

网络设备

第2版

规划、配置与管理大全 (Cisco版)

刘晓辉 编著



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。



网络设备 第2版

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

本书从交换机、路由器、安全设备、无线设备、服务器到网络存储的规划配置及管理,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、从事网络或相关工作的技术人员,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. —2 版. —北京: 电子工业出版社, 2012.10
ISBN 978-7-121-17950-1

I. ①网… II. ①刘… III. ①计算机网络—通信设备—设备管理 IV. ①TN915.05

中国版本图书馆 CIP 数据核字 (2012) 第 194275 号

策划编辑: 符隆美

责任编辑: 葛 娜

特约编辑: 赵树刚

印 刷: 北京市京科印刷有限公司

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: 50.25 字数: 1287 千字

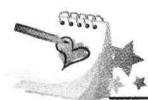
印 次: 2012 年 10 月第 1 次印刷

印 数: 3500 册 定价: 105.00 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不外乎交换机、路由器、安全设备和无线设备，它们称得上是网络构建的四大支柱。只要掌握了这四类设备的功能、选择、连接、配置、管理和排障，也就掌握了全面的网络构建技术，你就能成为一个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。没有交换机，计算机及网络设备之间就无法通信，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及局域网与 Internet 之间的互连。没有路由器，局域网就会与外部网络完全隔离，就是一座信息孤岛，因此，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，就好像任人宰割的羊群，将时刻遭受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，无论用户走到哪里，都可以实现无线漫游，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

第一，网络设备最全。涵盖了用于构建网络的所有硬件设备——交换机、路由器、安全设备、无线设备、服务器和网络存储设备。

第二，硬件设备最新。不仅介绍了最新的网络硬件设备，同时兼容仍在使用的网络产品，从而保证适合最大范围的读者群。

第三，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 CP 和 Cisco ASDM），以及简单易用的 Web 配置方式。

第四，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。

第五，突出实用性、针对性和技术性，紧贴局域网络搭建实践。

第六，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。

本书读者

本书适合以下读者朋友：

- 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专院校学生。
- 计算机培训学校网络专业的学生。

本书由刘晓辉编著，张瑞生、田俊乐、李海宁、陈志成、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、刘媛、张栋、黄成、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，受到众多读者的一致好评。本书是笔者的又一呕心沥血之作，希望能对读者的网络搭建、管理工作有所帮助。

笔者

目 录

第 1 章 网络设备综述	1	2.3.7 对称交换机与非对称交换机	36
1.1 网络设备简介	1	2.3.8 桌面交换机与机架式交换机	37
1.1.1 交换机简介	1	2.3.9 特殊用途交换机	38
1.1.2 路由器简介	1	2.4 交换机的主要参数	39
1.1.3 安全设备简介	2	2.4.1 三层交换机的主要参数	39
1.1.4 无线设备简介	2	2.4.2 二层交换机的主要参数	42
1.2 网络设备在网络中的应用	3	2.5 交换机的选择策略	45
1.2.1 交换机在网络中的应用	3	2.5.1 核心交换机的选择	46
1.2.2 路由器在网络中的应用	5	2.5.2 汇聚层交换机的选择	49
1.2.3 网络安全设备在网络中的应用	7	2.5.3 接入层交换机的选择	50
1.2.4 无线网络设备在网络中的应用	8	2.5.4 可网管交换机的选购	51
第 2 章 交换机概述	11	第 3 章 交换机的端口与连接	54
2.1 交换机的功能与工作原理	11	3.1 IEEE 802.3 系列标准	54
2.1.1 交换机的功能	11	3.1.1 IEEE 802.3 标准	54
2.1.2 交换机与交换式网络	13	3.1.2 IEEE 802.3u 标准	54
2.1.3 交换机的工作原理	14	3.1.3 IEEE 802.3z 和 802.3ab 标准	55
2.2 交换机技术	15	3.1.4 IEEE 802.3ae、802.3ak、802.3an 和 802.3aq 标准	57
2.2.1 高速链路技术	16	3.2 交换机端口类型	59
2.2.2 冗余链路技术	19	3.2.1 双绞线端口	60
2.2.3 虚拟局域网技术	21	3.2.2 光纤端口	60
2.2.4 多层交换技术	24	3.2.3 1GE 模块与插槽	61
2.2.5 路由冗余技术	27	3.2.4 10GE 模块与插槽	63
2.2.6 端口传输控制技术	29	3.2.5 复用端口	65
2.2.7 VoIP 技术	30	3.2.6 10GE 转换模块	65
2.3 交换机的分类与适用	31	3.3 跳线类型与适用	66
2.3.1 智能交换机与傻瓜交换机	31	3.3.1 双绞线跳线	66
2.3.2 固定端口交换机与模块化交换机	32	3.3.2 光纤跳线	67
2.3.3 接入层交换机、汇聚层交换机与 核心层交换机	33	3.3.3 光纤跳线与光纤端口	69
2.3.4 以太网交换机与 ATM 交换机	34	3.4 交换机的连接策略	69
2.3.5 二层交换机与多层交换机	34	3.4.1 不同性能交换机的连接策略	70
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	35	3.4.2 非对称交换机的连接策略	70
		3.4.3 对称交换机的连接策略	71
		3.5 交换机的级联	71

