

Broadview®  
www.broadview.com.cn

网管宝典



刘晓辉

编著

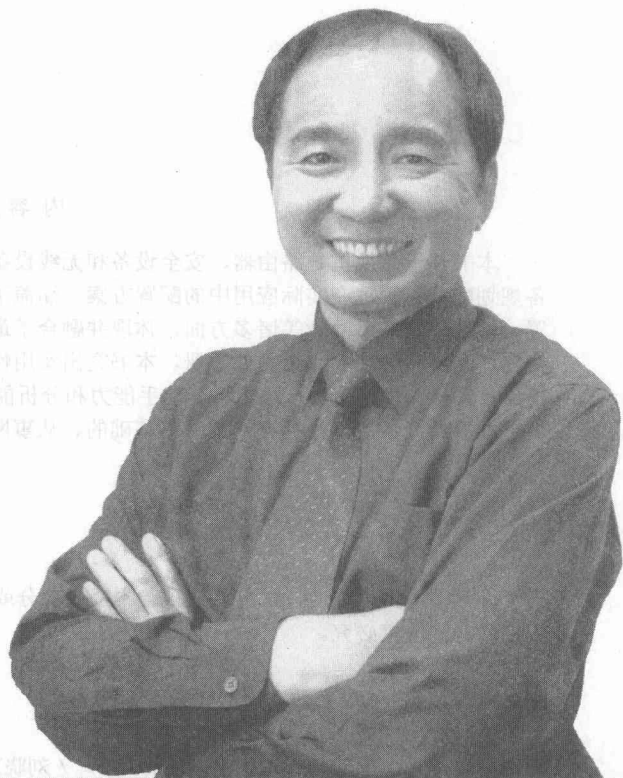
# 网络设备 规划、配置与管理 大全 (Cisco版)



随书含一张演示光盘，涵盖了书中所有重要的操作，  
读者只需根据光盘中的示例操作，即可实现相应的功能。



电子工业出版社  
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY  
<http://www.phei.com.cn>



# 网络设备 规划、配置与管理 大全 (Cisco版)



刘晓辉 编著

电子工业出版社

Publishing House of Electronics Industry

北京·BEIJING

## 内 容 简 介

本书基于交换机、路由器、安全设备和无线设备的规划配置及管理等方面内容,全面阐述了网络设备规划配置与管理在实际应用中的配置方案,涵盖了原理、参数、分类、适用、规划、接口、连接、配置、管理、监控及故障等诸多方面,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、配置和管理的完全硬件手册。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,注重培养动手能力和分析能力。

本书的读者定位为拥有一定网络基础的、从事网络或相关工作的人员,以及准备从事网络管理工作的大、中专学生。

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

### 图书在版编目(CIP)数据

网络设备规划、配置与管理大全(Cisco版)/刘晓辉编著. —北京:电子工业出版社,2009.3  
(网管宝典)  
ISBN 978-7-121-08000-5

I. 网… II. 刘… III. 计算机网络—设备管理 IV. TP393

中国版本图书馆CIP数据核字(2008)第199776号

责任编辑:朱沐红

印 刷:北京京科印刷有限公司

装 订:三河市皇庄路通装订厂

出版发行:电子工业出版社

北京市海淀区万寿路173信箱 邮编100036

开 本:850×1168 1/16 印张:43 字数:1210千字

印 次:2009年3月第1次印刷

印 数:3500册 定价:79.00元(含光盘1张)

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

质量投诉请发邮件至 zltz@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

构建大中型局域网的常用设备包括交换机、路由器、安全设备和无线设备，它们可以称得上是网络构建的四大支柱，或者称为网络世界的四大金刚。只要掌握了这四类设备的功能、选择、连接、配置、管理和排障，也就等于掌握了全面的网络构建技术，同时，就可以称得上是一位名副其实的网络管理员。

交换机负责连接各种网络设备（如交换机、路由器、无线 AP 和网络防火墙等）和网络终端（如计算机、服务器、网络摄像头和网络打印机等），用于构建各种类型和规模的局域网。若没有交换机，则计算机与网络设备之间就无法通信，也就不能搭建局域网，因此，交换机是网络构建的基础，没有交换机就没有局域网。同时，交换机的性能还从根本上决定着整个局域网的连接带宽和传输效率。

路由器则是不同网络之间的桥梁，用于实现局域网之间以及局域网与 Internet 之间的互联。若没有路由器，则局域网就会与外部网络完全隔离，即成为一座信息孤岛，因此可以形象地认为，网络对路由器的渴望不亚于岛民对跨海大桥的期盼。

安全设备通过一定的规则和限制来保证网络安全，是实现局域网内部安全的重要保障。没有安全设备保护的局域网，将时刻面临来自整个虚拟世界攻击的威胁，个人隐私和商业机密都将荡然无存。

无线网络用于实现移动用户的灵活接入，在无线信号覆盖的区域内，无论用户位于何处，都可以实现类似手机的无线漫游，只要笔记本电脑在手就可以随时随地上网，从而摆脱了网络线缆的束缚和羁绊。

可见，交换机、路由器、安全设备和无线设备各司其职、相互结合、彼此补充、缺一不可。

## 本书特点



- 网络设备最全。涵盖用于构建网络的所有硬件设备——交换机、路由器、安全设备和无线设备。
- 硬件设备最新。不仅介绍最新的网络硬件设备，同时兼容仍在使用的网络产品，从而保证最大范围的读者群。
- 配置方式简单。除了介绍传统的 CLI 配置方式外，还介绍了基于图形界面的配置管理软件（Cisco CNA、Cisco SDM 和 Cisco ASDM），以及简单易用的 Web 配置方式。
- 任务驱动。将相关的配置内容整合在一起，从而更加简洁、易懂和实用，摒弃技术文档式的配置方式介绍。
- 突出实用性、针对性和技术性，紧贴局域网搭建实践。
- 大量的经验、技巧、提示和注意，帮助读者避开各种危险的陷阱，迅速提高读者的技术水平。

