

# 2006

盘点2006年度18大热门局域网应用专题  
汇总2006年度36组主流局域网热点快报  
聚焦2006年度1000余条最新局域网操作技巧

# 网管员特训

智联教育 覃明揆 编著

## 18大应用专题

全面认识局域网、局域网设备的选购与连接、典型局域网组建方案、安装局域网服务器、Internet连接与共享、家庭局域网/学生宿舍网/企业局域网/无盘局域网/无线局域网/虚拟专用网络的组建与应用、局域网服务器的组建与应用、局域网热点应用、局域网的管理/升级与安全设置

## 36组热点快报

局域网设备的选购、大型局域网组建方案简介、安装Windows服务器的活动目录、SyGate共享服务器的搭建与管理、Windows XP对等网的组建与ADSL共享上网、企业局域网的软件分发、无线局域网的安全设置、VPN服务的组建与应用、升级网络设备

## 1000余条操作技巧

双绞线跳线的制作与测试、三机四网卡互连组建局域网、宿舍网的一线多机上网、员工私有与公用空间的分配、流媒体服务器的组建与应用、对等网上视频广播、远程登录服务器、自动升级客户端

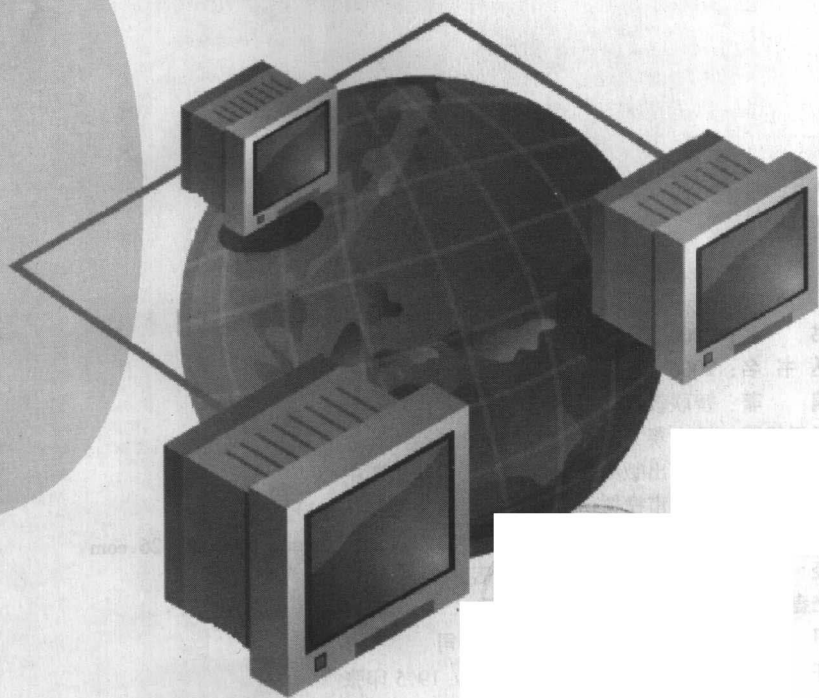
光盘内容

- 14大专题、27个局域网组建与应用 视频教学
- 65款局域网应用、管理、病毒专杀等工具软件大集合



# 2006 网管员特训

智联教育 覃明揆 编著



四川出版集团  
四川电子音像出版中心 • 出版

# 内 容 提 要

本书非常全面、系统、精辟地讲解了局域网的认识、规划、组建、应用、升级、管理、维护、故障排除等网管员入门、提高与特训的方方面面和操作技巧,内容详实、操作简单、知识点多。

本书内容主要包括:网管员认识与必备技能,全面认识局域网,局域网设备的选购与连接,典型局域网组建方案,安装 Windows 局域网服务器,局域网接入 Internet 与共享,家庭局域网、学生宿舍网、企业局域网、无盘局域网、无线局域网、虚拟专用网络等典型局域网的组建与应用,文件、打印、Web、FTP、E-mail、视频会议、视频点播与流媒体等局域网服务器的组建与应用,局域网热点应用方案设计与解决,局域网设备的管理,局域网服务器的远程管理,局域网的硬件与系统升级,局域网安全设置与局域网常见故障与排除方法等。你既可以循序地学习,也可以随查随用,使你学有所依、用有所循,快速步入局域网的神秘大门,得心应手地解决各类实际应用问题。

本书内容覆盖全面,知识点丰富,图解叙述,通俗易懂,实用性很强,是广大电脑初级、中级用户和家庭用户的首选案头手册,适合初、中级电脑用户以及广大的电脑爱好者阅读与收藏。

## 光盘内容:

1. 14 大专题、27 个局域网组建与应用 视频教学
2. 65 款局域网应用、管理、病毒专杀等工具软件大集合
3. 《局域网组建与维护教程》、《网络综合应用教程》两本 PDF 电子书

书 名: 2006 网管员特训

丛 书 名: 2006

编 著: 智联教育 覃明撰

责任编辑: 马 黎 许 明

出版发行: 四川出版集团 四川电子音像出版中心

地 址: 成都市槐树街 2 号四川出版大厦(610031)

营销部电话/传真: (028)8259443 E-mail: scdzyx@126.com

经 销: 全国新华书、软件连锁店

光盘制作: 东方光盘制造有限公司

印 刷: 重庆升光电力印务有限公司

开 本: 787mm×1092mm 16 开 19.5 印张

版 次: 2006 年 2 月第 1 版 2006 年 2 月第 1 次印刷

印 数: 1-5000 册

版 本 号: ISBN 7-900397-98-1/TP·90

定 价: 25.00 元(1CD+配套书)



# [前言]

3 年品牌、6 次再版

丛书畅销 100 多万册

电脑用户首选 DIY 品牌图书

本书非常全面、系统、精辟地讲解了局域网的认识、规划、组建、应用、升级、管理、维护、故障与排除等网管员入门、提高与特训的方方面面和操作技巧，内容详实、操作简单、知识点多。

本书内容主要包括：网管员认识与必备技能，全面认识局域网，局域网设备的选购、连接与测试，小型、中型与大型等典型局域网的组建方案规划与设计，安装 Windows 局域网服务器，局域网连接 Internet 与共享，家庭局域网、学生宿舍网、企业局域网、无盘局域网、无线局域网、虚拟专用网络等典型局域网的组建与应用，文件、打印、Web、FTP、E-mail、视频会议、视频点播与流媒体等局域网服务器的组建与应用，局域网热点应用方案设计与解决，局域网设备的管理，局域网服务器的远程管理，局域网的硬件与系统升级，局域网安全设置与局域网常见故障与排除方法等。你既可以循序地学习，也可以随查随用，使你学有所依、用有所循，快速步入电脑硬件的神秘大门，得心应手地解决各类实际应用问题。

《2006 网管员特训》每一个专辑都是经过编辑们精心提炼的热点问题；每一组快报都可以从头到尾帮你完成一项完整的应用任务；每一条技巧会让你有茅塞顿开的感觉。全书方案详尽、实用性强、汇集各种网管员入门、提高与特训的应用精萃。

本书内容覆盖全面，知识点丰富，图解叙述，通俗易懂，实用性很强，是广大电脑初级、中级用户和家庭用户的首选案头手册，适合初、中级电脑用户以及广大的电脑爱好者阅读与收藏。

本书由“智联教育”组织编著，参与策划、编辑、写作、排版的人员有：覃明揆、叶俊、赵乾伟、甘立富、何勇、尹小港、徐春红、曾全、许明等。由于编者经验有限，加之时间仓促，书中难免会有疏漏和不足之处，恳请专家和读者不吝赐教。