3.5.1	光纤端口的连接	72	第 6 章	使用 CNA 配置和管理交换机	136
3.5.2	双绞线端口的连接	73	6.1	Cisco CNA 简介	136
3.5.3	远程交换机的连接	75	6.1.1	Cisco CNA 视图	136
3.6	交换机的堆叠	76	6.1.2	集群和团体	137
3.6.1	堆叠与级联	76	6.2	向 Cisco CNA 添加交换机	138
3.6.2	GBIC/SFP 堆叠	77	6.2.1	为 Cisco CNA 准备交换机	138
3.6.3	StackWise 技术	78	6.2.2	将交换机添加至团体	140
3.6.4	StackWise Plus 技术	81	6.2.3	添加新的设备	143
3.6.5	FlexStack 技术	82	6.2.4	设置网络拓扑图	144
3.7	交换机与布线系统的连接	84	6.3	使用 Cisco CNA 配置交换机	147
3.7.1	交换机与双绞线链路的连接	84	6.3.1	配置端口属性	147
3.7.2	交换机与光纤链路的连接	86	6.3.2	配置端口角色	150
3.8	连接状态判断与链路测试	89	6.3.3	配置 EtherChannel	152
3.8.1	交换机工作状态判断	89	6.3.4	配置 STP	154
3.8.2	网络链路连通性测试	93	6.3.5	配置 VLAN	160
第 4 章	交换机配置方式与初始化	97	6.3.6	配置堆叠	164
4.1	交换机配置前的准备	97	6.3.7	配置 VLAN 路由	166
4.1.1	交换机配置前的规划	97	6.3.8	配置静态路由	170
4.1.2	交换机的配置源与管理端口	98	6.4	使用 Cisco CNA 管理交换机	171
4.1.3	交换机的配置方式	106	6.4.1	配置设备属性	171
4.1.4	配置信息准备	109	6.4.2	配置 SPAN 端口	179
4.2	CLI 命令行	109	6.4.3	重新引导交换机	181
4.2.1	CLI 命令行及使用	109	6.4.4	配置文件的备份与恢复	181
4.2.2	指定端口、VLAN、MAC 和 IP	115	6.4.5	升级系统映像	182
4.3	交换机初始化配置	117	6.4.6	管理文件系统	185
4.3.1	图形界面初始化配置	117	6.5	使用 Cisco CNA 监控交换机	185
4.3.2	对话式初始化配置	119	6.5.1	监控交换机端口状态	186
4.3.3	CLI 命令初始化配置	121	6.5.2	查看数据统计资料	186
6.5.3	CLI 命令初始化配置	121	6.5.3	系统资源和事件	187
第 5 章	使用 Web 配置和管理交换机	124	第 7 章	使用 CLI 基本配置交换机	188
5.1	登录 Web 配置界面	124	7.1	两层结构网络规划	188
5.2	配置交换机	125	7.2	两层结构核心交换机配置	190
5.2.1	设置端口属性	125	7.2.1	配置 VTP 服务器	190
5.2.2	设置端口角色	126	7.2.2	配置 VLAN	192
5.2.3	快速配置交换机	128	7.2.3	配置 VLAN 中继	197
5.3	监控交换机	129	7.2.4	配置 PVST	201
5.3.1	查看交换机端口状态	129	7.2.5	配置 MSTP	209
5.3.2	查看数据统计资料	130	7.2.6	配置 Uplink 和 X2 接口	214
5.3.3	查看端口健康状态和可用性	132	7.2.7	配置链路汇聚	217
5.4	管理交换机	133	7.2.8	配置 SVI 接口	223
5.4.1	重新启动交换机	133	7.2.9	配置单播路由	225
5.4.2	更新系统映像文件	134			

