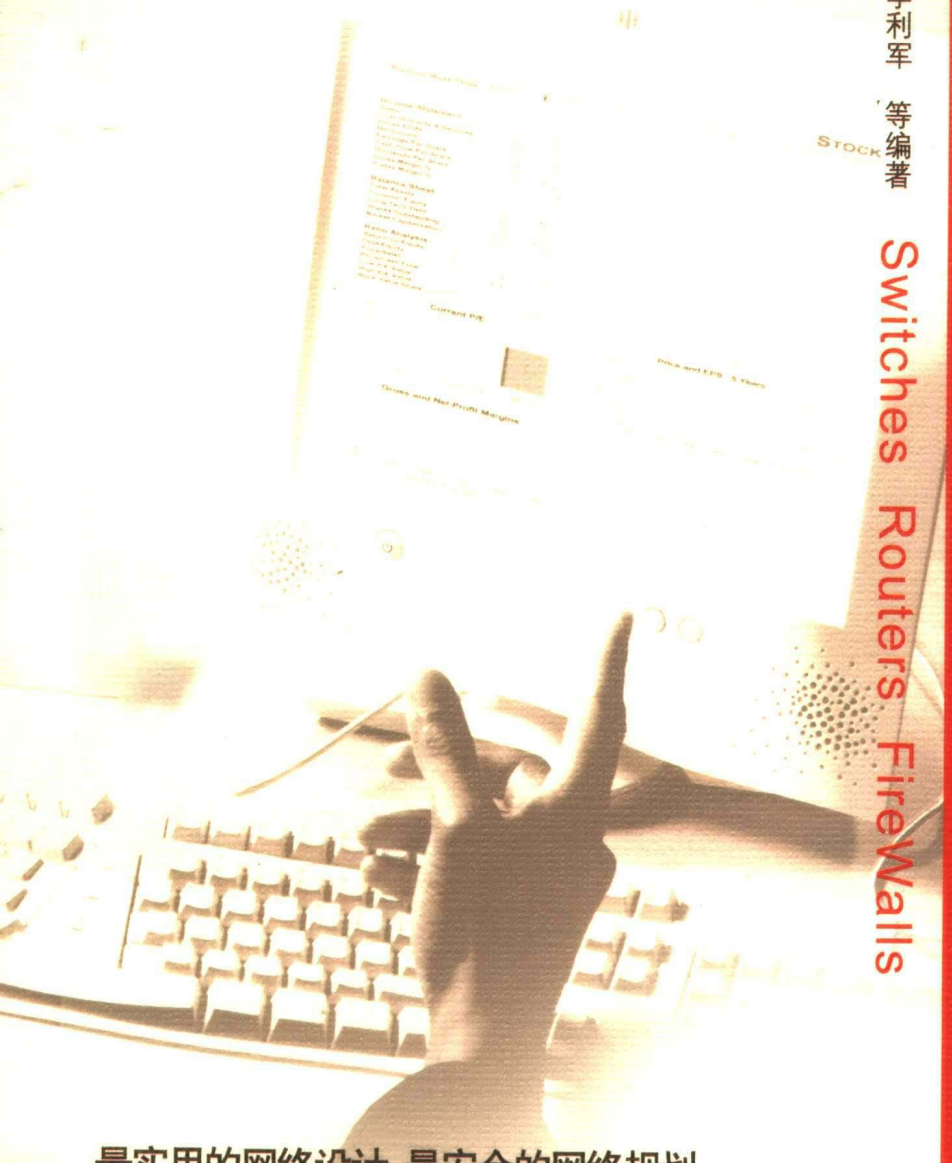
网管天下

交换机·路由器·防火墙

Switches Routers FireWalls

刘晓辉 李利军 等编著



最实用的网络设计 最安全的网络规划
最新式的网络设备 最流行的网络技术
最通用的网络配置 最智能的网络管理

- 交换机、路由器和防火墙的原理与使用
- 重要性能参数设置与设备选择
- 端口类型与设备连接策略
- 命令行和图形化配置与管理
- 网络搭建与管理的硬件解决方案