## 本书适合读者



- 行政机关、企事业单位中正在从事网络管理工作的网络管理员。
- 见习期或试用期的准网络管理员。
- 网吧管理员和机房管理员。



- 网络工程、信息安全技术、计算机网络技术和网络系统管理等网络相关专业的大、中专院校学生。
- 计算机培训学校网络专业的学生。

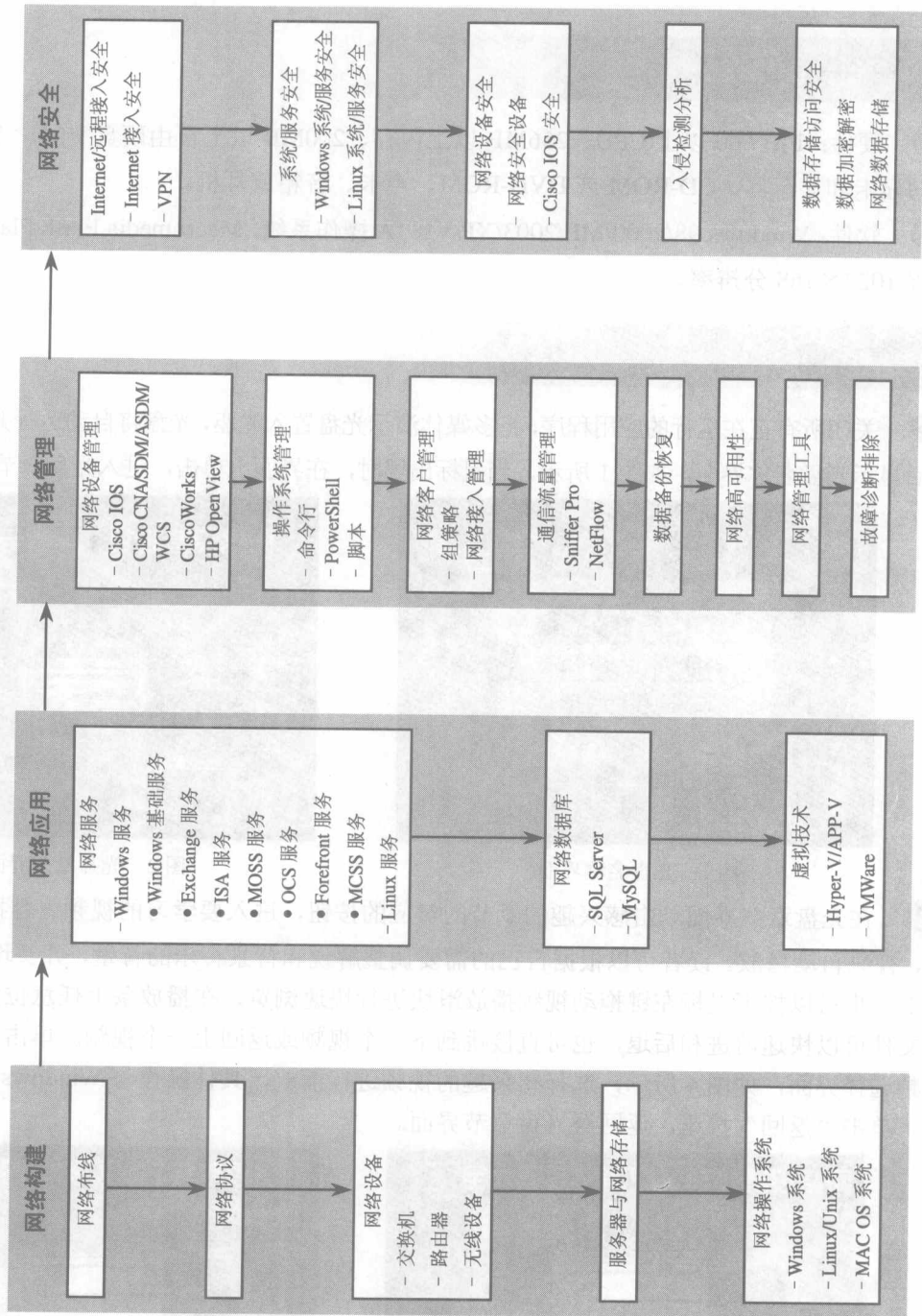
本书主要由刘晓辉编写，李寅、刘国增、李海宁、金素梅、刘淑梅、赵卫东、马倩、杨伏龙、李文俊、王同明、石长征、郭腾、白华、莫展宏、陈志成、田俊乐、王延杰、刘红、王淑江、王春海等也参与了部分章节的编写工作。笔者长期从事网络教学、实验和管理工 作，规划、设计、论证、实施、验收过多个大中型网络建设项目，具有较高的理论水平和丰富的实践经验，曾经出版过三十余部计算机类图书，均以易读、易学、实用的特点受到广大读者的一致好评。本书是笔者的又一呕心沥血之作，希望能对大家的网络搭建、管理工作有所帮助。

笔 者  
2008 年 10 月



# 网管宝典学习路线图

笔者就自己对网络管理体系的理解，对网络管理学习者给出一个粗略线路图：





# 光盘说明

## 软硬件需要

硬件：PIII 500 以上 CPU、256MB 以上内存、200MB 以上自由硬盘空间、支持 1024×768 分辨率的显卡和显示器、CD-ROM 或 DVD-ROM、声卡、音箱或耳机。

软件：Windows 98/2000/ME/2003/XP/VISTA 操作系统，Macromedia Flash Player 6.0 以上播放器、设置 1024×768 分辨率。

## 操作指南

关闭所有正在运行的应用程序，将多媒体演示光盘置入光驱，光盘将自动运行并播放宣传片头动画，然后显示光盘名称界面，如图 1 所示，当鼠标出现时，在界面上单击，进入光盘章节界面，如图 2 所示。