7.2.10	配置默认路由	228	9.3.5	配置 IP 源地址保护	298
7.3	两层结构接入交换机配置	229	9.4	配置 ACL 访问安全	299
7.3.1	配置 VTP 客户端	230	9.4.1	访问列表概述	299
7.3.2	配置二层接口	231	9.4.2	创建并应用 IP 访问列表	301
7.3.3	配置智能端口	236	9.4.3	创建并应用端口访问列表	305
7.3.4	配置 PortFast	239	9.4.4	创建并应用 VLAN 访问列表	306
7.3.5	接入交换机配置示例	241	9.5	配置 802.1X 基于端口的认证	307
第 8 章	使用 CLI 高级配置交换机	243	9.5.1	IEEE 802.1X 简介	307
8.1	三层结构网络规划	243	9.5.2	启用 IEEE 802.1X 认证	309
8.2	三层结构核心交换机配置	245	9.5.3	配置交换机到 RADIUS 服务器的 通信	309
8.2.1	配置三层接口	246	9.5.4	配置重新认证周期	310
8.2.2	配置 DHCP 中继	251	9.5.5	修改安静周期	311
8.2.3	配置 UDLD	254	9.6	配置基于 Web 的认证	311
8.2.4	配置 CEF	258	9.6.1	基于 Web 的认证简介	311
8.2.5	配置 HSRP	261	9.6.2	基于 Web 认证的默认配置	313
8.2.6	配置动态路由	267	9.6.3	基于 Web 认证的配置策略和限制	313
8.2.7	配置冗余管理引擎	267	9.6.4	基于 Web 认证的配置过程	314
8.2.8	配置 QoS	272	9.7	配置动态 ARP 检查	315
8.3	三层结构汇聚交换机配置	277	9.7.1	配置动态 ARP 检查	316
8.3.1	配置路由协议	277	9.7.2	显示动态 ARP 检查信息	320
8.3.2	配置 BackboneFast	277	第 10 章	使用 CLI 管理交换机	321
8.3.3	配置 Flex 链路	280	10.1	监控交换机	321
8.4	三层结构接入交换机配置	281	10.1.1	监控交换机系统状态	321
8.4.1	配置 UplinkFast	281	10.1.2	监控端模块和口状态	324
8.4.1	配置 PoE	284	10.1.3	查看 MAC 地址表	331
第 9 章	使用 CLI 安全配置交换机	285	10.1.4	TDR 线缆测试	332
9.1	基于端口的传输控制	285	10.2	管理交换机	332
9.1.1	风暴控制	285	10.2.1	TFTP 服务器	332
9.1.2	端口流控制	286	10.2.2	系统文件管理	333
9.1.3	端口带宽限制	286	10.2.3	配置文件管理	335
9.1.4	保护端口	287	10.2.4	IOS 软件映像管理	338
9.1.5	端口阻塞	288	10.3	配置网络远程管理	341
9.1.6	端口安全	288	10.3.1	配置 CDP	341
9.2	配置私有 VLAN	290	10.3.2	配置 RMON	343
9.2.1	PVLAN 概述	290	10.3.3	配置 SPAN 和 RSPAN	346
9.2.2	配置 PVLAN	292	10.3.4	配置系统消息日志	355
9.3	配置 DHCP 安全	295	第 11 章	路由器	361
9.3.1	DHCP 侦听概述	296	11.1	路由器概述	361
9.3.2	启用 DHCP 侦听	296	11.1.1	路由器的功能	361
9.3.3	在私有 VLAN 中启用 DHCP 侦听	297	11.1.2	路由器的工作原理	364
9.3.4	启用 DHCP 侦听绑定数据库代理	297			