读者在使用本书过程中如有其他问题、意见或建议，可以通过下面方式和我们联系：

Http://www.ChinaMook.com

E-mail: mook@vip.sina.com

QQ: 35691532

**智联教育**  
www.ChinaMook.com

# 目 录

## 第 1 章 网管员第一课——全面认识

### 局域网

|                              |    |
|------------------------------|----|
| 1.1 认识局域网                    | 1  |
| 1.1.1 局域网的特征                 | 1  |
| 1.1.2 局域网的种类                 | 1  |
| 1.1.3 局域网的应用                 | 2  |
| 1.2 局域网的组成                   | 3  |
| 1.2.1 硬件设备                   | 3  |
| 1.2.2 局域网操作系统                | 5  |
| 1.2.3 服务器                    | 5  |
| 1.2.4 网络防火墙                  | 7  |
| 1.2.5 UPS 不间断电源              | 8  |
| 1.3 局域网的拓扑结构                 | 8  |
| 1.3.1 总线型拓扑结构                | 9  |
| 1.3.2 星型拓扑结构                 | 9  |
| 1.3.3 环型拓扑结构                 | 10 |
| 1.3.4 其他拓扑结构                 | 10 |
| 1.4 局域网的通信协议                 | 11 |
| 1.4.1 通信协议的功能                | 11 |
| 1.4.2 TCP/IP 协议              | 11 |
| 1.4.3 NetBEUI 协议和 IPX/SPX 协议 | 11 |
| 1.4.4 IPv4 协议和 IPv6 协议       | 12 |
| 1.4.5 局域网通信协议的选择原则           | 14 |
| 1.5 局域网 IP 地址与分配方式           | 14 |
| 1.5.1 合法 IP 地址与保留 IP 地址      | 14 |
| 1.5.2 IP 地址信息                | 16 |
| 1.5.3 IP 地址段的选择              | 17 |
| 1.5.4 IP 地址的分配方式             | 18 |

## 第 2 章 网管员采购——局域网设备的

### 选购与连接

|              |    |
|--------------|----|
| 2.1 局域网设备的选购 | 19 |
| 2.1.1 网卡的选购  | 19 |
| 2.1.2 双绞线的选购 | 20 |

|                             |    |
|-----------------------------|----|
| 2.1.3 同轴电缆的选购               | 21 |
| 2.1.4 光纤的选购                 | 22 |
| 2.1.5 集线器的选购                | 23 |
| 2.1.6 交换机的选购                | 24 |
| 2.1.7 路由器的选购                | 26 |
| 2.1.8 硬件防火墙的选购              | 27 |
| 2.1.9 UPS 的选购               | 28 |
| 2.2 双绞线跳线的制作与测试             | 30 |
| 2.2.1 跳线制作工具                | 30 |
| 2.2.2 跳线制作所需材料              | 30 |
| 2.2.3 制作标准与跳线类型             | 31 |
| 2.2.4 双绞线跳线的制作              | 32 |
| 2.2.5 双绞线的测试                | 34 |
| 2.3 局域网的连接                  | 34 |
| 2.3.1 双机直连                  | 35 |
| 2.3.2 集线设备之间的连接策略           | 35 |
| 2.3.3 交换机之间的连接              | 36 |
| 2.3.4 集线器的连接                | 38 |
| 2.3.5 电脑与集线器的连接             | 38 |
| 2.3.6 路由器的连接                | 39 |
| 2.4 局域网连接成功的判断与测试           | 40 |
| 2.4.1 利用网卡和网络设备指示灯判断        | 40 |
| 2.4.2 利用 Ping、Tracert 等命令测试 | 41 |
| 2.4.3 利用专业设备测试              | 43 |

## 第 3 章 网管员规划——典型局域网

### 组建方案

|                      |    |
|----------------------|----|
| 3.1 小型局域网组建方案简介      | 44 |
| 3.1.1 组建廉价、低速的总线型以太网 | 44 |
| 3.1.2 组建廉价、低速的星型以太网  | 45 |
| 3.1.3 组建快速星型以太网      | 45 |
| 3.2 中型局域网组建方案简介      | 46 |
| 3.2.1 组建集中式中型企业局域网   | 46 |
| 3.2.2 组建分布式中型企业局域网   | 46 |
| 3.2.3 组建可靠式中型企业局域网   | 47 |
| 3.3 大型局域网组建方案简介      | 47 |



|                  |    |
|------------------|----|
| 3.3.1 组建校园网      | 47 |
| 3.3.2 组建医院网      | 48 |
| 3.3.3 组建数码化社区局域网 | 49 |

## 第4章 安装局域网服务器

|                               |    |
|-------------------------------|----|
| 4.1 安装 Windows 服务器的活动目录       | 50 |
| 4.1.1 安装活动目录前的准备              | 50 |
| 4.1.2 安装 Win 2000 Server 活动目录 | 51 |
| 4.1.3 安装 Win Server 2003 活动目录 | 51 |
| 4.2 安装 SCSI 和 RAID 卡          | 54 |
| 4.3 添加用户与用户组                  | 55 |
| 4.3.1 添加与修改用户                 | 55 |
| 4.3.2 添加与修改计算机                | 56 |
| 4.3.3 添加用户组                   | 57 |

## 第5章 Internet 连接与共享

|                        |    |
|------------------------|----|
| 5.1 Internet 接入方式与特点   | 59 |
| 5.1.1 ADSL             | 59 |
| 5.1.2 Cable Modem      | 59 |
| 5.1.3 FTTX+LAN         | 60 |
| 5.2 Internet 连接与共享     | 60 |
| 5.2.1 路由器方案            | 60 |
| 5.2.2 代理服务器方案          | 62 |
| 5.3 SyGate 共享服务器的搭建与管理 | 64 |
| 5.3.1 安装与设置 Sygate     | 65 |
| 5.3.2 Internet 访问限制    | 67 |
| 5.3.3 发布 Internet 服务器  | 68 |
| 5.3.4 设置客户端            | 68 |

## 第6章 家庭局域网的组建与应用

|                        |    |
|------------------------|----|
| 6.1 组建家庭局域网准备工作        | 69 |
| 6.1.1 家庭局域网的硬件准备       | 69 |
| 6.1.2 家庭局域网的布线规划       | 69 |
| 6.2 双机双网卡直连组建 局域网      | 70 |
| 6.2.1 最值得推荐的特殊连接法      | 70 |
| 6.2.2 直接电缆连接           | 72 |
| 6.2.3 双机 USB—Link 电缆连接 | 73 |
| 6.3 三机双网卡互连组建局域网       | 74 |
| 6.3.1 用双网卡实现三机互联       | 74 |
| 6.3.2 三机互联新招           | 75 |
| 6.3.3 IEEE 1394 连接上网   | 75 |

|                       |    |
|-----------------------|----|
| 6.4 三机四网卡互连组建局域网      | 76 |
| 6.4.1 路由的作用及所需的硬件设备   | 76 |
| 6.4.2 安装网卡            | 76 |
| 6.4.3 安装网络协议并指定 IP 地址 | 77 |
| 6.4.4 设置路由和远程访问       | 78 |
| 6.4.5 指定客户机的 IP 地址    | 79 |
| 6.4.6 测试网络连接          | 79 |

|                            |    |
|----------------------------|----|
| 6.5 Windows 98 对等网的组建与共享上网 | 79 |
| 6.5.1 硬件准备                 | 79 |
| 6.5.2 软件准备                 | 79 |
| 6.5.3 组建实战                 | 79 |
| 6.5.4 共享上网的实现              | 80 |

|                                  |    |
|----------------------------------|----|
| 6.6 Windows 2000 对等网的组建与共享上网     | 82 |
| 6.6.1 硬件安装                       | 82 |
| 6.6.2 安装网卡驱动                     | 82 |
| 6.6.3 组建实战                       | 83 |
| 6.6.4 共享上网                       | 84 |
| 6.6.5 Win 2000 与 Win 98 共享 IE 资源 | 86 |

|                                  |    |
|----------------------------------|----|
| 6.7 Windows XP 对等网的组建与 ADSL 共享上网 | 87 |
| 6.7.1 Windows XP 下的 ADSL 设置      | 87 |
| 6.7.2 Windows XP 局域网组建及共享        | 88 |
| 6.7.3 用网桥在 Windows XP 下实现共享上网    | 91 |

