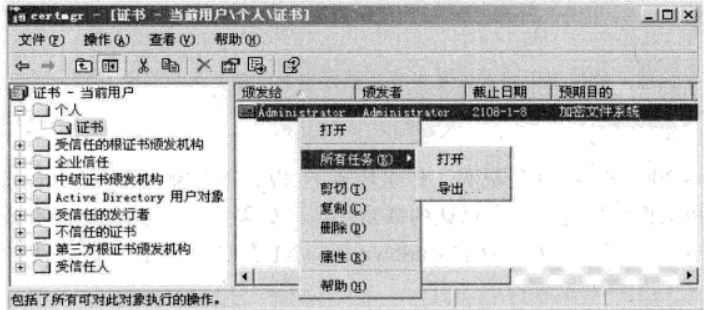


图 4-2-47 导出密钥

系统将打开“证书导出向导”指引操作，单击“下一步”按钮继续，向导将询问是否需要导出私钥，应该选择“导出私钥”，如图 4-2-48 所示，单击“下一步”按钮继续。

在“导出文件格式”窗口中保持默认的选项，如图 4-2-49 所示。单击“下一步”按钮继续，并按照向导的要求输入密码保护导出的私钥，然后选择存储导出后文件的位置即可完成。

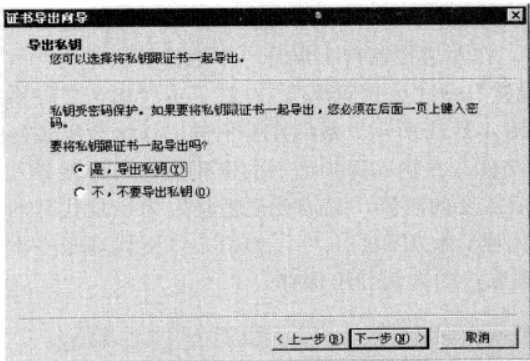


图 4-2-48 导出私钥

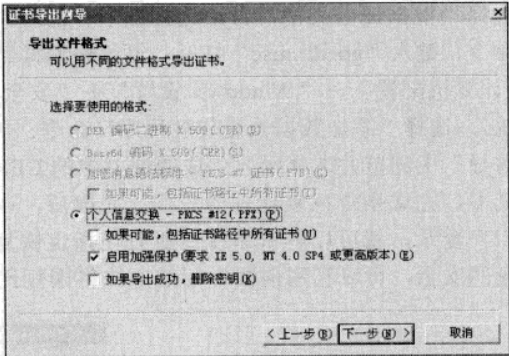


图 4-2-49 导出文件格式

建议将导出的证书存储在系统盘以外的其他磁盘上；以避免在使用 Ghost 之类的软件恢复系统时将备份的证书覆盖掉。备份后，当加密文件的账户出现问题或重新安装了系统后需要访问或解密以前加密的文件时，以任意账户登录操作系统，单击鼠标右键之前导出的“PFX”文件，选择“安装 PFX”，系统将弹出“证书导入向导”指引操作，只需要键入当初导出证书时输入用于保护备份证书的密码，然后选择“根据证书类型，自动选择证书存储区”，完成后该账号就可以访问以前被其他账户加密的文件了。

(2) 使用恢复代理。通过上面“备份密钥”的方法可以保证个人加密数据的安全，但对一个企业来说，网络管理员很难要求人人都备份密钥，而且由于人员流动离开企业，那么他加密的数据别人就没有办法再访问到。对于一个企业来说，需要让一个用户能解开所有账户的加密数据，以备应急，那就要使用“恢复代理”功能。因为被 EFS 加密过的文件，除了加密者本人之外还有恢复代理可以打开。恢复代理可以解密系统内所有通过内建加密功能加密的文件，用于网络管理员在网络上处理文件故障，并能使管理员在员工离职后解密其加密的工

作资料。

注意



恢复代理只能解密指定恢复代理后被加密的文件，所以应该在所有人开始使用加密功能前先指定恢复代理。

对于 Windows 2000 来说，在单机和工作组环境下，默认的恢复代理是 Administrator。Windows XP/2003 在单机和工作组环境下没有默认的恢复代理，如果需要恢复代理则必须自行指定。而在域环境中就完全不同了，所有加入域的 Windows 2000/XP/2003 计算机，默认的恢复代理全部是域管理员。

如果只是在使用一台单独的计算机，可以按照下面的步骤指定恢复代理。首先使用准备指定为恢复代理的用户账户登录，该用户必须是管理员或者拥有管理员权限的管理组成员，单击“开始”→“运行”命令，输入“cmd”打开 DOS 窗口，在命令行窗口中键入“cipher /r: d:\ab.txt”（ab.txt 可以是任何文件），命令行窗口将提示输入保护证书的密码，在 D 盘根目录生成两个文件，一个是 PFX 文件，一个是 CER 文件，如图 4-2-50 所示。

首先使用鼠标右键单击 PFX 文件，选择“安装 PFX”命令，通过弹出的“证书导入向导”选择“根据证书类型，自动选择证书存储区”导入证书。接下来再单击“开始”→“运行”命令，键入“gpedit.msc”打开“组策略编辑器”，在左边控制台上展开“本地计算机策略”→“计算机配置”→“Windows 设置”→“安全设置”→“公钥策略”，右键单击“加密文件系统”，选择“添加数据恢复代理程序”命令，如图 4-2-51 所示。最后在弹出的“添加数据恢复代理向导”中浏览并选择刚才生成的证书中的 CER 文件，在输入保护证书的密码后，向导将导入证书，完成指定恢复代理的工作。完成后，以后需要的时候，只需使用被指定为恢复代理的账户登录，就可以解密系统内所有在指定恢复代理后被加密的文件，如担心恢复代理账号本身的安全，可以利用前面介绍的方法将恢复代理账户的密钥导出保存。

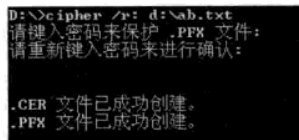


图 4-2-50 单独计算机的恢复代理

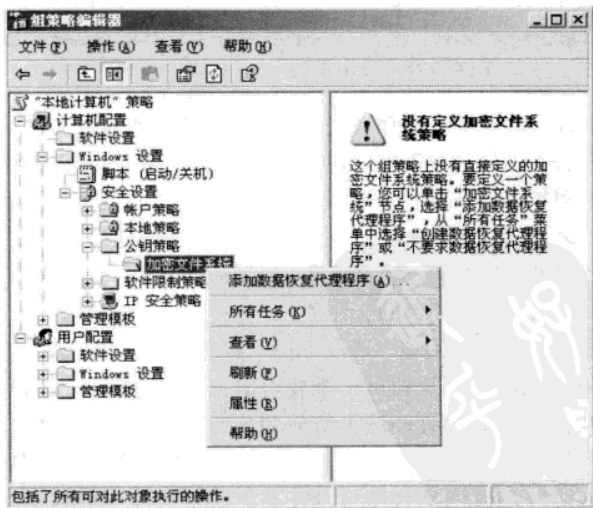


图 4-2-51 在组策略编辑器中添加恢复代理

6. 在本机上共享经 EFS 加密过的数据

加密过的文件只有加密者本人和恢复代理可以打开,如果要和本机的其他用户共享加密文件该怎么办?这种情况在 Windows 2000 中是不行的,不过在 Windows XP/2003 中可以做到。如果需要,可赋予其他用户对加密文件的完全访问权限,但要首先明确,Windows 所采用的是基于密钥的加密方案,并且是在用户第一次使用该功能时才为用户创建用于加密的密钥,因此准备赋予权限的用户也必须曾经使用过系统的加密功能,否则将无法成功赋予对方权限。Windows XP/2003 内建的文件加密功能只允许赋予其他用户访问加密文件的完全权限,而不允许将加密文件夹的权限再赋予给其他用户。

要赋予或撤销其他用户对加密文件的访问权限,可用鼠标右键单击已加密的文件,选择“属性”命令,在“属性”对话框的“常规”选项卡上单击“高级”按钮,在“高级属性”对话框中单击“详细信息”按钮,即可通过“添加”和“删除”按钮添加或删除其他可以访问该文件的用户。这里还可以查看文件的恢复代理账户,如图 4-2-52 所示。

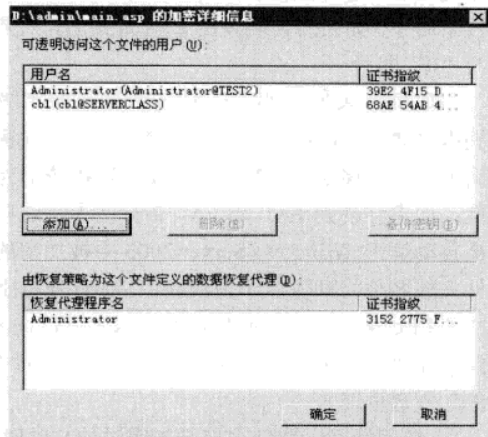


图 4-2-52 赋予或撤销其他用户对加密文件的访问权限

7. 禁止加密功能

在多用户共用计算机的环境下,可以将其他用户指定为普通用户权限,限制他们使用某些功能,但由于普通用户账号默认允许使用加密功能,因此一些多用户共用的计算机上经常会带来一些困扰。如果担心计算机上其他用户随意加密磁盘上的文件,可以将特定的文件夹设置成禁止加密,也可以完全禁止文件加密功能。

如果希望将某个文件夹设置为禁止加密,可以编辑一个文本文件,内容包括“[Encryption]”和“Disable=1”两行,然后命名为“Desktop.ini”,将其放到不希望被加密的文件夹中,并把该文件的安全权限只授予管理员即可。当其他用户试图加密该文件夹时,系统将提示用户该文件夹加密功能被禁止,如图 4-2-53 所示。但需要注意,只能使用这种方法禁止其他用户加密该文件夹,文件夹中的子文件夹将不受限制。

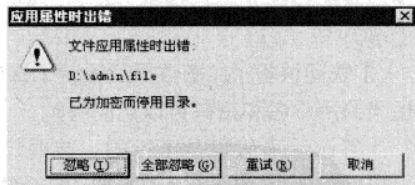


图 4-2-53 禁止文件夹加密提示

如果需要也可以完全禁止文件加密功能,在 Windows 2000 中,只需使用 Administrator 登录后右键单击如图 4-2-51 所示的“加密文件系统”→“属性”按钮,在属性对话框上取消“允许用户使用文件加密系统(EFS)来加密文件”复选框上的选中标记,如图 4-2-54 所示,然后重新启动计算机即可。

在 Windows XP/2003 上虽然也有相应的选项,但实际上并不能够起作用,需要通过编辑注册

表才能禁止文件加密功能。单击“开始”→“运行”命令，输入“Regedit”并按下回车键，打开注册表编辑器，找到 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\EFS，在“编辑”菜单上单击“新建”→“Dword 值”，输入“EfsConfiguration”作为键名，并设置键值为“1”，这样本机的 EFS 加密就被禁用了。如果想重新使用 EFS 加密时，只要把键值改为“0”即可。

如果把未加密的文件复制到具有加密属性的文件夹中，这些文件将会被自动加密。若是将加密数据移动出来，如果移动到 NTFS 分区上，数据依旧保持加密属性；如果移动到 FAT 或 FAT32 分区上，这些数据将会被自动解密。Windows Server 2003 中被加密的文件和文件夹的名称将默认显示为淡绿色，如计算机上被加密的文件和文件夹的名称不是彩色显示，可以选择“我的电脑”→“工具”→“文件夹选项”命令，然后在“文件夹选项”对话框中单击“查看”选项卡，选中“以彩色显示加密或压缩的 NTFS 文件”复选框即可。

【快问快答】为什么打开加密过的文件时不需要输入密码？

答：这正是 EFS 加密的一个特性，同时也是 EFS 加密和操作系统紧密结合的最佳证明。因为跟一般的加密软件不同，EFS 加密不是靠密码来确认用户身份的，EFS 加密的用户确认工作在登录到 Windows 时就已经进行了。一旦用适当的账户登录，就能打开相应的加密文件，并不需要提供什么额外的密码。

【快问快答】加密文件已经打不开了，可以通过把 NTFS 分区转换成 FAT32 分区来挽救文件吗？

答：这当然是不可能的了。很多人尝试过各种方法，如把 NTFS 分区转换成 FAT32 分区。使用 NTFS DOS 之类的软件到 DOS 环境下把文件复制到 FAT32 分区等，不过这些尝试都以失败告终。毕竟 EFS 是一种加密方法，而不是一般的权限之类的限制，这些方法对付 EFS 加密都是无济于事。

【快问快答】加密数据后重装了操作系统，现在加密数据不能访问了，如果使用跟前一个系统相同的用户名和密码可以访问吗？

答：这当然也是不行的，前面已经介绍过，和 EFS 加密系统密切相关的密钥是根据每个用户的 SID 得来的。尽管在新的系统中使用了相同的用户名和密码，但是这个用户的 SID 已经变了。

【快问快答】被 EFS 加密过的数据是不是就绝对安全？

答：当然不是，安全永远都是相对的。以被 EFS 加密过的文件为例，如果没有合适的密钥，虽然无法打开加密文件，不过仍然可以删除（有些破坏者确实会这样想，竟然敢加密，不让我看！那好，删了它，谁都别想看）。所以对于重要文件，最佳的做法是 NTFS 权限和 EFS 加密并用，同时还要做好备份。

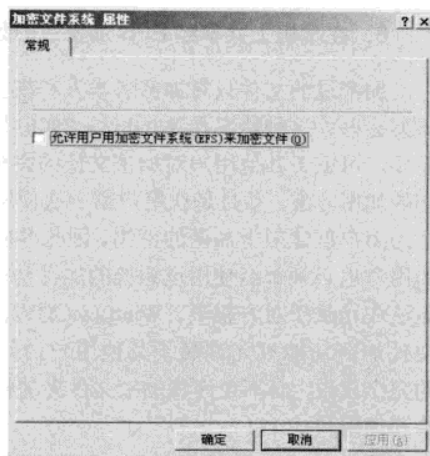


图 4-2-54 禁用文件加密

4.2.6 备份和还原

本节介绍一些经常需要备份的资源，包括网络参数，数据文件，操作系统，以备灾难恢复时使用。

实验 4-6 使用 Netsh 命令备份网络设置

谈到网络设置，一定会想到 IP 地址、子网掩码、网关、DNS 等，这些主要是接口 IP 配置参数。对于普通计算机来说，网络设置只有接口 IP 配置参数；而对于服务器而言，网络设置不仅仅包括前面所提到的接口 IP 配置参数，还有接口配置、端口代理配置、远程访问配置、路由配置、DNS 代理配置、NAT 配置、DHCP 中继代理配置等。上述的网络设置参数，根据服务器在网络中所起的特殊作用而有所不同。假如用 Windows Server 2003 服务器负责连接外网，并且连接内部多个子网，那么在该服务器上就要设置远程访问配置、路由配置、DNS 代理配置以及 NAT 配置。只有对上述网络设置做了适当、有效的备份，当遇到毁灭性破坏时，才能迅速及时地恢复网络。“Netsh”是 Windows Server 2003 操作系统自身提供的命令行脚本实用工具，它允许用户在本地或远程显示或修改当前正在运行的计算机的网络配置。为了存档、备份或配置其他服务器，Netsh 也可以将配置脚本保存在文本文件中。在虚拟机 1 上完成该实验，操作步骤如下。

STEP 1 查看当前接口配置 IP 参数。在 DOS 窗口中执行“ipconfig”，结果如图 4-2-55 所示。

```

C:\WINDOWS\system32\cmd.exe
C:\>ipconfig

Step 1, 查看当前IP配置参数

Windows IP Configuration

Ethernet adapter 本地连接:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.111.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.111.1

C:\>netsh dump > c:\back.txt

Step 2, 备份网络配置

C:\>netsh interface ip set address "本地连接" dhcp

Step 3, 修改IP为自动获取确定。

C:\>ipconfig

Step 4, 查看当前IP配置参数

Windows IP Configuration

Ethernet adapter 本地连接:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 0.0.0.0
    Subnet Mask . . . . . : 0.0.0.0
    Default Gateway . . . . . : 

C:\>netsh exec c:\back.txt > temp.txt

Step 5, 恢复网络配置

C:\>ipconfig

Step 6, 查看当前IP配置参数

Windows IP Configuration

Ethernet adapter 本地连接:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.111.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.111.1
  
```

图 4-2-55 Netsh 备份网络配置

STEP 2 备份网络设置。在 DOS 窗口输入 “netsh dump >c:\back.txt”，如图 4-2-55 所示，将网络设置参数备份到 c:\back.txt 文件中，该文件为一个文本文件。

STEP 3 修改网络设置。修改网卡的 IP 地址为自动获取，在 DOS 窗口中输入 “netsh interface ip set address “本地连接” dhcp”，如图 4-2-52 所示。

STEP 4 查看当前接口配置 IP 参数。在 DOS 窗口中执行 “ipconfig”，结果如图 4-2-52 所示。

STEP 5 恢复网络设置。在进行网络设置调整时，如果发生了操作错误，或者网络出现故障，可以利用备份快速恢复网络设置。操作方法是在 DOS 窗口中输入 “netsh exec c:\back.txt >temp.txt”，如图 4-2-52 所示。“>temp.txt” 不是必需的，用在这里主要是把屏幕的输出转到 “temp.txt” 文件中。

STEP 6 查看当前接口配置 IP 参数。在 DOS 窗口中执行 “ipconfig”，结果如图 4-2-52 所示。

通过 Netsh 命令对网络设置进行备份，操作简单方便，而且快速有效，无需其他软件辅助，非常适合网络管理人员用来对网络设置进行备份和恢复。

实验 4-7 远程定期自动备份指定数据

数据备份是日常工作中的重中之重。这里介绍一种方法可以异机定期自动备份用户指定的数据并且不需要增加任何投资。假设要将 “虚拟机 1” 的 “d:\web” 文件夹下的所有内容在每天 23 点自动备份到 “真实机” 的 “d:\backup” 文件夹中，其中 “真实机” 的 IP 为 192.168.111.1。“真实机” 的管理员账号是 administrator，密码是 123456。该备份的执行分为两大步骤。

STEP 1 编写批处理文件。在 “虚拟机 1” 上新建一个 “.bat” 结尾的批处理文件，如文件名叫 “backup.bat”，文件的内容如下：

```
net use z: \\192.168.111.1\d$ 123456 /user:administrator
xcopy d:\web\*. * z:\backup /E/Y
net use z: /delete
```

此 3 行简单的命令即可实现将 “虚拟机 1” D 盘 web 文件夹中的所有文件备份到 “真实机” 的 D 盘的 backup 文件夹中。对其中的每条命令说明如下。

● “net use” 映射网络驱动器，将远程计算机上的一个共享映射成本地的 “Z” 盘符，这里的 “d\$” 是系统的隐藏管理共享，“123456” 是 “administrator” 账户对应的密码。这里不一定要管理员访问 “d\$” 共享，任何用户访问任何共享都可以，关键是该用户对共享目录有写入权限即可。

● “Xcopy” 命令把本地 D 盘上 web 文件夹中的内容复制到本地的 “Z:\backup” 文件夹中，其实也就是复制到远程计算机的 “d:\backup” 文件夹中。其中 “/E” 的含义是复制文件夹以及子文件夹中的所有内容，“/Y” 的意思自动覆盖同名文件，因要多次复制，如果没有这个参数，系统就会停下来，询问是否需要覆盖。有关 Xcopy 更多的可选参数，请查看联机帮助。

● “net use z: /delete” 删除本地映射的网络盘符 “Z”，因下次批处理文件执行时会再次映射 “Z” 盘符。

STEP 2 定期自动执行批处理文件。在虚拟机 1，选择 “开始” → “程序” → “附件” → “系统工具” → “任务计划”，打开 “任务计划” 窗口，如图 4-2-56 所示。

双击 “添加任务计划” 图标，打开 “任务计划向导”，单击 “下一步” 按钮，打开如图 4-2-57 所示的对话框，单击 “浏览” 按钮，找到 Step 1 中建立了 “backup.bat” 文件。

接下来，给任务命名。单击 “下一步” 按钮，打开如图 4-2-58 所示的对话框，起始时间填入

“23:00”，运行这个任务选择“每天”，起始日期默认从当天开始。

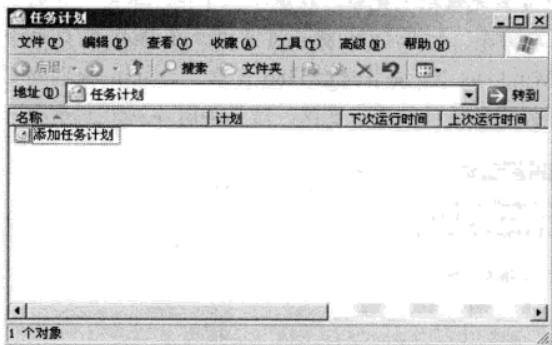


图 4-2-56 任务计划

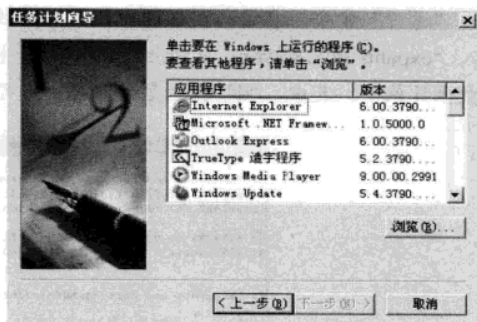


图 4-2-57 任务计划执行程序

单击“下一步”按钮，打开如图 4-2-59 所示的对话框。只有管理员组成员有权执行任务计划，输入虚拟机 1 的本地管理员信息，这样任务会自动运行。单击“下一步”按钮继续，在新对话框中单击“完成”按钮，完成任务计划向导。

经过上述操作设置，虚拟机 1 每天 23 点都会自动把“d:\web”文件夹中的所有内容全部复制到真实机“d:\backup”文件夹中，如果有同名文件则自动覆盖。读者可以调整虚拟机 1 的时钟到当前时间稍后几分钟，稍后可以看到屏幕有一个 DOS 窗口出现，执行文件复制，复制完成后屏幕自动关闭。该备份程序的执行不仅限于在同一个局域网内，备份服务器可以在另一个城市甚至是另一个国家（前提网络设备没有限制共享，可以远程访问到共享目录）。

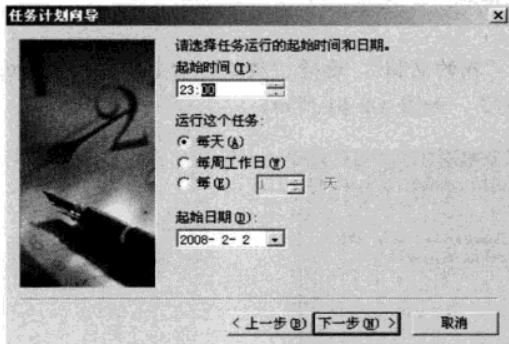


图 4-2-58 任务执行的时间和日期

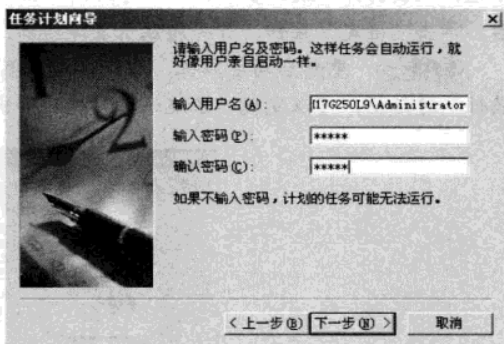


图 4-2-59 输入管理员信息

实验 4-8 Windows Server 2003 的系统还原

使用过 Windows XP 的用户都知道，在 Windows XP 中有一个很方便很实用的功能“系统还原”。该功能在系统运行正常时可以自动地创建多个还原点，当系统出现问题后可以帮助用户非常方便地还原到以前的某一个还原点，快速恢复系统。但在 Windows Server 2003 中，微软并没有集成该功能，这不能不令许多喜爱系统还原功能的用户感到遗憾。下面介绍如何将 Windows XP 中的系统还原功能移植到 Windows Server 2003 中，请先准备好一张 Windows XP

安装光盘, 如果没有安装光盘, 有 Windows XP 的 ISO 文件也可以。按如下步骤操作。

STEP 1 释放 sr.in_文件。将 Windows XP 安装光盘插入光驱, 在虚拟机 1 中, 单击“开始”→“运行”命令, 在运行对话框中输入“cmd”后回车, 打开 DOS 提示符窗口。在 DOS 窗口中输入“expand d:\i386\sr.in_ c:\sr.inf”后回车, 将 Windows XP 安装光盘 i386 目录下的 sr.in_提取到 C 盘根目录下。其中, “d”指光盘的盘符, 也可根据实际情况做适当修改。结果如图 4-2-60 所示。

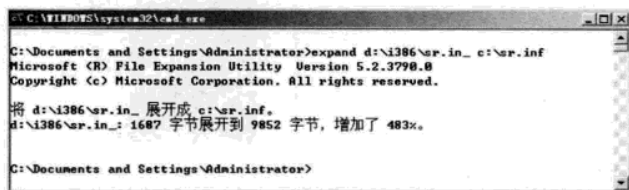


图 4-2-60 释放 sr.in_文件

STEP 2 打开资源管理器, 在 C 盘的根目录下用鼠标右键单击刚刚释放出来的 sr.inf 文件, 在快捷菜单中选择“安装”命令, 开始复制文件。在安装过程中, 安装程序会提示找不到某些文件, 此时可单击提示对话框的“浏览”按钮, 定位到 Windows XP 安装光盘的 i386 目录, 然后单击“确定”按钮即可。

STEP 3 安装完毕后系统会给出“系统设置改变”提示, 并要求重新启动计算机。

STEP 4 重新启动计算机后, 单击“开始”→“运行”命令, 在打开的“运行”对话框中输入“regedit”后回车, 打开注册表编辑器。依次展开 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SvcHost 分支, 在右侧窗口中找到名为“netsvcs”的多字符串值, 双击打开“编辑多字符串”对话框, 在“数值数据”文本框最后添加 SRService, 输入完毕后, 单击“确定”按钮, 并关闭注册表编辑器。

STEP 5 重新启动计算机, 用鼠标右键单击“我的电脑”, 选择“属性”命令, 打开“系统属性”对话框, 可以发现“系统还原”选项卡出现了, 如图 4-2-61 所示。

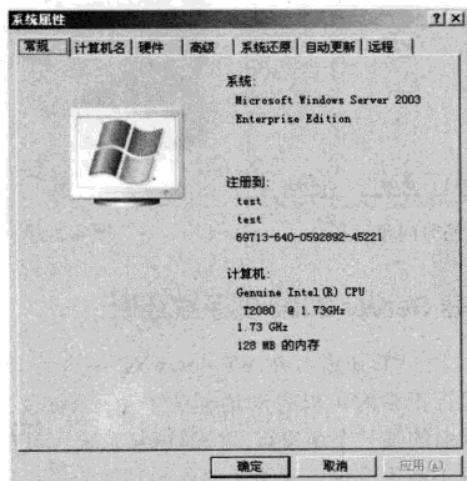


图 4-2-61 Windows Server 2003 的系统还原

4.3 远程管理

Windows Server 2003 中提供了“远程桌面”服务，该服务集成在 Windows Server 2003 中，不需要用户额外支付费用。又因完美的集成、超低的 CPU 使用而优于第三方的远程控制软件。有了远程桌面，用户可以从其他办公室、家中或在旅途中对计算机进行远程控制，复制文件等操作，甚至还可以把远程计算机的声音也带到本地。

4.3.1 配置服务端

默认情况下，Windows Server 2003 提供了“远程桌面”服务，但默认并没有启用。在虚拟机 1 上右键单击“我的电脑”，选择“属性”命令，打开“系统属性”对话框，单击“远程”选项卡，如图 4-3-1 所示。

选中“允许用户远程连接到这台计算机”复选框，这样就开启了远程桌面服务，默认情况下 administrators 组的成员具有远程管理的权限。如需添加其他的用户，单击“选择远程用户”按钮进行添加，添加的用户将属于“Remote Desktop Users”组。

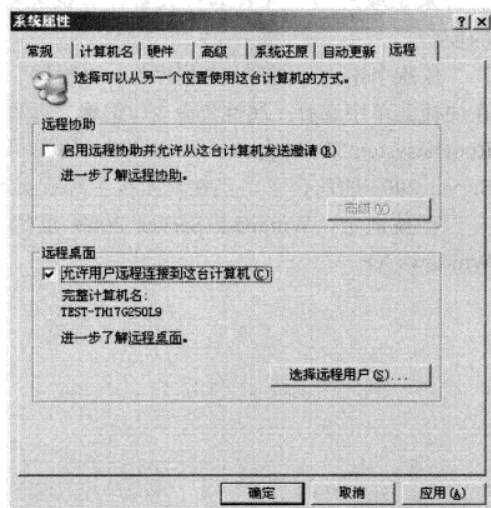


图 4-3-1 启用远程桌面

Windows Server 2003 既可以是“远程桌面”的服务端，也是“远程桌面”的客户端。在客户端上可以控制远程计算机后台和前台，可以共享磁盘或打印机等硬件。

1. 控制后台

在真实机上运行远程桌面客户端，选择“开始”→“程序”→“附件”→“通信”→“远程桌面连接”，可以打开远程桌面的客户端，如图 4-3-2 所示。

填入虚拟机 1 的 IP 地址“192.168.111.2”，单击“连接”按钮，提示输入用户名和密码，输入虚拟机 1 的用户名和密码，连接成功。在真实机上也可以操作虚拟机 1 的 Windows Server 2003 系统了，并且和虚拟机 1 的操作互不影响。因 Windows Server 2003 是一个多用户的操作系统，二者可以同时运行，VMware 中是虚拟机 1 的前台操作，真实机上的远程桌面是虚拟机 1 的后台

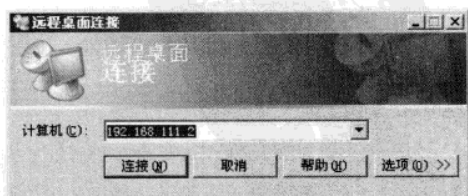


图 4-3-2 远程桌面客户端

操作。需要说明的是,虽然是多用户系统,但有些操作还是会互相影响的,如关机、删除文件等操作。

如果远程连接的是一台 Windows XP 系统,当前正在操纵的前台用户屏幕将自动被锁定。原因在于 Windows XP 是一个单用户的操作系统,同一时刻只允许单一用户操纵计算机,控制台的操作和远程桌面连接的操作相互影响。

2. 控制前台

Windows Server 2003 的远程桌面服务只允许连接两个后台,如果由于非正常退出,或被其他计算机占用了两个后,第三次后台连接将失败。在真实机上两次远程桌面连接虚拟机 1,不要关闭两个窗口,当第三次远程桌面连接登录时,屏幕提示“终端服务器超出了最大允许连接数”,如图 4-3-3 所示。这时就需要连接 Windows Server 2003 的前台,有时为了远程继续前台未完成的操作或者远程查看计算机屏幕的提示信息,都需要连接到 Windows Server 2003 的前台。

依次单击“开始”→“程序”→“附件”→“通信”,用鼠标右键单击“远程桌面连接”命令,在快捷菜单中选择“属性”命令,编辑“远程桌面连接”快捷方式,把目标文件更改为“%SystemRoot%\system32\mstsc.exe /console”,如图 4-3-4 所示。再次连接远程桌面控制的就是 Windows Server 2003 的前台了。当在真实机上远程桌面连接虚拟机 1 的前台时,VMware 中的虚拟机 1 屏幕自动被锁定,Windows Server 2003 虽然支持多用户,但前台只有一个,这时感觉有点类似 Windows XP。

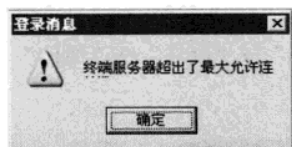


图 4-3-3 远程桌面连接数已满

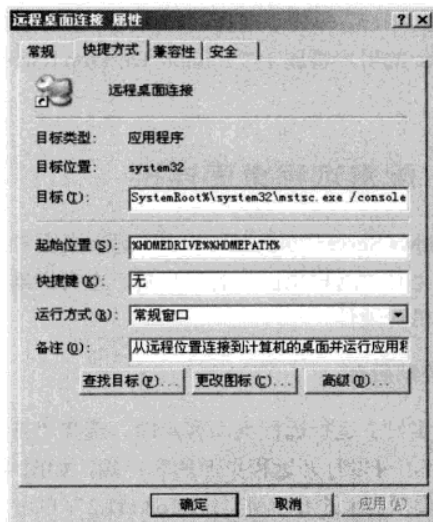


图 4-3-4 修改远程桌面连接为前台

注意



不要尝试在虚拟机 1 中通过远程桌面连接控制真实机的前台,否则将出现黑屏,只有重启计算机才能退出黑屏。原因是因为真实机中能看到虚拟机 1 的界面,而虚拟机 1 又能看到真实机的界面,二者出现了死锁。

3. 共享磁盘

通过远程桌面连接不仅可以远程管理计算机，还可以共享磁盘信息。单击如图 4-3-2 所示中的“选项”按钮，打开如图 4-3-5 所示的窗口。

单击“本地资源”选项卡，选中“磁盘驱动器”，如图 4-3-6 所示。

这样当真实机登录到虚拟机 1 时，就可以看到本地的磁盘驱动器，不同磁盘驱动器之间可以任意复制文件。真实机远程桌面连接虚拟机 1 后，打开虚拟机 1 的资源管理器，可以发现真实机的磁盘也被带到虚拟机 1 中，如图 4-3-7 所示。

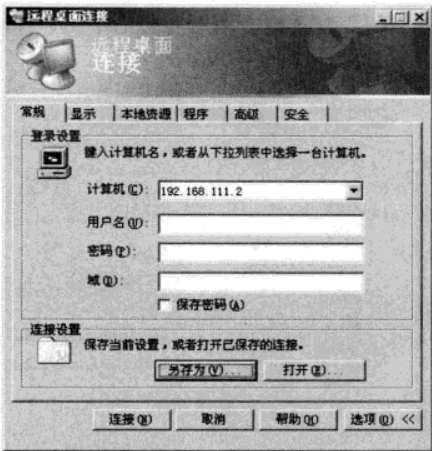


图 4-3-5 远程桌面选项窗口

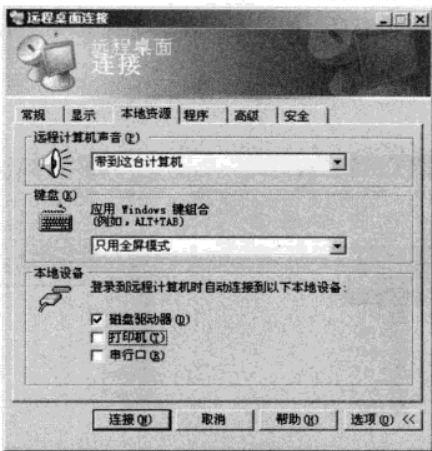


图 4-3-6 共享磁盘



图 4-3-7 带磁盘驱动器的远程桌面连接

从图 4-3-5 中可以看出，远程桌面连接的“选项”功能还有很多，有兴趣的读者不妨尝试。

4.3.3 配置远程桌面

管理员经常要管理多台计算机, 记住所有计算机的 IP 地址、以及用户名和密码是比较烦琐的, 这里可以借助“远程桌面”来实现。依次单击“开始”→“程序”→“管理工具”→“远程桌面”, 打开“远程桌面”窗口, 如图 4-3-8 所示。

右键单击如图 4-3-8 所示的“远程桌面”, 选择“添加新连接”命令, 打开“添加新连接”对话框。如图 4-3-9 所示填写, 首先填写远程计算机的 IP 地址; “连接名”中填入一个直观的名字; “连接到控制台”复选框指的是否要连接到前台; “登录信息”中填入登录时使用的账户和密码, 域是可选信息, 如果不想每次输入密码, 可选中“保存密码”复选框。填写完成后单击“确定”按钮, 保存新连接。

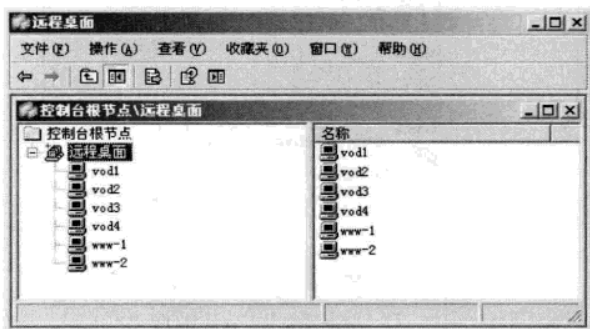


图 4-3-8 远程桌面

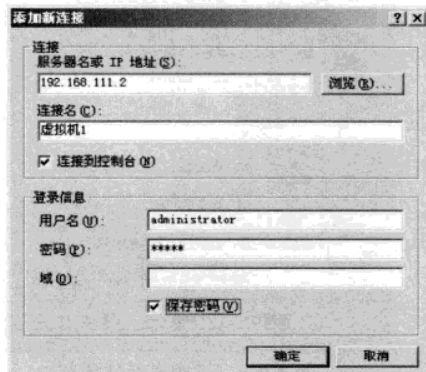


图 4-3-9 添加新连接

如图 4-3-8 所示的左边列表栏中, 出现新建的连接“虚拟机 1”, 选中“虚拟机 1”, 右键单击“虚拟机 1”, 在快捷菜单中单击“连接”, 自动打开到虚拟机 1 的连接, 结果如图 4-3-10 所示。用户可以依次在远程桌面中添加所有经常要使用远程桌面连接的计算机信息。

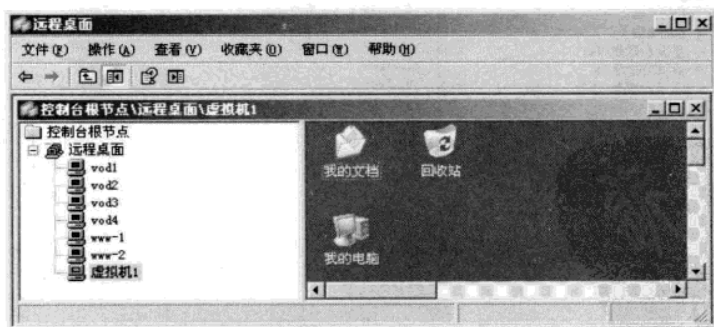
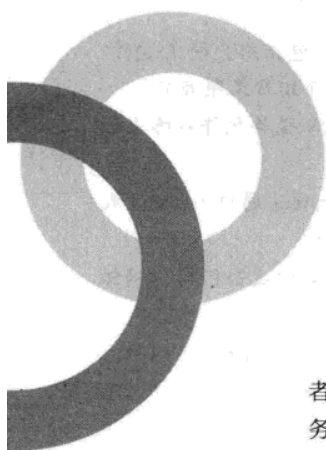


图 4-3-10 远程桌面



第 5 章 配置常用服务器

Chapter 5

本章主要介绍 Windows Server 2003 中常用服务的配置和管理。通过学习本章，读者可以掌握 DHCP、DNS、WWW、E-mail、FTP、路由和远程访问、视频、证书等服务器的配置，能够实现使用 DHCP 进行 IP 地址的动态分配；使用 DNS 提供域名服务；使用 WWW 发布信息；使用 E-mail 提供邮件服务；使用 FTP 提供文件上传下载服务；使用路由和远程访问提供内部用户接入广域网、远程用户访问内部网的服务；使用视频服务提供实况转播和视频会议、电视节目直播的功能；使用证书保护 Web 和邮件的安全等功能。

5.1 微软服务器可以实现的功能

Windows Server 2003 是一个多任务操作系统，它能够根据需要，以集中或分布的方式处理各种服务器角色。主要的服务器角色包括以下几种。

- 文件和打印服务器。文件服务器使用本计算机上的磁盘空间存储、管理和共享诸如文件和网络访问的应用程序的信息；打印服务器提供和管理打印机访问权限。本书的第 4 章对文件和打印服务器已经作过介绍。

- Web 服务器和 Web 应用程序服务器。可将 IIS (Internet Information Services, Internet 信息服务) 与其他可选技术和服务 (如 COM+ 和 ASP.NET) 一起安装部署。IIS 和 Windows Server 2003 家族通过 Intranet、Internet 或 Extranet 一起提供集成的、可靠的、灵活的、安全的且可管理的 Web 服务功能。

- 邮件服务器。向用户提供电子邮件服务，组建公司自己的邮件服务器，Windows Server 2003 家族中包含了 POP3 (Post Office Protocol Version 3, 邮局协议 3) 和 SMTP (Simple Mail Transfer Protocol, 简单邮件传输协议) 组件。

- 终端服务器。即远程桌面服务器，用户可从远程位置运行程序、保存文件并使用网络资源，仿佛这些资源都安装在自己的计算机上一样。本书第 4 章对远程桌面也已经作过介绍。

- 远程访问/代理/虚拟专用网络服务器。为远程计算机提供功能完备的软件路由器以及拨号和 VPN。它为 LAN 和 WAN 环境提供路由服务。另外，它还允许远程和移动人员通过拨号连接

服务或者使用 VPN 通过 Internet 访问公司网络。如果计划将远程人员与公司网络连接, 请将该服务器配置为远程访问和 VPN 服务器。它还可以用来实现代理功能, 通过单一连接实现整个组织的共享上网, 并可实施访问控制。

- 目录服务器。域控制器可存储目录数据, 管理用户和域之间的通信, 包括用户登录过程、身份验证和目录搜索, 方便组织资源的统一管理和高效使用。本书第 6 章将介绍目录服务器。

- 域名系统 (DNS)。在 Internet 上使用的 TCP/IP 名称解析服务, DNS 服务允许网络上的客户端计算机注册和解析用户友好的 DNS 名称。

- 流媒体服务器。提供 Windows Media Services, Windows Media Services 通过 Intranet 或 Internet 对 Windows Media 内容进行管理、交付和存档, 包括流式音频和视频。

- 证书服务器。防止信息被未经授权的获取、篡改或执行各种不同类型的攻击行为, 确保电子邮件、电子商务交易、文件传输等各类信息发送的安全。

- 群集功能。服务器群集是一组协同工作并运行 Microsoft Cluster Service (MSCS) 的独立服务器。服务器群集为资源和应用程序提供了高可用性、故障恢复能力、伸缩性和可管理性。服务器群集允许客户端在出现故障和计划中暂停时, 依然能够访问应用程序和资源。如果群集中的某一台服务器由于故障或维护需要而无法使用, 资源和应用程序将转移到可用的群集节点上。限于篇幅, 本书不介绍该内容, 感兴趣的读者可查阅相关资料, 借助 VMware 软件完成相关实验。

- 网络负载平衡。对于要求同时响应大量用户访问请求的服务器 (如 Web、FTP 服务器等), 仅使用单台服务器很难满足用户对性能的要求。使用网络负载平衡, 可将多个运行相同应用程序或服务的服务器群集到一起, 并共享一个虚拟 IP 地址, 客户机通过虚拟的 IP 地址访问群集中的服务器, 网络负载平衡负责将用户的访问请求均衡的分配给群集中不同的服务器。当某台服务器发生故障时, 网络负载平衡会在其他服务器之间重新分配工作量, 从而为应用程序提供高性能和高可用性。限于篇幅, 本书不谈及该内容, 感兴趣的读者可查阅相关资料, 借助 VMware 软件完成相关实验。

- 软 RAID 功能。提供基于软件的 RAID, 其中 RAID-5 卷中的磁盘上的信息的创建和重新生成将由“磁盘管理”来处理, 数据将跨磁盘阵列中的所有成员进行存储。本书的第 4 章对磁盘管理已经作过介绍。

5.2 DHCP 服务器

动态主机分配协议 (DHCP) 是一个简化主机 IP 地址分配管理的 TCP/IP 标准协议。用户可以利用 DHCP 服务器管理动态的 IP 地址分配及其他相关的环境配置工作 (如 DNS、WINS、Gateway 的设置等)。在使用 TCP/IP 的网络上, 每一台计算机都拥有唯一的计算机名和 IP 地址。当用户将计算机从一个子网移动到另一个子网的时候, 一定要改变该计算机的 IP 地址。如果采用静态 IP 地址的分配方法将增加网络管理员的负担, 而 DHCP 可以让用户将 DHCP 服务器中 IP 地址数据库中的 IP 地址动态地分配给局域网中的客户机, 从而减轻了网络管理员的负担, 避免因手工设置 IP 地址及子网掩码所产生的错误, 同时也避免了把一个 IP 地址分配给多台工作站所造成的地址冲突, 大大缩短了配置或重新配置网络中工作站所花费的时间, 同时通过对 DHCP 服务器的设置可灵活地设置地址租期。

在使用 DHCP 时，整个网络至少有一台服务器上安装了 DHCP 服务，要使用 DHCP 服务的工作站也需要配置成 DHCP 以获得 IP 地址。DHCP 服务器不仅可以为本地网络的 DHCP 客户机服务，也可以为跨网段的 DHCP 客户机服务，如图 5-2-1 所示。

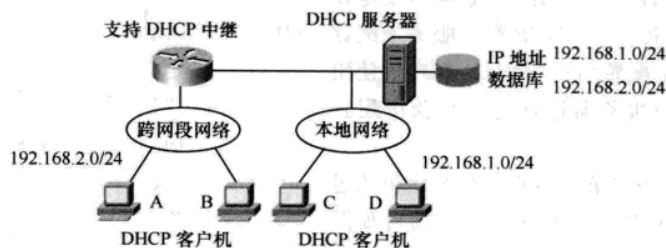


图 5-2-1 DHCP 示意图

5.2.1 DHCP 常用术语

DHCP 的一些常用术语，如表 5-2-1 所示。

表 5-2-1	DHCP 常用术语
术 语	描 述
作用域	作用域是一个网络中的所有可分配的 IP 地址的连续范围。作用域主要用来定义网络中单一的物理子网的 IP 地址范围。作用域是服务器用来管理分配给网络客户 IP 地址的主要手段
超级作用域	超级作用域是一组作用域的集合，它用来实现同一个物理子网中包含多个逻辑 IP 子网。在超级作用域中只包含一个成员作用域或子作用域的列表。然而超级作用域并不用于设置具体的范围，子作用域的各种属性需要单独设置
排除范围	排除范围是不用于分配的 IP 地址序列。它保证在这个序列中的 IP 地址不会被 DHCP 服务器分配给客户机
地址池	在用户定义了 DHCP 范围及排除范围后，剩余的地址组成了一个地址池，地址池中的地址可以动态地分配给网络中的客户机使用
租约期	租约期是 DHCP 服务器指定的时间长度，在这个时间范围内客户机可以使用所获得的 IP 地址。当客户机获得 IP 地址时租约被激活。在租约到期前客户机需要更新 IP 地址的租约，当租约过期或从服务器上删除则租约停止
保留地址	用户可以利用保留地址创建一个永久的地址租约。保留地址保证子网中的指定硬件设备始终使用同一个 IP 地址
选项类型	选项类型是 DHCP 服务器给 DHCP 工作站分配服务租约时分配的其他客户配置参数。经常使用的选项包括默认网关的 IP 地址（Gateway），WINS 服务器及 DNS 服务器。DHCP 管理器允许设置应用于服务器上所有范围的默认选项。大多数选项都是通过 RFC2132 预先设定好的，但用户可以根据需要利用 DHCP 管理器定义及添加自定义选项类型
选项类	选项类是服务器进一步分级管理提供给客户的选项类型的一种手段。当在服务器上添加一个选项类，该选项类的客户可以在配置时使用特殊的选项类型。在 Windows 2000 以上版本中，客户机在与服务器对话时也能够声明类 ID，而对于早期的 DHCP 客户机不支持类 ID。选项类包括两种类型：服务商类和客户类

5.2.2 DHCP 运行方式

如果客户机被设置成从 DHCP 服务器获得 IP 地址, 客户机利用其上的 DHCP 客户服务来配置它的 IP 地址和其他配置信息。DHCP 客户机使用两种不同的方法与服务器进行通信并获得配置信息。

(1) 第一次启动登录网络时的初始化租约过程。当 DHCP 客户机启动登录网络时通过如图 5-2-2 所示的过程从 DHCP 服务器获得租约, 具体过程如下。



图 5-2-2 DHCP 获取 IP 地址过程

STEP 1 DHCP 客户机在本地子网中先发送 DHCP discover (DHCP 租约) 信息, 此信息以广播的形式发送, 因为客户机现在不知道 DHCP 服务器的 IP 地址。

STEP 2 DHCP 服务器收到 DHCP 客户机广播的 DHCP discover 信息后, 它向 DHCP 客户机发送 DHCP offer (DHCP 租约提供) 信息, 其中包括一个可租用的 IP 地址。如果没有 DHCP 服务器对客户机的请求做出反应, 则客户机无法获得 IP 地址, 初始化失败。客户机从微软保留的 B 类网段 169.254.0.0 中挑选一个 IP 地址作为自己的 IP 地址, 子网掩码为 255.255.0.0。DHCP 客户机利用 ARP 广播来确定自己所挑选的 IP 地址是否已被网络上的其他设备使用, 如该 IP 地址已被使用则客户机再挑选另一个 IP 重新进行测试, 最多可以重试 10 个 IP 地址。如客户机挑选的 169.254.0.0 网段中的 IP 地址未被其他设备使用则它将这个地址分配给网卡使用。但客户机将在后台每隔 5 分钟发送 4 次 DHCP discover 信息, 直到它收到 DHCP offer 信息。

STEP 3 一旦客户机收到 DHCP offer 信息, 它发送 DHCP 租约选择信息到服务器表示它将使用服务器所提供的 IP 地址。

STEP 4 DHCP 服务器在收到 DHCP 租约选择信息后, 即发送 DHCP positive (DHCP 确认) 信息, 以确定此租约成立, 且此信息中还包含其他 DHCP 选项信息。

STEP 5 客户机收到确认信息后, 利用其中的信息配置它的 TCP/IP 属性, 并加入到网络中。

STEP 6 当客户机请求的是一个无效的或重复的 IP 地址, 则 DHCP 服务器在第五步发送 DHCP negative (DHCP 拒绝) 信息, 客户机收到 DHCP negative 信息后, 初始化失败。

(2) DHCP 客户机更新租约的过程。客户机重新启动或租期达到 50% 时, 客户机都需要更新租约, 过程如下。

STEP 1 如果在启动时客户机的租约仍然有效, 客户机直接向提供租约的服务器发送请求, 要求更新及延长现有地址的租约。

STEP 2 如果 DHCP 服务器收到请求, 它发送 DHCP 确认信息给客户机, 更新客户机的租约。

STEP 3 如果客户机无法与提供租约的服务器取得联系, 则客户机尝试 Ping 在租约中设置的默认网关。如果成功的 Ping 到默认网关, 则客户机认为它仍然在同一个网络中, 它将继续使用现有的租约。在租期达到 50% 时, 它在后台继续尝试更新租约, 客户机一直等到租期达到 87.5%

时, 客户机进入到一种重新申请的状态, 它向网络上所有的 DHCP 服务器广播 DHCP discover 请求以更新现有的地址租约。如果无法成功的 Ping 到默认网关, 则客户机认为它已被移动到一个没有 DHCP 服务的网络中, 客户机则利用前面所说的自动分配 IP 的功能给自己分配一个 IP 地址。

STEP 4 如有服务器响应客户机的请求, 那么客户机使用该服务器提供的地址信息更新现有的租约。

STEP 5 如果租约过期或无法与其他服务器通信, 客户机将无法使用现有的地址租约。

STEP 6 客户机返回到初始启动状态, 利用前面所述的步骤重新获取 IP 地址租约。

5.2.3 DHCP/BOOTP 中继代理

如果 DHCP 服务器与客户机分别位于不同的网段上, 如图 5-2-1 所示的 DHCP 服务器与“192.168.2.0”网段的 DHCP 客户机, 则用户的路由器必须符合 RFC1542 的规定, 即必须具备 DHCP/BOOTP Relay Agent (DHCP 中继) 的功能。

Relay Agent (中继代理) 是一个把某种类型的信息从一个网段转播到另一个网段的小程序。DHCP Relay Agent 是一个硬件或程序, 它能够把 DHCP/BOOTP 广播信息从一个网段转播到另一个网段上。

以如图 5-2-1 所示的实例来说明中继代理工作方式, 也就是“192.168.2.0”子网中的客户机如何从子网“192.168.1.0”中的 DHCP 服务器上获得 IP 地址租约的过程。

STEP 1 DHCP 客户机 A 在子网 2 上广播 DHCP discover 消息, 广播是将消息以 UDP 数据包的形式通过 67 端口发出的。

STEP 2 当中继代理 (在本例中是一个具有中继代理功能的路由器) 接收到这个消息后, 它检查包含在这个消息报头中的源 IP 地址, 如果 IP 地址为“0.0.0.0”, 则路由器用接收到广播的接口的 IP 地址替换它, 然后将其转发到 DHCP 服务器所在的子网 1 上。

STEP 3 当在子网 1 中的 DHCP 服务器收到这个消息后, 它开始检查消息中的网关 IP 地址是否包含在 DHCP 范围内, 从而决定它是否可以提供 IP 地址租约。

STEP 4 如果 DHCP 服务器含有多个 DHCP 范围, 消息中的网关 IP 地址被用来确定从那个 DHCP 范围中挑选 IP 地址并提供给客户。

STEP 5 DHCP 服务器将它所提供的 IP 地址租约 (DHCP offer) 直接发送给中继代理 (也就是本例中的路由器), 路由器将这个租约利用广播的形式转发给 DHCP 客户机。

5.2.4 DHCP 服务器的安装与配置

DHCP 服务器本身必须采用固定的 IP 地址, 规划 DHCP 服务器是需要考虑以下 3 方面的问题。

(1) 需要建立 DHCP 服务器的数量。通常认为每 10000 个客户需要两台 DHCP 服务器, 一台作为主服务器, 另一台作为备份服务器。但在实际工作中用户要考虑到路由器在网络中的位置, 是否在每个子网中都建立 DHCP 服务器, 以及网段之间的数据传输速率。如果两个网段间是用慢速拨号连接在一起, 那么用户就需要在每个网段设立一个 DHCP 服务器。对于一台 DHCP 服务器没有客户数的限制, 在实际中受用户所使用的 IP 地址所在的地址分类及服务器的配制 (如磁盘的容量、CPU 的处理速度等) 的限制。

(2) 支持其他子网 DHCP 功能。如果需要 DHCP 服务器支持网络中的其他子网, 要确定网段间是否用路由器连接在一起, 路由器是否支持 DHCP/BOOTP Relay Agent, 如果路由器不支持 Relay Agent, 那么可以通过架设一台有 DHCP Relay Agent 功能的服务器来解决。

(3) 规划企业网所须考虑的问题。DHCP 服务器于网络中心位置, 将通过路由器的广播降至最低; 为每个范围的 DHCP 客户机指定相应的选项类型并设置相应的数值; 要充分认识到慢速广域网连接所带来的影响。

安装 DHCP 服务器的步骤如下。

STEP 1 在真实机上依次单击“开始”→“设置”→“控制面板”, 在“控制面板”窗口, 双击“添加/删除程序”图标。

STEP 2 在“添加或删除程序”对话框中, 单击“添加/删除 Windows 组件”, 出现“Windows 组件向导”对话框, 从列表中选择“网络服务”如图 5-2-3 所示。

STEP 3 单击“详细信息”按钮, 从列表中选择“动态主机配置协议 (DHCP)”和“域名服务 (DNS)” (以后章节将介绍 DNS), 如图 5-2-4 所示, 单击“确定”按钮。

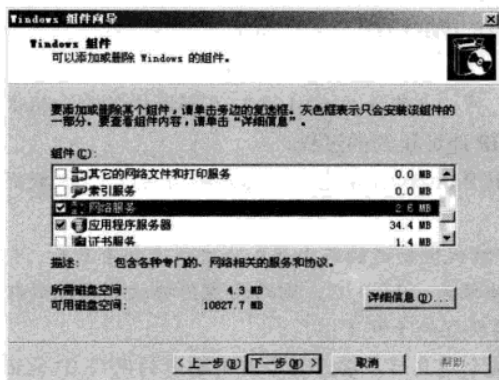


图 5-2-3 编辑网络服务

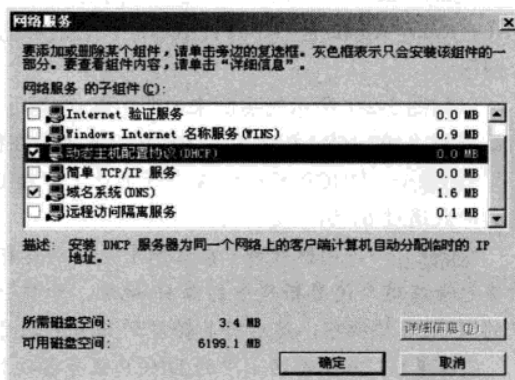


图 5-2-4 添加 DHCP 和 DNS

STEP 4 单击“下一步”按钮, 插入 Windows Server 2003 安装光盘或输入 Windows Server 2003 安装源文件的路径, 单击“确定”按钮, 开始安装 DHCP 服务和 DNS 服务。

STEP 5 最后单击“完成”按钮。安装完毕后在管理工具中新增了“DHCP”和“DNS”功能模块。

在 DHCP 服务器中添加作用域的步骤如下。

STEP 1 在真实机上依次单击“开始”→“程序”→“管理工具”→“DHCP”, 打开 DHCP 控制台, 在计算机名上单击右键, 选择快捷菜单中的“新建作用域”命令, 如图 5-2-5 所示, 打开“新建作用域向导”对话框。

STEP 2 在“新建作用域向导”中单击“下一步”按钮, 询问“作用域名”, 在名称栏中输入一个直观的名称。

STEP 3 单击“下一步”按钮, 输入作用域将分配的地址范围、子网掩码, 如图 5-2-6 所示。这里要注意的是, 如果是在培训环境中, 很多学员一起做实验, 同一个网段中将出现很多个 DHCP 服务器, 每个学员的虚拟机不一定能从真实机上获取到所需的 IP 地址, 此时可

以把 IP 地址的范围改成 192.168.111.0 网段,使用虚拟机 1 作为 DHCP 客户端测试机,虚拟机 1 和真实机的 VMnet1 网卡处在一个独立的网络中,这样即使很多人一起做实验,相互间也互不影响。

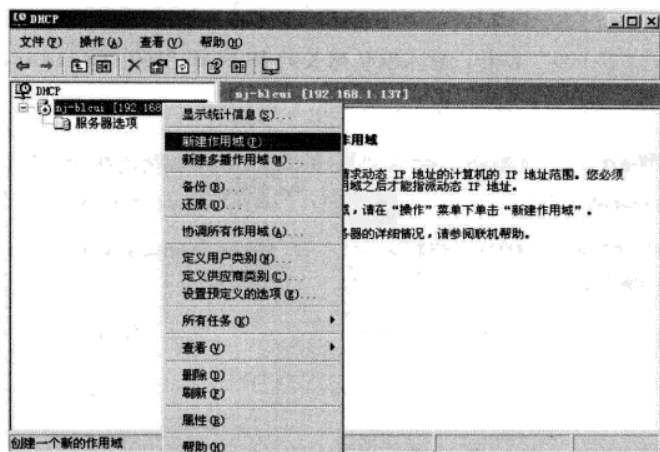


图 5-2-5 新建作用域

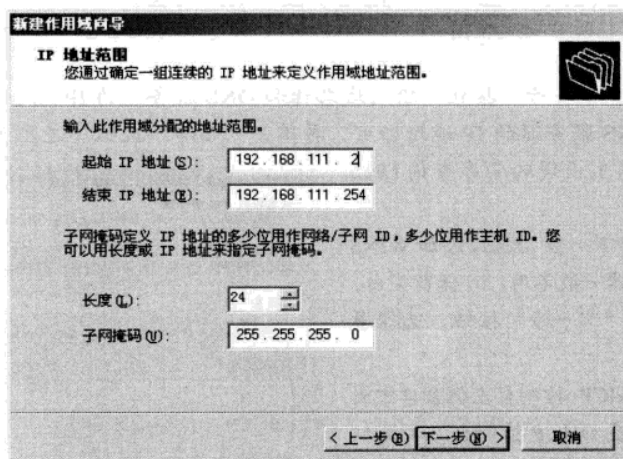


图 5-2-6 IP 地址范围

注意



如果使用虚拟机 1 做实验机,还需在真实机上依次单击“开始”→“程序”→“管理工具”→“服务”,在“服务”窗口中找到“VMware DHCP Service”服务,并停止该服务。因 VMware 中集成了 DHCP 功能,如不停止,虚拟机 1 将从 VMware 的 DHCP 服务中获取 IP 地址,无法验证在真实机上配置的 DHCP 服务。

STEP 4 单击“下一步”按钮，在“添加排除”对话框中，输入需要排除的地址范围，如图 5-2-7 所示，本实验中没有要排除的 IP 地址。

STEP 5 单击“下一步”按钮，询问租约期限，本实验中保持默认的 8 天。

STEP 6 单击“下一步”按钮，询问是否配置 DHCP 选项，选择“是，我想现在配置这些选项”单选框。

STEP 7 单击“下一步”按钮，输入默认网关的 IP 地址“192.168.111.1”，如图 5-2-8 所示，再单击“添加”按钮。

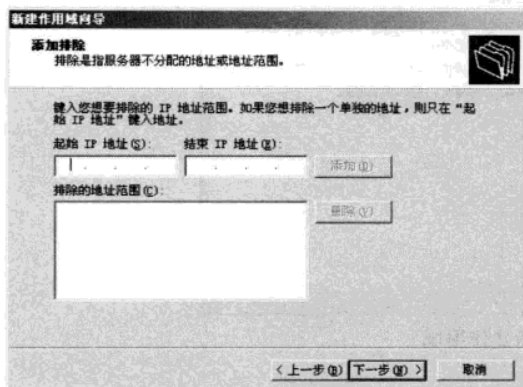


图 5-2-7 排除 IP 地址范围

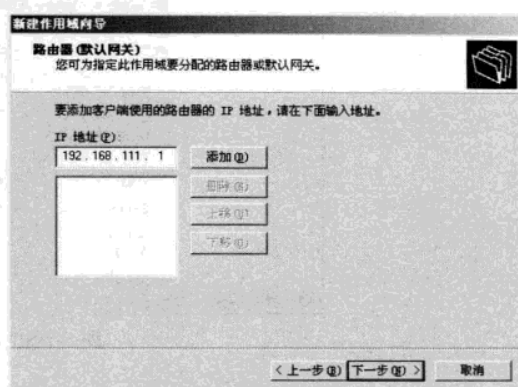


图 5-2-8 添加默认网关

STEP 8 单击“下一步”按钮，输入域名称和 DNS 服务器的 IP 地址，如图 5-2-9 所示。这里只需要填入 DNS 服务器的 IP 地址即可。再单击“添加”按钮，这里可以添加多个 DNS，DHCP 客户机将按这里出现的顺序查询 DNS 服务器。

STEP 9 单击“下一步”按钮，添加 WINS 服务器，WINS 服务器一般不用，可保留空白。

STEP 10 单击“下一步”按钮，选择激活作用域。

STEP 11 在 DHCP 控制台左侧窗口中出现新添加的作用域，在 DHCP 控制台右侧窗口中的状态列中显示为“活动”，表示作用域已启用，如图 5-2-10 所示。

设置完毕，当 DHCP 客户机启动时就可以从 DHCP 服务器获得 IP 地址租约及选项设置。在 DHCP 控制台中作用域下多了 4 项内容。

- 地址池：用于查看、管理现在的有效地址范围和排除范围。
- 地址租约：用于查看、管理当前的地址租用情况。
- 保留：用于添加、删除特定保留的 IP 地址。
- 作用域选项：用于查看、管理当前作用域提供的选项类型及其设置值。

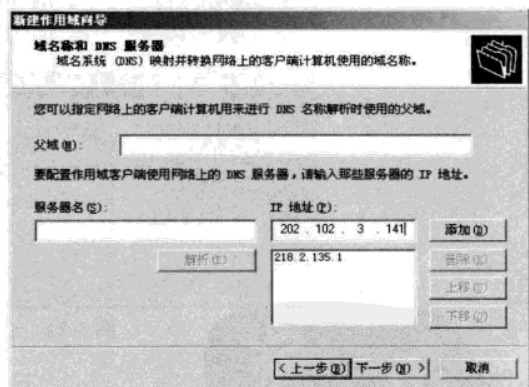


图 5-2-9 填入域名称和 DNS 服务器

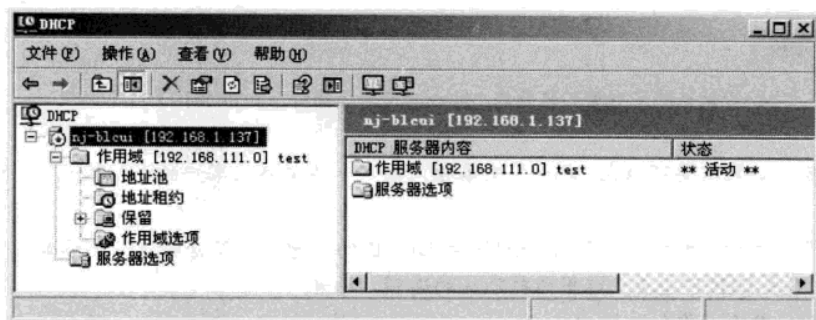


图 5-2-10 激活的作用域

注意



如果为提高容错性而在同一个网段上使用两台 DHCP 服务器，在分配 IP 地址范围时要注意考虑到 DHCP 服务器平衡使用的因素，一般采用 80/20 的规则，即将所有可用的 IP 地址范围按 8:2 的比率分开，一台 DHCP 服务器提供 80% 的 IP 地址租约，另一台提供其他 20% 的 IP 地址租约。假设要在某个网段上提供的 IP 地址范围是 192.168.111.1~192.168.111.254，具体设置方法是把两台服务器作用域分配的地址范围都设置为 192.168.111.1~192.168.111.254，只是在设置排除范围时加以区分，如表 5-2-2 所示。

表 5-2-2

DHCP 服务器的 IP 地址分配

服务器	分配的地址范围	排除的地址范围
服务器 1	192.168.111.1~192.168.111.254	192.168.111.201~192.168.111.254
服务器 2	192.168.111.1~192.168.111.254	192.168.111.1~192.168.111.200

如果想保留特定的 IP 地址给指定的客户机（如 DNS 服务器、IIS 服务器等），以便客户机在每次启动时都获得相同的 IP 地址，设置步骤如下。

STEP 1 在真实机上，选择如图 5-2-10 所示的 DHCP 控制台左侧窗口中的“保留”选项。

STEP 2 右键单击“保留”在快捷菜单中选择“新建保留”，弹出“新建保留”对话框，如图 5-2-11 所示。

STEP 3 在“保留名称”文本框中输入客户名称，如虚拟机 1。注意此名称只是一般的说明文字，并不是用户账号的名称，但此处不能为空白。

STEP 4 在如图 5-2-11 所示的“IP 地址”文本框中输入要保留的 IP 地址，如本例中的 192.168.111.88。

STEP 5 在“MAC 地址”文本框中输入上述 IP 地址要保留给网卡号。每一块网卡都有一个唯一的号码，可以通过命令“ipconfig /all”进行查看。这里添加虚拟机 1 的 MAC 地址。

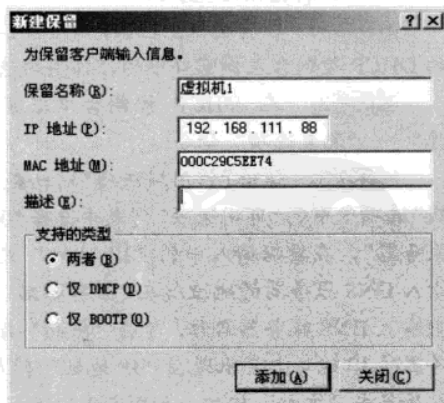


图 5-2-11 保留 IP 地址

注意



MAC 地址的填写格式是数值之间没有任何分隔符, 如图 5-2-11 所示。

STEP 6 如果需要可以在“描述”文本框内输入一些描述此客户的说明性文字, 该描述是可选信息。

STEP 7 选择“允许类型”。BOOTP 是 DHCP 的前身, 仅能分配有限的参数, 并且是永久的分配, 远不及 DHCP 灵活。这里保持默认的选项“两者”。

STEP 8 单击“添加”按钮。

STEP 9 如果需要添加其他保留地址, 重复上述步骤 4~步骤 9。

STEP 10 单击“关闭”按钮结束。

在真实机上添加完成后, 在虚拟机 1 上使用“ipconfig /renew”命令重新获取新的 IP 地址, 虚拟机 1 上提示获取到了新的 IP 地址 192.168.111.88。在真实机上利用单击“作用域”→“地址租约”项进行查看, 可以看到 192.168.111.88 项的“租约截止日期是”提示该项处于“活动”状态。

注意



如果在设置保留地址时, 网络上有多台 DHCP 服务器存在, 用户需要在其他服务器中将此保留地址排除, 以便其他客户机可以获得保留地址。

DHCP 服务器除了可以为 DHCP 客户机提供 IP 地址外, 还可以设置 DHCP 客户机启动时的工作环境, 如可以设置客户机登录的域名称、DNS 服务器、WINS 服务器、默认网关等。在客户机启动或更新租约时, DHCP 服务器可以自动设置客户机启动后的 TCP/IP 环境。

DHCP 服务器提供了许多的选项类型, 但其中只有几项用户非常关心, 如默认网关和 DNS。这些选项在上面添加作用域时用户已经设置过了, 在 DHCP 控制台中的作用域中有一项“作用域选项”中显示了用户所作的设置。为了进一步了解选项设置, 以在作用域中添加 DNS 选项为例, 说明 DHCP 的选项设置步骤。

STEP 1 在真实机上, 选择如图 5-2-10 所示的 DHCP 控制台左侧窗口中的“作用域选项”。

STEP 2 在 DHCP 控制台单击菜单“操作”→“配置选项”命令。

STEP 3 弹出“作用域选项”对话框, 在“常规”选项卡中的“可用选项”列表中选择“006 DNS 服务器”, 在数据输入中的“IP 地址”文本框中输入 DNS 服务器的地址或在“服务器名”文本框中输入 DNS 服务器名称, 单击“解析”按钮, 服务器的 IP 地址也会出现在“IP 地址”列表框中, 然后单击“添加”按钮, 如图 5-2-12 所示。

STEP 4 单击“确定”按钮结束。

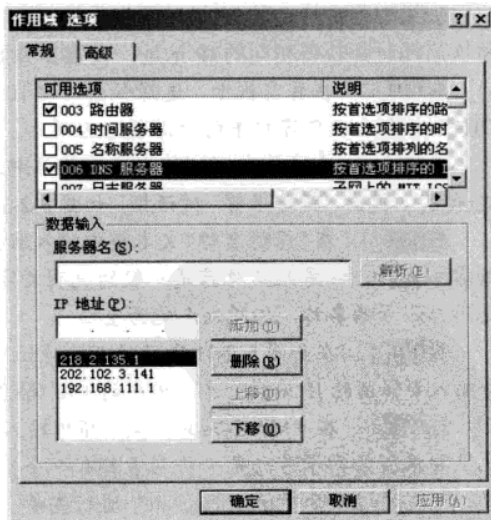


图 5-2-12 更改 DNS 服务器选项

在 Windows Server 2003 的 DHCP 服务器中用户可以针对不同的对象设置选项，上例用户是针对作用域所设置的选项，用户针对的对象包括默认服务器选项、作用域选项、类选项、保留客户选项，下面说明它们之间的关系。

● 服务器选项：这些选项的设置影响 DHCP 控制台窗口下该服务器下所有的作用域中的客户和类选项。

● 作用域选项：这些选项的设置，只影响该作用域下的地址租约。

● 类选项：这些选项的设置，只影响被指定使用该 DHCP 类 ID 的客户机。

● 保留客户选项：这些选项的设置只影响指定的保留客户。

如果在服务器选项与作用域选项中设置了相同的选项，则作用域的选项起作用，即在应用时作用域选项将覆盖服务器选项，同理类选项会覆盖作用域选项，保留客户选项覆盖以上 3 种选项，它们的优先级表示如下，“>”表示优于：

保留客户选项 > 类选项 > 作用域的选项 > 服务器选项

5.2.5 DHCP 客户机的设置

DHCP 服务器安装设置完成后，在客户机上开始启用 DHCP 获取 IP 地址，下面以虚拟机 1 为例，进行演示。

在虚拟机 1 上右键单击“网上邻居”，在快捷菜单中选择“属性”，打开“网络连接”窗口，右键单击“本地连接”，在弹出的快捷菜单中选择“属性”，在打开的“本地连接属性”对话框中双击“常规”选项卡下的“Internet 协议 (TCP/IP)”，打开如图 5-2-13 所示的对话框。选择“自动获取 IP 地址”和“自动获得 DNS 服务器地址”，单击“确定”按钮，完成虚拟机 1 的配置。

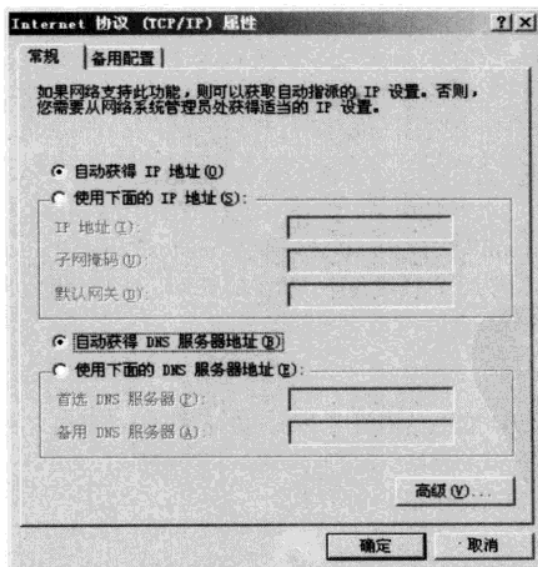


图 5-2-13 DHCP 客户端设置

在虚拟机 1 上执行“ipconfig /all”查看动态获取的 IP 地址,如图 5-2-14 所示;执行“ipconfig/release”释放获取的 IP 地址;执行“ipconfig /renew”重新获取 IP 地址。

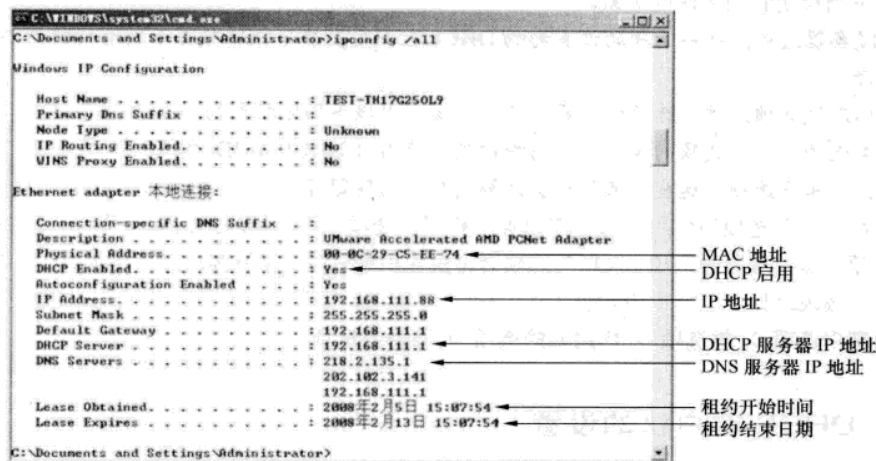


图 5-2-14 查看 DHCP 客户端设置

5.3 DNS 服务器

Windows Server 2003 Server 能够充当网络中的 DNS 服务器, DNS 作为 Windows Server 2003 的一个网络组件提供域名解析服务。本节介绍实现 DNS 服务器的方法和 DNS 服务器的配置。

DNS 服务器通过用户友好名称代替难记的 IP 地址以定位计算机和服务,用户使用域名地址,系统就会自动把域名地址转为 IP 地址。提供域名服务的服务器称之为 DNS 服务器,通过 DNS 服务器来应答域名服务的查询。首先分析一个域名和主机名的例子,如图 5-3-1 所示,在根域下分布了若干顶级域,顶级域下又分布有二级域。这一等级结构构成了 Internet 资源命名机制。例如,在根域下有“.com”

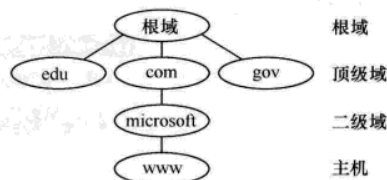


图 5-3-1 域名结构

顶级域,其下又有“microsoft”二级域,该域表示为 microsoft.com。“microsoft”子域中有一台主机名为“www”的计算机。为了定位这台计算机上的资源,需要使用全域名 www.microsoft.com。

5.3.1 域名解析方式

采用等级结构的命名机制虽然给网络用户带来方便,但是随之而来的名称解析问题亦需要解决,即客户机需要以某种方式将网络资源的全域名解析为可供 TCP/IP 网络进行计算机定位的 IP 地址。通常的域名解析方法有分布和集中两种。

1. 分布域名解析

分布域名解析是在客户机上维护一个静态的文本文件(文件名叫“host”),其中包含主机名

称与 IP 地址的映射, 该文件位于 “%systemroot%\system32\drivers\etc\” 目录下。随着网络规模的扩大, 分布式解析已显力不从心, 但仍有一定实际应用价值, 如不想别人使用某台计算机访问新浪网, 可以在这个文件的最后加入一行 “202.119.248.16 www.sina.com.cn”, 以后这台计算机访问新浪网时将转向 202.119.248.16 这台服务器, 该服务器为作者的个人主页, 但对除新浪网外的其他网址访问不受影响。之所以出现上述现象, 原因在于计算机对域名的解析是有顺序的, 先查计算机缓存, 再查 “host” 文件, 最后查 DNS 服务器。用户也可以用这种方法在公司所有计算机的 “host” 文件中添加公司未在公网注册的私有域名, 这样公司计算机就可以使用私有域名访问公司的服务器。

2. 集中式域名解析

集中式域名解析方式需要在网络中提供多台 DNS 服务器, 它们负责维护域名和 IP 地址映射数据库。客户机从指定的服务器获取域名对应的地址信息, 一旦客户机指定的 DNS 服务器中没有包含相应数据, 则由 DNS 服务器在网络中进行递归查询, 从其他服务器上获取地址信息。

DNS 服务器的工作原理如图 5-3-2 所示, 实线箭头代表请求信息流向, 虚线箭头代表应答信息流, 具体流程如下。

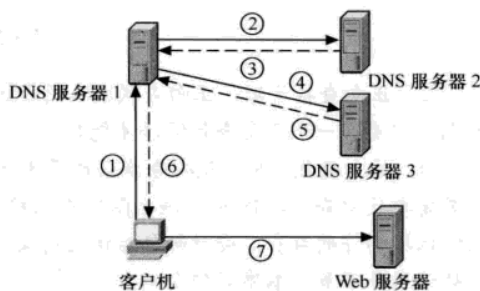


图 5-3-2 DNS 服务器工作原理

STEP 1 客户机将域名查询请求发送到本地 DNS 服务器 (即 DNS 服务器 1), DNS 服务器 1 将在本地数据库中查找客户机要求的映射。

STEP 2 如果 DNS 服务器 1 不能在本地找到客户机查询的信息, 将客户机请求发送到上一级域名 DNS 服务器 (即 DNS 服务器 2)。

STEP 3 DNS 服务器 2 负责解析客户机请求的根域部分, 它将包含下一级域名信息的 DNS 服务器地址 (即 DNS 服务器 3) 返回给客户机的 DNS 服务器 (即 DNS 服务器 1)。

STEP 4 客户机的 DNS 服务器 (即 DNS 服务器 1) 利用根域名服务器解析的地址访问下一级 DNS 服务器 (即 DNS 服务器 3)。

STEP 5 DNS 服务器 3 将解析出的 IP 地址返回给 DNS 服务器 1, 如果 DNS 服务器 3 上没有解析出域名对应的 IP 地址, 它将返回域名对应的 IP 地址再下一级域名的 DNS 服务器地址。按照上述递归方法逐级接近查找目标, 最后在维护有目标域名的 DNS 服务器上找到相应的 IP 地址信息。

STEP 6 客户机的本地 DNS 服务器将递归查询结果返回客户机。

STEP 7 客户机利用从本地 DNS 服务器查询得到的 IP 地址访问目标 Web 服务器。

5.3.2 创建查找区域

本章 5.2.4 小节, 已经介绍了如何在真实机中安装 DNS。依次单击 “开始” → “程序” → “管理工具” → “DNS”, 打开如图 5-3-3 所示的 DNS 管理器窗口。DNS 管理器的 DNS 服务器节点下有 “正向查找区域” 和 “反向查找区域” 两个子节点, 它们是 DNS 服务管理的基础。

本单位。

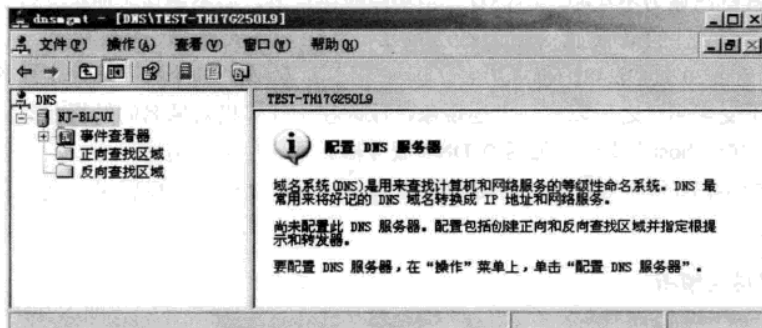


图 5-3-3 DNS 管理器

● 正向查找区域: 正向查找区域用于正向查找, 它将域名解析为 IP 地址。一台 DNS 服务器上至少要有个正向查找区域才能工作。

● 反向查找区域: 反向查找区域用于反向查找, 它将 IP 地址解析为域名。Nslookup 之类的工具需要反向查找, IIS 中的域名限制也依赖于反向查找来实现, 此外国外的一些邮件服务器为了减少垃圾邮件的存在, 会对邮件后缀进行反向解析, 把解析失败的邮件视为垃圾邮件。反向查找区域使用并不多, 本书不作介绍。

下面以创建正向查找区域为例, 介绍区域创建的具体步骤。

STEP 1 在 DNS 管理器中展开 DNS 服务器图标, 右击“正向查找区域”子节点, 在快捷菜单中单击“新建区域”, 打开 DNS “新建区域向导”, 单击“下一步”按钮。

STEP 2 选择区域类型。如图 5-3-4 所示, 指定新建正向查找区域的类型为主要区域、辅助区域或者存根区域。它们之间的区别如下。

● 主要区域: 它是一个新区域的标准主拷贝, 创建区域的计算机负责维护主要区域。

● 辅助区域: 它是一个已存在区域的副本, 辅助区域本身是只读的, 它从主要区域复制数据。辅助区域的用途是产生冗余, 一方面减少了主控服务器的流量负载, 另一方面降低了主要区域关机造成的时间损失。

● 存根区域: 如果希望该 DNS 服务器了解它委派给另一个 DNS 服务器的子区域所添加的所有 DNS 服务器, 则选择存根区域选项。

本书的实验中都选择“主要区域”, 选定区域类型后, 单击“下一步”按钮继续。

STEP 3 指定区域名称。填入区域名称, 如图 5-3-5 所示, 填入“test.com”。注意, 这里填的是域名, 不是 DNS 服务器的名字, 如微软公司的域名是“microsoft.com”, DNS 服务器的名称是“dns.microsoft.com”, 创建 DNS 正向查找区域, 填入的名称应该是“microsoft.com”, 而不是“microsoft”或“dns.microsoft.com”。

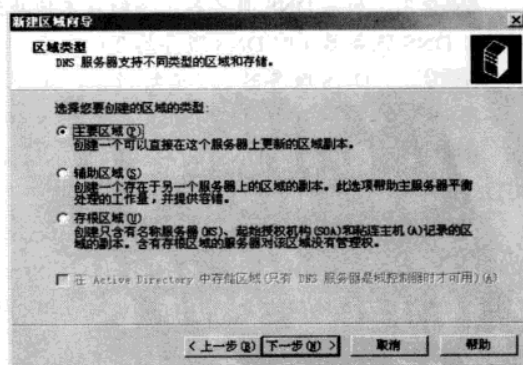


图 5-3-4 创建正向区域

STEP 4 指定区域文件名。根据前面所选区域类型的不同,这一步所配置的信息亦不相同。如果选择创建主要区域,则在此指定区域映射文件名称,或者指定一个现有文件作为区域文件,如图 5-3-6 所示,该文件保存在“%SystemRoot\system32\dns”文件夹下;如果选择创建辅助区域,则在此指定辅助区域所对应的主要区域 DNS 服务器,在“IP 地址”栏中填入主要 DNS 服务器地址,单击“添加”按钮加入列表,DNS 将按照列表中的主控服务器顺序逐一联系它们,单击“上移”或者“下移”,可以更改主控服务器在列表中的顺序。单击“下一步”按钮继续。

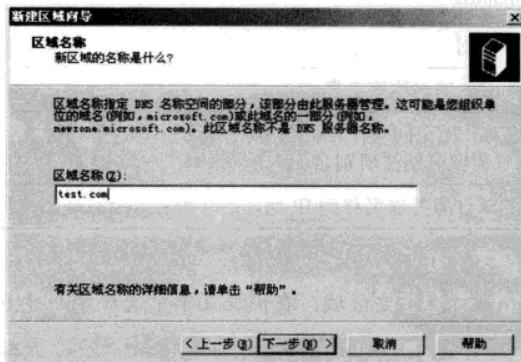


图 5-3-5 区域名称

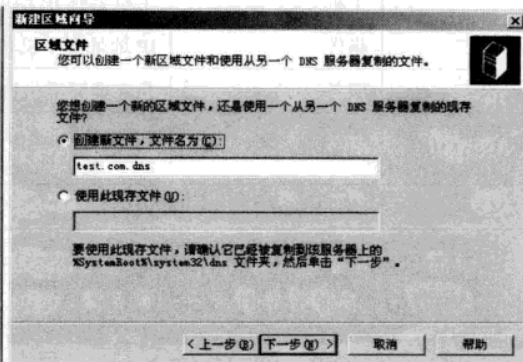


图 5-3-6 区域文件名

STEP 5 接下来的对话框中询问是否允许动态更新,出于安全方面的考虑,这里选择“不允许动态更新”。单击“完成”按钮,完成新建区域向导。添加完“test.com”的 DNS 管理器如图 5-3-7 所示。

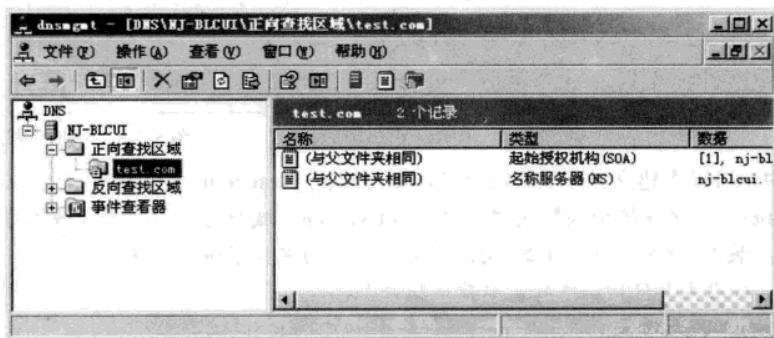


图 5-3-7 test.com 正向区域

5.3.3 添加资源记录

创建区域之后还需要向区域中添加资源记录才能使 DNS 服务器工作。资源记录就是某种类型的资源与地址的映射数据,如 Web 站点域名 www.test.com 映射为站点的 IP 地址 192.168.1.200,这就是一条资源记录。由于在 TCP/IP 网络中的资源种类众多,DNS 服务器的资源记录也有多种,表 5-3-1 列出了最常用的几种资源记录及其对应的网络服务。

表 5-3-1 DNS 资源记录

资源记录	DNS 管理单元名	描述
SOA	起始授权机构	指定当前区域数据的授权信息源服务器，区域数据库中的一个记录必须是 SOA 记录
NS	名称服务器	指定给某特定域的名称服务器
A	主机	主机名到 IP 地址的映射
PTR	指针	IP 地址到主机名的映射
SRV	服务	指定能够提供特别服务的名称服务器
CNAME	别名	同一主机的多个名称，如在同一计算机上实现多个虚拟服务器并共用同一 IP 地址时，就需要分别注册别名
MX	邮件中继	提供 SMTP 服务的邮件服务器名称到 IP 地址的映射

下面以主机资源记录为例，说明添加资源记录的方法。

STEP 1 右键单击图 5-3-7 所示的“test.com”标准主要区域，在快捷菜单中选择“新建主机”命令。

STEP 2 在如图 5-3-8 所示的“新建主机”对话框中，输入主机名称“www”，这里不需要完整域名，在下面提示了完全合格的域名是“www.test.com”。填入“www.test.com”主机对应的 IP 地址“192.168.1.200”，取消“创建相关的指针”复选框，单击“添加主机”按钮。

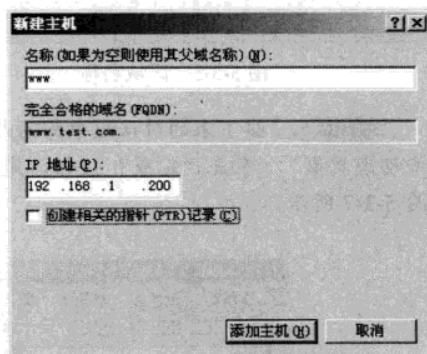


图 5-3-8 添加主机记录

STEP 3 在确认添加成功对话框中单击“确定”按钮。

STEP 4 按上述方法添加任意多个记录后，单击“完成”按钮。

在区域中也可以再建立子区域资源记录，如可以在“test.com”区域中建立“sales”子区域，这样加入“sales”子区域的记录默认属于“sales.test.com”域所有。创建子区域的方法如下。

STEP 1 展开 DNS 管理器中的 DNS 服务器“正向查找区域”节点，右键单击图 5-3-7 所示的“test.com”标准主要区域，选择“新建域”命令。

STEP 2 输入子域名称，如“sales”，单击“确定”按钮。

STEP 3 新的子域可以加入任何资源记录，也可以建立下一级子域。如果在新建的子域下新建一个主机记录“www”，则该主机完整的域名是“www.sales.test.com”。

添加其他记录的方法与此类似。需要添加菜单中没有的特殊资源记录时，右键单击区域并选择“其他新记录”命令，在列表中选择记录类型，单击“创建记录”，在新建资源记录对话框中详细指定新记录内容，单击“确定”按钮完成。

实验 5-1 备份和还原 DNS 服务

企业如果已有一台 DNS 服务器，最好再能配置一台备份 DNS 服务器，以备主 DNS 服务器故

障时替代进行工作。但一般中小企业都是只有一台 DNS 服务器,里面又保存了很多记录,一旦服务器瘫痪,重装系统后,所有的 A 记录、NS 记录、MX 记录都会丢失。微软的所有操作系统版本中都没有提供 DNS 的备份和还原操作,那如何能把 DNS 的数据库进行备份和还原呢?下面介绍 DNS (非活动目录上的 DNS 服务器)数据库的备份和还原操作,具体步骤如下。

STEP 1 依次单击“开始”→“程序”→“管理工具”→“DNS”,打开服务器的 DNS 管理界面,如图 5-3-9 所示,停止 DNS 服务,主要是为了把一些缓存中的记录也保存到文件中。

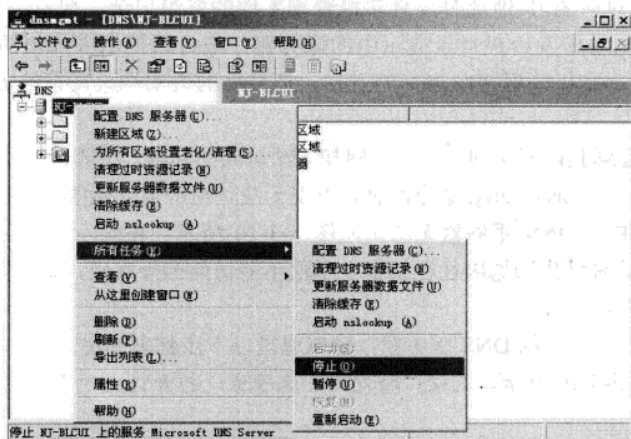


图 5-3-9 停止 DNS 服务器

STEP 2 打开服务器的资源管理器,浏览“%systemroot%\system32\dns”文件夹,可以发现有一个以“*.dns”的文件,*.是 DNS 主要区域的域名,备份此文件到其他计算机上。

STEP 3 如果此 DNS 服务器的记录发生变化想改回到以前的配置,只要把备份的“*.dns”文件覆盖现有的同名文件即可。

STEP 4 如果此 DNS 服务瘫痪,重新安装操作系统,添加 DNS 服务,然后把备份的“*.dns”文件覆盖同名文件即可。

实验 5-2 企业私有 DNS

很多企业并没有注册合法的 DNS 服务器,员工需要通过直接输入 IP 地址来访问企业内部的服务器。这样操作很不方便:一是 IP 地址较难记忆;二是服务器的 IP 地址一旦变更,要通知到每一位员工。为了方便使用,企业不用注册合法的域名,一样可以建立自己内部的 DNS 服务器。下面以 test 公司为例,公司 DNS 服务器的 IP 地址为“192.168.1.200”,随意为公司选个域名,如 test.com (但不能是因特网上已有的域名,如 microsoft.com, sina.com.cn 等)。配置步骤如下。

STEP 1 配置 DNS 服务器。把真实机当做企业的 DNS 服务器,配置方法参见 5.3.2 小节和 5.3.3 小节。

STEP 2 配置 DNS 客户机。在虚拟机 2 上,修改 TCP/IP 属性,把 DNS 更改为“192.168.1.200”。

STEP 3 测试。在虚拟机 2 上执行命令“ping www.test.com”,可以发现解析的 IP 地址是“192.168.1.200”,而“ping www.njut.edu.cn”解析出的 IP 地址为“202.119.248.65”,内外网访问均正常。依此方法,把整个企业内部计算机的 DNS 都指向“192.168.1.200”,这样就可以实现企

业员工通过域名访问内部的服务器,同时访问外网也不受影响。

在虚拟 2 上能解析出 `www.test.com` 的同时为何能解析出 `www.njut.edu.cn` 呢?如图 5-3-9 所示,右键单击计算机名,选择“属性”命令,打开计算机的 DNS 属性对话框,选择“根提示”选项卡,如图 5-3-10 所示。当虚拟机 2 查询 DNS 服务器 192.168.1.200 (也就是真实机) `www.test.com` 对应的 IP 地址时,真实机查询本地的资源记录,找到域名 `www.test.com` 对应的 IP 地址是 192.168.1.200,真实机返回这个记录给虚拟机 2, DNS 解析成功。当虚拟机 2 查询真实机 `www.njut.edu.cn` 对应的 IP 地址时,真实机查询本地的资源记录,找不到域名所对应的 IP 地址,真实机把查询请求转发给根目录提示中的服务器,根目录提示中列出的均是世界上权威的 DNS 服务器地址,真实机采用递归查询的方式,把最终的查询结果反馈给虚拟机 2,实现解析成功。

某些用户可能会遇到内网访问正常,外网却无法访问的问题。经测试,发现通过 IP 地址可以访问,域名却无法访问,通过 ping 命令测试,发现无法正常解析外网的域名。造成这种现象最大的可能是企业内网中的 DNS 服务器无法访问图 5-3-10 所示“根提示”选项卡中所列出的权威 DNS 服务器,造成这种结果的原因往往是很多单位不能访问国外站点,如很多教育网用户默认都不可以访问国外站点。

对于不能访问国外站点的 DNS 服务器,可以通过以下步骤来解决。

STEP 1 如图 5-3-10 所示,选择“转发器”选项卡,打开该选项卡如图 5-3-11 所示。

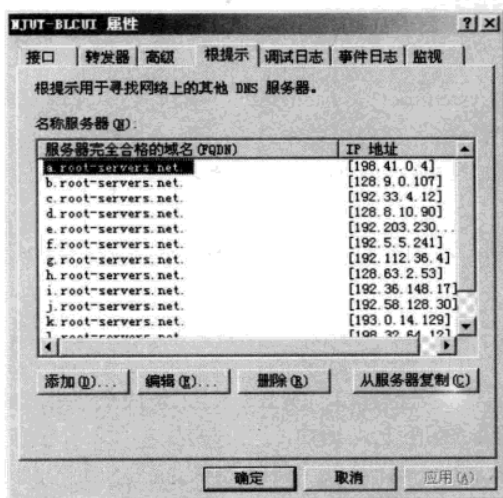


图 5-3-10 DNS 服务器根提示

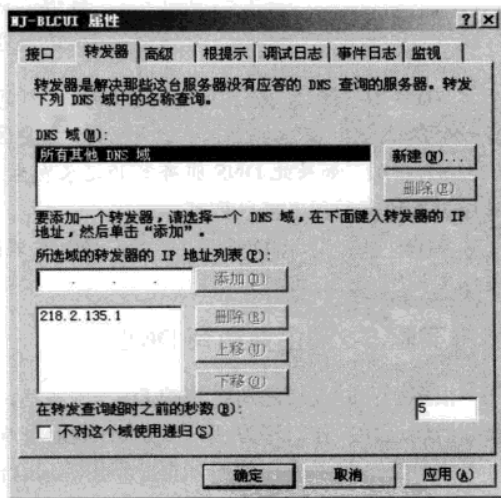


图 5-3-11 添加 DNS 转发器

STEP 2 填入 ISP 提供的 DNS 服务器地址,如 218.2.135.1,单击“添加”按钮,这里可以加入多个国内的 DNS 服务器地址。

这样真实机对不能解析的域名就优先转发给转发器中列举的 DNS 服务器。

实验 5-3 巧用 DNS 实现上网管理

因工作需要,企业需要屏蔽某些网站,借助企业内部的 DNS 服务器,可以很容易实现。

例如,想阻止企业员工访问*.163.com。在实验 5-2 的基础上,在真实机上新增一个正向查找区域“163.com”,不添加任何主机记录。在虚拟机 2 上执行命令“ping www.163.com”,发现解析失败。因为 DNS 服务器本身有正向区域 163.com,即使它解析不出 www.163.com,也不会转发 DNS 查询到其他 DNS 服务器上。这也是企业内部没有注册的 DNS 不能随便新建正向区域的原因。例如,如果新建了正向查找区域“edu.cn”,将导致不能解析中国的所有教育网网址。

把虚拟机 2 的 DNS 改成外网中的其他合法 DNS,发现解析 www.163.com 成功。也就是说通过在 DNS 管理器中新建一个正向区域仅仅能阻止内部使用该 DNS 服务器的用户对外进行域名解析,对不使用该 DNS 的用户则不起作用。为了阻止用户配置外网的 DNS,可以在企业出口设备上做限制,不允许内网访问外界 UDP 的 53 号端口(DNS 服务端口)。

依次添加多个正向区域,可以限制企业内部用户对这些外部网站的访问。但此方法无法限制用户通过 IP 地址对外网的访问,彻底封锁用户对外部某些网站的访问需在网关型设备上做限制设置。

实验 5-4 DNS 委派

可如果部门很大,如中国教育网“edu.cn”,管理中国众多高校,虽然可以通过 5.3.3 小节中新建子域的方法在“edu.cn”这台 DNS 服务器上为每一所高校新建一个子域,如为南京工业大学创建“njut”子域,再在“njut”子域中为南京工业大学的每台服务器创建主机名,如“www”,也就是“www.njut.edu.cn”指向 IP 地址 202.119.248.65,“online.njut.edu.cn”指向 IP 地址 202.119.248.87 等。在同一台服务器上维护全国所有大学的域名和主机名,服务器管理工作烦琐,且给各个高校主机名的管理增加很大的麻烦,因为每个高校主机名的开通、更新、删除都需要上报到中国教育网管理中心。解决的办法就是使用委派技术,把各个子域的管理委派给各个高校。

上面描述的问题可以抽象成如图 5-3-12 所示的拓扑,真实机相当于 DNS 服务器“test.com”,虚拟机 2 相当于 DNS 服务器“sales.test.com”,真实机把“sales.test.com”域的管理委派给虚拟机 2,使用虚拟机 1 进行测试。该实验难度较大,分别配置真实机和虚拟机 2 两台 DNS 服务器,然后在虚拟机 1 上完成测试。

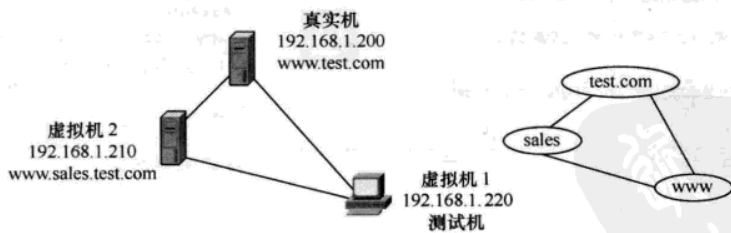


图 5-3-12 DNS 委派拓扑

真实机配置步骤如下。

- STEP 1** 新建正向区域 test.com。如果前面已经完成该步骤,直接跳到下一步骤。
- STEP 2** 在 test.com 中新建主机 www 指向 IP 地址 192.168.1.200。如果前面已经完成该步骤,

直接跳到下一步骤。

STEP 3 在 test.com 中新建主机 pc2 指向 IP 地址 192.168.1.210。

STEP 4 在 test.com 中新建委派，委派 sales.test.com 给虚拟机 2 管理。右键单击图 5-3-7 所示的“test.com”标准主要区域，选择“新建委派”命令，如图 5-3-13 所示。

STEP 5 在“新建委派向导”对话框中，单击“下一步”按钮，输入受委派的域名，如图 5-3-14 所示，输入“sales”。

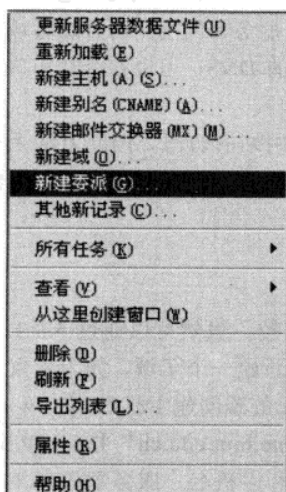


图 5-3-13 新建委派

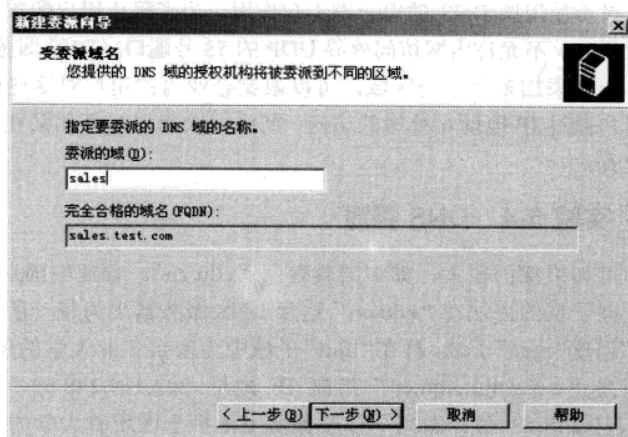


图 5-3-14 受委派域名

STEP 6 单击“下一步”按钮，要求输入名称服务器，如图 5-3-15 所示。

STEP 7 单击“添加”按钮，打开“新建资源记录”对话框。如图 5-3-16 所示，添加要将 sales.test.com 委派给管理计算机的 IP 地址；也可单击“浏览”按钮，在 test.com 域中找到 pc2.test.com 域名；或者直接输入 pc2.test.com，单击“解析”按钮。添加完后，单击“确定”按钮返回。

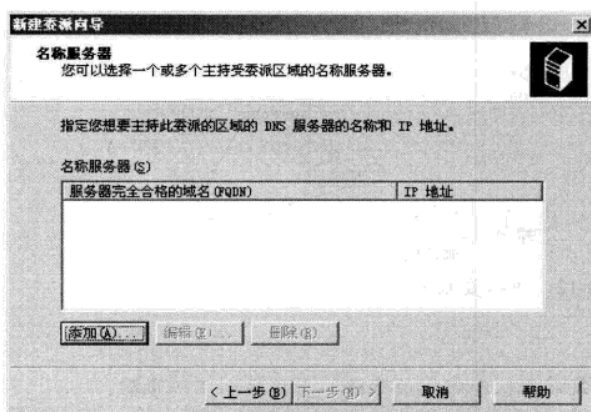


图 5-3-15 添加委派服务器

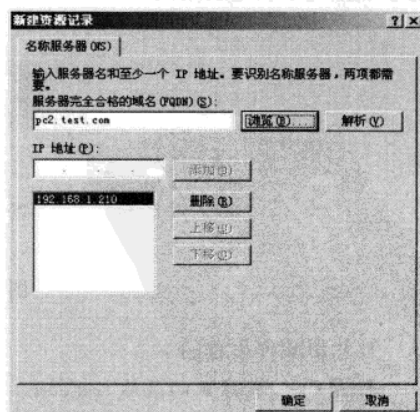


图 5-3-16 添加名称服务器

STEP 8 单击“下一步”按钮继续，完成子域的委派。

虚拟机2的配置步骤如下。

STEP 1 新建正向区域 sales.test.com。

STEP 2 在 sales.test.com 中新建主机 www 指向 IP 地址 192.168.1.210。

STEP 3 配置转发器。利用实验 5-2 中的方法，添加查询转发到 192.168.1.200（即真实机上的 DNS 服务地址）。这一步很关键，如果不添加该转发，配置成使用虚拟机2的 DNS 服务的客户机将无法正确解析出 www.test.com，原因是如果虚拟机2解析失败，虚拟机2 将把查询转发到根提示，根提示无法找到本实验中真实机这台 DNS 服务器。

虚拟机1的测试步骤如下。

STEP 1 更改虚拟机1的网卡类型为“Bridged”，IP地址为 192.168.1.220，网关为 192.168.1.1，DNS 配置成 192.168.1.200。

STEP 2 在虚拟机1执行命令“ping www.test.com”，可以成功的解析出 IP 地址为 192.168.1.200；执行“ping www.sales.test.com”可以成功的解析出 IP 地址为 192.168.1.210；“ping www.njut.edu.cn”可以成功的解析出 IP 地址为 202.119.248.65。

STEP 3 故障排除。如果配置错误已经修改，解析仍然会失败，那么需要在客户机上使用命令“ipconfig /flushdns”清除客户机上的 DNS 缓存记录；同时也要清除 DNS 服务器上的缓存记录，方法是如图 5-3-9 所示，选择“清除缓存”命令。

STEP 4 把虚拟机1的 DNS 修改成 192.168.1.210，使用命令“ipconfig /flushdns”清除虚拟机上的 DNS 缓存记录，执行步骤2中的所有测试，也能够成功解析出所有域名，则表示配置成功。

STEP 5 把真实机的 DNS 修改成自己的 IP 地址 192.168.1.200，把虚拟机2的 DNS 修改成自己的 IP 地址 192.168.1.210。修改完后，在真实机和虚拟机2上也可以进行测试。这一步不是必须，但为了降低后面实验的故障排除复杂程度，建议现在就更改所有计算机的 DNS 为 192.168.1.200 或 192.168.1.210。

5.4 WWW 服务器

互联网为企业带来新的发展契机，建立企业网站可以很好的宣传自身形象，发布实时信息，更有很多企业运用网络进行营销。Windows Server 2003 集成的 IIS（Internet Information Services，Internet 信息服务）中包括了 Web 服务。本节主要介绍 Web 服务器的基本配置，虚拟主机的实现，多 Web 站点服务器的安全设置。

5.4.1 IIS 的安装

配置 Web 服务器的第一步是安装 IIS。默认情况下，IIS 并没有与 Windows Server 2003 操作系统一起被安装，使用该项功能前需要安装 IIS 服务。为了顺利完成后面章节的实验，在真实机和虚拟机2中执行相同的操作，按以下步骤添加。

STEP 1 依次单击“开始”→“设置”→“控制面板”，然后双击“添加或删除程序”图标。

STEP 2 单击“添加/删除 Windows 组件”，显示“Windows 组件向导”对话框。

STEP 3 在 Windows 组件向导的列表中，单击“应用程序服务器”。

STEP 4 单击详细信息，如图 5-4-1 所示，根据网站需要，来决定是否安装 ASP.NET 支持，并选中“Internet 信息服务 (IIS)”复选框。

STEP 5 单击“详细信息”按钮，以查看 IIS 可选组件列表，如图 5-4-2 所示。

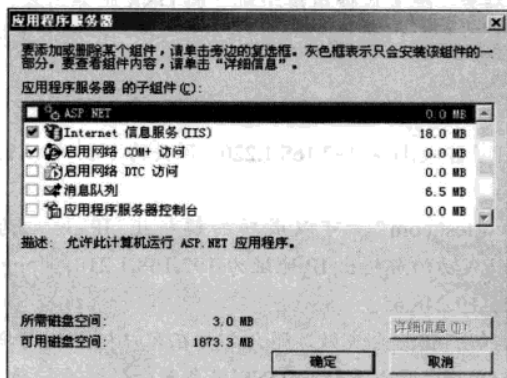


图 5-4-1 添加 IIS 组件

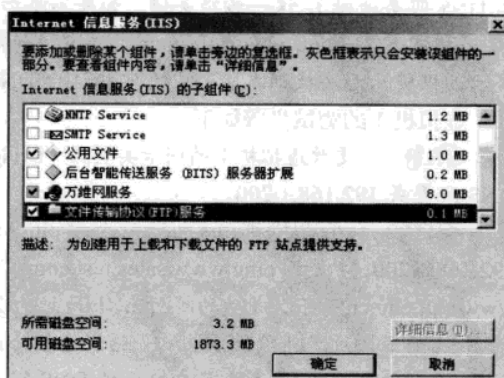


图 5-4-2 添加 FTP 服务

STEP 6 选择需要安装的可选组件。默认情况下“万维网服务”是选中的，再选中“文件传输协议 (FTP) 服务”。

STEP 7 单击“万维网服务”，然后单击“详细信息”按钮，“万维网服务”和“Active Server Pages”组件默认也是选中的。

STEP 8 单击“确定”按钮，直到返回“Windows 组件向导”对话框。

STEP 9 单击“下一步”按钮，根据提示，提供安装文件，完成“Windows 组件向导”。

STEP 10 在虚拟机 1 的 IE 地址栏中输入“http://www.sales.test.com”，显示如图 5-4-3 所示的界面，则表示虚拟机 2 的 IIS 添加成功。同理虚拟机 1 如能正常浏览“http://www.test.com”，则表示真实机的 IIS 安装成功。

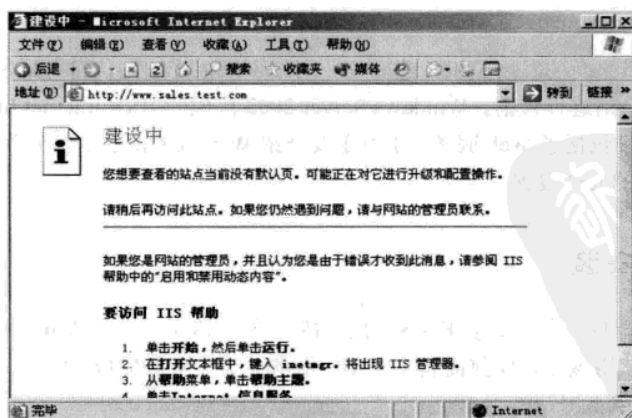


图 5-4-3 IIS 测试页面

5.4.2 Web 站点基本配置

本小节结合留言板代码实例讲解 Web 站点的基本配置。首先解压随书光盘 network.rar 文件中的 guest 文件夹到虚拟机 2 的 C 盘根目录下。在虚拟机 2 上进行如下操作。

STEP 1 在虚拟机 2 上,依次单击“开始”→“管理工具”→“Internet 信息服务 (IIS)”,打开“Internet 信息服务 (IIS) 管理器”窗口。

STEP 2 展开“网站”,如图 5-4-4 所示,右键单击“默认网站”,然后在快捷菜单中选择“属性”命令。

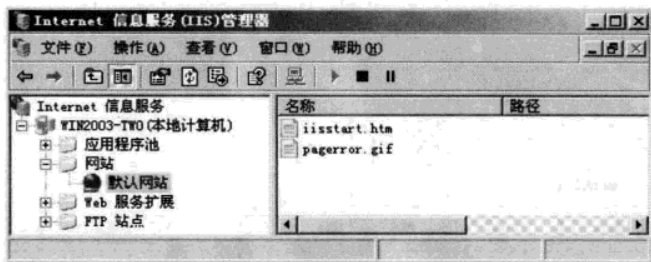


图 5-4-4 IIS 管理器窗口

STEP 3 设置“网站”选项卡。单击“网站”选项卡,如图 5-4-5 所示。

“描述”中填入网站的描述信息,如果一台服务器运行了多个网站,描述可以很容易的区别每个站点的用途;如果为计算机分配了多个 IP 地址(一台服务器上运行多个 Web 站点,有一种办法就是给此服务器配置多个 IP 地址),在“IP 地址”下拉框中选择要指定给此 Web 站点的 IP 地址,如果此站点对应了服务器中所有的未分配的 IP 地址,则选中“全部未分配”,这样访问该计算机中没有被其他计算机使用的 IP 地址,都可以访问到该站点;“TCP 端口”是该 Web 站点使用的 TCP 端口,默认是“80”,如果这里设置的是其他值,如“8080”,虚拟机 1 访问该站点时,需在网址后面添加端口号,如“http://www.sales.test.com:8080”;“SSL (Secure Socket Layer, 安全套接层) 端口”的端口号默认是 443,访问 SSL 网站需要使用“https://”的格式;“连接”选项可以根据网站的特征,对性能实行微调,这里保持默认;“启用日志记录”中单击“属性”按钮,打开“日志记录属性”对话框,如图 5-4-6 所示,可以对日志进行设置,如日志文件产生的周期,日志文件保存的位置。本实验中全部保持默认值。

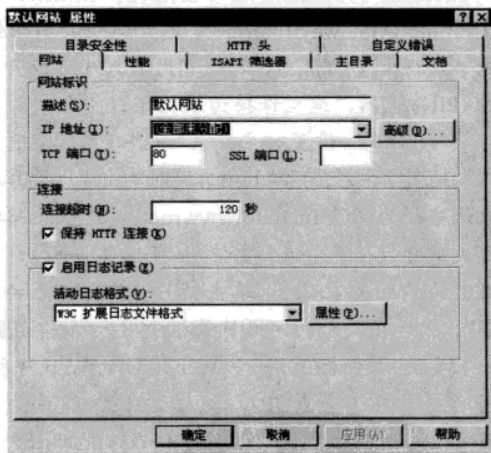


图 5-4-5 “网站”选项卡

STEP 4 设置“性能”选项卡。单击图 5-4-5 所示的“性能”选项卡,如图 5-4-7 所示。可设置该站点使用的网络带宽和允许的网站连接数。通过配置某个特定站点上的网络带宽,可以更

好地控制该站点的通信量。例如,通过在低优先级的 Web 站点上限制带宽,可以给其他站点提供更多的带宽。同样,当指定某个 Web 站点的连接数量时,就可以为其他站点释放资源。本书不涉及性能调整,这里保持为默认值。

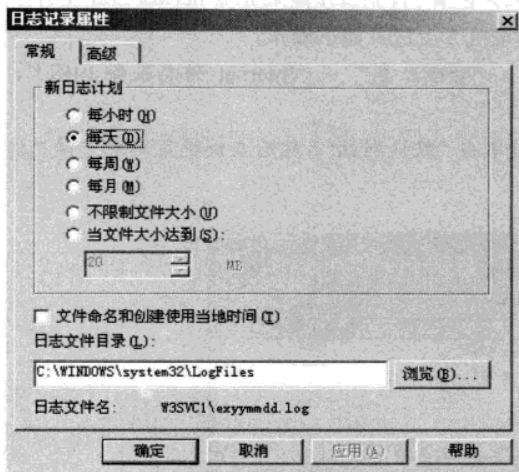


图 5-4-6 日志记录属性对话框

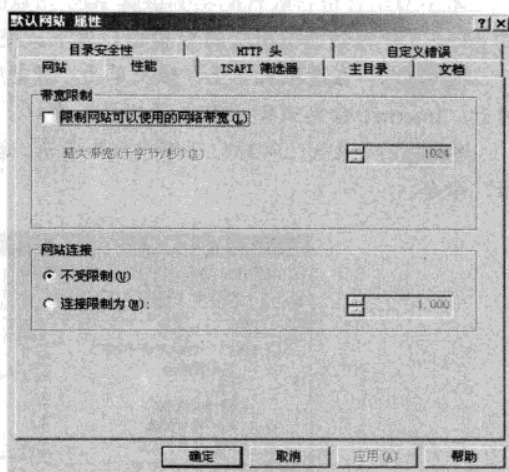


图 5-4-7 性能选项卡

STEP 5 设置“ISAPI 筛选器”选项卡。单击“ISAPI 筛选器”选项卡,ISAPI (Internet Server Application Programming Interface, Internet 服务器应用程序接口)作为一种可用来替代 CGI (Common Gateway Interface, 通用网关接口)的方法,ISAPI 与 Web 服务器结合紧密,功能强大,能够获得大量的信息,因此利用 ISAPI 可以开发出灵活高效的 Web 服务器增强程序。本书不涉及 ISAPI 筛选器,这里保持为默认值。

STEP 6 设置“主目录”选项卡。单击“主目录”选项卡,如图 5-4-8 所示,如果使用存储在本地计算机上的 Web 内容,则单击“此计算机上的目录”单选框然后在本地路径框中键入路径。默认路径为“C:\inetpub\wwwroot”,这里把路径改成“c:\guest”。如果要使用存储在另一台计算机上的 Web 内容,则单击“另一计算机上的共享”,然后在显示的网络目录框中键入所需位置。如果要使用存储在另一个 Web 地址的 Web 内容,则单击“重定向到 URL”,然后在“重定向到”框中键入所需位置。这里除了修改本地路径外,其他选项保持不变。

STEP 7 设置“文档”选项卡。单击“文档”选项卡,如图 5-4-9 所示,列表中显示的是“启动默认内容文档”的列表。如果要使用的文档没有出现在列表中,就必须添加它,这里需要添加“gb_view.asp”。单击“添加”按钮,在添加默认文档对话框中,键入“gb_view.asp”,然后单击“确定”

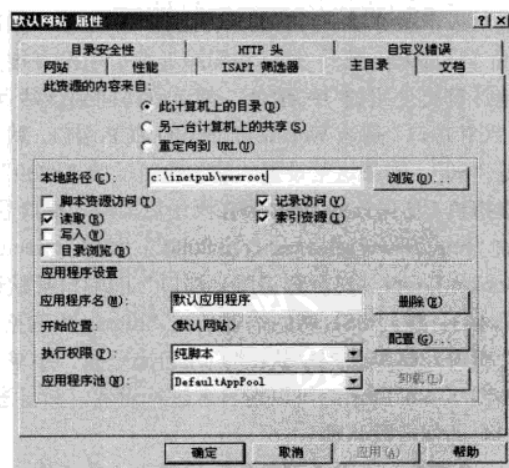


图 5-4-8 主目录选项卡

按钮。客户机浏览该 Web 站点时,将会从上至下查找文档中列出的文件,如找到则打开该文件,并且不再继续向下查找。为了节省时间,这里可以单击向上箭头按钮,把“gb_view.asp”显示在列表的顶部。

STEP 8 设置“目录安全性”选项卡。单击“目录安全性”选项卡,如图 5-4-10 所示。在“身份验证和访问控制”下,单击“编辑”按钮,可以看到默认情况下启用匿名访问,也就是使用 IUSR_COMPUTERNAME 访问网站;在“IP 地址和域名限制”下,单击“编辑”按钮,可以设置配置拒绝访问 IP 地址范围;“安全通信”的内容将在本章最后的证书应用中介绍。本实验中,这里保持默认值。

STEP 9 设置“HTTP 头”选项卡。单击“HTTP 头”选项卡,可以启用内容过期和编辑网页分级等,本书不涉及 HTTP 头,这里保持为默认值。

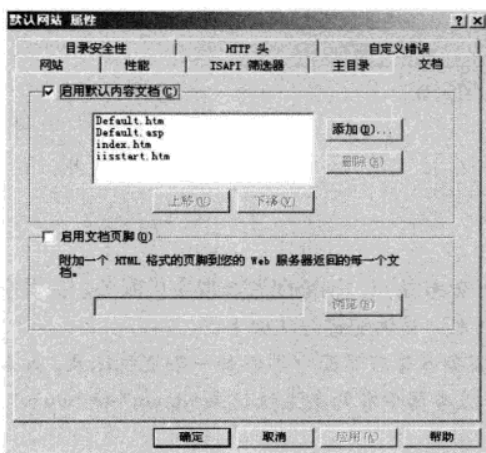


图 5-4-9 文档选项卡

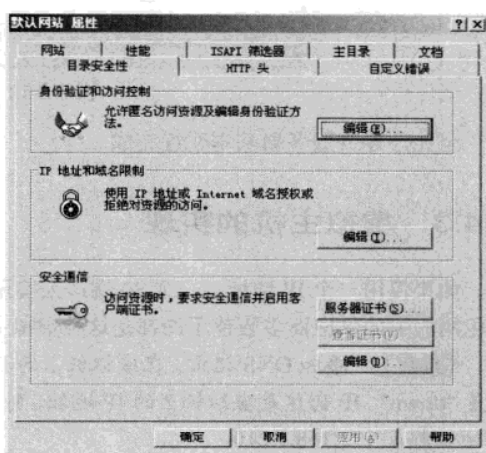


图 5-4-10 目录安全性选项卡

STEP 10 设置“自定义错误”选项卡。本实验中,这里保持默认值。

STEP 11 允许执行 ASP。Windows Server 2003 默认是不允许执行 ASP 代码的,在如图 5-4-11 所示的“Web 服务扩展”中允许“Active Server Pages”功能。

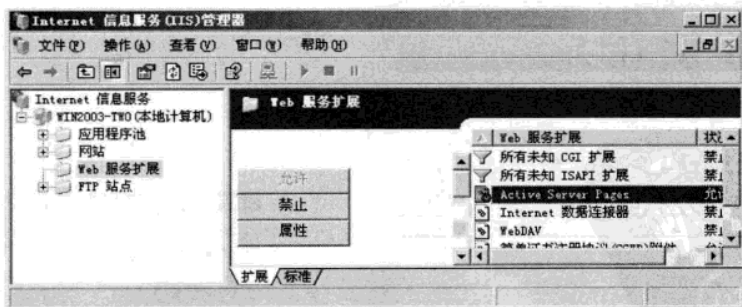


图 5-4-11 Web 服务扩展

STEP 12 测试。在虚拟机 1 的 IE 地址栏中输入“http://www.sales.test.com”,如图 5-4-12 所示,可以访问到留言板页面。

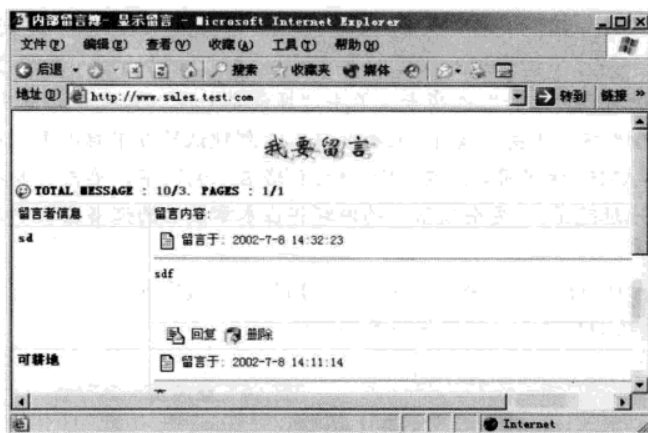


图 5-4-12 访问留言板

至此，Web 服务器基本配置完成。

5.4.3 虚拟主机的实现

如果仅用一个 IP 地址，一个 80 端口来实现多个 Web 站点，则需配置虚拟主机服务，提供空间租用服务的供应商多数使用的都是这种虚拟主机技术。具体配置方法如下。

STEP 1 添加 DNS 记录。在虚拟机 2 的 DNS 服务器管理界面中再添加一条主机记录，如名称是“down”，IP 仍然是虚拟机 2 的 IP 地址，则 DNS 服务器中有两条主机记录“down”和“www”，IP 地址都是 192.168.1.210。

STEP 2 修改默认站点属性。单击图 5-4-5 中的“高级”按钮，打开“高级网站标识”对话框，如图 5-4-13 所示。

单击“编辑”按钮，打开“添加/删除网站标识”对话框，在“主机头值”中填入对应的域名。如图 5-4-14 所示填写，IP 地址选择 192.168.1.210，主机头值中填入 www.sales.test.com，多次单击

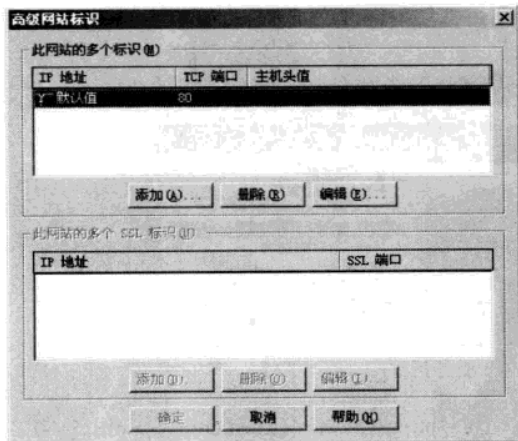


图 5-4-13 高级网站标识对话框

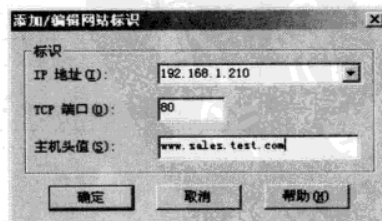


图 5-4-14 添加主机头值

“确定”按钮，完成主机头修改。

STEP 3 新建 Web 站点。右键单击如图 5-4-11 所示的“网站”选项，在快捷菜单中选择“新建”→“网站”命令，打开“网站创建向导”，单击“下一步”按钮，在网站描述中随便填入相应信息，如“down”，单击“下一步”按钮，打开如图 5-4-15 所示的对话框进行填写，网站 IP 地址是 192.168.1.210，端口号是 80，网站的主机头是 down.sales.test.com。

单击“下一步”按钮继续，“网站创建向导”要求输入该网站的主目录，这里填入“C:\”，并选中“允许匿名访问网站”复选框。单击“下一步”按钮，询问网站访问权限，如图 5-4-16 所示填写。选中“浏览”复选框的目的是如果网站在当前目录下找不到默认文档，将以列表的形式显示当前站点下所有文件和目录，单击“下一步”按钮，完成向导。

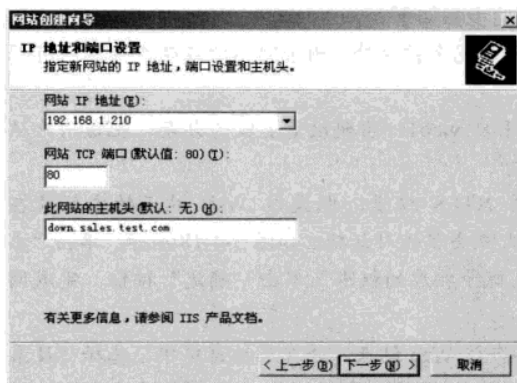


图 5-4-15 新建网站向导

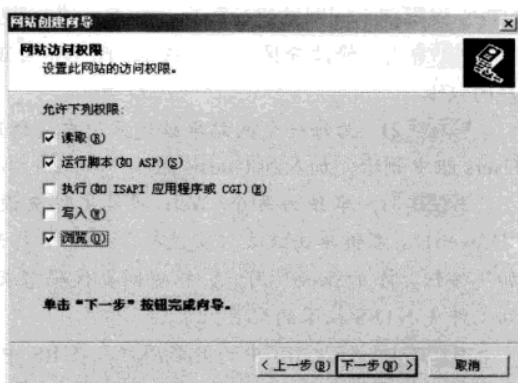


图 5-4-16 设置网站访问权限

STEP 4 测试。在虚拟机 1 的 IE 浏览器的地址栏中输入“www.sales.test.com”，显示的是留言板；输入“down.sales.test.com”，访问的窗口如图 5-4-17 所示，以超链接的方式显示当前目录下的文件。

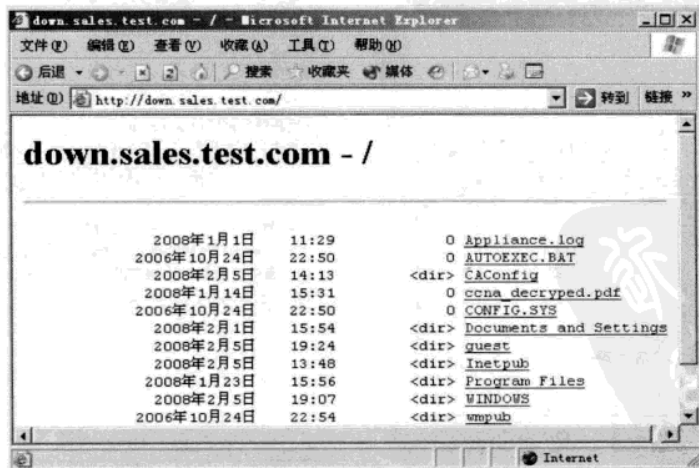


图 5-4-17 允许目录浏览的网站

重复前面的步骤,采用虚拟主机头的方式,在同一台服务器上,使用同一个 IP 地址,同一个 80 端口,可以同时提供多个 Web 站点。

实验 5-5 多 Web 站点服务器的安全配置

同一台服务器上多达几十个网站,因有些网站的 ASP 代码漏洞太多,如缺少图片上传验证机制,数据库没有防下载功能等,极易被有不良企图的人利用,通过攻破一个 Web 站点,进一步攻破所有 Web 站点,甚至控制整台服务器,牵一发而动全身。如何配置才能避免因一个网站的疏忽而危及整个服务器的安全呢?