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

网管天下

交换机·路由器·防火墙

刘晓辉　李利军　等编著

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

内 容 简 介

本书深入细致地介绍了用于构建网络的最重要的硬件设备——交换机、路由器和防火墙，涵盖了原理、参数、分类、适用、规划、接口、连接、配置、管理、监控、故障等诸多方面，体现并融合了最新技术、最新设备和最新应用，是一整套紧贴网络搭建、配置和管理实际的完全硬件解决方案。本书突出实用性和可操作性，语言表述流畅准确，理论讲解深入浅出，具体操作详略得当，注重培养读者的动手能力和分析问题能力。

本书适用于大中型网络管理员，以及所有准备从事网络管理的网络爱好者，并可作为大专院校计算机专业的教材。

图书在版编目(CIP)数据

交换机·路由器·防火墙 / 刘晓辉等编著.—北京：电子工业出版社，2007.8
(网管天下)
ISBN 978-7-121-04795-4

I. 交… II. 刘… III. ①局部网络－信息交换机②局部网络－路由选择③局部网络－防火墙 IV. TP393.1

中国版本图书馆 CIP 数据核字（2007）第 116592 号

责任编辑：郭鹏飞
印　　刷：北京市天竺颖华印刷厂
装　　订：三河市金马印装有限公司
出版发行：电子工业出版社出版
　　北京市海淀区万寿路 173 信箱　邮编：100036
开　　本：787×1092　1/16　印张：36　字数：876 千字
印　　次：2007 年 8 月第 1 次印刷
印　　数：6000 册　　定价：58.00 元

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

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

服务热线：（010）88258888。

前言

关于《网管天下》丛书

《网管天下》丛书是一套由国内资深网络专家写给网络建设与管理人员的应用实践手册，其目的在于帮助初、中级网络管理员，全方位地解决网络建设与管理中的各种实际问题，包括网络规划设计、网络布线实施、网络设备连接、网络配置管理、网络服务搭建、网络深入应用、网络故障排除、网络安全管理等诸多方面，囊括了网络管理中几乎所有的内容，其目的在于将网络理论与实际应用相结合，提高读者分析和解决具体问题的能力，将所学变为所用，将书本知识变为操作技能。

本丛书具有以下特点：

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

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

3. 理论新、技术新、设备新、案例新。所有的应用案例都发生在两年以内，而且案例中只涉及最主流的、最成熟的设备和技术，以及最新版本的软件，不再讨论那些已被淘汰或面临淘汰的东西，从而力求反映网络的新技术和新潮流。不仅让读者学了就能用，而且还可以拥有三年左右的“保鲜”期。

关于本书

交换机、路由器和防火墙是构成网络硬件的金三角。交换机用于实现计算机互联，构建局域网络；路由器实现网络互联，构建广域网络；防火墙实现互联限制，构建安全网络。没有交换机计算机之间就无法通信，就不能搭建局域网络，因此，交换机是网络构建的基石。没有路由器就不能实现与其他网络和 Internet 的连接，局域网就会成为信息孤岛，所以路由器是网络互联的桥梁。没有防火墙就不能实现网络内部的安全，客户端、服务器和数据信息就没有安全保障，因此，防火墙是安全稳定的保障。可见，交换机、路由器和防火墙三者各司其职、相互结合、缺一不可。

与其他网络类图书不同，本书从一个全新的角度，深入、全面、细致地介绍了交换机、路由器和防火墙的原理、参数、分类、适用、规划、接口、连接、配置、管理、监控、故障等诸多方面的内容，涵盖了从规划设计、网络搭建、设备配置到状态监控、故障诊断的所有重要硬件技术，是一本专门为大中型网络管理员量身打造的硬件设备教程，使之迅速完成从电脑爱好者向专业网管员的过渡。

全书共分为 17 章。第 1 章网络设备综述，分别介绍了交换机、路由器和防火墙在网络中的作用和应用。第 2 章至第 6 章介绍了交换机的工作原理、交换技术、分类与适用、参数与选择、端口与连接、状态与检测，以及交换机的配置。第 7 章至第 11 章，介绍了路由

器的工作原理、路由协议、分类与适用、参数与选择、端口与连接、状态与检测，以及路由器的配置。第 12 章至第 15 章详细介绍了安全设备的工作原理，IPS、IDS 和防火墙的优势与适用、参数与选择、端口与连接、状态与检测，以及安全设备的配置。第 16 章全面介绍了网络设备的管理方式，以及流量监控与分析。