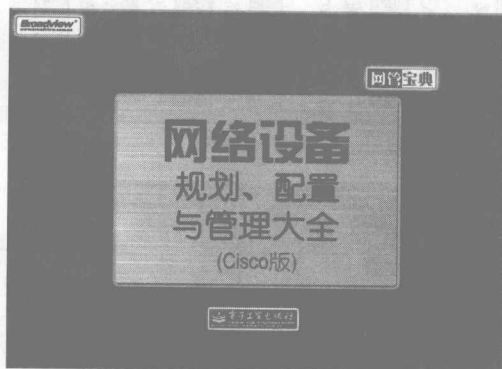


图 1 光盘名称界面



图 2 光盘章节界面

在光盘章节界面单击感兴趣的章节的对应的按钮，进入要学习的视频内容播放界面，如图 3 所示，视频自动播放。读者可以根据自己的需要调整解说和背景音乐的音量，并实现播放的暂停、快进、快退，也可以按下鼠标左键拖动视频播放滑块进行快速浏览，在播放条上任意位置单击鼠标左键，视频文件可以快速前进和后退，也可直接跳到下一个视频或返回上一个视频。单击视频选择按钮，弹出视频选择界面，如图 4 所示，选择感兴趣的视频进行播放，具体操作与 Windows Media Player 非常相似。单击“返回”按钮，返回至光盘章节界面。

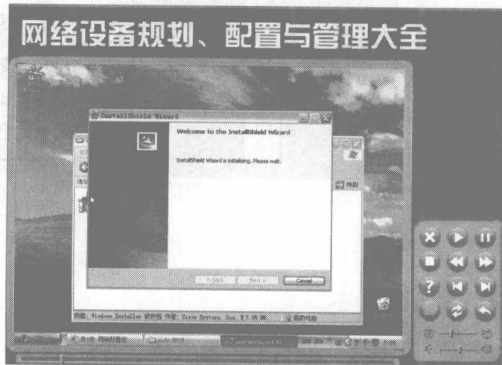



图 3 视频内容播放界面



图 4 视频选择界面

 在光盘章节界面和播放界面中，单击“光盘帮助”按钮，显示光盘使用帮助文件，如图 5 所示。

 单击“退出光盘”按钮，显示光盘的制作团队信息，如图 6 所示，在退出界面上单击鼠标左键将自动结束光盘播放。

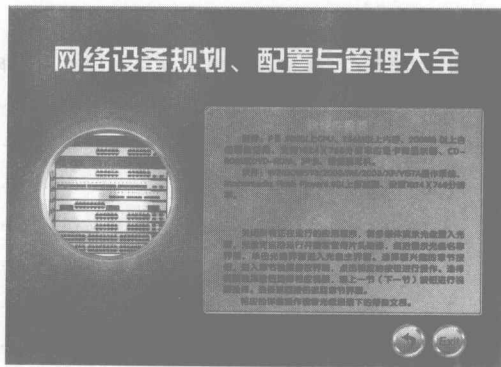


图 5 光盘使用帮助

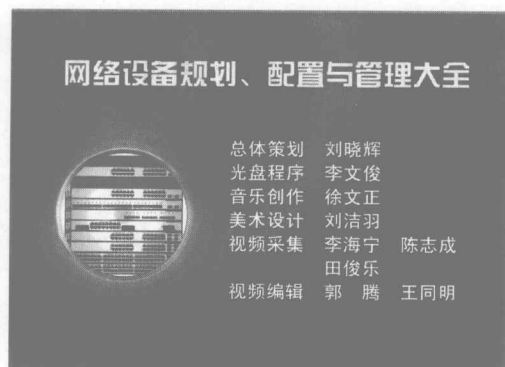


图 6 退出界面

## 第 2 章 网络基础

1.1 网络的发展与分类	1.1
1.2 网络的组成	1.2
1.3 网络的拓扑结构	1.3
1.4 网络的传输介质	1.4
1.5 网络的交换技术	1.5
1.6 网络的接入技术	1.6
1.7 网络的安全技术	1.7
1.8 网络的新技术	1.8
1.9 网络的应用	1.9
1.10 网络的未来	1.10
2.1 网络基础	2.1
2.2 网络基础	2.2
2.3 网络基础	2.3
2.4 网络基础	2.4
2.5 网络基础	2.5
2.6 网络基础	2.6
2.7 网络基础	2.7
2.8 网络基础	2.8
2.9 网络基础	2.9
2.10 网络基础	2.10
2.11 网络基础	2.11
2.12 网络基础	2.12
2.13 网络基础	2.13
2.14 网络基础	2.14
2.15 网络基础	2.15
2.16 网络基础	2.16
2.17 网络基础	2.17
2.18 网络基础	2.18
2.19 网络基础	2.19
2.20 网络基础	2.20



# 目 录

## 第 1 部分 概述

第 1 章 网络设备综述	1
1.1 网络设备简介	1
1.1.1 交换机简介	1
1.1.2 路由器简介	1
1.1.3 安全设备简介	2
1.1.4 无线设备简介	2
1.2 网络设备在网络中的应用	2
1.2.1 交换机在网络中的应用	3
1.2.2 路由器在网络中的应用	4
1.2.3 网络安全设备在网络中的应用	5
1.2.4 无线网络设备在网络中的应用	6

## 第 2 部分 交换机

第 2 章 交换机概述	8
2.1 交换机概述	8
2.1.1 交换机的功能	8
2.1.2 交换机与交换式网络	9
2.1.3 交换机的工作原理	10
2.2 交换机技术	11
2.2.1 高速链路技术	11
2.2.2 冗余链路技术	14
2.2.3 虚拟局域网技术	17
2.2.4 多层交换技术	20
2.2.5 路由冗余技术	22
2.2.6 端口传输控制技术	24
2.2.7 VoIP 技术	25
2.3 交换机的分类	26
2.3.1 智能交换机与傻瓜交换机	26
2.3.2 固定端口交换机与模板化交换机	27
2.3.3 接入层交换机、汇聚层交换机 与核心层交换机	28
2.3.4 以太网交换机与 ATM 交换机	29
2.3.5 二层交换机与三层交换机	29