首先要保证系统和系统盘的安全,其次把所有部门的网站都放置到非系统分区上,最后采用 NTFS 权限把不同网站进行隔离。对网站进行隔离的步骤如下。

STEP 1 修改分区 NTFS 权限。除保留管理员组完全控制外,删除网站所在磁盘分区所有用户的权限。

STEP 2 为每一个网站单独建立用户。新建用户 web1,密码设置要较为复杂,把该用户从 Users 组中删除,加入到 Guests 组。

STEP 3 单独为每个 Web 网站文件夹设置 NTFS 权限。假设该 Web 站点的主目录在“D:\web1”,右键单击该文件夹选择“属性”,打开文件夹属性对话框,如图 5-4-18 所示。单击“添加”按钮,添加 web1 用户,根据网页代码需求,赋予相应的权限。单击“确定”按钮,完成网站文件夹 NTFS 权限的配置。

STEP 4 修改 IIS 中的匿名用户。在 IIS 中单击该 Web 站点,并在属性窗口中,选择“目录安全性”选项卡,单击“身份验证和访问控制”框中的“编辑”按钮,打开“身份验证方法”对话框,如图 5-4-19 所示。

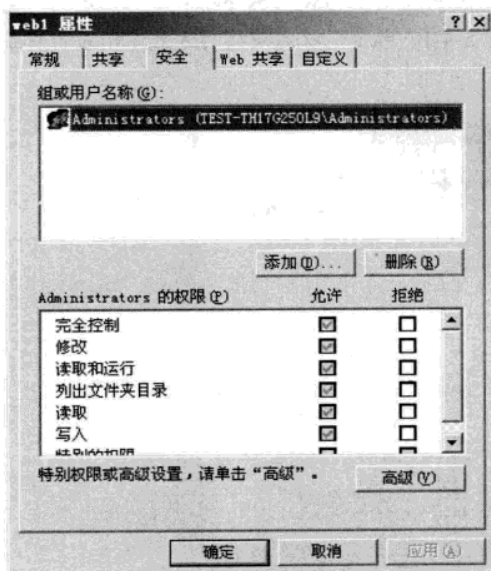


图 5-4-18 Web 目录的权限设置

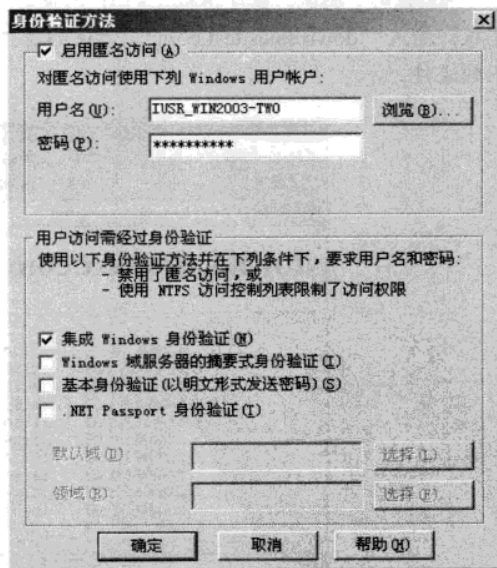


图 5-4-19 Web 站点的身份验证方式

把用户名从 IUSR_WIN2003-TWO 换成 web1, 密码填入 web1 用户对应的密码, 单击“确定”按钮完成配置。

STEP 5 重复步骤 **STEP 2**、**STEP 3**、**STEP 4**, 把每一个 Web 站点设置成使用不同的匿名用户, 同时 Web 站点对应的文件夹上赋予对应匿名用户的相应 NTFS 权限。

经过上述设置后, 即使有的网站被黑客上传了木马程序, 也只是危及该网站的安全, 不会波及到整套服务器, 其他 Web 站点不受影响。

【快问快答】 创建的 Web 服务器是提供影视服务, 为避免网络流量负荷过大, 如何实现限制本组织以外的用户访问?

答: 可以实现该功能。以虚拟机 2 上的默认站点为例, 单击如图 5-4-10 所示的“IP 地址和域名限制”框架中的“编辑”按钮, 打开如图 5-4-20 所示的对话框, 如图示进行操作。其结果是“默认情况下, 所有计算机都将被拒绝访问”, 添加进来的 IP 地址除外, 如单位地址是从 202.119.240.0 到 202.119.55.255 的 16 个 C 类地址, 只要添加如图 5-4-20 所示的一条就够了。这样就实现了只有这 16 个 C 类的 IP 地址可以访问该站点, 除此之外的 IP 访问, 如虚拟机 1, 都将收到如图 5-4-21 所示的错误提示网页。

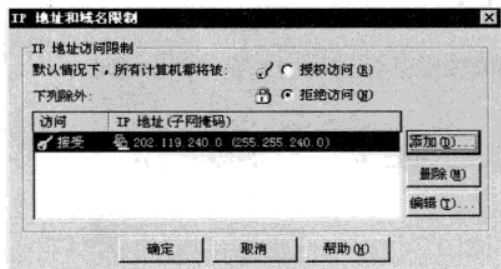


图 5-4-20 IP 地址访问限制

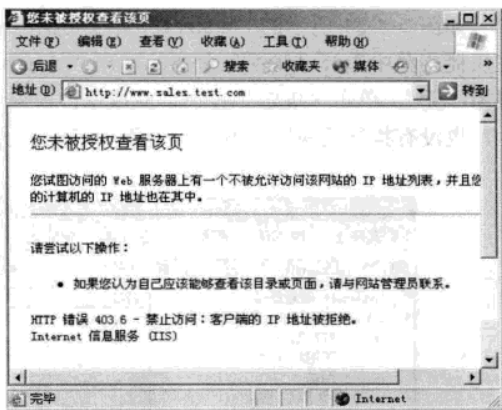


图 5-4-21 客户端的 IP 地址被拒绝

这样的错误提示对用户来说不够明确, 可以根据提示发现是 403.6 的错误, 单击如图 5-4-10 所示的“自定义错误”选项卡, 找到 403.6 对应的网页所在位置, 并使用网页编辑器修改此网页, 或者指向用户新建的网页, 以后客户端的出错提示信息就更直观了, 如图 5-4-22 所示。

【快问快答】 在 Windows 2000 Server 中运行正常的网页, 为何复制到 Windows Server 2003 中却无法正常运行?

答: Windows Server 2003 中默认是不允许使用“父路径”, 也就是在 ASP 的代码中不允许使用“../”的相对路径, 最简单的办法是 Windows Server



图 5-4-22 自定义错误网页

2003 启用“父路径”的支持。如图 5-4-8 所示,单击“配置”按钮,打开“应用程序配置”对话框,再单击“选项”选项卡,选中其中的“启用父路径”复选框,即可解决问题,如图 5-4-23 所示。

【快问快答】采用何种办法可以实现既不修改网站代码(因漏洞层出不穷,所以修改代码工作量大,且不能一劳永逸),又能保证服务器的安全?

答:一些 IIS+ASP (Active Server Page, 活动服务页) 的 Web 网站提供了文件上传功能,用户可以通过 Web 上传图片 and 附件。如果代码写得不严密,很可能就会被黑客加以利用,上传一些木马文件,如含有“海阳顶端”的 ASP 文件,通过木马文件,黑客可以远程操纵服务器上的文件,轻者网站瘫痪,重者系统崩溃,造成灾难性的后果。下面介绍防范的方法。

如图 5-4-24 所示的“images”文件夹就是网站用来上传文件的文件夹,右键单击“images”在快捷菜单中选择“属性”命令,打开“images 属性”对话框,修改“目录”选项卡下的执行权限为“无”,单击“确定”按钮,完成修改。修改后,即使黑客在 images 文件夹中上传了木马文件,也没有执行的权限,网站安全得到了一定的保障。

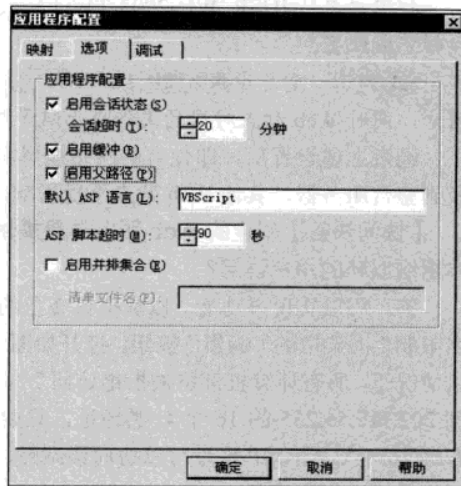


图 5-4-23 启用父路径



图 5-4-24 取消文件夹的执行权限

【快问快答】虽然提供了正确的管理员密码(可以用记事本打开 config.asp, 修改 Password 一行),可删除和回复留言为何失败?

答:查看“c:\guest”文件夹的 NTFS 权限,如图 5-4-26 所示。网站的匿名用户属于 Users 组成员,Users 组成员对文件夹“c:\guest”仅有读取的权限,而添加或删除留言都需要修改“c:\guest”文件夹中的“guest.mdb”这个数据库文件,因权限不够,无法添加或删除留言。修改 Users 组的权限,如图 5-4-26 所示,添加“修改”权限。再次测试,可以正常添加或删除留言。

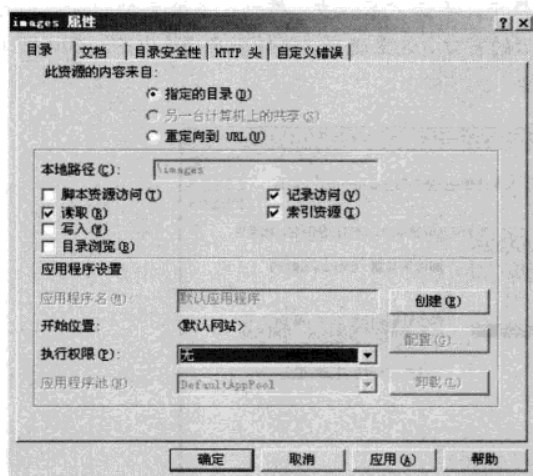


图 5-4-25 取消文件夹执行权限



图 5-4-26 网站文件夹的 NTFS 权限

5.5 E-mail 服务器

Windows 2000 Server 只带有 SMTP 服务（负责发送邮件），却没有 POP3 服务（负责收取邮件）。因此，在不使用第三方软件的情况下，根本无法利用 Windows 2000 Server 系统架设企业邮局。而新版的 Windows Server 2003 则带有完整的 SMTP 和 POP3 服务，并且能支持有活动目录和无活动目录两种环境，最关键的是该服务被集成，不需额外支付费用。本节以 Windows Server 2003 企业版非域控制器为例，介绍邮件服务器的使用。

5.5.1 安装 SMTP 和 POP3 服务

默认情况下，Windows Server 2003 并不随操作系统一起安装 SMTP 和 POP3 服务，使用前需添加此项服务。

STEP 1 在真实机上，依次单击“开始”→“程序”→“管理工具”→“管理您的服务器”，打开“管理您的服务器”窗口，如图 5-5-1 所示，单击“添加或删除角色”链接。

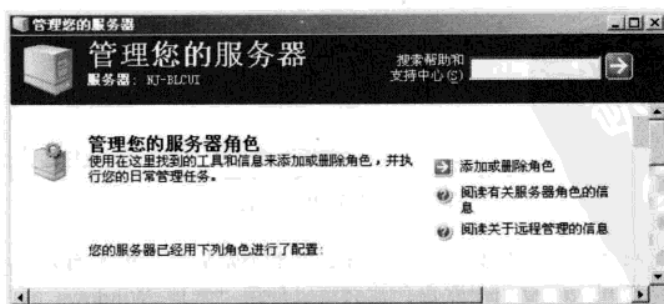


图 5-5-1 管理您的服务器窗口

STEP 2 在“配置您的服务器向导”对话框中，单击“下一步”按钮，系统自动扫描当前已经安装的服务，扫描完成后，出现如图 5-5-2 所示的窗口，这里选择“邮件服务器 (POP3, SMTP)”服务，单击“下一步”按钮开始安装邮件服务器。

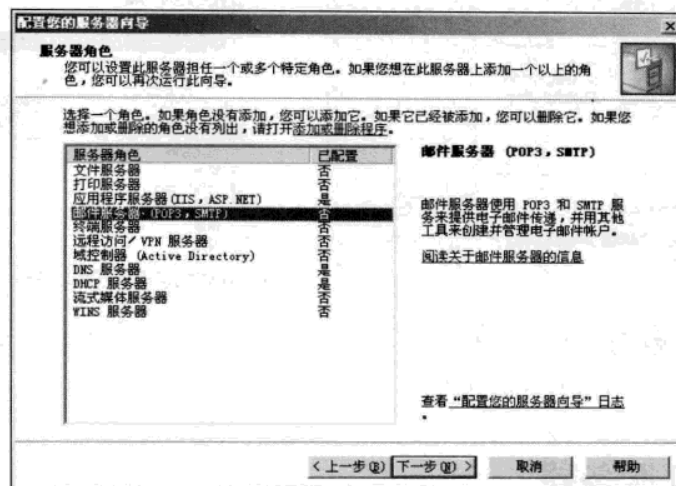


图 5-5-2 添加 POP3 和 SMTP 服务

STEP 3 随后出现如图 5-5-3 所示的对话框，这里需要填写身份验证方法和电子邮件域名。POP3 服务提供 3 种不同的身份验证方法来验证连接到邮件服务器的用户。在邮件服务器上创建任何电子邮件域之前，必须选择一种身份验证方法。

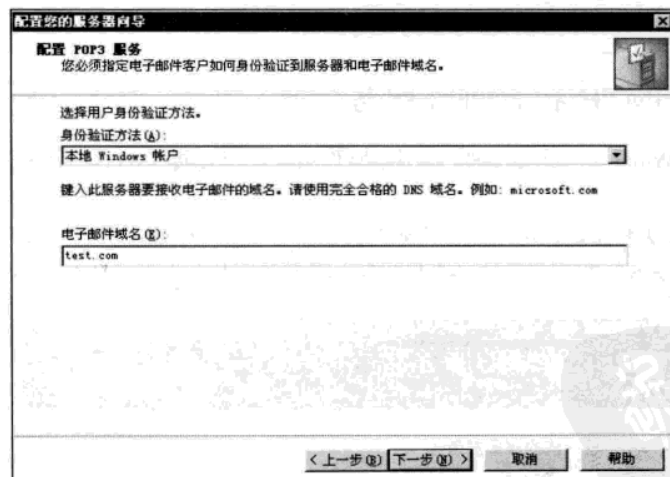


图 5-5-3 配置 POP3 服务

(1) 本地 Windows 账户身份验证。如果邮件服务器不是活动目录域的成员，并且希望在安装了邮件服务的本地计算机上存储用户账户，那么可以使用“本地 Windows 账户”身份验证方法来进行邮件服务的用户身份验证。本地 Windows 账户身份验证将邮件服务集成到本地计算机的安

全账户管理器 (SAM) 中。通过使用安全账户管理器, 在本地计算机上拥有用户账户的用户就可使用与由 POP3 服务提供的或本地计算机进行身份验证的相同的用户名和密码。

本地 Windows 账户身份验证可以支持一个服务器上的多个域, 但是不同域上的用户名必须唯一的。例如, 用户名为 `user@abc.net` 和 `user@bcd.com` 的用户不能同时在一个服务器上存在的。如果以相应的用户账户创建一个邮箱, 则该用户账户将被添加到“POP3 用户”本地组, 但“POP3 用户”组的成员不能在本地登录服务器。使用计算机的本地安全策略可以增强对本地登录的限制, 因此仅授权的用户有本地登录权限, 这样可以提高服务器的安全性。另外如果用户不能本地登录到服务器, 并不影响其使用 POP3 服务。

本地 Windows 账户身份验证同时支持明文和 SPA (Secure Password Authentication, 安全密码身份验证) 的电子邮件客户端身份验证。其中的明文以不安全和非加密的格式传输用户数据, 所以不推荐使用明文身份验证。而安全密码身份验证要求电子邮件客户端使用安全的身份验证传输用户名和密码, 因此推荐使用该方法来取代明文身份验证。

(2) Active Directory 集成的身份验证。如果安装 POP3 服务的服务器是活动目录域的成员或者是活动目录域控制器, 则可以使用活动目录集成的身份验证。同时, 使用活动目录集成的身份验证, 可以将 POP3 服务集成到现有的活动目录域中。如果创建的邮箱与现有的活动目录用户账户相对应, 则用户就可以使用现有的活动目录域用户名和密码来收发电子邮件。

可以使用活动目录集成的身份验证来支持多个 POP3 域, 这样就可以在不同的域中建立相同的用户名。例如, 可以使用名为 `admin@abc.net` 和 `admin@bcd.com` 的用户。每个邮箱都与一个活动目录用户账户相对应。当使用活动目录集成的身份验证时, 若要管理 POP3 服务, 则必须登录到活动目录域, 而不是登录到本地计算机上。

活动目录集成的身份验证同时支持明文和安全密码身份验证的电子邮件客户端身份验证。SPA 仅支持活动目录集成的身份验证和本地 Windows 账户身份验证。如果启用了 SPA, 则用户的电子邮件客户端也必须配置为使用 SPA。如果配置邮件服务器要求安全密码身份验证, 只会影响 POP3 服务而不会影响简单邮件传输协议 (SMTP) 服务。

(3) 加密密码文件身份验证。“加密的密码文件”身份验证对于还没有安装活动目录, 并且又不想在本地计算机上创建用户的大规模部署来说十分理想, 同时从一台本地计算机上就可以很轻松地管理可能存在的大量账户。

加密密码文件身份验证将使用用户的密码来创建一个加密文件, 该文件存储在服务器上用户邮箱的目录中。在用户的身份验证过程中, 用户提供的密码将被加密, 然后与存储在服务器上的加密文件进行比较。如果加密的密码与存储在服务器上的加密密码相匹配, 则用户通过身份验证。如果是使用加密密码文件身份验证, 则可以在不同的域中使用相同的用户名。

本书中选择“本地 Windows 账户”。电子邮件域名输入在公网上注册的有效域名, 如果邮件只是组织内部使用, 则可以随意配置, 这里的域名也就是要注册给用户的邮件账号“@”后面的后缀。本实验中, 填入“test.com”。单击“下一步”按钮, 完成邮件服务器的安装。

5.5.2 注册邮件账号

STEP 1 打开 POP3 服务界面。依次单击“开始”→“程序”→“管理工具”→“POP3 服务”, 打开如图 5-5-4 所示的 POP3 管理界面。

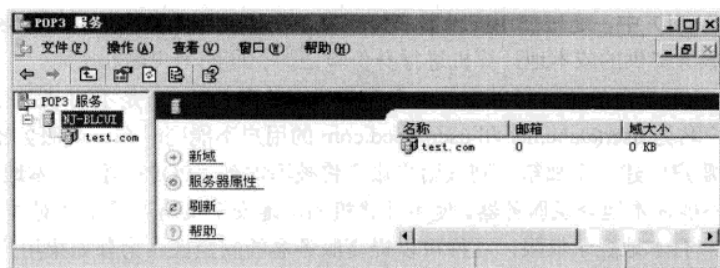


图 5-5-4 POP3 管理界面

STEP 2 添加邮箱。右键单击“test.com”，在快捷菜单中选择“新建”→“邮箱”，打开“添加邮箱”对话框，如图 5-5-5 所示。

邮箱名中填写要注册给用户的邮件账号“@”前面的字符，它与图 5-5-3 中所填写的域名共同组成了用户的邮件账号，如添加邮箱名“user1”，那么完整的邮箱应该是“user1@test.com”；如果创建邮件账号之前没有这样一个 Windows 账户存在，应选中“为此邮箱创建相关联的用户”复选框，否则会提示报错信息，提示 Windows 中找不到该账户；输入邮箱对应的密码。

注意



在计算机管理的“用户和组管理”中创建一个普通用户，该用户默认可以在本地登录服务器，但无法使用邮箱，如想使用 POP3 服务，需在 POP3 中新建该账户的邮箱，不要选中“为此邮箱创建相关联的用户”复选框，因 Windows 已经存在该账户，也就是说 POP3 中的账户和“用户和组管理”中的账户是同一个数据库；在 POP3 中添加邮箱时，选中“为此邮箱创建相关联的用户”复选框，创建邮箱的同时，添加了 Windows 账户，该 Windows 账户属于“POP3”用户组，有使用邮箱的权限，但默认没有在本机登录服务器的权限。

最后，单击“确定”按钮，完成用户账号的创建。此时会出现如图 5-5-6 所示的提示窗口，提示如果使用的是明文验证，登录邮件服务器的账户名是“user1@test.com”；如果使用的是安全密码身份验证，账户名是“user1”。

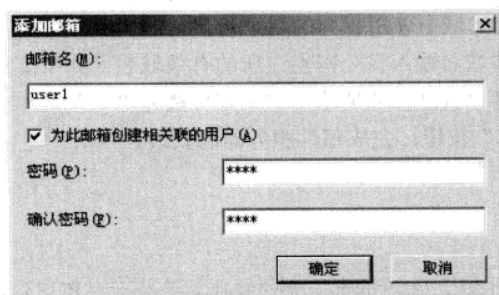


图 5-5-5 添加邮箱

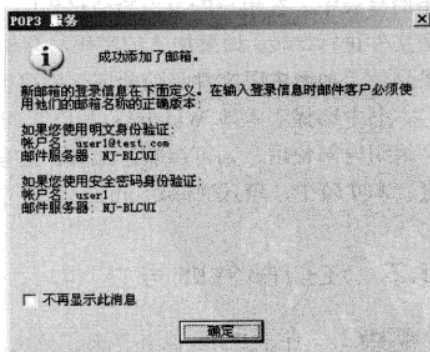


图 5-5-6 添加邮箱

注意



Windows 邮件服务器默认使用的是明文验证, 也就是说登录邮件服务器的账户名应该是完整的邮箱, 如 “user1@test.com”。

这样就建立了第一个邮箱 “user1@test.com”, 依此方法再创建第二个邮箱 “user2@test.com”。

STEP 3 添加邮件服务器域名。为了方便访问邮件服务器, 给邮件服务器添加域名。在真实机的 DNS 中新建一条主机记录, 名称为 “mail”, IP 为邮件服务器的地址, 本实验中仍填入真实机的 IP 地址 192.168.1.200。

5.5.3 Outlook Express 设置

E-mail 服务器设置完成后, 接下来是客户端软件的设置。Outlook Express 的设置步骤如下。

STEP 1 打开 “Internet 连接向导” 对话框。在虚拟机 1 中, 打开 Outlook Express, 如果是第一次使用 Outlook Express, 会自动打开 “Internet 连接向导”; 如果以前使用过 Outlook Express, 单击 “工具” 菜单中的 “账户” 子菜单, 打开 “Internet 账户” 对话框, 如图 5-5-7 所示。单击 “Internet 账户” 对话框中的 “添加” 按钮, 选择 “邮件” 子菜单, 打开 “Internet 连接向导”。

STEP 2 输入姓名。“Internet 连接向导” 要求输入显示的用户名, 这里填入 “user1”, 如图 5-5-8 所示。

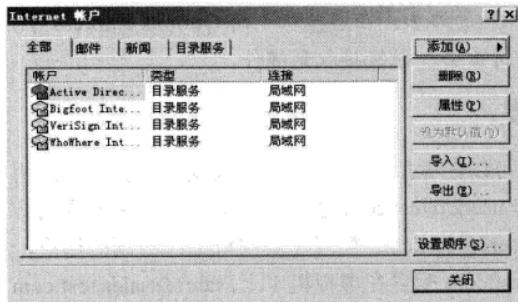


图 5-5-7 Internet 账户

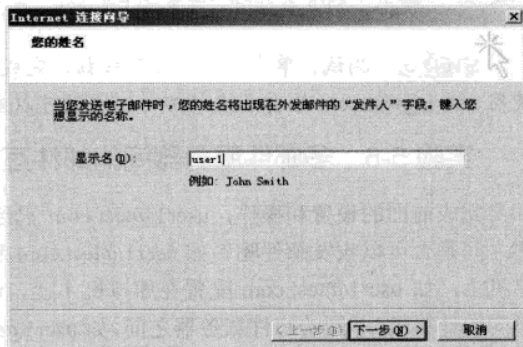


图 5-5-8 填入邮箱姓名

STEP 3 输入电子邮件地址。单击 “下一步” 按钮, 要求填入电子邮件地址, 填入 “user1@test.com”, 如图 5-5-9 所示。

STEP 4 输入电子邮件服务器地址。单击 “下一步” 按钮, 要求填入邮件服务器的地址, 如图 5-5-10 所示, 在 POP3 和 SMTP 服务器中均填入 “mail.test.com”, 或者填入 IP 地址 “192.168.1.200”。

STEP 5 填入邮件服务器登录信息。单击 “下一步” 按钮, 要求填入邮件服务器登录信息,

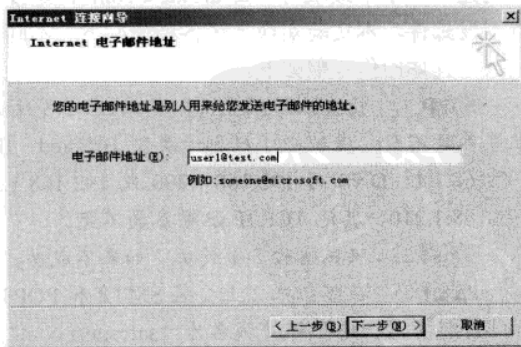


图 5-5-9 填入邮件地址

如图 5-5-11 所示, 因服务器上没有选中“使用安全密码验证登录 (SPA)”, 所以在“账户名”处填入“user1@test.com”, 填入邮箱账户的“密码”, 根据需要决定是否选中“记住密码”复选框, 但不要选中“使用安全密码验证登录 (SPA)”复选框。

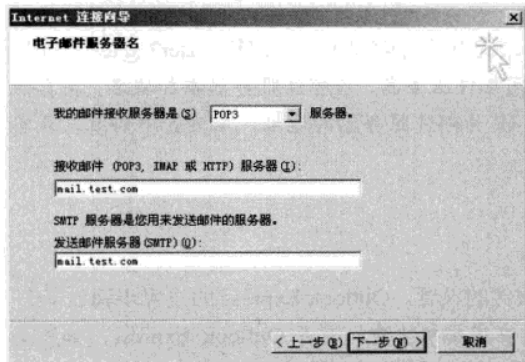


图 5-5-10 填入邮件服务器的地址

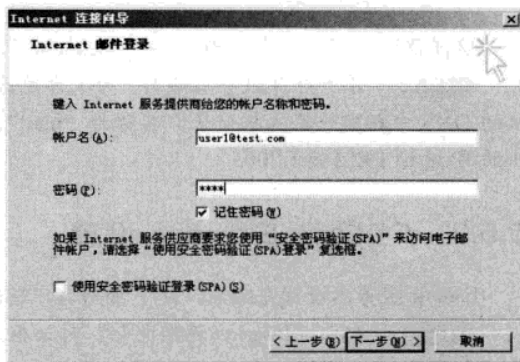


图 5-5-11 填入邮件服务器登录信息

注意



如果未采用 SPA 验证时, 账户名格式为 xxx@xxx.xxx, 本例中为 user1@test.com; 而如果使用了 SPA 验证时, 账号格式为 xxx, 本例中为 user1。

STEP 6 测试。单击“下一步”按钮, 完成邮箱的添加。在虚拟机 1 的 Outlook Express 中, 使用 user1@test.com 给自己发封邮件, 应该可以发送出去, 也能接收到邮件。

实验 5-6 多邮件服务器间的邮件互发

完成前面的设置和操作, user1@test.com 已经可以在虚拟机 1 上正常地收发邮件。但不同用户之间是否可以收发邮件呢? 如 user1@test.com 和 user2@test.com 之间; 不同的用户在不同的计算机上, 如 user1@test.com 配置在虚拟机 1 上, user2@test.com 配置在真实机上; 不同的用户, 不同的计算机, 不同的邮件服务器之间, 如 user1@test.com 配置在虚拟机 1 上, sale1@sales.test.com 配置在虚拟机 2 上。如公司的邮件域名为“@test.com”, 销售部门的邮件用户众多, 专门给销售部门建立一个下级域名“@sales.test.com”, 这样公司用户, 销售部门用户, 以及外部用户之间可以互发邮件。本实验实现上述各种情况下, 不同邮箱之间的邮件互发。本实验较为复杂, 牵扯面较大, 具体操作步骤如下。

STEP 1 检查网络配置。真实机的 DNS 改成自己的 IP 地址, 即 192.168.1.200, 其他 TCP/IP 配置参数不变; 虚拟机 1 的网卡类型 Bridged, IP 地址 192.168.1.220, 掩码 255.255.255.0, 网关 192.168.1.1, DNS 为 192.168.1.200 或 192.168.1.210; 虚拟机 2 的 DNS 改成自己的 IP 地址, 即 192.168.1.210, 其他 TCP/IP 配置参数不变。

STEP 2 确保实验 5-4 成功。如果不成功, 请先完成实验 5-4 的配置, 再继续本实验。

STEP 3 在虚拟机 2 上安装 SMTP 和 POP3 服务。依照 5.5.1 小节的步骤, 在虚拟机 2 上添加邮件服务器, 电子邮件域名为“sales.test.com”。

STEP 4 在虚拟机 2 上注册邮件账户。依照 5.5.2 小节的步骤, 在虚拟机 2 上添加邮箱

“sale1@sales.test.com”。并在虚拟机 2 的 DNS 中添加一条新的主机记录 mail.sales.test.com, IP 指向虚拟机 2 自己的 IP 地址 192.168.1.210。

STEP 5 添加 MX (Mail Exchanger, 邮件交换器) 记录。在真实机和虚拟机 2 上添加 MX 记录, 这里只演示真实机的操作, 虚拟机 2 的操作与真实机类似。在真实机的 DNS 管理器中, 右键单击“test.com”标准主要区域, 选择“新建邮件交换器 (MX)”, 打开“新建资源记录”对话框, 如图 5-5-12 所示进行填写, “主机或子域”保留为空, “邮件服务器的完全合格的域名”栏填入“mail.test.com”, “邮件服务器优先级”保持默认值“10”。在虚拟机 2 上, 这里要填入 mail.sales.test.com, 实际工作环境中, DNS 和邮件服务器往往不在一台服务器上, 这里的 MX 记录一定要指向邮件服务器。

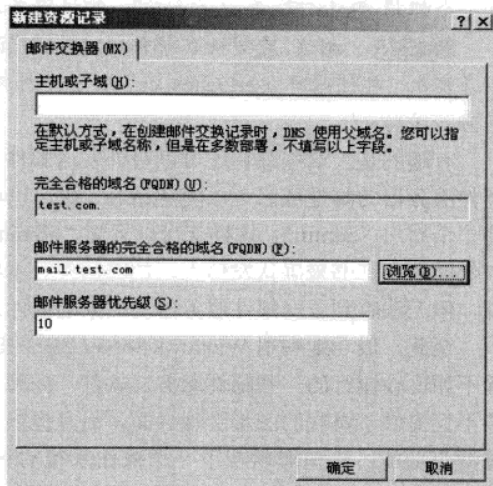


图 5-5-12 添加 MX 记录

STEP 6 配置邮件中继。Windows Server 2003 的 SMTP 虚拟服务器, 默认只允许在同一个域内发送邮件, 下面配置允许向任何地方发送邮件。在真实机和虚拟机 2 上, 依次单击“开始”→“程序”→“管理工具”→“Internet 信息服务 (IIS) 管理器”, 在“Internet 信息服务 (IIS) 管理器”窗口中右键单击“默认 SMTP 虚拟服务器”, 打开“默认 SMTP 虚拟服务器属性”对话框, 选择“访问”选项卡, 如图 5-5-13 所示。

单击“中继”按钮, 打开“中继限制”对话框, 如图 5-5-14 所示操作, 改变默认的选项“仅以下列表”, 选中“仅以下列表除外”单选框。

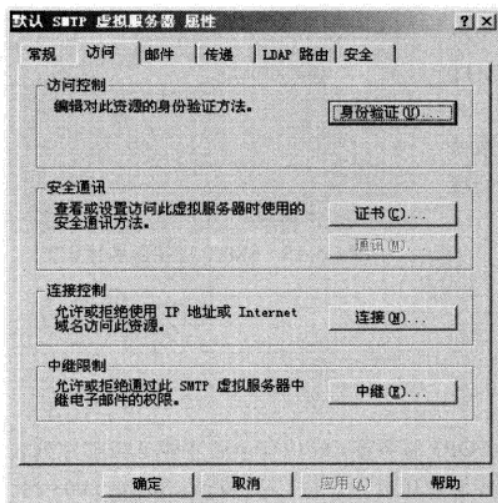


图 5-5-13 配置 SMTP 服务器

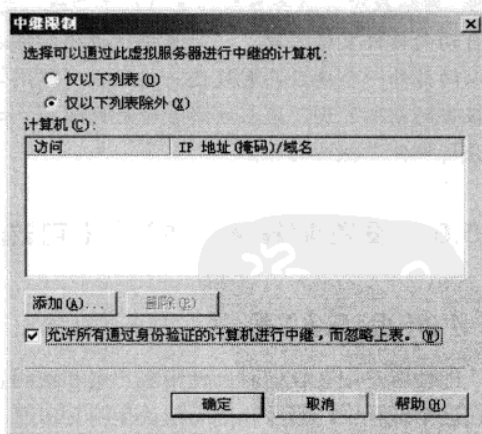


图 5-5-14 配置中继限制

STEP 7 添加邮件账户。依照 5.5.3 小节的方法, 在真实机上的 Outlook Express 中添加一个

邮箱 “user2@test.com”，邮件服务器的地址是 mail.test.com；在虚拟机 2 的 Outlook Express 中添加一个邮箱 “sale1@sales.test.com”，邮件服务器的地址是 mail.sales.test.com。

STEP 8 测试。虚拟机 1(邮件账户 user1@test.com)、虚拟机 2(邮件账户 sale1@sales.test.com) 和真实机(邮件账户 user2@test.com)，3 个邮件账户之间可以任意互发邮件，接收和发送均正常，则实验成功。

有趣的是，这些邮箱还可以对外发送邮件。很多垃圾邮件或者欺骗邮件都是这样来的，因为邮件服务器的邮件域名可以随意命名，账户也可以随便分配，如把邮件域名设为 “263.net”，再创建一个用户 “admin”，这样就可以冒充 “admin@263.net” 向外发信了，本章的最后一节会介绍如何借助数字证书来确认发信人，加密信件。本实验中的域名不是公网注册的，虽可以向外发送邮件，但无法收到公网邮件服务器发回来的信件。

至此，成功地利用 Windows Server 2003 架设了一套免费的邮件系统。但它的功能还很有限，远不如比较流行的一些邮件服务器软件，如国产的 Webeasymail 等，这些第三方的邮件服务器软件不仅提供了直观的图形管理界面，而且提供了自动回复、邮件监控、邮箱大小限制、垃圾邮件过滤等功能，希望微软在下一个操作系统的版本中能有所增强。为了便于大家的学习，下载的 network.rar 压缩包中提供了 Webeasymail 软件。

5.5.4 设置邮箱基本属性 (可选)

在如图 5-5-13 所示的对话框中，单击“邮件”选项卡，打开如图 5-5-15 所示的对话框。

● 限制每封邮件大小：可以在“邮件”选项卡中“限制邮件大小为 (KB)”设置每封外发邮件的最大尺寸 (以 KB 为单位)。

● 设置故障通知账号：如果邮件在发送中因大小超限，网络或对方服务器故障等情况不能送达时，SMTP 除自动向信件发送人发送一封未抵达说明邮件以外，还可以向另外一个地址同时发送一封副本。建议“将来传递报告的副本发到”填入网络管理员的邮箱，便于管理员分析邮件未抵达的原因。

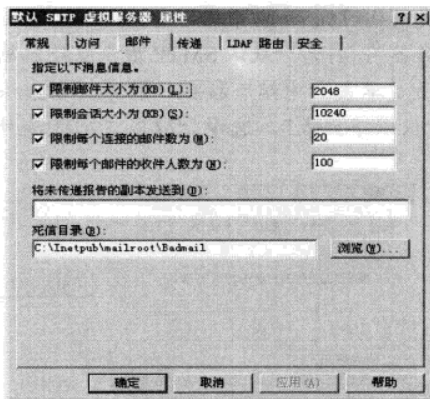


图 5-5-15 SMTP 虚拟服务器设置

5.5.5 设置邮箱安全属性 (可选)

1. POP3 安全设置

邮件客户端在收信时会使用账户名和密码登录 POP3 服务器，成功登录后才能下载邮件列表，而在这个过程中，账号和密码默认是明文传递，很容易被窃听器窃得。Windows Server 2003 自带的 POP3 服务器支持在服务器端和客户端共同部署 SPA 安全密码验证，对传输的账号和密码进行加密，来保证用户账号和密码的安全。

(1) SPA 服务器端设置。依次单击“开始”→“程序”→“管理工具”→“POP3 服务”，

打开“POP3 服务”控制台。打开 POP3 服务控制台窗口，右键单击计算机名，选择“属性”，打开如图 5-5-16 所示的对话框，选中“对所有客户端连接要求安全密码身份验证 (SPA)”复选框，提示要使此配置生效需要重启 POP3 服务，重启 POP3 服务，即完成服务器端 SPA 安全验证。

(2) SPA 客户端设置。Outlook Express 客户端软件支持 SPA 安全验证，在如图 5-5-7 所示的对话框中，选择对应的邮件账户，单击“属性”按钮，打开 Outlook Express 邮件账户属性设置对话框，单击“服务器”选项卡，如图 5-5-17 所示，选中“使用安全密码验证登录”复选框后，即完成客户端的安全验证，注意账户名要由“user1@test.com”或“user2@test.com”改成“user1”。

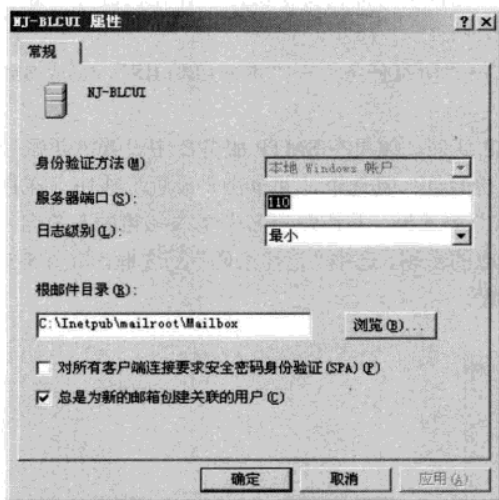


图 5-5-16 POP3 服务器的安全设置

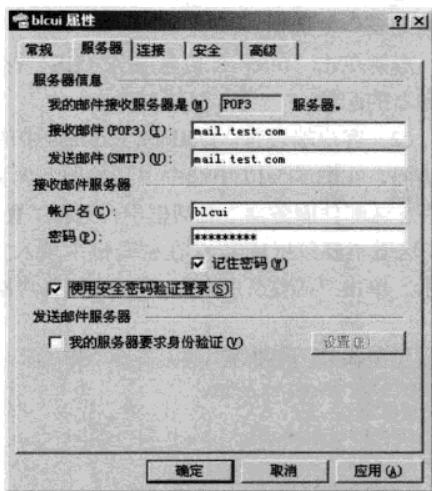


图 5-5-17 Outlook Express 的安全设置

注 意



服务器端与客户端均需设置为 SPA 验证，否则，将无法完成收信操作。到目前为止，邮件客户端软件 Foxmail 仍不支持 SPA 验证。

2. SMTP 安全设置

在默认情况下，SMTP 服务器启用的是“匿名访问”的验证方式。也就是说，任何人在没有账户的情况下都可以使用 SMTP 服务器来发送邮件，这也是垃圾邮件泛滥的一个原因，很多邮件服务器都开启了垃圾邮件检测功能，如果发现来自某一个邮件服务器的垃圾邮件过多，将该邮件服务器加入黑名单，拒收来自该邮件服务器的一切邮件，出于保护自身利益的考虑，很多邮件服务器发送邮件都要进行身份验证。而 SMTP 服务器既可以实现客户端发信时使用账号与密码进行验证连接，还可以通过 IP 地址验证连接，也可以使用证书进行更高级别的身份验证后再进行发信。

(1) 服务器端设置。单击如图 5-5-13 中所示的“身份验证”按钮，打开如图 5-5-18 所示类似的身份验证窗口中，选中“匿名访问”复选框，用户无需提供有效的账号与密码即可连接使用 SMTP 服务器；选中“基本身份验证”复选框，用户需要提供用户名和密码才能连接至 SMTP 服务器，但账号与密码是以明文传输，安全性较差；选中“集成的 Windows 身份验证”复选框，只有拥有有效 Microsoft Windows 账号的用户才能连接至 SMTP 服务器，同时，账号与密码都将使用 NTLM 进行加密，但信息数据不被加密。出于安全考虑，此处 SMTP 服务器需要身份验证，同时为了保证可以从其他服务器正常接收邮件，这里选择“匿名访问”和“基本身份验证”，如图 5-5-18 所示。

单击如图 5-5-13 所示的“中继”按钮，打开如图 5-5-14 所示的“中继限制”对话框，恢复默认选项，即选中“仅以下列表”单选框和选中“允许所有通过身份验证的计算机进行中继，而忽略上表”复选框。

右键单击“Internet 信息服务 (IIS) 管理器”→“所有任务”→“重新启动 IIS”，完成 SMTP 服务器的配置。

(2) 客户端设置。Outlook Express 中的 SMTP 认证，如果在 SMTP 服务器中设置需要账号密码访问，在图 5-5-17 中选中“我的服务器要求身份验证”复选框，并单击“设置”按钮。在打开的“发送邮件服务器”对话框中，选择“登录方式”单选框，并在账户名中填入邮箱的账户名（记住，这里不要包括域名），在密码框中填入账户对应的密码，选中“记住密码”复选框，如图 5-5-19 所示。单击“确定”按钮，完成邮件客户端的设置。

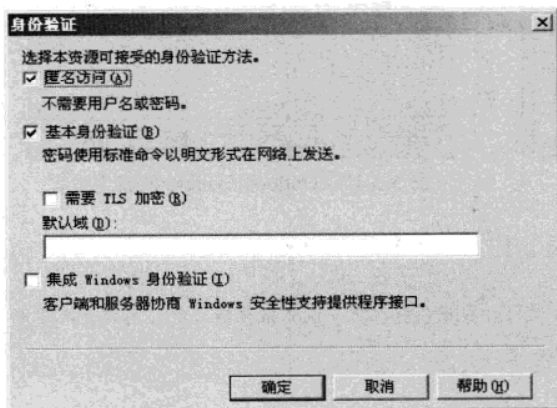


图 5-5-18 SMTP 的身份验证

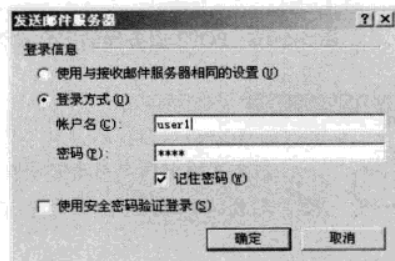


图 5-5-19 邮件发送服务器需要验证的客户端配置

感兴趣的读者可以配置真实机的 POP3 和 SMTP 服务器的安全属性，并使用 user1@test.com 和 user2@test.com 账户进行收发邮件的测试。

5.6 FTP 服务器

对于一个组织来说，为了方便资源的共享，建立 FTP 服务也是很有必要的，虽说文件共享能

起到文件传输的作用,但文件共享在 Internet 范围运用效果并不理想,且会被很多防火墙阻截。Windows Server 2003 也提供了 FTP 服务,但默认并不随操作系统一起被安装,本书在安装 IIS 服务时,同时也安装了 FTP 服务。FTP 服务安装完成后即可使用,FTP 服务的使用与前面介绍的 Web 服务的使用类似,且更为简单。

实验 5-7 实现 FTP 服务

配置真实机上的 FTP 服务,使用虚拟机 2 可以从真实机 c:\ 和 d:\ 下载文件。具体操作步骤如下。

STEP 1 打开 IIS 管理器。在真实机上依次单击“开始”→“程序”→“管理工具”→“Internet 信息服务 (IIS) 管理器”,打开 IIS 管理器,展开本地计算机,展开 FTP 站点,如图 5-6-1 所示。

STEP 2 查看站点主目录。在 FTP 站点中,右键单击“默认 FTP 站点”,选择“属性”命令,选择“主目录”选项卡,如图 5-6-2 所示,默认的本地路径是 c:\inetpub\ftproot 文件夹。

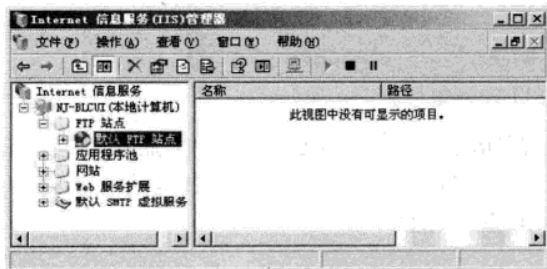


图 5-6-1 FTP 站点管理器

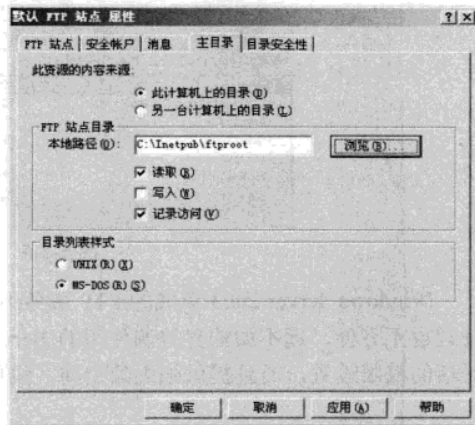


图 5-6-2 FTP 主目录

STEP 3 添加虚拟目录。如图 5-6-1 所示,右键单击“默认 FTP 站点”,依次选择“新建”→“虚拟目录”,打开“虚拟目录创建向导”对话框,单击“下一步”按钮,设置虚拟目录名,输入“disk-c”,单击“下一步”按钮,设置虚拟目录的路径,输入“c:\”,单击“下一步”按钮,设置虚拟目录的访问权限,如图 5-6-3 所示,因这里只提供下载,不允许上传,所以保持默认的读取权限,单击“下一步”按钮,完成 disk-c 虚拟目录的添加。类似地操作,再添加虚拟目录 disk-d,路径指向“d:\”。

STEP 4 创建文件夹。在 c:\inetpub\ftproot 文件夹下创建两个空文件夹,即 disk-c 和 disk-d。

STEP 5 测试。在虚拟机 2 的 IE 浏览的地址栏中输入“ftp://192.168.1.200”,可以访问到真实机上的 FTP 站点,如图 5-6-4 所示。

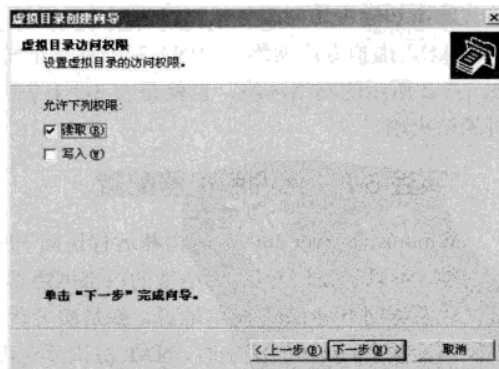


图 5-6-3 设置虚拟目录权限

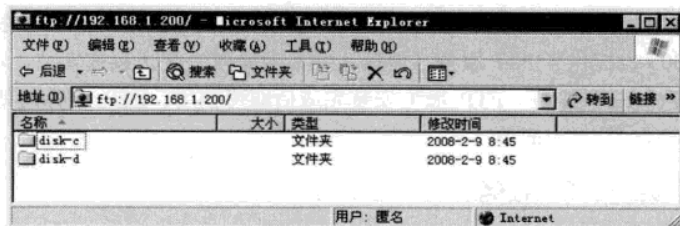


图 5-6-4 访问 FTP 站点

双击 disk-c 文件夹, 如图 5-6-5 所示, 空的 disk-c 文件夹下却出现了整个 C 盘的内容, 其实这里访问的并不是 disk-c 文件夹, 而是 disk-c 虚拟目录, 也就是说虚拟目录和文件夹同名时, 虚拟目录优先。类似的可以访问到 D 盘。

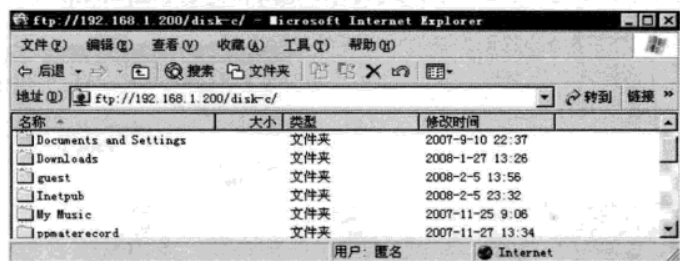


图 5-6-5 访问 FTP 虚拟目录

Windows Server 2003 集成的 FTP 服务用来提供匿名下载比较方便, 但该 FTP 服务功能较弱, 管理也不方便, 远不如业界普遍使用的 Serv-U 软件, Serv-U 软件不仅提供了方便的用户管理, 灵活的权限设置, 而且提供强大的空间、线程、速度限制等。

5.7 路由和远程访问服务器

路由和远程访问服务器可以为网络上的客户端和服务端启用多重协议 LAN 到 LAN 或者 LAN 到 WAN, 虚拟专用网络 (VPN) 和网络地址转换 (NAT) 等服务。在继续配置之前, 首先恢复如图 3-3-2 所示的网络环境, 也就是表 3-3-1 中的网络配置, 为便于 Ping 命令测试, 关闭所有计算机的防火墙。

实验 5-8 代理服务器配置

Windows Server 2003 “路由和远程访问”服务包括 NAT 路由协议, 通过此协议的网络地址转换功能, 可以让使用专用 IP 地址的内部网络客户端通过 NAT 服务转换成服务器外部接口的 IP 地址, 进而访问 Internet, 简单地说, 就是实现代理服务器的功能。实现的原理就是当内部网络客户端发送连接 Internet 的请求时, NAT 协议驱动程序会截获该请求, 并将其转发到目标 Internet 服务器。所有请求看上去都像是来自 NAT 服务器外部接口的 IP 地址一样, 这样就隐藏了内部 IP 配置。根据如图 3-3-2 所示的实验环境来配置 NAT, 实现虚拟机 1 的代理上网, 步骤如下。

STEP 1 网络环境测试。使用 ping 命令测试, 确信恢复了图 3-3-2 所示的网络拓扑, 代理服

服务器可以和内网（虚拟机1）及外网（虚拟机2）正常通信。

STEP 2 打开“路由和远程访问”管理控制台。依次单击“开始”→“程序”→“管理工具”→“路由和远程访问”，打开“路由和远程访问”管理控制台。

STEP 3 启用“路由和远程访问服务器安装向导”。在“路由和远程访问”控制台窗口中，右键单击服务器名称，选择“配置并启用路由和远程访问”，如图 5-7-1 所示。

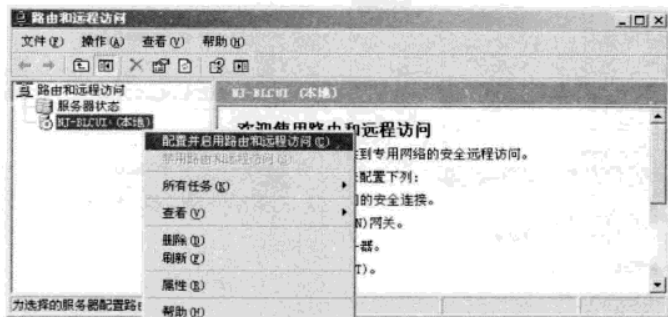


图 5-7-1 启用路由和远程访问

有时会提示出错，弹出如图 5-7-2 所示的窗口，要求停止“Windows 防火墙/Internet 连接共享服务”，并把该服务的启动类型改为“禁用”状态。选择“管理工具”→“服务”，找到“Windows Firewall/Internet Connection Sharing (ICS)”服务，停止并禁用该服务后，重新执行“配置并启用路由和远程访问”。

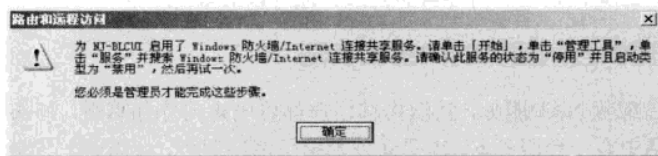


图 5-7-2 路由和远程访问提示框

STEP 4 选择服务类型。在“路由和远程访问服务器安装向导”对话框中，单击“下一步”，出现如图 5-7-3 所示的对话框，选择第二项“网络地址转换（NAT）”。

STEP 5 选择连接外部的接口。单击“下一步”按钮，提示选择连接到 Internet 的接口，选择真实机的物理网卡，也就是 IP 地址是“192.168.1.200”的接口。如图 5-7-4 所示，至于要不要选中“通过设置基本防火墙来在对选择的接口进行保护”复选框，则根据需要而定，一般选中，这样代理服务器本身也受到保护。如果此代理服务器还用作对外提供服务，请不要忘记打开对应的服务端口。本实验中，为了方便 ping 测试，不启用防火墙设置。

STEP 6 选择连接内部的接口。继续单击

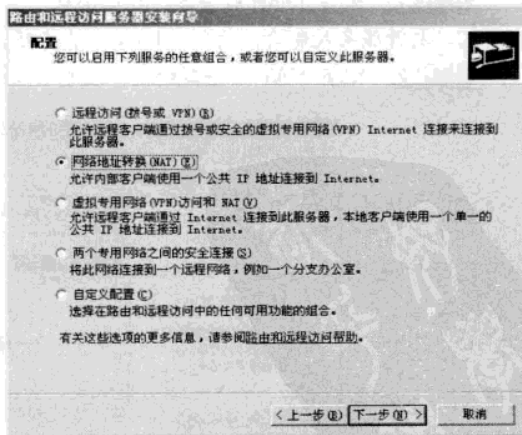


图 5-7-3 选择 NAT 服务

“下一步”按钮，选择连接内部的接口，这里选择 VMnet1，也就是 IP 地址是“192.168.111.1”的网卡，如图 5-7-5 所示。

STEP 7 完成配置。单击“下一步”按钮，再单击“完成”按钮，至此 NAT 服务配置完成。

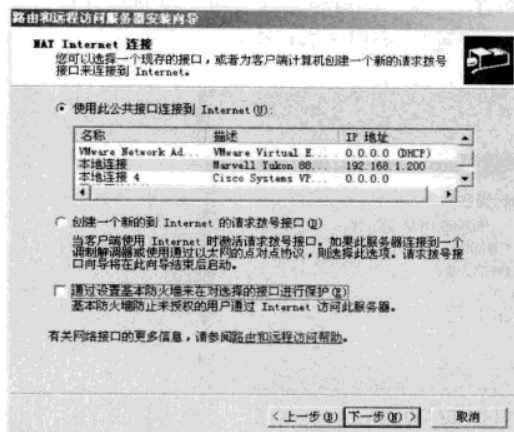


图 5-7-4 选择连接外部的接口

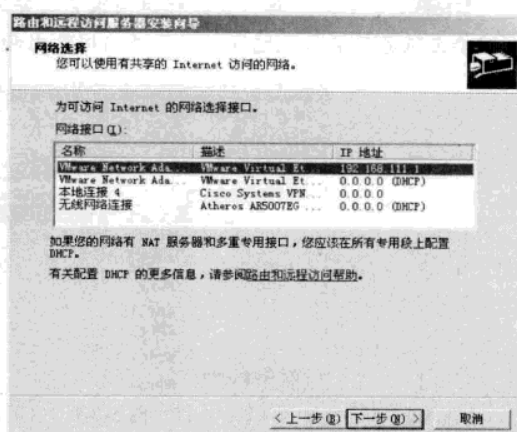


图 5-7-5 选择连接内部的接口

STEP 8 测试。内部网络客户端（这里的虚拟机 1）可以任意访问 Internet，如可以成功访问新浪网。虚拟机 1 也可以访问虚拟机 2，配置 NAT 之前是不可以的；但虚拟机 2 仍然不能访问虚拟机 1，代理服务器提供内网访问外网的同时，还可以有效地保护内部网络。

实验 5-9 提供公网服务的内部服务器

实验 5-8 中通过配置 NAT 服务，实现内部用户都可以访问外部网络，外部网络无法访问内部网络。如果内部网络中有一台服务器，需要向外部提供网络服务，就需要配置端口映射，把对 NAT 外部 IP 某个端口的访问映射到内部某个 IP 地址的某个端口上。如需要从外部主机（虚拟机 2）Telnet（远程登录）到内部主机（虚拟机 1），操作步骤如下。

STEP 1 配置 Telnet 服务器。在虚拟机 1 上，依次单击“开始”→“程序”→“管理工具”→“服务”，打开服务控制台，找到“Telnet”服务项，更改服务的启动类型为“手动”，并启动该服务。

STEP 2 配置 NAT 服务器的端口映射。如图 5-7-6 所示，右键单击对外的接口，选择“属

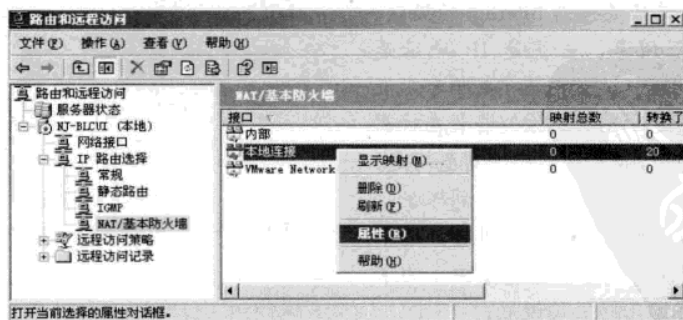


图 5-7-6 配置 NAT 对外接口

性”。在对外网卡的属性对话框，也就是“本地连接属性”对话框中，选择“服务和端口”选项卡，如图 5-7-7 所示，单击图中的“Telnet 服务器”。

在“编辑服务”对话框的“专用地址”栏中输入内部主机的 IP 地址 192.168.111.2。单击“确定”按钮，返回如图 5-7-7 所示的对话框，此时“Telnet 服务器”已经被选中。如果希望映射的服务和端口没有出现在图 5-7-7 中，可以单击图中的“添加”按钮，打开如图 5-7-8 所示的对话框进行添加。如在虚拟机 2 上既可以远程管理 NAT 服务器（真实机），又可以远程管理内部的主机（虚拟机 1），可只有一个 IP 地址，一个 3389 端口，这里可以借助 NAT 服务器的 3390（或任何未使用的 TCP 端口），把该端口映射到虚拟机 1 的 3389 上来。如图 5-7-8 所示，“服务描述”中随便填入一个直观的说明，如“自定义的远程桌面服务端口”；“传入端口”指的是外部主机访问的 NAT 服务器外部 IP 的端口号，这里填入 3390；“专用地址”栏中填入 192.168.111.2；“传出端口”指的是内部主机使用的端口，这里填入 3389（远程桌面的服务端口）。

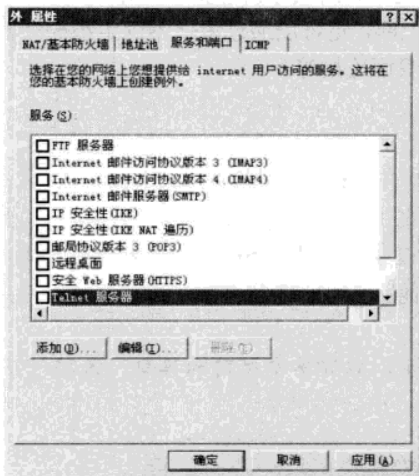


图 5-7-7 配置服务和端口

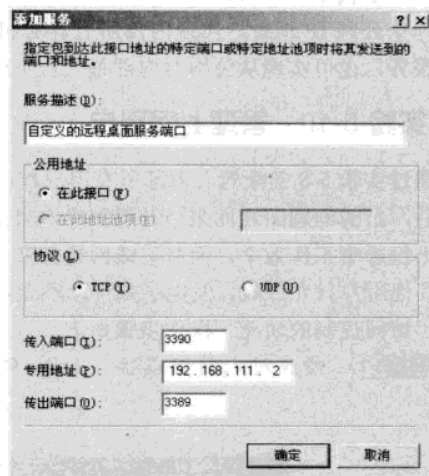


图 5-7-8 配置端口映射

单击“确定”按钮，返回如图 5-7-7 所示的对话框，其中的“Telnet 服务器”和新添加的“自定义的远程桌面服务端口”两项被选中，单击图 5-7-7 中的“确定”按钮，完成端口映射的配置。

STEP 3 测试 Telnet。在虚拟机 2 上打开 DOS 窗口，输入“telnet 192.168.1.200”，系统提示“您将要您的密码信息送到 Internet 区内的一台远程计算机上。这可能不安全。您还要送吗 (y/n):”，之所以出现这样的提示是出于安全考虑，因 Telnet 传送的是明文密码，很容易被截获。这里输入“y”继续，系统提示“login:”，输入 administrator，系统提示“password:”，输入管理员账户对应的密码。成功地登录到虚拟机 1 的 Telnet 服务器上，可以通过 DOS 命令远程管理虚拟机 1，很多用户对 DOS 的命令并不是很熟悉，接下来可通过远程桌面进行直观管理。

STEP 4 测试远程桌面。开启虚拟机 1 的远程桌面服务，在虚拟机 2 上启动远程桌面连接，填入“192.168.1.200:3390”，如图 5-7-9 所示，在 IP 地址的后面输入冒号和端口号。单击“连接”按钮，输入虚拟机 1 的管理员用户名和密码，在虚拟机 2 上成功地登录到内部主机虚拟机 1 上，

可以进行直观的操作。

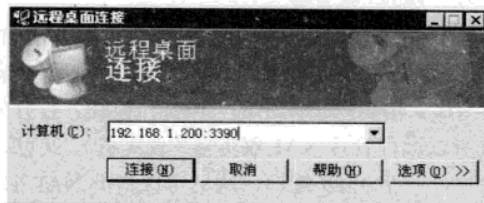


图 5-7-9 非默认端口的远程桌面连接

依照上面类似操作，用户还可以映射 TCP 的 3391 端口到内部主机 192.168.111.3 的 3389 端口，映射 TCP 的 3392 端口到内部主机 192.168.111.4 的 3389 端口等，这样就可以远程管理内部的每一台主机了。还可以把 80, 25, 110, 21 等服务端口分别映射到内部的主机上。这样就实现通过一个公网 IP 地址，实现内部所有计算机的共享上网，还可以通过内部不同主机向公网提供不同服务，也可实现从公网对内部每一台主机的远程桌面连接等。

实验 5-10 管理上网用户

通过实验 5-8 的配置，内部所有用户都可以自由访问 Internet。但这样还不算大功告成，网络开通后，新的问题随之而来。开通网络本来是为了提高工作效率，如果用来从事与工作无关的事情，不仅影响工作效率，而且造成网络拥塞，影响关键业务流量。因此可以设置除个别特权用户外，其他用户只允许收、发电子邮件，不允许使用其他服务。NAT 服务除了提供共享上网外，还集成了访问控制的功能。操作步骤如下。

STEP 1 修改对内接口属性。如图 5-7-10 所示，右键单击对内的接口，选择“属性”命令。

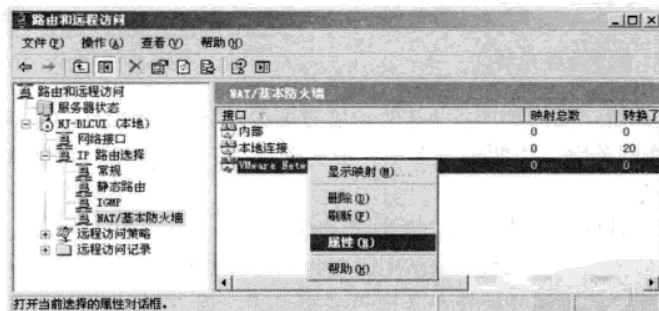


图 5-7-10 启用 NAT 服务的路由和远程访问

STEP 2 选择“入站筛选器”。在“VMware Network Adapter VMnet1 属性”对话框中，如图 5-7-11 所示，单击“入站筛选器”按钮，控制从内网进入代理服务器的通信流量。

STEP 3 编辑入站筛选器。在如图 5-7-12 所示的对话框中，单击“新建”按钮，编辑入站筛选器。

STEP 4 添加 IP 筛选器。如图 5-7-13 所示，在“添加 IP 筛选器”对话框中，可以对源网络、

目标网络 and 使用的协议进行过滤。

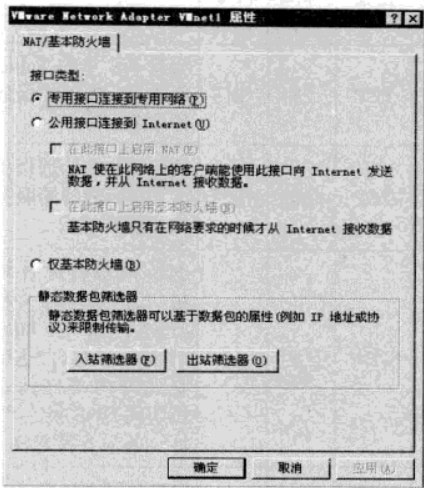


图 5-7-11 选择对内网卡的入站筛选

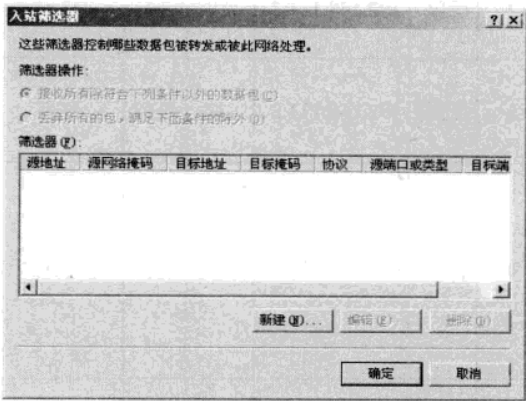


图 5-7-12 编辑入站筛选器

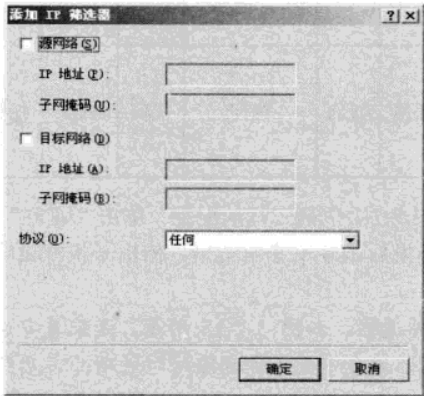


图 5-7-13 添加 IP 筛选器

表 5-7-1 列出了所需配置的条目，用户可以根据实际的需要进行配置，其中“任何”表示无需任何配置。

表 5-7-1 IP 筛选器配置

行号	源	IP 地址	掩码长度	目标	IP 地址	掩码长度	协议	源端口	目标端口	说 明
1	受限	192.168.111.8	/32	任何	任何	任何	任何	任何	任何	允许 192.168.111.8 这个 IP 地址访问任何目标地址，使用任何服务，如这个是主管使用的 IP 地址，可以添加多个

续表

行号	源	IP 地址	掩码长度	目标	IP 地址	掩码长度	协议	源端口	目标端口	说 明
2	受限	192.168.111.2	/32	任何	任何	任何	TCP	23	任何	实验 5-9 中的 Telnet 服务器, 内部的服务需要放开端口
3	受限	192.168.111.2	/32	任何	任何	任何	TCP	3389	任何	实验 5-9 中的远程桌面连接, 内部的服务需要放开端口
4	任何	任何	任何	受限	218.2.135.1	/32	UDP	任何	53	允许内部任何计算机访问主机 218.2.135.1 的 UDP 的 53 号端口, 也就是允许内部任何主机访问 DNS 服务器, 这一条最容易忽视
5	任何	任何	任何	任何	任何	任何	TCP	任何	25	SMTP 服务端口, 允许内部任何计算机使用外部任何服务器发送邮件
6	任何	任何	任何	任何	任何	任何	TCP	任何	110	POP3 服务端口, 允许内部任何计算机从外部任何服务器接收邮件

如图 5-7-14 所示是针对表 5-7-1 中第二行的配置, 单击“确定”按钮, 完成一个条目的添加。继续添加下一条。条目添加的先后顺序不影响结果, 但出于执行效率的考虑, 一般把使用频率最高的条目放置在最前面。

STEP 5 配置完成入站筛选器。如图 5-7-15 所示, 是配置完成后的入站筛选器, 尤其要注意, 选中的是“丢弃所有的包, 满足下面条件的除外”选项, 不然结果就恰好相反。

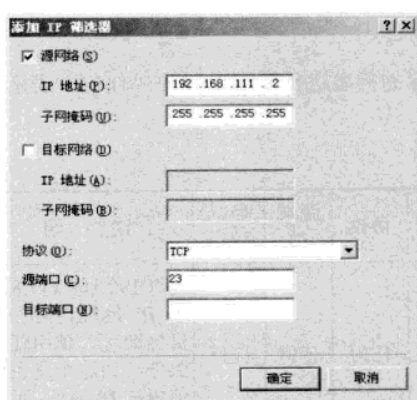


图 5-7-14 添加 IP 筛选器举例

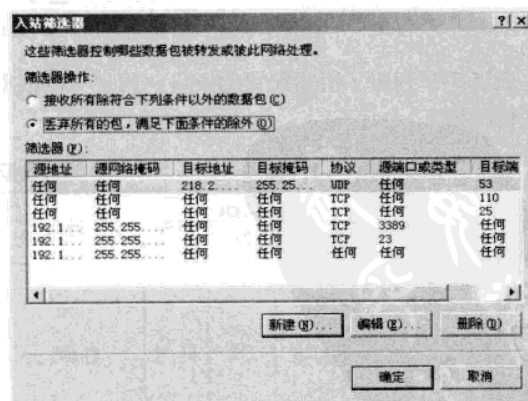


图 5-7-15 配置完的入站筛选器

STEP 6 测试。在虚拟机 1 上访问外部网站，如新浪网，则结果失败；在虚拟机 1 上配置 Outlook Express，可以正常收取公网邮件；虚拟机 2 远程桌面连接和 Telnet 登录虚拟机 1 均正常；把虚拟机 1 的 IP 地址改成 192.168.111.8，可以成功访问新浪网。

实验 5-11 VPN 服务器配置

员工出差到外地，如何安全地使用公司内部提供的服务；公司分部员工，如何安全地连接到公司总部网络，这些都需要配置 VPN 服务。这里假设虚拟机 2 是一个外网用户，虚拟机 1 是公司内网用户，配置真实机为 VPN 服务器，使虚拟机 2 可以安全地访问虚拟机 1，通过前面介绍的端口映射虽然也可以实现虚拟机 2 对虚拟机 1 的部分访问，但并没有提供安全保障，容易造成信息的泄漏。VPN 服务器的配置方法如下。

STEP 1 测试 NAT 配置。经过实验 5-8 的配置，可以实现虚拟机 1 访问 Internet；经过实验 5-9 的配置，可以实现虚拟机 2 访问虚拟机 1 的 Telnet 服务器和远程桌面连接；即使没有实验 5-10 的限制（可以禁用入站筛选），虚拟机 2 都无法 ping 通虚拟机 1。

STEP 2 禁用“路由和远程访问服务”。如图 5-7-1 所示，右键单击服务器名称，选择“禁用路由和远程访问”，系统提示要求确认操作，单击“是”按钮，禁用之前的所有配置。

STEP 3 重新配置“路由和远程访问服务”。按实验 5-8 的操作步骤，重新启用“路由和远程访问服务器安装向导”。在如图 5-7-3 所示的对话框中，选择“虚拟专用网络（VPN）访问和 NAT”。

STEP 4 选择连接外网接口。在如图 5-7-16 所示的“路由和远程访问服务器安装向导”中选择连接到外网的接口，并取消防火墙。单击“下一步”按钮继续。

STEP 5 指派 VPN 客户端可以访问的网络。指派远程 VPN 客户端可以使用的网络，如图 5-7-17 所示，选择 VMnet1 网卡。单击“下一步”按钮继续。

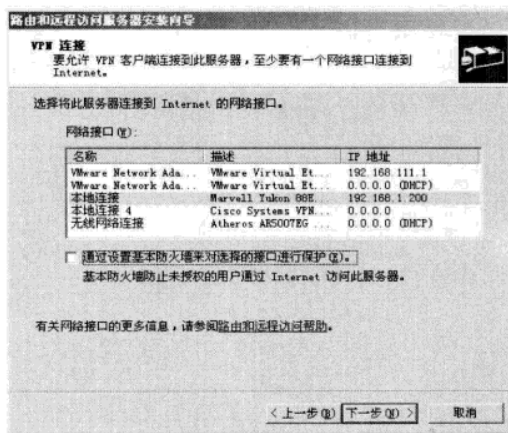


图 5-7-16 选择对外接口

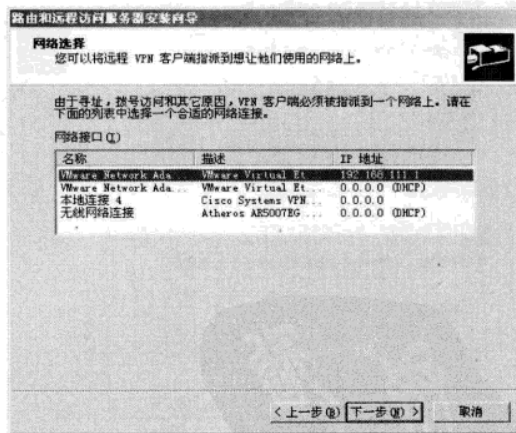


图 5-7-17 指派 VPN 客户端可以使用的网络

STEP 6 分配 VPN 客户端的 IP 地址。向导询问如何对远程 VPN 客户端分配 IP 地址，可以使用 DHCP，也可以使用一个指定的地址范围。这里选择“来自一个指定的地址范围”，如图 5-7-18 所示。

单击“下一步”按钮继续。打开“地址范围指定”对话框，单击“新建”按钮，打开“新建地址范围”对话框，如图 5-7-19 所示。输入 VPN 客户端的地址范围，这里随意填入一段没有使用的私有地址，如 192.168.100.100~192.168.100.200。单击“确定”按钮返回。

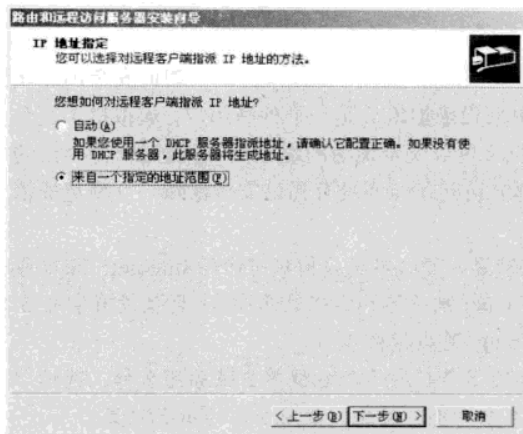


图 5-7-18 VPN 客户端地址分配方式

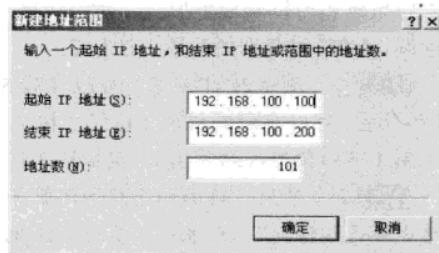


图 5-7-19 新建地址范围

STEP 7 选择 NAT 的对内接口。如图 5-7-20 所示，要求选择 NAT 的对内接口，选择 VMnet1 网卡。单击“下一步”按钮继续。

STEP 8 配置身份验证方式。如图 5-7-21 所示询问是否要采用 Radius 身份验证，保持默认的“否，使用路由和远程访问来对连接请求进行身份验证”选项。接下去的对话框中，单击“下一步”或“确定”按钮，完成“路由和远程服务器安装向导”。

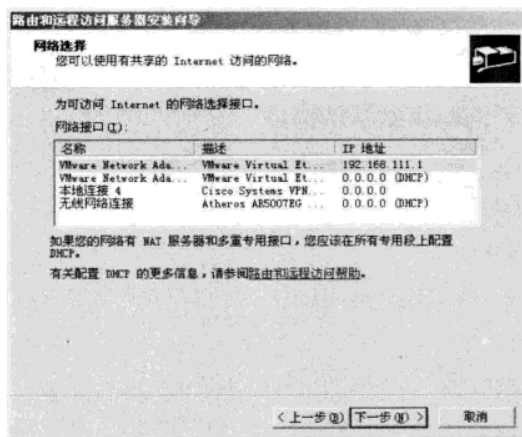


图 5-7-20 选择 NAT 的对内接口

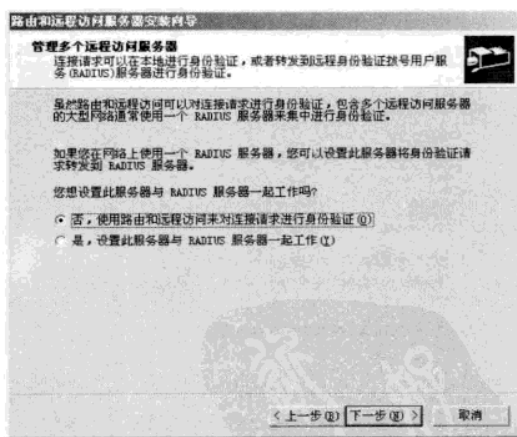


图 5-7-21 身份验证方式

STEP 9 添加 VPN 用户。在真实机中打开“计算机管理”窗口，添加一个用户“test”，并设置该用户的属性，如图 5-7-22 所示，选择“拨入”选项卡，选中“允许访问”；如果想为此用户分配固定的 IP 地址，可以选中“分配静态 IP 地址”选项，并填入预分配的 IP 地址，针对用户

的 IP 地址分配优先于 DHCP 或前面指定的地址范围。

STEP 10 VPN 客户端设置 (虚拟机 2)。在虚拟机 2 上右键单击“网上邻居”，选择“属性”命令，打开虚拟机 2 的“网络连接”窗口，如图 5-7-23 所示。

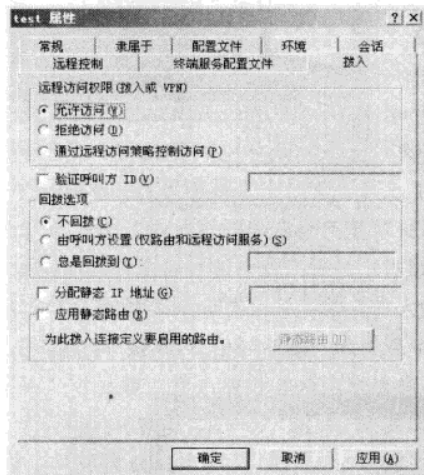


图 5-7-22 添加 VPN 用户

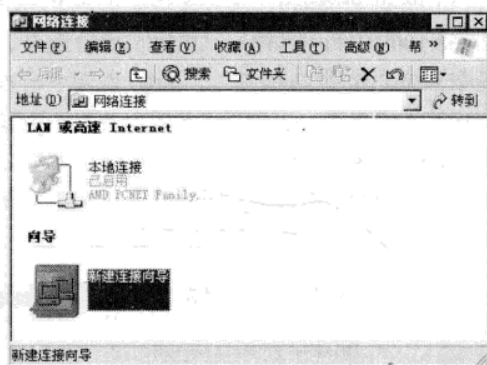


图 5-7-23 网络连接

双击“新建连接向导”图标，打开“新建连接向导”对话框，单击“下一步”按钮，打开“网络连接类型”选择对话框，如图 5-7-24 所示。

选择“连接到我的工作场所的网络”，单击“下一步”按钮，选择工作点如何与网络连接。如图 5-7-25 所示，选择“虚拟专用网络连接”。单击“下一步”按钮，连接名中输入一个名字，再单击“下一步”按钮，VPN 服务器的地址栏中填入 IP “192.168.1.200”，继续单击“下一步”按钮，完成“新建连接向导”。

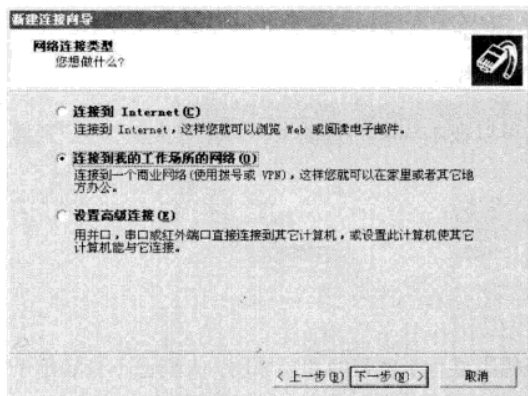


图 5-7-24 网络连接类型

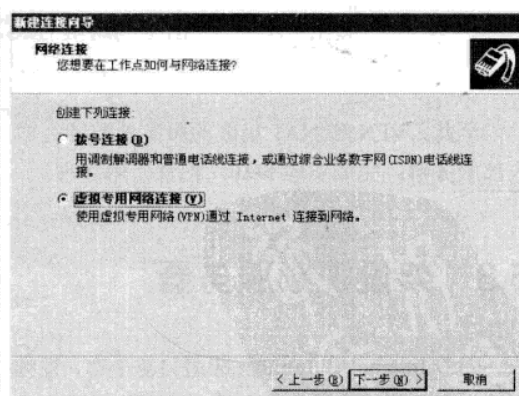


图 5-7-25 网络连接方式

STEP 11 VPN 连接。双击刚才新建的网络连接，打开如图 5-7-26 所示的窗口，填入用户名“test”和对应的密码后，单击“连接”按钮。弹出“连接到 192.168.1.200”对话框，提示“验证用户名和密码”→“正在网络上注册您的计算机”→“已连接”信息，对话框消失，任务栏上出

现一个新的网络连接图标。至此虚拟机 2 和真实机之间就建立了一个安全的私有通道, 数据流量被加密传输。如需断开 VPN 连接, 只需在网络连接图标上单击右键, 在快捷菜单中选“断开”命令即可断开 VPN 连接。

STEP 12 测试。VPN 连接成功后, 在虚拟机 2 (192.168.1.210) 上执行 ipconfig 可以发现新增一个 PPP (Point to Point Protocol, 点到点协议) 网卡, IP 地址是“192.168.100.101”, 掩码是“255.255.255.255”, 网关和 IP 地址相同。在虚拟机 2 上 ping 内网中的虚拟机 1 (192.168.111.2), 发现可以 ping 通, 如图 5-7-27 所示, 并可以进行远程桌面连接, 文件夹共享等操作。虚拟机 1 也可以通过访问 IP 地址“192.168.100.101”访问到虚拟机 2。

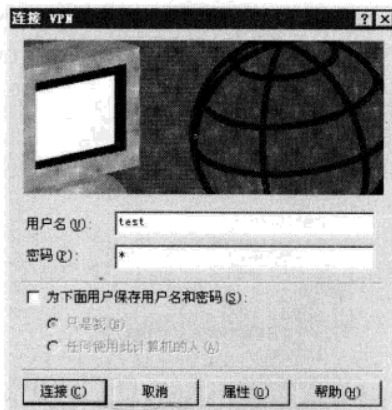


图 5-7-26 VPN 拨号窗口

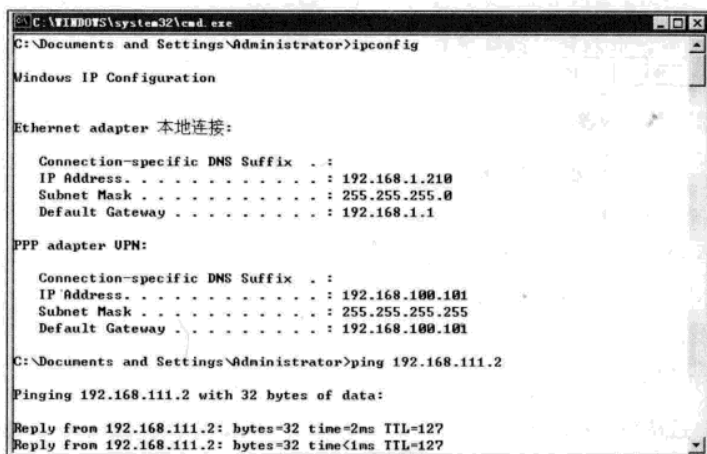


图 5-7-27 VPN 测试

至此, VPN 和 NAT 集成的服务器配置完成。可以在本实验的基础上, 再完成实验 5-9, 开通内部服务器; 完成实验 5-10, 配置上网管理。

5.8 架设视频服务器

随着 Internet 和 Intranet 应用日益丰富, 视频点播也盛行于宽带网和局域网。人们已不再满足于浏览文字和图片, 越来越多的人更喜欢在网上看电影、电视、听音乐。而视频点播和音频点播功能的实现, 需要依靠流媒体服务技术。目前, 流行的流媒体点播服务器有两种, 即 Windows Media 服务和 Real Server 服务。本节主要介绍在 Windows Server 2003 环境下视频点播、视频直播、电视直播等功能的实现。Windows Media 服务采用流媒体的方式来传输数据, 通常格式的多媒体文件必须完全下载到本地硬盘后, 才能够正常播放。而由于多媒体文件通常都比较大, 所以完全下载到本地

往往需要较长时间的等待。而流媒体格式文件只需先下载一部分在本地，然后可以一边下载一边播放。Windows Media 服务支持 ASF 和 WMV 格式的视频文件，以及 WMA 和 MP3 格式的音频文件。

5.8.1 安装 Windows Media 服务器

Windows Media 服务虽然是 Windows Server 2003 的组件之一，但是在默认情况下并没有安装，而是需要用户手动添加。在 Windows Server 2003 操作系统中，可以使用“添加/删除程序”来安装 Windows Media 服务，也可以通过“配置您的服务器向导”来安装。安装步骤如下。

STEP 1 在虚拟机 2 上，依次单击“开始”→“程序”→“管理工具”→“管理您的服务器”。单击窗口中的“添加或删除角色”超级链接，将显示“配置您的服务器向导”对话框。

STEP 2 单击“下一步”按钮，将显示“服务器角色”对话框，在“服务器角色”列表框中列出了所有可以安装的服务器。系统中大部分服务的安装和卸载都可以在该对话框中进行选择。

STEP 3 选择列表框中的“流式媒体服务器”选项，然后单击“下一步”按钮，将显示“选择总结”对话框，用来查看并确认所选择的选项。

STEP 4 单击“下一步”按钮，将显示“正在配置组件”对话框，并根据提示将 Windows Server 2003 安装光盘放入光驱。

STEP 5 放入安装光盘后单击“确定”按钮，系统开始从光盘中复制文件并安装 Windows Media 服务，并以进度条显示当前的安装进度。

STEP 6 安装完成后将显示安装完成对话框，表示已经成功地将此服务器设置为流式媒体服务器。

STEP 7 单击“完成”按钮关闭该向导，返回到“管理您的服务器”窗口，将显示流式媒体服务器已成功安装。

Windows Media 服务安装完成后，依次单击“开始”→“程序”→“管理工具”→“Windows Media Services”命令，显示 Windows Media Services 窗口，如图 5-8-1 所示。有关 Windows Media 服务的所有管理工作均可在该窗口中完成。窗口中介绍了关于流媒体的一些基础知识，有助于入门者对它进行了解。

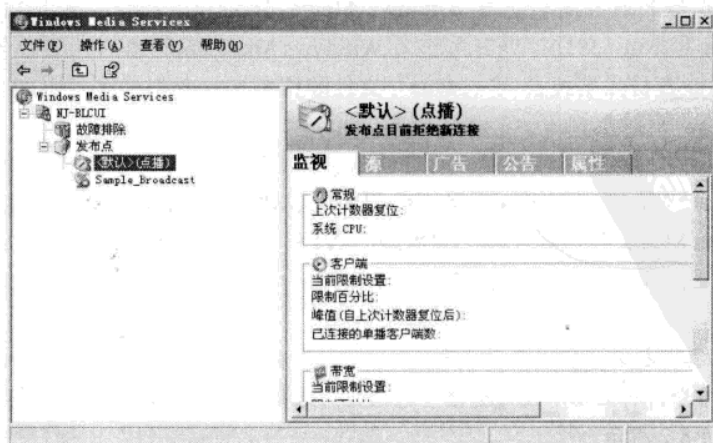


图 5-8-1 Windows Media Service 管理界面

5.8.2 安装 Windows Media 编码器

Windows Server 2003 中并没有 Windows Media 编码器, 下载的 network.rar 文件中包含了 Windows Media 编码器文件“WMEncoder_cn.exe”。需要注意的是, 编码器既可以安装在 Windows Media 服务器上, 同时也可以安装在其他计算机上。也就是说, 编码器只需安装在执行编码(即转换文件格式)工作的计算机上。

STEP 1 在真实机上, 双击 Windows Media 编码器安装文件“WMEncoder_cn.exe”, 将显示安装向导对话框, 在本安装向导中显示了可以安装的组件。

STEP 2 单击“下一步”按钮, 将显示“许可协议”对话框, 要求用户阅读最终用户许可协议, 单击“我接受许可协议中的条款”单选项。

STEP 3 单击“下一步”按钮, 显示“安装文件夹”对话框, 在“安装文件夹”文本框中显示了 Windows Media 编码器将要安装的路径。用户也可以键入其他的安装路径, 单击“浏览”按钮以选择其他的安装路径。

STEP 4 单击“下一步”按钮, 显示“准备安装”对话框, 可以开始安装 Windows Media 服务了。

STEP 5 单击“安装”按钮, 安装文件就会向硬盘中开始复制文件, 并进行 Windows Media 服务安装。在安装完成后就会显示安装完成对话框, 提示已经成功地完成 Windows Media 编码器 9 系列安装操作。

STEP 6 单击“完成”按钮以完成安装。

5.8.3 转换文件格式

视频点播服务一般需要发布流媒体文件。使用 Windows Media 编码器, 可以将文件扩展名为 wma、.wmv、.asf、.avi、.wav、.mpg、.mp3、.bmp 和 .jpg 等文件转换成为 Windows Media 服务使用的流文件。.asf、.wma 和 .wmv 文件扩展名代表标准的 Windows Media 文件格式。其中的 .asf 文件扩展名通常用于使用 Windows Media Tools 4.0 创建的基于 Microsoft Media 的内容。而 .wma 和 .wmv 文件扩展名是作为 Windows Media 编码器的标准命名约定引入的, 目的是使用户能够容易区别纯音频 (.wma) 文件和视频 (.wmv) 文件, 这 3 种扩展名可以交换使用。

转换文件格式的标准描述应当是“对存储信息源编码”, 也就是将保存在硬盘或光盘上的多媒体文件转换为 Windows Media 服务可使用的流媒体文件格式, 这个文件格式转换过程叫做编码。Windows Media 编码器可以将 MPG 和 AVI 格式的多媒体文件编码为 WMV 格式。下例是把真实机上的一个 AVI 格式文件转换成 Windows Media 服务器支持的 WMV 格式文件的操作步骤。

STEP 1 在真实机上, 依次单击“开始”→“所有程序”→“Windows Media”→“Windows Media 编码器”命令, 将显示“新建会话”对话框。选择其中的“转换文件”图标, 以准备转换视频文件, 如图 5-8-2 所示。

STEP 2 单击“确定”按钮, 将显示“新建会话向导”对话框。直接在“源文件”文本框中

键入要转换文件所在的文件夹和文件名，或者单击“浏览”按钮，以查找要转换的文件。默认状态下，输出文件与源文件均保存在同一文件夹，也可以重新指定保存的文件夹，如图 5-8-3 所示。

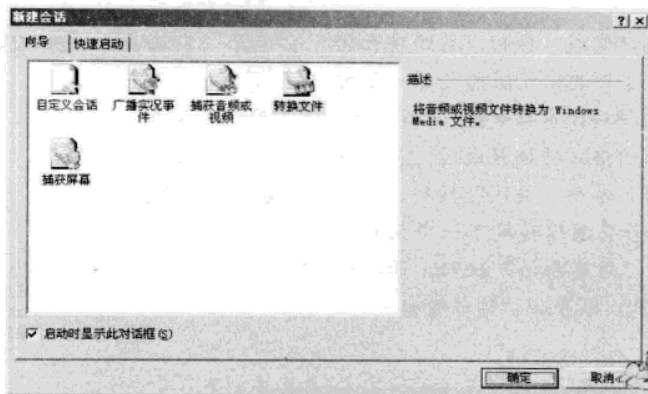


图 5-8-2 Media 编码器转换文件

STEP 3 单击“下一步”按钮，将显示“内容分发”对话框，以指定分发内容的方式。由于是为 Windows Media 服务制作节目，所以在这里应该要选择“Windows Media 服务器(流式处理)”选项，如图 5-8-4 所示。

STEP 4 单击“下一步”按钮，将显示“编码选项”对话框，如图 5-8-5 所示，在这里可以指定音频和视频编码方式。如果该视频文件只被用于局域网或宽带传输，可选择高质量的视频和音频，并指定较高帧速率，从而获得清晰的图像和逼真的声音。当然，此时所占用的网络带宽也偏高，文件存储空间也较大。在这里每选中一个比特率就会生成一个相应的 WMV 文件，因此通常情况下只需选中一个比特率即可。

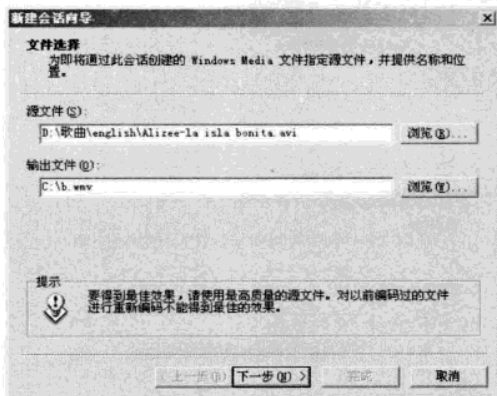


图 5-8-3 转换文件选择

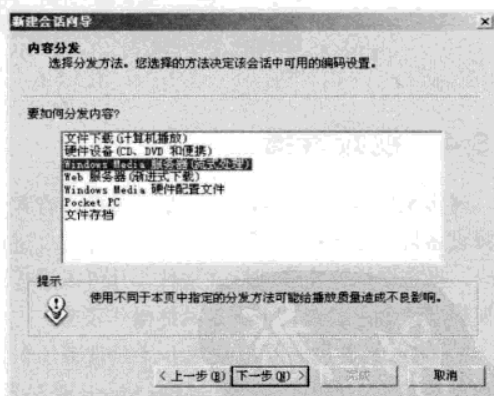


图 5-8-4 转换流式文件

STEP 5 单击“下一步”按钮，将显示“显示信息”对话框，分别在相应的文本框中键入该视频文件的相关信息，也可以不填写信息。

STEP 6 单击“下一步”按钮，将显示“设置检查”对话框，在这里可以显示并检查该视频

文件的相关信息。如果有任何错误，可以单击“上一步”按钮以返回至相关页面重新进行相关的设置。

STEP 7 单击“完成”按钮，系统将开始文件格式的转换。这个过程可能要花费一段时间，需耐心等待。文件转换窗口如图 5-8-6 所示。

STEP 8 文件的格式转换完成后，将显示“编码结果”对话框，单击“关闭”按钮，以结束格式转换过程。若要继续转换下一个视频文件，可单击其中的“新建会话”按钮。若要检查刚转换的视频文件，可单击“播放输出文件”按钮。

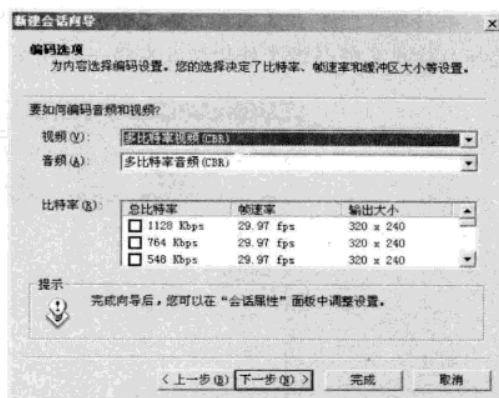


图 5-8-5 编码选项



图 5-8-6 文件转换窗口

5.8.4 视频直播

对实况信息源进行编码，就是指通过将音频或视频设备现场采集的音频、视频或图片等信息进行编码，将它们转换为流或流式文件，并可以进行网上视频和音频的直播，下面是具体操作步骤。

STEP 1 首先连接好视频和音频设备（如摄像头或麦克风），然后启动 Windows Media 编码器，在图 5-8-2 所示对话框上的“向导”选项卡中，选择“捕获音频或视频”图标，然后单击“确定”按钮，以运行“新建会话向导”对话框。首先显示“设备选项”对话框，在这里显示了用户可以使用视频和音频设备，如图 5-8-7 所示。

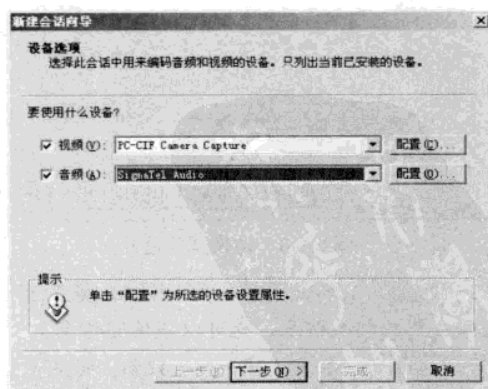


图 5-8-7 视频直播的设备选项

STEP 2 单击“下一步”按钮，将显示“输出文件”对话框，如果要将被创建的文件保存，需要在“文件名”文本框中键入保存路径，并自定义一个文件名，当然也可以单击“浏览”按钮来选择保存文件的文件夹。

STEP 3 单击“下一步”按钮，将显示“内容分发”对话框，在“要如何分发内容”列表框中列出可以使用的分发方式。由于是对实况源进行流式处理，所以在这里应该选择“Windows Media 服务器（流式处理）”选项。

STEP 4 单击“下一步”按钮，将显示“编码选项”对话框。在这里显示了所选择的分发方式的编码设置，其中包括视频、音频和比特率等。如果用户不想使用这些默认设置，也可以进行修改。

STEP 5 单击“下一步”按钮，将显示“显示信息”对话框。在这里可以为该编码文件添加显示信息，这些信息将在使用 Windows Media Player 时播放，并且启动字幕时才可以看到。

STEP 6 单击“下一步”按钮，将显示“设置检查”对话框。如果确认所进行的设置无误后，就可以单击“完成”按钮完成。在这里需要注意的是，如果选中“单击‘完成’后开始捕获”复选项，在单击“完成”按钮后会立即捕获信息并进行编码。否则不会立即进行捕获，因为还要进行视频直播，还需进行发布设置，这里不选中该复选框。

STEP 7 单击工具栏上的“属性”按钮，打开“会话属性”对话框，单击“输出”选项卡，如图 5-8-8 所示。选中“自编码器拉传递”复选框，并填入端口号，请事先确认该端口号没有被占用。

单击“应用”按钮，启用新设置，关闭该属性窗口。单击工具栏中的“开始编码”按钮，这时远程的收看者可以在 Media Player 中“打开 URL”，输入“mms://编码器计算机所用的 IP 地址:端口号”，这里在虚拟机 2 的 Media Player 中选择“打开 URL”，输入网址“mms://192.168.1.200:8080”即可看到真实机上的摄像头捕获到的视频画面。当“会话属性”设置完成后可以单击“文件”菜单中的“保存”子菜单以打开“另存为”对话框，将该流的配置信息进行保存，以便于以后再次使用或修改配置。

STEP 8 视频直播结束后，单击工具栏中的“停止”按钮，结束视频录制和直播，同时该视频还被以 WMV 的文件格式保存下来。

STEP 9 默认情况下，所有人都可以收看视频，如是机密视频，还需控制连接的客户端，不然就会泄密。单击“工具”菜单的“广播安全”命令，打开如图 5-8-9 所示的对话框。在对话框中添加允许

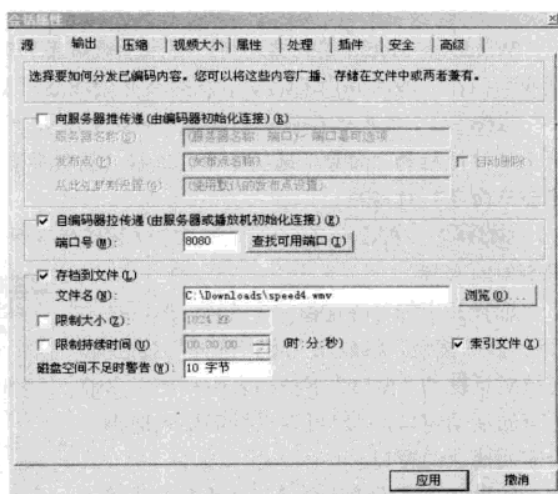


图 5-8-8 编码器的输出设置

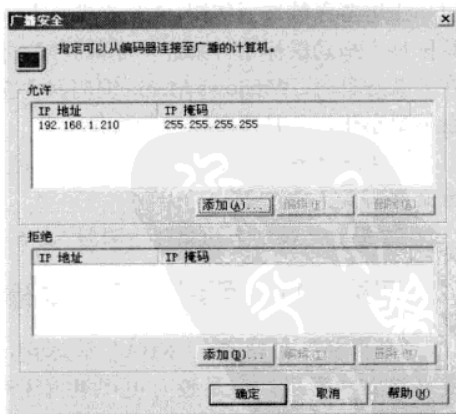


图 5-8-9 广播安全的设置

的 IP 地址, 除此 IP 地址之外的客户端将不能够连接到编码器。这里只添加虚拟机 2 的 IP 地址, 然后在真实机和虚拟机 2 上分别进行测试, 运行 Media Player 播放器, 选择“打开 URL”, 输入网址 “mms://192.168.1.200:8080”, 虚拟机 2 可以正常收看, 真实机则提示连接错误。

默认情况下, 在广播过程中编码器最多支持 5 个直接连接。通过在注册表中编辑项 HKEY_CLASSES_ROOT\Software\Microsoft\Windows Media Tools\Encoder\MaxClientConnections 编辑该子项, 使其反映出所需的直接连接最大数量, 可能的最大数量为 50。如所需连接的数量超过 50, 就需要使用 Windows Media Service, 将在接下来的“有线电视的网上直播”实验中进行演示。

5.8.5 实现网络教学

Windows Media 编码器还可以用来捕获屏幕和窗口, 并且还可以把屏幕或者屏幕中的特定区域或窗口在一段时间内的活动信息捕获并做成演示文件, 以供其他用户观看或下载。

STEP 1 首先连接好音频设备 (如麦克风), 然后启动 Windows Media 编码器, 在如图 5-8-2 所示的对话框的“向导”选项卡中, 选择“捕获屏幕”图标, 然后单击“确定”按钮, 以运行“新建会话向导”对话框。

STEP 2 在该对话框中列出了可以捕获的 3 种方式, 即特定窗口、屏幕区域和整个屏幕。如图 5-8-10 所示。

选择其中的“特定窗口”选项, 然后单击“下一步”按钮, 将显示“窗口选择”对话框。在该对话框的“窗口”下拉列表中列出了当前所有的活动窗口, 用户可以根据需要来选择需要一个需要捕获的窗口。

如果在“屏幕捕获会话”对话框中选择了“屏幕区域”选项, 单击“下一步”按钮后将显示“屏幕区域”对话框, 这时可以在坐标框中输入屏幕区域的位置。如果为了方便, 还可以单击屏幕区域选择按钮, 然后在要捕获的屏幕区域上拖动鼠标指针来选择屏幕区域。之后在捕获屏幕时, Windows Media 编码器主窗口会被最小化, 并且不会同时被捕获。

如果选择的是“整个屏幕”选项, 就会把整个屏幕的活动信息全部捕获下来, 并做成相应的流文件。

STEP 3 接下来的操作步骤同 5.8.4 小节所述。

实验 5-12 实现网上电视直播

“世界杯”足球赛、“NBA”篮球赛, 还有令人期待的“北京 2008”奥运会, 这些电视节目真是太精彩了, 但是没有电视机就无法收看这些节目, 尤其是各大高校, 计算机和网络的普及远远超过电视机和有线电视网的普及, 有时在网上找到一个提供电视直播的网址, 视频

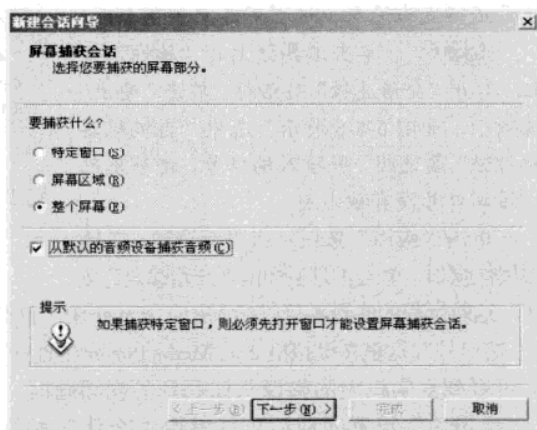


图 5-8-10 捕获屏幕设置

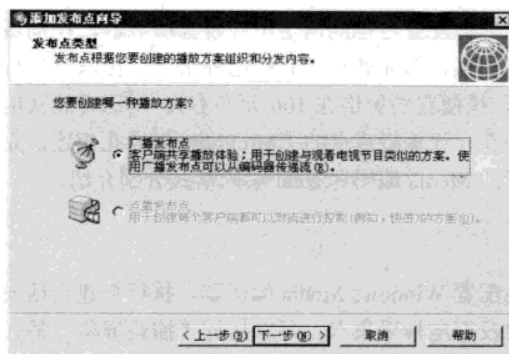


图 5-8-13 发布点类型选择

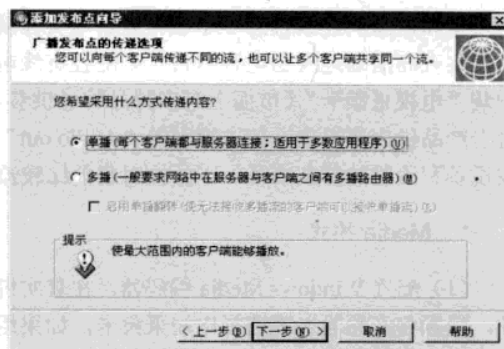


图 5-8-14 广播发布点的传递选项

STEP 7 单播日志记录。单击“下一步”按钮，发布点向导询问是否要使用日志，保持默认设置。

STEP 8 发布点摘要。单击“下一步”按钮，发布点向导显示发布点摘要信息，也保持默认，如图 5-8-16 所示。

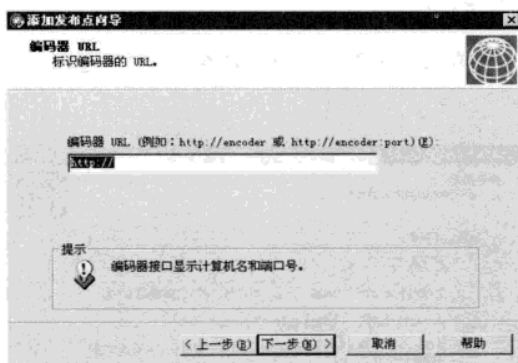


图 5-8-15 输入编码器 URL

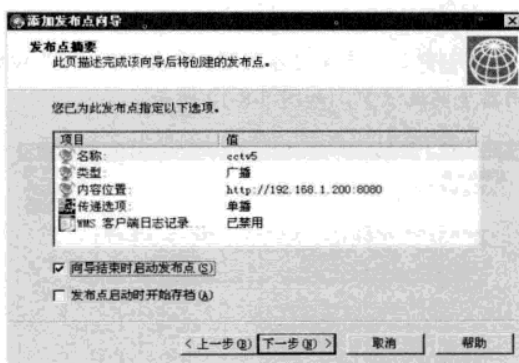


图 5-8-16 发布点摘要

STEP 9 完成。单击“下一步”按钮，完成“添加发布点向导”。如图 5-8-17 所示，根据需要选择是否要对外发布 Web 页面，这里不需要发布页面，取消“完成向导后”复选框。



图 5-8-17 完成发布点向导

STEP 10 使用 Windows Media Player 测试。在真实机上,运行 Windows Media Player,选择“打开 URL...”,输入“mms://192.168.1.210/cctv5”,如图 5-8-18 所示。此时可在 Media Player 看到电视节目。

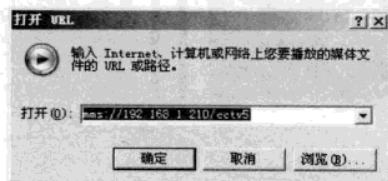


图 5-8-18 打开 URL

2. Real 格式

Real Networks 公司是网上流式音视频解决方案的提供商,提供从制作端、服务器端到客户端的所有产品。Real 格式具有很高的压缩比和很好的传输能力,适合在网络上进行信息发布。下面介绍发布 Real 格式电视直播节目的步骤。

STEP 1 安装 Real 服务器。安装 Real 服务器软件“Helix Server”V9.0 版,其功能和“Windows Media Services”类似,有关该软件的安装过程,这里不做介绍,这里记下服务端口号及用户名和密码。或者可以如图 5-8-19 所示进行操作。

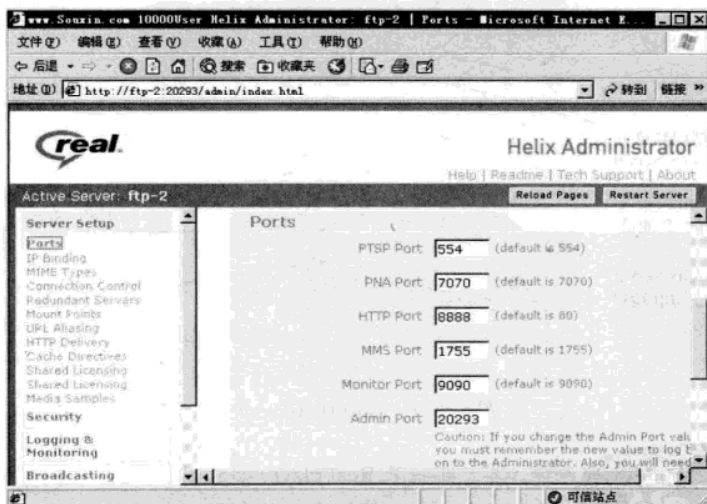


图 5-8-19 Helix Server 管理界面

STEP 2 安装和配置 Real Producer 软件。Real Producer 软件是由 Real 公司所出的 Real 格式文件制作工具,其功能和“Windows Media 编码器”类似,可将 WAV、MOV、AVI、AU、MPEG 文件压制成 Real 影音文件(.ra、.rm、.ram),以利于在网络上的传送和播放;也同样可以直接获取视频源,提供网络直播。该软件安装后的界面及功能按钮说明如图 5-8-20 所示。

单击如图 5-8-21 所示的“添加信号输出服务器”按钮,打开如图 5-8-20 所示的对话框。

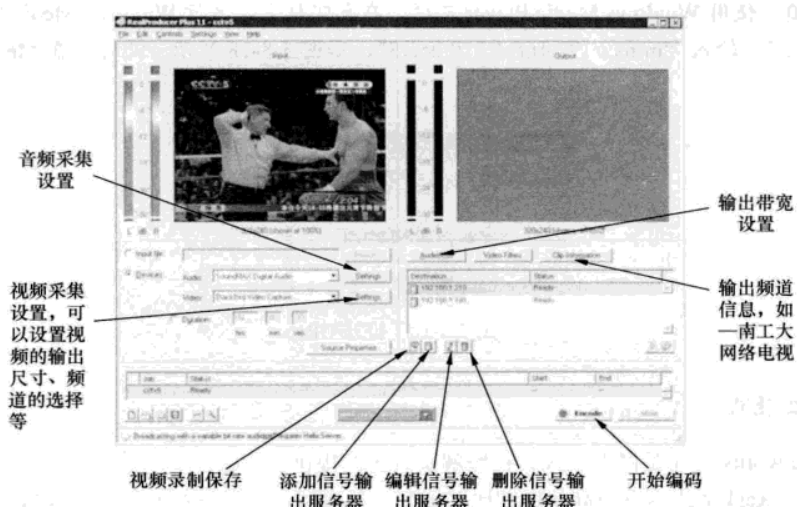


图 5-8-20 Real Produce 管理界面

如图 5-8-21 所示，填入对应信息，按“OK”按钮保存。继续操作，添加多台 Helix Server。然后单击图中的“Encode”按钮，开始编码。

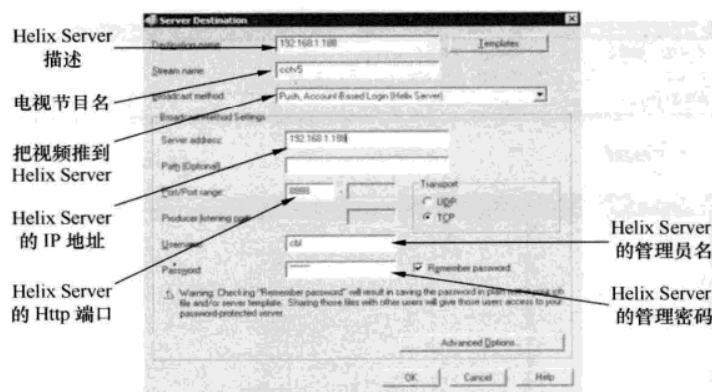


图 5-8-21 添加 Helix Server

STEP 3 Real player 中测试。客户端安装 Real player 播放器，单击“文件”→“打开”命令，输入“rtsp://real server 的 IP 地址/broadcast/cctv5”，即可收看网上直播。

5.9 证书服务

现在网络欺诈事件层出不穷，假的电子商务、假的网上银行、假的电子邮件，每年造成的损失难以估计，这种欺诈行为让广大用户对网上交易产生怀疑，甚至拒绝所有与网络相关的电子商

务。实际上,通过使用数字证书,很多损失都可以避免。作为一种比较成熟的安全产品,数字证书已经发展到一个较高的技术水平,而且它将在我们的网络生活中发挥越来越重要的作用。那么,数字证书能做什么呢?它和网络安全到底有什么关系呢?如何使用数字证书来进行一些具体的操作呢?本节将针对数字证书的具体应用,如利用数字证书对邮件进行签名、加密等,让读者对数字证书的使用有一个比较全面和直观的认识。

5.9.1 数字证书

数字证书称为数字标识(Digital Certificate,也称 Digital ID)。它提供了一种在 Internet 上身份验证的方式,是用来标志和证明网络通信双方身份的数字信息文件,与司机驾照或日常生活中的身份证相似。数字证书是由一个由权威机构即 CA 机构,又称为证书授权(Certificate Authority)中心发行的,人们可以在交往中用它来识别对方的身份。在网上进行电子商务活动时,交易双方需要使用数字证书来表明自己的身份,并使用数字证书来进行相关交易操作。通俗地讲,数字证书就是个人或单位在 Internet 上的身份证。

数字证书是一个经证书授权中心数字签名的包含公开密钥拥有者信息以及公开密钥的文件。最简单的证书包含一个公开密钥、名称以及证书授权中心的数字签名。一般情况下证书中还包括密钥的有效时间、发证机关(证书授权中心)的名称、该证书的序列号等信息,证书的格式遵循相关国际标准。如图 5-9-1 所示是一个数字证书在网络应用中的原理图。

为什么需要数字证书呢?由于 Internet 上电子商务技术使得网上购物的顾客能够极其方便轻松地获得商家和企业的信息,但同时也增加了对某些敏感和有价值的数据被滥用的风险。因而网络电子商务系统必须保证具有十分可靠的安全保密技术,也就是说,必须保证网络安全的四大要素,即信息传输的保密性、数据交换的完整性、发送信息的不可否认性、交易者身份的确定性。

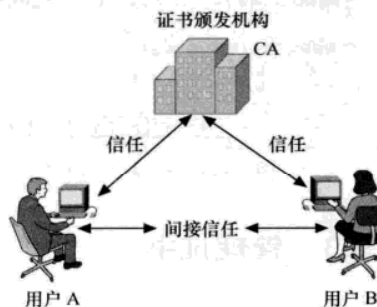


图 5-9-1 数字证书应用原理

5.9.2 安装证书服务

证书服务器的成功标准在于用户是否信任证书中的信息的有效性。因此,证书通常是通过一个互相信任的第三方组织来建立的,它被称为 Certificate Authority (CA)。CA 的主要职责是确认该组织注册到了一个证书,这样就可以确保证书中的标识信息的有效性。本节以 Windows Server 2003 的证书服务为例,介绍证书服务的安装和使用。Windows Server 2003 默认不安装证书服务,用户需添加此项服务。

STEP 1 在虚拟机 2 上单击“控制面板”→“添加或删除程序”→“Windows 组件向导”选项,选中“证书服务”选项后会弹出确认框,提醒安装证书后,计算机名和域成员身份都不能更改,如图 5-9-2 所示,单击“是”按钮,确认安装,再单击“下一步”按钮。

STEP 2 “Windows 组件向导”询问 CA 类型,如图 5-9-3 所示,这里选择“独立根 CA”。要安装企业 CA,需要 AD (Active Directory,活动目录),这里没有 AD 存在,因此前两项不可选。

STEP 3 接着单击“下一步”按钮,输入 CA 识别信息,如图 5-9-4 所示,填入此 CA 的公用名称。单击“下一步”按钮继续,打开“证书数据库设置”对话框,直接单击“下一步”按钮继续。系统提示要完成证书服务的安装,需要临时停止 IIS 服务,单击“是”按钮,确认停止 IIS 服务,完成证书服务的安装。

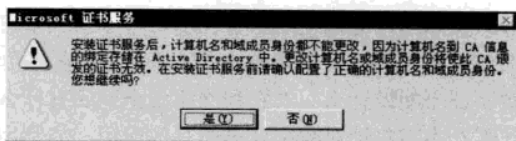


图 5-9-2 安装证书服务

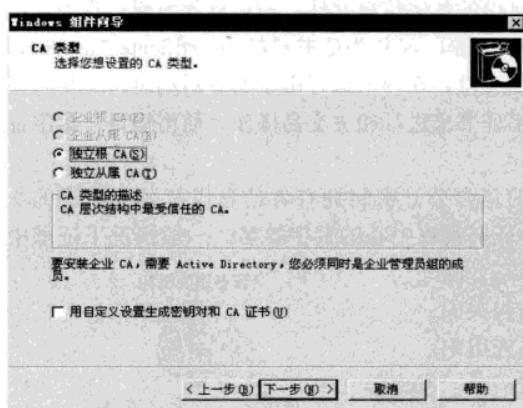


图 5-9-3 选择 CA 的类型

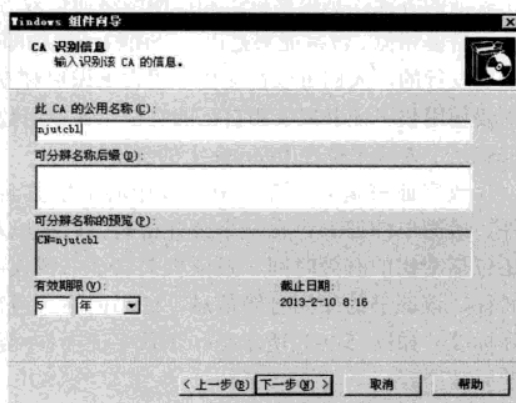


图 5-9-4 CA 识别信息设置

5.9.3 管理证书

1. 查看证书服务

打开 IIS 管理器,如图 5-9-5 所示,可以看到默认网站下有一个“CertSrv”的虚拟目录,客户端可以访问“http://www.sales.test.com/certsrv”地址,在线申请证书。

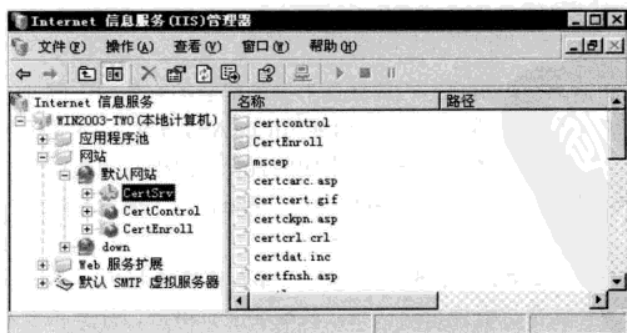


图 5-9-5 证书服务的虚拟目录

2. 申请证书服务

在真实机上访问“<http://www.sales.test.com/certsrv>”，可以打开如图 5-9-6 所示的窗口。如果不能正常显示页面内容，请检查虚拟机 2 上的 DNS 配置中有没有 www 主机记录，检查虚拟机 2 上虚拟主机部分配置是否正确，也就是检查 5.4.3 小节的操作是否正确；检查 DNS 委派实验（实验 5-4）是否正确；检查真实机 TCP/IP 属性中 DNS 是否指向 192.168.1.200，如果指向的是公网 DNS 服务器 218.2.135.1 是无法完成解析工作的。也可以取消虚拟机 2 默认网站的主机头，在图 5-4-14 所示的页面中删除“主机头值”，然后通过“<http://192.168.1.210/certsrv>”访问证书服务器。

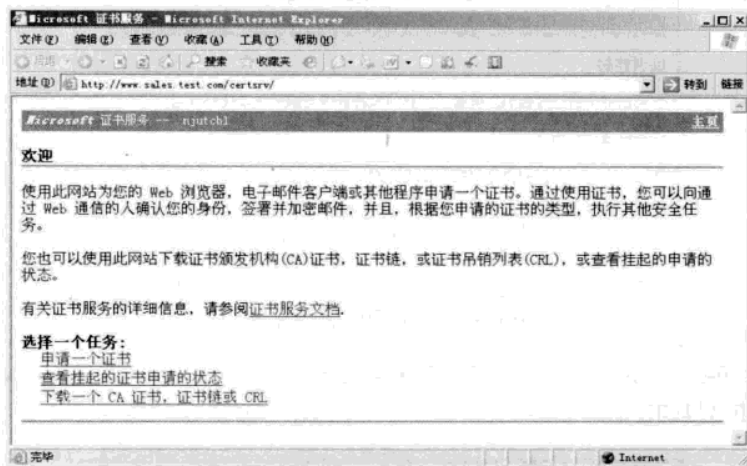


图 5-9-6 访问证书服务器

在真实机上单击如图 5-9-6 所示的“申请一个证书”超级链接，打开如图 5-9-7 所示的窗口，要求选择证书的类型，并单击“电子邮件保护证书”。

打开电子邮件保护证书申请表格，填写如图 5-9-8 所示的内容，这里填写的是用户信息，其



图 5-9-7 选择证书类型



图 5-9-8 电子邮件证书申请表

中电子邮件一栏一定要填写要使用证书的电子邮件的地址。因为真实机的 Outlook Express 中配置的邮件账户是 user2@test.com, 所以这里电子邮件地址中填入 user2@test.com。填写完后, 单击“提交”按钮, 提交证书申请。系统会提示“潜在的脚本冲突”, 不用理会, 单击“是”按钮发送请求。

证书提交后, 页面如图 5-9-9 所示。证书服务器的反馈信息证明证书申请已经收到, 但必须等待管理员颁发后才可安装。同时显示这次申请的 ID 是“2”。

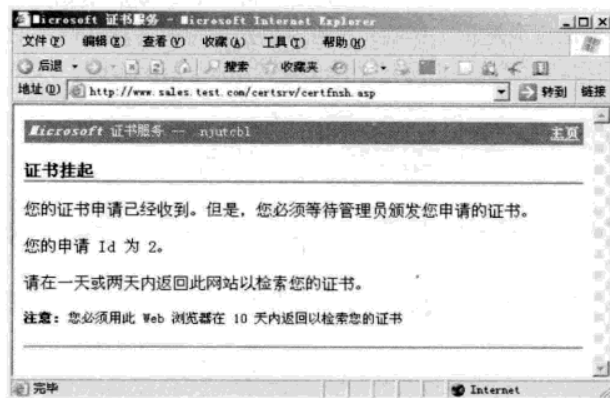


图 5-9-9 证书申请成功提交

单击如图 5-9-6 所示的“查看挂起的证书申请的状态”超链接, 打开如图 5-9-10 所示的窗口, 可以看到已经申请过的证书。

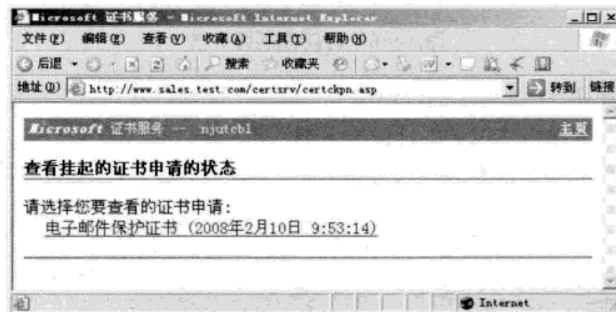


图 5-9-10 查看挂起的证书申请状态

单击该证书, 打开如图 5-9-11 所示的窗口。提示该证书仍然被挂起, 继续等待或催促证书服务器管理员, 并告之申请 ID 为 2。

到证书服务器上颁发这个申请。证书颁发后, 再次单击如图 5-9-10 所示的“查看挂起的证书申请的状态”超链接, 打开如图 5-9-12 所示的窗口, 可以看到证书已被颁发, 单击“安装此证书”。

系统会提示“潜在的脚本冲突”, 如图 5-9-13 所示, 不用理会, 单击“是”按钮。

系统弹出“安全性警告”, 如图 5-9-14 所示, 提醒用户安装电子邮件保护证书的同时, 还将安装证书服务器的根证书, 安装证书服务器的根证书后, Windows 将自动信任所有该证书服务器颁发的证书。同一个根证书在同一台计算机上只需安装一次, 以后在真实机再向虚拟机 2 申请并

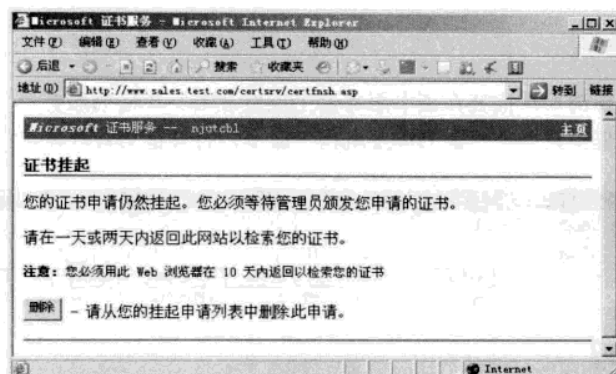


图 5-9-11 仍然被挂起的证书

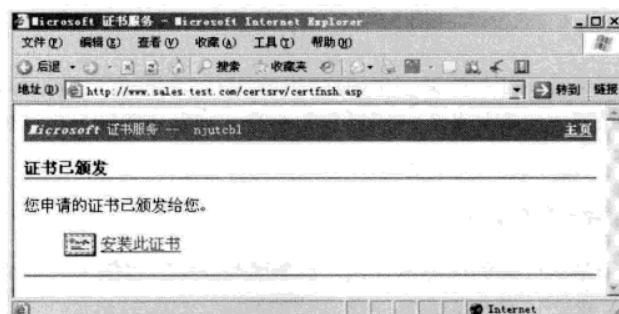


图 5-9-12 已获颁发的证书

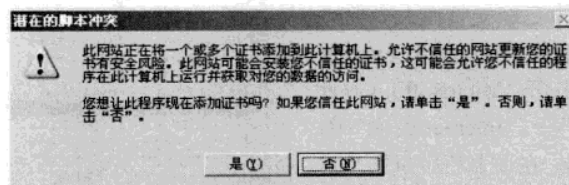


图 5-9-13 脚本冲突提示

安装任何证书时，都不会再出现如图 5-9-14 所示的“安全性警告”。单击“是”按钮，安装电子邮件保护证书和证书服务器的根证书。

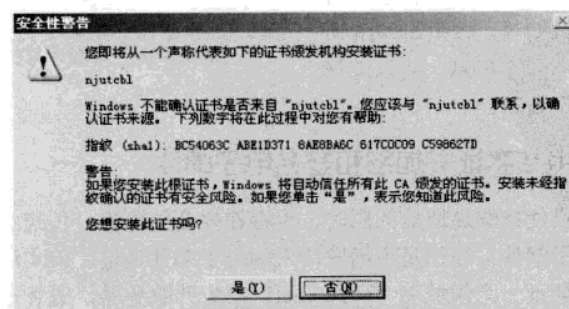


图 5-9-14 安全性警告

3. 管理证书服务器

客户端提交证书申请后，需要在证书服务器上颁发证书。在证书服务器（虚拟机 2）上依次单击“开始”→“管理工具”→“证书颁发机构”命令，打开证书管理器，如图 5-9-15 所示。

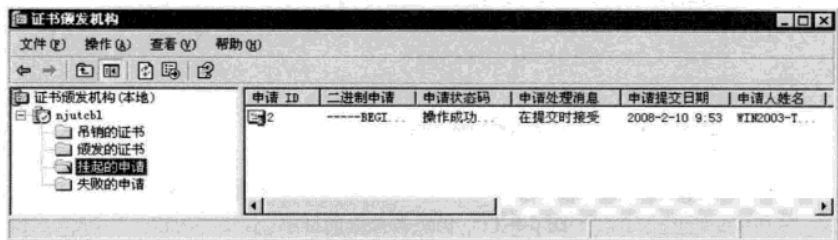


图 5-9-15 证书管理器

可以在挂起的申请中看到挂起的证书申请，“申请 ID”值是 2，可以用来和用户进行确认。右键单击这个申请，选择“所有任务”→“颁发”命令，颁发后的证书被移到图中的“颁发的证书”目录中。