## 第7章 学生宿舍网的组建与应用

|                         |    |
|-------------------------|----|
| 7.1 宿舍网的组建规划            | 92 |
| 7.1.1 网络拓扑结构            | 92 |
| 7.1.2 网络通讯协议            | 93 |
| 7.1.3 网络规划              | 93 |
| 7.1.4 网络硬件设备            | 94 |
| 7.2 宿舍网的硬件准备和成本计算       | 94 |
| 7.2.1 经济型宿舍网组建方案        | 94 |
| 7.2.2 实用型宿舍网组建方案        | 94 |
| 7.2.3 高性能宿舍网组建方案        | 95 |
| 7.3 组建宿舍网               | 95 |
| 7.3.1 准备工作              | 95 |
| 7.3.2 安装步骤              | 95 |
| 7.3.3 宿舍之间多个局域网互联       | 97 |
| 7.3.4 宿舍网接入校园网          | 98 |
| 7.4 宿舍网的一线多机上网          | 99 |
| 7.4.1 在 Win 98 下设置代理服务器 | 99 |



|                           |     |
|---------------------------|-----|
| 7.4.2 在 Win 2000 下配置代理服务器 | 102 |
| 7.4.3 ADSL 宽带路由器的安装及调试    | 103 |

## 第 8 章 企业局域网的组建与应用

|                                     |     |
|-------------------------------------|-----|
| 8.1 企业局域网的组建规划                      | 105 |
| 8.1.1 企业网站的优势                       | 105 |
| 8.1.2 明确建站目的                        | 105 |
| 8.1.3 申请网站域名                        | 106 |
| 8.1.4 准备网站存放空间                      | 106 |
| 8.1.5 网站内容设计与制作                     | 107 |
| 8.2 组建企业局域网                         | 107 |
| 8.2.1 硬件准备与组网方案                     | 107 |
| 8.2.2 组建 Windows Server 2003 域模式局域网 | 109 |
| 8.3 员工私有与公用空间的分配                    | 117 |
| 8.3.1 设置分区格式                        | 117 |
| 8.3.2 分配私有空间                        | 117 |
| 8.3.3 分配公用空间                        | 119 |
| 8.4 企业局域网的共享应用                      | 119 |
| 8.4.1 文件共享                          | 119 |
| 8.4.2 打印机共享                         | 121 |
| 8.4.3 使用 DFS 集中共享企业资源               | 123 |
| 8.5 企业局域网的软件分发                      | 125 |
| 8.5.1 设置共享目录                        | 125 |
| 8.5.2 设置组策略                         | 127 |
| 8.5.3 在工作站中安装软件                     | 128 |

## 第 9 章 无盘局域网的组建与应用

|                                |     |
|--------------------------------|-----|
| 9.1 无盘网络技术与应用                  | 129 |
| 9.2 基于 Win Server 2003 组建无盘局域网 | 129 |
| 9.2.1 实现目标                     | 130 |
| 9.2.2 准备工作                     | 130 |
| 9.2.3 设置服务端网络                  | 130 |
| 9.2.4 添加网络协议                   | 130 |
| 9.2.5 指定静态 IP 地址               | 131 |
| 9.2.6 安装设置 DHCP 服务             | 132 |
| 9.2.7 安装设置终端服务                 | 134 |
| 9.2.8 安装设置 Intel PXE-PDK 2.0   | 136 |
| 9.3 基于 DOSRDP XP 实现无盘终端        | 137 |
| 9.3.1 实现软盘终端远程登录               | 137 |
| 9.3.2 实现无盘终端远程登录               | 139 |

## 第 10 章 无线局域网的组建与应用

|                                       |     |
|---------------------------------------|-----|
| 10.1 无线局域网概述                          | 140 |
| 10.1.1 无线局域网的应用                       | 140 |
| 10.1.2 无线局域网的组成                       | 140 |
| 10.1.3 无线局域网的 4 种接入方式                 | 142 |
| 10.1.4 IEEE 802.11 与 802.16a          | 143 |
| 10.1.5 Wi-Fi 与 WiMAX                  | 144 |
| 10.2 无线局域网的组建                         | 144 |
| 10.2.1 无线设备的选购                        | 144 |
| 10.2.2 安装无线网卡                         | 145 |
| 10.2.3 安装无线网卡驱动程序                     | 145 |
| 10.2.4 无线 AP 的物理连接                    | 150 |
| 10.3 对等局域网的配置                         | 151 |
| 10.3.1 AVAYA 对等局域网的配置                 | 151 |
| 10.3.2 D-link 对等局域网的配置                | 154 |
| 10.4 接入点局域网的配置                        | 155 |
| 10.4.1 配置 AVAYA 接入点局域网                | 155 |
| 10.4.2 D-Link 接入点局域网的配置               | 158 |
| 10.5 无线漫游局域网的配置                       | 160 |
| 10.5.1 AVAYA 无线漫游局域网                  | 160 |
| 10.5.2 D-Link 无线漫游局域网                 | 161 |
| 10.5.3 客户端的设置                         | 161 |
| 10.6 无线局域网的 Internet 连接与共享            | 161 |
| 10.6.1 利用代理服务器实现 Internet 连接共享        | 161 |
| 10.6.2 利用 AVAYA 无线网关实现 Internet 连接共享  | 162 |
| 10.6.3 利用 D-Link 无线网关实现 Internet 连接共享 | 163 |
| 10.7 无线局域网的安全设置                       | 165 |
| 10.7.1 加密传输                           | 165 |
| 10.7.2 MAC 地址过滤                       | 165 |
| 10.7.3 身份认证                           | 166 |

## 第 11 章 虚拟专用网络的组建与应用

|                               |     |
|-------------------------------|-----|
| 11.1 VPN 服务的组建与应用             | 167 |
| 11.1.1 VPN 服务器的安装             | 167 |
| 11.1.2 VPN 服务器的应用             | 170 |
| 11.2 虚拟专用网络的连接                | 170 |
| 11.2.1 Win Server 2003 客户机的设置 | 170 |
| 11.2.2 Win 2000/XP 客户机的设置     | 172 |



|                             |     |
|-----------------------------|-----|
| 11.2.3 Windows 98/Me 客户机的设置 | 173 |
|-----------------------------|-----|

