

网管从业宝典

交换机 · 路由器 · 防火墙

经典案例分析 全新思路讲解 独特培训方法

- 精细讲解交换机连接方法
- 一网打尽交换机中高档配置方案
- 全面剖析路由器工作原理
- 全程图解路由器连接配置方法
- 深度解密防火墙配置流程
- 网管职业技巧点拨

■ 刘晓辉 编



重庆大学出版社

<http://www.cqup.com.cn>

TP393.07/45

:3

2008

网管从业宝典

交换机 · 路由器 · 防火墙

WANGGUAN CONGYE BAODIAN JIAOHUANJI · LUYOUQI · FANGHUOQIANG

刘晓辉 编

江苏工业学院图书馆
藏书章

重庆大学出版社

内 容 提 要

对于刚刚踏上网管岗位的读者来说,他们迫切需要了解核心网络设备的相关知识。本书对这些内容进行了详细的介绍和说明,其中包括网络交换机、核心路由器和网络硬件防火墙的基础知识与配置方法。读者通过本书可以快速掌握相关设备的使用方法,提升网络管理员的管理水平。本书风格活泼,实践内容丰富,适合广大学生、网络爱好者及网络从业人员阅读。

图书在版编目(CIP)数据

网管从业宝典 交换机·路由器·防火墙 / 刘晓辉编.
重庆:重庆大学出版社,2008.5
ISBN 978-7-5624-4478-7

I. 网… II. 刘… III. 计算机网络—管理—基础知识
IV. TP393.07

中国版本图书馆CIP数据核字(2008)第040984号

网管从业宝典 交换机·路由器·防火墙 刘晓辉 编

责任编辑:黄 成
责任校对:贾 梅

版式设计:王明娟
责任印制:赵 晟

*

重庆大学出版社出版发行

出版人:张鸽盛

社址:重庆市沙坪坝正街174号重庆大学(A区)内

邮编:400030

电话:(023) 65102378 65105781

传真:(023) 65103686 65105565

网址:<http://www.cqup.com.cn>

邮箱:fxk@cqup.com.cn (市场营销部)

全国新华书店经销

重庆科情印务有限公司印刷

*

开本:787×1092 1/16 印张:26.5 字数:520千

2008年5月第1版 2008年5月第1次印刷

ISBN 978-7-5624-4478-7 定价:48.50元

本书如有印刷、装订等质量问题,本社负责调换
版权所有,请勿擅自翻印和用本书
制作各类出版物及配套用书,违者必究

FOREWORD

前言

21 世纪是一个名副其实的信息时代，同时也是竞争激烈的时代。随着大学生的不断增多，学生就业成为了社会热点问题。学习一技之长，找到一份称心如意的工作是每个大学生的梦想，而网络管理员则是很多大学生理想中的职业。但是网络管理员这个职业对于理论与实践能力要求都非常高，对于那些没有实际工作能力的学生来说，他们很难胜任这样一份工作。

于是，我们便编撰了网管从业宝典系列书，现已出版了基础知识、组建实务、管理与维护和故障排除经典案例 4 个分册。本书系统地介绍局域网主要设备——交换机、路由器和防火墙的理论和配置方法。希望能对大家的网络管理工作有所帮助，同时也希望可以帮助读者轻松掌握网络管理员在工作中常用的各种知识。

本书根据问题的不同性质划分为 5 大部分。第 1 部分对网络设备进行了综述，让读者了解到相关的基础知识。第 2 部分是第 2 章到第 6 章，主要介绍交换机的软硬件基础知识和各种配置方法。第 3 部分是第 7 章到第 11 章，重点介绍了路由器的软硬件基础知识和各种配置方法。第 4 部分是第 12 章到第 16 章则是介绍防火墙的软硬件知识和相关的配置方法，第 5 部分是第 17 章，介绍了局域网一般故障的原因以及相应的解决办法。通过本书的学习，读者可以快速掌握网络核心设备的管理与配置方法，提升自己的网络管理水平。

本书作者是长期工作在网络教学和管理第一线的高校教师，既有扎实的理论基础，又有丰富的实践经验，并出版过十余册有关局域网方面的书籍。相信本书能够为所有准备从事网络管理工作的读者提供一些帮助，缩短大家熟悉工作的时间，并在求职时少走一些弯路。

本书是中小型网络管理人员的必备参考书，同时可作为局域网组建者的指导书，也可作为各类网络培训机构或各大中专院校相关课程的参考书。

读者调查表

www.cbook.com.cn 智的飞跃, 从读好书开始

《网管从业宝典 交换机·路由器·防火墙》重庆大学出版社

Book
远望图书

尊敬的读者, 在您阅读本产品后, 请将宝贵的意见通过下表方式及时反馈给我们(可另附页), 您将有机会获得我们送出的礼品。由衷感谢您对我们的支持, 谢谢!