4. 查看客户端已经安装的证书

客户端要认证一个带有证书的服务器（该证书由某个特别的 CA 建立），客户需要验证该 CA 处于 Web 浏览器的可信 CA 的列表中。大部分常见的 CA 根证书已经安装在大多数的 Web 浏览器中。要查看 Microsoft Internet Explorer 6 信任的 CA，打开“Microsoft Internet Explorer”，选择“工具”→“Internet 选项”命令，单击“内容”选项卡，在证书栏中单击“证书”按钮。打开“证书”对话框，证书管理对话框中的几个标签包含了这个 Internet Explorer 复制所知道的全部证书列表。每个证书都包含有“颁发者”和“颁发给”信息，包括它的有效性、开始日期和有效日期等，如图 5-9-16 所示。要查看一个数字证书中的信息，可以选择一个证书然后按“查看”按钮。

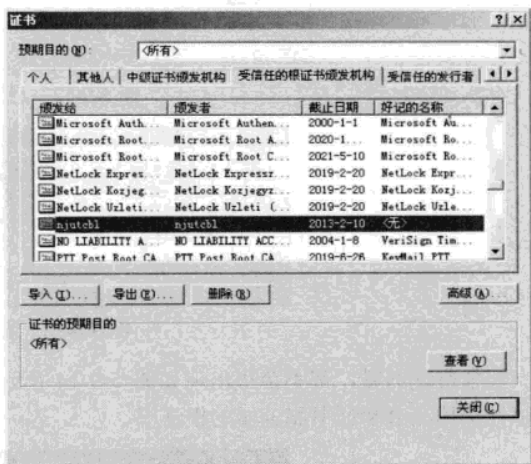


图 5-9-16 查看计算机中已安装的证书

实验 5-13 使用数字证书加密和签名电子邮件

电子邮件给人们提供便捷快速通信的同时，也存在安全的隐患。传统的书信，可以通过笔迹来识别真伪，但对于电子邮件，往往是根据发信人的电子邮件地址。但实际中冒充别人电子邮件地址又是如此方便，如架设一个假域名“@263.net”的邮件服务器，或者通过邮件组件，把发信人的地址填成想冒充的电子邮件地址。举一个简单的例子，如 user1 和 user2 正在恋爱，但两人相

处异地，经常是邮件传情，user3 也是 user1 的追求者，也知道 user1 的电子邮件地址，为了心中所爱，user3 冒充 user2 的电子邮件给 user1 发了封绝交邮件，引起 user1 和 user2 间的误会。user1 如能及时识别 user2 的身份就可以避免误会的发生，这就要求使用安全的电子邮件进行通信，也就是在电子邮件中使用证书。安全电子邮件证书中包含证书持有者的电子邮件地址、公钥及 CA 中心的签名。使用安全电子邮件证书可以收发加密和数字签名邮件，保证电子邮件传输中的机密性、完整性和不可否认性，确保电子邮件通信各方身份的真实性。证书可以存贮在硬盘或 U 盘中。安全电子邮件利用公钥算法保证用户签名的邮件不会被篡改，而加密的邮件除了邮件接收者以外的任何人均无法阅读其中的内容。需要注意的是，证书中的邮件地址必须同绑定的邮件账号一致。这样 user1 和 user2 就可以对自己的邮件进行签名和加密了。本实验在真实机上的 user2@test.com 和虚拟机 1 上的 user1@test.com 间完成，操作步骤如下。

STEP 1 修改虚拟机 1 的 TCP/IP 属性。把虚拟机 1 的网卡设置为 Bridged，IP 地址设置为 192.168.1.220，掩码为 255.255.255.0，网关为 192.168.1.1，DNS 为 192.168.1.200。

STEP 2 申请电子邮件保护证书。真实机上的 user@test.com 已经申请过，接下来在虚拟机 1 上为 user1@test.com 账户申请电子邮件保护证书，操作步骤与真实机的操作步骤类似，详见 5.9.3 小节。

STEP 3 在 Outlook Express 中配置电子邮箱与数字证书绑定。在真实机的 Outlook Express 中单击“工具”→“账户”命令，在“Internet 账户”对话框中，单击“邮件”选项卡，选中“mail.test.com”，再单击“属性”按钮，打开“mail.test.com 属性”窗口，单击“安全”选项卡，如图 5-9-17 所示。

单击签署证书下的“选择”按钮，打开图 5-9-18 所示的对话框，单击“确定”按钮返回，再单击如图 5-9-17 所示的加密首选项下的“选择”按钮，打开如图 5-9-18 所示的对话框，单击“确定”按钮返回。当使用电子邮箱 user2@test.com 对外发送电子邮件时，可以选择是否使用 user2 证书对发送出去的电子邮件进行签名或加密。

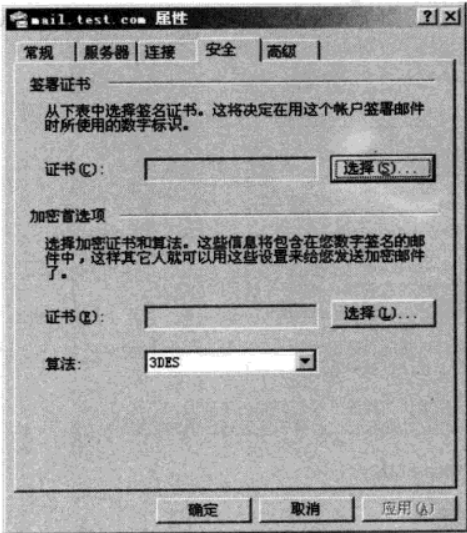


图 5-9-17 邮箱安全属性

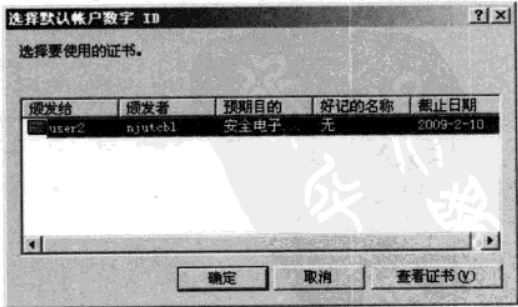


图 5-9-18 选择账户对应的证书

注意



如果单击“选择”按钮，没有显示相关的证书，请确认证书是否已经正确安装且没有过期。同时要确认在 Outlook Express 中所设置的邮箱与在申请数字证书时所提供的邮箱一致。

按照同样的方法，在虚拟机 1 上完成 user1@test.com 与数字证书的绑定。

STEP 4 发送有签名的电子邮件。在真实机上启动 Outlook Express，单击“创建邮件”，撰写新邮件，收件人栏中填入“user1@test.com”，同时选中“工具”栏中的“数字签名”选项，如图 5-9-19 所示。单击“发送”按钮，签名邮件发送成功。

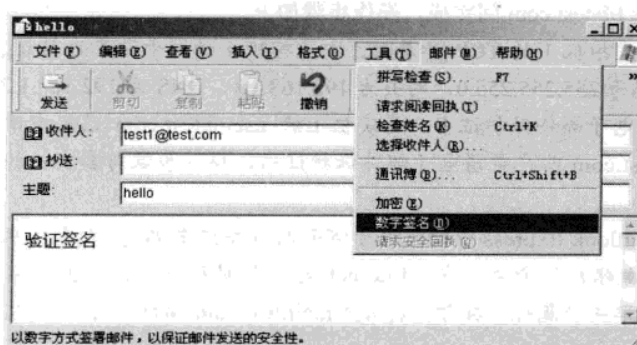


图 5-9-19 发送有数字签名的电子邮件

STEP 5 接收有签名的电子邮件。在虚拟机 1 接收邮件，Outlook Express 提示有一封新邮件，并提示该封邮件有数字签名，在右下角窗口中可以看到数字签名邮件的提示信息，如图 5-9-20 所示。

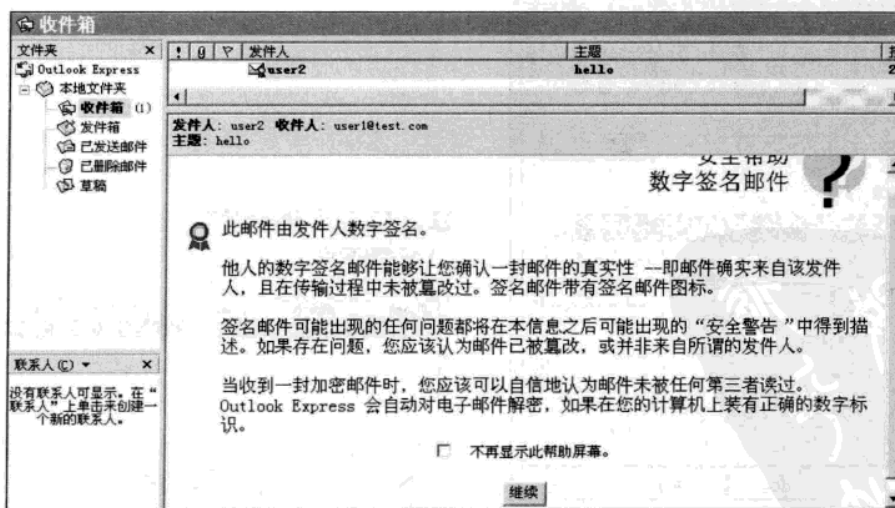


图 5-9-20 接收有数字签名的电子邮件

单击“继续”按钮后，如果邮件接收者信任该签名电子邮件的发证机构（CA），则可以正常浏览邮件内容，如图 5-9-21 所示。

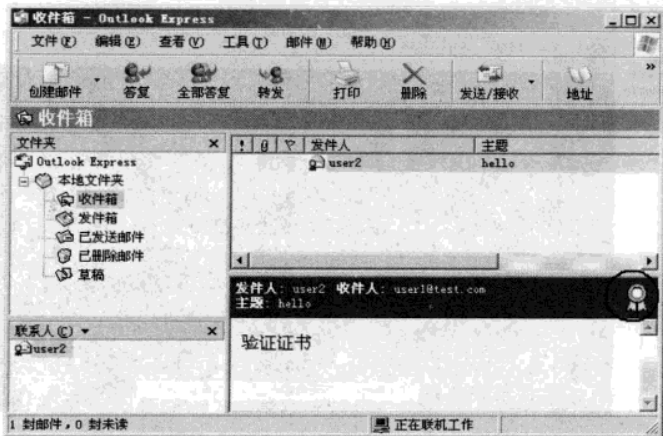


图 5-9-21 签名数字标识属性

可进一步查看该邮件发送者的信息，单击如图 5-9-21 所示的“数字签名”图标，打开邮件的“安全”选项卡，如图 5-9-22 所示，单击“查看证书”按钮，可以打开“查看证书”对话框，进一步查看“发件人证书”。

如果邮件接收者不信任该签名电子邮件的发证机构（CA），会发生什么情况呢？同样有签名的邮件，在真实机上再发一封。在局域网内找一台没有安装数字证书的计算机，如果真实机的硬件配置足够，也可以在真实机中使用虚拟机 3 来测试，配置第 4 台计算机的 TCP/IP 属性，IP 地址为 192.168.1.100，掩码为 255.255.255.0，网关为 192.168.1.1，DNS 为 192.168.1.200，配置 Outlook Express，添加邮箱 user1@test.com。

第 4 台计算机上也可以看到如图 5-9-20 所示的界面按钮后，单击“继续”按钮后，则打开如图 5-9-23 所示的窗口。如果接收到一封使用签名的电子邮件，而签署该电子邮件的 CA 不被接收计算机所信任，或发送的邮件被篡改过，都会出现“安全警告”提示。

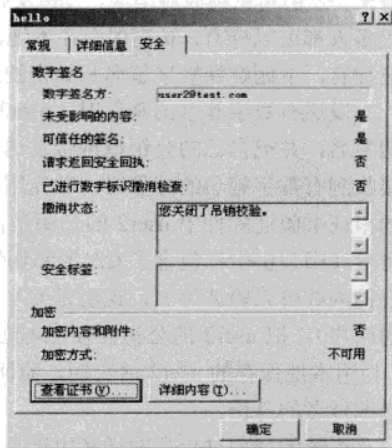


图 5-9-22 查看邮件证书

STEP 6 发送加密的电子邮件。单击如图 5-9-23 所示的“打开邮件”按钮，也可以看到如图 5-9-21 所示类似界面，可以正常查看邮件内容。这时可能会产生疑问，不是使用数字签名了吗，怎么没有安装证书的计算机还可以查看邮件的内容？这一点都不奇怪，因数字签名能做到信息的完整性（即不被篡改）和身份验证（即验证发送者），但无法保证机密，也就是说即使做了签名，信息本身并没有被加密，截获者一样可以浏览其中的内容。如果想做到保密，就要使用加密功能，发送加密邮件的方法与发送签名邮件的方法类似，发送邮件时选择“加密”命令，如图 5-9-19 所示。收取电子邮件实际上就是一个解密的过程，算法已经隐藏在后台运行了。值得注意的是发送

加密邮件前必须先获得接收方的数字标识, 不然会出现如图 5-9-24 所示的错误提示信息。

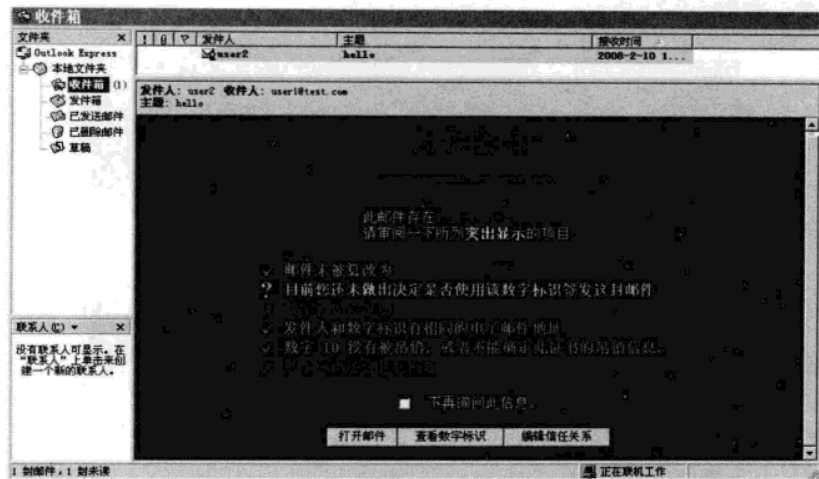


图 5-9-23 签名数字证书不被信任

出错的原因在于数字证书分为公钥和私钥, 公钥用于验证数字签名和加密, 私钥用于签署数字签名和解密。公钥和私钥成对出现, 公钥发布到 Internet 中, 很多人可以持有; 私钥保存在本地, 仅合法用户自己拥有。下面解释数字签名和加密的过程。

发送有数字签名的邮件时, user2 使用自己的私钥签名, 并把自己的公钥也携带发送出去。虚拟机 1 接收到有数字签名的邮件时, 首先用本地保存的 CA 的根证书验证邮件中 user2 的公钥是否可信, 经验证可信 (因公钥中都包含了 CA 的私钥签名, 用 CA 的公钥刚好可以验证签名, 说明是 CA 信任的用户。证书服务中, 所有用户都信任 CA 和 CA 信任的用户), 把 user2 的公钥保存在本地。同时也收到了 user2 发过来的有数字签名的邮件, 虚拟机 1 使用本地保存的 user2 的公钥, 验证使用 user2 的私钥签名的数字证书, 证明邮件的完整性和发送邮件者的身份。

加密的处理过程是发送者用接收者的公钥进行加密, 接收者用自己的私钥刚好可以解密, 即使邮件被非法截获, 但因非法者没有邮件接收者的私钥, 无法解密邮件, 信息不会泄漏。

根据数字签名和加密的过程, 解决上面错误提示的方法就是发送者可以首先让接收方给自己发一份签名邮件来获取对方的数字标识, 或者直接到电子商务安全认证中心的站点上面去查询下载来获取对方的数字标识。也就是虚拟机 1 上 user1@test.com 先给真实机上的 user2@test.com 发送一封有数字签名的邮件, 让真实机上具有 user1@test.com 的公钥, 就可以完成加密了。

STEP 7 接收加密的电子邮件。在虚拟机 1 上可以正常浏览被加密的邮件, 如图 5-9-25 所示。

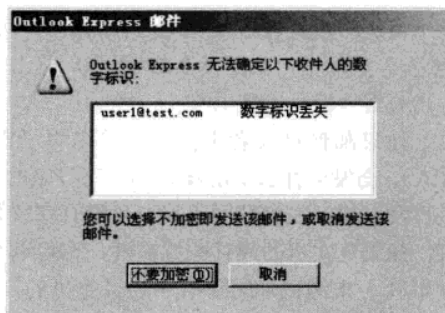


图 5-9-24 发送加密邮件失败

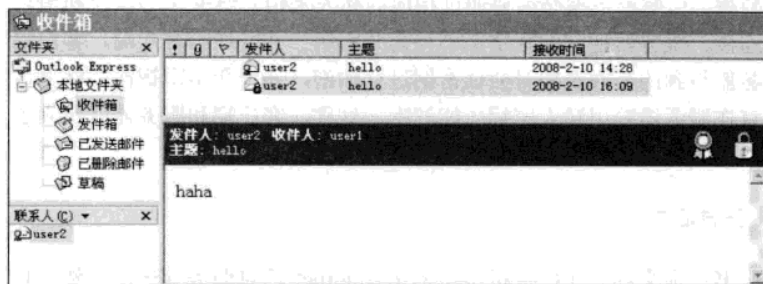


图 5-9-25 正常浏览被加密邮件

在第4台计算机上无法正常浏览被加密的邮件，如图5-9-26所示。

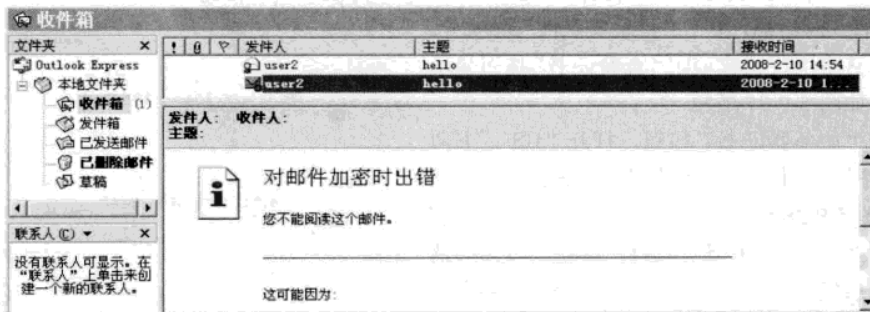


图 5-9-26 浏览加密邮件失败

通过上面的具体操作，可以发现只要发送方和接收方都安装有权威数字证书或者发送方和接收方都使用同一个证书服务器颁发的证书，电子邮件的安全是完全有保障的。

5.9.4 IIS 与数字证书

为了保障通信数据的安全或者是为特定用户服务的网站，可以要求客户端必须使用证书，而拒绝没有证书用户的访问。通过对证书的申请加以审核，用证书来保护 Web 网站的内容不被非法用户访问，另一方面通过使用 SSL 保证用户向服务器提交的数据不会被非法窃取。而 SSL 在电子商务中的应用已经广泛。

1. http 与 https 的相关知识

默认情况下所使用的 HTTP 是没有任何加密措施的，所有的消息全部都是以明文形式在网络上传送，恶意的攻击者可以通过安装监听程序来获得用户和服务器之间的通信内容。

除了匿名访问、基本验证和 Windows NT 请求/响应方式外，还有一种安全性更高的认证，就是通过 SSL (Security Socket Layer, 安全套接层) 安全机制使用数字证书。建立了 SSL 安全机制后，只有 SSL 允许的客户才能与 SSL 允许的 Web 站点进行通信，并且在使用 URL 资源定位器时，输入 https:// 而不是 http://。SSL 位于 HTTP 层和 TCP 层之间，建立用户与服务器之间的加密通信，确保所传递信息的安全性。SSL 是工作在公共密钥和私人密钥基础上的，任何用户都可以获得公

共密钥来加密数据,但解密数据必须要通过相应的私人密钥。使用 SSL 安全机制时,首先客户端与服务器建立连接,服务器把它的数字证书与公共密钥一并发送给客户端,客户端随机生成会话密钥,用从服务器得到的公共密钥对会话密钥进行加密,并把会话密钥在网络上传递给服务器,而会话密钥只有在服务器端用私人密钥才能解密,这样,客户端和服务器就建立了一个唯一的安全通道。

2. 申请服务器证书

(1) 生成证书请求文件。在虚拟机 2 中打开 Internet 信息服务管理器,然后打开要为之申请证书的站点的属性,因默认站点下有证书服务器运行,这里选择 5.4.3 小节中创建的“down”站点。单击右键,在弹出的快捷菜单中选择“属性”命令,打开“属性”对话框,单击“目录安全性”选项卡。如果以前从未用过该选项则“查看证书”按钮显示为灰色,如图 5-9-27 所示。

单击“服务器证书”按钮,打开“IIS 证书向导”对话框,单击“下一步”按钮,选择“新建证书”,如图 5-9-28 所示。

单击“下一步”按钮,选择“现在准备证书请求,但稍后发送”选项。单击“下一步”,要求输入新证书的名称,输入一个容易理解的名字,再选择私钥的长度,取默认值 1024。单击“下一步”按钮,要求输入单位和部门信息,填写相关内容。单击“下一步”,然后输入站点公用名称,注意“公用名称”是其完全合格的域名,是用来区分不同证书的最好方法,如果公用名称发生变化,则需要获取新证书。输入主机的域名“down.sales.www.test.com”,如图 5-9-29 所示,在 5.4.3 小节中配置过该站点。

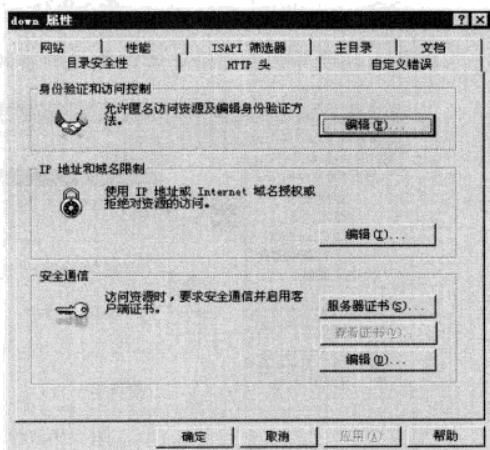


图 5-9-27 目录安全性选项卡

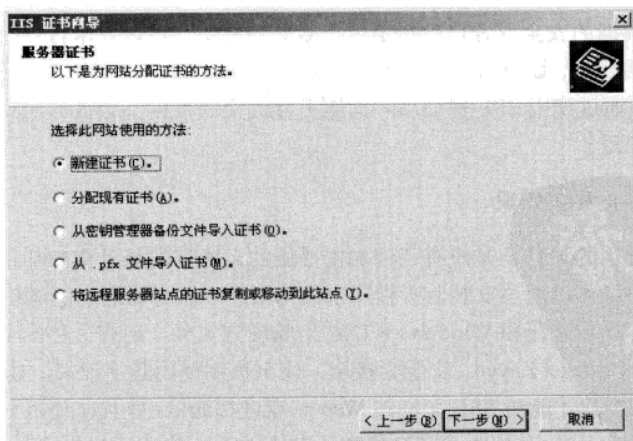


图 5-9-28 服务器证书分配方法

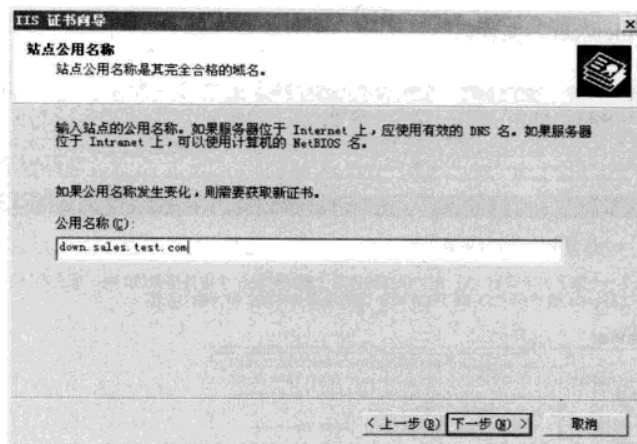


图 5-9-29 站点公用名称

单击“下一步”，输入地理信息。单击“下一步”，选择存储证书请求文件“certreq.txt”。单击“下一步”，显示文件申请的摘要信息。单击“下一步”，完成“IIS 证书向导”，这时申请步骤还没有完成，接下来要把刚才的证书申请文件提交。

(2) 提交证书请求文件。在虚拟机 2 的 IE 地址栏中输入“http://www.sales.test.com/ certsrv”打开证书申请页面，单击“申请一个证书”链接，再单击“高级证书申请”，打开如图 5-9-30 所示的页面，单击“使用 base64 编码...”链接文字。

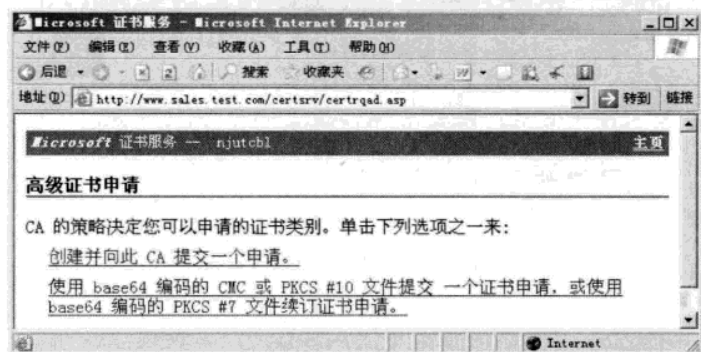


图 5-9-30 高级证书申请

用记事本打开刚才保存的“certreq.txt”文本文件，并选中全部文本内容，复制到“保存的申请”下的文本框中，如图 5-9-31 所示，单击“提交”按钮，完成证书申请文件的提交。

(3) 证书服务器颁发网站证书请求。在虚拟机 2 的证书服务器上颁发刚才 Web 网站服务器的证书申请。

3. 获得服务器证书和安装服务器证书

(1) 下载证书。当证书被颁发后，在虚拟机 2 的 IE 浏览器打开“http://www.sales.test.com/ certsrv”，单击“检查挂起的证书的申请状态”，再单击“保存的申请证书”，在新网页中单击“下

载证书”，保存“certnew.cer”文件。

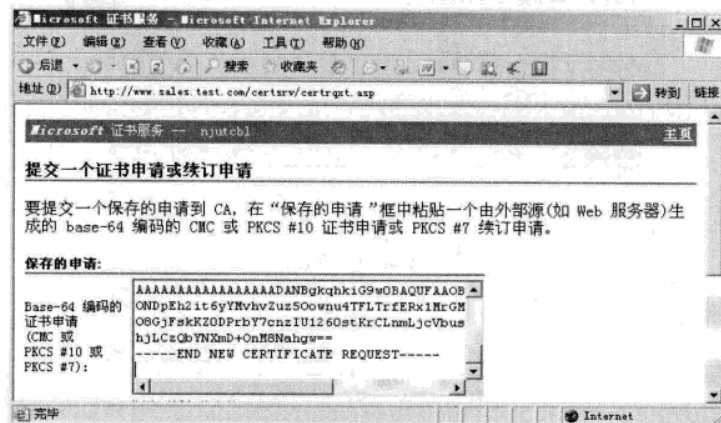


图 5-9-31 提交一个保存的文件证书申请

(2) 安装服务器证书。在 Windows Server 2003 中打开 Internet 信息服务管理器，然后打开刚才要为之申请证书的站点的属性对话框。单击“目录安全性”选项卡，单击“服务器证书”按钮，打开“IIS 证书向导”，单击“下一步”按钮，打开如图 5-9-32 所示的对话框，此时服务器已经挂起了一个证书请求。选择“处理挂起请求并安装证书”单选项，单击“下一步”按钮。

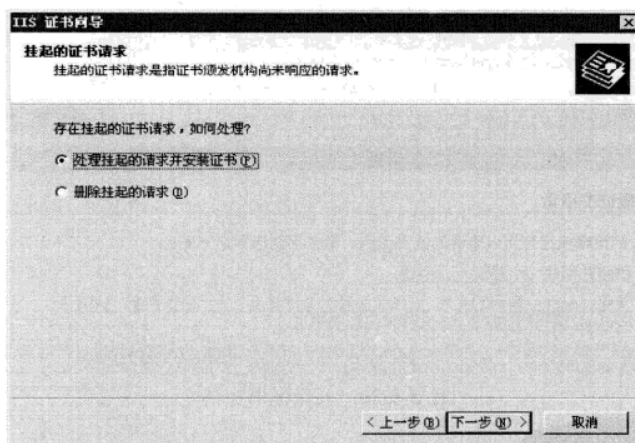


图 5-9-32 处理挂起的网站证书

输入上一步下载的证书文件“certnew.cer”的路径，继续单击“下一步”，提示 SSL 要使用的端口，保留默认的 443 端口，继续单击“下一步”，可以得到证书摘要信息，再单击“下一步”，完成服务器证书的安装。

(3) 设置服务器证书。单击站点“down 属性”对话框的“目录安全性”选项卡，可以发现“安全通信”框中的 3 个按钮都能够使用了。单击“编辑”按钮，打开“安全通信”对话框，如图 5-9-33 所示。

● 要求安全通道 (SSL)。

选择该选项可以将 Web 配置成要求加密通信链接来与该网站、目录或文件相连接。当选择该选项时，发送到该网站以及从该网站发送的所有数据都使用证书进行加密。也就是说选中此项，将进行安全的通信，但服务器的网址不再是以 http，而是以 https 开头。

● 要求 128 位加密。

选择该选项可以将 Web 配置成对于浏览器要求 128 位加密通信链接来与该网站、目录或文件相连接。

● 忽略客户端证书。

选择该选项可以允许用户不必提供客户端证书就可访问该站点。

● 接受客户端证书。

选择该选项可以允许具有客户端证书的用户进行访问，证书不是必需的。具有客户端证书的用户可以被映射；没有客户端证书的用户可以使用其他身份验证方法。

● 要求客户端证书。

选择该选项则仅允许具有有效客户端证书的用户进行连接，没有有效客户端证书的用户被拒绝访问该站点。选择该选项前，必须选择“要求安全通道 (SSL)”选项。

按照如图 5-9-34 所示的设置，完成后，虚拟机 1 浏览“http://down.sales.test.com”站点，如图 5-9-34 所示，提示该页必须通过安全通道查看。

输入“https://down.sales.test.com”，弹出如图 5-9-35 所示的对话框，要求提供证书，此时没有任何可用浏览器证书，单击“确定”按钮返回，页面提示“该页要求客户证书”，网页无法浏览。

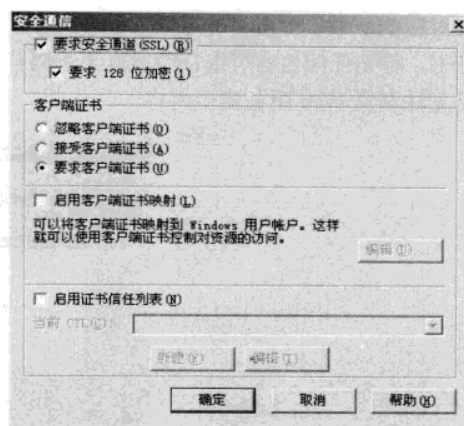


图 5-9-33 安全通信

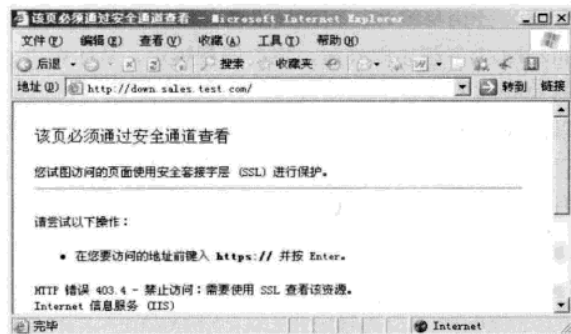


图 5-9-34 Web 出错提示

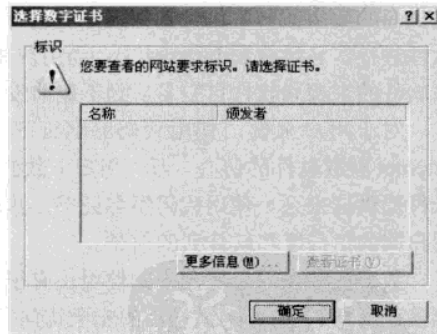


图 5-9-35 需要客户端证书

4. 申请 Web 浏览器证书

虚拟机 1 上访问“http://www.sales.test.com/certsrv”，单击“申请证书”，然后单击“Web 浏览器证书”，接下来的申请和安装证书与申请电子邮件证书类似。虚拟机 1 上安装完 Web 浏览器证书后，在 IE 地址栏中再次输入“https://down.sales.test.com”，弹出如图 5-9-36 所示的对话框，选

择对应的证书,单击“确定”按钮后,可以正常浏览网页的内容。如果没有安装任何 Web 浏览器证书,将无任何内容可选,当然也无法浏览 Web 服务器上内容。当然,如果安装的证书不正确也是无法浏览 Web 服务器上内容。

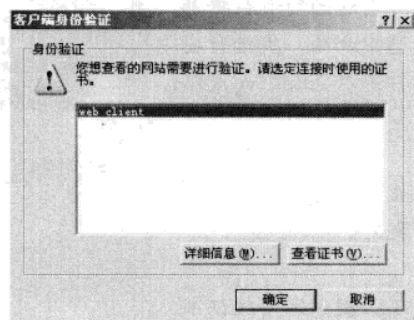


图 5-9-36 客户端 Web 浏览器证书选择

通过上面的设置,可以发现电子商务、Web 浏览只要设置得当,安全性可以有相当高的保障。

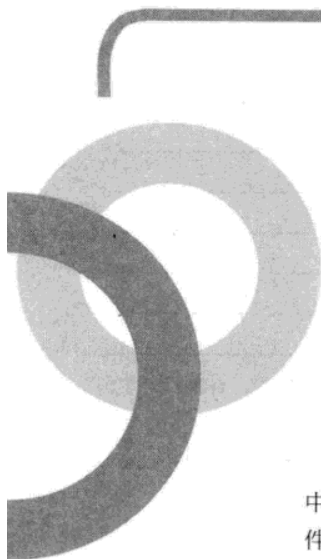
5.9.5 利用数字证书进行代码签名

在商店里购买软件时,软件的来源很清楚,可以分辨软件的提供商;同时,凭借软件的封装,也可以看到软件是否被拆封过。借此,人们可以决定对软件的信任程度。但是,当软件从 Internet 上下载时,还能有足够的信任吗?在计算机病毒横行的今天,也许正在下载的杀毒软件恰恰是一个病毒程序,这样的事情一点也不奇怪,那么在 Internet 上如何使软件得到充分的信任呢?

任何软件提供商要想通过网络来发布代码或程序,都会面临着软件被仿冒和篡改的风险。通过数字证书使用代码签名技术就可以有效地防范这些风险,代码签名证书是 CA 中心签发给软件提供商的数字证书,包含软件提供商的身份信息、公钥及签名。软件提供商使用代码签名证书对软件进行签名后放到 Internet 上,当用户在 Internet 上下载该软件时,将会得到提示,从而可以确信软件的来源和软件自签名后到下载前没有遭到修改或破坏。

对于用户来说,使用代码签名证书可以清楚了解软件的来源和可靠性,增强了用户使用 Internet 获取软件的信心。万一用户下载的是有害软件,也可以根据证书追踪到软件的来源。对于软件提供商来说,使用代码签名证书,其软件产品更加难以被仿造和篡改,增强了软件提供商与用户间的信任度和软件商的信誉。

数字证书在网络安全中的使用还有很多,如软件的版权签名、通过专门的数字签名软件给文档盖“公章”、进行网络站点的安全访问等。



第 6 章 组策略

Chapter 6

本章主要介绍组策略的功能和工作方式，并在 AD（Active Directory，活动目录）中配置和应用组策略，以集中的方式管理用户和计算机，并结合实验演示 MSI 格式文件的制作和软件分发的实现。

6.1 组策略简介

组策略是管理员为用户和计算机定义并控制程序、网络资源及操作系统行为的主要工具。本节主要介绍组策略的功能、组策略的工作方式以及应用组策略的要求。

6.1.1 组策略的功能

使用组策略可以设置各种软件、计算机和用户策略。例如，可使用“组策略”从桌面删除图标、自定义“开始”菜单并简化“控制面板”。此外，还可设置计算机上（在计算机启动或停止时，以及用户登录或注销时）的运行脚本，甚至可以配置 IE 浏览器，自动分发软件，限制用户可执行程序等功能。

使用组策略可以为用户组或计算机组定义自动的配置，包括许多基于注册表的设置、软件安装选项、登录和注销脚本、文件夹重定向、远程安装服务、Internet 浏览器维护，以及很多安全设置。组策略可以帮助管理服务器和客户端计算机，其中许多设置功能对服务器尤其有用。如表 6-1-1 所示，简单列举了组策略的一些功能。

表 6-1-1

组策略功能简表

组策略功能	描 述
软件安装	以集中方式安装、更新和删除软件
远程安装服务	管理远程安装服务
脚本（启动/关机）	在用户登录/注销和计算机启动/关机时应用脚本

续表

组策略功能	描 述
安全设置	管理安全性
文件夹重定向	建立重定向服务器文件夹来管理用户的文件和文件夹
IE 浏览器维护	管理 IE 浏览器
脱机文件和文件夹	使用户可以脱机使用网络文件
漫游用户配置文件	管理用户配置文件
管理模板	通过基于注册表的设置管理计算机和用户

组策略将会强制执行 GPO（Group Policy Object，组策略对象）中保存的设置，GPO 链接到选择的 Active Directory 对象。GPO 是一组被保存的组策略集合，它不仅对客户端和服务端进行配置，还要为用户提供软件和脱机文件等，共有近百种选择。使用 GPO 可以集中管理 Active Directory 结构中的计算机和用户，如域或 OU（Organizational Unit，组织单位）。

6.1.2 组策略的工作方式

组策略的工作方式是当计算机重新启动、用户登录或强制刷新组策略时，目标计算机利用 Active Directory 多层结构的特点，对每个 GPO 设置进行检查。这样，每次只须设置一个用户或一台计算机，可以将该策略强制执行到所有客户端计算机，直到下次更改组策略。从第一次强制执行开始，组策略设置会持续自动执行，并且它们的优先级高于用户设置的注册表或用户本地设置的首选项。如果发生冲突，在登录、重启、有计划的刷新或强制刷新的时候，组策略都会覆盖本地首选项。

6.1.3 应用组策略的要求

应用组策略需要具备下列条件。

- 如果网络中存在较早版本的计算机，如 Windows 95、Windows NT，组策略不会对它们产生影响。
- 组策略需要使用完全合法的域名，而不仅仅是 NetBIOS，所以域中需要存在 DNS，才能保证组策略被正常处理。而且，因为客户端或目标计算机必须可以 Ping 通网络上的域控制器，所以不要关闭 ICMP。如果目标计算机无法 Ping 通域控制器，组策略处理将会失败。
- 应用组策略需要 Active Directory，可以使用组策略来管理服务器和客户端计算机。如果没有建立 Active Directory 结构，大部分与组策略相关的功能将无法使用（当然还是可以在每台计算机上执行“gpedit.msc”，但在每台计算机上单独配置，浪费时间且容易出错），也就不能使用组策略来集中管理计算机和用户。
- 一定要根据 Active Directory 结构来部署组策略，尤其要考虑站点的地理位置，以及域控制器的物理位置。复制速度是需要特别考虑的，因为复杂 GPO 可能会很大，不要试图在大洋两岸使用同一个 GPO。
- 默认情况下只有域和企业管理员能够创建和链接 GPO，除非将这个任务委派给其他用户。

6.2 设置组策略

使用组策略需要启用 Active Directory，安装 Active Directory 之后，随时可以在企业内应用组策略。本节首先搭建域环境，然后介绍域配置选项的功能。

6.2.1 搭建域环境

为了顺利完成本节和后续的实验，首先要搭建域的实验环境，在虚拟机 2 安装 Active Directory，把虚拟机 1 加入到域中。实验环境的搭建包括以下部分。

1. 准备网络环境

STEP 1 还原虚拟机 2 的系统。经过前面章节配置，虚拟机 2 上启用了很多服务，这些服务不仅影响系统的性能，有些还会阻止 AD 的安装，最简单的办法就是利用 3.3.2 小节中备份的“Windows Server 2003 Enterprise Edition.vmdk”文件覆盖虚拟机目录下的同名文件，还原虚拟机 2 的系统。

STEP 2 虚拟机 2 的网络设置。虚拟机 2 的网卡类型为 Bridged，IP 地址是 192.168.1.210，掩码是 255.255.255.0，网关是 192.168.1.1，DNS 是 192.168.1.210。

STEP 3 虚拟机 1 的网络设置。虚拟机 1 的网卡类型为 Bridged，IP 地址是 192.168.1.220，掩码是 255.255.255.0，网关是 192.168.1.1，DNS 是 192.168.1.210。

2. 安装 Active Directory

STEP 1 运行安装向导。在虚拟机 2 上，选择“开始”→“运行”命令，在“运行”对话框中输入“dcpromo”命令，单击“确定”按钮，打开“Active Directory 安装向导”，单击“下一步”按钮继续，安装向导给出兼容性提示，提示一些旧版本的 Windows 操作系统无法工作在域中。单击“下一步”按钮继续。

STEP 2 域控制器类型。安装向导要求选择域控制器的类型，如图 6-2-1 所示，选择“新域的域控制器”。单击“下一步”按钮继续。

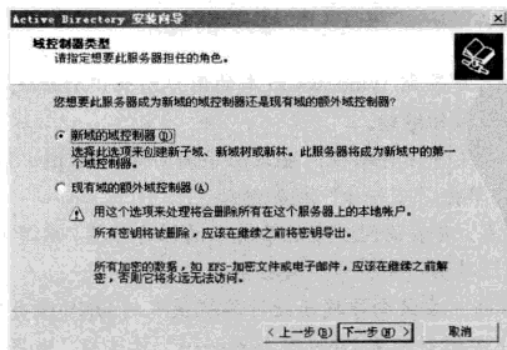


图 6-2-1 选择域控制器类型

STEP 3 创建一个新城。因该服务器是安装的第一个域控制器，这里选择“在新林中的域”，如图 6-2-2 所示。单击“下一步”按钮继续。

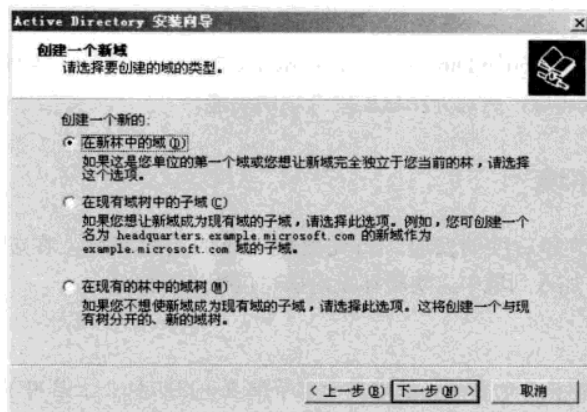


图 6-2-2 创建一个新城

STEP 4 新的域名。安装向导要求指定新城的名称，这里输入“abc.com”，如图 6-2-3 所示。单击“下一步”按钮继续。

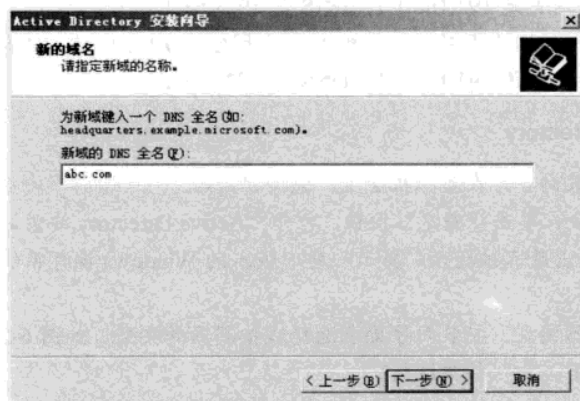


图 6-2-3 输入 AD 域名

STEP 5 NetBIOS 域名是早期 Windows 版本的用户用来识别新城的，安装向导默认使用的是“ABC”。单击“下一步”按钮继续。

STEP 6 数据库和日志文件保存路径。安装向导询问保存 Active Directory 数据库的位置，这里保持默认的保存路径。单击“下一步”按钮继续。

STEP 7 共享的系统卷。安装询问共享的系统卷的保存位置，共享系统卷的分区格式必须是 NTFS，这里保持默认路径。单击“下一步”按钮继续。

STEP 8 DNS 注册诊断。安装向导提示此计算机使用的 DNS 服务器没有响应的处理方法。这里选择“在这台计算机上安装并配置 DNS 服务器……”单选框，如图 6-2-4 所示，一般的操作都是把 AD 和 DNS 集成在一台服务器上。单击“下一步”按钮继续。

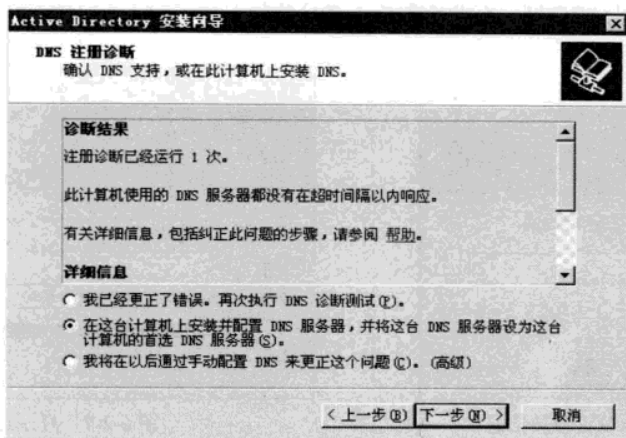


图 6-2-4 DNS 注册诊断

STEP 9 权限。因域环境中没有 Windows 2000 之前的系统存在，这里选择“域中与 Windows 2000 或 Windows Server 2003……”项。单击“下一步”按钮继续。

STEP 10 目录服务还原模式的管理员密码。输入并确认要分配给管理员账户的密码，该账户是该服务器用目录服务还原模式启动时使用的，这里保持为空。单击“下一步”按钮继续。

STEP 11 摘要。向导显示摘要信息。单击“下一步”按钮继续。

STEP 12 完成。系统提示重新启动计算机完成安装。

3. 虚拟机 1 加入域

在虚拟机 1 上右键单击“我的电脑”，在快捷菜单中选择“属性”命令，打开“系统属性”对话框，单击“计算机”选项卡，在“计算机”选项卡中单击“更改”按钮，打开“计算机名称更改”对话框，如图 6-2-5 所示，填入“abc.com”。

单击“确定”按钮，打开如图 6-2-6 所示的对话框。将虚拟机 1 加 abc.com 域，需要域管理员的授权，输入虚拟机 2 的管理员（也就是 abc.com 域管理员）的账户名和密码，单击“确定”按钮，弹出“欢迎加入 abc.com 域”对话框，单击“确定”按钮，系统提示需重新启动计算机。

虚拟机 1 重新启动，单击登录界面中的“选项”按钮，在“登录到”下拉列表框中有两种选择，登录本机或登录到 ABC 域。

4. 测试

在虚拟机 2 上，选择“开始”→“程序”→“管理工具”→“Active Directory 用户和计算机”命令，打开“Active Directory 用户和计算机”窗口，右键单击“abc.com”，在快捷菜单中选择“新建”→“用户”命令，如图 6-2-8 所示，添加用户“test1”。在虚拟机 1

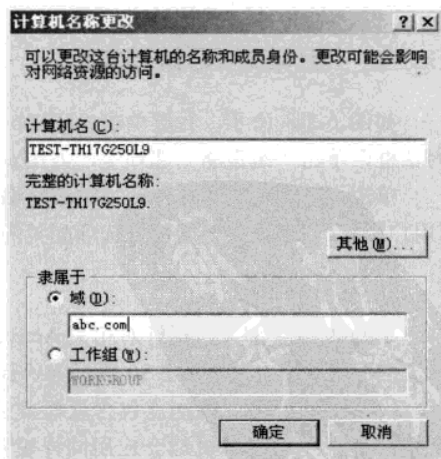


图 6-2-5 加入域

上使用 test1 账户登录 ABC 域，至此虚拟机 1 成功地加入到了 abc.com 域中。

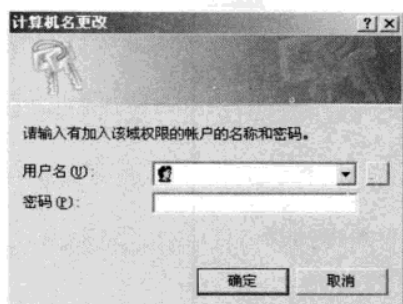


图 6-2-6 输入域管理员信息

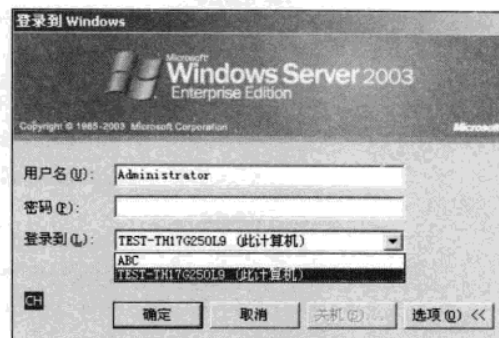


图 6-2-7 登录选择

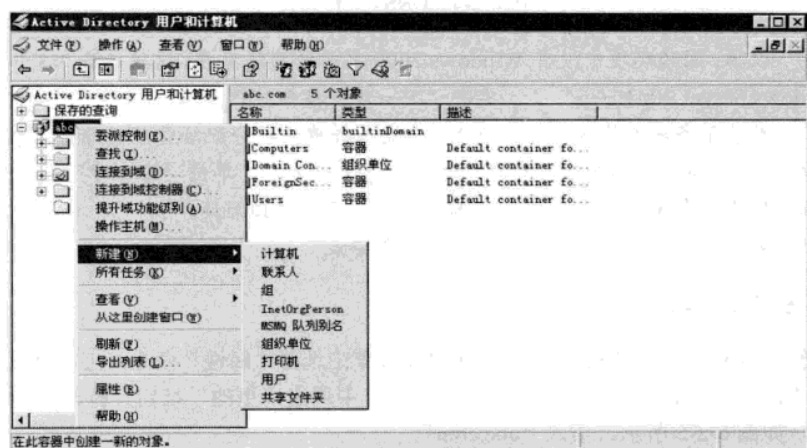


图 6-2-8 新建域用户

6.2.2 组策略配置选项

如图 6-2-8 所示，右键单击“abc.com”，在快捷菜单中选择“属性”，打开“abc.com 属性”对话框，单击“组策略”选项卡，如图 6-2-9 所示。

单击“编辑”按钮，打开“组策略编辑器”窗口，如图 6-2-10 所示，包括“计算机配置”和“用户配置”，这里仅说明部分选项配置的作用，更多的帮助信息可查阅相关的在线帮助。

1. 计算机配置

GPO 的这个部分包括针对相关 Active Directory 容器中的计算机的设置。这些设置影响到计算机上的所有用户，如图 6-2-10 所示为“计算机配置”中所有可以配置的选项。

(1) 软件设置。该结点包含软件安装，其中还包含应用到计算机的软件设置，而不论是哪个用户登录到该计算机都会应用同样设置。该文件夹中可能还会包含部署组策略过程中软件包的设置。

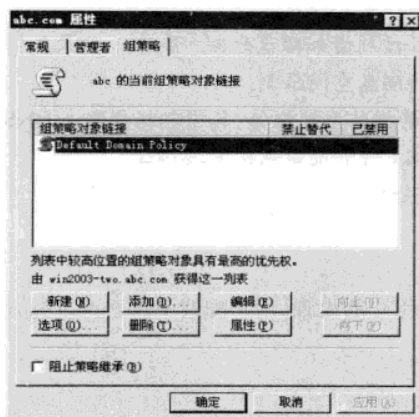


图 6-2-9 编辑组策略

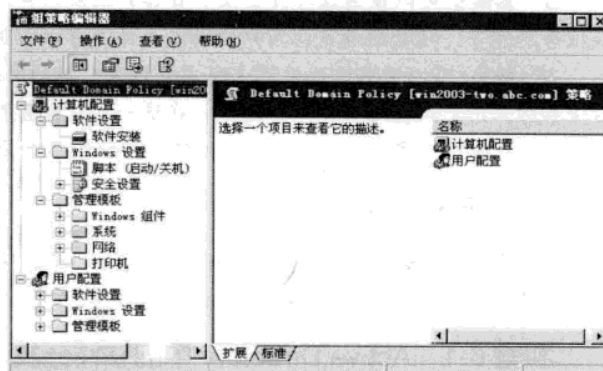


图 6-2-10 组策略编辑器

使用软件配置中的“软件安装”扩展可以集中部署、修补、升级和删除软件应用程序，而不必访问每台计算机，或者要求用户下载、修补、升级他们所需的软件。可以将应用程序指派到计算机，给计算机用户提供对所需应用程序的可靠访问。这些应用程序也会出现在“添加或删除程序”中。如果为站点、域或 OU 中的计算机指派了一个软件包，那么，当下一重新启动或登录时，就可以使用该软件。通过“添加或删除程序”来安装应用程序。尽管用户可以修补该软件，但只有本地或网络管理员才可以删除该软件。组策略的软件安装扩展使用基于 Windows Installer 软件包(.msi 文件)。如果需要部署非 Windows Installer 软件包，需要使用特殊的打包工具来创建必要的.msi 文件，后面的实验中演示如何生成.msi 文件。为站点、域或 OU 内的计算机指派软件之后，当计算机重新启动或用户登录时，该软件会自动安装。安装之后，不用担心用户会卸载它，因只有本地或网络管理员才可以删除它。

(2) Windows 设置。GPOE (组策略编辑器) 的“计算机配置”和“用户配置”结点中都有“Windows 设置”部分。“计算机配置”的“Windows 设置”是针对目标计算机的所有用户。该结点包括两个扩展：“脚本”和“安全设置”。

- 脚本：可以使用组策略分发的脚本来自动化计算机的启动和关机，需要使用“脚本”扩展分别指定启动和关机脚本。这些脚本运行在本地系统权限上。

- 安全设置：可以使用“安全设置”保护计算机和整个网络。可以为站点、域或任何层次的 OU 指定安全策略，其中包括账户策略、本地策略、公钥策略、事件日志、受限制组、系统服务、注册表、文件系统、软件限制策略、无线网络策略、IP 安全策略等。可以看出，可以使用组策略的安全设置扩展为计算机强制实施各种安全设置。不论什么时候处理 GPO，这些安全策略都会被应用到那些位于与 GPO 相关的 Active Directory 容器内的计算机，但一些设置在重新启动之前不会生效。“安全设置”可以增强现有的安全工具，例如，组策略中的其他部分，以及文件、文件夹、Active Directory 对象的属性窗口中的安全选项卡等。

(3) 管理模板。听到“组策略”这个词大多都会联想到管理模板，管理模板可以集中配置客户端的注册表。该扩展是组策略中基于注册表的管理模板，可以获得大约 700 个不同的设置。

- Windows 组件：可以使用这些设置为操作系统配置系统组件，如 Netmeeting、Internet

Explorer 和终端服务设置等。

- 系统: 可以使用这些设置来配置各种系统组件, 以控制诸如磁盘配额、脚本、登录和错误报告功能等。磁盘配额是指用户对特定文件夹可以占用的磁盘空间限制。

- 网络: 可以使用这些设置来配置连接客户端到网络的操作系统组件。其中包括指定主 DNS 后缀和防止用户对其进行更改。还可以在这一部分配置脱机文件和简单网络管理协议。

- 打印机: 这一部分包含管理网络打印机配置和公布选项的许多配置。

2. 用户配置

GPO 这个部分包括针对相关 Active Directory 容器中的用户的设置。用户配置中每个可以配置的项多数与“计算机配置”相似, 在此不再叙述。

实验 6-1 Active Directory 中的软件分发

面对网络环境下数量众多、需求各异的用户, 以及硬件配置不同、用途也不不同的计算机, 网络管理员几乎每天都有各种各样关于软件安装的需求。工作站无休止地进行软件安装、升级、维护、删除操作所带来的庞大工作量, 以及由此可能产生的安全问题一直都是令所有网管头疼的事情。使用 Windows Server 2003 组策略中的软件部署可以解决这个难题, 让这些令人烦恼的事情变得轻松起来, 使网管彻底摆脱软件部署的烦恼, 既省时又省力。

本实验结合 QQ2008 的安装, 介绍 Active Directory 中软件分发的实现。要使域中的所有计算机都需要安装 QQ2008, 其中虚拟机 2 是域控制器, 虚拟机 1 是域中的一台计算机, 通过在虚拟机 2 上部署软件分发, 实现域中所有计算机 (这里仅有虚拟机 1) 自动安装 QQ2008。该实验难度较大, 分以下几个步骤。

1. 准备安装文件

使用组策略部署软件分发的第一步是获取以 ZAP 或 MSI 为扩展名的安装文件包。MSI 安装文件包是微软专门为软件部署而开发的。有些软件的安装程序会直接提供这两个文件, 有些软件的安装程序是不提供的。如果软件的安装程序已经提供了 MSI 文件, 请直接跳到分发软件步骤。对于不提供 MSI 文件的软件可以使用 WininstallLE 的打包工具来创建, 通过使用它可以将一些没有提供 MSI 文件的软件打包生成 MSI 文件以便于实现组策略软件部署。WininstallLE 工具可以从 Windows 2000 安装光盘的\VALUEADD\3RDPARTY\MGMT 目录下找到, 但该软件实际使用的效果并不是很理想, 这里推荐使用 InstallShield AdminStudio5, 用它生成 MSI 文件在组策略中发布很成功。该文件较大, 有 502MB, 下载的 network.rar 中提供了该文件的 30 天试用版, 也可以从“<http://www.installshield.com/>”下载。本实验中要分发的 QQ2008 仅有一个 EXE 文件, 需要被打包成 MSI 文件才能被分发。

注意



因 AdminStudio5 文件较大, 安装时需要占用较多的硬盘空间, 安装时把安装路径改到 D 盘, 否则可能会提示 C 盘空间不足。

STEP 1 安装 InstallShield AdminStudio5。在虚拟机 2 上, 双击“adminstudio86.exe”文件, 开始安装。安装向导提示安装 AdminStudio5 前需要先安装 InstallShield 2008, InstallShield

2008 文件已经包含在文件 adminstudio86.exe 中，单击“Install”按钮，如图 6-2-11 所示，开始安装。该软件的安装比较简单，接下去单击“next”按钮，遇到许可协议时，要选择同意，完成软件的安装。安装的过程比较慢，这一点是受虚拟机性能所限，需要耗费相当长时间才能完成安装。

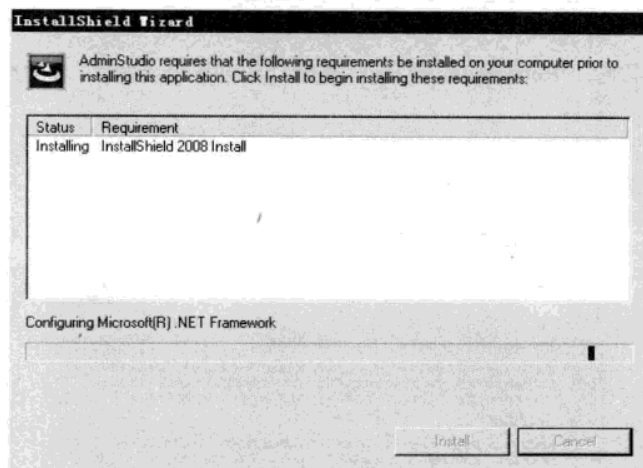


图 6-2-11 安装 AdminStudio5

STEP 2 运行 AdminStudio。在虚拟机 2 上，选择“开始”→“程序”→“Macrovision”→“AdminStudio 8.6 Tools”→“Repackager”命令，打开如图 6-2-12 所示的窗口。

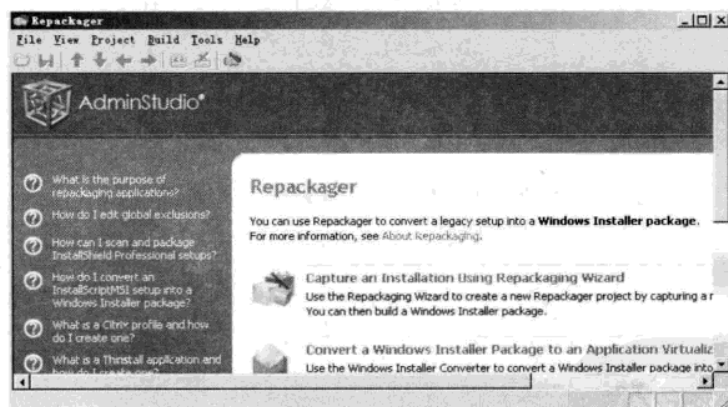


图 6-2-12 重新打包

STEP 3 执行向导。单击如图 6-2-12 所示的“Capture an Installation Using Repackaging Wizard”超级链接，使用重新打包向导捕获一个安装。如果弹出如图 6-2-13 所示的对话框，表示 AdminStudio 对有些文件的操作不太确定或者这个程序已经运行了一次，这都会引起最后打包的文件不准确，强烈建议重新启动计算机。这里建议，只要看到这个窗口，就要重新启动计算机，再执行该向导。

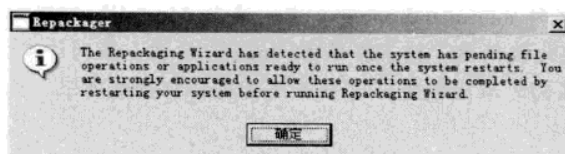


图 6-2-13 重新打包警告窗口

STEP 4 欢迎信息。“Repackager Wizard”重新打包向导开始运行，显示欢迎信息。单击“下一步”按钮。

STEP 5 打包方式选择。重新打包向导，询问重新打包的方式，使用推荐的“Installation Monitoring”监视安装，如图 6-2-14 所示，这个选项比 Snapshot 要快且准确。

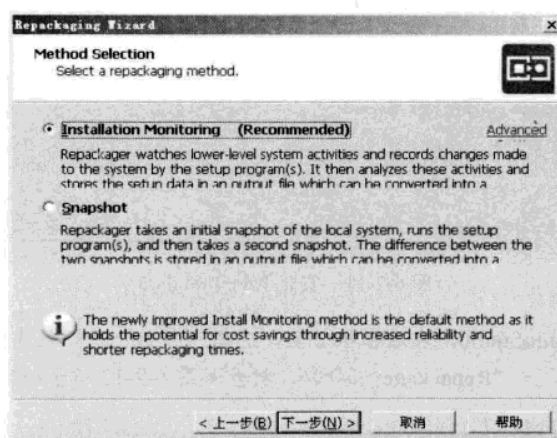


图 6-2-14 打包方式

STEP 6 收集软件信息。指定要安装的软件路径及以后生成的 MSI 文件名、版本号及公司信息等，如图 6-2-15 所示。

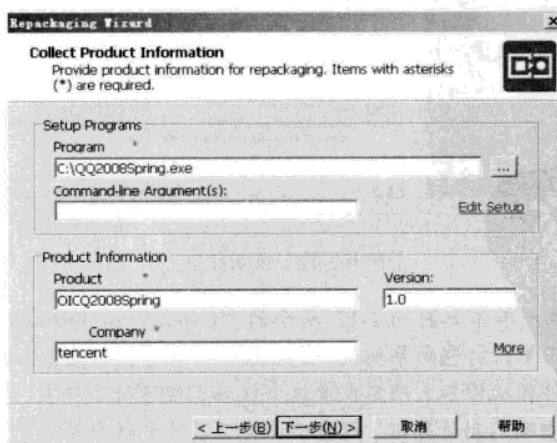


图 6-2-15 收集软件信息

STEP 7 选择存放路径。指定将要项目信息和捕获的文件的存放位置，根据需要指定一个目录，如图 6-2-16 所示。

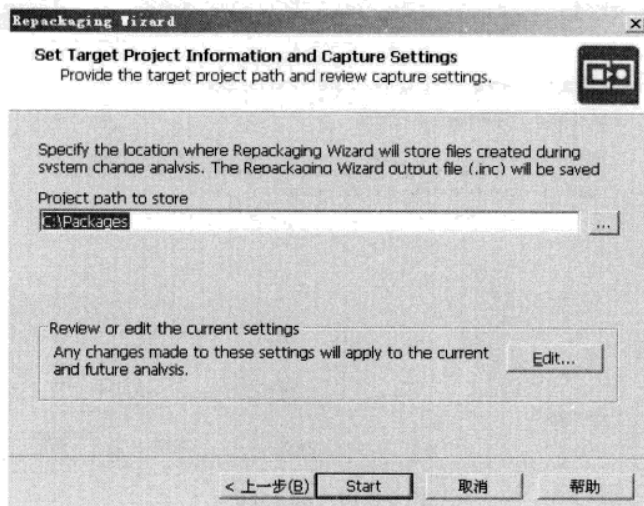


图 6-2-16 指定目标路径

STEP 8 开始软件安装。单击“Start”按钮即开始指定软件的正常安装，同时 InstallShield 也开始在后台监视安装的全过程，如图 6-2-17 所示。

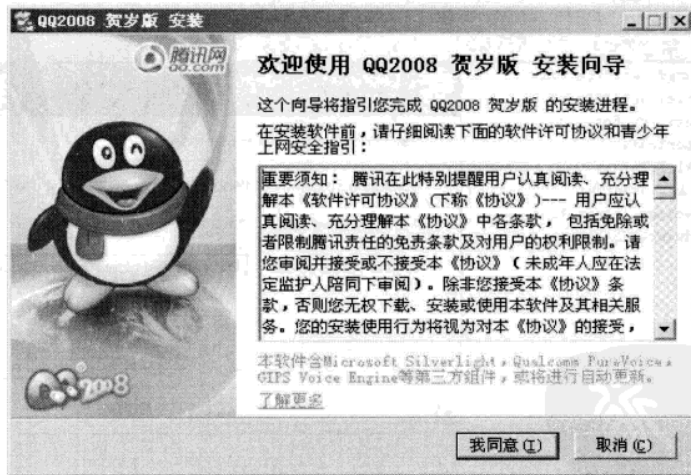


图 6-2-17 安装 QQ2008 软件

STEP 9 系统分析。“OICQ”按正常程序安装完成后，系统会出现如图 6-2-18 所示的提示，单击“Process”即开始提取刚才监视程序所记录的安装过程中所产生的各项信息，结束后出现汇总信息。

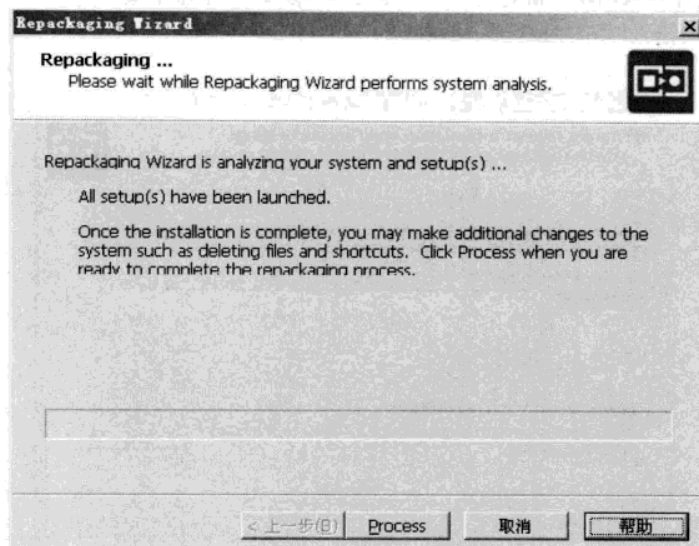


图 6-2-18 系统分析

STEP 10 捕获完成。单击汇总信息对话框中的“完成”按钮，系统调出刚才所提取出来的各项具体内容，准备开始制作 MSI 文件，如图 6-2-19 所示。

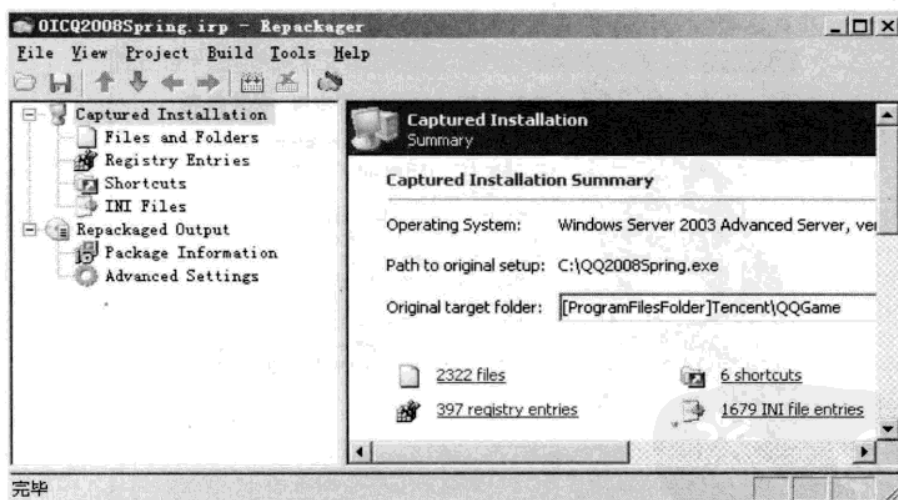


图 6-2-19 捕获安装文件

STEP 11 编辑捕获。可以查看到刚才软件安装时产生的文件、注册表记录、生成的快捷方式等。也可以进行编辑，如选中一个快捷方式后，单击“Exclude”，表示在将来的 MSI 文件安装过程中不生成这个快捷方式，如图 6-2-20 所示。当然与之相对应的是选择“Include”。

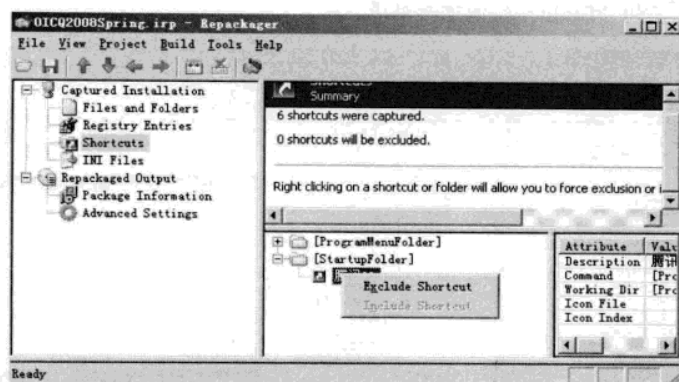


图 6-2-20 编辑快捷方式

STEP 12 编译。最后选择菜单“Build”下的“Build”按钮开始创建 MSI 文件，此时可以看到类似程序开发工具编译代码的创建过程。创建完成后，在指定的目录下可以发现新创建的 MSI 文件。

STEP 13 测试。把 OICQ2008Spring.msi 文件复制到真实机，双击进行安装，出现如图 6-2-21 所示的对话框，单击“Next”进行安装，这时发现 MSI 文件的安装比原来 EXE 文件的安装要省去很多步骤。

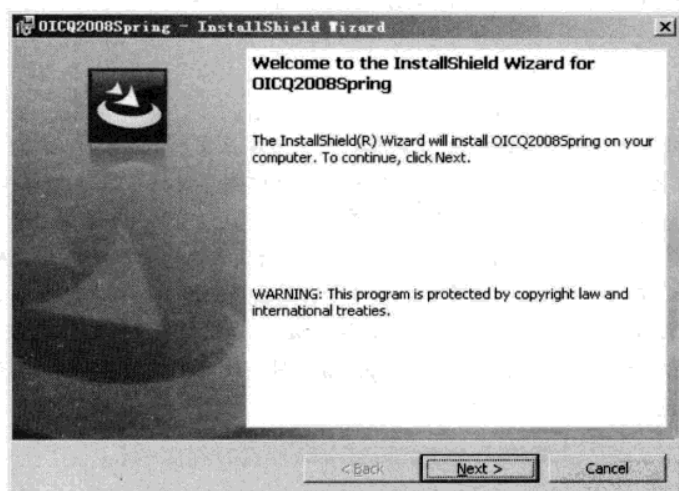


图 6-2-21 安装 MSI 包

在真实机上，选择“开始”→“程序”命令，发现有空白的项目，再选择下一级的 QQ 程序可以运行。出现这种现象的原因是因为 InstallShield AdminStudio5 试用版对中文的支持不好（需要购买中文语言包），所以在创建 MSI 文件里最好不要输入中文信息，即使本身原软件生成了中文的信息，也要尽量将其编辑成简单的英文信息，否则生成的 MSI 文件安装时会出现乱码。

STEP 14 修改 MSI 文件。在 AdminStudio5 中选择菜单“Project”→“Edit InstallShield Project”命令，在 InstallShield 2008 中进行编辑，如图 6-2-22 所示，编辑完成后。在 InstallShield 2008 中，

选择菜单“Build”下的“Build”按钮重新编译。

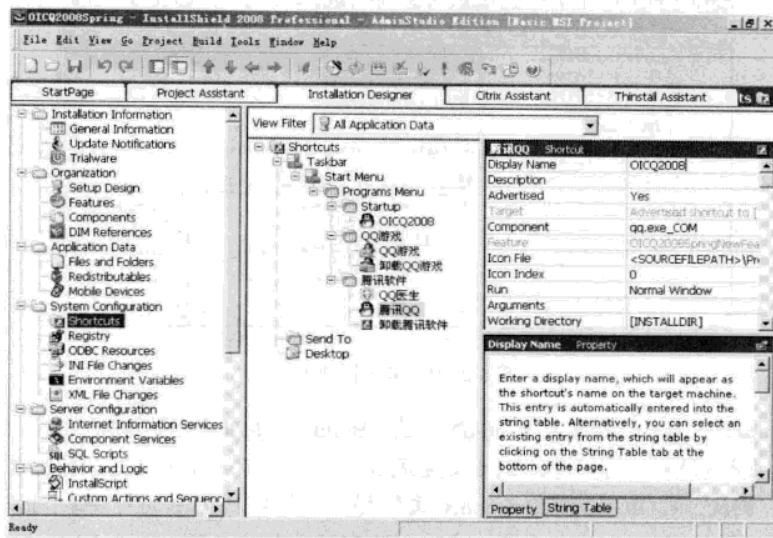


图 6-2-22 编辑安装文件

InstallShield AdminStudio5 的功能非常强大，可以输入一些程序的作者、主题、供应商、支持信息等个性化的内容。

2. 分发文件

STEP 1 建分发点。要发布或指派计算机程序，必须在发布服务器上创建一个分发点。把安装文件所在的文件夹创建一个共享网络文件夹，并对该共享设置权限以允许特定的 OU 才能够访问此分发程序包。在虚拟机 2 上，共享 c:\packages 文件，设置成 Everyone 都可以读取。

STEP 2 编辑组策略。在“Active Directory 用户和计算机”管理单元中，右键单击“abc.com”，在快捷菜单中选择“属性”，单击“组策略”选项卡，单击“编辑”按钮，打开组策略编辑器窗口。

STEP 3 指派/发布程序包。右键单击“软件安装”，在快捷菜单中选择“新建”→“程序包”命令，如图 6-2-23 所示。打开 OICQ2008Spring.msi 文件，这里一定填入网络路径，因为分发的用户要能从网络路径访问到这个文件。

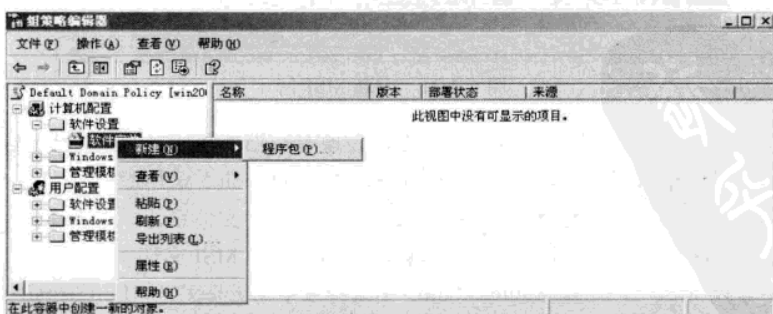


图 6-2-23 新建程序包

打开文件后,弹出“部署软件”对话框,选择“已指派”,如图6-2-24所示。

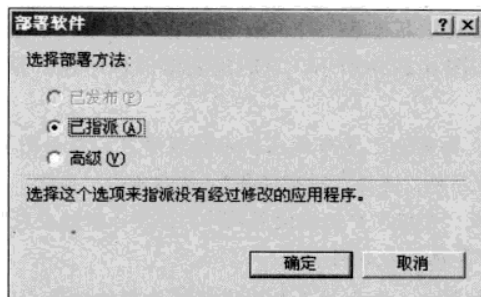


图 6-2-24 指派软件

添加完成后,如图6-2-25所示,注意其中的路径一定是网络路径。关闭组策略编辑器,单击“确定”按钮,完成组策略的编辑。

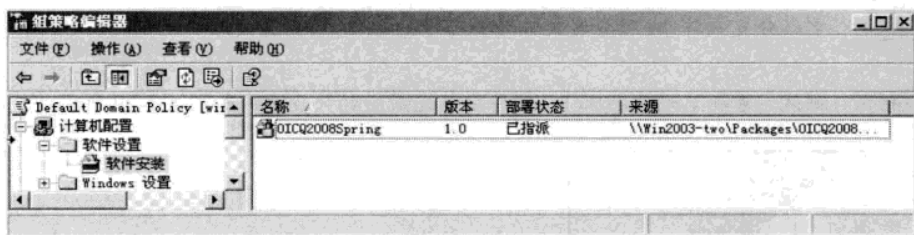


图 6-2-25 添加指派的软件安装

STEP 4 客户端软件的安装。开启虚拟机1,屏幕提示正在安装经过管理的软件 OICQ2008 Spring,如图6-2-26所示。

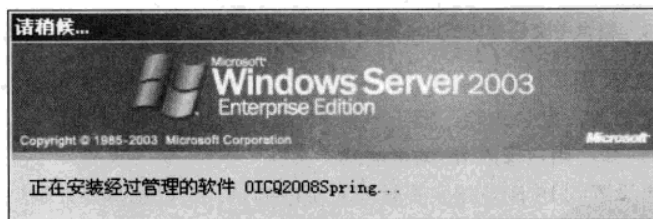


图 6-2-26 安装 OICQ2008Spring

该组策略是针对计算机的,因此不论是登录本机还是登录域,都会自动安装 OICQ2008 Spring。完装后,在虚拟机1上选择“开始”→“程序”→“ ”→“OICQ2008”命令,如图6-2-27所示,可以运行 OICQ。至于有些地方没有显示,是因为中文乱码的问题,而前面是因为已经把“腾讯 QQ”改成了“OICQ2008”,所以能够显示正常。



图 6-2-27 有中文乱码的快捷方式

3. 重新部署程序包

在某些情况下,可能需要重新部署一个软件程序包。例如,上述分发的程序包就不完美,有中文的地方出现乱码,如图 6-2-27 所示,这时需要修改程序包。重新部署程序包,操作步骤如下。

STEP 1 删除程序包。要删除已发布或已指派的程序包,在如图 6-2-25 所示的右侧窗格中,右键单击 OICQ2008Spring 程序包,选择“所有任务”,然后单击“删除”按钮,这里可以选择“立即从用户和计算机卸载软件”或“允许用户继续使用软件,但禁止新的安装”,然后单击“确定”。按钮这里选择“立即从用户和计算机卸载软件”。

STEP 2 重新启动虚拟机 1,提示“正在删除经过管理的软件 OICQ2008Spring”。登录后,发现刚才安装的 OICQ2008Spring 软件已经被成功卸载。

STEP 3 重新编辑 MSI 包。用如图 6-2-22 所示的方法重新编辑快捷方式,把中文字符换成英文字符,如图 6-2-28 所示。

编辑完成后。在 InstallShield 2008 中,选择菜单“Build”下的“Build”按钮重新编译。

STEP 4 重新分发文件。按照分发文件步骤 2 中的操作,重新分发编辑后的 OICQ2008 Spring 程序包。

STEP 5 测试。重新启动虚拟机 1,软件安装完成后的快捷方式如图 6-2-29 所示。

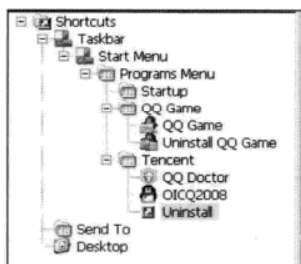


图 6-2-28 编辑中文快捷方式



图 6-2-29 删除中文乱码后的快捷方式

通过本实验的练习,用户可以把很多应用程序编辑成 MSI 文件,并在组策略中设置软件分发,自动完成软件的批量部署,批量删除,批量更新。

【快问快答】如何禁止用户修改 IE 浏览器的主页?

答:如果不希望设置的 IE 浏览器主页被随意更改的话,可以选择“开始”→“程序”→“管理工具”→“Active Directory 用户和计算机”命令,在弹出的窗口中右键单击想限制修改主页的 OU 或组织单位,并在弹出的快捷菜单中选择“属性”命令。在“属性”窗口中选择“组策略”选项卡,接着单击下方的“新建”按钮,然后单击“编辑”按钮,在打开的“组策略编辑器”窗口中依次单击“用户配置”→“管理模板”→“Windows 组件”→“Internet Explorer”命令,然后选择“禁用更改主页设置”组策略并启用即可。另外在这个窗格中,还提供了“更改历史记录设置”、“更改颜色设置”和“更改 Internet 临时文件设置”等项目的禁用功能。启用此策略后,在 IE 浏览器的“Internet 选项”对话框中,其“常规”选项卡的“主页”区域的设置将变灰。

【快问快答】假如有多个人同时使用一台计算机,如何控制指定用户不能运行特定的应用

程序？

答：可以把用户划分为不同的组织单位中，例如，一个机房有两个班同学使用，甲班不允许使用 Word，乙班不允许使用 Excel。这时可以建立两个组织单位：甲和乙，甲班属于甲组织单位，乙班属于乙组织单位。然后在甲组织单位上编辑组策略，打开“用户配置”→“Windows 设置”→“安全设置”→“软件限制策略”界面，如图 6-2-30 所示。

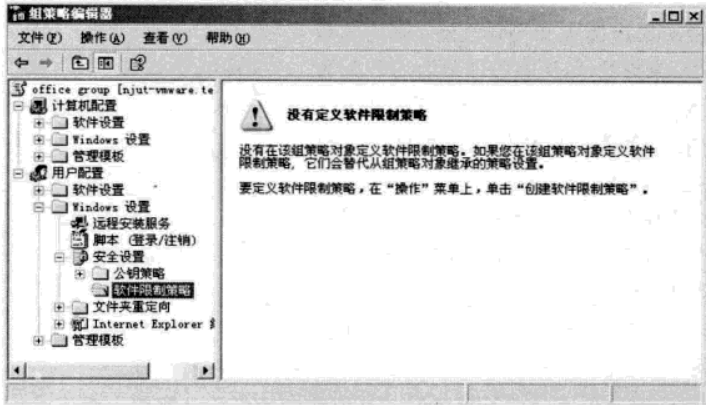


图 6-2-30 软件限制策略

在“软件限制策略”上右键单击，在快捷菜单中选择“创建软件限制策略”命令，软件限制策略下多出两个子项，在“其他规则”上单击右键，如图 6-2-31 所示，选择新建一条“哈希规则”，如图 6-2-32 所示。

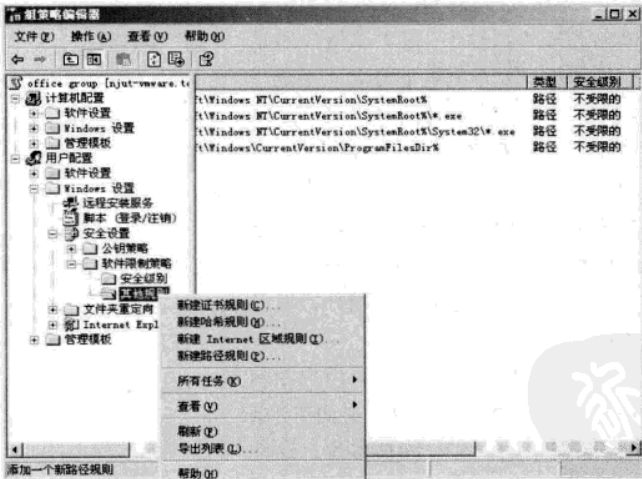


图 6-2-31 软件限制规则设置

在如图 6-2-32 所示的“新建路径规则”对话框的“文件哈希”栏中填入 Word 程序文件所在的路径，把安全级别设成“不允许”。这样甲班学生将不能够使用 Word 程序，类似再设置乙组织单位的组策略。这样就实现了对特定用户的软件限制，除此之外还能通过组策略限制用户只能运

行特定的软件, 甚至可以把用户的默认外壳程序(explorer.exe)换成特定的应用程序, 这些在此就不再举例, 总之, 域中的组策略功能非常强大。

【快问快答】文件夹重定向有什么好处?

答: 文件夹重定向提供了许多好处, 包括如下方面。

(1) 提高了漫游用户配置文件性能。因为只有部分文档需要复制, 所以当从服务器复制用户配置文件时, 性能得到了提高。每次用户登录时, 并不是用户配置文件中的所有数据都被传输到桌面——只有用户需要的数据才被传送。

(2) 储存在网络服务器上的数据可以作为系统管理日程的一部分被备份出来。这样就比较安全, 并且在用户端不需要做任何活动。

(3) 指定给一个用户的数据可以从装有操作系统文件的硬盘重定向到用户计算机上的一个不同的硬盘。如果操作系统需要重新安装, 这样做就保护了用户的数据。

(4) 即使当用户登录到不同的计算机时, 在网络中的任何计算机上都可得到相同的文档。

【快问快答】如何把“我的桌面”进行文件夹重定向, 使用户不管在哪台计算机上登录, 都显示一样的桌面?

答: 以域管理员身份登录 DC (域控制器), 然后依次单击“开始”→“程序”→“管理工具”→“Active Directory 用户和计算机”, 在弹出的窗口中右键单击想要实现文档重定向的 OU 或组织单位, 并在弹出的快捷菜单中选择“属性”。在“属性”对话框中选择“组策略”选项卡, 接着单击下方的“新建”按钮, 然后单击“编辑”按钮, 在打开的“组策略编辑器”对话框中依次单击“用户配置”→“Windows 设置”→“文件夹重定向”→“桌面”, 右键单击“桌面”, 在快捷菜单中选择“属性”, 如图 6-2-33 所示, 设置选择为“高级-为不同的用户指定位置”选项, 并在安全组成员身份列表框中加入需重定向“桌面”的用户, 以及重定向“桌面”在服务器上的位置。

单击“确定”按钮, 保存配置, 这样不管用户在网络中的任何计算机上登录, 都可得到相同的“桌面”, “桌面”中的内容可以随服务器中的内容一同被备份, 这使得数据安全又增加了保障。

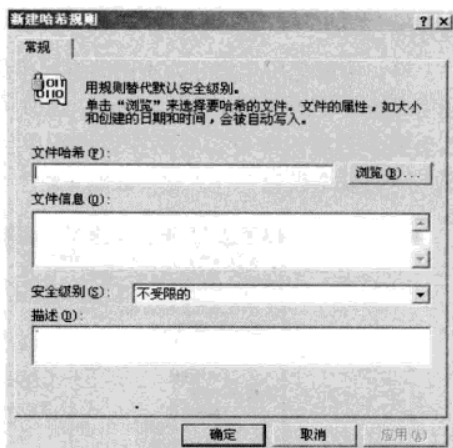


图 6-2-32 新建哈希规则

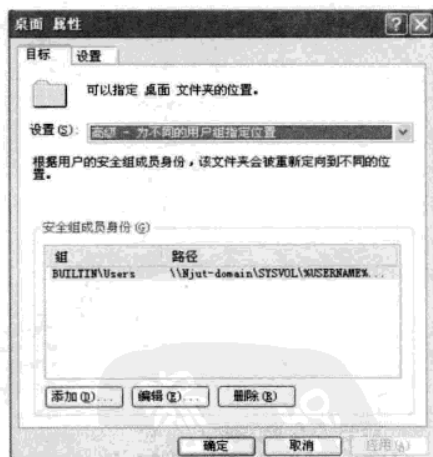


图 6-2-33 用户桌面重定向

Part

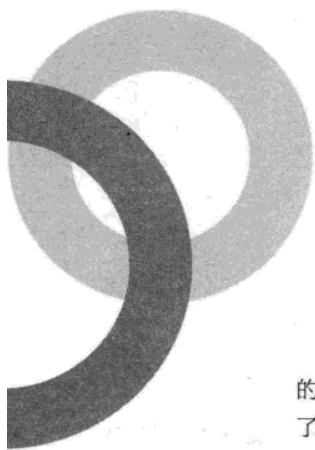
03

第 3 部分 路由和交换篇

本篇主要介绍网络的互联、网络的优化、网络的安全、网络的增值服务和网络的管理等内容。

路由器和交换机的生产厂商有很多，国外有著名的 Cisco（思科），国内的有华为、锐捷等。本书以思科产品为例介绍路由和交换这门技术的原因主要有两方面。一是因为思科公司是全球最大的互联网设备提供商，是众多业界标准的制定者；二是因为读者手边都有思科设备，方便动手实验。

书中将引入一款最新的模拟器，不仅可以做实验，还可以自己设计拓扑，自己选择设备型号、自己选择 IOS（路由器的操作系统），甚至可以把它用于实际生产环境，弥补没有设备的不足。



第7章 路由器的硬件和软件

Chapter 7

本章介绍路由器的硬件和软件，主要内容包括“Dynamips”机架的搭建、路由器的基本硬件、基本软件、路由器的可选模块及其功能描述。通过学习本章，读者可以了解路由器一般的操作和配置方式，其中包含一些 Exec 命令的使用示例。这既能使熟悉 Cisco 公司产品的读者温故而知新，同时也使缺乏 Cisco 产品使用经验的用户能够掌握 Cisco 路由器配置的必备知识。另外，完成本章实验环境的搭建是顺利完成本篇后续章节学习的前提。

7.1 搭建路由器和交换机实验机架

中国有句古话，叫“巧妇难为无米之炊”。学习网络知识更是如此，如果没有路由器和交换机，只能是纸上谈兵，不能动手实践，学习效果将会大打折扣，结果事倍功半。可 Cisco 的路由器和交换机价格昂贵，少则几千元人民币，多则几十万元人民币，远远超出了个人的购买能力。若要配置设备，除了参加社会培训外，几乎别无选择，可即使是参加社会培训，时间是短暂的，设备是有限的。但是不要沮丧，相信大家现在对 VMware 应该都不陌生，通过使用 VMware 软件，可以把一台计算机虚拟出很多台计算机，VMware 其实只是虚拟出一台计算机的硬件，至于安装什么操作系统，完全由用户选择。那么有没有一款能模拟出路由器和交换机硬件的软件呢？

这里推荐一款经典的路由器和交换机的模拟软件“Dynamips”。虽然以往也有很多款 Cisco 路由器和交换机的模拟软件，可任何一款路由器和交换机的模拟软件都不能与“Dynamips”相提并论，因它与以往的模拟软件有本质上的区别。首先，“Dynamips”模拟的是路由器和交换机的硬件，至于加载什么版本的 IOS，完全由用户决定，这一点很像 VMware。而以往的模拟软件都是同时模拟硬件和软件，无论如何模拟，它的软件也不可能和 Cisco 公司的 IOS 相媲美，功能受限不谈，往往更是 BUG 连连；其次，“Dynamips”模拟的路由器和交换机可以与真实的网络互联，甚至可以用于实际的生产环境中，而以往的模拟器只是一个虚拟环境，无法与真实的网络相连。

7.1.1 实验机架拓扑

为了便于完成本书相关的路由和交换实验，需要搭建如图 7-1-1 所示的“Network”拓扑。拓扑中包括 3 台 Cisco3640 的路由器，SW1 和 SW2 各配置一个 16 口的交换模块，R1 配备两个快速以太网模块；SW3 是不可配置交换机，一个端口接 R1 的 Fa0/0，另一个端口连接“真实机”的物理网卡，从图中可以看出“真实机”、“虚拟机 2”、Internet 等都接到了这个实验环境中。4 台 Cisco 3620 的路由器，用来模拟计算机。

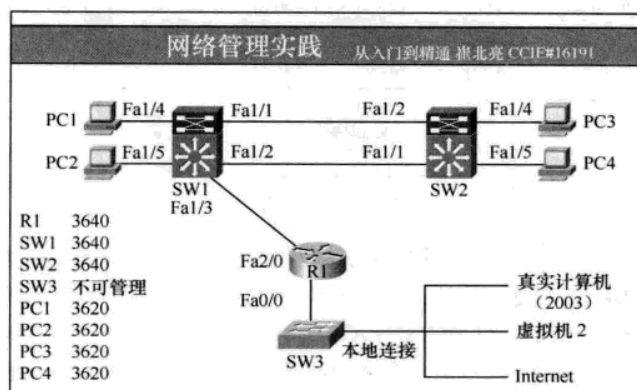


图 7-1-1 网络拓扑图

为了便于大家完成本书相关的安全实验，还需要搭建如图 7-1-2 所示的“Security”拓扑。拓扑中包括两台 Cisco7200 的路由器，一台 Cisco3640 的路由器，3 台路由器均配备了支持 VPN 功能的 IOS。两台交换机 SW1 和 SW2，它们都是不可配置的交换机。SW1 相当于连接在物理网卡上，与局域网有关；SW2 相当于连接在安装 VMware 时产生的 VMnet1 网卡，相当于内网，与内部的局域网隔离，以后用到此拓扑，需要启用 VMnet1 网卡，不然会报错。“虚拟机 1”的网卡类型是“Host-only”，“虚拟机 2”的网卡类型是“Bridged”。

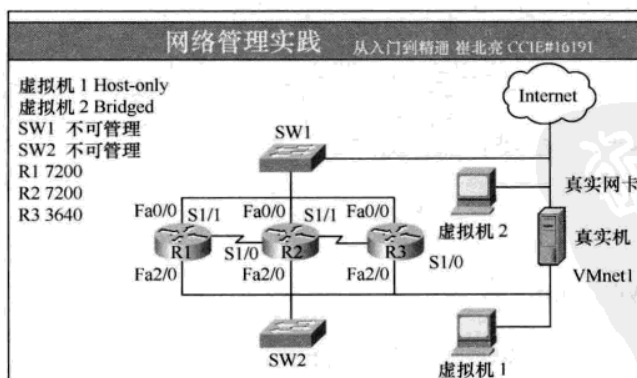


图 7-1-2 安全拓扑图

为了便于大家完成本书相关的语音实验，另外需要搭建如图 7-1-3 所示的“Voice”拓扑。语音拓扑和安全拓扑一样，区别在于语音拓扑中包括的是两台 Cisco3640 的路由器，一台 Cisco7200 的路由器，3 台路由器均配备了支持语音功能的 IOS。

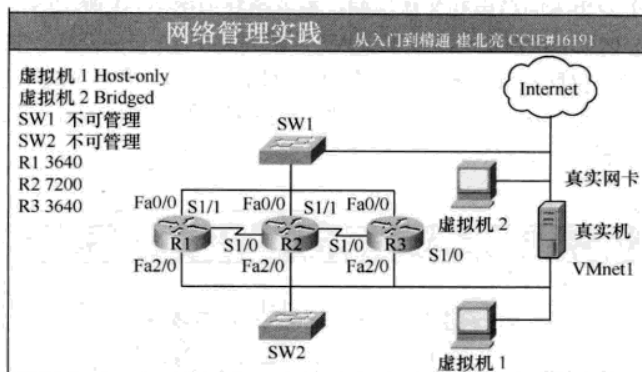


图 7-1-3 语音拓扑图

为了便于大家更进一步的学习，还需要搭建如图 7-1-4 所示的“CCNP”拓扑。拓扑中包括 8 台 Cisco7200 的路由器；一台连接到计算机真实网卡的交换机，同时也连接着所有路由器的 Fa0/0 口；一台 ATM 交换机，连接着 R1 和 R8 的 ATM2/0 口，R1 端的 PVC 是 1/100，R8 端的 PVC 是 2/200；一台帧中继交换机，分别连接着每个路由器的 S1/2 口，并配置了全互连，Rx 到 Ry 的 DLCI 号是 x0y，如 R1 到 R2 的 DLCI 号是 102，R2 到 R1 的 DLCI 号是 201，其他的依此类推。该机架几乎可以完成 CCNP 涉及到的所有路由实验。

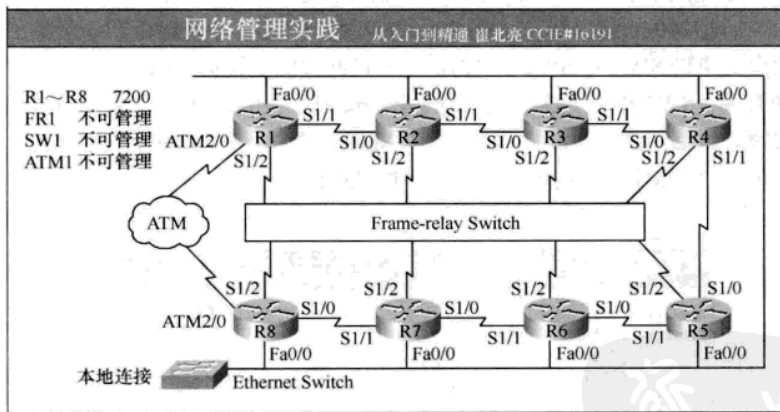


图 7-1-4 高级拓扑图

7.1.2 安装“Dynamips”

根据上面的拓扑，按如下步骤操作，进行初始化安装，很快就可拥有所有设备，以后可以直接使用。

- STEP 1** 把 Network.rar 中的 “Dynamips.rar” 文件解压缩到任何目录。
- STEP 2** 进入 setup 子目录对模拟器进行整体参数的配置。
- STEP 3** 双击 “1.安装 Win_Pcap”。根据系统提示完成 Win_Pcap 的安装。
- STEP 4** 双击 “2.获取网卡参数”，打开如图 7-1-5 所示的窗口。记得在获取之前，要禁用 VMnet8 网卡，启用 VMnet1 网卡，不然无法区分出哪一块网卡是 VMnet1。



图 7-1-5 获取网卡参数

- STEP 5** 单击 “3.修改网卡参数”，复制上一步骤中获取到的物理网卡的参数（如图 7-1-5 所示，为上面一条横线标记出的部分）后按下回车键，如图 7-1-6 所示。

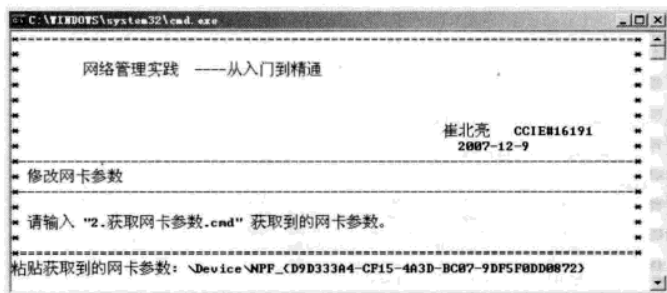


图 7-1-6 修改网卡参数

- STEP 6** 单击 “4.修改虚拟网卡参数”，用步骤 4 中的虚拟网卡参数（如图 7-1-5 所示，为下面一条横线标记出的部分）分别替换安全和语音机架中最后一行 SW2 交换机的对应网卡参数，如图 7-1-7 中被选中的部分。

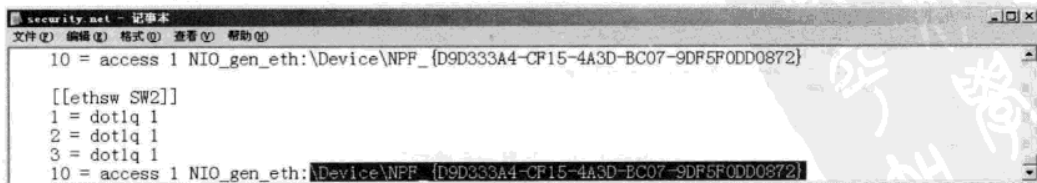


图 7-1-7 替换 SW2 的网卡参数

STEP 7 返回主目录。关闭所有窗口，完成实验机架的初始化。

STEP 8 双击“0.启动虚拟服务”打开控制台，会出现如图 7-1-8 所示的窗口。这是一个后台服务程序，实验结束前，请不要关闭该窗口。



图 7-1-8 Dynamips 服务界面

STEP 9 根据实验需求选择 Network、Security、Voice 或 CCNP 实验控制台，双击该文件，启动对应机架。如果要启动安全机架，双击“2.控制台 Security.cmd”会出现如图 7-1-9 所示窗口。

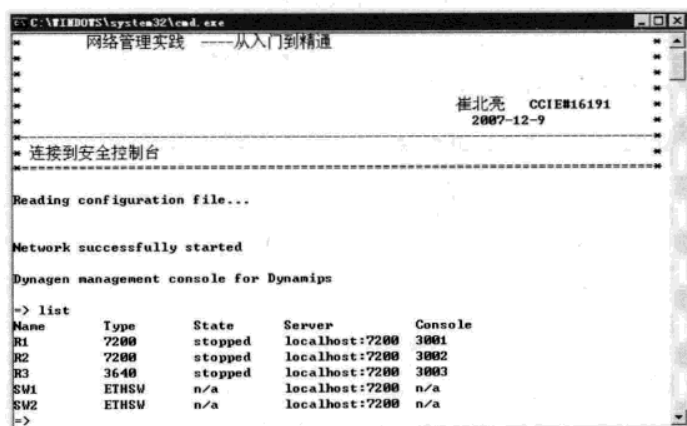


图 7-1-9 安全实验控制台

使用 list 命令查看路由器列表，然后使用命令 start R1 来启动路由器 R1，注意这里需要区分英文大小写。这时会出现如图 7-1-10 所示的提示信息，系统提示路由器 R1 没有配置 idle-pc 值，此时可以查看计算机的 CPU 利用率，一般都会在 50%以上。

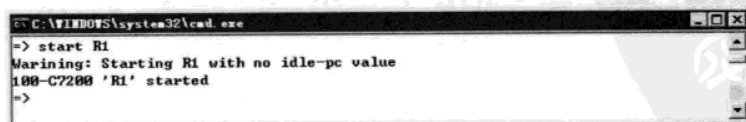


图 7-1-10 开启一台路由器

使用命令 idlepc get R1 来获得 idle-pc 值，稍后会出现如图 7-1-11 所示的画面。

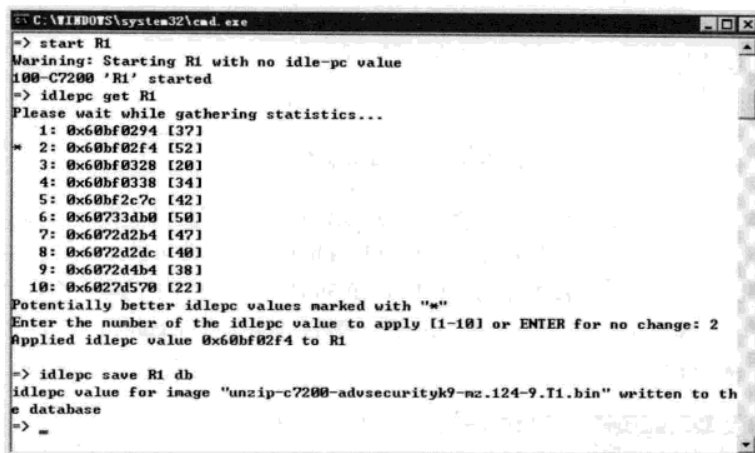


图 7-1-11 获取 idlepc 参数

带*号的 idlepc 值为系统推荐的最佳值，键入最佳选项前面对应的 1 到 10 编号，如果没有最佳推荐值，就选择 “[]” 括号中值最大的那个选项，回车后返回提示符状态。此时可以查看一下计算机的 CPU 利用率，一般都会降到 10% 以下。

为了避免每次启动路由器都需要调整 idlepc 参数，可以使用命令 `idlepc save R1 db`，把路由器 R1 的 idlepc 值保存，如图 7-1-11 所示。可以打开文件 “`dynamips\workingdir\idlepcdb.ini`”，如图 7-1-12 所示。该文件会记录下 IOS 文件名和对应的 idlepc 参数，以后再运行使用同样 IOS 文件的路由器时，自动使用此 idlepc 参数，也就是说对于很多个使用同一种 IOS 的路由器，idlepc 参数只需获取一次。

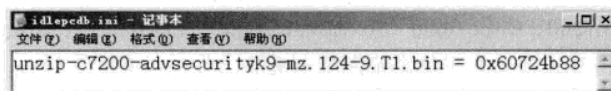


图 7-1-12 idlepc 文件

7.1.3 “Dynamips” 的使用方法

使用 “?” 可以查看所有可用的命令。注意设备名和命令是区分大小写的。

使用 “list” 命令可以查看实验台中的设备列表。

使用 “start” 命令可以开启路由器，如 “start R1” 用于开启 R1，“start /all” 用于开启所有设备。

使用 “stop” 命令可以关闭路由器，如 “stop R1” 用于 “stop /all”。

使用 “reload” 命令可以重启路由器，如 “reload R1” 用于 “reload /all”。到截稿为止，这款模拟器对该命令的支持仍很有限，建议不要使用此命令。可以使用 stop 和 start 组合来替代 reload 命令。

开启路由器后，使用 “telnet” 命令可以登录到路由器的 console 端口（路由器的控制台），例如，在安全机架的控制台中，“start R1” 开启路由器 R1，再执行 “telnet R1”，如图 7-1-13 所示。

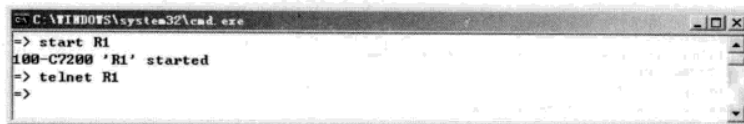


图 7-1-13 dynamips 的使用

输入“telnet R1”后按下回车键，打开 R1 的控制台窗口，如图 7-1-14 所示。或者也可以选择“开始”→“运行”命令，在运行栏中输入“telnet localhost 3001”即可登录到 R1 的控制台，也可以在远程计算机上“telnet 运行模拟器的计算机的 IP 3001”登录到 R1 的控制台。如果是 R2，只要把端口从 3001 改成 3002，R3 依次类推。为便于编辑，也可在“SecureCRT”软件中使用 Telnet 的方式打开路由器的控制台。

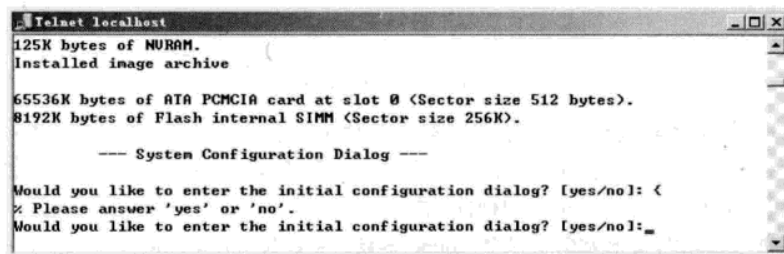


图 7-1-14 路由器 R1 的控制台

7.1.4 设计“Dynamips”的拓扑

至此，完成了 Network、Security、Voice 或 CCNP 机架的搭建。到目前为止，“Dynamips”支持的硬件型号有 Cisco 7200、Cisco 3600（3620/3640/3660）、Cisco 2691、Cisco 3725、Cisco 3745，这款模拟器软件还在不断完善，几乎每个星期都有更新。如果读者对这样的实验环境不满意，可以通过修改“dynamips\labini”目录下对应的文件来重新设计拓扑、修改设备型号、更换 IOS 版本等。例如，可以把安全机架的拓扑文件 security.net 中的 SW1 和 SW2 的网卡参数都设成 VMnet1 网卡的参数，则如图 7-1-2 所示的拓扑将变成如图 7-1-15 所示的拓扑。

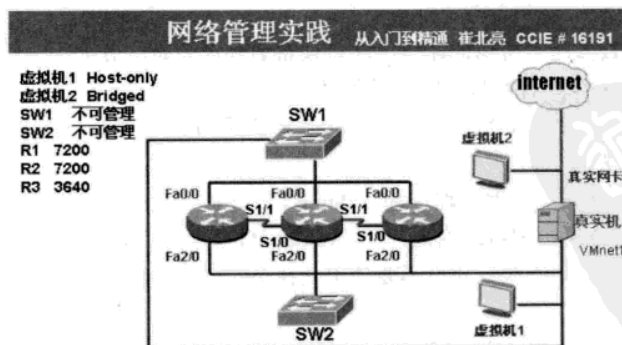


图 7-1-15 安全拓扑的改装

如果图 7-1-2 中安全拓扑的 SW1 和 SW2 的网卡参数换成物理网卡的参数, 将会呈现另外一个拓扑, 如果把虚拟机 1 和虚拟机 2 的网卡类型在 “Bridge” 和 “Host-only” 中调换, 呈现的也是一种新的拓扑。根据实验需要可以自由组合, 为了便于用户可以自己构建拓扑, 这里对 security.net 文件中的部分命令行解释如下, 斜体部分为注释。

autostart = false 开启机架后, 所有的设备都是停止状态, 需要手工启动。如果把这里的 false 改成 true, 则开启机架后, 所有的设备都自动开启。

[localhost] localhost 表示本机。

port = 7200 dynamips 服务使用的端口是 7200, 这里填入的端口要和 “0. 启动虚拟服务.bat” 文件中调用的端口一致。

workingdir = ..\workingdir\ dynamips 工作的目录在 dynamips\workingdir, 运行中产生的临时文件、保存的配置、idlepc.ini 文件等都保存在该目录。该目录下的所有文件都可以删除, 只是删除 idlepc.ini 后, 所有 IOS 的 idlepc 参数需重新获取, 建议可以删除 idlepc.ini 以外的其他文件。

[[router R1]] 第一台网络设备, 名字叫 R1。

image = ..\IOS\unzip-c7200-advsecurityk9-mz.124-9.T1.bin 该路由器使用的 IOS 文件名。可以根据需要换成所需版本的 IOS。

model = 7200 路由器的型号是 7200, 可以改成 dynamips 支持的其他型号设备, 如 3620, 3640, 3725 等。

console = 3001 该路由器使用的端口是 3001, 如果远程访问此设备的控制台, 可以 telnet 本机 IP 地址 + 端口号。机架中的所有设备使用的端口号不能相同。

npe = npe-400 网络处理引擎的类型是 npe-400, 7200 路由器支持 3 种网络处理引擎, 分别是 npe-225、npe-300、npe-400。

ram = 128 分配给该模拟器的内存是 128MB。

confreg = 0x2142 配置寄存器的值是 0x2142, 路由器重启时不加载用户配置文件, 如果需要加载用户配置文件, 可以把该值改成 0x2102。

exec_area = 64 可选参数, 利用主机内存的一部分来加快执行。

mmap = false 可选参数, 若不用 mmap=false, 启动和关机很慢, 运行速度也有不小的影响。

slot0 = PA-C7200-IO-FE 插槽 0 中插入的是一块以太网模块, 该模块配置一个快速以太网接口。具体哪个插槽支持什么样的模块, 模块上配置什么样的端口等, 根据设备型号的不同会有差异, 详细情况可以查询 “<http://dyna-gen.sourceforge.net/>”。

slot1 = PA-4T 插槽 1 中插入的是一块广域网模块, 该模块配置 4 个串行线接口。

slot2 = PA-FE-TX 插槽 2 中插入的是一块以太网模块, 该模块配置一个快速以太网接口。

f0/0 = SW1 1 路由器的 fast Ethernet 0/0 端口接交换机 SW1 的 1 端口。

f2/0 = SW2 1 路由器的 fast Ethernet 2/0 端口接交换机 SW2 的 1 端口。

s1/1 = R2 s1/0 路由器的 serial 1/1 端口接路由器 R2 的 serial 1/0 端口。

7.2 路由器基本硬件

Cisco 路由器系列包含有各种类型的路由器产品, 尽管这些产品的处理能力和所支持的接口数目具有相当大的差异, 但它们都由相似的核心硬件所组成。如图 7-2-1 所示, 展示了 Cisco 路由器系统的主要构成。尽管微处理器 (CPU)、ROM 和 RAM 的数目及所使用的端

口、介质转换器的数量和方式会因产品类别的差异而不同,但每一个路由器均含有如图 7-2-1 所示的硬件。本节通过对各类硬件功能的讨论,展示如何综合路由器的各部分构件而获得路由功能。

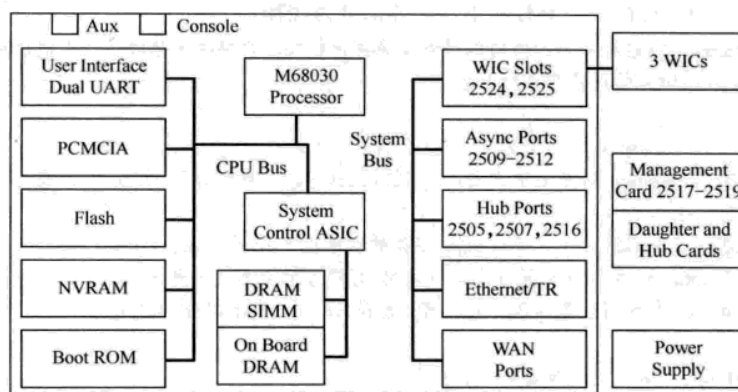


图 7-2-1 路由器的内部组成

1. 中央处理器 (CPU)

路由器的操作系统和用户通过控制台或远程登录所键入的命令,都是由 CPU 来执行的。因此, CPU 的处理性能直接与路由器的处理能力有关。相当于计算机的 CPU。

2. 闪存 (Flash)

闪存 (Flash Memory) 是一种可擦写、可编程的只读存储器。在大多数的路由器里,闪存是可选的,用于保留操作系统和路由器微代码映像。由于闪存存在更新内容时无须拔插芯片,因而花在这一项上的费用可节省芯片升级所耗的时间。只要有足够有效的空间,闪存可保留多于一个操作系统的映像,这对于测试新的系统映像是很有用的。路由器里的闪存也可用于通过 TFTP 传送操作系统映像到另一个路由器。另外,闪存可存放路由器配置文件的备份,这有利于当 TFTP 服务器失效或系统紧急恢复情况下的操作。这相当于计算机硬盘中的引导分区,用于存放操作系统。

3. 只读存储器 (ROM)

ROM 装载了系统加电时的诊断代码,这类似于通常计算机加电自检代码的功能。另外,在 ROM 中有一段启动程序用做操作系统代码的加载。尽管有很多种路由器需要通过拔插 ROM 芯片来实现软件升级,但也有其他采用不同方式的路由器。相当于计算机中的 CMOS 程序,用于开机自检。

4. 随机存取存储器 (RAM)

当设备在运行时, RAM 用来保存路由表,执行包缓冲,并对那些因某一端口超载而不能直接输出的包进行排队。另外, RAM 可缓存 ARP 中地址映射的信息,这样可减少地址解析消息的数量,并提高与路由器相连的局域网的通信能力。当路由器断电后, RAM 的内容就会丢失。它

相当于计算机中的内存，用于存放一些运行中的程序，断电后信息会全部丢失。

5. 非易失性随机存取存储器 (NVRAM)

NVRAM 即使在断电的时候仍保留其中的内容。若把配置文件保存到 NVRAM 中，则路由器可以很快地从断电灾难中得到恢复，而无须使用硬盘或软盘来备份路由器的配置文件。它相当于计算机中的硬盘，保存的信息重启后不会丢失。

由于 Cisco 路由器没有硬盘或软盘，配置文件通常存放在计算机中，这样，可使用文件编辑器方便地修改配置文件，通过网络的 TFTP 直接将配置文件加载到 NVRAM 上。当使用网络加载路由器的配置信息时，路由器应作为客户端而文件所在的计算机则应为服务器，即必须给计算机安装 TFTP 服务器软件来支持文件的存取。

6. 输入/输出端口和特定介质转换器 (I/O)

I/O 端口就是数据包进出路由器所通过的连接。每个 I/O 端口与一个特定介质转换器 (MSC) 相连，特定介质转换器为各种特定的介质，如以太网、令牌环局域网、RS-232 或 V.35 广域网提供物理上的转换接口。

在 Cisco 术语里，各种路由器功能（如路由协议更新和访问控制表）都与某个接口相关联，然而，实际上一个接口表示一个用接口子命令配置了的 I/O 端口。可以使用“show interface”命令来显示路由器中所有接口相关的信息。

如果在插进路由器的一个插槽中的通用适配卡上有一组端口，例如，在 7500、7200、3600 和 2600 型号的模块化路由器中，下述引用的形式用于指定一个特定的串行端口：

```
interface serial slot#/port#
```

除了串行端口，其他包括以太网、快速以太网、令牌环的端口也以相似的方式指定。运行安全机架，在安全机架的控制台中开启路由器 R1，再运行“telnet R1”，登录到 R1 的控制台，在特权模式下使用“show ip interface brief”命令来显示路由器上当前激活或未激活的网络接口，如图 7-2-2 所示。其中第一个快速以太网表示为安装在路由器 0 号插槽中的 0 号端口。通过使用 show interface 命令，除了可以显示路由器里的接口模块的 IP 信息外，还可以显示其他配置信息，如端口的速率、双工模式，数据链路层的封装协议，接收和发送数据包的情况等。

Interface	IP-Address	OK?	Method	Status	Prot
FastEthernet0/0	unassigned	YES	unset	administratively down	down
Serial1/0	unassigned	YES	unset	administratively down	down
Serial1/1	unassigned	YES	unset	administratively down	down
Serial1/2	unassigned	YES	unset	administratively down	down
Serial1/3	unassigned	YES	unset	administratively down	down
FastEthernet2/0	unassigned	YES	unset	administratively down	down

图 7-2-2 显示路由器上的所有网络接口

在 Cisco 7x00 系列设备中，可以在 1 个端口适配器卡上建立多个端口，而多个端口适配器卡可以安装在 1 个插槽中，因而上述引用的格式发生了变化。在这种情况下，下述命令格式将用来

引用一个特定的串行端口:

```
interface serial slot#/port-adapter#/port#
```

路由器中数据的流动情况是这样的。当从局域网中接收到一个包时,首先比较数据帧数据链路层的“目的 MAC 地址”与路由器接口的 MAC 地址是否相同,如果不同,则丢弃该帧,如果相同,它的第二层头信息被剥掉,然后把包放入 RAM;在 RAM 里,路由器检测包第三层的头信息,CPU 同时搜索路由表并匹配第三层地址以决定包应向哪里输出及以怎样的方式进行封装。

上述过程称为**交换处理模式**,这是因为每个包的处理过程都是由 CPU 查询路由表并决定将包发向哪里。Cisco 路由器还有一种称为快速交换的交换模式,这时路由器将目的 IP 地址和对应下一跳接口的信息保存在高速缓存 (Cache) 中并加以维护。

路由器通过保存先前从路由表中得到的信息来建立高速缓存中的内容,第一个到某一目的地址的包会使用 CPU 去查路由表,当得到该特定目的地址所对应下一跳接口信息后,将该信息插入到该路由器的快速交换缓存中。以后,当有发送到同一目的地址的新包要处理时,路由器无须查找路由表。这样,路由器以快得多的速度来交换包,大大降低了 CPU 的负载。

在如 7200 系列和 7500 系列包含有高端模块的特殊硬件体系结构中,快速交换模式会有所不同。然而,所有交换模式的原理在本质上是一致的,即在高速缓存中保留了目的地址与对应接口的映射关系。对于这种为“网流交换”的交换模式,高速缓存不单保存目的 IP 地址,还缓存源 IP 地址和上层 TCP 或 UDP 端口。传统方法只在如 7500 系列这种高端路由器平台上才采用这种交换模式。但在最新的 Cisco 操作系统 12.0 版本中,这种方式也被应用于如 2600 系列和 3600 系列的低端路由器平台上。

在交换处理模式中,路由器是基于每一个包来分配接口负载的。由于这里没有快速交换的高速缓存,每个包以循环方式发送到相继接口。尽管这里均匀地分配各接口的网络流量,但同时也增加了 CPU 的负担并降低了路由器的包转发率。在大多数情况下,最好使用快速交换模式并允许在多条网络路径上分配不等的流量。

7. 路由器初始化过程

当打开路由器的电源后,它会执行一个预定义的操作序列,还会根据预先的配置来执行其他的操作。为了进一步了解路由器的初始化过程,接下来说明路由器加电后的主要工作。

如图 7-2-3 所示是路由器初始化过程中所执行的主要功能的一个流程图。当打开路由器的电源后,它执行一系列诊断测试来校验其 CPU、存储器和接口的电路,由于这种测试在加电后即开始执行,所以它通常被称为**加电自检 (POST)**,当加电自检完成后,引导程序的加载器开始运行,其基本的功能是把操作系统的镜像复制到主存中。然而,这需要首先确定操作系统的镜像存放位置,这是因为镜像文件可能放在闪存或是 ROM 中,甚至可能是在网络上。

为了找到操作系统镜像文件的存放位置,引导加载器会检查配置寄存器的值。该值可以由硬

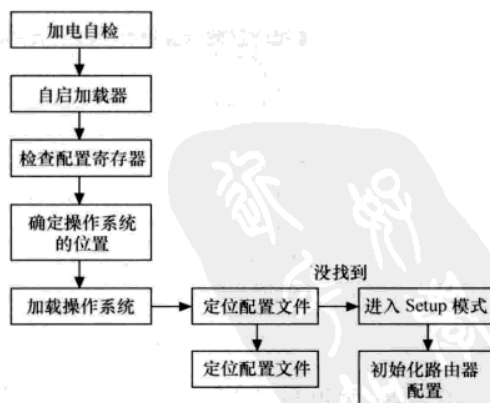


图 7-2-3 路由器的初始化过程

件跳线或软件来设置，这与路由器的型号有关。寄存器的设置指定了操作系统所在的位置并定义了其其他设备的功能，如路由器怎样响应控制台键盘的击键，以及是否将自检的信息显示到控制终端上等。

现在多数型号路由器的配置寄存器是存储在 NVRAM 里的一个 16 位的值，它并不是一个物理实体。在一些较老型号的路由器中，配置寄存器是一个具有 16 针的跳线，这是寄存器术语的起源。无论是软件还是硬件配置的寄存器，最后的 4 位（若是硬件寄存器，则是跳针）指明引导字段，引导字段告诉路由器配置文件的所在地。软件寄存器以 4 位十六进制数字表示，如 0X2142。在安全机架 R1 的控制台中输入“show version”命令来显示配置寄存器的值，如图 7-2-4 所示。“show version”命令除了可以用来显示配置寄存器的值外，还可以用来显示路由器的型号、IOS 的版本、接口类型和数量、NVRAM 大小等。

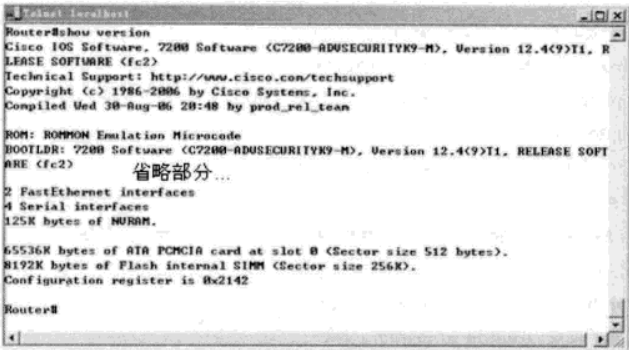


图 7-2-4 show version 的显示

每个十六进制数字代表 4 位二进制数，所以从右边数起的第一个数字即为引导字段。引导字段的取值可从 0~15。在前面的例子中，引导字段的值为“2”。如表 7-2-1 所示，说明了路由器是如何解释启动域中的数值。

表 7-2-1 路由器启动域中的数值	
自 启 域 值	路由器的解释
0	自动从 ROM 启动
1	RXBOOT 模式，如果有 Mini IOS，则加载
2~F	为 boot system 命令而检查在 NVRAM 中的配置文件

在大多数情况下，启动域取值为“2”，这将使路由器在配置文件中查找启动的命令。如果找不到，则路由器将加载在闪存中的第一个镜像文件。若闪存中无有效操作系统的镜像或根本找不到闪存，则路由器会尝试通过向广播地址发送 TFTP 请求操作系统镜像，从 TFTP 服务器上加载镜像文件。

当自启加载器读取了配置寄存器的值后，就知道了应从哪里加载操作系统的镜像并把它加载到 RAM 中。之后，路由器查找早先生成并保存在 NVRAM 中的配置文件。如果找到了，则路由器把它载入内存并逐行执行，这使得路由器可以根据预定义的网络环境开始工作。若先前在 NVRAM 中建立的文件并不存在，则路由器会显示“Would you like to enter the initial configuration

dialog?[yes/no]:”，如果回答“yes”，则执行被称为“建立会话”的预定顺序的提问来进行配置；如果回答“no”，则进行命令行配置模式。当操作者将配置信息被存储在 NVRAM 上，下次路由器重启时将加载保存在 NVRAM 中的配置。若把配置寄存器从右数起的第二位的数值置为“4”，则路由器在启动时会忽略 NVRAM 中的内容，这项功能可用来恢复路由器的密码时使用，实际中更多地被使用在实验环境中，当一个学员完成实验后，下一个学员只要重启设备，路由器启动时不会加载任何配置，注意图 7-2-4 中的配置寄存器值。

下面展示了当 Cisco 4500 路由器加电、自启、加载预定义的配置信息到内存时所产生的输出信息。注意显示信息末端的提示，否则初用者有时会白白地等待一段时间，而不知道只要按下回车键就可以进入系统了。

```
System Bootstrap, Version 5.2 (7b) [mkamson 7b], RELEASE SOFTWARE
(fc1)
Copyright (c) 1995 by cisco Systems, Inc.
C4500 processor with 8192 Kbytes of main memory
program load complete, entrypt: 0x80008000, size: 0x231afc
Self decompressing the image :
#####
#####
##### [OK]
Restricted Rights Legend
Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.
cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706
Cisco Internetwork Operating System Software
IOS (tm) 4500 Software (C4500-MR-M), Version 10.3 (8), RELEASE
SOFTWARE (fc2)
Copyright (c) 1986-1995 by cisco Systems, Inc.
Compiled Thu 14-Dec-95 22:10 by mkamson
Image text-base: 0x600087E0, data-base: 0x6043C000
cisco 4500 (R4K) processor (revision B) with 8192K/4096K bytes of
memory.
Processor board serial number 73160394
R4600 processor, Implementation 32, Revision 2.0
G.703/E1 software, Version 1.0.
Bridging software.
X.25 software, Version 2.0, NET2, BFE and GOSIPcompliant.
2 Ethernet/IEEE 802.3 interfaces.
```

```
1 Token Ring/IEEE 802.5 interface.  
2 Serial network interfaces.  
128K bytes of non-volatile configuration memory.  
4096K bytes of processor board System flash (Read/Write)  
4096K bytes of processor board Boot flash (Read/Write)  
Press RETURN to get started!
```

现在，已经了解路由器基本的硬件构件及其初始化过程，接下来介绍路由器的软件系统，以了解其中两个主要软件构件和路由器命令与软件构件的关系。

7.3 路由器基本软件

路由器中有两种主要的软件构件：操作系统的镜像文件和配置文件。操作系统文件可以决定路由器支持的功能，配置文件可以定制路由器的操作。

1. 操作系统镜像文件

操作系统镜像文件，也叫做 IOS。自启加载器根据配置寄存器所设定的内容定位操作系统镜像文件的位置，一旦找到镜像文件，便将其加载到内存的低端地址。操作系统的镜像文件包含一系列规则，这些规则规定如何通过路由器传送数据，管理缓存空间，支持不同的网络功能，更新路由表和执行用户命令。同一型号的路由器也有很多版本的 IOS，不同版本的 IOS 支持的功能不同，如是否支持 IP 高级特性、是否支持安全特性、是否支持语音特性等。例如，安全机架中的路由器加载支持 VPN 功能的 IOS，语音机架中的路由器加载支持语音功能的 IOS，网络机架中的路由器则只需加载最基本的 IOS 即可。基本功能的 IOS 支持的功能较少，但对硬件的要求相对较低，尤其是内存。不同版本的 IOS 对内存的需求也是不一样的，用户可以根据实际应用选择适合的 IOS 版本。

2. 配置文件

路由器第二种重要的软件构件就是配置文件。它由管理员创建，其中存放的配置内容由操作系统解释，操作系统指示路由器如何完成其中的各种功能。例如，配置文件可以定义一个或多个访问控制表，并要求操作系统设置不同的访问控制表来访问不同的接口，以提供流入该路由器的包的控制级别。尽管配置文件定义了如何完成影响路由器运行的各种功能，实际上是由操作系统来完成这些工作的，这是因为操作系统解释并响应配置文件中所述的要求。

配置文件的内容以文本形式保存，因此，其内容可在路由器控制台终端或远程终端上显示。这一点十分重要，因为当在一台与网络相连接的计算机上创建并修改配置文件然后使用 TFTP 将文件加载到路由器时，由于所使用的文本编辑器或字处理器通常会在保存的文件中加入一些控制字符，致使路由器不能识别文件的内容，所以当使用文件编辑器或字处理器创建并维护配置文件时，切记把文件保存为 ASCII 码的文本文件。配置文件保存后，就可存储在 NVRAM 中，并在每次路由器初始化时被加载到内存的高端地址空间中。

3. 数据流

可以通过探究路由器中的数据流动过程来了解配置信息,如图 7-3-1 所示,它展示了路由器中一般情况下的数据流图。

预先输入的命令告诉操作系统如何处理介质接口层的各种帧。例如,这些接口可以是以太网、令牌环网、光纤分布或数据接口 (FDDI),甚至可能是一个或一组如 X.25 的广域网端口或是帧中继 (Frame-relay) 接口。在定义接口时,必须提供一种或多种处理速率及其他参数来全面定义该接口。

一旦路由器获知它必须支持的接口类型,它就能校验到达数据的帧格式并按照该接口来生成正确的输出帧。另外,路由器能够使用适当的循环冗余校验码对到达帧的数据完整性进行校验。同样,路由器能为输出到该介质接口上的帧计算并添加循环冗余校验码。

路由表条目产生的方式由主存中的配置命令来控制。如果将其配置为静态路由条目,则该路由器不会与其他路由器交换路由条目信息。ARP 缓存是在内存中记录的 IP 地址与第二层 (MAC) 层地址映射关系的一块 RAM 区域。当接收到数据或准备发送数据时,数据将流入一个或多个优先级队列。在队列中优先级别低的业务量将被延时发送,路由器优先处理高优先级的业务量。若路由器能支持业务量的优先级别,则需要一些配置参数来告知路由器的操作系统如何完成优先处理任务,也就是 QoS (服务质量) 的配置。

当数据流入路由器后,它的位置及状态由保持队列 (hold queue) 来跟踪。路由表中的条目将指定包应从哪个目的接口转发出去。若包的目的地为局域网并且需要进行地址解释,路由器将使用 ARP 缓存来判定 MAC 层发送地址并进行封装;如果在缓存中找不到适当的地址,则路由器会生成并发出一个 ARP 包来请求所必需的第三层地址,俗称 ARP 请求包,目标设备收到 ARP 请求包后会进行应答,俗称 ARP 应答包。当确定包的地址和封装方法后,即可准备把包发送到输出端口。在包被传送到与介质连接的接口中的发送缓存区前,它会再一次被放到优先级队列中。

现在,已经了解了路由器中的两种软件构件,接下来探究如何编写路由器的配置文件。

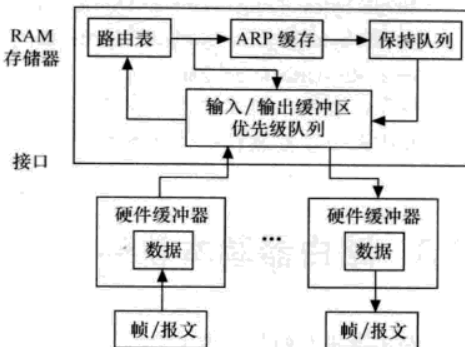


图 7-3-1 路由器中的数据流图

7.4 路由器的配置过程

在路由器第一次从包装盒取出加电后,可以使用 setup 命令,在运行该命令之前,应确保路由器的控制台 (Console) 端口与终端设备已用电缆连接。

1. 电缆连接的要点

在路由器上,系统的控制台端口被设置为数据终端设备 (Data Terminal Equipment, DTE) 端

口。由于在计算机上和在 ASCII 码终端设备上的 RS-232 通信也被设置为 DTE，所以不能用普通的直通电缆把路由器和终端设备连接在一起，必须使用全反电缆（又称翻转电缆）来连接。把全反电缆的一端接入路由器标志有“Console”的端口，另一端接 RJ-45 到 DB-9 的转接器，把转接器接在计算机的 COM 口上，如图 7-4-1 所示。现在更多的配置线缆都是一根整线，转接头和全反电缆已经固定在一起了。

当电缆正确连接后，在计算机上选择“开始”→“程序”→“附件”→“通信”→“超级终端”命令，打开如图 7-4-2 所示的对话框，选择对应的 COM 口。

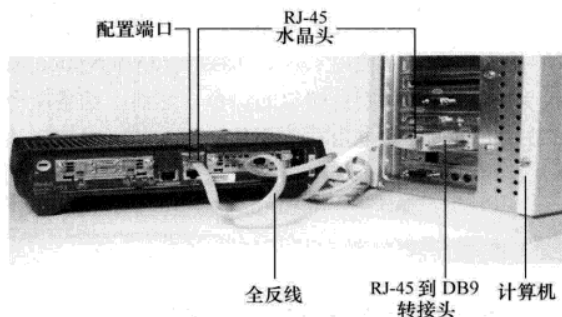


图 7-4-1 路由器初始配置接线图

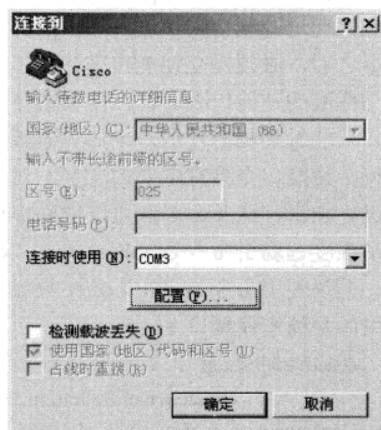


图 7-4-2 超级终端

2. 访问控制台

有多种通信程序可以用来通过控制台端口高效地访问路由器，SecureCRT 是一个更方便灵活、功能更齐全的通信程序，感兴趣的读者可以自行研究该软件的使用。

如图 7-4-2 所示，展示了使用超级终端程序来建立一个新的连接，该连接的名字由用户定义为 Cisco。由于是直接用电线连接计算机和路由器的控制台端口，设置“连接时使用”选项来说明该连接使用的是直接的串行通信口，现在很多新款笔记本电脑都不再集成 COM 口，解决的办法就是用一根 USB 转 COM 端口的转接线缆。在如图 7-4-2 所示的例子中，3 号串行通信口 (COM3) 被选择了。

一旦选择了适当直接连接的串行通信口并按下“确定”按钮，超级终端程序就会弹出一个对话框，来为连接所使用的串行通信口 COM3 设置参数。这个端口设置对话框可以对计算机通信参数配置或与路由器所使用的参数相匹配。如图 7-4-3 所示，端口设置对话框定义在计算机与路由器端口之间的通信设置，Cisco 路由器控制台端口的默认设置为 9600 比特、8 数据位、无奇偶检验和 1

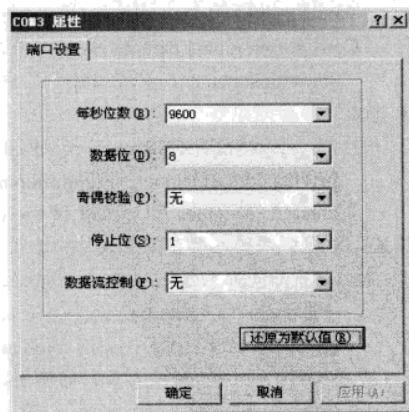


图 7-4-3 端口设置

停止位, 如图 7-4-3 所示。

3. 安装命令的要点

在 `setup` 命令的运行过程中, 可以为路由器取一个名字, 也可以为直接连接终端和虚终端设定口令。在 `setup` 命令即将进行结束时, 将提示是否接受刚输入的配置。

下面的配置是在安全机架 R1 上执行 `setup` 命令过程, 在这个例子中, 路由器的名字在先前的设置过程中被指定为 `Cisco7200`, 所以在输入提示符前显示了该名字。“#” 字提示符, 表明了当前正工作在路由器特权操作模式中, 其中斜体部分是加入的注释。注意, 使能口令被显示为 `cisco`。当有人通过控制台端口进入路由器并为使用可改变系统操作状态的 `EXEC` 特权命令而输入 `enable` 命令之后, 必须提交使能口令。除了使能口令外, 管理员还可以配置一个秘密使能口令, 它的作用与标准的使能口令一样, 但秘密使能口令以 `MD5` 的方式封装在配置文件中。当显示配置文件时, 只能看到秘密使能口令的封装版本, 这对于防止任何人通过获取路由器配置文件的复制而推知秘密使能口令具有重要的意义。对于一般的使能口令可以使用 `service password-encryption` 命令来进行加密, 这条命令还可以加密虚拟终端、附属端口和控制台端口的口令。然而, 这条命令的加密强度远弱于命令 `enable secret`, 以致很多在 Internet 上的自由软件在几分钟内就可以破译该密码。建议使用命令 `enable secret` 来加密口令。若同时使用秘密使能口令和通常的使能口令, 则起作用的是秘密使能口令。

```
Cisco7200#setup
--- System Configuration Dialog ---
Continue with configuration dialog? [yes/no]: y 是否要继续配置对话? 选择是或不是
At any point you may enter a question mark '?' for help. 任何时候可以输入? 号获取帮助
Use ctrl-c to abort configuration dialog at any prompt. 任何时候可以按 "Ctrl + c" 组合键放弃配置并退出
setup 模式
Default settings are in square brackets '[]'. 方括号显示的是默认设置, 直接回车表示接受默认配置
Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system 基本管理的 setup 配置可以为管理提供连接, 扩展管理的 setup
配置将会要求配置系统的每一个接口
Would you like to enter basic management setup? [yes/no]: y 要进行基本管理的 setup 配置模式吗?
Configuring global parameters: 全局配置参数
Enter host name [Cisco7200]: 输入路由器的名字, 方括号中是默认值, 如果接受, 不需重新输入,
直接按下回车键即可
The enable secret is a password used to protect access to
privileged EXEC and configuration modes. This password, after
entered, becomes encrypted in the configuration. 加密的使能密码被用来保护访问特权命令和进入配置
模式, 这个密码输入后在配置文件中会被加密
Enter enable secret [<Use current secret>]: cisco123 输入加密的使能密码
The enable password is used when you do not specify an
enable secret password, with some older software versions, and
some boot images. 没有加密的使用密码时, 将会使用这个使能密码
Enter enable password: cisco 输入使能密码
The virtual terminal password is used to protect
```

access to the router over a network interface. 虚拟终端密码用来保护从网络对设备的访问

Enter virtual terminal password: cisco 输入虚拟终端的密码

Configure System Management? [yes/no]: n 要配置系统管理吗?