## 第 12 章 局域网服务器的组建与应用

|                                      |     |
|--------------------------------------|-----|
| 12.1 文件服务器的组建与应用                     | 175 |
| 12.1.1 安装 Win Server 2003 文件服务       | 175 |
| 12.1.2 RAID 的创建与实现                   | 177 |
| 12.1.3 共享文件夹的创建与访问                   | 180 |
| 12.2 打印服务器的组建与应用                     | 183 |
| 12.2.1 安装和设置共享打印机                    | 184 |
| 12.2.2 网络打印机的设置                      | 187 |
| 12.2.3 设置访问权限                        | 188 |
| 12.2.4 设置优先级和打印队列                    | 189 |
| 12.3 Web 服务器的组建与应用                   | 190 |
| 12.3.1 安装 Web 服务                     | 190 |
| 12.3.2 Web 服务的配置                     | 191 |
| 12.3.3 设置 IP 地址和端口                   | 191 |
| 12.3.4 设置默认文档                        | 192 |
| 12.3.5 设置主目录                         | 192 |
| 12.3.6 创建虚拟目录                        | 193 |
| 12.4 FTP 服务器的组建与应用                   | 194 |
| 12.4.1 安装 FTP 服务                     | 194 |
| 12.4.2 FTP 站点的配置                     | 195 |
| 12.4.3 修改站点标识和 IP 地址                 | 195 |
| 12.4.4 设置主目录                         | 196 |
| 12.4.5 设置安全访问                        | 196 |
| 12.4.6 连接数量限制                        | 197 |
| 12.4.7 创建虚拟 FTP 站点                   | 197 |
| 12.4.8 创建虚拟目录                        | 199 |
| 12.4.9 FTP 站点的访问                     | 201 |
| 12.5 E-mail 服务器的组建与应用                | 203 |
| 12.5.1 安装 Windows Server 2003 电子邮件服务 | 203 |
| 12.5.2 设置身份验证方法                      | 204 |
| 12.5.3 设置邮件存储位置                      | 205 |
| 12.5.4 创建和管理域                        | 205 |
| 12.5.5 创建和管理邮箱                       | 206 |
| 12.6 视频会议服务器的组建与应用                   | 208 |
| 12.6.1 搭建视频服务器                       | 208 |
| 12.6.2 视频会议客户端的配置                    | 211 |
| 12.6.3 视频会议的实现                       | 213 |
| 12.7 流媒体服务器的组建与应用                    | 216 |
| 12.7.1 安装 Windows Media 服务           | 216 |

|                     |     |
|---------------------|-----|
| 12.7.2 制作流媒体文件      | 216 |
| 12.7.3 实现流式视频和音频的点播 | 220 |

## 第 13 章 局域网热点应用

|                           |     |
|---------------------------|-----|
| 13.1 共享文件                 | 229 |
| 13.1.1 同机用户间的共享           | 229 |
| 13.1.2 局域网共享的实现           | 230 |
| 13.2 映射网络驱动器              | 230 |
| 13.3 共享打印机                | 231 |
| 13.3.1 安装网络打印机            | 231 |
| 13.3.2 共享打印机的管理和维护        | 235 |
| 13.3.3 打印机访问的设置           | 237 |
| 13.4 共享刻录机                | 238 |
| 13.4.1 服务器端设置             | 239 |
| 13.4.2 客户端设置              | 239 |
| 13.4.3 刻录                 | 239 |
| 13.5 共享传真                 | 239 |
| 13.5.1 搭建传真服务器            | 240 |
| 13.5.2 设置客户端              | 240 |
| 13.5.3 网内共享传真服务           | 240 |
| 13.6 局域网热点应用实例            | 241 |
| 13.6.1 WinPopup 局域网聊天     | 241 |
| 13.6.2 Netsend 局域网聊天      | 241 |
| 13.6.3 NetMeeting 局域网视频会议 | 242 |
| 13.6.4 对等网上 E-mail 的实现    | 246 |
| 13.6.5 对等网上视频广播           | 247 |

## 第 14 章 远程管理服务器

|                             |     |
|-----------------------------|-----|
| 14.1 远程登录服务器                | 248 |
| 14.1.1 设置 pcAnywhere        | 248 |
| 14.1.2 利用 pcAnywhere 实现远程管理 | 252 |
| 14.2 远程监测服务器                | 253 |
| 14.2.1 设置 Service Monitor   | 253 |
| 14.2.2 使用 MRTG 实时流量监测       | 255 |

## 第 15 章 局域网设备的管理

|                 |     |
|-----------------|-----|
| 15.1 交换机与路由器的管理 | 257 |
| 15.1.1 配置端口与连接  | 257 |
| 15.1.2 CLI      | 261 |
| 15.2 UPS 的管理    | 263 |





|                            |     |
|----------------------------|-----|
| 15.2.1 通过串口管理 UPS .....    | 263 |
| 15.2.2 通过网络管理 UPS .....    | 264 |
| 15.2.3 UPS 与电池的使用与保养 ..... | 265 |

## 第 16 章 局域网的系统升级

|                            |     |
|----------------------------|-----|
| 16.1 自动升级服务的意义与应用 .....    | 268 |
| 16.2 安装自动升级服务器 .....       | 269 |
| 16.2.1 安装 IIS 服务 .....     | 269 |
| 16.2.2 安装自动升级服务器端 .....    | 270 |
| 16.2.3 配置自动升级服务器 .....     | 271 |
| 16.3 自动升级客户端 .....         | 272 |
| 16.3.1 安装 SUS 系统客户端 .....  | 272 |
| 16.3.2 设置自动更新 .....        | 272 |
| 16.3.3 设置利用组策略实现自动升级 ..... | 273 |

## 第 17 章 局域网的硬件升级

|                            |     |
|----------------------------|-----|
| 17.1 升级网络服务器的硬件配置 .....    | 275 |
| 17.1.1 升级网络服务器硬件 .....     | 275 |
| 17.1.2 升级处理性能 .....        | 275 |
| 17.1.3 升级 I/O 性能 .....     | 277 |
| 17.1.4 升级网络性能 .....        | 278 |
| 17.1.5 实现网络服务分担和群集 .....   | 279 |
| 17.2 升级网络设备 .....          | 279 |
| 17.2.1 升级网络设备选型原则 .....    | 279 |
| 17.2.2 升级中心交换机 .....       | 280 |
| 17.2.3 由百兆升级至千兆网络 .....    | 282 |
| 17.2.4 千兆标准与传输介质 .....     | 282 |
| 17.2.5 升级网络骨干 .....        | 282 |
| 17.2.6 升级网络服务器 .....       | 283 |
| 17.2.7 升级网络边缘 .....        | 283 |
| 17.2.8 升级千兆时应当注意的问题 .....  | 283 |
| 17.2.9 傻瓜交换机升级为智能交换机 ..... | 283 |
| 17.2.10 由集线器升级为交换机 .....   | 284 |

## 第 18 章 局域网安全设置

|                          |     |
|--------------------------|-----|
| 18.1 认识电脑病毒 .....        | 285 |
| 18.2 认识黑客 .....          | 285 |
| 18.3 常规局域网安全设置 .....     | 286 |
| 18.3.1 删除不需要的协议 .....    | 286 |
| 18.3.2 禁用 NETBIOS .....  | 286 |
| 18.3.3 禁用文件和打印共享服务 ..... | 286 |

|                                              |     |
|----------------------------------------------|-----|
| 18.3.4 启用 TCP/IP 筛选 .....                    | 287 |
| 18.3.5 禁用不必要的服务 .....                        | 287 |
| 18.3.6 系统更新与打补丁 .....                        | 288 |
| 18.4 Symantec AntiVirus 查杀病毒 .....           | 290 |
| 18.4.1 Symantec AntiVirus 安装顺序 .....         | 290 |
| 18.4.2 安装 Symantec 系统中心 .....                | 290 |
| 18.4.3 安装 Symantec Anti Virus<br>服务器程序 ..... | 293 |
| 18.4.4 升级病毒库和引擎 .....                        | 294 |
| 18.4.5 配置自动防护 .....                          | 296 |
| 18.4.6 安装 Symantec AntiVirus<br>客户端程序 .....  | 298 |
| 18.5 防火墙防御黑客攻击 .....                         | 301 |
| 18.5.1 防火墙常识 .....                           | 301 |
| 18.5.2 木马克星实现客户端安全上网 .....                   | 301 |

## 网管员第一课——全面认识局域网

知己知彼方能百战不殆，要成为一名合格的网络管理员，必须对局域网的相关知识有着全面、深刻的了解，比如局域网的特点、应用、组建、维护等，并能够把握网络发展方向，及时对所管理的网络进行升级。