笔者长期从事网络建设、网络管理、网络教学和网络实验工作，具有较高的理论水平和丰富的实践经验，曾经出版过 50 余部网络和系统方向的图书，均以易读、易学、实用的特点，得到众多读者的一致好评，并取得了不错的销售业绩。本书是笔者的又一呕心沥血之作，希望能对大家搭建和管理网络有所帮助。

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

刘晓辉

2007 年 6 月

目录

第 1 章　交换机・路由器・防火墙综述 1

1.1　交换机概述 2
1.1.1　交换机的功能 2
1.1.2　交换机与交换式网络 4
1.1.3　交换机的工作原理 6
1.2　路由器概述 8
1.2.1　路由器的功能 8
1.2.2　路由器的工作原理 11
1.3　防火墙概述 12
1.3.1　网络防火墙的功能 12
1.3.2　防火墙的工作原理 15
1.4　网络设备在网络中的应用 16
1.4.1　交换机在网络中的应用 16
1.4.2　路由器在网络中的应用 18
1.4.3　防火墙在网络中的应用 20

第 2 章　交换机概述 23

2.1　交换机简介 24
2.1.1　交换式工作原理 24
2.1.2　交换模式 27
2.2　交换机技术 30
2.2.1　虚拟网技术 30
2.2.2　私有虚拟网技术 34
2.2.3　第 3 层交换技术 35
2.2.4　第四层交换技术 37
2.2.5　扩展树技术 38

2.2.6 链路汇聚技术.....39
2.2.7 服务质量技术.....40
2.2.8 IP 语音技术.....41
2.2.9 基于端口的传输控制.....42
2.2.10 千兆位以太网技术.....43
2.2.11 万兆位以太网技术.....45
2.2.12 路由冗余.....47
2.3 交换机的分类.....50
2.3.1 智能交换机与傻瓜交换机.....50
2.3.2 固定端口交换机与模板化交换机.....51
2.3.3 接入层交换机、汇聚层交换机与核心层交换机.....52
2.3.4 以太网交换机与 ATM 交换机.....55
2.3.5 二层交换机与多层交换机.....55
2.3.6 快速以太网交换机、千兆位以太网交换机与万兆位以太网换机.....56
2.3.7 对称交换机与非对称交换机.....58
2.3.8 桌面交换机与机架式交换机.....58
2.3.9 特殊用途交换机.....59

第 3 章 交换机的参数与选择.....61

3.1 交换机的主要参数.....62
3.1.1 三层交换机的主要参数.....62
3.1.2 二层交换机的主要参数.....66
3.2 交换机的选择策略.....70
3.2.1 核心交换机的选择.....70
3.2.2 汇聚层交换机的选择.....74
3.2.3 接入层交换机的选择.....76
3.2.4 可网管交换机的选择.....78

第 4 章 交换机的端口与连接.....81

4.1 IEEE 802.3 系列标准.....82
4.1.1 IEEE 802.3 标准.....82
4.1.2 IEEE 802.3u 标准.....82
4.1.3 IEEE 802.3z 和 802.3ab 标准.....83
4.1.4 IEEE 802.3ae、802.3ak 和 802.3an 标准.....85

4.2 交换机端口类型 88
4.2.1 光纤端口 88
4.2.2 双绞线端口 89
4.2.3 GBIC 模块与插槽 91
4.2.4 SFP 模块与插槽 92
4.2.5 10GE 模块与插槽 93
4.2.6 共用端口 94
4.2.7 TwinGig 转换模块 95
4.2.8 跳线与使用 95
4.3 交换机的连接策略 99
4.3.1 不同性能交换机的连接策略 99
4.3.2 非对称交换机的连接策略 100
4.3.3 对称交换机的连接策略 100
4.4 交换机的连接 101
4.4.1 堆叠与级联 102
4.4.2 光纤端口的连接 103
4.4.3 双绞线端口的连接 105
4.4.4 远程交换机的连接 107
4.5 交换机的堆叠 108
4.5.1 Cisco 交换机的堆叠 108
4.5.2 3Com 交换机的堆叠 113
4.5.3 华为交换机的堆叠 114

第 5 章 交换机的基本配置 115

5.1 交换机配置前的准备 116
5.1.1 交换机的管理方式 116
5.1.2 CLI 命令行及使用 123
5.1.3 交换机配置前的规划 132
5.2 交换机的初始配置 133
5.2.1 配置前的准备 133
5.2.2 运行快速设置 134
5.2.3 CLI 初始配置 136
5.2.4 配置端口属性 137
5.3 使用 CNA 管理交换机 140