姓名: _____ 性别: _____ 年龄: _____ 职业: _____
邮编: _____ E-mail: _____ 联系电话: _____
联系地址: _____

「您的意见将是我们的改进工作、创造精品的源动力!」

(以下各题如页面不够, 可另附纸张)

1. 您如何得知本产品? 并请从设计风格、效果等方面对你看到的广告进行评价。

- ☐ 别人推荐 ☐ 《微型计算机》相关广告 ☐ 《计算机应用文摘》相关广告
☐ 网站或论坛相关广告
☐ 其他(请注明)

2. 您获得本产品的途径:

- ☐ 书摊 ☐ 新华书店 ☐ 专业科技书店 ☐ 邮购 ☐ 远望 eShop 订购 ☐ 借阅 ☐ 其他

3. 您购买本产品的时间: _____ 年 _____ 月 _____ 日

4. 您对本产品的总体评价:

- 文字角度: ☐ 很好 ☐ 较好 ☐ 一般 ☐ 差
技术角度: ☐ 很好 ☐ 较好 ☐ 一般 ☐ 差
印刷角度: ☐ 很好 ☐ 较好 ☐ 一般 ☐ 差

5. 您对本产品的封面设计的评价:

- ☐ 很好 ☐ 较好 ☐ 一般 ☐ 差

请寄: 重庆市渝北区洪湖西路 18 号远望资讯出版事业部
邮编: 401121
技术咨询电话: (023)67039637

更多精彩请见网站: www.cbook.com.cn

读编交流请至 bbs.PCShow.net(远望图书及光盘)

6. 哪些方面是吸引您购买或翻阅本产品的原因?(可多选)

☐ 选题

☐ 封面及装帧设计

☐ 价格

☐ 内容

☐ 远望图书或系列图书品牌

7. 您认为本套产品的价格:

☐ 偏高

☐ 适中

☐ 偏低

8. 您认为本书的技术含量:

☐ 较深

☐ 适中

☐ 偏低

9. 您对网络新技术:

☐ 很关心

☐ 一般关心

☐ 不关心

10. 您认为本书中还应该补充哪些方面的内容(例如您想看到但文中却没有的内容)?

11. 您认为本书还有哪些不足之处?

12. 您认为本书网络设备的相关知识对您是否有帮助? 您还需要了解那些设备?

13. 您在应聘网管时还遇到哪些问题?

裁
剪
线



第1章 网络设备综述

1.1 交换机概述	2	1.3 防火墙概述	10
1.1.1 交换机的功能	2	1.3.1 网络防火墙的功能	10
1.1.2 交换机与交换式网络	4	1.3.2 防火墙的工作原理	11
1.1.3 交换机的工作原理	5		
1.2 路由器概述	6	1.4 网络设备在网络中的应用	12
1.2.1 路由器的功能	6	1.4.1 交换机在网络中的应用	13
1.2.2 路由器的工作原理	8	1.4.2 路由器在网络中的应用	14
		1.4.3 防火墙在网络中的应用	16

第2章 交换机概述

2.1 交换机简介	18	2.2.11 万兆以太网技术	36
2.1.1 交换式工作原理	18	2.2.12 路由冗余	37
2.1.2 交换模式	20		
2.2 交换机技术	23	2.3 交换机的分类	40
2.2.1 虚拟网技术	23	2.3.1 智能交换机与傻瓜交换机	40
2.2.2 私有虚拟网技术	26	2.3.2 固定端口交换机与模板化交换机	40
2.2.3 第三层交换技术	28	2.3.3 接入层交换机、汇聚层交换机与核心层交换机	41
2.2.4 第四层交换技术	29	2.3.4 以太网交换机与ATM交换机	43
2.2.5 扩展树技术	30	2.3.5 二层交换机与多层交换机	43
2.2.6 链路汇聚技术	31	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	44
2.2.7 服务质量技术	32	2.3.7 对称交换机与非对称交换机	45
2.2.8 IP语音技术	33	2.3.8 桌面交换机与机架式交换机	45
2.2.9 基于端口的传输控制	33	2.3.9 特殊用途交换机	46
2.2.10 千兆以太网技术	34		

第3章 交换机的参数与选择

3.1 交换机的主要参数	48	3.2.1 核心交换机的选择	53
3.1.1 三层交换机的主要参数	48	3.2.2 汇聚层交换机的选择	57
3.1.2 二层交换机的主要参数	51	3.2.3 接入层交换机的选择	58
3.2 交换机的选择策略	53	3.2.4 可网管交换机的选择	60

第4章 交换机的端口与连接

4.1 IEEE 802.3系列标准	63	4.2.3 GBIC 模块与插槽	70
4.1.1 IEEE 802.3 标准	63	4.2.4 SFP 模块与插槽	71
4.1.2 IEEE 802.3u 标准	63	4.2.5 10GE 模块与插槽	71
4.1.3 IEEE 802.3z 和 802.3ab 标准	64	4.2.6 共用端口	72
4.1.4 IEEE 802.3ae、802.3ak 和 802.3an 标准	66	4.2.7 TwinGig 转换模块	72
		4.2.8 跳线与使用	72
4.2 交换机端口类型	68		
4.2.1 光纤端口	69	4.3 交换机的连接策略	75
4.2.2 双绞线端口	69	4.3.1 不同性能交换机的连接策略	75

4.3.2 非对称交换机的连接策略	75	4.4.4 远程交换机的连接	80
4.3.3 对称交换机的连接策略	76		
4.4 交换机的连接	76	4.5 交换机的堆叠	81
4.4.1 堆叠与级联	76	4.5.1 Cisco 交换机的堆叠	81
4.4.2 光纤端口的连接	77	4.5.2 3Com 交换机的堆叠	84
4.4.3 双绞线端口的连接	79	4.5.3 华为交换机的堆叠	85