本章中将介绍局域网的概念、组成、结构和协议等关键要素，并讲解了 IP 地址的概念与分配方式。

### 精彩看点

- 认识局域网
- 局域网的拓扑结构
- 局域网 IP 地址与分配方式

## 1.1 认识局域网

局域网的出现，使网络的功能获得更充分地发挥，在很短的时间内电脑网络就深入到各个领域。因此，局域网技术是目前非常活跃的技术领域，各种类型的局域网层出不穷，并得到广泛应用，极大地推进了信息化社会的发展。

尽管局域网是最简单的网络，但这并不意味着它们必定是小型的或简单的。局域网可以变得相当大、复杂，配有成百上千用户的局域网是很常见的事。

### 1.1.1 局域网的特征

局部区域网络 (Local Area Network) 通常简称为“局域网”，缩写为 LAN。局域网是结构复杂程度最低的电脑网络。局域网仅是在同一地点上经网络连在一起的一组电脑，局域网中的电脑通常相互之间很接近，它是目前应用最广泛的一类网络。

通常将具有如下特征的网络称为局域网：

- 局域网的组成
- 局域网的通信协议

- 网络覆盖的地理范围较小，通常不超过几十公里，甚至只在一幢建筑或房间内。
- 信息的传输速率比较高，其范围自 10Mbps 到 100Mbps，目前某些局域网已经达到 1000Mbps。

### 1.1.2 局域网的种类

架设局域网的方法很多，常见的有以下几种：

- 对等网
- 客户机/服务器网
- 无盘工作站网
- 无线局域网
- 虚拟专用网

#### 1. 对等局域网

对等网中的每一台设备可以同时是客户机和服务器。网络中的所有设备可直接访问数据、软件和其他网络资源。换言之，每一台网络电脑与其他连网的电脑是对等的，它们没有层次的划分。

对等网主要针对家庭、宿舍或者一些小型企业，



因为它不需要服务器，所以成本较低，但它只是局域网中最基本的一种，许多管理功能无法实现。

## 2. 客户机/服务器局域网

客户机/服务器 (Computer/Server) 网络又叫服务器网络，在客户机/服务器网络中，不同作用的电脑被划分为服务器和客户机。基于服务器的网络引进了层次结构，它是为了适应网络规模，增大所需的各种支持功能而专门设计的。通常将基于服务器的网络都称为客户机/服务器网络。

客户机/服务器网络应用于大中型企业，可以实现数据共享，对财务、人事等工作进行网络化管理，还可以召开网络会议，并且提供了强大的 Internet/Intranet Web 信息服务，其中包括 FTP、GOPHER、WWW 等功能，几乎是一种近乎完美的局域网构架方案。

## 3. 无盘工作站局域网

无盘工作站顾名思义就是没有硬盘、软驱，是基于服务器网络的一种结构，无盘工作站利用网卡上的启动芯片与服务器连接，使用服务器的硬盘空间进行资源共享。

“无盘工作站网络”可以实现“客户机/服务器网络”的所有功能，在它的工作站上，没有磁盘驱动器，但因为每台工作站都需要从“远程服务器”启动，所以对服务器、工作站以及网络组建的要求较高，因而成本并不比“客户机/服务器网络”成本低，但它的稳定性，安全性一直为大众所看好，特别是被一些安全系数要求较高的企业所喜爱。

## 4. 无线局域网

WLAN (Wireless Local Area Networks, 无线局域网) 是相当便利的数据传输系统，它是利用射频 (Radio Frequency, RF) 技术，取代旧式双绞铜线所构成的有线局域网，使得网络布线变的简单。

无线局域网绝不是用来取代有线局域网，而是用来弥补有线局域网之不足，以达到网络延伸的目的，下列情形可能须用无线局域网：

- 无固定工作场所的使用者
- 有线局域网架设受环境所限制
- 作为有线局域网的备用系统

## 5. 虚拟专用网络

VPN (Virtual Private Network, 虚拟专用网络)，它通过一个公用网络 (通常为 Internet) 建立一个安全的私有连接，是一条穿过不安全的公用网络的安

全、稳定的通道。

虚拟专用网提供了一个通过不安全的公用网络安全地对企业内部专用网络进行远程访问的连接方式，虚拟专用网是对企业内部网的扩展，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。在该网中的主机将不会觉察到公共网络的存在，仿佛所有的主机都处于一个内部网络中一样。

## 1.1.3 局域网的应用

使用局域网可以快速实现多台电脑之间的文件传输、磁盘共享、打印共享、协同工作、联机游戏等功能，从而将极大提高工作效率、减少设备资金投入。

### 1. 文件传输

有了局域网，传输文件就会截然不同，不再需要软盘、U 盘和刻录机，也不再需要压缩和拆分，几十兆甚至上百兆的文件，都能在极短的时间内传输完毕。

### 2. 文件共享

如果电脑没有联网，怎么让大家共享文档和文件？或者打印成文本，或者用磁盘拷贝。而在网络环境下，无论是谁，只要授予其查看或修改的权限，他就能在自己电脑运行、浏览和修改甚至删除这些文件。

### 3. 程序共享

现在，许多应用程序都提供了网络版本或提供了异地运行方式，这在由多人共同维护某一记录或文件时显得尤为重要。另外，既然应用程序可以在其它的电脑上运行，那么本地硬盘完全不必再安装，这对于节约本地有限的磁盘空间非常有益。

### 4. 资源共享

网络中，每一台电脑中的软盘、硬盘、CD-ROM、CD-R/W 和 DVD-ROM 等存储设备，以及这些存储设备中的文件都能够被用来共享。不仅可以从其他电脑的光盘、硬盘中读取文件，甚至还可以向其他电脑的磁盘中写入文件。

当然，在网络中，能够访问哪些资源、能够读写哪些文件必须有相应权限，否则将被拒绝访问 (即读和写)。

权限保证了网络资源的不被滥用，也保证了文件本身的安全。

## 5. 打印共享

在网络中,无论打印机连接在哪台电脑上,都可以在自己的电脑上进行网络打印。网络打印使得相关人员对打印的管理更加方便,只有拥有打印权的用户才能使用打印机,而那些未被授予打印权限的用户则将被打印服务器拒绝。

## 6. 传真共享

同打印共享一样,传真共享也可以使局域网内的任意一台电脑具备传真收发功能。服务器端能在后台自动完成传真收发任务,客户端不用安装任何插件就可以通过 IE 浏览器完成传真发送、接收、浏览、打印和转发 E-mail 的操作。

## 7. Internet 共享

Internet 共享接入的原理非常简单,将网络中的一台电脑作为代理服务器,使其通过 Modem 接入 Internet,网络中的其他电脑则通过该电脑,使用同一个 Internet 连接。

## 8. FTP 服务器

FTP 服务是 Internet 服务的又一重要组成部分,用于在 FTP 服务器和 FTP 客户端之间完成文件的传输,该传输过程是双向的,既可以从服务器下载到客户端,也可以从客户端上传到服务器。无论是提供软件的下载,还是实现 Web 站点的维护,都离不开借助于 FTP 服务。

## 9. E-mail 服务器

在局域网中可以建立属于该网络中的 E-Mail 服务器,发送邮件、转发文件、联系好友、随意设置邮箱的容量等设置,甚至还可以多设置几个账户,让你的同事也来分享。

通常 E-Mail 服务器系统由 POP3 服务、简单邮件传输协议 (SMTP) 服务以及电子邮件客户端三个组件组成。POP3 服务与 SMTP 服务一起使用,POP3 为用户提供邮件下载服务,SMTP 则用于发送邮件和邮件在服务器间的传递,电子邮件客户端则用于读取、撰写以及管理电子邮件。