5.3.1 CNA 简介 141
5.3.2 添加交换机 141
5.3.3 监控交换机 144
5.3.4 配置管理交换机 147
5.3.5 维护交换机 148
5.4 VLAN 配置 149
5.4.1 VLAN 配置策略 149
5.4.2 VLAN 默认配置 149
5.4.3 配置 VLAN 150
5.4.4 配置 VLAN Trunk 152
5.4.5 配置 VTP 155
5.4.6 配置 VMPS 161
5.5 私有 VLAN 配置 167
5.5.1 PVLAN 概述 167
5.5.2 配置 PVLAN 170
5.6 三层交换机基本配置 174
5.6.1 为第三层接口配置 IP 地址 174
5.6.2 设置默认网关 176
5.6.3 设置静态路由 176
5.6.4 配置三层 EtherChannel 177

第 6 章 交换机的高级配置 179

6.1 基于端口的传输控制 180
6.1.1 广播风暴控制 180
6.1.2 端口流控制 182
6.1.3 端口带宽限制 182
6.1.4 保护端口 184
6.1.5 端口阻塞 184
6.1.6 端口安全 185
6.2 冗余链接配置 187
6.2.1 配置 EtherChannel 187
6.2.2 STP 配置 191
6.2.3 配置 Postfast 端口 199
6.3 访问列表配置 201

6.3.1 访问列表概述.....201
6.3.2 创建并应用 IP 访问列表.....203
6.3.3 创建并应用端口访问列表.....209
6.3.4 创建并应用 VLAN 访问列表.....210
6.4 基于端口的认证配置.....211
6.4.1 IEEE802.1x 简介.....212
6.4.2 启用 IEEE 802.1X 认证.....213
6.4.3 配置交换机到 RADIUS 服务器的通信.....214
6.4.4 配置重新认证周期.....215
6.4.5 修改安静周期.....216
6.5 DHCP 中继.....216
6.5.1 DHCP 中继代理概述.....217
6.5.2 DHCP 默认配置.....218
6.5.3 DHCP 配置策略.....218
6.5.4 配置 DHCP 中继代理.....219
6.5.5 指定包转发地址.....220
6.5.6 启用 DHCP 侦听.....221
6.5.7 在私有 VLAN 中启用 DHCP 侦听.....222
6.5.8 启用 DHCP 侦听绑定数据库代理.....222
6.5.9 配置 IP 源地址保护.....223
6.6 QoS 配置.....225
6.6.1 QoS 概述.....225
6.6.2 配置 Auto-QoS.....226
6.7 配置 CDP.....232
6.7.1 CDP 概述.....232
6.7.2 CDP 默认配置.....233
6.7.3 CDP 配置.....233
6.8 配置 SPAN 和 RSPAN.....235
6.8.1 SPAN 和 RSPAN 简介.....235
6.8.2 SPAN 和 RSPAN 默认配置.....237
6.8.3 SPAN 会话中的流量监视限制.....237
6.8.4 配置本地 SPAN.....238
6.8.5 配置 RSPAN.....242
6.8.6 显示 SPAN 和 RSPAN 状态.....247

6.9 配置 HSRP 247
6.9.1 HSRP 概述 247
6.9.2 HSRP 默认配置 249
6.9.3 HSRP 的配置方针 250
6.9.4 启用 HSRP 250
6.9.5 配置 HSRP 优先权 251
6.9.6 配置 MHSRP 252
6.9.7 配置 HSRP 认证和时钟 252
6.9.8 配置 HSRP 组和簇 253
6.9.9 显示 HSRP 配置 253

第 7 章 路由器概述 255

7.1 路由器简介 256
7.1.1 路由器的主要功能 256
7.1.2 路由器工作原理 259
7.1.3 路由器在网络中的应用 260
7.2 路由器的分类与适用 262
7.2.1 按性能划分 262
7.2.2 按结构划分 263
7.2.3 按网络位置划分 264
7.2.4 按功能划分 264
7.2.5 按传输性能划分 265
7.2.6 按网络类型划分 265
7.3 路由协议 266
7.3.1 静态路由 266
7.3.2 RIP 路由协议 267
7.3.3 OSPF 路由协议 269
7.3.4 BGP 路由协议 274
7.3.5 IS-IS 路由协议 276
7.3.6 EIGRP 路由协议 278