11.2	路由器的分类与适用.....	365	12.3	路由器的连接.....	393
11.2.1	高端路由器与中低端路由器.....	365	12.3.1	路由器连接策略.....	393
11.2.2	模块化路由器与固定端口 路由器.....	366	12.3.2	路由器面板.....	394
11.2.3	核心路由器与接入路由器.....	366	12.3.3	与局域网设备的连接.....	400
11.2.4	通用路由器与专用路由器.....	366	12.3.4	连接器与电缆.....	400
11.2.5	有线路由器与无线路由器.....	367	12.3.5	与广域网接入设备的连接.....	402
11.3	路由器的参数.....	367	12.4	路由器的连接测试.....	403
11.3.1	路由器基本参数.....	367	12.4.1	Show 命令判断.....	403
11.3.2	路由器性能参数.....	370	12.4.2	LED 指示灯判断.....	403
11.4	路由器的选择策略.....	371	第 13 章	路由器配置方式与初始化.....	408
11.4.1	路由器的选型原则.....	371	13.1	路由器配置前的准备.....	408
11.4.2	路由器选型时应考虑的因素.....	373	13.1.1	路由器配置前的规划.....	408
11.5	静态路由与默认路由.....	374	13.1.2	路由器的外部配置源.....	409
11.5.1	直连路由.....	374	13.1.3	路由器的配置接口.....	410
11.5.2	静态路由.....	374	13.1.4	路由器与配置终端设备的连接.....	410
11.5.3	默认路由.....	376	13.1.5	路由器的配置方式.....	411
11.6	动态路由.....	377	13.2	路由器初始化配置.....	412
11.6.1	RIP 路由协议.....	377	13.2.1	路由器初始配置规划.....	412
11.6.2	OSPF 路由协议.....	378	13.2.2	使用设置命令工具初始配置.....	413
11.6.3	EIGRP 路由协议.....	382	13.2.3	使用设置命令工具初始配置.....	415
11.6.4	BGP 路由协议.....	384	13.2.4	使用 Cisco CP Express 初始配置.....	417
11.6.5	IS-IS 路由协议.....	384	第 14 章	使用 Cisco CP 配置路由器.....	429
第 12 章	路由器的接口与连接.....	386	14.1	路由器基本配置.....	429
12.1	路由器模块和接口卡.....	386	14.1.1	登录 Cisco CP.....	429
12.1.1	SPE.....	386	14.1.2	用户账户设置.....	430
12.1.2	SM.....	386	14.1.3	VTY 设置.....	431
12.1.3	AIM/ISM.....	387	14.1.4	配置 LAN 和 WAN 连接.....	432
12.1.4	WIC/HWIC/EHWIC.....	387	14.1.5	配置基本路由.....	434
12.1.5	NM/NME.....	388	14.1.6	创建“网络地址转换(NAT)” 规则.....	435
12.1.6	PVDM/PVDM2/PVDM3.....	388	14.1.7	配置动态路由协议.....	439
12.1.7	VIC/VWIC/EVM.....	389	14.2	路由器高级配置.....	441
12.2	路由器接口.....	390	14.2.1	创建防火墙.....	441
12.2.1	10Base-T/100Base-TX/1000Base-T 接口.....	390	14.2.2	配置 VPN、Easy VPN 和 DMVPN 连接.....	443
12.2.2	GBIC/SFP 插槽.....	390	14.2.3	安全审计及安全设置.....	446
12.2.3	SC/LC 接口.....	391	14.2.4	创建服务质量(QoS)策略.....	449
12.2.4	E1/T1 接口.....	391	14.2.5	创建访问控制列表.....	451
12.2.5	智能串行接口.....	392	14.3	管理路由器.....	452
12.2.6	异步/同步串口.....	392	14.3.1	SNMP 设置.....	453
12.2.7	ADSL 接口.....	393	14.3.2	管理访问策略.....	453
12.2.8	BNC 接口.....	393			

14.3.3	监视路由器的状态	454	15.8.2	静态地址转换的实现	502
14.3.4	监视路由器端口的状态	456	15.8.3	动态地址转换的实现	503
14.3.5	路由器日志	458	15.8.4	端口复用地址转换	504
14.3.6	恢复出厂默认设置	463	15.9	配置静态路由	505
第 15 章	使用 CLI 配置路由器	464	15.9.1	配置静态路由和默认路由	505
15.1	路由器基本配置	464	15.9.2	LAN 方式接入 Internet	506
15.1.1	路由器端口编号	464	15.9.3	DDN 接入远程网络	507
15.1.2	IP 协议配置原则	468	第 16 章	配置 IP 动态路由	509
15.1.3	配置主机名和密码	469	16.1	配置 RIP	509
15.1.4	配置快速以太网接口	469	16.1.1	RIP 的默认配置	509
15.1.5	配置同步串行接口	470	16.1.2	配置 RIP 路由	510
15.2	配置广域网接口	471	16.1.3	配置 RIP 认证	511
15.2.1	接口的一般配置	471	16.1.4	配置水平分割	512
15.2.2	同步串口配置	472	16.2	配置 EIGRP	512
15.3	配置逻辑接口	475	16.2.1	默认的 EIGRP 配置	513
15.3.1	Loopback 接口配置	475	16.2.2	配置基本 EIGRP 参数	513
15.3.2	NULL 接口配置	475	16.2.3	配置 EIGRP 接口	514
15.3.3	Tunnel 接口配置	475	16.2.4	配置 EIGRP 路由认证	515
15.3.4	Dialer 接口配置	477	16.2.5	查看 EIGRP 相关信息	515
15.3.5	子接口配置	478	16.3	配置 OSPF	516
15.4	配置 PPP 和 MP 协议	479	16.3.1	默认的 OSPF 配置	516
15.4.1	PPP 和 MP 协议概述	479	16.3.2	配置基本 OSPF 参数	517
15.4.2	PPP 协议的配置	480	16.3.3	配置 OSPF 接口	517
15.4.3	MP 协议的配置	482	16.3.4	配置 OSPF 区域参数	518
15.4.4	PPP 的监控	483	16.3.5	配置其他 OSPF 参数	519
15.5	配置 HDLC 协议	484	16.3.6	配置 Loopback 接口	520
15.5.1	HDLC 协议概述	484	16.3.7	查看 OSPF 相关信息	521
15.5.2	HDLC 配置	484	第 17 章	网络安全设备概述	522
15.6	配置帧中继协议	485	17.1	防火墙	522
15.6.1	帧中继概述	485	17.1.1	网络防火墙简介	522
15.6.2	帧中继的基本配置	487	17.1.2	防火墙的主要功能	523
15.6.3	帧中继子接口配置	489	17.1.3	防火墙的局限性与脆弱性	524
15.6.4	帧中继的高级配置	490	17.1.4	防火墙的分类与适用	525
15.6.5	帧中继监控和维护	491	17.2	IDS	532
15.7	配置 LAPB 和 X.25 协议	492	17.2.1	IDS 概述	533
15.7.1	LAPB、X.25 协议概述	492	17.2.2	IDS 优势的缺陷	534
15.7.2	配置 LAPB 协议	493	17.2.3	IDS 与防火墙联动	535
15.7.3	配置 X.25 协议	494	17.3	IPS	537
15.7.4	配置 X.25 高级功能	499	17.3.1	IPS 概述	537
15.7.5	显示 X.25 接口信息	500	17.3.2	IPS 的技术特征	538
15.8	网络地址转换	500	17.3.3	IPS 的分类	539
15.8.1	理解 NAT	501			