## 10. 协同工作

协同工作,举个例子来说,就是比如网络中的一组编辑者共同评阅某个文档。所有指定的人员都能访问、编辑或发送共享的文档,并且可以规定每个人对文档的编辑权限或选项。

在网络中,可以选择如何向评阅者分发文档,并可确定评阅者同时评阅或依特定顺序依次评阅。网络中安装集成化应用程序(如 Microsoft Exchange 或 Lotus Notes)后,可以通过电子邮件系统将该文档作为附件寄给不同的评阅者,甚至可以通过 Internet 进行发布。对于某些有赖于多个部门共同完成或维护的文档,协同工作不仅能够极大地提高工作效率,而且也有利于文档的及时更新。

## 11. 联机游戏

一个人玩游戏虽然也可以乐在其中,但总不免显得有些枯燥和冷清,局域网中联机游戏也就应运而生。从 Windows 的红心大战,到枪战、策略等諸多游戏,都支持联机对战。

# 1.2 局域网的组成

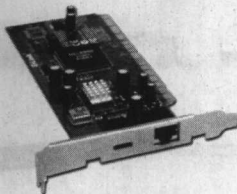
对于那些试图自己动手搭建一个局域网的网络管理员而言,透彻了解局域网的组成是非常重要的。需要注意的是,与电脑千篇一律的构成方式不同,局域网往往根据规模和应用的不同,而分别采用一些功能与性能各异的网络设备。

## 1.2.1 硬件设备

就像电脑中不同的板卡分别拥有不同的功能一样,局域网设备也在局域网中分别扮演着不同的角色。只有清楚了解它们各自的功能和作用后,才能根据网络建设的实际需要选择相应的设备。

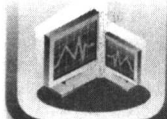
### 1. 网卡

网卡 (Network Interface Card, 简称 NIC), 也称网络界面卡, 或网络接口卡, 是电脑与局域网相互连接的接口。任何连接到局域网的电脑都必须拥有至少一块网卡。



网卡有很多种,不同类型的网络(如以太网、ATM、FDDI、令牌环等)、不同类型的介质(如双绞线、细缆、光纤、无线等)、不同速率的带宽(如 10Mbps、100Mbps、1000Mbps),以及不同





的应用（如工作站、服务器）应当分别选用不同的网卡。

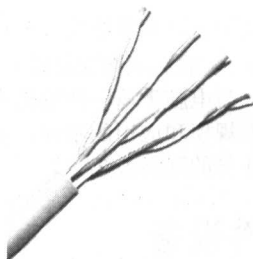
## 2. 传输介质

仅仅有一块网卡是不够的，如果想与其他电脑进行通讯，还必须借助于通信介质。常见的通信介质有双绞线、同轴电缆、无线电波和光缆等。

### (1) 双绞线

双绞线类似于普通的相互绞合的电线，只是拥有八根相互绝缘的8根铜芯。这8根铜线分为四对，每两根为一对，并按照规定密度和一定的规律相互缠绕。

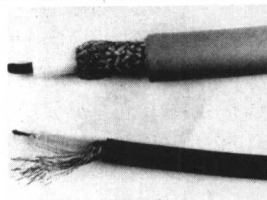
屏蔽双绞线由于价格昂贵、实施难度大、设备要求严格，在我国极少被应用于实践。目前，应用最多的是超五类和六类非屏蔽双绞线。如下图所示的为超五类非屏蔽双绞线。



### (2) 同轴电缆

同轴电缆的结构类似于有线电视的铜芯电缆，由一根空心的圆柱网状铜导体和一根位于中心轴线位置的铜导线组成，铜导线、空心圆柱导体和外界之间分别用绝缘材料隔开。

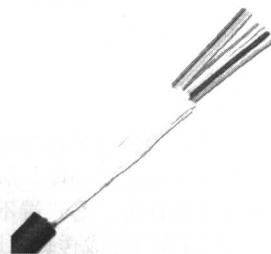
根据直径的不同，同轴电缆被分为细缆和粗缆两种。由于粗缆的安装和接头制作较为复杂，在中小型局域网已经很少被使用。细缆也由于传输率低，网络稳定性和可维护性差而逐渐被淘汰出局。下图所示的为同轴电缆。



### (3) 光缆

光缆，又称为光纤按照发光源的不同可分为单模光纤和多模光纤。单模光纤采用激光二极管 LD 作为光源，而多模光纤采用发光二极管 LED 为光源。

多模光纤传输频带宽、传输距离短、成本低，一般用于建筑物内或地理位置相邻的环境；单模光纤传输频带宽、传输距离长、成本较高，通常在建筑物之间或地域分散的环境中使用。随着光纤设备价格的回落，光纤传输是未来网络的发展方向。



### (4) 电磁波

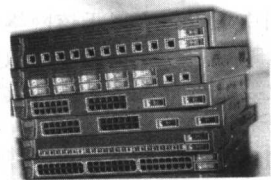
无线网络类似于现在流行的小灵通，是以电磁波作为信息的载体，实现电脑相互通讯而构成网络的。

虽然设备的价格颇为不菲，且传输速率偏低，但非常适用于移动办公一族，也适用于那些由于工作需要而不得不经常搬来搬去的公司或企业，如石油勘探、测绘等。

## 3. 集线设备

在绝大多数网络中（如使用双绞线和光纤连接的网络），集线设备是整个网络的中心，担当着连接网络中所有设备的重任。根据工作方式的不同，集线设备大致可以分为集线器和交换机两种。

集线设备性能也在很大程度上决定着整个网络的性能，决定着网络中数据的传输速度，如下图所示为 Cisco Catalyst 交换机。



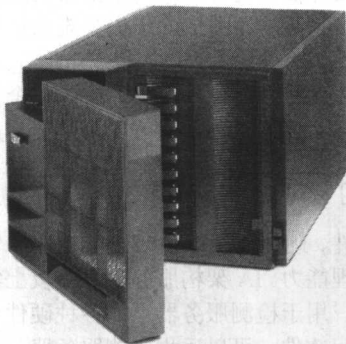
## 4. 服务器

服务器用于向用户提供各种网络服务，如文件服务、Web 服务、FTP 服务、E-mail 服务、数据库服务、打印服务、索引服务、传真服务、流媒体播放服务等。

服务器能在网络中提供哪些服务，完全是由服务器安装的应用软件所决定的。

服务器的硬件配置都非常好，多个高速 CPU、多块大容量硬盘、数以 GB 计的内存、冗余的电源等，以适应繁重的负荷，如下图所示为 IBM 服务器。





在对等网络中是没有服务器的，虽然用户之间也可以实现资源共享，但是，访问安全和权限受到很大限制。

## 5. 工作站

工作站是指在网络中享有服务，并用于直接完成某种工作和任务的电脑。客户端软件建立与服务器的连接，并将用户的请求定向并传送到服务器，共享服务器提供的各种资源和服务。

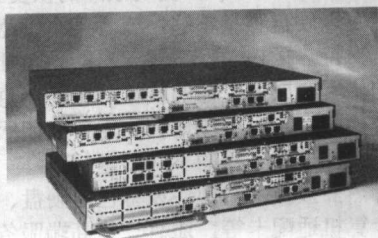
在对等网络中，每一台电脑既是客户机，又是服务器，既享受其他电脑提供的服务、又向其他电脑提供服务。