Configure SNMP Network Management? [no]: y 要配置简单网络管理协议吗?

Community string [public]: 输入简单网络管理协议的团体字符串

Current interface summary 当前的接口汇总

Interface	IP-Address	OK?	Method	Status	Pr
ocol					
FastEthernet0/0	unassigned	YES	unset	administratively down	do
Serial1/0	unassigned	YES	unset	administratively down	do
Serial1/1	unassigned	YES	unset	administratively down	do
Serial1/2	unassigned	YES	unset	administratively down	do
Serial1/3	unassigned	YES	unset	administratively down	do
FastEthernet2/0	unassigned	YES	unset	administratively down	do

Enter interface name used to connect to the management network from the above interface summary: fastethernet0/0 输入从上面哪一个接口来管理网络, 这里选择的是 fastethernet0/0, 这里接口命令不可缩写

Configuring interface FastEthernet0/0: 配置网络管理接口

Use the 100 Base-TX (RJ-45) connector? [yes]: 该接口是 100Mbps 的双绞线吗?

Operate in full-duplex mode? [no]: 操作在全双工模式吗?

Configure IP on this interface? [no]: y 要给接口配置 IP 地址吗?

IP address for this interface: 192.168.1.2 输入接口的 IP 地址

Subnet mask for this interface [255.255.255.0]: 输入接口的子网掩码

Class C network is 192.168.1.0, 24 subnet bits; mask is /24

The following configuration command script was created: 下面的配置命令脚本被创建

```
hostname Cisco7200
.....
省略部分
.....
end
```

[0] Go to the IOS command prompt without saving this config.选项 0 放弃保存, 退出配置模式

[1] Return back to the setup without saving this config.选项 1 放弃保存, 重新执行 setup

[2] Save this configuration to nvram and exit.选项 2 保存配置, 退出配置模式

Enter your selection [2]: 输入您的选项

上述 setup 命令显示的一部分配置信息被从中删除, 可以在每个项目的输入位置键入问号来获得在线帮助。一旦配置完成后, 路由器会生成一个命令行脚本, 来显示最近更改过的配置项。此时, 有 3 种选择: 一是不保存改动, 返回 IOS 命令提示行; 二是不保存改动, 返回到 Setup 模式重新再来; 三是保存配置。命令执行过程中, 随时可以按 “Ctrl+c” 组合键终止 Setup 模式。

注意



本书中所有的实验都不使用配置对话，路由器启动后，询问 “Would you like to enter the initial configuration dialog? [yes/no]:”，全部输入 “n”，不进行配置对话。

上面输入命令的方式叫做 CLI (Command-Line Interface, 命令行界面)，命令解释器负责解释输入的命令，所以它对所输入的路由器命令是非常关键的。接下来介绍命令解释器的功能。

4. 命令解释器

正如其名称所显示的，命令解释器是用来解释输入路由器的命令的，如 EXEC 命令。命令解释器检查每一个命令，并假设它们是正确输入的，然后执行所请求的操作。

假设一个管理者在建立 (Setup) 过程中输入了一个口令，在用户能输入一个 EXEC 命令之前，必须用正确的口令才能登录到路由器。实际上，在使用 EXEC 命令时需要两个口令，这是由于有两级 EXEC 命令层次：用户级和特权级。登录到路由器后，用户得到访问用户级 EXEC 命令的权限，它可以让用户连接另一个设备，用户也可以提供一个名字作为逻辑连接，改变终端的参数，显示已打开的连接，并执行对 Cisco 系统来说并不关键性的操作。

如果用户用 EXEC 的 enable 命令得到特权级命令的访问权限，则可以输入配置信息，将特权级命令打开或关闭，锁住终端，执行其他关键性功能等。如果有人先前已用 enable password 或者 enable secret 配置命令进行了设置，为了使用 EXEC enable 命令，用户需要输入使用口令。

(1) 用户模式的操作。当用户登录到路由器后，就进入了用户命令模式，在本模式中系统提示符为 “>”。如果用户先前已为路由器命名了，则路由器的名字将会位于 “>” 之前，否则，默认的 router 将会显示在 “>” 之前。

(2) 特权模式操作。既然用户可以通过路由器的特权 EXEC 模式的操作配置这个路由器，那么也可以对这个操作模式加上一个口令。如前面所讲的，用户应该用 enable password 配置命令，这就是说用户首先进入没有口令保护的特权模式，然后再设置口令保护此模式。

为了进入特权 EXEC 模式，需要在提示符 “>” 之后输入 enable 命令，然后机器会提示输入一个口令。口令输入正确之后，提示符将变为 “#”，这表明用户已经在特权 EXEC 模式。如果用户在用户或者特权访问模式时使用命令 “?”，则特权模式命令集包括了所有用户 EXEC 命令。此外，特权用户模式还包括配置命令，这个命令允许用户提供一个对路由器在全局上产生影响的参数表。

用户可以通过一个终端、存储器或者网络配置路由设备。管理员经常用文本编辑器在网络上创建一个配置文件，并以 ASCII 文本文件形式保存文件，然后再用 TFTP 将此文件传送到路由器。为了完成这些工作，用户要在计算机上安装一个 TFTP 服务器程序，并指明 TFTP 服务器程序的根目录路径。

如图 7-4-5 所示，显示了在真实机上运行的 Cisco 的 TFTP 服务器软件时的情况，可以从 Network.rar 中找到这个软件。选择如图 7-4-4 所示的 “view” → “options” 命令，可以修改 TFTP 服务器的根路径。

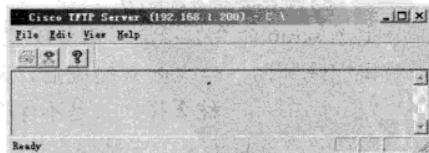


图 7-4-4 TFTP 服务器界面

如表 7-4-1 所示，总结了配置命令条目方法以及它们的操作结果，即使用不同的命令入口方法以及对访问和存储配置命令使用不同类型存储之间的联系。Cisco 在路由器操作系统的 10.3 版本开始改变了这些命令的格式，尽管旧版本的命令在某些方面将被停止使用，但是命令的两种形式在路由器最新的大多数版本中仍可使用，最新版本的命令用斜体字表示。

表 7-4-1 配置条目命令方法

命 令	操 作 结 果
configure terminal	进入全局配置模式
copy running-config startup-config	把正在运行的配置文件写入保存的配置文件
copy tftp running-config	把 TFTP 服务器中内容复制到运行配置中
write	保存配置，等同于 Copy running-config startup-config
show running-config	查看 RAM 中的内容，也就是正在起作用的配置
copy running-config tftp	将当前配置文件复制到 TFTP 服务器
show startup-config	查看保存在 NVRAM 中的配置
erase startup-config	清除 NVRAM 的内容，相当于清除保存的配置文件
reload	重启路由器

实验 7-1 用户自定义命令级别

路由器上默认有两级 EXEC 命令层次：用户级和特权级。用户级的权限级别是“1”，用户模式下可以执行所有级别 1 和级别 0 的命令；特权级的权限级别是“15”，特权模式下可以执行权限 0 到权限 15 的所有命令。默认情况下，级别 0 包括 5 个命令：disable、enable、exit、help、logout，权限 2 到权限 14 都没有使用，管理员可以把某些命令的权限级别从 15 降至 2 到 14 中的某个级别，并对这个级别设置 enable 密码，拥有该级别密码的用户将可以执行该级别及该级别以下的命令，如图 7-4-5 所示。

```

1 Router>show privilege
2 Current privilege level is 1
3 Router>clear line 1
4 % Invalid input detected at '^' marker.
5 Router>enable
6 Router#conf t
7 Enter configuration commands, one per line. End with CNTL/Z.
8 Router(config)#privilege exec all level 2 clear
9 Router(config)#enable secret level 2 cisco2
10 Router(config)#exit
11 Router#disa
12 Dec 11 11:06:54.955: %SYS-5-CONFIG_I: Configured from console by consoleble
13 Router>enable 2
14 Password:
15 Router#show privilege
16 Current privilege level is 2
17 Router#clear line 1
18 [confirm]
19 [OK]
20 Router#conf t
21 % Invalid input detected at '^' marker.
22 Router#
  
```

图 7-4-5 自定义命令级别

- 第 1 行, 执行 show privilege 命令。
- 第 2 行, 显示用户级的权限级别是 1。
- 第 3 行, 在用户模式下执行 clear line 1 命令。
- 第 4 行, 提示命令出错, 真正的原因是默认情况下, clear 是级别 15 的命令。
- 第 5 行, 执行 enable 命令, 进入特权模式。
- 第 6 行, 执行 conf t 命令, 进行全局配置模式。
- 第 7 行, 把所有 clear 命令及子命令的权限级别改成 2。
- 第 8 行, 把级别的使能密码设置成 cisco2。
- 第 9 行, 输入 disable 命令, 退出特权模式。
- 第 10 行, 输入 enable 2, 进入级别 2。
- 第 11 行, 输入密码 cisco2。
- 第 12 行, 执行 show privilege 命令, 显示当前的权限级别是 2。
- 第 13 行, 输入 clear line 1, 执行清线命令, 提示进行确认。现在发现级别 2 的用户可以执行 clear 命令了, 原因是 clear 命令已经被从级别 15 降级到级别 2 了。
- 第 14 行, 输入 conf t, 提示出错, 原因是因为 conf t 仍然是级别 15 的命令。

5. 配置命令种类

配置命令可分为 4 种类型, 具体内容如下。

(1) 全局配置命令。全局配置命令 (Global Configuration Commands) 定义了系统范围的参数, 包括路由器接口以及适用于这些接口的访问控制列表, 如果用户想要路由器运行, 有些全局配置命令是强制性的。例如, 用户必须配置自己的 LAN 和 WAN 口, 以便连接 Internet。其他的配置命令, 如创建并应用一个访问控制表, 则是可选的。用户进入路由器的配置模式后, 输入 “?” 命令, 路由器显示的一串全局配置命令是有效的。为了做到这些, 用户必须使用 enable 命令进入特权访问模式, 这是由于 configure 是一个特权命令。进入特权模式后, 输入命令 configure, 路由器的提示符改变为 router (config) #, router 是用户为路由器定义的名称, config 表示用户处于配置命令模式。在此模式中, 输入 “?” 子命令, 如图 7-4-6 所示, 列出了该路由器适用的全局配置命令。

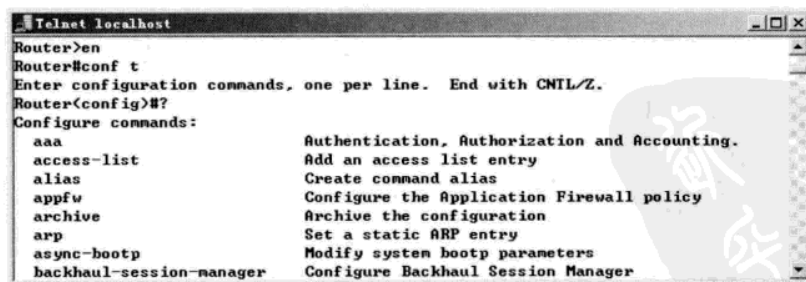


图 7-4-6 全局配置命令

如图 7-4-6 所示, 使用命令 “?” 可以得到一组用于某个路由器的全局配置命令, 这种内嵌

的帮助系统尽管在某些方面令人费解，但还是提供了一些信息，可以使用户不必再求助于参考书。例如，在日常繁琐的 LAN 和 WAN 设备的配置中，很容易就记住了由 Cisco 分配给不同类型的访问控制的数目、ICMP 类型的代码以及其他相似的信息。通过使用命令“？”，用户可以得到所需的信息。如图 7-4-7 所示，显示了使用命令“？”得到的有关访问控制的信息，图中内容显示了一串和不同类型的访问控制列表相联系的数字范围。

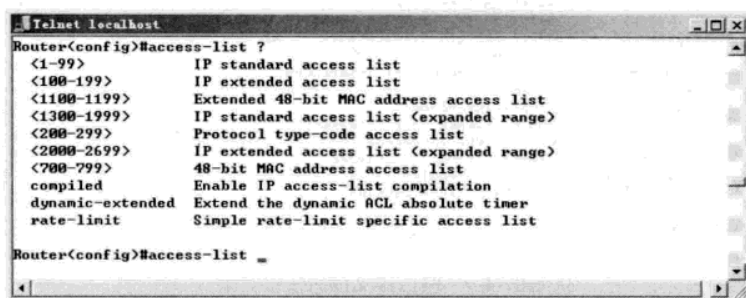


图 7-4-7 获取路由器访问控制表的联机帮助

如图 7-4-7 所示，可以注意到访问控制表的在线帮助对路由器支持的不同访问控制表的数字范围给出了基本概括。针对访问控制列表后续有专门的章节介绍。

(2) 接口命令。接口命令定义一个 LAN 和 WAN 的接口的特征。如图 7-4-8 所示，举例说明了使用 show interfaces serial 1/1 后跟“？”命令显示的部分接口配置命令列表，这些命令适用于串行接口。

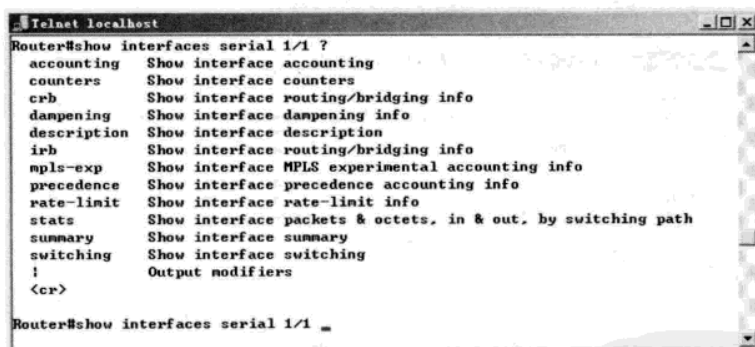


图 7-4-8 显示接口信息的命令

interface 命令允许用户既能将一个网络分配给一个特定的端口，又能为接口配置一个或多个具体参数。最常用的 interface 命令格式如下：

```
interface type number
```

此处 type 指出配置的接口类型，如图 7-4-9 所示，列出了路由器上支持的接口类型。

(3) 线路命令。线路命令 (Line Command) 修改串行终端线路的操作。如图 7-4-10 所示，举例说明了用 line 命令后跟“？”命令显示的一个可以用来配置的线路命令。

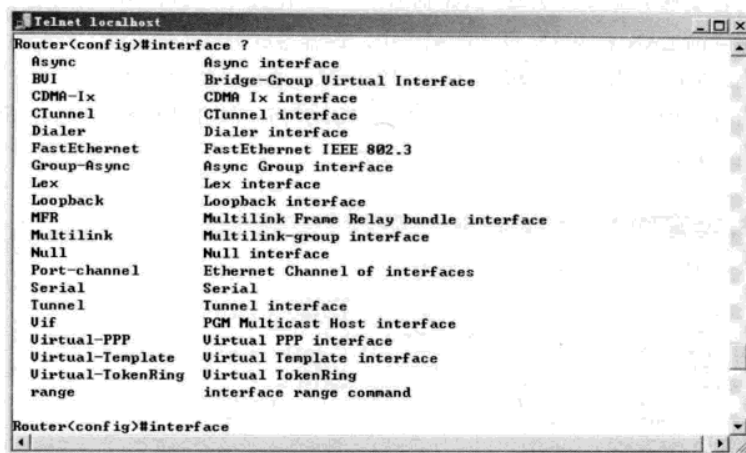


图 7-4-9 路由器支持的接口类型

可以使用 show line 命令查看当前线路正在被使用的情况, 如图 7-4-11 所示。从图中可以看到 line 0 (相当于 console 端口) 前面有一个 “*”, 表示 console 端口正在被使用; 还看到 line 2 (相当于 vty 0, 第一个 telnet 登录的用户) 前面也有一个 “*”, 表示有一个用户通过 telnet 登录到该路由器, 可以使用 clear line 2 断开该用户的连接。如果需要查询是哪一個用户或从哪一个 IP 地址登录路由器的, 可以使用 show user 命令查看。

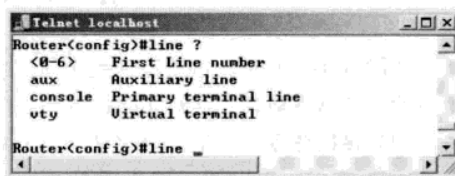


图 7-4-10 路由器支持的线路命令

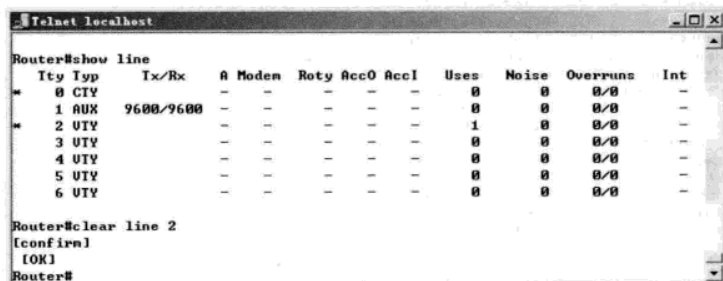


图 7-4-11 查看路由器的连线

(4) 路由器子命令。路由器子命令 (Router Subcommands) 配置 IP 路由选择协议的参数, 并跟在 router 命令之后使用。如图 7-4-12 所示, 说明了在命令 router 后加上 “?” 命令后, 显示了此路由器支持的路由协议列表。

6. 简写命令

在路由器上输入一个命令时, 并不需要将整词输入。一般来说, 命令的 3~4 个字母就可以使路由器分清所用的命令, 并执行相应的动作。例如, 以下命令:

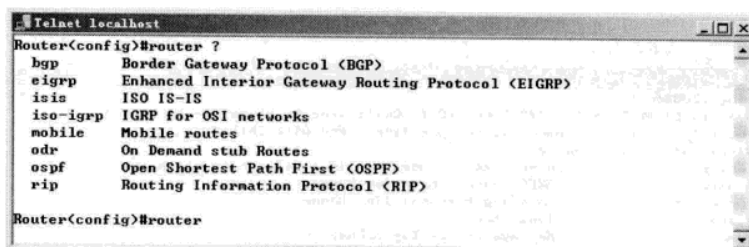


图 7-4-12 路由器支持的路由协议列表

```
Router#show interface serial1/1
```

能简写为:

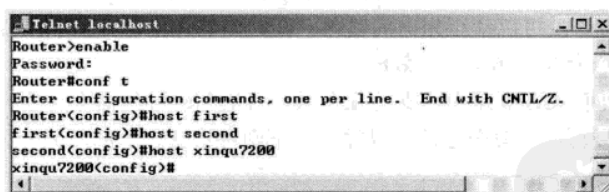
```
Router # sh int s1/1
```

当有疑问时, 首先输入命令最前面能记得清的字母, 然后再加一个“?”, 这样可得到路由器的上下文在线帮助, 路由器将会显示所有字符相匹配的命令, 然后, 用户可以输入足够多的字符来完成命令的输入。“?”是路由器用户的朋友, 通过使用内嵌的上下文敏感的帮助系统, 可以使一个 Cisco 的初学者也能确定正确的命令语法。

7. 一般控制台操作

首先介绍路由器完成一般操作的过程, 如为分配主机名、产生旗帜消息以及设置时间和日期等。完成这些之后, 还介绍如何对控制台操作进行调整, 如果需要可再产生日志消息。

(1) 主机名分配。用户路由器的命名与重命名是通过命令 `hostname` 完成的。由于命令 `hostname` 是一个配置命令, 所以用户必须在特权模式下才能对主机名进行设置或重新设置。如图 7-4-13 所示, 举例说明了通过执行命令 `enable` 进入特权模式, 再输入 `conf t` 命令进入全局配置后, 假设路由器先前没有被命名, 因此默认名为 `Router`, 执行命令 `Host first`, 将路由器的名称改为 `first`, 接下来的单词 `second` 表示将路由器的名称改为 `second`, 但在实际中, 主机名称应有某种意义, 特别是当用户管理一个复杂的网络时。如图 7-4-13 所示, 最后一个 `hostname` 命令使用了一个更有意义的名称 `xinqu7200`, 这样就能比较好地描述路由器的位置与类型。

图 7-4-13 使用 `hostname` 命令设置路由器的名称

(2) 旗帜创建。当执行某种初始化动作时, 显示所谓“旗帜”信息。在一个 Cisco 路由器环境中, 用户可以看到几种不同的旗帜消息。如图 7-4-14 所示, 举例说明了 `banner` 命令后跟参数“?”所显示的路由器所支持的旗帜消息。图中, `LINE` 不是一个旗帜选项, 而是用户输入旗帜文本消息的方式。例如, 为了显示消息 `welcome`, 用户在此单词前后需输入一对分界符, 如“#”, 因此, 这个线路命令输入变为 `#welcome#`。注意要小心选择作为分界符的字符, 它们不能在旗帜消息中

被使用。

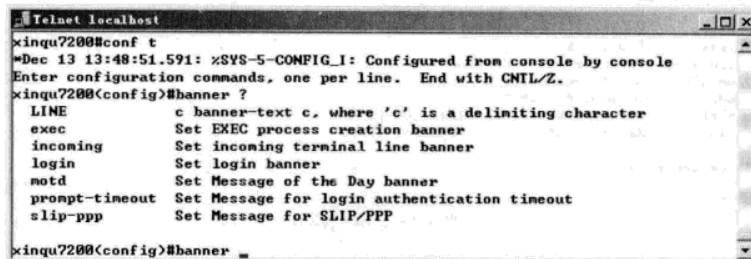


图 7-4-14 旗帜信息

Banner exec 命令是当一个线路命令激活时用来显示消息的，如出现一个虚拟终端 (VTY) 连接或一个相似的 EXEC 过程时，或者当用户需要一个 telnet 的登录连接路由器时，命令 banner login 也会导致消息的显示。这样，命令 banner login 的结果消息比 banner exec 命令的任何消息都早。其他的 banner 命令选项如图 7-4-14 所示，包括 incoming、motd、prompt-timeout 和 slip-ppp。

当一个网络上的 incoming 连接初始化时，显示 banner incoming 消息，motd 子命令允许用户说明日期信息，当任何时候与路由器任何类型的连接发生时，motd 旗帜将显示出来，因此，可以考虑用它来传送影响用户的信息。例如，命令：

```
Router(config)#banner motd * This router will be power off from 10:00 to 23:00 today*
```

当用户连接到路由器时，提示这台路由器今天从早上 10 点到晚上 23 点将被关闭。当一个登录认证过程超时时，promptpt - timeout 子命令显示一个消息。而 slip-ppp 子命令是用来显示通过其他协议访问的消息。

可以注意到旗帜消息的显示是有特定顺序的，而并不管用户设置旗帜信息命令的次序。如果有旗帜 motd，那么它的信息将会最先显示；接着，若配置了旗帜命令 incoming，它的旗帜信息将跟着显示；如果有一个用户登录，而又配置了旗帜命令 EXEC，它的旗帜信息也会显示出来。

使用加 no 的 banner 命令可以删除先前的一个条目，例如，在一个 banner login 命令之后输入一个 no banner login 命令，可以禁止先前的输入。在路由器任何命令前加上 no，对返回路由器的默认参数和清除前一个命令的影响是有效的。

(3) 设置日期/时间。Cisco 路由器支持几个系统日历和时钟的命令。用户可以用 clock set 命令设置路由器的系统日历，在命令之后可以输入以下两种格式之一的时间和日期：

```
hh:mm:ss day month year
hh:mm:ss month day year
```

用户输入日期的天数时用数字形式，而用英文表示月份，系统自动识别两种不同格式的输入。

(4) 终端定制。用户可以使用 terminal 命令来改变终端的参数以满足用户特殊的要求。一旦连接上路由器，用户可以通过 show terminal 命令来得到当前终端线路的信息。

下面举例说明一些普通终端参数的更改方法。

路由器会默认缓存用户输入的最近 10 条命令，可以通过上下箭头键调出历史命令。如果想缓

存更多命令，可以使用 `terminal history size` 设置，假设要缓存最近使用过的 20 条命令。使用下面的命令：

```
Router>terminal history size 20
```

假设要将终端设为 132 列，长为 32 行。首先使用 `terminal width` 命令，紧跟需要设置的列的数目，输入如下：

```
Router>terminal width 132
```

为了将屏幕设为 32 行，需使用 `terminal length` 命令，使用以下命令：

```
Router>terminal length 32
```

而加上 `no` 前缀的两个命令（`terminal no width`，`terminal no length`）将会重新将参数设置为默认的 80 列，24 行。

通过终端可以改变宽度和行数，但编辑起来还是有诸多不便，建议使用前面提到过的 SecureCRT 软件进行连接。

（5）日志。通过日志消息观察路由器的变化状态是一个被许多人所忽视的重要细节。日志消息是由 EXEC 特权模式控制的，一旦进入 EXEC 特权模式，用户可在全局配置命令中使用一个或多个子命令。如图 7-4-15 所示，列举了一个特定路由器支持的 `logging` 子命令选项。

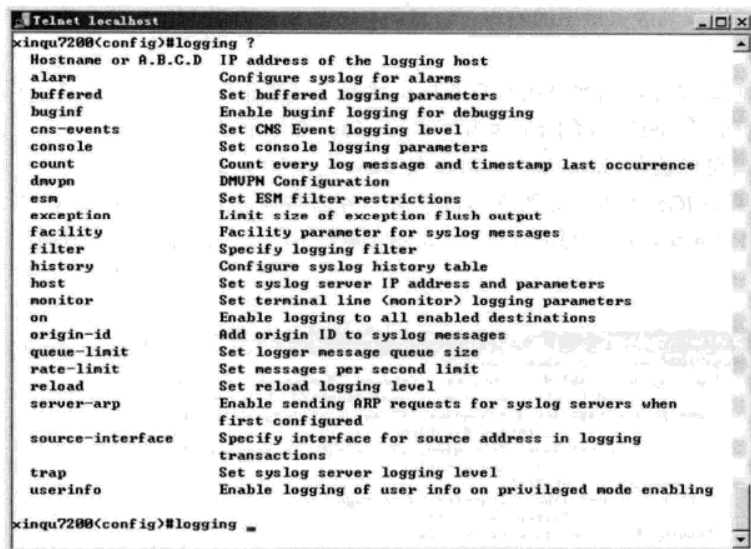


图 7-4-15 logging 日志选项

为了打开或关闭日志消息，用户可输入 `logging on` 命令或者 `no logging on` 命令。

`logging buffered` 配置命令允许信息写入存储器，如图 7-4-16 所示，举例说明了有效使用这个命令的各种选项，这些选项对于 `logging console`、`monitor`、`history` 以及 `trap` 等子命令也适用。如图 7-4-16 所示，可用 `logging buffered` 命令设置日志消息保存到存储器中，并将一块内存空间分配给日志消息，同时用户可以指定 8 种不同类型的消息显示和登录情况。早期版本的 IOS 使用数字优先级和不同的关键字允许用户限制日志消息被传送到控制台或者是其他地方。最后一点值得注意的是，再次用带 `no` 的命令将取消缓冲区的使用，并将恢复成将消息

显示到控制台终端。

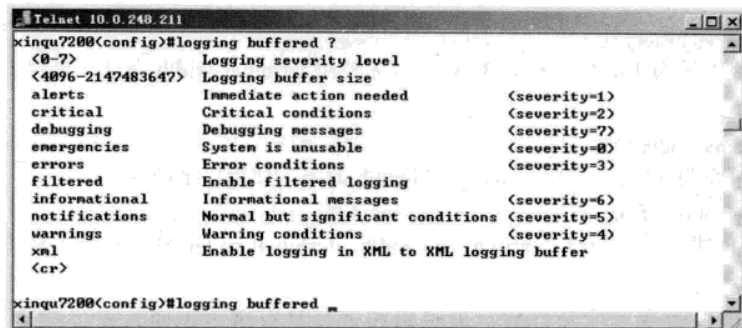


图 7-4-16 logging buffered 选项

logging trap 命令限制传送给系统日志服务器消息的数量。用户需要在命令之后输入如图 7-4-16 所示列出的一个关键字，这将限制向服务器发送那些与关键字同级或更高级的日志消息。

logging monitor 子命令和 trap 子命令相似，它负责限制哪些消息传送给终端。消息的记录是基于命令之后同级或高级关键字的输入。如图 7-4-16 所示，适用于 trap 命令的关键字同样也适用于 monitor 命令。

show logging 命令，它允许用户查看日志状态。这个命令的作用如图 7-4-17 所示。Show logging 命令前面加“do”的原因是因为所有的 show 命令都要在特权模式下输入，如果不退回到特权模式下就可以输入 show 命令，可以在 show 之前加上 do，该命令并不能总是这样使用，它依赖于所使用的 IOS 版本。如图 7-4-17 所示，中部提示默认日志空间为 8192 字节，如前面提到的，用户可以对缓冲区空间进行调整。如图 7-4-17 所示，下部显示路由的端口 UP 或 DOWN 的信息。

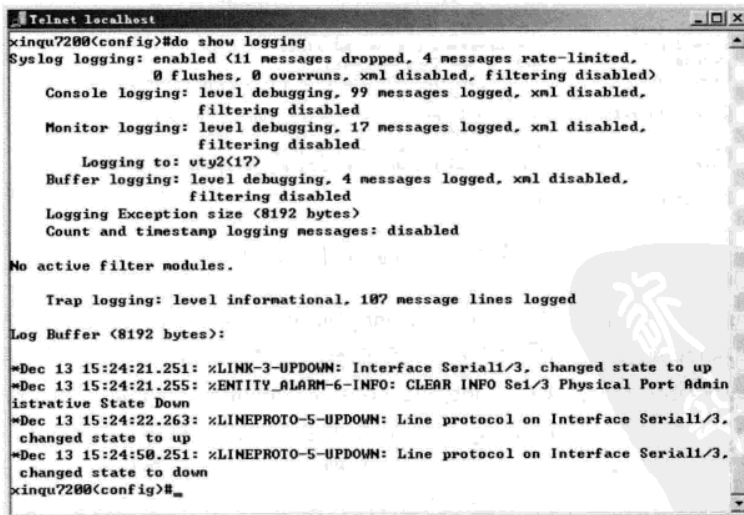


图 7-4-17 显示缓存中的日志

值得一提的是,如果是通过 telnet 方式登录到路由器,将不能看到实时的日志或 debug 消息,实时的日志和 debug 消息默认情况下只向 console 端口控制台输出。如需向 telnet 终端用户输出,需要先 telnet 登录路由器,然后在特权模式下输入 terminal monitor,开启虚拟终端监控即可。

实验 7-2 配置日志服务器

通过缓冲区来存放日志有很多不足,一是因为缓冲区空间有限,不可能存储大量的日志;二是因为缓冲区中的内容在断电或路由器重启的情况下都会丢失。长期大量的保存日志可以使用日志服务器。在真实机上安装 network.rar 包中的“Kiwi_Syslogd.exe”软件,让真实机充当日志服务器。如图 7-4-18 所示,配置路由器后,路由器将会把日志消息发送给“真实机”。

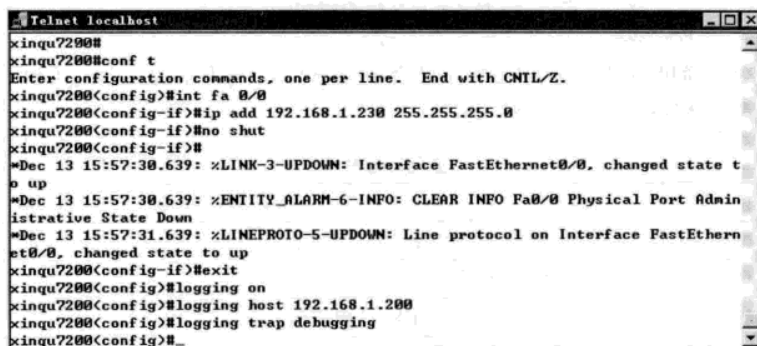


图 7-4-18 配置日志服务器

图中的命令解释如下,斜体部分是注释部分。

```
xinqu7200#conf t  进入全局配置模式
xinqu7200(config)#int fa 0/0  进入路由器的 Fa0/0 接口,安全机架的 Fa0/0 口和真实机的物理网卡连接
                              在同一个网段
xinqu7200(config-if)#ip add 192.168.1.230 255.255.255.0  给路由器的 Fa0/0 口配置 IP 地址
xinqu7200(config-if)#no shut  开启路由器的 Fa0/0 口,默认情况下,路由器的端口处在关闭状态
xinqu7200(config-if)#exit  返回上一级
xinqu7200(config)#logging on  开启日志
xinqu7200(config)#logging host 192.168.1.200  把日志发送到日志服务器 192.168.1.200
xinqu7200(config)#logging trap debugging  发送日志的级别是 debugging,级别 7,也就是发送所有级别的日志消息。
```

配置完成后,路由器将把相关的日志消息都发送到真实机 192.168.1.200。如图 7-4-19 所示,路由器已经把日志送到日志服务器,配置日志服务器,可以设置每天产生一个日志文件。

8. 安全管理要素

前面对路由器基本硬件和软件的构成以及它的 EXEC 命令模式进行总的介绍,接下来简单地介绍路由器的安全管理问题。不管用户打算如何使用一个路由器,一些关键的与安全相关的方面是必须考虑的。这些方面包括建立口令,以便能安全地访问路由器,配置 ACL (Access Control List,

访问控制列表），以便通过路由器控制可接受的数据流量。

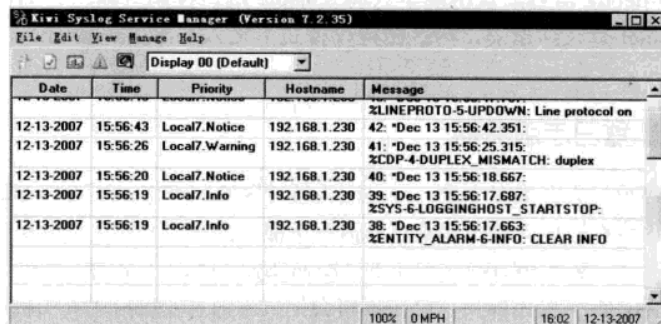


图 7-4-19 日志服务器

(1) 口令控制。通过使用如表 7-4-2 所示的命令，用户可以控制对路由器的访问，对特权 EXEC 命令的访问，甚至对通过口令访问虚拟终端。

表 7-4-2 安全管理命令	
命 令	操 作 结 果
line console 0	在控制台终端建立一个口令
line vty 0 4	为 telnet 连接建立一个口令
enable password	为进入特权级 EXEC 模式建立一个口令
enable secret	用 MD5 加密建立一个进入特权级 EXEC 模式口令
service password-encryption	保护口令的显示，使用 show running-config 看不到所有的口令

如图 7-4-20 所示，演示了线路口令的配置，经过这次设置之后，真实计算机就可以远程登录到路由器的配置模式。一般来说，用户在口令中考虑使用字母数字混合的口令是被着重强调的，它可以减少黑客使用字典攻击成功的可能。还要注意密码的前导空格被忽略，而结尾空格是有效的。

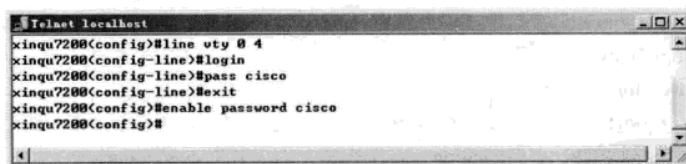


图 7-4-20 配置路由器的远程访问

在真实计算机中，选择“开始”→“运行”命令，在运行对话框中输入“telnet 192.168.1.230”，打开 DOS 窗口，如图 7-4-21 所示，系统要求输入虚拟终端的密码，输入“cisco”，验证密码正确，进入到用户模式。再输入“enable”，输入密码“cisco”，进入到特权模式。

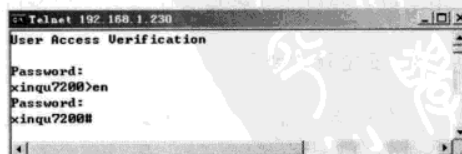


图 7-4-21 远程登录窗口

注 意



如图 7-4-21 所示,也可以对路由器进行配置,这是通过 telnet 192.168.1.230 命令完成的,通过路由器的 Fa0/0 端口对路由器访问,也称为虚拟终端访问(VTY)。而在安全机架的控制台中,可能通过 telnet R1,对 R1 进行配置,这时连接的是 R1 的控制台,因为虚拟路由器都是不可见的,更无法连接 console 端口。在安全机架的控制台中, telnet R1 相当于是连接到虚拟路由器 R1 的 console 端口,通过配置线对 R1 进行初始化配置,以后就可以通过网络线对 R1 进行远程配置了。

(2) 访问控制表。安全控制的第二方面可以通过路由器控制包的流量。要做到这些,用户要配置一个或多个访问控制表,并将这些表提供给一个或多个接口。有关访问控制列表的用法,本书第 11 章将专门进行介绍。这里仅举一个简单的例子,如图 7-4-22 所示的配置,实现仅有 IP 地址为 192.168.1.200 的主机可以 telnet 登录到该路由器。

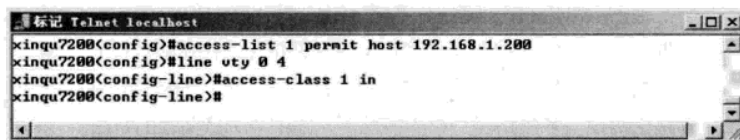
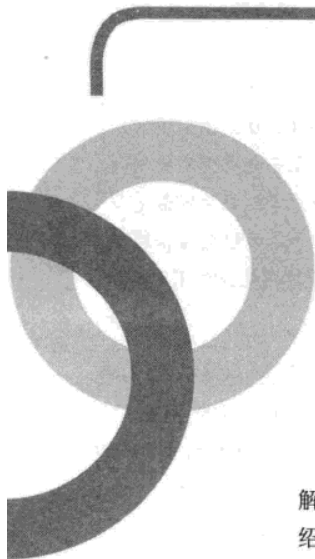


图 7-4-22 限制可登录路由器的 IP 地址



第8章 路由

Chapter 8

本章通过介绍 TCP/IP 网络中路由器的基本工作原理，讲解 IP 路由器的主要功能，解释静态路由协议、动态路由协议以及内部网关协议和外部网关协议的概念。同时介绍了目前最常见的直连路由、静态路由、默认路由和动态路由（包括 RIP 和 OSPF）这几种路由协议，并结合实验演示了这几种常见路由协议的配置。通过学习本章，读者可以根据实际情况，正确地选择使用路由协议，并配置路由协议；可以能够分析在多种路由协议或多条路径并存的情况下，路由器选择路径的方法。

8.1 路由知识

近十年来，随着计算机网络规模的不断扩大，大型互连网络（如 Internet）迅猛发展，路由技术在网络技术中已逐渐成为关键部分，路由器也随之成为最重要的网络设备。用户的需求推动着路由技术的发展和路由器的普及，人们已经不满足于仅在本地上网络上共享信息，而希望最大限度地利用全球各个地区、各种类型的网络资源。而在目前的情况下，任何一个有一定规模的计算机网络（如企业网、校园网、智能大厦等），无论采用的是快速以太网技术、FDDI 技术，还是 ATM 技术都离不开路由器，否则就无法正常运作和管理。

8.1.1 网络互连

把一个网络同其他的网络互连起来，从网络中获取更多的信息和向网络发布自己的消息，是网络互连的最主要的动力。网络的互连有多种方式，其中使用最多的是网桥互连和路由器互连。

1. 网桥互连网络

网桥工作在 OSI 模型中的第二层，即数据链路层。完成数据帧（Frame）的转发，主要目的是在连接的网络间提供透明的通信。网桥的转发是依据数据帧中的源地址和目的地址来判断一个帧是否应转发和转发到哪个端口。帧中的地址称为“MAC”地址或“硬件”地址，一般就是网卡的地址。

网桥的作用是把两个或多个网络互连起来,提供透明的通信。网络上的设备看不到网桥的存在,设备之间的通信就如同在一个网上一样方便。由于网桥是在数据帧上进行转发的,因此只能连接相同或相似的网络(相同或相似结构的数据帧),如以太网之间或以太网与令牌环之间的互连,对于不同类型的网络(数据帧结构不同),如以太网与 X.25 之间,网桥就无能为力了。

网桥扩大了网络的规模,提高了网络的性能,给网络应用带来了方便,在早期的网络中,网桥的应用较为广泛。但网桥互连也带来了不少问题。一个是广播风暴,网桥不阻挡网络中广播消息,当网络的规模较大时(几个网桥连接多个以太网段),有可能引起广播风暴,导致整个网络被广播信息充满,直至完全瘫痪。第二个问题是网络互连,网桥是数据链路层的设备,无法完成不同 IP 网段间的互连,也就是不管互连的设备有多少台,这些设备只能在同一个 IP 子网中,如果一个部门和另一个部门处在不同的 IP 子网中,网桥将不能完成网络的互连。第三个问题是网络安全,网桥无法实现连接不同的 IP 子网,解决的办法就是把两边的网络设备配置在同一个 IP 子网中,当与外部网络互连时,把内部和外部网络合二为一,成为一个网络,双方都自动向对方完全开放自己的网络资源,这在很多网络中都是不允许的。

通过网桥与外部网络互连显然是难以接受的,出于安全和性能方面的考虑,很多企业内部会根据分工划分成不同的 IP 子网,网桥也无法完成内部不同 IP 子网间的互连。

2. 路由器互连网络

路由器互连与网络的协议有关,本章仅讨论 TCP/IP 网络的情况。路由器工作在 OSI 模型中的第三层,即网络层。路由器利用网络层定义的“逻辑”地址(即 IP 地址)来区别不同的网络,实现网络的互连和隔离,保持各个网络的独立性。路由器不转发广播消息,而把广播消息限制在各自的网络内部。发送到其他网络的数据包先被送到路由器,再由路由器转发出去。

IP 路由器只转发 IP 分组,把其余的部分挡在网内(包括广播),从而保持各个网络具有相对的独立性,这样可以组成具有许多网络(子网)互连的大型网络。由于是在网络层的互连,路由器可方便地连接不同类型的网络,只要网络层运行的是 IP 协议,通过路由器就可互连起来。

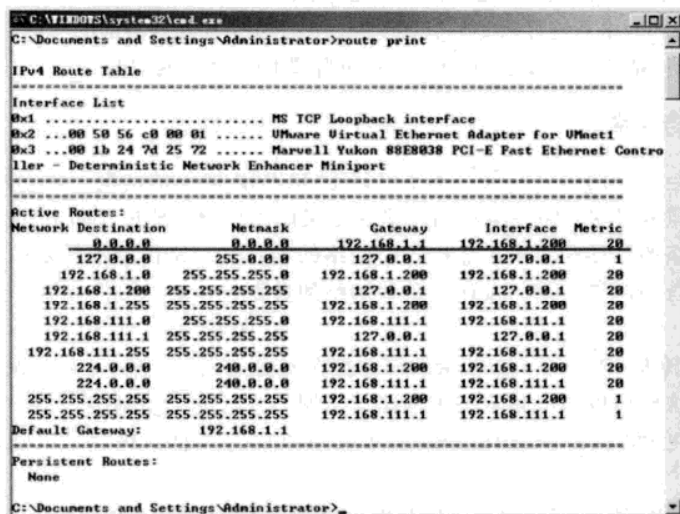
网络中的设备用它们的网络地址(TCP/IP 网络中为 IP 地址)互相通信。IP 地址是与硬件地址无关的“逻辑”地址。路由器根据 IP 地址来转发数据,IP 地址的结构有两部分,一部分定义为网络号,另一部分定义为网络内的主机号。目前,在 Internet 中采用子网掩码来确定 IP 地址中网络地址和主机地址。子网掩码与 IP 地址一样也是 32 位,并且两者是一一对应的,并规定子网掩码中数字为“1”所对应的 IP 地址中的部分为网络号,为“0”所对应的则为主机号。网络号和主机号合起来,才构成一个完整的 IP 地址。同一个网络中的主机 IP 地址,其网络号必须是相同的,这个网络称为 IP 子网。

具有相同网络号的主机之间可以直接通信,要与其他 IP 子网的主机进行通信,则必须经过同一网络上的某个路由器或网关(gateway)。不同网络号的 IP 地址不能直接通信,即使它们连接在一起,也不能通信。

路由器有多个端口,用于连接多个 IP 子网。每个端口的 IP 地址的网络号要与所连接的 IP 子网的网络号相同。不同的端口为不同的网络号,对应不同的 IP 子网,这样才能使各子网中的主机通过自己子网的 IP 地址把要发送出去的 IP 分组送到路由器。

8.1.2 路由原理

当 IP 子网中的一台主机发送 IP 分组给同一 IP 子网的另一台主机时, 它将直接把 IP 分组送到网络上, 这样对方就能收到。而要送给不同 IP 子网上的主机时, 它要选择一个能到达目的子网的路由器, 把 IP 分组送给该路由器, 由路由器负责把 IP 分组送到目的地。一般的主机都配置了“默认网关 (default gateway)”, “默认网关”是每台主机上的一个配置参数, 它是连接在同一个网络上的某个路由器端口的 IP 地址, 主机把所有未知网络的 IP 分组都发送给“默认网关”, 也就是出口路由器。在计算机上可以使用“route print”, 显示当前的主机路由, 如图 8-1-1 所示, 其中划线的一行是主机的默认路由, 默认路由的出口 (gateway) 是和主机在同一网段的路由设备接口的 IP 地址。还可以使用“route add”添加路由, “route delete”删除路由, 有关“route add/delete”的使用方法, 可以使用“route /?”命令查看在线帮助。



```

C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>route print

IPv4 Route Table
=====
Interface List
=====
0x1 ..... MS TCP Loopback interface
0x2 ...00 50 56 c0 00 01 ..... VMware Virtual Ethernet Adapter for VMnet1
0x3 ...00 1b 24 7d 25 72 ..... Marvell Yukon 88E8038 PCI-E Fast Ethernet Controller - Deterministic Network Enhancer Miniport
=====

Active Routes:
Network Destination  Netmask          Gateway           Interface        Metric
-----
0.0.0.0              0.0.0.0          192.168.1.1       192.168.1.200    20
127.0.0.0            255.0.0.0        127.0.0.1         127.0.0.1        1
192.168.1.0          255.255.255.0    192.168.1.200     192.168.1.200    20
192.168.1.200        255.255.255.255  127.0.0.1         127.0.0.1        20
192.168.1.255        255.255.255.255  192.168.1.200     192.168.1.200    20
192.168.111.0        255.255.255.0    192.168.111.1     192.168.111.1    20
192.168.111.1        255.255.255.255  127.0.0.1         127.0.0.1        20
192.168.111.255      255.255.255.255  192.168.111.1     192.168.111.1    20
224.0.0.0            240.0.0.0        192.168.1.200     192.168.1.200    20
224.0.0.0            240.0.0.0        192.168.111.1     192.168.111.1    20
255.255.255.255      255.255.255.255  192.168.1.200     192.168.1.200    1
255.255.255.255      255.255.255.255  192.168.111.1     192.168.111.1    1
Default Gateway:     192.168.1.1

Persistent Routes:
None
C:\Documents and Settings\Administrator>
    
```

图 8-1-1 主机的路由表

路由器转发 IP 分组时, 只根据 IP 分组目的 IP 地址的网络号部分, 选择合适的端口, 把 IP 分组发送出去。同主机一样, 路由器也要判定端口所连接的是否是目的子网, 如果是就直接把分组通过端口送到网络上, 否则也要选择下一个路由器来传送分组。路由器也有它的缺省网关, 用来传送不知道往哪儿送的 IP 分组。这样, 通过路由器把知道目的的 IP 分组正确转发出去, 把不知道的 IP 分组送给“默认网关”路由器 (在路由器上称为默认路由), 这样一级级地传送, IP 分组最终将送到目的地, 无法到达目的地的 IP 分组则被网络丢弃。

目前, TCP/IP 网络全部是通过路由设备互连起来, Internet 就是成千上万个 IP 子网通过路由设备互连起来的国际性网络。这种网络称为以路由器为基础的网络, 形成了以路由器为节点的互联网。在互联网中, 路由器不仅负责对 IP 分组的转发, 还要负责与别的路由器进行联络, 共同确定互联网的路由选择和维护路由表。

路由包括两个基本动作：**寻径和转发**。寻径即寻找到达目的地的最佳路径，由路由选择算法来实现。由于涉及不同的路由选择协议和路由选择算法，因此要相对复杂一些。为了判定最佳路径，路由选择算法必须启动并维护包含路由信息的路由表，其中路由信息依赖于所用的路由选择算法而不尽相同。路由选择算法将收集到的不同信息填入路由表中，根据路由表可将目的网络与下一站（next-hop）的关系告诉路由器。路由器间互通信息进行路由更新，更新维护路由表使之正确反映网络的拓扑变化，并由路由器根据度量值来决定最佳路径。这就是**路由协议**，也叫做**路由选择协议（routing protocol）**，如 RIP（Route Information Protocol，路由信息协议）、OSPF（Open Shortest-Path First，开放式最短路径优先协议）和 BGP（Border Gateway Protocol，边界网关协议）等。

转发即沿寻径好的最佳路径传送信息分组。路由器首先在路由表中查找，判明是否知道如何将分组发送到下一个站点（路由器或主机），如果路由器不知道如何发送分组，通常将该分组丢弃；否则就根据路由表的相应表项将分组发送到下一个站点，如果目的网络直接与路由器相连，路由器就把分组直接送到相应的端口上。

被路由协议和路由协议这两个概念很重要，它们经常出现且容易被搞混淆。它们是相互配合又相互独立的概念，被路由协议使用路由协议维护的路由表，同时路由协议要利用被路由协议提供的功能来发布路由协议数据分组。被路由协议是指可以被路由的协议（routed protocol），被路由协议要满足可以被路由的条件，即网址分成网络号+主机号，被路由协议有 IP、IPX 等。本书中提到的路由协议，除非特别说明都是指路由选择协议，这也是普遍的习惯。

8.1.3 路由协议

路由协议分为 IGP（Interior Gateway Protocol，内部网关协议）和 EGP（Exterior Gateway Protocol，外部网关协议）。内部网关协议是在同一个 AS（Autonomic Systems，自治系统）内运行的路由协议，这里的自治系统是指一个具有统一管理机构、统一路由策略的网络，IGP 协议又分为静态路由协议和动态路由协议。外部网关协议运行在不同的 AS 之间，目前使用最多的是 BGP 协议，BGP 协议也属于动态路由协议，BGP 协议对配置人员的要求比较高，多数人一般不会在实际工作环境中遇到，本书对 BGP 协议不做过多叙述。路由协议的详细分类如图 8-1-2 所示。

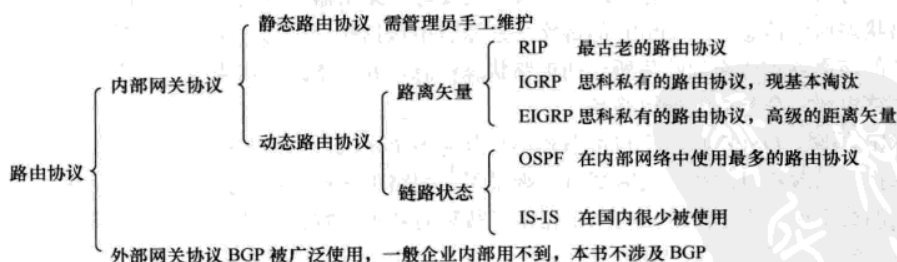


图 8-1-2 路由协议

静态路由是由管理员在路由器中手工添加的路由条目。除非网络管理员干预，否则静态路由

不会发生变化。由于静态路由不能对网络的改变做出反映,一般用于网络规模不大、拓扑结构固定的网络中。静态路由的优点是简单、高效、可靠。在所有的路由中,静态路由优先级最高。当动态路由与静态路由发生冲突时,以静态路由为准。

动态路由是网络中的路由器之间相互通信,传递路由信息,利用收到的路由信息更新路由表的过程。它能实时地适应网络结构的变化,如果路由更新信息表明发生了网络变化,路由选择软件就会重新计算路由,并发出新的路由更新信息。这些信息通过各个网络,引起各路由器执行路由算法,并更新各自的路由表以动态地反映网络拓扑变化。动态路由适用于网络规模大、网络拓扑复杂的网络。当然,各种动态路由协议会不同程度地占用网络带宽和 CPU 资源。

静态路由和动态路由有各自的特点和适用范围,因此在网络中动态路由通常作为静态路由的补充。当一个分组在路由器中进行寻径时,路由器首先查找静态路由,如果查到静态路由则根据相应的静态路由转发分组,否则再查找动态路由。但这也不是一成不变的,本章后续有专门的小节来介绍路由选路。

1. RIP 路由协议

RIP 协议是 Internet 中最古老的路由协议。RIP 采用距离向量算法,即路由器根据距离选择路由,所以也称为距离向量协议。路由器收集所有可到达目的地的不同路径,并且保存有关到达每个目的地的最少站点数的路径信息,除到达目的地的最佳路径外,任何其他信息均予以丢弃。同时路由器也把所收集的路由信息用 RIP 协议通知相邻的其他路由器。这样,正确的路由信息逐渐扩散到了全网。

RIP 的特点是简单,便于配置。但是 RIP 只适用于小型的网络,因为它允许的最大跳数为 15,任何超过 15 个站点的目的地均被标记为不可达。而且 RIP 每隔 30s 一次的路由信息广播也造成带宽的严重浪费,频繁的更新也影响路由器的性能。RIP 路由协议的收敛速度较慢,有时还会造成网络的环路,因此复杂的网络中最好配置 OSPF 协议。

2. OSPF 路由协议

20 世纪 80 年代中期, RIP 已不能适应大规模异构网络的互连, OSPF 随之产生。它是 IETF (The Internet Engineering Task Force, 互联网工程任务组) 的内部网关协议工作组为 IP 网络而开发的一种路由协议。

OSPF 是一种基于链路状态的路由协议,需要每个路由器向其同一管理域的所有其他路由器发送链路状态通告信息。在 OSPF 的链路状态通告中包括接口信息、量度值和其他一些变量。运行 OSPF 的路由器首先必须收集所有的链路状态信息,并以本路由器为根,使用 SPF (最短路径树) 算法算出到每个节点的最短路径。

与 RIP 不同, OSPF 将一个自治系统再划分为多个区域,当源和目的在同一区域时,采用域内路由选择;当源和目的在不同区域时,则采用区间路由选择。这就大大减少了网络开销,并增加了网络的稳定性。当一个区内的路由器出了故障时并不影响自治域内其他区域路由器的正常工作,这也给网络的管理、维护带来方便。

3. BGP 路由协议

BGP 是为 TCP/IP 互联网设计的外部网关协议,用于多个自治系统之间的信息交流。它既不

是基于纯粹的链路状态算法，也不是基于纯粹的距离向量算法。它的主要功能是与其他自治系统的 BGP 路由器交换网络可达信息。各个自治系统可以运行不同的内部网关协议。BGP 更新信息包括网络号、自治系统路径、度量值等多个信息。自治系统路径包括到达某个特定网络需经过的自治系统号，这些更新信息通过 TCP 传送出去，以保证传输的可靠性。

4. 路由算法

路由算法在路由协议中起着至关重要的作用，采用何种算法往往决定了最终的寻径结果，因此选择路由算法一定要慎重。通常需要综合考虑以下几个设计目标。

- (1) 最优化：指路由算法选择最佳路径的能力。
- (2) 简洁性：算法设计简洁，利用最少的软件和开销，提供最有效的功能。
- (3) 坚固性：路由算法处于非正常或不可预料的环境时，如硬件故障、负载过高或操作失误时，都能正确运行。由于路由器分布在网络连接点上，所以在它们出现故障时会产生严重后果。最好的路由器算法通常能经受时间的考验，并在各种网络环境下被证实是可靠的。
- (4) 快速收敛：路由收敛是指路由域中所有路由器对当前的网络结构和路由转发达成一致的状态。收敛时间是指从网络的拓扑结构发生变化到网络上所有的相关路由器都得知这一变化，并且相应地做出改变所需要的时间。当某个网络事件引起路由可用或不可用时，路由器就发出更新信息。路由更新信息遍及整个网络，引发重新计算最佳路径，最终达到所有路由器一致公认的最佳路径。收敛慢的路由算法会造成路径环路或网络中断。
- (5) 灵活性：路由算法可以快速、准确地适应各种网络环境。例如，某个网段发生故障，路由算法要能很快发现故障，并为使用该网段的所有路由选择另一条最佳路径。

链路状态算法（也称最短路径算法）发送路由信息到互联网上所有的结点，然而对于每个路由器，仅发送它的路由表中描述了其自身链路状态的那一部分。距离矢量算法则要求每个路由器发送其路由表全部或部分信息，但仅发送到邻近结点上。从本质上来说，链路状态算法将少量更新信息发送至网络各处，而距离向量算法发送大量更新信息至邻接路由器。

由于链路状态算法收敛更快，因此它在一定程度上比距离向量算法更不易产生路由循环。但另一方面，链路状态算法要求比距离向量算法有更强的 CPU 能力和更多的内存空间，因此链路状态算法将会在实现时显得更昂贵一些。除了这些区别，两种算法在大多数环境下都能很好地运行。

最后需要指出的是，路由算法使用了许多种不同的度量标准去决定最佳路径。复杂的路由算法可能采用多种度量来选择路由，通过一定的加权运算，将它们合并为单个的复合度量，再填入路由表中，作为寻径的标准。通常所使用的度量标准包括跳数、可靠性、时延、带宽、负载、花费等。

8.2 直连路由

根据路由器学习路由信息、生成并维护路由表的方式，路由分为直连路由（Connect）、静态路由（Static）和动态路由（Dynamic）。直连路由是由链路层协议发现的，一般指去往路由器的接口地址所在网段的路径，该路径信息不需要网络管理员维护，也不需要路由器通过某种算法进行计算获得，只要该接口处于激活状态（Active），路由器就会把通向该网段的路由信息填写到路由

表中去。

IP 的配置发生在每个接口上。在接口上设置主要的 IP 地址和子网掩码,可进入接口配置模式,并输入命令 `ip address ip-address mask`。在接口上设置多个 IP 地址是可能的,这将在本章的最后一节中讲述。注意,路由器的端口配置 IP 地址后,并不起作用,要使用 `no shutdown` 打开端口,如果端口没有接线,IP 地址也不会被激活。

使用 CCNP 机架中的路由器 R1、R2、R3,它们之间的 IP 地址分配如图 8-2-1 所示。读者也可以选择使用安全或语音机架中的 R1、R2、R3,这里之所以选择使用 CCNP 机架的原因,主要是因为 CCNP 机架中路由器的 IOS 功能相对较少,占用的系统资源不高,不会影响完成路由部分的配置,尤其是计算机配置不高的情况,更要选择使用 CCNP 机架。第一次使用 CCNP 机架中的路由器,要使用 7.1.2 节介绍的方法获取 `idlepc` 参数,降低 CPU 的使用率。本书后续的所有实验中,均需要为实验中用到的该款 IOS 获取有效的 `idlepc` 参数。

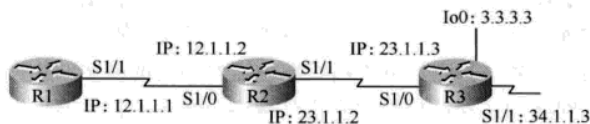


图 8-2-1 静态路由拓扑图

双击 `dynamips` 文件夹下的“0.启动虚拟服务.bat”,不要关闭该窗口,再双击“4.控制台 CCNP.cmd”,打开 CCNP 机架的控制台。在机架控制台中,给路由器 R1、R2、R3 加电,并使用 `telnet` 命令登录到每台路由器的控制台,如图 8-2-2 所示。

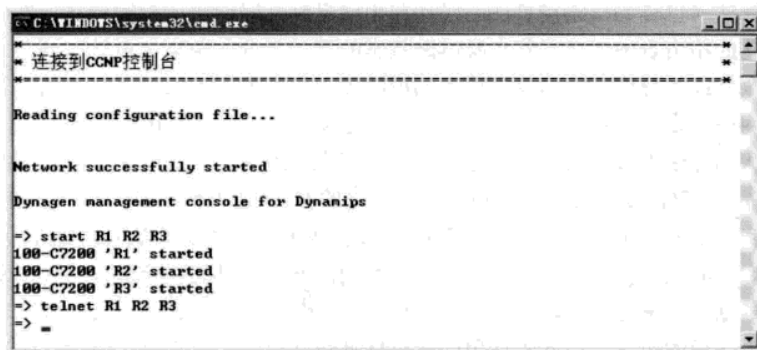


图 8-2-2 CCNP 的控制台

R1 的具体配置如下,其中斜体部分为注释:

```
Router>en  enable 命令的简写, 进入特权模式
Router#conf t  configure terminal 命令的简写, 进入全局配置模式
Router(config)#host R1  hostname 命令的简写, 更改路由器的名字, 更改路由器的名字需要在全局配置模式下操作
R1(config)#int s1/1  interface serial 1/1 命令简写, 从全局配置模式再进入到接口配置模式
R1(config-if)#ip add 12.1.1.1 255.255.255.0  ip address 命令的简写, 给 S1/1 口配置 IP 地址, 12.1.1.1 是 S1/1 接口的 IP 地址, 255.255.255.0 是对应的掩码
```

R1(config-if)#no shut *no shutdown* 命令的简写, 打开端口, 默认情况下, 路由器的所有物理端口都处在关闭状态

R2 的具体配置如下:

```
Router>en
Router#conf t
Router(config)#host R2
R2(config)#int s1/0
R2(config-if)#ip add 12.1.1.2 255.255.255.0
R2(config-if)#no shut
R2(config-if)#int s1/1
R2(config-if)#ip add 23.1.1.2 255.255.255.0
R2(config-if)#no shut
```

R3 的具体配置如下:

```
Router>en
Router#conf t
Router(config)#host R3
R3(config)#int s1/0
R3(config-if)#ip add 23.1.1.3 255.255.255.0
R3(config-if)#no shut
R3(config-if)#int s1/1
R3(config-if)#ip add 34.1.1.3 255.255.255.0
R3(config-if)#no shut
R3(config-if)#int loopback 0 interface loopback 命令的简写, loopback 是路由器上的虚拟接口, 主要用来模拟路由条目。又因这种端口比较稳定, 除非路由器断电, 否则该端口一直有效, 这种端口也被用于一些特殊用途, 如 OSPF 的 Router-id。
R3(config-if)#ip add 3.3.3.3 255.255.255.0
R3(config-if)#no shut
```

配置中的 s 表示的是 Serial (串行口), 主要用于广域网接入, 带宽是 1.544M 或 2.048M。连接串行口的线缆叫串行线缆, 这种线缆一端标明是 DCE (Data Circuit-Terminating Equipment, 数据通信设备), 另一端标明是 DTE (Data Terminal Equipment, 数据终端设备)。为了保存时钟同步, DCE 端要配置时钟, 使用的命令是 *clock rate*, 后面紧跟一个时钟频率值。在 *dynamips* 模拟器中, 时钟频率可以省略不配, 而工程中一般不可省略, 尤其是在低端的路由器上。

在路由器 R1 上执行 *show ip route*, 显示的结果如图 8-2-3 所示。

在图中, 可以发现 R1 上有一条由字母 C 开头的路由 12.1.1.0/24, 该路由是直连路由, 路由器能够自动产生激活端口 IP 所在网段的直连路由信息, 并且路由器的每个接口都必须单独占用一个网段。在 R3 上使用 *show ip route*, 可以发现 23.1.1.0/24 和 3.3.3.0/24 两条路由, 却发现不了 34.1.1.0/24, 原因是因为路由器 R3 的 serial1/1 口没有连线, 自然没有被激活, 路由器不会产生该接口的直连路由。

路由器中数据的流动情况是这样的。当从局域网中接收到一个包时, 在进入 RAM 之前, 首先检查它的第二层头信息, 如果是发往本路由器的, 第二层头信息被剥掉; 在 RAM 里, 路由器检测包第三层的头信息, CPU 同时搜索路由表并匹配第三层地址以决定包应向哪里输出及以怎样的方式进行封装。每个包的处理过程都是由 CPU 查询路由表并决定将包发向哪里。

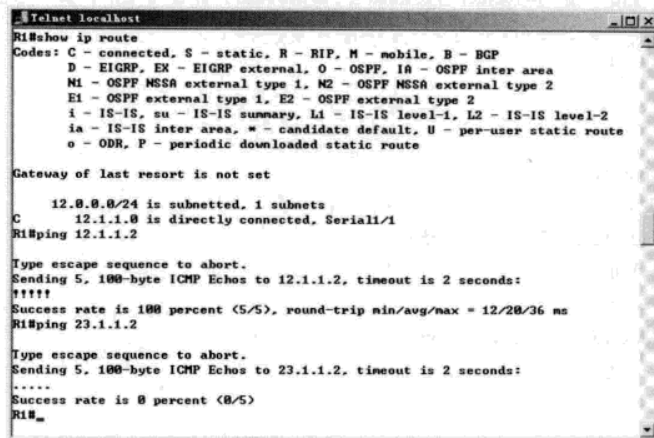


图 8-2-3 直连路由

路由器对自身产生的数据包也要查询路由表，找到出口。如图 8-2-3 所示，执行 ping 12.1.1.2，可以发现是成功的（路由器中“!”表示成功，“.”表示超时），但 ping 23.1.1.2 却是失败的。当在 R1 上 ping 12.1.1.2 时，R1 查询自己的路由表，送到 12.1.1.0/24 的包应该从 Serial1/1 端口发出去，当 R2 收到 R1 发过来的包后，发现是从 12.1.1.1 过来的，R2 查询自己的路由表，把包从 Serial1/0 端口发回来，结果是 R1 成功的 ping 通了 R2。当在 R1 上 ping 23.1.1.2 时，R1 查询自己的路由表，发现路由表中没有去往 23.1.1.2 的路由，R1 丢弃该数据包，结果是 R1 上 ping 23.1.1.2 失败。

8.3 静态路由

如图 8-2-3 所示，R1 无法 ping 通 23.1.1.2，有什么办法可以让 R1 能 ping 通呢，解决的办法之一就是配置静态路由。静态路由就是网段之间的路由需要人工加入。和动态路由相比，静态路由有几个优点。一个优点是路由器的日常开销较低，因为它并不经常计算和发送路由器更新；另一个优点是两个目的地之间的路径总是已知的，并且这帮助减少了故障可能出现的地点的数目。

如图 8-2-3 所示，如果 R1 知道把去往 23.1.1.2 的包发给 R2，那么结果就能 ping 通了。在 R1 上添加静态路由，命令如下：

```
R1(config)#ip route 23.1.1.0 255.255.255.0 12.1.1.2
```

或者：

```
R1(config)#ip route 23.1.1.0 255.255.255.0 s1/1
```

命令中的 ip route 23.1.1.0 255.255.255.0 12.1.1.2，其中 23.1.1.0 是要到达的目标网络，在静态路由中需要添加所有的非直连网络；255.255.255.0 为目标网络对应的子网掩码；12.1.1.2 为与本路由器直接相连的下一跳路由器的接口地址，这里特别要注意的是，即使要到达的网络与本路由器相隔数台路由器，这里填入的还是下一跳地址，而不是目标网络的前一跳，也就是说在静态路由中，只需要指出下一跳的地址，至于以后如何指向，那是下一跳路由器考虑的事情。

这两条命令的结果是相同的，都是在 R1 上添加一条去往 23.1.1.0/24 网段的路由。至于填写下一跳的地址，还是本路由器的出接口，两者之间还是有差别的。

区别一是上面一条命令引用的是下一跳路由器和本路由器相连接口的 IP 地址，该路由的管辖距离是 1，下面一条命令引用的是本路由器的出口，该路由的管辖距离是 0。另外，静态路由的管辖距离可以手工指定，指定了管辖距离的静态路由叫做“浮动静态路由”，浮动静态路由在链路备份的场合被广泛使用。有关管辖距离的内容，本章稍后介绍。

区别二是指本路由器出口命令仅能用在点对点的链路上，如本例中的串行线路，如果是以太网这种多路访问的链路，指出接口则路由器将不知道把包发往哪一台路由器。在多路访问的链路上，静态路由要指下一跳地址，而不能使用外出接口。如图 8-3-1 所示，假设 A 公司要访问 Internet，在 A 公司的路由器上如果设置的是路由器的出口，A 公司路由器在把包发送出去之前首先要封装目的 MAC 地址。因为以太网是一个多路访问的网络，如果不知道发往哪一个 IP 地址，就没有办法解析出 MAC 地址，更没有办法完成二层链路的封装，封装都完成不了，就更谈不上把包发送出去了。

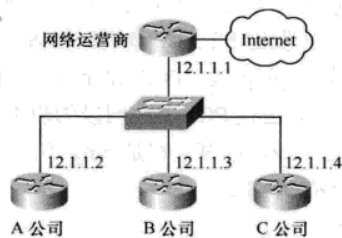


图 8-3-1 静态路由的下一跳

注意



真实环境中，在配置以太网这种多路访问的网络时，静态路由指下一路 IP 地址和本路由器的外出接口，结果均可成功的原因在于思科路由器的以太网接口默认启用了 Proxy-arp（代理 ARP）功能，如果关闭代理 ARP 功能，则外出接口将失败。

R1 上添加完静态路由后，再在 R1 上 ping 23.1.1.2，可以发现能够 ping 通了。然后在 R1 上 ping 23.1.1.3，结果发现又不通了，分析一下原因，仍然是对于去往 23.1.1.0/24 数据包，R1 会把数据包发给 R2，R2 查看本地的路由表，23.1.1.0/24 是直连路由，外出接口是 S1/1，R2 把数据包从 S1/1 口发出去，数据包到达目标 R3，R3 收到数据包，拆包后发现该数据包来自 12.1.1.1，R3 试图进行应答，可在 R3 上却找不到去往 12.1.1.1 的路由，R3 放弃应答。结果是 R1 收不到应答，提示超时。解决的办法是在 R3 上添加去往 12.1.1.0/24 的路由。

```
R3(config)#ip route 12.1.1.0 255.255.255.0 23.1.1.2
```

或者：

```
R3(config)#ip route 12.1.1.0 255.255.255.0 s1/0
```

在 R3 上添加完静态路由后，再次在 R1 上 ping 23.1.1.3，发现可以 ping 通了。如果想 R1 也能 ping 通 3.3.3.3，还需在 R1 和 R2 上添加 3.3.3.0 的静态路由。

```
R1(config)#ip route 3.3.3.0 255.255.255.0 12.1.1.2
```

```
R2(config)#ip route 3.3.3.0 255.255.255.0 23.1.1.3
```

下面总结一下配置静态路由的一般步骤。

- STEP 1** 为路由器每个接口配置 IP 地址。
- STEP 2** 确定本路由器有哪些直连网段。
- STEP 3** 确定网络中有哪些属于本路由器的非直连网段。
- STEP 4** 添加本路由器的非直连网段的相关路由信息。

下面介绍一种常见的静态路由排错方法。如图 8-3-2 所示，R1 可以 ping 通 PC2，PC1 却 ping 不通 PC2，所有设备的 IP 地址配置都正确，所有的接口都正常。出现上述现象的可能原因是什么？

R1 可能 ping 通 PC2，说明 R1 上添加了去往 PC2 所在网段的静态路由。分析 PC1 不能 ping 通 PC2 的原因，PC1 把去往 PC2 的包发往自己的网关，R1 上已经有去往 PC2 所在网段的静态路由了，R1 查询路由表，把包转发给 R2，R2 查询路由表，把包转发给 PC2，数据包正常到达了 PC2。PC2 知道是 PC1 发过来的 ping 包，PC2 进行应答，把包发给 PC2 的网关，也就是 R2，R2 查询自己的路由表，假如 R2 有去往 PC1 所在网段的静态路由，R2 把包发给 R1，R1 再把包发给 PC1，结果是 PC1 可以 ping 通 PC2，可事实却是 ping 不通，这只能说明前面的假设是错误的，即 R2 上没有去往 PC1 所在网段的静态路由。

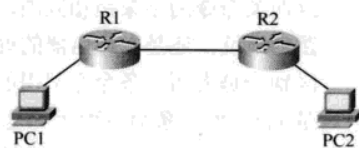


图 8-3-2 静态路由排错

8.4 默认路由

大家可以想象，在大型网络或互联网中，每一个路由器不可能确切地知道到每一个其他路由器的路由。这时就需要使用默认路由，也叫缺省路由，默认路由规定了将所有未知数据包发往何处。路由器假设它可以将未知数据包发往默认路由器，并且那个路由器知道如何处理。如果下一个路由器并不知道所需要的路由，它将数据包发送到它自己的默认路由，并且这个过程持续直至到达目的网络。

如果不允许配置默认路由，图 8-3-1 中的 A 公司需要访问 Internet，那么就需要在 A 公司的路由器上添加所有 A 类、B 类、C 类网络，下一跳都是运营商的路由器地址“12.1.1.1”，A 公司出口路由上的要添加 $(126 \text{ (A 类地址数)} + 2^{(16-2)} \text{ (B 类地址数)} + 2^{(24-3)} \text{ (C 类地址数)})$ 个路由条目，工作量得惊人，而且一般低端的路由器也没有办法维护这么多的路由条目。可随着默认路由的出现，这一切都迎刃而解。

如果在路由器的全局配置模式下执行“no ip routing”，关闭 IP 路由功能，静态默认路由的配置可以使用下面的命令完成：

`ip default-gateway A.B.C.D` (A.B.C.D 是默认网关的地址，如图 8-3-1 所示就是 12.1.1.1。所有普通计算机上默认都没有开启路由功能，为了可以去往所有未知的网络，都配置了默认网关)

在没有关闭 IP 路由功能时，静态默认路由的配置可以使用下面的命令完成：

`ip route 0.0.0.0 0.0.0.0 A.B.C.D` (A.B.C.D 是下一跳路由器的地址，如果是点对点链路，这里也可以是本路由器的外出接口)

可以通过输入下面的命令来查看当前默认路由的配置：

`show ip route`

如图 8-2-1 所示，R1 上可以把两条静态路由改成一条默认路由，命令如下：

`R1(config)#no ip route 23.1.1.0 255.255.255.0 12.1.1.2`

`R1(config)#no ip route 3.3.3.0 255.255.255.0 12.1.1.2`

`R1(config)#ip route 0.0.0.0 0.0.0.0 12.1.1.2`

在 Internet 上，大部分路由器都配置有默认路由。

8.5 动态路由协议

前一节介绍了静态路由的优点，但静态路由有一个明显缺点就是缺乏缩放能力。如图 8-5-1 所示，静态路由配置非常容易就可以实现，如果仅仅考虑少量网段时这是可行的，如要用大约 50 个路由器将 100 个网络段互相连接，在每台路由器上都要输入所有那些非直连路由，总开销是非常惊人的。静态路由还有一个缺点就是不能自动适应网络拓扑的变化，尤其是在有冗余路径的情况下。可以尝试使用静态路由完成如图 8-5-1 所示的拓扑配置。

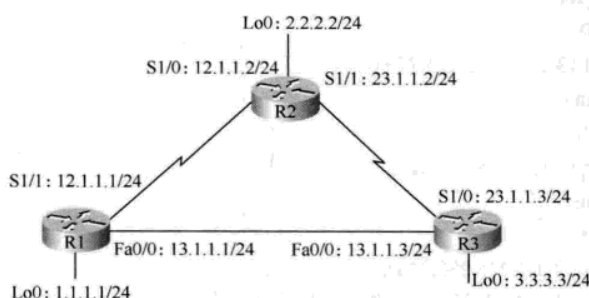


图 8-5-1 有冗余链路的拓扑

在 R1 上添加去 2.2.2.0/24 的路由：

```
R1(config)#ip route 2.2.2.0 255.255.255.0 12.1.1.2
```

此时 R1 可以到达 2.2.2.2，可如果 R1 和 R2 之间的串行链路发生故障，R1 将不能 ping 通 2.2.2.2，事实上 R1 还可以通过 R3 到达 R2 的环回口。可静态路由不会自动适应这一拓扑的变化。

下面简单回顾一下静态路由和动态路由的区别。静态路由是指由网络管理员手工配置的路由信息。当网络的拓扑结构或链路的状态发生变化时，网络管理员需要手工去修改路由表中相关的静态路由信息。静态路由信息在默认情况下是私有的，不会传递给其他的路由器。当然，网管员也可以通过对路由器进行设置使之成为共享的。静态路由一般适用于比较简单的网络环境，在这样的环境中，网络管理员易于清楚地了解网络的拓扑结构，便于设置正确的路由信息。动态路由是指路由器能够自动地建立自己的路由表，并且能够根据实际情况的变化适时地进行调整。动态路由的运作机制依赖路由器的两个基本功能：对路由表的维护和路由器之间适时的路由信息交换。

本节介绍两种普遍使用的动态路由协议：RIP 和 OSPF。

8.5.1 RIP 路由协议

RIP 是应用较早，使用较普遍的内部网关协议，适用于小型同类网络，是典型的距离向量 (distance-vector) 协议。

RIP 通过广播 UDP 报文来交换路由信息，每 30s 发送一次路由信息更新。RIP 提供跳计数 (hop count) 作为尺度来衡量路由距离，跳计数是一个包到达目标所经过的路由器的数目。如果到相同目标有二个不等速或不同带宽的路由，但跳计数相同，则 RIP 认为两个路由是等距离的。RIP 支

持的最大跳计数是 15，即在源和目的网络之间所要经过的最多路由器的数目为 15，跳计数 16 则目标不可达。

启用 RIP 的过程是在全局层次上进行，但是很多配置可以在接口基础上进行。通过输入下面的命令可以启用或者禁止 RIP：

```
[no] router rip
[no] network A.B.C.D (Network number, 这里填入的是主类网络号, 不是具体的 IP 地址, 也不是子网号)
```

如图 8-5-1 所示 R1 的配置如下：

```
Router>en
Router#conf t
Router(config)#host R1
R1(config)#int fa 0/0
R1(config-if)#ip add 13.1.1.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#int s1/1
R1(config-if)#ip add 12.1.1.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#int lo0
R1(config-if)#ip add 1.1.1.1 255.255.255.0
R1(config-if)#exit    loopback 环回口, 作为虚拟接口, 默认处于 no shut 状态, 习惯性的在接口下输入
no shut 也没有关系
R1(config)#router rip    进入 RIP 路由协议配置模式
R1(config-router)#network 12.0.0.0    加入直连接口 S1/1 所在的主类网络, 因 12.1.1.1 是 A 类网络, 网
络号是 12.0.0.0
R1(config-router)#network 13.0.0.0    加入 Fa0/0 所在的主类网络
R1(config-router)#network 1.0.0.0    加入 lo0 所在的主类网络
```

R2 的配置如下：

```
Router>en
Router#conf t
Router(config)#host R2
R2(config)#int s1/0
R2(config-if)#ip add 12.1.1.2 255.255.255.0
R2(config-if)#no shut
R2(config-if)#int s1/1
R2(config-if)#ip add 23.1.1.2 255.255.255.0
R2(config-if)#no shut
R2(config-if)#int lo0
R2(config-if)#ip add 2.2.2.2 255.255.255.0
R2(config-if)#no shut
R2(config-if)#router rip
R2(config-router)#net 12.0.0.0
R2(config-router)#net 23.0.0.0
R2(config-router)#net 2.0.0.0
```

R3 的配置如下:

```
Router>en
Router#conf t
Router(config)#host R3
R3(config)#int s1/0
R3(config-if)#ip add 23.1.1.3 255.255.255.0
R3(config-if)#no shut
R3(config-if)#int fa 0/0
R3(config-if)#ip add 13.1.1.3 255.255.255.0
R3(config-if)#no shut
R3(config-if)#int lo0
R3(config-if)#ip add 3.3.3.3 255.255.255.0
R3(config-if)#router rip
R3(config-router)#net 23.0.0.0
R3(config-router)#net 13.0.0.0
R3(config-router)#net 3.0.0.0
```

最好在 R1 和 R3 上多加一条命令 “no cdp run”, R1 的配置如下:

```
R1(config)#no cdp run
```

此命令的作用是关闭 CDP (Cisco Discovery Protocol, 思科发现协议), 因为 R1 和 R3 都启用了以太网接口, 如果不关闭 CDP, 路由器的控制台将会不停地出现下面的提示:

```
*Dec 15 18:57:47.875: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on FasEthernet0/0
(not full duplex), with Cisco-2950 FastEthernet1/16 (full duplex)
```

提示双工不匹配, 看起来很不舒服, 如果不需要 CDP, 建议关闭该协议, 以后就不会再出现提示了。

如果要运行 CDP, 可以在以太网接口下输入命令 “duplex half”, 关闭双工不匹配的报错信息, R1 的配置如下:

```
R1#conf t
R1(config)#int fa0/0
R1(config-if)#duplex half
```

R1、R2、R3 这 3 台路由器都配置完成后, 在 R1 上执行 show ip route 查看 R1 的路由表, 如图 8-5-2 所示。



图 8-5-2 R1 的路由表

如图 8-5-2 所示, 可以看到 R1 的路由表有 6 条, 其中 3 条前面有标记 C, 即直连路由; 还有 3 条前面标记是 R, 是通过 RIP 学来的路由。其中 R1 去往 23.0.0.0/8 的路由有两个下一跳, 跳计数都是 1。尽管 R1 和 R3 之间是 100M, R1 和 R2 之间是 1.544M, 如果 R1 有去往 23.0.0.0/8 的数据包, R1 会在两条路径上进行负载均衡, 因为 RIP 仅考虑跳计数, 而不考虑实际的带宽。

进入 R1 的 s1/1 端口, 执行 shutdown, 关闭 R1 和 R2 之间的接口, 在 R1 上连续多次执行 show ip route, 会发现显示的并不一样, 大概一分钟左右, R1 上的显示稳定下来, 如图 8-5-3 所示。

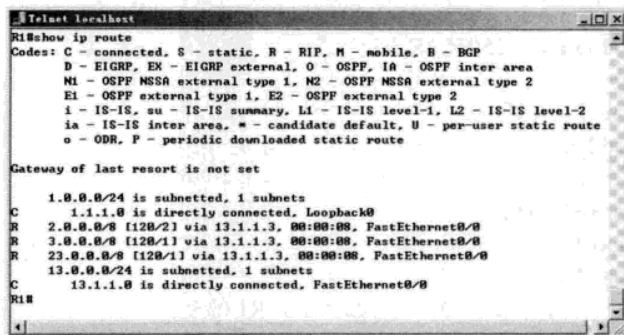


图 8-5-3 网络故障后 R1 的路由表

图 8-5-3 中的 R1 路由表和图 8-5-2 中的 R1 路由表相比有一些变化。首先, 路由表的条目变成了 5 条, 因关闭了 S1/1 接口, 导致 R1 和 R2 之间相连的接口都不再激活, 它们之间的路由条目也随之消失; 其次, R1 的路由表发生了自动调整, 本来去 2.0.0.0/8 的路由是直接发往 R2 的, 现在变成从 R3 绕行了。这样, 动态路由协议能够根据拓扑的变化, 调整路由表, 相比静态路由更灵活。

在前面的实验中, 为何要一分钟左右, 网络才能稳定下来呢? 原因是因为 RIP 是一个距离矢量的路由协议, 它只能定期地更新, 默认时间是 30s, 也就是说如果刚刚发送过更新, 即使网络拓扑发生了变化, 路由器也不进行更新, 要等待下一个更新周期才发送更新。但用户可以调整 RIP 的更新频率、存储或者从表中删除所需要的时间参数, 可以用 times basic 命令进行配置, 如下所示:

R1 (config-router) #timers basic update invalid holddown flush

默认情况下, 每隔 30s 发送 RIP 更新。通过 update 参数可以改变这个时间。当在特定的时间后没有从某个路由接收到更新, 则声明路由非法, 这个时间以 s 为单位, 是用 invalid 参数设置的, 这个数值默认是发送 RIP 更新周期的 6 倍, 也就是 180s。现在当某条路由非法时, 它进入了抑制周期, 这是下一个需要配置参数 holddown, 在抑制周期内, 路由器不学习该条路由的信息, 除非是一条更好的路由信息, 如本来是 3 跳, 在抑制周期内学到了一条 2 跳的路由信息, 则接受新的路由信息; 抑制周期过后, 即使是差的路由信息也接受, 抑制周期默认也是 180s, 当路由器处于抑制周期内, 它仍然用于向前转发数据包。最后的一个设置的参数是 flush, 规定了从路由表中删除路由条目所需要的时间, 它也是以 s 为单位, 默认是 240s。

距离矢量路由协议采用周期性的更新, 容易导致各路由器对网络的认知不一致, 从而导致路由环路。解决路由环路的办法有最大跳计数 (max hop)、水平分隔 (split-horizon)、触发更新 (triggered Update)、抑制定时器 (hold-down time)、毒性反转 (poison reverse)。在 CCNA 考试中,

这些方法都会涉及到, 因本书以培养能力为主, 对这些方法不再进一步讨论, 感兴趣的读者可以自行查阅相关资料。

如图 8-5-2 和图 8-5-3 所示, 显示的路由都是主类网络的路由。如何才能显示出明细的精确路由呢? 在 R1、R2 和 R3 上执行:

```
R1 (config) #router rip
R1 (config-router) #version 2    配置 RIP 版本 2, RIP 协议默认运行的是版本 1
R1 (config-router) #no auto-summary  关闭自动汇总
```

上面的命令是启用 RIP 版本 2, RIP 默认运行的是版本 1。在 RIP 版本 2 中可以关闭自动汇总, 在 RIP 版本 1 中也可以使用“no auto-summary”命令, 但该命令在版本 1 中不起作用。3 台路由器上都执行完上述命令, 重新打开 R1 的 S1/1 口。因 RIP 路由协议收敛速度较慢, 可以在 3 台路由器的特权模式下执行“clear ip route *”, 手工清除过时的路由条目。一段时间以后, 在 R1 上再次执行 show ip route, 显示的结果如图 8-5-4 所示。

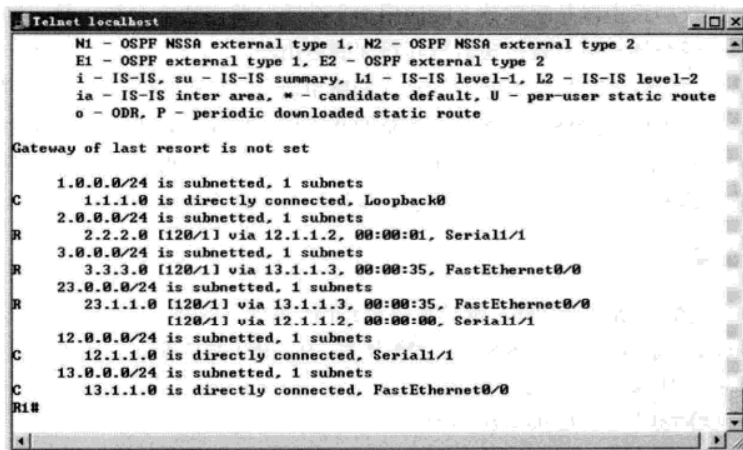


图 8-5-4 RIP V2 的路由表

图 8-5-4 和图 8-5-2 中显示的结果类似, 但通过 RIP 学到的 3 条路由都不再是汇总后的主类路由了, 而变成了具体的明细路由, 如 23.1.1.0/24, 不再是 23.0.0.0/8 了。另外 RIP 版本 2 还支持验证、使用组播更新、支持 VLSM (Variable Length Subnet Mask, 变长子网掩码)。建议工程中如果需要使用 RIP, 配置使用 RIP 版本 2, RIP V2 和 V1 配置起来一样简单, 但功能有很大增强。不要关闭实验台, 下一小节的实验将在本实验的基础上完成。

由于 RIP 路由协议容易产生路由环路, 收敛速度较慢, 不支持 CIDR (Classless InterDomain Routing, 无类域间路由), 现在被企业内部普遍使用的动态路由协议是 OSPF。

8.5.2 OSPF 路由协议

随着 Internet 技术在全球范围内的飞速发展, OSPF 已成为目前 Internet 广域网和 Intranet 企业网采用最多、应用最广泛的路由协议之一。OSPF 路由协议是由 IETF 中的 IGP 工作小组提出的, 是一种基于 SPF 算法的路由协议。

1. OSPF 概述

OSPF 路由协议是一种典型的链路状态(Link-state)路由协议,一般用于同一个自治系统(AS)。在这个 AS 中,所有同一个区域的 OSPF 路由器都维护一个相同的 LSDB (Link-State DataBase, 链路状态数据库),该数据库中存放的是路由域中相应链路的状态信息。链路状态路由协议只在网络拓扑发生变化后产生路由更新。当链路状态发生变化以后,检测到变化的设备创建 LSA (link state advertisement, 链路状态通告),通过使用组播地址传送给所有的邻居设备,然后每个设备复制一份 LSA,再转发 LSA 给其他的邻居设备,接着路由器更新它自己的 LSDB。这种 LSA 的洪泛(flooding)保证了所有的路由设备在更新自己的路由表之前更新它自己的 LSDB,OSPF 路由器正是通过这个数据库计算出其 OSPF 路由表的。

作为一种链路状态的路由协议,OSPF 将 LSA (链路状态通告,不是路由条目,更不是整个路由表)以组播的方式传送给在某一区域内的所有路由器,这一点与距离矢量路由协议不同。运行距离矢量路由协议的路由器是将部分(因启用水平分隔,路由器不会把从另一台路由器学来的路由再向回传送)或全部的路由表传递给与其相邻的路由器。

距离向量路由协议依靠邻居发给它的信息来做路由决策,路由器不需要保持完整的网络信息;而运行了链路状态路由协议的路由器保持有完整的网络信息的快照,而且每个路由器自己做出路由决策。完整 OSPF 的介绍,超出本书的范围,本书仅以单区域 OSPF 的配置为例,介绍 OSPF 的配置,有兴趣的读者可以参阅相关书籍,进一步学习 OSPF 原理和配置。

2. OSPF 配置

以图 8-5-4 中的配置结果为基础,继续在每个路由上配置 OSPF,其中 R1 的配置如下:

R1(config)#router ospf 1 进入 OSPF 协议配置模式,这里的 1 是进程号,只有本地意义,至于 R2 和 R3 使用什么进程号与 R1 没有关系,也不受影响。

R1(config-router)#net 12.1.1.0 0.0.0.255 area 0

R1(config-router)#net 13.1.1.0 0.0.0.255 area 0

R1(config-router)#net 1.1.1.0 0.0.0.255 area 0

net 12.1.1.0 0.0.0.255 area 0 语句中,12.1.1.0 表示的是要加入的直连网络地址,0.0.0.255 是反向掩码,area 0 表示的是把该网段放入区域 0,因本书只涉及到单区域的配置,所以把所有路由器的所有网段都加入到区域 0。在 R2 和 R3 上也增加配置 OSPF,因 R1、R2 和 R3 所有接口都运行 OSPF,路由器 R2 和 R3 上可以简写成下面的命令:

R2(config)#router ospf 1

R2(config-router)#net 0.0.0.0 0.0.0.0 area 0

R3(config)#router ospf 1

R3(config-router)#net 0.0.0.0 0.0.0.0 area 0

配置完所有路由器的 OSPF 后,在 R1 上执行 show ip route,结果如图 8-5-5 所示。

如图 8-5-5 所示,可以看到 R1 学到了 3 条有“O”标记的路由,是通过 OSPF 学来的,其中 2.2.2.2 和 3.3.3.3 均是 32 位的主机路由。OSPF 中默认学到的 loopback 端口路由都是 32 位的,如果不想看到 32 位的主机路由,可以在每台路由器的 loopback 端口下输入 ip ospf network point-to-point 取消 32 位主机路由。其中 R1 的操作如下:

R1(config-if)#ip ospf network point-to-point

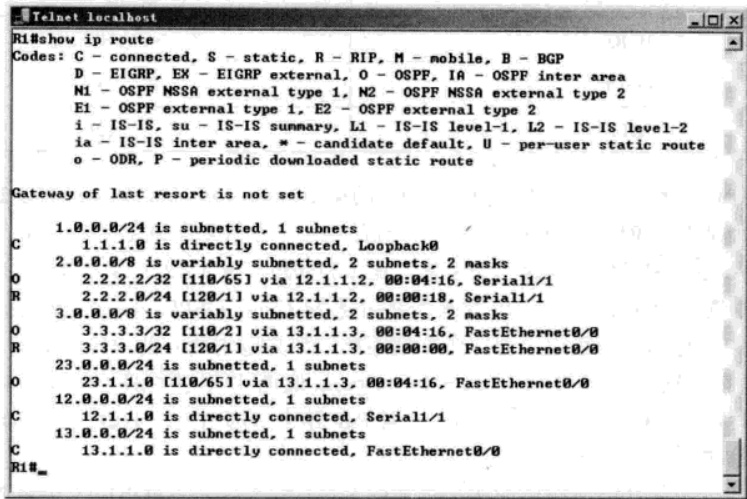


图 8-5-5 OSPF 和 RIP 共存的路由表

另一点特别要注意的是，在图 8-5-4 中 R1 上本来有一条被标记为“R”的路由 23.1.1.0/24，现在被标记为“O”的路由替代了。出现这样结果的原因将在“管辖距离”一节中有详细说明。不要关闭实验台，下一节的实验将在本实验的基础上完成。

通过配置 RIP 和 OSPF 两个动态路由协议，下面总结一下动态路由的一般配置步骤：

- STEP 1 为路由器每个接口配置 IP 地址
- STEP 2 确定本路由器有哪些直连网段
- STEP 3 添加本路由器的直连网段
- STEP 4 根据使用的不同动态路由协议，配置其他相关信息。

8.6 管辖距离

如果一个路由器从多个来源了解到某个网络的路由，它使用所谓的管辖距离排序，目的是确定将哪一个放置在它自己的 IP 路由选择表内。所有的路由，无论是动态或者是静态，都赋予一个管辖距离。管辖距离最小的那个路由将被采用。如表 8-6-1 所示，列出了常用路由协议的默认管辖距离。

表 8-6-1 管辖距离	
方 法	管 辖 距 离
直接连接	0
静态	1
EIGRP	90

续表

方 法	管 辖 距 离
IGRP	100
OSPF	110
RIP	120

现在再来分析图 8-5-4 中的“R 23.1.1.0/24”的路由在图 8-5-5 中为何会被“O 23.1.1.0/24”的路由替代。原因是通过 RIP 和 OSPF 学习的同样路由，一个管辖距离是 120，另一个管辖距离是 110，管辖距离小的 OSPF 学习的路由更可信。那么为何还有 R 2.2.2.0/24 和 R 3.3.3.0/24 两条 RIP 路由没有被替换呢？原因很简单，RIP 学来的路由是/24 位的，OSPF 学来的路由是/32 位的，它们属于不同路由，只有相同的路由才会比较管辖距离。如果取消所有的 RIP 路由，在所有路由器的 Loopback 端口下输入 ip ospf network point-to-point 取消 32 位主机路由，R1 路由器上将出现 O 2.2.2.0/24 和 O 3.3.3.0/24 的 OSPF 路由，并且 RIP 路由全部消失。不要关闭实验台，下一节的实验将在本实验的基础上完成。

接下来分析一个浮动静态路由的例子，如图 8-6-1 所示，某公司租用了一条 T1 (1.544M) 专线，用于连接 GAD 和 BHM 两个分支机构。假使两个分支机构运行的是 OSPF 路由协议，两地间运转正常。为了起到冗余，又开通了一条慢速的拨号线路，以期在专线故障后能够起用拨号线路。因为是慢速的拨号线路，所以不想在慢速的链路上再运行动态路由协议，毕竟动态路由协议要多耗费带宽。在两边配置静态路由互指对方后问题出现了，配置完静态路由后，发现两边的路由表中只有静态路由，没有了 OSPF 的路由，专线闲置不用，慢速的拨号却忙得不亦乐乎。原因就是管辖距离，静态路由的管辖距离是 1，比 OSPF 的管理距离 110 更可信，静态路由替代 OSPF 路由出现在路由表中。解决的办法就是使用浮动静态路由，浮动静态路由的配置命令如下：

```
GAD (config) #ip route 172.16.0.0 255.255.0.0 192.168.14.2 111
```

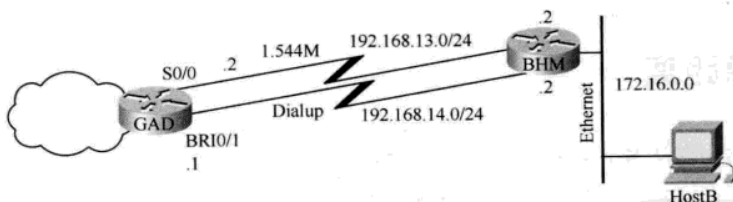


图 8-6-1 浮动静态路由

该命令最后的 111 是管辖距离，只要把该值设成大于动态路由的管辖距离即可。专线正常的情况下，GAD 可以通过 OSPF 学到 172.16.0.0/16 的路由，虽然静态路由也可以到达，但静态路由的管辖距离是 111，比 OSPF 的管辖距离 110 要大，路由器更相信管理距离小的 OSPF 路由，数据包从专线传送。当专线故障后，GAD 无法从 OSPF 学到 172.16.0.0/16 的路由，此时管理距离为 111 静态路由进入到路由表中，数据包从拨号线路传送。这种修改静态路由管辖距离的方式叫做浮动静态路由。

8.7 路由选路

当一个目标地址被多个目标网络覆盖，一个目标网络的多种路由协议的多条路径共存或当一个目标网络同一种路由协议的多条路径共存，路由器如何进行路由的选择呢？

路由器会依据以下选路原则进行路由选择。

第一条，子网掩码最长匹配。也就是如果一个目标地址被多个目标网络覆盖，它将优选最长的子网掩码的路由。如到达 10.1.1.1 的网络有两个：10.1.1.0/24 的下一跳是 12.1.1.2，10.1.0.0/16 的下一跳是 13.1.1.3，则路由器更相信子网掩码长的 10.1.1.0/24 的路由，因掩码长度 24 大于 16，路由器把数据包发往 12.1.1.2。如果路由器上发往 10.1.2.1 的数据包将选择 10.1.0.0/16 路由，因目标地址 10.1.2.1 不包括在路由条目 10.1.1.0/24 内。

第二条，管辖距离最小优先。在子网掩码长度相同的情况下，路由器优选管辖距离小的路由。如到达 10.1.1.0/24 的路由有两条，一条是通过 RIP 学习来的，另外一条是通过 OSPF 学习来的，则路由器相信 OSPF 学习来的路由，因它有更小的管辖距离 110，RIP 的管辖距离是 120。如图 8-5-5 所示，OSPF 取代 RIP 路由就是因为这个原因，R1 从 OSPF 和 RIP 都学到了 23.1.1.0/24 的路由，但 OSPF 有更小的管辖距离，结果标记为“O”的路由出现在路由表中。

如图 8-7-1 所示，R1 和 R2 之间相当于企业的内网，运行 OSPF 协议。R2 和 R3 之间相当于广域网，R2 是企业的出口路由器。R2 上配置一条默认路由，默认路由是静态路由的一个特例，管辖距离仍然是 1，OSPF 的管辖距离是 110，在 R2 上访问 1.1.1.1，会出现什么样的结果呢？数据包应该发往 R1 还是发往 R3 呢？答案当然发往 R1 了，因选路原则的第一条是子网掩码最长匹配，默认路由的子网掩码长度是 0，只要有明细路由，就使用不到默认路由。选路原则第一条就区分出路由的优先，用不着再比较第二条了。

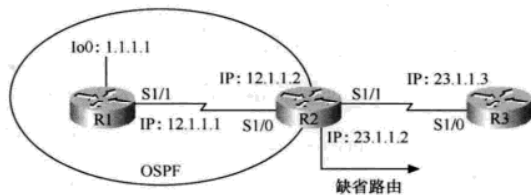


图 8-7-1 路由选路

在路由器 R1 上添加一条默认路由“ip route 0.0.0.0 0.0.0.0 1.1.1.2”，把未知数据包随便发往一个不存的 IP 地址，如图 8-7-2 所示。在 R1 上执行“show ip route”，可以发现最下面有一条“S* 0.0.0.0/0 [1/0] via 1.1.1.2”的默认路由，该路由的管辖距离是 1，如图 8-7-2 所示。然后在 R1 上 ping 2.2.2.2，发现可以 ping 通。说明 R1 上去往 2.2.2.2 的数据包并没有发往 2.2.2.2，而是选择了“O 2.2.2.2/32 [110/65] via 12.1.1.2, 00:03:00, Serial1/1”。因为路由选路原则先第一条，再第二条。

第三条，度量值最小优先。如果路由的子网掩码长度相同，管辖距离也相等，接下来比的就是度量值。如 RIP 比的是跳数，跳数越少越优先；OSPF 比的是花费（COST），花费越小越优先。如图 8-7-2 所示，R1 学到的这条路由：

```
"O 23.1.1.0 [110/65] via 13.1.1.3, 00:00:16, FastEthernet0/0"
```

“O”表示的是 OSPF 学来的路由，“23.1.1.0”是网络地址，“110”是 OSPF 的管辖距离，“65”是 OSPF 的花费，也叫度量值。65 是从何而来的呢？默认情况下，OSPF 用 100M 作为参考带宽，100M 除以实际的链路带宽得出链路花费，把整个路径上的所有花费加起来就得到度量值。R3 的

S1/0 口的带宽是 1.544M (可以使用 “show int s1/1” 查看), R1 的 Fa 0/0 口的带宽是 100M, 所以度量值是 $100/1.544+100/100=65$ 。同理可以算出 R1 从 R2 学过来 23.1.1.0 的度量值是 $100/1.544+100/1.544=128$, 结果花费小的路由被写入路由表。从 R1 发往 23.1.1.0/24 的数据包将发往 R3。可以断开 R1 的 Fa 0/0 后, 再查看 R1 的路由表, 可以验证 R1 从 R2 到达网络 23.1.1.0/24 的花费是 128。环回口的带宽是 8000M, 算出的花费是 0.01, 取整后是 1, R1 到 3.3.3.3 的度量值是 $100/8000+100/100=2$, 如图 8-7-2 所示, 可以看到下面这条路由:

"O 3.3.3.0 [110/2] via 13.1.1.3, 00:00:16, FastEthernet0/0"

```

Telnet localhost
R1(config)#ip route 0.0.0.0 0.0.0.0 1.1.1.2
R1(config)#do show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default, U - per-user static route
        o - ODR, P - periodic downloaded static route

Gateway of last resort is 1.1.1.2 to network 0.0.0.0

1.0.0.0/24 is subnetted, 1 subnets
C    1.1.1.0 is directly connected, Loopback0
2.0.0.0/24 is subnetted, 1 subnets
O    2.2.2.0 [110/65] via 12.1.1.2, 00:00:16, Serial1/1
3.0.0.0/24 is subnetted, 1 subnets
O    3.3.3.0 [110/2] via 13.1.1.3, 00:00:16, FastEthernet0/0
23.0.0.0/24 is subnetted, 1 subnets
O    23.1.1.0 [110/65] via 13.1.1.3, 00:00:16, FastEthernet0/0
12.0.0.0/24 is subnetted, 1 subnets
C    12.1.1.0 is directly connected, Serial1/1
13.0.0.0/24 is subnetted, 1 subnets
C    13.1.1.0 is directly connected, FastEthernet0/0
S*   0.0.0.0/0 [1/0] via 1.1.1.2
R1(config)#do ping 2.2.2.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2.2.2.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 24/48/64 ms
R1(config)#
    
```

图 8-7-2 选路原则

所以 OSPF 无法区分出 100M 以上的链路, 解决的办法是调整参考带宽, 如改成 10000M 作参考, 使用的命令是:

R1(config-router)#auto-cost reference-bandwidth 10000

用 10000M 作参考带宽后, OSPF 就可以区分出 100M、1000M、10000M 了。如果需要修改参考带宽, 需要在所有 OSPF 都修改, 不然会产生计算机标准的不一致性, 造成选路的不准确性。

现在可以关闭实验台, 本综合实验和讲解到此全部完成。

8.8 IP 主机表

IP 地址通常被映射成主机名。如果希望访问一个站点, 可以输入和那个特定位置相关的名称, 而不是记住一串数字。记住域名要比记住 IP 地址容易得多, 如记住 www.njut.edu.cn 要比记住 202.119.248.65 更容易。

Cisco 路由器可以配置主机名到 IP 地址的映射表。用 IP HOST 命令可以加入和删除条目。当使用这个命令时, 可以指定在建立连接时使用的 TCP 端口号, 默认值是 Telnet 端口 23。然后,

可以将多个 IP 地址绑定在同一个主机名上，最多可以绑定 8 个 IP 到一个主机名，如下所示：

```
ip host name [tcp-port-number] address1 [address2-address8]
[no] ip host name address1
```

这种方式相当于修改计算机中的 hosts 文件，但从没有通过修改 hosts 文件来访问整个互联网，这样的做法仅仅配置少量主机访问是可行的。路由器和计算机一样，也可以通过配置 DNS 来识别互联网的域名。在 Cisco IOS 中，默认情况下就启用了 DNS 功能。启动 CCNP 机架中的 R1 路由器，如下配置和测试路由器 R1 到 www.sina.com.cn（新浪网）的域名解析和连通情况：

```
Router>en
Router#conf t
Router(config)#host R1
R1(config)#int fa 0/0
R1(config-if)#ip add 192.168.1.250 255.255.255.0
R1(config-if)#no shut
R1(config-if)#exit
R1(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.1
R1(config)#ip name-server 218.2.135.1
R1(config)#do ping www.sina.com.cn
Translating "www.sina.com.cn"...domain server (218.2.135.1) [OK]

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 61.172.201.194, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/22/24 ms
```

从上面的执行结果，可以发现路由器 R1 不仅可以解析出新浪网的域名，还可以 ping 通新浪网的服务器。在实际配置路由器的过程中，往往不需要配置域名查找，尤其是初学者，一不小心输入错一个命令，路由器会以为输入的是一个主机名，然后进行广播式查找，经过很长时间返回一个错误消息。下面的就是路由器的错误输出：

```
R1#sdafsad
Translating "sdafsad"...domain server (218.2.135.1)

Translating "sdafsad"...domain server (218.2.135.1)
(218.2.135.1)
Translating "sdafsad"...domain server (218.2.135.1)
% Unknown command or computer name, or unable to find computer address
```

对于初学者来说，可以使用 no ip domain-lookup 命令，关闭路由器的域名查找功能，这样输入一个命令后很快就可以返回。如下所示：

```
R1(config)#no ip domain-lookup
R1(config)#exit
R1#sdafdrewq
*Feb 15 14:54:31.271: %SYS-5-CONFIG_I: Configured from console by console
Translating "sdafdrewq"
```

Translating "sdafdrewq"

% Unknown command or computer name, or unable to find computer address

接下来, 介绍一个很实用的命令。在配置路由器的过程中, 正在输入命令时忽然一个日志消息显示出来, 打断了用户的输入, 其实并没有打断, 只是影响显示而以, 用户可以继续输入后面字母, 完成本次输入。可对于初学者, 看不见前面的字母, 心里总感觉不踏实。可以通过下面的命令打开路由器的日志同步功能:

R1(config)#line console 0

R1(config-line)#logging synchronous

这样即使有日志影响了键盘输入, 路由器会在最下面的新行中重新恢复先前的输入。

8.9 辅助地址

Windows Server 2003 中, 同一块网卡可以配置多个 IP 地址, Cisco IOS 也提供了对单个接口的多个 IP 地址的支持, 叫做辅助地址。为理解这样做的优点, 可以设想这种情况。假设以前使用一个 C 类寻址方案, 共有 254 个可以使用的主机 IP。现在公司扩展了, 需要容纳 350 个用户, 而且它们都需要自己的 IP 地址。为避免增加更多的硬件或重新配置 IP 地址的烦琐, 可以在路由器上分配辅助 IP 地址, 以允许两个逻辑子网使用相同的物理接口。如图 8-9-1 所示, 有两台主机 PC1 和 PC2, 它们处于不同的逻辑子网上, 但是连接在路由器相同的物理接口上。

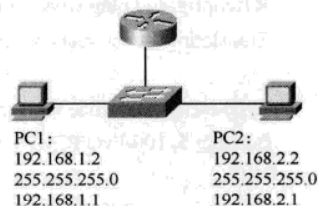


图 8-9-1 配置辅助 IP 地址

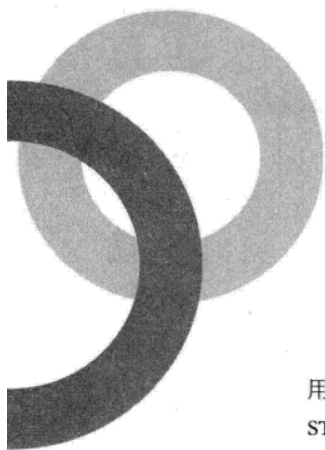
在路由器上配置下面的命令:

Router(config)#int fa 0/0

Router(config-if)#ip add 192.168.1.1 255.255.255.0

Router(config-if)#ip add 192.168.2.1 255.255.255.0 secondary

路由器的 Fa0/0 接口上配置了两个 IP 地址, 互连 PC1 和 PC2 所在的网段。第二个 IP 地址, 后面一定要加 “secondary” 参数, 不然会覆盖前一个 IP 地址。路由器同一个接口只能配置一个主地址, 但却可以配置很多个辅助地址。这种配置方式只能算是一种临时性的解决方案, 因两个子网间并不没有完全隔离, 它们相互间可以收到对方子网的广播, 通过修改 IP 地址到另一个子网, 流量不用通过路由器就可到达目标主机。也就是说这两个子网间根本没有安全可言, 路由器在这里仅仅是提供了方便, 并不能起到安全防护的作用。



第 9 章 交换机

Chapter 9

本章通过阐述冲突域和广播域的概念，介绍 Switch（交换机）在局域网分段中的作用，进一步讲解了交换机最常用的 VLAN（Virtual Local Area Network，虚拟局域网）、STP（Spanning Tree Protocol 生成树协议）、链路聚合的相关概念和配置。通过学习本章，读者可以正确配置 VLAN 来隔离广播，增强网络安全；可以正确配置 STP 来阻止交换机网络中的环路；可以正确配置链路聚合来满足高速链路的需求。

本章使用到的交换机均为 Cisco3640 路由交换机，本章涉及的所有实验均可在 dynamips 的路由和交换机架上完成。

9.1 交换概述

目前交换机在网络中的应用越来越广泛，并发挥着举足轻重的作用。本节的内容包括冲突域和广播域、局域网的分段以及交换机的分类。

9.1.1 冲突域和广播域

随着商业的发展，为商业提供大量信息的网络也得到飞速发展。而随着网络的飞速发展，网络带宽也成为了严重问题。简单地讲，带宽就是这样一个概念，它只能允许一定量的数据同时通过，当试图发送更多的数据时，就会出现瓶颈与拥塞现象。有两个概念对网络性能影响很大，一个是冲突域，另一个是广播域。下面介绍它们是如何影响网络性能的。

1. 冲突域

假如一个人想通过一个独木桥，但每次想通过的时候，对面都有一个人走过来，如果强行通过，两个人将会在桥中相遇，发生碰撞，这与使用 CSMA/CD（Carrier Sense Multiple Access with Collision Detection，带冲突检测的载波侦听多路访问）协议的以太网上发生的情况很相似。电气与电子工程师协会（IEEE）将 CSMA/CD 以太网定义成 802.3 标准，如今，该标准的使用遍及整个网络领域。开放系统互联模型（OSI）第二层的介质访问控制（MAC）子层，就是使用 CSMA/CD

协议访问物理介质。

网络中的所有节点在任何需要的时候都可以发送数据，而 CSMA/CD 网络却努力确保任一时刻只有一个节点发送数据。但是，两个节点却有可能同时发送数据，出现两台主机同时发送数据的情况，就会导致碰撞，如图 9-1-1 所示，所有 16 个结点和 5 台集线器构成了一个大的冲突域，任一时刻只能有一个结点发送数据。这与刚才所讲的两人同时通过独木桥一样，因为没有注意到桥的对面有人走过来，当两人走到桥中间时，发生碰撞，可能有人就要下河洗澡了。

网络节点虽然也会发生碰撞，但有一点和两个人过独木桥不同，两人相撞之后就很难恢复，而网络节点却可以继续侦听线路。如果一个设备检测到碰撞，它就停止发送，并将碰撞情况通知其他节点。其他所有正在发送的节点得到通知后停止发送，并等待一个随机的时间后，再次尝试发送，碰撞只发生在以太网中。值得关注的是，碰撞频率达到一定程度时才会影响网络性能。

在实际工作中，以太网 Hub 前面板上的 LED 指示灯能帮助用户检测何时网段上冲突达到饱和。尽管有很多个工具能够检测到网络速度变慢以及瓶颈问题，但是观察 Hub 上的 LED 指示灯既快又方便。

通过使用二层以上（包括二层）的设备，如网桥、交换机、路由器等，可以对局域网进行分段，有效的隔离冲突。尤其是在冲突经常发生的地方，可以考虑使用交换机代替集线器，因交换机每个端口就是一个单独的冲突域。

2. 广播域

在讨论广播域之前，必须先明白什么是广播。广播就是要发送到网段上的所有节点、而不是单个节点或一组节点的数据。要广播的节点将数据送到 MAC 地址 0xFFFFFFFF，就能实现上述目的。因此说，广播域由一组能够接收同组中所有其他节点发来的广播报文的节点构成。通常情况下，通过 Hub、网桥和非 VLAN 型交换机等接在路由器一个端口上的所有节点构成一个广播域，如图 9-1-2 所示。

对上述网络来说，所有 52 个节点、7 台集线器、一台网桥构成了一个广播域，二个冲突域。一个 Hub 上的节点发送广播，所有剩余的 51 台设备都能收到。随着网络规模的扩大，广播域中广播报文相遇的次数也随之增加。所有这些广播报文确实会影响网络的性能，如果管理不当，甚至会导致整个网络的崩溃。

通过使用 3 层以上（包括 3 层）的设备，如路由器或三层交换机，可以对局域网进行分段，有效地隔离广播。尤其是在节点众多的情况下，可以考虑使用三层设备进行广播隔离，提高性能，降低安全风险。

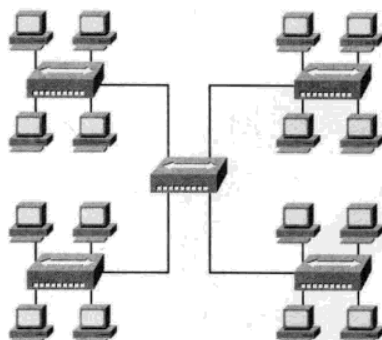


图 9-1-1 集线器构成的一个冲突域

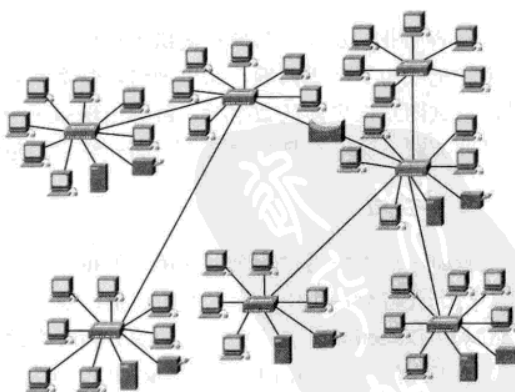


图 9-1-2 网桥和集线器构成的一个广播域

9.1.2 局域网分段

影响局域网性能的两个常见问题是过高的碰撞率和过多的广播业务。这两个问题都可通过“分段”方法解决，该方法将网络分割成较小的段。

网桥、交换机和路由器通过将冲突域分割成较小的部分，从而降低对带宽的竞争，减少碰撞。路由器还有一个好处，它可以控制广播业务流，也就是能将广播域分成更小的域。对广播域来说，“子网（subnet）”和“虚拟局域网（VLAN）”这两个词比“分段”更常见，一个子网可能会包含很多个冲突域。

1. 用网桥将 LAN 分段

可以用网桥分割冲突域，从而获得更好的网络性能。但是，如果网桥放置的位置不当，则会使网络性能下降而不是提高。网桥不同于路由器，它工作在 OSI 模型的第二层（数据链路层）的 MAC 子层。网桥会自动建立了一张表，记录了所有通过网桥的帧的源 MAC 地址，以及这些 MAC 地址所对应的网桥端口。通过检查帧中的目的 MAC 地址，决定是否转发该数据帧到其他端口，如果帧的源和目的 MAC 地址所在的网桥端口相同，网桥将不转发该数据帧到其他端口，否则网桥把数据帧转发到对应的网桥端口。但是，如果网桥不知道目的 MAC 地址所在的端口，它就用泛洪的方式向与其相连的除接收端口以外的所有端口转发该帧。

2. 用交换机将 LAN 分段

用交换机将 LAN 分段可提高终端用户设备的性能。交换机不仅是多端口网桥，而且采用专用集成电路构成的硬件完成网桥用软件实现的操作，数据转发速度比网桥更快。与网桥一样，交换机也基于源 MAC 进行学习，基于目的 MAC 地址进行转发，以确保将数据转发到正确的端口上。如图 9-1-3 所示就是一个用交换机将 LAN 分段的例子。与 Hub 相比，这种方法增加了带宽。因为每个网段都是在交换机上各自的专用端口内运作，只有目的地址为其他网段的业务流才会经过交换机，并且只在源端口和目的端口间发送，其他与该源和目的 MAC 地址无关的端口都不受影响。

有一点需要注意，由于交换机本质上是使用专用集成电路的多端口网桥，所以它也同样传递广播业务流。如图 9-1-3 所示，包括 4 个冲突域，1 个广播域。

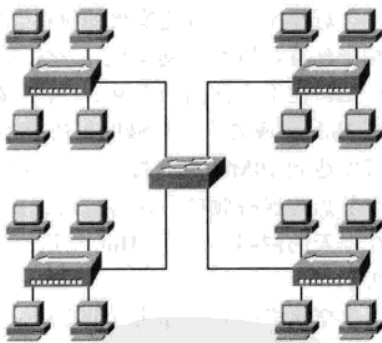


图 9-1-3 用交换机将 LAN 分段

注意



可以在支持 VLAN 配置的交换机上，通过划分 VLAN，把交换机端口分隔到不同的 VLAN 中，一个 VLAN 就是一个广播域，一个 VLAN 中的广播不会被交换机转发到其他 VLAN 中。支持 VLAN 的交换机上配置了多少个 VLAN，就有多少个广播域。

3. 用路由器将 LAN 分段

路由器能分割广播域，因为默认情况下，它不转发任何广播业务流。路由器工作在 OSI 模型的第三层（网络层），由于它不转发广播业务，因此就有一种减小广播域的简单方法，即把图 9-1-3 中的交换机换成路由器。

如图 9-1-3 和图 9-1-4 所示，两幅图的不同之处是把交换机换成了路由器。与路由器相连的 4 个网络，分别构成各自独立的广播域。因为路由器不转发任何广播业务流，所以从一个 Hub 上发出的广播报文不能传到其他任何一个 Hub 上。通过使用路由器互连不同的网络，隔离了不同的广播域，进一步降低了发生冲突的可能。

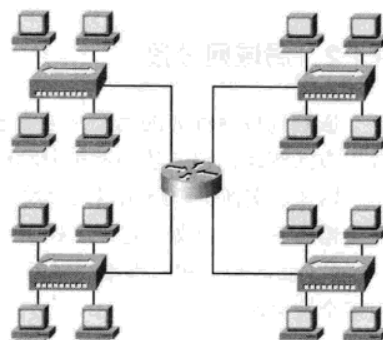


图 9-1-4 用路由器将 LAN 分段

9.1.3 交换机的分类

已经讨论过多种 LAN 分段方法，现在该仔细研究一下 LAN 中的交换技术。第三层交换和传统的第二层交换技术目前都被普遍使用。但二者的不同之处在于第三层交换是基于网络层目的地址转发分组，而第二层交换是基于 MAC 地址转发帧。

在网络出现的初期，使用同轴电缆的 10Base2 或者使用一两个 Hub 的 10BaseT 是可以接受的。大多数业务流并不需要很多的带宽，因此，可供用户共享的带宽很多。但在今天网络已连接到每一个职工的计算机，而视频以及音频电话会议这样的应用越来越普遍，带宽就成为一种相当宝贵的资源。