2.3.6 快速以太网交换机、千兆以太网 交换机与万兆以太网交换机	30
2.3.7 对称交换机与非对称交换机	31
2.4 交换机的主要参数	31
2.4.1 三层交换机的主要参数	32
2.4.2 二层交换机的主要参数	34
2.5 交换机的选择策略	37
2.5.1 核心交换机的选择	38
2.5.2 汇聚层交换机的选择	41
2.5.3 接入层交换机的选择	42
2.5.4 可网管交换机的选购	43

## 第 3 章 交换机的端口与连接

3.1 IEEE 802.3 系列标准	46
3.1.1 IEEE 802.3 标准	46
3.1.2 IEEE 802.3u 标准	46
3.1.3 IEEE 802.3z 和 802.3ab 标准	47
3.1.4 IEEE 802.3ae、802.3ak 和 802.3an 标准	49
3.2 交换机端口类型	51
3.2.1 光纤端口	51
3.2.2 双绞线端口	52
3.2.3 GBIC 模块与插槽	53
3.2.4 SFP 模块与插槽	54
3.2.5 10GE 模块与插槽	54
3.2.6 复用端口	55
3.2.7 TwinGig 转换模块	55
3.3 跳线类型与适用	55
3.3.1 双绞线跳线	56
3.3.2 光纤跳线	56
3.3.3 光纤跳线与光纤端口	58
3.4 交换机的连接策略	58
3.4.1 不同性能交换机的连接策略	58
3.4.2 不对称交换机的连接策略	59
3.4.3 对称交换机的连接策略	60
3.5 交换机的级联	60

3.5.1	光纤端口的连接	60	5.5.1	监控交换机端口状态	103
3.5.2	双绞线端口的连接	62	5.5.2	查看数据统计资料	103
3.5.3	远程交换机的连接	64	5.5.3	查看系统资源和事件	104
3.6	交换机的堆叠	65	5.5.4	发现交换机故障	104
3.6.1	堆叠与级联	65	5.6	配置交换机	105
3.6.2	GBIC/SFP 堆叠	66	5.6.1	设置端口属性	105
3.6.3	StackWise 堆叠	67	5.6.2	设置端口角色	106
3.7	连接状态判断与链路测试	69	5.6.3	设置 EtherChannel	106
3.7.1	交换机工作状态判断	70	5.6.4	设置 VLAN	107
3.7.2	网络链路连通性测试	72	5.6.5	配置受保护端口	109
第 4 章	使用 Web 配置和管理交换机	76	5.6.6	泛洪控制	109
4.1	配置前的准备	76	5.6.7	配置 SPAN 端口	110
4.1.1	交换机 Web 配置的特点	76	5.7	维护交换机	111
4.1.2	配置前的准备工作	76	5.7.1	配置文件的备份与恢复	111
4.2	配置交换机	77	5.7.2	升级系统映像	111
4.2.1	设置端口属性	77	第 6 章	CLI 与交换机基本配置	114
4.2.2	设置端口角色	79	6.1	CLI 命令行及使用	114
4.2.3	快速配置交换机	80	6.1.1	CLI 方式的适用	114
4.3	监控交换机	81	6.1.2	CLI 命令模式	114
4.3.1	查看交换机端口状态	81	6.1.3	使用帮助	116
4.3.2	查看数据统计资料	82	6.1.4	命令的简略方式	117
4.3.3	查看端口健康状态和可用性	84	6.1.5	使用 no 命令	118
4.4	管理交换机	85	6.1.6	命令行出错信息	118
4.4.1	重新启动交换机	85	6.1.7	命令行约定	118
4.4.2	更新系统映像文件	85	6.1.8	指定端口、VLAN、MAC 和 IP	119
第 5 章	使用 CNA 配置和管理交换机	87	6.2	交换机基本配置	120
5.1	交换机配置前的准备	87	6.2.1	交换机初始化配置	120
5.1.1	交换机的管理方式	87	6.2.2	配置 SNMP	122
5.1.2	交换机配置前的规划	92	6.2.3	配置端口属性	122
5.2	交换机的初始配置	93	6.2.4	配置智能端口	125
5.2.1	配置前的准备	93	6.3	配置 DHCP 中继	125
5.2.2	运行快速设置	94	6.3.1	DHCP 中继代理概述	126
5.2.3	为 CNA 准备 Catalyst 4500 交换机	95	6.3.2	DHCP 配置策略	126
5.3	CNA 简介	98	6.3.3	配置 DHCP 中继代理	127
5.3.1	CNA 可管理的设备	98	6.3.4	指定包转发地址	128
5.3.2	CNA 视图	98	6.3.5	启用 DHCP 侦听	129
5.3.3	团体和集群	99	6.3.6	在私有 VLAN 中启用 DHCP 侦听	130
5.4	添加交换机	100	6.3.7	启用 DHCP 侦听绑定数据库 代理	130
5.4.1	手动添加交换机	100	6.3.8	配置 IP 源地址保护	131
5.4.2	自动发现交换机	102	6.4	配置 CDP	132
5.5	监控交换机	103	6.4.1	CDP 概述	132