17.3.4	IPS 的优势与作用	540	19.4.4	配置非转换 NAT	584
17.3.5	IPS 的缺陷	541	19.4.5	配置 Cisco AnyConnect VPN 客户端	585
17.3.6	部署 IPS	542	19.5	配置 Site-to-Site VPN	586
17.3.7	IDS 与 IPS 比较	542	19.6	监控和管理安全设备	589
17.4	安全设备的主要参数与选择	544	19.6.1	监控安全设备运行状态	589
17.4.1	防火墙的参数与选择	544	19.6.2	查看和分析网络流量	589
17.4.2	IDS 的选择	548	19.6.3	查看和分析系统日志	591
17.4.3	IPS 的参数与选择	549	第 20 章	无线网络设备概述	592
第 18 章	安全设备的端口与连接	551	20.1	无线局域网标准	592
18.1	安全设备的端口	551	20.1.1	IEEE 802.11 系统标准	592
18.1.1	安全设备的物理端口	551	20.1.2	IEEE 802.16a 标准	596
18.1.2	防火墙逻辑端口	553	20.1.3	无线安全标准	596
18.1.3	安全设备端口的连接	553	20.1.4	无线产品兼容性	599
18.1.4	安全设备的 LED 指示灯	554	20.2	无线网络组件	600
18.2	网络安全设计与连接	557	20.2.1	无线网卡	601
18.2.1	网络防火墙设计与连接	557	20.2.2	无线 AP	601
18.2.2	入侵检测系统设计与连接	560	20.2.3	无线网桥	602
18.2.3	入侵防御系统设计与连接	562	20.2.4	无线路由器	602
18.2.4	综合安全设计与连接	563	20.2.5	无线天线	602
第 19 章	使用 ASDM 配置安全设备	565	20.2.6	无线局域网控制器	603
19.1	Cisco ASDM 初始化	565	20.2.7	其他无线设备	603
19.1.1	安装前的准备	565	20.3	无线网络模式特点与适用	603
19.1.2	使用 Startup Wizard	566	20.3.1	对等无线网络	604
19.1.3	防火墙基本配置	567	20.3.2	独立无线网络	604
19.1.4	安全策略设置	570	20.3.3	接入以太网的无线网络	605
19.2	配置 DMZ	570	20.3.4	无线漫游的无线网络	605
19.2.1	DMZ 网络结构	570	20.3.5	点对点 and 点对多点网络	606
19.2.2	为 NAT 创建 IP 地址池	571	20.4	无线设备的选择	606
19.2.3	配置内部客户端访问 DMZ 的 Web 服务器	573	20.4.1	无线 AP 的选择策略	606
19.2.4	配置内部客户端访问 Internet	573	20.4.2	无线网桥的选择	610
19.2.5	为 Web 服务器配置外部 ID	573	20.4.3	无线网络控制器的选择	610
19.2.6	允许 Internet 用户访问 DMZ 的 Web 服务	574	20.4.4	无线天线的选择	613
19.3	配置 NAT 方式接入 Internet	576	20.4.5	远程供电设备的选择	615
19.3.1	配置 NAT 规则	576	20.5	无线 AP 位置的选择	616
19.3.2	将内网服务器发布到 Internet	578	20.5.1	室内无线 AP 位置的选择	616
19.4	配置 SSL 加密的远程访问 VPN	579	20.5.2	室外无线 AP 位置的选择	617
19.4.1	SSL VPN 的网络结构	580	20.5.3	漫游网络无线 AP 的选择	617
19.4.2	运行 SSL VPN 配置向导	580	20.6	无线设备的端口与连接	618
19.4.3	配置 NAT	583	20.6.1	无线网络控制器的连接	618
			20.6.2	无线 AP 的端口与连接	620
			20.6.3	连接状态判断	621