近年来，随着交换机的价格迅猛下跌，交换机变得相当便宜，以至于交换机几乎完全取代了 Hub 的位置。例如，在本章前面的图 9-1-1 中，看到 16 个节点通过 5 个 Hub 构成的一个局域网。所有 16 个节点共享理论上可以达到 10Mbit/s 的带宽。如果在这种网络上同时向两个节点传送视频信号，可能就会出现带宽不足的问题。在今天的网络环境中，Hub 可用交换机代替，如图 9-1-5 所示。

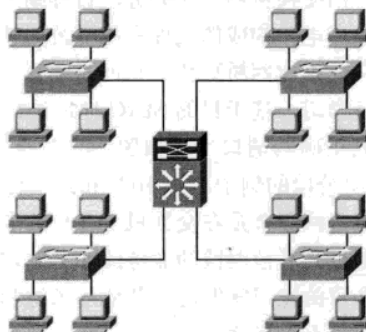


图 9-1-5 由 16 个节点构成的交换式网络

交换机的分类方法有很多种，如从网络覆盖范围划分、根据传输介质和数据传输速率划分、根据应用层次划分、根据交换机的结构划分、根据是否支持网管功能划分、根据交换机的功能层划分。本书只介绍根据交换机的功能层分类。

1. 传统的二层交换机

传统的二层交换机工作在 OSI 模型的第二层（数据链路层）。第二层交换机依赖于链路层中的信息（如 MAC 地址）完成不同端口数据间的线速交换，主要功能包括物理编址、错误校验、帧序列以及数据流控制。这是最原始的交换技术产品，不支持 VLAN 功能，所有端口都属于默认 VLAN。目前国内桌面型交换机一般是属于这种类型，因为桌面型的交换机一般来说所承担的工

作复杂性不是很强，又处于网络的基层，所以只需要提供最基本的网络接入功能即可。目前第二层交换机应用最为普遍（主要是价格便宜，功能符合小企业实际应用需求），一般应用于小型企业的接入层。要说明的是，所有的交换机在协议层次上来说都是向下兼容的，也就是说所有的交换机都能够工作在第二层。

2. VLAN 型交换机

VLAN 型交换机与传统型的二层交换机功能类似，区别在于 VLAN 型交换机支持 VLAN 功能，能添加、删除、修改 VLAN，并进行端口的划分。一般认为是 VLAN 型交换机有几个 VLAN 就有几个广播域，而传统的二层交换机只有一个广播域。此外，VLAN 型交换机都是可网管型交换机，远程管理和配置都比较方便，但价格相对传统型的二层交换机偏贵，一般应用于中、大型企业的接入层。

3. 路由交换机

路由交换机也叫做多层交换机，根据交换机的型号不同，路由交换机甚至可以工作在 OSI 模型的第七层（应用层），一般的路由交换机都可以工作在网络层，它比第二层交换机更加高级，功能更强。路由交换机因为能工作于 OSI 模型的网络层，所以它具有路由功能，并能实现不同网段间数据的线速交换。当网络规模较大时，可以根据特殊应用需求划分为小而独立的 VLAN 网段，以减小广播所造成的影响。通常这类交换机是采用模块化结构，以适应灵活配置的需要。在大型网络中，路由交换机已经成为基本配置设备，如图 9-1-5 中中间的交换机就属于路由交换机。

路由交换机既可工作在 OSI 的第三层，起到路由选择的功能，又具有几乎达到第二层交换的速度，且价格相对较低。三层交换机与路由器的区别成为困惑很多初学者的难题。接下来，这里对两者进行简单的对比。

传统的路由器在网络中有路由转发、防火墙、隔离广播等作用，不同网段之间通信需要通过路由器转发。路由器对数据包的处理延时比二层交换机长，因路由器首先要判断帧的目的 MAC 地址是否是发给路由器的，如果是发给路由器的，还要拆包，查找路由表，重新封装再转发，而二层交换机只需要根据帧的目的 MAC 进行转发。集线器对数据包的处理延时比交换机小，因集线器连查询 MAC 地址表的时间也不需要了。由于在局域网内，不同网段之间的通信数据量很大，这样，如果路由器要对每一个数据包都路由一次，延时变大。随着网络上数据量的不断增大，路由器和交换机之间的带宽也将成为瓶颈。如图 9-1-6 所示，SW1 交换机上 192.168.1.0/24 网段中的多台计算机需要访问 SW2 交换机上 192.168.2.0/24 网段中的多台计算机，所有的数据包都需要经过路由器处理，延时变大。尽管交换机的内部处理带宽可以达到几 Gbit/s，甚至是几十 Gbit/s，可 SW1 和 SW2 之间的吞吐量不会超过路由器和交换机之间的链路带宽。

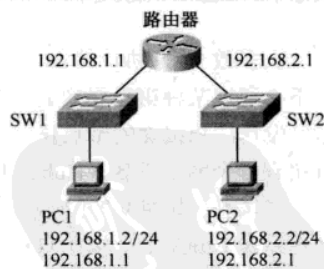


图 9-1-6 路由器互连不同的网段

第三层交换技术就是将路由技术与交换技术合二为一的技术。在对第一个数据流进行路由后，它将会产生一个 MAC 地址与 IP 地址的映射表，当同样的数据流再次通过时，将根据此表直接从二层通过而不用再次路由，从而消除了路由器进行路由选择而造成网络的延迟，提高了数据包转发的效率，这也就是我们常说的“一次路由，多次交换”。路由器的转发采用最长匹配的方式，实

现复杂, 通常使用软件来实现。而三层交换机的路由查找是针对流的, 它利用 CACHE 技术, 很容易采用 ASIC 实现, 因此, 可以大大节约成本, 并实现快速转发。此外, 如图 9-1-7 所示, 虚拟交换机 1 上 192.168.1.0/24 网段中的多台计算机需要访问虚拟交换机 2 上 192.168.2.0/24 网段中的多台计算机, 所有的数据包都在三层交换机的内部处理, 交换机内部处理带宽可以达到几 Gbit/s, 甚至是几十 Gbit/s, 而 192.168.1.0/24 网段和 192.168.2.0/24 网段之间的带宽不成问题。

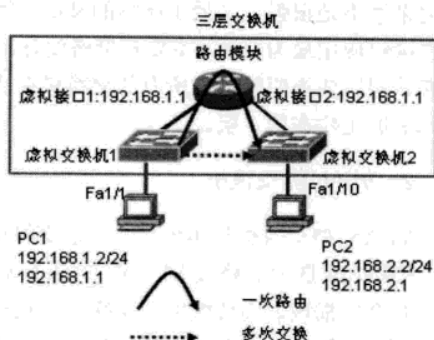


图 9-1-7 三层交换机互连不同的网段

从技术上讲, 路由器和三层交换机在数据包交换操作上存在着明显区别。路由器一般由基于微处理器的引擎执行数据包交换, 而三层交换机通过硬件执行数据包交换。与三层交换机相比, 路由器功能更为强大, 像 NAT、VPN 等功能仍无法被完全替代。处于同一个局域网中的各子网的互联, 可以用三层交换机来代替路由器, 但局域网必须与公网互联以实现跨地域的网络, 这时路由器就不可缺少。使用路由器将网络划分为多个子网, 通过路由所具备的功能来有效进行安全控制策略。三层交换机现在还不能提供完整的路由选择协议, 而路由器则具备同时处理多个协议的能力。当连接不同协议的网络, 像以太网和令牌环的组合网络, 依靠三层交换机是不可能完成网间数据传输的。

所以, 三层交换机并不等同于路由器, 也不可能完全取代路由器。

9.2 VLAN 的实现

本节从 VLAN 的概念和优点讲起, 介绍动态 VLAN 和静态 VLAN, 帧过滤和帧标记, VLAN 干线, VLAN 的封装和工作方式。并以实验的形式介绍 VLAN 的配置, VLAN 间路由的实现。

9.2.1 VLAN 的概念

大多数 LAN 协议的很多功能都依赖于广播。LAN 网段的特征是所有节点都能互相直接通信, 而不必通过某种第三层或更高层的设备, 如路由器。在大多数情况下, 这些直接通信是由向物理地址发送广播报文的节点建立, 然后用单播 MAC 地址实现的。在传统的局域网中, 如果一个节点接到一个网络设备 (Hub、中继器或网桥) 上, 那么它就与其他接在同一设备上的节点属于同一个局域网。如图 9-2-1 所示, 计算机 PCA 接在集线器 HubA 上。接在 HubA 上的任何其他第一层或第二层设备都是同一 LAN 的一部分, 并且接在这些设备 (中继器、集线器、网桥、非 VLAN 型的二层交换机, 以及图中的 Bridge 和 HubB) 上的节点与接在 HubA 上的节点属于同一个 LAN。且图 9-2-1 中所有设备属于同一个 LAN。



图 9-2-1 LAN 范围

从逻辑上讲, 只要不破坏规范, 就可增加或移去 Hub、中继器或网桥, 而 LAN 仍然存

在。说得更抽象一些，局域网实际上就是一组能互相发送广播报文的节点。如果一组节点能互相发送广播报文，就称它们处于同一个“广播域”。说得更明白一些，就是广播域是一组能互相发送广播报文的节点。广播域通常通过路由器互相连接，并且第二层的广播帧不能通过路由器。

广播域是隐含在 VLAN 后面的中心概念。为了简单起见（仅限于现在）称一个 VLAN 就是一个广播域。

虽然一个 VLAN 大致等价于一个广播域，但 VLAN 交换机并不等价于传统型的交换机。区别实际上非常简单，传统型的交换机只包含一个广播域，而 VLAN 交换机可以有多个。尽管对 VLAN 有很多误解，它实际上还是非常简单。普通交换机和 VLAN 交换机之间的主要区别有两个：一个是在同一机架内维护独立广播域的能力，另一个是在机架之间维护独立广播域的能力。

9.2.2 VLAN 的优点

目前 VLAN 在开销、灵活性和安全等方面都表现不错。

1. VLAN 降低了开销

VLAN 的一个优点是降低了开销。考虑一个有 8 个 LAN 的网络，或者说得更明确一点，有 8 个广播域的网络。至于为什么需要多个广播域，原因很多，如广播控制，安全以及资源分组等。如果采用传统的组网技术，实现 8 个广播域需要 8 台集线器和一台有 8 个端口的路由器，如图 9-2-2 所示。图中的集线器也可是一个非 VLAN 型的传统交换机。

通过将每个 LAN 中的节点合理分组，可以使所用的 Hub 数目达到最少。其中一种方法是按地理位置分组，例如，每一组可以代表一幢建筑，或者代表一层建筑。如果设计方案不好，各组比较分散，也就是说局域网的物理位置比较凌乱，就会需要更多的 Hub。设想一下按部门划分局域网，并且大多数部门要跨好几幢建筑的情况，这可能需要在每幢建筑内为每个 LAN 准备一个 Hub，如图 9-2-3 所示。

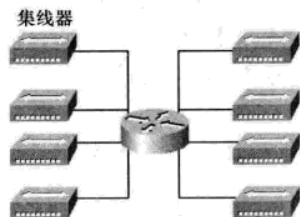


图 9-2-2 传统划分 LAN 的方式

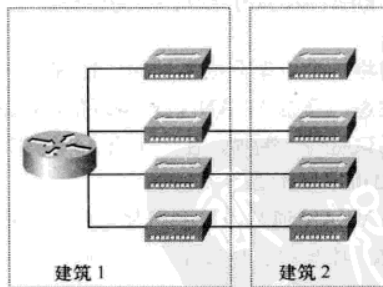


图 9-2-3 跨建筑物的 LAN

以最简单的方式设计 4 个局域网，每个局域网代表一幢 4 层建筑中的一层，每层需要一个 Hub，总共只需要 4 个 Hub。现在，考虑一下 4 个局域网分布在两幢建筑里的情况，就需要 8 个 hub。

现在考虑一个更复杂的设计, 每个局域网都与一个部门相关。园区内有 5 幢建筑, 每幢建筑内的每个部门都有人。这种设计至少需要 20 个 Hub, 如果按每幢建筑里的每个部门一个 hub 还不够容纳此幢建筑里的所有节点, 则需要更多的 Hub。这种设计方案很昂贵, 但主要花费不是在 Hub 上, 而是在楼群之间的布线上, 大多数园区并没有事先在敷设足够的电缆或光缆。如果需要将 LAN 分开, 所需的 Hub 数量就会增加, 并且还必须考虑这些设备之间的互连问题, 有时在楼群之间可能没有足够的物理线路。这就是将机架分成 VLAN 的概念真正有吸引力的原因。只要 VLAN 交换机有足够的端口, 每个传统的局域网就不需要一个单独的 Hub。

2. VLAN 增加了灵活性

对于 VLAN 增加了灵活性这一点, 可能已经非常明显。VLAN 中的节点可以与其所在的 LAN 无关。如果某个职员从一个部门调到另一个部门, 但办公位置并没有发生改变, 网络管理员只须改变对该职员的节点被指派的 VLAN 即可。

下面是动态 VLAN 增加灵活性的例子。同样考虑每个 VLAN 对应一个部门的情况, 如果某些职员经常变动位置, 网络管理员只须使用动态 VLAN, 那么不管这些人所处的地理位置如何, 他们都会在正确的 LAN 中。

3. VLAN 增加了安全

VLAN 能提高网络安全。如果网络划分为 VLAN, 那么不同 VLAN 中的节点要互相通信, 必须通过一个 3 层以上 (包括 3 层) 的设备, 如三层交换机、路由器或者是一个防火墙, 在 3 层设备上可以配置基于 IP 的访问控制。此外, VLAN 交换机能够控制节点访问特定的端口, 还能够防止某些节点通过与其他节点交换端口信息而绕过安全检查机制。如果每个 VLAN 是一个广播域, 那么不同 VLAN 之间的互联就需要一个路由器。在这种情况下, 就可在路由器上配置访问列表, 使其阻止部分业务流在 VLAN 之间流动。这与在路由器上利用访问列表阻止业务流从一个接口流向另一个接口的情况相似。由于业务流不能在一个交换机内的多个 VLAN 之间随意流动, 安全绝对可靠。

9.2.3 动态 VLAN 和静态 VLAN

如何将一个机架分成不同的广播域是一个值得探讨的问题。指派 VLAN 的方法主要有两种: 静态和动态。静态 VLAN 很容易理解, 静态 VLAN 由其所处的机架特征定义, 通常包括插槽、端口或端口组等。例如, 在一个有 16 个端口的交换机上, 1~8 号端口可以属于 1 号 VLAN, 9~16 号端口可以属于 2 号 VLAN。

动态 VLAN 通常由接到机架上的节点的某些特征定义。这可以是节点的 MAC 地址, 正在使用的协议, 甚至是某些认证信息, 如名字与口令等。

Cisco 既支持动态 VLAN 也支持静态 VLAN。Cisco 的动态 VLAN 基于 MAC 地址 (基于 MAC 地址的配置方法, 工作量巨大, 且不安全, 因 MAC 地址可以随意修改, 所以现在几乎没有企业使用基于 MAC 地址配置 VLAN。目前比较常见的是基本 802.1x 的动态配置 VLAN 的方式, 根据用户名和密码配置 VLAN, 本书将在第 4 部分介绍 802.1x 动态 VLAN 的配置), 而静态 VLAN 则基于指派端口。指派端口 (port-assigned) 指可以以单个端口为基础指定 VLAN。

9.2.4 帧过滤与帧标记

传统型的交换机（非 VLAN 交换机）是如何知道一个帧要发往哪个目的端口的呢？当一个帧进入交换机时，交换机必须决定将其送往何处。传统型的交换机只简单地检查此帧的目的 MAC 地址，再参照 MAC 地址表，然后将其转发到适当的端口，而不考虑此帧是从哪儿来的。如果不知道目的地址，或者目的地址为广播地址，那么交换机就用“泛洪法”将其转发到除发送此帧之外的所有端口。

在 VLAN 中，情况要稍复杂一些。除了要根据目的 MAC 地址作转发决定外，还必须考虑帧的源地址，因为该帧通常会影响到它所属的 VLAN，并因此影响它可能会被转发去的端口。追踪一个帧的源地址至少有两种显而易见的方法。第一种是确定帧进入的端口属于哪一个 VLAN，这种方法称为“帧标记”，也称“显式标记”。注意这个过程只发生在交换机的内部。帧本身不会被改动，但会单独记录与帧有关的其他信息。另一种追踪帧的源地址的方法是为每个 VLAN 保持一张 MAC 地址表（这张表由交换机通过某种方式完成）。确定目的地址后，就做出是否转发此帧的决定。这种方法称为“帧过滤”，也称“隐式标记”。从理论上讲，也可通过其他标准，如第三层信息实现帧过滤。

这两种方法的主要区别在于何时做出 VLAN 决定。在帧标记中，帧一进入 VLAN，决定就已经做出。在帧过滤中，当帧需要转发时才做出决定，帧刚进入交换机时，并不需要做出决定。对于交换机如何在其内部做出 VLAN 成员关系的决定，大多数讨论都是学术性的。事实上，交换机如何在其内部追踪 VLAN 并不重要，只要它能做出正确的转发决定。

帧标记的优点是能够立即标识 VLAN，并且不需要对帧作进一步的 VLAN 成员关系决定。标记过程通常通过为帧增加一个包含 VLAN 号的域来实现（Cisco 文档中有时将这个过程称为“VLAN 着色”（VLAN Coloring））。这种方法的缺点是大多数不支持 VLAN 的设备会把这种帧当成无效帧，因为它们没有遵照标准格式。同样，在帧标记方法中也有很多不兼容性问题，因此，使用帧标记通常会限制采购设备的范围。IEEE 802.1Q 标准定义一个标准的帧标记机制，以解决这个问题。

帧过滤的优点是不修改帧，因此，在帧通过标准网络时不会出现问题。缺点是所有 VLAN 设备必须能对每个帧做出唯一的 VLAN 决定。这意味着如果按数据帧中的源 MAC 地址进行过滤，那么所有 VLAN 交换机必须拥有一张 MAC 地址表，该表还要包含每个 MAC 地址所属的 VLAN。其他帧过滤方法也有同样的问题，例如，按第三层地址的过滤，即使是在 VLAN 与第三层地址直接相关的情况下过滤起来比较容易，也还是存在这种问题。要想使这种类型的设计方案可管理并可扩充，就需要一种能够用于 VLAN 交换机之间相互通信的协议。

对于这类考试，Cisco 要求知道这两种方法的区别。事实上，帧标记多少占了点上风。所有的交换机厂商在他们的实现方案中都喜欢采用帧标记，IEEE 里的相关标准也是为帧标记制定的，传统的骨干网（FDDI）支持帧标记，Cisco 还支持两种另外的帧标记。只有 ATM LANE 是个例外，它与帧过滤更相似。

9.2.5 VLAN 干线

本小节中有关帧标记和帧过滤的介绍将更多地侧重于如何在交换机之间运用这些思想，而不

是在单个交换机内部。VLAN 交换机的主要特点是能够在单个交换机内部或多个交换机之间支持多个独立的 VLAN。下面, 开始介绍如何在交换机之间扩展 VLAN。

对于多个 VLAN 交换机来说, 一条干线就是两个交换机之间的连接, 它在两个或两个以上的 VLAN 之间传输业务流。这与两个普通网桥之间的一条链路不同, 因为每个交换机必须确定它所收到的帧属于哪个 VLAN。虽然这增加了某种复杂性, 但同时也带来了很大的灵活性。考虑本章前面在多建筑园区中按部门定义 VLAN 的例子。即使通过将每幢建筑中的机架合并到一个机架中, 从而大量减少一幢建筑中的机架数, 在楼群之间每个 LAN 还是需要一条独立的链路。如果使用干线连接, 只要有足够的带宽, 每幢建筑只需要一条链路就够了, 如图 9-2-4 所示, 在每台交换机上建立 4 个 VLAN, 把端口划入对应的 VLAN, 2 台交换机之间使用干线连接, 干线上可以传输 4 个 VLAN 的数据。

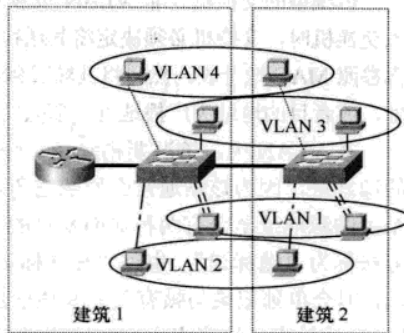


图 9-2-4 支持 VLAN 干线的链路

对于这种设计, 如何在 VLAN 内部处理帧就变得非常重要。交换机在其内部处理帧, 这使其在做 VLAN 决定时有很大的灵活性, 因为它通常能得到以多种方式处理 VLAN 决定时所需的足够信息。一旦帧离开了交换机处理器的控制而进入一段哑线路, VLAN 就会变得复杂一些。

为决定是不是对帧进行标记, 交换机必须知道它将帧发出去的线路的另一端是什么设备。最简单的情况是一个端节点, 如一台计算机或一台服务器。典型情况下, 端节点对 VLAN 一无所知 (可以在某些操作系统上运行支持 VLAN 的软件)。在端节点情况下, 交换机只需简单地将帧恢复成原始状态即可。

如果帧是放置在一个既有端节点, 又有交换机的网段上, 那就必须考虑是否使用帧标记, 因为某些节点可能会认为这样的帧是非法的。这通常不会造成什么故障, 因为大多数节点可能只是忽略这些帧而已; 如果是负责记录网络统计数据的节点, 那它也只是报错罢了。如果帧是送给另一个交换机, 发送方交换机就必须知道接收方交换机能处理的标记格式类型。至少有如下 3 种处理方法。

1. 静态干线配置

静态干线配置最容易理解。干线上每一个交换机都可由配置设定发送及接收使用特定干线连接协议的帧。在这种设置下, 端口通常专用于干线连接, 而不能用于连接端节点, 至少不能连接那些不使用干线连接协议的端节点。当自动协商机制不能正常工作或不可用时, 静态配置是非常有用的, 其缺点是必须手工维护。

2. 干线功能通告

交换机可以周期性地发送通告帧, 表明它们能够实现某种干线连接功能。例如, 交换机可以通告自己能够支持某种类型的帧标记 VLAN, 按这个交换机通告的帧格式向其发送帧是不会有错的。交换机的功能还不止这些, 它还可以通告它现在想为哪个 VLAN 提供干线连接服务。这类干线设置对于一个由端节点和干线混合组成的网段可能会很有用。

3. 干线自动协商

在这种情况下, 交换机周期性地发送指示帧, 表明它们希望转到干线连接模式。如果另一端的交换机收到并识别这些帧, 同时自动进行配置, 那么两端的交换机就会将这些端口设成干线连接模式。这种自动协商通常依赖于两端交换机 (在同一网段上) 之间已有的链路, 并且与这条链路相连的端口要专用于干线连接, 这与静态干线设置非常相似。

与几乎所有的 VLAN 交换机一样, Cisco 交换机也能通过配置进行静态干线传输设置。Cisco 交换机不使用通告报文决定何时发送干线帧, 但一旦通过某种其他方式激活了干线, 这些交换机的确会使用通告报文来指示哪些 VLAN 是可用的, 并且会维持这些 VLAN 的相关信息, 这项功能称为虚拟干线传输协议 (VTP)。例如, 在一个有几十台交换机的企业网中, 有十几个部门存在, 需要在每一个交换机中划分十几个 VLAN, 工作量较大, 这时可以把一台交换机设成 VTP Server, 并配置对应的 VLAN, 把其余的交换机设成 VTP Client, 使它们可以自动“学习”到 Server 上 VLAN 信息。当然并不是所有厂商的交换机都支持该功能, 限于篇幅, 本书不对 VTP 做讲解, 感兴趣的读者可以查阅相关的资料。Cisco 交换机支持自动协商机制, 这项功能的默认设置是半禁止状态, 因此交换机之间的每一条连接不会自动成为一条干线。在默认配置下, 如果用手工作方式将两个交换机中的一个配置成干线模式, 那么另一个也会自动地转换到干线模式。这表明要想使干线传输功能生效, 只需配置链路的一端即可。

9.2.6 VLAN 的封装和工作方式

下面介绍几个干线传输协议。Cisco 的 Catalyst 系列交换机支持 4 种干线传输协议: 交换机间链路 (ISL)、802.10、802.1Q 以及局域网仿真 (LANE)。并不是所有的干线传输协议在每一种型号 Catalyst 交换机上都能使用, 例如, LANE 作为一种 ATM 协议, 就不能在不支持 ATM 的低端交换机上使用。要想知道何种交换机支持何种干线传输协议, 请参考交换机的相关参数文档。802.10 和 LANE 并不常用, 本书仅针对最常使用的两种干线传输协议 ISL 和 802.1Q 进行介绍。

1. ISL

交换机间链路 (ISL) 是 Cisco 创建的私有干线传输协议。这里“私有”是指该协议不是由一个独立的标准组织创建并通过的。但这并非一定表明该协议在非 Cisco 产品中看不到。实际上多宿主服务器 (Multihome Server) 中就有一些网卡和驱动程序能够执行 ISL, 并且还有一种免费 Linux 驱动程序能够支持 DEC 公司基于 Tulip 的快速以太网卡, 有些交换机厂商也在它们的交换机产品中支持 ISL。

Cisco 在其路由器和 Catalyst 交换机产品的快速以太网端口上实现了 ISL 协议。在当前的软件中, ISL 可用于为以太网、FDDI 以及令牌环网干线传输 VLAN 业务流。当从一个 ISL 支持的 LAN 发出的帧要放置在 ISL 干线上时, 必须在这个帧的开头另外加上一个帧头, 称为 ISL 头。

稍后讨论这个帧头, 现在, 只简单地知道帧头中有 10 个 bit 用来标识 VLAN 即可。10 位可表示 1 024 个 VLAN 号, 该软件最早的版本只支持 256 个 VLAN。Cisco 目前只用 10 位表示 VLAN 号, 这能够表示 1024 个 VLAN, 编号为 0~1023, 其中有很多号是保留的。因此, 有些 Cisco 文

档中称可用的 VLAN 号是 1 000 个。

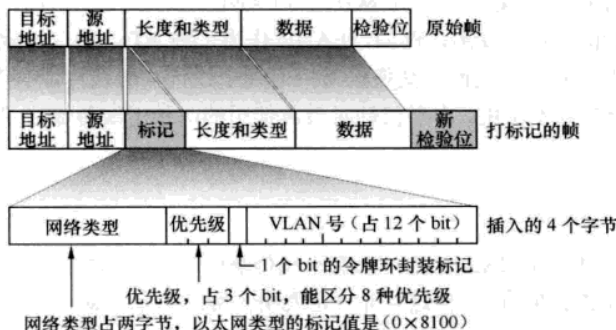
ISL 能支持多种不同大小的帧。ISL 头占用 26 字节, 当干线传输数据帧时, 这 26 字节也要加到帧里。同时, 在帧尾还要加上一个 4 字节的新的 CRC (循环冗余校验) 校验码。这种为帧增加一个新头与校验和的过程称为封装。ISL 封装整个帧, 而不做任何分割工作。

ISL 不能在 10Mbit/s 以太网上运行的原因有多个, 其中有一个技术方面的原因是因为 Cisco 用于 10Mbit/s 以太网的芯片组硬件上只支持最大帧长 1 518 字节, 公司不会再去设计一个新的 10Mbit/s 以太网芯片组。从这以及其他一些事情也能看出, 快速以太网硬件就其所能接受的帧范围来说要更灵活一些, 这一点在用软件升级时对兼容性很有帮助。例如, 为提高吞吐率而提出的增加快速以太网最大帧长的建议就很容易通过。

ISL 在现有的帧前加上一个头, 在尾部加上校验和并发送。为了使这样的主干协议尽可能简单, Cisco 以违反以太标准为代价, 要求采用专用端口, 毕竟它是一种有理由的折中。总之, 对 Cisco 的全部设备或其他一些决定采用 Cisco 协议的厂商而言, 这是非常合理的折中。

2. 802.1Q

802.1Q 协议, 即 Virtual Bridged Local Area Networks 协议, 主要规定了 VLAN 的实现标准。以前, 各个厂商都声称它们的交换机实现了 VLAN, 但各个厂商实现的方法都不相同, 所以彼此无法互连。这样, 用户一旦买了某个厂商的交换机, 就没法使用其他厂商的了。而现在, VLAN 的标准是 IEEE 提出的 802.1Q 协议, 只有支持相同的开放标准才能保证网络的互连互通, 以及保护网络设备投资。802.1Q 的帧是在原来的以太网帧头中的源地址后增加了一个 4 字节的 802.1Q 帧头, 帧之后重新计算 FCS (Frame Check Sequence, 帧检验序列), 用新的 FCS 替换原来帧中的 FCS, 其他字段保持不变。修改前后的帧如图 9-2-5 所示。



新增标签头中的 4 字节信息解释如下。

- 网络类型: 2 字节的标签协议标识, 以太网帧的值是 0x8100。
- VLAN 标识: 这是一个 12 位的域, 指明 VLAN 的 ID, 一共 4 096 个, 每个 802.1Q 的帧都会包含这个域, 以指明自己属于哪一个 VLAN。
- 令牌环标记: 这 1 位主要用于总线型的以太网与 FDDI、令牌环网交换数据时的帧格式。
- 优先级: 这 3 位指明帧的优先级。一共有 8 种优先级, 主要用于判断当交换机阻塞时, 优先发送哪个数据包。

3. VLAN 工作方式

接下来介绍 VLAN 的工作方式，因为 802.1Q 是一个标准协议，使用面广，所以接下来的分析和配置均以 802.1Q 为例。如图 9-2-6 所示，假使 PC1、PC3 属于 VLAN2，PC2 和 PC4 属于 VLAN3。当 PC1 发送一个数据包给 PC3 时，交换机 SW1 从 Fa1/4 端口接收一个数据包，SW1 会根据 Fa1/4 号端口所属的 VLAN 组，自动给该数据包添加一个该 VLAN 的标签头，然后再将数据包交给数据库查询模块，数据库查询模块会根据数据包的目的地址和所属的 VLAN 进行查询，发现目标 MAC 是从 Fa1/1 端口学习过来的，之后交给转发模块，转发模块看到这是一个包含标签头的数据包，Fa1/1 接的是 SW2 交换机并且 SW2 交换机也支持 VLAN，可以识别 802.1Q 标签头，SW1 把包含标签头的数据包保持原样从 Fa1/1 口发出去。SW2 从 Fa1/2 口收到一个包含标签头的数据包，因 SW2 的 Fa1/2 端口支持 VLAN，可以识别 802.1Q 标签头，将数据包交给数据库查询模块，数据库查询模块会根据数据包的目的地址和所属的 VLAN 进行查询，发现目标 MAC 是从 Fa1/4 端口学习过来的，并且 Fa1/4 端口也属于 VLAN2，该数据包被交给转发模块，转发模块看到这是一个包含标签头的数据包，由于 Fa1/4 接的是一台 PC，PC 不能识别 VLAN 信息，SW2 移除 802.1Q 标签头，把数据包从 Fa1/4 端口发出去。

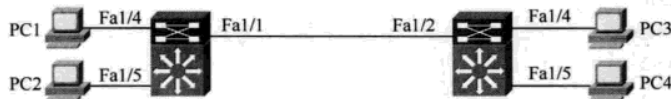


图 9-2-6 VLAN 工作方式

至于交换机何时添加或删除 802.1Q 标签头，与交换机的端口有关系，如果交换机的端口接的是一台计算机，那么该端口属于接入端口（Access），需要添加或移除 802.1Q 标签头；如果交换机的端口接的是另一台交换机，那么该端口属于主干端口（Trunk），一般 802.1Q 标签头不会被改变，特殊情况除外（Trunk 端口会添加或移除该端口 Native VLAN 的 802.1Q 标签头）。

9.2.7 配置 VLAN

打开 dynamips 模拟器的网络（也就是 Network）机架，启动 SW1、SW2、PC1、PC2、PC3、PC4 6 台设备，完成图 9-2-6 所示的 VLAN 的配置。所有设备的配置如下，其中斜体部分为对配置的解释。

SW1 的配置如下：

```
Router#conf t
Router(config)#host SW1
SW1(config)#no cdp run    关闭 CDP 协议，否则会提示快速以太网双工不匹配
SW1(config)#exit
SW1#vlan database    进入 VLAN 配置模式
SW1(vlan)#vlan 2    添加 VLAN 2，交换机上默认只有 VLAN 1
SW1(vlan)#vlan 3
SW1(vlan)#exit    添加的 VLAN 在 exit 或 apply 时才起作用，输入 abort 将放弃 VLAN 的修改
SW1#conf t
```

```
SW1(config)#int fa 1/4 进入接口配置模式
SW1(config-if)#switchport mode access 把端口设成接入端口
SW1(config-if)#switchport access vlan 2 把端口加入 VLAN 2, 默认情况下, 交换机的所有端口都属于 VLAN 1
```

```
SW1(config-if)#int fa 1/5
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 3
SW1(config-if)#int fa 1/1
SW1(config-if)#switchport mode trunk 把端口设成主干端口, 有些型号的交换机在把端口设成主干前, 要先指定 Trunk 的封装协议, 是 ISL 或 DOT1Q, 这里使用的交换机默认使用的封装协议是 DOT1Q, 所以不用指定了
```

```
SW1(config-if)#int fa 1/2
SW1(config-if)#shutdown 关闭这个不使用的端口
```

SW2 的配置如下:

```
Router#conf t
Router(config)#host SW2
SW2(config)#no cdp run
SW2(config)#exit
SW2#vlan database
SW2(vlan)#vlan 2
SW2(vlan)#vlan 3
SW2(vlan)#exit
SW2#conf t
SW2(config)#int fa 1/4
SW2(config-if)#switchport mode access
SW2(config-if)#switchport access vlan 2
SW2(config-if)#int fa 1/5
SW2(config-if)#switchport mode access
SW2(config-if)#switchport access vlan 3
SW2(config-if)#int fa 1/2
SW2(config-if)#switchport mode trunk
SW2(config-if)#int fa 1/1
SW2(config-if)#shutdown
```

PC1 的配置如下:

```
Router>en
Router#conf t
Router(config)#host PC1
PC1(config)#no cdp run
PC1(config)#int fa 0/0
PC1(config-if)#ip add 192.168.1.1 255.255.255.0
PC1(config-if)#no shut
```

PC2、PC3、PC4 的配置与 PC1 的配置类似, 只是 IP 地址不同, 它们的 IP 分别是 192.168.1.2、192.168.1.3、192.168.1.4。在 PC1 上依次 ping PC2、PC3、PC4 的 IP 地址, 测试网络的连通性, 结果如图 9-2-7 所示, PC1 只能 ping 通 PC3, 类似的 PC2 只能 ping 通 PC4。

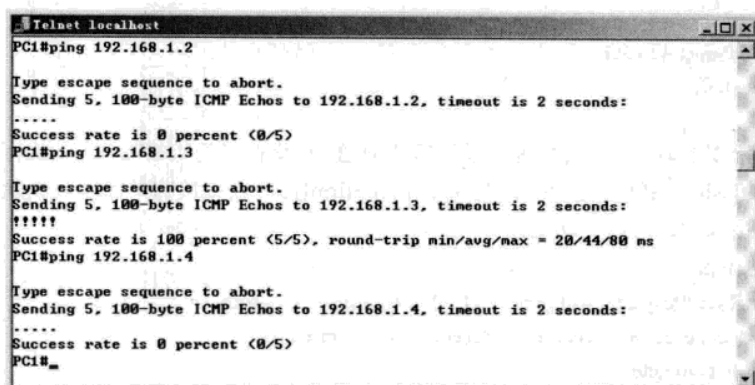


图 9-2-7 VLAN 测试结果

在 SW1 上验证 VLAN 的配置，使用命令 `show vlan-switch`，执行结果如图 9-2-8 所示。

VLAN Name	Status	Ports
1 default	active	Fa1/0, Fa1/2, Fa1/3, Fa1/6 Fa1/7, Fa1/8, Fa1/9, Fa1/10 Fa1/11, Fa1/12, Fa1/13, Fa1/14 Fa1/15
2 VLAN0002	active	Fa1/4
3 VLAN0003	active	Fa1/5
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

图 9-2-8 验证 VLAN 配置

注意



VLAN 的配置信息没有保存在 `startup-config` 文件中，也就是说不能通过删除启动配置文件来删除所有的 VLAN 信息。删除 VLAN 信息的方法有两种：一是在 VLAN 配置模式下，输入 `no vlan ID`，把 VLAN 一个一个地删除；二是执行 `SW1#delete vlan.dat`，删除 VLAN 配置文件，重启交换机后，所有 VLAN 都被删除了。

多次使用实验机架，当在交换机上添加 VLAN，退出时可能会提示 `flash` 空间不足，无法应用，退出失败，要求输入 `abort`，放弃 VLAN 的修改。如下所示：

```

SW1#vlan data
SW1(vlan)#vlan 3
VLAN 3 added:
    Name: VLAN0003
SW1(vlan)#exit
% not enough space on flash to store vlan database. trying squeeze...First creat
e squeeze log by erasing the entire device

% error squeezing flash - (Missing or corrupted log)

```

```
Error on database apply 40: NV storage failure
Use 'abort' command to exit
SW1(vlan)#abort
Aborting....
```

出现上述错误的原因，主要是因为模拟器的问题。在交换机的特权模式下，执行“**erase falsh**”，删除交换机的 flash。系统会提示确认删除，在[confirm]后，直接按回车键确认删除，然后再次添加 VLAN，应用修改，可以成功退出。

```
SW1#erase flash
Erasing the flash filesystem will remove all files! Continue? [confirm]
Erasing device... eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee ...erased
Erase of flash: complete
SW1#vlan data
SW1(vlan)#vlan 3
VLAN 3 added:
    Name: VLAN0003
SW1(vlan)#exit
APPLY completed.
Exiting....
SW1#
```

下面总结一下配置 VLAN 的步骤。

- STEP 1** 在交换机上添加或删除 VLAN。
- STEP 2** 把端口加入 VLAN，可以通过 show vlan-switch 命令检验。
- STEP 3** 如果 VLAN 跨越多个交换机，把交换机之间互连的端口设置成主干端口。

9.2.8 VLAN 间路由

实现 VLAN 间的互访可以借助于路由器或三层交换机。一般不使用路由器的多个端口连接不同的 VLAN，因路由器的端口成本较高，一般使用的是用路由器一个端口连接多个不同的 VLAN 的方式，俗称“单臂路由”。本小节首先介绍“单臂路由”的实现，然后再介绍使用三层交换互连不同 VLAN 的实现方式。

实验 9-1 配置单臂路由

打开 dynamips 模拟器的 Network 机架，启动 SW1、R1、PC1、PC2 这 4 台设备，这里把 SW1 假设成一台二层的 VLAN 型交换机（三层交换机没有额外配置的情况下，可以当成二层交换机使用），R1 是一台路由器。每个设备的 IP 地址配置如图 9-2-9 所示。所有设备的配置如下，其中斜体部分为对配置的解释。

R1 的配置如下：

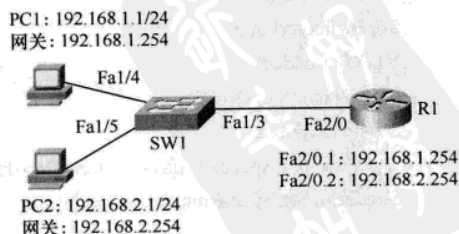


图 9-2-9 单臂路由


```

Router>en
Router#conf t
Router(config)#host R1
R1(config)#no cdp run
R1(config)#int fa 2/0
R1(config-if)#no shut  打开物理接口
R1(config-subif)#int fa 2/0.1 进入 Fa2/0 的第一个子接口，物理接口支持很多个子接口，至于使用哪个子接口没有什么区别，一般习惯使用和 VLAN 号相同的子接口。
R1(config-subif)#encapsulation dot1Q 1 给子接口配置 IP 地址前，要先封装 Trunk 协议，因交换机上封装的是 dot1Q，所以这里也要使用 dot1Q，后面的 1 是指 VLAN 号，VLAN 1 的计算机网关要指向该接口配置的 IP 地址。

```

```

R1(config-subif)#ip add 192.168.1.254 255.255.255.0
R1(config-subif)#int fa 2/0.2
R1(config-subif)#encapsulation dot1Q 2
R1(config-subif)#ip add 192.168.2.254 255.255.255.0

```

SW1 的配置如下：

```

Router#conf t
Router(config)#host SW1
SW1(config)#no cdp run
SW1(config)#no ip routing  关闭三层交换机的路由功能，让它模拟二层交换机，不关闭也没有关系，因本实验中并没有配置三层。

```

```

SW1(config)#exit
SW1#vlan database
SW1(vlan)#vlan 2
SW1(vlan)#exit
SW1#conf t
SW1(config-if)#int fa 1/5
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 2
SW1(config-if)#int fa 1/3
SW1(config-if)#switchport mode trunk

```

PC1 的配置如下：

```

Router>en
Router#conf t
Router(config)#host PC1
PC1(config)#no cdp run
PC1(config)#int fa 0/0
PC1(config-if)#ip add 192.168.1.1 255.255.255.0
PC1(config-if)#no shut
PC1(config-if)#exit
PC1(config-if)#no ip routing  关闭路由器的路由功能，让它模拟一台计算机
PC1(config)#ip default-gateway 192.168.1.254 配置计算机的网关，对于关闭路由协议的路由设备，要使用这条命令来指定默认路由；如果没有关闭路由协议，使用 ip route 0.0.0.0 0.0.0.0 配置默认路由。

```


PC2 的配置如下:

```
Router>en
Router#conf t
Router(config)#host PC2
PC2(config)#no cdp run
PC2(config)#int fa 0/0
PC2(config-if)#ip add 192.168.2.1 255.255.255.0
PC2(config-if)#no shut
PC2(config-if)#exit
PC2(config-if)#no ip routing
PC2(config)#ip default-gateway 192.168.2.254
```

在 PC1 上 ping 192.168.2.1 发现可以 ping 通 PC2。关闭路由器 R1 的 Fa2/0 口后,再次在 PC1 上 ping 192.168.2.1,发现 ping 不通了,原因是 PC1 和 PC2 分属于不同的网段,没有一个三层设备来提供路由,它们之间无法进行路由。不要关闭该机架,下一个实验可以在本实验的基础上完成。

实验 9-2 配置三层交换间路由

为了节省时间,在单臂路由配置的基础上,做些改动来完成三层交换。关闭 4 台设备中的 R1,开启 SW1 的路由功能,把它还原成一台路由交换机,PC1 和 PC2 的配置保持不变。每个设备的 IP 地址配置如图 9-2-10 所示。所有设备的配置如下,其中斜体部分为对配置的解释。

SW1 的配置如下:

```
Router#conf t
Router(config)#host SW1
SW1(config)#no cdp run
SW1(config)#ip routing 开启三层交换机的路由功能
SW1(config)#exit
SW1#vlan database
SW1(vlan)#vlan 2
SW1(vlan)#exit
SW1#conf t
SW1(config-if)#int fa 1/5
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 2
```

SW1(config)#int vlan 1 进入交换机的 SVI (Switch Virtual Interface) 接口,三层交换机支持三类接口:二层的交换端口,可以在端口配置模式下使用命令 `switchport` 改变;路由端口,可以在端口配置模式下使用命令 `no switchport` 改变,改变后这个端口就是一个路由端口,不再属于任何一个 VLAN;SVI 接口,也是三层接口,和路由端口一样也可以配 IP 地址,区别就是这个端口是一个看不见的虚拟端口,一般用做对应 VLAN 的网关,实现不同 VLAN 之间的路由。

```
SW1(config-if)#ip add 192.168.1.254 255.255.255.0
SW1(config-if)#no shut
```

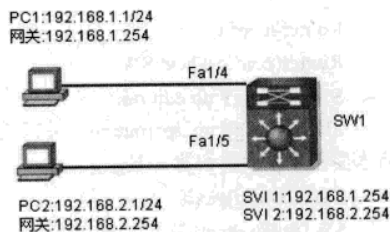


图 9-2-10 三层交换

```
SW1(config-if)#int vlan 2
SW1(config-if)#ip add 192.168.2.254 255.255.255.0
SW1(config-if)#no shut
```

PC1 和 PC2 的配置同单臂路由实验中的配置，在 PC1 上 ping PC2 的地址 192.168.2.1，发现可以 ping 通。如果是在单臂路由实验的基础上配置本实验，可能会 ping 不通。原因是因为 PC1 和 PC2 上已经缓存了它们网关的 MAC 地址，那个 MAC 地址还是 R1 的 Fa2/0 的 MAC 地址呢，可以通过 show arp 命令查看，clear arp 命令用于清除 ARP 缓存，然后再 ping 测试，如果配置无误就可以 ping 通了。

```
PC1#show arp
Protocol Address      Age (min) Hardware Addr  Type  Interface
Internet 192.168.1.1      -      cc03.0530.0000  ARPA   FastEthernet0/0
Internet 192.168.1.254    9      cc00.0530.0000  ARPA   FastEthernet0/0
PC1#clear arp
```

9.3 STP 的实现

在分层网络中，管理员不得不通过冗余拓扑来保障网络的高可用性。然而，网络中额外添加的链路连接着路由器和交换机，会引起流量的环路。这些链路必须能被动态管理，当一个交换机的连接丢失，另一条链路能快速地取代失败链路并且不会产生新的流量环路。本节将介绍 STP (Spanning-Tree Protocol, 生成树协议) 如何在交换网络中解决环路问题和一些高级 STP 的工作方式。主要包括冗余拓扑中存在的问题、STP 工作方式、生成树的端口状态、增强 STP 功能。通过本节的学习，读者可以判断网络中是否出现环路，并能配置 STP 来阻止二层交换网络中的环路。

9.3.1 冗余拓扑中存在的问题

如图 9-3-1 所示，PC1 和 PC3 之间可以通过 SW1 的 Fa1/1 和 SW2 的 Fa1/2 之间的链路连通，可是如果 SW1 和 SW2 之间的这条链路中断，将会导致 PC1 和 PC3 之间的通信中断。为了解决单一链路故障引起的网络问题，可以考虑在 SW1 和 SW2 之间再新增一条链路，如图 9-3-2 所示。

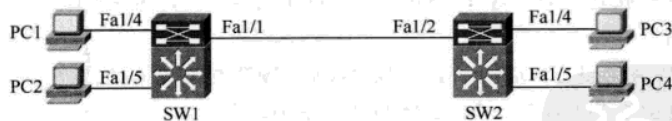


图 9-3-1 单一链路的拓扑

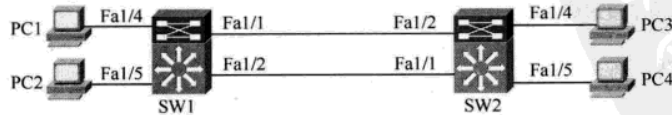


图 9-3-2 有冗余链路的拓扑

SW1 和 SW2 之间，任何一条链路的失败，将不会导致 PC1 和 PC3 之间的通信故障。冗余链

路很好地解决了 SW1 和 SW2 之间单链路故障引起的网络中断,但在执行冗余拓扑前,有些问题必须考虑。

1. 广播风暴

第二层的以太网帧不像路由器传送的第三层数据包有 TTL (Time To Live, 生命周期),如果有环路存在,第二层的以太网帧不能被适当终止,它们将在交换机和交换机之间永无止境地传递下去,造成网络拥塞甚至是瘫痪直到环路被人为破坏。

前面介绍过交换机的工作原理,交换机收到一个广播帧,为了确保在同一个广播域中的所有设备都能收到这个广播帧,它将向除接收端口以外的所有端口转发这个广播帧,如果有超过一个以上的端口转发这个帧,将造成无止境的环路。

下面分析一个广播风暴是如何形成的,具体过程如下。

STEP ① PC1 发出一个广播帧。

STEP ② SW1 收到这个广播帧,SW1 从 Fa1/1、Fa1/2、Fa1/5 端口向外转发这个广播帧。

STEP ③ SW2 从 Fa1/2 端口收到 SW1 从 Fa1/1 端口发过来的广播帧,然后 SW2 从 Fa1/1、Fa1/4、Fa1/5 端口把广播帧转发出去;SW2 从 Fa1/1 端口收到 SW1 从 Fa1/2 端口发过来的广播帧,然后 SW2 从 Fa1/2、Fa1/4、Fa1/5 端口把广播帧转发出去。

STEP ④ 同理 SW1 也从 Fa1/1 和 Fa1/2 端口接收到 SW2 转发过来的广播帧,然后从除接收端口之外的所有端口转发出去。

STEP ⑤ PC1、PC2、PC3、PC4 不停地接收到广播帧,根据广播帧的内容丢弃或处理广播帧。

STEP ⑥ 一个广播帧,在 SW1 和 SW2 间不停地被转发,永无止境,最终造成网络拥塞或瘫痪,影响网络正常使用。

2. MAC 地址表不稳定

广播风暴危害巨大,除了产生大量的流量之外,还造成交换机的 MAC 地址表不稳定,在广播风暴的形成过程中,具体过程如下。

STEP ① SW1 从 Fa1/4 接收到 PC1 的广播帧,SW1 根据帧的源 MAC 地址进行学习,记录下 PC1 的 MAC 在端口 Fa1/4。SW1 把广播帧转发给 SW2。

STEP ② 假设 SW2 从 Fa1/1 口先收到广播帧,SW2 记录下 PC1 的 MAC 在端口 Fa1/1,然后 SW2 从 Fa1/2 口也收到这个广播帧,SW2 更新 PC1 的 MAC 在端口 Fa1/2。SW2 把接收到的广播帧再转发到 SW1。

STEP ③ SW1 先后从 Fa1/2 和 Fa1/1 端口接收 SW2 转发过来的广播帧,依次更新 PC1 的 MAC 地址在端口 Fa1/2 和 Fa1/1。可真正的 PC1 在 Fa1/4 端口。

STEP ④ SW1 和 SW2 随着广播帧不停地被转发从而不停地更换 MAC 地址表,造成 CPU 使用率过高,影响交换机的性能。

3. 重复帧复制

冗余拓扑除了带来广播风暴和 MAC 地址表不稳定外,还会引起重复帧复制问题,具体过程如下。

STEP ① 假使 PC1 发出一个单播帧,目标是 PC3,SW1 收到这个单播帧,可 SW1 在 MAC 地址表中没有找到目标 PC3 的 MAC,SW1 从除接收端口以外的所有端口把这个单播帧转发出去。

STEP 2 SW2 从 Fa1/1 口收到 SW1 转发过来的单播帧,SW2 知道 PC3 接在 Fa1/4 端口,SW2 把这个单播帧只从 Fa1/4 端口转发给 PC3,PC3 接收到这个单播帧。

STEP 3 SW2 从 Fa1/2 口收到 SW1 转发过来的单播帧,SW2 知道 PC3 接在 Fa1/4 端口,SW2 把这个单播帧从 Fa1/4 端口转发给 PC3,PC3 再次接收到这个单播帧。

PC1 仅发送一次单播帧,PC3 却收到两次。在工程中,重复帧复制也存在不足,如在流量统计或计费软件的环境中,都带来计算不精确的问题。

实验 9-3 环路的判断

如何判断网络中出现环路了呢?直接的感觉就是网速变慢;直观的方法就是观察交换机或集线器的指示灯;理性分析应该是抓取数据包。这里用前面介绍过的 Sniffer 软件给大家演示环路判断方法。

STEP 1 构建网络拓扑。可以在计算机的前面加入一台集线器或不支持 STP 功能的交换机。如图 9-3-3 所示,用一根交叉的双绞线把设备的两个端口直接连接起来。

STEP 2 开始捕获包。在计算机上运行 Sniffer,单击“Start”按钮,开始抓包,如图 9-3-4 所示。

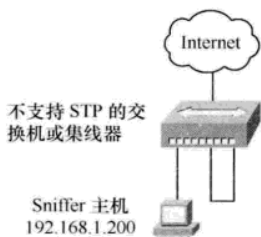


图 9-3-3 有环路的拓扑

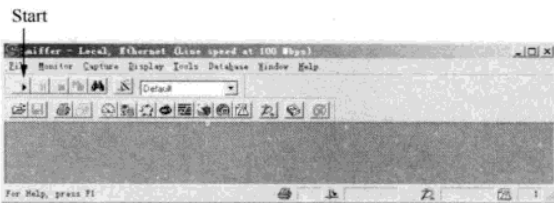


图 9-3-4 开始抓包

STEP 3 制造出一个广播包。实际网络环境中,不需要制造也会有很多广播包,这里在计算机中制造出一个广播包。选择“开始”→“运行”命令,输入“cmd”后按下回车键,打开 DOS 窗口。在 DOS 窗口中执行“arp-d”命令删除本机的 ARP 缓存,然后执行“ping 192.168.1.1”,ping 本机的网关,因本机的 ARP 缓存表中没有网关 IP 对应的 MAC 地址,本机会以广播形式发送 ARP 查询包,如图 9-3-5 所示。一个应答也没有收到,原因是因为网络已经产生了广播风暴。

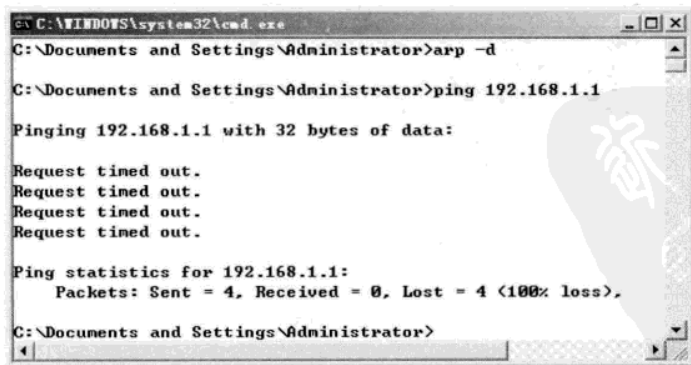


图 9-3-5 计算机发送 ARP 查询广播包

STEP 4 停止捕获包。此时图 9-3-4 所示窗口中的“Stop and Display”按钮变得可操作，单击该按钮，停止捕获，如图 9-3-6 所示。

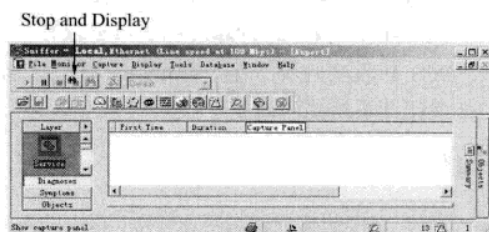


图 9-3-6 停止捕获包

STEP 5 显示捕获的包。停止捕获包后，显示图 9-3-7 所示的窗口，单击窗口中的“Decode”选项卡。

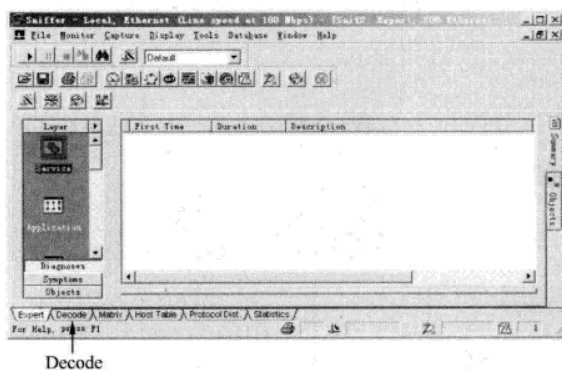


图 9-3-7 选择解码选项卡

STEP 6 分析捕获的包。在打开的解码窗口中，滚动第一个子窗口中的滚动条，可以显示出捕获的包，如图 9-3-8 所示。可以发现其中有大量的 ARP 广播包，源地址来自同一个 MAC。在第二个子窗口中可以发现，这是一个“ARP request”包，要解析的 IP 地址是“192.168.1.1”。

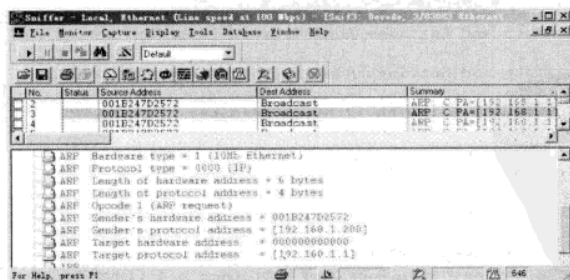


图 9-3-8 解码窗口

STEP 7 解决环路。找到并断开网络中的二层冗余路径，或者启用 STP 协议。

实际中网卡或其他网络接口损坏、环路、人为干扰破坏、黑客工具、病毒传播，都可能引起广播风暴，交换机会把大量的广播帧转发到每个端口上，这会极大地消耗链路带宽和硬件资源。当出现网络异常时，不妨用 Sniffer 抓包，然后分析捕获数据包的特征，判断有没有出现二层环路。下一节将讨论如何通过 STP 技术来有效地抑制广播风暴，避免网络拥塞。

9.3.2 STP 的工作方式

生成树是一个交换网络中检测和消除冗余链路以防止出现二层循环的一个协议。如果不运行 STP，帧有可能会在网络中循环发送，流量急剧升高，最后使整个网络彻底瘫痪。STP 的工作就是将某些端口置于阻塞状态，来防止冗余结构的网络拓扑中产生环路。STP 的工作分为以下 4 个步骤：每个 LAN 只能有一个根交换机；每个非根交换机有且只能有一个根端口；每个网段有且只能有一个指派端口；既不是根端口，也不是指派端口的端口将被阻塞。

1. 选举根交换机

交换机之间通过发送 BPDU (Bridge Protocol Data Unit, 桥协议数据单元) 来选举根交换机，BPDU 中的字段如图 9-3-9 所示。刚开始每个交换机都认为是根桥，向外发送自己的 BPDU，其中的 Root ID 字段填入自己的 Bridge ID。交换机接收其他交换机发过来的 BPDU，如果其中的 Root ID 比自己的 BID 更小，则交换机停止发送自己的 BPDU，转发根交换机的 BPDU。

交换机的 BID=优先级+交换机的 MAC 地址，如图 9-3-10 所示，共 8 字节，其中优先级 2 字节，MAC 地址 6 字节。在最初的 802.1D 标准中，BID 由优先级域和交换机的 MAC 地址组成，一个交换机上的所有 VLAN 对外表现为一个生成树实例，交换机的优先级可以是 0~65 535；因 PVST (Per Vlan Spanning Tree, 每个 VLAN 一个生成树) 要求每个 VLAN 有一个单独的生成树，BID 被要求包含 VLAN ID 信息，解决的办法是从优先级域的 16 个 bit 中拿出低位的 12 个 bit，称为扩展的 System ID，用来唯一标识每个 VLAN 号，剩下的 4 个 bit 用来表示 VLAN 的生成树优先级，这种情况下优先级的取值只有 $2^4=16$ 个，是 4096 的倍数。那么为何从优先级中拿出的是 12 个 bit 来表示 Extend System ID 呢？原因是 ISL 封装中只有 10 个 bit 用于 VLAN 标识，802.1Q 封装中有 12 个 bit 用于 VLAN 标识，不管是哪种封装，取 12 个 bit 都可以满足。

Bytes	Field
2	Protocol ID
1	Version
1	Message type
1	Flags
8	Root ID
4	Cost of path
8	Bridge ID
2	Port ID
2	Message age
2	Max age
2	Hello time
2	Forward delay

图 9-3-9 交换机的 BPDU

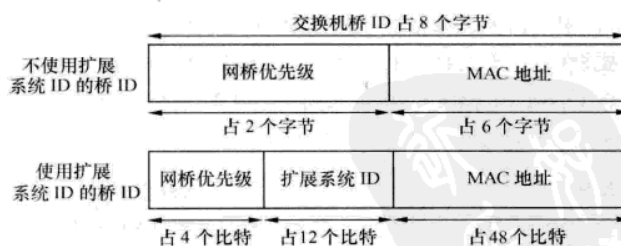


图 9-3-10 交换机的 BID

打开 Network 机架中的 SW1 和 SW2，它们的连接如图 9-3-11 所示。SW1 的 MAC 地址是 cc00.09e0.0000，SW2 的 MAC 地址是 cc01.09e0.0000，优先级都是默认的 32 768。

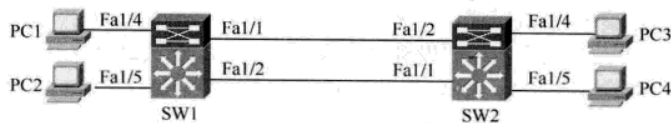


图 9-3-11 交换机连接图

如图 9-3-11 所示的交换机是由 Cisco 3640 的路由器添加了交换模块而来，和实际中的交换机还是有些差异，很多功能不被支持。例如，不支持很多高级的 QOS 特性，也不支持生成树的类型的选择。两台交换机都没使用扩展的 System ID，交换机 SW1 的 BID 是 32768+ cc00.09e0.0000，交换机 SW2 的 BID 是 32768+ cc01.09e0.0000，可以看出交换机 SW1 的 BID 小，SW1 是根交换机。在 SW2 上执行 show spanning-tree brief，结果如图 9-3-12 所示。

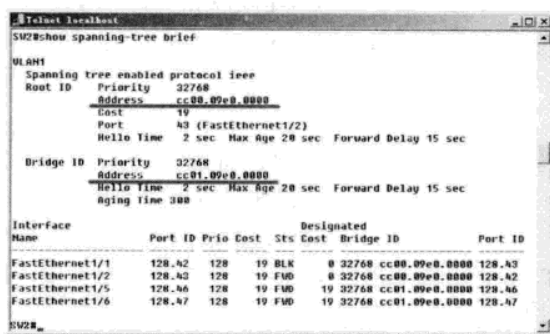


图 9-3-12 查看生成树

如图 9-3-12 所示，可以看出针对 VLAN 1（默认情况下交换机上只有 VLAN 1），网络中的根交换机是 SW1。可以在交换机 SW2 上使用下面的命令更改 SW2 的优先级：

SW2 (config) #spanning-tree vlan 1 priority 100

上面的命令把交换机 SW2 的优先级从 32768 降到 100，这时 SW2 的 BID 变小，SW2 成为 VLAN 1 的根交换机，可使用如图 9-3-12 所示的命令进行验证。

2. 选举根端口

每个非根交换机有且仅有一个根端口。非根交换机可能会从多个端口接收到根交换机的 BPDU，根端口的选举依照下面的原则，具体过程如下。

STEP 1 最低 COST 的端口成为根端口。如图 9-3-9 所示，可以看到 BPDU 中有一个字段路径花费（Cost of path），从根收到的 BPDU 中会包含路径花费。花费低的端口成为根端口。花费根据带宽而来，带宽和对应的 Cost 值请参照表 9-3-1。

表 9-3-1 Cost 参考值

速 度	Cost（修订后的 IEEE 规范）	Cost（早先的 IEEE 规范）
10 Gbit/s	2	1
1 Gbit/s	4	1
100 Mbit/s	19	10
10 Mbit/s	100	100

在图 9-3-13 中, SW1 是根交换机, 分析一下 SW2 和 SW3 的根端口是哪一个? 使用修订后的标准, SW2 的端口 1 接收到 BPDU 的路径花费是 100, 端口 2 接收到 BPDU 的路径花费是 38 (19+19), SW2 的根端口是端口 2。同理 SW3 的根端口是端口 1。

STEP 2 Cost 相同的情况下, 比较发送者的 BID。如图 9-3-14 所示, 交换机 SW4 从端口 1 和端口 2 都能收到根交换机的 BPDU, 两边的 Cost 相同, 都是 38, 接下来比较的就是发送者的 BID。假设 SW2 的 BID 是 32768+aaaa.aaaa.aaaa, SW3 的 BID 是 32768+bbbb.bbbb.bbbb, SW2 的 BID 小, 则 SW4 的端口 1 成为根端口。

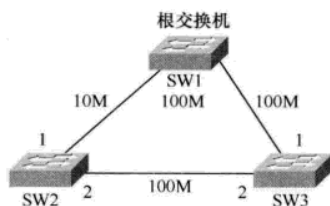


图 9-3-13 比较花费

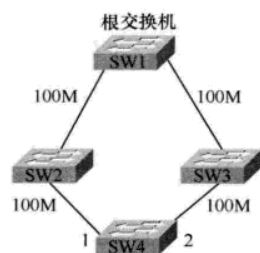


图 9-3-14 比较发送者的 BID

STEP 3 发送者 BID 相同的情况下, 比较发送者的 Port ID。如图 9-3-11 所示, SW1 是根交换机, SW2 的 Fa1/1 和 Fa1/2 到根交换机的花费相同, 发送者的 BID 也相同 (都是交换机 SW1 的 BID)。接下来比的是发送者的 Port ID, 在图 9-3-12 中可以看到 SW2 交换机 Fa1/1 口接收到的发送者 Port ID 是 128.43, Fa1/2 口接收到的发送者 Port ID 是 128.42。从图 9-3-12 中也可以看出 SW2 的根端口是 Fa1/2 口。

STEP 4 发送者的 Port ID 相同的情况下, 比较接收者的 Port ID。如图 9-3-15 所示, 交换机 SW1 的 Fa1/1 口连接着 SW2 的 Fa1/1 和 Fa1/2 口, 这样的拓扑往往是中间接了一台集线器。因前面都一样, 这里将比较接收者的 Port ID, Port ID=端口优先级+Port 号, 端口优先级默认都是 128, Fa1/1 的 Port 号小于 Fa1/2 的 Port 号, 所以 SW2 的 Fa1/1 口是根端口。

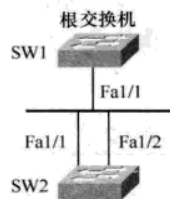


图 9-3-15 比较接收者的 PID

3. 选举指派端口

每个网段都有一个指派交换机, 该交换机负责把那个网段的数据发往根交换机。指派交换机上的端口叫指派端口。选指派端口的过程其实是先选指派交换机, 如果指派交换机上有多个端口, 再从多个端口中选出一个指派端口。

如果一个网段有多个交换机连接到根交换机, 首先比较哪个交换机到根交换机的 Cost 最小, 如果 Cost 相同, 则比较每台交换机的 BID, BID 最小的交换机成为指派交换机。指派交换机的上端口是指派端口, 如果指派交换机上有多个端口, 具有最小 Port ID 的端口成为指派端口。

4. 阻塞端口

既不是根端口也不是指派端口的端口将被阻塞。图 9-3-11 所示 SW2 的 Fa1/1 端口、图

9-3-13 所示 SW2 的 1 端口、图 9-3-14 所示 SW4 的 2 端口、图 9-3-15 所示 SW2 的 Fa1/2 端口都将被阻塞。

9.3.3 生成树的端口状态

Spanning-tree 使交换机端口在 4 个不同的状态间转换，注意端口的关闭还是打开不受 STP 的控制。如图 9-3-16 所示描述了一个端口转换到转发状态要经历的过程。

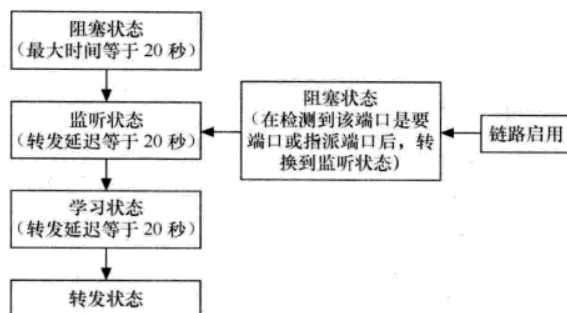


图 9-3-16 生成树的端口状态转换

Down（禁用）、Blocking（阻塞）、Listening（监听）、Learning（学习）、Forwarding（转发）这 5 种端口状态有什么区别呢？表 9-3-2 对各种状态的功能进行了对比，有助于记忆，端口状态每前进一步，功能就增强一步。表 9-3-2 中第一列表示端口的状态，第一行表示端口的功能，行列的交集处表示处在该状态的端口是否支持该功能。“×”表示不支持该功能，“√”表示支持该功能。

表 9-3-2 STP 端口功能表

	接收 BPDU	发送 BPDU	学习 MAC	转发 DATA
Down	×	×	×	×
Blocking	√	×	×	×
Listening	√	√	×	×
Learning	√	√	√	×
Forwarding	√	√	√	√

9.3.4 增强 STP 功能

从前面的介绍中可以发现，启用 STP 功能的交换机，一个端口从 UP 到 Forwarding 大约需要 50s 的时间，而普通的二层非网管型交换机，端口从 UP 到 Forwarding 瞬间就可以完成。那么为什么便宜的交换机反而快，贵的交换机价值体现在哪里呢？启用生成树的交换机，也可以使连接计算机的端口从 UP 到 Forwarding 瞬间就可以完成，做法就是把交换机上连接计算机的端口设成快速端口，实现的命令如下：

```
SW1 (config) #interface range fa1/1 - 10 一次修改多个端口
```

```
SW1 (config-if-range) #spanning-tree portfast 把交换机端口设成快速端口
```

上面的命令把交换机的 Fa1/1 到 Fa1/10, 共 10 个端口都设成快速端口。设置时, 交换机控制台会提示, 仅在连接计算机的端口上使用该功能, 不要在连接集线器、交换机、网桥的端口上使用该功能, 可能会导致临时性的生成树环路。还会提示在 TRUNK 端口使用该功能是无效的。

STP 还有新的功能, 如快速生成树 (RSTP)、多生成树 (MSTP)、增强的每个 VLAN 一个生成树 (PVST+)、每个 VLAN 一个快速生成树 (PVRST) 等。限于篇幅, 本书只介绍简单的生成树。

例如, 某单位的网络拓扑如图 9-3-17 所示, 在核心和汇聚层配置了两台思科 6509 的交换机, 两台交换机间使用千兆链路互连; 接入层配置的是 2950 交换机, 为了避免单链路故障, 接入层使用两条百兆链路分别上连到两台 6509 交换机的 Fa2/1 端口; 两台服务器均千兆和思科 6509 交换机相连。公司员工反映网速很慢。经测试, 发现两台服务器间的流量始终超过不了 100Mbit/s。初步分析, 可能是生成树的问题, 在两台 6509 交换机上使用 “show spanning-tree brief” 命令查看, 发现所有交换机的优先级都是默认的 32768, 但 2950 生成的日期较早, 有最小的 MAC 地址, 交换机 2950 是根交换机。右边 6509 的 Gi1/1 端口既不是根端口, 也不是指派端口, 被阻塞。至此, 原因找到了, 由于 2950 是根交换机, 两台 6509 间的千兆链路被阻塞, Server1 到 Server2 的流量全部经 2950 中转, 百兆链路是瓶颈, 这台 2950 交换机成了单位的核心交换机。

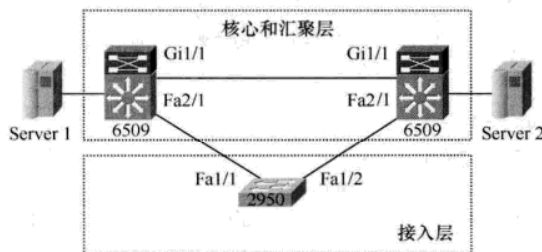


图 9-3-17 失败的 STP 配置

利用本章学到的知识, 把两台 6509 交换机分别配置成根交换机 (优先级改成 4096) 和备份的根交换机 (优先级改成 8192), 问题就可以解决。

9.4 链路聚合的实现

链路聚合使用的是 EtherChannel 特性, 在交换机到交换机、交换机到路由器之间提供冗余的、高速的连接方式, 简单说就是将两个设备间多条 FastEthernet 或 GigabitEthernet 物理链路捆在一起组成一条设备间逻辑链路, 从而达到增加带宽, 提供冗余的目的。如图 9-4-1 所示, 两台交换机到计算机的链路都是 100M, SW1 和 SW2 之间虽有两条 100M 的物理链路相连, 可由于生成树的原因, 只有 100M 链路可用, 交换机之间的链路很容易形成瓶颈。使用链路聚合技术, 把两个 100M 链路聚合成一个 200M 的逻辑链路, 当一条 100M 链路出现故障, 另一条 100M 链路会继续工作。下面介绍链路聚合对端口的要求和链路聚合的配置。

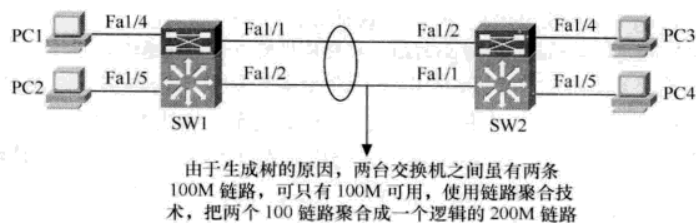


图 9-4-1 链路聚合

9.4.1 聚合端口的要求

构成 EtherChannel 的端口必须配置成相同的特性，如双工模式、速度、同为 FE 或 GE 端口、Trunk 端口的 native VLAN、Trunk 端口的允许的 VLAN range、Trunking 的状态和类型等都要一致。当 EtherChannel 中某一条链路故障时，不会影响 EtherChannel 中其他链路的正常工作。

9.4.2 配置链路聚合

当配置二层端口作 EtherChannel 时只要在成员端口配置模式下用 `channel-group n` 命令指定该端口要加入的 channel-group 组，这时 switch 会自动创建 port-channel 接口。

打开 dynamips 中的 Network 机架，运行 SW1 和 SW2 交换机，SW1 和 SW2 的配置类似，下面是 SW2 的具体配置：

```
SW2 (config) #int range fa 1/1 - 2
SW2 (config-if-range) #switchport mode trunk
SW2 (config-if-range) #channel-group 1 mode on
```

以上配置将交换机的 Fa1/1、Fa1/2 端口加入 channel-group 1，EtherChannel 的端口可为 access 端口，也可为 trunk 端口。配置完成后在 SW2 上执行命令 `show etherchannel 1 summary`，可以发现 Po1 口是一个二层端口（从图中的 Po1(SU)得出的结论，S 表示 layer2，U 表示 in use），并且正在使用，包含 Fa1/1 和 Fa1/2 两个物理端口，如图 9-4-2 所示。在交换机上执行命令 `show spanning-tree brief`，如图 9-4-2 所示，和图 9-3-12 所示相对比，可以发现看不到：

FastEthernet1/1	128.42	128	19 FWD	0 32768 cc01.0210.0000 128.42
FastEthernet1/2	128.43	128	19 BKN	0 32768 cc01.0210.0000 128.43

取而代之的是：

Port-channel1	129.65	128	12 FWD	0 32768 cc00.0210.0000 129.65
---------------	--------	-----	--------	-------------------------------

现在的逻辑端口是转发状态，没有被阻塞的端口，端口花费从 19 降到 12，是因为聚合端口的带宽是 200M，可以使用命令 `show interfaces port-channel 1` 命令查看端口带宽。

在交换机上使用 `show interfaces trunk`，可以看出 Po1 端口也处在 Trunk 模式。二层的聚合端口可以 Access，也可是 Trunk。有些交换机还支持三层端口，但模拟器上不支持三层的聚合端口。

```
SW2#show interfaces trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Po1	on	802.1q	trunking	1

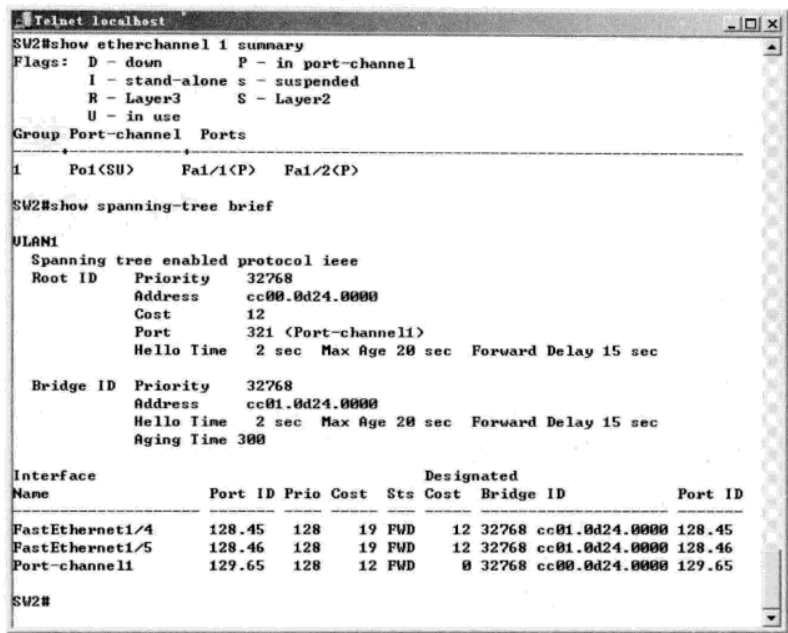


图 9-4-2 配置以太网通道

EtherChannel 在做数据转发时，是基于数据包的源或目的 MAC 地址随机选择 Ether Channel 中的一条物理 link 进行数据转发的。用户可以通过全局配置命令 `port-channel load-balance` 选择是根据什么信息进行数据转发来实现负载平衡，如图 9-4-3 所示。

例如，当有两台交换机，它们之间有几条链路组合在一起作 EtherChannel，交换机 A 一端连接一台服务器，交换机 B 一端连接多台客户计算机，这时交换机 A 一端的数据流是同一源 MAC 地址的数据包通过 EtherChannel 转发向不同目的 MAC 地址。这时，为了充分利用 EtherChannel 中的所有的物理线路，在交换机 A 一端就应该配置为基于数据包的目的 MAC 地址方式，而交换机 B 一端的数据流是不同源 MAC 地址的数据包通过 EtherChannel 转发向同一个目的 MAC 地址。在交换机 B 一端就应该配置为基于数据包的源 MAC 地址方式。

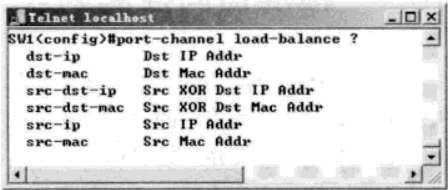


图 9-4-3 以太网通道的负载均衡



第 10 章 访问控制列表

Chapter 10

在路由器上，可通过使用 ACL（Access Control List，访问控制列表）来执行数据包过滤。访问控制列表可用来控制网络上数据包的传递，限制虚拟终端线路的通信量或者控制路由选择更新。本章内容包括标准、扩展、命名、自反、动态、基于时间、基于上下文的访问控制列表，通过本章学习，读者可以根据需求选择正确的访问控制列表，以便在工程中使用访问控制列表限制网络通信量，限制用户访问特定的网络和设备。

10.1 标准访问控制列表

IP 访问控制列表是应用于 IP 地址的允许或禁止规则的集合。对于每个数据包，路由器顺序执行某个访问控制列表中的语句。如果路由器到达了访问控制列表的底端而没有找到与该数据包相匹配的语句，则丢弃该数据包（该方式称做隐式的 deny any）。因此，每个访问控制列表都必须包含至少一个允许的语句，否则就没有任何意义。而且由于第一个匹配的语句将先执行，所以列表顺序是十分重要的。

对于每个访问控制列表，可以输入规则来允许或者禁止数据包，访问控制列表用号码来标识。对一个表的所有语句必须使用相同的号码或名字。使用的号码必须在如图 10-1-1 所示的范围内。本书仅介绍针对 IP 的访问控制列表。

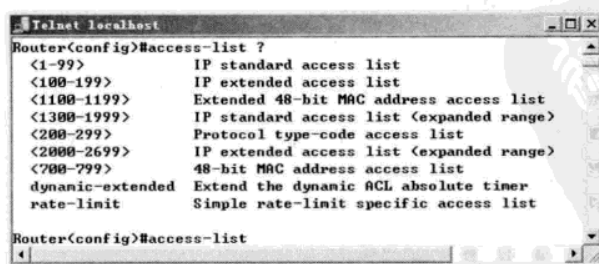


图 10-1-1 访问控制列表的号码范围

10.1.1 通配符掩码

开始配置访问控制列表之前，必须了解通配符掩码的作用和写法。路由器使用通配符掩码与源或目标地址一起来分辨匹配的地址范围。如同子网掩码告知路由器 IP 地址的哪一位属于网络号一样，通配符掩码告知路由器为了判断是否匹配，它需要检查 IP 地址中的多少位。这个地址掩码对可以只使用两个 32 位的号码来确定 IP 地址的范围。这是十分方便的，因为如果没有通配符掩码的话，需要对每个匹配的 IP 地址加入一个单独的访问控制列表语句，这将造成很多额外的输入和路由器大量额外的处理过程，所以地址掩码相当有用。

在子网掩码中，将掩码的一位设成 1 表示 IP 地址对应的位属于网络地址部分。相反，在访问控制列表中，将通配符掩码中的一位设成 1 表示 IP 地址中对应的位既可以是 1 又可以是 0。有时，可将其称作“不检查”位，因为路由器在判断是否匹配时并不关心它们。通配符掩码位设成 0 则表示 IP 地址中相对应的位必须精确匹配。下面举例说明一些在访问控制列表中可能出现地址掩码对是如何工作的。

192.168.1.0 0.0.0.255

通配符掩码是 0.0.0.255，前面是 24 个 0，最后是 8 个 1。通配符掩码中 0 表示必须精确匹配，也就是说要精确匹配前面的 24 位。通配符掩码中 1 表示忽略位，也就是最后的 8 位是 0 或 1 都没有关系。通配符掩码与前面的 IP 地址 192.168.1.0 结合在一起，实现的就是匹配从 192.168.1.0 到 192.168.1.255 的所有 IP 地址。

192.168.0.0 0.0.255.255

分析同上，实现的是匹配从 192.168.0.0 到 192.168.255.255 的所有 IP 地址。

192.168.16.0 0.0.7.255

并不是所有的通配符掩码的“精确匹配”位和“不检查”位都刚好是 8 的倍数。有时，计算是否匹配是十分困难的事。如将上例中第 3 个数进行二进制分解。

地址位：16 = 00010000

掩码位：7 = 00000111

可以看出，如果不管通配符掩码中为 1 的相对应的地址位，这对数字描述了 8 种可能的数字范围，从 16~23。如下所示，可以用二进制从 16~24 来验证它。

= 00010000

= 00010001

= 00010010

= 00010011

= 00010100

= 00010101

= 00010110

= 00010111

= 00011000

注意，当数到 24 时，地址上的第 21 位从 0 变成了 1。第 21 位不再符合通配符掩码，所以它不再属于这对描述的范围。整个的地址掩码对实现的是匹配从 192.168.16.0 到 192.168.23.255 的所有 IP 地址。

对于访问控制列表，判断是否匹配的过程实际分为 3 个步骤。在数据包过滤中，为进行匹配，

路由器检查 IP 数据包报头中的 IP 地址。假设访问控制列表语句中包含地址掩码对 192.168.0.0 0.0.0.255, 一个数据包中包含源 IP 地址 192.168.0.2, 路由器将如下操作。

STEP 1 用访问控制列表语句中的通配符掩码和地址执行逻辑或 (192.168.0.0 和 0.0.0.255 执行逻辑或), 该操作的结果为 192.168.0.255。

STEP 2 用访问控制列表语句中的通配符掩码和数据包报头中的 IP 地址执行逻辑或 (192.168.0.2 和 0.0.0.255 执行逻辑或), 结果是 192.168.0.255。

STEP 3 将两个结果相减。如果两个结果相等, 相减的结果精确为零, 则匹配; 如果相减的结果不为零, 则不匹配, 对下条语句重复执行上述 3 个步骤。

在 IP 访问控制列表地址掩码对中, 有两个关键字可用来省略一些输入。第一个是 “any”, 它可用来代替地址掩码对 0.0.0.0 255.255.255.255。可以看出, 该地址掩码对匹配任何的 IP 地址。

另一个是 “host”, 它只用于扩展访问控制列表中, 用来代替通配符掩码 0.0.0.0。在标准访问控制列表中, 当掩码是 0.0.0.0 时省略它, 如果省略了掩码, 则表示该掩码是 0.0.0.0。

10.1.2 配置标准访问控制列表

访问控制列表是在全局配置模式下输入的。增加标准访问控制列表的基本格式如下:

```
Access-list access-list-number {Deny | Permit} {Source [Source-wildcard] | Any}
```

参数 access-list-number 是 1~99 之间的整数, 然后规定条目是否允许或禁止从特定地址来的通信量。参数 Source 指明了访问控制列表规则应用的源 IP 地址。如果想增加子网地址, 则可以把源地址从特定的主机变成一个 IP 地址范围。参数 Source-wildcard 基本指明了地址字段中哪些位是匹配的。如果在末尾加上参数 any, 则表示地址 0.0.0.0 和通配符掩码 255.255.255.255, 这时所有的地址都是匹配的。开启 CCNP 机架中 R1、R2、R3 三台路由器, 它们的 IP 地址分配如图 10-1-2 所示。



图 10-1-2 标准访问控制列表

首先配置静态路由, 保证全网的连通性。其中 R1 的配置如下:

```
Router>en
Router#conf t
Router(config)#host R1
R1(config)#int s1/1
R1(config-if)#ip add 12.1.1.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#ip route 0.0.0.0 0.0.0.0 12.1.1.2
```

R2 的配置如下:

```
Router>en
Router#conf t
Router(config)#host R2
R2(config)#int s1/0
R2(config-if)#ip add 12.1.1.2 255.255.255.0
R2(config-if)#no shut
```

```
R2(config-if)#int s1/1
R2(config-if)#ip add 23.1.1.2 255.255.255.0
R2(config-if)#no shut
```

R3 的配置如下：

```
Router>en
Router#conf t
Router(config)#host R3
R3(config)#int s1/0
R3(config-if)#ip add 23.1.1.3 255.255.255.0
R3(config-if)#no shut
R3(config-if)#ip route 0.0.0.0 0.0.0.0 23.1.1.2
```

静态路由配置完成后，R1 可以 ping 通 R3 的 S1/0 端口的 IP 地址 23.1.1.3，R2 也可以 ping 通 R3 的 S1/0 端口的 IP 地址 23.1.1.3。要求配置访问控制列表，不允许 R1 访问 R3。配置访问控制列表分以下两个步骤。

STEP 1 创建列表。在路由器 R3 上创建访问控制列表，配置如下：

```
R3 (config) #access-list 1 deny 12.1.1.1    拒绝 R1 的 IP 地址 12.1.1.1，通配符掩码 0.0.0.0 可以省略
R3 (config) #access-list 1 permit any      允许所有的 IP 地址，这一行不能省略，因为访问控制列表最后隐含了一条 deny any 的规则，如果没有这一行，所有的 IP 地址都将被拒绝。
```

上面两行的顺序很重要，因为匹配的顺序是从上至下，当条件匹配即执行操作。如果把两行的顺序调换一下，当 IP 地址 12.1.1.1 试图通过时，12.1.1.1 是 any 中的一个地址，执行的操作是允许，永远不会执行第二条，所有的 IP 地址都被允许，这与要求不符。

STEP 2 应用列表。创建好列表以后，接下来还必须将它应用到每个想用它的接口。因只想拒绝 R1 访问 R3，其他的访问不受影响，可以把列表用在 R3 的 S1/0，当数据包进入 R3 的时候进行判断，配置如下：

```
R3 (config) #int s1/0
R3 (config-if) #ip access-group 1 in    在接口下调用访问控制列表 1，针对的是从 S1/0 端口进入路由器 R3 的流量。
```

两个步骤的操作顺序没有关系，但两者缺一不可，创建列表没有在接口下调用，或者在接口下调用一个没有被创建的列表，都不会起作用。配置完成后，在 R1 上 ping 23.1.1.3，ping 不通；在 R1 上 ping 12.1.1.2，可以 ping 通；在 R2 上 ping 23.1.1.3，也可以 ping 通。

10.2 扩展访问控制列表

标准访问控制列表只能使用源寻址作为过滤条件，提供了十分基本的过滤功能。扩展访问控制列表同时使用源地址和目标地址作为过滤条件，甚至允许使用协议类型、端口号、时间范围来过滤。扩展访问控制列表功能更强，可以更加精细地控制通信量。

10.2.1 配置扩展访问控制列表

在访问控制列表中匹配数据包时，扩展 IP 访问控制列表同时使用源地址和目标地址；还可以

有选择地使用协议类型信息来优化控制, 如 TCP、UDP 及它们的端口号; 还可以设置时间参数, 如实现上班时间不可以上网, 下班时间可以上网。许多在标准访问控制列表中使用的规则同样适用于扩展访问控制列表, 如访问控制列表本身不起任何作用, 必须将其应用于某个接口; 在访问控制列表的结尾, 默认情况下隐式地拒绝所有语句。

增加条目的基本格式如下:

Access-list access-list-number {Deny | Permit} Protocol Source Source-wildcard Destination Destination - wildcard

首先输入的是 Access-list 命令, 然后是访问控制列表的号码, 号码的范围是 100~199, 紧跟的参数是说明允许或者拒绝特定的通信量。然后需要指明将使用协议, 如 TCP、UDP、ICMP 或者 IP。用户可以告诉路由器明确的源地址和目标地址, 也可以使用 any。这里列举一个使用扩展访问控制列表的例子。

如图 10-1-2 所示, 拒绝 R1 去往 R3 的 Telnet 通信, 但允许其他的服。在标准访问控制列表中, 如果拒绝某个 IP 地址, 就是拒绝该 IP 主机的所有服务; 如果允许某个 IP 地址, 就是允许该 IP 主机的所有服务。如果只是拒绝 R1 去往 R3 的 Telnet 流量, 这时就需要使用扩展访问控制列表, 配置扩展访问控制列表也分为两个步骤。

STEP 1 创建列表。在路由器 R2 上创建访问控制列表, 配置如下:

R2 (config) #access-list 100 deny tcp host 12.1.1.1 host 23.1.1.3 eq Telnet 因只拒绝 Telnet 流量, Telnet 流量使用的是 TCP, 目标端口是 23, 所以这里拒绝的协议是 TCP, 源地址是 R1, 目标地址是 R3; 端口是 23 (配置语句中的 Telnet 表示 23)

R2 (config) #access-list 100 permit ip any any 隐含的是拒绝所有, 这一行的作用是允许其他所有的 IP 流量通过

上面两行的顺序同样很重要, 不能颠倒。

STEP 2 应用列表。创建好列表以后, 接下来还必须将它应用到每个想用它的接口。因只想拒绝 R1 访问 R3 的 Telnet 流量, 其他的访问不受影响, 可以把列表用在 R2 的 S1/0 端口, 当数据包进入 R2 的时候进行判断, 配置如下:

R2 (config) #int s1/0

R2 (config-if) #ip access-group 100 in 在接口下调用访问控制列表 100, 针对的是从 S1/0 端口进入路由器 R2 的流量。

两个步骤的操作顺序没有关系, 但两个步骤缺一不可, 创建列表没有在接口下调用, 或者在接口下调用一个没有被创建的列表, 都不会起作用。配置完成后, 在 R1 上 ping 23.1.1.3, 可以 ping 通; 在 R1 上 Telnet 23.1.1.3, 提示目标不可达, 如图 10-2-1 所示。

在 R2 上 ping 23.1.1.3, 可以 ping 通; 在 R2 上 Telnet 23.1.1.3, 可以连接, 但提示虚拟终端密码没有设置, 不允许远程登录, 如图 10-2-2 所示。

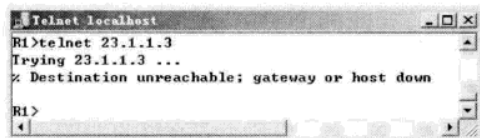


图 10-2-1 目标不可达

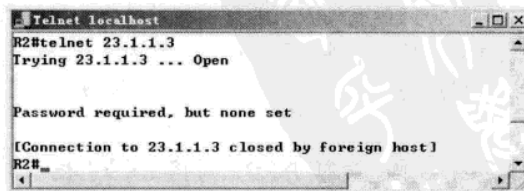


图 10-2-2 目标不允许登录

如需开通 R3 的远程登录和管理，则需在 R3 上进行如下配置：

```
R3(config)#line vty 0 4    配置虚拟终端接口
R3(config-line)#login      要求登录。如输入 no login，表示虚拟终端不需要登录，可以直接进入。出于安全考虑，一般工程中都要求登录。
R3(config-line)#pass cisco 虚拟终端的密码是 cisco
R3(config-line)#exit
R3(config)#enable pass cisco 使能密码是 cisco
```

有可能实验不成功，因为该实验是在静态路由配置成功的基础上完成的，首先确保静态路由配置无误。如果是在标准访问控制列表的基础上，继续配置扩展访问控制列表，需删除标准访问控制列表。在 R3 上取消标准访问控制列表的配置如下：

```
R3(config)#no access-list 1
R3(config)#int s1/0
R3(config-if)#no ip access-group 1 in
```

10.2.2 扩展访问控制列表的增强编辑功能

初期，对 Cisco 的 ACL 进行修改是件令人头疼的事情，因为 Cisco 的 ACL 只能向列表末尾添加语句，而不能在列表中间插入语句。有经验的工程师使用 `show running-config`，查看正在运行的配置文件，从中复制出要修改的访问控制列表，在文本编辑器中修改 ACL，修改完成后，在路由器上删除正在使用的 ACL，再粘贴文本编辑中的 ACL。这样修改起来比直接在路由器上取消列表的所有行，再一条条输入要方便很多，但还是有点不方便，要取消列表再应用。Cisco 在 IOS 12.2T8 及以后的版本中增强了扩展 ACL 的修改功能，用户可以向现存 ACL 的任意部位插入新的语句。如何判断正在使用的 IOS 是否支持扩展访问控制列表的增强编辑功能是比较困难的，这里可以使用一个直观的方法，如在路由器 R2 上执行 `show access-list 100`，有下面的输出：

```
R2#show access-lists
Extended IP access list 100
 10 deny tcp host 12.1.1.1 host 23.1.1.3 eq Telnet (3 matches) 这一条语句被匹配到 3 次，有些不容易看到结果的实验，可以借助访问控制列表中的匹配数来辅助测试。
 20 permit ip any any
```

从输出中，如果可以看到列表中每条语句之前加了行号（10 和 20），那么正在使用的 IOS 就支持扩展 ACL 的增强编辑功能。下面演示如何在路由器 R2 上向列表中间插入新的语句，以及验证插入语句后的 ACL，操作和输出如下：

```
R2(config)#ip access-list extended 100
R2(config-ext-nacl)#15 permit ip host 1.1.1.1 host 2.2.2.2
R2(config-ext-nacl)#do show access-list 100
Extended IP access list 100
 10 deny tcp host 12.1.1.1 host 23.1.1.3 eq Telnet (3 matches)
 15 permit ip host 1.1.1.1 host 2.2.2.2      在中间成功插入了一个新行
 20 permit ip any any
```

从上面的输出可以看到，由于新插入语句的行号为 15，因此它插在了行号为 10 和 20 的两句中间。可以使用 `ip access-list resequence access-list-number start-number increase-number` 命令对访问控制列表的序列号进行重新编号，其中“access-list-number”是列表号，“start-number”是列表的

起始行号, “increase-number” 是每一行的增量。例如:

```
R2(config)#ip access-list resequence 100 30 20
R2(config)#do show access-list 100
Extended IP access list 100
 30 deny tcp host 12.1.1.1 host 23.1.1.3 eq Telnet (3 matches)
 50 permit ip host 1.1.1.1 host 2.2.2.2
 70 permit ip any any
```

命令 “ip access-list resequence 100 30 20” 中, 100 表示扩展访问控制列表的编号, 30 表示起始的行号, 20 表示的是增量, 每一行递增 20, 这样得到新编号的行号是 30, 50, 70。

10.2.3 扩展 ACL 中的 Established

配置使用 TCP 的扩展 ACL 时, 有一个参数 Established (确定的) 特别值得关注, 它可以用来做 TCP 的单向访问控制, 功能效果类似防火墙, 一边可以访问另外一边, 另外一边却不能访问这一边。如在图 10-1-2 所示中, 实现 R1 可以 Telnet R3, 但 R3 不可以 Telnet R1。

在开始正式介绍之前, 先来回顾一下 TCP 建立连接的过程。如图 10-2-3 所示, 192.168.1.200 远程桌面连接 218.94.124.46 主机, 192.168.1.200 发给 218.94.124.46 的第一个数据包中没有 ACK 位, 后续的包中都有 ACK 位, 可以通过 Sniffer 捕获数据包, 如图 10-2-4 所示。

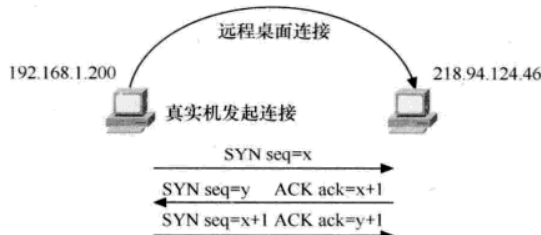


图 10-2-3 TCP 建立连接的过程

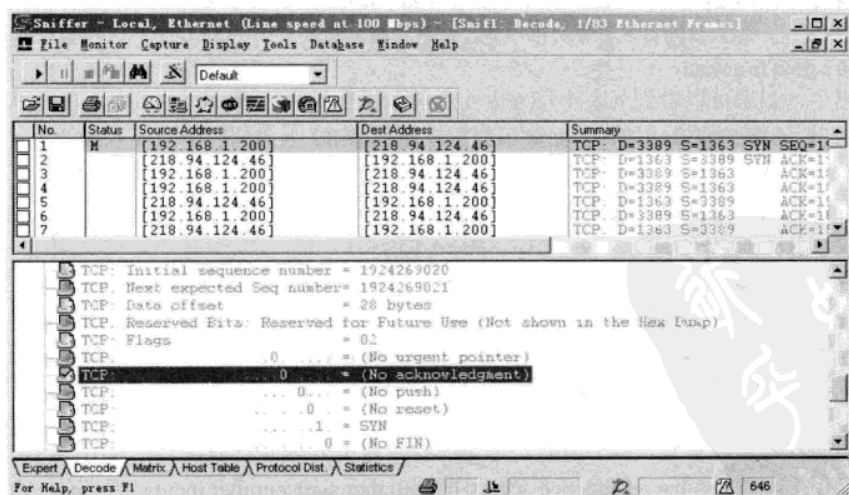


图 10-2-4 捕获 TCP 连接的发起包

通过这点可以很容易判断 TCP 连接的发起者，扩展 ACL 中的 Established 可以根据数据段中是否设置了 ACK 位来对分组进行过滤（没有 ACK 位的不符合 Established 条件）。

实验 10-1 配置基于 TCP 的单向访问

结合图 10-1-2 所示，可以把 R1 想象成内网，R2 想象成边界路由器，R3 想象成外网。当外界有 TCP 流量欲通过 R2 的 S1/1 口访问内网时，R2 上的访问控制列表，判断该数据包中有没有设置 ACK 位（也就是连接是否已建立 Established）。如果有，说明这个包不是第一个发起的包，允许通过；如果没有设置 ACK 位（也就是连接的发起者，连接尚未建立），不满足 Established 条件，丢弃数据包。该实验的步骤如下。

STEP 1 配置静态路由。如 10.1.2 节，配置 R1，R2，R3，保证网络连通性。

STEP 2 配置远程登录。如 10.2.1 节，配置 R1 和 R3 的远程登录，并在 R1 上 Telnet R3，在 R3 上 Telnet R1 进行测试。

STEP 3 配置访问控制列表。在 R2 上如下配置：

```
R2(config)#access-list 100 permit tcp any any established
R2(config)#int s1/1
R2(config-if)#ip access-group 100 in
```

STEP 4 测试。现在 R1 可以正常登录 R3，R3 不能登录 R1。

访问控制列表 100 作为进站列表应用在 R2 的 S1/1 端口上，也就是说从 23.1.1.3 发往 12.1.1.1 的数据包中都必须包含 ACK 位，否则会被拒绝。

注意



Established 只能用于基于 TCP 的应用，例如，Telnet、FTP、HTTP 等。对基于 UDP、ICMP 等协议则不起作用，后面 10.5 节介绍的自反访问控制列表却可以很好地解决这一问题。

10.3 命名访问控制列表

命名访问控制列表使用名字取代列表号，支持标准命名列表和扩展命名列表。在 IOS11.2 以后版本中，可以使用命名访问控制列表。由于这是 11.2 版中新增加的功能，所以它并不向下兼容。通过命名列表，可以标识 IP 访问控制列表，无论是标准型或者扩展型，用名字来代替号码。这可以突破原来在一台路由器上最多只能创建 99 个（因标准列表号从 1~99）标准列表，100 个扩展访问控制列表的限制。另外不管是扩展的命名列表，还是标准的命名列表，都可以很方便地增加或删除一行。

要使用这种访问控制列表，首先需要输入命令将模式转变到输入命名访问控制列表的方式：

```
IP Access-list Standard name or IP Access-list Extended name.
```

然后输入如下命令：

```
[no] {DENY | PERMIT} protocol source source-wildcard destination destination-wildcard.
```

命名列表和标准及扩展列表的使用规则是一样的，上面的语法例子是扩展命名访问控制列表的，也可以变成匹配标准访问控制列表语法。然后输入 Exit 退出访问控制列表配置状态。使用命名的扩展访问控制列表完成实验 10-1 中 R2 的配置，替换的列表如下：

```
R2(config)#ip access-list extended tcp-firewall
R2(config-ext-nacl)#permit tcp any any established
R2(config-ext-nacl)#exit
R2(config)#int s1/1
R2(config-if)#ip access-group tcp-firewall in
```

检验 IP 访问控制列表，配置完 IP 访问控制列表后，可以使用 show access-list 命令和 show ip access-lists 命令来检验 IP 访问控制列表、列表最后括号的内容。

Show ip interface 命令提供了接口配置的 IP 指定方面的信息。它被专用来查询应用于接口的数据包过滤。它并不显示访问控制列表的内容，而只有访问控制列表的号码，如图 10-3-1 所示。

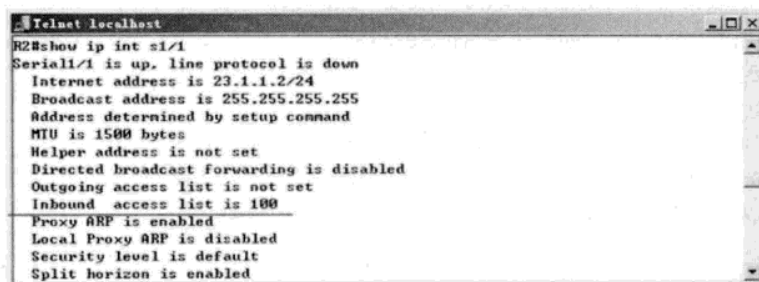


图 10-3-1 验证端口的 IP 配置

10.4 配置标准访问控制列表的注意事项

前面三节，介绍了标准、扩展和命名访问控制列表。本节介绍应用访问控制列表的一些注意事项。

1. 标准列表要应用在靠近目标端

标准访问控制列表究竟用在哪台设备上，用在哪个接口上，还是用在哪个方向上是有区别的。标准的访问控制列表只能针对源地址进行控制，10.1.2 节中把 12.1.1.1 作为源地址，R3 就成为目标地址，数据流的方向就是从左到右，如图 10-4-1 所示。从 R1 到 R3，数据包共经过了 4 个接口，如果用在 R1 的 S1/1 端口，方向应该是 out；如果用在 R2 的 S1/0 端口，方向应该是 in；如果用在 R2 的 S1/1 端口，方向应该是 out；如果用在 R3 的 S1/0 端口，方向应该是 in。接下来分析把列表分别用在 4 个端口上的区别，可以通过实验来验证下面的结论。

如果用在 R1 的 S1/1 端口，方向是 out。结果将不起作用，原因是访问控制列表仅对穿越路由器的数据包进行过滤，对本路由器起源的数据包不做过滤。

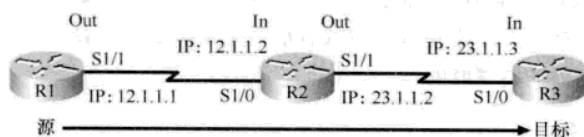


图 10-4-1 数据流的方向

如果用在 R2 的 S1/0 端口，方向是 in。结果起作用，R1 不能访问 R3 了，可 R1 也不能访问 R2 了，因为标准访问控制列表只能针对源地址，当 R1 访问 R2 的数据包进入路由器 R2 的 S1/0 端口时，源地址不符合，数据包被丢弃。

如果用在 R2 的 S1/1 端口，方向是 out。结果正确。

如果用在 R3 的 S1/0 端口，方向是 in。结果也正确。

从上面的实验中可以得出结论，标准访问控制列表要尽量用在靠近目标端，不然可能会带来错误影响，因为标准列表只能针对源地址进行过滤。

2. 扩展访问控制列表要应用在靠近源端

10.2.1 小节中扩展列表编辑完后，与标准访问控制列表一样，也有 4 个接口可供选择，方向也和标准访问控制列表一样。关键是应用在哪个接口比较合适，可以通过实验验证下面的结论。

- 如果用在 R1 的 S1/1 端口，方向是 out。结果将不起作用。
- 如果用在 R2 的 S1/0 端口，方向是 in。结果正确。
- 如果用在 R2 的 S1/1 端口，方向是 out。结果正确。
- 如果用在 R3 的 S1/0 端口，方向是 in。结果正确。

既然后 3 种情况下都可以，那么选哪一种更合适呢？一般来说扩展的访问控制列表用在靠近源的地方，因为既然不允许的数据包早晚都会被丢弃，晚丢弃不如早丢弃，早丢弃还可以节省中间链路的带宽。扩展访问控制列表用在靠近源端，会不会像标准访问控制列表一样带来错误影响呢？回答是不会，因为扩展访问控制列表中写明源地址和目标地址。

3. 访问控制列表只对穿越流量起作用

10.1.2 小节中，如果把访问控制列表用在 R1 的 S1/1 端口，方向是 out，那么结果将不起作用，原因是访问控制列表仅对穿越路由器的数据包进行过滤，对本路由器发起的数据包不做过滤。这一点很容易被大家忽视，包括一些很有经验的工程师也会犯类似的错误。

4. 放置的顺序

从 10.1.2 小节中可以看出，因为明确拒绝 R1，而允许其他的访问，所以访问控制列表中把拒绝 R1 放在第一条，允许其他的放在第二条。如果把访问控制列表中两个条目的顺序换一下，结果如何呢？结果是所有 IP 都可以访问 R3，包括 R1。原因是当 R1 用 12.1.1.1 来访问 R3 时，访问控制列表用第一条语句去匹配，12.1.1.1 是属于 any 中的一员，IP 匹配后，接下来执行操作，动作是允许，不管任何地址访问 R3，第一条都匹配，永远不会执行第二条，实验配置失败。在 IP

访问控制列表中, 语句的前后顺序很重要, 列表从上往下查找, 如果找到一条匹配, 就执行操作并不再往下继续查找。如果两条语句放在前或后都不影响结果, 一般把被较多使用的那条放在前面, 这样可以减小路由器的查找时间。

5. 隐含的拒绝所有

IP 访问控制列表的最后一句隐含的是拒绝所有。它表示必须明确允许通信量, 否则自动设成禁止。

6. 列表的编辑

访问控制列表建立后, 任何在列表中增加的语句都被放在表的末端, 用户不能有选择地增加或删除语句。唯一可以执行的删除是删除整个访问控制列表, 命令是 `no access-list access-list-number`, 显然, 当访问控制列表很大时维护是十分麻烦的。为了节省时间, 可以将表的内容剪切, 然后粘贴成文本文档来编辑。命名访问控制列表和扩展访问控制列表的增强编辑功能可用于克服这一缺点。

7. 列表的调用

一个访问控制列表可用于同一个路由器的许多不同的端口, 并不需要对每个需要它的端口定义相同的访问控制列表。如果不给端口提供任何访问控制列表, 或者提供一个未定义的访问控制列表, 则默认情况下它将传递所有通信量。如果想让访问控制列表对两个方向都有用, 则在端口调用访问控制列表两次, 一个用于入站, 另一个用于出站。对于每个协议的每个接口的每个方向, 只能提供一个访问控制列表。

值得一提的是, 如果想限制登录某台设备, 应该是进入虚拟终端线路, 使用 `access-class` 来实现, 而不是在所有接口上限制 Telnet 登录, 这个配置在前面叙述路由器安全的时候已经介绍过, 可以查阅如图 7-4-20 所示。

10.5 反射 ACL

10.2.3 小节介绍的单向访问控制方法是使用 ACL 中的 `Established` 参数检测 TCP 中是否有 ACK 位来实现的, 但这种方法仅用于基于 TCP 的上层协议, 而对于其他上层协议 (如 UDP、ICMP 等) 则无法实现单向访问控制。

本节将要介绍的反射 ACL (也称自反 ACL) 提供了一种真正意义上的单向访问控制, 它的工作原理是, 当内部网络发起一个会话 (基于 IP、ICMP、TCP、UDP 的都可以), 并且将数据发送给外部网络时, 反射 ACL 被触发并且生成一个新的临时条目。如果从外部网络过来的数据流符合临时条目, 则允许其进入内部网络, 否则禁止其进入内部网络, 如图 10-5-1 所示。



图 10-5-1 反射 ACL 示意

注 意



Cisco IOS 只支持使用扩展的命名访问控制列表来定义反射列表。

反射列表生成的临时条目在会话结束后应当被删除。对于 TCP 会话，如果路由器检测到两组 FIN 标记的分组，则在 5s 内将临时条目删除；如果路由器检测到 RST 位的分组（说明会话突然关闭），则立刻删除临时条目。对于 UDP 和其他协议，由于没有专门的机制来判断会话是否结束，因此路由器只能为其会话启动一个倒计时的计时器（全局超时），如果在计时器到期期间没有收到此会话的任何分组，则将临时条目删除（默认 300s）。

可以使用 `ip reflexive-list timeout seconds` 命令对全局超时时间进行修改。下面的命令把超时时间从 300s 改成到 60s。

```
R2(config)#ip reflexive-list timeout 60
```

下面结合实验 10-2 来讲解反射访问控制列表的配置。

实验 10-2 配置基于 IP 的单向访问（网络防火墙）

如图 10-5-2 所示，虚拟 2 相当于外网的一台主机，虚拟机 1 相当于内网的一台主机，R1 是企业的边界路由器。使用反射列表配置路由器 R1，使用虚拟机 1 可以 ping 通虚拟机 2，但虚拟机 2 却 ping 不通虚拟机 1；使用虚拟机 1 可以 Telnet 登录虚拟机 2，但虚拟机 2 不能 Telnet 登录虚拟机 1。由内网（虚拟机 1）始发的流量到达配置了自反访问表的的路由器（R1），路由器根据此流量的第 3 层和第 4 层信息自动生成一个临时性的访问表，临时性访问表的创建依据下列原则：protocol 不变，Source-IP 地址和 Destination-IP 地址严格对调，Source-port 和 Destination-port 严格对调，对于 ICMP 这样的协议，会根据类型号进行匹配。路由器将此流量传出，流量到达目标（虚拟 2），然后响应流量从目标返回到配置了自反访问列表的路由器。路由器对入站的响应流量进行评估，只有当返回流量的第 3、4 层信息与先前基于出站流量创建的临时性访问表的第 3、4 层信息严格匹配时，路由器才会允许此流量进入内部网络。该实验的步骤具体如下。

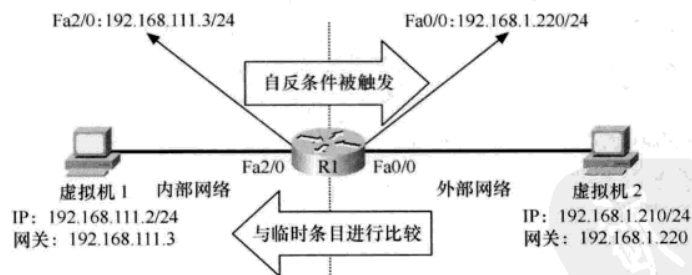


图 10-5-2 配置 IP 单向访问

STEP 1 配置 R1 的接口 IP 地址。启动安全机架中的 R1，如下配置接口的 IP 地址：

```
Router>en
Router#conf t
Router(config)#host R1
```

```
R1(config)#no cdp run
R1(config)#int fa 0/0
R1(config-if)#ip add 192.168.1.220 255.255.255.0
R1(config-if)#no shut
R1(config-if)#int fa 2/0
R1(config-if)#ip add 192.168.111.3 255.255.255.0
R1(config-if)#no shut
```

STEP 2 配置虚拟机 1。虚拟机 1 的网卡类型是 host-only, IP 地址是 192.168.111.2, 子网掩码是 255.255.255.0, 网关是 192.168.111.3 (指向 R1 的 Fa2/0 端口); 在虚拟机 1 的服务控制台中启动 Telnet 服务。

STEP 3 配置虚拟机 2。虚拟机 2 的网卡类型是 Bridged, IP 地址是 192.168.1.210, 子网掩码是 255.255.255.0, 网关是 192.168.1.220 (指向 R1 的 Fa0/0 端口); 在虚拟机 2 的服务控制台中启动 Telnet 服务。虚拟机 2 升级成域控制器后, 速度可能会变慢, 读者可以使用备份的“Windows Server 2003 Enterprise Edition.vmdk”文件恢复虚拟机 2 的操作系统。

STEP 4 测试 ping 和 Telnet。在虚拟机 1 和虚拟机 2 上分别 Telnet 和 ping 对方, 应该都是成功的。

STEP 5 配置反射列表。R1 上的反射 ACL 配置如下, 其中斜体部分为注释:

R1(config)#ip access-list extended out-acl 创建扩展的命名 ACL, 名字叫 out-acl, 用在路由器 R1 外部端口 Fa0/0 的外出方向

R1(config-ext-nacl)#permit ip any any reflect out-ip 允许所有的 IP 流量, 并对外出的 IP 流量进行反射, 反射的名字叫 out-ip, 其实就是创建临时的访问控制列表

R1(config-ext-nacl)#exit

R1(config)#ip access-list extended in-acl 创建扩展的命名 ACL, 名字叫 in-acl, 用在路由器 R1 外部端口 Fa0/0 的进入方向

R1(config-ext-nacl)#evaluate out-ip 评估反射列表, 其实就是调用前面创建的临时列表

R1(config-ext-nacl)#int fa 0/0

R1(config-if)#ip access-group out-acl out 调用访问控制列表, 要注意方向, 外出的时候做反射

R1(config-if)#ip access-group in-acl in 调用访问控制列表, 要注意方向, 进入的时候做评估

STEP 6 再次测试 ping 和 Telnet。在虚拟机 1 上 Telnet 和 ping 虚拟机 2, 应该都是成功的; 在虚拟机 2 上 Telnet 和 ping 虚拟机 1, 应该都是失败的。在路由器 R1 上查看访问控制列表, 可以发现反射访问列表 out-ip 下多出两个临时条目, 超时时间默认是 300s。

```
R1#show access-lists
Extended IP access list in-acl
  10 evaluate out-ip
Extended IP access list out-acl
  10 permit ip any any reflect out-ip (45 matches)
Reflexive IP access list out-ip
  permit tcp host 192.168.1.220 eq Telnet host 192.168.111.2 eq 54567 (27 matches) (time left 290)
  permit icmp host 192.168.1.220 host 192.168.111.2 (20 matches) (time left 246)
```

该配置并不能适用所有的服务, 如最常用的 FTP 服务。默认情况下, 虚拟机 1 访问虚拟机 2 上的 FTP 服务是成功的, 某些情况下, 虚拟机 1 访问虚拟机 2 上的 FTP 服务会失败。因为 FTP 有两种工作模式: 主动模式 (Active FTP) 和被动模式 (Passive FTP)。

在主动模式下,FTP 客户端随机开启一个大于 1024 的端口 N 向服务器的 21 号端口发起连接,然后开放 $N+1$ 号端口进行监听,并向服务器发出 PORT $N+1$ 命令。服务器接收到命令后,会用其本地的 FTP 数据端口(通常是 20)来连接客户端指定的端口 $N+1$,进行数据传输。

在被动模式下,FTP 客户端随机开启一个大于 1024 的端口 N 向服务器的 21 号端口发起连接,同时会开启 $N+1$ 号端口。然后向服务器发送 PASV 命令,通知服务器自己处于被动模式。服务器收到命令后,会开放一个大于 1024 的端口 P 进行监听,然后用 PORT P 命令通知客户端,自己的数据端口是 P 。客户端收到命令后,会通过 $N+1$ 号端口连接服务器的端口 P ,然后在两个端口之间进行数据传输。

总的来说,主动模式的 FTP 是指服务器主动连接客户端的数据端口,被动模式的 FTP 是指服务器被动地等待客户端连接自己的数据端口。被动模式的 FTP 通常用在处于防火墙之后的 FTP 客户访问外界 FTP 服务器的情况,因为在这种情况下,防火墙通常配置为不允许外界访问防火墙之后主机,而只允许由防火墙之后的主机发起的连接请求通过。因此,在这种情况下不能使用主动模式的 FTP 传输,而被动模式的 FTP 可以良好地工作。

在什么情况下使用 FTP 的主动模式呢?如为了保证服务器的安全,服务器对外界只开放了 20 和 21 号端口,这时就需要使用 FTP 的主动模式。

通过对 FTP 两种模式的分析,可以知道如果 FTP 客户端使用主动模式,客户端(虚拟机 1)发起到服务器(虚拟机 2) 21 号端口的连接,服务器用 20 号端口初始化到客户端一个大于 1024 以上的端口的连接,用于数据传输,由于自反访问控制列表中,只能由内部(也就是虚拟机 1)发起连接,服务器发起的连接被拒绝,FTP 服务失败。解决的办法有如下两种。

方法一,修改 FTP 客户端。FTP 客户端使用被动模式,在虚拟机 1 上,打开 IE 浏览器。选择“工具”菜单→“Internet”命令,打开“Internet 选项”对话框,单击“高级”选项卡,如图 10-5-3 所示,选中“使用被动 FTP”复选框。单击“确定”按钮返回,重新打开 IE 浏览器即可。

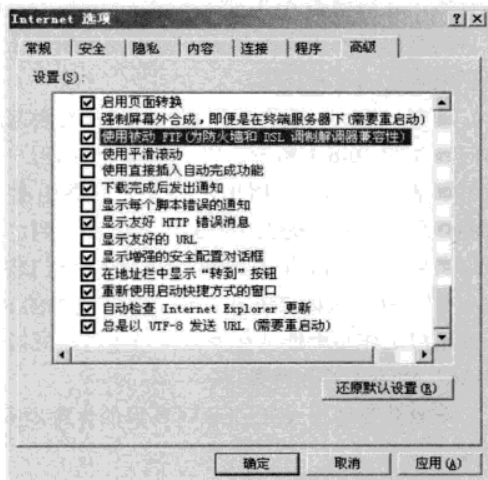


图 10-5-3 客户端取消使用被动 FTP

注意



IE 浏览器中默认使用的是 FTP 被动模式,如果 FTP 服务器对外只开放了 20 和 21 号端口,FTP 客户端就要使用主动模式,取消图 10-5-3 所示的“使用被动 FTP”复选框即可。

方法二,修改访问控制列表。修改路由器外部接进入方向的访问控制列表,在评估反射列表前,允许外部的 TCP 20 号端口访问内部的任何端口。这种方式更灵活,不管客户端(虚拟机 1)使用主动还是被动 FTP 模式,都可以正常访问外界的 FTP 服务器(虚拟机 2)。

R1(config)#ip access-list extended in-acl 创建扩展的命名 ACL, 名字叫 in-acl, 用在路由器 R1 外部接口 Fa0/0 的进入方向

R1(config-ext-nacl)#permit tcp any eq 20 any 允许外部 FTP 服务器使用 TCP 的 20 号端口主动连接内部任何主机的任何 TCP 端口

R1(config-ext-nacl)#evaluate out-ip 评估反射列表, 其实就是调用前面创建的临时列表

本章 10.8 小节中将介绍基于内容的访问控制列表, 使用该列表可以更好地解决类似 FTP 服务这种动态协商端口的问题。

10.6 动态 ACL

本节详细介绍动态 ACL, 动态 ACL 是对传统 ACL 的一种功能增强。传统的标准 ACL 和扩展 ACL 不能创建动态访问条目。一旦在传统 ACL 中加入了一个语句, 除非手工删除, 该语句将一直产生作用。而在动态 ACL 中, 网络管理员可以根据用户认证过程来创建特定的、临时的 ACL。

动态 ACL 使用动态扩展 ACL 过滤 IP 流量。当配置了动态 ACL 之后, 临时被拒绝的 IP 流量可以获得暂时性的许可。动态 ACL 临时修改路由器端口下已经存在的 ACL, 允许 IP 流量到达目标设备, 之后动态 ACL 把端口状态还原。通过动态 ACL 获得访问目标设备权限的用户, 首先要开启到路由器的 Telnet 会话, 接着动态 ACL 自动对用户进行认证, 如果认证通过, 那么用户就获得了临时性的访问权限。

动态 ACL 一般用于控制外网用户对内网服务器的访问, 如图 10-6-1 所示。当 Internet 上的用户需要访问内网的服务器时, 外网用户需要先向路由器发起一个 Telnet 会话, 并且提供相应的用户名和密码, 在用户被认证之后, 路由器将一个临时的 ACL 语句添加到动态 ACL 中, 并且关闭 Telnet 会话, 动态添加的 ACL 对被认证用户工作站地址进行授权, 当条目超时后, 删除动态 ACL 中添加的临时条目。

下面介绍动态 ACL 中临时条目的生存周期和 Telnet 设置。



图 10-6-1 动态 ACL 原理图

1. 临时条目的生存周期

和自反 ACL 一样, 动态 ACL 也会创建临时条目, 其生存周期有两个参数: 空闲时间和绝对时间。当路由器产生临时条目时, 该临时条目的空闲计时器和绝对计时器同时启动。空闲计时器在每有一个报文匹配动态访问表项时进行复位, 当空闲计时器计时到期时, 该临时条目被删除。绝对计时器永不复位, 当绝对计时器到期时, 该临时条目被删除, 而忽略空闲计时器的值和当前连接状态。通常情况下, 绝对时间应设置得大一些, 如 24 小时; 而空闲时间应设置得远远小于绝对时间, 如 5 分钟。

2. Telnet 的设置

设置动态 ACL 以后,所有的 Telnet 请求都会被路由器认为是要开启一个动态 ACL 条目,当用户被认证之后, Telnet 会话很快就会被关闭。这就带来了一个问题,网络管理员将不再能够通过 Telnet 对路由器进行管理。

解决上述问题的方法是在一部分 VTY 线路上使用 rotary (旋转) 命令开启其他的 Telnet 端口,例如,“rotary 1”命令开启 3001 端口、“rotary 2”命令开启 3002 端口,依此类推。

实验 10-3 动态 ACL

如图 10-6-2 所示,通过使用动态 ACL 实现让内网用户(虚拟机 1 所在网段)能够访问 Internet,但 Internet 上的用户(虚拟机 2 所在网段)需要访问内网时,需要先到路由器上认证。该实验的配置步骤如下。

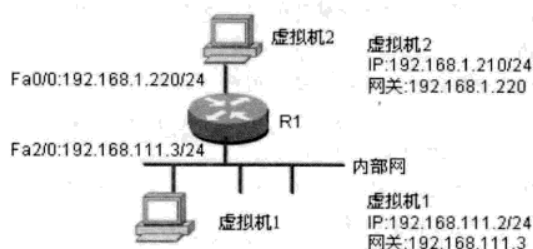


图 10-6-2 动态 ACL 实验

STEP 1 基本网络配置。配置虚拟机 1, 虚拟机 2, 配置安全机架中路由器 R1 的端口 IP 地址等。同实验 10-2 中的配置。

STEP 2 测试。在路由器 R1 上使用 show access-lists 验证 ACL, 显示如下:

```
R1#show access-lists
Extended IP access list 100
 10 permit tcp any host 192.168.1.220 eq telnet
 20 permit tcp any host 192.168.1.220 eq 3001
 30 permit tcp any any established
 40 permit udp any any gt 1023
 50 Dynamic cisco permit ip any any
```

虚拟机 1 和虚拟机 2 相互 Telnet 对方的 IP 地址, 应该都可以访问。

STEP 3 动态 ACL 配置。路由器 R1 动态 ACL 的配置如下, 其中斜体部分为解释语句:

R1(config)#access-list 100 permit tcp any host 192.168.1.220 eq 23 允许外网 Telnet 路由器进行身份验证
R1(config)#access-list 100 permit tcp any host 192.168.1.220 eq 3001 允许外网 Telnet 路由器的 3001 端口进行管理。工程中, 很少在 Internet 上使用 Telnet, 因为密码明文传输, 很不安全。如果工程中使用的是其他网管协议, 记得放开对应的端口

R1(config)#access-list 100 permit tcp any any established 允许内网出去的 TCP 流量可以正常返回, 详见实验 10-1

R1(config)#access-list 100 permit udp any any gt 1023 允许内网出去的 UDP 流量可以返回, 一般服务

端使用的都是小于 1024 的端口，客户端使用大于 1023 的端口

R1(config)#access-list 100 dynamic cisco timeout 120 permit ip any any 创建动态 ACL，命名为 cisco，该语名中的第一个 any 关键字将被通过认证的用户的 IP 地址替代，第二个 any 代指内网所有主机。当然这里可以变成特定的主机，这样做的结果是，即使外网用户通过路由器的验证也只能访问内网中的特定主机；还可以把 IP 协议换成其他协议，如 TCP 的 80，这样做的结果是，即使外网用户通过路由器的验证也只能访问内网中特定主机 TCP 的 80 端口，也就是 web 主页。Timeout 是绝对时间，120 分钟，也就是两小时

R1(config)#user cisco pass cisco 创建用户 cisco，用于身份验证

R1(config)#line vty 0 3 虚拟终端用户 0, 1, 2, 3

R1(config-line)#login local 使用路由器本地的用户名和密码验证

R1(config-line)#autocommand access-enable host timeout 5 这里的参数输入一定要正确，即使输入错误也没有提示，其中 host 参数的意思是认证主机的源 IP 地址替换动态 ACL 中的 any 关键字，timeout 时间是指空闲时间，其后面的 5 代表 5 分钟

R1(config-line)#line vty 4 虚拟终端用户 4

R1(config-line)#login local 使用路由器本地的用户名和密码验证

R1(config-line)#rotary 1 设置 VTY 4 号线路为管理员使用 Telnet 对路由器进行管理，Telnet 端口为 3001

R1(config-line)#int fa 0/0

R1(config-if)#ip access-group 100 in 在路由器外网端口上应用 ACL

STEP 4 测试。在虚拟机 1 上 Telnet 虚拟机 2，可以访问。在虚拟机 2 上 Telnet 虚拟机 1，失败。在虚拟机 2 上 Telnet 路由器的外网端口 192.168.1.220，要求验证，如图 10-6-3 所示。输入用户名 cisco，密码 cisco，验证通过，Telnet 会话自动被终止。在虚拟机 2 上再次 Telnet 虚拟机 1，可以正常访问了。

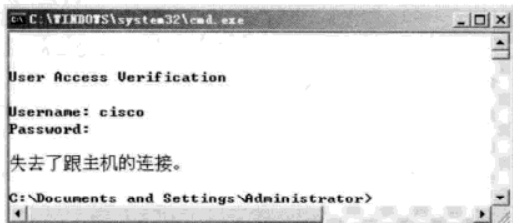


图 10-6-3 动态 ACL 验证

在路由器 R1 上使用 show access-lists 验证 ACL，显示如下：

```
R1#show access-lists
Extended IP access list 100
 10 permit tcp any host 192.168.1.220 eq telnet (183 matches)
 20 permit tcp any host 192.168.1.220 eq 3001
 30 permit tcp any any established (42 matches)
 40 permit udp any any gt 1023 (2 matches)
 50 Dynamic cisco permit ip any any
    permit ip host 192.168.1.210 any (17 matches) (time left 121)
```

从上面的输出中，可以发现最后一行是路由器产生的一个动态 ACL 条目。该条目超过 121s 将被删除。

10.7 基于时间的访问控制列表

基于时间的 ACL 是对传统 ACL 的一种功能增强，它在传统扩展 ACL 中加入了时间范围以增强 ACL 的控制功能。要使用基于时间的 ACL，首先要创建一个时间范围，然后在扩展 ACL 中进

行调用。创建时间的范围的格式如下，斜体部分为注释：

```
R1(config)#time-range working 定义时间范围的名字
R1(config-time-range)#? 寻求在线帮助
Time range configuration commands:
  absolute absolute time and date 定义绝对时间范围，只能以时间（hh:mm）为参数，时间参数必须以 24 小时制来表示
  default Set a command to its defaults
  exit Exit from time-range configuration mode
  no Negate a command or set its defaults
  periodic periodic time and date 定义周期性的时间范围，可以是星期几（记得要写英文）、daily（每天）、weekday（周一至周五）、weekend（周末）和时间（hh:mm）为参数
```

注 意



Cisco IOS 只支持使用扩展访问控制列表定义基于时间的 ACL。

实验 10-4 配置基于时间的 ACL

下面举一个例子来说明基于时间的 ACL 的定义方法。如某单位希望在企业出口路由器上使用基于时间的 ACL，实现从周一到周五（工作日）的上午从 8:00 到 12:00，下午从 13:30 到 17:30 只允许所有用户收发邮件，而在非工作时间允许所有的访问。本实验可以在虚拟机 1 和虚拟机 2 上测试。该实验的配置步骤如下。

STEP 1 设置路由器 R1 的时间。在路由器的特权模式下，使用 `clock set` 调整路由器的时间。

STEP 2 定义时间范围。

```
R1(config)#time-range working 定义上班时间范围
R1(config-time-range)#periodic weekdays 8:00 to 12:00 周一至周五每天从 8 点到 12 点
R1(config-time-range)#periodic weekdays 13:30 to 17:30 周一至周五每天从 13:30 到 17:30，两个小时加起来就是从早 8 点到下午的 5 点半，除去中午一个半小时的休息时间。
```

STEP 3 编辑 ACL。