6.4.2	CDP 配置	133	8.5.3	配置 UDLD	182
<b>第 7 章</b>	<b>交换机 VLAN 与 VTP 配置</b>	<b>135</b>	<b>第 9 章</b>	<b>交换机 IP 路由配置</b>	<b>184</b>
7.1	配置 VTP	135	9.1	IP 路由概述	184
7.1.1	VTP 简介	135	9.1.1	IP 路由由分类	184
7.1.2	VTP 配置	137	9.1.2	IP 路由由配置步骤	184
7.2	配置 VLAN	140	9.1.3	IP 地址默认配置	185
7.2.1	VLAN 配置策略	140	9.2	配置三层接口	185
7.2.2	配置 VLAN	140	9.2.1	配置逻辑三层接口	186
7.2.3	配置 VLAN Trunk	143	9.2.2	配置物理三层接口	187
7.3	配置 PVLAN	145	9.2.3	配置三层 EtherChannel	188
7.3.1	PVLAN 概述	145	9.3	配置静态 IP 路由	190
7.3.2	配置 PVLAN	147	9.3.1	启用 IP 单播路由	190
7.4	配置 VMPS	150	9.3.2	设置默认网关	191
7.4.1	客户端交换机配置	151	9.3.3	设置静态路由	191
7.4.2	VMPS 服务器配置	152	9.4	其他基本路由设置	196
<b>第 8 章</b>	<b>交换机冗余连接配置</b>	<b>156</b>	9.4.1	使用零位子网	196
8.1	扩展树	156	9.4.2	配置 Cisco 快速转发	196
8.1.1	Spanning-Tree 简介	156	9.5	动态 IP 路由	197
8.1.2	STP 配置	159	<b>第 10 章</b>	<b>交换机安全配置</b>	<b>198</b>
8.1.3	配置 MSTP	161	10.1	配置基于端口的传输控制	198
8.1.4	配置 Trunk 端口负载均衡	164	10.1.1	配置端口属性	198
8.1.5	配置 PostFast 端口	167	10.1.2	广播风暴控制	200
8.1.6	配置 UplinkFast 端口	169	10.1.3	端口流量控制	202
8.2	柔性链路	169	10.1.4	端口带宽限制	202
8.2.1	Flex Links 概述	170	10.1.5	保护端口	203
8.2.2	Flex Links 配置策略	170	10.1.6	端口阻塞	204
8.2.3	配置 Flex Links	170	10.2	配置端口安全	204
8.3	端口汇聚	171	10.2.1	配置安全端口	205
8.3.1	EtherChannel 配置策略	172	10.2.2	设置端口安全老化	206
8.3.2	EtherChannel 端口模式	172	10.3	配置 IEEE 802.1x	206
8.3.3	创建 EtherChannel	174	10.3.1	IEEE 802.1x 简介	206
8.3.4	配置 EtherChannel 负载均衡	174	10.3.2	启用 IEEE 802.1x 认证	207
8.3.5	从 EtherChannel 中移除接口	175	10.3.3	配置交换机到 RADIUS 服务器的通信	208
8.3.6	移除 EtherChannel	175	10.3.4	配置重新认证周期	209
8.4	热备份路由	176	10.3.5	修改安静周期	209
8.4.1	HSRP 和 MHSRP 概述	176	10.4	配置动态 ARP 检查	210
8.4.2	HSRP 配置策略	178	10.4.1	配置动态 ARP 检查	210
8.4.3	配置 HSRP	178	10.4.2	显示动态 ARP 检查信息	214
8.4.4	配置 MHSRP	180	10.5	配置访问列表	215
8.5	单向链路检测	181	10.5.1	访问列表概述	215
8.5.1	UDLD 的默认配置	181	10.5.2	创建并应用 IP 访问列表	217
8.5.2	UDLD 的配置方针	182			

10.5.3	创建并应用端口访问列表	222
10.5.4	创建并应用 VLAN 访问列表	222
10.6	单向链路检测	224
10.6.1	UDLD 默认配置	224
10.6.2	UDLD 配置原则	225
10.6.3	配置 UDLD	225
<b>第 11 章</b>	<b>交换机日志与监控配置</b>	<b>227</b>
11.1	配置系统日志	227
11.1.1	系统日志概述	227
11.1.2	系统日志配置	227
11.2	配置 SPAN/RSPAN	234
11.2.1	SPAN 和 RSPAN 概述	234
11.2.2	SPAN 和 RSPAN 默认配置	236
11.2.3	配置本地 SPAN	236
11.2.4	配置 RSPAN	239

## 第 3 部分 路由器

<b>第 12 章</b>	<b>路由器概述</b>	<b>244</b>
12.1	路由器概述	244
12.1.1	路由器的功能	244
12.1.2	路由器的工作原理	246
12.2	路由器的分类与适用	247
12.2.1	按性能划分	247
12.2.2	按结构划分	248
12.2.3	按网络位置划分	248
12.2.4	按功能划分	248
12.2.5	按传输性能划分	249
12.2.6	按网络类型划分	249
12.3	路由协议	249
12.3.1	静态路由	249
12.3.2	RIP 路由协议	250
12.3.3	OSPF 路由协议	252
12.3.4	BGP 路由协议	255
12.3.5	IS-IS 路由协议	257
12.3.6	EIGRP 路由协议	258
<b>第 13 章</b>	<b>路由器的端口与连接</b>	<b>261</b>
13.1	路由器接口	261
13.1.1	局域网接口	261
13.1.2	广域网接口	263
13.1.3	路由器配置接口	264
13.2	路由器的连接	265

13.2.1	路由器连接策略	265
13.2.2	路由器面板	266
13.2.3	路由器连接	267
13.3	路由器的连接测试	270
13.3.1	Show 命令判断	270
13.3.2	LED 指示灯判断	270
<b>第 14 章</b>	<b>使用 SDM 配置路由器</b>	<b>273</b>
14.1	路由器初始化配置	273
14.2	Cisco SDM 概述	275
14.2.1	Cisco SDM 简介	275
14.2.2	Cisco SDM 应用	278
14.2.3	Cisco 路由器准备	279
14.2.4	Cisco SDM 安装配置	280
14.3	配置路由器	286
14.3.1	配置 LAN 和 WAN 连接	286
14.3.2	创建防火墙	288
14.3.3	配置 VPN、Easy VPN 和 DMVPN 连接	289
14.3.4	安全审计及安全设置	291
14.3.5	配置基本路由	294
14.3.6	创建“网络地址转换”(NAT) 规则	295
14.3.7	创建服务质量(QoS) 策略	298
14.4	管理路由器	300
14.4.1	监视路由器的状态	300
14.4.2	监视路由器端口的状态	302
14.4.3	查看路由器的日志	305
<b>第 15 章</b>	<b>使用 CLI 配置路由器</b>	<b>308</b>
15.1	路由器基本配置	308
15.1.1	路由器端口编号	308
15.1.2	IP 协议配置原则	313
15.1.3	配置主机名和密码	315
15.1.4	配置快速以太网接口	316
15.1.5	配置同步串行接口	316
15.2	配置广域网接口	317
15.2.1	接口的一般配置	317
15.2.2	同步串口配置	319
15.3	配置逻辑接口	321
15.3.1	Loopback 接口配置	321
15.3.2	NULL 接口配置	321
15.3.3	Tunnel 接口配置	322
15.3.4	Dialer 接口配置	323