第5章 交换机的简单配置

5.1 交换机配置前的准备	87	5.2.4 为 CNA 准备 Catalyst 4500 交换机	96
5.1.1 交换机的管理方式	87		
5.1.2 交换机配置前的规划	91	5.3 使用 CNA 管理交换机	98
5.2 交换机的初始配置	93	5.3.1 CNA 简介	98
5.2.1 配置前的准备	93	5.3.2 添加交换机	100
5.2.2 运行快速设置	93	5.3.3 监控交换机	101
5.2.3 CLI 初始配置	95	5.3.4 配置交换机	103
		5.3.5 维护交换机	107

第6章 交换机的高级配置

6.1 基于端口的传输控制	110	6.5.6 启用 DHCP 侦听	140
6.1.1 广播风暴控制	110	6.5.7 在私有 VLAN 中启用 DHCP 侦听	141
6.1.2 端口流控制	111	6.5.8 启用 DHCP 侦听绑定数据库代理	142
6.1.3 端口带宽限制	112	6.5.9 配置 IP 源地址保护	143
6.1.4 保护端口	113	6.6 QoS 配置	144
6.1.5 端口阻塞	114	6.6.1 QoS 概述	144
6.1.6 端口安全	114	6.6.2 配置 Auto-QoS	145
6.2 冗余链接配置	116	6.7 配置 CDP	150
6.2.1 配置 EtherChannel	116	6.7.1 CDP 概述	150
6.2.2 STP 配置	118	6.7.2 CDP 默认配置	151
6.2.3 配置 Postfast 端口	124	6.7.3 CDP 配置	151
6.3 访问列表配置	125	6.8 配置 SPAN 和 RSPAN	152
6.3.1 访问列表概述	125	6.8.1 SPAN 和 RSPAN 简介	152
6.3.2 创建并应用 IP 访问列表	127	6.8.2 SPAN 和 RSPAN 默认配置	153
6.3.3 创建并应用端口访问列表	132	6.8.3 SPAN 会话中的流量监视限制	154
6.3.4 创建并应用 VLAN 访问列表	133	6.8.4 配置本地 SPAN	154
6.4 基于端口的认证配置	134	6.8.5 配置 RSPAN	157
6.4.1 IEEE802.1x 简介	134	6.8.6 显示 SPAN 和 RSPAN 状态	161
6.4.2 启用 IEEE 802.1X 认证	135	6.9 配置 HSRP	161
6.4.3 配置交换机到 RADIUS 服务器的通讯	136	6.9.1 HSRP 概述	161
6.4.4 配置重新认证周期	137	6.9.2 HSRP 默认配置	163
6.4.5 修改安静周期	137	6.9.3 HSRP 的配置方针	163
6.5 DHCP 中继	138	6.9.4 启用 HSRP	164
6.5.1 DHCP 中继代理概述	138	6.9.5 配置 HSRP 优先权	164
6.5.2 DHCP 默认配置	138	6.9.6 配置 MHSRP	165
6.5.3 DHCP 配置策略	138	6.9.7 配置 HSRP 认证和时钟	166
6.5.4 配置 DHCP 中继代理	139	6.9.8 配置 HSRP 组和簇	166
6.5.5 指定包转发地址	140	6.9.9 显示 HSRP 配置	167

第7章 路由器概述

7.1 路由器简介	169	7.2.5 按传输性能划分	175
7.1.1 路由器的主要功能	169	7.2.6 按网络类型划分	175
7.1.2 路由器工作原理	171	7.3 路由协议	175
7.1.3 路由器在网络中的应用	172	7.3.1 静态路由	175
7.2 路由器的分类与适用	173	7.3.2 RIP 路由协议	176
7.2.1 按性能划分	173	7.3.3 OSPF 路由协议	178
7.2.2 按结构划分	174	7.3.4 BGP 路由协议	182
7.2.3 按网络位置划分	174	7.3.5 IS-IS 路由协议	183
7.2.4 按功能划分	174	7.3.6 EIGRP 路由协议	185

第8章 路由器的参数与选择

8.1 路由器的参数	188	8.2 路由器的选择	193
8.1.1 路由器基本参数	188	8.2.1 路由器的选购原则	193
8.1.2 路由器性能参数	192	8.2.2 选购时应考虑的因素	194

第9章 路由器的接口与连接

9.1 路由器接口	197	9.2.2 路由器面板	201
9.1.1 常用网络接口	197	9.2.3 路由器连接	203
9.1.2 路由器配置接口	200	9.3 路由器的连接测试	206
9.2 路由器的连接	201	9.3.1 Show 命令判断	206
9.2.1 路由器连接策略	201	9.3.2 LED 指示灯判断	207

第10章 Cisco 路由器的基本配置

10.1 使用 SDM 配置	210	10.2.2 安全审计	224
10.1.1 路由器初始化配置	210	10.2.3 路由	227
10.1.2 使用 SDM 配置路由器	213	10.2.4 NAT	228
10.2 SDM 配置路由器	222	10.2.5 服务质量	231
10.2.1 接口和连接	222	10.2.6 其他任务	232

第11章 Cisco 路由器的高级配置

11.1 配置广域网接口	237	11.3.3 MP 协议的配置	248
11.1.1 接口的一般配置	237	11.3.3 PPP 的监控	249
11.1.2 同步串口配置	239	11.4 配置 HDLC 协议	250
11.2 配置逻辑接口	241	11.4.1 HDLC 协议概述	250
11.2.1 Loopback 接口配置	241	11.4.2 HDLC 配置	251
11.2.2 NULL 接口配置	241	11.5 配置帧中继协议	251
11.2.3 Tunnel 接口配置	241	11.5.1 帧中继概述	251
11.2.4 Dialer 接口配置	243	11.5.2 帧中继的基本配置	253
11.2.5 子接口配置	243	11.5.3 帧中继子接口配置	256
11.3 配置 PPP 和 MP 协议	245	11.5.4 帧中继的高级配置	257
11.3.1 PPP 和 MP 协议概述	245	11.5.5 帧中继监控和维护	258
11.3.2 PPP 协议的配置	246		