第 21 章	使用 Web 配置无线网络	624	22.5.1	创建 VLAN	659
21.1	无线 AP 基本配置	624	22.5.2	配置 WPA	659
21.1.1	首次配置无线 AP	624	22.5.3	配置 VPN Passthrough	660
21.1.2	管理无线 AP	628	22.5.4	配置 QoS	661
21.1.3	配置无线设置	629	22.5.5	配置 CCX	661
21.1.4	配置本地认证	630	22.5.6	创建 AP 组	663
21.1.5	配置 WLAN	630	22.5.7	将 AP 指定至 AP 组	663
21.1.6	配置 QoS	633	22.6	无线资源管理	664
21.1.7	配置过滤	634	22.6.1	配置 RF 组	664
21.1.8	配置 SNMP	635	22.6.2	发现流氓 AP	665
21.1.9	配置系统消息日志	635	22.6.3	配置静态传输信道和传输功率	666
21.2	无线漫游网络的配置	636	22.6.4	配置 CCX 无线管理	666
21.2.1	无线 AP 配置规划	636	22.7	配置轻型无线 AP	667
21.2.2	配置 WDS 服务器	636	第 23 章	服务器与网络存储	668
21.2.3	配置 WDS 设备	637	23.1	网络服务器	668
21.2.4	无线客户端配置	637	23.1.1	网络服务器的特性	668
21.3	点对点 and 点对多点网络的配置	639	23.1.2	网络服务器的类型	670
21.3.1	点对点网络配置	639	23.1.3	网络服务器选型原则	671
21.3.2	点对多点网络配置	642	23.1.4	网络操作系统	672
第 22 章	配置无线局域网控制器	643	23.2	网络存储技术	672
22.1	无线局域网控制器初始化	643	23.2.1	DAS	673
22.2	配置无线局域网控制器的 端口和接口	644	23.2.2	NAS	673
22.2.1	无线网络控制器的登录	645	23.2.3	SAN	674
22.2.2	配置接口属性	645	23.2.4	iSCSI	675
22.2.3	配置 LAG 端口	646	23.3	DAS	675
22.3	配置无线局域网控制器设置	647	23.3.1	DAS 的类型与连接	675
22.3.1	修改 SNMP 字符串	647	23.3.2	DAS 的配置	676
22.3.2	启用系统日志	648	23.4	SAN	678
22.3.3	配置客户漫游参数	649	23.4.1	网络存储系统组件	678
22.4	配置无线局域网控制器安全	649	23.4.2	SAN 与网络的连接	679
22.4.1	配置 TACACS+	650	23.4.3	SAN 的配置	679
22.4.2	配置本地用户	650	23.5	iSCSI	686
22.4.3	配置 LDAP	651	23.5.1	iSCSI 与网络的连接	686
22.4.4	配置本地 EAP	652	23.5.2	iSCSI 的配置	687
22.4.5	配置访问列表	654	第 24 章	网络设备故障的诊断与排除	692
22.4.6	配置 IDS 传感器	656	24.1	网络故障概述	692
22.4.7	上传/下载 IDS 签名	656	24.1.1	故障主要原因与现象	692
22.4.8	禁用/启用 IDS 签名	657	24.1.2	网络故障排除过程	693
22.4.9	查看 IDS 签名事件	658	24.2	交换机故障诊断	695
22.5	配置 WLAN	658	24.2.1	交换机故障诊断方法	695
			24.2.2	交换机故障诊断顺序	697

24.2.3	电源故障	698	25.2.3	独立接入交换机的配置	730
24.2.4	端口故障	700	25.2.4	核心交换机的配置	733
24.2.5	接口故障	701	25.2.5	路由器配置	740
24.2.6	GBIC/SFP 故障	704	25.3	经济型以太网升级方案	743
24.2.7	背板故障	705	25.3.1	可用性升级方案	744
24.2.8	引擎故障	705	25.3.2	安全性升级方案	745
24.2.9	线卡故障	706	第 26 章	豪华型万兆以太网方案	747
24.2.10	系统故障	707	26.1	网络拓扑与设备选购方案	747
24.2.11	配置错误	708	26.1.1	网络需求调查	747
24.3	路由器故障	709	26.1.2	网络拓扑结构	747
24.3.1	路由器一般故障	709	26.1.3	网络技术设计	750
24.3.2	路由器故障诊断	712	26.1.4	网络设备选择	751
第 25 章	经济型万兆以太网方案	714	26.2	网络设备配置方案	757
25.1	网络拓扑与设备选购方案	714	26.2.1	IP 地址和 VLAN 规划	757
25.1.1	网络需求调查	714	26.2.2	核心交换机的配置	758
25.1.2	网络拓扑结构	714	26.2.3	路由器配置	774
25.1.3	网络技术设计	715	26.2.4	防火墙配置	780
25.1.4	网络设备选择	716	26.3	万兆以太网升级方案	785
25.2	网络设备配置方案	719	26.3.1	无线网络升级方案	785
25.2.1	IP 地址和 VLAN 规划	719	26.3.2	安全升级方案	787
25.2.2	汇聚交换机配置	720	26.3.3	服务器群集设计	790