15.3.5	子接口配置	324
15.4	配置 PPP 和 MP 协议	325
15.4.1	PPP 和 MP 协议概述	325
15.4.2	PPP 协议的配置	326
15.4.3	MP 协议的配置	328
15.4.4	PPP 的监控	329
15.5	配置 HDLC 协议	330
15.5.1	HDLC 协议概述	330
15.5.2	HDLC 配置	331
15.6	配置帧中继协议	331
15.6.1	帧中继概述	331
15.6.2	帧中继的基本配置	333
15.6.3	帧中继子接口配置	336
15.6.4	帧中继的高级配置	337
15.6.5	帧中继监控和维护	338
15.7	配置 LAPB 和 X.25 协议	338
15.7.1	LAPB、X.25 协议概述	339
15.7.2	配置 LAPB 协议	339
15.7.3	配置 X.25 协议	340
15.7.4	配置 X.25 高级功能	345
15.7.5	显示 X.25 接口信息	347
15.8	网络地址转换	347
15.8.1	理解 NAT	347
15.8.2	静态地址转换的实现	348
15.8.3	动态地址转换的实现	349
15.8.4	端口复用地址转换	351
15.9	配置静态路由	352
15.9.1	配置静态路由	352
15.9.2	LAN 方式接入 Internet	353
15.9.3	DDN 接入 Internet	354
<b>第 16 章</b>	<b>IP 动态路由配置</b>	<b>355</b>
16.1	配置 EIGRP	355
16.1.1	默认的 EIGRP 配置	355
16.1.2	配置基本 EIGRP 参数	356
16.1.3	配置 EIGRP 接口	356
16.1.4	配置 EIGRP 路由认证	357
16.1.5	查看 EIGRP 相关信息	358
16.2	配置 RIP	358
16.2.1	RIP 的默认配置	359
16.2.2	配置 RIP 路由	359
16.2.3	配置 RIP 认证	361
16.2.4	配置水平分割	361
16.3	配置 OSPF	362

16.3.1	默认的 OSPF 配置	362
16.3.2	配置基本 OSPF 参数	363
16.3.3	配置 OSPF 接口	364
16.3.4	配置 OSPF 区域参数	365
16.3.5	配置其他 OSPF 参数	366
16.3.6	配置 Loopback 接口	367
16.3.7	查看 OSPF 相关信息	367
<b>第 17 章</b>	<b>QoS 配置</b>	<b>369</b>
17.1	QoS 概述	369
17.2	配置 QoS	370
17.2.1	Auto-QoS 配置简介	370
17.2.2	Auto-QoS 配置注意事项	371
17.2.3	配置 Auto-QoS	372

## 第 4 部分 安全设备

<b>第 18 章</b>	<b>网络安全设备概述</b>	<b>376</b>
18.1	防火墙	376
18.1.1	网络防火墙简介	376
18.1.2	防火墙的主要功能	377
18.1.3	防火墙的局限性与脆弱性	378
18.1.4	防火墙的分类与适用	379
18.2	IDS	387
18.2.1	IDS 概述	387
18.2.2	IDS 优势的缺陷	388
18.2.3	IDS 与防火墙联动	390
18.3	IPS	391
18.3.1	IPS 概述	391
18.3.2	IPS 的技术特征	392
18.3.3	IPS 的分类	393
18.3.4	IPS 的优势与作用	394
18.3.5	IPS 的缺陷	395
18.3.6	部署 IPS	396
18.3.7	IDS 与 IPS 的比较	396
18.4	安全设备的主要参数与选择	398
18.4.1	防火墙的参数与选择	398
18.4.2	IDS 的选择	402
18.4.3	IPS 的参数与选择	402
<b>第 19 章</b>	<b>安全设备的端口与连接</b>	<b>405</b>
19.1	安全设备的端口	405
19.1.1	安全设备的物理端口	405
19.1.2	防火墙逻辑端口	407

19.1.3	安全设备端口的连接	407
19.1.4	安全设备的 LED 指示灯	409
19.2	网络安全设计与连接	411
19.2.1	网络防火墙设计与连接	411
19.2.2	入侵防御系统设计与连接	414
19.2.3	综合安全设计与连接	415
<b>第 20 章</b>	<b>使用 ASDM 配置安全设备</b>	<b>417</b>
20.1	Cisco ASDM 概述	417
20.1.1	Cisco ASDM 简介	417
20.1.2	Cisco ASDM 应用	420
20.1.3	Cisco 安全设备准备	420
20.1.4	Cisco ASDM 安装配置	421
20.2	配置安全设备	423
20.2.1	Cisco ASDM 初始化	424
20.2.2	网络设备集成化管理	424
20.2.3	安全策略设置	425
20.2.4	DMZ 配置	425
20.2.5	IPsec VPN 远程访问配置	431
20.2.6	Site-to-Site VPN 配置	438
20.3	管理安全设备	440
20.3.1	监视安全设备运行状态	441
20.3.2	查看和分析网络流量	441
20.3.3	查看和分析系统日志	443