11.6 配置 LAPB 和 X.25 协议	259	11.8.1 默认的 OSPF 配置	271
11.6.1 LAPB、X.25 协议概述	259	11.8.2 配置基本 OSPF 参数	271
11.6.2 配置 LAPB 协议	260	11.8.3 配置 OSPF 接口	272
11.6.3 配置 X.25 协议	261	11.8.4 配置 OSPF 区域参数	272
11.6.4 配置 X.25 高级功能	265	11.8.5 配置其他 OSPF 参数	273
11.6.5 显示 X.25 接口信息	267	11.8.6 配置 Loopback 接口	275
11.7 配置 RIP	267	11.8.7 监控 OSPF	275
11.7.1 RIP 的默认配置	267	11.9 配置 EIGRP	276
11.7.2 配置 RIP 路由	268	11.9.1 默认的 EIGRP 配置	276
11.7.3 配置 RIP 认证	269	11.9.2 配置基本 EIGRP 参数	277
11.7.4 配置水平分割	270	11.9.3 配置 EIGRP 接口	277
11.8 配置 OSPF	270	11.9.4 配置 EIGRP 路由认证	278
		11.9.5 监视 EIGRP	279

第 12 章 安全设备概述

12.1 防火墙	281	12.2.2 IDS 优势的缺陷	292
12.1.1 网络安全防护的重要意义	281	12.2.3 IDS 与防火墙联动	294
12.1.2 网络防火墙简介	283	12.3 IPS	295
12.1.3 防火墙的主要功能	284	12.3.1 IPS 概述	295
12.1.4 防火墙技术原理	285	12.3.2 IPS 的技术特征	296
12.1.5 防火墙的防御攻击技术	287	12.3.3 IPS 的分类	297
12.1.6 防火墙的局限性与脆弱性	289	12.3.4 IPS 的优势与作用	298
12.2 IDS	290	12.3.5 IPS 的缺陷	299
12.2.1 IDS 概述	291	12.3.6 部署 IPS	300
		12.3.7 IDS 与 IPS 比较	301

第 13 章 防火墙的主要参数与选择

13.1 防火墙的主要参数	304	13.2.5 按照防火墙在网络中的位置划分	314
13.1.1 防火墙的性能参数	304	13.3 防火墙的选择	315
13.1.2 防火墙的功能参数	305	13.3.1 防火墙的选择策略	315
13.2 防火墙的分类与适用	307	13.3.2 Cisco PIX 与 ASA	315
13.2.1 按照软硬件形式划分	307	13.4 IDS 与 IPS 的选择	316
13.2.2 按照实现技术划分	309	13.4.1 IDS 的选择	316
13.2.3 按照硬件结构划分	311	13.4.2 IPS 的选择	318
13.2.4 按照硬件实现技术划分	312		

第 14 章 防火墙的端口与连接

14.1 防火墙的端口	321	14.2.2 内部网络与 Internet 的连接之间	326
14.1.1 防火墙物理端口	321	14.2.3 连接局域网和广域网	327
14.1.2 防火墙逻辑端口	322	14.2.4 内部网络与第三方网络的连接之间	328
14.1.3 防火墙端口的连接	322	14.2.5 内部网络不同部门的连接之间	329
14.1.4 防火墙的 LED 指示灯	324	14.2.6 连接同一部门的不同网络	329
14.2 防火墙的应用环境与连接	325	14.2.7 用户与中心服务器的连接之间	330
14.2.1 防火墙连接策略	326	14.3 IPS 的网络应用与连接	331
		14.3.1 路由防护	331

14.3.2 交换防护	331	14.3.4 混合防护	332
14.3.3 多链路防护	331		

第 15 章 防火墙的配置

15.1 Cisco ASDM 配置	334	15.2 CLI 方式配置	348
15.1.1 Cisco ASDM 简介	334	15.2.1 网络访问控制	348
15.1.2 Cisco ASDM 初始化	337	15.2.2 PPTP 方式 VPN	353
15.1.3 DMZ 配置	338	15.2.3 L2TP 方式 VPN	355
15.1.4 IPsec VPN 远程访问配置	343	15.2.4 PPPoE 拨号配置	361
15.1.5 Site-to-Site VPN 配置	346		

第 16 章 网络设备的管理

16.1 系统和配置文件的管理	364	16.3.1 CiscoWorks 2000 安装系统需求	371
16.1.1 TFTP 服务器	364	16.3.2 安装 CiscoWorks 2000	372
16.1.2 配置文件的获取与备份	364	16.3.3 对设备的监控与管理	373
16.1.3 配置文件的恢复与更新	365	16.3.4 连接测试工具	375
16.1.4 备份系统软件映像	366	16.3.5 查看设备信息	375
16.1.5 恢复或升级系统软件映像	366	16.3.6 查看网络拓扑图	376
		16.3.7 查看失败设备	377
16.2 恢复网络设备密码	367	16.4 网络流量监控	378
16.2.1 密码的类型	367	16.4.1 网络设备吞吐率测试	378
16.2.2 密码丢失后的恢复	368	16.4.2 网络带宽测试	380
16.3 Cisco 网络设备管理	371	16.4.3 网络流量实时监控	381