```
R1(config)#access-list 100 permit tcp any any eq 25 允许发送邮件
R1(config)#access-list 100 permit tcp any any eq 110 允许接收邮件
R1(config)#access-list 100 permit udp any any eq 53 允许使用外网的 DNS 服务器
R1(config)#access-list 100 deny ip any any time-range working 在工作时间阻止所有的 IP 通信
R1(config)#access-list 100 permit ip any any 允许所有的 IP 通信
```

STEP 4 调用 ACL。

```
R1(config)#int fa 0/0 进入对外接口
R1(config-if)#ip access-group 100 out 调用访问控制列表
```

STEP 5 测试。调整路由器的时间，测试虚拟机 1 和虚拟机 2 在不同时间使用不同应用程序的现象。结果是虚拟机 1 一直可以使用虚拟机 2 上的邮件服务（如架设邮件服务器比较复杂，这里可以换成 Telnet 测试，Telnet 的端口是 TCP 的 23），但其他服务只有在非工作时间才可以使用。

10.8 基于上下文的访问控制列表

CBAC (Context-Based Access Control, 基于上下文的访问控制) 是 Cisco IOS 防火墙特征集中的一个特性。本节将介绍 CBAC 的功能和配置方法, 并通过一个实验演示 CBAC 的应用。

10.8.1 CBAC 功能

CBAC 可以基于应用层协议的会话信息智能地过滤 TCP 和 UDP 包, 可以提供对网络的多级保护, 包括流量过滤、流量检查、警告和审计、入侵检测等。

1. 流量过滤

CBAC 智能地根据应用层协议会话信息过滤 TCP 和 UDP 包, 可以配置 CBAC 允许指定的 TCP 和 UDP 流量仅当连接由保护的网路中发起时穿过防火墙。CBAC 可以拦截起源于防火墙任意方向的流量, 而且 CBAC 可以用在网络内部、网络外部和互联网边缘。CBAC 使用状态表来维护会话的状态信息, 它在防火墙的接口上动态地建立和删除 ACL 条目以检查返回内部网络的流量。最后的实例中将演示这一功能。

如果没有 CBAC, 流量过滤是仅限于在网络层检查访问列表, 或者最多也就是在传输层。但 CBAC 检查的不仅是网络层和传输层的信息, 也检查应用层的信息 (如 FTP 连接信息), CBAC 可以识别控制通道中应用程序特有的命令, 学习关于会话的状态信息, 这就允许支持有多通道协商的协议。最后的实例也将演示这一功能。

使用 CBAC 可以配置用来基于服务器地址或者完全地拒绝嵌入了压缩包的 Java 小程序。保护用户下载使用 Java 的时候对网络造成的不良风险。为了更好的保护网络, 降低风险, 可以在所有用户的浏览器中禁用 Java, 也可以建立一个 CBAC 拦截规则来在防火墙过滤, 如果是用户必须使用的 Java 程序就放行。

2. 流量检查

CBAC 检查穿过防火墙的流量来探索和管理 TCP 和 UDP 会话的状态信息。这个状态信息是用来建立临时通道打开防火墙的访问控制列表允许的流量返回, 以及允许会话的附加数据连接。

由于在应用层检查包, 维护 TCP 和 UDP 会话信息, CBAC 通过限制半开会话数量来有效地防止 DDoS (Distributed Denial of Service, 分布式拒绝服务) 攻击。

3. 警告和审计

CBAC 怀疑网络中存在攻击行为时, 它可以产生警告信息并且阻止来自被怀疑对象的数据包。CBAC 能生成实时警报和审计痕迹。加强审计特性用 SYSLOG 来跟踪所有网络处理情况, 记录时间戳、源和目的使用的端口及传输字节数, 还有基于会话报告的高级功能。实时警报基于积极的探测, 可疑情况和错误信息被发送给 SYSLOG 服务器。使用 CBAC 监视规则, 可以配置警报和

跟踪信息，并且基于每一个协议。最后的实例中会演示这一功能。

4. 入侵检测

CBAC 提供一种有限的入侵检测保护指定的 SMTP 攻击。使用入侵检测，SYSLOG 信息显示和监控制定的“攻击特征”，特定的网络攻击类型有指定的角色或特征。当 CBAC 检测到攻击，可以复位有关连接，发送 SYSLOG 到 SYSLOG 服务器。

CBAC 提供附加的有限的入侵检测，Cisco IOS 防火墙特性集提供入侵检测技术给中等级别和高端路由器平台使用 Cisco IOS 防火墙 IDS。考虑到网络大小，尤其是路由器作为附加和扩展的安全性，这在网络段之间是非常必要的。

Cisco IOS 防火墙入侵检测能识别一些种常见的攻击，使用特征来探测网络流量使用，能有效阻止对安全构成危险的大多数普通网络攻击和摄取信息的扫描。

注 意



只有具有防火墙特性集的 IOS 才支持 CBAC，可在安全机架的路由器 R1 中完成本节的操作。

10.8.2 配置 CBAC

具体配置 CBAC 包括以下部分或全部配置选项。

1. 设置全局参数（可选）

- “ip inspect tcp synwait-time seconds” 命令用于定义在丢弃会话之前，CBAC 将等待多长时间使 TCP 会话达到已建立状态，该时间参数的默认值为 30s。

- “ip inspect tcp finwait-time seconds” 命令用于定义当防火墙检测到 TCP 会话的 FIN 信号时，它还将管理这个会话多长时间，该时间参数的默认值为 5s。

- “ip inspect tcp idle-time seconds” 命令用于定义 TCP 的空闲超时值，该时间参数的默认值为 3600s，即 1 小时。

- “ip inspect udp idle-time seconds” 命令用于定义 UDP 的空闲超时值，该时间参数的默认值为 30s。

- “ip inspect dns-timeout seconds” 命令用于定义 DNS 的空闲超时值，该时间参数的默认值为 5s。

上小节曾经提到过“半开会话”这个词，对于 TCP 来讲，半开会话是指会话没有达到建立状态，即 TCP 三次握手还没有完成；对于 UDP 来讲，半开会话是指防火墙在一定时间内没有检测到返回的流量。如果路由器检测到过多的半开会话，说明网络中可能存在 DoS 攻击。

- “ip inspect max-incomplete high number” 命令用于定义半开会话数量的最大值，当半开会话的数量超过此阈值时，CBAC 开始删除现有的半开会话，该参数的默认值为 500。“ip inspect max-incomplete low number” 命令用于定义半开会话数量的最小值，当半开会话的数量降低到此阈值时，CBAC 停止删除半开会话，该参数的默认值为 400。

- “ip inspect one-minute high number” 命令用于定义新连接的尝试速率的最大值，当

新连接的尝试速率超过此阈值时, CBAC 开始删除现有的半开会话, 以安排新的请求, 该参数的默认值为 500。“ip inspect one-minute low number” 命令用于定义新连接的尝试速率的最小值, 当新连接的尝试速率降低到此阈值时, CBAC 停止删除半开会话, 该参数的默认值为 400。

“ip inspect tcp max-incomplete host number block-time minutes” 命令用于限制发往相同主机地址的半开会话的数量。

2. 设置端口到应用的映射 (PAM)

PAM (Port-to-ApplicationMapping, 映射端口到应用程序) 可以为网络服务或应用定制 TCP 和 UDP 端口号。PAM 让 CBAC 可以审查运行在非标准端口上的应用。

Cisco IOS 定义了一个默认 PAM 表, 可以使用 show ip port-map 命令进行查看。

如果有运行在非标准端口上的应用就需要在 PAM 表中添加自定义条目, 例如, 实验部分将 2121 端口也映射为 FTP 服务, 可以使用命令:

```
Router(config)#ip port-map ftp port tcp,21 2121
```

3. 定义协议审查规则

ip inspect name inspection-name protocol [alert {on | off}] [audit-trail {on | off}][timeout seconds] 命令可以定义一组审查规则。如表 10-8-1 所示是对该命令各参数的解释。

表 10-8-1 审查规则参数

参 数	解 释
inspection-name	审查规则的名称
protocol	定义要审查的协议
alert {on off}	设置是否产生告警消息
audit-trail {on off}	设置是否产生审计跟踪
timeout seconds	制定一个不同的空闲超时时间, 该参数会覆盖特定协议的全局 TCP 或 UDP 空闲超时时间

实验 10-5 配置 CBAC 防火墙

配置 CBAC 可使只有内部网络发起的流量才允许通过路由器返回, 并能对特定流量产生警告并进行跟踪。这里以 FTP 为例, 把虚拟机 2 当成外网, 虚拟机 1 当成内网, FTP 服务器使用的端口是 2121, 要求跟踪主动和被动 FTP 模式, 展示两种模式的区别。实验拓扑如图 10-6-2 所示, 配置步骤如下。

STEP 1 基本网络配置。配置虚拟机 1, 虚拟机 2, 配置安全机架中路由器 R1 的端口 IP 地址等。如实验 10-2 所示的配置。

STEP 2 测试。虚拟机 1 可以正常使用虚拟机 2 上的 FTP 和 Telnet 服务, 虚拟机 2 也可以使用虚拟机 1 上的 FTP 和 Telnet 服务。

STEP 3 配置 CBAC。路由器 R1 上 CBAC 的配置如下, 其中斜体部分为解释语句:

R1(config)#ip port-map ftp port tcp 21 2121 在 21 和 2121 端口上审查 FTP 服务, 如果这里不添加 2121, CBAC 默认只在 21 端口审查 FTP 服务

R1(config)#ip inspect name cisco ftp alert on audit-trail on timeout 300 创建审查规则 cisco, 审查 FTP 服务, 打开告警和跟踪

R1(config)#int fa 0/0

R1(config-if)#ip inspect cisco out 以数据包外出时调用跟踪规则

R1(config-if)#ip access-group 102 in 调用 ACL 102, 静止所有的包从外部端口进入

R1(config-if)#exit

R1(config)#access-list 102 deny ip any any

STEP 4 测试服务。虚拟机 1 访问虚拟机 2 上的 FTP 服务, 可以正常访问; 虚拟机 1 使用 Telnet 登录虚拟机 2, 失败。虚拟机 2 访问虚拟机 1 上的所有服务都失败。

STEP 5 跟踪 FTP 的被动模式。虚拟机 1 使用默认的被动模式访问虚拟机 2 上的 FTP 服务时, 路由器上出现以下日志:

```
*Feb 21 10:39:35.803: %FW-6-SESS_AUDIT_TRAIL_START: Start ftp session: initiator (192.168.111.2:1062) -- responder (192.168.1.210:21)
```

```
*Feb 21 10:39:35.979: %FW-6-SESS_AUDIT_TRAIL_START: Start ftp-data session: initiator (192.168.111.2:1063) -- responder (192.168.1.210:1308)
```

在被动模式下, FTP 客户端随机开启一个大于 1024 的端口 N 向服务器的 21 号端口发起连接, 同时会开启 $N+1$ 号端口。然后向服务器发送 PASV 命令, 通知服务器自己处于被动模式。服务器收到命令后, 会开放一个大于 1024 的端口 P 进行监听, 然后用 PORT P 命令通知客户端, 自己的数据端口是 P 。客户端收到命令后, 会通过 $N+1$ 号端口连接服务器的端口 P , 然后在两个端口之间进行数据传输。注意第二行的内容。

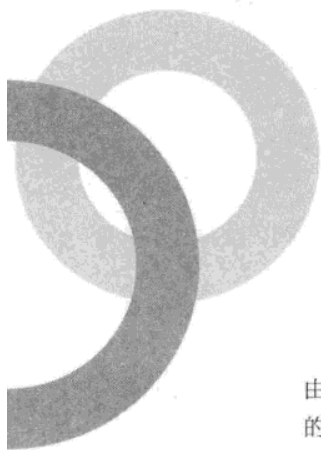
STEP 6 跟踪 FTP 的主动模式。如图 10-5-3 所示, 在虚拟机 1 上取消选择“使用 FTP 的被动...”, 换成使用 FTP 的主动模式, 当虚拟机 1 再次访问虚拟机 2 上的 FTP 服务时, 路由器上出现以下日志:

```
*Feb 21 10:23:05.811: %FW-6-SESS_AUDIT_TRAIL_START: Start ftp session: initiator(192.168.111.2:1050) -- responder (192.168.1.210:21)
```

```
*Feb 21 10:23:06.043: %FW-6-SESS_AUDIT_TRAIL_START: Start ftp-data session: initiator (192.168.1.210:20) -- responder (192.168.111.2:1051)
```

在主动模式下, FTP 客户端随机开启一个大于 1024 的端口 N 向服务器的 21 号端口发起连接, 然后开放 $N+1$ 号端口进行监听, 并向服务器发出 PORT $N+1$ 命令。服务器接收到命令后, 会用其本地的 FTP 数据端口 (通常是 20) 来连接客户端指定的端口 $N+1$, 进行数据传输。注意第二行, 两种模式区别在于第二行的内容。





第 11 章 AAA（认证、授权、记账）

Chapter 11

介绍 AAA 之前，先介绍一个实际遇到的工程，江苏某市某个通信公司有几十台路由器分布在全市各地，IT 部门有员工近十人。为了方便远程管理，公司几十台路由器的密码设置都一样，所有 IT 部门的员工都知道。如果 IT 部门有一位员工工作调动，几十台路由器的密码要全部重设一遍，工作量大且不说，关键是如果有人误操作，将无法责任到人，因为所有 IT 部的人都有特权密码。通过使用 AAA 服务，可以把账号集中管理，如果有员工离开，只要从服务器上删除该账号就可以了；还可以使用 AAA 对路由器可执行命令进行授权，普通员工只能执行一些查看命令，不允许修改关键配置；更重要的是，可以启用 AAA 服务中的记账功能，记录下哪个用户何时执行何操作，出了问题很容易查找到某个人。

11.1 AAA 简介

访问控制是控制访问网络中的服务器或路由器的权限，允许使用什么服务。通过使用认证、授权和记账，可以很好地保障网络和服务的安全。

通常，AAA 访问控制系统由 3 部分组成：AAA 服务器、AAA 客户端和最终客户端，如图 11-1-1 所示。最终客户端向 AAA 客户端请求服务，AAA 客户端把最终客户端的验证信息转发给 AAA 服务器，AAA 服务器提供认证、授权和记账服务，三者协同工作以构成一个完整的访问控制系统。AAA 的定义如下。

- Authentication（认证）：对用户的身份进行验证，决定是否允许该用户访问网络，即“是谁？”。

- Authorization（授权）：给不同的用户分配不同的权限，限制每个用户可以使用的网络服务，即“可以做什么？”。

- Accounting（记账）：对用户的行为进行审计和计费，即“做了什么？”。

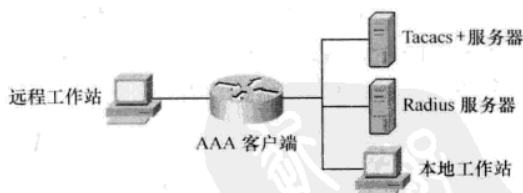


图 11-1-1 AAA 拓扑图

Cisco Secure ACS 是一款 AAA 服务端软件,它支持的协议有 TACACS+和 RADIUS。TACACS+使用的是 TCP,为思科私有;RADIUS 使用的是 UDP,是 IETF 标准。Cisco Secure ACS 可以使用 RADIUS 或 TACACS+协议与 Cisco 设备协同工作。

11.2 Cisco Secure ACS

本节介绍 Cisco Secure ACS 安装和安装过程中的注意事项,了解 ACS 的 Web 管理界面和基本配置。

Cisco Secure ACS 是一款用来控制对网络访问的安全软件,它可以对用户进行认证、授权和审计。Cisco Secure ACS 分为 Windows 和 Unix 两个版本,其中 For Windows 的版本只能安装在服务器版本的操作系统上,如 Windows 2000 Server (sp4) 或 Windows 2003 Server。

Cisco Secure ACS 管理起来十分简单,用户可以使用 Web 浏览器完成对它的所有管理。本章提到的 ACS (Access Control Server, 访问控制服务器) 均指 Cisco Secure ACS for windows version 3.3。

11.2.1 安装 ACS

ACS 的安装过程如下。

STEP 1 安装前准备工作。配置虚拟机 2 的网卡类型是 Bridged, IP 地址 192.168.1.210, 子网掩码 255.255.255.0, 网关为 192.168.1.1, DNS 为 218.2.135.1。

STEP 2 开始安装。在虚拟机 2 中打开 ACS 3.3 文件夹, 双击文件夹中的 setup.exe 文件, 开始安装。如果虚拟机的内存小于 256MB, 会出现警告, 但不会影响使用, 单击“确定”按钮继续。

STEP 3 接受许可协议。单击“Accept”接受许可协议。

STEP 4 安装的前提条件。单击“Next”按钮, 弹出图 11-2-1 所示对话框, 必须选中 4 个复选框, 才可以继续往下安装。第一个复选框提示终端用户要能够连接到 AAA 客户端, 相当于图 11-1-1 所示的工作站要能连通路由器; 第二个复选框提示 ACS 服务器要能 ping 通 AAA 客户端, 相当于图 11-1-1 所示的 Radius 或 Tacacs+服务器能够 ping 通路由器; Cisco 设备作为 AAA 客户端, 要运行 Cisco IOS 11.1 以后的版本; 安装有 IE v6.0 或 Netscape v7.02 以后的浏览器。选中 4 个复选框后, 单击“Next”继续。

注 意



这里还需要安装 Java run time (JRE)。JRE 的最新版本可以从 www.sun.com 下载, 本书提供的下载文件 network.rar 中提供了一个 j2re-1_4_2_12 版本。安装完 Java 需要重新启动计算机。ACS 和 Java 的安装不分先后, 但运行 ACS 前一定要安装好 Java, 因为 ACS 需要 Java 支持。

STEP 5 安装路径选择。保持默认的安装路径。单击“Next”继续。

STEP 6 验证数据库的配置。在如图 11-2-2 所示的对话框中, 提示选择验证数据库。有两种选择: 选项一只使用 ACS 的数据库验证, 选项二 Windows 和 ACS 数据库同时使用。如果让

ACS 能和 AD 活动目录联动, 则需选择使用 Windows 数据库, 否则只使用 ACS 数据库即可。这里选第一个, 只使用 ACS 数据库。单击 “Next” 按钮继续。

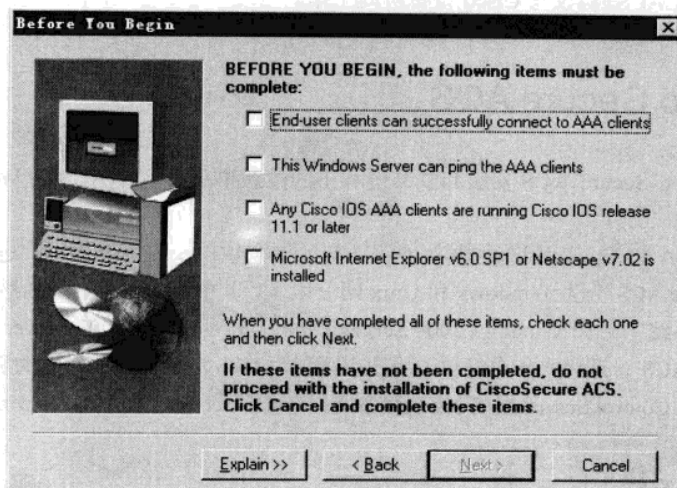


图 11-2-1 ACS 安装的前提

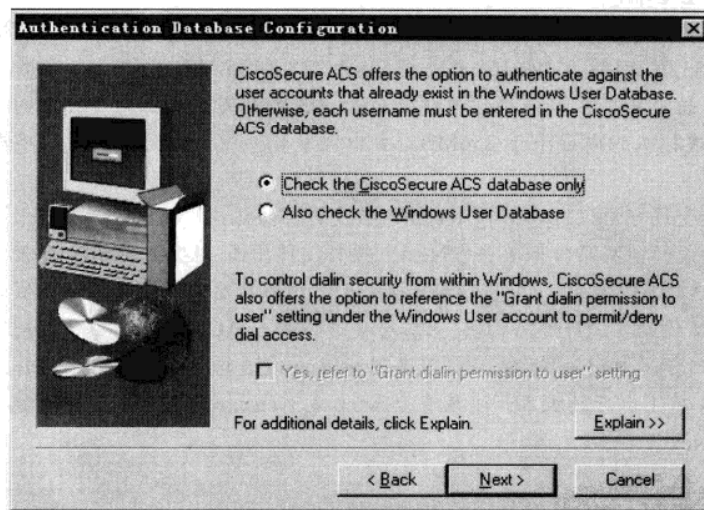


图 11-2-2 配置验证数据库

STEP 7 高级选项。安装程序开始复制文件, 大约一分钟后, 弹出如图 11-2-3 所示的对话框, 提示选择高级选项, 这些高级选项暂不要选中, 以后如果需要可以添加。接下来根据提示单击 “Next” 按钮完成安装。

STEP 8 完成安装。接下来在安装对话框中, 都是直接单击 “Next” 按钮, 直至单击 “Finish” 按钮完成安装。

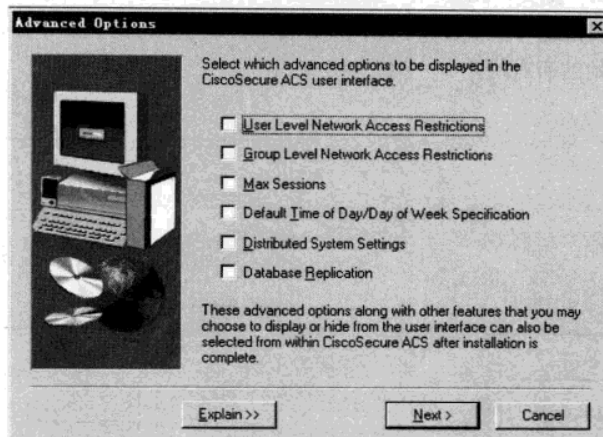


图 11-2-3 高级选项

11.2.2 ACS 的基本配置

双击桌面上的 ACS 快捷图标或在浏览器的地址栏里输入“http://hostname(or IP address):2002”访问 ACS 的 Web 配置页面。运行 ACS 时，会自动运行 Java，如果屏幕弹出图 11-2-4 所示对话框，表示 Java 没有安装，请安装 Java 重启计算机后，再次打开 ACS 管理界面。

ACS 的管理界面如图 11-2-5 所示，ACS 的 Web 页面分为两部分，其左边一排按钮为配置导航条，当用户单击导航条中的某个选项时，该选项的具体内容会在页面的右边出现。

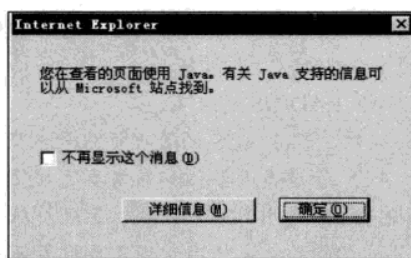


图 11-2-4 未安装 Java 提示

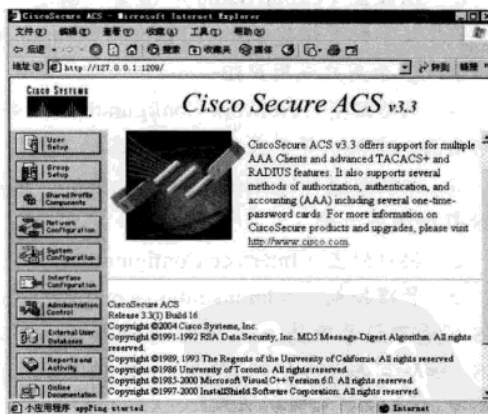


图 11-2-5 ACS 主界面

例如，单击“User Setup”导航条以后，打开“User Setup”页面，如图 11-2-6 所示，在“User:”栏中填入用户名，如填入 cisco，再单击“Add/Edit”按钮。

打开如图 11-2-7 所示页面。页面中有很多选项，只有图中所示的密码是必填项，其他项都保

持默认。单击“Submit”提交，cisco 用户添加成功。在图 11-2-6 所示界面中，还可以输入一个用户名，单击“Find”按钮进行查找；单击图 11-2-6 所示界面下方的某一个字母或数字，系统会列出以该字母或数字开始的所有用户。

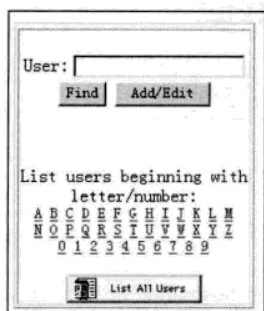


图 11-2-6 新建用户

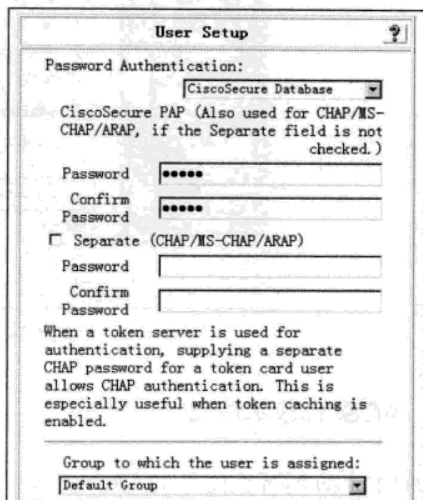


图 11-2-7 用户信息

这里对 ACS 的导航条进行简单介绍。

- 用户设置 (User Setup): 查看、创建、编辑、删除用户账号。
 - 组设置 (Group Setup): 查看、创建、编辑用户组设置。
 - 共享配置组建 (Shared Profile Components): 包括一些可共享的授权组件，它们可以应用于一个或多个用户或用户组。
 - 网络配置 (Network Configuration): 查看、创建、编辑、删除 AAA 客户端 (网络设备，如路由器、交换机等) 或 AAA 服务器的参数。
 - 系统配置 (System Configuration): 启动或停止 ACS 服务，创建或删除网络日志，控制 ACS 数据库同步等。
 - 接口配置 (Interface Configuration): 配置 TACACS+和 RADIUS 的选项。
 - 管理控制 (Administration Control): 查看、创建、编辑、删除 ACS 的管理员账号参数。
- ACS 没有默认管理员，从 ACS 服务器本地可以直接打开 ACS 管理界面，但如果需要远程管理 ACS，如从真实机上管理 ACS，如图 11-2-8 所示，则需要输入管理的用户名和密码。管理员从远程管理 ACS 的权限可以在 ACS 本地进行指定，可以创建不同的管理员，根据管理需要设置不同的用户组，可以使 ACS 的管理功能更灵活。
- 外部数据库 (External User Database): 配置 ACS 的外部数据库类型以及未知的用户策略。
 - 报告和活动 (Report and Activity): 查看 TACACS+和 RADIUS 的审计报告、Failed Attempts 报告以及已经登录的用户信息等。

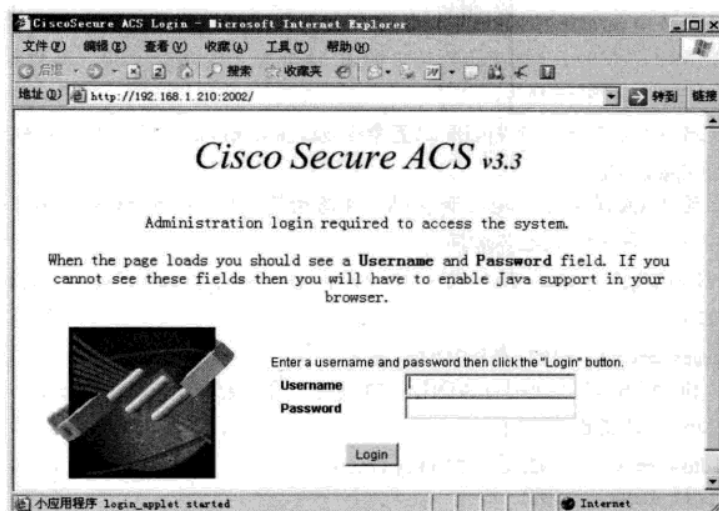


图 11-2-8 ACS 的远程管理

- 在线文档 (Online Documentation): 提供关于 ACS 的更详细的文档。

本节简单介绍了 ACS 的安装和基本配置, 有关 ACS 更多更高级的应用将在下节介绍。

11.3 配置 AAA 认证

回忆本章开始介绍的某通信公司实例, 有几十台路由被分散管理的弊端。本节结合实验介绍 Cisco IOS 中 AAA 认证的配置方法, 通过配置 AAA, 实现图 11-3-1 所示两台路由器的集中管理, 当然也可以添加更多路由器。

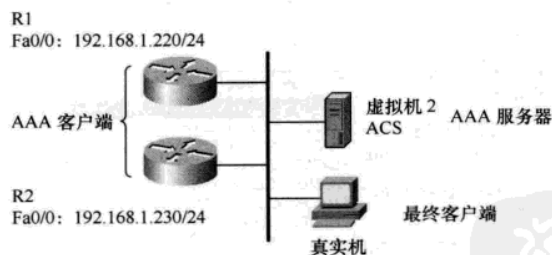


图 11-3-1 AAA 认证

当真实机通过虚拟终端方式远程管理路由器 R1 和 R2 时, 真实机尝试连接路由器 R1 或 R2, 路由器收到真实机的连接请求后, 路由器给出验证信息, 真实机提供相关的用户名和密码, 路由器把用户名和密码信息发送到 ACS 服务器, ACS 验证用户的合法性, 如合法则允许用户登录路由器, 否则拒绝用户的连接。因为使用的是 Radius 或 Tacacs+, 验证的具体细节会有点差异, 但上面的验证过程不影响用户的理解。具体操作步骤如下。

STEP 1 配置路由器的端口 IP 地址。开启安全机架中的路由器 R1 和 R2, R1 的 Fa0/0 端口的 IP 地址是 192.168.1.220 和 R2 的 Fa0/0 端口的 IP 地址是 192.168.1.230。路由器 R1 和 R2 的配置类似, 以下仅以 R1 的配置为例。

STEP 2 开启 AAA 服务。使用全局配置命令 `aaa new-mode` 启用 AAA 服务。

R1(config)#aaa new-model

STEP 3 配置 AAA 服务器的地址和密码。在路由器 R1 上配置 ACS 服务器的地址和密码, 根据使用的协议不同, 命令格式也不相同。

AAA Client 和 ACS 之间使用 TACACS+协议时, 命令格式是 `tacacs-server host IP_address key key`, R1 的配置如下:

R1(config)#tacacs-server host 192.168.1.210 key cisco

AAA Client 和 ACS 之间使用 RADIUS 协议时, 命令格式是 `radius-server host IP_address radius-server key key`, R1 的配置如下:

R1(config)#radius-server host 192.168.1.210 key cisco

本实验中, 仅以 Tacacs+为例。

STEP 4 配置 ACS 服务器。在 ACS 导航条中单击“Network Configuration”, 单击中间栏“AAA Clients”下的“Add Entry”按钮, 添加 AAA 的客户端, 进入 AAA 客户端添加页面, 按如图 11-3-2 所示填写。在“AAA Client IP Address”栏中填入路由器 R1 的 IP 地址 192.168.1.220; “Key”栏中输入 cisco, 这里要保证和 AAA 客户端, 也就是路由器 R1 上配置一致; “Authenticate Using”验证方式栏中选择“TACACS+ (Cisco IOS)”, 如果使用的是 Radius 协议, 这里选择“RADIUS (IETF)”。输入完成后, 单击“Submit+Restart”按钮, 完成 AAA 客户端的添加。类似操作, 再添加 AAA 客户端 R2。

图 11-3-2 添加 AAA 客户端

STEP 5 定义认证的方法。常用的认证方法及解释如表 11-3-1 所示。

表 11-3-1

常用认证方法

认证方法	解释与命令示例
enable	使用 enable 口令进行身份验证 aaa authentication login name enable
local	使用路由器本地数据库进行身份验证 aaa authentication login name local
TACACS+	使用 TATCACS+服务器进行身份验证 aaa authentication login name group tacacs+
RADIUS	使用 RADIUS 服务器进行身份验证 aaa authentication login name group radius
none	不进行身份验证 aaa authentication login name none

如表 11-3-1 所示的 name 是验证方法名, 需要调用才起作用, 如果 name 填写的是 default, 则该验证方法对所有采用默认验证方式的验证有效。还可以在一个方法列表中包含多种身份验证方式, 这样可以确保在第一种方式失效的时候, 设备可以使用备用的身份验证方式, 例如

```
aaa authentication login name group tacacs+ local
```

在上面的例子中, Cisco IOS 软件会先使用 tacacs+服务器对用户身份进行验证, 如果设备无法联系到所配置的 tacacs+服务器, 则开始尝试使用路由器本地数据库进行身份验证。

注 意



如果 TACACS+服务器可以正常联系, 但验证失败 (如 TACACS+服务器中没有这个用户名或密码不正确) 将不会尝试使用路由器本地数据库进行验证; 如果 TACACS+服务器关机或因为网络的原因, AAA Client 无法联系到 tacacs+服务器, 则使用路由器本地数据库进行验证。

路由器 R1 的认证方法配置如下:

```
R1(config)#aaa authentication login cisco group tacacs+ local
```

如果无法联系到 TACACS+服务器, 则使用路由器本地数据库进行身份验证

```
R1(config)#user admin privilege 15 pass admin
```

在路由器本地数据库中添加一个级别 15 的用户, 如果 TACACS+服务无法验证, 将使用这个用户登录。这是一个好的习惯, 使用本地数据库可以避免因网络的故障或是 ACS 服务器故障, 造成路由器不能登录

STEP 6 调用验证方法。在线路上加载认证方法列表, 使其对某个线路上的认证产生作用。步骤 5 中定义了验证方法, 因为验证方法的名字为 cisco, 不是 default, 需要在线路上调用。用户可以将不同的方法列表应用于不同的线路, 值得注意的是, 如果不特别指明, 每个线路上会使用默认方法列表 (名称为 default)。调用验证方法的格式是:

```
R1(config)#line vty 0
```

```
R1(config-line)#login authentication cisco
```

对 VTY 0 线路使用 cisco 验证方法, 也就是先使用 TACACS+, 如果联系不到 TACACS+服务器, 就使用本地用户进行验证。

STEP 7 测试。在“真实机”打开第一个 DOS 窗口，输入 telnet 192.168.1.220，提示输入用户名和密码，输入 admin 和 admin，结果失败；输入 cisco 和 cisco，成功登录路由器。如图 11-3-3 所示。出现这种现象的原因是当 TACACS+服务器可用时，不使用本地验证，使用 ACS 中的用户进行验证。读者可以禁用虚拟机 2 的网卡，在真实机进行登录测试，发现 admin 账号可以登录，cisco 账号无法登录。

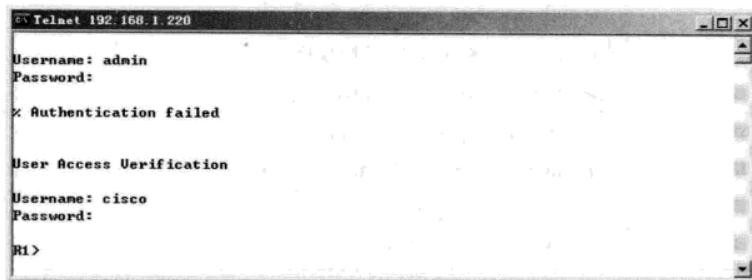


图 11-3-3 远程登录验证

特别值得一提的是，在路由器中也可以进行验证测试，测试的方法如图 11-3-4 所示。

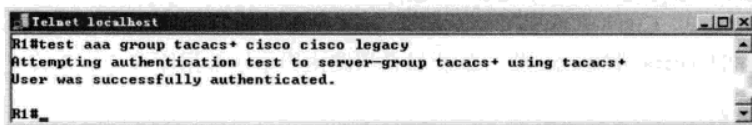


图 11-3-4 在路由器上进行 AAA 登录测试

不要关闭如图 11-3-3 所示窗口，再打开一个 DOS 窗口，输入 telnet 192.168.1.220，提示输入用户名和密码，不管输入的 admin 账号还是 cisco 账号，结果都失败。原因是 VTY 0 线路使用 cisco 方法验证，VTY 1 线路没有定义验证，使用的是 default 方法验证，但没有定义 default 方式。读者可以再定义一种新的验证方法，然后在 VTY 1 线路上进行调用测试。

同样方法，在真实机上，输入 telnet 192.168.1.230，使用 cisco 账号也可以登录。这样就实现了多个 Cisco 设备的集中管理，只需要维护 ACS 服务器上的用户账号就可以了。

这里不要关闭实验机架，继续下一节的学习。

11.4 配置 AAA 授权

根据本章某通信公司的实例，IT 部门的所有员工都可以登录路由器，并有权任意配置，如果输错命令或恶意破坏，引起网络故障，会造成不必要的损失。这时可以使用 AAA 授权，限制部分用户的权限级别；限制用户可以执行的命令。本节结合实验介绍 Cisco IOS 中 AAA 授权的配置方法，包括使用 AAA 在 Cisco IOS 中对用户的等级进行授权、使用 AAA 在 Cisco IOS 中对用户可使用的命令进行授权。

实验 11-1 使用 ACS 对用户的等级进行授权

实验 7-1 中介绍了 IOS 命令的权限级别, Cisco IOS 设备使用 3 种权限级别。当用户通过 VTY 线路登录到路由器时, 默认可以执行等级 0 和等级 1 的所有命令; 如果用户输入 `enable` 命令并且输入了正确的密码 (提示符由 `>` 改为 `#`), 则权限变为等级 15。通过使用 AAA 授权, 可以在用户登录路由器时就对用户的等级进行授权。在 Cisco IOS 中配置 AAA 授权主要步骤如下。

STEP 1 认证。具体操作见 11.3 节。

STEP 2 定义授权方法列表。

STEP 3 调用授权方法。在线路上加载授权方法列表, 使其对某个线路上的授权产生作用。

STEP 4 对用户进行授权。

在 11.3 节中, 完成了用户的认证, 当用户通过 `cisco` 或 `admin` 账号登录后, 都处于用户模式下, 如果试图输入 `enable` 进入特权模式, 路由器提示 “Error in authentication” (认证出错), 这是因为路由器上没有配置 `enable` 密码。通过使用 AAA 授权, 不需要 `enable` 密码, 也可以让用户进入到特权模式下。在 ACS 上新添加一个用户 `cisco2`, 密码也是 `cisco2`, 当该用户登录后, 该用户所在的权限级别是 2; 再新添加一个用户 `cisco15`, 密码也是 `cisco15`, 当该用户登录后, 将直接进入特权模式下。用户还可以对 Cisco CLI 的命令权限级别进行修改, 本书实验 7-1 中介绍过如何修改命令的权限级别。例如, `clear line` 命令的默认级别为 15, 但是可以使用 `privilege exec` 命令将其权限修改为级别 2。

```
R1 (config) # privilege exec level 2 clear line
```

具体的操作步骤如下。

STEP 1 配置认证。详见 11.3 节。

STEP 2 定义授权方法。

`R1(config)#aaa authorization exec vty-authorization group tacacs+ local` 定义授权方法, 该授权方法的名字为 `vtty-authorization`, 对 EXEC 命令授权, 使用 TACACS+服务器授权, 如果 TACACS+服务器失败, 将使用路由器本地数据库授权。

STEP 3 调用授权方法。

```
R1(config)#line vty 0
```

`R1(config-line)#authorization exec vty-authorization` 对 VTY 0 线路使用 `vtty-authorization` 定义的授权方法进行授权。如果定义是授权方法名字为 `default`, 这里就不需要调用了, 因为默认使用的授权方法就是 `default`

STEP 4 对用户进行授权。对用户授权分为路由器本地授权和 AAA 服务器授权, 路由器本地授权的命令格式是:

```
Username 用户名 privilege 权限级别 password 密码
```

如在路由器本地新建一个权限级别 2 的用户 `admin2`, 命令如下:

```
R1(config)#username admin2 privilege 2 password admin2
```

在 ACS 服务器中对用户授权, 首先新建用户 `cisco2`, 如图 11-4-1 所示, 选择用户所在的组, 如选择 “Group 1”, 再新建用户 `cisco15`, 选择用户所在的组, 如 “Group 2”。其次对用户所在的组进行授权, 单击左侧导航栏中的 “Group Setup”, 在中间栏的 Group 下拉列表中, 选择 Group 1, 单击 “Edit Settings” 按钮, 打开 Group Setting (组设置) 页面。

在组设置页面, 向下拖动中间栏的滚动条, 如图 11-4-2 所示修改用户的权限, 选中 “Shell(exec)”

和“Privilege level”复选框，并在“Privilege level”复选框后面的文本框中输入“2”，单击“Submit+Restart”按钮。类似的再修改 Group 2，把权限级别设成 15。

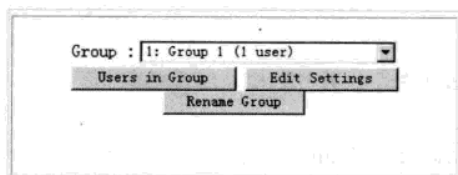


图 11-4-1 编辑组

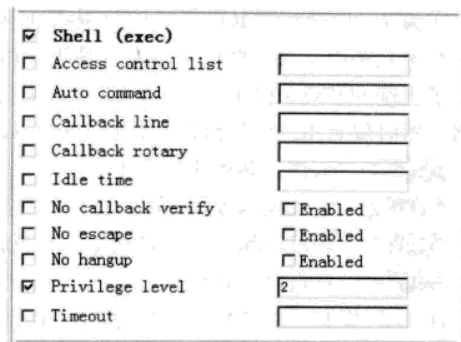


图 11-4-2 修改用户权限级别

STEP 5 测试。通过以上设置，在真实机上 telnet 192.168.1.220。使用 cisco2 账号登录，使用 show privilege 命令查看用户当前的权限级别。如图 11-4-3 所示，cisco2 账号的权限级别是 2。退出 Telnet 会话，用 cisco15 账号登录，可以发现用户的权限级别是 15。禁用虚拟机 2 的网卡，使用 admin 和 admin2 登录，分别查看用户所拥有的权限级别。

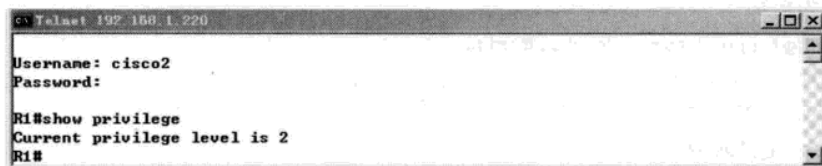


图 11-4-3 查看用户权限级别

这里也不要关闭实验机架，继续下一个实验的学习。

实验 11-2 使用 AAA 对用户可使用的命令进行授权

ACS 支持 IOS 命令的授权，它可以限制用户所能够使用的命令以及命令参数。普通管理员 cisco14（等级 15）可以执行所有的 show 命令和 clear arp（清除 ARP 缓存）命令，但无法进入配置模式对设备的配置进行修改；超级管理员 cisco15（等级 15）可以使用所有命令。操作步骤如下。

STEP 1 对用户组授权。在实验 11-1 的配置的基础上，再添加一个用户 cisco14，密码 cisco14，该用户属于 Group 3。修改 Group 3 的设置，如图 11-4-2 所示，授予 cisco14 级别 15 的权限。继续向下拖动中间栏的滚动条到“Shell Command Authorization Set”，如图 11-4-4 所示操作，选择“Per Group Command Authorization”（针对每个组进行命令授权）单选框；“Unmatched Cisco IOS commands”（不匹配的 Cisco IOS 命令）下选“Deny”单选框（表示对不匹配的命令采取拒绝动作）；选中“Command”复选框，在命令行中输入“show”，“Arguments”（参数）栏保留为空；“Unlisted arguments”（没有列出的参数）下选“Permit”单选框（表示允许执行所有的 show 命令）。单击“Submit+Restart”按钮。

继续编辑 Group 3 组的设置，向下拖动中间栏的滚动条到如图 11-4-4 所示的位置，可以发现，在 show 命令后面又多出一个“Command”选项，如图 11-4-5 所示。在命令中输入 clear，参数中填入“permit arp”，“Unlisted arguments”（没有列出的参数）下选“Deny”单选框（表示不允许 clear 执行没有列出的参数，也就是只允许执行 clear arp）。单击“Submit+Restart”按钮，完成该用户组命令的授权。

编辑 Group 2 组的设置，向下拖动中间栏的滚动条到图 11-4-4 所示的位置。按如图 11-4-6 所示填写，在“Unmatched Cisco IOS commands”（不匹配的 Cisco IOS 命令）下选“Permit”单选框（表示对不匹配的命令采取允许动作）。单击“Submit+Restart”按钮，完成该用户组命令的授权，该用户组可以执行所有命令。

Shell Command Authorization Set

☐ None

☐ Assign a Shell Command Authorization Set for any network device

☒ Per Group Command Authorization

Unmatched Cisco IOS commands

☐ Permit

☒ Deny

☒ Command:

show

Arguments:

Unlisted arguments

☒ Permit

☐ Deny

图 11-4-4 对可执行命令授权

☒ Command:

clear

Arguments:

permit arp

Unlisted arguments

☐ Permit

☒ Deny

图 11-4-5 继续添加用户可执行命令

Shell Command Authorization Set

☐ None

☐ Assign a Shell Command Authorization Set for any network device

☒ Per Group Command Authorization

Unmatched Cisco IOS commands

☒ Permit

☐ Deny

☐ Command:

Arguments:

Unlisted arguments

☐ Permit

☒ Deny

图 11-4-6 授予组执行所有命令权限

STEP 2 在 IOS 设备上配置命令授权。

R1(config)# aaa authorization commands 1 default group tacacs+ none 对级别 1 的命令进行授权，如果 TACACS+失败，对级别 1 的命令不使用授权

R1(config)# aaa authorization commands 15 default group tacacs+ none 对级别 15 的命令进行授权，如果 TACACS+失败，对级别 15 的命令不使用授权

STEP 3 测试。在真实机上 telnet 192.168.1.220, 使用 cisco14 账号登录, 如图 11-4-7 所示, 执行 clear arp 正常, 执行 clear ip route *, 提示 “Command authorization failed” (命令授权失败), 执行所有的 show 命令均可以, 执行 conf t, 再次被拒绝。当使用 cisco15 账号登录时, 可以执行所有的命令。

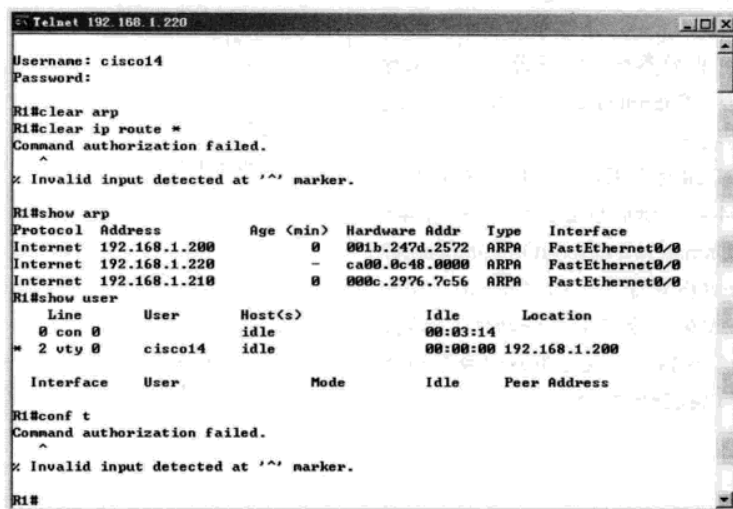


图 11-4-7 命令授权测试

不要关闭实验机架, 继续下一个实验的学习。

11.5 配置 AAA 记账

对于本章开始介绍的某通信公司实例, 虽然采用实验 11-1 和实验 11-2 的方法对用户的权限级别和用户可执行的命令进行了限制, 可毕竟高级管理员不止一个, 责任还是不够明确。通过使用 AAA 记账, 可以记录哪个用户何时执行了何命令, 很容易追踪到错误配置命令, 并帮助恢复操作, 也有助于责任到人。本节结合实验介绍 Cisco IOS 中 AAA 记账的配置方法, 包括使用 AAA 在 Cisco IOS 认证代理中对用户上网进行授权、使用 802.1x 技术实现动态 VLAN 划分、使用基于 PPPOE 的技术实现用户共享上网和认证管理。

本节将接着实验 11-2 继续介绍, 因此关于认证和授权部分的配置, 这里不再重复。

在 ACS 服务器上配置 AAA 记账, 记录管理员每次登录的时间和所使用的命令, 配置命令如下:

```

Router(config)# aaa accounting exec default start-stop group tacacs+    对用户的登录和退出进行记录
Router(config)# aaa accounting commands 1 default start-stop group tacacs+    记录级别 1 命令的执行
Router(config)# aaa accounting commands 15 default start-stop group tacacs+    记录级别 15 命令的执行
    
```

完成设置后, 在真实机上, 使用 cisco15 账号登录路由器, 执行 show ip route, clear arp, conf t,

int fa 2/0, no shut 等操作后, 退出路由器。在 ACS 的导航栏中单击“Report and Activity”, 可以看到如图 11-5-1 所示界面。

其中“TACACS + Accounting”中记录了用户登录的记录, 单击“TACACS + Accounting”, 在右侧栏中列出所有的记录文件, 默认每天产生一个日志文件, 单击“TACACS+ Accounting active.csv”打开当天的用户登录记录, 如图 11-5-2 所示。

其中“TACACS + Administration”中记录了用户曾经使用的命令记录, 单击“TACACS + Administration”, 在右侧栏中列出所有的记录文件, 默认每天产生一个日志文件, 单击“Tacacs+ Administration active.csv”打开当天的用户使用的命令记录, 如图 11-5-3 所示。

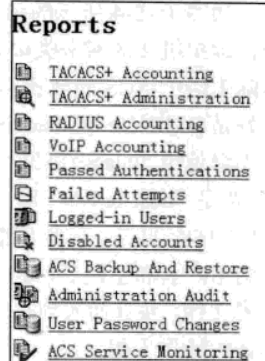


图 11-5-1 报告

实验 11-3 Cisco IOS 认证代理 (上网用户管理和计费)

认证代理是 Cisco IOS 12.3 防火墙特性集中的一个功能, 它可以在用户访问 Internet 时对用户进行认证和授权。如图 11-5-4 所示就是一个使用 IOS 的认证代理功能控制用户访问 Internet 的例子。

TACACS+ Accounting active.csv								
Date ↓	Time	User-Name	Group-Name	Caller-Id	Acct-Flags	elapsed_time	service	bytes_in
02/21/2008	22:10:46	cisco15	Group 2	192.168.1.200	stop	40	shell	..
02/21/2008	22:10:05	cisco15	Group 2	192.168.1.200	start	..	shell	..
02/21/2008	22:09:58	cisco15	Group 2	192.168.1.200	stop	33	shell	..
02/21/2008	22:09:24	cisco15	Group 2	192.168.1.200	start	..	shell	..
02/21/2008	22:07:15	cisco15	Group 2	192.168.1.200	stop	67	shell	..
02/21/2008	22:06:08	cisco15	Group 2	192.168.1.200	start	..	shell	..

图 11-5-2 用户的登录记录

Tacacs+ Administration active.csv									
Date ↓	Time	User-Name	Group-Name	cmd	priv-lvl	service	NAS-Portname	task_id	NAS-IP-Address
02/21/2008	22:10:41	cisco15	Group 2	no shutdown <cr>	15	shell	tty2	32	192.168.1.220
02/21/2008	22:10:37	cisco15	Group 2	interface FastEthernet 2/0 <cr>	15	shell	tty2	31	192.168.1.220
02/21/2008	22:10:35	cisco15	Group 2	clear arp-cache <cr>	15	shell	tty2	29	192.168.1.220
02/21/2008	22:10:34	cisco15	Group 2	configure terminal <cr>	15	shell	tty2	30	192.168.1.220
02/21/2008	22:10:08	cisco15	Group 2	show ip route <cr>	1	shell	tty2	28	192.168.1.220

图 11-5-3 用户使用的命令的记录

如图 11-5-4 所示的拓扑来自于 dynamips 中的安全机架, 虚拟机 2 的网卡类型为 Bridged, 充当 ACS 服务器, 实际生活中 ACS 的放置位置可以是内网, 也可以是外网, 最好是 DMZ(De-Militarized Zone, 隔离区或非军事化区)。路由器使用 Tacacs+ 协议与服务器通信。虚拟机 1 的网卡类型是 host-only, 网关是路由器 Fa2/0 端口的 IP 192.168.111.3, 充当内部主机, 当用户在虚拟机 1 输入正确用户名和密码后, 路由器从 ACS 上获取用户的访问配置文件, 并且加入到相应的访问控制列表中。下面列出具体的操作步骤。

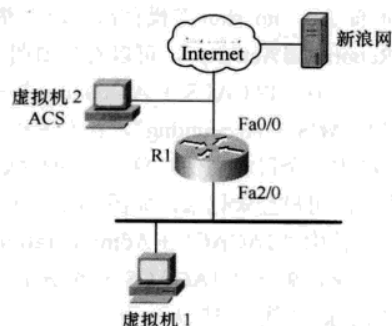


图 11-5-4 使用 IOS 认证代理控制用户访问 Internet

STEP 1 基本网络配置。配置虚拟机 1 的基本参数,

网卡类型 Host-only, IP 地址为 192.168.111.2, 子网掩码 255.255.255.0, 网关是 192.168.111.3, DNS 为 218.2.135.1。配置虚拟机 2 的基本参数, 网卡类型 Bridged, IP 地址为 192.168.1.210, 子网掩码 255.255.255.0, 网关为 192.168.1.1, DNS 是 218.2.135.1。配置路由器的接口地址, 命令如下:

```
Router>en
Router#conf t
Router(config)#host R1
R1(config)#no cdp run
R1(config)#int fa 0/0
R1(config-if)#ip add 192.168.1.220 255.255.255.0
R1(config-if)#no shut
R1(config-if)#int fa 2/0
R1(config-if)#ip add 192.168.111.3 255.255.255.0
R1(config-if)#no shut
```

STEP 2 配置 NAT (Network Address Translation, 网络地址转换)。配置 NAT, 实现内部主机通过路由器共享上网。有关 NAT 配置的说明, 请参考本书第 4 部分, 这里仅列出所需的配置, 但不要忘记配置默认路由:

```
R1(config)#int fa 0/0
R1(config-if)#ip nat outside    配置 NAT 的对外接口
R1(config-if)#int fa 2/0
R1(config-if)#ip nat inside    配置 NAT 的对内接口
R1(config-if)#exit
R1(config)#access-list 1 permit any    允许所有地址
R1(config)#ip nat inside source list 1 interface fa 0/0 overload    允许内部所有地址使用路由器 Fa0/0 端口的 IP 地址共享上网
R1(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.1    默认路由
```

配置完前两步后, 虚拟机 1 可以成功访问新浪网。接下来配置用户上网管理。

STEP 3 配置 AAA。配置认证和授权方法, 并且配置 Tacacs+服务器的参数。

```
R1(config)#aaa new-model    启用 AAA
R1(config)#aaa authentication login default group tacacs+ local    配置 AAA 认证方式, 先使用 TACACS+ 验证, 如果 TACACS+ 故障, 使用路由器本地数据库验证
```


R1(config)#aaa authorization auth-proxy default group tacacs+ 配置认证代理授权方式使用 TACACS+

R1(config)#tacacs-server host 192.168.1.210 key cisco 配置 TACACS+服务器 IP 地址和 key 参数

R1(config)#username admin privilege 15 password admin 配置路由器本地用户

STEP 4 在 ACS 上将路由器设置为 AAA client。在 ACS 导航栏中单击“Network Configuration”，在 AAA client 中单击“Add Entry”添加 AAA 客户端，前面的实验中已经添加过，可查阅本章 11.3 节的 Step 4。

STEP 5 在 ACS 上配置认证代理。在 ACS 导航栏中单击“Interface Configuration”，在中间栏中单击“Tacacs + (Cisco IOS)”进入 Tacacs + (Cisco IOS) 界面，按如图 11-5-5 所示填写。在 New Services 中添加一个新的服务，名称为“auth-proxy”，服务前面的复选框要选中，否则新添加的服务不起作用。单击“Submit”按钮，完成修改。

STEP 6 添加用户。在 ACS 中添加用户 net，密码 cisco，并且将用户分配到“Group 4”组中。

STEP 7 编辑用户组属性。在 ACS 导航栏中单击“Group Setup”，选中相应“group 4”组，单击“Edit Settings”，将滚动条拉到最底端，按如图 11-5-6 所示填写。选中 auth-proxy 和 Custom Attributes 复选框，在 Custom Attributes 的文本框中输入该组用户的授权文件。单击“Submit + Restart”提交重启路由器。

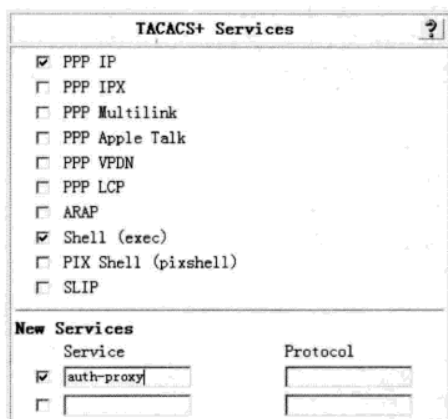


图 11-5-5 添加新的服务

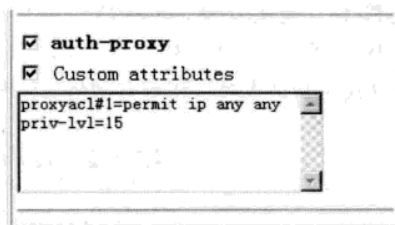


图 11-5-6 编辑用户组属性

用户授权文件其实就是将来路由器要加载的 ACL，每条语句使用 proxyacl#n 的形式来表示，并且只能包含 permit 语句。路由器下载授权文件后，它会自动将每条语句中的源地址 (any) 替换成用户的源 IP 地址。下面是对授权文件的解释：

proxyacl#1=permit ip any any 代理 ACL 的第一行，如果是第二行应该写成 proxyacl2。语句的内容是允许所有的 IP 流量，可以根据单位的实际需要设置，如只放 TCP 的 80 端口等。

priv-lvl=15 授权文件的最后一行必须以 priv-lvl=15 结尾

注意



授权文件的最后一行必须以 priv-lvl=15 结尾。

STEP 8 在路由器上定义进站访问控制列表。在路由器内网添加访问控制列表, 除访问 DNS 服务器外, 拒绝所有流量。值得注意的是, 如果 ACS 服务器放在内网, 这里要允许 ACS 的 AAA 流量进入路由器。

```
R1(config)#access-list 100 permit udp any any eq 53 允许访问 DNS 服务器的流量进入
R1(config)#access-list 100 deny ip any any 拒绝所有的 IP 流量
R1(config)#interface fa2/0 路由器连接内网的端口
R1(config-if)#ip access-group 100 in 调用访问控制列表来阻止除 DNS 外的所有 IP 流量
此时虚拟机 1 访问新浪网失败, 在路由器上使用 show access-list 检查 ACL:
```

```
R1#show access-lists
Standard IP access list 1
  10 permit any (93 matches)
Extended IP access list 100
  10 permit udp any any eq domain (6 matches)
  20 deny ip any any (13 matches)
```

STEP 9 打开路由器的 HTTP 服务。

```
R1(config)#ip http server 允许通过 Web 方式访问路由器, no ip http server 关闭该功能
```

STEP 10 配置认证代理。

```
R1(config)# access-list 2 permit 192.168.111.0 0.0.0.255 定义访问控制列表
R1(config)# ip auth-proxy name cisco http list 2 定义认证代理 cisco; 该认证代理使用的是 http 方式,
也可换成 Telnet 或 FTP 方式; 满足 ACL 2 的流量触发认证代理, 列表是可选的, 如果不挂列表, 所有 IP 地
址的 http 访问都可以触发认证代理
R1(config)# interface fa2/0 进入路由器连接内网的接口
R1(config-if)# ip auth-proxy cisco 调用认证代理 cisco
```

STEP 11 测试。在虚拟机 1 的 IE 地址栏中输入 www.sina.com.cn 后回车, IE 中会弹出图 11-5-7 所示的 Web 页面提示用户输入用户名和密码。Username 填入 net, Password 填入 cisco。弹出一个新的窗口提示验证成功, 稍后自动切换到新浪网主页。



图 11-5-7 web 认证页面

STEP 12 检查认证缓冲区中的认证记录。使用 show ip auth-proxy cache 命令可以查看缓冲区中的认证记录, 显示如下:

```
R1#show ip auth-proxy cache
Authentication Proxy Cache
Client Name net, Client IP 192.168.111.2, Port 1125, timeout 60, Time Remaining
60, state ESTAB
```

显示客户的名字为 net，客户使用的 IP 地址是 192.168.111.2，空闲超时时间设置为 60 分钟，现在还剩下 60 分钟，连接已经建立。

此时，再检查访问控制列表 100，可以发现访问控制列表 100 的最前面被添加了一条语句，允许 192.168.111.2 使用任何 IP 流量。

```
R1#show access-lists 100
Extended IP access list 100
    permit ip host 192.168.111.2 any (186 matches)
    10 permit udp any any eq domain (6 matches)
    20 deny ip any any (60 matches)
```

使用 clear ip auth-proxy cache 可以把用户清线，强制用户再次认证。

```
R1#clear ip auth-proxy cache *
```

STEP 13 完善计费。经过前面的配置，可以实现上网用户管理，没有账号的用户不能访问 Internet。但仍然存在一个问题，一个账号可以多人同时使用，读者可以再复制一台虚拟机，如虚拟机 3，网卡类型 Host-only，IP 地址 192.168.111.4，掩码 255.255.255.0，网关 192.168.111.3，DNS 为 218.2.135.1。在虚拟机 3 的 IE 地址栏中输入 www.net.cn，要求进行登录，使用 net 账号可以登录，也可以访问 Internet。

使用 show ip auth-proxy cache 可以发现两个客户端使用着同一个账号，使用 show access-list 100，可以发现两个客户端 IP 地址都被允许访问 Internet。

```
R1#show ip auth-proxy cache
Authentication Proxy Cache
Client Name net, Client IP 192.168.111.4, Port 1061, timeout 60, Time Remaining
60, state ESTAB
Client Name net, Client IP 192.168.111.2, Port 1146, timeout 60, Time Remaining
60, state ESTAB
```

```
R1#show acce
R1#show access-l
R1#show access-lists 100
Extended IP access list 100
    permit ip host 192.168.111.4 any (166 matches)
    permit ip host 192.168.111.2 any (167 matches)
    10 permit udp any any eq domain (66 matches)
    20 deny ip any any (266 matches)
```

要实现一个账号同时只能登录一次，需修改以下两点。

第一，限制一个账号只能登录一次。单击 ACS 导航栏中的“Interface Configuration”，在中间栏中单击“Advanced Options”，在高级选项中，选中“Max Session”，如图 11-5-8 所示，单击“Submit”提交。

编辑组属性, 在 ACS 导航栏中单击“Group Setup”, 选中相应“group 4”组, 单击“Edit Settings”, 将滚动条下拉到中间位置的“Max Sessions”处, 如图 11-5-9 所示填写, “Sessions available to group” (组会话数) 选择“Unlimited” (没有限制), “Sessions available to users of this group” (组中单个用户会话数) 填入“1” (组中每个用户只能有一个会话)。单击“Submit + Restart”提交重启路由器。

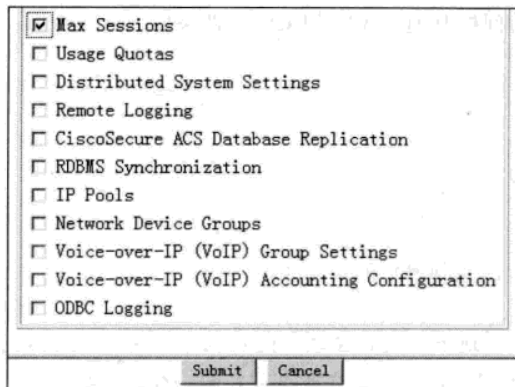


图 11-5-8 修改高级选项

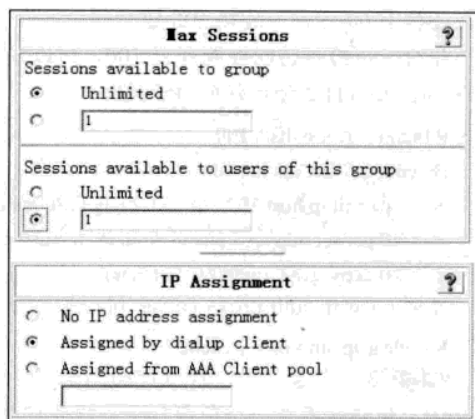


图 11-5-9 限制组中用户可以使用的会话数

第二, 启用记账。只限制组中用户会话数, 还不能限制单一账号同时只能在线一次, 还需启用记账。路由器的配置如下:

```
R1(config)#aaa accounting auth-proxy default start-stop group tacacs+
```

配置完成后, 使用 net 账号在虚拟机 1 上登录后, 在虚拟机 3 上就不能使用此账号登录, 在路由器上使用“clear ip auth-proxy cache *”清除认证缓存, 在虚拟机 3 上使用 net 账号可以登录, 但虚拟机 1 上不再能登录。管理员还可以禁用账号, 规定账号的有效期, 如图 11-5-10 所示。

至此, 完成了用户的计费工作。

STEP 14 设置相关的时间参数以及认证标志。

缓冲区中的认证记录是有空闲时间限制的, 当已认证的记录空闲时间过期后, 路由器会提示用户重新进行认证。当用户连接空闲时, 非活动计时器 (inactivity) 开始计时。如果用户在计时器超时之前有符合认证代理列表规定的流量, 则计时器复位;

如果用户在计时器超时之后建立了一个连接, 则路由器会提示用户重新进行认证。该计时器的默认值为 60 分钟。而绝对计时器 (absolute) 永远不复位, 当绝对计时器计时到期时, 用户需要重新进行认证。该计时器的默认值为 0, 即不使用该计时器。

非活动计时器和绝对计时器可以同时使用, 但是绝对计时器的值一定要大于非活动计时器的值, 否则非活动计时器永远不会产生作用。

使用 ip auth-proxy inactivity-timer min 和 ip auth-proxy absolute-timer min 命令可以对计时器的

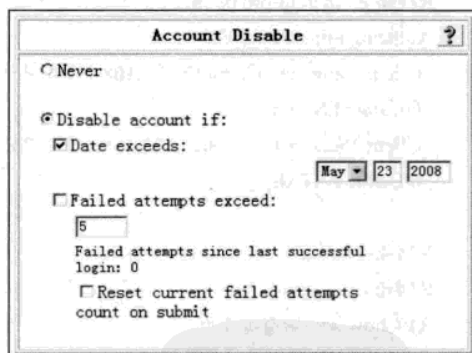


图 11-5-10 设置账号有效期

值进行修改, 例如,

```
R1 (config) # ip auth-proxy inactivity-timer 60
```

使用 `sh ip auth-proxy configuration` 命令可以查看认证代理的相关参数, 例如,

```
R1#show ip auth-proxy configuration
```

```
Authentication Proxy Banner not configured
Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication global init state time is 2 minutes
Authentication Proxy Session ratelimit is 100
Authentication Proxy Watch-list is disabled
Authentication Proxy Auditing is disabled
Max Login attempts per user is 5
```

```
Authentication Proxy Rule Configuration
```

```
Auth-proxy name cisco
```

```
http list 2 inactivity-timer 60 minutes
```

使用 `ip auth-proxy auth-proxy-banner http text` 命令可以修改认证的标志, 例如,

```
Router (config) # ip auth-proxy auth-proxy-banner http &
```

```
Pelase enter your username and password &
```

通过使用 Cisco IOS 认证代理, 实现了上网用户的管理和计费, 但还存在一点缺陷, 那就是认证记录的空闲时间设置, 如果设得太短, 用户需要经常认证; 如果设得太长, 合法用户离线后, 非法用户可以盗用合法用户的 IP 地址, 不需认证即可上网。实验 11-5 通过采用 PPPOE 认证可以有效地解决这个问题。

实验 11-4 基于 802.1x 的动态 VLAN

IEEE 802.1x 名为基于端口的访问控制协议 (Port Based Network Access Control Protocol), 它源于 IEEE 802.11 无线以太网, 也称 dot1x。该协议的认证体系结构中采用了“可控端口”和“不可控端口”的逻辑功能, 从而可以实现认证与业务的分离, 保证了网络传输的效率。用户通过认证后, 业务流和认证流分开, 对后续的数据包处理没有特殊要求。

本节介绍如何在 Catalyst 系列交换机上使用 802.1x 实现动态 VLAN 技术。当用户计算机连接到交换机后, 弹出对话框, 要求输入用户名和密码, 用户提供用户名和密码, 交换机把用户名和密码转发到 ACS 服务器上, ACS 服务器对用户身份进行验证, 如果验证通过把用户所属的 VLAN 号等信息下发到交换机, 交换机把用户计算机所连的端口划分到对应的 VLAN 中。拓扑如图 11-5-11 所示, 该实验需要在真实的交换机上完成。

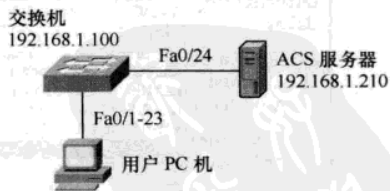


图 11-5-11 802.1x 认证

STEP 1 基本配置。配置交换 IP 地址, 创建 VLAN, 启用 AAA, 配置认证和授权。

```
switch(config)#vlan 5 在交换机上创建 vlan 5
```

```
switch(config-vlan)#vlan 10 在交换机上创建 vlan 10
```

```
switch(config-vlan)#int vlan 1  进入交换机的默认管理 VLAN
switch(config-if)#ip add 192.168.1.100 255.255.255.0  给交换机配置 IP 地址, 交换机使用此 IP 地址与
AAA 服务器通信
switch(config-if)#no shut  打开 VLAN
switch(config-if)#aaa new-model  启用 AAA
switch(config)#aaa authentication dot1x default group radius  配置 dot1x 的验证方式采用 RADIUS 服务器
switch(config)#aaa authorization network default group radius  配置网络访问的授权方式采用 RADIUS 服务器
```

STEP 2 配置 AAA 服务器参数。

```
switch(config)#radius-server host 192.168.1.210 key cisco
switch(config)#radius-server vsa send  配置动态 VLAN, 需要发送一些厂商指定属性值, 这些值是非标
准的 radius 参数, 该命令让交换机发送 VSA(Vendor-specific attributes, 厂商指定属性值)给 radius 服务器。
```

STEP 3 启动 802.1x。

```
switch(config)#dot1x system-control  全局开启 802.1x
switch(config)#interface range fa0/1 - 23  批量配置交换机端口
switch(config-if-range)#switchport mode access  把交换机端口配置成接入端口
switch(config-if-range)#dot1x port-control auto  在端口上开启 802.1x
```

STEP 4 添加 AAA 客户端。单击 ACS 导航条中的 “Network Configuration”，单击中间栏 “AAA Clients” 下的 “Add Entry” 按钮，添加 AAA 的客户端，进入 AAA 客户端添加页面，按如图 11-5-12 所示填写。在 “AAA Client IP Address” 栏中填入交换机的 IP 地址 192.168.1.100，“Key” 栏中输入 cisco，这里要保证和 AAA 客户端，也就是交换机上的配置一致，“Authenticate Using” 验证方式栏中选择 “Radius (IETF)”。输入完成后，单击 “Submit+Restart” 按钮，完成 AAA 客户端的添加。

STEP 5 修改接口配置。单击 ACS 导航条中 “Interface Configuration”，再单击中间栏中的 “RADIUS (IETF)”，进入 RADIUS (IETF) 页面，如图 11-5-13 所示。选中 “[064] Tunnel-Type”、“[065] Tunnel-Medium-Type” 和 “[081] Tunnel-Private-Group-ID” 复选框，单击 “submit” 按钮。

图 11-5-12 添加 AAA client

图 11-5-13 接口配置

STEP 6 添加用户。单击 ACS 导航条中“User Setup”，添加用户 vlan1，该用户属于“Group 5”组，再添加用户 vlan2，该用户属于“Group 6”组。

STEP 7 单击 ACS 导航条中“Group Setup”，编辑“Group 5”组的设置，在组设置页面中向下拖动滚动条到最后，如图 11-5-14 所示。将“[064] Tunnel-Type”标签 1 的值设置为“VLAN”，将“[065] Tunnel-Medium-Type”标签 1 的值设置为“802”，将“[081] Tunnel-Private-Group-ID”标签 1 的值设置为该组用户所对应的 VLAN ID，如 5。同样的方法编辑“Group 6”组的设置，把“[081] Tunnel-Private-Group-ID”标签 1 的值设置为该组用户所对应的 VLAN ID，如 10。单击“Submit + Restart”提交重启。实验中经常发现添加不成功，这里没有必要进一步探究原因，只须确认添加成功，如果没有添加成功，再重新操作一次该步骤。

STEP 8 编辑系统配置。单击 ACS 导航条中“System configuration”，再单击中间栏中的“Global Authentication Setup”，拖动“Global Authentication Setup”页面中的滚动条到最下方，如图 11-5-15 所示，清除“Allow LEAP (For Aironet only)”复选框的选取。

图 11-5-14 编辑组属性

图 11-5-15 清除“Allow LEAP”

STEP 9 测试计算机设置。目前支持 802.1x 认证的 windows 操作系统有 Windows 2000 sp4、Windows XP 和 Windows Server 2003，将计算机接到交换机端口前还需将“本地连接”的验证方式选为“MD5-质询”，如图 11-5-16 所示。

STEP 10 测试。将计算机接入到交换机上，稍后任务栏上会弹出提示框，提示输入用户名和密码，如图 11-5-17 所示。

单击该消息，弹出如图 11-5-18 所示的对话框，在对话框中输入用户名和密码，如果正确，可以在交换机上使用 show vlan 命令查看 VLAN 信息，连接交换机的端口被分配到用户所属的 VLAN 中。这里可以用 vlan1 账号登录，查看交换机上的 VLAN 配置，然后拔下网线，再次连接，用 vlan2 账号登录，再次查看交换机上的 vlan 配置。可以发现同一个交换机端口，

图 11-5-16 修改本地连接的验证方式

第一次被划入 VLAN 5，第二次被划入 VLAN 10。



图 11-5-17 任务栏提示

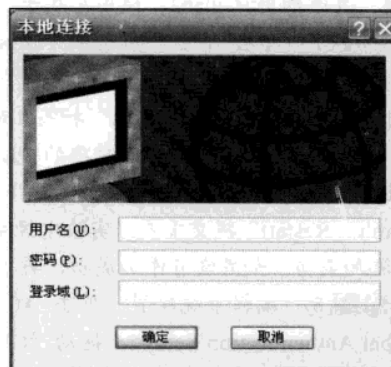


图 11-5-18 802.1x 认证对话框

如果是 Windows 2000 系统，在服务器控制台中找到“Wireless Configuration”服务，启动该服务。

实验 11-5 配置 PPPoE（电信级的用户管理和计费）

有些 ISP（Internet 服务提供商）在网上使用 PPPoE（Point to Point Protocol over Ethernet）来验证用户的计算机。这些 ISP 会向用户提供相关的软件来启动用户的计算机的 PPPoE 协议，Windows XP 和 Windows Server 2003 并不需要额外的软件来启动 PPPoE，操作系统本身已经提供了对该协议的支持。

使用 PPPoE 方式上网，用户端不需要设置 IP、掩码、网关和 DNS 等网络参数，这些参数将在拨号后自动获取，避免了 IP 冲突、网关错误等各种问题；使用 PPPoE 可以有效地控制染病毒的电脑对其他电脑和整个网络的影响；使用 PPPoE 结合 ACS 可以更加方便地对各上网用户进行更加完善的管理。

如图 11-5-19 所示的拓扑来自于 dynamips 中的安全机架，虚拟机 2 的网卡类型为 Bridged，充当 ACS 服务器，实际生活中 ACS 的放置位置可以是内网，可以是外网，最好是 DMZ（De-Militarized Zone，隔离区或非军事化区）。路由器使用 Radius 协议与服务器通信。虚拟机 1 的网卡类型是 host-only，无需配置 IP 地址，充当内部主机，用户在虚拟机 1 上进行 PPPoE 连接，输入用户名和密码后，路由器把用户名和密码转发到 ACS 服务器上身份验证，身份验证成功后，虚拟机 1 从路由器上获取 IP 地址，成功接入 Internet，虚拟机 1 断开连接后，IP 地址被释放，该方法解决了实验 11-3 中的不足。本实验较为复杂，对路由器（AAA 客户端、PPPoE 服务端、NAT 设备、DHCP 服务器）、虚拟机 2（ACS 服务器）、虚拟机 1（PPPoE 客户端）分别进行配置。

路由器的具体配置步骤如下。

STEP 1 基本网络配置。配置路由器的接口地址，命令如下，注意 Fa2/0 只需打开就可以。

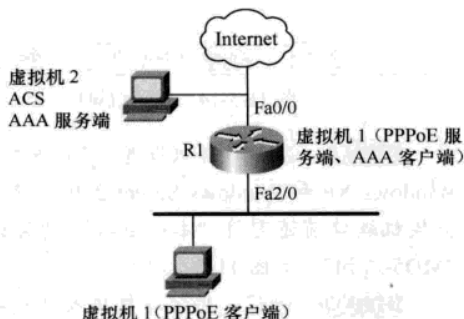


图 11-5-19 PPPoE 拓扑

```

Router>en
Router#conf t
Router(config)#host R1
R1(config)#no cdp run
R1(config)#int fa 0/0
R1(config-if)#ip add 192.168.1.220 255.255.255.0
R1(config-if)#no shut
R1(config-if)#int fa 2/0
R1(config-if)#no shut

```

STEP 2 配置 DHCP。路由器上如何配置 DHCP，本书第 4 部分给出了专门的实验，这里只给出配置和简单的解释：

```

R1(config)#ip dhcp excluded-address 10.0.0.1 在 DHCP 分配的地址中排除 10.0.0.1(虚拟接口的地址)
R1(config)#ip dhcp pool cisco 配置 DHCP 地址池，地址池的名字叫 cisco
R1(dhcp-config)#network 10.0.0.0 /24 配置用户获取的地址段
R1(dhcp-config)#dns-server 218.2.135.1 配置用户获取的 DNS

```

STEP 3 配置 AAA。路由器的配置如下：

```

R1(config)#aaa new-model 启用 AAA
R1(config)#aaa authentication ppp default group radius 对 PPP 访问使用 RADIUS 验证
R1(config)#radius-server host 192.168.1.210 key cisco 配置 RADIUS 服务器
R1(config)#aaa authorization network default group radius 对网络访问使用 RADIUS 授权
R1(config)#aaa accounting network default start-stop group radius 对网络访问使用 RADIUS 记账，记账
的目的和实验 11-3 相同，为了实现同一时刻一个账号只能被一台计算机使用。

```

STEP 4 配置 PPPoE。路由器的配置如下：

```

R1(config)#vpdn enable 启用路由器的 PPPoE 功能
R1(config)#vpdn-group 1 启用路由器的 VPDN 组 1
R1(config-vpdn)#accept-dialin 接受用户的拨入
R1(config-vpdn-acc-in)#protocol pppoe 使用 PPPoE 协议
R1(config-vpdn-acc-in)#virtual-template 1 启用虚拟接口 1
R1(config-vpdn-acc-in)#exit
R1(config-vpdn)#exit
R1(config)#int virtual-template 1 配置虚拟接口 1
R1(config-if)#ip add 10.0.0.1 255.255.255.0 配置内网使用的地址段
R1(config-if)#ppp authentication chap 使用 PPP 协议中的 CHAP 验证
R1(config-if)#peer default ip address dhcp-pool cisco 指定拨入用户的 IP 地址如何获取
R1(config-if)#int fa 2/0
R1(config-if)#pppoe enable 接内网的接口，启用 PPPOE

```

STEP 5 配置 NAT。路由器的默认路由和 NAT 配置如下：

```

R1(config)#int fa 0/0
R1(config-if)#ip nat outside
R1(config-if)#int virtual-template 1 虚拟接口 1 是 NAT 中的对内接口
R1(config-if)#ip nat inside
R1(config-if)#access-list 1 permit any
R1(config)#ip nat inside source list 1 interface fa 0/0 overload
R1(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.1

```

虚拟机 2 的具体配置步骤如下。

STEP 1 虚拟机 2 的基本参数。网卡类型 Bridged, IP 地址 192.168.1.210, 子网掩码 255.255.255.0, 网关为 192.168.1.1, DNS 是 218.2.135.1。

STEP 2 添加 AAA Client。修改客户端 192.168.1.220, 验证协议使用的是“RADIUS(IETF)”。

STEP 3 添加用户。添加 ppp1 用户, 该用户属于“Group 7”组。

STEP 4 修改组属性。如图 11-5-9 所示进行操作, 把“Group 7”组中的用户会话数限制为 1。

虚拟机 1 的具体配置步骤如下。

STEP 1 配置虚拟机 1 的基本参数。IP 地址随便配置或者自动获取。

STEP 2 新建连接。在虚拟机 1 的“网络连接”窗口中, 如图 11-5-20 所示, 双击“新建连接向导”图标, 打开“新建连接向导”对话框。

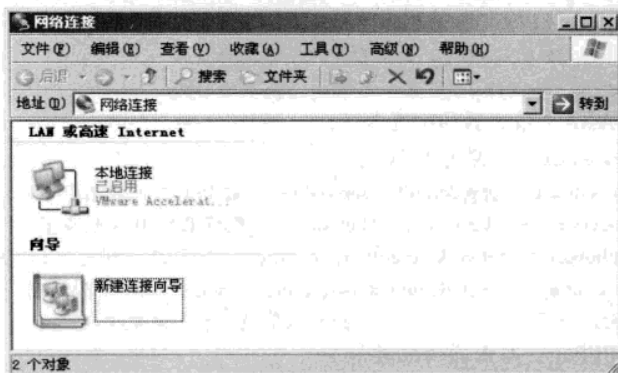


图 11-5-20 网络连接

STEP 3 网络连接类型。在网络连接类型中选择“连接到 Internet”, 如图 11-5-21 所示, 单击“下一步”按钮继续。

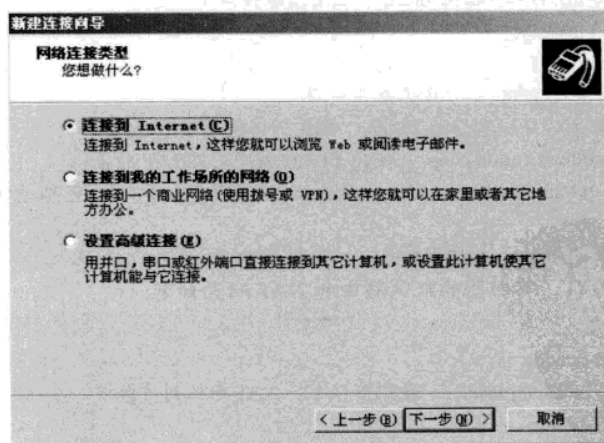


图 11-5-21 网络连接类型

STEP 4 网络连接方式。新建连接向导询问怎样连接到 Internet, 选择第二个选项“用要求

用户名和密码的宽带连接来连接”，如图 11-5-22 所示。单击“下一步”按钮继续。

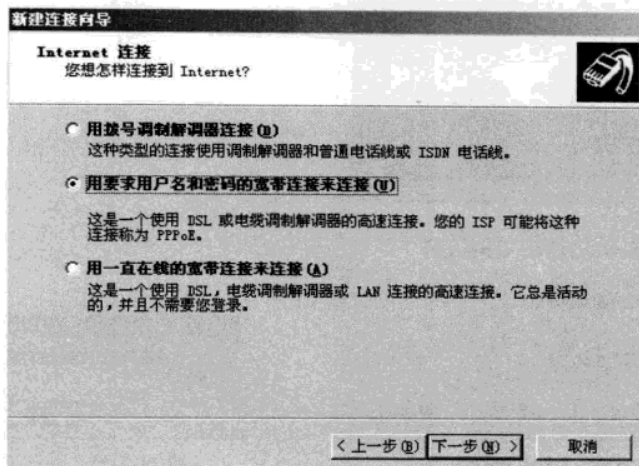


图 11-5-22 网络连接方式

STEP 5 ISP 的名称。随意填入一个名称，如“pppoe”，单击“下一步”按钮继续。

STEP 6 账户信息。在账户信息中输入 ACS 服务器的用户名 pppl 和对应的密码，如图 11-5-23 所示。单击“下一步”按钮继续，完成 PPPoE 客户端的设置。

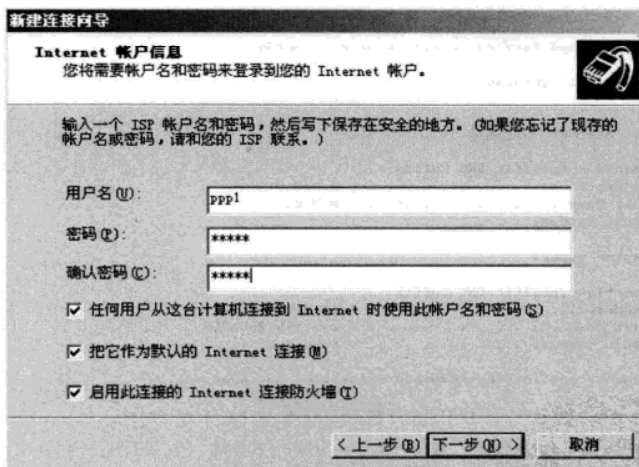


图 11-5-23 PPPoE 客户端信息

下面进行测试。

双击虚拟机 1“网络连接”窗口中新建的“pppoe”连接，打开“连接 pppoe”窗口，如图 11-5-24 所示。

单击“连接”按钮，屏幕提示“正在核对用户名和密码”，用户名和密码验证通过后，又提示“正在网络上注册您的计算机”，如图 11-5-25 所示。



图 11-5-24 连接 pppoe

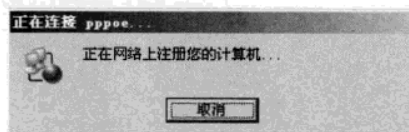


图 11-5-25 注册 PPPoE 客户端

注册成功后，“网络连接”窗口中的“pppoe”连接变亮，在 DOS 窗口中查看虚拟机 1 的 IP 地址，如图 11-5-26 所示。这时可以看出虚拟机 1 中新增出了一块“PPP”网卡，该网卡的 IP 地址是“10.0.0.2”，掩码是“255.255.255.255”，这样的子网掩码可以有效地防止局域网内的攻击，虚拟机 1 可以 ping 通南京工业大学 WWW 服务器，并能正常使用其他网络服务。

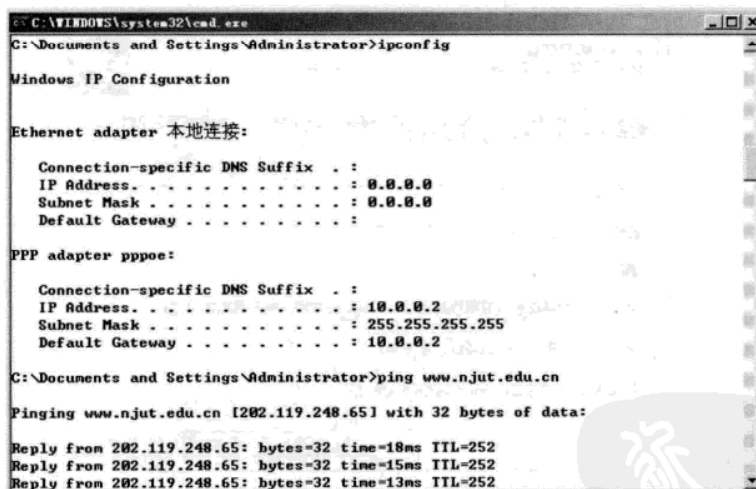


图 11-5-26 PPPoE 客户端测试

不要断开虚拟机 1 的 PPPoE 连接，在虚拟机 3 也建立同样的连接，双击进行连接，系统提示“连接到 pppoe 时出错”，如图 11-5-27 所示。因 ppp1 账户当前正在使用，在虚拟机 1 上，右键单击“网络连接”窗口中的“pppoe”连接，选择“断开”，在虚拟机 3 上，再次测试连接，连接成功。

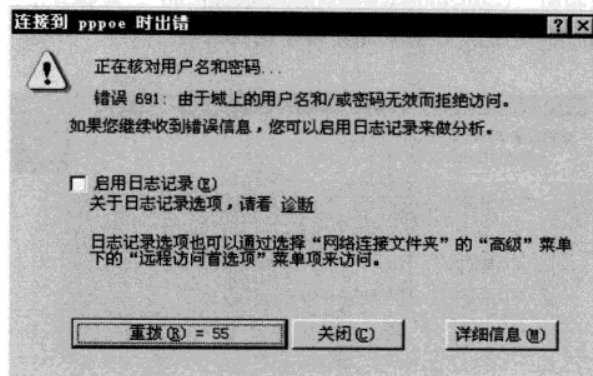


图 11-5-27 连接 PPPoE 时出错

使用 PPPoE 结合 ACS，省去了客户端 IP 地址的配置，很好地实现了用户的身份验证，上网用户的管理、计费（比较适合根据日期，如果想根据流量或上网时长来计费，需要二次开发）和网络安全等。

11.6 ACS 中用户密码的修改

通过前面的介绍，相信对 ACS 都有了一定的了解，尤其 PPPoE 结合 ACS 进行上网用户管理和计费，既方便又实用。在 ACS 中用户如何修改自己的密码呢？这些工作如果由管理员一个人来完成，将给用户和管理员都带来非常大的麻烦。一些流行的计费软件都允许客户远程修改自己的密码，ACS 中也提供了这一功能。

UCP (User changeable Password, 用户改变密码) 是 ACS 的一个配套工具，它可以允许用户通过 Web 页面修改自己账号对应的密码。UCP 可以安装在运行 IIS 的 Windows 服务器上（包括 Windows 2000 和 Windows 2003）。UCP 服务器可以和 ACS 安装在不同的服务器上，如果安装在不同的服务器上设置相对繁琐，这里把 UCP 和 ACS 安装在同一台服务器（虚拟机 2）上，如想安装在不同的服务器上，可以参阅 ACS3.3 文件夹中的“ACS Utilities\User Changeable Password\ucp33.pdf”帮助文件。下面介绍 UCP 安装的主要步骤。

STEP 1 安装 IIS 服务器。使用本书第 5 章介绍的方法，在虚拟机 2 上添加“Internet 信息服务 (IIS)”。

STEP 2 新建两个文件夹。在“C:\inetpub\wwwroot”文件夹下新建两个文件夹“secure”（UCP 的 HTML 文件默认被安装到这个目录下）和“securecgi-bin”（UCP 使用的 CGI 文件将被安装到这个目录下）。

STEP 3 新建虚拟目录。在“Internet 信息服务 (IIS) 管理器”中，右键单击“默认网站”命令，在快捷菜单中选择“新建”→“虚拟目录”，在“虚拟目录创建向导”对话框中填入别名“secure”，路径指向“C:\inetpub\wwwroot\secure”，虚拟目录访问权限是“读取”，如图 11-6-1 所示。单击“下一步”按钮，完成虚拟目录的添加。同样的方法再新建一个虚拟目录，别名

“securecgi-bin”，路径指向“C:\inetpub\wwwroot\securecgi-bin”，虚拟目录访问权限是“执行（如 ISAPI 应用程序或 CGI）”，也就是如图 11-6-1 所示的第三项。

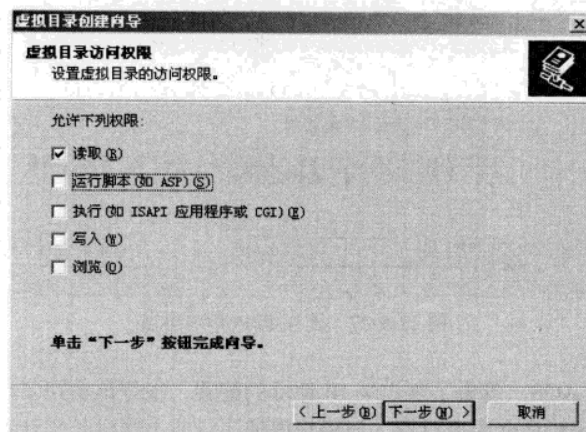


图 11-6-1 设置虚拟目录访问权限

STEP 4 在 IIS 中允许执行未知的 CGI 扩展。单击“Web 服务扩展”，将“所有未知 CGI 扩展”设置为“允许”，如图 11-6-2 所示。

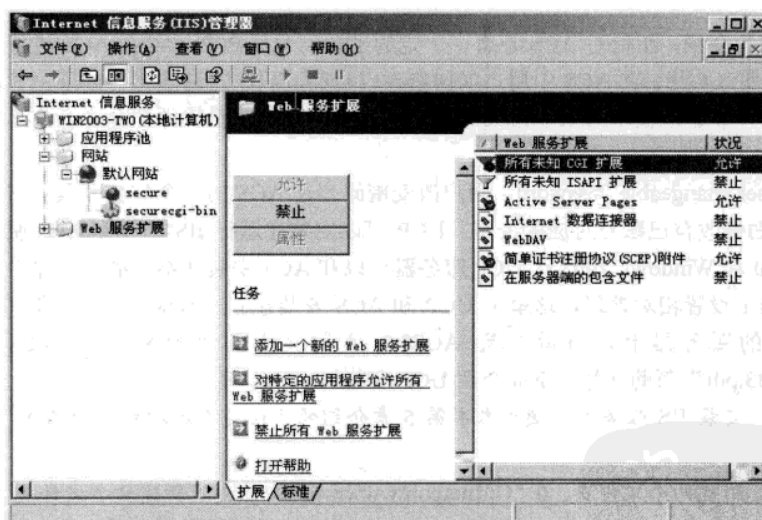


图 11-6-2 允许执行 CGI 扩展

STEP 5 配置 SSL 通信（可选）。为了保证通信安全，Cisco 建议用户在 UCP 服务器上开启 SSL 通信，感兴趣的用户可以参阅本书的 5.9.4 小节。

STEP 6 安装 UCP。打开 ACS3.3 文件夹中的“\ACS Utilities\User Changeable Password”目录，双击“setup.exe”进行安装，弹出如图 11-6-3 所示的对话框，当所有条件都满足时，才可以

单击“Next”按钮。

各选项的内容含义如下。

● 第一条：ACS 服务器必须正在运行，并且可以到达。这里满足，因为虚拟机 2 上的 ACS 正在运行，UCP 和 ACS 安装在同一台服务器上，也满足可达。

● 第二条：安装 UCP 计算机的 IP 地址“192.168.1.210”必须出现在 ACS 的“AAA Server”中，UCP 和 ACS 在同一台服务器上，“192.168.1.210”已经出现在 ACS 的“AAA Server”中，这一条也满足。

● 第三条：Web 服务器已经安装，最好运行 SSL。前面已经安装了 IIS 服务，SSL 是可选配置，这一条也满足。

● 第四条：Web 服务器上要有一个可以执行的虚拟目录，一些脚本文件将被复制到此虚拟目录中。前面已经创建过“securecgi-bin”虚拟目录。这一条也满足。

● 第五条：Web 服务器上要有一个可以读取的虚拟目录，一些 HTML 文件将被复制到此虚拟目录中。前面已经创建过“secure”虚拟目录。这一条也满足。

选中如图 11-6-3 所示的所有复选框，单击“Next”按钮开始安装 UCP。如果没有使用 SSL，接下去的所有对话框中均保持默认设置，直至单击“Finish”按钮，完成 UCP 的安装。如果启用了 SSL，需要把其中的“https://10.1.1.3/secure”更换成“https://10.1.1.3/secure”，其他步骤保持不变。

STEP 7 测试 UCP。完成所有设置后，在真实机的 IE 地址栏中输入“https://192.168.1.210/secure/login.htm”，打开如图 11-6-4 所示的页面。

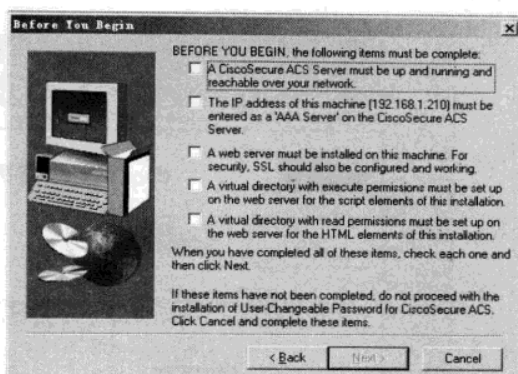


图 11-6-3 安装 UCP 的前提条件



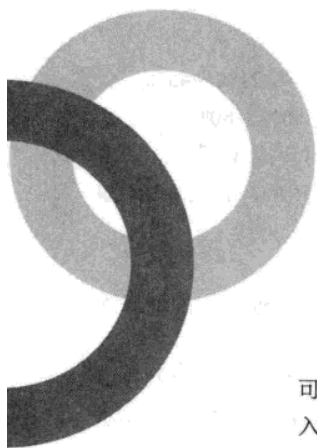
图 11-6-4 UCP 登录界面

输入正确的用户名和密码以后，如创建的 ppp1 用户和对应的密码，单击“login”，打开如图 11-6-5 所示的页面，填入对应的密码，单击“Submit”按钮完成密码的修改。



图 11-6-5 修改 ACS 用户密码

用户可以用网页编辑软件编辑“securecgi-bin”和“secure”文件夹中的 HTML 文件来美化页面。



第 12 章 VPN（虚拟专用网）

Chapter 12

本章介绍了 VPN 基础知识和 IPSec VPN 的技术原理与实现，通过学习本章，读者可以了解 VPN 的优点和实现原理，以便在工程中正确配置站点到站点 VPN 和远程接入 VPN 来提供对远程办公场所的访问，同时保护用户数据的安全。

12.1 VPN 基础知识

虚拟专用网（VPN）被定义为通过一个公用网络（通常是 Internet）建立一个临时的、安全的连接，是一条穿过混乱的公用网络的安全、稳定的隧道。虚拟专用网是对企业内部网的扩展。虚拟专用网可以帮助远程用户、公司分支机构、商业伙伴及供应商同公司的内部网建立可信的安全连接，并保证数据的安全传输。虚拟专用网可用于不断增长的移动用户的全球 Internet 接入，以实现安全连接；可用于实现企业网站之间安全通信的虚拟专用线路，用于经济有效地连接到商业伙伴和用户的安全虚拟专用网。

目前，用于企业内部自建 VPN 的主要有两种技术——IPSec VPN 和 SSL VPN。IPSec VPN 和 SSL VPN 主要解决的是基于互联网的远程接入和互联，适用于需要安全但又对价格敏感的用户。本书仅介绍 IPSec VPN，如图 12-1-1 所示描述了一个典型的 VPN 环境。公司的分支办公室和移动用户或家庭用户通过公有网络（Internet）与公司总部的服务器建立连接。VPN 与传统的使用专线或帧中继连接的网络相比，其最大的好处就是降低了成本，增强了灵活性。

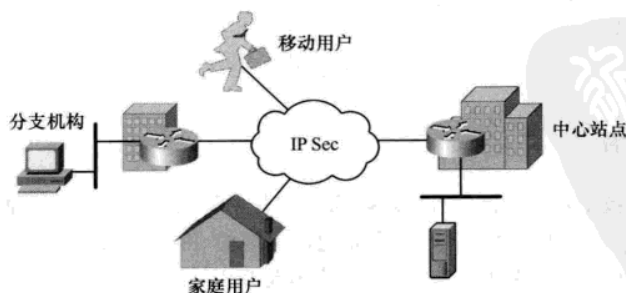


图 12-1-1 使用 VPN 进行连接的网络

12.1.1 VPN 优点

VPN 解决方案具有如下优点。

(1) 经济性。如果企业放弃租用专线而采用 VPN，其整个网络的成本可节省 21%~45%，至于采用以电话拨号方式连网存取数据的公司，采用 VPN 则可以节约通信成本 50%~80%。

(2) 伸缩性。能够随着网络的扩张，很灵活地加以扩展。当增加新的用户或子网时，只需修改已有网络软件配置，在新增客户机或网关上安装相应软件并接入 Internet 后，新的 VPN 即可工作。

(3) 安全性。VPN 可以验证用户的身份并实现收发数据的机密性与完整性。

(4) 灵活性。除了能够方便地将新的子网扩展到企业的局域网之外，由于 Internet 的全球连通性，VPN 可以使企业随时安全地将信息存取到全球的商贸伙伴和客户。

(5) 易于管理。用专线将企业的各个子网连接起来时，随着子网数量的增加，需要的专线数以几何级数增长。而使用 VPN 时 Internet 的作用类似一个 Hub，只需要将各个子网接入 Internet 即可，不需要为每个连接申请专用线路。

12.1.2 IPSec VPN 分类

基于 IPSec VPN 的网络大致上可以分为两大类：站点到站点 VPN 和远程访问 VPN。

1. 站点到站点 VPN

站点到站点 VPN 面向的对象是端对端网络，例如，公司总部与分支办公室的连接，这种连接以往都是通过专线或帧中继来完成的。站点到站点 VPN 相对与传统的专线连接相比，具有很大的价格优势。如图 12-1-2 所示就是一个使用 VPN 进行站点到站点连接的拓扑图。

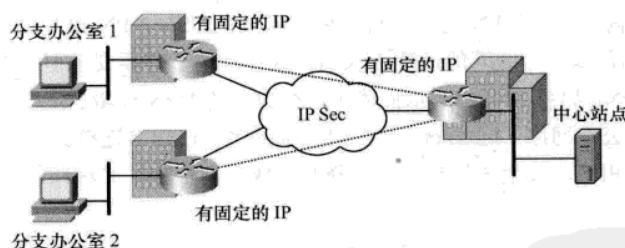


图 12-1-2 站点到站点 VPN 拓扑

2. 远程访问 VPN

远程访问 VPN 技术是拨号网络技术的革新，它是为移动办公用户提供服务的。如图 12-1-3 所示，移动用户或家庭用户以及远程办公室先通过本地的 ISP 接入 Internet 连接，然后在通过 Internet 安全地接入到公司网络中，它们的共同点就是都没有固定的 IP 地址，只有中心站点有固定的 IP 地址。

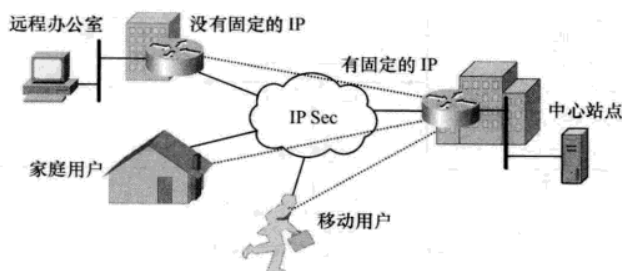


图 12-1-3 远程访问 VPN 拓扑

12.2 IPSec (IP 安全)

IPSec (IP Security, IP 安全) 产生于 IPv6 的制定之中, 用于提供 IP 层的安全性保障。由于所有支持 TCP/IP 的主机进行通信时, 都要经过 IP 层的处理, 所以提供了 IP 层的安全机制就相当于为整个网络提供了安全通信的基础。鉴于 IPv4 的应用仍然很广泛, 所以在 IPSec 的制定中也增添了对 IPv4 的支持。

IPSec 是一个公开标准的框架, 它工作于网络层, 用于保护和鉴别 IPSec 对等体之间的数据包。本节将对 IPSec 的功能、传输模式、涉及的相关协议进行介绍。

12.2.1 IPSec 功能

IPSec 提供的保护功能有数据机密性、数据完整性、起源认证和防重放保护等。

1. 数据机密性

数据机密性的定义是数据发送方使用数学方法对数据进行加密, 使数据在传输过程中变得不可读; 数据接收方对接收到的数据使用一定的算法对其进行解密, 最后将数据还原成原来的样子。

(1) 加密算法。加密算法大致上可以分为两类: 对称式加密和非对称式加密。对称式加密是指发送方和接收方使用相同的密钥来加密和解密数据; 非对称式加密是指发送方和接收方使用不同的密钥来加密和解密数据。

对称式加密算法有 DES、3DES 和 AES。其中, DES 使用 56 位密钥进行加密; 3DES 是 DES 算法的变种, 它使用 3 个独立的 56 位密钥对数据进行加密; AES 是最新的加密标准, 它使用 128 位密钥进行加密。从加密的强壮程度上讲, 3DES 优于 DES, AES 优于 3DES。如图 12-2-1 所示描述了对称式加密和解密的过程, 发送方使用密钥加密, 接收方使用同样的密码进行解密。因加密和解密使用的密钥相同, 所以要保证密钥的安全, 如果密钥泄露出去, 加密就失去意义了, 对称式加密一般用于对数据内容的加密。

非对称式加密算法有 RSA。如图 12-2-2 所示描述了非对称式加密的过程, 发送方和接收方各生成两个密钥——私钥和公钥, 并且将公钥发送给对方 (私钥自己保留)。发送方在发送数据时使用接收方的公钥进行加密, 接收方使用自己的私钥进行解密。由于公钥和私钥成对出现, 只有使

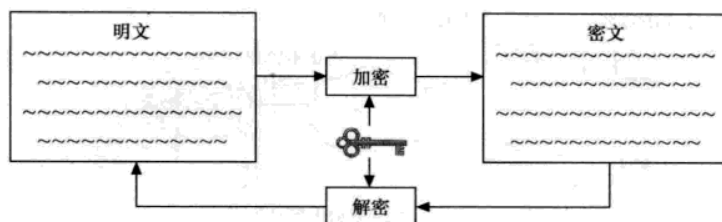


图 12-2-1 对称式加密算法

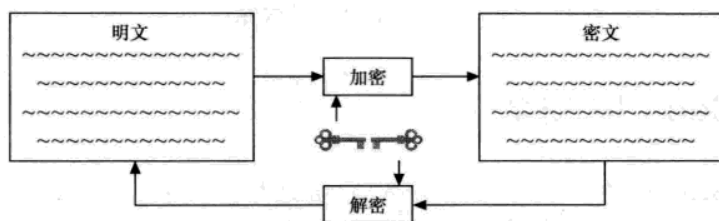


图 12-2-2 非对称式加密算法

用对应的私钥才能解密公钥对数据的加密，因此整个通信过程是安全的。因公钥是要发布出去的，所有人都可能获得，为了保证不能从公钥破解出私钥，这就要求公钥要有一定的长度来保证复杂性，所以 RSA 算法的运行效率不高，IPSec 不使用 RSA 进行数据内容加密，一般用于数字签名和密钥本身的交换。

(2) DH 密钥交换。无论是 DES、3DES、AES 还是 RSA，它们都需要使用密钥，这就引出一个问题，IPSec 对等体如何生成密钥呢？

DH (Diffie-Hellman, 发明此算法的两个人名) 密钥交换可以为对等体生成加密所需的密钥，它的算法也因强壮程度不同分为 DH 组 1、DH 组 2、DH 组 5 和 DH 组 7。如图 12-2-3 所示描述了 DH 的简要过程。

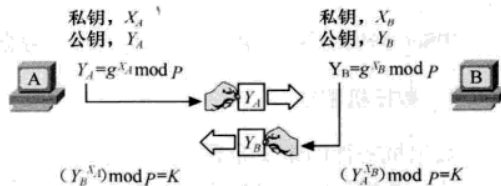


图 12-2-3 DH 过程

DH 算法比较复杂，除非进行理论研究，读者没必要了解详细过程。大致的过程是用户 A 和 B 产生各自的私钥和公钥，并且互相交换公钥，然后用自己的私钥和对方的公钥进行计算，最终算出相同的共享密钥。

2. 数据完整性

数据完整性用于保证数据在传输过程中不被修改。如图 12-2-4 所示，发送方在发送数据时，为消息附加了一个 Hash 值 1。该 Hash 值 1 是消息源文和共享密钥经过 Hash 算法 (也称散列算法) 得出的一个值，Hash 算法本身的不可逆性保证了中间接收者很难根据 Hash 值 1 算出共享密钥。接收方在接收数据时重新计算消息的 Hash 值 2，如果计算出的 Hash 值 2 和消息中附加的 Hash 值 1 一样，则说明数据没有被篡改。

Hash 算法使用共享密钥将不同长度的消息转换成固定长度的字符串，其运算过程是不可逆的，也就是说 Hash 值是无法被还原成消息的。Hash 值是附加在消息中发送的，如果消息在传输过程中被修改，接收方重新计算的 Hash 值和消息中原本附加的 Hash 值就无法匹配。

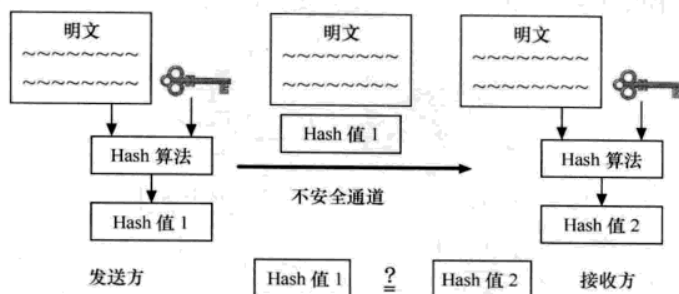


图 12-2-4 数据完整性检查

目前有两种通用的散列算法：HMAC-MD5 和 HMAC-SHA-1。其中 HMAC-MD5 使用 128 位共享密钥进行散列计算，而 HMAC-SHA-1 使用 160 位共享密钥进行散列计算。HMAC-SHA-1 更安全，但占用的资源相对也多。

注意



单纯使用数据完整性检查只能识别数据有没有被篡改，并能保证数据不泄密，在图 12-2-4 所示中可以看到，发送的数据仍然是明文。

3. 起源认证

起源认证是指对数据发送者的身份进行识别，目前主要有两种方法：预共享密钥和 RSA 签名。

(1) 预共享密钥。预共享密钥是指在 IPSec 对等体上预先设置好相同的密钥，当它们进行认证时，发送方将预共享密钥和身份信息进行散列计算，然后将计算出的散列发送给接收方；接收方对收到的消息进行散列处理，如果能生成相同的散列，则发送方被验证。预共享密钥比较容易配置，但是扩展性很不好，仅使用于小型 VPN 网络。

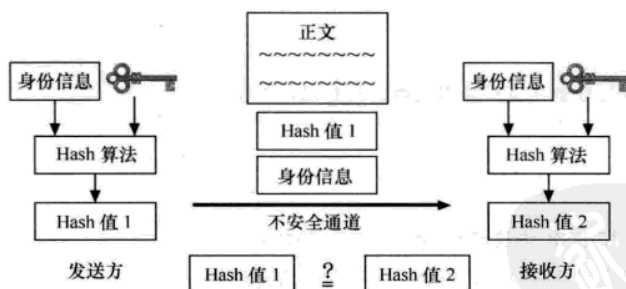
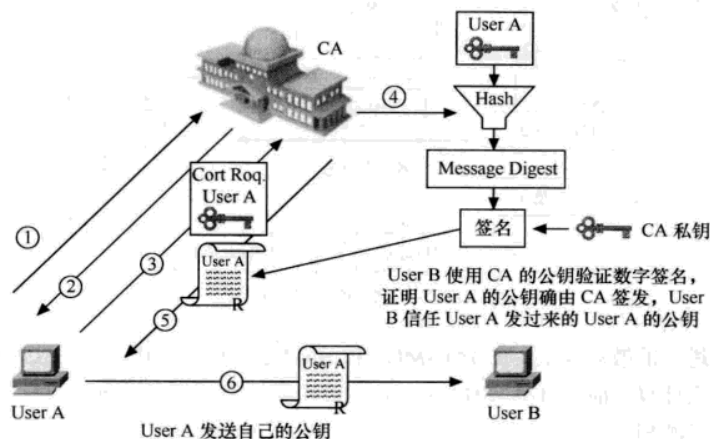


图 12-2-5 预共享密钥验证起源

(2) RSA 签名。RSA 签名的过程和 RSA 数据加密的过程恰好相反。发送方使用自己的私钥对身份信息进行加密，形成签名，接收方使用发送方的公钥对签名进行解密，将解密得到的身份信息与发送过来的明文身份信息进行比较，如果一致，则签名被确认。

实现 RSA 签名时，需要用到 CA 服务器，本书的第 5 章已经介绍过证书服务。CA 用于存储

数字证书和证明证书的可靠性, 如图 12-2-6 所示描述了证书使用的过程, 具体步骤如下。



- STEP 1** 用户 A 向 CA 请求根证书, 也就是 CA 的公钥。
- STEP 2** CA 把自己的公钥发送给用户 A。
- STEP 3** 用户 A 生成一对密钥: 公钥和私钥。用户 A 把公钥发送到 CA 服务器。请求 CA 签名, 相当于是获得 CA 的认可。
- STEP 4** CA 使用自己的私钥对用户 A 发过来的用户 A 的公钥进行签名, 相当于认可用户 A 的身份。
- STEP 5** CA 把用自己私钥签名过的用户 A 的公钥发给用户 A。
- STEP 6** 用户 A 把获得 CA 签名后的公钥发送给用户 B。用户 B 如何鉴别这就是用户 A 的公钥, 不是别人冒充用户 A 发过来的呢? 因为用户 B 也信任根 CA, 用户 B 使用 CA 的公钥对用户 A 发过来的公钥验证数字签名, 因该公钥被 CA 使用私钥签名过, 用户 B 验证了用户 A 的公钥是自己信任的 CA 签名的, 用户 B 信任用户 A 的公钥。

注意



单纯使用起源认证只能识别数据的起源, 并能保证数据不泄密和没有被修改。

4. 防重放保护

后面要提到 AH 和 ESP 协议都包含一个 32 位的序列数, IPSec 通过比较目标主机上的滑动窗口和接收到的数据包中的序列数来辨别数据包是否是被复制的, 这样就可以防止攻击者截取 IPSec 数据包后又将它们重新插入会话。

12.2.2 IPSec 工作模式

IPSec 可以使用两种模式来传输 IP 数据包: 传输模式 (Transport Mode) 和隧道模式 (Tunnel Mode)。如图 12-2-7 所示, 对比了两种传输模式的主要区别。

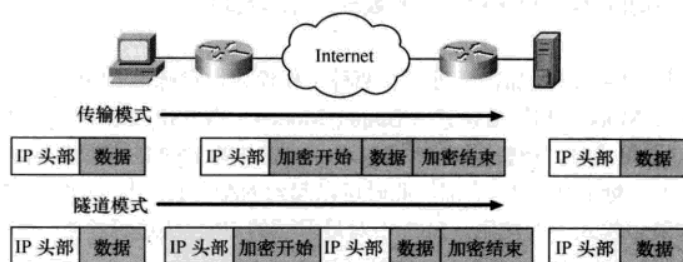


图 12-2-7 传输模式和隧道模式

如图 12-2-7 所示, 传输模式主要用于端到端的连接, 它使用原始 IP 包头中的地址进行寻址。传输过程中, 源和目标 IP 地址不发生改变。如图 12-2-7 所示, 如果客户机和服务器都有公网 IP 地址, 可以使用传输模式, 当然也可以使用隧道模式。

隧道模式一般用于两个安全网关 (如路由器) 之间的连接, 它通过将新的 IP 包头添加到原始 IP 包头之前来实现 IP-in-IP 的封装。原始 IP 包头在隧道中传输的时候被保留, 直到隧道终端删除附加包头时才使用。如图 12-2-7 所示, 如果客户机和服务器都没有公网 IP 地址, 只能使用隧道模式。

12.2.3 IPsec 相关协议

前面已经提到 IPsec 主要功能为加密和认证, 为了进行加密和认证 IPsec 还需要有密钥的管理和交换的功能, 以便为加密和认证提供所需要的密钥并对密钥的使用进行管理。这 3 方面的工作分别由 AH、ESP 和 IKE 3 个协议规定。为了介绍这 3 个协议, 需要先引入一个非常重要的术语 SA (Security Association, 安全关联)。所谓安全关联是指安全服务与它服务的载体之间的一个“连接”。AH 和 ESP 都需要使用 SA, 而 IKE 的主要功能就是 SA 的建立和维护。只要实现 AH 和 ESP 都必须提供对 SA 的支持。

通信双方如果要用 IPsec 建立一条安全的传输通路, 需要事先协商好将要采用的安全策略, 包括使用的加密算法、密钥、密钥的生存期等。当双方协商好使用的安全策略后, 就说明双方建立了一个 SA。SA 就是能向其上的数据传输提供某种 IPsec 安全保障的一个简单连接, 可以由 AH 或 ESP 提供。当给定了一个 SA, 就确定了 IPsec 要执行的处理, 如加密、认证等。

1. ESP (Encapsulating Security Payload, 封装安全负载)

ESP 主要用来处理对 IP 数据包的加密, 此外对数据完整性认证、提供起源认证和防重放保护也提供某种程度的支持。ESP 是与具体的加密算法相独立的, 几乎可以支持各种对称密钥加密算法, 如 DES、3DES、AES 等。ESP 协议数据单元格式由 3 个部分组成, 除了头部、加密数据部分外, 在实施认证时还包含一个可选尾部。头部有两个域: 安全策略索引 (SPI) 和序列号 (Sequence Number)。使用 ESP 进行安全通信之前, 通信双方需要先协商好一组将要采用的加密策略, 包括使用的算法、密钥以及密钥的有效期等。“安全策略索引”用来标识发送方是使用哪组加密策略来处理 IP 数据包的, 当接收方看到了这个序号就知道了对收到的 IP 数据包应该如何处理。“序列号”用来区分使用同一组加密策略的不同数据包。加密数据部分除了包含原 IP

数据包的有效负载和填充域（用来保证加密数据部分满足块加密的长度要求）外其余部分在传输时都是加密的。

前面已经提到用 IPSec 进行加密是可以有两种工作模式，意味着 ESP 协议有两种工作模式：传输模式（Transport Mode）和隧道模式（Tunnel Mode）。当 ESP 工作在传输模式时，采用当前的 IP 头部。而在隧道模式时，把整个 IP 数据包进行加密作为 ESP 的有效负载，并在 ESP 头部前增添以网关地址为源地址的新的 IP 头部，此时可以起到 NAT 的作用。如图 12-2-8 所示，对比了 ESP 有传输模式和隧道模式中的使用。ESP 不对最前面的 IP 包头进行检查。因此即使在 ESP 封装之后对数据包进行 NAT，也不会对 ESP 的认证造成影响。

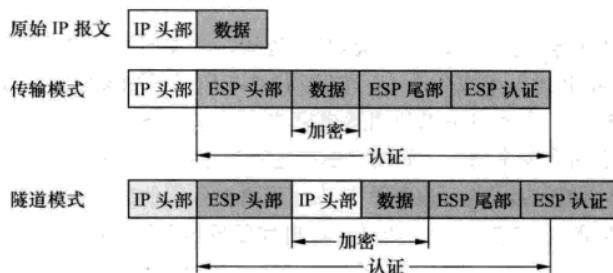


图 12-2-8 传输模式和隧道模式中的 ESP

2. AH（Authentication Header，验证头部）

AH 可以确保数据完整性、提供起源认证和防重放保护，但是 AH 不提供数据机密功能。AH 虽然在功能上和 ESP 有些重复，但 AH 除了可以对 IP 的有效负载进行认证外，还可以对 IP 头部实施认证。主要是处理数据时，可以对 IP 头部进行认证，而 ESP 的认证功能主要是面对 IP 的有效负载。AH 既可以单独使用，也可和 ESP 联用。如图 12-2-9 所示，AH 对整个数据包进行验证，因此如果网络中存在 NAT 的话，应在 AH 封装之前使用 NAT，否则 AH 验证将无法通过。AH 支持 HMAC-MD5 和 HMAC-SHA-1 算法。

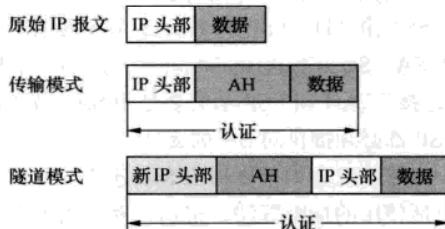


图 12-2-9 传输模式和隧道模式中的 AH

3. IKE（Internet Key Exchange，Internet 密钥交换）

IKE 协议主要是对密钥交换进行管理，它主要包括 3 个功能：对使用的协议、加密算法和密钥进行协商。

12.3 IPSec 操作过程

本节讲述站点到站点 IPSec VPN 配置的过程，站点到站点 IPSec VPN 的操作过程如图 12-3-1 所示，可以分为以下 5 步：定义感兴趣流、IKE 阶段 1、IKE 阶段 2、数据传输和隧道终止。

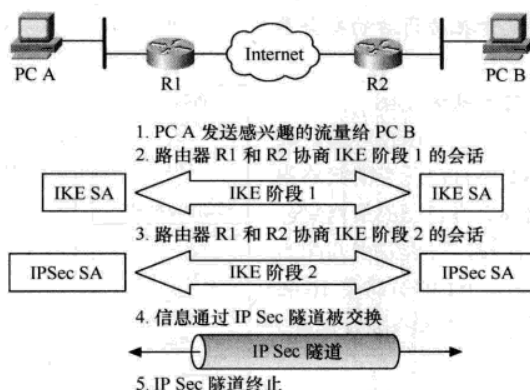


图 12-3-1 IPSec VPN 操作过程

STEP 1 定义感兴趣的流量。配置 VPN 的第一步就是指定哪些流量需要使用 IPsec 来保护，Cisco 路由器和防火墙使用 ACL 来标识这部分流量。

如图 12-3-2 所示，路由器 R1 使用 ACL 来检查流量是否感兴趣，ACL 如下：

```
R1(config)#access-list 100 permit ip 10.0.1.0 0.0.0.255 10.0.2.0 0.0.0.255
```

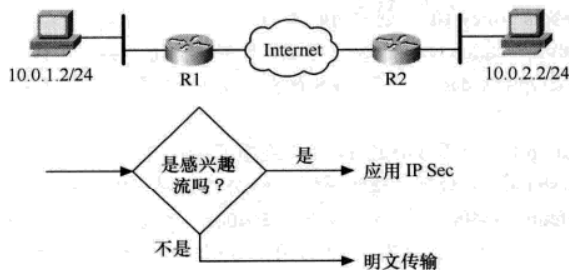


图 12-3-2 定义感兴趣流

如果流量符合 ACL 将使用 IPsec 进行保护，不满足 ACL 的流量明文传输，如上图 10.0.1.2 主机去往 10.0.2.2 主机的流量将使用 IPsec，10.0.1.2 去往 Internet 的流量将被明文传输。如图 12-3-2 所示内网使用的是私有地址，内网访问 Internet 的流量需要使用 NAT，但要把 10.0.1.0/24 去往 10.0.2.0/24 的流量排除使用 NAT。

STEP 2 IKE 阶段 1。阶段 1 的任务是：协商 IKE 策略、交换密钥、认证对等体，并且在对等体之间建立一个安全的通道。阶段 1 有两种模式：主要模式和主动模式。

主要模式需要进行 3 次交换，共发送 6 个消息，过程如下。

- 第一次交换，两对等体使用 ISAKMP (Internet Security Association and Key Management Protocol, Internet 安全关联和密钥管理协议) 协商 IKE 策略，包括加密和 Hash 算法。一去一回包括 2 个消息。

- 第二次交换，两对等体使用 DH 产生共享密钥。一去一回包括 2 个消息。

- 第三次交换，对等体认证。一去一回包括 2 个消息。

主动模式只发送 3 个信息，具体如下。

- 第一个消息，发起者发送所有的安全参数，包括 IKE 策略、DH 公钥、对等体认证等。

● 第二个消息, 接受者把协商后的安全参数发回发起者。

● 第三个消息, 发起者确认交换。

Cisco 设备使用策略集来协商 IKE 参数, 如图 12-3-3 所示, 路由器 R1 将自己所有的策略集发送到路由器 R2, 路由器 R2 将自己的策略集分别和路由器 R1 的策略集比较, 直到发现匹配为止。此例中, 可以看到路由器 R1 的策略集 10 和路由器 R2 的策略集 10 匹配, 如果没有发现匹配, 会话将被拆除。

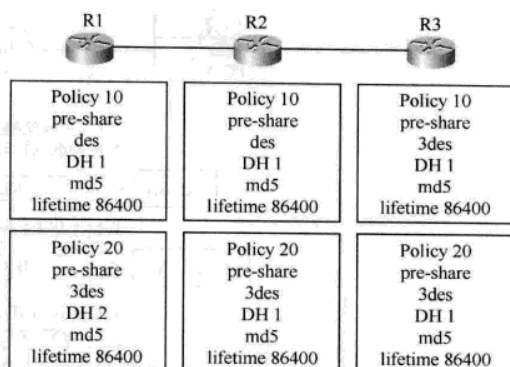


图 12-3-3 IKE 策略协商

在点对点链路上, 每端只需要一个策略集就可以了, 可在 Hub and Spoke 结构中, Hub 端可能需要配置多个策略集来适应不同的 Spoke 端, 如图 12-3-3 所示, 路由器 R3 的策略集 20 和路由器 R2 的策略集 20 匹配。策略集匹配的原则是从上至下, 一般把高安全策略集的编号设得比低安全策略集的编号小, 这样可以先使用高安全的进行协商, 高安全的策略集协商不成, 再使用低安全策略集的进行协商。

如图 12-3-3 所示, 路由器 R1 策略集 10 的创建命令如下:

```
R1(config)#crypto isakmp policy 10 创建策略集 10
R1(config-isakmp)#authentication pre-share 验证方法采用的是预共享密钥, 默认使用的是数字证书
R1(config-isakmp)#encryption des 采用 DES 加密, 默认加密的方式就是 DES, 如果是默认值可以省略不写
R1(config-isakmp)#group 1 采用 DH 组 1, 默认值就是 DH 组 1
R1(config-isakmp)#hash md5 散列算法使用的是 MD5, 散列算法默认使用的是 SHA
R1(config-isakmp)#lifetime 86400 生存期设置成 86400s, 也就是 24 小时, 默认是生存期是 24 小时
```

STEP 3 IKE 阶段 2。阶段 2 仅有一个模式, 即快速模式。它主要完成两个功能。功能 1 是使用 IPsec 转换集 (Transform Set) 协商 IPsec 参数, 也就是协商数据如何被加密和认证的相关参数。和 IKE 策略集类似, IPsec 转换集用于协商 IPsec 参数, 发送方路由器将自己的转换集全部发送给接收方路由器, 接收方路由器将自己的转换集分别和发送方路由器的转换集比较, 直到发现匹配为止。功能 2 是执行完美前向保密 (Perfect Forward Security, PFS), 功能 2 是可选的, 阶段 2 默认使用阶段 1 的 DH 协商结果, 用户也可以选择重新进行 DH 协商。

STEP 4 数据传输。隧道建立起来以后, IPsec 对等体间的流量通过安全的通道交换。

STEP 5 隧道终止。当用户终止链路或指定的生存周期 (lifetime) 过期时, IPsec 的安全关联就超时了, 此时密钥也会丢失。对于后来的数据, IKE 会执行一个新的阶段 2 协商。

12.4 VPN 配置实例

本节借助安全机架, 介绍使用预共享密钥建立站点到站点 VPN、使用 SDM (Security Device Manager, 安全设备管理) 的图形化界面配置站点到站点 VPN 和使用 SDM 建立远程接入 VPN 的方法。

实验 12-1 使用预共享密钥建立站点到站点 VPN

某公司总部和分部分别接入 Internet, 但总部和分部都只有一个公网 IP 地址, 如图 12-4-1 所示。要保证公司总部和分部的计算机都能访问 Internet; 而且因为办公需要, 公司总部和分部的内部计算机要能安全互访。

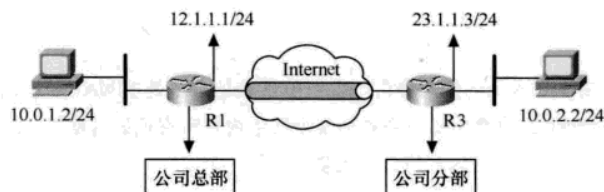


图 12-4-1 使用预共享密钥建立站点到站点 VPN

如果要保证内部很多计算机通过一个公网 IP 地址同时上网, 这就要求在总部和分部的出口路由器上配置 NAT; 要保证总部和分部的内部网络能够安全互访, 这就需要配置总部到分部的 VPN, 通过配置 VPN 既安全, 又节省费用。

使用安全机架完成本实验, 如图 12-4-1 所示的拓扑可以抽象成图 12-4-2 中的实验拓扑。本实验的操作步骤如下。

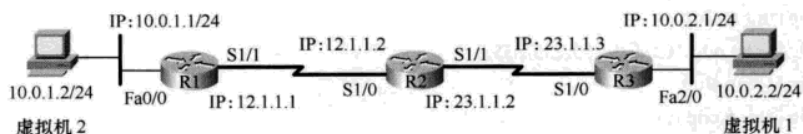


图 12-4-2 配置站点到站点 VPN

STEP 1 配置虚拟机 IP 地址。配置虚拟机 1 网卡类型 Host-only, IP 地址 10.0.2.2, 掩码 255.255.255.0, 网关 10.0.2.1, DNS 为 218.2.135.1。配置虚拟机 2 网卡类型 Bridged, IP 地址 10.0.1.2, 掩码 255.255.255.0, 网关 10.0.1.1, DNS 为 218.2.135.1。

STEP 2 基本路由配置。配置路由器 R1、R2 和 R3 的端口 IP 地址, 并配置静态路由, 保证 R1、R2 和 R3 之间的公网 IP 地址可以互通。R1 的配置如下:

```
Router#conf t
Router(config)#host R1
R1(config)#int fa 0/0
R1(config-if)#ip add 10.0.1.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#ip add 12.1.1.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#no cdp run
R1(config)#ip route 0.0.0.0 0.0.0.0 12.1.1.2
```

R2 的配置如下:

```
Router>en
Router#conf t
Router(config)#host R2
```

```
R2(config)#int s1/0
R2(config-if)#ip add 12.1.1.2 255.255.255.0
R2(config-if)#no shut
R2(config-if)#int s1/1
R2(config-if)#ip add 23.1.1.2 255.255.255.0
R2(config-if)#no shut
```

注意



R2 上不需要添加任何静态路由, 因为 10 网段的地址是被 NAT 转换成公网地址后才发出来的。就像 Internet 上的路由器不会添加某个网络内部私有地址的路由一样, 事实也是无法添加的, 因为使用同一段私有地址的公司太多了。

R3 的配置如下:

```
Router>en
Router#conf t
Router(config)#host R3
R3(config)#int s1/0
R3(config-if)#ip add 23.1.1.3 255.255.255.0
R3(config-if)#no shut
R3(config)#int fa 2/0
R3(config-if)#ip add 10.0.2.1 255.255.255.0
R3(config-if)#no shut
R3(config-if)#no cdp run
R3(config)#ip route 0.0.0.0 0.0.0.0 23.1.1.2
```

STEP 3 配置 NAT。有关 NAT 的配置请参照第 4 部分的 NAT 实验, 这里仅给出配置和简单解释。R1 的配置如下:

```
R1(config)#int fa 0/0
R1(config-if)#ip nat inside
R1(config-if)#int s1/1
R1(config-if)#ip nat outside
R1(config-if)#exit
R1(config)#access-list 100 deny ip 10.0.1.0 0.0.0.255 10.0.2.0 0.0.0.255 因为 10.0.1.0/24 去往 10.0.2.0/24 的数据包不需要做地址转换, 它们之间的流量需要被加密, 使用隧道模式, 隧道会在 IP 包中添加新的 IP 包头。
R1(config)#access-list 100 permit ip any any 除走隧道外的所有流量都允许被 NAT
R1(config)#ip nat inside source list 100 interface s1/1 overload
```

R3 的配置如下:

```
R3(config)#int fa 2/0
R3(config-if)#ip nat inside
R3(config-if)#int s1/0
R3(config-if)#ip nat outside
R3(config)#access-list 100 deny ip 10.1.2.0 0.0.0.255 10.0.1.0 0.0.0.255
R3(config)#access-list 100 permit ip any any
R3(config)#ip nat inside source list 100 interface s1/0 overload
```


至此, 虚拟机 1 和虚拟机 2 应该可以 ping 通所有的公有地址, 如 12.1.1.1、12.1.1.2、23.1.1.2 和 23.1.1.3。但虚拟机 1 和虚拟机 2 之间无法 ping 通。

STEP 4 定义感兴趣流。R1 的配置如下:

```
R1(config)#access-list 101 permit ip 10.0.1.0 0.0.0.255 10.0.2.0 0.0.0.255
```

R3 的配置如下:

```
R3(config)#access-list 101 permit ip 10.0.2.0 0.0.0.255 10.0.1.0 0.0.0.255
```

STEP 5 配置 IKE 阶段 1。主要是完成 key 的交换和对等体的认证, R1 的配置如下:

```
R1(config)#crypto isakmp policy 10
```

```
R1(config-isakmp)#authentication pre-share
```

```
R1(config-isakmp)#hash sha
```

```
R1(config-isakmp)#encryption 3des
```

```
R1(config-isakmp)#group 2
```

R1(config)#crypto isakmp key 0 cisco address 23.1.1.3 验证对等体, 共享密钥是 cisco, 对等体的地址是 23.1.1.3

R3 的配置如下:

```
R3(config)#crypto isakmp policy 10
```

```
R3(config-isakmp)#authentication pre-share
```

```
R3(config-isakmp)#hash sha
```

```
R3(config-isakmp)#encryption 3des
```

```
R3(config-isakmp)#group 2
```

```
R3(config)#crypto isakmp key 0 cisco address 12.1.1.1
```

STEP 6 配置 IKE 的阶段 2。完成数据的加密协商, R1 的配置如下:

R1(config)#crypto ipsec transform-set ccnp esp-sha-hmac esp-3des 配置转换集, 转换集的名字叫 ccnp, 采用 esp sha 进行认证, 采用 esp 3des 进行加密

R3 的配置如下:

R3(config)#crypto ipsec transform-set ccnp esp-sha-hmac esp-3des 配置转换集, 转换集的名字叫 ccnp, 这里的名字可以和 R1 不一样, 但对数据的加密算法要一致, 不然协商会失败

STEP 7 配置加密映射表。R1 的配置如下:

R1(config)#crypto map vpn-map 10 ipsec-isakmp 创建映射表 vpn-map, 这里的 10 是编号, 同一个映射表可以有多个编号, 在 Hub and Spoke 结构下, 一台路由器要建立到多个 VPN 对等体的连接, 编号 10 可以是 R3, 编号 20 可以是 R 等。和不同的对等体可以有不同的感兴趣流, 可以采用不同的加密和认证方式

```
R1(config-crypto-map)#set peer 23.1.1.3 对等体的地址是 23.1.1.3
```

```
R1(config-crypto-map)#match address 101 感兴趣的流是 ACL 101
```

```
R1(config-crypto-map)#set transform-set ccnp 变换集使用前面定义的变换集 ccnp
```

R3 的配置如下:

```
R3(config)#crypto map vpn-map 10 ipsec-isakmp
```

```
R3(config-crypto-map)#set peer 12.1.1.1
```

```
R3(config-crypto-map)#match address 101
```

```
R3(config-crypto-map)#set transform-set ccnp
```

STEP 8 在接口上应用加密映射表。R1 的配置如下:

```
R1(config)#int s1/1 在路由器的对外端口上调用加密映射表
```

```
R1(config-if)#crypto map vpn-map
```

R3 的配置如下:

```
R3(config)#int s1/0    在路由器的对外端口上调用加密映射表
```

```
R3(config-if)#crypto map vpn-map
```

STEP 9 测试。在虚拟机 1 上 ping 虚拟机 2 的 IP 地址 10.0.1.2 可以 ping 通, 但前面会有 1 到 2 个包超时, 原因是因为第一个 ping 包是感兴趣的流量触发 VPN, VPN 的建立需要一定的时间, 当 VPN 建立起来后, 后来的 ping 包都可以正常 ping 通了。

在路由器 R1 上使用 show crypto isakmp sa, 结果如下, 可以看到 12.1.1.1 和 23.1.1.2 的连接状态是 ACTIVE。

```
R1#show crypto isakmp sa
```

```
IPv4 Crypto ISAKMP SA
```

dst	src	state	conn-id	slot	status
23.1.1.3	12.1.1.1	QM_IDLE	1001	0	ACTIVE

```
IPv6 Crypto ISAKMP SA
```

在路由器 R1 上使用 show access-lists, 结果如下, 可以看到访问控制列表后面有匹配条目。

```
R1#show access-lists
```

```
Extended IP access list 100
```

```
10 deny ip 10.0.1.0 0.0.0.255 10.0.2.0 0.0.0.255 (6 matches)
```

```
20 permit ip any any (2 matches)
```

```
Extended IP access list 101
```

```
10 permit ip 10.0.1.0 0.0.0.255 10.0.2.0 0.0.0.255 (11 matches)
```

在路由器 R1 上使用 show crypto ipsec sa, 部分显示结果如下, 可以看到感兴趣的流量, 外出和进入被加密的数据包的类型和数量。

```
R1#show crypto ipsec sa
```

```
interface: Serial1/1
```

```
Crypto map tag: vpn-map, local addr 12.1.1.1
```

```
protected vrf: (none)
```

```
local ident (addr/mask/prot/port): (10.0.1.0/255.255.255.0/0/0)
```

```
remote ident (addr/mask/prot/port): (10.0.2.0/255.255.255.0/0/0)
```

```
current_peer 23.1.1.3 port 500
```

```
inbound esp sas:
```

```
spi: 0xD0DBB4F3(3504059635)
```

```
transform: esp-3des esp-sha-hmac ,
```

```
in use settings = {Tunnel, }
```

```
conn id: 1, flow_id: 1, crypto map: vpn-map
```

```
sa timing: remaining key lifetime (k/sec): (4478684/3268)
```

```
IV size: 8 bytes
```

```
replay detection support: Y
```

```
Status: ACTIVE
```

```
inbound pcp sas:
```

```
outbound esp sas:
```

```
spi: 0xC8DBC989(3369847177)
```

```
transform: esp-3des esp-sha-hmac ,
```

```
in use settings = {Tunnel, }
```

```
conn id: 2, flow_id: 2, crypto map: vpn-map
```

```

sa timing: remaining key lifetime (k/sec): (4478684/3267)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE
outbound ah sas:
outbound pcp sas:

```

STEP 10 配置文件下载 (实验补充)。下载文件 network.rar 中提供了路由器 R1, R2 和 R3 的 show running-config 配置。读者只需要在全局配置下粘贴, 并打开所有使用的端口, 即可测试。

STEP 11 使用路由器测试。如计算机配置较低, 同时运行 3 台路由器和两台虚拟机可能有难度。可以在路由器上借助扩展 ping 来测试本实验, 扩展 ping 比普通的 ping 提供更多的选项, 更强的功能, 测试的过程和解释如下:

```

R1#ping 输入 ping 直接回车
Protocol [ip]: 使用的是 IP 协议, 直接回车就可以了
Target IP address: 10.0.2.1 要去的目标地址
Repeat count [5]: 发送 ping 包的数量
Datagram size [100]: 数据包的大小是 100
Timeout in seconds [2]: 超时时间设置, 2 秒内没有收到应答就认为超时
Extended commands [n]: y 要扩展 ping 命令吗?
Source address or interface: 10.0.1.1 ping 命令要使用的源地址, 如果不输入, 路由器将使用离目标最近
的端口作为源地址, 也就是说, 这里如果不输入 10.0.1.1, 将使用的是 12.1.1.1, 这个流量不是 VPN 感兴
趣的流量, 不能触发 VPN 连接。更多选项这里不作介绍, 接下去的窗口全部直接按回车键就可以了。
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.2.1, timeout is 2 seconds:
Packet sent with a source address of 10.0.1.1
!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 24/30/44 ms

```

实验 12-2 使用 SDM 建立站点到站点 VPN

通过命令行的方式配置 VPN 即复杂又容易出错。思科提供了 SDM 配置软件, 用户只要了解 VPN 配置的步骤, 通过图形化界面, 很容易即可完成 VPN 的配置, 且不容易出错。使用 SDM 配置使用共享密钥站点到站点 VPN 的配置步骤如下。

STEP 1 配置同实验 12-1。

STEP 2 配置同实验 12-1。

STEP 3 配置同实验 12-1。

STEP 4 安装 SDM。在真实机上, 解压缩 “SDM-V241-zh 中文版.zip” 文件到某个文件夹, 双击文件夹中的 “setup.exe”, 开始安装 SDM 软件。安装向导检查真实机上有无具备 Java 环境,

如果之前没有安装过 Java, 请安装下载文件 network.rar 中的 “11/j2re-1_4_2_12-windows-i586-p.exe” 文件。接下来, 安装向导会询问 SDM 文件安装的位置, 如图 12-4-3 所示, 选择 “本地计算机”, 单击 “下一步” 按钮继续, 完成 SDM 的安装。

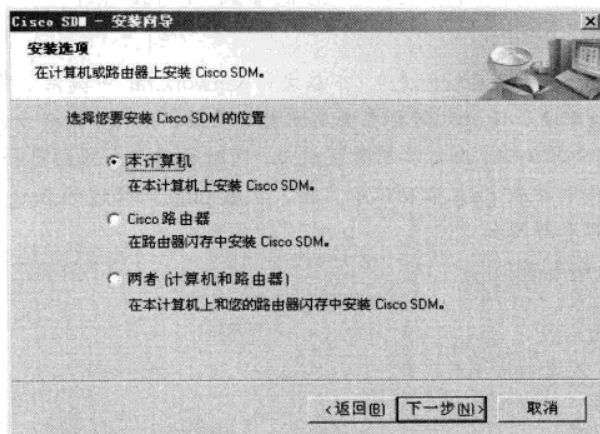


图 12-4-3 安装 SDM

STEP 5 准备使用 SDM。配置路由器 R1 和 R3, 配置 SDM 连接使用的接口 IP 地址, 同时还要启用路由器的 HTTP 服务。路由器 R1 的配置如下:

```
R1(config)#int fa 0/0
R1(config-if)#ip add 192.168.1.201 255.255.255.0 secondary 给接口配置第二个 IP 地址, 真实机的 SDM
软件通过这个 IP 地址连接路由器, 并进行配置, secondary 是关键字, 不能省略, 不然会替换接口 IP 地址
R1(config-if)#exit
R1(config)#ip http server 开启路由器的 HTTP 服务
路由器 R3 的配置如下:
```

```
R3(config)#int fa 0/0
R3(config-if)#ip add 192.168.1.203 255.255.255.0
R3(config-if)#no shut
R3(config-if)#exit
R3(config)#ip http server
```

STEP 6 使用 SDM。在真实机上, 双击桌面的 “Cisco SDM (Chinese Edition)” 图标, 输入路由器 R1 的 IP 地址 192.168.1.201, 如图 12-4-4 所示。

单击 “启动” 按钮, 系统会弹出 “警告-安全” 窗口, 单击 “是”, 信任该软件。有的系统可能会弹出一个代码窗口, 如果弹出代码窗口, 需要更改 IE 浏览器的设置。在 IE 浏览器中选择 “工具” 菜单 → “Internet 选项” 命令, 打开 “Internet 选项” 窗口, 单击 “高级” 选项卡, 如图 12-4-5 所示。选中 “允许活动内容在我的计算机上的文件中运行”, 单击 “确定” 按钮, 关闭 IE 浏览器窗口, 使用 SDM 再重新连接。

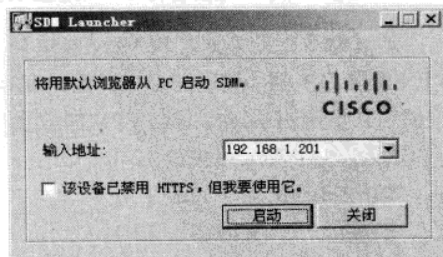


图 12-4-4 SDM 连接路由器

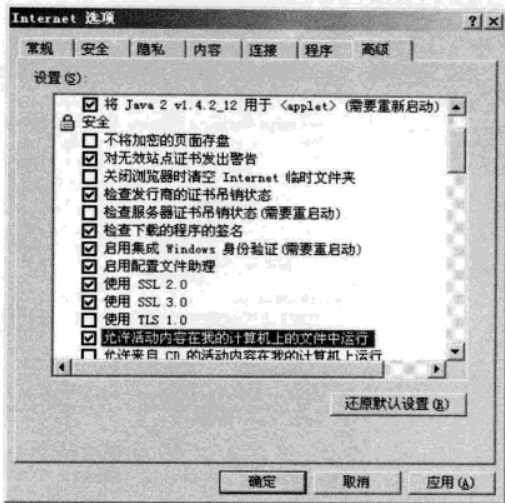


图 12-4-5 允许执行活动内容

打开后的 SDM 主界面如图 12-4-6 所示。从该界面中可以看到路由器的型号、内存和闪存大小、IOS 的版本、SDM 的版本、支持的功能（包括 IP、防火墙、VPN、IPS、NAC）等。

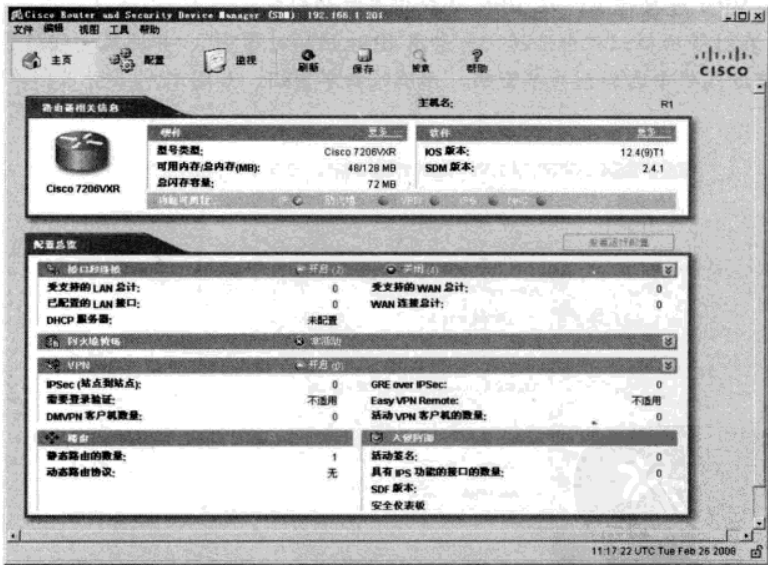


图 12-4-6 SDM 主界面

STEP 7 启动 VPN 向导。单击 SDM 主界面工具栏中的“配置”图标，选择左侧导航栏中的“VPN”图标→中间栏中的“站点到站点 VPN”，选中右侧窗口中的“创建站点到站点 VPN”，单击“启动选定的任务”，如图 12-4-7 所示，打开 VPN 配置向导。

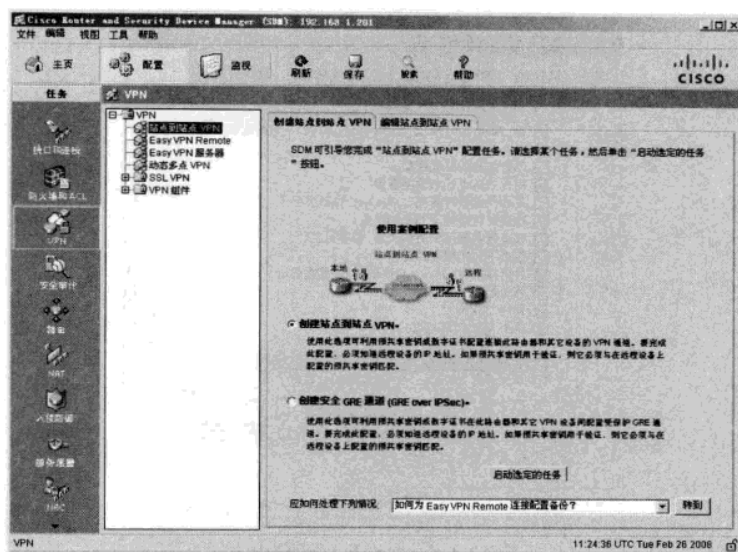


图 12-4-7 配置 VPN 向导

STEP 8 逐步操作向导。在“站点到站点 VPN 向导”中，单击“逐步操作向导”，单击“下一步”按钮。

STEP 9 VPN 连接信息。在 VPN 连接信息对话框中，为 VPN 连接选择接口，这里选择“Serial 1/1”；在对等项标识栏中选择“有静态 IP 地址的对等项”，并填入远程对等项的 IP 地址 23.1.1.3；验证方式栏中选择预共享密钥，并填入共享密钥，如图 12-4-8 所示。单击“下一步”按钮继续。

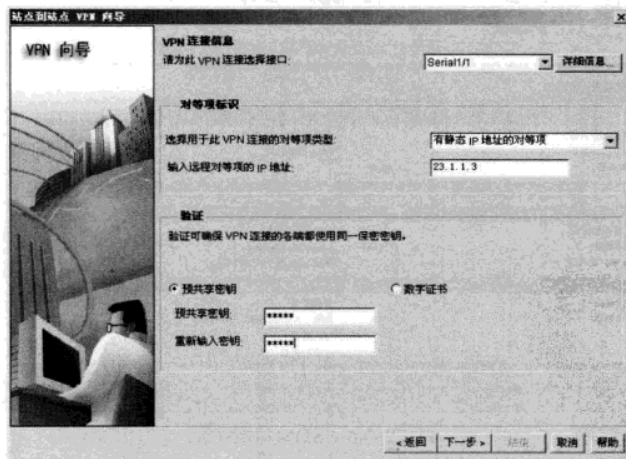


图 12-4-8 VPN 连接信息

STEP 10 IKE 提案。其实也就是配置 IKE 的阶段 1，配置 IKE 的策略集，这里使用默认的策略集，单击“下一步”按钮继续。

STEP 11 转换集。其实也就是配置 IKE 的阶段 2，配置数据加密的方法，这里使用默认转换集，单击“下一步”按钮继续。

STEP 12 要保护的通信。如图 12-4-9 所示，配置要保护的通信，选择“保护下列子网间的所有通信”，在本地网中填入 10.0.1.0/24，在远程网中填入 10.0.2.0/24。或者也可以选择“创建/选择 IPSec 通信访问列表”，这里使用的列表其实也就是实验 12-1 中的访问列表 101。单击“下一步”按钮继续。

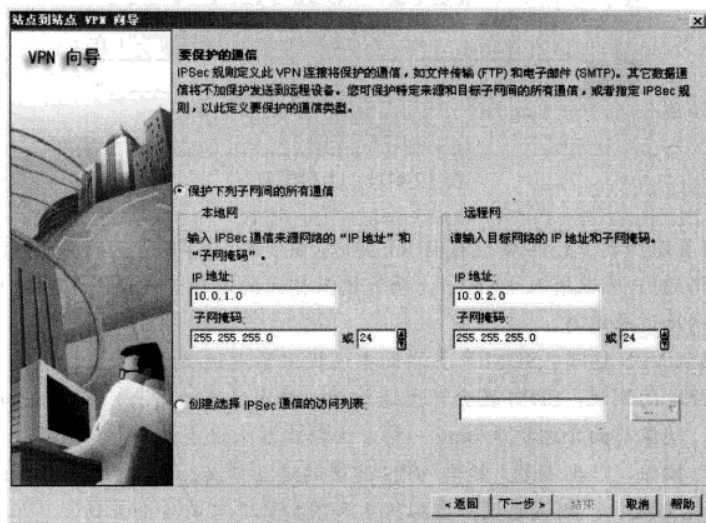


图 12-4-9 要保护的通信

STEP 13 完成配置。单击“完成”按钮，结束 VPN 配置向导，向导会提示一些不兼容问题，如图 12-4-10 所示，单击“是”按钮，接受修改就可以了。

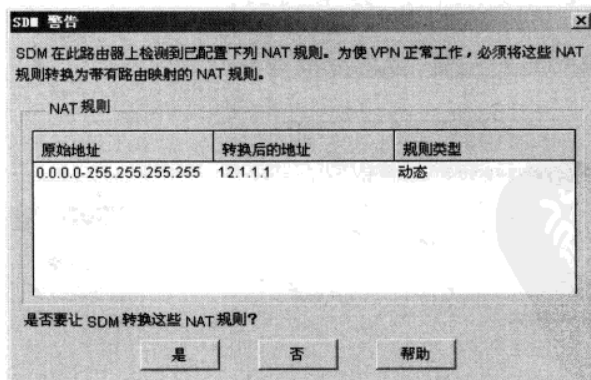


图 12-4-10 SDM 警告

SDM 弹出如图 12-4-11 所示的对话框，SDM 把配置命令上传到路由器。

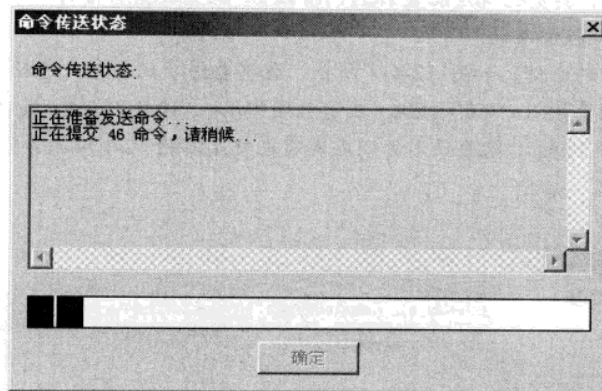


图 12-4-11 上传配置

STEP 14 配置路由器 R3。操作过程与 R1 类似, 在如图 12-4-8 所示的界面中选择“Serial 1/0”接口, 远程对等体的 IP 地址填入 12.1.1.1, 两边填入相同的密钥。在如图 12-4-9 所示的界面中, 把本地网和远程网反过来填写。

STEP 15 测试 VPN 通道。SDM 配置界面中还提供了测试功能, 单击配置完成界面中的“测试通道”, 开始 VPN 的测试, SDM 还会产生通信量, 触发通道的建立, 如图 12-4-12 所示, 填入流量的目标地址, 就像前面介绍扩展 ping 一样, 由路由器来产生流量。

单击“继续”按钮, 产生流量, 检查 VPN 通道的建立情况, 全部完成, 弹出如图 12-4-13 所示对话框, VPN 建立成功, 测试通过, 虚拟机 1 和虚拟机 2 可以安全互访。

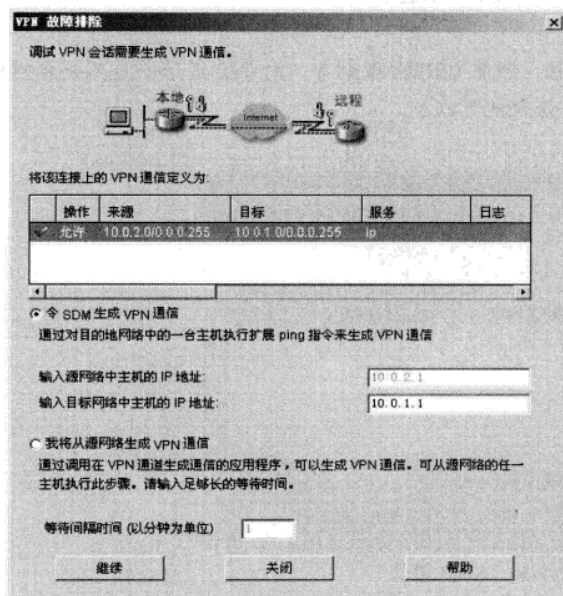


图 12-4-12 VPN 模拟流量

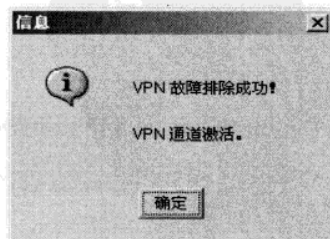


图 12-4-13 VPN 通道建立成功

实验 12-3 使用 SDM 建立远程接入 VPN

如图 12-4-14 所示, 某公司总部接入 Internet, 并有一个公网 IP 地址; 远程办公室也接入了 Internet, 出于节省费用方面考虑, 并未申请固定的 IP 地址, 远程办公室的成员要能安全访问公司总部内的资源; 一部分移动和家庭用户也要能安全访问公司总部内的资源。在这种情况下, 因远程办公室、移动和家庭用户没有固定的 IP 地址, 不具备使用站点到站点 VPN 的条件, 这就需要配置远程接入 VPN, 也称 Easy VPN。

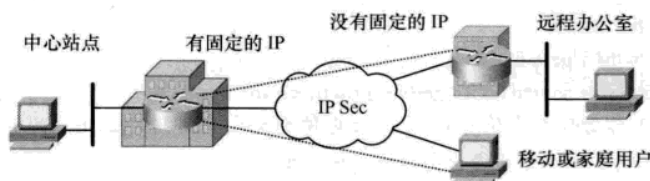


图 12-4-14 远程接入 VPN 拓扑

要保证远程办公室和公司总部人员都可以访问 Internet, 这就要求在总部和远程办公室的出口路由器上配置 NAT; 要保证移动和家庭用户能安全访问公司总部内的资源, 需要在公司总部配置 Easy VPN Server, 在移动和家庭用户计算机上配置 Easy VPN Client; 要保证远程办公室的成员都能安全访问公司总部内的资源, 这就要求在公司总部配置 Easy VPN Server 端, 在远程办公室的出口设备上配置 Easy VPN Remote 端; 网络能够安全互访, 这就需要配置总部到分部的 VPN, 通过配置 VPN 即安全, 又节省费用。

使用安全机架完成本实验, 如图 12-4-14 所示的拓扑可以抽象成如图 12-4-15 所示的实验拓扑。该实验难度较大, 借助 SDM 可以使配置简单化, 并且不容易出错和遗漏配置, 用户可以查看 SDM 向导产生的配置文件, 学习 Easy VPN 相关的配置命令, 也可通过命令行对配置文件进行修改。本实验分为网络基本配置、Easy VPN Server 配置、Easy VPN Client 配置和 Easy VPN Remote 配置 4 个大步骤, 每个大步骤中又包括若干细节步骤。

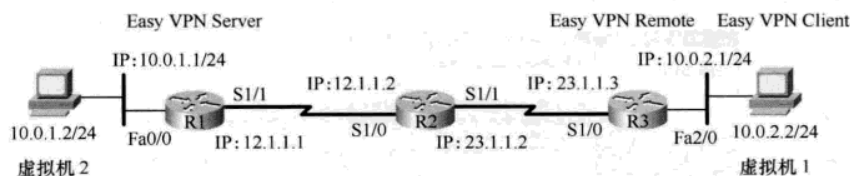


图 12-4-15 远程接入实验拓扑

1. 网络基本配置

- STEP 1** 配置虚拟机 IP 地址。同实验 12-1。
- STEP 2** 基本路由配置。同实验 12-1。
- STEP 3** 配置 NAT。

```
R1(config)#int fa 0/0
R1(config-if)#ip nat inside
R1(config-if)#int s1/1
```

```
R1(config-if)#ip nat outside
R1(config-if)#exit
R1(config)#access-list 1 permit ip any
R1(config)#ip nat inside source list 1 interface s1/1 overload
```

R3 的配置如下:

```
R3(config)#int fa 2/0
R3(config-if)#ip nat inside
R3(config-if)#int s1/0
R3(config-if)#ip nat outside
R3(config)#access-list 1 permit ip any
R3(config)#ip nat inside source list 1 interface s1/0 overload
```

至此, 虚拟机 1 和虚拟机 2 应该可以 ping 通所有的公有地址, 如 12.1.1.1、12.1.1.2、23.1.1.2 和 23.1.1.3。但虚拟机 1 和虚拟机 2 之间无法 ping 通。

2. 配置 Easy VPN Server

STEP 1 配置路由器 R1 支持 SDM。配置如下:

```
R1(config)#int fa 0/0
R1(config-if)#ip add 192.168.1.201 255.255.255.0 secondary
R1(config-if)#exit
R1(config)#ip http server
```

STEP 2 启用 AAA。配置 Easy VPN Server 需要启用 AAA。

```
R1(config)#aaa new-model
R1(config)#username cisco privilege 15 password cisco123
```

STEP 3 启动 Easy VPN 服务器向导。在真实机的 SDM 管理器中, 填入路由器 R1 的 IP 地址 192.168.1.201, 打开 R1 的图形化配置界面, 和图 12-4-7 类似, 单击 SDM 主界面工具栏中的“配置”图标, 选择左侧导航栏中的“VPN”图标→中间栏中的“Easy VPN 服务器”, 单击右侧窗口中的“启动 Easy VPN 服务器向导”。打开 Easy VPN 服务器向导, 如图 12-4-16 所示, 此向导将

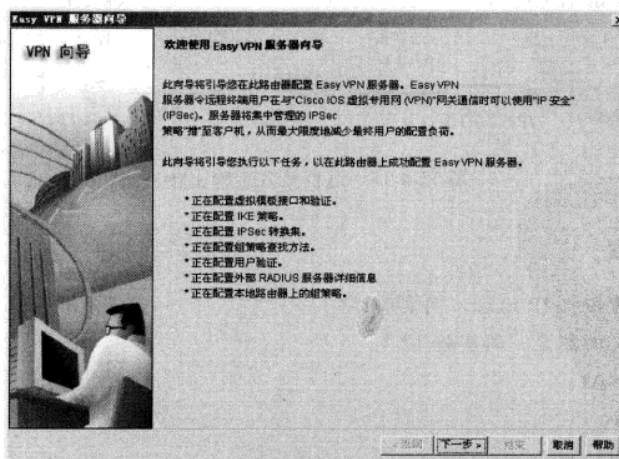


图 12-4-16 Easy VPN 服务器向导

执行图中列出的任务。单击“下一步”按钮继续。

STEP 4 接口和验证。如图 12-4-17 所示, 接口栏中选择“未编号对象为”, 在下拉列表中选择 Serial1/1 接口, 也就是 Easy VPN Server 对外提供服务的端口; 在验证栏中, 选择“预共享密钥”, 单击“下一步”按钮继续。

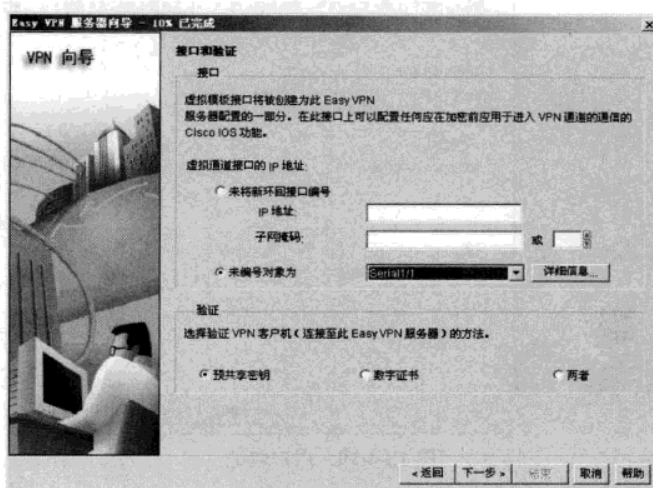


图 12-4-17 接口和验证

STEP 5 IKE 提案。保持使用默认的策略集, 单击“下一步”按钮继续。

STEP 6 转换集。保持使用默认的转换集, 单击“下一步”继续。

STEP 7 组授权和组策略查找。如图 12-4-18 所示, 选择“本地”, 因没有配置 RADIUS 和 TACACS+ 服务器, 这里使用本地的用户组。用户可以结合第 11 章, 配置基于 RADIUS 或 TACACS+ 的认证, 单击“下一步”按钮继续。

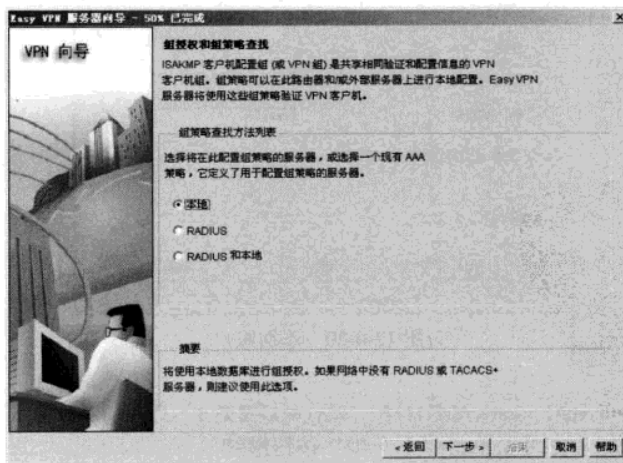


图 12-4-18 组授权和组策略查找

STEP 8 用户验证。如图 12-4-19 所示，选择“启用用户验证”并选择“仅限本地”，同样也可以结合第 11 章，配置基于 RADIUS 或 TACACS+ 的认证。

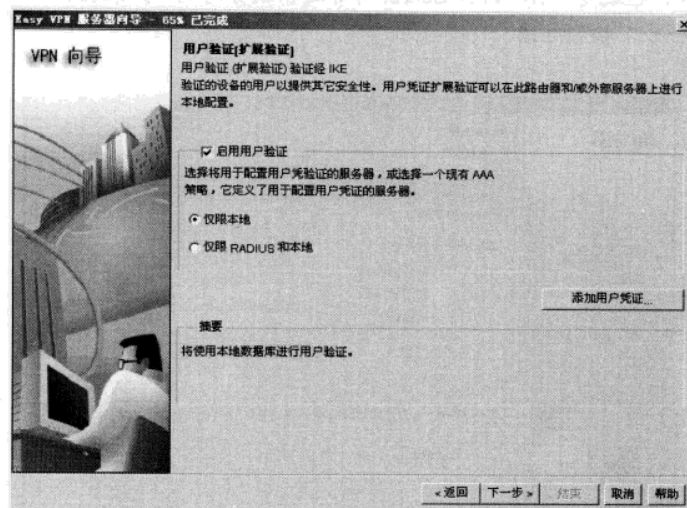


图 12-4-19 用户验证

单击“添加用户凭证”按钮，打开如图 12-4-20 所示的对话框，进行用户添加。如输入用户名 vpn1，密码 111111，权限级别是 1，单击“确定”按钮返回，这里的配置相当于下面的命令行：

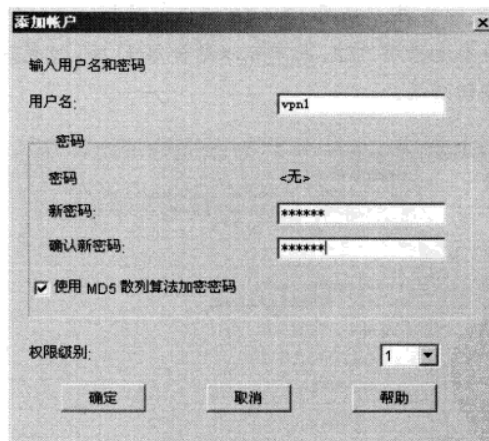


图 12-4-20 添加账户

```
R1(config)#username vpn1 password 111111 默认的级别是 1
```

用户可以继续添加，也可以单击“下一步”按钮继续。

STEP 9 组授权和用户组策略。这一步骤很关键，如图 12-4-21 所示。

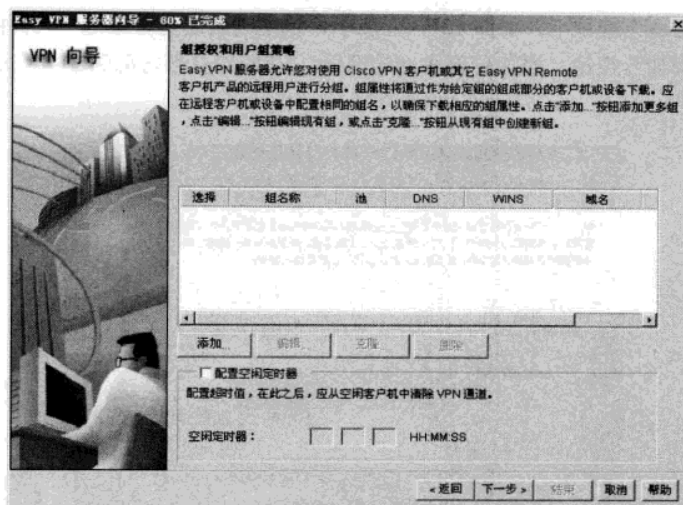


图 12-4-21 组授权和用户组策略

单击“添加”按钮，打开“添加组策略”对话框，选择“一般”选项卡，如图 12-4-22 所示填写，组的名称输入 ccnp；共享密钥输入 cisco；在“地址池信息”，选择“创建新池”，并在起始 IP 地址中填入 10.100.0.1，结束 IP 地址中填入 10.100.0.200，子网掩码中填入 255.255.255.0，VPN 客户端连上来将被分配地址池中的地址，允许最大连接数填入 100，表示的是不管组中实际有多少用户，但能同时在线的 VPN 用户不能超过 100 个。单击“DNS/WINS”选项卡，填入 VPN 客户端被分配的 DNS 或 WINS 服务器的 IP 地址。

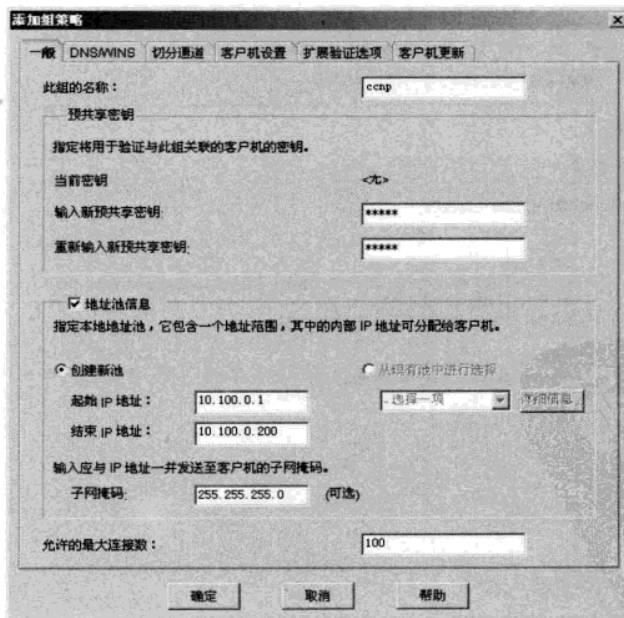


图 12-4-22 组策略一般选项卡

选择“切分通道”选项卡，如图 12-4-23 所示，选中“启用切分隧道”，选择“输入受保护子网”后，单击“添加”按钮，添加总部内部的网址，VPN 到总部内部的通信流量将被分离出来，也就是被加密保护。

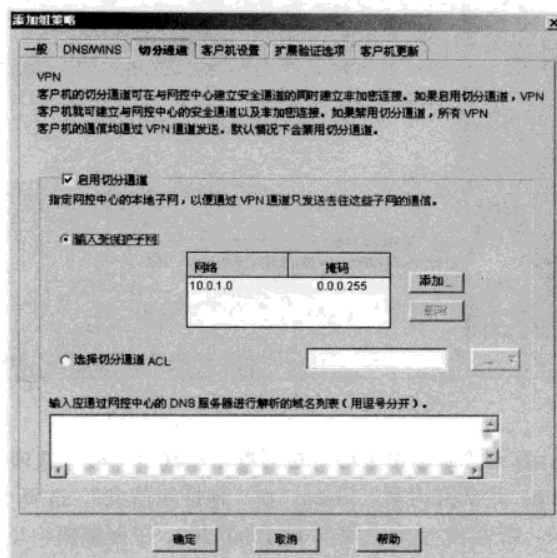


图 12-4-23 切分通道选项卡

“客户机设置”选项卡中保持默认，不做任何改变。单击“扩展验证选项”选项卡，如图 12-4-24

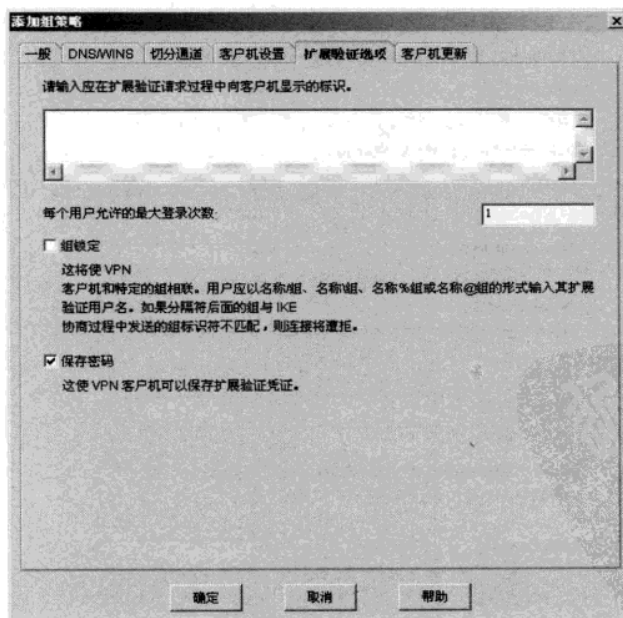


图 12-4-24 扩展验证选项卡

所示填写,“每个用户允许的最大登录次数”也就是同一个用户允许同时在线的人数限制,出于记账目的,可以设成 1。选中“保存密码”,VPN 客户端第一次连接需要密码,以后客户端连接选项中会多出一个“保存密码”选项。“客户机更新”选项卡保持默认。单击“确定”按钮,返回如图 12-4-21 所示的对话框。单击“下一步”按钮继续,最后完成 Easy VPN Server 配置向导。

3. 配置 Easy VPN Client

STEP 1 测试。在虚拟机 1 上 ping 虚拟机 2 的 IP 地址 10.0.1.2,测试连通性,结果是 ping 不通。

STEP 2 安装 VPN Client 软件。在虚拟机 1 上,双击“vpnclient-win-msi-4.8.01.0300-k9.exe”文件,开始安装 VPN Client 软件。安装完成后,重新启动虚拟机 1。

STEP 3 配置 VPN Client 软件。选择“开始”→“程序”→“Cisco Systems VPN Client”→“VPN Client”,打开 VPN Client 软件,界面如图 12-4-25 所示。

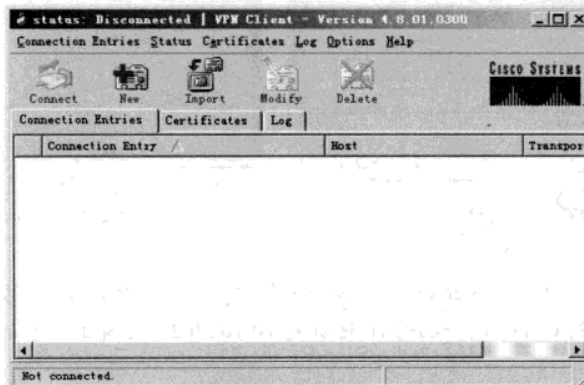


图 12-4-25 VPN Client 窗口

单击工具栏中的“New”按钮,打开 VPN 连接建立对话框,如图 12-4-26 所示填写,在

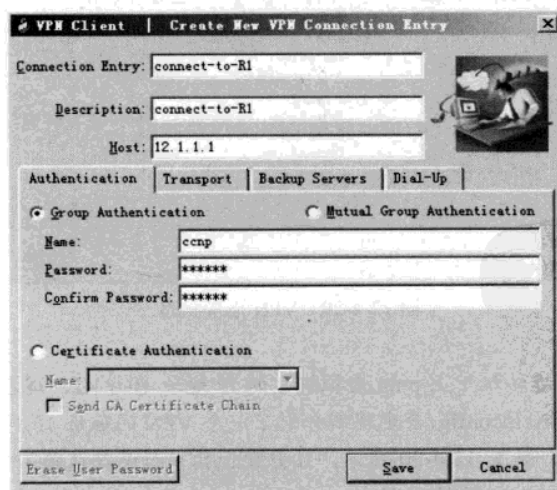


图 12-4-26 新建 VPN 连接

“Connection Entry” (连接条目) 和 “Description” (描述) 中随意输入些直观信息; 在 “Host” (主机) 栏中输入 Easy VPN Server 服务器的 IP 地址, 这里是 12.1.1.1; 组的名称中填入 ccnp, 密码填入对应的 cisco, 单击 “Save” 按钮保存这个连接, 返回到如图 12-4-25 所示的界面。

双击图 12-4-25 中新建的连接, 稍后打开用户验证对话框, 输入用户名 vpn1 和对应的密码 111111, 如图 12-4-27 所示, 单击 “OK” 按钮。

Easy VPN Client 开始连接 Easy VPN Server, 稍后, 任务栏右下角的那把小锁被锁起来, 右键单击小锁图标, 弹出如图 12-4-28 所示的快捷菜单, 可以选择 “Disconnect” 命令, 断开连接。再次连接时, 图 12-4-27 所示的对话框中, 将会多出一个复选框 “Save Password”, 选中该复选框, 相当于是保存密码, 以后再次连接, 就不需输入用户名和密码了。

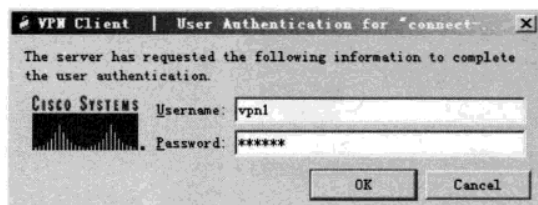


图 12-4-27 用户验证

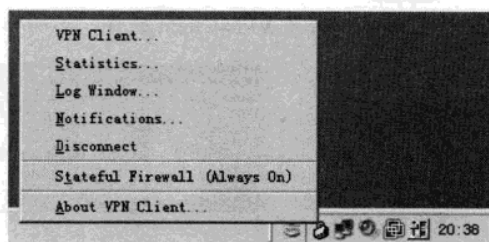


图 12-4-28 VPN 连接快捷菜单

单击如图 12-4-28 所示的 “Statistics” (状态) 菜单, 显示 VPN Client 的连接状态信息, 如图 12-4-29 所示。可以看到 Client 被分配的 IP 地址是 10.100.0.2, 还有加密和认证方法。

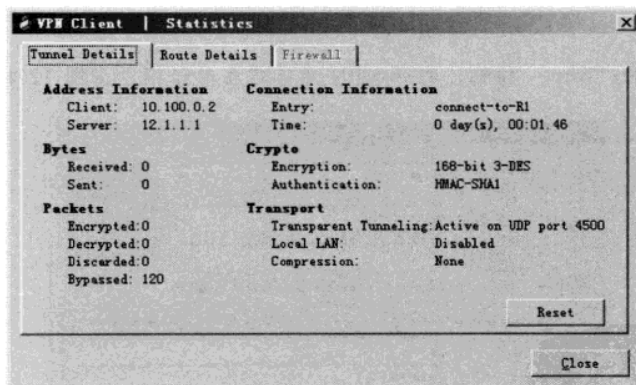


图 12-4-29 VPN 连接状态

STEP 4 测试。在虚拟机 1 上 ping 虚拟机 2 的 IP 地址 10.0.1.2, 现在可以 ping 通了。在虚拟机 1 的 DOS 窗口中输入 ipconfig, 会发现新分配了一个 VPN 的地址 10.100.0.2; 使用 route print, 查看虚拟机 1 的路由表, 如图 12-4-30 所示, 注意最上面一行是默认路由, 出口仍然是网关, 第二行是受保护的流量, 出口是 VPN 通道。

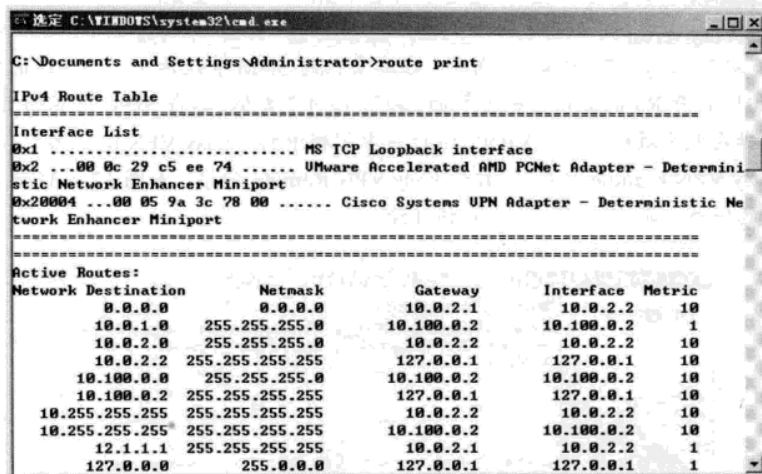


图 12-4-30 VPN Client 的路由表

在虚拟机 2 仍然不能 ping 通虚拟机 1 的 IP 地址 10.0.2.2, 但可以 ping 通 10.100.0.2。

在路由器 R1 上使用 show ip route 查看路由表, 部分显示如下, 注意 R1 的路由表中多出一条 10.100.0.3/32 的静态路由, 外出接口是 Virtual-Access2, 从这个接口发出的流量使用是隧道模式。

```

R1#show ip route
Gateway of last resort is 12.1.1.2 to network 0.0.0.0

    10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.0.1.0/24 is directly connected, FastEthernet0/0
S       10.100.0.3/32 [1/0] via 0.0.0.0, Virtual-Access2
    12.0.0.0/24 is subnetted, 1 subnets
C       12.1.1.0 is directly connected, Serial1/1
C       192.168.1.0/24 is directly connected, FastEthernet0/0
S*    0.0.0.0/0 [1/0] via 12.1.1.2
  
```

4. 配置 Easy VPN Remote

如果 R3 是一个远程办公室, 办公室内有很多个用户, 该远程办公室没有固定的 IP 地址, 配置站点到站点的 VPN 配置不太合适, 如果所有用户都自己安装 VPN Client 软件, 配置成 VPN Client, 虽可以安全访问总部内部的资源, 但要在每台计算机上配置, 工作量太大。Easy VPN Remote 刚好可以解决上面的难题, Remote 不需要有固定的 IP 地址, 却可以提供远程办公室多用户可以同时安全访问总部内部的资源, 远程办公室内部的计算机也不需要安装 VPN Client 软件。Easy VPN Remote 端 (R3) 的配置步骤如下:

STEP 1 配置 R3 支持 SDM。R3 的配置如下:

```

R3(config)#int fa 0/0
R3(config-if)#ip add 192.168.1.203 255.255.255.0
R3(config-if)#no shut
  
```

```
R3(config-if)#exit
R3(config)#ip http server
```

STEP 2 启动 Easy VPN Remote 向导。在真实机的 SDM 管理器中，填入路由器 R3 的 IP 地址 192.168.1.203，打开 R3 的图形化配置界面，和图 12-4-7 类似，单击 SDM 主界面工具栏中的“配置”图标，选择左侧导航栏中的“VPN”图标→中间栏中的“Easy VPN Remote”，单击右侧窗口中的“启动 Easy VPN Remote 向导”。打开 Easy VPN Remote 向导，如图 12-4-31 所示，此向导将执行图中列出的任务。单击“下一步”按钮继续。

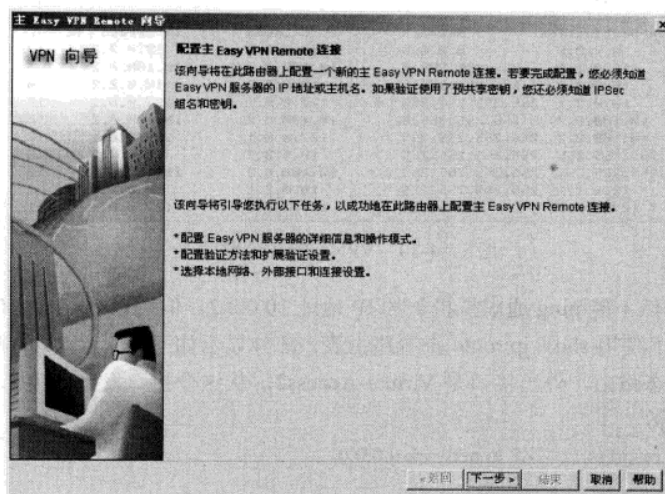


图 12-4-31 Easy VPN Remote 向导

STEP 3 服务器信息。如图 12-4-32 所示，填写服务器信息，连接名称随意填入一个直观的

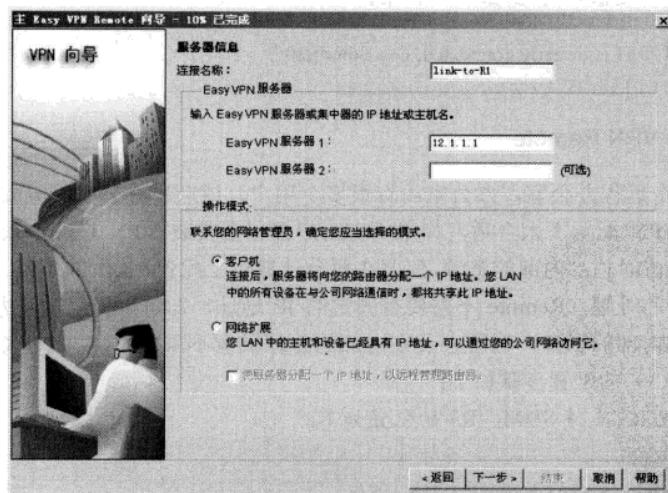


图 12-4-32 服务器信息设置

名称; Easy VPN 服务器 1 中填入路由器 R1 提供 VPN 服务的接口 IP 地址 12.1.1.1; 操作模式中选择“客户机”, 单击“下一步”按钮继续。

STEP 4 验证。如图 12-4-33 所示进行填写, 在设备验证中, 将验证方式选择为“预共享密钥”; “用户组”填入 ccnp, 密码填入 cisco; 用户验证 (扩展验证) 中选择“将扩展验证凭证保存至此路由器”; 在“用户名”中填入 vpn1, 密码填入 111111, 单击“下一步”按钮继续。

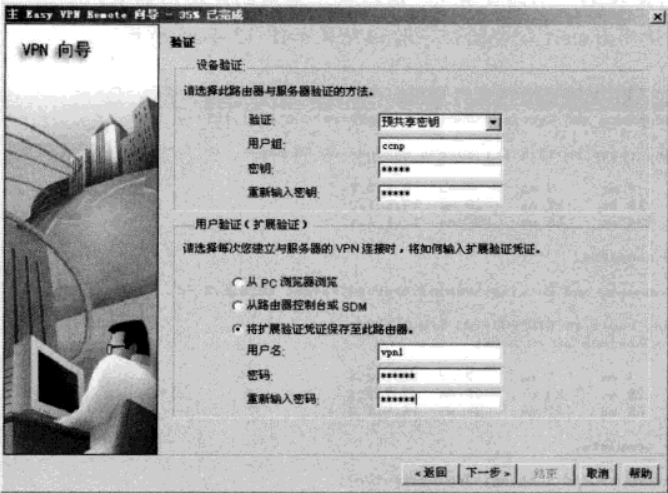


图 12-4-33 验证

STEP 5 接口和连接设置。如图 12-4-34 所示进行填写, 在“接口”中选择通过通道连接至 Easy VPN 服务器后面的网络的本地网络, 这里指的是 Easy VPN Remote 端的本地网络, 所以选择“FastEthernet2/0(10.0.2.0/24)”; R3 连接到 Internet 的端口是“Serial 1/0”; “连接设置”选择“自动”。单击“下一步”按钮继续, 完成 Easy VPN Remote 配置向导。

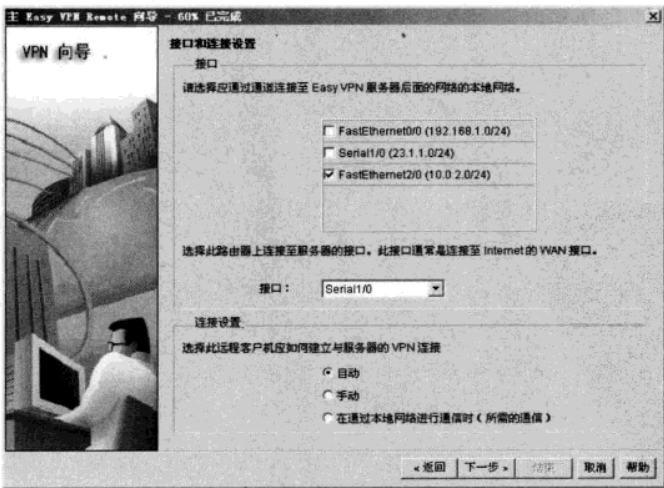


图 12-4-34 接口和连接设置

STEP 6 测试。本实验中相当于 R3 是 Easy VPN Client, R3 首先建立到 Easy VPN Server(R1 路由器)的连接, R3 内部的计算机通过 R3 共享访问公司总部内的计算机。虚拟机 1 不需要使用 VPN Client 软件, 即可 ping 通 10.0.1.2 (从虚拟机 1 到路由器 R3 之间使用的是不安全通道, 没有加密和认证。从路由器 R3 到路由器 R1 之间使用的是 VPN 隧道, 虚拟机 1 借用的是路由器 R3 的 10.100.0.4 这个 IP 地址, 实际中可能是地址池的另一个地址), 也可以 ping 通 12.1.1.1、12.1.1.2、23.1.1.2 等 (使用的是 NAT, 不涉及隧道, 虚拟机 1 借用的是路由器 R3 的 23.1.1.3 这个 IP 地址)。可以在虚拟机 1 上使用 tracert 命令验证, 验证结果如图 12-4-35 所示。

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>tracert 12.1.1.1 -d

Tracing route to 12.1.1.1 over a maximum of 30 hops

  1    4 ms    7 ms    3 ms  10.0.2.1
  2   18 ms   12 ms   10 ms  23.1.1.2
  3   24 ms   55 ms   55 ms  12.1.1.1

Trace complete.

C:\Documents and Settings\Administrator>tracert 10.0.1.2 -d

Tracing route to WIN2003-TWO [10.0.1.2]
over a maximum of 30 hops:

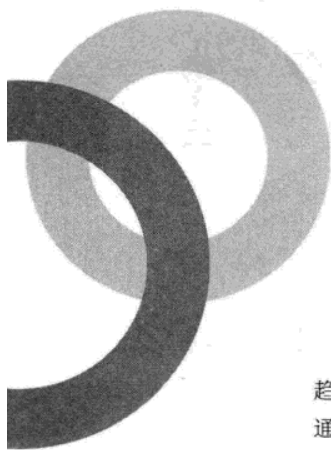
  1    3 ms    5 ms    2 ms  10.0.2.1
  2   29 ms   24 ms   26 ms  12.1.1.1
  3   65 ms   27 ms   31 ms  10.0.1.2

Trace complete.

C:\Documents and Settings\Administrator>
```

图 12-4-35 tracert 测试路由

路由器 R1 上多出一条 32 位的静态路由。路由器 R3 上多出一个 Loopback (环回) 接口, 该接口的 IP 地址就相当于 VPN Client 获取到的 IP 地址, 和 R1 上多出的那条 32 位主机路由相同。虚拟机 2 无法访问到虚拟机 1。



第 13 章 VoIP (IP 电话)

Chapter 13

如今, VoIP 已开始普遍被个人用户及企业用户所接受, VoIP 也是未来电话的发展趋势。本章主要介绍 VoIP 的基础知识、VoIP 模块接口类型、VoIP 呼叫建立的过程。通过学习本章后, 读者不仅可以了解 VoIP 的相关知识, 更可以在没有任何硬件支持的情况下, 配置和测试 VoIP 电话。

13.1 IP 电话的基础知识

VoIP 电话, 英文全名为 Voice over IP, 是一种将模拟语音信号数字化, 并进行压缩后经路由或交换(如 Internet)至目的地, 然后 VoIP 电话再将其还原成语音信号的语音通信方式。数据网络对数据信息采用的是“存储—转发”的分组交换技术进行传递和交换。语音信号在 IP 网上传送前要先进行模拟信号的数字化处理, 经过压缩后, 被数据通信网中的 IP 电话网关“打包”, 成为分组, 在每个分组中有被叫电话号码所对应的 IP 地址, 形成数据流, 然后才送到网络上进行传送。

如图 13-1-1 所示是使用传统电话机(也就是常见的普通电话机)和 IP 电话机进行 VoIP 通话的工作原理图。

使用传统电话机的 VoIP, 即图 13-1-1 中的上半部分, 网关将 PSTN(Public Switched Telephone Network, 公共交换电话网络, 即常用旧式电话系统)和 Internet/Intranet 连接起来, 网关一侧连接 Internet, 另一侧与 PSTN 相连。它能够把来自 Internet 网的 IP 包经过解包、解压缩后, 经过数/模变换成模拟语音信号传送给 PSTN; 也能够把来自 PSTN 的电话语音信号经过模/数转换, 压缩打包成适合在 Internet 中传送的 IP 包, 送往 Internet 传输。

用户使用普通电话首先拨打 IP 电话网关提供的号码, 然后类似于使用 300 卡智能网业务, 输入账号和密码, IP 网关对用户确认后, 根据用户拨打的被叫用户的电话号码寻找一条最佳路由, 连接到被叫电话最近的网关, 最后由该网关实现对被叫用户的呼叫, 这样两个普通电话用户便可以经过 Internet/Intranet 进行通话。

使用 IP 电话的 VoIP, 即图 13-1 中的下半部分, 与使用传统电话的区别是, IP 电话可直接输出和接收数字信号, 不再需要数据模转换过程。有关这一部分内容, 读者可以在实验 13-1 和实验 13-2 中动手实践, 亲身体会。

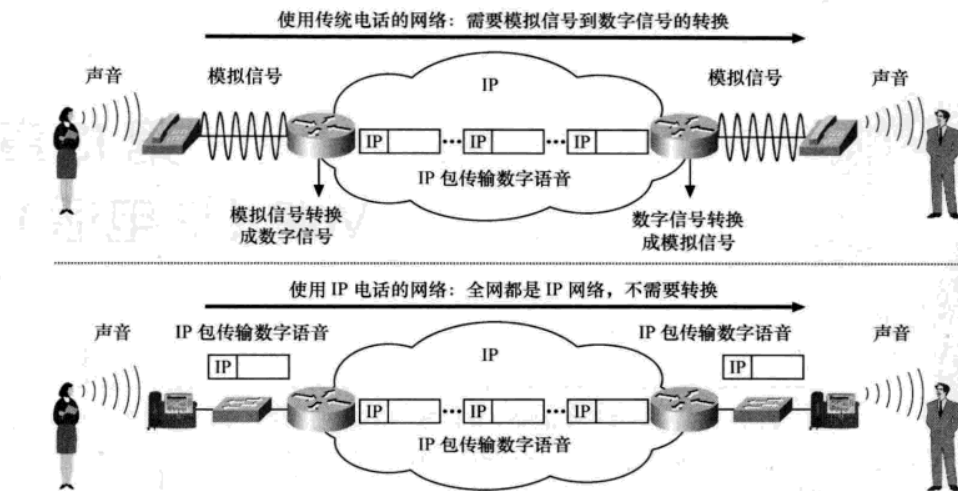


图 13-1-1 VoIP 连接图

【快问快答】什么是 VoIP?

答: VoIP 是传输语音的一种方式, 它把语音分解成构成数据的字节通过互联网传输到目的地。在目的地, 这些被传输过来的字节再被还原成语音。语音就像网页及音频文件等其他互联网数据一样在网络上传输。普通电话要求用户使有一个专用电路, 而 VoIP 是利用所有用户共享的互联网空间。因此, VoIP 技术的效率要高于普通电话技术。

【快问快答】如何使用 VoIP?

答: 普通电话机就只能作为电话机使用。而 VoIP 电话机的种类有许多种, 它可以是一个硬件设备, 它看起来像普通电话, 但它有一个可以连入宽带网的内核。VoIP 电话机还可以是一个软电话机, 也就是一个可以把用户的计算机转换成 VoIP 的软件程序。本章实验中使用的 VoIP 电话机就是软电话机。

【快问快答】除了省钱, VoIP 还具有哪些优点?

答: 由于 VoIP 是直接指向一个 IP 地址而不是一个特定地点, 因此 VoIP 提供商可以开发出许多普通电话很难具备的功能。例如, 具备方便的电话号码在线查找功能, 还可以像接收电子邮件那样接收语音邮件, 方便地进行语音留言; 还可以在任何一个宽带连接处接入 VoIP, 配置后可以直接使用。

【快问快答】VoIP 有哪些不足?

答: VoIP 已经得到了很大的改进, 但是 VoIP 的通话质量仍比不上普通电话, 特别是 VoIP 与普通电话之间的通话更是如此。如果是在一个局域网内使用 VoIP, 那么通话质量不成问题。

13.2 VoIP 模块的接口类型

如果使用是传统电话, 则需要进行数/模和模/数转换, 这就需要专门的语音模块, 如图 13-2-1 所示。PBX (Private Branch eXchange) 是指电信专用分组交换机, 而 PSTN 是指公共交换电话网

络。FXO 和 FXS 是模块的接口类型, 成对出现, 一端是 FXO, 而另一端就是 FXS。

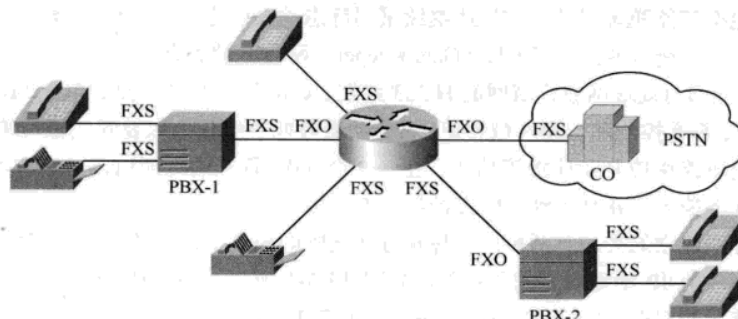


图 13-2-1 语音模块的接口类型

FXS (Foreign Exchange Station Interface) 就是通常的普通电话业务接口。它的物理接口是常用的 RJ-11 接口。标准家庭电话线就被配置为 FXS。FXS 口可以直接与普通电话机或传真机相连, 也就是如果想连接传统的语音电话, 路由器上需要添加的是 FXS 模块。如公司总部在北京, 还有一个分部在南京, 总部和分部之间经常需交流, 可以在南京和北京的路由器上各添加一块 FXS 的语音模块, 这种语音模块上提供了 RJ-11 接口, 直接把普通电话接到 FXS 模块上, 然后稍加配置, 北京和南京之间就可以进行 VoIP 通话了, 电话号码可以自己指定, 没有通话费用。该内容在 13.4 小节有具体的配置。

FXO (Foreign Exchange Office Interface) 就是二线环路中继接口。它采用 RJ-11 接口, 可以直接与 PBX 相连。一般用来连接程控交换机, 如要用路由器来连接到 PSTN, 则需添加的是 FXO 模块。如图 13-2-2 所示为真实的实验, 在南京放置一台路由器, 把该路由器配置成语音网关, 如何把路由器配置成语音网关, 将 13.4 小节进行介绍。在北京的计算机上安装软件, 这样计算机就成为软 IP 电话机。配置软电话机, 使之连接到南京的语音网关上, 在软电话机上拨“066666666”就连接到普通电话机“025-66666666”, 通话质量还可以, 虽然在北京打电话, 却是按南京本地的市话费标准计费, 如果对方开通了来电显示, 看到的号码将是“77777777”。

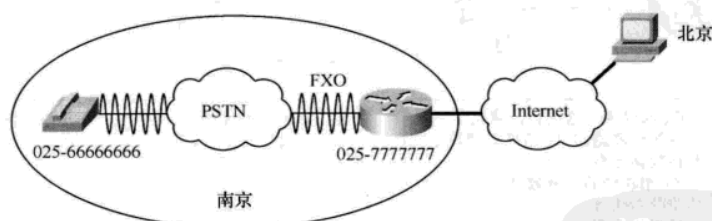


图 13-2-2 异地用计算机呼叫普通电话

13.3 呼叫建立的过程

在进行 VoIP 的呼叫时, 语音网关根据用户拨打的号码, 需要去查找该电话号码的语音网关的 IP 地址, 然后和对方的语音网关建立呼叫连接, 所以在路由器内部需要维护一份电话号码和语音网关的 IP 地址对应的关系表, 在 VoIP 网络规模比较小的时候, 可以将这对应关系直接利用命令

行的方式,静态配置到路由器内部,但是当 VoIP 网络的规模增大时,而且这种对应关系可能会随时发生变动,也有可能随时增减,如果还继续采用静态的映射方式,在路由器内部维护这种对应关系,便很困难了,所以便引入了 GK (Gate Keeper, 网守) 的概念。

GK 是一个能够对局域网或广域网的 H.323 终端、GW 或一些多点控制单元 MCU, 提供地址翻译、访问许可、带宽控制和管理区域管理、安全检查呼叫控制信令以及呼叫管理等功能的 H.323 实体,有时也提供路由控制和计费等功能。在一个由 GK 管理的区域内,对所有呼叫来说, GK 不仅提供呼叫业务控制,并且起到了中心控制点的作用。

根据建立呼叫建立的类型有两种:一种是分布式呼叫建立,每台路由器内部需要维护一份电话号码和语音网关的 IP 地址对应的关系表,如图 13-3-1 所示;另一种是集中式呼叫建立,每台路由器把呼叫转发到 GK,由 GK 查找呼叫路由,如图 13-3-2 所示。

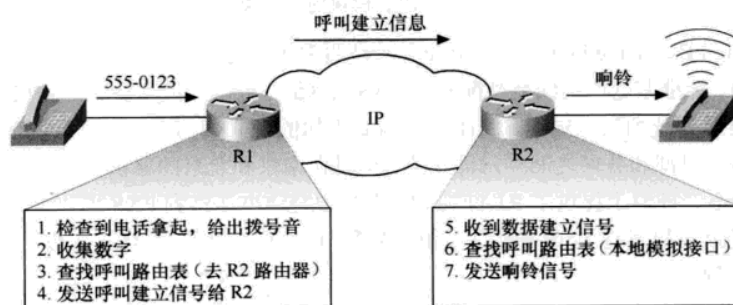


图 13-3-1 分布式呼叫建立的过程

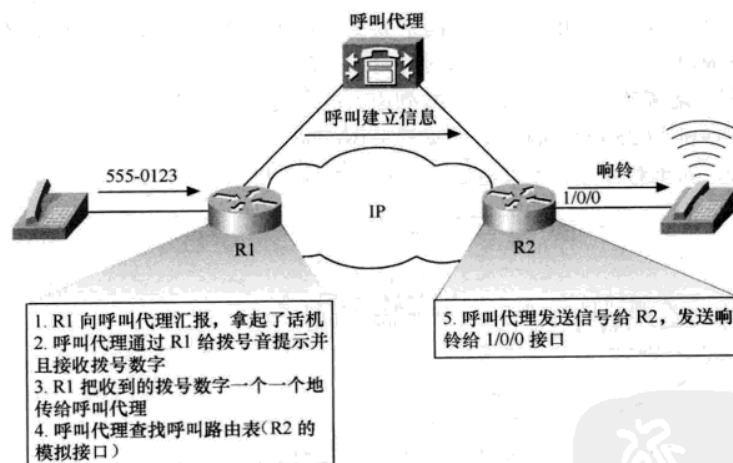


图 13-3-2 集中式呼叫建立的过程

如图 13-3-1 所示是分布式呼叫建立的过程,具体说明如下。

- (1) 路由器 R1 (这里充当语音网关) 检查到用户拿起电话, 路由器给出拨号音。
- (2) 路由器 R1 收集用户的数字拨号。
- (3) 路由器 R1 查找呼叫路由表 (去 R2 路由器)。
- (4) 路由器 R1 发送呼叫建立信号给路由器 R2。

(5) 路由器 R2 收到呼叫建立信号。

(6) 路由器 R2 查找呼叫路由表, 发现被呼叫号码是本地的模拟接口。

(7) 路由器 R2 发送响铃信号给电话机。

在分布式呼叫中, 本地路由器能自动决定路由, 不需要依赖其他设备。这种方式可扩展性不强, 不便于大范围的部署。

如图 13-3-2 所示为集中式呼叫建立的过程, 具体说明如下。

(1) R1 向呼叫代理汇报, 用户拿起了话机。

(2) 呼叫代理通知 R1 给用户拨号音提示, 并且接收拨号数字。

(3) R1 把收到的拨号数字一个一个地传给呼叫代理。

(4) 呼叫代理查找呼叫路由表, 找到该电话号码配置在路由器 R2 上。

(5) 呼叫代理发送信号给 R2, R2 发送响铃给 1/0/0 接口的电话机。

在集中式呼叫中, 本地路由器不能决定呼叫路由, 需要把请求转发给呼叫代理, 呼叫代理查找呼叫路由表, 然后两个语音路由器之间建立起连接。连接建立以后, 两个语音路由器间直接通信, 不涉及呼叫代理。

13.4 VoIP 电话的配置

本节介绍 VoIP 电话的配置和测试, 如图 13-4-1 所示是一个公司总部和分部之间的 VoIP 连接拓扑和 VoIP 相关配置。因为没有物理设备, 图 13-4-1 中的配置读者无法动手完成, 但可以动手实践实验 13-1 和实验 13-2。R1 的配置和说明如下。

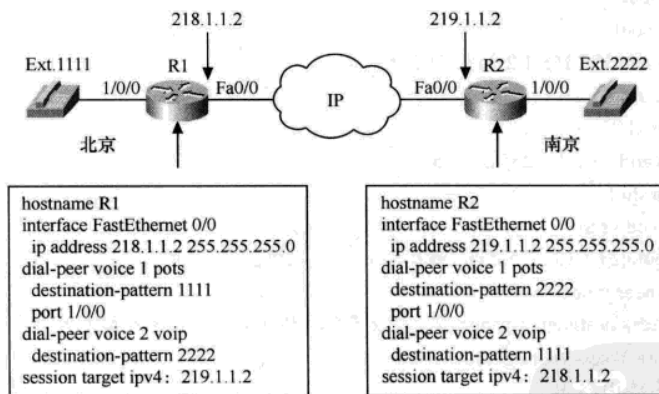


图 13-4-1 分布式呼叫建立的配置

```

R1(config)#int fa 0/0
R1(config-if)#ip add 218.1.1.2 255.255.255.0
R1(config)#dial-peer voice 1 pots    配置语音端口 1, 该接口类型是 pots, 接的是模拟电话
R1(config-dial-peer)#destination-pattern 1111    模拟电话被分配的号码是 1111
R1(config-dial-peer)#port 1/0/0    语音端口 1 使用的 port 1/0/0 物理接口, 也就是说接在 port 1/0/0 接口的模拟电话被分配的号码是 1111
  
```

R1(config)#dial-peer voice 2 voip 配置语音端口 1, 该接口类型是 voip, 使用 IP 传输
 R1(config-dial-peer)#destination-pattern 2222 对方的号码是 2222
 R1(config-dial-peer)#session target ipv4:219.1.1.2 目标在 219.1.1.2, 也就是说如果要拨打 2222 号码, 路由器把呼叫路由到 219.1.1.2 这个设备上, 也就是如图 13-4-1 所示的路由器 R2

在两台虚拟机上安装“VTGO-PC”来模拟 IP 电话, 使用语音机架完成本章实验。接口和 IP 地址的配置如图 13-4-2 所示, 虚拟机 1 安装 VTGO-PC 软件后, 将会被分配到电话号码“2001”, 虚拟机 2 安装 VTGO-PC 软件后, 将会被分配到电话号码“1001”。

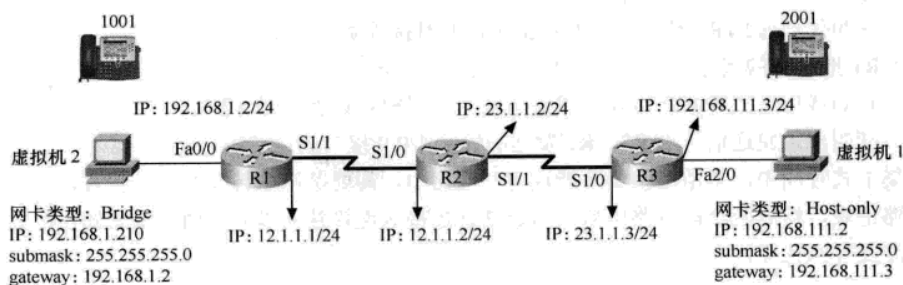


图 13-4-2 VoIP 配置拓扑图

实验 13-1 分布式 IP 电话部署

R1 和 R3 充当语音网关, R2 相当于是互联网, 具体配置的步骤如下。

STEP 1 配置路由器 R1。配置和解释如下:

```
Router#conf t
Router(config)#host R1
R1(config)#int fa 0/0
R1(config-if)#ip add 192.168.1.2 255.255.255.0
R1(config-if)#no shut
R1(config-if)#int s1/1
R1(config-if)#ip add 12.1.1.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#no cdp run
R1(config)#ip route 23.1.1.0 255.255.255.0 12.1.1.2 配置静态路由
R1(config)#dial-peer voice 1 voip
R1(config-dial-peer)#destination-pattern 2... 以 2 开始的所有 4 位电话号码都发给 IP 地址为 23.1.1.3 的设备
R1(config-dial-peer)#session target ipv4:23.1.1.3
```

STEP 2 配置路由器 R2。

```
Router#conf t
Router(config)#host R2
R2(config)#int s1/0
R2(config-if)#ip add 12.1.1.2 255.255.255.0
R2(config-if)#no shut
R2(config-if)#int s1/1
R2(config-if)#ip add 23.1.1.2 255.255.255.0
R2(config-if)#no shut
```

STEP 3 配置路由器 R3。

```

Router>en
Router#conf t
Router(config)#host R3
R3(config)#int s1/0
R3(config-if)#ip add 23.1.1.3 255.255.255.0
R3(config-if)#no shut
R3(config-if)#int fa 2/0
R3(config-if)#ip add 192.168.111.3 255.255.255.0
R3(config-if)#no shut
R3(config)#no cdp run
R3(config)#ip route 12.1.1.0 255.255.255.0 23.1.1.2
R3(config)#dial-peer voice 1 voip
R3(config-dial-peer)#destination-pattern 1...
R3(config-dial-peer)#session target ipv4:12.1.1.1

```

STEP 4 配置路由器 R1 支持 IP 电话，配置步骤如下：

R1 (config) #telephony-service setup 配置电话服务

--- Cisco IOS Telephony Services Setup ---

Do you want to setup DHCP service for your IP Phones? [yes/no]: no 要不要为 IP 电话提供 DHCP 服务？

Do you want to start telephony-service setup? [yes/no]: yes 要开始建立电话服务吗？

Configuring Cisco IOS Telephony Services :

Enter the IP source address for Cisco IOS Telephony Services :192.168.1.2 用户提供 IP 电话服务的 IP 地址是多少？填入路由器一个地址，IP 电话机需要提供这个地址

Enter the Skinny Port for Cisco IOS Telephony Services : [2000]: 提供 IP 电话服务的端口是多少？直接回车使用默认的 2000 号端口，IP 电话机上默认使用的就是 2000 号端口

How many IP phones do you want to configure : [0]: 5 这台路由器要支持几部 IP 电话？

Do you want dual-line extensions assigned to phones? [yes/no]: no 没有关系的设置，回答 NO 就可以了

What Language do you want on IP phones :

- 0 English
- 1 French
- 2 German
- 3 Russian
- 4 Spanish
- 5 Italian
- 6 Dutch
- 7 Norwegian
- 8 Portuguese
- 9 Danish
- 10 Swedish
- 11 Japanese

[0]: 直接按下回车键

Which Call Progress tone set do you want on IP phones :

- 0 United States

- 1 France
- 2 Germany
- 3 Russia
- 4 Spain
- 5 Italy
- 6 Netherlands
- 7 Norway
- 8 Portugal
- 9 UK
- 10 Denmark
- 11 Switzerland
- 12 Sweden
- 13 Austria
- 14 Canada
- 15 Japan

[0]: 直接按下回车键

What is the first extension number you want to configure : 1001 起始的电话号码是多少? 这里填的是本地要分配的号码, 因要支持 5 部电话, 号码是从 1001 至 1005, 连续的 5 个号码

Do you have Direct-Inward-Dial service for all your phones? [yes/no]: no 没有关系的设置, 回答 NO 就可以了

Do you want to forward calls to a voice message service? [yes/no]: no 没有关系的设置, 回答 NO 就可以了

Do you wish to change any of the above information? [yes/no]: no 没有关系的设置, 回答 NO 就可以了

CNF-FILES: Clock is not set or synchronized, retaining old versionStamps

---- Setup completed config ---

R1(config)#

STEP 5 配置路由器 R3 支持 IP 电话。配置步骤类似第 4 步, 但要把 IP 地址从“192.168.1.2”改成“192.168.111.3”, 第一个电话号码从“1001”改成“2001”, 其他步骤一样。

STEP 6 在两台虚拟机上安装声卡。编辑两台虚拟机, 添加声卡硬件, 如图 13-4-3 所示。

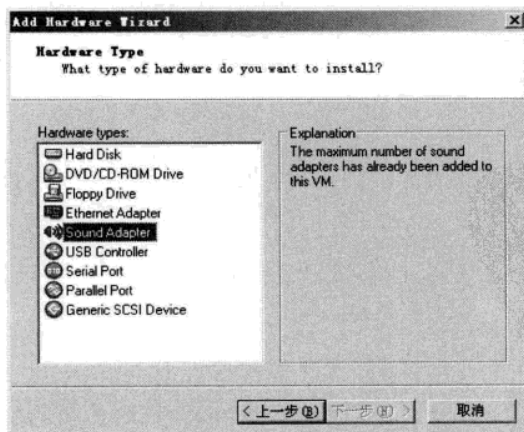


图 13-4-3 添加声卡

特别值得一提的是, 添加的声卡类型和真实机上安装的声卡类型并不一样, 而是“Sound Blaster Audio PCI”类型, 下载的 network.rar 软件包中提供了该网卡的驱动, 把文件“bicrew98.exe”复制到一个空的文件夹, 双击“bicrew98.exe”文件, 弹出如图 13-4-4 所示的窗口, 按下“y”键, 网卡驱动文件被解压缩到当前文件夹中。

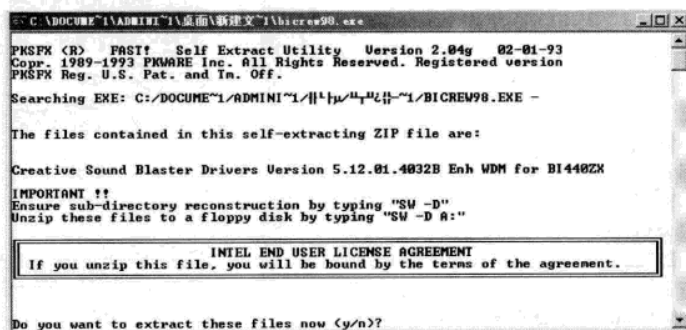


图 13-4-4 释放压缩文件

该声卡的安装不像一般声卡驱动的安装, 比较简单。为了读者能顺利完成安装, 这里给出具体步骤。双击解压后“SBSETUP.EXE”文件, 弹出如图 13-4-5 所示的对话框, 选择“安装软件”, 单击“下一步”按钮继续, 开始安装声卡驱动。

像安装很多软件一样, 系统会提示兼容性问题, 单击“仍然继续”。系统又提示找不到某些文件, 复制错误, 如图 13-4-6 所示, 单击“浏览”按钮, 定位到刚才驱动被解压缩的文件夹, 单击“重试”按钮, 完成驱动程序的安装。

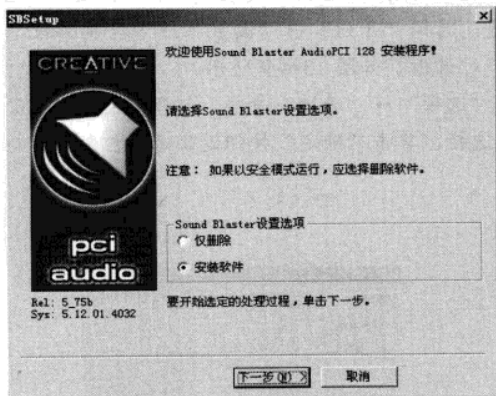


图 13-4-5 安装声卡驱动

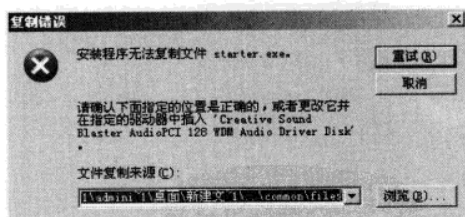


图 13-4-6 复制错误

提示安装完成, 但从“设备管理器”窗口中, 发现该设备前面还有个感叹号, 选中该设备, 在右键快捷菜单中单击“更新驱动程序”, 如图 13-4-7 所示, 定位到驱动程序文件夹, 类似前面的兼容性提示和复制错误还会再出现一次, 同上操作, 更新后声卡设备显示正常。

现在声卡还不能使用, 选择“控制面板”的“声音和音频设备”, 打开“声音和音频设备属性”对话框, 如图 13-4-8 所示, 选中“启用 Windows 音频”复选框, 单击“确定”按钮, 重启计算机,

声卡可以使用了。

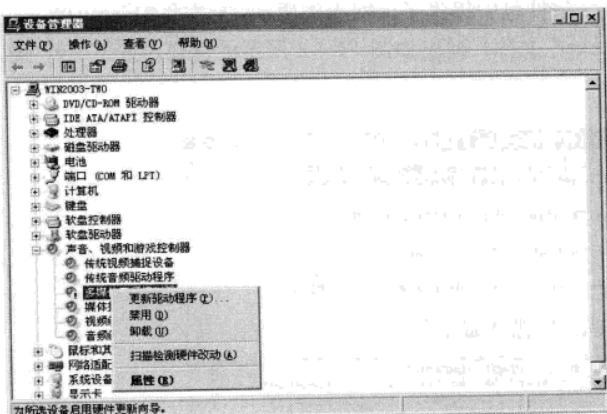


图 13-4-7 更新驱动程序

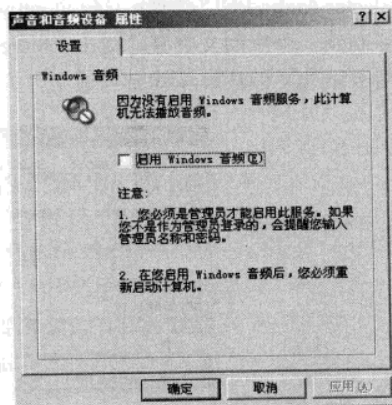


图 13-4-8 启用音频

STEP 7 配置虚拟机的 IP 地址。配置虚拟机 1 网络参数，网卡类型 host-only，IP 地址 192.168.111.2，子网掩码 255.255.255.0，网关 192.168.111.3，DNS 为 218.2.135.1；配置虚拟机 2 网络参数，网卡类型 Bridged，IP 地址 192.168.1.210，子网掩码 255.255.255.0，网关 192.168.1.2，DNS 为 218.2.135.1。

STEP 8 在两台虚拟机上安装 IP 电话软件。在两台虚拟机上解压缩“VTGO-PC.zip”文件，双击“VTGO-PC Advanced 2.10.1.msi”进行安装，安装过程比较简单。安装完成后，把压缩包中的“VTGO-PC.exe”复制到安装目录，覆盖同名文件，双击“induct.reg”文件，导入注册表完成破解。

STEP 9 设置麦克风。这里演示虚拟机 2 的设置，确保声卡被正确安装，不然 VTGO-PC 无法正常运行。声卡安装成后，取消麦克风的静音设置，选择“开始”→“设置”→“控制面板”→“声音和音频设备”，打开“声音和音频设备属性”对话框，如图 13-4-9 所示。

单击“高级”按钮，打开音量控制窗口，选择“选项”→“属性”命令，打开如图 13-4-10 所示的音量控制属性对话框，选中“麦克风音量”复选框，单击“确定”按钮返回音量控制对话框。

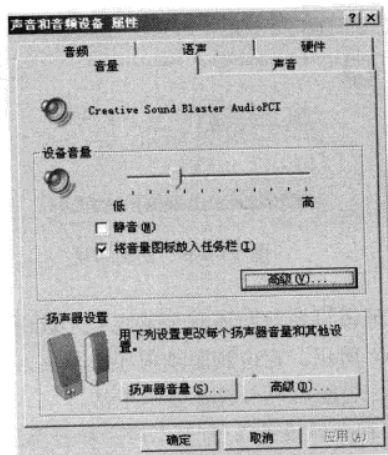


图 13-4-9 设置声音和音频设备属性

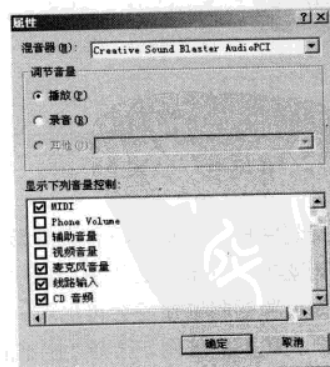


图 13-4-10 音频属性

在“音量控制”对话框中,取消麦克风音量下方的“静音”复选框,如图 13-4-11 所示。

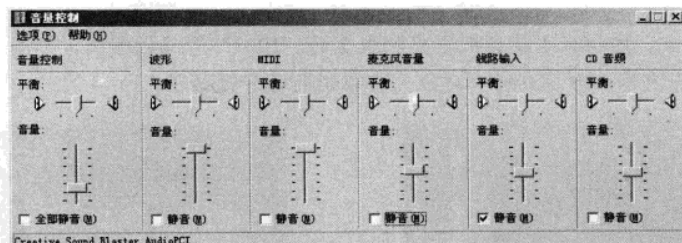


图 13-4-11 音量控制

STEP 10 设置 VTGO-PC。第一次运行 VTGO-PC, 自动执行配置向导。第 1 步是选择声音设备, 直接单击“Next”按钮继续; 第 2 步是测试音箱和麦克风音量, 如图 13-4-12 所示, 单击图中的“Headset”或“Speaker”按钮, 然后对着麦克风说话, 5 秒钟后自动回放, 单击“Next”按钮继续。

第 3 步是询问网络连接, 单击“Next”按钮继续; 第 4 步比较关键, 设置 VoIP 服务器的 IP 地址, 如图 13-4-13 所示, 填入路由器 R1 的 Fa0/0 接口的 IP 地址“192.168.1.2”, 虚拟机 1 则填入路由器 R3 的 Fa2/0 接口的 IP 地址“192.168.111.3”。单击“Next”按钮, 完成向导。

VTGO-PC 启动后, 提示要使用软电话, 需要设置 CallManager (呼叫中心) 的 IP 地址。单击 VTGO-PC 的“Tools menu”, 打开“Settings”对话框, 如图 13-4-14 所示, 在“Primary CallManager”后填入语音路由器的 IP 地址 192.168.1.2, 单击“确定”按钮, 完成配置。

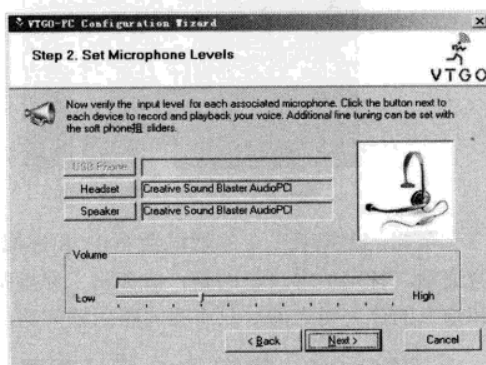


图 13-4-12 调节音量

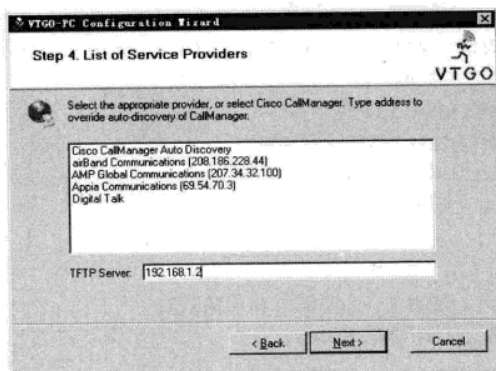


图 13-4-13 配置语音网关的地址

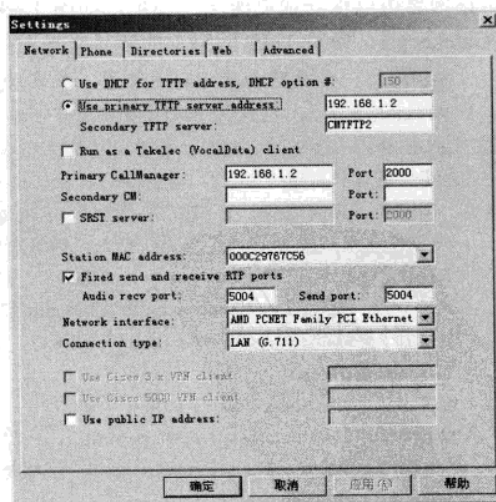


图 13-4-14 配置 CallManager 地址

STEP 11 测试。虚拟机 2 被分配了一个电话号码“1001”，如图 13-4-15 所示，呼叫“2001”电话号码。

STEP 12 测试。虚拟机 1 收到来自虚拟机 2 的“1001”号码的呼叫，如图 13-4-16 所示。单击“Answer”进行应答，IP 电话呼叫建立，可以进行语音通话了。



图 13-4-15 软 IP 电话界面



图 13-4-16 IP 电话正在被呼叫

至此，虚拟机 1 上的软电话 2001 和虚拟机 2 上的软电话 1001 之间建立了连接，可以进行语音通话。特别值得注意的是，虚拟机 1 和虚拟机 2 之间的路由是不通的，也就是说北京的总公司和南京的分公司之间，只有语音路由器间路由可达，内部的使用什么 IP 地址是没有关系的。

实验 13-2 集中式 IP 电话部署

实验 13-1 完成了分布式电话的部署，但如果公司规模很大，遍布全球，每个分公司要和集团内的所有公司通话，就需要在每个分公司路由器上添加所有分公司的电话号码和对应的 IP 地址，不仅工作量大，而且关键是不灵活，一个分公司有变动，所有的分公司都要跟着变动。集中式 IP 电话部署可以很好地克服这一不足，如图 13-4-2 所示，R1 和 R3 充当 GK 客户端，R2 充当 GK (Gatekeeper，负责 VoIP 网路上的信号交换及控制功能)。

STEP 1 更改路由器 R1 的配置。在实验 13-1 的基础上，进行如下配置：

R1(config)#int s1/1 路由器作为语音网关设备，当配置成为 GK Client 方式来管理时，需要和网络上的 GK Server 进行交互通信，将路由器自身的信息在 GK Server 上注册，同时从 GK Server 上得到其他的语音网关的信息，所以要指定一个接口，用来和 GKServer 进行通信，该接口就是 H.323 网关接口，以太网口、异步串口、同步口等都可以成为 H.323 网关接口，只有在指定 H.323 网关接口后，GK Client 功能才能被激活。

注意：这里配置的不能是 Fa0/0 接口，因 R2 没有 192.168.1.0/24 的路由

R1(config-if)#h323-gateway voip interface 指定该接口为 H.323 语音网关接口

R1(config-if)#h323-gateway voip id R2 ipaddr 12.1.1.2 1719 配置 GK Server 的名称和 IP 地址

R1(config-if)#h323-gateway voip h323-id R1 配置本设备显示在 GK 上的名字

R1(config-if)#exit

R1(config)#dial-peer voice 1 voip

R1(config-dial-peer)#destination-pattern 除本地外，所有的 4 位号码，相当默认路由

R1(config-dial-peer)#session target ras 目标是 RAS，相当于 GK Server

R1(config-dial-peer)#exit

R1(config)#gateway 激活该语音网关的 GK Client 功能，前面加 no 是关闭

STEP 2 更改路由器 R2 的配置。在实验 13-1 的基础上, 进行如下配置:

```
R2(config)#gatekeeper    进入 GK Server 配置模式
R2(config-gk)#zone local R2 test.com 12.1.1.2    配置本地 GK Server 信息
R2(config-gk)#no shut    启动 GK Server 服务
```

STEP 3 更改路由器 R3 的配置。在实验 13-1 的基础上, 进行如下配置:

```
R3(config)#int s1/0
R3(config-if)#h323-gateway voip interface
R3(config-if)#h323-gateway voip id R2 ipaddr 12.1.1.2 1719
R3(config-if)#h323-gateway voip h323-id R3
R3(config-if)#exit
R3(config)#dial-peer voice 1 voip
R3(config-dial-peer)#destination-pattern ....
R3(config-dial-peer)#session target ras
R3(config-dial-peer)#exit
R3(config)#gateway
```

接下来的配置及测试与分布式 IP 电话的部署相同。如果路由器配置正确, 将可以在 R1 和 R3 上看到“Gateway R1 registered with Gatekeeper R2”和“Gateway R3 registered with Gatekeeper R2”。表示 R1 和 R3 成功在 R2 上被注册, 在 R2 上进行查看, 如图 13-4-17 所示。可以看到 R1 和 R3 的电话号码均在 R2 上被成功注册, 这里显示的信息可以动态更新, 在 R3 上进行如下操作:

```
R3(config-if)#int s1/0
R3(config-if)#no h323-gateway voip interface    取消注册
```

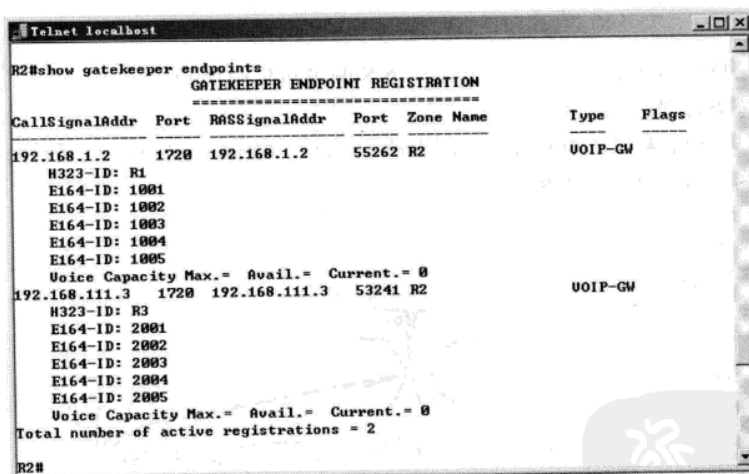
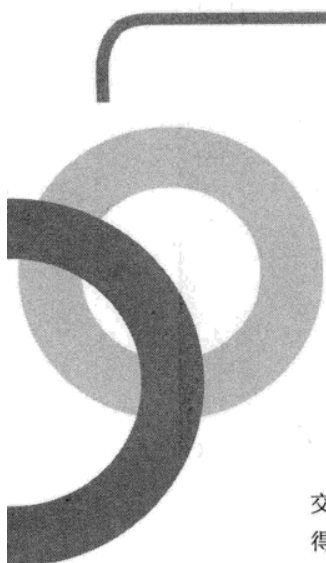


图 13-4-17 显示 Gatekeeper 上注册的终端

在 R2 上再次使用命令“show gatekeeper endpoints”查看时, 将只能看到 R1 注册的电话号码。

从上面的配置中可以看出, GK Client 只需要向 GK Server 注册, 并配置默认的呼叫路由, 即可成功呼叫 GK Server 上注册的所有 GK Client。假如有新的 GK Client 加入, 所有现存的 GK Server 和 GK Client 不需要任何改动。集中式电话部署扩展性更强, 适于大规模的部署。



第 14 章 SolarWinds 网管系统

Chapter 14

随着计算机网络规模爆炸式增长，越来越多的网络设备（包括防火墙、路由器、交换机和服务器）被加入到网络中来，厂家不一、型号各异的众多设备使网络管理变得越来越复杂和难以驾驭。如何更有效地利用企业 IT 资源，实现稳定的网络支持和网络效益一直是网络管理者们备感棘手的问题，SolarWinds 网管系统可以井然有序、简单易行并及时高效地管理各种网络资源。

14.1 功能简介

这里结合某单位的网络应用，简单介绍一下 SolarWinds 的功能。

(1) 设备分类管理。

将各类设备，如思科、华为和锐捷的网络设备，以及 Windows 和 Linux 系统的服务器等自动分类管理，如图 14-1-1 所示的左侧列表栏。

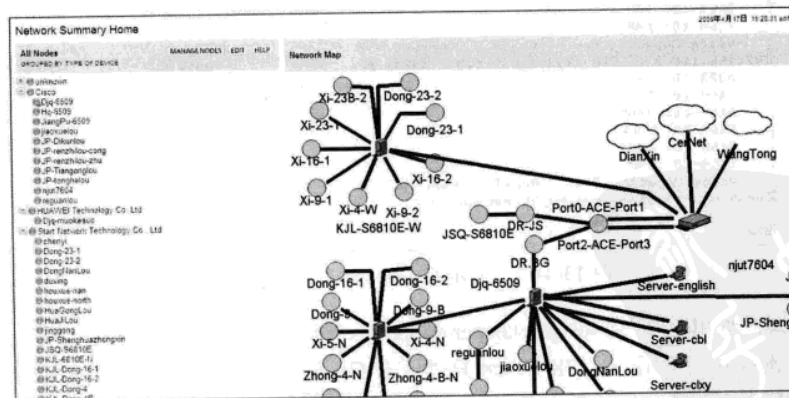


图 14-1-1 设备分类管理

(2) 企业拓扑管理。

将企业所有的网络设备，包括路由器、交换机、服务器和计算机，以及所有可配置 IP 地址的设备统一管理起来，并在如图 14-1-2 所示的页面中描述这些设备之间的连接关系，使网络管理员可以一目了然地查看全公司的网络设备的连接状态和运行状况。当实际的设备或线缆故障时，图中的相应图标会显示为红色。而在设备运转正常的情况下，可以单击设备，打开设备详细信息的查看窗口。

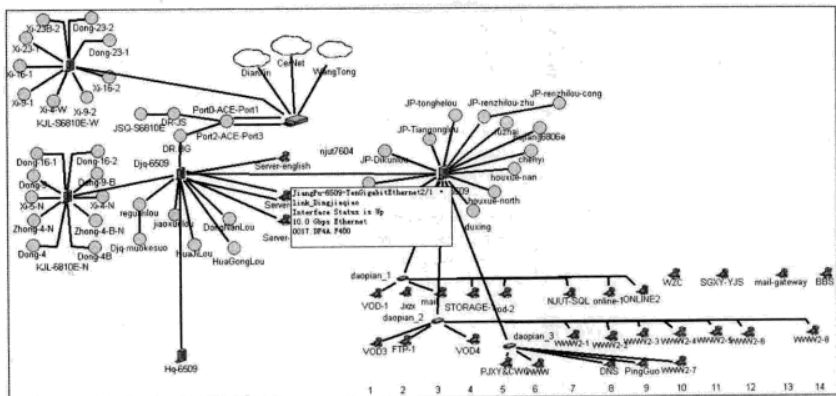


图 14-1-2 设备之间的连接关系

(3) 故障报警功能。

当某台设备或接口发生故障时，系统可以发出声音报警，也可以发送邮件等。如图 14-1-3 所示为“Xi-9-1”交换机发生故障时网络管理计算机收到的信息，提示该交换机故障。网络管理员还可以定制 CPU、内存及带宽利用率报警等选项。

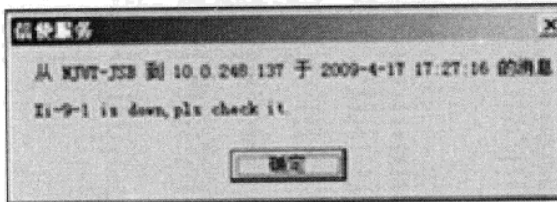
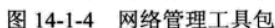


图 14-1-3 报警信息

(4) 网络管理工具。

可以安装 SolarWinds 的管理工具包, 其中 IP Network Browser 用于扫描与设定的 SNMP 字符串相同的网络设备; Trace Route 用于跟踪路由, 查看经过的路由地址; Ping 用于 ping 主机; Web Browse 用于以 Web 方式管理设备; DNS Analysis 用于扫描定位本地 DNS 数据库错误; Telnet 用于设备的远程登录; CPU Gauge 用于监控 win2k、Cisco 路由器或交换机 CPU 的工作状况; Real-Time Interface Monitor 用于监控设备端口的实时利用情况; Remote Desktop 用于远程桌面连接 Windows 系统, 如图 14-1-4 所示。



当网络异常时可以查看，找出异常的端口，然后隔离故障的影响范围，如图 14-1-5 所示。

图 14-1-5 核心设备每个端口的实时流量情况

可以查看设备 CPU 和内存的利用率情况, 如图 14-1-6 所示。

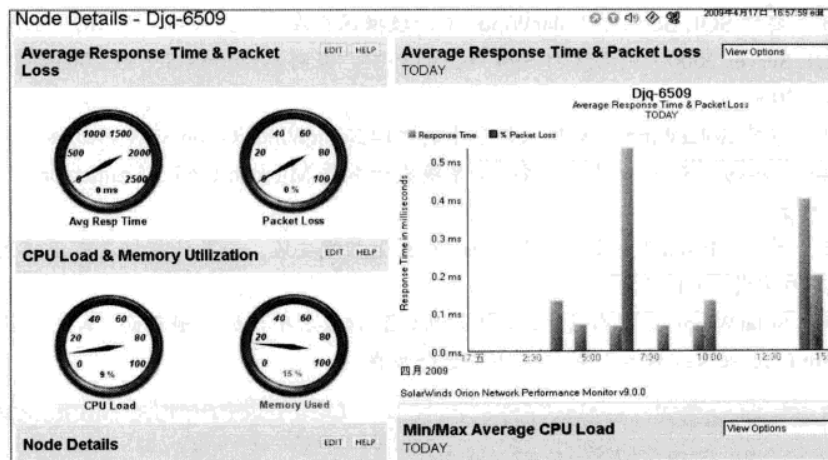


图 14-1-6 CPU 和内存等的利用率

(7) 统计报表。

可以根据需要定制报表，如图 14-1-7 所示为统计接口利用率的报表，网络管理员可以根据需要查询特定信息的统计报表。

Node	Interface	Transmit Traffic	Receive Traffic	Transmit % Utilization	Receive % Utilization
ru47604	GigabitEthernet1/2 to_dianxin1000	889 Mbps	648 Mbps	88 %	84 %
Djq-6509	GigabitEthernet1/3 75045ip-com&acenet-shuan1/19	843 Mbps	635 Mbps	84 %	83 %
Djq-6509	TenGigabitEthernet7/11 To1/1	367 Mbps	266 Mbps	3 %	2 %
ru47604	GigabitEthernet1/1 to_susho_1000000	270 Mbps	306 Mbps	26 %	30 %
Jiangpu-6509	TenGigabitEthernet2/1 link_dongliangao	222 Mbps	302 Mbps	2 %	3 %
JSQ-S6610E	GigabitEthernetSFP 2/1 - G0/1	291 Mbps	211 Mbps	29 %	21 %
Jiangpu-6509	GigabitEthernet1/7 10-10-10-10	282 Mbps	121 Mbps	28 %	12 %
ru47604	GigabitEthernet1/6 To_CERNET	170 Mbps	140 Mbps	16 %	13 %
KJL-6610E-4	GigabitEthernetSFP 3/2 - UPLINK-WLZX-S6506	150 Mbps	52 Mbps	15 %	5 %
Djq-6509	GigabitEthernet1/1 to_chuangdong	74 Mbps	122 Mbps	7 %	12 %
ru47604	MSFC_to_JWCERNET	103 Mbps	53 Mbps	10 %	5 %
Djq-6509	GigabitEthernet1/7 To_HongGuo_XiaoGu	53 Mbps	87 Mbps	5 %	8 %
Jiangpu-6509	GigabitEthernet1/6 shenqiao	37 Mbps	89 Mbps	3 %	8 %
Jiangpu-6509	GigabitEthernet1/11 link_dianxin_susho1	102 Mbps	3.83 Mbps	10 %	0 %
Djq-6509	GigabitEthernet1/9 to_huangshihuan	41 Mbps	56 Mbps	4 %	5 %
Djq-6509	GigabitEthernet1/6 To_Dongliangao	31 Mbps	63 Mbps	3 %	6 %
ru47604	GigabitEthernet1/3 to_chuangdong	41 Mbps	49 Mbps	4 %	4 %
NJUT-S6610E-W	GigabitEthernetSFP 1/24 - UPLINK-WLZX-R7604	47 Mbps	37 Mbps	4 %	3 %
Djq-6509	GigabitEthernet1/3	14 Mbps	40 Mbps	1 %	3 %

图 14-1-7 接口利用率报表

14.2 安装 SolarWinds

安装 SolarWinds 比较简单，但是所需环境较为复杂。本节以 Windows Server 2003 为例，介绍一下 SolarWinds 的安装步骤。

STEP 1 首先将 Windows Server 2003 打 SP2 以上的补丁。

STEP 2 添加 IIS（可参照本书的 4.3.1 小节）。

STEP 3 安装 SQL Server, SolarWinds 中的数据保存在其中, 可以安装 SQL Server 2005。如果只有 SQL Server 2000, 则需要打 SP4 以上的补丁, 否则 Windows Server 2003 不支持低版本的 SQL Server 2000。

STEP 4 安装 SolarWinds, 解压软件包中的 “14\SolarWinds.Orion.SLX.v9.0.rar” 文件。双击 “SolarWinds-Orion-v9.0-SLX.exe” 开始安装, 系统提示需要 Microsoft .NET Framework 3.5 的环境, 如图 14-2-1 所示。

STEP 5 单击 “Install” 按钮, 开始从 Internet 上在线安装。如果计算机没有连接到 Internet, 则需要提前下载安装 .NET 环境。

STEP 6 SolarWinds 安装临近结束, 会出现如图 14-2-2 所示的注册页面。单击 “Skip This and Enter Software License Key Now” 按钮, 跳过这个步骤。

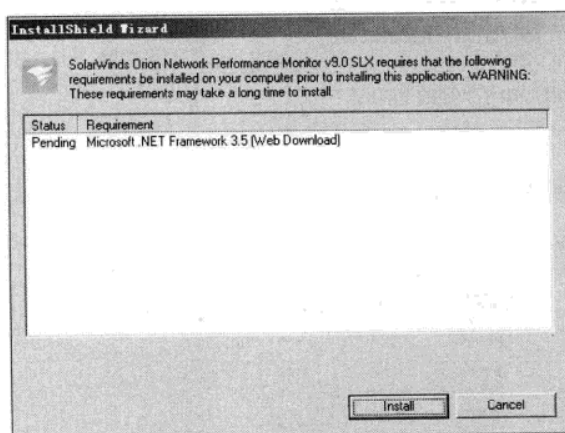


图 14-2-1 提示安装 Microsoft .NET Framework 3.5

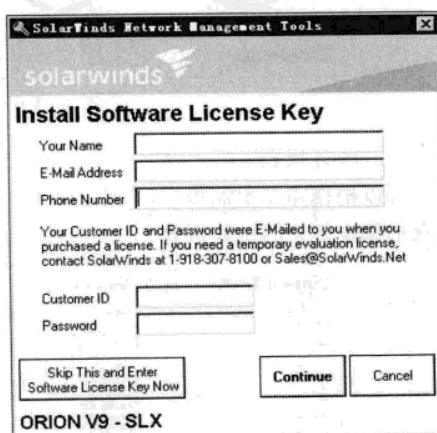


图 14-2-2 注册页面

STEP 7 显示输入注册码页面, 根据 “Software Serial Number” 输入相应的注册码, 如图 14-2-3 所示。

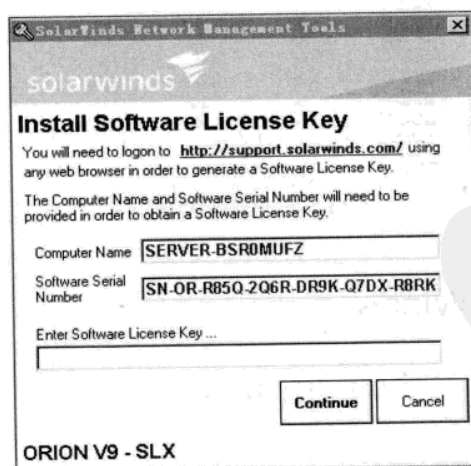


图 14-2-3 输入注册码

14.3 配置 SolarWinds

配置 SolarWinds 的具体操作步骤如下。

14.3.1 配置数据库

STEP 1 单击输入注册的页面中的“Continue”按钮，SolarWinds 弹出配置向导窗口，如图 14-3-1 所示。以后也可以单击“开始”→“程序”→“SolarWinds Orion”→“Configuration Wizard”，再次启动配置向导。

STEP 2 单击“Next”按钮，弹出“Database Settings”对话框，如图 14-3-2 所示。在“SQL Server”下拉列表框中输入 SQL Server 服务器的 IP 地址，如果是在同一台计算机上，则输入“(local)”。

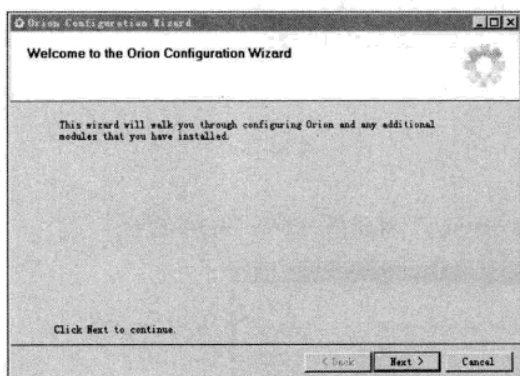


图 14-3-1 配置向导窗口

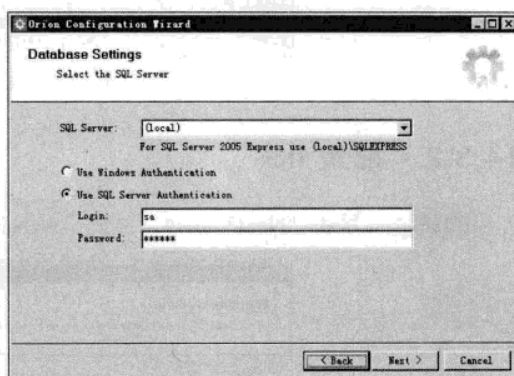


图 14-3-2 “Database Settings”对话框

STEP 3 选择“Use SQL Server Authentication”单选按钮，使用 SQL Server 认证，并在下面的文本框中分别输入 SQL Server 超级管理员账号“sa”和对应的密码。

STEP 4 单击“Next”按钮，弹出“Database Settings”对话框，如图 14-3-3 所示。

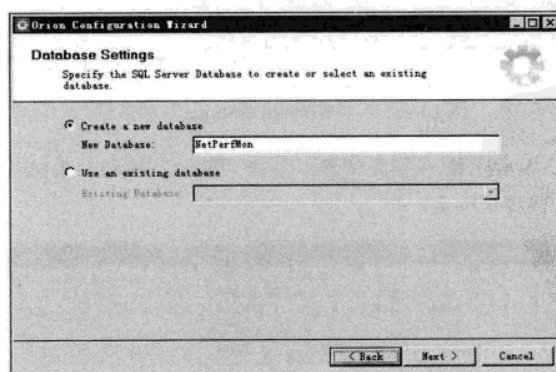


图 14-3-3 创建数据库

STEP 5 输入数据库名, SQL Server 将为 SolarWinds 创建数据库 “NetPerfMon”。单击 “Next” 按钮, 弹出 “Database Account” 对话框, 如图 14-3-4 所示。输入账户名和密码, SQL Server 将为数据库 “NetPerfMon” 创建一个账户, SolarWinds 通过该账户操作 SQL Server 中的 “NetPerfMon” 数据库。

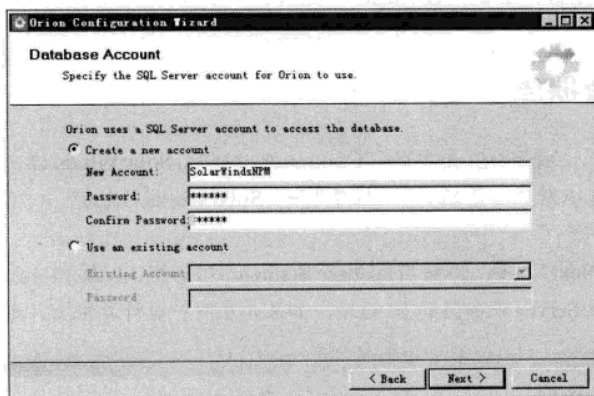


图 14-3-4 “Database Account” 对话框

14.3.2 配置 IIS

STEP 1 单击 “Next” 按钮, 弹出 “Website Settings” 对话框, 如图 14-3-5 所示。

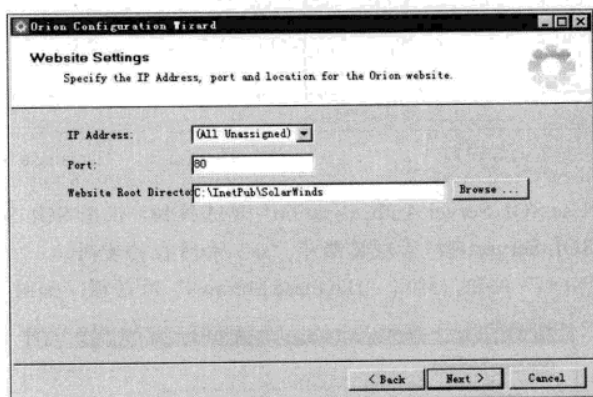


图 14-3-5 “Website Settings” 对话框

STEP 2 如图 14-3-5 所示输入各类信息。单击 “Next” 按钮, 系统提示该 IP 地址和 TCP 的端口已经被占用, 如图 14-3-6 所示。

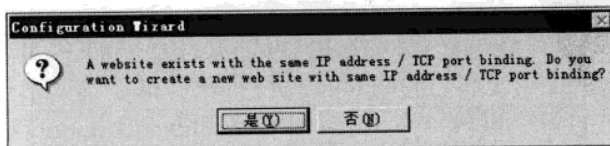


图 14-3-6 站点冲突提示

STEP 3 单击“是”按钮，停用已有且未使用的站点。

14.3.3 设置服务

接下来是服务设置，在如图 14-3-7 所示的“Service Settings”对话框中，保持默认选项。单击“Next”按钮，直到最后完成配置向导。

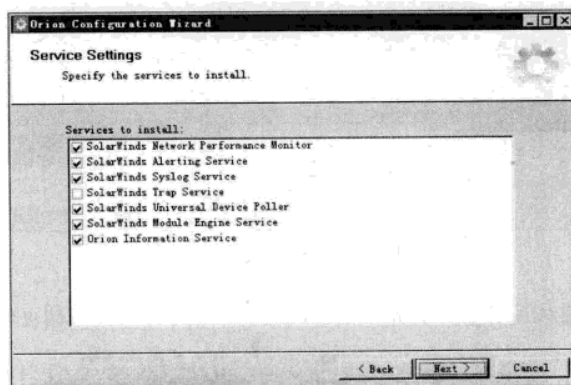


图 14-3-7 “Service Settings”对话框

14.3.4 系统管理

STEP 1 单击“开始”→“程序”→“SolarWinds Orion”→“System Manager”选项，打开系统管理界面，如图 14-3-8 所示。

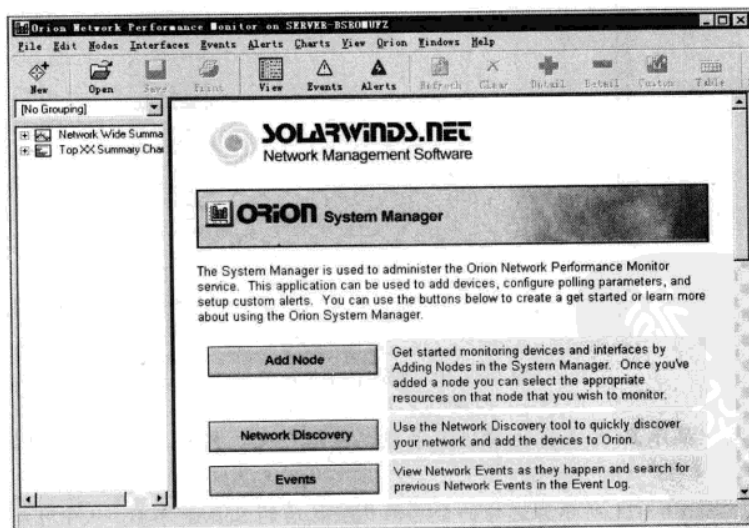


图 14-3-8 系统管理界面

STEP 2 单击“Add Node”按钮，打开“Add Node”对话框，如图 14-3-9 所示。在 IP 地址文本框中输入 ROS 的 IP 地址“10.0.248.231”或其他支持 SNMP 协议设备的 IP 地址，SNMP 使用的端口是 161，SNMP 使用的密钥默认是 public，多数设备都支持 SNMP 版本 2。

STEP 3 在思科交换机路由器上配置 SNMP 密钥的命令如下：

Switch(config)#snmp-server community public ro 其中的 public 是密钥，ro 表示 read-only（只读），rw 表示 read-write（可读可写）。

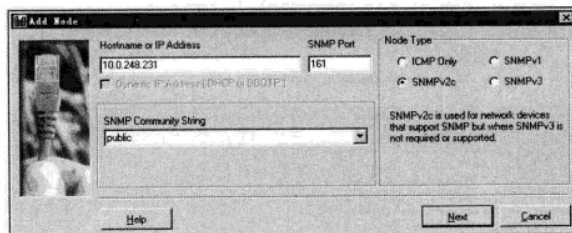


图 14-3-9 “Add Node”对话框

STEP 4 SNMP 连接成功后，打开如图 14-3-10 所示的资源使用情况窗口。

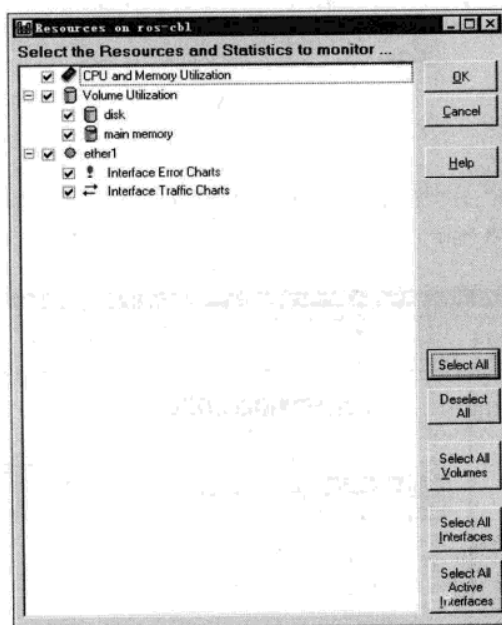


图 14-3-10 资源使用情况窗口

STEP 5 其中显示 ROS 支持的 SNMP 参数，包括 CPU、内存、磁盘及接口的使用情况等。选中关注的对象，单击“OK”按钮。

STEP 6 如图 14-3-11 所示为选择一台思科交换机后的 SNMP 参数，从中可以看到该交换机的端口数量，以及正在使用的端口等。

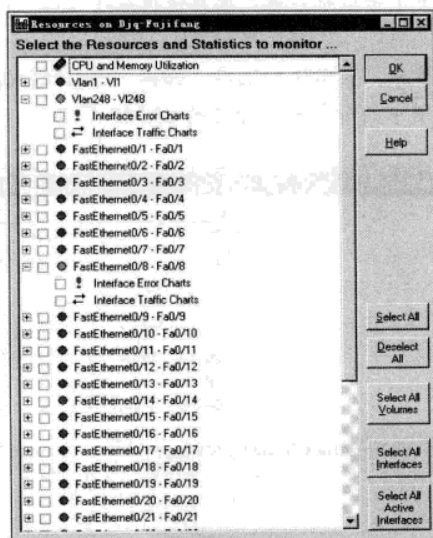


图 14-3-11 一台思科交换机的 SNMP 参数

14.3.5 管理拓扑图

根据网络设备的实际连接和布局情况绘制企业的拓扑图，使得所有设备都在一个界面中直观的显示。

STEP 1 单击“开始”→“程序”→“SolarWinds Orion”→“Map Maker”选项，打开“MapMaker”窗口。单击“New Map”按钮，设计一个新的拓扑，如图 14-3-12 所示。

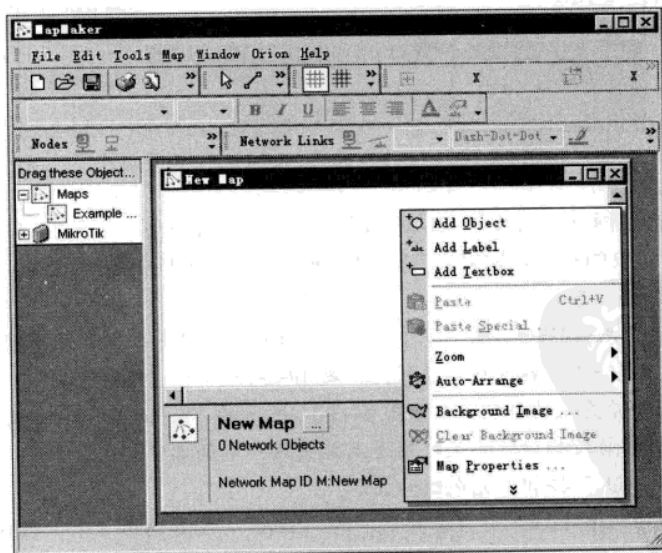


图 14-3-12 设置一个新的拓扑

STEP 2 在新拓扑窗口中单击鼠标右键，选择快捷菜单中的“Add Object”选项，在拓扑图中添加一个新的节点。

STEP 3 右击新添加的节点，显示快捷菜单，选择“Object Properties”（对象属性）选项，如图 14-3-13 所示，关联拓扑图中的对象和要管理的 SNMP 节点。

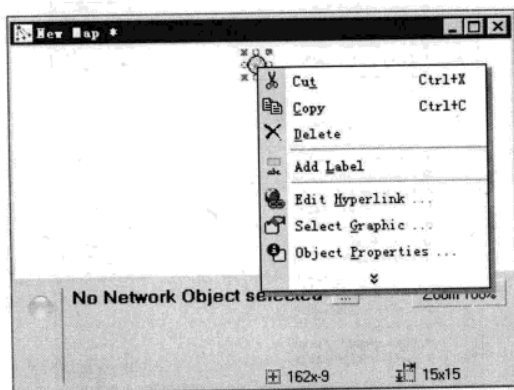


图 14-3-13 快捷菜单

STEP 4 打开“Select Network Object”对话框，如图 14-3-14 所示。从分类中选择欲关联的对象，单击“OK”按钮，完成对象的关联。

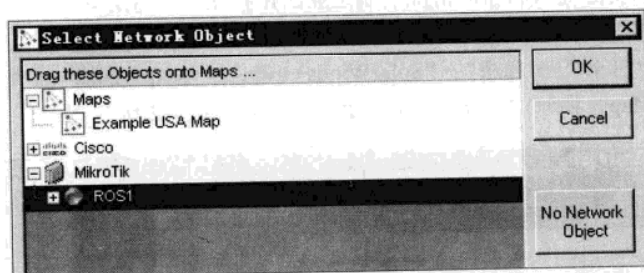


图 14-3-14 “Select Network Object”对话框

以类似方法，添加网络中的其他 SNMP 管理节点，可以是交换机、路由器、服务器和计算机等所有支持 SNMP 协议的设备。如果不支持 SNMP 协议，只要能配置 IP 地址，也可以通过 ping 命令测试设备是否在线。

STEP 5 单击“MapMaker”窗口工具栏中的“Line”（线）按钮，用来连接不同的 SNMP 节点。连接完成后，进一步编辑连线的属性，如图 14-3-15 所示。

STEP 6 为线选择关联的对象，在如图 14-3-16 所示的“Select Network Object”对话框中显示线两端设备的所有被管理接口，不足之处是只能关联一端的端口。

STEP 7 单击“OK”按钮，完成线的关联。

STEP 8 单击“MapMake”窗口工具栏中的“Save”（左起的第 3 个）按钮，把新设计的拓扑图保存，命名为“test”，后缀名是“.OrionMap”。