## 第 5 部分 无线设备

<b>第 21 章</b>	<b>无线网络设备概述</b>	<b>445</b>
21.1	无线局域网标准	445
21.1.1	IEEE 802.11 系统标准	445
21.1.2	IEEE802.16a 标准	449
21.1.3	无线安全标准	449
21.1.4	无线产品兼容性	452
21.2	无线网络组件	454
21.2.1	无线网卡	454
21.2.2	无线 AP	454
21.2.3	无线路由器	456
21.2.4	无线天线	456
21.2.5	无线局域网控制器	456
21.2.6	其他无线设备	457
21.3	无线网络模式特点与适用	457
21.3.1	对等无线网络	457
21.3.2	独立无线网络	458
21.3.3	接入以太网的无线网络	458

21.3.4	无线漫游的无线网络	459
21.3.5	点对点 and 点对多点网络	460
21.4	无线设备的选择	460
21.4.1	无线 AP 的选择	461
21.4.2	无线网桥的选择	463
21.4.3	无线网络控制器的选择	463
21.4.4	无线天线的选择	466
21.4.5	远程供电设备的选择	468
21.5	无线 AP 位置的选择	469
21.5.1	室内无线 AP 位置的选择	469
21.5.2	室外无线 AP 位置的选择	470
21.5.3	漫游网络无线 AP 的选择	471
21.6	无线设备的端口与连接	472
21.6.1	无线网络控制器的连接	472
21.6.2	无线 AP 的端口与连接	473
21.6.3	连接状态判断	474
<b>第 22 章</b>	<b>使用 Web 配置无线网络</b>	<b>477</b>
22.1	无线 AP 基本配置	477
22.1.1	首次配置无线 AP	477
22.1.2	管理无线 AP	481
22.1.3	配置无线设置	483
22.1.4	配置本地认证	483
22.1.5	配置 WLAN	483
22.1.6	配置 QoS	487
22.1.7	配置过滤	488
22.1.8	配置 SNMP	489
22.1.9	配置系统消息日志	490
22.2	无线漫游网络的配置	490
22.2.1	无线 AP 配置规划	490
22.2.2	配置 WDS 服务器	491
22.2.3	配置 WDS 设备	492
22.2.4	无线客户端配置	493
22.3	点对点 and 点对多点网络的配置	495
22.3.1	点对点网络配置	495
22.3.2	点对多点网络配置	498
<b>第 23 章</b>	<b>配置无线网络控制器</b>	<b>499</b>
23.1	配置端口和接口	499
23.1.1	无线网络控制器的接口	499
23.1.2	配置接口属性	500
23.1.3	配置 LAG 端口	500
23.2	配置控制器设置	502
23.2.1	修改 SNMP 字符串	502

23.2.2	启用系统日志	502	25.2.8	引擎故障	558
23.2.3	配置客户漫游参数	503	25.2.9	线卡故障	559
23.3	配置安全方案	503	25.2.10	系统故障	560
23.3.1	配置 TACACS+	504	25.2.11	配置错误	561
23.3.2	配置本地用户	505	25.3	路由器故障	562
23.3.3	配置 LDAP	506	25.3.1	路由器一般故障	562
23.3.4	配置本地 EAP	506	25.3.2	路由器故障诊断	566
23.3.5	配置访问列表	508	25.3.3	路由器崩溃和挂起	567
23.3.6	配置 IDS 传感器	510	25.3.4	路由器接口故障	579
23.3.7	上传/下载 IDS 签名	510	25.4	无线网络故障	582
23.3.8	禁用/启用 IDS 签名	511	25.4.1	无线桥接网络故障	582
23.3.9	查看 IDS 签名事件	511	25.4.2	无线 AP 连接故障	588
23.4	无线资源管理	512	第 26 章	经济型千兆以太网方案	592
23.4.1	配置 RF 组	512	26.1	网络拓扑与设备选购方案	592
23.4.2	发现流氓 AP	513	26.1.1	网络需求调查	592
23.4.3	配置静态传输信道和传输功率	514	26.1.2	网络拓扑结构	592
23.4.4	配置 CCX 无线管理	515	26.1.3	网络技术设计	593
23.5	配置轻型无线 AP	515	26.1.4	网络设备选择	594
第 24 章	网络设备统一管理	517	26.2	网络设备配置方案	597
24.1	系统和配置文件的管理	517	26.2.1	IP 地址和 VLAN 规划	597
24.1.1	TFTP 服务器	517	26.2.2	汇聚交换机配置	598
24.1.2	配置文件的备份与还原	518	26.2.3	独立接入交换机的配置	608
24.1.3	映像文件的备份、还原与升级	519	26.2.4	核心交换机的配置	612
24.2	密码丢失后的恢复	520	26.2.5	路由器配置	618
24.2.1	密码的类型	520	26.3	千兆以太网升级方案	621
24.2.2	密码丢失后的恢复	520	26.3.1	可用性升级方案	621
24.3	CiscoWorks	523	26.3.2	安全性升级方案	623
24.3.1	安装系统需求	524	第 27 章	豪华型万兆以太网方案	625
24.3.2	安装 CiscoWorks 2000	524	27.1	网络拓扑与设备选购方案	625
24.3.3	查看被管设备	531	27.1.1	网络需求调查	625
24.3.4	网络设备拓扑服务	535	27.1.2	网络拓扑结构	625
第 25 章	网络设备故障	543	27.1.3	网络技术设计	628
25.1	网络故障概述	543	27.1.4	网络设备选择	629
25.1.1	网络故障主要原因与现象	543	27.2	网络设备配置方案	636
25.1.2	网络故障排除过程	544	27.2.1	IP 地址和 VLAN 规划	636
25.2	交换机故障诊断	546	27.2.2	核心交换机的配置	637
25.2.1	交换机故障诊断方法	546	27.2.3	路由器配置	654
25.2.2	交换机故障诊断顺序	547	27.2.4	防火墙配置	660
25.2.3	电源故障	549	27.3	万兆以太网升级方案	664
25.2.4	端口故障	551	27.3.1	无线网络升级方案	665
25.2.5	接口故障	552	27.3.2	安全升级方案	667
25.2.6	GBIC/SFP 故障	556	27.3.3	服务器群集设计	670
25.2.7	背板故障	557			