第 17 章 网络故障的诊断与排除

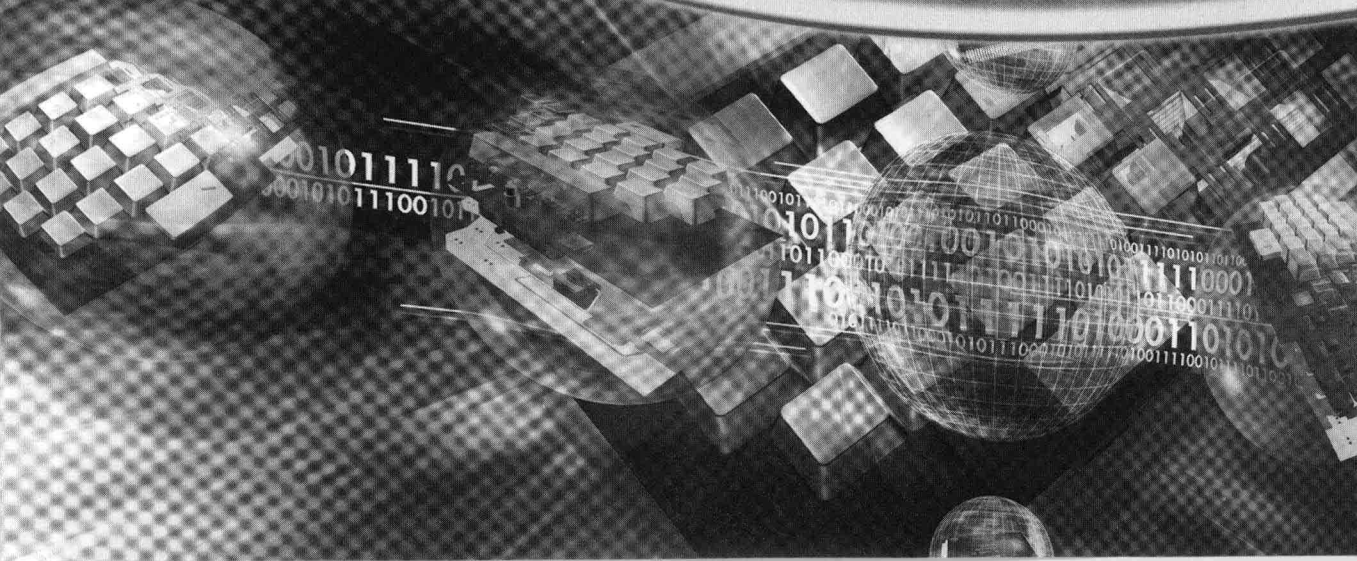
17.1 故障主要原因与现象	387	17.4 网络链路故障	398
17.1.1 网络链路	387	17.4.1 物理链路故障	398
17.1.2 配置文件和选项	387	17.4.2 逻辑链路故障	400
17.1.3 网络协议	388	17.5 网卡和网络协议故障	402
17.1.4 网络服务故障	388	17.5.1 网卡故障	402
		17.5.2 网络协议故障	403
17.2 网络故障排除过程	388	17.6 交换机故障诊断	404
17.2.1 识别故障现象	389	17.6.1 交换机故障诊断方法	404
17.2.2 对故障现象进行详细描述	389	17.6.2 交换机故障诊断顺序	406
17.2.3 列举可能导致错误的原因	389	17.6.3 电源故障	408
17.2.4 缩小搜索范围	389	17.6.4 端口故障	409
17.3 故障诊断与排错	390	17.6.5 模块故障	410
17.3.1 链路故障	390	17.6.6 背板故障	411
17.3.2 协议故障	392	17.6.7 引擎故障	411
17.3.3 配置故障	393	17.6.8 线卡故障	412
17.3.4 服务器故障	394	17.6.9 系统故障	413
17.3.5 网络拓扑故障	397	17.6.10 配置错误	414

第1章

网络设备综述

内容提要

- 1.1 交换机概述
- 1.2 路由器概述
- 1.3 防火墙概述
- 1.4 网络设备在网络中的应用





刘老师：在以前的图书当中，我给大家介绍局域网基础知识、网络组建、网络管理以及网络故障排除等内容。那些知识可以帮助读者成为一名合格网络管理员。但是如果要想成为网络高手，在知识层面上还有一些差距，在本书当中，我们就将重点放在提高网管员知识层次与技术水平方面。

交换机、路由器和防火墙是大多数局域网都要使用的基本设备。其中，交换机将其他网络设备（如集线器、交换机、路由器等）和所有终端设备（如计算机、服务器、网络打印机等）连接在一起，实现彼此之间的通讯。路由器用于实现局域网之间，以及局域网与 Internet 的互联，将所有的网络连接在一起。防火墙则用于在内部网络之间，以及内部网络和 Internet 之间创建一个安全屏障，将恶意攻击阻拦在内部网络之外。可见，对于任何局域网而言，交换机、路由器和防火墙一个都不能少。这里就让我们看看它们的基础知识。



1.1 交换机概述

随着网络技术和制造技术的不断发展，传统的集线设备——集线器（Hub）已经退出历史舞台，而交换机（Switch）则牢牢地占据了 90% 以上的市场份额。

1.1.1 交换机的功能

交换机是构建局域网不可或缺的集线设备。其主要功能包括：

1. 连接设备

所谓局域网（Network），简单地说，其实就是若干计算机的集合。而这些计算机就是借助交换机才能相互连接在一起，因此，交换机往往拥有数量众多的端口（通常为 8~48 个端口）。如图 1-1 所示为 Cisco Catalyst 2950 系列网络交换机。