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 之间的互连；安全设备则用于监控和保护内部网络的安全；无线网络是有线网络的补充，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）是构建局域网最重要的设备之一。作为集线设备，交换机的作用是将作为传输介质的线缆汇聚在一起，实现网络设备（如交换机、路由器、网络防火墙、无线局域网控制器、无线 AP 等）之间、集线设备与网络终端（如计算机、网络打印机、网络摄像头、IP 电话等）之间的连接。交换机与综合布线系统一起构成网络的骨架，实现网络设备、网络终端的互连互通。如图 1-1 所示为 Cisco Catalyst 3750 系列交换机。

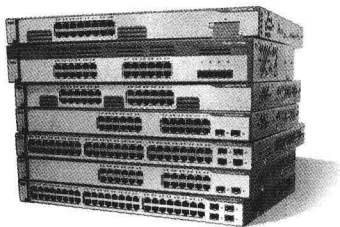


图 1-1 Cisco Catalyst 3750 系列交换机

1.1.2 路由器简介

路由器其实是一种特殊用途的专用计算机，用于计算并选择数据在网络间进行传输的路由。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。

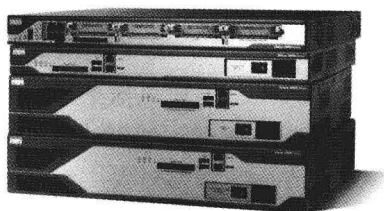


图 1-2 Cisco 2800 系列路由器

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，可以为网络设备或者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，限制网络间的互访，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。

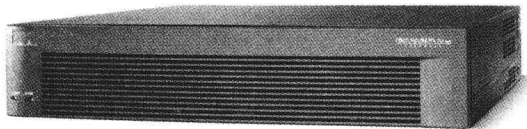


图 1-3 Cisco 防火墙

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、攻击行为或者攻击结果，以保证网络系统资源的安全。IDS 可以实现与防火墙的联动，即 IDS 一旦发现某种攻击，即由防火墙做出某种反应。如图 1-4 所示为 Cisco IDS 设备。



图 1-4 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，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。IPS 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 1-5 Cisco IPS 设备

1.1.4 无线设备简介

搭建无线局域网所需的硬件设备较为复杂，主要包括无线网卡、无线接入点 (AP, Access Point) /网桥 (Bridge)、无线路由器、无线局域网控制器和无线天线等 5 种，需要根据不同的网络环境和无线网络模式进行选择。例如，无线客户端接入无线网络时要用到无线适配器，无线局域网与以太网连接时要用到无线 AP，局域网远程无线互连时要用到无线网桥，无线局域网接入 Internet 时要用到无线路

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，要用到无线天线。构建对等无线网络时，只需要无线网卡；构建点对点和点对多点网络时，只需要无线网桥；构建接入无线网络时，则需要无线 AP 和无线接入点；构建无线网络时，则需要无线局域网控制器和无线 AP，等等。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。

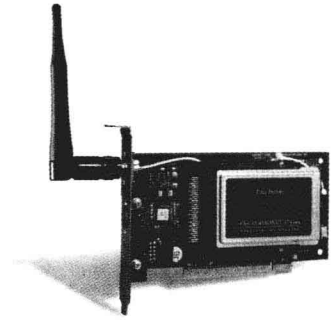


图 1-6 PCI 接口无线网卡

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。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 接入或与网络互连。网络防火墙并不是必需的网络设备，如果网络对安全性的要求不是太高，也可以不选择。

1.2.1 交换机在网络中的应用

1. 提供网络接口

交换机在网络中最重要的应用就是提供网络接口，所有网络设备的互连都必须借助交换机才能实现。包括：

- 连接交换机、路由器、网络防火墙、IPS、IDS、无线局域网控制器和无线接入点等网络设备。
- 连接计算机、服务器、网络存储等计算机设备。
- 连接网络打印机、网络摄像机、IP 电话等其他网络终端。