# 第 1 章 网络设备综述

常见的网络设备包括交换机、路由器、安全设备和无线设备。其中，交换机和路由器是几乎所有局域网都要使用的基本设备。交换机将其他网络设备（如集线器、交换机和路由器等）和所有终端设备（如计算机、服务器和网络打印机等）连接在一起，实现彼此之间的通信；路由器用于实现局域网之间以及局域网与 Internet 之间的互联；安全设备则用于监控和保护内部网络的安全；无线设备是有线网络的补充，用于实现无线漫游和无线接入等重要业务。

## 1.1 网络设备简介

就像计算机中不同的板卡分别拥有不同的功能一样，网络设备也在网络中分别扮演着不同的角色。因此，只有清楚它们各自的功能和用途后，才能根据网络建设的实际需要选择相应的设备。

### 1.1.1 交换机简介

交换机（Switch）是集线器的换代产品，其作用也是将作为传输介质的线缆汇聚在一起，以实现计算机之间的连接。所不同的是，交换机能够为网络提供更高的传输速率。如图 1-1 所示为 Cisco Catalyst 3750 系列交换机。

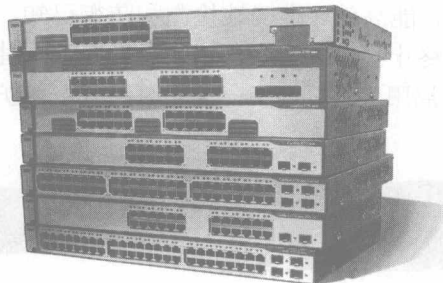


图 1-1 Cisco Catalyst 3750 系列交换机

虽然交换机与集线器外表相似，但两者的工作原理截然不同。交换机的传输方式和集线器不同，所有端口间都建立有信号通道，任何两个端口之间的计算机都可以随时通信，从而使得网络的传输速率大大提高。由于制造成本的原因，交换机的价格也比集线器略高一些。

交换机是目前应用最为广泛的网络集线设备，在大型网络中，还可以利用交换机的 VLAN 功能划分广播域，从而减少广播风暴对整个网络带来的负面影响。

### 1.1.2 路由器简介

路由器其实就是一种特殊的计算机，主要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。如图 1-2 所示为 Cisco 2800 系列路由器。

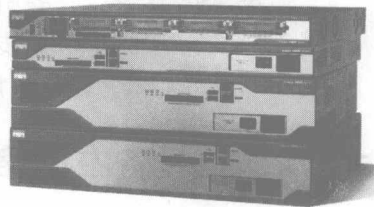


图 1-2 Cisco 2800 系列路由器



### 1.1.3 安全设备简介

安全设备包括防火墙、IDS 和 IPS，这 3 种安全设备分布在不同的位置，可以为网络设备或网络分支提供全方位的安全保护。

#### 1. 防火墙

“防火墙”(Fire Wall)的本意是指发生火灾时，用来防止火势蔓延的一道障碍物，一般都修筑在建筑物之间。网络防火墙则是指设置在计算机网络之间的一道隔离装置，可以隔离两个或者多个网络，限制网络互访，以保护内部网络用户和数据的安全。如图 1-3 所示为 Cisco 防火墙。

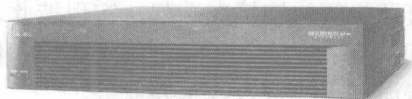


图 1-3 Cisco 防火墙

#### 2. IDS

IDS (Intrusion Detection System, 入侵检测系统)作为一种网络安全的监测设备，可以依照一定的安全策略，对网络、系统的运行状况进行监视，及时发现各种攻击企图、攻击行为或攻击结果，以保证网络系统资源的安全。如图 1-4 所示为 Cisco IDS 设备。

#### 3. IPS

IPS (Intrusion Prevention System, 入侵防御系统)的设计基于一种全新的思想和体系架构，它工作于串联 (In-Line) 方式，采用 ASIC、FPGA 或 NP (网络处理器) 等硬件设计技术实现网络数据流的捕获。检测引擎综合特征检测、异常检测、DoS 检测、缓冲区溢出检测等多种手段，并使用硬件加速技术进行深层数据包分析处理，能高效、准确地检测和防御已知、未知的攻击及 DoS 攻击，并实施多种响应方式，如丢弃数据包、终止会话、修改防火墙策略、实时生成警报和日志记录等，突破了传统 IDS 只能检测不能防御入侵的局限性，提供了一个完整的入侵防护解决方案。如图 1-5 所示为 Cisco IPS 设备。

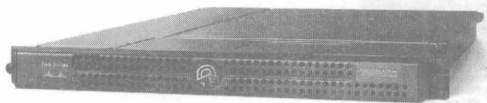


图 1-4 Cisco IDS 设备

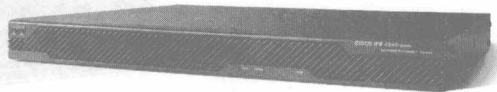


图 1-5 Cisco IPS 设备

### 1.1.4 无线设备简介

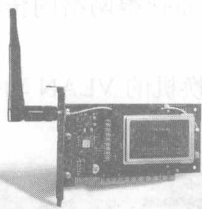


图 1-6 PCI 接口无线网卡

搭建无线局域网所需的硬件设备非常简单，主要包括无线网卡、无线 AP、无线路由器和无线天线 4 种。其中无线网卡是必需的设备，而其他的组件则可以根据不同的网络环境选择使用。例如，无线网与以太网连接时就要用到无线 AP，无线局域网接入 Internet 时就要用到无线路由器，接收远距离传输的无线信号或者需要扩展网络覆盖范围时，就要用到无线天线。如图 1-6 所示为常见的 PCI 接口无线网卡，适用于普通的台式计算机。

## 1.2 网络设备在网络中的应用

交换机、路由器和防火墙作为最基本的网络设备，被广泛应用于各种规模的局域网络。其中，交换机作为必不可少的网络设备，将计算机和其他所有网络设备连接在一起。路由器用于实现 Internet