交换机最主要功能就是连接计算机、服务器、网络打印机、网络摄像头、IP 电话等终端设备，并实现与其他交换机、无线接入点、路由器等网络设备的互联，从而构建局域网，实现所有设备之间的通讯。如图 1-2 所示为交换机与终端设备和网络设备的连接。

作为局域网的核心与枢纽，交换机的性能决定着网络性能，交换机的带宽决定着网络带宽。因此，局域网的升级往往就是交换机的升级。当然，前提条件是网络布线必须能够满足网络传输的需要。

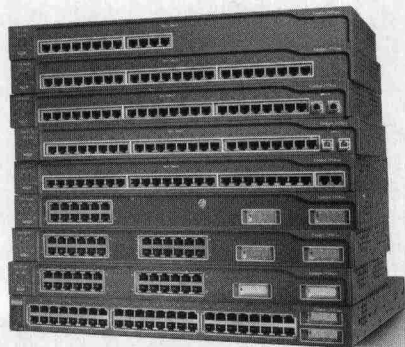


图 1-1 Cisco Catalyst 2950 系列网络交换机

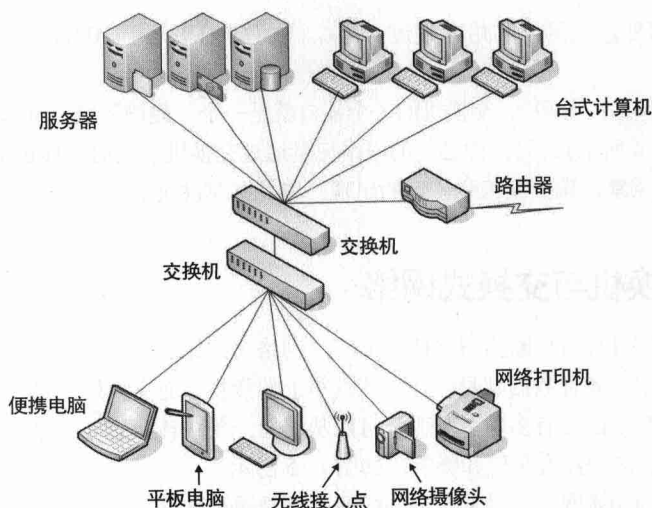


图 1-2 交换机的功能

2. 隔离碰撞

以太网的工作机制为先侦听后讲话，类似于会议讨论时的自由发言。当某个人想发表自己的言论时，首先要先听一听（即“侦听”，Carrier Sense）有没有其他人正在讲话。如果有，就再等待一段时间；如果没有，就立即起立发言。如果碰巧有两个人同时开口（即“碰撞”，Collision Detect），那么，两个人就会同时坐下，然后，稍等片刻后，其中一人再起立发言。这种机制虽然保证了同一时刻只有一个人在发言，从而使得每个人都能够清楚地听到这个人的讲话。但是，问题也随之出现了：

- 第一，当两个人需要私下交流时，也将占用大家的发言时间；
- 第二，当多个人需要相互交流时，只能耐心等待其他人讲话，而不能同时进行；
- 第三，人数越多，同时发言的可能性就越大，浪费的时间就越多。

由集线器构建的网络就是这样一个低效率的广播网络。对于集线器而言，它对连接到自己身上的电脑一点儿也不认识，它的任务就是将一个端口传来的数据广播到其它所有的端口上，如图 1-3 所示。至于究竟是哪一台电脑应该接收数据，由这些电脑自己来决定，如果是自己的就接收，不是自己的就扔掉不管。由于集线器中只能同时存在一个广播，所以，同一时刻只能有两个端口传递数据。同时，不断地碰撞将耽误大量的宝贵的传输时间，从而降低网络的传输效率。

由此可见，如果网络中拥有大量的用户、繁忙的应用程序和各式各样的服务器，那么，整个网

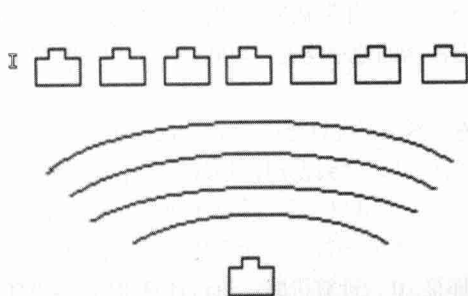


图 1-3 低效的广播网络

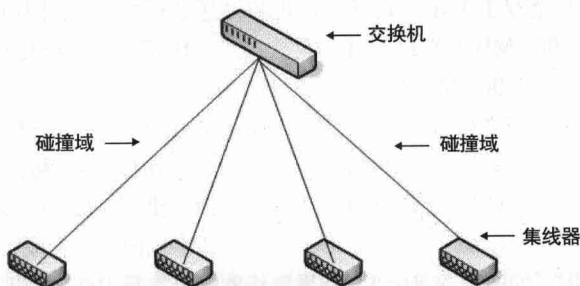


图 1-4 隔离碰撞域



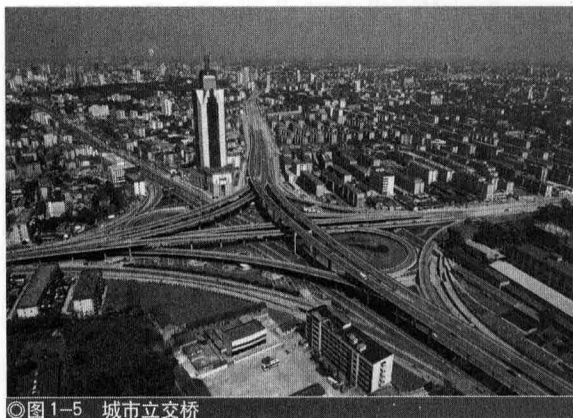
络的性能可能会非常低。当网络利用率超过 40%，并且碰撞率大于 10% 时，交换机可以有效地解决这一问题。