如图 1-7 所示为大中型网络中交换机与其他设备相连接的拓扑示意图。

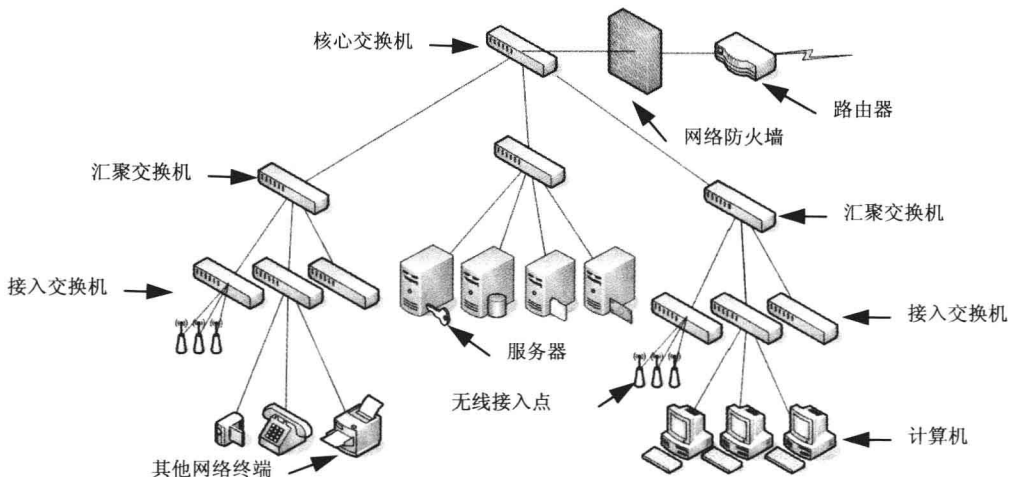


图 1-7 大中型网络中的交换机

需要注意的是，网络拓扑图描述的只是网络设备之间的逻辑连接状况，而这些设备在机柜中的物理安装方式则如图 1-8 所示。

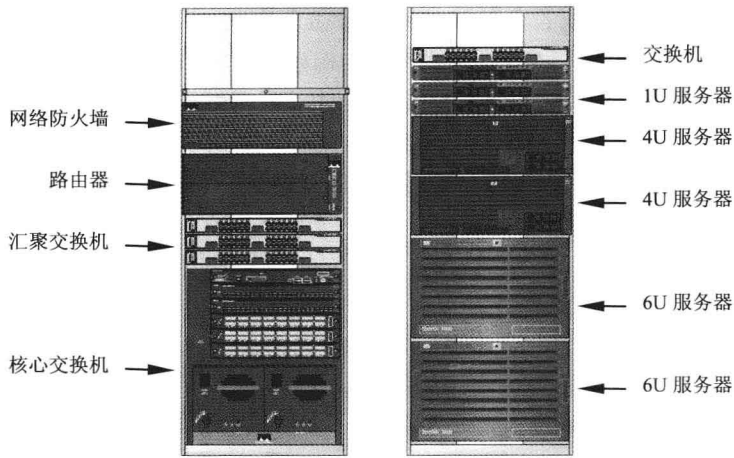


图 1-8 网络设备机架安装示意图

如图 1-9 所示为小型网络中交换机与其他设备相连接的拓扑示意图。

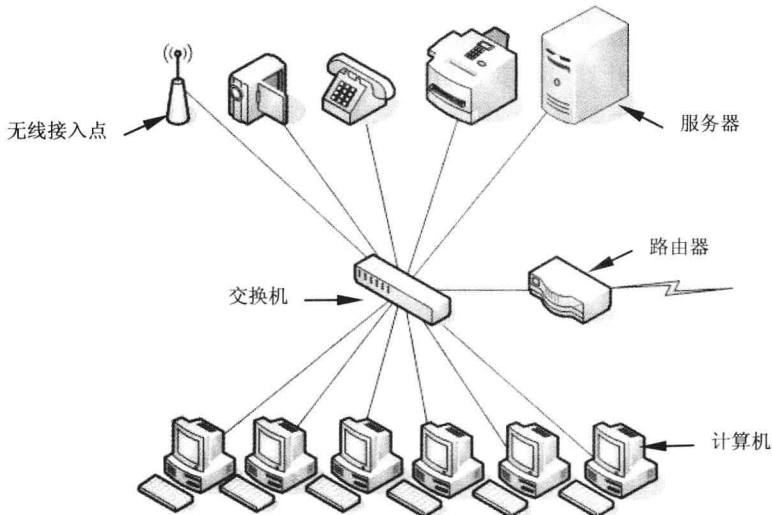


图 1-9 小型网络中的交换机

2. 扩充网络接口

尽管交换机大都拥有较多数量的端口（通常为 8~52 个），但是，当网络规模较大时，一台交换机所能提供的网络接口往往不够。此时，就必须将两台或更多的交换机连接在一起，从而成倍地扩充网络接口。如图 1-10 所示，每台交换机拥有 50 个端口，而将 3 台交换机连接在一起，就可以提供多达 146 个端口。

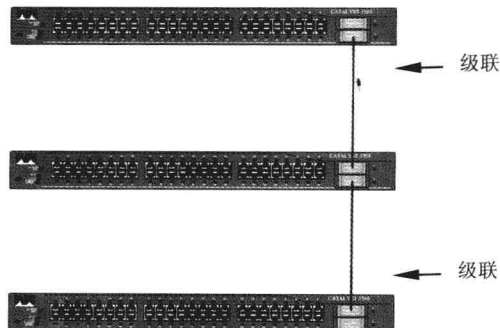


图 1-10 扩充网络接口