第 8 章 路由器的参数与选择 281

8.1 路由器的分类 282
8.1.1 按性能划分 282

8.1.2 按结构划分.....283
8.1.3 按网络位置划分.....283
8.1.4 按功能划分.....284
8.1.5 按传输性能划分.....284
8.1.6 按网络类型划分.....284
8.2 路由器的参数.....284
8.2.1 路由器基本参数.....285
8.2.2 路由器性能参数.....288
8.3 路由器的选择.....290
8.3.1 路由器的选购原则.....290
8.3.2 选购时应考虑的因素.....292

第 9 章 路由器的接口与连接.....293

9.1 路由器接口.....294
9.1.1 常用网络接口.....294
9.1.2 路由器配置接口.....299
9.2 路由器的连接.....299
9.2.1 路由器连接策略.....299
9.2.2 路由器面板.....300
9.2.3 路由器连接.....303
9.3 路由器的连接测试.....306
9.3.1 Show 命令判断.....307
9.3.2 LED 指示灯判断.....307

第 10 章 Cisco 路由器基本配置.....311

10.1 使用 SDM 配置.....312
10.1.1 路由器初始化配置.....312
10.1.2 使用 SDM 配置路由器.....315
10.2 路由器基本配置.....330
10.2.1 路由器端口编号.....330
10.2.2 IP 协议配置原则.....333
10.2.3 配置主机名和密码.....334
10.2.4 配置快速以太网接口.....335
10.2.5 配置同步串行接口.....336

10.3 配置静态路由 337
10.3.1 配置静态路由 337
10.3.2 LAN 方式接入 Internet 338
10.3.3 DDN 接入 Internet 339
10.4 网络地址转换 341
10.4.1 理解 NAT 341
10.4.2 静态地址转换的实现 343
10.4.3 动态地址转换的实现 343
10.4.4 端口复用地址转换 345

第 11 章 Cisco 路由器的高级配置 347

11.1 配置广域网接口 348
11.1.1 接口的一般配置 348
11.1.2 同步串口配置 350
11.2 配置逻辑接口 353
11.2.1 Loopback 接口配置 353
11.2.2 NULL 接口配置 353
11.2.3 Tunnel 接口配置 354
11.2.4 Dialer 接口配置 356
11.2.5 子接口配置 357
11.3 配置 PPP 和 MP 协议 358
11.3.1 PPP 和 MP 协议概述 358
11.3.2 PPP 协议的配置 360
11.3.3 MP 协议的配置 363
11.3.4 PPP 的监控 364
11.4 配置 HDLC 协议 365
11.4.1 HDLC 协议概述 365
11.4.2 HDLC 配置 366
11.5 配置帧中继协议 366
11.5.1 帧中继概述 366
11.5.2 帧中继的基本配置 369
11.5.3 帧中继子接口配置 372
11.5.4 帧中继的高级配置 374
11.5.5 帧中继监控和维护 375

11.6 配置 LAPB 和 X.25 协议 376
11.6.1 LAPB、X.25 协议概述 376
11.6.2 配置 LAPB 协议 377
11.6.3 配置 X.25 协议 379
11.6.4 配置 X.25 高级功能 385
11.6.5 显示 X.25 接口信息 386
11.7 配置 RIP 387
11.7.1 RIP 的默认配置 387
11.7.2 配置 RIP 路由 387
11.7.3 配置 RIP 认证 389
11.7.4 配置水平分割 390
11.8 配置 OSPF 391
11.8.1 默认的 OSPF 配置 391
11.8.2 配置基本 OSPF 参数 392
11.8.3 配置 OSPF 接口 393
11.8.4 配置 OSPF 区域参数 394
11.8.5 配置其他 OSPF 参数 395
11.8.6 配置 Loopback 接口 397
11.8.7 监控 OSPF 398
11.9 配置 EIGRP 398
11.9.1 默认的 EIGRP 配置 399
11.9.2 配置基本 EIGRP 参数 399
11.9.3 配置 EIGRP 接口 400
11.9.4 配置 EIGRP 路由认证 401
11.9.5 监视 EIGRP 402

第 12 章 安全设备概述 403

12.1 防火墙 404
12.1.1 网络安全防护的重要意义 404
12.1.2 网络防火墙简介 406
12.1.3 防火墙的主要功能 407
12.1.4 防火墙技术原理 409
12.1.5 防火墙的防御攻击技术 411
12.1.6 防火墙的局限性与脆弱性 413