交换机也可以将网络“分段”。交换机的每个端口就是一个“碰撞”域，可以将碰撞有效地隔离在每个端口内（如图 1-4 所示），只允许必要的网络流量通过交换机。同时，通过交换机的过滤和转发，可以有效的隔离广播风暴，减少误包和错包的出现，避免共享冲突。

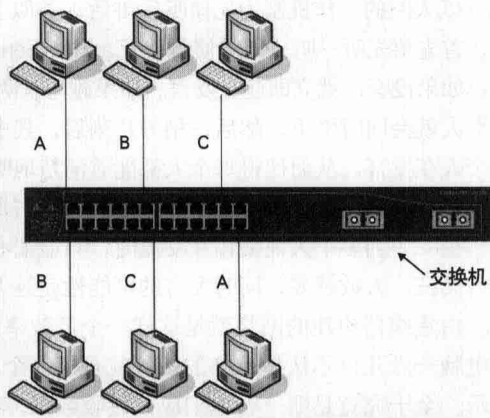
1.1.2 交换机与交换式网络

我们可以形象地把计算机比喻为写字楼或工厂，网络布线比喻为城市马路或高速公路，网络应用比喻为不同类型的汽车，各种数据则是装在这些汽车上的货物，而交换机就是连接来自所有道路的立交桥。毫无疑问，立交桥都拥有多向多车道，可以从任何一条路转向另外其他一条路，而且所有车辆都可以自行其道，相互之间没有阻碍和影响，如图 1-5 所示。

而由交换机构建的局域网络，计算机之间的通讯也是同时进行，彼此互不影响，并且每个通讯都可以“独享”带宽，即拥有端口所能提供的传输速率。这就好像在限速 80 km/h 的立交桥上，每辆车都可以占用一个车道，都可以跑到 80 km/h。如图 1-6 所示为 6 台计算机同时通讯的情形。



◎图 1-5 城市立交桥



◎图 1-6 计算机同时通讯

由交换机构建的网络称为“交换式网络”。交换式网络的工作模式通常为“全双工”（Full Duplex），即终端设备可以同时接收和发送数据，数据流是双向的（如图 1-7 所示）。对于 100 Mb/s 端口而言，在全双工工作模式下，接收和发送数据的速率均为 100 Mb/s，总带宽即可达到 200 Mb/s；对于 1 000 Mb/s 端口而言，在全双工工作模式下，接收和发送数据的速率均为 1 000 Mb/s，总带宽即可达到 2 000 Mb/s。

与之相对应，集线器（Hub）就像是一座单车道的小桥，不仅每次只允许一个方向的车辆通过，而且每次只能通行一辆汽车。对较长一段时间的网络通讯进行统计，就会发现，集线器的带宽实际上是由所有计算机来共享的。因此，由集线器构建的网络被称为“共享式网络”。共享式网络的工作模式通常为“半双工”（Half Duplex），即终端设备或者接收数据，或者发送数据，而不能同时接收和发送数据（如图 1-8 所示）。如果集线器的带宽是 100 Mb/s，当连接 10 台计算机时，每台计算机所能分享的带宽为 10 Mb/s；而当连接 20 台计算机时，每台计算机所能分享的带宽就只有区区的 5 Mb/s 了。

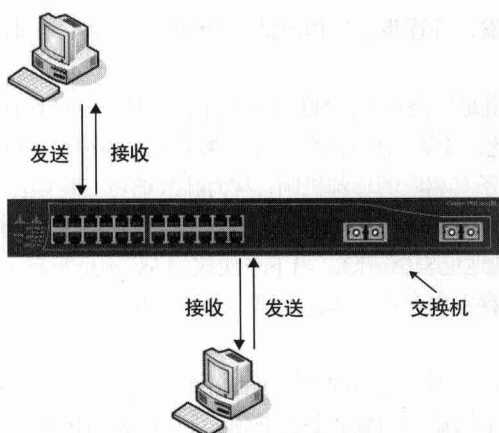


图 1-7 全双工示意图

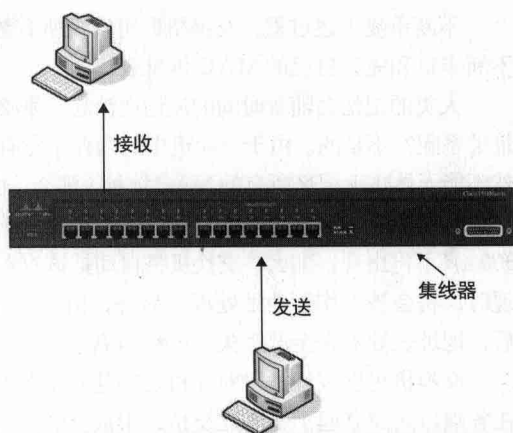


图 1-8 半双工示意图

1.1.3 交换机的工作原理

交换机位于 OSI 模型中的链路层（即第 2 层），是一种基于 MAC 地址（Media Access Control，介质访问控制）识别，完成数据的封装和转发的网络设备。交换机可以“学习” MAC 地址，并把其存放在内部地址表中，通过在数据帧的始发者和目标接收者之间建立临时的交换路径，使数据帧直接从源地址到达目的地址。因此，交换机就像是一个业务熟练的调度员，能够准确地将装载数据的汽车从出发路口直接派到达目的地路口。当然，要完成这样繁重和智能化的工作，交换机也需要一个学习和记忆的过程。