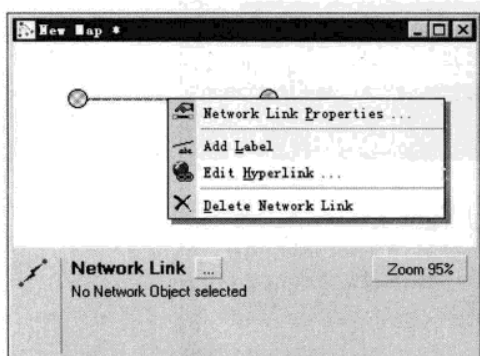


图 14-3-15 编辑 SNMP 连线的属性

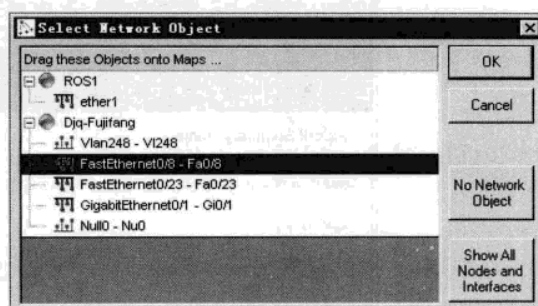


图 14-3-16 “Select Network Object”对话框

14.3.6 SolarWinds 管理界面

STEP 1 在任意计算机的 IE 浏览器地址栏中，输入 SolarWinds 服务器的 IP 地址，打开如图 14-3-17 所示的登录界面。

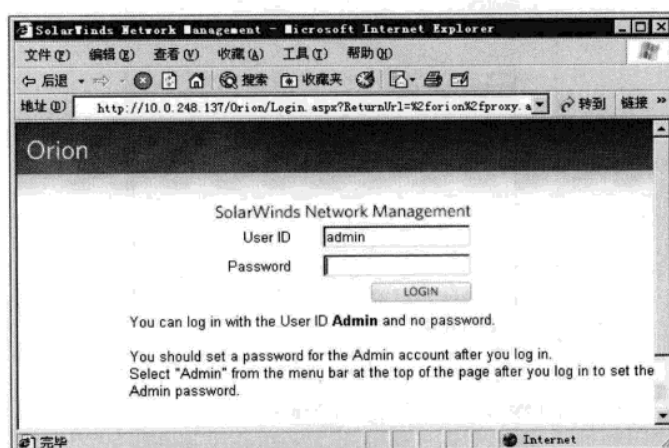


图 14-3-17 SolarWinds 登录界面

STEP 2 SolarWinds 初始的用户名是 admin，密码为空，登录后可以修改密码。SolarWinds 登录成功后的界面如图 14-3-18 所示。

STEP 3 其中顶部是菜单栏，左侧列表栏中分类显示所有的节点，右上方是默认的网络拓扑图。单击拓扑图右上角的“Edit”按钮，打开“Edit Network Map”窗口，如图 14-3-19 所示。

STEP 4 选择前面设计的拓扑“test”，并输入拓扑显示的比例大小，单击“SUBMIT”按钮进行提交。

此时，首页右上角的拓扑将变成企业的拓扑，可以单击图中的某个节点，打开该设备的链接查看其状态。也可把光标停在某个节点或连线上，查看设备或设备之间的连接情况。

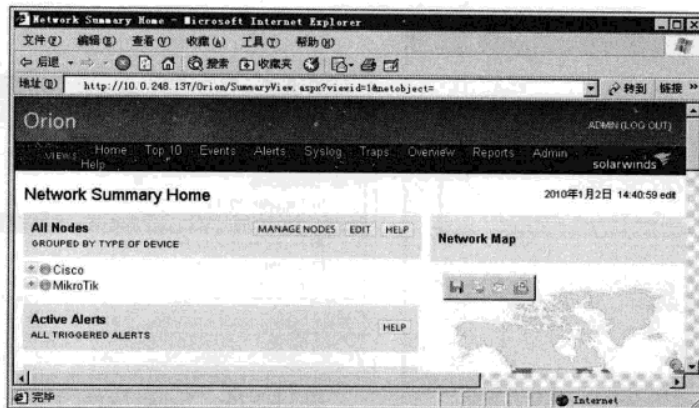


图 14-3-18 登录成功后的界面

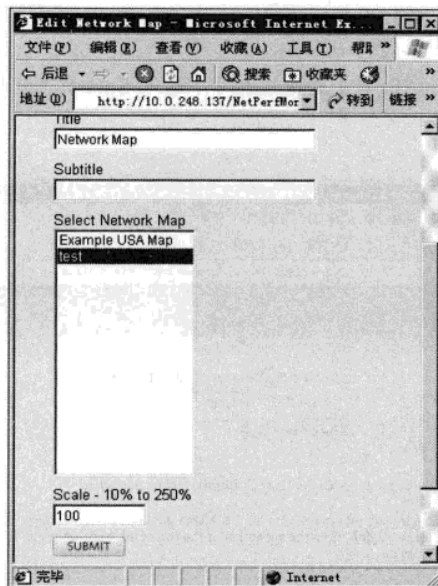


图 14-3-19 “Edit Network Map” 窗口

14.3.7 配置报警

当某个设备故障时，SolarWinds 为网络管理员发送报警信息，提示某设备故障。

STEP 1 单击“开始”→“程序”→“SolarWinds Orion”→“Advanced Alert Manager”选项，打开“Alert Manager”窗口。单击“Configure Alerts”按钮，弹出“Manage Alerts”对话框，选中“Alert me when a node goes down”（当某个节点 down 时通知我）复选框，如图 14-3-20 所示。

STEP 2 单击“Edit”按钮，显示“Edit Alert”窗口，打开“Trigger Actions”（触发动作）选项卡。然后单击“Add New Action”按钮，打开“Select an Action”对话框，如图 14-3-21 所示。

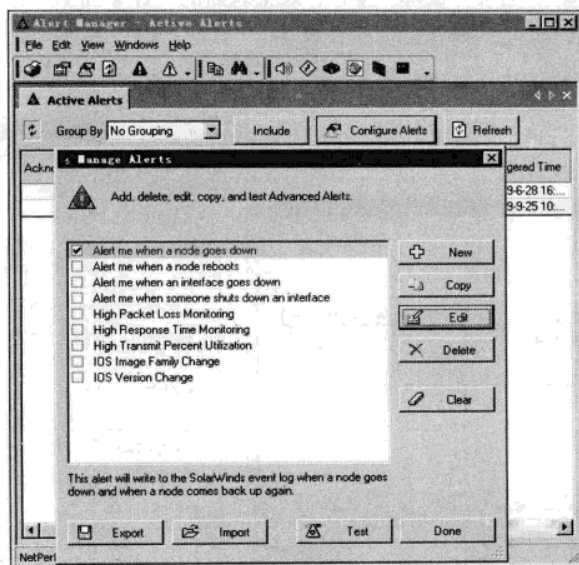


图 14-3-20 配置报警

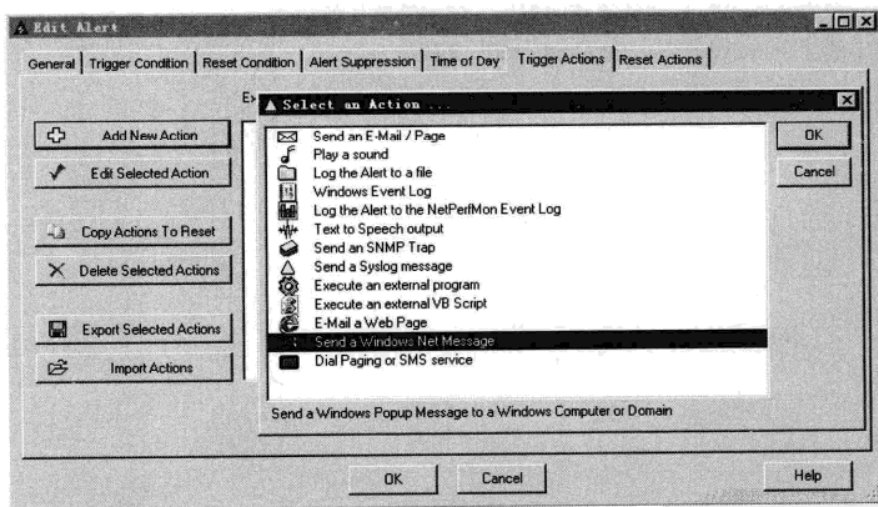


图 14-3-21 “Select an Action”对话框

STEP 3 选择要执行的操作，可以是发邮件、播放声音及发送 Windows 的信使服务等。这里以发送 Windows 的信使服务为例，选择“Send Windows Net Message”选项。单击“OK”按钮，弹出如图 14-3-22 所示的“Edit Net Message Action”对话框。在 IP 地址中输入需要接收信使服务提示的计算机的 IP 地址，在信息内容中输入“\$(NodeName) is down,pls check it”。其中\$(NodeName)是变量名，会自动替换成故障设备的名称，单击“OK”按钮。

STEP 4 在接收信息服务的计算机上启动信息服务，单击“开始”→“设置”→“控制面板”

→ “管理工具” → “服务”，打开“服务”窗口，双击找到的“Messenger”条目。打开“Messenger 的属性”对话框，如图 14-3-23 所示配置信使服务，“启动类型”下拉列表框中选择“自动”，并启动该服务。

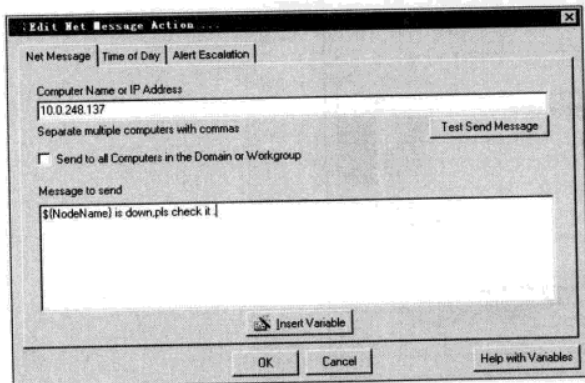


图 14-3-22 “Edit Net Message Action”对话框

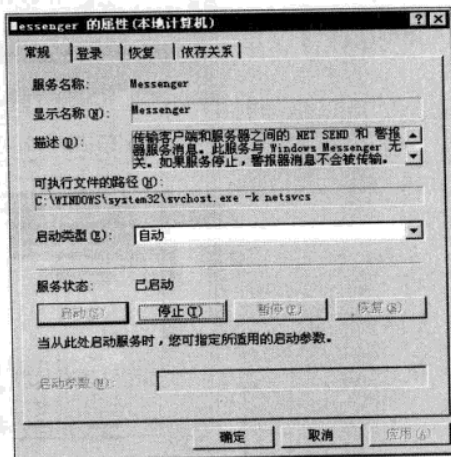


图 14-3-23 配置信使服务

至此，完成 SolarWinds 网管系统的配置，该网管软件的功能远不止此，感兴趣的读者可以参考软件包中的“OrionAdministrator Guide.pdf”文档。

Part

04

第 4 部分 高级应用和故障排除篇

上文已经介绍了网络的基础知识、Windows Server 2003 上各种服务的配置、路由和交换机的相关知识，但在实际工作中还有很多难题困扰用户。本篇结合实际工作中的突出问题，有针对性地介绍一些常见的网络应用和故障排除方法。

实验 A 路由器上配置 DHCP

某公司有两幢办公楼，网管想减轻 IP 地址手工分配的负担，计划使用 DHCP 功能，该公司拓扑如图 A-1 所示。而且网管也不想配置多台 DHCP 服务器，打算仅在公司主楼的一台路由器上实现全公司计算机 IP 地址的自动分配。

本书第 5 章介绍过可以使用 Windows Server 2003 作为 DHCP 服务器，如果专门使用一台服务器来分配地址有很多不便，更好的方法可以在思科的路由器或交换机上配置 DHCP，来提供 IP 地址的动态分配。如图 A-1 所示的拓扑可以用如图 A-2 所示的实验拓扑来替换。

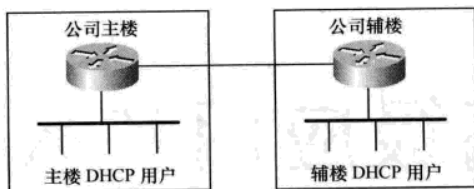


图 A-1 DHCP 拓扑

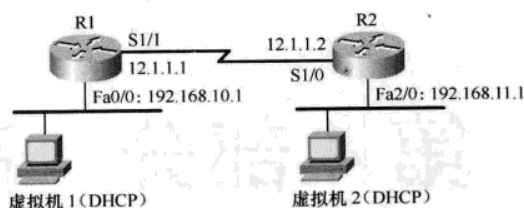


图 A-2 DHCP 实验

使用安全机架中的路由器 R1 和 R2，本实验的操作步骤如下。

STEP 1 基本网络配置。R1 的配置如下：

```
Router>en
Router#conf t
Router(config)#host R1
R1(config)#int fa 0/0
R1(config-if)#ip add 192.168.10.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#int s1/1
R1(config-if)#ip add 12.1.1.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#no cdp run
R1(config)#ip route 192.168.11.0 255.255.255.0 12.1.1.2
```

R2 的配置如下：

```
Router>en
Router#conf t
Router(config)#host R2
R2(config)#int fa 2/0
R2(config-if)#ip add 192.168.11.1 255.255.255.0
R2(config-if)#no shut
R2(config-if)#int s1/0
R2(config-if)#ip add 12.1.1.2 255.255.255.0
R2(config-if)#no shut
R2(config-if)#no cdp run
R2(config)#ip route 192.168.10.0 255.255.255.0 12.1.1.1
```

STEP 2 基本 DHCP 服务。R1 的配置如下:

R1(config)#ip dhcp pool zhulou	配置主楼 DHCP 地址池
R1(dhcp-config)#network 192.168.10.0 255.255.255.0	动态分配 192.168.10.0/24 这个网段内的 IP 地址
R1(dhcp-config)#dns-server 218.2.135.1	为主楼计算机配置 DNS 服务器
R1(dhcp-config)#default-router 192.168.10.1	为主楼的客户机配置默认网关
R1(dhcp-config)#lease 30	IP 地址租期是 30 天
R1(dhcp-config)#ip dhcp pool fulou	配置辅楼 DHCP 地址池
R1(dhcp-config)#network 192.168.11.0 /24	动态分配 192.168.11.0/24 这个网段内的 IP 地址
R1(dhcp-config)#dns-server 218.2.135.1	为辅楼计算机配置 DNS 服务器
R1(dhcp-config)#default-router 192.168.11.1	为辅楼的客户机配置默认网关
R1(dhcp-config)#lease 60	IP 地址租期是 60 天
R1(dhcp-config)#exit	
R1(config)#ip dhcp excluded-address 192.168.10.1	排除主楼客户机的网关, 因该 IP 地址已经被路由器的接口使用, 从分配的地址池中排除这个地址范围, 如果网络内还有其他的服务器, 譬如 WWW、FTP、DNS 等服务器, 也要从地址池中排除服务器的 IP 地址。如果不排除也没有关系, DHCP 服务器在分配一个 IP 地址出去之前会查询该 IP 地址是否已经被使用, 如果被使用, 则分配地址池中的下一个可用 IP 地址。
R1(config)#ip dhcp excluded-address 192.168.11.1	排除辅楼客户机的网关
R1(config)#no ip dhcp conflict logging	这一步是可选配置, 取消地址冲突日志的记录功能。

STEP 3 配置 DHCP 中继。前面已经介绍了路由器有隔离广播的作用, DHCP 客户端请求 IP 地址时, 需要发送广播包与 DHCP 服务器进行交互。虚拟机 2 的 DHCP 请求包被路由器 R2 阻止, 无法到达 DHCP 服务器 R1。配置路由器 R2, 允许进行 DHCP 中继, 把虚拟机 2 发送的广播包转变成单播包, 由路由器 R2 把包转发出去。路由器 R2 上配置 DHCP 中继的命令是:

R2(config)#int fa 2/0 进入连接 DHCP 客户端的以太网接口

R2(config-if)#ip helper-address 12.1.1.1 配置辅助寻址, 指向 DHCP 服务器的地址, 即路由器 R2 的 IP 地址

STEP 4 测试。配置虚拟机 1 和虚拟机 2 使用 DHCP, 如图 A-3 所示, 虚拟机 1 和虚拟机 2 的 IP 地址和 DNS 均使用自动获得。

STEP 5 在虚拟机 1 的 DOS 窗口中, 使用 ipconfig /all 命令查看 IP 地址获取情况, 如图 A-4 所示, 可以看到虚拟机 1 从 DHCP 服务器 12.1.1.1 获取到 IP 地址 192.168.11.2, 类似的可以查看虚拟机 2 获取到 IP 地址 192.168.10.2, 在虚拟机 1 上 ping 虚拟机 2 的 IP 地址 192.168.10.2, 可以 ping 通。如果获取不到 IP 地址或者获取到的 IP 地址不正确, 可以检查虚拟机 1 和虚拟机 2 的网卡类型是否配置正确, 即虚拟机 1 是 Host-only, 虚拟机 2 是 Bridged, 同时还要停止网络上的其他 DHCP 服务器, 包括 VMware 自身提供的 DHCP 服务。

至此, 通过启用 Cisco 路由器的 DHCP Server 功能, 使公司内部不同网段中的主机都可以自动获得 IP 地址。从稳定性和功能上看, 在路由器实现的 DHCP 服务比在服务器上用 Windows/Linux 操作系统实现的 DHCP 服务要优越得多。

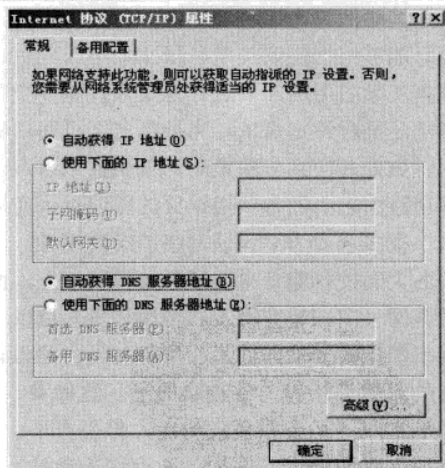


图 A-3 配置客户机使用 DHCP



图 A-4 查看 DHCP 客户端信息

实验 B 策略路由

路由器依据由路由协议产生的路由表, 根据目的 IP 地址进行报文转发。在这种机制下, 路由器只能根据报文的目的 IP 地址为用户提供比较单一的路由方式, 它更多的是解决网络数据的转发问题, 而不能提供有差别的服务。

基于策略的路由为网络管理者提供了比传统路由协议对报文的转发和存储更强的控制能力。基于策略的路由比普通路由控制能力更强, 使用更灵活, 它使网络管理者不仅能够根据目的地址, 而且能够根据协议类型、报文大小、应用、IP 源地址或者其他的策略来选择转发路径。策略可以根据实际应用的需要进行定义来控制多个路由器之间的负载均衡、单一链路上报文转发的 QoS 或者满足某种特定需求。当数据包经过路由器转发时, 路由器根据预先设定的策略对数据包进行匹配, 如果匹配到一条策略, 就根据该条策略指定的路径进行转发; 如果没有匹配到任何策略, 就使用路由表中的各项根据目的地址对报文进行转发。

很多企业为了保证网络的高可用性, 一般都向两个或两个以上的 ISP 申请了宽带接入, 如国内各大高校普遍是电信和教育双网接入, 两条链路并行。一般的做法如图 B-1 所示, 对去往国内教育网 (中国教育网上有地址列表, 可以下载) 的流量使用教育网出口, 对去往国际流量 (教育网出国流量要根据流量收费) 和国内除教育网外的流量使用电信网出口。当一条链路故障时, 所有的流量都从另一条链路通过。这种做法虽实现了冗余和负载均衡, 但也有不尽如人意的地方, 例如, 教育网的地址列表发生改变, 管理员需要重新调整列表; 本来电信出口已经很拥挤了, 可去往国内非教育网的流量还是从电信出口走, 或许从教育网走的网速更快; 用户

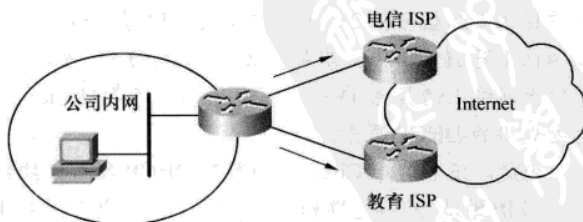


图 B-1 双出口网络

本身不能选择出口链路。

如下实例，某公司有双 ISP 接入，除配置出口路由器实现负载均衡（根据目标 IP 地址选择出口）和冗余（任一条 ISP 链路故障，另一条 ISP 链路可以转发所有流量）外，还部署了策略路由。具体做法是给每一个用户分配两个 IP 地址，如 192.168.11.2 和 192.168.12.2，其中 192.168.11.0（奇数）网络从 ISP1（R1）出口，192.168.12.0（偶数）网络从 ISP2（R3）出口，用户自己可以变换 IP 地址，来选择不同的出口。该实验可以在如图 B-2 所示的拓扑中完成。

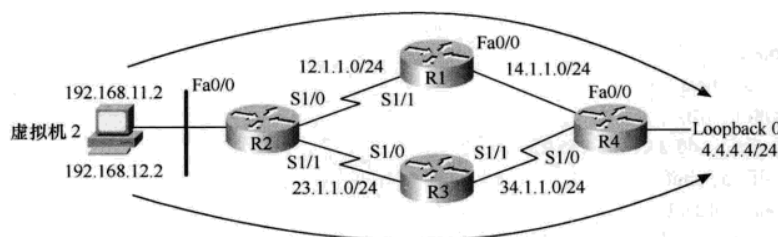


图 B-2 策略路由实验

运行 CCNP 机架中的 R1、R2、R3 和 R4，该实验的配置步骤如下：

STEP 1 基本网络配置。R1 的配置如下：

```
Router>en
Router#conf t
Router(config)#host R1
R1(config)#int s1/1
R1(config-if)#ip add 12.1.1.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#int fa 0/0
R1(config-if)#ip add 14.1.1.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#no cdp run
R1(config)#router rip 本实验中配置 RIP 动态路由协议，来提供全网的可达性
R1(config-router)#net 12.0.0.0
R1(config-router)#net 14.0.0.0
```

R2 的配置如下：

```
Router>en
Router#conf t
Router(config)#host R2
R2(config)#no cdp run
R2(config)#int s1/0
R2(config-if)#ip add 12.1.1.2 255.255.255.0
R2(config-if)#no shut
R2(config-if)#int s1/1
R2(config-if)#ip add 23.1.1.2 255.255.255.0
R2(config-if)#no shut
R2(config-if)#int fa 0/0
```

```
R2(config-if)#ip add 192.168.11.1 255.255.255.0
R2(config-if)#ip add 192.168.12.1 255.255.255.0 secondary
R2(config-if)#no shut
R2(config-if)#router rip
R2(config-router)#net 12.0.0.0
R2(config-router)#net 23.0.0.0
R2(config-router)#net 192.168.11.0
R2(config-router)#net 192.168.12.0
```

R3 的配置如下:

```
Router>en
Router#conf t
Router(config)#host R3
R3(config)#int s1/0
R3(config-if)#ip add 23.1.1.3 255.255.255.0
R3(config-if)#no shut
R3(config-if)#int s1/1
R3(config-if)#ip add 34.1.1.3 255.255.255.0
R3(config-if)#no shut
R3(config-if)#router rip
R3(config-router)#net 23.0.0.0
R3(config-router)#net 34.0.0.0
```

R4 的配置如下:

```
Router>en
Router#conf t
Router(config)#host R4
R4(config)#no cdp run
R4(config)#int s1/0
R4(config-if)#ip add 34.1.1.4 255.255.255.0
R4(config-if)#no shut
R4(config-if)#int fa 0/0
R4(config-if)#ip add 14.1.1.4 255.255.255.0
R4(config-if)#no shut
R4(config-if)#int loopback 0
R4(config-if)#ip add 4.4.4.4 255.255.255.0
R4(config-if)#router rip
R4(config-router)#net 14.0.0.0
R4(config-router)#net 34.0.0.0
R4(config-router)#net 4.0.0.0
```

STEP 2 测试。虚拟机 2 的网卡类型是 Bridged, IP 地址配成 192.168.11.2, 子网掩码是 255.255.255.0, 网关是 192.168.11.1, DNS 是 218.2.135.1。在虚拟机 2 的 DOS 窗口中使用 tracert 命令, 验证数据包的通信路径, 如图 B-3 所示, 显示数据包经过的路径是 R2→R3→R4, 这里的显示并不准确, 稍后进行细致的说明; 把虚拟机 2 的 IP 地址换成 192.168.12.2 时, 显示数据包经过的路径仍然是 R2→R3→R4。

在路由器 R2 上使用 traceroute 测试到 4.4.4.4 经过的路径, 结果如图 B-4 所示。

图 B-4 显示的结果比图 B-3 显示的要准确得多, tracert (在路由器上是 traceroute) 命令每测

一跳都发出 3 个包, 3 个包可能有不同的下一跳, 可图 B-3 中只显示了一个下一跳的地址。图 B-4 中的路由器把 3 个测试包单独列出来, 如图 B-4 所示, 可以看出路由器去往 4.4.4.4 的测试包有不同的下一跳, 第 1 个包从 R1 走, 第 2 个包从 R3 走, 第 3 个包又从 R1 走, 如果有第 4 个包, 将从 R3 走。

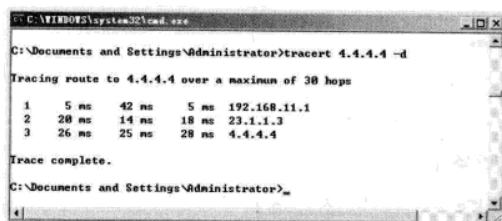


图 B-3 tracert 测试路径

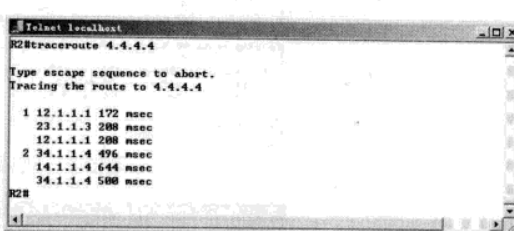


图 B-4 traceroute 测试路径

STEP 3 配置策略路由第一步, 区分流量。在路由器 R2 上, 使用 ACL 把来源 192.168.11.0 和来源 192.168.12.0 的数据包区分开发。R2 的配置如下:

```
R2(config)#access-list 100 permit ip 192.168.11.0 0.0.0.255 4.4.4.0 0.0.0.255
```

```
R2(config)#access-list 101 permit ip 192.168.12.0 0.0.0.255 4.4.4.0 0.0.0.255
```

STEP 4 配置策略路由第二步, 创建 route-map。R2 的配置如下:

R2(config)#route-map out-traffic permit 10 创建 route-map, 名字叫 out-traffic; 10 是行号, 一个 route-map 可以有多个行号, 就像扩展的 ACL 的匹配过程一样, 从小的行号开始顺序执行, 当条件满足时, 执行操作, 并且退出 route-map, 不再继续往下比较

R2(config-route-map)#match ip address 100 条件是满足 ACL100, 也就是从 192.168.11.0/24 去往 4.4.4.0/24 的流量

R2(config-route-map)#set ip next-hop 12.1.1.1 把数据包的下跳转发到 12.1.1.1 (路由器 R1), 尽管路由表 R2 的路由表中, 去往 4.0.0.0/8 有两个下一跳, 但数据包将被转发到 12.1.1.1, 因策略路由的执行优于路由表

```
R2(config-route-map)#route-map out-traffic permit 20
```

R2(config-route-map)#match ip address 101 条件是满足 ACL101, 也就是从 192.168.12.0/24 去往 4.4.4.0/24 的流量

```
R2(config-route-map)#set ip next-hop 23.1.1.3 把数据包的下跳转发到 23.1.1.3 (路由器 R3)
```

STEP 5 配置策略路由第三步, 调用 route-map。R2 的配置如下:

```
R2(config)#int fa 0/0 在流量进入的接口使用策略路由, 流量是从路由器 R2 的 Fa0/0 进入的
```

```
R2(config-if)#ip policy route-map out-traffic 使用策略路由, 调用的 route-map 是前面创建的 out-traffic
```

STEP 6 测试。把虚拟机 2 的 IP 地址配置成 192.168.11.2, 掩码 255.255.255.0, 网关设置成 192.168.11.1, 测试去往 4.4.4.4 的路径, 结果是 R2→R1→R4, 如图 B-5 所示。

STEP 7 把虚拟机 2 的 IP 地址配置成 192.168.12.2, 子网掩码 255.255.255.0, 网关设置成 192.168.12.1, 测试去往 4.4.4.4 的路径, 结果是 R2→R3→R4, 如图 B-6 所示。

路由器一般是基本目标 IP 地址进行数据包转发, 本实验中的策略路由完成了根据源 IP 地址进行数据包的转发。工程中还可以根据数据包的长度、IP 地址、接口等进行转发, 下面是路由器 R2 支持的判断条件, 读者可以根据工程实际情况, 配置出更符合实际的策略路由。如公司有两条出口, 可以配置一般网络流量从繁忙的 ISP1 走, 关键的业务流从相对空闲的 ISP2 走, 虽然是同一台计算机, 有的流量从 ISP1 走, 有的流量从 ISP2 走。

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter 本地连接:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.11.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.11.1

C:\Documents and Settings\Administrator>tracert 4.4.4.4 -d

Tracing route to 4.4.4.4 over a maximum of 30 hops:

  0  446 ms  298 ms  374 ms  192.168.11.1
  1  1285 ms  1238 ms  1238 ms  12.1.1.1
  2  2216 ms  2387 ms  2026 ms  4.4.4.4

Trace complete.
```

图 B-5 测试策略路由 1

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter 本地连接:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.12.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.12.1

C:\Documents and Settings\Administrator>tracert 4.4.4.4 -d

Tracing route to 4.4.4.4 over a maximum of 30 hops:

  0  481 ms  374 ms  378 ms  192.168.11.1
  1  1231 ms  1122 ms  1164 ms  23.1.1.3
  2  1898 ms  1987 ms  1923 ms  4.4.4.4

Trace complete.
```

图 B-6 测试策略路由 2

```
R2(config)#route-map out-traffic permit 10
R2(config-route-map)#match ?
as-path          Match BGP AS path list
clns             CLNS information
community       Match BGP community list
extcommunity     Match BGP/VPN extended community list
interface       Match first hop interface of route
ip              IP specific information
ipv6            IPv6 specific information
length          Packet length
metric          Match metric of route
mpls-label      Match routes which have MPLS labels
nlri            BGP NLRI type
policy-list     Match IP policy list
route-type      Match route-type of route
tag             Match tag of route

R2(config-route-map)#match ip ?
address         Match address of route or match packet
next-hop       Match next-hop address of route
route-source   Match advertising source address of route
```

注意



如果策略被拒绝,没有匹配策略的时候,包文仍然被路由,采用的是普通的路由转发机制。

实验 C 路由器 NAT 实验

随着 Internet 的迅速发展, IP 地址短缺已成为一个十分突出的问题。为了解决这个问题, 出现了多种解决方案。下面介绍一种在目前网络环境中比较有效的方法 NAT (Network Address Translation, 网络地址转换)。

NAT 提供了连接 Internet 的一种简单方式, 并且通过隐藏内部网络地址的手段为用户提供了安全保护。内部网络用户 (位于 NAT 设备的内侧) 连接 Internet 时, NAT 设备将数据包中的源 IP 地址 (也就是用户的内部网络 IP 地址) 转换成一个外部公共 IP 地址 (存储于 NAT 的地址池), 并在 NAT 地址转换表中记录下这个转换项; 当外部网络数据返回时, NAT 设备查询 NAT 地址转换表项, 将目标 IP 地址替换成初始的内部用户的 IP 地址, 把数据包转发给内部网络用户。由于这样对外隐藏了内部网络的 IP 地址, 因此, 外部用户无法直接发起到内部用户的连接, 从而保护了内部网络。

使用 NAT 有很多优点和好处。

- NAT 节省了公网地址。一个企业申请的合法 IP 地址很少, 而内部网络用户很多, 可以通过 NAT 功能实现多个用户同时共用一个合法 IP 与外部网络进行通信。

- NAT 增加了连接到公网的弹性。可以使用多地址池, 备份地址池, 负载均衡地址池, 确保可靠的公网连接。

- NAT 允许内部网络编址的一致性。如果一个单位没有使用私有地址和 NAT, 当公有地址发生改变时, 要改变公司内的所有主机, 工作量巨大。如果采用了 NAT, 只需更改 NAT 设备的 IP 地址池配置, 内部网络的编址不受影响。这意味着, 一个单位可以更换 ISP 而不需要改变内部主机的 IP 地址。

- NAT 提高了内部网络的安全。一个企业不想让外部网络用户知道自己内部网络的结构, 可以通过 NAT 将内部网络与外部 Internet 隔离开, 则外部用户根本不知道通过 NAT 设备的内部 IP 地址。NAT 虽能提高内部网络的安全, 但无法取代防火墙。

然而使用 NAT 也带来一些不足。

- NAT 影响性能。转换每一个包头中的 IP 地址需要时间, NAT 增加了交换延时。路由器必须检查每一个包来决定是否需要转换, 路由器需要转换 IP 头, 有时还需要转换 TCP 或 UDP 头部。

- NAT 缺乏对一些应用的支持。很多 Internet 协议和应用依赖于端到端的应用, 包从源到目的不能被修改。通过修改端到端的地址, NAT 阻止了一些应用。例如, 一些安全应用, 如数字签名就会失败, 因为源 IP 地址发生了改变。

- NAT 不利于追踪。经过多次 NAT, 端到端的追踪变得非常困难。另一方面, 因为 NAT 的存在, 也很难追踪或获得黑客使用的真实 IP 地址。

- NAT 使一些隧道协议变得复杂。因为 NAT 修改了包头中的值, 给 IPsec 或其他隧道协议的完整性检查带来困难。

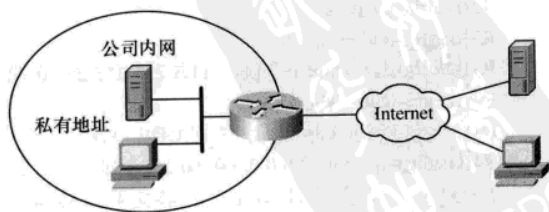


图 C-1 NAT 拓扑

一个有 NAT 能力的设备大多部署在根网络的边缘,如图 C-1 所示,路由部署在公司网络的边界,公司仅有少量的公共 IP 地址,全公司的计算机都需要访问 Internet。公司内的计算机访问公司内的服务器,它们使用本来的私有 IP 地址;如果想访问外部服务器时,数据包被转发给路由器,路由器执行 NAT 操作,把内部的私有地址转换成外部的、可路由(私有地址本身也是可路由的,只是大多数 ISP 的路由被配置成拒绝转发私有地址的流量)的公共 IP 地址后,再转发出去;当外部的计算机想访问公司内部的服务时,它们访问公司公布出去的公共 IP 地址,当数据流量被发送到路由器时, NAT 设备查询内部定义的静态转换条目,把对公共 IP 地址的访问转换成对内部私有 IP 地址的访问。

如图 C-1 所示的拓扑可以在如图 C-2 所示的实验环境中实现。公司只申请到少量的合法地址(这里假设只申请到一个,也就是路由器 Fa0/0 接口的 IP 地址 192.168.1.220,事实上 192.168.1.220 仍然是私有地址,在本实验中假设这就是一个申请到的合法 IP 地址),要提供全公司的用户都可以访问 Internet。虚拟机 1 是公司内部的一台计算机,实验成功后,虚拟机 1 可以成功访问新浪网;公司内部有一台 Web 服务器,这里仍然用虚拟机 1 充当,当从外部(虚拟机 2)访问 http://192.168.1.220 时,可以成功地访问到虚拟机 1 上 Web 主页。

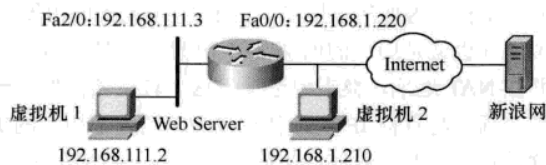


图 C-2 NAT 实验拓扑

配置 NAT 的方式有静态 NAT、动态 NAT、NAT 超载等几种方式, NAT 超载是使用最多的一种地址转换方式,也称复用动态地址转换,或称 PAT (Port Address Translation, 端口地址转换)。复用动态地址转换首先是一种动态地址转换,但是它可以允许多个内部本地地址共用一个内部合法地址。只申请到少量 IP 地址,但却经常同时有多于合法地址个数的用户访问外部网络的情况,这种转换极为有用。PAT 采用的工作原理是当多个用户同时使用一个 IP 地址时,路由器利用上层的 TCP 或 UDP 端口号等唯一标识某台计算机。这里使用安全机架中的路由器 R1,本实验的配置步骤如下。

配置 NAT 的方式有静态 NAT、动态 NAT、NAT 超载等几种方式, NAT 超载是使用最多的一种地址转换方式,也称复用动态地址转换,或称 PAT (Port Address Translation, 端口地址转换)。复用动态地址转换首先是一种动态地址转换,但是它可以允许多个内部本地地址共用一个内部合法地址。只申请到少量 IP 地址,但却经常同时有多于合法地址个数的用户访问外部网络的情况,这种转换极为有用。PAT 采用的工作原理是当多个用户同时使用一个 IP 地址时,路由器利用上层的 TCP 或 UDP 端口号等唯一标识某台计算机。这里使用安全机架中的路由器 R1,本实验的配置步骤如下。

STEP 1 配置基本网络环境。配置虚拟机 1,网卡类型 Host-only, IP 地址 192.168.111.2,子网掩码 255.255.255.0,网关 192.168.111.3, DNS 是 218.2.135.1。配置虚拟机 2,网卡类型 Bridged, IP 地址 192.168.1.210,子网掩码 255.255.255.0,网关 192.168.1.1, DNS 是 218.2.135.1。路由器 R1 的配置基本配置如下:

```
Router>en
Router#conf t
Router(config)#host R1
R1(config)#int fa 0/0
R1(config-if)#ip add 192.168.1.220 255.255.255.0 路由器连接 Internet 的接口,配置申请到的合法 IP 地址
R1(config-if)#no shut
R1(config-if)#int fa 2/0
R1(config-if)#ip add 192.168.111.3 255.255.255.0 路由器连接内网的接口,随便配置一段私有地址
R1(config-if)#no shut
R1(config-if)#no cdp run 关闭 CDP 协议
R1(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.1 配置路由器的默认路由
```

STEP 2 配置 NAT 第 1 步,指定对外接口。R1 的配置如下:

```
R1(config)#int fa 0/0
```

R1(config-if)#ip nat outside 指明这个接口是对外的接口

STEP 3 配置 NAT 第 2 步, 指定对内接口。R1 的配置如下:

R1(config)#int fa 2/0

R1(config-if)#ip nat inside 指明这个接口是对内的接口

STEP 4 配置 NAT 第 3 步, 创建地址池。R1 的配置如下:

R1(config)#ip nat pool out-pool 192.168.1.220 192.168.1.220 netmask 255.255.255.0 创建地址池, 地址池的名字叫 out-pool, 地址池中起始的地址是 192.168.1.220, 地址池中结束的地址是 192.168.1.220, 使用的掩码是 255.255.255.0。这个地址池中只有一个地址, 工程中如果申请到多个合法 IP 地址, 这里配置成一个范围

STEP 5 配置 NAT 第 4 步, 允许被 NAT 的条件。R1 的配置如下:

R1(config)#access-list 1 permit 192.168.111.0 0.0.0.255 配置允许被 NAT 的条件, 这里可以只允许一部分 IP 地址被 NAT, 也可以使用扩展 ACL 限制只允许访问一部分外部主机, 还可以使用协议, 只允许外部的部分服务

STEP 6 配置 NAT 第 5 步, 把允许被 NAT 的列表和地址池关联起来。R1 的配置如下:

R1(config)#ip nat inside source list 1 pool out-pool overload 把允许被 NAT 的 ACL 1 和前面创建的地址池 out-pool 关联起来, 这里的 overload 是超载的意思, 也就是允许使用上层的 UDP 和 TCP 端口标识会话, 尤其是在内网上网主机多于地址池中合法 IP 地址的情况下, 这个关键字必不可少

注 意



工程中, 一般单位可能不需要对外提供服务, 这时往往会选择使用动态宽带接入 (这种方式比静态宽带接入收费要低), 也就是路由器的对外接口使用 DHCP 动态获取 IP 地址, 因 IP 地址不固定, 无法创建地址池。此时可以把配置 NAT 的第 3 步和第 5 步合成一步, 配置如下:

R1(config)#ip nat inside source list 1 interface fa 0/0 overload 把允许被 NAT 的 ACL 和路由器对外接口关联起来, 无论路由器对外接口获取到什么 IP 地址, 路由器都使用对外接口的 IP 地址进行 NAT。本实验中, 路由器接口虽是使用静态 IP 地址, 因地址池中只有一个 IP 地址, 该配置同样适用

STEP 7 配置 NAT 第 6 步, 可选额外配置。由于本实验中虚拟机 1 还需对外提供 Web 服务, 所以在路由器上配置端口映射, R1 的配置如下:

R1(config)#ip nat inside source static tcp 192.168.111.2 80 int fa0/0 80 配置端口映射, 外界对 Fa0/0 接口 IP 地址 80 端口的访问被静态的转换到内网 192.168.111.2 计算机的 80 端口。实际工程中, 这里可以换成其他的 TCP 或 UDP 端口, 还可以创建多个条目, 也可以把不同的端口映射到不同的内部计算机上

STEP 8 测试。在虚拟机 1 上访问新浪网, 可以成功访问新浪网。在虚拟机 2 的 IE 地址栏中输入 http://192.168.1.220, 可以成功访问到虚拟机 1 上 Web 主页。在大量的实验中, 发现配置都正确的情况下, 有时虚拟机 2 并不能成功访问到虚拟机 1 上的 Web 主页或其他服务, 这多数是用户系统本身的问题, 在工程实际中不会出现这样的情况。

实验 D 网关冗余

本篇实验 B 的策略路由中提到很多单位为了保证网络的高可用性, 一般都采用双链路接入, 如图 B-1 所示。在图 B-1 中, 如果单位的出口路由器故障, 即使两条链路都是正常的, 内部用户仍然无法访问 Internet。本实验中介绍一种新的技术 HSRP (Hot Standby Routing Protocol, 热备份路由协议), 使用 HSRP 可以有效地解决由单一链路或单设备故障引起的网络通信中断问题。

实现 HSRP 的条件是网络中有多台路由器或三层交换机, 它们组成一个“热备份组”, 这个组构造

一个虚拟路由器。在任何时刻，一个组内只有一个路由器是活跃的，并由它来转发数据包，如果活跃路由器发生了故障，将选择一个备用路由器来替代活跃路由器，但是在本网络内的主机看来，虚拟路由器没有改变。所以主机仍然保持连接，没有受到故障的影响，这样就较好地解决了路由器的切换问题。

如图 D-1 所示，公司两台出口路由器组成一个“热备份组”，这个热备份组向外提供一个虚拟的 IP 地址。两台路由器选出一个作为活跃路由器，另一个作为备用路由器，活跃路由器负责处理发往虚拟 IP 地址的所有数据包，备用路由器处在等待状态，当活跃路由器故障，备用路由器成活跃路由器，负责处理发往虚拟 IP 地址的所有数据包。公司内网中的计算机把网关指向虚拟 IP 地址，两台路由器中任何一台故障，公司内网中用户的 Internet 访问只会受到很小的影响，很快转换到正常状态，用户几乎察觉不到网络发生过中断。

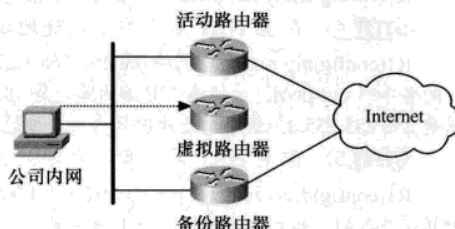


图 D-1 网关冗余拓扑

如果只有一台路由器来转发流量，那另一台路由器和另一条链路一直处在备用状态，是不是有点太浪费呢？工程中，可以配置多个热备份组并存，每个热备份组提供一个虚拟 IP 地址，它有一个众所周知的 MAC 地址和一个 IP 地址。当在一个局域网上有多个热备份组并存时，把局域网中的计算机网关指向不同的虚拟 IP 地址，可以使负载得到分担。

HSRP 协议利用一个优先级方案来决定哪个配置 HSRP 协议的路由器成为默认的活跃路由器。如果一个路由器的优先级设置得比其他所有路由器的优先级高，则该路由器成为活跃路由器。路由器的默认优先级是 100，所以如果只设置一个路由器的优先级高于 100，则该路由器将成为活跃路由器。

通过在设置了 HSRP 协议的路由器之间广播 HSRP 优先级，HSRP 协议选出当前的活跃路由器。当在预先设定的一段时间内活跃路由器不能发送 hello 消息，或者说 HSRP 检测不到活跃路由器的 hello 消息时，将认为活跃路由器有故障，这时 HSRP 会选择优先级最高的备用路由器变为活跃路由器，同时会将按 HSRP 优先级在配置了 HSRP 的路由器中再选择一台路由器作为新的备用路由器。

如图 D-1 所示的拓扑可以在如图 D-2 所示的实验环境中实现。虚拟机 1 相当于是公司内网中的计算机，计算机的网关指向虚拟路由器 192.168.111.254；路由器 R1 和 R3 相当于是公司的两台出口路由器，其中有一台是活跃路由器，负责处理内网发到 192.168.111.254 的数据包；虚拟机 2 相当于是公网中的一台计算机。虚拟机 1 连续不断地 ping 虚拟机 2 的 IP 地址，依次断开 R1 和 R2 之间的链路，R3 和 R2 之间的链路，观察故障中断和恢复的情况。运行安全机架中的路由器 R1、R2 和 R3，该实验的具体步骤如下。

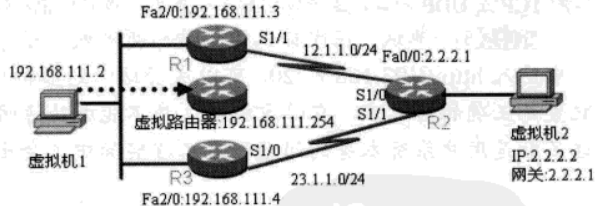


图 D-2 网关冗余实验拓扑

STEP 1 虚拟机 IP 网络配置。配置虚拟机 1，网卡类型 Host-only，IP 地址 192.168.111.2，子网掩码 255.255.255.0，网关 192.168.111.254，DNS 是 218.2.135.1。配置虚拟机 2，网卡类型 Bridged，IP 地址 2.2.2.2，子网掩码 255.255.255.0，网关 2.2.2.1，DNS 是 218.2.135.1。

STEP 2 配置路由器的接口 IP 和路由。R1 的配置如下：

```

Router>en
Router#conf t
Router(config)#host R1
R1(config)#int fa 2/0
R1(config-if)#ip add 192.168.111.3 255.255.255.0
R1(config-if)#no shut
R1(config-if)#int s1/1
R1(config-if)#ip add 12.1.1.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#no cdp run
R1(config)#ip route 0.0.0.0 0.0.0.0 12.1.1.2
R2 的配置如下:

```

```

Router>en
Router#conf t
Router(config)#host R2
R2(config)#int fa 0/0
R2(config-if)#ip add 2.2.2.1 255.255.255.0
R2(config-if)#no shut
R2(config-if)#int s1/0
R2(config-if)#ip add 12.1.1.2 255.255.255.0
R2(config-if)#no shut
R2(config-if)#int s1/1
R2(config-if)#ip add 23.1.1.2 255.255.255.0
R2(config-if)#no shut
R2(config-if)#no cdp run
R3 的配置如下:

```

```

Router>en
Router#conf t
Router(config)#host R3
R3(config)#int fa 2/0
R3(config-if)#ip add 192.168.111.4 255.255.255.0
R3(config-if)#no shut
R3(config-if)#int s1/0
R3(config-if)#ip add 23.1.1.3 255.255.255.0
R3(config-if)#no shut
R3(config-if)#no cdp run
R3(config)#ip route 0.0.0.0 0.0.0.0 23.1.1.2

```

STEP 3 配置 NAT。路由器 R1 和 R3 是公司出口路由器，只有少量合法的 IP 地址，却要提供全公司计算机对 Internet 的访问，需要在两台路由器上配置 NAT 服务。R1 的配置如下：

```

R1(config)#int fa 2/0
R1(config-if)#ip nat inside
R1(config-if)#int s1/1
R1(config-if)#ip nat outside
R1(config-if)#exit
R1(config)#access-list 1 permit any
R1(config)#ip nat inside source list 1 int s1/1 overload

```


R3 的配置如下:

```
R3(config)#int fa 2/0
R3(config-if)#ip nat inside
R3(config-if)#int s1/0
R3(config-if)#ip nat outside
R3(config-if)#exit
R3(config)#access-list 1 permit any
R3(config)#ip nat inside source list 1 int s1/0 overload
```

STEP 4 配置 HSRP。R1 的配置如下:

R1(config)#int fa 2/0 进入热备份路由器要提供 HSRP 服务的接口
 R1(config-if)#standby 1 ip 192.168.111.254 创建 HSRP 组 1, 组 1 提供的虚拟 IP 地址是 192.168.111.254
 R1(config-if)#standby 1 priority 101 配置该路由器在 HSRP 组 1 中的优先级, 默认优先级是 100, 在同一个 HSRP 组中, 优先级高的路由器成为活跃路由器, 如果两个路由器的优先级一样, IP 地址高的路由器成为活跃路由器

R1(config-if)#standby 1 preempt 配置 IP 地址抢占功能, 如果没有配置抢占功能, 路由器 R1 因某种原因 (如重启) 失去活跃路由器的身份, 路由器无法再次成为活跃路由器

R1(config-if)#standby 1 track s1/1 HSRP 组 1 追踪 S1/1 端口状态, 如果 S1/1 端口变成非激活端口, HSRP 组 1 的优先级默认减 10, 这个值可以配置。注意图 D-2 中, 如果没有配置端口追踪, R1 是活跃路由器, 假如 R1 和 R2 之间的链路中断, 而 R1 在 HSRP 组 1 中的优先级仍然是 101, 仍然是活跃路由器, 内网中的计算机 (虚拟机 1) 仍然把数据包发到路由器 R1 上, 结果都到达不了 Internet (虚拟机 2)。如果配置了端口追踪, R1 和 R2 之间的链路中断, R1 在 HSRP 组 1 中的优先级变成 91, R3 成为活跃路由器, 内网中的计算机 (虚拟机 1) 把数据包发到路由器 R3 上, 进而到达 Internet (虚拟机 2)。

R3 的配置如下:

```
R3(config)#int fa 2/0
R3(config-if)#standby 1 ip 192.168.111.254
R3(config-if)#standby 1 preempt
R3(config-if)#standby 1 track s1/0
```

STEP 5 测试。在路由器 R1 上使用 show standby brief 命令, 查看 HSRP 组的情况, 显示如下:

```
R1#show standby brief
P indicates configured to preempt.
|
Interface Grp Pri P State Active Standby Virtual IP
Fa2/0 1 101 P Active local 192.168.111.4 192.168.111.254
```

从上面的输出中可以看出 R1 参与的接口是 Fa2/0, 参与的 HSRP 组是 1, 优先级是 101, 配置了抢占机制 (preempt), 本路由器的状态是 Active, 活跃路由器是本路由器, 备用路由器是 192.168.111.4, 虚拟的 IP 地址是 192.168.111.254。

STEP 6 在路由器 R3 上使用 show standby brief 命令, 查看 HSRP 组的情况, 显示如下:

```
R3#show standby brief
P indicates configured to preempt.
|
Interface Grp Prio P State Active Standby Virtual IP
Fa2/0 1 100 P Standby 192.168.111.3 local 192.168.111.254
```

STEP 7 在虚拟机 1 上打开一个 DOS 窗口, 输入 “ping 2.2.2.2 -t”, 持续不断地 ping 虚拟机

2, 在路由器 R1 上使用 shutdown 命令关闭 S1/1 端口, 过几分钟再使用 no shut 命令打开 S1/1 端口。虚拟机 1 上的 DOS 窗口显示如图 D-3 所示, 可以看出在断开路由器 R1 的 S1/1 端口时, 虚拟机丢了一个 ping 包, 然后就正常了; 当路由器 R1 的 S1/1 端口重新被打开时, 虚拟机 1 没有丢失任何 ping 包。

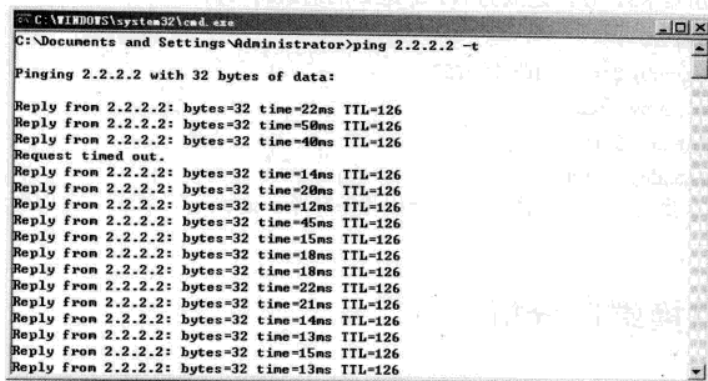


图 D-3 测试 HSRP 协议

整个测试过程中, 路由器 R3 的显示如图 D-4 所示。断开路由器 R1 的 S1/1 端口前, 在路由器 R3 上查看 HSRP 组的状态, 可以发现 R3 是备用路由器; 断开路由器 R1 的 S1/1 口后, 路由器 R3 的控制台提示, R3 由备用 (Standby) 状态切换到活跃 (Active) 状态, 原因是 R1 因为 S1/1 端口 Down 掉, HSRP 组 1 的优先级被减 10, 变成了 91, 而 R3 的 HSRP 组 1 优先级是 100; 再次在路由器 R3 上查看 HSRP 组的状态, 可以发现 R3 是活跃路由器, R1 成为备用路由器; 重新打开路由器 R1 的 S1/1 口后, 控制台提示路由器 R3 从活跃状态切换到发言状态 (Speak), 然后由发言状态又切换到备用状态, R1 重新又变成了活跃路由器。

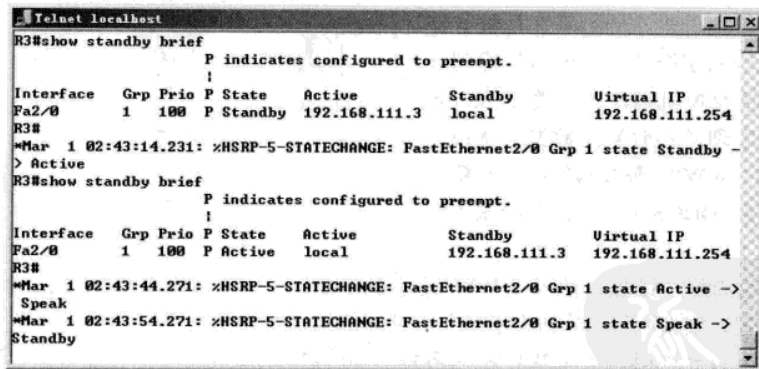


图 D-4 HSRP 状态切换

在本实验中, 正常情况下虚拟机 1 (内网) 访问虚拟机 2 (外网) 的流量都从 R1 转发出去, R3 到 R2 的链路始终闲置不用。如果内网中还有别的主机, 所有流量仍然从 R1 走, 显然有点不合理, 此时可以把内网中第二台计算机的网关指向 192.168.111.253, 同时如下配置 R1, 使之成为 HSRP 组 2 的备用路由器:


```
R1(config)#int fa 2/0
R1(config-if)#standby 2 ip 192.168.111.253
R1(config-if)#standby 2 preempt
R1(config-if)#standby 2 track s1/1
```

如下配置路由器 R3，使用之成为 HSRP 组 2 的活跃路由器：

```
R3(config)#int fa 2/0
R3(config-if)#standby 2 ip 192.168.111.253
R3(config-if)#standby 2 priority 101
R3(config-if)#standby 2 preempt
R3(config-if)#standby 2 track s1/0
```

经过这样配置就充分使用了两台路由器和两条链路，起到了冗余和负载均衡的作用。

实验 E 交换端口分析

在开始本实验之前，先介绍实际的案例：有一天，用户反映上网的速度非常慢。本单位的网络拓扑如图 E-1 所示，网管尝试着使用 telnet 登录到核心交换机，发现一切正常，再尝试着登录到出口路由器，等了很长时间才出现输入用户名和密码的窗口，好不容易连上去了，根本没有办法执行一些命令进行排错。在设备间，笔记本直接连在路由器的 Console（控制台）口上进行排查，发现路由器的反映仍然很慢，这就排除了路由器和核心交换机之间的链路故障问题；拔下路由器连接三层交换机的光纤，发现问题仍然存在，这就排除了来自内网攻击的可能；拔下路由器连接 Internet 的光纤，路由器恢复正常，初步判断攻击来自 Internet。是什么原因导致路由器的 CPU 过载，性能下降呢？由于没有光纤接口的计算机，抱着侥幸的心理，把核心交换机连接路由器的那个端口的流量镜像到连接网管工作站的交换机端口上，通过 Sniffer 捕获数据包，发现数不胜数数据包从很多个公网 IP 发往 WWW 服务器的乱七八糟端口，就是所谓的 DDOS（分布式拒绝服务）攻击。

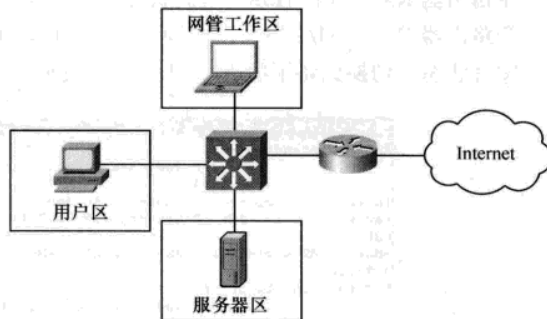


图 E-1 常见企业网络拓扑

读者可能会奇怪，既然是针对 WWW 服务器的攻击，怎么 WWW 服务器没瘫痪，出口路由器反而瘫痪了呢？根据回忆，当初为了避免内部网络用户对 WWW 服务器进行攻击，在三层交换机设置了 ACL，只允许用户访问 WWW 服务器的 80 端口，Internet 上的大量攻击包被核心交换机给丢弃了，服务器受到的影响不大。在路由器上编写 ACL，应用在路由器的对外接口，拒绝所有对 WWW 服务器非 80 端口的访问，网络恢复正常。

上面的案例中提到一种技术，交换机的端口镜像。在交换式以太网的环境下，一般交换机两个端口的通信是不会传输到交换机第三个端口的，但在某些情况下，可能需要传输到第 3 个端口，用来进行侦听，如协议分析、流量分析、入侵检测等。为此可以配置交换机的 SPAN（Switched Port

Analyzer, 交换端口分析), 有些文档上也叫端口镜像、映射端口等。SPAN 分析经过某个本地端口或 VLAN 的流量信息, 发送一份流量的拷贝给连接安全设备的交换机端口。SPAN 有 3 种模式。

- SPAN: 源端口和目标端口都处于同一交换机, 并且源端口可以是一个或多个交换机端口。
- 基于 VLAN 的交换式端口分析 (VSPAN): SPAN 的一种变体, 源端口不是物理端口, 而是 VLAN。
- 远程交换式端口分析 (RSPAN): 源端口和目标端口处于不同的交换机。

注意



一旦启用了 SPAN, VSPAN 或 RSPAN, 目标端口的 STP 功能就被禁止, 可能会造成环路。

侦听的对象可以是一个或多个交换机端口, 或者整个 VLAN。如果要侦听的端口 (源端口) 或 VLAN 和连接监控工作站或协议分析仪的端口 (目标端口) 在同一台交换机上, 如图 E-2 所示, 只需要配置 SPAN 即可。SPAN 可以在 Network 机架上配置, 如果在真实的设备上配置, 可以在协议分析设备上看到效果。启动 Network 机架中的 SW1, 配置 SPAN 的步骤如下。

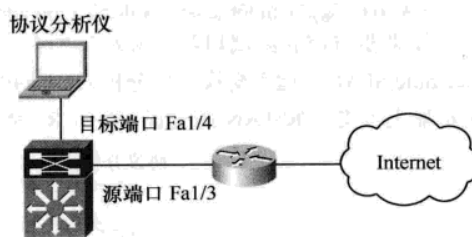


图 E-2 SPAN 拓扑

STEP 1 定义 SPAN 会话的源端口。对于有些型号的交换机, 会话数只支持两条, 即 1 和 2, 还可以定义监听流量的方向, 默认监听双向流量。如果要监听多个源端口, 可以重复多次输入命令, 也可一次输入所有端口, 本实验中假设监听 Fa1/3 和 Fa1/6-10 端口。借助在线帮助, SW1 的输入如下:

```
SW1(config)#monitor session ?      显示在线帮助, 提示该交换机只能支持 2 个会话
<1-2> SPAN session number
SW1(config)#monitor session 1 ?   要定义会话 1 的源端口还是目标端口。filter 用在源端口为 Trunk 的
端口进行 VLAN 限制过滤, 只允许指定 VLAN 的流量被复制到目的端口
destination SPAN destination interface or VLAN
filter       SPAN filter VLAN
source       SPAN source interface or VLAN
SW1(config)#monitor session 1 source ? 定义会话 1 的源端口, 源可以是端口, 也可能是 VLAN
interface   SPAN source interface
vlan        SPAN source VLAN
SW1(config)#monitor session 1 source interface ? 源端口的类型, 也可以是以太网通道
FastEthernet FastEthernet IEEE 802.3
Port-channel  Ethernet Channel of interfaces
SW1(config)#monitor session 1 source interface fa 1/3 ? 源端口的输入格式
, Specify another range of interfaces
- Specify a range of interfaces
both Monitor received and transmitted traffic
rx Monitor received traffic only
```

```
tx Monitor transmitted traffic only
```

```
<cr>
```

SW1(config)#monitor session 1 source interface fa 1/3 , fa 1/6 - 10 ? 监听源端口 Fa1/3 和 Fa1/6-10 哪个方向的流量

```
, Specify another range of interfaces
```

```
both Monitor received and transmitted traffic
```

```
rx Monitor received traffic only
```

```
tx Monitor transmitted traffic only
```

```
<cr>
```

SW1(config)#monitor session 1 source interface fa 1/3 , fa 1/6 - 10 both 监听接收和发送的双向流量

STEP 2 定义 SPAN 会话的目标端口。每条 SPAN 会话只能有一个目标端口。

SW1(config)#monitor session 1 destination interface fa 1/4 会话 1 的目标端口是 Fa1/4

如果要监控的源端口和目标端口不在同一台交换机上,如图 E-3 所示,需要配置 RSPAN (Remote SPAN, 远程交换端口分析)。不同的交换机对 RSPAN 有不同的限制,请参考设备文档,模拟器上不支持 RSPAN 的配置。配置 RSPAN 的步骤具体如下。

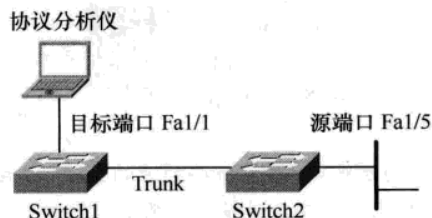


图 E-3 RSPAN 拓扑

STEP 1 创建 RSPAN 专用的 VLAN, 配置如下:

Switch1(config)#vlan 100 创建 VLAN 100

Switch2(config)#vlan 100

STEP 2 定义该 VLAN 为 RSPAN VLAN:

Switch1(config-vlan)#remote-span VLAN 100 专门用于 RSPAN

Switch2(config-vlan)#remote-span

STEP 3 定义源交换机的源端口:

Switch2(config)#monitor session 1 source interface Fa1/5 交换机 2 的源端口是物理端口 Fa1/5

STEP 4 定义源交换机的目标端口:

Switch2(config)#monitor session 1 destination remote vlan 100 交换机 2 的目标是 VLAN 100

STEP 5 定义目标交换机的源端口:

Switch1(config)#monitor session 1 source remote vlan 100 交换机 1 的源是 VLAN 100

STEP 6 定义目标交换机的目标端口:

Switch1(config)#monitor session 1 destination interface Fa1/1 交换机 1 的目标端口是 Fa1/1

注 意



配置 RSPAN 之前要先定义一个 RSPAN 专用的 VLAN。如果在 VTP 服务器上配置了 RSPAN VLAN, 那么 VTP 服务器自动将这个新加的 VLAN 信息传播给其他交换机; 否则要确保每台中间的交换机都配置有 RSPAN VLAN。

实验 F 配置 QoS

QoS (Quality of Service, 服务质量) 是网络的一种安全机制, 是用来解决网络延迟和阻塞等问题的一种技术。一般情况下, 如果网络只运行对时间不敏感的应用系统, 并不需要 QoS, 如 Web 应用或 E-mail 等。但是对关键应用和多媒体应用就十分必要, 当网络过载或拥塞时, QoS 能确保重要业务量不受延迟或丢弃, 同时保证网络的高效运行。

QoS 的执行离不开分类、标记和队列。

(1) 分类。分类是识别哪种应用产生哪种数据包, 没有分类, 网络就没有办法对特殊数据包进行特殊的处理。所有应用都会在数据包上留下可以用来识别的标识, 分类就是检查这些标识, 识别数据包是由哪个应用产生的。可以根据很多特征来识别流量, 最常使用的就是 ACL, 还可以是流量进入的接口、IP 优先级、数据包的大小等。最好是数据包一进入网络, 就能对之识别, 进行分类。

(2) 标记。在识别数据包之后, 要对它进行标记, 这样中间的网络设备才能方便地识别这种数据。由于分类可能非常复杂, 因此最好只进行一次。识别应用之后就必须对其数据包进行标记处理, 以便确保网络上的交换机或路由器可以对该应用进行优先级处理。

(3) 队列。把流量进行分类标记后, 可以使用各种队列机制对数据包进行排队, 常见的队列有 FIFO (First In First Out, 先进先出队列), LLQ (Low Latency Queuing, 低延迟队列), WFQ (Weighted Fair Queuing, 加权公平队列), CBWFQ (Class-Based Weighted Fair Queuing, 基于类的加权公平队列)。

简单了解了 QoS 的概念和工作机制后, 下面来看一个实例。某单位的网络拓扑如图 F-1 所示, 单位出口带宽有限, 可有大量的上网用户和服务器竞争有限的带宽资源, 服务器上的关键应用经常被拥塞, 导致服务器对外界的响应速度很慢, 影响了单位的效益和对外形象。现要求配置 QoS, 在网络发生拥塞时, 优先保证服务器的出口流量。

如图 F-1 所示的拓扑可以在如图 F-2 所示的实验环境中实现。在图 F-2 中, 真实机是 FTP 服务器, 虚拟机 1 和虚拟机 2 是 FTP 客户端, 两台虚拟机都可以从 FTP 服务器上下载文件。如果只有一台虚拟机下载, 该虚拟机独享带宽, 如果有两台虚拟机下载, 它们共享串行线路 1.544MB/s 的带宽。本实验要求配置 QoS, 当两台虚拟机同时下载时, 优先保证虚拟机 1 的下载, 如果虚拟机 1 不使用的情况下, 虚拟机 2 可以使用所有的可用带宽。该实验的配置步骤如下。

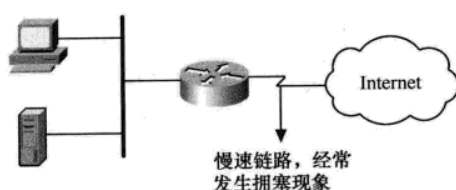


图 F-1 QoS 拓扑

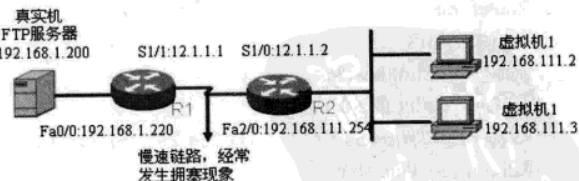


图 F-2 QoS 实验拓扑

STEP 1 配置计算机的 IP 地址。配置虚拟机 1, 网卡类型 Host-only, IP 地址 192.168.111.2, 子网掩码 255.255.255.0, 网关 192.168.111.254, DNS 是 218.2.135.1。配置虚拟机 2, 网卡类型 Host-only, IP 地址 192.168.111.3, 子网掩码 255.255.255.0, 网关 192.168.111.254, DNS 是 218.2.135.1。配置真实

机,物理网卡的 IP 地址 192.168.1.200,子网掩码 255.255.255.0,网关 192.168.1.220,DNS 是 218.2.135.1。

STEP 2 安装 Serv-U。这里不使用 IIS 集成的 FTP 服务,在真实机上安装第 5 章介绍的 Serv-U 软件,把真实机配置成 FTP 服务器。这里使用 Serv-U 的主要原因是因为在 Serv-U 的管理界面中可以看到每一个客户正在下载的速度。Serv-U 安装后的界面如图 F-3 所示,这里 FTP 服务使用的端口是 2121,用户也可以更改成其他任何没有被使用的端口。

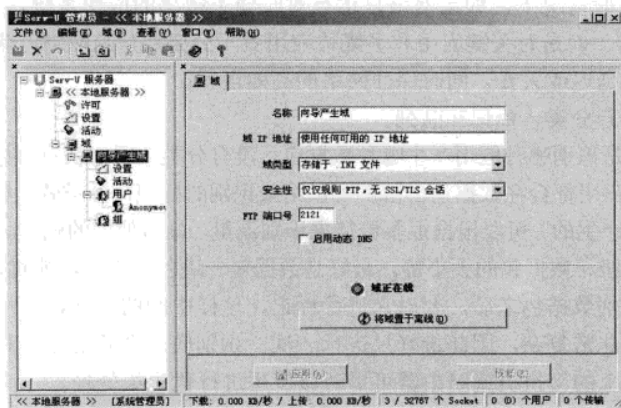


图 F-3 Serv-U 主界面

STEP 3 配置路由器。R1 的配置如下:

```
Router>en
Router#conf t
Router(config)#host R1
R1(config)#int fa 0/0
R1(config-if)#ip add 192.168.1.220 255.255.255.0
R1(config-if)#no shut
R1(config-if)#int s1/1
R1(config-if)#ip add 12.1.1.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#no cdp run
R1(config)#ip route 0.0.0.0 0.0.0.0 12.1.1.2
```

R2 的配置如下:

```
Router>en
Router#conf t
Router(config)#host R2
R2(config)#int fa 2/0
R2(config-if)#ip add 192.168.111.254 255.255.255.0
R2(config-if)#no shut
R2(config-if)#int s1/0
R2(config-if)#ip add 12.1.1.2 255.255.255.0
R2(config-if)#no shut
R2(config-if)#no cdp run
R2(config)#ip route 0.0.0.0 0.0.0.0 12.1.1.1
```


STEP 4 测试两台虚拟机的下载速度。在虚拟机 1 和虚拟机 2 上同时从 FTP 服务器上下载文件。在真实机上打开 Serv-U 控制台,如图 F-4 所示,最下面的状态栏上显示下载的速度是“114.0KB/秒”,从右边的窗口中,可以看到有两个用户正在下载,分别是虚拟机 1 和虚拟机 2,当前选中的是虚拟机 2,提示虚拟机 2 下载的速度是“53.17KB/秒”,可以看出两台虚拟机下载的速度相差无几。

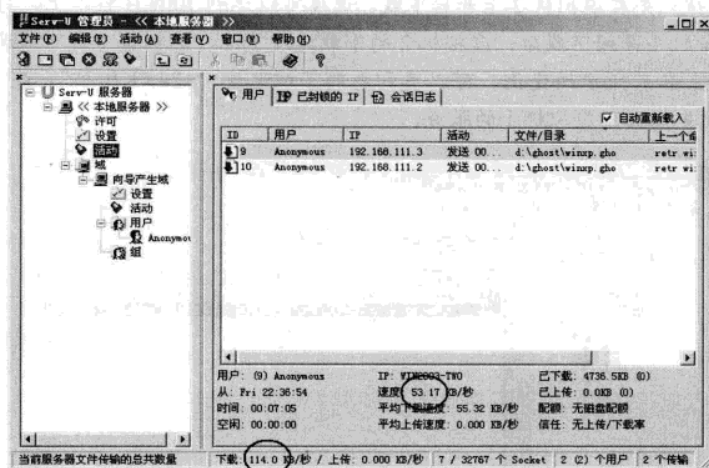


图 F-4 应用 QoS 前查看下载用户

STEP 5 配置 QoS 第 1 步,区分流量。这里使用 ACL 抓取虚拟机 1 的流量, R1 的配置如下:
 R1(config)#access-list 100 permit ip any host 192.168.111.2 在路由器 R1 上,把从 FTP 服务器返回到虚拟机 1 的流量区分出来

STEP 6 配置 QoS 第 2 步,创建分类 class-map。R1 的配置如下:

R1(config)#class-map pc1 创建 class-map, 名字叫 pc1

R1(config-cmap)#match access-group 100 满足 ACL 100 的流量属于 pc1 这个类

STEP 7 配置 QoS 第 3 步,创建策略 policy-map。R1 的配置如下:

R1(config)#policy-map llq 配置 policy-map, 名字叫 llq, 这里取的名字比较直观,是 LLQ (低延迟队列的意思)

R1(config-pmap)#class pc1 调用类,符合前面定义的 pc1 类的流量

R1(config-pmap-c)#priority ? priority 是优先的意思,也就是说拥塞发生时,类 pc1 可以得到带宽保证,这时也称绝对优先,配置的是一个 LLQ (低延迟队列)。有两种方式分配优先带宽,一种是绝对值,如多少 KB,串行线路的默认带宽是 1554KB/s,但默认只能使用带宽的 75%,除非在接口下使用命令“max-reserved-bandwidth 100”,申明要使用所有的带宽。另一种是使用百分比,默认情况下,也不允许使用超过 75%。

<8-2000000> Kilo Bits per second

percent % of total bandwidth

R1(config-pmap-c)#priority percent 70 优先使用接口带宽的 70%,相当于优先使用 1.544*0.75*0.7MB/s 带宽

R1(config-pmap-c)#exit

R1(config-pmap)#class class-default 一个策略下可以有多个类,使用类之前要先定义类,但有一个类除外,那就是 class-default,这个是系统预定义好的类,意指所有默认流量。这个名字要记住,不能拼错

R1(config-pmap-c)#fair-queue 对默认类,采用加权公平队列

可以在策略中针对某个特殊的类使用 set 命令进行标记,如设置 IP 优先级,尤其是中间要经

过多台设备时,中间设备可以使用 IP 优先级来区别对待流量。

STEP 8 配置 QoS 第 4 步,应用策略 service-policy。R1 的配置如下:

R1(config)#int s1/1 在路由器 R1 的外出接口

R1(config-if)#service-policy output llq 在流量的外出方向应用策略 llq

STEP 9 测试。先在虚拟机 2 上开始下载,速度可以达到 100KB/秒以上,再在虚拟机 1 上也开始下载。虚拟机 1 开始下载后,虚拟机 2 的下载速度下降,虚拟机 1 的下载速度增加。一段时间后,显示如图 F-5 所示的变化,可以看到总的下载速度“124.5KB/秒”,虚拟机 1 占用了“111.4KB/秒”,优先保证了虚拟机 1 的服务。

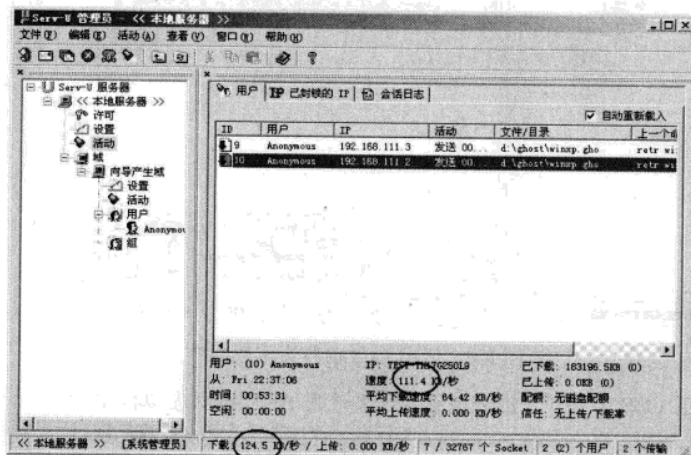


图 F-5 应用 QoS 后查看下载用户

在实际工程中,可以根据使用的服务、数据包的特征、时间段等定义出更灵活、更符合实际的 QoS 策略。现在 QoS 比较常见被部署在有语音服务的网络中,因语音包对延时和抖动比较敏感,需要保证绝对的优先。

实验 G 网络负载均衡

高性能服务器通常是通过 SMP、MPP 等并行扩展技术实现的,然而通过并行扩展技术实现的高性能服务器在现代企业或一些关键行业应用中,逐步显露出种种弊端。技术实现难度大,配置和管理都较复杂,而且像 SMP 这种常见的扩展技术还受到诸多限制,性能提高非常有限,很难应对大规模的网络应用。一台服务器难免会遇到像死机、系统升级等必须重新启动才能解决的问题,可服务器一旦重启或死机,就会造成服务的中断,影响用户的使用,再好再完善的服务器也难保证 365×24 无间断运行。解决的办法就是采用集群技术,多台服务器之间相互协作,实现冗余和负载均衡,以保证整个服务的可用性。

从 Windows 2000 Advanced Server 起,微软将群集技术纳入了操作系统。在 Windows Server 2003 中,微软提供了 3 种类型的群集技术:服务器群集、组件负载均衡和网络负载均衡。网络负载均衡群集和服务器群集在说法上比较相近,很容易造成混淆。下面对两者的功能和作用简单描

述如下。

● 网络负载均衡。对于要求同时响应大量用户访问请求的服务器（如 Web、FTP 服务器等），仅使用单台服务器很难满足用户对性能的要求。使用网络负载均衡，可将多个运行相同应用程序或服务的服务器群集到一起，并共享一个虚拟 IP 地址，客户机通过虚拟的 IP 地址访问群集中的服务器，网络负载均衡负责将用户的访问请求均衡的分配给群集中不同的服务器。当某台服务器发生故障时，网络负载均衡会在其他服务器之间重新分配工作量，从而为应用程序提供高性能和高可用性。Windows Server 2003 的 NLB（Network Load Balancing，网络负载均衡）功能最多可将 32 个服务器群集到一起。

● 服务器群集。服务器群集允许客户端在出现故障和计划中的暂停时，依然能够访问应用程序和资源。如果群集中的某一台服务器由于故障或维护需要而无法使用，资源和应用程序将转移到可用的群集节点上。对于“Windows 群集”解决方案，使用“高可用性”这个术语要比使用“容错”更为合适。服务器群集无法保证无间断运作，但是确实能够为多数关键任务应用程序提供足够的可用性。群集服务可以对应用程序和资源进行监控，并能够自动识别和恢复众多故障状况，这为在群集中管理工作负荷提供了灵活性。另外，还提高了整个系统的可用性。

通过上面的对比，可以看出网络负载均衡强调的是冗余和负载均衡，适合于只提供浏览或下载的场所；服务器群集强调是高可用性，更适合于需要用户提交数据的场合。本实验中仅介绍网络负载均衡。

网络负载均衡使用由两个或多个主机相互协作而构成的群集提供 Web 服务器或其他应用程序服务器的高可用性和可伸缩性，客户端使用单一的 IP 地址访问群集。客户机不能区分单个服务器和群集。服务器程序也无法识别它们是否运行在群集中。然而，网络负载均衡的群集明显区别于运行单个服务器程序的单个主机，这是因为即使某个群集主机出现故障，网络负载均衡的群集也能提供不间断的服务。群集还能对客户请求做出比单个主机更快的反应。如果某个主机发生故障或脱机，网络负载均衡通过把接收的网络通信重定向到正在工作的群集主机来提供高可用性。当与某个脱机主机的现有连接丢失，在多数情况下（例如，使用 Web 服务器时），客户软件会自动重试失败的连接，并在接收响应时仅有几秒的延迟。

网络负载均衡通过将进入的网络通信分布在一个或多个指定到网络负载均衡群集的虚拟 IP 地址来实现性能的可伸缩性。群集中的主机可同时响应不同的客户请求，即使是同一主机的多个请求也是如此。例如，Web 浏览器可以在一个 Web 页中显示来自网络负载均衡群集中不同主机的多个图像，这样可以加快处理客户请求的速度并缩短对客户响应时间。在单个子网内，所有使用网络负载均衡群集的主机同时在群集的主 IP 地址（以及在多宿主主机的其他 IP 地址）上检测接收的网络通信。在每个群集主机上，网络负载均衡驱动程序就像是群集适配器驱动程序和 TCP/IP 之间的筛选器，允许由主机接收部分传入的网络通信。

网络负载均衡使用完整的分布式算法进行统计并通过外来客户端的 IP 地址、端口和其他信息将其映射到群集主机。检查到达的数据包时，所有的主机同时执行该映射，以迅速确定负责处理该数据包的主机。除非群集主机的数目改变，否则该映射保持不变。为了协调这些操作，网络负载均衡主机在群集内周期性地交换多播或广播消息。这允许它们监视群集的状态。当群集状态改变时（如主机失败，离开或加入群集），网络负载均衡调用一个叫做收敛的过程，在此过程中主机交换消息来确定群集新的一致状态，并选出拥有最高主机优先级的主机作为默认主机。当所有群集主机对群集的新状态达成一致后，它们将在 Windows Server 2003 事件日志中记

录收敛的完成情况。

在收敛过程中,正常主机继续处理接收的网络通信,但故障主机不能接收客户请求,正在工作的主机客户请求不受影响。在收敛完成时,故障主机的通信被重新分发到其余的主机。如果某个主机添加到群集中,收敛允许该主机接管端口的处理,并接收它承担的负载均衡通信。群集的扩展不影响正在进行的群集操作,并对客户端和服务端程序透明。然而,由于客户端可能会被重新映射到不同的群集主机上,它可能会影响跨越多个 TCP 连接的客户端会话。

网络负载均衡假设群集中的主机只要能够与群集中的其他主机间进行正常的报文交换,该主机便是正常的。如果其他主机在报文交换的某些时段内不能从某个成员接收到响应,它们将初始收敛来重新分配由故障主机处理的负载。用户可以控制启动收敛操作所需的报文交换周期和丢失报文的数目。默认值分别为 1 000 毫秒 (1s) 和 5 个丢失报文。由于这些参数不经常修改,所以它们在“网络负载均衡属性”对话框中是不可配置的。若有必要可在注册表中手工调整。本实验拓扑如图 G-1 所示,实验的操作步骤如下。

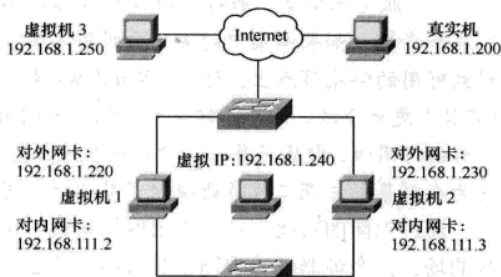


图 G-1 网络负载均衡实验拓扑

STEP 1 网络基本配置。编辑虚拟机 1 和虚拟机 2,

每台虚拟机都配置两块网卡。配置虚拟机 1, 第一块网卡类型 Host-only, IP 地址 192.168.111.2, 子网掩码 255.255.255.0, 网关无, DNS 是 218.2.135.1; 第二块网卡类型 Bridged, IP 地址 192.168.1.220, 子网掩码 255.255.255.0, 网关 192.168.1.1, DNS 是 218.2.135.1。配置虚拟机 2, 第一块网卡类型 Host-only, IP 地址 192.168.111.3, 子网掩码 255.255.255.0, 网关无, DNS 是 218.2.135.1; 第二块网卡类型 Bridged, IP 地址 192.168.1.230, 子网掩码 255.255.255.0, 网关 192.168.1.1, DNS 是 218.2.135.1。

对内网卡是群集内部通信所用,有些文档中也称心跳线。

STEP 2 管理员设置。虚拟机 1 和虚拟机 2 都安装 Window 2003 操作系统,并设置相同的管理员用户名和密码。在实验中发现,如果两台计算机的用户名和密码不一样,连接的时候会产生“错误代码 0x800706d5”的错误提示,如果两台计算机都加入了域,则无需用户名和密码一致。

STEP 3 网络负载均衡中配置群集参数。在虚拟机 1 上,选择“开始”→“程序”→“管理工具”→“网络负载均衡管理器”,打开“网络负载均衡管理器”对话框,选择“群集”菜单的“新建”命令,打开“群集参数”对话框,如图 G-2 所示进入配置。

在群集 IP 配置中填入虚拟 IP 地址 (192.168.1.240)、子网掩码、完整 Internet 名称 (申请的有效域名,本实验中使用 IP 测试,这里保持默认值就可以了),在群集操作模式中选择“多播”。工程中根据网络环境选择“单播”或“多播”,二者各有优缺点。单击“下一步”按钮继续。

STEP 4 网络负载均衡配置中添加群集 IP 地址。如图 G-3 所示,询问群集虚拟的 IP 地址,如果虚拟的 IP 不止一个,可以单击“添加”按钮,继续添加新的虚拟 IP,因本实验中只虚拟一个 IP 地址 192.168.1.240,单击“下一步”按钮继续。

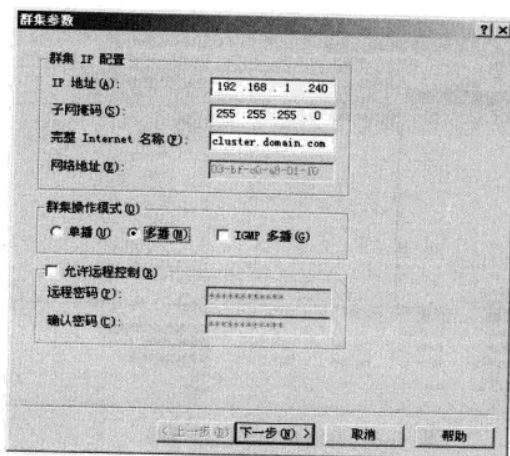


图 G-2 群集参数配置

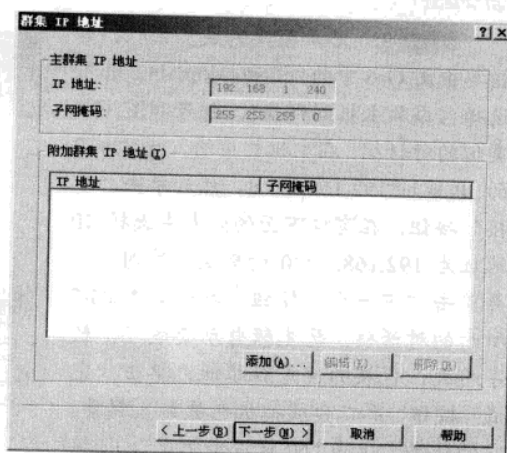


图 G-3 群集 IP 地址

STEP 5 网络负载均衡中编辑端口规则。新建群集向导会询问端口规则设置，这里保持默认设置，单击“下一步”按钮继续。

STEP 6 网络负载均衡中连接成员主机。在“连接”对话框中，输入群集第一个成员主机的 IP 地址，如 192.168.111.2，单击“连接”按钮，下面窗口中列出了该主机可用的端口，如图 G-4 所示。选中群集接口，也就是 IP 地址为 192.168.1.220 的那块网卡。单击“下一步”按钮继续。

STEP 7 网络负载均衡中设置主机参数。新建群集向导会询问主机参数设置，如图 G-5 所示，这里保持默认设置，单击“完成”按钮继续。

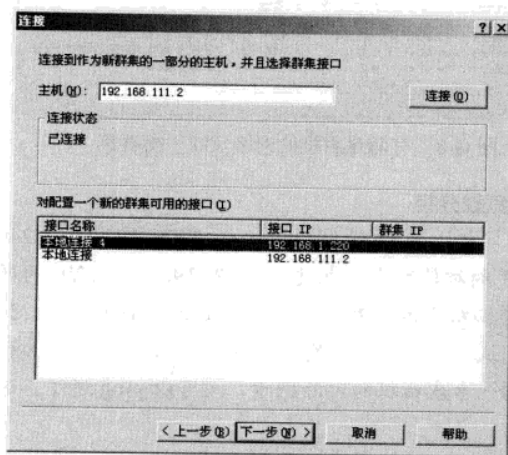


图 G-4 连接成员主机

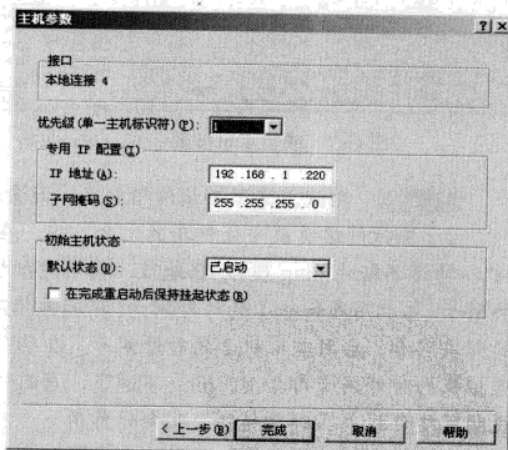


图 G-5 主机参数

STEP 8 完成新建群集向导。新建群集向导完成后，界面如图 G-6 所示，注意右边窗口中已经有了一个成员主机，当前的状态是“挂起”，稍后变成“正在聚合”，再等一会儿，状态会变成“已聚合”。

STEP 9 添加群集的成员主机。右键单击图 G-6 中的“cluster.domain.com”，选择“添加主机到群集”，打开和图 G-4 类似的对话框，在主机栏中输入虚拟机 2 的 IP 地址 192.168.111.3，然后单击“连接”按钮，在窗口下面的列表中选择 IP 地址为 192.168.1.230 的那块对外网卡，再单击“下一步”按钮，打开如图 G-7 所示的对话框，优先级自动变成 2，数字越大，代表的优先级越低。单击“完成”按钮，第二台虚拟机也被加入群集。它的状态变化是“NLB 没有绑定”→“挂起”→“正在聚合”→“已聚合”。

至此，有两台服务器的网络负载均衡群集已经完成，如图 G-8 所示。

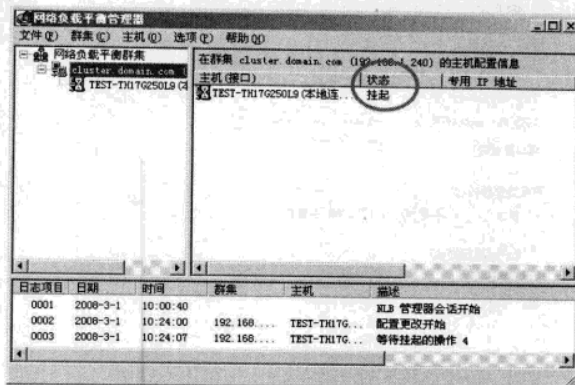


图 G-6 网络负载均衡管理器

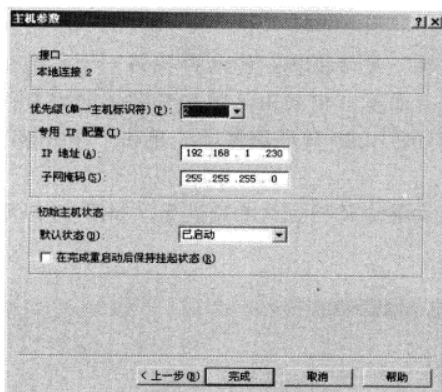


图 G-7 成员主机参数

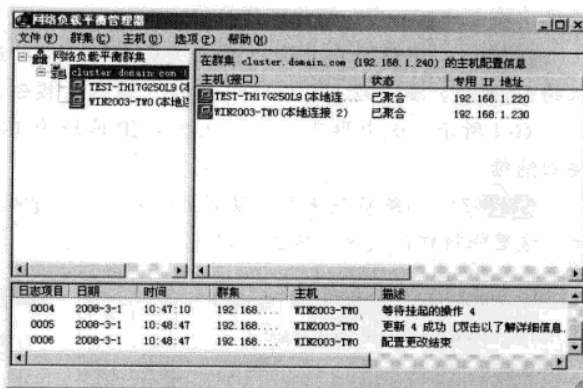


图 G-8 有两台主机的网络负载均衡群集

STEP 10 测试。这里测试两项内容：冗余和负载分担。

● 测试网络负载均衡群集的冗余作用。在真实机上的 DOS 窗口中执行“ping 192.168.1.240 -t”，持续不断地 ping 虚拟 IP 地址。禁用虚拟机 1 的对外网卡，也就是 IP 为 192.168.1.220 的那块网卡，再启用虚拟机 1 的对外网卡；稍后再禁用虚拟机 2 的对外网卡，也就是 IP 为 192.168.1.230 的那块网卡，启用虚拟机 2 的对外网卡。在整个测试过程中，可以发现 ping 一直是通的。把两台虚拟机的对外网卡都禁用，ping 不通了，启用任意一台虚拟机的对外网卡，又可以 ping 通了。这说明网络负载均衡群集起到了冗余的作用。

● 测试网络负载均衡群集的负载分担作用。在参与网络负载均衡群集的虚拟机 1 和虚拟机 2 上都配置 IIS 服务，使两个 Web 站点的内容不同。在真实机的 IE 地址栏中输入 http://192.168.1.240，在虚拟机 3 的 IE 地址栏中也输入 http://192.168.1.240，发现两台计算机上看到的 Web 内容不同，关闭群集中的虚拟机 1。在真实机和虚拟机 3 上访问 http://192.168.1.240，都可以访问，两台计算机看到的 Web 内容相同。这说明网络负载均衡群集起到了负载平衡以及

冗余的作用。实际中如果想到负载均衡的作用，需要在各个群集成员服务器中提供相同的内容。

实验 H 限制 BT 流量

对于一般单位来说，BT（BitTorrent，比特洪流）下载是个令人头痛的问题。BT 下载是基于 P2P 技术实现点对点来传输数据，不仅有大量的下载流量，还有大量的上传活动，这种下载方式可以抢占带宽来达到下载目的。如果内网有大量的 BT 下载，可能引起内部网络拥塞、造成数据传输延迟，更加严重的可能会造成整个网络的瘫痪。下面介绍几种限制 BT 下载的方法。

1. 限制浏览 BT 网站

BT 网站很多，但考虑到 BT 下载的特点是下载的人数越多，速度越快；种子越多，速度越快。只有比较热门 BT 网站的 Torrent 文件（BT 的种子文件）下载的人才会比较多，一般的 BT 网站用户比较少，下载的人数也少，所以下载速度也比较慢。因此针对比较热门的 BT 网站，获得服务器地址后就可以到核心服务器上对该地址进行封锁。以 Cisco 设备为例，具体命令为：

```
Router(config)#access-list 100 deny ip any host 59.33.38.103 假设这里的 59.33.38.103 是一个 BT 热门站点
Router(config)#access-list 100 permit ip any any 允许其他所有的流量
Router(config)#int fa 0/0 配置路由器的对外接口
Router(config-if)#ip access-group 100 out 调用 ACL 100，拒绝发往 BT 站点的流量
```

这种方法使用 ACL 命令来控制，实现起来比较容易。但由于 BT 网站比较多而且层出不穷，因而 ACL 命令的条数会因为 BT 服务器的数量增加而增加，随着 ACL 命令条数的增多，路由器的负荷也随之增加。从实际操作上来看，BT 的种子网站众多，而且无须固定的服务器，因而这种监控难度也很大，技术上难以实现。

2. 封闭 BT 下载端口

解决 BT 对局域网的危害，最彻底的方法是不允许进行 BT 下载，BT 一般使用 TCP 的 6881~6889 的端口，网络管理员可以根据网络流量的变化进行判断，在网关中将特定的种子发布站点和端口封掉，在 BT 下载软件中可以获得这些信息。但是现在大多数 BT 软件可以修改端口号，因此网管可以根据实际情况，利用访问控制列表在不影响正常业务的情况下尽可能将封闭的端口范围扩大，把一些特定的种子发布站点和端口进行封闭。以 Cisco 设备为例，具体命令为：

```
Router(config)#access-list 101 deny tcp any any range 6880 6890
Router(config)#access-list 101 deny tcp any range 6880 6890 any
Router(config)#access-list 101 permit ip any any
```

接着进入相应的端口，调用 ACL，配置生效后，网络带宽马上就会释放出来，网络速度得到提升。

这种方法也使用 ACL 命令来控制，实现起来比较容易。但是由于 BT 可以自由变换端口，因此势必要封堵大量的端口，封闭端口必然影响网络的应用。有些网络管理员甚至仅仅打开 80、53、21、25、110 等常用端口而封闭其他所有端口。

3. 使用 QoS 结合 NBAR

上面介绍的两种方法，一个是对数据包的目标地址进行封锁，另一个是对数据包使用的端口进行封锁，虽然在一定范围内有效，但不能起到全面禁止 BT 的作用，通过使用 QoS 结合 NBAR (Network Based Application Recognition, 基于网络应用识别) 的方法来封锁 BT 就不存在这个问题。本实验的拓扑如图 H-1 所示，虚拟机 1 是 BT 客户端，通过配置路由器限制 BT 下载。启动安全机架中的路由器 R1，本实验的配置步骤如下。

STEP 1 准备虚拟机。配置虚拟机 1，网卡类型 Host-only，IP 地址 192.168.111.2，子网掩码 255.255.255.0，网关 192.168.111.254，DNS 是 218.2.135.1。在虚拟机 1 上安装 dianlei_3.0.exe (电雷) 软件。

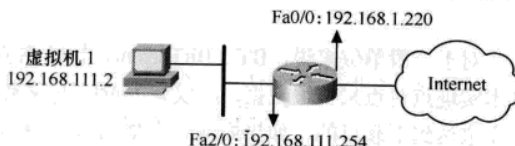


图 H-1 限制 BT 流量拓扑

STEP 2 配置路由器共享上网。R1 的配置如下：

```
Router>en
Router#conf t
Router(config)#host R1
R1(config)#int fa 0/0
R1(config-if)#ip add 192.168.1.220 255.255.255.0
R1(config-if)#no shut
R1(config-if)#ip nat outside
R1(config-if)#int fa 2/0
R1(config-if)#ip add 192.168.111.254 255.255.255.0
R1(config-if)#no shut
R1(config-if)#ip nat inside
R1(config-if)#no cdp run
R1(config)#access-list 1 permit any
R1(config)#ip nat inside source list 1 interface fa 0/0 overload
R1(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.1
```

STEP 3 测试 BT 下载。在虚拟机 1 上测试 BT 下载速度，如图 H-2 所示，下载的速度是 192.85KB/s。

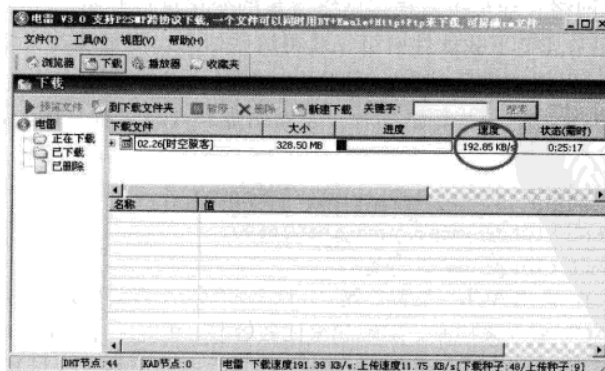


图 H-2 限制 BT 下载前

STEP 4 配置 QoS 和 NBAR。

R1(config)#class-map bt 创建一个类, 名字叫 bt
 R1(config-cmap)#match protocol bittorrent 满足使用的协议是 bittorrent, 这里使用的是 NBAR 功能, 工程中的路由器可能不支持 BT 选项, 读者可以升级 IOS 到新版, 或者从思科网站下载 PDLM (Packet Description Language Module, 包描述语言模块), 并把 PDLM 加载到路由器中

R1(config-cmap)#exit
 R1(config)#policy-map deny-bt 创建 policy-map, 名字叫 deny-bt
 R1(config-pmap)#class bt 调用前面创建的类 bt
 R1(config-pmap-c)#drop 对满足 bt 类的流量, 进行丢弃, 这里也可以进行限速操作
 R1(config-pmap-c)#int fa 0/0 进入路由器的对外接口
 R1(config-if)#service-policy output deny-bt 丢弃上传的 BT 流量
 R1(config-if)#int fa 2/0 进入路由器的对内接口
 R1(config-if)#service-policy output deny-bt 丢弃下载的 BT 流量

STEP 5 测试。观察虚拟机 1 上 BT 下载的速度, 如图 H-3 所示, 下载的速度是 6.79KB/s, 可以看到, BT 下载的速度已大大降低。但是 BT 怎么没有被完全禁止掉? 原因是因为 BT 软件也在不断更新变化, NBAR 并没有识别所有的 BT 特征码。

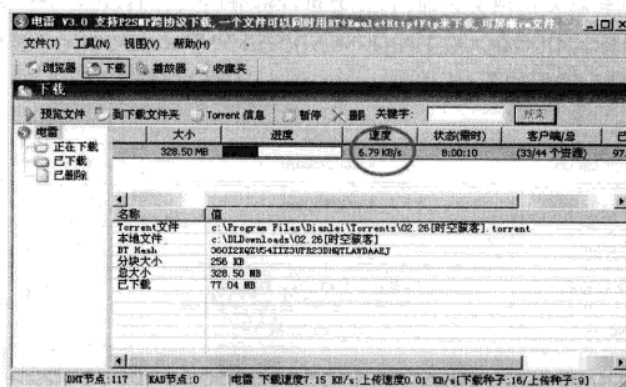


图 H-3 限制 BT 下载后

如果不想全封, 而是限制流量在一个范围内, 可以把步骤 4 中的 drop 换成 police, 再跟上具体的限速范围; 如果只想在特定的时间段封, 在写 CLASS-MAP 时可以写多个匹配, 编写基本时间段的 ACL。如下面的配置:

R1(config)#access-list 100 permit ip any any time-range work 先定义上班时间段 work
 R1(config)#class-map bt 创建一个类, 名字叫 bt
 R1(config-cmap)#match protocol bittorrent 满足使用的协议是 BT
 R1(config-cmap)#match access-group 100 满足 ACL 100, 同一个类中写了两个条件, 它们之间的关系由创建类的时候决定, class-map bt 相当于 class-map match-all bt, 读者可以使用 show running-config 进行验证, 也就是说所有条件都要满足。如果想创建一个类, 里面的条件是或的关系, 可以使用 class-map match-any 类名。如果创建类的时候没有指明是 match-all 还是 match-any, 缺省使用的是 match-all。这里创建的 bt 类是指既满足是 ACL 100 发出的, 同时又是 BT 的流量, 也就是上班时间进行 BT 下载将被拒绝

使用 QoS 结合 NBAR 的方法也有缺陷, 如果数据包流量很大, NBAR 会占用很多的 CPU; BT 软件不断在更新, BT 的特征码也在发生变化, NBAR 并不能识别所有的 BT 特征码, 有

时达不到理想的效果。目前比较理想的封锁 BT 的方法，一般都是在应用层的网关设备上进行封锁。

实验 I ARP 攻击的攻、判、防

ARP 攻击不是病毒——因而几乎所有的杀毒软件对之都无可奈何；但它却胜似病毒——因为它轻可造成通信变慢、网络瘫痪，重则造成信息的泄密。多年来，ARP 攻击一直存在，却没有一个好的解决办法。很多网络用户深受其害，网管人员更是无从下手、苦不堪言。本实验从分析 ARP 协议和欺骗原理入手，介绍如何实施 ARP 攻击，如何判断正在遭受 ARP 攻击，如何防范和解决 ARP 攻击。

1. ARP 协议及欺骗原理

(1) 以太网的工作原理。

在以太网中，数据包被发送出去之前，首先要进行拆分(把大的包进行分组)、封装(在 Network 层添加源 IP 地址和目标的 IP 地址，在 Data Link 层添加源 MAC 地址和下一跳的 MAC 地址)，变成二进制的比特流，整个过程如图 I-1 所示。

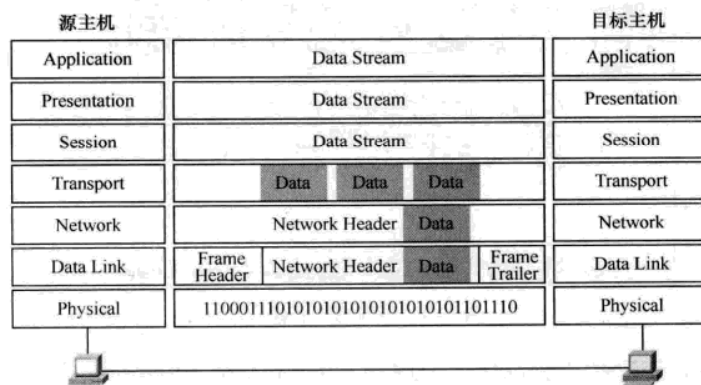


图 I-1 数据的封装和解封装

数据包到达目标后再执行与发送方相反的过程，把二进制的比特流转变成帧，解封装 (Data Link 层首先比较目标的 MAC 是否与本机网卡的 MAC 相同或者是广播 MAC，如相同则去除帧头，再把数据包传给 Network 层，否则丢弃；Network 层比较目的地 IP 地址是否与本机相同，相同则继续处理，否则丢弃)。如果发送方和接收方位于同一个网络内，则下一跳的 MAC 就是目标的 MAC，如发送方和接收方不在同一个网络内，则下一跳的 MAC 就是网关的 MAC。从这个过程不难发现，以太网中数据的传输仅知道目标的 IP 地址是不够的，还需要知道下一跳的 MAC 地址，这需要借助于另外一下协议 ARP (地址解析协议)。

(2) ARP 的工作原理。

计算机发送封装数据之前，对比目标 IP 地址，判断源和目标在不在同一个网段，如在同一网段，则封装目标的 MAC；如不在同一网段，则封装网关的 MAC。封装之前，查看本机

的 ARP 缓存,看有没有下一跳对应的 IP 和 MAC 映射条目,如有则直接封装;如没有则发送 ARP 查询包。

ARP 查询和应答包的格式如图 I-2 所示,查询包中“以太网目的地址”为 0xffffffff 广播地址,“以太网源地址”为本机网卡的 MAC 地址,“帧类型”为 0x0806 表示 ARP 应答或请求,“硬件类型”为 0x0001 表示以太网地址,“协议类型”为 0x0800 表示 IP 地址,“OP”为 ARP 的请求或应答,ARP 请求包的 OP 值为 1,ARP 应答包的 OP 值为 2,“发送端以太网地址”为发送者的 MAC 地址,“发送端 IP”为发送者的 IP 地址,“目的以太网地址”这里为 0x000000000000,“目的 IP”为查询 MAC 地址的 IP。此包以广播形式发送到网络上,局域网中所有的计算机均收到此包,只有本机 IP 地址为“目的 IP”的计算机对此数据包进行响应,并回复此数据包。当始发送端方收到此 ARP 应答包后,即获取到目标 IP 对应的 MAC 地址,然后就可进行数据包的封装了。

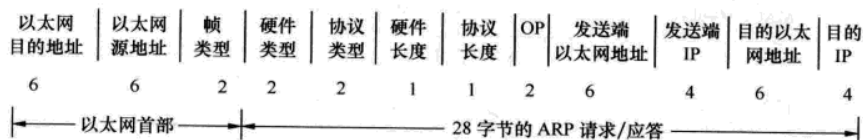


图 I-2 ARP 的查询和应答包格式

(3) ARP 的欺骗。

与 TCP 通过序列号和确认号字段不同,实施 3 次握手来保证数据传输的可靠性,ARP 是一个无状态的协议,也就是说不管有没有发送 ARP 请求,只要有发往本机的 ARP 应答包,计算机都不加验证的接收,并更新自己的 ARP 缓存。了解 ARP 的工作原理后,只要有意图地填充图 I-2 中的某些字段,即可达到 ARP 攻击的效果:IP 地址冲突、ARP 欺骗、ARP 攻击等。

● IP 地址冲突。计算机检测本机 IP 地址是否在网上被使用的方法是用本机 IP 地址作为目的 IP 地址,发送 ARP 查询包,如果收到应答,则说明本 IP 地址已经在网上被使用,弹出 IP 地址被使用对话框,释放出本机的 IP 地址。ARP 攻击者利用这一原理,用任意的 MAC 地址(非被攻击者真实的 MAC 地址)填充“发送端以太网地址”字段,用被攻击者的 IP 地址填充“发送端 IP”字段,用被攻击者的真实 MAC 地址填充“目的以太网地址”字段,用被攻击者的 IP 地址填充“目的 IP”字段,OP 的值为“2”,如图 I-3 所示。当被攻击者收到这样的 ARP 应答后,就认为本机的 IP 地址在网络上已经被使用,弹出 IP 地址冲突对话框。

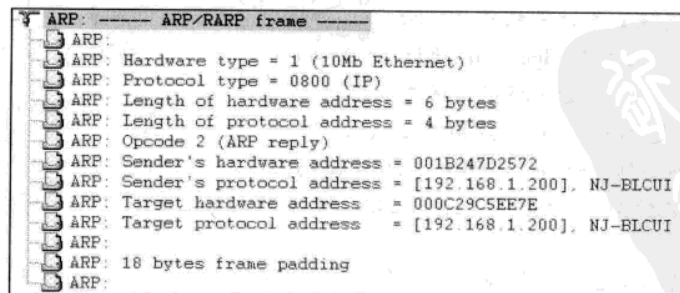


图 I-3 IP 地址冲突的 ARP 应答包

● ARP 欺骗。如图 I-4 所示, PC1 是攻击者, 攻击的目的是“中断 PC2 与网关的通信”。PC1 生成一个 ARP 应答信息包, “发送端的 IP” 填写成网关的 IP 地址, “发送端以太网地址” 填写一个非网关的 MAC 地址 (这个地址可以随机生成), “目的 IP” 填写 PC2 的 IP 地址, “目的以太网地址” 填入 PC2 的 MAC 地址。主机 PC2 收到这个最新的 ARP 应答信息包后, 就会用这个不正确的网关的 MAC 地址更新自己的 ARP 缓存表, 以后 PC2 后就这个错误的 MAC 地址进行封装, 造成封装后的数据包无法正确到达网关; PC1 类似的再发送一个不正确 ARP 应答包给网关, “发送端的 IP” 填写成 PC2 的 IP 地址, “发送端以太网地址” 填写一个非 PC2 的 MAC 地址 (这个地址可以随机生成), “目的 IP” 填写网关的 IP 地址。网关收到这样的 ARP 应答信息后, 也在缓存中保存了错误的 PC2 映射条目。PC1 周期性向网关和 PC2 发送这样的包, 以免它们的 ARP 表老化, 这样就达到了阻止它们通信的目的。

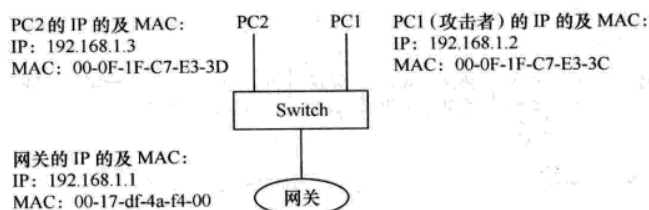


图 I-4 ARP 欺骗示意图

● ARP 攻击。又称为中间人攻击 (Man-in-the-middle Attack), 与 ARP 欺骗类似, 只是 PC1 发送 ARP 请求时, 所填入的“发送端以太网地址”不是随机生成, 而是替换成 PC1 本机的 MAC 地址, 开启 PC1 的路由功能——修改 (添加) 注册表选项 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\IPEnableRouter = 0x1, 同时在 PC1 上安装窃听软件, 截获 PC2 与网关之间所有的通信包。

2. 如何实施 ARP 攻击

这里介绍两款 ARP 攻击软件的使用方法, 拓扑如图 I-5 所示。

第一款软件主要用于攻击, 破坏正常的网络通信, 如图 I-5 所示, 在虚拟机 2 上安装“网络执法官”软件, 破坏虚拟机 1 和真实机之间的正常通信, 实验步骤如下。

STEP 1 正确配置各计算机的 IP 地址。虚拟机 1 的网卡类型 Bridged, IP 地址是 192.168.1.220, 掩码 255.255.255.0, 网关 192.168.1.1, DNS 是 218.2.135.1。虚拟机 2 的网卡类型 Bridged, IP 地址是 192.168.1.210, 掩码 255.255.255.0, 网关 192.168.1.1, DNS 是 218.2.135.1。真实机的 IP 地址是 192.168.1.200, 掩码 255.255.255.0, 网关 192.168.1.1, DNS 是 218.2.135.1。

STEP 2 在虚拟机 2 上安装 WinPcap。解压缩“网络执法官.rar”文件, 双击“WinPcap30.exe”文件, 开始安装 WinPcap。

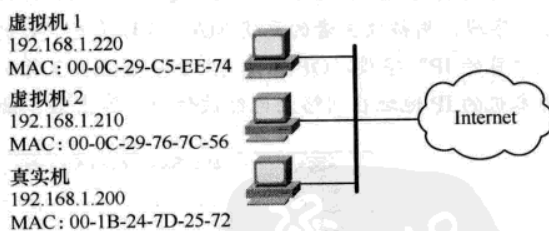


图 I-5 ARP 攻击

STEP 3 在虚拟机 2 上安装网络执法官软件。双击“网络执法官 2.8 破解版.exe”文件开始安装网络执法官。

STEP 4 运行网络执法官。第一次运行执法官，打开如图 I-6 所示的对话框，提示进行监控参数选择。

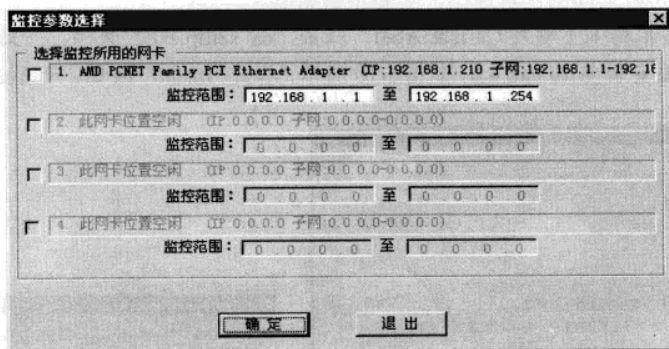


图 I-6 监控参数选择

STEP 5 因为只有一块网块，选中最上面的网卡复选框，单击“确定”按钮。打开如图 I-7 所示的“监控范围选择”对话框，在指定监控范围中列出网卡所在子网的所有可用 IP 地址，单击“添加/修改”按钮，把监控范围加入后，单击“确定”按钮。

STEP 6 攻击前测试。在虚拟机 1 上，打开 DOS 窗口，输入“ping 192.168.1.200 -t”，持续地 ping 真实机的 IP 地址，可以发现是通的。不要关闭该窗口。

STEP 7 开始攻击。网络执法官软件可以监测到同一个子网中所有在线的主机，在网络执法官的管理界面中，右键单击真实机，从快捷菜单中选择“手工管理”命令，如图 I-8 所示。

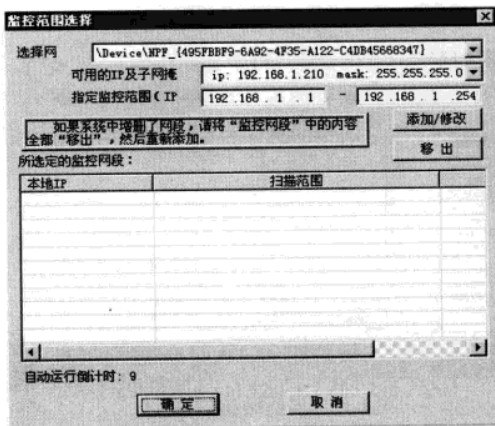


图 I-7 监控范围选择



图 I-8 执法官管理界面

STEP 8 在如图 I-9 所示的对话框中，选中第 3 个选项“禁止与所有其他主机...”，单击“开始”按钮，此时可以发现虚拟机 1 和真实机之间的 ping 测试开始提示“Request timed out”，通信

中断了。在实际环境中，还可以只选中“禁止与关键主机连接...”，然后单击“关键主机”按钮，加入网关的地址，这样被攻击计算机只会中断与网关的连接，和局域网内计算机之间的通信却不会因此而中断。

第二款软件主要用于窃取有用信息，如图 I-5 所示，在虚拟机 1 上安装“Cain & Abel”软件，破坏虚拟机 1 和真实机之间的正常通信，实验步骤如下。

STEP 1 在虚拟机 1 上安装 Cain & Abel。双击“ca_setup.exe”文件，开始安装，安装接近尾声时，会提示需要安装 WinPcap 4.0，如图 I-10 所示，单击“Install”按钮，开始安装 WinPcap 4.0。

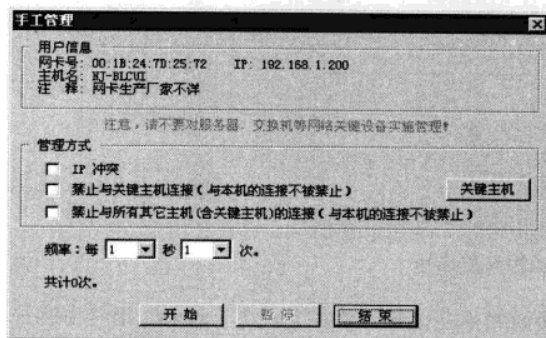


图 I-9 手工管理计算机

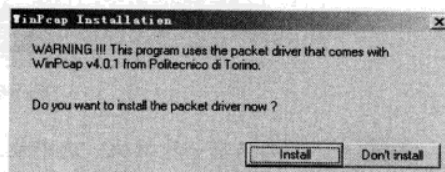


图 I-10 安装 WinPcap4.0

STEP 2 运行 Cain & Abel。双击桌面上的“Cain”图标，打开 Cain & Abel 的管理界面，单击管理界面中的“Start/Stop Sniffer”图标，如图 I-11 所示，开始抓包。

STEP 3 集线器环境下的密码获取。单击图 I-11 中上方的“Sniffer”选项卡，再单击下方的“Passwords”选项卡，开始捕获敏感的密码信息，包括邮件、Telnet、FTP 等。在虚拟机 2 上开启 Telnet 服务，在真实机上 telnet 192.168.1.210，然后输入用户和密码进行登录，如图 I-12 所示，左侧导航栏中的 Telnet 提示捕获了一条信息。

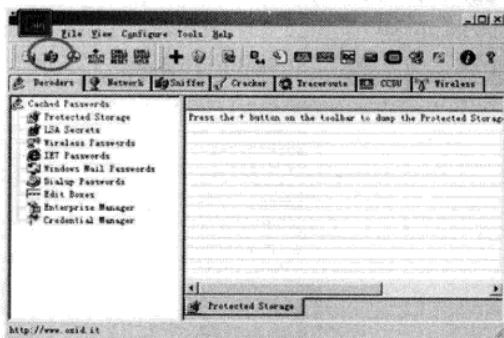


图 I-11 开始 Sniffer

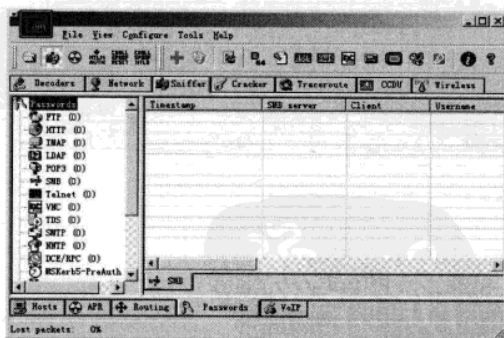


图 I-12 监听敏感信息

STEP 4 单击左侧导航栏中的“Telnet”，在右边的列表栏中，右键单击捕获的那个条目，在快捷菜单中选择“View”命令，打开如图 I-13 所示的记事本文件，从中不难看出用户名是 administrator，密码是 cisco。图中 administrator 单词中每个字母显示了两遍，这是因为有一次是 telnet 的回显。



图 I-13 捕获的密码文件

STEP 5 交换机环境下的密码获取。刚才很容易获取密码的原因是因为虚拟机 1 和虚拟机 2，以及真实机都是连接在真实机的网卡上，相当于都接在一台集线器上，在现实环境中，更常见的是交换机，交换机不会把两台主机或某台主机与网关之间的通信传给攻击者的主机。这时就需要使用 ARP 欺骗，单击如图 I-12 所示下方的“ARP”选项卡，再单击“Add to list”工具栏图标，如图 I-14 所示。

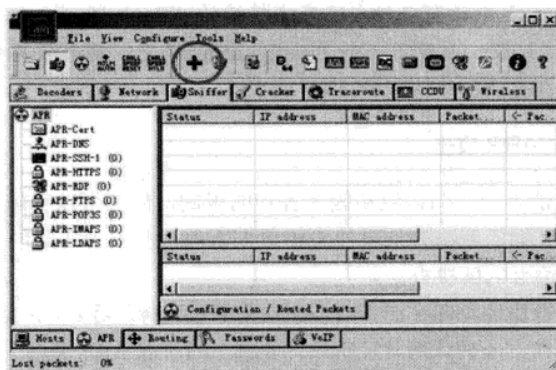


图 I-14 增加 ARP 欺骗到列表

STEP 6 打开 ARP 的条目如图 I-15 所示，在左栏选中一个 IP 地址，然后在右栏选中一个 IP 地址，这两个 IP 地址的主机将被欺骗。

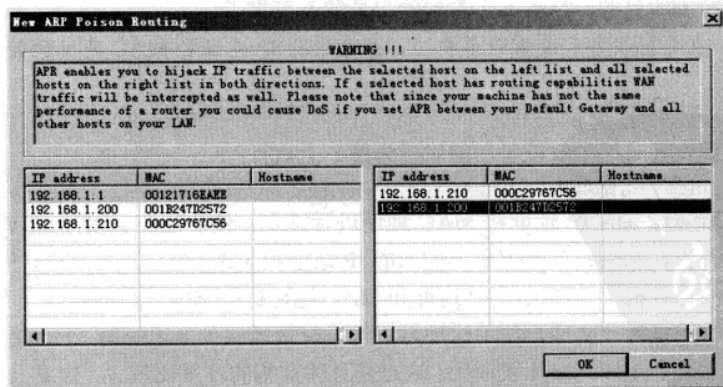


图 I-15 选择被欺骗的计算机

STEP 7 单击“OK”按钮返回,再单击图 I-11 中工具栏“Start/Stop Sniffer”图标右边的“Start/Stop ARP”图标,开始执行 ARP 欺骗,如图 I-15 所示,选择的计算机之间的通信将从虚拟机 1 中转,虚拟机 1 自然可以获取它们之间的明文敏感信息。由此看来交换机的网络也存在安全隐患。

3. 如何判断正在遭受 ARP 攻击

上面介绍的 ARP 欺骗攻击不会造成网络阻塞,但却会发生泄密,接下来介绍解决的办法。判断是否存在第一种 ARP 攻击的方法比较简单,具体步骤如下。

STEP 1 持续 ping 不能访问的 IP 地址。在出现问题计算机(虚拟机 1)的 DOS 窗口中输入“ping 192.168.1.200 -t”,用来测试网络的连通性;192.168.1.200 是不能正常通信的计算机(这里是真实机),实际工程中换成不能访问的同一网段的目标计算机的 IP 地址。如果正在遭受 ARP 攻击,屏幕将会提示“Request time out”。

STEP 2 在受害计算机(虚拟机 1)上开启另外一个 DOS 窗口,输入“arp -d”,arp 是一个 DOS 命令,能解析出 IP 地址对应的网卡 MAC 地址,-d 用来清除本机缓存的所有 IP 和 MAC 地址的对应。如果发现 Step 1 中的窗口的内容变成持续的“Reply from...”,则表示曾遭受过 ARP 攻击,现在已经正常了;如果仅出现了一个“Reply from...”包,后面又变成了“Request time out”包,则表明该计算机正在遭受持续不断的 ARP 攻击。

4. 如何防范和解决 ARP 攻击

ARP 攻击的解决办法五花八门,但却因为各种的限制,最终可以实施的非常少,甚至连一种可以实施的都找不到。下面的解决办法虽然不能包罗万象,但不管实际的网络硬件配备如何,一定可以从中找到一种最适合的解决办法。

● 方法 1: 经过判断已经发现存在 ARP 攻击,如果攻击持续存在,在受害的计算机上执行“arp -d”后,再执行“arp -a”,-a 的作用是显示该计算机上的所有 ARP 缓存。从中我们可能会发现有几条记录,其中一个记录是网关或要访问的目标主机,还有一条其他记录,也可能有几条。多执行几次“arp -d”、“arp -a”,总结一下,出现最多的那条记录基本上就是 ARP 攻击者的真实 IP 地址。

该方法的优点是比较简单,几乎适合所有的网络环境,不需要任何辅助软件,也不需要网管有非常专业的知识,即可找出攻击者,然后对攻击者进行网络隔离。缺点是如果攻击者仅仅是破坏,而不是出于控制的目的,“arp -a”看到的记录就不可靠了。

● 方法 2: 在目标设备和受害计算机上,分别进行 IP 地址和 MAC 地址的静态绑定。例如,在计算机上执行:

```
arp -s 192.168.1.1 00-aa-00-62-c6-09
```

在路由或交换设备(这里仅以思科的设备为例)上执行:

```
Cisco-6509(config)# arp 192.168.1.2 0009.6be2.3ca3 ARPA
```

把要保护的目标设备的 IP 地址和 MAC 地址进行绑定,使非法的 ARP 攻击无孔可入。并不是每一个用户都有权在网关设备上把自己使用的 IP 地址和 MAC 地址进行绑定,但用户至少可以做到的是在自己的计算机上把网关的 IP 地址和 MAC 地址进行绑定,最好做成一个批处理文件,每次计算机启动时都执行该文件,使用这种方法可以有效地避免上述的第二种泄密攻击。

该方法的优点是小规模网络比较适用。缺点是具体实施的难度比较大,如果上网主机比较多,并且主机经常变化,如高校这一群体,每年都有新报到和毕业的学生,静态绑定工作量巨大,难

以实施；太多的绑定条目会影响设备的执行速度，降低效率；即使 ARP 攻击不会影响上网，但大量的 ARP 包仍被发送，还是要占用大量的有用带宽；要求设备支持静态绑定功能。

● 方法 3：采用动态 ARP 检测技术，结合 DHCP 的功能，实现 IP 和 MAC 的自动绑定。该方法和方法 2 类似，但绑定是自动完成的，可以在接入层交换机上部署，非法的 ARP 包将被交换机丢弃，感兴趣的朋友，可查找相关设备的技术文档。

该方法的优点是解决 ARP 攻击最好的方法，不需要管理人员的协助，非法的 ARP 包也无法进入网络。既不会存在危害，也不会影响网络性能。缺点是要求管理员有较好的技术；要求网络设备的支持，思科公司支持这种功能的设备至少要 3 层以上（国内很少有企业在接入层使用 3 层设备），很多厂家的设备目前尚未支持。

● 方法 4：在网管型交换机，用 1 分钟的时间即可找出攻击者。在前面的解决方法 1 中，可以发现目标 IP 的 MAC 地址并不是真实的 MAC，记下这个 MAC 地址，假使这个 MAC 是“0050.bae3.2305”，在网管型交换机（这里仅以思科设备为例）上执行：

```
Cisco-2950#show arp | include 0050.bae3.2305
Internet 10.168.168.9      239  0050.bae3.2305  ARPA  FastEthernet1/17
```

第一行是执行的命令，单纯的“show arp”会显示出交换机学习到的所有 MAC 地址，从中找到攻击 MAC 非常困难，“| include 0050.bae3.2305”起到过滤功能，仅显示对应的行。第二行是执行结果，会发现这个 MAC 地址来自 Fa1/17 端口。找到该端口对应的主机即找到了攻击源，如果该端口接的不是一台计算机，而是另一台交换机，重复刚才的方法，直到找出最终的计算机。

该方法的优点是最具可操作性，执行比较快捷，所有的网管型交换机均支持该功能，强烈推荐。缺点是还有很多单位仍在使用非网管型交换机或集线器。

● 方法 5：在非网管型交换机或集线器的情况下，用 10 分钟的时间即可找出攻击者。在被攻击者的计算机（虚拟机 1）上打开两个 DOS 窗口，一个窗口执行“ping 192.168.1.200 -t”，另一个 DOS 窗口中间隔性执行“arp -d”，如果有多台非网管型交换机或集线器，依次切断它们的电源，何时发现第二个 DOS 窗口中出现持续的“Reply from...”，则可以断定 ARP 攻击源来自这台网络设备。接下来恢复该设备的电源，把网线一根根地拔下来，何时发现第二个 DOS 窗口中出现持续的“Reply from...”，则可以断定，该网线所接的设备就是 ARP 攻击源。如果这种查找方法慢，可以使用二分查找法，即一次拔下一半的线，测一下，一般不超过 10 分钟即可找出攻击源。

该方法的优点是几乎适合任何网络环境。缺点是执行起来有点辛苦，最好还是换成网管型的交换机吧。

● 方法 6：普通用户的自救方法。作为一名普通的网络使用者，向网管报修可能得不到及时解决，编写一个批处理文件，在计算机上执行，即可解决 ARP 的攻击问题。批处理文件的内容如下：

```
: a
Arp -d
Ping 1.1.1.1 -n 1 -w 100
Goto a
```

把该文本文件保存为 a.bat，然后在用户的计算机上双击执行，会打开一个 DOS 窗口，程序会循环执行，不要关闭该窗口即可解决 ARP 攻击问题。如果 ARP 清除方法的速度太慢，可以改变上面的 100（表示 0.1s）为想要的数值。

该方法的优点是普通用户也可以解决 ARP 攻击问题，几乎适合任何网络环境。缺点是频繁地清除 ARP 缓存，频繁地发送 ARP 广播包，会给本地计算机和网络带来额外负担。