## 6. 共享资源和外设

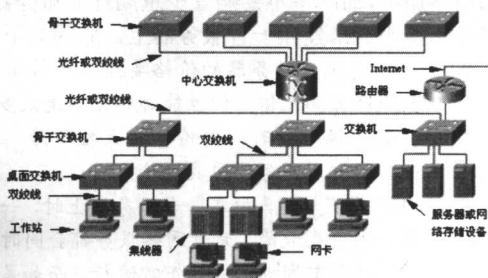
共享资源和外设包括连接到服务器的存储设备（如硬盘、磁盘阵列、磁带机、CD-R、CD-RW 等）、光盘驱动器（CD-ROM、光盘阵列和 DVD-ROM 等）、打印机、绘图仪，以及其他一切允许授权用户使用的设备。

## 7. 路由器

路由器就是一种专用电脑，用于计算并确定数据传输的路由。路由器的主要作用有两个，一是用于连接不同类型的网络，二是用于隔离广播域，避免广播风暴。无论是局域网之间的连接，还是局域网接入 Internet，都离不开路由器，如下图所示为 Cisco 路由器。



各网络设备在网络中的位置如下图所示。



## 1.2.2 局域网操作系统

如同电脑只有硬件而没有软件将既不能启动、也无法运行，更无法完成任何工作一样，没有局域网操作系统和网络协议的网路，也将无法实现电脑之间彼此的通讯。

### 1. 局域网操作系统

根据电脑在局域网络中地位的不同，可以将局域网络分为对等网络和客户端/服务器网络。而电脑在网络中的地位，主要是由局域网操作系统来决定的。

服务器运行专用的网络操作系统，如 Windows NT/2000 Server、Windows Server 2003、NetWare、Unix、Linux 等。

工作站的操作系统既可以是商用客户端软件，如 Windows NT Workstation、Windows 2000/XP Professional，也可以是家用操作系统，如 Windows 9X/Me/XP Home 等。

### 2. 通信协议

通信协议用来协调不同的网络设备间的信息交换。通信协议能够建立起一套非常有效的机制，每个设备均可据此识别来自其他设备的有意义的信息。其实，通信协议就好像是语言规则。无论汉语、英语、法语还是德语，都能够用来很好地进行交流。

当然，这只有交谈双方都使用同一种语言，并遵守相应的语言规则时，彼此之间才能够听得懂。就好像不同的民族大都使用不同的语言规则一样，在不同的网络操作系统中也大都使用不同的通信协议，如 TCP/IP、NetBEUI、IPX/SPX、AppleTalk 等等。

## 1.2.3 服务器

随着网络规模的扩大和网络应用服务的丰富，也就对服务器也就提出了更多和更高的要求。当网络服务较多时，建议购置多台服务器，分别承担不



同的网络服务,而尽量不要购置少量高性能服务器,将多种网络服务搭建在一台服务器上。原因如下:

- 一台高配置服务器的价格要比若干较低配置服务器高几倍,但性能却相差不是太多,并且在很短的时间内价格会大幅下降。因此,低配置服务器更具性价比。
- 当诸多服务都集中在一台服务器上时,一旦服务器发生故障,大量网络服务都会同时终止,将严重影响网络的正常运行。而如果将服务分散到几台服务器上,即使发生故障,也不会妨碍其他网络服务的提供。
- 在一台服务器上安装多种网络服务,会占用大量的系统资源。当多种服务并发访问时,将导致服务器性能大幅下降,无法及时响应客户的请求。如果由多台服务器分担不同的网络服务,将由于并发访问量的减少,避免类似问题的发生。
- 将过多的网络服务放置在一台服务器上时,即使有强劲的 CPU 和大量的内存,网络接口带宽和硬盘读取速率都有可能成为服务器的瓶颈。
- 当服务器的性能不能满足网络访问需要时,可以利用多台低配置服务器构建服务器群集,或利用软件、硬件等方式实现服务器的负载均衡,既可以提高服务器的整体处理性能,又可以有效地延长服务器的使用寿命。

对于办公 OA 或数据库之类的服务器,应当选择高性能服务器。如果采用性能较差的服务器,将由于系统不堪重负而瘫痪,或者处理能力有限而响应缓慢。因此,必须采用双 CPU 架构的部门级服务器,用于进行快速的数据处理,及时响应大量的并发访问。

在选购服务器时,应注意以下几个方面的因素:

## 1. 扩展性

服务器应该是具有高度可扩展性的。可扩展是指服务器的配置,如内存、硬盘、处理器等,可以在原有的基础上很方便根据需要来增加。

服务器具有较多的扩展插槽,较多的驱动器支架及较大的内存扩展能力,提供冗余电源、冗余风扇、冗余硬盘,方便用户在需要时作必要的扩充,以保护原有的投资。

## 2. 可靠性

服务器的可靠性都要比普通计算机要高得多,因为服务器是在网络中一般是连续不断工作的。

许多重要的数据都保存在服务器上,许多网络

服务都在服务器上运行,一旦服务器发生故障,将会丢失大量的数据,造成的损失是难以估计的,而且服务器上运行的服务器,如代理上网、安全验证、电子邮件服务等都将失效,从而造成整个网络的瘫痪,因此,对服务器可靠性的要求是非常高的。

## 3. 可管理性

从软件、硬件的设计上,IA 架构服务器具备较完善的管理能力。IA 架构服务器在主板上集成了各种传感器,用于检测服务器上的各种硬件设备,同时配合相应软件,可以远程监测服务器,从而使网络管理员对服务器系统进行及时有效的管理。

有些服务器随机安装了服务器管理软件,它可以远程检测服务器主板上的传感器记录的信号,对服务器进行远程的监测和资源分配。而计算机由于其应用场合较为简单,所以没有较完善的硬件管理系统。

## 4. 处理能力

服务器是为网络上其他计算机提供服务的,由于服务器要将其数据、硬件提供给网络共享,在运行某些应用程序时要处理大量的数据,很有可能需要同时响应几十台、几百台甚至上千台计算机的请求,因此服务器的速度应该比普通的计算机快得多。越是高档的服务器,其速度也越快。

## 5. I/O 能力

由于服务器需要同时响应多个用户的并发请求,因此,必须具有较高的 I/O 能力。第一,应拥有快速的 SCSI 接口,并借助 RAID 技术实现多硬盘的同时读取,从而加快对数据的读取和存储能力;第二,应采用计算机 I-X 等新型接口技术,实现高带宽的数据传输;第三,应提供千兆网络连接,实现与网络的高速连接。

## 6. 故障恢复能力

热插拔技术可以方便地对服务器进行维护,并且在不中断服务的情况下,实现故障的恢复和扩展。例如,当发现硬盘容量不够,或者某个硬盘损坏,如果硬盘支持热插拔,只需要把新的硬盘插上服务器预留的位置,或者把坏的硬盘从服务器直接拔下来进行替换即可,所有操作都不需要关闭服务器系统,从而保证了服务器的不间断运行。

支持热插拔技术的硬件设备包括硬盘、电源、风扇、计算机适配卡等,还有一些高端服务器甚至支持内存、CPU 的热插拔。

凡是支持热插拔技术的硬件，都可以在线（不关闭服务器电源）直接插上新的部件或者从服务器上拔下旧的部件，从而极大地方便了服务器的维护，确保服务器 7×24 不间断运行。

## 1.2.4 网络防火墙

在 FTTX+LAN 方式中，不再需要路由器作为远程接入设备。但是，该方式将直接导致网络安全性的大大降低，遭受恶意攻击和病毒侵害的可能性明显增加，因此，对网络安全提出了更高的要求。

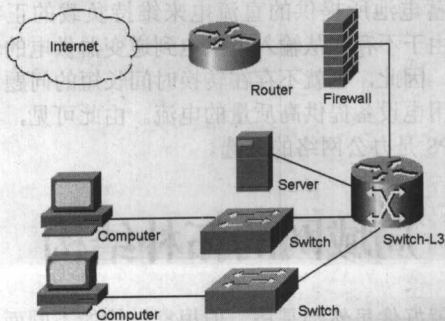
所以，必须选用网络防火墙，关闭未被使用的 TCP/UDP 端口，以避免蠕虫病毒和网络木马的入侵，保证网络内部计算机和网络服务器的安全，防止重要和敏感数据的丢失。