计算机借助网卡连接到局域网络，而每块网卡都有与生俱来的“胎记”——MAC 地址。交换机通过“学习”，会把连接到每个端口的 MAC 地址记住，形成一个端口与 MAC 地址对应表。

交换机的工作过程如下：

第一步，当交换机从某个端口收到一个数据包，先读取包头中的源 MAC 地址，从而建立源端口与源 MAC 地址的对应关系，并将其添加至地址表。由于交换机能够自动根据收到的以太网帧中的源 MAC 地址更新地址表的内容，所以，交换机使用的时间越长，学习到的 MAC 地址就越多，未知的 MAC 地址就越少，因而广播的包就越少（如果目的 MAC 地址未知，则将该包作广播包处理），处理速度就越快。

第二步，读取包头中的目的 MAC 地址，并在地址表中查找相应的端口。

第三步，如果地址表中有与这目的 MAC 地址对应的端口，把数据包直接复制到该端口上。由于不是将该帧发送到所有端口，从而使那些既非源端口又非目的端口的端口间仍然可以进行相互间的通信，从而提供了更高的传输速率。

第四步，如果在 MAC 地址表中没有找到该 MAC 地址，也就是说，该目的 MAC 地址是首次出现，则将该帧发送到所有其它端口（源端口除外），相当于该帧是一个广播帧。拥有该 MAC 地址的网卡在接收到该广播帧后，将立即做出应答，从而使交换机将“端口号-MAC 地址”对照表添加到地址表。



刘老师提醒

MAC 地址是识别局域网节点的标识，所有网络设备（包括每块网卡、交换机和路由器的每个端口）都有一个唯一的 MAC 地址，通常是由网卡生产厂家直接烧入 EPROM 中，是传输数据时真正赖以标识发出数据的设备和接收数据的设备的标志。



不断重复上述过程，交换机即可实现所有数据的转发，并逐步学习和记忆整网络中的 MAC 地址，不断丰富和完善自己的 MAC 地址表。

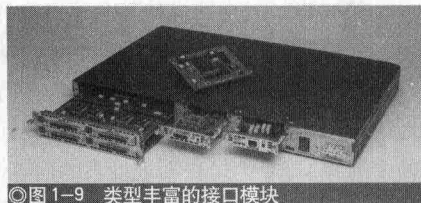
人类的记忆会随着时间的流逝而淡忘。那么，交换机是否会永久性地记住所有的端口号—MAC 地址关系呢？不是的。由于交换机中的内存毕竟有限，因此，能够记忆的 MAC 地址数量也是有限的。既然不能无休止地记忆所有的 MAC 地址，那么，也必须赋予其相应的忘却机制，从而吐故纳新。事实上，交换机设计了一个自动老化时间（Auto-aging Time）机制，若某 MAC 地址在一定时间内（默认为 300 s）不再出现，那么，交换机将自动把该 MAC 地址从地址表中清除。当下一次该 MAC 地址重新出现时，将会被当作新地址处理。另外，由于地址表是保存在内存中，因此，当交换机断电或重新启动后，地址表数据将全部丢失，必须重新学习。

交换机可以在任意一对端口之间建立临时专用通道，不同端口间的转发可以并行操作。这就像是在各端口间建立起了一座立交桥，形成立体交叉结构，不同流向的数据各行其道，每个端口均能够独享固定带宽，传输速率几乎不受计算机数量增加影响。另外，当两个或两个以上的端口与同一目的端口进行通讯时，交换机将把这些数据帧暂时保存在缓存中，然后，根据顺序对其逐一处理和转发，从而实现“多”对“一”的通讯。

由此可见，交换机的工作过程可以概括为“学习——记忆——接收——查找——转发”。通过广播方式“学习”网卡 MAC 地址，并将“MAC 地址—端口号”的对应关系创建一个地址表“记忆”在内存中。从源端口“接收”到数据后，在地址表中“查找”与目的 MAC 地址相对应的端口，然后，将数据帧“转发”至目的端口。

1.2 路由器概述

路由器是一种用于连接多个网络。以路由器为基础构建（Router Based Network）的网络称为“网间网”。事实上，Internet 就是由数以万计的路由器构建的、超大规模的、国际性的“网间网”。虽然严格意义上讲，路由器是广域网设备，但是，作为局域网实现与其他网络和 Internet 互联的必需设备，也往往被归类于局域网设备之列。



◎图 1-9 类型丰富的接口模块

1.2.1 路由器的功能

路由器（Router），顾名思义，是一种智能选择数据传输路由的设备。路由器的端口数量虽然较少，但是，种类却非常丰富，可以满足各种类型网络接入的需要。如图 1-9 所示为 Cisco 2621 路由器及其类型丰富的接口模块。

1. 连接网络

路由器也称为网关（Gateway）。将局域网络连接在一起，组建更大规模的广域网络，并在每个局