12.2 IDS 414
12.2.1 IDS 概述 415
12.2.2 IDS 优势与缺陷 416
12.3.3 IDS 与防火墙联动 418
12.3 IPS 420
12.3.1 IPS 概述 420
12.3.2 IPS 的技术特征 421
12.3.3 IPS 的分类 422
12.3.4 IPS 的优势与作用 423
12.3.5 IPS 的缺陷 425
12.3.6 部署 IPS 426
12.3.7 IDS 与 IPS 比较 427

第 13 章 防火墙的主要参数与选择 429

13.1 防火墙的主要参数 430
13.1.1 防火墙的性能参数 430
13.1.2 防火墙的功能参数 431
13.2 防火墙的分类与适用 433
13.2.1 按照软硬件形式划分 433
13.2.2 按照实现技术划分 435
13.2.3 按照硬件结构划分 438
13.2.4 按照硬件实现技术划分 440
13.2.4 按照防火墙在网络中的位置划分 442
13.3 防火墙的选择 442
13.3.1 防火墙的选择策略 443
13.3.2 Cisco PIX 与 ASA 443
13.4 IDS 与 IPS 的选择 444
13.4.1 IDS 的选择 445
13.4.2 IPS 的选择 446

第 14 章 防火墙的端口与连接 449

14.1 防火墙的端口 450
14.1.1 防火墙物理端口 450
14.1.2 防火墙逻辑端口 452

14.1.3 防火墙端口的连接.....453
14.1.4 防火墙的 LED 指示灯.....455
14.2 防火墙的应用环境与连接.....457
14.2.1 防火墙连接策略.....458
14.2.2 内部网络与 Internet 的连接之间.....459
14.2.3 连接局域网和广域网.....460
14.2.4 内部网络与第三方网络的连接之间.....461
14.2.5 内部网络不同部门的连接之间.....462
14.2.6 连接同一部门的不同网络.....462
14.2.7 用户与中心服务器的连接之间.....463
14.3 IPS 的网络应用与连接.....464
14.3.1 路由防护.....464
14.3.2 交换防护.....464
14.3.3 多链路防护.....465
14.3.4 混合防护.....466

第 15 章 防火墙的配置.....467

15.1 Cisco ASDM 配置.....468
15.1.1 Cisco ASDM 简介.....468
15.1.2 Cisco ASDM 初始化.....473
15.1.3 DMZ 配置.....474
15.1.4 IPsec VPN 远程访问配置.....483
15.1.5 Site-to-Site VPN 配置.....489
15.2 CLI 方式配置.....492
15.2.1 网络访问控制.....492
15.2.2 PPTP 方式 VPN.....498
15.2.3 L2TP 方式 VPN.....501
15.2.4 PPPoE 拨号配置.....507

第 16 章 网络设备的管理.....509

16.1 系统和配置文件的管理.....510
16.1.1 TFTP 服务器.....510
16.1.2 配置文件的获取与备份.....510
16.1.3 配置文件的恢复与更新.....511

16.1.4 备份系统软件映像.....512
16.1.5 恢复或升级系统软件映像.....513
16.2 恢复网络设备密码.....514
16.2.1 密码的类型.....514
16.2.2 密码丢失后的恢复.....514
16.3 Cisco 网络设备管理.....518
16.3.1 CiscoWorks 2000 安装系统需求.....518
16.3.2 安装 CiscoWorks 2000.....519
16.3.3 对设备的监控与管理.....520
16.3.4 连接测试工具.....523
16.3.5 查看设备信息.....524
16.3.6 查看网络拓扑图.....525
16.3.7 查看失败设备.....528
16.4 网络流量监控.....529
16.4.1 网络设备吞吐率测试.....529
16.4.2 网络带宽测试.....533
16.4.3 网络流量实时监控.....534
16.5 网络流量分析.....539
16.5.1 端口镜像.....539
16.5.2 Sniffer-Pro 概述.....541
16.5.3 配置网络适配器.....541
16.5.4 仪表的使用.....542
16.5.5 捕获查看分析数据.....546
16.5.6 监控网络模式.....551
16.5.7 设置数据过滤包.....555
16.5.8 分析网络协议.....559