网络防火墙是目前最为流行、也是使用最为广泛的一种网络安全技术。网络防火墙，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。如果没有防火墙，内部网络上的服务器都暴露在局域网或 Internet 上，极易受到攻击。也就是说，内部网络的安全性要由每一台服务器来决定，并且整个内部网络的安全性等于其中防护能力最弱的系统。防火墙作为一个分离器、限制器和分析器，用于执行两个网络之间的访问控制策略，有效地监控了内部网和 Internet 之间的任何活动。

网络防火墙通常位于路由器的后端，或者代理服务器的前端，从而为整个网络提供安全保障。



### 1. 网络防火墙的重要作用

在构建安全网络环境的过程中，防火墙作为第一道安全防线，既可为内部办公网络提供必要的访问控制，但又不会造成网络的瓶颈，并通过安全策略控制进出系统的数据，保护办公网络内部的关键资源。由此可见，对于联接到 Internet 的内部办公网络而言，选用防火墙是非常必要的。

对于办公网络而言，网络防火墙的作用如下：

#### (1) 网络安全的屏障

防火墙可通过过滤不安全的服务而降低风险，极大地提高内部网络的安全性。由于只有经过选择并授权允许的应用协议才能通过防火墙，所以，网络环境变得更安全。

防火墙可以禁止诸如不安全的 NFS 协议进出受保护网络，使攻击者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。防火墙能够拒绝以上所有类型攻击的报文，并将情况及时通知防火墙管理员。

#### (2) 强化网络安全策略

通过以防火墙为中心的安全方案配置，能将所有安全软件（如口令、加密、身份认证、审计等）配置在防火墙上。

与将网络安全问题分散到各个主机上相比，防火墙的集中安全管理更经济。例如，在网络访问时，一次一密口令系统和其它的身份认证系统完全可以不必分散在各个主机上，而集中在防火墙上。

#### (3) 对网络存取和访问进行监控审计

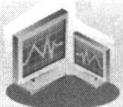
由于所有的访问都必须经过防火墙，所以防火墙就不仅能够创建完整的日志记录，而且还能够提供网络使用情况的统计数据。

当发生可疑动作时，防火墙能进行适当的报警，并提供网络是否受到监测和攻击的详细信息。另外，收集一个网络的使用和误用情况也是一项非常重要的工作。这不仅有助于了解防火墙是否能够抵挡攻击者的探测和攻击，了解防火墙的控制是否充分有效，而且有助于作出网络需求分析和威胁分析。

#### (4) 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，限制内部网络中不同部门之间互相访问，从而保障了网络内部敏感数据的安全。另外，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，甚至由此而暴露了内部网络的某些安全漏洞。使用防火墙就可以





隐蔽那些内部细节,如 Finger、DNS 等服务。

Finger 显示了主机的所有用户的用户名、真名、最后登录时间和使用 shell 类型等。但是 Finger 显示的信息非常容易被攻击者所获悉。

攻击者可以知道一个系统使用的频繁程度,这个系统是否有用户正在连线上网,这个系统是否在被攻击时引起注意等等。防火墙可以同样阻塞有关内部网络中的 DNS 信息,这样一台主机的域名和 IP 地址就不会被外界所了解。

## 2. 硬件防火墙与软件防火墙

防火墙分为软件防火墙和硬件防火墙两种。软件防火墙是安装在计算机平台的软件产品,它通过在操作系统底层工作来实现网络管理和防御功能的优化。硬件防火墙的硬件和软件都单独进行设计,有专用网络芯片处理数据包。

同时,采用专门的操作系统平台,从而避免通用操作系统的安全性漏洞。并且对软硬件的特殊要求,使硬件防火墙的实际带宽与理论值基本一致,有着高吞吐量、安全与速度兼顾的优点。

国内市场的硬件防火墙,大部分都是“软硬件结合的防火墙”,即“定制机箱+X86 架构+防火墙软件模块”(大多数基于 Linux 或 UNIX 系统开发)。其核心技术实际上仍然是软件,吞吐量不高,容易造成带宽瓶颈。由于计算机架构本身不稳定,因此,往往难以适应 7×24 的不间断运行。

所以,这种防火墙一般只能满足中低带宽的安全要求,在高流量环境下往往会造成网络堵塞甚至系统崩溃。

## 3. 硬件防火墙类型的选择

硬件防火墙分为包过滤防火墙、应用网关防火墙和规则检查防火墙。对于办公网络而言,通常应当选择包过滤防火墙。

包过滤防火墙是基于源地址和目的地址、应用或协议以及每个 IP 包的端口是否作出允许通过判断的防火墙。

路由器便是传统的包过滤防火墙,大多路由器都能通过检查这些信息来决定是否将所收到的包转发,但它不能判断出一个 IP 包来自何方,去向何处。先进的包过滤防火墙可以判断这一点,它可以提供内部信息以说明所通过的连接状态和一些数据流的内容,把判断信息同规则表进行比较,在规则表中定义了各种规则来表明是否同意或拒绝包的通过。

包过滤防火墙检查每一条规则直至发现包中的信息与某规则相符。如果没有一条规则能符合,防火墙就会使用默认规则,一般情况下,默认规则就

是要求防火墙丢弃该包。其次,通过定义基于 TCP 或 UDP 数据包的端口号,防火墙能够判断是否允许建立特定的连接,如 Telnet、FTP 连接。

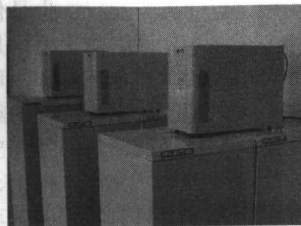
网络级防火墙的优点是简洁、速度快、费用低,并且对用户透明,缺点是对网络的保护很有限,因为它只检查地址和端口,对网络更高协议层的信息无理解能力。

## 1.2.5 UPS 不间断电源

随着用电量的不断增加,电力供需矛盾日益突出,特别是在冬夏两季的用电高峰,断电事故频频发生,并且电压忽高忽低很不稳定。

毫无疑问,不稳定的电压不仅会导致系统瘫痪,甚至还会造成服务器和网络设备的硬件故障、丢失宝贵数据,酿成重大事故。

因此,办公网络应当配置在线式不间断电源(UPS 电源),由 UPS 为所有设备提供稳定的电源输出,保障网络设备和服务器的正常运行。UPS 的总功率应当按照每台服务器不少于  $1\text{KW} \times 8$  小时,每台网络设备不少于  $0.5\text{KW} \times 8$  小时计算。



在线式 UPS 开机后,逆变器始终处于工作状态,因此,在输入电异常转为电池放电时没有转换时间,即零中断。当输入电供电正常时,它首先将输入交流电变为直流电,接下来逆变器将直流电变为功率放大的脉宽调制驱动电源信号,再经逆变器的输出滤波器重新变成交流电提供给负载。

当在线式 UPS 的输出端承受 100% 的加载或减载时,它的输出电压波动小于 5%,而且即便是这样小的瞬态电压波动也会在 20ms 内恢复到正常稳压值。当输入电供电中断时,UPS 中的逆变器利用机内蓄电池所提供的直流电来维持负载的正常运转,由于不存在从输入电供电到逆变器供电的转换步骤,因此,也就不存在转换时间长短的问题。可以向用电设备提供高质量的电流。由此可见,在线式 UPS 是办公网络的首选。

## 1.3 局域网的拓扑结构

就好像虽然都是桥,但根据结构的不同而分为